**Projektgruppe „Datenschutz, Persönlichkeitsrechte“**

Arbeitsergebnis zum Punkt 2.1 (*streitige Textpassagen sind kursiv gesetzt*.)

**Inhaltsverzeichnis**

# Kapitel 2.1 Prinzipien, Ziele, Werte

## 2.1.1 Schutzgegenstand

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

Zentraler Anknüpfungspunkt des bestehenden Datenschutzkonzepts sind die sog. „personenbezogenen Daten“. [Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 100.] Im Mittelpunkt der Abwägungen des Datenschutzes aber stehen Informationen, nicht Daten. Es geht regelmäßig um Interessen der Grundrechtsträger, dass staatliche Stellen oder Dritte etwas nicht als Information erfahren und nutzen können, und auf der anderen Seite deren Wissens- und Verwertungsinteressen.

Personenbezogene Daten werden definiert als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (Art. 2 lit. a DSRL, § 3 Abs. 1 BDSG). Der Begriff wird weit verstanden und umfasst praktisch jede Information, die mit einer natürlichen Person in Verbindung gebracht werden kann. Es genügt also eine „Personenbeziehbarkeit“. [Fußnote: *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 40.] Angaben über persönliche Verhältnisse betreffen etwa Identifikationsmerkmale, äußere Merkmale, aber

auch innere Zustände (z.B. Meinungen), Angaben über sachliche Verhältnisse dagegen alle Beziehungen des Betroffenen zu Dritten und zur Umwelt (z.B. Eigentumsverhältnisse, Vertragsbeziehungen). [ Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 101.]

Auch das BVerfG geht in seiner ständigen Rechtsprechung von einem weiten Verständnis aus. So hat das Gericht in seinem wegweisenden Volkszählungsurteil zu den Angaben personenbezogener Daten ausgeführt: „Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr.“ [Fußnote: BVerfGE 65, 1, 45.]

Weiterer regulatorischer Anknüpfungspunkt ist der Umgang mit diesen Daten. Dabei werden in der DSRL und im BDSG unterschiedliche Begrifflichkeiten verwendet. Während in der DSRL die „Verarbeitung“ (im weiteren Sinne) der Daten als Oberbegriff für jeden Vorgang im Zusammenhang mit den personenbezogenen Daten zu verstehen ist (Art. 2 lit. b DSRL), unterscheidet das BDSG zwischen den einzelnen Vorgängen der Erhebung, Verarbeitung (im engeren Sinne) und (sonstigen) Nutzung der Daten (§ 4 Abs. 1 BDSG). Materiell erfasst sind vor allem die Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung und Löschung von personenbezogenen Daten. Dabei ist ein technikneutrales Verständnis zu Grunde zu legen. Erfasst sind sowohl automatische als auch nicht-automatische Verfahren. [Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 49.]

Für einen kleinen Ausschnitt der personenbezogenen Daten gilt, in Anpassung an die Vorgaben der EG-Datenschutzrichtlinie 95/46, ein erhöhtes Schutzniveau: Hierzu gehören die sog. sensiblen Daten wie rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit und Daten über die Gesundheit und die Sexualität (vgl. Art. 8 DSRL, § 3 Abs. 9 BDSG).

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

Absatz streitig

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

Bis Z. 102 alternativer Textvorschlag zu vorstehendem Absatz.

*Allerdings ist diese Erkenntnis nicht so neu. Daten und Informationen können je nach Kontext, in dem sie relevant werden, personenbeziehbar werden. Deshalb hat der Gesetzgeber im Bundesdatenschutzgesetz mit einem weit auszulegenden Begriff des Personenbezuges reagiert, um sicherzustellen, dass jedenfalls Daten nicht von vornherein aus dem Schutz herausfallen dürfen. Gerade weil erst der jeweilige Verwendungskontext entscheidet, kann es*

*wie das BVerfG hervorgehoben hat, keine per se trivialen, nicht-schutzwürdigen Daten geben.*

*Im Hinblick auf einen noch vorgelagerten gefährdungsabhängigen Schutz ist es allerdings notwendig, die Dogmatik des Personenbezugs dynamisch weiterzuentwickeln. So zeigt das Beispiel der Geodaten, aber auch der Scoring-Diskussion, dass die gezielte Verarbeitung von Daten schon vor ihrer Zusammenführung hinsichtlich einer bestimmten Person Risiken dann bergen, wenn sie letztlich darauf abzielen, Einzelne statistisch einzuteilen und damit erhebliche Benachteiligungen für Personen oder Personengruppen nach sich ziehen können, wie dies z.B. beim Wohnortscoring der Fall ist.*

### 2.1.2 Grundprinzipien des Datenschutzrechts

Erlaubnisvorbehalt

Ein zentraler Grundsatz des Datenschutzrechts lässt sich in einem Satz wie folgt formulieren: Der Umgang mit personenbezogenen Daten ist verboten, es sei denn, der Betroffene willigt ein oder eine Rechtsnorm legitimiert ihn. Dieser Grundsatz ist sowohl im Gemeinschaftsrecht (Art. 7 DSRL), als auch im nationalen allgemeinen (§ 4 Abs. 1 BDSG) und bereichsspezifischen Datenschutzrecht (z.B. § 12 TMG) normiert. Demnach bestimmt sich die Zulässigkeit eines jeden einzelnen Datenverarbeitungsvorgangs danach, ob der Betroffene den Vorgang erlaubt hat oder ob er sich auf einen gesetzlichen Erlaubnistatbestand stützen lässt. [Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 130 f.]
Die Einwilligung ist vor allem im nicht-öffentlichen Bereich, neben den vertraglichen Legitimationen, von erheblicher Bedeutung.

[Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 131.] Sie legitimiert einen Datenverarbeitungsvorgang nur dann, wenn sie wirksam erteilt wurde, wofür das Gesetz bestimmte Mindestanforderungen vorsieht (vgl. § 4a BDSG oder auch Art. 7 lit. a) DSRL wonach die betroffene Person „ohne jeden Zweifel ihre Einwilligung gegeben“ haben muss). Nach nationalem Recht (§ 4a BDSG) ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, also ohne Zwang erfolgt. Dies setzt voraus, dass der Einzelne Bedeutung und Tragweite seiner Entscheidung erkennen kann.

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

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

*Überall dort, wo eine gestörte Vertragsparität vorliegt, sollte die Einwilligung des Betroffenen unwirksam sein, so insbesondere im Abhängigkeitsverhältnis Arbeitnehmer bzw. Bewerber zum Arbeitgeber sowie Bürger - bspw. als Leistungsempfänger - zum Staat , sofern es für die Abfrage dieser persönlichen Daten keine gesetzliche Grundlage gibt. Auch bei Verträgen zwischen Verbrauchern und Unternehmen existiert keine Parität. So kann z.B. bei internetbasierten Dienste, die ohne die Einwilligung zur Preisgabe persönlicher Daten, die für die Erbringung des Dienstes selbst nicht benötigt werden, nicht abgeschlossen werden, von einer freiwilligen Einwilligung nicht ausgegangen werden, wenn diese Dienstleistung nicht auch ohne Datenerhebung erhältlich ist.*

Absatz streitig, Alternativtext folgt im nächsten Absatz.

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

Alternativtext zu vorstehendem Absatz.

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

Nach datenschutzrechtlichen Grundsätzen ist eine Einwilligung also nur dann wirksam, wenn sie in Kenntnis der

entscheidungsrelevanten Umstände erteilt wird. Der Betroffene muss auf der Grundlage der ihm vorliegenden Informationen Bedeutung und Tragweite seiner Entscheidung zur Datenfreigabe erkennen können. Im Hinblick auf die spezifischen Bedingungen im digitalen Bereich ergeben sich hier neue Herausforderungen.

