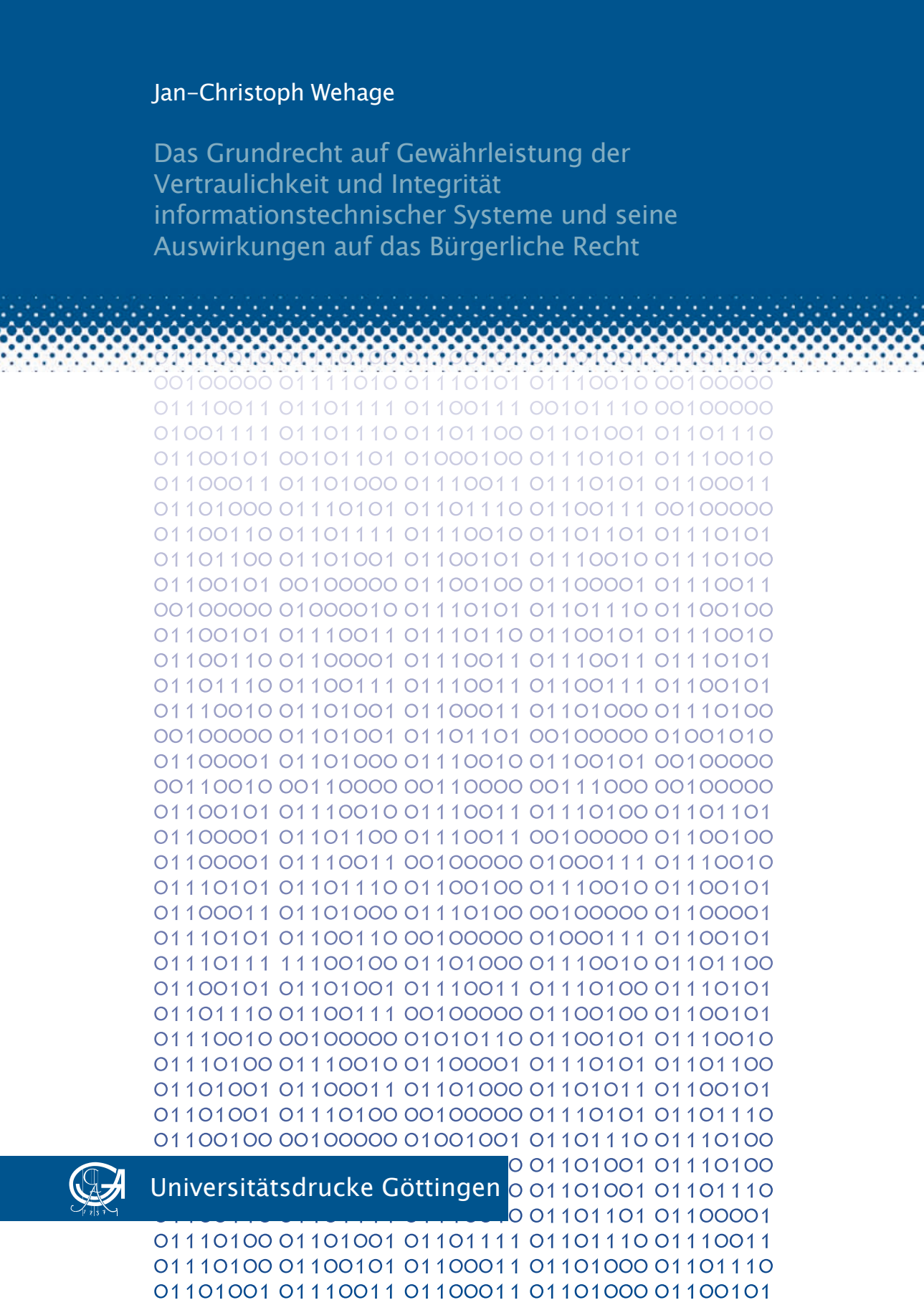
Jan-Christoph Wehage

# Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das Bürgerliche Recht



Universitätsdrucke Göttingen

Jan-Christoph Wehage

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das Bürgerliche Recht

erschienen in der Reihe der Universitätsdrucke
im Universitätsverlag Göttingen 2013

Jan-Christoph Wehage

# Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das Bürgerliche Recht

Universitätsverlag Göttingen
2013

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

*Autorenkontakt*
Jan-Christoph Wehage
e-mail: jan.wehage@gmx.de



Satz und Layout: Jan-Christoph Wehage
Umschlaggestaltung: Franziska Lorenz


http://univerlag.uni-goettingen.de
ISBN: 978-3-86395-123-8

# Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2011/2012 von der Juristischen Fakultät der Georg-August-Universität Göttingen als Dissertation angenommen. Das Manuskript wurde im Juni 2013 fertiggestellt. Soweit dies möglich und inhaltlich sinnvoll war, wurden Rechtsprechung und Literatur bis Ende 2012 berücksichtigt.

Mein Dank gilt zunächst meinem Doktorvater, Herrn Prof. Dr. Gerald Spindler, der das Thema der vorliegenden Arbeit anregte und mir während der Erstellung stets beratend zur Seite stand. Frau Prof. Dr. Christine Langenfeld danke ich für die schnelle Erstellung des Zweitgutachtens.

Besonderer und herzlicher Dank geht an meine Eltern für ihre Förderung auf meinem bisherigen Lebensweg und während der Promotion. Ihnen widme ich diese Arbeit. Caterina danke ich sowohl für zahlreiche hilfreiche Diskussionen als auch für ihre liebevolle Unterstützung. Schließlich gilt mein Dank den zahlreichen Personen aus meinem Freundes- und Kollegenkreis, die mich stets motiviert und auf vielfältige Weise zur Fertigstellung der Arbeit beigetragen haben.

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| AuR | Arbeit und Recht |
| a.F. | alte Fassung |
| a.A. | andere Ansicht |
| Abs. | Absatz |
| AcP | Archiv für die civilistische Praxis |
| AEUV | Vertrag über die Arbeitsweise der europäischen Union |
| AGB | Allgemeine Geschäftsbedingungen |
| Anm. | Anmerkung |
| AnwBl | Anwaltsblatt |
| AöR | Archiv des öffentlichen Rechts |
| Aufl. | Auflage |
| BB | Betriebs-Berater |
| BDSG | Bundesdatenschutzgesetz |
| BGB | Bürgerliches Gesetzbuch |
| BGBl. | Bundesgesetzblatt |
| BGH | Bundesgerichtshof |
| BGHZ | Entscheidungen des Bundesgerichtshofs in Zivilsachen |
| BKAG | Bundeskriminalamtgesetz |
| BMI | Bundesministerium des Innern |
| BMJ | Bundesministerium der Justiz |
| BR-Drucks. | Bundesratsdrucksache |

| | |
|---|---|
| BSIG | Gesetz über das Bundesamt für Sicherheit in der Informationstechnik |
| BT-Drucks. | Bundestagsdrucksache |
| BVerfG | Bundesverfassungsgericht |
| BVerfGE | Entscheidungen des Bundesverfassungsgerichts |
| BVerfGG | Bundesverfassungsgerichtsgesetz |
| bzw. | beziehungsweise |
| CCC | Chaos Computer Club |
| CR | Computer und Recht |
| d.h. | das heißt |
| ders. | derselbe |
| DÖV | Die öffentliche Verwaltung |
| DRiZ | Deutsche Richterzeitung |
| DuD | Datenschutz und Datensicherheit |
| DVBl | Deutsche Verwaltungsblätter |
| EG | Europäischen Gemeinschaften |
| EuGH | Europäischer Gerichtshof |
| EuGRZ | Europäische Grundrechte-Zeitschrift |
| EUV | Vertrag über die Europäische Union |
| EuZW | Europäische Zeitschrift für Wirtschaftsrecht |
| FAS | Frankfurter Allgemeine Sonntagszeitung |
| FAZ | Frankfurter Allgemeine Zeitung |
| Fn. | Fußnote |
| GA | Goltdammer's Archiv für Strafrecht |
| GG | Grundgesetz |
| GS | Gedächtnisschrift |
| EL | Ergänzungslieferung |
| FS | Festschrift |
| GRUR | Gewerblicher Rechtsschutz und Urheberrecht |
| HRRS | Onlinezeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht |
| Hrsg. | Herausgeber |
| i.V.m. | in Verbindung mit |
| i.d.S. | in diesem Sinne |
| i.S.d. | im Sinne des/der |
| ITRB | IT-Rechtsberater |
| JA | Juristische Arbeitsblätter |
| JR | Juristische Rundschau |
| juris PR-ITR | juris PraxisReport IT-Recht |
| JuS | Juristische Schulung |
| JZ | Juristenzeitung |
| K&R | Kommunikation und Recht |

| | |
|---|---|
| KritV | Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft |
| MMR | Multimedia und Recht |
| m.w.N. | mit weiteren Nachweisen |
| nds. VBL | niedersächsische Verwaltungsblätter |
| n.F. | neue Fassung |
| NJOZ | Neue juristische Online-Zeitschrift |
| NJW | Neue Juristische Wochenschrift |
| NVwZ | Neue Zeitschrift für Verwaltungsrecht |
| OLG | Oberlandesgericht |
| RDV | Recht der Datenverarbeitung |
| RGZ | Entscheidungen des Reichsgerichts in Zivilsachen |
| Rn. | Randnummer |
| RuP | Recht und Politik |
| StPO | Strafprozessordnung |
| StraFO | Strafverteidiger-Forum |
| StV | Strafverteidiger |
| SZ | Süddeutsche Zeitung |
| TKG | Telekommunikationsgesetz |
| u.a. | und andere |
| UWG | Gesetz gegen den unlauteren Wettbewerb |
| VersR | Versicherungsrecht |
| vgl. | vergleiche |
| VuR | Verbraucher und Recht |
| WRP | Wettbewerb in Recht und Praxis |
| ZD | Zeitschrift für Datenschutz |
| ZRP | Zeitschrift für Rechtspolitik |

# Einleitung und Problemstellung

## A. Hintergrund

„*Das allgemeine Persönlichkeitsrecht (Art.2 Abs. 1 i. V. m. Art. 1 Abs.1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.*“

Der erste Leitsatz des Urteils des *Bundesverfassungsgerichts* (BVerfG) vom 27. Februar 2008[1] ließ den eigentlichen Gegenstand der zugrundeliegenden Verfassungsbeschwerden in den Hintergrund treten. Das Gericht hielt letztere nicht nur für weitgehend begründet und stellte die Nichtigkeit des § 5 Abs. 2 Nr. 11 des *Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen* (VSG NRW 2007)[2] fest. Es hatte darüber hinaus in den Urteilsgründen eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG benannt: Das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Gegenstand der Verfassungsbeschwerden in den Verfahren 1 BvR 370/07 und 1 BvR 595/07 waren einzelne Vorschriften des VSG NRW 2007. Nach § 5 Abs. 2 Nr. 11 VSG NRW 2007 stand dem nordrhein-westfälischen Innenministerium als Verfassungsschutzbehörde zur Informationsbeschaffung als nachrichten-

[1] *BVerfG*, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07 = *BVerfGE* 120, 274.

[2] *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen* in der Fassung des Gesetzes vom 20.12.2006 (Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen, S. 620).

dienstliches Mittel u.a. auch „der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel“ zur Verfügung. Die Norm enthielt damit die erste und bis dahin einzige ausdrückliche Ermächtigung einer staatlichen Behörde zu der sog. *Online-Durchsuchung*.[3] Das *BVerfG* stellte hierzu fest:[4]

> „*§ 5 Abs.2 Nr. 11 S. 1 Alt. 2 VSG, der den heimlichen Zugriff auf informationstechnische Systeme regelt, verletzt das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Diese Ausprägung des allgemeinen Persönlichkeitsrechts 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.*“

Die darin zum Ausdruck kommende lückenschließende Gewährleistung des allgemeinen Persönlichkeitsrechts begründete das *BVerfG* wie folgt:

> „*Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit. Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.*“[5]

Aus der zunehmenden Verbreitung vernetzter informationstechnischer Systeme würden jedoch nicht nur neue Möglichkeiten der Persönlichkeitsentfaltung, sondern auch neue Persönlichkeitsgefährdungen folgen:

> „*Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind.* […] *In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden.*

---

[3] Eine entsprechende Ermächtigung zum verdeckten Eingriff in informationstechnische Systeme enthält seit dem 1.1.2009 auch § 20k des *Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Artikel 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten)* (*Bundeskriminalamtgesetz* vom 7.7.1997 (BGBl. I S. 1650), zuletzt geändert durch Art. 3 des Gesetzes vom 21.7.2012 (BGBl. I S. 1566) (BKAG); erneut sind wiederum gegen diese und weitere Bestimmungen des BKAG in der Fassung vom 31.12.2008 (BGBl. I S. 3083), mit denen dem *Bundeskriminalamt* Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus eingeräumt werden, bei dem *BVerfG* als Verfahren BvR 966/09, 1 BvR 1140/09 Verfassungsbeschwerden anhängig.

[4] *BVerfGE* 120, 274 (302).

[5] *BVerfGE* 120, 274 (303).

> *Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen.*“[6]

Das aus diesen Gefährdungen folgende Schutzbedürfnis für den Einzelnen schlägt sich sodann in der Formulierung des Schutzbereichs der weiteren Ausprägung des allgemeinen Persönlichkeitsrechts nieder[7]:

> „*Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen*“.

Dem Urteil folgte in den Allgemeinmedien eine umfassende Diskussion der Entscheidung und ihrer möglichen Folgen. Zahlreiche Publikationen berichteten über das „neue“ Grundrecht. Die Bezeichnungen „Computergrundrecht“ oder „IT-Grundrecht“ schienen dabei griffiger als die von dem *BVerfG* gewählte Bezeichnung. Der Diskussion war insgesamt Zuspruch für das Urteil zu entnehmen. Die *Frankfurter Allgemeine Zeitung* sprach von einem „neuen Grundrecht auf der Höhe der Zeit“.[8] Der *Chaos Computer Club* begeisterte sich für ein neues Grundrecht auf digitale Intimsphäre, das er seit über 25 Jahren gefordert habe.[9] *Der Spiegel* stellte fest, dass die Richter des *BVerfG* „das Grundgesetz ins Informationszeitalter katapultiert“ hätten.[10] Die juristische Fachliteratur hingegen nahm das Urteil deutlich differenzierter auf. Ein überwiegender Zuspruch ließ sich allenfalls hinsichtlich des Schutzumfangs des Grundrechts[11] feststellen. Dogmatische Herleitung und Begründungszusammenhang wurden hingegen teils deutlich kritisiert. Dies gilt insbesondere für das Verhältnis des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (*GVIiS*[12]) zu dem ebenfalls als Ausprägung des allgemeinen Persönlichkeitsrechts durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleisteten Recht auf informationelle Selbstbestimmung (*RiS*). Tatsächlich bleibt das Urteil an vielen Stellen unklar. So verwendet

---

[6] *BVerfGE* 120, 274 (305).

[7] *BVerfGE* 120, 274 (314).

[8] *FAZ* v. 28.2.2008 (abrufbar unter: http://www.faz.net/aktuell/feuilleton/urteil-zur-online-durchsuchung-ein-neues-grundrecht-auf-der-hoehe-der-zeit-1516245.html); alle Internetquellen wurden zuletzt am 28.5.2013 abgerufen.

[9] Pressemitteilung des *CCC* Nr. CCC20080227 vom 27.2.2008.

[10] *Der Spiegel* 10/2008, „Digitales Domino“, S. 42.

[11] Kritisch zum Begriff des „Grundrechts“ etwa *Heise*, RuP 2009, 94.

[12] Abkürzung übernommen von *T. Böckenförde*, JZ 2008, 925 (927).

das Gericht für die Namensgebung der gegenständlichen Ausprägung des allgemeinen Persönlichkeitsrechts mit den Begriffen der Vertraulichkeit und Integrität zwar anerkannte Begriffe der Informationstechnik. Deren konkrete Bedeutung für den Schutzbereich gerade im Unterschied zum Verständnis der Informationstechnik wird hingegen nicht erläutert. Das *BVerfG* gibt leider nur eine eher knappe Beschreibung des mit den Begriffen umschriebenen Schutzgehalts. Ferner erhält gerade der zentrale Begriff des informationstechnischen Systems keine abstrakte Definition. Das Gericht gibt hier lediglich einzelne Beispiele technischer Umgebungen, die es als ein solches System versteht. Dies ist insbesondere dahingehend problematisch, da das informationstechnische System als Zugriffsobjekt staatlicher Überwachungsmaßnahmen schutzbereichseröffnend wirkt. Im Rahmen der Erörterung der Grundrechtskonkurrenzen fehlt es zudem an einigen Stellen an eindeutigen Formulierungen für eine klare Abgrenzung der einzelnen Schutzbereiche.

War die Aufmerksamkeit bei Verkündung des gegenständlichen Urteils im Februar 2008 noch enorm, fand das *GVIiS* in den Folgejahren in der Rechtsprechung nur in Einzelfällen und am Rande Erwähnung. Seit dem Urteil des *BVerfG* wird das *GVIiS* bei informations- und datenschutzrechtlichen Fragen zwar regelmäßig in einer Grundrechtstrias mit dem Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG und dem *RiS* genannt. Seine genauen Inhalte blieben aber weiterhin größtenteils unklar. In den allgemeinen Blickpunkt rückte es erst wieder mit der Diskussion um den sog. *Staatstrojaner*.[13]

[13] Siehe hierzu *Skistims/Roßnagel*, ZD 2012, 3, auf der Grundlage einer technischen Analyse der Software durch den *CCC* (abrufbar unter: http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf); die Autoren stellen dabei einen Eingriff in den Schutzbereich des *GVIiS* fest (ZD 2012, 3 (6)); siehe auch *Braun/Roggenkamp*, K&R 2011, 681 (682).

## B. Begriffliche Vorabklärung

Das *BVerfG* definierte den in § 5 Abs. 2 Nr. 11 VSG NRW 2007 vorgesehenen heimlichen Zugriff auf ein informationstechnisches System als

> „*eine technische Infiltration* […], *die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt. Die Infiltration des Zielsystems ermöglicht es, dessen Nutzung zu überwachen oder die Speichermedien durchzusehen oder gar das Zielsystem fernzusteuern*".[14]

Ein Zugriff auf ein informationstechnisches System setzt damit den Zugang zu dem System und damit die Möglichkeit der Kenntnisnahme von dort abgelegten Informationen auf einem *technisch* nicht dafür vorgesehenen Weg voraus.[15] Eine solche Kenntnisnahme liegt hingegen nicht schon in der bloßen Internetaufklärung, die neben dem heimlichen Zugriff auf informationstechnische Systeme in § 5 Abs. 2 Nr. 11 Alt. 1 VSG NRW 2007 vorgesehen war. Mit der technischen Infiltration eines informationstechnischen Systems wird zunächst derjenige Vorgang beschrieben, ein bestimmtes informationstechnisches Systems so zu kompromittieren, dass Dritten über eine Software der unkörperliche Zugang zu dem System ermöglicht wird.[16] Die Informationskanäle, die in einem informationstechnischen System potentiell auftreten, werden u.a. in legitime und verdeckte Kanäle aufgeteilt.[17] Legitim sind diejenigen Kanäle, die ein Subjekt[18] i.d.R. für den Informationsaustausch nutzt, verdeckte Kanäle solche, die nicht für einen Informationstransfer vorgesehen sind, aber dazu missbraucht werden können.[19] Eine zur Infiltration eines informationstechnischen Systems eingesetzte Software kann über einen derartigen (verdeckten) Eingabekanal Handlungsanweisungen empfangen,

---

[14] *BVerfGE* 120, 274 (276); der Begriff der *Online-Durchsuchung* wurde in der Folge von dem *Bundesministerium des Innern* allgemein definiert als „die verdeckte Suche unter Einsatz elektronischer Mittel nach verfahrensrelevanten Inhalten auf informationstechnischen Systemen […], die sich nicht im direkten physikalischen Zugriff der Sicherheitsbehörden befinden, aber über Kommunikationsnetze erreichbar sind" (Antwort des *BMI* vom 22.8.2007 auf den Fragenkatalog des *Bundesministeriums der Justiz* zu den vorgesehenen Tätigkeiten des Bundeskriminalamts im Rahmen seiner Präventivbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus, S. 2 (abrufbar unter http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf); weitere Definitionen bei *BGH* MMR 2007, 237; *Hornung*, *DuD* 2007, 575; *Warntjen*, JURA 2007, 581; *Beulke/Meininghaus*, StV 2007, 60 (64); *Bizer*, DuD 2007, 640; *Schlegel*, GA 2007, 649 (650).

[15] Vgl. *BVerfGE* 120, 274 (276, 340).

[16] Vgl. *Hansen/Pfitzmann*, DRiZ 2007, 225f.

[17] *Eckert*, IT-Sicherheit, Ziff. 1.1 S. 4.

[18] Als Subjekte des informationstechnischen Systems werden seine Benutzer und alle Objekte, die im Auftrag von Benutzern im System aktiv sein können, wie z.B. Prozesse, Server und Prozeduren, bezeichnet (*Eckert*, IT-Sicherheit, Ziff. 1.1. S. 5).

[19] *Eckert*, IT-Sicherheit, Ziff. 1.1 S. 4.

die entsprechenden Daten anschließend über einen (verdeckten) Ausgabekanal versenden sowie auf dem System gespeicherte Daten manipulieren.[20]

Daneben greifen auch der ausdrücklich benannte Zugriff unter Ausnutzung einer Sicherheitslücke des informationstechnischen Systems sowie „Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben“[21] in den Schutzbereich des *GVIiS* ein. Ausgehend von der Definition des „heimlichen Zugriffs“ durch das *BVerfG* ist die letztgenannte Eingriffsmodalität dahingehend auszulegen, dass nicht schon die bloße Datenerhebung gegen oder ohne Willen des Betroffenen genügt, sondern Datenverarbeitungsvorgänge des informationstechnischen Systems gerade mit zusätzlichen *technischen* Mitteln wahrnehmbar gemacht werden. Die hierzu bestehende Vielzahl an Umsetzungen kann zunächst in zwei Gruppen aufgeteilt werden.

Es ist dabei zwischen solchen Methoden zu unterscheiden, die eine (unbewusste) Mitwirkung des Nutzers voraussetzen und solchen, die ohne Zutun des Nutzers umsetzbar sind.[22] Der ersten Gruppe wird dabei das Zusenden von Programmdateien als Anhang einer E-Mail an den Nutzer des Zielsystems zugeordnet, durch deren Öffnen der Nutzer unbemerkt die für den Zugriff des Dritten notwendige Software installiert.[23] Daneben kann der Betroffene ebenso durch den Besuch bestimmter Webseiten zur Ausführung entsprechender Installationsdateien verleitet werden.[24] Dabei wird durch eine unbemerkte Manipulation der Webseite bei deren Aufruf durch das Zielsystem das Installationsprogramm der Durchsuchungssoftware gestartet.[25] Schließlich können entsprechende Installationsdateien dem Nutzer auch mittels präparierter Datenträger gezielt zugespielt werden.[26]

[20] *Hansen/Pfitzmann*, DRiZ 2007, 225
[21] *BVerfGE* 120, 274 (315).
[22] *Hansen/Pfitzmann*, DRiZ 2007, 225 (227); *Pohl*, DuD 2007, 684 (685f.).
[23] *Hansen/Pfitzmann*, DRiZ 2007, 225 (227); *Fox*, DuD 2007, 827 (829); *Buermeyer*, HRRS 2007, 154 (164).
[24] *Hansen/Pfitzmann*, DRiZ 2007, 225 (227); *Fox*, DuD 2007, 827 (829).
[25] *Fox*, DuD 2007, 827 (829).
[26] *Hansen/Pfitzmann*, DRiZ 2007, 225 (227); *Fox*, DuD 2007, 827 (829); *Pohl*, DuD 2007, 684 (686).

Der zweiten Gruppe kann insbesondere das gezielte Ausnutzen von Sicherheitslücken, die in den Anwendungsprogrammen oder dem Betriebssystem des informationstechnischen Systems vorhanden sein können, zugeordnet werden[27]. Schließlich bleibt ist hier auch noch der körperliche Zugriff des Dritten auf das System zu nennen, um eine entsprechende Spähsoftware zu installieren.[28]

Die verschiedenen Infiltrationsmethoden allein bedeuten nicht zwangsläufig auch Unterschiede in der rechtlichen Bewertung. Das *BVerfG* beschreibt den Vorgang des technischen Zugriffs auf ein informationstechnisches Systems nicht anhand einer ganz bestimmten technischen Umsetzung dieses Zugriffs. Das Gericht argumentiert vielmehr allein von dem Erfolg der Infiltration aus. Namentlich sind dies die Möglichkeiten zur Überwachung des Zielsystems, der Durchsicht seiner Speichermedien oder der Fernsteuerung des Systems.[29] Sofern eine erfolgreiche Infiltration vorliegt, bestehen die sich daraus ergebenden Folgen für den Betroffenen unabhängig von der vorangegangenen technischen Umsetzung. Es ist dies die Persönlichkeitsgefährdung des Nutzers eines solchen informationstechnischen Systems, das allein oder in seinen technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten *kann*, „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".[30] Der folgenden Darstellung liegt daher keine bestimmte Infiltrationsmethode zugrunde, sondern die mit dem erfolgreichen Zugriff auf das System verbundene Persönlichkeitsgefährdung des Nutzers, die von einer bestimmten Zugriffsmethode unabhängig ist. Eine solche Persönlichkeitsgefährdung ist dabei nicht allein auf den Zugriff gegen den Willen des berechtigten Nutzers beschränkt, sondern besteht grundsätzlich auch dann, wenn der Nutzer in den Zugriff auf sein System durch einen Dritten einwilligt.

---

[27] *Hansen/Pfitzmann*, DRiZ 2007, 225 (227); *Fox*, DuD 2007, 827 (829); *Buermeyer*, HRRS 2007, 154 (163); hinsichtlich der dabei ausgenutzten Sicherheitslücken wird zwischen sog. *Zero-Day-Exploits* und sog. *Less-Than-Zero-Day-Exploits* unterschieden (hierzu etwa *Pohl*, DuD 2007, 684 (685)). Ein Exploit ist der Angriff auf Schwachstellen in informationstechnischen Systemen zur Ausnutzung dieser Schwachstellen (*Eckert*, IT-Sicherheit, S. 22 Ziff. 1.3.2). Bei Zero-Day-Exploits sind solche Sicherheitslücken bereits veröffentlicht, so dass ein Angriff in der Regel nur noch am Tag der Veröffentlichung („Zero Day") gestartet wird. Less-Than-Zero-Day-Exploits hingegen nutzen nicht veröffentlichte Sicherheitslücken aus und sind und auch dem Hersteller der Software noch nicht bekannt.

[28] *Hansen/Pfitzmann*, DRiZ 2007, 225 (227); *Fox*, DuD 2007, 827 (829); *Pohl*, DuD 2007, 684 (686).

[29] *BVerfGE* 120, 274 (276).

[30] *BVerfGE* 120, 274 (314).

## C. Gang der Untersuchung

Es wird zunächst umfassend das neu formulierte *GVIiS* betrachtet (Kapitel 1), um den sachlichen Schutzbereich dieses Grundrechts zu bestimmen, der dessen etwaige privatrechtliche Wirkungen vorgeben wird. Hierbei wird mangels weiterer spezifischer Rechtsprechung maßgeblich auf die Ausführungen aus dem eingangs erwähnten Urteil des *BVerfG* zurückgegriffen. Inwieweit diese Ausführungen den Inhalt des *GVIiS* vorgeben, richtet sich nach der Reichweite der Bindungswirkung von Entscheidungen des *BVerfG* gem. § 31 BVerfGG. Zum besseren Verständnis werden entscheidende Ausführungen des Urteils wörtlich zitiert. Den dogmatischen Grundlagen der Entscheidung folgt die Darstellung des *GVIiS* anhand des klassischen Aufbaus von Schutzbereich, Eingriff und Verfassungsmäßigkeit des Eingriffs. Diese Darstellung umfasst das Konkurrenzverhältnis insbesondere zu den speziellen Freiheitsrechten und beinhaltet auch die Frage nach der Anwendbarkeit des *GVIiS* auf juristische Personen. Schließlich erfolgt im Rahmen des sachlichen Schutzbereichs noch eine kurze Prüfung der Anwendbarkeit des Entwurfs der Europäischen Kommission einer Datenschutz-Grundverordnung[31] (DS-GVO-E) auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme nach Maßgabe des Urteils des *BVerfG*. Der sachliche Schutzbereich des *GVIiS* wird anhand der Begriffe des informationstechnischen Systems sowie derjenigen der Vertraulichkeit und Integrität herausgearbeitet. Soweit notwendig werden dabei eigene Definitionen dieser Begriffe entwickelt. Als Ausgangspunkt dient dabei das Verständnis in der Informationstechnik. Unterschiede in der Verwendung der Begriffe durch das *BVerfG* werden herausgearbeitet.

Es schließt sich daran die Darstellung der Auswirkungen des *GVIiS* auf das Bürgerliche Recht an (Kapitel 2). Solche Auswirkungen setzen zunächst zwingend die Feststellung eines objektiv-rechtlichen Schutzgehalts des *GVIiS* voraus. Anhand der bekannten Figuren der mittelbaren Drittwirkung und der Schutzpflichten werden der de lege lata bestehende und ein u.U. de lege ferenda zu schaffender Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme auf privatrechtlicher Ebene herausgearbeitet. Hierbei wird zwischen der oben beschriebenen Infiltration des informationstechnischen Systems und der Einwilligung des Nutzers in den Zugriff unterschieden. Die Untersuchung umfasst das Schuldrecht, insb. das Recht der Allgemeinen Geschäftsbedingungen sowie das Deliktsrecht und Abwehransprüche aus § 1004 Abs. 1 BGB.

Den Abschluss der Arbeit bildet eine Schlussbetrachtung (Kapitel 3). Technische Ausführungen werden sich auf das für das Verständnis der rechtlichen Betrachtungen zwingend notwendige Maß beschränken.

---

[31] Vorschlag für eine Verordnung des *Europäischen Parlaments* und des *Rates* zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (*Datenschutz-Grundverordnung*) vom 25.1.2012, KOM (2012) 11 endgültig.

# Kapitel 1 – Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

## A. Dogmatische Grundlagen

Das *GVIiS* wurde von dem *BVerfG* als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG benannt. Es werden zunächst die dogmatischen Grundlagen des allgemeinen Persönlichkeitsrechts dargestellt und das *GVIiS* in diesen grundgesetzlichen Kontext eingeordnet. Daran schließt sich die Erörterung der Frage an, inwieweit die Entscheidungsgründe des gegenständlichen Urteils den Schutzbereich des *GVIiS* bestimmen können. Es ist dahingehend die Reichweite der Bindungswirkung von Entscheidungen des *BVerfG* gem. § 31 Abs. 1 BVerfGG zu klären.

### I. Freie Entfaltung der Persönlichkeit, Art. 2 Abs. 1 GG

Art. 2 Abs. 1 GG gewährleistet die freie Entfaltung der Persönlichkeit. Als „allgemeine Handlungsfreiheit“[32] oder „allgemeines Freiheitsrecht“[33] ist diese Gewährleistung nicht auf bestimmte Lebensbereiche beschränkt, sondern schützt

[32] *BVerfGE* 113, 88 (103); 114, 371 (383f.); 115, 97 (109).
[33] *BVerfGE* 63, 45 (60); 98, 218 (261).

„jede Form menschlichen Handelns ohne Rücksicht darauf, welches Gewicht der Betätigung für die Persönlichkeitsentfaltung zukommt".[34] Ein „besonders prägender Bezug zur Entfaltung der Individualpersönlichkeit" wird nicht verlangt.[35] Geschützt werden jedes menschliche Verhalten[36] und damit auch „banale Tätigkeiten und alltägliche Verhaltensweisen".[37] Denn die Freiheit des Einzelnen wird gerade dadurch verwirklicht, dass die Art der Entfaltung individuell bestimmt wird.[38] Daraus folgt, dass Art. 2 Abs. 1 GG ein Auffanggrundrecht[39] ist, das hinter spezielle Freiheitsgrundrechte zurücktritt, soweit deren Schutzbereiche einschlägig sind.[40] Art. 2 Abs. 1 GG kommt somit nur subsidiär zur Anwendung.[41] Sofern die speziellen Freiheitsrechte Lücken aufweisen, werden diese von Art. 2 Abs.1 GG ausgefüllt.[42]

## II. Das allgemeine Persönlichkeitsrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

### *1. Ausgestaltung und Schutzbereich*

Das allgemeine Persönlichkeitsrecht als Ergebnis richterlicher Rechtsfortbildung des *BVerfG*[43] gewährleistet „im Sinne des obersten Konstitutionsprinzips der Würde des Menschen" […] die „engere persönliche Lebenssphäre und die Erhal-

---

[34] *BVerfGE* 80, 137 (152); 90, 145 (171); 91, 335 (338); anders etwa die sog. *Persönlichkeitskerntheorie*: Danach soll das Persönlichkeitsrecht des Art. 2 Abs. 1 GG „jedem - dem Ausdruck echten Menschentums entsprechend – die Auswirkung seiner ihm vom Schöpfer verliehenen Persönlichkeit ermöglichen" (*Peters*, in: FS Laun, S. 669 (673f.)) und befinde sich somit auf einer „höheren Ebene des Kernbezirks des Persönlichen" (*Peters*, Freie Entfaltung der Persönlichkeit, 1963, S. 49).

[35] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 27.

[36] *BVerfGE* 113, 29 (45).

[37] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 27.

[38] *Lorenz*, in: BK GG, Bd. 1, Art. 2 Rn. 40.

[39] Rechtstechnisch mag die Bezeichnung als Auffanggrundrecht vielfach gerechtfertigt sein, es wird damit aber der hohe Rang des allgemeinen Freiheitsrechts unterschlagen, so dass die Bezeichnung der materiellen Bedeutung des Art. 2 Abs. 1 GG im Wertsystem der Grundrechte nicht gerecht wird (*Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 7). Seine Bezeichnung als Auffanggrundrecht darf daher nicht als abschätzig missverstanden werden (*Dreier*, in. *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 30); kritisch zu dieser Einordnung („Beliebigkeitsfreiheit") *Vesting*, in: *Götting/Schertz/Seitz* (Hrsg.), Hdb. Persönlichkeitsrecht, § 6 Rn. 2, anders *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 20: Die Verfestigung eines Schutzprofils durch dogmatische Verfeinerung und Schaffung von Rechtsklarheit durch Fallgruppenbildung unter Berufung auf die Gewährleistung des Art. 2 Abs. 1 GG ist kein Akt kreativer Beliebigkeit.

[40] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1, Rn. 21; *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 30; *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 10; *Pieroth/Schlink*, Grundrechte, Rn. 387; *Kahl*, Schutzergänzungsfunktion, 2000, S. 2.

[41] *BVerfGE* 30, 292 (336) ; 32, 98 (107); 58, 358 (363); 67, 157 (171);89, 48 (61).

[42] *Jarass/*Pieroth, GG, Art. 2 Rn. 2; *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 10, *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 12.

[43] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 I Rn. 68; *Vesting*, in: *Götting/Schertz/Seitz* (Hrsg.), Hdb. Persönlichkeitsrecht, § 6 Rn. 1.

tung ihrer Grundbedingungen", insb. „im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen Persönlichkeit".[44] Es sichert jedem Einzelnen einen autonomen Bereich privater Lebensgestaltung, in dem er seine Individualität entwickeln und wahren kann[45] und schützt damit die „Integrität der menschlichen Person in geistig-seelischer Beziehung".[46] Das allgemeine Persönlichkeitsrecht erfasst dabei diejenigen „Elemente der Persönlichkeit, die nicht (schon) Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, aber diesen in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen".[47] Es ergänzt dabei die speziellen Freiheitsrechte aber nur insoweit, als diese keinen Schutz gewähren.[48] Das allgemeine Persönlichkeitsrecht steht hierbei selbständig neben den speziellen Freiheitsrechten.[49] Seine Ausprägungen sind jeweils anhand des zu entscheidenden Falles herauszuarbeiten.[50]

Grundlage des allgemeinen Persönlichkeitsrechts ist Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[51] Aus dieser Verbindung zweier Grundgesetznormen ergibt sich keine kumulative Anwendung,[52] sondern die Menschenwürde dient lediglich als „Interpretationsdirektive und Schutzbereichsverstärkung".[53] Art. 1 Abs. 1 GG wird nicht selbständiger Prüfungsmaßstab, sondern das hinter der Menschenwürdegarantie stehende Menschenbild zur Auslegung des Art. 2 Abs. 1 GG herangezogen.[54] Das allgemeine Persönlichkeitsrecht hebt sich demnach als „Recht auf Respektierung der geschützten Persönlichkeitsentfaltung" aufgrund des Zusammenhangs mit Art. 1 Abs. 1 GG von der allgemeinen Handlungsfreiheit ab[55] und ist ihr gegenüber lex specialis.[56] Es ergänzt als „unbenanntes Freiheitsrecht"[57] die speziellen Freiheitsrechte i.S.e. lückenschließenden Gewährleistung „insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann".[58] Bereits von der Rechtsprechung entwickelte Konkretisierungen können

---

[44] *BVerfGE* 54, 148 (153); 72, 155 (170); 79, 256 (268).
[45] *BVerfGE* 35, 202 (220); 79, 256 (268).
[46] *Starck*, in: *V. Mangoldt/Klein/Starck*, GG, Bd. 1, Art. 2 Rn. 86.
[47] *BVerfGE* 99, 185 (193); 106, 28 (39); 118, 168 (183); 120, 274 (303).
[48] *BVerfGE* 109, 279 (326).
[49] *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 138; *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 25; *Kube*, in: HStR VII³, § 148 Rn. 35.
[50] *BVerfGE* 54, 148 (153f.); 79, 256 (268).
[51] *BVerfGE* 34, 239 (245); 35, 202 (219); 65, 1 (41); 72, 155 (170); 82, 236 (269); 90, 263 (270).
[52] *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 63; *Starck*, in: *V. Mangoldt/Klein/Starck*, GG, Bd. 1, Art. 2 Rn. 89; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 30.
[53] *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 103.
[54] *Starck*, in: *V. Mangoldt/Klein/Starck*, GG, Bd. 1, Art. 2 Rn. 15; *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 68 („programmatische Leit- und Auslegungsrichtlinie").
[55] *BVerfGE* 54, 143 (153).
[56] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 64; *Kube*, in: HStR VII³, § 148 Rn. 35.
[57] *BVerfGE* 54, 148 (153).
[58] *BVerfGE* 118, 168 (183); 120, 274 (303).

daher den Inhalt des Persönlichkeitsrechts nicht abschließend umschreiben.[59] Auf der Grundlage dieser Rechtsprechung versteht das *BVerfG* das *GVIiS* als weitere Ausprägung des allgemeinen Persönlichkeitsrechts, die vor Eingriffen in informationstechnische Systeme schützt, soweit dieser Schutz nicht durch andere Grundrechte gewährleistet ist:[60]

> „*Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet*".[61]

### *2. Das Recht auf informationelle Selbstbestimmung*

Das *BVerfG* griff die Entwicklungsoffenheit des allgemeinen Persönlichkeitsrechts auch am 15. Dezember 1983 auf, um „den mit Abstand wichtigsten Beitrag der Rechtsprechung zum Datenschutz in Deutschland"[62] zu leisten. Als besondere Ausprägung des allgemeinen Persönlichkeitsrechts hat das Gericht im sog. *Volkszählungsurteil*[63] aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG das *Recht*[64] *auf informationelle Selbstbestimmung* herausgearbeitet.[65] Gegenstand des Verfahrens waren Verfassungsbeschwerden, die sich gegen das *Volkszählungsgesetz 1983*[66] richteten, das die Durchführung einer Volks- und Berufszählung mit gebäude- und wohnungsstatistischen Fragen sowie eine Zählung der nichtlandwirtschaftlichen Arbeitsstätten und Unternehmen (Arbeitsstättenzählung) vorsah (vgl. § 1 VZG 1983). §§ 2-4 VZG 1983 enthielten einen umfangreichen Katalog zu erfassender Einzelangaben der zur Auskunft verpflichteten Personen, so etwa Name, Anschrift, Geschlecht, Religionszugehörigkeit (§ 2 Nr. 1 VZG 1983). Eine auf die *Orwell'sche* Schilderung eines totalen Überwachungsstaats zurückgehende Furcht vor Gefährdungen der individuellen Freiheit durch den Daten sammelnden und verarbeitenden Staat[67] hielt auch das *BVerfG* nicht für gänzlich unbegründet, wenn es ausführt, dass die Möglichkeiten moderner Datenverarbeitung bei dem einzelnen Bürger die „Furcht

---

[59] *BVerfGE* 65, 1 (41).
[60] *BVerfGE* 120, 274 (303).
[61] *BVerfGE* 120, 274 (313).
[62] *Schaar*, Tätigkeitsbericht 2007/2008, Ziff. 15.3 S. 145.
[63] *BVerfGE* 65, 1ff.
[64] Schon in *BVerfGE* 65, 1 Leitsatz Nr. 1 („Das Grundrecht") auch als „Grundrecht" bezeichnet; beispielhaft ferner *BVerfGE* 84, 239 (280) („Grundrecht auf Datenschutz"), 103, 21 (29) („Grundrecht auf informationelle Selbstbestimmung").
[65] *BVerfGE* 65, 1 (43).
[66] *Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung* (Volkszählungsgesetz 1983) vom 25.3.1982 (BGBl I, Nr. 12, S. 369), VZG 1983.
[67] Vgl. *Hoffmann-Riem*, JZ 2008, 1009.

vor einer unkontrollierbaren Persönlichkeitserfassung“ auslösen könne.[68] Das *BVerfG* betonte erneut die Bedeutung des allgemeinen Persönlichkeitsrechts hinsichtlich der mit den modernen Entwicklungen verbundenen neuartigen Gefährdungen der menschlichen Persönlichkeit.[69] Da die bisherigen Konkretisierungen durch die Rechtsprechung den Inhalt des Persönlichkeitsrechts nicht abschließend umschrieben hätten, schützt letzteres mit dem *RiS*

> „*die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden*“. […] *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 sie weiß.*“ […] „*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.*“ […] „*Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*“[70]

Diese Befugnis sei besonders deswegen gefährdet gewesen, da mit Hilfe der automatisierten Datenverarbeitung personenbezogene Daten technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar seien. Sie könnten darüber hinaus mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann.[71] Hierbei zeigen sich deutliche Parallelen zwischen dem *Volkszählungsurteil* und der gegenständlichen Entscheidung zur sog. *Online-Durchsuchung*. Damals wie heute ist die durch das *BVerfG* vorgenommene Konkretisierung des allgemeinen Persönlichkeitsrechts Folge einer Gefährdungslage, die sich durch die technische Entwicklung stellt. War es zur Zeit des *Volkszählungsurteils* die gerade erst aufkommende Datenverarbeitung durch die Verwendung moderner Computertechnologie, so erging das Urteil des *BVerfG* zur Online-Durchsuchung in einer Zeit, in der sich der Alltag des Einzelnen dem sog. *Ubiquitous Computing*[72] immer mehr annähert.

---

[68] *BVerfGE* 65, 1 (4).
[69] *BVerfGE* 65, 1 (41).
[70] *BVerfGE* 65, 1 (42f.).
[71] *BVerfGE* 65, 1 (42).
[72] Als *Ubiquitous Computing* lässt sich eine Welt bezeichnen, in der viele Alltagsgegenstände mit Sensor-, Kommunikations- und Rechnertechnik ausgestattet sind, so dass der Mensch bei sämtlichen Tätigkeiten unbemerkt durch eine allgegenwärtige, in den Hintergrund tretende Datenverarbeitung unterstützt wird (vgl. *Roßnagel/Müller*, CR 2004, 625).

### *3. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*

Erneut verwies das *BVerfG* dabei auf die lückenschließende Gewährleistung des allgemeinen Persönlichkeitsrechts, neuartigen Gefährdungen durch den wissenschaftlich-technischen Fortschritt zu begegnen.[73] Eine solche Lücke schließe das *GVIiS* als weitere Konkretisierung des allgemeinen Persönlichkeitsrechts. Es „bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik" […].[74] Stand beim *Volkszählungsurteil* die Angst vor einer noch unbekannten und u.U. nicht kontrollierbaren Technologie im Vordergrund, so ist es heute gerade die Allgegenwärtigkeit von Informationstechnologie, auf deren Nutzung der Bürger angewiesen ist oder angewiesen zu sein glaubt, derer er sich jedenfalls aber nicht ohne Weiteres entziehen kann. Gerade die „Allgegenwärtigkeit" informationstechnischer Systeme (z.B. „Personalcomputer", „Mobiltelefone", „elektronische Terminkalender"[75]) in sämtlichen Lebensbereichen des Einzelnen und ihre Nutzung für verschiedenste Zwecke führt zur Generierung vielfältigster und umfangreicher Datenbestände durch die verwendeten Systeme und begründet dadurch die Gefahr einer Profilbildung durch einen bloß einmaligen Zugriff auf ein solches informationstechnisches System. Die Vertraulichkeit und die Integrität informationstechnischer Systeme werden daher nicht um des Systems willen gewährleistet:

> „*Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt.*"[76]

Das *GVIiS* schützt das eigene informationstechnische System deshalb und nur insoweit, als der Einzelne zur Persönlichkeitsentfaltung auf dessen Nutzung angewiesen ist und sich aus dieser Nutzung eine besondere Gefährdungslage für die Persönlichkeit des Nutzers ergibt.[77] Die Vertraulichkeit und Integrität eigener informationstechnischer Systeme werden als Grundbedingungen der Persönlichkeitsentfaltung in einer von der modernen Informationstechnik geprägten Lebensführung des Einzelnen angesehen. Der Schutz informationstechnischer Systeme geht jedoch nicht dahin, die staatliche informationstechnische Infrastruktur als solche zu schützen. Die Eröffnung des Schutzbereichs des *GVIiS* hängt vielmehr von der individuellen Nutzung des „eigenen" informationstechnischen Systems ab. Der Einzelne macht dieses System erst durch den aus der Nutzung folgenden

---

[73] *BVerfGE* 120, 274 (303).
[74] *BVerfGE* 120, 274 (313).
[75] *BVerfGE* 120, 274 (314).
[76] *BVerfGE* 120, 274 (315).
[77] *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (126).

Personenbezug zu einem schützenswerten Aspekt seiner Persönlichkeitsentfaltung.[78] Eine weitere Eingrenzung erfährt der Schutzbereich dadurch, dass nur solche Systeme erfasst werden, deren potentieller Bestand an personenbezogenen Daten, einen Einblick in wesentliche Teile der Lebensgestaltung oder ein aussagekräftiges Bild der Persönlichkeit ermöglicht.[79] Damit wird aber von vornherein ein subjektiv-rechtlicher Ausgangspunkt verfolgt und keine nachträgliche subjektive Eingrenzung eines bloß objektiv-rechtlichen Schutzes vorgenommen.[80] Ausgangspunkt der Begründung des Schutzbedarfs ist damit der Schutz der Persönlichkeitsentfaltung des Einzelnen, die sich mit der zunehmenden Verbreitung der Informationstechnik auf die Nutzung informationstechnischer Systeme verlagert. Ist der Einzelne in Folge dieser Verlagerung auf die Nutzung informationstechnischer Systems angewiesen, so müssen ihm nicht nur Schutz gegen die staatliche Einflussnahme auf die konkrete Form der Persönlichkeitsentfaltung, sondern auch Schutz gegen die Beeinträchtigung ihrer Grundbedingungen zustehen. Das *GVIiS* weist mit der Anknüpfung an das informationstechnische System zwar auch einen objektiv-rechtlichen Schutzgehalt auf. Als Ausgangspunkt des grundrechtlichen Schutzes lassen sich hingegen nur die individuellen Entfaltungsmöglichkeiten des Einzelnen – die Nutzung des informationstechnischen Systems – und die Sicherung der hierzu notwendigen Grundbedingungen ausmachen. Diese Ausrichtung wiederum ist jedoch als eine allein subjektiv-rechtliche – mangels spezieller Grundrechte – dem Schutzbereich des allgemeinen Persönlichkeitsrechts zuzuordnen[81] und steht der Entwicklung eines „apersonalen technikorientierten Grundrechts“[82] entgegen. Auf diesen an der Persönlichkeitsentfaltung des Einzelnen ausgerichteten Ansatz deutet schon der von dem *BVerfG* verwendete Datenbegriff hin. Der Begriff des personenbezogenen Datums des § 3 Abs. 1 BDSG setzt Daten mit Einzelangeben, mithin Informationen,[83] gleich. Daten werden dort nicht als gefährdungsneutrales Abstraktum geschützt. Gefährdungen der Persönlichkeit des Einzelnen ergeben sich nicht aus einem Datum selbst, sondern

---

[78] A.A. *Lepsius*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 21 (27f.): Schutz des informationstechnischen Systems als solches, unabhängig von dessen tatsächlicher individueller Inanspruchnahme; i.d.S. wohl auch *Wieczorek*, DuD 2012, 476 (477f.): Scheinbar bewusste Ausklammerung eines Schutzes, der über die reine Architektur des informationstechnischen Systems hinausgeht und auch die Persönlichkeitsrelevanz der informationsverarbeitenden Prozesse als solche anspricht.

[79] *BVerfGE* 120, 274 (314).

[80] A.A. *Lepsius*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 21 (35); nach *Ladeur*, DÖV 2009, 45 (54f.), könne mit der Herausarbeitung des *GVIiS* auch die Stärkung der objektiv-rechtlichen Dimension des *RiS* begonnen haben.

[81] So auch *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (126); *T. Böckenförde*, JZ 2008, 925 (929 mit Fn. 38); *Hoffmann-Riem*, JZ 2008, 1009, (1014 mit Fn. 62); *Hörnig*, JURA 2009, 207 (209f. mit Fn. 63).

[82] *Eifert*, NVwZ 2008, 521 (522).

[83] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 5; *Gola/Schomerus*, BDSG, § 3a Rn. 3; *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 3 Rn. 21; Taeger/Gabel-*Buchner*, § 3 BDSG Rn. 4.

aus den Informationen, die sich aus Daten gewinnen lassen.[84] Mit dem Schutz des informationstechnischen Systems werden die auf diesem System enthaltenen Informationen des Betroffenen vor dem unberechtigten Zugriff geschützt.[85]

### III. Konkretisierung im Wege richterlicher Rechtsfortbildung

Mit der Herausarbeitung des *GVIiS* als weiterer Konkretisierung des allgemeinen Persönlichkeitsrechts konnte das *BVerfG* zwangsläufig kein „neues" Grundrecht entwickeln.[86] Als Teil der rechtsprechenden Gewalt (vgl. Art. 92 Hs. 2 GG) ist es schon kein Legislativorgan. Neue Grundrechte zu schaffen ist allein dem verfassungsändernden Gesetzgeber vorbehalten und setzt die ausdrückliche Änderung und Ergänzung des Wortlauts des Grundgesetzes (Art. 79 Abs. 1 S. 1 GG) durch ein Gesetz voraus, das der Zustimmung von zwei Dritteln der Mitglieder des Bundestages und zwei Dritteln der Stimmen des Bundesrates bedarf (Art. 79 Abs. 2 GG). Wie jedem anderen Gericht fällt dem *BVerfG* aber die Aufgabe der Rechtsfindung auf der Basis des jeweiligen Prüfungsmaßstabs, der für das *BVerfG* allein das Grundgesetz ist.[87] Auch das *BVerfG* ist bei seiner Rechtsfindung den anerkannten Auslegungsregeln unterworfen.[88] So ist auch der Inhalt des Grundgesetzes nach den Kriterien der Wortbedeutung, grammatischer Konstruktion, des Bedeutungszusammenhangs, der Regelungsabsicht des historischen Gesetzgebers und objektiv-teleologischer Gesichtspunkte zu bestimmen.[89] Inbegriff der Auslegung einer Rechtsnorm sind die Beschäftigung mit neuartigen Erscheinungen und die Prüfung und Bewertung, ob diese Erscheinungen von der Norm erfasst sind.[90] Die Ergänzung der speziellen Freiheitsrechte durch das allgemeine Persönlichkeitsrecht betrifft vor allem neuartige Gefährdungen der menschlichen Persönlichkeit durch den wissenschaftlich-technischen Fortschritt und gewandelter Lebensverhältnisse. Die Herausarbeitung des *GVIiS* ist danach zunächst nur das Ergebnis einer Konkretisierung der bestehenden grundgesetzlichen Gewährleistung des allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hinsichtlich neuartiger Persönlichkeitsgefährdungen durch die moderne Informationstechnologie. Die erstmalige Erwähnung des *GVIiS* ist somit keine grundrechtliche Neuschöpfung des *BVerfG*, sondern die gefährdungsspezifische Präzisierung des Schutzbereichs des allgemeinen Persönlichkeitsrechts. Auch wenn das *GVIiS* wie auch die anderen Ausprägungen des Schutzes der Persön-

---

[84] *Schneider/Härting*, ZD 2012, 199 (200).

[85] Vgl. *Hoffmann-Riem*, JZ 2008, 1009 Fn. 2.

[86] Es ist daher zumindest missverständlich, im Zusammenhang der Entscheidung des *BVerfG* von der „Schaffung eines neuen Grundrechts" zu sprechen; so aber u.a. *Herrmann*, IT-Grundrecht, S. 25, der an anderer Stelle trotz der dogmatischen Ungenauigkeit die Bezeichnung als „neues Grundrecht" für vertretbar hält (S. 109).

[87] Siehe die enumerative Aufzählung in Art. 93 Abs. 1 GG.

[88] *Starck*, Verfassungen, S. 125.

[89] *Starck*, in: HStR VII[1], § 164 Rn. 16.

[90] *Starck*, in: HStR VII[1], § 164 Rn. 16.

lichkeit nicht im Grundrechtsteil des Grundgesetzes ausdrücklich angesprochen werden, sind sie jedenfalls in diesem fundiert.[91] Das allgemeine Persönlichkeitsrecht soll die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen gewährleisten.[92] Damit knüpft der Schutzzweck jedoch nicht an bestimmte enumerative aufgezählte Verhaltensweisen oder Gefährdungslagen des Grundrechtsberechtigten an. Der durch das allgemeine Persönlichkeitsrecht gewährleistete Schutzumfang muss dementsprechend auch unabhängig von der Bekanntheit konkreter Gefährdungen sein, nämlich sich hinsichtlich neu auftretender Persönlichkeitsgefährdungen an eben dieser Gewährleistung orientieren. Denn das allgemeine Persönlichkeitsrecht dient gerade dazu, „bestimmte, enger umgrenzte Entstehungsbedingungen freier, autonomer Individualität zu sichern".[93] Diese Bedingungen kann das allgemeine Persönlichkeitsrecht aber nur dann schaffen, wenn der gewährleistete Persönlichkeitsschutz sich an dem Individuum und eben nicht an einer bestimmten abschließend umschriebenen Gefährdungslage orientiert. Bei Verabschiedung des Grundgesetzes konnte der verfassungsgebende Gesetzgeber moderne Gefährdungslagen der Persönlichkeit zwangsläufig nicht vorhersehen. Allein aus dieser Unvorhersehbarkeit tatsächlicher Entwicklungen und der daraus folgenden Gefährdungslagen erklärt sich das Fehlen einer speziellen grundrechtlichen Regelung.[94] Deren Fehlen erschwert damit zwar die Erfassung neuartiger Bedrohungen, bedeutet aber keine bewusste Entscheidung gegen einen grundrechtlichen Schutz.[95] Vor diesem Hintergrund muss das Grundgesetz in der Lage sein, neuen Herausforderungen angemessen zu begegnen, mithin muss sie zukunftsoffen und flexibel sein.[96] Neben der formalen Verfassungsänderung durch den Gesetzgeber ist somit die Fortentwicklung der Verfassung anhand ihrer Interpretation durch das *BVerfG* von entscheidender Bedeutung.[97] Lückenhaftigkeit oder die Änderung tatsächlicher Verhältnisse setzen richterliche Rechtsfortbildung auch bei der Auslegung des Grundgesetzes voraus,[98] sofern gerade diese Fortentwicklung zur Wahrung der ordnenden und begrenzenden Funktion der Verfassung notwendig ist.[99] Seiner Aufgabe, die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, kann das allgemeine Persönlichkeitsrecht nur dann gerecht werden,

---

[91] *Hoffmann-Riem*, JZ 2008, 1009 (1014f.).
[92] *BVerfGE* 54, 143 (153); 72, 155 (170); 79, 256 (268).
[93] *Kube*, in: HStR VII³, § 148 Rn. 29.
[94] *Lorenz*, in: *Scholz* u.a., Realitätsprägung durch Verfassungsrecht, S. 17 (21); *Durner*, in: *Maunz/Dürig*, GG, Bd. 2, Art. 10 Rn. 59, kritisiert demgegenüber, dass ein seit langem voranschreitender Bedeutungsverlust des Verfassungswortlauts mit der Formulierung des *GVIiS* nochmals erheblich verstärkt worden sei.
[95] Vgl. insoweit auch *BVerfGE* 109, 279 (309) zum „Großen Lauschangriff".
[96] *Voßkuhle*, JZ 2009, 917 (919).
[97] *Voßkuhle*, JZ 2009, 917 (919).
[98] Vgl. *Starck*, Verfassungen, S. 155.
[99] *Starck*, Verfassungen, S. 127.

wenn sein Schutzniveau unter Berücksichtigung neuartiger Gefährdungen aufrechterhalten wird.

Die Herausarbeitung des *GVIiS* als Ausprägung des allgemeinen Persönlichkeitsrechts ist dementsprechend nicht mit einer inhaltlichen Änderung der entsprechenden Normen verbunden. Weiterhin ist Ausgangspunkt der Persönlichkeitsschutz des Einzelnen. Dieser Schutz muss sich notwendigerweise an bestehenden Gefährdungen orientieren. Wenn der Schutzbereich des allgemeinen Persönlichkeitsrechts durch die weitere Ausprägung des *GVIiS* konkretisiert wird, ändert sich aufgrund des gleichbleibenden Ausgangspunkts des grundrechtlichen Schutzes nicht die grundlegende Bedeutung der grundrechtlichen Verbürgung der freien Entfaltung der Persönlichkeit. Mit der Entwicklung dieser neuartigen Ausprägung des allgemeinen Persönlichkeitsrechts kann dann auch kein Verfassungswandel verbunden sein. Der Begriff soll hier dahingehend verstanden werden, dass sich der Sinn einer Verfassungsnorm ändert, ohne dass auch der Verfassungstext geändert wird.[100] Eine solche Änderung ist mit der Herausarbeitung des *GVIiS* nicht verbunden. Denn Verfassungswandel beruht vor allem auf der ausdrücklichen oder schleichenden Änderung der Rechtsprechung des *BVerfG*.[101] Inhaltliche Änderung kann dabei von vornherein nicht die Änderung des normativen Gehalts einer Verfassungsnorm sein.[102] Einer solchen Änderung stünde schon das Textänderungsgebot des Art. 79 Abs. 1 S. 1 GG entgegen.[103] Mit der Herausarbeitung des *GVIiS* ist jedoch keine inhaltliche Änderung des Art. 2 Abs. 1 GG in dem Sinne verbunden, dass die Schutzrichtung der menschlichen Persönlichkeit aufgegeben würde. Das vom Grundgesetz gewährleistete Schutzniveau wird durch diese weitere Ausprägung des allgemeinen Persönlichkeitsrechts nicht ausgeweitet, sondern es werden dessen Freiheitsgewährleistungen bewahrt.[104] Denn der umfassenden Gewährleistung individueller Freiheit entspricht ein variabler Schutzbereich, der im konkreten Einzelfall dort verfestigt wird, wo bestimmte neuartige Freiheitsgefährdungen in typischer Weise auftreten.[105] Die „Erfindung" neuer Grundrechte stellt daher die Fortentwicklung der Verfassung im Wege ihrer Interpretation dar, um auf neue Herausforderungen angemessen reagieren zu können.[106] Es werden dabei nicht am verfassungsändernden Gesetzgeber vorbei neue Schutzgehalte geschaffen, sondern ein bestehender Schutzbereich mittels Fallgruppenbildung dogmatisch verfeinert und Rechtsklarheit geschaf-

[100] So *Stern*, Staatsrecht I, § 5 III 2, S. 161; *Voßkuhle*, in: *Wahl* (Hrsg.), Verfassungsänderung, S. 201 (203).
[101] *Walter*, AöR 125 (2000), 517 (521).
[102] *Voßkuhle*, in: *Wahl* (Hrsg.), Verfassungsänderung, S. 201 (209).
[103] *Hain*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 2, Art. 79 Rn. 13.
[104] *Michael/Morlok*, Grundrechte, Rn. 34, welche die Formulierung des *GVIiS* aber als Beispiel für einen Verfassungswandel nennen.
[105] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 19.
[106] *Voßkuhle*, JZ 2009, 917 (919f.).

fen.[107] Die Fallgruppen des allgemeinen Persönlichkeitsrechts sind daher keine verselbständigten Freiheitsrechte, sondern tatbestandliche Konkretisierungen des Schutzbereichs der allgemeinen Handlungsfreiheit.[108] Der innovationsoffene Grundrechtstatbestand des allgemeinen Persönlichkeitsrechts setzt sich somit aus Einzelkomponenten zusammen, die „aus Rück- und Vorgriffen auf seine eigene Anwendungsgeschichte in einem prinzipiell endlosen Prozess der Rechtsfortbildung erzeugt werden".[109] In einem solchen Vorgang werden die Schutzgehalte eines wichtigen Grundrechts vom *BVerfG* aus den „mageren Anhaltspunkten des Grundgesetzes" fortdauernd entwickelt.[110] Das *BVerfG* hat somit in der vorliegenden Entscheidung kein „neues" Grundrecht geschaffen,[111] sondern das allgemeine Persönlichkeitsrecht durch weitere Ausdifferenzierung konkretisiert.[112]

### IV. Bindungswirkung von Entscheidungen des BVerfG, § 31 Abs. 1 BVerfGG

Die inhaltliche Bestimmung des Schutzbereiches des *GVIiS* hängt maßgeblich von den Urteilsgründen der gegenständlichen Entscheidung ab. Inwieweit diese Gründe zwingende inhaltliche Vorgaben machen, hängt von der Reichweite der Bindungswirkung der Entscheidung des *BVerfG* ab. Gem. § 31 Abs. 1 BVerfGG binden die Entscheidungen des *BVerfG* die Verfassungsorgane des Bundes und der Länder sowie alle Gerichte und Behörden. In den Fällen des Abs. 2 kommt der Entscheidung des *BVerfG* Gesetzeskraft zu. Diese Bindungswirkung umfasst zunächst den Tenor einer verfassungsgerichtlichen Entscheidung.[113] Dieser ist gegebenenfalls unter Heranziehung der Urteilsgründe zu interpretieren.[114] Nach Ansicht des *BVerfG* erstreckt sich die Bindungswirkung des § 31 Abs. 1 BVerfGG darüber hinaus auch auf die sog. „tragenden Gründe" einer Entscheidung,[115] sofern diese die Auslegung und Anwendung des Grundgesetzes betreffen.[116] Verfassungsgerichtlichen Entscheidungen komme nach § 31 BVerfGG Bindungswirkung insoweit zu, als es die Funktion des Bundesverfassungsgerichts als „maßgeblicher Interpret und Hüter der Verfassung" erfordert.[117] Das *BVerfG* versteht sich

---

[107] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 20.
[108] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 131.
[109] *Vesting*, in: *Götting/Schertz/Seitz*, Hdb. Persönlichkeitsrecht, § 6 Rn. 3.
[110] *Jarass*, in: *Erichsen/Kollhosser/Welp* (Hrsg.), Recht der Persönlichkeit, S. 89 (103).
[111] A.A. *Gudermann*, Online-Durchsuchung, S. 173: Das *BVerfG* habe sich zum Normsetzer gemacht.
[112] *Hoffmann-Riem*, JZ 2008, 1009 (1022); a.A. *Lepsius*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 21.
[113] *BVerfGE* 104, 151 (197).
[114] *Schlaich/Korioth*, Bundesverfassungsgericht, Rn. 485; *Voßkuhle*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 3, Art. 94 Rn. 32.
[115] *BVerfGE* 1, 14 (37); 19, 377 (392); 20, 56 (87); 104, 151 (197); 112, 268 (277).
[116] *BVerfGE* 19, 377 (392); 40, 88 (93f.); 112, 268 (277).
[117] *BVerfGE* 40, 88 (93).

danach als die „verbindliche Instanz in Verfassungsfragen".[118] Den Begriff der tragenden Gründe einer Entscheidung definiert das *BVerfG* wie folgt:[119]

> „*Tragend für eine Entscheidung sind solche Rechtssätze, die nicht hinweg gedacht werden können, ohne dass das konkrete Entscheidungsergebnis nach dem in der Entscheidung zum Ausdruck gekommenen Gedankengang entfiele. Nicht tragend sind dagegen bei Gelegenheit einer Entscheidung gemachte Rechtsausführungen, die außerhalb des Begründungszusammenhangs zwischen genereller Rechtsregel und konkreter Entscheidung stehen. Bei der Beurteilung, ob ein tragender Grund vorliegt, ist von der niedergelegten Begründung in ihrem objektiven Gehalt auszugehen.*"

Diese Auffassung sieht sich einiger Kritik ausgesetzt. Eine solche Bindungswirkung auch der tragenden Gründe einer Entscheidung beinhalte legislative Elemente. *Schlaich/Korioth* kritisieren, das *BVerfG* mache sich so zum „authentischen Interpreten" der Verfassung.[120] Mit der selbständigen Bindung auch der tragenden Entscheidungsgründe ohne die Koppelung an den konkreten Streitfall würden abstrakt-genereller Rechtssätze aufgestellt. Deren Formulierung sei jedoch dem Gesetz- bzw. Verfassungsgeber vorbehalten.[121] Das *BVerfG* werde mithin als Gesetzgeber im materiellen Sinne tätig.[122] Weiter werden daneben auch Abgrenzungsschwierigkeiten eingewandt. Schon eine klare Abgrenzung der tragenden von den nicht tragenden Gründen sei gar nicht möglich.[123] Zuletzt sei gerade die vom *BVerfG* häufig betonte Entwicklungsoffenheit des Grundgesetzes gefährdet. Mit der Einbeziehung der tragenden Gründe in die Bindungswirkung des § 31 Abs. 1 BVerfGG erfolge eine Festschreibung des Verfassungsrechts, die der notwendigen Offenheit des Grundgesetzes für künftige Entwicklungen zuwiderlaufe.[124] Aufgrund dieser Festschreibung entfalle die Auseinandersetzung mit widersprechenden Fachgerichten.[125] Anlässe zu kritischer Selbstüberprüfung würden durch eine solche weitreichende Entscheidungsbindung „bereits im Keim erstickt".[126] Im Gegensatz zu den Leitsätzen des gegenständlichen Urteils findet das *GVIiS* im Urteilstenor keine Erwähnung:

---

118 *BVerfGE* 40, 88 (94).
119 *BVerfGE* 96, 375 (404); 115, 97 (110).
120 *Schlaich/Korioth*, Bundesverfassungsgericht, Rn. 486.
121 *Hoffmann-Riem*, Der Staat [1974], 335 (357).
122 *Wischermann*, Rechtskraft und Bindungswirkung, S 68f.
123 *Schaich/Korioth*, Bundesverfassungsgericht, Rn. 488ff.; *Hoffmann-Riem*, Der Staat [1974], 335 (349); *Voßkuhle*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 3, Art. 94 Rn 32.
124 *Schlaich/Korioth*, Bundesverfassungsgericht, Rn. 490; *Wischermann*, Rechtskraft und Bindungswirkung, S. 117ff.; *Schulze Fielitz*, in: FS 50 Jahre BVerfG, Bd. 1, S. 385 (391); *Voßkuhle*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 3, Art. 94 Rn. 32.
125 *Schlaich/Korioth*, Bundesverfassungsgericht, Rn. 492; *Schulze Fielitz*, in: FS 50 Jahre BVerfG, Bd. 1, S. 385 (391).
126 *Voßkuhle*, in: *V. Mangoldt/Klein/Starck*, GG, Bd. 3, Art. 94 Rn 32.

> *„(1) § 5 Absatz 2 Nummer 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen in der Fassung des Gesetzes vom 20. Dezember 2006 (Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen, Seite 620) ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, Artikel 10 Absatz 1 und Artikel 19 Absatz 1 Satz 2 des Grundgesetzes unvereinbar und nichtig.*“[127]

Der von der Bindungswirkung des § 31 Abs. 1 BVerfGG unstreitig erfasste Urteilstenor wird definiert als die konkrete Entscheidung des *BVerfG* über die streitgegenständliche Frage.[128] Dies ist im Rahmen der Verfassungsbeschwerde die Frage, ob der Beschwerdeführer durch einen bestimmten Akt der öffentlichen Gewalt in einem bestimmten Grundrecht oder grundrechtsgleichen Recht verletzt ist[129] (vgl. Art. 93 Abs. 1 Nr. 4a GG). Im gegenständlichen Verfahren rügten die Beschwerdeführer hinsichtlich der Norm des § 5 Abs. 2 Nr. 11 VSG NRW eine Verletzung von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 13 Abs. 1 GG.[130] Mit der Feststellung der Unvereinbarkeit des § 5 Abs. 2 Nr. 11 VSG NRW mit Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 und Art. 10 GG sowie der Feststellung der Nichtigkeit der Norm wird zugleich dergestalt über den Streitgegenstand entschieden, dass die behauptete Grundrechtsverletzung besteht. Der Tenor ist insofern eindeutig und bedarf keiner weiteren Auslegung unter Heranziehung der Urteilsgründe. Gesetzgeber und Fachgerichte hätten die Ausführungen des *BVerfG* zum *GVIiS* in den Entscheidungsgründen somit nur dann zu berücksichtigen, wenn es sich bei diesen Ausführungen um tragende Gründe i.S.d. Rechtsprechung des *BVerfG* handelte und diese Gründe von der Bindungswirkung des § 31 Abs. 1 GG erfasst wären. Die Ausführungen zum *GVIiS* dürften daher nicht hinweg gedacht werden können, ohne dass die Unvereinbarkeit des § 5 Abs. 2 Nr. 11 VSG NRW mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und die Feststellung der Nichtigkeit der Norm nach dem konkreten Begründungsgang entfielen.

Das *GVIiS* wird als eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts formuliert. Zwar würde sich der Entscheidungstenor nicht ändern, wenn sich die Unvereinbarkeit aus dem *RiS* als alleinigem Prüfungsmaßstab für den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme ergeben würde. In beiden Fällen wäre das allgemeine Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG heranzuziehen. Das Ergebnis der Entscheidung würde aber auf einem gänzlich anderen Gedankengang aufbauen. Die Formulierung einer speziell auf den Schutz informationstechnischer Systeme ausgerichteten Konkretisierung des allgemeinen Persönlichkeitsrechts bliebe unberücksichtigt. Anforderungen an die Verhältnismäßigkeit i.e.S. ergeben sich speziell aus der festgestellten neuartigen Persönlichkeitsgefährdung durch die weitverbreitete Nutzung

---

127 *BVerfGE* 120, 274 (275).
128 *BVerfGE* 104, 151 (197).
129 *Hillgruber/Goos*, Verfassungsprozessrecht, Rn. 91.
130 *BVerfGE* 120, 274 (290).

informationstechnischer Systeme.[131] Die Norm wird gerade an diesen Folgen eines technischen Zugriffs für die Persönlichkeitsentfaltung des Einzelnen geprüft. Diese Gefährdung unterscheidet sich aber wesentlich von derjenigen, die das *RiS* mit dem Schutz des personenbezogenen Datums erfasst. Bei den Ausführungen zum *GVIiS* handelt es sich somit nicht um solche, die außerhalb des Begründungszusammenhangs der konkreten Entscheidung stehen. Es ist daher nach dem anzulegenden objektiven Betrachtungsmaßstab unentbehrlich, auf den denjenigen Gedankengang der Urteilsbegründung, der die Ausführungen zum *GVIiS* enthält, zurückzugreifen, um zu dem Tenor der Entscheidung in der konkreten Form zu gelangen. Die Ausführungen in den Entscheidungsgründen zum *GVIiS* werden daher als „tragende Gründe" i.S.d. Rechtsprechung des *BVerfG* verstanden. Gegenstand der Bindungswirkung des § 31 Abs. 1 GG müssten damit auch solche tragenden Gründe sein.

Für eine solche Reichweite lässt sich zunächst der Wortlaut des § 31 Abs. 1 BVerfGG abführen. Dieser spricht ausdrücklich von „Entscheidung", nicht dagegen wie Abs. 2 S. 3, 4 von der „Entscheidungsformel". Aufgrund dieser sprachlichen Unterscheidung steht der Gesetzeswortlaut einem weiten Verständnis des Begriffs der Entscheidung über die bloße Entscheidungsformel hinaus nicht von vornherein entgegen. Das Verständnis des *BVerfG* kann sich weiter auf den historischen Ursprung der Norm berufen. Nach dem gesetzgeberischen Willen verpflichtet die Bindungswirkung des § 31 Abs. 1 BVerfGG „alle Organe, Gerichte und Behörden des Bundes und der Länder künftig bei ihren Maßnahmen die Entscheidungen, solange das Bundesverfassungsgericht seine Rechtsprechung nicht ändert, zu beachten".[132] Der vom *BVerfG* festgestellte Inhalt einer Verfassungsnorm sollte für alle staatlichen Organe „nicht nur für den konkreten Anlass, sondern für alle gleichliegenden Anlässe" verbindlich sein.[133] Eine solche Verbindlichkeit setzt die Einbeziehung der tragenden Gründe der Entscheidung voraus. Denn die Konkretisierung des Verfassungsrechts und seine inhaltliche Bestimmung geschehen nicht im Tenor, sondern in den Gründen der Entscheidung.[134] Die Einheit der Verfassung als Grundordnung des Gemeinwesens lässt sich jedenfalls auf Dauer nur durch eine verbindliche einheitliche Auslegung der Verfassung garantieren.[135] Der Sinn einer Bindungswirkung liegt in ihrer verbindlich klärenden und stabilisierenden Funktion.[136] Dieser Funktion würde die Möglich-

[131] Vgl. *BVerfGE* 120, 274 (303ff.).

[132] RegE zu § 27 Abs. 1 BVerfGG (wortgleich zu § 31 Abs. 1 BVerfGG), BT-Drucks. 1/788, S. 27.

[133] Berichterstatter des Rechtsausschusses Abgeordneter *Dr. Wahl*, Verhandlungen des dt. Bundestages, Sten. Bericht, I/S. 4226 Rn. B; dagegen spreche, so *Voßkuhle* in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 3, Art. 94 Rn. 32, dass die Vorschrift über das Wiederholungsverbot in § 95 Abs. 1 S. 2 BVerfGG und die in § 67 S. 3 BVerfGG vorgesehene Möglichkeit, bestimmte Auslegungsergebnisse in den Urteilstenor aufzunehmen, bei Annahme einer weiten Bindungswirkung überflüssig wären.

[134] *Benda/Klein*, Verfassungsprozessrecht, Rn. 1456.

[135] *Heusch*, in: *Umbach/Clemens/Dollinger* (Hrsg.), BVerfGG, § 31 Rn. 59.

[136] *Lange*, JuS 1978, 1 (5).

keit von Gerichten und Behörden entgegenstehen, Entscheidungen zu treffen, die den tragenden Gründen von Entscheidungen des *BVerfG* zuwiderlaufen. Es bestünde dabei die Gefahr, sich vom Kern der verfassungsgerichtlichen Entscheidung möglicherweise weiter zu entfernen, als der vom *BVerfG* im konkreten Fall aufgehobene Akt selbst entfernt war.[137] Dies stünde in Widerspruch zu der verfassungsrechtlichen Aufgabenstellung des *BVerfG*. Die letztverbindliche Auslegung der Verfassung ist dem *BVerfG* durch das Grundgesetz anvertraut.[138] Die Wahrnehmung dieser Aufgabe setzt voraus, dass die der Verfassung entnommenen Aussagen, die für das im konkreten Verfahren gewonnene Ergebnis tragend sind, für alle und nicht lediglich für die an diesem Verfahren beteiligten Staatsorgane verbindlich sind.[139] Bei einer Bindung allein an den Tenor der Entscheidung wären die in § 31 Abs. 1 BVerfGG genannten staatlichen Stellen rechtlich effektiv nicht gehindert, sich in einem parallel gelagerten Fall entgegen der Auslegung des *BVerfG* zu verhalten.[140] Damit die verfassungsgerichtliche Entscheidung Einfluss auf das Verhalten der staatlichen Organe über den konkreten Einzelfall hinaus haben kann, bedarf es daher einer Erstreckung der Bindungswirkung auf die tragenden Gründe der Entscheidung.[141] Ginge man demgegenüber von einer Bindungswirkung nur des Entscheidungstenors aus, würden den Fachgerichten zudem verbindliche einheitliche Maßstäbe für die Berücksichtigung der Grundrechte auf privatrechtlicher Ebene fehlen. Einer einheitlichen Rechtsprechung stünde stets die Unsicherheit entgegen, ob sich die Gerichte den Ausführungen des *BVerfG* anschließen, obwohl sie dazu rechtlich nicht verpflichtet wären. Der Gesetzgeber seinerseits benötigt für seine legislative Tätigkeit verlässliche inhaltliche Vorgaben seiner nach Art. 20 Abs. 3 GG bestehenden Bindung an die verfassungsmäßige Ordnung. Einer sich aus dem jeweiligen Grundrecht ergebenden Schutzpflicht kann nur dann genügt werden, wenn die tragenden Gründe einer Entscheidung verbindliche Auslegungsrichtlinien des jeweiligen Schutzbereichs vermitteln, und damit den Inhalt der Schutzpflicht präzisieren. Daher ist es gerade für die Herausarbeitung des Schutzbereichs des *GVIiS* im Wege der richterlichen Rechtsfortbildung entscheidend, ob die tragenden Gründe der gegenständlichen Entscheidung des *BVerfG* von der Bindungswirkung des § 31 Abs. 1 BVerfGG erfasst sind.

Diese lassen sich von den nicht tragenden Gründen ohne weiteres unterscheiden. Entscheidende Abgrenzungsschwierigkeiten bestehen nicht. Eine weite Bindungswirkung beschränkt sich zudem auf gleichgelagerte Fälle und ist inhaltlich allein auf die Entscheidungsgründe ausgerichtet, so dass ein ausreichender Spielraum für Differenzierungsmöglichkeiten besteht und Innovationen möglich blei-

---

137 *Lange*, JuS 1978, 1 (5).
138 *Heusch*, in: *Umbach/Clemens/Dollinger* (Hrsg.), BVerfGG, § 31 Rn. 59.
139 *Heusch*, in: *Umbach/Clemens/Dollinger* (Hrsg.), BVerfGG, § 31 Rn. 59.
140 *Heusch*, in: *Umbach/Clemens/Dollinger* (Hrsg.), BVerfGG, § 31 Rn. 59.
141 Benda/*Klein*, Verfassungsprozessrecht, Rn. 1456.

ben.[142] Die Verbindlichkeit der Verfassungsauslegung macht das *BVerfG* nicht auch zum authentischen Interpreten der Verfassung, denn das Gericht kann nicht über die Verfassung als seinem eigenen Prüfungsmaßstab selbst verfügen.[143] Allerdings hat es die Kompetenz zur autoritativen letztverbindlichen Auslegung des Grundgesetzes, wodurch ihm hierüber die entscheidende Interpretationsherrschaft zukommt.[144] Es wird daher der Ansicht des *BVerfG* gefolgt. Die Bindungswirkung des § 31 Abs. 1 BVerfGG erstreckt sich danach auch auf die tragenden Gründe der vorliegenden Entscheidung. Bindungswirkung in diesem Sinne kommt somit sämtlichen Ausführungen des *BVerfG* zur Ausgestaltung des *GVIiS* zu. Diese Ausführungen sind sodann der verbindliche Maßstab für die Berücksichtigung des *GVIiS* auf privatrechtlicher Ebene. Nach *Schulze-Fielitz*[145] relativiere sich der Streit um die Reichweite der Bindungswirkung des § 31 Abs. 1 BVerfGG schon dadurch, dass eine bestehende Bindungswirkung ohnehin praktisch nur begrenzt durchsetzbar wäre, würde es dem *BVerfG* nicht gelingen, dass seine Entscheidungen in der allgemeinen wie der fachlich-juristischen Öffentlichkeit akzeptiert würden, also inhaltlich zu überzeugen. Eine solche Akzeptanz zieht *Schirrmacher*[146] nach Bekanntwerden der Einzelheiten des Einsatzes des sog. *Staatstrojaners* und dessen Funktionalität grundsätzlich in Zweifel: „Reicht es wirklich, nur auf die Grundgesetztreue des Staates und seiner Diener zu hoffen, wenn der Code, den nur die Auftraggeber und die Eingeweihten verstehen, diese Treue bereits durchbricht?".

[142] Benda/*Klein*, Verfassungsprozessrecht, 2. Aufl., Rn. 1330.
[143] *Hillgruber/Goos*, Verfassungsprozessrecht, Rn. 15.
[144] *Hillgruber/Goos*, Verfassungsprozessrecht, Rn. 15.
[145] *Schulze-Fielitz*, in: FS 50 Jahre BVerfG, Bd. 1, S. 383 (394)).
[146] „Code ist Gesetz", *FAS* v. 9.10.2011 (abrufbar unter: http://www.faz.net/aktuell/feuilleton/staatstrojaner-code-ist-gesetz-11486546.html)

## B. Einzelbetrachtung

Die Feststellung der verbindlichen Auslegungsmaßstäbe für die Bestimmung des Inhalts des *GVIiS* bildet die Grundlage für eine detaillierte Darstellung dieser Ausprägung des allgemeinen Persönlichkeitsrechts. Die Darstellung orientiert sich dabei an dem klassischen Prüfungsaufbau bestehend aus sachlichem und personalem Schutzbereich, Eingriff und dessen verfassungsrechtlicher Rechtfertigung. Einen Schwerpunkt bildet die inhaltliche Bestimmung der namensgebenden informationstechnischen Begrifflichkeiten des *GVIiS*. Bei der Erörterung des sachlichen Schutzbereichs wird ausführlich auf die Subsidiarität des allgemeinen Persönlichkeitsrechts zu den speziellen Freiheitsrechten eingegangen. So wurde in der Diskussion um die Zulässigkeit der sog. *Online-Durchsuchung*, die im Vorfeld der gegenständlichen Entscheidung des *BVerfG* stattfand, vielfach auf Art. 13 Abs. 1 GG als maßgebliche Grundrechtsnorm für den Schutz vor der Infiltration informationstechnischer Systeme abgestellt. Das Verhältnis des *GVIiS* zum Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG verdient insbesondere hinsichtlich der Abgrenzung des technischen Zugriffs auf ein informationstechnisches System von der sog. *Quellen-Telekommunikationsüberwachung* Aufmerksamkeit. Großer Kritik seitens der juristischen Fachwelt sah sich die Abgrenzung des *GVIiS* von dem *RiS* ausgesetzt, die das *BVerfG* vornahm. Hier wird vor allem der Unterschied zwischen dem Schutzansatz des *RiS*, der auf das Schutzgut des personenbezogenen Datums ausgerichtet ist, und demjenigen des *GVIiS*, der auf eine bestimmte technische Sphäre der Persönlichkeitsentfaltung abstellt, herausgearbeitet. Es folgt sodann noch ein Exkurs zur DS-GVO-E. Dieser untersucht den Anwendungsbereich des Entwurfs hinsichtlich des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner Ausformung durch das *BVerfG*. Der personale Schutzbereich des *GVIiS* schließlich enthält mit der Nutzung des informationstechnischen Systems „als eigenes“[147] eine spezifische Voraussetzung einer grundrechtlich anzuerkennenden Persönlichkeitsentfaltung. Der Schutz juristischer Personen nach Art. 19 Abs. 3 GG wird ebenfalls erörtert.

### I. Sachlicher Schutzbereich

Das *BVerfG* geht in seiner Entscheidung von einer zweistufigen Eröffnung des sachlichen Schutzbereichs des *GVIiS* aus.[148] Ausgangspunkt ist zunächst das informationstechnische System. Die Eröffnung des Schutzbereichs richtet sich zunächst nicht nach einem bestimmten Verhalten des Betroffenen, sondern nach dem zu der grundrechtlich geschützten Persönlichkeitsentfaltung notwendigen Gegenstand. Die vom Schutzbereich des *GVIiS* erfassten informationstechni-

[147] *BVerfGE* 120, 274 (315).
[148] Ebenso *Holznagel/Schumacher*, MMR 2009, 3 (5).

schen Systeme werden dem Nutzer als besondere Schutzzone zugewiesen, in die der Staat nur ausnahmsweise eindringen darf.[149] Insofern ähnelt das *GVIiS* mit dem formalen Anknüpfungspunkt der Errichtung einer besonderen Schutzzone der Privatheit strukturell der speziellen Garantie der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG.[150] Letzterer gewährleistet dem Einzelnen einen allein räumlichen Rückzugsort der Persönlichkeitsentfaltung. Das *GVIiS* schützt darüber hinaus einen von räumlichen Grenzen unabhängigen technisch definierten Privatbereich. Es ergänzt also insofern den durch Art. 13 Abs. 1 GG geschützten real-räumlichen um einen „virtuell-informationstechnischen Bereich freier Persönlichkeitsentfaltung".[151] Anders aber als Art. 13 Abs. 1 GG, der die Eröffnung des sachlichen Schutzbereichs nur davon abhängig macht, dass die Wohnung des Grundrechtsträgers Gegenstand eines staatlichen Eingriffs ist, erschöpft sich die Schutzbereichseröffnung des *GVIiS* eben nicht in dieser „Verdinglichung"[152] des Schutzbereichs. In einem zweiten Schritt muss das informationstechnische System eine gewisse technische Komplexität aufweisen. Die Persönlichkeitsentfaltung des Grundrechtsträgers wird bei der Eröffnung des Schutzbereichs des Art. 13 Abs. 1 GG schon bei der Auslegung des Begriffs der Wohnung berücksichtigt. Dem Einzelnen wird ein „elementaren Lebensraum"[153] und darin das Recht gewährleistet, „in Ruhe gelassen zu werden".[154] Demgegenüber stellt das *BVerfG* nicht jedes informationstechnische System unter den Schutz des *GVIiS*. Die Begründung einer besonderen Relevanz für die Persönlichkeitsentfaltung setzt voraus, dass der potentielle Zugriff auf das informationstechnische System überhaupt eine besondere, gerade dem Schutzbereich des *GVIiS* eigene Gefährdungslage begründen kann.

### *1. Informationstechnisches System*

Das *BVerfG* gebraucht in seiner Entscheidung den Begriff des informationstechnischen Systems, ohne ihn abstrakt zu definieren. Im Hinblick auf die namensgebende Funktion des Begriffs ist dies vielleicht nur überraschend. Bezüglich der schutzbereichseröffnenden Funktion führt die fehlende Definition jedoch zu Schwierigkeiten bei der Formulierung des Schutzbereichs des *GVIiS*. Das Gericht gibt lediglich einzelne Beispiele solcher Systeme, die es unter denjenigen Begriff des informationstechnischen Systems fasst, der auch in Bezug auf das *GVIiS* schutzbereichseröffnend wirkt: Das Internet als „elektronischer Verbund von

[149] *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (119).
[150] *Bäcker*, in: *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (9); *Pieroth/Schlink*, Grundrechte, Rn. 400 *Britz*, DÖV 2008, 411 (412); *Hornung*, CR 2008, 299 (302).
[151] *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn 73c.
[152] *Hornung*, CR 2008, 299 (302).
[153] *BVerfGE* 42, 212 (219); 51, 97 (110).
[154] *BVerfGE* 27, 1 (6); 51, 97 (107); 103, 142 (150).

Rechnernetzwerken“ sowie das einzelne Rechnernetzwerk selbst[155], „Personalcomputer“[156], „Telekommunikationsgeräte oder elektronische Geräte, die in Wohnungen („elektronische Steuerungsanlagen der Haustechnik“[157]) oder Kraftfahrzeugen enthalten sind“[158] sowie „mobile informationstechnische Systeme wie Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone“.[159]

Ebenso wenig findet sich in den Gesetzgebungsmaterialien insb. der Begründung des Gesetzentwurfs des VSG NRW 2007[160] eine Definition des Begriffs des informationstechnischen Systems, auf die das *BVerfG* hätte zurückgreifen können.

In seiner von dem *BVerfG* eingeholten sachkundigen Stellungnahme[161] definiert *Andreas Bogk* vom *CCC* den Begriff des informationstechnischen Systems wie folgt:

> „*Der Begriff der ‚informationstechnischen Systeme‘, wie er in § 2 Abs. 2 Nr. 11 VSG NRW verwendet wird, ist sehr weit, und umfasst eine Vielzahl von Gegenständen aus praktisch allen Bereichen des Alltags. Formal gesehen sind das alle Systeme, in denen eine elektronische Datenverarbeitung stattfindet, was im Allgemeinen durch das Vorhandensein eines digitalen Prozessors sowie eines Programms zur Ablaufsteuerung desselben charakterisiert ist.*“

Auch dieser Definition fehlen diejenigen abstrakten Merkmale des strukturellen Aufbaus eines informationstechnischen Systems, anhand derer die beispielhafte Aufzählung des *BVerfG* nachgezeichnet werden könnte. Für die Eröffnung des Schutzbereichs des *GVIiS* fehlen daher verlässliche und verallgemeinerungsfähige Kriterien, so dass für jeden Einzelfall die Vergleichbarkeit mit den vom *BVerfG* bloß beispielhaft aufgezählten informationstechnischen Systemen geprüft werden müsste. Daher sollen im Folgenden diejenigen gemeinsamen Strukturen und Funktionen der benannten Beispiele herausgearbeitet werden, die gerade schutzbereichseröffnend wirken, um eine möglichst abstrakte Definition des Begriffs des informationstechnischen Systems zu finden.[162]

---

[155] *BVerfGE* 120, 274 (276); für die Anwendung des *GVIiS* auch auf den einzelnen WLAN-Router *Roßnagel/Schnabel*, NJW 2008, 3534 (3536), dagegen *Hoffmann*, CR 2010, 515 (516).

[156] *BVerfGE* 120, 274 (303).

[157] *BVerfGE* 120, 274 (313).

[158] *BVerfGE* 120, 274 (304).

[159] *BVerfGE* 120, 274 (311).

[160] RegE, LT-NRW-Drucks. 14/2211.

[161] *Bogk*, Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07 vom 23.9.2007, S. 4.

[162] So wird auch der Begriff der Wohnung i.S.d. Art. 13 Abs. 1 GG nicht anhand von Beispielen definiert, sondern in abstrakter Form als Privatsphäre gerade in räumlicher Hinsicht (*BVerfGE* 65, 1 (40)) oder als „räumliche Sphäre, in der sich das Privatleben entfaltet“ (*BVerfGE* 89, 1 (12)).

a. Definition

Dabei ist zu berücksichtigen, dass das *BVerfG* den Begriff des informationstechnischen Systems als verfassungsrechtlichen Begriff gebraucht.[163] Das Grundgesetz nimmt im Rangordnungssystem der innerstaatlichen Rechtsquellen den obersten Rang ein und geht damit dem einfachen Bundesrecht vor.[164] Schon aufgrund dieser Normenhierarchie kann kein einfaches Bundesrecht zur Auslegung eines verfassungsrechtlichen Begriffs herangezogen werden, sondern ein einfachgesetzlicher Begriff allenfalls gleichbedeutend mit einem verfassungsrechtlichen sein. Folglich können einfachgesetzliche Definitionen und Begriffe der Informationstechnik zwar die Grundlage der Begriffsbestimmung liefern. Die unterschiedslose Übernahme einzelner Begrifflichkeiten setzt jedoch jedenfalls voraus, dass die Vorgaben, die das *BVerfG* in seinem Urteil macht, der Übernahme nicht entgegenstehen.

i. Bundesministerium des Innern (BMI)

Im Rahmen des Gesetzgebungsprozesses zur Änderung des BKAG wird das informationstechnische System zunächst von dem *BMI* definiert. Es wählt den Begriff bewusst weit, um der derzeitigen und zukünftigen technischen Entwicklung Rechnung tragen zu können.[165] Der Begriff bezeichnet demnach ein „System, welches aus Hard- und Software sowie aus Daten besteht, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient". Zwar geht diese Definition auf Komponenten und Funktionen des informationstechnischen Systems ein, gerade der Begriff des Systems selbst wird jedoch auch hier nicht definiert.

ii. Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKAG-E)

Auch im Gesetzentwurf der großen Koalition zur Änderung des BKAG[166] findet sich ein Hinweis auf die Merkmale eines informationstechnischen Systems. Danach soll der verwendete Begriff des informationstechnischen Systems dem des § 2 Abs. 2 Nr. 1 BSIG[167] entsprechen und wurde bewusst weit gewählt, um alle nach der Rechtsprechung des *BVerfG* schutzbedürftigen informationstechnischen Systeme zu erfassen.[168] Gem. § 2 Abs. 2 Nr. 1 BSIG bedeutet Sicherheit in der

---

[163] *Hoffmann-Riem*, JZ 2008, 1009 (1012).
[164] Vgl. *Ossenbühl*, in: HStR V³, § 100 Rn. 92f.
[165] Antwort des *BMI* vom 22.8.2007 auf den Fragenkatalog des *BMJ* (Fn. 14), S. 2.
[166] *Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*, BT-Drucks. 16/9588.
[167] *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* (BSI-Gesetz - BSIG) vom 14.8.2009 (BGBl. I S. 2821).
[168] BT-Drucks. 16/9588 S. 26f.

Informationstechnik die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen (Nr. 1) in *informationstechnischen Systemen* oder Komponenten. Der Begriff des informationstechnischen Systems selbst wird hingegen nicht auch legaldefiniert. Auch in der Begründung des BSIG-E der Bundesregierung[169] findet sich keine Definition. Es wird dort lediglich erläutert, was unter der Einhaltung von Sicherheitsstandards i.S.d. § 2 Abs. 2 Nr. 1 BSIG zu verstehen sei. Gemeint seien ein technischer Sicherheitsstandard (z.B. automatische Verschlüsselung gespeicherter oder übertragener Informationen) sowie ergänzend oder alternativ Sicherheitsvorkehrungen bei Anwendung der Informationstechnik (z.B. baulicher, organisatorischer Art).[170] Einen Hinweis auf die Merkmale des informationstechnischen Systems gibt aber das Zusammenspiel von § 2 Abs. 1 und Abs. 2 BSIG. Informationstechnik i.S.d. BSIG umfasst nach Abs. 1 alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen. Sicherheit in der Informationstechnik wiederum bedeutet nach Abs. 2 Nr. 1 die Einhaltung bestimmter Sicherheitsstandards durch Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten. Letztere sind mithin die konkreten Bezugsobjekte zur Einhaltung informationstechnischer Sicherheitsstandards. Zumindest informationstechnische Systeme und deren Komponenten fallen daher zwangsläufig unter die Legaldefinition der Informationstechnik des § 2 Abs. 1 BSIG. Ein informationstechnisches System wäre demnach ein technisches Mittel zur Verarbeitung oder Übertragung von Informationen.

iii. Stellungnahme

Auf beide Definitionen nimmt das *BVerfG* in seiner Entscheidung weder ausdrücklich noch erkennbar stillschweigend Bezug. Die bewusst weit gefassten Definitionen entsprechen insofern der Verwendung des Begriffs durch das Gericht, als sie sich nicht an detaillierten und abschließenden technischen Spezifikationen orientieren. Ebenso offen habe das *BVerfG* den Begriff des informationstechnischen Systems formuliert, der jedes elektronische System erfasse, mit dem Informationen verarbeitet werden.[171] Ein solcher offener Begriff sei unvermeidlich, um der rasanten technischen Entwicklung im Bereich der Informationstechnologie zu begegnen. Der Schutzzweck des allgemeinen Persönlichkeitsrechts einer lückenschließenden Gewährleistung und derjenige des *GVIiS* als dessen besonderer Ausprägung würden mit der Notwendigkeit der dauernden und zeitnahen Präzisierung des Schutzbereichs nicht mehr erreicht.

---

169 RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84ff.).

170 RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84).

171 *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (126); *ders.*, in: *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (10).

Ein weiter Ansatzpunkt begegnet daher der Gefahr einer zu stark technikorientierten Bestimmung des Schutzbereichs, der aufgrund technischer Neuerungen gegebenenfalls ständig neu erweitert werden müsste.[172]

iv. Eigener Definitionsansatz

(1) Vorbemerkungen

Mangels Erkennbarkeit einer Bezugnahme des *BVerfG* auf eine der genannten Definitionen ist deren unveränderte Übernahme nicht ohne weiteres möglich. Im Folgenden soll daher ein Definitionsansatz entwickelt werden, der sich im Ausgangspunkt an den Ausführungen des *BVerfG* orientiert und im Einklang mit diesen Vorgaben zusätzliche Quellen zur Begriffsbestimmung heranzieht. Am Ende steht eine möglichst abstrakte Definition des informationstechnischen Systems. Damit entfällt die Notwendigkeit, die Schutzbereichseröffnung mittels einer Parallele zu den vom *BVerfG* genannten Beispielen prüfen zu müssen, ohne im Einzelnen diejenigen gemeinsamen Merkmale der benannten Systeme zu kennen, die gerade schutzbereichseröffnend wirken. Eine solche abstrakte Betrachtung enthält zudem den Vorteil, dass die notwendige Entwicklungsoffenheit des verfassungsrechtlichen Begriffs des informationstechnischen Systems besser berücksichtigt werden kann und zukünftige technische Gestaltungen nicht anhand eines Vergleichs mit den genannten Beispielen, sondern aufgrund abstrakter Merkmale unter den Schutzbereich des *GVIiS* gefasst werden können. Damit würde auch das etwaige Problem mangelnder Vergleichbarkeit neuer Technologien vermieden.

(2) Funktionen

Der Funktionsumfang eines informationstechnischen Systems, das in den Schutzbereich des *GVIiS* fällt, wird wiederum nicht abstrakt beschrieben, sondern es werden die Funktionen nur im Zusammenhang mit der persönlichkeitsrechtlichen Relevanz informationstechnischer Systeme aufgezählt:

> „*Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind.*“[173]

> „[…] *Die mit der Vernetzung verbundene Erweiterung der Nutzungsmöglichkeiten* [führt] *dazu, dass gegenüber einem alleinstehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden*“.[174]

[172] *Hornung*, CR 2008, 299 (302).
[173] *BVerfGE* 120, 274 (305).
[174] *BVerfGE* 120, 274 (305).

