FORUM Wirtschaftsrecht - Band 6

Institut für Wirtschaftsrecht

Judith Klink

Datenschutz in der elektronischen Justiz

kassel university press

FORUM Wirtschaftsrecht

Band 6

Herausgegeben vom
Institut für Wirtschaftsrecht an der Universität Kassel

Datenschutz in der elektronischen Justiz

Judith Klink

kassel
university
press

Die vorliegende Arbeit wurde vom Fachbereich Wirtschaftswissenschaften der Universität Kassel als Dissertation zur Erlangung des akademischen Grades eines Doktors der Rechtswissenschaften (Dr. jur.) angenommen.

Erster Gutachter: Prof. Dr. Alexander Roßnagel
Zweiter Gutachter: Prof. Dr. Dr. Walter Blocher

Tag der mündlichen Prüfung 13. Juli 2010

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar

Zugl.: Kassel, Univ., Diss. 2010
ISBN print: 978-3-89958-962-7
ISBN online: 978-3-89958-963-4
URN: http://nbn-resolving.de/urn:nbn:de:0002-9633

© 2010, kassel university press GmbH, Kassel
www.upress.uni-kassel.de

Printed in Germany

Für Tobias

Zusammenfassung

Jüngste Gesetzesänderungen haben zum Ziel, die Justiz der Bundesrepublik Deutschland effizienter und transparenter für den Bürger zu machen. Im Vergleich zum E-Government hat die elektronische Justiz mittlerweile sogar schon eine Vorreiterrolle eingenommen. Die neuen Verfahrensabläufe führen jedoch auch zu neuartigen Herausforderungen für den Datenschutz, die bislang kaum beleuchtet wurden. Aufgabe dieser Dissertation ist es daher, die maßgeblichen Fragestellungen zu identifizieren, zu bewerten und Verbesserungspotentiale aufzuzeigen. Grundlage ist der Literatur- und Gesetzesstand vom April 2010.

Die Untersuchung erfolgt am Beispiel des Bundesgerichtshofs sowie der Oberlandes-, Land- und Amtsgerichte von Rheinland-Pfalz. Die Modernisierungen betreffen vor allem das Zivilverfahren, das Zwangsvollstreckungsverfahren, das Zwangsversteigerungsverfahren, das Insolvenzverfahren, die Grundbuchordnung und das Handelsgesetzbuch, welche in der Arbeit ausführlich betrachtet werden. Es werden jeweils die technischen Neuerungen und deren Bedeutung für den prozessualen Ablauf vorgestellt und aus Sicht des Datenschutzes bewertet. Es zeigt sich dabei, dass insbesondere Veröffentlichungen in Internet-Registern und Internet-Bekanntmachungen sowie Verschlüsselung und qualifizierte elektronische Signaturen relevant sind.

Zweifellos lässt die Elektronisierung die Anforderungen an den Datenschutz steigen. Die Arbeit kommt zu dem Ergebnis, dass neben den bereits vom Gesetzgeber getroffenen Bestimmungen weitere rechtliche und technische Maßnahmen erforderlich sind, um ein den herkömmlichen Verfahren vergleichbares Schutzniveau zu gewährleisten. Insbesondere ist aufgrund der herrschenden Gemengelage eine Vereinheitlichung datenschutzrechtlicher Vorschriften geboten.

Durch den technischen Fortschritt ist die elektronische Justiz dem Datenschutz teilweise enteilt. Die entstandene Lücke sollte sich aber vollständig schließen lassen, wenn den bestehenden einzelnen Ansätzen konsequent gefolgt wird und diese systematisiert werden.

Abstract

Recent law changes aim at making the justice of the Federal Republic of Germany more efficient and more transparent for the citizens. Compared to e-government, e-justice has already taken the lead. But new procedures also imply new types of challenges with respect to data protection, challenges which have hardly been examined so far. The purpose of this thesis is to identify and to assess relevant problems and to show how these problems could be solved.

The evaluation considers the „Bundesgerichtshof“ (Federal Supreme Court of Justice) as well as the „Oberlandesgerichte“ (higher regional courts), the „Landgerichte“ (district courts) and the „Amtsgerichte“ (local courts) of Rhineland-Palatinate. The modernization has a major impact on the „Zivilverfahren“ (civil procedure), the „Zwangsvollstreckungsverfahren“ (execution proceedings), the „Zwangsversteigerungsverfahren“ (compulsory auction proceedings), the „Insolvenzverfahren“ (insolvency proceedings), the „Grundbuchordnung“ (Land Registry Act) and the „Handelsgesetzbuch“ (Code of Commercial Law) all of which are treated in detail in the thesis. Technological improvements and their relevance for the course of the procedure are explained and evaluated showing that, from a data protection perspective, especially publications in Internet registers and Internet announcements as well as encryption and qualified electronic signatures have to be taken into account.

Electronization unquestionably increases the requirements for data protection. The dissertation shows the need for additional legal and technical measures apart from the already existing ones in order to ensure a level of protection comparable to that achieved by conventional procedures. Due to the current mixture of data protection regulations, a standardization of data protection regulations is necessary.

Technical progress in e-justice has data protection partially left behind. It should, however, be possible to close this gap by following and systemizing those individual approaches that already exist.

Vorwort der Herausgeber

Die elektronische Bearbeitung von Geschäftsvorfällen ist eine wesentliche Grundlage für den gegenwärtigen und – noch viel mehr – den künftigen Rechts- und Geschäftsverkehr. Dies gilt ebenso für die Informationsverarbeitung innerhalb der Justiz als auch erst recht für die Verlängerung des Rechts- und Geschäftsverkehrs in die Kommunikation mit der Justiz hinein. Gerade die Justiz ist vielfach durch typisierte und formalisierte Verfahrensabläufe gekennzeichnet, die sich für eine automatisierte Bearbeitung in besonderer Weise eignen. Daher ist die Justiz schon seit langem und vorrangig Gegenstand von Anwendungen der automatisierten Datenverarbeitung.

Zugleich ist aber zu beachten, dass in der Justiz besondere Bedingungen herrschen, an die die Datenverarbeitung angepasst werden muss. Zum einen darf die Abhängigkeit von technischen Abläufen nicht die Unabhängigkeit der Justiz gefährden. Zum anderen muss in der Kommunikation mit den Rechtssuchenden einerseits die Rechtssicherheit von Prozesshandlungen gewährleistet werden, andererseits aber dürfen der Rechtsgewährleistung keine zu hohen formalen Hürden entgegengestellt werden. In diesem Konflikt ist ein notwendiger, aber schwieriger Ausgleich zu finden.

Die Justiz ist ein hoch regulierter Bereich, in dem die Einführung automatisierter Datenverarbeitung immer wieder neuer oder angepasster gesetzlicher Regelungen bedarf. Diese sind auch notwendig, um Unabhängigkeit, Rechtssicherheit und Rechtsgewährleistung sicherzustellen und diese Anforderungen gegeneinander und gegenüber dem Effizienzbestreben auszugleichen. Der Gesetzgeber hat schon früh entsprechende Regelungen getroffen und bis heute durch vielfältige Novellierungen der Justizgesetze die elektronische Justiz forciert.

Bei dieser rasanten Umformung der Justizabläufe darf allerdings die informationelle Selbstbestimmung aller Beteiligten nicht vernachlässigt werden. In den justiziellen Verfahren werden immer personenbezogene Daten verarbeitet, die vielfach eine hohe Sensitivität aufweisen. Auch hier gilt es, widersprechende Zielsetzungen zum Ausgleich zu bringen: Datenschutz, Akten- und Mandatsgeheimnis einerseits und Öffentlichkeit der Verfahren und Register andererseits.

Hier setzt die Arbeit von Frau Klink an. Sie untersucht die sich aus der Anwendung von elektronischen Verfahrensabläufen ergebenden datenschutzrechtlichen Fragestellungen im Zivilverfahren, in der Zwangsvollstreckung, in der Zwangsversteigerung, im Insolvenzverfahren, im Grundbuchverfahren und im Handelsregister. Hierfür fehlt es bisher an einer aktuellen umfassenden oder gar monographischen rechtswissenschaftlichen Untersuchung, die zusammenhängend die gemeinsamen Datenschutzfragen dieser verschiedenen Gerichtsverfahren zum Gegenstand hätte. Mit der vorgelegten Arbeit füllt Frau Klink daher eine Lücke in der Rechtswissenschaft des elektronischen Rechtsverkehrs.

Die Analyse der Herausforderungen für die informationelle Selbstbestimmung in den Datenverarbeitungsprozessen der Justiz und die Erarbeitung von Vorschlägen zu ihrer datenschutzgerechten Gestaltung sind gleichermaßen praktisch wie methodisch hochrelevante Herausforde-

rungen einer interdisziplinär orientierten Rechtswissenschaft. Indem die Arbeit zeigt, welche Risiken für das Grundrecht auf informationelle Selbstbestimmung die Justizverfahren beinhalten und in welcher Weise die geltenden Rechtsregeln diesen Risiken begegnen, leistet sie einen wertvollen Beitrag zur Rechtsdogmatik der Justizgesetze wie der Datenschutzregelungen. Indem sie die geltenden Regelungen und die auf ihnen beruhenden Verfahren bewertet und Vorschläge für den praktischen Datenschutz und die Rechtsfortbildung entwickelt, liefert sie einen wichtigen Beitrag sowohl für die Rechtspolitik als auch für die Justizpraxis.

Im Ergebnis wird zum einen die geltende Rechtslage für den Datenschutz in der elektronischen Justiz in den wichtigsten Verfahrensordnungen umfassend, systematisch und detailliert untersucht. Zum anderen enthält die Arbeit konstruktive Vorschläge sowohl für die technisch-organisatorische Gestaltung elektronischer Justizverfahren, die Defizite und Risiken aus Sicht des Rechts auf informationelle Selbstbestimmung beseitigen können, als auch zur Rechtsfortbildung für die datenschutzgerechte Regelung der elektronischen Justiz. Drittens hat Frau Klink in methodischer Hinsicht exemplarisch gezeigt, dass und wie sich aus den generellen Interessensbewertungen und Lösungsmodellen der Verfassung und gesetzlicher Regelungen Gestaltungsziele für die Gewährleistung des Datenschutzes in der elektronischen Justiz entwickeln lassen. Insgesamt zeigt die Arbeit, dass in der elektronischen Justiz die Herausforderungen des Datenschutzes erkannt und berücksichtigt werden, dass aber Verbesserungen notwendig und möglich sind und wie eine verbesserte datenschutzadäquate Gestaltung der elektronischen Justiz aussehen kann.

Es ist der Arbeit zu wünschen, dass sie von den verantwortlichen Personen in Politik, Ministerialverwaltung und Justiz zur Kenntnis genommen und in der weiteren Entwicklung der elektronischen Justiz berücksichtigt wird.

Für die Herausgeber
Kassel, im Juli 2010 *Alexander Roßnagel*

Vorwort der Autorin

Die Idee zu der vorliegenden Dissertation entstand im Rahmen der Tätigkeit der Autorin bei der Behörde des Landesbeauftragten für den Datenschutz Rheinland-Pfalz. Von den vielen Bürgern, die sich an den Beauftragten wenden, werden immer wieder auch Anfragen zu Verfahren gestellt, bei denen sich die Justiz neuer Technologien bedient. Konkret bezogen sich in der Vergangenheit Anfragen darauf, dass nach der Einstellung eines Insolvenzverfahrens Angaben von Amtsgerichten im Internet nicht gelöscht werden sowie auf die Veröffentlichung von Wertgutachten in Zwangsversteigerungsverfahren durch private Anbieter.

Aufgrund der Sensibilität der Daten, die in der Justiz täglich verarbeitet werden, lag daher für mich als Richterin die Frage nahe, ob der Gesetzgeber datenschutzrechtliche Aspekte bei der Elektronisierung und Modernisierung hinlänglich berücksichtigt hat. Ich bin froh, dass ich mit Herrn Prof. Dr. Alexander Roßnagel einen Spezialisten auf dem Gebiet des Datenschutzrechts für die Betreuung meiner Arbeit gewinnen konnte. Ihm gebührt mein größter Dank für die wertvollen Gespräche und seine fachlichen Inspirationen – insbesondere aber auch für seine stets sympathische und hilfsbereite Art. Herrn Prof. Dr. Dr. Walter Blocher danke ich dafür, dass er freundlicherweise das Zweitgutachten übernommen hat.

Diese Arbeit wäre nicht entstanden ohne meine Abordnung zum Landesdatenschutzbeauftragten Herrn Edgar Wagner, die er und das Ministerium der Justiz mir ermöglicht hatten. In dem hochinteressanten Umfeld der Behörde mit ihren breit gefächerten Fragestellungen konnte ich wertvolle Erfahrungen sammeln. Herrn Wagner persönlich danke ich für seine fortwährend herzliche Art und die bereichernden Gespräche zu rechtspolitischen und praktischen Aspekten des Datenschutzes. Von den ehemaligen Kollegen, die zum guten Arbeitsklima beigetragen haben, möchte ich Frau Judith Hartig und Herrn Helmut Eiermann hervorheben und ihnen für die Zusammenarbeit bei der Neufassung des gemeinsamen Kommentars zum Landesdatenschutzgesetz danken.

Vor allem aber danke ich meinem Mann Tobias für seine Geduld, seine Zuversicht und seine Hilfsbereitschaft während der gesamten Dauer der Arbeit. Ihm widme ich diese Dissertation.

Judith Klink

Inhaltsverzeichnis

Verzeichnis der Abkürzungen

ABl. EG	Amtsblatt der EG
ADD	Aufsichts- und Dienstleistungsdirektion
AfP	Archiv für Presserecht
AiB	Arbeitsrecht im Betrieb
AnwBl	Anwaltsblatt
Art.	Artikel
BArchVG	Bundesarchivgesetz
BayDSG	Bayerisches Datenschutzgesetz
BB	Betriebs-Berater
BbDSG	Brandenburgisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
BDVR-Rundschreiben	Rundschreiben des Bundes deutscher Verwaltungsrichterinnen und Verwaltungsrichter
BeurkG	Beurkundungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BInDSG	Berliner Datenschutzgesetz
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Technologie
BNotO	Bundesnotarordnung
BPG-E	Entwurf eines Bürgerportalgesetzes
BRAK-Mitt.	Bundesrechtsanwaltskammer-Mitteilungen
BRAO	Bundesrechtsanwaltsordnung
BremDSG	Bremisches Datenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnologie
BVBl.	Bundesversorgungsblatt
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BWV	Bundeswehrverwaltung
c't	Magazin für Computertechnik
CR	Computer und Recht

CRi	Computer und Recht International
DB	Der Betrieb
dbr	der betriebsrat
DGVZ	Deutsche Gerichtsvollzieherzeitung
DNotZ	Deutsche Notar-Zeitschrift
DONot	Dienstordnung für Notare
DRiG	Deutsches Richtergesetz
DRiZ	Deutscher Richterbund
DSB	Datenschutzbeauftragter
DSG M.-V.	Datenschutzgesetz Mecklenburg-Vorpommern
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DSG-LSA	Datenschutzgesetz Sachsen-Anhalt
DSRL	Datenschutzrichtlinie
DStR	Deutsches Steuerrecht
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
DVR	Datenverarbeitung im Recht
DZWIR	Deutsche Zeitschrift für Wirtschafts- und Insolvenzrecht
DÖV	Die öffentliche Verwaltung
E-Government	Electronic Government
EDV	Elektronische Datenverarbeitung
EEAR	Europäische EDV-Akademie des Rechts
EGSRL	Signaturrichtlinie
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EHUG	Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
eJustice	Electronic Justice
ELENA	Elektronischer Entgeltnachweis
ELENA-Verfahrensgesetz	Gesetz über das Verfahren des elektronischen Entgeltnachweises
ERJuKoG	Gesetz über elektronische Register und Justizkosten für Telekommunikation
ERVGBG	Gesetz zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Akte im Grundbuchverfahren sowie zur Änderung weiterer grundbuch-, register- und kostenrechtlicher Vorschriften
EU	Europäische Union
EuR	Europa und Recht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWiR	Entscheidungen zum Wirtschaftsrecht
FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit

FormVAnpG	Formvorschriftenanpassungsgesetz
FTP	File Transfer Protocol
GBAbVfG	Verordnung über Grundbuchabrufverfahrensgebühren
GG	Grundgesetz
gGmbH	Gemeinnützige GmbH
GmbHR	GmbH-Rundschau
GmS-OGB	Gemeinsamer Senat der obersten Gerichtshöfe des Bundes
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GVBl.	Gesetz- und Verordnungsblatt
GVG	Gerichtsverfassungsgesetz
GVNRW	Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen
GVOBl.	Gesetz- und Verordnungsblatt
HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
HmbDSG	Hamburgisches Datenschutzgesetz
HmbGVBl	Hamburgisches Gesetz- und Verordnungsblatt
HRV	Handelsregisterverordnung
i'X	Magazin für professionelle Informationstechnik
IFG	Informationsfreiheitsgesetz
IHK	Industrie- und Handelskammer
IMAP	Internet Message Access Protocol
Information StW	Die Information für Steuerberater und Wirtschaftsprüfer
InsbürO	Zeitschrift für das Insolvenzbüro
InsO	Insolvenzordnung
InsO-Änderungsgesetz	Gesetz zur Änderung der Insolvenzordnung und anderer Gesetze
InsoBekV	Insolvenzbekanntmachungsverordnung
InsVerfVereinfG	Gesetz zur Vereinfachung des Insolvenzverfahrens
IntVerstZVG	Gesetz über die Internetversteigerung in der Zwangsvollstreckung und zur Änderung anderer Gesetze
IP	Internet Protocol
IT	Informationstechnologie
ITSG-GmbH	Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH
IuKDG	Informations- und Kommunikationsdienstegesetz
JA	Juristische Arbeitsblätter
JKomG	Justizkommunikationsgesetz
Jura	Jura (Ausbildungszeitschrift)
JurBüro	Das Juristische Büro
JurPC	Jur-PC
JuS	Juristische Schulung
JustizModG	Gesetz zur Modernisierung der Justiz

JVKostO	Justizverwaltungskostenordnung
JZ	Juristenzeitung
KJ	Kritische Justiz
KKZ	Kommunal-Kassen-Zeitschrift
K&R	Kommunikation und Recht
LAN	Local Area Network
LBG	Landesbeamtengesetz
LDSG	Landesdatenschutzgesetz
LSchrAG	Landesschriftgutaufbewahrungsgesetz
LV	Landesverfassung
MDR	Monatsschrift für Deutsches Recht
MiStra	Mitteilungen in Strafsachen
MittBayNot	Mitteilungen des Bayerischen Notarvereins, der Notarkasse und der Landesnotarkammer Bayern
MiZi	Mitteilungen in Zivilsachen
MMR	MultiMedia und Recht
NDSG	Niedersächsiches Datenschutzgesetz
NJ	Neue Justiz
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
NZI	Neue Zeitschrift für Insolvenzrecht und Sanierung
PAuswG	Personalausweisgesetz
PersR	Der Personalrat
PersV	Die Personalvertretung
PKH	Prozesskostenhilfe
POP	Post Office Protocol
PostG	Postgesetz
PStR	Praxis Steuerstrafrecht
Rbeistand	Der Rechtsbeistand
RDV	Recht der Datenverarbeitung
RegE	Regierungsentwurf
RegVBG	Registerverfahrensbeschleunigungsgesetz
RFID	Radio Frequency Identification
Rpfleger	Der Deutsche Rechtspfleger
RpflStud	Rechtspfleger Studienhefte
RVKG	Registrierungsverzeichnis für Kommunikationsdienste
S.A.F.E.	Secure Access to Federated eJustice/eGovernment
SchlHA	Schleswig-Holsteinische Anzeigen
SchrAG	Schriftgutaufbewahrungsgesetz

Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SchuVVO	Schuldnerverzeichnisverordnung
SDSG	Sächsisches Datenschutzgesetz
SigG	Signaturgesetz
SigV	Signaturverordnung
sj	steuer-journal.de
SMTP	Simple Mail Transfer Protocol
SozSich	Soziale Sicherheit
StGB	Strafgesetzbuch
StV	Strafverteidiger
SächsDSG	Sächsisches Datenschutzgesetz
TCP	Transmission Control Protocol
ThürDSG	Thüringer Datenschutzgesetz
TKMR	Telekommunikations- und Medienrecht
TMG	Telemediengesetz
UDP	User Datagramm Protocol
UPR	Umwelt und Planungsrecht
URL	Uniform Resource Locator
VwVfG	Verwaltungsverfahrensgesetz
VwZG	Verwaltungszustellungsgesetz
WLAN	Wireless Local Area Network
WpHG	Gesetz über den Wertpapierhandel
WRP	Wettbewerb in Recht und Praxis
ZEV	Zeitschrift für Erbrecht und Vermögensnachfolge
ZfIR	Zeitschrift für Immobilienrecht
ZInsO	Zeitschrift für das gesamte Insolvenzrecht
ZIP	Zeitschrift für Wirtschaftsrecht
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZSR	Zentrales Schutzschriftenregister
ZustRG	Zustellungsreformgesetz
ZVG	Zwangsversteigerungsgesetz
ZVI	Zeitschrift für Vermögens- und Immobilienrecht
ZwVollStrÄndG	Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung
ZZP	Zeitschrift für Zivilprozeß

Kapitel 1

Einleitung

1.1 Problemaufriss und Stand der Forschung

Die Justiz hat im Vergleich zur behördlichen Verwaltung im Modernisierungsprozess eine Vorreiterrolle eingenommen.[1] Der Gesetzgeber hat gerade im justiziellen Bereich eine ganze Reihe von Vorschriften erlassen, die eine Elektronisierung von Verfahrensabläufen beinhalten. Dies trifft vor allem auf das Zivilverfahren, die Zwangsvollstreckung, die Zwangsversteigerung, das Insolvenzverfahren und die freiwillige Gerichtsbarkeit zu. Zu nennen sind hier etwa das Registerverfahrensbeschleunigungsgesetz[2] (RegVBG) aus dem Jahr 1993, das Formvorschriftenanpassungsgesetz[3] (FormVAnpG) und das Zustellungsreformgesetz[4] (ZustRG) aus dem Jahr 2001, das Justizkommunikationsgesetz[5] (JKomG) aus dem Jahr 2005, das Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister[6] (EHUG) aus dem Jahr 2007, das Gesetz zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Akte im Grundbuchverfahren sowie zur Änderung weiterer grundbuch-, register- und kostenrechtlicher Vorschriften[7] aus dem Jahr 2009 (ERVGBG) sowie das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung[8] (ZwVollStrÄndG), ebenfalls aus dem Jahr 2009 stammend.

