Hochschule für Politik München (Dr. Petri)

Sommersemester 2014: Einführung in Datenerfassung und Datenschutz (G)

Grundlagenskript

Version 2.0 (30.4.2014)

1. Allgemeine Hinweise

Folgende Grundlagentexte werden bei jeder Vorlesungsstunde benötigt (bitte mitbringen!):

- Grundgesetz (GG, abrufbar unter www.gesetze-im-internet.de)
- Bundesdatenschutzgesetz (BDSG, abrufbar unter www.gesetze-im-internet.de);
- Bayerisches Datenschutzgesetz (BayDSG, abrufbar unter www.gesetze-bayern.de).

Buchempfehlungen: Wer sich über dieses Grundlagenskript hinaus mit dem Thema Datenschutz auseinandersetzen will, dem wird das Buch von Jan-Hinrik Schmidt / Thilo Weichert (Hrsg.), Datenschutz, Bundeszentrale für politische Bildung, Band 1190 (4,50 Euro zzgl. Porto) empfohlen. Beiträge aus diesem Buch werden als Literaturhinweis im Skript wie folgt zitiert: Verfasser/in in BPB, Seiten. Andere Einführungen in das Datenschutzrecht bieten z.B. Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, Oldenbourg-Verlag, 5. Auflage 2012 (zitiert nur mit Namen und Seitenangabe) und Kühling/Seidel/Sivridis, Datenschutzrecht, C.F.Müller-Verlag, 2. Auflage 2011 (zitiert mit Namen und Seitenangabe).

Jeweils am Ende eines Textabschnitts befinden sich **Lektürehinweise**, die aus den empfohlenen Büchern entnommen sind. Um den Lesefluss nicht unnötig zu beeinträchtigen, werden sie nur am Ende eines jeweiligen Textabschnittes aufgeführt. Sie sind mit einem Pfeil gekennzeichnet:

- ⇨ Literaturhinweis

Sonstige **Quellennachweise** im Text werden in eckige Klammern […] gesetzt. Sie haben in erster Linie eine Nachweisfunktion – die Lektüre der Quellennachweise wird nicht erwartet, es sei denn, es wird ausdrücklich darauf verwiesen („Lesen!“).

2. Was soll privat, was öffentlich sein?

Der langjährige Chief Executive Officer von Google, Eric Smith, wird sinngemäß dahingehend zitiert, dass seiner Auffassung nach der Schutz der Privatsphäre überholt sei:

> **"***Wir wissen wo du bist, wir wissen wo du warst und wir wissen mehr oder weniger auch, was du gerade denkst.*"
>
> [Interview, The Atlantic", 1. Oktober 2010]
>
> "*If you have something that you don't want anyone to know, maybe you shouldn't do it in the first place.*"
>
> [Interview, CNBC, 3. Dezember 2009][1]

Dem Gründer von Facebook Marc Zuckerberg wird die Äußerung nachgesagt, der Umgang der Menschen mit ihren Daten habe sich stark verändert. Die Menschen fühlten sich heutzutage wohl, wenn sie persönliche Informationen mit vielen Menschen teilen. Die sozialen Normen hätten sich in dieser Beziehung verändert. Die Rolle von Facebook bestehe lediglich darin, die aktuellen sozialen Normen zu reflektieren.

Natürlich sind derartige Äußerungen von führenden Repräsentanten großer Internetunternehmen von wirtschaftlichen Eigeninteressen geprägt. Und Facebook reflektiert nicht nur den gesellschaftlichen Wandel in Bezug auf Privatsphäre, sondern versucht ihn selbst auch in seinem Sinne aktiv voranzutreiben. Allerdings stehen sie mit ihrer Auffassung nicht völlig allein. Nach der **Post-Privacy-Bewegung** führt das Internet dazu, dass die „*Privatsphäre als persönlicher Raum …praktisch tot*" sei (und viele Vertreter von Post Privacy begrüßen diesen Befund). Anstatt einen vergeblichen Kampf zur Verteidigung des Datenschutzes durchzuführen, sei die Frage wichtiger, wie *wir das Leben ohne die Sicherheiten der Privatsphäre lebenswert machen können* [Christian Heller, Post-Privacy – Prima Leben ohne Privatsphäre, 2011, Umschlagtext].

- ⇨ Franziska Bluhm in BPB, S. 237 ff.
- ⇨ Michael Seemann in BPB, S. 243 ff.

Unbestreitbar hat das Internet zu einer Veränderung im Verhältnis Privatsphäre – Öffentlichkeit geführt, was auch immer man unter diesen beiden Begriffen zu verstehen hat.[2] Wer die Abschaffung der Privatsphäre befürwortet, vernachlässigt jedoch den Umstand, dass Menschen von Natur aus nicht nur „öffentliche Wesen" sind. Für eine gesunde Identitätsentwick-

[1] Eric Smith wies in einem späteren Interview auf der Computermesse CeBIT 2012 darauf hin, das zweite Zitat sei aus dem Zusammenhang gerissen worden. Es habe sich auf den Patriot Act bezogen. Privatsphäre sei wichtig.
[2] Die Bedeutung hängt ganz erheblich von dem fachlichen Zugang (Rechtswissenschaft, Informatik, Psychologie, Soziologe usw.) und natürlich auch vom Vorverständnis des jeweiligen Betrachters ab.

lung benötigen sie gleichzeitig Formen der Selbstoffenbarung *und* der Privatsphäre.[3] **Aus psychologischer Sicht** beschreibt der Begriff Privatsphäre, inwieweit ein Mensch anderen Menschen Zutritt zu seiner eigenen Welt gewährt. Jeder Mensch muss versuchen, für sich eine **ausgewogene Balance zwischen Zurückgezogenheit und Selbstöffnung** zu finden. Dieses Verhältnis verändert sich permanent und ist insbesondere von den jeweiligen Lebensumständen des Betroffenen abhängig [zur Identitätsbildung und Sozialisation von Jugendlichen vgl. z.B. Johannes Burger, Die öffentliche Privatsphäre Jugendlicher auf Social Networks Sites, Wien 2010, S. 28 ff.]. Eine intakte Privatsphäre erfüllt dabei mehrere wichtige Funktionen:

- Autonomie:
  Privatsphäre ermöglicht es, soziale Normen zu durchbrechen, mit neuem Verhalten und Gedanken zu experimentieren
- Emotionale Erleichterung:
  Man kann sich in wertfreier Umgebung – allein oder mit anderen – den Anforderungen und der Stimulation der Umwelt entziehen
- Selbstevaluation:
  Privatsphäre ermöglicht es, aufrichtig zwischen den persönlichen Idealen und der eigenen Leistung abzuwägen
- Geschützte Kommunikation:
  Sie schafft eine Situation, die vertrauten Anderen Einblicke in das „wahre Ich" gewährt und in denen mentale Distanz gering ist.

[nach Westin, Privacy and Freedom, New York, Atheneum. 1967]

Soziale Netzwerke wie Facebook, Google+ usw. kommen zwar dem Bedürfnis der Menschen nach Selbstoffenbarung entgegen. Letztlich beeinflussen Soziale Netzwerke jedoch das Verhältnis zwischen Selbstöffnung und Privatsphäre, indem sie die Balance zulasten der Privatsphäre verschieben. Die „Spielregeln" werden dabei maßgeblich und nicht immer fair von den Anbietern vorgegeben.

[3] Das scheint im Übrigen nicht nur für Menschen zu gelten. Auch zahlreiche im Sozialverbund lebende Tiere zeigen gewisse Verhaltensweisen der „Privatsphäre". Beispielsweise gehört es auch bei Gruppentieren in aller Regel zur artgerechten Haltung, dass Einzeltiere die Gelegenheit haben, sich bei Bedarf von der Gruppe zurückzuziehen.

Dramatische Cyber-Mobbing Fälle wie die von Amanda Todd oder Reatha Parsons zeugen jedenfalls davon, dass der mangelnde Respekt vor dem informationellen Persönlichkeitsrecht dramatische Auswirkungen haben kann.[4]

- ⇨ Sabine Trepte in BPB, S. 59-66.
- ⇨ Ulrike Wagner/Christa Gebel/Niels Brüggen in BPB, S. 226-236.

Die Entwicklung der Informationstechnologie hat nicht nur Einfluss auf die Gestaltung der Privatsphäre, sondern auch auf die Selbstbestimmung im Übrigen. Offenkundig ist dies beispielsweise bei technik-gestützten Überwachungsmaßnahmen. Das wird nachfolgend am Beispiel der **Videoüberwachung öffentlicher Räume** erörtert: Sie dient in aller Regel (zumindest auch) der Verhaltenssteuerung: Sie soll nämlich vor Allem potenzielle Täter davon abhalten, Straftaten zu begehen. Ihre Eignung ist jedoch nur für einige Räume und Kriminalitätsformen belegt. Beispielsweise gilt es als nachgewiesen, dass Diebstähle von und aus Kraftfahrzeugen in Parkhäusern durch Videoüberwachung durchaus erheblich reduziert werden, wenn die Überwachung mit einer besseren Beleuchtung kombiniert wird. Demgegenüber scheint die Videoüberwachung im Öffentlichen Personennahverkehr kaum zu einem Kriminalitätsrückgang beizutragen [Stiftung Deutsches Forum zur Kriminalitätsprävention, CCJG-Review: Die Wirksamkeit von Videoüberwachung, 2005, siehe auch Dieter Kammerer, Bilder der Überwachung, Frankfurt 2008, S. 73 ff.]. Insgesamt scheint der Erfolg von Videoüberwachung im öffentlichen Raum maßgeblich davon abzuhängen, ob sie von anderen Maßnahmen begleitet wird (z.B. bauliche Maßnahmen, polizeiliche Einsatzkonzepte, die ein schnelles Eingreifen sicherstellen usw.).
Mittlerweile gibt es einige Untersuchungen der Wirksamkeit von Videoüberwachung. Selten sind demgegenüber Untersuchungen der Frage, welche **Auswirkungen Videoüberwachung auf das Verhalten der beobachteten Personen und auf unsere Gesellschaft** hat. *Dass* sie Auswirkungen auf die Persönlichkeit der so Beobachteten und auf unsere Gesellschaft entfaltet, liegt zumindest sehr nahe. Im öffentlichen Raum oder auch im persönlichen Gespräch können sich Menschen üblicherweise wechselseitig ansehen. Ein „Blickwechsel“ erleichtert die Einordnung eines fremden Menschen. Eine unangemessen lange Beobachtung durch einen uns fremden Betrachter werten wir als Verstoß gegen die gesellschaftliche Interaktionsordnung und sanktionieren sie notfalls auch (unangemessen ist z.B. das „Anstarren“ während einer Bus- oder Zugfahrt oder im Aufzug). Menschliche Beobachtung ist also typischerweise kein einseitiger Prozess, sondern eine Form der menschlichen Interaktion. Das ist bei der

[4] Beide jungen Frauen begangen Selbstmord. Bei Amanda Todd kursierten Intim-Fotos im world wide web, bei Rethae Parsons Bilder ihrer Vergewaltigung.

Überwachung durch Videokameras regelmäßig anders. Ob die Bilder einer Videoüberwachung überhaupt, ob sie angemessen oder missbräuchlich verwendet werden, lässt sich oft nicht unmittelbar erkennen. Ähnlich wie bei Sozialen Netzwerken wird damit vermutlich auch die Videoüberwachung eine Veränderung des Verhältnisses Privatsphäre – Öffentlichkeit bewirken. Einige Soziologen vermuten beispielsweise, dass die Gewöhnung an Videokameras und Webcams zu einer massenhaften Lust an intimer Beobachtung („Big Brother"-Formate) beigetragen hat [Markus Schroer, Sehen, Beobachten, Überwachen – ein Beitrag zu einer Soziologie der Aufmerksamkeit, in Leon Hempel und Jörg Metelmann, Bild-Raum-Kontrolle, Frankfurt 2005, S. 336 f., ebendort auch Werner Rammert, Gestörter Blickwechsel durch Videoüberwachung? Ambivalenzen und Asymmetrien soziotechnischer Beobachtungsordnungen, S. 353]. Es spricht auch einiges dafür, dass Videoüberwachung das individuelle Verantwortungsgefühl beeinträchtigt. Immerhin zeichnet die Kamera ein mögliches Fehlverhalten auch von Helfern auf. Zugleich suggeriert sie eine zeitnahe Reaktion von berufener Seite (etwa von Sicherheitskräften) – ohne dass diese immer tatsächlich gewährleistet ist. Videoüberwachung ist also ambivalent. Unter bestimmten Voraussetzungen kann sie einerseits ein sinnvolles Überwachungsinstrument etwa zum Schutz von Eigentum sein. Die mit ihr verbundene Beobachtung menschlichen Verhaltens kann andererseits auch bloßstellend wirken. Zu berücksichtigen ist dabei, dass die weitaus überwiegende Anzahl der so Beobachteten keinen Anlass für die Überwachung gegeben hat.

Verallgemeinert man diesen Befund, dann drängt sich die Schlussfolgerung auf, dass die technik-gestützte Beschaffung von personenbezogenen Daten in aller Regel wertneutral ist. Damit ist gemeint, dass personenbezogene Datenverarbeitung einerseits für legitime Zwecke eingesetzt werden kann, andererseits auch zu Risiken für unsere Selbstbestimmung führt. Das **Bundesverfassungsgericht** hat die möglichen individuell-gesellschaftlichen Auswirkungen der modernen Informationstechnologie im berühmten **Volkszählungsurteil** bereits im Jahr 1983 wie folgt treffend beschrieben:

> *„Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener*

Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Artikel 8, 9 Grundgesetz) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“

[Bundesverfassungsgericht, Urteil vom 15.12.1983 – Aktenzeichen: 1 BvR 209/83 u.a., unter C.II.1.a)]

Welche Antworten das Datenschutzrecht auf diesen Befund gibt, wird nach einem kurzen Abriss der Entwicklung des Datenschutzes in Abschnitt 4 und Abschnitt 5 untersucht.

3. Geschichte des Datenschutzes

Die Geschichte der Privatsphäre hängt eng mit den bereits angesprochenen Vorstellungen zusammen, was unter „privat“ und was unter „öffentlich“ zu verstehen sei. Diese Vorstellungen unterliegen einem ständigen Wandel. Die Entwicklung des Städtewesens und des modernen Staates (Bürokratie jeweils inklusive), die Entdeckung des Individuums, der Buchdruck, die Entwicklung von Massenmedien und der Informationstechnologie haben dabei sicherlich eine Rolle gespielt.

Die **Entwicklung des Datenschutzes als Antwort auf die Entwicklung der Informations- und Kommunikationstechnologie** beginnt Anfang der 1960er Jahre. Wegbereitend ist das sogenannte Mikrozensusurteil vom 16. Juli 1969.[5] Das Bundesverfassungsgericht stellte seinerzeit fest, dass das Grundgesetz dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung gewährt. „Unantastbar“ bedeutet, dass eine Datenverarbeitung von kernbereichsrelevanten Daten durch die öffentliche Gewalt unter keinen Umständen gerechtfertigt ist. Das Bundesverfassungsgericht hat dies mit der Menschenwürde aus Art. 1 Abs. 1 des Grundgesetzes (GG) begründet:

> *„Im Lichte dieses Menschenbildes kommt dem Menschen in der Gemeinschaft ein sozialer Wert- und Achtungsanspruch zu. Es widerspricht der menschlichen Würde, den Menschen zu einem bloßen Objekt im Staat zu machen (…). Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandaufnahme in jeder Beziehung zugänglich ist.*
>
> *Ein solches Eindringen in den Persönlichkeitsbereich durch eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Bürger ist dem Staat auch deshalb versagt, weil dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum“ verbleiben muss, in dem er „sich selbst besitzt“ und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt (…).“*
>
> *[BVerfG, U.v. 16.07.1969 – 1 BvL 19/63, unter C.II.1 b)]*

Im Jahr 1970 trat in Hessen das erste Datenschutzgesetz der Welt in Kraft, weitere Datenschutzgesetze von anderen Bundesländern folgten. Ein erstes Bundesdatenschutzgesetz

[5] Entscheidungen des Bundesverfassungsgerichts ab Januar 1998 sind auf der Webseite des Gerichts abrufbar: www.bundesverfassungsgericht.de unter „Entscheidungen“. Ältere Entscheidungen sind dort leider nicht verfügbar, aber oft anderweitig im www zu recherchieren. Die nachfolgende Mikrozensus-Entscheidung ist beispielsweise unter http://www.telemedicus.info/urteile/Allgemeines-Persoenlichkeitsrecht/420-BVerfG-Az-1-BvL-1963-Mikrozensus.html abrufbar (Abrufdatum: 3.5.2013).