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

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

Einwilligungen werden unbefristet erteilt. Eine echte Transparenz und ein Überblick über die erteilten Einwilligungen ist für die Nutzer angesichts der Vielzahl der eingeforderten Einwilligungen nur schwer zu behalten. Der Betreiber des Dienstes unterscheidet sich oftmals von der datenverarbeitenden Stelle, eine Transparenz darüber, welche Dienste bzw. Unternehmen welche Daten erhalten, ist oftmals nicht vorhanden. In einer solchen Situation können die Arbeitnehmer/Bürger/Nutzer ihre Informations-, Widerrufs-, Korrektur- und Löschrechte nur unzureichend geltend machen.

Eine autonome Entscheidung über die Preisgabe eigener Daten im Internet können Menschen dann fällen, wenn sie Vor- und Nachteile ihrer Einwilligung einschätzen und Handlungsalternativen erkennen können. Die Medienkompetenz des Einzelnen trägt wesentlich dazu bei, informierte Einwilligungen zu ermöglichen und zu befördern. Diese kann aber nicht in gleicher Ausprägung von allen Personen erwartet werden und kann nicht als Ersatz für bedürfnisgerechtere Anforderungen an Transparenz, Information und Einwilligung stehen.

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

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

<u>Erforderlichkeitsgrundsatz</u>

Der Erforderlichkeitsgrundsatz folgt aus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz und ist zudem in Art. 7 lit. b) bis f) DSRL festgeschrieben. Er steht in engem Zusammenhang mit dem Grundsatz der Zweckfestlegung und der Zweckbindung. Demnach ist der Umgang mit personenbezogenen Daten auf das zum Erreichen des angestrebten Zieles erforderliche Minimum zu beschränken. [Fußnote: BVerfGE 65, 1, 46.] Es sollen nur so viele Daten erhoben, verarbeitet oder genutzt werden, wie zur Zweckerreichung unbedingt notwendig. Für den öffentlichen Bereich ist der Grundsatz in §§ 13 bis 16 (insbesondere in den Abs. 1) normiert, wobei der zulässige Zweck

auf die öffentliche Aufgabenerfüllung begrenzt ist. Der Erforderlichkeitsgrundsatz gilt aber auch im nicht-öffentlichen Bereich, wo seine effektive Verwirklichung durch eine möglichst genaue Zweckbestimmung bedingt ist. [Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 136.]

Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz besagt, dass die Daten, die für einen bestimmten Zweck erhoben worden sind, auch nur zu diesem Zweck verarbeitet oder genutzt werden dürfen. [Fußnote: *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 48.] Der Zweck der Datenerhebung begrenzt folglich den weiteren Umgang mit den erhobenen Daten. Sie dürfen nur zu dem Zweck weiter verwendet werden, der von der Einwilligung oder der konkret legitimierenden Rechtsnorm erfasst ist. Das setzt voraus, dass das Ziel der Datenverarbeitung und/oder -nutzung bereits vor der Datenerhebung so genau wie möglich bestimmt ist. Eine Speicherung auf Vorrat für künftige, noch nicht bekannte Zwecke ist dagegen grundsätzlich unzulässig. [Fußnote: *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 48.]

*Vor allem im nicht-öffentlichen Bereich stößt die Beibehaltung dieses Grundsatzes auf praktische Probleme. In einer vernetzten Welt ist der Datenaustausch oftmals durch Spontanität und gerade nicht durch eine vorherige Festlegung des Verarbeitungszweckes bestimmt. [Fußnote: Kühling, Verw 40 (2007), 153, 159.]*

Absatz streitig.

*Die Frage der Freiwilligkeit einer Einwilligung hat in der digitalen Welt an Brisanz gewonnen. Wenn beispielsweise die Nutzung eines Online-Dienstes voraussetzt, dass der Nutzer durch Ankreuzen einer Checkbox der Erhebung seiner Daten zustimmt, so sind sich die Betroffenen über die Tragweite ihrer Entscheidung häufig nicht im Klaren. Da sie die entsprechenden Datenschutzbestimmungen*

Ergänzungsantrag bis Zeile 344, streitig.

*des Anbieters bzw. dessen Allgemeine Geschäftsbedingungen, in die erstere bisweilen integriert sind, häufig nicht oder nur oberflächlich zur Kenntnis nehmen, erteilen sie im Zweifel alle Einwilligung, die sie bei genauerer Überlegung nicht erteilt hätten. Um zu klären, ob die für eine informierte und freiwillige Entscheidung wichtigen Informationen tatsächlich in ausreichend transparenter Weise vorgelegen haben, ist es dann jedoch bereits zu spät: Die Daten werden erhoben, und der Betroffene ist sich darüber häufig nicht im Klaren. Folglich kommt es im Nachhinein auch nicht mehr zur Überprüfung der Rechtsgültigkeit der erteilten Einwilligung. Die Erfahrung zeigt, dass die Mehrzahl der Internetnutzer Datenschutzerklärungen ebenso wenig liest wie Allgemeine Geschäftsbedingungen und dennoch am elektronischen Geschäftsverkehr teilnimmt. Dies deutet darauf hin, dass die Mehrzahl der auf diesem Wege erteilten Einwilligungen nicht freiwillig erteilt worden sind, woraus zu schließen werde, dass in zahlreichen Fällen Daten ohne rechtliche Grundlage erhoben und gespeichert werden. Man erkennt hier, dass die an sich begrüßenswerte Intention des Gesetzgebers, einen maximalen Schutz der personenbezogenen Daten des Einzelnen zu ermöglichen, im Internetzeitalter nicht mehr verwirklicht wird. Die Praxis der elektronischen Einwilligung nach §13 Abs. 2 TMG wird von Diensteanbietern systematisch dazu genutzt, den Datenschutz zu unterlaufen, indem sie sich auf diese Weise die Zustimmung zu Datenerhebungen von den Nutzern erteilen lassen, die in aller Regel deren Interesse, die eigene Privatsphäre zu schützen, zuwiderlaufen. Anders gesagt: Das bloße „Abklicken“ einer Einwilligung in die Erhebung und Verwendung personenbezogener Daten zu allerlei Zwecken ist nur formal eine freiwillige Einwilligung. Faktisch werden Bürgerinnen und Bürger auf diese Weise entmündigt. Dahinter steht das Interesse der Anbieter, diese Daten zu monetarisieren. Derartige Geschäftsmodelle laufen den*

*Interessen der Bürgerinnen und Bürger auch dann zuwider, wenn sie eine kostenfreie Nutzung des betreffenden Dienstes allererst ermöglichen, weil sie darauf basieren, die Privatsphäre des Einzelne dem Primat der wirtschaftlichen Wertschöpfung zu unterwerfen. Schon heute ist bei vielen Onlinediensten für die Nutzer nicht mehr durchschaubar, wozu ihre Daten genutzt werden und in welcher Weise sie im Rahmen von Datenhandel weiterverbreitet werden.*

*Um das Datenschutzrecht in einer bürgerfreundlichen Weise weiterzuentwickeln, sind Regelungen zu schaffen, die dem Nutzer seine verlorene Souveränität wiedergeben. Ihm müssen Mittel an die Hand gegeben werden, die es ihm ermöglichen, die Kontrolle über die Erhebung personenbezogener Daten tatsächlich, nicht nur formal selbst auszuüben. Privacy-by-default-Modelle sind hierfür geeignete Ansatzpunkte. Denkbar sind auch verbindliche Vorgaben für die Diensteanbieter, die es diesen auferlegen, stets auch eine Alternative zu der Option einer „freiwilligen“ Zustimmung zur umfassenden Erhebung personenbezogener Daten anzubieten. Dies könnte beispielsweise dadurch realisiert werden, dass ein aktives Anklicken verschiedener Berechtigungen zwingend vorgeschrieben wird. Der Betroffene müsste dann jeweils gesondert in die Erhebung und Verarbeitung personenbezogener Daten zu unterschiedlichen Verwendungszwecken, in den Einsatz unterschiedlicher Webtracking-Techniken und unterschiedlicher Cookies einwilligen. Zu bedenken wäre auch, die Einwilligung unter dem Vorbehalt einer Erneuerung zeitlich zu befristen, sodass nach Ablauf einer gewissen Zeit der Nutzer seine Zustimmung erneut abgeben müsste.*