---

1 *Britz*, DVBl 2007, 994 mit Verweis auf eine Rede der damaligen Justizministerin Zypries auf der Messe CeBIT am 15.3.2007.

2 BGBl. 1993 I, 2182.

3 BGBl. 2001 I, 1542.

4 BGBl. 2001 I, 3138.

5 BGBl. 2005 I, 837.

6 BGBl. 2006 I, 2553.

7 BGBl. 2009 I, 2713.

8 BGBl. 2009 I, 2258. Zum Inkrafttreten der wesentlichen Regelungen ab dem 1.1.2013 vgl. allerdings Art. 6. Die Regelungen, die bereits beschlossen, jedoch noch nicht in Kraft getreten sind, werden in dieser Arbeit mit „neu“ gekennzeichnet.

Sicherlich haben die Elektronisierungsbestrebungen der Justiz viele Vorteile.[9] So ist es komfortabel, per Internet zu prüfen, ob eine Person im Schuldnerverzeichnis eingetragen ist. Dies spart Zeit verglichen mit dem Gang zum Amtsgericht. Auch ist es bequemer, eine elektronische Akte vom eigenen Rechner aus einzusehen, als diese per Post anzufordern oder sich gar zur Geschäftsstelle begeben zu müssen. Wer kennt aber die Identität der abrufenden Person? Wer weiß, ob diese zum Abruf berechtigt ist? Wer kann sich sicher sein, dass das elektronische Dokument an den richtigen Anwalt zugestellt wird? Wer kann gewährleisten, dass die Daten von Internetbekanntmachungen im Insolvenzverfahren nicht massenweise heruntergeladen und nach Ablauf der amtlichen Löschfrist weiter im Internet zu finden sind?[10] Nur wenn die Elektronisierungsprozesse in der Justiz auch das Recht auf informationelle Selbstbestimmung und das neue Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme hinreichend beachten, werden diese langfristig erfolgreich sein und das Vertrauen der Bürger gewinnen.

Deshalb beschäftigt sich diese Dissertation mit dem Datenschutz in der elektronischen Justiz.[11] Sie untersucht die sich aus der Anwendung von elektronischen Verfahrensabläufen ergebenden datenschutzrechtlichen Fragestellungen im Zivilverfahren, der Zwangsvollstreckung, der Zwangsversteigerung, dem Insolvenzverfahren, dem Grundbuchverfahren und dem Handelsgesetzbuch. Dagegen ist das Strafprozessrecht nicht Gegenstand der Betrachtung. Die Untersuchung wird am Beispiel des Bundesgerichtshofes, der Oberlandesgerichte und der Land- und Amtsgerichte von Rheinland-Pfalz vorgenommen.

Die Literatur hat sich mit den sich aus der Elektronisierung dieser Verfahrensabläufe ergebenden datenschutzrechtlichen Problemen bisher kaum auseinandergesetzt.

Eine Dissertation zu diesem Thema stammt von Marcus Werner.[12] Der Titel der Arbeit lautet „Untersuchungen zum Datenschutz und zur Datensicherung bei der Anwendung Elektronischer Datenverarbeitung im Zivilprozeß“. Diese Arbeit stammt allerdings von 1994. Sie berücksichtigt daher nicht Änderungen in der Zivilprozessordnung (ZPO), die etwa durch das Formvorschriftenanpassungsgesetz 2001, das Zustellungsreformgesetz 2001 und das Justizkommunikationsgesetz 2005 entstanden sind. Außerdem betrachtet sie den Datenschutz ausschließlich im Zivilverfahren.

Aus dem gleichen Jahr stammt eine Dissertation von Brigitta Liebscher.[13] Ihr Titel lautet „Datenschutz bei der Datenübermittlung im Zivilverfahren“. Die Autorin versteht den Begriff des Zivilverfahrens weit und untersucht den Datenschutz daher auch im Vollstreckungsverfahren

---

9 Vgl. hierzu etwa *Viefhues/Volesky*, TKMR 2003, 245 f.; *Krüger/Bütter*, MDR 2003, 182 oder *Schwoerer*, 2005, 27 ff.

10 Vgl. zu dieser Problematik *Bundesregierung*, BT-Drs. 15/181.

11 Statt elektronischer Justiz wird gelegentlich auch der englische Begriff Electronic Justice (E-Justice; auch eJustice geschrieben) synonym verwendet. Die vorliegende Arbeit gebraucht jedoch ausschließlich den deutschen Begriff elektronische Justiz. Zur besseren Lesbarkeit wird bei Überschriften zudem „elektronisch(e)“ durch „E-“ ersetzt.

12 *Werner*, 1995.

13 *Liebscher*, 1994.

und in der freiwilligen Gerichtsbarkeit. Allerdings beschränkt sich die Arbeit auf den Teilaspekt der Datenübermittlung. Der Datenschutz im internen Bereich bei den Gerichten wird zum Beispiel nicht beleuchtet. Die Dissertation berücksichtigt zudem ebenfalls nicht wichtige Änderungen in der ZPO und im Registerrecht.

Die Dissertation von Gabriele Straub mit dem Titel „Das Schuldnerverzeichnis unter besonderer Berücksichtigung des Datenschutzes“ stammt aus dem Jahr 1995.[14] Sie beleuchtet den Datenschutz ausschließlich in einem ganz speziellen Gebiet, nämlich dem der Schuldnerverzeichnisse. In diesem prüft sie die Vereinbarkeit des informationellen Selbstbestimmungsrechts mit dem bislang noch papiergebunden geführten Schuldnerverzeichnis. Mit dem Gesetz zur Reform in der Sachaufklärung wurde die Einführung eines Internet-Schuldnerverzeichnisses beschlossen. Die sich damit ergebenden neuen datenschutzrechtlichen Fragestellungen werden in der Arbeit nicht thematisiert.

Weitere Dissertationen oder andere Buchpublikationen zu diesem Thema gibt es – soweit ersichtlich – nicht. Auch die Aufsätze, die sich mit dem Datenschutz in den genannten Verfahrensordnungen befassen, sind rar:

Prütting zum Beispiel beschäftigt sich in einem Aufsatz „Datenschutz und Zivilverfahren in Deutschland“ mit dem Verhältnis der Datenschutzgesetze zum Zivilprozess und beleuchtet das Spannungsverhältnis der Verfahrensgrundsätze zum Datenschutz.[15] Auch geht er auf datenschutzrechtliche Probleme im Registerrecht ein. Da die Arbeit aus dem Jahr 1993 stammt, berücksichtigt sie jedoch nicht die durch die oben genannten Gesetze erfolgten Änderungen in den Verfahrensordnungen.

Marcus Werner beleuchtet im „Handbuch Datenschutzrecht“, herausgegeben von Alexander Roßnagel, im Jahr 2003 in einem Aufsatz “Datenschutz im Zivil- und Verwaltungsprozess“ den Rechtsrahmen des Datenschutzes in diesen Gerichtsverfahren.[16] Gegenstand des Aufsatzes ist aber nicht das Mahn- und Vollstreckungsverfahren. Zudem ist der Aufsatz im Hinblick auf die Änderungen in der ZPO nicht mehr aktuell. Auch Marcus Werner erkennt die Forschungslücke der Thematik des Datenschutzes in der Rechtspflege, wenn er schreibt: „Trotz der Brisanz der Problematik gibt es nur sehr vereinzelt Urteile und nur wenig einschlägige Literatur zum Thema des Datenschutzes im Zivil- und Verwaltungsprozess.“[17]

Dietmar Wullweber setzt sich in dem Praxishandbuch „Datenschutz in Anwaltschaft, Notariat und Justiz“ mit dem Aufsatz „Datenschutz im Zivilprozess einschließlich der Verfahren der freiwilligen Gerichtsbarkeit“ auch mit dem Datenschutz in der Rechtspflege in den hier zu untersuchenden Bereichen auseinander.[18] Der Beitrag stammt jedoch aus dem Jahr 2003 und ist ebenfalls nicht mehr aktuell. Wie oben dargelegt, stammt etwa das Justizkommu-

14 *Straub*, 1995.
15 *Prütting*, ZZP 1993, 427.
16 *Werner*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 1419.
17 *Werner*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 1420.
18 *Wullweber*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 157.

nikationsgesetz aus dem Jahr 2005 oder das Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister aus dem Jahr 2007.

Hendrik Schöttle setzt sich in einem Beitrag in dem Kommentar und Handbuch „Elektronischer Rechtsverkehr“ aus dem Jahr 2006 mit dem Datenschutz im elektronischen Rechtsverkehr auseinander.[19] Dieser Beitrag stellt lediglich einen Überblicksaufsatz dar. So werden der Rechtsrahmen und die verschiedenen Rechte und Pflichten im Datenschutzrecht allgemein erörtert. Der Beitrag untersucht jedoch nicht spezielle datenschutzrechtliche Probleme in den hier in Rede stehenden Verfahrensordnungen.

Darüber hinaus gibt es noch Aufsätze, die Einzelaspekte im Datenschutz in der Justiz ansprechen. Helmut Bäumler und Christine Nordmann etwa beschäftigen sich in einem Beitrag zum o.g. Praxishandbuch mit dem gerichtlichen Datenschutzbeauftragten,[20] Ulrich Vultejus beleuchtet in einem kurzen Beitrag das Datengeheimnis des Richters[21]. Werner Schmidt widmet sich den Grenzen datenschutzrechtlicher Kontrolle in der Rechtspflege am Beispiel des Landes Rheinland-Pfalz.[22]

Eine Gesamtdarstellung des Datenschutzes in der Justiz, die die jüngsten Modernisierungsprozesse im Zivilverfahren, der Zwangsvollstreckung, der Zwangsversteigerung, dem Insolvenzverfahren, dem Grundbuchverfahren und dem Handelsgesetzbuch nach den erfolgten Gesetzesänderungen berücksichtigt, gibt es jedoch nicht.

In der Literatur wurde der Datenschutz im Electronic Government (E-Government) bereits ausreichend beleuchtet. Nuriye Yildirim hat in einer Dissertation aus dem Jahr 2004 die datenschutzrechtlichen Problemstellungen im E-Government detailliert herausgearbeitet und praktische Gestaltungsmöglichkeiten für ein datenschutzgerechtes E-Government entwickelt.[23] In ihrer Dissertation ging sie von einem engen Verständnis von E-Government aus, d.h sie sah nur Modernisierungsformen der behördlichen Verwaltung als von diesem Begriff umfasst an. Folglich musste sie sich mit dem Modernisierungsprozess in der Justiz nicht auseinandersetzen. Dies trifft weitgehend auch auf die weiteren in der Literatur zu findenden Zeitschriften-, Buchpublikationen oder sonstigen Veröffentlichungen zum Datenschutz im E-Government zu.[24] Die zum Datenschutz im E-Government gefundenen Ergebnisse können jedoch – wie sich noch zeigen wird – wegen des in Art. 20 Abs. 3 Grundgesetz (GG) verankerten Gewaltenteilungsprinzips nicht ohne weiteres auf die elektronische Justiz übertragen werden.

---

19 *Schöttle*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 176.
20 *Bäumler/Nordmann*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 129.
21 *Vultejus*, ZRP 1996, 329.
22 *Schmidt*, RDV 1995, 215.
23 *Yildirim*, 2004.
24 Vgl. zum Beispiel *DSB-Konferenz*, 2003.

1.2 Ziel und Gliederung der Arbeit

Die vorliegende Arbeit will die beschriebene Forschungslücke schließen und in einer Gesamtbetrachtung die für die elektronische Justiz maßgeblichen datenschutzrechtlichen Fragestellungen identifizieren, bewerten und nötigenfalls Verbesserungsvorschläge aufzeigen.

Die Arbeit gliedert sich in drei Teile.

Im ersten Teil werden die Grundlagen dargestellt. Dabei werden zuerst die relevanten Begriffe eingeführt. Der Begriff der elektronischen Justiz wird von den Begriffen des E-Government, des elektronischen Rechtsverkehrs und des elektronischen Geschäftsverkehrs abgegrenzt. In diesem Zusammenhang wird vor allem der Frage nachgegangen, ob es eines eigenständigen Begriffs für Modernisierungsformen der Justiz bedarf. Anschließend werden die Ziele dargestellt, die mit der Elektronisierung der Justiz verbunden sind. Sodann wird aufgezeigt, dass die Elektronisierungsziele sowohl in der rechtlichen Verankerung als auch in der tatsächlichen Realisierung Spuren hinterlassen haben. Hier wird die Rechtsentwicklung in den zu untersuchenden Bereichen dargestellt und die tatsächliche Situation am Beispiel des Bundesgerichtshofes und der ordentlichen Gerichtsbarkeit in Rheinland-Pfalz vorgestellt. Schließlich wird untersucht, welche Herausforderungen der Einsatz von modernen Informationstechniken an den Datenschutz stellt. Zunächst wird aufgezeigt, welche personenbezogenen Daten in der elektronischen Justiz überhaupt anfallen, um die Gefährdungen für die in den einzelnen Verfahrensordnungen anfallenden Inhaltsdaten zu erörtern.

Der zweite Teil der Arbeit widmet sich dem Rechtsrahmen, beginnend mit den rechtlichen Grundlagen im EU-Recht. Dann werden die verfassungsrechtlichen Grundlagen herausgearbeitet. Sodann wird aufgezeigt, dass der Umgang mit Daten in der Justiz nicht durch eine geschlossene Kodifikation bestimmt ist, sondern dass vielmehr unterschiedliche Rechtsquellen zusammenwirken. Zunächst werden das Bundesdatenschutzgesetz (BDSG) und das Landesdatenschutzgesetz (LDSG) Rheinland-Pfalz vorgestellt. Dabei wird vor allem der Anwendungsbereich für Gerichte, Rechtsanwälte, Parteien und Verfahrensbeteiligte bestimmt. Des Weiteren werden die für die Justiz bedeutsamen bereichsspezifischen Gesetze, nämlich das Justizmitteilungsgesetz und das Schriftgutaufbewahrungsgesetz, näher beschrieben. Schließlich werden die Gesetze vorgestellt, die für die Datensicherheit in der elektronischen Justiz von Bedeutung sind oder werden können. Hierzu gehören das Signaturgesetz (SigG)und das Personalausweisgesetz (PAuswG). An dieser Stelle wird auch auf den Entwurf eines Bürgerportalgesetzes (BPG-E) eingegangen. Im Folgenden werden datenschutzrechtliche Anforderungen nach dem BDSG und dem LDSG aus rechtlicher und technisch-organisatorischer Sicht formuliert. Schließlich wird die Thematik Datenschutzkontrolle v.a. im Hinblick auf das Verhältnis zur richterlichen Unabhängigkeit diskutiert.

Die gewonnenen Ergebnisse werden nun in Teil III dazu genutzt, die Datenschutzprobleme in den zu untersuchenden Bereichen aufzuzeigen und Lösungsmöglichkeiten zu finden. Die Untersuchung folgt spiegelbildlich zu den in Teil I bereits vorgestellten technischen Verfahren. Sie ist bewusst in die Zukunft gerichtet. So werden zum Beispiel die zum 1.1.2013 in Kraft

tretenden Änderungen durch das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung genauso betrachtet und bewertet wie etwaige Überlegungen, das ELENA-Verfahren mit dem Prozesskostenhilfeverfahren zu verbinden. Die Untersuchung in Teil III folgt jeweils einem einheitlichen Aufbau. Zunächst wird der prozessuale Ablauf vorgestellt und sodann werden Verbesserungsvorschläge unterbreitet. Im Zivilverfahren stehen dabei – auch beispielhaft für die anderen Verfahrensordnungen – v.a. Maßnahmen der Datensicherheit im Vordergrund. So wird etwa für die einzelnen Verfahrensschritte geprüft, inwieweit der Einsatz von Verschlüsselungstechniken oder der Einsatz von qualifizierten elektronischen Signaturen für die Durchführung eines rechtssicheren Zivilprozesses erforderlich sind. An dieser Stelle wird auch untersucht, inwieweit neue Erscheinungsformen wie etwa der elektronische Personalausweis[25] oder die Bürgerportale[26] für den Datenschutz in der elektronischen Justiz einen Gewinn bringen können. In den anderen Verfahrensordnungen spielen vor allem die verschiedenen bereits existierenden oder künftigen Internet-Register eine bedeutende Rolle. In diesem Zusammenhang werden die für die verschiedenen Register maßgeblichen unterschiedlichen Gründe für eine hohe Publizität jeweils herausgearbeitet und das Spannungsverhältnis zum informationellen Selbstbestimmungsrecht beleuchtet. Es wird sodann geprüft, ob und warum der Gesetzgeber bestimmte Register als unbeschränkt oder beschränkt einsehbare Register ausgestaltet hat und inwieweit etwaige Beschränkungen durch das Internet als Veröffentlichungsmedium faktisch eine Änderung erfahren haben.

[25] Vgl. hierzu etwa *Roßnagel/Hornung/Schnabel*, DuD 2008, 168.
[26] Vgl. hierzu etwa *Stach*, DuD 2008, 184.

Teil I

Grundlagen

Kapitel 2

Elektronische Justiz: Begriff, Ziele, Entwicklung

2.1 Begriff

Um den Datenschutz speziell in der elektronischen Justiz zu beleuchten, muss zunächst geklärt werden, was hierunter zu verstehen ist. Allgemein versteht man unter dem Begriff elektronische Justiz den Einsatz von Verfahren der Informations- und Kommunikationstechnik innerhalb der Justiz und zwischen Organen der Justiz, der öffentlichen Verwaltung und Privatpersonen.[27] Es ist dabei abzugrenzen zum E-Government,[28] dem elektronischen Rechtsverkehr und dem elektronischen Geschäftsverkehr.

2.1.1 Abgrenzung zum E-Government

Im Jahr 2000 hat sich die Speyerer Definition von E-Government herausgebildet. Demnach beschreibt E-Government die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien.[29] Ungefähr zur gleichen Zeit wurde von der Gesellschaft für Informatik eine eigene Definition veröffentlicht. In dem sog. Electronic-Government Memorandum wird unter E-Government die Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung und der Leistungserstellung in Politik, Staat und Verwaltung verstanden.[30] Die Unterschiede zwischen den beiden Definitionen bestehen darin, dass die Speyerer Definition E-Government nur auf Geschäftsprozesse der Verwaltung, d.h. das normale Verwaltungshan-

[27] *Berlit*, JurPC Web-Dok. 2007, Abs. 1.

[28] Der Begriff des E-Government darf nicht mit dem des E-Governance verwechselt werden. E-Governance bezeichnet die Gestaltung der Rahmenbedingungen der Informationsgesellschaft von staatlicher wie auch von privater Seite. E-Government wird dementsprechend als die Umsetzung konkreter Anwendungen innerhalb der so geschaffenen Rahmenbedingungen verstanden, vgl. hierzu *König*, DÖV 2001, 617.

[29] *von Lucke/Reinermann*, 2000, 1.

[30] *GI*, 2000, 3.

deln auf kommunaler, Landes- und Bundesebene, bezieht.[31] Im Electronic-Government Memorandum werden hingegen auch die demokratischen Willensbildungsprozesse als Teil von E-Government begriffen.[32] Beide Definitionen umfassen in ihrer Bedeutung jedoch nicht Modernisierungsformen der Justiz als dritte Gewalt. Sie gehen deshalb von einem engen Verständnis von E-Government aus. Andere verstehen den Begriff des E-Government weiter. Danach stellt der Begriff des E-Government einen Oberbegriff dar für moderne Kommunikationsformen im gesamten öffentlichen Sektor, mithin in Legislative, Exekutive und Judikative. In dieser Bedeutung wird „E-Government in der Justiz“ mit dem Begriff der elektronischen Justiz gleichgesetzt.[33]

In dieser Arbeit wird von einem engen Verständnis von E-Government ausgegangen. Zwar gab es in der Vergangenheit schon Vorhaben, die als E-Government Projekte bezeichnet wurden und auch den Einsatz von Informationstechnologie (IT) in der Justiz vorsahen. So waren etwa vom Projekt BundOnline 2005 etliche IT-Dienstleistungen der Justiz umfasst.[34] Die Justiz ist jedoch nicht Teil des politisch-administrativen Handelns, sondern nach Art. 20 Abs. 3 GG eine eigene Staatsgewalt mit justizspezifischen Besonderheiten. So sind die Richter persönlich und sachlich unabhängig und nur dem Gesetz unterworfen.[35] Selbst den Rechtspflegern gewährt das Gesetz sachliche Unabhängigkeit, so dass auch in dem weiten Feld der Rechtspflege die Unabhängigkeit in der Sachentscheidung maßgebende Maxime ist.[36] Nimmt man zudem das Legalitätsprinzip der Strafprozessordnung noch in den Blick, wird deutlich, dass auch im Bereich der staatsanwaltschaftlichen Tätigkeit dem Grunde nach für das viel berufene Weisungsrecht in der Praxis wenig Raum ist.[37] Diese Besonderheiten wirken sich immer auch auf den Modernisierungsprozess aus. Dies zeigen beispielsweise die Diskussionen darüber, inwieweit von einem Richter der Umgang mit Computern verlangt werden kann.[38] Das Bundesjustizministerium und die Landesjustizministerien haben diesen Besonderheiten bei der Ausgestaltung der Rahmenbedingungen von IT-Anwendungen hinreichend Rechnung zu tragen.[39] Insofern ist es geboten, begrifflich zwischen Modernisierungsprozessen im administrativen Bereich und im

---

31 Auch E-Administration genannt.

32 Gemeint sind damit etwa sog. elektronische Abstimmungen oder Wahlen oder elektronische Diskussionsforen wie z.B. `www.e-konsultation.de`.

33 *Häfner*, DRiZ 2005, 151.

34 *Bernhard*, JurPC Web-Dok. 2007, Abs. 3. Zur elektronischen Klageeinreichung bei den Bundesgerichten im Rahmen von BundOnline2005, vgl. *Schwoerer*, 2005, 23. Daneben haben auch verschiedene länderspezifische E-Government Masterpläne IT-Dienstleistungen der Justiz umfasst. Speziell dazu wiederum *Bernhard*, JurPC Web-Dok. 2007, Abs.3.

35 Art. 97 GG, § 1 GVG, §§ 25 ff. DRiG.

36 *Koebler*, NJW 2006, 2090.

37 *Koebler*, NJW 2006, 2090.

38 Zum Aktenausdruck aus dem elektronisch geführten Handelsregister, vgl. Dienstgericht Düsseldorf, BDVR-Rundschreiben 2009, 68. Weitere Nachweise auch bei *Schwoerer*, 2005, 97 f.