„*Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung.*“[175]

„*Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.*“[176]

„*Ein solcher heimlicher Zugriff auf ein informationstechnisches System öffnet der handelnden staatlichen Stelle den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. Dies liegt an der Vielzahl unterschiedlicher Nutzungsmöglichkeiten, die komplexe informationstechnische Systeme bieten und die mit der Erzeugung, Verarbeitung und Speicherung von personenbezogenen Daten verbunden sind.*“[177]

Danach muss ein informationstechnisches System nach der Formulierung des *BVerfG* jedenfalls zur „Erzeugung, Verarbeitung und Speicherung von Daten“ in der Lage sein. Die Urteilsgründe beschränken sich wiederum auf die bloße Benennung dieser Funktionen. Eine nähere Erläuterung findet sich nicht. Dabei hätte sich eine Bezugnahme auf die einfachgesetzlichen Begriffe des BDSG[178] derart angeboten, wie sie bereits im *Volkszählungsurteil* hinsichtlich des Begriffs der personenbezogenen Daten erfolgte.[179] Ein solcher Gleichlauf wurde hingegen nicht hergestellt. Nach § 3 Abs. 4 S. 1 BDSG ist Verarbeiten das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Speichern definiert § 3 Abs. 4 S. 2 Nr. 1 BDSG als das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung. Nach den Definitionen des BDSG beinhaltet die Verarbeitung personenbezogener Daten bereits auch deren Speicherung. Der Begriff der Erzeugung findet im BDSG keine Definition. Die in den Urteilsgründen durchgängig eingehaltene Reihenfolge bei der Nennung der Funktionen enthält aber eine zeitliche Abfolge der einzelnen Arbeitsschritte. Die von den Vorschriften des BDSG verschiedene Begriffswahl muss daher nicht notwendig auch inhaltliche Unterschiede bedingen.

---

175 *BVerfGE* 120, 274 (313).
176 *BVerfGE* 120, 274 (314).
177 *BVerfGE* 120, 274 (322).
178 *Bundesdatenschutzgesetz* in der Fassung der Bekanntmachung vom 14.1.2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 14.8.2009 (BGBl. I S. 2814).
179 *BVerfGE* 65, 1 (42).

Das vom Begriff des Speicherns nach § 3 Abs. 4 S. 2 Nr.1 BDSG umfasste „Aufnehmen" beinhaltet das Fixieren von Daten auf einem Medium mittels Aufnahmetechniken.[180] Beschreibt mithin die „Erzeugung" von Daten deren erstmaliges Anlegen, könnte dennoch der Begriff des Aufnehmens als Auslegungsansatz herangezogen werden.

(3) Aufbau

Es fehlen sodann auch die grundsätzlichen Merkmale hinsichtlich Aufbau und Komponenten des informationstechnischen Systems. Um den Schutzbereich des *GVIiS* möglichst umfassend und in generalisierender Weise - insbesondere auch losgelöst vom Ermittlungsinstrument der sog. *Online-Durchsuchung* - beschreiben zu können, werden im Folgenden Auslegungsansätze für den Begriff der Informationstechnik sowie den hiermit kombinierten Systembegriff erarbeitet.

(a) Informationstechnik

Der Begriff der Informationstechnik wird in § 2 Abs. 1 BSIG definiert als „alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen". Der Begriff der „Verarbeitung" umfasst dabei die „Erfassung", „Darstellung" und „Speicherung" von Daten.[181] Hiermit wird bewusst eine Parallele sowohl zur datenschutzrechtlichen Terminologie gezogen, als auch zum Begriffsverständnis des *BVerfG* im *Volkszählungsurteil*.[182] Einer Verwendung der Begrifflichkeiten des BSIG steht daher nicht von vornherein entgegen, dass im Unterschied zum *Volkszählungsurteil* und der gegenständlichen Entscheidung des *BVerfG* in § 2 Abs. 1 der Gegenstand einer Verarbeitung und Übertragung nicht Daten, sondern Informationen sind. Letzterer wird lediglich deshalb gebraucht, um dem Missverständnis vorzubeugen, § 2 Abs. 1 BSIG erfasse ausschließlich personenbezogene Daten.[183] Eine Information ist danach jede Nachricht unabhängig von ihrer Form („Sprache, Text, Bild oder sonstiges Datum").[184] Ein von dieser Definition der Informationstechnik von vornherein verschiedenes Begriffsverständnis lässt sich dem Urteil des *BVerfG* nicht entnehmen. *Hoffmann-Riem*, Berichterstatter des gegenständlichen Urteils des *BVerfG*, weist darauf hin, dass das Gericht den Begriff des informationstechnischen Systems der informationstechnischen Literatur entnommen habe.[185] Es liegt damit nahe, auf das BSIG als maßgebliche gesetzliche Grundlage derjenigen staatlichen Einrichtung zurückzugreifen, deren Aufgabe die Förderung der Sicherheit in der Informationstechnik ist (§ 3 Abs. 1 S. 1 BSIG).

---

[180] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 115; *Gola/Schomerus*, BDSG, § 3 Rn. 26.
[181] RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84).
[182] RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84).
[183] RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84).
[184] RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84).
[185] *Hoffmann-Riem*, JZ 2008, 1009 (1012).

(b) Systembegriff

Sodann bleibt zu untersuchen, welche informationstechnischen Gestaltungen ein gleichnamiges „System" darstellen. Das *BVerfG* hat zwar keine enumerative Aufzählung derjenigen informationstechnischen Systeme vorgenommen, die vom Schutzbereich des *GVIiS* erfasst werden. Es fehlt umgekehrt aber auch gerade eine abstrakte Definition. In der Informatik lässt sich unter einem System die Zusammenfassung mehrerer Komponenten zu einer als Ganzes aufzufassenden Einheit verstehen.[186] Diese Definition bietet sich für die Anwendung auf das gegenständliche Urteil vor allem deshalb an, weil sie eine abstrakte Betrachtung eines bestimmten Kontexts ermöglicht, ohne auf dessen Inhalt oder konkrete technische Gestaltungen eingehen zu müssen. Eine solche Betrachtung löst sich von den vom *BVerfG* aufgezählten Beispielen und ermöglicht unter Berücksichtigung von Gemeinsamkeiten eine entwicklungsoffene Begriffsbestimmung.

Ein System wird als offen bezeichnet, wenn es von seiner Umgebung beeinflusst wird und auf diese reagiert.[187] Der Zustand des Systems wiederum beschreibt vollständig einen speziellen Ausschnitt des Systems zu einem gegebenen Zeitpunkt.[188] Kann das System überabzählbar viele Zustände annehmen, ist es kontinuierlich.[189] Diese allgemeinen Merkmale des Systembegriffs können hier nun durch die Kombination mit dem Begriff der Informationstechnik konkretisiert werden. Damit wären die einzelnen Systemkomponenten *solche technischen Mittel, die der Verarbeitung und Übertragung von Informationen dienen*.[190] Die vom Schutzbereich des *GVIiS* erfassten informationstechnischen Systeme können dabei nur offene Systeme i.S.d. oben genannten Definition sein. Als Ausprägung des allgemeinen Persönlichkeitsrechts reagiert der Schutzbereich des *GVIiS* auf die Bedeutung, die informationstechnische Systeme für die Persönlichkeitsentfaltung des Einzelnen erlangt haben.[191] Diese persönlichkeitsrechtliche Bedeutung stellt sich wiederum in der Nutzung informationstechnischer Systems dar. So liegt es etwa bei der Nutzung des PCs für die „umfassende Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten" oder in „vielfältiger Form als Unterhaltungsgerät".[192] Informationstechnische Systeme würden nach den „gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum

---

[186] *Fischer/Hofer*, Lexikon Informatik, Stichwort „System"; *Duden*, Informatik A-Z, Stichwort „System".

[187] *Duden*, Informatik A-Z, Stichwort „System".

[188] *Duden*, Informatik A-Z, Stichwort „System".

[189] *Duden*, Informatik A-Z, Stichwort „System".

[190] Zu eng ist hingegen insbesondere vor dem Hintergrund, dass das *BVerfG* ausdrücklich auch von dem Internet als informationstechnischem System spricht (*BVerfGE* 120, 274 (276)), die Begrenzung der Definition des informationstechnischen Systems von *Herrmann*, IT-Grundrecht, S. 121, auf „Geräte"; *Wegener/Muth*, JURA 2010, 847 (849), begründen die weite Beschreibung des informationstechnischen Systems mit der Auslagerung personenbezogener Daten ins Internet, so dass ein an einem konkreten Gerät festgemachter Grundrechtsschutz keinen Sinn ergäbe.

[191] *BVerfGE* 120, 274 (303).

[192] Hierzu *BVerfGE* 120, 274 (304).

Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild oder Tondateien, genutzt".[193] Der auf einem System verfügbare Datenbestand könne „detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen".[194] Die persönlichkeitsrechtliche Relevanz der Nutzung informationstechnischer Systeme kann sich dementsprechend jedoch nur dann ergeben, wenn das System Eingaben des Nutzers entgegennimmt, verarbeitet und ihm ein entsprechendes Ergebnis liefert, mithin ein Informationsfluss mit der Umgebung des Systems möglich ist. Der Betroffene muss das informationstechnische System überhaupt „als eigenes"[195] nutzen können.

Nimmt man hingegen die Diskussion um die sog. *Online-Durchsuchung* als Ausgangspunkt für die Definition des *GVIiS*, so stellt sich die Frage, ob zusätzlich ein besonderes Konnektivitätserfordernis begriffsbildend vorausgesetzt wird. Das *BMI* versteht unter der Online-Durchsuchung „die verdeckte Suche unter Einsatz elektronischer Mittel nach verfahrensrelevanten Inhalten auf informationstechnischen Systemen […], die sich nicht im direkten physikalischen Zugriff der Sicherheitsbehörden befinden, aber über Kommunikationsnetze erreichbar sind".[196] Die Gesetzesbegründung zu § 20k Abs. 1 BKAG sieht das „Kopieren bestimmter Dateien von der Festplatte eines Rechners und deren elektronische Übertragung an das BKA"[197] vor. In beiden Fällen erfordert die Durchführung einer Online-Durchsuchung die Einbindung des betroffenen informationstechnischen Systems in ein Kommunikationsnetz. Gegen ein besonderes Konnektivitätserfordernis spricht aber die Abgrenzung, die das *BVerfG* hinsichtlich des Schutzbereichs des *GVIiS innerhalb* des Begriffs des informationstechnischen Systems vornimmt. Außen vor bleiben Systeme, die nach ihrer „technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen" enthalten.[198] Als Beispiel nennt das BVerfG hier „nicht vernetzte elektronische Steuerungsanlagen der Haustechnik".[199] Solche Systeme werden vom *BVerfG* zwar vom Schutzbereich des *GVIiS* ausgenommen, aber ebenfalls unter den Begriff des informationstechnischen Systems gefasst. Der Schutzbereich des *GVIiS* beschränkt sich auf solche Systeme, die „*allein* oder in ihren technischen Vernetzungen personenbezogene Daten in einem Umfang und in einer Vielfalt enthalten können", dass ein Zugriff auf das informationstechnische System ein umfassendes

[193] *BVerfGE* 120, 274 (322f.).
[194] *BVerfGE* 120, 274 (323).
[195] *BVerfGE* 120, 274 (315).
[196] Antwort des *BMI* vom 22.8.2007 auf den Fragenkatalog des *BMJ* (Fn. 14), S. 2.
[197] BT-Drucks. 16/9588, S. 26.
[198] *BVerfGE* 120, 274 (313).
[199] *BVerfGE* 120, 274 (313).

Persönlichkeitsbild des Nutzers ermöglicht.[200] Dieser potentielle Datenbestand ergibt sich aber gerade nicht zwingend nur aus der Vernetzung des Systems. Letztere ist damit nicht begriffsbildend für das informationstechnische System, sondern trägt nur innerhalb der zweistufigen Eröffnung des Schutzbereichs zur besonderen Gefährdungslage der Profilbildung bei. Ferner können in den Schutzbereich des Art. 13 Abs. 1 GG eingreifende Überwachungsmaßnahmen „auch ein System betreffen, das offline arbeitet".[201] Ein über die Eigenschaft der Offenheit des Systems hinausgehendes Konnektivitätserfordernis lässt sich damit nicht ausmachen. Da sich die Zustände der einzelnen Komponenten eines solchen informationstechnischen Systems in Abhängigkeit von dieser Nutzung ständig ändern, etwa durch die Installation- und Deinstallation von Software oder sonst durch die Veränderung des Datenbestands, sind die vom *GVIiS* erfassten informationstechnischen Systeme auch kontinuierlich i.S.d. oben genannten Definition.

(4) Zwischenergebnis

Der Begriff des informationstechnischen Systems, wie ihn das *GVIiS* namensgebend verwendet, kann danach definiert werden als

> *eine abgrenzbare Zusammenfassung zusammenwirkender technischer Komponenten, welche die Fähigkeit zur Erzeugung, Verarbeitung und Speicherung von Daten besitzt und die Interaktion mit einem menschlichen Nutzer und mit weiteren technischen Komponenten zulässt.*

Die Bestimmung des Schutzgegenstands hängt damit wiederum auch von der betrachteten technischen Ebene ab. So kann der einzelne PC in einem Netzwerk Komponente sein, wenn es um das System eines *Netzwerks* geht. Er ist aber zugleich auch ein selbständiges informationstechnisches System, dessen Elemente die Hard- und Softwarekomponenten des PCs darstellen. Eine solche Differenzierung nimmt auch das *BVerfG* vor. Es beschreibt das Internet als elektronischen Verbund von Rechnernetzwerken.[202] Nicht nur diese Netzwerke seien informationstechnische Systeme, sondern auch das Internet selbst. Peripheriegeräte erweitern ein System und stellen durch ihre Verbindung danach ebenfalls Komponenten dieses Systems dar. So wird etwa der an einen PC angeschlossene USB-Stick zur Komponente des informationstechnischen Systems eines auf diese Weise erweiterten *PCs*.

[200] *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).
[201] *BVerfGE* 120, 274 (310).
[202] *BVerfGE* 120, 274 (276).

Er stellt aber für sich gesehen mangels eigener Fähigkeit zur Verarbeitung oder Übertragung von Informationen kein informationstechnisches System dar.[203] Weiter ist die Gewährleistung der Vertraulichkeit und Integrität nicht auf solche informationstechnischen Systeme begrenzt, deren Komponenten in einem abgrenzbaren körperlichen Gegenstand enthalten sind. Das *BVerfG* nimmt eine solche konstruktionsbedingte Einschränkung gerade nicht vor, wenn es auch das Internet ausdrücklich unter den von ihm gebrauchten Begriff des informationstechnischen Systems fasst. Eine Begrenzung der Betrachtungsebene setzen allein die notwendige Fähigkeit des Systems zur Erzeugung, Verarbeitung und Speicherung von Daten. Der Rückgriff auf die vorgenannten Begrifflichkeiten der Informatik findet sich auch bei *Eckert*. Dort werden informationstechnische Systeme als geschlossene oder offene, dynamische technische Systeme mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen beschrieben.[204] Die Informationen werden dabei wiederum durch Daten oder Datenobjekte repräsentiert. Bei der Erörterung technischer Fragen des Schutzbereichs des *GVIiS* verwenden auch *Hansen/Pfitzmann* einen weiten Begriff des informationstechnischen Systems. Dieser umfasse alle elektronischen Geräte, in denen Daten in digitaler Form verarbeitet oder gespeichert werden.[205] In der Beschränkung auf „Geräte" kommt hingegen nicht der vom *BVerfG* gewählte weite Begriffsansatz zum Ausdruck. Diesem entspricht eher die Beschreibung des informationstechnischen Systems als eine spezielle IT-Installation mit einem definierten Zweck und einer bekannten Einsatzumgebung, die sich im Allgemeinen aus mehreren Hardware- und Software-Komponenten zusammensetzt.[206]

v. Datum und Information

Dem Begriff des personenbezogenen Datums kommt für die Beschreibung des sachlichen Schutzbereichs des *GVIiS* nicht diejenige Bedeutung zu, die er hierfür bei der Anwendung des *RiS* hat. Der Begriff stellt nicht den zentralen Schutzgegenstand der Persönlichkeitsentfaltung dar. Er dient lediglich als Anknüpfungspunkt für das Bestehen einer schützenswerten technischen Persönlichkeitssphäre. Das *BVerfG* verwendet den Begriff des personenbezogenen Datums, um die Persönlichkeitsrelevanz der Nutzung eines informationstechnischen Systems auszu-

---

[203] *T. Böckenförde*, JZ 2009, 921 (925 Fn. 41); *Hornung*, CR 2008, 299 (303); so auch *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (127 Fn. 120), nach dem jedoch mit Anschluss externer Speichermedien ein vernetztes System entsteht. Nach dem hier angewandten Begriffsverständnis wird das Speichermedium dagegen Teil eines durch die Verbindung entstehenden Systems; ebenso *T. Böckenförde*, JZ 2009, 921 (925 Fn. 41).

[204] *Eckert*, IT-Sicherheit, Ziff. 1.1 S. 4.

[205] *Hansen/Pfitzmann*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 131 (149).

[206] *Information Technology Security Evaluation Criteria* (ITSEC), S. 7 Ziff. 1.4 (abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile).

drücken. In den Schutzbereich des *GVIiS* fallen nur solche informationstechnischen Systeme, die

> „[…] *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*“.[207]

(1) Der Begriff des personenbezogenen Datums

§ 3 Abs. 1 BDSG definiert den Begriff der personenbezogenen Daten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Einzelangabe kann dabei jede Information sein.[208] Die Legaldefinition des § 3 Abs. 1 BDSG unterscheidet damit genauso wenig zwischen Daten und Informationen[209] wie diejenige der Informationstechnik des § 2 Abs. 1 BSIG. Dessen Gesetzesbegründung weist ausdrücklich auf eine beabsichtigte Parallele der im BSIG verwendeten Begrifflichkeiten zur datenschutzrechtlichen Terminologie hin.[210] Beiden Gesetzen liegt damit ein identisches Verständnis des Begriffs des personenbezogenen Datums zugrunde. Die Unterschiede der verwendeten Begrifflichkeiten bedeuten nicht auch einen Unterschied in der Erfassung persönlichkeitsrechtlicher Gefährdungen.

Mitunter wird zwischen Daten und Informationen dergestalt unterschieden, dass Informationen als „bei den Empfängern oder in Kommunikationssystemen gebildete Sinngehalte“ verstanden werden,[211] während Daten eine „stabile und eindeutige, gewissermaßen zeit- und kontextlose Bedeutung“, mithin einen interpretationsfreien Sinn hätten.[212] Daten als die bloßen Zeichen auf einem Datenträger seien danach nicht identisch mit Informationen, sondern dadurch gekennzeichnet, dass den zugrunde liegenden Daten eine Bedeutung zugewiesen werde.[213] Der Informationsgehalt, den Daten gewinnen, werde damit immer erst durch interpretative Leistungen in sozialen Situationen erzeugt.[214] Daten als solche würden noch keine Informationen ausmachen, sondern müssten vielmehr aufgegriffen und über eine Deutungs- und Rekonstruktionsleistung verstanden

---

[207] *BVerfGE* 120, 274 (314).

[208] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 5; *Gola/Schomerus*, BDSG, § 3a Rn. 3; *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 3 Rn. 21; Taeger/Gabel-*Buchner*, § 3 BDSG Rn. 4.

[209] Siehe auch *Bäcker*, Der Staat [2012], 91 (92f.).

[210] RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84).

[211] *Hoffmann-Riem*, JZ 2008, 1009 Fn. 2.

[212] *Vesting*, in: *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle* (Hrsg.), Grundlagen Verwaltungsrecht, Bd. II, § 20 Rn. 11f.

[213] *Hoffmann-Riem*, in: *Ders./Schmidt-Aßmann* (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, S. 9 (12).

[214] *Albers*, Informationelle Selbstbestimmung, S. 89.

werden.[215] Informationen seien daher interpretierte Daten.[216] Somit dürften die aus Daten gewonnenen Informationen nicht mit dem Datum und ihrer Vergegenständlichung auf dem jeweiligen Datenträger verwechselt werden.[217]

Die auf einem informationstechnischen System gespeicherten Daten werden aber gerade wegen der mit ihnen transportierten Informationen geschützt.[218] Denn der Schutz von Informationen setzt den Schutz der jeweiligen Daten voraus, durch welche diese Informationen im System repräsentiert werden.[219] Auch die EG- Datenschutzrichtlinie[220] differenziert nicht in dieser Form zwischen Daten und Informationen, wenn dort in Art. 2 Ziff. a) personenbezogene Daten als alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person") definiert werden.

Der Definition der Informationstechnik in § 2 Abs. 1 BSIG wurde ausdrücklich das Begriffsverständnis des *BVerfG* zur Datenverarbeitung aus dem *Volkszählungsurteil* zugrunde gelegt[221]. Darin definiert das Gericht personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person"[222]. Hierbei wird auf die insofern übereinstimmende Definition in § 2 Abs. 1 BDSG 1977[223] verwiesen, die sich mittlerweile in § 3 Abs. 1 BDSG findet. In dem hier gegenständlichen Urteil wird der Begriff der personenbezogenen Daten nicht definiert, sondern sein Inhalt als bekannt vorausgesetzt. Der Gegenstand der Verfahren führt jedoch wiederum zur Begriffsdefinition des BDSG. Gem. § 28 VSG NRW 2007 finden bei der Erfüllung der Aufgaben nach § 3 VSG NRW 2007 durch die Verfassungsschutzbehörde grds. die Vorschriften des *Datenschutzgesetzes Nordrhein-Westfalen* (DSG NRW)[224] Anwendung. § 3 Abs. 1 DSG NRW definiert den Begriff der personenbezogenen Daten in Übereinstimmung mit dem *BVerfG* und dem BDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Gem. § 5 Abs. 1 VSG NRW 2007 darf die Verfassungsschutzbehörde die zur Erfüllung ihrer Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten verarbeiten. Gleichfalls dürfen gem. § 7 Abs. 1 VSG NRW 2007 zur Aufgabenerfüllung personenbezogene Daten mit den Mitteln

---

215 *Albers*, Informationelle Selbstbestimmung, S. 90.

216 Roßnagel/*Trute*, Hdb. Datenschutzrecht, Ziff. 2.5 Rn. 18.

217 *Vesting*, in: *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle* (Hrsg.), Grundlagen Verwaltungsrecht, Bd. II, § 20 Rn. 14-17.

218 Vgl. *Hoffmann-Riem*, JZ 2008, 1009 Fn. 2.

219 *Eckert*, IT-Sicherheit, S. 4 Ziff. 1.1.

220 Richtlinie 95/46/EG des *Europäischen Parlaments* und des *Rates* vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23.11.1995, S. 0031 - 0050.

221 RegE zum BSIG in der Fassung v. 22.12.1989, abgedruckt in DuD 1990, 81 (84).

222 *BVerfGE* 65, 1 (42).

223 *Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung* (*Bundesdatenschutzgesetz* - BDSG) vom 27.1.1977, BGBl. I 1977, S. 201.

224 *Datenschutzgesetz Nordrhein-Westfalen* (DSG NRW) vom 9.6.2000, GV NRW 2000, S. 542.

gemäß § 5 Abs. 2 VSG NRW 2007 erhoben werden. Diese Mittel umfassen damit auch den in § 5 Abs. 2 Nr. 11 VSG NRW 2007 geregelten heimlichen Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Somit wird für denselben Sachverhalt sowohl innerhalb der Gesetzessystematik des VSG NRW 2007 und DSG NRW als auch vom *BVerfG* in den Verfahren gegen die Vorschriften des VSG NRW 2007 der Begriff des personenbezogenen Datums verwendet. Das Verständnis des verwendeten Datenbegriffs orientiert sich somit am Begriff der personenbezogenen Daten des § 3 Abs. 1 BDSG.
Das *BVerfG* verwendet in seinen Ausführungen den Begriff der personenbezogenen Daten, ohne Abweichungen von der Definition des BDSG festzustellen. Damit weist der verfassungsrechtliche Begriff der personenbezogenen Daten keine Besonderheiten gegenüber dem einfachgesetzlichen Begriff auf.[225] Die Auslegung des Begriffs der Daten als Gegenstand der Funktionen eines informationstechnischen Systems wird folglich anhand der Definition der personenbezogenen Daten gem. § 3 Abs. 1 BDSG vorgenommen.

(2) Einzelbetrachtung des Begriffs der personenbezogenen Daten i.S.d. § 3 Abs. 1 BDSG

(a) Einzelangaben

Einzelangabe kann zunächst jede Information sein.[226] Herkunft und Ausgestaltung der Information sind dabei nicht relevant.[227] Gleiches gilt für die Form der Repräsentation (natürliche Sprache, formalisierte Sprache, maschinenlesbarer Code, vereinbarte oder allgemein bekannte Zeichensprache) und die Darstellung der Zeichen (analog, digital, numerisch, alphanumerisch).[228] Auf die Art des Datenträgers und die Mittel der Verarbeitung kommt es somit nicht an.[229]

(b) Persönliche oder sachliche Verhältnisse

Diese Informationen müssen sich auf persönliche oder sachliche Verhältnisse der natürlichen Person beziehen. Ein Datum muss damit Informationen über den Betroffenen selbst oder über einen auf ihn beziehbaren Sachverhalt enthalten.[230] Die Unterscheidung zwischen persönlichen und sachlichen Verhältnissen ist dabei praktisch und rechtlich unerheblich.[231] Denn die Vorschrift soll alle Informationen unabhängig von Aspekt und betroffenem Lebensbereich erfassen.[232] Angaben

[225] So auch *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 175; *Vogelgesang*, Informationelle Selbstbestimmung, S. 25.
[226] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 5.
[227] *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 79 Ziff. C. I.
[228] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 4.
[229] Däubler/Klebe/Wedde/*Weichert*, BDSG, § 3 Rn. 16.
[230] *Gola/Schomerus*, BDSG, § 3 Rn. 5; Däubler/Klebe/Wedde/*Weichert*, BDSG, § 3 Rn. 19.
[231] *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 3 BDSG Rn. 23.
[232] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 7.

über persönliche Verhältnisse sind Angaben über den Betroffenen selbst, seine Identifizierung und Charakterisierung,[233] persönliche Tatsachen, Eigenschaften, Errungenschaften oder Vorlieben.[234] Erfasst sind etwa Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Beruf, Erscheinungsbild, Aussehen, Gesundheitszustand, Überzeugungen.[235] Sachliche Verhältnisse enthalten einen auf den Betroffenen beziehbaren Sachverhalt.[236] Dies können etwa Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen und alle sonstigen Beziehungen zu Dritten und zur Umwelt sein.[237] Der Begriff der personenbezogenen Daten nach § 3 Abs. 1 BDSG umfasst damit alle Informationen über eine natürliche Person, unabhängig davon, auf welchen Aspekt der betroffenen Person Bezug genommen wird.[238]

(c) Natürliche Person

Auf eine Einbeziehung juristischer Personen oder nichtrechtsfähiger Personengruppen hat der Gesetzgeber trotz Feststellung eines Schutzbedürfnisses gegenüber dem Informationsinteresse Dritter bewusst verzichtet.[239] Personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG können somit nur solche Angaben sein, die sich auf natürliche Personen beziehen. Die fehlende Einbeziehung juristischer Personen in den Begriff des personenbezogener Datums steht jedoch nicht in Zusammenhang mit der generellen Ablehnung der wesensmäßigen Anwendbarkeit des *RiS* auf juristische Personen i.S.d. Art. 19 Abs. 3 GG.

(d) Personenbezug

Personenbezogen ist ein Datum, wenn die Information einer Person zugeordnet werden kann.[240] Bestimmt ist die Person, wenn sich aus den Daten unmittelbar die Identität der natürlichen Person ergibt.[241] Hierfür kann es ausreichen, dass die Daten mit dem Namen der Person versehen sind, wenn innerhalb des in Betracht kommenden Personenkreises nur eine Person mit diesem Namen existiert und somit keine weiteren Angaben zur Herstellung des Personenbezugs erforderlich sind.[242] Der erforderliche Personenbezug kann aber auch darin bestehen, dass die Person bestimmbar ist. Bestimmbar ist eine Person dann, wenn sie zwar nicht

---

233 *Gola/Schomerus*, BDSG, § 3 Rn. 6.
234 *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 3 BDSG Rn. 24.
235 *Gola/Schomerus*, BDSG, § 3 Rn. 6.
236 *Gola/Schomerus*, BDSG, § 3 Rn. 7.
237 *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 80 Ziff. C. I. 1.
238 Roßnagel/*Tinnefeld*, Hdb. Datenschutzrecht, Ziff. 4.1 Rn. 18.
239 RegE BDSG, BT-Drucks. 7/1027, S. 19 Ziff. 3.9.4.
240 *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 3 Rn. 20.
241 *Gola/Schomerus*, BDSG, § 3 Rn. 10; Roßnagel/*Tinnefeld*, Hdb. Datenschutzrecht, Ziff. 4.1 Rn. 18; *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 80 Ziff. C. I. 2.
242 *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 22.

allein durch die Daten eindeutig identifiziert werden, die Identität aber mit Hilfe weiterer Informationen festgestellt werden kann.[243]

Dabei ist die weitere Auslegung des Begriffs der Bestimmbarkeit streitig:[244] Wird von einem relativen Begriff des Personenbezugs ausgegangen,[245] kann die Frage nach der Bestimmbarkeit eines Datums nicht allein aus der Angabe selbst abgeleitet werden, sondern hängt von den dem Datenverwender zur Verfügung stehenden Ressourcen sowie seinem jeweiligen Zusatzwissen ab.[246] Es kommt dann auf die Kenntnisse, Mittel und Möglichkeiten der verarbeitenden Stelle an.[247] Diese müsse den Personenbezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand herstellen können.[248]

Nach der Gegenansicht, die auf eine objektiv Bestimmung abstellt,[249] ergibt sich der Personenbezug ohne Rücksicht auf Kenntnisse, Mittel und Möglichkeiten der datenverarbeitenden Stelle allein aus der objektiven Eignung des Inhalts der Daten, den Personenbezug herzustellen.[250] Entscheidend sei, ob die realistische Möglichkeit besteht, die Daten ohne unzumutbaren Aufwand auf eine natürliche Person zu beziehen.[251] Ausreichend sei daher, dass der Personenbezug nur unter Mitwirkung eines Dritten hergestellt werden könnte,[252] mithin nicht die speichernde wohl aber eine andere Stelle über die Zuordnungsmöglichkeiten zu einem Pseudonym verfügt.[253] Lediglich wenn eine Zuordnung nur nicht mehr oder nur

---

243 *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 21; Roßnagel/*Tinnefeld*, Hdb. Datenschutzrecht, Ziff. 4.1 Rn. 22; *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 81 Ziff. C. I. 2.

244 Differenzierend dagegen Taeger/Gabel-*Buchner*, § 3 BDSG Rn. 13: Maßgeblich seien sowohl objektive als auch subjektive Kriterien, so dass die Bestimmbarkeit zunächst relativ aus der Perspektive der datenverarbeitenden Stelle, jedoch die Frage, welches Wissen für diese „verfügbar" ist, nach objektiven Kriterien zu bestimmen sei; Art. 4 Nr. 1 DS-GVO-E stellt für die Bestimmbarkeit auf Mittel ab, die der Datenverarbeitende „nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde"; dem Wortlaut der Norm lässt sich damit weder ein allein absoluter noch relativer Ansatz eindeutig entnehmen; hierzu ausführlicher *Schneider/Härting*, ZD 2012, 199 (200); *Härting*, BB 2012, 459 (463); *Lang*, K&R 2012, 145 (146).

245 *LG Frankenthal*, MMR 2008, 687 (689); *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 32; *Gola/Schomerus*, BDSG, § 3 Rn. 10; *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 3 BDSG Rn. 16; Roßnagel/*Tinnefeld*, Hdb. Datenschutzrecht, Ziff. 4.1 Rn. 22; *Eckhardt*, K&R 2007, 602; *Moos*, K&R 2008, 137 (139); *Roßnagel/Scholz*, MMR 2000, 722 (723).

246 Roßnagel/*Tinnefeld*, Hdb. Datenschutzrecht, Ziff. 4.1 Rn. 22.

247 *Gola/Schomerus*, BDSG, § 3 Rn. 10.

248 *Gola/Schomerus*, BDSG, § 3 Rn. 10; *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 3 BDSG Rn. 16.

249 Däubler/Klebe/Wedde/*Weichert*, BDSG, § 3 Rn. 13, 15; *Schaar*, Datenschutz im Internet, Rn. 153; *Pahlen-Brandt*, DuD 2008, 34 (37ff.); *dies*., K&R 2008, 287 (289).

250 *Pahlen-Brandt*, K&R 2008, 287 (291).

251 *Schaar*, Datenschutz im Internet, Rn. 153.

252 *Schaar*, Datenschutz im Internet, Rn. 153.

253 Däubler/Klebe/Wedde/*Weichert*, BDSG, § 3 Rn. 13.

mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft möglich ist, fehle es am Personenbezug.[254]

Bei dem Zugriff auf ein informationstechnisches System dürfte es auf diesen Streit regelmäßig nicht ankommen. Angesichts der hohen Persönlichkeitsrelevanz der Nutzung des Systems kommen zunächst bereits der Personenbezug aus den betroffenen Daten selbst und damit die Bestimmtheit des Betroffenen in Betracht. Daneben wird der Personenbezug angesichts des Umfangs und der Vielfalt des Datenbestands aus der Verknüpfung der einzelnen Daten für den infiltrierenden Dritten herstellbar sein. Schließlich wird der Zugriff auf das informationstechnische System aber vielfach auf eine gezielte Infiltration zurückgehen, so dass dem Dritten die Identität des Nutzers bekannt ist und er damit den Personenbezug der Daten ohne nennenswerten Aufwand herstellen kann.

(3) Einzelfälle

Personenbezogenes Datum ist die nicht anonyme E-Mail-Adresse.[255] Bei anonymen Adressen hingegen hängt der Personenbezug von der (mit vertretbarem Aufwand erlangbaren) Kenntnis des Klarnamens ab.[256] Personenbezogenes Datum kann auch schon die Bezeichnung einer Datei sein, in der Daten gespeichert sind, da sich aus der Dateibezeichnung regelmäßig die Selektionskriterien für die Aufnahme in die Datei ergeben.[257] Bei IP-Adressen[258] ist zu unterscheiden: Eine statische IP-Adresse ist ein personenbezogenes Datum, wenn das darüber identifizierte Endgerät einer natürlichen Person zugeordnet ist.[259] Bei dynamischen IP-Adressen kann der Access-Provider einen Personenbezug zwischen Adressen und Nutzer herstellen, solange er die jeweiligen Verbindungsdaten speichert und aufbewahrt.[260] In diesem Zeitraum lässt sich die zugewiesene IP-Adresse noch einem bestimmten Nutzungszeitraum und einem bestimmten Nutzer zuordnen.[261] Per-

[254] Däubler/Klebe/Wedde/*Weichert*, BDSG, § 3 Rn. 13.

[255] Vgl. *Härting*, CR 2008, 743 (748); Personenbezug ohne Differenzierung zwischen anonymer und nicht anonymer Adresse bejahend *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 3 BDSG Rn. 29.

[256] Näher zur Herstellung des Personenbezugs *Dammann*, in *Simitis* (Hrsg.), BDSG, § 3 Rn. 62.

[257] *Hess. VGH*, RDV 1991, 187 (188).

[258] Die IP-Adresse (Internet-Protocol-Adresse) ist eine rein numerische, in vier Gruppen zu 8 Bits (dezimal 0 bis 255) unterteilte 32-Bit-Kennung für den Anschluss von Gerätekomponenten aller Art (Arbeitsstation, Router, Server usw.) im TCP/IP-Netz (Internet) (*Fischer/Hofer*, Lexikon Informatik, Stichwort „IP-Adresse"). Lediglich zeitweilig im Netz befindliche Komponenten können sog. dynamische IP-Adressen zugewiesen werden, die bloß für die Dauer einer Verbindung die Adresse bilden. Dauerhaft mit dem Netz verbundene Komponenten besitzen gewöhnlich eine sog. statische IP-Adresse.

[259] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 63; Däubler/Klebe/Wedde/*Weichert*, BDSG, § 3 Rn. 14.

[260] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 63; *Härting*, CR 2008, 743 (745).

[261] Diese Differenzierung findet sich hingegen nicht in *EuGH* Urt. v. 24.11.2011 - C-70/10 - Scarlet/SABAM, GRUR 2012, 265, wo das Gericht IP-Adressen generell als personenbezogene Daten ansieht, da diese „die genaue Identifizierung der Nutzer ermöglichen".

sonenbezogene Daten können auch in sog. *Cookies*[262] enthalten sein. In einem Cookie abgelegte Informationen können ein bestimmtes Datum, Zugangspasswörter, Wiederaufsetzpunkte früherer Kommunikation, Layouteinstellungen besuchter Webseiten oder der virtuelle Warenkorb beim Einkaufen im Internet sein.[263] Diese Informationen können ausgelesen und nach ihrer Auswertung zu Nutzerprofilen zusammengefügt werden.[264] Allerdings kann der Inhalt eines Cookies bei der Abfrage durch einen Webserver regelmäßig nur der IP-Adresse des Nutzers zugeordnet werden. Die Zuordnung zu dem Nutzer selbst setzt voraus, dass dieser seinen Namen in ein Formular auf der Webseite eingibt und der Name anschließend in dem Cookie abgelegt wird.[265] Somit liegt ein Personenbezug jedenfalls dann vor, wenn der Cookie den Klarnamen des Nutzers selbst oder etwa in Form einer E-Mail-Adresse enthält.[266] Sofern der Cookie lediglich eine Ziffernkombination speichert, die der Identifikation des Cookies dient und dem Betreiber einer Website keine weiteren Informationen zur Verfügung stehen, kann der Betreiber nicht feststellen, wer der Besucher der Website ist, sondern nur, dass der jeweilige Nutzer die Seite bereits zuvor besucht hat.[267] Eine pauschale Beantwortung der Frage nach der Personenbezogenheit von Cookies ist somit nicht möglich, sondern es ist vielmehr der Inhalt des Cookie und die Möglichkeit der Verknüpfung mit anderen Daten zu berücksichtigen.[268] Mangels Informationsgewinnung auf einem *technisch* hierfür nicht dafür vorgesehenen Weg, ist die grundsätzliche Zulässigkeit des Anlegens und Auslesens von Cookies aber keine Frage eines Eingriffs in den Schutzbereich des *GVIiS*. Es fehlt insoweit an der Nutzung *versteckter* Informationskanäle.

(4) Von besonderer Relevanz für den Schutzbereich des GVIiS

Im Einzelnen benennt das *BVerfG* als Gegenstand der Funktionen eines informationstechnischen Systems „private Text-, Bild oder Tondateien", Daten mit „detaillierten Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen".[269] Ebenso betroffen sind „private Film- oder Tondokumente", „schriftliche Verkörperungen des höchstpersönlichen Erlebens" oder Inhalte von

---

[262] *Cookies* sind kleine Textdateien, wie sie durch gewisse Webserver generiert und auf dem Rechner des sie besuchenden Browsers installiert werden, um Verbindungsinformationen zu speichern und/oder die Interaktion beim Wiederbesuch zu beschleunigen (*Fischer/Hofer*, Lexikon Informatik, Stichwort „Cookie").

[263] *Wichert*, DuD 1998, 273 (274).

[264] *Schaar*, DuD 2000, 275; *ders.*, DuD 2001, 383 (384); *Ihde*, CR 2000, 413 (421).

[265] *Wichert*, DuD 1998, 273 (275).

[266] *Ihde*, CR 2000, 413 (416).

[267] *Meyer*, WRP 2002, 1028 (1030); *Lapp*, ITRB 2001, 113.

[268] *Meyer*, WRP 2002, 1028 (1030).

[269] *BVerfGE* 120, 274 (322f.).

„E-Mails oder anderen Kommunikationsdiensten des Internet“.[270] Des Weiteren kommen allgemein „Kommunikationsinhalte sowie Daten mit Bezug zur Netzkommunikation“[271] in Betracht. Dies betrifft die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich des Nutzers gespeicherten „Inhalte und Umstände einer Telekommunikation“.[272] Hinzu kommen Daten, die bei der Nutzung von Personalcomputern „für eine Vielzahl unterschiedlicher Zwecke“ anfallen, „etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät“.[273] Ebenso können „flüchtige oder nur temporär gespeicherte Daten“ (Cache-Speicher von Web-Browsern oder anderen Programmen, Passwörter) eine besondere Relevanz für die Persönlichkeit des Betroffenen aufweisen oder einen Zugriff auf weitere, besonders sensible Daten ermöglichen.[274]

vi. Ergebnis

Der vom *BVerfG* gebrauchte Begriff des informationstechnischen Systems lässt sich damit definieren als eine

> *abgrenzbare Zusammenfassung zusammenwirkender technischer Komponenten, welche die Fähigkeit zur Erzeugung, Verarbeitung und Speicherung von Daten besitzt und die Interaktion mit einem menschlichen Nutzer und mit weiteren technischen Komponenten zulässt.*

Diese Definition ist bewusst offen gestaltet, um entsprechend des Schutzzwecks des allgemeinen Persönlichkeitsrechts einer lückenschließenden Gewährleistung auch künftigen technischen Gestaltungen gerecht zu werden. Die begriffliche Weite kann als besonders zu berücksichtigende verfassungsrechtliche Vorgabe ausgemacht werden, die gegenüber den Begrifflichkeiten der informationstechnischen Literatur zu berücksichtigen ist. Für den Begriff der technischen Komponenten konnte auf § 2 Abs. 1 BSIG abgestellt werden. Der verwendete Datenbegriff greift auf den einfachgesetzlichen Begriff des § 3 Abs. 1 BDSG zurück. Die notwendigen Funktionen des informationstechnischen Systems ergeben sich aus den Gründen des gegenständlichen Urteils. Ein besonderes Konnektivitätserfordernis wird dort nicht begriffsbildend verwendet.

---

[270] *BVerfGE* 120, 274 (335f.).

[271] *BVerfGE* 120, 274 (305).

[272] *BVerfGE* 120, 274 (307); nach Beendigung des Übertragungsvorgangs bestehen hinsichtlich der bei einem Kommunikationsteilnehmer gespeicherten Daten dieser Kommunikation die spezifischen Gefahren einer räumlich distanzierten Kommunikation nicht mehr fort. Soweit der Teilnehmer eigene Schutzvorkehrungen gegen den ungewollten Datenzugriff treffen kann, sind diese Daten nicht von Art. 10 Abs. 1 GG geschützt (*BVerfGE* 115, 166 (184); 120, 274 (308)). Sie fallen in den Schutzbereich des *RiS* oder des *GVIiS*.

[273] *BVerfGE* 120, 274 (304).

[274] *BVerfGE* 120, 274 (324).

b. Zusätzliches Erfordernis der besonderen Gefährdungslage

i. Vorbemerkungen

Der Schutzbereich des *GVIiS* umfasst nicht ausnahmslos jedes informationstechnische System. Für die Eröffnung des Schutzbereichs wird neben dem Vorliegen eines informationstechnischen Systems als zweite Voraussetzung eine besondere Gefährdungslage für die Persönlichkeitsentfaltung des Betroffenen, in diesem Falle den Nutzer des informationstechnischen Systems, vorausgesetzt.[275] Das *BVerfG* umschreibt diese Gefährdungslage an verschiedenen Stellen:

> „*Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.* […] *In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeit des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen.*“[276]

Komplexe informationstechnische Systeme würden

> „*nach den gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt. Der verfügbare Datenbestand kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen. Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.*“[277]

Diese für die Eröffnung des Schutzbereichs des *GVIiS* erforderliche besondere Gefährdungslage ist vor allem im Rahmen der Abgrenzung des *GVIiS* zum *RiS* entscheidend:[278]

> „*Das Recht auf informationelle Selbstbestimmung trägt solchen Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist*

---

[275] *Herrmann*, IT-Grundrecht, S. 121 nimmt dieses Erfordernis dagegen bereits in die Definition des informationstechnischen Systems auf.

[276] *BVerfGE* 120, 274 (305).

[277] *BVerfGE* 120, 274 (323).

[278] *BVerfGE* 120, 274 (313).

> *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*."

Eine solche Persönlichkeitsgefährdung, die nicht mehr vom Schutzbereich des *RiS* erfasst wird, ist bei informationstechnischen Systemen gegeben,

> „*die alleine 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*".[279]

Diese Möglichkeit ergebe sich etwa bei einem PC aus der Auswertung des Nutzungsverhaltens, das regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen lasse.[280] Ebenfalls werde die spezifische Grundrechtsgefährdung aus den in vielfältiger Art erfassten und gespeicherten personenbezogenen Daten von Mobiltelefonen oder elektronischen Terminkalendern mit großem Funktionsumfang begründet.[281] Dementsprechend können herkömmliche klassische Mobiltelefone, deren Anwendungsbereiche ganz oder überwiegend auf das bloße Telefonieren oder den Versand von SMS beschränkt war, angesichts mangelnder Vielfältigkeit ihrer Nutzungsmöglichkeiten und der hierbei erfassten und gespeicherten Daten die angesprochene Gefährdungslage nicht begründen.[282] Moderne Smartphones jedenfalls, die in ihren Nutzungsmöglichkeiten dem klassischen PC kaum noch nachstehen, darüber hinaus aber auch zusätzliche Funktionen aufweisen können, sind angesichts ihrer zentralen Rolle im Alltagsleben vom Schutzbereich des *GVIiS* erfasst. Kernelemente der vom *BVerfG* ausgemachten besonderen Persönlichkeitsgefährdung sind damit die Möglichkeiten „weitreichender Rückschlüsse" auf die Persönlichkeit, u.U. sogar einer „Profilbildung" des Nutzers eines informationstechnischen Systems sowie eines Einblicks in „wesentliche Teile der Lebensgestaltung" oder der Gewinnung eines „aussagekräftigen Bildes der Persönlichkeit". Gerade die von dem *BVerfG* angesprochenen Beispiele informationstechnischer Systeme haben sich zu ständigen Begleitern des Einzelnen entwickelt. Die damit immer weiter fortschreitende Digitalisierung bedingt auch einen Wechsel der jeweiligen Informationsträger. Mit der Konzentration vielfältiger Nutzungsmöglichkeiten in einem Gegenstand werden zugleich auch in diesem

[279] *BVerfGE* 120, 274 (314).
[280] *BVerfGE* 120, 274 (314).
[281] *BVerfGE* 120, 274 (314).
[282] *Hornung* CR 2008, 299 (302).

Gegenstand die zugehörigen Informationen dieser Nutzungen gebündelt. So stellt das *BVerfG* fest, dass die jüngere Entwicklung der Informationstechnik dazu geführt habe, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.[283] Es drückt damit eine funktionale Abhängigkeit der Persönlichkeitsentfaltung von der Vertraulichkeit und Integrität informationstechnischer Systeme aus.[284] Die Festplatten zahlloser Personalcomputer würden in der heutigen Zeit ein „getreuliches Spiegelbild der persönlichen Interessen, Neigungen, der ökonomischen Situation sowie nicht zuletzt auch der physischen und psychischen Befindlichkeit ihrer Nutzer" bieten.[285] Die Vermittlungsleistung eines informationstechnischen Systems ermöglicht damit die Aggregation einzelner personenbezogener Daten zu einer „auf einmal und immer wieder zugänglichen, dynamischen Gesamtheit", die den Betroffenen bei unberechtigtem Zugang „in seiner persönlichen Lebensführung entblößen kann".[286] Diese „Akkumulation einer Vielzahl von Daten" werde in der modernen Informationsgesellschaft noch zunehmen.[287] Das *BVerfG* „zeichnet damit ein kritisches Bild, der Gefährdungslage, die durch die alltägliche, unausweichliche Nutzung der Informationstechnik entstanden ist".[288] Ein so gewonnenes teilweise oder weitestgehend vollständiges Persönlichkeitsbild kann von dem Betroffenen nicht ausreichend auf seine Richtigkeit und Verwendung kontrolliert werden, so dass durch die Möglichkeit eines Zugriffs auf das informationstechnische System auf den Einzelnen der psychische Druck öffentlicher Anteilnahme einwirkt.[289]

ii. Art, Umfang und Vielfalt der enthaltenen Daten

Der Umschreibung dieser besonderen Gefährdungslage lassen sich zugleich auch die Kriterien für deren Feststellung entnehmen. Dazu gehört zunächst die Art der gespeicherten Daten. Hierbei kommt wieder das Merkmal des Personenbezugs zum Tragen, um die persönlichkeitsrechtliche Relevanz der Nutzung des informationstechnischen Systems zu erfassen. Besonderer Aufmerksamkeit bedürfen weiter die Kriterien des Umfangs und der Vielfalt gespeicherter Daten. Denn vorrangiger und entscheidender Anknüpfungspunkt des Schutzbereichs des *GVIiS* ist die Komplexität eines informationstechnischen Systems in Bezug auf seine

283 *BVerfGE* 120, 274 (303).
284 Vgl. *Hornung*, CR 2008, 299 (302).
285 *Kutscha*, NJW 2008, 1042 (1043).
286 *T. Böckenförde*, JZ 2008, 925 (928).
287 *Sieber*, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen, S. 15.
288 So *Bartsch*, CR 2008, 613.
289 *BVerfGE* 120, 274 (305) unter Verweis auf *BVerfGE* 65, 1 (42).

Nutzungsmöglichkeiten. Schließlich gilt es zu untersuchen, inwieweit diese Gefährdungslage erst durch die Vernetzung des informationstechnischen Systems begründet werden kann.

(1) Art

Der Beschreibung der besonderen Gefährdungslage lässt sich zunächst entnehmen, welcher Art diejenigen Daten sein müssen, aus denen sich diese Gefährdungslage ergeben kann. In den Schutzbereich des *GVIiS* fallen informationstechnische 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*".[290]

Notwendige Eigenschaft der enthaltenen Daten ist daher zunächst diejenige des *Personenbezugs*. Diese Voraussetzung ist nach der Konzeption des *GVIiS* als Ausprägung des allgemeinen Persönlichkeitsrechts stimmig. Das *GVIiS* schützt die Persönlichkeitsentfaltung mittels der Nutzung informationstechnischer Systeme. Eine besondere Gefährdungslage für die *Persönlichkeitsentfaltung* des betroffenen Nutzers kann aber nur bei einer entsprechenden Relevanz der Nutzung für die Persönlichkeit des Nutzers bestehen. Weisen enthaltene Daten keinerlei Personenbezug auf, ist also der Betroffene nicht bestimmt oder bestimmbar, ist auch kein Einblick in „wesentliche Teile der Lebensgestaltung" oder „ein aussagekräftiges Bild der Persönlichkeit" zu gewinnen. Diese besondere Gefährdungslage lässt sich nur über personenbezogene Daten begründen.

(2) Umfang und Vielfalt

Jedoch ist der Schutzbereich des *GVIiS* nicht eröffnet, soweit ein informationstechnisches System nach seiner technischen Konstruktion lediglich Daten mit bloß punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen verarbeitet.[291] Eine besondere Persönlichkeitsgefährdung wird daher auch dann begründet, wenn entweder der Bezug zu einem einzigen Lebensbereich nicht bloß punktuell ist, oder der Bezug zwar nur punktuell ist aber mehrere Lebensbereiche umfasst. Hinsichtlich Datenumfang und -vielfalt ist auf die Nutzungsmöglichkeiten des informationstechnischen Systems abzustellen. Die vom *GVIiS* erfassten neuartigen Persönlichkeitsgefährdungen „ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind".[292] Soweit aber der

[290] *BVerfGE* 120, 274 (314).
[291] *BVerfGE* 120, 274 (313).
[292] *BVerfGE* 120, 274 (305).

Funktionsumfang eines informationstechnischen Systems schon konstruktiv derart begrenzt ist, dass lediglich Daten mit bloß punktuellem Bezug auf einen bestimmten Lebensbereich des Nutzers betroffen sind, führt dieser begrenzte Funktionsumfang dazu, dass Umfang und Vielfalt der betroffenen Daten lediglich eine solches Maß erreichen können, das es gerade nicht erlaubt, einen Einblick in „in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten". Mit der technischen Konstruktion des Systems wird dabei ein rein objektiver Anknüpfungspunkt gewählt. Entscheidend sind die konstruktionsbedingt möglichen Nutzungen des informationstechnischen Systems. Die subjektive Widmung des Nutzers bleibt außen vor. Unerheblich ist daher, ob der Betroffene den Funktionsumfang des informationstechnischen Systems auch tatsächlich ausschöpft. Dementsprechend stellt das *BVerfG* zu Recht nicht auf Umfang und Vielfalt des *tatsächlich vorhandenen* Datenbestands ab, sondern darauf, dass informationstechnische Systeme

> „*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.*"[293]

Der auf dem betroffenen System vorhandene Datenbestand muss den notwendigen Umfang und die notwendige Vielfalt, der eine besondere Gefährdungslage begründen kann, *nicht auch tatsächlich* aufweisen. Diese Voraussetzungen muss nur der Datenbestand erfüllen, der aufgrund der Nutzungsmöglichkeiten des informationstechnischen Systems denkbar anfallen kann:

> „*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.*"[294]

Für die Eröffnung des Schutzbereichs des *GVIiS* ist demnach weder die Erhebung personenbezogener Daten maßgeblich noch, inwieweit solche Daten überhaupt auf dem informationstechnischen System tatsächlich vorhanden sind.[295] Entscheidend sind allein die Speicher- und Verarbeitungs*kapazitäten* des betroffenen informationstechnischen Systems nicht aber sein *konkreter Dateninhalt*.[296] Das *BVerfG* begründet den „Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielzahl bei weitem übertreffen *kann*", gerade mit der „Vielzahl unterschiedlicher Nutzungsmöglichkeiten" komplexer informa-

---

[293] *BVerfGE* 120, 274 (314).
[294] *BVerfGE* 120, 274 (313).
[295] So auch *T. Böckenförde*, JZ 2008, 925 (928).
[296] *Hornung*, CR 2008, 299 (302); *Luch*, MMR 2011, 75 (76), setzt hingegen die Komplexität des informationstechnischen Systems mit der *enthaltenen* Datenmenge und -vielfalt gleich (Hervorhebungen nur hier).

tionstechnischer Systeme.[297] Diesem Ansatz ist zuzustimmen. Vertraulichkeit und Integrität eines informationstechnischen Systems sind schon dann aufgehoben, wenn dem Dritten nur der Zugriff auf das informationstechnische System möglich ist. Ab diesem Zeitpunkt hängt die Zugänglichkeit des Systems nicht mehr von dem Willen des Betroffenen ab. Die „technische Hürde", welche die Eröffnung des Schutzbereichs des *GVIiS* markiert, ist schon ab diesem Zeitpunkt genommen.[298]

(3) Kriterium der Vernetzung

Die besondere Gefährdungslage kann sich auch erst aus der „Vernetzung" des informationstechnischen Systems ergeben. Das *GVIiS* schützt auch solche Systeme, die erst durch ihre „*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".[299] Ein für sich gesehen wenig komplexes informationstechnisches System kann daher die für die Eröffnung des Schutzbereichs notwendige Komplexität auch durch die „Vernetzung" mit anderen informationstechnischen Systemen erreichen.[300] Eine inhaltliche Erläuterung erhält der Begriff der „Vernetzungen" nicht. Er soll aber jedenfalls die Verbindung eigenständiger informationstechnischer Systeme durch das Internet erfassen.[301] Entscheidend dürfte hierbei aber nicht ein erweiterter Datenbestand sein, sondern die Erweiterung des Funktionsumfangs des eigenen Systems.[302] Durch den erweiterten Funktionsumfang bieten sich dem Betroffenen zusätzliche Möglichkeiten der Persönlichkeitsentfaltung. Diese bedeuten aber zugleich auch einen vielfältigeren und erweiterten Einblick in seine persönliche Sphäre.

*2. Vertraulichkeit und Integrität*

Entscheidende Bedeutung für die Beschreibung des sachlichen Schutzbereichs des *GVIiS* kommt den Begriffen der Vertraulichkeit und Integrität zu. Es stellt sich hier jedoch wiederum das gleiche Problem wie bei der Erörterung des Begriffs des informationstechnischen Systems. Das *BVerfG* definiert auch die Begriffe der Vertraulichkeit und Integrität nicht abstrakt. Letzterer wird noch relativ fassbar mit der Überwindung technischer Zugriffshindernisse beschrieben. Die Ausfül-

297 *BVerfGE* 120, 274 (322) (Hervorhebung nur hier).
298 *BVerfGE* 120, 274 (314).
299 *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).
300 *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (127); *ders.*, in: *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (11).
301 *BVerfGE* 120, 274 (304).
302 Vgl. *BVerfGE* 120 274(305).

lung des Begriffs der Vertraulichkeit erschöpft sich demgegenüber in der Wiederholung des zugehörigen Adjektivs:[303]

> „*Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.*“

Der Berichterstatter des gegenständlichen Urteils, *Hoffmann-Riem*, verweist für den Begriff des informationstechnischen Systems auf dessen Bedeutung in der informationstechnischen Literatur.[304] Diese Verweisung vorausgesetzt sollte auch für die Auslegung der Begriffe der Vertraulichkeit und Integrität auf die informationstechnische Terminologie abgestellt werden.[305]

a. Bedeutung in der Informationstechnik

Der Vorläufer des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI), die *Zentralstelle für Sicherheit in der Informationstechnik* formulierte 1989 die „klassischen Sicherheitsziele“[306] der Informationstechnik:[307] Der *unbefugte Informationsgewinn* als Verlust der Vertraulichkeit, die *unbefugte Modifikation* von Informationen als Verlust der Integrität und die *unbefugte Beeinträchtigung der Funktionalität* als Verlust der Verfügbarkeit. Die *ITSEC* griffen diese Ziele bei ihrer Definition der IT-Sicherheit auf: Danach ist IT-Sicherheit die Kombination von Vertraulichkeit als *Schutz vor unbefugter Offenbarung* von Informationen, Integrität als *Schutz vor unbefugter Veränderung* der Informationen und Verfügbarkeit als Schutz vor *unbefugtem Vorenthalten* von Informationen oder Ressourcen.[308]

---

303 *BVerfGE* 120, 274 (314).

304 *Hoffmann-Riem*, JZ 2008, 1009 (1012 Fn. 26).

305 So auch *Bäcker*, in: *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (13); *Hansen/Pfitzmann*, in: *Roggan*, Online-Durchsuchungen, S. 131 (132); *Holznagel/Schumacher*, MMR 2009, 3; *Hornung*, CR 2008, 299 (303).

306 So *Amann/Atzmüller*, DuD 1992, 286 (287, 290).

307 Abrufbar unter: https://www.bsi-fuer-buerger.de/cae/servlet/contentblob/478190/publicationFile/30233/itgruend_pdf.pdf;jsessionid=5283809269D5E5CECB5E1049AABDC6EC.

308 *ITSEC*, Ziff. 0.2 S. 1.

i. Vertraulichkeit

Ein informationstechnisches System gewährleistet die Vertraulichkeit der enthaltenen Informationen, wenn es keine unautorisierte Informationsgewinnung ermöglicht.[309] Erforderlich sind hierfür die Festlegung von Berechtigungen und Kontrollen.[310] Vertraulichkeit bedeutet demnach, dass Informationen nur berechtigten Personen bekannt werden.[311] Berechtigt in diesem Sinne ist eine Person dann, wenn ihr gegenüber bewusst eine technische Zugriffsmöglichkeit eingerichtet wurde.[312]

ii. Integrität

Die Integrität der enthaltenen Daten gewährleistet ein informationstechnisches System, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.[313] Die enthaltenen Informationen müssen vollständig, richtig und aktuell sein oder es muss deutlich erkennbar sein, dass dies nicht der Fall ist.[314] Der Begriff der Integrität bezieht sich nicht nur auf die einzelnen auf einem informationstechnischen System enthaltenen Daten, sondern auch auf das informationstechnische System als Ganzes.[315] Denn die Integrität der Daten kann nur sichergestellt werden, wenn gleichfalls die ordnungsgemäße Übertragung oder Verarbeitung durch das informationstechnische System sichergestellt ist.

b. Inhaltliche Unterschiede in der Begriffsverwendung

Die sich aus dem Rückgriff auf die Informationstechnik ergebenden Auslegungsansätze sind sodann anhand des Schutzkonzepts zu präzisieren, das hinter der Formulierung des *GVIiS* steht. Das informationstechnische System wird aufgrund seiner Bedeutung als Mittel der Persönlichkeitsentfaltung geschützt. Mithin muss hinter der Auslegung der Begriffe der Vertraulichkeit und Integrität der Schutzzweck des allgemeinen Persönlichkeitsrechts stehen. Die sich so ergebenden inhaltlichen Unterschiede in der Begriffsverwendung werden im Folgenden aufgezeigt.

309 *Eckert*, IT-Sicherheit, Ziff. 1.2 S. 9f.
310 *Eckert*, IT-Sicherheit, Ziff. 1.2 S. 9f.
311 *Hansen/Pfitzmann*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 131 (132); *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 8.
312 *Hansen/Pfitzmann*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 131 (132).
313 *Eckert*, IT-Sicherheit, Ziff. 1.1 S. 9.
314 *Hansen/Pfitzmann*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 131 (132).
315 *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 7.

i. Informationstechnik

Die Schutzziele der Vertraulichkeit und Integrität präzisieren im informationstechnischen Zusammenhang die Beschränkung und Kontrolle des Zugriffs auf Informationen bzw. Daten als die zu schützenden Güter informationstechnischer Systeme.[316] Dabei stellt Informationssicherheit diejenige Eigenschaft eines funktionssicheren informationstechnischen Systems dar, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen.[317] Wird noch zwischen den Begriffen der Informationen und der Daten unterschieden, beschreibt Datensicherheit die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen.[318] Funktionssicherheit wiederum bildet die Grundlage für Informations- und Datensicherheit und lässt sich als diejenige Eigenschaft verstehen, dass die realisierte Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt.[319] Anhand der zur Bewertung der Sicherheit informationstechnischer Systeme entwickelten Kriterienkataloge[320] lässt sich angeben, inwieweit die Schutzziele der Vertraulichkeit und Integrität erreicht werden. Abhängig von den Unterschieden in den Sicherheitseigenschaften informationstechnischer Systeme weist der Grad an Vertraulichkeit und Integrität dieser Systeme entsprechende Unterschiede auf. Wegen der dynamischen Änderung von Systemeigenschaften ist die Sicherstellung der Informations- und Datensicherheit aber ein Prozess,[321] so dass IT-Sicherheit nicht als Konstante aufgefasst werden darf.[322] Die Begriffe der Vertraulichkeit und Integrität werden daher in ihrer informationstechnischen Bedeutung als Schutzziele für einen ganz bestimmten zu erreichenden Zustand verwendet. Die Übereinstimmung des tatsächlichen Zustands eines informationstechnischen Systems mit diesem zu erreichenden Zustand ist demnach abhängig von dessen Sicherheitseigenschaften. So verwenden etwa die *ITSEC* den Begriff der Vertraulichkeit als „Eigenschaft eines Objekts, die ausdrückt, *inwieweit* die unbefugte Offenlegung von Informationen verhindert werden kann“[323] und denjenigen der Integrität als „Eigenschaft eines Objekts, die ausdrückt, *inwieweit* unbefugte Änderungen von Informationen verhindert werden können“[324].

316 *Eckert*, IT-Sicherheit, Ziff. 1.2 S. 7.
317 *Eckert*, IT-Sicherheit, Ziff. 1.2 S. 6.
318 *Eckert*, IT-Sicherheit, Ziff. 1.2 S. 6.
319 *Eckert*, IT-Sicherheit, Ziff. 1.2 S. 6.
320 Siehe hierzu etwa *Eckert*, IT-Sicherheit, Ziff. 5 S. 231ff.
321 *Eckert*, IT-Sicherheit, Ziff. 1.1 S. 6.
322 *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 4.
323 *ITSEC*, Glossar, Ziff. 6.1.5, S. 112 (Hervorhebung nur hier).
324 *ITSEC*, Glossar, Ziff. 6.4.1. S. 114 (Hervorhebung nur hier).

ii. Individueller Zustand von Vertraulichkeit und Integrität

Hiervon unterscheidet sich die Verwendung der Begriffe der Vertraulichkeit und Integrität in der gegenständlichen Entscheidung in einem wichtigen Punkt. Das *GVIiS* stellt eine Ausprägung des allgemeinen Persönlichkeitsrechts dar, deren Schutzbereich auf die Nutzung der Informationstechnik für die Persönlichkeitsentfaltung ausgerichtet ist. Die Vertraulichkeit und die Integrität informationstechnischer Systeme werden daher nur insoweit geschützt, als sich mit diesen Begriffen die Persönlichkeitsrelevanz der Nutzung informationstechnischer Systeme erfassen lässt. Schutzzweck ist, dem Einzelnen die ungehinderte Persönlichkeitsentfaltung durch die Nutzung des informationstechnischen Systems zu ermöglichen. Der persönliche und private Lebensbereich soll vor einem staatlichen Zugriff im Bereich der Informationstechnik geschützt werden.[325] Diese Persönlichkeitsentfaltung setzt voraus, dass bestehende Möglichkeiten einer Einsicht- und Einflussnahme auf das Verhalten des Einzelnen nicht durch den psychischen Druck öffentlicher Anteilnahme einwirken.[326] Somit muss dieser darauf vertrauen können, dass das von ihm genutzte informationstechnische System so funktioniert, wie er dies berechtigterweise erwarten darf. Geschützt wird somit die berechtigte Erwartung des Betroffenen gegenüber der staatlichen Gewalt, dass er allein derjenige ist, der über den Zugang zu den von seinem System „erzeugten, verarbeiteten und gespeicherten Daten" und die Möglichkeit der Nutzung von dessen „Leistungen, Funktionen und Speicherinhalten" entscheidet. Er soll nicht wegen der Ungewissheit, inwieweit die persönlichkeitsrelevante Nutzung Gegenstand staatlicher Überwachungsmaßnahmen ist, von der Ausübung seiner grundrechtlich geschützten Freiheit abgehalten werden. Schutz besteht somit davor, dass ein *bestehender* Zustand von Vertraulichkeit und Integrität, deren Reichweite der Betroffene als Berechtigter im Sinne dieser Begriffe bestimmt, aufgehoben wird.

Das *BVerfG* gebraucht beide Begriffe dahingehend, dass die Eröffnung des Schutzbereichs des *GVIiS* nicht davon abhängig ist, dass informationstechnische Systeme einen ganz bestimmten Grad an Vertraulichkeit und Integrität aufweisen müssen, sondern dass Vertraulichkeit und Integrität unabhängig von der Reichweite der Erfüllung dieser informationstechnischen Schutzziele ein zu erhaltender Zustand sind. Das *GVIiS* „*bewahrt* den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik […]".[327] Sein Schutz ist mithin darauf gerichtet, „dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich *bleiben*"[328]. Ein Grundrechtseingriff liegt zudem dann vor, wenn die Integrität des geschützten informationstechnischen Sys-

[325] *BVerfGE* 120, 274 (313).
[326] *BVerfGE* 120, 274 (305) unter Verweis auf *BVerfGE* 65, 1 (42).
[327] *BVerfGE* 120, 274 (313) (Hervorhebung nur hier).
[328] *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).

tems *angetastet wird* […]".[329] „Bleiben" kann nur, was schon vorher bestand, ebenso wie nur ein bereits bestehender Zustand „angetastet" werden kann. Einen bestimmten Grad an Vertraulichkeit oder Integrität i.S.d. der Erfüllung bestimmter Bewertungskriterien muss das informationstechnische System des Betroffenen daher nicht aufweisen.[330] Der grundrechtliche Schutz informationstechnischer Systeme unterscheidet sich nicht danach, ob der Zugriff auf das System leicht oder nur mit erheblichem Aufwand möglich ist.[331]

Der Schutz eines bestehenden individuellen Zustands kommt weiter auch in der Beschreibung des Schutzbedürfnisses des Betroffenen zum Ausdruck. Der Einzelne sei darauf angewiesen sei, „dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung *berechtigten Erwartungen* an die Integrität und Vertraulichkeit derartiger Systeme *achtet*".[332] Es finden sich hier Übereinstimmungen mit dem Wortlaut des Art. 1 Abs. 1 S. 2 Alt. 1 GG überein, wonach bekanntlich alle staatliche Gewalt verpflichtet ist, die Würde des Menschen zu *achten*. In dieser Pflicht wird allgemein die *Abwehrdimension* der Menschenwürdegarantie gesehen, staatliche Eingriffe zu *unterlassen*.[333] Mit dieser Wortwahl des Gerichts liegt der Schwerpunkt des grundrechtlichen Schutzes deutlich stärker auf der Funktion des allgemeinen Persönlichkeitsrechts als Abwehrrecht auf „Respektierung des geschützten Bereichs" als seiner Funktion der Sicherung einer „aktiven […] Entfaltung"[334] der Persönlichkeit. Für die Nutzung informationstechnischer Systeme besteht damit das Bedürfnis des Betroffenen gerade in der Unterlassung der Infiltration und damit von Eingriffen bloß in seine *berechtigten Erwartungen* an die Vertraulichkeit und Integrität des Systems. Dann kann aber auch aus der Formulierung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kein „uneinlösbarer Schutzauftrag" folgen.[335] Denn geschützt ist nicht die umfassende Vertraulichkeit und Integrität des Sys-

---

[329] *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).

[330] Für ein solches Verständnis spricht auch die Einschätzung des Sachverständigen *Bogk*, Antworten Fragenkatalog (Fn. 163), S. 3, wonach aufgrund von Sicherheitsmaßnahmen wie Personal Firewalls, Virenscannern und automatischen Sicherheitsupdates ein Schutzniveau erreicht würde, bei dem auch ein durchschnittlicher PC nur noch mit erheblichem Aufwand kompromittiert werden könne. Zudem seien schon in der Standardkonfiguration alle auf einem PC gespeicherten Daten gegen das Auslesen durch Dritte geschützt, so dass es einer positiven Willensäußerung (Datenfreigabe zur gemeinsamen Nutzung, Hochladen der Datei auf einen öffentlich zugänglichen Server) durch den Nutzer bedürfe, um Dritten selektiv den Zugang zu ermöglichen. Im Regelfall sei daher davon auszugehen, dass die enthaltenen Daten vertraulich bleiben; i.d.S. auch *Bartsch*, CR 2008, 613 (616).

[331] So ausdrücklich *BVerfGE* 120, 274 (315).

[332] *BVerfGE* 120, 274 (306) (Hervorhebung nur hier).

[333] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 1 Abs. 1 Rn. 135; *Herdegen*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 1 Abs. 1 Rn. 75; *Zippelius*, in: BK GG, Bd. 1, Art. 1 Abs. 1, 2 Rn. 22 (Hervorhebung nur hier).

[334] *BVerfGE* 54, 148 (153); zu den unterschiedlichen Funktionen auch MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 133; *Ehmann*, JURA 2011, 437 (444); *Jarass*, NJW 1989, 857 (859).

[335] So aber *Lepsius*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 21 (55).

tems, sondern ein *individueller Zustand* hiervon als Ausdruck individueller Persönlichkeitsentfaltung. Das *GVIiS* verlangt somit nicht die Herstellung eines bestimmten Schutzniveaus, sondern schützt denjenigen Zustand der Vertraulichkeit und Integrität des informationstechnischen Systems des Betroffenen, den dieser anhand seiner Kontrolle über den Zugriff auf das System selbstbestimmt herstellt. Hierin kommt die individuelle Selbstbestimmung des Einzelnen als Schutzgut des allgemeinen Persönlichkeitsrechts zum Ausdruck, die im *Volkszählungsurteil* speziell hinsichtlich der Offenbarung persönlicher Lebenssachverhalte bemüht wurde.[336]

iii. Weitergehende Schutzziele

Der Gegenstand von Vertraulichkeit und Integrität ist das informationstechnische System. Dies folgt schon aus der Bezeichnung des Grundrechts. Der Begriff der Integrität geht dabei über die Formulierung eines Schutzziels zum Erreichen von Datensicherheit hinaus. Neben den „Speicherinhalten" eines informationstechnischen Systems werden auch „Leistungen"[337] und „Funktionen" geschützt. Der für die Beschreibung des sachlichen Schutzbereichs des *GVIiS* gebrauchte Begriff der Integrität erfasst schon den Zugriff auf das System selbst, mit dem eine „Ausspähung, Überwachung oder Manipulation" ermöglicht wird. Das *GVIiS* schützt insoweit den Lebensbereich des Betroffenen „auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten".[338]

c. Zwischenergebnis

Die für die Beschreibung des Schutzbereichs des *GVIiS* entscheidenden Begriffe der Vertraulichkeit und Integrität orientieren sich inhaltlich an ihrer Bedeutung in der Informationstechnik. Der entscheidende Unterschied liegt darin, dass das *GVIiS* nur den jeweils individuellen Zustand an Systemsicherheit schützt. Darin kommt die selbstbestimmte Verfügung des Nutzers über das informationstechnische System zum Ausdruck. Eine solche Verfügung wiederum entspricht der Selbstbestimmung als zentralem Bestandteil des allgemeinen Persönlichkeitsrechts. Das Erreichen eines bestimmten Sicherheitsstandards ist hingegen nicht Regelungsgegenstand des *GVIiS*.

---

336 *BVerfGE* 65, 1 (42); 72, 155 (170).

337 Als Leistung wird in der Informatik die Geschwindigkeit und Qualität bezeichnet, mit der ein Auftrag, also die Anforderung an eine Rechenanlage, eine bestimmte Datenverarbeitungsleistung zu erbringen, oder eine Menge von Aufträgen von einer Datenverarbeitungsanlage verarbeitet wird (*Duden*, Informatik A-Z, Stichwort „Leistung"). Eine der Größen zur Bewertung der Leistung ist auch die Verfügbarkeit der Datenverarbeitungsanlage.

338 *BVerfGE* 120, 274 (313).

### *3. Grundrechtskonkurrenzen*

Das *BVerfG* hat das *GVIiS* als weitere Konkretisierung des allgemeinen Persönlichkeitsrechts formuliert. Letzteres kommt gegenüber den speziellen Freiheitsrechten des Grundgesetzes nur subsidiär zur Anwendung. Eine solche Grundrechtskonkurrenz setzt voraus, dass auf ein Verhalten eines Grundrechtsträgers mehrerer Grundrechte anwendbar sind.[339] Dabei folgt schon aus dem lex-specialis-Grundsatz, dass sich beim Zusammentreffen zweier Freiheitsrechte, die zueinander im Verhältnis der Spezialität stehen, allein das spezielle Grundrecht einschlägig ist.[340] Die Spezialität reicht dabei soweit, als der Schutzbereich des spezielleren Grundrechts einschlägig ist.[341] Das allgemeine Persönlichkeitsrecht ist neben den speziellen Freiheitsrechten des Grundgesetzes nur insoweit einschlägig, als diese den insgesamt notwendigen grundrechtlichen Schutz der Persönlichkeit nicht gewährleisten. Folglich kommt auch das *GVIiS* als Ausprägung des allgemeinen Persönlichkeitsrechts nur nach dieser Maßgabe zur Anwendung. Eine durch das *GVIiS* zu schließende Schutzlücke kann daher nur innerhalb des Anwendungsbereichs des allgemeinen Persönlichkeitsrechts bestehen. Der Schutzbereich des *GVIiS* ist nur insoweit eröffnet, als von einer staatlichen Maßnahme die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betroffen ist, diese Gewährleistung aber nicht bereits vom Schutzbereich eines speziellen Freiheitsrechts erfasst wird.

#### a. Gewährleistung des Telekommunikationsgeheimnisses, Art. 10 Abs. 1 GG

##### i. Schutzbereich

Das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs.[342] Geschützt werden nicht nur bestimmte sondern sämtliche mit Hilfe der verfügbaren Telekommunikationstechniken erfolgende Übermittlungen von Informationen.[343] Art. 10 Abs. 1 GG erfasst damit auch die Kommunikationsdienste des Internets.[344] Das Grundrecht schützt nicht nur die Inhalte der Telekommunikation vor Kenntnisnahme, sondern auch deren Umstände.[345] Solche Umstände sind insb. ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen kommuniziert oder ein solcher Versuch unternommen wurde.[346] Der Schutz des Art. 10 Abs. 1 GG ist dabei aber

---

339 *V. Münch*, in: *Ders./Kunig* (Hrsg.), GG, Bd. 1, Vorb. Art. 1-19 Rn. 47.
340 *Pieroth/Schlink*, Grundrechte, Rn. 351; *Sodan*/Ziekow, Grundkurs Öffentliches Recht, § 25 Rn. 2.
341 *Sodan*/Ziekow, Grundkurs Öffentliches Recht, § 25 Rn. 2.
342 *BVerfGE* 115, 166 (182); 120, 274 (306f.); *BVerfG* NJW 2009, 2431 (2432).
343 *BVerfGE* 106, 28 (36); 115, 166 (182).
344 *BVerfGE* 113, 348 (383); 120, 274 (307); *BVerfG* NJW 2009, 2431 (2432).
345 *BVerfGE* 67, 157 (172); 85, 386 (396); 100, 313 (358); 107, 299 (312f.); 120, 274 (307).
346 *BVerfGE* 67, 157 (172); 85, 386 (396); 100, 313 (358); 107, 299 (312f.); 120, 274 (307).

insgesamt auf solche staatlichen Überwachungsmaßnahmen beschränkt, die Inhalte und Umstände allein der *laufenden* Telekommunikation erheben oder darauf bezogene Daten auswerten.[347] Dabei ist unerheblich, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt.[348] Aus dem Schutzbereich des Art. 10 Abs. 1 GG fallen hingegen die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit es dem Teilnehmer möglich ist, eigene Schutzvorkehrungen gegen einen heimlichen Datenzugriff zu treffen.[349] Die spezifischen Gefahren, vor denen das Telekommunikationsgeheimnis schützt, liegen in der räumlichen Distanz zwischen den Kommunikationspartnern und den Zugriffsmöglichkeiten für Dritte.[350] Die Kommunikationspartner haben anders als bei einem Gespräch zwischen Anwesenden nicht die Möglichkeit, nur allein die Rahmenbedingungen der Kommunikation festzulegen und hierbei deren Privatheit und die an der Kommunikation beteiligten Personen zu überwachen.[351] Sie sind aufgrund der zwischen ihnen bestehenden räumlichen Distanz auf einen technischen Übermittlungsvorgang angewiesen, der nicht in ihren ausschließlichen Einflussbereich fällt.[352] Diese Gefahren bestehen bei einer Speicherung der Kommunikationsinhalte und -umstände im Herrschaftsbereich eines Teilnehmers nicht fort.[353] Vor diesem Hintergrund ist der Begriff des Telekommunikationsvorgangs nicht mit dem rein technischen Begriff des § 3 Nr. 22 TKG gleichzusetzen.[354] Ein „laufender" Telekommunikationsvorgang kann daher auch ein statischer Zustand ohne dynamische Signalübermittlung sein.[355]

Der Schutzbereich des Art. 10 Abs. 1 GG überschneidet sich mit dem des allgemeinen Persönlichkeitsrechts insoweit, als die Übermittlung *persönlicher* Äußerungen unter Zuhilfenahme Dritter betroffen ist.[356] Insoweit schützt Art. 10 Abs. 1 GG den spezifischen Aspekt der Persönlichkeitsentfaltung, der in der unkörperlichen Übermittlung von Informationen an einen bestimmten Empfänger zum Ausdruck kommt. Für den Bereich der *laufenden* Telekommunikation ist Art. 10 Abs. 1 GG somit gegenüber Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG die speziellere

[347] *BVerfGE* 115, 166 (183); 120, 274 (307) (Hervorhebung nur hier).
[348] *BVerfGE* 106, 28 (37f.); 115, 166 (186f.); 120, 274 (307).
[349] *BVerfGE* 115, 166 (185f.); 120. 274 (307f.).
[350] *Gusy*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 10 Rn. 18; *Pieroth/Schlink*, Grundrechte, Rn. 826.
[351] *BVerfGE* 106, 28 (36).
[352] *BVerfGE* 106, 28 (36).
[353] *BVerfGE* 115, 166 (184); 120, 274 (308).
[354] *BVerfG* NJW 2009, 2431 (2432).
[355] *BVerfG* NJW 2009, 2431 (2432).
[356] *Hermes*, in: *Dreier* (Hrsg.), GG, Bd. 1, Art. 10 Rn. 94 (Hervorhebung nur hier).

Norm.[357]. Diese Spezialität gilt damit auch für das *GVIiS*.[358] Der Schutzbereich des Telekommunikationsgeheimnisses ist aber dann nicht eröffnet, wenn eine staatliche Stelle nicht auf eine laufende Telekommunikation zugreift, sondern die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht.[359]

ii. Datenübermittlung als Telekommunikation des Betroffenen i.S. d. Art. 10 Abs. 1 GG

Ein Eingriff in Art. 10 Abs. 1 GG liegt dabei nicht schon dann vor, wenn zur Übermittlung der erhobenen Daten eine Telekommunikationsverbindung genutzt wird.[360] Der Betroffene verliert zwar auch bei einer erfolgreichen Infiltration seines Systems die Verfügungsbefugnis über seine Daten; dieser Verlust beruht aber gerade nicht auf einer telekommunikationsspezifischen Gefährdungslage.[361] Bei der späteren Übermittlung der erlangten Informationen an die Ermittlungsbehörden gehen sowohl die Veranlassung der Übermittlung als auch die Bestimmung des Empfängers nicht von dem Betroffenen aus. Die Übermittlung der gewonnenen Informationen stellt damit zwar einen Telekommunikationsvorgang dar. Dieser Vorgang ist aber keine Telekommunikation *des* Betroffenen.[362] Weiter ist zu berücksichtigen, dass die bestehende Kommunikationsverbindung zwischen dem infiltrierten System des Betroffenen und einem Dritten nicht Gegenstand der Überwachung ist. Die Verbindung wird lediglich aus technischen Gründen zum Zwecke der Übertragung auf dem infiltrierten System bereits gespeicherter Daten genutzt.[363] Der Inhalt des hierbei bestehenden Telekommunikationsvorgangs soll gerade nicht erfasst werden.[364]

---

[357] *BVerfGE* 67, 157 (171); 110, 33 (53).

[358] Vgl. *BVerfGE* 120, 274 (307); die Subsidiarität des *GVIiS* gegenüber Art. 10 Abs. 1 GG wird ausdrücklich in *BVerfG* NJW 2009, 2431 (2433) festgestellt. Danach ist die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver eines Providers allein am Grundrecht auf Gewährleistung des Telekommunikationsgeheimnisses aus Art. 10 Abs.1 GG zu prüfen. Es erfolgt dort jedoch keine inhaltliche Prüfung, ob der Schutzbereich des *GVIiS* in diesem Fall überhaupt eröffnet war, und damit eine Situation der Grundrechtskonkurrenz vorlag. Insb. erfolgt keine Subsumtion des E-Mail-Postfachs des Betroffenen unter den Begriff des eigenen informationstechnischen Systems.

[359] *BVerfGE* 120, 274 (308); insoweit missverständlich *Hoffmann*, CR 2010, 515 (516), der für einen Eingriff in den Schutzbereich des *GVIiS* durch Datenerfassungen von *Google-Street-View*-Fahrzeugen auch auf abgefangene E-Mails und pauschal den Datenstrom in einem Netzwerk abstellt.

[360] *BVerfGE* 120, 274 (308).

[361] *Buermeyer*, HRRS 2007, 329 (330) = RDV 2008, 8 (9); *Weiß*, Online-Durchsuchungen, S. 103.

[362] Ebenso *Buermeyer*, HRRS 2007, 329 (330) = RDV 2008, 8 (9).

[363] Vgl. *BGH* MMR 2007, 237 (239).

[364] *Rux*, JZ 2007, 285 (292).

Folglich ist der Zugriff *durch* Telekommunikation nicht notwendig mit einem Eingriff *in die Freiheit* der Telekommunikation gleichzusetzen.[365] Allein der bloße Bezug zu einem Telekommunikationsvorgang führt damit noch nicht zur Eröffnung des Schutzbereichs des Art. 10 Abs. 1 GG.

iii. Sog. Quellen-Telekommunikationsüberwachung

Vielmehr ist nach den Ausführungen des *BVerfG* entscheidend, ob sich der Zugriff auf das informationstechnische System allein auf eine sog. *Quellen-Telekommunikationsüberwachung* (*Quellen-TKÜ*)[366] beschränkt. Diese Überwachungsmaßnahme greift nicht auf den Übertragungsweg der Informationen zu, sondern setzt am informationstechnischen System des Betroffenen als dem Endgerät der Telekommunikation an. Ein solches Gerät könne nach Ansicht des *BVerfG* auch ein vernetztes komplexes informationstechnisches System sein.[367] Dem ist zuzustimmen. Das Abhören der Internettelefonie durch Ausleiten der Gesprächsinhalte vor deren Verschlüsselung aus einem der an der Kommunikation beteiligten Geräte mittels einer eingeschleuster Software unterscheidet sich aus grundrechtlicher Perspektive nicht von einem an einem Telefon hardwareseitig angebrachten Abhörgerät.[368] Aber auch der Einsatz eines sog. *Keyloggers*[369] eröffnet bereits die Möglichkeit, den Inhalt verschiedenster Kommunikationsdienste mitzuverfolgen.

Die *Quellen-TKÜ* unterfalle aber nur dann allein Art. 10 Abs. 1 GG, wenn durch „technische Vorkehrungen und rechtliche Vorgaben sichergestellt" ist, dass die Überwachung „ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang" beschränkt ist.[370] Ermöglicht die zur Überwachung notwendige technische Infiltration den Zugang zu dem gesamten informationstechnischen System, entstünden aufgrund des dadurch bestehenden Risikos der Erhebung von Daten über Inhalte und Umstände der Telekommunikation hinaus Gefährdungen der Persönlichkeit, die von Art. 10 Abs. 1 GG nicht oder nicht hinreichend erfasst

365 *Buermeyer*, HRRS 2007, 329 (331) = RDV 2008, 8 (9) (Hervorhebung nur hier).

366 *Quellen-Telekommunikationsüberwachung* wird als der heimliche, technische Eingriff in ein informationstechnisches System zum Zweck der Telekommunikationsüberwachung verstanden (*BVerfGE* 120, 274 (308); ebenso *BKAG-E*, BT-Drucks. 16/9588, S. 29). In Abgrenzung zur *Online-Durchsuchung* sollen ausschließlich Telekommunikationsinhalte und nicht auch sonstige Daten erhoben werden (Antwort des *BMI* vom 22.8.2007 auf den Fragenkatalog des *BMJ* (Fn. 14), S. 2).

367 *BVerfGE* 120, 274 (307).

368 *Buermeyer*, HRRS 2007, 329 (331) = RDV 2008, 8 (10).

369 Ein Keylogger ist ein Programm oder eine bestimmte Hardware zur Protokollierung von Tastatureingaben und ihrer anschließenden Archivierung oder unerkannten Versendung (*Pierrot*, in: *Ernst* (Hrsg.), Hacker, Cracker und Computerviren, Rn. 49).

370 *BVerfGE* 120, 274 (309); ebenso schon *Buermeyer*, HRRS 2007, 329 (335, 337).

würden.[371] In ihrem Ausgangspunkt der unterschiedlichen grundrechtlichen Gefährdungslagen mag diese Abgrenzung überzeugen. Fraglich ist aber zum einen die Umsetzbarkeit „technischer Vorkehrungen" zum anderen die Wirksamkeit „rechtlicher Vorgaben". Jedenfalls zu dem Zeitpunkt, als das Urteil des *BVerfG* erging, war die Realisierbarkeit solcher technischer Vorkehrungen noch sehr zweifelhaft.[372] Zudem fehlt es an solchen Vorkehrungen schon dann, wenn eine bereits installierte Überwachungssoftware die Möglichkeit bietet, nachträglich mit weiteren Funktionen ausgestattet zu werden, die über eine reine *Quellen-TKÜ* hinausgehen.[373] Daneben bestehen gegen die Wirksamkeit „rechtlicher Vorgaben" grundsätzliche Bedenken. Eine Software zur *Quellen-TKÜ* beinhaltet immer die Gefahr, auch für eine umfassende Überwachung des informationstechnischen Systems missbraucht zu werden.[374] Allein durch die Installation der Software ist bereits die Integrität des gesamten informationstechnischen Systems gefährdet.[375] Eine solche Gefährdung stellt auch das *BVerfG* ausführlich fest. Das Gericht erkennt selbst, dass mit der technischen Infiltration des informationstechnischen Systems zum Zwecke der *Quellen-TKÜ* auch diejenige technische Hürde genommen sei, „das System insgesamt auszuspähen".[376] Es scheint dennoch überzeugt zu sein, dieser Gefährdung durch die vorbenannten Kriterien wirksam begegnen zu können. Das Gericht ist insoweit zumindest in großen Teilen widerlegt worden. Ein unerfreuliches Anschauungsbeispiel hierzu stellt der von dem *CCC* analysierte „Staatstrojaner" dar. Dieser genügte zunächst in technischer Hinsicht nicht den Vorgaben des *BVerfG* an eine zulässige *Quellen-TKÜ*, da seine Funktionalitäten nicht auf eine reine Telekommunikationsüberwachung beschränkt waren. Darüber hinaus schien den die Software einzusetzenden Strafverfolgungsbehörden nicht aufgefallen zu sein, dass es deshalb an einer tauglichen Ermächtigungsgrundlage für den Einsatz der Software fehlte.[377]

---

[371] *BVerfGE* 120, 274 (308f.); unter ausdrücklichem Hinweis auf die Entscheidung des *BVerfG* hat das *LG Landshut*, MMR 2011, 690 (691) insoweit festgestellt, dass § 100a StPO zwar eine taugliche Ermächtigung zur *Quellen-TKÜ* sein kann. Die Norm bildet hingegen keine Rechtsgrundlage für das Kopieren und Speichern grafischer Bildschirminhalte (das Fertigen sog. *Screenshots*), wenn zu diesem Zeitpunkt noch kein Telekommunikationsvorgang stattfindet; siehe hierzu auch *LG Hamburg*, MMR 2011, 693.

[372] *Hoffmann-Riem*, JZ 2008, 1009 (1022); *Hornung*, CR 2008, 299 (301); *Buermeyer/Bäcker*, HRRS 2009, 433 (439).

[373] Vgl. *Petri*, Prüfbericht Quellen-TKÜ v. 30.7.2012, S. 30ff. (abrufbar unter: http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf); zustimmend *Tinnefeld*, ZD 2012, 451 (453); offen hingegen *Skistims/Roßnagel*, ZD 2012, 3 (6).

[374] *Skistims/Roßnagel*, ZD 2012, 3 (5f.).

[375] *Skistims/Roßnagel*, ZD 2012, 3 (5f.); ebenso *Braun/Roggenkamp*, K&R 2011, 681 (684); *Buermeyer/Bäcker*, HRRS 2009, 433 (439); aus strafprozessualer Sicht merkt *Popp*, ZD 2012, 51 (53), an, dass schon die geforderten rechtlichen Vorgaben an keiner Stelle in den §§ 100a ff. StPO zu finden seien; ebenso *Braun/Roggenkamp*, K&R 2011, 681 (683); *Buermeyer/Bäcker*, HRRS 2009, 433 (439ff.) sowie bereits *Hoffmann- Riem*, JZ 2008, 1009 (1022).

[376] *BVerfG* 120, 274 (308).

[377] Siehe auch *Skistims/Roßnagel*, ZD 2012, 3 (6).

iv. Zwischenergebnis

Das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG ist allein maßgeblich, wenn eine staatliche Überwachungsmaßnahme ausschließlich Informationen aus einer laufenden Telekommunikation betrifft. Stellt sich diese Spezialität nicht, findet allein das *GVIiS* Anwendung, wenn die Vertraulichkeit und Integrität informationstechnischer Systeme betroffen ist. Nach umstrittener Ansicht des *BVerfG* soll an dieser Abgrenzung auch dann festgehalten werden, wenn die Telekommunikationsüberwachung den Zugriff auf ein informationstechnisches System voraussetzt.[378] Dies trifft etwa auf den Fall der sog. *Quellen-TKÜ* zu.

b. Unverletzlichkeit der Wohnung, Art. 13 Abs. 1 GG

Dem Schutz der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG wurde im Vorfeld des gegenständlichen Urteils des *BVerfG* besondere Aufmerksamkeit zuteil. Gegenstand der Diskussion war dabei die Frage, inwieweit die Maßnahme der sog. *Online-Durchsuchung* an Art. 13 Abs. 1 GG zu messen ist.[379] Der großen Zahl an Abhandlungen hierzu steht die eher kurze Beantwortung dieser Frage durch das *BVerfG* gegenüber. Das Gericht verzichtet dabei aber zu Recht auf eine pauschale Beantwortung der Konkurrenz zwischen Art. 13 Abs. 1 GG und dem allgemeinen Persönlichkeitsrecht:

> „*Art. 13 Abs.1 GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet.*“[380]

---

[378] Grds. kritisch *Schantz*, KritV 2007, 310 (322): Mit der vom Schutzgehalt des Art. 10 Abs. 1 GG umfassten Gewährleistung der Bedingungen einer freien Kommunikation wäre die Befürchtung der Bürger, der Staat würde die Empfangsbereitschaft für eine Kommunikation zur Infiltration ausnutzen, unvereinbar, da sich diese Befürchtung auf das Kommunikationsverhalten negativ auswirken und einen freien Meinungs- und Informationsaustausch beeinträchtigen könnte. In diese Richtung auch *Bizer*, DuD 2007, 640: Allein die Möglichkeit einer Online-Durchsuchung werde die Nutzung des Internets in eine Vertrauenskrise stürzen. Dagegen insofern *BVerfGE* 120, 274 (323), wonach die Möglichkeit, dass eine unbefangene Individualkommunikation verhindert wird, zwar das Gewicht eines Eingriffs prägt, diesem Gewicht aber mit entsprechend hohen Rechtfertigungsanforderungen begegnet werden könne; ebenso auch *Kemper*, ZRP 2007, 105 (106): Keine Planung eines „Schnüffelstaats“.

[379] Dafür: *Huster*, LT-NRW-Stellungnahme 14/641, S. 4; *Sokol*, LT-NRW-Stellungnahme 14/625, S. 9ff.; *Bär*, MMR 2007, 239 (240); *Bizer*, DuD 2007, 640; *Buermeyer*, HRRS 2007, 329 (332) = RDV 2008, 8 (11); *Harrendorf*, StraFO 2007, 149 (151); *Hornung*, JZ 2007, 828 (829); *ders.*, DuD 2007, 575 (577f.); *Jahn/Kudlich*, JR 2007, 57 (60); *Kutscha*, NJW 2007, 1169 (1170f.); *Rux*, JZ 2007, 285 (292); *Sachs/Krings*, JuS 2008, 481 (483); *Schaar/Landwehr*, K&R 2007, 202 (204); *Warntjen*, JURA 2007, 581 (583); dagegen: *Gusy*, LT-NRW-Stellungnahme 14/629, S. 7; *Bundesamt für Verfassungsschutz*, LT-NRW-Stellungnahme 14/639, S. 5; *Roth*, LT-NRW-Stellungnahme 14/645, S. 18; *Schwarz*, LT-NRW-Stellungnahme 14/650, S. 5; *Beulke/Meininghaus*, StV 2007, 60 (64); *Gercke*, CR 2007, 245 (250); *Hofmann*, NStZ 2005, 121 (124); *Schlegel*, GA 2007, 645 (656f.).

[380] *BVerfGE* 120, 274 (310).

Die Eröffnung des Schutzbereichs des Art. 13 Abs. 1 GG hinsichtlich des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme ist mithin von der konkreten Art und Weise des Zugriffs auf das System abhängig. Denn die Unterschiede in den Zugriffsmodalitäten bestimmen maßgeblich das im Einzelfall zu berücksichtigende Konkurrenzverhältnis zwischen den speziellen Freiheitsrechten und dem allgemeinen Persönlichkeitsrecht. Der Schutz informationstechnischer Systeme wird nur dann bereits vom Schutz der Unverletzlichkeit der Wohnung erfasst, wenn mit einem Zugriff auf das System zugleich der Schutzbereich des Art. 13 Abs. 1 GG eröffnet ist. Im Folgenden werden dahingehende Kriterien erarbeitet und die erfassten Zugriffsmodalitäten fallgruppenartig zusammengefasst.

i. Schutzbereich

Das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG garantiert dem Einzelnen einen „elementaren Lebensraum“[381] und sichert ihm das Recht, darin „in Ruhe gelassen zu werden“.[382] Der Begriff der Wohnung umschreibt hierbei einen Raum, den der Mensch zum Zwecke seines Aufenthalts der allgemeinen Zugänglichkeit entzieht[383] und der damit zur „räumlichen Privatsphäre“[384] wird. Schutzgut des Grundrechts ist folglich diese räumliche Sphäre, in der sich das Privatleben entfaltet.[385] Trägern öffentlicher Gewalt ist es danach grds. verboten, gegen den Willen des Wohnungsinhabers in die Wohnung einzudringen und darin zu verweilen.[386] Soweit Eingriffe in die räumliche Privatsphäre des Wohnungsinhabers Gegenstand der grundrechtlichen Prüfung sind, geht Art. 13 Abs. 1 GG als spezielle Gewährleistung dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vor.[387] Diese Spezialität reicht jedoch nur soweit als sich beide Schutzbereiche überschneiden. Erschöpft sich der Eingriff nicht allein in der Überwindung räumlicher Grenzen der Privatsphäre, sondern erfährt er eine zusätzliche grundrechtsrelevante Qualität, werden Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG insoweit nicht verdrängt.[388]

Das *BVerfG* präzisierte die Reichweite des Schutzbereichs des Art. 13 Abs. 1 GG hinsichtlich moderner technischer Überwachungsmöglichkeiten bereits im Jahre 2004 in seinem Urteil zum „Großen Lauschangriff“:

> „*Im Zeitpunkt der Schaffung des Grundgesetzes diente das Grundrecht des Art. 13 Abs. 1 GG primär dem Schutz des Wohnungsinhabers vor unerwünschter physischer*

[381] *BVerfGE* 42, 212 (219); 51, 97 (110); 103, 142 (150).
[382] *BVerfGE* 32, 54 (75); 89, 1 (12); 103, 142 (150); 109, 279 (309).
[383] *Gornig*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 13.
[384] *BVerfGE* 32, 54 (72); 65, 1 (40).
[385] *BVerfGE* 89, 1 (12); 103, 142 (150f.); 120, 274 (309); *Papier*, in: *Maunz/Dürig*, GG, Bd. 2, Art. 13 Rn. 1.
[386] *BVerfGE* 76, 83 (89f.); 109, 279 (309).
[387] *BVerfGE* 109, 279 (325).
[388] Vgl. *BVerfGE* 115, 166 (187f.).

*Anwesenheit eines Vertreters der Staatsgewalt. Seitdem sind neue Möglichkeiten für Gefährdungen des Grundrechts hinzugekommen. Die heutigen technischen Gegebenheiten erlauben es, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes 1 umfasst wäre.*"[389]

Die Gewährleistung des Art. 13 Abs. 1 GG beschränkt sich demnach nicht nur auf das Verbot körperlichen Eindringens und Verweilens in der Wohnung. Trägern staatlicher Gewalt ist es ebenso verboten, Abhörgeräte in der Wohnung zu installieren oder diese dort zu verwenden.[390]

ii. Eingriff

Der Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG setzt stets die Verletzung der geschützten räumlichen Privatsphäre voraus. Neben dem körperlichen Eindringen in eine Wohnung stellt jede Form akustischer oder optischer Wohnraumüberwachung einen Eingriff in Art. 13 Abs. 1 GG dar, wenn bei dieser Überwachung unter Einsatz besonderer Hilfsmittel Vorgänge innerhalb der Wohnung erfasst werden, die der *natürlichen Wahrnehmung von außerhalb der Wohnung entzogen sind.*[391] Der Eingriff knüpft dabei nicht an eine bestimmte Art und Weise des Eindringens in die geschützte Räumlichkeit an. Art. 13 Abs. 1 GG garantiert den Schutz der räumlichen Privatsphäre umfassend.[392] Die nach außen dringende und ohne technische Hilfsmittel hörbare Kommunikation fällt hingegen nicht in den Schutzbereich des Art. 13 Abs. 1 GG, „weil der Betroffene die räumliche Privatsphäre nicht zu seinem Schutz nutzt, wenn er die Wahrnehmbarkeit der Kommunikation von außen selbst ermöglicht".[393]

(1) Verletzung der räumlichen Privatsphäre durch die Wahrnehmung von Vorgängen innerhalb der Wohnung

Sowohl dem körperlichen Eindringen in einen als Wohnung geschützten räumlichen Bereich als auch dem Einsatz besonderer technischer Hilfsmittel ist somit gemeinsam, dass ein Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG stets die Verletzung der räumlichen Privatsphäre durch das Gewinnen von „Einblicken in Vorgänge innerhalb der Wohnung, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind",[394] voraussetzt.

