

# ENQUETE-KOMMISSION INTERNET UND DIGITALE GESELLSCHAFT

## DATENSCHUTZ, PERSÖNLICHKEITSRECHTE ZWISCHENBERICHT (STAND: 10. OKTOBER 2011)

BERATUNGSUNTERLAGE FÜR DIE 13. SITZUNG DER ENQUETE-KOMMISSION INTERNET UND DIGITALE GESELLSCHAFT  
AM 17. OKTOBER 2011

### WICHTIGE HINWEISE:

Das Dokument enthält

- alle in der Sitzung der Enquete-Kommission am 11. April bereits verabschiedeten Berichtsteile
- alle in der Sitzung der Enquete-Kommission am 17. Oktober noch zu beratenden Texte, d. h. den Abschnitt 2.1.10 (S. 42 – 46), Kapitel 3 (S. 79 – 129) und Kapitel 5 (ab S. 130).

Die noch zu beratenden Texte sind durch einen Rahmen optisch hervorgehoben. Zusätzliche Hinweise (auf die Antragsteller, streitiger oder unstreitiger Textvorschlag etc.) finden sich oberhalb des jeweiligen Rahmens.

Um die Beratung der Texte zu erleichtern, sind korrespondierende oder alternative Textpassagen verschiedener Antragsteller hintereinander aufgeführt. Um eine *inhaltliche* Zuordnung zu ermöglichen, sind Handlungsempfehlungen in Einzelfällen abweichend von der *Reihenfolge* in den Originaldokumenten aufgenommen worden.

## 29 Inhaltsverzeichnis

30	<b>1</b>	<b>BESTANDSAUFNAHME BESTEHENDER DATENSCHUTZREGELUNGEN .....</b>	<b>4</b>
31	1.1	VÖLKERRECHT .....	4
32	1.1.1	<i>Allgemeine völkerrechtliche Abkommen zum Schutz der Menschenrechte .....</i>	4
33	1.1.2	<i>Datenschutz in völkerrechtlichen Spezialregelungen .....</i>	5
34	1.2	EUROPARECHT .....	7
35	1.2.1	<i>Europäisches Primärrecht.....</i>	7
36	1.2.2	<i>Europäisches Sekundärrecht .....</i>	9
37	1.2.3	<i>Rechtsprechung des Europäischen Gerichtshofs .....</i>	13
38	1.3	NATIONALES RECHT.....	15
39	1.3.1	<i>Grundrechte.....</i>	15
40	1.3.2	<i>Einfaches Bundesrecht.....</i>	17
41	1.3.3	<i>Landesrecht .....</i>	19
42	1.3.4	<i>Rechtsprechung des Bundesverfassungsgerichts .....</i>	19
43	1.3.5	<i>Rechtsprechung nationaler Verwaltungs- und Zivilgerichte.....</i>	22
44	1.3.6	<i>Verwaltungs- und Anwendungspraxis.....</i>	25
45	<b>2</b>	<b>DATENSCHUTZ .....</b>	<b>25</b>
46	2.1	PRINZIPIEN, ZIELE, WERTE.....	25
47	2.1.1	<i>Schutzgegenstand .....</i>	25
48	2.1.2	<i>Grundprinzipien des Datenschutzrechts.....</i>	27
49	2.1.3	<i>Datenschutz im Grundgesetz.....</i>	30
50	2.1.4	<i>Das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts ..</i>	32
51	2.1.5	<i>Einschränkungen von Grundrechten / Kollidierende Rechtsgüter .....</i>	33
52	2.1.6	<i>Anonymität und Identitätsmanagement im Internet .....</i>	38
53	2.1.7	<i>Sicherheit von Daten/Technischer Datenschutz .....</i>	38
54	2.1.8	<i>Selbstdatenschutz und Medienkompetenz.....</i>	39
55	2.1.9	<i>Die Grenzen des nationalen Datenschutzes .....</i>	40
56	2.2	DATENSCHUTZ IM ÖFFENTLICHEN BEREICH .....	47
57	2.2.1	<i>Datenschutz in öffentlichen Einrichtungen.....</i>	47
58	2.2.1.1.	<i>Einführung .....</i>	47
59	2.2.1.2.	<i>Das Bundesdatenschutzgesetz (BDSG) .....</i>	48
60	2.2.1.3.	<i>Staatliche Datenverarbeitung im Wandel.....</i>	49
61	2.2.1.4.	<i>Herausforderungen für das Datenschutzrecht in öffentlichen Einrichtungen.....</i>	50
62	2.2.1.5.	<i>Cloud Computing in der öffentlichen Verwaltung .....</i>	52
63	2.2.2	<i>Mögliche Erweiterung des Grundgesetzes im Hinblick auf das Grundrecht auf informationelle</i>	
64		<i>Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer</i>	
65		<i>Systeme 53</i>	
66	2.2.3	<i>Datensicherheit .....</i>	54
67	2.2.4	<i>Datenschutzaudit und Gütesiegel zum Zwecke der Vertrauensbildung .....</i>	55
68	2.3	DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH.....	55
69	2.3.1	<i>Datennutzung als Bestandteil innovativer Dienste.....</i>	55
70	2.3.1.1.	<i>Datenschutz in der Informations- und Kommunikationsgesellschaft: Zum Spannungsverhältnis und Gebot der</i>	
71		<i>Abwägung zwischen Persönlichkeitsrechten und Kommunikationsgrundrechten .....</i>	55
72	2.3.1.2.	<i>Geschäftsmodelle von Internet-Diensten / Online-Werbung.....</i>	59
73	2.3.1.3.	<i>Bildung von Persönlichkeitsprofilen / Tracking über die Grenzen einzelner Webseiten hinweg .....</i>	61
74	2.3.2	<i>Ausgestaltung und Reichweite von Transparenzinstrumenten (Informationspflichten, Auskunftsrechte) ...</i>	63
75	2.3.3	<i>Cloud Computing .....</i>	65
76	2.3.4	<i>„Verfallsdaten“ im Internet, regelmäßig erneuerbare Zustimmungspflicht.....</i>	68

77	2.3.5	„Privacy by design“ („privacy by design“ / „privacy by default“)	70
78	2.3.6	Datenweitergabe und -handel	70
79	2.3.7	Spannungsfeld Datenschutz und Wettbewerbsbedingungen am Beispiel sozialer Netzwerke	73
80	2.3.8	Datenschutz als Standortfaktor	74
81	2.3.9	Selbstverpflichtungen und Selbstregulierungen der Internetwirtschaft	74
82	2.3.10	Übertragbarkeit der regulierten Selbstregulierung auf den Bereich des Datenschutzes	75
83	2.3.11	Schadensersatzansprüche im Datenschutzrecht	76
84	2.3.12	Beschäftigtendatenschutz	77
85	2.3.13	Probleme der föderalen Aufsichtsstruktur	77
86	<b>3</b>	<b>HANDLUNGSEMPFEHLUNGEN</b>	<b>79</b>
87	3.1	VORGABEN FÜR NATIONALEN, EUROPÄISCHEN UND INTERNATIONALEN DATENSCHUTZ	81
88	3.2	DATENSCHUTZ ALS STANDORTFAKTOR	84
89	3.3	EINWILLIGUNG	85
90	3.4	AGB UND DATENSCHUTZ	86
91	3.5	PRIVACY BY DESIGN / BY DEFAULT	86
92	3.6	VERFALLSDATEN	87
93	3.7	SELBSTDATENSCHUTZ UND MEDIENKOMPETENZ	88
94	3.8	SOZIALE NETZWERKE	88
95	3.9	DATENSCHUTZAUFSICHT	90
96	3.10	VORBILDWIRKUNG ÖFFENTLICHER IT-PROJEKTE	91
97	3.11	SMARTGRIDS UND ANDERE INTELLIGENTE NETZE	93
98	<b>4</b>	<b>SONDERVOTEN (ZU ERGÄNZEN)</b>	<b>129</b>
99	<b>5</b>	<b>BÜRGERBETEILIGUNG IN DER PROJEKTGRUPPE DATENSCHUTZ, PERSÖNLICHKEITSRECHTE</b>	<b>130</b>
100	5.1	BÜRGERBETEILIGUNG IM FORUM ZUM THEMA EINWILLIGUNG	130
101	5.2	BÜRGERBETEILIGUNG AUF DER ONLINE-BETEILIGUNGSPLATTFORM DER ENQUETE-KOMMISSION	131
102			

# 103 **1 Bestandsaufnahme bestehender Datenschutzregelungen<sup>1</sup>**

## 104 **1.1 Völkerrecht**

### 105 1.1.1 Allgemeine völkerrechtliche Abkommen zum Schutz der Menschenrechte

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

109 So hat nach Art. 8 der Europäischen Menschenrechtskonvention<sup>2</sup> (EMRK) „jede Person [...] das  
 110 Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“. Der  
 111 Schutz des Privatlebens umfasst auch den Schutz persönlicher, insbesondere medizinischer oder  
 112 sozialer Daten.<sup>3</sup> Als Korrespondenz im Sinne von Art. 8 EMRK gelten auch die  
 113 Individualkommunikation mittels E-Mail, Telefon und Internettelefonie.<sup>4</sup> Staatliche Eingriffe sind nur  
 114 auf gesetzlicher Grundlage unter den in der Vorschrift genannten Voraussetzungen zulässig, zum  
 115 Beispiel zur Verhütung von Straftaten oder zum Schutz der Rechte und Freiheiten anderer. Die  
 116 Regelung stellt nicht nur ein Abwehrrecht gegen staatliche Eingriffe dar, sie begründet auch staatliche  
 117 Schutz- und Handlungspflichten, etwa zum Erlass entsprechender Regelungen.<sup>5</sup> Nach Art. 1 EMRK  
 118 sichern die Vertragsparteien dieses völkerrechtlichen Vertrages allen ihrer Hoheitsgewalt  
 119 unterstehenden Personen unter anderem die in Art. 8 EMRK bestimmten Rechte und Freiheiten zu. In  
 120 Deutschland stellt Art. 8 EMRK unmittelbar geltendes Recht dar.

121 In ähnlicher Weise bestimmt Art. 17 des Internationalen Paktes über bürgerliche und politische Rechte  
 122 (IPBürgR)<sup>6</sup>, dass „niemand [...] willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben,  
 123 seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen  
 124 seiner Ehre und seines Rufes ausgesetzt werden“ darf. „Jedermann hat Anspruch auf rechtlichen  
 125 Schutz gegen solche Eingriffe oder Beeinträchtigungen.“ Wie bei der EMRK ist auch bei diesem  
 126 Menschenrechtsabkommen der Vereinten Nationen der Datenschutz ein Element der Privatsphäre. Die  
 127 Regelung gilt sowohl hinsichtlich staatlicher Eingriffe, als auch bei Eingriffen Privater. Die  
 128 Vertragsstaaten, darunter die Bundesrepublik Deutschland, sind verpflichtet, Rechtsschutz gegenüber  
 129 staatlichen Eingriffen zu ermöglichen und Regelungen zum Schutz vor privaten Eingriffen zu treffen.<sup>7</sup>

130

---

<sup>1</sup> Stand: 7. April 2011.

<sup>2</sup> Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, BGBl. II 1952, S. 686.

<sup>3</sup> Vgl. Meyer-Ladewig, Jens: EMRK, Handkommentar. 3. Auflage 2011, Art. 8 EMRK Rn. 40.

<sup>4</sup> Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 37.

<sup>5</sup> Vgl. Meyer-Ladewig, Jens: EMRK, Handkommentar. 3. Auflage 2011, Art. 8 EMRK Rn. 2.

<sup>6</sup> Internationaler Pakt über bürgerliche und politische Rechte vom 19. Dezember 1966, BGBl. II 1973, S. 1533.

<sup>7</sup> Vgl. Hofmann, Rainer/Boldt, Nicki: Kommentar zu dem Internationalen Pakt über bürgerliche und politische Rechte, in: Köble, Josef (Hrsg.). Das Deutsche Bundesrecht - Systematische Sammlung der Gesetze und Verordnungen mit Erläuterungen. Hauptband 1949, Erl. zu Art. 17 IPbR.

131 Art. 16 der so genannten Kinderrechtskonvention<sup>8</sup> („Schutz der Privatsphäre“) deckt sich im Wortlaut  
 132 mit Art. 17 IPBürgRG. Träger der gewährten Rechte ist nach Art. 16 des Kinderrechte-  
 133 Übereinkommens jedoch ausdrücklich das Kind.

134 Da bei den vorgenannten Menschenrechtsabkommen der Datenschutz nur als Teil des Schutzes des  
 135 Privatlebens anzusehen und daher sehr allgemein ausgeprägt ist, ergeben sich datenschutzspezifische  
 136 Details allenfalls aus Einzelfallentscheidungen der jeweils zuständigen Instanzen. Allerdings enthält  
 137 gerade die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) zu Art. 8  
 138 EMRK zahlreiche Hinweise auf den Schutzbereich des Datenschutzes und entsprechende  
 139 Eingriffsvoraussetzungen.

140 In dem jüngeren Übereinkommen über die Rechte von Menschen mit Behinderungen der Vereinten  
 141 Nationen (Behindertenrechtskonvention – BRK)<sup>9</sup> werden in Art. 22 („Achtung der Privatsphäre“), der  
 142 in seinem sonstigen Wortlaut weitgehend Art. 17 IPBürgR entspricht, Fragen der informationellen  
 143 Selbstbestimmung und des Datenschutzes ausdrücklich thematisiert. So sind neben dem  
 144 Schriftverkehr ausdrücklich auch „andere Arten der Kommunikation“ vor willkürlichen und  
 145 rechtswidrigen Eingriffen geschützt. Außerdem erklären die Vertragsstaaten, „auf der Grundlage der  
 146 Gleichberechtigung mit anderen die Vertraulichkeit von Informationen über die Person, die  
 147 Gesundheit und die Rehabilitation von Menschen mit Behinderungen“ zu schützen.

#### 148 1.1.2 Datenschutz in völkerrechtlichen Spezialregelungen

149 Die „Leitlinien der OECD für den Schutz des Persönlichkeitsrechts und den grenzüberschreitenden  
 150 Verkehr personenbezogener Daten“<sup>10</sup>, bei denen es sich nicht um einen völkerrechtlichen Vertrag,  
 151 sondern um eine Empfehlung an die Mitgliedstaaten der Organisation handelt, stellen einen frühen  
 152 Versuch dar, Datenschutz, freien Informationsfluss und freien Handelsverkehr in Ausgleich zu  
 153 bringen. Da neben EU-Mitgliedern u. a. die USA Mitglied der OECD sind, waren hierbei europäische  
 154 und US-amerikanische Ansätze des Datenschutzes zu berücksichtigen.<sup>11</sup> In den Leitlinien wird  
 155 zwischen „sensitiven“ und „trivialen“ Angaben<sup>12</sup>, von denen offensichtlich keine Gefahr ausgeht,  
 156 unterschieden. Letztere können von der Anwendung der Leitlinien ausgeschlossen werden. Neben  
 157 verschiedenen Verarbeitungsgrundsätzen für den innerstaatlichen Bereich enthalten die Leitlinien  
 158 Empfehlungen zur Sicherung des freien Informationsflusses zwischen Mitgliedstaaten. So soll etwa  
 159 auf unangemessen hohe Datenschutzregelungen, die den grenzüberschreitenden Datenverkehr  
 160 behindern, verzichtet werden. Der Selbstregulierung wird gleicher Stellenwert wie der (nationalen)  
 161 Gesetzgebung eingeräumt.<sup>13</sup> Die Leitlinien gelten als „Indiz für die internationale Verbreitung  
 162 bestimmter Datenschutzgrundsätze“<sup>14</sup>, die jedoch weder völkerrechtliche Verbindlichkeit noch einen

---

<sup>8</sup> Übereinkommen der Vereinten Nationen über die Rechte des Kindes vom 20. November 1989, BGBl. II 1992, S. 122.

<sup>9</sup> Übereinkommen über die Rechte von Menschen mit Behinderungen vom 13. Dezember 2006, BGBl. II 2008, S. 1419.

<sup>10</sup> OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data vom 23. September 1980, Bundesanzeiger Nr. 251 vom 14. November 1981.

<sup>11</sup> Vgl. Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 36.

<sup>12</sup> Vgl. Simitis, Spiros, in: ders. (Hrsg.). Bundesdatenschutzgesetz. 6. Auflage 2006, Einleitung Rn. 186.

<sup>13</sup> Vgl. Simitis, Spiros, in: ders. (Hrsg.). Bundesdatenschutzgesetz. 6. Auflage 2006, Einleitung Rn. 198.

<sup>14</sup> Ennulat, Mark: Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und –einrichtungen. 2008, S. 72.

163 hohen Schutzstandard aufweisen. Dessen ungeachtet sollen sie jedoch auch dazu beigetragen haben,  
 164 „den Datenschutz als Gegenstand internationaler Regulierung zu etablieren.“<sup>15</sup>

165 Die Europäische Datenschutzkonvention des Europarates<sup>16</sup> begründet hingegen rechtliche  
 166 Verpflichtungen der Unterzeichnerstaaten, einen bestimmten Katalog von Datenschutzgrundsätzen  
 167 einzuhalten und in nationales Recht umzusetzen.<sup>17</sup> Dazu gehört insbesondere die Einhaltung  
 168 bestimmter Verarbeitungsgrundsätze nach Art. 5 des Übereinkommens, die zugleich einen Kanon der  
 169 heute noch gültigen Grundregeln des Datenschutzes darstellen. Personenbezogene Daten, die im  
 170 öffentlichen oder nicht-öffentlichen Bereich automatisch verarbeitet werden, müssen nach Treu und  
 171 Glauben und auf rechtmäßige Weise beschafft und verarbeitet werden. Die Speicherung und  
 172 Verwendung ist nur für festgelegte, rechtmäßige Zwecke zulässig. Die Daten müssen im Sinne des  
 173 Verhältnismäßigkeitsgrundsatzes diesen Zwecken entsprechen und dürfen nicht darüber hinaus gehen.  
 174 Die sachliche Richtigkeit der Daten, gegebenenfalls durch spätere Aktualisierung, ist genauso  
 175 vorgeschrieben wie die Anonymisierung der Daten nach Zweckerfüllung. Das Übereinkommen sieht  
 176 weiterhin ein spezifisches Schutzniveau für besonders sensible Daten (etwa über politische  
 177 Anschauungen oder Gesundheitsdaten) und bestimmte Rechte der Betroffenen vor. Nach Art. 1 des  
 178 Zusatzprotokolls „betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr“ vom 8.  
 179 November 2001<sup>18</sup> sind unabhängige Kontrollstellen einzurichten, die insbesondere die Einhaltung der  
 180 in nationales Recht umgesetzten Grundsätze für den Datenschutz gewährleisten sollen. Sie nehmen  
 181 ihre Aufgaben „in völliger Unabhängigkeit“ wahr. Das Zusatzprotokoll beschränkt weiterhin in Art. 2  
 182 die Datenübermittlung in Staaten, die nicht Mitglied des Übereinkommens sind. Sie ist nur dann  
 183 zulässig, wenn im Empfängerstaat ein „angemessenes Schutzniveau“ gewährleistet ist. Die  
 184 Weitergabe der Daten kann aber beispielsweise auch dann erlaubt werden, wenn vertragliche  
 185 Garantien von der zuständigen Behörde für ausreichend befunden wurden.

186 Die Cybercrime Convention des Europarates vom 23. November 2001<sup>19</sup> enthält strafrechtliche  
 187 Mindeststandards bei Angriffen auf Computer- und Telekommunikationssysteme sowie ihrem  
 188 Missbrauch zur Begehung von Straftaten, Vorgaben zu strafprozessualen Maßnahmen, zur  
 189 Durchsuchung und Beschlagnahme bei solchen Straftaten und Regelungen zur Verbesserung der  
 190 internationalen Zusammenarbeit einschließlich der Rechtshilfe bei deren Verfolgung.<sup>20</sup>

---

<sup>15</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 36.

<sup>16</sup> Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981, BGBl. II 1985, S. 538.

<sup>17</sup> 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.

<sup>18</sup> Zusatzprotokoll zu dem Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 8. November 2001, BGBl. II 2002, S. 1882.

<sup>19</sup> 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.

<sup>20</sup> Vgl. Denkschrift zu dem Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (I. Allgemeines), BT-Drs. 16/7218, S. 40.

191

192 Als datenschutzrechtliche Spezialregelung mit globalem Anwendungsbereich kann der Beschluss der  
 193 Generalversammlung der Vereinten Nationen vom 14. Dezember 1990 über „Richtlinien betreffend  
 194 personenbezogene Daten in automatisierten Dateien“ gelten.<sup>21</sup> Die Richtlinien, die jedoch ein  
 195 niedrigeres Datenschutzniveau aufweisen als die oben genannten Abkommen, haben lediglich den  
 196 Charakter einer Empfehlung.

## 197 1.2 Europarecht

### 198 1.2.1 Europäisches Primärrecht

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

201 Die grundsätzliche Regelung findet sich im Vertrag über die Arbeitsweise der Europäischen Union  
 202 (AEUV). Sie ist mit Art. 16 AEUV an herausgehobener Stelle im Titel II (Allgemein geltende  
 203 Bestimmungen) verortet und soll so gewährleisten, dass der Datenschutz bei sämtlichen in den EU-  
 204 Verträgen erfassten Bereichen und Politiken gilt.<sup>22</sup> Art. 16 AEUV [Datenschutz] lautet:

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

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

212 Art. 16 AEUV enthält in Absatz 1 erstmals ein primärrechtliches Grundrecht des Datenschutzes<sup>23</sup>, das  
 213 sowohl gegenüber den Organen, Einrichtungen und sonstigen Stellen der EU gilt als auch gegenüber  
 214 den Mitgliedstaaten, soweit sie im Anwendungsbereich des Unionsrechts handeln. Korrespondierend  
 215 zu diesem Rechtsanspruch auf Datenschutz ist in Absatz 2 erstmals auf primärrechtlicher Ebene eine  
 216 einzige und allgemeine Rechtsetzungsbefugnis der EU ausschließlich zum Schutz personenbezogener  
 217 Daten normiert. So werden das Europäische Parlament und der Rat der EU im Bereich des  
 218 Datenschutzes ermächtigt, Gesetzgebungsakte nach dem ordentlichen Gesetzgebungsverfahren zu  
 219 beschließen.<sup>24</sup>

---

<sup>21</sup> Guidelines on the Use of Computerized Personal Data Flow, Resolution der Generalversammlung vom 14. Dezember 1990, UN Doc. A/Res/45/95.

<sup>22</sup> Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Auflage 2010, Art. 16 AEUV Rn. 7.

<sup>23</sup> Vgl. 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.

<sup>24</sup> 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, Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, Dok.-Nr. 6655/08, vom 15. April. 2008.

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

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

229 Art. 39 EUV knüpft an die allgemeine Vorschrift des Art. 16 AEUV an, verlangt aber für die nähere  
 230 Regelung des Datenschutzes im Bereich der Gemeinsamen Außen- und Sicherheitspolitik ein anderes  
 231 Verfahren der Rechtsetzung, und zwar einen Beschluss des Rates.<sup>25</sup>

232 Mit dem Vertrag von Lissabon wurde schließlich die Charta der Grundrechte der Europäischen  
 233 Union<sup>26</sup> (GRC) im Dezember 2009 rechtsverbindlich. Sie steht nun auf gleicher Hierarchiestufe wie  
 234 das Primärrecht.<sup>27</sup> Die Vorschrift des Art. 8 GRC, die parallel zu Art. 16 AEUV den Schutz  
 235 personenbezogener Daten regelt, stimmt in ihrem Abs. 1 wörtlich mit Art. 16 Abs. 1 AEUV überein;  
 236 Abs. 2 formt das unionale Grundrecht näher aus.<sup>28</sup> Art. 8 GRC („Schutz personenbezogener Daten“) lautet:

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

239 (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der  
 240 betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet  
 241 werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten  
 242 und die Berichtigung der Daten zu erwirken.

243 (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

244 Das Grundrecht auf Datenschutz gemäß Art. 8 GRC verpflichtet nach Art. 51 Abs. 1 S. 1 GRC  
 245 zunächst die Organe und Einrichtungen der EU bei sämtlichen ihrer Aktivitäten; es gibt keinen  
 246 grundrechtsfreien Raum in der EU.<sup>29</sup> Darüber hinaus sind auch die Mitgliedstaaten auf das unionale  
 247 Grundrecht auf Datenschutz „bei der Durchführung des Rechts der Union“ gemäß Art. 51 Abs. 1 S. 1  
 248 GRC verpflichtet.<sup>30</sup> Eine Bindung der Mitgliedstaaten an das unionale Grundrecht des Datenschutzes  
 249 ist damit in jedem Fall bei der legislativen Umsetzung von Richtlinien und beim administrativen  
 250 Vollzug von Verordnungen oder unmittelbar anwendbaren Richtlinien durch die Mitgliedstaaten  
 251 gegeben.<sup>31</sup> Nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) sind die Grundrechte der

<sup>25</sup> Vgl. Geiger, Rudolf, in: ders./Khan, Daniel-Erasmus/Kotzur, Markus. EUV/AEUV, 5. Auflage 2010, Art. 39 EUV Rn. 3.

<sup>26</sup> ABl. EU Nr. C 83 vom 30. März 2010, S. 393, in Kraft getreten am 1. Dezember 2009.

<sup>27</sup> S. Art. 6 Abs. 1 EUV.

<sup>28</sup> Vgl. 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.

<sup>29</sup> Vgl. Jarass, Hans D.: Charta der Grundrechte der Europäischen Union. 2010, Art. 51 Rn. 4.

<sup>30</sup> Vgl. hierzu Rohleder, Kristin: Grundrechtsschutz im europäischen Mehrebenen-System, 2009, S. 396 ff.

<sup>31</sup> Vgl. 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.



252 Union von den Mitgliedstaaten jedoch über die bloße Durchführung des Unionsrechts hinaus schon  
 253 dann anzuwenden, wenn eine nationale Maßnahme in den Anwendungsbereich des Unionsrechts fällt,  
 254 zum Beispiel in den Fällen, in denen die Mitgliedstaaten Grundfreiheiten des Binnenmarkts  
 255 einschränken.<sup>32</sup> Überwiegend wird in der Rechtswissenschaft davon ausgegangen, dass diese weite  
 256 Auslegung des EuGH durch das Verbindlichwerden der GRC nicht tangiert wird.<sup>33</sup> Festzuhalten  
 257 bleibt, dass das unionale Grundrecht auf Datenschutz nur dann nicht in den Mitgliedstaaten zum  
 258 Tragen kommt, wenn sie allein im Rahmen ihrer nationalen Kompetenzen agieren.<sup>34</sup>

### 259 1.2.2 Europäisches Sekundärrecht

260 Das zentrale Datenschutzinstrument auf europäischer Ebene ist die Datenschutzrichtlinie 95/46/EG<sup>35</sup>  
 261 aus dem Jahr 1995 (DSRL). Die Richtlinie verpflichtet die Mitgliedstaaten, für die Verarbeitung  
 262 personenbezogener Daten bestimmte Mindeststandards in ihre nationale Gesetzgebung zu  
 263 übernehmen. Sie zielt darauf ab, den Schutz der Privatsphäre natürlicher Personen und den  
 264 grundsätzlich erwünschten freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten in  
 265 Einklang zu bringen. Deshalb sieht die Richtlinie auch vor, dass der freie Verkehr personenbezogener  
 266 Daten zwischen den Mitgliedstaaten nicht unter Hinweis auf den Schutz der Grundrechte und  
 267 Grundfreiheiten, insbesondere des Schutzes der Privatsphäre, beschränkt oder untersagt werden darf.  
 268 Die Mitgliedstaaten können also keine Datenschutzstandards einführen, die von den in der Richtlinie  
 269 festgelegten Mindeststandards abweichen, wenn dadurch der freie Verkehr der Daten innerhalb der  
 270 EU eingeschränkt wird. Die Datenschutzrichtlinie ist nicht anwendbar auf die Verarbeitung  
 271 personenbezogener Daten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts vor dem  
 272 Vertrag von Lissabon fallen. Hierunter fallen insbesondere Tätigkeiten der Europäischen Union in den  
 273 Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (frühere 3. Säule). Eine  
 274 Anpassung der Richtlinie an die mit dem Vertrag von Lissabon bewirkte Auflösung der  
 275 Säulenstruktur ist bislang noch nicht erfolgt.<sup>36</sup>

276 Die in der Richtlinie vorgeschriebenen datenschutzrechtlichen Mindeststandards betreffen

- 277 - die Qualität der Daten (u. a. Verarbeitung nach Treu und Glauben, auf rechtmäßige Weise
- 278 sowie für festgelegte Zwecke);
- 279 - die Zulässigkeit der Datenverarbeitung (u. a. bei Einwilligung der betroffenen Person oder
- 280 Erforderlichkeit der Datenverarbeitung aus bestimmten in der Richtlinie festgelegten
- 281 Gründen);

---

<sup>32</sup> 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).

<sup>33</sup> 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).

<sup>34</sup> Vgl. Jarass, Hans D.: Charta der Grundrechte der Europäischen Union, 2010, Art. 51 Rn. 10.

<sup>35</sup> 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). Im Folgenden „Datenschutzrichtlinie“.

<sup>36</sup> Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Auflage 2010, Art. 16 AEUV Rn. 37.

- 282 - erhöhte Schutzanforderungen für besonders sensible Daten, etwa betreffend die politische  
 283 Meinung oder die religiöse Überzeugung;  
 284 - bestimmte Informationen, die der für die Verarbeitung Verantwortliche der betroffenen Person  
 285 übermitteln muss;  
 286 - Auskunftsrechte sowie Rechte auf Berichtigung, Löschung und Sperrung von Daten;  
 287 - Widerspruchsrechte;  
 288 - die Vertraulichkeit und Sicherheit der Verarbeitung;  
 289 - Meldepflichten gegenüber einer Kontrollstelle;  
 290 - Rechtsbehelfe, Haftung und Sanktionen.

291 Die Richtlinie sieht weiterhin die Einrichtung von Kontrollstellen vor, die ihre Aufgaben in völliger  
 292 Unabhängigkeit wahrnehmen und legt Grundsätze für die Übermittlung personenbezogener Daten an  
 293 Drittländer fest. Voraussetzung hierfür ist, dass der Drittstaat ein „angemessenes Schutzniveau“<sup>37</sup>  
 294 gewährleistet. Bei welchen Staaten dies der Fall ist, entscheidet die Kommission.

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

297 Bei der Umsetzung der Vorschriften über die Datenübermittlung in Drittländer ergaben sich  
 298 gegenüber den USA Probleme, die zum Abschluss der „Safe Harbor“-Vereinbarung führten.  
 299 Aufgrund unterschiedlicher datenschutzrechtlicher Ansätze verfolgen die USA in Fragen des  
 300 Datenschutzes einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften,  
 301 Verordnungen und Selbstregulierung beruht, während in der EU Regelungen in Form umfassender  
 302 Datenschutzgesetze überwiegen. Angesichts dieser Unterschiede bestanden Unsicherheiten, ob bei der  
 303 Übermittlung personenbezogener Daten in die USA ein angemessenes Schutzniveau im Sinne des EU-  
 304 Datenschutzrechts gegeben sei.<sup>38</sup> Um ein angemessenes Datenschutzniveau zu gewährleisten, haben  
 305 die EU und das US-Handelsministerium im Juli 2006 eine Vereinbarung zu den Grundsätzen des so  
 306 genannten sicheren Hafens (Safe Harbor) geschlossen.<sup>39</sup> Als Safe-Harbor-Prinzipien wurden sieben  
 307 Grundsätze für die Datenverarbeitung festgelegt (betreffend u. a. Informationspflichten und  
 308 Auskunftsrechte, Möglichkeit des Opt-out bei der Weitergabe an Dritte oder der Nutzung für andere  
 309 Zwecke, Sicherheitsvorkehrungen gegen Verlust, unbefugten Zugriff oder Missbrauch  
 310 personenbezogener Daten, Rechtsbehelfe und Sanktionen). Das Abkommen sieht vor, dass sich US-  
 311 amerikanische Unternehmen öffentlich zur Einhaltung der Safe-Harbor-Prinzipien verpflichten  
 312 können. Die Zertifizierung erfolgt durch Meldung an die Federal Trade Commission (FTC). Eine  
 313 Liste der beigetretenen Unternehmen wird von der FTC im Internet veröffentlicht. Die

---

<sup>37</sup> Art. 25 DSRL.

<sup>38</sup> 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.

<sup>39</sup> Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000, ABl. EG Nr. L 215 vom 25. August 2000, S. 7.

314 Datenübermittlung an ein zertifiziertes Unternehmen ist dann möglich, ohne dass es einer weiteren  
315 behördlichen Feststellung des angemessenen Schutzniveaus bedürfte.<sup>40</sup>

316 Als bereichsspezifische Ergänzung zur Datenschutzrichtlinie regelt die E-Privacy-Richtlinie  
317 2002/58/EG<sup>41</sup> datenschutzrechtliche Aspekte im Bereich der elektronischen Kommunikation, die  
318 durch die Datenschutzrichtlinie nicht ausreichend abgedeckt wurden. Dies betrifft etwa die  
319 Vertraulichkeit der Kommunikation, Regelungen über Verkehrsdaten, Standortdaten,  
320 Einzelgebühreennachweis, Rufnummernanzeige und unerbetene Werbenachrichten. Juristische  
321 Personen werden in den Schutzbereich der Richtlinie einbezogen. Die Richtlinie dient neben der  
322 Harmonisierung der mitgliedstaatlichen Datenschutzvorschriften auch der Gewährleistung des freien  
323 Verkehrs von Daten und elektronischen Kommunikationsgeräten beziehungsweise -diensten in der  
324 Gemeinschaft.

325 Die E-Privacy-Richtlinie wurde mit Richtlinie 2009/136/EG<sup>42</sup> geändert. Erstmals wurde auf EU-  
326 Ebene eine Informationspflicht der Diensteanbieter bei Datensicherheitsverletzungen eingeführt, die  
327 Installation von Cookies oder Spyware von der Einwilligung des Internetnutzers abhängig gemacht,  
328 die Rechte Betroffener gegen unerbetene kommerzielle Nachrichten gestärkt und die Durchsetzung  
329 der Datenschutzbestimmungen durch Sanktionen verbessert. Die Umsetzung dieser Änderungen hat  
330 bis zum 25. Mai 2011 zu erfolgen.<sup>43</sup>

331 In der im Jahr 2000 verabschiedeten E-Commerce-Richtlinie 2000/31/EG<sup>44</sup>, mit der ein europäischer  
332 Rechtsrahmen für den elektronischen Geschäftsverkehr geschaffen wurde, werden Fragen des  
333 Datenschutzes ausgeklammert<sup>45</sup> und insoweit auf anderweitige Rechtsakte der Union verwiesen. In  
334 den Erwägungen der Richtlinie (Nr. 14) wird allerdings betont, dass die Grundsätze des Schutzes  
335 personenbezogener Daten bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu  
336 beachten sind, insbesondere in Bezug auf nicht angeforderte kommerzielle Kommunikation und die  
337 Verantwortlichkeit von Vermittlern.

---

<sup>40</sup> 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](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.

<sup>41</sup> 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. Im Folgenden „E-Privacy-Richtlinie“.

<sup>42</sup> 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.

<sup>43</sup> 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>.

<sup>44</sup> 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. Im Folgenden „E-Commerce-Richtlinie“.

<sup>45</sup> A.a.O. (S. 3), Erwägungsgrund Nr. 14, sowie Artikel 1 Abs. 5 b) der genannten Richtlinie.

338 Die Datenschutzverordnung für die EU-Organe 45/2001/EG<sup>46</sup> beschreibt den datenschutzrechtlichen  
 339 Rahmen für das Handeln der EU-Organe. Adressat der Verordnung sind also nicht die  
 340 Mitgliedstaaten, sondern alle „Organe und Einrichtungen der Gemeinschaft“. Durch die Verordnung  
 341 wird weiterhin der Europäische Datenschutzbeauftragte eingesetzt, der für die unabhängige Kontrolle  
 342 der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU zuständig ist.

343 Mit der Vorratsdatenspeicherungsrichtlinie 2006/24/EG<sup>47</sup> werden die Vorschriften der Mitgliedstaaten  
 344 über die Vorratsspeicherung bestimmter Daten, die von Telekommunikationsdienstleistern etwa im  
 345 Rahmen von Internet und Telefonie erzeugt oder verarbeitet werden, harmonisiert. Auf diese Weise  
 346 soll sichergestellt werden, dass die Daten zu Zwecken der Ermittlung und Verfolgung schwerer  
 347 Straftaten verfügbar sind.<sup>48</sup> Die Richtlinie schreibt die vorsorgliche anlasslose Speicherung von  
 348 Kommunikationsdaten vor und trifft u. a. Feststellungen zu den Kategorien der zu speichernden  
 349 Daten, zu Speicherungsfristen und Fragen des Datenschutzes und der Datensicherheit. Daten, die  
 350 Kommunikationsinhalte betreffen (Inhaltsdaten), sind nicht zu speichern.<sup>49</sup>

351 Im Bereich der justiziellen Zusammenarbeit in Strafsachen und bei der polizeilichen Zusammenarbeit  
 352 existiert als allgemeiner Rechtsakt der Rahmenbeschluss 2008/977/JI des Rates über den Schutz  
 353 personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in  
 354 Strafsachen verarbeitet werden.<sup>50</sup> Sein eng gefasster Anwendungsbereich erstreckt sich auf  
 355 personenbezogene Daten, die von mitgliedstaatlichen Behörden zur Verhütung, Ermittlung,  
 356 Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen  
 357 erhoben beziehungsweise verarbeitet werden. Der Beschluss gilt nur bei zwischenstaatlichem  
 358 Datenaustausch und ist daher auf rein nationale Sachverhalte nicht anwendbar.<sup>51</sup> Im Gegensatz zur  
 359 Datenschutzrichtlinie setzt der Rahmenbeschluss 2008/977/JI zwischen den Mitgliedstaaten lediglich  
 360 einen Mindeststandard fest. Die einzelnen Mitgliedstaaten sind daher nicht daran gehindert, strengere  
 361 nationale Bestimmungen im Regelungsbereich des Rahmenbeschlusses zu erlassen.<sup>52</sup>

---

<sup>46</sup> 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.

<sup>47</sup> Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher 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.

<sup>48</sup> Art. 1 der Richtlinie, a.a.O. Im Folgenden „Vorratsdatenspeicherungsrichtlinie“.

<sup>49</sup> 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 1.3.4.

<sup>50</sup> 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.

<sup>51</sup> Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Aufl. 2010, Art. 16 Rn. 48.

<sup>52</sup> Vgl. Zerdick, Thomas, in: Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.). EU-Verträge. 5. Aufl. 2010, Art. 16 Rn. 50.

362 Die Europäische Kommission hat im November 2010 ein *Gesamtkonzept für den Datenschutz in der*  
 363 *Europäischen Union*<sup>53</sup> vorgelegt und für 2011 einen Vorschlag für die Änderung der  
 364 Datenschutzrichtlinie angekündigt.

### 365 1.2.3 Rechtsprechung des Europäischen Gerichtshofs

366 Erste Entscheidungen des EuGH zur Datenschutzrichtlinie datieren aus dem Jahr 2003.<sup>54</sup> In einem  
 367 2003 entschiedenen Verfahren<sup>55</sup> wandten sich Mitarbeiter des Österreichischen Rundfunks gegen eine  
 368 österreichische Regelung, aufgrund derer ihre Jahresbezüge mit ihren Namen dem Rechnungshof  
 369 mitzuteilen waren und nachfolgend vom Rechnungshof veröffentlicht wurden. Besonders streitig war  
 370 in diesem Zusammenhang, ob die Datenschutzrichtlinie, die auf die Kompetenz der Gemeinschaft zur  
 371 Errichtung des Binnenmarktes gestützt wird und durch Harmonisierung der nationalen Vorschriften  
 372 den freien Datenverkehr zwischen den Mitgliedstaaten gewährleisten soll, auf diesen Sachverhalt  
 373 überhaupt anwendbar war. Denn im konkreten Fall lag ein Zusammenhang mit den europarechtlichen  
 374 Grundfreiheiten eher fern. Das Gericht hat die Anwendbarkeit der Richtlinie dennoch bejaht. Nach  
 375 Auffassung des Gerichts kann die Anwendbarkeit der Richtlinie im Einzelfall nicht davon abhängen,  
 376 ob ein Zusammenhang mit dem freien Verkehr zwischen den Mitgliedstaaten besteht.<sup>56</sup>

377 Die Darstellung anderer Personen ohne deren Zustimmung auf einer privaten schwedischen Website  
 378 war Gegenstand im Fall „Lindqvist“<sup>57</sup>. In seinem Urteil nahm der EuGH erstmals zur  
 379 Veröffentlichung personenbezogener Daten im Internet Stellung und entschied, dass die Einstellung  
 380 ins Internet zwar eine Verarbeitung von Daten im Sinne der Datenschutzrichtlinie darstelle, nicht aber  
 381 als Übermittlung in Drittländer und damit nicht als grenzüberschreitender Datenaustausch anzusehen  
 382 sei. Das Gericht äußerte sich auch zur Frage des Ausgleichs zwischen Datenschutz und  
 383 widerstreitenden Grundrechten, insbesondere der Meinungsfreiheit. Es sei Sache der nationalen  
 384 Behörden und Gerichte, ein angemessenes Gleichgewicht zwischen den betroffenen Rechten und  
 385 Interessen einschließlich geschützter Grundrechte herzustellen und hierbei insbesondere den  
 386 Grundsatz der Verhältnismäßigkeit zu wahren. Im Übrigen sei es zulässig, dass die Mitgliedstaaten  
 387 den Geltungsbereich ihrer Datenschutzgesetze über den Anwendungsbereich der Richtlinie hinaus  
 388 ausdehnen, soweit dem keine Bestimmung des Gemeinschaftsrechts entgegenstehe.

389 Zur Übermittlung von Fluggastdaten an die USA nahm der EuGH im Mai 2006 Stellung.<sup>58</sup> Er erklärte  
 390 die zugrunde liegende Genehmigung des Abkommens zwischen der EU und den USA durch den Rat  
 391 für nichtig. Dasselbe gelte für die zum selben Sachverhalt ergangene Entscheidung der Kommission,  
 392 mit der das US-amerikanische Datenschutzniveau für angemessen im Sinne des Art. 25 DSRL erklärt  
 393 wurde. Wie sich aus den Begründungserwägungen ergebe, seien Sinn und Zweck der  
 394 Datenübermittlung in die USA die Terrorismusbekämpfung. Gegenstand beider Rechtsakte sei daher

---

<sup>53</sup> 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](http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-de.pdf)

<sup>54</sup> Vgl. Roßnagel, Alexander: Anmerkung zu EuGH Urt. v. 6. November 2003, C-101/01, Slg. 2003, I-12971 Rn 87 – Lindqvist = MMR 2004, 95 (99).

<sup>55</sup> EuGH, Urteil vom 20. Mai 2003, Rs. C-465/00, Slg. I-04989 - Österreichischer Rundfunk.

<sup>56</sup> 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](http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/Arbeit/Artikel/200503_OesterreichischerRundfunk.html?nn=408918)

<sup>57</sup> EuGH, Urteil vom 6. November 2003, C-101/01, Slg. 2003, I-12971 – Lindqvist.

<sup>58</sup> 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.

395 das Strafrecht. Daher sei die Datenschutzrichtlinie<sup>59</sup> keine geeignete Rechtsgrundlage. Mangels  
 396 Rechtsgrundlage waren der Ratsbeschluss und die Kommissionsentscheidung deshalb für nichtig zu  
 397 erklären.

398 In einem Urteil vom Februar 2009 über die Vorratsdatenspeicherungsrichtlinie<sup>60</sup> konzentriert sich der  
 399 EuGH ebenfalls auf Fragen der Rechtsetzungskompetenz. Grundrechtliche Fragen waren hingegen  
 400 nicht Gegenstand des Verfahrens. Die Vorratsdatenspeicherungsrichtlinie stelle keine Regelung der  
 401 Strafverfolgung dar, sondern habe – anders als bei der Fluggastdatenübermittlung – den Zweck, durch  
 402 Harmonisierung das Handeln der Telekommunikationsdienstleister im Binnenmarkt zu erleichtern.  
 403 Die Richtlinie sei daher zu Recht auf der Grundlage der Binnenmarktcompetenz erlassen worden.  
 404 Anders als von der Klage geltend gemacht sei ein Rahmenbeschluss nach den Bestimmungen über die  
 405 polizeiliche und justizielle Zusammenarbeit nicht erforderlich.

406 Im Hinblick auf das zentrale deutsche Ausländerregister entschied der EuGH mit Urteil vom 16.  
 407 Dezember 2008<sup>61</sup>, dass die Speicherung und Verarbeitung personenbezogener Daten namentlich  
 408 genannter Personen zu statistischen Zwecken nicht dem Erforderlichkeitsgebot<sup>62</sup> im Sinne der  
 409 Datenschutzrichtlinie entspreche und die Nutzung der im Register enthaltenen Daten zur Bekämpfung  
 410 der Kriminalität gegen das Diskriminierungsverbot verstoße. Denn diese Nutzung stelle auf die  
 411 Verfolgung von Verbrechen und Vergehen unabhängig von der Staatsangehörigkeit ab. Ein System  
 412 zur Verarbeitung personenbezogener Daten, das der Kriminalitätsbekämpfung diene, aber nur EU-  
 413 Ausländer erfasse, sei mit dem Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit  
 414 unvereinbar.

415 Zum Verhältnis von Pressefreiheit und Datenschutz äußerte sich der EuGH in seiner Entscheidung  
 416 vom 16. Dezember 2008<sup>63</sup>. Das Unternehmen Markkinapörssi veröffentlichte Steuerdaten (Namen und  
 417 Einkommen), die bei den finnischen Steuerbehörden öffentlich zugänglich waren. Der EuGH sah auch  
 418 diese Weiterveröffentlichung bereits öffentlich zugänglicher Informationen als Datenverarbeitung im  
 419 Sinne der Datenschutzrichtlinie an. Um Datenschutz und Meinungsfreiheit in Ausgleich zu bringen,  
 420 seien die Mitgliedstaaten aufgerufen, Einschränkungen des Datenschutzes vorzusehen. Diese seien  
 421 jedoch nur zu journalistischen, künstlerischen oder literarischen Zwecken, die unter das Grundrecht  
 422 der Meinungsfreiheit fallen, zulässig. In Anbetracht der hohen Bedeutung der Meinungsfreiheit müsse  
 423 der Begriff des „Journalismus“ und damit zusammenhängende Begriffe weit ausgelegt werden.  
 424 Andererseits müssten sich Einschränkungen des Datenschutzes aus Gründen der Meinungsfreiheit auf  
 425 das absolut Notwendige beschränken.

426 Mit Urteil vom 9. März 2010 entschied der EuGH in einem Vertragsverletzungsverfahren, das die EU-  
 427 Kommission gegen Deutschland angestrengt hatte.<sup>64</sup> Die organisatorische Einbindung der  
 428 Datenschutzaufsicht für den nicht-öffentlichen Bereich in die Innenministerien einiger Bundesländer  
 429 sowie die Aufsicht der Landesregierungen über die Datenschutzbehörden entspreche nicht den

---

<sup>59</sup> S. a. Artikel 3 Abs. 2 zweiter Spiegelstrich DSRL.

<sup>60</sup> EuGH, Urteil vom 10. Februar 2009, Rs. C-301/06, MMR 2009, 244 ff. – Vorratsdatenspeicherung.

<sup>61</sup> EuGH, Urteil vom 16. Dezember 2008, Rs. C-524/06, MMR 2009, 171 ff. – Huber.

<sup>62</sup> Artikel 7 Buchst. e DSRL.

<sup>63</sup> EuGH, Urteil vom 16. Dezember 2008, Rs. C-73/07, Slg. 2007, I-7075 – Markkinapörssi.

<sup>64</sup> EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland.

430 Vorgaben der Datenschutzrichtlinie. Vielmehr sei nach Art. 28 DSRL erforderlich, dass diese Stellen  
431 ihre Aufgabe „in völliger Unabhängigkeit“ wahrnehmen.

432 Um den Widerstreit von Transparenz und Datenschutz geht es in der Rechtssache „Bavarian Lager“  
433 vom 29. Juni 2010.<sup>65</sup> Die EU-Kommission hatte es abgelehnt, gegenüber der Gesellschaft Bavarian  
434 Lager Company die Namen der Teilnehmer eines im Rahmen eines Vertragsverletzungsverfahrens  
435 abgehaltenen vertraulichen Treffens offenzulegen. Die Kommission berief sich darauf, dass der  
436 Zugang zu Dokumenten nur unter Beachtung des Datenschutzes zulässig sei. Das Europäische Gericht  
437 hatte 2007 in erster Instanz entschieden, dass die Herausgabe der Dokumente nur dann verweigert  
438 werden könne, wenn der Schutz der Privatsphäre verletzt werde. Das sei bei einer bloßen  
439 Namensnennung auf einer Teilnehmerliste im beruflichen Kontext nicht der Fall. Auf der Grundlage  
440 der Datenschutzverordnung für die EU-Organe sowie der Verordnung 1049/2001/EG<sup>66</sup> entschied der  
441 EuGH im Juni 2010, dass die Kommission rechtmäßig gehandelt habe. Die in dem Sitzungsprotokoll  
442 aufgeführten Teilnehmernamen seien personenbezogene Daten. Da Bavarian Lager Argumente für die  
443 Notwendigkeit der Übermittlung dieser Daten oder ein berechtigtes Interesse nicht vorgetragen habe,  
444 könne die Kommission keine Interessenabwägung vornehmen. Die Verpflichtung zur Transparenz sei  
445 daher im konkreten Fall von der Kommission hinreichend gewahrt worden.

446 Demgegenüber sah das Gericht bei der Internetveröffentlichung der Namen aller natürlichen  
447 Personen, die EU-Agrarsubventionen empfangen haben, den Grundsatz der Verhältnismäßigkeit  
448 verletzt. Denn hierbei wurde nicht nach einschlägigen Kriterien wie Häufigkeit oder Art und Höhe der  
449 Beihilfen unterschieden. Das Interesse der Steuerzahler an Informationen über die Verwendung  
450 öffentlicher Gelder rechtfertige einen solchen Eingriff in das Recht auf Schutz der personenbezogenen  
451 Daten nach Art. 8 GRC nicht.<sup>67</sup>

## 452 453 1.3 Nationales Recht

### 454 1.3.1 Grundrechte

455 Das Grundgesetz kennt kein ausdrückliches Datenschutz-Grundrecht. Allerdings hat das  
456 Bundesverfassungsgericht (BVerfG) bereits 1983 in seinem so genannten „Volkszählungsurteil“<sup>68</sup> das  
457 Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen  
458 Persönlichkeitsrechtes (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) formuliert. Forderungen,  
459 den Datenschutz ausdrücklich als Grundrecht im Grundgesetz zu verankern, fanden bisher nicht die  
460 erforderliche Mehrheit.<sup>69</sup> Nach der Rechtsprechung des BVerfG beinhaltet das Grundrecht auf  
461 informationelle Selbstbestimmung die Befugnis des Einzelnen, „grundsätzlich selbst über die  
462 Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.<sup>70</sup> Die Unsicherheit, wo welche

<sup>65</sup> EuGH, Urteil vom 29. Juni 2010, Rs. C-28/08, EuZW 2010, 617 - Bavarian Lager Company.

<sup>66</sup> 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).

<sup>67</sup> EuGH, Urteil vom 9. November 2010, Rs. C-92/09, C-93/09, EuZW 2010, 939 – Scheck GbR und Eifert gegen Land Hessen.

<sup>68</sup> BVerfGE 65,1.

<sup>69</sup> 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.

<sup>70</sup> BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, 45 - Volkszählung.

463 personenbezogenen Informationen gespeichert, verwendet oder weitergegeben werden, würde „nicht  
 464 nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das  
 465 Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf  
 466 Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen  
 467 demokratischen Gemeinwesens ist.“<sup>71</sup> „Mit dem Recht auf informationelle Selbstbestimmung wären  
 468 eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der  
 469 Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.<sup>72</sup> In  
 470 den Schutzbereich dieses Grundrechts fallen alle Formen der Erhebung personenbezogener Daten.  
 471 Angesichts der Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie geht das  
 472 BVerfG davon aus, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein  
 473 „belangloses“ Datum mehr“ gebe.<sup>73</sup>

474 Im Hinblick auf die Fragestellungen der Enquete-Kommission sind als weitere Ausprägungen des  
 475 allgemeinen Persönlichkeitsrechts das Recht am eigenen Bild von Bedeutung, das u. a. den Einzelnen  
 476 vor der Aufnahme, Darbietung, Verbreitung und sonstigen Verwertung seines Abbildes schützt<sup>74</sup>,  
 477 sowie das 2008 durch das BVerfG formulierte „Grundrecht auf Gewährleistung der Vertraulichkeit  
 478 und Integrität informationstechnischer Systeme“.<sup>75</sup> Nach der Rechtsprechung des Gerichts handelt es  
 479 sich um ein subsidiäres Grundrecht, das hinter anderen Grundrechten, etwa dem Brief-, Post- und  
 480 Fernmeldegeheimnis (Art. 10 GG) oder der Unverletzlichkeit der Wohnung (Art. 13 GG) zurücktritt  
 481 und erst dann zur Anwendung kommt, wenn vorrangige Grundrechte keinen hinreichenden Schutz vor  
 482 Eingriffen in informationstechnische Systeme gewähren.<sup>76</sup>

483 Grundlegend für den Datenschutz sind weiterhin die Grundrechte nach Art. 10 GG (Brief-, Post- und  
 484 Fernmeldegeheimnis, auch als „Telekommunikationsgeheimnis“ bezeichnet) und Art. 13 GG  
 485 (Unverletzlichkeit der Wohnung). Das Grundrecht der Unverletzlichkeit der Wohnung schützt u. a.  
 486 vor Durchsuchungen und Abhörmaßnahmen, etwa wenn hierfür in die Wohnung eingedrungen wird.<sup>77</sup>  
 487 Durch das Fernmeldegeheimnis wird die unbeobachtete, nicht öffentliche Kommunikation unabhängig  
 488 von der Übertragungsart (Kabel, Funk, analoge oder digitale Vermittlung) und unabhängig von deren  
 489 Ausdrucksformen (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) geschützt, und zwar auch  
 490 über das Internet, etwa als E-Mail.<sup>78</sup> Der Schutz erstreckt sich nicht nur auf die Inhalte der  
 491 Kommunikation, sondern auch auf die Kommunikationsumstände<sup>79</sup>, etwa die beteiligten Personen,  
 492 Zeit, Ort und Häufigkeit der Kommunikation. An Art. 10 GG zu messen ist weiterhin der  
 493 Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen von geschützten  
 494 Kommunikationsvorgängen anschließt, sowie der Gebrauch, der von den so erlangten Kenntnissen  
 495 gemacht wird.<sup>80</sup> Da das Telekommunikationsgeheimnis vorrangig vor der Manipulation des

<sup>71</sup> BVerfGE 65, 1, 43 - Volkszählung.

<sup>72</sup> BVerfGE 65, 1, 43 - Volkszählung.

<sup>73</sup> BVerfGE 65, 1, 45- Volkszählung. Zum Grundrecht auf informationelle Selbstbestimmung vgl. im Übrigen unter 2.1.5.

<sup>74</sup> Di Fabio, Udo, in: Maunz, Theodor/Dürig, Günter. Grundgesetz. 57. Auflage 2010, Art. 2 GG Rn. 193.

<sup>75</sup> BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370, 595/07, BVerfGE 120, 274, 302 ff. – Onlinedurchsuchung.

<sup>76</sup> Zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vgl. im Übrigen unter 2.1.3.

<sup>77</sup> BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 u. 1 BvR 1084/99, BVerfGE 109, 279 – Großer Lauschangriff.

<sup>78</sup> BVerfGE 120, 274, 307 – Onlinedurchsuchung.

<sup>79</sup> BVerfG, Urteil vom 27. Juli 2005 - 1 BvR 668/04, BVerfGE 113, 348, 364 – Vorbeugende Telekommunikationsüberwachung.

<sup>80</sup> BVerfGE 113, 348, 365 – Vorbeugende Telekommunikationsüberwachung.



496 technischen Übertragungsvorgangs schützt, endet der Schutz des Fernmeldegeheimnisses, sobald der  
 497 Übertragungsvorgang abgeschlossen ist. Bezogen auf die Telekommunikation enthält Art. 10 GG eine  
 498 spezielle Garantie, die das Recht auf informationelle Selbstbestimmung verdrängt und aus der sich  
 499 besondere Anforderungen für die Daten ergeben, die durch Eingriffe in das Fernmeldegeheimnis  
 500 erlangt werden. Nach der Rechtsprechung des BVerfG lassen sich allerdings die Maßgaben, die für  
 501 das Recht auf informationelle Selbstbestimmung gelten, weitgehend auf Eingriffe in das  
 502 Fernmeldegeheimnis übertragen.

503

### 504 1.3.2 Einfaches Bundesrecht

505 Das Bundesdatenschutzgesetz (BDSG)<sup>81</sup> stellt das Kernstück des Datenschutzrechts auf Bundesebene  
 506 dar. Es wurde 1990 als umfassende Novelle des Bundesdatenschutzgesetzes von 1977 in Reaktion auf  
 507 das „Volkszählungsurteil“ verabschiedet, um – den Vorgaben des BVerfG entsprechend – eine  
 508 gesetzliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten zu schaffen und  
 509 so den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechtes zu schützen. Als Teil des  
 510 allgemeinen Datenschutzrechts enthält es keine bereichsspezifischen Regelungen und gilt sowohl für  
 511 Datenverarbeitung in IT-Systemen als auch auf für manuelle Verfahren.

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

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

536

---

<sup>81</sup> 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).

537 Der räumliche Anwendungsbereich des BDSG ist in § 1 Abs. 5 BDSG geregelt. Erhebt oder  
 538 verarbeitet ein ausländisches Unternehmen mit Sitz innerhalb der EU bzw. innerhalb des EWR Daten  
 539 im Inland, ist das BDSG nur dann anwendbar, wenn das Unternehmen durch eine deutsche  
 540 Niederlassung tätig wird. Bei Datenerhebung und -verarbeitung im Inland durch ein Unternehmen mit  
 541 Sitz außerhalb der EU bzw. außerhalb des EWR findet das BDSG hingegen Anwendung.<sup>82</sup>

542 Gegenüber spezielleren Vorschriften des Bundesrechts tritt das BDSG zurück (§ 1 Abs. 3 BDSG).  
 543 Wegen zahlreicher bereichsspezifischer Regelungen in anderen Gesetzen wird das BDSG daher als  
 544 Auffanggesetz des insgesamt zersplitterten Datenschutzrechts angesehen.<sup>83</sup> Beispiele für  
 545 Spezialregelungen sind das Bundespolizeigesetz, das Bundeskriminalamtsgesetz, das  
 546 Bundeszentralregistergesetz, die Grundbuchordnung, das Personenstandgesetz, §§ 8 ff.  
 547 Handelsgesetzbuch und die Grundbuchordnung.<sup>84</sup> In gesonderten Vorschriften außerhalb des BDSG  
 548 ist auch der Datenschutz der öffentlich-rechtlichen Religionsgemeinschaften geregelt. Im  
 549 Sozialgesetzbuch (SGB) Band X (Zweites Kapitel „Schutz der Sozialdaten, §§ 67 ff.)<sup>85</sup> finden sich die  
 550 datenschutzrechtlichen Bestimmungen für den Sozialleistungsbereich. Sozialdaten sollen nach der  
 551 Vorstellung des Gesetzgebers einem erhöhten, dem Steuergeheimnis vergleichbaren Schutz  
 552 unterliegen.<sup>86</sup> Ergänzende Bestimmungen für verschiedene Zweige der Sozialversicherung enthalten  
 553 die jeweils einschlägigen Bücher des SGB.

554 Für das Internet von besonderer Bedeutung ist das Telemediengesetz (TMG).<sup>87</sup> Telemedien sind  
 555 Waren- und Dienstleistungsangebote im Netz unter Einbeziehung redaktionell gestalteter Online-  
 556 Angebote, ausgenommen jedoch der Rundfunk.<sup>88</sup> Für diese Medien enthält das TMG Vorschriften  
 557 über den Umgang mit personenbezogenen Nutzerdaten (§§ 11 ff. TMG). Auch im TMG gelten die  
 558 Grundsätze der Zweckbindung, der Datenvermeidung und –sparsamkeit. Den allgemeinen  
 559 Datenschutzgrundsätzen folgend ist auch im Bereich der Telemedien die Erhebung und Verarbeitung  
 560 personenbezogener Daten nur mit Einwilligung des Betroffenen oder auf gesetzlicher Grundlage  
 561 zulässig. Zugeschnitten auf den Bereich der Telemedien sind in § 13 TMG die Voraussetzungen für  
 562 eine elektronische Einwilligung geregelt. Über Daten, die für die Begründung, inhaltliche  
 563 Ausgestaltung oder Änderung des Vertragsverhältnisses zwischen Diensteanbieter und Nutzer  
 564 erforderlich sind (Bestandsdaten), darf der Diensteanbieter nach § 14 TMG auf Anordnung der  
 565 zuständigen Stellen im Einzelfall Auskunft erteilen, etwa zum Zwecke der Strafverfolgung, zur  
 566 Gefahrenabwehr, zur Terrorbekämpfung oder zur Durchsetzung der Rechte am geistigen Eigentum.