39 Die Justizministerinnen und Justizminister betonen deshalb auch immer ihre Eigenständigkeit beim Einsatz von IT-Anwendungen in der Justiz. Vgl. hierzu etwa der Beschluss der 80. Justizministerkonferenz am 24./25.6.2009 in Dresden zu TOP I.10 (Möglichkeiten länderübergreifender Zusammenarbeit im Bereich der IT vor dem Hintergrund der Föderalismusreform – Art. 91c GG): „Bei der Realisierung der Ziele des Artikel 91c GG werden die institutionelle Sonderstellung der Justiz sowie die aus der verfassungs- und ein-

justiziellen Bereich zu unterscheiden.[40] An versteckter Stelle hatte dies im Übrigen auch der Bundesgesetzgeber getan und der EDV-Gerichtstag hatte bereits 2000 seine Beratungen unter das Motto E-Justice gestellt.[41]

2.1.2 Abgrenzung zum elektronischen Rechtsverkehr

Auch beim elektronischen Rechtsverkehr gibt es verschiedene Auffassungen dazu, was hierunter zu verstehen ist. Eine Ansicht fasst den Begriff weit.[42] Danach wird unter dem elektronischen Rechtsverkehr sowohl die rechtsverbindliche Kommunikation mit Gerichten und Verfahrensbeteiligten, die elektronischen Register, die ganze interne elektronische Sachbehandlung und Aktenführung bis hin zur elektronischen Archivierung verstanden. Kurz gesagt geht es hierbei um sämtliche IT-Anwendungen in der Justiz sowohl im Binnenbereich, als auch im Außenbereich. Versteht man den elektronischen Rechtsverkehr in diesem Sinne, so ist der Begriff gleichbedeutend mit dem der elektronischen Justiz. Eine andere Ansicht geht von einer engeren Bedeutung aus. Diese Ansicht subsumiert unter dem Begriff nicht alle IT-Anwendungen der Justiz, sondern nur solche, die die Außenbeziehungen des Gerichts zu Dritten betreffen.[43]

Richtigerweise ist von einem engen Verständnis des elektronischen Rechtsverkehrs auszugehen. So gab es schon seit den 60er Jahren verschiedene Vorschläge zur Einführung von IT in der Justiz. Diese reichten von der Einführung einer einfachen Textverarbeitung über die vollständige Textverwaltung, von Möglichkeiten der Gesetzesverwaltung und -pflege bis hin zur Unterstützung des Geschäftsbetriebs der Gerichte.[44] Zu diesem frühen Zeitpunkt wurde jedoch noch nicht von dem Begriff des elektronischen Rechtsverkehrs gesprochen. Vielmehr ging es hier um Fragen der Einführung der „Elektronischen Datenverarbeitung“ bei Gericht.[45] Der Begriff des elektronischen Rechtsverkehrs hat sich erst so richtig herauskristallisiert, als das Internet bekannt wurde und man erwogen hatte, dieses Medium für die Justiz, v.a. für den rechtsverbindlichen Austausch von Dokumenten, nutzbar zu machen.[46] Aus diesem Grund scheint es angebracht, für diese Untersuchung von diesem engen Verständnis auszugehen. Aller-

fachrechtlich garantierten Position der unabhängigen Rechtspflegeorgane resultierenden Besonderheiten zu beachten sein.“

40 So auch *Koebler*, NJW 2006, 2090; *Bund-Länder-Kommission*, JurPC Web-Dok. 2009, Abs. 36 ff.

41 *Bernhard*, JurPC Web-Dok. 2007, Abs. 2. Auch die EU-Kommission geht von dieser Begrifflichkeit aus, vgl. hierzu `http://ec.europa.eu/deutschland/press/pr_releases/index_7817_de.htm` (Zugriff am 10.1.2010).

42 *Hähnchen*, JurPC Web-Dok. 2007, Abs. 3; *Viefhues/Volesky*, TKMR 2003, 245.

43 Zu dieser Unterscheidung vgl. *Britz*, DVBl 2007, 994.

44 *Werner*, 1995, 23.

45 *Werner*, 1995, 23.

46 Den politischen Startschuss zur elektronischen Übermittlung von Dokumenten über das Internet gab dabei die 70. Konferenz der Justizministerinnen und Justizminister am 7./9.6.1999 in Baden-Baden. So heißt es hier unter TOP I.1 (Elektronischer Geschäftsverkehr mit Gerichten und Staatsanwaltschaften): „Die Justizministerinnen und -minister halten es für notwendig, im Zuge einer weiteren Rationalisierung des Geschäftsablaufs bei den Gerichten und Staatsanwaltschaften und im Hinblick auf den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt den Geschäftsverkehr mit Gerichten und Staatsanwaltschaften

dings darf der Begriff dann nicht so eng verstanden werden, dass er nur den rechtsverbindlichen Austausch von Dokumenten umfasst. Vielmehr sollte man zwischen Innenbeziehungen und Außenbeziehungen unterscheiden. Von dem Begriff des elektronischen Rechtsverkehrs sollten daher alle Außenbeziehungen erfasst werden, also nicht nur der Austausch von Dokumenten, sondern zum Beispiel auch Registerabfragen und Bekanntmachungsplattformen.

2.1.3 Abgrenzung zum elektronischen Geschäftsverkehr

Letztlich darf der Begriff der elektronischen Justiz auch nicht mit dem des elektronischen Geschäftsverkehrs verwechselt werden. Der Begriff des elektronischen Geschäftsverkehrs entstand mit der kommerziellen Nutzung des Internet.[47] Er umfasst allein den materiellen Rechtsverkehr. Es geht hier ausschließlich um den entgeltlichen Vertrieb von Waren und oder Dienstleistungen über das Internet und nicht um rechtsverbindliche prozessuale Erklärungen.[48] Dementsprechend wird der Begriff auch in § 312e Abs. 1 Bürgerliches Gesetzbuch (BGB) als die Lieferung von Waren und die Erbringung von Dienstleitungen über einen Tele- oder Mediendienst legaldefiniert.[49] Nur vereinzelt wird unter dem Begriff des elektronischen Geschäftsverkehrs auch der prozessuale Rechtsverkehr verstanden.[50] Aufgrund der ganz beträchtlichen Unterschiede zwischen prozessualen und materiellem Rechtsverkehr sollte jedoch zwischen diesen beiden Formen auch begrifflich unterschieden werden. Den Begriff des elektronischen Geschäftsverkehrs als Oberbegriff für den prozessualen und den materiellen Rechtsverkehr zu verwenden, würde nur zu Verwirrungen führen.

2.2 Ziele

Nachdem die Begriffe geklärt sind, wird nun auf die Ziele eingegangen, die mit dem Einsatz neuer Techniken in der Justiz verbunden sind. Im E-Government wurden die Ziele der Verwaltungsmodernisierung anhand von verschiedenen Leitbildern ausführlich beschrieben und diskutiert.[51] Es geht hier um „die Automation von Abläufen und Ergebnisrückmeldung, um Informationsmehrung durch Datenubiquität, um Reduktion örtlicher und zeitlicher Schranken, um Parallelisierung und Integration bislang sequentiell und hochgradig arbeitsteilig durchgeführter Aufgaben. Kurzum: Es geht um die IT-gesteuerte Rundum-Erneuerung der Verwaltung.“[52] Für die elektronische Justiz lassen sich ähnlich weitgehende Leitbildformulierungen seltener

(...) auch im Wege der elektronischen Übermittlung zu ermöglichen und dies in Modellversuchen zu erproben.“

47 *Schwoerer*, 2005, 22.

48 *Schwoerer*, 2005, 22.

49 Zum Teil wird aber auch jeder Geschäftsverkehr über elektronische Medien, also auch der über Telefax oder Telefon als elektronischer Geschäftsverkehr verstanden, da auch bei diesen Medien die Elektronik genutzt wird. Sie hierzu *Schwoerer*, 2005, 22 m.w.N.

50 So *Fritsche*, NJ 2002, 169; *Suermann*, DRiZ 2001, 291.

51 *Yildirim*, 2004, 20 ff.

52 *Britz*, DVBl 2007, 994.

finden.[53] Im Vordergrund stehen hier vorwiegend Einsparpotenziale. Auch der Bürgernähe, die im E-Government eine entscheidende Rolle spielt, kommt in der elektronischen Justiz eine eher untergeordnete Rolle zu. Die Ziele der elektronischen Justiz lassen sich daher sehr kurz zusammenfassen. Es geht hier um Verfahrensbeschleunigung, Kostenminimierung und Transparenz, soweit die Verfahrensordnungen sie erfordert.[54]

2.2.1 Verfahrensbeschleunigung

Ein wesentliches Qualitätsmerkmal in der dritten Gewalt ist der effiziente und zügige Ablauf von gerichtlichen Verfahren. Mit dem Einsatz neuer Techniken ist daher in erster Linie die Hoffnung verbunden, gerichtliche Verfahren zu beschleunigen und die Justiz dadurch zu entlasten. Hierzu sollen vor allem die elektronische Übermittlung von Dokumenten und die elektronische Aktenführung beitragen. Eine kürzere Verfahrensdauer verspricht man sich von der Übermittlung von Dokumenten in elektronischer Form und der damit einhergehenden geringeren Transportzeiten.[55] Die elektronische Akte ermöglicht eine gleichzeitige Bearbeitung durch die Geschäftsstelle und die Richter und soll von daher zu einer Straffung des Verfahrens führen. In diesem Zusammenhang ist auch die Möglichkeit der elektronischen Akteneinsicht zu sehen. Deren Ziel ist es vor allem, eine zeitweise Handlungsunfähigkeit des Gerichts aufgrund der Aktenversendung und der damit verbundenen Umstände zu vermeiden.

2.2.2 Kostenminimierung

Mit der elektronischen Übermittlung von Dokumenten werden Porto- und Zustellkosten minimiert. Berechnungen für Österreich ergaben Einsparungen an Porto- und Zustellkosten von einer Millionen Euro pro Jahr. Umgerechnet auf die Bevölkerungszahl Deutschlands lässt dies eine jährliche Einsparung von 10 Millionen Euro erwarten.[56] Kostensenkungen werden vor allem auch von den elektronischen Bekanntmachungen im Internet erwartet. So bewogen den Gesetzgeber unter anderem die hohen Druckkosten bei den herkömmlichen Printmedien dazu, die Bekanntmachungen der Gerichte ins Internet zu verlagern.[57]

---

53 *Britz*, DVBl 2007, 994.

54 Vgl. zu den Zielen *Zypries*, 2007; *Britz*, DVBl 2007, 994; *Viefhues*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 145 ff.

55 *Viefhues*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 147 hält dieses Argument jedoch nicht für durchschlagend. Wenn ein gerichtliches Verfahren einige Monate oder gar Jahre dauert, habe es praktisch keine Auswirkungen, ob ein Schriftsatz einen Tag oder zehn Sekunden unterwegs sei.

56 *Viefhues*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 147.

57 Vgl. etwa BT-Drs. 16/3227, 2.

2.2.3 Transparenz

In den Verfahrensordnungen finden sich viele Vorschriften, welche darauf ausgerichtet sind, einen großen Kreis von Lesern zu erreichen. Hierzu gehören etwa die Bekanntmachungen von Terminen über stattfindende Zwangsversteigerungen,[58] die Veröffentlichungen von Insolvenzdaten[59] oder auch von Jahresabschlüssen[60]. Nicht nur um Kosten zu sparen, sondern auch um das Verfahren für die Allgemeinheit transparenter zu machen, bedient sich die Justiz hierfür zunehmend des Internets als Veröffentlichungsmedium.

2.3 Entwicklung

Die Elektronisierungsziele haben heute sowohl in der rechtlichen Verankerung, als auch in der tatsächlichen Realisierung Spuren hinterlassen. Im Folgenden wird daher die Entwicklung dieser Verfahren dargestellt. Wie bereits erläutert, betreffen diese vor allem das Zivilverfahren, die Zwangsvollstreckung, die Zwangsversteigerung, das Insolvenzverfahren, die Grundbuchordnung und das Handelsgesetzbuch, die nun im Detail betrachtet werden.

2.3.1 Zivilverfahren

2.3.1.1 E-Schriftsätze an das Gericht

Durch das Formvorschriftenanpassungsgesetz[61] wurden in Umsetzung von Art. 9 der Richtlinie über den elektronischen Geschäftsverkehr[62] mit Wirkung vom 1.8.2001 die Formvorschriften des BGB geändert und elektronische Dokumente im Rechtsverkehr materiell-rechtlich vorgesehen.[63] Diese Änderungen des materiellen Rechts erforderten eine Anpassung auch der prozessrechtlichen Vorschriften.[64] Mit dem FormVAnpG änderte der Gesetzgeber daher zugleich Vorschriften in der ZPO und führte neue Vorschriften ein. So wurde im Hinblick auf die Abwicklung des gerichtlichen Verfahrens insbesondere § 130a ZPO neu eingefügt.[65]

Nach § 130a ZPO darf heute alles, was in schriftlicher Form von den Parteien, ihren Bevollmächtigten und Dritten bei Gericht eingereicht werden kann, als elektronisches Dokument an das Gericht übermittelt werden, d.h. in Form einer E-Mail.[66]

---

58 § 39 ZVG.

59 § 9 InsO i.V.m. mit den hierauf verweisenden Vorschriften.

60 §§ 325 ff. HGB.

61 BGBl. 2001 I, 1542.

62 ABl. EG L 178, 1.

63 Vgl. §§ 126 Abs. 3, 126a BGB.

64 *Krüger/Bütter*, MDR 2003, 181.

65 Ob die Einführung der Vorschrift erforderlich war oder ob die elektronische Übermittlung von Schriftsätzen auch ohne gesetzliche Grundlage erforderlich gewesen wäre, ist fraglich. Jedenfalls ist sie aber aus Gründen der Rechtsklarheit als positiv zu beurteilen.

66 BGH, NJW-RR 2009, 357.

§ 130a Abs. 1 Satz 2 ZPO bestimmt dabei, dass das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz (§ 2 Nr. 3 SigG) versehen werden soll.[67] Diese Soll-Vorschrift stieß im Gesetzgebungsverfahren auf den Widerstand des Bundesrates: Der Bundesrat wollte die elektronische Signatur für bestimmende Schriftsätze aus Gründen der Rechtssicherheit zwingend, d.h. nicht nur als Sollvorschrift einführen. Im Vermittlungsausschuss einigte man sich nicht etwa auf einen eindeutigen Wortlaut, sondern auf eine Regelinterpretation: Im Protokoll wurde festgehalten, man gehe davon aus, dass die Soll-Bestimmung in § 130a ZPO wie der bisherige § 130 ZPO für bestimmende Schriftsätze als Muss-Vorschrift auszulegen ist.[68]

Gemäß § 130a Abs. 2 ZPO bestimmen die Bundes- und Landesregierungen durch Rechtsverordnung jeweils den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können.[69] Der Bund hat im Zivilverfahren die Einreichung elektronischer Dokumente für die beim Bundesgerichtshof zugelassenen Rechtsanwälte seit November 2001 ermöglicht.[70] In der rheinland-pfälzischen ordentlichen Gerichtsbarkeit besteht diese Möglichkeit im Unterschied zu der dortigen Fachgerichtsbarkeit und bestimmten Land- und Amtsgerichten anderer Bundesländer noch nicht.[71]

Dabei kommen heute zwei unterschiedliche Lösungen zum Einsatz[72]: Der E-Mail-Versand und das elektronische Gerichtspostfach, wobei bei ersterem der Schriftsatz als gewöhnlicher E-Mail-Anhang an das Gericht übermittelt und dort in Empfang genommen wird. Beim elektronischen Gerichtspostfach nutzt der Bediener ein entsprechendes Programm zum Verbindungsaufbau.[73] Der Zugang zum Gerichtspostfach wird eröffnet, indem der Nutzer sein Passwort und seinen Namen angibt. Das Postfach fragt sodann ab, ob es sich um einen Neueingang einer Klageschrift handelt oder um einen Schriftsatz in einem bereits laufenden Verfahren. Im ersten Fall wird das Dokument zu einer zentralen Eingangsstelle des Gerichts geleitet. Dort wird dann ein neues Verfahren angelegt. Anderenfalls fragt das Gericht das Aktenzeichen ab, bevor die automatische Weiterleitung des Dokuments bewirkt wird. Vom Gerichtspostfach wird dann eine Eingangsbestätigung auf elektronischem Wege übermittelt. Diese Nachrichten können auch mit Anhängen versehen und ggf. auch elektronisch signiert werden. Die Übertragung erfolgt standardmäßig über verschlüsselte Leitungen.

---

67 Vgl. hierzu BGH, NJW 2008, 2649. Nach dieser Entscheidung tritt eine qualifizierte elektronische Signatur an die Stelle der eigenhändigen Unterschrift im Sinne des § 130 Nr. 6 ZPO.

68 Vgl. hierzu *Stadler*, ZZP 2002, 420 m.w.N.

69 Bedenklich ist deshalb die Praxis vieler Gerichte, auf ihrer Homepage die E-Mail Adresse anzugeben. Um den Anschein von widersprüchlichen Verhalten zu vermeiden, ist ein Hinweis erforderlich, dass eine elektronische Klageeinreichung nicht zulässig ist.

70 BGBl. 2001 I, 3225.

71 Nähere Informationen unter `http://www.verwaltung.rlp.de/eGovernment/-,7993/Elektronischer-Rechtsverkehr.htm` (Zugriff am 11.1.2010). Einen Überblick zu allen Gerichtsbarkeiten im Bundesgebiet gibt *Degen*, NJW 2008, 1473.

72 *Viefhues*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 5.

73 Das Elektronische Gerichts- und Verwaltungspostfach `www.egvp.de` ist ein Dienst, mit der Gerichte und Behörden mit ihren „Kunden“ (z.B. Verfahrensbeteiligten, Antragstellern) und untereinander besonders sicher unstrukturierte Nachrichten im sog. OSCI-Format austauschen können.

2.3.1.2 E-Zustellungen des Gerichts

Mit dem Zustellungsreformgesetz[74] wurde mit Wirkung zum 1.7.2002 in § 174 Abs. 3 ZPO erstmals auch die Möglichkeit der Zustellung elektronischer Dokumente durch das Gericht an Prozessbeteiligte vorgesehen. § 174 Abs. 3 ZPO verlangt im Gegensatz zu § 130a ZPO (als Soll-Vorschrift) hierfür zwar nicht eine qualifizierte elektronische Signatur; vielmehr genügt auch eine einfache Signatur.[75] Dafür schreibt § 174 Abs. 3 ZPO jedoch – wiederum im Gegensatz zu § 130a ZPO – vor, dass das Dokument gegen unbefugte Kenntnisnahme Dritter zu schützen ist.

Empfänger von elektronischen Dokumenten können zum einen der in § 174 Abs. 1 ZPO aufgezählte Kreis aus Behörden, öffentlich-rechtlichen Körperschaften, Anstalten, Rechtsanwälten, Notaren oder Steuerberatern oder sonstige aufgrund ihres Berufes erhöht zuverlässige Personen sein. Daneben kann ein elektronisches Dokument auch anderen Beteiligten zugestellt werden, wenn sie der Übermittlung elektronischer Dokumente ausdrücklich zugestimmt haben. Im Referenten- und Regierungsentwurf war es noch ausdrücklich abgelehnt worden, Zustellungen gegen Empfangsbekenntnis an jedermann zuzulassen. Erst im Rechtsausschuss sprach man sich hierfür aus, da der Kreis der Adressaten, denen im Rechtsverkehr zugestellt werden könne, nicht zu eng gezogen werden sollte.[76] Im Gegensatz zu § 130a Abs. 2 Satz 1 ZPO ist für die Vornahme von elektronischen Zustellungen nicht der Erlass einer Rechtsverordnung erforderlich. § 174 Abs. 3 ZPO ist aufgrund des eindeutigen Wortlauts des § 130a Abs. 2 Satz 1 ZPO auch nicht in Zusammenhang mit dieser Vorschrift zu lesen.[77]

Der Bundesgerichtshof hat seit dem 1.7.2002 förmliche Zustellungen vorgenommen.[78] In der ordentlichen Gerichtsbarkeit von Rheinland-Pfalz wird diese Zustellungsform – soweit ersichtlich – noch nicht praktiziert. Die Oberlandesgerichte, Land- und Amtsgerichte der anderen Bundesländer machen hiervon zum Teil Gebrauch.

2.3.1.3 E-Mitteilungen des Gerichts

Die ZPO erachtet an verschiedenen Stellen – so zum Beispiel in §§ 104 Abs. 1 Satz 4, 251a Abs. 2 Satz 3, 270 Satz 1, 329 Abs. 2 Satz 1, 497 Abs. 1 Satz 1 ZPO – auch die formlose Mitteilung an die Verfahrensbeteiligten als ausreichend. In diesen Fällen hat die Rechtsprechung bislang eine telefonische Bekanntgabe von Beschlüssen und Verfügungen für ausreichend erachtet.[79] In diesen Fällen ist daher auch eine elektronische Übermittlung von Nachrichten möglich.[80] Ob diese vorgenommen wird, hängt von dem Verhalten des zuständigen Richters

74 BGBl. 2001 I, 1206.
75 BT-Drs. 14/4554, 19.
76 BT-Drs. 14/5564, 20.
77 Anders jedoch *Hess*, NJW 2002, 2420; *Kampen/Engelhardt*, ArbuR 2003, 247. So wie hier *Holin*, 2008, 146.
78 *Holin*, 2008, 188.
79 *Krüger/Bütter*, MDR 2003, 185.
80 *Krüger/Bütter*, MDR 2003, 185.

im Einzelfall ab und lässt sich daher nicht feststellen. Es ist jedoch davon auszugehen, dass hiervon bislang die wenigsten Richter Gebrauch machen.

2.3.1.4 E-Akteneinsicht

Mit § 299 Abs. 3 ZPO wurde durch das Justizkommunikationsgesetz, welches am 1.4.2005 in Kraft getreten ist[81] die Möglichkeit geschaffen, Akteneinsicht auf elektronischem Wege zu erhalten. Den Parteien stehen dabei optional folgende Möglichkeiten zur Verfügung: Einmal kann Akteneinsicht gewährt werden, indem der Akteninhalt ganz oder teilweise ausgedruckt wird. Zum anderen ist es möglich, dass die Übermittlung von Akten und Aktenteilen per E-Mail oder auf elektronischem Datenträger, der per Post versandt wird, erfolgt. Schließlich ist auch eine Online-Einsicht auf der Geschäftsstelle möglich. Für die Übermittlung elektronischer Dokumente schreibt § 299 Abs. 3 Satz 4 ZPO dabei vor, dass die Gesamtheit der Dokumente mit einer qualifizierten elektronischen Signatur zu versehen ist und gegen unbefugte Kenntnisnahme zu schützen ist.