---

[389] *BVerfGE* 109, 279 (309).
[390] *BVerfGE* 109, 279 (309); ebenso bereits *BVerfGE* 65, 1 (40).
[391] *BVerfGE* 109, 279 (327); 120, 274 (310) (Hervorhebung nur hier).
[392] *Gornig*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 1.
[393] *BVerfGE* 109, 279 (327).
[394] *BVerfGE* 120, 274 (310).

(a) Körperliches Eindringen

Ein solcher Einblick lässt sich zunächst dadurch gewinnen, dass die räumliche Privatsphäre durch das körperliche Betreten staatlicher Ermittlungspersonen verletzt wird. Unerheblich ist dabei, ob ein solcher Einblick das Ziel des Handelns darstellt. Selbst wenn es einer Person nicht darauf ankommen sollte, den Innenbereich der Wohnung wahrzunehmen, kann sie diese Wahrnehmung nicht unterdrücken.[395] Für den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme bedeutet dies, dass Art. 13 Abs. 1 GG gegenüber dem *GVIiS* das speziellere Grundrecht ist, „wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren".[396] Denn dann wird für die Dauer des Infiltrationsvorgangs auch die räumliche Privatsphäre der Wohnung durch die Anwesenheit der Ermittlungspersonen verletzt. Der notwendige Persönlichkeitsschutz wird in diesem Fall bereits von Art. 13 Abs. 1 GG gewährleistet. Die Grundrechtsrelevanz des körperlichen Zugriffs auf das informationstechnische System kann jedoch über die einmalige Verletzung der räumlichen Privatsphäre hinausgehen, wenn sich durch die Infiltration eine dauerhafte Zugangsmöglichkeit zu dem System ergibt. Diese Möglichkeit dauert über das einmalige Betreten der Wohnung hinaus fort. Sofern die räumliche Privatsphäre nicht mehr betroffen ist, wird aber auch die fortdauernde Infiltration des informationstechnischen Systems nicht mehr von dem Persönlichkeitsschutz des Art. 13 Abs. 1 GG erfasst. Hinsichtlich dieser fortdauernden Gefährdungslage verbleibt somit eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu schließen ist. Sofern Ermittlungspersonen zum Zwecke der technischen Infiltration eines informationstechnischen Systems in eine als Wohnung geschützte Räumlichkeit körperlich eindringen, ist Art. 13 Abs. 1 GG somit nur dann alleiniger grundrechtlicher Maßstab, sofern sich die Grundrechtsrelevanz der Maßnahme in der einmaligen Verletzung der räumlichen Privatsphäre erschöpft.

(b) Verwendung besonderer technischer Hilfsmittel

Einblicke in Vorgänge innerhalb der Wohnung können weiter aber auch ohne körperliches Betreten mittels der eingangs erwähnten technischen Hilfsmittel erlangt werden. Das *BVerfG* erwähnt hier verschiedene Modalitäten eines Eingriffs in die räumlich geschützte Privatsphäre.

---

[395] *Cassardt*, in: *Umbach/Clemens* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 38.
[396] *BVerfGE* 120, 274 (310).

(i) Messung elektromagnetischer Abstrahlungen (sog. TEMPEST)

Der natürlichen Wahrnehmung von außerhalb der Wohnung entzogen seien Einblicke, die durch „die Messung elektromagnetischer Abstrahlungen“[397] gewonnen werden, „mit der die Nutzung eines informationstechnischen Systems in der Wohnung überwacht werden kann“[398]. Von dieser Maßnahme könne auch ein informationstechnisches System betroffen sein, „das offline arbeitet“.[399] In diesem Fall führt der Einsatz technischer Hilfsmittel - begrenzt auf den Bereich der Wohnung - zur Überwindung der räumlichen Grenze, die der natürlichen Wahrnehmung der aufgezeichneten Informationen entgegensteht. Ist die räumliche Privatsphäre einer Wohnung dagegen nicht betroffen, ist die Maßnahme alleine an den Vorgaben des *GVIiS* zu messen.[400]

(ii) Keylogger

Auch der Einsatz eines sog. *Keyloggers* lässt sich nicht pauschal auf seine grundrechtliche Relevanz beantworten. *Rux* hält die „Aufzeichnung von Tastatureingaben und Mausbewegungen“ schon dann für mit dem Einsatz eines Richtmikrofons vergleichbar, wenn sich das überwachte informationstechnische System innerhalb einer von Art. 13 Abs. 1 GG geschützten Räumlichkeit befindet.[401] Allein aus dem Standort des Systems innerhalb einer Wohnung folgt nicht schon notwendigerweise, dass gerade solche Einblicke in Vorgänge innerhalb der Wohnung erlangt werden, die sonst der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen wären. Die Installation eines Hardware-Keyloggers zur Aufzeichnung der Tastatureingaben setzt zwingend das körperliche Betreten der geschützten Räumlichkeit durch staatliche Ermittlungspersonen zum Einbau der entsprechenden Komponente voraus. Eine solche Maßnahme verletzt schon deswegen die räumliche Privatsphäre einer Wohnung und wäre an Art. 13 Abs. 1 GG zu messen. Gleiches gilt für einen Software-Keylogger, wenn für dessen Installation ebenfalls Ermittlungspersonen in die Wohnung eindringen. Anders dürfte die Installation eines Software-Keyloggers allein über ein Kommunikationsnetz

---

397 Sog. *TEMPEST* (Transient Electromagnetic Pulse Emanation Standard); Forschungsprogramm der britischen und US-amerikanischen Militärbehörden aus den 1950er Jahren, das den Austritt von elektromagnetischen Flüssen aus elektronischen Geräten untersuchte; heute ein Standard zur Abschirmung und Einschränkung dieser Flüsse (*Fischer/Hofer*, Lexikon Informatik, Stichwort „Tempest“); ferner *Online-Lexikon für Informationstechnologie* (http://www.itwissen.info, Stichwort „Tempest“): Sicherheitslücken, die durch elektromagnetische Strahlung verursacht werden. Es ist dies kompromittierende Strahlung von Geräten, Kabeln und vor allem Bildschirmen, die abgefangen und mit entsprechenden Empfangseinrichtungen aus einiger Entfernung erfasst und auswertet werden kann. Es werden dadurch zeitgleich diejenigen Informationen auf einem Bildschirm sichtbar gemacht, die der Nutzer selbst sieht.

398 *BVerfGE* 120, 274 (310); *Hornung*, JZ 2007, 828 (829).

399 *BVerfGE* 120, 274 (310).

400 *BVerfGE* 120, 274 (315).

401 So aber *Rux*, JZ 2007, 285 (292).

ohne die physische Anwesenheit von Ermittlungspersonen zu bewerten sein. Da die bloße Installation der Software keinen Eingriff in die räumliche Privatsphäre des Betroffenen darstellt, müsste die anschließende Aufzeichnung der Tastatureingaben als Eingriff in Art. 13 Abs. 1 GG zu bewerten sein. Dies setzt voraus, dass diese Aufzeichnungen mit Einblicken in die Vorgänge innerhalb der Wohnung mittels besonderer technischer Hilfsmittel gleichgesetzt werden können. Das *BVerfG* erwähnt in diesem Zusammenhang nur die sog. *Hardware-Keylogger*. Deren *Einsatz* falle ausschließlich unter den Schutzbereich des *GVIiS*.[402] Zugleich fasst das Gericht aber die für die Installation eines *Hardware-Keyloggers* zwingend notwendige physische Manipulation eines informationstechnischen Systems unter den Schutzbereich des Art. 13 Abs. 1 GG.[403] Es werden danach die verschiedenen Maßnahmen auch an verschiedenen Grundrechten gemessen. Dieser Einzelbetrachtung muss dann aber auch eine Differenzierung zwischen der Infiltration des informationstechnischen Systems und der sich daran anschließenden Aufzeichnung der Tastatureingaben folgen. Diese Differenzierung ist auf den Einsatz eines *Software-Keyloggers* übertragbar. Die bloße Aufzeichnung von Tastatureingaben allein ist nicht schon mit einem Einblick in Vorgänge innerhalb der Wohnung gleichzusetzen.[404] Der bloße *Einsatz* eines Keyloggers stellt danach auch dann keinen Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG dar, wenn sich das gegenständliche informationstechnische System innerhalb einer Wohnung befindet.

(iii) Verwendung der an ein informationstechnisches System angeschlossenen Peripheriegeräte

Im Ausgangpunkt zu Recht prüft das *BVerfG* dagegen ausschließlich Art. 13 Abs. 1 GG, wenn ein in einer geschützten Räumlichkeit befindliches informationstechnisches System infiltriert wird, um bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa unter Verwendung der an das System angeschlossenen, Peripheriegeräte wie Mikrofon oder Kamera.[405] In diesem Fall liegt die relevante Persönlichkeitsverletzung gerade in dem missbräuchlichen Einsatz der Peripheriegeräte als technische Hilfsmittel, um einen ansonsten verwehrten Einblick in Vorgänge innerhalb der Wohnung zu erhalten. Diese Bestimmung des Konkurrenzverhältnisses muss sowohl für die Infiltration des Systems durch ein körperliches Betreten der geschützten Räumlichkeit als auch für die unkörperliche Infiltration

---

[402] *BVerfGE* 120, 274 (315) (Hervorhebung nur hier).

[403] Vgl. *BVerfGE* 120, 274 (310).

[404] A.A. *Rux*, JZ 2007, 831.

[405] *BVerfGE* 120, 274 (310); ebenso bereits *Buermeyer*, HRRS 2007, 329 (336) = RDV 2008, 8 (14); *Huber*, NVwZ 2007, 880 (883); *Schlegel*, GA 2007, 648 (656); *Schantz*, KritV 2007, 310 (311 Fn.15); siehe hierzu beispielhaft auch die Meldung der *Süddeutschen Zeitung* vom 16.7.2010: „Per Webcam beobachtet - Cyber-Spanner spioniert Schülerinnen aus“ (abrufbar unter: http://www.sueddeutsche.de/digital/per-webcam-beobachtet-cyber-spanner-spioniert-schuelerinnen-aus-1.976146).

über ein Kommunikationsnetz gelten. Die grundrechtliche Relevanz der unkörperlichen Infiltration ist dann nicht gesondert neben der sich anschließenden Verletzung der räumlichen Privatsphäre zu berücksichtigen. Dahingehend liegt in der zeitlichen Abfolge der maßgebliche Unterschied zu der vorbenannten Gestaltung, in der die Infiltration des informationstechnischen Systems nach Beendigung der Verletzung der räumlichen Privatsphäre noch andauert. Es stellt sich sodann jedoch das gleiche Problem wie bei der Prüfung des Konkurrenzverhältnisses zu Art. 10 Abs. 1 GG, das an dieser Stelle des Urteils jedoch nicht erneut Erwähnung findet. Rechtliche Vorgaben und technische Vorkehrungen müssten sicherstellen, dass die Infiltration des informationstechnischen Systems auf die Möglichkeit der Verwendung der an das System angeschlossenen Peripheriegeräte begrenzt wird.[406] Sofern eine solche Begrenzung nicht erfolgt oder technisch nicht erfolgen kann, erschöpft sich die Grundrechtsrelevanz der unkörperlichen Infiltration nicht in der Verletzung der räumlichen Privatsphäre durch die Überwachung der Wohnung. Die Infiltration eines informationstechnischen Systems wird somit bereits von Art. 13 Abs. 1 GG erfasst, sofern die Infiltration mit der Verletzung der räumlichen Privatsphäre einer Wohnung verbunden ist, und sich die Grundrechtsrelevanz der Infiltration *allein* in dieser Verletzung erschöpft.

(2) Keine Verletzung der räumlichen Privatsphäre durch die Wahrnehmung von Vorgängen innerhalb der Wohnung

Die Eröffnung des Schutzbereichs des Art 13 Abs. 1 GG setzt jedoch stets voraus, dass der Schutzgegenstand der räumlichen Privatsphäre betroffen ist. Diese ist jedoch auch bei einem Zugriff auf ein informationstechnisches System, das sich innerhalb einer von Art. 13 Abs. 1 GG geschützten Räumlichkeit befindet, nicht in jedem Fall berührt.

(a) Reichweite der räumlichen Privatsphäre

Bei einem physischen Eindringen in eine Wohnung werden stets die Grenzen einer räumlichen Sphäre überwunden. Fraglich ist demgegenüber, welchen Zugriffsmodalitäten auf ein informationstechnisches System ebenfalls diese Grenzen entgegenstehen, so dass der Zugriff als der Einsatz technischer Mittel im oben beschriebenen Sinne zu begreifen ist. Für die sog. *Online-Durchsuchung* wurde dies teilweise bejaht, sofern sich das betroffene informationstechnische System innerhalb einer durch Art. 13 Abs. 1 GG geschützten Räumlichkeit befindet.[407]

---

406 Vgl. insofern die Vorgaben hinsichtlich der *Quellen-TKÜ*, *BVerfGE* 120, 274 (309).

407 Dafür *Sokol*, LT-NRW-Stellungnahme 14/625, S. 9f.; *Buermeyer*, HRRS 2007, 329 (333) = RDV 2008, 8 (11); *Jahn/Kudlich*, JR 2007, 57 (60); *Kutscha*, NJW 2007, 1169 (1170); *Rux*, JZ 2007, 285 (292); *Schaar/Landwehr*, K&R 2007, 202 (204).

(i) Ausbildung durch räumliche Abschottung

Laut *Schantz* ergebe sich schon aus der in Art. 13 Abs. 3-6 GG geregelten Möglichkeit der Überwachung einer Wohnung mit technischen Mitteln, dass deren Schutz umfassend und nicht nur gegenüber dem körperlichen Eindringen oder einer anderen Art der Überwindung einer räumlichen Barriere gewährleistet sei.[408] Dem lässt sich entgegenhalten, dass Ausgangspunkt des grundrechtlichen Schutzes des Art. 13 Abs. 1 GG allein die durch eine Wohnung ausgebildete *räumliche* Privatsphäre ist.[409] Somit kann auch nur diese Sphäre Gegenstand eines etwaigen umfassenden Schutzes sein. Eine räumliche Privatsphäre kann eine Wohnung i.S.d. Art. 13 Abs. 1 GG aber zwangsläufig nur dann ausbilden, wenn sie ein Mindestmaß an physischer und informationeller Abschottung des geschützten Raumes nach außen aufweisen kann.[410] Ein solches Mindestmaß ist jedoch denklogisch nicht mit der Unüberwindbarkeit dieser Abschottung gleichzusetzen.[411] Geschützt ist vielmehr derjenige Raum, in dem der Einzelne begründetermaßen und somit auch für Dritte erkennbar die Möglichkeit hat, frei von öffentlicher Beobachtung und der von ihr erzwungenen Selbstkontrolle zu sein.[412] Die Unverletzlichkeit der Wohnung ist folglich nur dann betroffen, wenn gerade diejenigen Grenzen der natürlichen Wahrnehmung überwunden werden, die durch die geschützte Räumlichkeit gesetzt werden, um einen Einblick in die Vorgänge innerhalb der Wohnung zu erhalten. Eine Wohnung i.S.d. Art. 13 Abs. 1 GG vermag aber nur räumliche Grenzen *physischer*, *optischer* oder *akustischer* Art zu setzen.[413] Es muss aber gerade dieses Wahrnehmungshindernis, das die Wände einer Wohnung bilden, überwunden[414] und damit die durch *bauliche Vorkehrungen* gesicherte Privatheit durchbrochen werden.[415] Räumliche Lebenssphäre i.S.d. Art. 13 Abs. 1 GG meint die Errichtung eines nicht ohne weiteres betretbaren, einsehbaren und belauschbaren Raumes.[416]

Demgegenüber beruht der Schutz eines informationstechnischen Systems in einer Wohnung i.S.d. Art. 13 Abs. 1 GG nicht auf der Funktion des Raumes, in dem sich das System befindet, sondern auf Einstellungen in seinen Programmabläufen, wodurch ein Zugriff von außerhalb des Systems gewöhnlich unterbunden wird.[417] Der Zugriffsschutz erfolgt auf der Ebene der anwendungsorientierten

---

[408] *Schantz*, KritV 2007, 310 (317).

[409] So etwa *BVerfGE* 109, 279 (314): Wohnung als „räumliches Substrat" vertraulicher Kommunikation.

[410] *Hermes*, in: *Dreier* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 16.

[411] A.A. *Weiß*, Online-Durchsuchungen, S. 122.

[412] Vgl. *BVerfGE* 101, 361 (383f.).

[413] *T. Böckenförde*, Ermittlung im Netz, S. 219 (Hervorhebung nur hier).

[414] *T. Böckenförde*, JZ 2007, 925 (926).

[415] *Schwarz*, LT-NRW-Stellungnahme 14/650, S. 6 (Hervorhebung nur hier).

[416] *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 10; *Gornig*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 13.

[417] Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung, S. 541.

oder auch der logischen Verbindungsarchitektur,[418] nicht hingegen auf der Ebene der räumlichen Abschottung. Diese Abschottung ist für Online-Zugriffe unerheblich.[419] Der Schutz vor einem derartigen Zugriff steht in keinem Zusammenhang mit der physischen Zugänglichkeit des informationstechnischen Systems.[420] Folglich lässt die Infiltration eines informationstechnischen Systems, welche die Verbindung des Systems zu einem Netzwerk ausnutzt, „die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt".[421] Ein solcher Zugriff bedeutet keinen Eingriff in die von Art. 13 Abs. 1 GG geschützte räumliche Integrität. Denn wo räumliche Grenzen von vornherein nicht existieren, kann sich eine räumliche Privatsphäre, die durch die Abschottung eines bestimmten Raumes durch eben diese Grenzen gebildet wird, von vornherein nicht ausbilden. Die Begründung von *Schlegel* hingegen, die sog. *Online-Durchsuchung* eines PCs vollziehe sich in einem genau abgegrenzten Raum innerhalb der Wohnung und enthalte nicht die Gefahr, dass wie bei einer realen Durchsuchung oder einem „Großen Lauschangriff" der *gesamte räumliche Schutzbereich* und damit auch der Rückzugsbereich für den Einzelnen negiert werde,[422] ist nicht damit nicht ausreichend genau. Denn der PC begründet für sich keine räumliche Privatsphäre und damit auch keinen Teilbereich derjenigen räumlichen Privatsphäre, die durch eine Wohnung begründet wird.[423] Vielmehr nimmt der PC nur als körperlicher Gegenstand an der räumlichen Schutzwirkung der Wohnung teil und dies ausschließlich deshalb, da seine physische Lage innerhalb der Wohnung nur durch einen Eingriff in Form des körperlichen Betretens der Wohnung geändert werden kann.[424] Es existieren mithin insoweit gegen die sog. *Online-Durchsuchung* keine Grenzen der natürlichen Wahrnehmung, die mittels technischer Mittel überwunden werden könnten. Hierin liegt der entscheidende Unterschied zur akustischen Wohnraumüberwachung von außerhalb der geschützten Räumlichkeit. Denn diese Überwachung überwindet gerade die Wände, Böden und Decken einer Wohnung, die der natürlichen Wahrnehmung des überwachten Wortes entgegenstehen, und verletzt dadurch die durch Art. 13 Abs. 1 GG geschützte Privatsphäre in *räumlicher* Hinsicht.[425]

An dieser Auslegung kritisieren *Schaar/Landwehr*, dass ihr eine rein technische Betrachtungsweise zugrunde liege, welche verfassungsrechtliche Vorgaben nicht berücksichtige.[426] Art. 13 Abs. 1 GG enthalte vielmehr den Verfassungsauftrag, vor einem Datenzugriff auf einem informationstechnischen System innerhalb einer Wohnung zu schützen. Dem ist zu widersprechen. Die Ablehnung der Er-

418 *T. Böckenförde*, Ermittlung im Netz, S. 224.
419 *Beulke/Meininghaus*, StV 2007, 60 (64); *Martini*, JA 2009, 839 (840).
420 *Germann*, Gefahrenabwehr und Strafverfolgung, S. 541.
421 *BVerfGE* 120, 274 (310).
422 *Schlegel*, GA 2007, 648 (659) (Hervorhebung im Original).
423 A.A. *Buermeyer*, HRRS 2007, 329 (336) = RDV 2008, 8 (14).
424 Ebenso wiederum auch *Schlegel*, GA 2007, 648 (657).
425 A.A. *Weiß*, Online-Durchsuchungen, S. 118.
426 *Schaar/Landwehr*, K&R 2007, 202 (204).

öffnung des Schutzbereichs des Art. 13 Abs. 1 GG folgt gerade daraus, dass sich dessen Gewährleistung einer *verfassungsrechtlich* geschützten Privatsphäre aus einer *räumlichen* Abschottung ergibt. Gerade hierin liegt der für die besonderen Freiheitsrechte typische spezifische Persönlichkeitsschutz des Art. 13 Abs. 1 GG. Der grundrechtliche Schutz der persönlichen Lebens- und Privatsphäre durch die Unverletzlichkeit der Wohnung erfasst nur die für diesen Schutz notwendigen *räumlichen* Voraussetzungen.[427] Nur insoweit lassen sich Eingriffe auf Grundlage des Art. 13 Abs. 1 GG abwehren.[428]

Weiter greift auch der Einwand, dass es aus der Sicht des Einzelnen keinen Unterschied machen könne, ob er einen Brief oder ein Tagebuch in Papierform aufbewahrt oder sie auf einer Festplatte speichert,[429] nicht durch. Der Wohnungsinhaber müsste nämlich in die Schutzwirkung seiner Wohnung auch gegenüber solchen Gefährdungen seiner Persönlichkeit vertrauen, bei denen die Wände einer Wohnung nicht in ihrer typischen Beschaffenheit als physische, optische oder akustische Barriere überwunden werden. Ob für dieses Vertrauen berechtigterweise der Schutz des Art. 13 Abs. 1 GG zu fordern ist, ist angesichts des Schutzgegenstands des Grundrechts sehr fraglich.[430] Denn ein Brief oder Tagebuch in Papierform sind nicht wegen ihres sensiblen Inhalts vom Schutzbereich des Art. 13 Abs. 1 GG erfasst. Für dessen Eröffnung genügt nicht schon, dass vertrauliche Informationen nicht mehr in körperlicher Form in der Wohnung aufbewahrt werden, sondern als unkörperliche Daten auf dem Computer gespeichert werden.[431] Körperliche Gegenstände, die sich in einer Wohnung befinden, nehmen nicht um ihrer selbst willen am Schutz der Unverletzlichkeit der Wohnung teil, sondern weil für den Zugriff auf diese Gegenstände die räumliche Privatsphäre durch die Überwindung gerade der *physischen* Grenzen einer Wohnung verletzt werden muss.

(ii) Zu gewinnende Informationen als Anknüpfungspunkt

Auch die Informationen, welche mittels des unkörperlichen Zugriffs auf das informationstechnische System gewonnen werden können, taugen nicht als Anknüpfungspunkt für den Schutzbereich des Art. 13 Abs. 1 GG. Teilweise wird ein Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG allein damit begründet, dass die Informationsgewinnung aufgrund eines über das Internet erfolgenden Zugriffs eine Durchsuchung der Wohnung und die anschließende Beschlagnahme der relevanten Datenträger entbehrlich mache.[432] Insofern sei die sog. *Online-*

---

[427] Vgl. *BVerfGE* 51, 97 (107) (Hervorhebung nur hier).

[428] *Gornig*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 11; *Papier*, in: *Maunz/Dürig*, GG, Bd. 2, Art. 13 Rn. 1.

[429] *Schantz*, KritV 2007, 310 (317); *Rux*, JZ 2007, 285 (293); in diese Richtung auch *Sokol*, LT-NRW-Stellungnahme 14/625, S. 10.

[430] Dahingehend aber *Buermeyer*, HRRS 2007, 329 (333); *Schaar/Landwehr*, K&R 2007, 202 (204); *Schantz*, KritV 2007, 310 (317); *Gudermann*, Online-Durchsuchung, S. 100.

[431] A.A. *Schantz*, KritV 2007, 310 (314).

[432] So *Rux*, JZ 2007, 285 (292); *Sokol*, LT-NRW-Stellungnahme 14/625, S. 10.

*Durchsuchung* eine typische Ersatzmaßnahme für eine Hausdurchsuchung.[433] Das Auslesen der auf einer Festplatte oder einem anderen Medium gespeicherten Daten entspreche der Durchsuchung eines dreidimensionalen Raums.[434] Diese Argumentation überzeugt nicht. Die sog. *Online-Durchsuchung* stellt kein besonderes technisches Hilfsmittel dar, um in die räumliche Sphäre einer Wohnung anders als durch ein körperliches Betreten einzudringen, um einen der natürlichen Wahrnehmung entzogenen Einblick zu erhalten. Der Zugriff steht in keinem Zusammenhang mit der Überwindung räumlicher Abgrenzungen und berührt den Schutzbereich des Art. 13 Abs. 1 GG folglich selbst dann nicht, wenn sich die entsprechende Hardware in einer Wohnung befindet.[435] Vielmehr muss die Nutzung informationstechnischer Systeme als eigenständiger Vorgang der Persönlichkeitsentfaltung angesehen werden, dessen verfassungsrechtliche Bewertung wegen seiner Unabhängigkeit von einem Raumbezug keine Differenzierungen nach dem Standort des Systems zulässt.[436] Zuzugeben ist aber, dass der Schutzbereich des Art. 13 Abs. 1 GG auch die Beherrschung von Informationen über die Vorgänge und Gegenstände in der Wohnung und damit die Entscheidungsbefugnis darüber erfasst, welche Informationen aus dem Bereich der Wohnung Dritten gegenüber zugänglich sind.[437] Diese Entscheidungsbefugnis beruht aber nicht auf dem u.U. sensiblen Inhalt körperlicher Informationsträger oder der auf einem Datenträger innerhalb einer Wohnung enthaltenen Daten.[438] Ebenso wenig ergibt sich der Schutz körperlicher Gegenstände innerhalb einer Wohnung daraus, dass diese Gegenstände Informationen über den Wohnungsinhaber enthalten.[439] Art. 13 Abs. 1 GG besteht nicht deshalb, weil bestimmte Informationen besonders zu schützen sind, sondern bestimmte Informationen sind besonders geschützt, weil Art. 13 Abs. 1 GG besteht und diese Informationen an der räumlichen Abschottung durch die geschützte Lebenssphäre teilhaben.[440] Die Qualität des Eingriffs durch eine Wohnungsdurchsuchung ergibt sich nicht zwingend aus der besonderen Persönlichkeitsrelevanz der entdeckten Gegenstände.[441] Vielmehr ist die Erlangung von Informationen in Bezug auf die Wohnung nur dann an Art. 13 Abs. 1 GG zu messen, wenn hierbei das an die öffentliche Gewalt gerichtete grundsätzliche Verbot des Eindringens in die Wohnung als allein räumliche Privatsphäre oder des Verweilens darin gegen den Willen des Wohnungsinhabers missachtet

[433] So *Buermeyer*, HRRS 2007, 329 (333) = RDV 2008, 8 (12); *Schantz*, KritV 2007, 310 (314); *Sokol*, LT-NRW-Stellungnahme 14/625, S. 10.
[434] *Rux*, JZ 2007, 285 (294).
[435] Vgl. *Cassardt*, in: *Umbach/Clemens* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 43.
[436] *Hörnig*, JURA 2009, 207 (208).
[437] *Hermes*, in: *Dreier* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 12.
[438] So aber *Kutscha*, NJW 2007, 1169 (1171).
[439] So aber *Schantz*, KritV 2007, 310 (314).
[440] Ähnlich *Schlegel*, GA, 2007, 648 (657).
[441] *Lorenz*, in: *Scholz* u.a., Realitätsprägung durch Verfassungsrecht, S. 17 (23).

wird.[442] Diese Befugnis hat der Betroffene aber nur aufgrund der räumlichen Privatsphäre, die diese Informationen vor dem Zugriff Dritter schützt, und welche die Informationsgewinnung von der Verletzung dieser räumlichen Privatsphäre abhängig macht, sei es durch ein körperliches Eindringen oder durch Einsatz technischer Hilfsmittel. Folglich ist der durch Art. 13 Abs. 1 GG vermittelte Schutz vor staatlicher Informationsgewinnung räumlich formalisiert.[443]

Für die Eröffnung des Schutzbereichs spricht somit auch nicht bereits, dass der Inhalt der auf einem informationstechnischen System gespeicherten Daten Rückschlüsse auf das Verhalten geben könnte, das sich nicht in der Öffentlichkeit abspielt, sondern in einem grundrechtlich besonders geschützten Raum.[444] Art. 13 Abs. 1 GG umfasst den grundrechtlichen Schutz der persönlichen Lebens- und Privatsphäre nur dahingehend, als dieser auf den Schutz der hierfür notwendigen *räumlichen* Voraussetzungen angewiesen ist.[445] Anknüpfungspunkt des grundrechtlichen Schutzes des Art. 13 Abs. 1 GG ist nicht der Inhalt der erlangbaren Informationen. Allerdings besteht nur in ihrem Inhalt gerade die Vergleichbarkeit von unkörperlichen Daten und körperlichen Informationsträgern.[446] Während jedoch auf einen körperlichen Informationsträger nur durch Verletzung der räumlichen Privatsphäre durch physisches Betreten der Wohnung zugegriffen werden kann, setzt die Erhebung unkörperlicher Daten weder eine solche Verletzung der *räumlichen* Sphäre noch den Einsatz besonderer technischer Hilfsmittel hierfür zwingend voraus. Daher ist der Schutzbereich des Art. 13 Abs. 1 GG nicht schon deswegen betroffen, weil sich die Daten auf einem Träger innerhalb einer geschützten Räumlichkeit befinden und aus dieser heraus erhoben werden.[447]

Soweit durch den „Online-Zugriff" ein Privatheitsanspruch des Betroffenen berührt wird, so ist dieser Anspruch nicht räumlich begründet.[448] Denn es ist in Bezug auf die bloße Datenerhebung aus einem informationstechnischen System zwischen der Infiltration und der anschließenden Datenerhebung zu differenzieren: Die infolge der Infiltration ermöglichte Datenerhebung unterfällt nach dem *BVerfG* unter keinen Umständen Art. 13 Abs. 1 GG.[449] Da diese Abgrenzung nicht auf bestimmte Zugriffsmodalitäten beschränkt ist, kann folglich auch für den Fall nichts anderes gelten, bei dem die Infiltration des Systems mittels eines physischen Zugriffs auf das System erfolgt und somit einen Eingriff in Art. 13 Abs. 1 GG darstellt. Das *BVerfG* zieht hier eine Parallele des Verhältnisses von

---

[442] So schon *BVerfGE* 65, 1 (40); ebenso *Lorenz*, in: *Scholz* u.a., Realitätsprägung durch Verfassungsrecht, S. 17 (23).
[443] *Schmitt Glaeser*, in: HStR VI², § 129 Rn. 4.
[444] So aber *Kutscha*, NJW 2007, 1169 (1170).
[445] Vgl. *BVerfGE* 51, 97 (107).
[446] *Schlegel*, GA 2007, 648 (657); a.A. *Kutscha* NJW 2007, 1169 (1171).
[447] So aber *Buermeyer*, HRRS 2007, 329 (333) = RDV 2008, 8 (11); *Bär*, MMR 2007, 237 (240); *Sokol*, LT-NRW-Stellungnahme 14/625, S. 10f.
[448] *T. Böckenförde*, Ermittlung im Netz, S. 224.
[449] *BVerfGE* 120, 274 (311).

Infiltration und Datenerhebung zu dem Verhältnis von Wohnungsdurchsuchung (§ 102 StPO) und Beschlagnahme (§ 94 Abs. 2 StPO).[450] Hierbei stelle nur die Durchsuchung einer Wohnung einen Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG dar, nicht jedoch auch die sich anschließende Beschlagnahme eines Gegenstands aus der Wohnung.[451] Diese Parallele ist angesichts des gelieferten Begründungszusammenhangs nur konsequent. Denn der Auswertung eines beschlagnahmten informationstechnischen Systems fehlt es an einer „technischen Infiltration". Der Zugang zu den enthaltenen Informationen beruht nicht auf der Manipulation von Zugriffsberechtigungen, sondern an der verlorenen sozialen Kontrolle des Berechtigten über sein System. Der Zugriff wird durch den unmittelbaren körperlichen Zugang zu dem System ermöglicht, nicht hingegen dadurch, dass Datenverarbeitungsvorgänge des informationstechnischen Systems mit zusätzlichen technischen Mitteln wahrnehmbar gemacht werden.[452] Die Beschlagnahme eines komplexen informationstechnischen Systems stellt danach keinen Eingriff in den Schutzbereich des *GVIiS* dar. Die Beschlagnahme eines körperlichen Gegenstands ist an Art. 14 Abs. 1 GG zu messen, da der Grundrechtseingriff in der fortdauernden Besitzentziehung liegt.[453] Wird kein körperlicher Gegenstand beschlagnahmt, richtet sich die Zulässigkeit der Maßnahme nach Art. 2 Abs. 1 GG.[454] Sofern Daten von der Beschlagnahme betroffen sind, greift sodann das *RiS*,[455] da die von diesem Recht[456] geschützte Befugnis, grds. selbst über Preisgabe und Verwendung persönlicher Daten zu entscheiden, berührt wird.[457] Einen Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG stellt demnach nur die Durchsuchung dar.[458] Die durch die Infiltration eines informationstechnischen Systems ermöglichte Datenerhebung lässt sich somit nicht als Argument für die Anwendbarkeit des Art. 13 Abs. 1 GG anführen. Denn schon weil die Phase der Datenerhebung keinen Eingriff mehr in die Unverletzlichkeit der Wohnung darstellt, kann es für die Eröffnung des Schutzbereichs des Art. 13 Abs. 1 GG auf den Inhalt und die Sensibilität der so zu gewinnenden Informationen nicht ankommen.

(iii) Gefahr der Reduzierung der grundrechtlichen Gewährleistung

Daher greift auch der Einwand, mit der Ablehnung der Eröffnung des Schutzbereichs des Art. 13 Abs. 1 GG sei die Gefahr verbunden, die Reichweite des Schutzbereichs von den technischen Möglichkeiten der Ermittlungsbehörden

450 *BVerfGE* 120, 274 (311).
451 *BVerfGE* 113, 29 (45); *BVerfGK* 1, 126 (133).
452 Siehe hierzu oben S. 4.
453 Vgl. *BVerfG* NJW 2009, 281 (282); MMR 2009, 673 (675).
454 *BVerfGE* 113, 29 (45).
455 *BVerfGE* 113, 29 (45); *BVerfG* MMR 2009, 673 (675).
456 *BVerfGE* 65, 1 (43).
457 *BVerfGE* 113, 29 (46).
458 Vgl. *BVerfG* NStZ 2002, 377 (378).

abhängig zu machen und damit kontinuierlich zu reduzieren,[459] nicht durch. Sicherlich darf technischer Fortschritt nicht zu einer Verkürzung des grundrechtlichen Schutzes führen. Jedoch setzt eine solche Verkürzung voraus, dass ein zu reduzierender Schutzbereich überhaupt betroffen ist. In Hinblick auf Art. 13 Abs. 1 GG erfordert dies jedoch, dass „die heutigen technischen Gegebenheiten es erlauben, in die *räumliche* Sphäre […] einzudringen".[460] Folglich muss es sich bei technisch neuartigen Ermittlungsmethoden um solche handeln, bei denen die neuartige Technik ein körperliches Betreten zur Überwindung dieser räumlichen Sphäre ersetzt, dabei aber gerade die räumliche Sphäre vorhanden ist, die überwunden werden muss. Wenn aber von vornherein ein Überwinden mangels körperlicher Grenzen nicht notwendig ist, ist auch der spezifische grundrechtliche Schutzgehalt mangels Abwehrfunktion nicht betroffen. Daher dürfte auch der Argumentation des *BVerfG*, „der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein",[461] keine Konstruierung des Schutzbereichs des Art. 13 Abs. 1 GG allein aus der Perspektive der das System infiltrierenden Ermittlungsbehörde zu entnehmen sein.[462] Der Schutzbereich des Art. 13 Abs. 1 GG ist nicht deswegen nicht eröffnet, weil die Ermittlungsbehörden aufgrund ihrer Unkenntnis vom Standort des informationstechnischen Systems nicht wissen könnten, wann der Zugriff den Anforderungen der verfassungsrechtlichen Rechtfertigung eines Eingriffs in Art. 13 Abs. 1 GG genügen müsste.[463] Vielmehr dürften die Ausführungen so zu verstehen sein, dass es für die technische Durchführbarkeit der Maßnahme regelmäßig keinen Unterschied macht, wo sich das System befindet, die räumliche Privatsphäre keine besonderen Anforderungen an die Realisierbarkeit stellt und der Standort des Systems deshalb „ohne Belang" ist. Der physische Zugriff auf ein informationstechnisches System ist demgegenüber wie der Zugriff auf einen körperlichen Informationsträger weiterhin an Art. 13 Abs. 1 GG zu messen.

(iv) Unzureichende dogmatische Begründung

Schließlich überzeugt auch die Kritik an der gegenständlichen Entscheidung nicht, es sei dogmatisch nicht überzeugend, dass gerade die Ablehnung des Schutzbereichs des Art. 13 Abs. 1 GG zur Begründung der verfassungsrechtlichen Schutz-

[459] *Hornung*, JZ 2007, 828 (829); *ders.*, CR 2008, 299 (301); ähnlich auch *Schantz*, KritV 2007, 310 (317) („Vorbehalt des technischen Fortschritts") und *Sokol*, LT-NRW-Stellungnahme 14/625, S. 10 (Reduzierung des Grundrechtsschutzes nur aufgrund der Nutzung moderner Kommunikations- und Speichermedien).

[460] *BVerfGE* 109, 279 (309) (Hervorhebung nur hier).

[461] *BVerfGE* 120, 274 (311).

[462] So aber *Hornung*, CR 2008, 299 (301); ebenso schon *ders.*, DuD 2007, 575 (578); *Schantz*, KritV 2007, 310 (317).

[463] So aber *Weiß*, Online-Durchsuchungen, S. 127f.

lücke führe, die durch das *GVIiS* ausgefüllt wird.[464] Denn die lückenschließende Funktion des allgemeinen Persönlichkeitsrechts setzt gerade voraus, dass die Schutzbereiche der besonderen Freiheitsrechte - in diesem Fall derjenige des Art. 13 Abs. 1 GG - hinsichtlich bestimmter Elemente der Persönlichkeit nicht eröffnet sind, deren Bedeutung aber nicht hinter den besonderen Freiheitsrechten zurücksteht.[465] Die Erfassung dieser Elemente durch neue Konkretisierungen des allgemeinen Persönlichkeitsrechts im Wege richterlicher (Verfassungs-)Rechtsfortbildung ist die logische Folge und nicht originär und einzigartig mit dem *GVIiS* verbunden. Vielmehr kommen die gleichen normativen Prämissen zur Anwendung, auf denen die Konkretisierungen der anderen Schutzdimensionen des Persönlichkeitsrechts gründen.[466] Das *BVerfG* hält lediglich an den Grundsätzen seiner bisherigen Rechtsprechung fest.[467] Insofern lässt sich zwar die Ablehnung des Schutzbereichs des Art. 13 Abs. 1 GG an sich kritisieren, nicht jedoch die sich daran notwendigerweise anschließende lückenschließende Funktion des allgemeinen Persönlichkeitsrechts.

(v) Zwischenergebnis

Die Unverletzlichkeit der Wohnung steht einer ungewollten Informationsgewinnung nur dann entgegen, wenn diese den Grenzen der durch eine Wohnung vermittelten räumlichen Privatsphäre unterworfen ist. Art. 13 Abs. 1 GG schützt nur vor solchen Einblicken in die Privatsphäre, denen sich der Einzelne durch eine räumliche Abschottung entziehen kann. Wenn eine räumliche Barriere gegenüber einer bestimmten Form der Informationsgewinnung keinerlei Grenze setzen kann, kann sich dieser Zugriffsmethode gegenüber zwangsläufig auch keine räumliche Privatsphäre ausbilden. Anders als beim Einsatz technischer Hilfsmittel i.S.d. „Großen Lauschangriffs" existiert beim Zugriff auf ein informationstechnisches System über ein Kommunikationsnetz keine räumliche Grenze, die überwunden werden müsste. Für den Vorgang der Informationsgewinnung macht es keinen Unterschied, ob sich das System in einer Wohnung befindet oder nicht. Ein raumbezogener Schutz erfasst die spezifische Gefährdung eines informationstechnischen Systems daher nicht generell, sondern der durch Art. 13 Abs. 1 GG vermittelte Schutz vor der Infiltration eines informationstechnischen Systems ist

---

464 So *Hornung*, CR 2008, 299 (301); ähnlich *Kudlich*, JA 2008, 475 (478): Ablehnung des Schutzbereichs des Art. 13 Abs. 1 GG „dogmatisch ganz sicher nicht zwingend"; kritisch auch *Heise*, RuP 2009, 94 (97): Möglichkeit extensiver Auslegung bestehender Grundrechte wird nicht in Betracht gezogen.

465 *BVerfGE* 99, 185 (193); 106, 28 (39); 118, 168 (183); 120, 274 (303).

466 *Hoffmann-Riem*, JZ 2008, 1009 (1015).

467 *Hirsch*, NJOZ 2008, 1907 (1910); *Petri*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Vortrag zum 17. Wiesbadener Forum Datenschutz (abrufbar unter: http://www.datenschutz.hessen.de/forum2009.htm#entry3294).

von der Zugriffsmodalität abhängig.[468] Nur wenn der Zugriff mit der Überwindung der räumlichen Privatsphäre einer Wohnung verbunden ist, greift auch Art. 13 Abs. 1 GG.

(b) Keine Wahrnehmung von Vorgängen innerhalb der geschützten Räumlichkeit durch Infiltration

Schließlich scheitert die Eröffnung des Schutzbereichs des Art. 13 Abs. 1 GG hinsichtlich der bloßen Infiltration eines informationstechnischen Systems über ein Kommunikationsnetz noch aus einem weiteren Grund. Die Unverletzlichkeit der Wohnung schützt nur insoweit vor dem Einsatz besonderer technischer Hilfsmittel, als dadurch ein Einblick in Vorgänge innerhalb der Wohnung gewonnen wird. Die bloße Infiltration eines informationstechnischen Systems ermöglicht jedoch erst den *Zugang* zu Speicherinhalten und Funktionen des Systems, gewährt aber dadurch noch keinen solchen Einblick.[469] Anders als bei der Infiltration zwecks Überwachung der Wohnung durch die Peripheriegeräte des informationstechnischen Systems fehlt es an einer einheitlichen Maßnahme der Wohnraumüberwachung. Die Infiltration selbst ermöglicht nur eine im Anschluss erfolgende Erhebung der auf einem informationstechnischen System gespeicherten Daten. Da es somit allein durch die Infiltration jedenfalls dahingehend zu keiner Informationsgewinnung kommt, können schon deshalb keine Einblicke in Vorgänge innerhalb der Wohnung gewonnen werden.[470] Die sich anschließende und auf die Speichermedien des Systems begrenzte Datenerhebung ist wiederum nicht mehr mit einem Eingriff in die räumliche Lebenssphäre einer Wohnung verbunden.

iii. Ergebnis

Die Infiltration eines informationstechnischen Systems lässt sich nur dann als Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG verstehen, wenn

*(1)* sich das System überhaupt in einer als Wohnung geschützten Räumlichkeit befindet und

*(2)* der Zugriff unter Verletzung der räumlichen Privatsphäre einen Einblick in Vorgänge innerhalb der Wohnung verschafft, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind.

---

[468] *BVerfGE* 120, 274 (310).

[469] So auch *Schlegel*, GA 2007, 648 (656).

[470] Gegen eine Gleichsetzung der auf einem informationstechnischen System gespeicherten Daten mit „Einblicken in Vorgänge innerhalb der Wohnung" *Kemper*, ZRP 2007, 105 (109); *Gusy*, LT-NRW-Stellungnahme 14/636, S. 6; *Schwarz*, LT-NRW-Stellungnahme 14/650, S. 5; anders *Schlegel*, GA 2007, 645 (656): „Das Ergebnis, die Verkörperung von Vorgängen, welche sich in der Wohnung abgespielt haben".

Letzteres setzt voraus, dass die Grenzen einer Wohnung dergestalt überwunden werden, dass das physische Hindernis ihrer Wände, Decken und Böden, das der natürlichen Wahrnehmung des Beobachters entgegensteht, aufgehoben wird. Nur sofern die Privatsphäre des Einzelnen gerade in dieser Räumlichkeit betroffen ist, greift die Gewährleistung der Unverletzlichkeit der Wohnung. Da jedoch nicht sämtlichen Zugriffsmöglichkeiten auf ein informationstechnisches System diese Grenzen entgegenstehen, besteht gegenüber den verbleibenden Möglichkeiten kein Persönlichkeitsschutz durch Art. 13 Abs. 1 GG. Dahingehend besteht die notwendige Schutzlücke der Ergänzungsfunktion des allgemeinen Persönlichkeitsrechts.

c. Schutz der Privatsphäre, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Diese von den Gewährleistungen der speziellen Freiheitsrechte belassene Schutzlücke sieht das *BVerfG* auch nicht von bisherigen Konkretisierungen des allgemeinen Persönlichkeitsrechts geschlossen. Zunächst wird der notwendige Schutz nicht von der Ausprägung des allgemeinen Persönlichkeitsrechts als Schutz der Privatsphäre gewährleistet.[471] Als solches sichert das allgemeine Persönlichkeitsrecht „einen räumlich und thematisch näher bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll".[472] Die räumliche Bestimmung dieses Bereichs richtet sich nach der Möglichkeit für den Einzelnen, „zu sich zu kommen, sich zu entspannen oder auch gehen zu lassen", während in thematischer Hinsicht Angelegenheiten erfasst werden, deren Erörterung oder Zurschaustellung als unschicklich gilt, das Bekanntwerden als peinlich empfunden wird oder nachteilige Reaktionen der Umwelt auslöst.[473] Der Mensch soll „unbeobachtet sich selbst überlassen" sein oder „mit Personen seines besonderen Vertrauens ohne Rücksicht auf gesellschaftliche Verhaltenserwartungen und ohne Furcht vor staatlichen Sanktionen" verkehren können.[474] Wie weit dieser Schutz der Privatsphäre reicht, lässt sich nicht generell und abstrakt festlegen.[475] Der Schutz erschöpft sich jedoch nicht in der Abwehr der körperlichen Zugänglichkeit eines solchen privaten Bereichs, sondern beinhaltet auch diejenige der bloß kognitiven Zugänglichkeit.[476] Privatsphärenschutz bedeutet damit vornehmlich Schutz gegen Informationseingriffe.[477] Der durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vermittelte Schutz der Privatsphäre erfasst damit auch die private Information, und somit auch den Inhalt der von einem informationstechnischen System gespeicherten Daten.

---

[471] *BVerfGE* 120, 274 (311).
[472] *BVerfGE* 120, 274 (311).
[473] *BVerfGE* 101, 361 (382f.).
[474] *BVerfGE* 90, 255 (260).
[475] *BVerfGE* 120, 180 (199).
[476] Vgl. *Horn*, in: HStR VII³, § 149 Rn. 46.
[477] *Lorenz*, in: BK GG, Bd. 1, Art. 2 Abs. 1 Rn. 280.

Da die Abgrenzung der Schutzbereiche der einzelnen grundrechtlichen Gewährleistungen im gegenständlichen Urteil nicht anhand konkreter Daten erfolgte, lassen sich hier nur die vom *BVerfG* benannten typischen Fallgruppen der Nutzung eines informationstechnischen Systems anführen. Unter den thematisch geschützten Bereich der Privatsphäre des allgemeinen Persönlichkeitsrechts dürften etwa „private Text-, Bild oder Tondateien", Daten mit „detaillierten Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private […] Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen"[478] sowie „schriftliche Verkörperungen des höchstpersönlichen Erlebens"[479] fallen. Nicht erfasst wären demgegenüber die geschäftliche Korrespondenz oder *sämtliche* Inhalte von „E-Mails oder anderen Kommunikationsdiensten des Internet"[480] und *alle* „flüchtigen oder nur temporär gespeicherten Daten"[481]. Somit können die auf einem informationstechnischen System gespeicherten Daten nicht allein der Privatsphäre des Betroffenen zugeordnet werden.[482] Schon die Nutzung eines informationstechnischen Systems für geschäftliche Zwecke führt dazu, dass auch Daten anfallen, die nicht privater Natur sind. Daneben steht einem umfassenden Schutz durch die grundrechtlich gesicherte Privatsphäre entgegen, dass die Zuordnung eines Datums zur geschützten Privatsphäre die Erkennbarkeit des privaten Charakters voraussetzt. Der Privatsphärenschutz ist nicht gleichbedeutend mit der Definition von Privatheit, sondern beinhaltet die Selbstbestimmung des Betroffenen innerhalb eines objektiv eröffneten Schutzbereichs, welchen Umstand er in seinen bestehenden Privatsphärenschutz einbeziehen möchte.[483] Der Einzelne muss begründetermaßen und somit auch für Dritte erkennbar davon ausgehen können, sich innerhalb der Grenzen der geschützten Privatsphäre zu bewegen.[484] Lassen sich diese Grenzen objektiv nicht erkennen, weil etwa der „Kontext, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden"[485] können, für Dritte nicht erkennbar ist, ist für diese Daten auch der Schutzbereich nicht eröffnet. Durch die Infiltration des informationstechnischen Systems verliert der Betroffene die von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützte Möglichkeit, über die Zugänglichkeit von Informationen zu bestimmen, die seiner Privatsphäre zuzuordnen sind. Die Infiltration ermöglicht jedoch nicht nur die Erhebung nur privater Daten. Den umfassenden Zugriff auf das informationstechnische System vermag der Privatsphärenschutz des allgemeinen Persönlichkeitsrechts somit nicht zu vermitteln.

---

478 *BVerfGE* 120, 274 (322f.).
479 *BVerfGE* 120, 274 (336).
480 *BVerfGE* 120, 274 (336).
481 *BVerfGE* 120, 274 (324).
482 *BVerfGE* 120, 274 (311).
483 *Horn*, in: HStR VII³, § 149 Rn. 44.
484 Vgl. *BVerfGE* 101, 361 (384).
485 *BVerfGE* 120, 274 (311).

d. Das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Zuletzt sah das *BVerfG* das besondere Schutzbedürfnis des Nutzers eines informationstechnischen Systems auch nicht als vom Schutzbereich des *RiS* erfasst an. Für diese Abgrenzung innerhalb des allgemeinen Persönlichkeitsrechts sah sich das Gericht starker Kritik ausgesetzt. Diese störte sich vor allem an einer vermeintlichen Verkürzung des Schutzbereichs des *RiS*, die erst zur Notwendigkeit der Formulierung des *GVIiS* geführt habe. Dessen Schutzbereich hätte auch im Rahmen der Verhältnismäßigkeitsprüfung innerhalb des *RiS* Berücksichtigung finden können. Tatsächlich bleibt die Argumentation des *BVerfG* an vielen Stellen unklar und auch teilweise verwirrend. Im Ergebnis ist der vorgenommenen Abgrenzung aber zuzustimmen. Die Schutzansätze des *GVIiS* und des *RiS* sind gänzlich anders konzipiert. Im Folgenden werden diese Unterschiede dargestellt und die entsprechenden Passagen des gegenständlichen Urteils kritisch untersucht.

i. Schutzbereich und Eingriff

Das *RiS* gibt dem Einzelnen die Befugnis grds. selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[486] Diese Befugnis ist nicht auf Informationen beschränkt, die bereits ihrer Art nach sensibel sind.[487] Der Schutz des *RiS* reicht dahingehend weiter als der Privatsphärenschutz des allgemeinen Persönlichkeitsrechts. Er knüpft nicht entscheidend an die Art der Information an, sondern an ihre Nutzbarkeit und Verwendungsmöglichkeit durch den Staat, so dass ein inhaltlich belangloses Datum insofern nicht existiert.[488] Der Schutz des *RiS* ist daher unabhängig von der qualitativen Aussagekraft der betroffenen persönlichen Daten.[489] Das *RiS* verschafft dem Einzelnen zur freien Entfaltung seiner Persönlichkeit Schutz gegen die „unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten".[490] Diese Maßnahmen stellen jeweils einen eigenständigen unabhängig von seiner Erheblichkeit gesondert zu beurteilenden Grundrechtseingriff dar.[491] Das *RiS* sichert das sich aus dem Gedanken der Selbstbestimmung folgende Recht, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[492] Seinen Schutzbereich kennzeichnet der funktionale Bezug auf die in der potentiellen Verwendung der verfügbaren Daten liegende Persönlichkeitsgefährdung.[493] Das *RiS* verlagert insoweit den grundrechtlichen Schutz von Ver-

[486] *BVerfGE* 65, 1 (43); 84, 192 (194); 118, 168 (184); 120, 274 (312).
[487] *BVerfGE* 118, 168 (185); 120, 274 (312).
[488] *BVerfGE* 65, 1 (45); 118, 168 (185).
[489] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 174.
[490] *BVerfGE* 65, 1 (43).
[491] Vgl. *Hufen*, Staatsrecht II, § 12, Rn. 8f.
[492] *BVerfGE* 65, 1 (42).
[493] *Lorenz*, in: BK GG, Bd. 1, Art. 2 Abs. 1 Rn. 331.

haltensfreiheit und Privatheit auf die Stufe der Grundrechtsgefährdung vor.[494] Erhebung, Verknüpfung, Verarbeitung und Nutzung personenbezogener Daten und Informationen können schwerwiegende Eingriffe in die Freiheit und Privatheit des Betroffenen nach sich ziehen, gegen die sich der Betroffene nicht mehr erfolgreich zur Wehr setzen kann, wenn er mit den Ergebnissen staatlicher Informationsprozesse erst bei einem solchen Eingriff konfrontiert wird.[495]

ii. Schutzlücke gegenüber neuartigen Gefährdungen

Die ausgemachte Schutzlücke grundrechtlichen Persönlichkeitsschutzes aufgrund von Gefährdungen, die sich aus der Nutzung informationstechnischer Systeme ergeben, wird von dem *BVerfG* folgendermaßen begründet:[496]

> „*Jedoch trägt das Recht auf informationelle Selbstbestimmung 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.*“

Einen solchen Schutzbedarf sieht das Gericht aber nicht bei sämtlichen informationstechnischen Systemen:

> „*Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält* […] *unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen.*“ [497]

Eine Persönlichkeitsgefährdung, die über den Schutz der menschlichen Persönlichkeit durch das *RiS* hinausgeht, bestünde nur bei solchen informationstechnischen Systemen,

> „*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*“[498].

---

494 *BVerfGE* 118, 168 (184); 120, 274 (312); *Bäcker*, Der Staat [2012], S. 91 (96) (102).
495 *Bäcker*, in: *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (4); *ders.*, Der Staat [2012], 91 (96).
496 *BVerfGE* 120, 274 (313).
497 *BVerfGE* 120, 274 (313).
498 *BVerfGE* 120, 274 (314).

Die so festgestellte Schutzlücke kann das *RiS* aber nur dann belassen, wenn die nach Ansicht des *BVerfG* bestehenden neuartigen Gefährdungen der Persönlichkeit, die mit der Nutzung eines informationstechnischen Systems verbunden sind, nicht von dem Schutz des Einzelnen durch das *RiS* gegen die „unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" erfasst wären. Dies ist aus mehreren Gründen nicht der Fall.

(1) Personenbezogenes Datum als Schutzgegenstand

Das *RiS* hat zunächst einen anderen Schutzgegenstand als das *GVIiS*. Es knüpft an den Begriff des personenbezogenen Datums an.[499] Letzterer kann den Schutzbereich des *GVIiS* nur unzureichend beschreiben. Die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung personenbezogener Daten zu entscheiden" überschneidet sich zwar mit dem Interesse des Nutzers eines informationstechnischen Systems an der Vertraulichkeit der auf dem System gespeicherten Daten. Für den Zugriff auf das System und damit die Zugänglichkeit der vermittelten Informationen ist gleichfalls die Entscheidung des berechtigten Nutzers entscheidend. Der Schutzbereich des *RiS* erfasst aber nicht den einer Datenerhebung vorgelagerten bloßen Zugriff auf das informationstechnische System selbst.[500] In den Schutzbereich des *GVIiS* wird bereits mit der Infiltration des Systems eingegriffen, ohne dass dabei schon personenbezogene Daten erhoben wurden.[501] Mit diesem Zugriff verschafft sich der Dritte unberechtigterweise eine Zugriffsmöglichkeit auf das informationstechnische System, so dass allein mit diesem Zugriff nicht mehr sichergestellt ist, dass Informationen nur dem berechtigten Nutzer des Systems zugänglich sind. Die Vertraulichkeit des informationstechnischen Systems ist somit schon durch den bloßen Zugriff auf das System betroffen. Ihr Schutz reicht also weiter als der Schutz nur gegen die Erhebung personenbezogener Daten.[502] Das *GVIiS* schützt ferner auch dagegen, dass auf das informationstechnische System insgesamt zugegriffen wird, und nicht nur auf gespeicherte Daten.[503] Zusätzlich setzt der Schutz der Vertraulichkeit keinen Personenbezug der betroffenen Daten voraus. Der Schutzbereich des *GVIiS* erfasst auch reine Sachdaten. In gleicher Weise wird die Integrität des informationstechnischen Systems bereits durch dessen technische Infiltration verletzt, ohne dass es zu einer Datenverarbeitung i.w.S. kommen muss. Schon die Infiltration setzt zwangsläufig die Manipulation des Systems voraus.[504] Eine relevante Erhebung u.U. auch personenbezogener Daten, anhand derer die besondere Persönlichkeitsgefährdung schon der Infiltration hinreichend berücksichtigt werden kann, liegt

499 *BVerfGE* 65, 1 (42), verweist hierzu auf die Definition des § 2 Abs. 1 BDSG 1977.
500 A.A. *Gudermann*, Online-Durchsuchung, S. 90, 166f.
501 *Petri*, Vortrag Wiesbadener Forum (Fn. 467), Ziff. 2.2.
502 A.A. *Eifert*, NVwZ 2008, 521.
503 *BVerfGE* 120, 274 (313).
504 *Buermeyer/Bäcker*, HRRS 2009, 433 (439); *Braun/Roggenkamp*, K&R 2011, 681 (684); *Skistims/Roßnagel*, ZD 2012, 3 (5f.).

allein in der bloßen Infiltration noch nicht. Mit der Infiltration ist aber diejenige technische Hürde genommen, das System auszuspähen, zu überwachen oder zu manipulieren.[505] Der Schutzbereich des *GVIiS* beginnt damit bereits vor einer konkreten Datenerhebung.[506] Es schließt insofern eine Schutzlücke, die das *RiS* in Bezug auf lediglich potentielle Datenerhebungen lässt.[507]

Der Schutzgegenstand des *GVIiS* ist damit nicht das personenbezogene Datum, sondern das informationstechnische System als besondere technische Sphäre der Persönlichkeitsentfaltung.[508] Die Konzipierung des Schutzbereichs des *GVIiS* ähnelt demnach mehr derjenigen des Art. 13 Abs. 1 GG als derjenigen des *RiS*. Eine solche Parallele ergibt sich bereits aus dem Wortlaut der Urteilsgründe: Das *GVIiS* „bewahrt den persönlichen und privaten *Lebensbereich* der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als *auf das informationstechnische System insgesamt* zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten".[509] Das Gericht benennt hier ausdrücklich einen zu schützenden Bereich, dessen Schutz nicht allein über die Anknüpfung an den Schutzgegenstand des einzelnen Datums umzusetzen ist. Der Einzelne wird schon vor dem Zugriff auf das informationstechnische System selbst geschützt. Bereits in diesem Zugriff liegt der Grundrechtseingriff. Noch deutlicher wird der Wortlaut der Urteilsgründe bei der Erörterung des Konkurrenzverhältnisses des *GVIiS* zu Art. 13 Abs. 1 GG: „*Auch* die durch Art. 13 Abs. 1 GG gewährleistete Garantie der Unverletzlichkeit der Wohnung verbürgt dem Einzelnen mit Blick auf seine Menschenwürde sowie im Interesse der Entfaltung seiner Persönlichkeit einen *elementaren Lebensraum* […]."[510] Dem Schutz der räumlichen und demjenigen der technischen Sphäre der Persönlichkeitsentfaltung liegt damit ein vergleichbares Schutzkonzept zugrunde. Der Begriff des personenbezogenen Datums wird daher vom *BVerfG* nur in Bezug auf den Funktionsumfang des informationstechnischen Systems schutzbereichseröffnend gebraucht. Dieser Umfang muss in Bezug auf die Erzeugung, Verarbeitung und Speicherung personenbezogener Daten generell zur Profilbildung geeignet sein. Das informationstechnische System muss in Bezug auf seine Funktionen eine Komplexität aufweisen, dass auf dem System „personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten [sein] 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

505 *BVerfGE* 120, 274 (314).
506 *Petri*, DuD 2008, 443 (446); *Karg*, ZD 2012, 255 (259).
507 *Petri*, Vortrag Wiesbadener Forum (Fn. 467), Ziff. 2.1.
508 Vgl. *Bäcker*, in: *Uerpmann-Wittzack* (Hrsg.) Computergrundrecht, S. 1 (9); *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (119); *ders.*, Der Staat [2012], S. 91 (93f.). ähnlich *Popp*, ZD 2012, 51 (52): Durch informationstechnisches System vergegenständlichte informationelle Geheimsphäre.
509 *BVerfGE* 120, 274 (313) (Hervorhebungen nur hier).
510 *BVerfGE* 120, 274 (309) (Hervorhebungen nur hier).

Persönlichkeit zu erhalten".[511] Tatsächlich gefordert wird hingegen nur die Fähigkeit, einen solchen Datenbestand zu generieren, nicht hingegen, dass dieser auch tatsächlich auf dem betroffenen System vorhanden ist. Dieser Schutzansatz ist nur konsequent. Denn die „entscheidende technische Hürde" wird bei dem Zugriff auf ein informationstechnisches System bereits genommen, bevor ein solcher Datenbestand verlässlich festzustellen ist. Ein vollumfänglicher Persönlichkeitsschutz, der auch den Schutzbereich des *GVIiS* umfasst, lässt sich damit allein über das Tatbestandsmerkmal des personenbezogenen Datums nicht realisieren.[512] Das *BVerfG* hat folgerichtig die Schutzgegenstände des allgemeinen Persönlichkeitsrechts über das personenbezogene Datum hinaus auf das informationstechnische System erweitert.[513] Die Ausnahme wenig komplexer Systeme mit einem bloß „punktuellen Bezug zu einem bestimmten Lebensbereich" lässt sich damit begründen, dass sich in diesen Fällen die Persönlichkeitsrelevanz nicht aus der Entfaltung des Nutzers mittels der Nutzung zahlreicher in einem Gegenstand vereinter Funktionen ergibt, sondern aus dem bloßen Informationsgehalt der Daten eines ganz spezifischen Ausschnitts der Persönlichkeit. Insoweit kann die Relevanz dieses Informationszugriffs für die Persönlichkeit des Betroffenen mit dem Merkmal des Personenbezugs vollständig erfasst werden.

(2) Einzigartige Informationsquelle

Aus diesem Schutzgegenstand folgt, dass für das Konkurrenzverhältnis zwischen dem *GVIiS* und dem *RiS* nicht allein die „Erhebung, Speicherung, Verwendung und Weitergabe" gespeicherter personenbezogener Daten maßgeblich sind. Setzt man die hierin liegenden zeitgleichen zahlreichen Eingriffe in das *RiS* mit dem Zugriff auf ein informationstechnisches System gleich, so ließe sich für eine Schutzlücke des bisherigen Schutzumfangs anführen, dass der umfangreiche und vielfältige Bestand potentiell auf einem informationstechnischen System vorhandener Daten aus sich heraus bereits ein vollständiges Profilbild des Betroffenen verschaffen kann. Es entfällt das Erfordernis, einzelne Daten des Betroffenen noch miteinander zu verknüpfen oder weitere Daten aus anderen Quellen zu beschaffen. Personenbezogene Daten werden von dem informationstechnischen System zu einer auf einmal und immer wieder zugänglichen, dynamischen Gesamtheit aggregiert.[514] Für ein vollständiges Persönlichkeitsprofil genügt die eine Erhebung dieser Datengesamtheit. Eine derartige Fülle von Informationen ließ sich in der Vergangenheit entweder gar nicht oder nur durch aufwändige Ermitt-

[511] *BVerfGE* 120, 274 (314).

[512] I.d.S. auch *Karg*, ZD 2012, 255 (259), der die Eignung des Merkmals des Personenbezugs zur vollständigen Erfassung der Gefährdung von Persönlichkeitsrechten verneint; ebenso *Schneider/Härting*, ZD 2011, 63 (65).

[513] *Härting/Schneider*, ZRP 2011, 233 (235).

[514] *T. Böckenförde*, JZ 2008, 925 (928); i.d.S. betont auch *Wieczorek*, DuD 2012, 476 (477), die Leistungsfähigkeit des informationstechnischen Systems zur Aufbereitung des informativen Gehaltes der gespeicherten Daten in persönlichkeitsrechtsgefährdender Art und Weise.

lung zusammentragen.[515] Bestehende Verarbeitungs- und Verknüpfungsmöglichkeiten des Erhebenden werden irrelevant, da das informationstechnische System bereits ein vollständiges Bild der Persönlichkeit liefern kann. Allerdings schützt auch schon das *RiS* vor der Erstellung von Persönlichkeitsbildern durch die Verwertung einzelner Datenerhebungen.[516] Die mit der Erfassung des gesamten Datenbestands eines informationstechnischen Systems verbundenen einzelnen Eingriffe in das *RiS* ließen sich daher auch in ihrer Gesamtheit als einziger besonders schwerer Eingriff behandeln.[517] Wird eine Person zur Verfolgung derselben Zwecke weitgehend zeitgleich einer Vielzahl gleicher Grundrechtseingriffe ausgesetzt, macht die daraus resultierende potenzierte Beeinträchtigung dieses einen Grundrechts eine Addierung der einzelnen Eingriffe zu einer Gesamtbeeinträchtigung anstelle der gesonderten grundrechtlichen Prüfung punktueller Beeinträchtigungen notwendig (sog. additiver Grundrechtseingriff).[518] Zur angemessenen Berücksichtigung der Gesamtbelastung eines solchen Eingriffsbündels böten sich besondere Anforderungen an die Verhältnismäßigkeit i.e.S. innerhalb der verfassungsrechtlichen Rechtfertigung des Einzeleingriffs an.[519] In gleicher Form könnte auch die Vielfalt der personenbezogenen Daten erfasst werden.[520] Die Abgrenzung beider Schutzbereiche kann daher nicht allein auf die Vielfalt und den Umfang der zu erlangenden Daten beschränkt werden. Gegen eine solche Abgrenzung wird zu Recht eingewandt, dass dem *RiS* ohne nähere Begründung die Schutzfähigkeit für einen viel gewichtigeren Eingriff als einer einzelnen Datenerhebung abgesprochen würde.[521] Insoweit formuliert das *BVerfG* zumindest missverständlich, wenn in

---

[515] *Bäcker*, in: *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (8).

[516] *BVerfGE* 65, 1 (42); 112, 304 (319).

[517] So auch *Britz*, DÖV 2008, 411 (413); *Hornung*, CR 2008, 299 (301f.); *Heise*, RuP 2009, 94 (98); *Martini*, JA 2009, 839 (840); *Kube*, in: HStR VII³, § 148 Rn. 70; *Hoffmann-Riem*, JZ 2008, 1009 (1016), bezweifelt, ob das *RiS* auch solche personenbezogenen Daten schützt, die der Betroffene nicht selbst anlegt, sondern die von einem informationstechnischen System selbsttätig generiert werden. Denn problematisch sei, dass die Schutzmöglichkeiten des Betroffenen nicht nur ein besonderes Gefahrenbewusstsein und beträchtlichen technischen Sachverstand voraussetzten, die nicht von allen Nutzern erwartet werden könnten, sondern die Unterbindung der Generierung solcher Daten mit nicht unerheblichen Funktionseinbußen verbunden sein könnten. Zu bedenken ist aber, dass das *RiS* gerade nicht nur diejenigen personenbezogenen Daten schützt, von denen der Betroffene Kenntnis hat, sondern voraussetzt, dass der Bürger eben diese Kenntnis erlangen kann, wer was wann und bei welcher Gelegenheit über ihn weiß (vgl. *BVerfGE* 65, 1 (43)). Die fehlende Kenntnis von der Existenz bestimmter personenbezogener Daten beseitigt nicht die Befugnis, über ihre Preisgabe und Verwendung zu entscheiden. Hierfür spricht etwa die Entscheidung des *BVerfG* zur automatischen Kennzeichenerfassung, deren Zulässigkeit am *RiS* geprüft wird (*BVerfG* 120, 378 (397ff.)). Jedenfalls aber dürfte angesichts der Schwierigkeiten der Wahrnehmung von Schutzmöglichkeiten keine einverständliche Preisgabe personenbezogener Daten bloß darin gesehen werden kann, dass entsprechende Selbstschutzmethoden nicht ergriffen wurden.

[518] *Lücke*, DVBl. 2001, 1469 (1470).

[519] *Voßkuhle/Kaiser*, JuS 2009, 313 (314); vgl. auch *BVerfGE* 112, 304 (319f.).

[520] So auch ausdrücklich *BGH* MMR 2007, 237 (238).

[521] *T. Böckenförde*, JZ 2008, 925 (927).

den Urteilsgründen ausgeführt wird, dass der Zugriff auf ein informationstechnisches System „in seinem Gewicht für die Persönlichkeit des Betroffenen über *einzelne Datenerhebungen*, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus[geht]".[522] Das *RiS* schützt gerade nicht nur vor „einzelnen Datenerhebungen".[523]

Allein der Umfang und die Vielfalt des enthaltenen Bestands an personenbezogenen Daten und damit die bloße Zahl der Eingriffe in das *RiS* können jedoch für die Abgrenzung nicht entscheidend sein. Der Schutz des *GVIiS* ist an einem bloß potentiellen Datenbestand ausgerichtet, dessen Umfang und Vielfalt aber im konkreten Fall nicht tatsächlich nachgewiesen werden müssen, sondern angesichts der vielfältigen Nutzungsmöglichkeiten eines hinreichend komplexen informationstechnischen Systems typischerweise vorliegen. Hingegen können Umfang und Vielfalt des tatsächlich vorhandenen Datenbestands im Einzelfall sehr unterschiedlich ausfallen und damit auch die Zahl der Eingriffe in das *RiS*, zu denen es bei der Erfassung des gesamten Datenbestands kommt. Die gleichen Unterschiede würden sich demzufolge auch bei der grundrechtlichen Relevanz der staatlichen Maßnahme ergeben. Der Rechtfertigungsbedarf müsste sich also mal erhöhen und dann auch wieder nur geringeren Anforderungen genügen müssen. Wenn aber eine tatsächlich erfolgende Datenerfassung nicht die Grundlage des Schutzes des *GVIiS* ist, können folglich auch Umfang und Vielfalt des betroffenen Datenbestands und damit Zahl und Schwere der Eingriffe in das *RiS* nicht die Grundlage der Abgrenzung zum *GVIiS* sein.

Eingriffe in den Schutzbereich des *GVIiS* macht das *BVerfG* unabhängig vom konkreten Datenbestand von einheitlichen hohen Voraussetzungen abhängig. Denn schon das Eindringen in die technisch definierte Schutzsphäre begründet einen persönlichkeitsrechtlichen Eingriff, ohne dass dessen Relevanz von dem tatsächlich vorhandenen Datenbestand abhängig wäre. Vielmehr ergibt sich schon aus einem bloß einmaligen Informationseingriff eine fortlaufende Informationsquelle. Der technische Zugriff auf ein informationstechnisches System erfasst nicht allein die Erhebung oder Verarbeitung personenbezogener Daten, sondern beschreibt die Überwindung der technischen Sicherungen des Systems, so dass dieses dem Dritten unbeschränkt zugänglich ist. Je nach Infiltrationsmethode - ausdrücklich werden vom *BVerfG* das Ausnutzen von Sicherheitslücken oder die Installation eines Spähprogramms genannt[524] - wird der Ermittlungsbehörde unter Umständen jedoch der Zugang zu dem System über einen längeren Zeitraum ermöglicht. Die einer Ausspähung oder Überwachung entgegenstehende technische Hürde wird grundsätzlich überwunden.[525] Gelingt die Installation eines sog.

[522] *BVerfGE* 120, 274 (313) (Hervorhebungen nur hier).
[523] Insoweit zu Recht *Britz*, DÖV 2008, 411 (413); *Eifert*, NVwZ 2008, 521; *Hoeren*, MMR 2008, 365 (366); *Hornung*, CR 2008, 299 (301); *Sachs/Krings*, JuS 2008, 482 (484); *Volkmann*, DVBl. 2008, 590 (591).
[524] *BVerfGE* 120, 274 (276).
[525] *Hoffmann-Riem*, JZ 2008, 1009 (1017).

Spähprogramms, so stehen der Ermittlungsbehörde „Leistungen, Funktionen und Speicherinhalte“ des informationstechnischen Systems solange zur Verfügung, als dieses Programm vom Betroffenen nicht entdeckt und entfernt oder in seiner Funktionsfähigkeit beeinträchtigt wird. Bleibt das Programm vom Nutzer unentdeckt, so dauert die Infiltration solange an, bis das Programm von der Ermittlungsbehörde selbst deinstalliert oder gelöscht wird und die Kompromittierung des Systems - sofern technisch überhaupt möglich - rückgängig gemacht wird. Sofern der Zugriff über einen Exploit geschieht und eine Sicherheitslücke der Softwarekomponenten des Systems ausnutzt, öffnet sich für die Ermittlungsbehörde dieselbe dauerhafte Informationsquelle, sofern die Kompromittierung des Systems über die Ermöglichung des einmaligen Zugangs hinausgeht. Auch hierbei stünde die Informationsquelle solange zur Verfügung, als die von dem Exploit ausgenutzte Sicherheitslücke vom Betroffenen nicht geschlossen wird. Der hierdurch bestehenden fortlaufenden Gefährdung der Persönlichkeitsentfaltung des Betroffenen durch die Infiltration seines Systems und der damit verbundenen dauerhaften Möglichkeit des Staates, jederzeit die von dem informationstechnischen System erzeugten, verarbeiteten und gespeicherten personenbezogenen Daten zu erheben, kann nicht mit dem *RiS* begegnet werden. Denn diese dauerhafte Gefährdungslage der fortdauernden Aufhebung der Vertraulichkeit und Integrität des informationstechnischen Systems durch die einmalige Überwindung der technischen Sicherungen des Systems wird von einer isolierten Betrachtung der konkreten Datenerhebung nicht erfasst.[526] Denn das *RiS* ist auf einzelne Datenerhebungen ausgerichtet, nicht aber auch auf die permanente Erhebung und Verknüpfung von personenbezogenen Daten, die sich an eine Infiltration anschließen.[527]

Eine solche Erhebung und Verknüpfung fällt genau aus diesem Grunde gleichfalls in den Schutzbereich des *GVIiS*.[528] Zwar schützt auch das *RiS* schon vor der Erstellung von Persönlichkeitsbildern durch die Verwertung einzelner Datenerhebungen.[529] Die dauerhafte Infiltration des informationstechnischen Systems verschafft dem Zugreifenden aber eine Informationsquelle über den Betroffenen, deren Umfang und Vielfalt an personenbezogenen Daten die Erschließung weiterer Informationsquellen entbehrlich macht. Das *BVerfG* spricht davon, dass der zu erlangende Datenbestand „herkömmliche Informationsquellen […] bei weitem übertreffen kann“.[530] Daneben entfällt auch die Notwendigkeit, die Informationen verschiedener Quellen miteinander verknüpfen zu müssen. Unberücksichtigt blie-

---

[526] Ebenso *Hoffmann-Riem*, JZ 2008, 1009 (1017): Das *RiS* schützt nicht davor, dass „ein virtueller Fuß in die Tür“ zur Persönlichkeit gestellt wird.

[527] *Kahl/Ohlendorf*, JuS 2008, 682 (685).

[528] I.E. ebenso *Hoffmann-Riem*, JZ 2008, 1009 (1019); *Hoffmann*, CR 2010, 514 (517): Das *GVIiS* ist stets einschlägig, wenn für die Datenerhebung auf ein informationstechnisches System zugegriffen wird.

[529] *BVerfGE* 65, 1 (42); 112, 304 (319).

[530] *BVerfGE* 120, 274 (322).

be schließlich auch der Informationswert reiner Sachdaten. Der Informationsgehalt eines solchen Grundrechtseingriffs liegt daher über der Summe des Informationsgehalts einzelner vorhandener personenbezogener Daten.[531] Die Ausführungen des *BVerfG*, dass das *RiS* nur vor einzelnen Datenerhebungen schütze, werden daher eher nicht normativ, sondern primär deskriptiv hinsichtlich der spezifischen Eingriffssituation zu verstehen sein.[532] Die geschaffene Informationsquelle ist gerade die spezifische Folge des Eindringens in die durch das informationstechnische System gebildete technische Sphäre der Persönlichkeitsentfaltung.

Die grundrechtlich relevante Bedrohung der Persönlichkeit resultiert bereits aus der ständigen Verfügbarkeit einer Informationsquelle, deren Umfang und Vielfalt andere Quellen entbehrlich macht. Somit setzt das *GVIiS* ebenso wie das *RiS* bereits auf der Ebene der Persönlichkeitsgefährdung an. Gegenüber dem *RiS* wird dieser Schutz aber noch einmal vorgelagert, da eine „Erhebung, Speicherung, Verwendung und Weitergabe" personenbezogener Daten tatsächlich nicht erfolgen muss. Geschützt wird bereits die eigengenutzte Infrastruktur zum Erhalt der Möglichkeit des selbstbestimmten Umgangs mit Daten sowie zum Erhalt der Freiheit und Integrität der über diese Infrastrukturen vermittelten Kommunikation.[533] Anknüpfungspunkt des Schutzes ist damit nicht das gespeicherte Datum, sondern das informationstechnische System, das als bestimmter Abschnitt der persönlichen Entfaltung und des gesellschaftlichen Lebens gegen staatliche Eingriffe abgeschirmt wird.[534] Der Betroffene soll davor bewahrt werden, dass seine Persönlichkeit „einer weitgehenden Ausspähung durch die Ermittlungsbehörden preisgegeben wird".[535] Diese Gefahr besteht bei den vom Schutzbereich des *GVIiS* ausgenommenen wenig komplexen informationstechnischen Systemen nicht. Denn soweit der Zugriff auf ein informationstechnisches System lediglich die Erhebung eines Datenbestands mit bloß punktuellem Bezug zu einem bestimmten Lebensbereich ermöglicht, wird durch diesen Zugriff gerade keine Informationsquelle geschaffen, welche die Erschließung anderer Quellen entbehrlich macht. Ein wesentlicher Einblick in die Lebensgestaltung des Betroffenen setzt hier noch die Erhebung von Informationen aus anderen Quellen und die anschließende Verknüpfung voraus.

Schwieriger stellt sich die Abgrenzung der Schutzbereiche des *GVIiS* und desjenigen des *RiS* bei der körperlichen Beschlagnahme von informationstechnischen Systemen oder deren Speichermedien dar: „Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen weist ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen auf. Dies gilt bereits für einmalige und punktuelle Zugriffe wie beispielsweise die Beschlagnahme oder Kopie von Speichermedien solcher Systeme." Das *BVerfG* verweist hierbei auf

[531] Vgl. auch *Wieczorek*, DuD 2012, 476 (477).
[532] *Hörnig*, JURA 2009, 207 (209); *Petri*, Vortrag Wiesbadener Forum (Fn. 467), Ziff. 2.1 a.E.
[533] *Hoffmann-Riem*, JZ 2008, 1009 (1016).
[534] *Bäcker*, in: *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (9).
[535] *BVerfGE* 120, 274 (328).

vorangegangene Entscheidungen, in denen jedoch nur das *RiS* Erwähnung fand.[536] Der Wortlaut der Urteilsgründe bleibt unklar, ob es bei dieser Ausgestaltung des Persönlichkeitsschutzes bleiben soll. Es liegt jedoch nahe, dass mit „einmaligen und punktuellen Zugriffen" keine hier diskutierten Zugriffe auf *technischem* Wege gemeint sind, die für die Eröffnung des Schutzbereiches des *GVIiS* notwendig wären. Eine Bezugnahme bestünde dann nur auf das angesprochene Ausforschungspotential. Denn infolge der Beschlagnahme eines vom Schutzbereich des *GVIiS* grundsätzlich erfassten Systems kann zwar ebenfalls ein umfangreicher und vielfältiger Datenbestand erfasst werden. Dieser Datenbestand ist aber auf den Zeitpunkt der Beschlagnahme begrenzt, so dass sich den Ermittlungsbehörden keine dauerhafte Informationsquelle im oben beschriebenen Sinn öffnet. Die Zugänglichkeit des Datenbestands wird nicht durch eine „technische Infiltration" des informationstechnischen Systems erreicht. Es fehlt an der Möglichkeit, die Persönlichkeitsentfaltung des Betroffenen innerhalb der geschützten technischen Sphäre fortlaufend zu überwachen. Datenverarbeitungsvorgänge werden nicht mit zusätzlichen technischen Mitteln auf einem technisch nicht vorgesehenen Weg wahrnehmbar gemacht. Die konkreten Nutzungsgewohnheiten des Betroffenen können nicht mehr zum Überwachungsgegenstand gemacht werden. Der Informationsgewinn beschränkt sich auf dauerhaft gespeicherte Daten. Flüchtige Daten einer gegenwärtigen Nutzung können technisch bedingt regelmäßig nicht mehr erhoben werden. Daher schützt gegen die sich an die körperliche Beschlagnahme eines informationstechnischen Systems anschließende Erhebung und Verwendung der gespeicherten personenbezogenen Daten das *RiS* und nicht das *GVIiS*.[537]

(3) Neuartige Gefährdungen

Neben der Schaffung einer solchen dauerhaften und gegenüber der einmaligen Datenerhebung umfangreicheren Informationsquelle, begründet der Zugriff auf ein informationstechnisches System weitere Gefahrenquellen für die Persönlichkeit des Betroffenen, denen jedenfalls mit der bisherigen Ausprägung des *RiS* als Schutz vor „Erhebung, Speicherung, Verwendung und Weitergabe" personenbezogener Daten nicht begegnet werden kann. Die gestiegene Bedeutung informationstechnischer Systeme für die grundrechtlich geschützte Persönlichkeitsentfaltung setzt voraus, dass gleichzeitig auch die Bedingungen gesichert sind, dass der Einzelne seine Persönlichkeit mittels der Nutzung dieser Systeme entfalten kann. Grundlegende Bedingung für die ungehinderte Persönlichkeitsentfaltung ist, dass der Einzelne nicht an der Ausübung seiner grundrechtlich geschützten Freiheiten dadurch gehindert wird, dass er sich nicht sicher sein kann, inwieweit seine Grundrechtsausübung staatlicher Kontrolle unterliegt und aus Furcht vor möglichen Nachteilen von vornherein auf die Grundrechtsausübung verzichtet.[538]

---

[536] *BVerfGE* 120, 274 (322).
[537] A.A. *Herrmann*, IT-Grundrecht, S. 137f.; *Kutscha*, DuD 2012, 461 (463).
[538] Vgl. etwa *BVerfGE* 65, 1 (43).

Demnach setzt das mit der Nutzung informationstechnischer Systeme verbundene grundrechtliche Schutzbedürfnis voraus, dass der Staat die berechtigte Erwartung des Einzelnen an die Vertraulichkeit und Integrität seines informationstechnischen Systems achtet.[539] Das allgemeine Persönlichkeitsrecht beinhaltet auch die Erhaltung der Grundbedingungen der engeren persönlichen Lebenssphäre des Menschen.[540] Dieses Schutzbedürfnis geht aber über den Schutz vor der Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten hinaus.[541] Denn die selbstbestimmte Nutzung aller Funktionen des Systems zur Persönlichkeitsentfaltung erfasst nicht nur die Speicherung personenbezogener Daten. Überdies fehlt es an einer Selbstbestimmung schon dann, wenn nur die technische Infiltration des informationstechnischen Systems erfolgt ist, nicht aber auch schon eine darüberhinausgehende Datenerhebung. Voraussetzung dieser Selbstbestimmung ist, dass die eingesetzte Hard- und Software und insgesamt die eigengenutzten informationstechnischen Kommunikationsinfrastrukturen so funktionieren, wie der Nutzer dies erwarten darf.[542] Eine solche notwendige Vorverlagerung des Schutzes kann aber dann nicht erreicht werden, wenn die Gewährleistung der Integrität mit dem Schutz vor einer Datenerhebung, die sich an die Infiltration eines informationstechnischen Systems anschließt, gleichgesetzt wird.[543] Denn es soll das informationstechnische System als Grundbedingung einer freien und ungehinderten Persönlichkeitsentfaltung geschützt werden.[544]

Dagegen ist der Zugriff auf ein informationstechnisches System zunächst auch darauf angelegt und dazu geeignet, eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff zu unterlaufen.[545] Die mit der technischen Infiltration des informationstechnischen Systems verbundene Integritätsverletzung nur den Rechtfertigungsanforderungen einer Datenerhebung zu unterwerfen,[546] würde voraussetzen, dass sich die persönlichkeitsbezogenen Gefahren in der Datenerhebung erschöpfen. Jedoch verletzt die Infiltration nicht nur die Befugnis des Betroffenen, grds. selbst über Preisgabe und Verwendung der erhobenen personenbezogenen Daten zu entscheiden. Die Überwindung der technischen Hürde, die einem Zugriff durch Dritte entgegensteht, beseitigt die Möglichkeit vollständig, von dieser Befugnis überhaupt Gebrauch machen zu können. Denn der Eingriff beschränkt sich nicht nur auf die auch durch das *RiS* erfassbare Heimlichkeit der Maßnahme. Es werden dem Betroffenen die Bedingungen seiner informationellen Selbstbestimmung genommen, nämlich die tatsächliche Möglichkeit, der einzige zu sein, der über Preisgabe und Verwendung

539 *BVerfGE* 120, 274 (306).
540 *BVerfGE* 54, 143 (153); 72, 155 (170); 79, 256 (268).
541 So auch *Hoffmann-Riem*, JZ 2008, 1009 (1016).
542 *Hoffmann-Riem*, JZ 2008, 1009 (1012).
543 So aber *Eifert*, NVwZ 2008, 521 (522).
544 *Jäger*, jurisPR-ITR 12/2008 Anm. 2, S. 4.
545 *BVerfGE* 120, 274 (324).
546 Dafür *Eifert*, NVwZ 2008, 521 (522).

der personenbezogenen Daten entscheidet. Der Betroffene hat mit der alleinigen Verwendung des Systems und der lokalen (und gerade nicht öffentlichen) Speicherung seiner Daten von der Befugnis, über die Preisgabe seiner Daten zu entscheiden, Gebrauch gemacht. Diese bewusste Entscheidungsmöglichkeit wird ihm jedoch genommen, wenn die hierfür notwendige Grundbedingung seiner Persönlichkeitsentfaltung[547] – seine informationstechnische Infrastruktur – manipulationsbedingt nicht mehr so funktioniert, wie der Betroffene dies berechtigterweise erwarten durfte. Hierin lässt sich durchaus ein „realistisches, persönlichkeitsrelevantes, eigenständiges Gefahrenpotenzial"[548] sehen. Elektronische Kommunikationsmedien müssen so beschaffen sein, dass sie dem Betroffenen eine freiheitliche Informations- und Kommunikationsteilhabe ermöglichen.[549] Die Integrität informationstechnischer Systeme ist demnach nicht ausschließlich deshalb beeinträchtigt, weil sie zur Ermöglichung der Erhebung personenbezogener Daten zwangsläufig aufgehoben wird.

Die gleiche berechtigte Erwartung darf der Betroffene an die grds. fehlerfreie Verarbeitung und Speicherung seiner personenbezogenen Daten richten. Die Fernwirkungen der Infiltration, welche von den im Rahmen der gegenständlichen Verfassungsbeschwerdeverfahren angehörten sachkundigen Auskunftspersonen festgestellt wurden, blieben unberücksichtigt, wenn die Erhebung des personenbezogenen Datums isoliert als Rechtfertigungsanforderungen setzende staatliche Maßnahme angesehen würde.[550] So könnten Wechselwirkungen zwischen dem Vorgang technischer Infiltration und dem Betriebssystem des Systems zu Datenverlusten führen.[551] Eine fehlerfreie Interaktion könne schon angesichts der unvollständigen Informationen über die Spezifikationen des Zielsystems und angesichts seiner Komplexität nicht erwartet werden.[552] Ferner könnten bereits die eingebrachten Softwarekomponenten eigene Sicherheitsprobleme enthalten. Auch

---

[547] *Gusy*, DuD 2009, 31 (34f.), spricht insofern von der Notwendigkeit nicht nur informationeller Selbstbestimmung über die Kommunikationsteilhabe, sondern der Garantie informationeller Selbstbestimmung bei der Kommunikationsteilhabe.

[548] Vgl. *Eifert*, NVwZ 2008, 521 (522).

[549] *Gusy*, DuD 2009, 33 (35); insofern greift der Ansatz von *Herrmann*, IT-Grundrecht, S. 61 zu kurz, wenn dort zur Begründung eines der konkreten Datenerhebung vorgelagerten Systemschutzes pauschal auf die Folgen von Hackerangriffen verwiesen wird. Ein solcher Ansatz berücksichtigt nicht, dass das System nicht um seiner selbst willen, sondern als Mittel zum Ausdruck der Persönlichkeitsentfaltung des Einzelnen geschützt wird.

[550] Damit die Datenerhebung von einem informationstechnischen System allein den Rechtfertigungsanforderungen einer Datenerhebung unterworfen werden kann, dürfte der grundrechtliche Schutzbedarf nur an der Qualität der Daten, mithin an der Persönlichkeitsrelevanz ihres Inhalts, auszurichten sein. Diese müsste die einzige Bemessungsgröße des Schutzbedarfs sein, vgl. hierzu *Hoffmann-Riem*, JZ 2008, 1009 (1016 Fn. 73). Die Verletzung der Integrität eines informationstechnischen Systems ist nicht deswegen gerechtfertigt, weil die Datenerhebung von einem solchen System entsprechend hohe Rechtfertigungsanforderungen aufstellt, sondern umgekehrt haben diese hohen Anforderungen ihren Ursprung in den Wirkungen der Integritätsverletzung.

[551] Vgl. *BVerfGE* 120, 274 (325).

[552] Vgl. *Bogk*, Antworten Fragenkatalog (Fn. 161), S. 16.

bestünde die Möglichkeit, dass eine eingebrachte Software nicht wieder vollständig entfernt werden kann, sondern eine Neuinstallation des Betriebssystems inklusive der Anwendungssoftware erforderlich wird.[553] Die Integrität des Systems sei weiter dadurch gefährdet, dass die zugreifende Ermittlungsbehörde Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen könnte.[554] Die gleiche Gefahr drohe durch Dritte, welche den durch die Infiltration geschaffenen Zugang ausnutzen. Denn sowohl der Missbrauch einer von der Ermittlungsbehörde eingebrachten Software,[555] als auch die Ausnutzung derselben Sicherheitslücke[556] durch private Dritte ließen sich nicht ausschließen.

Jedenfalls diese zusätzlichen Gefährdungen, welche die Infiltration eines informationstechnischen Systems mit sich bringt, sprechen dafür, auch die sich an diesen Zugriff anschließende Datenerhebung von einem informationstechnischen System ausschließlich dem *GVIiS* und nicht dem *RiS* zu unterstellen. Denn eine isolierte Betrachtung allein der Datenerhebung berücksichtigt nicht die zusätzlichen oder Folgegefährdungen, die mit der Infiltration des Systems zur Ermöglichung der Datenerhebung verbunden sind. Sofern dafür argumentiert wird, dass der Schutzbereich des *GVIiS* auch durch eine besondere Verhältnismäßigkeitsprüfung i.R.d. *RiS* hätte aufgefangen werden können,[557] bleibt unberücksichtigt, dass die gegenüber dem *RiS* neuartigen Gefährdungen nicht aus der Datenerhebung folgen, sondern aus der dieser Erhebung vorangehenden technischen Infiltration des informationstechnischen Systems. Die besondere Schwere des Eingriffs resultiert daher nicht allein aus der Erhebung eines umfangreicheren und vielfältigeren Datenbestandes. Unabhängig von dem letztlich im Anschluss an die Infiltration

---

553 *Freiling*, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, S. 7.

554 *BVerfGE* 120, 274 (325).

555 *Fox*, Stellungnahme zur „Online-Durchsuchung" – Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, S. 15; *Sieber*, Stellungnahme (Fn. 287), S. 18.

556 *Freiling*, Stellungnahme (Fn. 553), S. 7.

557 Dafür *Britz*, DÖV 2008, 411 (412); *Sachs/Krings*, JuS 2008, 481 (484); für die Gewährleistung der Vertraulichkeit ebenso *Eifert*, NVwZ 2008, 521 (522); differenzierend dagegen *Hornung*, CR 2008, 299 (301), der die Abhängigkeit des Einzelnen von der Nutzung informationstechnischer Systeme als dem *RiS* fremden Gedanken hervorhebt; dagegen *T. Böckenförde*, JZ 2008, 925 (928), nach dem sich die Eingriffsvoraussetzungen des Zugriffs auf informationstechnische Systeme von denen in das *RiS* so sehr unterschieden, dass eine einheitliche Prüfung nicht möglich wäre und es zu einer unübersichtlichen Zersplitterung innerhalb des Verhältnismäßigkeitsgrundsatzes kommen würde; dem folgend *Herrmann*, IT-Grundrecht, S. 60; hiergegen wiederum *Gudermann*, Online-Durchsuchung, S. 169, wonach gerade durch die Flexibilität des Verhältnismäßigkeitsgrundsatzes der jeweils besonderen Gewichtung der Beeinträchtigung Rechnung getragen werden könne; unklar *Heise*, RuP 2009, 94 (98), der zwar die vom *BVerfG* festgestellte Schutzlücke anzweifelt, aber eine unübersichtliche Verhältnismäßigkeitsprüfung gerade als Folge der Formulierung des *GVIiS* ansieht; *Wegener/Muth*, JURA 2010, 847 (848), nennen als Alternative zur Anerkennung des *GVIiS* wegen der Schwächen des *RiS* mit seinem Bezug auf personenbezogene Daten die Rückführung allein auf das allgemeine Persönlichkeitsrecht.

erhobenen Datenbestand bestehen diese zusätzlichen Gefahren in gleichem Maße bei jeder technischen Infiltration eines informationstechnischen Systems. Ihre Berücksichtigung würde keine Einzelfallprüfung darstellen, sondern generell bei jeder Verhältnismäßigkeitsprüfung anfallen und bei jedem Eingriff identische hohe Anforderungen an die verfassungsmäßige Rechtfertigung stellen. Dies würde zu einer Verlagerung der Voraussetzungen, die generell an eine Eingriffsnorm zu stellen wären, hin zur einzelfallbezogenen Schranken-Schranke der Verhältnismäßigkeit i.w.S. führen. Wird den über den Schutz der bisherigen Ausprägung des *RiS* hinausgehenden Gefährdungen dagegen mittels einer weiteren Ausprägung des allgemeinen Persönlichkeitsrechts begegnet, so wird das neuartige Gefährdungspotential mit einem typisierend ausgestalteten Schutz erfasst.[558]

In seiner bisherigen Ausprägung würde das *RiS* die neuartigen Persönlichkeitsgefährdungen, die sich in Folge der Nutzung informationstechnischer Systeme schon durch den bloßen Zugriff auf ein solches System ergeben, nicht erfassen.[559] Weitergehende Maßnahmen im Anschluss an die technische Infiltration wären nur dann vom *RiS* erfasst, wenn diese die „*Er*hebung, Speicherung, Verwendung und Weitergabe" personenbezogener Daten zum Gegenstand hätten. Da sich hierin aber die mit der Nutzung informationstechnischer Systems verbundenen Gefährdungen der Persönlichkeitsentfaltung nicht erschöpfen, hätte der Schutzbereich des *RiS* dahingehend angepasst und erweitert werden müssen.[560] Der Schutzbereich des allgemeinen Persönlichkeitsrechtes hätte somit auch auf diesem Weg weiterer Konkretisierung bedurft. Da aber Schutzziel und Schutzniveau des *RiS* unverändert bleiben und nur die Erweiterung auf zusätzliche Dimensionen des Persönlichkeitsschutzes unterbleibt, bedeutet die Ausbildung einer weiteren Konkretisierung keine Minimalisierung dieses Rechts.[561] Die weitere Konkretisierung des allgemeinen Persönlichkeitsrechts durch die Ausprägung des *GVIiS* hat demgegenüber den Vorteil, dass sie einen Anknüpfungspunkt für den grundrechtlichen Schutz setzt, der auf sämtliche der ausgemachten neuartigen Persönlichkeitsgefährdungen zugeschnitten ist.[562] Sie erleichtert es, neue Qualitäten der Gefährdung und den entsprechenden Schutzbedarf schon auf Schutzbereichsebene zu berücksichtigen, die damit verbundene Notwendigkeit besonderer Anforderungen

[558] *Hoffmann-Riem*, JZ 2008, 1009 (1019).

[559] So auch schon *Germann*, Gefahrenabwehr und Strafverfolgung, S. 542; i.E. auch *Herrmann*, IT-Grundrecht, S. 62.

[560] Anders *Gudermann*, Online-Durchsuchung, S. 171f., wonach bereits die bisherige Ausgestaltung des *RiS* den Schutzbereich des *GVIiS* umfasse.

[561] Ebenso *Hoffmann-Riem*, JZ 2008, 1009 (1015); *Hörnig*, JURA 2007, 207 (208); *Herrmann*, IT-Grundrecht, S. 130; a.A. *Eifert*, NVwZ 2008, 521 (523); *Volkmann*, DVBl. 2008, 590 (591); *Lepsius*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 21 (31).