(BDSG) folgte im Jahr 1977. Die **erste Generation von Datenschutzgesetzen** sah für den Einzelnen in erster Linie nur einen **Schutz vor der missbräuchlichen Verwendung** vor. § 1 Abs. 1 BDSG 1977 beschreibt den Zweck des Gesetzes wie folgt (Auszug):

> *„Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Missbrauch … der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken."*

Von bahnbrechender Bedeutung für die Entwicklung des Datenschutzes war jedoch die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983. In diesem **Volkszählungsurteil** verdeutlichte das Bundesverfassungsgericht zunächst die grundrechtlichen Wurzeln des Datenschutzes aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1, Art. 1 Abs. 1 GG). Zugleich stellte es fest, dass das allgemeine Persönlichkeitsrecht einen Datenschutz verlangt, der weit über einen Missbrauchsschutz hinausgeht. Datenschutz ist auch nicht nur mit dem Schutz der Privatsphäre im Sinne der Abwehr staatlicher Ausforschung gleichzusetzen. Das Bundesverfassungsgericht leitet vielmehr aus dem Persönlichkeitsrecht ein **Recht auf informationelle Selbstbestimmung** ab. Das Bundesverfassungsgericht definiert dieses Recht wie folgt:

> „*Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." [BVerfG, U.v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, unter C.II.1.a)]*

Das Gericht hat freilich auch klargestellt, dass diese Befugnis nicht als uneingeschränktes Herrschaftsrecht missverstanden werden darf. Die betroffene Person kann also nicht wie beim Eigentum über ihre Daten verfügen und andere von der Datenverarbeitung gänzlich nach Belieben ausschließen. Die hoheitliche Datenverarbeitung muss aber gesetzlich legitimiert sein und ist für die Betroffenen so transparent wie möglich zu gestalten (zur Reichweite und zu den Beschränkungen des Grundrechts auf Datenschutz siehe unter Abschnitt 4).

Ein weiteres Urteil des Bundesverfassungsgerichts hat die Entwicklung des Datenschutzrechts vorangetrieben. Seine Auswirkungen sind gegenwärtig noch nicht vollständig abschätzbar. Diese Entscheidung vom 27.02.2008 (1 BvR 370, 595/07) betrifft die so genannte Online-Durchsuchung. Das Bundesverfassungsgericht hatte dabei die Frage zu beurteilen, ob und

unter welchen verfassungsrechtlichen Voraussetzungen Sicherheitsbehörden mithilfe von Schadsoftware („Staatstrojaner“) in informationstechnische Systeme von Verdächtigen eindringen können. Das Bundesverfassungsgericht leitete aus dem allgemeinen Persönlichkeitsrecht eine neue Schutzdimension ab: das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**. In der Literatur wird es häufig verkürzt als „**IT-Grundrecht**“ bezeichnet. Es schützt vor der heimlichen

> „*Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können.*“

Das Bundesverfassungsgericht hat in diesem Urteil zum ersten Mal das datenschutzrechtliche Problem aufgegriffen, dass es aufgrund der Technikentwicklung neben Chancen auf Bedrohungen für informationelle Freiheiten gibt, selbst wenn die verwendeten Daten (noch) keinen Personenbezug aufweisen. Die grundrechtlich relevante Besonderheit der Infiltration von IT-Systemen liegt darin, dass die Maßnahme zumeist auf einem Schlag den Zugriff auf äußerst aussagekräftige Datenbestände eröffnet. Zugleich wird die Integrität des so angegriffenen IT-Systems verletzt. Dementsprechend haben Beeinträchtigungen dieses neuen IT-Grundrechts regelmäßig ein hohes Eingriffsgewicht. Sie sind nur unter strengen Voraussetzungen zu rechtfertigen (siehe dazu Abschnitt 4).

Nicht nur die Rechtsprechung insbesondere des Bundesverfassungsgerichts hat zur Entwicklung des Datenschutzrechts in Deutschland und in Bayern beigetragen. Die deutsche Gesetzgebung zum Datenschutz ist spätestens seit den 1990er Jahren auch nachhaltig durch **Europäisches Datenschutzrecht** geprägt. Bedeutsam ist zunächst die allgemeine EG-Datenschutzrichtlinie 95/46/EG. Sie ist im Jahr 2002 durch eine Richtlinie über den Datenschutz bei der elektronischen Kommunikation (RL 2002/58/EG – „E-Privacy-Richtlinie“) ergänzt worden. Die beiden Richtlinien haben den Anwendungsbereich des deutschen Datenschutzrechts erweitert, indem sie die althergebrachte Unterscheidung zwischen öffentlichem und nichtöffentlichem Bereich[6] weitgehend aufgelöst haben. Die im Jahr 2000 verabschiedete EU-Grundrechte-Charta sieht überdies in Art. 8 ausdrücklich ein Grundrecht auf Datenschutz vor. Mit Inkrafttreten des Vertrags von Lissabon ist die Grundrechte-Charta zum Bestandteil des Europäischen Primärrechts geworden und zählt damit zu den „verfassungsrechtlichen“ Grundlagen des Europäischen Rechts. Auf sie stützt die Europäische Kommission beispielsweise ihre Vorschläge für eine **Neuordnung des Europäischen Datenschutzrechtsrahmens**

[6] Grob vereinfacht ausgedrückt betrifft der öffentliche Bereich den Umgang von Behörden oder sonstigen öffentlichen Stellen mit personenbezogenen Daten, während der nichtöffentliche Bereich die Erhebung und Verwendung von Daten durch Unternehmen, Vereine oder sonstige Private umfasst. Siehe dazu z.B. § 2 BDSG.

[die deutsche Fassung des Vorschlags für eine Datenschutz-Grundverordnung ist abgedruckt in Bundesrats-Drucksache 52/12, abrufbar unter www.bundesrat.de unter Drucksachen]
Die frühe Datenschutzgesetzgebung war in erster Linie darauf ausgerichtet, die staatliche oder besser die hoheitliche Datenverarbeitung zu regeln. Im Laufe der Zeit ist jedoch deutlich geworden, dass die Datenverarbeitung von Unternehmen ebenfalls erhebliche Risiken für die Menschen als Beschäftigte und als Verbraucher erzeugt. Anpassungen im Verbraucherschutz und im Bundesdatenschutzgesetz sollten diese Risiken begrenzen und gleichzeitig den Wirtschaftsgrundrechten der Privatwirtschaft Rechnung tragen. Wie bereits unter Abschnitt 2 angesprochen, stellt heute das Internet mit völlig neuen Gefährdungspotenzialen eine der wesentlichen Herausforderungen für das Datenschutzrecht dar. Dementsprechend gewinnt die **technische Ausgestaltung des Datenschutzes** (z.B. „Privacy by Design“, „Privacy by Default“) immer mehr an Bedeutung.

- ⇨ Von Lewinski in BPB, S. 23 – 33
- ⇨ Tinnefeld/Buchner/Petri, S. 3-36

4. Datenschutz als Grundrechtsschutz

Der Datenschutz als eine Ausprägung des Persönlichkeitsrechts ist weltweit anerkannt. Die Allgemeine Erklärung der Menschenrechte (Vereinte Nationen, Resolution 217 A (III) der Generalversammlung vom 10.12.1948) sieht beispielsweise in Artikel 12 mit bestimmten datenschutzrechtlich relevanten Verbürgungen vor:

> *Artikel 12*
> *Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.*

Die Vereinten Nationen haben auch am 14.12.1990 „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien“ beschlossen. Die Vorschriften für den Einzelnen sind freilich nur bedingt durchsetzbar.

- ⇨ Marita Körner in BPB, S, 426 ff.
- ⇨ Kühling/Seidel/Sivridis, S. 5-6.
- ⇨ Tinnefeld/Buchner/Petri, S. 70-72.

Ein völkerrechtlich verbindlicher Vertrag zum Schutz von Menschenrechten ist der **Internationale Pakt über bürgerliche und politische Rechte (IPbpR)** vom 19.12.1966. Er enthält mit Artikel 17 eine Vorschrift, die nahezu wortgleich zu Art. 12 AEMR ist. Der Einzelne hat allerdings auch insoweit keine gerichtlichen Möglichkeiten, eine solche Verletzung seiner Rechte völkerrechtlich verbindlich feststellen zu lassen. Effektiver ausgestaltet ist daher der europäische Grundrechtsschutz nach der Europäischen Menschenrechtskonvention (EMRK), der auch gerichtlich durchsetzbar ist.

> Beispiel:
> Die Enthüllungen des Whistleblowers Edward Snowden zur sogenannten **NSA-Spähaffäre** lassen vermuten, dass angloamerikanische Nachrichtendienste die grundrechtlichen Gewährleistungen des Art. 17 IPbpR vielfach verletzt haben. Der IPbpR sieht allerdings in den Art. 28 – 45 vor, dass ein Ausschuss für Menschenrechte gebildet wird. Ein Individuum kann sich an diesen Menschenrechtsausschuss mit der Behauptung wenden, Opfer der Verletzung eines im IPbpR niedergelegten Rechts zu

sein. Die Sachentscheidung des Menschenrechtsausschusses hat jedoch keine völkerrechtlich bindenden Wirkungen.

Demgegenüber kann jedermann Menschenrechtsklage beim Europäischen Gerichtshof für Menschenrechte erheben, wenn er sich durch die Maßnahme eines Vertragsstaats in seinen Rechten aus der EMRK verletzt fühlt. Wegen der geheimdienstlichen Überwachungsaktivitäten im Zusammenhang mit der NSA-Spähaffäre ist gegen Großbritannien eine solche Menschenrechtsklage anhängig. Nach Art. 46 Absatz 1 EMRK wäre Großbritannien als Vertragsstaat der EMRK verpflichtet, das endgültige Urteil des Gerichtshofs zu befolgen.

Datenschutzrechtliche Bezüge haben insbesondere Art. 8 der Europäischen Menschenrechtskonvention (4.1). Im Rechtsrahmen der Europäischen Union sind Art. 7 und Art. 8 der EU-Grundrechtecharta zu beachten (4.2).

4.1. Europäische Menschenrechtskonvention (EMRK)

Aus Sicht des Grundrechtsschutzes ist die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention - EMRK) eine besondere Erfolgsgeschichte. Weltweit ist sie das am weitesten entwickelte überstaatliche Menschenrechtsschutzsystem. Einen großen Beitrag dazu hat der Europäische Gerichtshof für Menschenrechte (EGMR) geleistet. Urteile mit datenschutzrechtlichen Bezügen hat der EGMR dabei zumeist mit dem Grundrecht auf Achtung des Privat- und Familienlebens aus Art. 8 EMRK begründet.

Art. 8 EMRK hat folgenden Wortlaut:

„*Recht auf Achtung des Privat- und Familienlebens*

1. *Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.*
2. *Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.*“

Alle vier genannten Einzel-Gewährleistungen des Art. 8 EMRK (Privatleben, Familienleben, Wohnung, Korrespondenz) haben starke datenschutzrechtliche Bezüge. Der Datenschutz wird überdies durch ein „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ vom 28. Januar 1981 konkretisiert. Die Bundesrepublik Deutschland hat dieses Abkommen ratifiziert und im Jahr 1985 als Gesetz verabschiedet (Bundesgesetzblatt 1985 II S. 539).
Obwohl Artikel 8 Absatz 2 EMRK eine Vielzahl von Einschränkungen der verbrieften Grundrechte ermöglicht, hat der EGMR auch für Deutschland eine ganze Reihe von Impulsen zum Datenschutz gegeben. Zur Veranschaulichung werden nachfolgend drei Leitentscheidungen aus dem Bereich des Sicherheitsrechts vorgestellt.

Fall 1: Klass gegen Deutschland (Urteil vom 09.09.1978)

Im Jahr 1968 verabschiedete der Deutsche Bundestag nach heftigen innenpolitischen Auseinandersetzungen die sogenannte „Notstandsverfassung“. Sie führte zu einigen Änderungen des Grundgesetzes. Insbesondere wurde der heutige Art. 10 Absatz 2 Satz 2 GG eingefügt (Artikel 10 GG lesen!). Er führte zu dem sogenannten „**Abhörstreit**“. Das Bundesverfassungsgericht erklärte die Grundgesetzänderung in einer Mehrheitsentscheidung (5:3) mit der Maßgabe für verfassungsgemäß, dass Art. 10 Abs. 2 Satz 2 GG im Hinblick auf den Grundsatz der Verhältnismäßigkeit nur so verstanden werden könne, dass er die nachträgliche Benachrichtigung des Überwachten in den Fälle fordere, in denen eine Gefährdung des Zweckes der Überwachungsmaßnahme und eine Gefährdung des Schutzes der freiheitlich-demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes ausgeschlossen werden könne (BVerfG, Urteil vom 15.12.1970, BVerfGE 30, Seite 1 ff.). Ein ehemaliger Oberstaatsanwalt, Herr Klass, hielt mit einigen Beschwerdeführern diese Grundgesetzänderung für einen Verstoß gegen Art. 8 EMRK. Der EGMR stellte in seinem Urteil fest, dass die Befugnis bestimmter Behörden, Brief- und Postsendungen zu öffnen und einzusehen, den Fernschreibverkehr mitzulesen und Telefongespräche abzuhören, einen Eingriff in Grundrechte aus Art. 8 EMRK darstellt. Betroffen seien das Privatleben und die Korrespondenz. Zu Art. 10 Abs. 2 GG stellte der Gerichtshof fest, diese Bestimmung müsse eng ausgelegt werden, da sie eine Ausnahme zu einem von der EMRK geschützten Recht enthalte. Befugnisse zur geheimen Überwachung von Bürgern, wie sie für den Polizeistaat typisch sind, könnten danach nur insoweit hingenommen werden, als sie zur Erhaltung der demokratischen Einrichtungen „unbedingt notwendig“ sind. Mit erkennbarem Unbehagen akzeptierte der EGMR, dass der deutsche Gesetzgeber bei der Einrichtung von Überwachungssystemen

einen gewissen Gestaltungsspielraum hatte, der hier noch nicht überschritten worden war. Allerdings stellte das Gericht gleichzeitig klar, dass die EMRK auch Grenzen setzt:

> *„Gleichwohl unterstreicht der Gerichtshof, dass dies nicht bedeutet, die Vertragsstaaten hätten ein unbegrenztes Ermessen (latitude illimitée / unlimited discretion), Personen innerhalb ihres Hoheitsbereichs geheimer Überwachung zu unterwerfen. Im Bewusstsein der Gefahr, die ein solches Gesetz in sich birgt, nämlich die Demokratie mit der Begründung, sie zu verteidigen, zu untergraben oder sogar zu zerstören, bekräftigt der Gerichtshof, dass die Vertragsstaaten nicht im Namen des Kampfes gegen Spionage und Terrorismus zu jedweder Maßnahme greifen dürfen, die ihnen geeignet erscheint“ (Randnummer 49 der Urteilsbegründung).*

Der EGMR konnte sich in seiner Frühphase (er hatte im Herbst 1960 seine Spruchtätigkeit aufgenommen, die Beschwerde zu Fall 1 wurde im Jahr 1971 eingelegt) offenbar nicht dazu durchringen, der Beschwerde stattzugeben. Gleichwohl ist die Entscheidung bedeutend. Sie erstreckt den Grundrechtsschutz des Art. 8 EMRK auf die Vertraulichkeit des Post-, Brief- und Telekommunikationsverkehrs. Zugleich deutet das Urteil spätere Rechtsprechung bereits an, wonach die EMRK nur dann eine staatliche Überwachung erlaubt, wenn sie für einen legitimen Zweck erforderlich ist (siehe dazu beispielsweise Fall 3!).

Fall 2: Leander gegen Schweden (Urteil vom 26.03.1987)

Herr Leander, ein schwedischer Bürger, beschwerte sich beim EGMR darüber, dass er unter anderem in seinem Grundrecht aus Art. 8 EMRK verletzt worden sei. Im Rahmen seines Anstellungsverfahrens beim staatlichen schwedischen Marinemuseum habe eine Personalüberprüfung stattgefunden. Dabei sei ihm wegen bestimmter unveröffentlichter Daten aus einem geheimen Polizeiregister eine unbefristete Anstellung verwehrt worden.