Einem Bevollmächtigtem, der Mitglied einer Rechtsanwaltskammer ist, kann darüber hinaus auch der Online-Zugriff aus seiner Kanzlei gestattet werden. Die Maßnahme steht im Ermessen des Vorsitzenden. Sofern der Online-Zugriff gestattet wird, ist nach § 299 Abs. 3 Satz 3 ZPO sicher zu stellen, dass der Zugriff nur durch den Bevollmächtigten erfolgt. Wie den Gesetzgebungsmaterialien zu entnehmen ist, geht diese Regelung auf eine Forderung des Bundesrates zurück. Dieser hatte damals bemängelt, dass der Entwurf zwar die Online-Einsicht in den Verfahren der Verwaltungs-, Finanz- und Sozialgerichtsbarkeit vorsah, nicht jedoch im Zivilverfahren. Im Sinne der Einheitlichkeit der Verfahrensordnungen sei daher auch die Online-Einsicht im Zivilverfahren zu ermöglichen.[82] Eine elektronische Akteneinsicht ist derzeit weder beim Bundesgerichtshof noch in der ordentlichen Gerichtsbarkeit von Rheinland-Pfalz möglich.[83] In anderen Bundesländern wird sie zum Teil in Pilotprojekten erprobt.[84]

2.3.1.5 E-Bekanntmachungen nach der ZPO

Durch das Justizkommunikationsgesetz wurde darüber hinaus festgelegt, dass, soweit Veröffentlichungen im Bundesanzeiger erfolgen, also in den Fällen der §§ 187, 948, 950, 956, 1014, 1017 Abs. 2, 1020 und 1022 Abs. 1 ZPO,[85] diese im elektronischen Bundesanzeiger vorzunehmen sind. Ferner wurde die Möglichkeit geschaffen, öffentliche Bekanntmachungen der Gerichte

[81] BGBl. 2005 I, 837.

[82] BR-Drs. 609/04, 16.

[83] Eine elektronische Akteneinsicht und eine Verfahrensstandabfrage wird in Rheinland-Pfalz jedoch von der Fachgerichtsbarkeit zur Verfügung gestellt, vgl. hierzu `http://www.verwaltung.rlp.de/eGovernment/-,7993/Elektronischer-Rechtsverkehr.htm` (Zugriff am 11.1.2010).

[84] Zum Beispiel beim Amtsgericht Westerstede, wo im Rahmen einer Verfahrensstandabfrage eine Einsichtnahme in Verfahrensdaten möglich ist, vgl. hierzu *Holin*, 2008, 191.

[85] Vgl. hierzu nunmehr §§ 435, 437, 441, 475, 478, 482 FamFG.

in den Fällen der §§ 186 Abs. 2, 948 Abs. 1 und 1009 ZPO[86] in einem vom Gericht bestimmten elektronischen Informations- und Kommunikationssystem zu veröffentlichen. Erwähnenswert ist in diesem Zusammenhang, dass datenschutzrechtliche Fragestellungen bei der Schaffung dieser Normen keine Rolle gespielt haben. Im Gegenteil: Dem Bundesrat gingen die von der Bundesregierung im Entwurf vorgeschlagenen Regelungen nicht weit genug: Er forderte – mit Blick auf die bisherigen positiven Erfahrungen bei den Internetinsolvenzbekanntmachungen[87] – dass in allen Fällen, in denen eine Veröffentlichung im elektronischen Bundesanzeiger vorgesehen ist, zusätzlich eine Veröffentlichung in einem vom Gericht bestimmten elektronischen Informations- und Kommunikationssystem zu erfolgen hat.[88] Mit Blick auf die genannten Vorgaben sind auf der Internetseite `www.ebundesanzeiger.de` des elektronischen Bundesanzeigers die Bekanntmachungen nach der ZPO von allen Gerichten in der Bundesrepublik und damit auch von den rheinland-pfälzischen Gerichten enthalten. Von der Möglichkeit, Bekanntmachungen auch in einem vom Gericht bestimmten elektronischen Informations- und Kommunikationssystem zu veröffentlichen, hat das Land bislang jedoch noch keinen Gebrauch gemacht.

2.3.1.6 E-Akte

In § 298a ZPO hat der Gesetzgeber mit dem Justizkommunikationsgesetz Regelungen zur Führung elektronischer Akten getroffen, welche den Justiz-Workflow bestimmen. Gemäß § 298a Abs. 1 Satz 2 ZPO bestimmen die Bundesregierung und die Landesregierungen durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Akten geführt werden. Die Rechtsverordnung kann dabei die Einführung der elektronischen Akte auf bestimmte Gerichte und Verfahren beschränken. Die Beschränkung auf einzelne Verfahren und Gerichte erlaubt des Weiteren die Begrenzung auf einzelne Spruchkörper oder Verfahren. Erforderlich ist in diesem Fall allerdings, dass die Verfahren, deren Prozessakten elektronisch zu führen sind, nach abstrakt generellen Kriterien bestimmt oder bestimmbar sind.[89] Für die elektronische Aktenführung bei der ordentlichen Gerichtsbarkeit in Rheinland-Pfalz gibt es bislang noch keine derartige Rechtsverordnung. Auch existiert beim Bundesgerichtshof für die hier interessierenden Bereiche noch keine Verordnung. Seit dem 1.3.2010 ist allerdings eine elektronische Aktenführung beim Bundesgerichtshof in Patentstreitigkeiten[90] möglich.

---

86 Vgl. hierzu nunmehr §§ 435, 470 FamFG.

87 Vgl. hierzu die Ausführungen unten unter Abschnitt 2.3.3.1.

88 BR-Drs. 609/04, 11.

89 Zur elektronischen Akten und richterlichen Unabhängigkeit speziell, vgl. *Berlit*, JurPC Web-Dok. 2008, Abs. 29 ff.; allgemein zur richterlichen Unabhängigkeit vgl. *Berlit*, in: *Schulze-Fielitz/Schütz* (Hrsg.), Justiz und Justizverwaltung zwischen Ökonomisierungsdruck und Unabhängigkeit, 135.

90 Verordnung über die elektronische Aktenführung bei dem Patentamt, dem Patentgericht und dem Bundesgerichtshof, vgl. BGBl. 2010 I, 83.

2.3.1.7 E-Mahnverfahren

Mit der Vereinfachungsnovelle von 1976[91] hat der Gesetzgeber die gesetzlichen Grundlagen für die Einführung eines maschinellen Mahnverfahrens geschaffen (§§ 696 Abs. 2, 703b, 703c ZPO)[92]. Diese wurden als erstes am 1.10.1982 am Amtsgericht Stuttgart und am Amtsgericht Stuttgart Bad-Cannstatt in die Praxis umgesetzt.[93] Die rechtlichen Grundlagen für die elektronische Übermittlung der Mahnanträge gemäß § 690 Abs. 3 ZPO wurden mit dem Rechtspflegevereinfachungsgesetz von 1990 geschaffen.[94] In Rheinland-Pfalz werden Mahnanträge bereits seit 1988 maschinell bearbeitet und zwar zentral für das gesamte Bundesland beim Amtsgericht Mayen.[95] Seit dem 1.4.2005 ist das Amtsgericht Mayen auch für die Bearbeitung der Mahnanträge für das Saarland zuständig.[96] Des Weiteren existieren heute in Schleswig, Hamburg, Bremen, Berlin, Uelzen, Aschersleben, Hagen, Euskirchen, Hünfeld, Coburg und Stuttgart zentrale Mahngerichte. Bei diesen sowie bei dem Amtsgericht Mayen können Mahnanträge auf zwei Wegen eingereicht werden: Einmal durch das – ältere – Belegverfahren. Die Antragsteller füllen in diesem Fall die Daten auf einem Papiervordruck aus. Dieser Vordruck wird dann bei Gericht eingescannt. Zum anderen durch einen elektronischen Datenaustausch. Dies bedeutet, dass der Mahnantrag dem Gericht entweder in einer Datei mittels Diskette oder über das Internet übermittelt wird. Seit dem 1.12.2008 ist es für Anwälte gemäß § 690 Abs. 3 Satz 2 ZPO Pflicht, Anträge auf Erlass eines Mahnbescheides im Wege eines elektronischen Datenaustausches einzureichen. § 690 Abs. 3 Satz 2 ZPO geht auf das 2. Justizmodernisierungsgesetz zurück.[97] Der Gesetzgeber wollte mit der Neuregelung erreichen, dass das Verfahren beschleunigt und der Rechtsverkehr gefördert wird. Im Vergleich zu einer elektronischen Übermittlung eines Mahnantrags hielt er den Weg über das Belegverfahren für zeitaufwändiger, weil die Qualität der Daten schlechter sei und das Einscannen fehleranfälliger.[98]

2.3.1.8 ELENA und Prozesskostenhilfe

Das Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) ist hinsichtlich seiner wesentlichen Regelungen am 2.4.2009 in Kraft getreten.[99] Unter dem ELENA-Verfahren versteht man ein Verfahren, mit dem Einkommensnachweise elektronisch erbracht werden sollen. Das ELENA-Verfahrensgesetz beinhaltet derzeit noch keine Einbindung von gerichtlichen Arbeitsabläufen in der Justiz. Allerdings gibt es hierzu schon

91 BGBl. 1976 I, 3281.
92 Hierzu *Mayer*, NJW 1983, 92; *Keller*, NJW 1981, 1184.
93 *Sujecki*, MMR 2006, 370.
94 BGBl. 1990 I, 2847.
95 Landesverordnung über die Einführung der maschinellen Bearbeitung der Mahnverfahren und über die Zuständigkeit im Mahnverfahren, GVBl. 1988, 151.
96 Landesgesetz zu dem Staatsvertrag zwischen dem Land Rheinland-Pfalz und dem Saarland über die Errichtung eines gemeinsamen Mahngerichts, GVBl. 2005, 61.
97 BGBl. 2006 I, 3416.
98 BT-Drs. 16/3038, 40.
99 BGBl. 2009 I, 634.

konkrete Überlegungen.[100] So gab es im Rahmen des JobCard-Verfahrens bereits ein Pilotprojekt „Elektronisches Scheidungsverfahren bei dem Amtsgericht Olpe“. Im Rahmen dieses Modells wurde untersucht, inwieweit die bei ELENA in der zentralen Stelle vorhandenen Daten für das Prozesskostenhilfeverfahren genutzt werden können. In Zusammenarbeit mit Vertretern des JobCard-Verfahrens wurde eine vorläufige Bescheinigung entwickelt, die alle bei der Prozesskostenhilfe-Bewilligung maßgeblichen Daten abdeckt. Dabei geht es vor allem um Daten aus der Entgelt-/Gehaltsbescheinigung des Arbeitgebers, der Bescheinigung über das Krankengeld, der Bescheinigung über den Bezug von Sozialhilfe, den Arbeitslosengeldbescheid und etwaige Rentenbescheide.

2.3.1.9 E-Schutzschriftenregister

Die Europäische EDV-Akademie des Rechts (EEAR) betreibt heute unter der Internet-Adresse `www.schutzschriftenregister.de` ein zentrales Schutzschriftenregister (ZSR). In dieses können Prozessbevollmächtigte eine Schutzschrift online bei einer zentralen Stelle hinterlegen. Einige Amts- und Landgerichte[101] haben sich verpflichtet, bei Eingang eines Antrages auf Erlass einer einstweiligen Verfügung eine Abfrage in diesem Register zu tätigen. Rheinland-Pfälzische Gerichte gehören noch nicht dazu. Allerdings wird es nur eine Frage der Zeit sein, bis sich auch die Gerichte in Rheinland-Pfalz dem ZSR anschließen werden.

2.3.2 Zwangsvollstreckung und Zwangsversteigerung

2.3.2.1 E-Schuldnerverzeichnis

Schuldnerverzeichnisse werden bislang noch bei den Amtsgerichten papiergebunden geführt.[102] Mit dem Gesetz über die Änderung zum Schuldnerverzeichnis[103] vom 15.7.1994 wurden in den §§ 915 ff. ZPO vereinzelt Bestimmungen geschaffen, die den Einsatz von neuen Techniken bei der Übermittlung von Schuldnerdaten vorsahen.[104]

So wurde in § 915d Abs. 1 ZPO geregelt, dass die Vollstreckungsgerichte an die in § 915e ZPO genannten Stellen wie zum Beispiel den Kammern oder der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) Abdrucke aus den Schuldnerverzeichnissen auch durch Übermittlung

100 *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 169 ff.

101 Landgerichte: Arnsberg, Baden-Baden, Bielefeld Bochum, Bremen, Cottbus, Darmstadt, Detmold, Dortmund, Duisburg, Düsseldorf, Essen, Frankfurt a.M., Frankfurt / Oder, Freiburg, Fulda, Gießen, Hagen, Hamburg, Hanau, Heidelberg, Kassel, Kleve, Krefeld, Leipzig, Limburg, Mannheim, Marburg, Mönchengladbach, Mosbach, Münster, Nürnberg-Fürth, Paderborn, Ravensburg, Saarbrücken, Siegen, Stuttgart, Tübingen, Ulm, Waldshut-Tiengen, Wiesbaden, Wuppertal. Amtsgerichte: Adelsheim, Bad Liebenwerda, Brakel, Brandenburg an der Havel, Bühl, Frankfurt-Oder, Fürth/Odw., Kehl, Künzelsau, Lemgo, Lübbecke, Möchengladbach, Nürtingen, Siegen, Stuttgart-Bad Cannstatt.

102 BR-Drs. 304/08, 1.

103 BGBl. 1994 I, 1566.

104 Einen Überblick über die damaligen Änderungen geben *Abel*, RDV 1988, 185; *Straub*, 1995 und *Hornung*, Rpfleger 1995, 233.

in nur maschinell lesbarer Form zum laufenden Bezug erteilen können. Zum anderen wurde in § 915e Abs. 2 ZPO bestimmt, dass die genannten Stellen Auskünfte an ihre Kammermitglieder und Kunden auch im Wege eines automatisierten Abrufverfahrens erteilen können. Zudem ist bestimmt worden, dass Kammern Abdrucke in Listen zusammenzufassen können und diese gemäß § 915f ZPO ihren Mitgliedern – wiederum durch Übermittlung in einer nur maschinell lesbaren Form – überlassen dürfen. Mit § 915h Abs. 2 ZPO hat der Gesetzgeber schließlich den Landesregierungen die Möglichkeit eingeräumt, Schuldnerdaten mehrerer örtlicher Schuldnerverzeichnisse an einem Vollstreckungsgericht zu einem zentralen Verzeichnis für die Bezirke mehrerer Amtsgerichte zusammenzufassen. § 915h Abs. 2 ZPO sieht dabei vor, dass die jeweiligen Amtsgerichte dem zentralen Gericht ihre Daten mitzuteilen haben; im Wege eines automatisierten Abrufverfahrens können diese Gerichte sodann Daten beim zentralen Gericht abfragen. Aufgrund von § 915h Abs. 2 ZPO gibt es bislang zum Beispiel zentrale Mahngerichte beim Amtsgericht Hamburg[105] oder beim Amtsgericht Hagen,[106] nicht aber in Rheinland-Pfalz.

Diese Regelungen sind zwar heute noch in Kraft. Am 29.7.2009 hat der Bundestag jedoch mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung weitgehende Änderungen bei der Ausgestaltung der Schuldnerverzeichnisse beschlossen.[107] In Zukunft beschränkt sich der Technikeinsatz nicht auf vereinzelte Bestimmungen bei der Übermittlung von Schuldnerdaten. Vielmehr wird ein landesweites Internet-Schuldnerverzeichnis eingerichtet werden. Wie bisher wird dieses Schuldnerverzeichnis jedermann einsehen können, der darlegt, Angaben aus dem Schuldnerverzeichnis für die in § 915 Abs. 3 ZPO bestimmte Zwecke zu benötigen. Die Einsichtnahme wird dabei nach Registrierung und Zahlung einer Gebühr im Wege eines automatisierten Abrufverfahrens erfolgen. Nach § 882h ZPO bestimmen die Landesregierungen durch Rechtsverordnung, welches Gericht die Aufgaben des zentralen Vollstreckungsgerichts wahrzunehmen hat. Das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung ist am 31.7.2009 im Bundesgesetzblatt verkündet worden.[108] Die Regelungen zum Schuldnerverzeichnis in den §§ 882b bis 882h ZPO neu treten nach Art. 6 zum 1.1.2013 in Kraft. Lediglich die Bestimmungen, die Bundes- oder Landesregierung zum Erlass von Verordnungen im Zusammenhang mit der Ausgestaltung des künftigen Schuldnerverzeichnisses ermächtigen,[109] sind nach Art. 6 bereits seit dem 1.8.2009 in Kraft.

2.3.2.2 E-Vermögensverzeichnis

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung wurde zudem mit § 802k Abs. 1 ZPO neu auch die Rechtsgrundlage für die Errichtung eines landesweiten Vermögensverzeichnisses geschaffen, welches in elektronischer Form bei einem zentralen

105 HmbGVBl. 1994, 263.
106 GV.NRW 2002, 22.
107 Vgl. zum Gesetzgebungsverfahren: Gesetzesantrag der Länder Baden-Württemberg, Bayern, Hessen, Niedersachsen, Sachsen (BR-Drs. 308/08); Gesetzentwurf des Bundesrats (BT-Drs. 16/10069); Beschlussempfehlung und Bericht (BT-Drs. 16/13432).
108 BGBl. 2009 I, 2258.
109 § 882g Abs. 8 und § 882h Abs. 2 und 3 ZPO.

Vollstreckungsgericht geführt werden wird. Auch die Vermögensverzeichnisse wurden bislang lediglich lokal bei den Gerichten und in Papierform geführt.[110] Neben den Gerichtsvollziehern werden nach § 802k Abs. 2 ZPO neu unter anderem Vollstreckungsgerichte, Insolvenzgerichte und Registergerichte sowie Staatsanwaltschaften Daten aus dem Vermögensverzeichnis zur Einsichtnahme abrufen können. Nach § 802k Abs. 3 ZPO bestimmen die Landesregierungen durch Rechtsverordnung, welches Gericht die Aufgaben des zentralen Vollstreckungsgerichts nach Absatz 1 wahrzunehmen hat. Sie können diese Befugnis auf die Landesjustizverwaltungen übertragen. Die Regelungen zum elektronischen Vermögensverzeichnis treten nach Artikel 6 – wiederum mit Ausnahme der Verordnungsermächtigungen, die schon seit dem 1.8.2009 gelten[111] – zum 1.1.2013 in Kraft.

2.3.2.3 E-Antragstellung für Pfändungs- und Überweisungsbeschluss

Mit dem Justizkommunikationsgesetz wurde mit § 829 Abs. 4 ZPO die Möglichkeit geschaffen, durch Rechtsverordnung Formulare für den Antrag auf Erlass eines Pfändungs- und Überweisungsbeschlusses einzuführen, die elektronisch bearbeitet werden können. Eine derartige Rechtsverordnung gibt es in Rheinland-Pfalz noch nicht. Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung wurde § 829a ZPO eingefügt: Im Falle eines elektronischen Auftrags zur Zwangsvollstreckung im Wege der Pfändung und Überweisung von Geldforderungen auf der Grundlage von Vollstreckungsbescheiden kann nunmehr zukünftig in bestimmten Fällen die Übermittlung der Ausfertigung des Vollstreckungsbescheides in Papierform entbehrlich sein, um eine vollautomatische Auftragserteilung zu erreichen. Gemäß Art. 6 des Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung treten die neuen Änderungen zu § 829a ZPO ebenfalls zum 1.1.2013 in Kraft.

2.3.2.4 E-Akteneinsicht

Darüber hinaus wurde mit dem Justizkommunikationsgesetz § 760 Satz 2 ZPO dahingehend ergänzt, dass Akteneinsicht in die vom Gerichtsvollzieher elektronisch geführten Akten durch Erteilung von Ausdrucken, durch Übermittlung von elektronischen Dokumenten oder durch Wiedergabe auf einem Bildschirm zu erfolgen hat. Eine Online-Einsicht von Rechtsanwälten in die Verfahrensakten – wie es § 299 Abs. 3 ZPO vorsieht – war im Laufe des Gesetzgebungsverfahrens dagegen bewusst nicht in Erwägung gezogen worden.[112] In Rheinland-Pfalz wird eine elektronische Akteneinsicht nach § 760 Satz 2 ZPO – soweit ersichtlich – noch nicht praktiziert.

---

110 BR-Drs. 304/08, 1.
111 § 802k Abs. 3 und 4 ZPO.
112 BT-Drs. 15/4952, 10.

2.3.2.5 E-Bekanntmachungen nach dem ZVG

§ 39 Abs. 1 Zwangsversteigerungsgesetz (ZVG) geht ebenfalls auf das Justizkommunikationsgesetz von 2005 zurück und schafft die Möglichkeit, die Terminsbestimmungen in Zwangsversteigerungsverfahren auch in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem öffentlich bekannt zu machen. Darüber hinaus kann das Gericht seit dem Erlass des 2. Justizmodernisierungsgesetzes nach § 38 Abs. 2 ZVG Wertgutachten und Abschätzungen ebenfalls in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem öffentlich bekannt machen. Die Regelung zu § 39 Abs. 1 ZVG war im Referentenentwurf und Regierungsentwurf zum Justizkommunikationsgesetz noch nicht enthalten. Sie geht zurück auf die Stellungnahme des Bundesrates. Der Bundesrat bemängelte damals, dass der Entwurf keine Regelungen zu elektronischen Bekanntmachungen im Verfahren der Zwangsversteigerung enthalte. Angesichts der praktischen Bedeutung der Zwangsversteigerung und der erheblichen Kosten, die durch die Bekanntmachung von Versteigerungsterminen im Internet bestehen, sei diese Lücke zu schließen.[113]

Mit dem Portal `www.zvg-portal.de` haben die Landesjustizverwaltungen heute eine Plattform zu Informationen über Zwangsversteigerungsverfahren geschaffen. Seit dem 1.3.2007 wurden im Rahmen eines Testbetriebes von verschiedenen Amtsgerichten die Veröffentlichungen zu Zwangsversteigerungsverfahren über dieses Portal bekannt gemacht. Darüber hinaus werden im Zuge einer Pilotierung von einigen Amtsgerichten auch Gutachten, Exposés und Fotos von Objekten zum Download bereitgestellt. Dieses Angebot erfolgt zusätzlich zu den üblichen Veröffentlichungen und ist zur Zeit kostenlos. Daneben veröffentlicht die Firma hansen marketing e.K. im Auftrag von Amtsgerichten verschiedener Bundesländer Zusammenfassungen aus Wertgutachten des jeweils zuständigen Sachverständigen über Objekte, die zur Zwangsversteigerung stehen.[114] Die Wertgutachten enthalten u.a. Straße und Hausnummer sowie ein Foto des Gebäudes, das Aktenzeichen des Zwangsversteigerungsverfahrens, das Grundbuchblatt und die Grundstücksgröße. Derzeit nutzen 18 rheinland-pfälzische Gerichte diesen Service. Des Weiteren sind aber auch die Länder Baden-Württemberg, Bayern, Hessen, Niedersachen, Saarland, Schleswig-Holstein und Thüringen vertreten.