[562] Ebenso *Hörnig*, JURA 2007, 207 (209).

an Schranken zu erkennen sowie auf die Gefährdung ausgerichtete Schutzvorkehrungen zu entwickeln.[563] Die Herausbildung des *GVIiS* legitimiert sich insofern daraus, dass das *GVIiS* erstmalige oder spezifisch andere Anforderungen an die Eingriffsvoraussetzungen stellt.[564]

iii. Subsidiarität des GVIiS gegenüber bestehenden Ausprägungen des allgemeinen Persönlichkeitsrechts insb. dem Recht auf informationelle Selbstbestimmung

Grundrechtskonkurrenzen setzen voraus, dass mehrere Grundrechte auf ein Verhalten des Grundrechtsträgers anwendbar sind. Sofern aber der Schutzbereich eines Grundrechts nicht eröffnet ist, besteht auch keine Konkurrenzsituation. Der Vorrang der Grundrechte der Art. 10 Abs. 1 und Art. 13 Abs. 1 GG gegenüber dem *GVIiS* ergibt sich schon aus ihrer Spezialität gegenüber dem allgemeinen Persönlichkeitsrecht. Sofern der staatliche Zugriff auf ein informationstechnisches System bereits in den Schutzbereich des Telekommunikationsgeheimnisses oder der Unverletzlichkeit der Wohnung fällt, gehen diese dem *GVIiS* vor. Die Konkurrenzfrage hinsichtlich weiterer benannter Freiheitsrechte richtet sich danach, ob der spezifische Persönlichkeitsschutz bereits von dem speziellen Grundrecht erfasst wird.

Fraglich ist dagegen das Verhältnis des *GVIiS* zu den anderen Konkretisierungen des allgemeinen Persönlichkeitsrechts. Das *GVIiS* tritt als weitere Ausprägung des allgemeinen Persönlichkeitsrechts zu den anderen Konkretisierungen dieses Grundrechts sowie zu den Grundrechten der Art. 10 Abs. 1 und Art. 13 Abs. GG hinzu, „soweit diese keinen oder keinen hinreichenden Schutz bieten".[565] Aufgrund dieser Formulierung wird teilweise vertreten, das *GVIiS* sei gegenüber den bisherigen Ausprägungen des allgemeinen Persönlichkeitsrechts, insb. dem *RiS*, subsidiär.[566] Gegen ein solches Verständnis spricht jedoch, dass das *BVerfG* im Folgenden die *lückenschließende* Gewährleistung des allgemeinen Persönlichkeitsrechts betont, neuartige Gefährdungen infolge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse zu erfassen.[567] Das allgemeine Persönlichkeitsrecht trage dem Schutzbedarf gegenüber der Nutzung informationstechnischer Systeme in seiner *lückenfüllenden* Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet.[568] Ausdrücklich wird

[563] *Hoffmann-Riem*, JZ 2008, 1009 (1018).
[564] *T. Böckenförde*, JZ 2008, 925 (928).
[565] *BVerfGE* 120, 274 (303).
[566] *Jäger*, jurisPR-ITR 12/2008 Anm. 2, S. 3 und 4; *Petri*, DuD 2008, 443 (444); *Volkmann*, DVBl. 2008, 590 (591); *Wedde*, AuR 2009, 373; *Hoffmann*, CR 2010, 515 (516); *Herrmann*, IT-Grundrecht, S. 112; ausdrücklich nur hinsichtlich des *RiS Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 138; *Britz*, DÖV 2008, 411 (414); *Eifert*, NVwZ 2008, 521 (522).
[567] *BVerfGE* 120, 274 (303).
[568] *BVerfGE* 120, 274 (313).

hinsichtlich der Schutzbereiche des Art. 10 Abs. 1 GG („bleibt eine Schutzlücke“[569]) und des Art. 13 Abs. 1 GG („belässt aber Schutzlücken“[570]) ausgeführt, dass die neuartigen Gefahren, die sich aus der Nutzung informationstechnischer Systeme für die Persönlichkeit des Einzelnen ergeben, nicht vollständig erfasst werden. Die Ausführungen beziehen sich daher auf die Begründung einer Schutzlücke, nicht dagegen unmittelbar auf das Konkurrenzenzverhältnis des *GVIiS* zu den bestehenden Ausprägungen des allgemeinen Persönlichkeitsrechts.[571]

Gerade auch die Feststellung dieser Schutzlücke lässt sich als Argument gegen die Annahme eines Konkurrenzverhältnisses zwischen dem *GVIiS* und den angeführten Ausprägungen des allgemeinen Persönlichkeitsrechts heranziehen. Danach *genüge* die Gewährleistung des Schutzes der Privatsphäre dem Schutzbedürfnis des Nutzers eines informationstechnischen Systems nicht, da dieses Bedürfnis *weiterreiche* als der Schutz privater Daten[572]. Auch das *RiS* trage den Persönlichkeitsgefährdungen der Nutzung informationstechnischer Systeme nicht *vollständig* Rechnung, da der Zugriff auf ein solches System in seinem Gewicht für die Persönlichkeit über einzelne Datenerhebungen, vor denen das *RiS* schützt, *weit hinausgeht*.[573] Die Begründung einer Schutzlücke gegenüber diesen Ausprägungen des allgemeinen Persönlichkeitsrechts beschreibt zugleich die fehlende Konkurrenzsituation. Denn weder der Schutz der Privatsphäre noch das *RiS* erfassen *sämtliche* Gefahren der Persönlichkeit nur einer Zugriffsmodalität vollständig. Wegen der Spezialität des Art. 13 Abs.1 GG gegenüber dem allgemeinen Persönlichkeitsrecht wären diese Ausprägungen überhaupt nur auf die unkörperliche technische Infiltration eines informationstechnischen Systems anwendbar. Jene Ausprägungen würden jedoch nicht sämtliche Gefährdungen der Persönlichkeit begegnen, die mit einem solchen Zugriff verbunden wären. Der Schutz der Privatsphäre würde nur den thematischen Privatheitsanspruch bestimmter Daten erfassen, das *RiS* ausschließlich die „Erhebung, Speicherung, Verwendung und Weitergabe“ personenbezogener Daten. Die Subsidiarität eines Grundrechts setzt jedoch voraus, dass der Grundrechtsschutz in vollem Umfang mindestens auch durch das verdrängende Grundrecht gewährleistet wird.[574] Die Begründung einer Schutzlücke gegenüber bestehenden Konkretisierungen des allgemeinen Persönlichkeitsrechts beruht aber gerade darauf, dass diese Konkretisierungen den Zugriff auf ein informationstechnisches System selbst nur hinsichtlich bestimmter einzelner Modalitäten gewährleisten können.

---

569 *BVerfGE* 120, 274 (308).
570 *BVerfGE* 120, 274 (309).
571 So auch *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (132); *Hoffmann-Riem*, JZ 2009, 1009 (1019 Fn. 91).
572 *BVerfGE* 120, 274 (311) (Hervorhebung nur hier).
573 *BVerfGE* 120, 274 (313) (Hervorhebung nur hier).
574 *Berg*, in: HGR III, § 71 Rn. 26.

Es besteht daher kein für die Annahme von Subsidiarität notwendiger vollumfänglicher Grundrechtsschutz. Da es somit an der Anwendbarkeit zweier Grundrechte auf denselben Sachverhalt fehlt, ist das *GVIiS* auch nicht subsidiär gegenüber bestehenden Ausprägungen des allgemeinen Persönlichkeitsrechts.[575]

iv. Ergebnis

Die Begründung einer Schutzlücke des aktuellen grundrechtlichen Persönlichkeitsschutzes hinsichtlich bestehender Ausprägungen des allgemeinen Persönlichkeitsrechts beruht darauf, dass nicht nur bestimmte Modalitäten des technischen Zugriffs auf ein informationstechnisches System nicht erfasst wären, sondern diese Ausprägungen zu keinem Zeitpunkt in der Lage sind, sämtliche Gefährdungen, die mit einem solchen Zugriff verbunden sind, zu erfassen. Ihr Schutz kann lediglich einen begrenzten Ausschnitt dieser Gefährdungen erfassen. Da sich die Schutzbereiche somit nicht überschneiden, besteht keine Konkurrenzsituation. Ein Spezialitätsverhältnis des *RiS* zum *GVIiS* kann damit zwangsläufig nicht vorliegen.

e. Zusammenfassung

Der Schutzbereich des *GVIiS* überschneidet sich teilweise mit denen der Art. 10 Abs. 1 und Art. 13 Abs. 1 GG. Sofern die mit dem technischen Zugriff auf das informationstechnische System verbundenen Gefährdungen für die Persönlichkeit des Betroffenen abschließend erfasst werden, greift das Spezialitätsverhältnis des Telekommunikationsgeheimnisses und der Unverletzlichkeit der Wohnung gegenüber dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Hinsichtlich der bisherigen Ausprägungen des allgemeinen Persönlichkeitsrechts ergibt sich jedoch kein Konkurrenzverhältnis. Die Anwendung des *GVIiS* steht nicht unter einem Subsidiaritätsvorbehalt hinsichtlich des *RiS*.

*4. Exkurs: Entwurf einer Datenschutz-Grundverordnung*

Nach der Vorstellung des Entwurfs einer Datenschutz-Grundverordnung[576] (DS-GVO-E) durch die *Europäische Kommission* am 25. Januar 2012 könnten für den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme künftig allein europarechtliche Regelungen maßgeblich sein. Es bliebe dann nicht allein bei der Frage nach der Spezialität der Grundrechte des Grundgesetzes zueinander, sondern zusätzlich wäre der Vorrang von europäischem Recht gegenüber den grundgesetzlichen Maßstäben des allgemeinen Persönlichkeitsrechts zu prüfen. Im Folgenden wird dargelegt, dass der geplanten Verordnung in ihrer gegenwärtigen Gestaltung nach Wortlaut, Systematik und Konzeption die Gewährleistung der

[575] I.E. ebenso *Luch*, MMR 2011, 75 (76f.).

[576] Vorschlag für eine Verordnung des *Europäischen Parlaments* und des *Rates* zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (*Datenschutz-Grundverordnung*) vom 25.1.2012, KOM (2012) 11 endgültig.

Vertraulichkeit und Integrität informationstechnischer Systeme nach Maßgabe des gegenständlichen Urteils des *BVerfG* nicht entnommen werden kann. Der Verordnung käme demnach kein Vorrang vor den Art. 2 Abs. 1, Art. 1 Abs.1 GG zu. Die folgende Untersuchung des Verordnungsentwurfs beschränkt sich daher auch nur auf den Schutz der selbstbestimmten Verfügung über das eigene informationstechnische System.

a. Vorbemerkungen

Die geplante Verordnung soll die EG-Datenschutzrichtlinie von 1995[577] ersetzen, vgl. Art. 88 Nr. 1 DS-GVO-E. Anlass für eine Neuregelung sind nach Erwägungsgrund (ErwG) 5 der rasche technologische Fortschritt und die Globalisierung. Zwar würden die Ziele und Grundsätze der Richtlinie weiterhin fortgelten, letztere habe jedoch eine unterschiedliche Handhabung des Datenschutzes in der Union, Rechtsunsicherheit sowie die weit verbreitete öffentliche Meinung, dass speziell im Internet der Datenschutz nicht immer gewährleistet sei, nicht verhindern können (ErwG 7). Nach Ansicht des *Europäischen Gerichtshofs* (*EuGH*) war hingegen schon die EG-Datenschutzrichtlinie nicht auf eine Mindestharmonisierung beschränkt, sondern führte zu einer „grundsätzlich umfassenden Harmonisierung".[578] Die Gewährleistung eines hohen Maßes an Datenschutz für den Einzelnen und die Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten setze die Gleichwertigkeit des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten voraus (ErwG 8). Der Entwurf betont den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten als (europäisches) Grundrecht und verweist dabei auf das in Art. 8 Abs. 1 GR-Charta[579] sowie Art. 16 Abs. 1 AEUV[580] festgeschriebene Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten (ErwG 1). Die Kommission beruft sich für ihr Vorhaben auf Art. 16 Abs. 2 AEUV. Letzterer ermächtigt das Europäische Parlament und den Rat zum Erlass von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, sowie über den freien Datenverkehr. Das Rechtsinstrument der Verordnung sei für das Vorhaben am besten geeignet, da sie aufgrund ihrer unmittelbaren Anwendbarkeit

---

[577] Richtlinie 95/46/EG des *Europäischen Parlaments* und des *Rates* vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23.11.1995, S. 0031 - 0050.

[578] *EuGH*, Urt. v. 6.11.2003 – Rs. C-101/01, Slg. 2003, I-12971 - *Lindqvist*, Rn. 96; Urt. v. 16.12.2008 - C-524/06, Slg. 2008, I-09705 – *Huber*, Rn. 51; Urt. v. 24.11.2011 – C-469/10 - *ASNEF*, *FECEMD*, Rn. 29.

[579] *Charta der Grundrechte der Europäischen Union*, Amtsblatt Nr. C 83 vom 30.3.2010, S. 389-403.

[580] *Vertrag über die Arbeitsweise der Europäischen Union*, Amtsblatt Nr. C 326 vom 26.10.2012, S. 47-390 (konsolidierte Fassung 2012).

nach Art. 288 AEUV zur Rechtsvereinheitlichung beitrage und die Rechtssicherheit durch die Einführung harmonisierter Kernbestimmungen und durch einen besseren Grundrechtsschutz erhöhe.[581] Damit werde zugleich für einen besser funktionierenden Binnenmarkt gesorgt. Die Regelung in einer Verordnung soll zudem Unternehmen an der Verschaffung von Wettbewerbsvorteilen durch bloße Sitzverlagerungen innerhalb Europas hindern.[582]

b. Der Anwendungsvorrang des Unionsrechts

Gerade die Wahl des Regelungsinstruments aber ist mit weitreichenden Folgen verbunden. Einer Verordnung kommt gem. Art. 288 Abs. 2 S. 2 AEUV in allen Mitgliedsstaaten unmittelbare Wirkung zu. Während eine Richtlinie lediglich hinsichtlich ihres Ziels verbindlich ist (Art. 288 Abs. 3 AEUV), verbleiben den Mitgliedsstaaten bei einer Verordnung keinerlei Umsetzungsspielräume. Für die Auslegung der Verordnung ist allein der *EuGH* im Vorabentscheidungsverfahren gem. Art. 267 Abs. 1 lit. b AEUV zuständig.[583] Nationale Gerichte und Behörden wenden daher unmittelbar die Regelungen der Verordnung an. Insoweit treten nationale Regelungen zurück. Nach Ansicht des *EuGH* genießt das Unionsrecht uneingeschränkten Vorrang gegenüber dem nationalen Recht der Mitgliedsstaaten.[584] Dieser Vorrang erstrecke sich auch auf das nationale Verfassungsrecht der Mitgliedsstaaten.[585] Eine ausdrückliche Kollisionsregel enthält das Unionsrecht nicht. In der Erklärung Nr. 17 der Schlussakte zum Vertrag von Lissabon[586] wird hingegen ausdrücklich auf die Rechtsprechung des *EuGH* zum Vorrang des Unionsrechts verwiesen. Der Anwendungsvorrang bedeutet mithin eine Kollisionsregel zugunsten des Unionsrechts, ohne die Wirksamkeit des innerstaatlichen Rechts zu berühren.[587] Auch der *EuGH* konkretisierte den von ihm festgestellten Vorrang

[581] Ziff. 3.1 Abs. 2 der Begründung zur DS-GVO-E.

[582] *Reding*, ZD 2012, 195 (196).

[583] Die sich ergebende individuelle Rechtsschutzsituation wird überwiegend kritisch betrachtet: *Hornung*, ZD 2012, 99 (100), merkt an, dass der *EuGH* weit davon entfernt sei, eine dem *BVerfG* vergleichbare Grundrechtsdogmatik zu entwickeln; ihm folgend *Schwartmann*, RDV 2012, 55 (58); *ders.*, RDV 2012, 55 (59), hält unterschiedliche Auslegungsmaßstäbe der Gerichte - Sicherung individueller Freiheiten (*BVerfG*) und Wahrung der Gemeinschaftsziele (*EuGH*) - bei der Grundrechtsprüfung für problematisch; ihm folgend spricht *v. Lewinski*, DuD 2012, 564 (569), dem *EuGH* die „hervorragende Rolle des *BVerfG* für den Individualrechtsschutz" ab; ebenso vermisst *Hornung*, ZD 2012, 99 (100), im Unionsrecht einen der Verfassungsbeschwerde vergleichbaren Individualrechtsbehelf; auch *Masing*, Der Abschied von den Grundrechten, SZ v. 9.1.2012, S. 10, gibt daher zu bedenken, dass der einzelne Bürger in der Regel keinen Zugang zu dem *EuGH* hat; dieser sei insofern kein Bürgergericht und verstehe sich zu Recht nicht als Grundrechtegericht; dementsprechend kritisch zu den hohen Voraussetzungen einer individuellen Nichtigkeitsklage gem. Art. 263 Abs. 4 AEUV *Schwartmann*, RDV 2012, 55 (58f.).

[584] Grundlegend *EuGH*, Urt. v. 15.7.1964 - Rs. 6/64, Slg. 1964, 1259 (1269ff.) - *Costa ./. E.N.E.L.*; st. Rspr. zum *Gemeinschaftsrecht*.

[585] Vgl. *EuGH*, Urt. v. 9.3.1977 - Rs. 106/77, Slg. 1978, 629 - *Simmenthal II*, Rn. 17/18.

[586] Amtsblatt Nr. C 306 vom 17.12.2007, S. 256; Nr. C 83 vom 30.3.2010, S. 344.

[587] *Herdegen*, Europarecht, § 10 Rn. 3; *Streinz*, Europarecht, Rn. 220.

des Unionsrechts in der Entscheidung *IN.CO.GE* im Sinne eines Anwendungsvorrangs.[588]

Ein solcher Vorrang könne dem Unionsrecht nach Ansicht des *BVerfG* aber nur dann zukommen, wenn das Unionsrecht einen allgemein verbindlichen Grundrechtsstandard enthält, der auf Dauer demjenigen des Grundgesetzes genügt.[589] Einen solchen Standard sah das *BVerfG* in der *Solange-II*-Entscheidung erreicht. Im Hoheitsbereich der Europäischen Gemeinschaften sei danach „ein Maß an Grundrechtsschutz erwachsen, das nach Konzeption, Inhalt und Wirkungsweise dem Grundrechtsstandard des Grundgesetzes im Wesentlichen gleichzuachten sei".[590] Solange ein derartiger Schutz generell gewährleistet sei, werde das *BVerfG* seine Gerichtsbarkeit über die Anwendbarkeit von sekundärem Unionsrecht als Rechtsgrundlage hoheitlichen Handelns deutscher Gerichte und Behörden nicht mehr ausüben und somit keine Überprüfung am Maßstab der Grundrechte des Grundgesetzes vornehmen.[591] Entsprechende Verfassungsbeschwerden und Vorlagen im Wege der konkreten Normenkontrolle, die eine Verletzung von Grundrechten durch sekundäres Gemeinschaftsrecht geltend machen, sind von vornherein unzulässig, sofern nicht dargelegt wird, dass ein Absinken des europäischen Grundrechtsstandards nach Maßgabe der *Solange-II*-Entscheidung vorliegt.[592] Das *BVerfG* hat sich dabei zuletzt ausdrücklich auf einen Anwendungsvorrang des Unionsrechts festgelegt.[593]

Als Folge hieraus würden nicht nur einschlägige Normen der deutschen Bundes- und Landesdatenschutzgesetze verdrängt. Auch würde der Inhalt einfachgesetzlicher Regelungen nicht mehr durch die Grundrechte des Grundgesetzes vorgegeben.[594] Dies würde insbesondere auch das *RiS* und das *GVIiS* als Ausprägungen des allgemeinen Persönlichkeitsrechts der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1

---

[588] *EuGH*, Urt. v. 22.10.1998 - verb. Rs. C-10/97 - C-22/97, IN.CO.GE. '90 u.a., Slg. 1998, I-6307, Rn. 21.

[589] *BVerfGE* 37, 271 (280); 73, 339 (376); 89, 155 (174f.).

[590] *BVerfGE* 73, 339 (378).

[591] *BVerfGE* 73, 339 (387); 102, 147 (162f.); 118, 79 (95).

[592] *BVerfGE* 102, 127 (147).

[593] *BVerfGE* 123, 267 (398, 400); 126, 286 (302).

[594] Sehr kritisch *Masing* (Fn. 583), S. 10: Die Nichtanwendbarkeit der deutschen Grundrechte wäre „grundstürzend". Die Regulierungsvorschläge der Kommission hätten ihrer Wirkung nach das Potential einer tiefgreifenden Verfassungsänderung.

GG betreffen.[595] Der Anwendungsvorrang der DS-GVO-E hängt mithin von ihrer Reichweite ab. Nur insoweit der sachliche Anwendungsbereich der Verordnung nicht eröffnet ist, können die Grundrechte des Grundgesetzes den Maßstab des notwendigen Rechtsrahmens vorgeben.

c. Sachlicher Anwendungsbereich der DS-GVO-E

Die DS-GVO-E findet gem. Art. 2 Nr. 1 DS-GVO-E Anwendung auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Die Begriffe der Vertraulichkeit und Integrität werden dabei an keiner Stelle des Entwurfs als Schutzziele der selbstbestimmten Verfügung über das eigene informationstechnische System verwendet. Der sachliche Anwendungsbereich der DS-GVO-E setzt allein am Begriff der personenbezogenen Daten an. Letztere sind in Art. 1 Nr. 1 DS-GVO-E als Regelungsgegenstand festgehalten. Danach enthält die Verordnung Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

i. Wortlaut

Im Verordnungstext schließlich tauchen jedoch an keiner Stelle die Begriffe der Vertraulichkeit und Integrität als Ausdruck der selbstbestimmten Verfügung über das eigene informationstechnische System auf. Das gegenständliche Urteil des *BVerfG* und seine Vorgaben an die Vertraulichkeit und Integrität informationstechnischer Systeme seien zwar bei dem Reformvorhaben der Kommission berücksichtigt worden.[596] Man habe sich sogar in vielen Punkten am BDSG orientiert, das hohe deutsche Datenschutzniveau sei Richtschnur und Messlatte für die

[595] Die *Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam* - „Ein hohes Datenschutzniveau für ganz Europa!“, S. 1f. (abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/83DSK_EU_Rechtsrahmen.pdf?__blob=publicationFile), fordert, dass eine kommende Verordnung den Mitgliedstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen müsse, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absicherten und Raum für eine innovative Rechtsfortbildung schaffen würden. Nur so könnten auch die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden; ebenso vermissen der *Ausschuss für Fragen der Europäischen Union*, der *Ausschuss für Innere Angelegenheiten* und der *Rechtsausschuss*, BR-Drucks. 52/1/12, S. 2, ausdrückliche Ermächtigungen zu Konkretisierungen durch den nationalen Gesetzgeber der Mitgliedstaaten; auch *Masing* (Fn. 583), S. 10, stellt die Frage, ob nicht die Gewährleistung eines Mindeststandards reiche, der es den Mitgliedstaaten ermöglicht, ihre eigenen Grundrechtstraditionen ergänzend zur Anwendung zu bringen.

[596] Mitteilung der *Kommission* an das *Europäische Parlament*, den *Rat*, den *Europäischen Wirtschafts- und Sozialausschuss* und den *Ausschuss der Regionen* - Gesamtkonzept für den Datenschutz in der Europäischen Union vom 4.11.2010, KOM (2010) 609 endgültig, S. 6 Ziff. 2.1.1.

Reformvorschläge gewesen.[597] Jedoch überschneiden sich lediglich die in Art. 30 DS-GVO-E an den für die Verarbeitung Verantwortlichen gestellten Verpflichtungen in Bezug auf die Sicherheit der Datenverarbeitung mit den informationstechnischen Schutzzielen der Vertraulichkeit und Integrität.[598] Auch die Definition des Begriffs der Verarbeitung führt nicht entscheidend weiter. Dieser erfasst nach Art. 4 Abs. 3 DS-GVO-E jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, den Abgleich oder die Verknüpfung sowie das Löschen oder Vernichten der Daten. Aufgrund dieser weiten Definition wäre vom Wortlaut auch die Erhebung personenbezogener Daten mittels des Zugriffs auf ein informationstechnisches System erfasst. Die Definition stimmt jedoch nahezu wörtlich mit derjenigen aus Art. 2 lit. b) der EG-Datenschutzrichtlinie überein, ohne dass demgegenüber eine Erweiterung des Begriffs in Bezug auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme erkennbar wird. Der Entwurf betont vielmehr, dass die Ziele und Grundsätze der EG-Datenschutzrichtlinie weiterhin gültig seien (ErwG 7) und die in Art. 5 DS-GVO-E bestimmten Grundsätze für die Verarbeitung personenbezogener Daten denen des Art. 6 der EG-Datenschutzrichtlinie entsprächen.[599] Der in der deutschen Fassung verwendete Begriff des Zusammenhangs ist insofern ungenau, als personenbezogene Daten gerade Objekt des Verarbeitungsvorgangs sein müssen.[600] Der Zugriff auf ein informationstechnisches System hat jedoch zunächst das System selbst zum Angriffsziel. Überdies dürfte sich die weite Begriffsdefinition auch mit dem von der Kommission beabsichtigten technologieneutralen Schutzansatz erklären lassen (vgl. ErwG 13).[601]

ii. Systematik

Auch der mit dem Entwurf eingeführte Begriff der Verletzung des Schutzes personenbezogener Daten (Art. 4 Abs. 3 DS-GVO-E) umfasst nicht auch die selbstbestimmte Verfügung über das eigene informationstechnische System. Die Verletzung des Schutzes personenbezogener Daten ist danach eine Verletzung der Si-

---

[597] *Reding*, ZD 2012, 195 (197).

[598] *Münch*, RDV 2012, 72 (73f.).

[599] Ziff. 3.4.2 Abs. 1 der Begründung zur DS-GVO-E.

[600] Vgl. hierzu die englische ([…] 'processing' means any operation or set of operations which **is performed upon** personal data or sets of personal data […]) und französische Fassung („traitement de données à caractère personnel": toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et **appliquée(s) à** des données à caractère personnel […]) der DS-GVO-E (Hervorhebungen nur hier).

[601] *Reding*, ZD 2012, 195 (198), nennt die Offenheit der EU-Datenschutzreform für künftige technologische und gesellschaftliche Entwicklungen einen von sieben wichtigen Grundbausteinen.

cherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Mit dem Zugriff auf das informationstechnische System verschafft sich der Dritte den unbefugten Zugang zu den auf dem System vorhandenen personenbezogene Daten. Insofern lässt sich zwar der unberechtigte Zugriff auf ein informationstechnisches System dem Begriff der Verletzung des Schutzes personenbezogener Daten unterordnen. Jedoch wird dieser ausschließlich in Verbindung mit der Pflicht des für die Datenverarbeitung Verantwortlichen zur Meldung eines Verstoßes an die Aufsichtsbehörden (Art. 31 DS-GVO-E) und die betroffene Person (Art. 32 DS-GVO-E) verwendet. Der Begriff wird hingegen an keiner Stelle der Verordnung i.S.e. individuellen Abwehranspruchs des Betroffenen gegen die Beeinträchtigung der Vertraulichkeit und Integrität des von ihm genutzten Systems gebraucht. Die Normen nehmen vielmehr den für die Datenverarbeitung Verantwortlichen in die Pflicht, nicht aber den unbefugt Zugreifenden. Die Meldepflicht soll wirtschaftliche Schäden und soziale Nachteile einschließlich des Identitätsbetrugs für die betroffene Person vermeiden.[602]

Ein Abwehranspruch ist auch in dem entsprechend benannten eigenen Kapitel III zu den Rechten des Betroffenen nicht zu finden. Festgehalten sind dort lediglich Vorgaben zur Transparenz der Datenverarbeitung (Abschnitt 1), Informationspflichten des für die Datenverarbeitung Verantwortlichen und das Auskunftsrecht des Betroffenen (Abschnitt 2), Berichtigungs-und Löschungsansprüche (Abschnitt 3) sowie das Recht auf Widerspruch gegen die Datenverarbeitung (Abschnitt 4). Die Verordnung will die Kontrolle der betroffenen Person über ihre personenbezogenen Daten sicherstellen (ErwG 6). Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordere eine Stärkung und Präzisierung der Rechte der betroffenen Personen sowie eine Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden. Der Entwurf geht demnach von einem solchen wirksamen Schutz schon durch die festgehaltenen Betroffenenrechte aus, so dass mit der Festlegung der Rechte des Betroffenen zugleich die Reichweite des Schutzes personenbezogener Daten konkretisiert wird.

---

602 ErwG 67; Ziff. 3.4.4.2 Abs. 2 der Begründung zur DS-GVO-E verweist wegen des Regelungsinhalts auf Art. 4 Abs. 3 der Richtlinie 2002/58/EG des *Europäischen Parlaments* und des *Rates* vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (*Datenschutzrichtlinie für elektronische Kommunikation*), Amtsblatt Nr. L 201 vom 31.7.2002, S. 37-47, nach Maßgabe des Vorschlags für eine Richtlinie des *Europäischen Parlaments* und des *Rates* zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, KOM (2007) 698 endgültig vom 13.11.2007.

Schließlich sieht der Entwurf einen Schadensersatzanspruch der betroffenen Person wegen einer rechtswidrigen Verarbeitung oder einer anderen mit der Verordnung nicht zu vereinbarenden Handlung gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter vor (Art. 77 Nr. 1 DS-GVO-E).[603] Auch der Zugriff auf ein informationstechnisches System wäre grds. eine solche Handlung, da dieser die selbstbestimmte Verfügung des Betroffenen über persönliche Informationen aufhebt. Ausweislich der Entwurfsbegründung stützt sich der Anspruch auf die Regelung des Art. 23 EG-Datenschutzrichtlinie.[604] Rechtswidrige Verarbeitung ist aber nur die Verarbeitung personenbezogener Daten entgegen Art. 6 DS-GVO-E. ErwG 118 adressiert hierfür ausdrücklich den für die Verarbeitung Verantwortlichen. Mithin dürfte sich Art. 77 Nr. 1 Alt. 2 DS-GVO-E auf diejenigen Pflichten beziehen, die dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter in Kapitel IV auferlegte werden.[605] ErwG 67 benennt die Gefahr wirtschaftlicher Schäden als Grund der Meldepflicht in Art. 31, 32 DS-GVO-E. Art. 22 Abs. 1 DS-GVO-E konkretisiert diese Pflichten dahingehend, zu sichern, dass personenbezogene Daten in Übereinstimmung mit der Verordnung verarbeitet werden. Mithin lässt sich der Norm ein Schadensersatzanspruch hinsichtlich der Schutzgüter der Privatsphäre oder des Persönlichkeitsrechts im Allgemeinen kaum entnehmen, wenn sich die verletzten Pflichten auf den Umgang mit personenbezogenen Daten beziehen.[606] Ersatzpflichtig ist nur der Schaden, der sich aus der Verletzung des Zieles des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten ergibt, vgl. Art. 1 Abs. 1 DS-GVO-E.

---

[603] Die *Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutz-Grundverordnung* (abrufbar unter: http://www.lda.brandenburg.de/sixcms/media.php/lbm1.a.3310.de/DSK_Stellungnahme_Grundverordnung.pdf), S. 31, kritisiert eine unklare Fassung der in Kapitel VII der DS-GVO-E vorgesehen Regelungen; diese erfüllten nicht die Voraussetzungen eines unionsweit wirksamen Rechtsschutzes für den Betroffenen.

[604] Ziff. 3.4.8 Abs. 5 der Begründung zur DS-GVO-E.

[605] In diese Richtung auch *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 23 Ziff. 2.3: Mit den einzelstaatlichen Vorschriften zur Umsetzung der Richtlinie nicht zu vereinbarende Handlung ist die Nichterfüllung einer Pflicht des Verantwortlichen gegenüber der betroffenen Person, z.B. zur Information oder Auskunft; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 23 Rn. 8, benennen ebenfalls unterlassene Informations- und Aufklärungspflichten als haftungsbegründende Handlungen; *Brühann*, in: *Grabitz/Hilf/Nettesheim/Wolf* (Hrsg.), Recht der EU, Bd. IV, A 30 Rn. 5, sieht hingegen in der zweiten Tatbestandsalternative keine wesentliche Erweiterung der Haftung; der *Bundesrat* (BR-Drucks. 52/1/12(B)(2), S. 24 Ziff. 55) kritisiert entsprechend der Empfehlung des *Ausschusses für Fragen der Europäischen Union*, des *Ausschusses für Innere Angelegenheiten* und des *Rechtsausschusses* (BR-Drucks. 52/1/12 S. 31 Ziff. 78), dass der Vorschrift nicht mit der für eine Haftungsnorm hinreichenden Klarheit entnommen werden könne, was unter einer „mit dieser Verordnung nicht zu vereinbarenden Handlung" zu verstehen ist.

[606] *Schneider/Härting*, ZD 2012, 199 (202).

iii. Schutzzweck

Auch dem Schutzzweck der Verordnung lässt sich der Schutz der selbstbestimmten Verfügung über das eigene informationstechnische System nicht entnehmen. Die Verordnung hat gem. Art. 1 Nr. 2 DS-GVO-E den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten zum Ziel. Diese Zielsetzung wird maßgeblich vom sachlichen Anwendungsbereich der Verordnung bestimmt. Dieser ist vom Vorliegen personenbezogener Daten abhängig. Anders als die EG-Datenschutzrichtlinie von 1995, deren Art. 1 Abs. 1 den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Gegenstand der Richtlinie machte, mithin personenbezogene Daten bloß zum Zwecke des Schutzes der Privatsphäre geschützt wurden, macht die Verordnung das personenbezogene Datum selbst zum Schutzgegenstand.[607] Der Entwurf formuliert damit keine abstrakten Schutzziele, sondern macht die Reichweite des grundrechtlichen Schutzes allein von dem Begriff des personenbezogenen Datums abhängig. Ohne Personenbezug ist der Anwendungsbereich der Verordnung nicht eröffnet. Nicht der Schutz der Persönlichkeit des Betroffenen ist entscheidend, sondern der abstrakte Begriff des personenbezogenen Datums.[608] Der Begriff wird als „Schlüsselkonzept" der geltenden Datenschutzvorschriften der Europäischen Union zum Schutz von Privatpersonen angesehen.[609] Die DS-GVO-E übernehme daher das geltende Regelungsprinzip des deutschen und europäischen Datenschutzrechts.[610] Dieser Ansatz findet sich auch in den aufgeführten Normen zur Grundlage des unionsrechtlichen Datenschutzes.[611] Die DS-GVO-E verweist auf Art. 8 GR-Charta und Art. 16 AEUV (ErwG 1). Auch die Mitteilung der Kommission zum *Schutz der Privatsphäre in einer vernetzten Welt* entnimmt diesen Normen den Schutz

[607] Kritisch hinsichtlich einer dadurch fehlenden Abwägungsmöglichkeit zwischen Privatsphäre und freier Kommunikation *Schneider/Härting*, ZD 2012, 199 (200); *dies.*, ZD 2011, 63 (64) (zum BDSG); im Falle der Kollisionen grundrechtlicher Positionen läge daher ein dem § 823 Abs. 1 BGB vergleichbarer Abwägungstatbestand daher näher als ein Verbot mit Erlaubnisvorbehalt, *Härting*, AnwBl 2012, 716 (717); *Abel*, Stellungnahme zur EU-Datenschutz-Grundverordnung, Ausschuss-Drucks. 17 (4) 584 B, S. 1f. Ziff. 2.

[608] Kritisch *Härting*, BB 2012, 459 (463); *Abel*, Stellungnahme zur EU-Datenschutz-Grundverordnung, Ausschuss-Drucks. 17 (4) 584 B, S. 1f. Ziff. 3a).

[609] Mitteilung der *Kommission* an das *Europäische Parlament*, den *Rat*, den *Europäischen Wirtschafts- und Sozialausschuss* und den *Ausschuss der Regionen* - Gesamtkonzept für den Datenschutz in der Europäischen Union vom 4.11.2010, KOM (2010) 609 endgültig, S. 5 Ziff. 2.1.1; nach *v. Lewinski*, DuD 2012, 564 (567), erfassen dagegen die europäischen Datenschutzgewährleistungen über die ganz auf den *Daten*schutz fokussierte deutsche Dogmatik hinaus auch den eigentlichen Schutz des Menschen (Hervorhebung im Original).

[610] *Karg*, ZD 2012, 255 (256).

[611] *Britz*, EuGRZ 2009, 1 (8), vermisst bislang eine konzeptionelle Beschreibung des europäischen Datenschutzgrundrechts durch den EuGH.

personenbezogener Daten in Europa.[612] Mit übereinstimmendem Wortlaut sichern Art. 16 Abs. 1 AEUV und Art. 8 Abs. 1 GR-Charta jeder Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Art. 16 Abs. 1 AEUV bestätigt damit das schon in Art. 8 GR-Charta enthaltene Recht auf Datenschutz.[613] Einen darüberhinausgehenden Schutz verschafft die Norm nicht.[614] Art. 16 AEUV trat mit dem *Vertrag von Lissabon*[615] an die Stelle des Art. 286 EG.[616] Danach fanden die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und dem freien Verkehr solcher Daten auf die durch den EGV oder auf der Grundlage dieses Vertrags errichteten Organe und Einrichtungen der Gemeinschaft Anwendung. Diese umfassende Bindung an das sekundärrechtliche Datenschutzrecht erfasste insbesondere die EG-Datenschutz- und die *EG-Telekommunikationsdatenschutzrichtlinie*.[617] Zu diesen Richtlinien trat später die *Datenschutzrichtlinie für elektronische Kommunikation* hinzu.[618] Die EG-Datenschutzrichtlinie stellt damit den Grundbaustein des europäischen Datenschutzrechts dar.[619] Der Anwendungsbereich der dieser Richtlinien ist jeweils vom Begriff des personenbezogenen Datums abhängig.[620] Art. 16 Abs. 1 AEUV übernimmt folglich das Konzept der EG-Datenschutzrichtlinie.[621] Der Norm liegt damit ein am Begriff der personenbezogenen Daten ausgerichtetes Schutzkonzept zugrunde. Art. 8 GR-Charta stützt sich u.a. wiederum auf Art. 286 EGV und die EG-Datenschutzrichtlinie.[622] Der Schutz personenbezogener Daten ist nicht nur als ein Teilbereich des Persönlichkeitsschutzes, sondern als eigenständiges Recht festgeschrieben. Art. 8 GR-Charta ist lex specialis zu dem Recht

---

612 Mitteilung der Kommission an das *Europäische Parlament*, den *Rat*, den *Europäischen Wirtschafts- und Sozialausschuss* und den *Ausschuss der Regionen* - Der Schutz der Privatsphäre in einer vernetzten Welt; ein europäischer Datenschutzrahmen für das 21. Jahrhundert vom 25.1.2012, KOM (2012) 9 endgültig, Ziff. 1 Abs. 2.

613 *Sobotta*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), Recht der EU, Bd. 1, AEUV Art. 16 Rn. 16.

614 Streinz/*Herrmann*, Art. 16 AEUV Rn. 5; *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 19 Ziff. B. I. 2. c); *Spiecker gen. Döhmann/Eisenbarth*, JZ 2011, 169 (172).

615 *Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft*, Amtsblatt Nr. C 306 vom 17.12.2007, S. 1-271.

616 *Vertrag zur Gründung der Europäischen Gemeinschaft*, Amtsblatt Nr. C 321 E vom 27.12.2006, S. 37ff. (konsolidierte Fassung 2006).

617 Richtlinie /66/EG des *Europäischen Parlaments* und des *Rates* vom 15.12.1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, Amtsblatt Nr. L 24 vom 30.1.1998, S. 0001-0008.

618 Richtlinie 2002/58/EG des *Europäischen Parlaments* und des *Rates* vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Amtsblatt Nr. L 201 vom 31.7.2002, S. 37-47.

619 *Artikel-29-Datenschutzgruppe/Arbeitsgruppe Polizei und Justiz*, Die Zukunft des Datenschutzes - Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten, WP168 S. 6 (abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_de.pdf).

620 Siehe jeweils Art. 1 Abs. 1, Art. 3 Abs. 1.

621 *Streinz*, in: *Ders.* (Hrsg.), EUV/AEUV, Art. 8 GR-Charta Rn. 8.

622 Erläuterungen zur Charta der Grundrechte, Amtsblatt Nr. C 303 vom 14.12.2007, S. 17 (20f.).

auf Achtung des Privatlebens in Art. 7 GR-Charta[623] und regelt damit einen speziellen Aspekt des Schutzes der Privatsphäre.[624] Das Grundrecht des Art. 8 GR-Charta entspreche insoweit dem *RiS*.[625] Soweit der *EuGH* eine gemeinsame Prüfung von Art. 7 und 8 GR-Charta vornimmt,[626] lässt sich diese Subsumtion darauf zurückführen, dass sich der *EuGH* für das ungeschriebene europäische Datenschutzgrundrecht am Schutz des Privatlebens aus Art. 8 EMRK[627] orientierte.[628] Letztere Norm wird in der Begründung zur DS-GVO-E ebenfalls in Bezug genommen (Ziff. 3.3). Art. 8 EMRK wird dort aber ausdrücklich nur unter dem Aspekt des Rechts auf Schutz personenbezogener Daten genannt. Der Verweis dürfte daher nur soweit reichen, als der EuGH in seiner Rechtsprechung zur Ausgestaltung des europäischen Datenschutzes Art. 8 EMRK heranzog.[629]

Dieser Schutzansatz spricht gegen die Erfassung der Vertraulichkeit und Integrität informationstechnischer Systeme. Der Schutzbereich des *GVIiS* lässt sich mit dem Begriff des personenbezogenen Datums nur unzureichend beschreiben. Letzterer ist nur insoweit schutzbereichseröffnend, als es um den Funktionsumfang des informationstechnischen Systems geht. Voraussetzung ist lediglich die Eignung zur Verarbeitung personenbezogener Daten in einem bestimmten Umfang und einer bestimmten Art. Das tatsächliche Vorliegen personenbezogener Daten ist nach der Konzeption des *BVerfG* hingegen nicht schutzbereichseröffnend. Ferner schützt das *GVIiS* auch Daten ohne Personenbezug, sofern ihre Erhebung die Folge des Zugriffs auf das informationstechnische System des Betroffenen ist. Die Abhängigkeit der Eröffnung des Anwendungsbereichs der DSGVO-E vom Vorliegen eines personenbezogenen Datums entspricht nicht dem Schutz der selbstbestimmten Verfügung über das eigengenutzte informationstechnische System. Der Persönlichkeitsschutz ist gänzlich anders konzipiert. Mit dem gegenständlichen Urteil hat das *BVerfG* den Umfang der durch das allgemeine Persönlichkeitsrecht geschützten Gegenstände über das personenbezogene Datum hinaus auf das informationstechnische System erweitert.[630] Das *GVIiS* schützt das informationstechnische System als eine besondere Privatheitssphäre und damit einen bestimmten Rückzugsbereich der Persönlichkeitsäußerung.[631] Ein vollumfänglicher Persönlichkeitsschutz, der auch den Schutzbereich des *GVIiS* umfasst,

---

[623] *Streinz*, in: *Ders.* (Hrsg.), EUV/AEUV, Art. 8 GR-Charta Rn. 7; *Kingreen*, in: *Callies/Ruffert* (Hrsg.), EUV/AEUV, GRCh Art. 8 Rn. 1; *Guckelberger*, EuZW 2011, 126 (127).

[624] *Streinz*, in: *Ders.* (Hrsg.), EUV/AEUV, GR-Charta Art. 8 Rn. 7

[625] *Reding*, ZD 2011, Editorial S. 1.

[626] *EuGH*, Urt. v. 9.11.2010 - verb. Rs. C-92/09 und C-93/09, Slg. 2010, I-11063 - *Schecke/Eifert*, Rn. 52, 64, 72, 76, 79f., 85ff.; kritisch *Guckelberger*, EuZW 2011, 126 (127).

[627] *Konvention zum Schutz der Menschenrechte und Grundfreiheiten* in der Fassung der Bekanntmachung vom 22.10.2010, BGBl. II S. 1198.

[628] *Britz*, EuGRZ 2011, 1 (6f.) m.w.N.; *Spiecker gen. Döhmann/Eisenbarth*, JZ 2011, 169 (171) m.w.N.

[629] Hierzu etwa *EuGH*, Urt. v. 20.5.2003, verb. Rs. C-465/00, C-138/01 und C-139/01 - ORF, Rn. 71ff.

[630] *Härting/Schneider*, ZRP 2011, 233 (235).

[631] *Bäcker*, Der Staat [2012], S. 91 (93f.).

lässt sich allein über das Tatbestandsmerkmal des personenbezogenen Datums nicht realisieren.[632] Die Verletzung von Persönlichkeitsrechten durch eine bestimmte Datenverarbeitung lässt sich nur kontextabhängig feststellen und kann nicht allein in Bezug auf den technischen Vorgang der „Datenverarbeitung" pauschal beurteilt und schematisch geregelt werden.[633]

Ferner steht neben dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten noch das Regelungsziel des freien Verkehrs solcher Daten, Art. 1 Abs. 1 DS-GVO-E.[634] Die besondere Betonung des freien Datenverkehrs geht auf die ursprüngliche wirtschaftliche Motivation für eine europäische Datenschutzregelung zurück.[635] Die EG-Datenschutzrichtlinie gründete auf der Harmonisierungskompetenz des Art. 95 EG (Art. 100a EWGV; jetzt: Art. 114 AEUV) zur Errichtung und zum Funktionieren des Binnenmarktes.[636] Der Datenschutz fand demnach als Thema der Verwirklichung des Binnenmarktes Eingang in das Unionsrecht.[637] Wiederum wird das Erreichen eines grenzenlosen digitalen Binnenmarktes auch als stärkstes Argument für das Regelungsinstrument der Verordnung angeführt.[638] Der Rechtsrahmen der DS-GVO-E soll i.E. dahingehend gerade auch die digitale Wirtschaft fördern.[639] Der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme nach dem hier vertretenen Verständnis hat jedoch keine solche wirtschaftliche Komponente. Der Schutz betrifft nicht das Vertrauen des Betroffenen in den ordnungsgemäßen Umgang der von ihm einem anderen gegenüber willentlich preisgegebenen personenbezogenen Daten. Es geht um den Schutz der Persönlichkeitsentfaltung vor Überwachung in einer technischen Sphäre. Das *GVIiS* schützt die ungehinderte Persönlichkeitsentfaltung mittels der Nutzung informationstechnischer Systeme.[640]

Schließlich entspringt die einschlägige Entscheidung des *BVerfG* zum *GVIiS* Verfassungsbeschwerden über das VSG NRW 2007. Die Maßgaben des *GVIiS* in der Beziehung des Bürgers zum Staat betreffen den Bereich der nationalen Si-

---

632 I.d.S. auch *Karg*, ZD 2012, 255 (259), der die Eignung des Merkmals des Personenbezugs zur vollständigen Erfassung der Gefährdung von Persönlichkeitsrechten verneint; ebenso *Schneider/Härting*, ZD 2011, 63 (65).

633 *Abel*, Stellungnahme zur EU-Datenschutz-Grundverordnung, Ausschuss-Drucks. 17 (4) 584 B, S. 5 Ziff. 3c).

634 Nach *Sommer*, Stellungnahme zur EU-Datenschutz-Grundverordnung, Ausschuss-Drucks. 17 (4) 584 C, S. 3 Ziff. I, komme darin ein europäischer Datenschutz zum Ausdruck, der nicht auf die größtmögliche Verwirklichung des europäischen Datenschutzgrundrechtes gerichtet ist, sondern zum Zwecke der Herstellung des digitalen Binnenmarktes besteht; i.d.S. auch *Wagner*, DuD 2012, 676.

635 *Reding*, ZD 2012, 195; diese Motivation ergebe sich auch aus dem Titel der EG-Datenschutzrichtlinie.

636 *Spiecker gen. Döhmann/Eisenbarth*, JZ 2011, 169 (170), sehen darin einen Beleg für die wirtschaftliche Ausrichtung des Datenschutzes.

637 *Artikel-29-Datenschutzgruppe/Arbeitsgruppe Polizei und Justiz*, WP 168 (Fn. 619), S. 7.

638 *Reding*, ZD 2012, 195 (196).

639 ErwG 6 sowie Ziff. 1 S. 1f. der Begründung zur DS-GVO-E.

640 *BVerfGE* 120, 274 (306).

cherheit und der Strafverfolgung. Für diese Bereiche ist der Anwendungsbereich der DS-GVO-E hingegen ausdrücklich nicht eröffnet, vgl. Art. 2 a), e) DS-GVO-E.

d. Zusammenfassung

Die DS-GVO-E erfasst den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme aus verschiedenen Gründen nicht. Schon der Wortlaut des Entwurfs lässt sich für einen dahingehenden sachlichen Anwendungsbereich nicht heranziehen. Auch seiner Systematik lässt sich ein notwendiger individueller Abwehranspruch gegen den unberechtigten Zugriff auf ein informationstechnisches System nicht entnehmen. Schließlich steht das Schutzkonzept des europäischen Datenschutzrechts, das wiederum auch in der DS-GVO-E zum Ausdruck kommt, dem Schutz der selbstbestimmten Verfügung über das eigene informationstechnische System entgegen. Die Persönlichkeitsrelevanz der besonderen technischen Sphäre, die durch die Nutzung eines komplexen informationstechnischen Systems geschaffen wird, lässt sich mit dem Begriff des personenbezogenen Datums nicht vollständig erfassen. Ein etwaiger Anwendungsvorrang der europäischen Regelung würde daher das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG formulierte *GVIiS* nicht erfassen.

II. Personaler Schutzbereich

Der personale Schutzbereich des *GVIiS* weist gegenüber anderen Ausprägungen des allgemeinen Persönlichkeitsrechts eine entscheidende Besonderheit auf. Während Art. 2 Abs. 1 GG keine Einschränkungen des personalen Anwendungsbereichs vorsieht, fordert das *BVerfG* für das *GVIiS*, dass der Betroffene das informationstechnische System „als eigenes" nutzt.[641] Die Ausführungen zum personalen Schutzbereich beschäftigen sich daher zunächst mit der Grundrechtsberechtigung hinsichtlich des allgemeinen Persönlichkeitsrechts. Auf dieser Grundlage wird dann ein mögliches Verständnis des vom *BVerfG* für die Eröffnung des Schutzbereichs des *GVIiS* vorausgesetzten „eigenen" informationstechnischen Systems herausgearbeitet. Schließlich wird noch die Anwendbarkeit des *GVIiS* auf juristische Personen gem. Art. 19 Abs. 3 GG geprüft.

Das allgemeine Persönlichkeitsrecht stellt zwar eine Verknüpfung der Grundrechtstatbestände des Art. 2 Abs. 1 und Art. 1 Abs. 1 GG dar. Letzterer wird dadurch aber nicht selbständiger Prüfungsmaßstab, sondern lediglich das hinter der Menschenwürdegarantie stehende Menschenbild zur Auslegung des Art. 2 Abs. 1 GG herangezogen.[642] Grundlage des allgemeinen Persönlichkeitsrechts ist

[641] Siehe hierzu *BVerfGE* 120, 274 (315).
[642] *Starck*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 15.

daher Art. 2 Abs. 1 GG.[643] Danach hat jeder das Recht auf freie Entfaltung seiner Persönlichkeit. Eine Eingrenzung des personalen Schutzbereichs erfolgt nicht. Art. 2 Abs. 1 GG steht daher als Jedermannsgrundrecht[644] zunächst allen lebenden natürlichen Personen zu.[645] Gleiches gilt somit zunächst auch für das *GVIiS* als Ausprägung des allgemeinen Persönlichkeitsrechts.

*1. Nutzung des Systems „als eigenes"*

a. Vorbemerkungen

Im Gegensatz zu anderen Ausprägungen des allgemeinen Persönlichkeitsrechts erschöpfen sich damit noch nicht die Voraussetzungen für die Eröffnung des personalen Schutzbereichs des *GVIiS*: Auf dessen Schutz kann sich nur berufen, wer ein informationstechnisches System „als eigenes" nutzt:[646]

> „*Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt.*"

Eine nähere Erläuterung, wann der Betroffene das System „als eigenes" nutzt und damit darüber „selbstbestimmt verfügt", erfolgt jedoch nicht. Dementsprechend werden verschiedene Ansatzpunkte für das Verständnis des Begriffs diskutiert.

i. Definitionsansätze

„Eigenes" sei begrifflich grundsätzlich eine zivilrechtliche Kategorie, die auf die Eigentums- und Besitzkonzepte des BGB verweise.[647] „Verfügungsgewalt" habe im Grunde nur der Eigentümer, so dass jedenfalls nicht das Eigentum an dem informationstechnischen System, sondern die tatsächliche Sachherrschaft und damit der Besitz gemeint sein könnten. Andere wiederum halten eine Auslegung des Begriffs alleine anhand von sachenrechtlichen Kategorien nicht für zwingend.[648] Zwar sei der Begriff allein anhand von rechtlichen Zuordnungen zu be-

---

643 So ausdrücklich *BVerfGE* 56, 37 (41f.); *Schmitt Glaeser*, in: HStR VI², § 129 Rn. 26; *Starck*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 89; vgl. auch *BVerfGE* 35, 202 (219); 82, 236 (269); 90, 263 (270).

644 Als *Jedermannsrechte* lassen sich diejenigen Grundrechte bezeichnen, die keine Eingrenzung der Grundrechtsberechtigung in persönlicher Hinsicht vorsehen und dementsprechend jedermann zustehen (*Pieroth/Schlink*, Grundrechte, Rn. 121).

645 *Kube*, in: HStR VII³, § 148 Rn. 72.

646 *BVerfGE* 120, 274 (315); bei *Herrmann*, IT-Grundrecht, S. 121 ist dieses Erfordernis dagegen bereits Teil der Definition des informationstechnischen Systems.

647 *Hoeren*, MMR 2008, 365 (366).

648 *T. Böckenförde*, JZ 2008, 925 (929); *Hornung*, CR 2008, 299 (303); *Moos*, K&R 2009, 154 (155); *Stögmüller*, CR 2008, 435 (436); *Wegener/Muth*, JURA 2010, 847 (850); Kilian/Heussen/*Polenz*, CHB Kap. 130 Rn. 36; *Bartsch*, CR 2008, 613 (614).

stimmen, dies wären aber neben dem sachenrechtlichen Eigentum insbesondere vertragliche Nutzungs- und Ausschlussrechte.[649] Weitergehend sind Auslegungsansätze, die sich von der Begriffsbestimmung allein anhand rechtlicher Kriterien lösen: Für das Begriffsverständnis kämen demnach sowohl technische – der Standort des Systems oder Zugriffssicherungen – als auch rechtliche Kriterien – gesetzliche oder vertragliche Zugriffsbefugnisse und Abwehransprüche – in Frage.[650] Ebenso könne der Begriff auch eine bloß tatsächliche Nutzungsberechtigung meinen.[651] Insofern sei jedenfalls der Begriff nicht der „eigenen", sondern der „eigengenutzten" informationstechnischen Systeme passender, da diese sprachliche Präzisierung eine Zuordnung nur anhand von sachenrechtlichen Kriterien vermeide.[652] Denn die Nutzung eines informationstechnischen Systems „als eigenes" stelle auch die Rechnernutzung in einem Internetcafé dar.[653] Eine Eigennutzung liege ebenfalls vor, wenn das informationstechnische System bloß Gegenstand einer Leihe ist.[654] Sämtliche Definitionsansätze, die auf einfachgesetzliche Begrifflichkeiten zurückgreifen, haben jedenfalls gemeinsam, dass dieser Rückgriff den verfassungsrechtlichen Schutzgegenstand abbildet. Keinesfalls kann umgekehrt der einfachgesetzliche Begriff zur Auslegung der grundrechtlichen Gewährleistung herangezogen werden.[655]

ii. Private und geschäftliche Nutzung

Der Grundrechtsschutz des *GVIiS* erstreckt sich nicht nur auf die Nutzung des informationstechnischen Systems für private Zwecke, sondern erfasst ausdrücklich auch die geschäftliche Nutzung.[656] Denn auch bei dieser lasse sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Damit dürfte auch die Nutzung stationärer PCs, Notebooks und elektronischer Terminkalender von Unternehmensmitarbeitern vom Schutzbereich des *GVIiS* erfasst sein, sofern diese von den entsprechenden Mitarbeitern eigenverantwortlich genutzt werden.[657] Grundrechtsträger ist in diesem Fall der einzelne

---

[649] *Bäcker*, in: *Rensen/Brink* (Hrsg.), Rechtsprechung des Bundesverfassungsgerichts, S. 99 (128); *Ders.*, in : *Uerpmann-Wittzack* (Hrsg.), Computergrundrecht, S. 1 (12).

[650] *Hornung*, CR 2008, 299 (303).

[651] *T. Böckenförde*, JZ 2008, 925 (929).

[652] *Hoffmann-Riem*, JZ 2008, 1009 (1019 Fn. 95).

[653] *T. Böckenförde*, JZ 2008, 925 (929); *Hoffmann-Riem*, JZ 2008, 1009 (1019 Fn. 95).

[654] *T. Böckenförde*, JZ 2008, 925 (929).

[655] Vgl. insoweit zum Verhältnis grundrechtlicher Gewährleistung und privatrechtlicher Zuordnung bei Art. 13 Abs. 1 GG AK-GG-*Berkemann*, Bd. 1, Art. 13 Rn. 15: „Die grundrechtliche Gewährleistung […] setzt die Befugnis des einzelnen voraus, eine räumliche Ausgrenzung zum Medium seiner privaten Entfaltung gegenüber anderen zu machen, indem er die ihm zuerkannte Definitionsmacht über die Funktion eines räumlich-gegenständlichen Dispositionsspielraums und dessen hierauf bezogene, von ihm kontrollierte Zugänglichkeit verbindlich ausübt. […] Gegenüber dem staatlichen Zugriff ist insoweit nicht die privatrechtliche Rechtmäßigkeit, sondern der sozial anerkannte Anspruch auf Beachtung privater Zugänglichkeit maßgebend."

[656] *BVerfGE* 120, 274 (314).

[657] *Stögmüller*, CR 2008, 435 (436).

Mitarbeiter, dessen Persönlichkeitsprofil in Folge der Infiltration des betroffenen informationstechnischen Systems erstellt werden kann. Da aber die private und geschäftliche Nutzung des informationstechnischen Systems die Eröffnung des Schutzbereichs alternativ begründen können, greift der Schutz des *GVIiS* bereits, ohne dass zwingend die Nutzung des vom Arbeitgeber überlassenen informationstechnischen Systems auch zu privaten Zwecken notwendig wäre. Ob die Nutzung des Systems neben geschäftlichen auch für private Zwecke erfolgt, ist daher bei der Eröffnung des Schutzbereichs des *GVIiS* nicht zu berücksichtigen. Die erforderliche Eigennutzung stellt somit nicht auf eine Unterscheidung zwischen privater und geschäftlicher Nutzung des informationstechnischen Systems ab.

b. Eigentum im Sinne des § 903 BGB

Die Nutzung des informationstechnischen Systems „als eigenes" könnte daher zunächst voraussetzen, dass das System im Eigentum des Nutzers steht. Der Schutzbereich des *GVIiS* würde dann die Nutzung informationstechnischer Systeme nur insoweit erfassen, als der Nutzer des Systems zugleich auch dessen Eigentümer ist.

i. Notwendigkeit eines körperlichen Gegenstands

Die Gleichstellung mit sachenrechtlichen Kategorien wie dem Eigentum gem. § 903 BGB oder dem Besitz gem. §§ 854ff. BGB setzt voraus, dass die Bezugsobjekte Sachen i.S.d. § 90 BGB, mithin körperliche Gegenstände sind. Sofern die Hard- und Softwarekomponenten des betroffenen informationstechnischen Systems konstruktionsbedingt einen in sich abgeschlossenen körperlichen Gegenstand bilden – so etwa ein Laptop oder ein Mobiltelefon –, wäre die Sacheigenschaft zu bejahen und die Anknüpfung an sachenrechtliche Kategorien nicht von vornherein ausgeschlossen. Eine solche Konstruktion, die auf einen einzigen körperlichen Gegenstand begrenzt ist, ist jedoch nicht zwingend. Greift der Nutzer über das Internet auf Softwarekomponenten oder Webspace zu, können diese durch die Verbindung mit dem zugreifenden System wiederum Teil eines durch diese Verbindung entstehenden informationstechnischen Systems werden. Diese Softwarekomponenten oder nicht körperlich sondern nur logisch abgrenzbarer Speicherplatz werden auf einem Datenträger zur Verfügung gestellt, an dem ein Dritter Eigentum und/oder Besitz hat. Sowohl diese Softwarekomponenten als auch der zugewiesene Webspace stellen für sich genommen keine körperlichen Gegenstände dar. Sachen i.d.S. § 90 BGB sind nur die Datenträger auf denen die

jeweiligen Daten verkörpert sind.[658] Allein die Anknüpfung an das Eigentum oder auch den Besitz könnte somit den Begriff des „eigenen" informationstechnischen Systems nicht vollständig erfassen, da unkörperliche Systemkomponenten kein taugliches Bezugsobjekt darstellen würden.

ii. Verfassungsrechtliche Vorgaben

Gegen die Gleichstellung mit dem zivilrechtlichen Eigentumsbegriff spricht zunächst die vom Schutzbereich des *GVIiS* ausdrücklich erfasste geschäftliche Nutzung eines informationstechnischen Systems. Denn das von einem Mitarbeiter in einem Unternehmen an seinem Arbeitsplatz genutzte oder ihm für die Zeit seiner Anstellung überlassene informationstechnische System wird regelmäßig im Eigentum des beschäftigenden Unternehmens stehen.

Daneben lässt sich auch hier eine Parallele zu Art. 13 Abs. 1 GG ziehen.[659] Die Gewährleistung der Unverletzlichkeit der Wohnung soll dem Einzelnen mit Blick auf die Menschenwürde und im Interesse der Entfaltung der Persönlichkeit einen elementaren Lebensraum sichern.[660] Die Eröffnung des Schutzbereichs knüpft nicht an das Eigentum an der Wohnung an.[661] Schutzgut des Art. 13 Abs. 1 GG ist die räumliche Privatsphäre und nicht das Eigentum an der Räumlichkeit.[662] Vielmehr genießt derjenige Schutz, der tatsächlich wohnt.[663] Das *GVIiS* dient als Ausprägung des allgemeinen Persönlichkeitsrechts der Gewährleistung der engeren persönlichen Lebenssphäre und der Erhaltung ihrer Grundbedingungen.[664] Der persönlichkeitsrechtliche Bezug der auf dem informationstechnischen System enthaltenen Daten besteht nicht zwingend zu dem Eigentümer des Systems, sondern zu demjenigen, der durch die Nutzung des Systems diesem „persönliche

---

658 *OLG Karlsruhe* NJW 1996, 200 (201); MüKoBGB-*Wagner* § 823 Rn. 103; davon zu trennen ist die Frage nach dem deliktsrechtlichen Schutz der Daten, durch deren Löschung das Eigentum an dem Datenträger i.S.d. § 823 Abs. 1 BGB verletzt wird (*OLG Karlsruhe* NJW 1996, 200 (201); MüKoBGB-*Wagner* § 823 Rn. 103; *Meyer/Wehlau*, NJW 1998, 1585 (1588); *Bartsch*, CR 2000, 721 (723); Staudinger/*Hager* (1999), § 823 Rn. B60, *Taeger*, Außervertragliche Haftung, S. 261; a.A. LG Konstanz, NJW 1996, 2662). Die Anerkennung des Schutzes aus § 823 Abs. 1 BGB ist jedoch nicht gleichbedeutend mit der Anerkennung der Sachqualität der enthaltenen Daten. Überdies setzt der deliktsrechtliche Schutz das Eigentum am modifizierten Datenträger voraus, das wiederum nicht einhergehen muss mit der Nutzung der Speicherkapazitäten und der Berechtigung an den enthaltenen Daten.

659 Siehe hierzu bereits oben auf S. 25; *Rux*, JZ 2007, 285 (293f.), argumentiert sogar für eine analoge Anwendung der Schranken des Art. 13 Abs. 2-7 GG auf den Zugriff auf informationstechnische Systeme, die sich außerhalb einer Wohnung befinden, um dem Schutz mit Hilfe der modernen Informationstechnologie geschaffenen virtuellen Räume gerecht zu werden.

660 *BVerfGE* 42, 212 (219); 51, 97 (110); 89, 1 (12); 103, 142 (150).

661 *Papier*, in: *Maunz/Dürig*, GG, Bd. 2, Art. 13 Rn. 12; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 12; *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 21.

662 *Jarass*/Pieroth, GG, Art. 13 Rn. 6.

663 *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 12.

664 *BVerfGE* 54, 148 (153).

Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert".[665] Die technische Infiltration des informationstechnischen Systems muss einen Einblick in wesentliche Teile der Lebensgestaltung oder ein aussagekräftiges Bild der Persönlichkeit des Nutzers des Systems ermöglichen. Dessen Eigentum an dem informationstechnischen System ist daher keine Voraussetzung für die Entstehung des persönlichkeitsrechtlichen Schutzbedarfs. Dieser ist aber der entscheidende Bezugspunkt des grundrechtlichen Systemschutzes.[666]

iii. Begründung der Persönlichkeitsrelevanz

Ferner spricht gegen die Anknüpfung des Begriffs der „eigenen Systeme" an den Eigentumsbegriff des BGB, dass die Persönlichkeitsgefährdung, die den Schutzgegenstand des *GVIiS* ausmacht, auf den Informationen beruht, die von den Daten vermittelt werden, die auf dem informationstechnischen System enthalten sind. Daten und Informationen sind jedoch keine körperlichen Gegenstände im Sinne des § 90 BGB. Der Anknüpfungspunkt der Auslegung des Begriffs des „eigenen" oder „eigengenutzten" informationstechnischen Systems muss aber die Grundlage der zu begegnenden Gefährdungslage sein. Diese Gefährdungslage wird durch die vermittelten Informationen unabhängig vom Eigentum an dem informationstechnischen Systems begründet. Die Persönlichkeitsrelevanz für den Nutzer des Systems setzt nicht das Eigentum an dem genutzten System voraus. So verhält es sich insbesondere bei der Nutzung eines informationstechnischen Systems durch den Arbeitnehmer im Rahmen eines Beschäftigungsverhältnisses. Dieses wird regelmäßig im Eigentum des Arbeitgebers stehen, aber ausschließlich persönlichkeitsrechtliche Relevanz hinsichtlich des Arbeitnehmers haben.[667]

iv. Wortlaut

Schließlich lässt sich noch einwenden, dass die Eröffnung des Schutzbereichs des *GVIiS* gerade nicht voraussetzt, dass der Betroffene ein *eigenes* informationstechnisches System nutzt. Voraussetzung ist nur, dass ein System *als* eigenes genutzt wird.[668]

v. Zwischenergebnis

Der Begriff des „eigenen" informationstechnischen Systems ist damit nicht i.S.d. zivilrechtlichen Eigentumsbegriffs des BGB zu verstehen sein. Mit dem Schutzgegenstand des *GVIiS* wäre es nicht vereinbar, stets das Eigentum des Betroffenen an dem genutzten System vorauszusetzen. Die von dem *BVerfG* ausgemachte Gefährdung der Persönlichkeit des Betroffenen besteht unabhängig von dem Eigentum an dem informationstechnischen System.

---

[665] *BVerfGE* 120, 274 (313).
[666] Vgl. *Hoffmann-Riem*, JZ 2008, 1009 (1012 Fn. 26).
[667] Ebenso *Wedde*, AuR 2009, 373 (375).
[668] So auch *Bartsch*, CR 2008, 613 (614); *Hornung*, CR 2008, 299 (303).

c. Besitz i.S.d. §§ 854ff. BGB

Es kommt sodann eine Auslegung des Begriffs des „eigenen" Systems anhand des zivilrechtlichen Besitzverständnisses in Betracht. Hierbei sind zunächst die gleichen verfassungsrechtlichen Besonderheiten wie bei der Auslegung anhand des zivilrechtlichen Eigentumsbegriffs zu berücksichtigen. Ausgangspunkt der Überlegungen muss wiederum die hinter dem Schutz des *GVIiS* stehende Persönlichkeitsgefährdung des Nutzers eines informationstechnischen Systems sein. Wie auch das zivilrechtliche Eigentum setzt Besitz einen körperlichen Gegenstand, mithin eine Sache i.S.d. § 90 BGB voraus. Insofern ergeben sich keine Unterschiede in der Argumentation und es kann auf die vorangegangenen Ausführungen verwiesen werden.

i. Begründung der Persönlichkeitsrelevanz

Die Persönlichkeitsgefährdung des Nutzers eines informationstechnischen Systems ergibt sich aus den auf dem System enthaltenen unkörperlichen personenbezogenen Daten. Der Besitz an einem informationstechnischen System ist ebenso wenig gleichbedeutend mit der persönlichkeitsrechtlichen Relevanz seiner Nutzung wie das Eigentum an diesem System. Es muss von den Gefährdungen, die aus der Nutzung des informationstechnischen Systems folgen, nicht notwendig diejenige Person betroffen sein, die Besitz an dem System hat. Diese Überlegung zeigt sich zunächst bei der Rechtsfigur des Besitzdieners. Gem. § 855 BGB ist nicht derjenige Besitzer, der die tatsächliche Gewalt über eine Sache für einen anderen ausübt und dabei dessen Weisungen unterliegt, sondern der andere. Dürfte also nur der Besitzer eines informationstechnischen Systems davon ausgehen, „dass er […] über das informationstechnische System selbstbestimmt verfügt", so wäre der Besitzdiener, der mit der Nutzung dieses Systems zugleich auch die tatsächliche Gewalt darüber ausübt, nie erfasst. Gleichzeitig bestünde die Gefahr einer umfangreichen Ausforschung der Persönlichkeit durch den Zugriff auf das informationstechnische System nur gegenüber dem Besitzdiener, dessen Nutzungs- und Kommunikationsverhalten erst den hierfür notwendigen umfangreichen und vielfältigen Bestand an personenbezogenen Daten begründen könnte. Die Gleichsetzung der Nutzung eines informationstechnischen Systems „als eigenes" mit dem Besitz an diesem System müsste aber dazu führen, dass ein Arbeitnehmer, dem im Rahmen seines Arbeitsverhältnisses informationstechnische Systeme für die Ausübung seiner Tätigkeit überlassen werden, den Schutz des *GVIiS* nicht in Anspruch nehmen könnte. Denn regelmäßig hat der Arbeitnehmer keinen Besitz an den von ihm verwendeten Gegenständen des Arbeitgebers, sondern ist

i.d.R. nur Besitzdiener.[669] Dieses Ergebnis wiederum widerspräche der ausdrücklichen Einbeziehung der geschäftlichen Nutzung informationstechnischer Systeme in den Schutzbereich des *GVIiS*.[670]

ii. Verfassungsrechtliche Vorgaben

Auch hier lässt sich wie bei dem Definitionsansatz, der auf den zivilrechtlichen Eigentumsbegriff abstellt, ein Vergleich mit dem grundrechtlichen Schutz des Art. 13 Abs. 1 GG herstellen. Ebenso wenig wie dieser an das Eigentum an einer Wohnung anknüpft, ist auch der Besitz an einer Wohnung die entscheidende Grundlage für die Eröffnung des personalen Schutzbereichs. Denn Schutzgegenstand des Art. 13 Abs. 1 GG ist nicht das Besitzrecht an einer Wohnung, sondern deren Privatheit.[671] Der personale Schutzbereich des Art. 13 Abs. 1 GG ist demzufolge auch nur für den unmittelbaren Besitzer einer Wohnung eröffnet, nicht erfasst ist jedoch der mittelbare Besitzer.[672] Dass der Besitzdiener gem. § 855 BGB nicht als Besitzer einer Sache gilt, nimmt diesem hingegen nicht den Schutz des Art. 13 Abs. 1 GG. Für die Eröffnung des personalen Schutzbereichs kommt es auf zivilrechtliche Einordnungen nicht entscheidend an.[673] Denn die nach den Begriffen des BGB fehlende Besitzstellung des Besitzdieners steht der Begründung einer nach Art. 13 Abs. 1 GG schutzwürdigen Sphäre nicht notwendig entgegen.[674] Auch für den Besitzdiener können Räumlichkeiten ein „Reservat privater Lebensgestaltung" darstellen.[675] Würde somit der Begriff des „eigenen" informationstechnischen Systems mit dem Besitz im Sinne des § 854 BGB gleichgesetzt werden, so wäre derjenige, der als Besitzdiener das System nutzt, diesem dabei „persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert", nicht vom Schutzbereich des *GVIiS* erfasst, obwohl er durch die Nutzung des Systems „Einblicke in wesentliche Teile seiner Lebensgestaltung" gibt. Die besondere Persönlichkeitsgefährdung, die Ausgangspunkt des grundrechtlichen Schutzes des *GVIiS* ist, liegt somit auch bei dem Besitzdiener i.S.d. § 855 BGB vor.

Fasst man darüber hinaus auch die Nutzung eines PCs in einem Internetcafé unter eine „(temporäre) Eigennutzung",[676] so stellt sich die Frage, ob der Nutzer überhaupt den für eine Nutzung des PCs als „eigenen" notwendigen Besitz an dem von ihm verwendeten Gerät erlangen würde. Der Erwerb des unmittelbaren

669 *BAG* NJW 1999, 1049 (1051).
670 *BVerfGE* 120 , 274 (314).
671 *BVerfGE* 89, 1 (12).
672 *Jarass*/Pieroth, GG, Art. 13 Rn. 6; *Herdegen*, in: BK GG, Bd. 3, Art. 13 Rn. 36; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 13.
673 *Herdegen*, in: BK GG, Bd. 3, Art. 13 Rn. 36; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 13.
674 *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 13.
675 *Herdegen*, in: BK GG, Bd. 3, Art. 13 Rn. 36.
676 So *Hoffmann-Riem*, JZ 2008, 1009 (1019 Fn. 95); *T. Böckenförde*, JZ 2008, 925 (929).

Besitzes im Sinne des § 854 Abs. 1 BGB vollzieht sich durch die Betätigung eines Besitzwillens durch Begründung faktischer Sachherrschaft.[677] Für die tatsächliche Sachherrschaft über eine Sache ist zunächst die Möglichkeit der physischen Einwirkung auf die Sache erforderlich.[678] Diese Einwirkungsmöglichkeit wird dem Nutzer zwar von dem Betreiber gerade bewusst eingeräumt. Ist hier aber daneben jedenfalls schon der zur Erlangung des unmittelbaren Besitzes erforderliche Besitzerwerbswille[679] des Nutzers fraglich, scheitert die rechtliche Qualifikation des Nutzers eines PCs in einem Internetcafé, der faktisch der Sachherrschaft zweier Personen unterliegt, als Besitzer desselben schon daran, dass nach der für die Beurteilung der Besitzverhältnisse maßgeblichen Verkehrsanschauung[680] ausschließlich der Betreiber des Cafés als alleiniger Besitzer der zur Verfügung gestellten Geräte anzusehen ist.[681]

iii. Zwischenergebnis

Zwar können der Besitz i.S.d. § 854 BGB an einem informationstechnischen System und die Begründung der besonderen Gefährdungslage der Persönlichkeit in Folge der Nutzung eines solchen Systems zusammenfallen. Jedoch muss das informationstechnische System nicht in jedem Fall einen abgrenzbaren körperlichen Gegenstand darstellen, so dass eine Besitzstellung schon an der fehlenden tatsächlichen Gewalt über eine Sache scheitert. Ferner begründen die Nutzung eines Systems zur Persönlichkeitsentfaltung und die Ausübung der tatsächlichen Gewalt an diesem System nicht schon die zivilrechtliche Besitzstellung. Die Nutzung eines informationstechnischen Systems „als eigenes" lässt sich somit nicht mit dem Besitz i.S.d. BGB gleichsetzen.

d. Grundlage der Persönlichkeitsentfaltung

Die Nutzung eines informationstechnischen Systems „als eigenes" kann schließlich auch deshalb nicht allein an den Begriffen Eigentum oder Besitz festgemacht werden, da diese Nutzung Aspekte enthält, die sich allein mit diesen Begriffen nicht vollständig erfassen lassen. Das allgemeine Persönlichkeitsrecht schützt die

677 Staudinger/*Bund* (2007) § 854 Rn. 3.

678 MüKoBGB-*Joost*, § 854 Rn. 5.

679 Staudinger/*Bund* (2007) § 854 Rn. 14 m.w.N.

680 *BGH* NJW 1987, 2812 (2813); Staudinger/*Bund* (2007) § 854 Rn. 11; Soergel/*Stadler*, § 854 Rn. 4; *Wolf/Wellenhofer*, Sachenrecht, § 4 Rn. 8; kritisch MüKoBGB-*Joost*, § 854 Rn. 4.

681 Dem steht nicht entgegen, dass zwischen den Parteien ein Mietvertrag zustande kommt oder jedenfalls mietvertragliche Vorschriften auf die Rechnernutzung anzuwenden sind. Denn § 535 Abs. 1 BGB setzt nur voraus, dass der Vermieter dem Mieter die Sache zum Gebrauch überlässt. Die vertraglichen Vereinbarungen bestimmen Art und Umfang der Gebrauchsüberlassung (*BGH* NJW 2007, 2394 (2395)). Nur wenn danach der Gebrauch der Mietsache den Besitz des Mieters voraussetzt, umfasst die Gebrauchsüberlassung auch die Verschaffung des unmittelbaren Besitzes an der Mietsache (*BGH* NJW 2002, 3322 (3323); *BGH* NJW-RR 1989, 589). Ansonsten genügt die Verschaffung nur des Zugangs zur Mietsache (*BGH* NJW 2007, 2394 (2395)).

engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen[682] und sichert dem Einzelnen einen autonomen Bereich privater Lebensgestaltung, in dem er seine Individualität entwickeln und wahren kann[683]. Damit die Vertraulichkeits- und Integritätserwartung des Einzelnen hinsichtlich des von ihm genutzten informationstechnischen Systems grundrechtlich anzuerkennen ist, müsste dessen engere persönliche Lebenssphäre betroffen und sein autonomer Bereich privater Lebensgestaltung, in dem er seine Individualität entwickeln und wahren kann, gefährdet sein. Dies setzt umgekehrt voraus, dass der Betroffene das informationstechnische System in diesem Sinne zur Persönlichkeitsentfaltung nutzt und ihm die hierfür entscheidende Bedeutung beimisst, deren Schutz durch das *GVIiS* gesichert werden soll.

i. Nutzungsberechtigung

Der Betroffene muss zunächst davon ausgehen dürfen, „dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das System selbstbestimmt verfügt". Für eine Prüfung einer Nutzungsberechtigung als selbständige Voraussetzung der Nutzung des informationstechnischen Systems „als eigenes" spricht, dass sich die Begriffe der Vertraulichkeit und Integrität als Eigenschaften informationstechnischer Systems nur am zu schützenden Datenobjekt orientieren. Die Berechtigung i.d.S. beschreibt daher nicht notwendig auch, ob die Nutzung des informationstechnischen Systems überhaupt rechtmäßig erfolgt. Wann eine solche Berechtigung vorliegt, lässt sich den Ausführungen des *BVerfG* nicht entnehmen. Vorausgesetzt wird aber, dass die Nutzungsberechtigung so ausgestaltet ist, dass sie zu der grundrechtlichen Anerkennung der Vertraulichkeits- und Integritätserwartung des Betroffenen führen kann. Eine Nutzungsberechtigung kann sich damit nur aus einer von der Rechtsordnung anerkannten Konstruktion ergeben. Ein Nutzer, der sich den Besitz an einem informationstechnischen System durch verbotene Eigenmacht verschafft hat, kann sich daher grds. nicht auf den Schutz des *GVIiS* berufen.[684] Denn die Herstellung der Nutzungsmöglichkeit steht durch den unfreiwilligen Besitzverlust gerade im Widerspruch zur Rechtsordnung. Auch wenn der unrechtmäßige Besitzer dem System durch dessen Nutzung „persönliche Daten anvertrauen oder schon allein durch dessen Nutzung zwangsläufig liefern" wird, hat die dadurch entstehende Persönlichkeitsrelevanz ihre Grundlage jedoch in der bewusst rechtswidrig erlangten und ausgeübten Besitzposition. Eine daraus folgende Vertraulichkeits- und Integritätserwartung dürfte bereits deswegen regelmäßig nicht grundrechtlich anzuerkennen sein. Insoweit vergleichbar ist die Frage der Grundrechtsberechtigung eines Hausbesetzers aus Art. 13 Abs. 1 GG hinsichtlich des von ihm besetzten Wohnraums: Al-

682 *BVerfGE* 54, 143 (153); 72, 155 (170); 79, 256 (268).
683 *BVerfGE* 35, 202 (220); 79, 256 (268).
684 Insoweit ebenfalls die Eröffnung des Schutzbereichs anzweifelnd *Hoeren*, MMR 2008, 365 (366).

lein die Hausbesetzung kann nicht zu einer Grundrechtsberechtigung führen.[685] Die Strafbarkeit wegen Hausfriedensbruchs gem. § 123 StGB schließe zwar nicht zwingend die Ausbildung einer schützenswerten Privatsphäre aus.[686] Da aber die Rechtswidrigkeit der Besitzbegründung von der Frage der Herausbildung einer Lebenssphäre zu trennen sei, sei hinsichtlich der Grundrechtsberechtigung des Hausbesetzers die wertende Betrachtung des Einzelfalls entscheidend.[687] Für eine Grundrechtsberechtigung spreche dabei die soziale Akzeptanz der rechtswidrigen Inanspruchnahme des Wohnraums. Dem lässt sich aber entgegenhalten, dass eine solche Einbeziehung in den Schutzbereich des Art. 13 Abs. 1 GG die klar erkennbare Duldung des Hauseigentümers i.S.e. bewussten Absehens von Gegenmaßnahmen voraussetzt.[688] Denn eine rechtswidrige Position als Grundrechtsgut zu begreifen, deren Beseitigung unter Umständen Gegenstand der staatlichen Schutzpflicht aus Art. 14 Abs. 1 GG ist, wäre mit der Einheit der Rechtsordnung kaum zu vereinbaren.[689]

Der Eigentümer eines informationstechnischen Systems, das einen körperlichen Gegenstand i.S.d. § 90 BGB darstellt, ist schon aufgrund seiner Eigentumsposition dazu berechtigt mit der ihm gehörenden Sache nach Belieben zu verfahren (vgl. Art. 14 Abs. 1 S. 1 GG, § 903 S. 1 BGB). Sofern er nicht einem Dritten die ausschließliche Nutzung gestattet hat, folgt aus dem Eigentum des Betroffenen zugleich auch die Berechtigung zur Nutzung des informationstechnischen Systems.

Der Betroffene kann ebenso durch eine schuldrechtliche Vereinbarung zur Nutzung berechtigt sein. Als solche kommen vertragliche Gestaltungen in Betracht, die auf den Gebrauch des Vertragsgegenstands ausgelegt sind, etwa die Miete (§ 535 BGB) oder eine Leihe (§ 598 BGB). Erstere würde etwa den Nutzer eines PCs in einem Internetcafé zu einem berechtigten Nutzer i.d.S. machen, sofern man diese Nutzung überhaupt als ausreichend erachtet, die zur Eröffnung des Schutzbereichs des *GVIiS* notwendige besondere Gefährdungslage für die Persönlichkeitsentfaltung zu begründen. Unter diese Kategorie würde dann auch der Arbeitnehmer fallen, dem auf der Grundlage seines Arbeitsvertrags zur Erbringung seiner Arbeitsleistung informationstechnische Systeme zur alleinigen Verwendung überlassen wurden.

Darüber hinaus dürfte auch ein bloßes Gefälligkeitsverhältnis als ausreichend anzusehen sein, den Nutzer des Systems als berechtigt im oben genannten Sinne anzusehen. Die Nutzungsberechtigung wäre somit nicht notwendig schuldrechtlich auszugestalten, sondern kann auch in einem rechtlich unverbindlichen Einverständnis des berechtigten Nutzers oder Eigentümers des Systems bestehen.

---

685 *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 14.
686 *Werwigk*, NJW 1983, 2366 (2367); *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 14.
687 *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 14.
688 *Herdegen*, in: BK GG, Bd. 3, Art. 13 Rn. 38.
689 *Herdegen*, in: BK GG, Bd. 3, Art. 13 Rn. 38.

Die Anerkennung der Vertraulichkeits- und Integritätserwartung setzt aber nur voraus, dass der Nutzer *davon ausgehen darf*, über das informationstechnische System selbstbestimmt zu verfügen. Die Rechtswirksamkeit der Nutzungsberechtigung dürfte damit nicht in jedem Fall Voraussetzung für die Eröffnung des Schutzbereichs sein. Zudem betrifft die Nutzungsberechtigung den Inhalt einer Grundrechtsnorm, der generell nicht von einfachgesetzlichen Normen abhängt. Positive Kenntnis sowie fahrlässige Unkenntnis von der Rechtsunwirksamkeit der Nutzungsberechtigung können jedoch vorbehaltlich einer konkreten Einzelfallbetrachtung der Schutzbereichseröffnung entgegenstehen.

ii. Persönlichkeitsentfaltung des Nutzers

Der Betroffene muss das informationstechnische System gerade zum Zwecke der eigenen Persönlichkeitsentfaltung tatsächlich nutzen. Das System muss ihm als Grundlage der Persönlichkeitsentfaltung in einer Welt allgegenwärtiger Informationstechnik dienen. Die vom *BVerfG* ausgemachte zentrale Bedeutung informationstechnischer Systeme für die Lebensführung vieler Bürger muss sich in der Nutzung des gegenständlichen Systems durch den Betroffenen darstellen.

(1) Tatsächliche Nutzung

Hierzu gehört zunächst die Nutzung des Systems im oben genannten Sinne. Der Betroffene muss das gegenständliche System i.S.d. Entfaltungsmöglichkeiten nutzen, die informationstechnische Systeme für die Persönlichkeit des Einzelnen bieten. Damit kann jedoch nicht ein bestimmtes Nutzungsverhalten oder die Erzeugung eines bestimmten Datenbestands verlangt werden. Der Schutzbereich des *GVIiS* setzt nicht den Nachweis eines tatsächlich vorhandenen besonders umfangreichen und vielfältigen Bestands an personenbezogenen Daten oder den eines bestimmten Nutzungsverhaltens voraus. Ausgangspunkt ist der durch die typische Nutzung angesichts der zahlreichen Funktionen komplexer informationstechnischer Systeme potentiell vorhandene Datenbestand. Diese Vermutung, dass die Verwendung eines vom Schutzbereich des *GVIiS* erfassten informationstechnischen Systems grundsätzlich „personenbezogene Daten in einem Umfang und in einer Vielfalt enthalten können", die „einen Einblick in wesentliche Teile der Lebensgestaltung […] oder gar ein aussagekräftiges Bild der Persönlichkeit […]" enthalten, bedarf aber einer geeigneten Tatsachengrundlage. Ohne die Nutzung des Systems könnte schon von vornherein kein Datenbestand erzeugt werden, der eine solche Profilbildung ermöglicht. Dem System würde somit der Bezug zur Persönlichkeitsentfaltung des Betroffenen fehlen und damit auch die Grundlage

für eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung. Denn das *GVIiS* schützt das informationstechnische System eben nicht um seiner selbst willen, sondern nur insoweit, als dessen Vertraulichkeit und Integrität Persönlichkeitsrelevanz aufweisen.[690]

(2) Selbstbestimmte Verfügung

Diese Tatsachengrundlage setzt weiter voraus, dass das konkrete informationstechnische System als grundsätzlich geeignet anzusehen ist, zur Persönlichkeitsentfaltung des Betroffenen genutzt zu werden. Das *GVIiS* schützt das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben sowie vor einem Zugriff auf das System, durch den dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.[691] Voraussetzung dieses Schutzes ist somit, dass der Nutzer davon ausgehen kann, dass Vertraulichkeit und Integrität des von ihm genutzten informationstechnischen Systems gewährleistet sind. Er muss somit davon ausgehen können, Berechtigter i.S.d. Begriffe der Vertraulichkeit und Integrität zu sein und damit über die Zugänglichkeit der von dem System erzeugten, verarbeiteten und gespeicherten Daten, sowie über die Nutzung von Leistungen, Funktionen und Speicherinhalten des Systems zu entscheiden. Diese Erwartung des Nutzers kann als berechtigt anzusehen sein, soweit Sicherungen rechtlicher, sozialer oder technischer Art gegen den Zugriff Dritter bestehen.[692] Als rechtliche Sicherungen i.d.S. kommen trotz der oben dargestellten Schwierigkeiten der Einordnung in sachenrechtliche Kategorien auch die Abwehransprüche der § 1004 Abs. 1 und §§ 861 Abs. 1, 862 Abs. 1 BGB in Betracht. Unter soziale Sicherungen könnte die Kontrolle des Betroffenen über den körperlichen Zugriff Dritter auf das System gefasst werden. Ein sozialer Selbstschutz wird ebenso wie der technische Selbstschutz ausdrücklich vom *BVerfG* angesprochen.[693] Der Gruppe der technischen Sicherungen unterfielen Zugriffssicherungen vor einer technischen Infiltration, ausdrücklich benannt werden vom *BVerfG* etwa „die Verschlüsselung oder die Verschleierung sensibler Daten".[694]

Jedoch stellt das *BVerfG* auch fest, dass ein wirkungsvoller sozialer und technischer Selbstschutz zumindest den durchschnittlichen Nutzer überfordern könne.[695] Daher dürften die Anforderungen an diese Sicherungen nicht allzu hoch angesetzt werden. Hierfür spricht auch, dass der Schutzbereich des *GVIiS* unabhängig davon eröffnet ist, ob eine technische Infiltration des informationstechni-

690 *Hoffmann-Riem*, JZ 2008, 1009 (1012).
691 *BVerfGE* 120, 274 (314).
692 Insofern anders *Hornung*, CR 2008, 299 (303) (nur technische und rechtliche Kriterien); *Bäcker*, in: *Rensen/ Brink*, Rechtsprechung des Bundesverfassungsgerichts, S. 99 (128) (allein rechtliche Zuordnungen entscheidend).
693 *BVerfGE* 120, 274 (306).
694 *BVerfGE* 120, 274 (306).
695 *BVerfGE* 120, 274 (306).

schen Systems „leicht oder nur mit erheblichem Aufwand“ möglich ist.[696] Die angesprochenen Sicherungen müssen aber so weit reichen, dass der Betroffene überhaupt in der Lage ist, den Zugriff auf das informationstechnische System zu kontrollieren. Sofern dies nicht der Fall ist, nutzt der Betroffene das System nicht als eigenes. Denn dann fehlt es an denjenigen Umständen, aufgrund derer er davon ausgehen kann, über das informationstechnische System selbstbestimmt zu verfügen. So erfasst etwa auch der Schutzbereich des Art. 13 Abs. 1 GG deshalb keine nach außen dringende oder ohne technische Hilfsmittel hörbare Kommunikation, „weil der Betroffene die räumliche Privatsphäre nicht zu seinem Schutz nutzt, wenn er die Wahrnehmbarkeit der Kommunikation von außen selbst ermöglicht“.[697] Nutzt der Betroffene das informationstechnische System, ohne den Zugriff darauf kontrollieren zu können, so erfolgt die fortgesetzte Nutzung in dem Bewusstsein, dass die persönlichkeitsrelevante Nutzung des informationstechnischen Systems nicht vor Einblicken Dritter geschützt ist.[698] Soweit der Betroffene aufgrund solcher Sicherungen davon ausgehen kann, dass er über die Zugänglichkeit der auf dem von ihm genutzten System gespeicherten Daten sowie über die Nutzung von dessen Leistungen, Funktionen und Speicherinhalten entscheidet, darf er den Umständen nach davon ausgehen, dass er über das informationstechnische System selbstbestimmt verfügt. Im Gegensatz zum zivilrechtlichen Begriff der Verfügungsgewalt als die (rechtliche) *Befugnis*, ein bestimmtes Recht unmittelbar zu übertragen, zu ändern oder aufzuheben,[699] beschreibt Verfügungsgewalt hier die *tatsächliche Entscheidungsmacht* über die Zugänglichkeit der von dem System erzeugten, verarbeiteten und gespeicherten Daten, sowie über die Nutzung von Leistungen, Funktionen und Speicherinhalten des Systems: Insoweit ist die Vertraulichkeits- und Integritätserwartung des Nutzers grundrechtlich anzuerkennen.

---

[696] *BVerfGE* 120, 274 (315).

[697] *BVerfGE* 109, 279 (327).

[698] Diesbezüglich ist der Ansicht von *Holznagel/Schumacher* zuzustimmen, das *GVIiS* erfasse nur solche informationstechnischen Systeme, denen der Betroffene personenbezogene Daten anvertraut, mithin in dem Glauben an deren Unzugänglichkeit herausgibt (MMR 2009, 3 (4)). Der von *Holznagel/Schumacher* darüber hinaus gemachten Einschränkung, informationstechnische Systeme würden nur insoweit erfasst, als diese Daten nicht bloß eigenständig sammeln und speichern, ist jedoch nur dahingehend zuzustimmen, dass damit Systeme ausgeschlossen werden, deren gespeicherter Datenbestand nicht auf dem individuellen Nutzungsverhalten des Betroffenen zur oben beschriebenen Persönlichkeitsentfaltung beruht. Denn die angegebene Passage der gegenständlichen Entscheidung, das *RiS* trage 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“ (*BVerfGE* 120, 274 (312f.) (Hervorhebung nur hier)), stellt die bewusste Herausgabe personenbezogener Daten und deren infolge der Nutzung „zwangsläufige Lieferung“ in ein Alternativverhältnis.

[699] Vgl. *Wolf/Wellenhofer*, Sachenrecht, § 7 Rn. 19ff.

e. Ergebnis

Die Nutzung des informationstechnischen Systems „als eigenes“ setzt voraus, dass die Nutzung des Systems so erfolgt, dass die Vertraulichkeits- und Integritätserwartung des Nutzers an das von ihm genutzte System grundrechtlich anzuerkennen ist. Zivilrechtliches Eigentum und Besitz an dem informationstechnischen System können diese Erwartung begründen. Die Begriffe sind jedoch ungeeignet, die persönlichkeitsrechtlichen Zusammenhänge vollständig zu erfassen. Eine schützenswerte Vertraulichkeits- und Integritätserwartung des Nutzers ist anhand des Schutzgegenstands des *GVIiS* zu bestimmen. Neben einer bestehenden Nutzungsberechtigung setzt diese Erwartung voraus, dass der Nutzer aufgrund bestimmter Sicherungen rechtlicher, sozialer oder technischer Art davon ausgehen darf, über den Zugriff auf das System und damit über die Berechtigung i.S.d. Vertraulichkeit und Integrität zu entscheiden.

f. Fernzugriff

Der Schutzbereich des *GVIiS* erfasst bei einem Fernzugriff auf das eigene informationstechnische System auch das System, über das dieser Zugriff erfolgt:

> „*Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.*“[700]

Demnach macht es für die Eröffnung des Schutzbereichs des *GVIiS* keinen Unterschied, ob die technische Infiltration an dem informationstechnischen System des anderen oder desjenigen des Betroffenen erfolgt. Dieser kann einen Zugriff auf das System des anderen als eigene Grundrechtsbeeinträchtigung abwehren. Mit einem solchen Fernzugriff wird das informationstechnische System des anderen aber nicht zugleich zu einem eigenen System des Betroffenen. Die Verfügungsgewalt über das System hat weiterhin der andere inne, der dem Betroffenen den Zugang zu seinem informationstechnischen System gestattet. Bei einem Fernzugriff ist vielmehr insoweit eine Ausnahme vom Erfordernis der Nutzung eines informationstechnischen Systems als eigenes zu machen ist. Denn es fehlt bei dem System des anderen an der Persönlichkeitsrelevanz des Betroffenen. Gleichzeitig führt aber der Fernzugriff dazu, dass durch die Verwendung des informationstechnischen Systems des anderen eine weitere Möglichkeit zur Infiltration des Systems des Betroffenen entsteht.

---

[700] *BVerfGE* 120, 274 (315); der benannte „Fernzugriff“ dürfte sämtliche anderen technischen Gestaltungen als die unmittelbare räumlich Nutzung des informationstechnischen Systems erfassen; „remote“ steht hierbei für „entfernt operierend“ (*Fischer/Hofer*, Lexikon Informatik, Stichwort „remote“)*;* ein „remote Control“ bezeichnet daher die Fernsteuerung eines Systems.

### 2. *Anwendbarkeit auf juristische Personen, Art. 19 Abs. 3 GG*

Die Formulierung des *GVIiS* als Ausprägung des allgemeinen Persönlichkeitsrechts ist nicht von vornherein gleichbedeutend mit einem auf natürliche Personen begrenzten personalen Schutzbereich. Nach Art. 19 Abs. 3 GG gelten die Grundrechte auch für inländische juristische Personen, soweit sie ihrem Wesen nach auf diese anwendbar sind. Damit kommt neben der Grundrechtsberechtigung natürlicher Personen grds. auch die Anwendung des *GVIiS* auf juristische Personen in Betracht.[701]

#### a. Begriff der juristischen Person i.S.d. Art. 19 Abs. 3 GG

Der Begriff der juristischen Person ist dabei nicht mit der einfachgesetzlichen Rechtsfähigkeit gleichzusetzen. Ansonsten würde der Inhalt eines verfassungsrechtlichen Begriffs vom einfachen Recht abhängig gemacht und somit der Gesetzgeber die Grundrechtsträgerschaft bestimmen.[702] Juristische Person i.S.d. Art. 19 Abs. 3 GG sind zunächst alle voll- oder teilrechtsfähigen juristischen Personen des Privatrechts.[703] Ferner werden auch nichtrechtfähige Personenzusammenschlüsse erfasst,[704] nicht aber bloße Organisationen, die nach einfachem Recht in keiner Weise rechtsfähig sind,[705] also bloß schlichte Personenmehrheiten.[706] Ebenso können sich juristische Personen des öffentlichen Rechts grundsätzlich nicht auf die Grundrechte berufen.[707] Der Staat kann nicht gleichzeitig Adressat und Berechtigter der Grundrechte sein.[708]

#### b. Wesensmäßige Anwendbarkeit

Während damit der Begriff der juristischen Person weitgehend geklärt ist, haben sich für denjenigen der „wesensmäßigen Anwendbarkeit" zwei relevante Auslegungen entwickelt.

Die *Durchgriffsthese* oder *Lehre vom personalen Substrat* stellt für die wesensmäßige Anwendbarkeit des Grundrechts auf die hinter einer juristischen Person stehenden natürlichen Personen ab. Danach ist die Einbeziehung der juristischen Perso-

---

[701] Dafür ohne Begründung *Jäger*, JurisPR-ITR 12/2008 Anm. 2, S. 3; offen *Haertel*, NdsVBl. 2008, 276 (279).

[702] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 19 Abs. 3 Rn. 46; *Jarass*/Pieroth, GG, Art. 19 Rn. 20.

[703] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 19 Abs. 3 Rn. 44ff.; *Remmert*, in: *Maunz/Dürig*, GG, Bd. 3, Art. 19 Rn. 38f.

[704] *BVerfGE* 3, 19 (22), 3, 383 (391f.).

[705] *Remmert*, in: *Maunz/Dürig*, GG, Bd. 3, Art. 19 Rn. 41.