567 Telekommunikationsdienste sind hingegen solche Dienste, die ganz oder überwiegend in der  
 568 Übertragung von Signalen über Telekommunikationsdienste bestehen, darunter nach Vorstellung des  
 569 Gesetzgebers auch Internet-Telefonie, Internet-Access-Provider und E-Mail-Übertragung.<sup>89</sup> Der

---

<sup>82</sup> Anderes gilt nach § 1 Abs. 5 S. 4 BDSG im Fall des „Transits“.

<sup>83</sup> Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 1 Rn. 14.

<sup>84</sup> Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo. Bundesdatenschutzgesetz - Kommentar. 3. Auflage 2010, Einleitung, Rn. 73.

<sup>85</sup> 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).

<sup>86</sup> BT-Drs. 8/4022, S. 96.

<sup>87</sup> Telemediengesetz vom 26. Februar 2007, BGBl. I, S. 179, zuletzt geändert durch Gesetz vom 14. August 2009, BGBl. I, S. 2814.

<sup>88</sup> Hoeren, Thomas: Das Telemediengesetz, NJW 2007, 801.

<sup>89</sup> BT-Drs. 16/3078, S. 13.

570 Datenschutz für die Teilnehmer ist im Telekommunikationsgesetz (TKG)<sup>90</sup>, insbesondere §§ 91 ff.  
 571 TKG, geregelt. Geschützt sind Angaben über persönliche und sachliche Verhältnisse, u. a.  
 572 Informationen über das Kommunikationsverhalten, d.h. „wer wann mit wem von welchem Anschluss  
 573 aus telefoniert hat.“<sup>91</sup> Das TKG enthält Regelungen u. a. über Bestands- und Verkehrsdaten,  
 574 Entgeltermittlung und -abrechnung.

### 575 1.3.3 Landesrecht

576 Die Landesdatenschutzgesetze gelten für die Verarbeitung personenbezogener Daten durch die  
 577 jeweiligen Landesbehörden und andere öffentlich-rechtliche Einrichtungen der Länder. Sie enthalten  
 578 Bestimmungen über die Landesdatenschutzbeauftragten. Ganz überwiegend gilt auch für die  
 579 Landesdatenschutzgesetze der Grundsatz der Subsidiarität gegenüber anderen datenschutzrechtlichen  
 580 Regelungen.<sup>92</sup> Da der Datenschutz in nahezu allen Bereichen der Landesverwaltung von Bedeutung  
 581 ist, weist eine Unzahl landesrechtlicher Gesetze Spezialregelungen zum Datenschutz auf, u. a. die  
 582 Landesgesetze zum (Jugend-)Strafvollzug und zur Untersuchungshaft, die Rettungsdienstgesetze,  
 583 Brand- und Katastrophenschutzgesetze, Schulgesetze.

584 Anders als im Bundesrecht finden sich auf Landesebene auch Formen untergesetzlicher Regelungen  
 585 zum allgemeinen Datenschutzrecht, d. h. Rechtsverordnungen und Verwaltungsvorschriften.<sup>93</sup>

### 586 1.3.4 Rechtsprechung des Bundesverfassungsgerichts

587 Neben den unter 1.3.1 erwähnten grundlegenden Entscheidungen, dem „Volkszählungsurteil“ sowie  
 588 dem Urteil zur „Online-Durchsuchung“, hat sich das BVerfG in einer Reihe weiterer Entscheidungen  
 589 mit Fragen der informationellen Selbstbestimmung und verwandter Grundrechte befasst. Die  
 590 Rechtsprechung des BVerfG enthält im Bereich des Datenschutzes vielfach sehr konkrete und  
 591 detaillierte Vorgaben für das gesetzgeberische Handeln.<sup>94</sup> Aus der umfangreichen Rechtsprechung des  
 592 Gerichts zum Datenschutz sei beispielhaft auf folgende Entscheidungen hingewiesen:

593 Gegenstand des Urteils vom 14. Juli 1999<sup>95</sup> waren erweiterte Befugnisse des  
 594 Bundesnachrichtendienstes zur Überwachung, Aufzeichnung und Auswertung des  
 595 Telekommunikationsverkehrs sowie zur Übermittlung der daraus erlangten Daten an andere  
 596 Behörden. 1994 war das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G  
 597 10) mit dem Ziel geändert worden, Informationen u. a. im Bereich des internationalen Terrorismus,  
 598 des Drogenhandels und der Geldwäsche zu erlangen, um sie nachfolgend den zuständigen Behörden  
 599 zur Verhinderung, Aufklärung und Verfolgung von Straftaten zur Verfügung zu stellen.<sup>96</sup> Mit

---

<sup>90</sup> 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.

<sup>91</sup> Robert, Anna, in: Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian (Hrsg.). Beck'scher TKG-Kommentar. 3. Auflage 2006, § 91 Rn. 12.

<sup>92</sup> Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 1 Rn. 33.

<sup>93</sup> Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo. Bundesdatenschutzgesetz - Kommentar. 3. Auflage 2010, Einleitung, Rn. 70.

<sup>94</sup> Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035; Wolff, Heinrich A.: Vorratsdatenspeicherung. NVwZ 2010, 751.

<sup>95</sup> BVerfG, Urteil vom 14. Juli 1999 - 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, BVerfGE 100, 313 ff. – Telekommunikationsüberwachung.

<sup>96</sup> Verbrechenbekämpfungsgesetz vom 28. Oktober 1994, BGBl. I, S. 3186.

600 Beschluss vom 5. Juli 1995<sup>97</sup> bestimmte das BVerfG im Rahmen einer einstweiligen Anordnung, dass  
 601 einzelne der neugefassten Vorschriften zunächst nur eingeschränkt angewendet werden dürften. In der  
 602 Hauptsache urteilte das Gericht 1999, einzelne Vorschriften verstießen gegen Art. 10 GG. Das  
 603 Fernmeldegeheimnis schütze in erster Linie den Kommunikationsinhalt vor staatlicher  
 604 Kenntnisnahme, daneben aber auch die Kommunikationsumstände. Der Schutz erstreckte sich auch auf  
 605 den Informations- und Datenverarbeitungsprozess, der sich an zulässige Kenntnisnahmen von  
 606 geschützten Kommunikationsvorgängen anschließe, und den Gebrauch, der von den erlangten  
 607 Kenntnissen gemacht werde. Solle der Bundesnachrichtendienst zu Eingriffen in das  
 608 Fernmeldegeheimnis ermächtigt werden, sei der Gesetzgeber verpflichtet, Vorsorge gegen Gefahren  
 609 zu treffen, die sich aus der Erhebung und Verwertung personenbezogener Daten ergeben. Hierzu  
 610 verwies das Gericht auf die im Volkszählungsurteil entwickelten Kriterien für Eingriffe in Art. 2 Abs.  
 611 1 i. V. m. Art. 1 Abs. 1 GG. Diese seien auch auf die speziellere Regelung des Art. 10 GG  
 612 übertragbar. Speicherung und Verwendung erlangter Daten seien grundsätzlich an den Zweck  
 613 gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt habe. Zweckänderungen seien  
 614 nur durch Allgemeinbelange gerechtfertigt, die die grundrechtlich geschützten Interessen überwiegen.  
 615 Eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht  
 616 bestimmbar Zwecken sei mit diesen Vorgaben unvereinbar.

617 Mit Beschluss vom 14. Dezember 2000<sup>98</sup> stellt das Gericht fest, dass die Feststellung, Speicherung  
 618 und künftige Verwendung des „genetischen Fingerabdrucks“ auf der Grundlage von § 81g StPO und §  
 619 2 DNA-Identitätsfeststellungsgesetz in das Recht auf informationelle Selbstbestimmung eingreife, es  
 620 sich aber um einen rechtlich zulässigen Grundrechtseingriff handele, da u. a. das Gebot der  
 621 Normenklarheit, das Übermaßverbot und der Richtervorbehalt gewahrt seien.

622 Im Urteil vom 12. April 2005<sup>99</sup> äußerte sich das BVerfG zu einer weiteren Vorschrift der  
 623 Strafprozessordnung. Gesetzliche Grundlage für Beweiserhebungen unter Einsatz eines  
 624 satellitengestützten Ortungssystems (Global Positioning System, „GPS“) und die Verwertung der  
 625 Erkenntnisse war im zu Grunde liegenden Sachverhalt § 100c Abs. 1 Nr. 1 Buchst. b  
 626 Strafprozessordnung (StPO) damaliger Fassung, wonach ohne Wissen des Betroffenen „besondere für  
 627 Observationszwecke bestimmte technische Mittel“ eingesetzt werden konnten. Die Vorschrift sei  
 628 verfassungsgemäß, da sie hinreichend bestimmt sei und nicht in den unantastbaren Kernbereich  
 629 privater Lebensgestaltung eingreife. Wegen des schnellen und für den Grundrechtsschutz riskanten  
 630 informationstechnischen Wandels sei der Gesetzgeber aber aufgerufen, die technischen  
 631 Entwicklungen aufmerksam zu verfolgen und notfalls korrigierend einzugreifen.

632 Die Durchsuchung und Beschlagnahme des gesamten elektronischen Datenbestands einer gemeinsam  
 633 betriebenen Rechtsanwaltskanzlei und Steuerberatungsgesellschaft (Beschluss vom 12. April 2005<sup>100</sup>)  
 634 – im Rahmen eines gegen einen der Berufsträger gerichteten Ermittlungsverfahrens – qualifizierte das  
 635 BVerfG als erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung. Dem müsse  
 636 durch strikte Beachtung des Verhältnismäßigkeitsgrundsatzes und bestimmter Verfahrensregelungen  
 637 Rechnung getragen werden. Zu berücksichtigen sei u. a., dass das Vertrauensverhältnis zwischen  
 638 Rechtsanwälten und Mandanten rechtlich besonders geschützt und durch die Streubreite der

---

<sup>97</sup> BVerfG, Beschluss vom 5. Juli 1995 - 1 BvR 2226/94, BVerfGE 93, 181 – Rasterfahndung I.

<sup>98</sup> BVerfG, Beschluss vom 14. Dezember 2000 - 2 BvR 1741/99, 276, 2061/00, BVerfGE 103, 21 - Genetischer Fingerabdruck I.

<sup>99</sup> BVerfG, Urteil vom 12. April 2005 - 2 BvR 581/01, BVerfGE 112, 304 - GPS-Überwachung.

<sup>100</sup> BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02, BVerfGE 113, 29, 46 - Beschlagnahme von Datenträgern.

639 sichergestellten Daten eine Vielzahl gänzlich unbeteiligter Personen von der Beschlagnahme betroffen  
640 sei.

641 Zu den verfassungsrechtlichen Grenzen der Rasterfahndung, bei der den Polizeibehörden von anderen  
642 Stellen personenbezogene Daten übermittelt und nachfolgend einem automatisierten Abgleich nach  
643 bestimmten Merkmalen unterzogen werden, hat das BVerfG mit Beschluss vom 4. April 2006  
644 entschieden. Eine präventive polizeiliche Rasterfahndung stelle einen Grundrechtseingriff von  
645 besonderer Intensität dar und sei daher mit dem Grundrecht auf informationelle Selbstbestimmung nur  
646 dann vereinbar, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die  
647 Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben  
648 sei<sup>101</sup>. Eine allgemeine Bedrohungslage, wie etwa seit dem 11. September 2001, ohne das Vorliegen  
649 weiterer Tatsachen, sei dafür nicht ausreichend.

650 Mit Beschluss vom 13. Juni 2007<sup>102</sup> erklärte das Gericht Vorschriften zum automatischen  
651 Kontenabruf teilweise für verfassungswidrig, da gegen den verfassungsrechtlichen  
652 Bestimmtheitsgrundsatz verstoßen werde. Die angegriffenen Regelungen ermächtigten einzelne  
653 Behörden zur automatisierten Abfrage von Daten, die von den Kreditinstituten vorgehalten werden  
654 müssen. Soweit das Gebot der Normenklarheit nicht eingehalten worden sei, verstoße die Regelung  
655 gegen das Recht auf informationelle Selbstbestimmung. Einen solchen Verstoß bejahte das Gericht  
656 hinsichtlich § 93 Abs. 8 Abgabenordnung (AO) damaliger Fassung, da der Kreis der zur  
657 Kontenabfrage berechtigten Behörden und die dabei verfolgten Zwecke nicht hinreichend festgelegt  
658 worden seien.

659 Auch eine Geschwindigkeitsmessung auf der Grundlage einer Verwaltungsvorschrift stellt nach der  
660 Rechtsprechung des BVerfG (Beschluss vom 11. August 2009<sup>103</sup>) eine unzulässige Einschränkung des  
661 Rechts auf informationelle Selbstbestimmung dar, da eine solche Maßnahme nur auf gesetzlicher  
662 Grundlage, die dem Gebot der Normenklarheit und Verhältnismäßigkeit zu entsprechen habe, zulässig  
663 sei.

664 Die Einführung der Vorratsdatenspeicherung durch das „Gesetz zur Neuregelung der  
665 Telekommunikationsüberwachung“<sup>104</sup> zur Umsetzung der Richtlinie 2006/24/EG in deutsches Recht  
666 ist Gegenstand mehrerer Entscheidungen des BVerfG. Nach § 113a TKG waren  
667 Telekommunikationsdiensteanbieter verpflichtet, Verkehrsdaten von Telefondiensten (Festnetz,  
668 Mobilfunk, Fax, SMS, MMS), E-Mail-Diensten und Internetdiensten vorsorglich anlasslos für die  
669 Dauer von sechs Monaten zu speichern. Die zulässigen Zwecke der Datenverwendung waren in §  
670 113b TKG, die Verwendung der Daten für die Strafverfolgung in § 100g StPO geregelt. Nachdem das  
671 Gericht mit Beschluss vom 28. Oktober 2008<sup>105</sup> im Wege der einstweiligen Anordnung Teile der  
672 Vorratsdatenspeicherung außer Kraft gesetzt hatte, entschied es mit Urteil vom 2. März 2010<sup>106</sup> in der  
673 Hauptsache, dass die Regelungen des TKG und der StPO über die Vorratsdatenspeicherung mit Art.  
674 10 Abs. 1 GG unvereinbar und damit nichtig seien. Die Vorratsdatenspeicherung durch private

---

<sup>101</sup> BVerfGE 93, 181 – Rasterfahndung I.

<sup>102</sup> BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03, NJW 2007, 2464 - Automatisierte Abfrage von Kontostammdaten.

<sup>103</sup> BVerfG, Beschluss vom 11. August 2009 – 2 BvR 941/08, NJW 2009, 3293 - Verkehrsüberwachung.

<sup>104</sup> Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007, BGBl. I, S. 3198.

<sup>105</sup> BVerfG, Beschluss vom 28. Oktober 2008 - 1 BvR 256/08, BVerfGE 122, 120 - Vorratsdatenspeicherung/Datenermittlung.

<sup>106</sup> BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 - Vorratsdatenspeicherung.

675 Telekommunikationsunternehmen greife in den Schutzbereich des Fernmeldegeheimnis ein, da diese  
 676 als „Hilfspersonen“ für die Aufgabenerfüllung staatlicher Behörden in Anspruch genommen würden.  
 677 Zwar sei eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin  
 678 verfassungswidrig. Es fehle aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden  
 679 Ausgestaltung. Datensicherheit, Begrenzung der Verwendungszwecke, verfassungsrechtliche  
 680 Transparenz und Rechtsschutzanforderungen seien nicht hinreichend gewährleistet.

681 Für die Frage, zum Schutz welcher Rechtsgüter der Datenabruf als verhältnismäßig anzusehen ist,  
 682 differenziert das Gericht zwischen der unmittelbaren und mittelbaren Nutzung der Daten. Der Abruf  
 683 und die unmittelbare Nutzung der Daten seien nur verhältnismäßig, wenn sie überragend wichtigen  
 684 Aufgaben des Rechtsgüterschutzes dienen. Im Bereich der Strafverfolgung setze dies einen durch  
 685 bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr  
 686 und die Erfüllung der Aufgaben der Nachrichtendienste dürften diese Maßnahmen nur bei Vorliegen  
 687 tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für  
 688 den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr  
 689 zugelassen werden.

690 Soweit die Behörden in §§ 113b Satz 1 Halbs. 2, 113 TKG zur Identifizierung von IP-Adressen  
 691 berechtigt wurden, von Diensteanbietern auf der Grundlage gespeicherter Verkehrsdaten die Identität  
 692 bestimmter, bereits bekannter IP-Adressen zu erfragen, sei diese nur mittelbare Nutzung der Daten  
 693 auch unabhängig von begrenzenden Straftaten- oder Rechtsgüterkatalogen für die Strafverfolgung,  
 694 Gefahrenabwehr und die Wahrnehmung nachrichtendienstlicher Aufgaben zulässig. Für die  
 695 Verfolgung von Ordnungswidrigkeiten könnten solche Auskünfte hingegen nur in gesetzlich  
 696 ausdrücklich benannten Fällen von besonderem Gewicht erlaubt werden.

### 697 1.3.5 Rechtsprechung nationaler Verwaltungs- und Zivilgerichte

698 Zulässigkeit und Grenzen personenbezogener Bewertungsportale im Internet sind Gegenstand der  
 699 Entscheidung des Bundesgerichtshofs (BGH) vom 23. Juni 2009<sup>107</sup>. Der BGH lehnte einen Anspruch  
 700 der klagenden Lehrerin auf Löschung oder Unterlassung der Veröffentlichung ihres Namens, des  
 701 Namens der Schule, der unterrichteten Fächer sowie einer Bewertung durch die Nutzer ab. Auch  
 702 Meinungsäußerungen über eine bestimmte oder bestimmbare Person oder diesbezügliche  
 703 Bewertungen stellten personenbezogene Daten dar. Die Erhebung, Speicherung und Übermittlung  
 704 solcher Beurteilungen richte sich daher nach dem BDSG. Im konkreten Fall sei die Erhebung und  
 705 Speicherung der Bewertung trotz fehlender Einwilligung der Lehrerin gemäß § 29 BDSG zulässig.  
 706 Voraussetzung hierfür ist nach § 29 BDSG, dass „kein Grund zu der Annahme besteht, dass der  
 707 Betroffene ein schutzwürdiges Interesse an dem Ausschluss“ der Datenerhebung und -speicherung  
 708 hat. Bei der Prüfung des „schutzwürdigen Interesses“ hat der BGH eine Abwägung zwischen der  
 709 Meinungsfreiheit der Nutzer aus Art. 5 Abs. 1 GG und dem Persönlichkeitsrecht der Bewerteten  
 710 vorgenommen und im Hinblick auf den konkreten Sachverhalt der Meinungsfreiheit den Vorrang  
 711 eingeräumt.<sup>108</sup>

712

---

<sup>107</sup> BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 – spickmich.de.

<sup>108</sup> Die gegen das Urteil eingelegte Verfassungsbeschwerde hat das BVerfG mit Beschluss vom 16. August 2010 nicht zur Entscheidung angenommen (Az. 1 BvR 1750/09).

713 Mit Urteil vom 9. Dezember 2003<sup>109</sup> hat der BGH zivilrechtliche Ansprüche auf Unterlassung der  
 714 Veröffentlichung in der Presse von Luftbildaufnahmen, die Privathäuser einer Prominenten zeigten,  
 715 abgelehnt. Das Fotografieren der Außenansicht eines Grundstücks von einer allgemein zugänglichen  
 716 Straße aus und die Verbreitung dieser Fotos stelle regelmäßig keine Verletzung des  
 717 Persönlichkeitsrechts dar. Wenn aber jemand „unter Überwindung bestehender Hindernisse oder mit  
 718 geeigneten Hilfsmitteln (Teleobjektiv, Leiter, Flugzeug)“ ein privates Anwesen ausspähe, liege  
 719 grundsätzlich ein Eingriff in die Privatsphäre vor. Im konkreten Fall hat das Gericht dennoch einen  
 720 Unterlassungsanspruch verneint, da bei Abwägung der betroffenen Grundrechte die Pressefreiheit aus  
 721 Art. 5 Abs. 1 GG überwiege. Von der Pressefreiheit nicht gedeckt sei aber die Veröffentlichung einer  
 722 Wegbeschreibung zum Grundstück. Auch die Installation von Überwachungskameras auf einem  
 723 Privatgrundstück kann das Persönlichkeitsrecht eines vermeintlich überwachten Nachbarn  
 724 beeinträchtigen (BGH-Urteil vom 16. März 2010).<sup>110</sup>

725 Zur Frage der internationalen Zuständigkeit deutscher Gerichte gemäß § 32 Zivilprozessordnung  
 726 (ZPO) für Klagen aus unerlaubten Handlungen gegen Veröffentlichungen im Internet hat sich der  
 727 BGH mit Urteil vom 29. März 2011<sup>111</sup> geäußert. Deutsche Gerichte seien für Verletzungen des  
 728 Persönlichkeitsrechts durch Veröffentlichungen im Internet dann zuständig, wenn die fraglichen  
 729 Inhalte „objektiv einen deutlichen Bezug zum Inland (...) aufweisen“. Voraussetzung hierfür sei, dass  
 730 eine Kollision der widerstreitenden Interessen, d. h. des Persönlichkeitsrechts einerseits und des  
 731 Interesses an der Gestaltung des eigenen Internetauftritts oder an der Berichterstattung andererseits,  
 732 nach den Umständen des konkreten Falls, insbesondere auf Grund des konkreten Inhalts der  
 733 Veröffentlichung, im Inland tatsächlich eingetreten sei oder eintreten könne. Das hat das Gericht im  
 734 konkreten Fall verneint, da es sich um die Beschreibung eines privaten Treffens in Russland – verfasst  
 735 auf russisch und in kyrillischer Schrift – handelte. Aus dem deutschen Wohnsitz des Klägers und dem  
 736 Standort des Servers in Deutschland ergebe sich kein hinreichend deutlicher Inlandsbezug.

737 Mit Urteil vom 2. März 2010<sup>112</sup> hat der BGH die Zuständigkeit deutscher Gerichte für eine Klage  
 738 gegen eine Internetveröffentlichung der „New York Times“ hingegen bejaht. Der deutliche  
 739 Inlandsbezug ergab sich nach Auffassung des Gerichts aus dem Inhalt des veröffentlichten Artikels (u.  
 740 a. die Wiedergabe von Berichten deutscher Strafverfolgungsbehörden über das deutsche Unternehmen  
 741 des Klägers) und der Tatsache, dass die „New York Times“ als international anerkannte Zeitung auch  
 742 in Deutschland wahrgenommen werde.

743 In der Rechtsprechung des Bundesarbeitsgerichts (BAG) sind Fragen des Datenschutzes und der  
 744 Persönlichkeitsrechte u. a. in folgenden Entscheidungen aufgegriffen worden: Arbeitgeber und  
 745 Betriebsrat seien grundsätzlich befugt, eine Videoüberwachung im Betrieb einzuführen. Die  
 746 Zulässigkeit des damit verbundenen Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer richte

---

<sup>109</sup> BGH, Urteil vom 9. Dezember 2003 - VI ZR 404/02, NJW 2004, S. 766 – Luftbildaufnahmen.

<sup>110</sup> BGH, Urteil vom 16. März 2010 - VI ZR 176/09, NJW 2010, S. 1533 – Überwachungskamera.

<sup>111</sup> BGH, Urteil vom 29. März 2011 - VI ZR 111/10.

<sup>112</sup> BGH, Urteil vom 2. März 2010 – VI ZR 23/09.

747 sich nach dem Grundsatz der Verhältnismäßigkeit (Beschluss vom 26. August 2008).<sup>113</sup> Bei  
 748 Abschluss von Betriebsvereinbarungen sei gemäß § 75 Abs. 2 Satz 1 Betriebsverfassungsgesetz  
 749 (BetrVG) die freie Entfaltung der Persönlichkeit der beschäftigten Arbeitnehmer zu schützen und  
 750 hierbei auch der Grundsatz der Verhältnismäßigkeit zu wahren. Mit Beschluss vom 12. August  
 751 2008<sup>114</sup> äußerte sich das Gericht zum Leserecht einzelner Mitglieder des Betriebsrates. Das Recht, die  
 752 elektronisch gespeicherten Unterlagen des Betriebsrats einzusehen, umfasse auch das Leserecht auf  
 753 elektronischem Weg, und zwar jederzeit, wie dies in § 34 Abs. 3 BetrVG vorgesehen sei. Dem  
 754 stünden auch die Schweigepflicht der Mitglieder des Betriebsrats und datenschutzrechtliche  
 755 Vorschriften nicht entgegen.

756 Das Bundesverwaltungsgericht (BVerwG) hat mit Urteil vom 8. März 2002<sup>115</sup> die Herausgabe von  
 757 Stasi-Unterlagen mit personenbezogenen Informationen über Personen der Zeitgeschichte, Inhaber  
 758 politischer Funktionen oder Amtsträger in Ausübung ihres Amtes nach der damaligen Fassung des  
 759 Stasi-Unterlagen-Gesetzes für unzulässig erklärt, wenn diese systematisch vom Staatssicherheitsdienst  
 760 ausgespäht wurden. Im Hinblick auf eine mögliche Änderung des Gesetzes weist das Gericht darauf  
 761 hin, dass bei der Weitergabe rechtsstaatswidrig erworbener Informationen dem Persönlichkeitsrecht  
 762 ein höherer Schutz zukomme, als dies bei der sonstigen Veröffentlichung von Informationen über  
 763 Personen der Zeitgeschichte und Amtsträger in Ausübung ihres Amtes der Fall sei.<sup>116</sup>

764 Werden personenbezogene Informationen durch eine sachlich unzuständige Behörde weitergegeben,  
 765 stellt dies einen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung dar. Das  
 766 BVerwG hat hierzu mit Urteil vom 9. März 2005 entschieden, ein Eingriff in das informationelle  
 767 Selbstbestimmungsrecht sei grundsätzlich auch dann nicht gerechtfertigt, wenn die Daten zwar von  
 768 einer anderen Behörde rechtmäßig hätten weitergegeben werden dürfen, im konkreten Fall aber eine  
 769 sachlich unzuständige Behörde gehandelt habe.<sup>117</sup>

770 Nach § 7 Bundesnachrichtendienstgesetz (BNDG) in Verbindung mit § 15 Abs. 1  
 771 Bundesverfassungsschutzgesetz (BVerfSchG) erteilt der Bundesnachrichtendienst dem Betroffenen  
 772 auf Antrag Auskunft über die zu seiner Person gespeicherten Daten, soweit er ein besonderes Interesse  
 773 an der Auskunft darlegt. Das BVerwG hat mit Urteil vom 24. März 2010<sup>118</sup> ausgeführt, dass eine  
 774 Auskunftserteilung unter Berufung auf die in § 15 Abs. 2 BVerfSchG aufgeführten

---

1.1 <sup>113</sup> 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.“

<sup>114</sup> BAG, Beschluss vom 12. August 2009 - 7 ABR 15/08, NZA 2009, 1218.

<sup>115</sup> BVerwG, Urteil vom 08. März 2002 - 3 C 46/01, BVerwGE 116, 104 - Herausgabe von Stasi-Unterlagen.

<sup>116</sup> 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).

<sup>117</sup> BVerwG, Urteil vom 9. März 2005 - 6 C 3/04, NJW 2005, 2330 - Scientology..

<sup>118</sup> BVerwG, Urteil vom 24. März 2010 - 6 A 2/09, DVBl. 2010, 1307 - Auskunftsanspruch BND.



775 Geheimhaltungsgründe nur dann abgelehnt werden könne, wenn eine Abwägung im Einzelfall ergebe,  
 776 dass das Auskunftsinteresse zurückstehen müsse. Dagegen erstreckte sich die Auskunftspflichtung  
 777 von vornherein nicht auf die Herkunft der Daten (§ 15 Abs. 3 BVerfSchG).

### 778 1.3.6 Verwaltungs- und Anwendungspraxis

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

785 Unterschiede in der Verwaltungspraxis, etwa im Bereich von Ermessensentscheidungen, sind daher  
 786 möglich, was insbesondere für deutschlandweit agierende Unternehmen von Bedeutung sein kann, da  
 787 diese im Einzelfall der Aufsicht mehrerer Datenschutzbehörden unterliegen. Zwar wird nach  
 788 langjähriger Praxis die Behörde tätig, in deren Zuständigkeit der Sitz des Unternehmens liegt. Bei  
 789 Unternehmen mit mehreren selbstständigen Regionalgesellschaften bleibt es dennoch bei der  
 790 Zuständigkeit mehrerer Aufsichtsbehörden<sup>119</sup>.

791 Die obersten Landesdatenschutzbehörden für die Aufsicht im nicht-öffentlichen Bereich haben  
 792 deshalb als Koordinierungsgremium den Düsseldorfer Kreis gegründet, dessen Treffen und  
 793 Beschlüsse eine einheitliche Verwaltungspraxis befördern können. Beschlüsse des Düsseldorfer  
 794 Kreises, die allerdings nur einstimmig getroffen werden können, betreffen unterschiedliche Bereiche  
 795 der Aufsicht, im Jahr 2010 etwa die Prüfpflichten des Datenexporteurs im Rahmen des „Safe-  
 796 Harbor“- Abkommens.<sup>120</sup> Bei einer unterschiedlichen Praxis verbleibt es, wenn eine Einigung im  
 797 Düsseldorfer Kreis nicht zustande kommt. So wird etwa die Praxis von Auskunfteien, vor der  
 798 Erteilung von Auskünften zur Identitätsüberprüfung die Zusendung einer Kopie des  
 799 Personalausweises zu verlangen, von den Aufsichtsbehörden teilweise als unzulässig, teilweise aber  
 800 auch als erforderlich angesehen. Auch bei der Videoüberwachung auf Bahnhöfen gab es  
 801 unterschiedliche Bewertungen.

802

## 803 2 Datenschutz

### 804 2.1 Prinzipien, Ziele, Werte

#### 805 2.1.1 Schutzgegenstand

806 Datenschutz bildet den zentralen Motor des Vertrauens und der Akzeptanz moderner  
 807 informationstechnischer Entwicklungen. Ziel des Datenschutzrechts ist der Erhalt und die Stärkung  
 808 des Persönlichkeitsrechts unter den Bedingungen der Datenverarbeitung und -erhebung, insbesondere  
 809 in Gestalt des Rechts auf informationelle Selbstbestimmung. Der Erhalt der Kontrolle über den  
 810 Umgang mit Daten und Informationen, die einen selbst betreffen, ist das zwingende Äquivalent einer

<sup>119</sup> 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).

<sup>120</sup> 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](https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/index.php) (zuletzt aufgerufen am: 17. März 2011).

811 auf die Stärkung des Einzelnen wie auch unseres demokratischen Gemeinwesens insgesamt  
812 abzielenden gesellschaftlichen Gesamtentwicklung.

813 Zentraler Anknüpfungspunkt des bestehenden Datenschutzkonzepts sind die so genannten  
814 „personenbezogenen Daten“.<sup>121</sup> Im Mittelpunkt der Abwägungen des Datenschutzes aber stehen  
815 Informationen, nicht Daten. Es geht regelmäßig um Interessen der Grundrechtsträger, dass staatliche  
816 Stellen oder Dritte etwas nicht als Information erfahren und nutzen können, und auf der anderen Seite  
817 um deren Wissens- und Verwertungsinteressen.

818 Personenbezogene Daten werden definiert als „Einzelangaben über persönliche oder sachliche  
819 Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person“ (Art. 2 lit. a DSRL, § 3 Abs. 1  
820 BDSG). Der Begriff wird weit verstanden und umfasst praktisch jede Information, die mit einer  
821 natürlichen Person in Verbindung gebracht werden kann. Es genügt also eine  
822 „Personenbeziehbarkeit“.<sup>122</sup> Angaben über persönliche Verhältnisse betreffen etwa  
823 Identifikationsmerkmale, äußere Merkmale, aber auch innere Zustände (z.B. Meinungen), Angaben  
824 über sachliche Verhältnisse dagegen alle Beziehungen des Betroffenen zu Dritten und zur Umwelt  
825 (z.B. Eigentumsverhältnisse, Vertragsbeziehungen).<sup>123</sup>

826 Auch das BVerfG geht in seiner ständigen Rechtsprechung von einem weiten Verständnis aus. So hat  
827 das Gericht in seinem wegweisenden Volkszählungsurteil zu den Angaben personenbezogener Daten  
828 ausgeführt: „Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen  
829 einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der  
830 Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab.  
831 Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit  
832 gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum  
833 mehr.“<sup>124</sup>

834 Weiterer regulatorischer Anknüpfungspunkt ist der Umgang mit diesen Daten. Dabei werden in der  
835 DSRL und im BDSG unterschiedliche Begrifflichkeiten verwendet. Während in der DSRL die  
836 „Verarbeitung“ (im weiteren Sinne) der Daten als Oberbegriff für jeden Vorgang im Zusammenhang  
837 mit den personenbezogenen Daten zu verstehen ist (Art. 2 lit. b DSRL), unterscheidet das BDSG  
838 zwischen den einzelnen Vorgängen der Erhebung, Verarbeitung (im engeren Sinne) und (sonstigen)  
839 Nutzung der Daten (§ 4 Abs. 1 BDSG). Materiell erfasst sind vor allem die Erhebung, Speicherung,  
840 Veränderung, Übermittlung, Sperrung und Löschung von personenbezogenen Daten. Dabei ist ein  
841 technikneutrales Verständnis zu Grunde zu legen. Erfasst sind sowohl automatische als auch nicht-  
842 automatische Verfahren.<sup>125</sup>

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

---

<sup>121</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 100.

<sup>122</sup> Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 40.

<sup>123</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 101.

<sup>124</sup> BVerfGE 65, 1, 45 - Volkszählung.

<sup>125</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 49.

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

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

859 2.1.2 Grundprinzipien des Datenschutzrechts

### 860 Erlaubnisvorbehalt

861 Ein zentraler Grundsatz des Datenschutzrechts lässt sich in einem Satz wie folgt formulieren: Der  
862 Umgang mit personenbezogenen Daten ist verboten, es sei denn, der Betroffene willigt ein oder eine  
863 Rechtsnorm legitimiert ihn. Dieser Grundsatz ist sowohl im Gemeinschaftsrecht (Art. 7 DSRL), als  
864 auch im nationalen allgemeinen (§ 4 Abs. 1 BDSG) und bereichsspezifischen Datenschutzrecht (z. B.  
865 § 12 TMG) normiert. Demnach bestimmt sich die Zulässigkeit eines jeden einzelnen  
866 Datenverarbeitungsvorgangs danach, ob der Betroffene den Vorgang erlaubt hat oder ob er sich auf  
867 einen gesetzlichen Erlaubnistatbestand stützen lässt.<sup>126</sup>

868 Die Einwilligung ist vor allem im nicht-öffentlichen Bereich, neben den vertraglichen Legitimationen,  
869 von erheblicher Bedeutung.<sup>127</sup> Sie legitimiert einen Datenverarbeitungsvorgang nur dann, wenn sie  
870 wirksam erteilt wurde, wofür das Gesetz bestimmte Mindestanforderungen vorsieht (vgl. § 4a BDSG  
871 oder auch Art. 7 lit. a) DSRL). Nach nationalem Recht (§ 4a BDSG) ist eine Einwilligung nur  
872 wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, also ohne Zwang erfolgt. Dies  
873 setzt voraus, dass der Einzelne Bedeutung und Tragweite seiner Entscheidung erkennen kann.

874 Die Einwilligung in die Datenerhebung oder -verarbeitung ist daher nur dann zulässig, wenn die  
875 betreffende Person „ohne jeden Zweifel ihre Einwilligung gegeben“<sup>128</sup> hat. Dies impliziert, dass die  
876 Einwilligung informiert, aktiv und freiwillig zu geschehen hat. Eine informierte Einwilligung setzt  
877 Transparenz und Kenntnis voraus. Allein durch die Nutzung einer Website kann keine aktive  
878 Einwilligung erteilt werden. Auch das Beibehalten von Einstellungen von Internetdiensten oder  
879 Browsern, die in der Voreinstellung nicht „privacy by default“ vorsehen, genügt nicht der Fiktion  
880 einer aktiven Einwilligung. Hier wird die Kenntnis der möglichen Einstellungen und ihrer  
881 Veränderungsmöglichkeiten vorausgesetzt, die jedoch weder bei jedem Nutzer gleichermaßen  
882 gegeben noch von allen Diensteanbietern gefördert wird.

883 An der Möglichkeit zu einer freien Entscheidung kann es fehlen, wenn die Einwilligung in einer  
884 Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird oder wenn der  
885 Betroffene durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten  
886 verleitet wird.

<sup>126</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 130 f.

<sup>127</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 131.

<sup>128</sup> Vgl. Art. 7 lit. a) DSRL.

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

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

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

903  
904 Die Frage von Transparenz- und Informationspflichten stellt sich in besonderem Maße. Auch Art und  
905 Weise der Informationspraxis sind bestimmend dafür, in welchem Umfang Bürgerinnen und Bürger  
906 bei Erteilung ihrer Einwilligung einschätzen können, welche Daten zu welchem Zweck gespeichert  
907 werden sollen.

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

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

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

930

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

### 933 **Erforderlichkeitsgrundsatz**

934 Der Erforderlichkeitsgrundsatz folgt aus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz  
935 und ist zudem in Art. 7 lit. b) bis f) DSRL festgeschrieben. Er steht in engem Zusammenhang mit dem  
936 Grundsatz der Zweckfestlegung und der Zweckbindung. Demnach ist der Umgang mit  
937 personenbezogenen Daten auf das zum Erreichen des angestrebten Zieles erforderliche Minimum zu  
938 beschränken.<sup>129</sup> Es sollen nur so viele Daten erhoben, verarbeitet oder genutzt werden, wie zur  
939 Zweckerreichung unbedingt notwendig. Für den öffentlichen Bereich ist der Grundsatz in §§ 13 bis 16  
940 BDSG (insbesondere in den Abs. 1) normiert, wobei der zulässige Zweck auf die öffentliche  
941 Aufgabenerfüllung begrenzt ist. Der Erforderlichkeitsgrundsatz gilt aber auch im nicht-öffentlichen  
942 Bereich, wo seine effektive Verwirklichung durch eine möglichst genaue Zweckbestimmung bedingt  
943 ist.<sup>130</sup>

### 944 **Zweckbindungsgrundsatz**

945 Der Zweckbindungsgrundsatz besagt, dass die Daten, die für einen bestimmten Zweck erhoben  
946 worden sind, auch nur zu diesem Zweck verarbeitet oder genutzt werden dürfen.<sup>131</sup> Der Zweck der  
947 Datenerhebung begrenzt folglich den weiteren Umgang mit den erhobenen Daten. Sie dürfen nur zu  
948 dem Zweck weiter verwendet werden, der von der Einwilligung oder der konkret legitimierenden  
949 Rechtsnorm erfasst ist. Das setzt voraus, dass das Ziel der Datenverarbeitung und/oder -nutzung  
950 bereits vor der Datenerhebung so genau wie möglich bestimmt ist. Eine Speicherung auf Vorrat für  
951 künftige, noch nicht bekannte Zwecke ist dagegen grundsätzlich unzulässig.<sup>132</sup>

952 Vor allem im nicht-öffentlichen Bereich stößt die Beibehaltung dieses Grundsatzes auf praktische  
953 Probleme. In einer vernetzten Welt ist der Datenaustausch oftmals durch Spontanität und gerade nicht  
954 durch eine vorherige Festlegung des Verarbeitungszweckes bestimmt.<sup>133</sup>

### 955 **Transparenzgrundsatz**

956 Die informationelle Selbstbestimmung setzt nach Auffassung des Bundesverfassungsgerichts voraus,  
957 dass Bürger wissen und grundsätzlich auch entscheiden können sollen, „wer was wann und bei  
958 welcher Gelegenheit“ über sie weiß.<sup>134</sup> Das setzt wiederum voraus, dass Datenerhebungs-, -  
959 verarbeitungs- und -nutzungsvorgänge transparent gestaltet werden. Zudem ist der  
960 Transparenzgrundsatz die grundlegende Voraussetzung dafür, dass Betroffene aktive  
961 Datenschutzrechte wahrnehmen können. Transparenz wird in erster Linie durch den Grundsatz der  
962 Direkterhebung verwirklicht, wonach die Daten grundsätzlich beim Betroffenen zu erheben sind (§ 4  
963 Abs. 2 S. 1, Abs. 3 BDSG), sodass er unmittelbar Kenntnis von dem Vorgang erlangt. Nur unter  
964 engen Voraussetzungen darf die Datenerhebung ohne Mitwirkung des Betroffenen erfolgen (§ 4 Abs.

---

<sup>129</sup> BVerfGE 65, 1, 46 - Volkszählung.

<sup>130</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 136.

<sup>131</sup> Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 48.

<sup>132</sup> Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003, S. 48.

<sup>133</sup> Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung. Verw 2007, 153 (159).

<sup>134</sup> BVerfGE 65, 1, 43 - Volkszählung.

965 2 S. 2 BDSG). Flankiert wird das Transparenzgebot durch Auskunftsrechte und Informations-,  
 966 Benachrichtigungs-, Unterrichts-, Hinweis- und Aufklärungspflichten der verantwortlichen  
 967 Stelle.<sup>135</sup>

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

## 970 **Prinzip der Datenvermeidung und Datensparsamkeit**

971 Der Grundsatz der Datenvermeidung und Datensparsamkeit ist – obwohl nicht durch die DSRL  
 972 vorgegeben – in § 3a BDSG normiert und besagt, dass so wenig personenbezogene Daten wie möglich  
 973 erhoben, verarbeitet oder genutzt werden sollen und auch die Datenverarbeitungssysteme an diesem  
 974 Ziel auszurichten sind. Dabei handelt es sich um eine Konkretisierung des  
 975 Erforderlichkeitsgrundsatzes auf technischer Ebene: Schon durch die entsprechende  
 976 Technikgestaltung soll das Recht auf informationelle Selbstbestimmung präventiv geschützt  
 977 werden.<sup>136</sup> Da der Grundsatz nicht sanktionsbewehrt ist, ist er – obwohl als Rechtspflicht formuliert –  
 978 eher als Programmsatz zu verstehen.<sup>137</sup>

### 979 2.1.3 Datenschutz im Grundgesetz

## 980 **Verfassungsrechtliche Verortung**

981 Der Grundrechtskatalog des Grundgesetzes enthält im Gegensatz zur Grundrechtecharta der  
 982 Europäischen Union (GRC) kein explizites Grundrecht des Datenschutzes.<sup>138</sup> Gleichwohl ist der  
 983 Datenschutz ein Wert von Verfassungsrang und nimmt über verschiedene Grundrechte am  
 984 Grundrechtsschutz teil. Namentlich finden sich datenschutzrechtliche Gehalte im Allgemeinen  
 985 Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG), im Brief-, Post- und  
 986 Fernmeldegeheimnis (Art. 10 GG) und im Grundrecht der Unverletzlichkeit der Wohnung (Art. 13  
 987 GG). Als vorläufiger Höhepunkt in der Judikatur des verfassungsrechtlichen Datenschutzes wird das  
 988 „IT-Grundrecht“ auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer  
 989 Systeme angesehen.<sup>139</sup>

## 990 **IT-Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer** 991 **Systeme**

992 Als besondere Ausprägung des allgemeinen Persönlichkeitsrechts hat das Bundesverfassungsgericht  
 993 im Hinblick auf Online-Durchsuchungen das sog. IT- bzw. Computergrundrecht auf Gewährleistung  
 994 der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt.<sup>140</sup> Es „schützt vor  
 995 Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie  
 996 insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung

---

<sup>135</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 136.

<sup>136</sup> Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 3a Rn. 1.

<sup>137</sup> Gola, Peter/Schomerus, Rudolf. BDSG. Kommentar. 10. Auflage 2010, § 3a Rn. 2.

<sup>138</sup> 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.

<sup>139</sup> Vgl. Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1036).

<sup>140</sup> BVerfGE 120, 274, 302 ff. – Onlinedurchsuchung.

997 gewährleistet ist.“<sup>141</sup> Der Schutz des Art. 10 Abs. 1 Var. 3 GG versagt, wenn der  
 998 Kommunikationsvorgang beendet ist oder der Zugriff außerhalb eines laufenden  
 999 Kommunikationsvorgangs des Betroffenen erfolgt, was bei der Infiltration eines Computers  
 1000 regelmäßig der Fall ist.<sup>142</sup> Art. 13 GG bietet raumbezogenen Schutz, welcher „nicht in der Lage ist,  
 1001 die spezifische Gefährdung des informationstechnischen Systems abzuwehren“, da der Eingriff  
 1002 standortunabhängig über das Internet erfolgen kann.<sup>143</sup> Das Recht auf informationelle  
 1003 Selbstbestimmung trägt „den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich  
 1004 daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung  
 1005 informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut  
 1006 oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System  
 1007 zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen,  
 1008 ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein  
 1009 solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne  
 1010 Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit  
 1011 hinaus.“<sup>144</sup>

1012 Erfasst sind Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des  
 1013 Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System  
 1014 es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen  
 1015 oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“, wie z. B. bei Personalcomputern  
 1016 oder Mobiltelefonen und elektronischen Terminkalendern, die über einen großen Funktionsumfang  
 1017 verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.<sup>145</sup> Geschützt  
 1018 wird nicht nur vor einer Verletzung der Vertraulichkeit dieser Daten, sondern bereits vor dem  
 1019 Antasten der Integrität des Systems, da hierdurch „die entscheidende technische Hürde für eine  
 1020 Ausspähung, Überwachung oder Manipulation des Systems genommen“ ist.<sup>146</sup>

1021 Dabei betont das Bundesverfassungsgericht, dass „der Standort des Systems ... ohne Belang und  
 1022 oftmals für die Behörde nicht einmal erkennbar“ sei, was „insbesondere für mobile  
 1023 informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder  
 1024 Mobiltelefone“ gelte.<sup>147</sup> Daraus lässt sich schließen, dass der Schutz unabhängig davon zu  
 1025 gewährleisten ist, wo der Datenbestand gespeichert ist.

1026 Die Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung erfolgt in erster Linie nach  
 1027 quantitativen Gesichtspunkten. Während das Grundrecht auf informationelle Selbstbestimmung  
 1028 Schutz vor Zugriff auf einzelne personenbezogene Daten gewährt, geht es beim (IT-)Grundrecht auf  
 1029 Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme um den Schutz  
 1030 einer Vielzahl von (personenbezogenen) Daten (Datenbestand), die auf einem  
 1031 informationstechnischen System gespeichert sind. Denn wenn lediglich Daten mit einem punktuellen  
 1032 Bezug zu einem bestimmten Lebensbereich abgerufen werden, unterscheidet sich der staatliche

---

<sup>141</sup> BVerfGE 120, 274, 302 – Onlinedurchsuchung.

<sup>142</sup> BVerfGE 120, 274, 307 f. – Onlinedurchsuchung.

<sup>143</sup> BVerfGE 120, 274, 310 – Onlinedurchsuchung.

<sup>144</sup> BVerfGE 120, 274, 312 f. – Onlinedurchsuchung.

<sup>145</sup> BVerfGE 120, 274, 314 – Onlinedurchsuchung.

<sup>146</sup> BVerfGE 120, 274, 314 – Onlinedurchsuchung.

<sup>147</sup> BVerfGE 120, 274, 310 f. – Onlinedurchsuchung.

1033 Zugriff auf informationstechnische Systeme nicht von anderen Datenerhebungen und das Recht auf  
 1034 informationelle Selbstbestimmung ist anzuwenden.<sup>148</sup> Abgrenzungskriterium sind demnach Umfang  
 1035 und Vielfalt der Daten und das Ausmaß der durch die Daten zu gewinnenden Rückschlüsse auf die  
 1036 Person des Betroffenen. Ermöglicht die Datenerhebung potentiell eine umfassende  
 1037 Erkenntnisgewinnung über den Betroffenen, so ist das (IT-)Grundrecht auf Gewährleistung der  
 1038 Vertraulichkeit und Integrität informationstechnischer Systeme einschlägig.<sup>149</sup>

1039 2.1.4 Das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen  
 1040 Persönlichkeitsrechts

1041 Das allgemeine Persönlichkeitsrecht wird aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet. Es  
 1042 enthält mehrere Elemente und dient einerseits dem Schutz eines sozialen und räumlichen  
 1043 Rückzugsbereichs des Einzelnen und andererseits dem Schutz der individuellen Freiheit, selbst über  
 1044 die Präsentation der eigenen Person bestimmen zu können.<sup>150</sup>  
 1045 Zur zweiten Gruppe gehören das Recht am eigenen Bild und am eigenen Wort und das seit dem  
 1046 Volkszählungsurteil aus dem Jahr 1983<sup>151</sup> verfassungsgerichtlich anerkannte Recht auf  
 1047 informationelle Selbstbestimmung. „Das Grundrecht gewährleistet insoweit die Befugnis des  
 1048 Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu  
 1049 bestimmen.“<sup>152</sup>

1050 Informationelle Selbstbestimmung und Internet

1051 Das Internet gibt den Menschen die Chance, selbstbestimmt und selbstbewusst ihr Leben zu gestalten.  
 1052 Innovative Nutzungsmöglichkeiten prägen den heutigen Alltag und stellen sich oft als Bereicherung  
 1053 oder praktische Hilfe dar. Die Möglichkeiten zur Information, Kommunikation und Interaktion  
 1054 werden erweitert.

1055 Viele dieser Chancen und Möglichkeiten gehen einher mit der Speicherung, Verarbeitung und  
 1056 Übermittlung zahlreicher Daten. Voraussetzung für viele Informations- und Kommunikationsdienste  
 1057 sind personenbezogene Daten. Diese Dienste sind aber auch missbrauchs anfällig, sei es, dass mehr  
 1058 Daten als erforderlich gespeichert werden, sei es, dass Nichtberechtigte Zugang zu sensiblen Daten  
 1059 erlangen. Der Umgang mit personenbezogenen Daten hat sich im digitalen Zeitalter erheblich  
 1060 verändert. Im Kontext des Internet ist die Verarbeitung von personenbezogenen Daten vielfach ein  
 1061 wirtschaftliches Geschäftsmodell. Insbesondere in sozialen Netzwerken, aber auch bei anderen  
 1062 Diensten im Internet, werden eine Vielzahl von Daten von Nutzerinnen und Nutzern selbst zur  
 1063 Verfügung gestellt.

1064 Durch die zunehmende Vernetzung, die Möglichkeit der Verknüpfung von personenbezogenen Daten  
 1065 (Persönlichkeitsprofile) und die ständige Weiterentwicklung automatischer Datenerfassungssysteme  
 1066 potenziert sich die Gefahr für das allgemeine Persönlichkeitsrecht in einer „Welt der allgegenwärtigen  
 1067 Datenverarbeitung“<sup>153</sup>. Diese Gefahr besteht nicht nur im Verhältnis Bürger - Staat, sondern auch im

---

<sup>148</sup> BVerfGE 120, 274, 313 – Onlinedurchsuchung.

<sup>149</sup> Hinz, Christian: Onlinedurchsuchungen. JURA 2009, 141 (144).

<sup>150</sup> Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1037).

<sup>151</sup> BVerfGE 65, 1 - Volkszählung.

<sup>152</sup> BVerfGE 65, 1, 43 - Volkszählung.

<sup>153</sup> Zum diesem Begriff: Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung. Verw 2007, 153 (155 ff.).



1068 Verhältnis Bürger - Bürger und Verbraucher - Unternehmen untereinander. Dies zeigt sich besonders  
 1069 deutlich bei den Diensteanbietern im Internet. Der Erfolg von Google oder sozialen Netzwerken wie  
 1070 Facebook und studiVZ oder Internet Providern ist geradezu dadurch bedingt, dass diese gigantische  
 1071 informationelle Infrastrukturen bereithalten.<sup>154</sup> Hier sind die Grundrechte zwar nicht (unmittelbar)  
 1072 anwendbar. Der Staat ist aber verpflichtet, „dem Einzelnen Schutz davor zu bieten, dass private Dritte  
 1073 ohne sein Wissen und ohne seine Einwilligung Zugriff auf die seine Individualität kennzeichnenden  
 1074 Daten nehmen“<sup>155</sup> (grundrechtliche Schutzpflicht). Schließlich hat die Verbreitung und Verarbeitung  
 1075 der eigenen personenbezogenen Daten im Internet mittlerweile die Grenzen der Nachvollziehbarkeit  
 1076 für den Einzelnen erreicht.

1077 Der gegenwärtig diskutierte Datenschutz in sozialen Netzwerken wirft aber auch weitere Fragen auf.  
 1078 Diese betreffen insbesondere das Verhältnis der Nutzerinnen und Nutzer zu den Anbietern  
 1079 entsprechender Plattformen, beispielsweise wenn im Hintergrund personenbezogene Daten gesammelt  
 1080 und in Profilen zusammengeführt werden. Auch in diesem Fall muss der Schutz auf informationelle  
 1081 Selbstbestimmung erhalten bleiben. Schließlich setzt die freie Entfaltung der Persönlichkeit auch  
 1082 voraus, dass der Einzelne gegen die unbegrenzte Erhebung, Speicherung, Verwendung und  
 1083 Weitergabe seiner persönlichen Daten geschützt wird.<sup>156</sup> Durch diese Schutzwirkung wird der  
 1084 abschreckende Effekt fremden (staatlichen und in Unternehmen vorhandenen) Geheimwissens  
 1085 gehemmt, „der entstehen und zur Beeinträchtigung bei der Ausübung anderer Grundrechte führen  
 1086 kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit  
 1087 über ihn weiß.“<sup>157</sup> Mit anderen Worten: Wer befürchten muss, dass seine „Verhaltensweisen jederzeit  
 1088 notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird  
 1089 versuchen, nicht durch solche Verhaltensweisen aufzufallen.“<sup>158</sup>

1090 Mittlerweile hat sich daher ein kontextbezogener und gesetzlich zu gewählender Schutzrahmen mit  
 1091 unterschiedlichen Komponenten auf verschiedenen Ebenen herausgebildet. Dies reicht von  
 1092 gesetzlichen Regelungen im BDSG (wie beispielsweise dem bußgeldbewährten Kopplungsverbot des  
 1093 § 28 Abs. 3b BDSG), über die Auferlegung entsprechender Transparenz- und Informationspflichten  
 1094 für Betreiber von Diensten im Internet, bis hin zu einer Förderung der Medienkompetenz der  
 1095 Nutzerinnen und Nutzer für einen verantwortungsvollen Umgang mit den eigenen personenbezogenen  
 1096 Daten.

#### 1097 2.1.5 Einschränkungen von Grundrechten / Kollidierende Rechtsgüter

1098 Gerade im Bereich des Internet sind zum Teil schwierige Grundrechtskollisionen vorgezeichnet, wie  
 1099 z.B. die so genannte Spickmich-Entscheidung des BGH zeigt.<sup>159</sup> Pauschale Gegenüberstellungen etwa  
 1100 mit dem Eigentumsgrundrecht oder der Berufsausübungsfreiheit aber verbieten sich, da oft genug  
 1101 gefragt werden muss, ob bestimmte Grundrechtsausübungen zugleich den Schutz des Umgangs mit  
 1102 den Daten von dritten Grundrechtsträgern umfassen. Hier ist eine besonders differenzierte Darstellung  
 1103 zu empfehlen.

---

<sup>154</sup> Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035 (1039).

<sup>155</sup> BVerfG, Urteil vom 13. Februar 2007 - 1 BvR 421/05, BVerfGE 117, 202, 229 - Vaterschaftsfeststellung.

<sup>156</sup> BVerfGE 65, 1, 43 - Volkszählung.

<sup>157</sup> BVerfGE 113, 29, 46 - Beschlagnahme von Datenträgern.

<sup>158</sup> BVerfGE 65, 1, 43 - Volkszählung.

<sup>159</sup> BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328; vgl. auch unter 1.3.5.

1104 Jedermann hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten  
 1105 grundsätzlich selbst zu bestimmen. Einschränkungen dieses Rechts auf informationelle  
 1106 Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Dieses „Recht auf  
 1107 informationelle Selbstbestimmung“, wie es das Bundesverfassungsgericht 1983 in seiner  
 1108 Entscheidung zur Volkszählung, also im Hinblick auf eine staatliche Maßnahme, beschrieben hat, ist  
 1109 einerseits - als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1  
 1110 Abs. 1 GG – ein individuelles Abwehrrecht gegenüber staatlichen Eingriffen.

1111 Nach der Rechtsprechung des Bundesverfassungsgerichts wirkt sich das Recht auf informationelle  
 1112 Selbstbestimmung aber andererseits im Sinne einer Drittwirkung auch auf die Auslegung und  
 1113 Anwendung privatrechtlicher Vorschriften aus und begründet staatliche Schutzpflichten. Die  
 1114 staatliche Gewalt ist danach verpflichtet, dem Einzelnen seine informationelle Selbstbestimmung im  
 1115 Verhältnis zu Dritten zu ermöglichen.<sup>160</sup> Gegebenenfalls müssen staatlicherseits die rechtlichen  
 1116 Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an  
 1117 Kommunikationsprozessen teilnehmen kann.<sup>161</sup>

1118 Nicht jede Beeinträchtigung eines grundrechtlichen Schutzbereichs führt per se zur  
 1119 Verfassungswidrigkeit der Maßnahme. Zum einen kann der Betroffene in die Maßnahme einwilligen  
 1120 und seine Daten freiwillig preisgeben, was vom Staat zu respektieren ist.<sup>162</sup> Aber auch ohne  
 1121 Einwilligung wird der verfassungsrechtliche Datenschutz nicht grenzenlos gewährleistet, sondern  
 1122 kann beschränkt werden. Das Bundesverfassungsgericht hat hierzu bereits 1983 im so genannten  
 1123 Volkszählungsurteil dargelegt: "Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen,  
 1124 grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.  
 1125 Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im  
 1126 überwiegenden Allgemeininteresse zulässig." <sup>163</sup>

1127 Für diese Schrankenziehung hat das Bundesverfassungsgericht seit dem Volkszählungsurteil eine  
 1128 Reihe von Vorgaben aufgestellt, die es zu beachten gilt. Dabei gelten für die genannten Grundrechte  
 1129 weitgehend die gleichen Maßstäbe.<sup>164</sup>

1130 Grundlegende Voraussetzung für einen zulässigen Eingriff in das Recht auf informationelle  
 1131 Selbstbestimmung ist das Vorhandensein einer gesetzlichen Grundlage, welche die Voraussetzungen  
 1132 und den Umfang der Beschränkungen klar erkennen lässt.<sup>165</sup> Das Erfordernis einer gesetzlichen  
 1133 Grundlage (Gesetzesvorbehalt) folgt bereits aus Art. 2 Abs. 1 GG, wonach das allgemeine  
 1134 Persönlichkeitsrecht nur innerhalb der verfassungsmäßigen Ordnung gewährleistet wird. Die  
 1135 gesetzliche Grundlage muss dem Gebot der Normenklarheit entsprechen, was bedeutet, dass Anlass,

---

<sup>160</sup> BVerfG, Beschluss vom 23. Oktober 2006 – BvR 2027/02, Rn. 30.

<sup>161</sup> BVerfG, Beschluss vom 23. Oktober 2006 – BvR 2027/02, Rn. 33.

<sup>162</sup> Vgl. BVerfG, Beschluss vom 23. Oktober 2006 – BvR 2027/02, Rn. 34; Schoch, Friedrich: Das Recht auf informationelle Selbstbestimmung. JURA 2008, 352 (357).

<sup>163</sup> BVerfGE 65, 1, 43 – Volkszählung.

<sup>164</sup> 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.).

<sup>165</sup> BVerfGE 65, 1, 44 - Volkszählung.