2.3.2.6 E-Versteigerungen

Am 30.7.2009 ist mit dem Gesetz über die Internetversteigerung in der Zwangsvollstreckung (IntVerstZVG)[115] die Versteigerung gepfändeter beweglicher Sachen im Internet als Regelfall neben die öffentliche Versteigerung vor Ort gestellt worden. Der Gesetzgeber hielt die Präsenzversteigerung für nicht mehr zeitgemäß. Im Vergleich zu einer Präsenzversteigerung würde eine Internetversteigerung Vorteile bieten. Der potentielle Bieterkreis sei wegen der leichten Zugänglichkeit erheblich größer als bei einer Präsenzversteigerung. Ein größerer Bieter-

[113] BR-Drs. 609/1/04, 9.
[114] Vgl. hierzu `http://www.hanmark.de` (Zugriff am 22.1.2010).
[115] BGBl. 2009 I, 2474.

kreis bedeute mehr Konkurrenz und damit höhere Erlöse für die versteigerten Gegenstände.[116] Das Gesetz ist am 4.8.2009 im Bundesgesetzblatt verkündet worden und gemäß Art. 9 zum 5.8.2009 in Kraft getreten. § 814 Abs. 2 Nr. 2 ZPO sieht nunmehr vor, dass eine öffentliche Versteigerung als allgemein zugängliche Versteigerung im Internet über eine Versteigerungsplattform erfolgen kann. Nach § 814 Abs. 3 ZPO bestimmen die Landesregierungen für die Versteigerung im Internet durch Rechtsverordnung u.a. den Zeitpunkt, von dem an die Versteigerung zugelassen ist und die zu nutzende Versteigerungsplattform. Diese können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen. Eine derartige Rechtsverordnung haben die Landesregierungen bzw. Landesjustizverwaltungen aber noch nicht erlassen.

2.3.3 Insolvenzverfahren

2.3.3.1 E-Bekanntmachungen

Durch das Gesetz zur Änderung der Insolvenzordnung und anderer Gesetze (InsO-Änderungsgesetz) wurde § 9 InsO mit Wirkung vom 1.12.2001[117] dahingehend novelliert, dass fakultativ neben herkömmlichen Printbekanntmachungen Bekanntmachungen im Internet veröffentlicht werden konnten.[118] Darüber hinaus wurde mit § 9 Abs. 2 Satz 2 und 3 InsO a.F. eine Ermächtigungsgrundlage geschaffen, wonach in einer Verordnung Vorschriften zu treffen sind, die Löschfristen vorsehen sowie Regelungen, die sicherstellen, dass die Veröffentlichungen unversehrt, jederzeit ihrem Ursprung zugeordnet und nach dem Stand der Technik durch Dritte nicht kopiert werden können. Weder der Regierungsentwurf noch der Änderungsvorschlag des Bundesrates sahen diese Verordnungsermächtigung zunächst vor. Diese Bestimmung ist erst auf die Empfehlung des Rechtsausschusses in den Gesetzestext aufgenommen worden.[119] Der Grund hierfür war, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sich inzwischen in das Gesetzgebungsverfahren eingeschaltet hatte und Bedenken hinsichtlich der Eingriffe in das Persönlichkeitsrecht von Schuldnern erhoben hat, die über das hinausgingen, was bei Printveröffentlichungen in Zeitungen und Amtsblättern im Hinblick auf die begrenzten Auswertungsmöglichkeiten hinzunehmen sei.[120] Er forderte, die Internetveröffentlichungen zu befristen und spezielle Vorkehrungen, um die Integrität und die Authentizität zu sichern und eine automatische Übernahme der Daten zu verhindern.

---

116 BT-Drs. 16/13444, 6.

117 BGBl. 2001 I, 2710.

118 Das deutsche Recht folgt dabei einer Entwicklung, die ihren Ursprung in Österreich hatte. Der österreichische Gesetzgeber hatte bereits 1997 die rechtliche Möglichkeit geschaffen, Bekanntmachungen elektronisch über die sog. Insolvenzdatei vorzunehmen. Vgl. hierzu *Duursma/Duursma-Kepplinger*, in: *Plöckinger/Duursma/Helm* (Hrsg.), Aktuelle Entwicklungen im Internet-Recht, 89; *Duursma/Duursma-Kepplinger*, ZInsO 2002, 913; *Mohr*, ZIP 2000, 997.

119 *Riebeling*, 2005, 57.

120 Vgl. hierzu *BfDI*, 19. Tätigkeitsbericht, Tz. 1.5.

Mit Wirkung vom 12.2.2002 hat das Bundesjustizministerium von dieser Verordnungsermächtigung Gebrauch gemacht und mit Zustimmung des Bundesrates die Verordnung zu öffentlichen Bekanntmachungen im Internet (InsOBekV) erlassen.[121] Unter anderem hatten § 9 Abs. 2 Satz 3 Nr. 3 InsO a.F. und § 2 Abs. 1 Satz 3 a.F. InsOBekV damals Regelungen zu einem Kopierschutz enthalten. Damit sollte das massenhafte Herunterladen von Insolvenzdaten verhindert werden.

Mit dem EHUG,[122] das am 1.1.2007 in Kraft getreten ist, wurden die Vorschriften zum Kopierschutz jedoch wieder gestrichen. Dies erfolgte damals auf eine Prüfbitte des Bundesrates hin. Dieser hatte zu Bedenken gegeben, dass sich ein Kopierschutz in der Praxis nicht durchsetzen ließe und diese Vorschriften deshalb derzeit überflüssig seien.[123] Die Bundesregierung stimmte damals dem Vorschlag des Bundesrates zu, die genannte Vorschrift zum Kopierschutz aufzuheben, da nach dem derzeitigen Stand der Technik und wohl auch in absehbarer Zukunft ein Schutz gegen ein Kopieren von Veröffentlichungen im Internet nicht erreicht werden könne. Die Frage, wie dem Schutzzweck der genannten Vorschriften auf andere Weise genügt werden könne, werde – so die Bundesregierung weiter – noch geprüft werden müssen; ggf. werde eine entsprechende Regelung auch in einem anderen Gesetzgebungsverfahren mit stärkerem Sachzusammenhang berücksichtigt werden können.[124]

Mit dem Gesetz zur Vereinfachung des Insolvenzverfahrens (InsVerfVereinfG) vom 13.4.2007,[125] welches seit dem 1.7.2007 in Kraft ist, ist schließlich die Veröffentlichung von Insolvenzdaten zwingend vorgeschrieben worden.[126] Zu Verwirrungen führte im Gesetzgebungsverfahren dabei jedoch zunächst der Regierungsentwurf, welcher eine Streichung der Kopierschutzregelung vorsah, obwohl diese schon durch das EHUG erfolgt ist.[127] Tabelle 1 zeigt die beschriebenen Änderungen an § 9 InsO.

Bis zum Erlass der Rechtsverordnung vom 12.2.2002 haben einige Insolvenzgerichte (Amtsgericht Darmstadt, sächsische Insolvenzgerichte) insolvenzrechtliche Vorgänge auf ihren eigenen Homepages veröffentlicht.[128] Die Länder machten in der Folge dann nur nach und nach davon Gebrauch, die Bekanntmachungen im Internet zu veröffentlichen. Als erstes Land bot Nordrhein-Westfalen eine Internetplattform unter der Adresse `www.insolvenzen-nrw.de` mit Wirkung zum 1.7.2002 an.[129] Inzwischen haben sich alle anderen Bundesländer der Plattform Nordrhein-Westfalens angeschlossen. Das Portal Nordrhein-Westfalens hat sich damit zu einem Gesamtportal entwickelt. Unter `www.insolvenzbekanntmachungen.de` sind heute alle Insolvenzbekanntmachungen sämtlicher deutschen Gerichte abrufbar.

---

121 BGBl. 2002 I, 677.
122 BGBl. 2007 I, 2866.
123 BR-Drs. 942/05, 30.
124 BT-Drs. 16/960, 95.
125 BGBl. 2007 I, 509.
126 Vgl. hierzu *Wimmerer*, DB 2006, 233; *Pape*, NZI 2007, 480; *Sternal*, NZI 2008, 158.
127 BT-Drs. 16/3227, 5.
128 *Bundesregierung*, BT-Drs. 15/181, 2.
129 Vgl. hierzu *Riebeling*, 2005, 62; *Viefhues*, MMR 2002, XIII.

alte Fassung (bis 30.6.2007)	**aktuelle Fassung (ab 1.7.2007)**
(1) Die öffentliche Bekanntmachung erfolgt durch Veröffentlichung in dem für amtliche Bekanntmachungen des Gerichts bestimmten Blatt oder in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem; die Veröffentlichung kann auszugsweise geschehen.	(1) Die öffentliche Bekanntmachung erfolgt durch eine zentrale und länderübergreifende Veröffentlichung im Internet; diese kann auszugsweise geschehen.
Dabei ist der Schuldner genau zu bezeichnen, insbesondere sind seine Anschrift und sein Geschäftszweig anzugeben. Die Bekanntmachung gilt als bewirkt, sobald nach dem Tag der Veröffentlichung zwei weitere Tage verstrichen sind.	
(2) Das Insolvenzgericht kann weitere und wiederholte Veröffentlichungen veranlassen. Das Bundesministerium der Justiz wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Einzelheiten der Veröffentlichung in einem elektronischen Informations- und Kommunikationssystem und die Datenübermittlung an das Unternehmensregister zu regeln.	(2) Das Insolvenzgericht kann weitere Veröffentlichungen veranlassen, soweit dies landesrechtlich bestimmt ist. Das Bundesministerium der Justiz wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Einzelheiten der zentralen und länderübergreifenden Veröffentlichung im Internet zu regeln.
Dabei sind insbesondere Löschungsfristen vorzusehen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen 1. unversehrt, vollständig und aktuell bleiben, 2. jederzeit ihrem Ursprung nach zugeordnet werden können,	
3. nach dem Stand der Technik durch Dritte nicht kopiert werden können.	3. (bereits weggefallen durch EHUG)
(3) Die öffentliche Bekanntmachung genügt zum Nachweis der Zustellung an alle Beteiligten, auch wenn dieses Gesetz neben ihr eine besondere Zustellung vorschreibt.	

Tabelle 1: Änderungen an § 9 InsO durch EHUG InsVerfVereinfG.

2.3.3.2 E-Tabellen und E-Verzeichnisse

Mit Ausnahme der Insolvenzbekanntmachungen beantwortet die InsO die Frage des Einsatzes von IT nur rudimentär.[130] So bestimmt § 5 Abs. 4 InsO bei den Verfahrensgrundsätzen der Insolvenzordnung, dass Tabellen und Verzeichnisse maschinell hergestellt und bearbeitet werden können. Die Landesregierungen werden damit ermächtigt, durch Rechtsverordnung nähere Bestimmungen über die Führung der Tabellen und Verzeichnisse, ihre elektronische Einreichung sowie die elektronische Einreichung der dazugehörigen Dokumente und deren Aufbewahrung zu treffen. Dabei können sie auch Vorgaben für die Datenformate der elektronischen Einreichung machen. Die Landesregierungen können die Ermächtigung auf die Landesjustizverwaltungen übertragen. Eine derartige Rechtsverordnung gibt es in Rheinland-Pfalz noch nicht. In der

[130] Dies wird auch in der Dissertation von *Riebeling*, 2005 deutlich, der einen großen Teil seiner Arbeit den Bekanntmachungen nach der InsO gewidmet hat.

Literatur ist diese Vorschrift des Öfteren kritisiert worden. Ebenso gut hätte auch geregelt werden können, dass im Insolvenzverfahren Papier im Format DIN A 3 benutzt werden dürfe; das Zustandekommen von § 5 Abs. 4 InsO sei allenfalls mit naiver Begeisterung für technische Hilfsmittel, gepaart mit Regelungseuphorie zu erklären, die in ihrer spürbar unreflektierten Angst vor Regelungsdefiziten eher Rückständigkeit als Fortschrittlichkeit offenbare.[131]

2.3.3.3 E-Forderungsanmeldung

§ 174 Abs. 4 InsO bestimmt, dass die Forderungsanmeldung auch durch Übermittlung eines elektronischen Dokuments erfolgen kann, wenn der Insolvenzverwalter der Übermittlung elektronischer Dokumente ausdrücklich zugestimmt hat. In diesem Fall sollen die Urkunden, aus denen sich die Forderung ergibt, unverzüglich nachgereicht werden. § 174 Abs. 4 InsO ist mit dem Justizkommunikationsgesetz von 2005 eingeführt worden. Die Einschränkung, dass der Insolvenzverwalter der elektronischen Übermittlung der Anmeldung ausdrücklich zugestimmt haben muss, soll sicherstellen, dass elektronische Anmeldungen in einer vom Insolvenzverwalter verwendbaren Form erfolgen.[132] Einige Insolvenzverwalter verfügen heute bereits über eine eigene Homepage. Auf diesen bieten sie teilweise auch Online-Forderungsanmeldungen an, bei der über ein Internetformular der Gläubiger die Daten erfassen kann und an den Insolvenzverwalter übertragen kann.

2.3.3.4 E-Kommunikation nach § 4 InsO und E-Mitteilungen

Nach § 4 InsO gelten für das Insolvenzverfahren, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften der Zivilprozessordnung entsprechend. Aufgrund von § 4 InsO i.V.m. § 130a ZPO ist es daher möglich, elektronische Schriftsätze an das Gericht einzureichen, vorausgesetzt die entsprechende Rechtsverordnung ist bereits erlassen worden.[133] Bislang trifft dies allerdings für keines der Bundesländer zu. Über § 4 InsO sind auch die Zustellungsvorschriften der ZPO anzuwenden. Daraus folgt, dass elektronische Zustellungen nach Maßgabe des § 174 Abs. 3 ZPO zulässig sind. Demnach können also Insolvenzgerichte unter den Voraussetzungen des § 174 Abs. 3 ZPO Dokumente zum Beispiel an den Insolvenzverwalter und an Gläubiger elektronisch zustellen.[134] Soweit ersichtlich, wird dies jedoch an den Gerichten noch nicht getan. Wie im Zivilverfahren ist im Übrigen auch im außerförmlichen Bereich des Insolvenzverfahrens die Möglichkeit gegeben, Mitteilungen des Gerichts oder des Insolvenzverwalters per E-Mail zu versenden.[135] Es ist jedoch davon auszugehen, dass auch hiervon bislang die wenigsten Richter Gebrauch machen. Nach § 4 InsO i.V.m. § 299 ZPO kann Einsicht auch in die Akten des Insolvenzverfahrens genommen werden. Die diesbezüglichen elektronischen

131 Vgl. hierzu *Riebeling*, 2005, 5 m.w.N.
132 BT-Drs. 15/4067, 54.
133 *Riebeling*, 2005, 12.
134 *Keller*, NZI 2002, 581.
135 Vgl. hierzu für das Gericht: §§ 215 Abs. 1 Satz 2, 258 Abs. 3 Satz 2 InsO. Und für den Insolvenzverwalter: §§ 158 Abs. 2 Satz 1, 160 Satz 1, 262 Satz 1 InsO. Nähere Ausführungen auch bei *Riebeling*, 2005, 28.

Akteneinsichtsrechte gelten daher entsprechend. Dabei ist allerdings zu berücksichtigen, dass es im Insolvenzverfahren spezielle Einsichtsrechte gibt, die dem nach § 4 InsO i.V.m. § 299 ZPO vorgehen[136] und mangels entsprechender Regelungen ohne Technikeinsatz wahrgenommen werden müssen. Hierzu gehören die Einsichtsrechte nach §§ 66 Abs. 2 Satz 2, 150 Satz 2, 154, 175 Abs. 1 Satz 2 und 234 InsO.

2.3.4 Grundbuchordnung

2.3.4.1 E-Grundbuch

Das Grundbuch wurde bis weit über die Mitte des 20. Jahrhunderts in Form gebundener Bände geführt. Dies brachte es mit sich, dass alle Eintragungen handschriftlich durchgeführt werden mussten. Weil sich dies als umständlich erwies, führte man in den 60er Jahren ein Loseblattgrundbuch ein. Dadurch wurde erstmals die Verwendung normaler Schreibmaschinen möglich. In der Folge ging man in den 80er Jahren zu automationsunterstützten Verfahren über, die die Dateneingabe am Bildschirm, die Mehrfachverwendung einmal eingegebener Daten und den Aufbau von elektronischen Suchverzeichnissen zuließen.

Am 24.12.1993 wurde das Registerverfahrensbeschleunigungsgesetz (RegVGB) vom 20.12.1993 verkündet.[137] § 126 Grundbuchordnung (GBO) gestattet seitdem den Landesregierungen die elektronische Führung des Grundbuchs. § 126 Abs. 1 GBO ist hierfür die entsprechende Ermächtigungsgrundlage zum Erlass einer diesbezüglichen Rechtsverordnung. Die Einführung des elektronischen Grundbuchs ist inzwischen in nahezu allen Bundesländern erfolgt,[138] in Rheinland-Pfalz geschah dies am 1.11.2000.[139] Eine wichtige Neuerung dieses Gesetzes war auch die Einführung des automatisierten Abrufverfahrens in §§ 133 ff. GBO. Durch das automatisierte Abrufverfahren wurde die Einsicht in das Grundbuch erleichtert. Gerichte, Behörden, Notare und öffentliche Vermessungsingenieure müssen heute das berechtigte Interesse an der Einsicht nicht mehr darlegen. Diese Stellen dürfen das Abrufverfahren uneingeschränkt nutzen. Für andere Stellen gibt es bestimmte Einschränkungen; insbesondere bedarf es der Angabe der Gründe für den Abruf, wenn auch in schematisierter Form. Die Einrichtung eines automatisierten Abrufverfahrens ist gemäß § 133 Abs. 2 Satz 1 GBO nur mit Genehmigung der Landesjustizverwaltung zulässig. In Rheinland-Pfalz ist die zuständige Behörde für die Erteilung einer Genehmigung – sowohl für das uneingeschränkte als auch das eingeschränkte Abrufverfahren – der Präsident des Oberlandesgerichts Zweibrücken.[140] In allen Bundesländern mit Ausnahme von Mecklenburg-Vorpommern besteht heute die Möglichkeit, in das Grundbuch auf elektronischem Wege Einsicht zu nehmen. Die gemeinsame Internetplattform `www.grundbuch-portal.de` der Länder bietet allgemeine Informationen über die

136 *Hesseler*, ZInsO 2001, 882; *Graf/Wunsch*, ZIP 2001, 1800.
137 BGBl. 1993 I, 2182.
138 BT-Drs. 16/12319, 16.
139 § 6 der Landesverordnung über das maschinell geführte Grundbuch vom 19.10.2000, GVBl. 2000, 442.
140 § 4 der Landesverordnung über das maschinell geführte Grundbuch vom 19.10.2000, GVBl. 2000, 442.

Online-Einsicht. Bezüglich weiterer detaillierter Informationen wird auf die einzelnen Landesseiten der Justizministerien verwiesen.

2.3.4.2 E-Grundakte

Mit dem Gesetz zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Akte im Grundbuchverfahren sowie zur Änderung weiterer grundbuch-, register- und kostenrechtlichen Vorschriften[141] vom 11.8.2009 wurde das Grundbuchrecht weiter modernisiert.[142] In dem Gesetz wurde mit § 135 Abs. 2 GBO die Rechtsgrundlage für die Einführung der elektronischen Grundakte geschaffen. § 135 Abs. 2 GBO bestimmt nunmehr, dass die Landesregierungen ermächtigt werden, durch Rechtsverordnung den Zeitpunkt zu bestimmen, von dem an die Grundakten elektronisch geführt werden können. Die Ermächtigung kann nach Abs. 3 der Vorschrift auf die Landesjustizverwaltungen übertragen werden. Dabei kann die Anordnung auf einzelne Grundbuchämter oder auf Teile des bei einem Grundbuchamt geführten Grundaktenbestandes beschränkt werden. In diese Grundakte kann der oben genannte Personenkreis gemäß § 139 Abs. 3 GBO nach den gleichen Kriterien automatisiert einsehen. Die elektronische Grundakte wurde nicht auf neu eingehende elektronische Dokumente beschränkt. Das Gesetz eröffnet vielmehr nach § 138 Abs. 1 GBO die Möglichkeit, die künftig noch in Papierform eingehenden Dokumente oder vom Grundbuchamt selbst gefertigten Dokumente in die elektronische Form zu übertragen. Die Originaldokumente sollen anschließend ausgesondert werden können. Nach Artikel 5 Abs. 1 des ERVGBG traten die entsprechenden Vorschriften zur Einführung der Grundakte zum 1.10.2009 in Kraft. Eine Rechtsverordnung zur Einführung der elektronischen Grundakte gibt es derzeit noch in keinem Bundesland, d.h. die Grundakten werden heute noch papiergebunden geführt.

2.3.4.3 E-Übermittlung von Schriftsätzen

Mit § 135 Abs. 1 GBO wurde – ebenfalls durch das ERVGBG – die Grundlage für die Einführung des elektronischen Rechtsverkehrs geschaffen. Die Vorschrift ermöglicht es allen Verfahrensbeteiligten, ihre Schriftsätze und Erklärungen als elektronisches Dokument einzureichen. Wie etwa § 130a ZPO sieht das Gesetz in § 135 Abs. 1 Satz 2 Nr. 1 GBO vor, dass die jeweiligen Landesjustizverwaltungen Zeit und Umfang der Einführung des elektronischen Rechtsverkehrs erst noch zu bestimmen haben. Die elektronische Einreichung von Dokumenten wurde dabei gemäß § 135 Abs. 1 Satz 2 Nr. 4 GBO nur für Notare verpflichtend eingeführt. Nach § 15 Abs. 3 Satz 2 Bundesnotarordnung (BNotO) muss nämlich jeder Notar seit dem 1.4.2006 über die notwendigen technischen Einrichtungen verfügen. Für die anderen in Betracht kommenden Kommunikationspartner, Kreditunternehmen und Behörden, wurde die Teilnahme am elektronischen Rechtsverkehr nicht vorgeschrieben. Erst wenn bei diesem

[141] BGBl. 2009 I, 2713. Wichtige Drucksachen: Regierungsentwurf (BT-Drs. 16/12319); Stellungnahme Bundesrat (BR-Drs. 66/09); Beschlussempfehlung und Bericht (BT-Drs. 16/13437).