[706] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 19 Abs. 3 Rn. 54; *Pieroth/Schlink*, Grundrechte, Rn. 162.

[707] Anerkannt sind Ausnahmen für juristische Personen des öffentlichen Rechts, die hinsichtlich der ihnen von der Rechtsordnung übertragenen Aufgaben unmittelbar einem durch bestimmte Grundrechte geschützten Lebensbereich zugeordnet sind (Universitäten und Fakultäten; Rundfunkanstalten) oder diesem Lebensbereich kraft ihrer Eigenart von vornherein zugehören (Kirchen), *BVerfGE* 61, 82 (102) m.w.N.; auch sind die Verfahrensgrundrechte auf juristische Personen des öffentlichen Rechts anwendbar, *BVerfGE* 18, 441 (447); 21; 362 (373); 61, 82 (104f.).

[708] *BVerfGE* 21, 362 (370).

nen in den Schutzbereich der Grundrechte gerechtfertigt, „*wenn ihre Bildung und Betätigung Ausdruck der freien Entfaltung der natürlichen Personen sind, besonders wenn der ‚Durchgriff' auf die hinter den juristischen Personen stehenden Menschen dies als sinnvoll und erforderlich erscheinen lässt*".[709] Gegen diesen Ansatz spricht jedoch, dass Grundrechtsträger i.S.d. Art. 19 Abs. 3 GG nicht nur die hinter der juristischen Person stehenden natürlichen Personen sind. Art. 19 Abs. 3 GG normiert eine eigene Grundrechtssubjektivität juristischer Personen.[710] Die Grundrechtsberechtigung der hinter der juristischen Person stehenden natürlichen Personen ist aber stets unbestritten.[711] Ferner könne der Grundrechtsfähigkeit einer juristischen Person nicht entgegenstehen, dass sie gar kein personales Substrat, vor allem keine Menschen als Mitglieder hat, so etwa Großkonzerne, private Stiftungen und Aktiengesellschaften, deren Mitglieder Kapitalgesellschaften sind.[712]

Die wesensmäßige Anwendbarkeit der Grundrechte auf juristische Personen sei damit überzeugender durch die flexiblere These vom Erfordernis einer *grundrechtstypischen Gefährdungslage* gegenüber einem Hoheitsträger zu begründen.[713] Diese Gefährdungslage sei dann anzunehmen, wenn sich die betreffende juristische Person hinsichtlich desjenigen Tätigkeitsbereichs, für den sie Grundrechtsschutz beansprucht, gegenüber dem grundrechtsgefährdenden Staat in demselben Verhältnis befindet wie eine natürliche Person.[714] Das *BVerfG* verwendet den Begriff der grundrechtstypischen Gefährdungslage nicht einheitlich. Einmal wird allein auf diese Gefährdungslage abgestellt,[715] in einem anderen Fall orientiert sich das Gericht dann aber wiederum an der *Lehre vom personalen Substrat*, indem eine grundrechtstypische Gefährdungslage nicht vorliege, sofern nicht die individuellen Rechte der hinter der juristischen Peron stehenden natürlichen Personen betroffen sind.[716]

Unabhängig davon, welchem Auslegungsansatz gefolgt wird, kommt eine wesensmäßige Anwendbarkeit der Grundrechte auf juristische Personen allerdings von vornherein dort nicht in Betracht, wo der Grundrechtsschutz an Eigenschaften, Äußerungsformen oder Beziehungen anknüpft, die nur natürlichen Personen wesenseigen sind.[717] Eine solche Anknüpfung wird umso eher vorliegen, als der Grundrechtsschutz im Interesse der Menschenwürde gewährt wird.[718] Da eine

[709] *BVerfGE* 21, 362 (369); 61, 82 (101) („Durchblick"); 68, 193 (205f.); 75, 192 (195f.).
[710] *V. Mutius*, in: BK GG, Bd. 4, Art. 19 Abs. 3 Rn. 34; *Rüfner*, in: HStR V², § 116 Rn. 31; *Isensee*, in: HStR V², § 118 Rn. 5.
[711] *Stern*, Staatsrecht III/1, § 71 I 6, S. 1088.
[712] *Rüfner*, in: HStR V², § 116 Rn. 31; *BVerfGE* 46, 73 (83) und *BVerwGE* 40, 347 (349) bejahen die Grundrechtsfähigkeit von Stiftungen ohne Problematisierung des fehlenden personalen Substrats.
[713] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 19 Abs. 3 Rn. 33.
[714] Vgl. *v. Mutius*, BK GG, Bd. 4, Art. 19 Abs. 3 Rn. 115.
[715] *BVerfGE* 61, 82 (105); 106, 28 (43).
[716] *BVerfGE* 45, 63 (79).
[717] *BVerfGE* 95, 220 (242); 106, 28 (42); 118, 168 (203).
[718] *BVerfGE* 95, 220 (242).

juristische Person jedoch keine Menschenwürde besitzt, scheidet die wesensmäßige Anwendbarkeit eines Grundrechts aus, sofern sich der geltend gemachte grundrechtliche Schutz aus dem Menschenwürdegehalt des Art. 1 Abs. 1 GG ergibt. Für einen grundrechtlichen Schutz auch der juristischen Person spricht demgegenüber die Möglichkeit korporativer Betätigung des jeweiligen Grundrechts.[719] Auf diese Möglichkeit der korporativen Betätigung hat das *BVerfG* etwa bei der Frage der wesensmäßigen Anwendbarkeit des Art. 13 Abs. 1 GG abgestellt. Der historische Ursprung der Unverletzlichkeit der Wohnung als Individualrecht, das dem Einzelnen aufgrund seiner Menschenwürde und seines Interesse an einer freien Entfaltung zukomme, sei demgegenüber nur nachrangig zu berücksichtigen.[720]

c. Anwendbarkeit des allgemeinen Persönlichkeitsrechts auf juristische Personen

Die wesensmäßige Anwendbarkeit des allgemeinen Persönlichkeitsrechts gem. Art. 19 Abs. 3 GG wird nicht uneinheitlich beantwortet. Gegen die Anwendbarkeit wird vorgebracht, dass ihr der Menschenwürdegehalt des allgemeinen Persönlichkeitsrechts entgegenstünde.[721] Diesem Einwand lässt sich aber schon entgegenhalten, dass Art. 19 Abs. 3 GG, wenn man von einem bestimmten Menschenwürdebezug jedes Grundrechts ausgeht, dann fundamental widersprüchlich wäre.[722] Sofern jedoch die dogmatische Grundlage des allgemeinen Persönlichkeitsrechts als subjektives Recht allein in Art. 2 Abs. 1 GG gesehen wird,[723] steht der grundsätzlichen Anwendbarkeit des allgemeinen Persönlichkeitsrechts auf juristische Personen nichts entgegen.[724] Denn der Wortlaut des Art. 19 Abs. 3 GG („soweit") lässt eine wesensmäßige Anwendbarkeit nur von Teilbereichen eines Grundrechts ausdrücklich zu.[725] Allerdings variieren die einzelnen Teilgehalte des allgemeinen Persönlichkeitsrechts in ihrem Menschenwürdebezug.[726] Somit lässt sich seine wesensmäßige Anwendbarkeit auf juristische Personen nicht allgemein beantworten, sondern es ist nach den verschiedenen Ausprägungen zu differenzieren.[727]

Eine wesensmäßige Anwendbarkeit des allgemeinen Persönlichkeitsrechts scheidet daher aus, sofern der beanspruchte grundrechtliche Schutz Gegenstand

---

[719] *BVerfGE* 106, 28 (43); 118, 168 (203).

[720] *BVerfGE* 42, 212 (219) m.w.N.

[721] *Kau*, Funktionsschutz, S. 95ff; *Jarass*, NJW 1989, 857 (860); *Kunig*, JURA 1993, 595 (599); *ders.*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 39.

[722] *Stern*, Staatsrecht III/1, § 71 III 2, S. 1098.

[723] So ausdrücklich *BVerfGE* 56, 37 (41f.); *Schmitt Glaeser*, in: HStR VI², § 129 Rn. 26; *Starck*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 89; vgl. auch *BVerfGE* 35, 202 (219); 82, 236 (269); 90, 263 (270).

[724] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 224; *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 77; *Kube*, in: HStR VII³, § 148 Rn. 75.

[725] *Wilms/Roth*, JuS 2004, 577 (578).

[726] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 19 Abs. 3, Rn. 38.

[727] *BVerfGE* 118, 168 (203).

einer Ausprägung des allgemeinen Persönlichkeitsrechts ist, die vor allem aufgrund der Menschenwürde des Betroffenen besteht.[728] Der Schutz vor dem Zwang zur Selbstbezichtigung als Teil des allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG ist insbesondere aus Gründen der Menschenwürde zu vermeiden und kann damit nicht auf juristische Personen erstreckt werden.[729] Auch der Schutz der Ehe und Familie aus Art. 6 Abs. 1 GG erstreckt sich seinem Wesen nach nur auf natürliche Personen.[730] Personenbezogene Gleichbehandlungsansprüche bestehen zwangsläufig nicht hinsichtlich derjenigen Kriterien, die allein an menschliche Eigenschaften anknüpfen (Geschlecht, Sprache, Abstammung, Rasse, Behinderung), wohl aber hinsichtlich geschützter Verhaltensweisen (Glauben, politische oder religiöse Anschauungen).[731] Das Recht am gesprochenen Wort als Ausprägung des allgemeinen Persönlichkeitsrechts wiederum setzt keinen besonderen personalen Kommunikationsinhalt voraus.[732] Es soll das eigenbestimmte und situationsangemessene Verhalten der Beteiligten in der Kommunikation gesichert werden, so dass insofern auch die durch eine natürliche Person kommunizierende juristische Person sich in einer grundrechtstypischen Gefährdungslage befindet. Der grundrechtliche Schutz des Rechts am gesprochenen Wort ergibt sich daher allein aus Art. 2 Abs. 1 GG.

Daher kommt nur der Schutz durch solche Teilgehalte in Betracht, die nicht wesensmäßig mit natürlichen Personen verbunden sind. Der Schutzbereich des allgemeinen Persönlichkeitsrechts ist daher im Hinblick auf juristische Personen von vornherein auf Art. 2 Abs. 1 GG begrenzt.[733] Das *BVerfG* entnimmt demnach den Schutz juristischer Personen durch das *RiS* allein Art. 2 Abs. 1 GG.[734] Juristische Personen hätten ein natürlichen Personen im Ansatz entsprechendes Bedürfnis nach Schutz vor staatlichen informationellen Maßnahmen.[735] Letztere könnten auch in Bezug auf juristische Personen Gefährdungen oder Verletzungen grundrechtlich geschützter Freiheiten herbeiführen und einschüchternd auf die Ausübung von Grundrechten wirken. Im Unterschied zu natürlichen Personen richte sich dieses Schutzbedürfnis aber nach dem konkreten Tätigkeitskreis juristischer Personen, der regelmäßig durch eine bestimmte Zwecksetzung begrenzt wird. Einer juristischen Person fehlt die „Mehrdimensionalität" menschlicher Persönlichkeit, so dass eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts einer juristischen Person einen bestimmten Geschäfts- oder Betriebsbezug voraussetzt.[736] So besteht etwa eine grundrechtlich erhebliche Gefährdungslage in

[728] *BVerfGE* 118, 168 (203).
[729] *BVerfGE* 95, 220 (242):
[730] *BVerfGE* 13, 290 (297f.).
[731] *Remmert*, in: *Maunz/Dürig*, GG, Bd. 3, Art. 19 Abs. 3 Rn. 101 mit Fn. 3 m.w.N.
[732] *BVerfGE* 106, 28, (43f.):
[733] Vgl. *BVerfGE* 106, 28 (43f.).
[734] *BVerfGE* 118, 168 (203); 128, 1 (43).
[735] *BVerfGE* 118, 168 (203f.).
[736] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 224 (Hervorhebung nur hier).

Bezug auf das *RiS* nicht bereits deshalb, weil von staatlicher Seite Kenntnisse mit Bezug zu einer bestimmten juristischen Person und ihrer Tätigkeit erlangt werden. Die juristische Person muss vielmehr gerade hierdurch einer Gefährdung ihrer spezifischen Freiheitsausübung ausgesetzt werden.[737]

d. Anwendbarkeit des *GVIiS* auf juristische Personen

Somit kommt der Schutz juristischer Personen durch das *GVIiS* von vornherein nur insoweit in Betracht, als sich dessen Schutz allein aus Art. 2 Abs. 1 GG ergibt. Der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme ist jedoch nicht allein natürlichen Personen wesenseigen. Im Rahmen der wesensmäßigen Anwendbarkeit des *RiS* hat das *BVerfG* auch in Bezug auf juristische Personen die Möglichkeit eines Einschüchterungseffekts durch staatliche informationelle Maßnahmen gesehen. Dieser Einschüchterungseffekt könne entstehen, „wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden.“.[738] Das *BVerfG* verweist auch in der gegenständlichen Entscheidung hinsichtlich der Folgen des Zugriffs auf ein informationstechnisches System auf die im *Volkszählungsurteil* beschriebenen Persönlichkeitsgefährdungen.[739] Danach könne das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme beeinflusst werden.[740] Wird aber die gleiche grundrechtliche Gefährdungslage, aufgrund derer juristischen Personen ein Schutzbedürfnis nach dem *RiS* zugesprochen wird, auch für das *GVIiS* angeführt, muss konsequenterweise auch dessen wesensmäßige Anwendbarkeit bejaht werden. Zugleich kommt auch im Schutzbereich des *GVIiS* der Gedanke der Selbstbestimmung in der Verfügung über die Vertraulichkeit und Integrität des eigenen informationstechnischen Systems zum Ausdruck. Dessen besondere technische Sphäre können auch juristische Personen ausbilden. Sie sind dabei ebenso wie bei der Betätigung in einer räumlichen Privatsphäre schutzbedürftig. Nach dem *BVerfG* können sich auch juristische Personen auf Art. 13 Abs. 1 GG berufen, da das Grundrecht auf Unverletzlichkeit der Wohnung mit der berechtigten Inhaberschaft der juristischen Person an einer Wohnung auch korporativ wahrgenommen werden könne.[741] Das Gericht fasst dabei auch Arbeits-, Betriebs- und Geschäftsräume unter den Wohnungsbegriff.[742] Die berechtigte Nutzung eines informationstechnischen Systems ist gleichfalls nicht allein nur natürlichen Personen möglich.

So wie aber die Unterschiede, die zwischen den Schutzbedürfnissen natürlicher und juristischer Personen hinsichtlich des *RiS* bestehen, bei der Reichweite von

[737] *BVerfGE* 118, 168 (204).
[738] *BVerfGE* 113, 29 (46).
[739] *BVerfGE* 120, 274 (305), mit Verweis auf *BVerfGE* 65, 1 (42).
[740] *BVerfGE* 65, 1 (42).
[741] *BVerfGE* 42, 212 (219).
[742] *BVerfGE* 32, 54 (69ff.); 42, 212 (219); 44, 353 (371); 76, 83 (88).

dessen grundrechtlicher Gewährleistung zu berücksichtigen sind,[743] so reichen die Schutzbedürfnisse juristischer Personen hinsichtlich des *GVIiS* weniger weit als diejenigen natürlicher Personen. Informationstechnische Systeme dienen juristischen Personen nicht „in vielfältiger Form als Unterhaltungsgerät",[744] können aber „zur umfassenden Verwaltung und Archivierung der […] geschäftlichen Angelegenheiten"[745] und als „digitale Bibliothek"[746] verwendet werden. Ebenso kommt die Nutzung „zahlreicher neuartiger Kommunikationsdienste"[747] des Internets in Betracht, zwar nicht zum Aufbau und zur aktiven Pflege sozialer Verbindungen, wohl aber zur Verfolgung des spezifischen Zwecks der juristischen Person. Insoweit stellt die selbstbestimmte Nutzung informationstechnischer Systeme eine Grundlage dieser Zweckverfolgung dar. Damit kann aber auch der grundrechtliche Schutzbedarf nur soweit reichen, wie diese Grundbedingung gefährdet ist.

Juristische Personen bedürfen damit insoweit des Schutzes durch das *GVIiS*, als sie zur Verfolgung ihrer bestimmten Zwecksetzung auf die Vertraulichkeit und Integrität der dafür eingesetzten informationstechnischen Systeme angewiesen sind. Sofern es jedoch um den Schutz vor einer Ausspähung eines informationstechnischen Systems geht, kommt insbesondere bei juristischen Personen mit wirtschaftlichem Tätigkeitsfeld eine Spezialität der Art. 12 Abs. 1 und Art. 14 Abs. 1 GG in Betracht. So werden etwa Betriebs- und Geschäftsgeheimnisse allein von den letztgenannten Grundrechten erfasst, da die wirtschaftliche Betätigung betroffen ist, und Betriebs- und Geschäftsgeheimnisse einen durch den Einsatz von Kapital und Arbeit erwirtschafteten Vermögenswert darstellen.[748] Das *GVIiS* greift aber bereits vor einer konkreten Datenerhebung. Der Schutzbereich ist bereits mit Einrichtung der technischen Möglichkeit der Erhebung betroffen. So wie eine natürliche Person aus Furcht vor einer Ausforschung ihrer Personen vom Gebrauch einer grundrechtlich geschützten Freiheit absehen kann, so ist auch eine juristische Person unter Berücksichtigung ihres konkreten Existenzzwecks auf die Vertraulichkeit und Integrität informationstechnischer Systeme angewiesen, um nicht von der grundrechtlich geschützten Verfolgung dieses Zwecks abgehalten zu werden.

Das *GVIiS* erfasst jedoch nur solche informationstechnischen Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten 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".[749]

---

[743] *BVerfGE* 118, 168 (204).
[744] *BVerfGE* 120, 274 (304).
[745] *BVerfGE* 120, 274 (304).
[746] *BVerfGE* 120, 274 (304).
[747] *BVerfGE* 120, 274 (304).
[748] *Breuer*, in: HStR VI², § 148 Rn. 26.
[749] *BVerfGE* 120, 274 (314).

Zwangsläufig kann in Bezug auf eine juristische Person kein Einblick in wesentliche Teile der Lebensgestaltung oder ein aussagekräftiges Bild der Persönlichkeit gewonnen werden. Jedoch besteht auch bei der Infiltration der von einer juristischen Person genutzten informationstechnischen Systeme die Möglichkeit, dass mit dem technischen Zugriff die gesamte Tätigkeit der juristischen Person dem staatlichen Zugriff offensteht und insoweit eine Informationsgewinnung ermöglicht wird, die einem Einblick in wesentliche Teile der Lebensgestaltung oder einem aussagekräftigen Bild der Persönlichkeit einer natürlichen Person gleichsteht. Die Beschränkung des Begriffs der personenbezogenen Daten i.S.d. § 3 Abs. 1 BDSG auf natürliche Personen kann der wesensmäßigen Anwendbarkeit des *GVIiS* auf juristische Personen ebenso wenig entgegenstehen wie derjenigen des *RiS*. Zunächst ergibt sich der Begriff des personenbezogenen Datums erst aus einem grundrechtlichen Schutzbedürfnis, stellt aber nicht den Ausgangspunkt des grundrechtlichen Schutzes der informationellen Selbstbestimmung dar (vgl. § 1 Abs. 1 BDSG). Daneben ergibt sich der persönlichkeitsrechtliche Aspekt des Begriffs des personenbezogenen Datums aus dem Informationsgehalt der „Einzelangabe über persönliche oder sachliche Verhältnisse". Die einfachgesetzliche Nichteinbeziehung juristischer Personen beruht lediglich auf einer auf die Bedürfnisse natürlicher Einzelpersonen zugeschnittenen Regelung, die den grundlegenden Unterschieden in den Existenz- und Funktionsbedingungen natürlicher und juristischer Personen Rechnung trägt.[750] Schließlich steht auch das Erfordernis, dass der Betroffene das informationstechnische System „als eigenes" nutzen müsse, der wesensmäßigen Anwendbarkeit nicht entgegen. Denn so wie hinsichtlich des *Rechts am eigenen Wort* die juristische Person „durch natürliche Personen kommuniziert",[751] kann eine juristische Person durch natürliche Personen eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung aufbauen.

Folglich können sich juristische Personen i.S.d. Art. 19 Abs. 3 GG gegenüber dem grundrechtsgefährdenden Staat in demselben Verhältnis befinden wie eine natürliche Person. Eine grundrechtstypische Gefährdungslage hinsichtlich des *GVIiS* ist nicht von vornherein ausgeschlossen. Wird die wesensmäßige Anwendbarkeit dagegen mittels des Durchgriffs auf die hinter der juristischen Person stehenden Personen begründet, so dürfte aber auch diese Ansicht zur Anwendbarkeit des *GVIiS* kommen. Neuartige Gefährdungen infolge der Nutzung informationstechnischer Systeme bestehen auch bei einer geschäftlichen Nutzung, so dass diese ausdrücklich vom Schutzbereich des *GVIiS* erfasst ist.[752] Auch bei der Nutzung informationstechnischer Systeme für geschäftliche Zwecke lasse sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen.

---

[750] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 17f.
[751] *BVerfGE* 106, 28 (43).
[752] *BVerfGE* 120, 274 (314).

## III. Eingriffe

Einzelne Beispiele eines Eingriffs in den Schutzbereich des *GVIiS* sind bereits in den vorstehenden Ausführungen erwähnt worden. Im Folgenden werden die allgemeinen Voraussetzungen an einen solchen Eingriff beschrieben sowie einzelne von dem *BVerfG* ausdrücklich benannte Eingriffsmodalitäten dargestellt.

Die ungehinderte Persönlichkeitsentfaltung durch die Nutzung informationstechnischer Systeme setzt voraus, dass der Betroffene darauf vertrauen kann, dass das von ihm genutzte informationstechnische System so funktioniert, wie er dies berechtigterweise erwarten darf. Voraussetzung ist hierfür, dass der Betroffene über den Zugriff auf das System und damit über die Berechtigung i.S.v. Vertraulichkeit und Integrität entscheidet. Ein Grundrechtseingriff ist jedes staatliche Handeln, das dem Einzelnen ein vom Schutzbereich eines Grundrechts umfasstes Verhalten ganz oder teilweise unmöglich macht.[753] Ein Eingriff in den Schutzbereich des *GVIiS* liegt somit bei jeder staatlichen Maßnahme vor, welche die beschriebene Verfügungsgewalt beschränkt.[754]

Das *GVIiS* schützt zunächst das Interesse des Nutzers, „dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben".[755] Diese Vertraulichkeit eines informationstechnischen Systems ist dann gewährleistet, wenn keine unautorisierte Informationsgewinnung möglich ist. Da der Betroffene über die Berechtigung entscheidet, stellt ein Grundrechtseingriff hinsichtlich der Vertraulichkeit somit jede staatliche Maßnahme dar, durch die eine vom Betroffenen nicht autorisierte staatliche Informationsgewinnung ermöglicht wird. Daneben schützt das *GVIiS* auch davor, dass die Integrität des informationstechnischen Systems aufgehoben wird, „indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können".[756] Parallel zum Schutzgegenstand der Vertraulichkeit entscheidet der Betroffene auch hinsichtlich der Integrität über die Berechtigung eines Zugriffs. Somit ist die Integrität des informationstechnischen Systems bei jeder staatlichen Maßnahme betroffen, aufgrund derer die Nutzung von Leistungen, Funktionen und Speicherinhalten des informationstechnischen Systems nicht mehr der Kontrolle durch den Betroffenen unterliegt. Da die Vertraulichkeit und Integrität des informationstechnischen Systems nicht tatsächlich vorliegen müssen, sondern der Betroffene von deren Bestehen nur berechtigterweise ausgehen muss, ist ein Eingriff in den Schutzbereich des *GVIiS* nicht schon deshalb abzulehnen, weil das betroffene System bereits erfolgreich infiltriert wurde und daher schon aufgrund des vorangegangen Zugriffs Vertraulichkeit Integrität tatsächlich nicht mehr bestehen.

---

753 *Peine*, in: HGR III, § 57 Rn. 13; *Pieroth/Schlink*, Grundrechte, Rn. 253.

754 *Roßnagel/Schnabel*, NJW 2008, 3534 (3536) sprechen insofern von dem Verlust der Kontrolle des Nutzers über das informationstechnische System.

755 *BVerfGE* 120, 274 (314).

756 *BVerfGE* 120, 274 (314).

Die vom *BVerfG* ausdrücklich benannten Eingriffsmodalitäten lassen sich unter die Begriffe der Datenerhebung und -auswertung und der bereits beim Schutzgegenstand der Integrität angeführten Ausspähung, Überwachung oder Manipulation zusammenfassen. Vorrangig wurde im gegenständlichen Urteil der technische Zugriff auf ein informationstechnisches System betrachtet. Darüber hinaus sind auch alle Folgemaßnahmen, die erst durch diese Infiltration ermöglicht werden, am Schutzbereich des *GVIiS* zu messen. Die Durchführung dieser Maßnahmen bedingt die fortdauernde Aufhebung der Vertraulichkeit und Integrität des informationstechnischen Systems. Solche Folgemaßnahmen lassen sich in ihrer grundrechtlichen Relevanz demnach nicht isoliert bewerten, sondern stets nur unter Berücksichtigung auch der Infiltration. Schon deshalb ist auch die bloße Datenerhebung im Anschluss an die Infiltration am Maßstab des *GVIiS* zu messen.[757] Eingriffe in den Schutzbereich des *GVIiS* sind danach:

> Die „technische Infiltration" des informationstechnischen Systems, die es ermöglicht, „dessen Nutzung zu überwachen oder die Speichermedien durchzusehen oder gar das Zielsystem fernzusteuern";[758]
>
> die Erhebung und anschließende Auswertung von im Arbeitsspeicher und auf den Speichermedien informationstechnischer Systeme enthaltener Daten;[759]
>
> der technische Zugriff, „um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren";[760]
>
> die Überwachung der Nutzung des informationstechnischen Systems als solcher oder die Durchsuchung der Speichermedien des Systems sowie die „Ausspähung des informationstechnischen Systems insgesamt";[761]
>
> die Erfassung des „Verhalten[s] bei der Bedienung eines Personalcomputers für eigene Zwecke, der Abrufhäufigkeit bestimmter Dienste, insbesondere auch des Inhalts angelegter Dateien oder - soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert - […] [des] Verhalten[s] in der eigenen Wohnung";[762]
>
> die umfassende Überwachung des Zielsystems über einen längeren Zeitraum;[763]

[757] I.E. ebenso *Hoffmann-Riem*, JZ 2008, 1009 (1019).
[758] *BVerfGE* 120, 274 (276).
[759] *BVerfGE* 120, 274 (305).
[760] *BVerfGE* 120, 274 (306).
[761] *BVerfGE* 120, 274 (308).
[762] *BVerfGE* 120, 274 (308f.).
[763] *BVerfGE* 120, 274 (324).

> durch den Zugriff selbst verursachte Datenverluste sowie die versehentliche Löschung von Datenbeständen oder das Löschen, Verändern oder Neuanlegen von Datenbeständen durch gezielte Manipulation[764] sowie
>
> die „Vollüberwachung der Nutzung des Zielsystems".[765]

Daneben können aber auch solche Maßnahmen einen Eingriff in den Schutzbereich des *GVIiS* darstellen, die keine Infiltration des informationstechnischen Systems voraussetzen.[766] Hierunter werden ausdrücklich der Einsatz von Hardware-Keyloggern oder die Messung der elektromagnetischen Abstrahlung von Bildschirm und Tastatur als

> „*Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben*",

gefasst.[767] Fraglich ist aber, ob in diesen Fällen stets die Möglichkeit „weitreichender Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung"[768] besteht. Der Schutzgegenstand der Integrität i.S.d. im gegenständlichen Urteil verwendeten Bedeutung ist nur dann betroffen, wenn die einer Ausspähung, Überwachung und Manipulation entgegenstehende technische Hürde mittels der Infiltration des informationstechnischen Systems überwunden wird. Entfällt die Infiltration wie bei der rein passiven Messung elektromagnetischer Abstrahlung der Komponenten, so lassen sich bei der Intensität des Eingriffs diejenigen Gefährdungen, die speziell auf den Vorgang eines technischen Zugriffs zurückzuführen sind, nicht berücksichtigen. Die Intensität des Eingriffs kann sich allein aus der Verletzung der Vertraulichkeit ergeben. Anders aber als bei der Infiltration des Zielsystems, kann eine auf diesem Wege erfolgende staatliche Datenerhebung nur diejenigen Daten zum Gegenstand haben, die durch die elektromagnetische Abstrahlung des jeweiligen Systems erhoben werden können. Der Vollzugriff auf das informationstechnische System ist gerade nicht möglich. Die staatliche Datenerhebung ist auf diejenigen Daten beschränkt, die zum Überwachungszeitpunkt Gegenstand der konkreten Nutzung des Systems durch den Betroffenen sind. Eine Erhebung der im Arbeitsspeicher und auf den Speichermedien des Systems enthaltenen Daten ist demgegenüber ohne Zutun des Nutzers

---

764 *BVerfGE* 120, 274 (325).

765 *BVerfGE* 120, 274 (336).

766 *Hoffmann*, CR 2010, 515 (517), legt schon den Begriff der Infiltration zu eng aus, da er den damit bezeichnete Zugriff auf ein informationstechnisches System allein mit der Installation einer Spähsoftware gleichsetzt; das *BVerfG* fasst unter den Begriff der Infiltration hingegen ausdrücklich auch das bloße Ausnutzen von Sicherheitslücken des Systems, *BVerfGE* 120, 274 (276).

767 *BVerfGE* 120, 274 (315); *Schulz*, DuD 2012, 395 (398), fasst hierunter auch vom Nutzer unbemerkte Datenerhebungen im Rahmen von Social-Media-Angeboten; dagegen spricht, dass es an der technischen Visualisierung von Datenverarbeitungsvorgängen fehlt, wenn vom Nutzer selbst eingegebene Daten bloß gegen dessen Willen von Dritten erhoben werden.

768 *BVerfGE* 120, 274 (305).

nicht möglich. Ähnlich verhält es sich bei der Installation eines Hardware-Keyloggers. Zwar können mit dessen Hilfe sämtliche Tastatureingaben des Betroffenen gespeichert werden. Die staatliche Datenerhebung ist aber auf solche Daten beschränkt, die sich aus den Tastatureingaben des Betroffenen ergeben. Mit der Beschränkung auf die Erfassung der Tastatureingaben wird ebenfalls kein Vollzugriff auf das informationstechnische System ermöglicht. Die Erhebung der mit den vielfältigen Nutzungsmöglichkeiten des informationstechnischen Systems anfallenden Daten ist somit auf die Tastatureingaben des Nutzers beschränkt. Ferner ermöglicht die Installation eines Hardware-Keyloggers die Erfassung der Tastatureingaben nur ab dem Zeitpunkt seiner Installation. Solche Datenerhebungen dürften aber nur dann vom Schutzbereich des *GVIiS* erfasst sein, sofern die konkrete technische Ausgestaltung nicht allein auf „einzelne Datenverarbeitungsmaßnahmen" beschränkt ist. Denn solche Maßnahmen werden ausdrücklich vom Schutzbereich des *RiS* erfasst. Dies müsste dann aber auch für eine Infiltration gelten, die von vornherein auf die Ermöglichung einer bloß punktuellen Datenerhebung begrenzt ist. Denn gerade der nur punktuelle Bezug zu einem bestimmten Lebensbereich ist von dem Schutzbereich des *GVIiS* nicht erfasst. Zudem sieht das *BVerfG* ausdrücklich die Möglichkeit technischer Vorkehrungen zur Beschränkung der Zugänglichkeit von Informationen vor.[769]

Ein Eingriff in den Schutzbereich des *GVIiS* liegt somit in jeder staatlichen Maßnahme, mit der die selbstbestimmte Verfügung des berechtigten Nutzers über sein informationstechnisches System auf technischen Wege beeinträchtigt wird. Hierfür muss nicht auf das System „insgesamt" zugegriffen werden.[770] Soweit das *GVIiS* nach den Urteilsgründen „den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit [bewahrt], als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten", kommt in dieser Beschreibung des Schutzbereichs keine Einschränkung, sondern gerade die lückenfüllende Funktion des allgemeinen Persönlichkeitsrechts zum Ausdruck. Nicht nur vor *konkreten* Kommunikationsvorgängen (Art. 10 Abs. 1 GG) oder Datenerhebungen (*RiS*) ist der Einzelne geschützt, sondern unabhängig hiervon auch vor einem Zugriff auf das informationstechnische System selbst.

## IV. Verfassungsrechtliche Rechtfertigung

In den Normen des VSG NRW 2007, die Gegenstand der Verfassungsbeschwerden waren, denen das vorliegende Leiturteil des *BVerfG* folgte, war die sog. *Online-Durchsuchung* als nachrichtendienstliches Mittel zur Informationsbeschaffung vorgesehen. Das *BVerfG* ging über diesen konkreten Beschwerdegegenstand insoweit

769 So zur *Quellen-TKÜ BVerfGE* 120, 274 (309).
770 So aber Kilian/Heussen/*Polenz*, CHB Kap. 130 Rn. 35.

hinaus, als es generell die Möglichkeit der verfassungsrechtlichen Rechtfertigung eines Eingriffs ansprach. Eingriffe in den Schutzbereich des *GVIiS* können danach sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein.[771]

### *1. Schranken des allgemeinen Persönlichkeitsrechts*

Art. 2 Abs. 1 GG sichert jedem das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. Der zweite Halbsatz des Art. 2 Abs. 1 GG enthält als sog. S*chrankentrias* die Grundrechtsschranken der allgemeinen Handlungsfreiheit.[772] Diese gelten auch für das allgemeine Persönlichkeitsrecht [773] müssen aber wegen dessen Menschenwürdebezugs i.R.d. Verhältnismäßigkeitsprüfung höhere Rechtfertigungsanforderungen erfüllen. Die Schranke der „Rechte anderer" umfasst sämtliche subjektiven Rechtsstellungen.[774] Da die „Rechte anderer" aber durch Normen des objektiven Rechts begründet werden, werden sie bereits von der Schranke der „verfassungsmäßigen Ordnung" erfasst.[775] Insofern kommt den „Rechten anderer" als Schranke des Art. 2 Abs. 1 GG keine eigenständige Bedeutung zu.[776]

Der Begriff der verfassungsmäßigen Ordnung beschreibt die Gesamtheit der Normen, die formell und materiell verfassungsgemäß sind.[777] Von dieser Gesamtheit sind damit Bundes- und Landesgesetze, Rechtsverordnungen und Satzungen erfasst.[778] Diese weite Einschränkbarkeit ist Konsequenz der ebenfalls weiten Bestimmung des Schutzbereichs der allgemeinen Handlungsfreiheit.[779] Da das allgemeine Persönlichkeitsrecht aber einen spezifischen Grundrechtstatbestand darstellt, kann für seine Begrenzung nicht schon die bloße Verfassungsmäßigkeit ausreichend sein.[780]

---

[771] *BVerfGE* 120, 274 (315).

[772] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 37; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 19.

[773] *BVerfGE* 97, 228 (269); 97, 391 (401): 99, 185 (195); 106, 28 (48); 114, 339 (347); 120, 180 (201).

[774] *Lorenz*, in: BK GG, Bd. 1, Art. 2 Abs. 1 Rn. 113; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 20.

[775] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 44; *Dreier*, GG, Bd. 1, Art.2 Rn. 53; *Jarass*/Pieroth, GG, Art. 2 Rn. 18; *Degenhart*, JuS 1990, 161 (164).

[776] *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 19; *Jarass*/Pieroth, GG, Art. 2 Rn. 18.

[777] *BVerfGE* 6, 32 (37f.); 80, 137 (153); 90, 145 (171f.); 96, 10 (21).

[778] *Lorenz*, in: BK GG, Bd. 1, Art. 2 Abs. 1 Rn. 117; *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 54.

[779] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 54; *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 39; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 22; *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 89; *Starck*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 25.

[780] *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 25.

Mit dem Verweis auf das Sittengesetz soll das Handeln des Einzelnen durch gewisse ungeschriebene, für Bestand und Wertorientierung der Gemeinschaft aber unverzichtbare Gebote der Moralität und Sittlichkeit beschränkt sein.[781] Jede Grundrechtsbeschränkung bedarf jedoch einer Konkretisierung durch ein Gesetz, so dass eine solche Konkretisierung der Schranke des Sittengesetzes wiederum bereits von der verfassungsmäßigen Ordnung erfasst wird.[782] Insoweit stellt auch das Sittengesetz keine selbständige, verfassungsunmittelbare Grundrechtsschranke dar.[783] Eigenständige Bedeutung als Grundrechtsschranke der allgemeinen Handlungsfreiheit kommt somit nur noch der verfassungsmäßigen Ordnung zu.[784] Ob für einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts die verfassungsmäßige Ordnung generell nur insoweit taugliche Schranke ist, als eine formell und materiell verfassungsmäßige Rechtsnorm hier nur ein formelles Gesetz sein kann, ist umstritten.[785]

### *2. Besondere Anforderungen an die Eingriffsnorm*

#### a. Formelles Gesetz

Als Ausprägung des allgemeinen Persönlichkeitsrechts sind auf das *GVIiS* gleichfalls die Schranken des Art. 2 Abs. 1 2. Hs. GG anzuwenden. Angesichts des oben beschriebenen Verständnisses der Schranke der verfassungsmäßigen Ordnung kommt zur Rechtfertigung von Eingriffen in den Schutzbereich des *GVIiS* zunächst jede materiell und formell verfassungsmäßige Norm in Betracht. Beschränkungen des *GVIiS* setzen ausdrücklich eine „verfassungsmäßige *gesetzliche* Grundlage" voraus.[786] Offen bleibt jedoch, ob mit der „gesetzlichen" Grundlage ein formelles Bundes- oder Landesgesetz gemeint ist,[787] oder gesetzliche Grundlage i.d.S. auch ein Gesetz im materiellen Sinn sein kann und damit auch hier jede Rechtsnorm ausreicht. Nach der sog. *Wesentlichkeitslehre* bestimmt sich die Notwendigkeit einer formal-gesetzlichen Regelung danach, dass der Gesetzgeber verpflichtet ist, „in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, soweit diese staatlicher Regelung zugänglich ist, alle wesentlichen Entscheidungen selbst zu treffen".[788] Wesentlich i.d.S. ist eine Ent-

---

[781] *Lorenz*, in: BK GG, Bd. 1, Art. 2 Abs. 1 Rn. 135.

[782] *Lorenz*, in: BK GG, Bd. 1, Art. 2 Abs. 1 Rn. 134.

[783] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 60; *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 26; *Starck*, in: *V. Mangoldt/Klein/Starck* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 36.

[784] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs.1 Rn. 39; *Pieroth/Schlink*, Grundrechte, Rn. 407.

[785] Dafür etwa *Lorenz*, in: BK GG, Bd. 1, Art. 2 Abs. 1 Rn. 404; *ders.*, JZ 2005, 1121 (1126); *Kunig*, in: *V. Münch/Kunig* (Hrsg.), GG, Bd. 1, Art. 2 Rn. 42; dagegen etwa *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 107; *BVerfGE* 65, 1 (44) setzt für Beschränkungen des *RiS* eine „gesetzliche Grundlage" voraus, *BVerfGE* 92, 191 (197) verlangt hierfür ausdrücklich ein „Gesetz".

[786] *BVerfGE* 120, 274 (315) (Hervorhebung nur hier).

[787] Dafür - hinsichtlich der identischen Formulierung im *Volkszählungsurteil* (*BVerfGE* 65, 1 (44)) - *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 30.

[788] *BVerfGE* 49, 89 (126); 61, 260 (275); 88, 103 (116).

scheidung dann, wenn sie „wesentlich für die Verwirklichung der Grundrechte" ist.[789] Auch sei bei der Frage nach der Wesentlichkeit der Entscheidung die Intensität der Einwirkung zu berücksichtigen.[790] Demgegenüber existiere im Grundgesetz jedoch weder ein Totalvorbehalt des Gesetzes noch eine Kompetenzregel des Inhalts, dass alle „objektiv wesentlichen" Entscheidungen vom Gesetzgeber zu treffen seien.[791]

Für die Notwendigkeit der Regelung von Beschränkungen des *GVIiS* in einem formellen Gesetz spricht die vom *BVerfG* an verschiedenen Stellen im gegenständlichen Urteil hervorgehobene besondere grundrechtliche Relevanz der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung des Einzelnen. Das Gericht beschreibt zunächst die *Allgegenwärtigkeit* und die *zentrale* Bedeutung informationstechnischer Systeme für die Lebensführung vieler Bürger.[792] Dementsprechend könne der Zugriff auf ein solches System „*weitreichende* Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen".[793] Das grundrechtlich *erhebliche* Schutzbedürfnis des Einzelnen ist auf den Schutz vor einem Zugriff gerichtet, der es ermöglichen kann, „einen Einblick in *wesentliche* Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[794] Der heimliche Zugriff auf informationstechnische Systeme stelle einen besonders intensiven Grundrechtseingriff dar.[795] Schon bei einem einmaligen und punktuellen Zugriff weise eine staatliche Datenerhebung ein beträchtliches Potential für die Ausforschung der Persönlichkeit auf.[796] Es bestehe das naheliegende Risiko der Ermöglichung „weitreichender Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen"[797] Die Datenerhebung sei von besonderer Schwere, wenn durch die technische Infiltration eine längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht werden.[798] Denn die so zu erhebenden flüchtigen oder temporär gespeicherten Daten wiesen eine besondere Relevanz für die Persönlichkeit des Betroffenen auf, da zum Einen ihre Auswertung mittelbar Schlüsse über Vorlieben oder Kommunikationsgewohnheiten zulässt, und daneben Passwörter Zugang zu technisch gesicherten Inhalten ermöglichen.[799] Besonderes Gewicht komme ferner der Vereitelung informationellen Selbstschutzes durch die technische Infiltration zu, die darauf angelegt und dazu geeignet sei, den Einsatz

[789] *BVerfGE* 47, 46 (79); 98, 218 (251); 105, 279 (305).
[790] *BVerfGE* 49, 89 (127); 58, 257 (274); 98, 218 (252).
[791] *BVerfGE* 68, 1 (109).
[792] *BVerfGE* 120, 274 (303) (Hervorhebung nur hier).
[793] *BVerfGE* 120, 274 (305) (Hervorhebung nur hier).
[794] *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).
[795] *BVerfGE* 120, 274 (322, 332).
[796] *BVerfGE* 120, 274 (322).
[797] *BVerfGE* 120, 274 (323).
[798] *BVerfGE* 120, 274 (323).
[799] *BVerfGE* 120, 274 (324).

von Verschlüsselungstechnologien zu umgehen.[800] Die Heimlichkeit der Maßnahme bedürfe besonderer Rechtfertigung.[801] Das Gewicht eines Eingriffs in den Schutzbereich des *GVIiS* werde noch durch die Gefahren für die Integrität des zu infiltrierenden informationstechnischen Systems bestimmt.[802] Schließlich bestehe noch die Gefahr der Erhebung von Daten, die dem absolut geschützten Kernbereich privater Lebensgestaltung zuzuordnen sind.[803] Aufgrund der Heimlichkeit des Zugriffs liege ein vollständiger Kontrollverlust des Betroffenen darüber vor, ob die ermittelnde staatliche Stelle den Kernbereich privater Lebensgestaltung achtet.[804]

Mit zunehmender Verbreitung der Informationstechnik verlagert sich auch die Persönlichkeitsentfaltung des Einzelnen auf die sich aus dieser Verbreitung ergebenden Entfaltungsmöglichkeiten. Infolgedessen bildet die Nutzung informationstechnischer Systeme einen zentralen Bestandteil der Persönlichkeitsentfaltung, so dass der Vertraulichkeit und Integrität des von dem Betroffenen genutzten informationstechnischen Systems in dieser Hinsicht ein entsprechend hoher Stellenwert zukommt. Der Einzelne kann seine Persönlichkeit jedoch nur dann ungehindert entfalten, wenn seine berechtigte Erwartung des Bestehens von Vertraulichkeit und Integrität vom Staat geachtet wird. Angesichts der Allgegenwärtigkeit und zentralen Bedeutung informationstechnischer Systeme ist mit der Frage nach der Vertraulichkeit und Integrität ein umfangreicher Teil der Persönlichkeitsentfaltung betroffen. Die Achtung der Vertraulichkeits- und Integritätserwartung ist damit wesentlich für die grundrechtlich geschützte Persönlichkeitsentfaltung. Jedenfalls hinsichtlich eines Eingriffs in Form der technischen Infiltration auf informationstechnische Systeme besteht die Aussicht, einen potentiell besonders vielfältigen und umfangreichen Datenbestand zu erheben, so dass der Betroffene der umfangreichen Ausspähung durch die Ermittlungsbehörde preisgegeben wird.[805] Diese Aussicht besteht abhängig von ihrer technischen Ausgestaltung auch bei „Datenerhebung mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben". Die damit verbundenen Möglichkeiten einer staatlichen Einsicht- und Einflussnahme können die ungehinderte Persönlichkeitsentfaltung mittels der Nutzung informationstechnischer Systeme schon durch den psychischen Druck staatlicher Anteilnahme verhindern. Die Intensität eines Eingriffs in den Schutzbereich des *GVIiS* wird noch besonders dadurch geprägt, dass Datenerhebungsmaßnahmen, welche die Nutzung eines informationstechnischen Systems zum Gegenstand haben, auf eine heimliche Ausführung ausgelegt sind, da sich nur bei der heimlichen Durchführung die

[800] *BVerfGE* 120, 274 (324).
[801] *BVerfGE* 120, 274 (325).
[802] *BVerfGE* 120, 274 (325).
[803] *BVerfGE* 120, 274 (335f.).
[804] *BVerfGE* 120, 274 (336).
[805] *BVerfGE* 120, 274 (328).

gerade mit solchen Maßnahmen verbundenen ermittlungstaktischen Vorteile ergeben.

Zwar ist das *GVIiS* nicht schrankenlos gewährleistet, jedoch sind angesichts der Bedeutung, die ein Eingriff in den Schutzbereich des *GVIiS* für die Persönlichkeitsentfaltung des Betroffenen hat, umfangreiche Überlegungen hinsichtlich des Ausgleichs grundrechtlich geschützter Freiheit des Einzelnen und des mit einer Maßnahme verfolgten Zwecks notwendig. Diesen Ausgleich hat vorrangig der demokratisch legitimierte Gesetzgeber herzustellen. Denn inwieweit der Verfolgung des Eingriffszwecks der Vorrang eingeräumt wird, bestimmt unmittelbar die verbleibende Reichweite grundrechtlicher Freiheit und stellt damit eine für die Grundrechtsausübung wesentliche Entscheidung dar. Eine diesbezügliche Ermächtigung dürfte damit ein förmliches Bundes- oder Landesgesetz erfordern.

b. Verhältnismäßigkeitsgrundsatz

Die Entscheidung des *BVerfG* betraf die Frage nach der Verfassungsmäßigkeit einer ganz bestimmten Eingriffsnorm, so dass die in der gegenständlichen Entscheidung enthaltenen Ausführungen nur insoweit zur Schrankenbildung des *GVIiS* herangezogen werden können, als bestimmte Rechtfertigungsvoraussetzungen sich nicht auf den konkreten Eingriffszweck und den konkreten Eingriff des heimlichen technischen Zugriffs auf informationstechnische Systeme beschränken, sondern diese Voraussetzungen darüber hinaus allgemein für Eingriffe in den Schutzbereich des *GVIiS* aufgestellt werden.

i. Legitimer Zweck, Geeignetheit und Erforderlichkeit

Eingriffe in den Schutzbereich des *GVIiS* können sowohl zu präventiven Zwecken als auch solchen der Strafverfolgung verfassungsgemäß sein.[806] Die technische Infiltration eines informationstechnischen Systems verfolge einen legitimen Zweck, sofern die Eingriffsnorm darauf abzielt, Gefahren durch terroristische oder andere Bestrebungen für die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und der von ihm zu gewährleistenden Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit zu begegnen.[807] Bei der Wahrnehmung dieser Aufgaben sind die Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und die Möglichkeiten zur Verschlüsselung und Verschleierung von Daten zu berücksichtigen.[808] Unter Berücksichtigung des Einschätzungsspielraums des Gesetzgebers sei die heimliche technische Infiltration als geeignet anzusehen, diesem Zweck zu dienen.[809] Diese Eignung setzt nicht voraus, dass eine technische Infiltration stets oder auch nur im Regelfall Erfolg verspricht. Da nicht als selbstverständlich unterstellt werden

[806] *BVerfGE* 120, 274 (315).
[807] *BVerfGE* 120, 274 (319).
[808] *BVerfGE* 120, 274 (320).
[809] *BVerfGE* 120, 274 (320).

könne, dass jede Zielperson technische Selbstschutzmaßnahmen zur wirkungsvollen Verhinderung eines solchen Zugriffs nutzt und tatsächlich fehlerfrei implementiert, sei die gesetzgeberische Prognose einer erfolgreichen technischen Infiltration zumindest nicht offensichtlich fehlerhaft.

Hinsichtlich der *präventiven* Zielsetzung stehe der Geeignetheit auch nicht der möglicherweise begrenzte Beweiswert aufgrund fehlender Erfüllung forensischer Ansprüche[810] der durch die Infiltration des informationstechnischen Systems erlangten Daten entgegen.[811] Denn um den Verfassungsschutzbehörden Kenntnisse zu verschaffen genüge insoweit schon, dass den Daten überhaupt ein Informationswert zukommt.[812] Die Zweifel an der Erfüllung forensischer Maßstäbe einer Datengewinnung durch den Zugriff auf informationstechnische Systeme könnten der Geeignetheit dieser Ermittlungsmethode zu Strafverfolgungszwecken nur insofern entgegenstehen, als es auf die Gewinnung revisionsfester Beweise in einem Strafverfahren ankommt.[813] Die Infiltration eines informationstechnischen Systems wird hingegen nicht von der Rechtfertigungsmöglichkeit zu Strafverfolgungszwecken ausgenommen. Sofern es um den bloßen Informationswert der zu gewinnenden Daten geht, dürfte die u.U. nicht vorhandene Erfüllung forensischer Maßstäbe angesichts der ausdrücklichen Einbeziehung der Strafverfolgung in die einen Eingriff in den Schutzbereich des *GVIiS* legitimierenden Zwecke der Geeignetheit nicht generell entgegenstehen.[814]

Von der Einschätzungsprärogative des Gesetzgebers sei ferner die Einschätzung erfasst, dass keine den Betroffenen weniger belastende aber ebenso wirksame Maßnahme gegeben sei, die auf informationstechnischen Systemen vorhandenen Daten zu erheben, als durch eine technische Infiltration, so dass auch der Grundsatz der Erforderlichkeit nicht verletzt werde.[815] Denn nur hierdurch werde die umfassende Sichtung der abgelegten Dateien inklusive verschlüsselter Daten, die Verfolgung von Änderungen über einen längeren Zeitraum, die umfassende Überwachung des informationstechnischen Systems oder auch der Zugriff auf verschlüsselte Inhalte der Internetkommunikation ermöglicht.

ii. Angemessenheit

Das Gebot der Angemessenheit setzt voraus, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf.[816] Die in der gegenständlichen Entscheidung für die

[810] So etwa *Hansen/Pfitzmann*, DRiZ 2007, 225 (228); *dies.*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 131 (135); *Freiling*, Stellungnahme (Fn. 553), S. 6; zweifelnd auch *Fox*, DuD 2007, 827 (832); *Gercke*, CR 2007, 245 (247); *Sieber*, Stellungnahme (Fn. 287), S. 17.

[811] *BVerfGE* 120, 274 (320f.).

[812] *BVerfGE* 120, 274 (321).

[813] Vgl. *BVerfGE* 120, 274 (321).

[814] Dafür *Weiß*, Online-Durchsuchungen, S. 244.

[815] *BVerfGE* 120, 274 (321).

[816] *BVerfGE* 90, 145 (173); 113, 348 (382); 120, 274 (321f.).

Schwere des Eingriffs in diese Abwägung eingebrachten grundrechtlichen Schutzgegenstände, der Umfang und die Schwere ihrer Beeinträchtigung sowie sonstige Interessen und Schutzgüter, sind somit unabhängig von dem mit der Infiltration eines informationstechnischen Systems verfolgten Zweck zu berücksichtigen. Sie sind damit stets in die Prüfung der Angemessenheit einer Eingriffsnorm einzubringen, die den Zugriff auf informationstechnische Systeme vorsieht.

Zu berücksichtigen ist demnach zunächst das beträchtliche Potential einer staatlichen Datenerhebung aus komplexen informationstechnischen Systemen für die Ausforschung der Persönlichkeit des Betroffenen. Der heimliche Zugriff auf ein informationstechnisches System verschaffe der staatlichen Stelle angesichts der Vielzahl unterschiedlicher Nutzungsmöglichkeiten komplexer Systeme Zugang zu einem herkömmliche Informationsquellen an Umfang und Vielfältigkeit potentiell bei weitem übertreffenden Datenbestand.[817] Zu beachten seien dabei die gegenwärtigen Nutzungsgepflogenheiten, komplexe informationstechnische Systeme bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität zu nutzen.[818] Hinsichtlich der Erhebung von Daten in Bezug zur Kommunikation des Betroffenen mit Dritten sei die mittelbare Beeinträchtigung der Freiheit der Bürger durch die mögliche Verhinderung einer unbefangenen Individualkommunikation aufgrund der Furcht vor einer Überwachung zu bedenken. Zudem würden von dieser Datenerhebung notwendigerweise die Kommunikationspartner des Betroffenen erfasst, ohne dass ihnen gegenüber das Vorliegen der Voraussetzungen für eine solche Erhebung geprüft würde.[819]

In die Abwägung einzubeziehen ist ferner das besondere Gewicht einer technischen Infiltration informationstechnischer Systeme, die eine längerfristige Überwachung der Nutzung und die laufende Erfassung entsprechender Daten ermöglicht.[820] Denn Umfang und Vielfältigkeit des so zu erlangenden Datenbestands seien gegenüber einer einmaligen und punktuellen Datenerhebung erheblich größer, da auch lediglich im Arbeitsspeicher vorhandene flüchtige oder temporär auf den Speichermedien des Zielsystems enthaltene Daten zugänglich sind.[821] So könnten Vorlieben oder Kommunikationsgewohnheiten des Betroffenen ebenso wie Passwörter erfasst werden. Das Gewicht des Grundrechtseingriffs werde weiter durch das Unterlaufen von Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff erhöht.[822]

Zu berücksichtigen sei weiter die Heimlichkeit der Maßnahme. Denn die Heimlichkeit staatlicher Maßnahmen stelle in einem Rechtsstaat einen Ausnahmefall dar und bedarf besonderer Rechtfertigung, da Möglichkeiten der Einflussnahme des Betroffenen in Form der Interessenwahrnehmung vor der Durchfüh-

[817] *BVerfGE* 120, 274 (322).
[818] *BVerfGE* 120, 274 (322f.).
[819] *BVerfGE* 120, 274 (323).
[820] *BVerfGE* 120, 274 (323).
[821] *BVerfGE* 120, 274 (324).
[822] *BVerfGE* 120, 274 (324).

rung der Maßnahme, nämlich gerichtlicher Rechtsschutz sowie die faktische Einflussnahme auf die staatliche Maßnahme, ausgeschlossen würden.[823]

Hinzu komme die Gefahr eines Datenverlusts durch den Zugriff oder diejenige, dass Datenbestände versehentlich oder durch gezielte Manipulation gelöscht, verändert oder neu angelegt werden.[824] Zudem könnte die zur technischen Infiltration eingesetzte Software an Dritte weitergeleitet werden.[825] Schließlich sei noch der Zielkonflikt zu berücksichtigen, Sicherheitslücken zu schließen oder wegen ihrer Notwendigkeit zur Infiltration passiv oder aktiv gegen ihre Entdeckung zu arbeiten, wodurch das Vertrauen der Bevölkerung in das Bemühen des Staates um eine möglichst hohe Sicherheit der Informationstechnologie beeinträchtigt werden könnte.[826]

(1) Tatbestand der Eingriffsnorm

Angesichts der somit bestehenden Eingriffsintensität ist die heimliche technische Infiltration informationstechnischer Systeme zu den oben genannten präventiven Zwecken nur dann angemessen, wenn „bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt“ und daneben der Grundrechtsschutz des Betroffenen durch geeignete Verfahrensvorkehrungen gesichert wird.[827] Diese verfassungsrechtlichen Anforderungen an die Regelung des tatsächlichen Eingriffsanlasses gelten für alle Ermächtigungen zu einem heimlichen Zugriff auf informationstechnische Systeme zu präventiven Zwecken.[828] Eine behördenbezogene Differenzierung, etwa zwischen Polizei- und Verfassungsschutzbehörden, erfolgt nicht, da das Risiko einer weitgehenden staatlichen Ausspähung der Persönlichkeit des Betroffenen unabhängig von der handelnden Behörde besteht.

Überragend wichtige Rechtsgüter sind Leib, Leben und Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.[829] Hierzu ist auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen zu zählen. Das Erfordernis der konkreten Gefahr bezeichnet eine „Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein

[823] *BVerfGE* 120, 274 (325).
[824] *BVerfGE* 120, 274 (325).
[825] *BVerfGE* 120, 274 (326).
[826] *BVerfGE* 120, 274 (326).
[827] *BVerfGE* 120, 274 (326).
[828] *BVerfGE* 120, 274 (329).
[829] *BVerfGE* 120, 274 (328).

Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird".[830] Die Prognose dieser Gefahr muss von der Feststellung bestimmter Tatsachen getragen werden.

(2) Verfahrensrechtliche Anforderungen

Zur verfahrensrechtlichen Absicherung der Interessen des Betroffenen muss die Ermächtigung zu einem heimlichen technischen Zugriff auf informationstechnische Systeme insbesondere den grundsätzlichen Vorbehalt richterlicher Anordnung enthalten.[831] Eine andere Stelle darf zur vorbeugenden Kontrolle einer geplanten Ermittlungsmaßnahme nur bei gleicher Gewähr für Unabhängigkeit und Neutralität eingesetzt werden.[832] Ausnahmen von dem Erfordernis der vorherigen Kontrolle der Maßnahme können für Eilfälle vorgesehen werden, soweit die Überprüfung durch eine neutrale Stelle im Anschluss an die Infiltration erfolgt.[833]

(3) Kernbereichsschutz

Eine gesetzliche Grundlage zur Einschränkung des *GVIiS* ist nur dann verfassungsmäßig, wenn diese hinreichende Vorkehrungen enthält, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden. Heimliche Überwachungsmaßnahmen staatlicher Stellen haben einen durch Art. 1 Abs. 1 GG geschützten unantastbaren Kernbereich privater Lebensgestaltung zu bewahren,[834] in den selbst aufgrund überwiegender Interessen der Allgemeinheit nicht eingegriffen werden kann.[835] Der Einzelne soll so die Möglichkeit haben, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst einer hierauf bezogenen staatlichen Überwachung zum Ausdruck zu bringen.[836] Von diesem absoluten Schutz können die auf einem informationstechnischen System gespeicherte tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente sowie Inhalte von E-Mails oder anderer Kommunikationsdienste des Internets erfasst sein.[837] Besteht die Möglichkeit, dass eine Überwachungsmaßnahe den Kernbereich privater Lebensgestaltung berührt, hat die gesetzliche Ermächtigung so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden.[838] Sofern die Bewertung des Kernbereichsbezugs der betroffenen Informationen vor

[830] *BVerfGE* 120, 274 (328).
[831] *BVerfGE* 120, 274 (331); dafür auch schon *Kemper* ZRP 2007, 105 (109) und *Schlegel*, GA 2007, 649 (660).
[832] *BVerfGE* 120, 274 (332).
[833] *BVerfGE* 120, 274 (333).
[834] *BVerfGE* 109, 279 (313); 113, 348 (391); 120, 274 (335); siehe auch *BVerfGE* 6, 32 (41); 27, 1 (6); 32, 373 (378f.); 34, 238 (245); 80, 367 (373f.).
[835] *BVerfGE* 34, 238 (245); 109, 279 (313); 120, 274 (335).
[836] *BVerfGE* 109, 279 (313); 120, 274 (335).
[837] *BVerfGE* 120, 274 (335f.).
[838] *BVerfGE* 120, 274 (337).

der Kenntnisnahme praktisch nicht möglich ist, setzt hinreichender Schutz in der Auswertungsphase der erhobenen Daten voraus, dass kernbereichsbezogene Daten unverzüglich gelöscht werden und ihre Verwertung ausgeschlossen wird.[839]

Aus den Schwierigkeiten bei der Infiltration informationstechnischer Systeme, die Kernbereichsrelevanz der überwachten Vorgänge nicht stets vor oder bei der Datenerhebung abschätzen zu können – sei es bei Einsatz technischer Such- und Ausschlussmechanismen oder durch eine natürliche Person – folge nach Ansicht des *BVerfG* keine verfassungsrechtliche Notwendigkeit, die technische Infiltration wegen des Risikos einer Kernbereichsverletzung bei der Datenerhebung von vornherein zu unterlassen.[840] Der Schutz des absoluten Kernbereichs privater Lebensgestaltung lasse sich auch bei der Infiltration informationstechnischer Systeme im Rahmen eines zweistufigen Schutzkonzeptes gewährleisten.[841] Danach müsse die Erhebung kernbereichsrelevanter Daten soweit wie informations- und ermittlungstechnisch möglich unterbleiben und es sind im Falle einer Erhebung kernbereichsrelevanter Daten diese Daten unverzüglich zu löschen und ihre Weitergabe und Verwertung auszuschließen.[842] Das bloße Risiko der Verletzung des absolut geschützten Kernbereichs privater Lebensgestaltung erfordere angesichts tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut nicht, die Infiltration des informationstechnischen Systems von vornherein zu unterlassen.[843] Eine Datenerhebung hat nur dann grds. zu unterbleiben, wenn im Einzelfall konkrete Anhaltspunkte dafür vorliegen, dass der Kernbereich privater Lebensgestaltung berührt wird.[844]

*Absolut* ist der Kernbereichsschutz damit aber erst auf sekundärer Ebene.[845] Die Ansicht des *BVerfG* berücksichtigt die Besonderheiten der Nutzung informationstechnischer Systeme zur Persönlichkeitsentfaltung jedoch nicht in ausreichendem Maße. Das Gericht selbst stellt ausdrücklich fest, dass informationstechnische Systeme nach den gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität genutzt werden.[846] Naheliegend ist somit, dass die Infiltration eines informationstechnischen Systems nicht nur vereinzelt mit dem Risiko der Erhebung kernbereichsrelevanter Daten verbunden ist, sondern dass die Verletzung des Kernbe-

[839] *BVerfGE* 109, 279 (318f.); 113, 348 (391f.); 120, 274 (337).
[840] *BVerfGE* 120, 274 (338).
[841] *BVerfGE* 120, 274 (338).
[842] Vgl. *BVerfGE* 109, 279 (318f.); 113, 348 (391f.); 120, 274 (338f.); zur Kritik an diesem Schutzkonzept siehe die abweichende Meinung der Richterinnen *Jaeger* und *Hohmann-Dennhardt*, *BVerfGE* 109, 279 (382ff.).
[843] *BVerfGE* 120, 274 (338).
[844] *BVerfGE* 109, 279 (318); 113, 348 (391f.); 120, 274 (338).
[845] *Murswiek*, in: *Sachs* (Hrsg.), GG, Art. 2 Rn. 106.
[846] *BVerfGE* 120, 274 (322f.).

reichs privater Lebensgestaltung der Regelfall sein wird.[847] Eine staatliche Überwachungsmaßnahme muss aber schon dann unterbleiben, wenn nach der Lebenserfahrung typischerweise mit einem Eingriff der Maßnahme in den Kernbereich zu rechnen ist.[848] So spricht etwa im Bereich der akustischen Wohnraumüberwachung im Interesse der Effektivität des Schutzes der Menschenwürde die Vermutung dafür, dass Gespräche des Einzelnen mit seinen engsten Vertrauten in seiner Wohnung zum absolut geschützten Kernbereich privater Lebensgestaltung gehören.[849] Wenn aber auch für die Infiltration eines informationstechnischen Systems konkrete Anhaltspunkte dafür verlangt werden, dass eine Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so werden damit die tatsächlichen Nutzungsgewohnheiten informationstechnischer Systeme ignoriert, angesichts derer in gleicher Weise wie bei der akustischen Wohnraumüberwachung von einer tatsächlichen Vermutung für das Vorhandensein von kernbereichsrelevanten Daten auszugehen sein müsste. Der Kernbereich privater Lebensgestaltung wäre demnach gerade *nicht unerwartet* betroffen.

Die vom *BVerfG* ausdrücklich festgestellte bewusste Verwendung informationstechnischer Systeme auch zum Speichern sensibler Daten und die damit verbundene naheliegende Erhebung von Daten mit Bezug zum absolut geschützten Kernbereich privater Lebensgestaltung sprechen mithin dafür, bei der Infiltration eines informationstechnischen Systems verstärkten Wert auf die Zuverlässigkeit technischer oder auch personeller Such- und Ausschlussmechanismen zu legen. Deren fehlende Zuverlässigkeit darf aber gerade nicht als Argument für die Notwendigkeit der Realisierung des Kernbereichsschutzes bloß auf Auswertungsebene herangezogen werden.[850] Der Schutz des Kernbereichs privater Lebensgestaltung erst bei der Durchsicht erhobener Daten ist stets mit dem Problem verbunden, dass einmal gesichtete Daten in Erinnerung der jeweiligen Ermittlungsperson bleiben.[851] Die Vermeidung einer Erhebung kernbereichsrelevanter Daten unter dem Vorbehalt des informations- und ermittlungstechnisch Möglichen trägt zwar den Ermittlungsinteressen des Staates Rechnung, läuft aber Gefahr, dass der Kernbereichsschutz auf Erhebungsebene überhaupt nicht mehr zum Tragen kommt, weil er technisch nicht realisiert werden kann. Insofern wird der Kernbereichsschutz mit der nachträglichen Sicherstellung, dass die Intensität der Kernbe-

847 A.A. insofern *Bär*, MMR 2007, 237 (242), wonach auf einem PC nur in den seltensten Fällen tatsächlich dem Kernbereich privater Lebensgestaltung zuzuordnende Inhalte gespeichert würden.

848 *Hörnig*, JURA 2009, 207 (212).

849 *BVerfGE* 109, 279 (320).

850 *Baldus*, JZ 2008, 218 (226), rechtfertigt die Infiltration informationstechnischer Systeme trotz fehlender Differenzierungs- und Selektionsmöglichkeiten bei der Datenerhebung mit dem Verständnis eines abwägungsoffenen Kernbereichskonzepts, wonach die Wahrscheinlichkeit der Erhebung kernbereichsrelevanter Daten mit dem Schutz höchstpersönlicher Formen der Freiheitsentfaltung hinter dem höher zu bewertenden Schutz von Individual- und Kollektivgütern zurücktreten müsse.

851 *Petri*, DuD 2008, 443 (447).

reichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben, auf ein Optimierungsgebot reduziert.[852]

Fraglich ist, inwiefern dieses Optimierungsgebot mit der vom *BVerfG* selbst aufgestellten Vorgabe zu vereinbaren ist, dass nicht in den absoluten Kernbereich privater Lebensgestaltung eingegriffen werden darf, um erst den Kernbereichsbezug der Informationserhebung festzustellen.[853] Wird trotz des Fehlens zuverlässiger technischer und personeller Such- und Ausschlussmechanismen die Infiltration informationstechnischer Systeme zugelassen, so wird akzeptiert, dass eine zuverlässige Feststellung des Kernbereichsbezugs erst in der Auswertungsphase erfolgt. Der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung wird damit nicht mehr durch das Unterbleiben oder den Abbruch der Überwachung im Vorfeld einer Überwachungsmaßnahme gewährleistet, sondern bloß noch durch die nachträgliche Filterung der erhobenen Daten auf ihren Kernbereichsbezug.[854] Etwas anderes muss jedoch für die ausdrücklich vom Schutzbereich des *GVIiS* erfasste Nutzung des informationstechnischen Systems für geschäftliche Zwecke gelten. Typischerweise dürften bei der ausschließlich geschäftlichen Nutzung auch die enthaltenen Daten geschäftlichen Inhalts sein und damit nicht zum Kernbereich privater Lebensgestaltung zu rechnen sein[855]. Fraglich ist daher, ob in dieser Rechtsprechung eine nachhaltige Bekräftigung und damit weitere Stärkung des Kernbereichsschutzes und mit diesem des Schutzes der menschlichen Würde als unantastbares Schutzgut gesehen werden kann.[856] Vielmehr wäre verfassungsrechtlich konsequent gewesen, unter Berücksichtigung gerade der Unantastbarkeit des Kernbereichsschutzes solche Überwachungsmaßnahmen als für mit dem Grundgesetz schlechthin unvereinbar zu betrachten, die zwangsläufig in den Kernbereich privater Lebensgestaltung eingreifen.[857]

[852] *Volkmann*, DVBl. 2008, 590 (593).
[853] So zum „Großen Lauschangriff" *BVerfGE* 109, 279 (323).
[854] *Volkmann*, DVBl. 2008, 590 (593).
[855] Vgl. insoweit zum „Großen Lauschangriff" *BVerfGE* 109, 279 (320f.).
[856] So aber *Hörnig*, JURA 2009, 207 (213).
[857] *Kutscha*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 155 (166f.)

# Kapitel 2 – Auswirkungen auf das Bürgerliche Recht

Die vorangegangene Darstellung des *GVIiS* sollte als Grundlage dafür dienen, die Auswirkungen dieser Ausprägung des allgemeinen Persönlichkeitsrechts auf das Bürgerliche Recht feststellen zu können. Dabei werden zunächst die allgemeinen dogmatischen Grundlagen des Zusammenwirkens von Verfassungs- und Zivilrecht dargestellt. Daran schließen sich die Überlegungen an, an welcher Stelle und in welchem Ausmaß der verfassungsrechtliche Schutz des *GVIiS* auf der Grundlage der bestehenden Dogmatik im Bürgerlichen Recht zu berücksichtigen ist.

## A. Grundrechte als objektive Wertordnung

Die Funktion der Grundrechte des Grundgesetzes liegt vorrangig darin, Eingriffe des Staates in grundrechtlich gesicherte Freiheiten abzuwehren. Sie gewinnen aber über diese Funktion hinaus noch Bedeutung als objektive Wertordnung, die das *BVerfG* im sog. *Lüth*-Urteil wie folgt beschreibt:[858]

[858] *BVerfGE* 7, 198 (204f.); siehe auch *BVerfGE* 42, 143 (148); 49, 89 (141f.); 50, 290 (337); 73, 261 (269).

„*Ohne Zweifel sind die Grundrechte in erster Linie dazu bestimmt, die Freiheitsrechte des einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern; sie sind Abwehrrechte des Bürgers gegen den Staat.* […] *Ebenso richtig ist aber, dass das Grundgesetz, das keine wertneutrale Ordnung sein will* […], *in seinem Grundrechtsabschnitt auch eine objektive Wertordnung aufgerichtet hat und dass gerade hierin eine prinzipielle Verstärkung der Geltung der Grundrechte zum Ausdruck kommt.* […] *Dieses Wertsystem, das seinen Mittelpunkt in der innerhalb der sozialen Gemeinschaft sich frei entfaltenden menschlichen Persönlichkeit und ihrer Würde findet, muss als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gelten; Gesetzgebung, Verwaltung und Rechtsprechung empfangen von ihm Richtlinien und Impulse. Das ergibt sich aus der geistesgeschichtlichen Entwicklung der Grundrechtsidee wie aus den geschichtlichen Vorgängen, die zur Aufnahme von Grundrechten in die Verfassungen der einzelnen Staaten geführt haben. Diesen Sinn haben auch die Grundrechte des Grundgesetzes, das mit der Voranstellung des Grundrechtsabschnitts den Vorrang des Menschen und seiner Würde gegenüber der Macht des Staates betonen wollte.*“

Auch wenn den Grundrechten insofern ein „Doppelcharakter“ zukommt,[859] ist diese objektive Wertordnung durch die vorrangige Funktion der Grundrechte als Abwehrrechte des einzelnen gegen den Staat begrenzt. Die objektive Wirkung der Grundrechte kann nicht vom subjektiv-rechtlichen Schutz gelöst werden, da damit die Wertentscheidungen zu einem subjektiven Grundrechtsschutz auf der Ebene des objektiv-rechtlichen Grundrechtsgehalts unterlaufen würden:[860]

„*Nach ihrer Geschichte und ihrem heutigen Inhalt sind sie* [die Grundrechte] *in erster Linie individuelle Rechte, Menschen- und Bürgerrechte, die den Schutz konkreter besonders gefährdeter Bereiche menschlicher Freiheit zum Gegenstand haben.* […] *Sie* [die Funktion der Grundrechte als objektive Prinzipien] *lässt sich deshalb nicht von dem eigentlichen Kern lösen und zu einem Gefüge objektiver Normen verselbständigen, in dem der ursprüngliche und bleibende Sinn der Grundrechte zurücktritt.*“[861]

## I. Schutzpflichten

Mit der Funktion der Grundrechte auch als objektiver Wertordnung sind zunächst die staatlichen Schutzpflichten verbunden. Diese verlangen vom Staat, die in den Grundrechten zum Ausdruck kommenden Werte und Rechtsgüter gegen Verletzungen zu schützen.[862] Die Aufgabe des Staates beschränkt sich daher nicht darauf, selbst Eingriffe in grundrechtlich geschützte Freiheiten zu unterlassen, sondern den einzelnen Bürger vor Übergriffen privater Dritter zu schützen und mittels geeigneter Maßnahmen Rechtsgutsverletzungen zu vermeiden.[863] Der Staat

[859] Vgl. *Stern*, Staatsrecht III/1, § 69 I 3, S. 906.
[860] *Herdegen*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 1 Abs. 3 Rn. 26.
[861] *BVerfGE* 50, 290 (337).
[862] *Canaris*, AcP 184 (1984), 201 (225f.).
[863] *Dreier*, in: *Ders.* (Hrsg.), GG, Bd. 1, Vorb. Rn. 101.

hat somit auch die Unversehrtheit grundrechtlicher Güter zwischen Privaten und damit die Sicherheit in den privaten Beziehungen zu garantieren.[864] Die Schutzpflichten beinhalten folglich staatlichen Schutz gegen nichtstaatliche Eingriffe.[865] Sie setzen daher eine Dreierbeziehung aus Staat, privatem Dritten und Betroffenem voraus.[866] Aus den Grundrechten folgt insofern die Verpflichtung zum Handeln der Gesetzgebung, Verwaltung und Rechtsprechung.[867]

*1. Begründung der Schutzpflichten durch das BVerfG*

*BVerfGE* 39, 1 (41) verweist zur Begründung der staatlichen Pflicht, jedes menschliche Leben zu schützen, ausdrücklich auf die im *Lüth*-Urteil beschriebene objektive Wertordnung der Grundrechte, entnimmt diese Pflicht jedoch unmittelbar Art. 2 Abs. 1 GG. Daneben ergebe sich die Schutzpflicht auch aus Art. 1 Abs. 1 S. 2 GG. Ohne den Verweis auf die objektive Wertordnung kommt *BVerfGE* 46, 160 (164) aus, wo die Schutzpflicht des Staates gegenüber dem menschlichen Leben Art. 2 Abs. 2 S. 1 i.V.m. Art. 1 Abs. 1 S. 2 GG entnommen wird. Ausschließlich mit dem Verweis auf die objektive Wertordnung werden in *BVerfGE* 49, 89 (141f.) hinsichtlich des Grundrechts des Art. 2 Abs. 2 S. 1 GG verfassungsrechtliche Schutzpflichten aufgestellt, rechtliche Regelungen so auszugestalten, dass auch die Gefahr von Grundrechtsverletzungen eingeschränkt bleibt. Die Verpflichtung der staatlichen Gewalt aus Art. 1 Abs. 1 S. 2 GG, die Würde des Menschen zu achten und zu schützen, wird hier nur noch als Verdeutlichung objektiv-rechtlicher Wertentscheidungen der Verfassung angeführt. Der Hinweis auf die objektive Rechtsordnung fehlt wiederum in *BVerfGE* 53, 30 (57) und 56, 54 (73), wo für die Begründung der aus dem objektiv-rechtlichen Gehalt des Art. 2 Abs. 2 GG folgenden Schutzpflicht gegenüber Leben und körperlicher Unversehrtheit, auf „anerkannte Rechtsprechung" verwiesen wird und auch der Bezug zu Art. 1 Abs. 1 S. 2 GG nicht mehr enthalten ist. Dieser Verweis wird dann in *BVerfGE* 77, 170 (210) wiederum mit der „objektiv-rechtlichen Wertentscheidung der Verfassung" verknüpft. Die Grundlage der *Schutzpflicht*[868] des Staates gegenüber dem ungeborenen Leben sieht *BVerfGE* 88, 203 (251) dagegen in Art. 1 Abs. 1 GG, deren Gegenstand und Maß aber Art. 2 Abs. 2 GG näher bestimmt.

[864] *Isensee*, in: HStR V², § 111 Rn. 3.
[865] *Merten*, in: GS für *Burmeister*, S. 227 (236).
[866] *Isensee*, in: HStR V², § 111 Rn. 87; *Erichsen*, JURA 1997, 85.
[867] *Isensee*, in: HStR V², § 111 Rn. 3.
[868] Hervorhebung im Original.

*2. Inhalt*

In Bezug auf den Schutz des ungeborenen Lebens wird der Begriff der Schutzpflichten vom *BVerfG* wie folgt präzisiert:[869]

> „*Die Schutzpflicht des Staates ist umfassend. Sie verbietet nicht nur - selbstverständlich - unmittelbar staatliche Eingriffe in das sich entwickelnde Leben, sondern gebietet dem Staat auch, sich schützend und fördernd vor dieses Leben zu stellen, das heißt vor allem es auch vor rechtwidrigen Eingriffen von seiten anderer zu bewahren. An diesem Gebot haben sich die einzelnen Bereiche der Rechtsordnung, je nach ihrer besonderen Aufgabenstellung auszurichten.*"

Schutzpflichten kommen aber von vornherein nur dort in Betracht, wo das einzelne Grundrecht auf einen „absoluten und allwirksamen" und nicht nur einen „relativen, auf das Verhältnis des einzelnen zum Staat beschränkten Schutz" gerichtet ist.[870] Daraus folgt für den Persönlichkeitsschutz, dass Ausprägungen des verfassungsrechtlich gewährleisteten Persönlichkeitsrechts nur nach Maßgabe der Erforderlichkeit eines rechtlichen Schutzes unter Anpassung an die besonderen Erfordernisse des Privatrechtsverkehrs in den Schutzbereich des Persönlichkeitsrechts des § 823 Abs. 1 BGB aufzunehmen sind.[871] Jedoch spricht eine objektive Wertordnung ohne Beschränkung auf bestimmte Grundrechte dafür, zunächst jedem Grundrecht einen objektiv-rechtlichen Gehalt und damit entsprechende Schutzpflichten entnehmen zu können.[872] Einer ausdrücklichen Feststellung bedürfte es dann nicht. Der grundrechtliche Schutzbereich ist im Rahmen der Erfüllung von Schutzpflichten vorrangig als Schutzgut zu verstehen, dessen Integrität vom Staat gegen Dritte zu sichern ist.[873] Somit kommen Schutzpflichten von vornherein nur dort in Betracht, wo der Schutzbereich des betroffenen Grundrechts überhaupt eröffnet ist.[874] Für die Legislative begründen Schutzpflichten einen Gesetzgebungsauftrag mit dem Inhalt, dem Schutzbedarf entsprechende Normen zu erlassen, einen Mindeststandard ausreichender Schutznormen zu halten und bei Änderung der Verhältnisse bestehende Normen entsprechend anzupassen.[875] Exekutive und Judikative kommt ein entsprechender Vollzugsauftrag zur Gewährleistung effektiven Schutzes zu. Gegenstand der Schutzpflicht kann nicht nur die aktuelle Rechtsverletzung, sondern auch die bloß theoretisch vorhersehbare Möglichkeit eines Schadenseintritts sein.[876]

---

[869] *BVerfGE* 39, 1 (42) (Hervorhebung nur hier); vgl. auch *BVerfGE* 88, 203 (251).
[870] *Merten*, in: GS *Burmeister*, S. 227 (233); ähnlich *Erichsen*, JURA 1997, 85 (87), keine Schutzpflicht bei „ausschließlicher Staatsgerichtetheit" eines Grundrechts.
[871] *Baston-Vogt*, Persönlichkeitsrecht, S. 123f.
[872] Vgl. *Jarass*, AöR 110 (1985), 363 (371f.).
[873] *Isensee*, in: HStR V², § 111 Rn. 3.
[874] *Canaris*, Grundrechte und Privatrecht, S. 72.
[875] *Isensee*, in: HStR V², § 111 Rn. 90.
[876] *Isensee*, in: HStR V², § 111 Rn. 106.

In wesentlichen Teilen lässt sich dabei das einfache Recht als Verwirklichung der Schutzgebotsfunktion der Grundrechte verstehen.[877] Die Schutzfunktion der Grundrechte verlangt aber, „das Privatrecht so zu gestalten, dass die in den Grundrechten verkörperte objektive Ordnung gewahrt wird".[878] Vor dem Hintergrund des Untermaßverbots ist hierfür aber lediglich ein insgesamt effizienter Schutz notwendig, dessen Ausgestaltung im Einzelnen offenbleiben muss.[879] Regelmäßig liegt damit die Funktion des Privatrechtsgesetzgebers in der Abstimmung der Individualinteressen der am Privatrechtsverkehr Teilnehmenden.[880] Dabei ist der Schutz des Staates jedoch subsidiär gegenüber der Möglichkeit des Betroffenen, eigenverantwortlich für seine Sicherheit zu sorgen, sofern ihm zumutbar ist, sein Recht selbst u.U. auch auf gerichtlichem Wege zu verteidigen.[881]

### *3. Gestaltungsfreiheit und Untermaßverbot*

Gesetzgeber und vollziehende Gewalt haben bei der Erfüllung von Schutzpflichten einen weiten Einschätzungs-, Wertungs- und Gestaltungsbereich.[882] Daher ist die Reichweite der hierauf gerichteten gerichtlichen Überprüfbarkeit begrenzt.[883] Aufgrund der gewaltenteilenden Funktionenordnung des Grundgesetzes ist die Rechtsetzung prinzipiell dem parlamentarischen Gesetzgeber oder auf Grund entsprechender Ermächtigungen auch exekutiven Organen zugewiesen.[884] Allerdings ist auch die Grenze dieser Gestaltungsfreiheit jedenfalls dann erreicht, wenn von der öffentlichen Gewalt entweder überhaupt keine Schutzvorkehrungen getroffen wurden oder die zum Schutz eines Grundrechts getroffenen Vorkehrungen „gänzlich ungeeignet" oder „völlig unzulänglich" sind.[885] Gleiches gilt, wenn den staatlichen Organen eine „evidente Verletzung der in den Grundrechten verkörperten Grundentscheidungen" vorgeworfen werden kann.[886] Die Gestaltungsfreiheit wird so durch die Gewährleistung des verfassungsgebotenen Mindeststandards an Grundrechtssicherheit begrenzt.[887] Dieses *Untermaßverbot* erfordert einen unter Berücksichtigung entgegenstehender Rechtsgüter angemessenen und als solchen wirksamen Schutz.[888] Ein verfassungswidriges Unterlassen seitens des

---

[877] *Canaris*, Grundrechte und Privatrecht, S. 82.
[878] *BVerfGE* 98, 365 (395).
[879] *Canaris*, Grundrechte und Privatrecht, S. 84.
[880] *Götz*, in: *Heyde/Starck* (Hrsg.), Vierzig Jahre Grundrechte, S. 35 (46f.).
[881] *Isensee*, in: HStR V², § 111 Rn. 142.
[882] *BVerfGE* 77, 170 (214f.); 79, 174 (202); 85, 191 (212); vgl. auch *BVerfGE* 90, 145 (173); 109, 279 (336); 120, 274 (320).
[883] *BVerfGE* 77, 170 (215); 79, 174 (202); 90, 145 (173).
[884] *Sodan*, NVwZ 2000, 601 (603f.).
[885] *BVerfGE* 77, 170 (215); 92, 26, (46); anders aber *BVerfGE* 88, 203 (263), wonach der Schutzpflicht des Staates gegenüber dem menschlichen Leben gerade nicht schon Maßnahmen genügen, „die nicht gänzlich ungeeignet oder völlig unzulänglich sind".
[886] *BVerfGE* 56, 54 (81); vgl. auch *BVerfGE* 33, 303 (333).
[887] *Isensee*, in: HStR V², § 111 Rn. 165.
[888] *BVerfGE* 88, 203 (254) (Hervorhebung nur hier).

Staates setzt somit das Unterschreiten des verfassungsrechtlich gebotenen Schutzminimums voraus.[889] Die Schutzpflicht des Staates reicht umso weiter, je höher der Rang des betroffenen Rechtsguts innerhalb der Wertordnung des Grundgesetzes ist.[890] Die generell relevanten Wertungsgesichtspunkte für das Bestehen von Schutzpflichten - neben dem Rang des betroffen Grundrechts seine Art, die Schwere des drohenden Eingriffs und die Intensität der Gefährdung, die Möglichkeit des Betroffenen zu effektivem Selbstschutz sowie das Gewicht gegenläufiger Grundrechte und Interessen - sind zum Erfordernis einer Schutzpflicht in eine Abwägung einzustellen.[891]

## II. Mittelbare Drittwirkung der Grundrechte

Neben der Begründung von Schutzpflichten folgt aus der Eigenschaft der Grundrechte als objektive Wertordnung auch ihr Einfluss auf das Zivilrecht im Wege der sog. *mittelbaren Drittwirkung*. Es soll die freiheitssichernde Zielsetzung als Wertentscheidung auch im Privatrecht gewährleistet werden.[892] Mit dem Begriff der Drittwirkung der Grundrechte lässt sich die horizontale Richtung der Grundrechte im Verhältnis der Bürger zueinander im Gegensatz zur vertikalen Richtung der Grundrechte im Verhältnis des Bürgers zum Staat beschreiben.[893] Anders als im Verhältnis des Bürgers zum Staat, wo die Grundrechte Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht binden (Art. 1 Abs. 3 GG), kommen die grundrechtlichen Wertungen im Verhältnis der Bürger zueinander aber nicht direkt, sondern nur mittelbar zur Anwendung. Unter Ablehnung einer unmittelbaren Wirkung der Grundrechte zwischen Privaten begründete zunächst *Dürig*[894] deren bloß mittelbare Wirkung auf das Privatrecht: Das von den Grundrechten gebildete gegen den Staat gerichtete Anspruchssystem enthalte gerade auch das Recht, über individuelle Lebensbeziehungen zu anderen rechtlich autonom disponieren zu können. Deshalb werde aber zwangsläufig die Wirkung der Grundrechte im Verhältnis Privater aufgrund der grundrechtlich geschützten Individualautonomie und der Eigenverantwortung relativiert. Somit unterliege der Rechtsverkehr Privater untereinander gerade aufgrund verfassungsrechtlicher Vorgaben dem Sonderrecht des Privatrechts und dies auch hinsichtlich der Abwehr von Angriffen Privater auf Rechte anderer. Sofern spezielle zivilrechtliche Schutznormen zur Abwehr solcher Angriffe fehlen, stellten die „wertausfüllungsfähigen und wertausfüllungsbedürftigen Generalklauseln" die normativen Mittel dar, mit denen das objektive Privatrecht den Schutzauftrag des Art. 1 Abs.

---

889 *Canaris*, AcP 184 (1984), 201 (228); *Erichsen*, JURA 1997, 85 (88).
890 *BVerfGE* 39, 1 (42).
891 *Canaris*, Grundrechte und Privatrecht, S. 80; siehe auch *Isensee*, in: HStR V² § 111 Rn. 90 sowie *BVerfGE* 49, 89 (142).
892 Vgl. *BVerfGE* 52, 131 (166).
893 So *v. Münch*, in: *Ders./Kunig* (Hrsg.), GG, Bd. 1, Vorb. Art. 1-19 Rn. 28.
894 *Dürig*, in: FS *Nawiasky*, S. 157 (176).

1 S. 2 GG erfüllt. Obwohl dieses Verständnis auf dem Gedanken der Privatautonomie der Beteiligten aufbaut, soll es laut *Dürig* auch im außervertraglichen Bereich Anwendung finden, da sich hier ebenfalls anders als im Verhältnis des Bürgers zum Staat zwei Grundrechtberechtigte gegenüberstünden, wodurch „die qualitativ andere Bedeutung der Grundrechte auch in außervertraglichen Rechtsbeziehungen" gerechtfertigt sei.[895]

Im *Lüth*-Urteil beschreibt das *BVerfG* i.S.d. *Lehre von der mittelbaren Drittwirkung* die „Ausstrahlungswirkung"[896] der Grundrechte auf das Privatrecht wie folgt:[897]

> „*So beeinflusst es* [das grundrechtliche Wertesystem] *selbstverständlich auch das bürgerliche Recht; keine bürgerlich-rechtliche Vorschrift darf im Widerspruch zu ihm stehen, jede muss in seinem Geiste ausgelegt werden. Der Rechtsgehalt der Grundrechte als objektiver Normen entfaltet sich im Privatrecht durch das Medium der dieses Rechtsgebiet unmittelbar beherrschenden Vorschriften. Wie neues Recht im Einklang mit dem grundrechtlichen Wertsystem stehen muss, so wird bestehendes älteres Recht inhaltlich auf dieses Wertsystem ausgerichtet; von ihm her fließt ihm ein spezifisch verfassungsrechtlicher Gehalt zu, der fortan seine Auslegung bestimmt.* […] *Der Einfluss grundrechtlicher Wertmaßstäbe wird sich vor allem bei denjenigen Vorschriften des Privatrechts geltend machen, die zwingendes Recht enthalten* […]. *Der Rechtsprechung bieten sich zur Realisierung dieses Einflusses vor allem die ‚Generalklauseln', die* […] *zur Beurteilung menschlichen Verhaltens auf außer-zivilrechtliche, ja zunächst überhaupt außerrechtliche Maßstäbe* […] *verweisen.* […] *Deshalb sind mit Recht die Generalklauseln als die ‚Einbruchstellen' der Grundrechte in das bürgerliche Recht bezeichnet worden* […]. *Der Richter hat kraft Verfassungsgebots zu prüfen, ob die von ihm anzuwendenden materiellen zivilrechtlichen Vorschriften in der beschriebenen Weise grundrechtlich beeinflusst sind; trifft das zu, dann hat er bei Auslegung und Anwendung dieser Vorschriften die sich daraus ergebende Modifikation des Privatrechts zu beachten. Dies ist der Sinn der Bindung auch des Zivilrichters an die Grundrechte (Art. 1 Abs. 3 GG).*"

Die Grundrechte sind demnach aber nur vorrangig und nicht ausschließlich über die Generalklauseln des Privatrechts zu berücksichtigen. Auch eine Norm mit festem Tatbestand kann zur Verwirklichung der Grundrechte beitragen.[898] Zudem ist nicht von vornherein gesichert, dass stets eine geeignete Generalklausel vorhanden ist und ob eine vorhandene Generalklausel stets ausreichenden Grundrechtsschutz vermittelt.[899] Die umfassende Schutzfunktion der Grundrechte erfordert, nicht nur die Generalklauseln, sondern alle Privatrechtsnormen i.d.S. zu interpretieren.[900] Die Generalklauseln sind aufgrund ihrer dahingehenden Offen-

---

[895] *Dürig*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 3 Abs.1 Rn. 513.
[896] *BVerfGE* 7, 198 (207); in letzter Zeit *BVerfGE* 112, 332 (358).
[897] *BVerfGE* 7, 198 (205f.); siehe auch *BVerfGE* 25, 256 (263); 34, 269 (280); 42, 143 (148); 52, 131 (165f.); 73, 261 (269); 81, 242 (254); 99, 185 (196); 115, 51, 66f.).
[898] *Canaris*, AcP 184 (1984), S. 201 (223) mit Beispielen.
[899] *Canaris*, AcP 184 (1984), S. 201 (223) mit Beispielen.
[900] *Stern*, Staatsrecht III/1, § 76 IV 7, S. 1584.

heit „nicht ausschließliches, sondern nur bevorzugtes Einfallstor".[901] Ihre besondere Bedeutung erlangen sie allein aufgrund ihrer größeren Interpretationsfähigkeit.[902] Entscheidend sind vielmehr die generelle Verfassungsmäßigkeit des Zivilrechts und die seiner Anwendung.[903] Erhebliches Gewicht kommt der Ausstrahlungswirkung der Grundrechte somit bei der Rechtsfortbildung zu.[904] Allerdings wird auch vertreten, die Auswirkung der Grundrechte auf das Privatrecht nicht über eine mittelbare Drittwirkung, sondern innerhalb der staatlichen Schutzpflichten zu behandeln. Die Aktualisierung des objektiv-rechtlichen Gehalts der Grundrechte im Rahmen der Drittwirkung stelle gerade die Schutzpflicht des Richters dar[905]. Die Frage nach der aktiven Gewährung gerichtlichen Schutzes gegenüber privaten Dritten hänge von einer eventuellen staatlichen Schutzpflicht ab.[906] Mit der Figur der grundrechtlichen Schutzpflichten könnten die Auswirkungen der Grundrechte auf das Privatrecht insgesamt und somit nicht nur die Verpflichtung des Gesetzgebers zur grundrechtskonformen Ausgestaltung, sondern auch diejenige des Richters zur grundrechtskonformen Auslegung des Privatrechts beschrieben werden.[907] Für die Heranziehung der Schutzpflichtenlehre spreche zudem, dass darin die Grundrechte der Beteiligten allein auf den Staat gerichtet sind, deren Binnenbeziehung aber auslassen, so dass deren Privatautonomie komplett unangetastet bliebe.[908] Die Frage nach der Drittwirkung der Grundrechte lasse sich jedenfalls nur unter Berücksichtigung ihrer Funktion als auch in der Privatrechtsordnung wirksame objektive Ordnungsprinzipien befriedigend lösen.[909]

Der Einfluss der Grundrechte auf die Privatrechtsordnung vollzieht sich somit auf den zwei Ebenen der „grundrechtsgeleiteten Gesetzgebung" und der „Konkretisierung gesetzlicher Bestimmungen durch den Richter im Lichte der Grundrechte".[910]

---

[901] *Stern*, Staatsrecht III/1, § 76 IV 7, S. 1584.
[902] *Classen*, AöR 122 (1997), 65 (71).
[903] *Rüfner*, in: HStR V², § 117, Rn. 73.
[904] *BVerfGE* 96, 375 (398).
[905] *Papier*, in: HGR II, § 55, Rn. 10.
[906] *Oeter*, AöR 119 (1994), 529 (536f.).
[907] *Papier*, in: HGR II, § 55, Rn. 10
[908] *Isensee*, in: HStR V², § 111 Rn. 135.
[909] *Stern*, Staatsrecht III/1, § 76 III 4, S. 1561.
[910] *Herdegen*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 1 Abs. 3 Rn. 20.

# B. Wirkungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

## I. Objektiv-rechtlicher Gehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Nach diesen Maßstäben kommt grds. auch eine objektiv-rechtliche Wirkung des *GVIiS* in Betracht.[911] Zu bestimmen ist hierfür zunächst der objektiv-rechtliche Gehalt des *GVIiS*, der im Verhältnis zwischen Privatpersonen zu berücksichtigen ist.

### *1. Anwendbarkeit auf das Verhältnis zwischen Privatpersonen*

Dafür müsste der Schutzgegenstand des *GVIiS* zunächst überhaupt auch über das Verhältnis des einzelnen Bürgers zum Staat hinaus auch auf das Verhältnis von Privaten zueinander anwendbar sein. Die Begriffe der Vertraulichkeit und Integrität beschreiben einen bestimmten Zustand der Kontrolle des Berechtigten über den Zugriff auf das von ihm genutzte informationstechnische System. Dieser Zustand ist jedoch nicht auf das Verhältnis des Einzelnen zum Staat beschränkt. „Das Interesse des Nutzer, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben",[912] wird nicht allein in der Beziehung des Bürgers zum Staat ausgemacht. In gleicher Weise ist auch das Antasten der Integrität des informationstechnischen Systems, „indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können",[913] nicht auf den staatlichen Zugriff beschränkt. Die Schutzgegenstände der Vertraulichkeit und Integrität werden unabhängig von der Person des Eingreifenden definiert. Der Schutz des *GVIiS* gerade gegenüber der staatlichen Gewalt ergibt sich somit nicht bereits aus der Definition beider Begrifflichkeiten, sondern aus der Funktion des allgemeinen Persönlichkeitsrechts in der Beziehung des Einzelnen zum Staat als Abwehrrecht grundrechtlicher Beeinträchtigungen. Daher werden die neuartigen Persönlichkeitsgefährdungen durch die Nutzung informati-

911 So auch *Hörnig*, JURA 2009, 207 (211); siehe hierzu auch das Interview mit BVR a.D. *Hoffmann-Riem* in der *FAZ* v. 10.10.2011, S. 5, zu dem 2009 in einem Ermittlungsverfahren in Bayern eingesetzten Spähprogramm: „Eingriffe *Privater* in Freiheiten können ähnlich gefährlich sein wie staatliche Eingriffe. Private sind aber nicht ohne weiteres an die Grundrechte gebunden. Hier aber hilft das *Lüth-Urteil* des Bundesverfassungsgerichts aus dem Jahr 1958. Die Grundrechte enthalten auch einen *Auftrag an den Staat*, die allgemeine Rechtsordnung so einzurichten, dass Freiheitsschutz auch gegen Private möglich wird" (Hervorhebungen nur hier).

912 *BVerfGE* 120, 274 (314).

913 *BVerfGE* 120, 274 (314).

onstechnischer Systeme nicht auf das Verhältnis des Einzelnen zum Staat beschränkt,[914] sondern es ist in diesem Zusammenhang die Rede von Gefährdungen, die durch „Dritte" drohen:

> Wird die im Arbeitsspeicher und auf den Speichermedien informationstechnischer Systeme enthaltene Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers „von *Dritten* erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen";[915]
>
> die Vernetzung eines informationstechnischen Systems öffnet „*Dritten* eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren";[916]
>
> „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."[917]

Auch die Definition des Schutzgegenstands der Integrität ist nicht auf die persönlichkeitsrechtliche Bedrohung durch den Staat beschränkt, denn der grundrechtliche Schutzbereich ist dann betroffen,

> „*wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können*".[918]

Dieser Definition der Gefährdungslage ist vollumfänglich zuzustimmen. Für den Betroffenen macht es keinen entscheidenden Unterschied, ob er sich der staatlichen Überwachung oder derjenigen eines privaten *Dritten* ausgesetzt sieht. Die verschiedene Zielsetzung der Überwachung, auf Seiten des Staates die Überwachung des Verhaltens der Zielperson an sich, auf Seiten des privaten Dritten die Beschaffung sensibler Informationen, macht für den Betroffenen hinsichtlich der Beeinträchtigung seiner Persönlichkeitsentfaltung keinen entscheidenden Unterschied. Auch private Informationshandlungen können die Entfaltungsfreiheit des Betroffenen erheblich gefährden.[919] Der Zugriff durch einen privaten Dritten ist

914 I.E. ebenso *Stögmüller*, CR 2008, 435 (437).
915 *BVerfGE* 120, 274 (305) (Hervorhebung nur hier).
916 *BVerfGE* 120, 274 (306) (Hervorhebung nur hier).
917 *BVerfGE* 120, 274 (313) (Hervorhebung nur hier).
918 *BVerfGE* 120, 274 (314).
919 *Bäcker*, Der Staat [2012], 91 (101).

in gleicher Weise geeignet, den Betroffenen durch die Furcht vor einer potentiellen Kontrolle von der Ausübung seiner grundrechtlich vermittelten Freiheit abzuhalten.