Auch wenn die Beschwerde im Ergebnis erfolglos blieb, ist die Entscheidung des EGMR datenschutzrechtlich bedeutsam. Denn der EGMR stellte fest, dass sowohl die Speicherung von Daten über Herrn Leander im Polizeiregister als auch die weitere Verwendung dieser Daten im Verfahren der Personalüberprüfung Eingriffe in das Recht auf Achtung des Privatlebens seien. Außerdem wies das Gericht darauf hin, dass eine Regelung, die wie die Verordnung über Personalüberprüfungen auf alle Bürger Anwendung findet, klare gesetzliche Grundlagen erfordert. Die gesetzliche Vorschrift muss also genügend Angaben darüber machen, in welchen Fällen und unter welchen Voraussetzungen die öffentliche Gewalt berechtigt ist, einen solchen geheimen und potentiell gefährlichen Eingriff in das Privatleben vorzunehmen. In Weiterentwicklung dieser Rechtsprechung zur Verwendung geheimdienstlicher Daten stellte

der EGMR beispielsweise im **Fall Rotaru gegen Rumänien** (Urteil vom 04.05.2000) einen Verstoß gegen Art. 8 EMRK fest, weil die näheren Eingriffsvoraussetzungen in der gesetzlichen Grundlage nicht klar genug festgelegt waren.

Fall 3: S. und Michael Marper gegen Vereinigtes Königreich (Urteil vom 04.12.2008)
Gegenstand der Beschwerde der beiden Beschwerdeführer war die Speicherung von DNA-Proben und Fingerabdrücken durch die britische Polizei. Die Beschwerdeführer waren wegen des Verdachts von Straftaten festgenommen worden. In beiden Fällen erhärtete sich der Straftat nicht. Gleichwohl lehnte die Polizei es ab, die DNA-Daten und die Fingerabdruckdaten in den polizeilichen Datenbanken zu löschen. Die Klage der Beschwerdeführer vor britischen Gerichten blieb erfolglos, weil die Urteile sinngemäß darauf verwiesen, die Erfassung von Fingerabdrücken und DNA-Proben seien auch ohne entsprechenden Tatverdacht zulässig.
Und in der Tat konnte die Speicherung auf eine eindeutige gesetzliche Grundlage gestützt werden (Unterschied zum Fall Rotaru, siehe Fall 2 am Ende!). § 64 Police and Criminal Evidence Act 1984 sah vor, dass im Zusammenhang mit der Untersuchung von Straftaten genommene Fingerabdrücke oder Proben aufbewahrt werden dürfen, nachdem sie den Zweck erfüllt haben, zu dem sie genommen wurden. Die Speicherung der Fingerabdrücke hatte damit eine eindeutige Grundlage im innerstaatlichen Recht.
Trotzdem sah der EGMR die Speicherung als Verletzung des Art. 8 EMRK an. Er erkannte zwar an, dass die Erfassung der Fingerabdrücke und der DNA-Daten einem legitimen Zweck diente, nämlich der effektiven Kriminalitätsbekämpfung. Die umfassende und wahllose Befugnis zur Speicherung von Fingerabdrücken, Zellproben und DNA-Profilen von verdächtigten, aber nicht verurteilten Personen traf aber keinen gerechten Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen. Das Vereinigte Königreich hatte deshalb in dieser Hinsicht „jeden akzeptablen Ermessensspielraum“ überschritten. Die umstrittene Speicherung begründete somit einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens, der nicht als notwendig in einer demokratischen Gesellschaft angesehen werden konnte.

- ⇨ Kühling/Seidel/Sivridis, S. 6-13
- ⇨ Tinnefeld/Buchner/Petri, S. 72-76

4.2 Charta der Grundrechte der Europäischen Union

Seit den Römischen Verträgen des Jahres 1957 hat die EU gewaltige Integrationsschritte unternommen. Der vorerst letzte bedeutende Wegabschnitt dieser Integration ist der Vertrag von Lissabon, der am 1. Dezember 2009 in Kraft getreten ist. Aus grundrechtlicher Sicht ist für die Fortentwicklung des Europäischen Datenschutzrechtsrahmens vor Allem Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (Grundrechte-Charta - GRCh) wichtig. Sie lauten wie folgt:

> *Art. 7 GRCh*
> *Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.*
>
> *Art. 8 GRC Schutz personenbezogener Daten*
> *(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*
> *(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.*
> *(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.*

Die Ähnlichkeit des Art. 7 GRCh zu Art. 8 EMRK ist nicht zufällig. In der Zeit vor dem Inkrafttreten des Vertrags von Lissabon wurde der Grundrechtsschutz in der EU durch die EMRK sowie die Menschenrechte und Grundfreiheiten gewährleistet, „wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben." Auch heute noch nimmt der EU-Vertrag hierauf Bezug (in Art. 6 Abs. 3 EUV).

Obwohl Art. 7 und 8 GRCh erst mit Inkrafttreten des Vertrags von Lissabon verbindliches EU-Primärvertragsrecht sind, gibt es hierzu bereits zwei wichtige Entscheidung des Europäischen Gerichtshofs (EuGH):

Fall 1: Veröffentlichung der Empfänger von EU-Agrarsubventionen (EuGH, Urteil vom 09.11.2010 – Rechtssache C-92/09 und C-93/09)

Eine EU-Verordnung (VO Nr. 259/2008/EG) verpflichtete die Mitgliedstaaten der EU, Empfänger von EU-Agrarsubventionen „allgemein zu veröffentlichen". Zu publizieren waren die

jeweiligen Empfänger aus zwei bestimmten Landwirtschaftlichen EU-Fonds und die empfangenen Beträge (in Deutschland wurden diese Informationen auf der Internetseite der Bundesanstalt für Landwirtschaft und Ernährung veröffentlicht). In dem Ausgangsverfahren klagten zwei Landwirte gegen das Land Hessen, um die Veröffentlichung ihrer personenbezogenen Daten zu unterbinden, die die Kläger als Empfänger von Mitteln aus zwei Landwirtschaftlichen Fonds betrafen. Das angerufene Verwaltungsgericht teilte die Zweifel der Kläger und legte dem Europäischen Gerichtshof (EuGH) den Fall zur Vorabentscheidung vor. Der EuGH stellte zunächst fest, dass die in den Art. 7 und 8 GRCh anerkannte Achtung des Privatlebens sich hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft. Dementsprechend greift die Veröffentlichung der Daten in das Grundrecht auf Achtung des Privatlebens aus Art. 7 GRCh ein und stellt eine Datenverarbeitung im Sinne des Art. 8 Abs. 2 GRCh dar. Der EuGH stellte weiterhin fest, dass die Veröffentlichung auf einer gesetzlichen Grundlage beruhe. Auch diene sie einem legitimen Ziel, nämlich die Transparenz in Bezug auf die Verwendung der Gemeinschaftsmittel und durch eine stärkere öffentliche Kontrolle der verwendeten Mittel, die Wirtschaftlichkeit der Haushaltsführung bei diesen Fonds zu verbessern. Die Einschränkung der in den Art. 7 und 8 der Charta verankerten Rechte stehe aber nicht in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck. Denn die verschiedenen beteiligten Interessen seien im Rahmen der Interessenabwägung nicht erkennbar ausgewogen gewichtet worden. Insbesondere sei nicht geprüft worden, ob mildere Eingriffe ähnlich geeignet wären. In Betracht käme etwa die Beschränkung der Veröffentlichung von Daten unter namentlicher Nennung der Empfänger. So hätte der EU-Gesetzgeber prüfen müssen, ob man hinsichtlich der Empfänger von geringfügigen Subventionen auf die namentliche Nennung verzichten könnte. Die Kommission hat dem Europäischen Parlament und dem Rat der Europäischen Union einen Vorschlag gemacht, wie die Entscheidung des EuGH umgesetzt werden kann (Entwurf einer Änderungsverordnung - COM(2012)551; dazu Bayerischer Landesbeauftragter für den Datenschutz, 25. Tätigkeitsbericht 2012, Nr. 12.11, abrufbar unter www.datenschutz-bayern.de unter Tätigkeitsberichte).

Fall 2: Vorratsspeicherung von Telekommunikationsverkehrsdaten (EuGH, Urteil vom 08.04.2014 – verbundene Rechtssache C-293/12, C-594/12)

Eine lange Vorgeschichte hat der Streit über die sogenannte Vorratsdatenspeicherung, über den der EuGH im April 2014 entschieden hat. Eine EG-Richtlinie (2006/24/EG) verpflichtete

die Mitgliedstaaten, eine verbindliche **Vorratsspeicherung von Telekommunikationsverkehrsdaten** einzuführen. Das Bundesverfassungsgericht hatte in einer Entscheidung vom 02.03.2010 noch die sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter nicht schlechthin mit dem Fernmeldegeheimnis aus Art. 10 GG unvereinbar angesehen. Lediglich das deutsche Gesetz zur Umsetzung der Richtlinie 2006/24/EG genügte nicht den Anforderungen des Art. 10 Abs. 1 GG. Demgegenüber legten der High Court of Ireland und der Österreichische die Frage der Grundrechtskonformität dieser Richtlinie dem EuGH zur Vorabentscheidung vorgelegt.

In einer vielbeachteten Entscheidung hat der EuGH nun die EG-Richtlinie für ungültig erklärt abrufbar unter www.curia.europa.eu). In seinen wesentlichen Erwägungen ist der EuGH dabei den Feststellungen des EGMR im vorgestellten Fall Marper gegen Vereinigtes Königreich (siehe Abschnitt 4.1, Fall 3) gefolgt.
Der Europäische Gerichtshof erkennt zunächst an, dass die Bekämpfung schwerer Straftaten ein legitimes Regelungsziel sein kann. Die Vorratsspeicherung von Telekommunikationsverkehrsdaten ist auch ein „nützliches Mittel“, das zur Aufklärung schwerer Straftaten geeignet sein kann. Zugleich weist der Gerichtshof jedoch darauf hin, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Ein solcher Eingriff in die von Art. 7 und Art. 8 der Europäischen Grundrechte-Charta garantierten Rechte ist nur gerechtfertigt, soweit er auf das absolut notwendige Maß beschränkt bleibt. Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Insbesondere schrieb sie die Speicherung von Verkehrsdaten fast der gesamten europäischen Bevölkerung vor. Auch solche Personen mussten erfasst werden, deren Verhalten nicht einmal in einem mittelbaren oder entfernten Zusammenhang zu schweren Straftaten steht oder die einem Berufsgeheimnis unterliegen. Auch musste kein Zusammenhang zwischen den auf Vorrat gespeicherten Daten und einer Bedrohung der öffentlichen Sicherheit bestehen.

Welche Folgen sich aus der vorliegenden Entscheidung ergeben, ist gegenwärtig noch unklar. Ein neuer Rechtsakt ist zwar nicht völlig ausgeschlossen, müsste aber vor allem einen inhaltlichen Zusammenhang zwischen Vorratsdatenspeicherung und schweren Straftaten herstellen. Eine flächendeckende, undifferenziert angeordnete Vorratsspeicherung von Telekommunikationsverkehrsdaten ist jedenfalls im Lichte der Europäischen Grundrechte nicht zulässig. Ob

hierdurch die effektive Bekämpfung von schweren Straftaten leidet, ist unklar: Zwar haben Verteidiger der Richtlinie 2006/24/EG immer wieder plakative Einzelfälle zum Anlass genommen, um die Notwendigkeit der Vorratsspeicherung hervorzuheben. Es fehlt jedoch nach wie vor der konkrete Nachweis, dass sich die Sicherheitslage ohne Vorratsdatenspeicherung wesentlich verschlechtert. Auch in der mündlichen Verhandlung vor dem EuGH wurde die Notwendigkeit einer flächendeckenden Vorratsspeicherung von Telekommunikationsverkehrsdaten nicht belegt.

- ⇨ Hielke Hijmans / Owe Langfeldt in BPB, S, 403 ff.
- ⇨ Kühling/Seidel/Sivridis, S. 13-22.
- ⇨ Tinnefeld/Buchner/Petri, S. 76-87.

4.3 Datenschutz und deutscher Grundrechtsschutz

Ein Grundrecht auf Datenschutzrecht ist im deutschen Grundgesetz (GG) nicht ausdrücklich vorgesehen. Trotzdem ist der Datenschutz grundrechtlich verankert. Zunächst gibt es einige Grundrechte, die spezielle Fragen des Datenschutzes betreffen. Dazu zählen das Brief-, Post- und Fernmeldegeheimnis aus Art. 10 GG und die Garantie der Unverletzlichkeit der Wohnung in Art. 13 GG (die zitierten Grundrechtsartikel bitte lesen!).
Üblicherweise wird der grundrechtliche Datenschutz aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitet (lesen - zur geschichtlichen Entwicklung siehe bereits Abschnitt 3).

Auch heute noch herausragende Bedeutung für den Datenschutz hat das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983.

Fall 1: Volkszählungsgesetz 1983 (Urteil vom 15.12.1983, BVerfGE 65, S. 1 ff.)
Das Bundesverfassungsgericht hatte in diesem Fall das „Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983)“ vom 25.03.1982 (Bundesgesetzblatt I S. 369) zu beurteilen. Volkszählungen werden durchgeführt, um die Grundlage für politische Planungsentscheidungen vorzubereiten. Die Volkszählung 1983 war allerdings besonders gelagert, weil sie zum ersten Mal in Deutschland mithilfe der automatisierten Datenverarbeitung durchgeführt wurde. Viele Proteste entzündeten sich vor allem an dem Umstand, dass die erhobenen Daten dem Volkszählungsgesetz zufolge nicht nur für statistische Zwecke verwendet werden sollten. Vielmehr sollten sie auch dazu verwendet werden, um die Melderegister auf ihre Richtigkeit und Vollständigkeit zu überprüfen.

Wegen dieser Möglichkeit der personenbezogenen Datenverarbeitung wandten sich über zweitausend Beschwerdeführer an das Bundesverfassungsgericht – mit Erfolg. Das Bundesverfassungsgericht erklärte einige Regelungen für verfassungswidrig. Vor Allem aber leitete das Gericht aus dem allgemeinen Persönlichkeitsrecht ein **Recht auf informationelle Selbstbestimmung** ab. Hier die drei ersten Leitsätze des Urteils, welche die Reichweite des neuen Grundrechts beschreiben:

1. *Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art 2 Abs 1 GG in Verbindung mit Art 1 Abs 1 GG umfasst. Das Grund-*

recht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. *Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.*
3. *Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind.*
   Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und Informationsverarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen.

Das Volkszählungsurteil ist bedeutend, weil es die Vorgaben des allgemeinen Persönlichkeitsrechts an die modernen Bedingungen der automatisierten Datenverarbeitung angepasst hat (siehe Leitsatz 1). Über die Leitsätze hinaus hat das Gericht in der Urteilsbegründung hervorgehoben, dass es unter den Bedingungen der automatisierten Datenverarbeitung **keine belanglosen Daten** mehr gibt. Um die Auswirkungen einer Datenverarbeitung für das Persönlichkeitsrecht beurteilen zu können, muss vielmehr der konkrete **Verwendungszusammenhang** bekannt sein.

Beispiel: Der Name eines bekannten Politikers ist ein scheinbar wenig sensibles Datum. Wird er jedoch in Verbindung mit dem Vorwurf der Korruption gebracht, hat das Datum für den Betroffenen eine Existenz bedrohende Bedeutung.

In anderen Entscheidungen hat das Bundesverfassungsgericht klargestellt, dass die Erhebung und Verwendung von Daten, die dem **Kernbereich der privaten Lebensgestaltung** zuzuordnen sind, strikt verboten ist. Der Schutz dieser Daten leitet sich letztlich aus der Menschenwürde aus Art. 1 Abs. 1 GG ab. Die Würde des Menschen ist jedoch unantastbar – sie darf nicht beeinträchtigt werden.

Beispiel: Selbst zur Aufklärung eines Mordfalls dürfen Strafverfolgungsbehörden nicht ein vertrauliches Beichtgespräch des mutmaßlichen Täters mit einem Seelsorger abhören.