- 1136 Zweck und Grenzen eines Eingriffs in der Ermächtigung bereichsspezifisch, präzise und für den  
 1137 Bürger klar erkennbar festgelegt werden müssen.<sup>166</sup>
- 1138 Weiterhin muss der Verhältnismäßigkeitsgrundsatz beachtet werden. Das bedeutet, dass die  
 1139 Maßnahme einen legitimen Zweck verfolgen, zu dessen Erreichung geeignet, erforderlich und  
 1140 verhältnismäßig sein muss.<sup>167</sup> Der Zweck muss von vornherein bestimmt sein. Die ständige  
 1141 Rechtsprechung des Bundesverfassungsgerichts bringt deutlich zum Ausdruck, „dass dem Staat eine  
 1142 Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbar  
 1143 Zwecken verfassungsrechtlich strikt untersagt ist.“<sup>168</sup>
- 1144 Es besteht demnach ein "Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung,  
 1145 Verwendung und Weitergabe seiner persönlichen Daten". Das Grundrecht auf informationelle  
 1146 Selbstbestimmung wird als besondere Ausprägung des schon zuvor grundrechtlich geschützten  
 1147 allgemeinen Persönlichkeitsrechts angesehen. Wie dieses wird es verfassungsrechtlich aus Art. 2  
 1148 Abs. 1 (so genannte allgemeine Handlungsfreiheit) in Verbindung mit Art. 1 Abs. 1 GG  
 1149 (Menschenwürde-Garantie) hergeleitet.
- 1150 In der Verhältnismäßigkeitsprüfung findet eine Güterabwägung zwischen dem verfolgten Zweck und  
 1151 dem Recht auf informationelle Selbstbestimmung statt. Dabei ist von der Prämisse auszugehen, dass  
 1152 Grundrechte „jeweils nur soweit beschränkt werden dürfen, als es zum Schutze öffentlicher Interessen  
 1153 unerlässlich ist.“<sup>169</sup> In der Abwägung ist vor allem das Gewicht der Grundrechtsbeeinträchtigung zu  
 1154 beachten. Bei der Beurteilung der Schwere des Eingriffs sind z. B. die folgenden Kriterien zu  
 1155 berücksichtigen:
- 1156 • in welche Sphäre die Maßnahme eingreift (Sozial-, Privat- oder Intimsphäre);<sup>170</sup> die  
 1157 unterschiedliche Schutzintensität der drei Sphären kann aber nicht im Sinne eines starren  
 1158 Schemas verstanden werden, sondern nur als erster Orientierungspunkt für die Intensität der  
 1159 Grundrechtsbeeinträchtigung und für die Gewichtung der diese Beeinträchtigung  
 1160 rechtfertigenden Gründe;
  - 1161 • wie viele Grundrechtsträger betroffen sind;<sup>171</sup>
  - 1162 • wie intensiv die Beeinträchtigungen sind;<sup>172</sup>
  - 1163 • welche Inhalte von dem Eingriff erfasst werden, insbesondere welchen Grad an  
 1164 Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung  
 1165 mit anderen aufweisen;<sup>173</sup>

<sup>166</sup> Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht. 2008, S. 79 m.w.N. aus der Rechtsprechung des BVerfG.

<sup>167</sup> BVerfGE 115, 320, 345 ff. – Rasterfahndung II.

<sup>168</sup> BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08, NJW 2010, 833 (839 Rn. 213) - Vorratsdatenspeicherung.

<sup>169</sup> BVerfGE 65, 1, 44 - Volkszählung.

<sup>170</sup> In die Intimsphäre darf gar nicht eingegriffen werden, in die Privat- oder Geheimnisphäre 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.

<sup>171</sup> BVerfGE 115, 320, 347 – Rasterfahndung II.

<sup>172</sup> BVerfGE 115, 320, 347 – Rasterfahndung II.

<sup>173</sup> BVerfGE 115, 320, 348 – Rasterfahndung II.

- 1166 • ob besondere Vertraulichkeitserwartungen verletzt werden;<sup>174</sup>
- 1167 • auf welchem Weg die Inhalte erlangt werden;<sup>175</sup>
- 1168 • welche weiteren Folgen oder Nachteile die Datenerhebung nach sich ziehen kann, z. B.
- 1169 - das Risiko, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, das über das allgemeine
- 1170 Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden,
- 1171 - eine stigmatisierende Wirkung;<sup>176</sup>
- 1172 • die Heimlichkeit einer staatlichen Maßnahme, welche z.B. die Möglichkeit der
- 1173 Inanspruchnahme von Rechtsschutz im Vergleich zur offenen Datenerhebung wesentlich
- 1174 erschwert;<sup>177</sup>
- 1175 • der Verdachtsgrad;
- 1176 • über welchen Zeitraum die Daten erhoben, verarbeitet und genutzt werden können;
- 1177 • und die Streubreite einer Maßnahme.

1178 Zum zuletzt genannten Punkt hat das Bundesverfassungsgericht ausgeführt: „Grundrechtseingriffe, die  
 1179 sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei  
 1180 denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in  
 1181 keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht  
 1182 veranlasst haben – weisen grundsätzlich eine hohe Eingriffsintensität auf. (...) Denn der Einzelne ist in  
 1183 seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen  
 1184 Eingriff Anlass gegeben hat. Von solchen Eingriffen können ferner Einschüchterungseffekte  
 1185 ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können. (...) Es  
 1186 gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu  
 1187 beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen (...)“<sup>178</sup>

1188 Das Bundesverfassungsgericht hat eine anlasslose Speicherung von  
 1189 Telekommunikationsverkehrsdaten zwar nicht schlechthin als verfassungswidrig angesehen, aber  
 1190 betont, dass es sich um einen besonders schweren Eingriff handle, der höchsten  
 1191 verfassungsrechtlichen Anforderungen bei der Ausgestaltung der Regelungen unterliegt.

1192 Je schwerer die Grundrechtsbeeinträchtigung wiegt, desto höher muss das staatliche Schutzgut  
 1193 wiegen, um den Eingriff rechtfertigen zu können. In die Waagschale gelegt werden können hier z. B.:

- 1194 • die Sicherheit des Staates als verfasste Friedens- und Ordnungsmacht und die von ihm zu
- 1195 gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit;<sup>179</sup>

---

<sup>174</sup> BVerfGE 115, 320, 348 – Rasterfahndung II.

<sup>175</sup> BVerfGE 115, 320, 348 – Rasterfahndung II.

<sup>176</sup> BVerfGE 115, 320, 351 ff. – Rasterfahndung II.

<sup>177</sup> 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.

<sup>178</sup> BVerfGE 115, 320, 354 f. – Rasterfahndung II.

<sup>179</sup> BVerfGE 120, 274, 319 und 328 – Onlinedurchsuchung.

- 1196 • die Abwehr von Beeinträchtigungen der Grundlagen einer freiheitlichen demokratischen  
1197 Grundordnung;<sup>180</sup>
- 1198 • die Sicherung der Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher  
1199 Versorgungseinrichtungen;<sup>181</sup>
- 1200 • die Verhütung und Verfolgung von Straftaten von erheblicher Bedeutung<sup>182</sup> bzw.  
1201 schwerwiegender Straftaten.<sup>183</sup>
- 1202 Eine absolute Grenze der Zulässigkeit einer Datenerhebung bildet die Schranken-Schranke des  
1203 unantastbaren Kernbereichs privater Lebensgestaltung, insbesondere im Bereich der Intimsphäre.  
1204 Staatliche Stellen „haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren,  
1205 dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt. (...) Selbst überwiegende Interessen der  
1206 Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen. (...) Zur Entfaltung der Persönlichkeit  
1207 im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie  
1208 Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art  
1209 ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.“<sup>184</sup> Deshalb hat  
1210 das Bundesverfassungsgericht als Voraussetzung für einen Zugriff auf einen Bereich, in dem solche  
1211 Kernbereichsdaten (z. B. tagebuchartige Aufzeichnungen, private Film- oder Tondokumente,  
1212 höchstpersönliche Telefonate oder E-Mails) zu vermuten sind, das Erfordernis besonderer gesetzlicher  
1213 Vorkehrungen aufgestellt, um den Kernbereich der privaten Lebensgestaltung zu schützen.<sup>185</sup> So lässt  
1214 sich die (beiläufige) Erfassung solcher Daten nicht immer verhindern. Jedoch sind entsprechende  
1215 Maßnahmen abubrechen, sobald erkannt wird, dass sie in den Kernbereich vordringen, oder  
1216 zumindest im Nachhinein umgehend zu löschen.<sup>186</sup>
- 1217 Aber auch unabhängig von diesem Kernbereich hat der Gesetzgeber „organisatorische und  
1218 verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des  
1219 Persönlichkeitsrechts entgegenwirken.“<sup>187</sup> Dazu gehört auch die Sicherheit der Daten. So hat das  
1220 Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung vor allem die  
1221 „gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit“ eingefordert.<sup>188</sup>
- 1222 Im Falle des heimlichen Zugriffes auf die Datenverarbeitungsanlagen von Privatpersonen durch  
1223 Sicherheitsbehörden (so genannte Online-Durchsuchung) bestehen besonders hohe Hürden für den  
1224 Gesetzgeber, die sich vorrangig aus dem neugeschaffenen Grundrecht auf Gewährleistung der  
1225 Vertraulichkeit und Integrität informationstechnischer Systeme ableiten. Sie sind nur zulässig, wenn  
1226 Gefahren für überragend wichtige Rechtsgüter bestehen, die sich in Gestalt von tatsächlichen

---

<sup>180</sup> BVerfGE 115, 320, 358 – Rasterfahndung II.

<sup>181</sup> BVerfGE 120, 274, 328 – Onlinedurchsuchung.

<sup>182</sup> BVerfGE 113, 348, 385 – Vorbeugende Telekommunikationsüberwachung.

<sup>183</sup> BVerfG, NJW 2010, 833, 848 Rn. 279 - Vorratsdatenspeicherung.

<sup>184</sup> BVerfGE 120, 274, 335 – Onlinedurchsuchung.

<sup>185</sup> BVerfGE 120, 274, 336 ff. – Onlinedurchsuchung.

<sup>186</sup> BVerfGE 120, 274, 337 – Onlinedurchsuchung.

<sup>187</sup> BVerfGE 65, 1, 44 - Volkszählung.

<sup>188</sup> BVerfG, NJW 2010, 833, 840 Rn. 221 - Vorratsdatenspeicherung.

- 1227 Anhaltspunkten einer konkreten Gefahr manifestieren. Neben dem grundsätzlich geltenden Vorbehalt  
 1228 richterlicher Anordnung müssen u.a. auch Vorkehrungen getroffen werden, die den Kernbereich  
 1229 privater Lebensgestaltung schützen.
- 1230 2.1.6 Anonymität und Identitätsmanagement im Internet
- 1231 Schwierige rechtliche Fragen wirft das zunehmend auch und gerade wegen des Internets geforderte  
 1232 Recht auf Anonymität auf. Gerade angesichts der zunehmend ubiquitären alltäglich gewordenen  
 1233 digitalen Erfassung erscheint es als eine adäquate Antwort. Im Internet entfällt diese grundlegende  
 1234 Bedingung informationeller Freiheit häufig aus technischen Gründen. Der Gesetzgeber hat  
 1235 folgerichtig den Anbietern von Internetdiensten im Wirkungsbereich des Bundesdatenschutzgesetzes  
 1236 eine Rechtspflicht zur Anonymisierung bzw. Pseudonymisierung bei der Ausgestaltung von Verfahren  
 1237 auferlegt (§ 3a BDSG). Für den Bereich der Telemediendienste hat er die Pflicht der Ermöglichung  
 1238 der anonymen bzw. pseudonymen Nutzung von Telemedien und ihrer Bezahlung festgelegt (§ 13 Abs.  
 1239 6 TMG).
- 1240 Technische Möglichkeiten zur Anonymisierung helfen Nutzerinnen und Nutzern des Internets, ihr  
 1241 Recht auf informationelle Selbstbestimmung wirksam ausüben zu können. Sie sind daher auch  
 1242 weiterhin als ein Instrument des Selbstdatenschutzes zu fördern.
- 1243 Die Wahrung der Anonymität gehört in der analogen Welt zu einem selbstbestimmten Leben. Diese  
 1244 Möglichkeit muss auch im Internet gelten. Anders als in der analogen Welt fallen hier aber  
 1245 personenbezogene Daten systembedingt an. Die Erhebung und Verwendung muss dennoch auf ein  
 1246 Mindestmaß beschränkt werden.
- 1247 Mit dem Recht auf Anonymität geht auch die Möglichkeit eines selbstbestimmten  
 1248 Identitätsmanagement im Internet einher. Jedem Nutzer ist es selbst überlassen, wie viele und welche  
 1249 persönlichen Daten und Identitäten er in der digitalen Welt verwenden und preisgeben möchte. Dies  
 1250 schließt die Verwendung von Pseudonymen ausdrücklich ein.
- 1251 Profilbildung kann Anonymität einschränken. Sie ist daher nur zulässig, wenn sie auf einer  
 1252 gesetzlichen Grundlage beruht (z. B. BDSG oder TMG). Der Begriff und die Konsequenzen einer  
 1253 Profilbildung sind allerdings noch nicht abschließend diskutiert und gesetzlich konkretisiert.
- 1254 2.1.7 Sicherheit von Daten/Technischer Datenschutz
- 1255 Die Entscheidungen des Bundesverfassungsgerichts zur Online-Durchsuchung<sup>189</sup> sowie zur  
 1256 Vorratsdatenspeicherung<sup>190</sup> unterstreichen die gewachsene Bedeutung der Datensicherheit als einem  
 1257 wesentlichen Element des Datenschutzes.
- 1258 Datensicherheit muss die mit der zunehmenden Vernetzung und Digitalisierung gewachsene  
 1259 Zugänglichkeit personenbezogener Daten und die damit verbundenen Risiken einfangen.  
 1260 Konzeptionell konzentriert sich die Diskussion auf präventiv angelegte und flexible  
 1261 Datensicherheitskonzepte unter Formulierung abstrakter Schutzziele.
- 1262 Beim technischen Datenschutz ist auf eine technikneutrale Ausgestaltung von gesetzlichen  
 1263 Regelungen zu achten. Ein geeignetes Vorgehen kann hier die Formulierung von Schutzzielen

---

<sup>189</sup> BVerfGE 120, 274 - Onlinedurchsuchung.

<sup>190</sup> BVerfG, NJW 2010, 833 – Vorratsdatenspeicherung.

- 1264 darstellen, wie es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihren  
 1265 Eckpunkten für ein „Modernes Datenschutzrecht für das 21. Jahrhundert“<sup>191</sup> fordern.
- 1266 Mit „privacy by design“, „privacy by default“ können bereits die Hersteller von Hard- als auch  
 1267 Software verpflichtet werden, Produkte zu entwickeln, die über den gesamten Lebenszyklus hinweg  
 1268 zentralen Datenschutzprinzipien sowie den Zielen der Datensicherheit gerecht werden, nämlich:
- 1269 - Vertraulichkeit
  - 1270 - Integrität
  - 1271 - Intervenierbarkeit
  - 1272 - Verfügbarkeit
  - 1273 - Transparenz
  - 1274 - Möglichkeiten der Nichtverknüpfbarkeit.
- 1275 Beispielsweise können mit Hilfe von Verschlüsselungstechniken, die dem Stand der Technik  
 1276 entsprechen, Kommunikationen als auch sensible Datenbestände abgesichert werden. Internetseiten  
 1277 könnten derart ausgestaltet werden, dass die Möglichkeit selbstbestimmter und informierter  
 1278 Entscheidung der Nutzer in Design und Technik bereits optimal eingebettet erfolgt. Im Bereich des  
 1279 technischen Datenschutzes bestehen erhebliche Entwicklungsspielräume für den Schutz der  
 1280 Bürgerinnen und Bürger.
- 1281 Den Datenschutzgesetzen würden so bei neuen technischen Entwicklungen nicht immer neue  
 1282 spezifische Regelungen hinzugefügt, sondern es müssten lediglich konkrete Maßnahmen für die  
 1283 Einhaltung des Datenschutzes spezifiziert werden. Aus übergeordneten Schutzziele wären  
 1284 gesetzliche Neuregelungen im Bedarfsfall idealerweise ohne neue Grundsatzdiskussionen abzuleiten.
- 1285 2.1.8 Selbstschutz und Medienkompetenz
- 1286 Die Stärkung allein des Datenschutzbewusstseins ist von der Stärkung der Medienkompetenz, zu der  
 1287 auch die Datenschutzkompetenz zu zählen wäre, zu unterscheiden. Nutzer sind oft beim Umgang mit  
 1288 eigenen Daten nicht umsichtig genug. Weder erkennen sie, dass personenbezogene Daten anfallen,  
 1289 noch die Reichweite und die möglichen Folgen der Sammlung und Verarbeitung der angegebenen  
 1290 personenbezogenen Daten. Ohne diese Erkenntnis ist ein bewusster Umgang mit Daten aber nicht  
 1291 möglich.
- 1292 Daher muss den Nutzern sowohl das praktische und technische Verständnis für einen sorgfältigen  
 1293 Umgang mit den eigenen personenbezogenen Daten (z. B. auch deren Schutz vor unerwünschtem  
 1294 Zugriff oder Weitergabe) als auch die Fähigkeit, mögliche Folgen und Konsequenzen der Nutzung  
 1295 entsprechender Angebote zu erkennen, vermittelt werden. Dies hilft nicht nur, datenschutzrechtliche  
 1296 Risiken für den Einzelnen zu minimieren, sondern eröffnet zugleich auch die Chance, sein Recht auf  
 1297 informationelle Selbstbestimmung bewusst auszuüben. Neben anderen Voraussetzungen ermöglicht  
 1298 die Kenntnis der Prozesse der Datenverarbeitung einen eigenverantwortlichen Umgang mit den Daten.

---

<sup>191</sup> 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.

- 1299 Eine Stärkung des Selbst Datenschutzes kann eine Ergänzung zu, aber kein Ersatz von gesetzlichen  
 1300 Datenschutzregeln darstellen. Vor dem Hintergrund der Schwierigkeiten bei der Entwicklung  
 1301 international gültiger Datenschutzstandards gewinnt der Selbstschutz auch weiter an Bedeutung.
- 1302 Die Vermittlung eines praktischen und rechtlichen Verständnisses muss daher eine  
 1303 gesamtgesellschaftliche Aufgabe sein.
- 1304 2.1.9 Die Grenzen des nationalen Datenschutzes
- 1305 Die Regeln der Datenerhebung und -verarbeitung bei Dienstleistungen, die sich an Bürger der  
 1306 Europäischen Union wenden, bestimmen sich nach dem europäischen oder darüber hinausgehendem  
 1307 nationalen Recht. Die DSRL verbietet es grundsätzlich, personenbezogene Daten aus EU-  
 1308 Mitgliedstaaten in Staaten zu übertragen, die über kein dem EU-Recht vergleichbares  
 1309 Datenschutzniveau verfügen. Sie stellt allerdings eine Anzahl von Instrumenten zur Verfügung, die  
 1310 ein angemessenes Datenschutzniveau bei der Datenübermittlung in Drittstaaten sicherstellen sollen.  
 1311 Gegenwärtig erfolgt eine grundlegende Revision der DSRL, die auf Verbesserungen des  
 1312 Datenschutzes auch in diesem Bereich abzielt.
- 1313 Die seit 2000 existierende „Safe Harbor“-Vereinbarung soll ein angemessenes Datenschutzniveau bei  
 1314 US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der „Safe  
 1315 Harbor“-Vereinbarung vorgegebenen Grundsätze verpflichten. In einem Beschluss vom April 2010  
 1316 hat der Düsseldorfer Kreis die Anforderungen an die Nachweise und auch an deutsche Unternehmen,  
 1317 die an Nicht-EU-Unternehmen Daten übermitteln, verstärkt.<sup>192</sup>
- 1318 Dem Grunde nach existieren Vorschriften, die europäische Bürger und Verbraucher schützen. Durch  
 1319 die offenbar mangelnde Durchsetzung der Sondervereinbarung mit den USA wurden diese Rechte  
 1320 allerdings geschwächt. Derzeit befindet sich die EU-Kommission (DG Justice) in Verhandlungen mit  
 1321 den USA über ein so genanntes Allgemeines Datenschutzabkommen, das neben „Safe Harbor“ treten  
 1322 soll und insbesondere nach dem Inkrafttreten des Vertrags von Lissabon und der damit den EU-  
 1323 Institutionen zugewachsenen Mitzuständigkeit für Fragen der justiziellen und polizeilichen  
 1324 Zusammenarbeit von besonderer Bedeutung ist.
- 1325 Ziel dieser Verhandlungen muss die Anwendbarkeit und Durchsetzbarkeit des europäischen  
 1326 Datenschutzrechts sein. Dabei wird u. a. ein Geschäftssitz in Europa als Bedingung für die Erhebung  
 1327 und Verarbeitung von Daten diskutiert.
- 1328 Gegenwärtig gilt nach dem BDSG das Sitzlandprinzip.<sup>193</sup> Danach kommt dasjenige Recht zur  
 1329 Anwendung, das am Sitz des für die Entscheidung über die Datenverarbeitung Verantwortlichen gilt.  
 1330 Damit wird ein harmonisierter EWR-Rechtsraum begründet. Eine Ausnahme bilden Verarbeitungen,  
 1331 bei denen noch eine Niederlassung im Inland besteht, sodass nationales Datenschutzrecht zur  
 1332 Anwendung kommt. Eine weitere Ausnahme vom Sitzlandprinzip bilden Verarbeitungen, bei denen  
 1333 Verantwortliche außerhalb des EWR-Raumes befindlich sind. So gilt beispielsweise mit Blick auf US-

---

<sup>192</sup> „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](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.

<sup>193</sup> § 1 Abs. 5 BDSG.



1334 amerikanische Unternehmen das Territorialitätsprinzip und damit grundsätzlich bundesdeutsches  
1335 Recht, sodass es auf den Ort der Datenverarbeitung bzw. auf die Frage ankommt, ob sich  
1336 automatisierte Mittel zur Datenerhebung räumlich gesehen in Deutschland befinden. Genau diese  
1337 Verräumlichung als Anknüpfungspunkt birgt mit Blick auf reine Webinhaltsangebote Probleme. So  
1338 wird die Anwendbarkeit bundesdeutschen Rechts auf bestimmte Facebook-Bestandteile etwa dann  
1339 bejaht, wenn es sich um eine Datenverarbeitung handelt, bei der ein so genanntes cookie auf dem  
1340 Programm der Internetnutzer platziert wird, weil dessen privater Rechner im Inland belegen ist. Für  
1341 andere Angebote ohne Verwendung dieser Technologie hingegen wird – zumindest von Teilen der  
1342 Aufsichtsbehörden – von einer fehlenden Anwendbarkeit mangels Inlandsbezuges der  
1343 Datenverarbeitung ausgegangen. Die „Verhandlungen“ des Hamburgischen Datenschutzbeauftragten  
1344 mit Google und Facebook sind nur vor diesem Hintergrund nachvollziehbar. Handelte es sich um  
1345 einen unproblematischen Fall, wären verwaltungsrechtliche Anordnungen ergangen.

1346 Auf europäischer und weltweiter Ebene muss die Bundesrepublik Deutschland ihrer Verantwortung  
1347 als führender Wirtschaftsnation gerecht werden und für einen ausgeprägten Datenschutz streiten. Die  
1348 Praxis global agierender Internetunternehmen erfordert ein abgestimmtes Vorgehen über die Grenzen  
1349 des Nationalstaates hinaus. Bei internationalen Ausformulierungen von Datenschutzvorgaben sollte  
1350 jeweils das höchste beteiligte Datenschutzniveau Grundlage sein.

1351

1352 *Der nachfolgende Text wurde in der Projektgruppe von allen Fraktionen getragen; die Fraktion*  
 1353 *DIE LINKE hat den Text jedoch streitig gestellt und einen alternativen Vorschlag vorgelegt, s. u.*  
 1354 *ab Zeile 1435.*

1355 2.1.10 Datenschutz für Kinder und Jugendliche

1356  
 1357 Der Datenschutz bei besonders schutzwürdigen Gruppen bedarf besonderer Aufmerksamkeit. Die  
 1358 neuen informationstechnischen Möglichkeiten dürfen nicht zulasten der schwächsten Mitglieder  
 1359 unserer Gesellschaft (etwa von Kindern) gehen. Gleichzeitig sollen diese aber auch nicht von einer  
 1360 angemessenen Teilhabe an der Informationsgesellschaft ausgeschlossen sein.

1361 Daten von Kindern werden in einem kaum geringeren Umfang als Daten von Erwachsenen erhoben  
 1362 und verarbeitet. Die Mehrzahl der Unternehmen unterscheidet hinsichtlich ihrer Internetangebote und  
 1363 der damit verknüpften Datenverarbeitungen nicht zwischen Erwachsenen und Kindern  
 1364 beziehungsweise Jugendlichen. Auch Kinder und Jugendliche sind aktive Nutzer von  
 1365 Informationsdiensten und setzen diese zum Informationsaustausch ein. Selbstverständlich sind dabei  
 1366 Kinder von Geburt an ebenso wie Erwachsene Träger von Grundrechten. Dazu gehört auch das Recht  
 1367 auf informationelle Selbstbestimmung, sodass auch Kinder und Jugendliche Datenschutzrechte und  
 1368 damit grundsätzlich das Recht haben, über die Herausgabe und Verwendung ihrer personenbezogenen  
 1369 Daten selbst zu bestimmen. Sie wachsen bereits mit der Nutzung digitaler Technik und der  
 1370 Angebotsvielfalt des Internets auf und sind damit die am besten vernetzte Altersgruppe: 98 Prozent  
 1371 der Zehn- bis 18-Jährigen nutzen mittlerweile das Internet. Dies hat eine Studie (*Jugend 2.0*) im  
 1372 Auftrag des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V.  
 1373 (BITKOM)<sup>194</sup> ergeben. Danach sind selbst Kinder im Alter von zehn bis zwölf Jahren zu 96 Prozent  
 1374 online. Hierbei überwiegen nach Angaben der Studie zwar die positiven Online-Erfahrungen, jedoch  
 1375 hat jeder dritte Jugendliche (34 Prozent) auch Negatives erlebt.

1376 Die Studie zeigt auch, dass das Internet für Jugendliche zwar eine herausragende Bedeutung hat,  
 1377 jedoch Freundschaften und Schule nicht verdrängt. Freunde, Familie und gute Noten sind wichtiger  
 1378 als das Netz. 98 Prozent der Jugendlichen sind ihre Freunde wichtig, 86 Prozent sagen dies vom  
 1379 Internetzugang. Die große Mehrheit der Zehn- bis 18-Jährigen verbringt mehr Zeit mit Freunden oder  
 1380 Hausaufgaben als im Internet. Die meisten Jugendlichen (76 Prozent) wissen bereits jetzt, das Internet  
 1381 sinnvoll zur Suche nach Informationen für Schule und Ausbildung einzusetzen. 64 Prozent haben nach  
 1382 eigenen Angaben so ihr Wissen verbessert, 38 Prozent ihre Leistungen in Schule oder Ausbildung.

1383 Fast schon selbstverständlich ist für Teenager die Mitgliedschaft in Internetgemeinschaften. Nach der  
 1384 Studie sind 77 Prozent in „Communitys“ angemeldet, 74 Prozent nutzen sie aktiv. Es gibt aber auch  
 1385 Unterschiede nach Altersgruppen: So sind 93 Prozent der 16- bis 18-Jährigen in den Netzwerken  
 1386 aktiv, aber nur 42 Prozent der Zehn- bis Zwölfjährigen.<sup>195</sup> SchülerVZ liegt insgesamt vor Facebook.

<sup>194</sup> BITKOM: Jugend 2.0, Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen. 2011, online abrufbar unter: [http://www.bitkom.org/files/documents/BITKOM\\_Studie\\_Jugend\\_2.0.pdf](http://www.bitkom.org/files/documents/BITKOM_Studie_Jugend_2.0.pdf) (zuletzt aufgerufen am 21. März 2011).

<sup>195</sup> Mädchen kommunizieren intensiver als Jungen. Das gilt nicht nur für Internet-Communitys, die von 82 Prozent der Mädchen aktiv genutzt werden, gegenüber 64 Prozent bei Jungen (BITKOM: Jugend 2.0, Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen. 2011, S. 26, online abrufbar unter: [http://www.bitkom.org/files/documents/BITKOM\\_Studie\\_Jugend\\_2.0.pdf](http://www.bitkom.org/files/documents/BITKOM_Studie_Jugend_2.0.pdf) (zuletzt aufgerufen am 21. März 2011).

- 1387 Teenager haben in ihrer jeweils meistgenutzten Community im Durchschnitt 133 Kontakte, davon 34  
 1388 „gute Freunde“. Die BITKOM-Untersuchung zeigt, dass sich 58 Prozent der Zehn- bis 18-Jährigen  
 1389 mehr Datenschutz wünschen.
- 1390 Da bereits mehr als drei Viertel aller deutschen Kinder und Jugendlichen in sozialen Netzwerken  
 1391 organisiert sind und regelmäßig über diese Plattformen kommunizieren, entsteht teilweise bereits von  
 1392 jungen Teenagern ein genaues Persönlichkeitsprofil und ein digitales Abbild ihrer Wünsche,  
 1393 Vorlieben, Beziehungsgeflechte. Ihre Bedürfnisse werden ausgewertet.
- 1394 Mit der gesellschaftlichen Debatte um die digitale Privatsphäre und Datenschutz in den letzten Jahren  
 1395 hat auch ein Erkenntnisprozess bei Kindern und Jugendlichen eingesetzt. Zunehmend werden schon  
 1396 Schulkindern die Probleme bewusst, die mit der Veröffentlichung von persönlichen Daten im Internet  
 1397 verbunden sein können. Sie überlegen sich bereits, was sie ins Netz stellen, ob sie ihren richtigen  
 1398 Namen verwenden etc. Auch Eltern erkennen die Gefahren des Internets für ihre Kinder in  
 1399 steigendem Maße.
- 1400 Die Studie *Jugend 2.0* untersucht spezielle Bedürfnisse von Kindern und Jugendlichen. Sie zeigt  
 1401 zudem, dass die Erfahrungen und das Wissen im Umgang mit Datenschutz und Persönlichkeitsrechten  
 1402 bereits mehrheitlich vorhanden sind, jedoch teilweise noch nicht in ausreichendem Maße. Bei  
 1403 Angeboten für Kinder und Jugendliche ist daher besonders auf eine altersgerechte Information und  
 1404 Aufklärung über die Datenerhebung, -verarbeitung sowie deren mögliche Konsequenzen zu achten.  
 1405 Nur so können Kinder und Jugendliche ihre Einwilligung in die Erhebung und Verarbeitung von  
 1406 personenbezogenen Daten überhaupt vornehmen. Dies ist unter anderem deshalb von besonderer  
 1407 Bedeutung, weil auch die Daten von Kindern und Jugendlichen bereits zu Profilen für gezielte  
 1408 Werbemaßnahmen zusammengefasst werden können. Kindern fällt es aber oftmals noch schwerer als  
 1409 Erwachsenen<sup>196</sup> zu erkennen, ob es sich um allgemeine oder aber speziell auf sie zugeschnittene  
 1410 Angebote handelt. Daher stellt sich letztlich auch die Frage, ob Kinder und Jugendliche, die nicht wie  
 1411 Erwachsene langfristige Folgen ihres Handelns abschätzen können, in stärkerem Maße einer  
 1412 öffentlichen Fürsorge und eines gesetzlichen Schutzes bedürfen.
- 1413 Unterschiedliche Alterskategorien in verschiedenen Gesetzen erschweren eine Zuordnung. Bislang  
 1414 gilt, dass die gesetzlichen Vertreter des Kindes ihre Einwilligung in jede Verarbeitung der Daten des  
 1415 Kindes geben, bis das Kind selbst in der Lage ist, einzuwilligen. Die Einwilligungsfähigkeit des  
 1416 Kindes knüpft dabei an seine Einsichtsfähigkeit an, mit deren Zunahme sie graduell je nach der  
 1417 individuellen Entwicklung von den Eltern auf das Kind übergeht. Eine gesetzliche Vorgabe gibt es  
 1418 hierfür nicht.
- 1419 Für Anbieter von Diensten ist das Alter des Nutzers oftmals nicht klar erkennbar. Dies gilt  
 1420 insbesondere bei der – aus Datenschutzgründen wünschenswerten – anonymen Nutzung von Diensten.  
 1421 Auch wechselnde Nutzer an einem Endgerät, wie es in Familien die Regel ist, erschweren eine klare  
 1422 Zuordnung zu bestimmten Altersklassen.
- 1423 Deutliche Differenzierungen in den Schutzkonzepten erscheinen (wie zum Beispiel im Angebot beim

---

<sup>196</sup> Vgl. hierzu Kapitel 2.3.1.2.

1424 sozialen Netzwerk SchülerVZ) wünschenswert, um einen verbesserten Schutz zu erreichen, wenn  
 1425 Angebote sich vollständig oder überwiegend an Jugendliche und Kinder wenden. Gegebenenfalls sind  
 1426 hier auch – entsprechend den jeweiligen Gefahren – gesetzgeberische Maßnahmen erforderlich.  
 1427 Unklarheiten der Auslegung des BDSG hinsichtlich der Einwilligungsfähigkeit von Jugendlichen und  
 1428 der damit verbundenen Anforderungen an eine wirksame Einwilligung sollten beseitigt werden. Auch  
 1429 eine Begrenzung der zu erhebenden Daten beziehungsweise eine nur eingeschränkte kommerzielle  
 1430 Verwertung käme diesbezüglich in Betracht.

1431 Einer Altersverifikation, die zu einer eindeutigen Identifizierung des Nutzers führt, würde jedoch das  
 1432 Datenschutzrecht entgegenstehen. Denn dies hätte einen viel gravierenderen Eingriff zur Folge als  
 1433 das bisherige Fehlen datenschutzrechtlich hinreichend bedarfsgerecht zugeschnittener Angebote.

1434

1435 **Alternativer (streitiger) Textvorschlag der Sachverständigen Constanze Kurz und der Fraktion DIE**  
 1436 **LINKE.**

1437 2.1.10 Datenschutz für Kinder und Jugendliche

1438 Der Datenschutz bei besonders schutzwürdigen Gruppen bedarf besonderer Aufmerksamkeit. Die  
 1439 Ausnutzung der neuen informationstechnischen Möglichkeiten darf nicht zulasten der schwächsten  
 1440 Mitglieder unserer Gesellschaft (etwa von Kindern und Jugendlichen) gehen. Gleichzeitig sollen diese  
 1441 aber auch nicht von einer angemessenen Teilhabe an der Informationsgesellschaft ausgeschlossen  
 1442 sein.

1443 Daten von Kindern werden in einem kaum geringeren Umfang als Daten von Erwachsenen erhoben,  
 1444 verarbeitet und weitergegeben. Eine Vielzahl der Unternehmen unterscheidet hinsichtlich ihrer  
 1445 Internetangebote und der damit verknüpften Datenverarbeitungen nicht oder kaum zwischen  
 1446 Erwachsenen und Kindern beziehungsweise Jugendlichen. Auch Kinder und Jugendliche sind heute  
 1447 selbstverständlich aktive Nutzer von Informationsdiensten und setzen diese zum  
 1448 Informationsaustausch ein. Doch ebenso selbstverständlich sind dabei Kinder von Geburt an wie  
 1449 Erwachsene Träger von Grundrechten. Dazu gehört auch das Grundrecht auf informationelle  
 1450 Selbstbestimmung, sodass auch Kinder und Jugendliche alle Datenschutzrechte und damit  
 1451 grundsätzlich das Recht haben, über die Herausgabe und Verwendung ihrer personenbezogenen Daten  
 1452 selbst zu bestimmen. Sie wachsen bereits mit der Nutzung digitaler Technik und der Angebotsvielfalt  
 1453 des Internets auf und sind damit die am besten vernetzte Altersgruppe: 98 Prozent der Zehn- bis 18-  
 1454 Jährigen nutzen mittlerweile das Internet. Dies hat eine Studie (*Jugend 2.0*) im Auftrag des Verbandes  
 1455 BITKOM ergeben. Danach sind selbst Kinder im Alter von zehn bis zwölf Jahren zu 96 Prozent  
 1456 online.

1457 Fast schon selbstverständlich ist für Teenager die Mitgliedschaft in Internetgemeinschaften. Nach der  
 1458 Studie sind 77 Prozent in verschiedenen „Communities“ angemeldet, 74 Prozent nutzen sie aktiv. Es  
 1459 gibt aber auch Unterschiede zwischen verschiedenen Altersgruppen: So sind 93 Prozent der 16- bis  
 1460 18-Jährigen in den Netzwerken aktiv, aber nur 42 Prozent der Zehn- bis Zwölfjährigen. SchülerVZ  
 1461 liegt derzeit insgesamt vor Facebook, die Nutzung der Angebote unterliegt jedoch einem schnellen  
 1462 Wandel. Teenager haben in ihrer jeweils meistgenutzten Community im Durchschnitt 133 Kontakte,  
 1463 davon 34 werden als „gute Freunde“ gesehen.

1464 Da bereits mehr als drei Viertel aller deutschen Kinder und Jugendlichen in sozialen Netzwerken  
1465 organisiert sind und regelmäßig über diese Plattformen kommunizieren, entsteht teilweise bereits von  
1466 jungen Teenagern ein genaues Persönlichkeitsprofil und ein digitales Abbild ihrer Wünsche,  
1467 Vorlieben, Beziehungsgeflechte, Gewohnheiten. Bekanntlich beruht das Geschäftsmodell der sozialen  
1468 Netzwerke im Wesentlichen darauf, Daten ihrer Nutzer zu erheben und kommerziell zu verwerten.  
1469 Schon im Hinblick auf Erwachsene erscheint diese Nutzbarmachung von Teilen der Privatsphäre für  
1470 wirtschaftliche Zwecke bedenklich, erst recht jedoch bei Kindern und Jugendlichen. Letztere verfügen  
1471 häufig noch nicht über das nötige Reflektionsvermögen, um die Nutzung des Angebots mit dem  
1472 Geschäftsmodell in Verbindung zu bringen. Einfacher gesagt: Sie sind sich oft gar nicht darüber im  
1473 Klaren, dass sie statt mit Geld mit ihren persönlichen Daten für diese Angebote bezahlen. Erst recht  
1474 überblicken sie oft noch nicht die langfristigen Folgen ihres Handelns, können also etwa die Gefahr  
1475 einer vom Nutzer nicht kontrollierbaren Profilbildung oder erstellten Prognosen durch die Anbieter  
1476 noch nicht zutreffend einschätzen und bewerten. Darüber kann auch ein diffuses Unwohlsein und die  
1477 wachsende Sensibilisierung der Betroffenen im Hinblick auf den Datenschutz nicht hinwegtäuschen.  
1478 So heißt es etwa in der erwähnten BITKOM-Untersuchung, 58 Prozent aller Zehn- bis 18-Jährigen  
1479 wünschten sich mehr Datenschutz. Es wäre jedoch gewagt, hieraus zu folgern, die Betroffenen wären  
1480 sich der umfassenden Nutzung ihrer Daten zu kommerziellen Zwecken der Anbieter stets bewusst  
1481 oder gar in der Lage, sich auf der Grundlage solcher Kenntnis aktiv gegen die Nutzung ihrer Daten zu  
1482 entscheiden.

1483 Was bei den Geschäftsmodellen der sozialen Netzwerke problematisch ist, ist bei Angeboten, die  
1484 speziell auf Kinder und Jugendliche zugeschnitten sind, besonders bedenklich. Dies gilt nicht nur für  
1485 die Auswertung des Nutzungs- und Surfverhaltens, sondern auch für die Werbepraktiken bei solchen  
1486 Angeboten. So können die Betroffenen häufig Werbung und redaktionelle Inhalte weniger klar  
1487 auseinanderhalten, als dies Erwachsenen möglich ist. Sie sind für personalisierte Werbung mithin  
1488 empfänglicher und somit manipulierbarer als andere Nutzerinnen und Nutzer, die über mehr  
1489 Medienerfahrung verfügen. Insbesondere bemerken Kinder oft nicht, wenn sie von redaktionell  
1490 betreuten Seiten auf rein kommerzielle Werbeangebote umgeleitet werden, weil die Trennung  
1491 redaktioneller Inhalte von Werbeinhalten häufig nicht klar erkennbar ist oder bewusst verschleiert  
1492 wird. Ein Datenschutzproblem ergibt sich daraus beispielsweise schon dann, wenn in diesem  
1493 Zusammenhang von Werbetreibenden Cookies gesetzt werden, die eine weitere Auswertung des  
1494 Surfverhaltens der Nutzer auch jenseits des ursprünglichen Angebots ermöglichen.

1495 Ein weiteres, eng damit verbundenes Problem ist die zunehmende Verschuldung schon von  
1496 Minderjährigen. Beruhend auf der Analyse ihrer hinterlassenen Daten werden Jugendliche oft mit auf  
1497 sie zugeschnittenen, manipulativen Werbebotschaften zu übermäßigem, ihren finanziellen  
1498 Verhältnissen nicht angemessenen Konsum angeregt.

1499 Als Konsequenz aus den obigen Befunden stellt sich letztlich die Frage, ob Kinder und Jugendliche,  
1500 die nicht wie Erwachsene langfristige Folgen ihres Handelns abschätzen können, in stärkerem Maße  
1501 einer öffentlichen Fürsorge und eines gesetzlichen Schutzes bedürfen oder ob die altersbedingte  
1502 Unerfahrenheit durch verstärkte Maßnahmen zur Förderung von Medienkompetenz ausgeglichen  
1503 werden kann.

1504 Hierüber gehen die Meinungen in der Projektgruppe auseinander. Bislang gilt, dass die  
1505 gesetzlichen Vertreter des Kindes ihre Einwilligung in jede Verarbeitung der Daten des Kindes geben,  
1506 bis das Kind selbst in der Lage ist, einzuwilligen. Die Einwilligungsfähigkeit des Kindes knüpft dabei  
1507 an seine Einsichtsfähigkeit an. Mit Zunahme der Einsichtsfähigkeit und Risikoeinschätzung geht sie  
1508 graduell je nach der individuellen Entwicklung von den Eltern auf das Kind über. Eine gesetzliche  
1509 Vorgabe gibt es hierfür nicht.

1510 Eine Mehrheit der Projektgruppe ist jedoch der Ansicht, dass die Erfahrungen und das Wissen im  
1511 Umgang mit Datenschutz und Persönlichkeitsrechten bei Kindern und Jugendlichen bereits  
1512 überwiegend vorhanden sind, jedoch teilweise noch nicht in ausreichendem Maße. Bei Angeboten für  
1513 Kinder und Jugendliche sei daher besonders auf eine altersgerechte Information und Aufklärung über  
1514 die Datenerhebung, -verarbeitung sowie deren mögliche Konsequenzen zu achten. Nur so könnten  
1515 Kinder und Jugendliche ihre Einwilligung in die Erhebung und Verarbeitung von personenbezogenen  
1516 Daten überhaupt erteilen.

1517 Eine Minderheit ist hingegen der Ansicht, dass Kinder und Jugendliche durchaus eines besonderen  
1518 gesetzlichen Schutzes bedürfen. Gegebenenfalls müsse in diesem Zusammenhang auch die  
1519 Einschränkung von Geschäftsmodellen der Anbieter ermöglicht werden, die nach dem derzeitigen  
1520 Datenschutzrecht noch legal sind.

1521

1522

1523 **2.2 Datenschutz im öffentlichen Bereich**

## 1524 2.2.1 Datenschutz in öffentlichen Einrichtungen

1525 2.2.1.1. *Einführung*

1526 Das deutsche Datenschutzrecht beruht seit seinen Anfängen auf einer Unterscheidung zwischen  
 1527 Datenschutz im Bereich öffentlicher Einrichtungen und nicht öffentlicher Stellen, insbesondere in der  
 1528 Privatwirtschaft. Diese Differenzierung, die sich auch in der Struktur des BDSG niedergeschlagen hat,  
 1529 findet ihren Ausgangspunkt in der Konzeption des Rechts auf informationelle Selbstbestimmung als  
 1530 einem individuellen Abwehrrecht gegenüber staatlichen Eingriffen. In diesem Zusammenhang wird  
 1531 darauf hingewiesen, dass die grundrechtlichen Grenzen für staatliche Datenverarbeitung enger sind als  
 1532 im nichtöffentlichen Bereich. Die öffentliche Gewalt wird durch die Grundrechte verpflichtet und  
 1533 kann sich nicht auf eigene entgegenstehende Grundrechte berufen. Zwischen staatlichen und  
 1534 nichtstaatlichen Gefährdungen der informationellen Selbstbestimmung besteht daher weiterhin ein  
 1535 Unterschied.<sup>197</sup> Die DSRL kennt diese Zweiteilung jedoch nicht. Das deutsche Recht sieht derzeit  
 1536 zumindest teilweise eine Gleichstellung öffentlicher und privater Datenverarbeitung vor, etwa für  
 1537 Telemedien.<sup>198</sup>

1538 Da das Grundgesetz keine zentrale Kompetenznorm für die Gesetzgebung im Bereich des  
 1539 Datenschutzes enthält, ergibt sich die Zuständigkeit für die Gesetzgebung als Teil der  
 1540 Regelungskompetenz für das jeweilige Verwaltungsverfahren aus den Sachkompetenzen der Art. 73  
 1541 und 74 GG.<sup>199</sup> Bundesgesetze können daher den Datenschutz nur für Bereiche der Gesetzgebung des  
 1542 Bundes regeln. Entsprechendes gilt für Landesgesetze.

1543 Neben der Unterscheidung datenschutzrechtlicher Bestimmungen für den privaten und öffentlichen  
 1544 Bereich ergibt sich also noch eine weitere Differenzierung zwischen bundes- und landesrechtlichen  
 1545 Normen. Dieses Nebeneinander bundes- und landesrechtlicher Vorschriften kennzeichnet besonders  
 1546 den öffentlichen Bereich, da im privaten Bereich im Rahmen der konkurrierenden  
 1547 Gesetzgebungskompetenz nach Art. 74 Nr. 11 GG („Recht der Wirtschaft“) viele Bereiche –  
 1548 einschließlich der jeweiligen datenschutzrechtlichen Aspekte – durch Bundesgesetze geregelt sind, so  
 1549 dass für den privaten Bereich wenig Regelungsmöglichkeiten für die Länder verbleiben.<sup>200</sup>

1550 Darüber hinaus sind in vielen Fallkonstellationen Fragen der Spezialität und Subsidiarität von Normen  
 1551 zu beantworten. So haben etwa nach § 1 Abs. 3 BDSG andere datenschutzrechtliche Vorschriften des  
 1552 Bundes Vorrang vor dem BDSG. Vollziehen Landesbehörden Bundesrecht, gelten auf Grund einer  
 1553 weiteren Subsidiaritätsregelung (§ 1 Abs. 2 Nr. 2 BDSG) statt des BDSG die  
 1554 Landesdatenschutzgesetze, dies jedoch nur, soweit das zu vollziehende Bundesrecht (z. B. SGB,  
 1555 StVG) keine datenschutzrechtlichen Bestimmungen enthält.<sup>201</sup> Ganz überwiegend gilt auch für die

---

<sup>197</sup> Vgl. auch Di Fabio, Udo, in : Maunz/Dürig, Grundgesetz - Kommentar. 58. Ergänzungslieferung 2010, Art. 2, Rn. 190.

<sup>198</sup> Vgl. § 1 Abs. 1 Satz 2 TMG.

<sup>199</sup> Kühling, Jürgen / Seidel, Christian / Siviridis, Anastasios: Datenschutzrecht. 2008, S. 74.

<sup>200</sup> Kilian, Wolfgang/Weichert, Thilo, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch 28. Ergänzungslieferung 2010, 1. Abschnitt, Teil 13, Punkt I., Rn. 3.

<sup>201</sup> Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht. Stand April 2010, Ziff. 3.3.2.2.

1556 Landesdatenschutzgesetze der Grundsatz der Subsidiarität gegenüber anderen datenschutzrechtlichen  
1557 Regelungen.<sup>202</sup>

1558 Vielfach wird daher ein unübersehbares „Dickicht des bereichsspezifischen Datenschutzes“<sup>203</sup> beklagt.  
1559 Im Ergebnis hat dies dazu geführt, dass im Bereich öffentlicher Einrichtungen das BDSG nicht das  
1560 zentrale Regelungsinstrument darstellt.<sup>204</sup>

1561 Die deutliche Unterscheidung zwischen Datenschutz im öffentlichen und privaten Bereich gilt auch  
1562 für die Organisation der Aufsicht und Kontrollorgane. Während Bundes- und  
1563 Landesdatenschutzbeauftragte die jeweilige Kontrolle über Bundes- und Landesverwaltung ausüben,  
1564 wird die Kontrolle im privaten Bereich ausschließlich auf Länderebene, teilweise durch die  
1565 Landesdatenschutzbeauftragten, teilweise durch gesonderte Aufsichtsbehörden, ausgeübt. Gesonderte  
1566 Kontrolleinrichtungen gibt es etwa im Bereich der Kirchen und öffentlich-rechtlicher  
1567 Rundfunkanstalten.

1568 Der Datenschutzaufsicht kommt für die Verwirklichung eines effizienten Datenschutzes eine  
1569 herausragende Rolle zu. Stärkung der Aufsichtsbehörden bedeutet somit zugleich eine Verbesserung  
1570 des Datenschutzes. Vor dem Hintergrund der jüngsten Rechtsprechung des EuGH<sup>205</sup> ist es zwingend  
1571 notwendig, die völlige Unabhängigkeit der Datenschutzaufsicht zu gewährleisten. Durch die  
1572 Entscheidung des EuGH könnte auch ein gesetzgeberisches Handeln auf Bundesebene erforderlich  
1573 sein. Ein entsprechender Auftrag zur Prüfung ist bereits durch die fraktionsübergreifende  
1574 EntschlieÙung vom 16.12.2010 erteilt worden.<sup>206</sup> Die DSRL gibt vor, dass die Datenschutzaufsicht  
1575 rechtlich, organisatorisch und finanziell unabhängig sein muss. Hierbei unterscheidet die Richtlinie  
1576 nicht zwischen öffentlichem und privatem Bereich.

#### 1577 2.2.1.2. *Das Bundesdatenschutzgesetz (BDSG)*

1578 Das BDSG<sup>207</sup> ist ein Schutzgesetz, das natürliche Personen schützen soll. Verstöße dagegen können  
1579 Schadenersatzansprüche begründen. Allerdings begrenzt das BDSG die Möglichkeit einer  
1580 verschuldensunabhängigen Haftung für Datenschutzverstöße auf die öffentlichen Einrichtungen (§§ 7,  
1581 8 BDSG).

1582

1583 Das Datenschutzgesetz ist daneben ein Eingriffsgesetz, mit dem Eingriffe in das Grundrecht auf  
1584 informationelle Selbstbestimmung gerechtfertigt werden. Die konkreten Eingriffsnormen bzw.  
1585 Eingriffe müssen durch ein überwiegendes Allgemeininteresse gerechtfertigt sein. Sie müssen zudem  
1586 den Grundsätzen der Verhältnismäßigkeit und der Normenklarheit genügen und Schutzvorkehrungen  
1587 zum Zwecke der Datensicherheit und der Sicherheit der Betroffenenrechte vorsehen.

---

<sup>202</sup> Gola, Peter / Schomerus, Rudolf: BDSG, Kommentar. 2010, § 1, Rn. 33.

<sup>203</sup> Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht. Stand April 2010, Ziff. 4.1.2.

<sup>204</sup> Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht. Stand April 2010, Ziff. 3.2.7.

<sup>205</sup> EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland. Vgl. hierzu auch unter 1.2.3.

<sup>206</sup> BT-Drs. 17/4179, S. 5.

<sup>207</sup> Vgl. auch Kapitel 1.3.2.



1588 Nach dem BDSG gilt – wie im gesamten Datenschutzrecht - wegen des mit der Datenverarbeitung  
 1589 verbundenen Grundrechtseingriffs und dem Gesetzesvorbehalt das Verbot mit Erlaubnisvorbehalt (§ 4  
 1590 Abs. 1 BDSG). Das heißt, Datenverarbeitung ist nur dann zulässig, wenn entweder eine  
 1591 Rechtsvorschrift dies ausdrücklich vorsieht oder der Betroffene ausdrücklich eingewilligt hat.

1592 Hierbei sind im Sinne der Rechtsprechung des BVerfG besonders hervorzuheben:

- 1593 • die Zweckbindung für die Verwendung personenbezogener Daten,
- 1594 • eine strikte Beschränkung der Datenverarbeitung und -nutzung auf das Erforderliche,
- 1595 • die größtmögliche Selbstbestimmung der Betroffenen sowie
- 1596 • die Transparenz der Datenverarbeitung.

1597 Nur bei Beachtung dieser Anforderungen ist der notwendige Schutzzweck für ein modernes  
 1598 Datenschutzrecht gewährleistet.

1599 Über das BDSG hinaus finden sich weitere Datenschutzregelungen mit Relevanz für den staatlichen  
 1600 Bereich in dem Bundespersonalvertretungsgesetz (BPersVG) sowie den jeweiligen  
 1601 Landespersonalvertretungsgesetzen, dem Betriebsverfassungsgesetz (BetrVG), den jeweiligen  
 1602 Landesvorschriften zum Datenschutz, den sozialrechtlichen Vorschriften (SGB), dem  
 1603 Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) sowie diversen EU- und UN-  
 1604 Richtlinien betreffend personenbezogene Daten.

1605 Durch die engen Vorgaben zu Eingriffen in das Recht auf informationelle Selbstbestimmung wird  
 1606 dem Staat in Fragen des Datenschutzes eine Vorbildfunktion für nichtstaatliche Akteure  
 1607 zugeschrieben.

1608 Auch wenn es im staatlichen Bereich einige Spezifika bezüglich des Beschäftigtendatenschutzes gibt,  
 1609 wird an dieser Stelle nicht darauf eingegangen. Vielmehr wird das Thema Beschäftigtendatenschutz  
 1610 übergreifend, sowohl für den privaten als auch den öffentlichen Sektor, Gegenstand des Kapitels 2.3.  
 1611 sein.

1612

### 1613 2.2.1.3. *Staatliche Datenverarbeitung im Wandel*

1614 Die Anfänge der Datenschutzbewegung in Europa wie auch in den USA wandten sich gegen als  
 1615 übermächtig und bedrohlich empfundene Datenerhebungsprojekte staatlicher Stellen.

1616 Hinter diesen Projekten stand die zunehmende Computerisierung der Verwaltung, die neue  
 1617 Möglichkeiten einer Zusammenführung und Auswertung von personenbezogenen Daten erst  
 1618 ermöglichte. Die geplante Volkszählung zu Beginn der 80er-Jahre und das daraufhin 1983 ergangene  
 1619 Volkszählungsurteil des BVerfG<sup>208</sup> etablierten dann endgültig die bis dahin noch streitigen rechtlichen  
 1620 Grundprinzipien des Datenschutzes.

1621 Nachfolgend haben Gesetzgeber und Verwaltung in der Verfolgung ihrer Aufgaben weiterhin  
 1622 Instrumente und Verfahren vorangetrieben, die zumindest mit Blick auf den Datenschutz erhebliche  
 1623 Probleme aufgewiesen haben. Dies gilt in zunehmendem Maße auch für Vorhaben auf europäischer

---

<sup>208</sup> BVerfGE 65,1 - Volkszählung.

1624 Ebene. Die Vielzahl an Entscheidungen des BVerfG zu Bundes- und Landesgesetzen (z. B. G 10-  
 1625 Entscheidung<sup>209</sup>, Großer Lauschangriff<sup>210</sup>, Online-Durchsuchung<sup>211</sup>, Rasterfahndung<sup>212</sup>, KFZ-  
 1626 Kennzeichenerfassung<sup>213</sup>, Vorratsdatenspeicherung<sup>214</sup>) markiert dabei einen aktuellen Stand des  
 1627 Datenschutzes im öffentlichen Bereich, der auf den Widerstreit zwischen den von staatlichen Stellen  
 1628 in Anschlag gebrachten öffentlichen Interessen einerseits sowie dem insbesondere vom BVerfG  
 1629 betonten verfassungsrechtlichen Persönlichkeitsrecht andererseits hinweist.

1630 Die Auseinandersetzung beschränkt sich dabei nicht auf den Sicherheitsbereich, sondern findet ihre  
 1631 Fortsetzung auch in anderen Bereichen der öffentlichen Verwaltung, so etwa in den aktuellen  
 1632 Auseinandersetzungen um Grenzen zulässiger Datenerhebung bei Hartz-IV-Empfängern oder die  
 1633 Ausweitung staatlicher Kontodatenzugriffe.

#### 1634 2.2.1.4. Herausforderungen für das Datenschutzrecht in öffentlichen Einrichtungen

1635 Die Informationsverarbeitung öffentlicher Stellen stellt besondere Herausforderungen an den  
 1636 Datenschutz, denn:

- 1637 - viele staatliche und kommunale Aufgaben, z. B. in den Bereichen Steuerverwaltung, Justiz,  
 1638 Sicherheit, Sozialhilfe und Gesundheitswesen, erfordern naturgemäß die Erfassung und  
 1639 Verarbeitung personenbezogener Daten, die einen besonderen Schutzbedarf aufweisen  
 1640 können;
- 1641 - die mit der Informationsverarbeitung einhergehenden Fachaufgaben, insbesondere in der  
 1642 Eingriffsverwaltung, sind gesetzlich legitimiert;
- 1643 - die vollständige Durchdringung der öffentlichen Verwaltung mit IT hat zur Konsequenz, dass  
 1644 die öffentliche Verwaltung in ihrer Gesamtheit über ein fast lückenloses Datenprofil aller  
 1645 Bürger verfügt.

1646 Datenschutz im öffentlichen Bereich muss vor diesem Hintergrund sicherstellen, dass

1647

- 1648 - die Informationsverarbeitung und die damit verbundene Einschränkung des  
 1649 informationellen Selbstbestimmungsrechtes in jedem Anwendungsfall rechtlich legitimiert  
 1650 und angemessen ist (Erforderlichkeitsgrundsatz);
- 1651 - die personenbezogenen Daten nur zu dem Zweck verwendet werden, für den sie erfasst  
 1652 wurden (Zweckbindungsgrundsatz);

---

<sup>209</sup> Beschluss vom 20. Juni 1984 - 1 BvR 1494/78, BVerfGE 67, 157 – G 10.

<sup>210</sup> BVerfGE 109, 279 – Großer Lauschangriff.

<sup>211</sup> BVerfGE 120, 274 – Onlinedurchsuchung.

<sup>212</sup> BVerfGE 93, 181 – Rasterfahndung I; BVerfGE 115, 320, 345 ff. – Rasterfahndung II.

<sup>213</sup> BVerfG, Urteil vom 11. März 2008 - 1 BvR 2074/05 - KFZ-Kennzeichenerfassung, teilweise abgedruckt in MMR 2008, 308.

<sup>214</sup> BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 – Vorratsdatenspeicherung.

- 1653 - betroffene Bürger wissen, welche öffentlichen Stellen welche Daten über sie gespeichert  
1654 haben (Transparenzgrundsatz), und
- 1655 - nur solche personenbezogenen Daten von Bürgern erfasst und gespeichert werden, die zur  
1656 Erledigung der jeweiligen Aufgabe unbedingt erforderlich sind (Datenvermeidungs- und  
1657 Datensparsamkeitsgrundsatz).
- 1658 Die bereichsspezifischen Regelungen zum Datenschutz sollen nicht nur einer materiellen Verletzung  
1659 dieser Grundsätze vorbeugen, sondern darüber hinaus auch vermeiden, dass die persönlichen  
1660 Grundrechte durch ein diffuses Gefühl totaler staatlicher Überwachung<sup>215</sup> eingeschränkt oder  
1661 beeinträchtigt werden.
- 1662 Gerade um diesem diffusen Gefühl totaler staatlicher Überwachung entgegenzutreten, wird diskutiert,  
1663 ob und wie Auskunftsrechte für Bürgerinnen und Bürger und Auskunftspflichten staatlicher Stellen,  
1664 etwa im Zusammenhang mit den Informationsfreiheitsgesetzen der Länder und des Bundes, überprüft  
1665 und gegebenenfalls ausgebaut werden sollten.
- 1666 Bei bisherigen Gesetzgebungsvorhaben konnten oft während des parlamentarischen Verfahrens noch  
1667 Veränderungen hin zu einer Reduzierung der Menge an gesammelten personenbezogenen Daten  
1668 erreicht werden, jedoch nicht ein vollständiger Verzicht auf das jeweilige Vorhaben. Gesetzliche  
1669 Schutzprogramme für den Datenschutz können zudem vielfach mit der technischen Entwicklung nicht  
1670 Schritt halten.
- 1671 Beim Betrieb bestehender oder der Einführung neuer IT-Infrastrukturen in öffentlichen Einrichtungen  
1672 ergeben sich daher eine Vielzahl datenschutzrechtlicher Fragestellungen.
- 1673 Deren frühzeitige Einbeziehung in alle Projekte, u. a. bei der Entwicklung der jeweiligen Hard- und  
1674 Software, ist unabdingbar. Die Umstellung bestehender Verwaltungsverfahren auf elektronische Basis  
1675 birgt dabei auch Chancen für den Datenschutz. Die zukünftige Technik kann bereits frühzeitig nach  
1676 den Geboten der Datensparsamkeit und -sicherheit gestaltet werden.<sup>216</sup>
- 1677 Fragen des Datenschutzes in öffentlichen Einrichtungen werden vielfach unter den Stichworten  
1678 „eGovernment und Datenschutz“ thematisiert. Als besondere Herausforderungen werden hierbei unter  
1679 anderem beschrieben:<sup>217</sup>
- 1680 • Zunahme personenbezogener Daten, d. h. die gesamte Kommunikation Einzelner mit Behörden  
1681 kann erfasst und analysiert werden; im Gegensatz dazu fallen etwa bei formlosen (fern-  
1682 )mündlichen Anfragen bei einer Behörde üblicherweise keinerlei Daten an;<sup>218</sup>
  - 1683 • Zunahme zentraler, bereichsübergreifender Datenbestände, etwa wenn  
1684 Verwaltungsdienstleistungen unterschiedlicher Behörden oder Behördenbereiche an einer  
1685 zentralen Stelle (etwa One-Stop-Government oder Lebenslagenkonzept) angeboten werden;

<sup>215</sup> BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08, NJW 2010, 833 (Absatz-Nr. 212) - Vorratsdatenspeicherung.