*Wo von vornherein eine gestörte Vertragsparität vorliegt, sollte die Einwilligung des Betroffenen auch dann unwirksam sein, wenn sie nach derzeit geltendem Recht freiwillig erteilt wurde, da in Abhängigkeitsverhältnissen grundsätzlich nicht davon auszugehen*

*ist, dass Freiwilligkeit im Sinne der gesetzgeberischen Intention tatsächlich gegeben ist. Wenn etwa Sozialhilfeempfänger gegenüber der Bundesagentur für Arbeit in die Speicherung einwilligen, weil sie fürchten, dass diese Einwilligung eine Voraussetzung für den Leistungsbezug darstellen könnte, ist dies ebenso problematisch, wie wenn Arbeitnehmer ihrem Arbeitgeber umfassende personenbezogene Daten zur Verfügung stellen. Der im Bundesdatenschutzgesetz vorgesehene Vorbehalt der freiwilligen Einwilligung in die Erhebung personenenbezogener Daten ist deshalb nicht unreflektiert auf das Beschäftigungsverhältnis zu übertragen. Vielmehr ist im Falle gestörter Vertragsparität eine Regelung vorzusehen, die die Rechte der jeweils schwächeren Partei wirksam schützt.*

Transparenzgrundsatz

Die informationelle Selbstbestimmung setzt nach Auffassung des BVerfG voraus, dass Bürger wissen und grundsätzlich auch entscheiden können sollen, „wer was wann und bei welcher Gelegenheit“ über ihn weiß. [Fußnote: BVerfGE 65, 1, 43.]Das setzt wiederum voraus, dass Datenerhebungs-, -verarbeitungs- und -nutzungsvorgänge transparent gestaltet werden. Zudem ist der Transparenzgrundsatz die grundlegende Voraussetzung dafür, dass Betroffene aktive Datenschutzrechte wahrnehmen können. Transparenz wird in erster Linie durch den Grundsatz der Direkterhebung verwirklicht, wonach die Daten grundsätzlich beim Betroffenen zu erheben sind (§ 4 Abs. 2 S. 1, Abs. 3 BDSG), so dass er unmittelbar Kenntnis von dem Vorgang erlangt. Nur unter engen Voraussetzungen darf die Datenerhebung ohne Mitwirkung des Betroffenen erfolgen (§ 4 Abs. 2 S. 2 BDSG). Flankiert wird das Transparenzgebot durch Auskunftsrechte und Informations-, Benachrichtigungs-, Unterrichtungs-, Hinweis- und

Aufklärungspflichten der verantwortlichen Stelle. [Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 136.]

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

<u>Prinzip der Datenvermeidung und Datensparsamkeit</u>

Der Grundsatz der Datenvermeidung und Datensparsamkeit ist – obwohl nicht durch die DSRL vorgegeben – in § 3a BDSG normiert und besagt, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen und auch die Datenverarbeitungssysteme an diesem Ziel auszurichten sind. Dabei handelt es sich um eine Konkretisierung des Erforderlichkeitsgrundsatzes auf technischer Ebene: Schon durch die entsprechende Technikgestaltung soll das Recht auf informationelle Selbstbestimmung präventiv geschützt werden. [Fußnote: *Gola/Schomerus*, BDSG, § 3a Rn. 1.] Da der Grundsatz nicht sanktionsbewehrt ist, ist er – obwohl als Rechtspflicht formuliert – eher als Programmsatz zu verstehen. [Fußnote: *Gola/Schomerus*, BDSG, § 3a Rn. 1.]

Absatz streitig

*Das Prinzip der Datenvermeidung und Datensparsamkeit sollte durch klare Normierung gestärkt werden. Die zahlenreichen Datenskandale der letzten Zeit haben deutlich gemacht, dass die Umsetzung des datenschutzrechtlichen Erforderlichkeitsgrundsatzes in technische Features nur funktionieren kann, wenn die Aufsichtsbehörden bei Nichtbeachtung der Vorschrift wirksame Sanktionen verhängen können. Ziel muss es sein, nur die für einen bestimmten Zweck tatsächlich notwendigen Daten sammeln zu dürfen. Dazu ist eine Normierung des Grundsatzes „privacy-by-design“ erforderlich. Es ist Aufgabe des Gesetzesgebers, entsprechende Anreize zu schaffen.*

*Vorstellbar ist beispielsweise ein System der abgestuften Erwiderung, bei dem Anbietern, die sich rechtswidrig verhalten, zunächst ein Warnhinweis zugestellt wird, bevor weitere Sanktionen greifen.*

### 2.1.3 Datenschutz im Grundgesetz

Verfassungsrechtliche Verortung

Der Grundrechtekatalog des Grundgesetzes enthält im Gegensatz zur Grundrechtecharta der Europäischen Union (GRC) kein explizites Grundrecht des Datenschutzes. [Fußnote: Vgl. zur Forderung eines Grundrechtes auf Datenschutz *Kloepfer/Schärdel*, JZ 2009, 453 ff.] Gleichwohl ist der Datenschutz ein Wert von Verfassungsrang und nimmt über verschiedene Grundrechte am Grundrechtsschutz teil. Namentlich finden sich datenschutzrechtliche Gehalte im Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), im Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG) und im Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 GG). Als vorläufiger Höhepunkt in der Judikatur des verfassungsrechtlichen Datenschutzes wird das „IT-Grundrecht“ auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme angesehen. [Fußnote: Vgl. *Gurlit*, NJW 2010, 1035, 1036.]

IT-Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Als besondere Ausprägung des allgemeinen Persönlichkeitsrechts hat das BVerfG im Hinblick auf Online-Durchsuchungen das sog. IT- bzw. Computergrundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt. [Fußnote: BVerfGE 120, 274, 302 ff.] Es „schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz

nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist.“ [Fußnote: BVerfGE 120, 274, 302.]Der Schutz des Art. 10 Abs. 1 Var. 3 GG versagt, wenn der Kommunikationsvorgang beendet ist oder der Zugriff außerhalb eines laufenden Kommunikationsvorgangs des Betroffenen erfolgt, was bei der Infiltration eines Computers regelmäßig der Fall ist. [Fußnote: BVerfGE 120, 274, 307 f.] Art. 13 GG bietet raumbezogenen Schutz, welcher „nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren“, da der Eingriff standortunabhängig über das Internet erfolgen kann. [Fußnote: BVerfGE 120, 274, 310.]Das Recht auf informationelle Selbstbestimmung trägt „den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.“ [Fußnote: BVerfGE 120, 274, 312 f.]

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

Personalcomputern oder Mobiltelefonen und elektronischen Terminkalendern, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können. [Fußnote: BVerfGE 120, 274, 314.]Geschützt wird nicht nur vor einer Verletzung der Vertraulichkeit dieser Daten, sondern bereits vor dem Antasten der Integrität des Systems, da hierdurch „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen“ ist. [Fußnote: BVerfGE 120, 274, 314.]

Dabei betont das BVerfG, dass „der Standort des Systems … ohne Belang und oftmals für die Behörde nicht einmal erkennbar“ sei, was „insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone“ gelte. [Fußnote: BVerfGE 120, 274, 310 f.] Daraus lässt sich schließen, dass der Schutz unabhängig davon zu gewährleisten ist, wo der Datenbestand gespeichert ist.

Die Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung erfolgt in erster Linie nach quantitativen Gesichtspunkten. Während das Grundrecht auf informationelle Selbstbestimmung Schutz vor Zugriff auf einzelne personenbezogene Daten gewährt, geht es beim (IT-)Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme um den Schutz einer Vielzahl von (personenbezogenen) Daten (Datenbestand), die auf einem informationstechnischen System gespeichert sind. Denn wenn lediglich Daten mit einem punktuellen Bezug zu einem bestimmten Lebensbereich abgerufen werden, unterscheidet sich der staatliche Zugriff auf informationstechnische Systeme nicht von anderen Datenerhebungen und das Recht auf informationelle Selbstbestimmung ist anzuwenden. [Fußnote: BVerfGE 120, 274, 313.] Abgrenzungskriterium sind demnach Umfang und Vielfalt der

Daten und das Ausmaß der durch die Daten zu gewinnenden Rückschlüsse auf die Person des Betroffenen. Ermöglicht die Datenerhebung potentiell eine umfassende Erkenntnisgewinnung über den Betroffenen, so ist das (IT-)Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einschlägig. [Fußnote: *Hinz*, JURA 2009, 141, 144.]