Sieht man von diesen absolut geschützten Daten ab, können Eingriffe in das Recht auf informationelle Selbstbestimmung gerechtfertigt sein. Denn personenbezogene Daten „gehören“ nicht nur dem betroffenen Menschen. Jeder Mensch ist Teil einer miteinander kommunizierenden Gemeinschaft. Dementsprechend sind Einschränkungen des Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse verfassungsrechtlich durchaus möglich. Dazu müssen sie allerdings zunächst auf einer **hinreichend bestimmten gesetzlichen Grundlage** beruhen. Das bedeutet in erster Linie, dass der Gesetzgeber den Verwendungszweck der zu erhebenden Daten bestimmt und klar festlegt. Die Verwaltung ist an die gesetzlich festgelegten Zwecke gebunden. Dieses **Zweckbindungsprinzip** ist eines der zentralen Prinzipien auch des einfachgesetzlichen Datenschutzrechts. Für Verwendungsbereiche mit besonderer Grundrechtsrelevanz sind bereichsspezifische Regelungen erforderlich.

> Beispiel: Für die polizeiliche Datenverarbeitung haben die Polizeigesetze Regelungen vorzusehen, welche die polizeilichen Besonderheiten berücksichtigen.

> Beispiel: Das Sozialgesetzbuch enthält eine abgeschlossene Regelung des Datenschutzes für den Bereich der staatlichen sozialen Leistungen.

Das Zweckbindungsprinzip soll sicherstellen, dass der Einzelne zumindest grundsätzlich überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind. Er soll abschätzen können, was ein Kommunikationspartner über ihn weiß. Danach dürfen Daten im Grundsatz nur zu dem gleichen Zweck verwendet und insbesondere weitergegeben werden, zu dem sie erhoben worden sind. Nachträgliche Zweckänderungen sind zwar möglich, erfordern aber ihrerseits eine verfassungsgemäße Rechtsgrundlage (ob der erwünschte Überblick aufgrund der Vielzahl von gesetzlich erlaubten Zweckänderungen noch realistisch ist, ist eine andere Frage).

Die Festlegung des Verwendungszweckes ist auch notwendig, um die **Verhältnismäßigkeit** eines informationellen Grundrechtseingriffs beurteilen zu können. Das Bundesverfassungsgericht hat beispielsweise verschiedentlich deutlich gemacht, dass der Staat die „*technischen Veränderungen – schon um seiner grundrechtlichen Pflicht zum Schutz von Leib, Leben oder Freiheit seiner Bürgerinnen und Bürger aus Artikel 2 Abs. 2 GG zu genügen – bei der Gefahrenbekämpfung und Verfolgung von Straftaten nicht unberücksichtigt lassen (kann). Gleich-*

wohl dürfen bei der Ausbalancierung von Freiheit und Sicherheit die Gewichte nicht grundlegend verschoben werden." (Urteil vom 04.04.2006, BVerfGE 115, S. 320 ff. Mit dieser Entscheidung wurde eine großangelegte präventiv-polizeiliche Rasterfahndung aus den Jahren 2001/2002 für verfassungswidrig erklärt).

Der Grundsatz der **Verhältnismäßigkeit** besagt, dass eine hoheitliche Maßnahme einen *legitimen Zweck* verfolgen muss.[7] Sie muss dabei *geeignet* und *erforderlich* sein, um das Ziel zu erreichen.

> Beispiel 1: Videoüberwachung kann unter bestimmten Voraussetzungen die Aufklärung von Straftaten erleichtern. Sofern die Voraussetzungen vorliegen, ist sie zu diesem Zweck *geeignet*.
>
> Beispiel 2: Die Polizei hat mithilfe einer Videoüberwachung einen Straftäter ermittelt. Andere Ermittlungsansätze gab es nicht. Die Videoaufzeichnung war zur Ermittlung des Straftäters *erforderlich*, weil es keine milderen Mittel zur Zweckerreichung gab.
>
> Beispiel 3: Der Straftäter in Beispiel 2 ist rechtskräftig verurteilt worden und sitzt seine Strafe ab. Jetzt ist die Aufzeichnung nicht mehr erforderlich, weil sie ihren Zweck schon erreicht hat.

Um verhältnismäßig zu sein, muss die Maßnahme angemessen sein: Die mit ihr verbundene Belastung des Betroffenen darf nicht außer Verhältnis zu dem angestrebten Ziel stehen.

> Beispiel: Die Polizei filmt eine friedliche Versammlung, obwohl es keine Anhaltspunkte für eine Gefahr der öffentlichen Sicherheit gibt. Das Filmmaterial wird nur vorsorglich gespeichert, um etwaige Rechtsverstöße von einzelnen Versammlungsteilnehmern nachträglich nachvollziehbar zu machen. Derartige Übersichtsaufzeichnungen auf Vorrat greifen unverhältnismäßig in das Grundrecht auf Versammlungsfreiheit aus Art. 8 GG ein und sind damit verfassungswidrig (nachgebildet: BVerfG, Beschluss vom 17.02.2009, BVerfGE 122, 342 – „Bayerisches Versammlungsgesetz").

[7] Beachte: Die Verhältnismäßigkeit eines Gesetzes ist gegeben, wenn das Gesetz a) einen legitimen Zweck verfolgt, und b) hierzu geeignet, erforderlich und angemessen ist. Bei der Verhältnismäßigkeit einer Maßnahme zum Gesetzesvollzug (z.B. Verwaltungshandeln) ist der „legitime Zweck" gleichbedeutend mit dem Gesetzeszweck. Die Geeignetheit, Erforderlichkeit und Angemessenheit ist also auf den Zweck der gesetzlichen Befugnis zu beziehen, auf die sich die Maßnahme stützt.

Mit anderen Worten kommt es bei der Verhältnismäßigkeitsprüfung auf eine **Abwägung der widerstreitenden Rechtsgüter** (Datenschutz des Einzelnen gegen Allgemeininteresse) an.

Achtung: Greift eine Maßnahme in ein Grundrecht ein, ohne dass es hierzu eine gesetzliche Grundlage gibt, ist die Maßnahme schon deshalb rechtswidrig. Dieser **grundrechtliche Gesetzesvorbehalt** ist eine besondere Ausprägung der Gesetzmäßigkeit der Verwaltung und zählt zu den zentralen Prinzipien unseres Rechtsstaates (Art. 20 Abs. 3 GG lesen). Die Prüfung des Verhältnismäßigkeitsgrundsatzes erübrigt sich in einem solchen Fall.

> Beispiel: Die Strafprozessordnung sieht die Befugnis zur sogenannten Online-Durchsuchung nicht vor (zur Online-Durchsuchung siehe Fall 4 unten) Selbst wenn die Strafverfolgungsbehörden einen Mord aufklären wollen, dürfen sie hierzu eine Online-Durchsuchung nicht einsetzen.

Ob der Verhältnismäßigkeitsgrundsatz beachtet worden ist, ist oft eine **Bewertungsfrage**. Das verdeutlicht auch der nachfolgende Fall, bei dem es um eine Beeinträchtigung des Fernmeldegeheimnisses aus Artikel 10 GG geht:

Fall 2: Vorratsspeicherung von Telekommunikationsverkehrsdaten (Urteil vom 02.03.2010, BVerfGE 125, S. 260 ff.)

Oben wurde bereits die Richtlinie 2006/24/EG erwähnt (siehe Ende des Abschnitts 4.2). Auch der deutsche Gesetzgeber hat versucht, diese Richtlinie durch neue Vorschriften im Telekommunikationsgesetz (TKG) und in der Strafprozessordnung (StPO) umzusetzen.

Auf eine Vielzahl von Verfassungsbeschwerden hin erklärte das Bundesverfassungsgericht diese Vorschriften für nichtig, weil sie gegen das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG verstießen. Das Bundesverfassungsgericht hielt zwar eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Dienstleister nicht schlechthin mit Art. 10 GG unvereinbar. Denn die Strafverfolgung, die Gefahrenabwehr und die Aufgaben der Nachrichtendienste seien legitime Zwecke. Unter dem Gesichtspunkt der Verhältnismäßigkeit sei jedoch zu beachten, dass eine solche Speicherung „*einen besonders schweren Eingriff mit einer Streubreite (ist), wie sie die Rechtsordnung bisher nicht kennt: Erfasst werden über den gesamten Zeitraum von sechs Monaten praktisch sämtliche Telekommunikationsverkehrsdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfba-*

res Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation.“

Trotzdem hielt das Gericht eine solche vorsorglich anlasslose Speicherung der Telekommunikationsverbindungsdaten (das sind Daten zum Zeitpunkt, zur Dauer, zu beteiligten Anschlüsse sowie bei Mobiltelefonen zum jeweiligen Standort) unter engen verfassungsrechtlichen Voraussetzungen gerade noch für möglich. Es hielt allerdings den folgenden Hinweis für notwendig: „*Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (Nachweis), für deren Wahrung sich die Bundesrepublik Deutschland in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.“*

Die Verfassungsgerichte einiger anderer EU-Mitgliedstaaten kamen zu einer anderen Einschätzung. Sie hielten die Vorratsdatenspeicherung für einen Verstoß gegen Art. 8 EMRK. Diese Vorschrift gewähre den Schutz der vertraulichen Korrespondenz. Dieser Schutz könne zwar ausnahmsweise unter gesetzlich näher beschriebenen Voraussetzungen eingeschränkt werden. Die Anordnung der Vorratsdatenspeicherung durch die Richtlinie 2006/24/EG verkehre jedoch dieses Regel-Ausnahme-Verhältnis in ihr Gegenteil. Wie dargestellt, hat der EuGH eine Vorratsdatenspeicherung nicht schlechthin für grundrechtswidrig gehalten, verlangt aber eine am Maßstab der unbedingten Notwendigkeit differenzierte Regelung und insbesondere einen Zusammenhang zwischen den zu speichernden Daten und der Bekämpfung schwerer Straftaten.

Je unterschiedlicher die Verwendungszwecke sind, umso problematischer kann die zweckändernde Datenverwendung sein. Hierauf hat das Bundesverfassungsgericht in einer Entscheidung vom 24.04.2013 hingewiesen:

Fall 3: Antiterrordateigesetz (Urteil vom 24.04.2013)

Gegenstand dieses Urteils ist das Antiterrordateigesetz (ATDG). Es regelt die Errichtung einer Antiterrordatei als Verbunddatei verschiedener Sicherheitsbehörden zur Bekämpfung des internationalen Terrorismus. Den Zugriff auf die Antiterrordatei erhalten Nachrichtendienste und Polizeibehörden. Beide Behördenarten müssen auch bestimmte Personen und Personen-

daten in die Antiterrordatei einspeichern. Verfassungsrechtlich problematisch ist dabei der Umstand, dass diese beiden Kategorien von Sicherheitsbehörden höchst unterschiedliche Sicherheitsaufgaben erfüllen und deshalb auch unterschiedliche Befugnisse haben. Nachrichtendienste haben die Funktion einer strategischen Aufklärung terroristischer Bestrebungen weit im Vorfeld einer konkreten Gefahr. Sie unterliegen nicht dem Grundsatz, dass Daten offen zu erheben sind. Im Gegenzug haben sie keinerlei Zwangsbefugnisse, sie dürfen solche Befugnisse auch nicht im Wege der Amtshilfe bei der Polizei einfordern. Demgegenüber haben die Polizeibehörden eine operative Verantwortung – sie müssen konkrete Gefahren für die öffentliche Sicherheit notfalls auch mithilfe von Zwangsmaßnahmen abwehren. Ihre Datenverarbeitungsbefugnisse sind ihrem Aufgabenprofil entsprechend strenger gefasst. Die Polizeibehörden haben den Grundsatz der offenen Datenerhebung zu beachten. Zwar setzt die Aufgabenwahrnehmung der Polizei in erheblichem Umfang auch verdeckte Ermittlungen voraus. Dies stellt aber das Prinzip des „offenen Visiers“ der Polizei nicht infrage. So sind die betroffenen Personen grundsätzlich zu informieren, sobald die Geheimhaltungsgründe einer verdeckten Maßnahme entfallen.

Vor diesem Hintergrund hat das Bundesverfassungsgericht folgende Feststellung getroffen:

> „*Für die Beurteilung der Verhältnismäßigkeit eines Informationsaustauschs zwischen verschiedenen Behörden kommt es insbesondere auf die Vergleichbarkeit der verschiedenen Informationszusammenhänge an. Je verschiedenartiger Aufgaben, Befugnisse und Art der Aufgabenwahrnehmung sind, desto größeres Gewicht hat der Austausch entsprechender Daten. (Absatz 114 der Urteilsbegründung)*
>
> *…*
>
> *Regelungen, die dem Austausch von Daten der Polizeibehörden und Nachrichtendiensten ermöglichen, unterliegen angesichts dieser Unterschiede gesteigerten verfassungsrechtlichen Anforderungen. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt insoweit ein* ***informationelles Trennungsprinzip****. Danach dürfen Daten zwischen Nachrichtendiensten und Polizeibehörden grundsätzlich nicht ausgetauscht werden.“ (Absatz 123 der Urteilsbegründung)*

Angesichts der großen Bedeutung der Terrorismusbekämpfung hat das Bundesverfassungsgericht allerdings für das ATDG eine Durchbrechung dieses Grundsatzes zugelassen und vom Gesetzgeber lediglich Korrekturen hinsichtlich des Umfangs der Antiterrordatei sowie verfahrensrechtliche Schutzvorkehrungen eingefordert.

Damit der Betroffene sein Grundrecht auf informationelle Selbstbestimmung wahren kann, müssen zudem **verfahrensrechtliche Schutzvorkehrungen** geschaffen werden. Dazu zählen Transparenzrechte (z.B. Informations- und Auskunftsrechte) und Gestaltungsrechte (z.B. Berichtigungs- und Löschungsansprüche). Im Interesse eines vorgezogenen Rechtsschutzes ist auch die Kontrolle durch unabhängige Datenschutzbeauftragte bedeutsam.

Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG gewinnt im Verhältnis zu den speziellen Freiheitsrechten z.B. aus Art. 10 und 13 GG an Bedeutung, wo moderne Entwicklungen neue Gefährdungen für die menschliche Persönlichkeit erzeugen können. So hat das Bundesverfassungsgericht im Jahr 2008 aus dem allgemeinen Persönlichkeitsrecht auch ein „**Grundrecht auf Gewährleistungen der Vertraulichkeit und Integrität informationstechnischer Systeme**“ abgeleitet. Häufig wird dieser komplizierte Namen meist durch die etwas unpräzise Kurzform „IT-Grundrecht“ ersetzt. Die neue grundrechtliche Gewährleistung ist notwendig, weil die Nutzung der modernen Informationstechnologie schnell zugenommen hat. Zugleich kann der Nutzer wegen der technischen Komplexität oft nicht mehr selbst die Vertraulichkeit und Integrität seiner IT-Systeme (z.B. sein Smartphone) sicherstellen. Das Recht auf informationelle Selbstbestimmung und auch andere Persönlichkeitsrechte laufen leer, weil sie nur die Daten und ihre Kommunikation, nicht aber das IT-System schützen. Das IT-Grundrecht schließt diese Schutzlücke. Es sichert den persönlichen Bereich auch dann, wenn auf das IT-System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.

Fall 4: Online-Durchsuchung (Urteil vom 27.02.2008 – BVerfGE 120, S. 274 ff.)
Einige Polizeigesetze und einige Verfassungsschutzgesetze sehen die Befugnis zur sogenannten **Online-Durchsuchung** vor. Bei dieser Maßnahme infiltriert die Sicherheitsbehörde das von ihr angegriffene IT-System heimlich mit Hilfe eines Spähprogramms („Staatstrojaner“), um an die auf dem IT-System gespeicherten Daten zu gelangen. Eine derartige Online-Durchsuchung ist ein schwerwiegender Eingriff in das IT-Grundrecht. Die Integrität des IT-System ist verletzt und in aller Regel erkennen die Betroffenen diese verdeckte Manipulation nicht. Zugleich kann die Ermittlungsbehörde mit einem Schlag Zugriff auf einen Datenbestand erhalten, der ein aussagekräftiges Persönlichkeitsbild über den betroffenen Nutzer zeichnet. Da heute viele Nutzer mithilfe ihrer IT-Systeme auch telefonieren und E-Mails austauschen können, kann eine solche Infiltration auch die Überwachung von Telekommunikation ermöglichen. Angesichts der äußerst hohen Eingriffsintensität ist eine Online-

Durchsuchung nur unter strengen Voraussetzungen verfassungskonform. Es müssen tatsächliche Anhaltspunkte für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut wie Leib, Leben oder Freiheit der Person vorliegen. Die Maßnahme darf grundsätzlich nur auf richterliche Anordnung hin erfolgen.
Die Strafprozessordnung sieht übrigens bislang keine Online-Durchsuchung vor. Da ein Grundrechtseingriff stets nur auf gesetzliche Grundlage erlaubt sein kann, ist eine Online-Durchsuchung zur Strafverfolgung in Deutschland nicht gestattet.