<sup>216</sup> Bizer, Johann (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein): eGovernment: Chance für den Datenschutz, abrufbar unter: <https://www.datenschutzzentrum.de/e-government/dud-200507.htm> (zuletzt aufgerufen am: 22. März 2011).

<sup>217</sup> 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](http://www.lfd.niedersachsen.de/live/live.php?navigation_id=13010&article_id=56234&_psmand=48) (zuletzt aufgerufen am: 22. März 2011).

<sup>218</sup> Vgl. hierzu auch Yildirim, Nuriye: Datenschutz im Electronic Government. 2004, S. 64.

- 1686 beispielsweise durch den „einheitlichen Ansprechpartner“ nach der EU-Dienstleistungsrichtlinie,  
 1687 der als zentrale Anlaufstelle insbesondere für elektronische Behördendienste fungiert;<sup>219</sup>  
 1688 • Fragen der Datensicherheit im Rahmen der elektronischen Kommunikation mit dem Bürger,  
 1689 etwa Gefährdungen des internen IT-Systems durch Systemöffnung, Notwendigkeit der  
 1690 Authentisierung bei Übermittlung personenbezogener Daten;  
 1691 • Fragen der internen Datensicherheit;  
 1692 • datenschutzrechtliche Verantwortlichkeiten bei Zusammenarbeit mehrerer Stellen,  
 1693 gegebenenfalls auch von Bund, Ländern und Kommunen;<sup>220</sup>  
 1694 • Einschaltung (privater) technischer Dienstleister.

1695 2.2.1.5. *Cloud Computing in der öffentlichen Verwaltung*

1696 Cloud Computing als Möglichkeit, Speicherkapazitäten, Rechenleistung und Software  
 1697 bedarfsspezifisch über das Internet zu beziehen, könnte perspektivisch auch in öffentlichen  
 1698 Einrichtungen an Bedeutung gewinnen. Die gemeinsame Nutzung von Hard- und Software sowie  
 1699 Rechenkapazitäten, die auf verschiedenen Servern nachfrage- und einzelfallabhängig zur Verfügung  
 1700 gestellt werden, könnte auch für Behörden, Ministerien und kommunale  
 1701 Selbstverwaltungskörperschaften möglicherweise Sparpotentiale durch Senkung der Ausgaben für  
 1702 eigene Hard- und Software eröffnen.<sup>221</sup>

1703 Allerdings steht diese Form der Vernetzung behördlicher IT-Infrastrukturen, also der von  
 1704 unterschiedlichen Trägern der öffentlichen Verwaltung eingesetzten Hard- und Software, noch am  
 1705 Anfang.<sup>222</sup> Soweit ersichtlich, gibt es in Deutschland noch keine Nutzung von Cloud-Anwendungen  
 1706 durch öffentliche Stellen, wohl aber entsprechende Prüfungen.<sup>223</sup> Dabei wird davon ausgegangen, dass  
 1707 sich nur Modelle einer abgeschlossenen („privaten“) Cloud in alleiniger Verantwortung der  
 1708 öffentlichen Verwaltung als mögliche Option erweisen könnten.<sup>224</sup>

1709

1710 Daneben stehen andere Formen der Zusammenarbeit von öffentlichen Einrichtungen im IT-Bereich,  
 1711 etwa als „Shared Services Center“. Hierbei werden verwaltungsunterstützende Leistungen für die  
 1712 öffentliche Verwaltung zentral und gemeinschaftlich erbracht. Interne Dienstleistungen (etwa  
 1713 Personalverwaltung oder Gebäude-Management) werden also mittels gemeinsamer Nutzung von  
 1714 Ressourcen für mehrere Organisationseinheiten erbracht.

---

<sup>219</sup> Vgl. hierzu auch Petersen, Christin: Einheitlicher Ansprechpartner und Datenschutz. LKV 2010, 344 ff.

<sup>220</sup> 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. Online abrufbar unter: [http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile) (zuletzt aufgerufen am: 22. März 2011).

<sup>221</sup> Vgl. Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung. MMR 2010, 75.

<sup>222</sup> Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung. MMR 2010, 75.

<sup>223</sup> Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 12.. Abrufbar unter: <https://www.datenschutzzentrum.de/cloud-computing/> (zuletzt aufgerufen am: 22. März 2011).

<sup>224</sup> Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 78.

1715 Die Bundesregierung strebt an, die Entwicklung und Einführung von Cloud Computing zu  
 1716 beschleunigen. Neben mittelständischen Unternehmen soll gerade der öffentliche Sektor frühzeitig  
 1717 von den Chancen profitieren. Unter anderem die Bereiche Sicherung und Schutz von Daten sind an  
 1718 die spezifischen Anforderungen von Cloud Computing anzupassen. Datenschutz und Datensicherheit  
 1719 seien eine der hierbei sich ergebenden rechtlichen Herausforderungen.<sup>225</sup> Hierzu hat die  
 1720 Bundesregierung ein „Forschungsprogramm Sichere Internet-Dienste – Cloud Computing für  
 1721 Mittelstand und öffentlichen Sektor (Trusted Cloud)“ aufgelegt.<sup>226</sup>

1722 Datenschutzrechtlich wird die Nutzung cloud-basierter Dienste bei der Verarbeitung  
 1723 personenbezogener Daten zumeist als eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG  
 1724 eingeordnet. Verantwortlich für die Einhaltung datenschutzrechtlicher Vorschriften ist weiterhin der  
 1725 Auftraggeber (§ 11 Abs. 1 BDSG). Dieser ist insbesondere verpflichtet, den Gegenstand des  
 1726 Auftragsverhältnisses schriftlich hinsichtlich diverser Einzelaspekte genau festzulegen (etwa die nach  
 1727 § 9 BDSG zu treffenden technischen und organisatorischen Schutzmaßnahmen oder die Berechtigung  
 1728 zur Begründung von Unterauftragsverhältnissen). Diese rechtlichen Vorgaben setzen der cloud-  
 1729 basierten Verarbeitung personenbezogener Daten bisher enge Grenzen.<sup>227</sup> Im Übrigen gelten insoweit  
 1730 ähnliche Überlegungen wie für die datenschutzrechtliche Beurteilung von Cloud Computing durch  
 1731 private Unternehmen.<sup>228</sup>

1732 2.2.2 Mögliche Erweiterung des Grundgesetzes im Hinblick auf das Grundrecht auf informationelle  
 1733 Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität  
 1734 informationstechnischer Systeme

1735 Der Schutz der informationellen Selbstbestimmung ist ebenso wie der Schutz der Vertraulichkeit der  
 1736 Kommunikation ein in vielen Landesverfassungen sowie internationalen Konventionen anerkanntes  
 1737 Grund- und Menschenrecht. Mit der europäischen Charta der Grundrechte wurde zudem ein  
 1738 Grundrecht auf Datenschutz geschaffen.<sup>229</sup> Das Grundgesetz enthält weder ein explizites Grundrecht  
 1739 auf informationelle Selbstbestimmung noch ein Grundrecht auf Gewährleistung der Vertraulichkeit  
 1740 und Integrität informationstechnischer Systeme. Das BVerfG hat jedoch in Rechtsfortbildung<sup>230</sup> diese  
 1741 beiden Grundrechte – das Recht auf informationelle Selbstbestimmung und das Recht auf Schutz der

---

<sup>225</sup> Bundesministerium für Wirtschaft und Technologie (Hrsg.): IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, abrufbar unter: <http://www.bmwi.de/Dateien/BBA/PDF/ikt-strategie-der-bundesregierung.property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf> (zuletzt aufgerufen am 16. Juni 2011).

<sup>226</sup> Bundesministerium für Wirtschaft und Technologie (Hrsg.): IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, abrufbar unter: <http://www.bmwi.de/Dateien/BBA/PDF/ikt-strategie-der-bundesregierung.property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf> (zuletzt aufgerufen am 16. Juni 2011).

<sup>227</sup> Vgl. Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 6.1., abrufbar unter: <https://www.datenschutzzentrum.de/cloud-computing/> (zuletzt aufgerufen am 11. November 2010); Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, 78 f. Zum Cloud Computing vgl. im Übrigen unter 2.3.3.

<sup>228</sup> Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, 78.

<sup>229</sup> Vgl. Art. 8 der Grundrechtecharta.

<sup>230</sup> 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.

- 1742 Vertraulichkeit und Integrität informationstechnischer Systeme - aus den vorhandenen Art. 1 Abs. 1 i.  
1743 V. m. Art. 2 Abs. 1 GG hergeleitet und angewendet.
- 1744 Für eine ausdrückliche Aufnahme der beiden Grundrechte in die Verfassung wird vorgetragen, dass  
1745 der Bedeutung der Entwicklung einer demokratischen und offenen digitalen Gesellschaft Rechnung  
1746 getragen würde. Zudem hätte dies eine bessere Erkennbarkeit für den Bürger zur Folge. Mit der  
1747 Aufnahme beider Grundrechte könnte auch der Verfassungsgesetzgeber die Rechtswirklichkeit an die  
1748 veränderten Umstände in einer digitalen Gesellschaft anpassen, zumal das Recht auf informationelle  
1749 Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität  
1750 informationstechnischer Systeme in den kommenden Jahren noch weiter an Bedeutung gewinnen  
1751 werden.
- 1752 Eine entsprechende Ergänzung um das Grundrecht auf informationelle Selbstbestimmung sowie das  
1753 Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme  
1754 würde zudem die Übernahme des durch das BVerfG beschrittenen Weges durch den  
1755 Verfassungsgesetzgeber unterstreichen.
- 1756 Gleichwohl fanden entsprechende Vorschläge für eine Verfassungsänderung im Deutschen Bundestag  
1757 bisher keine Mehrheit.<sup>231</sup> Gegen die vorgeschlagenen Formulierungen wird vorgetragen, dass das  
1758 Schutzniveau gegenüber der bestehenden Rechtslage senken könnten. Außerdem müsse sichergestellt  
1759 sein, dass weiterhin Raum für eine künftige Auslegung des Grundgesetzes bleibe, sodass auf neue  
1760 Fragen, die sich im Zusammenhang mit der technischen und gesellschaftlichen Entwicklung stellen,  
1761 verfassungsrechtliche Antworten gefunden werden können.
- 1762 2.2.3 Datensicherheit
- 1763 Datenschutz lässt sich in der Praxis nur dann sicherstellen, wenn die informationstechnischen Systeme  
1764 des öffentlichen Bereiches gegen unberechtigten Zugriff und missbräuchliche Nutzung von innen und  
1765 außen geschützt sind. Die hierfür einschlägigen Schutzregelungen (z. B. Anlage zu § 9 BDSG)  
1766 stammen aus einer Zeit, als Datenverarbeitung im öffentlichen Bereich durch Großrechner in  
1767 abgeschotteten Rechenzentren gekennzeichnet war. Die jüngere Rechtsprechung<sup>232</sup> stellt in ihren  
1768 Entscheidungen zunehmend auch auf die Bedeutung der informationstechnischen Sicherheit bei der  
1769 Verarbeitung der personenbezogenen Daten ab.
- 1770 Im Zuge des E-Government kommen längst Online-Verfahren zum Einsatz, bei denen Bürger selbst  
1771 auf die IT-Systeme der Verwaltung zugreifen. Durch diese Entwicklung und die fortschreitende  
1772 Vernetzung der Verwaltungssysteme untereinander wird es zunehmend schwieriger, das technisch  
1773 veraltete Regelwerk auf neue Technologien und vernetzte Infrastrukturen anzuwenden.
- 1774 Weitere Gesichtspunkte und Fragen der Datensicherheit werden zu einem späteren Zeitpunkt im  
1775 Schlussbericht der Enquete-Kommission im Kapitel „Zugang, Struktur und Sicherheit im Netz“  
1776 aufgegriffen.<sup>233</sup>

---

<sup>231</sup> Vgl. zuletzt BT-Drs. 16/9607 vom 18. Juni 2008 und BT-Drs. 16/13218 vom 27. Mai 2009

<sup>232</sup> Vgl. BVerfG zur Online-Durchsuchung, BVerfGE vom 27. Februar 2008 - 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.

<sup>233</sup> Vgl. im Übrigen auch unter 2.1.7.

## 1777 2.2.4 Datenschutzaudit und Gütesiegel zum Zwecke der Vertrauensbildung

1778 Datenschutz in öffentlichen Einrichtungen (sowie bei nicht-öffentlichen Stellen) kann durch  
 1779 Auditierungsverfahren gefördert und erleichtert werden. Die Verleihung von Gütesiegeln sowie die  
 1780 Zertifizierung und Durchführung von Audit-Verfahren können wirkungsvolle, marktsteuernde  
 1781 Anreize für besseren Datenschutz geben. Ähnlich wie bei der technischen Betriebssicherheit (dem  
 1782 TÜV) können Normen und Verfahren einen integrierten technischen Datenschutz fördern und  
 1783 gewährleisten. Die in den Bundesländern eingerichteten Datenschutzauditverfahren sowie das  
 1784 europäische Gütesiegel (EuroPriSe) können als praktische Beispiele hierfür angeführt werden.

1785 Dabei wird das Datenschutzkonzept durch einen unabhängigen Gutachter förmlich geprüft und von  
 1786 einer unabhängigen öffentlichen Stelle bestätigt.

1787 Im Unterscheid zu einer allgemeinen Beratung erfolgt beim Datenschutzaudit ein Mehr: Die Beratung  
 1788 bezieht sich auf die jeweils konkret vorgelegte Frage bzw. auf den unterbreiteten Sachverhalt. Ob die  
 1789 gegebenen Empfehlungen umgesetzt werden, bleibt offen und auch Veränderungen maßgeblicher  
 1790 Umstände werden nach Abschluss der Beratung nicht berücksichtigt. Das Audit hingegen ist auf eine  
 1791 dauerhafte Verbesserung der Datenschutzorganisation gerichtet. In Anlehnung daran könnte eine  
 1792 staatlich gestützte Datenschutzstiftung als Gütesiegelgarantie wirken und der Vertrauensbildung  
 1793 Vorschub leisten.

## 1794 2.3 Datenschutz im nicht-öffentlichen Bereich

### 1795 2.3.1 Datennutzung als Bestandteil innovativer Dienste

1796 Viele im Internet angebotene Dienste gehen auf Grund technischer Gegebenheiten mit einer Erhebung  
 1797 und Verarbeitung von Daten, in der Regel auch personenbezogener Daten, einher. Auf diese Art und  
 1798 Weise sind die Personalisierbarkeit und Interaktivität von Diensten im Internet realisierbar. Dienste  
 1799 können umso stärker an Interessen und Vorlieben ihrer Nutzer angepasst werden, je mehr Daten über  
 1800 das Verhalten der Nutzer verwertet werden. Auf diese Weise können die Anbieter auch möglichst  
 1801 passgenaue Werbung anbieten.

1802 Strenge Datenschutzvorschriften können die Entwicklung neuer Anwendungen erschweren oder sie  
 1803 unbequemer in der Nutzung machen. Andererseits können strengere Vorschriften auch geeignet sein,  
 1804 Verbrauchervertrauen aufzubauen, das die Nutzerzahlen erhöhen kann.

1805 Eine Missachtung der berechtigten Datenschutzerwartungen der Nutzer kann auch zu einer  
 1806 Gegenreaktion und Ablehnung eines Dienstes führen. Letztlich setzen Geschäftsmodelle, die auf der  
 1807 Verwendung von personenbezogenen Daten beruhen, immer auch eine Akzeptanz des Nutzers voraus.  
 1808 Hieraus kann sich ein Selbstkorrektiv in der Entwicklung von Diensten ergeben, solange sichergestellt  
 1809 ist, dass die Nutzer über Art und Umfang der vorgenommenen Datenverarbeitung informiert sind.

1810

1811 2.3.1.1. *Datenschutz in der Informations- und Kommunikationsgesellschaft: Zum*  
 1812 *Spannungsverhältnis und Gebot der Abwägung zwischen Persönlichkeitsrechten und*  
 1813 *Kommunikationsgrundrechten*

1814 Dass das allgemeine Persönlichkeitsrecht kann mit der Meinungsfreiheit in Konflikt geraten kann, ist  
 1815 allgemein bekannt und Gegenstand des Äußerungsrechts. Die Berichterstattung durch die Medien  
 1816 (Presse und Rundfunk), aber auch die Wahrnehmung der Meinungsfreiheit durch den Einzelnen kann  
 1817 Persönlichkeitsrechte verletzen. Es handelt sich um das klassische Spannungsverhältnis zwischen

- 1818 Persönlichkeitsrechten und Meinungsfreiheit, und zwar unabhängig davon, ob die Meinungsfreiheit  
1819 individuell vom Einzelnen oder durch Medien wahrgenommen wird.
- 1820 In der Informations- und Kommunikationsordnung des Internet gewinnt dieses Spannungsverhältnis  
1821 erheblich an Bedeutung. Dies liegt vor allem daran, dass der Einzelne im Internet ohne nennenswerte  
1822 Zugangsschranken an der (Massen-)Kommunikation mitwirken kann. Die starren Grenzen zwischen  
1823 Medien und Rezipienten verschwimmen.
- 1824 Die moderne Internetkommunikation wirft eine Vielzahl von Fragen auf, die u.a. die Zuordnung  
1825 bestimmter Dienste zu den grundrechtlich geschützten Kommunikationsfreiheiten betreffen. Weil  
1826 diese Zuordnungsfragen noch nicht geklärt sind, bereitet es oftmals Schwierigkeiten, die im Internet  
1827 auftretenden Probleme als grundrechtliche Konflikte zwischen Persönlichkeitsgrundrechten und  
1828 Kommunikationsgrundrechten wahrzunehmen. Recht einfach liegen die Dinge bei Blogs und  
1829 sonstigen meinungsbildenden Portalen („Spick-mich“ etc.), die sich auf Grund dieser  
1830 meinungsbildenden Funktion im Schutzbereich der Kommunikationsgrundrechte bewegen. Es handelt  
1831 sich letztlich um den klassischen Konflikt zwischen Meinungsäußerungsfreiheit und dem allgemeinen  
1832 Persönlichkeitsrecht des Betroffenen.
- 1833 Besondere Zuordnungsprobleme ergeben sich jedoch etwa bei solchen Diensten  
1834 („Informationsintermediäre“), die im Gegensatz zu klassischen Medien Informationen nicht nach  
1835 meinungsbezogenen, publizistischen Gesichtspunkten zusammenstellen und veröffentlichen, sondern  
1836 nach „meinungsneutralen“ formalen Kriterien Informationen zusammentragen, speichern und  
1837 verbreiten. So bereitet beispielsweise die rechtliche Einordnung von Suchmaschinen erhebliche  
1838 Schwierigkeiten, auch wenn sich ihre Input-Funktion aus allgemein zugänglichen Quellen speist und  
1839 die Benutzung von Suchmaschinen durch User als Ausübung der grundrechtlich geschützten  
1840 Informationsfreiheit (Art. 5 Abs. 1 Satz 1 Alt. 2 GG, Art. 10 Abs. 1 Satz 2 EMRK, Art. 11 Abs. 1 Satz  
1841 2 GRC) zu qualifizieren ist. Ungeachtet dieser grundrechtlichen Zuordnungsprobleme steht in jedem  
1842 Fall fest, dass solche Suchmaschinen aus der Informations- und Kommunikationsordnung des Internet  
1843 nicht wegzudenken und für die Funktionsfähigkeit der modernen Informationsgesellschaft schlechthin  
1844 unverzichtbar sind. Sofern solche Suchmaschinen personenbezogene Daten des Einzelnen  
1845 zusammentragen, speichern und ein mehr oder weniger umfangreiches Persönlichkeits- oder  
1846 Bewegungsprofil des Betroffenen auf Abruf zur Verfügung stellen, handelt es sich um einen Konflikt  
1847 zwischen Kommunikationsgrundrechten und Persönlichkeitsrechten. Auch insoweit gilt es, durch  
1848 Abwägung die einander widerstreitenden Güter im Sinne praktischer Konkordanz zu einem  
1849 wechselseitig möglichst schonenden Ausgleich zu bringen.
- 1850 Als weiteres Beispiel für die Schwierigkeiten, neue Internetdienste den klassischen  
1851 Kommunikationsgrundrechten zuzuordnen, seien soziale Netzwerke genannt. Gleichwohl würde es  
1852 die grundrechtliche Perspektive verengen, wenn man soziale Netzwerke ausschließlich aus dem  
1853 Blickwinkel des verfassungsrechtlich geschuldeten Schutzes des Grundrechts der informationellen  
1854 Selbstbestimmung betrachtete.
- 1855
- 1856 Viele Nutzer von sozialen Netzwerken und anderen Plattformen geben heute eine Vielzahl von Daten  
1857 preis, darunter auch sensible Daten wie die religiöse oder politische Überzeugung und die sexuelle  
1858 Orientierung. Die bewusste Verwendung und Offenbarung der eigenen Daten ist nicht pauschal zu  
1859 kritisieren oder gar zu verurteilen. Sie ist vielmehr die Wahrnehmung des Grundrechts auf  
1860 informationelle Selbstbestimmung, also die Ausübung grundrechtlich geschützter Freiheit.
- 1861 Ungeklärt ist, ob eine solche Preisgabe personenbezogener Daten darüber hinaus auch Ausdruck des  
1862 Grundrechts der Meinungsfreiheit ist. In diesem Zusammenhang ist zunächst festzuhalten, dass



1863 jedenfalls die Veröffentlichung personenbezogener Daten in entsprechenden Datenbanken sozialer  
 1864 Netzwerke („Profile“ ö. ä.) sowie die nachgelagerte Kommunikation zwischen „Freunden“ oder  
 1865 sonstigen Teilnehmern des Kommunikationsnetzwerkes auch der individuellen und öffentlichen  
 1866 Meinungsbildung dient und daher kommunikationsgrundrechtlich geschützt ist. Für den Schutz oder  
 1867 die Werthaltigkeit der Kommunikationsordnung kommt es auf den privaten bzw. nichtprivaten  
 1868 Charakter der Informationen prinzipiell nicht an. Auch die Offenbarung privater Informationen dient  
 1869 dem Kommunikationsprozess. War die Berichterstattung über Privates (insbesondere von  
 1870 Prominenten) in der Vergangenheit regelmäßig den Medien vorbehalten, die sich insoweit auf die  
 1871 grundrechtlich geschützte Presse- bzw. Rundfunkfreiheit berufen können<sup>234</sup>, kann nunmehr der  
 1872 Einzelne im Internet Privates offenbaren. Diese Form der Freiheitsbetätigung beruht auf doppeltem  
 1873 Grundrechtsboden: Sie ist Ausdruck des Grundrechts auf informationelle Selbstbestimmung und  
 1874 zugleich Wahrnehmung der grundrechtlich geschützten Meinungsfreiheit. Der Schutz der  
 1875 Kommunikationsordnung ist umfassend und unteilbar. Er lässt sich nicht zwischen schutzbedürftigen,  
 1876 weniger schutzbedürftigen oder schutzlosen Informationen unterteilen. Dies gilt insbesondere unter  
 1877 den Bedingungen der modernen Internetkommunikation, in der – wie das Beispiel sozialer Netzwerke  
 1878 zeigt – die Grenze zwischen privaten und nichtprivaten Informationen zunehmend verschwimmt.

1879 Hieraus erhellt, dass die Veröffentlichung personenbezogener Daten in entsprechenden Datenbanken  
 1880 sozialer Netzwerke („Profile“ o. ä.) als solche nicht nur Ausfluss des Grundrechts der  
 1881 informationellen Selbstbestimmung, sondern auch der Meinungsfreiheit ist. Zwar hat das  
 1882 Bundesverfassungsgericht im seinem Volkszählungsurteil die Verpflichtung zu Angaben im Rahmen  
 1883 statistischer Erhebungen nicht an der (negativen) Meinungsäußerungsfreiheit des Art. 5 Abs. 1 Satz 1  
 1884 GG gemessen, weil solche Angaben nicht durch Elemente der Stellungnahme, des Dafürhaltens und  
 1885 des Meinens gekennzeichnet sind.<sup>235</sup> Anders liegen die Dinge indes bei der Veröffentlichung  
 1886 personenbezogener Daten in sozialen Netzwerken. Zum einen beruhen solche Daten nicht nur auf  
 1887 „nackten“ Tatsachen, sondern oftmals auf persönlichen Einschätzungen, denen Wertungen zugrunde  
 1888 liegen (zum Beispiel: Selbsteinschätzung der politischen Überzeugung in sozialen Netzwerken,  
 1889 „Gefällt-mir“-Button).

1890 Und zum anderen ist die Veröffentlichung von personenbezogenen Tatsachen, die für sich genommen  
 1891 keine „Meinungen“ sind, Voraussetzung für den Aufbau entsprechender Kommunikationsnetzwerke,  
 1892 in denen sich die grundrechtlich geschützte Kommunikation vollzieht. Wegen dieses engen  
 1893 funktionalen Zusammenhangs wird man die Veröffentlichung auch solcher Daten als Ausdruck der  
 1894 Meinungsäußerungsfreiheit qualifizieren können. Das gilt auch deshalb, weil die Preisgabe  
 1895 personenbezogener Daten im Rahmen der Kommunikation zwischen „Freunden“ oder sonstigen  
 1896 Teilnehmern des Kommunikationsnetzwerkes dem Schutz der Meinungsfreiheit unterfällt.

1897 Eine pauschale Implementierung der datenschutzrechtlichen Grundsätze überall dort, wo  
 1898 grundrechtlich geschützte Kommunikationsinteressen betroffen sind, würde das verfassungsrechtliche  
 1899 Spannungsverhältnis zwischen dem grundrechtlich gebotenen Persönlichkeitsschutz einerseits und den  
 1900 Kommunikationsgrundrechten andererseits verfehlen. Von Verfassungs wegen gilt es, die einander  
 1901 widerstreitenden Güter im Sinne praktischer Konkordanz zu einem wechselseitig möglichst  
 1902 schonenden Ausgleich zu bringen.

---

<sup>234</sup> 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.

<sup>235</sup> Vgl. BVerfGE 65, 1, 40 f. – Volkszählung.

1903 Im Folgenden seien einige Abwägungsmaßstäbe genannt:

- 1904 • Ob und in welchem Umfang der (volljährige) Einzelne personenbezogene Daten im Internet  
 1905 offenbart, ist prinzipiell seine Entscheidung. Der Staat hat kraft seiner ihm obliegenden  
 1906 Schutzpflichten allein – etwa durch Auferlegung entsprechender Transparenz- und  
 1907 Informationspflichten der Anbieter sozialer Netzwerke – dafür Sorge zu tragen, dass der  
 1908 Einzelne Bedeutung und Tragweite seiner Entscheidung erkennen kann. Die  
 1909 grundrechtliche Schutzpflicht des Staates darf indes nicht in einen „Datenschutz vor sich  
 1910 selbst“ umschlagen. Nicht der Staat, sondern der Einzelne hat in Wahrnehmung seines  
 1911 Grundrechts auf informationelle Selbstbestimmung darüber zu entscheiden, ob und in  
 1912 welchem Umfang er personenbezogene Daten im Internet veröffentlicht und wem er diese  
 1913 öffentlich zugänglich macht (Prinzip der Eigenverantwortlichkeit). Im Rahmen der  
 1914 Abwägung ist dem möglicherweise ganz unterschiedlichen Schutzbedürfnis der  
 1915 verschiedenen betroffenen Personengruppen Rechnung zu tragen. Neben den individuellen  
 1916 Interessen des Einzelnen sind auch die Informationsinteressen der Allgemeinheit zu  
 1917 berücksichtigen. Alle diese Aspekte sind zu beachten, wenn der Gesetzgeber etwa vor der  
 1918 Entscheidung zwischen Opt-in- oder Opt-out-Regelungen steht.
- 1919 • Letztlich muss der Einzelne autonom entscheiden, ob und in welchem Umfang und zu  
 1920 welchem Zweck er personenbezogene Daten in sozialen Netzwerken preisgibt und auf diese  
 1921 Weise nicht nur von seinem Grundrecht auf informationelle Selbstbestimmung, sondern  
 1922 auch von seinem Grundrecht der Meinungsfreiheit Gebrauch macht. Die Entscheidung über  
 1923 die Preisgabe personenbezogener Daten und über die Kommunikation mit anderen in  
 1924 sozialen Netzwerken obliegt allein dem Einzelnen. Die besondere Problematik besteht  
 1925 indes darin, dass es „den“ User nicht gibt. Um nur ein Beispiel zu nennen: Während der  
 1926 eine weniger Wert auf die Zweckbestimmung der erhobenen Daten legt, weil sich im  
 1927 Zeitpunkt der Informationspreisgabe die künftigen Verwendungszwecke noch nicht  
 1928 absehen lassen und weil er in der unterschiedlichen Verwendung seiner Daten gerade einen  
 1929 Vorteil sieht, ist für den anderen genau eine solche exakte Zweckbestimmung  
 1930 unverzichtbar. Hier ergeben sich in regulatorischer Hinsicht erhebliche Probleme.
- 1931 • Für die Lösung dieses Konflikts ist insbesondere von Bedeutung, mit welcher Intensität in  
 1932 das Grundrecht auf informationelle Selbstbestimmung eingegriffen wird. Eingriffe in den  
 1933 Kernbereich des Grundrechts bzw. in die Intimsphäre sind grundsätzlich unzulässig. Die  
 1934 Veröffentlichung von Daten aus dem Kernbereich privater Lebensgestaltung und Ehre oder  
 1935 der Intimsphäre und die Veröffentlichung aussagekräftiger Persönlichkeitsprofile durch  
 1936 einen Anderen sind schon zum Schutz der Menschenwürde generell unzulässig. Im Bereich  
 1937 der Privatsphäre wird zum Schutz des Grundrechts auf informationelle Selbstbestimmung  
 1938 regelmäßig eine ausdrückliche Zustimmung (Opt-In) erforderlich sein. Im äußeren Bereich  
 1939 der Sozialsphäre kann hingegen eine ausdrückliche Ablehnung (Opt-Out) ausreichend sein,  
 1940 um die Bedeutung der Kommunikationsfreiheit hinreichend zu berücksichtigen.
- 1941
- 1942 • Je mittelbarer der Personenbezug von Daten ist, desto weniger gewichtig ist das Recht auf  
 1943 informationelle Selbstbestimmung im Rahmen des erforderlichen Güterausgleichs. Weiter  
 1944 kommt es bei der Gewichtung darauf an, ob das Recht auf informationelle  
 1945 Selbstbestimmung in der Intim-, Privat- oder Sozialsphäre betroffen ist.
- 1946 • Nicht nur unter den Bedingungen der modernen Informations- und  
 1947 Kommunikationsordnung muss sich der Einzelne auch der Kontrolle und Kritik durch die

1948 Gesellschaft stellen. In ständiger Rechtsprechung weist das Bundesverfassungsgericht  
 1949 darauf hin, dass das allgemeine Persönlichkeitsrecht (im Bereich der Sozialsphäre) dem  
 1950 Träger keinen Anspruch darauf verleiht, nur so in der Öffentlichkeit dargestellt zu werden,  
 1951 wie er sich selber sieht oder gesehen werden möchte.<sup>236</sup> Die Grenzen zulässiger  
 1952 Berichterstattung sind erst bei schwerwiegenden Auswirkungen auf das  
 1953 Persönlichkeitsrecht überschritten, also dann, wenn eine Stigmatisierung, soziale  
 1954 Ausgrenzung oder Prangerwirkung zu besorgen sind, wie es der Bundesgerichtshof kürzlich  
 1955 in der sogenannten Spickmich-Entscheidung nochmals klargestellt hat.<sup>237</sup>

1956 • Sofern personenbezogene Daten aus allgemein zugänglichen Quellen (Internet ö. ä.)  
 1957 stammen und deshalb dem besonderen Schutz des Grundrechts der Informationsfreiheit  
 1958 (Art. 5 Abs. 1 Satz 1 Alt. 2 GG, Art. 10 Abs. 1 Satz 2 EMRK, Art. 11 Abs. 1 Satz 2 GRC)  
 1959 unterfallen und nicht der Kernbereich des informationellen Selbstbestimmungsrechts bzw.  
 1960 die Intimsphäre betroffen sind, ist die Erhebung, Speicherung und Verwendung  
 1961 personenbezogener Daten zulässig, es sei denn, dass das Betroffeneninteresse offensichtlich  
 1962 überwiegt. Dieses Wertungsmodell könnte als Leitprinzip für die Ausgestaltung künftiger  
 1963 Konfliktsituationen dienen.

1964 Sofern der Einzelne in Kontakt oder Kommunikation mit anderen tritt (Sozialsphäre) und damit die  
 1965 persönliche Sphäre seiner Mitmenschen oder die Belange der Gemeinschaft berührt, muss er sich – im  
 1966 Interesse umfassender Kommunikation – Beschränkungen seines allgemeinen Persönlichkeitsrechts  
 1967 und seines Rechts auf informationelle Selbstbestimmung gefallen lassen. Insbesondere hat er keinen  
 1968 Anspruch darauf, in der Öffentlichkeit nur so dargestellt zu werden, wie er möchte.

#### 1969 2.3.1.2. *Geschäftsmodelle von Internet-Diensten / Online-Werbung*

1970 Das Internet besteht sowohl aus Inhalten und Diensten, die allen Nutzern kostenlos zur Verfügung  
 1971 stehen, als auch aus Inhalten und Diensten, die lediglich gegen Entgelt abgerufen werden können (=  
 1972 „Paid Content“ bzw. „Paid Services“). Dabei ist die überwiegende Zahl der Inhalte derzeit entgeltfrei  
 1973 abrufbar. Viele dieser unmittelbar kostenfreien Inhalte und Dienste werden kommerziell erbracht,  
 1974 wobei Online-Werbung nicht nur der Refinanzierung der Kosten dienen kann, sondern auch der  
 1975 Erzielung von Gewinnen. Aber auch nicht-kommerzielle Angebote setzen Online-Werbung ein, um  
 1976 zumindest einen Teil der mit der Bereitstellung verbundenen Kosten zu decken.

1977 Online-Werbung kann damit die Bereitstellung bestimmter Angebote ermöglichen und einen Beitrag  
 1978 zur Vielfalt im Wettbewerb leisten. Auch im Online-Bereich ist es beispielsweise über  
 1979 Bannerwerbung möglich, Werbung ohne die Erhebung von Nutzerdaten zu schalten.

1980 Gegenüber anderen Werbeformen bietet die zielgerichteten Online-Werbung allerdings aufgrund der  
 1981 technisch angelegten individualisierten Bereitstellung von Inhalten für den Nutzer auch die  
 1982 Möglichkeit, auf die vermutlichen individuellen Interessen der Nutzer abgestimmte Informationen  
 1983 und Werbebotschaften zu liefern. Hierdurch steigt die Wahrscheinlichkeit, dass ein Werbeinhalt vom  
 1984 Empfänger als relevant erachtet wird. Dies erhöht wiederum die erzielbaren Gewinne je angezeigter  
 1985 Werbung. Damit kann sich auch die Menge der ungezielten Werbung reduzieren, die notwendig ist,  
 1986 um eine Finanzierung des Web-Angebots zu erreichen. Es besteht dabei aber keine Garantie, dass  
 1987 tatsächlich weniger Werbung eingesetzt wird.  
 1988

<sup>236</sup> 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 - Missbrauchsbeziehung; BVerfG, Beschluss vom 10. November 1998 - 1 BvR 1531/96, BVerfGE 99, 185, 194 - Scientology; BVerfGE, 101, 361, 380 – Caroline von Monaco II.

<sup>237</sup> BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 – spickmich.de.

- 1989 Es gibt eine Vielzahl von Technologien und Vorgehensweisen (Algorithmen), mit deren Hilfe bei  
 1990 verhaltensbezogener Werbung („Behaviourial Advertising“) eine Vorhersage über das vermutliche  
 1991 Interesse des Werbeadressaten getroffen wird. Die Methoden nutzen in sehr verschiedener Weise und  
 1992 in sehr unterschiedlichem Umfang und Intensität Daten aus der aktuellen bzw. vorangegangenen  
 1993 Internetnutzung des Werbeempfängers.
- 1994 Allerdings muss verhaltensbezogene Werbung nicht unbedingt darauf beruhen, dass Informationen  
 1995 über das Surfverhalten der Nutzer dauerhaft gespeichert werden. Sie kann auch über eine  
 1996 anonymisierte Zuordnung zu Interessenkategorien realisiert werden, die auf einer bestimmten Art der  
 1997 Verwendung der Cookie-Technik basiert. Diese Cookies kann der Nutzer gegebenenfalls manuell  
 1998 wieder entfernen. Allerdings gibt es keine Möglichkeit auszuschließen, dass Webseiten, die Cookies  
 1999 auf dem Rechner des Nutzers ablegen, bei diesem Nutzer auch Daten erheben.
- 2000 In allen Fällen, in denen nutzungsbezogene Daten verarbeitet werden, muss es allerdings eine zentrale  
 2001 Voraussetzung sein, dass der Nutzer Informationen über die vorgenommene Verwendung erhält und  
 2002 ihm eine Wahlmöglichkeit zusteht, mit der er den Einsatz solcher individualisierender  
 2003 Werbetechniken beeinflussen kann.
- 2004 Neben dem schlichten Schalten von Werbeeinblendungen werden Kunden zum Zweck der  
 2005 Verkaufsförderung auch gezielt angesprochen. Dies geschieht auch über Anzeigen mit besonderen  
 2006 Angeboten oder Gutscheinen für Neukunden und Aktionen wie Treue-Boni oder Rabatte zur  
 2007 langfristigen Bindung von Bestandskunden.
- 2008 Die eingesetzten Techniken ermöglichen es, sowohl Werbung, Zielseiten, aber auch Angebote und  
 2009 Preise in Echtzeit auf die speziellen Verhaltensweisen eines Nutzers auszurichten. Durch die  
 2010 Techniken des so genannten „Targeting“ ist es teilweise möglich, den Nutzer beim Besuch der Seite  
 2011 wiederzuerkennen, das jeweilige Verhalten zu erfassen und Webinhalte und –services  
 2012 dementsprechend dynamisch den Nutzerpräferenzen anzupassen. Für die Nutzer der Seite ist es dabei  
 2013 nicht mehr erkennbar, ob es sich um für sie bereits angepasste Webseiten und Werbeangebote oder  
 2014 aber Standardwebseiten handelt, die für alle Nutzer gleich sind.<sup>238</sup> Oftmals werden darüberhinaus auch  
 2015 Kombinationen von mehreren Techniken eingesetzt.
- 2016 Jenseits des Schutzes der Privatsphäre sind daher die Auswirkungen auf die Marktposition der  
 2017 Nutzer/Verbraucher im Internet erheblich und müssen in Transparenz- sowie  
 2018 Einwilligungserfordernissen berücksichtigt werden.
- 2019
- 2020 Die Zulässigkeit, Transparenz- und Einwilligungserfordernisse hängen wesentlich von den  
 2021 eingesetzten Techniken, der Sensibilität der erhobenen Daten und der Datennutzung ab. So ist von  
 2022 Bedeutung, ob Nutzungsdaten aggregiert erhoben sowie verarbeitet werden und eine individualisierte  
 2023 Auswertung nicht beabsichtigt ist. Relevant ist dabei auch, ob sie pseudonymisiert oder anonymisiert  
 2024 werden.
- 2025 Ebenso ist es relevant, ob die Datenverarbeitung durch den Anbieter der Webseite selbst erfolgt oder  
 2026 ob die Daten durch an dem Leistungsverhältnis gar nicht beteiligte Dritte erhoben und verwendet

---

<sup>238</sup> 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 Besonderen siehe Klein, A./ Leithold, Franziska/ Zell, Christine/Roosen, Jutta: „Digitale Profilbildung und Gefahren für die Verbraucher“. TU München, Gutachten im Auftrag des Verbraucherzentrale Bundesverbandes e.V., November 2010. Zusammenfassung abrufbar unter: [http://www.vzbv.de/mediapics/digitale\\_profilbildung\\_tu\\_muenchen\\_leithold\\_2010.pdf](http://www.vzbv.de/mediapics/digitale_profilbildung_tu_muenchen_leithold_2010.pdf) (zuletzt aufgerufen am 16. Juni 2011).

2027 werden. Während die Datenverarbeitung im ersten Fall auf Basis der vom Webseitenanbieter  
 2028 bereitgestellten Datenschutzerklärung transparent gemacht werden kann und der Nutzer die  
 2029 Möglichkeit erhält, gegenüber einem klar identifizierbaren Ansprechpartner von seinem Wahlrecht  
 2030 hinsichtlich der Datenerhebung und -verwendung Gebrauch zu machen, ist im letzteren Fall die  
 2031 geforderte Transparenz für den Nutzer oft nicht mehr gegeben und es fehlt ihm häufig die  
 2032 Möglichkeit, Einfluss auf die Datenerhebung und -verwendung zu nehmen.

2033 Die Kontrolle des Nutzers wird auch davon beeinflusst, ob die Daten – etwa in Form von Cookies –  
 2034 auf seinem Gerät und damit in seinem Herrschaftsbereich gespeichert werden, so dass er  
 2035 beispielsweise über Browser-Einstellungen einwirken kann, oder ob gesammelte Daten zentral und  
 2036 damit seinem Zugriff entzogen gespeichert werden.

2037 Schließlich können besondere Umstände einen besonders schwerwiegenden Eingriff darstellen und  
 2038 deshalb auch unzulässig sein. Dies ist etwa der Fall, wenn für die zielgerichtete Ansprache (Targeting)  
 2039 auch sensible Daten verwendet werden, wie etwa Informationen über Gesundheit oder sexuelle  
 2040 Orientierung. Problematisch ist auch, wenn Daten aus besonders geschützten Bereichen wie etwa der  
 2041 Individualkommunikation gewonnen werden, etwa durch die Analyse von E-Mail-Inhalten.  
 2042 Besondere Fragen wirft auch die übergreifende Nachverfolgung („Tracking“) des Surfverhaltens  
 2043 einzelner Nutzer über eine Vielzahl von Webangeboten hinweg auf, da hier nicht nur Informationen  
 2044 bezüglich der Nutzung eines bestimmten Angebots gewonnen, sondern ein umfassendes  
 2045 Bewegungsprofil der Nutzer im Netz gewonnen werden.

#### 2046 2.3.1.3. *Bildung von Persönlichkeitsprofilen / Tracking über die Grenzen einzelner Webseiten hinweg*

2047 Personenbezogene Daten können in unterschiedlicher Intensität Aussagen über Personen und deren  
 2048 soziale Beziehungen enthalten. Je nach Umfang und Qualität der Daten lassen sich Daten durch  
 2049 Zusammenführung aus unterschiedlichen sozialen Zusammenhängen zu Persönlichkeitsbildern  
 2050 verdichten. Dem entspricht, beispielsweise übertragen auf das Internet, die Zusammenführung von  
 2051 Daten über das Nutzungsverhalten von unterschiedlichen Webangeboten. Entsprechende  
 2052 Geschäftsmodelle reichen von der Zusammenführung von Nutzungsdaten innerhalb des  
 2053 Webangebotes eines einzelnen Anbieters bis hin zu komplexen webseitenübergreifenden  
 2054 Kooperationen unterschiedlicher Anbieter, oftmals unter Einschaltung von Dienstleistern (z. B.  
 2055 doubleclick; Facebook-Like-Button). Aufgegriffen wurde der Begriff der Profilbildung u. a. vom  
 2056 Bundesverfassungsgericht im Volkszählungsurteil.<sup>239</sup> Das Gericht betont das Verbot von  
 2057 Profilbildungen, die geeignet sind, die Persönlichkeit von Menschen vollständig oder nur teilweise  
 2058 abzubilden. Befürchtet wird, dass die in öffentlicher Hand und zu ganz unterschiedlichen Zwecken  
 2059 gesammelten Datenbestände zusammengeführt werden und ein nahezu lückenloses Bild der Bürger  
 2060 zum Zweck der Herrschaftsausübung schaffen könnten. Als Risiko im Kontext der Privatwirtschaft  
 2061 gilt der Missbrauch entsprechend reichhaltiger Profile und die oftmals intransparent bleibende  
 2062 Beeinflussung der wirtschaftlichen Entscheidungen der Verbraucher durch gezielte Werbung. In Folge  
 2063 der technischen Entwicklung spielen Fragen der Profilbildung nicht nur im öffentlichen Bereich (z. B.  
 2064 Rasterfahndungen), sondern auch im nicht-öffentlichen Bereich eine große Rolle. Dabei ist zwischen  
 2065 ganz unterschiedlichen Arten von Profilen und deren Nutzung zu unterscheiden.

2066 Im Internet sind für bestimmte Nutzergruppen angepasste oder sogar besonders detaillierte und  
 2067 personalisierte Angebote möglich und gängig. Seit Jahren werden Auswertungstools verwendet, mit  
 2068 denen das Nutzerverhalten auf einer Website statistisch erfasst und analysiert werden kann. Die dabei  
 2069 untersuchten Daten werden häufig nur aggregiert und/oder pseudonymisiert ausgewertet. Ob es sich

---

<sup>239</sup> Vgl. BVerfGE 65, 1 – Volkszählung.

2070 dabei um anonyme und damit nicht mehr dem Anwendungsbereich der Datenschutzgesetze  
 2071 unterfallende Profildaten handelt, ist jedoch umstritten. In einigen Fällen wird allerdings durch die  
 2072 Einbeziehung von personenbezogenen Webangeboten (soziale Netzwerke; Mailangebote) insgesamt  
 2073 eine Personenbeziehbarkeit des Profils herbeigeführt. Es besteht Einigkeit, dass solche  
 2074 Nutzungsprofile bei Einhaltung bestimmter Vorgaben, zulässig sind.<sup>240</sup> Anhand dieser  
 2075 Nutzungsprofile können Websites z. B. nutzerfreundlicher gestaltet werden. Durch eine entsprechende  
 2076 Optimierung der Website können Effizienzgewinne bei der Bewerbung und dem Verkauf von  
 2077 Produkten erreicht werden.

2078 Auch andere Methoden der Profilbildung wie etwa das so genannte Scoring, d. h. die Bewertung von  
 2079 Personen anhand der Zuordnung von statistischen Erfahrungswerten, sind in der Wirtschaft üblich.  
 2080 Der Gesetzgeber hat darauf reagiert und Grenzen wie das Verbot automatisierter Einzelbewertung  
 2081 sowie zusätzliche Transparenzanforderungen geschaffen. Die Ergebnisse der Profilbildung beim  
 2082 Scoring basieren zumeist auf statistischen Annahmen, die ohne weiteres auf Individuen angewandt  
 2083 werden. Entscheidungen zu Personen, die auf Grundlage solcher Profile getroffen werden, basieren  
 2084 damit nicht mehr auf individuellen Gegebenheiten, obwohl es im Einzelfall stets ganz anders sein  
 2085 kann als im statistischen Mittel. Dementsprechend können Diskriminierungen bis hin zur  
 2086 Ausgrenzung ganzer Gruppen eintreten. Diese Nichtberücksichtigung individueller Verhältnisse  
 2087 berührt Grundrechte des Persönlichkeitsschutzes wie auch die Menschenwürde.

2088 Weitergehende Analysen z. B. auf der Grundlage aller zu einer Person verfügbaren Informationen (z.  
 2089 B. webseitenübergreifend wie durch den Facebook-Like-Button) sind denkbar. Durch die Möglichkeit  
 2090 allgegenwärtiger Datenverarbeitung (ubiquitous computing) und Vernetzung potenzieren sich die  
 2091 Möglichkeiten als auch das Risikopotenzial von Profilbildung im Internet. Dementsprechend wird  
 2092 auch und gerade im Kontext des Internets die eingehende Regulierung des zulässigen Einsatzes der  
 2093 Profilbildung gefordert (so zuletzt die Konferenz der Datenschutzbeauftragten in ihrem  
 2094 Eckpunktepapier zur Modernisierung des Datenschutzes).<sup>241</sup> Diskutiert werden in diesem  
 2095 Zusammenhang eine gesetzliche Definition der Profilbildung und die Schaffung von gesetzlichen  
 2096 Grundlagen, die dem besonderen Gefährdungspotential von Profilbildungen Rechnung tragen. Für die  
 2097 Beurteilung des Gefährdungspotentials kommt es maßgeblich darauf an, welche Art von Daten, in  
 2098 welcher Form und zu welchem Zweck und in welchem Umfang erfasst und ausgewertet werden  
 2099 können. Gefordert wird auch eine Anonymisierung, soweit dies möglich ist. Zusätzliche  
 2100 Transparenzanforderungen wie die Pflicht zur Erläuterung von Profilbildungsverfahren sollen  
 2101 Verbrauchern helfen, die Folgen der Nutzung von entsprechenden Angeboten einschätzen zu können.

2102

---

<sup>240</sup> 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](http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile) (zuletzt aufgerufen am 23. März 2011).

<sup>241</sup> 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](http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile) (zuletzt aufgerufen am: 22. März 2011).

2103

2104 2.3.2 Ausgestaltung und Reichweite von Transparenzinstrumenten (Informationspflichten,  
2105 Auskunftsrechte)

2106 Transparenz und damit Informationen sind Kernelemente für informierte Entscheidungen und  
2107 Aktivitäten der Aufsichtsbehörden, Wettbewerber bzw. anderer Unternehmen und Verbraucher. Eine  
2108 wesentliche Voraussetzung für die auch praktische Durchsetzung des Datenschutzes – und damit der  
2109 Realisierung des Rechts auf informationelle Selbstbestimmung – ist die Kenntnis über sowohl das  
2110 Recht bzw. die eigenen Rechte als auch über die tatsächlich durchgeführte Datenerhebung und -  
2111 verarbeitung.

2112 Transparenz für die Nutzer setzt voraus, dass sich der Nutzer seinem Bedarf entsprechend und  
2113 frühzeitig über Art und Umfang der Datenerfassung und -verarbeitung informieren kann. Dabei ist es  
2114 angesichts oft komplexer technischer Zusammenhänge besonders wichtig, für die Verständlichkeit der  
2115 vermittelten Informationen zu sorgen.

2116 Wie wichtig Transparenz für den Nutzer ist, zeigt das Beispiel der Einführung neuer Technologien  
2117 und Dienste: Am Anfang steht, wie z.B. bei Apps, das positive Nutzungserlebnis und die Freude über  
2118 den Mehrwert der Innovation. Ohne vorherige Information kämen erst nach und nach Erfahrungen  
2119 dazu, die aufhorchen und die Frage nach dem Datenschutz und möglichen Missbrauchsszenarien laut  
2120 werden lassen. Die berechtigte Sorge wird dabei aus dem Umstand genährt, dass Dinge im  
2121 Hintergrund passieren, die unbekannt und vermeintlich nicht beeinflussbar bzw. kontrollierbar sind.

2122 Hier ist der Ansatz für Transparenz und deren Instrumente. Der Nutzer soll in die Lage versetzt  
2123 werden zu verstehen, was mit den Daten passiert und ob er das so und in diesem Umfang will.

2124 Letztlich muss der Nutzer derjenige bleiben, der diese Entscheidung trifft. Damit wird die Frage der  
2125 Reichweite bzw. der Grenze von Transparenzinstrumenten angesprochen.

2126 Ziel sollte also die verständliche, neutrale Information über die tatsächlichen technischen Vorgänge  
2127 sein. Dem Nutzer muss klar werden, wer persönliche Daten verarbeitet, wie, in welchem Umfang und  
2128 zu welchen Zwecken dies geschieht und wer sein Ansprechpartner für Fragen und – besonders wichtig  
2129 – die Ausübung seiner Selbstbestimmung über die Datenverarbeitung ist.

2130 Das Bundesdatenschutzgesetz (BDSG), das Telemediengesetz (TMG) und das  
2131 Telekommunikationsgesetz (TKG) sehen jeweils bereits eine Reihe von Transparenzinstrumenten vor.  
2132 Diese Regelungen sind somit eine gesetzliche Konkretisierung des Rechts auf informationelle  
2133 Selbstbestimmung.

#### 2134 Informationspflichten von Diensteanbietern

2135 Diensteanbieter haben grundsätzlich die Pflicht, die Nutzer über Art, Umfang und Zweck von  
2136 Erhebung und Verwendung personenbezogener Daten zu unterrichten (§ 13 TMG, § 33 BDSG). Die  
2137 Informationspflichten sollen sicherstellen, dass die Adressaten Kenntnis erhalten über die  
2138 Datenverarbeitung. Es muss über die Identität der verantwortlichen Stelle informiert werden, damit  
2139 bekannt ist, wer die Daten erhebt und als Adressat eines Auskunftsanspruchs zur Verfügung steht.  
2140 Über sämtliche Zweckbestimmungen der Verarbeitung und Nutzung der Daten muss informiert  
2141 werden, soweit sie über die zur Vertragsdurchführung erforderlichen Daten hinausgehen. Der oder die  
2142 Empfänger der Daten müssen zumindest als Kategorie bekannt sein (vgl. § 33 Abs. 1 Satz 3 BDSG).  
2143 Eine namentliche Nennung der Empfänger ist jedoch nicht erforderlich, sodass eine lückenlose  
2144 Verfolgung des Weges der Daten nicht ohne weitere Informationen bzw. Auskunftersuchen möglich

2145 ist. Dieses Wissen ist für eine Person jedoch notwendig, um die Auskunftsrechte bei allen Stellen, die  
2146 Daten über diese Person haben, geltend machen zu können.

2147 Die Unterrichtung muss in einer allgemein verständlichen Form geschehen. Damit soll gewährleistet  
2148 werden, dass die Bürger eine informierte Entscheidung zur Preisgabe ihrer persönlichen Daten treffen  
2149 und ggf. eine Einwilligung verweigern können. In der Regel sind diese Informationen in den  
2150 allgemeinen Geschäftsbedingungen (AGB) und Nutzungsbedingungen der Diensteanbieter enthalten.  
2151 Da es sich zumeist um umfangreiche und aufgrund gesetzlicher Vorgaben rechtssicher zu  
2152 formulierende Texte handelt, sind sie für viele Menschen oftmals nicht in Gänze nachvollziehbar und  
2153 nur schwer zu verstehen.

#### 2154 Auskunftsrechte des Betroffenen

2155 Neben der Informationspflicht der Diensteanbieter bei Erhebung, Speicherung und Verwendung von  
2156 personenbezogenen Daten sind in § 34 BDSG umfassende Auskunftsrechte für Betroffene  
2157 festgeschrieben. Diese berechtigen Betroffene dazu, jederzeit und bedingungslos zu erfahren, welche  
2158 personenbezogenen Daten über sie von einer verantwortlichen Stelle erhoben, verarbeitet oder genutzt  
2159 werden, und woher die Daten stammen, an wen die Daten weitergeleitet werden und zu welchem  
2160 Zweck diese Daten gespeichert werden. Unter bestimmten Bedingungen kann die verantwortliche  
2161 Stelle die Auskunft allerdings verweigern, etwa zur Wahrung von Geschäftsgeheimnissen (vgl. § 34  
2162 BDSG). Wengleich diese Auskunftsrechte ein starkes Instrument zur Wahrung der informationellen  
2163 Selbstbestimmung für Betroffene sind, erscheint die praktische Nutzung in einer Umgebung, in der  
2164 immer mehr Anwendungen im Alltag personenbezogene Daten nutzen, zunehmend weniger  
2165 handhabbar.

2166 In letzter Zeit ist deshalb die Idee des so genannten Datenbriefs im Gespräch. Unternehmen, Behörden  
2167 oder sonstige Institutionen könnten gesetzlich verpflichtet werden, Bürgerinnen und Bürger  
2168 regelmäßig darüber zu informieren und zu erläutern, welche Daten zu welchem Zweck über sie  
2169 gespeichert werden. Dies käme einem Paradigmenwechsel gleich: Das derzeitige Auskunftsrecht  
2170 würde durch eine Informationspflicht ergänzt. Der Betroffene müsste also nicht mehr selbst aktiv  
2171 werden, um zu erfahren, welche Daten wo über ihn gespeichert sind, sondern würde automatisch  
2172 darüber benachrichtigt.

2173 Für den Datenbrief wird angeführt, dass viele Betroffene derzeit oft gar nicht wissen würden, wo  
2174 überall Daten über sie gespeichert werden. Sie könnten daher gar nicht von ihrem gesetzlich  
2175 eingeräumten Auskunftsrecht Gebrauch machen. Dieser Anspruch würde daher häufig ins Leere  
2176 laufen. Mit dem Datenbrief würde zudem das Verantwortungsbewusstsein der für die  
2177 Datenverarbeitung verantwortlichen Stellen gestärkt. Sie würden unter Umständen genauer prüfen, ob  
2178 und wie lange personenbezogene Daten tatsächlich gespeichert werden müssten.

2179 Gegen den Datenbrief wird angeführt, dass er zunächst bei vielen datenverarbeitenden Stellen zu einer  
2180 zentralen Zusammenführung der Daten führen könnte. An diese Konzentration von Daten müssten  
2181 dann nicht nur höhere Sicherheitsanforderungen gestellt werden, sondern dies könnte auch wegen  
2182 einer damit verbundenen Möglichkeit der verstärkten Profilbildung zu einer Beeinträchtigung des  
2183 Rechts auf informationelle Selbstbestimmung führen. Auch die praktische Umsetzung des Datenbriefs  
2184 wird als zu bürokratisch und kostenintensiv für die betroffenen Unternehmen kritisiert.

#### 2185 Informationspflichten bei „Datenpannen“

2186 Die „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten“ (§ 42a BDSG)  
2187 verpflichtet verantwortliche Stellen im nicht-öffentlichen Bereich, die Betroffenen sowie die  
2188 zuständigen Aufsichtsbehörden umgehend zu informieren, wenn gespeicherte sensible



2189 personenbezogene Daten unrechtmäßig an Dritte gelangen. Diese Regelung wurde jedoch erst im Jahr  
 2190 2009 in das BDSG aufgenommen. Ursache hierfür waren vorhergegangene unerlaubte und  
 2191 missbräuchliche Erhebungen und Verarbeitungen von personenbezogenen Daten in der Wirtschaft.

2192 Ziel aller Informationspflichten ist es, Transparenz über die Speicherung und Verarbeitung von Daten  
 2193 herzustellen. Diese Transparenz ist Voraussetzung dafür, die informationelle Selbstbestimmung  
 2194 tatsächlich ausüben zu können. Ohne ausreichende Transparenz kann keine informierte Einwilligung  
 2195 erteilt werden. Wenn Betroffene in die Lage versetzt werden sollen, bereits nach dem BDSG  
 2196 bestehende Auskunfts-, Lösch-, Widerspruchs- und Berichtigungsrechte auch tatsächlich geltend  
 2197 machen zu können, ist die Kenntnis notwendig, wer welche Daten zu welchem Zweck gespeichert hat.

### 2198 2.3.3 Cloud Computing

#### 2199 Beschreibung

2200 Angesichts stetig steigender Datenvolumina und einer wachsenden mobilen Nutzung von Daten stellt  
 2201 sich dem Nutzer – sei es Privatperson oder Unternehmer – zunehmend die Frage „Wohin mit den  
 2202 Daten, die anfallen?“ und „Wie kann ich Datenverarbeitungsprozesse effizienter und kostengünstiger  
 2203 machen?“. Als Lösung wird zunehmend das so genannte Cloud Computing angeführt, übersetzt  
 2204 „Datenverarbeitung in der Wolke“.

2205

2206 Von Cloud Computing wird dann gesprochen, wenn eine oder mehrere der IT-Dienstleistungen, wie  
 2207 Infrastruktur (Rechenleistung, Hintergrundspeicher, etc.), Plattform oder Anwendungssoftware  
 2208 aufeinander abgestimmt und nach tatsächlicher Nutzung abrechenbar über ein Netz durch Dritte  
 2209 bereitgestellt werden.<sup>242</sup> Obwohl die Online-Speicherung von Daten, Online-Adressbüchern oder  
 2210 Online-Kalendern oder etwa die webbasierte Nutzung von E-Mail-Diensten bereits als alltägliche  
 2211 Cloud-Anwendungen von vielen genutzt werden, kann zum gegenwärtigen Zeitpunkt noch nicht  
 2212 davon ausgegangen werden, dass der Begriff und die dahinter liegende Technik des Cloud Computing  
 2213 geläufig sind. Es ist davon auszugehen, dass sich das Cloud Computing in den nächsten Jahren vor  
 2214 allem im Bereich der Geschäftsanwendungen und der Serverkapazitäten immer weiter etablieren wird.