*2. Bezeichnung des Grundrechts*

Teilweise wird allein aus der Bezeichnung als Grundrecht auf *Gewährleistung* der Vertraulichkeit und Integrität informationstechnischer Systeme ein objektiver Schutzauftrag des Staates abgeleitet.[920] Dagegen lässt sich jedoch einwenden, dass Gewährleistung nur ein allgemein verwendeter Ausdruck für Grundrechtsgarantien sei, der noch keine Aussage über immanente Schutzpflichten enthält.[921] Im Unterschied zum Begriff des Schutzbereichs komme durch denjenigen des Gewährleistungsgehalts lediglich der gesamte normative Inhalt einer Grundrechtsnorm, der nach gegenwärtigem Grundrechtsverständnis über die klassische Funktion des Abwehrrechts hinausgeht, zum Ausdruck.[922] Der Gewährleistungsinhalt eines Grundrechts enthält aber lediglich allgemein die normative Aussage über die Reichweite an Schutz, Freiheit, Teilhabe etc.[923] Auch der Gewährleistungsinhalt ist demnach für jedes Grundrecht auch eigenständig zu ermitteln.[924] Mangels erkennbarer grundsätzlicher dogmatischer Umorientierung würden die Begriffe des Schutz- und desjenigen des Gewährleistungsbereichs vom *BVerfG* austauschbar verwendet.[925]

*3. Selbstschutz*

Für einen objektiv-rechtlichen Gehalt des *GVIiS* lassen sich aber wiederum die Ausführungen des *BVerfG* zu den Möglichkeiten des Selbstschutzes des Betroffenen heranziehen:

> „*Der Einzelne kann solche Zugriffe* [zur Ausspähung oder Manipulation der auf dem System vorhandenen Daten] *zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten - etwa die Verschlüsselung oder die Verschleierung sensibler Daten -*

---

920 So *Petri*, DuD 2008, 443 (446); *Schulz*, DuD 2012, 395 (396); für einen damit verdeutlichten Schutzauftrag des Staates in allen Lebensbereichen *Hoffmann-Riem*, JZ 2008, 1009 (1020 Fn. 100).

921 *Starck*, Verfassungsauslegung I, S. 56f.

922 *Hoffmann-Riem*, Der Staat [2004], 203 (226).

923 *E.-W. Böckenförde*, Der Staat [2003], 165 (174).

924 *E.-W. Böckenförde*, Der Staat [2003], 165 (174).

925 So *Hoffmann-Riem*, Der Staat [2004], 203 (226); vgl. auch *Stern/Sachs*, Staatsrecht III/2, § 77 II 4, S. 26f. m.w.N.

*werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.*"[926]

Danach werden die Möglichkeiten des Einzelnen, allein die Vertraulichkeit und Integrität seines informationstechnischen Systems sicherzustellen, nicht umfänglich als ausreichend angesehen. Genügt aber der eigene Schutz des Einzelnen vor dem Umgang anderer mit seinen Daten und seinem eigenen unbefangenen Gebrauch der Technik nicht mehr, kommt vor allem dem Staat die Aufgabe zu, zum Schutz der Persönlichkeit seiner Bürger zu gewährleisten, dass Informationen und Daten über ihre Person vor fremden Zugriffen geschützt werden.[927] Der Einzelne kann nicht auf bloßen Selbstschutz verwiesen werden, soweit ihm dieser gar nicht möglich ist. Aus dem allgemeinen Persönlichkeitsrecht ergibt sich daher die Schutzpflicht des Staates, wirkungsvolle rechtliche Voraussetzungen eines informationellen Selbstschutzes zu schaffen.[928]

Die Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und die mit dieser Nutzung verbundenen Persönlichkeitsgefährdungen begründen „ein grundrechtlich erhebliches Schutzbedürfnis". Da aber die Möglichkeit des Einzelnen, über den Zugriff auf sein informationstechnisches System selbstbestimmt zu entscheiden, ebenso wenig wie die sich aus der Nutzung des Systems ergebenden neuartigen Gefährdungen der Persönlichkeit nicht auf das Verhältnis des Bürgers zum Staat beschränkt sind, entfaltet das *GVIiS* im Rahmen der oben dargelegten Maßstäbe seine Wirkung auch im Zivilrecht. Dem Staat kommt damit die Pflicht zu, dem Einzelnen die selbstbestimmte Verfügung über das von ihm genutzte informationstechnische System auch im Verhältnis zu anderen Privatpersonen zu ermöglichen.[929] Die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht verlangt von den zuständigen staatlichen Stellen, hierfür die rechtlichen Voraussetzungen bereitzustellen. Folglich beschränkt sich der Schutz durch das *GVIiS* nicht allein darauf, staatliche Zugriffe auf das eigene informationstechnische System abzuwehren, sondern umfasst auch die Pflicht, vor solchen Eingriffen durch Private zu schützen.

Die Begriffe der Vertraulichkeit und Integrität i.S.d. *GVIiS* bezeichnen nach dem hier vertretenen Verständnis nur einen individuellen Zustand des informationstechnischen Systems. Folglich geht es um den Schutz allein dieses Systemzustands unabhängig davon, welches Sicherheitsniveau erreicht wird. Es ist damit aber gerade kein bestimmter Zustand der Systemsicherheit verlangt. Der objektivrechtliche Gehalt des *GVIiS* gegenüber privaten Dritten kann dann aber nur in

[926] *BVerfGE* 120, 274 (306).
[927] *Hohmann-Dennhardt*, RDV 2008, 1 (2).
[928] *BVerfG* MMR 2007, 93.
[929] Vgl. *BVerfG* MMR 2007, 93 zum *RiS*.

der Umsetzung seiner Abwehrfunktion liegen. Diese besteht in der bloßen Sanktionierung eines Eingriffs in die selbstbestimmte Verfügung über das informationstechnische System. Schutzpflichten können sich schon aus der Durchsetzung der Abwehrfunktion eines Grundrechts ergeben.[930] Im Folgenden erschöpft sich diese Pflicht in der Reichweite der Abwehrdimension. Es ist allein der Eingriff in den vom betroffenen Nutzer selbst geschaffenen Zustand von Vertraulichkeit und Integrität abzuwehren.

#### *4. Ergebnis*

Auch das *GVIiS* weist nach den allgemeinen Maßstäben einen objektivrechtlichen Gehalt auf, der im Verhältnis von Privatpersonen untereinander zu berücksichtigen ist. Dessen Wirkung ist jedoch wie auch der Schutz des *GVIiS* als Abwehrrecht gegen staatliche Eingriffe, auf die bloße Abwehr eines Eingriffs privater Dritter in den individuellen Zustand von Vertraulichkeit und Integrität des informationstechnischen Systems beschränkt.[931]

### II. Schutzpflichten

#### *1. Bestehender Schutz*

Nach Maßgabe der Reichweite, in der das *GVIiS* vor einem staatlichen Eingriff in die selbstbestimmte Verfügung über das eigene informationstechnische System schützt, bestehen somit auch Schutzpflichten des Staates gegen Übergriffe Privater. Zunächst stellt sich die Frage, inwieweit dieser Schutz bereits de lege lata gewährleistet wird. Die Erörterung konkreter gesetzgeberischer Maßnahmen erübrigt sich, wenn die gegenwärtige Rechtslage einen Schutz gewährleistet, der nach Maßgabe des Untermaßverbots für die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auf privatrechtlicher Ebene ausreichend ist. Dabei kommt vor allem dem Schutzbereich des einfachgesetzlichen allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB Bedeutung zu. Allerdings ist § 823 Abs. 1 BGB hinsichtlich des Schutzes vor einer unzulässigen Datenverarbeitung nicht anwendbar, soweit das BDSG als persönlichkeitsrechtliche Spezialnorm die Rechte des Betroffenen aus einer unzulässigen Datenverarbeitung abschließend regelt.[932] Ansprüche wegen der Verletzung des allgemeinen Persönlichkeitsrechts bestehen nach § 823 Abs. 1 BGB hingegen dort, wo das BDSG auf einen Informationseingriff erkennbar nicht oder nicht abschließend reagieren

---

[930] Vgl. *Isensee*, in: HStR V², § 111 Rn. 13.

[931] A.A. *Luch*, MMR 2011, 75 (79), die - allerdings ohne Benennung der konkreten rechtlichen Konstruktion - .auch einen positiven Anspruch auf Schutz der durch einen Diensteanbieter zur Nutzung bereitgestellten Systeme vor unberechtigten Zugriffen Dritter fordert.

[932] *BGHZ* 80, 311 (319); 89, 218 (226); 91, 233 (238); *BGH* NJW 1986, 2505 (2506f.); kritisch Staudinger/*Hager* (1999), § 823 Rn. C173.

will.[933] Als besondere Ausprägungen des Persönlichkeitsschutzes schließen die Vorschriften des BDSG weitergehende allgemeine Ansprüche aber nur aus, soweit dies dem Wortlaut und dem Zweck der Norm entnommen werden kann.[934]

a. Bundesdatenschutzgesetz (BDSG)

Die Prüfung der möglichen Spezialität des BDSG gegenüber § 823 Abs. 1 BGB deckt sich dabei in Teilen mit der Prüfung des sachlichen Anwendungsbereichs der DS-GVO-E.

i. Wortlaut

Bereits die Begriffe der Vertraulichkeit und Integrität finden sich nicht im Text des BDSG. § 9 S. 1 BDSG i.V.m. der Anlage zu § 9 S. 1 enthält Vorgaben zu technischen und organisatorischen Maßnahmen der Datenverarbeitung i.w.S, die sich lediglich inhaltlich mit den Schutzzielen der Vertraulichkeit und Integrität teilweise überschneiden.[935] Die Vorgaben beziehen sich jedoch alleine auf Gestaltungsanforderungen der Datenverarbeitung, ohne erkennbaren Gebrauch der Begriffe der Vertraulichkeit und Integrität nach Maßgabe des Schutzbereichs des *GVIiS* als Ausdruck der selbstbestimmten Verfügung über das eigene informationstechnische System.[936] Auch § 9 BDSG geht insofern über den Schutzzweck des BDSG nicht hinaus. Die Regelung dient nach ihrem Wortlaut und der Gesetzesbegründung[937] allein der Gewährleistung der Durchsetzung der Normen des BDSG.

ii. Systematik

Ähnlich der DS-GVO-E fehlt es im BDSG an einem individuellen Abwehranspruch gegen die Beeinträchtigung der Vertraulichkeit und Integrität informationstechnischer Systeme.

§ 42a S. 1 BDSG behandelt zwar die unrechtmäßige Kenntniserlangung personenbezogener Daten durch einen Dritten. Vom Wortlaut erfasst wäre daher auch die Informationsgewinnung infolge des Zugriffs auf ein informationstechnisches System. Die Norm sieht ihrem Wortlaut sowie der amtlichen Überschrift nach jedoch lediglich eine Informationspflicht der verantwortlichen Stelle vor.[938] An-

933 MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 112.

934 MüKoBGB-Rixecker, Allg. PersönlR Rn. 112.

935 Zur ähnlichen Situation in der DS-GVO-E, siehe bereits oben S. 106 sowie wiederum kritisch dazu *Münch*, RDV 2012, 72 (73f.); *Popp*, ZD 2012, 51 (55) sowie *Braun/Roggenkamp*, K&R 2011, 681 (684), ziehen die Norm hinsichtlich der Anforderungen an kryptographische Standards einer Software zur Quellen-TKÜ heran.

936 Ähnlich *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 1 Rn. 44: Das *GVIiS* gehe mit dem unmittelbaren Schutz des informationstechnischen Systems selbst über die Vorgaben des § 9 BDSG hinaus.

937 Vgl. BT-Drucks. 7/1027, S. 23.

938 Weitere Informationspflichten enthält für den Bereich des Beschäftigtendatenschutz § 32j BDSG-E des RegE eines *Gesetzes zur Regelung des Beschäftigtendatenschutzes*, BT-Drucks. 17/4230.

sprüche des Betroffenen gegen den Kenntnis erlangenden Dritten regelt die Norm nicht. Die Norm knüpft u.a. an den Vorschlag der Europäischen Kommission zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation[939] an.[940] Die dort vorgeschlagene Meldepflicht für Sicherheitsverletzungen wiederum soll mögliche wirtschaftliche Schäden oder soziale Nachteile vermeiden, die sich aus solchen Sicherheitsverletzungen ergeben.[941] Diesen Regelungszweck wiederholt die Gesetzesbegründung und nennt beispielhaft für materielle Schäden die Erlangung von Kreditkarteninformationen oder für soziale Nachteile den Identitätsbetrug.[942]

Ein Abwehranspruch gegen den privaten Dritten findet sich auch nicht in den §§ 33-35 BDSG des mit „Rechte des Betroffenen" überschriebenen zweiten Unterabschnitts des dritten Abschnitts des BDSG. Dort sind lediglich Rechte des Betroffenen auf Benachrichtigung (§ 33 BDSG), Auskunft (§ 34 BDSG) sowie Berichtigung, Löschung und Sperrung von Daten (§ 35 BDSG). Die Vorschrift des § 33 BDSG sollte im Rahmen der gesetzgeberischen Umsetzung des *Volkszählungsurteils* für mehr Transparenz bei der Datenverarbeitung sorgen und damit die Rechtsausübung des Betroffenen erleichtern.[943] Es wurden damit die im *Volkszählungsurteil* geforderten, verfassungsrechtlich zu gewährleistenden Verfahrensanforderungen umgesetzt.[944] Denn erst die Auskunft über gespeicherte personenbezogene Daten ermöglicht die Ausübung der Rechte aus §§ 34, 35 BDSG.[945] Damit liegt den Rechten des Betroffenen aber ein Inhalt zugrunde, der sich allein aus den verfassungsrechtlichen Vorgaben des *RiS* ergibt.

Der in § 7 BDSG geregelte Schadensersatzanspruch schließlich setzt, soweit es um den Anwendungsbereich des BDSG geht, eine nach dem BDSG unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung personenbezogener Daten

---

[939] Vorschlag für eine Richtlinie des *Europäischen Parlaments* und des *Rates* zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz vom 13.11.2007, KOM (2007) 698 endgültig.

[940] BT-Drucks. 16/12011, S. 34.

[941] Vorschlag für eine Richtlinie des *Europäischen Parlaments* und des *Rates* zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz vom 13.11.2007, KOM (2007) 698 endgültig, S.12.

[942] BT-Drucks. 16/12011, S. 34.

[943] BT-Drucks. 11/4306, S. 51; ebenso *Gola/Schomerus*, BDSG, § 33 Rn. 1. *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 2, § 33 Rn. 9.

[944] *Dix*, in: *Simitis* (Hrsg.), BDSG, § 33 Rn. 2; *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 2, § 33 Rn. 10.

[945] *Dix*, in: Simitis (Hrsg.), BDSG, § 33 Rn. 1; *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 2, § 33 Rn. 9.

des Betroffenen voraus. Der Anspruch ist daher von vornherein auf Daten mit Personenbezug beschränkt. Reine Sachdaten außerhalb des § 3 Abs. 1 BDSG werden nicht erfasst. Der Schutzbereich des *GVIiS* ist demgegenüber nicht vom tatsächlichen Vorhandensein personenbezogener Daten abhängig. Der Begriff ist insofern nicht schutzbereichseröffnend, da Personenbezug nicht deckungsgleich mit dem Schutz der selbstbestimmten Verfügung über das eigengenutzte informationstechnische System ist.[946] Eine erkennbar abschließende Regelung auch des technischen Zugriffs auf ein informationstechnisches System liegt hierin nicht. Zudem sind über § 7 BDSG nach wohl h.M. nur materielle Schäden ersatzfähig.[947] Die Regelung geht auf die Umsetzung des Art. 23 EG-Datenschutzrichtlinie zurück.[948] Deren Gegenstand ist aber gerade „insbesondere der Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten" (Art. 1 Abs. 1). Anhand dieses Schutzgegenstands ist auch die Reichweite der Haftung nach Art. 23 EG-Datenschutzrichtlinie zu bestimmen.[949] Entsprechendes muss dann auch für die Auslegung des § 7 BDSG gelten. Dieser Schutzgegenstand wiederum entspricht nicht der Konzeption des Persönlichkeitsschutzes, der dem *GVIiS* zugrunde liegt.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nach § 4 Abs. 1 BDSG nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Unter einem Erheben ist dabei das Beschaffen von Daten über den Betroffenen zu verstehen (§ 3 Abs. 3 BDSG), Verarbeiten wird als das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten (§ 3 Abs. 4 S. 1 BDSG) und Nutzen als jede Verwendung personenbezogener Daten definiert, soweit es sich nicht um Verarbeitung handelt (§ 3 Abs. 5 BDSG). Fehlt die Einwilligung des Betroffenen entscheidet mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nicht der Nutzer des informationstechnischen Systems über die Zugänglichkeit der Daten, sondern die erhebende, verarbeitende oder nutzende Stelle. Das Interesse des Nutzers eines informationstechnischen Systems an der Vertraulichkeit der erzeugten, verarbeiteten und gespeicherten personenbezogenen Daten wird insofern zwar von dem Schutz vor dem unbefugten Umgang mit personenbezogenen Daten durch das BDSG erfasst. Sein Interesse geht aber darüber hinaus. Denn die Entscheidung über den Zugang zu den auf einem informationstechnischen System enthaltenen Daten verliert der Betroffene schon dann, wenn der technische Zugriff auf das informationstechnische System ermöglicht wurde, dieser Zugriff aber als vorgelagerte Handlung noch nicht mit den vorbenannten Verarbeitungsphasen erfasst werden kann. Die Integrität des informati-

946 Siehe hierzu bereits oben S. 86.

947 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 7 Rn. 32; *Gola/Schomerus*, BDSG, § 7 Rn. 12f.; *Däubler*/Klebe/Wedde/Weichert, BDSG, § 7 Rn. 19f.; Taeger/*Gabel* (Hrsg.), § 7 BDSG Rn. 10f.; a.A. *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 7 BDSG Rn. 12.

948 BT-Drucks. 14/4329, S. 38.

949 Vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 23 Rn. 2.2.

onstechnischen Systems kann somit ebenfalls nur insofern vom Schutz des BDSG erfasst werden, als diese sich mit dem Schutz personenbezogener Daten vor unbefugtem Umgang deckt.

Die Nutzung von „Speicherinhalten" lässt sich unter den gleichlautenden Begriff des § 3 Abs. 5 BDSG fassen, wonach Nutzen jede Verwendung personenbezogener Daten außer ihrer Verarbeitung ist. Die „Manipulation" des Systems fällt, sofern es um die inhaltliche Umgestaltung personenbezogener Daten also die Änderung ihres Informationswerts[950] geht, unter den Begriff der Veränderung des § 3 Abs. 4 S. 2 Nr. 2 BDSG. Beinhaltet die „Manipulation" das Löschen personenbezogener Daten, greift § 3 Abs. 4 S. 2 Nr. 5 BDSG. Jedoch ist die Integrität des informationstechnischen Systems ausdrücklich auch schon dann angetastet, wenn auf das System so zugegriffen wird, „*da*ss dessen Leistungen, Funktionen und Speicherinhalte […] genutzt werden *können*".[951] Die Integrität des informationstechnischen Systems wird schon dann aufgehoben, wenn bloß „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen wird".[952] Wie auch beim Schutzgegenstand der Vertraulichkeit setzt der Schutz der Integrität schon an, bevor das BDSG greift, nämlich vor einer Datenverarbeitung i.w.S. Die Nutzung von „Leistungen" und „Funktionen" des informationstechnischen Systems werden hingegen vom BDSG nicht erfasst. „Ausspähung" und „Überwachung" des Systems lassen sich wiederum insoweit unter den Schutz des BDSG fassen, als diese mit der Erhebung personenbezogener Daten i.S.d. § 3 Abs. 3 BDSG verbunden sind.

Der bloße technische Zugriff auf das informationstechnische Systems als Beseitigung der „entscheidenden technischen Hürde" wird jedoch ebenso wenig vom BDSG erfasst, wie die fortdauernde Aufhebung der Vertraulichkeit und Integrität des informationstechnischen Systems infolge der Infiltration. Sofern sich Eingriffe in den Schutzbereich des *GVIiS* somit nicht mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten decken, belässt das BDSG eine Schutzlücke gegenüber dem Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme hinsichtlich der Übergriffe Privater. Das BDSG ist damit aber weiter auch nicht abschließend hinsichtlich der Erhebung, Verarbeitung und Nutzung personenbezogener Daten *infolge* der Infiltration eines informationstechnischen Systems. Eine solche Datenverarbeitung bildet mit der vorangegangenen Infiltration eine zusammenhängende Persönlichkeitsverletzung, deren aufeinanderfolgende Einzelschritte sich gegenseitig bedingen. Diese zusammenhängende Verletzung geht in ihrer Relevanz für die Persönlichkeit des Einzelnen über die punktuelle Verletzung seines *RiS* hinaus. Letztere kann daher nicht isoliert von der Infiltration des Systems betrachtet werden. Die Infiltration des informationstechnischen Systems selbst ist aber gerade nicht Regelungsgegenstand des BDSG.

---

950 *Gola/Schomerus*, BDSG, § 3 Rn. 30.
951 *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).
952 *BVerfGE* 120, 274 (314).

Aufgrund des für den Anwendungsbereich des BDSG zentralen Begriffs des personenbezogenen Datums kommt das BDSG erst bei der sich an die Infiltration anschließende Datenerhebung zur Anwendung. In diesem Zeitpunkt wurde aber bereits in den Schutzbereich des *GVIiS*, der insofern demjenigen des *RiS* vorgelagert ist, eingegriffen. Die Zulässigkeit der Datenverarbeitung nach Maßgabe des *GVIiS* würde somit erst geprüft, wenn eine Beeinträchtigung bereits vorliegt, nicht aber im Vorfeld des Eingriffs. Vergleichbar der Kritik an der Ausgestaltung des Kernbereichsschutzes bei staatlichen Eingriffen in den Schutzbereich des *GVIiS* käme es zunächst zu einer Beeinträchtigung des Persönlichkeitsrechts des Betroffenen, die erst im Anschluss an die Beeinträchtigung verlässlich auf die Möglichkeit der Rechtfertigung geprüft werden könnte, ohne dass bereits erfolgte Informationserhebungen rückgängig zu machen wären. Es fehlt aber im Regelfall an technischen Mitteln, den Zugriff auf das informationstechnische System allein auf die benötigten Daten zu beschränken. Selbst wenn im Anschluss an den Zugriff nur solche Daten erhoben würden, bliebe die Gefährdung der Persönlichkeit des Betroffenen durch die Möglichkeit vollumfänglicher Überwachung außer Acht. Daher ist bereits die Anwendbarkeit der Erlaubnistatbestände des BDSG für die Datenverarbeitung durch nichtöffentliche Stellen insgesamt fraglich. Zwar ist das *GVIiS* nicht schrankenlos,[953] so dass es dem Gesetzgeber freistünde, Erlaubnistatbestände für die private Datenverarbeitung zu schaffen. Insoweit fehlt es aber im BDSG an einer Entscheidung des Gesetzgebers, die den Schutzbereich des *GVIiS* in seiner objektiv-rechtlichen Gestalt berücksichtigt.

Überdies stünden der Datenerhebung aus informationstechnischen Systemen mittels eines technischen Zugriffs die schutzwürdigen Interessen des Betroffene gem. § 28 Abs. 1 Nr. 2 BDSG entgegen.[954] Der Begriff ist anhand des Schutzziels des § 1 Abs. 1 BDSG zu bestimmen.[955] Entscheidender Anhaltspunkt ist hierbei die spezifische Verarbeitungssituation, aus der die Konsequenzen für den Betroffenen zu entnehmen sind.[956] Diese Konsequenzen können bei dem technischen Zugriff auf ein informationstechnisches System zu einer weitgehenden Profilbildung des Betroffenen führen.[957] Schon das *RiS* steht der Ausweitung der Datenerhebung auf detaillierte Informationen über persönliche Gewohnheiten und Verhaltensweisen und der minutiösen Rekonstruktion des täglichen Verhaltens des Betroffenen entgegen.[958] Insbesondere ist der Kernbereich privater Lebensgestaltung zu wahren, schon bei dem ersten Anschein der Datenerhebung aus

---

953 *BVerfGE* 120, 274 (315).

954 Für die Berücksichtigung des *GVIiS* als „schutzwürdiges Interesse" schon *Roßnagel/Schnabel*, NJW 2008, 3534 (3538); *Wedde*, AuR 2009, 373 (377f.).

955 *Gola/Schomerus*, BDSG, § 28 Rn. 26; *Bergmann/Möhrle/Herb*, § 28 Rn. 236; vgl. auch *BGH* NJW 1984, 436 (437); NJW 1984, 1889 (1890).

956 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 28 Rn. 127.

957 *BVerfGE* 120, 274 (305).

958 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 28 Rn. 138f.

diesem Bereich liegt daher die Abwägung zugunsten des Betroffenen nahe.[959] Gleiches muss sodann für den potentiell zu erlangenden Bestand an personenbezogenen Daten bei dem technischen Zugriff auf ein informationstechnisches System gelten. Hierfür spricht insbesondere die Feststellung des *BVerfG*, dass informationstechnische Systeme nach den „gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität" genutzt würden.[960]

Zentrales Schutzinstrument des BDSG ist zudem der Begriff des personenbezogenen Datums, vgl. § 1 Abs. 1 BDSG. Der Begriff bestimmt damit aber zugleich auch den Anwendungsbereich des Gesetzes.[961] Der Schutz der Persönlichkeit des Einzelnen wird abschließend nur insoweit geregelt, als er sich über den Schutz personenbezogener Daten realisieren lässt.[962] Der Begriff müsste demnach auch den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme vollständig erfassen können. Problematisch ist dabei bereits das Merkmal des Personenbezugs. Der Schutzbereich des *GVIiS* ist zwar ohnehin nur dann eröffnet, wenn der Betroffene das informationstechnische System „als eigenes nutzt", so dass der Personenbezug der mit der Nutzung des Systems anfallenden personenbezogenen Daten regelmäßig zu dem Betroffenen bestehen wird. Das BDSG ist hingegen auf reine Sachdaten von vornherein nicht anwendbar. Der Schutz des Interesses des Nutzers, „dass die von einem vom Schutzbereich [des GVIiS] erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten *Daten* vertraulich bleiben",[963] ist aber nicht auf Daten mit Personenbezug beschränkt. Der Schutzbereich des *GVIiS* ist zwar nur dann eröffnet, wenn eine besondere persönlichkeitsrechtliche Gefährdungslage dahingehend ausgemacht werden kann, dass auf dem betroffenen informationstechnischen System „*personenbezogene Daten* des Betroffenen in einem Umfang und in einer Vielfalt enthalten [sein] 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".[964] Der Begriff des personenbezogenen Datums wird in der Beschreibung dieser Gefährdungslage jedoch nur insofern schutzbereichseröffnend verwendet, als es um die Komplexität des informationstechnischen Systems mithin seinen Funktionsumfang geht. Das System muss lediglich die Eignung aufweisen, einen umfangreichen und vielfältigen Bestand an personenbezogenen Daten zu umfassen. Tatsächlich muss ein solcher Datenbestand nicht vorliegen. Die Abhängigkeit der Eröffnung des Anwendungs-

[959] *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 28 Rn. 238.
[960] *BVerfGE* 120, 274 (323).
[961] BT-Drucks. 7/1027, S. 22.
[962] BT-Drucks. 7/1027, S. 22.
[963] *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).
[964] *BVerfGE* 120, 274 (314) (Hervorhebung nur hier).

bereichs des BDSG vom Vorliegen eines personenbezogenen Datums entspricht damit nicht der Konzeption des Schutzes der selbstbestimmten Verfügung über das eigengenutzte informationstechnische System.

iii. Schutzzweck

Das BDSG verfolgt den Zweck, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem (verfassungsrechtlichen[965]) Persönlichkeitsrecht beeinträchtigt wird (vgl. § 1 Abs. 1 BDSG). Schon der pauschale Bezug auf das Persönlichkeitsrecht sei missverständlich, da konkret die informationelle Selbstbestimmung vor Beeinträchtigungen geschützt werden soll.[966] § 1 Abs. 1 BDSG 1977 sprach noch davon, „der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken". Dieser Schutzzweck wurde in § 1 Abs. 1 BDSG 1990[967] zu dem Schutz des Einzelnen davor, dass er […] „in seinem Persönlichkeitsrecht beeinträchtigt wird". Die Neufassung des BDSG diente dabei insbesondere der Umsetzung des *Volkszählungsurteils*[968], wobei nunmehr das Persönlichkeitsrecht als das Grundrecht geschützt wurde, „dem das Recht auf informationelle Selbstbestimmung immanent ist".[969]

Der Begriff des „Umgangs" wird im BDSG nicht definiert. Mithin ließe sich zunächst grds. auch der Zugriff auf ein informationstechnisches System unter den Begriff fassen. Denn aus dem Zugriff ergibt sich entgegen des Nutzerwillens der Zugang zu den auf dem System enthaltenen personenbezogenen Daten. Den Anwendungsbereich de BDSG konkretisiert § 1 Abs. 2 BDSG hingegen auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten (§ 1 Abs. 2 BDSG. Dementsprechend regelt § 4 Abs. 1 BDSG auch nur die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Erlaubnis oder Anordnung nach dem BDSG oder einer anderen Rechtsvorschrift oder durch die Einwilligung des Betroffenen. Der weite Begriff des „Umgangs" beruht damit weniger auf der gesetzgeberischen Absicht einer umfassenden Regelung, als vielmehr auf der Entstehungsgeschichte der Norm.[970] Er stellt den Oberbegriff für die in § 3 Abs. 4 und 5 BDSG definierten Datenverarbeitungen i.w.S. dar.[971] Selbst wenn man den Begriff des „Umgangs" mit personenbezogenen Daten auf technische und organisatorische Maßnahmen nach § 9 BDSG erstreckt,[972] erweitert sich der Anwendungsbereich des BDSG dadurch nicht auf die Schutzgegen-

965 Vgl. *Gola/Schomerus*, BDSG, § 1 Rn. 6.
966 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 1 Rn. 25; *Bergmann/Möhrle/Herb*, BDSG, Bd. 1, § 1 Rn. 7.
967 Bundesdatenschutzgesetz (BDSG) vom 20.12.1990, BGBl. I S. 2954.
968 BT-Drucks. 11/4306, S. 35.
969 BT-Drucks. 11/4306, S. 39.
970 *Simitis*, in: *Ders.* u.a. (Hrsg.), BDSG, 4. Aufl., § 1 Rn. 187.
971 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 1 Rn. 76; *Gola/Schomerus*, BDSG, § 1 Rn. 22; Däubler/Klebe/Wedde/*Weichert*, BDSG, § 1 Rn. 7.
972 So *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 1 Rn. 76; dem folgend Taeger/Gabel-*Schmidt*, § 1 BDSG Rn. 6.

stände der Vertraulichkeit und Integrität. Denn die Norm ist nicht Ausdruck der selbstbestimmten Verfügung über das eigene informationstechnische System. Mithin müsste sich die Beeinträchtigung der Vertraulichkeit und/oder Integrität informationstechnischer Systeme abschließend mit den Begriffen der Erhebung, Verarbeitung und Nutzung erfassen lassen.

iv. Zusammenfassung

Eine abschließende Regelung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme enthält das BDSG danach nicht.[973] Sein Schutz ist allein auf das *RiS* ausgerichtet. Das Gesetz verwendet demnach das personenbezogene Datum als zentrales Regelungsinstrument. Mit diesem Begriff lässt sich jedoch der Inhalt des *GVIiS* nicht vollständig abbilden. Einen individuellen Abwehranspruch, der speziell auf die Beeinträchtigung der Vertraulichkeit und Integrität informationstechnischer Systeme ausgerichtet ist, sieht das BDSG nicht vor. Mithin kann auch § 28 BDSG keine taugliche Rechtsgrundlage für den Zugriff auf ein informationstechnisches System durch einen privaten Dritten bieten.

b. § 823 Abs. 1, 2 BGB

Mangels abschließender Regelung durch das BDSG ist damit der Rückgriff auf § 823 BGB eröffnet. Einzelnen konkreten Eingriffsmodalitäten kann mit dem Schutz der benannten Rechte des § 823 Abs. 1 BGB sowie Normen des StGB als Schutzgesetze i.S.d. § 823 Abs. 2 BGB begegnet werden. Entscheidender ist hingegen die Umsetzung der sich aus dem objektiv-rechtlichen Inhalt des *GVIiS* ergebenden Schutzpflicht durch Anerkennung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme als Teil des privatrechtlichen allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB.

i. § 823 Abs. 1 BGB

Nach § 823 Abs. 1 BGB ist derjenige, der vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.

(1) Eigentum

Einzelne Schutzgehalte des *GVIiS* lassen sich dabei zunächst über das Rechtsgut des Eigentums verwirklichen. Zivilrechtliches Eigentum kann jedoch wie oben bereits angesprochen nur an Sachen bestehen (vgl. § 903 S. 1 BGB), so dass eine Eigentumsverletzung stets einen körperlichen Gegenstand voraussetzt (§ 90 BGB). Der deliktsrechtliche Eigentumsschutz kann somit den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme von vornherein nur inso-

[973] So auch *Härting/Schneider*, ZRP 2011, 233 (235); *Kutscha*, DuD 2012, 391 (394).

weit erfassen, als das informationstechnische System Sachqualität aufweist und der Betroffene hieran Eigentum hat. Eigentum kann abgesehen von der Entziehung oder der Belastung des Eigentumsrechts sowie der nachteiligen Einwirkung auf den jeweiligen körperlichen Gegenstand durch jede sonstige Störung der Nutzbarkeit der Sache verletzt werden.[974] Eine Eigentumsverletzung ist daher auch die nicht unerhebliche Beeinträchtigung der bestimmungsgemäßen Verwendung der Sache.[975]

Ein körperlicher Gegenstand i.S.d. § 90 BGB sind jedenfalls die Speichermedien des informationstechnischen Systems. Die Funktion von Datenträgern liegt neben der Aufnahme von Daten auch darin, die aufgenommenen Daten zu bewahren und wiederzugeben.[976] Kommt es zu einem Datenverlust, wird der Eigentümer darin gehindert, mit dem Datenträger seinem Wunsch entsprechend (§ 903 S. 1 BGB) zu verfahren.[977] Die Veränderung oder Löschung der auf einem Datenträger gespeicherten Informationen ist somit eine Eigentumsverletzung i.S.d. § 823 Abs. 1 BGB.[978] Daneben kommt aber noch eine Beeinträchtigung der Funktionsfähigkeit des informationstechnischen Systems selbst in Betracht. Eine solche Eigentumsverletzung könnte darin liegen, dass die Infiltration des informationstechnischen Systems zwar nicht zu Datenlöschungen, wohl aber zu Fehlern in den Programmabläufen des Betriebssystems und der auf dem System installierten Software führt. Bewirken diese eine derartige Funktionsstörung des informationstechnischen Systems, dass die Verwendungsfähigkeit praktisch aufgehoben wird,[979] dürfte von einer nicht unerheblichen Beeinträchtigung der bestimmungsgemäßen Verwendung auszugehen sein.[980] Der zivilrechtliche Eigentumsschutz erfasst damit die „Manipulation" des informationstechnischen Systems, setzt aber notwendig das Eigentum des Betroffenen hieran voraus.[981]

---

974 MüKoBGB-*Wagner*, § 823 Rn. 102.

975 *BGH* NJW 1994, 517 (518) m.w.N.; NJW 1998, 1942 (1943) m.w.N.

976 *Bartsch*, CR 2000, 721 (723).

977 *OLG Karlsruhe* NJW 1996, 200 (201); kritisch *Meyer/Wehlau*, NJW 1998, 1585 (1588): Wegen physikalischer Messbarkeit der Veränderung der Magnetisierung einer Festplatte sei schon die Sachsubstanz des Datenträgers betroffen.

978 *OLG Karlsruhe* NJW 1996, 200 (201); MüKoBGB-*Wagner*, § 823 Rn. 103; Staudinger/*Hager* (1999), § 823 Rn. B60 („Software"); *Bartsch*, CR 2000, 721 (723); *Taeger*, Außervertragliche Haftung, S. 261.

979 Vgl. MüKoBGB-*Wagner*, § 823 Rn. 118.

980 I.E. ebenso *Koch*, NJW 2004, 801 (802); zur Problematik der Übertragung der Rechtsprechung zum weiterfressenden Mangel auf Softwaremängel *Abel*, CR 1999, 680 (682); *Spindler*, NJW 1999, 3737 (3738); *ders.*, NJW 2004, 3145 (3146). Anders als dort geht es hier aber nicht um Mängel der Software, sondern um einen gänzlich außerhalb eines etwaigen Äquivalenzinteresses gelegenen zielgerichteten Angriffs auf die Integrität des allgemeinen Persönlichkeitsrechts.

981 Auch wegen dieser Einschränkung bestünde Bedarf nach der Anerkennung eines „Rechts am eigenen Datenbestand" als sonstiges Recht i.S.d. § 823 Abs. 1 BGB, so Bamberger/Roth/*Spindler*, § 823 Rn. 93; ebenso für eine Anerkennung *Meyer/Wehlau*, NJW 1998, 1585 (1588f.); *Faustmann*, VuR 2006, 260 (262).

(2) Allgemeines Persönlichkeitsrecht

Der privatrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme kann sich schließlich auch aus dem allgemeinen Persönlichkeitsrecht des § 823 Abs. 1 BGB ergeben.

(a) Bild- und Tonaufnahmen

Die Infiltration eines informationstechnischen Systems zur Überwachung des Nutzers mittels der Peripheriegeräte wie Mikrofon oder Kamera stellt nur dann einen Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG und nicht in denjenigen des *GVIiS* dar, soweit Gegenstand der Überwachung Vorgänge innerhalb einer als Wohnung geschützten Räumlichkeit sind. Außerhalb einer solchen Räumlichkeit greift die Spezialität des besonderen Freiheitsrechts nicht, so dass hier der Schutzbereich des *GVIiS* eröffnet wäre. Greift der Dritte auf die Peripheriegeräte des informationstechnischen Systems zu, so nutzt er jedenfalls Leistungen und Funktionen des Systems und manipuliert das System dahingehend.

Schutz gegen die Überwachung des Nutzers mittels des Mikrofons eines informationstechnisches Systems besteht durch § 823 Abs. 1 BGB insoweit, als der Schutzbereich des *Rechts am eigenen Wort* als Ausprägung des allgemeinen Persönlichkeitsrechts reicht. Dieses Recht schützt den Einzelnen darin, selbst über die Zugänglichkeit seiner Worte und deren Festhalten auf einem Tonträger zu entscheiden.[982] Infolge der Aufzeichnung wird auch ein aus der Spontaneität heraus formulierter Gedanke durch die Möglichkeit der jederzeitigen Abrufbarkeit und Wiederholbarkeit objektiviert.[983] Für mündliche Äußerungen ist hingegen das Bewusstsein der Flüchtigkeit des gesprochenen Wortes und seiner jederzeitigen Korrigierbarkeit charakteristisch.[984] Die Aufzeichnung und das Abspielen einer Aufzeichnung gegenüber Dritten setzen daher grundsätzlich die Einwilligung des Betroffenen voraus.[985] Diese Entscheidungsbefugnis über die Zugänglichkeit der eigenen Worte ist aber auch beim bloßen Mithören durch einen Dritten betroffen.[986] Anknüpfungspunkt ist jedoch allein das gesprochene Wort. Sofern dieses nicht Gegenstand der ungewollten Aufzeichnung oder Wahrnehmung Dritter ist, kann auch die zur Überwachung notwendige Infiltration des informationstechnischen Systems nicht vom Schutz des *Rechts am gesprochenen Wort* erfasst werden.

Die Herstellung von Bildnissen ohne Zustimmung des Betroffenen stellt einen Eingriff in das *Recht am eigenen Bild* als Ausprägung des durch § 823 Abs. 1 BGB geschützten allgemeinen Persönlichkeitsrechts dar.[987] Danach steht allein dem Abgebildeten die Entscheidung zu, ob und in welcher Weise er anderen gegenüber

[982] *BGH* NJW 1958, 1344; NJW 1982, 277.
[983] *BGH* NJW 1988, 1016 (1017).
[984] *BGH* NJW 1988, 1016 (1017).
[985] *BGH* NJW 1979, 647 (648) m.w.N.; NJW 1982, 277; NJW 1988, 1016 (1017).
[986] *BGH* NJW 2003, 1727 (1728).
[987] *BGH* NJW 1957, 1315 (1316); NJW 1995, 1955 (1956).

bildlich dargestellt wird.[988] Diese Entscheidung betrifft insbesondere die Anfertigung von Videoaufnahmen.[989] Schutz gegen die Infiltration informationstechnischer Systeme kann demnach aber auch nur insoweit durch das *Recht am eigenen Bild* bestehen.

(b) Zugriff auf ein informationstechnisches System

Der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme lässt sich über das *BDSG* nicht umfassend realisieren. Dessen Schutzkonzept basiert auf dem Begriff des personenbezogenen Datums. Allein mit diesem Begriff lässt sich das informationstechnische System als besondere technische Privatheitssphäre nicht umschreiben. Die Persönlichkeitsrelevanz, die mit dem Eindringen in diese Sphäre verbunden ist, lässt sich in den wenigsten Fällen nur mit dem Personenbezug eines Datums gleichsetzen. Der Zugang zu reinen Sachdaten bliebe überdies vollkommen unberücksichtigt. Der Eigentumsschutz des § 823 Abs. 1 BGB erfasst nur unter bestimmten Voraussetzungen und selbst dann auch nur einzelne Aspekte der Vertraulichkeit und Integrität. Die besonderen Ausprägungen des allgemeinen Persönlichkeitsrechts in Form der Rechte am gesprochenen Wort und am eigenen Bild erfassen ebenfalls nur bestimmte Eingriffsmodalitäten. Der Zugriff auf ein informationstechnisches System selbst, mithin nach den Worten des *BVerfG* die „technische Infiltration“[990] und „Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben“,[991] werden demgegenüber nicht erfasst. Ein von bestimmten Eingriffsmodalitäten unabhängiger Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme insgesamt ist auf privatrechtlicher Ebene bisher nicht ausdrücklich formuliert worden.

Eine solche Formulierung kommt auf zweierlei Weise in Betracht: Zunächst ist anhand des Schutzbereichs des privatrechtlichen Allgemeinen Persönlichkeitsrechts zu prüfen, ob und inwieweit dieser auch den Schutz des eigengenutzten informationstechnischen Systems umfasst.[992] Im Anschluss stellt sich dann die

988 *BGH* NJW 1996, 1128 (1129) m.w.N.; NJW 1974, 1947 (1948f.); NJW-RR 1987, 231; NJW 1992, 2084.

989 *BGH* NJW 1995, 1955 (1956).

990 *BVerfGE* 120, 274 (276).

991 *BVerfGE* 120, 274 (315).

992 Hierfür, jedoch ohne nähere und dogmatische Begründung, *Herrmann*, IT-Grundrecht, S. 188; Palandt/*Sprau*, § 823 Rn. 112; *Roßnagel/Schnabel*, NJW 2008, 3534 (3536); für einen Schadensersatzanspruch aus § 823 Abs. 1 BGB unter Verweis auf die erstmalige zivilrechtliche Formulierung als Entstehungshintergrund des verfassungsrechtlichen allgemeinen Persönlichkeitsrechts auch *Kutscha*, DuD 2012, 391 (393).

Frage nach der Notwendigkeit, den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme als ein weiteres und eigenes sonstiges Recht des § 823 Abs. 1 BGB anzuerkennen.[993]

(i) Persönlichkeitsrechtliche Schutzpflichten

Das verfassungsrechtliche allgemeine Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verpflichtet den Staat, den Einzelnen vor Gefährdungen dieses Rechts durch private Dritte zu schützen.[994] Verfassungsdogmatische Grundlage des allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB ist daher die sich aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ergebende Schutzpflicht des Staates.[995] Aus dieser Verpflichtung folgt die Subsumtion des Schutzbereichs des *GVIiS* unter das Allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB. Denn gerade letzteres dient im privatrechtlichen Bereich dem in den Art. 2 Abs. 1 und Art. 1 Abs. 1 GG enthaltenen Persönlichkeitsschutz.[996] Der Schutzbereich des allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB stellt die Umsetzung dieser grundrechtlichen Wertungen dar.[997] Wie das verfassungsrechtliche Persönlichkeitsrecht füllt das allgemeine Persönlichkeitsrecht aus § 823 Abs. 1 BGB Lücken im Schutz der Persönlichkeit, die neben anerkannten einzelnen Persönlichkeitsrechten verbleiben.[998] Denn soweit sich die aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ergebende Schutzpflicht die Gerichte trifft, haben diese die dem Schutz der Persönlichkeit dienenden zivilrechtlichen Normen nach den grundrechtlichen Maßgaben anzuwenden.[999]

---

[993] Diesen Ansatz diskutieren etwa *Bartsch*, CR 2008, 613ff., und diesem folgend Bamberger/Roth/*Spindler*, § 823 Rn. 93.

[994] *BVerfGE* 114, 339 (346f.); vgl. auch *BVerfGE* 73, 118 (201); 97, 125 (146); 99, 185 (194f.).

[995] MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 2; *Canaris*, AcP 184 (1984) 201 (231); *ders.*, JuS 1989, 161 (169); *Götting*, in: *Ders./Schertz/Seitz* (Hrsg.), Hdb. Persönlichkeitsrecht, § 3 Rn. 6; *Larenz/Canaris*, Schuldrecht BT II/2, § 80 I 3a) (allerdings zweifelnd hinsichtlich der Notwendigkeit der Anerkennung eines „allgemeinen" Persönlichkeitsrechts).

[996] *BVerfGE* 34, 269 (281).

[997] *Baston-Vogt*, Persönlichkeitsrecht, S. 101.

[998] *BVerfGE* 34, 269 (281).

[999] *BVerfGE* 114, 339 (346f.); *BVerfG* NJW 2006, 595 a.E.; allg. auch *BVerfGE* 101, 361 (388); *BVerfG* NJW 2006, 3409 (3410).

(ii) Entwicklung des privatrechtlichen allgemeinen Persönlichkeitsrechts

In der sog. *Leserbrief-Entscheidung*[1000] erkannte der *BGH* entgegen der ständigen Rechtsprechung des *RG*[1001] erstmals unter Berufung auf Art. 1 und Art. 2 GG ein allgemeines Persönlichkeitsrecht als sonstiges Recht i.S.d. § 823 Abs. 1 BGB an.[1002] Die hierin und in den folgenden Entscheidungen benannten Schutzgehalte sind von dem Selbstbestimmungsrecht des Einzelnen geprägt.[1003] In der Leserbriefentscheidung kam dieses Selbstbestimmungsrecht in der Entscheidungshoheit über die Veröffentlichung eigener Aufzeichnungen zum Ausdruck. Jede sprachliche Festlegung eines bestimmten Gedankeninhalts sei Ausfluss der Persönlichkeit des Verfassers, so dass „grundsätzlich dem Verfasser allein die *Befugnis* zusteht, darüber zu *entscheiden*, ob und in welcher Form seine Aufzeichnungen der Öffentlichkeit zugänglich gemacht werden".[1004] Im Folgenden war das allgemeine Persönlichkeitsrecht maßgeblich für die Zulässigkeit der Veröffentlichung von Krankenakten.[1005] Dabei komme es entscheidend auf die „*Mißachtung des Willens* an, so höchstpersönliche Dinge wie die gesundheitliche Verfassung vor fremdem Einblick zu bewahren".[1006] In der *Herrenreiter-Entscheidung* umschrieb der *BGH* das allgemeine Persönlichkeitsrecht sodann als „jenen inneren Persönlichkeitsbereich, der grundsätzlich nur der *freien und eigenverantwortlichen Selbstbestimmung* des Einzelnen untersteht".[1007] In der *Soraya-Entscheidung* fasste der *BGH* unter das allgemeine Persönlichkeitsrecht das Recht der dortigen Klägerin „selbst darüber *zu bestimmen*, ob sie mit eigenen Äußerungen über ihre Privatsphäre öffentlich hervortreten wollte und, wenn sie diesen Wunsch hatte, in welcher Form dies geschehen sollte".[1008] Der Aspekt der Selbstbestimmung kommt sodann auch in der *Tonträger-Entscheidung* zum Ausdruck, wenn der *BGH* dort dem allgemeinen Persönlichkeitsrecht die Befugnis des Menschen zuordnet, „selbst darüber *zu bestimmen*, ob seine

---

1000 *BGHZ* 13, 334 (338): „Nachdem nunmehr das Grundgesetz das Recht des Menschen auf Achtung seiner Würde (Art. 1 GG) und das Recht auf freie Entfaltung seiner Persönlichkeit auch als privates, von jedermann zu achtendes Rechts anerkennt, […], muß das allgemeine Persönlichkeitsrecht als ein verfassungsmäßig gewährleistetes Grundrecht angesehen werden." Zur Kritik an dieser Begründung und der darin zum Ausdruck kommenden *unmittelbaren* Drittwirkung *Larenz/Canaris*, Schuldrecht BT II/2, § 80 I 3a).

1001 Siehe nur RGZ 69, 401 (403f.); 79, 397 (398).

1002 Verfassungsrechtliche Bedenken gegen diese Rechtsprechung hatte das *BVerfG* nicht, *BVerfGE* 34, 269 (281f.); nach *Kutscha*, DuD 2012, 391 (393), sei das *GVIiS* schon aufgrund der erstmaligen Formulierung eines „allgemeinen Persönlichkeitsrechts" im Zivilrecht auch auf die Wirkung gegenüber Privatpersonen angelegt (Hervorhebung nur hier).

1003 Ebenso *Ehmann*, in: FS Georgiades, S. 113 (140) sowie JURA 2011, 437 (438): „Befugnis der Selbstbestimmung"; MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 2: Schutz vor Gefährdung der „immateriellen Integrität und Selbstbestimmung".

1004 *BGHZ* 13, 334 (338f.) (Hervorhebung nur hier).

1005 *BGHZ* 24, 72.

1006 *BGHZ* 24, 72 (81).

1007 *BGHZ* 26, 349 (354).

1008 *BGH* NJW 1965, 685 (686).

Worte einzig seinem Gesprächspartner, einem bestimmten Kreis oder der Öffentlichkeit zugänglich sein sollen, und erst recht, ob seine Stimme mittels eines Tonträgers festgehalten werden darf".[1009] Allgemein umschreibt das Gericht dort den Schutzbereich des allgemeinen Persönlichkeitsrechts als die „dem Menschen in seinem inneren Persönlichkeitsbereich […] gebührende *Freiheit und Selbstbestimmung* […], die für die Entfaltung der Persönlichkeit unerläßlich ist".[1010]

(iii) Selbstbestimmung

Dieser Ansatz der Selbstbestimmung kommt gleichfalls im *GVIiS* zum Ausdruck. Schutzbereichseröffnend ist gerade, dass „der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System *selbstbestimmt verfügt*".[1011] Das *GVIiS* schützt einen individuellen Zustand von Vertraulichkeit und Integrität und damit die selbstbestimmte Verfügung über das eigene informationstechnische System. Der Privatsphärenschutz des § 823 Abs. 1 BGB sichert jedermann „einen autonomen Bereich der eigenen Lebensgestaltung […], in der er seine Individualität unter Ausschluss anderer entwickeln und wahrnehmen kann".[1012] Solch einen autonomen Bereich stellt auch die technische Sphäre des eigenen informationstechnischen Systems dar. Das *BVerfG* formuliert den Schutz des „persönlichen und privaten Lebensbereich[s] […] vor staatlichem Zugriff im Bereich der Informationstechnik".[1013] Das *GVIiS* umfasst dahingehend die Befugnis des Einzelnen, selbst darüber zu entscheiden, wem er Zugriff auf die technische Privatsphäre gewährt, die er durch die selbstbestimmte Nutzung seines informationstechnischen Systems schafft. In dieses Selbstbestimmungsrecht greift ein, wer den vom Nutzer geschaffenen Grad an Vertraulichkeit und Integrität missachtet. Ein Dritter, der sich Zugang zu Informationen verschafft, die nach dem anzuerkennenden Willen des Betroffenen über einen beschränkten Personenkreis hinaus nicht weiter bekannt werden sollen, widersetzt sich dem Selbstbestimmungsrecht des Betroffenen und greift damit in dessen Persönlichkeitsrecht ein.[1014] Im Falle von Daten zeigt sich die zu missbilligende Nichtachtung fremder Selbstbestimmung etwa in dem Bruch „mechanischer Verriegelungen oder systemimmanenter Codes".[1015] Einen solchen anzuerkennenden Willen vermittelt die Nutzung des informationstechnischen Systems „als eigenes", aus der sich mit der damit verbundenen selbstbestimmten Verfügung die grundrechtlich anzuerkennende Ver-

[1009] *BGHZ* 27, 284 (286).
[1010] *BGHZ* 27, 284 (286).
[1011] *BVerfGE* 120, 274 (315) (Hervorhebung nur hier).
[1012] *BGHZ* 131, 332 (337).
[1013] *BVerfGE* 120, 274 (313).
[1014] MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 100.
[1015] MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 101.

traulichkeits- und Integritätserwartung ergibt.[1016] In dem Schutz dieses Selbstbestimmungsrechts kommt daher die auf privatrechtlicher Ebene allein zu berücksichtigende Abwehrfunktion[1017] des verfassungsrechtlichen allgemeinen Persönlichkeitsrechts zum Ausdruck.

(iv) Entwicklungsoffener Schutzbereich

Der Schutzbereich des allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB ist dabei wie derjenige des Rechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nicht abschließend. Der *BGH* stellte in der *Krankenakten*-Entscheidung fest,[1018] „daß der Begriff des allgemeinen Persönlichkeitsrechts von generalklauselartiger Weite und Unbestimmtheit ist. Wie sich das Wesen der Persönlichkeit mit ihrer Dynamik nicht in feste Grenzen einschließen läßt, so ist auch das allgemeine Persönlichkeitsrecht seinem Inhalte nach *nicht abschließend festzulegen*." Das Gericht hat den privatrechtlichen Persönlichkeitsschutz in der Leserbriefentscheidung nicht über die Anerkennung bloß einzelner Persönlichkeitsgüter, sondern mittels eines umfassenden allgemeinen Persönlichkeitsrechts formuliert.[1019] Der Schutzbereich des allgemeinen Persönlichkeitsrechts ist daher nicht abschließend. Für die Ausgestaltung als Generalklausel spricht die Möglichkeit der schnellen und effizienten Anpassung des Persönlichkeitsschutzes an neue Gefährdungen.[1020] Solche Gefährdungen sieht auch der *BGH* als entscheidend für die Rechtsentwicklung im Bereich des zivilrechtlichen Persönlichkeitsschutzes an. Er stellt dabei neben den sich seit Inkrafttreten des *BGB* veränderten sozialen auch auf technische Entwicklungen ab, die „ganz neue, für den Gesetzgeber schlechthin unvorsehbare Möglichkeiten einer Verletzung von Persönlichkeitsgütern" geschaffen hätten.[1021] Mit der Weiterentwicklung der technischen Möglichkeiten steige die Gefahr des Eindringens in die Bereiche von Privatheit, Vertraulichkeit und Intimität.[1022]

---

[1016] Vgl. *BVerfGE* 120, 274 (315).

[1017] MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 133; Erman/*Ehmann*, 12. Aufl., Anh § 12 Rn. 13, 268a; *ders*., in: FS Georgiades, S. 113 (127); *ders*., JURA 2011, 437 (444); ähnlich *Larenz/Canaris*, Schuldrecht BT II/2, § 80 II 6a), *Baston-Vogt*, Persönlichkeitsrecht, S. 127ff.: Kein Schutz der allgemeinen Handlungsfreiheit durch § 823 Abs. 1 BGB.

[1018] *BGHZ* 24, 72 (78) (Hervorhebung nur hier).

[1019] *BGHZ* 13, 334 (337f.); in nachfolgenden Entscheidungen bezeichnet der *BGH* das allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB daher auch als „Auffangtatbestand", *BGHZ* 50, 133 (143); 80, 311 (319); 91, 233 (238f).

[1020] Erman/*Klass*, Anh § 12 Rn. 11; *Larenz/Canaris*, Schuldrecht BT II/2, § 80 I 3b); *Baston-Vogt*, Persönlichkeitsrecht, S. 100.

[1021] *BGHZ* 39, 124 (131); ebenso *Canaris*, Grundrechte und Privatrecht, Ziff. VI. 2. b) bb); *Larenz/Canaris*, Schuldrecht BT II/2, § 80 I 2.

[1022] *Bamberger*/Roth, § 12 Rn. 93.

(v) Schutz des persönlichen Bereichs vor unbefugtem Eindringen

Die Bestimmung des Schutzbereichs des allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB erfolgt wohl am häufigsten anhand der Bildung von Fallgruppen.[1023] Mit im Einzelnen unterschiedlichen Bezeichnungen beschreibt eine dieser Fallgruppen den *Schutz des persönlichen Bereichs vor unbefugtem Eindringen*.[1024] Es wird hier zunächst die heimliche Anfertigung von Fotografien innerhalb des privaten Bereichs des Abgebildeten diskutiert. In den Schutzbereich des allgemeinen Persönlichkeitsrecht wird eingegriffen, wenn „die heimliche Festlegung der äußeren Erscheinung einer Person innerhalb ihres privaten Bereichs in der Absicht vorgenommen wird, das Bildnis der Öffentlichkeit zugänglich zu machen, ohne hierzu die Erlaubnis des Abgebildeten einzuholen".[1025] Ebenso wird innerhalb der Fallgruppe die heimliche Beobachtung der Ehefrau innerhalb der gemeinsamen Wohnung durch einen Dritten auf Veranlassung des Ehemannes[1026] angeführt. Der geschützte persönliche Bereich ist hingegen nicht auf den häuslichen Bereich beschränkt, sondern in die Privatsphäre des Abgebildeten greift auch außerhalb des eigenen häuslichen Bereichs ein, wer die „Arglosigkeit des Betreffenden, der sich unbeobachtet wähnt, für seine Zwecke ausnutzt. Das ist dann der Fall, wenn er den Betreffenden gleichsam durch das Schlüsselloch beobachtet und ihn auf diese Weise heimlich mit der Anfertigung von Bildnissen überrascht."[1027] Die mit der selbstbestimmten Verfügung über ein informationstechnisches System begründete Vertraulichkeits- und Integritätserwartung geht über diese Arglosigkeit noch hinaus, da es bei dem technischen Zugriff auf ein informationstechnisches System an der allgemeinen Zugänglichkeit der zu gewinnenden Informationen gerade fehlt. Eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts kann auch schon die Befürchtung darstellen, durch vorhandene Überwachungsgeräte beobachtet zu werden, wenn diese Befürchtung aufgrund konkreter Umstände als nachvollzieh-

---

[1023] So etwa *Bamberger*/Roth, § 12 Rn. 134ff.; Erman/*Klass*, Anh § 12 Rn. 94ff.; Erman/*Ehmann*, 12. Aufl., Anh § 12 Rn. 18ff.; *ders*., in: FS Georgiades, S. 113 (145ff.); *ders*. JURA 2011, 437 (439ff.); Jauernig/*Teichmann*, § 823 Rn. 70ff.; MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 45ff.; Staudinger/*Hager* (1999), § 823 Rn. C63ff.; *Götting*/*Schertz*/*Seitz* (Hrsg.), Hdb. Persönlichkeitsrecht, §§ 19ff.; *Larenz*/*Canaris*, Schuldrecht BT II/2, § 80 II; *Fuchs*/*Pauker*, Delikts- und Schadensersatzrecht, S. 42ff.; kritisch zu dieser Methode Soergel/*Beater*, § 823 Anh IV Rn. 34; *Baston-Vogt*, Persönlichkeitsrecht, S. 177f.

[1024] *Bamberger*/Roth, § 12 Rn. 140ff.; Erman/*Klass*, Anh § 12 Rn. 117, 122ff.; Erman/*Ehmann*, 12. Aufl., Anh § 12 Rn. 113; *ders*., FS Georgiades, S. 113 (146ff.); *ders*. JURA 2011, 437 (440f.); Jauernig/*Teichmann*, § 823 Rn. 74ff.; MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 89ff., der als Grundlage dieser Fallgruppe die private Sphäre autonomer Lebensgestaltung als traditionelles Schutzgut des Persönlichkeitsrechts nennt, Rn. 89; *Wanckel*, in: *Götting*/*Schertz*/*Seitz* (Hrsg.), Hdb. Persönlichkeitsrecht, § 19; *Larenz*/*Canaris*, Schuldrecht BT II/2, § 80 II 4; *Fuchs*/*Pauker*, Delikts- und Schadensersatzrecht, S. 43.

[1025] *BGHZ* 24, 200 (209).

[1026] *BGH* NJW 1979, 1848.

[1027] *BGHZ* 131, 332 (340).

bar und verständlich erscheint.[1028] Das *BVerfG* verweist insofern vergleichbar in der gegenständlichen Entscheidung zum *GVIiS* ausdrücklich auf die im *Volkszählungsurteil* geschilderten Gefährdungen der Persönlichkeitsentfaltung durch die andauernde Befürchtung staatlicher Überwachung.[1029] Einfluss auf das Verhalten des Einzelnen könne bereits der psychische Druck einer möglichen öffentlicher Anteilnahme haben.[1030] Schließlich wird unter der Fallgruppe auch die Zulässigkeit von Taschenkontrollen im Supermarkt gelistet. Solche Kontrollen bedeuten regelmäßig erhebliche Eingriffe in das allgemeine Persönlichkeitsrecht.[1031]
Der Fallgruppe lässt sich auch die technische Infiltration eines informationstechnischen Systems zuordnen.[1032] Der Dritte dringt gegen den Willen des Betroffenen und in aller Regel heimlich in denjenigen persönlichen Bereich des Betroffenen ein, den dieser durch die Nutzung des Systems zur Entfaltung seiner Persönlichkeit schafft. Die selbstbestimmte Verfügung des Nutzers über das informationstechnische System mit seinen zahlreichen Nutzungsmöglichkeiten lässt einen „virtuell-informationstechnischen Bereich freier Persönlichkeitsentfaltung“[1033] entstehen. Dieser Bereich ist nach Maßgabe der abwehrrechtlichen Funktion des allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG gegen das unbefugte Eindringen privater Dritter zu schützen.

Der so beschriebene Privatsphärenschutz darf jedoch nicht mit demjenigen des Grundgesetzes gleichgesetzt werden. Die Ausführungen des *BVerfG* zur Reichweite des Schutzes der Privatsphäre als Ausprägung des verfassungsrechtlichen allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hinsichtlich der Vertraulichkeit und Integrität informationstechnischer Systeme[1034] sind daher nicht auf die privatrechtliche Ebene zu übertragen. Die im Persönlichkeitsschutz des Grundgesetzes zu beachtenden Spezialitätsverhältnisse bestehen auf privatrechtlicher Ebene in dieser Form nicht. Hier gibt es keine der Systematik des Grundgesetzes entsprechenden speziellen Freiheitsrechte des Persönlichkeitsschutzes.[1035] Während das verfassungsrechtliche allgemeine Persönlichkeitsrecht dort verdrängt wird, wo spezielle Freiheitsrechte dem Schutz der Persönlichkeit dienen, schließt das privatrechtliche Persönlichkeitsrecht deren Elemente in den meisten Fällen ein.[1036] Dementsprechend hat der *BGH* die Zulässigkeit von Luftbildaufnahmen der Anwesen prominenter Personen an § 823 Abs. 1 BGB geprüft,[1037] ohne dass insoweit abzugrenzen war, ob durch die Aufnahmen in eine

[1028] *BGH* NJW 2010, 1533 (1534) m.w.N.
[1029] *BVerfGE* 120, 274 (305).
[1030] *BVerfGE* 65, 1 (42).
[1031] *BGHZ* 124, 39 (43f.); *BGH* NJW 1996, 2574 (2576).
[1032] Ebenso *Bamberger*/Roth, § 12 Rn. 142; Jauernig/*Teichmann*, § 823 Rn. 75.
[1033] *Murswiek*, in: *Sachs*, GG, Art. 2 Rn. 73c.
[1034] *BVerfGE* 120, 274 (311).
[1035] *Baston-Vogt*, Persönlichkeitsrecht, S. 124.
[1036] *Jarass*, NJW 1989, 857 (858).
[1037] *BGH* NJW 2004, 762; 2004, 766.

„räumliche Privatsphäre“[1038] i.S.d. Art. 13 Abs. 1 GG eingegriffen wird. In dem Fall des heimlichen Beobachtens der Ehefrau in der gemeinsamen Wohnung durch einen von dem Ehemann dort versteckten Dritten sah der *BGH* den mit der Unverletzlichkeit der Wohnung durch Art. 13 Abs. 1 GG geschützten persönlichen Bereich vom allgemeinen Persönlichkeitsrecht des § 823 Abs. 1 BGB umfasst an.[1039] Schließlich fasst der *BGH* auch den Inhalt des *RiS* auf privatrechtlicher Ebene unter den Schutzbereich des allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB.[1040] Die auf verfassungsrechtlicher Ebene bestehenden Konkurrenzverhältnisse und Abgrenzungen sind demnach nicht maßgeblich für die Umsetzung des privatrechtlichen Persönlichkeitsschutzes.

Der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme lässt sich danach mit der Fallgruppe des Eindringens in den persönlichen Lebensbereich erfassen. Dem *GVIiS* kann damit nach Maßgabe seines objektivrechtlichen Gehalts durch das allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB Geltung verschafft werden. Die grundsätzliche Gleichsetzung der privaten und geschäftlichen Nutzung des informationstechnischen Systems hinsichtlich der Persönlichkeitsgefährdung des Betroffenen[1041] ist dabei auch auf privatrechtlicher Ebene nachzuziehen. Diese Gleichsetzung knüpft nicht an spezifische Aspekte des Verhältnisses des Bürgers zum Staat an, sondern an die Eignung der zu gewinnenden Informationen für die Persönlichkeitsgefährdung. Die geschäftliche Nutzung des informationstechnischen Systems lässt sich nicht für jeden Sachverhalt mit dem Recht am eingerichteten und ausgeübten Gewerbebetrieb oder dem Geheimnisschutz des § 17 Abs. 2 Nr. 1a) UWG erfassen. Diese durch das *BVerfG* vorgesehene Gleichstellung ist auch dem allgemeinen Persönlichkeitsrecht des § 823 Abs. 1 BGB nicht gänzlich fremd. Der *BGH* unterstellte bereits die berufliche Sphäre dem privatrechtlichen Persönlichkeitsschutz.[1042] Der so definierte privatrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme setzt die entsprechende Rechtsanwendung voraus. Das *BVerfG* räumt der Rechtsprechung gerade im Zusammenhang mit der Entwicklung des allgemeinen Persönlichkeitsrecht des § 823 Abs. 1 BGB sogar die Befugnis zu „schöpferischer Rechtsfindung“ ein.[1043] Eine über den gegenwärtigen Schutzzweck des allgemeinen Persönlichkeitsrechts hinausgehende Rechtsfortbildung ist hingegen mit dem privatrechtlichen Schutz der Vertraulichkeit und Integrität des eigenen informationstechnischen Systems nicht verbunden. Es fehlt damit an dem Bedürfnis, neben

---

[1038] *BVerfGE* 89, 1 (12); 103, 142 (150f.); 120, 274 (309); *Papier*, in: *Maunz/Dürig*, GG, Bd. 2, Art. 13 Rn. 1.

[1039] *BGH* NJW 1970, 1848.

[1040] *BGHZ* 80, 311 (319); 89, 218 (226); 91, 233 (238); *BGH* NJW 1986, 2505 (2506f.); NJW 2010, 1035 (1036).

[1041] *BVerfGE* 120, 274 (314).

[1042] *BGHZ* 24, 200 (208) (Einzelhandelsgeschäft); 80, 25 (42) (Aufzeichnungen über Redaktionskonferenz); *BGH* NJW 1981, 1366 (1367) (Darstellung der beruflichen Tätigkeit).

[1043] *BVerfGE* 34, 269 (287).

dem allgemeinen Persönlichkeitsrecht ein weiteres speziell anhand des Schutzbereichs des *GVIiS* definiertes sonstiges Recht zu entwickeln. Es ist die Anerkennung sonstiger Rechtsgüter auf das verfassungsrechtlich Notwendige zu beschränken.[1044] Eine allgemeine deliktische Generalklausel hat der Gesetzgeber des BGB gerade nicht schaffen wollen.[1045]

Die weitere Konkretisierung des verfassungsrechtlichen Persönlichkeitsrechts durch die Formulierung des *GVIiS* ist nicht mit der Anerkennung eines sonstigen Rechts i.S.d. § 823 Abs. 1 BGB vergleichbar. Denn die einzelnen Ausprägungen des Rechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sind nicht wie das sonstige Recht des § 823 Abs. 1 BGB verselbständigte Rechte, sondern bloß tatbestandliche Konkretisierungen.[1046] Schon aufgrund der verschiedenen Adressaten und damit der unterschiedlichen Wirkung von verfassungs- und privatrechtlichem Persönlichkeitsrecht scheidet eine unmittelbare Übertragung dieser tatbestandlichen Beschreibung auf das Privatrecht aus.[1047] Die pauschale Aufnahme der verschiedenen Konkretisierungen des verfassungsrechtlichen in den Schutzbereich des privatrechtlichen Persönlichkeitsrechts käme i.E. einer unmittelbaren Drittwirkung gleich.[1048]

Das allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB lässt sich danach auch auf den Schutz der Vertraulichkeit und Integrität informationstechnischer System erstrecken. Der Schutzansatz des privatrechtlichen Persönlichkeitsrechts kommt auch im *GVIiS* zum Ausdruck. Dessen Schutzbereich lässt sich in anerkannte Fallgruppen der zivilrechtlichen Rechtsprechung einordnen. Die aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG für das *GVIiS* folgende Schutzpflicht lässt sich mittels der sich aus § 823 Abs. 1 BGB ergebenden individuellen Ansprüche erfassen. Diese Ansprüche bestehen unabhängig von der Erhebung personenbezogener Daten infolge eines Zugriffs.[1049] Denn bereits der Zugriff selbst als Beseitigung der „entscheidenden technischen Hürde“[1050] stellt den Eingriff dar. Das *GVIiS* ist damit nicht allein in seiner verfassungsrechtlichen Ausprägung im Wege der mittelbaren Drittwirkung bei der Auslegung und Anwendung einfachgesetzlicher Normen zu berücksichtigen, sondern nach Maßgabe seines objektivrechtlichen Gehalts auch als durch § 823 Abs. 1 BGB unmittelbar geschütztes sonstiges Recht. In der Folge ist der Eingriff in die selbstbestimmte Verfügung über das eigengenutzte informationstechnische System durch private Dritte selbst vorbehaltlich der einzelfallbezogenen Interessenabwägung rechtfertigungsbedürftig.

---

[1044] BGB-RGRK/*Steffen*, § 823 Rn. 26.
[1045] Vgl. *Mugdan* (Hrsg.), Materialien zum BGB, Bd. 2, S. 1076f. Rn. 2723f., S. 1117 Rn. 2849.
[1046] *Di Fabio*, in: *Maunz/Dürig*, GG, Bd. 1, Art. 2 Abs. 1 Rn. 131.
[1047] Vgl. auch *Baston-Vogt*, Persönlichkeitsrecht, S. 124.
[1048] *Baston-Vogt*, Persönlichkeitsrecht, S. 137.
[1049] A.A. *Hoffmann*, CR 2010, 515 (518).
[1050] *BVerfGE* 120, 274 (314).

(c) Interessenabwägung

Die Feststellung der Rechtswidrigkeit einer Verletzung des allgemeinen Persönlichkeitsrechts setzt aufgrund seiner generalklauselartigen Weite eine umfassende Güter- und Interessenabwägung voraus.[1051] Bei dieser Abwägung ist wiederum auf Seiten des Betroffenen zu berücksichtigen, dass der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme nicht lediglich einfachgesetzlich, sondern auch verfassungsrechtlich geschützt ist. Eine solche Interessenabwägung wird bei der Infiltration eines informationstechnischen Systems regelmäßig aus mehreren Gründen von vornherein zu Gunsten des Betroffenen ausfallen.

Zunächst besteht im Rahmen der Infiltration eines informationstechnischen Systems stets die Gefahr, dass Daten aus dem absolut geschützten Bereich privater Lebensgestaltung erhoben werden.[1052] Mit diesem absolut geschützten Bereich dürfte aber zugleich die i.R.d. sog. *Sphärentheorie* herausgebildete Intimsphäre betroffen sein. In dieser Sphäre scheidet eine Güter- und Interessenabwägung jedoch aus.[1053] Das Grundrecht der Informationsfreiheit gem. Art. 5 Abs. 1 S. 1 Alt. 2 GG ist auf Seiten des Dritten schon deswegen nicht einschlägig, da die zu erlangenden Informationen nicht aus einer allgemein zugänglichen Quelle stammen. Allgemein zugänglich ist nur eine Informationsquelle, die geeignet und bestimmt ist, der Allgemeinheit, also einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen.[1054] Dem informationstechnischen System des Betroffenen fehlen diese Eignung und Bestimmung. Die Informationsgewinnung aus dem informationstechnischen System ist mit erheblichem Aufwand verbunden und erfordert besondere Sachkenntnis. Zudem sollen die enthaltenen Informationen nach dem erkennbaren Willen des Betroffenen gerade nicht einem unbestimmten Personenkreis zugänglich sein. Auch die Pressefreiheit aus Art. 5 Abs. 1 S. 1 Alt. 1 GG wäre von vornherein nicht in die Abwägung einzubeziehen. Deren Schutzbereich reicht zwar von der Beschaffung der Information bis zur Verbreitung der Meinung oder Nachricht,[1055] dies jedoch nur insoweit, als zur *Beschaffung* der Information keine rechtswidrigen Methoden angewandt werden.[1056] Die Informationsbeschaffung erfolgt jedoch gerade unter Verletzung des allgemeinen Persönlichkeitsrechts des Betroffenen aus § 823 Abs. 1 BGB. Im Ergebnis ist daher kaum ein praktischer Fall denkbar, in dem die Rechtswidrigkeit der Infiltration aufgrund einer Interessenabwägung entfällt.

---

1051 *BGHZ* 13, 334 (338); 24, 72 (80); 50, 133 (143); 128, 1 (10).
1052 *BVerfGE* 120, 274 (335).
1053 *BVerfGE* NJW 1990, 563 (565); *BGH* NJW 1985, 1617 (1618).
1054 *BVerfGE* 27, 71 (83); 33, 52 (65); 90, 27 (32); 103, 44 (60).
1055 *BVerfGE* 10, 118 (121); 50, 234 (240); 77, 346 (354).
1056 *BVerfGE* 66, 116 (137) (Hervorhebung nur hier).

(3) Recht am eingerichteten und ausgeübten Gewerbebetrieb

Schließlich wird der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme auf privatrechtlicher Ebene ausschnittsweise auch durch das *Recht am eingerichteten und ausgeübten Gewerbebetrieb* (ReaG) gewährleistet. Als sonstiges absolut geschütztes Recht i.S.d. § 823 Abs. 1 BGB erfasst das *ReaG* den Gewerbebetrieb im gesamten Bereich der gewerblichen Betätigung[1057] und stellt in diesem Bereich ein subjektives Recht auf störungsfreie gewerbliche Betätigung dar.[1058] Geschützt wird damit umfassend all das, was den Gewerbebetrieb in seiner Gesamtheit zur Entfaltung und Beteiligung in der Wirtschaft befähigt.[1059] Aufgrund der generalklauselartigen Weite dieses Schutzbereichs setzt die Verletzung des *ReaG* die Betriebsbezogenheit[1060] des Eingriffs voraus. Der Eingriff muss sich gegen den Betrieb als solchen richten und darf nicht lediglich vom Gewerbebetrieb ablösbare Rechtspositionen beeinträchtigen.[1061]

Die technische Infiltration eines informationstechnischen Systems, die an dem *ReaG* zu messen ist, liegt demzufolge von vornherein nur dann vor, wenn die Infiltration gerade diese betrieblichen Grundlagen zum Gegenstand hat. In Betracht kommt hier zunächst die Störung betrieblich eingesetzter Systeme sowie die Löschung und Veränderung von Betriebsdaten. Sofern diese Beeinträchtigung eine gezielte Sabotage zur Störung des Betriebsablaufs darstellt, wäre dieser Eingriff auch betriebsbezogen.[1062] Denn er zielt nach dem Willen des Verletzers gerade auf die betriebliche Betätigung. Als subsidiärer Auffangtatbestand[1063] setzt das *ReaG* jedoch die Lückenhaftigkeit des geschriebenen Rechts voraus.[1064] Diese Subsidiarität gilt folglich auch hinsichtlich des Eigentumsschutzes des § 823 Abs. 1 BGB.[1065] Die beschriebene Verletzungshandlung stellt zugleich eine Beeinträchtigung der Nutzungsmöglichkeit des jeweiligen informationstechnischen Systems dar. Der Schutz des Eigentums des Inhabers des Gewerbetriebs an diesem System wäre daher vorrangig. Der Anwendungsbereich des *ReaG* wäre demnach überhaupt nur dann eröffnet, wenn der Inhaber des Gewerbebetriebs an dem infiltrierten System kein Eigentum hat oder zivilrechtliches Eigentum mangels Sachqualität des Systems ausscheidet. Die Subsidiarität des *ReaG* gilt ebenso gegenüber den Vorschriften des UWG. Letzteres setzt jedoch das Vorliegen einer geschäftlichen Handlung i.S.d. § 2 Abs. 1 Nr. 1 UWG voraus. Schließlich geht auch das BDSG

1057 *BGHZ* 3, 270 (279f.); 8, 142 (144); 29, 65 (69); *BGH* NJW 1963, 484; NJW 1987, 2222 (2225).
1058 *OLG München* NJW-RR 1994, 1054 (1055).
1059 Staudinger/*Hager* (1999), § 823 Rn. D9.
1060 *BGHZ* 29, 65 (74); 41, 123 (127); 55, 153 (161); 59, 30 (35); 69, 128 (139); 74, 9 (18); 76, 387 (395); 86, 152 (156); 90, 113 (123).
1061 *BGHZ* 29, 65 (74); 55, 153 (161); 86, 152 (156).
1062 Eine solche gezielte Sabotage könnte etwa das Einschleusen einer individuell angepassten Schadsoftware wie z.B. *Stuxnet* sein.
1063 *BGHZ* 45, 296 (307); 59, 76 (79); 65, 325 (328); 69, 128 (138f.); 105, 346 (350); dies gilt nicht für vorsätzliche Eingriffe, so *BGHZ* 59, 30 (34f.); 69, 128 (139)
1064 *BGHZ* 36, 252 (257); 38, 200 (204); 43, 359 (361).
1065 *BGHZ* 55, 153 (158f.); 105, 346 (350).

als Spezialregelung dem *ReaG* vor.[1066] Dieses Recht findet damit keine Anwendung, soweit der Umgang mit personenbezogenen Daten i.S.d. §§ 3 Abs. 1, 4 Abs. 1 BDSG betroffen ist.

Der Schutzbereich des *ReaG* setzt anders als der Schutzbereich des *GVIiS* keine besondere Persönlichkeitsrelevanz der Infiltration voraus. Die Infiltration informationstechnischer Systeme stellt eine Beeinträchtigung dieses Rechts unabhängig von der Komplexität und des potenziell vorhandenen Datenbestands dar. Umgekehrt decken sich beide Schutzbereiche aber nur dahingehend, als die Suche nach den jeweiligen Informationen den notwendigen Betriebsbezug aufweist. Sofern es um den Schutz juristischer Personen durch das *GVIiS* geht, dürfte in dem Umfang ihrer wirtschaftlichen Betätigung zugleich auch die Betriebsbezogenheit i.S.d. *ReaG* zu bejahen sein. Letzteres kann etwa auch dann betroffen sein, wenn sich Dritte Betriebsgeheimnisse verschaffen.[1067] Anderes dürfte hingegen für natürliche Personen gelten. Die ausdrücklich vom Schutzbereich des *GVIiS* erfasste geschäftliche Nutzung eines informationstechnischen Systems muss sich nicht notwendig mit dem Schutzbereich des *ReaG* überschneiden. Dies gilt etwa für die geschäftliche Nutzung eines informationstechnischen Systems durch Personen, die nicht Inhaber des Gewerbebetriebs sind. Für diese kommt zwangsläufig der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme durch das *ReaG* nicht in Betracht.

ii. § 823 Abs. 2 BGB i.V.m. StGB

Die Vertraulichkeit und Integrität informationstechnischer Systeme fällt nicht nur in den Schutzbereich der absoluten Rechtsgüter des § 823 Abs. 1 BGB, sondern für einen entsprechenden Schutz kommt daneben auch § 823 Abs. 2 BGB i.V.m. einzelnen Normen des StGB in Betracht. Die Verpflichtung zum Schadensersatz nach § 823 Abs. 1 BGB trifft nach § 823 Abs. 2 BGB auch denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Schutzgesetz i.S.d. § 823 Abs. 2 BGB ist nach Art. 2 EGBGB jede Rechtsnorm. Unerheblich ist das Rechtsgebiet, dem die Norm entstammt.[1068] Der Begriff erfasst daher auch Normen des StGB. Die Qualifizierung einer Norm als Schutzgesetz setzt weiter voraus, dass die Norm neben dem Schutz der Allgemeinheit zumindest auch dem Schutz des Einzelnen zu dienen bestimmt ist.[1069] Entscheidend sind dabei Inhalt und Zweck des Gesetzes sowie, ob ein wegen der behaupteten Verletzungen geltend gemachter Rechtsschutz zugunsten von Einzelpersonen oder bestimmten

[1066] *BGH* NJW 1986, 2505 (2506f.).
[1067] *BGHZ* 16, 172 (175f.); 17, 41 (50f.); 107, 117 (122); a.A. *Larenz/Canaris*, Schuldrecht II/2, § 81 III 5b).
[1068] Siehe nur Staudinger/*Hager* (1999), § 823 Rn. G9.
[1069] *BGHZ* 12, 146 (148); 100, 13 (14); 125, 366 (374); *BGH* NJW-RR 2005, 673; NJW-RR 2005, 680; NJW 2005, 2923 (2924).

Personenkreisen vom gesetzgeberischen Willen umfasst ist.[1070] Stellt danach die jeweilige Norm ein Schutzgesetz dar, muss schließlich noch der persönliche und sachliche Schutzbereich der Norm eröffnet sein. Der Verletzte muss zu dem von der Norm geschützten Personenkreis gehören[1071] und der Schaden an einem von der Norm geschützten Rechtsgut entstanden sein.[1072]

Dieser persönliche Schutzbereich ist hinsichtlich der Normen des StGB, die für den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme in Betracht kommen, eröffnet. Im Folgenden ist der berechtigte Nutzer eines informationstechnischen Systems zugleich auch der Geschädigte. Etwaige Schäden fallen zudem in den sachlichen Schutzbereich dieser Normen. Insoweit diese die Vertraulichkeit und Integrität informationstechnischer Systeme erfassen, schützen sie die selbstbestimmte Verfügung des berechtigten Nutzers über das von ihm genutzte System. Die Aufhebung oder Störung dieser Verfügung ist damit ein Schaden, der an den geschützten Rechtsgütern entsteht.

(1) § 201 StGB - Verletzung der Vertraulichkeit des Wortes

Der Schutzbereich des *GVIiS* ist vorbehaltlich der Spezialität des Art. 13 Abs. 1 GG eröffnet, wenn eine Überwachung mittels der Peripheriegeräte eines informationstechnischen Systems wie Mikrofon oder Kamera erfolgt. Eine solche Überwachung könnte zunächst den Tatbestand des § 201 StGB erfüllen.

Geschütztes Rechtsgut des § 201 StGB ist die Unbefangenheit des nichtöffentlich gesprochenen Wortes.[1073] Ebenso soll auch der Nutzer eines informationstechnischen Systems nicht wegen der Ungewissheit, inwieweit die persönlichkeitsrelevante Nutzung Gegenstand von Überwachungsmaßnahmen ist, von der Ausübung seiner geschützten Freiheit abgehalten werden. Der Schutz des § 201 StGB hat seine Grundlage im allgemeinen Persönlichkeitsrecht.[1074] Die Norm zielt daher gerade auf einen Individualschutz und weist somit die Eigenschaft eines Schutzgesetzes i.S.d. § 823 Abs. 2 BGB auf.[1075] Hierbei stellt § 201 Abs. 1 Nr. 1 StGB die unbefugte Aufnahme des nichtöffentlich gesprochenen Wortes eines anderen auf einen Tonträger unter Strafe. Nichtöffentlich gesprochenes Wort ist das nicht an die Allgemeinheit gerichtete ohne weiteres wahrnehmbare gesprochene Wort einer anderen Person.[1076] Entscheidend sind die Abgeschlossenheit des Zuhörerkreises und die Kontrollmöglichkeit über die Reichweite der Äußerung.[1077] Aufnehmen bezeichnet das Fixieren des gesprochenen Wortes auf einem Tonträger derart,

[1070] *BGH* NJW 1992, 241 (242); NJW-RR 2005, 673; NJW-RR 2005, 680; NJW 2005, 2923 (2924); NJW 2006, 2110 (2112).
[1071] *BGHZ* 29, 100 (102); 62, 186 (188); 84, 312 (314).
[1072] *BGHZ* 12, 213 (217); 19, 114 (126); 114, 161 (163).
[1073] Siehe nur LK-*Schünemann*, StGB § 201 Rn. 2.
[1074] S/S-*Lenckner/Eisele*, § 201 Rn. 2; *Fischer*, StGB, § 201 Rn. 2; LK-*Schünemann*, § 201 Rn. 2.
[1075] So auch ohne Begründung *Hoppe*, GRUR 2004, 990 (994).
[1076] *Fischer*, StGB, § 201 Rn. 3.
[1077] *Fischer*, StGB, § 201 Rn. 4.

dass eine erneute Wiedergabe ermöglicht wird.[1078] Dem Begriff des Tonträgers unterfallen alle Sachen, die analog oder digital gespeicherte akustische Signale enthalten, welche durch Hilfsmittel dem Ohr wahrnehmbar gemacht werden können.[1079] Dazu gehören auch die elektronisch lesbaren, binär codierten Daten- bzw. Informationsträger.[1080]

Dieser Definition des Tonträgers unterfällt auch ein vom Schutzbereich des *GVIiS* erfasstes informationstechnisches System. Ein solches System ermöglicht jedenfalls in der zur Eröffnung des Schutzbereichs des *GVIiS* notwendigen Komplexität die digitale Fixierung akustischer Signale und deren Wiedergabe mittels entsprechender Software entweder durch bereits integrierte oder externe Lautsprecher.[1081] Sofern diese Voraussetzungen vorliegen, steht die Fixierung des nichtöffentlichen gesprochenen Wortes auf einem Speichermedium, das Element des informationstechnischen Systems aber kein außerhalb dieses Systems stehender Gegenstand ist, der Eröffnung des Schutzzwecks des § 201 StGB nicht entgegen. Die Unbefangenheit des nichtöffentlich gesprochenen Wortes ist in gleicher Weise wie bei der Aufzeichnung auf einem vom eigentlichen Aufnahmegerät abgrenzbaren Gegenstand betroffen. Eine so angefertigte heimliche Aufnahme kann in gleicher Weise ohne Einwilligung des Sprechenden oder gar dessen erklärten Willen verwertet werden.[1082]

Wegen der Verletzung der Vertraulichkeit des nichtöffentlich gesprochenen Wortes macht sich ferner nach § 201 Abs. 2 Nr. 1 StGB strafbar, wer unbefugt das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört. Abhörgerät ist dabei jede technische Einrichtung, die das Wort über dessen natürlichen Klangbereich hinaus für den Täter hörbar macht.[1083] Entscheidend ist die konkrete Nutzung und nicht eine bestimmte äußerlich erkennbare Gattung von Geräten.[1084] Abhören setzt die gezielte Nutzung des Abhörgeräts zur sinnlichen Wahrnehmung des nichtöffentlich gesprochenen Wortes voraus, erfordert aber keine unmittelbare Wahrnehmung.[1085] Es genügt eine u.U. automatisch ausgelöste Aufzeichnung zur späteren Wiedergabe,[1086] so dass auch die Koppelung eines Abhörgeräts mit einer Aufnahmevorrichtung tatbestandsmäßig ist.[1087]

---

[1078] LK-*Schünemann*, StGB, § 201 Rn. 14; MüKoStGB-*Graf*, § 201 Rn. 20.

[1079] Siehe nur *Fischer*, StGB, § 11 Rn. 35.

[1080] LK-*Hilgendorf*, § 11 Rn. 117; MüKoStGB-*Radtke*, § 11 Rn. 145.

[1081] I.E. ebenso *Sankol*, CR 2008, 13 (16): Grundsätzliche Strafbarkeit nach § 201 Abs. 1 Nr. 1 StGB bei Einsatz von Spyware zur Überwachung von Internettelefonie auf einem PC; Tonträgereigenschaft eines Notebooks ohne Begründung bejahend *OLG Celle*, Urt. v. 17.09.2008, Az. 31 Ss 21/08.

[1082] Diesbezüglich zum *Recht am gesprochenen Wort BVerfGE* 34, 238 (247); 106, 28 (40).

[1083] *Fischer*, StGB, § 201 Rn. 7; MüKoStGB-*Graf*, § 201 Rn. 32; S/S-*Lenckner/Eisele*, § 201 Rn. 19.

[1084] *Fischer*, StGB, § 201 Rn. 7a; S/S- *Lenckner/Eisele*, § 201 Rn. 19.

[1085] S/S-*Lenckner/Eisele*, § 201 Rn. 20; LK-*Schünemann*, § 201 Rn. 21; MüKoStGB- *Graf*, § 201 Rn. 31.

[1086] MüKoStGB-*Graf*, § 201 Rn. 31.

[1087] LK-*Schünemann*, § 201 Rn. 21; S/S-*Lenckner/Eisele*, § 201 Rn. 20.

Die bestimmungsgemäße Verwendung eines Mikrofons als technische Komponente eines informationstechnischen Systems ist nicht die Nutzung als Abhörgerät. Die Infiltration des Systems des Betroffenen ermöglicht jedoch einem Dritten die gezielte Wahrnehmung des nichtöffentlich gesprochenen Wortes über dessen natürlichen Klangbereich hinaus durch die Übertragung der von dem Mikrofon aufgezeichneten Worte mittels eines Kommunikationsnetzes. Ein derart von einem Dritten genutztes Mikrofon stellt daher ein Abhörgerät i.S.d. Norm dar.[1088] Die Überwachung des Betroffenen mittels der Peripheriegeräte eines informationstechnischen Systems dürfte daher - im Rahmen seiner einfachgesetzlichen Reichweite - nicht nur einen Eingriff in den Schutzbereich des *GVIiS* bedeuten, sondern daneben grds. auch nach § 201 Abs. 2 Nr. 1 StGB strafbar sein.[1089]

(2) § 201a StGB - Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

Strafbar macht sich gem. § 201a Abs. 1 StGB, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt. Schutzgut der Norm ist der höchstpersönliche Lebensbereich.[1090] Dieser wird als Teilbereich des allgemeinen Persönlichkeitsrechts geschützt.[1091] § 201a StGB dient daher gerade dem Schutz des Einzelnen und ist somit Schutzgesetz i.S.d. § 823 Abs. 2 BGB.[1092]

(a) Wohnung oder gegen Einblicke besonders geschützter Raum

Sofern die an ein informationstechnisches System angeschlossenen Peripheriegeräte wie Mikrofon oder Kamera zur Überwachung von Vorgängen innerhalb einer dem verfassungsrechtlichen Begriff der Wohnung unterfallenden Räumlichkeit genutzt werden, ist allein der Schutzbereich des Art. 13 Abs. 1 GG einschlägig.[1093] Derartige Eingriffe privater Dritter richten sich somit ausschließlich nach den einfachgesetzlichen Wirkungen des Grundrechts der Unverletzlichkeit der Wohnung. Privatrechtliche Wirkungen des *GVIiS* kommen insofern nicht in Betracht. Dessen Schutzbereich ist im Folgenden nur hinsichtlich solcher Räumlichkeiten zu berücksichtigen, die nicht vom verfassungsrechtlichen Begriff der Wohnung umfasst werden.

Ausgangspunkt der Bestimmung des Wohnungsbegriffs des § 201a Abs. 1 StGB ist zunächst § 123 StGB.[1094] Danach ist die Wohnung der Inbegriff von

[1088] I.E. ebenso S/S-*Lenckner/Eisele*, § 201 Rn. 19; MüKoStGB-*Graf*, § 201 Rn. 32.
[1089] Hinsichtlich der Überwachung der Internettelefonie ist wiederum das Spezialitätsverhältnis zu Art. 10 Abs. 1 GG zu beachten.
[1090] *Fischer*, StGB, § 201a Rn. 3; LK-*Valerius*, § 201a Rn. 6; S/S-*Lenckner/Eisele*, § 201a Rn. 2.
[1091] *Fischer*, StGB, § 201a Rn. 3; S/S-*Lenckner/Eisele*, § 201a Rn. 2.
[1092] Ebenso *Fischer*, StGB, § 201a Rn. 3.
[1093] *BVerfGE* 120, 274 (310).
[1094] *Fischer*, StGB, § 201a Rn. 7.

Räumlichkeiten, deren Hauptzweck die ständige Benutzung von Menschen ist, und die nicht vorrangig Arbeitsräume sind.[1095] Stellt der so verwendete Begriff der Wohnung zugleich eine Räumlichkeit dar, die auch in den Schutzbereich des Art. 13 Abs. 1 GG fallen würde, sind von vornherein nur die privatrechtlichen Wirkungen des Grundrechts der Unverletzlichkeit der Wohnung zu berücksichtigen. Hinsichtlich der Erfüllung der Anforderungen an den einfachgesetzlichen Schutzumfang des *GVIiS* ist die Norm nur insoweit zu berücksichtigen, als der Begriff der Wohnung i.S.d. § 201a StGB weiter reicht als derjenige des Art. 13 Abs. 1 GG. Hingegen dürfte die Norm hinsichtlich des einfachgesetzlichen Schutzumfangs des *GVIiS* vermehrt einschlägig sein, als sie neben Wohnungen auch besonders geschützte Räume erfasst. Für diese ist nicht der Schutz vor dem körperlichen Eindringen anderer Personen, sondern der Sichtschutz entscheidend.[1096] Erfasst wird der Bereich privater Lebensgestaltung, der sich mit dem durch die Rechtsprechung des *BVerfG* verwendeten und in der zivilrechtlichen Rechtsprechung näher ausgeformten Begriffs der Intimsphäre beschreiben lässt.[1097] Erfasst werden daher zunächst solche Räumlichkeiten, in denen diese Sphäre typischerweise offengelegt und ein Sichtschutz gerade aus diesem Grund geschaffen wird.[1098] Anders als bei Art. 13 Abs. 1 GG steht hinter diesem Schutz gerade nicht die räumliche Sphäre, in der sich das Privatleben entfaltet.

Insgesamt kann § 201a Abs. 1 StGB daher nur insoweit zur Gewährleistung einfachgesetzlichen Schutzes des *GVIiS* herangezogen werden, als die betroffene Räumlichkeit im konkreten Fall zwar einen höchstpersönlichen Lebensbereich darstellt, nicht aber zugleich auch räumliche Sphäre ist, in der sich das Privatleben entfaltet. Keinen Schutz bietet die Norm hingegen gegen Überwachungen infolge derer keine Wohnung oder ein besonders geschützter Raum mithin nicht der höchstpersönliche Lebensbereich i.S.d. Norm betroffen ist.

(b) Bildaufnahmen

Bildaufnahmen sind gegenständliche, perpetuierbare und zur Vervielfältigung geeignete Verkörperungen eines visuell erfassbaren Abbildes.[1099] Ein solches Abbild verkörpern sowohl Fotos als auch Filme.[1100] Der Begriff des Herstellens erfasst diejenigen Handlungen, wodurch das Abbild auf einem Bild- oder Datenträ-

[1095] Siehe nur *Fischer*, StGB, § 123 Rn. 6; umstritten ist, ob dieser Begriff unverändert übernommen werden kann (so S/S-*Lenckner/Eisele*, § 201a Rn. 6), oder zur Berücksichtigung des Rechtsguts des höchstpersönlichen Lebensbereichs eine engere Auslegung erforderlich ist (so *Fischer*, StGB, § 201a Rn. 7; Lackner/*Kühl*, StGB, § 201a Rn. 2; LK-*Valerius*, § 201a Rn. 15). Entscheidend ist dieser Streit hier nicht, da sich die Reichweite des Anwendungsbereichs des § 201a Abs. 1 StGB hinsichtlich des Schutzvorgaben des *GVIiS* ohnehin nach dem Wohnungsbegriff des Art. 13 Abs. 1 GG richtet.

[1096] BT-Drucks. 15/2466, S. 5.

[1097] BT-Drucks. 15/2466, S. 5.

[1098] S/S-*Lenckner/Eisele*, § 201a Rn. 7.

[1099] Siehe nur *Fischer*, StGB, § 201a Rn. 4.

[1100] *Fischer*, StGB, § 201a Rn. 4; LK-*Valerius*, StGB, § 201a Rn. 9.

ger abgespeichert wird.[1101] Während dies eine dauerhafte Fixierung voraussetzt,[1102] soll mit der Variante des Übertragens aber klargestellt werden, dass die Norm darüber hinaus auch Echtzeitübertragungen durch Web- oder Spycams unter Strafe stellt, ohne dass die aufgenommenen Bilder dauerhaft gespeichert werden müssten.[1103] Vorbehaltlich des Konkurrenzverhältnisses zu Art. 13 Abs. 1 GG fällt die unberechtigte Nutzung der an ein informationstechnisches System angeschlossenen Kamera durch einen Dritten[1104] in den Schutzbereich des *GVIiS*. Diese Nutzung wird von § 201a Abs. 1 StGB erfasst, sofern die von dieser Norm geschützte höchstpersönliche Lebenssphäre betroffen ist. Stellt diese keine Wohnung i.S.d. Art. 13 Abs. 1 GG dar, vermittelt die über § 823 Abs. 2 BGB zu berücksichtigende strafrechtliche Sanktion auch den einfachgesetzlich vorausgesetzten Schutz des *GVIiS*.