Bislang sind die Gefahren für den grundrechtlichen Datenschutz beschrieben worden, die von Behörden ausgehen. Damit angesprochen war die Funktion der **Grundrechte als Abwehrrechte** gegenüber dem Staat (bitte Art. 1 Abs. 3 GG lesen!). Zunehmend gehen jedoch viele Gefährdungen des Persönlichkeitsrechts von **privaten Unternehmen** aus.

> Beispiel: Ein Arbeitgeber installiert heimlich Videokameras, mit denen er seine Beschäftigten überwacht.

> Beispiel: Kreditinstitute und Versicherungen machen den Abschluss von Verträgen mit Verbrauchern oft von umfangreichen Datenerhebungen abhängig.

Wenn das Bundesverfassungsgericht in seinem Volkszählungsurteil festhält: „*Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer, was wann und bei welcher Gelegenheit über einen weiß“*, dann gilt dieser Hinweis auch für den Umgang privater Unternehmen mit personenbezogenen Daten.
Das allgemeine Persönlichkeitsrecht fordert hier vom Staat, dass er auch insoweit die Bürgerinnen und Bürger schützt. Bei der Ausübung dieser **grundrechtlichen Schutzpflicht** muss er dabei einen angemessenen Ausgleich zwischen den konkurrierenden Freiheitsrechten auf Datenschutz einerseits und wirtschaftliche Betätigungsfreiheit andererseits schaffen. Dies geschieht durch einfachgesetzliche Regelungen (z.B. die Datenschutzgesetze). Als Mindestanforderungen sind dabei insbesondere eine angemessene Zweckbindung der Datenverarbeitung, die Sicherheit der Daten und die Transparenz des Datenumgangs sicherzustellen.
Die Inhalte der widerstreitenden Grundrechte sind dann im Rahmen der Auslegung des einfachen Gesetzesrechts zu berücksichtigen (**mittelbare Drittwirkung von Grundrechten**).

Schwierig zu beurteilen sind oft Fälle, bei denen Kommunikationsgrundrechte aus Art. 5 GG zu einer Beeinträchtigung des Persönlichkeitsrechts führen.

> Beispiel 1: Ein Fernsehsender strahlt eine Fernsehdokumentation zur besten Sendezeit aus, die einen konkreten, einige Jahre zurückliegenden Mordfall beleuchtet. Dabei werden die Person des Straftäters und sein Privatleben ausgeleuchtet.
>
> Beispiel 2: Ein Zeitungsverlag unterhält auf seinem Internetportal ein Onlinearchiv seiner alten Zeitungsberichte. Dieses Archiv enthält unter anderen alte Berichte über einen namentlich benannten, verurteilten Straftäter, der mittlerweile aus der Haft entlassen wurde. Er sieht sich durch die alten Berichte sein Persönlichkeitsrecht verletzt.

Das Beispiel 1 betrifft den sogenannten „Lebach-Fall“. Der betroffene Straftäter hatte vergeblich versucht, bei den Fachgerichten Rechtsschutz gegen die Ausstrahlung eines Fernsehfilms zu erlangen. Auf seine Verfassungsbeschwerde hin gab das Bundesverfassungsgericht ihm Recht: Zwar könne sich die Fernsehanstalt auf die Rundfunkfreiheit aus Art. 5 Abs. 1 GG stützen. Die beabsichtigte Sendung beeinträchtige jedoch den Straftäter in seinem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG. Die hier einschlägigen Vorschriften der §§ 22, 23 Kunsturhebergesetz könnten und müssten so ausgelegt werden, dass **einzelfallbezogen die Intensität des Eingriffes in den Persönlichkeitsbereich gegen das Informationsinteresse der Öffentlichkeit abzuwägen** sei. Hierbei habe keiner der beiden Verfassungswerte von vorneherein einen Vorrang zu beanspruchen. Zwar verdiene das Informationsinteresse der Öffentlichkeit im allgemeinen Vorrang vor dem Persönlichkeitsschutz des Straftäters gehe, soweit aktuell über eine schwere Straftat als solche berichtet werde. Jedoch sei auf den unantastbaren innersten Lebensbereich und auf den Grundsatz der Verhältnismäßigkeit zu achten. Dementsprechend lasse es der verfassungsrechtliche Schutz der Persönlichkeit nicht zu, dass das Fernsehen sich über die aktuelle Berichterstattung hinaus etwa in Form eines Dokumentarspiels zeitlich unbeschränkt mit der Person des Straftäters und seiner Privatsphäre befasse. Die Verfassungsbeschwerde war unter anderem deshalb erfolgreich, weil die nachträgliche Berichterstattung dem Betroffenen nach Verbüßung nach seiner Strafe die Chance erschwert hätte, sich wieder in die Gesellschaft zu integrieren [Bundesverfassungsgericht, Urteil vom 5.6.1973 – BVerfGE 35, S. 202 ff.].

Beispiel 2 ist einem Fall nachgebildet, den der Bundesgerichtshof (BGH) im Jahr 2011 zu beurteilen hatte. Hier hat sich der Zeitschriftenverlag erfolgreich auf die Pressefreiheit aus Art. 5 Abs. 1 GG berufen. Die Veröffentlichung der Altberichte im Onlinearchiv beeinträchtigte zwar das Persönlichkeitsrecht des Haftentlassenen (betroffen war das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG). Der BGH hat aber den geltend gemachten Unterlassungsanspruch anhand von §§ 823 Abs. 1, 1004 Abs. 1 BGB und § 57 Abs. 1 Satz 1 RStV überprüft und im Rahmen seiner Einzelfallabwägung festgestellt, dass der betroffene Haftentlassene die Beeinträchtigung durch die Altberichte hinnehmen müsse. Hier überwiege das durch Art. 5 GG geschützte Veröffentlichungsinteresse des Verlags. Es bestehe ein anerkennenswertes Interesse der Öffentlichkeit nicht nur an der Information über das aktuelle Zeitgeschehen, sondern auch an der Möglichkeit, vergangene zeitgeschichtliche Ereignisse zu recherchieren. Eine Kenntnisnahme vom Inhalt der beanstandeten Meldung hätte überdies eine gezielte Suche vorausgesetzt, weil der Verlag die Altberichte zum Mordfall lediglich in das Archiv eingestellt und nicht in besonderer Weise auf sie aufmerksam gemacht hatte [BGH, Urteil vom 22.02.2011, Aktenzeichen: VI ZR 346/09, abrufbar unter www.bundesgerichtshof.de unter Entscheidungen – aktuelle Entscheidungen].

Näheres zum Datenschutzrechts im nichtöffentlichen Bereich wird unter Abschnitt 5 ausgeführt.

- ⇨ Zum Datenschutz als Grundrechtsschutz: Hans-Jürgen Papier in BPB, S. 67 ff.
- ⇨ Kühling/Seidel/Sivridis, S.50-71.
- ⇨ Tinnefeld/Buchner/Petri, S. 91-111.

5. Einfachgesetzliches Datenschutzrecht

Wie bereits in den vorangegangenen Kapiteln angesprochen, ist ein wichtiger Bestandteil des Datenschutzes das Datenschutzrecht. Das einfachgesetzliche Datenschutzrecht wird in diesem Kapitel in seinen wesentlichen Grundzügen vorgestellt. Ebenso wichtig ist die Gewährleistung des Datenschutzes durch Technik, Organisation und Verfahren (Kapitel 6). Andere Themen wie vor allem der Datenschutz als Bildungsauftrag [dazu Edgar Wagner in BPB, S. 88-98, Frank und Thomas Spaeing in BPB, S. 249-256] können hier nur erwähnt werden.

5.1 Warum es ein Bundesdatenschutzgesetz und Landesdatenschutzgesetze gibt

Die Europäische Datenschutzrichtlinie unterscheidet hinsichtlich der Datenverarbeitung grundsätzlich nicht zwischen öffentlichen Stellen (insbesondere Behörden) und nicht-öffentlichen Stellen (insbesondere Unternehmen und Vereine). In Deutschland ist dies unter anderem wegen verfassungsrechtlichen Gründen anders. Art. 70 Abs. 1 GG [lesen!] sieht vor, dass die Länder das Recht der Gesetzgebung haben, soweit das Grundgesetz nicht dem Bund eine Gesetzgebungsbefugnis verleiht.

Die Befugnisse der Bundesverwaltung werden ausschließlich durch Bundesgesetze geregelt.[8] Dem entsprechend gilt das **Bundesdatenschutzgesetz** (BDSG) gemäß § 1 Abs. 2 Nr. 1 BDSG für den Umgang **öffentlicher Stellen des Bundes** mit personenbezogenen Daten (auf die Stellen des Bundes anwendbar sind der erste, zweite, vierte und fünfte Abschnitt des BDSG, bei öffentlich-rechtlichen Wettbewerbsunternehmen auch dessen dritter Abschnitt).

Der Bund hat auch das Recht der Gesetzgebung für die Datenverarbeitung sogenannter **nicht-öffentlicher Stellen**. Sie ist vor Allem aus Art. 74 Abs. 1 Nr. 1 (bürgerliches Recht), Nr. 3 (Vereinsrecht) und Nr. 11 (Recht der Wirtschaft) und Nr. 12 (Arbeitsrecht) abzuleiten. Für sie sind der erste sowie der dritte bis fünfte Abschnitt des BDSG anzuwenden.

Sofern der Bund keine Gesetzgebungskompetenz hat, haben die **Länder** das Recht der Gesetzgebung. Das gilt insbesondere für die Verarbeitung personenbezogener Daten durch **öffentliche Stellen der Länder**. Diese Datenverarbeitung ist in den Landesdatenschutzgesetzen geregelt, siehe z.B. Artikel 2 Abs. 1, Abs. 2 Bayerisches Datenschutzgesetz (BayDSG, lesen!).

- ⇨ Kühling/Seidel/Sivridis, S. 50.
- ⇨ Tinnefeld/Buchner/Petri, S. 114 – 119.

[8] Das ergibt sich mittelbar aus Art. 84 Abs. 1 Satz 1, Art. 85 Abs. 1 Satz 1 GG sowie teilweise ausdrücklich aus Art. 87 GG. Teilweise wird Bundeskompetenz auch aus den Sachkompetenzen in Art. 73 und Art. 74 GG abgeleitet.

5.2 Allgemeine Datenschutzgesetze und „bereichsspezifischer“ Datenschutz

Einschränkungen des Grundrechts auf Datenschutz bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss (siehe bereits Teil I Abschnitt 4.3).

Greift der Umgang mit personenbezogenen Daten intensiv in das Persönlichkeitsrecht ein, müssen die gesetzlichen Befugnisse besonders klar und bestimmt geregelt sein. Deshalb können die allgemeinen Datenschutzgesetze zwar die allgemeine Verarbeitung durch die Verwaltung bzw. die nicht-öffentlichen Stellen regeln. Für besonders eingriffsintensive Verarbeitungen oder besondere Fallgestaltungen müssen jedoch **bereichsspezifische Datenschutzregelungen** geschaffen werden.

Es gibt eine Vielzahl von solchen Spezialregelungen. Einige Beispiele für solche Vorschriften aus dem Sicherheitsbereich wurden bereits in Teil I vorgestellt. Besondere Regelungen gibt es auch im Melderecht, im Bereich der Finanz- und Steuerverwaltung [dazu: Polenz in BPB S. 145-153], in der Bildungsverwaltung (Schul- und Hochschulrecht), im Bereich der planenden Verwaltung, im Prozessrecht, für den Beschäftigtendatenschutz [Däubler in BPB, S. 188-198, Wolf in BPB, S. 199-205, Perreng in BPB, S. 206-213], für den Gesundheitsbereich usw. [Überblick bei Tinnefeld/Buchner/Petri, S. 221-222, S. 139-214 und S. 296-318]. Zumeist gibt es dabei „Mischbereiche“, in denen grundsätzlich das allgemeine Datenschutzrecht gilt und einige Besonderheiten durch Spezialregelungen geregelt werden. Zum Rangverhältnis zwischen Spezialregelungen und allgemeinen Datenschutzregeln schreibt § 1 Abs. 3 BDSG vor: „*Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten …anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.“*

Nachfolgend werden nur drei Bereiche vorgestellt, in denen es spezielle Regelungen gibt: Das Recht der inneren Sicherheit (5.2.1), das Sozialrecht (5.2.2) und das Telemedienrecht (5.2.3).

5.2.1 Das Recht der inneren Sicherheit

In Deutschland wird das Recht der inneren Sicherheit durch eine Vielzahl von Gesetzen geregelt. Es gibt auch zahlreiche Behörden, die für die öffentliche Sicherheit und Ordnung sorgen sollen. Dabei sind die Begriffe wie „innere Sicherheit“ und „öffentliche Sicherheit und Ordnung“ sehr weit zu verstehen.

Beispiel: Die Gewerbeaufsicht hat zu kontrollieren, ob Gewerbeunternehmen die Vorschriften des Arbeits-, Umwelt- und Verbraucherschutzes einhalten. Die Vorschriften über das Arbeitsschutzrecht, das Umweltrecht und das Verbraucherschutzrecht gehören zur

„öffentlichen Sicherheit“[9]. Die Behörden der Gewerbeaufsicht sind insoweit auch Ordnungsbehörden.

In politischen Auseinandersetzungen werden vor Allem die Befugnisse von Nachrichtendiensten, der Polizei und der Strafverfolgungsbehörden diskutiert. Insoweit bietet es sich an, beim Recht der inneren Sicherheit vereinfachend mehrere Entwicklungsstufen zu unterscheiden:

1. Vorfeld einer Gefahr für die öffentliche Sicherheit.
   Hier werden personenbezogene Daten verarbeitet, ohne dass ein Rechtsgut konkret gefährdet sein muss. Typisches Beispiel: Beschaffung von Informationen über Vorgänge, die möglicherweise den Bestand des Staates gefährden könnten.
2. Gefahrenlage.
   Personenbezogene Daten werden im Zusammenhang mit einer Situation verarbeitet, die bei ungehindertem Geschehensablauf voraussichtlich zu einer Schädigung eines Rechtsguts führen würde. Typisches Beispiel: Polizeiliche Ermittlungen zur Aufklärung und Abwendung von Gefahren.
3. Schädigendes Ereignis.
   Personenbezogene Daten stehen im Zusammenhang mit einer bereits begangenen Straftat oder Ordnungswidrigkeit oder eines anderen schädigenden Ereignisses. Typisches Beispiel: Ermittlungen zur Aufklärung und Verfolgung von Straftaten oder Ordnungswidrigkeiten.
4. Gerichtliche Beurteilung.
   Personenbezogene Daten werden im Zusammenhang mit einem Gerichtsverfahren verwendet. Typische Beispiele: gerichtliche Strafverfahren und Bußgeldverfahren.
5. Vollzug einer gerichtlichen Entscheidung. Typisches Beispiel: Strafvollzug.

Das Rechtsstaatsprinzip und insbesondere die Grundrechte verlangen es, dass die verschiedenen Phasen unterschiedliche Voraussetzungen erfüllen müssen. Vor Allem müssen die Behörden insoweit auch unterschiedliche Befugnisse haben.

Beispiel 1: Bei Stufe 1 gibt es noch keinen konkreten Verdacht einer Rechtsgutgefährdung. In aller Regel sind deshalb nur die **Nachrichtendienste** zu einer solchen Aufklä-

[9] In der Polizeirechtsliteratur wird die öffentliche Sicherheit wie folgt definiert: „Unverletzlichkeit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter des Einzelnen sowie der Einrichtungen und Veranstaltungen des Staates oder sonstiger Träger der Hoheitsgewalt“. Der Schutz privater Rechtsgüter wird allerdings durch die öffentliche Sicherheit nur eingeschränkt gewährleistet.

rung befugt. Sie haben jedoch keine Zwangsbefugnisse. Das ist sehr wichtig und auch gut so! Ansonsten könnten rechtstreue Bürger mit dem diffusen Hinweis auf die allgemeine Sicherheitslage mit Zwangsmaßnahmen überzogen werden. Die Datenverarbeitung der Verfassungsschutzbehörden wird in den Verfassungsschutzgesetzen des Bundes und der Länder geregelt, darüber hinaus gibt es besondere Gesetze für den für die Auslandsaufklärung zuständigen Bundesnachrichtendienst (BND) und den Militärischen Abschirmdienst (MAD).