2215 Angebotene Dienstleistungen im Cloud Computing können u. a. bereitgestellter Speicher oder  
 2216 Rechenzeit sein, aber auch z. B. komplette Datenverarbeitungsverfahren. Beim Cloud Computing  
 2217 wird zum einen unterschieden nach der Art der angebotenen Dienstleistung in der Cloud, und zwar  
 2218 zwischen Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service  
 2219 (IaaS). Zum anderen wird nach der Beschaffenheit der Cloud zwischen Privaten und Public Clouds  
 2220 unterschieden. Private Clouds sind vernetzte Rechner, die alle unter der rechtlichen Verantwortung  
 2221 einer einzigen Daten verarbeitenden Stelle stehen.<sup>243</sup> Als Private Clouds werden aber auch  
 2222 Rechnernetze von rechtlich zueinander in einem engen Verhältnis stehenden Stellen bezeichnet, z. B.  
 2223 Stellen der öffentlichen Verwaltung oder eines Konzerns.<sup>244</sup>

---

<sup>242</sup> Bundesamt für Sicherheit in der Informationstechnik. Essoh, Alexander Didier: Cloud Computing und Sicherheit - Geht denn das?, Folie 4.  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/4GS\\_Tag/07\\_essoh\\_bsi.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/4GS_Tag/07_essoh_bsi.pdf?__blob=publicationFile) (zuletzt aufgerufen am  
 23. März 2011).

<sup>243</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (679).

<sup>244</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

2224 Eine Public Cloud ist eine öffentliche Cloud, welche von einer Vielzahl von Personen und Firmen  
 2225 genutzt werden kann. Die Public Cloud ist nicht auf eine bestimmte Institution, ein bestimmtes  
 2226 Unternehmen oder einen bestimmten Personen-/Nutzerkreis beschränkt. Wesentliches Merkmal ist,  
 2227 dass sie jedermann zugänglich ist und dass der Anwender nicht mitbestimmen kann, mit welchen  
 2228 Anwendern er sich die Nutzung einer Hardware teilt, also mit welchen anderen virtuellen Maschinen  
 2229 seine virtuelle Maschine auf derselben physischen Hardware läuft.<sup>245</sup> Dabei wird die Rechenleistung  
 2230 von „Dritten“ i. S. d. Datenschutzrechts (§ 3 Abs. 8, S. 2 BDSG) angeboten.<sup>246</sup> Zu den Anbietern  
 2231 solcher Public Clouds gehören IT-Unternehmen, wie z. B. Google, Amazon, IBM, SAP oder die  
 2232 Deutsche Telekom. Neben diesen beiden Formen existiert auch eine Mischform von Public und  
 2233 Private Cloud, die Hybrid Cloud, bei der eine Nutzung von eigenen und fremden Ressourcen  
 2234 stattfindet.

2235 Eine der Besonderheiten des Cloud Computing liegt, je nach Angebot, in der zumeist flexiblen und  
 2236 grenzüberschreitenden Bereitstellung von Cloud Ressourcen durch eine Vielzahl von Beteiligten.

### 2237 Offene Fragen im Bereich des Datenschutzes und der Datensicherheit im Cloud Computing

2238 Die Auslagerung von Daten und Datenverarbeitung in die Cloud wirft datenschutz- und  
 2239 datensicherheitsrelevante Fragestellungen auf. Wenn Unternehmen ihre IT-Strukturen in eine Cloud  
 2240 auslagern, wird der Umfang der Datensicherheit und des Datenschutzes vom Anbieter der Cloud  
 2241 bestimmt.

#### 2242 a) Datensicherheit

2243 Das zentrale Problem hinsichtlich der Datensicherheit besteht darin, die Integrität  
 2244 (Datenveränderungen können erkannt werden) und Vertraulichkeit (nur Befugte können auf Daten  
 2245 zugreifen) der Datenverarbeitung und die Verfügbarkeit (Daten stehen in einem angemessenen  
 2246 Zeitraum zur Verfügung) zu gewährleisten.<sup>247</sup> Wie aktuell die Datensicherheit auf Netzwerk- und  
 2247 Datenebene in der Cloud gewährleistet wird, welche möglichen Probleme es gibt und inwieweit sich  
 2248 daraus politischer Handlungsbedarf ergibt, sollte auf Grund des Sachzusammenhangs von der  
 2249 Projektgruppe „Zugang, Struktur und Sicherheit im Netz“ geprüft werden.

#### 2250 b) Datenschutz

2251 Bei manchen Formen des Cloud Computing stellen sich besondere Herausforderungen, weil  
 2252 Rechtsgrundlagen wie Auftragsdatenverarbeitung oder Übermittlung das Cloud Computing nicht  
 2253 vollständig erfassen. Zudem werden damit typische, bereits bekannte Probleme des Outsourcings  
 2254 nicht nur potenziert, sondern sie gewinnen auch eine neue Qualität. Im Hinblick auf Rechenprozesse  
 2255 kann nicht mehr mit Bestimmtheit gesagt werden, auf welchen der oftmals weltweit verbundenen  
 2256 Server und damit bei welchen Beteiligten konkret welche Datenverarbeitungsprozesse vollzogen  
 2257 werden.

2258 Dies führt zu rechtlichen Unsicherheiten bei der Nutzung und dem Betreiben entsprechender  
 2259 Angebote.

2260

---

<sup>245</sup> Birk, Dominik/Wegener, Christoph: Über den Wolken: Cloud Computing im Überblick. DuD 2010, 641 (642).

<sup>246</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

<sup>247</sup> Heidrich, Jörg/Wegener, Christoph: Sichere Datenwolken – Cloud Computing und Datenschutz. MMR 2009, 803 (804).

2261 Gerade im Fall eines grenzüberschreitend angelegten Cloud Computing ergeben sich Fragen nach der  
 2262 Verantwortlichkeit sowie den Zugriffsmöglichkeiten Dritter. Um die Datenverarbeitung innerhalb der  
 2263 EU zu harmonisieren, wurde die Europäische Datenschutz- Richtlinie (DSRL) geschaffen. Da der  
 2264 Umstand einer grenzüberschreitenden Datenverarbeitung innerhalb des europäischen Binnenmarktes  
 2265 kein rechtliches Hindernis darstellen soll, dürfen gemäß Art. 1 Abs. 2 DSRL personenbeziehbare  
 2266 Daten im gesamten Europäischen Wirtschaftsraum (EWR) verarbeitet werden.<sup>248</sup> Für eine  
 2267 Anwendbarkeit nationalen Rechts kommt es gemäß Art. 4 Abs. 1 a, b DSRL deshalb darauf an, in  
 2268 welchem Mitgliedstaat die Daten verarbeitende Niederlassung ihren Sitz hat.<sup>249</sup> Damit auch  
 2269 Unternehmen, welche keine Niederlassung im Europäischen Wirtschaftsraum haben,  
 2270 personenbezogene Daten verarbeiten können, wurde in § 1 Abs. 5 S. 3 BDSG bestimmt, dass diese  
 2271 Unternehmen einen Datenschutzbeauftragten innerhalb der EU benennen, welcher dann für die  
 2272 Einhaltung der Richtlinien verantwortlich ist.

2273 Hinsichtlich der Verantwortlichkeit legt die DSRL in Art. 2 c fest, dass derjenige für den Datenschutz  
 2274 verantwortlich ist, der die Verarbeitung angeordnet hat. Dies ist grundsätzlich der Cloud-Nutzer und  
 2275 nicht der Anbieter.

2276 Insgesamt sind alle Datensätze, die nicht als personenbeziehbar gelten (§ 3 Abs. 1 BDSG) zur  
 2277 Verarbeitung in Clouds vollkommen unproblematisch. Datenschutzrelevant ist die Form der Nutzung  
 2278 des Cloud Computing nach deutschem Recht nur dann, wenn personenbezogene Daten verarbeitet  
 2279 werden (§ 3 BDSG). Da im Rahmen der Nutzung Cloud-basierter Dienstleistungen oft  
 2280 personenbezogene Daten auf dem System des Cloud-Anbieters gespeichert und auch verarbeitet  
 2281 werden und bei grenzüberschreitenden Systemen auch auf Speichermedien, die europa- bzw. sogar  
 2282 weltweit verteilt sind, stellt sich die Frage nach der Behandlung dieser Verlagerung der Daten in die  
 2283 Cloud. Aus rechtlicher Sicht kann es sich um eine Auftragsdatenverarbeitung i. S. d. § 11 BDSG  
 2284 handeln. Diese erfährt datenschutzrechtlich die Grenzen ihrer Zulässigkeit zum einen dort, wo dem  
 2285 Verantwortlichen (dem Nutzer der Cloud) durch den Dienstleister keine Angaben über Art und Ort der  
 2286 Verarbeitung und Sicherungsmaßnahmen gemacht werden. Zum anderen ist dies der Fall, wenn die  
 2287 datenverarbeitende Stelle außerhalb Deutschlands, eines Mitgliedstaates der EU oder des EWR liegt,  
 2288 in dem kein vergleichbares Datenschutzniveau existiert. In diesem Fall handelt es sich um eine  
 2289 Weitergabe an Dritte, wobei der Gesetzgeber unterstellt, dass bei derartigen  
 2290 Übermittlungskonstellationen besondere persönlichkeitsrechtliche Risiken entstehen, weil von der  
 2291 verantwortlichen Stelle, vom Betroffenen oder von den staatlichen Aufsichtsbehörden keine  
 2292 hinreichende Kontrolle der Datenverarbeitung möglich ist.<sup>250</sup>

2293 Hinzu kommt, dass die in § 11 Abs. 2 BDSG geforderte „sorgfältige“ Auswahl des Auftragnehmers  
 2294 „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und  
 2295 organisatorischen Maßnahmen“ in der Praxis nur schwer einzuhalten ist, da u. a. der Auftragnehmer  
 2296 dem Auftraggeber in der Regel nicht derart tiefgehende Einblicke in seine IT-Struktur gewährt.

2297 Je nach verwendetem Angebot (beispielsweise Verteilung der Daten auf mehrere weltweit verteilte  
 2298 Server) kann die Verlagerung der Daten in die Cloud zu einer Erhöhung der Gefahr von  
 2299 Zugriffsmöglichkeiten durch Dritte führen. Wichtig ist daher, dass der früher selbst  
 2300 Datenverarbeitende die Herrschaft über die Daten bewahrt und Kenntnis und Einfluss über die  
 2301 ergriffenen Sicherungsmaßnahmen hat.

---

<sup>248</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

<sup>249</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

<sup>250</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (682).

2302 Folgeproblem der Verlagerung und der Verteilung der Daten auf europa- und weltweite Server ist eine  
 2303 erschwerte Datenschutzkontrolle. Eine Datenschutzkontrolle durch die Aufsichtsbehörden ist auf das  
 2304 jeweilige Landesterritorium bzw. auf das Bundesterritorium begrenzt. Europaweit kann gegenseitig  
 2305 eine Amtshilfe der Aufsichtsbehörden erfolgen. Über das europäische Territorium hinaus sind  
 2306 koordinierte oder gemeinsame Kontrollen in Clouds mit Drittauslandsbezug praktisch nicht  
 2307 möglich.<sup>251</sup> Dies eröffnet datenschutzrechtlich verantwortlichen Stellen die Möglichkeit, sich  
 2308 Datenschutzkontrollen zu entziehen, in dem gezielt Clouds mit Drittlandsbezug genutzt werden.  
 2309 Daneben ist besonders problematisch, wenn die Datenverarbeitung in Staaten erfolgt, die nicht nur  
 2310 keinen ausreichenden Datenschutz gewährleisten, sondern auch bewusst und gezielt gegen  
 2311 Menschenrechte verstoßen und den Zugriff auf Daten in der Cloud zu politischer Überwachung und  
 2312 Verfolgung benutzen.<sup>252</sup>

2313 Der Ort, wo die Daten gespeichert und verarbeitet werden, spielt also eine zentrale Rolle. Dies zeigt  
 2314 sich auch für Daten, welche für Steuerzwecke benötigt werden. Diese dürfen gem. § 146 Abs. 2 S. 1  
 2315 Abgabenordnung (AO) nur im Inland gespeichert werden. Auch hier stellt sich das Problem bei  
 2316 länderübergreifenden Netzen und der Information, in welchem Land die Daten gelagert und  
 2317 verarbeitet werden. Nach § 146 Abs. 2 a AO kann die zuständige Finanzbehörde bewilligen, dass die  
 2318 Finanzdokumente auch außerhalb der EU oder des EWR archiviert werden.<sup>253</sup> Auch hier könnten die  
 2319 Steuerermittlungsbehörden vor Probleme gestellt werden, weil nicht ohne weiteres ein Zugriff auf die  
 2320 Daten erfolgen kann.

2321 Im Ergebnis ist festzuhalten, dass es noch offene datenschutzrechtliche Fragen gibt, wenn  
 2322 personenbezogene Daten in die Cloud verlagert werden. Dies kann die Nutzung, aber auch die sich  
 2323 bietenden Möglichkeiten und Innovationen des Cloud Computing einschränken. Bisher können  
 2324 datenschutzrechtliche Erfordernisse nur durch besonders umfangreiche und detaillierte  
 2325 Vertragsvereinbarungen gewährleistet werden. Für die Ermittlung von Straftaten und  
 2326 Ordnungswidrigkeiten stellt die Speicherung von Daten in der Cloud dann ein Problem dar, wenn  
 2327 durch die Art und den Ort der Datenverarbeitung ein Zugriff für die Ermittlungsbehörden nicht  
 2328 möglich ist.<sup>254</sup> Im Inland stehen Staatsanwaltschaften und auf Anordnung auch ihren  
 2329 Ermittlungspersonen gemäß § 110 Abs. 3 StPO seit dem Jahr 2008 entsprechende Befugnisse auf  
 2330 Durchsicht von Speichermedien zu.

2331 2.3.4 „Verfallsdaten“ im Internet, regelmäßig erneuerbare Zustimmungspflicht

2332 Im Kontext des Internet bereitet die Rückgängigmachung einer einmal gewollten Datennutzung oder  
 2333 auch Datenveröffentlichung bei geänderter Einschätzung besondere Schwierigkeiten.

2334 Schwierig stellt sich die Lage bei veröffentlichten Daten dar. Auf Grund der einfachen  
 2335 Vervielfältigung digitaler Daten im Internet ist wegen der technischen Gegebenheiten davon  
 2336 auszugehen, dass einmal veröffentlichte Daten nicht mehr „zurückzuholen“ sind. Selbst wenn es  
 2337 gelingt, die weitere Verwendung bzw. Veröffentlichung an einer bestimmten Stelle zu unterbinden, ist  
 2338 bei Daten anzunehmen, dass sie an anderer Stelle bereits dupliziert wurden.

---

<sup>251</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (684).

<sup>252</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (684).

<sup>253</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

<sup>254</sup> Weichert, Thilo: Cloud Computing und Datenschutz. DuD 2010, 679 (680).

2339 Seit einigen Jahren wird mit zunehmender Bedeutung des Internets auch die Diskussion über ein  
 2340 „Recht auf Vergessen an den eigenen Daten“ geführt. Allerdings sind die hierfür in der Diskussion  
 2341 verwendeten Begrifflichkeiten noch sehr unterschiedlich. So wird neben dem „Recht auf  
 2342 Vergessen“<sup>255</sup>, beispielsweise auch vom „programmierten Vergessen“<sup>256</sup>, „Verfallsdaten“ oder dem  
 2343 „digitalen Radiergummi“<sup>257</sup> gesprochen. Die unterschiedlich verwendeten Terminologien haben  
 2344 teilweise nicht nur unterschiedliche Argumentationsansätze, sondern auch eine sehr unterschiedliche  
 2345 Reichweite. Auch wenn sie daher nicht vollständig als Synonym für das „Recht auf Vergessen“  
 2346 verwendet werden sollten, haben sie einen gemeinsamen Kerngedanken. Demnach soll der Nutzer des  
 2347 Internets mit Hilfe einer oder mehrerer technischen Lösungen selbst darüber bestimmen können, wie  
 2348 lange seine personenbezogenen Daten im Internet gespeichert bleiben sollen bzw. nach welcher Zeit  
 2349 der „menschliche Vorgang“ des Vergessens beginnen soll. Er kann im Idealfall bereits mit dem  
 2350 Einstellen der personenbezogenen Daten festlegen, dass eine (vollständige) Löschung der Daten an  
 2351 einem zuvor bestimmten Datum in der Zukunft erfolgen soll. Auf Grund der nahezu unbegrenzten  
 2352 Speicher- und Vervielfältigungsmöglichkeiten des Internets stellt dies die bisherigen technischen  
 2353 Gegebenheiten vor besondere Anforderungen.

2354 Bereits jetzt existieren einzelne webbasierte Anwendungen, die dem Nutzer ermöglichen sollen, die  
 2355 Abrufbarkeit der Daten zeitlich zu begrenzen. Allerdings fehlt es bisher an einer Gesamtlösung für  
 2356 alle Bereiche des Internets und insbesondere für die besonders datenintensiven sozialen Netzwerke.  
 2357 Erste technische Ansätze hierfür wurden bereits vor zwei Jahren in den USA entwickelt. Die  
 2358 University of Washington programmierte eine entsprechende Technik für den Verfall der eigenen  
 2359 personenbezogenen Daten, die auch auf soziale Netzwerke angewendet werden kann.<sup>258</sup> Die  
 2360 Universität des Saarlandes stellte im vergangenen Jahr ein vergleichbares Produkt vor.<sup>259</sup> Beide  
 2361 Techniken stehen jedoch noch am Anfang der Entwicklung und verhindern keineswegs die  
 2362 Möglichkeit der Vervielfältigung von eingestellten personenbezogenen Daten (insbesondere Bildern).  
 2363 Ein „Recht auf Vergessen“ kann somit aus technischer Sicht zum jetzigen Zeitpunkt nicht  
 2364 durchgesetzt oder gewährleistet werden.

2365 Ungehindert dessen, hat die politische und rechtliche Diskussion um ein „Recht auf Vergessen“ in den  
 2366 letzten Monaten weiter an Fahrt gewonnen. Auch die EU-Kommission hat das „Recht auf Vergessen“  
 2367 als prüfungswerten Punkt für eine Überarbeitung der Datenschutzrichtlinie 95/46/EG mit in die  
 2368 bevorstehende Konsultation aufgenommen.<sup>260</sup>

---

255 Mayer-Schönberger, Viktor: Delete: The Virtue of Forgetting in the Digital Age. 2009. Rosen, Jeffrey: 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).

256 Bull, Hans Peter: Persönlichkeitsschutz im Internet : Reformeifer mit neuen Ansätzen. NVwZ 2011, 257 (260).

257 Vgl. dazu die Rede des ehemaligen Bundesinnenministers Dr. Thomas de Maizière zu den Grundlagen für eine gemeinsame Netzpolitik der Zukunft. Berlin, 22. Juni 2010. Thesenpapier online abrufbar unter: [http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED\\_Verwaltung/Informationsgesellschaft/thesen\\_netzpolitik.pdf?\\_\\_blob=publicationFile](http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/thesen_netzpolitik.pdf?__blob=publicationFile) (zuletzt aufgerufen am 7. April 2011).

258 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).

259 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).

260 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.

2369 2.3.5 „Privacy by design“ („privacy by design“ / „privacy by default“)

2370 „Privacy by design“ beschreibt den Ansatz, bereits bei der Konzeption und Ausgestaltung von  
 2371 Technologien den Datenschutz mit einzubeziehen.<sup>261</sup> Nachträglich möglicherweise auftretende  
 2372 Schwierigkeiten bei der Einhaltung der gesetzlichen Vorgaben der Datenschutzgesetze können so  
 2373 bereits im Vorfeld vermieden und verhindert werden. Eine Korrektur solcher Schwierigkeiten im  
 2374 Nachhinein ist oft nur sehr mühsam und mit viel Aufwand zu bewältigen.

2375 In einer Zeit, in der zunehmend auch technische Geräte des Alltags beginnen, personenbezogene  
 2376 Daten zu erfassen und über das Internet zu kommunizieren, werden die Herausforderungen an die  
 2377 Sicherung des Rechts auf informationelle Selbstbestimmung und den Vollzug des geltenden  
 2378 Datenschutzrechts wachsen.

2379 Die konsequente und frühzeitige Umsetzung von „privacy by design“ stellt auch eine Möglichkeit zur  
 2380 Problemlösung im Bereich der Einwilligung nach § 4 BDSG dar. Elemente von „privacy by design“  
 2381 können beispielsweise eine grundsätzliche Verschlüsselung von Daten, die Löschung von Daten nach  
 2382 erfolgter Funktionserfüllung oder technische Vorkehrungen zur Einhaltung des  
 2383 Zweckbindungsgrundsatzes sein.<sup>262</sup> Sie unterstützen damit den Nutzer technischer Geräte und helfen  
 2384 ihm, sein gesetzlich gewährleistetes Recht auf informationelle Selbstbestimmung auch tatsächlich  
 2385 ausüben zu können. Gleichzeitig konkretisieren sie auf diese Weise das Gebot der Datensparsamkeit  
 2386 und Datenvermeidung.

2387 In Ergänzung zu „privacy by design“ stellt das Prinzip des „privacy by default“ eine wichtige Option  
 2388 zur Gestaltung von elektronischen Diensten und Anwendungen wie etwa sozialen Netzwerken oder so  
 2389 genannten „location based services“ dar. Nach diesem Prinzip gestaltete Dienste sehen ab dem ersten  
 2390 Moment der Nutzung die jeweils höchstmöglichen nutzbaren Datenschutzeinstellungen vor.  
 2391 Nutzerinnen und Nutzer können dann mittels eines so genannten „opt-out“ die Einstellungen des  
 2392 Datenschutzniveaus nach ihren Vorstellungen anpassen. Eine konsequente Anwendung des Prinzips  
 2393 „privacy by default“ erscheint gerade angesichts der Vielfalt der einzelnen technischen Einstellungen  
 2394 vieler webbasierter Angebote und der oftmals nicht leicht erkennbaren Konsequenzen sinnvoll.

2395 „privacy by design“ und „privacy by default“ orientieren sich an den Vorgaben der Datenvermeidung  
 2396 und Datensparsamkeit (§ 3e BDSG) und damit an einer zentralen Leitlinie des Datenschutzrechts. Sie  
 2397 sind als immanente Grundprinzipien geeignet, den gegenwärtigen und zukünftigen Herausforderungen  
 2398 für einen Datenschutz wirksam und effektiv zu begegnen.

2399 2.3.6 Datenweitergabe und -handel

2400 Personenbezogene Daten (wie beispielsweise Adress- oder Kontaktdaten oder auch Daten zum  
 2401 Einkaufsverhalten) sind Gegenstand von Transaktionen. Sie werden zwischen Unternehmen verkauft,  
 2402 vermietet oder aber getauscht.

2403

---

261Schaar, Peter : Privacy by Design. Identity in the Information Society 2010, 267-274.

262Unterrichtung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung. Technikfolgenabschätzung (TA) / Zukunftsreport – Ubiquitäres Computing vom 6. Januar 2010, BT-Drs. 17/405, S. 126.

2404 Neben legalem Handel mit Daten kommt es im und über das Internet zu einem illegalen Handel mit  
 2405 personenbezogenen Daten (national wie international). Dieser illegale Handel umfasst sowohl Daten,  
 2406 die unter bestimmten Voraussetzungen gehandelt werden dürfen (z. B. Adress- oder Daten zum  
 2407 Einkaufsverhalten), als auch Daten, deren Handel in jedem Fall unzulässig ist (z. B. Passwörter zu E-  
 2408 Mailkonten).

2409 Darüber hinaus wurde in der Vergangenheit aber auch eine „Grauzone“ im Bereich der  
 2410 Datenweitergabe und des Datenhandels festgestellt.<sup>263</sup> Diese Grauzone erstreckte sich insbesondere  
 2411 auf die Bereiche des E-Mail- und Telefon-Marketings, die beide nicht unmittelbar unter das  
 2412 Bundesdatenschutzgesetz fallen, sondern vornehmlich dem Telemediengesetz (vgl. § 6 TMG), dem  
 2413 Telekommunikationsgesetz (vgl. § 95 TKG) und dem Gesetz gegen den unlauteren Wettbewerb (vgl.  
 2414 § 7 Abs. 2 Nr. 2, 3 UWG) unterliegen. Aber auch bei anderen Angeboten, die dem  
 2415 Bundesdatenschutzgesetz unmittelbar unterliegen, fällt eine Abgrenzung zwischen zulässiger  
 2416 Handlung und möglichem Verstoß gegen datenschutzrechtliche Vorschriften nicht immer leicht. Dies  
 2417 gilt insbesondere für die Fälle, in denen das Geschäftsmodell auch darauf abzielt, personenbezogene  
 2418 Daten von möglichst vielen Nutzern zu erheben und ggf. an Dritte weiterzugeben. Aber auch die in  
 2419 der Praxis beliebte Form der Freundschaftswerbung wirft immer wieder schwierige  
 2420 datenschutzrechtliche Fragen auf.

2421 Der Bereich der Datenweitergabe und des Datenhandels im Bundesdatenschutzgesetz wurde im Jahr  
 2422 2009 umfangreich novelliert. Seitdem schreibt das Bundesdatenschutzgesetz vor, dass  
 2423 personenbezogene Daten wie Adressen grundsätzlich nur dann an andere weitergegeben werden  
 2424 dürfen, wenn der Kunde hierzu vorher eingewilligt hat (so genanntes Opt-in-Verfahren). Eine  
 2425 Ausnahme von diesem Verfahren bildet das so genannte Listenprivileg, das das  
 2426 Bundesdatenschutzgesetz in § 28 Abs. 2 Nr. 1b BDSG bereits vor der letzten Novellierung der  
 2427 Werbewirtschaft beim Versand von (Papier-)Werbung einräumte. Das Listenprivileg erlaubt die  
 2428 Übermittlung oder Nutzung von Daten, sofern es sich um listenmäßig zusammengefasste  
 2429 personenbezogene Daten über Angehörige einer Personengruppe handelt, die sich auf Beruf, Name,  
 2430 Titel, akademischen Grad, Anschrift, Geburtsjahr und Angabe über die Zugehörigkeit des Betroffenen  
 2431 zu einer bestimmten Personengruppe (z. B. männliche Studienanfänger unter 25 Jahren in Berlin)  
 2432 beschränken und dabei kein überwiegendes schutzwürdiges Interesse des Betroffenen verletzt wird.

2433 Mit der letzten Novellierung des Bundesdatenschutzgesetzes neu eingeführt wurde die Regelung, dass  
 2434 Betroffene über die Herkunft ihrer Adressdaten auf dem Werbemittel mit Klarnamen und in  
 2435 drucktechnisch deutlicher Gestaltung informiert werden müssen (vgl. § 28 Abs. 3. S. 4 BDSG). Die  
 2436 Verwendung von Listendaten ist demnach erlaubt, wenn dies für die Bewerbung eigener Angebote der  
 2437 verantwortlichen Stelle erforderlich ist.

2438 Mit der letzten Novellierung des Bundesdatenschutzgesetzes sind zudem einige Tatbestände  
 2439 hinzugekommen, die die Werbung für eigene Angebote mit zuvor erhobenen personenbezogenen  
 2440 Daten erleichtern. Die datenerhebende Stelle muss hierfür diese Listendaten beim Verbraucher im  
 2441 Rahmen des Vertragsschlusses bzw. im Rahmen einer Anfrage als Interessent erhoben haben.  
 2442 Ergänzend können die Listendaten auch aus allgemein zugänglichen Adress-, Rufnummern-,  
 2443 Branchen- oder vergleichbaren Verzeichnissen erhoben worden sein. Um Profile für eine  
 2444 individualisierte Werbung erstellen zu können, darf die verantwortliche Stelle für die Bewerbung

---

<sup>263</sup> 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](https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/19_DIB/DIB_2009.pdf) (zuletzt aufgerufen am 7. April 2011).

2445 eigener Angebote zu den Listendaten weitere Daten hinzufügen, wenn diese personenbezogenen  
2446 Daten ebenfalls zuvor rechtmäßig erhoben wurden.

2447 Einzelne Fallgestaltungen sehen wie folgt aus:

2448 1. So genanntes Lettershop-Verfahren

2449 Unternehmen nutzen zur Neukundengewinnung Kundendaten, die von anderen Unternehmen für  
2450 Werbezwecke vermietet werden. In diesem Fall beauftragt die verantwortliche Stelle – das  
2451 Unternehmen, das Kundendaten etwa im Rahmen einer Geschäftsbeziehung erworben hat – einen  
2452 Dienstleister mit der Nutzung seiner Kundendaten zur Erstellung eines Werbeschreibens. Das zu  
2453 versendende Werbematerial wird dann von dem Unternehmen zur Verfügung gestellt, das die Daten  
2454 zur Neukundengewinnung nutzen möchte.

2455 Das dargestellte Verfahren ist mit den Vorgaben des Bundesdatenschutzgesetzes vereinbar, wenn das  
2456 Unternehmen (verantwortliche Stelle), welches seine erworbenen Kundendaten für die Bewerbung  
2457 von Produkten oder Dienstleistungen anderer Unternehmen zur Verfügung gestellt hat, für den  
2458 Empfänger eindeutig erkennbar ist. Dies ist der Fall, wenn die Nennung des Unternehmens im  
2459 Klartext erfolgt und der Empfänger so das Unternehmen ohne Zweifel und mit seinen Kenntnissen  
2460 und Möglichkeiten identifizieren kann.

2461 2. Übermittlung von Kundendaten (Kauf oder Tausch)

2462 Beim Kauf oder Tausch von Kundendaten findet eine Übermittlung der Kundendaten von einem zu  
2463 einem anderen Unternehmen statt. Das empfangende Unternehmen erhält die Kundendaten zur  
2464 eigenen Verwendung und kann diese fortan für eigene werbliche Zwecke nutzen. Erfolgte die  
2465 Übermittlung der Kundendaten ohne vorherige Einwilligung der Kunden ist der Vorgang nur dann  
2466 rechtlich zulässig, wenn die gesetzlichen Informations-, Dokumentations- und Transparenzpflichten  
2467 eingehalten werden.

2468 Die gesetzliche Informationspflicht ist eingehalten, wenn der Kunde bei der Datenerhebung auf den  
2469 Verwendungszweck eines Kaufs oder Tausches der erhobenen Kundendaten hingewiesen wurde. Zu  
2470 beachten ist zudem, dass ein Kauf oder Tausch nur innerhalb der Gruppe möglich ist, die dem Kunden  
2471 bei der Datenerhebung genannt wurde. Der gesetzlichen Dokumentationspflicht wird entsprochen,  
2472 wenn die übermittelnde Stelle für den Zeitraum von zwei Jahren den Empfänger der Kundendaten  
2473 speichert. Gleichzeitig muss der Empfänger der Kundendaten den Übermittler und den zulässigen  
2474 Verwendungszweck für ebenfalls mindestens zwei Jahre speichern.

2475 Ebenso wie im oben genannten Lettershop-Verfahren muss gegenüber dem Empfänger der Werbung  
2476 die Quelle der Adresswerbung genannt werden. Ausfluss der gesetzlichen Transparenzpflicht ist  
2477 zudem, dass gegenüber dem Empfänger der Werbung das Unternehmen zu benennen ist, welches  
2478 erstmals die Kundendaten erhoben hat.

2479 Die Übermittlung von Kundendaten zum Zwecke der Werbung ist somit letztlich, wie oben bereits  
2480 dargestellt, auf die so genannten Listendaten begrenzt. Will ein Unternehmen darüber hinausgehende  
2481 Daten übermitteln, muss eine Einwilligung des Betroffenen vorliegen.

2482 3. Weitere Sonderfälle

2483 Mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 wurden zwei weitere Sonderfälle  
2484 gesetzlich für zulässig erklärt. Hierzu gehört die Nutzung und Übermittlung von Listendaten zur  
2485 Bewerbung von Produkten und Dienstleistungen im gewerblichen Bereich. Allerdings erstreckt sich  
2486 die gesetzliche Privilegierung auch auf Funktionsträger in Unternehmen (z. B. Abteilungsleiter



- 2487 Einkauf). Abgrenzungsmerkmal ist demnach, dass die Werbung im Hinblick auf die berufliche  
 2488 Tätigkeit des Betroffenen erfolgen muss. Zudem darf nicht die Privatadresse, sondern es muss die  
 2489 berufliche Anschrift des Betroffenen verwendet werden. Fallen beide Adressen zusammen, kann  
 2490 trotzdem von der gesetzlichen Privilegierung Gebrauch gemacht werden.
- 2491 Die Ausnahmeregelung für den gewerblichen Bereich erfasst sowohl die Vermietung von Listendaten  
 2492 als auch den Kauf oder Tausch der Daten. Gegenüber den oben genannten Regelungen besteht beim  
 2493 Vorliegen einer gewerblichen Ansprache keine Pflicht, die ursprüngliche Quelle der Daten zu  
 2494 eröffnen. Auch die dargestellten Dokumentationspflichten müssen nicht eingehalten werden. Zudem  
 2495 ist für das werbende Unternehmen auch ein Rückgriff auf allgemein zugängliche Quellen zulässig.  
 2496 Die Adressdaten können somit beispielsweise auch über das Internet unmittelbar erhoben werden.
- 2497 Eine weitere Ausnahme bei der Verwendung von Listendaten gilt, wenn steuerbegünstigte  
 2498 Organisationen für Spenden werben wollen. Auch bei diesem Fall bedarf es keiner Pflicht zur Angabe  
 2499 der Quelle, bei der erstmals die Daten erhoben wurden.
- 2500 2.3.7 Spannungsfeld Datenschutz und Wettbewerbsbedingungen am Beispiel sozialer Netzwerke
- 2501 Eine große datenschutzrechtliche Herausforderung im Internet sind inzwischen die sozialen  
 2502 Netzwerke, die in jüngerer Zeit die Nutzung der Möglichkeiten des Internet zunehmend prägen.  
 2503 Betreiber sozialer Netzwerke haben ihren Sitz derzeit sowohl außerhalb des europäischen  
 2504 Wirtschaftsraums (EWR) als auch innerhalb. Es stellen sich daher zunächst die grundsätzlichen  
 2505 Fragen der Anwendbarkeit und Durchsetzbarkeit nationalen oder aber europäischen  
 2506 Datenschutzrechts.<sup>264</sup>
- 2507 Bei sozialen Netzwerken konnte festgestellt werden, dass besonders bei Änderungen des angebotenen  
 2508 Dienstes unterschiedliche datenschutzrechtliche Regelungen zur Anwendung kommen. Nach  
 2509 europäischem Datenschutzrecht muss beispielsweise jede Änderung eines Dienstangebots, bei der  
 2510 personenbezogene Daten betroffen sind, vom Nutzer bestätigt werden. Das umgekehrte Verfahren (so  
 2511 genanntes Opt-out) wird in den USA angewendet. Dieses führt zu weniger Rückläufern und  
 2512 ermöglicht damit eine stärkere Durchsetzung des eigenen Angebotes auf dem Markt.<sup>265</sup>
- 2513 Hinzu kommt, dass derzeit Nutzer vor der Eröffnung eines Kontos bei sozialen Netzwerken nicht in  
 2514 vergleichbar gut verständlicher Form über die Möglichkeiten der Datenverwendung für den Betreiber  
 2515 informiert werden. Zwar gibt es beispielsweise bei Facebook zahlreiche differenzierte Möglichkeiten,  
 2516 unter den Kontoeinstellungen oder Privatsphäre-Einstellungen den Zugriff auf Daten durch Dritte  
 2517 einzuschränken. Aber auf diese Möglichkeiten wird der Nutzer bei Einrichtung des Kontos nicht  
 2518 hingewiesen. Hier ist die datenschutzrechtliche Gefährdung höher als bei einer „Opt-out“-Lösung, bei  
 2519 der der Nutzer bei Kontoeröffnung über die die Möglichkeit der Einstellungen informiert wird. Eine  
 2520 zusätzliche und besonders brisante Dimension kommt dann noch hinzu, wenn die Datenbestände  
 2521 sozialer Netzwerke mit anderen Kommunikationsformen datenmäßig miteinander kombiniert werden  
 2522 (etwa zwischen Facebook und Skype), ohne dass sich die Nutzer dessen auch nur bewusst wären.

---

<sup>264</sup> Vgl. Darstellung in 2.1.9.

<sup>265</sup> 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](http://www.bundestag.de/internetenquete/dokumentation/2010/Sitzungen/20100705/A-Drs_17_24_004-D_-_Stellungnahme_Hinrichs.pdf) (zuletzt aufgerufen am 7. April 2011).

2523 2.3.8 Datenschutz als Standortfaktor

2524 Datenschutz ist angesichts der internationalen Reichweite für viele Dienste ein wesentliches  
2525 Wettbewerbselement und damit auch ein Standortfaktor einer innovativen und dynamischen  
2526 Internetwirtschaft in Deutschland.

2527 Dabei bestehen hier durchaus zwei gegensätzliche Argumentationen:

2528 Vertreten wird die Auffassung, striktere Datenschutzregeln seien hinderlich oder jedenfalls  
2529 kostentreibend, wenn es darum gehe, mit neuen Diensten Marktanteile zu gewinnen. Für  
2530 Unternehmen, die im internationalen Wettbewerb stehen, könne ein niedrigeres Datenschutzniveau  
2531 sowohl zu einer Vereinfachung der Produktgestaltung als auch zu einer Erleichterung bei den Kosten  
2532 führen.

2533 Auf der anderen Seite wird vertreten, ein hohes Sicherheits- und Datenschutzniveau könne durch  
2534 zusätzliches Kundenvertrauen zu einem positiven Unterscheidungsmerkmal im Wettbewerb werden.  
2535 Wie bereits festgestellt, besteht durchaus ein Bewusstsein für die Relevanz hoher Sicherheits- und  
2536 Datenschutzstandards und damit eine Nachfrage nach entsprechend ausgestalteten Produkten. Gelingt  
2537 es also, ohne relevante Einbußen der sonstigen Wettbewerbsfähigkeit, hier ein Mehr gegenüber  
2538 internationalen Diensten anzubieten, kann das hohe deutsche Schutzniveau auch als Standortvorteil  
2539 verstanden und positioniert werden.

2540 Von in Deutschland tätigen Unternehmen wird der Datenschutz aber auch deswegen zunehmend als  
2541 negativer Standortfaktor wahrgenommen, weil sowohl die föderale Struktur der Datenschutzaufsicht  
2542 als auch die Vielzahl bereichsspezifischer Regelungen eine einheitliche Anwendung und Auslegung  
2543 innerhalb Deutschlands erschweren.

2544 So hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder festgestellt: „Eine  
2545 Vielzahl von Spezialregelungen, die das Bundesdatenschutzgesetz (BDSG) ganz oder teilweise  
2546 überlagern und verdrängen, haben das Recht für Anwenderinnen und Anwender wie Betroffene  
2547 unübersichtlich und unverständlich gemacht.“<sup>266</sup>

2548 2.3.9 Selbstverpflichtungen und Selbstregulierungen der Internetwirtschaft

2549 Staatliche Aufsicht ist unverzichtbar, gleichzeitig muss man aber anerkennen, dass sie systembedingt  
2550 auch an Grenzen stößt. Selbst bei großer Sachnähe und einer hinreichenden personellen Ausstattung  
2551 werden sich Behörden schwer tun, alle sich ständig wandelnden Phänomene im Internet in ihrer  
2552 technischen Komplexität und Dynamik wirksam zu erfassen und eine hinreichende Aufsicht zu  
2553 gewährleisten. Schließlich ergibt sich angesichts der Vielzahl der im Netz angebotenen Dienste  
2554 unweigerlich ein Ressourcenproblem, das eine effektive, hinreichend enge Kontrolle der tatsächlichen  
2555 Praxis bei den verantwortlichen Stellen erschwert.

2556 Diese potentiellen Defizite staatlicher Aufsicht könnten durch eine Einbindung der Unternehmen in  
2557 die Festsetzung und Durchsetzung von Datenschutzstandards ausgeglichen werden.

---

<sup>266</sup>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.  
[http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktetpapierBroschuere.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktetpapierBroschuere.pdf?__blob=publicationFile) (zuletzt aufgerufen am: 22. März 2011).

2558 Darüber hinaus können Selbstverpflichtungen der Internetwirtschaft in Zukunft auch im Datenschutz  
 2559 eine wichtige Ergänzung zu gesetzlichen Vorgaben darstellen. Gerade in einem sich schnell  
 2560 wandelnden Technikumfeld, aus dem sich ständig neue Geschäftsmodelle entwickeln, kann mit  
 2561 diesem Instrument flexibel auf Veränderungen reagiert und auf spezielle Bedürfnisse in einzelnen  
 2562 Anwendungsfällen eingegangen werden. Während mit der Gesetzgebung abstrakt-generelle  
 2563 Wertungen und Vorgaben von einer gewissen Nachhaltigkeit geschaffen werden müssen, kann mit  
 2564 Selbstverpflichtungen kurzfristiger und detaillierter eingegriffen werden, um auf Entwicklungen in  
 2565 einzelnen Geschäftsfeldern zu reagieren.

2566 Dabei sind verschiedene formale und inhaltliche Ausgestaltungen denkbar, die von einseitigen  
 2567 Verpflichtungserklärungen der Verantwortlichen bis zu einer gesetzlich eingebundenen regulierten  
 2568 Selbstregulierung gehen. Bereits im geltenden BDSG stellt § 38a einen rechtlichen Anknüpfungspunkt  
 2569 dar, über den Selbstverpflichtungen in den gesetzlichen Rahmen integriert werden können. Bislang  
 2570 wurde dieses Instrument kaum genutzt. Jüngste Beispiele wie der Datenschutz-Kodex für  
 2571 Geodatendienste<sup>267</sup> könnten jedoch der Anfang einer deutlich intensiveren Nutzung dieses  
 2572 Regulierungsinstruments sein. Diese Entwicklung ist zu beobachten und gegebenenfalls durch  
 2573 entsprechende Ergänzung des Rechtsrahmens zu fördern. Auch die EU-Kommission hat in ihrer  
 2574 Mitteilung angekündigt, „Möglichkeiten zur verstärkten Förderung von Initiativen zur  
 2575 Selbstregulierung zu prüfen, darunter die aktive Förderung von Verhaltenskodizes.“<sup>268</sup>

2576 So wird zurzeit auf europäischer Ebene auch die Einführung von Selbstregulierungsmechanismen für  
 2577 angemessene Formen der Datenerhebung und -verwendung im Zusammenhang mit Online-Werbung  
 2578 erörtert. Dies könnte ein wichtiger Schritt sein, um auch in diesem Bereich zu mehr Transparenz und  
 2579 Selbstbestimmungsmöglichkeiten für die Nutzer zu kommen. Denn klare Kennzeichnungen von  
 2580 verpflichtungskonformen Angeboten bieten dem Nutzer eine zusätzliche Transparenz und eine  
 2581 einfache Orientierungsmöglichkeit.

2582 2.3.10 Übertragbarkeit der regulierten Selbstregulierung auf den Bereich des Datenschutzes

2583 Insbesondere im Jugendmedienschutz hat sich neben staatlicher Regulierung und reiner  
 2584 Selbstregulierung eine Form der so genannten „regulierten Selbstregulierung“ bzw. Co-Regulierung  
 2585 entwickelt. Sie ist dadurch gekennzeichnet, dass die staatliche Hand einen gesetzlichen Rahmen  
 2586 schafft, innerhalb dessen die Selbstkontrolle der Wirtschaft in eigener Verantwortung die  
 2587 Ausgestaltung und Anwendung von Verhaltensgrundsätzen organisieren kann. Sie unterliegt dabei  
 2588 aber wiederum einer übergeordneten Erfolgskontrolle durch die staatliche Hand, die im Falle von  
 2589 Fehlentwicklungen bzw. Verstößen gegen den vorgegebenen Rahmen ihrerseits durchgreifen kann.  
 2590 Der Erfolg dieses Modells im Jugendmedienschutz hängt wesentlich damit zusammen, dass es in  
 2591 diesem Bereich einen Beurteilungsspielraum bei der Bewertung der der Kontrolle unterliegenden  
 2592 Medieninhalte gibt. Für die Einschätzung der potentiellen Entwicklungsbeeinträchtigung und der  
 2593 damit verbundenen Altersklassifizierung existieren keine gesetzlichen Vorgaben, sodass diese rein  
 2594 tatsächliche Beurteilung am besten von möglichst sachnahen Personen durchgeführt werden sollte.

2595

---

<sup>267</sup> BITKOM. Datenschutzkodex für Geodatendienste - Entwurf. Dezember 2010.

[http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/rote\\_linie\\_kodex.pdf?\\_\\_blob=publicationFile](http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/rote_linie_kodex.pdf?__blob=publicationFile) (zuletzt aufgerufen am 7. April 2011).

<sup>268</sup> 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).

2596 Einen solchen Beurteilungsspielraum kennt das viel stärker von Rechts- als von Tatsachenfragen  
 2597 geprägte Datenschutzrecht allerdings nicht. Hier bestehen bereits aus verfassungsrechtlichen Gründen  
 2598 durchgehende gesetzliche Regelungen, deren Auslegung zwar im Einzelfall schwierig und auch  
 2599 streitig sein kann, die aber trotzdem mit einem vollumfänglichen Geltungsanspruch ausgestattet sind.  
 2600 Es erscheint daher fraglich, ob es im Datenschutz einen dem Jugendmedienschutz vergleichbaren  
 2601 Spielraum für die sachliche Ausfüllung von Tatbestandselementen gibt, die das Modell einer  
 2602 „regulierten Selbstregulierung“ tragen könnten. Es liegt näher, dass sich in diesem Bereich angesichts  
 2603 des voll umfänglichen Geltungsanspruchs staatlicher Regulierung nur ein Nebeneinander, aber eben  
 2604 kein ineinander verwobenes Miteinander von staatlicher Regulierung einerseits und Selbstregulierung  
 2605 der Wirtschaft andererseits entwickeln kann.

### 2606 2.3.11 Schadensersatzansprüche im Datenschutzrecht

2607 Bei der Verletzung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. mit Art. 1  
 2608 Abs. 1 GG tritt selten ein materieller, sondern ein immaterieller Schaden ein. Dem Betroffenen steht  
 2609 nach § 7 BDSG (in Umsetzung von Art. 23 DSRL) gegenüber der verantwortlichen (nicht-  
 2610 öffentlichen und öffentlichen) Stelle ein Schadensersatzanspruch zu, sofern personenbezogene Daten  
 2611 unzulässig oder unrichtig erhoben, verarbeitet oder genutzt wurden und ein Schaden entstanden ist.  
 2612 Die fehlerhafte Datenverarbeitung muss ursächlich für den Schaden geworden und i. S. v. § 276 BGB  
 2613 schuldhaft, d. h. durch vorsätzlichen oder fahrlässigen Umgang erfolgt sein.<sup>269</sup> Dabei wird zunächst  
 2614 schuldhaftes Handeln durch die verantwortliche Stelle unterstellt, die nach § 7 S. 2 BDSG jedoch den  
 2615 Entlastungsbeweis führen kann und damit die Möglichkeit zur Exkulpation hat. Der zugefügte  
 2616 Schaden muss eine materielle Beeinträchtigung des Betroffenen zur Folge haben, d. h. ein sogenannter  
 2617 Vermögensschaden muss vorliegen, der konkret beziffert werden muss.

2618 Nach § 8 Abs. 1 BDSG (ebenfalls in Umsetzung von Art. 23 DSRL) besteht bei automatisierter  
 2619 Datenverarbeitung durch öffentliche Stellen für den Betroffenen ein Schadensersatzanspruch bei  
 2620 unzulässiger oder unrichtiger Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten.  
 2621 Diese verschuldensunabhängige Gefährdungshaftung soll die „typische Automationsgefährdung“  
 2622 abdecken, also Schäden, die durch automatisierte Verfahren eingetreten sind.<sup>270</sup> Es besteht keine  
 2623 Exkulpationsmöglichkeit für die datenverarbeitende Stelle. Ersetzt werden nicht nur materielle,  
 2624 sondern auch immaterielle Schäden, sofern eine schwere Verletzung des Persönlichkeitsrechts geltend  
 2625 gemacht werden kann.

2626 Das Verhältnis der gesetzlichen Ansprüche von §§ 7, 8 BDSG zu dem deliktischen  
 2627 Schadensersatzanspruch nach § 823 BGB ist bisher jedoch noch umstritten. Hierzu werden  
 2628 verschiedene Auffassungen vertreten, die jedoch im Ergebnis mehrheitlich auch einen Ersatz von  
 2629 immateriellen Schäden bei einer schwerwiegenden Verletzung aufgrund eines unzulässigen oder  
 2630 unrichtigen Datenumgangs annehmen.<sup>271</sup> Hierzu gibt es jedoch noch keine Rechtsprechung.

2631 Bei öffentlichen Stellen kann sich eine über §§ 7, 8 BDSG hinausgehende Haftung im Rahmen  
 2632 hoheitlicher Tätigkeit nach Art. 34 GG i. V. m. § 839 BGB oder im fiskalischen Bereich aufgrund  
 2633 vertraglicher oder deliktischer Haftung nach §§ 31, 89 bzw. 831 BGB ergeben.<sup>272</sup> Darüber hinaus

---

<sup>269</sup> Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 7, 8.

<sup>270</sup> Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 8 Rn. 9.

<sup>271</sup> Vgl. Kühling, Jürgen/Bohnen, Simon: Zur Zukunft des Datenschutzrechts. JZ 2010, 600 (609).

<sup>272</sup> Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 17.

2634 können sich Schadensersatzansprüche gemäß § 280 BGB wegen schuldhaft rechtswidriger bzw.  
2635 missbräuchlicher Datenverarbeitung aus vorvertraglicher bzw. vertraglicher Haftung ergeben.<sup>273</sup>

2636 Der Nutzen von Schadensersatzansprüchen im Datenschutzrecht ist in der Praxis dadurch beschränkt,  
2637 dass es oftmals schwierig ist, einen konkreten ersatzfähigen Schaden aufzuzeigen. In vielen Fällen  
2638 kann ein Schaden gar nicht beziffert werden, weil keine konkrete materielle Einbuße vorliegt.  
2639 Immaterielle Schäden sind wiederum im deutschen Recht generell nur unter sehr engen  
2640 Einschränkungen ersatzfähig. Schließlich kann aufgrund der technischen Zusammenhänge auch der  
2641 Nachweis der Kausalität für den Schadenseintritt Schwierigkeiten bereiten.

#### 2642 2.3.12 Beschäftigtendatenschutz

2643 Seit Jahrzehnten wird die Schaffung umfassender gesetzlicher Regelungen für den  
2644 Arbeitnehmerdatenschutz diskutiert. Die christlich-liberale Koalition hat sich daher bereits im  
2645 Koalitionsvertrag vom 26. Oktober 2009 für eine Erweiterung des Bundesdatenschutzgesetzes  
2646 ausgesprochen. Denn gegenwärtig existieren nur wenige spezifische gesetzliche Vorschriften zum  
2647 Schutz der personenbezogenen Daten von Beschäftigten. Für zahlreiche Fragen der Praxis zum  
2648 Beschäftigtendatenschutz bestehen keine speziellen gesetzlichen Regelungen. Teilweise ergibt sich  
2649 der rechtliche Rahmen für den Beschäftigtendatenschutz aus verschiedenen allgemeinen Gesetzen wie  
2650 dem Bundesdatenschutzgesetz und dem Betriebsverfassungsgesetz. Daneben existiert eine Vielzahl an  
2651 gerichtlichen Einzelfallentscheidungen, anhand derer wichtige Grundsätze für den  
2652 Beschäftigtendatenschutz entwickelt worden sind. Jedoch sind insbesondere die gerichtlichen  
2653 Entscheidungen für die betroffenen Beschäftigten teilweise nur schwer zu erschließen.

2654 Durch die Erweiterung des Bundesdatenschutzgesetzes<sup>274</sup> soll die Rechtssicherheit für Arbeitgeber  
2655 und Beschäftigte erhöht werden. So sollen einerseits die Beschäftigten vor der unrechtmäßigen  
2656 Erhebung und Verwendung ihrer personenbezogenen Daten geschützt werden, andererseits soll das  
2657 Informationsinteresse des Arbeitgebers beachtet werden. Beides dient dazu, ein vertrauensvolles  
2658 Arbeitsklima zwischen Arbeitgebern und Beschäftigten am Arbeitsplatz zu unterstützen.

2659 Es sollen für Zwecke des Beschäftigungsverhältnisses nur solche Daten verarbeitet werden dürfen, die  
2660 für dieses Verhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das  
2661 Beschäftigungsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante  
2662 Gesundheitszustände beziehen, sollen (zukünftig) ausgeschlossen sein. Mit den Neuregelungen sollen  
2663 Mitarbeiter an ihrem Arbeitsplatz zudem wirksam vor Bespitzelungen geschützt und gleichzeitig den  
2664 Arbeitgebern verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen und den  
2665 Kampf gegen Korruption an die Hand gegeben werden.<sup>275</sup>

#### 2666 2.3.13 Probleme der föderalen Aufsichtsstruktur

2667 In ähnlicher Weise wie im internationalen Bereich gibt es auch im Inland vielfältig Situationen, in  
2668 denen bestehende Rechtsvorschriften unterschiedlich angewendet und ausgelegt werden. Von Vorteil  
2669 ist zwar, dass der Datenschutz im nicht-öffentlichen Bereich maßgeblich durch das  
2670 Bundesdatenschutzgesetz geprägt wird und damit bundeseinheitliche Vorgaben bestehen.

---

<sup>273</sup> Gola, Peter/Schomerus, Rudolf: BDSG, Kommentar. 2010, § 7 Rn. 18.

<sup>274</sup> Gesetzesentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes. BT-Drs. 17/4230 vom 15. Dezember 2010.

<sup>275</sup> Gesetzesentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes. BT-Drs. 17/4230 vom 15. Dezember 2010, S. 12

2671 Durch die weitgehende Zuständigkeit der Bundesländer für die Datenschutzaufsicht kommt es  
2672 allerdings häufig zu einer unterschiedlich strikten Anwendung und teils weiteren, teils engeren  
2673 Auslegung vor allem von eher unbestimmten Regelungen. Manche verantwortliche Stellen sind  
2674 zudem gleich mehreren Aufsichtsbehörden unterworfen, insbesondere wenn die Aufsicht teils dem  
2675 Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, teils der  
2676 Landesdatenschutzaufsicht obliegt.

2677 Andererseits wird vorgetragen, dass der Erfolg der deutschen Datenschutzaufsicht wesentlich auf den  
2678 „föderalen Wettbewerb“ und die Herausbildung von „best practices“ zurückzuführen ist. Zudem kann  
2679 darauf verwiesen werden, dass erst die dezentrale Struktur eine flächendeckende Aufsicht "vor Ort"  
2680 zu gewährleisten im Stande ist.

2681 Eine Abstimmung der Aufsichtsbehörden erfolgt weitgehend informell, insbesondere in Form von  
2682 Konferenzen („Konferenz der Datenschutzbeauftragten des Bundes und der Länder“ vor allem für den  
2683 öffentlichen Bereich, „Düsseldorfer Kreis“ für den nicht-öffentlichen Bereich). Die Konferenzen und  
2684 die daraus resultierenden Veröffentlichungen geben Orientierung, können aber formal keine  
2685 unmittelbaren normativen Wirkungen entfalten und die bestehenden Rechtsunsicherheiten nicht  
2686 gänzlich auflösen.

### 2687 **3 Handlungsempfehlungen**<sup>276</sup>

2688 *Der nachfolgende Text ist in der Projektgruppe unstrittig.*

#### 2689 **Einleitung**

2690 Die anhaltenden Veränderungen der IT-Technologien ziehen notwendig Veränderungen in nahezu  
 2691 allen Lebensbereichen und damit auch bei den dafür geschaffenen Datenschutzbestimmungen nach  
 2692 sich. Seit ihren Anfängen haben sich die Anforderungen an den Schutz personenbezogener Daten  
 2693 laufend stark verändert. Nicht nur, aber besonders auch aufgrund des Erfolges des Internets (zum  
 2694 Beispiel schnell steigende Rechner- und Leitungskapazitäten, Ausweitung und fortlaufende  
 2695 Verbesserung von Software sowie von mobilen Anwendungen) und der zunehmenden Vernetzung in  
 2696 den Diensten und Anwendungen des Web 2.0 bis hin zu einer praktisch allgegenwärtigen  
 2697 rechnergestützten Informationsverarbeitung (Ubiquitous Computing) haben sich die  
 2698 Herausforderungen an den Datenschutz in den letzten Jahren potenziert.

2699 Sowohl der nationale als auch der europäische Gesetzgeber sind diesem rasanten technischen und  
 2700 kulturellen Wandel in Teilen gefolgt. Seit den 1970er Jahren wurden daher die datenschutzrechtlichen  
 2701 Bestimmungen immer wieder angepasst und fortgeschrieben. Dies hat dazu geführt, dass in  
 2702 Deutschland mittlerweile vergleichsweise sehr differenzierte Aussagen sowohl zu den Inhalten als  
 2703 auch zu den Grenzen des Datenschutzes existieren. Obwohl bereits mehrere Anläufe zu einer  
 2704 grundsätzlichen Modernisierung auf nationaler und auf europäischer Ebene unternommen wurden,  
 2705 konnten sie bisher allerdings noch nicht erfolgreich abgeschlossen werden. Aufgrund des  
 2706 technologischen Fortschritts steht der Gesetzgeber jedoch weiterhin unter einem ständigen  
 2707 Veränderungs- und Nachbesserungsdruck, ein Leerlaufen bestehender Regelungen aufgrund des  
 2708 technologischen Fortschritts zu vermeiden. Hinzu kommt, dass auch die zu schützenden Werte in  
 2709 einer digitalen Gesellschaft in dem Maße weiter an Wert und Bedeutung zunehmen werden, in dem  
 2710 diese durch den technologischen Wandel unter Druck geraten. Viele datenschutzrechtliche  
 2711 Grundprinzipien beruhen noch immer auf dem Schutzmodell der 1970er Jahre. Ihr Fortbestand und  
 2712 ihre Anwendbarkeit auf die digitale Gesellschaft werden daher vor dem Hintergrund der großen  
 2713 Anzahl neu aufgeworfener Fragen und Probleme kritisch diskutiert.

2714 Auch wenn der Datenschutz einem gesellschaftlichen Wandel und somit auch unterschiedlichen  
 2715 „Strömungen“ unterliegt, sind sich die Mitglieder der Enquete-Kommission einig, dass das  
 2716 Grundrecht auf informationelle Selbstbestimmung nach wie vor Geltung beansprucht und dieser  
 2717 Anspruch auch nicht aufgegeben werden darf. Es ist ein Grundelement einer freien und  
 2718 demokratischen Kommunikationsverfassung und damit elementare Funktionsbedingung eines  
 2719 freiheitlich-demokratischen Gemeinwesens, das auf die Handlungs- und Mitwirkungsfähigkeit seiner  
 2720 Bürger angewiesen ist. Es vermag über die mittelbare Drittwirkung auf das Privatrecht einzuwirken  
 2721 und kann den Gesetzgeber in seinem objektiv-schutzrechtlichen Gehalt zu effektiven  
 2722 Schutzmaßnahmen verpflichten. In der digitalen Gesellschaft ist ihm und seiner adäquaten  
 2723 Ausgestaltung ein noch höherer Wert beizumessen.

---

<sup>276</sup> Bei dem in [ ] gesetzten Text handelt es sich um Einfügungen des Sekretariats. Es handelt sich um sprachliche Überleitungen zwischen verschiedenen Textpassagen.

2724 Gesellschaftliche Veränderungen hinsichtlich der Wahrnehmung des Umgangs mit  
 2725 (personenbezogenen) Daten im Internet sind in Deutschland spätestens seit der breiten, öffentlichen  
 2726 Diskussion über Anbieter von Geodatendiensten im Jahr 2010 erkennbar. Zwar entzündete sich diese  
 2727 öffentliche Diskussion aus datenschutzrechtlicher Sicht an einem wenig geeigneten Thema, weil es  
 2728 sich zumindest bei den bildmäßig erfassten Hausfassaden um überwiegend öffentlich wahrnehmbare  
 2729 Objekte handelt, bei denen bereits der Personenbezug streitig ist. Dennoch kommt darin eine  
 2730 zunehmende Besorgnis gegenüber den möglichen Folgen des technologischen Fortschritts im Internet  
 2731 zum Ausdruck.