(3) § 202a StGB - Ausspähen von Daten

Wegen Ausspähens von Daten gem. § 202a Abs. 1 StGB macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. § 202a StGB schützt die Entscheidung des an den Daten Verfügungsberechtigten über den Zugang zu den in den Daten verkörperten Informationen.[1105] Aufgrund des dahingehend bezweckten Individualschutzes fällt § 202a StGB unter die Definition eines Schutzgesetzes.[1106]

Der Schutzbereich des *GVIiS* erfasst zunächst das Interesse des Nutzers eines informationstechnischen Systems, dass die von dem System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.[1107] Ein Eingriff in den Schutzbereich stellt ferner das Antasten der Integrität des informationstechnischen durch einen Zugriff dar, infolgedessen die Leistungen, Funktionen und Speicherinhalte des Systems durch Dritte genutzt werden können.[1108] Das *GVIiS* schützt demnach in vergleichbarer Form die selbstbestimmte Verfügung des zur Nutzung Berechtigten. Der vom *BVerfG* gebrauchte Datenbegriff ist weiter als derjenige des § 202a StGB. Daten sind hiernach nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (§ 202a Abs. 2 StGB). Sie sind mithin kodierte Informationen.[1109] Der Begriff

---

[1101] BT-Drucks. 15/2466, S. 5.
[1102] *Fischer*, StGB, § 201a Rn. 12f.; Lackner/*Kühl*, StGB, § 201a Rn. 4; LK-*Valerius*, StGB, § 201a Rn. 21.
[1103] BT-Drucks. 15/2466, S. 5.
[1104] Vgl. *BVerfGE* 120, 274 (310).
[1105] *Fischer*, StGB, § 202a Rn. 2; LK-*Hilgendorf*, StGB, § 202a Rn. 6; MüKoStGB-*Graf*, § 202a Rn. 2; S/S-*Lenckner/Eisele*, StGB, § 202a Rn. 1.
[1106] I.E. ebenso *Wiebe*, BB 1993, 1094 (1102).
[1107] *BVerfGE* 120, 274 (314).
[1108] *BVerfGE* 120, 274 (314).
[1109] LK-*Hilgendorf*, StGB, § 202a Rn. 7.

erstreckt sich auch auf Programme.[1110] Einen bestimmten Inhalt der Daten setzt die Vorschrift nicht voraus.[1111] Erlangt der Dritte Zugang zu Daten nach dem Begriffsverständnis des *BVerfG*, liegt darin stets auch ein Zugang i.S.d. § 202a StGB. Zugang zu den Daten eines verarbeitenden Systems hat der Täter jedoch erst, wenn der Datenzugriff ohne weiteren Zwischenakt möglich ist.[1112] Insoweit dürfte die Aufhebung der Vertraulichkeit eines informationstechnischen Systems durch die Möglichkeit der Datenerhebung und diejenige der Integrität durch die Möglichkeit der Nutzung von Leistungen, Funktionen und Speicherinhalten des Systems durch Dritte infolge der Infiltration gleichbedeutend mit dem Begriff des Zugangs i.S.d. § 202a Abs. 1 StGB sein. Denn wenn ein Datenzugriff ohne weiteren Zwischenakt möglich ist, besteht auch eine entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems nicht mehr. Keine Voraussetzung ist hingegen die Kenntnisnahme der Daten.[1113] Das Verschaffen des Zugangs zu den Daten erfordert nicht auch, dass der Täter sich auch Daten verschafft.[1114] Ebenso setzt auch der Eingriff in den Schutzbereich des *GVIiS* gerade nicht voraus, dass nach der erfolgreichen Infiltration des informationstechnischen Systems auch tatsächlich Daten erhoben werden. Ausreichend ist, dass eine Erhebung bloß ermöglicht wird.

Anders als der Schutzbereich des *GVIiS* erfordert § 202a Abs. 1 StGB jedoch, dass die Daten gegen den unberechtigten Zugang besonders gesichert sind. Eine solche Sicherung verlangt Vorkehrungen, die den unbefugten Zugriff auf die Daten ausschließen oder erheblich erschweren.[1115] Dies sind weder Maßnahmen bloß organisatorischer Art[1116] noch Sicherungen gegen das unbefugte Benutzen der Hardware.[1117] Vorrangig wird auf software- und hardware-integrierte Sicherungen abgestellt.[1118] Eine Durchbrechung der Zugangssicherung darf nicht ohne weiteres möglich sein.[1119] Allerdings stellt § 202a StGB hinsichtlich der besonderen Zugangssicherung nur auf die tatgegenständlichen Daten ab. Zwar ist mittelbar auch das datenverarbeitende System geschützt, dies jedoch dann nicht, wenn nicht das System als Ganzes, sondern nur die einzelnen Daten besonders geschützt sind.[1120] Um auf einfachgesetzlicher Ebene den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme gewährleisten zu können, muss demnach die besondere Zugangssicherung das gesamte System erfassen und nicht nur einzelne

---

1110 BT-Drucks. 10/5058, S. 29; ebenso MüKoStGB-*Wieck-Noodt*, § 303a Rn. 8.
1111 *Fischer*, StGB, § 202a Rn. 4; MüKoStGB-*Graf*, § 202a Rn. 10.
1112 LK-*Hilgendorf*, StGB, § 202a Rn. 15.
1113 BT-Drucks. 10/5058, S. 29; *Fischer*, StGB, § 202a Rn. 11; Lackner/*Kühl*, StGB, § 202a Rn. 5; MüKoStGB-*Graf*, § 202a Rn. 51; S/S-*Lenckner-Eisele*, § 202a Rn. 10.
1114 BT-Drucks. 16/3656, S. 9.
1115 *Fischer*, StGB, § 202a Rn. 8; S/S-*Lenckner/Eisele*, StGB, § 202a Rn. 7.
1116 *Fischer*, StGB, § 202a Rn. 8a; LK-*Hilgendorf*, StGB, § 202a Rn. 29.
1117 BT-Drucks. 16/3656, S. 10; *Fischer*, StGB, § 202a Rn. 8a; LK-*Hilgendorf*, StGB, § 202a Rn. 30.
1118 *Fischer*, StGB, § 202a Rn. 9.
1119 BT-Drucks. 16/3656, S. 10 m.w.N.
1120 *Gröseling/Höfinger*, MMR 2007, 549 (551).

Daten. Der Schutzbereich des *GVIiS* ist unabhängig davon eröffnet, ob der Zugriff auf das informationstechnische System leicht oder nur mit erheblichem Aufwand möglich ist.[1121] Ein nicht unerheblich erschwerter Zugriff ist kein leichter Zugriff. Regelmäßig dürfte daher der von dem Nutzer ergriffene technische Selbstschutz nicht die Anforderungen einer besonderen Zugangssicherung erfüllen.

Der vom *GVIiS* vorausgesetzte einfachgesetzliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme lässt sich daher nur insoweit über § 202a Abs.1 StGB realisieren, als die von dem Nutzer des Systems ergriffenen Schutzmaßnahmen die Schwelle einer besonderen Zugangssicherung erreichen.

(4) § 202b StGB - Abfangen von Daten

Nach § 202b Alt. 2 StGB ist strafbar, wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. Das von § 202b StGB geschützte Rechtsgut stimmt mit dem des § 202a StGB überein,[1122] so dass auch § 202b StGB als Schutzgesetz i.S.d. § 823 Abs. 2 BGB anzusehen ist. Sofern derjenigen Ansicht gefolgt wird, dass die Norm entgegen dem gesetzgeberischen Willen[1123] ihrem Wortlaut nach auch bereits gespeicherte Daten außerhalb eines Übermittlungsvorgangs erfasst,[1124] lässt sie sich zur einfachgesetzlichen Umsetzung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme heranziehen. Die Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur werden ausdrücklich als Eingriff in den Schutzbereich des *GVIiS* benannt.[1125]

(5) § 303a Abs. 1 StGB - Datenveränderung

Die Strafbarkeit nach § 303a Abs. 1 StGB setzt voraus, dass der Täter rechtswidrig Daten i.S.d. § 202a Abs. 2 StGB löscht, unterdrückt, unbrauchbar macht oder verändert. Die Norm schützt das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit von Daten.[1126] Mit dem so bezweckten Individualschutz stellt § 303a StGB ebenfalls ein Schutzgesetz dar.[1127] Entscheidend ist für § 303a Abs. 1 StGB allein die Integrität der Daten, nicht jedoch ihr wirtschaftlicher, inhaltlicher oder Beweiswert.[1128] Dem Informationsgehalt der Daten kommt somit

[1121] *BVerfGE* 120, 274 (315).
[1122] BT-Drucks. 16/3656, S. 11; *Fischer*, StGB, § 202b Rn. 2.
[1123] BT-Drucks. 16/3656, S. 11.
[1124] So LK-*Hilgendorf*, StGB, § 202b Rn. 12; S/S-*Eisele*, § 202b Rn. 5; a.A. *Fischer*, StGB, § 202b Rn. 3.
[1125] *BVerfGE* 120, 274 (315).
[1126] Lackner/*Kühl*, StGB, § 303a Rn. 1; LK-*Wolff*, StGB, § 303a Rn. 4; MüKoStGB-*Wieck-Noodt*, § 303a; S/S-*Stree/Hecker*, § 303a Rn. 1; Rn. 2
[1127] So auch ohne Begründung *Wuermeling*, CR 1994, 585 (591).
[1128] *Fischer*, StGB, § 303a Rn. 3; LK-*Wolff*, StGB, § 303a Rn. 6.

keine Bedeutung zu.[1129] Die Daten müssen gegen den unbefugten Zugriff nicht besonders gesichert sein.[1130] Tathandlungen des § 303a Abs. 1 StGB sind das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten. Löschen entspricht der Zerstörung einer Sache in § 303 Abs. 1 StGB und führt zur unwiederbringlichen vollständigen Unkenntlichkeit.[1131] Der Begriff ist mit dem des § 3 Abs. 4 S. 2 Nr. 5 BDSG vergleichbar.[1132] Unterdrückt werden Daten, wenn sie dem Zugriff Berechtigter entzogen und deshalb nicht mehr verwendet werden können.[1133] Eine Beeinträchtigung der physischen Integrität ist nicht erforderlich.[1134] Das Unbrauchbarmachen beeinträchtigt die Daten so in ihrer Gebrauchsfähigkeit, dass sie nicht mehr ordnungsgemäß verwendet werden und damit ihren Zweck nicht mehr erfüllen können.[1135] Eine tatbestandsmäßige Funktionseinbuße muss demnach nicht notwendig in der Veränderung der betroffen Daten liegen, sondern kann auch durch zusätzliche Daten bewirkt werden.[1136] Daten werden verändert, wenn Funktionsbeeinträchtigungen eine Änderung des Informationsgehalts oder Aussagewerts bewirken.[1137] Ausdrücklich soll darunter das inhaltliche Umgestalten i.S.d. § 3 Abs. 4 S. 2 Nr. 2 BDSG fallen.[1138]

§ 303a Abs. 1 StGB lässt sich zunächst insoweit hinsichtlich des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme heranziehen, als durch die Infiltration eines Systems verursachte Datenverluste sowie die versehentliche Löschung von Datenbeständen oder das Löschen, Verändern oder Neuanlegen von Datenbeständen durch gezielte Manipulation relevant werden.[1139] Eine versehentliche Datenlöschung kann jedoch nur dann tatbestandsmäßig sein, wenn hierin im Gegensatz zu einer gezielten Manipulation ein bloß eventualvorsätzliches Handeln gesehen wird, vgl. § 15 StGB. Ferner kommt die Norm dann in Betracht, wenn die technische Infiltration eines informationstechnischen Systems über die Installation eines Spähprogramms erfolgt. Die tatbestandliche

---

1129 LK-*Wolff*, StGB, § 303a Rn. 6.

1130 *Fischer*, StGB, § 303a Rn. 3; LK-*Wolff*, StGB, § 303a Rn. 6; MüKoStGB-*Wieck-Noodt*, § 303a Rn. 8; S/S-*Stree/Hecker*, § 303a Rn. 2; *Ernst*, in: *Ders.* (Hrsg.), Hacker, Cracker und Computerviren, Rn. 268.

1131 BT-Drucks. 10/5058, S. 34; ebenso *Fischer*, StGB, § 303a Rn. 9; Lackner/*Kühl*, StGB, § 303a Rn. 3; LK-*Wolff*, StGB, § 303a Rn. 21; MüKoStGB-*Wieck-Noodt*, § 303a Rn. 12.

1132 BT-Drucks. 10/5058, S. 34.

1133 BT-Drucks. 10/5058, S. 34f.

1134 *Fischer*, StGB, § 303a Rn. 10; LK-*Wolff*, StGB, § 303a Rn. 24; MüKoStGB-*Wieck-Noodt*, § 303a Rn. 13; *Ernst*, in: *Ders.* (Hrsg.), Hacker, Cracker und Computerviren, Rn. 274.

1135 BT-Drucks. 10/5058, S. 35.

1136 LK-*Wolff*, StGB, § 303a Rn. 26; vgl. auch BT-Drucks. 10/5058, S. 35.

1137 BT-Drucks. 10/5058, S. 35.

1138 BT-Drucks. 10/5058, S. 35.

1139 *BVerfGE* 120, 274 (325).

Relevanz hängt jedoch von der Ausgestaltung des Programms ab. Das bloße Hinzufügen von Daten ist kein Verändern i.S.d. § 303a Abs. 1 StGB,[1140] solange der Bedeutungsgehalt bereits vorhandener Daten nicht geändert wird.[1141]

(6) § 303b Abs. 1 Nr. 1, 2 StGB - Computersabotage

Wegen Computersabotage gem. § 303b Abs. 1 StGB macht sich strafbar, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er eine Tat nach § 303a Abs. 1 StGB begeht (Nr. 1), Daten (§ 202a Abs. 2 StGB) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt (Nr. 2) oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert (Nr. 3). § 303b StGB schützt das Interesse der Betreiber und Nutzer von Datenverarbeitungen allgemein an deren ordnungsgemäßer Funktionsweise.[1142] Daher stellt auch § 303b StGB aufgrund des so bezweckten Individualschutzes eine Schutznorm i.S.d. § 823 Abs. 2 BGB dar.[1143] Datenverarbeitung beschreibt den gesamten Umgang mit elektronisch gespeicherten Daten von der Erhebung bis zur Verwendung.[1144] Ausreichend ist, dass Datenverarbeitungsvorgänge bloß geplant oder beabsichtigt sind.[1145] Aufgrund des Merkmals der Wesentlichkeit der Datenverarbeitung sind Sabotageakte von untergeordneter Bedeutung nicht tatbestandsmäßig.[1146] Das Merkmal der Wesentlichkeit bestimmt sich bei Privatpersonen als Geschädigte danach, „ob die Datenverarbeitungsanlage für die Lebensgestaltung der Privatperson eine zentrale Funktion einnimmt".[1147] Eine solche Funktion wird vom *BVerfG* für die vom *GVIiS* erfassten informationstechnischen Systeme ausdrücklich bejaht, indem das Gericht feststellt, „dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist".[1148] Wesentliche Bedeutung für einen Betrieb, ein Unternehmen oder eine Behörde (vgl. § 303b Abs. 2 StGB) hat die Datenverarbeitung, wenn sie für die Organisation und die Verwaltungs- und Arbeitsabläufe grundlegend ist,[1149] so dass diese von der Funktionsfähigkeit der Datenverarbeitung ganz oder jedenfalls überwiegend abhängig sind.[1150]

---

1140 *Ernst*, in: *Ders.* (Hrsg.), Hacker, Cracker und Computerviren, Rn. 268; *ders.*, NJW 2003, 3233 (3238).
1141 *Fischer*, StGB, § 303a Rn. 12.
1142 BT-Drucks 16/3656, S. 13.
1143 So auch ohne Begründung *Wuermeling*, CR 1994, 585 (591).
1144 BT-Drucks 10/5058, S. 35; Lackner/*Kühl*, StGB, § 303b Rn. 2; S/S-*Stree/Hecker*, § 303b Rn. 3.
1145 *Fischer*, StGB, § 303b Rn. 5.
1146 BT-Drucks. 10/5058, S. 35.
1147 BT-Drucks. 16/3656, S. 13.
1148 *BVerfGE* 120, 274 (303).
1149 Siehe nur LK-*Wolff*, StGB, § 303b Rn. 10.
1150 *Fischer*, StGB, § 303b Rn. 6; MüKoStGB-*Wieck-Noodt*, § 303b Rn. 8.

§ 303b Abs. 1 StGB setzt das erhebliche Stören einer Datenverarbeitung voraus. Der Begriff beschreibt keine bloße Tätigkeit, sondern verlangt als Erfolg,[1151] dass der reibungslose Ablauf der Datenverarbeitung nicht unerheblich beeinträchtigt wird.[1152] Tatbestandsmäßig sind etwa Programmveränderungen, die zu Systemabstürzen führen, sowie die Verhinderung einer Datenverarbeitung durch die Löschung der hierfür notwendigen, nicht alsbald einsetzbaren Software.[1153] Unter diesen Voraussetzungen sind die bereits bei § 303a StGB angesprochenen Gefahren für die Integrität des informationstechnischen Systems durch die Infiltration tatbestandsmäßig. § 303b Abs. 1 Nr. 2 StGB kommt aber nur insoweit in Betracht, als die Eingabe oder Übermittlung von Daten zugleich eine technische Infiltration des betroffenen informationstechnischen Systems darstellt.

iii. Schaden

Die Herleitung von Rechtsfolgen aus den § 823 Abs. 1, 2 BGB setzen ferner einen Schaden voraus. Schaden ist jede Beeinträchtigung eines Interesses.[1154] Dieses Interesse kann vermögenswerter oder rein ideeller Art sein.[1155] Die vorangegangene Prüfung orientierte sich mangels einer Spezialnorm für den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme an den von dem *BVerfG* konkret benannten Eingriffsmodalitäten. Diese bestimmen neben der jeweils einschlägigen Norm zugleich auch den konkreten Schaden. Gemeinsam ist jedoch allen Eingriffsmodalitäten, dass die selbstbestimmte Verfügung des berechtigten Nutzers über das von ihm genutzte informationstechnische System beeinträchtigt oder aufgehoben wird. Folglich sind umgekehrt all diejenigen Schadenspositionen zu berücksichtigen, die sich auf die Aufhebung der Vertraulichkeit und Integrität zurückführen lassen. Hierbei kann eine vermögenswerte oder bloß eine ideelle Rechtsposition betroffen sein.

Bei einer Verletzung des Eigentums oder des allgemeinen Persönlichkeitsrechts in Form der Datenlöschung, ist im Rahmen der *Differenzhypothese*[1156] der Wert der gelöschten Daten für den Betroffenen als Vermögensschaden anzusetzen.[1157] Ein Vermögensschaden kann ferner dann gegeben sein, wenn schon der Kenntnis von den in den vorhandenen Daten verkörperten Informationen selbst ein Vermögenswert zukommt. Hingegen lässt sich die Persönlichkeitsrelevanz einer Aufhebung der Vertraulichkeit und Integrität informationstechnischer Systeme aufgrund der bloßen Infiltration des Systems zur Überwachung des Nutzers oder zur Einsicht bereits vorhandener Daten ebenso wenig in Geld beziffern wie

---

1151 *Fischer*, StGB, § 303b Rn. 9; MüKoStGB-*Wieck-Noodt*, § 303b Rn. 18.
1152 BT-Drucks. 10/5058, S. 35.; Lackner/*Kühl*, StGB, § 303b Rn. 7; LK-*Wolff*, StGB, § 303b Rn. 26; S/S-*Stree/Hecker*, § 303b Rn. 9.
1153 *Fischer*, StGB, § 303b Rn. 9.
1154 Siehe nur MüKoBGB-*Oetker*, § 249 Rn. 16 m.w.N.
1155 MüKoBGB-*Oetker*, § 249 Rn. 16.
1156 Hierzu MüKoBGB-*Oetker*, § 249 Rn. 18ff.
1157 Vgl. *BGH* MMR 2009, 250 (252).

die im Anschluss tatsächlich erfolgende Überwachung oder Einsichtnahme. Es ist hierbei das allein ideelle Interesse des Nutzers betroffen, selbst darüber zu entscheiden, inwieweit seine Persönlichkeitsentfaltung Gegenstand der Wahrnehmung durch Dritte wird. Dieses Interesse wird nicht nur durch die unberechtigte Wahrnehmung selbst beeinträchtigt, sondern vor allem auch durch die fehlende Möglichkeit, das Ausmaß dieser Wahrnehmung festzustellen. Der Betroffene muss sich u.U. aber ein Mitverschulden nach § 254 Abs. 1, 2 BGB anrechnen lassen, sofern er bei der Aufhebung der Vertraulichkeit und Integrität des informationstechnischen Systems unbewusst mitgewirkt und dabei notwendige Sorgfaltsmaßstäbe außer Acht gelassen hat.

iv. Rechtsfolge, §§ 249ff. BGB

Art, Inhalt und Umfang des Schadensersatzes aus § 823 Abs. 1, 2 BGB richten sich nach den §§ 249ff. BGB. Der entstandene Schaden ist grds. im Wege der Naturalrestitution zu ersetzen. Es ist also derjenige Zustand herzustellen, der bestehen würde, wenn der zum Ersatz verpflichtende Umstand nicht eingetreten wäre (§ 249 Abs. 1 BGB).[1158]

(1) Naturalrestitution

Unter Zugrundelegung des soeben definierten Schadens erfordert die Naturalrestitution hinsichtlich der Vertraulichkeit und Integrität informationstechnischer Systeme die Beseitigung sämtlicher Handlungsfolgen, die zur Aufhebung der selbstbestimmten Verfügung des Nutzers geführt haben. Stellt diese Aufhebung die Folge der Infiltration des informationstechnischen Systems dar, bedeutet Naturalrestitution die Deinfiltration des Systems. Ist der Eingriff nicht mit der Infiltration des Systems verbunden, so etwa bei „Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben“,[1159] genügt zunächst die bloße Unterlassung der Überwachung. In dem Umfang, in dem es in beiden Fällen zu Datenerhebungen gekommen ist, ist der Dritte zur endgültigen Löschung dieser Daten verpflichtet.[1160] Sofern die Deinfiltration und die Unterlassung weiterer Überwachung zur Wiederherstellung des ursprünglichen Zustands von Vertraulichkeit und Integrität nicht ausreichend sind,[1161] hat der Verletzer auch die Kosten hierfür notwendiger

[1158] Siehe zum Folgenden auch *Hansen/Pfitzmann*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 131 (139f.).

[1159] *BVerfGE* 120, 274 (315).

[1160] *Bartsch*, CR 2008, 613 (616), mahnt zu Recht an, dass sich die vollständige Beseitigung der gewonnenen Informationen bei dem Dritten kaum verlässlich feststellen lässt.

[1161] *Hansen/Pfitzmann*, in: *Roggan* (Hrsg.), Online-Durchsuchungen, S. 131 (140), sehen eine dahingehende Notwendigkeit bei nach der Deinfiltration verbleibenden Sicherheitslücken sowie der möglichen Kenntnis des Verletzers von den vom Betroffenen für das System verwendeten Passwörtern u.ä.

Softwareneuinstallationen zu ersetzen (§ 249 Abs. 2 BGB). Kommt es zu Datenlöschungen ist der zur Wiederherstellung der gelöschten Daten erforderliche Aufwand zu ersetzen.[1162]

(2) Geldanspruch bei immaterieller Beeinträchtigung

In Betracht kommt ferner ein über den Ersatz der reinen Vermögensschäden hinausgehender Anspruch wegen der Beeinträchtigung bloß immaterieller Interessen. Ein Geldanspruch wegen der Beeinträchtigung immaterieller Interessen kann sich hier nur aus der Verletzung des allgemeinen Persönlichkeitsrechts des § 823 Abs.1 BGB ergeben.[1163] Nur bei schwerwiegenden Beeinträchtigungen folgt ein solcher Anspruch aus § 823 BGB i.V.m. Art. 1 Abs. 1, Art. 2 Abs. 1 GG.[1164] Dessen Zuerkennung unterliegt noch den einschränkenden Voraussetzungen, dass *(1)* eine schwerwiegende Verletzung des allgemeinen Persönlichkeitsrechts vorliegt, bei der *(2)* die Beeinträchtigung nach der Art der Verletzung nicht in anderer Weise befriedigend ausgeglichen werden kann.[1165]

(a) Schwerwiegende Beeinträchtigung

Ob eine schwerwiegende Verletzung des allgemeinen Persönlichkeitsrechts anzunehmen ist, richtet sich insbesondere nach der Bedeutung und Tragweite des Eingriffs, Anlass und Beweggrund des Handelnden sowie nach dem Grad seines Verschuldens.[1166] Gegenständliche informationstechnische Systeme können „allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten […], 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".[1167] Dem müssen die auf dem informationstechnischen System tatsächlich vorhandenen personenbezogenen Daten zwar nicht entsprechen. Jedoch ist der Vorgang der Infiltration gerade durch die Annahme veranlasst, dass sich eine solche Möglichkeit der Informationsgewinnung bietet. Denn Umfang und Vielfalt der tatsächlich vorhandenen personenbezogenen Daten sind von vornherein erst im Anschluss an die Infiltration verlässlich festzustellen. Die Intention des Handelnden zielt allein auf eine Datengewinnung unter Aufhebung der Vertraulichkeit und Integrität des informationstechnischen Systems. Er setzt sich damit willentlich und zum eigenen Vorteil über die selbstbestimmte Verfügung über das eigene informationstechnische System hinweg, die durch das allgemeine Persönlichkeits-

1162 *BGH* MMR 2009, 250 (251); *Meyer/Wehlau*, NJW 1998, 1585 (1588).
1163 So i.E. ohne nähere Begründung auch *Bartsch*, CR 2008, 613 (616).
1164 *BGH* NJW 1995, 861 (864); NJW 2000, 2195 (2197); NJW 2005, 215 (216).
1165 *BGHZ* 132, 13 (27); 143, 214 (218); *BGH* NJW 1985, 1617 (1619); NJW 1995, 861 (864); NJW 1996, 985 (986); NJW 2000, 2195 (2197); NJW 2005, 215 (216).
1166 *BGHZ* 132, 13 (27); *BGH* NJW 1985, 1617 (1619); NJW 1995, 861 (864); NJW 1996, 985 (986); NJW 2005, 215 (217).
1167 *BVerfGE* 120, 274 (314).

recht des § 823 Abs. 1 BGB geschützt wird. Damit der Eingriff sein Ziel erreichen kann, wird er regelmäßig heimlich erfolgen, so dass überhaupt schon die Wahrnehmung der Persönlichkeitsverletzung unsicher ist. Ferner kann die Infiltration mit der Löschung vorhandener Daten oder Funktionsstörungen des Systems verbunden sein. Im Rahmen der notwendigen Gesamtabwägung stellt die Infiltration eines informationstechnischen Systems die für einen Geldanspruch aufgrund immaterieller Beeinträchtigungen notwendige schwerwiegende Verletzung des allgemeinen Persönlichkeitsrechts dar.

(b) Fehlende Ausgleichsmöglichkeit

Dazu besteht nicht in jedem Fall eine andere befriedigende Ausgleichsmöglichkeit als eine Geldentschädigung. Anders als bei der Infiltration eines informationstechnischen Systems durch Strafverfolgungs- oder Gefahrenabwehrbehörden dürfte bei einem Handeln von Privatpersonen weniger die Erstellung eines Persönlichkeitsprofils als solches zentraler Beweggrund sein, sondern es werden wirtschaftliche Interessen im Vordergrund stehen. Ziel ist die Erlangung sensibler Informationen aus dem Verfügungsbereich des Betroffenen, um diese zu Anschlusstaten zu verwenden. Der Verletzer ist zwar bereits nach den §§ 249ff. BGB zur Deinfiltration des informationstechnischen Systems und zur Löschung erhobener personenbezogener Daten verpflichtet. Das Ausmaß der Informationsgewinnung durch den Verletzer wird der Betroffene jedoch kaum verlässlich feststellen können. Auch lässt sich eine bereits erfolgte Informationsgewinnung durch die anschließende Löschung der diese Informationen verkörpernden Daten nicht wieder rückgängig machen, sondern eine Löschung beseitigt lediglich die Möglichkeit des Informationszugriffs für die Zukunft.

Das Vorliegen eines auf Beseitigung gerichteten Anspruchs schließt jedoch die Zuerkennung eines darüberhinausgehenden Geldanspruchs nur dann aus, sofern bereits mit diesem Beseitigungsanspruch ein hinreichender Ausgleich für die Rechtsbeeinträchtigung erreicht wird.[1168] Gerade die Schwierigkeit, verlässlich festzustellen, welche Daten ein Dritter erhoben hat und welche Informationen bei diesem zurückbleiben, steht der Annahme eines solchen Ausgleichs entgegen.[1169] Wegen der Eigenart der Verletzung entfällt diese Ungewissheit durch den auf Beseitigung des Eingriffs und auf die künftige Unterlassung gerichteten Anspruch nicht. Der von dem Verletzer erlangte Informationsvorteil lässt sich nicht verlässlich abschöpfen. So würde die fehlende Feststellbarkeit eines Vermögensschadens der Zuerkennung eines Schadensersatzanspruchs entgegenstehen, obwohl der Verletzer womöglich sein Ziel der Informationsgewinnung erreicht hat. Jedoch

[1168] So für den Widerruf einer das allgemeine Persönlichkeitsrecht verletzenden Äußerung *BGH* NJW 1995, 861 (864).

[1169] So kommt etwa ein Anspruch auf Geldentschädigung dann in Betracht, wenn nicht sichergestellt ist, dass gerade diejenigen Empfänger einer bestimmten das allgemeine Persönlichkeitsrecht des Betroffenen beeinträchtigenden Tatsachenbehauptung durch einen Widerruf erreicht werden (*BGHZ* 132, 13 (29)).

rechtfertigt sich der Geldanspruch für bloß immaterielle Beeinträchtigungen des allgemeinen Persönlichkeitsrechts in erster Linie durch die Überlegung, dass das Persönlichkeitsrecht gegenüber erheblichen Beeinträchtigungen ansonsten ohne ausreichenden Schutz bliebe,[1170] der „Rechtsschutz der Persönlichkeit verkümmern würde".[1171] Die Ablehnung einer Geldentschädigung hätte jedoch gerade eine solche Schutzlücke zur Folge, da eine unbelastete Persönlichkeitsentfaltung in Form der selbstbestimmten Verfügung über das eigene informationstechnische System mangels eines „echten Hemmungseffekts"[1172] gegenüber Eingriffen Dritter nicht gewährleistet wäre.[1173] Von einer solchen selbstbestimmten Verfügung kann der Betroffene nur dann ausgehen, wenn die Aufhebung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Dritten derartige empfindliche Folgen haben kann, dass diese die Erwartung des Betroffenen begründen können, der Dritte werde aufgrund der ihm drohenden Sanktionen von einer entsprechenden Verletzungshandlung abgehalten.

Nicht zu entscheiden ist hingegen die Frage, ob juristischen Personen durch einen Geldanspruch wegen der Verletzung des allgemeinen Persönlichkeitsrechts überhaupt Genugtuung[1174] verschafft werden kann.[1175] Ist der Betroffene eine juristische Person, werden sowohl eine konkrete Informationsgewinnung als auch die besondere Ungewissheit über deren tatsächliches Ausmaß regelmäßig in Geld bezifferbar sein. Denn von der Aufhebung der Vertraulichkeit und Integrität sind Daten und hierin verkörperte Informationen betroffen, die der Verfolgung des spezifischen Zwecks der juristischen Person dienen. Diesen Informationen kommt daher regelmäßig ein wirtschaftlicher Wert zu, so dass bereits kein immaterieller Nachteil gegeben wäre.

### c. Produzentenhaftung

Der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme durch das allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB führt nur zu einem geringfügig erweiterten Anwendungsbereich der deliktsrechtlichen Produzentenhaftung. Seine diesbezügliche bloß „marginale Bedeutung"[1176] ändert sich

---

1170 *BGH* NJW 1971, 698 (699); NJW 1985, 1617 (1619).

1171 *BGH* NJW 1996, 985 (987); NJW 2000, 2195 (2197); NJW 2005, 215 (217).

1172 Hierzu *BGH* NJW 1995, 861 (865); *OLG Hamm* NJW-RR 2004, 919 (922).

1173 Die *Artikel-29-Datenschutzgruppe* benennt als nach Art. 23 Abs. 1 EG-Datenschutzrichtlinie ersatzfähigen immateriellen Schaden das Gefühl, sich sowohl im öffentlichen wie im privaten Bereich nicht länger unbeobachtet bewegen zu können, WP 168 (Fn. 619), S. 20 Ziff. 70 Fn. 21; ErwG 119 der DS-GVO-E fordert für Verstöße gegen die Verordnung wirksame, verhältnismäßige und *abschreckende* Sanktionen (Hervorhebung nur hier).

1174 Im Rahmen des Anspruchs auf Geldentschädigung wegen einer Verletzung des allgemeinen Persönlichkeitsrechts steht dieser Gesichtspunkt der Genugtuung des Betroffenen im Vordergrund (*BGH* NJW 1995, 861 (865) m.w.N.).

1175 Dafür: *BGHZ* 78, 274 (280); MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 249, dagegen: *BGH* NJW 1980, 2807 (2810).

1176 Produkthaftungshandbuch/*Foerste*, § 21 Rn. 128.

nicht grundlegend. Die Produzentenhaftung basiert auf der Vorstellung, dass der Hersteller eines Produkts mit dessen Inverkehrbringen eine Gefahrenquelle schafft, zu deren vorheriger und begleitender Sicherung er als Nutznießer verpflichtet ist.[1177] Die Sacheigenschaft des Produkts ist keine Voraussetzung für die Anwendung der Produzentenhaftung.[1178] Produkt kann daher grundsätzlich auch Software sein.[1179] Diese unterfällt ungeachtet der aus ihrer Komplexität folgenden besonderen Anfälligkeit für Programmierfehler den Grundsätzen der Produzentenhaftung.[1180] Aus dem Bewusstsein der Fehlerhaftigkeit ergeben sich vielmehr entsprechend höhere Anforderungen an die Produktbeobachtungspflicht.[1181] Die Infiltration eines informationstechnischen Systems kann insbesondere durch die Ausnutzung von Sicherheitslücken in der auf dem System verwendeten Software erfolgen. Insoweit kommt die deliktische Haftung des Softwareproduzenten nach den Grundsätzen der Produzentenhaftung in Betracht. Die Infiltration des informationstechnischen Systems eines berechtigten Nutzers stellt jedenfalls eine Verletzung des allgemeinen Persönlichkeitsrechts des Nutzers dar. Sofern entweder das System selbst Sachqualität aufweist und der Nutzer hieran Eigentum oder der Nutzer Eigentum an dem Datenträger hat, von dem Daten gelöscht wurden, kommt auch eine Eigentumsverletzung durch eine Datenlöschung in Betracht. Mit dem Inverkehrbringen der fehlerhaften Software beruht die Rechtsgutsverletzung auf einer adäquat kausalen Handlung des Produzenten. Die Ausnutzung einer Sicherheitslücke in der auf einem informationstechnischen System installierten Software ist ein gängiger Weg zur Infiltration eines solchen Systems.

i. Verkehrssicherungspflichten

Der Produzent müsste ferner objektiv gegen eine Verkehrssicherungspflicht verstoßen haben. Diesen Pflichten genügt er nur dann, wenn er diejenigen Maßnahmen trifft, die im konkreten Fall zur Vermeidung oder Beseitigung einer Gefahr sowohl erforderlich als auch zumutbar sind.[1182] Die Verletzung von Verkehrssicherungspflichten wird anhand von Konstruktions-, Fabrikations-, Instruktions- oder Entwicklungsfehlern des Produkts konkretisiert. Die zur Infiltration eines informationstechnischen Systems ausgenutzte Sicherheitslücke dürfte dabei regelmäßig einen Konstruktions- oder Entwicklungsfehler darstellen. Konstruktionsfehler beziehen sich auf die Pflicht des Produzenten, dass ein von ihm in Ver-

[1177] Bamberger/Roth/*Spindler*, § 823 Rn. 478.
[1178] Vgl. Bamberger/Roth/*Spindler*, § 823 Rn. 483; MüKoBGB-*Wagner*, § 823 Rn. 599; Staudinger/*Hager* (2009), § 823 Rn. F6.
[1179] Staudinger/*Hager* (2009), § 823 Rn. F6; *Taeger*, Außervertragliche Haftung, S. 239ff; *Spindler*, NJW 1999, 3737; *ders.*, NJW 2004, 3145.
[1180] *Meier/Wehlau*, CR 1990, 95 (95f.); *Spindler*, CR 2005, 741; *Taeger*, Außervertragliche Haftung, S. 246.
[1181] *Meier/Wehlau*, CR 1990, 95 (97); *Spindler*, NJW 2004, 3145 (3147).
[1182] *BGH* NJW 1988, 2611; NJW 1990, 906 (907).

kehr gebrachtes Produkt seinem Bauplan nach die geforderte Sicherheit bietet.[1183] Solche Konstruktionsfehler stellen auch Sicherheitslücken dar, durch welche die Infiltration eines informationstechnischen Systems ermöglicht wird.[1184] Für einen solchen Fehler kann sich der Produzent nur durch den Nachweis der Durchführung von höchsten Sicherheitsansprüchen genügenden Qualitätsprüfungen und Funktionstests entlasten.[1185] Entwicklungsfehler stellen nur dann keinen Verstoß gegen eine Verkehrssicherungspflicht dar, wenn sie zum Zeitpunkt der Inverkehrgabe des Produkts nicht erkennbar oder nicht vermeidbar waren.[1186] Maßgeblich ist das objektiv zugängliche Gefahrenwissen.[1187] Die Verkehrssicherungspflichten des Produzenten enden jedoch nicht mit der Inverkehrgabe des Produkts. Der Produzent muss im Anschluss sowohl sein Produkt auf bisher unbekannte schädliche Eigenschaften hin beobachten als auch Information über sonstige eine Gefahrenlage schaffende Verwendungsfolgen einholen.[1188] Softwarehersteller können ihren Produktbeobachtungspflichten vor allem dadurch genügen, dass sie auf Fehlermeldungen reagieren und Updates oder Patches zum Download bereitstellen.[1189] Die Reichweite der Produktbeobachtungspflichten richtet sich in erster Linie nach der drohenden Gefahr.[1190] Mit zunehmender Verbreitung einer Software sind nicht nur mehr Nutzer von einer Sicherheitslücke betroffen, sondern die am weitesten verbreitete Software ist regelmäßig auch das bevorzugte Angriffsziel.[1191] Bei der Bestimmung der Reichweite der Produktbeobachtungspflichten ist dann auch das allgemeine Persönlichkeitsrecht in Form der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu berücksichtigen. Angesichts des Potenzials der Infiltration zur Profilbildung des Nutzers kann im Einzelfall eine schwere Persönlichkeitsverletzung einer Vielzahl von Betroffenen drohen. Umgekehrt erfordert die Vermeidung dieser Gefahr keine zusätzlichen Anforderungen an den Produzenten. Die ausdrückliche Konkretisierung des Schutzbereichs des allgemeinen Persönlichkeitsrechts auch auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme erweitert den Umfang möglicher Pflichten nicht. Allein mit dem Schließen der Sicherheitslücke kann die Gefahr einer Profilbildung wie die einer Datenlöschung oder sonstiger außerhalb des Schutzbereichs der Gewährleistung der Vertraulichkeit

---

1183 MüKoBGB-*Wagner*, § 823 Rn. 628.
1184 Konkrete Beispiele bei *Sodtalbers*, Softwarehaftung im Internet, Rn. 235.
1185 *Meier/Wehlau*, CR 1990, 95 (97); *Taeger*, Außervertragliche Haftung, S. 247.
1186 *BGHZ* 51, 91 (105f.); 80, 186 (197).
1187 Staudinger/*Hager* (2009), § 823 Rn. F19.
1188 *BGHZ* 80, 199 (202).
1189 *Sodtalbers*, Softwarehaftung im Internet, Rn. 545
1190 Speziell für Software: *Taeger*, Außervertragliche Haftung, S. 255; *Abel*, CR 1999, 680 (683); *Spindler*, CR 2005, 741 (743); allgemein: Bamberger/Roth/*Spindler*, § 823 Rn. 511; MüKoBGB-*Wagner*, § 823 Rn. 647; Staudinger/*Hager* (2009), § 823 Rn. F21.
1191 *Sodtalbers*, Softwarehaftung im Internet, Rn. 545.

und Integrität informationstechnischer Systeme liegender Gefahren beseitigt werden. Die einen Produzenten dahingehend im Einzelfall treffenden Pflichten gehen mithin nicht über denjenigen Umfang hinaus, der ihn schon zuvor treffen konnte.

ii. Haftung für Verhalten Dritter

Verkehrssicherungspflichten erfassen grundsätzlich auch solche Gefahren, die erst das vorsätzliche Eingreifen eines Dritten begründet.[1192] Eine Haftung des Softwareproduzenten kommt daher auch für solche Schäden in Betracht, die erst von Programmierern von Viren[1193] oder Würmern[1194] sowie von Hackern verursacht werden.[1195] Hingegen kann die Verkehrssicherungspflicht nicht jedes Risiko abdecken, wenn der Dritte einfacher und mit geringerem Aufwand als der Pflichtige einen Schaden vermeiden kann.[1196] Kriterien für die Abwägung, ob den Nutzer eines informationstechnischen Systems Verkehrssicherungspflichten zum Einsatz von Sicherungsmaßnahmen treffen, sind bei einer Abwägung von Aufwand und Gefährdungslage die Bekanntheit des Problems und seiner Lösung, die technische und wirtschaftliche Zumutbarkeit sowie eine Beurteilung der notwendigen Aktualität des Systems durch den Nutzer.[1197] Zwar unterfällt ein informationstechnisches System unabhängig von der konkreten Sicherung dem Schutzbereich des *GVIiS*. Die Anerkennung eines solchen Schutzbereichs ist jedoch nicht gleichzusetzen mit der Festsetzung eines entsprechend weiten zivilrechtlichen Haftungsmaßstabs. Der Definition des grundrechtlichen Schutzbereichs liegt die Erwägung zugrunde, dass die Zulässigkeit einer Überwachung nicht von einer besonderen Sicherung des Systems abhängig sein kann, sofern nur eine berechtigte Vertraulichkeits- und Integritätserwartung besteht. Der zu gewinnende Einblick in die Persönlichkeit ist unabhängig davon schutzwürdig, dass hiergegen besondere technische Sicherungen bestehen. Die Bewertung der Schutzbedürftigkeit eines bestimmten Rechtsguts enthält nicht gleichzeitig auch die Beantwortung der Frage, wer für eine Verletzung dieses Rechtsguts wie und in welchem Maße haftet. Die Haftung des Produzenten für Schäden aufgrund der Infiltration eines informationstechnischen Systems durch Dritte lässt sich daher nur für jeden Einzelfall bestimmen.

---

1192 *BGH* NJW 1971, 459 (460f.); VersR 1976, 149 (150); NJW 1980, 223; NJW 1990, 1236 (1237).

1193 Der Virus ist ein pathologisches auf ein Wirtsprogramm angewiesenes Kleinstprogramm, das bei dem Wirt schlummert und seine meist destruktive Wirkung nach dem Eintreten eines Auslösers (Zeit, Ladehäufigkeit etc.) entfaltet (*Fischer/Hofer*, Lexikon Informatik, Stichwort „Virus").

1194 Eine Wurm ist eine Form eines sabotierenden Malware-Programms mit, das sich im Arbeitsspeicher eines Systems stark vermehrt, selbst lauffähig und deshalb nicht auf ein Wirtsprogramm angewiesen ist (*Fischer/Hofer*, Lexikon Informatik, Stichwort „Wurm").

1195 *Spindler*, CR 2005, 741 (743f.).

1196 Bamberger/Roth/*Spindler*, § 823 Rn. 242.

1197 *Mantz*, K&R 2007, 566 (571).

iii. Rechtsfolge

Ist die Infiltration des informationstechnischen Systems mit einer Datenlöschung verbunden, entsteht dem Betroffenen ein Vermögensschaden. Zu ersetzen ist regelmäßig der finanzielle Aufwand zur Deinfiltration und Wiederherstellung der gelöschten Daten. Hingegen kommt der Ersatz eines bloß ideellen Nachteils aufgrund der Verletzung des allgemeinen Persönlichkeitsrechts nicht in Betracht. Die Haftungsgrundlage der Produzentenhaftung und diejenige der Geldentschädigung bei schwerwiegenden Persönlichkeitsrechtsverletzungen beruhen auf unterschiedlichen Erwägungen. Als Nutznießer der Inverkehrgabe eines Produkts soll der Produzent zur Sicherung vor mit diesem Produkt verbundenen Gefahren verpflichtet sein. Die Persönlichkeitsverletzung durch die Infiltration des informationstechnischen Systems liegt jedoch gerade in der individuellen Missachtung der Entscheidung über die Verfügung des Betroffenen über das von ihm genutzte System durch den Dritten. Die Ausforschung der Persönlichkeit des Betroffenen und die Ungewissheit darüber, welche Informationen der Dritte über den Betroffenen erlangt hat, sind an die bestimmte Person des Dritten gebunden. Der aus dem Eingriff folgende ideelle Nachteil ist gerade keine Schadensposition, die losgelöst von der Person des Verletzers ersatzfähig wäre. Genugtuung i.S. einer Kompensation von Nachteilen, die auf andere Art und Weise nicht ausgeglichen werden können,[1198] kann dem Betroffenen nur durch einen Anspruch gegen den unmittelbar handelnden Dritten, nicht jedoch gegenüber dem Produzenten verschafft werden.[1199]

d. § 1004 Abs. 1 BGB (analog) (i.V.m. § 823 Abs. 1 BGB)

Auch die Ansprüche aus § 1004 Abs.1 BGB (analog) i.V.m. § 823 Abs. 1 BGB kommen wiederum sowohl gegen den unmittelbar handelnden Dritten als auch gegen an der Rechtsverletzung nur mittelbar Beteiligte in Betracht.

i. Rechtsgutsbeeinträchtigung

Die Infiltration eines informationstechnischen Systems kann zunächst Datenlöschungen oder Funktionsstörungen des Systems zur Folge haben, so dass sich Ansprüche aus § 1004 Abs. 1 S. 1, 2 BGB zunächst aufgrund der Beeinträchtigung des Eigentums an dem System oder einem zu dem System gehörenden Datenträger ergeben können. Entgegen seines Wortlauts findet § 1004 BGB über den Schutz des Eigentums hinaus aber auch (analoge[1200]) Anwendung auf Beeinträchtigungen des allgemeinen Persönlichkeitsrechts.[1201] Daher können Ansprüche auf

[1198] MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 238.
[1199] I.d.S. weist auch Produkthaftungshandbuch/*Foerste*, § 21 Rn. 128, auf die besonderen Voraussetzungen des Ersatzes immaterieller Schäden hin.
[1200] Siehe z.B. *OLG Hamburg* ZUM 2007, 483 (484f.).
[1201] Siehe z.B. *BGH* NJW 1990, 1986 (1988); NJW 2006, 207 (208).

Beseitigung und Unterlassung auch aufgrund der bloßen Aufhebung der Vertraulichkeit und/oder Integrität des informationstechnischen Systems bestehen. Infolge der Infiltration des Systems steht die private Sphäre autonomer Lebensgestaltung des Betroffenen dem Zugriff des Dritten offen. Der Beseitigungsanspruch des § 1004 Abs. 1 S. 1 BGB setzt ferner voraus, dass die Beeinträchtigung gegenwärtig und gerade nicht in der Vergangenheit abgeschlossen ist.[1202] Notwendig ist daher eine fortdauernde Funktionsstörung. Eine Datenlöschung darf sich nicht in einer bloß einmaligen Löschung erschöpfen. Ebenso muss die Beeinträchtigung des allgemeinen Persönlichkeitsrechts in einer noch andauernden Aufhebung der Vertraulichkeit und/oder Integrität des informationstechnischen Systems liegen.

ii. Störer

Den Schuldner der Ansprüche auf Beseitigung oder Unterlassung bezeichnet § 1004 Abs. 1 BGB als Störer. Dies ist derjenige, dem die Beeinträchtigung zugerechnet werden kann.[1203] Nach der Unterscheidung zwischen Handlungs- und Zustandsstörer ist Handlungsstörer, wer die Beeinträchtigung des betroffenen Rechtsguts durch positives Tun oder pflichtwidriges Unterlassen adäquat verursacht hat.[1204] Als Störer kommt demnach jedenfalls in Betracht, wer die Beeinträchtigung durch sein eigenes Handeln oder pflichtwidriges Unterlassen herbeigeführt hat.[1205] Gegner der Ansprüche aus § 1004 Abs. 1 BGB kann daher zunächst der unmittelbar handelnde Dritte sein, der mit der Infiltration des informationstechnischen Systems dessen Vertraulichkeit und/oder Integrität selbst aufhebt. Darüber hinaus begründet aber auch schon die nur mittelbare Verursachung die Störereigenschaft.[1206] Mittelbarer Störer ist, wer sich Beeinträchtigungen, die er nicht selbst, sondern ein Dritter unmittelbar vorgenommen hat, zurechnen lassen muss.[1207] Es ist danach auch die Inanspruchnahme desjenigen denkbar, der eine Infiltration nur mittelbar mitverursacht hat. Als ein solcher Verursachungsbeitrag käme etwa das Offenlassen einer Sicherheitslücke in der von dem Betroffenen verwendeten Software in Betracht, die von dem unmittelbar Handelnden zur Infiltration ausgenutzt wird.

(1) Willentlicher und adäquat kausaler Beitrag

Im Sinne einer solchen nur mittelbaren Verursachung kann bei der Verletzung absoluter Rechte in Anspruch genommen werden, wer ohne Täter oder Teilnehmer zu sein in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des

[1202] Bamberger/Roth/*Fritzsche*, § 1004 Rn. 50; MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 220; Soergel/*Münch*, § 1004 Rn. 63ff.; Staudinger/*Gursky* (2006), § 1004 Rn. 17.
[1203] MüKoBGB-*Baldus*, § 1004 Rn. 149.
[1204] *BGH* NJW 2005, 1366 (1368); NJW 2007, 432.
[1205] Soergel/*Münch*, § 1004 Rn. 114.
[1206] *BGH* NJW 2000, 2901 (2902); NJW 2006, 992.
[1207] Soergel/*Münch*, § 1004 Rn. 135.

geschützten Rechts beiträgt.[1208] Es kann dabei bereits die Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlich handelnden Dritten genügen, sofern der in Anspruch genommene die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte.[1209] Das Offenlassen einer Sicherheitslücke stellt einen solchen willentlichen Beitrag des mittelbar Handelnden dar. Zwar liegt das Schließen einer solchen Lücke auch in dessen eigenem Interesse. Eine dahingehende Unterlassung wird mithin kaum mit einer bewussten Entscheidung für die Sicherheitslücke verbunden sein. Schon deren Existenz wird dem mittelbar Handelnden regelmäßig nicht bekannt sein. Allein entscheidend ist jedoch, dass der Verursachungsbeitrag des mittelbar Handelnden ein vom menschlichen Willen steuerbares Verhalten darstellt. Das Merkmal der Willentlichkeit enthält kein Wissenselement, sondern dient allein dem Ausschluss nicht willentlich gesteuerter Verhaltensweisen.[1210] Die Infiltration des informationstechnischen Systems ist in der hier zu § 1004 BGB betrachteten Konstellation nur mittels des Ausnutzens einer Sicherheitslücke in der auf dem System installierten Software möglich. Das Offenlassen dieser Lücke und damit der Verursachungsbeitrag des mittelbar Handelnden ist daher notwendige Voraussetzung und zugleich ursächlich für die Infiltration des Systems. Die notwendige Adäquanz liegt ebenfalls vor. Voraussetzung ist eine Eignung dergestalt, dass ein Erfolg dieser Art im Allgemeinen und nicht nur unter besonders eigenartigen, unwahrscheinlichen und nach dem gewöhnlichen Verlauf der Dinge außer Betracht zu lassenden Umständen herbeigeführt wird.[1211] Gerade das Ausnutzen einer Sicherheitslücke ist ein üblicher Weg der technischen Infiltration eines informationstechnischen Systems.

(2) Prüfungspflichten

Als haftungsbegrenzende Voraussetzung muss auf Seiten des nur mittelbar Handelnden die Verletzung von Prüfungspflichten hinzutreten. Der Umfang solcher Pflichten richtet sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist.[1212] Im Gegensatz zu den Verkehrssicherungspflichten des Produzenten im Rahmen der deliktischen Produzentenhaftung fehlt der Störerhaftung das weitere Korrektiv eines Verschuldenserfordernisses. Für die Bestimmung der Reichweite der Prüfungspflichten bietet sich eine Parallele zu den allgemeinen Verkehrssicherungspflichten des § 823 Abs. 1 BGB an.[1213] Verkehrssicherungspflichten bestehen für denjenigen,

[1208] *BGH* NJW 2010, 2061 (2062) m.w.N.; für einen diese Form der Verantwortlichkeit beschreibenden sog. engen Störerbegriff u.a. *Hartmann*, Unterlassungsansprüche im Internet, S. 31f., 47; *Ahrens*, WRP 2007, 1281 (1281f.).

[1209] *BGH* NJW 1999, 1960; NJW 2001, 3265 (3266).

[1210] *Wiebe*, CR 2002, 53 (54); *Wiebe*, in: *Ernst/Vassilaki/Wiebe*, Hyperlinks, Rn. 42.

[1211] *BGH* NJW 2000, 2901 (2902) m.w.N.

[1212] *BGH* NJW 2010, 2061 (2062) m.w.N.

[1213] So *Spindler/Volkmann*, WRP 2003, 1 (7); *Spindler*, GRUR 2011, 101 (102); *Leistner/Stang*, WRP 2008, 533 (534ff.).

der in seinem Verantwortungsbereich eine Gefahr schafft oder andauern lässt.[1214] Als eine solche Gefahr kommt hier entsprechend den Ausführungen zur Produzentenhaftung das Inverkehrbringen der Software in Betracht. Bei der Bestimmung der Prüfungspflichten sind Funktion und Aufgabenstellung des mittelbaren Störers sowie die Eigenverantwortung des unmittelbar handelnden Dritten zu berücksichtigen.[1215] In der vorliegenden Gestaltung wäre der mittelbare Störer lediglich derjenige, der die Software des infiltrierten Systems erstmalig in Verkehr gebracht hat. Er betreibt keine eigene Plattform, auf der die Rechtsverletzung stattfindet. Anders als bei dem Betreiber solcher Handelsplattformen, der gerade mit deren Betrieb eigene wirtschaftliche Interessen verfolgt, aus denen eine besondere Rücksichtnahmepflicht auf durch den Betrieb gefährdete Rechtsgüter verlangt werden kann,[1216] erschöpft sich das wirtschaftliche Interesse hier in dem bloßen Vertrieb der Software. Es fehlt damit bereits an einem „Einsatz organisatorischer oder technischer Mittel".[1217] Die in Rede stehende Rechtsverletzung erfolgt gerade nicht über die Infrastruktur des mittelbaren Störers, sondern über diejenige des Betroffenen. Die verwendete Software befindet sich außerhalb der Einflusssphäre des mittelbar Handelnden. Ein Zugriff ist regelmäßig nur über Kommunikationsnetze mit Einverständnis des Betroffenen möglich. Diesem Beitrag des mittelbaren Störers steht das vorsätzliche Verhalten des Dritten gegenüber. Dieser nutzt gezielt eine Sicherheitslücke zur Infiltration aus. Die hierbei verfolgten Interessen stehen in keinerlei Zusammenhang mit den Interessen des Softwareproduzenten.

Zwar können bei einem Produkt, das nicht nur rechtmäßig, sondern auch für Eingriffe in Rechte Dritter verwendet werden kann, Prüfungspflichten dahingehend bestehen, dass der rechtsverletzende Gebrauch des Produkts durch selbständig handelnde Dritte bei objektiver Betrachtung nicht außerhalb aller Wahrscheinlichkeit liegt.[1218] In der betrachteten Konstellation verwendet jedoch nicht der Dritte ein Produkt des mittelbar Handelnden, sondern der Betroffene. Der Dritte nimmt vielmehr eine rechtsverletzende Manipulation des Produkts vor. Damit liegt der unterstützende Beitrag des mittelbar Handelnden aber völlig außerhalb der bestimmungsgemäßen Verwendung des Produkts. In dieser Konstellation ist dem nur mittelbar Handelnden die Prüfung einer fortbestehenden Gefahr von Rechtsverletzungen nicht zumutbar. Sein adäquat kausaler Beitrag tritt gegenüber dem eigenverantwortlichen Handeln des unmittelbar handelnden Dritten völlig zurück. Prüfungspflichten kommen daher von vornherein nicht in Betracht.

---

[1214] *BGHZ* 14, 83 (85); 123, 102 (105f.).
[1215] *BGH* GRUR 2004, 693 (695); GRUR 2003, 969 (970).
[1216] Vgl. *BGH* MMR 2004, 668 (671); NJW 2010, 2061.
[1217] Hierzu *BGH* GRUR 1999, 418 (420).
[1218] Hierzu *BGH* MMR 2009, 625 (626); *OLG Hamburg* ZUM-RD 2007, 569.

iii. Interessenabwägung

Zur im Rahmen der Feststellung der Rechtswidrigkeit der Beeinträchtigung notwendigen Güter- und Interessenabwägung siehe die Ausführungen zum allgemeinen Persönlichkeitsrecht des § 823 Abs. 1 BGB.[1219]

iv. Rechtsfolge

Der Betroffene kann von dem Störer die Beseitigung der Beeinträchtigung verlangen, § 1004 Abs. 1 S. 1 BGB, sowie diesen bei der Befürchtung weiterer Beeinträchtigungen auf Unterlassung in Anspruch nehmen, § 1004 Abs. 1 S. 2 BGB.

(1) Beseitigung, § 1004 Abs. 1 S. 1 BGB

Der Anspruch auf Beseitigung ist auf die Beendigung der gegenwärtigen Störung für die Zukunft gerichtet.[1220] Der Störer hat seine Einwirkungshandlung aufzugeben[1221] und die Beeinträchtigung vollständig zu beseitigen.[1222] Er schuldet jedoch nicht auch die Beseitigung von Behinderungen und Beschädigungen, die sich aus dem störenden Eingriff als weitere Folge ergeben.[1223] Hingegen kann der Störer auch zur anschließenden Beseitigung solcher Beeinträchtigungen verpflichtet sein, die notwendig mit der Beseitigung der unmittelbaren Beeinträchtigung verbunden sind.[1224] Der Beseitigungsanspruch umfasst damit auch die unmittelbaren Fortwirkungen der Beeinträchtigung.[1225] In diesem Sinne erfordert sowohl die Beseitigung der Eigentumsbeeinträchtigung als auch diejenige des allgemeinen Persönlichkeitsrechts die Deinfiltration des informationstechnischen Systems. Notwendig ist die vollständige Beseitigung fortdauernder Funktionsstörungen und Datenlöschungen. Der Zugang des Dritten zu der privaten Sphäre autonomer Lebensgestaltung des Betroffenen und die hierdurch ermöglichte Informationsgewinnung sind für die Zukunft zu unterbinden. Notwendig ist daher die Beendigung der mit der Infiltration verbundenen Manipulation des Systems. Da der Störer den Erfolg seiner störenden Tätigkeit rückgängig oder für die Zukunft wirkungslos zu machen hat,[1226] kann eine Beendigung der Manipulation wiederum auch deren Umkehrung bedeuten.

Der so festgestellte Umfang der Beseitigungspflicht wird zum Einen dann erweitert, wenn sich die Manipulation zwar rückgängig machen lässt, aber zur Beseitigung der Störung nicht ausreichend ist. Dies wäre dann der Fall, wenn es trotz

[1219] Siehe S. 168.
[1220] Bamberger/Roth/*Fritsche*, § 1004 Rn. 56.
[1221] Staudinger/*Gursky* (2006), § 1004 Rn. 136.
[1222] Staudinger/*Gursky* (2006), § 1004 Rn. 144.
[1223] MüKoBGB-*Baldus*, § 1004 Rn. 225.
[1224] *BGH* NJW 1986, 2640 (2641f.); NJW 1996, 845 (846f.); NJW 1997, 2234 (2235); NJW 2005, 1366 (1367).
[1225] Bamberger/Roth/*Fritsche*, § 1004 Rn. 60.
[1226] MüKoBGB-*Baldus*, § 1004 Rn. 225.

der Deinfiltration des Systems weiterhin zu Funktionsstörungen und/oder Datenlöschungen kommt oder das System weiterhin dem Zugriff Dritter offensteht. Dann kann der Beseitigungsanspruch auch die notwendige Neuinstallation der betroffenen Software erfassen. Denn die Ursache der Beeinträchtigung ist nicht allein die Manipulation selbst, sondern sind auch sämtliche mit der Manipulation verbundenen Veränderungen an der Software des Systems. Diese Veränderungen können nicht isoliert von der Manipulation betrachtet werden. Ebenso wird eine Neuinstallation notwendig, wenn die Manipulation bereits aus technischen Gründen nicht isoliert rückgängig gemacht werden kann. Auch dann wäre eine Neuinstallation vom Beseitigungsanspruch des § 1004 Abs. 1 S. 1 BGB erfasst. Denn der Störer trägt das Risiko, aufgrund der technischen Gegebenheiten eine erweiterte Leistung erbringen zu müssen, als es zu der Beseitigung der reinen Störung an sich erforderlich wäre.[1227]

(2) Unterlassung, § 1004 Abs. 1 S. 2 BGB

Der Anspruch auf Unterlassung setzt gem. § 1004 Abs. 1 S. 2 BGB eine Wiederholungsgefahr voraus. Dies ist die auf konkrete Anhaltspunkte gegründete objektive ernstliche Besorgnis weiterer Störungen.[1228] Die Wiederholungsgefahr wird regelmäßig durch die bereits erfolgte rechtswidrige Beeinträchtigung begründet.[1229] An die Widerlegung dieser Vermutung sind hohe Anforderungen zu stellen.[1230] Hingegen dürfte mit dem Schließen der zur Infiltration genutzten Sicherheitslücke oder der dauerhaften Entfernung eines entsprechenden Schadprogramms die Vermutung der Wiederholungsgefahr hinsichtlich dieser konkreten Infiltrationsmethode widerlegt sein. Wenn die konkrete Infiltrationsmethode schon technisch nicht mehr realisierbar ist, kann mangels objektiver Möglichkeit der Wiederholung[1231] zwangsläufig auch keine dahingehende Gefahr bestehen. Umgekehrt ist das Interesse des Dritten an den zu erlangenden Informationen zu berücksichtigen. Sofern das informationstechnische System des Betroffenen i.d.S. eine dauerhaft interessante Informationsquelle darstellt, dürfte die Wiederholungsgefahr allenfalls durch die Abgabe einer strafbewehrten Unterlassungserklärung[1232] zu widerlegen sein. Besteht hingegen nur die konkrete Gefahr einer erstmaligen zukünftigen Rechtsverletzung, kommt auch ein vorbeugender Unterlassungsan-

[1227] *BGH* NJW 2005, 1366 (1368).
[1228] *BGH* GRUR 1992, 318 (319); Palandt/*Bassenge*, § 1004 Rn. 32.
[1229] *BGH* GRUR 1992, 318 (319); NJW 2004, 1035 (1036); GRUR 2005, 76 (78); Bamberger/Roth/*Fritsche*, § 1004, Rn. 83; MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 214.
[1230] *BGH* NJW 1994, 1281 (1283); NJW 1999, 356 (359).
[1231] Siehe hierzu etwa *BGH* GRUR 1992, 318 (319f.); NJW 1995, 132 (134).
[1232] *BGH* NJW 1996, 723 (724).

spruch in Betracht.[1233] Ein solcher Anspruch dürfte hier jedoch ohnehin leerlaufen, da die Infiltration eines informationstechnischen Systems typischerweise weder angekündigt wird noch vorausgesehen werden kann.[1234]

### *2. Schutzlücke*

Der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme lässt sich damit schon de lege lata auch auf privatrechtlicher Ebene umsetzen. Das allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB kann im Rahmen der bestehenden Fallgruppen einer Rechtsverletzung ohne entscheidende Ausweitung des bestehenden Schutzbereiches auch auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme konkretisiert werden. Von den (schadensersatzrechtlichen) Rechtsfolgen einer Infiltration dürfte jedenfalls ein solcher Hemmungseffekt ausgehen, dass zumindest der Nutzer eines informationstechnischen Systems die berechtigte Erwartung begründen kann, dass Dritte aufgrund der ihnen drohenden Folgen grundsätzlich von entsprechenden Verletzungshandlungen abgehalten werden. Aufgrund dieser Erwartung wird dem Nutzer eine ungehinderte Persönlichkeitsentfaltung durch die Nutzung seines informationstechnischen Systems auch auf privatrechtlicher Ebene ermöglicht.

Damit ist das Untermaßverbot als Grenze des gesetzgeberischen Gestaltungsspielraums nicht erreicht.[1235] Es bestehen insofern Schutzvorkehrungen, die jedenfalls nicht gänzlich ungeeignet sind. Die Notwendigkeit der Erweiterung der strafrechtlichen Sanktionsmöglichkeiten ergibt sich aus dem Schutzauftrag, der mit dem objektiv-rechtlichen Gehalt des *GVIiS* verbunden ist, nicht. Eine hinter dem grundrechtlich gebotenen Umfang zurückbleibende Lücke hinsichtlich des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme auf privatrechtlicher Ebene lässt sich danach nicht feststellen.[1236] Entscheidende Bedeutung kommt § 823 Abs. 1 BGB insoweit zu, als mit der Infiltration eines informationstechnischen Systems die Schwelle der Strafbarkeit gem. § 202a Abs. 1 StGB schon mangels Überwindung einer besonderen Zugangssicherung nicht erreicht ist.[1237] Ein spezifisch auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme ausgelegter Schutz, der dem Verhältnis des BDSG zum *RiS* ent-

---

[1233] *BGH* NJW 2004, 3701 (3702); Bamberger/Roth/*Fritsche*, § 1004 Rn. 87f.

[1234] *Bartsch*, CR 2008, 613 (616).

[1235] *Härting/Schneider*, ZRP 2011, 233 (235); ZD 2011, 63 (68), entnehmen der gegenständlichen Entscheidung hingegen einen konkreten Gesetzgebungsauftrag, „klare Regeln für die Sammlung und Nutzung von Datenbeständen zu schaffen"; auch *Kutscha*, DuD 2012, 391 (394), sieht zum Erhalt der selbstbestimmten Teilnahme des Einzelnen an Informations- und Kommunikationsnetzen die Notwendigkeit „positivrechtlicher Ausgestaltung und wirksamer Umsetzungskontrolle"; *Schulz*, DuD 2012, 395 (396), entnimmt dem Urteil des *BVerfG* eine „staatliche Infrastrukturverantwortung" ohne bei den angeführten Beispielen konkret auf die Voraussetzungen der Eröffnung des Schutzbereiches des *GVIiS* einzugehen.

[1236] A.A. *Bartsch*, CR 2008, 613 (616).

[1237] Ebenso generell zum allgemeinen Persönlichkeitsrecht des § 823 Abs. 1 BGB MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 101.

spricht, kann jedoch keiner der geprüften Normen des BGB entnommen werden. Diese Rechtslage führt damit zu einer Zersplitterung des Schutzes auf verschiedene Normen. Zwar werden die von dem *BVerfG* aufgelisteten Eingriffsmodalitäten und die mit einem Zugriff verbundenen Nebenfolgen von der aktuellen Rechtslage erfasst. Die einschlägigen Normen sind jedoch jeweils anhand der konkreten Umstände des Zugriffs auf das informationstechnische System in unnötig komplizierter Weise abzugrenzen.

### III. Mittelbare Drittwirkung

Nach der bisherigen Darstellung ist der Schutzbereich des *GVIiS* dann betroffen, wenn die selbstbestimmte Verfügung des berechtigten Nutzers eines informationstechnischen Systems gegen dessen Willen aufgehoben wird. Neben einem solchen unberechtigten Zugriff auf das System kann der Nutzer aber auch in den Zugriff durch einen Dritten einwilligen. Gegenstand privatrechtlicher Streitigkeiten hinsichtlich der selbstbestimmten Verfügung des berechtigten Nutzers über sein informationstechnisches System ist grds. allein das allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB. Denn letzteres schützt umfassend die Vertraulichkeit und Integrität informationstechnischer Systeme auf zivilrechtlicher Ebene in der Gestalt, die es aufgrund der Ausübung verfassungsrechtlicher Schutzpflichten den Schutzbereich des *GVIiS* betreffend durch die Rechtsprechung hat. Beruft sich der Betroffene auf die objektiv-rechtliche Dimension des allgemeinen Persönlichkeitsrechts im Zivilrecht, bleibt sein Anspruch gegen des Verpflichteten allein zivilrechtlicher Natur.[1238]

#### *1. Einwilligung*

Eine wirksame und im Zeitpunkt des Eingriffs vorliegende Einwilligung des Betroffenen in die Verletzung eines durch § 823 Abs. 1 BGB geschützten Rechtsguts lässt die Rechtswidrigkeit des Eingriffs entfallen.[1239] Aufgrund des einverständlichen Zugriffs scheiden Ansprüche aufgrund der Verletzung des allgemeinen Persönlichkeitsrechts nach § 823 Abs. 1 BGB sowie nach § 823 Abs. 2 BGB i.V.m. Normen des StGB aus. Die Voraussetzungen einer wirksamen Einwilligung ergeben sich wiederum aus den Vorgaben, die aus dem Schutzbereich des *GVIiS* folgen.

---

[1238] *BVerfGE* 101, 361 (388); *Ladeur*, in: *Götting/Schertz/Seitz* (Hrsg.), Hdb. Persönlichkeitsrecht, § 9 Rn. 19.

[1239] So *BGHZ* 29, 46 (49ff.); 106, 391 (397f.); 166, 336 (339) (zum ärztlichen Heileingriff); Bamberger/Roth/*Spindler*, § 823 Rn. 14; Erman/*Klass*, Anh § 12 Rn. 229 (für das allgemeine Persönlichkeitsrecht); Soergel/*Spickhoff*, § 823 Rn. 119; *Larenz/Canaris*, Schuldrecht BT II/2, § 75 II 2c.

a. Dispositionsbefugnis

Komplexe informationstechnische Systeme können personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten, „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". Der Zugriff auf ein informationstechnisches System ermöglicht aus sich heraus ein vollständiges Persönlichkeitsprofil des Betroffenen, ohne dass einzelne personenbezogene Daten aufwendig miteinander verknüpft oder aus anderen Quellen beschafft werden müssten. Die Beendigung des Zugriffs und die Löschung der bei dem Dritten gespeicherten Daten können eine bereits erfolgte Wahrnehmung der Informationen nicht ungeschehen machen. Aufgrund der insoweit nicht rückgängig zu machenden besonderen Beeinträchtigung des allgemeinen Persönlichkeitsrechts stellt sich die Frage nach der Notwendigkeit einer Abwägung zwischen dem staatlichen Schutz des Persönlichkeitsrechts und der Selbstbestimmung des Grundrechtsträgers.[1240]

Die Einwilligung des Betroffenen in den Zugriff auf das eigengenutzte informationstechnische System setzt daher zunächst die Dispositionsbefugnis des Betroffenen über den Schutz der Vertraulichkeit und Integrität seines informationstechnischen Systems voraus. Insofern wird unter Dispositionsbefugnis die Rechtsmacht verstanden, einem anderen eine Handlung oder Unterlassung zu erlauben, die ohne diese Erlaubnis rechtswidrig wäre.[1241] Die Einwilligung des betroffenen Nutzers müsste demnach überhaupt rechtfertigende Wirkung haben können. Für eine solche Rechtsmacht spricht, dass das *GVIiS* gerade denjenigen Zustand an Vertraulichkeit und Integrität schützt, den der berechtigte Nutzer anhand seiner Kontrolle über den Zugriff auf das System selbstbestimmt schafft. Die selbstbestimmte Verfügung über das eigengenutzte informationstechnische System besteht in der Entscheidungsmacht über den Grad an Vertraulichkeit und Integrität des Systems. Das *GVIiS* ist schon nicht schrankenlos gewährleistet. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein.[1242] Wenn aber staatliche Eingriffe in den Schutzbereich des Grundrechts verfassungsmäßig sein können, muss im Gegenzug auf privatrechtlicher Ebene die Einwilligung des Betroffenen grundsätzlich rechtfertigende Wirkung haben können. Zur persönlichen Freiheit des Einzelnen gehört auch, nach seiner Entscheidung auf die Ausübung grundrechtlicher Befugnisse zu verzichten.[1243] Ihm steht es frei, für die eigene Person Risiken zu übernehmen und Schäden in Kauf zu nehmen.[1244] Denn eine Ausübung grundrechtlicher Freiheit ist

[1240] Hierzu *Ohly*, Einwilligung im Privatrecht, S. 82ff.
[1241] So *Ohly*, Einwilligung im Privatrecht, S. 392.
[1242] *BVerfGE* 120, 274 (315).
[1243] *Lerche*, in: HStR V², § 122 Rn. 45; *Merten*, in: HGR III, § 73 Rn. 27.
[1244] *Isensee*, in: HStR V², § 111 Rn. 113.

auch das selbstgefährdende Verhalten des Einzelnen.[1245] So hat etwa der Staat im Rahmen der Privatautonomie getroffene Regelungen auch dann grundsätzlich zu respektieren, wenn diese mit Einschränkungen grundrechtlicher Freiheiten verbunden sind.[1246]

Das allgemeine Persönlichkeitsrecht schützt die private Sphäre autonomer Lebensgestaltung, in der der Mensch sich selber gehört und seine Individualität unter Ausschluss anderer entwickeln und wahrnehmen kann. Es stellt dem Einzelnen diese Sphäre jedoch zur eigenen Verfügung. Ihm steht es frei, anderen Zugang zu dieser Sphäre zu gewähren. Die selbstbestimmte Verfügung über das eigengenutzte informationstechnische System setzt nach dem hier vertretenen Verständnis voraus, dass der Betroffene selbst über den Grad an Vertraulichkeit und Integrität entscheidet. Er entscheidet grundsätzlich selbst, wie seine ungehinderte Persönlichkeitsentfaltung aussieht. Die dahingehende Selbstbestimmung umfasst auch die Auswahl derjenigen Personen, denen der Betroffene Zugang zu dem von ihm genutzten informationstechnischen System gewährt. Der Einzelne hat seine Kommunikationsbeziehungen grundsätzlich selbst zu gestalten und in diesem Rahmen zu entscheiden, ob er bestimmte Informationen preisgibt oder zurückhält:[1247] Auch die Freiheit, persönliche Informationen zu offenbaren, ist grundrechtlich geschützt.[1248] Der mit der Einwilligung in den Zugriff auf ein informationstechnisches System verbundene Verzicht auf Vertraulichkeit und Integrität ist demnach Ausdruck der selbstbestimmten Verfügung über das System.[1249] Der Betroffene wird gerade dahingehend geschützt, dass er allein über den Zugriff auf das von ihm genutzte informationstechnische System entscheidet.

b. Freiwilligkeit

Es stellt sich daher nicht die Frage, ob der Betroffene überhaupt über sein System verfügen kann, sondern wann eine Einwilligung in den Zugriff eine *selbstbestimmte* Verfügung darstellen kann. Dies setzt voraus, dass der Betroffene die Aufhebung der Vertraulichkeit und Integrität, die mit dem Zugriff des Dritten auf sein System verbunden sind, kennt und auch aus einem laienhaften Verständnis beurteilen kann.

Um zum Zwecke der Persönlichkeitsentfaltung selbstbestimmt an Kommunikationsprozessen teilnehmen zu können, muss dem Einzelnen ein informationeller Selbstschutz auch tatsächlich möglich und zumutbar sein.[1250] Selbstbestim-

[1245] *BVerfG* NJW 1999, 3399 (3401).
[1246] *BVerfGE* 81, 242 (254); 114, 73 (89f.); so ausdrücklich zum *RiS* bei vertraglicher Obliegenheit zur Schweigepflichtentbindung *BVerfG* MMR 2007, 93.
[1247] *BVerfG* MMR 2007, 93.
[1248] *BVerfG* MMR 2007, 93.
[1249] So zum *RiS* ausdrücklich *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 2.
[1250] *BVerfG* MMR 2007, 93.

mung darf nicht in Fremdbestimmung verkehrt werden.[1251] Informationeller Selbstschutz scheidet jedoch von vornherein dort aus, wo der Einzelne den Schutzbedarf gar nicht mehr abschätzen kann oder eine Schutzmöglichkeit gar nicht besteht.[1252] Der Komplexitätsgrad heutiger informationstechnischer Systeme könne zumindest den durchschnittlichen Nutzer in Bezug auf einen wirkungsvollen sozialen oder technischen Selbstschutz überfordern.[1253] Die Selbstbestimmung des Betroffenen setzt daher voraus, dass er weiß, welche personenbezogenen oder gegebenenfalls seine Persönlichkeit betreffenden Daten über die von ihm eingegebenen hinaus bei der Nutzung des informationstechnischen Systems generiert, wo und wie lange sie gespeichert werden und in welchen Zusammenhängen sie durch wen genutzt werden.[1254] Hierbei kann nicht auf besonders gefahrenbewusste und technikerfahrene Personen abgestellt werden.[1255]

So ist etwa die Einwilligung in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gem. § 4a Abs. 1 S. 1 BDSG nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dieser ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen (§ 4a Abs. 1 S. 2 BDSG). Ohne ausreichende Information kann der Betroffene nicht wirksam einwilligen.[1256] Damit setzt eine wirksame Einwilligung jedenfalls die Kenntnis des Betroffenen darüber voraus, welche personenbezogenen Daten von der Einwilligung erfasst sein sollen.[1257] Der Betroffene ist hierüber in einer für ihn verständlichen Weise zu informieren.[1258] Pauschal gehaltene Erklärungen über die Verwendung der Daten genügen nicht.[1259] Die Einwilligung muss vielmehr jedenfalls die gebilligten Verarbeitungsziele und Verarbeitungsphasen enthalten.[1260] Die Einwilligung muss Ausdruck privatautonomer Selbstbestimmung sein und darf gerade nicht mangels Bewusstsein und Verständnis ihrer Reichweite in eine bloße Fiktion von Selbstbestimmung umschlagen.[1261] Entspricht die konkrete Einwilligung gerade nicht der Funktion als Erlaubnistatbestand, greift die staatliche Schutzpflicht, eine selbstbestimmte Entscheidung zu ermöglichen.[1262] Das *BVerfG* sieht die sich aus der zunehmenden Verbreitung komplexer informationstechnischer Systeme

---

1251 So zu den Voraussetzungen der Privatautonomie *BVerfGE* 89, 214 (232); 103, 89 (100f.); 114, 1 (34f.); 114, 73 (90).

1252 *Hoffmann-Riem*, JZ 2008, 1009 (1018).

1253 *BVerfGE* 120, 274 (306).

1254 *Hoffmann-Riem*, JZ 2008, 1009 (1012f.).

1255 *Hoffmann-Riem*, JZ 2008, 1009 (1016).

1256 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 76.

1257 *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 4a BDSG Rn. 76; *Gola/Schomerus*, BDSG, § 4a Rn. 26; *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 72.

1258 *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 4a BDSG Rn. 77; *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 72.

1259 *Gola/Schomerus*, BDSG, § 4a Rn. 26; *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 77; Taeger/Gabel-*Taeger*, § 4a BDSG Rn. 29.

1260 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 80.

1261 Vgl. *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4 Rn. 7; *Buchner*, DuD 2010, 39 (40).

1262 *Bäcker*, Der Staat [2012], 91 (105f.,107) zum *RiS*.

folgenden neuen Persönlichkeitsgefährdungen schon darin, dass diese Systeme „ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind".[1263] Unter Berücksichtigung dieser besonderen Gefährdungslage ergeben sich bei entsprechender Anwendung der Vorgaben zu § 4a Abs. 1 S. 1, 2 BDSG mehrere kumulative Voraussetzungen einer wirksamen Einwilligung in den Zugriff auf ein informationstechnisches System:

*(1)* Es sind die überwachten Funktionen sowie
*(2)* die bei deren Nutzung gewöhnlich anfallenden Daten genau zu benennen; daneben ist
*(3)* ein konkreter Verwendungszweck der zu erhebenden Daten anzugeben.
Die entsprechende Information des Betroffenen darf von diesem
*(4)* keinen besonderen technischen Sachverstand verlangen, sondern muss auch für einen Laien verständlich sein.

Sofern hinsichtlich der Wirksamkeit der Einwilligung allein oder zumindest auch auf die Einsichtsfähigkeit des Betroffenen abgestellt wird,[1264] die Bedeutung und Tragweite des Eingriffs und das Einverständnis hiermit beurteilen zu können, scheitert diese Fähigkeit dann, wenn keine ausreichende Information des Betroffenen im beschriebenen Umfang vorliegt.[1265]

---

[1263] *BVerfGE* 120, 274 (305).

[1264] So MüKoBGB-*Wagner*, § 823 Rn. 731; Palandt/*Sprau*, § 823 Rn. 38; Soergel/*Spickhoff*, § 823 Rn. 123; Erman/*Klass*, Anh § 12 Rn. 238, fordern insoweit zur Wahrung der Selbstbestimmung des Betroffenen ausdrücklich eine dem Medizin- und Datenschutzrecht entsprechende informierte Einwilligung; im Anwendungsbereich des BDSG: *Gola/Schomerus*, BDSG, § 4a Rn. 25; *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 20ff.; *Däubler*/Klebe/Wedde/Weichert, BDSG, § 4a Rn. 5 (insofern für Gleichstellung mit Eingriffen in körperliche Unversehrtheit).

[1265] Der Spielehersteller *Electronic Arts* (EA) ist wegen mangelhafter Aufklärung seiner Kunden über die Reichweite der Funktionen seiner mit dem PC-Spiel „*Battlefield 3*" zwingend zu installierenden Zusatzsoftware „*Origin*" durch die *Verbraucherzentrale Bundesverband* (VZBV) abgemahnt worden (Pressemitteilung des *VZBV* vom 30.11.2011). Die Nutzer würden beim Kauf des Spiels nicht erfahren, was die Software genau auf dem PC mache. Gleichzeitig seien die Allgemeinen Geschäftsbedingungen von *EA* so weit gefasst, dass nach Auffassung des *VZBV* unklar bleibe, welche Daten der Hersteller erfassen, weiterverarbeiten und anderweitig nutzen dürfe. So behalte sich *EA* das Recht vor, anhand der erfassten Daten Nutzerprofile zu erstellen und diese ohne gesonderte Einwilligung der Kunden für Werbezwecke zu verwenden. Welche Daten dies genau sind, lasse der Hersteller offen. Den aufgetauchten Vorwurf, *Origin* sei Spyware, konnte das *Magazin für Computertechnik* (c't), Ausgabe 25/11, S. 42 nicht bestätigen. Die Protokollierung des Zugriffsverhaltens der Software habe kein außergewöhnliches Verhalten ergeben.

### *2. Allgemeine Geschäftsbedingungen, §§ 305ff. BGB*

#### a. Anwendbarkeit der §§ 305ff. BGB

Sofern eine solche Einwilligung in Allgemeinen Geschäftsbedingungen enthalten ist, ist eine entsprechende Klausel an den §§ 305ff. BGB zu messen.[1266] Formularvertragliche Einwilligungen in Beeinträchtigungen des allgemeinen Persönlichkeitsrechts fallen in den Anwendungsbereich der §§ 305ff. BGB.[1267] Auf die Rechtsnatur der Einwilligung und ihre Qualifikation als Vertragsbedingung kommt es insofern nicht an. Entscheidend ist allein, dass der Verwender bei der von dem Vertragspartner abzugebenden Erklärung die rechtsgeschäftliche Gestaltungsfreiheit für sich ebenso in Anspruch nimmt wie bei der Vorformulierung eines Vertragstextes und der Kunde nur darauf, ob er die Erklärung abgeben will, nicht aber auf ihren Inhalt Einfluss hat.[1268]

#### b. Überraschende Klauseln, § 305c Abs. 1 BGB

Die formularvertragliche Einwilligung in den Zugriff auf das informationstechnische System des Vertragspartners könnte zunächst eine überraschende Klausel i.S.d. § 305c Abs. 1 BGB darstellen. Danach werden Bestimmungen in Allgemeinen Geschäftsbedingungen nicht Vertragsbestandteil, die nach den Umständen, insbesondere nach dem äußeren Erscheinungsbild des Vertrags, so ungewöhnlich sind, dass der Vertragspartner des Verwenders mit ihnen nicht zu rechnen braucht. Die hierfür zunächst notwendige objektive Ungewöhnlichkeit einer Klausel kann sich auch aus ihrer Unvereinbarkeit mit dem Leitbild des Vertrages ergeben.[1269] Der Zugriff auf das informationstechnische System müsste daher überhaupt in Zusammenhang mit dem Vertragszweck stehen. Eine Klausel müsste daneben auch einen Überrumpelungs- oder Übertölpelungseffekt auf den Vertragspartner haben.[1270] Der Zugriff auf ein informationstechnisches System ist hingegen regelmäßig mit technischen Maßnahmen verbunden, die eine Mitwirkung des Betroffenen voraussetzen. Eine dahingehende Mitteilung dürfte, sofern nicht schon eine Individualabrede nach § 305b BGB vorliegt, einem Überrumpelungs- oder Übertölpelungseffekt entgegenstehen. Denn ein solcher Effekt scheidet bei einem ausdrücklichen Hinweis auf die jeweilige Klausel aus.[1271]

---

1266 Vgl. *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 4a Rn. 26ff.; *Gola/Schomerus*, BDSG, § 4a Rn. 23; *Däubler*/Klebe/Wedde/Weichert, BDSG, § 4a Rn. 31ff.

1267 *BGH* NJW 1999, 1864; NJW 1990, 2313 (2314); NJW 1999, 2279 (2282); NJW 2000, 2677; NJW 2010, 864 (865).

1268 *BGH* NJW 1999, 1864; NJW 2000, 2677; *Ulmer/Habersack*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 305 Rn. 16.

1269 Vgl. *BGHZ* 121, 107 (113).

1270 *BGHZ* 100, 83 (85); *BGH* NJW 90, 576 (577); NJW-RR 2004, 780 (781).

1271 *BGHZ* 109, 197 (203); 131, 55 (59); *BGH* NJW 1992, 1822 (1823); NJW 1997, 2677.

c. Inhaltskontrolle, § 307 Abs. 1, 2 Nr. 1 BGB

Die Gestattung des Zugriffs auf ein informationstechnisches System muss dann der Inhaltskontrolle des § 307 Abs. 1, 2 BGB standhalten. Eine entsprechende Klausel darf den Betroffenen nicht entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine solche Benachteiligung ist im Zweifel anzunehmen, wenn eine Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist (§ 307 Abs. 2 Nr. 1 BGB). Während § 307 Abs. 1 BGB den Grundtatbestand der Inhaltskontrolle enthält,[1272] konkretisiert § 307 Abs. 2 BGB den unbestimmten Rechtsbegriff der „unangemessenen Benachteiligung" durch zwei Regelbeispiele.[1273] Es soll damit die Inhaltskontrolle durch die Angabe typischer rechtlicher Kriterien des Hinweises auf einen fehlenden angemessenen Interessenausgleich erleichtert werden.[1274] Anhand dieser Vorgaben soll die folgende Darstellung allgemeingültige Maßstäbe hinsichtlich der Zulässigkeit eines formularvertraglichen Einverständnisses mit der Aufhebung der Vertraulichkeit und Integrität informationstechnischer Systeme aufstellen.

i. Wesentliche Grundgedanken, § 307 Abs. 2 Nr. 1 BGB

Das BDSG findet keine Anwendung auf den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme. Die ausdrückliche Regelung der Einwilligungserfordernisse des § 4a BDSG in Bezug auf die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten kann daher nicht unmittelbar herangezogen werden. Über § 307 Abs. 2 Nr. 2 BGB können aber auch die in zwingenden Normen zum Ausdruck kommenden gesetzlichen Wertungen als Leitbild der Interessenabwägung berücksichtigt werden.[1275] So ist der wesentliche Grundgedanke des BDSG die grundsätzliche Entscheidung für den Schutz personenbezogener Daten.[1276] Zwar sieht auch das BDSG in § 4 Abs. 1 Alt. 1 BDSG die Möglichkeit der Einwilligung in die Verarbeitung personenbezogener Daten vor. Diese Einwilligung muss jedoch den besonderen Voraussetzungen des § 4a Abs. 1 BDSG genügen.[1277] Die so zum Ausdruck kommende gesetzgeberische Wertung ist auch hinsichtlich der Einwilligung in die Aufhebung der Vertraulichkeit und Integrität informationstechnischer Systeme zu berücksichtigen. Denn mit der Einwilligung in den Zugriff auf das System hat der Verwender Zugang zu sämtlichen auf dem System enthaltenen Informationen. Wenn demnach die Voraussetzungen des § 4a Abs. 1 BDSG unabhängig vom Umfang der betroffenen perso-

[1272] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 93; *Wolf*, in: *Ders./Lindacher/Pfeiffer*, AGB-Recht, § 307 Rn. 74.
[1273] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 193; Palandt/*Grüneberg*, § 307 Rn. 28.
[1274] *Stoffels*, AGB-Recht, Rn. 496.
[1275] *BGH* NJW 2010, 2272 (2273); *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 209; Staudinger/*Coester* (2006), § 307 Rn. 232 a.E.
[1276] *BGH* NJW 1981, 1738 (1739); NJW 1986, 46 (47).
[1277] Siehe hierzu z.B. *OLG Schleswig* NJW-RR 1998, 54 (56).

nenbezogenen Daten vorliegen müssen, so ist den Voraussetzungen erst recht zu genügen, wenn der Zugriff auf eine derart umfangreiche und vielfältige Informationsquelle wie ein komplexes informationstechnisches System gestattet werden soll. Über § 307 Abs. 2 Nr. 1 BGB sind damit die sich aus § 4a Abs. 1 BDSG ergebenden Anforderungen an eine wirksame Einwilligung entsprechend zu berücksichtigen. Diese Anforderungen werden wiederum erfüllt, sofern eine Einwilligung die oben dargestellten Voraussetzungen an eine freiwillige Entscheidung erfüllt. Eine Missachtung dieser Anforderungen kann somit nach § 307 Abs. 2 Nr. 1 BGB zur Unwirksamkeit einer vorformulierten und allgemein gehaltenen Einwilligungserklärung führen.[1278] Unangemessen dürfte ferner eine Regelung sein, in der sich der Betroffene für den Erhalt der vertraglich geschuldeten Leistung verpflichtet, den Zugriff des Vertragsgegners auf das informationstechnische System zu erlauben. Insoweit liegt der Rückgriff auf die gesetzgeberische Wertung des in § 28 Abs. 3b BDSG enthaltenen Koppelungsverbots nahe.

ii. Generalklausel, § 307 Abs. 1 S. 1 BGB

Sofern sich die Unwirksamkeit der Klausel nicht bereits aus § 307 Abs. 2 Nr. 1 BGB ergibt, ist dennoch nicht von vornherein auch eine unangemessene Benachteiligung nach § 307 Abs. 1 S. 1 BGB ausgeschlossen.

(1) Benachteiligung

Eine solche Benachteiligung setzt zunächst voraus, dass der Adressat der Klausel im Vergleich zur Rechtslage ohne diese Klausel schlechter gestellt wird.[1279] Eine solche Schlechterstellung liegt hier vor. Die Infiltration des informationstechnischen Systems eines berechtigten Nutzers stellt eine rechtfertigungsbedürftige Verletzung des allgemeinen Persönlichkeitsrechts aus § 823 Abs. 1 BGB dar. Mit der formularvertraglichen Einwilligung verzichtet der Betroffene entgegen der grundsätzlichen Rechtslage auf den Schutz seines allgemeinen Persönlichkeitsrechts.

(2) Interessenabwägung

Die vorzunehmende Interessenabwägung setzt zunächst die Ermittlung der zu berücksichtigenden Interessen des Verwenders und des Vertragsgegners voraus. Zu berücksichtigen sind dann alle rechtlich anerkannten Interessen.[1280]

---

[1278] *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 84 zu den Anforderungen des § 4a Abs. 1 BDSG.

[1279] Staudinger/*Coester* (2006), § 307 Rn. 90; Bamberger/Roth/*Schmidt*, § 307 Rn. 24; *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 100; *Stoffels*, AGB-Recht, Rn. 467.

[1280] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 120; *Wolf*, in: *Ders./Lindacher/Pfeiffer*, AGB-Recht, § 307 Rn. 174.

(a) Interessen des Verwenders

Typisches Interesse des Verwenders ist zunächst die Rationalisierung der Geschäftsabwicklung.[1281] Einheitliche Regelungen gegenüber allen Kunden tragen zur Standardisierung der Vertragsanbahnung und dessen Durchführung bei.[1282] Ein solches Interesse dürfte hier von vornherein keine Berücksichtigung finden. Die Einwilligung in die Infiltration des informationstechnischen Systems führt zu keinerlei Vereinfachung oder Vereinheitlichung i.d.S. Denn es geht um die Einräumung zusätzlicher Rechte an den Verwender, nicht hingegen um die Vereinheitlichung vom Verwender typischerweise erbrachter Leistungen. Die sich aus der Infiltration ergebenden Vorteile kommen allein dem Verwender zugute. Auch ist eine mögliche Lückenfüllungs- oder Typisierungsfunktion[1283] einer solchen Klausel nicht zu berücksichtigen. Soweit auf den konkreten Vertragszweck passendes dispositives Gesetzesrecht fehlt oder nicht vorhanden ist, kommt Allgemeinen Geschäftsbedingungen auch die Funktion zu, entsprechende Regelungen zu schaffen.[1284] Eine solche Funktion hat die gegenständliche Klausel nicht. Ihr Gegenstand ist nicht die Entwicklung von im geschriebenen Recht nicht enthaltenen Regelungen, sondern allein die Einräumung zusätzlicher Befugnisse an den Verwender. Es kommen daneben noch sonstige wirtschaftliche Interessen in Betracht. Dies ist zum einen das Interesse des Verwenders an den auf einem informationstechnischen System enthaltenen oder durch dessen Nutzung erzeugten Informationen. Dem Einzelnen steht es grundsätzlich frei, persönliche Informationen anderen gegenüber zu offenbaren, indem er die vertragliche Verpflichtung oder Obliegenheit zur Mitteilung solcher Informationen an den Vertragspartner eingeht.[1285] Daneben kann der Anbieter von Software ein Interesse daran haben, das Nutzungsverhalten des Betroffenen zu protokollieren,[1286] um die so erlangten Informationen entweder zur Fehlerbehebung oder zur am Nutzungsverhalten orientierten Funktionsoptimierung zu nutzen. Schützenswertes Interesse ist auch dasjenige des Inhabers von Rechten des geistigen Eigentums, an jeder wirtschaftlichen Nutzung seiner Werke angemessen beteiligt zu werden.[1287] Insofern kommt die Einwilligung des Adressaten in die Installation von Kopierschutzsoftware auf seinem informationstechnischen System in Betracht. Jedenfalls berücksichtigungsfähig muss das Interesse des Verwenders sein, sich diejenigen Rechte einräumen zu lassen, um eine vertraglich geschuldete Leistung überhaupt erst erbringen zu

[1281] *BGH* NJW 1981, 117 (118); NJW 1996, 988 (989); NJW 2010, 2719 (2020f.); *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 121. Bamberger/Roth/*Schmidt*, § 307 Rn. 31.
[1282] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 121.
[1283] MüKoBGB-*Basedow*, Vor § 305 Rn. 3; *Stoffels*, AGB-Recht, Rn. 71.
[1284] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 124.
[1285] *BVerfG* MMR 2007, 93.
[1286] *Roßnagel/Schnabel*, NJW 2008, 3534 (3537); *Herrmann*, IT-Grundrecht, S. 187.
[1287] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 125.

können. Insofern besteht dieses Interesse parallel zu dem Leistungsinteresse des Vertragspartners. Jener möchte insbesondere die nach dem Vertragsinhalt berechtigterweise zu erwartende Leistung ungeschmälert erhalten.[1288]

(b) Interessen des Vertragspartners

Dieses Interesse ist damit zunächst auf Seiten des Vertragspartners zu berücksichtigen. Es beinhaltet die Ermöglichung der Verwirklichung des Vertragszwecks und insbesondere der Durchsetzung des geplanten Leistungsaustausches.[1289] Die Berücksichtigung eines solchen Leistungsinteresses setzt demnach voraus, dass zur Erreichung des Vertragszwecks der Zugriff auf das informationstechnische System des Vertragspartners notwendig ist. Eine solche Notwendigkeit wird vor allem im Rahmen von Softwarepflegeverträgen[1290] vorliegen, sofern die Arbeiten mittels einer Fernwartung ausgeführt werden sollen. Die Möglichkeit einer Fernwartung setzt notwendigerweise den Fernzugriff auf das zu pflegende informationstechnische System voraus. Das Leistungsinteresse des Vertragspartners dürfte ferner im Rahmen des *Application Service Providing* (ASP)[1291] und *Software as a Service* (SaaS)[1292] zu berücksichtigen sein. Mit dem vertragsgemäßen Zugriff des Nutzers auf die ihm zur Verfügung gestellten Softwarekomponenten und den zugehörigen Speicherkapazitäten werden diese durch die telekommunikative Verbindung mit dem zugreifenden System wiederum Teil eines weiteren informationstechnischen Systems. Dabei stellt die vertragliche Vereinbarung solche Umstände dar, aufgrund derer der Vertragspartner davon ausgehen kann, über dieses System selbstbestimmt zu verfügen. Eine Eigennutzung wäre damit gegeben. Die Spezialität des Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG) gegenüber dem allgemeinen Persönlichkeitsrecht ist dabei nicht zu berücksichtigen. Der Schutzbereich des Art. 10 Abs. 1 GG ist mangels Übermittlung von Informationen an einen oder mehrere individuelle Empfänger nicht eröffnet.[1293]

Zu berücksichtigen ist weiter das auf den Erhalt des vorhandenen eigenen Vermögens und sonstiger Rechtsgüter gerichtete sog. Integritätsinteresse des Vertragspartners.[1294] Es sind danach auch bloß immaterielle Interessen zu berücksichtigen.[1295] Insofern ist auch das Interesse des Vertragspartners am größtmöglichen

---

[1288] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 127.

[1289] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 127.

[1290] Hierzu etwa *Marly*, Praxishandbuch Softwarerecht, Rn. 1020ff.

[1291] Grundlage des ASP ist die Idee, Computersoftware nicht auf jedem einzelnen Arbeitsplatzrechner zu installieren, sondern für den Anwender auf einem Internetserver zum Abruf mittels Telekommunikationsverbindungen bereitzuhalten (*Marly*, Praxishandbuch Softwarerecht, Rn. 1071).

[1292] SaaS basiert wie ASP auf dem Geschäftsmodell einer zeitlich befristeten Softwareüberlassung, weist gegenüber ASP aber eine deutlich höhere Anpassung der Softwarelösungen an die konkreten Kundenbedürfnisse auf (*Marly*, Praxishandbuch Softwarerecht, Rn. 1078).

[1293] Hierzu *BVerfGE* 115, 166 (182) m.w.N.

[1294] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 127.

[1295] Bamberger/Roth/*Schmidt*, § 307 Rn. 38; Staudinger/*Coester* (2006), § 307 Rn. 161.

Erhalt der Vertraulichkeit und Integrität seines informationstechnischen Systems und damit der selbstbestimmten Verfügung über das System in die Abwägung einzustellen. Bei der Abwägung sind auch mögliche Nebenwirkungen des Zugriffs zu berücksichtigen.