### 2.1.4 Das Recht auf informationelle Selbstbestimmung als Bestandteil des Allgemeinen Persönlichkeitsrechts

Das allgemeine Persönlichkeitsrecht wird aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet. Es enthält mehrere Elemente und dient einerseits dem Schutz eines sozialen und räumlichen Rückzugsbereichs des Einzelnen und andererseits dem Schutz der individuellen Freiheit, selbst über die Präsentation der eigenen Person bestimmen zu können. [Fußnote: *Gurlit*, NJW 2010, 1035, 1037.]

Zur zweiten Gruppe gehören das Recht am eigenen Bild und am eigenen Wort und das seit dem Volkszählungsurteil aus dem Jahr 1983 [Fußnote: BVerfGE 65, 1.] verfassungsgerichtlich anerkannte Recht auf informationelle Selbstbestimmung. „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ [Fußnote: BVerfGE 65, 1, 43.]

Informationelle Selbstbestimmung und Internet

bis Z. 581 streitig, Alternativvorschlag folgt.

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

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

*Durch die zunehmende Vernetzung, die Möglichkeit der Verknüpfung von personenbezogenen Daten (Persönlichkeitsprofile) und die ständige Weiterentwicklung automatischer Datenerfassungssysteme potenziert sich die Gefahr für das allgemeine Persönlichkeitsrecht in einer „Welt der allgegenwärtigen Datenverarbeitung“[Fußnote:* Zum diesem Begriff: *Kühling*, Verw 40 (2007), 153, 155 ff.*]. Diese Gefahr besteht nicht nur im Verhältnis Bürger – Staat, sondern auch im Verhältnis Bürger – Bürger und Verbraucher – Unternehmen untereinander. Dies zeigt sich besonders deutlich bei den Diensteanbietern im Internet. Der Erfolg von Google oder sozialen Netzwerken wie*

*Facebook und studiVZ oder Internetprovidern ist geradezu dadurch bedingt, dass diese gigantische informationelle Infrastrukturen bereithalten.[Fußnote: Gurlit*, NJW 2010, 1035, 1039.*] Hier sind die Grundrechte zwar nicht (unmittelbar) anwendbar. Der Staat ist aber verpflichtet, „dem Einzelnen Schutz davor zu bieten, dass private Dritte ohne sein Wissen und ohne seine Einwilligung Zugriff auf die seine Individualität kennzeichnenden Daten nehmen“[Fußnote:* BVerfGE 117, 202, 229.*] (grundrechtliche Schutzpflicht). Schließlich hat die Verbreitung und Verarbeitung der eigenen personenbezogenen Daten im Internet mittlerweile die Grenzen der Nachvollziehbarkeit für den Einzelnen erreicht.*

*Der gegenwärtig diskutierte Datenschutz in sozialen Netzwerken wirft aber auch weitere Fragen auf. Diese betreffen insbesondere das Verhältnis der Nutzerinnen und Nutzer zu den Anbietern entsprechender Plattformen, beispielsweise wenn im Hintergrund personenbezogene Daten gesammelt und in Profilen zusammengeführt werden. Auch in diesem Fall muss der Schutz auf informationelle Selbstbestimmung erhalten bleiben. Schließlich setzt die freie Entfaltung der Persönlichkeit auch voraus, dass der Einzelne gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten geschützt wird.[Fußnote: BVerfGE 65, 1, 43.] Durch diese Schutzwirkung wird der abschreckende Effekt fremden (staatlichen und in Unternehmen vorhandenen) Geheimwissens gehemmt, „der entstehen und zur Beeinträchtigung bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß.“[Fußnote: BVerfGE 113, 29, 46.] Mit anderen Worten: Wer befürchten muss, dass seine „Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“ [Fußnote: BVerfGE 65, 1, 43.]*

571

572 *Mittlerweile hat sich daher ein kontextbezogener und gesetzlich zu*
573 *gewährender Schutzrahmen mit unterschiedlichen Komponenten*
574 *auf verschiedenen Ebenen herausgebildet. Dies reicht von*
575 *gesetzlichen Regelungen im Bundesdatenschutzgesetz (wie*
576 *beispielsweise dem bußgeldbewährten Kopplungsverbot des § 28*
577 *Abs. 3b BDSG), über die Auferlegung entsprechender Transparenz-*
578 *und Informationspflichten für Betreiber von Diensten im Internet,*
579 *bis hin zu einer Förderung der Medienkompetenz der Nutzerinnen*
580 *und Nutzer für einen verantwortungsvollen Umgang mit den*
581 *eigenen personenbezogenen Daten.*

582

583 ***Alternativer Textvorschlag zu 2.1.4***

alternativer Textvorschlag zum vorstehenden streitigen Text

584 *Informationelle Selbstbestimmung und Internet*

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

591 *Erst dieser Mehrwert machte „das Internet“ auch wirtschaftlich*
592 *erfolgreich.*

593 *Viele dieser Chancen und Möglichkeiten gehen einher mit der*
594 *Speicherung, Verarbeitung und Übermittlung zahlreicher Daten.*
595 *Technische und wirtschaftliche Voraussetzung für viele*
596 *Informations- und Kommunikationsdienste sind personenbezogene*
597 *benutzen Daten zur Gewährleistung der Funktionalität und zur*
598 *Nutzung als Wirtschaftsgut. Die personenbezogenen Nutzerdaten*

*sind die ökonomische Basis der meisten kostenlosen kommerziellen Internetdienste, bei denen die Nutzerdaten zu einem Teil die Finanzierung ergänzen, aber vor allem der „kostenlosen“ Informations- und Kommunikationsangebote, für die die Werbe-, also die Nutzerdaten, die Haupteinnahmequelle darstellten. Häufig wurden diese Angebote erst durch die Nutzung der Kundendaten zu anderen Zwecken wirtschaftlich erfolgreich. Neben den Online-Spielen haben vor allem soziale Netzwerke die Bereitschaft der Nutzerinnen und Nutzer zur Herausgabe ihrer personenbezogenen Daten gefördert und gesellschaftsfähig gemacht. Der „Wandel der Privatheit“ ist somit zuerst die Erschließung der Privatheit für kommerzielle Nutzung.*

*Diese Dienste sind aber auch missbrauchsanfällig, sei es, dass mehr Daten als erforderlich gespeichert werden, sei es, dass Nichtberechtigte Zugang zu sensiblen Daten erlangen.*

*Durch die zunehmende Vernetzung, die Möglichkeit der Verknüpfung von personenbezogenen Daten (Persönlichkeitsprofile) und die ständige Weiterentwicklung automatischer Datenerfassungssysteme potenziert sich die Gefahr für das allgemeine Persönlichkeitsrecht in einer Welt, die zunehmend als „Welt der allgegenwärtigen Datenverarbeitung“[36] erlebt wird. Mit der Computerisierung des Alltags geht die Speicherung nahezu jeder Lebensäußerung der Menschen einher. Vom „smarten“ Bad bis hin zur elektronischen Fahrkarte und der online-Reservierung für das Abendessen wird nahezu das gesamte Leben einzelner Personen zum Gegenstand von Datenverarbeitungen. Diese Entwicklung hat zweifellos auch positive Seiten. Die mit ihr einher gehenden Risiken gehen jedoch das allgemeine Persönlichkeitsrecht weit hinaus und betreffen alle Bereiche der menschlichen Existenz in ihren wirtschaftlichen, kulturellen, religiösen, politischen, sozialen und wissenschaftlichen*

*Beziehungen Hier geht es also nicht nur um das Verhältnis Bürger – Staat, sondern auch um das Verhältnis Bürger – Bürger und Verbraucher – Unternehmen untereinander.*