2732 Die gesellschaftliche Reaktion auf die genannten Veränderungen sind in Deutschland deutlich. In  
 2733 Umfragen<sup>277</sup> wünscht sich regelmäßig eine deutliche Mehrheit der Bundesbürger einen verbesserten  
 2734 Schutz ihrer Daten. Denn viele Bürgerinnen und Bürger fürchten den Missbrauch ihrer  
 2735 personenbezogenen Daten, besonders bei der Nutzung des Internets.

2736 Beispiele wie Google Street View oder der vergleichbare Dienst Microsoft Streetside, aber auch zum  
 2737 Beispiel die Möglichkeiten, in sozialen Netzwerken Fotos und Adressbücher (und damit Daten  
 2738 Dritter) einzustellen, führen dazu, dass es zunehmend schwerer wird, sich einer ungewollten Erhebung  
 2739 und Weiterverarbeitung personenbezogener Daten im Internet gänzlich zu entziehen. Hierdurch kann  
 2740 auch eine Verschiebung der „Handlungslast“ auf die Betroffenen eintreten. Dies gilt insbesondere für  
 2741 den Fall, dass diese nicht mit einer Veröffentlichung ihrer personenbezogenen Daten einverstanden  
 2742 waren. Häufig müssen sie nun von sich aus aktiv tätig werden, um entstandene digitale Spuren zu  
 2743 entfernen. Doch Besorgnis und Zutrauen liegen nicht weit auseinander. So werden viele der mit dem  
 2744 Schlagwort Web 2.0 umschriebenen neuen Anwendungen und Dienste bereits nach kurzer Zeit  
 2745 ausgiebig auch von Nutzerinnen und Nutzern in Deutschland in Anspruch genommen. Dies legt die  
 2746 Vermutung nahe, dass Einschätzungen zu den möglichen Folgen einer solchen Nutzung für das eigene  
 2747 oder das Recht anderer auf informationelle Selbstbestimmung oftmals vernachlässigt werden oder  
 2748 aber bei einer Nutzen-Risiko-Abwägung der Nutzen zu überwiegen scheint. Ein Beispiel hierfür  
 2749 stellen einmal mehr die sozialen Netzwerke als wesentlicher Kern des Web 2.0 dar. Schon die ersten  
 2750 Formen wurden sehr ausgiebig von mehreren Millionen Menschen unterschiedlichen Alters weltweit  
 2751 genutzt. Bis heute haben sie nichts an ihrer Attraktivität eingebüßt. Im Gegenteil: rasante  
 2752 gesellschaftliche und auch politische Veränderungen lassen sich weltweit u. a. auch auf soziale  
 2753 Netzwerke als Kommunikationsinstrument zurückführen. Die auf der Mitteilung und Eingabe von  
 2754 personenbezogenen Daten (zum Beispiel Lebensweisen, Gewohnheiten und Präferenzen) basierenden  
 2755 Netzwerke haben sich jedoch auch schon als Bumerang für manchen Nutzer erwiesen. Dies gilt  
 2756 insbesondere, wenn Dritte sich unberechtigt Zugang zu schützenswerten Daten verschaffen konnten  
 2757 oder sich bereits eingestellte personenbezogene Daten nachträglich nicht mehr „zurückholen“ ließen.  
 2758 Besonderen Aufwand erfordern auch die datenschutzrechtlichen Grundeinstellungen für die  
 2759 Nutzerinnen und Nutzer. So gelten pseudonyme Nutzungen bei Facebook als mit den AGB  
 2760 unvereinbar. Ein Teil der eingestellten Daten und Informationen steht zunächst allen Mitgliedern und  
 2761 teilweise auch der Öffentlichkeit zur Verfügung, wenn diese nicht aktiv von sich aus Veränderungen  
 2762 an den Einstellungen vornehmen.

---

<sup>277</sup> siehe u. a. „Datenschutz im digitalen Zeitalter – Trends und Spannungsfelder“, Studie von TNS im Auftrag von Microsoft, Mai/Juni 2011, abrufbar unter: [download.microsoft.com/.../TNS\\_Studie\\_Datenschutz\\_im\\_Internet2011.pdf](http://download.microsoft.com/.../TNS_Studie_Datenschutz_im_Internet2011.pdf); „Die Einstellung der Deutschen zum Thema Datenschutz“, Studie des Instituts für Demoskopie Allensbach im Auftrag der SCHUFA Holding AG, September 2010; "Datenschutz im Internet", BITKOM, Juni 2011, abrufbar unter: [http://www.bitkom.org/files/documents/BITKOM\\_Publikation\\_Datenschutz\\_im\\_Internet.pdf](http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf)



2763 In der digitalen Gesellschaft zeichnet sich eine Entwicklung dahingehend ab, dass Dienste oder  
 2764 Anwendungen, die mit einer Individualisierung einhergehen, als attraktiver wahrgenommen werden.  
 2765 Eine solche Individualisierung setzt die Eingabe oder Bereitstellung personenbezogener Daten durch  
 2766 die Nutzerin oder den Nutzer selbst voraus. Oft erheben und verarbeiten die Anbieter vom Nutzer  
 2767 zunächst unbemerkt Daten, um individualisierte Dienste zur Verfügung zu stellen. Der Nutzer und  
 2768 sein Verhalten werden damit zum Mittelpunkt. Bei vielen Diensten und Anwendungen werden aber  
 2769 auch personenbezogene Daten erhoben, obwohl dies nicht unmittelbar zu einem erkennbaren  
 2770 Mehrwert für den Nutzer führt.

2771 Für den Nutzer hat all dies zur Folge, dass er sich fortlaufend an die veränderten Gegebenheiten  
 2772 anpassen muss, will er neue Dienste beziehungsweise die Weiterentwicklung bestehender Dienste  
 2773 weiterhin nutzen und dabei wirksam von seinem Recht auf informationelle Selbstbestimmung  
 2774 Gebrauch machen. Hierzu bedarf es nicht nur des notwendigen Wissens und damit eines entsprechend  
 2775 kompetenten Umgangs mit dem Medium Internet, sondern auch einer permanenten Aktualisierung  
 2776 und Erweiterung des Wissens über die Funktionsweisen und Auswirkungen der vorhandenen und  
 2777 benutzten Anwendungen und Dienste.

2778 Auch für die Anbieter steigt durch diese Ausrichtung ihrer Geschäftstätigkeit die Verantwortung im  
 2779 Umgang mit den Daten und Informationen ihrer Kundinnen und Kunden. Hinreichend konkrete  
 2780 Vorgaben für die Einhaltung und Umsetzung datenschutzrechtlicher Bestimmungen stärken dabei  
 2781 sowohl das Vertrauen der Nutzer als auch die Rechtssicherheit der Anbieter. In diesem  
 2782 Zusammenhang sollte der Datenschutz nicht als Grenze technologischer Entwicklungen gesehen,  
 2783 sondern auch als Chance zur Erhöhung der Akzeptanz neuer Technologien ausgestaltet werden.

2784 Die Beratungen in der Enquete-Kommission zum Thema Datenschutz und Persönlichkeitsrechte  
 2785 haben gezeigt, dass es einen breiten Konsens über die Grundprinzipien, Ziele und Werte des  
 2786 Datenschutzes gibt. Alle Mitglieder der Enquete-Kommission heben hervor, dass Datenschutz und  
 2787 eine Gewährleistung des Grundrechts auf informationelle Selbstbestimmung Akzeptanz und  
 2788 Vertrauen schaffen. Beide sind unabdingbar für den technologischen Fortschritt in einer digitalen  
 2789 Gesellschaft.

2790 Vor diesem Hintergrund gibt die Enquete-Kommission nachfolgende Handlungsempfehlungen:

2791

### 2792 3.1 Vorgaben für nationalen, europäischen und internationalen Datenschutz

2793 *Der nachfolgende Text ist in der Projektgruppe unstrittig.*

2794 Die Zukunft des Datenschutzes liegt längst nicht mehr allein auf nationaler, sondern auf europäischer  
 2795 und insbesondere auf internationaler Ebene. Die Enquete-Kommission begrüßt daher grundsätzlich  
 2796 das Ziel der Mitteilung der EU-Kommission vom 4. November 2010 - KOM (2010) 609 -, das  
 2797 bestehende Datenschutzrecht auf europäischer Ebene zu novellieren und zu modernisieren, um es so  
 2798 an die neuen technischen Anforderungen des digitalen Zeitalters anzupassen. Insbesondere die  
 2799 Zielsetzung der EU-Kommission, die Rechte des Einzelnen zu stärken, den Verwaltungsaufwand für  
 2800 die Unternehmen zu verringern und ein einheitlich hohes Schutzniveau in und außerhalb der EU zu  
 2801 gewährleisten, unterstützt die Enquete-Kommission grundsätzlich.

2802

2803 Aber auch die Anstrengungen der EU-Kommission, die Zusammenarbeit mit Drittstaaten und  
2804 internationalen Organisationen, einschließlich der Vereinten Nationen, des Europarats und der OECD  
2805 sowie internationaler Normungsorganisationen, wie dem Europäischen Komitee für Normung (CEN),  
2806 der Internationalen Organisation für Normung (ISO), dem World Wide Web Consortium (W3C) und  
2807 der Internet Engineering Task Force (IETF), zu verbessern, finden die Unterstützung durch die  
2808 Enquete-Kommission. Aus Sicht der Enquete-Kommission sollte daher die Bundesregierung sowohl  
2809 prüfen, ob sie ihre eigenen Anstrengungen in den vorgenannten Gremien im Hinblick auf den  
2810 Datenschutz intensivieren kann als auch ob es der Anregung weiterer Verhandlungsmandate für die  
2811 EU-Kommission bedarf.

2812 1. Die Enquete-Kommission sieht Handlungsbedarf darin, die Wettbewerbsposition deutscher  
2813 Anbieter von Internetdiensten gegenüber ausländischen Mitbewerbern durch den Gesetzgeber  
2814 weiter fortlaufend zu analysieren. Gerade im Bereich der sozialen Netzwerke halten sich  
2815 ausländische Anbieter, die keinen Sitz in Deutschland haben, teilweise nicht an nationale  
2816 datenschutzrechtliche Bestimmungen. Zugleich besteht auf nationaler Ebene ein Vollzugsdefizit,  
2817 das geltende Recht auch wirksam gegenüber ausländischen Anbietern von Diensten umzusetzen,  
2818 wenn diese über keinen inländischen Sitz verfügen. Die Enquete-Kommission regt daher eine  
2819 kurzfristige Befassung des Deutschen Bundestags an, wie die Probleme des Anwendungsbereichs  
2820 und bestehende Vollzugsdefizite zielgerichtet behoben werden können. Im Rahmen einer solchen  
2821 Diskussion gibt die Enquete-Kommission zu bedenken, dass nationales Datenschutzrecht nicht  
2822 immer bei weltweiten Angeboten angewendet werden kann.

2823 2. Aus Sicht der Enquete-Kommission sollte die Bundesregierung prüfen, ob zukünftig bei  
2824 international und europaweit tätigen Unternehmen mit mehreren Niederlassungen in  
2825 Mitgliedstaaten der EU in Fragen des Datenschutzes im Internet eine stärkere Koordinierung der  
2826 datenschutzrechtlichen Aufsicht sowohl auf europäischer wie auch nationaler Ebene, etwa durch  
2827 den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, wahrgenommen  
2828 werden sollte. Hierzu wäre die Schaffung eines verbindlichen Abstimmungsverfahrens  
2829 erforderlich.

2830 3. Aus Sicht der Enquete-Kommission ist es fraglich, ob die bisherigen nationalen und europäischen  
2831 Regelungen zur Auftragsdatenverarbeitung für eine rechtssichere Teilnahme von Unternehmen  
2832 am so genannten Cloud-Computing ausreichend sind. Im Zuge der Novellierung der  
2833 Datenschutzrichtlinie sollten daher Regelungen geschaffen werden, die Unternehmen die  
2834 Nutzung von Cloud-Computing und neue Entwicklungen in diesem Bereich ermöglichen. Diese  
2835 Regelungen sollten gleichzeitig ein hohes Datenschutzniveau sicherstellen und damit die Belange  
2836 der Nutzerinnen und Nutzer berücksichtigen sowie den Wirtschaftsstandort Europa stärken.

2837 4. Aus Sicht der Enquete-Kommission muss ein novelliertes europäisches Datenschutzrecht der  
2838 modernen Arbeitsweise international organisierter Konzerne stärker als bisher Rechnung tragen.  
2839 Datenschutz und Datenaustausch in verbundenen Unternehmen müssen unter Beachtung des  
2840 Rechts auf informationelle Selbstbestimmung rechtssicher und damit gegebenenfalls vereinfacht  
2841 ausgestaltet werden.

2842 5. Die Enquete-Kommission regt eine Prüfung auf europäischer Ebene an, ob dem Datenschutzrecht  
2843 ein wettbewerbsschützender Charakter zugeschrieben werden kann. Schließlich könnte dies zu  
2844 einer stärkeren gegenseitigen Kontrolle der Marktteilnehmer im nicht-öffentlichen Bereich und  
2845 somit zu einer besseren Durchsetzbarkeit des Datenschutzes führen.

2846  
2847

2848 ***Streitiger Ergänzungsantrag der Fraktionen CDU/CSU und FDP.***

2849 **6.** Aus Sicht der Enquete-Kommission kann eine datenschutzrechtliche Folgenabschätzung zwar zu  
 2850 einer Förderung des Datenschutzes von Beginn an führen. Sie kann zugleich aber auch zu einem  
 2851 erheblichen bürokratischen Mehraufwand für betroffene Unternehmen führen. Sie sollte daher nur  
 2852 in bestimmten Fällen, in denen sensible Daten verarbeitet werden, oder wenn die jeweilige  
 2853 Verarbeitung mit besonderen Risiken verbunden ist, verbindlich eingeführt werden.

2854

2855 ***Streitiger Ergänzungsantrag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der***  
 2856 ***Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.***

2857 **7.** Bereits im geltenden europäischen wie auch im nationalen Datenschutzrecht gibt es ein  
 2858 umfassendes System des individuellen Rechtsschutzes. Die Enquete-Kommission kann daher  
 2859 nicht erkennen, wie die Einführung eines Verbandsklagerechts zu einer Verbesserung dieses  
 2860 individuellen Rechtsschutzes führen kann. Sie gibt zudem zu bedenken, dass im  
 2861 Datenschutzrecht keine vergleichbare Position des Betroffenen wie im Verbraucherschutzrecht  
 2862 besteht. Schließlich gibt es im Datenschutzrecht gerade kein Verhältnis von Unternehmer und  
 2863 Verbraucher, sondern nur Rechtsbeziehungen zwischen nicht-öffentlichen und öffentlichen  
 2864 Stellen sowie zwischen einzelnen Privatpersonen. Verbandsklagen könnten jedoch, wenn  
 2865 überhaupt, nur in einzelnen Konstellationen zu einer Stärkung der Individualrechte führen. Sie  
 2866 würden im Gegenzug jedoch zu erheblichen Rechtsunsicherheiten bei allen betroffenen  
 2867 Unternehmen führen.

2868

2869 ***Alternativer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE***  
 2870 ***GRÜNEN zum Vorschlag der Fraktionen CDU/CSU und FDP.<sup>278</sup>***

2871 **Verbandsklage**

2872 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,  
 2873 eine gesetzliche Regelung zu schaffen, die Verbraucherschutz- und Datenschutzverbänden eine  
 2874 „fremdnützig“ Klagebefugnis einräumt, ähnlich dem Instrument des Verbandsklagerechts. Eine  
 2875 solche Befugnis soll es den Verbänden ermöglichen, im Namen von Betroffenen und im Interesse der  
 2876 Allgemeinheit auch dann gegen Datenschutzverstöße vorzugehen, wenn die Betroffenen keine  
 2877 rechtlichen Schritte gegen den Rechtsverletzer einleiten.

2878

2879

2880

---

<sup>278</sup> Der nachfolgende Text befand sich in der eingereichten Textfassung der Fraktionen SPD, BÜNDNIS 90/DIE GRÜNEN und DIE LINKE. an anderer Stelle. Um eine Gegenüberstellung mit der entsprechenden Textpassage der Fraktionen CDU/CSU und FDP zu ermöglichen, wird er in der vorliegenden Textfassung bereits an dieser Stelle aufgeführt.

2881 ***Streitiger Ergänzungsantrag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.***

2882 Darüber hinaus empfiehlt die Enquete-Kommission Internet und digitale Gesellschaft dem Deutschen  
2883 Bundestag:

2884 Die zunehmende grenzüberschreitende Vernetzung und Globalisierung von  
2885 Kommunikationsinfrastrukturen macht eine Abstimmung und Modernisierung auch auf supra- wie  
2886 internationaler Ebene notwendig. Zusätzlichen Anlass auf EU-Ebene bieten die Änderungen durch  
2887 den Lissabon-Vertrag und die Inkorporation der Grundrechtecharta, darunter das Grundrecht auf  
2888 Datenschutz. Vor diesem Hintergrund ist der Reformansatz der EU-Kommission zu begrüßen.

2889

2890 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,

2891

2892 die Bundesregierung aufzufordern, sich für eine umfassende Novellierung der Datenschutzrichtlinie  
2893 einzusetzen, bei der auch der öffentliche Sektor einschließlich der Sicherheitsbehörden in die  
2894 Harmonisierung einbezogen werden sollte. Regelungen insbesondere zu Privacy by Design, zum  
2895 Profiling sowie zum Daten- und Personenbezugsbegriff müssen neu geschaffen beziehungsweise  
2896 vorhandene Regelungen grundlegend überarbeitet werden. Die Revision der Richtlinie muss dabei  
2897 insbesondere den Herausforderungen der digitalen Gesellschaft, wie zum Beispiel dem Cloud-  
2898 Computing Rechnung tragen.

2899

2900 **3.2 Datenschutz als Standortfaktor**

2901 ***Der nachfolgende Text ist in Projektgruppe unstrittig.***

2902 Die Einhaltung von datenschutzrechtlichen Bestimmungen und die Schaffung eines hohen  
2903 Datenschutzniveaus könnten gerade im europäischen und internationalen Vergleich zu einem  
2904 positiven Wirtschaftsfaktor und somit zu einem vermarktungsfähigen Alleinstellungsmerkmal werden.  
2905 Diese dürfen daher nicht nur als möglicher Kostenfaktor gesehen werden. Das Bewusstsein der  
2906 Nutzerinnen und Nutzer für datenschutzfreundliche Angebote muss jedoch weiter gestärkt werden,  
2907 damit sie den Markt entsprechend mitgestalten.

2908 Die Enquete-Kommission regt an, nationale und verstärkt auch internationale Initiativen für  
2909 Datenschutz zusammenzufassen.

2910 Nationale Initiativen könnten dabei unter einem Markenzeichen wie beispielsweise „Made in  
2911 Germany“ oder „Made in Europe“ zusammengeführt werden, um so das hohe nationale  
2912 Datenschutzniveau als Qualitätsmerkmal besser herausstellen und vermarkten zu können. Einen  
2913 wichtigen Beitrag hierzu können freiwillige Gütesiegel und Audits, die auf verbindlichen  
2914 Auditierungsverfahren beruhen und von unabhängiger Stelle angeboten und durchgeführt werden,  
2915 leisten.

2916

2917 3.3 **Einwilligung**2918 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

2919 Die Enquete-Kommission hat in ihrem Bericht herausgearbeitet, dass eine informierte und freiwillige  
 2920 Einwilligung des Einzelnen oft nicht stattfindet – und zwar aus unterschiedlichen Gründen. Darüber  
 2921 hinaus ist ein Überblick für die Nutzerinnen und Nutzer über bereits erteilte Einwilligungen nur  
 2922 schwer zu behalten.

2923

2924 Deshalb empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

- 2925 1. die Informationspflichten so auszugestalten, dass die Informationen von der Art und vom Umfang  
 2926 her die Grundlage für informierte und freiwillige Einwilligungen bilden,
- 2927 2. die 2009 verabschiedete Regelung der elektronischen Einwilligung nach § 28 Abs. 3a BDSG in den  
 2928 Allgemeinen Teil des Bundesdatenschutzgesetzes unter § 4a BDSG zu übernehmen, damit ihr  
 2929 Anwendungsbereich sich nicht nur auf Werbeeinwilligungen, sondern auf alle elektronischen  
 2930 Einwilligungen erstreckt,
- 2931 3. zu prüfen, ob es erforderlich erscheint, § 13 Abs. 2 TMG im Hinblick auf ein gesetzlich geregeltes  
 2932 Opt-in-Verfahren (bei dem Betroffene aktiv in die Datenerhebung und -verarbeitung einwilligen,  
 2933 zum Beispiel durch Ankreuzen oder Haken setzen) zu konkretisieren und die Anforderungen  
 2934 technikneutral auszugestalten,
- 2935 4. zu prüfen, ob eine zeitliche Befristung von Einwilligungen sinnvoll und zielführend ist und welche  
 2936 Konsequenzen sich hieraus für das bestehende Recht der Einwilligung ergeben könnten,
- 2937 5. in Betracht zu ziehen, den Widerruf der Einwilligung im Bundesdatenschutzgesetz klarstellend zu  
 2938 regeln. Dies gilt insbesondere mit Blick auf die Weitergabe von Daten. Hier wird empfohlen, dass  
 2939 bereits der Widerruf bei der Stelle genügt, die erstmals die Daten erhoben und weitergegeben hat.  
 2940 Der Widerruf wäre durch diese Stelle an die weiteren Stellen weiterzureichen,
- 2941 6. die in der E-Privacy-Richtlinie vorgesehenen Anforderungen an Information und Zustimmung bei  
 2942 der Platzierung von Cookies für einen wirksamen Schutz bei der Verarbeitung personenbezogener  
 2943 Daten durch den Gesetzgeber in deutsches Recht umzusetzen.

2944

2945 *Streitiger Ergänzungsantrag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.*

2946 Darüber hinaus wird dem Deutschen Bundestag empfohlen, in Rechtsbeziehungen, in denen von einer  
 2947 wirklich freien Einwilligungsentscheidung nicht ausgegangen werden kann, weil die betroffene  
 2948 Person nicht dieselbe Machtposition hat wie ihr Gegenüber (also zum Beispiel die öffentliche Stelle  
 2949 beziehungsweise der Internetdiensteanbieter gegenüber dem Nutzer) eine Einwilligung nur dort  
 2950 zuzulassen, wo ihre Erteilung ebenso wie ihre Ablehnung im freien Ermessen der betroffenen Person  
 2951 steht.

2952

2953 **3.4 AGB und Datenschutz**

2954 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

2955 Insbesondere die in kurzem zeitlichen Abstand erfolgenden mehrfachen Änderungen der  
 2956 Datenschutzbestimmungen in AGB von Anbietern von Internetdiensten, darunter auch Anbieter  
 2957 sozialer Netzwerke, werfen rechtliche Fragen auf. Die Enquete-Kommission fordert, gesetzlich  
 2958 klarzustellen, dass Anbieter von Diensten verpflichtet sind, den rechtzeitigen Vorabzugang  
 2959 veränderter Datenschutzbestimmungen an alle Nutzerinnen und Nutzer sicherzustellen.

2960 Auch wenn es Ziel aller Anbieter von Diensten sein sollte, den Nutzern Datenschutzinformationen in  
 2961 prägnanter und kurzer Form anzubieten, um so eine bewusste Kenntnisnahme deutlich zu erleichtern  
 2962 und das Vertrauen in netzbasierte Anwendungen und Transaktionen zu stärken, gelingt dies nur in den  
 2963 wenigsten Fällen. Nach wie vor müssen viele Nutzer zunächst umfangreiche, teilweise auch schwer  
 2964 verständliche und oft juristisch formulierte allgemeine Geschäftsbedingungen zur Kenntnis nehmen.

2965 Die Bundesregierung sollte daher prüfen,

2966 1. ob die Möglichkeit besteht, leicht verständliche und nachvollziehbare Datenschutzerklärungen zu  
 2967 entwickeln, die für eine Vielzahl von Angeboten im Internet anwendbar sind. Damit könnte die  
 2968 Transparenz für die Nutzer erhöht und eine erhebliche Vereinfachung für die betroffenen  
 2969 Unternehmen erzielt werden,

2970 2. ob die Möglichkeit besteht, Verwender von Datenschutzerklärungen in allgemeinen  
 2971 Geschäftsbedingungen gesetzlich zu verpflichten, diese bereits auf der Startseite in kurzer und  
 2972 verständlicher Form zum Abruf bereitzuhalten.

2973

2974 **3.5 Privacy by Design / by Default**

2975 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

2976 Privacy by Design und Privacy by Default orientieren sich an den Vorgaben der Datenvermeidung  
 2977 und Datensparsamkeit und damit an den zentralen Leitlinien des Datenschutzrechts.

2978 Elemente von Privacy by Design sind beispielsweise eine grundsätzliche Verschlüsselung von Daten  
 2979 oder die automatisierte Löschung von Daten nach Funktionserfüllung.

2980 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, das Prinzip Privacy by Design  
 2981 grundsätzlich als verpflichtende Vorgabe bei der Entwicklung und dem Einsatz neuer Technologien  
 2982 zu formulieren.

2983 Der Grundsatz Privacy by Default gewährleistet, dass die Nutzer bei der Reduzierung des  
 2984 Schutzniveaus von Diensten, Technologien und Anwendungen aktiv entscheiden müssten, welche  
 2985 Veränderungen des höchstmöglichen Schutzniveaus sie zulassen möchten.

2986 Die Enquete-Kommission sieht im Prinzip des Privacy by Default eine wichtige Option zur  
 2987 Gestaltung von elektronischen Diensten und Anwendungen im Internet (zum Beispiel bei deutschen

2988 sozialen Netzwerken oder so genannten location based services<sup>279</sup>). Die Anwendung von  
 2989 datenschutzfreundlichen Voreinstellungen erscheint gerade angesichts der Vielfalt der einzelnen  
 2990 technischen Einstellungen vieler webbasierter Angebote und der oftmals nicht leicht erkennbaren  
 2991 Konsequenzen sinnvoll. Sie begrüßt daher, dass viele Anbieter von Diensten im Internet sich bereits  
 2992 freiwillig zu einer Umsetzung von Privacy by Default verpflichtet haben.

2993 Die Enquete-Kommission regt an, die bereits bestehenden gesetzlichen Vorgaben der  
 2994 Datenvermeidung und Datensparsamkeit (vgl. § 3a BDSG) mit dem Prinzip Privacy by Default  
 2995 gesetzlich zusammenzuführen.

2996

2997 ***Streitiger Ergänzungsantrag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.***

2998 Darüber hinaus wird dem Deutschen Bundestag empfohlen, die Anbieter von Diensten und  
 2999 Anwendungen, die auf der Erhebung, Verarbeitung und Speicherung personenbezogener Daten  
 3000 basieren beziehungsweise die zu ihrer Funktionserfüllung personenbezogene Daten erheben,  
 3001 verarbeiten und speichern, zu verpflichten, grundsätzlich die höchstmöglichen  
 3002 Datenschutzeinstellungen voreinzustellen (Privacy by Default).

3003

3004 **3.6 Verfallsdaten**

3005 ***Der nachfolgende Text ist in Projektgruppe unstrittig.***

3006 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, die Diskussion um Verfallsdaten im  
 3007 Internet auf nationaler und europäischer Ebene weiter zu verfolgen, denn die Entwicklung von  
 3008 technologischen Lösungen für ein Vergessen im Internet steht erst am Anfang. Die Enquete-  
 3009 Kommission sieht in der Initiative der Bundesregierung, mit Hilfe eines Ideenwettbewerbs  
 3010 entsprechende technische Möglichkeiten zu entwickeln, einen richtigen Ansatz.

3011 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag daher, Anreize zu schaffen, die  
 3012 Verfallsdatentechnik und andere technische Maßnahmen zum Schutz der Privatsphäre (etwa „sticky  
 3013 policies“)<sup>280</sup> möglichst intensiv weiterzuentwickeln. Je stärker bereits die technische Infrastruktur  
 3014 datenschutzrechtliche Aspekte berücksichtigt, desto leichter wird es Nutzerinnen und Nutzern fallen,  
 3015 ihre Rechte aktiv wahrzunehmen.

3016

<sup>279</sup> Anmerkung: standortbezogene Dienste.

<sup>280</sup> Mit sticky policies wird eine Art von digitalem Rechtemanagement für Daten bezeichnet: Durch angeheftete Metadaten werden zugelassene Verwendungszwecke definiert. Mit "sticky" ist gemeint, dass diese Metadaten bei Kopiervorgängen "haften bleiben", also mitübertragen werden (siehe auch die Studie „Ergänzende und alternative Techniken zu Trusted Computing (TC-Erg./-A.) - Teil 1-“ im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik, 29.01.2010, S. 20 f., abrufbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/TC\\_ErgA/TC-ErgA\\_Teil1.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/TC_ErgA/TC-ErgA_Teil1.pdf))

3017

3018 **3.7 Selbstdatenschutz und Medienkompetenz**3019 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

3020 Die Enquete-Kommission hält die Ausbildung und kontinuierliche Förderung von Kompetenz und  
 3021 Eigenverantwortung der Nutzer digitaler Medien und dem damit verbundenen Umgang mit eigenen  
 3022 und fremden personenbezogenen Daten für unverzichtbar. Sie geht davon aus, dass die Nutzung  
 3023 zukünftiger (mobiler) Internetdienste die Entwicklung hin zu einem nutzerorientierten  
 3024 Datenschutzmanagement noch weiter verstärken wird. (Selbst-)Datenschutz, Datenschutzmanagement  
 3025 und IT-Sicherheit müssen deshalb kontinuierlich thematisiert und gestärkt werden. Bildungsangebote  
 3026 müssen für alle Altersstufen entwickelt und zur Verfügung gestellt werden.

3027 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag deshalb, darauf hinzuwirken, dass die  
 3028 bisherigen Akteure, wie beispielsweise die Daten- und Verbraucherschutzverbände, der  
 3029 Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zusammen mit der geplanten  
 3030 Stiftung Datenschutz noch stärker als bisher zur Förderung von Selbstdatenschutz und  
 3031 Medienkompetenz beitragen. Die Enquete-Kommission betont, dass über die finanzielle Ausstattung  
 3032 der Landesbeauftragten für den Datenschutz allein die Länder entscheiden, unterstützt aber eine  
 3033 Fortführung des Engagements in diesem Bereich.

3034 Hinsichtlich weiterer Handlungsempfehlungen wird auf den Bericht der Enquete-Kommission zum  
 3035 Thema „Medienkompetenz“<sup>281</sup> und die Handlungsempfehlungen zur Stiftung Datenschutz<sup>282</sup>  
 3036 verwiesen.

3037

3038 **3.8 Soziale Netzwerke**3039 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

3040 Aus datenschutzrechtlicher Sicht werfen soziale Netzwerke eine Reihe von spezifischen  
 3041 Fragestellungen auf. Diese können in Abhängigkeit von den konkreten Produkten der jeweiligen  
 3042 Netzwerkanbieter variieren. Von grundlegender Bedeutung für die Bewertung ist eine klare Trennung  
 3043 zwischen einerseits der Datenverarbeitung durch die Anbieter der Netzwerke selbst und andererseits  
 3044 der Datenverarbeitung durch die Nutzerinnen und Nutzer der Plattformen. Die Enquete-Kommission  
 3045 regt daher an, bestehende Vollzugsdefizite schnellstmöglich zu beseitigen, und empfiehlt zugleich  
 3046 dem Deutschen Bundestag, den Datenschutz bei sozialen Netzwerken in geeigneter Weise zu  
 3047 verbessern.

3048 Für soziale Netzwerke sollten datenschutzfreundliche Grundeinstellungen (Privacy by Default)  
 3049 gesetzlich vorgeschrieben sein. Diese sollten auch die Funktionalität beinhalten, dass in sozialen  
 3050 Netzwerken abgelegte Profile in externen Suchmaschinen nur nach ausdrücklicher Zustimmung des  
 3051 Nutzers auffindbar werden. Zudem müssen die Nutzerinnen und Nutzer eines sozialen Netzwerks

<sup>281</sup> noch einzufügen: entsprechende Drucksachennummer.

<sup>282</sup> siehe unten (noch einzufügen).



3052 jederzeit ihren Account einfach und nachhaltig elektronisch löschen können, das heißt es muss auch  
 3053 zu einer Löschung der Daten auf dem Server des Anbieters kommen. Die Weitergabe von  
 3054 personenbezogenen Daten durch die Betreiber sozialer Netzwerke an Dritte darf neben gegebenenfalls  
 3055 geltenden gesetzlichen Erlaubnistatbeständen nur nach ausdrücklicher Einwilligung durch den Nutzer  
 3056 zulässig sein.

3057

3058 ***Streitiger Ergänzungsantrag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.***

3059 Die Enquete-Kommission hat in ihrem Bericht herausgearbeitet, dass es in sozialen Netzwerken  
 3060 zahlreiche Besonderheiten und Probleme im Umgang mit Daten und Informationen durch die  
 3061 Betreiber der Plattformen gibt.

3062 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag deshalb weiterhin,

- 3063 1. die Betreiber sozialer Netzwerke zu verpflichten, höchstmögliche Sicherheitsvorkehrungen zu  
 3064 treffen, um Datendiebstähle und Systemeinbrüche zu vermeiden. Regelmäßige Kontrollen, die  
 3065 Nutzung aktueller und effektiver Technologien sowie der Vorrang des Schutzes der Nutzerdaten  
 3066 vor dem Komfort sind dabei zu gewährleisten. Technische Neuerungen müssen vor ihrer  
 3067 Einführung von den Plattformbetreibern auf ihre Auswirkungen auf den Schutz der Daten und  
 3068 Inhalte der Mitglieder umfassend geprüft werden;
- 3069 2. den Anbietern zu untersagen, die Nutzungsmöglichkeit von sozialen Netzwerken an eine  
 3070 Einwilligung in die über die Erfüllung des Vertragszwecks hinausgehende Datennutzung zu  
 3071 koppeln;
- 3072 3. einen gesetzlichen Anspruch der Nutzerinnen und Nutzer sozialer Netzwerke auf Löschung des  
 3073 Accounts inklusive aller gespeicherter Nutzerdaten zu schaffen. Dies entspricht den  
 3074 datenschutzrechtlichen Vorgaben. Eine bloße Deaktivierung des Accounts als einzige Option der  
 3075 Abmeldung ist nicht ausreichend, da hierbei alle Daten weiterhin gespeichert bleiben und der  
 3076 Account samt der vorhandenen Daten jederzeit wieder aktiviert werden kann. Die Löschung des  
 3077 Accounts muss für die Nutzer ohne Hürden möglich sein. Die Löschungspflicht der Daten sollte  
 3078 gesetzlich verankert werden;
- 3079 4. die Anbieter sozialer Netzwerke zu verpflichten, in einer verständlichen Formulierung der  
 3080 Nutzungs- und Datenschutzbestimmungen die Nutzer über die möglichen Risiken der Nutzung  
 3081 sozialer Netzwerke aufzuklären;
- 3082 5. die Betreiber zu verpflichten, bei der Neuanmeldung in einem sozialen Netzwerk die  
 3083 Datenerhebung auf ein Minimum der für die Anmeldung erforderlichen Daten beschränken. Ein  
 3084 Recht auf pseudonyme Nutzung sollte ebenfalls gewährleistet sein;
- 3085 6. die Anbieter sozialer Netzwerke zu verpflichten, die Voreinstellungen der Nutzerprofile auf das  
 3086 Minimum der für die Nutzung des Netzwerks notwendigen Daten zu beschränken, sodass  
 3087 Nutzerinnen und Nutzer sich aktiv für die Freigabe ihrer Daten entscheiden können. Da sich  
 3088 gezeigt hat, dass Datenschutzinformationen bei der Anmeldung zu einem sozialen Netzwerk selten  
 3089 gelesen werden, empfiehlt es sich, dass während der Nutzung des Dienstes eingebaute, kontext-  
 3090 sensitive Funktionen Nutzerinnen und Nutzer über die möglichen Konsequenzen ihres Handelns  
 3091 informieren, etwa wenn sie Datenschutzeinstellungen verändern;

3092 7. die Anbieter sozialer Netzwerke zu verpflichten, bei der Umsetzung von Programmierschnittstellen  
 3093 für externe Anwendungen, die so genannten Apps, dafür Sorge zu tragen, dass Dritte nur mit einer  
 3094 aktiven und informierten Einwilligung der Nutzerinnen und Nutzer auf Daten zugreifen können.  
 3095 Die Betreiber der sozialen Netzwerke haben ebenfalls dafür Sorge zu tragen, dass die Schnittstelle  
 3096 von Netzwerk und externer Anwendung nicht zum Missbrauch genutzt werden kann. Auch die  
 3097 Daten Dritter, wie von „Freunden“ der die externe Anwendung nutzenden Person, dürfen über die  
 3098 Schnittstelle nicht ohne explizite Einwilligung der betroffenen Person preisgegeben werden.

3099

### 3100 3.9 Datenschutzaufsicht

3101 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

3102 Die bestehenden Regelungen zur Datenschutzaufsicht sollten aus Sicht der Enquete-Kommission  
 3103 dahingehend überprüft werden, ob sie auch bei den neuen Organisationsformen und vernetzten  
 3104 Prozessen (zum Beispiel Cloud-Computing, Auftragsdatenverarbeitung im Konzern, internationale  
 3105 Diensteanbieter im Internet) einen effektiven Datenschutz sicherstellen. Es sollten die  
 3106 Anordnungsbefugnisse des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an  
 3107 dessen Aufsichtsbeugnisse angepasst werden.

3108 Darüber hinaus hat das Urteil des Europäischen Gerichtshofes vom 9. März 2010 zur Unabhängigkeit  
 3109 der deutschen Datenschutzbehörden im nicht-öffentlichen Bereich noch einmal die besondere Rolle  
 3110 der Kontroll- beziehungsweise Aufsichtsbehörden für den Datenschutz hervorgehoben. Aus Sicht der  
 3111 Enquete-Kommission ist es daher unabdingbar, dass die Kontroll- und Aufsichtsbehörden über  
 3112 ausreichende finanzielle, personelle und technische Mittel verfügen, um die ihnen übertragenen  
 3113 Aufgaben effizient und angemessen zu erfüllen. Denn es ist wichtig, dass die Kontroll- und  
 3114 Aufsichtsbehörden die vorhandenen gesetzlichen Befugnisse intensiv ausüben können, damit die  
 3115 bestehenden Datenschutzgesetze effektiv durchgesetzt und Rechtssicherheit geschaffen werden kann.

3116 Die Enquete-Kommission regt darüber hinaus an, dass die Entscheidungen des Düsseldorfer Kreises  
 3117 sowie Einzelpositionen der dort vertretenen Kontroll- und Aufsichtsbehörden grundsätzlich zukünftig  
 3118 veröffentlicht werden und nur in begrenzten Ausnahmefällen eine Veröffentlichung unterbleibt. Auch  
 3119 wenn die Entscheidungen des Düsseldorfer Kreises formal keine unmittelbaren normativen  
 3120 Wirkungen entfalten können, können sie für betroffene Unternehmen zumindest grundlegende  
 3121 Anhaltspunkte bei bestehenden Rechtsunsicherheiten bieten.

3122

3123 *Streitiger Ergänzungsantrag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.*

3124 Weiterhin unterstützt die Enquete-Kommission die auch von der Konferenz der  
 3125 Datenschutzbeauftragten des Bundes und der Länder geforderten nachfolgenden gesetzgeberischen  
 3126 Maßnahmen und empfiehlt,

3127 1. dafür Rechnung zu tragen, dass eine wirksame Kontrolle zur Voraussetzung eines erfolgreichen  
 3128 Datenschutzes wird. Wenn man Datenschutz zudem zunehmend als Querschnittsaufgabe begreifen  
 3129 will, muss dies auch institutionelle Folgen haben. Um die – auch von der Datenschutzrichtlinie

- 3130 geforderte und vom EuGH bestätigte – vollständige Unabhängigkeit der Datenschutzinstanzen zu  
 3131 stärken und um Interessenkonflikte zu vermeiden, sollte der Bundesbeauftragte für den  
 3132 Datenschutz und die Informationsfreiheit weder dem Bundesministerium des Innern noch einer  
 3133 anderen Bundesbehörde zugeordnet sein. Er sollte frei von Rechts- oder Fachaufsicht seiner  
 3134 Aufsichtstätigkeit nachgehen können. Eine Dienstaufsicht ist allenfalls in eingeschränkter Form  
 3135 zulässig;
- 3136 2. das Urteil des EuGH <sup>283</sup> zu berücksichtigen und die gesetzlichen Grundlagen für die  
 3137 Unabhängigkeit der Kontrollstellen im Sinne der Datenschutzrichtlinie umzusetzen;
- 3138 3. dafür zu sorgen, dass § 38 BDSG dahingehend überarbeitet wird, dass
- 3139 - das Anordnungsrecht gemäß § 38 Abs. 5 BDSG effektiver ausgestaltet und den üblichen  
 3140 Grundsätzen des Verwaltungsvollzugs angepasst wird,
- 3141 - eine gesetzliche Mitwirkungspflicht der kontrollierten Stelle gegenüber der Aufsichtsbehörde  
 3142 geschaffen wird, ähnlich der Mitwirkungspflicht im Sinne des § 24 Abs. 4 BDSG oder des § 5 des  
 3143 Gesetzes zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung;
- 3144 4. dafür zu sorgen, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die  
 3145 den Länderbehörden zustehenden Anordnungsbefugnisse in entsprechender Weise für alle  
 3146 Bereiche, in denen er die Aufsicht führt, also auch für die Aufsicht über die nicht-öffentlichen  
 3147 Stellen nach dem Telekommunikationsgesetz sowie dem Postgesetz erhält<sup>284</sup>;
- 3148 5. die Ausdehnung der Zeugnisverweigerungsrechte und Beschlagnahmeverbote auf Informationen  
 3149 und Unterlagen, die die Aufsichtsbehörden bei Berufsheimnisträgerinnen und -trägern erlangt  
 3150 haben, gesetzlich zu regeln;
- 3151 6. eine Strafantragsbefugnis für die Datenschutzaufsichtsbehörden in § 205 StGB festzulegen.

3152

### 3153 3.10 Vorbildwirkung öffentlicher IT-Projekte

#### 3154 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

3155 Die Enquete-Kommission weist darauf hin, dass sowohl bei der Planung von öffentlichen IT-  
 3156 Projekten und E-Government-Angeboten als auch bei der späteren Aus- und Durchführung die  
 3157 aktuellen technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz in  
 3158 besonderer Weise beachtet und bei technischen Weiterentwicklungen auch fortgeschrieben werden  
 3159 müssen. Nur so können aufkommende Zweifel am sicheren Umgang mit personenbezogenen Daten

<sup>283</sup> EuGH, Urteil vom 9. März 2010, Rs. C-518/07, NJW 2010, 1265 – EU-Kommission gegen Deutschland.

<sup>284</sup> Postgesetz vom 22. Dezember 1997, BGBl. I S. 3294, zuletzt geändert durch Verordnung vom 31. Oktober 2006, BGBl. I S. 2407.

3160 von Beginn an ausgeräumt werden. Öffentliche IT-Projekte sollten mit Blick auf ihre Vorbildwirkung  
3161 etwa für die Privatwirtschaft auf hohem Datenschutzniveau durchgeführt werden.

3162 In den letzten Jahren haben verschiedene IT-Großprojekte zum Teil Kritik von Datenschützern  
3163 erfahren. Die Enquete-Kommission empfiehlt daher,

- 3164 1. dass öffentliche IT-Projekte auf hohem Schutzniveau basieren und ihrer Vorbildwirkung gerecht  
3165 werden,
- 3166 2. dass E-Government-Angebote im Bereich der Dienstleistungen für Bürgerinnen und Bürger den  
3167 aktuellsten technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz  
3168 genügen müssen.

3169  
3170 Darüber hinaus empfiehlt die Enquete-Kommission bei zentralen IT-Projekten, auch bei jenen, die  
3171 von der EU eingeleitet werden,

- 3172 1. den Datenschutz bereits von Beginn an in der Konzeption zu berücksichtigen. Wo dies nicht der  
3173 Fall ist, muss es auch weiterhin möglich sein, die Umsetzung entsprechender Projekte zu  
3174 verweigern. Wenn Aufträge für die Entwicklung solcher Projekte vergeben werden, sollten sie stets  
3175 die Programmierung entsprechender technischer Begrenzungen beinhalten. Im Interesse der  
3176 Verwirklichung möglichst vorbildlichen Datenschutzes sollte dies bereits bei der finanziellen  
3177 Planung berücksichtigt werden.
- 3178 2. den besonderen datenschutzrechtlichen Herausforderungen eines verwaltungsübergreifenden  
3179 Arbeitens zu begegnen. Um national wie international bei Outsourcing einen unsensiblen Umgang  
3180 mit Datenschutzbelangen frühzeitig zu verhindern, bedarf es hier einer stärkeren aktiven  
3181 Einbeziehung datenschutzrechtlicher Aspekte in alle Planungsetappen.

3182  
3183 Zudem empfiehlt die Enquete-Kommission dem Deutschen Bundestag, die Forschung im Bereich des  
3184 Datenschutzes auch weiterhin mit öffentlichen Mitteln zu fördern und zusätzliche finanzielle  
3185 Anstrengungen zu prüfen, um die Entwicklung von Datenschutztechnologien zu fördern.

3186

3187 ***Streitiger Ergänzungsantrag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.***

3188 Weiterhin wird der Bundesregierung empfohlen,

- 3189 1. bei öffentlichen IT-Projekten der Vorbildwirkung gerecht zu werden und auf ein besonders hohes  
3190 Schutzniveau zu drängen. Dabei ist auf weitere Datensammelprojekte großen Umfangs zu  
3191 verzichten, die Kritik der Datenschützer ernst zu nehmen und in eine breite gesellschaftliche  
3192 Debatte mit staatlichen und nicht staatlichen Akteuren zu treten;
- 3193 2. die genannten Projekte einer erneuten Prüfung zu unterwerfen, die insbesondere die technischen  
3194 Grundlagen einer ergebnisoffenen datenschutzrechtlichen Evaluation zugänglich macht. E-  
3195 Government-Angebote im Bereich der Dienstleistungen für Bürgerinnen und Bürger müssen den  
3196 aktuellsten technischen und organisatorischen Anforderungen an einen wirksamen Datenschutz  
3197 genügen;
- 3198 3. eine stärkere aktive Einbeziehung datenschutzrechtlicher Aspekte in alle Planungsetappen im  
3199 Bereich des verwaltungsübergreifenden Arbeitens sicherzustellen, weil dies eine besondere  
3200 Herausforderung in datenschutzrechtlicher Hinsicht darstellt. Dies insbesondere mit dem Ziel,

- 3201 national wie international, bei Offshoring und Outsourcing einen unsensiblen Umgang mit  
3202 Datenschutzbelangen frühzeitig zu verhindern;
- 3203 4. bei zentralen IT-Projekten, auch jenen, die von der EU eingeleitet werden, den Datenschutz bereits  
3204 von Beginn an in der Konzeption zu berücksichtigen;
- 3205 5. beim Einkauf komplexer Standardprodukte wie Zeiterfassungs- oder Zugangskontrollsysteme für  
3206 öffentliche Einrichtungen sicherzustellen, dass die erfassten Daten tatsächlich nur im Rahmen ihrer  
3207 Zweckbestimmung verwertet werden. Wenn Aufträge für die Entwicklung solcher Projekte  
3208 vergeben werden, sollten sie stets die Programmierung entsprechender technischer Begrenzungen  
3209 beinhalten. Im Interesse der Verwirklichung möglichst vorbildlichen Datenschutzes sollte dies  
3210 bereits bei der finanziellen Planung berücksichtigt werden;
- 3211 6. in Ämtern und Behörden wegen des erhöhten Einsatzes von Software und des Zugriffs hierauf  
3212 durch verschiedene Mitarbeiter Vorkehrungen zu treffen, die eine Verletzung insbesondere des  
3213 Sozialdatenschutzes ebenso ausschließen wie des Steuergeheimnisses;
- 3214 7. dafür Sorge zu tragen, dass in den kommenden fünf Jahren mindestens 10 Prozent der  
3215 Forschungsgelder aus dem Bereich IT in Bereichen der Datenschutztechnologien gebunden  
3216 werden. Über die Verwendung der Gelder sollte nach Beratung mit dem Bundesbeauftragten für  
3217 den Datenschutz und die Informationsfreiheit, der geplanten Stiftung Datenschutz und  
3218 Interessenvertretern der betroffenen Akteure entschieden werden;

3219

### 3220 3.11 Smartgrids und andere intelligente Netze

#### 3221 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

3222 Die Möglichkeit, mithilfe intelligenter Stromzähler den tatsächlichen Stromverbrauch kontrollieren zu  
3223 können, kann einen ökonomischen Mehrwert für den Verbraucher schaffen und beträchtliche  
3224 ökologische Vorteile mit sich bringen. Bei ihrem Betrieb fallen jedoch auch umfangreiche und  
3225 differenzierte Datenbestände (Lastprofile) an, die durch geeignete technische und organisatorische  
3226 Maßnahmen wirksam vor dem Zugriff durch Unberechtigte geschützt werden müssen. Auch muss  
3227 sichergestellt werden, dass die Datenhoheit, insbesondere ausreichende Kontrollmöglichkeiten,  
3228 grundsätzlich beim Verbraucher verbleiben und dieser selbst darüber entscheiden kann, wem er  
3229 welche Daten zur Verfügung stellen möchte. Dabei muss angesichts der zunehmenden Bedeutung  
3230 regenerativer Energien bei der Stromversorgung ein effektives Netzmanagement möglich sein.

3231 Es muss sichergestellt werden, dass personenbezogene Daten in der Regel nur den Verbrauchern zur  
3232 Verfügung gestellt und Verbrauchswerte nur für die Abrechnung personenbezogen verwendet werden  
3233 dürfen. Darüber hinaus sollten bei ihrer Verwendung zu Zwecken eines verbesserten  
3234 Netzmanagements Verschlüsselungstechniken zur Anwendung kommen, die eine  
3235 datenschutzkonforme Datenübermittlung ermöglichen. Zudem müssen ausreichende  
3236 Sicherheitsvorkehrungen vorgehalten werden, die einen unerlaubten Zugriff auf die Daten verhindern.  
3237 Nicht nur im Energiesektor werden derzeit intelligente Netze aufgebaut, zu deren Betrieb umfassend  
3238 Daten kommuniziert werden müssen. Auch im Verkehrssektor (Verkehrstelematik und E-Mobility),  
3239 im Gesundheitswesen (Gesundheitstelematik und E-Health) und dem Bildungswesen (E-Learning)

3240 befinden sich intelligente Netze in Planung. In diesen Netzen sollen künftig Daten über das eigene  
3241 Mobilitätsverhalten bis hin zu sensiblen Daten wie dem persönlichen Gesundheitszustand und der  
3242 Gesundheitshistorie kommuniziert werden.

3243 Datensparsamkeit und Datenvermeidung im Rahmen der für die Nutzung von Zukunftstechnologien  
3244 erforderlichen Datenverarbeitung sollten Ausgangspunkt entsprechender gesetzgeberischer Initiativen  
3245 sein. Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, in diesen Bereichen die  
3246 Notwendigkeit gesetzlicher Vorgaben eingehend zu prüfen und darauf hinzuwirken, dass neue  
3247 Technologien auch bei intelligenten Netzen datenschutzkonform ausgestaltet werden.  
3248 Einzelfallgesetze für bestimmte Dienste sind dabei nach Möglichkeit zu vermeiden.

3249

3250

3251

3252 *Über die vorstehenden Handlungsempfehlungen hinaus haben die Fraktionen zu weiteren*  
 3253 *Themenkomplexen Vorschläge für Handlungsempfehlungen vorgelegt. Die Texte sind*  
 3254 *ausnahmslos streitig. Zur Mehrzahl der Themenkomplexe stehen sich zwei Textentwürfe (jeweils*  
 3255 *von CDU/CSU und FDP einerseits und von SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN*  
 3256 *andererseits) alternativ gegenüber. Eine Nummerierung der nachfolgenden*  
 3257 *Handlungsempfehlungen erfolgt nach der Beschlussfassung im Rahmen der redaktionellen*  
 3258 *Schlussbearbeitung.*

3259

3260 *Streitiger Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.*

3261 **Hintergrund und Ausgangslage**

3262 Maßgeblicher Ausgangspunkt für die Notwendigkeit datenschutzrechtlicher Reformen waren und sind  
 3263 die tiefgreifenden Veränderungen der Informations- beziehungsweise Kommunikationstechnologien  
 3264 sowie die damit einhergehenden Veränderungen der Angebote und Dienste, des Nutzungsverhaltens  
 3265 und insbesondere des Verhaltens der datenverarbeitenden Stellen. Die letzte größere Reform des  
 3266 Datenschutzrechts erfolgte Ende der 1990er Jahre zu einer Zeit, als beispielsweise das Internet sich  
 3267 noch in einer ersten Aufbruchphase befand, dort vollkommen andere Anwendungen und  
 3268 Technologien zum Einsatz kamen und es nicht annähernd die heutigen Nutzerzahlen aufwies.  
 3269 Grundlegende und nach wie vor geltende Regelungselemente des Datenschutzrechts basieren auf der  
 3270 Vorstellung der Großrechnertechnologie und der Rechenzentren der 1970er Jahre.

3271 Mittlerweile hat sich eine wesentlich veränderte Informations- und Kommunikationsgesellschaft  
 3272 herausgebildet. Das weltweite Internet ist zur zentralen Kommunikationsinfrastruktur moderner  
 3273 Nationalstaaten aufgerückt. Zu den prägenden Entwicklungen auf der technischen Seite wie auch auf  
 3274 der Seite der Anwender zählen etwa – unter stetiger Reduktion der Kosten – weiter ansteigende  
 3275 Rechnerkapazitäten, Miniaturisierung, verbesserte Chip- und Mikroprozessortechnologien, die  
 3276 Ausweitung der Netztechnologie, Profiling-Technologien sowie die mobilen Anwendungen. Die heute  
 3277 zentralen Angebote des Internet, welche unter dem Schlagwort Web 2.0 zusammengefasst werden,  
 3278 sind durch interaktive Dienste gekennzeichnet. Damit gewinnen der „User“ und sein Verhalten, vor  
 3279 allem seine eigene Datenverarbeitungspraxis, an Bedeutung.

3280

3281 Geprägt werden das Internet wie auch der Mobilfunkmarkt zudem durch oligopolistische Strukturen,  
 3282 sodass einige wenige Unternehmen maßgeblichen Einfluss auf zentrale Entwicklungen ausüben. Die  
 3283 Verarbeitung von Daten und Informationen insbesondere zum Zweck der personalisierten  
 3284 Werbeansprache strukturiert die Geschäftskonzepte der größten Webunternehmen. Quantität wie auch  
 3285 Qualität der Datensammlungen in den Händen privater Stellen haben in den vergangenen Jahren  
 3286 exponentiell zugenommen und sind u. a. auch für staatliche Stellen von weiter wachsendem Interesse.  
 3287 Das belegen die Debatten um die Einführung verpflichtender Speicherungen von  
 3288 Telekommunikationsverkehrsdaten, von Finanztransaktionsdaten wie auch von Flugpassagierdaten.

3289

3290 In wichtigen gesellschaftlichen Bereichen wie dem Internet, der Telekommunikation, bei Mobilität  
 3291 und Verkehr, den öffentlichen Räumen des täglichen Lebens oder bei Finanz- und Geldgeschäften hat  
 3292 die Digitalisierung dazu geführt, dass das Verhalten von Bürgern registriert, gespeichert und  
 3293 zumindest nachträglich für zunehmend länger zurückliegende Zeiträume nachvollzogen werden kann.  
 3294 Zudem steht die Gesellschaft erst heute, allerdings nun tatsächlich vor dem Eintritt in das bereits 2000  
 3295 im damaligen Modernisierungsgutachten<sup>285</sup> etwas vorschnell prognostizierte Ubiquitous Computing,  
 3296 die so genannte allgegenwärtige Datenverarbeitung. Darauf deuten zunehmend geodatengestützte  
 3297 Anwendungen, erste marktgängige Nutzungen von RFID<sup>286</sup>-Chips, die weit verbreitete  
 3298 Videoüberwachung, die Telematik im Automobilssektor oder auch das in Zukunft realisierte Smart  
 3299 Grid / Metering im Energiesektor hin. Damit steht der Datenschutz heute vor der Situation, dass ganze  
 3300 Infrastrukturen erfassbar und auswertbar werden. Eine verkürzte, allein auf die Vorstellung eines  
 3301 eigentumsanalogen Verfügungsrechts verengte Schutzperspektive wird dieser veränderten Risikolage  
 3302 nicht gerecht. Umfang und Qualität der Datenverarbeitung haben vielmehr massive, auch  
 3303 gesamtgesellschaftliche Auswirkungen. Die damit verbundenen überindividuellen Risiken etwa des  
 3304 Missbrauchs von Daten, des damit einhergehenden breiten Vertrauensverlustes bei Nutzerinnen und  
 3305 Nutzern sowie der möglichen Vermeidung der Nutzung ganzer Kommunikationsinfrastrukturen  
 3306 sind konzeptionell bislang nicht hinreichend berücksichtigt.

3307

3308 Der Reformstau im Bereich des Datenschutzes ist weitgehend unbestritten. Die Modernisierung des  
 3309 Datenschutzes führte bereits 1998 zur Befassung des Deutschen Juristentages, der weitreichende  
 3310 Änderungsvorschläge unterbreitete. Die damalige Bundesregierung beabsichtigte eine zweistufige und  
 3311 grundlegend ansetzende Reform. Realisiert wurde lediglich die erste Stufe in Gestalt der Umsetzung  
 3312 der dringlichsten Anforderungen der Datenschutzrichtlinie. Der durch ein umfangreiches  
 3313 wissenschaftliches Gutachten<sup>287</sup> vorbereitete zweite Reformschritt konnte nicht mehr verwirklicht  
 3314 werden. Seit 2009 hat auch die Europäische Kommission die Reform der Datenschutzrichtlinie  
 3315 angekündigt, Konsultationen in den Mitgliedstaaten durchgeführt sowie Ende 2010 erste Eckpunkte  
 3316 einer Reform vorgelegt, die neben dem Bereich der Privatwirtschaft auch eine Harmonisierung der  
 3317 staatlichen Datenverarbeitung, insbesondere bei den Polizei- und Justizbehörden der Mitgliedstaaten,  
 3318 herbeiführen soll.

3319

3320 Die gesellschaftliche Reaktion auf die genannten Veränderungen fällt in Deutschland recht deutlich  
 3321 aus. In Umfragen wünscht sich eine klare Mehrheit der Bundesbürger einen verbesserten Schutz ihrer  
 3322 Daten. Die Ausweitung des Internethandels gilt durch Vertrauensdefizite in der Bevölkerung

<sup>285</sup> Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern. 2002.

<sup>286</sup> Radio Frequency Identification.

<sup>287</sup> Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern. 2002.



3323 zumindest als belastet. Denn viele Bürger fürchten sich vor dem Missbrauch ihrer personenbezogenen  
3324 Daten, besonders bei der Nutzung des Internet. Anstrengungen beim Datenschutz hingegen können  
3325 die Akzeptanz für neue Technologien erhöhen und das Vertrauen in deren Nutzung stärken.

3326

3327 Eine Gruppe von besonders internetaffinen Nutzern hat auch außerhalb Deutschlands eine  
3328 „Postprivacy“-Debatte angestoßen, die den Wert des Datenschutzes im Internetzeitalter neu  
3329 thematisiert. Kernaussage ist dabei die eher empiristische These vom Kontrollverlust hinsichtlich der  
3330 Daten im Internet. Weil es im Kontext des Internet faktisch nicht mehr möglich sei, im Wege des  
3331 Selbstschutzes eigene Daten vor der Weiterverarbeitung durch Dritte zu schützen, habe sich der  
3332 Datenschutz überlebt und werde einer neuen Kultur der Transparenz weichen. Dem wird in der  
3333 öffentlichen Debatte allerdings entgegengehalten, es handele sich um einen Fehlschluss, weil aus dem  
3334 so beschriebenen Sein allein kein Sollen ableitbar sei. Auch gilt die These vom Kontrollverlust schon  
3335 deswegen als wenig zielführend, weil sie ein verkürztes Schutzprogramm des Datenschutzes  
3336 beschreibt, bei dem aufgrund der Fehlvorstellung eines ausschließlich individuellen Verfügungsrechts  
3337 primär Elemente des Selbst Datenschutzes dem Datenschutz zugerechnet werden. Allerdings besteht  
3338 Datenschutz längst aus einer Vielzahl von weit darüber hinausgehenden Schutzvorkehrungen und  
3339 Maßnahmen.