Beispiel 2: Die **Polizei** hat Zwangsbefugnisse, die sie einsetzen kann, um ein konkretes Rechtsgut zu beschützen. Das Polizeirecht ist deshalb stark vom Effektivitätsgrundsatz geprägt. Zugleich muss die Verhältnismäßigkeit der eingesetzten Mittel gewahrt bleiben. Bei der personenbezogenen Datenerhebung müssten also strengere Regeln gelten als bei Stufe 1, die für die Polizei grundsätzlich ein Tabu ist. Die Datenverarbeitung der Landespolizeien wird teilweise in den Polizeigesetzen der Länder geregelt. Im Übrigen gilt das allgemeine Datenschutzrecht.

Beispiel 3: Bei den Stufen 3 und 4 geht es darum, bereits begangene Taten aufzuklären. Eine Beschädigung eines Rechtsguts hat also– etwa durch eine Straftat - schon stattgefunden. Zwar sollen die **Strafverfolgungsbehörden** die Straftaten aufklären und verfolgen. Es soll aber möglichst auch sichergestellt werden, dass nicht unschuldige Personen bestraft werden. Deshalb ist das Strafverfahrensrecht sehr justizförmig ausgestaltet. So steht die Ermittlungstätigkeit der Polizei hier unter der **Verfahrensherrschaft der Staatsanwaltschaft**. Die Datenerhebung und Datenverwendung im Zusammenhang mit der Strafverfolgung wird überwiegend in der Strafprozessordnung (StPO) geregelt.

- ⇨ Zum Thema der Prävention: Marion Albers in BPB, S. 102-114.
- ⇨ Thomas Petri in BPB, S. 115-128.
- ⇨ Jörg Ziercke in BPB, S. 129-136.

5.2.2 Das Sozialgesetzbuch (SGB)

In vielen Situationen sind einzelne Menschen auf die Unterstützung des Staates angewiesen. Das Sozialstaatsprinzip verlangt die Verwirklichung von sozialer Gerechtigkeit und sozialer Sicherheit. Sozialleistungen einschließlich sozialer und erzieherischer Hilfen sollen dazu beitragen, ein menschenwürdiges Dasein zu sichern, gleiche Voraussetzungen für die freie Ent-

faltung der Persönlichkeit zu schaffen, die Familien zu schützen und zu fördern, den Erwerb des Lebensunterhalts durch eine frei gewählte Tätigkeit zu ermöglichen und besondere Belastungen des Lebens abzuwenden oder auszugleichen [§ 1 Abs. 1 SGB 1 – Aufgaben des Sozialgesetzbuchs].
Das Sozialrecht gewährt allerdings zumeist nur Anspruch auf Sozialleistungen, wenn die anspruchsberechtigten **Menschen in einer besonders schutzbedürftigen Lage** sind.

> Beispiele für Sozialleistungen: Arbeitslose erhalten eine Grundsicherung, es gibt eine Arbeitsförderung (SGB 2, SGB 3), Kranken-, Unfall- und Rentenversicherung (SGB 4, SGB 5, SGB 7, SGB 6), Kinder- und Jugendschutz (SGB 8), Rehabilitation und Teilhabe behinderter Menschen (SGB 9), Soziale Pflegeversicherung (SGB 11)

Die Sozialverwaltung verwendet dementsprechend personenbezogene Daten, die für die betroffene Person besonders risikoträchtig sein können. Arbeitslosigkeit und gesundheitliche Beeinträchtigungen können beispielsweise zu gesellschaftlichen Diskriminierungen führen. Minderjährige sind ebenfalls besonders schutzwürdig. Dementsprechend sieht das Sozialgesetzbuch für Sozialdaten in § 35 SGB 1 ausdrücklich ein **Sozialgeheimnis** vor. § 35 Abs. 1 Sätze 1 und 2 lauten wie folgt:

> *„Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 Zehntes Buch) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.“*

Der **Sozialdatenschutz** weist einige Besonderheiten auf. Zunächst wird er **im Sozialgesetzbuch abschließend geregelt**. Ein Rückgriff auf die allgemeinen Datenschutzgesetze ist also nicht vorgesehen. Im SGB 10 gibt es allgemeine sozialdatenschutzrechtliche Vorschriften (§§ 67 – 85a SGB 10), die durch bereichsspezifische Regelungen in den einzelnen Büchern ergänzt werden.

> Beispiel: Im Bereich der Kinder- und Jugendhilfe werden die Vorschriften des SGB 10 durch die §§ 61-68 SGB 8 ergänzt und teilweise durch strengere Regelungen ersetzt. So sieht § 65 SGB 8 einen besonderen Vertrauensschutz für Sozialdaten vor, die den Jugendämtern im Zusammenhang mit der persönlichen und erzieherischen Hilfe anvertraut worden sind.

Sozialleistungen werden regelmäßig **nur auf Antrag** hin gewährt. Die Sozialbehörden haben dann zu prüfen, ob die Voraussetzungen für die beantragte Sozialleistung vorliegen. Die Antragsteller müssen diese Prüfung unterstützen, vor Allem indem sie die notwendigen Auskünfte erteilen und erbetene Unterlagen vorlegen. Sie haben also **Mitwirkungspflichten**, die überwiegend in den §§ 60 – 67 SGB 1 und § 21 Abs. 2 SGB 10 geregelt sind. Im Sozialdatenschutzrecht wird sehr häufig über die Reichweite und die Grenzen der Mitwirkungspflichten gestritten.

> Beispiel 1: Muss ein Arbeitsloser der zuständigen Behörde die Auszüge seiner Girokonten vorlegen? Für welchen Zeitraum kann die Behörde die Vorlage solcher Auszüge verlangen? Darf der Arbeitslose bestimmte Daten schwärzen? Usw.
>
> Beispiel 2: Außendienstmitarbeiter von Sozialbehörden führen Hausbesuche bei Antragstellern von Sozialleistungen durch. Insbesondere geht es um die Aufdeckung so genannte „Bedarfsgemeinschaften“. Danach bestehen bestimmte Leistungsansprüche nicht, wenn die arbeitslosen Antragsteller mit Personen in einer Bedarfsgemeinschaft zusammenleben, die den gemeinsamen Lebensunterhalt aus eigenen Mitteln bestreiten können. Die gesetzlichen Vorschriften sehen hierzu weder ausdrücklich eine Mitwirkungspflicht der Antragsteller dahingehend vor, in solche Hausbesuche einzuwilligen noch gibt es ausdrücklich eine Duldungspflicht. Was geschieht aber, wenn der Antragsteller sie verweigert?

Die in Beispiel 1 aufgeworfenen Fragen wurden vom Bundessozialgericht (BSG) im Jahr 2008 grundlegend geklärt [BSG, Urteil vom 19.09.2008, Aktenzeichen: B 14 AS 45/07 R]. Das BSG stellte fest, dass Leistungsempfänger nach dem SGB 2 auf Verlangen der Behörde zwar verpflichtet sind, ihre Kontoauszüge zumindest der letzten drei Monate vorzulegen [vgl. § 60 Abs. 1 Nr. 3 SGB 1]. Die Leistungsempfänger dürfen aber die Empfänger von Zahlungen in den Kontoauszügen schwärzen, wenn andernfalls besondere personenbezogene Daten (Parteizugehörigkeit, konfessionelles Bekenntnis usw.) offengelegt werden müssten.

Kommt der Antragsteller einer Sozialleistung seinen Mitwirkungspflichten nicht nach und wird hierdurch die Klärung der Anspruchsvoraussetzungen erheblich erschwert, kann der So-

zialleistungsträger die beantragte Leistung versagen oder entziehen. Das gilt solange, bis die Voraussetzungen nachgewiesen sind.

Beispiel 2 ist aus datenschutzrechtlicher Sicht ein rechtsstaatliches Ärgernis. Zwar gibt es sicherlich Sachverhalte, in denen ein Hausbesuch angebracht ist, etwa um einen Sozialleistungsbetrug aufzudecken. Der Sache nach stellen Hausbesuche aber einen Eingriff in die grundrechtliche Garantie der Unverletzlichkeit der Wohnung aus Art. 13 GG dar. Ein solcher Eingriff muss gesetzlich klar geregelt sein. Etwas anderes würde nur gelten, wenn die Antragsteller freiwillig in den entsprechenden Hausbesuch einwilligen würden. Davon können die Behörden bei unangekündigten Hausbesuchen jedoch aus mehreren Gründen regelmäßig nicht ausgehen. Zunächst wird die Einwilligung in den weitaus meisten Fällen nicht freiwillig erfolgen. Die so besuchten Personen müssen befürchten, dass ihre Sozialleistungen gekürzt werden, wenn sie den Zutritt zu ihrer Wohnung verweigern. Darüber hinaus steht der Überraschungseffekt ebenfalls einer wirksamen Einwilligung entgegen. Verweigern die Antragsteller den Zutritt gleichwohl, müssen sie das Fehlen einer Bedarfsgemeinschaft nachweisen [§ 7 Abs. 3a SGB 2]. Wie soll man jedoch etwas nachweisen, was nicht existiert?!

⇨ Tinnefeld/Buchner/Petri, S.304-308.

5.2.3 Telemedienrecht[10]

Das Thema Datenschutz wird in der Öffentlichkeit häufig im Zusammenhang mit der Nutzung des Internet diskutiert. Tatsächlich erzeugt jede Handlung in der „Online-Welt“ digitale Datenspuren.

> Beispiel: Internetprotokoll-Adressen (IP-Adressen) bilden die technische Grundlage des internetbasierten Informationsaustauschs. Sowohl der am Internet angeschlossene Rechner des Absenders von Daten als auch der Rechner eines Datenempfängers weisen jeweils eine IP-Adresse auf. Sie wirken wie die Adressangabe auf einem Briefumschlag.

Im Beispiel besteht allerdings ein erheblicher Unterschied zwischen der IP-Adresse und einem Brief. Abgesehen von seltenen Ausnahmen wie etwa Einschreiben wird der Brief zugestellt, ohne dass der Postdienstleister die Adresse des Absenders und des Empfängers regis-

[10] Dieser Abschnitt folgt in großen Teilen BayLfD, 25. Tätigkeitsbericht 2012, Abschnitt 1.3, ohne dass dies im Weiteren besonders gekennzeichnet wird.

triert. Anders im Internet: Hier gehört die Protokollierung der IP-Adresse zur vielgeübten Praxis. Daneben werden aber auch regelmäßig Daten über das Betriebssystem, sowie Art und Version des verwendeten Browsers mitsamt der verwendeten Einstellungen erfasst. Die meisten Anbieter von Webseiten legen überdies Cookies oder vergleichbare Kleindateien auf den Rechnern der Nutzer ab. Sie geben bei etwaigen mehrfachen Besuchen ein und derselben Webseite Aufschluss über frühere Aufrufe. Zusammengetragen ergeben solche Datenspuren sehr schnell ein genaues Profil der Interessen und Gewohnheiten des Betroffenen. Insbesondere wenn der Nutzer sich gegenüber einem Anbieter identifiziert, können entsprechende Zuordnungsmöglichkeiten zu einer nun namentlich bekannten Person entstehen.
Die Nutzung des world wide web ist also nicht nur mit Chancen, sondern auch mit gewissen Risiken verbunden. Ein hinreichender Grund für den Bundesgesetzgeber, die Zulässigkeit der Datenverarbeitung durch WWW-Dienste bereichsspezifisch im **Telemediengesetz** (TMG) zu regeln. Es trägt damit auch dem grundrechtlich besonders geschützten **Fernmeldegeheimnis** aus Art. 10 GG Rechnung.
Das Internetdatenschutzrecht ist nicht zuletzt deshalb kompliziert, weil ein und derselbe Nutzungsvorgang von mehreren Gesetzen geregelt wird:

1. Soweit es allein um die technische Übertragung von Signalen über Telekommunikationsnetze oder um telekommunikationsgestützte Dienste geht, findet das **Telekommunikationsgesetz** (TKG) Anwendung. Beispiel: Internet-Telefonie als Dienstleistung ist nach dem TKG zu beurteilen. Die Abgrenzung ist heutzutage bisweilen schwer zu treffen, weil insbesondere Smartphones Dienste anbieten, die dem Telemedien- und dem Telekommunikationsbereich zugeordnet werden könnten (**Medienkonvergenz**).
2. Das **Telemediengesetz** gilt nur für die **elektronischen Informations- und Kommunikationsdienste**, soweit sie nicht bestimmte Telekommunikationsdienste nach dem Telekommunikationsgesetz sind [§ 1 TMG lesen!]. Typische Beispiele: Meinungsforen, Weblogs, Suchmaschinen, Datendienste, Bestell- und Buchungsdienste, Onlinespiele, elektronische Presse usw.[11]
3. Sogenannte **Inhaltsdaten** sind nach den **allgemeinen Datenschutzgesetzen** zu beurteilen. Beispiel: Erfasst ein Online-Bestelldienst (z.B. Amazon, zvab, Ebay usw.) das Nutzungsverhalten, muss er das TMG beachten. Sofern der Nutzer für die Durchführung der Bestellung Angaben macht, ist die Weiterverarbeitung dieser Angaben nach dem BDSG zu beurteilen.

[11] Der Rundfunk fällt formal nicht unter das TMG, die Regeln des TMG sind aber gemäß dem Rundfunkstaatsvertrag weitgehend analog anzuwenden.

Vereinfacht ausgedrückt sieht das TMG in den §§ 7 - 10 eine beschränkte Verantwortlichkeit der Anbieter von Telemediendiensten für fremde Inhalte vor. Wie die allgemeinen Datenschutzgesetze verlangt auch das TMG in § 12 für jede Verarbeitung personenbezogener Daten eine Legitimation und statuiert den Grundsatz der Zweckbindung. Nach § 13 TMG sind Anbieter gegenüber ihren Nutzern zur **Transparenz der Erhebung und Verwendung** personenbezogener Daten verpflichtet. Soweit eine gesetzliche Erlaubnis zum Umgang mit personenbezogenen Daten fehlt, ist bei den Nutzern eine **Einwilligung** einzuholen. Sie kann zwar elektronisch erteilt werden. Allerdings muss der Anbieter dann u.a. gewährleisten, dass der Nutzer seine Erklärung auch zu einem späteren Zeitpunkt nachvollziehen kann. Werden die Nutzer an andere Dienste weitergeleitet, ist ihnen dies anzuzeigen. Im Rahmen des Zumutbaren muss ein Dienst die anonyme und **pseudonyme Nutzung** ermöglichen. Der Umgang mit Bestandsdaten nach § 14 TMG und Nutzungsdaten nach § 15 TMG folgt strikt dem **Prinzip der Erforderlichkeit**. Bei aller Kritik im Einzelnen hat das Telemediengesetz im Großen und Ganzen sachgerechte Antworten auf das WWW des 20. Jahrhunderts gegeben.
Ob dieses Gesetz auch noch auf die Herausforderungen des Web2.0 ("Social Web") des 21. Jahrhunderts angemessen antworten kann, ist allerdings äußerst fraglich. Im sogenannten Web2.0 wirken technische Fortentwicklungen (z.B. einfache Suche mittels wirkmächtiger Suchmaschinen, Erweiterung von Speicher- und Übertragungskapazitäten), veränderte ökonomische Rahmenbedingungen (z.B. Finanzierung der Datenverarbeitung für breite Bevölkerungsschichten) und soziokulturelle Veränderungen (Wertewandel) zusammen. Was den Umgang mit personenbezogenen Daten anbelangt, schlüpfen Nutzer in die Rolle von "**produsern**" (Nutzer und Datenverarbeitende). Daten werden mehr und mehr vernetzt, immer neue Angebote und Nutzungsmöglichkeiten entstehen, Datenverarbeitungsträger werden immer kleiner und leistungsfähiger, können überall und jederzeit genutzt werden - die Datenverarbeitung wird mit anderen Worten allgegenwärtig. Gerade Telemediendienste werden auf vielfache Weise miteinander verschränkt und verknüpft, ohne dass dies für die Nutzer immer erkennbar ist.