*In dieser Situation ist die Gesellschaft verpflichtet, Antworten über die Grenzen der juristischen Rahmenbedingungen hinaus zu finden. Vor einer juristischen Formung muss der technologische Wandel kulturell, wissenschaftlich und damit letztlich ethisch bewertet werden.*

*Bisher hat sich ein kontextbezogener und gesetzlich zu gewährender Schutzrahmen mit unterschiedlichen Komponenten auf verschiedenen Ebenen herausgebildet. Dies reicht von europäischen Vorgaben über die gesetzlichen Regelungen im Bundesdatenschutzgesetz (wie beispielsweise dem bußgeldbewährten Kopplungsverbot des § 28 Abs. 3b BDSG), über die Auferlegung entsprechender Transparenz- und Informationspflichten für Betreiber von Diensten im Internet, bis hin zu einer Förderung der Medienkompetenz der Nutzerinnen und Nutzer für einen verantwortungsvollen Umgang mit den eigenen personenbezogenen Daten.*

*Dieser verfassungsrechtliche „status quo“ ist zu erhalten und auszubauen, denn er setzt nach wie vor an der richtigen Grundprämisse an: personenbezogene Daten können potentiell in einem Maße in die Freiheitsverbürgerungen der Verfassung eingreifen, dass deren Nutzung staatlichen Schutz auslösen muss. Neuartige Schutzkonzepte zu entwickeln, die den modernen technischen Entwicklungen gerecht werden und die Selbstbestimmung der Bürgerinnen und Bürger über ihre Daten stärken, ist dabei die größte Herausforderung für eine zukunftsorientierte Datenschutzpolitik.*

***Ergänzender Textvorschlag zu 2.1.4 (bis Z. 703)***

ergänzender Textvorschlag , ebenfalls streitig.

*Insbesondere im Hinblick auf das Kopplungsverbot besteht in der digitalen Welt aber noch erheblicher Nachbesserungsbedarf. Diese Vorschrift besagt, dass der Abschluss von Verträgen nicht an die Zustimmung zur Datenweitergabe oder Werbezusendung gekoppelt werden darf. Eine solche Einwilligung ist dem Gesetz zufolge unwirksam, wenn für den Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne Einwilligung nicht zumutbar ist.*

*Gleichwohl verlangen zahlreiche Diensteanbieter ihren Kunden ab, in die Einwilligung zur Erhebung von weit mehr persönlichen Daten einzuwilligen, als für die Nutzung des betreffenden Angebots nötig wäre. So brauchen etwa ein Onlinehändler keineswegs zu speichern, welche Angebote sich Besucher ihrer Seite ansehen. Schon gar nicht brauchen sie die entsprechenden Daten an Dritte weiterzugeben. Gleichwohl lassen sich zahlreiche Onlinehändler genau diese Genehmigung „freiwillig“ einräumen, wenn der Nutzer zum ersten Mal einen Kauf tätigt. Einige dieser Anbieter haben zweifellos eine marktbeherrschende Stellung, datenschutzfreundliche Alternativen stehen häufig nicht zur Verfügung.*

*Noch bedenklicher sieht es bei vielen sozialen Netzwerken aus. Dass diese personenbezogene Daten der Nutzer erheben, liegt zunächst in der Natur der Sache – der Wunsch, persönlich identifizierbar zu sein, liegt der Nutzung eines solchen Angebots schließlich zugrunde. Gleichwohl verlangen zahlreiche Soziale Netzwerke ihren Kunden aber auch eine Einwilligung in die Weitergabe solcher Daten an Dritte ab. Stimmt der Kunde den entsprechenden Allgemeinen Geschäftsbedingungen nicht zu, kann er in der Regel das Angebot des betreffenden Netzwerks nicht nutzen. Datenschutzfreundliche Alternativen gibt es kaum, zumal*

*Nutzer unterschiedlicher Netzwerke sich aufgrund der hegemonistischen Abschottung dieser Portale gegen die Konkurrenz nur schwer untereinander vernetzen können.*

*Da manche sozialen Netzwerke zweifelsohne marktbeherrschende Unternehmen sind, kann auch hier nicht davon ausgegangen werden, dass dem Nutzer solchermaßen erzwungene Einwilligungen bei Vertragsabschluss zuzumuten sind. Die Praxis steht also klar im Widerspruch zum geltenden Recht, wird aber derzeit stillschweigend geduldet, weil die Monetarisierung der Privatsphäre der Bürgerinnen und Bürger für viele Internetunternehmen das einzige Geschäftsmodell ist. Privatwirtschaftlichen Interessen wird hier der Vorrang gegenüber Datenschutzbelangen eingeräumt.*

### 2.1.5 Einschränkungen von Grundrechten / Kollidierende Rechtsgüter

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

Jedermann hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Dieses „Recht auf informationelle Selbstbestimmung“, wie es das Bundesverfassungsgericht 1983 in seiner Entscheidung zur Volkszählung, also im Hinblick auf eine staatliche Maßnahme,

beschrieben hat, ist einerseits - als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG – ein individuelles Abwehrrecht gegenüber staatlichen Eingriffen.

Nach der Rechtsprechung des Bundesverfassungsgerichts wirkt sich das Recht auf informationelle Selbstbestimmung aber darüberhinaus im Sinne einer Drittwirkung auch auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus und begründet staatliche Schutzpflichten. Die staatliche Gewalt ist danach verpflichtet, dem Einzelnen seine informationelle Selbstbestimmung im Verhältnis zu Dritten zu ermöglichen. [Fußnote: BVerG, Beschluss vom 23.10.2006 – BvR 2027//02, Rn 30.]Gegebenenfalls müssen staatlicherseits die rechtlichen Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an Kommunikationsprozessen teilnehmen kann. [Fußnote: BVerG, Beschluss vom 23.10.2006 – BvR 2027//02, Rn. 33.]

Nicht jede Beeinträchtigung eines grundrechtlichen Schutzbereichs führt per se zur Verfassungswidrigkeit der Maßnahme. Zum einen kann der Betroffene in die Maßnahme einwilligen und seine Daten freiwillig preisgeben, was vom Staat zu respektieren ist. [Fußnote: Vgl. BVerfG-K, 1 BvR 2027/02 vom 23.10.2006, Absatz-Nr. 34, http://www.bverfg.de/entscheidungen/rk20061023_1bvr202702.html; *Schoch*, JURA 2008. 352, 357.] Aber auch ohne Einwilligung wird der verfassungsrechtliche Datenschutz nicht grenzenlos gewährleistet, sondern kann beschränkt werden. Das Bundesverfassungsgericht hat hierzu bereits 1983 im sogenannten Volkszählungsurteil dargelegt: ″Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts

auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig."

Für diese Schrankenziehung hat das BVerfG seit dem Volkszählungsurteil eine Reihe von Vorgaben aufgestellt, die es zu beachten gilt. Dabei gelten für die genannten Grundrechte weitgehend die gleichen Maßstäbe. [Fußnote: Vgl. BVerfGE 115, 320, 347; *Gurlit*, NJW 2010, 1035, 1037 f.]

Grundlegende Voraussetzung für einen zulässigen Eingriff in das Recht auf informationelle Selbstbestimmung ist das Vorhandensein einer gesetzlichen Grundlage, welche die Voraussetzungen und den Umfang der Beschränkungen klar erkennen lässt. [Fußnote: BVerfGE 65, 1, 44.] Das Erfordernis einer gesetzlichen Grundlage (Gesetzesvorbehalt) folgt bereits aus Art. 2 Abs. 1 GG, wonach das allgemeine Persönlichkeitsrecht nur innerhalb der verfassungsmäßigen Ordnung gewährleistet wird. Die gesetzliche Grundlage muss dem Gebot der Normenklarheit entsprechen, was bedeutet, dass Anlass, Zweck und Grenzen eines Eingriffs in der Ermächtigung bereichsspezifisch, präzise und für den Bürger klar erkennbar festgelegt werden müssen. [Fußnote: *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 79 m.w.N. aus der Rspr. des BVerfG.]