3340

3341 Die massive Zunahme der Verarbeitung personenbezogener Daten in einem zunehmend  
3342 unübersichtlicheren Feld von Akteuren fordert vom Gesetzgeber eine konsequente Neuausrichtung  
3343 des Regelungsfeldes. Der bestehende ordnungsrechtliche Regelungsansatz, wie er insbesondere im  
3344 Bundesdatenschutzgesetz sowie dem Telemediengesetz und Telekommunikationsgesetz zum  
3345 Ausdruck kommt, ist nicht grundsätzlich obsolet geworden. Ein allgemeiner Rückzug auf  
3346 Selbstregulierungen, wie er zum Teil etwa mit Blick auf Fragen des Internetdatenschutzes  
3347 vorgeschlagen wird, verfehlt jedoch die Vorgaben der verfassungsgerichtlichen Rechtsprechung zur  
3348 mittelbaren Drittwirkung sowie den grundrechtlichen Schutzpflichten. Andererseits bedarf es einer  
3349 sachgerechteren Beurteilung und Behandlung von Datenschutzfragen vor Ort bei den verarbeitenden  
3350 Stellen selbst. Dem entspricht eher die Orientierung an Konzepten regulierter Selbstregulierung  
3351 beziehungsweise Koregulierung. Es bedarf auch weiterhin klarer Vorgaben hinsichtlich der  
3352 Zulässigkeit bestimmter Datenverarbeitungen, verbunden mit eben so deutlichen Regelungen zu den  
3353 Konsequenzen von Verstößen. Die Durchsetzung dieser Regelungen muss durch ein unabhängiges  
3354 und effizientes Aufsichtssystem gewährleistet sein. Nicht zuletzt das Bundesverfassungsgericht sieht  
3355 dieses Ordnungssystem als maßgeblich an, weil der Umgang mit personenbezogenen Daten und  
3356 Informationen zu einem großen Teil dem Schutzbereich insbesondere des Grundrechts auf  
3357 informationelle Selbstbestimmung unterfällt. Hinsichtlich der Zielsetzung des Datenschutzes ist  
3358 bedeutsam, ist bedeutsam, dass sich aus dem Grundrecht auf informationelle Selbstbestimmung eine  
3359 Vielzahl unterschiedlicher Schutzerfordernisse ergibt.

3360

3361

## 3362 Daten und Informationen

3363 Sachangemessene Regelungen bedürfen einer differenzierten begrifflichen Beschreibung. Die  
 3364 bisherige Verwendung der Begriffe Daten und Informationen greift zu kurz. Daten sind Zeichen, die  
 3365 auf Datenträgern vergegenständlicht festgehalten werden und als Informationsgrundlagen dienen.  
 3366 Informationen selbst hingegen werden als Sinnelemente erst in bestimmten sozialen  
 3367 Verwendungszusammenhängen durch aktive Deutungsleistungen (sozialer Kontext) erzeugt und  
 3368 genutzt.<sup>288</sup> Mit dieser Unterscheidung wird die im Datenschutz durchaus bekannte  
 3369 „Kontextabhängigkeit“ für die Bewertung der mit Datenverarbeitungen verbundenen Risiken besser  
 3370 herausgearbeitet. In der Folge wird es möglich, zusätzliche Anknüpfungspunkte für präzisere  
 3371 Schutzmaßnahmen zu formulieren. Zukünftig sollte die Unterscheidung von Daten und Informationen  
 3372 deshalb vom Gesetzgeber besser herausgearbeitet werden.

3373

## 3374 Anwendungsbereich/Personenbezug

3375 Bei der Reform des Datenschutzes ist zu berücksichtigen, dass der grundlegende Ansatz des  
 3376 Datenschutzrechts, nämlich die Personenbezogenheit eines Datums, in der digitalen Welt  
 3377 weiterentwickelt werden muss. Zwar ist auch im Internet nicht jedes Datum personenbezogen, doch  
 3378 grundsätzlich sind alle Daten personenbeziehbar. Es gibt kein belangloses Datum mehr. Denn durch  
 3379 die Verknüpfung mit anderen Daten kann ein Personenbezug jederzeit hergestellt werden. Das  
 3380 bedeutet vor allem, dass Daten nicht von vornherein aus dem Schutz herausfallen dürfen. Es kommt  
 3381 mehr denn je darauf an, einen abgestuften gefährdungsabhängigen Schutz zu entwickeln, damit der  
 3382 Anwendungsbereich des Datenschutzrechts nicht beliebig weit geöffnet und damit konturlos wird.

3383 Die technischen Möglichkeiten der Verkettung verschiedener Datensätze haben sich grundlegend  
 3384 erweitert. Dem muss die zukünftige gesetzgeberische Gestaltung Rechnung tragen.

3385

## 3386 Abwehr- und Schutzkomponente

3387 Datenschutz beinhaltet verfassungsrechtlich gesehen weit mehr als eine bloße Abwehr von Eingriffen  
 3388 in das Recht auf informationelle Selbstbestimmung. Die Schutzkomponenten betreffen nicht nur das  
 3389 Verhältnis zum Staat, sondern aufgrund konkreter Gefahren der personenbeziehbaren  
 3390 Datenverarbeitung auch den Bereich der Privatwirtschaft. Im Sinne der Gewährleistung einer freien  
 3391 Persönlichkeitsentfaltung der Bürgerinnen und Bürger beinhaltet die Schutzkomponente des  
 3392 Datenschutzes deshalb auch eine staatliche Verpflichtung, Maßnahmen zu treffen, die gewährleisten,  
 3393 dass die Daten des Einzelnen wirksam geschützt sind und dass er über die Verarbeitung dieser Daten  
 3394 informiert wird.

3395

---

<sup>288</sup> Vgl. M. Albers, Umgang mit personenbezogenen Daten und Informationen, in: Schmidt-Aßmann/ Hoffmann-Riem/ Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts II 2008, § 22.

3396

3397 *Streitiger Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.*3398 **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer**  
3399 **Systeme/Grundrecht auf informationelle Selbstbestimmung**3400 Angesichts der Bedeutung des Schutzes der personenbezogenen Daten für nahezu alle Lebensbereiche  
3401 und der wegweisenden Rechtsprechung des Bundesverfassungsgerichts, insbesondere mit Blick auf  
3402 die zukünftige technische Entwicklung, empfiehlt die Enquete-Kommission dem Deutschen  
3403 Bundestag, zu prüfen,

3404

3405 1. ob die vom Bundesverfassungsgericht geschaffenen Grundrechte auf informationelle  
3406 Selbstbestimmung sowie auf Gewährleistung der Vertraulichkeit und Integrität  
3407 informationstechnischer Systeme in den Grundrechtekatalog des Grundgesetzes als eigenständig  
3408 formulierte Grundrechte aufgenommen werden sollten.3409 2. ob es der Fortentwicklung des Post- und Fernmeldegeheimnisses nach Art. 10 GG hin zu einem  
3410 übergreifenden Recht auf Schutz des Kommunikationsgeheimnisses bedarf.

3411

3412 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer u. teilweise ergänzender*  
3413 *Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*3414 **Grundprinzipien des Datenschutzrechts**3415 Die verschiedenen Grundprinzipien des deutschen Datenschutzrechts sind durch die Enquete-  
3416 Kommission im Kapitel 2.1 ausführlich dargestellt worden. Die Enquete-Kommission geht davon  
3417 aus, dass trotz rasanter technischer Weiterentwicklungen diese Grundprinzipien auch in Zukunft einen  
3418 Anspruch auf Geltung haben müssen. Dabei sollten die Grundsätze der Verhältnismäßigkeit, der  
3419 Datensicherheit und -sparsamkeit, der Zweckbindung und Transparenz noch stärker zur Geltung  
3420 gebracht werden.3421 Es muss jedoch auch Anspruch des nationalen Gesetzgebers sein, das Datenschutzrecht unter  
3422 Berücksichtigung der europarechtlichen Vorgaben fortlaufend weiterzuentwickeln. Vorrang sollte  
3423 hierbei eine technikneutrale Ausgestaltung von datenschutzrechtlichen Bestimmungen haben.  
3424 Angesichts einer zunehmenden Komplexität und Länge der Regelungen müssen auch  
3425 Übersichtlichkeit, Lesbarkeit und die Verständlichkeit eine größere Rolle einnehmen.3426 Neben sprachlichen Vereinfachungen und Verbesserungen sollten auch aktuelle und zukünftige  
3427 Entwicklungen bei den Definitionen und Begriffsbestimmungen (beispielsweise zur  
3428 Personenbeziehbarkeit) durch den Deutschen Bundestag beobachtet werden.3429 **Auskunfts- und Widerrufsrechte**3430 Bereits nach dem geltenden Datenschutzrecht ist die Wirtschaft gefordert, für Transparenz beim  
3431 Umgang mit personenbezogenen Daten zu sorgen und den Nutzer nicht im Unklaren über die  
3432 Speicherung und Nutzung seiner Daten zu lassen. Für die Zukunft empfiehlt die Enquete-Kommission

3433 dem Deutschen Bundestag, den Transparenzgrundsatz technikneutral auszugestalten. Für die  
 3434 Nutzerinnen und Nutzer muss insbesondere erkennbar sein, von welcher verantwortlichen Stelle  
 3435 personenbezogene Daten erhoben werden. Wenn Daten weitergegeben oder von anderen genutzt  
 3436 werden, soll unter Berücksichtigung der technisch vorhandenen Möglichkeiten und unter Wahrung  
 3437 des Betriebs- und Geschäftsgeheimnisses eine Rückverfolgbarkeit für den Betroffenen geschaffen  
 3438 werden. Dies könnte die Geltendmachung der Rechte auf Auskunft, Löschung, Sperrung oder  
 3439 Widerspruch weiter erleichtern.

3440

3441 Die Enquete-Kommission empfiehlt zudem eine Befassung des Deutschen Bundestages mit der Frage  
 3442 der Ausübung und weiteren Stärkung von Betroffenenrechten im Bundesdatenschutzgesetz  
 3443 (vergleiche §§ 33 ff. BDSG), insbesondere ob verantwortliche Stellen zu einer besseren und  
 3444 verständlicheren Information der Betroffenen über die Verwendung der Daten bei der Erhebung  
 3445 verpflichtet werden können und ob eine effektivere Ausgestaltung der bereits vorhandene Rechte auf  
 3446 Auskunft, Löschung, Sperrung oder Widerspruch (vergleiche § 4 Abs. 2 und 4 BDSG) denkbar ist.  
 3447 Dabei sollte dem Einsatz moderner Technologien (etwa dem Recht auf elektronische Auskunft über  
 3448 die gespeicherten Daten und einem elektronischen Widerspruchsrecht) besondere Bedeutung  
 3449 zukommen. Denn die Geltendmachung der Betroffenenrechte sollte auf die gleiche Art möglich sein,  
 3450 wie in die Datenerhebung eingewilligt wurde, bei Angeboten im Internet konsequenterweise auch  
 3451 elektronisch.

3452

3453

3454 *Alternativer und teilweise ergänzender (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE.*  
 3455 *und BÜNDNIS 90/DIE GRÜNEN.*

3456 **Grundprinzipien des Datenschutzrechts/Änderungsbedarf Bundesdatenschutzgesetz**  
 3457 **(Modernisierung, Vereinfachung, Sprache)**

3458 Die Grundprinzipien des deutschen Datenschutzes wurden in Kapitel 2.1 dieses Berichts dargestellt.  
 3459 Wie die Enquete-Kommission in ihrer Beschreibung jedoch feststellt, werden diese Prinzipien in  
 3460 vielen Konstellationen nicht beachtet beziehungsweise nachrangig zu anderen Interessen gestellt.

3461

3462 Sie gibt deshalb dem Deutschen Bundestag nachfolgende Handlungsempfehlungen:<sup>289</sup>

3463 1. die ins Stocken gekommene Modernisierung des unübersichtlichen Datenschutzrechts  
 3464 fortzusetzen. Das Ziel der Modernisierung muss eine deutliche Vereinfachung und Integration  
 3465 datenschutzrechtlicher Bestimmungen sein, wobei das bestehende Schutzniveau nicht abgesenkt  
 3466 werden darf. Dieses Ziel wird nur dann verwirklicht werden können, wenn das geltende

<sup>289</sup> Der nachfolgende Katalog umfasst in der eingereichten Textfassung 20 Punkte. Um für die Beratung und Abstimmung eine Gegenüberstellung mit entsprechenden Textpassagen der Fraktionen CDU/CSU und FDP zu ermöglichen, werden in der vorliegenden Textfassung drei Punkte (betreffend Nr. 12 Koppelungsverbot, Nr. 14 Datenbrief, Nr. 18 Lokalisierungsdaten) weiter unten aufgeführt.

- 3467 Datenschutzrecht um neue Datenschutzzinstrumente ergänzt wird. Hierbei wird der  
3468 Implementierung eines Datenschutzes durch Technik große Bedeutung zukommen;
- 3469 2. zu überprüfen, inwieweit es einer Weiterentwicklung der Grundbegriffe und der bestehenden  
3470 Dogmatik des Datenschutzrechts bedarf, insbesondere im Hinblick auf eine bessere Abgrenzung  
3471 der Begriffe Daten, Informationen und Wissenskontext sowie die der sich daraus ergebenden  
3472 Konsequenzen. Dies ist geboten, weil ein allein auf Daten bezogenes und individualistisches  
3473 Verständnis des Datenschutzrechts unsachgerecht schutzverkürzend wirken kann;
- 3474 3. ein allgemeines, nicht subsidiäres Gesetz für einen modernen Datenschutz zu verabschieden, das  
3475 unter Vermeidung von Doppelregelungen eine klare Abgrenzung zwischen allgemeinen und  
3476 bereichsspezifischen Regelungen erlaubt. Wenn möglich, soll es zu einem Verzicht, jedenfalls zu  
3477 einer Reduzierung, bereichsspezifischer Regelungen führen. Das Gesetz soll darüber hinaus auch  
3478 allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation,  
3479 zur Datenschutzkontrolle und zur Selbstregulierung enthalten. Zudem soll es weitaus stärker auf  
3480 die bereits im Gesetz verankerten Grundprinzipien Datensparsamkeit und Datenvermeidung  
3481 setzen;
- 3482 4. bei der Erarbeitung eines allgemeinen Datenschutzgesetzes die zur Verwirklichung der  
3483 informationellen Selbstbestimmung wesentlichen Schutzziele, wie Datensparsamkeit und  
3484 Datenvermeidung, Datensicherheit, Zweckfestlegung und –bindung, Systemdatenschutz,  
3485 Transparenz, Gestaltungsrechte (Auskunfts-, Widerspruchs-, Benachrichtigungs-, Korrektur- und  
3486 Lösungsrechte), Nichtverkettbarkeit (als technische Sicherung der Zweckbindung) sowie  
3487 Interventionsrechte (als technische Gestaltung von Verfahren zur Ausübung der  
3488 Betroffenenrechte)<sup>290</sup>, als übergreifende Grundprinzipien voranzustellen;
- 3489 5. dass die allgemeinen Datenschutzgrundsätze gleichermaßen für den öffentlichen und für den  
3490 nicht-öffentlichen Bereich gelten sollten;
- 3491 6. den Zweckfestlegungs- beziehungsweise Zweckbindungsgrundsatz in Verbindung mit dem  
3492 Erforderlichkeitsgrundsatz durch eine eigene Norm hervorzuheben und zu konkretisieren. Dabei  
3493 sollten auch Vorgaben für die Änderung bei Zweckfestlegung und Zweckbindung klar geregelt  
3494 sein. In diesem Zusammenhang müssen Regelungen erarbeitet werden, nach denen es  
3495 Nutzerinnen und Nutzern möglich ist, auch in der vernetzten Welt die Kontrolle über die  
3496 Verwendung ihrer persönlichen Daten ausüben zu können;
- 3497 7. zu prüfen, inwieweit Sanktionen bei Verstößen gegen den Zweckfestlegungs- beziehungsweise  
3498 Zweckbindungsgrundsatz eingeführt werden sollten. Den Aufsichtsbehörden muss ermöglicht  
3499 werden, gegen Unternehmen, die nachgewiesenermaßen anlasslos oder zweckwidrig Daten  
3500 erheben, speichern, verarbeiten und nutzen, wirkungsvolle Sanktionen zu verhängen. In diesem  
3501 Zusammenhang ist die bereits im BDSG verankerte Löschungspflicht zu betonen. Ein

<sup>290</sup> 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.

- 3502 Verwertungsverbot für Daten, die durch rechtswidrige Änderung des ursprünglichen  
3503 Erhebungszwecks erlangt worden sind, sollte gesetzlich verankert werden. Regelungsbedarf  
3504 besteht etwa im Hinblick auf die Verwertung von unrechtmäßig erlangten Daten in  
3505 Gerichtsprozessen;
- 3506 8. dass die Informationspflichten privater Anbieter gegenüber Nutzerinnen und Nutzern erweitert  
3507 und die Auskunftsansprüche der Nutzerinnen und Nutzern gegenüber Anbietern gestärkt werden;
- 3508 9. die Informationspflichten sowohl öffentlicher als auch nicht-öffentlicher Stellen gegenüber den  
3509 Betroffenen bei Datenpannen zu erweitern;
- 3510 10. dass, um Unsicherheiten bei der Festlegung der Verantwortlichkeit von vornherein zu vermeiden,  
3511 die Formulierung „Daten verarbeitende (beziehungsweise speichernde) Stelle“ dem Wortlaut der  
3512 Europäischen Datenschutzrichtlinie angepasst wird („die natürliche oder juristische Person,  
3513 Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die  
3514 Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“). Darüber  
3515 hinaus bedarf es einer gesetzlichen Klärung für die zunehmenden Konstellationen, bei denen eine  
3516 Vielzahl von Beteiligten die Datenverarbeitung durchführen;
- 3517 11. die Informationspflichten darüber hinaus wie folgt zu erweitern:
- 3518 a. durch klare und eindeutige Offenlegung der Verantwortlichkeit für die Datenverarbeitung bei  
3519 mehreren Stellen gegenüber den Betroffenen;
- 3520 b. durch prominente Platzierung der datenschutzrechtlich verantwortlichen Stelle und der  
3521 zuständigen Datenschutzbehörde;
- 3522 c. durch eine Verpflichtung der verantwortlichen Stelle, Herkunft und Empfänger von Daten zu  
3523 dokumentieren sowie Datenbankzugriffe zu protokollieren, wenn personenbezogene Daten an  
3524 Dritte weitergegeben werden;
- 3525 d. durch eine gesetzliche Festschreibung der Möglichkeit, Widerspruchsrechte ohne Medienbrüche  
3526 auszuüben. Die Ausübung des Widerspruchsrechts wird von den Anbietern bisweilen absichtlich  
3527 erschwert. Häufig lassen sie einen Widerspruch gegen die Datenerhebung nur schriftlich zu,  
3528 während die Einwilligung in die Erhebung durchaus auf elektronischem Wege erteilt werden  
3529 kann;
- 3530 *[Nr. 12 siehe Zeile 3597]*
- 3531 13. eine Befassung des Deutschen Bundestages mit der Frage, wie Betroffenenrechte im  
3532 Bundesdatenschutzgesetz gestärkt werden können (vergleiche §§ 33 ff. BDSG). Dabei sollte dem  
3533 Einsatz moderner Technologien (etwa dem Recht auf elektronische Auskunft über die  
3534 gespeicherten Daten und einem elektronischen Widerspruchsrecht) besondere Bedeutung  
3535 zukommen. Die Auskunftsrechte der Betroffenen sind zu vereinfachen und bürgerfreundlicher  
3536 auszugestalten,
- 3537 a. durch entsprechende Bereitstellung technischer Mittel, die die Wahrnehmung der Rechte  
3538 vereinfachen;

- 3539 b. durch eine Einführung eines allgemeinen Rechts auf elektronische Auskunft, u. a. im Hinblick auf  
 3540 die Verknüpfung beziehungsweise Zusammenführung von Daten sowie die über den eigentlichen  
 3541 Zweck der Erhebung hinausgehende Nutzung;
- 3542 c. durch eine Verpflichtung der Anbieter, Nutzerinnen und Nutzer über Änderungen der für das  
 3543 betreffende Angebot geltenden Datenschutzbedingungen effektiv zu informieren;
- 3544 *[Nr. 14 siehe Zeile 3619]*
- 3545 15. dass das Auskunftsrecht sich auch auf Datenverkettungen beziehen sollte. Welche persönlichen  
 3546 Daten bei einem bestimmten Anbieter mit anderen verknüpft werden und nach welchen  
 3547 Selektionskriterien dies geschieht, können datenschutzbewusste Nutzerinnen und Nutzer derzeit  
 3548 nicht in Erfahrung bringen;
- 3549 16. sicherzustellen, dass Betroffene, deren personenbezogene Daten an Dritte übermittelt werden,  
 3550 über den tatsächlichen Empfänger ihrer Daten informiert werden müssen. Wenn  
 3551 personenbezogene Daten an Dritte übermittelt werden, muss der Betroffene bislang lediglich über  
 3552 die „Kategorien von Empfängern“ (§ 33 Abs. 1 BDSG) unterrichtet werden. Er erfährt jedoch  
 3553 nicht, wer seine Daten tatsächlich bekommen hat. Dieser Missstand wäre mit einer schlichten  
 3554 Formulierungsänderung im Gesetz leicht zu beheben. Verstöße gegen diese Regelung könnten  
 3555 zudem mit einem Bußgeld belegt werden;
- 3556 17. die Formulierung einer einheitlichen allgemeinen technunabhängigen Vorschrift zur  
 3557 transparenten Datenerhebung, -verarbeitung und -nutzung, die u. a. folgende Punkte regelt:
- 3558 a. ein grundsätzliches Verbot der unbemerkten Datenerhebung mit Sanktionen im Falle des  
 3559 Verstoßes;
- 3560 b. eine Informationspflicht gegenüber den Betroffenen über die Funktionsweise und Art der  
 3561 Datenerhebung, die Identität der verantwortlichen Stelle sowie Rechte der Betroffenen.
- 3562 *[Nr. 18 siehe Zeile 4254]*
- 3563 19. für die Betroffenen eine Anspruchsnorm mit Sanktionierung bei Nichtbeachtung zu schaffen, die  
 3564 die verantwortliche Stelle dazu verpflichtet, ihre Systeme und Verfahren so auszurichten, dass nur  
 3565 Daten erhoben werden, die auch erforderlich sind;
- 3566 20. entsprechend der europäischen Datenschutzrichtlinien gleiche Regeln für öffentliche und nicht-  
 3567 öffentliche Stellen zu schaffen und dabei verbindliche datenschutzrechtliche Mindeststandards  
 3568 festzuschreiben. Dies begründet sich, neben zahlreichen weiteren Argumenten, auch in dem als  
 3569 zunehmend problematisch erscheinenden Umgang mit öffentlich zugänglichen  
 3570 personenbezogenen Daten. Darf beispielsweise die Polizei Daten über Demonstrationsteilnehmer  
 3571 in sozialen Netzwerken recherchieren und unbeschränkt miteinander verknüpfen?  
 3572 Personenbezogene Daten, welche aus „allgemein zugänglichen Quellen“ stammen oder vom  
 3573 Betroffenen „zur Veröffentlichung vorgesehen“ sind, dürfen nach derzeitiger Rechtslage erhoben  
 3574 werden. Aufgrund der besonderen Gefahren, die die Erhebung solcher Daten allein schon durch  
 3575 die Möglichkeit der nachfolgenden Verkettung mit sich bringt, erscheint dies unbefriedigend. Die

3576 Privilegierung öffentlich zugänglicher Daten sollte auf solche Verwendungen eingeschränkt  
 3577 werden, die im offensichtlichen oder erklärten Interesse des Betroffenen liegen beziehungsweise  
 3578 diesem nicht widersprechen. Die Unterscheidung zwischen öffentlichen und nicht-öffentlichen  
 3579 Regeln im Datenschutz ist nicht mehr zeitgemäß. Zur Einhaltung datenschutzrechtlicher  
 3580 Mindeststandards für den öffentlichen und nicht-öffentlichen Bereich sollten effektive und  
 3581 abschreckende Sanktionen festgelegt werden. Ebenfalls angebracht scheint eine Erweiterung der  
 3582 Bußgeldtatbestände, insbesondere für unbefugte Datennutzung und unzulässige Beobachtung  
 3583 (Videoüberwachung).

3584

3585 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
 3586 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3587 **Koppelungsverbot**

3588 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, am bestehenden Koppelungsverbot in  
 3589 § 28 Abs. 3b BDSG festzuhalten. Die bisherige Regelung verbietet es, den Vertragsschluss von der  
 3590 Angabe personenbezogener Daten abhängig zu machen, wenn ein anderer Zugang zu gleichwertigen  
 3591 Angeboten und Diensten ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist, also  
 3592 wenn Unternehmen eine marktbeherrschende Stellung haben. Sie stellt einen ausgewogenen  
 3593 Ausgleich zwischen den zu berücksichtigenden Interessen der Nutzer und der Unternehmen dar. Eine  
 3594 Ausweitung des Koppelungsverbot würde letztlich zu einem vollständigen und damit unnötigen,  
 3595 mithin einem unverhältnismäßigen, gesetzlichen Verbot von Diensten führen.

3596

3597 *Alternativer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
 3598 *GRÜNEN.*

3599 [*Die Enquete-Kommission gibt dem Deutschen Bundestag nachfolgende Handlungsempfehlung,*]

3600 [12.] das so genannte Koppelungsverbot auch auf solche Unternehmen und Dienste auszuweiten, die  
 3601 keine marktbeherrschende Stellung haben. Nach geltender Rechtslage darf der Abschluss eines  
 3602 Vertrages (etwa bei der Nutzung von Internetdiensten) nicht an eine Einwilligung gekoppelt  
 3603 werden, die eine über die Dienstleistung hinausgehende Datenerhebung und –nutzung erlaubt.  
 3604 Dies gilt allerdings nur für solche Unternehmen, die eine marktbeherrschende Stellung innehaben.

3605



3606

3607 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
 3608 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3609 **Datenbrief**

3610 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, ein Datenbrief-Konzept nicht weiter  
 3611 in Erwägung zu ziehen. Der Datenbrief entspräche nicht dem Grundsatz der Datensparsamkeit  
 3612 (vergleiche § 3a BDSG). Für die Zustellung des Datenbriefes wären zumindest die Adresse des  
 3613 betroffenen Nutzers oder andere Kontaktdaten erforderlich, die für den eigentlich in Anspruch  
 3614 genommenen Dienst eventuell gar nicht anfallen würden. Die Daten des Betroffenen müssten  
 3615 möglicherweise zentral – mit erhöhtem Aufwand für die Datensicherheit – in einer Datenbank geführt  
 3616 und laufend aktualisiert werden. Es besteht das Risiko, dass selbst sensible Daten der Betroffenen an  
 3617 unberechtigte Dritte gelangen. Der bürokratische Aufwand aller Beteiligten steht in keinem Verhältnis  
 3618 zum erwarteten Nutzen.

3619 *Alternativer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
 3620 ***GRÜNEN.***

3621 *[Die Enquete-Kommission gibt dem Deutschen Bundestag nachfolgende Handlungsempfehlung,]*

3622 [14.]Konzepte wie den vom Chaos Computer Club (CCC) vorgeschlagenen Datenbrief, der  
 3623 Unternehmen verpflichtet, in regelmäßigen Abständen Bürgerinnen und Bürger über ihre bei den  
 3624 Unternehmen gespeicherten persönlichen Daten zu unterrichten, in die Überlegungen für eine  
 3625 Stärkung der informationellen Selbstbestimmungsrechte einzubeziehen. Der Datenbrief ist  
 3626 kritisch zu bewerten, wenn und soweit damit eine eigene Sammlung und Zusammenführung von  
 3627 Daten zu Personen verbunden ist und ein nicht zu bewältigender Aufwand für die betroffenen  
 3628 Unternehmen droht. Diesen Problemen muss in der Ausgestaltung eines Konzeptes wie des  
 3629 Datenbriefs Rechnung getragen werden.

3630

3631 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, Textvorschlag der Fraktionen SPD,*  
 3632 *DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3633 **Anonyme Bezahlssysteme**

3634 Mit dem technischen Fortschritt nimmt auch der elektronische Zahlungsverkehr im Internet zu.  
 3635 Zunehmend werden alltägliche Einkäufe im Internet abgewickelt. Hierbei fallen auch eine Vielzahl  
 3636 personenbezogener Daten an. Die Einführung eines digitalen Bargeldes könnte jedoch zu einer  
 3637 Reduzierung der personenbezogenen Daten im Zahlungsverkehr des Internets führen. Darüber hinaus  
 3638 würde eine Einführung des digitalen Bargeldes eine Annäherung an alltägliche Barzahlungsgeschäfte  
 3639 in der „realen Welt“ fördern. Sie bietet allerdings auch Risiken, da ein weitestgehend anonymer  
 3640 Zahlungsverkehr zugleich eine Erleichterung für die Begehung von Straftaten sein könnte und damit  
 3641 das Internet als Tatmittel missbraucht würde. Internationale Lösungen sollten daher dann unterstützt  
 3642 werden, wenn sie Chancen und Risiken eines solchen Bezahlungssystems in einen angemessenen  
 3643 Ausgleich setzen. Die Enquete-Kommission regt daher gegenüber der Bundesregierung an,

3644 entsprechende Forschungsvorhaben, die sich mit der Einführung eines digitalen Bargelds  
3645 auseinandersetzen, positiv zu begleiten.

3646

3647 *Weiterer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
3648 *GRÜNEN.*

3649 **Anonymität und Pseudonymität**

3650 Die Enquete-Kommission hat in ihrer Bestandsaufnahme festgestellt, dass auch eine anonyme und  
3651 pseudonyme Nutzung des Internets zur Ausübung des Rechts auf informationelle Selbstbestimmung  
3652 gehören kann. Deshalb empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

3653

- 3654 1. durch gesetzgeberische Maßnahmen zur Stärkung der Möglichkeit der anonymen Nutzung  
3655 elektronischer Medien den Datenschutz zu verbessern;
- 3656 2. die allgemeine gesetzliche Verpflichtung der Dienstleister, anonyme und pseudonyme  
3657 Nutzungsmöglichkeiten von Internetdiensten anzubieten, weiter zu stärken. Verstöße gegen die  
3658 Möglichkeit und Wahrung von Pseudonymität und Anonymität sollten ferner sanktioniert werden  
3659 können.

3660

3661 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
3662 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3663 **Technischer Datenschutz**

3664 Datenschutz lässt sich in der Praxis nur dann sicherstellen, wenn die informationstechnischen Systeme  
3665 im öffentlichen und nicht-öffentlichen Bereich gegen unberechtigten Zugriff und missbräuchliche  
3666 Nutzung von innen und außen geschützt sind. Die hierfür einschlägigen Schutzregelungen (zum  
3667 Beispiel die Anlage zu § 9 BDSG) stammen aus einer Zeit, als Datenverarbeitung durch Großrechner  
3668 in abgeschotteten Rechenzentren gekennzeichnet war.

3669

3670 Beispielsweise kommen im Zuge des E-Government längst Onlineverfahren zum Einsatz, bei denen  
3671 Bürger selbst auf die IT-Systeme der Verwaltung zugreifen. Durch diese Entwicklung und die  
3672 fortschreitende Vernetzung der Verwaltungssysteme untereinander wird es zunehmend schwieriger,  
3673 das Regelwerk auf neue Technologien und vernetzte Infrastrukturen anzuwenden. Die Enquete-  
3674 Kommission hält es für erforderlich zu prüfen, ob die technisch-organisatorischen Maßnahmen zur  
3675 Sicherstellung des Datenschutzes (Anlage zu § 9 BDSG und entsprechende Regelungen in den  
3676 Datenschutzgesetzen der Länder) durch technikneutrale Schutzziele ersetzt werden müssen, die dann  
3677 durch dokumentierte Rahmen- und Verfahrenskonzepte umgesetzt und dem aktuellen Stand der  
3678 Technik entsprechend fortgeschrieben werden müssten.

3679

3680 *Alternativer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
3681 *GRÜNEN.*

3682 **Technischer Datenschutz**

3683 Die Enquete-Kommission hat in ihrem Bericht festgestellt, dass die aktuellen Rechtsnormen oft nicht  
3684 mehr geeignet sind, Datensicherheit und Datenschutz zu gewährleisten, weil sie weder zeitgemäß sind  
3685 noch technikneutral formuliert sind. Sie hat auch festgehalten, dass eine technikneutrale Formulierung  
3686 zum Beispiel anhand von Schutzziele – wie dies die Konferenz der Datenschutzbeauftragten des  
3687 Bundes und der Länder empfiehlt – geeignet sein kann, gesetzliche Normen trotz der ständigen  
3688 technischen Weiterentwicklung beständiger zu gestalten.

3689 Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

3690 1. die technischen und organisatorischen Maßnahmen (im Sinne der Anlage zu § 9 BDSG) zu  
3691 reformieren, indem die Definitionen der elementaren Schutzziele aufgenommen werden, so dass  
3692 sich daraus einfache, flexible und praxistaugliche Maßnahmen ableiten lassen.

3693

3694 2. Bei der Definition der Schutzziele sollten folgende Punkte beachtet werden:

3695 a. Die Schutzziele sollten einfach, verständlich, praxistauglich und technologieunabhängig formuliert  
3696 sein;

3697 b. Maßgabe bei der Definition sollten in erster Linie die Vorgaben des Datenschutzes sein, nicht  
3698 Vorgaben zur IT-Sicherheit;

3699 c. Die Umsetzung muss frühzeitig ansetzen und durch entsprechende Maßnahmen (wie etwa  
3700 Risikoanalysen und Sicherheitskonzepte, die vor Freigabe des Verfahrens vorgelegt und  
3701 fortgeschrieben werden müssen) abgesichert werden.

3702

3703

3704 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
 3705 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3706

3707 **Datenschutz für Kinder und Jugendliche**

3708 Aktuelle Studien zeigen, dass viele Kinder und Jugendliche mit der Nutzung moderner Technik  
 3709 bereits sicher und selbstverständlich umgehen können. Dennoch hält die Enquete-Kommission auch  
 3710 für die Zukunft ein verstärktes Bemühen um Aufklärung und Bildung im Bereich des Datenschutzes  
 3711 für geboten. Vielversprechende Bildungsangebote staatlicher sowie nicht-staatlicher Organisationen  
 3712 liegen hierzu bereits vor. Es gilt daher, diese Angebote noch sichtbarer für die Nutzerinnen und  
 3713 Nutzer zu machen. Die Enquete-Kommission sieht bei der Stärkung des Selbstdatenschutzes von  
 3714 Kindern und Jugendlichen auch die Länder aufgrund ihrer Zuständigkeit für den Bildungsbereich in  
 3715 der Pflicht.

3716 Unternehmen, die Dienste im Internet anbieten, können die Einwilligungsfähigkeit von  
 3717 Minderjährigen bisher nur schwer feststellen. Die Enquete-Kommission empfiehlt daher der  
 3718 Bundesregierung, die gesetzlichen Voraussetzungen der Einwilligungsfähigkeit von Minderjährigen  
 3719 zu überprüfen. In die vorzunehmende Prüfung sollte die bisher maßgebliche Einsichtsfähigkeit, aber  
 3720 auch die Möglichkeit einer festen Altersgrenze einbezogen werden. Dabei ist zu beachten, dass die  
 3721 Informations- und Kommunikationsrechte von Minderjährigen auch in Zukunft gewahrt bleiben.

3722

3723 *Alternativer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
 3724 *GRÜNEN.*

3725 **Datenschutz für Kinder und Jugendliche**

3726 Die Enquete-Kommission stellt fest, dass es verschiedene schutzwürdige Gruppen im Bereich des  
 3727 Datenschutzes gibt. Dabei ist besonders die Gruppe der Kinder und Jugendlichen hervorzuheben, weil  
 3728 sie aufgrund ihrer (noch) nicht ausreichenden Einsichtsfähigkeit in der digitalen  
 3729 Informationsgesellschaft besonders schutzwürdig sind.

3730 Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

- 3731 1. mit klaren gesetzlichen Regelungen festzulegen, ab wann und unter welchen Voraussetzungen  
 3732 Minderjährige eigenständig einwilligen und ihre Betroffenenrechte wahrnehmen können;
- 3733 2. allgemein gesetzlich festzulegen, dass bei Angeboten für Kinder und Jugendliche die Erhebung  
 3734 von personenbezogenen Daten auf das erforderliche Mindestmaß für die Dienstleistung  
 3735 beschränkt bleiben muss. Zuwiderhandlungen beziehungsweise Verstöße müssen besonders stark  
 3736 sanktioniert werden;
- 3737 3. zu prüfen, inwieweit darüber hinaus spezielle Datenschutzregelungen für Kinder und Jugendliche  
 3738 getroffen werden müssen, zum Beispiel im Hinblick auf den Bereich der sozialen Netzwerke oder  
 3739 bei Kaufangeboten wie Onlinespielen, Klingeltönen etc.;

- 3740 4. Anbieter von Onlinediensten, die von Kindern und Jugendlichen genutzt werden, zu verpflichten,  
 3741 die Hinweise zum Datenschutz so verständlich zu machen, dass Kinder und Jugendliche diese  
 3742 auch verstehen. So könnten beispielsweise die AGB und die Datenschutzerklärungen neben den  
 3743 juristisch verbindlichen Textversionen in leicht verständlichen Versionen angeboten werden;  
 3744 5. auf die Einführung eines allgemein gültigen Datenschutzgütesiegels hinzuwirken, speziell zur  
 3745 Orientierung für Kinder und Jugendliche, wie es der Bundesbeauftragte für den Datenschutz und  
 3746 die Informationsfreiheit bereits gefordert hat. Dies könnte zum Beispiel durch die Stiftung  
 3747 Datenschutz vergeben werden;  
 3748 6. sich für eine Stärkung der Medienkompetenz durch Bildungsangebote, etwa der Stiftung  
 3749 Datenschutz, einzusetzen. Es ist notwendig, das Bewusstsein für den Schutz eigener und fremder  
 3750 Daten bei Kindern und Jugendlichen zu entwickeln und zu fördern;  
 3751 7. Anbieter von Internetdiensten zu verpflichten, etwaig erstellte Persönlichkeitsprofile zu löschen  
 3752 und die über die Kinder bekannten Informationen umgehend zu anonymisieren, sobald diesen  
 3753 Anbietern das Alter eines minderjährigen Kindes bekannt wird;  
 3754 8. Anbietern von Internetdiensten die Weitergabe und den Weiterverkauf von Daten von Kindern  
 3755 und Jugendlichen sowie Profilen von minderjährigen Nutzerinnen und Nutzern zu untersagen;  
 3756 9. die Erhebung und Erstellung von Persönlichkeits-, Konsum- und Vorliebenprofilen von  
 3757 minderjährigen Nutzerinnen und Nutzern grundsätzlich zu untersagen.
- 3758 Hinsichtlich weiterer entsprechender Handlungsempfehlungen wird auf die Projektgruppe  
 3759 Medienkompetenz der Enquete-Kommission verwiesen.

3760

3761 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
 3762 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

### 3763 **Profilbildung**

3764 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag zu prüfen, ob die Bildung bestimmter  
 3765 personenbezogener Profile gesetzlich zu regeln ist. Dabei könnten bestimmte Profilbildungen von  
 3766 einer ausdrücklichen gesetzlichen Regelung oder aber der Einwilligung der Betroffenen abhängig  
 3767 gemacht werden.

3768 Insbesondere durch Berechnungen, Vergleiche und statistische Korrelationssoftware können in  
 3769 bestimmten Fällen personenbezogene Daten, die Unternehmen im Rahmen von Internetdiensten  
 3770 erhoben haben, zu umfassenden Profilen zusammengeführt und zu vielfältigen Zwecken genutzt  
 3771 werden. Durch solche Profile können in einigen Bereichen Verhalten, Gewohnheiten und Neigungen  
 3772 eines Nutzers abgebildet und kategorisiert werden, ohne dass es diesem zuvor offen gelegt wird.

3773 Für bestimmte Profilbildungen sind daher eine gesetzliche Definition dieses Begriffs sowie  
 3774 Regelungen zum Umgang mit ihnen zu erwägen. Dabei ist zu berücksichtigen, dass nicht jede  
 3775 Verknüpfung von Informationen mit einer natürlichen Person zu einem schwerwiegenden Eingriff in  
 3776 das informationelle Selbstbestimmungsrecht führt und eine gesetzliche Regelung erfordert. Wichtig ist  
 3777 daher, für diese Fälle eine klare Unterscheidung zu treffen. Transparenz für Betroffene und  
 3778 Informationen über Umfang sowie Herkunft der Profildaten und die beabsichtigte Verwendung des

3779 Profils sind notwendig. Diese Ziele könnten auch mit Hilfe von Selbstverpflichtungen erreicht  
3780 werden.

3781

3782 *Alternativer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
3783 *GRÜNEN.*

3784 **Profilbildung**

3785 Die Enquete-Kommission stellt in ihrem Bericht fest, dass die Zusammenführung und Verknüpfung  
3786 personenbezogener Daten zu Profilen (wie zum Beispiel durch das so genannte Behavioral Targeting)  
3787 eine besondere Gefahr für das Persönlichkeitsrecht darstellen kann. Durch solche Techniken können  
3788 das Verhalten, die Interessen und die Gewohnheiten eines Menschen vorhersehbar gemacht werden,  
3789 was nicht zuletzt eine gezielte Manipulation ermöglicht, unabhängig davon, ob dies zu Werbe- oder  
3790 sonstigen Zwecken erfolgt.

3791 Aufgrund des Gefährdungspotentials empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

- 3792 1. die Schaffung einer gesetzlichen Definition der Profilbildung und deren grundsätzliches, gesetzlich  
3793 verankertes Verbot mit einem allgemeinen Ermächtigungsvorbehalt sowie die Schaffung von  
3794 gesetzlichen Ausnahmen, die nur zulässig sind, wenn sie dem besonderen Gefährdungspotential  
3795 Rechnung tragen oder durch freiwillige, aktive und informierte Einwilligung der Betroffenen  
3796 legitimiert sind. Diese Einwilligung setzt eine umfassende Information über Umfang und Herkunft  
3797 der verwandten Daten, Zweck und Verwendung des Profils, die verantwortliche Stelle und die  
3798 vorgesehene Lösungsfrist voraus. Die Einwilligung muss freiwillig und jederzeit widerrufbar  
3799 sein. Der Widerruf muss die sofortige Löschung des Profils zur Folge haben, auch bei den Stellen,  
3800 an die es übermittelt worden ist;
- 3801 2. angesichts des umfassenden und weit verbreiteten Einsatzes von Instrumenten zum Zwecke des  
3802 Behavioral Targeting Initiativen zu unterstützen, die eine anbieterunabhängige, aktive Information  
3803 der Öffentlichkeit über Funktionsweisen, eingesetzte Techniken, mögliche Schutzmechanismen  
3804 sowie die derzeitigen rechtlichen Regelungen zum Inhalt haben;
- 3805 3. die Webseitenbetreiber ebenso wie Werbewirtschaftsunternehmen zu verpflichten, verständlich und  
3806 leicht einsehbar über die konkret eingesetzten Analyse-Techniken zu informieren und die  
3807 Möglichkeit einer begrenzten Einwilligung aufzuzeigen.

3808

3809 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
 3810 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3811 **Veröffentlichung von Daten im Internet**

3812 Bei der Veröffentlichung von personenbezogenen Daten im Internet sind in der Regel immer mehrere  
 3813 Grundrechte in einen angemessenen Ausgleich zu bringen. Neben dem Grundrecht auf informationelle  
 3814 Selbstbestimmung sind dies beispielsweise auch das Grundrecht auf Meinungsfreiheit und das  
 3815 Grundrecht auf Informationsfreiheit. Aber auch die Freiheit der Berichterstattung und das  
 3816 Informationsinteresse der Allgemeinheit können zu berücksichtigen sein. Gesetzliche Regelungen für  
 3817 diesen Bereich können mithin nur eine Konkretisierung verfassungsrechtlicher Grenzen darstellen.  
 3818 Die Enquete-Kommission empfiehlt daher der Bundesregierung, diesen Bereich weiterhin sorgfältig  
 3819 zu beobachten und den Schutz vor schwerwiegenden Eingriffen in das Persönlichkeitsrecht  
 3820 sicherzustellen.

3821 Widerspruchsrechte gegen bestimmte Veröffentlichungen im Internet, die vorrangig auf der Basis von  
 3822 Selbstverpflichtungen von Plattformbetreibern umgesetzt werden könnten, können ein wirksames  
 3823 Mittel zur Wahrung des Grundrechts auf informationelle Selbstbestimmung sein. Allerdings muss es  
 3824 auch hierbei zu einer angemessenen Berücksichtigung verschiedener, möglicherweise auch  
 3825 gegenläufiger, Interessen kommen. Dies muss durch entsprechende verfahrensrechtliche Regelungen  
 3826 abgesichert sein. Bereits bestehende Widerspruchsregelungen (vergleiche § 35 Abs. 5 BDSG, Art. 14  
 3827 Datenschutzrichtlinie) sind mit einzubeziehen.

3828

3829 *Alternativer (streitiger) Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
 3830 ***GRÜNEN.***

3831 **Veröffentlichung von Daten im Internet**

3832 Mit der Verbreitung von so genannten Web 2.0 Anwendungen wird die Veröffentlichung von  
 3833 personenbeziehbaren Informationen insbesondere durch andere Privatpersonen im Rahmen der  
 3834 Nutzung zum Beispiel von sozialen Netzwerken möglich. Mit dem Wegfall technischer Grenzen der  
 3835 Publizierbarkeit häufen sich Konflikte um Veröffentlichungen, die gegen Persönlichkeitsrechte  
 3836 verstoßen können oder von den Betroffenen aus anderen Gründen abgelehnt werden.

3837 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,

3838 zu prüfen, ob durch ein allgemeines, auch gegenüber den Internetanbietern geltend zu machendes  
 3839 Widerspruchsrecht gegen personenbezogene Internetveröffentlichungen ein wesentlich verbesserter  
 3840 Schutz des Persönlichkeitsrechts der Betroffenen bewirkt werden kann.

3841

3842

3843 *Streitiger Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN<sup>291</sup>.*

3844 **Cloud-Computing**

3845 Die Enquete-Kommission stellt fest, dass das Cloud-Computing zukünftig eine große  
3846 Herausforderung für den Datenschutz darstellt. Deshalb ist es unerlässlich, dass sich die  
3847 Bundesregierung auf internationaler und europäischer Ebene dafür einsetzt, Vereinbarungen und  
3848 Standards zu erreichen, die einem hohen – möglichst deutschen beziehungsweise europäischen –  
3849 Schutzniveau entsprechen.

3850 Darüber hinaus empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

- 3851 1. gesetzliche Regelungen zu schaffen, die datenschutzrechtliche Mindeststandards dafür festlegen,  
3852 unter welchen Umständen personenbezogene beziehungsweise personenbeziehbare Daten  
3853 ausgelagert werden dürfen. Die Nichteinhaltung dieser Mindeststandards muss sanktioniert  
3854 werden;
- 3855 2. weitere gesetzliche Regelungen zu schaffen, die Verantwortlichkeiten und entsprechende  
3856 Dokumentationspflichten über die Auslagerung beziehungsweise Weitergabe von Daten klar  
3857 regeln;
- 3858 3. die Anbieter von Clouds zu verpflichten, Art und Ort der Datenverarbeitung offenzulegen sowie  
3859 Angaben zu den Sicherungsmaßnahmen zu machen;
- 3860 4. eine gesetzliche Regelung zu schaffen, die sicherstellt, dass personenbezogene Daten nur auf  
3861 deutschen beziehungsweise europäischen Servern gespeichert werden dürfen, bei denen ein  
3862 entsprechendes Datenschutzniveau sichergestellt ist.

3863

3864 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer u. teilweise ergänzender*  
3865 *Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3866 **Regulierte Selbstregulierung**

3867 Aus Sicht der Enquete-Kommission ist Selbstregulierung durch die Wirtschaft ein wichtiges  
3868 Instrument des Datenschutzes. Im Vergleich zur Gesetzgebung ist sie flexibler und kann schneller auf  
3869 neue Entwicklungen reagieren. Selbstverpflichtungen der Wirtschaft können darüber hinaus das  
3870 Datenschutzniveau heben, zum Beispiel durch Vorgaben zur Datenvermeidung und Datensparsamkeit.  
3871 Dort, wo sich die Selbstregulierung im Interesse der Nutzerinnen und Nutzer sowie der Unternehmen  
3872 bewährt, ist dann ein Handeln durch den Gesetzgeber nicht notwendig.

3873 Eine zentrale Informations- und Widerspruchsstelle, wie sie beispielsweise der Datenschutz-Kodex  
3874 für Geodatendienste vorsieht und von der – ohne eine zentrale Speicherung – Widersprüche an die  
3875 jeweiligen Unternehmen weitergegeben werden, erleichtert es den Nutzerinnen und Nutzern, ihr

<sup>291</sup> Vergleiche auch die konsensuale Textpassage zum Cloud-Computing, Zeilen 2830 ff.



3876 Widerspruchsrecht auszuüben. Für die Beilegung von Streitigkeiten über die Ausübung von  
 3877 Nutzerrechten kann auf dieser Grundlage eine Schlichtungsstelle Datenschutz zur effektiven  
 3878 unbürokratischen Durchsetzung der gesetzlichen Rechte auf Löschung, Sperrung und Widerspruch  
 3879 beitragen. Diese könnte unter Beteiligung von Wirtschaft und Datenschutzverbänden realisiert  
 3880 werden.

3881

3882 *Alternativer und teilweise ergänzender (streitiger)Textvorschlag der Fraktionen SPD, DIE LINKE.*  
 3883 *und BÜNDNIS 90/DIE GRÜNEN.*

### 3884 **Regulierte Selbstregulierung und Auditierung**

3885 Die Enquete-Kommission stellt fest, dass eine Selbstregulierung im Datenschutz eine wertvolle  
 3886 Ergänzung zu den gesetzlichen Regelungen darstellen kann, weil sie den gerade für den  
 3887 Internetbereich wichtigen Vorzug der Flexibilität und Anpassung an neue Gegebenheiten besitzt. Ein  
 3888 hohes Schutzniveau wird jedoch nur erreichbar sein, wenn die Selbstregulierung in einen gesetzlichen  
 3889 Rahmen eingebunden ist, es sich also der Sache nach um eine Koregulierung handelt. Ein Beispiel  
 3890 bietet § 38a BDSG, der aber bislang mangels Akzeptanz in der Privatwirtschaft noch nicht die  
 3891 beabsichtigte Wirkung entfalten konnte. Reine Selbstregulierungen bleiben sinnvoll und notwendig,  
 3892 wenn es sich unterhalb der gesetzlichen Regelungsziele um freiwillige zusätzliche Bemühungen der  
 3893 Wirtschaft handelt.

3894 Die Enquete-Kommission stellt darüber hinaus fest, dass Datenschutzaudits und  
 3895 Datenschutzgütesiegel ein wesentliches Instrument zur Vertrauensbildung im gegenseitigen Verhältnis  
 3896 von Bürgern, Unternehmen und Staat darstellen können.

3897 Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

- 3898 1. zu prüfen, wie die Integration von selbstregulativen Elementen in das Konzept des  
 3899 Bundesdatenschutzgesetzes verbessert werden kann, ohne das Schutzniveau zu senken. Mit § 38a  
 3900 BDSG existiert zwar eine Norm mit explizit selbstregulativen Elementen, die sogar im Grundsatz  
 3901 sowohl von den Unternehmen als auch von den Datenschutzbeauftragten begrüßt wird, jedoch in  
 3902 der Praxis kaum angewandt wird. Es steht zu vermuten, dass dies an den nicht hinreichend  
 3903 konkret ausgestalteten Verfahren liegt;
- 3904 2. ein Datenschutzauditgesetz gemäß § 9a BDSG zu verabschieden, welches den Unternehmen die  
 3905 Möglichkeit eines Audits auf freiwilliger Basis bietet und dessen Verfahren unbürokratisch, aber  
 3906 verbindlich ausgestaltet sein muss;
- 3907 3. im Rahmen von Vergabegesetzen eine Verpflichtung öffentlicher Stellen zu verankern, solche  
 3908 auditierten beziehungsweise zertifizierten Produkte bevorzugt einzusetzen. Soweit keine  
 3909 Vergabegesetze bestehen, ist im Rahmen der Ausschreibungen zu berücksichtigen, dass  
 3910 besonders datenschutzfreundliche Produkte bevorzugt eingekauft oder genutzt werden.

3911

3912

3913 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
 3914 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

3915 **Stiftung Datenschutz**

3916 Die Enquete-Kommission ist der Ansicht, dass die Errichtung einer Stiftung Datenschutz mit dem  
 3917 Auftrag, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, ein  
 3918 Datenschutzaudit zu entwickeln und Bildung im Bereich des Datenschutzes zu stärken, den  
 3919 Selbstdatenschutz durch Aufklärung verbessern kann. Sie begrüßt daher im Grundsatz die von der  
 3920 Bundesregierung geplante Stiftung Datenschutz.

3921 Diese Stiftung kann u. a. Kriterien für die Zertifizierung von Diensten sowie für ein einheitliches  
 3922 Gütesiegel aufstellen und damit eine leicht nachzuvollziehende Vergleichbarkeit für Unternehmen und  
 3923 Bürger herstellen. Dadurch kann sich auch eine Erleichterung bei der Auswahl zwischen einer  
 3924 Vielzahl von Anbietern ergeben und zugleich das Vertrauen der Bürger in neue Technologien gestärkt  
 3925 werden. Für Unternehmen kann sie Anreize setzen, hohe datenschutzrechtliche Anforderungen  
 3926 einzuhalten.

3927 Weitere Aufgaben können die Stärkung des Selbstdatenschutzes sowie Aufklärung und Bildung im  
 3928 Datenschutz sein.

3929 Die Enquete-Kommission fordert daher die Bundesregierung bei Errichtung der Stiftung auf, folgende  
 3930 Punkte – die für eine wirkungsvolle Arbeit einer Stiftung Datenschutz mit vorstehendem Auftrag von  
 3931 großer Bedeutung sind – zu berücksichtigen:

- 3932 1. Die Stiftung ist mit Distanz zu den zu bewertenden Unternehmen zu organisieren. Personell ist  
 3933 darauf zu achten, dass bei der Besetzung der Gremien Unternehmen oder Verbände zwar beteiligt  
 3934 werden, aber auf die Unabhängigkeit der Stiftung an sich keinen Einfluss haben. Dies könnte zum  
 3935 Beispiel durch die Beteiligung in einem Beirat, der beratende Funktion hat, geschehen. Finanziell  
 3936 sollte die Stiftung nicht allein vom Bundeshaushalt abhängig sein. Bei der Annahme von  
 3937 Zuwendungen hat die Stiftung jedoch darauf zu achten, dass ihre Unabhängigkeit nicht gefährdet  
 3938 werden darf.
- 3939 2. Bei der Entwicklung von Gütesiegeln durch die Stiftung ist darauf zu achten, dass ein  
 3940 einheitliches Gütesiegel geschaffen und somit eine inflationäre Handhabung bei der Vergabe  
 3941 vermieden wird. Ebenso ist das Verfahren für die Vergabe transparent zu gestalten. Die  
 3942 Gütesiegel sind nur für eine bestimmte Zeit zu erteilen und müssen überprüfbar sein.
- 3943 3. Im Bereich der Bildung sollte die Stiftung Datenschutz sowohl schulisch als auch außerschulisch  
 3944 tätig sein. Sofern sie im schulischen Bereich tätig wird, sollten durch eine Abstimmung mit den  
 3945 Ländern von Beginn an Zuständigkeitsverletzungen ausgeschlossen werden.
- 3946 4. Im Bereich der Aufklärung wird der Stiftung empfohlen, ein zentrales Informationsportal oder ein  
 3947 virtuelles Datenschutzbüro zu schaffen. Die Stiftung sollte hier auch eine koordinierende  
 3948 Funktion hinsichtlich entsprechender bereits bestehender Bildungsinitiativen übernehmen.
- 3949 5. Im Bereich der Datenschutzforschung wird angeregt zu prüfen, ob die Stiftung Datenschutz  
 3950 insbesondere bei der Entwicklung und dem Ausbau von Instrumenten des technischen  
 3951 Datenschutzes tätig werden kann. Mögliche Tätigkeitsfelder eröffnen sich sowohl im Bereich der

3952 Koordination der Forschungsmittelvergabe als auch für den Bereich eigener  
3953 Forschungsanstrengungen.

3954

3955 *Alternativer (streitiger)Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
3956 *GRÜNEN.*

3957 **Stiftung Datenschutz**

3958 Die Enquete-Kommission stellt fest, dass die geplante Stiftung Datenschutz, wenn die richtigen  
3959 Vorgaben für die inhaltliche Ausgestaltung gefunden werden, als wirkungsvolle Plattform vorhandene  
3960 Angebote zusammenführen und so ihrem geplanten Auftrag für Aufklärung und Information gerecht  
3961 werden kann. Sie begrüßt daher im Grundsatz die von der Bundesregierung auf den Weg gebrachte  
3962 Stiftung Datenschutz. Diese Stiftung kann u. a. Kriterien für die Zertifizierung von Diensten sowie für  
3963 ein einheitliches Gütesiegel aufstellen und damit mehr Transparenz für Unternehmen und Bürger  
3964 erwirken. Dadurch kann sich auch eine Erleichterung bei der Auswahl zwischen einer Vielzahl von  
3965 Anbietern ergeben und zugleich das Vertrauen der Bürgerinnen und Bürger in neue Technologien  
3966 gestärkt werden. Für Unternehmen kann sie Anreize setzen, hohe datenschutzrechtliche  
3967 Anforderungen einzuhalten. Neben der Festlegung von Kriterien nimmt sie die Vergabe von  
3968 Gütesiegeln nach einem gesetzlich geregelten Verfahren vor.

3969 Bei der Einrichtung der Stiftung Datenschutz ist darauf zu achten, dass vergleichende Tests nach  
3970 verschiedenen Kriterien, unter Einschluss des Datenschutzes, bereits etwa durch die Stiftung  
3971 Warentest durchgeführt werden; und zwar für Güter, Produkte und Dienstleistungen, die sich explizit  
3972 an Endverbraucher richten. Eine klare Zuordnung der Zuständigkeit in diesem Bereich ist deshalb in  
3973 der Satzung zu verankern. Eine Überschneidung der Zuständigkeiten zwischen den beiden Stiftungen  
3974 sollte vermieden werden. Vielmehr sollen diese sich in ihren Angeboten ergänzen.

3975 Weitere Aufgaben können die Stärkung des Selbst Datenschutzes sowie Aufklärung und Bildung im  
3976 Datenschutz sein.

3977 Die Enquete-Kommission fordert daher die Bundesregierung auf, bei Einsetzung der Stiftung folgende  
3978 Punkte – die für eine wirkungsvolle Arbeit einer Bundesstiftung Datenschutz mit vorstehendem  
3979 Auftrag unabdinglich sind – zu berücksichtigen:

- 3980 1. Die Stiftung ist wirtschaftlich und organisatorisch, also finanziell und personell, unabhängig von  
3981 den zu bewertenden Unternehmen zu organisieren. Personell ist darauf zu achten, dass bei der  
3982 Besetzung der Gremien die zu prüfenden datenverarbeitenden Unternehmen zwar beteiligt werden,  
3983 aber auf die Unabhängigkeit der Stiftung keinen Einfluss haben. Dies könnte zum Beispiel durch  
3984 die Einsetzung eines Beirats, der beratende Funktion hat, geschehen. Finanziell sollte die  
3985 Bundesstiftung nicht allein vom Bundeshaushalt abhängig sein. Bei der Annahme von  
3986 Zuwendungen hat die Stiftung jedoch darauf zu achten, dass ihre Unabhängigkeit gewahrt bleibt.
- 3987 2. In der Satzung ist das Verhältnis zu den Datenschutzbehörden zu klären. Es ist festzuhalten, dass  
3988 diesen allein die Kontrolle über die Einhaltung der Gesetze obliegt und die Aufsichtstätigkeit nicht  
3989 durch die Arbeit der Stiftung beeinflusst werden darf. Ebenso dürfen die von der Stiftung  
3990 Datenschutz erteilten Audits und Gütesiegel keine rechtliche Bindungswirkung gegenüber den

- 3991 Datenschutzbehörden entfalten, das heißt die Aufsichtsbehörden müssen die entsprechenden  
 3992 Unternehmen dennoch anlassbezogen überprüfen dürfen.
- 3993 3. Es ist in der Satzung zu regeln, wer die materiellen Standards für Zertifizierungsverfahren setzt.  
 3994 Dabei sind ein Höchstmaß an Transparenz sowie eine enge Kooperation mit den  
 3995 Datenschutzbehörden unabdingbar.
- 3996 4. Die Vergabe von Audits kann durch die Stiftung Datenschutz aufgrund eines bundeseinheitlich  
 3997 gesetzlich festgelegten Auditierungsverfahrens erfolgen. Hierfür bedarf es eines Gesetzes im Sinne  
 3998 von § 9a BDSG. Dabei ist zu beachten, dass bereits existierende Auditverfahren (wie zum Beispiel  
 3999 in Bremen oder Schleswig-Holstein) in die Ausgestaltung und Vergabe eingebunden werden.
- 4000 5. Bei der Vergabe von Gütesiegeln durch die Stiftung ist darauf zu achten, dass ein einheitliches  
 4001 Gütesiegel entwickelt wird und eine inflationäre Handhabung bei der Vergabe vermieden wird.  
 4002 Ebenso ist das Verfahren für die Vergabe transparent zu gestalten. Die Gütesiegel sind nur für eine  
 4003 bestimmte Zeit (zum Beispiel für zwei Jahre) zu erteilen und müssen turnusgemäß geprüft werden.
- 4004 6. Im Bereich der Bildung darf die Stiftung Datenschutz nicht die Zuständigkeit der Länder verletzen.  
 4005 Die Länder sind deshalb mitentscheidend einzubeziehen. Schwerpunkt der Stiftungstätigkeit sollte  
 4006 deshalb die außerschulische Bildung sein.
- 4007 7. Im Bereich der Aufklärung wird der Stiftung empfohlen, ein zentrales Informationsportal oder ein  
 4008 virtuelles Datenschutzbüro (wie derzeit beim ULD Schleswig-Holstein<sup>292</sup> praktiziert) zu schaffen.
- 4009 8. Die Stiftung Datenschutz sollte perspektivisch auch im Bereich der Datenschutzforschung,  
 4010 insbesondere der Entwicklung und dem Ausbau von Instrumenten des technischen Datenschutzes,  
 4011 tätig werden. Mögliche Tätigkeitsfelder eröffnen sich sowohl im Bereich der Koordination der  
 4012 Forschungsmittelvergabe als auch für den Bereich eigener Forschungsanstrengungen.