> Beispiel: Auf immer mehr Webangeboten sind sogenannte **Social Plugins** wie der Like-Button ("Gefällt mir") von Facebook oder der "+1-Button" von Google zu finden. Sie sollen kostengünstig die Reichweite von Webangeboten erhöhen. Problematisch hieran ist der Umstand, dass Social Plugins oft technisch direkt in die Webseiten eingebunden werden. Beim Laden der Webseite (etwa www.webseite_xyz.de) wird der Browser dabei angewiesen, eine weitere Webseite von dem Sozialen Netzwerk zu la-

den und an der vorgesehenen Stelle innerhalb der anderen Webseite anzuzeigen. Dabei werden zumindest der Zeitpunkt des Aufrufs der Referenzwebseite und die IP-Adresse des Nutzerrechners an das Soziale Netzwerk übertragen. Dies geschieht ohne jegliche Mitwirkung der Nutzer, regelmäßig auch ohne deren Wissen.

Die direkte Einbindung von Social Plugins ist häufig, verstößt aber gegen das TMG. Sie ist nicht zur Erbringung des Telemediendienstes erforderlich [§ 15 Abs. 1 TMG lesen!]. Darüber wird der Nutzer zu Beginn des Nutzungsvorgangs nicht über Art, Umfang und Zwecke der Erhebung und Verwendung von Daten unterrichtet [§ 13 Abs. 1 TMG lesen!].

Heftig umstritten ist auch die Frage, ob und inwieweit Stellen im Rahmen ihrer **Öffentlichkeitsarbeit eine Fanseite in einem Sozialen Netzwerk** datenschutzkonform errichten können [dazu z.B. Orientierungshilfe „Fanpages bayerischer öffentlicher Stellen in sozialen Netzwerken zum Zwecke der Öffentlichkeitsarbeit“, abrufbar unter www.datenschutz-bayern.de unter Veröffentlichungen / Broschüren / Orientierungshilfen].

- ⇨ Kühling/Seidel/Sivridis, S. 221-259.
- ⇨ Tinnefeld/Buchner/Petri, S. 387-412.

5.3 Wesentliche Grundsätze des einfachgesetzlichen Datenschutzrechts

5.3.1 Jeder Umgang mit personenbezogenen Daten bedarf einer Legitimation

Der Umgang mit personenbezogenen Daten ist grundsätzlich verboten, wenn er nicht durch eine **Rechtsvorschrift** oder durch die **Einwilligung** der betroffenen Person erlaubt wird [§ 4 Abs. 1 BDSG, Art. 15 Abs. 1 BayDSG].

Beispiel 1: Arbeitgeber und Betriebsrat regeln in einer Betriebsvereinbarung, dass der Arbeitgeber in näher bestimmten Grenzen im Betrieb Videoüberwachung durchführen kann.

Beispiel 2: Ein Kreditinstitut schließt mit einem Verbraucher einen Darlehensvertrag. In den Allgemeinen Geschäftsbedingungen ist vorgesehen, dass das Kreditinstitut die Bonität des Kunden überprüfen darf.

Beispiel 3: Wer in einem Kaufhaus oder Supermarkt mit EC-Karte zahlt, unterschreibt häufig eine „Datenschutzerklärung“ auf der Rückseite des Kassenbelegs. Diese Datenschutzklauseln haben zumeist zwei Regelungsinhalte: Sofern der Versuch des Unternehmens scheitert, den Kaufbetrag einzuziehen, stimmt der Kunde zu, dass das Unternehmen von dem kontoführenden Kreditinstitut die Adressdaten des Kunden erhält. Für diesen Fall stimmt der Kunde auch zu, dass er in eine Sperrdatei aufgenommen wird.

Eine Rechtsvorschrift ist zumeist eine gesetzliche Regelung [zu Beispielen außerhalb des BDSG siehe bereits Abschnitt 5.2]. Das muss aber nicht so sein. Die in Beispiel 1 genannte **Betriebsvereinbarung** wird ebenfalls im Grundsatz als „Rechtsvorschrift“ anerkannt. Auch **Satzungen,** wie sie etwa durch Kommunen oder auch durch Vereine verabschiedet werden, sind andere Rechtsvorschriften im Sinne des Datenschutzrechts. Solche untergesetzlichen Rechtsvorschriften sind allerdings nur wirksam, wenn sie nicht im Widerspruch zu höherrangigem Recht stehen.

Rechtsvorschriften im öffentlichen Bereich ergeben sich zunächst aus bereichsspezifischen Regelungen. Das allgemeine Datenschutzrecht sieht für Stellen des Bundes Befugnisse insbesondere in den §§ 13-16 BDSG vor. Bayerische öffentliche Stellen müssen die Voraussetzungen der Art. 15-23 BayDSG beachten, sofern nicht speziellere Regelungen bestehen. Extrem knapp zusammengefasst kann eine Datenverarbeitung im Eigeninteresse der öffentlichen Stelle nur zulässig sein, soweit sie durch eine entsprechende Aufgabe gerechtfertigt ist. Im Allgemeinen ist der Umgang öffentlicher Stellen mit personenbezogenen Daten stärker reguliert

als die Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen. Denn die Verwaltung ist in besonderer Weise an Recht und Gesetz gebunden [Art. 20 Abs. 3 GG – lesen!].

Rechtsvorschriften im nicht-öffentlichen Bereich sind vor Allem in den §§ 28-29 BDSG geregelt. Die Vorschriften sind für nicht-öffentliche Stellen zumeist weniger streng, weil nicht nur die betroffenen Personen, sondern auch die verarbeitenden Stellen von grundrechtlichen Freiheiten sind [siehe bereits Teil I, Abschnitt 4.3, Seite 25-27].

Der in Beispiel 2 genannte **Vertrag** zwischen dem Kreditinstitut und einem Verbraucher ist keine Rechtsvorschrift und auch keine Einwilligung. Gleichwohl kann die vorgesehene Datenverarbeitung zulässig sein. Denn § 28 Abs. 1 Nr. 1 BDSG erklärt den Umgang mit personenbezogenen Daten für zulässig, wenn er „für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist." Sind diese Anforderungen erfüllt, ist die vorgesehene Verarbeitung personenbezogener Daten durch eine Rechtsvorschrift gedeckt. Ob diese Voraussetzungen erfüllt sind, muss anhand des jeweiligen Geschäftszweckes ermittelt werden.
Den Umgang mit personenbezogenen Daten für **eigene Geschäftszwecke** wird für nicht-öffentliche Stellen vor allem in § 28 BDSG geregelt [diese Vorschrift vollständig lesen!]. Der wohl am weitesten gehende gesetzliche Erlaubnistatbestand für nicht-öffentliche Stellen ergibt sich dabei vor allem aus § 28 Abs. 1 Nr. 2 BDSG. Diese Vorschrift erlaubt eine Verarbeitung, wenn die Stelle dazu ein berechtigtes Interesse hat, die Datenverarbeitung hierfür erforderlich ist und kein Grund für die Annahme besteht, dass schutzwürdigen Interessen der betroffenen Person entgegenstehen. Geboten ist hier also eine **Interessenabwägung**. Die Verarbeitung allgemein zugänglicher Daten wird nach § 28 Abs. 1 Nr. 3 BDSG erleichtert.
§ 28 Abs. 3 bis 4 BDSG regelt die Verwendung von Daten zu Werbezwecken und zum Zweck des Adresshandels.
Besondere gesetzliche Erlaubnistatbestände im BDSG außerhalb des § 28 BDSG betreffen die **Datenweitergabe an Auskunfteien** nach § 28a BDSG sowie das sogenannte **Scoringverfahren** nach § 28b BDSG. Bildet der Umgang mit personenbezogenen Daten den eigentlichen Geschäftszweck, so muss die Stelle § 29 BDSG beachten. Diese Vorschrift betrifft vor Allem die Tätigkeiten von Auskunfteien, von Adresshändlern oder Unternehmen der Werbebranche.

Die Datenschutzerklärung in Beispiel 3 ist demgegenüber eine **Einwilligungserklärung** [dazu bitte § 4a BDSG und Art. 15 Abs. 2-4 BayDSG lesen!]. Sie ist nur wirksam, wenn u.a. die

betroffene Person informiert und freiwillig ihre Zustimmung zur Verarbeitung ihrer Daten erteilt. Darüber hinaus muss sie regelmäßig schriftlich erteilt werden.

- ⇨ Dagmar Hartge in BPB, S. 280-289.
- ⇨ Dirk Heckmann in BPB, S. 267-279.

5.3.2 Zweckbindung

Das Prinzip der Zweckbindung ist ein zentraler datenschutzrechtlicher Grundsatz. Er besagt, dass der Umgang mit personenbezogenen Daten auf einen bestimmten Zweck auszurichten ist. Das schließt eine Verarbeitung von Daten zu anderen Zwecken zwar nicht generell aus. Diese Zweckänderung muss aber ihrerseits besonders legitimiert sein.

> Beispiel 1: Die (relativ schwache) Bindung nicht-öffentlicher Stellen an einen bestimmten Verarbeitungszweck ist im Allgemeinen durch § 28 Abs. 1 Satz 2 und § 28 Abs. 2 und Abs. 3 geregelt [die zitierten Vorschriften bitte lesen!]. Danach kann ein Unternehmen die Daten, die es aufgrund eines Vertragsverhältnisses mit der betroffenen Person erlangt hat, auch für andere Zwecke verwenden, wenn dies durch eine Interessenabwägung nach § 28 Abs. 2 Nr. 1 in Verbindung mit § 28 Abs. 1 Nr. 2 BDSG gerechtfertigt ist.

> Beispiel 2: Für die öffentliche Verwaltung des Bundes sieht § 14 Abs. 2 BDSG Regeln vor, die bei einer zweckändernde Speicherung, Veränderung oder Nutzung von Daten zu beachten sind. § 14 Abs. 2 BDSG sieht zwar für die allgemeine Verwaltungstätigkeit einen Katalog von 9 erlaubten Zweckänderungen vor.

An dieser Stelle wird noch einmal daran erinnert, dass allgemeine Datenschutzregeln nur angewendet werden können, soweit es keine bereichsspezifischen Regelungen gibt.

> Beispiel 3: Eine Verfassungsschutzbehörde erhebt und verarbeitet personenbezogene Daten in aller Regel für die Zwecke ihrer Aufgabenerfüllung. Eine Übermittlung an die Polizei für deren Aufgaben richtet sich nicht nach den allgemeinen Datenschutzgesetzen [bitte § 15 BDSG und Art. 18 BayDSG lesen], sondern nach dem für die Behörde geltenden Verfassungsschutzgesetz.

Als Faustformel kann man sich merken: Eine Änderung des Verarbeitungszweckes ist normalerweise zulässig, wenn die verantwortliche Stelle die Daten nach einer Rechtsvorschrift oder wirksamen Einwilligung unabhängig von dem ursprünglichen Zweck auch zu dem anderen Zweck erheben und verwenden dürfte.

5.3.3 Erforderlichkeit und Interessenabwägung

Fast alle Vorschriften, die eine Erhebung, Verarbeitung oder Nutzung erlauben, verlangen hierfür, dass der jeweilige Verarbeitungsvorgang für den vorgesehenen Zweck erforderlich ist.

> Fallbeispiel: Eine Kunde hat ein Kontovertrag bei einer Bank gekündigt. Noch zwei Jahre später speichert die Bank die Daten des früheren Kunden. Sie will ihn nach wie vor mit gezielten Marketingmaßnahmen zurückgewinnen.

Ursprünglich mag die Bank die Kundendaten auf § 28 Abs. 1 Nr. 1 BDSG gestützt haben. Die jetzige Datenspeicherung zur Zurückgewinnung von ehemaligen Kunden kann die Bank jedoch nicht mehr auf § 28 Abs. 1 Nr. 1 BDSG stützen. Denn die weitere Aufbewahrung der Daten ist nicht erforderlich, um das Vertragsverhältnis mit dem ehemaligen Kunden zu begründen, durchzuführen oder zu beenden. Will man die besagte weitere Speicherung für Rückgewinnungsaktionen rechtfertigen, müsste man also eine andere Legitimationsgrundlage heranziehen.

Bevor Sie weiterlesen, versuchen Sie bitte folgende Frage eigenständig zu beantworten: Welche Rechtsgrundlagen würden Sie in Betracht ziehen?

Wenn die Bank den ehemaligen Kunden zurückgewinnen will, wird sie ihm besondere Angebote unterbreiten. Letztlich ist eine solche Nutzung von personenbezogenen Daten eine Form der Werbung. Die Datenverarbeitung ist folglich nach § 28 Abs. 3 – 4 BDSG zu beurteilen. Diese Vorschrift ist eine Spezialvorschrift gegenüber § 28 Abs. 1 Nr. 2 BDSG – er darf auf den gebildeten Fall nicht angewendet werden.

Im Ergebnis wird eine Speicherung nur in Betracht kommen, wenn die betroffene Person in eine Verwendung ihrer Daten zum Zweck der Werbung wirksam eingewilligt hat. Denn § 28 Abs. 3 Satz 6 sieht vor, dass eine Verwendung der Daten zu Werbezwecken nach Abs. 3 Satz 2-4 nur zulässig ist, soweit **schutzwürdige Interessen des Betroffenen** nicht entgegenstehen. Dies ist eine Klausel, die in Datenverarbeitungsvorschriften sehr häufig vorkommt. Sie ver-

langt nach einer Abwägung zwischen legitimen Verarbeitungsinteressen der verantwortlichen Stelle (hier: Bank) und den schutzwürdigen Belangen der betroffenen Person (hier: ehemaliger Bankkunde). Für ein überwiegendes schutzwürdiges Interesse des ehemaligen Bankkunden spricht, dass er selbst die ursprüngliche Vertragsbeziehung beendet hat. Damit hat der Kunde zugleich den Vertrauenstatbestand beseitigt, der ursprünglich eine Datenverwendung zu Werbezwecken gerechtfertigt hatte.[12] Eine andere Bewertung ist gerechtfertigt, wenn die betroffene Person wirksam in die weitere Verwendung der Daten durch die Bank eingewilligt hat.

5.3.4 Betroffenenrechte

Eine „informationelle Selbstbestimmung", wie sie das Grundrecht auf Datenschutz verlangt, ist nur möglich, wenn die von einer Verarbeitung betroffene Person bestimmte Rechte einfordern kann. Betroffenenrechte sind unverzichtbare Werkzeuge des Datenschutzrechts und zugleich ein wesentlicher **Bestandteil des Selbstdatenschutzes**.
Man kann die Betroffenenrechte in **Transparenzrechte**, in **Steuerungsrechte** und „**Sanktionsrechte"[13]** unterteilen.
Das wichtigste Transparenzrecht ist der **Anspruch auf Auskunft** [§ 34 BDSG, Art. 10 BayDSG lesen!]. Danach hat die verantwortliche Stelle der betroffenen Person auf Verlangen regelmäßig mitzuteilen, welche Daten sie konkret über sie gespeichert hat, zu welchen Zwecken diese Speicherung erfolgt, woher die Informationen stammen und an wen sie übermittelt worden sind. Das Auskunftsrecht wird durch verschiedene andere Informations-, Unterrichtungs- und Benachrichtigungsrechte ergänzt [z.B. § 4 Abs. 3 BDSG, § 6c Abs 1 BDSG, § 33 BDSG, Art. 13 BayDSG, Art. 16 Abs. 3 BayDSG; speziell zur Transparenz von Videoüberwachung: § 6b Abs. 2 BDSG, Art. 21a Abs. 2 BayDSG].

Die Transparenzrechte sind für die betroffene Person sehr wichtig, weil sie oft nur so von einer Verarbeitung ihrer personenbezogenen Daten erfährt. Nur dann kann sie auch von anderen Rechten Gebrauch machen. Trotzdem werden die Transparenzrechte nicht ausnahmslos gewährleistet, sondern können **in bestimmten Fällen eingeschränkt** werden. Allgemein gesagt, darf eine Auskunft verweigert werden, soweit legitime Geheimhaltungsinteressen des Staates oder Privater der Auskunft entgegenstehen.

[12] Es wäre allenfalls denkbar, dass die Bank innerhalb kurzer Frist ein Versuch zur Rückgewinnung des Kunden unternimmt. Im gebildeten Beispiel sind jedoch bereits mehr als zwei Jahre verstrichen.
[13] Im eigentlichen juristischen Wortsinn wird der Begriff der Sanktion zumeist als Strafmaßnahme verstanden. Hier sollen Sanktionen weitergehend als Maßnahmen verstanden werden, die an begangene Rechtsverstöße anknüpfen.