Weiterhin muss der Verhältnismäßigkeitsgrundsatz beachtet werden. Das bedeutet, dass die Maßnahme einen legitimen Zweck verfolgen, zu dessen Erreichung geeignet, erforderlich und verhältnismäßig sein muss. [Fußnote: BVerfGE 115, 320, 345 ff.] Der Zweck muss von vornherein bestimmt sein. Die ständige Rechtsprechung des BVerfG bringt deutlich zum Ausdruck, „dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist.“ [Fußnote: BVerfG NJW 2010, 833, 839 Rn. 213.]

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

In der Verhältnismäßigkeitsprüfung findet eine Güterabwägung zwischen dem verfolgten Zweck und dem Recht auf informationelle Selbstbestimmung statt. Dabei ist von der Prämisse auszugehen, dass Grundrechte „jeweils nur soweit beschränkt werden dürfen, als es zum Schutze öffentlicher Interessen unerlässlich ist.“ [Fußnote: BVerfGE 65, 1, 44.] In der Abwägung ist vor allem das Gewicht der Grundrechtsbeeinträchtigung zu beachten. Bei der Beurteilung der Schwere des Eingriffs sind z.B. die folgenden Kriterien zu berücksichtigen:

- in welche Sphäre die Maßnahme eingreift (Sozial-, Privat- oder Intimsphäre). [Fußnote: In die Intimsphäre darf gar nicht eingegriffen werden, in die Privat- oder Geheimnissphäre nur unter besonders strenger Wahrung des Verhältnismäßigkeitsgrundsatzes und in die Sozialsphäre bereits nach den Kriterien, die für einen Eingriff in die allgemeine Handlungsfreiheit gelten. Vgl. *Murswiek*, in: Sachs, GG, Art. 2 Rn. 104 m.w.N.] Die unterschiedliche Schutzintensität der drei Sphären kann aber nicht im Sinne eines starren Schemas verstanden werden, sondern nur als erster Orientierungspunkt für die Intensität der Grundrechtsbeeinträchtigung und für die Gewichtung der diese Beeinträchtigung rechtfertigenden Gründe.

- wie viele Grundrechtsträger betroffen sind; [Fußnote: BVerfGE 115, 320, 347.]
- wie intensiv die Beeinträchtigungen sind; [Fußnote: BVerfGE 115, 320, 347.]
- welche Inhalte von dem Eingriff erfasst werden, insbesondere welchen Grad an Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen; [Fußnote: BVerfGE 115, 320, 348.]
- ob besondere Vertraulichkeitserwartungen verletzt werden; [Fußnote: BVerfGE 115, 320, 348.]
- auf welchem Weg die Inhalte erlangt werden; [Fußnote: BVerfGE 115, 320, 348.]
- welche weiteren Folgen oder Nachteile die Datenerhebung nach sich ziehen kann, z.B.
    - das Risiko, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht-ausgesetzt zu werden,
    - eine stigmatisierende Wirkung; [Fußnote: BVerfGE 115, 320, 351 ff.]
- die Heimlichkeit einer staatlichen Maßnahme, welche z.B. die Möglichkeit der Inanspruchnahme von Rechtsschutz im Vergleich zur offenen Datenerhebung wesentlich erschwert; [Fußnote: Vgl. z.B. BVerfGE 120, 274, 325; 124, 43, 62 f. und 65 f.]
- der Verdachtsgrad;

- über welchen Zeitraum die Daten erhoben, verarbeitet und genutzt werden können;

- und die Streubreite einer Maßnahme.

Zum zuletzt genannten Punkt hat das BVerfG ausgeführt: „Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben – weisen grundsätzlich eine hohe Eingriffsintensität auf…. Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat. Von solchen Eingriffen können ferner Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können. … Es gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen … .“ [Fußnote: BVerfGE 115, 320, 354 f.]

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

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

- die Sicherheit des Staates als verfasste Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit;[ Fußnote: BVerfGE 120, 274, 319 und 328.]

- die Abwehr von Beeinträchtigungen der Grundlagen einer freiheitlichen demokratischen Grundordnung; [Fußnote: BVerfGE 115, 320, 358.]

- die Sicherung der Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen; [Fußnote: BVerfGE 120, 274, 328.]

- die Verhütung und Verfolgung von Straftaten von erheblicher Bedeutung [Fußnote: BVerfGE 113, 348, 385.]bzw. schwerwiegender Straftaten. [Fußnote: BVerfG NJW 2010, 833, 848 Rn. 279.]

Eine absolute Grenze der Zulässigkeit einer Datenerhebung bildet die Schranken-Schranke des unantastbaren Kernbereichs privater Lebensgestaltung, insbesondere im Bereich der Intimsphäre. Staatliche Stellen „haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt. … Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen … Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.“ [Fußnote: BVerfGE 120, 274, 335.] Deshalb hat das BVerfG als Voraussetzung für einen Zugriff auf einen Bereich, in dem solche Kernbereichsdaten (z.B. tagebuchartige Aufzeichnungen, private Film- oder Tondokumente, höchstpersönliche Telefonate oder Emails) zu vermuten sind, das

Erfordernis besonderer gesetzlicher Vorkehrungen aufgestellt, um den Kernbereich der privaten Lebensgestaltung zu schützen. [Fußnote: BVerfGE 120, 274, 336 ff.]So lässt sich die (beiläufige) Erfassung solcher Daten nicht immer verhindern. Jedoch sind entsprechende Maßnahmen abzubrechen, sobald erkannt wird, dass sie in den Kernbereich vordringen oder zumindest im Nachhinein umgehend zu löschen. [Fußnote: BVerfGE 120, 274, 337.]

Aber auch unabhängig von diesem Kernbereich hat der Gesetzgeber „organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.“ [Fußnote: BVerfGE 65, 1, 44.] Dazu gehört auch die Sicherheit der Daten. So hat das BVerfG in seiner Entscheidung zur Vorratsdatenspeicherung vor allem die „gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit“ eingefordert. [Fußnote: BVerfG NJW 2010, 833, 840 Rn. 221.]

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

### 2.1.6 Anonymität und Identitätsmanagement in Internet

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

Technische Möglichkeiten zur Anonymisierung helfen Nutzerinnen und Nutzern des Internets, ihr Recht auf informationelle Selbstbestimmung wirksam ausüben zu können. Sie sind daher auch weiterhin als ein Instrument des Selbstdatenschutzes zu fördern.

Die Wahrung der Anonymität gehört in der analogen Welt zu einem selbstbestimmten Leben. Diese Möglichkeit muss auch im Internet gelten.

Anders als in der analogen Welt fallen hier aber personenbezogene Daten systembedingt an. Die Erhebung und Verwendung muss dennoch auf ein Mindestmaß beschränkt werden.

*Maßnahmen wie die vorerst gescheiterte Vorratsdatenspeicherung, bei der sämtliche Bewegungen und Kontakte der Nutzer automatisch aufgezeichnet und gespeichert werden, stellen*

Absatz streitig

*unverhältnismäßige Eingriffe in deren Privatsphäre dar und stehen im Widerspruch zu ihrem Recht auf Anonymität. Auch Netzwerkmanagementmaßnahmen, etwa mit Hilfe von Deep-Packet-Inspection, bei der die von Nutzern gesendeten und empfangenen Inhalte durchleuchtet werden, sind mit einem Recht auf Anonymität nicht vereinbar.*

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

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

streitig

*Während jedoch im Bundesdatenschutzgesetz für die Erhebung von Daten grundsätzlich eine freiwillige Einwilligung des Betroffenen vorgesehen ist, erlaubt das Telemediengesetz eine Erhebung und Verwendung von Nutzerdaten, „soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien ermöglichen und abzurechnen.“ Insofern dies eine Identifikation des Nutzers voraussetzt, ist hier eine anonyme Nutzung nicht möglich.*

bis Z. 1008: alternativer Textvorschlag zu Z. 970-974

*Allerdings dürfen diese Nutzungsdaten ohne Einwilligung nicht zu anderen als zu Abrechnungszwecken verwendet werden. Insbesondere dürfen sie nicht mit Nutzungsprofilen verknüpft werden, welche der Diensteanbieter vorbehaltlich eines Widerspruchs des Nutzers „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der*