[142] Vgl. hierzu *Aufderhaar/Jaeger*, ZfIR 2009, 681.

Personenkreis die entsprechenden technischen Vorkehrungen flächendeckend verbreitet sind, soll die Teilnahme am elektronischen Rechtsverkehr für alle Beteiligten verbindlich eingeführt werden.[143] Bislang existiert noch in keinem Bundesland eine Rechtsverordnung zur Einführung des elektronischen Grundbuchverkehrs.

2.3.4.4 E-Eigentümerverzeichnis

Mit dem RegVGB wurde § 12a GBO eingeführt. Nach § 12a GBO können Eigentümerverzeichnisse statt in Papierform auch in maschineller Form geführt werden. Davor wurden sie in Karteiform, in Loseblattform oder in Buchform geführt. Für die Führung des Eigentümerverzeichnisses ist die Genehmigung der Landesjustizverwaltung erforderlich. Wird ein Verzeichnis elektronisch geführt, so gelten die Vorschriften der § 126 Abs. 2 und § 133 GBO entsprechend. Dies bedeutet also insbesondere, dass für die Einrichtung eines automatisierten Abrufverfahrens die für das maschinell geführte Grundbuch aufgestellten Anforderungen gelten.[144]

2.3.5 Handelsgesetzbuch

2.3.5.1 E-Handelsregister

Die Grundlagen für das elektronische Handelsregister wurden mit dem RegVBG geschaffen. Dieses gab den Ländern die Möglichkeit, vergleichbar mit dem Grundbuch, das Handelsregister maschinell zu führen und ein Online-Abrufverfahren von Daten aus dem Handelsregister zuzulassen. Im Hinblick auf das Abrufverfahren sah das RegVBG dabei vor, dass von diesem sowohl öffentliche als auch private Stellen Gebrauch machen dürfen. Voraussetzung war allerdings eine vorherige Genehmigung der Landesjustizverwaltung. Diese durfte öffentlichen Stellen erteilt werden, soweit der Abruf der Erfüllung der gesetzlich zugewiesenen Aufgaben diente.[145] Bei Privaten war Voraussetzung, dass der Abruf zur Wahrnehmung eines berechtigten beruflichen oder gewerblichen Interesses erfolgt.[146] Der Abruf war auf Daten von Eintragungen in das Handelsregister sowie die zum Handelsregister eingereichten aktuellen Gesellschafterlisten und jeweils gültigen Satzungen beschränkt.[147] Die Länder machten von diesen ihnen durch das RegVBG geschaffenen Möglichkeiten jedoch lange keinen Gebrauch. Auch in Rheinland-Pfalz wurde das Handelsregister erst am 1.6.2005 in elektronischer Form eingeführt.[148] Die

[143] BT-Drs. 16/12319, 16.

[144] Daneben gestattet § 12a GBO auch die Verwendung des Liegenschaftskatasters. Dieses wird jedoch vom Katasteramt geführt und soll daher hier nicht weiter vertieft werden.

[145] Vgl. § 9a Abs. 2 Satz 2 Nr. 1 HGB, Fassung 1993.

[146] Vgl. § 9a Abs. 2 Satz 2 Nr. 2 HGB, Fassung 1993.

[147] § 9a Abs. 1 HGB, Fassung 1993.

[148] § 1 und § 7 der Landesverordnung über das maschinell geführte Handels-, Genossenschafts-, Partnerschafts- und Vereinsregister vom 4.5.2005, GVBl. 2005, 179.

Durchführung des Abrufverfahrens wurde dabei ebenfalls dem Pfälzischen Oberlandesgericht Zweibrücken zugewiesen.[149]

Obwohl das maschinell geführte Grundbuch und das Abrufverfahren von den Ländern noch nicht eingeführt wurde, hat der Gesetzgeber bereits im Jahr 2001 mit dem Gesetz über elektronische Register und Justizkosten für Telekommunikation[150] (ERJuKoG) weitere Vorschriften für das elektronische Handelsregister erlassen. So hatte er vor allem den Genehmigungsvorbehalt für die Teilnahme an einem automatisierten Abrufverfahren abgeschafft und diesen durch einen Verbotsvorbehalt ersetzt. D.h. von nun an konnte jeder – nach Zahlung einer Gebühr – das Handelsregister auch von zu Hause aus im Online-Verfahren einsehen. Nur im Fall einer missbräuchlichen Anwendung konnte er vom Abrufverfahren ausgeschlossen werden. Der Gesetzgeber hat die Änderungen zum einen mit dem hohen Verwaltungsaufwand begründet, der durch eine Genehmigung entstehen würde. Zum anderen hielt er das Erfordernis einer Genehmigung auch nicht mit den europäischen Regelungen für vereinbar, welche voraussetzen, dass jedermann in das Handelsregister einsehen kann.[151] Mit dem 1. Justizmodernisierungsgesetz von 2004 wurde der Online-Abruf auf alle Handelsregisterdaten erweitert.[152]

Mit dem EHUG[153] wurde schließlich bestimmt, dass das Handelsregister von den Gerichten elektronisch geführt werden muss.[154] Entsprechendes wurde in § 8 Abs. 1 Handelsgesetzbuch (HGB) normiert. Hintergrund dieses Gesetzes waren europarechtliche Vorgaben. So wurde mit dem Gesetz die Publizitätsrichtlinie in der Fassung des Jahres 2003[155] umgesetzt. Art. 3 Abs. 1 der Richtlinie schreibt vor, dass in jedem Mitgliedstaat entweder bei einem zentralen Register oder bei einem Handels- oder Gesellschaftsregister für jede der dort eingetragenen Gesellschaften eine Akte angelegt wird. Seit 2003 bestimmt die Richtlinie, dass Dokumente und Angaben spätestens bis zum 1.1.2007 in elektronischer Form in der Akte hinterlegt werden müssen und dass Dokumente aus der Zeit vor 2007 auf Antrag in elektronische Form zu bringen sind. Damit macht die Richtlinie also die Führung eines elektronischen Handelsregisters erforderlich. Diesen Vorgaben sind inzwischen alle Bundesländer nachgekommen.

2.3.5.2 E-Anmeldung zum Handelsregister

Mit der zwingenden Einführung des elektronischen Handelsregister war auch die Vorgabe verbunden, die Dokumente zum Handelsregister ab dem 1.1.2007 elektronisch einzureichen. Auch dies beruhte auf der Publizitätsrichtlinie von 2003. So bestimmt Art. 3 Abs. 2 Satz 2: „Die Mitgliedstaaten sorgen dafür, dass die Gesellschaften und sonstige anmelde- oder mitwirkungspflichtige Personen und Stellen alle Urkunden und Angaben (...) spätestens ab dem

[149] § 4 der Landesverordnung über das maschinell geführte Handels-, Genossenschafts-, Partnerschafts- und Vereinsregister vom 4.5.2005, GVBl. 2005, 179.
[150] BGBl. 2001 I, 3422.
[151] BT-Drs. 14/6855, 18.
[152] BGBl. 2004 I, 2198. Zur Begründung vgl. hierzu Beschlussempfehlung und Bericht, BT-Drs. 15/3482, 25.
[153] BGBl. 2006 I, 2553.
[154] Überblicksaufsätze *Noack*, NZG 2006, 801; *Seibert/Decker*, DB 2006, 2446.
[155] ABl. EG L 221, 13.

1.1.2007 in elektronischer Form einreichen können.“ Und weiter in Art. 3 Abs. 2 Satz 3: „Die Mitgliedstaaten können außerdem den Gesellschaften aller oder bestimmter Rechtsformen die Einreichung aller oder eines Teils der betreffenden Urkunden und Angaben in elektronischer Form vorschreiben.“ In Umsetzung dieser Richtlinie bestimmt § 12 Abs. 1 und 2 HGB heute, dass Anmeldungen zur Eintragung in das Handelsregister sowie Dokumente – zwingend – elektronisch in beglaubigter Form einzutragen sind.[156] Die Landesverordnung von Rheinland-Pfalz hat die elektronische Einreichung ab dem 1.1.2007 ermöglicht.[157] Nach Art. 61 Abs. 1 EGHGB konnten die Landesregierungen noch bis Ende 2009 die Einreichung in Papierform gestatten. In Rheinland-Pfalz war dies bis zum 30.9.2007 der Fall.[158] Auch alle anderen Bundesländer verfügen nunmehr über entsprechende Rechtsverordnungen.

2.3.5.3 E-Bekanntmachungen

Des Weiteren wurde mit dem EHUG verbindlich festgeschrieben, dass Bekanntmachungen nur noch elektronisch erfolgen können.[159] In § 10 HGB ist bestimmt, dass dies durch das Gericht in einem elektronischen Informations- und Kommunikationssystem zu erfolgen hat.[160] § 9 Abs. 1 Satz 4 i.V.m. § 10 HGB ermöglicht es jedoch den Ländern, auch ein gemeinsames Kommunikationsmedium zu bestimmen. Dies haben sie getan. Seit dem Inkrafttreten des EHUG veröffentlichen die Registergerichte aller Bundesländer die Bekanntmachungen nach dem Handelsgesetzbuch auf der Seite `www.handelsregisterbekanntmachungen.de`. Diese elektronische Form der Veröffentlichung ist durch die Richtlinie nicht zwingend vorgeschrieben. Die Mitgliedstaaten haben vielmehr von Art. 3 Abs. 4 Gebrauch gemacht, wonach sie beschließen können, „die Bekanntmachung im Amtsblatt durch eine andere ebenso wirksame Form der Veröffentlichung zu ersetzen, die zumindest die Verwendung eines Systems voraussetzt, mit dem die offen gelegten Informationen chronologisch geordnet über eine zentrale elektronische Plattform zugänglich gemacht werden.“

2.3.5.4 E-Unternehmensregister

Mit dem EHUG wurde zudem ein zentrales Unternehmensregister geschaffen. Die Errichtung dieses Registers beruhte auf der Publizitätsrichtlinie von 2003[161] und auf der Transparenz-

156 Vgl. hierzu *Jeep/ Wiedemann*, NJW 2007, 2439.

157 §§ 5, 6 Abs. 2 der Landesverordnung über den elektronischen Rechtsverkehr mit den für die Führung der Handels-, Genossenschafts- und Partnerschaftsregister zuständigen Amtsgerichten vom 12.12.2006, GVBl. 2006, 444.

158 §§ 5, 6 Abs. 2 der Landesverordnung über den elektronischen Rechtsverkehr mit den für die Führung der Handels-, Genossenschafts- und Partnerschaftsregister zuständigen Amtsgerichten vom 12.12.2006, GVBl. 2006, 444.

159 Nach Art. 61 Abs. 4 EGHGB war die Zeitungspublizität jedoch bis zum 31.12.2008 zwingend.

160 Dies bedeutet, dass die Bekanntmachungen für jedes der 16 Bundesländer in einem gesondert zu bestimmenden Portal zu erfolgen haben. Vgl. hierzu etwa *Schlotter*, BB 2007, 2.

161 Vgl. Art. 3 Abs. 1 und 2: „eine Akte“.

richtlinie von 2004.[162] Im HGB finden sich die entsprechenden Vorschriften für das zentrale Unternehmensregister in § 8b. Nach der Gesetzesbegründung soll das Unternehmensregister die Informationen aus mehreren Datenbanken an einer Stelle zentral bündeln und dadurch die Markttransparenz fördern, die ein moderner Wettbewerb erfordert.[163] Die Führung dieses Registers obliegt grundsätzlich dem Bundesministerium der Justiz nach § 8b Abs. 1 HGB. Sie kann aber gemäß § 9a HGB durch Beleihung übertragen werden. Derzeit wird es vom Betreiber des elektronischen Bundesanzeigers geführt. Auch die Daten von rheinland-pfälzischen Gerichten sind in diesem Register seit dem 1.1.2007 zu finden.

2.4 Zusammenfassung

Für Modernisierungsprozesse in der Justiz bedarf es eine eigenständige Begrifflichkeit. Im Unterschied zum elektronischen Rechtsverkehr, welcher nur die Beziehungen nach außen erfasst, umfasst der Begriff der elektronischen Justiz einen weiten, heterogenen Bereich unterschiedlicher Möglichkeiten des Einsatzes von Informations- und Kommunikationstechniken in der Justiz. Dabei ist der Begriff nicht gleichbedeutend mit dem des elektronischen Geschäftsverkehrs, der nur den materiellen Rechtsverkehr erfasst.

Das Ziel von technischen Modernisierungsprozessen in der Justiz besteht darin, das Verfahren zu beschleunigen und Kosten sowohl für die Justiz, als auch für die Anwaltschaft, die Notare und die Parteien und Verfahrensbeteiligten zu minimieren. Oftmals wird als Ziel der Modernisierungsprozesse auch die Transparenz von Verfahrensabläufen angegeben. Im Unterschied zum E-Government spielt die Bürgernähe als Ziel der Modernisierungsprozesse eher eine untergeordnete Rolle.

Der Modernisierungsprozess in der Justiz ist bereits weit fortgeschritten. Im Zivilverfahren gibt es seit längerem schon das elektronische Mahnverfahren, außerdem können inzwischen an verschiedenen Gerichten elektronische Dokumente eingereicht werden. Des Weiteren werden die Bekanntmachungen im Internet veröffentlicht und beim Bundesgerichtshof können in Patentstreitigkeiten Akten elektronisch geführt werden. Zudem gibt es ein zentrales Schutzschriftenregister. Auch wird die Einbeziehung von ELENA beim Prozesskostenhilfeverfahren diskutiert. Im Zwangsvollstreckungs- und Zwangsversteigerungsverfahren ist der Modernisierungsprozess noch nicht so weit vorangeschritten wie im Zivilverfahren. Bislang gab es nur vereinzelt elektronische Anwendungen. Wenn ab dem 1.1.2013 jedoch das zentrale Schuldnerverzeichnis und das zentrale Vermögensverzeichnis eingesetzt werden, wird sich dies grundlegend ändern. Im Insolvenzverfahren sind vor allem die Insolvenzbekanntmachungen von Bedeutung. Die weiteren Anwendungen ergeben sich hauptsächlich aufgrund der Verweisungen der InsO auf die ZPO und spielen bislang noch eine eher untergeordnete Rolle. Als sehr weit fortgeschritten kann der Modernisierungsprozess dagegen im Grundbuchverfahren und im Handelsgesetzbuch bezeich-

[162] ABl. EG L 390, 38. Vgl. Art. 21 Abs. 2: „amtlich bestelltes System für die zentrale Speicherung vorgeschriebener Informationen“.

[163] Vgl. BT-Drs. 16/960, 39.

net werden. Das Grundbuch wurde fast komplett auf den elektronischen Betrieb umgestellt. Es ist zu erwarten, dass mit den neuen Änderungen in der GBO der Modernisierungsprozess in tatsächlicher Hinsicht schnell weiter voranschreiten wird. Als fast schon abgeschlossen kann der Elektronisierungsprozess schließlich im Handelsgesetzbuch bezeichnet werden. Hierfür waren jedoch auch europarechtliche Vorgaben maßgeblich. Die nachfolgende Tabelle führt die wichtigsten Modernisierungen auf.

	Elektronische Anwendungen	**Rechtsgrundlage**	**Realisierung**
Allgemein	Klageeinreichung	§ 130a ZPO	BGH 11/2001; Land (–)
	Zustellungen	§ 174 Abs. 3 ZPO	BGH 7/2002, Land (–)
	Formlose Mitteilungen	z.B. §§ 104 Abs. 1 Satz 4, 251a Abs. 2 Satz 3 ZPO	Einzelfall
	Akteneinsicht	§ 299 Abs. 3 ZPO	(–)
Speziell	Mahnverfahren	§ 689 Abs. 1 ZPO	seit 1.10.1988
	öff. Bekanntmachungen	z.B. § 9 InsO	seit 1.12.2007 zwingend
	Schutzschriften	(–)	Land (–)
Projekte	ELENA und PKH	ELENA-VerfahrensG	(–)
Elektr. Register	Schuldnerverzeichnis	§ 882h Abs. 1 ZPO neu	ab 1.1.2013
	Vermögensverzeichnis	§ 802k Abs. 1 ZPO neu	ab 1.1.2013
	Grundbuch	§ 126 GBO	seit 1.11.2000
	Handelsregister	§ 8 HGB	seit 1.1.2007
	Unternehmensregister	§ 8b Abs. 1 HGB	seit 1.1.2007
Weitere Besonderheiten	Versteigerungen	§ 814 Abs. 2 Nr. 2 ZPO	(–)
	Antrag für PfüB	§ 829a ZPO	ab 1.1.2013
	Forderungsanmeldung	§ 174 Abs. 4 InsO	Einzelfall
	Anmeldung Handelsreg.	§ 12 Abs. 1 HGB	seit 1.1.2007
Interner Bereich	Elektr. Akte	§ 298a ZPO	BGH (–), Land (–)
	Elektr. Grundakte	§ 135 Abs. 2 GBO	(–)
	Tabellen und Verzeichnisse	§ 5 Abs. 4 InsO	(–)
	Eigentümerverzeichnis	§ 12a GBO	Einzelfall

Tabelle 2: Elektronische Anwendungen in den untersuchten Verfahrensordnungen.

Kapitel 3

Herausforderung für den Datenschutz

Nachdem die Zielvorgaben und die IT-Anwendungen vorgestellt wurden, wird im Folgenden auf datenschutzrechtliche Herausforderungen der neuen Techniken eingegangen. Dazu wird zunächst allgemein dargestellt, welche Besonderheiten sich durch die Informationsverarbeitung mit Hilfe von IT-Systemen ergeben. Da für die Übermittlung in der Regel das Internet und dessen Protokolle eingesetzt werden, widmen sich die folgenden Abschnitte den entsprechenden technischen Grundlagen und den sich daraus ergebenden konkreten Gefährdungen.

3.1 Eigenheiten elektronischer Datenverarbeitung

Eine papiergestützte Verarbeitung, Speicherung und Übertragung von Informationen erfolgt typischerweise mit Hilfe von Akten, Schriftstücken oder Vermerken. Beim kompletten oder teilweisen Übergang zu einer elektronischen Datenverarbeitung ergeben sich in heutigen IT-Systemen aufgrund des Formats und der dadurch gegebenen Automatisierbarkeit eine Vielzahl von neuen oder zumindest erheblich effizienteren Nutzungsmöglichkeiten. Sofern diese personenbezogene Daten umfassen, sind sie unter dem Gesichtspunkt des Datenschutzrechts zu betrachten. Wesentliche Aspekte sind die Möglichkeit der Aufbereitung, der vereinfachte Zugriff, die fehlende Wahrnehmbarkeit ohne technische Hilfsmittel, die Flüchtigkeit von Informationen bei elektronischer Speicherung und die langfristige Verfügbarkeit.[164]

- *Aufbereitungsmöglichkeiten:* Informationen, die elektronisch vorliegen, können sehr leicht aufbereitet und weiterverarbeitet werden. Das bedeutet etwa, dass Datensätze leicht nach Namen, Aktenzeichen oder Gegenstand des Verfahrens sortiert und gefiltert werden können. Auch ist ein automatisiertes Abgleichen und/oder Verknüpfen mit anderen Datenbeständen in kurzer Zeit möglich. Über eine Volltextsuche kann darüber hinaus auch auf unstrukturierte Inhaltsdaten zugegriffen werden. Somit lassen sich leicht Profile erstellen.[165]

[164] Vgl. hierzu etwa auch *Yildirim*, 2004, 55 ff.; *DSB-Konferenz*, 2003, 26 ff.; *DSB-Konferenz*, 2006, 5 f.
[165] *DSB-Konferenz*, 2006, 5.

Im Vergleich dazu müssen bei konventioneller Verarbeitung Daten manuell erfasst werden. Eine Sortierung oder Filterung ist etwa mit Hilfe von Karteikarten möglich, aber nur sofern eine entsprechende Indizierung gegeben ist. Liegt der Aktenbestand z.B. nur nach Aktenzeichen sortiert vor, so ist es nur mit hohem Aufwand möglich, alle Akten mit einer bestimmten Person als Verfahrensbeteiligtem zu finden. Auch sind größere Anstrengungen für einen Abgleich mit anderen Datensätzen erforderlich.

- *Vereinfachter Zugriff:* Bei elektronischer Verarbeitung ist es möglich, dass mehrere Personen gleichzeitig – ggf. sogar von unterschiedlichen Orten aus – die Informationen einsehen. Dabei ist die Latenzzeit niedrig, selbst wenn eine vorherige Übertragung über eine größere Entfernung erforderlich ist. Eine Einsicht elektronisch aufbereiteter Daten ist also in Sekundenschnelle möglich.

  Im papiergebundenen Verfahren existiert dagegen in der Regel nur ein Originaldokument, das immer nur von einer bestimmten Person an einem bestimmten Ort eingesehen werden kann. Die Einsichtnahme gestaltet sich aufwändig, weil sich entweder die betreffende Person zum Dokument begeben oder das Dokument zur betreffenden Person kosten- und zeitaufwändig verschickt werden muss.

- *Unsichtbarkeit:* Elektronisch gespeicherte und übertragene Daten sind körperlos und ohne technische Hilfsmittel nicht lesbar.[166] Dies kann dazu führen, dass Nutzer nicht mehr in der Lage sind, zu prüfen, ob die Daten tatsächlich in der von ihnen gewollten Weise verarbeitet, gespeichert oder gelöscht wurden. Zudem kann auch nicht überprüft werden, ob es sich um eine Kopie oder das Original handelt.[167]

  Im papiergebundenen Verfahren sind keine technischen Hilfsmittel erforderlich, um das Dokument zu lesen; auch lassen sich Original und Kopie besser voneinander unterscheiden.