(c) Abwägung

Mit dem Zugriff auf ein komplexes informationstechnisches System ist die Möglichkeit verbunden, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Insofern ist auch bei der Abwägung nach § 307 Abs. 1 S. 1 BGB nicht auf den tatsächlichen Bestand an personenbezogenen Daten abzustellen. Denn zu berücksichtigen sind die generell möglichen Wirkungen einer Klausel, nicht die tatsächlich eingetretenen Nachteile.[1296] Allgemein gilt für die Gewichtung und Abwägung der betroffenen Interessen, dass die Rechtfertigungsanforderungen umso höher liegen, je intensiver der Verwender in die geschützte Interessensphäre des Vertragspartners eingreift.[1297] Die vorzunehmende Gewichtung hat auch zu berücksichtigen, ob ein verfassungsrechtlich besonders geschütztes oder lediglich allgemein von der Rechtsordnung anerkanntes Interesse betroffen ist.[1298] Der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme ist daher auf Seiten des Betroffenen nicht lediglich als Ausprägung des allgemeinen Persönlichkeitsrechts des § 823 Abs. 1 BGB, sondern auch als sich aus dem Grundgesetz ergebendes Interesse zu berücksichtigen. Angesichts der hohen Persönlichkeitsrelevanz der Vertraulichkeit und Integrität informationstechnischer Systeme und des dem Grundgesetz zu entnehmenden Schutzbereichs muss eine auf die Einwilligung in den Zugriff gerichtete Klausel ebenso hohen Anforderungen auf Seiten des Verwenders genügen. Eine unangemessene Benachteiligung liegt dann vor, wenn der Verwender missbräuchlich eigene Interessen auf Kosten des Vertragspartners durchzusetzen versucht, ohne von vornherein auch dessen Belange hinreichend zu berücksichtigen und ihm einen angemessenen Ausgleich zuzugestehen.[1299]

(i) Parallele zur Telefonwerbung

So ist nach Entscheidungen des IV. und des XI. Senats des *BGH* im Rahmen der formularvertraglichen Einwilligung in Telefonwerbung im privaten Bereich der Schutz der Individualsphäre stets vorrangig gegenüber wirtschaftlichen Interessen.[1300] Angesichts vielfältiger Werbemethoden sei ein Eindringen auch in den

[1296] MüKoBGB-*Kieninger*, § 307 Rn. 37; Staudinger/*Coester* (2006), § 307 Rn. 110.
[1297] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 104; *Stoffels*, AGB-Recht, Rn. 470.
[1298] *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 104.
[1299] *BGH* NJW 1984, 1182; NJW 1985, 53 (55); NJW 2005, 1774 (1775); NJW 2008, 1064 (1065).
[1300] *BGH* NJW 1999, 1864 (1865); NJW 1999, 2279 (2282); kritisch *Jankowski*, GRUR 2010, 495 (498).

privaten Bereich des Verbrauchers nicht erforderlich. Telefonwerbung stelle eine besonders schwerwiegende Beeinträchtigung der verfassungsrechtlich geschützten Privatsphäre des Angerufenen dar, da sie u.a. ein praktisch unkontrollierbares Eindringen in die Lebensgewohnheiten der Zielperson bedeute.[1301] Die Initiative zur Wiederherstellung der ungestörten Privatsphäre werde auf den Betroffenen verlagert.[1302] Hingegen ging der I. Senat des *BGH* von der grundsätzlichen Zulässigkeit einer formularvertraglichen Einwilligung aus und kam erst im Wege einer Einzelfallprüfung zur Unzulässigkeit der konkreten Klausel.[1303] Selbst wenn man in der *Payback*-Entscheidung des *BGH*[1304] eine Tendenz zu einer weniger restriktiven Rechtsprechung sieht,[1305] lässt sich eine etwaige Lockerung nicht auch auf die formularvertragliche Einwilligung in den Zugriff auf ein informationstechnisches System übertragen. Die dortige formularmäßige Einwilligung in die SMS- bzw. E-Mail-Werbung sah vor, dass der Vertragsgegner aktiv ein Kästchen ankreuzen musste, wenn er seine Einwilligung nicht erteilen wollte („Opt-out"). Der *BGH* entschied, dass eine solche Gestaltung gegen § 7 Abs. 2 Nr. 3 UWG verstoße.[1306] Die Norm verlange vielmehr die Erteilung der Einwilligung mittels einer gesonderten Erklärung („Opt-in"). Hierin wurde teilweise zugleich eine Entscheidung für die grundsätzliche Zulässigkeit der formularvertraglichen Einwilligung in die Telefonwerbung gesehen.[1307]

Die Qualität der Beeinträchtigung der privaten Sphäre des Einwilligenden geht aber über den der schlichten Telefonwerbung weit hinaus. Diese stellt nur einen vor allem technisch bedingt bloß punktuellen Eingriff dar. Telefonwerbung hat nicht das Potential einer nahezu umfassenden Erfassung der Persönlichkeitsentfaltung. Soweit der Zugriff auf das informationstechnische System reicht, wird dem Verwender der unbegrenzte und praktisch nicht zu kontrollierende Zugriff auf einen Teilbereich der Privatsphäre des Vertragspartners erlaubt. Die „entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems"[1308] wäre überwunden. Die Persönlichkeitsrelevanz der Telefonwerbung ist auf die fernmündliche Anpreisung von Waren beschränkt. Der Zugriff auf das informationstechnische System des Betroffenen hingegen verschafft dem

1301 *BGH* NJW 1999, 2279 (2282).
1302 *BGH* NJW 1999, 1864 (1865).
1303 *BGH* NJW 2000, 2677f.; dem folgend *OLG Hamburg* GRUR-RR 2009, 351 (352); MMR 2009, 557; offen: *OLG Köln* MMR 2009, 470; GRUR-RR 2008, 316 (317); *OLG Hamm* MMR 2007, 54 (55).
1304 *BGHZ* 177, 253.
1305 So *Jankowski*, GRUR 2010, 495 (497f.); *Bernreuther*, WRP 2009, 390 (400).
1306 *BGHZ* 177, 253 (263 Rn. 27).
1307 So *Jankowski*, GRUR 2010, 495 (497); *Bernreuther*, WRP 2009, 390 (400).
1308 *BVerfGE* 120, 274 (314).

Dritten eine umfassende und dauerhafte Informationsquelle, deren Inanspruchnahme der Betroffene kaum verlässlich überblicken kann. Die Beeinträchtigung seines Persönlichkeitsrechts geht daher über diejenige der Telefonwerbung weit hinaus.

(ii) Wirtschaftliche Interessen

Sofern der Verwender allein wirtschaftliche Interessen i.S.e. werbemäßigen Verwertung der erlangten Informationen geltend machen kann, dürfte die formularvertragliche Einwilligung des Zugriffs auf das informationstechnische System des Vertragspartners nur im Einzelfall keine unangemessene Benachteiligung darstellen. Ausgangspunkt müssen der Umfang und die Dauer des Zugriffs und damit die erlangbaren persönlichen Informationen sein. Stellt der Verwender dem Betroffenen etwa eine Software unentgeltlich zur Verfügung[1309] und lässt sich hierfür im Gegenzug Zugriffsrechte auf das informationstechnische System des Betroffenen einräumen, so ist die Bedeutung dieses Vorteils derjenigen des Nachteils der Persönlichkeitsgefährdung gegenüberzustellen. Diese Problematik dürfte sich vor allem im Bereich der kostenlosen Bereitstellung von Applikationen für Smartphones stellen, in deren Gegenzug umfangreichen Datenzugriffen zugestimmt wird.[1310] Je nach Reichweite des Zugriffs wird dem Verwender eine umfangreiche Profilbildung des Betroffenen ermöglicht. Der Verwender einer solchen Klausel wird auf genau diese Möglichkeiten abzielen. Der Betroffene hingegen ist an den fortdauernden Erlösen aus der Verwertung seiner personenbezogenen Daten nicht unmittelbar beteiligt. Sein Vorteil erschöpft sich in einer einmaligen Leistung des Verwenders. Jedenfalls bei einem vollständigen Zugriff auf das informationstechnische System des Betroffenen wird dessen Interesse an einem größtmöglichen Erhalt der Vertraulichkeit und Integrität des Systems und damit an der selbstbestimmten Verfügung über seine persönlichen Lebenssachverhalte von dem Verwender nicht ausreichend berücksichtigt. Einen angemessenen Ausgleich für die besondere Persönlichkeitsgefährdung erhält er nicht.

Die Einwilligung in die Protokollierung lediglich des Nutzungsverhaltens einer auf dem informationstechnischen System des Vertragspartners installierten Software des Verwenders dürfte demnach jedenfalls nicht von vornherein ausgeschlossen sein. Die Protokollierung stellt eine Überwachung des Systems dar, von der der Betroffene nur dann profitiert, wenn die Protokollierung allein der Fehlerbehebung der Software dient und er in der Folge von dieser fehlerbereinigten und optimierten Version Gebrauch machen kann. Dieser Gebrauch muss zusätzlich

[1309] Einzelne Beispiele u.a. bei *Buchner*, DuD 2010, 39.

[1310] Siehe hierzu etwa die Pressemitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LDI) Rheinland-Pfalz vom 30.7.2012 (abrufbar unter: http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2012073001) sowie das Forderungspapier der VZBV vom 8.8.2011 - „Smartphones und Verbraucherschutz“ (abrufbar unter: http://www.surfer-haben-rechte.de/cps/rde/xbcr/digitalrechte/Forderungspapier_Smartphones.pdf).

aber in einem hinreichend konkreten Zusammenhang mit der Protokollierung auf dem System des Vertragspartners stehen. Das einzelfallbezogene Einverständnis in die Übersendung eines Fehlerberichts anstelle der automatischen Übersendung würde dabei dem Interesse des Vertragspartners am Erhalt der Vertraulichkeit seines informationstechnischen Systems entgegenkommen.

Ebenfalls lässt sich keine abschließende Abwägung mit dem Interesse des Verwenders am Schutz von Rechten des geistigen Eigentums vornehmen. So sieht § 95a Abs. 1 Urheberrechtsgesetz (UrhG) ausdrücklich vor, unerlaubte Nutzungshandlungen durch technische Maßnahmen zu verhindern oder einzuschränken. Solche Maßnahmen sind nach § 95a Abs. 2 S. 1 UrhG Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, geschützte Werke oder andere nach dem UrhG geschützte Schutzgegenstände betreffende Handlungen, die vom Rechtsinhaber nicht genehmigt sind, zu verhindern oder einzuschränken. Damit die von dem Verwender eingesetzten Maßnahmen dieser Definition unterfallen, müsste ihr Zweck allein darin liegen, unerlaubte Nutzungshandlungen zu verhindern oder einzuschränken. Für darüberhinausgehende Funktionen lässt sich die gesetzliche Wertung hinter § 95a UrhG nicht heranziehen. Eine Kopierschutzmaßnahme wie das „Sony-BMG-Rootkit" dürfte hingegen schon allein wegen der mit der Maßnahme verbundenen Nebenwirkungen für die Integrität des informationstechnischen Systems unzulässig sein.[1311]

(iii) Vertragszweck

Keine unangemessene Benachteiligung ist dann anzunehmen, wenn die Einwilligung in den Zugriff auf das informationstechnische System gerade eine zwingende Voraussetzung für die Vertragserfüllung darstellt. Dies gilt für eine Fernwartung des Systems im Rahmen eines Softwarepflegevertrags. Das Erbringen der von dem Vertragspartner begehrten Leistung setzt zwingend seine Einwilligung in den Zugriff voraus. Mit der Wahl eines solchen Leistungsprogramms hat der Vertragspartner bereits vor Abschluss des Vertrages sein Selbstbestimmungsrecht dahin ausgeübt, dass er einer bestimmten Art der Vertragserfüllung den Vorrang vor dem Erhalt der Vertraulichkeit und Integrität seines informationstechnischen Systems einräumt.

iii. Insbesondere Arbeitsverträge

Die vorgenannte Abwägung ist auch bei der formularvertraglichen Einwilligung in die Überwachung informationstechnischer Systeme durch den Arbeitgeber vorzunehmen (vgl. § 310 Abs. 4 S. 2 Hs. 1). In diesem Zusammenhang wird insbesondere die Zulässigkeit der Überwachung des E-Mail-Verkehrs und der Internetnutzung problematisiert.[1312] Entscheidend ist hierbei jedoch die Art der Kontrolle:

[1311] Hierzu *Hansen*, DuD 2006, 95.

[1312] Siehe hierzu etwa *Mengel*, BB 2004, 2014; *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 135; *Wolf/Mulert*, BB 2008, 442; zusammenfassend *Wybitul*, ZD 2011, 69ff.

Anforderungen durch den Schutzbereich des *GVIiS* kommen von vornherein nur dort in Betracht, wo die Überwachung mittels des technischen Zugriffs auf das informationstechnische Systems erfolgt. Eine Informationsgewinnung durch den unmittelbaren räumlichen Zugang zu dem System ohne eine technische Manipulation fällt demgegenüber nicht in den Schutzbereich des *GVIiS*. Sie ist am *RiS* und gegebenenfalls an Art. 13 Abs. 1 GG zu messen.

Als abwägungsfähige Interessen des Arbeitgebers kommen u.a. die Kontrolle anfallender Kosten, die Leistungskontrolle des Arbeitnehmers und der Schutz von Geschäftsgeheimnissen[1313] sowie der Schutz vor Viren und Trojanern[1314] in Betracht.[1315] Persönlichkeitsrechte des Arbeitnehmers (Art. 10 Abs. 1 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und das Eigentumsrecht des Arbeitgebers (Art. 14 Abs. 1 S. 1 GG) sind in Einklang zu bringen.[1316] Anforderungen durch das *GVIiS* können sich hierbei nur dann ergeben, sofern nicht das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts vorrangig zu berücksichtigen ist.[1317] Diese Spezialität erfasst nur den Zugriff auf eine laufende Kommunikation. Die Überwachung des E-Mail-Verkehrs unterfällt damit nur dann dem Schutzbereich des *GVIiS*, sofern nicht erst mit dem Absenden der E-Mail die Überwachungsmaßnahme greift, sondern bereits das Schreiben selbst überwacht wird. Der Schutzbereich des Art. 10 Abs. 1 GG erfasst damit nicht die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation. Die Durchsicht der auf dem informationstechnischen System des Arbeitnehmers gespeicherten E-Mails wäre demnach ebenfalls am Schutzbereich des *GVIiS* zu messen. Bei der Überwachung der Internetnutzung kommt eine Spezialität des Telekommunikationsgeheimnisses etwa dann in Betracht, wenn über das informationstechnische System stattfindende Internettelefonie überwacht wird. Die Überwachung durch den Arbeitgeber ist jedoch nur dann allein an den Vorgaben des Telekommunikationsgeheimnisses zu messen, soweit der bloß punktuelle Zugriff entsprechend den Vorgaben zur Quellen-TKÜ[1318] durch technische Vorkehrungen und vertragliche Verpflichtungen abgesichert wird.

---

1313 *Mengel*, BB 2004, 2014 (2016).

1314 Ein Trojanisches Pferd ist ein Anwendungsprogramm, das neben seiner eigentlichen Aufgabe ‚unbemerkt' einen Virus oder andere Malware transportiert und einschleust (*Fischer/Hofer*, Lexikon Informatik, Stichwort „Trojanisches Pferd").

1315 *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 135 (136).

1316 *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 135; *Mengel*, BB 2004, 2014 (2014f.).

1317 Diese Subsidiarität übersieht *Herrmann*, IT-Grundrecht, S. 202ff.; *Wedde*, AuR 2009, 373, bleibt insoweit unklar, als für den Schutzbereich des *GVIiS* allgemein Daten über das Kommunikationsverhalten aus VoIP-Telefonanlagen angeführt werden.

1318 *BVerfGE* 120, 274 (309).

(1) Erlaubnisnorm der Überwachung

Im Anwendungsbereich des *GVIiS* bedarf es dabei keiner Differenzierung, ob dem Arbeitnehmer eine private Nutzung der Betriebsmittel erlaubt ist oder nicht. Diese Unterscheidung dient zunächst vorrangig der Feststellung der einschlägigen Regelung, nämlich, ob die Überwachungsmaßnahme den Anforderungen des BDSG oder denen des TKG unterliegt.[1319] Der Schutzbereich des *GVIiS* und mit ihm die daraus abzuleitenden Anforderungen in objektiv-rechtlicher Hinsicht kommen hingegen ohnehin nur in Betracht, soweit nicht der Schutzbereich des Art. 10 Abs. 1 GG spezieller ist. Das BDSG ist ebenso wenig einschlägig. Neben der allgemeinen Norm des § 28 Abs. 1 BDSG ist auch die speziell für den Beschäftigtendatenschutz geltende Norm des § 32 Abs. 1 BDSG nicht auf den technischen Zugriff auf informationstechnische Systeme anwendbar. Es gelten hier dieselben Argumente wie zu § 28 Abs. 1 BDSG. Weder dem Wortlaut der Norm noch der Gesetzesbegründung zu § 32 BDSG[1320] lässt sich die Anwendbarkeit entnehmen. Ersterer benennt nur die personenbezogenen Daten des Beschäftigten als Regelungsgegenstand, ohne die spezifische Erhebungssituation bei dem Zugriff auf ein informationstechnisches System zu berücksichtigen. Die Gesetzesbegründung verweist ausdrücklich nur auf die „von der Rechtsprechung aus dem verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrecht […] abgeleiteten allgemeinen Grundsätzen zum Datenschutz im Beschäftigungsverhältnis".[1321] Auch dem Entwurf der Bundesregierung eines Gesetzes zur Regelung des Beschäftigtendatenschutzes[1322] lässt sich eine Erlaubnisnorm nicht entnehmen. Der Anwendungsbereich des § 32 BDSG wird insbesondere auch durch die §§ 32c, 32e Abs. 2 und 32i Abs. 4 BDSG-E nicht erweitert. Dem steht wiederum zunächst der Wortlaut der Normen entgegen. § 32c Abs. 1 BDSG-E stellt allein auf Beschäftigtendaten als personenbezogene Daten von Beschäftigten (vgl. § 3 Abs. 12 BDSG-E) ab, benennt hingegen nicht auch das informationstechnische System als Zugriffsobjekt. Gleiches gilt für § 32e Abs. 2 BDSG-E. Zudem untersagt § 32e Abs. 4 Nr. 3 BDSG-E die heimliche Erhebung von Beschäftigtendaten mittels besonderer technischer Mittel, die für Beobachtungszwecke bestimmt sind. Auch der Wortlaut des § 32i Abs. 4 BDSG-E gibt eine Anwendbarkeit auf den technischen Zugriff auf ein informationstechnisches System nicht her. Sein Anwendungsbereich ist ebenfalls auf Telekommunikationsdaten (i.S.v. Verkehrsdaten gem. § 3 Nr. 30 TKG[1323]) sowie -inhalte als Zugriffsobjekte begrenzt. Zugleich lässt die Norm mit der Differenzierung zwischen beruflichen/dienstlichen und privaten Daten und Inhalten die oben beschriebene Gleichsetzung der privaten

[1319] Vgl. *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 135 (136); *Mengel*, BB 2004, 2014 (2015f.); *Wolf/Mulert*, BB 2008, 442 (445f); *Wybitul*, ZD 2011, 69 (71f.).

[1320] BT-Drucks. 16/13657, S. 20ff.

[1321] BT-Drucks. 16/13657, S. 21.

[1322] BT-Drucks. 17/4230.

[1323] BT-Drucks. 17/4230, S. 20.

und geschäftlichen Nutzung von informationstechnischen Systemen erkennbar außer Acht.[1324] Die Gesetzesbegründung erwähnt die Vorgaben des *GVIiS* nicht. Mithin ergibt sich auch für das Arbeitsverhältnis keine Spezialität des BDSG gegenüber § 823 Abs. 1 BGB. Maßgeblich für die Zulässigkeit eines technischen Zugriffs auf informationstechnische Systeme ist mithin das allgemeine Persönlichkeitsrecht.

(2) Private und geschäftliche Nutzung

Der Differenzierung zwischen privater und ausschließlich geschäftlicher Nutzung kommt darüber hinaus aber auch keine schutzbereichseröffnende Funktion hinsichtlich des *GVIiS* zu. Der Schutzbereich des *GVIiS* ist nicht allein auf die private Nutzung begrenzt. Er umfasst gleichberechtigt die geschäftliche Nutzung eines informationstechnischen Systems. Denn auch bei einer geschäftlichen Nutzung lasse sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen.[1325] Daher darf auch im Falle der ausschließlich geschäftlichen Nutzung eine ungehinderte Persönlichkeitsentfaltung nicht durch die Unsicherheit über möglicherweise vorhandene technische Überwachungsmaßnahmen verhindert werden. Parallel dazu ist wiederum der unmittelbare privatrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme nach § 823 Abs. 1 BGB zu bestimmen. Es ist somit auch bei einer nach dem Arbeitsvertrag vorgesehenen ausschließlich geschäftlichen Nutzung in gleicher Weise wie bei einer privaten Nutzung grundsätzlich das Interesse des Vertragspartners am größtmöglichen Erhalt der Vertraulichkeit und Integrität seines informationstechnischen Systems und damit der selbstbestimmten Verfügung über das System in die Abwägung der entgegenstehenden Interessen einzustellen. Im konkreten Einzelfall ist aber auch die ausschließlich geschäftliche Nutzung als Nutzung des informationstechnischen Systems „als eigenes" anzusehen. Eine solche Nutzung kommt insbesondere dann in Betracht, wenn dem Arbeitnehmer informationstechnische Systeme zum eigenverantwortlichen Gebrauch überlassen werden.[1326] Die Gestattung einer privaten Nutzung des Systems ist jedoch keine Frage der Schutzbereichseröffnung. Das *BVerfG* stellt vielmehr die Persönlichkeitsrelevanz der bloß geschäftlichen Nutzung derjenigen der privaten Nutzung vollumfänglich gleich. Eine Differenzierung findet weder hinsichtlich der Schutzbereichseröffnung noch hinsichtlich der Rechtfertigungsvoraussetzungen eines

[1324] Die Eröffnung des Schutzbereichs des *GVIiS* ist hingegen nicht davon abhängig, dass der Arbeitgeber auch die private Nutzung gestattet; so aber *Tinnefeld/Petri/Brink*, MMR 2010, 727 (734).

[1325] *BVerfGE* 120, 274 (314).

[1326] Siehe hierzu bereits oben auf S. 108 sowie *Petri*, Vortrag Wiesbadener Forum (Fn. 467), auf der Grundlage eines Beschlusses des *VGH Kassel* vom 19.5.2009 - 6 A 2672/08.Z (NJW 2009, 2470); es ist damit nicht entscheidend, dass etwaige Überwachungsmaßnahmen des Arbeitgebers bloß an von ihm zur Verfügung gestellten Betriebsmitteln stattfinden, nicht hingegen an privaten Systemen des Arbeitnehmers, so aber MüArbR/*Reichold* § 88 Rn. 4.

Eingriffs statt. Auf die Qualifikation der enthaltenen Daten als privat oder geschäftlich kommt es demnach nicht an. Eine solche Differenzierung scheidet hingegen auch von vornherein aus. Denn die Eröffnung des Schutzbereichs des *GVIiS* knüpft zunächst nur an einen potentiell enthaltenen Datenbestand an. Diese Daten müssen lediglich personenbezogen sein. Inhaltliche Anforderungen bestehen nur insoweit, als der Funktionsumfang des informationstechnischen Systems einen besonders umfangreichen und vielfältigen Datenbestand möglich macht. Dieser kann jedoch gleichfalls privater als auch geschäftlicher Art sein. Folglich kann hinsichtlich der Rechtfertigungsvoraussetzungen von Überwachungsmaßnahmen im Arbeitsverhältnis, die mit einer technischen Infiltration des informationstechnischen Systems verbunden sind, die Unterscheidung zwischen der nach dem Arbeitsvertrag erlaubten privaten und der ausschließlich geschäftlichen Nutzung nicht aufrechterhalten werden.[1327]

Eine für die Feststellung der Rechtswidrigkeit einer Beeinträchtigung notwendige Interessenabwägung dürfte dabei nicht in jedem Fall von vornherein zu Lasten des Arbeitgebers ausfallen. Die bereits zur Interessenabwägung nach § 307 Abs. 1 BGB aufgeführten Interessen des Arbeitgebers sind ebenso nach Maßgabe der mittelbaren Drittwirkung der Art. 12 Abs. 1 S. 1 und Art. 14 Abs. 1 S. 1 GG zu berücksichtigen. Die Gleichsetzung der geschäftlichen mit der privaten Nutzung von informationstechnischen Systemen beseitigt nicht die Möglichkeit, sämtliche Unterschiede in den Nutzungsgepflogenheiten zu berücksichtigen. Ob ein informationstechnisches System, dass dem Arbeitnehmer eigenverantwortlich i.S.d. der Nutzung „*als eigenes*“ überlassen wurde, „*typischerweise* bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität […][1328]“ genutzt wird, erscheint fraglich. Die Interessenabwägung dürfte vielmehr vorbehaltlich der ihr immanenten Einzelfallabwägung aufgrund einer unzulässigen Totalüberwachung des Arbeitnehmers zu Lasten des Arbeitgebers ausfallen.[1329] Gerade vor einer solchen Profilbildung soll das *GVIiS* schützen.[1330] Der bloß punktuelle Zugriff zum Zwecke der softwareseitigen Wartung des Systems dürfte demnach mangels einer dauerhaften Überwachung zulässig sein.[1331] Hierfür spricht auch das eigene Interesse des Arbeitgebers an der Sicherheit des genutzten Systems und damit wiederum der Schutz vor unberechtigten Zugriffen Dritter.

---

[1327] Ebenso *Wedde*, AuR 2009, 373 (376); für eine generelle Unzulässigkeit einer Überwachung bei auch privater Nutzung *Herrmann*, IT-Grundrecht, S. 202.

[1328] *BVerfGE* 120, 274 (323) (Hervorhebung nur hier).

[1329] Vgl. *BAG* NZA 2003, 1193 (1194); NZA 2004, 1278 (1282); NZA 2008, 1187 (1190).

[1330] *BVerfGE* 120, 274 (305).

[1331] *Stögmüller*, CR 2008, 435 (438) schlägt für diesen Fall eine ausdrückliche individualvertragliche Vereinbarung zwischen Arbeitgeber und -nehmer vor.

(3) Einwilligung

Schließlich kommt noch die Einwilligung des Arbeitnehmers in den Zugriff in Betracht. Unabhängig von der konkreten Ausgestaltung der Einwilligungserklärung stellt sich die Frage nach der rechtfertigenden Wirkung der Einwilligung für die Verarbeitung von Arbeitnehmerdaten.[1332] Die Freiwilligkeit einer solchen Einwilligung kann angesichts unterschiedlicher Verhandlungsmacht und der wirtschaftlichen Abhängigkeit des Arbeitnehmers fraglich sein.

*3. Treu und Glauben, § 242 BGB*

Kaum zusätzliche und weitere Besonderheiten kommen dem *GVIiS* demgegenüber i.R.d. § 242 BGB zu. Ein Schuldner ist gem. § 242 BGB verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern. Die §§ 307ff. BGB sind jedoch gegenüber § 242 BGB die speziellere Norm.[1333] Allerdings ist § 242 BGB dann neben der Inhaltskontrolle anwendbar, wenn es um die Frage geht, ob die Berufung auf eine wirksame Klausel im Einzelfall gegen Treu und Glauben verstößt.[1334] § 242 BGB ist folglich direkt anwendbar, sofern eine individualvertragliche Einwilligung in den Zugriff auf das informationstechnische System vorliegt. Da die Inhaltskontrolle des § 307 Abs. 1 BGB ebenfalls an den objektiven Maßstab des § 242 BGB anknüpft,[1335] dürften sich in der vorzunehmenden Abwägung der verschiedenen Interessen keine Unterschiede dahingehend ergeben, ob diese Abwägung im Rahmen des § 307 Abs. 1 BGB oder des § 242 BGB erfolgt.

---

1332 Vgl. hierzu etwa *Gola*, Datenschutz und Multimedia am Arbeitsplatz, Rn. 324ff.; *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, § 4a Rn. 5a; *Gola*, RDV 2002, 109; § 32l Abs. 1 BDSG-E des RegE zur Regelung des Beschäftigtendatenschutzes sieht vor, dass der Einwilligung des Beschäftigten nur rechtfertigende Wirkung zukommt, wenn das Gesetz dies ausdrücklich bestimmt; gem. Art. 7 Abs. 4 DS-GVO-E bietet die Einwilligung keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht. ErwG 34 der DS-GVO-E nennt als Beispiel für ein solches Ungleichgewicht auch das Arbeitsverhältnis; nach der Art-29-Datenschutzgruppe komme im Anwendungsbereich der EG-Datenschutzrichtlinie eine rechtfertigende Wirkung der Einwilligung auch im Arbeitsverhältnis grds. in Betracht, allerdings sei es in den Fällen, in denen ein Arbeitgeber zwangsläufig aufgrund des Beschäftigungsverhältnisses personenbezogene Daten verarbeiten muss, irreführend, wenn dieser versucht, die Verarbeitung auf die Einwilligung der betroffenen Person zu stützen. Auf die Einwilligung des Arbeitnehmers sollte nur dann zurückgegriffen werden, wenn dieser eine echte Wahl hat und seine Einwilligung später auch ohne Nachteile widerrufen kann, WP 48, S. 3, 27f. (abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48de.pdf); vgl. auch WP 168, S. 19 Rn. 66 (Fn. 619).

1333 MüKoBGB-*Kieninger*, Vor § 307 Rn. 11.

1334 *BGHZ* 105, 71 (88); *BGH* NJW-RR 86, 271 (272).

1335 *Fuchs*, in: *Ulmer/Brandner/Hensen*, AGB-Recht, § 307 Rn. 97; MüKoBGB-*Kieninger*, § 307 Rn. 32.

### *4. Sittenwidrigkeit, § 138 Abs. 1 BGB*

Die Einwilligung des berechtigten Nutzers in den Zugriff auf sein informationstechnisches System könnte ferner an § 138 Abs. 1 BGB zu messen sein. Danach ist ein Rechtsgeschäft, das gegen die guten Sitten verstößt, nichtig.

#### a. Verhältnis zu § 307 Abs. 1 BGB

Soweit eine formularvertragliche Einwilligung vorliegt, die schon nach § 307 Abs. 1 BGB unwirksam ist, bleibt dahingehend für § 138 Abs. 1 BGB kein Raum. Umstritten ist dann aber, ob auch die unwirksame Klausel in die nach § 138 Abs. 1 BGB vorzunehmende Gesamtbetrachtung aller Umstände die Wirksamkeit des gesamten Rechtsgeschäfts betreffend einbezogen werden kann.[1336] Dafür spreche u.a., dass ein Verstoß gegen § 138 BGB über § 139 BGB anders eine unwirksame Klausel nach § 306 Abs. 1 BGB regelmäßig zur Nichtigkeit des gesamten Rechtsgeschäfts führe.[1337] Kommt der Einwilligung in den Zugriff auf das informationstechnische System die Rechtsnatur eines Rechtsgeschäfts zu, wird demnach regelmäßig bei Sittenwidrigkeit der Einwilligung der gesamte Vertrag nichtig sein. Eine unangemessene formularvertragliche Einwilligung hingegen ist zwar auch bei einer Würdigung des gesamten Vertrages zu berücksichtigen, berührt jedoch nach dem gesetzlichen Regelfall des § 306 Abs. 1 BGB die Wirksamkeit des übrigen Teils nicht.

#### b. Sittenwidrigkeit der Einwilligung

Steht hingegen die Sittenwidrigkeit allein der individualvertraglichen Einwilligung im Raum, müsste § 138 Abs. 1 BGB zunächst überhaupt auf die entsprechende Regelung anwendbar sein. Der Anwendungsbereich des § 138 Abs.1 BGB erstreckt sich seinem Wortlaut nach auf Rechtsgeschäfte sowie darüber hinaus auch auf rechtsgeschäftsähnliche Handlungen.[1338] Der individualvertraglichen Einwilligung müsste daher überhaupt eine entsprechende Rechtsnatur zugesprochen werden.[1339]

---

[1336] Dafür *Stoffels*, AGB-Recht, Rn. 384ff.; *Wolf*, in: *Ders./Lindacher/Pfeiffer*, AGB-Recht, § 307 Rn. 24; Staudinger/*Coester* (2006), § 307 Rn. 32ff.; dagegen: MüKoBGB-*Kieninger*, Vor § 307 Rn. 10; Palandt/*Ellenberger*, § 138 Rn. 16; Palandt/*Grüneberg*, Überbl v § 305 Rn. 15; Erman/*Roloff*, Vor §§ 307-309 Rn. 11.

[1337] *Stoffels*, AGB-Recht, Rn. 384; *Wolf*, in: *Ders./Lindacher/Pfeiffer*, AGB-Recht, § 307 Rn. 22.

[1338] Bamberger/Roth/*Wendtland*, § 138 Rn. 3; Palandt/*Ellenberger*, § 138 Rn. 11.

[1339] Zur Rechtsnatur der Einwilligung siehe etwa den Überblick bei Staudinger/*Hager* (1999), § 823 Rn. C176; MüKoBGB-*Wagner*, § 823 Rn. 731; *Ohly*, Einwilligung im Privatrecht, S. 201ff.; differenzierend MüKoBGB-*Rixecker*, Allg. PersönlR Rn. 54: Doppelnatur, sofern Einwilligung und Gestattung kommerzieller Nutzung von Bildnissen zusammenfallen; letztere habe rechtsgeschäftlichen Charakter; zustimmend Staudinger/*Hager* (1999), § 823 Rn. C176; speziell zur Einwilligung nach § 4a BDSG: Rechtsgeschäft: *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 20; rechtsgeschäftsähnliche Handlung: *Däubler*/Klebe/Wedde/Weichert, BDSG, § 4a Rn. 5; Realhand-

i. Objektiver Inhalt

Zunächst kann § 138 Abs. 1 BGB schon aufgrund des objektiven Inhalts des Rechtsgeschäfts einschlägig sein. Sittenwidrig ist danach ein Rechtsgeschäft, dessen Inhalt gegen grundlegende Wertungen der Rechts- und Sittenordnung verstößt.[1340] Grundlegend sind insofern insbesondere die Wertungen des Grundgesetzes oder wesentliche der Rechtsordnung immanente rechts- und sozialethische Werte.[1341] Das Bewusstsein der Parteien von der Sittenwidrigkeit oder die Kenntnis der die Sittenwidrigkeit begründenden Umstände ist dann nicht erforderlich.[1342] Ein solcher Verstoß kann hier nicht schon aufgrund der bloßen Einwilligung in eine Rechtsverletzung angenommen werden. Zwar hat die Einwilligung die Beeinträchtigung eines auch grundgesetzlich geschützten Verhaltens zum Gegenstand. Der Verzicht auf den entsprechenden Schutz ist hingegen ebenfalls grundrechtlich geschützt. Der Einzelne entscheidet grundsätzlich selbst über die Art seiner ungehinderten Persönlichkeitsentfaltung.

Hingegen kann ein anderes Ergebnis aus den Anforderungen an die Freiwilligkeit der Einwilligung folgen. Enthält die individualvertragliche Regelung nicht diejenigen notwendigen Angaben, um den Anforderungen an eine informierte Einwilligung zu genügen, so fehlt es an einer selbstbestimmten Verfügung des Betroffenen. Im Anwendungsbereich des BDSG ist die Einwilligung in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur bei ausreichender Information des Betroffenen gem. § 4a Abs. 1 S. 2 BDSG wirksam.[1343] Liegen dessen Voraussetzungen nicht vor, ist die Datenverarbeitung unzulässig.[1344] Da die Einwilligung nach § 4a BDSG wiederum gerade Ausübung informationeller Selbstbestimmung ist,[1345] führen die Anforderungen des § 4a Abs. 1 S. 2 BDSG zu einer unmittelbaren Realisierung des Selbstbestimmungsrechts über die Offenbarung persönlicher Lebenssachverhalte. Gerade über die zivilrechtlichen Generalklauseln wie § 138 Abs. 1 BGB finden die Grundrechte im Wege der mittelbaren Drittwirkung Anwendung auch in Privatrechtsverhältnissen.[1346] Stellt eine Einwilligung in den Zugriff auf das informationstechnische System mangels ausreichender Information keinen Ausdruck der Selbstbestimmung des Betroffenen über seine persönlichen Informationen dar, kann eine solche Regelung wiederum auch keine selbstbestimmte Verfügung über die Vertraulichkeit und Integrität des eigenen informationstechnischen Systems sein. Der Betroffene wäre ungewollt einer Persönlichkeitsgefährdung von besonderem Ausmaß ausgesetzt, namentlich der

lung: *Gola/Schomerus*, BDSG, § 4a Rn. 25; offen: *Bergmann/Möhrle*/Herb, Datenschutzrecht, Bd. 1, § 4a BDSG Rn. 9 (nicht Geschäfts-, sondern Einsichtsfähigkeit entscheidend).

1340 Bamberger/Roth/*Wendtland*, § 138 Rn. 16ff., 20; Palandt/*Ellenberger*, § 138 Rn. 3f..

1341 Bamberger/Roth/*Wendtland*, § 138 Rn. 17f.

1342 *BGHZ* 94, 268 (272).

1343 *Gola/Schomerus*, BDSG, § 4a Rn. 26; *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 76.

1344 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 76.

1345 *Simitis*, in: *Ders.* (Hrsg.), BDSG, § 4a Rn. 2.

1346 *BVerfGE* 7, 198 (206); 81, 242 (256); 89, 214 (229).

Möglichkeit des Vertragsgegners „einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten". Die Anerkennung einer solchen Einwilligung als wirksam würde gerade im Widerspruch zu dem *GVIiS* als insoweit zu berücksichtigender objektiver Wertentscheidung stehen.

ii. Gesamtwürdigung

Ist ein Rechtsgeschäft nicht bereits aufgrund seines objektiven Inhalts als sittenwidrig anzusehen, so kann sich seine Sittenwidrigkeit daneben in erster Linie aus einer Gesamtwürdigung von Inhalt, Motiv und Zweck des Rechtsgeschäfts ergeben.[1347]

(1) Objektive Sittenwidrigkeit

Objektiv sittenwidrig dürfte eine solche Regelung sein, in der sich der Betroffene für den Erhalt der vertraglich geschuldeten Leistung verpflichtet, den Zugriff des Vertragsgegners auf das informationstechnische System zu erlauben. Die Nichtigkeitsfolge des § 138 Abs. 1 BGB kommt dabei aber von vornherein nur für solche Fälle in Betracht, in denen der Zugriff keine zwingende Voraussetzung für die Erbringung der Leistung ist. Im Anwendungsbereich des BDSG könnte eine solche Regelung gegen das Koppelungsverbot des § 28 Abs. 3b BDSG verstoßen. Mangels Freiwilligkeit der Entscheidung läge keine wirksame Einwilligung i.S.d. § 4a Abs. 1 S. 1 BDSG vor. Die Hinnahme der durch den Zugriff begründeten besonderen Gefährdung seiner Persönlichkeit ist dann nicht Ausdruck der Selbstbestimmung des Betroffenen, sondern durch seine strukturelle Unterlegenheit dem Vertragsgegner gegenüber bedingt.[1348] In beiden Fällen verkehrt sich dann die Selbstbestimmung des Betroffenen über die Offenbarung persönlicher Lebenssachverhalte in eine Fremdbestimmung des Vertragsgegners.[1349] Zusätzlich ist dann noch im Wege der mittelbaren Drittwirkung die Beschränkung des *GVIiS* als Ausprägung auch des verfassungsrechtlichen allgemeinen Persönlichkeitsrechts in die vorzunehmende Gesamtwürdigung einzubeziehen.

(2) Subjektive Sittenwidrigkeit

Sofern sich die Sittenwidrigkeit des Rechtsgeschäfts nicht bereits allein aus seinem objektiven Inhalt ergibt, muss dem Vertragspartner auch subjektiv ein Vorwurf gemacht werden können. Es sind hierfür die Umstände des Zustandekommens des Rechtsgeschäfts sowie die Absichten und Motive der Parteien zu berücksichtigen.[1350] Notwendig und ausreichend ist bei einem objektiv sittenwidrigen Verhalten allein gegenüber dem Geschäftspartner ein dem anderen Teil vorwerfbares

[1347] *BGH* NJW 1961, 822; NJW 1965, 580 (580f.); NJW 1998, 2047; NJW 2001, 1127.
[1348] Vgl. zu Bürgschaftsverträgen etwa *BVerfG* NJW 1994, 36.
[1349] *BVerfGE* 89, 214 (232); 103, 89 (101); 114, 1 (34); 114, 73 (90).
[1350] *BGH* NJW-RR 1998, 590 (591).

Verhalten.[1351] Dabei setzt das subjektive Element der Sittenwidrigkeit jedenfalls die Kenntnis der Tatsachen voraus, aus denen sich die Sittenwidrigkeit ergibt.[1352] Ein solcher Verstoß könnte sich hier aus einer bewussten Ausnutzung eines Informationsdefizits des Betroffenen ergeben. Im Gegensatz zu dem Betroffenen wird derjenige, der sich entsprechende Zugriffsrechte einräumen lässt, regelmäßig um die Möglichkeiten der sich ihm bietenden Informationsgewinnung wissen. Gleichzeitig wird er dann umgekehrt aber auch das fehlende technische Verständnis des Betroffenen kennen. Im zweiten Fall könnte sich das subjektive Element der Sittenwidrigkeit aus der bewussten Ausnutzung des Bedarfs des Betroffenen an der vertraglichen Leistung ergeben.

### *5. Vertragliche Schutzpflichten, § 241 Abs. 2 BGB*

Ein Schuldverhältnis kann jeden Teil zur Rücksicht auf die Rechte, Rechtsgüter und Interessen verpflichten, § 241 Abs. 2 BGB. Die Schutzpflichten des § 241 Abs. 2 BGB bezwecken die Erhaltung des Integritätsinteresses des anderen Teils.[1353] Solche Pflichten kommen hier in zweierlei Hinsicht in Betracht: Zunächst sind durch den Zugriff selbst verursachte Datenverluste sowie die versehentliche Löschung von Datenbeständen[1354] zu vermeiden. Der Missbrauch eines Zugriffsprogramms ist insbesondere durch technische Maßnahmen zu verhindern. Daneben ist aber auch das Interesse des Betroffenen am größtmöglichen Erhalt der Vertraulichkeit und Integrität des informationstechnischen Systems zu berücksichtigen. Ein zur Erbringung der vertraglichen Leistung zwingend notwendiger Zugriff auf das System hat sich auf denjenigen Umfang zu beschränken, der für die Leistungserbringung unabdingbar ist.

### *6. Ergebnis*

Durch die Einwilligung des berechtigten Nutzers in den Zugriff auf sein informationstechnisches System entfällt die Rechtswidrigkeit der damit verbundenen Verletzung des allgemeinen Persönlichkeitsrechts und sonstiger von § 823 Abs. 1 BGB geschützter absoluter Rechte. Ebenso entfällt ein Anspruch aus § 823 Abs. 2 BGB. Auch die Gestattung des Zugriffs auf das eigene informationstechnische System kann Ausdruck der Persönlichkeitsentfaltung sein. Anders als die Einwilligung nach § 4a Abs. 1 BDSG ist die Einwilligung in den Zugriff auf das eigengenutzte informationstechnische System nicht ausdrücklich gesetzlich geregelt. § 4a Abs. 1 S. 2 BDSG legt jedoch schon für die Einwilligung in den Umgang mit einzelnen personenbezogenen Daten besondere Voraussetzungen fest. Daher müssen diese Voraussetzungen erst recht gelten, wenn der Zugriff auf eine derart umfangreiche und vielfältige Informationsquelle wie ein komplexes informations-

[1351] *BGHZ* 50, 63 (70).
[1352] *BGH* NJW-RR 1998, 590 (591); NJW 2005, 2991.
[1353] MüKoBGB-*Roth*, § 241 Rn. 109; Palandt/*Grüneberg*, § 241 Rn. 6.
[1354] *BVerfGE* 120, 274 (325).

technisches System gestattet werden soll. Denn nur wenn der Nutzer die Bedeutung seiner Entscheidung überblicken kann, kann diese Entscheidung auch Ausdruck seines Selbstbestimmungsrechts sein. Eine solche Einwilligung kann grundsätzlich auch formularvertraglich erfolgen. Bei der notwendigen Interessenabwägung nach § 307 Abs. 1 BGB ist die enorme Persönlichkeitsrelevanz des Zugriffs auf das informationstechnische System zu berücksichtigen. Die in die Interessenabwägung einzustellenden Aspekte finden entsprechend bei § 138 Abs. 1 BGB Berücksichtigung. Den Vertragspartner des Betroffenen treffen dann Pflichten nach § 241 Abs. 2 BGB zur Vermeidung von Fernwirkungen des Zugriffs sowie zum größtmöglichen Erhalt der Vertraulichkeit und Integrität des Systems.

# Kapitel 3 – Schlussbetrachtung

Seit der Entscheidung des *BVerfG* vom 27. Februar 2008 spielte das *GVIiS* in der verfassungsgerichtlichen Rechtsprechung keine besondere Rolle mehr. Zwangsläufig blieb damit auch eine fehlende Konkretisierung des Schutzbereichs des Grundrechts anhand weiterer zu entscheidender Sachverhalte aus. Der Schutzgehalt dieser neuen Ausprägung des allgemeinen Persönlichkeitsrechts konnte damit allein den tragenden Gründen der Entscheidung über die Verfassungsbeschwerden gegen das VSG NRW 2007 entnommen werden. Dennoch bietet schon die vorliegende Entscheidung konkrete Vorgaben, um das *GVIiS* in das grundrechtliche Gefüge einzuordnen. Die Konkurrenzverhältnisse zu den speziellen Freiheitsrechten sowie innerhalb des allgemeinen Persönlichkeitsrechts lassen sich aus den Entscheidungsgründen herausarbeiten. Diesen lässt sich insbesondere keine Subsidiarität zu dem *RiS* entnehmen. Die Begrifflichkeiten der Vertraulichkeit und Integrität können anhand einer Parallele zur Informationstechnik definiert werden. Eine konkrete Definition des informationstechnischen Systems hingegen hätte im vorliegenden Fall das Verständnis der Entscheidung erleichtert. So konnte nur aus der Begriffsverwendung in den Entscheidungsgründen auf eine möglichst weite Definition geschlossen werden. Ebenso hätte eine Definition der Verwendung des Systems „als eigenes" zum Verständnis der Entscheidung beigetragen. Hier wäre eine Präzisierung durch zukünftige Entscheidungen wünschenswert. Jedoch bleiben Zweifel, ob dies bereits in der Entscheidung in den Verfahren 1 BvR 370/07 und 1 BvR 595/07 zu einzelnen Normen des BKAG

geschehen wird. Der parlamentarische Gesetzgeber hat in § 20k BKAG die Formulierungen aus den Entscheidungsgründen des Urteils vom 27. Februar 2008 größtenteils wörtlich übernommen.

Die bisher geringe Bedeutung des *GVIiS* in der verfassungsgerichtlichen Rechtsprechung ist allerdings nicht gleichzusetzen mit der Bedeutung des *GVIiS* für den Schutz der Persönlichkeitsentfaltung des Einzelnen. Konsequent hat das *BVerfG* sein Verständnis von dem allgemeinen Persönlichkeitsrecht als lückenschließender Gewährleistung zum Ausdruck gebracht. Aus diesem Verständnis folgt notwendig, dass mit der Entscheidung des *BVerfG* keine Erweiterung des Schutzbereichs des allgemeinen Persönlichkeitsrechts verbunden sein kann, sondern dessen Schutzbereich lediglich hinsichtlich neuartiger Gefährdungen der Persönlichkeit durch den technischen Fortschritt präzisiert wurde. Der im Grundgesetz angelegte vollumfassende Schutz der menschlichen Persönlichkeit erfasst auch den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme. In dieser Ausprägung des allgemeinen Persönlichkeitsrechts kommt kein allein objektiver Systemschutz zum Ausdruck. Geschützt wird die selbstbestimmte Verfügung des Einzelnen über das von ihm genutzte informationstechnische System. Diese Form der Selbstbestimmung über persönliche Lebenssachverhalte kommt darin zum Ausdruck, dass das *GVIiS* den Gesetzgeber nicht verpflichtet, besondere Sicherheitsstandards der Informationstechnologie zu schaffen. Vielmehr schützt das Grundrecht die besondere technische Persönlichkeitssphäre, die sich der Einzelne durch die Nutzung eines informationstechnischen Systems schafft. Die Reichweite der Abschirmung dieser Sphäre gegenüber den Einblicken Dritter bestimmt aber allein der individuelle Nutzer. Das *GVIiS* ist daher in erster Linie i.S.d. klassischen Grundrechtsfunktion auf die Abwehr staatlicher Eingriffe in persönliche technische Sphäre eines informationstechnischen Systems angelegt.

Im Rahmen der Rechtsfiguren der grundrechtlichen Schutzpflichten und der mittelbaren Drittwirkung kommen dem *GVIiS* auch Wirkungen innerhalb von Privatrechtsverhältnissen zu. Der ganz große Umbruch bleibt hierbei jedoch aus. Ein Abwehranspruch des Einzelnen gegen Beeinträchtigungen des von ihm selbst geschaffenen Zustands von Vertraulichkeit und Integrität ist bereits über entsprechende Normen des BGB umzusetzen. Das BDSG stellt keine abschließende Regelung für die Vertraulichkeit und Integrität informationstechnischer Systeme dar. Daher bleibt das allgemeine Persönlichkeitsrecht des § 823 Abs. 1 BGB anwendbar. Der notwendige Abwehranspruch gegen Zugriffe Dritter lässt sich ohne entscheidende Ausweitung des Schutzbereichs innerhalb der anerkannten Fallgruppe des Eindringens in den persönlichen Bereich des Betroffenen formulieren. Der Schutzgehalt des *GVIiS* entspricht dem prägenden Aspekt des zivilrechtlichen Persönlichkeitsrechts in Gestalt der Selbstbestimmung über die eigene Persönlichkeit. Das StGB erfasst in einzelnen Normen bestimmte Eingriffsmodalitäten. Entscheidende Auswirkungen auf die Rechtsfiguren der Störer- und derjenigen der Produzentenhaftung sind mit der privatrechtlichen Umsetzung des Schutzgehalts des *GVIiS* nicht verbunden.

Die Einwilligung in den Zugriff auf ein informationstechnisches System ist grds. als Ausprägung persönlichkeitsrechtlicher Selbstbestimmung zulässig. Die Zulässigkeit einer formularvertraglichen Einwilligung hängt dabei entscheidend von dem Anlass der Einwilligung ab. Das Interesse an der werblichen Verwertung personenbezogener Daten des Einzelnen könnte die Bedeutung des Schutzbereichs des *GVIiS* auf privater Ebene eher auf den Bereich der Frage nach der Wirksamkeit der Einwilligung in den Zugriff auf das eigengenutzte informationstechnische System verschieben. Angesichts des hohen wirtschaftlichen Wertes, den die in Daten verkörperten Informationen in der heutigen Wirtschaftswelt haben, dürfte der heimlichen Infiltration informationstechnischer Systeme eine besondere Bedeutung eher im Bereich der Betriebsspionage zukommen.

Für den Bereich des Arbeitsverhältnisses kommt der prinzipiellen Gleichsetzung der privaten und geschäftlichen Nutzung informationstechnischer Systeme durch das *BVerfG* entscheidende Bedeutung zu. Die Reichweite der Zulässigkeit etwaiger Kontroll- und Überwachungsmaßnahmen ist entsprechend beschränkt. Zugriffsrechte sind nur nach Maßgabe einer informierten Einwilligung, die das Selbstbestimmungsrecht des Nutzers über sein informationstechnisches System ausreichend berücksichtigen, zulässig.

Der gläserne Mensch mag in unserer digitalen Welt nicht mehr weit entfernt sein. Zudem hat der sog. *Staatstrojaner* die Diskussion um den Ausgleich der Reichweite staatlicher Ermittlungsbefugnisse und der Wahrung der Freiheitsrechte des einzelnen Bürgers, wie sie bereits im Vorfeld der Entscheidung vom 27. Februar 2008 geführt wurde, wieder aufleben lassen. Das *BVerfG* hatte mit seiner Entscheidung aber wie schon im *Volkszählungsurteil* unmissverständlich klargemacht: Technischer Fortschritt kann zwar immer mit neuartigen Gefährdungen der Persönlichkeitsentfaltung des Einzelnen einhergehen. Der Einzelne genießt jedoch stets auch vor diesen Gefährdungen Schutz. Denn technischer Fortschritt kann und darf keinesfalls umgekehrt den Schutz der Persönlichkeit des Einzelnen reduzieren.

# Literaturverzeichnis


*Abel, Stefan*, Der Millennium-Bug und der lange Arm der Produzentenhaftung, CR 1999, S. 680-683

*Ahrens, Hans-Jürgen*, 21 Thesen zur Störerhaftung im UWG und im Recht des Geistigen Eigentums, WRP 2007, S. 1281-1290

*Albers, Marion*, Informationelle Selbstbestimmung, Baden-Baden 2005

*Altenburg, Stephan/v. Reinersdorff, Wolfgang/Leister, Thomas*, Telekommunikation am Arbeitsplatz, MMR 2005, S. 135-139

*Amann, Esther/Atzmüller, Hugo*, IT-Sicherheit – was ist das? DuD 1992, S. 286-292

*Bäcker, Matthias*, Die Vertraulichkeit der Internetkommunikation, in: *Rensen, Hartmut/Brink, Stefan* (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts - Erörtert von den wissenschaftlichen Mitarbeitern, Berlin 2009

*Bäcker, Matthias*, Grundrechtlicher Informationsschutz gegen Private, Der Staat [2012], S. 91-116

*Baldus, Manfred*, Der Kernbereich privater Lebensgestaltung – absolut geschützt, aber abwägungsoffen, JZ 2008, S. 218-227

*Bamberger, Heinz Georg/Roth, Herbert* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch; Band 1, §§ 1-610, CISG, 3. Aufl., München 2012 (zit.: Bamberger/Roth/*Bearbeiter*)

*Bamberger, Heinz Georg/Roth, Herbert* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch; Band 2, §§ 611-1296, AGG, ErbbauVO, WEG, 3. Aufl., München 2012 (zit.: Bamberger/Roth/Bearbeiter)

*Bär, Wolfgang*, Anmerkung zu BGH, Beschluss vom 31.1.2007 - StB 18/06, MMR 2007, S. 239-242

*Bartsch, Michael*, Computerviren und Produkthaftung, CR 2000, S. 721-725

*Bartsch, Michael*, Die „Vertraulichkeit und Integrität informationstechnischer Systeme" als sonstiges Recht nach § 823 Abs. 1 BGB, in: CR 2008, S. 613-617

*Bassenge, Peter/Brudermüller, Gerd/Diederichsen, Uwe/Ellenberger, Jürgen/Grüneberg, Christian/Sprau, Hartwig/Thorn, Karsten/Weidenkaff/Walter* (Bearb.), Palandt; Bürgerliches Gesetzbuch mit Nebengesetzen, 72. Aufl., München 2013 (zit.: Palandt/*Bearbeiter*)

*Baston-Vogt, Marion*, Der sachliche Schutzbereich des zivilrechtlichen allgemeinen Persönlichkeitsrechts, Tübingen 1997

*Benda, Ernst/Klein, Eckart* , Verfassungsprozessrecht, Ein Lehr- und Handbuch, 2. Aufl., Heidelberg 2001

*Benda, Ernst/Klein, Eckart/Klein, Oliver*, Benda/Klein, Verfassungsprozessrecht, Ein Lehr- und Handbuch, 3. Aufl., Heidelberg 2012

*Bergmann, Lutz/Möhrle, Roland/Herb, Armin* , Datenschutzrecht, Kommentar, Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, bereichsspezifischer Datenschutz, Band 1, Teile I bis III, Systematik, Text, Kommentar (Loseblatt), 45. EL (Juli 2012), Stuttgart u.a.

*Bernreuther, Friedrich*, Neues zur Telefonwerbung, WRP 2009, 390-407

*Beulke, Werner/Meininghaus, Florian*, Anmerkung zu BGH (Ermittlungsrichter), Beschluss vom 21.2.2006 - 3 BGs 31/06, StV 2007, S. 63-65

*Bizer, Johann*, Gegen die Online-Durchsuchung, DuD 2007, S. 640

*Böckenförde, Ernst-Wolfgang*, Schutzbereich, Eingriff, verfassungsimmanente Schranken – Zur Kritik gegenwärtiger Grundrechtsdogmatik, Der Staat [2003], S. 165-192

*Böckenförde, Thomas*, Die Ermittlung im Netz, Tübingen 2003

*Böckenförde, Thomas*, Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, S. 925-939

*Bogk, Andreas,* Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07, 2007 (abrufbar unter: http://web.archive.org/web/20071215135215/http://www.andreas.org/stellungnahme-bverfg.pdf)

*Braun, Frank/Roggenkamp, Jan Dirk* , 0zapftis – (Un)Zulässigkeit von „Staatstrojanern", K&R 2011, S. 681-686

*Britz, Gabriele*, Vertraulichkeit und Integrität informationstechnischer Systeme - Einige Fragen zu einem „neuen Grundrecht", DÖV 2008, S. 411-415

*Britz, Gabriele*, Europäisierung des grundrechtlichen Datenschutzes? EuGRZ 2009, S. 1-11

*Buchner, Benedikt*, Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument, DuD 2010, S. 39-34

*Buermeyer, Ulf*, Die „Online-Durchsuchung" – Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 154-166

*Buermeyer, Ulf*, Die „Online-Durchsuchung" – Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 329-337

*Buermeyer, Ulf*, Verfassungsrechtliche Grenzen der „Online-Durchsuchung", RDV 2008, S. 8-15

*Buermeyer, Ulf/Bäcker, Matthias*, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO, HRRS 2009, S. 433-441

*Callies, Christian/Ruffert, Matthias* (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 4. Aufl., München 2011

*Canaris, Claus-Wilhelm*, Grundrechte und Privatrecht, AcP 184 (1984), S. 201-246

*Canaris, Claus-Wilhelm*, Grundrechte und Privatrecht – eine Zwischenbilanz, Berlin 1999

*Classen, Claus Dieter*, Die Drittwirkung der Grundrechte in der Rechtsprechung des Bundesverfassungsgerichts, AöR 122 (1997), S. 65-107

*Claus, Volker/Schwill, Andreas*, Duden - Informatik A-Z, Fachlexikon für Studium, Ausbildung und Beruf, 4. Aufl., Mannheim 2006

*Dammann, Ulrich/Simitis, Spiros*, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997

*Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo*, Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, 3. Aufl., Frankfurt a. M. 2010

*Degenhart, Christoph*, Die allgemeine Handlungsfreiheit des Art. 2 I GG, JuS 1990, S. 161-169

*Dolzer, Rudolf/Kahl, Wolfgang/Waldhoff, Christian/Graßhof, Karin* (Hrsg.), Bonner Kommentar zum Grundgesetz (BK) (Loseblatt), Band 1 - Einleitung-Art. 4, 160. EL (März 2013), Heidelberg (zit.: *Bearbeiter*, in: BK GG)

*Dolzer, Rudolf/Kahl, Wolfgang/Waldhoff, Christian/Graßhof, Karin* (Hrsg.), Bonner Kommentar zum Grundgesetz (BK) (Loseblatt), Band 3 - Art. 6 II-14, 160. EL (März 2013), Heidelberg (zit.: *Bearbeiter*, in: BK GG)

*Dolzer, Rudolf/Kahl, Wolfgang/Waldhoff, Christian/Graßhof, Karin* (Hrsg.), Bonner Kommentar zum Grundgesetz (BK) (Loseblatt), Band 4 Art. 15-19, 160. EL (März 2013), Heidelberg (zit.: *Bearbeiter*, in: BK GG)

*Dreier, Horst* (Hrsg.), Grundgesetz; Kommentar, Band 1, Präambel, Art. 1-19, 2. Aufl., Tübingen 2004

*Dunz, Walter/Heimann-Trosien, Georg/Nüßgens, Karl/Steffen, Erich* (Bearb.), Das Bürgerliche Gesetzbuch mit besonderer Berücksichtigung der Rechtsprechung des Reichsgerichts und des Bundesgerichtshofes, Kommentar herausgegeben von Mitgliedern des Bundesgerichtshofes, Bd. II, 5. Teil, §§ 812-831, 12. Aufl. Berlin, New York 1989 (zit.: BGB-RGRK/*Bearbeiter*)

*Dürig, Günter*, Grundrechte und Privatrechtsprechung, in: *Maunz, Theodor* (Hrsg.), Vom Bonner Grundgesetz zur gesamtdeutschen Verfassung, Festschrift zum 75. Geburtstag von Hans Nawiasky, München 1956, S. 157-190

*Eckert, Claudia*, IT-Sicherheit, Konzepte – Verfahren – Protokolle, 7. Aufl., München 2012

*Eckhardt, Jens*, Anmerkung zu AG Berlin Mitte, Urteil vom 27.3.2007 - 5 C 314/06, K&R 2007, S. 601-604

*Ehmann, Eugen/Helfrich, Marcus*, EG-Datenschutzrichtlinie, Kurzkommentar, Köln 1999

*Ehmann, Horst*, Das Persönlichkeitsrecht als Wert, als Grundrecht und als absolut-subjektives Recht, in: *Stathopoulos, Michael/Beys, Kostas/Doris, Philippos/Karakostas, Ioannis* (Hrsg.), Festschrift für Apostolos Georgiades zum 70. Geburtstag, Athen u. a. 2006, S. 113-157

*Eifert, Martin*, Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, S. 521-523

*Erichsen, Hans-Uwe*, Grundrechtliche Schutzpflichten in der Rechtsprechung des Bundesverfassungsgerichts, JURA 1997, S. 85-89

*Ernst, Stefan/Vassilaki, Irini/Wiebe, Andreas*, Hyperlinks – Rechtsschutz, Haftung, Gestaltung, Köln 2002

*Ernst, Stefan* (Hrsg.), Hacker, Cracker & Computerviren, Köln 2004

*Eser, Albin/Heine, Günter/Perron, Walter/Sternberg-Lieben, Walter/Eisele, Jörg/Bosch, Nikolaus/Hecker, Bernd/Kinzig, Jörg*, Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl., München 2010 (zit.: S/S-*Bearbeiter*)

*Faustmann, Jörg*, Der deliktische Datenschutz, VuR 2006, S. 260-263

*Fischer, Thomas*, Strafgesetzbuch und Nebengesetze, 60. Aufl. München 2013

*Foerste, Ulrich/Westphalen, Friedrich Graf von* (Hrsg.), Produkthaftungshandbuch, 3. Aufl., München 2012 (zit.: Produkthaftungshandbuch/*Bearbeiter*)

*Fox, Dirk,* Realisierung, Grenzen und Risiken der „Online-Durchsuchung", DuD 2007, S. 827-834

*Fox, Dirk*, Stellungnahme zur „Online-Durchsuchung", Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, 2007 (abrufbar unter: http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf)

*Freiling, Felix C.,* Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, Mannheim 2007 (abrufbar unter: http://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf)

*Fuchs, Maximilian/Pauker, Werner*, Deliktsrecht, 8. Aufl., Berlin u. a. 2012

*Gercke, Marco*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit; der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten, CR 2007, S. 245-253

*Germann, Michael*, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000

*Gola, Peter*, Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, RDV 2002, 109-116

*Gola, Peter*, Datenschutz und Multimedia am Arbeitsplatz – Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 3. Aufl., Heidelberg u.a. 2010

*Gola, Peter/Klug, Christoph/Körffer, Barbara/Schomerus, Rudolf* (Bearb.), Gola/Schomerus, BDSG – Bundesdatenschutzgesetz, Kommentar, 11. Aufl., München 2012

*Götting, Horst-Peter/Schertz, Christian/Seitz, Walter* (Hrsg.), Handbuch des Persönlichkeitsrechts, München 2008

*Götz, Volkmar*, Die Verwirklichung der Grundrechte durch die Gerichte im Zivilrecht, in: *Heyde, Wolfgang/Starck, Christian* (Hrsg.), Vierzig Jahre Grundrechte in ihrer Verwirklichung durch die Gerichte, München 1990, S. 35-90

*Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin* (Hrsg.), Das Recht der Europäischen Union, Bd. I – EUV/AEUV (Loseblatt), 49. EL (November 2012), München

*Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin* (Hrsg.), Das Recht der Europäischen Union, Bd. IV – Sekundärrecht (Loseblatt), 40. EL (Oktober 2009), München

*Gröseling, Nadine/Höfinger, Frank Michael*, Hacking und Computerspionage – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, S. 549-553

*Guckelberger, Annette*, Veröffentlichung der Leistungsempfänger von EU-Subventionen und unionsgrundrechtlicher Datenschutz, EuZW 2011, S. 126-130

*Gudermann, Anne*, Online-Durchsuchung im Lichte des Verfassungsrechts – Die Zulässigkeit eines informationstechnologischen Instruments moderner Sicherheitspolitik, Hamburg 2010

*Gusy, Christoph*, Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Neuer Grundrechtsname oder neues Grundrechtsschutzgut?, DuD 2009, S. 33-41

*Haertel, Ines*, Altes im neuen Gewande? Die Fortentwicklung der Grundrechtsdogmatik am Beispiel des BVerfG-Urteils zur Online-Durchsuchung, Nds-VBl. 2008, S. 276-283

*Hansen, Markus*, DRM-Desaster: Das Sony BMG-Rootkit – Dubiose DRM-Software unterwandert System-Sicherheit, DuD 2006, S. 95-97

*Hansen, Markus/Pfitzmann, Andreas*, Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme, DRiZ 2007, S. 225, 227-228

*Harrendorf, Stefan*, Anmerkung zu BGH, Beschluss vom 31.1.2007 - StB 18/06, StraFO 2007, S. 149-152

*Härting, Niko*, Datenschutz im Internet – Wo bleibt der Personenbezug, CR 2008, S. 743-748

*Härting, Niko*, Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf, BB 2012, S. 459-466

*Härting, Niko*, Datenschutzrecht: Verbotsprinzip und Einwilligungsfetisch – Warum die alten Rezepte versagen - Plädoyer aus Sicht eines Anwalts, AnwBl 2012, S. 716-720

*Härting, Niko/Schneider, Jochen*, Das Dilemma der Netzpolitik, ZRP 2011, S. 233-236

*Hartmann, Alexander*, Unterlassungsansprüche im Internet, München 2009

*Heise, Michael*, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme? Zum Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, RuP 2009, S. 94-101

*Herdegen, Matthias*, Europarecht, 14. Aufl., München 2012

*Herrmann, Christoph*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Entstehung und Perspektiven, Frankfurt a. M. 2010

*Herzog, Roman/Scholz, Rupert/Herdegen, Matthias/Klein, Hans H.* (Hrsg.), Maunz/Dürig, Grundgesetz, Band I, Texte – Art. 5 (Loseblatt), 66. EL, (August 2012), München

*Herzog, Roman/Scholz, Rupert/Herdegen, Matthias/Klein, Hans H.* (Hrsg.), Maunz/Dürig, Grundgesetz, Band II, Art. 6-15 (Loseblatt), 66. EL, (August 2012), München

*Herzog, Roman/Scholz, Rupert/Herdegen, Matthias/Klein, Hans H.* (Hrsg.), Maunz/Dürig, Grundgesetz, Band III, Art. 16-27 (Loseblatt), 66. EL, (August 2012), München

*Hillgruber, Christian/Goos, Christoph*, Verfassungsprozessrecht, 3. Aufl., Heidelberg, München u. a. 2011

*Hirsch, Burkhard*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, NJOZ 2008, S. 1907-1915

*Hoffmann, Christian*, Die Verletzung der Vertraulichkeit informationstechnischer Systeme durch Google Street View, CR 2010, S. 514-518

*Hoffmann-Riem, Wolfgang*, Beharrung oder Innovation – Zur Bindungswirkung verfassungsgerichtlicher Entscheidungen, Der Staat [1974], S. 335-364

*Hoffmann-Riem, Wolfgang*, Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: *Ders./Schmidt-Aßmann, Eberhard* (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000

*Hoffmann-Riem, Wolfgang*, Grundrechtsanwendung unter Rationalitätsanspruch - Eine Erwiderung auf Kahls Kritik an neueren Ansätzen in der Grundrechtsdogmatik, Der Staat [2004], S. 203-233

*Hoffmann-Riem, Wolfgang*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2009, S. 1009-1022

*Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas* (Hrsg.), Grundlagen des Verwaltungsrechts, Band II – Informationsordnung, Verwaltungsverfahren, Handlungsformen, 2. Aufl., München 2012

*Hofmann, Manfred*, Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme, NStZ 2005, S. 121-125

*Hohmann-Dennhardt, Christine*, Informationeller Selbstschutz als Bestandteil des Persönlichkeitsrechts, RDV 2008, S. 1-7

*Holznagel, Bernd*, Recht der IT-Sicherheit, München 2003

*Holznagel, Bernd/Schumacher, Pascal*, Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID-Chips, MMR 2009, S. 3-8

*Hörnig, Dieter*, „Neues" Grundrecht, neue Fragen? Zum Urteil des BVerfG zur Online-Durchsuchung, JURA 2009, S. 207-213

*Hornung, Gerrit*, Ermächtigungsgrundlage für die „Online-Durchsuchung"? Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren, DuD 2007, S. 575-580

*Hornung, Gerrit*, Die Festplatte als „Wohnung"?, JZ 2007, S. 828-831

*Hornung, Gerrit*, Ein neues Grundrecht, CR 2008, S. 299-306

*Hornung, Gerrit*, Eine Datenschutz-Grundverordnung für Europa?, ZD 2012, S. 99-106

*Huber, Bertold*, Trojaner mit Schlapphut – Heimliche „Online-Durchsuchung" nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, NVwZ 2007, S. 880-884

*Hufen, Friedhelm*, Staatsrecht II, Grundrechte, 3. Aufl., München 2011

*Ihde, Rainer*, Cookies – Datenschutz als Rahmenbedingung der Internetökonomie, CR 2000, S. 413-423

*Isensee, Josef/Kirchhof, Paul* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band V, Allgemeine Grundrechtslehren, 2. Aufl., Heidelberg 2000 (zit.: *Bearbeiter*, in: HStR)

*Isensee, Josef/Kirchhof, Paul* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VI, Freiheitsrechte, 2. Aufl., Heidelberg 2001 (zit.: *Bearbeiter*, in: HStR)

*Isensee, Josef/Kirchhof, Paul* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VII, Normativität und Schutz der Verfassung – Internationale Beziehungen, Heidelberg 1992 (zit.: *Bearbeiter*, in: HStR)

*Isensee, Josef/Kirchhof, Paul* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band V, Rechtsquellen, Organisation, Finanzen, 3. Aufl., Heidelberg 2007 (zit.: *Bearbeiter*, in: HStR)

*Isensee, Josef/Kirchhof, Paul* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VII, Freiheitsrechte, 3. Aufl., Heidelberg 2009 (zit.: *Bearbeiter*, in: HStR)

*Jäger, Marc*, Verfassungsmäßigkeit der sog. Online-Durchsuchung und der Internetaufklärung durch staatliche Behörden, jurisPR-ITR 12/2008 Anm. 2

*Jahn, Matthias/Kudlich, Hans*, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, S. 57-61

*Jankowski, Julia*, Nichts ist unmöglich! – Möglichkeiten der formularmäßigen Einwilligung in die Telefonwerbung, GRUR 2010, S. 495-501

*Jarass, Hans Dieter*, Grundrechte als Wertentscheidungen bzw. objektivrechtliche Prinzipien in der Rechtsprechung des Bundesverfassungsgerichts, AöR 110 (1985), S. 363-397

*Jarass, Hans Dieter*, Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, S. 857-862

*Jarass, Hans Dieter*, Die Entwicklung des allgemeinen Persönlichkeitsrechts in der Rechtsprechung des Bundesverfassungsgerichts, in: *Erichsen, Hans-Uwe/Kollhauser, Helmut/Welp, Jürgen* (Hrsg.), Recht der Persönlichkeit, Berlin 1996

*Jarass, Hans Dieter/Pieroth, Bodo*, Grundgesetz für die Bundesrepublik Deutschland, 12. Aufl., München 2012

*Jauernig, Othmar* (Hrsg.), Bürgerliches Gesetzbuch mit Allgemeinem Gleichbehandlungsgesetz (Auszug), 14. Aufl., München 2011

*Joecks, Wolfgang/Miebach, Klaus* (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Band 1, §§ 1–37 StGB, 2. Aufl., München 2011 (zit.: MüKoStGB-*Bearbeiter*)

*Joecks, Wolfgang/Miebach, Klaus* (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Band 4, §§ 185-262 StGB, 2. Aufl., München 2012 (zit.: MüKoStGB-*Bearbeiter*)

*Joecks, Wolfgang/Miebach, Klaus* (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Band 4, §§ 263–358 StGB, §§ 1–8, 105, 106 JGG, München 2006 (zit.: MüKoStGB-*Bearbeiter*)

*Kahl, Wolfgang*, Die Schutzergänzungsfunktion von Art. 2 I GG, Tübingen 2000

*Kahl, Wolfgang/Ohlendorf, Lutz*, Grundfälle zu Art. 2 I i.V.m. 1 I GG, JuS 2008, S. 682-687

*Karg, Moritz*, Die Rechtsfigur des personenbezogenen Datums – Ein Anachronismus des Datenschutzes? ZD 2012, S. 255-260

*Kau, Wolfgang*, Vom Persönlichkeitsrecht zum Funktionsschutz – Persönlichkeitsschutz juristischer Personen des Privatrechts in verfassungsrechtlicher Sicht, Heidelberg 1989

*Kemper, Martin*, Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten, ZRP 2007, S. 105-109

*Kudlich, Hans*, Enge Fesseln für „Landes- und Bundestrojaner" – Anforderungen an die Zulässigkeit einer (sicherheitsrechtlichen) Online-Durchsuchung, JA 2008, S. 475-478

*Kühl, Kristian, Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl., München 2011

*Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios*, Datenschutzrecht, 2. Aufl., Heidelberg u. a. 2011

*Kunig, Philip*, Der Grundsatz informationeller Selbstbestimmung, JURA 1993, S. 595-604

*Kutscha, Martin*, Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung, NJW 2007, S. 1169-1172

*Kutscha, Martin*, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042-1044

*Kutscha, Martin*, Das „Computer-Grundrecht" – eine Erfolgsgeschichte?, DuD 2012, S. 391-394

*Kutscha, Martin*, Grundrechtlicher Persönlichkeitsschutz bei der Nutzung des Internet - Zwischen individueller Selbstbestimmung und staatlicher Verantwortung, DuD 2012, S. 461-646

*Ladeur, Karl-Heinz*, Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, S. 45-55

*Lang, Markus*, Reform des EU-Datenschutzrechts – Einheitliche Regelungen mit hohem Datenschutzniveau geplant, K&R 2012, S. 145-151

*Lange, Klaus*, Rechtskraft, Bindungswirkung und Gesetzeskraft der Entscheidungen des Bundesverfassungsgerichts, JuS 1978, S. 1-8

*Lapp, Thomas*, Cookies: Monster oder harmlose Kekse? Analyse der rechtlichen Auswirkungen und Schutzmöglichkeiten gegenüber der Verwendung von Cookies, ITRB 2001, S. 113-115

*Larenz, Karl/Canaris, Claus-Wilhelm*, Lehrbuch des Schuldrechts, Zweiter Band, Besonderer Teil, 2. Halbband, 13. Aufl., München 1994

*Laufhütte, Heinrich Wilhelm/Rissing-van Saan, Ruth/Tiedemann, Klaus* (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Erster Band, Einleitung, §§ 1-31, 12. Aufl., Berlin 2007 (zit.: LK-*Bearbeiter*, StGB)

*Laufhütte, Heinrich Wilhelm/Rissing-van Saan, Ruth/Tiedemann, Klaus* (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Sechster Band, §§ 146-210, 12. Aufl., Berlin 2010 (zit.: LK-*Bearbeiter*, StGB)

*Laufhütte, Heinrich Wilhelm/Rissing-van Saan, Ruth/Tiedemann, Klaus* (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Zehnter Band, §§ 284-305a, 12. Aufl., Berlin 2008 (zit.: LK-*Bearbeiter*, StGB)

*Leistner, Mathias/Stang, Felix*, Die Neuerung der wettbewerbsrechtlichen Verkehrspflichten - Ein Siegeszug der Prüfungspflichten? Zugleich ein Beitrag zur dogmatischen Fortentwicklung des Maßstabs der Prüfungspflichten, WRP 2008, S. 533-555

*v. Lewinski, Kai*, Europäisierung des Datenschutzrechts - Umsetzungsspielraum des deutschen Gesetzgebers und Entscheidungskompetenz des BVerfG, DuD 2012, S. 564-570

*Lorenz, Dieter*, Die verdeckte Online-Durchsuchung als Herausforderung an die Grundrechtsdogmatik, in: *Scholz, Rupert/Lorenz, Dieter/Pestalozza, Christian/Kloepfer, Michael/Jarass, Hans D./Degenhart, Christoph/Lepsius, Oliver*, Realitätsprägung durch Verfassungsrecht, Kolloquium aus Anlass des 80. Geburtstages von Peter Lerche, Berlin 2008

*Luch, Anika D.*, Das neue „IT-Grundrecht" – Grundbedingung einer „Online-Handlungsfreiheit", MMR 2011, 75-79

*Lücke, Jörg*, Der additive Grundrechtseingriff sowie das Verbot der übermäßigen Gesamtbelastung des Bürgers, DVBl. 2001, S. 1469-1478

*v. Mangoldt, Hermann/Klein, Friedrich/Starck, Christian* (Hrsg.), Kommentar zum Grundgesetz, Band 1: Präambel, Art. 1-19, 6. Aufl., München 2010

*v. Mangoldt, Hermann/Klein, Friedrich/Starck, Christian* (Hrsg.), Kommentar zum Grundgesetz, Band 2: Art. 20-82, 6. Aufl., München 2010

*v. Mangoldt, Hermann/Klein, Friedrich/Starck, Christian* (Hrsg.), Kommentar zum Grundgesetz, Band 3: Art. 83-146, 6. Aufl., München 2010

*Mantz, Reto*, Haftung für kompromittierte Computersysteme – § 823 Abs. 1 BGB und Gefahren aus dem Internet, K&R 2007, S. 566-570

*Marly, Jochen*, Praxishandbuch Softwarerecht – Rechtsschutz und Vertragsgestaltung, 5. Aufl., München 2009

*Martini, Mario*, Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, JA 2009, S. 839-845

*Meier, Klaus/Wehlau, Andreas*, Produzentenhaftung des Softwareherstellers - § 823 Abs. 1 BGB und das Produkthaftungsgesetz, CR 1990, S. 95-100

*Mengel, Anja*, Kontrolle der E-Mail- und Internetkommunikation am Arbeitsplatz, BB 2004, S. 2014-2021

*Merten, Detlef*, Grundrechtliche Schutzpflichten und Untermaßverbot, in: *Stern, Klaus/Grupp, Klaus* (Hrsg.), Gedächtnisschrift für Joachim Burmeister, Heidelberg 2005, S. 227-244

*Merten, Detlef/Papier, Hans-Jürgen* (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band II, Grundrechte in Deutschland: Allgemeine Lehren I, Heidelberg 2006 (zit.: *Bearbeiter*, in: HGR)

*Merten, Detlef/Papier, Hans-Jürgen* (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band III, Grundrechte in Deutschland: Allgemeine Lehren II, Heidelberg 2009 (zit.: *Bearbeiter*, in: HGR)

*Meyer, Klaus/Wehlau, Andreas*, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, S. 1585-1591

*Meyer, Sebastian*, Cookies & Co. – Datenschutz und Wettbewerbsrecht, WRP 2002, S. 1028-1035

*Michael, Lothar/Morlok, Martin*, Grundrechte, 3. Aufl., Baden-Baden 2012

*Moos, Flemming*, Die Entwicklung des Datenschutzrechts im Jahr 2007, K&R 2008, S. 137-145

*Mugdan, Benno* (Hrsg.), Die gesammten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich, Bd. 2: Recht der Schuldverhältnisse, Stockstadt a. M. 2005 (Nachdruck)

*v. Münch, Ingo/Kunig, Philip* (Hrsg.), Grundgesetz, Kommentar, Band 1: Präambel bis Art. 69, 6. Aufl. 2012, München 2012

*Münch, Peter*, Lässt der Entwurf einer Europäischen Datenschutz-Grundverordnung eine Modernisierung des technisch-organisatorischen Datenschutzes erwarten?, RDV 2012, S. 72-77

*Oeter, Stefan*, „Drittwirkung" der Grundrechte und die Autonomie des Privatrechts – Ein Beitrag zu den funktionell-rechtlichen Dimensionen der Drittwirkungsdebatte, AöR 119 (1994), S. 529-563

*Ohly, Ansgar*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, Tübingen 2002

*Pahlen-Brandt, Ingrid*, Zur Personenbezogenheit von IP-Adressen, K&R 2008, S. 288-290

*Pahlen-Brandt, Ingrid*, Datenschutz braucht scharfe Instrumente, Beitrag zur Diskussion um „personenbezogene Daten", DuD 2008, S. 34-40

*Peters, Hans*, Die freie Entfaltung der Persönlichkeit als Verfassungsziel, in: Festschrift für Rudolf Laun, Hamburg 1953, S. 669-678

*Peters, Hans*, Das Recht auf freie Entfaltung der Persönlichkeit in der höchstrichterlichen Rechtsprechung, Köln, Opladen 1963

*Pieroth, Bodo/Schlink, Bernhard*, Grundrechte, Staatsrecht II, 28. Aufl., Heidelberg u.a. 2012

*Pohl, Hartmut*, Zur Technik der heimlichen Online-Durchsuchung, DuD 2007, S. 684-688

*Polenz, Sven*, Verfassungsrechtliche Grundlagen des Datenschutzes, in: *Kilian, Wolfgang/Heussen, Benno* (Hrsg.), Computerrechtshandbuch - Informationstechnologie in der Rechts- und Wirtschaftspraxis, Kap. 130 (Loseblatt), 31. EL, Mai 2012, München (zit. Kilian/Heussen/*Bearbeiter*, CHB)

*Popp, Andreas*, Die „Staatstrojaner"-Affäre: (Auch) ein Thema für den Datenschutz – Kurzer Überblick aus strafprozessualer und datenschutzrechtlicher Sicht, ZD 2012, S. 51-55

*Reding, Viviane*, Herausforderungen an den Datenschutz bis 2020: Eine europäische Perspektive, ZD 2011, Editorial S. 1-2

*Reding, Viviane*, Sieben Grundbausteine der europäischen Datenschutzreform, ZD 2012, S. 195-198

*Richardi, Reinhard/Wlotzke, Otfried/Wißmann, Hellmut/Oetker, Hartmut* (Hrsg.), Münchener Handbuch zum Arbeitsrecht, Bd. 1 – Individualarbeitsrecht, 3. Aufl., München 2009 (zit.: MüArbR/*Bearbeiter*)

*Roggan, Fredrik* (Hrsg.), Online-Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin 2008

*Roßnagel, Alexander* (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003

*Roßnagel, Alexander/Müller, Jürgen*, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR 2004, S. 625-632

*Roßnagel, Alexander/Schnabel, Christoph*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534-3538

*Roßnagel, Alexander/Scholz, Philip*, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721-731

*Rux, Johannes*, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden – Rechtsfragen der „Online-Durchsuchung", JZ 2007, S. 285-295

*Rux, Johannes*, Analogie oder besondere Ausprägung des Verhältnismäßigkeitsprinzips, JZ 2007, S. 831-833

*Sachs, Michael* (Hrsg.), Grundgesetz, Kommentar, 6. Aufl., München 2011

*Sachs, Michael/Krings*, Thomas, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, 481- 485

*Säcker, Franz Jürgen/Rixecker, Roland* (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, Allgemeiner Teil, §§ 1-240, ProstG, AGG, 6. Aufl., München 2012 (zit. MüKoBGB-*Bearbeiter*)

*Säcker, Franz Jürgen/Rixecker, Roland* (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2, Schuldrecht Allgemeiner Teil, §§ 241-432, 6. Aufl., München 2012 (zit. MüKoBGB-*Bearbeiter*)

*Säcker, Franz Jürgen/Rixecker, Roland* (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 5, Schuldrecht Besonderer Teil III, §§ 705-853. Partnerschaftsgesellschaftsgesetz, Produkthaftungsgesetz, 5. Aufl., München 2009 (zit. MüKoBGB-*Bearbeiter*)

*Säcker, Franz Jürgen/Rixecker, Roland* (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, Sachenrecht, §§ 854-1296, Wohnungseigentumsgesetz, Erbbaurechtsgesetz, 6. Aufl., München 2013 (zit. MüKoBGB-*Bearbeiter*)

*Sankol, Barry*, Überwachung von Internettelefonie – Ein Schatten im Lichte der §§ 100a ff. StPO, CR 2008, S. 13-18

*Schaar, Peter*, Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, DuD 2000, S. 275-277

*Schaar, Peter*, Persönlichkeitsprofile im Internet, DuD 2001, S. 383-388

*Schaar, Peter*, Datenschutz im Internet – Die Grundlagen, München 2002

*Schaar, Peter*, Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 22. Tätigkeitsbericht

*Schaar, Peter/Landwehr, Sebastian*, K&R Kommentar, Anmerkung zu BGH, Beschluss vom 31.1.2007 – StB 18/06, K&R 2007, S. 202-205

*Schantz, Peter*, Verfassungsrechtliche Probleme von „Online-Durchsuchungen", KritV 2007, S. 310-330

*Schlaich, Klaus/Korioth, Stefan*, Das Bundesverfassungsgericht – Stellung, Verfahren, Entscheidungen, 9. Aufl., München 2012

*Schlegel, Stephan*, Warum die Festplatte keine Wohnung ist – Art. 13 GG und die „Online-Durchsuchung", GA 2007, S. 648-663

*Schneider, Jochen/Härting, Niko*, Warum wir ein neues BDSG brauchen – Kritischer Beitrag zum BDSG und dessen Defiziten, ZD 2011, S. 63-68

*Schneider, Jochen/Härting, Niko*, Wird der Datenschutz nun endlich internettauglich? - Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht, ZD 2012, S. 199-203

*Scholz, Rupert/Pitschas, Rainer*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984

*Schulz, Gabriel*, Das neue IT-Grundrecht – staatliche Schutzpflicht und Infrastrukturverantwortung, DuD 2012, S. 395-400

*Schulze-Fielitz, Helmuth*, Wirkung und Befolgung verfassungsgerichtlicher Entscheidungen, in: *Badura, Peter/Dreier, Horst* (Hrsg.), Festschrift 50 Jahre Bundesverfassungsgericht, Erster Band, Verfassungsgerichtsbarkeit, Verfassungsprozess, Tübingen 2001

*Schwartmann, Rolf*, Ausgelagert und ausverkauft – Rechtsschutz nach der Datenschutz-Grundverordnung, RDV 2012, S. 55-60

*Sieber, Ulrich*, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen (abrufbar unter: http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf)

*Siebert, Wolfgang* (Hrsg.), Soergel, Bürgerliches Gesetzbuch mit Einführungsgesetz, Band 12: Schuldrecht 10, §§ 823-853, ProdHG, UmweltHG, 13. Aufl., Stuttgart 2005

*Siebert, Wolfgang* (Hrsg.), Soergel, Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Band 14: Sachenrecht 1, §§ 854-984, 13. Aufl., Stuttgart 2002

*Siebert, Wolfgang* (Hrsg.), Soergel, Bürgerliches Gesetzbuch mit Einführungsgesetz, Band 15/1: Sachenrecht 2/1, §§ 985-1017, ErbbauVO, 13. Aufl., Stuttgart 2007

*Simitis, Spiros* (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011

*Simitis, Spiros/Dammann, Ulrich/Geiger, Hansjörg/Mallmann, Otto/Walz, Stefan*, Kommentar zum Bundesdatenschutzgesetz, 4. Aufl., Baden-Baden 1992

*Skistims, Hendrik/Roßnagel, Alexander*, Rechtlicher Schutz vor Staatstrojanern – Verfassungsrechtliche Analyse einer Regierungs-Malware, ZD 2012, S. 3-7

*Sodan, Helge*, Der Anspruch auf Rechtssetzung und seine prozessuale Durchsetzbarkeit, NVwZ 2000, S. 601-609

*Sodan, Helge/Ziekow, Jan*, Grundkurs Öffentliches Recht, Staats- und Verwaltungsrecht, 5. Aufl., München 2012

*Sodtalbers, Axel*, Softwarehaftung im Internet, Frankfurt a. M. 2006

*Spiecker gen. Döhmann, Indra/Eisenbarth, Markus*, Kommt das „Volkszählungsurteil" nun durch den EuGH? – Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon, JZ 2011, S. 169-177

*Spindler, Gerald*, Das Jahr 2000-Problem in der Produkthaftung: Pflichten der Hersteller und der Softwarenutzer, NJW 1999, S. 3737-3745

*Spindler, Gerald*, IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, S. 3145-3150

*Spindler, Gerald*, Haftung und Verantwortlichkeit im IT-Recht – Ein Rück- und Ausblick zu den Bewährungsproben der allgemeinen Grundsätze des Haftungsrechts, CR 2005, S. 741-747

*Spindler, Gerald*, Präzisierungen der Störerhaftung im Internet – Besprechung des BGH-Urteils „Kinderhochstühle im Internet", GRUR 2011, S. 101-108

*Spindler, Gerald/Volkmann, Christian*, Die zivilrechtliche Störerhaftung der Internet-Provider, WRP 2003, 1-15

*Starck, Christian*, Praxis der Verfassungsauslegung I, Baden-Baden 1994

*Starck, Christian*, Verfassungen - Entstehung, Auslegung, Wirkungen und Sicherung, Tübingen 2009

*v. Staudinger, Julius* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 2, Recht der Schuldverhältnisse, §§ 305-310, UKlaG (Recht der Allgemeinen Geschäftsbedingungen), Neubearbeitung 2006 (zit.: Staudinger/*Bearbeiter*)

*v. Staudinger, Julius* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Zweites Buch, Recht der Schuldverhältnisse, §§ 823-825, 13. Bearbeitung 1999, Berlin 1999 (zit.: Staudinger/*Bearbeiter*)

*v. Staudinger, Julius* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 2, Recht der Schuldverhältnisse, §§ 823 E-I, 824, 825 (Unerlaubte Handlungen 1 – Teilband 2), Neubearbeitung 2009, Berlin 2009 (zit.: Staudinger/*Bearbeiter*)

*v. Staudinger, Julius* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 3, Sachenrecht, Einleitung zum Sachenrecht, §§ 854-882 (Allgemeines Liegenschaftsrecht 1), Neubearbeitung 2007, Berlin 2007 (zit.: Staudinger/*Bearbeiter*)

*v. Staudinger, Julius* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 3, Sachenrecht, §§ 985-1011 (Eigentum 3), Neubearbeitung 2006, Berlin 2006 (zit.: Staudinger/*Bearbeiter*)

*Stern, Klaus*, Das Staatsrecht der Bundesrepublik Deutschland, Band I, Grundbegriffe und Grundlagen des Staatsrechts, Strukturprinzipien der Verfassung, 2. Aufl., München 1984

*Stern, Klaus*, Das Staatsrecht der Bundesrepublik Deutschland, Band III/1, Allgemeine Lehren der Grundrechte, München 1988

*Stern, Klaus/Sachs, Michael*, Das Staatsrecht der Bundesrepublik Deutschland, Band III/2, Allgemeine Lehren der Grundrechte, München 1994

*Stoffels, Markus*, AGB-Recht, 2. Aufl., München 2009

*Stögmüller, Thomas*, Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen, CR 2008, S. 435-439

*Streinz, Rudolf*, Europarecht, 9. Aufl., Heidelberg u. a. 2012

*Streinz, Rudolf* (Hrsg.), EUV/AEUV, Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Aufl., München 2012

*Taeger, Jürgen*, Außervertragliche Haftung für fehlerhafte Computerprogramme, Tübingen 1995

*Taeger, Jürgen/Gabel, Detlev* (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Frankfurt a. M. 2010

*Tinnefeld, Marie-Theres*, Die „Staatstrojaner" aus verfassungsrechtlicher Sicht – Gedanken zum Prüfbericht des Bayerischen Landesbeauftragten für den Datenschutz, ZD 2012, S. 451-454

*Tinnefeld, Marie-Theres/Petri, Thomas/Brink, Stefan*, Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz – Eine erste Analyse und Bewertung, MMR 2010, S. 727-735

*Uerpmann-Wittzack, Robert* (Hrsg.), Das neue Computergrundrecht, Berlin 2009

*Ulmer, Peter/Brandner, Hans Erich/Hensen, Horst-Diether* (Hrsg.), AGB-Recht, Kommentar zu den §§ 305-310 BGB und zum UKlaG, 11. Aufl., Köln 2011

*Umbach, Dieter C./Clemens, Thomas* (Hrsg.), Grundgesetz, Mitarbeiterkommentar und Handbuch, Band I, Heidelberg 2002

*Umbach, Dieter C./Clemens, Thomas/Dollinger, Franz-Wilhelm* (Hrsg.), Bundesverfassungsgerichtsgesetz, Mitarbeiterkommentar und Handbuch, 2. Aufl., Heidelberg 2005

*Vogelgesang, Klaus*, Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987

*Volkmann, Uwe*, Anmerkung zum Urteil des BVerfG vom 27.2.2008, 1 BvR 370/07 und 1 BvR 595/07, DVBl. 2008, S. 590-593

*Voßkuhle, Andreas*, Gibt es und wozu nutzt eine Lehre vom Verfassungswandel?, in: *Wahl, Rainer* (Hrsg.), Verfassungsänderung, Verfassungswandel, Verfassungsinterpretation, Berlin 2008

*Voßkuhle, Andreas*, Stabilität, Zukunftsoffenheit und Vielfaltssicherung - Die Pflege des verfassungsrechtlichen „Quellcodes" durch das BVerfG, JZ 2009, 917-924

*Voßkuhle, Andreas/Kaiser, Anna-Bettina*, Grundwissen – Öffentliches Recht: Der Grundrechtseingriff, JuS 2009, S. 313-315

*Wagner, Edgar*, Der Entwurf einer Datenschutz-Grundverordnung der Europäischen Kommission, DuD 2012, S. 676-678

*Walter, Christian*, Hüter oder Wandler der Verfassung? Zur Rolle des Bundesverfassungsgerichts im Prozess des Verfassungswandels, AöR 125 (2000), S. 517-550

*Warntjen, Maximilian*, Die verfassungsrechtlichen Anforderungen an eine gesetzliche Regelung der Online-Durchsuchung, JURA 2007, 581-585

*Wassermann, Rudolf* (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Bd. 1, Art. 1-37, 2. Aufl., Neuwied 1989 (zit. AK-GG-*Bearbeiter*)

*Wedde, Peter*, Das Grundrecht auf Vertraulichkeit und Integrität in informationstechnischen Systemen aus arbeitsrechtlicher Sicht, AuR 2009, S. 373-378

*Wegener, Bernhard W./Muth, Sven*, Das „neue" Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, JURA 2010, S. 847-852

*Weiß, André*, Online-Durchsuchungen im Strafverfahren, Hamburg 2009

*Wenwigk, Ulrich*, Zur Geltung des Richtervorbehalts bei der Durchsuchung von besetzten Häusern, NJW 1983, S. 2366-2368

*Westermann, Harm Peter* (Hrsg.), Erman, Bürgerliches Gesetzbuch, Handkommentar mit AGG, EGBGB (Auszug), ErbbauRG, HausratsVO, LPartG, ProdhaftG, UKlaG, VAHRG und WEG, Bd. I, 12. Aufl., Köln 2008 (zit. Erman/*Bearbeiter*, 12. Aufl.)

*Westermann, Harm Peter/Grunewald/Barbara/Maier-Reimer, Georg* (Hrsg.), Erman, Bürgerliches Gesetzbuch, Handkommentar mit AGG, EGBGB (Auszug), ErbbauRG, LPartG, ProdhaftG, UKlaG, VBVG, VersAusglG und WEG, Bd. I, 13. Aufl., Köln 2011 (zit. Erman/*Bearbeiter*)

*Wichert, Michael*, Web-Cookies – Mythos und Wirklichkeit, DuD 1998, S. 273-276

*Wiebe, Andreas*, Rechtsschutz für Software in den neunziger Jahren, BB 1993, S. 1094-1103

*Wiebe, Andreas*, Anmerkung zu OLG Köln, Urteil vom 2.11.2001 - 6 U 12/01 (LG Köln), CR 2002, S. 53-55

*Wieczorek, Mirko Andreas*, Informationsbasiertes Persönlichkeitsrecht – Überlegungen zur Restauration des Persönlichkeitsschutzes im Internetzeitalter, DuD 2012, S. 476-481

*Wilms, Jan/Roth, Jan*, Die Anwendbarkeit des Rechts auf informationelle Selbstbestimmung auf juristische Personen i. S. v. Art. 19 Abs. 3 GG, JuS 2004, S. 577-580

*Wischermann, Norbert*, Rechtskraft und Bindungswirkung verfassungsgerichtlicher Entscheidungen – Zu den funktionsrechtlichen Auswirkungen des extensiven Auslegung des § 31 Abs. 1 BVerfGG, Berlin 1979

*Wolf, Manfred/Wellenhofer, Marina*, Sachenrecht, 27. Aufl., München 2012

*Wolf, Manfred/Lindacher, Walter F./Pfeiffer, Thomas* (Hrsg.), AGB-Recht, Kommentar, 5. Auf., München 2009

*Wolf, Thomas/Mulert, Gerrit*, Die Zulässigkeit der Überwachung von E-Mail-Korrespondenz am Arbeitsplatz, BB 2008, S. 442-447

*Wuermeling, Ulrich*, Einsatz von Programmsperren, CR 1994, 585-595

*Wybitul, Tim*, Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber, ZD 2011, S. 69-74

In seinem Leiturteil zur sog. Online-Durchsuchung formulierte das Bundesverfassungsgericht im Jahre 2008 erstmals das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das Urteil zog eine enorme Aufmerksamkeit auf sich. Ihm wurde eine dem Volkszählungsurteil vergleichbare Bedeutung für den Datenschutz zugeschrieben. Der genaue Schutzgehalt des Grundrechts blieb jedoch mangels weiterer einschlägiger Rechtsprechung bis heute größtenteils unklar. Die vorliegende Arbeit untersucht und ergänzt daher zunächst die einzelfallbezogenen Ausführungen des Urteils, um den Schutzgehalt des Grundrechts in verallgemeinerungsfähiger Form zu formulieren. Hierbei wird das Grundrecht in den Grundrechtskatalog eingeordnet und seine maßgebliche Funktion als individuelles Abwehrrecht gegen technische Überwachungsmaßnahmen herausgearbeitet. Auf dieser Grundlage basiert die sich anschließende Prüfung, inwieweit der verfassungsrechtliche Schutzgehalt auf das Rechtsverhältnis zwischen Privaten zu übertragen ist.

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

ISBN: 978-3-86395-123-8

Universitätsdrucke Göttingen