*Telemedien“ auch dann erstellen darf, wenn der Nutzer ein Pseudonym verwendet. Vielmehr ist die Erstellung von Nutzungsprofilen nur unter der Voraussetzung erlaubt, dass diese „nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.“*

*Personenbezogene Daten dürfen nach dem Telemediengesetz nicht ohne Einwilligung des Betroffenen erhoben werden. Auch kann die Erhebung solcher Daten nicht allein mit der Notwendigkeit einer Abrechnung gerechtfertigt werden, da Diensteanbieter verpflichtet sind, „die Nutzung von Telemedien und ihre Bezahlung anonym und unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“ und den Nutzer über diese Möglichkeit zu informieren.*

*Anonyme Nutzung und die Verwendung von Pseudonymen sind also grundsätzlich durch das Telemediengesetz geschützt. Gleichwohl wird diskutiert, ob angesichts der grundsätzlichen Personenbeziehbarkeit von Nutzungsprofilen, die eine Folge der technischen Entwicklung ist, eine stärkere gesetzliche Normierung der Vorschriften zur Profilbildung nötig ist. Das Bundesdatenschutzgesetz weist in dieser Hinsicht eine Schutzlücke auf.*

### 2.1.7 Sicherheit von Daten/Technischer Datenschutz

Die Entscheidungen des BVerfG zur Online-Durchsuchung (vom 27. Februar 2008 1 BvR 370/07) sowie zur Vorratsdatenspeicherung (vom 2. März 2010 – 1 BvR 256/08) unterstreichen die gewachsene Bedeutung der Datensicherheit als einem wesentlichen Element des Datenschutzes.

Datensicherheit muss die mit der zunehmenden Vernetzung und Digitalisierung gewachsene Zugänglichkeit personenbezogener

Daten und die damit verbundenen Risiken einfangen. Konzeptionell konzentriert sich die Diskussion auf präventiv angelegte und flexible Datensicherheitskonzepte unter Formulierung abstrakter Schutzziele.

Beim technischen Datenschutz ist auf eine technikneutrale Ausgestaltung von gesetzlichen Regelungen zu achten. Ein geeignetes Vorgehen kann hier die Formulierung von Schutzzielen darstellen, wie es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihren Eckpunkten für ein „Modernes Datenschutzrecht für das 21. Jahrhundert“ fordern.

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

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

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

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

### 2.1.8 Selbstdatenschutz und Medienkompetenz

Die Stärkung allein des Datenschutzbewusstseins ist von der Stärkung der Medienkompetenz, zu der auch die Datenschutzkompentenz zu zählen wäre, zu unterscheiden. Nutzer sind oft beim Umgang mit eigenen Daten nicht umsichtig genug. Einerseits erkennen sie nicht, dass personenbezogene Daten überhaupt anfallen. Andererseits erkennen sie aber auch nicht die Reichweite und die möglichen Folgen der Sammlung und Verarbeitung der angegebenen personenbezogenen Daten. Sie müssen dies aber erkennen, um bewusst mit ihren Daten umzugehen.

Text streitig

*Daher muss den Nutzern sowohl das praktische und technische Verständnis für einen sorgfältigen Umgang mit den eigenen personenbezogenen Daten (z. B. auch deren Schutz vor unerwünschtem Zugriff oder Weitergabe) als auch die Fähigkeit, mögliche Folgen und Konsequenzen der Nutzung entsprechender Angebote zu erkennen, vermittelt werden. Dies hilft nicht nur datenschutzrechtliche Risiken für den Einzelnen zu minimieren, sondern eröffnet zugleich auch die Chance, sein Recht auf informationelle Selbstbestimmung bewusst auszuüben. Neben anderen Voraussetzungen ermöglicht die Kenntnis der Prozesse der*

*Datenverarbeitung einen eigenverantwortlichen Umgang mit den Daten.*

*Eine Stärkung des Selbstdatenschutzes kann eine Ergänzung zu, aber kein Ersatz von gesetzlichen Datenschutzregeln darstellen. Vor dem Hintergrund der Schwierigkeiten mit der Entwicklung international gültiger Datenschutzstandards gewinnt der Selbstdatenschutz auch weiter an Bedeutung.*

*Allerdings kann die Förderung eines selbstbewussten Umgangs mit den eigenen Daten nicht als Alternative zu gesetzlichem Datenschutz begriffen werden. Im Gegenteil, je weniger offensichtlich für den einzelnen Bürger erkennbar ist, dass Daten von ihm erhoben, womöglich gar im Hintergrund verknüpft werden, desto mehr ist der Gesetzgeber in der Pflicht, mit klaren Normierungen dafür zu sorgen, dass das Recht auf informationelle Selbstbestimmung keine Leerformel bleibt. Die Anbieter, die auf elektronischem Wege Daten erheben, um diese zu monetarisieren, haben naturgemäß kein Interesse daran, in transparenter Weise darzustellen, zu welchen Zwecken Daten erhoben und genutzt werden, weil sie dann riskieren würden, dass datenschutzbewusste Nutzer zu konkurrierenden Angeboten wechseln würden. Das Ziel, es Nutzern zu ermöglichen, möglichst kompetent, informiert und selbstverantwortlich mit ihren Daten umzugehen, steht also in einem direkten Widerspruch zum Geschäftsmodell der meisten Anbieter. Mehr Datenschutz- und Medienkompetenz auf Seiten der Nutzer zu fordern, darf für den Gesetzgeber deshalb nicht die Alternative zu klaren Regelungen sein, durch die die Anbieter einerseits zu Transparenz, andererseits zur Einhaltung geltender datenschutzrechtlicher Bestimmungen gezwungen werden. Auch dürfen Schwierigkeiten bei der Durchsetzung von Datenschutz im internationalen Kontext kein Vorwand dafür sein, auf datenschutzrechtliche Neugestaltung zu verzichten und stattdessen*

Alternativer Textvorschlag zu vorstehender Textpassage, streitig

*auf die Eigenverantwortlichkeit der Nutzer zu verweisen. Die Förderung der Kompetenz zum Selbstdatenschutz kann vielmehr stets nur eine Ergänzung zu datenschutzrechtlichen Regeln sein, die den Spielraum jener Unternehmen, deren Geschäftsmodelle auf Datenhandel basieren, auf ein zivilgesellschaftlich verträgliches Maß reduzieren.*

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

### 2.1.9 Die Grenzen des nationalen Datenschutzes

Die Regeln der Datenerhebung und –verarbeitung bei Dienstleistungen, die sich an Bürger der Europäischen Union wenden, bestimmen sich nach dem europäischen oder darüber hinausgehenden nationalen Recht. Die Richtlinie 95/46/EG (Datenschutzrichtlinie) verbietet es grundsätzlich, personenbezogene Daten aus EG-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EG-Recht vergleichbares Datenschutzniveau verfügen. Sie stellt allerdings eine Anzahl von Instrumenten zur Verfügung, die ein angemessenes Datenschutzniveau bei der Datenübermittlung in Drittstaaten sicherstellen sollen. Gegenwärtig erfolgt eine grundlegende Revision der Datenschutzrichtlinie, die auf Verbesserungen des Datenschutzes auch in diesem Bereich abzielt.

Die seit 2000 existierende Vereinbarung „Safe Harbor“ soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten.