4013

4014

4015 ***Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der***  
 4016 ***Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.***

#### 4017 **Schadensersatzansprüche im Datenschutzrecht**

4018 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, weiter zu beobachten, ob das  
 4019 Sanktionssystem im Datenschutzrecht auch zukünftig effektiven Schutz gewährleistet. Auch ein  
 4020 Wegfall von Antragerfordernissen bei bestimmten Straftaten im Bereich der Datenverarbeitung, die  
 4021 über individuelle Verstöße hinausgehen, kann zu einer Verbesserung in Betracht gezogen werden.

4022 Wenn eine verantwortliche Stelle dem Betroffenen durch eine datenschutzrechtlich unzulässige oder  
 4023 unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zufügt, macht sie sich  
 4024 schadensersatzpflichtig. Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, zu  
 4025 evaluieren, inwieweit die Ansprüche praxistauglich sind und sich als Instrument neben Bußgeldern  
 4026 und Sanktionen etablieren. Falls Verbesserungen erforderlich erscheinen und Unterlassungs- sowie  
 4027 Beseitigungsansprüche nicht ausreichen, könnte u. a. ein Ersatz immaterieller Schäden wie im  
 4028 öffentlichen Bereich auch für den nicht-öffentlichen Bereich in die Überlegungen miteinbezogen  
 4029 werden.

<sup>292</sup> Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

4030 *Alternativer (streitiger)Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
 4031 *GRÜNEN.*

4032 **Schadensersatzansprüche**

4033 Im Ergebnis stellt die Enquete-Kommission fest, dass Handlungsbedarf im Bereich des  
 4034 Schadensersatzrechts besteht.

4035 Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

- 4036 1. bezugnehmend auf die Vorschläge der Konferenz des Bundes- und der  
 4037 Landesdatenschutzbeauftragten eine Gefährdungshaftung auch gegenüber nicht-öffentlichen  
 4038 Stellen einzuführen;  
 4039 2. einen pauschalierten Schadensersatzanspruch bei Datenschutzverstößen einzuführen, der die  
 4040 Problematik der Bezifferbarkeit des Schadens löst und alle datenverarbeitenden Stellen zum Ersatz  
 4041 immaterieller Schäden verpflichtet, unabhängig von nachweisbaren weiteren und höheren Schäden;  
 4042 3. zu prüfen, ob nicht die Festlegung einer Mindest- und einer Höchstgrenze der Ersatzsumme  
 4043 erfolgen sollte.

4044

4045 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
 4046 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

4047 **Beschäftigtendatenschutz**

4048 Die Enquete-Kommission begrüßt, dass die Bundesregierung ein Gesetz zur Regelung des  
 4049 Beschäftigtendatenschutzes auf den Weg gebracht hat. Die Regelungen sollten einen Ausgleich  
 4050 zwischen den Interessen der Arbeitnehmer und Arbeitgeber und damit insgesamt eine Verbesserung  
 4051 des Arbeitnehmerdatenschutzes beinhalten. Es sollten nur solche Daten verarbeitet werden, die für das  
 4052 Arbeitsverhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das  
 4053 Arbeitsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante  
 4054 Gesundheitszustände beziehen, müssen ausgeschlossen sein.

4055 Der Einsatz von Informations- und Kommunikationstechnologie am Arbeitsplatz ist heute nicht mehr  
 4056 wegzudenken. Das Spannungsverhältnis zwischen den Interessen von Arbeitnehmern und  
 4057 Arbeitgebern muss vor allem beim Einsatz von webbasierten Kontrollinstrumenten und im Rahmen  
 4058 der gestatteten auch privaten Nutzung betrieblicher Telekommunikationsmittel praxisgerecht und  
 4059 rechtsklar ausgestaltet werden. Hierfür sollte eine eigenständige Regelung getroffen werden. Es muss  
 4060 jedoch auch Raum für Betriebsvereinbarungen und Einwilligungen als unmittelbares, gestalterisches  
 4061 Mittel von spezifischen Gegebenheiten vor Ort bleiben, wobei das aktuell bestehende Schutzniveau  
 4062 nicht unterschritten werden darf.

4063

4064

4065 *Alternativer (streitiger)Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
 4066 *GRÜNEN.*

4067 **Beschäftigtendatenschutz**

4068 Die Enquete-Kommission stellt fest, dass es im Bereich des Datenschutzes für Beschäftigte  
 4069 gesetzgeberischen Handlungsbedarf gibt. Hierbei sind insbesondere die Rechte der Beschäftigten bei  
 4070 Überwachung und Screening zu wahren.

4071 Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag, ein entsprechendes Gesetz  
 4072 unter Beachtung nachfolgender Kriterien zu beschließen:

- 4073 1. Der Beschäftigtendatenschutz ist in einem eigenständigen Gesetz zu regeln. Die derzeit  
 4074 bestehenden Regelungen im Bundesdatenschutzgesetz sind nicht effektiv genug. Denn es finden  
 4075 die allgemeinen Regelungen des Datenschutzes auch auf das Beschäftigungsverhältnis  
 4076 Anwendung. Diese sind oft nicht explizit auf den Persönlichkeitsrechtsschutz der Beschäftigten  
 4077 zugeschnitten.
- 4078 2. Eine eigenständige gesetzliche Regelung muss die dem Arbeitsverhältnis immanente  
 4079 Abhängigkeit der Beschäftigten vom Arbeitgeber aufgreifen und eine Generaleinwilligung für die  
 4080 Datenerhebung und -nutzung schon bei Aufnahme des Arbeitsverhältnisses, aber auch während  
 4081 des Arbeitsverhältnisses verhindern.
- 4082 3. Das Gesetz muss die anlasslose Beobachtung und Überwachung von Beschäftigten am  
 4083 Arbeitsplatz, aber auch im privaten Umfeld verbieten. Dieses grundsätzliche Verbot muss die  
 4084 direkte Überwachung durch Beauftragte, Externe oder Mitarbeiter, aber auch die indirekte  
 4085 Überwachung durch Video- oder Tonaufnahmen umfassen. Auch biometrische oder  
 4086 ferngesteuerte Systeme (RFID, GPS oder Fernwartungssoftware auf Mitarbeiter-PCs) dürfen  
 4087 nicht über eng begrenzte Zwecke hinaus eingesetzt werden und bedürfen der Vorabkontrolle.
- 4088 4. Bei der Nutzung von Internet und E-Mail ist dem Persönlichkeitsrecht der Beschäftigten in  
 4089 besonders hohem Maße Rechnung zu tragen. Es muss ein grundsätzliches Verbot des Zugriffs auf  
 4090 personenbezogene oder -beziehbare Nutzerdaten bei der Verwendung dieser modernen  
 4091 Kommunikationsmittel festgelegt werden. Dieses Verbot darf nicht durch eine  
 4092 Generaleinwilligung der Beschäftigten – etwa mit Abschluss des Arbeitsvertrages –  
 4093 ausgeschlossen werden.
- 4094 5. Ausgehend von dem Grundsatz, dass der Zweck des Datenschutzes darin besteht, die Einzelnen  
 4095 vor Missbrauch ihrer Daten zu schützen, können Ausnahmen nur für gesetzlich ausdrücklich  
 4096 geregelte Fälle vorgesehen werden. Dies ist insbesondere nur dann zuzulassen, wenn eine andere  
 4097 Aufklärung, namentlich durch die Polizei oder die Staatsanwaltschaft, nicht möglich ist.  
 4098 Ausnahmen sind für Fälle des begründeten Verdachts einer Straftat oder der schwerwiegenden  
 4099 Schädigung des Arbeitgebers zuzulassen. Hierzu sind das Zustimmungserfordernis der  
 4100 Interessenvertretung oder, sofern nicht vorhanden, die Einbeziehung einer neutralen Stelle (zum  
 4101 Beispiel des Landesdatenschutzbeauftragten) erforderlich.<sup>293</sup>

<sup>293</sup> (siehe hierzu: Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo: Kompaktkommentar zum BDSG. 2010, S. 558 ff.).

- 4102 6. Es ist notwendig, das Fragerecht des Arbeitgebers bei der Einstellung und die Möglichkeit der  
 4103 Anordnung von ärztlichen Untersuchungen im Gesetz auf die durch die Rechtsprechung  
 4104 beurteilten Fälle zu beschränken. Die Anordnung von ärztlichen Untersuchungen bedarf der  
 4105 Zustimmung des Betriebsrates.
- 4106 7. Vor der Erhebung von Beschäftigtendaten im Rahmen eines Einstellungsverfahrens ist über die  
 4107 Art der auszuübenden Tätigkeit und deren Einordnung in den Arbeitsablauf des Betriebs zu  
 4108 unterrichten.
- 4109 8. Es bedarf einer Sonderregelung im Gesetz für den folgenden Fall: Sind Beschäftigte auch Kunden  
 4110 ihres Arbeitgebers, müssen die Daten des Kundenbereichs gesondert geführt und geschützt  
 4111 werden. Personalverantwortliche dürfen keinen Zugriff auf diese Kundendaten haben.
- 4112 9. Fälle des so genannten Whistleblowings sind gesetzlich gesondert zu verankern und mit einem  
 4113 Maßregelungsverbot zu versehen.<sup>294</sup>
- 4114 10. Ein eigenständiges Beschäftigtendatenschutzgesetz muss die Rechtsposition des betrieblichen  
 4115 Datenschutzbeauftragten stärken, so zum Beispiel durch eine weiter verbesserte  
 4116 Kündigungsschutzregelung.
- 4117 11. Die Mitbestimmungsrechte der Betriebsräte beim Datenschutz sind durch das Gesetz zu stärken.
- 4118 12. Für die Daten von Mitgliedern des Betriebsrats und von Aufsichtsräten ist ein Immunitätsschutz  
 4119 für die Dauer ihrer Amtszeit zu prüfen beziehungsweise darüber hinaus in Anlehnung an die  
 4120 Vorschriften zum Sonderkündigungsschutz, die im Kündigungsschutzgesetz gelten.
- 4121 13. Um die von Datenschutzverstößen betroffenen Beschäftigten in der Rechtsdurchsetzung zu  
 4122 stärken, muss das Gesetz eine Verbandsklagemöglichkeit vorsehen. Denn im bestehenden  
 4123 Arbeitsverhältnis wird eine Klage gegen den Arbeitgeber erfahrungsgemäß nicht angestrengt.  
 4124 Hierzu ist die Gefahr von Repressalien zu groß.
- 4125 14. In einem Beschäftigtendatenschutzgesetz ist ein konkreter Anspruch auf Schmerzensgeld für den  
 4126 in seinem Persönlichkeitsrecht verletzten Beschäftigten (zum Beispiel entsprechend § 15  
 4127 Allgemeines Gleichbehandlungsgesetz<sup>295</sup>) zu verankern.
- 4128 15. In dem Gesetz müssen die Ansprüche der Beschäftigten bei Verstößen gegen den  
 4129 Beschäftigtendatenschutz konkret, klar und verständlich geregelt werden. Es bedarf u. a. eines  
 4130 Unterlassungsanspruchs gegenüber dem Arbeitgeber sowie eines Schadensersatzanspruchs für  
 4131 Vermögensschäden und immaterielle Schäden.

4132

---

<sup>294</sup> ausführlich zur Thematik des Whistle-Blowings: Tinnefeld, Marie-Theres/Rauhofer, Judith: Whistleblower: Verantwortungsbewusste Mitarbeiter oder Denunzianten? DuD 2008, S.717 ff.

<sup>295</sup> Allgemeines Gleichbehandlungsgesetz vom 14. August 2006, BGBl. I S. 1897, zuletzt geändert durch Art. 15 Abs. 66 des Gesetzes vom 5. Februar 2009, BGBl. I S. 160.

4133

4134 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, Textvorschlag der Fraktionen SPD,*  
 4135 *DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

4136 **Datenschutz und Internet der Dinge**

4137 Mit der flächendeckenden Einführung des Internetprotokolls IPv6 wird die bisher vorhandene  
 4138 Beschränkung von IP-Adressen auf 4,3 Milliarden Adressen aufgehoben. Zukünftig stehen 340  
 4139 Sextillionen Adressen allen Nutzerinnen und Nutzern im Internet zur Verfügung. Schon heute  
 4140 zeichnet sich ab, dass sich hierdurch ein Internet der Dinge oder auch „Smart Life“ entwickeln kann.  
 4141 Immer mehr elektronische Geräte (zum Beispiel Kühlschränke) sowie Garagen und Autos können  
 4142 über lokale oder auch überregionale Netzwerke verbunden und so elektronisch gesteuert werden.  
 4143 Diese technologische Weiterentwicklung stellt auch besondere Anforderungen an den Datenschutz, da  
 4144 für das Internet der Dinge insbesondere personenbezogene Verbrauchs- und Gewohnheitsdaten von  
 4145 besonderer Bedeutung sind. Die Enquete-Kommission regt daher an, bereits zu Beginn der Einführung  
 4146 von Smart- Life-Anwendungen durch die Anbieter für eine Vertrauenskultur bei Nutzerinnen und  
 4147 Nutzern zu werben. Dies setzt zunächst voraus, dass datenschutzrechtliche Grundsätze auch hier  
 4148 beachtet werden.

4149

4150

4151 *Weiterer (streitiger)Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
 4152 *GRÜNEN.*

4153 **Ubiquitous Computing**

4154 Nach den Datenschutzkonzepten der 1960er und 1970er Jahre, denen die damalige  
 4155 Großrechner-Technologie zugrunde lag, bedarf es jetzt schlüssiger Antworten auf die weltweite  
 4156 Vernetzung von Rechnern in einem eigenen "virtuellen Sozialraum" des Internets. Gleichzeitig  
 4157 beginnt mit der vernetzten Digitalisierung von Infrastrukturen (zum Beispiel im Bereich Verkehr oder  
 4158 bei Stromnetzen) und Alltagsgegenständen u. a. mit Sensoren wie den RFID (etwa des so genannten  
 4159 intelligenten Kühlschranks) bereits die nächste große Herausforderung, auf die es noch keine  
 4160 regulatorische Antwort gibt. Kennzeichen dieser unter dem Stichwort Ubiquitous Computing  
 4161 zusammengefassten Entwicklung ist die (oft ad hoc erfolgende) Verknüpfung der körperlichen  
 4162 Alltagswelt mit der virtuellen Welt des Internets. Die mit Sensortechnik ausgestatteten  
 4163 Alltagsgegenstände nehmen Veränderungen ihrer Umwelt wahr, vernetzen sich mit vergleichbaren  
 4164 Gegenständen und reagieren kontextbezogen. Über die Verbindung mit den Besitzern der  
 4165 Gegenstände erfolgen zumindest mittelbar umfangreiche Speicherungen personenbezogener Daten  
 4166 auf Vorrat sowie Nutzerprofile. In der Summe können auf diese Weise verhältnismäßig dichte  
 4167 Überwachungsnetze hinsichtlich der sich in diesen interaktiven Umgebungen bewegenden Personen



4168 entstehen. Mit den bisherigen Grundprinzipien des Datenschutzes sind diese Anwendungen kaum in  
4169 Einklang zu bringen.<sup>296</sup>

4170 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag im Hinblick auf die Entwicklungen  
4171 der allgegenwärtigen Datenverarbeitung,

- 4172 1. die beginnende tatsächliche Ausbreitung von Anwendungen des Ubiquitous Computing ständig  
4173 sorgsam zu beobachten;
- 4174 2. der Grundsatz verpflichtender technischer Vorkehrungen (Privacy by Design) bei der  
4175 Entwicklung und dem Einsatz von Produkten des Ubiquitous Computing muss mit Blick auf die  
4176 Funktionsweise und die besonderen Risiken gegebenenfalls gesetzlich konkretisiert werden;
- 4177 3. Einschränkungen, die sich hinsichtlich der Anwendbarkeit zentraler Grundsätze des bisherigen  
4178 Datenschutzrechts ergeben, durch angemessene, ein vergleichbar hohes Schutzniveau  
4179 gewährleistende anderweitige Vorgaben zu kompensieren;
- 4180 4. dafür Sorge zu tragen, dass die eingesetzten Technologien zugleich für Nutzerinnen und Nutzer  
4181 die Möglichkeit einer kontinuierlichen Erläuterung und Abrufbarkeit ihres Status – mit Blick auf  
4182 zum Beispiel Profilbildung oder Vernetzungsgrad mit anderen Anwendungen – gewährleisten, da  
4183 der Grundsatz der Transparenz angesichts der weitgehend im Hintergrund stattfindenden  
4184 vielfältigen Datenverarbeitungen besondere Bedeutung gewinnt.

4185

4186

4187 *Streitiger Textvorschlag der Fraktionen CDU/CSU und FDP, alternativer Textvorschlag der*  
4188 *Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN folgt.*

#### 4189 **Geodaten und Geolocating**

4190 Geodaten werden sowohl von öffentlichen Stellen (im Rahmen von INSPIRE<sup>297</sup>) als auch von nicht-  
4191 öffentlichen Stellen (zum Beispiel Google Street View und Microsoft Streetside) erhoben und zum  
4192 Teil im Internet der Öffentlichkeit zur Verfügung gestellt. Dabei ist zu beachten, dass Geodaten allein  
4193 keine personenbezogenen Daten sind. Durch ihre Personenbeziehbarkeit und die Möglichkeit, sie mit  
4194 personenbezogenen Daten zu verknüpfen, können sie jedoch datenschutzrechtlich relevant werden.  
4195 Zudem sind sie aufgrund ihrer zunehmenden Detailschärfe und vielseitigen Einsetzbarkeit eine  
4196 beliebte, zumeist kostenlose, Informationsquelle, die sowohl von Unternehmen als auch von  
4197 Privatpersonen genutzt und in bestehende Angebote integriert wird.

4198 Durch die gestiegene Verbreitung der Geodatendienste haben sich vielfältige Abgrenzungsfragen der  
4199 Personenbeziehbarkeit von Daten, aber auch weitere Folgeprobleme, wie zum Beispiel der nicht  
4200 einvernehmlichen Löschung von Geodaten zu speziellen Objekten, ergeben. Die Enquete-

2 <sup>296</sup> vgl. dazu insgesamt Roßnagel, Alexander: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung. MMR 2005, S. 71.

<sup>297</sup> Infrastructure for Spatial Information in the European Community (Geodateninfrastruktur in der Europäischen Gemeinschaft).

4201 Kommission empfiehlt daher dem Deutschen Bundestag, diese Problematik in seine Überlegungen  
4202 über gesetzliche Änderungen des Bundesdatenschutzgesetzes mit einzubeziehen.

4203 Geolokalisationsdienste zeichnen sich demgegenüber dadurch aus, dass Daten über die Position der  
4204 Nutzerin bzw. des Nutzers von mobilen Geräten übertragen werden. Eine Auswertung dieser Daten  
4205 erlaubt die Erstellung von umfassenden Bewegungsprofilen. Nach dem geltenden Recht sind solche  
4206 Dienste nur mit Einwilligung des Nutzers zulässig (vergleiche § 4a BDSG). Die Enquete-Kommission  
4207 empfiehlt dem Deutschen Bundestag, an dieser Regelung weiter festzuhalten und durch einen  
4208 stringenten Vollzug der gesetzlichen Vorgaben sicherzustellen, dass die Nutzerinnen und Nutzer vor  
4209 einer Erhebung von personenbezogenen Daten hierüber auch umfassend informiert wurden. Dies gilt  
4210 insbesondere für den Fall, dass die Daten nicht lediglich zur technischen Durchführung des Dienstes  
4211 anfallen, sondern darüber hinaus genutzt werden sollen.

4212 *Alternative (streitige)Textvorschläge der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE*  
4213 *GRÜNEN.*

#### 4214 **Geolocation/Geodaten**

4215 Die Enquete-Kommission stellt fest, dass sich mit der digitalen Gesellschaft zunehmend auch eine  
4216 digitale Öffentlichkeit herausbilden wird. Zu dieser digitalen Öffentlichkeit gehört auch das Angebot  
4217 und die Nutzung von Geoinformationen beziehungsweise Geodiensten und -anwendungen im Internet,  
4218 zum Beispiel Kartierungs- und Lokalisierungsdienste wie Google-Street-View, Microsoft Streetside,  
4219 Facebook-Places oder Qupe.

4220 Wie in der analogen Welt gilt es, die Öffentlichkeit und den öffentlichen Raum als eine  
4221 Grundvoraussetzung einer demokratisch verfassten offenen Gesellschaft zu erhalten und gleichzeitig  
4222 die Privatheit zu schützen. Das bedeutet auch, die grundrechtlich abgesicherten Positionen wie  
4223 Wissenschafts-, Presse- und unternehmerische Freiheit mit anderen Grundrechten wie dem  
4224 Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen.  
4225 Die Enquete-Kommission hält fest, dass Selbstverpflichtungen der in diesem Bereich tätigen  
4226 Unternehmen hilfreiche Instrumente darstellen. Wenn Persönlichkeitsrechte betroffen sind, bedürfen  
4227 Sie aber jedenfalls eines gesetzlichen Rahmens.

4228 Sie nimmt Bezug auf die Forderungen der Datenschutzbeauftragten des Bundes sowie der Länder und  
4229 empfiehlt dem Deutschen Bundestag, eine allgemeine, technikenabhängige Regelung zur  
4230 Verarbeitung von personenbezogenen Geoinformationen beziehungsweise -daten zu schaffen, die sich  
4231 an den jeweiligen Risiken orientiert. Hierbei sollten folgende Gesichtspunkte beachtet werden:

4232 **a.** Es sollten Kriterien geschaffen werden, die festlegen, über welche Verfahren eine  
4233 Interessenabwägung zwischen Persönlichkeitsschutz und Informationsinteresse vorgenommen  
4234 werden kann, und auf deren Grundlage wonach eine klare Abgrenzung zwischen reinem Sachbezug  
4235 und Personenbeziehbarkeit möglich ist.

4236 **b.** Es sollte eine gesetzliche Verpflichtung geschaffen werden, wonach den Betroffenen die Tatsache  
4237 der konkreten Ortung in verständlicher Form anzuzeigen ist, zum Beispiel durch ein akustisches  
4238 Signal, sobald die oder der Betroffene geortet wurde.

4239 c. Weiterhin ist eine Regelung zu treffen, wonach der Einsatz von Tracking-Systemen, also jede Form  
 4240 der Ortung durch Dritte, die der Betroffene nicht beeinflussen kann, nur mit dessen Einwilligung  
 4241 (nach dem Vorbild von § 98 TKG) zulässig ist.

4242 d. Unternehmen, die grundsätzlich sachbezogene, aber personenbeziehbare Geoinformationen,  
 4243 welche schutzwürdige entgegenstehende Interessen der Betroffenen berühren können, im Internet  
 4244 zur Nutzung oder zur Verarbeitung veröffentlichen, müssen diesen (zum Beispiel Eigentümern  
 4245 oder Mietern) ein Widerspruchsrecht anbieten. Das entsprechende Recht muss gesetzlich  
 4246 festgeschrieben und kann nicht allein durch eine Selbstverpflichtung der anbietenden Unternehmen  
 4247 geregelt werden.

4248 e. Verstöße gegen entsprechende Regelungen müssen sanktioniert werden, wobei die Aufsicht  
 4249 hierüber den Datenschutzbeauftragten des Bundes und der Länder sowie den Aufsichtsbehörden  
 4250 über den Datenschutz im nicht-öffentlichen Bereich obliegen sollte.

4251 *weiterer Textvorschlag der Fraktionen SPD, DIE LINKE. BÜNDNIS 90/DIE GRÜNEN zu derselben*  
 4252 *Fragestellung, im Originaltext der Antragsteller an anderer Stelle, vgl. Zeile 3562.*

4253 *[Die Enquete-Kommission gibt dem Deutschen Bundestag nachfolgende Handlungsempfehlung,]*

4254 18. die Schaffung einer allgemeinen, technikunabhängigen Regelung zur Verarbeitung  
 4255 personenbezogener Lokalisierungsdaten unter Verpflichtung der Lokalisierungsdienstleister, die  
 4256 konkrete Ortung des Betroffenen durch ein Signal anzuzeigen sowie innerhalb von Tracking-  
 4257 Systemen die Einwilligung des Betroffenen vorzusehen. Der E-Privacy-Richtlinie zufolge ist für  
 4258 die Verarbeitung von Positionsdaten aus GSM/UMTS (Mobilfunk), bei denen es sich stets um  
 4259 Tracking-Systeme handelt, ausdrücklich eine Einwilligung des Betroffenen erforderlich. Bislang  
 4260 ist diese Vorgabe der Richtlinie jedoch nicht in das Bundesdatenschutzgesetz aufgenommen  
 4261 worden. Das Gesetz ist in diesem Punkt deshalb bislang nicht europarechtskonform. Bei der  
 4262 Ausgestaltung ist auf Technikneutralität zu achten. Ferner muss es Betroffenen ermöglicht  
 4263 werden, im Rahmen der technischen Möglichkeiten eine Ortung der eigenen Person zu  
 4264 verhindern. Positionsdaten sollten in die Kategorie der besonders schützenswerten („sensitiven“)  
 4265 Daten ins Bundesdatenschutzgesetz (§ 3 Abs. 9) aufgenommen werden;

4266

4267 *Streitiger Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.*

#### 4268 **Videüberwachung**

4269 Der Einsatz von Videüberwachungstechnik in öffentlich zugänglichen Räumen breitet sich weiterhin  
 4270 aus. Damit verbunden sind massenhafte Bildfassungen und Bildspeicherungen von völlig  
 4271 unbeteiligten Personen. Die tatsächlichen Einsatzbedingungen, beispielsweise die Frage des konkreten  
 4272 Zwecks, technische Möglichkeiten wie etwa das Zoomen oder die Frage, ob es sich um eine  
 4273 internetgestützte Bildübertragung handelt, bleiben für die Betroffenen weithin intransparent. Darüber  
 4274 hinaus fehlt es an einer hinreichenden und aktuellen Übersicht, in welchem Umfang vor allem  
 4275 städtische Räume bereits von Videüberwachungen betroffen sind. Die Datenschutzbeauftragten der  
 4276 Länder haben in den vergangenen Jahren auf zahlreiche weitere Probleme des zunehmenden

4277 Kameraeinsatzes aufmerksam gemacht, darunter insbesondere das gewaltige Vollzugsdefizit  
 4278 hinsichtlich der Beachtung der gesetzlichen Vorschriften. Die bestehenden gesetzlichen Regelungen,  
 4279 insbesondere § 6b BDSG, haben auch inhaltlich keine Einschränkung dieser Entwicklung bewirken  
 4280 können und bieten den Bürgern nur unzureichenden rechtlichen Schutz.

4281 Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

- 4282 1. im Rahmen einer Reform insbesondere des Bundesdatenschutzgesetzes die Zulässigkeit der  
 4283 Bilderfassung öffentlich zugänglicher Räume enger zu begrenzen;
- 4284 2. sachgerechte Regelungen für eine verbesserte Transparenz und Sicherheit beim Einsatz von  
 4285 Videotechnik auf den Weg zu bringen, darunter auch Maßnahmen zur laufenden Beobachtung  
 4286 und Erfassung der Ausbreitung;
- 4287 3. die Bundesregierung anzuhalten, im Rahmen der Erneuerung der Datenschutzrichtlinie auf  
 4288 zulässigkeitsbegrenzende Bestimmungen für den Einsatz von Videoüberwachungen zu drängen.

4289

4290 *Streitiger Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.*

#### 4291 **Datenschutz auf technischer Ebene (Deep Packet Inspection und IPv6)**

4292 Der Datenverkehr von Nutzern im Internet sollte einem vollständigen Telekommunikationsgeheimnis  
 4293 unterliegen. Die Kommunikation von Bürgerinnen und Bürgern untereinander, mit staatlichen Stellen  
 4294 oder mit privaten Unternehmen gehört, wenn sie nicht von den Betroffenen selbst öffentlich gemacht  
 4295 wird, zur schützenswerten Privatsphäre jedes Einzelnen. Netzwerkmanagementmaßnahmen, etwa mit  
 4296 Hilfe von so genannter Deep Packet Inspection (DPI), bei der die von Teilnehmern gesendeten und  
 4297 empfangenen Inhalte durchleuchtet beziehungsweise auch auf der Inhaltsebene ausgelesen und  
 4298 analysiert werden, sind unter diesem Gesichtspunkt abzulehnen.

4299 Durch die rasant ansteigende Zahl von Geräten, die mit dem Internet verbunden sind  
 4300 beziehungsweise darüber kommunizieren, ist bereits seit geraumer Zeit klar, dass der verwendbare  
 4301 Adressraum des IPv4-Protokolls ausgeschöpft und nicht zukunftsfähig ist. Die anstehende Einführung  
 4302 des IPv6-Protokolls in den Internetalltag bietet den Vorteil einer ungleich größeren Anzahl möglicher  
 4303 IP-Adressen im Internet. Mit Nutzung von IPv6 ist es daher technisch möglich jedem internetfähigen  
 4304 Endgerät eine dauerhafte, nur einmal vergebene IP-Adresse zuzuweisen. Somit ist die  
 4305 Kommunikation eines einzelnen Endgerätes theoretisch über Jahre hinweg nachvollziehbar.

4306 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,

- 4307 1. die Verwendung von Methoden zur inhaltlichen Analyse von (IP-)Datenpaketen (zum Beispiel  
 4308 DPI) beziehungsweise die Analyse selbst zu untersagen. Dies gilt für Eingriffe von staatlicher und  
 4309 nicht staatlicher Seite gleichermaßen und muss technikneutral formuliert werden;
- 4310 2. Internet-Zugangsanbieter zu verpflichten, ihren Kunden ohne Mehrkosten die Auswahl zwischen  
 4311 dauerhaft festen und wechselnden IP-Adressen für ihre Anschlüsse beziehungsweise Endgeräte  
 4312 anzubieten.

4313

4314  
4315 *Streitiger Textvorschlag der Fraktionen SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.*

4316 **Sicherheitsbehörden und die Evaluierung von Eingriffsbefugnissen**

4317 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, die bestehenden Aufgaben und  
4318 Befugnisse von Sicherheitsbehörden und Diensten, die mit Grundrechtseingriffen verbunden sind,  
4319 umfassend hinsichtlich ihrer Notwendigkeit, Wirksamkeit und Effizienz sowie ihrer  
4320 grundrechtswahrenden Funktion unabhängig, auf wissenschaftlicher Grundlage und ergebnisoffen zu  
4321 evaluieren. Dies betrifft insbesondere die verdeckten Ermittlungsmaßnahmen. Zwar bestehen in  
4322 zahlreichen Gesetzen bereits Evaluierungsvorschriften, die jedoch in der Umsetzung diesen  
4323 Ansprüchen zumeist nicht genügen.

4324 *Streitiger Textvorschlag der Fraktion SPD und SV Alvar Freude, Lothar Schröder und Dr.*  
4325 *Wolfgang Schulz, zwei Textvorschläge der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE*  
4326 *GRÜNEN zur Vorratsdatenspeicherung folgen.*

4327 **Vorratsdatenspeicherung**

4328 Der grundrechtliche Schutz informationeller Selbstbestimmung wurde durch die Rechtsprechung des  
4329 Bundesverfassungsgerichts in jüngerer Zeit schärfer konturiert, nicht zuletzt durch die Entscheidung  
4330 zur Vorratsdatenspeicherung. Das Bundesverfassungsgericht hat am 2. März 2010<sup>298</sup> entschieden,  
4331 dass die Vorratsdatenspeicherung in Deutschland in ihrer bisherigen Umsetzung verfassungswidrig  
4332 sei, da das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzerinnen und  
4333 Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit  
4334 vorsehe, und hat zudem die Hürden für den Abruf dieser Daten als zu niedrig bewertet. Das Urteil  
4335 verpflichtete deutsche Telekommunikationsanbieter zur sofortigen Löschung der bis dahin  
4336 gesammelten Daten. Das Bundesverfassungsgericht hat jedoch auch festgestellt, dass die  
4337 Vorratsdatenspeicherung unter schärferen Sicherheits- und Transparenzvorkehrungen sowie  
4338 begrenzten Abrufmöglichkeiten für die Sicherheitsbehörden grundsätzlich zulässig sei.

4339 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,

4340 - eine grundsätzliche und offene Debatte über die Notwendigkeit und auch die Grenzen der  
4341 Vorratsdatenspeicherung zu führen. Dabei ist auch zu klären, ob und wie eine Speicherung auf Vorrat  
4342 grundrechtsschonend und verfassungskonform ausgestaltet werden könnte. Die Enquete-Kommission  
4343 geht dabei davon aus, dass es eine Zustimmung des Deutschen Bundestages für die  
4344 Vorratsdatenspeicherung nur geben kann, wenn es zu einer grundsätzlichen Überarbeitung der  
4345 damaligen Vorgaben zur Umsetzung der Vorratsdatenspeicherung und auch der europäischen  
4346 Rechtsgrundlage kommt;

4347 - auch mögliche Alternativen zu einer anlasslosen Vorratsdatenspeicherung zu prüfen;

- 4348 - zu klären, ob bezüglich der Dauer einer Speicherung und des Datenumfangs eine Rückkehr zu  
 4349 der bis circa 2006 geltenden Situation möglich ist: Internet-Access-Provider haben damals IP-  
 4350 Adressen circa 80 Tage gespeichert, E-Mail-Verbindungsdaten hingegen nur wenige Tage zu  
 4351 technischen Analyse Zwecken;
- 4352 - dass, sofern eine Datenspeicherung auf Vorrat erfolgen soll, die Art der zu speichernden Daten  
 4353 als auch die Speicherdauer nicht einzelnen Unternehmen überlassen werden darf, sondern gesetzlicher  
 4354 Regelungen bedürfen.
- 4355 Die Enquete-Kommission fordert deshalb den Deutschen Bundestag auf,
- 4356 1. die Bundesregierung aufzufordern, auf europäischer Ebene darauf hinzuwirken, dass die  
 4357 Vorratsdatenspeicherungsrichtlinie grundlegend überarbeitet und eine Verkürzung der  
 4358 Speicherfrist auf deutlich unter 6 Monaten aufgenommen wird. Dabei sollten insbesondere für  
 4359 sensible Daten wie beispielsweise Telefon-Verbindungsdaten, Mobilfunk-Ortsdaten und E-Mail-  
 4360 Verbindungsdaten maximal eine auf wenige Tage beschränkte Speicherdauer und hohe  
 4361 Zugriffshürden gelten. Bei den weniger sensiblen, aber in der Praxis wichtigeren IP-Adressen  
 4362 sind längere Speicherfristen denkbar;
- 4363 2. dass, sollte an der Vorratsdatenspeicherung festgehalten werden, verfassungskonforme  
 4364 gesetzliche Regelungen notwendig sind, die eine Speicherung von und den staatlichen Zugriff auf  
 4365 diese Daten regeln und mit dem Urteil des Bundesverfassungsgerichts vereinbar sind.
- 4366 Bei der konkreten Fassung der Regelungen sollten folgende Anforderungen mit aufgenommen  
 4367 werden:
- 4368 a. Der Abruf und die Nutzung der Verbindungsdaten darf nur bei Verdacht auf schwerste Straftaten  
 4369 erfolgen. Das sind insbesondere Straftaten gegen das Leben, die körperliche Unversehrtheit und  
 4370 die sexuelle Selbstbestimmung.
- 4371 b. Als milderer und weniger eingriffsintensives Mittel kann eine Beauskunftung von IP-Adressen  
 4372 geregelt werden. Dabei sollte ein Abruf innerhalb einer kurzen Frist von wenigen Tagen ab  
 4373 Speicherung zudem zum Zwecke der Verfolgung von Straftaten erfolgen können. Nach Ablauf  
 4374 dieser Frist darf der Datenabruf bis zur Löschung der Daten nur noch zur Verfolgung schwerster  
 4375 Straftaten erfolgen.
- 4376 c. Für Berufsheimlichkeitsverpflichtete ist ein absolutes Verwertungsverbot vorzusehen.
- 4377 d. Der Abruf aller Verbindungsdaten soll unter Richtervorbehalt stehen.
- 4378 e. Es ist eine Unterrichtungspflicht für die von einem Datenabruf Betroffenen aufzunehmen. Dies  
 4379 gebietet das Rechtsstaatsverständnis und entspricht im Übrigen den verfassungsrechtlichen  
 4380 Vorgaben.
- 4381 f. Die Bestimmungen zum technischen Datenschutz müssen entsprechend den  
 4382 verfassungsgerichtlichen Vorgaben deutlich ausgebaut werden. Dazu gehören namentlich eine  
 4383 getrennte Speicherung, die sichere Verschlüsselung von Daten, das Vier-Augen-Prinzip  
 4384 verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den  
 4385 Schlüsseln und eine revisionssichere Protokollierung von Zugriff und Löschung.
- 4386 g. Eine effektive Kontrolle muss gewährleistet werden, Verstöße müssen wirksam sanktioniert  
 4387 werden.

- 4388 h. Eine Nutzung der Daten darf ausschließlich für strafrechtliche, nicht für zivilrechtliche Auskünfte  
 4389 erfolgen.  
 4390
- 4391 Eine unterschiedliche Behandlung von IP-Adressen und anderen sensiblen Daten ist bereits im  
 4392 genannten Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung angelegt, ergibt sich  
 4393 aber auch aus der Eingriffstiefe und Sensibilität der Daten. Mit Telefon- und E-Mail-  
 4394 Verbindungsdaten lassen sich umfangreiche Nutzungs- sowie Kommunikationsprofile, mit  
 4395 Mobilfunkdaten zusätzliche Bewegungsprofile erstellen. Die mit dem Grimme Online Award  
 4396 ausgezeichnete<sup>299</sup> Visualisierung von Zeit Online der aufgrund der ehemaligen gesetzlichen Vorgaben  
 4397 gespeicherten Vorratsdaten von Malte Spitz zeigt eindrucksvoll, was eine allgegenwärtige  
 4398 Beobachtung bedeutet.<sup>300</sup>
- 4399 Eine viel geringere Eingriffstiefe hat jedoch die Speicherung der Zuordnung von IP-Adressen zu  
 4400 Anschlussinhabern bei Internetverbindungen. Anders als vielfach behauptet ist damit keine komplette  
 4401 Überwachung des Surfverhaltens der Nutzerinnen und Nutzer möglich. Im Gegensatz zur  
 4402 Durchführung einer gezielten Telekommunikationsüberwachung kann damit nicht festgestellt werden,  
 4403 welche Webseiten ein Internetnutzer aufgerufen hat. Es ist ausschließlich möglich, im Nachhinein  
 4404 nach einer konkreten Straftat bei Kenntnis der IP-Adresse den Anschlussinhaber herauszufinden. Die  
 4405 Sorge einer Totalüberwachung der Bevölkerung ist daher im Gegensatz zur Speicherung von Handy-  
 4406 und E-Mail-Daten unbegründet.  
 4407
- 4408 Bei Straftaten, die mit Hilfe des Internets begangen werden, ist die IP-Adresse oftmals die einzige  
 4409 verwertbare Spur. Daher ist der Wunsch der Ermittlungsbehörden nachvollziehbar, dieses  
 4410 Ermittlungsinstrument nutzen zu können. Dennoch sollten die Transparenzpflichten erhöht und die  
 4411 Speicherfristen auf ein Maß verkürzt werden, das auch vor der Vorratsdatenspeicherung jahrelang  
 4412 üblich war.  
 4413
- 4414 In der Bevölkerung besteht die Sorge, dass die Speicherung von IP-Adressen weiter zu  
 4415 Massenabmahnungen bei der Nutzung von Peer-to-Peer-Tauschbörsen führt. Allerdings sind diese  
 4416 Abmahnungen auch ohne Speicherung der IP-Adressen durch Echtzeitabfragen oder entsprechende  
 4417 Speicheranforderungen („Quick Freeze“) möglich.  
 4418
- 4419 Da mit der skizzierten Regelung sowohl den berechtigten Interessen der Strafverfolgung als auch der  
 4420 Privatsphäre der Bürger Rechnung getragen wird und damit eine grundrechtsschonende Lösung  
 4421 vorliegt, empfiehlt die Enquete-Kommission dem Deutschen Bundestag auf europäischer Ebene, eine  
 4422 entsprechende Initiative zu empfehlen und in Deutschland auf den Weg zu bringen.  
 4423

<sup>299</sup> Zur Begründung der Jury siehe <http://www.grimme-institut.de/html/index.php?id=1345> (zuletzt aufgerufen am: 30. Juni 2011).

<sup>300</sup> Vgl. <http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten> und <http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/> (zuletzt aufgerufen am: 30. Juni 2011).

4424 *Streitiger Textvorschlag der Fraktion DIE LINKE.*

4425 **Vorratsdatenspeicherung**

4426 Mit Urteil vom 2. März 2010<sup>301</sup> hat das Bundesverfassungsgericht das deutsche Gesetz zur  
 4427 Vorratsdatenspeicherung nach Beschwerden Tausender Bürgerinnen und Bürger aufgehoben. Die  
 4428 Aufhebung der Vorratsdatenspeicherung durch das Bundesverfassungsgericht ist in der Folge ohne  
 4429 Einfluss auf die Aufklärung von Internetdelikten geblieben. Ob Verbindungsdaten der gesamten  
 4430 Bevölkerung ohne Anlass auf Vorrat gesammelt werden oder ob eine Speicherung nur gezielt im  
 4431 Bedarfsfall erfolgt, hat keinerlei statistisch signifikante Auswirkung auf die registrierte Anzahl von  
 4432 Straftaten oder die Aufklärungsquote. Der Wissenschaftliche Dienst des Bundestages kann in einer  
 4433 Bilanz der europäischen Anwendungen für die Jahre 2005 bis 2010 keine signifikanten Änderungen  
 4434 der Aufklärungsquoten feststellen.<sup>302</sup> Im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres  
 4435 (LIBE) des Europäischen Parlaments konnte der Vertreter der EU-Kommission am 15. Juni 2011 auf  
 4436 Nachfrage kein Beispiel nennen, bei dem die Vorratsdatenspeicherung für die Aufklärung eines  
 4437 grenzüberschreitenden Delikts eine entscheidende Rolle gespielt hätte.

4438 Gleichwohl plant die Bundesregierung eine Wiedereinführung einer Vorratsdatenspeicherung, wenn  
 4439 auch in eingeschränkter Form, u. a. mit dem Argument, es ginge um die Umsetzung der europäischen  
 4440 Richtlinie. Die Vorratsdatenspeicherung beschädigt jedoch in eklatanter Weise das Recht auf  
 4441 informationelle Selbstbestimmung, wonach jeder Mensch das Recht haben muss, über seine Daten  
 4442 selbst entscheiden zu können, und damit Herr über seine sozialen, politischen und wissenschaftlichen  
 4443 Kontakte und Verbindungen ist.

4444 Mit der Vorratsdatenspeicherung hätte der Staat durch die komplette Protokollierung des  
 4445 Kommunikationsverhaltens der Bevölkerung Zugriff auf unvorstellbar viele Informationen über seine  
 4446 Bürgerinnen und Bürger. Die anlass- und verdachtslose Vorratsdatenspeicherung ist der sanktionierte  
 4447 Ausdruck eines Generalverdachts gegenüber der gesamten Bevölkerung. Denn auch die Registrierung  
 4448 „nur“ der Verbindungsdaten erlaubt weitgehende Rückschlüsse auf den Inhalt der Kommunikation.  
 4449 Die Vorratsdatenspeicherung ist daher ein nicht zu rechtfertigender unverhältnismäßiger Eingriff in  
 4450 die Bürgerrechte.

4451 Die Enquete-Kommission empfiehlt dem Deutschen Bundestag daher,

- 4452 - keine weiteren gesetzgeberischen Maßnahmen in Richtung anlassloser und
- 4453 verdachtsunabhängiger Vorratsdatenspeicherung zu ergreifen;
- 4454 - auf europäischer Ebene nicht nur die Reform der Richtlinie zur Vorratsdatenspeicherung
- 4455 mitzugestalten, sondern den vollständigen Verzicht auf dieses Instrument durchzusetzen.

<sup>301</sup> BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 - Vorratsdatenspeicherung.

<sup>302</sup> Becher, Johannes (2011). Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedstaaten. Wissenschaftliche Dienste. WD 7 – 3000 – 036/11 (Link wird noch vom Sekretariat ergänzt.)



4456 *Streitiger Textvorschlag der Fraktion BÜNDNIS 90 /DIE GRÜNEN.*

4457 **Vorratsdatenspeicherung**

4458 Verpflichtende anlasslose Speicherungen personenbezogener Daten auf Vorrat sind mit den  
4459 datenschutzrechtlichen Grundsätzen von Zweckfestlegung und Erforderlichkeit nicht vereinbar. Sie  
4460 betreffen eine Vielzahl von völlig unbescholtenen Personen unverhältnismäßig und entfalten damit  
4461 eine maximale grundrechtsbeeinträchtigende Streubreite. Zudem eröffnen sie eine höchst  
4462 missbrauchsanfällige Datenquelle und können das Vertrauen in die Nutzung moderner Informations-  
4463 und Kommunikationssysteme beeinträchtigen. Für den behaupteten Nutzen der  
4464 Vorratsdatenspeicherung fehlt es, auch angesichts der besonderen Eingriffsschwere, an empirisch  
4465 überzeugenden Nachweisen.

4466 Verfassungsrechtlich sind sie deshalb als schwerer Grundrechtseingriff u. a. in das Grundrecht auf  
4467 informationelle Selbstbestimmung allenfalls in engsten Grenzen zulässig und unterliegen besonders  
4468 hohen Eingriffsschwellen. Das Bundesverfassungsgericht hat in seinem Urteil vom 2. März 2010<sup>303</sup>  
4469 zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten zusätzliche Anforderungen  
4470 festgelegt, die für eine Realisierung von Vorratsdatenspeicherungsvorhaben erhebliche tatsächliche als  
4471 auch rechtliche Hürden bedeuten.

4472 Mit Blick auf die weiter fortbestehende Verpflichtung zur Umsetzung der  
4473 Vorratsdatenspeicherungsrichtlinie der Europäischen Union und die anhaltende Diskussion um die  
4474 Wiedereinführung der Vorratsdatenspeicherung empfiehlt die Enquete-Kommission dem Deutschen  
4475 Bundestag:

- 4476 **1.** Gesetzliche Vorhaben zur anlasslosen verpflichtenden Vorratsdatenspeicherung von  
4477 Telekommunikationsverkehrsdaten sind abzulehnen.
- 4478 **2.** Gesetzliche Vorhaben zu anderweitigen anlasslosen verpflichtenden Vorratsdatenspeicherungen  
4479 personenbezogener Daten begegnen grundlegenden Bedenken hinsichtlich ihrer  
4480 verfassungsrechtlichen Zulässigkeit und sind deshalb grundsätzlich zu vermeiden.

4481 **4 Sondervoten (zu ergänzen)**

4482  
4483  
4484  
4485  
4486  
4487  
4488

<sup>303</sup> BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08; 1 BvR 263/08 und 1 BvR 586/08, NJW 2010, 833 - Vorratsdatenspeicherung.

4489

4490 **5 Bürgerbeteiligung in der Projektgruppe Datenschutz, Persönlichkeitsrechte**4491 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

4492 Fragen des Datenschutzes und der Persönlichkeitsrechte im Internet betreffen jeden Einzelnen  
 4493 unmittelbar. Auch aus diesem Grund nehmen diese Themen in der öffentlichen Diskussion breiten  
 4494 Raum ein. Die Projektgruppe Datenschutz, Persönlichkeitsrechte war deshalb besonders interessiert  
 4495 daran, die Sichtweise und Ideen der Bürgerinnen und Bürger in ihre Diskussionen einzubeziehen.

4496 **5.1 Bürgerbeteiligung im Forum zum Thema Einwilligung**4497 *Der nachfolgende Text ist in Projektgruppe unstrittig.*

4498 Das Thema Einwilligung war in der Projektgruppe lange Zeit besonders strittig. Um neue Impulse für  
 4499 die projektgruppeninterne Diskussion zu erhalten, sollte die Öffentlichkeit gezielt befragt werden. Im  
 4500 Forum auf der Microsite der Enquete-Kommission konnten vom 20. Dezember 2010 bis 9. Januar  
 4501 2011 Meinungen und Anregungen zu den folgenden fünf Punkten geäußert werden:

4502 *1. Voraussetzungen der Einwilligung*

4503 *Welche Voraussetzungen sollten nach Ihrer Meinung für eine wirksame Einwilligung in die Erhebung*  
 4504 *und Verarbeitung personenbezogener Daten gegeben sein, und in welcher Form? Inwieweit ist für die*  
 4505 *Einwilligung zu differenzieren, z. B. nach der Art der jeweils betroffenen Daten oder nach dem*  
 4506 *jeweiligen Zweck der Datenverarbeitung? [...]*

4507 *2. Information und Transparenz*

4508 *Welche Informationen müssen für Sie vorliegen, damit Sie eigenverantwortlich entscheiden können,*  
 4509 *ob und in welchem Umfang Sie Ihre Daten zur Verfügung stellen? [...]*

4510 *3. Grenzen der Freiwilligkeit und „faktische Zwänge“*

4511 *Welchen Stellenwert haben „faktische Zwänge“, einen bestimmten Dienst (z. B. soziale Netzwerke),*  
 4512 *zu nutzen und deshalb auch in die jeweilige Datenerhebung und -verarbeitung einzuwilligen? [...]*

4513 *4. Einwilligung und Widerspruch*

4514 *Wie bewerten Sie die Möglichkeit, die Einwilligung in bestimmten Fällen durch einen von Ihnen zu*  
 4515 *erhebenden Widerspruch zu ersetzen (opt-in und opt-out)? [...]*

4516 *5. Praktische Ansätze*

4517 *Wie sieht aus Ihrer Sicht eine Einwilligung aus, die einfach und praktikabel ist und Ihnen die*  
 4518 *Ausübung Ihres Rechts auf informationelle Selbstbestimmung ermöglicht? [...]*

4519

4520 Am Ende dieser Konsultationsphase lagen insgesamt 63 Antworten vor. Im Thread „Information und  
 4521 Transparenz“ wurden die meisten Antworten geschrieben (18). Die wenigsten Antworten (6) gingen  
 4522 im Thread „Praktische Ansätze“ ein.

4523 Die Projektgruppe hat sich in ihrer Sitzung am 17. Januar 2011 ausführlich mit den Kommentaren und  
 4524 Ideen der Bürgerinnen und Bürger auseinandergesetzt. Viele der geäußerten Gesichtspunkte finden  
 4525 sich in den Texten der Projektgruppe wieder, wenn auch möglicherweise mit anderen  
 4526 Schlussfolgerungen. Beispielsweise wurde von mehreren Nutzern auf die Bedeutung der Transparenz  
 4527 hingewiesen. Zu dieser Frage hat sich die Projektgruppe in ihrem Bericht unter *2.1.2 Grundprinzipien*  
 4528 *des Datenschutzrechts – Transparenzgrundsatz* und unter *2.3.2 Ausgestaltung und Reichweite von*  
 4529 *Transparenzinstrumenten* ausführlich geäußert. Die von Nutzern mehrfach angesprochene Problematik  
 4530 der begrenzten Anwendbarkeit und Durchsetzbarkeit nationaler Datenschutzregelungen ist  
 4531 Gegenstand des Abschnitts *2.1.9 Die Grenzen des nationalen Datenschutzes*.

4532 Da die Projektgruppe Datenschutz, Persönlichkeitsrechte eine der ersten Projektgruppen der Enquete-  
 4533 Kommission Internet und digitale Gesellschaft war, standen in den ersten Monaten ihrer Tätigkeit  
 4534 Beteiligungsmöglichkeiten aus technischen Gründen noch nicht in vollem Umfang zur Verfügung.  
 4535 Auch die Befragung der Bürgerinnen und Bürger zum Thema Einwilligung wurde zu einem Zeitpunkt  
 4536 durchgeführt, an dem außer dem Forum auf der Microsite der Enquete-Kommission andere  
 4537 Beteiligungstools noch nicht genutzt werden konnten.

## 4538 **5.2 Bürgerbeteiligung auf der Online-Beteiligungsplattform der Enquete-Kommission**

### 4539 ***Der nachfolgende Text ist in Projektgruppe unstrittig.***

4540 Nachdem am 24. Februar 2011 die Online-Beteiligungsplattform der Enquete-Kommission  
 4541 freigeschaltet worden war, hat die Projektgruppe Datenschutz, Persönlichkeitsrechte die Öffentlichkeit  
 4542 im Rahmen von zwei weiteren Beteiligungsphasen in ihre Arbeit einbezogen. Beginnend am 15. März  
 4543 2011 wurden dort alle Texte, die von der Projektgruppe erarbeitet worden waren, zur Diskussion und  
 4544 Kommentierung eingestellt. Dies waren 61 Texte der Kapitel *1. Bestandsaufnahme bestehender*  
 4545 *Datenschutzregelungen*, *2.1 Datenschutz – Prinzipien, Ziele, Werte* und *2.2 Datenschutz im*  
 4546 *öffentlichen Bereich* und *2.3 Datenschutz im nicht-öffentlichen Bereich*. Entsprechend dem Fortgang  
 4547 der Arbeiten in der Projektgruppe wurden die Texte fortlaufend ergänzt. Bis zum 30. März 2011  
 4548 konnten Texte bearbeitet und nachfolgend bis zum 4. April 2011 über Vorschläge abgestimmt werden.

4549 Die Resonanz auf diese Papiere war gering. Dies ist möglicherweise darauf zurückzuführen, dass –  
 4550 bedingt durch den Zeitpunkt der Freischaltung der Online-Beteiligungsplattform – ein Einstieg in die  
 4551 Beteiligung erst erfolgen konnte, als die Arbeiten der Projektgruppe schon weit fortgeschritten waren.  
 4552 Eine kontinuierliche Beteiligung der Bürger durch alle Phasen der Projektgruppenarbeit war daher  
 4553 nicht mehr möglich.

4554 Dass es auch anders geht, zeigte sich im Verlauf der zweiten Beteiligungsphase. Wesentliches Ziel der  
 4555 Enquete-Kommission Internet und digitale Gesellschaft ist es, politische Handlungsempfehlungen zu  
 4556 erarbeiten, die der weiteren Verbesserung der Rahmenbedingungen der Informationsgesellschaft in

4557 Deutschland dienen.<sup>304</sup> Daher war es wichtig, gerade bei der Formulierung der  
 4558 Handlungsempfehlungen, die sozusagen das Herzstück der Projektgruppenarbeit sind,  
 4559 Bürgerbeteiligung zu ermöglichen. Um eine erleichterte Beteiligung zu gewährleisten, wurde in dieser  
 4560 Beteiligungsphase auf die systemseitig eigentlich vorgesehene formalisierte Abstimmung verzichtet.  
 4561 Stattdessen erfolgte die Abstimmung über die Bewertungsmöglichkeit direkt am Vorschlag selbst.

4562 Zwischen dem 20. April 2011 und dem 17. Mai 2011 konnten entsprechende Vorschläge eingestellt  
 4563 werden. Die Ergebnisse wurden in den Projektgruppensitzungen am 9. Mai, 27. Mai und 6. Juni 2011  
 4564 diskutiert.

4565 Insgesamt haben sich mittlerweile 119 Online-Mitglieder für die Projektgruppe „Datenschutz und  
 4566 Persönlichkeitsrechte“ der Beteiligungsplattform registriert und 32 Vorschläge<sup>305</sup> sowie 73  
 4567 Kommentare abgegeben<sup>306</sup>. Davon wiesen 25 Vorschläge einen – häufig sehr direkten – inhaltlichen  
 4568 Bezug zu Problemstellungen auf, die von der Projektgruppe bei der Erarbeitung der  
 4569 Handlungsempfehlungen diskutiert worden waren, wie zum Beispiel die Vorschläge  
 4570 „Selbstdatenschutz fördern“ und „Schutz unseres Wohnungs-Nutzungsverhaltens im Zeitalter  
 4571 elektronischer Zähler“. Vier Vorschläge betrafen Fragen, die in der Projektgruppe bisher nicht erörtert  
 4572 worden waren. Dies gilt etwa für die Forderung, § 5 des Gesetzes über das Bundesamt für Sicherheit  
 4573 in der Informationstechnik (BSIG) aufzuheben, oder für das Modell eines „FairTrade“ von Daten im  
 4574 Internet. Drei Vorschläge beinhalteten nicht spezifisch datenschutzrechtliche Fragen.

4575 In einigen Fällen deckten sich die Vorschläge der Bürgerinnen und Bürger vollständig oder zumindest  
 4576 sehr weitgehend mit Vorschlägen, die aus den Reihen der Projektgruppenmitglieder in die Diskussion  
 4577 eingebracht worden waren. Dies betrifft etwa die Empfehlungen, ein Verwertungsverbot für  
 4578 rechtswidrig erteilte Auskünfte über Nutzer von Internetdiensten einzuführen und erteilte  
 4579 Einwilligungen grundsätzlich zu befristen, sowie die Vorschläge, bei Datenschutzverstößen eine  
 4580 verschuldensunabhängige Ersatzpflicht auch für nicht-öffentliche Stellen und eine pauschalierte  
 4581 Entschädigung immaterieller Schäden vorzusehen.

4582 In anderen Fällen haben sich Mitglieder der Projektgruppe Vorschläge aus der Online-  
 4583 Beteiligungsplattform der Enquete-Kommission zu eigen gemacht und in ihre Texte übernommen.  
 4584 Diese Punkte sind also ausschließlich durch die Mitarbeit der Bürgerinnen und Bürger in die  
 4585 Projektgruppe hineingetragen worden. So sind die Forderung, dass im Hinblick auf die Einführung  
 4586 von IPv6 bei jedem Einwahlvorgang die dynamische Zuteilung einer neuen IP-Adresse anzubieten sei,  
 4587 und der Vorschlag „*Systematische Evaluierung aller Überwachungsgesetze*“ aus der  
 4588 Beteiligungsplattform in die Handlungsempfehlungen einzelner Fraktionen übernommen worden.<sup>307</sup>

<sup>304</sup> Vgl. Beschluss zur Einsetzung einer Enquete-Kommission Internet und digitale Gesellschaft, BT-Drs.17/950, S. 4.

<sup>305</sup> Zwei dieser Vorschläge stammten bereits aus der ersten Beteiligungsphase (15. März bis 4. April 2011).

<sup>306</sup> Stand: 30. Juni 2011.

<sup>307</sup> nach Beschlussfassung in der Enquete-Kommission: Fundstellen der beiden Vorschläge im Zwischenbericht in die Fußnote einfügen; ggf. ist der Satz nach Abstimmung in der Enquete-Kommission zu aktualisieren.

4589 Insgesamt hat sich gezeigt, dass die große Mehrzahl der Themen, die für die teilnehmenden  
4590 Nutzerinnen und Nutzer wichtig waren, auch in den sonstigen Berichtsteilen der Projektgruppe  
4591 Datenschutz, Persönlichkeitsrechte (das heißt insbesondere im Kapitel 2.) aufgegriffen und erörtert  
4592 wurden.

4593

4594 Zu ergänzen:

4595

4596 Literaturverzeichnis etc.

---