Beispiel: Die Polizei verdächtigt eine betroffene Person, dass sie Mitglied eine Mafiabande ist. Sie ermittelt deshalb verdeckt. Eine Auskunftserteilung würde den Erfolg der Ermittlungen unmöglich machen. In einem solchen Fall kann die Polizei eine Auskunft beschränken oder ganz unterlassen.

Sofern eine betroffene Person die Datenverarbeitung kennt, kann sie bestimmte Steuerungsrechte wahrnehmen. Wichtig sind die Rechte auf Berichtigung, Löschung und Sperrung [§ 20 BDSG, § 35 BDSG, Art. 11 und 12 BayDSG lesen!]:

1. **Berichtigung** ist die Korrektur unrichtiger Daten.
2. **Löschung** kann verlangt werden, soweit personenbezogene Daten zu Unrecht gespeichert werden. Zu Unrecht sind Daten gespeichert, wenn sie für einen legitimen Zweck nicht mehr erforderlich sind - oder nie waren.
3. Kommt eine Löschung nicht in Betracht, kann die **Sperrung** verlangt werden. Sie kommt in Betracht, wenn a) die Richtigkeit bestritten wird aber noch nicht geklärt ist, b) an und für sich gelöscht werden müsste, eine Löschung jedoch aus rechtlichen Gründen unzulässig wäre.

Erfolgte eine Verarbeitung personenbezogener Daten rechtswidrig, kommen bestimmte Sanktionsrechte in Betracht. Als Betroffene einer strafbaren Verarbeitung kann eine Person **Strafantrag** stellen. Darüber hinaus hat sie bei schwerwiegenden Verletzungen ihres Persönlichkeitsrechts auch das Recht auf **Schadensersatz** [§§ 7 und 8 BDSG, § 44 Abs. 2 BDSG, Art. 14 und 37 Abs. 3 BayDSG lesen].
Gerade im Zeitalter des Internet sind die dargestellten Betroffenenrechte zentral für einen effektiven Datenschutz. Zugleich sind sie im besonderen Maße gefährdet, wenn und weil insbesondere die rechtlichen Vorgaben zur Transparenz missachtet werden. Deshalb wird es immer wichtiger, dass die Ausübung von Betroffenenrechten von vorneherein technisch unterstützt werden. Die rechtlichen Vorgaben für einen **Systemdatenschutz** in diesem Sinne sind allerdings noch weithin unbefriedigend ausgestaltet [zum Systemdatenschutz siehe Peter Schaar in BPB, S. 363-371].

- ⇨ Alexander Dix in BPB, S. 290-297.
- ⇨ Kühling/Seidel/Sivridis, S. 185-196.
- ⇨ Tinnefeld/Buchner/Petri, S. 270-279

5.3.5 Datenschutzkontrolle und Sanktionen

„Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch vorgezogene Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung."

Mit diesen Worten beschreibt das Bundesverfassungsgericht die Rolle der Datenschutzbehörden im Volkszählungsurteil vom 15.12.1983.

Das allgemeine Datenschutzrecht sieht jedoch auch eine **stelleninterne Datenschutzkontrolle** vor. Sie wird durch **betriebliche bzw. behördliche Datenschutzbeauftragte** vorgenommen. Die Beauftragten haben die Aufgabe, auf die Einhaltung der Datenschutzvorschriften hinzuwirken. Sie sind dabei Ansprechpartner für die Stellen und für betroffene Personen. Dabei müssen die verantwortlichen Stellen eine gewisse Unabhängigkeit der Beauftragten gewährleisten [§§ 4f, 4g BDSG, Art. 25 BayDSG lesen!]

Die **externe Kontrolle** wird durch die Datenschutzbeauftragten des Bundes und der Länder sowie durch das Bayerische Landesamt für Datenschutzaufsicht[14] wahrgenommen [zu Rechtsstellung und Aufgaben bitte § 22 – 24 BDSG, § 38 BDSG, Art. 29-35 BayDSG lesen].

Daneben gibt es eine Reihe von besonders gelagerten Fällen der Datenschutzkontrolle. Sie ist jeweils der verfassungsrechtlich gewährleisteten Unabhängigkeit der zu kontrollierenden Stelle geschuldet. Für die Überwachung des Bayerischen Rundfunks ist die Datenschutzbeauftragte des Bayerischen Rundfunks zuständig. Eine Datenverarbeitung der Bayerischen Landeszentrale für neue Medien wird von dem Datenschutzbeauftragten bei dieser Landeszentrale kontrolliert. Der Datenschutz bei den Kirchen unterliegt der Kontrolle durch die Datenschutzbeauftragten dieser Religionsgemeinschaften.

Erhebliche Datenschutzverstöße können in den gesetzlich geregelten Fällen durch Bußgelder, teilweise durch Strafen geahndet werden [bitte §§ 44, 45 BDSG, Art. 37 BayDSG lesen!].

- ⇨ Meike Kamp / Sarah Thomé in BPB, S. 298-309.
- ⇨ Kühling/Seidel/Sivridis, S. 197-206, S. 216.
- ⇨ Tinnefeld/Buchner/Petri, S. 279-292

[14] In Bayern ist – anders als in den übrigen Bundesländern – die Kontrolle der öffentlichen Stellen und die Aufsicht über die nicht-öffentlichen Stellen nach § 38 BDSG organisatorisch getrennt.

6. Datenschutz durch Technik, Organisation und Verfahren

IT-Sicherheit beschäftigt sich mit der Einhaltung von Sicherheitsstandards. Sie sollen insbesondere sicherstellen, dass die verarbeiteten Daten verfügbar, integer und vertraulich bleiben. Zwar ist **IT-Sicherheit** kein Teilgebiet des Datenschutzes, weist aber große Schnittmengen mit dem technikbezogenen Datenschutz auf. Manchmal stehen Anforderungen der IT-Sicherheit auch in einem Spannungsverhältnis zum technischen Datenschutz.

> Beispiel 1: Nach betriebsinternen Vorgaben sind Serverräume zumeist abzuschließen. Zu ihnen hat nur die Systemadministration Zutritt. Damit wird eine Forderung der IT-Sicherheit erfüllt (Der unbefugte Zugriff auf die IT wird erschwert, damit werden insbesondere die Ziele der Integrität und Vertraulichkeit verfolgt). Zugleich werden hierdurch datenschutzrechtliche Vorgaben erfüllt [Zutrittskontrolle, lesen Sie dazu bitte Anlage zu § 9 BDSG, Nr. 1]

> Beispiel 2: Um missbräuchliche Datenverwendung zu unterbinden, ordnen zahlreiche Arbeitgeber eine Protokollierung der Internetnutzung an. Dies kann unter bestimmten Umständen aus Gründen der IT-Sicherheit (und unter Umständen des technischen Datenschutzes, lesen Sie Anlage zu § 9 BDSG, Nr. 5) geboten sein. Zugleich berühren sie den Datenschutz der betroffenen Beschäftigten.

Die geltende Gesetzeslage zum technischen Datenschutz fordert „angemessene technische und organisatorische Maßnahmen“, die erforderlich sind, um die Datenschutzgesetze zu gewährleisten. Insbesondere verlangt die Anlage zu § 9 BDSG (ähnlich Art. 7 Abs. 2 BayDSG):

1. Zutritts-, Zugangs- und Zugriffskontrollen (Anlage zu § 9 BDSG Nr. 1, 2, 3): Danach dürfen nur berechtigte Personen die Räume der IT-Systeme betreten, sie verwenden und auf die dort gespeicherten Daten zugreifen.
2. Weitergabekontrolle (Anlage zu § 9 BDSG Nr.4): Sie soll die Vertraulichkeit der Daten im Rahmen von Übermittlungen und sonstigen Weitergaben sichern. Die Verschlüsselung ist ein typisches Beispiel hierfür.
3. Eingabekontrolle (Anlage zu § 9 BDSG Nr.5): Sie ermöglicht es nachzuvollziehen, wer wann welche personenbezogene Daten auf IT-Systemen verarbeitet hat (siehe dazu Beispiel 2).
4. Auftragskontrolle (Anlage zu § 9 BDSG Nr. 6): Sie betrifft das Spezialproblem der sogenannten Auftragsdatenverarbeitung, bei der eine verantwortliche Stelle die eigene

Datenverarbeitung an externe Stellen auslagert. Dies geht nur unter bestimmten Voraussetzungen, die § 11 BDSG beschreibt. Die Einhaltung dieser Voraussetzungen muss für den Auftraggeber kontrollierbar sein.

5. Verfügbarkeitskontrolle (Anlage zu § 9 BDSG Nr. 7): Sie betrifft den Schutz vor Verlust oder zufälliger Zerstörung. Kreditinstitute und Versicherungen unterhalten dazu beispielsweise in der Regel mehrere räumlich von einander getrennte Rechenzentren, in denen jeweils komplett die Kundendaten gespeichert werden.
6. Trennungsgebot (Anlage zu § 9 BDSG Nr.8): Personenbezogene Daten, die zu einem bestimmten Zweck verwendet werden sollen, dürfen nicht für andere Zwecke verwendet werden. Das soll durch eine getrennte Datenhaltung unterstützt werden. Beispielsweise dürften Mitarbeiterdaten der Lohnbuchhaltung nicht auch von der Marketingabteilung eines Unternehmens eingesehen werden.

Um diese Vorgaben umzusetzen, bedarf es oft aufwändiger technischer und organisatorischer Maßnahmen. Sie werden häufig als „IT-Management“ oder „**Datenschutz-Management**“ bezeichnet. Dazu muss die verantwortliche Stelle zunächst die Ausgangslage analysieren und die technisch-organisatorischen Prozesse definieren. Hierbei spielen die oben aufgelisteten Vorgaben der Anlage zu § 9 BDSG, bzw. des Art. 7 Abs. 2 BayDSG eine große Rolle. Hat die Stelle so die Mindestanforderungen des technischen Datenschutzes festgestellt, muss es ein bestimmtes Sicherheitsniveau festlegen.

Hierzu sehen die allgemeinen Datenschutzgesetze vor, dass **betriebliche bzw. behördliche Datenschutzbeauftragte** auf die Einhaltung des Datenschutzes hinwirken sollen [Lesen Sie dazu bitte § 4f, § 4g BDSG und Art. 25 BayDSG]. Bevor datenschutzrelevante Verarbeitungsprozesse in Gang gesetzt werden, haben sie zu prüfen, ob das jeweils geplante Verfahren datenschutzkonform ist. Dabei gibt es durchaus Unterschiede zwischen den Vorgaben des BDSG [lesen Sie bitte § 4d Abs. 5, 6 BDSG] und des BayDSG [lesen Sie bitte Art. 26 BayDSG]. Die vorhandenen Verarbeitungsverfahren sind zu dokumentieren [§ 4d, § 4e BDSG; Art. 27 BayDSG].

- ⇨ Angelika Martin in BPB, S. 390-399
- ⇨ Tinnefeld/Buchner/Petri, S. 415-448

Das hier nur grob skizzierte Konzept des technikbezogenen Datenschutzes stammt im Wesentlichen aus den 1960er und 1970er Jahren. Es ist zwar später punktuell ergänzt worden (etwa durch das Trennungsgebot oder die Ziele der Datenvermeidung und Datensparsamkeit

in § 3a BDSG). Angesichts der rasanten Entwicklung der Informations- und Kommunikationstechnologie ist dieses Regelungskonzept jedoch nicht mehr zeitgemäß. Charakteristisch für diese Entwicklung ist eine immer kleiner und leistungsfähiger werdende Informationstechnik. Zugleich werden IT-Dienstleistungen heute immer häufiger über **Netzwerke** bereitgestellt [zu den damit verbundenen Herausforderungen der IT-Sicherheit siehe Martin Schallbruch in BPB, S. 372-380].

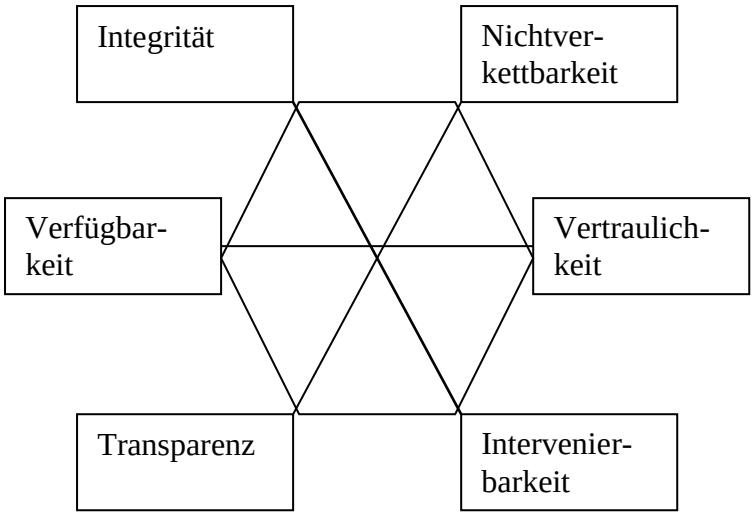
> Beispiel 1: Smartphones sind Mobiltelefone, die eine vergleichsweise große Rechnerkapazität und einen großen Funktionsumfang aufweisen. Die Funktionen der marktgängigen Smartphones lassen sich durch Apps nahezu beliebig erweitern. Diese Erweiterungen lädt sich der Nutzer oder die Nutzerin zumeist von Webseiten der Hersteller herunter.

> Beispiel 2: Die Stichworte Smart Grid, Smart Metering und Smart-Home bezeichnen Erscheinungsformen der „intelligenten“ Stromerzeugung und – versorgung. Dies geschieht durch einen netzbasierten Datenaustausch zwischen Versorgern und Geräten in den Haushalten der Nutzer.

Wie hat also der technische Datenschutz auf die veränderten technischen Rahmenbedingungen der heutigen Datenverarbeitung zu reagieren?

Ein wirksamer Datenschutz baut auf ein effektives Zusammenwirken von rechtlichen Vorgaben und technischen Maßnahmen. Bei vernetzten IT-Systemen kann ein effektiver DAtenschutz jedoch nur gewährleistet werden, wenn sie den Datenschutz „eingebaut“ haben („**Privacy by Design“).** Verfahren müssen datenschutzfreundliche Voreinstellungen bieten („**Privacy by Default**“). Als wichtige Systemkomponenten sind die Zielsetzungen der Datenvermeidung und Datensparsamkeit künftig verbindlicher auszugestalten. Dazu gehört es, dass verantwortliche Stellen personenbezogene Daten nach Möglichkeit anonymisieren oder zumindest pseudonymisieren [zu den Begriffen lesen Sie bitte § 3 Abs. 6 und Abs. 6a BDSG]. Vor Allem aber wäre es praxisgerecht, wenn die bisher geltenden technisch-organisatorischen Vorgaben des § 9 BDSG (und des Art. 7 Abs. 2 BayDSG) durch **elementare Schutzziele des Datenschutzes** ersetzt werden. Schutzziele haben gegenüber den bisherigen Kontrollvorgaben den Vorzug, dass sie entwicklungsoffener formuliert sind. Zugleich nähern sie die Vorgehensweisen zur Sicherstellung des technischen Datenschutzes und zu IT-Sicherheitsstandards

stärker aneinander an. Neben den bereits erwähnten IT-Schutzzielen der Verfügbarkeit (der Zugriff auf Informationen ist sicherzustellen), Vertraulichkeit (unbefugte Kenntnisnahmen sind zu unterbinden) und Integrität (das IT-System hat ausschließlich seine zweckbestimmte Funktion zuverlässig und erwartungsgemäß zu erfüllen) sind die Schutzziele der Intervenierbarkeit (Betroffenenrechte sind technisch abzubilden), Transparenz (die Verarbeitungsprozesse müssen nachvollziehbar sein) und Nichtverkettbarkeit (technische Abbildung der Zweckbindung) datenschutzrechtlich von besonderer Bedeutung. Aus den elementaren Schutzzielen lassen sich weitere Schutzziele ableiten.



Wer das Konzept der Schutzziele durchdenkt, stößt unvermeidlich auf die Feststellung, dass die Schutzziele in einem wechselseitigen Spannungsverhältnis zu einander stehen. Beispielsweise beeinflusst eine transparente Datenverarbeitung die Vertraulichkeit, die Gewährleistung von Betroffenenrechte die Integrität usw. Verschiedene Schutzziele sind also im Rahmen eines Datenschutzkonzepts in Einklang zu bringen.

- ⇨ Martin Rost in BPB, S. 353-362
- ⇨ Peter Schaar in BPB, S. 363-371