In einem Beschluss vom April 2010 hat der Düsseldorfer Kreis die Anforderungen an die Nachweise und auch an deutsche

Unternehmen, die an nicht-EU Unternehmen Daten übermitteln, verstärkt. [Fußnote: „Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US- Unternehmen übermitteln.“]

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

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

Gegenwärtig gilt nach dem Bundesdatenschutzgesetz das Sitzlandprinzip. Danach kommt dasjenige Recht zur Anwendung, das am Sitz des für die Entscheidung über die Datenverarbeitung Verantwortlichen gilt. Damit wird ein harmonisierter EWR-Rechtsraum begründet. Eine Ausnahme bilden Verarbeitungen, bei denen noch eine Niederlassung im Inland besteht, so dass nationales Datenschutzrecht zur Anwendung kommt. Eine weitere Ausnahme vom Sitzlandprinzip bilden Verarbeitungen, bei denen Verantwortliche außerhalb des EWR-Raumes befindlich sind. So

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

Absatz streitig

*Zudem darf die Tatsache, dass das nationale Datenschutzrecht zwar über EU-weit harmonisierte Regelungen hinausgehen kann, dann jedoch nur begrenzt anwendbar und durchsetzbar ist, nicht als Vorwand dafür missbraucht werden, eine Durchsetzung datenschutzrechtlicher Bestimmungen nicht zu forcieren. Unternehmen, die mit Angeboten auf dem deutschen Markt auftreten, müssen sich zwingend an hiesige Datenschutzvorschriften halten.*

Auf europäischer und weltweiter Ebene muss die Bundesrepublik Deutschland ihrer Verantwortung als führender Wirtschaftsnation gerecht werden und für einen ausgeprägten Datenschutz streiten.

Die Praxis global agierender Internetunternehmen erfordert ein abgestimmtes Vorgehen über die Grenzen des Nationalstaates hinaus. Bei internationalen Ausformulierungen von Datenschutzvorgaben sollte jeweils das höchste beteiligte Datenschutzniveau Grundlage sein.

### 2.1.10 Datenschutz für Kinder und Jugendliche

Abschnitt 2.1.0 streitig

*Der Datenschutz bei besonders schutzwürdigen Gruppen bedarf besonderer Aufmerksamkeit. Die neuen informationstechnischen Möglichkeiten dürfen nicht zulasten der schwächsten Glieder (etwa Kinder) unserer Gesellschaft gehen. Gleichzeitig sollen sie aber auch nicht von einer angemessenen Teilhabe an der Informationsgesellschaft ausgeschlossen sein.*

*Daten von Kindern werden in einem kaum geringeren Umfang als Daten von Erwachsenen erhoben und verarbeitet. Die Mehrzahl der Unternehmen unterscheidet hinsichtlich ihrer Internetangebote und der damit verknüpften Datenverarbeitungen nicht zwischen Erwachsenen und Kindern bzw. Jugendlichen. Auch Kinder und Jugendliche sind aktive Nutzer von Informationsdiensten und setzen diese zum Informationsaustausch ein. Selbstverständlich sind dabei auch Kinder von Geburt an ebenso wie Erwachsene Träger von Grundrechten. Dazu gehört auch das Recht auf informationelle Selbstbestimmung, so dass auch Kinder und Jugendliche Datenschutzrechte und damit grundsätzlich das Recht haben, über die Herausgabe und Verwendung ihrer personenbezogenen Daten selbst zu bestimmen. Sie wachsen bereits mit der Nutzung von digitaler Technik und der Angebotsvielfalt des Internets auf und sind damit die am besten vernetzte Altersgruppe: 98 Prozent der 10- bis 18-Jährigen nutzen mittlerweile das Internet. Dies hat eine Studie im Auftrag des Verbandes BITKOM „Jugend*

*2.0“ [Fußnote: Jugend 2.0, Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen, BITKOM, 2011] ergeben. Selbst Kinder von 10 bis 12 Jahren sind zu 96 Prozent online. Hierbei überwiegen nach den Angaben der Studie zwar die positiven Online-Erfahrungen, doch jeder dritte Jugendliche (34 Prozent) hat auch Negatives erlebt.*

*Diese Studie zeigt auch, dass das Internet für Jugendliche zwar eine herausragende Bedeutung hat, jedoch Freundschaften und Schule nicht verdrängt. Freunde, Familie und gute Noten sind wichtiger als das Netz. 98 Prozent der Jugendlichen sind ihre Freunde wichtig, 86 Prozent sagen dies vom Internetzugang. Die große Mehrheit der 10- bis 18-Jährigen verbringt mehr Zeit mit Freunden oder Hausaufgaben als im Internet. Die meisten Jugendlichen (76 Prozent) wissen bereits jetzt, das Internet sinnvoll zur Suche nach Informationen für Schule und Ausbildung einzusetzen. 64 Prozent haben nach eigenen Angaben so ihr Wissen verbessert, 38 Prozent ihre Leistungen in Schule oder Ausbildung.*

*Fast schon selbstverständlich ist für Teenager die Mitgliedschaft in Internet-Gemeinschaften. Nach der Studie sind 77 Prozent in „Communitys“ angemeldet, 74 Prozent nutzen sie aktiv. Es gibt aber auch Unterschiede nach Altersgruppen: So sind 93 Prozent der 16- bis 18-Jährigen in den Netzwerken aktiv, aber nur 42 Prozent der 10- bis 12-Jährigen. [Fußnote: Mädchen kommunizieren intensiver als Jungen. Das gilt nicht nur für Internet-Communitys, die von 82 Prozent der Mädchen aktiv genutzt werden, gegenüber 64 Prozent bei Jungen (Jugend 2.0, Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen, BITKOM, 2011, S. 26.)] SchülerVZ liegt insgesamt vor Facebook. Teenager haben in ihrer jeweils meistgenutzten Community im Durchschnitt 133 Kontakte, davon 34 „gute Freunde“. Die BITKOM-*

*Untersuchung zeigt, dass sich 58 Prozent der 10- bis 18-Jährigen mehr Datenschutz wünschen.*

*Die Studie „Jugend 2.0“ definiert somit spezielle Bedürfnisse von Kindern und Jugendlichen. Sie zeigt zudem, dass die Erfahrungen und das Wissen im Umgang mit Datenschutz und Persönlichkeitsrechten bereits mehrheitlich vorhanden sind, jedoch teilweise noch nicht ausreichend. Bei Angeboten für Kinder und Jugendliche ist daher besonders auf eine altersgerechte Information und Aufklärung über die Datenerhebung, –verarbeitung sowie mögliche Konsequenzen aus dieser zu achten. Nur so können Kinder und Jugendliche, ihre Einwilligung in die Erhebung und Verarbeitung von personenbezogenen Daten überhaupt vornehmen.*

*Unterschiedliche Alterskategorien in verschiedenen Gesetzen erschweren jedoch die Zuordnung. Abhängig von der jeweils vorhandenen Einsichtsfähigkeit sollen Regeln ausgestaltet sein. Bislang gilt, dass die gesetzlichen Vertreter des Kindes ihre Einwilligung in jede Verarbeitung der Daten des Kindes geben, bis das Kind selbst in der Lage ist, einzuwilligen.*

*Das Einwilligungsrecht geht dabei mit Zunahme der Einsichtsfähigkeit des Kindes graduell je nach der individuellen Entwicklung von den Eltern auf das Kind über. Eine gesetzliche Vorgabe gibt es hierfür nicht.*

*Anbietern von Diensten ist das Alter des Nutzers oftmals nicht klar erkennbar ist, Dies gilt insbesondere bei der - aus Datenschutzgründen wünschenswerten - anonymen Nutzung von Diensten.*

*Auch wechselnde Nutzer an einem Endgerät, wie es in Familien die Regel ist, erschweren eine klare Zuordnung zu bestimmten*

*Altersklassen. Deutliche Differenzierungen in den Schutzkonzepten erscheinen (wie z.B. im Angebot beim sozialen Netzwerk SchülerVZ) wünschenswert, um einen verbesserten Schutz zu erreichen, wenn Angebote sich vollständig oder überwiegend an Jugendliche und Kinder wenden. Gegebenenfalls. sind hier auch - entsprechend den jeweiligen Gefahren - gesetzgeberische Maßnahmen erforderlich. Unklarheiten der Auslegung des BDSG hinsichtlich der Einwilligungsfähigkeit von Jugendlichen und der damit verbundenen Anforderungen an eine wirksame Einwilligung sollten beseitigt werden. Auch eine Begrenzung der zu erhebenden Daten bzw. eine nur eingeschränkte kommerzielle Verwertung käme diesbezüglich in Betracht.*

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