- *Flüchtigkeit:* Elektronisch gespeicherte Informationen können verloren gehen, ohne dass irgendwelche Spuren zurück bleiben. Ursache können Entmagnetisierung von Datenträgern durch Alterung, Temperatur, Luftfeuchtigkeit, äußere Magnetfelder, versehentliches Löschen oder Überschreiben von Dateien sowie technisches Versagen von Festplatten oder anderen Speichermedien wie CDs, DVDs, Magnetbänder sein.[168]

  Im papiergebundenen Verfahren kann es zwar auch vorkommen, dass ein Dokument verloren geht. Die Wahrscheinlichkeit aber, dass ein Dokument dergestalt vernichtet wird, dass es nicht mehr rekonstruiert werden kann, ist jedoch niedriger.

- *Langfristige Verfügbarkeit:* Elektronisch gespeicherte Informationen können in beliebiger Zahl kopiert werden. Eine Unterscheidung von Original und Kopie ist nicht möglich.[169]

[166] *DSB-Konferenz*, 2003, 26.
[167] *DSB-Konferenz*, 2003, 26.
[168] *DSB-Konferenz*, 2003, 26.
[169] *DSB-Konferenz*, 2003, 26.

Wenn elektronisch aufbereitete Informationen einmal verbreitet sind – zum Beispiel im Internet –, können sie nicht mehr gelöscht werden. Sie bleiben dauerhaft verfügbar.

Im herkömmlichen papiergebundenen Verfahren gestaltet sich das Erstellen von Kopien dagegen aufwändiger. Die Kopie kann vom Original unterschieden werden und Papierkopien lassen sich zudem schnell vernichten.

3.2 Technische Grundlagen

3.2.1 Internet-basierte Kommunikation

Der Bund und die Länder[170] betreiben so genannte Verwaltungsnetze, die zur Verbindung von Behörden untereinander dienen und als großes zusammenhängendes Netz aufgefasst werden können. Sie nutzen zwar intern eigene Leitungen, gestatten aber auch über definierte und kontrollierte Übergänge die Kommunikation mit Benutzern, die über das Internet erreichbar sind (Parteien, Anwälte, Notare).

3.2.1.1 Schichtenmodell

Anhand eines Schichtenmodells bestehend aus Ebenen, die verschiedene Aufgaben bei der Kommunikation erfüllen, lässt sich der Ablauf einer Netzwerkkommunikation beschreiben.[171] Die allgemeine Architektur des so genannten OSI-Referenzmodells mit sieben Schichten findet beim Internet in einer vereinfachten Form als TCP/IP-Referenzmodell mit lediglich vier Ebenen wieder, nämlich der Anwendungsschicht, Transportschicht, Internetschicht sowie Netzzugangsschicht.[172] Bei jeder Kommunikation über das Internet werden die gesendeten Daten durch Protokolle der entsprechenden Schicht auf beiden Seiten sowie teilweise auch auf den an der Weiterleitung beteiligten Systemen verarbeitet. Abbildung 1 zeigt das TCP/IP-Referenzmodell mit typischen Verfahren, die im Folgenden beschrieben werden.

Anwendungsschicht	z.B. HTTP, E-Mail (SMTP, POP), FTP
Transportschicht	TCP, UDP
Internetschicht	IP
Netzzugangsschicht	Ethernet, WLAN, DSL

Abbildung 1: TCP/IP-Referenzmodell mit Beispielen.

[170] In Rheinland-Pfalz ist dies z.B. das rlp-Netz, siehe `http://www.ldi.rlp.de/kommunikation/top.htm` (Abruf am 22.1.2010).

[171] *Tanenbaum*, 2003, 42 ff.

[172] *Tanenbaum*, 2003, 58 ff.; *Eckert*, 2009, 85 ff.

Anwendungsschicht Aus Sicht des Benutzers repräsentiert die Anwendungsschicht den für ihn erkennbaren Typ und Adressat der Kommunikation, verknüpft mit einem bestimmten Programm auf seinem Computer (Webbrowser, FTP-, E-Mail-Client etc.).

Typische Kommunikationsvorfälle zwischen Gericht und Partei sind die folgenden:

- *Informationsabruf von einer Webseite des Gerichts:* Genutzt wird dafür das Hypertext Transfer Protocol, das vom Webbrowser interpretiert wird. Das entsprechende Kürzel `http://` findet sich daher am Anfang einer Webadresse wieder.
- *Formular-Download von einem FTP-Server des Gerichts:* FTP, das File Transfer Protocol,[173] eignet sich besonders für größere Dateien oder umfangreichere Sammlungen. Zur Nutzung wird ein eigenes Programm (sog. FTP-Client) benötigt, wobei auch die gängigen Webbrowser dieses Protokoll unterstützen. Entsprechende Ressourcen sind mit einem vorangestellten `ftp://` gekennzeichnet.[174]
- *E-Mail-Austausch zwischen Gericht und Partei:* Für die Kommunikation per E-Mail kommen, da eine Nachricht nicht direkt dem Rechner des Adressaten zugestellt wird, zwei verschiedene Protokolltypen zum Einsatz: Das Simple Mail Transfer Protocol[175] (SMTP) dient zur Übergabe der Nachricht vom E-Mail-Programm des Senders an seinen Mailserver und von dort zum Mailserver des Empfängers. Zum Abruf eingehender E-Mails nutzt der Empänger POP[176] (Post Office Protocol) oder IMAP[177] (Internet Message Access Protocol).

Transportschicht und Internetschicht Anfragen und Antworten (im Fall von HTTP oder FTP) sowie Nachrichten (im Fall von E-Mail) werden durch die Transportschicht für die Übertragung vorbereitet. Diese Aufgabe übernimmt, für den Benutzer nicht erkennbar, das Betriebssystem seines Rechners. Die eigentliche Datenübertragung im Internet erfolgt in der Internetschicht mit Hilfe von IP[178] (Internet Protocol). Auf dieser Ebene werden als kleinste Einheiten IP-Pakete verschickt, die eine bestimmte Größe nicht überschreiten dürfen. Um die Übertragung größerer Datenmengen – etwa umfangreicherer Formulare oder in Webseiten eingebetteter Grafiken – zu ermöglichen, werden die Daten in der übergeordneten Transportschicht in geeignete Einheiten zerlegt. Diese Aufgabe übernimmt TCP[179] (Transmission

[173] *Postel/Reynolds*, FTP.

[174] Da HTTP auch das Herunterladen von Dateien erlaubt, daneben aber durch die Möglichkeiten der grafischen Gestaltung und Verlinkung einen höheren Komfort für den Benutzer bietet, spielt FTP heutzutage in der Kommunikation mit Endbenutzern nur noch eine untergeordnete Rolle. Jedoch wird es für den, insbesondere auch automatisierten, Datenaustausch zwischen Servern verwendet. Ein Beispiel dafür ist die Übertragung der zu veröffentlichenden Inhalte von den Insolvenzgerichten zu Kopfstellen in den jeweiligen Ländern und von dort zu einem zentralen Server.

[175] *Klensin*, SMTP.

[176] *Myers/Rose*, POP3.

[177] *Crispin*, IMAP.

[178] *Postel*, IP.

[179] *Postel*, TCP.

Control Protocol), welches auf der Empfängerseite auch dafür sorgt, dass die unabhängig voneinander über das Internet versandten IP-Pakete in der richtigen Reihenfolge wieder zusammengefügt und verloren gegangene Pakete beim Sender erneut angefordert werden. Ein alternatives Protokoll auf dieser Schicht ist das einfachere UDP[180] (User Datagramm Protocol), welches z.B. für Internet-Telefonie verwendet wird, jedoch nicht wie TCP eine zuverlässige logische Verbindung zwischen den Endpunkten bereitstellt.

IP-Pakete verfügen mit der in ihnen enthaltenen Adressen über eindeutige Kennungen für Quelle und Ziel des Pakets. Jedes direkt mit dem Internet verbundene System benötigt eine derartige Kennung. IP-Adressen können statisch, d.h. über einen längeren Zeitraum fest zugeordnet, oder dynamisch sein. Letzteres ist insbesondere bei Endbenutzern der Fall, die sich über einen Breitbandanschluss wie DSL mit dem Internet verbinden. Von ihrem Zugangsprovider bekommen sie eine IP-Adresse zugewiesen, welche aber nach Beendigung der Verbindung einem anderen Kunden zugeteilt werden kann. Zumindest für die Dauer der Verbindung ist die IP-Adresse aber ein festes Pseudonym, welches Dritten die Verkettbarkeit von Aktivitäten des Anschlussinhabers ermöglicht. Dem Zugangsprovider ist dies ohnehin möglich, da durch den Nutzer eine Authentifizierung erfolgt.[181]

Netzzugangsschicht Die vierte Ebene des Modells beschreibt den physikalischen Aspekt der paarweisen Kommunikation zwischen an der Übertragung beteiligten Systemen. Bereits genannt wurde DSL als leitungsgebundene Technologie zwischen Benutzer und Zugangsprovider. Bei der zunehmend populärer werdenden mobilen Nutzung werden GSM/UMTS als drahtlose Technologien zwischen Endbenutzer und Mobilfunkanbieter eingesetzt. Innerhalb größerer Organisationen, häufig auch bei Privatnutzern, wird zur Verbindung mehrerer Systeme, die sich eine Internetanbindung teilen, ein lokales Netzwerk (s.u.) aufgebaut. So sind heute die Arbeitsplatzrechner von Richtern und Mitarbeitern der Geschäftsstellen i.d.R. durch Ethernet,[182] eine kabelgebundene Technologie, vernetzt. In vielen Firmen, aber auch bei Privatnutzern wird auch Wireless Local Area Network (WLAN) als drahtloses Technologie verwendet, die im Empfangsbereich des Funksignals ein flexibles ortsungebundenes Arbeiten mit Laptops ermöglicht.

3.2.1.2 Zusammenschaltung von Netzen und Routing

Die oben beschriebenen Protokolle werden häufig auch in Form eines lokalen Netzes, einem sog. LAN (Local Area Network) eingesetzt. Viele Firmen, Behörden, aber auch Privatpersonen betreiben heutzutage ein eigenes LAN, durch das sie ihre Rechner verbinden. In der Regel sind die daran beteiligten Systeme nicht direkt mit dem Internet verbunden, sondern nutzen einen zentralen Übergang, der auch unbefugte Zugriffe aus dem Internet unterbindet (Firewall).

180 *Postel*, UDP.
181 Vgl. hierzu *Yildirim*, 2004, 58 m.w.N.
182 *Tanenbaum*, 2003, 304 ff.

Typischerweise werden auch im lokalen Netz Server betrieben, etwa für interne Webseiten oder Dateiablagen.

Ein Gericht wird i.d.R. wegen des damit verbundenen Aufwands keinen eigenen Mailserver betreiben, sondern auf einem von einem öffentlichen Rechenzentrum oder einem privaten Anbieter betriebenen zurückgreifen. In diesem Fall schreibt etwa ein Geschäftsstellenbeamter eine E-Mail und übergibt diese zur Auslieferung an seinen Mailserver (Anwendungsschicht). Während dieses Vorgangs wird die Nachricht durch die Transportschicht in IP-Pakete unterteilt, die nacheinander über eine Kabel- oder drahtlose Verbindung ins lokale Netz übergeben werden. Da die Zieladresse des Mailservers nicht zum lokalen Netz des Gerichts gehört, muss ein so genanntes Routing, d.h. eine Weiterleitung über das eigene Netz hinaus in Richtung des Zielnetzes erfolgen.[183] Dieser Vorgang wiederholt sich nach der Übergabe eines Pakets vom lokalen Netz ins Internet, möglicherweise über mehrere Zwischenstationen. Diese so genannten Router verfügen über Adressierungsinformationen, die den Weg eines Pakets steuern. Da Verbindungen ausfallen oder Geräte überlastet sein können, sind diese Adressierungsinformationen nicht statisch; vielmehr können sich die Netzwerkgeräte untereinander auf neue Routen verständigen.

3.2.2 Personenbezogene Daten

Auch ohne technischen Einsatz fallen in der Justiz bereits eine Vielzahl von personenbezogenen Daten an.[184] Im Zivilprozess werden z.B. Vor- und Nachname von Parteien und Prozessbevollmächtigten mit deren Anschriften sowie Angaben zum Streitgegenstand erhoben. Des Weiteren kann es z.B. sein, dass Daten von Zeugen erhoben werden. Kommt es dann zur Zwangsvollstreckung, wird eine neue Akte angelegt; neben den bereits im Erkenntnisverfahren gewonnenen Daten werden dann über den Beklagten zusätzlich Angaben zu den Vermögensverhältnissen erfasst; darüber hinaus kann er auch im Schuldnerverzeichnis eingetragen werden.

Der Einsatz moderner Informationstechnologie insbesondere zur Speicherung und der Kommunikation über das Internet bringt es jedoch mit sich, dass technisch bedingt zusätzliche Daten anfallen.

Zur rechtlichen Abgrenzung dient ein dem o.g. TCP/IP-Referenzmodell ähnliches Schichtenmodell, wobei es jedoch keine direkte Korrespondenz der Ebenen gibt.

Inhaltsebene	Datenschutz-Gesetze
Anwendungsebene	TMG
Transportebene	TKG

Abbildung 2: Schichtenmodell zur Abgrenzung personenbezogener Daten bei elektronischer Kommunikation.

183 *Tanenbaum*, 2003, 48.

184 Siehe hierzu etwa *Abel*, RDV 1991, 233; *Geiger*, CR 1986, 37.

3.2.2.1 Nutzungsdaten

Die Justiz betreibt verschiedene Internetportale und automatisierte Abrufverfahren. Damit ist sie Anbieterin eines Telemediendienstes gemäß § 1 Abs. 1 Telemediengesetz (TMG). Bei jeder Inanspruchnahme eines Telemediendienstes fallen Nutzungsdaten an, d.h. personenbezogene Daten, die erforderlich sind, um einem Nutzer die Inanspruchnahme von Telemedien zu ermöglichen oder abzurechnen.[185] Es handelt sich hierbei insbesondere um Merkmale zur Identifikation des Nutzers,[186] Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die in Anspruch genommenen Telemediendienste. Zu letzteren gehören Steuerungsinformationen[187] und Informationen zur Bestimmung der Interaktionspartner.[188]

3.2.2.2 Verkehrsdaten

Bei Angeboten, die sich auf die reine Übermittlung von Daten beschränken (z.B. die Bereitstellung eines SMTP-/POP-Servers durch einen E-Mail-Provider oder die Schaltung eines DSL-Anschlusses durch einen Internetzugangsprovider), handelt es sich nicht um Telemediendienste, sondern um Telekommunikationsdienste.[189] Die bei der Erbringung von Telekommunikationsdiensten anfallenden Daten sind Verkehrsdaten im Sinne des Telekommunikationsrechts. Verkehrsdaten bei E-Mail-Diensten sind insbesondere E-Mail-Adressen, Zeitpunkte der Sendung oder Zustellung und Routing-Informationen. Nicht zu den Verkehrsdaten gehören Angaben mit Bezug zum Inhalt, also auch Bezeichnungen von Datei-Inhalten und der Betreff.

3.2.2.3 Bestandsdaten

Bestandsdaten sind solche Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über

185 Vgl. § 15 Abs. 1 TMG.

186 Dies sind z.B. Benutzername und Passwort und, sofern für den Dienst erforderlich, die (dynamische) IP-Adresse oder ein Cookie (Datensatz, der über mehrere unabhängige Anfragen eine Re-Identifizierung erlaubt, siehe *Tanenbaum*, 2003, 679).

187 Diese enthalten etwa die Angabe des Protokolls wie HTTP oder FTP, den Namen des Servers sowie eine eindeutige Kennzeichnung, unter der der gewünschte Dienst dort zu finden ist; zusammen bilden diese Angaben einen Uniform Resource Locator (URL). Im Fall der Nutzung einer Suchmaschine werden zusätzlich die Suchbegriffe mit übergeben.

188 Etwa eine Nutzerkennung, wie z.B. eine E-Mail-Adresse, oder eine statische IP-Adresse, die eine Identifikation des Nutzers gestattet. Vgl. *Dix/Schaar*, in: *Roßnagel*, Recht der Multimedia-Dienste, § 6 Rn. 82.

189 Im elektronischen Rechtsverkehr bereitet die Abgrenzung zwischen Telemediendiensten und Telekommunikationsdiensten dann Schwierigkeiten, wenn das Dokument über einen elektronischen Gerichtsbriefkasten übermittelt wird. Richtigerweise ist hier jedoch von einem Telemediendienst auszugehen, da dem Nutzer ein technischer Mehrwert etwa durch die teilautomatisierte Verarbeitung strukturierter Daten oder durch das Versehen von Eingängen mit einem elektronischen Posteingangsstempel geboten wird. Vgl. hierzu *Schöttle*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 185.

die Nutzung von Telemedien erforderlich sind.[190] Als typische Arten von personenbezogenen Daten, die zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines derartigen Vertrages erforderlich sind, gelten Name, Anschrift, E-Mail-Adresse, Fax-Nummer, Telefon- und Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel, Benutzerkennung, statische IP-Adressen und ähnliche Angaben.[191]

3.2.2.4 Inhaltsdaten

Als Inhaltsdaten werden die eigentlichen Nutzdaten bezeichnet, die mittels elektronischer Kommunikation übermittelt werden, wobei aus technischen Gründen Nutzungs- bzw. Verkehrsdaten anfallen. Beim elektronischen Rechtsverkehr sind dies Daten, die Gegenstand eines Verfahrens sind, also etwa die elektronische Akte und Dokumente mit den eingangs genannten Angaben.[192] Diese Arbeit beschäftigt sich mit dem Datenschutz in den Verfahrensordnungen. Vor diesem Hintergrund geht es vorliegend um den Schutz von Inhaltsdaten.

3.3 Gefährdungen

Aus der vorgenannten Architektur und Funktionsweise ergeben sich, sofern nicht besondere Schutzmaßnahmen ergriffen werden, verschiedene Gefährdungen der IT-Sicherheit. Angreifer mit entsprechenden Fähigkeiten können diese ausnutzen, wodurch sich u.U. erhebliche Risiken für den Datenschutz und die Datensicherheit ergeben können.[193]

3.3.1 Unbefugte Kenntnisnahme

Unbefugte Kenntnisnahme verletzt das Schutzziel der Vertraulichkeit von Daten,[194] die im Rahmen der Kommunikation übermittelt werden.[195] Für einen Angreifer werden typischerweise Inhaltsdaten ein interessantes Angriffsziel sein.[196] Das Abhören einer Verbindung setzt voraus, dass der Angreifer Zugriff auf eine der beteiligten Übertragungsstrecken oder Knotenpunkte erhält. Zudem kann es sein, dass etwa Bedienstete auf Daten zugreifen können, zu deren Nutzung sie eigentlich nicht autorisiert sind.

---

190 Vgl. § 14 Abs. 1 TMG.

191 *Dix*, in: *Roßnagel*, Recht der Multimedia-Dienste, § 5 Rn. 27.

192 *Schöttle*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 185.

193 Zu den technischen Hintergründen der Gefährdungen siehe ausführlich *Eckert*, 2009.

194 Gemeint sind Inhaltsdaten und Nutzungsdaten.

195 Siehe hierzu auch Abschnitt 7.1.1.

196 Doch auch Nutzungsdaten können einige Informationen über die Umstände der Kommunikation wie etwa Identität der Beteiligten, Ort, Datenumfang preisgeben.

3.3.1.1 Abhören der Verbindung

Am einfachsten gelingt ein Abhören, wenn beim Sender oder Empfänger ein Funknetz eingesetzt wird. Die über diese Verbindung übermittelten elektromagnetischen Signale können prinzipiell durch Dritte – sofern sie sich im Empfangsbereich befinden – unbemerkt aufgezeichnet werden. Neben einem mobilen Rechner ist dazu lediglich frei im Internet erhältliche Software erforderlich, die sich auch von Laien benutzen lässt.[197] Auch bei kabelgebundenen lokalen Netzen ist ein ähnlicher Angriff möglich, sofern der Angreifer Zugang zum Netzwerk z.B. über den Anschluss in einem allgemein zugänglichen Besprechungsraum oder dergleichen erhält.[198]

3.3.1.2 Abhören an Kommunikationsknoten

IP-Pakete werden, wie oben erwähnt, in der Regel nicht direkt vom Sender zum Empfänger gelangen, sondern über mehrere zwischengeschaltete Router, die von Internet-Providern betrieben werden, übermittelt. Selbst bei einer Kommunikation, deren Endpunkte sich in Deutschland befinden, kann im Einzelfall (etwa bei Leitungsüberlastung oder -ausfall) eine Route gewählt werden, die über Systeme im Ausland verläuft. Es wurden bereits Methoden auf die Routing-Protokolle des Internet beschrieben, mit denen es ein Angreifer erreichen kann, sich Pakete über ein von ihm kontrolliertes System umleiten zu lassen.[199]

Auch das sendende und das empfangende System zählen zu den Kommunikationsknoten, auf die Angriffe möglich sind. Durch Schadsoftware (etwa ein Trojanisches Pferd oder Spyware) können Daten auf dem Rechner des Senders einer E-Mail oder dem Aufruf einer Webseite ausgespäht werden. Im Falle von E-Mail oder zugangsgeschützten Webseiten ist die Vertraulichkeit der Daten lediglich von einem Passwort abhängig. Sofern nicht entsprechende Regeln vorgegeben werden, ist immer zu befürchten, dass einzelne Benutzer schwache, d.h. leicht zu erratende, Passwörter wählen.[200]

3.3.1.3 Unzureichende Benutzer-Autorisierung

Eng verwandt damit ist die Bedrohung des Ausnutzens von Lücken der Benutzer-Autorisierung, d.h. der Verwaltung und Prüfung von Zugriffsberechtigungen. Einen derartigen Angreifer bezeichnet man als Innentäter, da er zwar über eine Benutzerkennung verfügt, aber die damit verbundenen Rechte überschreitet. Entsprechende Situationen können eintreten, wenn ihm etwa Fachanwendungen oder Unterlagen zugänglich sind, die nicht oder nicht mehr zur Aufgabenerfüllung innerhalb seiner spezifischen Verfahren erforderlich sind. Auch die gemeinsame

197 *Eckert*, 2009, 823 ff.
198 *Eckert*, 2009, 90 f.
199 *Eckert*, 2009, 109.
200 *Eckert*, 2009, 432.

Nutzung einer Benutzerkennung durch mehrere Beschäftigte (sog. Account Sharing) birgt Gefahren, da eine Trennung auf Ebene des einzelnen Sachbearbeiters nicht mehr möglich ist.[201]

3.3.2 Unbefugte Veränderung von Daten

Für die Verletzung des Schutzziels der Integrität gilt das zuvor Gesagte: Eine Manipulation kann auf Übertragungsstrecken oder den Knotenpunkten, einschließlich des Ausgangs- und Zielsystems selbst, auf dem eine dauerhafte oder vorübergehende Speicherung stattfindet, erfolgen. Lücken in der Autorisierung erleichtern einen Angriff erheblich. Jedoch ist das Verändern von Daten während ihrer Übertragung in der Regel schwieriger als das reine Mitlesen, da es hierzu erforderlich ist, die vom legitimen Sender stammenden Daten abzufangen, ihre Weiterleitung an den legitimen Empfänger zu unterdrücken und gleichzeitig die manipulierten Daten einzuspielen.

Sollte es einem Angreifer gelingen, sich durch Hacking (d.h. Ausnutzen einer Sicherheitslücke, die einen Zugang erlaubt) eines IT-Systems zu bemächtigen, so könnte er die darauf gespeicherten Daten leicht verändern. Zu berücksichtigen ist weiterhin die Möglichkeit, dass einer der Kommunikationspartner selbst die Nachricht abändert, was ihm offenkundig sehr leicht möglich ist.

3.3.3 Vortäuschen einer falschen Identität

Das Schutzziel der Authentizität wird verletzt, wenn sich ein Angreifer für einen anderen ausgeben kann und etwa in dessen Namen Nachrichten erstellt oder Transaktionen veranlasst. Es ist eng verwandt mit dem Schutzziel der Integrität und der zuvor beschriebenen Gefährdung: Angenommen eine Partei stellt einen Antrag an das Gericht. Gelingt es einem Angreifer beispielsweise, diese per E-Mail abgegebene Erklärung zu seinen Gunsten zu verändern und unter Vorspiegelung des Adressaten an das Gericht zu senden, würde der zunächst eingereichte Antrag mit einem verfälschten Inhalt an das Gericht gelangen.

3.3.3.1 Fälschen einer Benutzerkennung

Ein erhebliches Risiko besteht in der Nutzung von E-Mail, wenn diese für die Abgabe von Erklärungen oder Anträgen zulässig ist. Bei gewöhnlicher E-Mail ist es ohne weiteres möglich, Nachrichten unter einer falschen Absender-Adresse zu verschicken. Zwar ist für den Versand eine Anmeldung per SMTP unter Angabe von Benutzername (typischerweise die E-Mail-Adresse oder ein Teil davon) und Passwort am Mailserver erforderlich. Viele Mailserver lassen es aber zu, dass eine andere Absender-Adresse, z.B. `Partei_P@gmx.net` beim Versand angegeben wird. Für den technisch nicht versierten Empfänger ist dieser Vorgang nicht erkennbar, da ledig-

[201] *DSB-Konferenz*, 2006, 17.

lich die (im E-Mail-Programm nicht direkt sichtbaren) Nutzungsdaten im Header darüber Auskunft geben können.

3.3.3.2 Täuschen des Kommunikationspartners

Eine andere Angriffsvariante nutzt die Tatsache, dass viele Privatnutzer – aber auch kleinere Anwaltskanzleien – Kunde bei einem der großen E-Mail-Anbieter wie AOL, GMX, T-Online oder WEB.DE sind. Diese bieten, oftmals sogar kostenlos, jedermann ein Postfach an. Bei der Registrierung ist der Nutzername frei wählbar, eine Prüfung der persönlichen Angaben findet dabei nicht statt. Die Echtheit der angegebenen Personalien kann somit nicht vorausgesetzt werden.[202] Aufgrund von Namensgleichheiten unter den zahlreichen Nutzern der großen Anbieter sind zudem Schreibvarianten wie `peter.maier@web.de`, `p.maier_mainz@web.de`, `peter.maier1965@web.de` häufig anzutreffen. Für den Empfänger ist nicht erkennbar, ob überhaupt ein Peter Maier und wenn ja, welcher, sich hinter den genannten Adressen verbirgt. Für einen Angreifer ist es ein Leichtes, ein Postfach unter einer Schreibvariante anzulegen und von dort aus Nachrichten zu verschicken. Datenschutzrechtlich relevant ist dies, da das Gericht damit entweder veranlasst werden kann, Daten ohne Rechtsgrundlage zu erheben und zu speichern oder – was gravierender ist – Daten an Unbefugte zu übermitteln. Folgendes Fallbeispiel mag die Gefährdungen verdeutlichen.

3.3.3.3 Fallbeispiel

Um Akteneinsicht zu bekommen, wird vorgetäuscht, der Anwalt einer Partei zu sein und dem Gericht eine Anschrift oder E-Mail-Adresse schriftlich oder elektronisch mitgeteilt.

Auf der so genannten Eingangsseite, d.h. bei der Mitteilung der Daten an das Gericht, können aus datenschutzrechtlicher Sicht keine spezifischen IT-Gefährdungen festgestellt werden. In einem schriftlichen Dokument können die Absenderangaben, der Briefkopf und die Unterschrift des Anwalts genauso gefälscht werden, wie man sich eine E-Mail-Adresse mit dem Namen des Anwalts beschaffen kann.

Anders gestaltet sich die Situation jedoch auf der so genannten Ausgangsseite, nämlich dann, wenn das Gericht die Akte durch Einschaltung eines Postunternehmens oder eines Gerichtsvollziehers an die angegebene Adresse übersenden will. Denn der Postbedienstete oder der Gerichtsvollzieher merkt in der Regel, dass der Name des Anwalts nicht am Briefkasten steht. Er nimmt deshalb die Akte wieder mit. Bei der elektronischen Zustellung ist dies dagegen anders. Hier ist keine Person dazwischengeschaltet, die die Übereinstimmung der genannten Daten überprüfen kann. Die Gefahr, dass das Dokument bei einem Unbefugten ankommt, ist daher bei der elektronischen Übermittlung größer.

Nun kann es zwar auch sein, dass der Angreifer sein Briefkastenschild mit dem Namen des Anwalts überklebt. In diesem Fall wird der Postbote oder der Gerichtsvollzieher das Dokument

[202] Vgl. hierzu *Buggisch*, NJW 2004, 3519; *Roßnagel/Pfitzmann*, NJW 2003, 1209.

einwerfen. Der Missbrauch kann bei der Übermittlung per Post jedoch besser zurückverfolgt werden. Denn es ist möglich, über die Daten beim Einwohnermeldeamt auf die Person zu schließen, die tatsächlich an der angegebenen Adresse wohnt. Über die E-Mail-Adresse ist eine Rückverfolgbarkeit hingegen aufgrund der oben erwähnten fehlenden Prüfung der Identität beim Anlegen eines Postfachs nicht gegeben.

3.3.4 Beeinträchtigungen der Beweisbarkeit

Neben der generellen Problematik der Manipulierbarkeit sind der mangelnde Zugangsnachweis sowie ein möglicher Verlust der Beweiskraft über die Zeit wichtige Aspekte.

3.3.4.1 Zugang einer Nachricht

Wie beschrieben, wird bei E-Mail eine Nachricht beim Sendevorgang vom Rechner des Absenders dem eigenen Mailserver übergeben. Der Absender bekommt dabei keine direkte Bestätigung über die Zustellung oder den Abruf durch den Empfänger. Durch Beeinträchtigungen im Netzwerk während der Übertragung, Überschreitung des Speicherplatzes oder aufgrund der Einstufung und möglichen Löschung als Spam kommt es immer wieder dazu, dass Nachrichten ihren Empfänger überhaupt nicht oder erst verzögert erreichen. Aufgrund dieser technischen Unzuverlässigkeit kann bei E-Mail plausibel der (rechtzeitige) Zugang einer Nachricht bestritten werden. Auch genügt dem Absender die Bestätigung über die erfolgreiche Übergabe an den eigenen Mailserver nicht als Nachweis des Versands.

3.3.4.2 Verlust der Beweisbarkeit

Informationen, die durch Daten elektronisch repräsentiert sind, können über die Zeit an Beweiskraft verlieren. Abhängig von der zur Erstellung, Verarbeitung, Anzeige und Speicherung von Dokumenten verwendeten Software gibt es verschiedene Dateiformate, gemäß derer die Daten organisiert sind. Durch Versions- oder Produktwechsel sowie Inkompatibilitäten zwischen Anwendungen kann es dazu kommen, dass Dokumente nicht mehr oder nur in Teilen lesbar sind. Ein ähnliches Problem betrifft den technischen Fortschritt bei Speichermedien und -formaten und die langfristige Haltbarkeit von Daten-CDs und -DVDs.[203] Im Zusammenhang mit der Verwendung von elektronischen Signaturen sind zudem besondere Maßnahmen zu treffen, um eine Prüfbarkeit der Signatur auch Jahre oder gar Jahrzehnte nach dem Zeitpunkt der Erstellung zu gewährleisten.[204]

[203] *Gieselmann*, c't 2005, 44.
[204] Siehe hierzu auch Abschnitt 7.6.1.

3.3.5 Perpetuierung von Vorgängen

Online bereit gestellte Datenbanken wie etwa das Handelsregister oder die Insolvenzbekanntmachungen oder das künftige elektronische Schuldnerverzeichnis bergen aufgrund der dauernden Verfügbarkeit von Daten im Internet und der Unkontrollierbarkeit der Speicherdauer beim Abrufenden weitere Gefährdungen in sich. Adresshändler, Verlage oder Wirtschaftsauskunfteien können sich die Informationen aus dem Internet für ihre Zweck zunutze machen und das informationelle Selbstbestimmungsrecht beeinträchtigen.[205] In diesem Zusammenhang sind folgende Punkte relevant.

3.3.5.1 Keine effiziente Löschungsmöglichkeit

Der Betreiber der Internetplattform hat keinen Einfluss darauf, ob und wann die Daten im Internet gelöscht werden. Zwar kann er die Daten auf der Originalseite löschen. Daten, die über eine Webseite bereitgestellt werden, werden oftmals aber auch zwischengespeichert. Diese Daten können auf unbestimmte Dauer im Hintergrund (Cache)[206] noch zu finden sein. Die in einer Zeitung veröffentlichten Daten können zwar auch für immer in der Welt bleiben. Die Aufbewahrung und eine spätere Suche sind jedoch um ein Vielfaches aufwändiger.

3.3.5.2 Unkontrollierbarkeit der Speicherdauer

Die im Internet veröffentlichten Daten können auf den eigenen Rechner heruntergeladen und zeitlich unbegrenzt gespeichert werden. Die in Printmedien veröffentlichten Daten können zwar auch zeitlich unbegrenzt aufbewahrt werden. Dies bedarf jedoch zum einen mehr Platz und zum anderen ist eine Suche nach bestimmten Veröffentlichungen wesentlich schwerer. Um die in den Printmedien veröffentlichten Daten schließlich zu speichern, müssen die Daten zunächst mühsam entweder durch manuelle Erfassung der Veröffentlichungstexte oder durch Einscannen und elektronische Weiterverarbeitung mit einer Texterkennungssoftware aufbereitet werden.

3.3.5.3 Verstärkte Nutzung zu kommerziellen Zwecken

Adresshändler, Verlage oder Wirtschaftsauskunfteien können die Daten etwa aus den zentralen Bekanntmachungsplattformen komplett abrufen und auswerten. Mit Hilfe von so genannten Webcrawlern, also Programmen, die automatisiert die Seiten eines Webauftritts aufrufen, inhaltlich analysieren und auch Verlinkungen nachverfolgen, können massenhaft Daten beschafft

[205] Siehe hierzu auch Abschnitt 9.1.4.

[206] Das so genannte Caching ist eine Methode, um den Benutzern häufig benötigte Inhalte schneller anbieten zu können. Ein Caching kann auf einem System des Zugangsproviders (einem so genannten Web-Proxy), auf dem System des Benutzers (im Browser-Cache), durch Suchmaschinen oder auf Seiten Dritter erfolgen, seien es private Angebote oder Einrichtungen wie etwa das Internet Archive (`www.archive.org`).

und erschlossen werden.[207] Adresshändler, Verlage oder Wirtschaftsauskunfteien können Profile erstellen, die ein möglichst umfassendes und realitätsgetreues Bild einer Person zeichnen. Eine Profilbildung ist dabei durch Auswertung der alten Datenbestände (Datenhistorie) oder durch eine Verknüpfung mit weiteren Datenbeständen möglich.[208]

Im Bereich des Insolvenzrechts und des Zwangsversteigerungsrechts bedeutet dies etwa, dass die dauerhaft zur Verfügung stehenden Daten einen Zustand wiedergeben können, der heute längst nicht mehr der tatsächlichen Situation entspricht. Ein Schuldner, gegen den ein Insolvenzverfahren betrieben oder dessen Haus zwangsversteigert worden ist, bleibt damit für immer als nicht zahlungskräftig gebrandmarkt, selbst wenn er inzwischen vermögend geworden ist. Im Bereich des Handelsrechts kann die dauerhafte Speicherung alter Daten v.a. dazu führen, dass mit deren Hilfe ein Verlauf gezeichnet werden kann, was nicht Zweck der damaligen (punktuellen) Veröffentlichungen war. So ist es z.B. möglich, anhand der Datensätze genau zu ermitteln, wie oft etwa eine bestimmte Person im Lauf ihres Lebens verschiedene Firmen angemeldet hat oder als Geschäftsführer abbestellt worden ist.[209]

Eine Verknüpfung ist mit Datensätzen aus den gerichtlichen Internetplattformen möglich. So können beispielsweise die Datensätze aus dem Insolvenzbekanntmachungsportal, dem Zwangsversteigerungsportal und dem Portal des elektronischen Bundesanzeigers zusammengeführt werden. Somit lässt sich beispielsweise genau ermitteln, welcher Schuldner einmal Grundbesitz besaß, wann er insolvent geworden ist und wie oft eine Klageschrift vor seiner Insolvenz gegen ihn öffentlich zugestellt werden musste. Die Datensätze lassen sich aber auch mit beliebig vielen Parametern aus anderen Datenbanken verknüpfen. Beispielsweise könnte etwa die Ortsangabe als Geo-Datum verwendet werden, um über Dienste wie Google Maps z.B. Landkarten sämtlicher aktueller Insolvenzschuldner zu erstellen (siehe Abbildung 3). Dies würde es erlauben, schnell einen nicht zahlungskräftigen potentiellen Kunden zu erkennen und nach Sammlung von Daten über einen längeren Zeitraum sogar systematisches Scoring basierend auf Adressangaben zu betreiben.[210]

3.4 Zusammenfassung

Man kann sagen, dass der Modernisierungsprozess im Vergleich zu herkömmlichen Anwendungen mit einer stärkeren Bedrohung für den Datenschutz einhergeht. Vorliegend geht es um das informationelle Selbstbestimmungsrecht in den Verfahrensordnungen und damit um den Schutz von Inhaltsdaten. Die Inhaltsdaten können durch die aufgezeigten Anwendungen bei der Übermittlung von Dokumenten v.a. durch eine unbefugte Einsichtnahme und durch das

[207] Webcrawler werden typischerweise von Suchmaschinen in großem Stil eingesetzt, entsprechende Programme können aber auch von interessierter Seite zielgerichtet genutzt werden, um etwa eine Website systematisch auf den eigenen Rechner zu spiegeln. Sind die Daten einmal dort angelangt, kann die ursprüngliche Quelle keinen Einfluss mehr auf die weitere Speicherung, Verbreitung oder sonstige Nutzung nehmen.

[208] *Klink*, D-A-CH, 25.

[209] *Klink*, D-A-CH, 25.

[210] *Klink*, D-A-CH, 26.

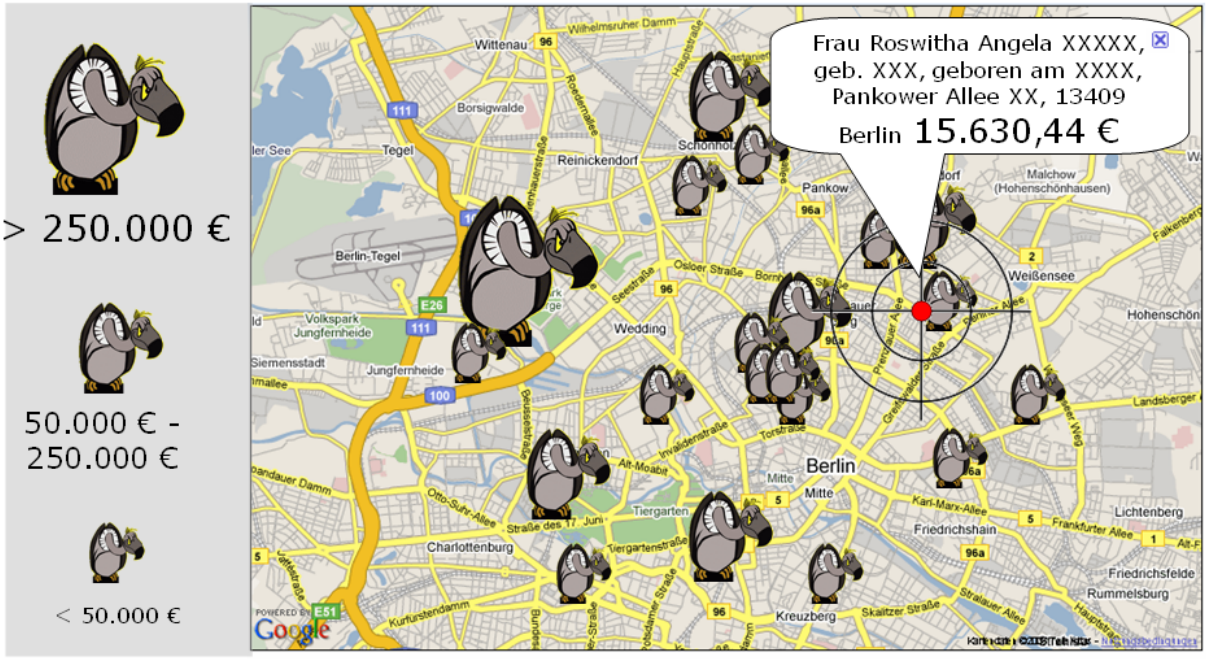

Abbildung 3: Beispielhafte Verknüpfung von Geo- und Insolvenzdaten.

Vortäuschen einer falschen Identität gefährdet sein und bei der Abfrage von Registern durch das weltweit zugängliche Internet. Bei der elektronischen Aktenführung bestehen Probleme vor allem durch die Möglichkeiten der Vervielfältigung einerseits, aber auch des Verlustes der Daten andererseits.

Teil II

Rechtsrahmen

Kapitel 4

Rechtsquellen

Die vorherigen Abschnitte haben gezeigt, dass der Modernisierungsprozess in der elektronischen Justiz weit vorangeschritten ist. Es wurde festgestellt, dass mit den neuen technischen Anwendungen beachtenswerte Ziele verfolgt werden. Gleichzeitig wurde jedoch auch in technischer Hinsicht aufgezeigt, dass mit den Modernisierungsprozessen neue Gefährdungen für den Datenschutz einhergehen. In diesem Kapitel werden nun die Rechtsquellen des Datenschutzes und der Datensicherheit, die für die Justiz von Bedeutung sind, dargestellt. Entsprechend der Normenhierarchie wird zunächst das Recht der EU beleuchtet, dann die verfassungsrechtliche Ebene und schließlich das einfache Recht. Da sich das nächste Kapitel ausführlich mit den Anforderungen des Datenschutzes in der elektronischen Justiz beschäftigt, beschränken sich die nachfolgenden Ausführungen zu den allgemeinen Datenschutzgesetzen in diesem Kapitel auf deren Anwendungsbereich.

4.1 Das Recht der Europäischen Union

Am 4.6.1999 hat der Europäische Rat in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen.[211] In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern." Die Grundrechtscharta der EU wurde daraufhin in einem Verfassungskonvent[212] unter dem Vorsitz des ehemaligen Bundespräsidenten und ehemaligen Präsidenten des Bundesverfassungsgerichts Roman Herzog erarbeitet und in Nizza im Jahr 2001 feierlich

[211] ABl. EG C 364, 1.

[212] Mit der Einsetzung eines Verfassungskonvents hatte Europa im Vergleich zu seiner vorherigen kritisierten „Kabinettspolitik" einen ganz neuen Weg beschritten. In dem Verfassungskonvent saßen 15 Beauftragte der nationalen Regierungen, ein Mitglied der EU-Kommission, 16 Angehörige des Europäischen Parlaments und 30 Angehörige der nationalen Parlamente. Vgl. hierzu im Einzelnen *Baer*, ZRP 2000, 363.

proklamiert.[213] In Art. 8 enthält sie das Recht auf Datenschutz.[214] Auch die Datenschutzbeauftragten des Bundes und der Länder hatten in einer Entschließung aus dem Jahr 1999 Bundesregierung, Bundestag und Bundesrat aufgefordert, sich für die Einfügung eines Grundrechts auf Datenschutz in den Katalog europäischer Grundrechte einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.[215] Der am 7.12.2007 unterzeichnete[216] und am 1.12.2009 in Kraft getretene[217] Vertrag von Lissabon enthält weitgehende Änderungen des Vertrages über die Europäische Union (EUV), die sich unter anderem auf den Grundrechts- und damit auch auf den Datenschutz in der EU auswirken.[218] In Art. 6 Abs. 1 EUV ist ein direkter Verweis auf die Charta der Grundrechte aufgenommen worden. Nach Art. 6 Abs. 1 2. Hs. EUV enthält sie nunmehr denselben Rang und dieselbe Rechtsverbindlichkeit wie die Gründungsverträge selbst. Außerdem sieht Art. 6 Abs. 2 EUV den Beitritt der EU zur Europäischen Menschenrechtskonvention vor und bestätigt gemäß Art. 6 Abs. 3 EUV die bisherige – auf der Grundlage von Art. 6 Abs. 2 EUV a.F. vorgenommene – Geltung der Gemeinschaftsgrundrechte als allgemeine Rechtsgrundsätze. Diese Fülle an grundrechtlichen Bindungen bringt sicherlich die Bedeutung des Grundrechtsschutzes in der EU deutlich zum Ausdruck. Es bleibt jedoch abzuwarten, ob sie auch einem wirksamen und für die EU-Bürger transparenten Grundrechtsschutz zuträglich sind.[219]

Die EG-Datenschutzrichtlinie[220] bezweckt eine einheitliche Regelung zur Verarbeitung personenbezogener Daten im gesamten europäischen Raum, um die Übermittlung personenbezogener Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat zu ermöglichen, ohne damit eine Gefährdungslage für den Datenschutz herzustellen.[221] Vom Anwendungsbereich

---

213 Am 12.12.2007 wurde die Charta der Grundrechte auf der Plenarsitzung des Parlaments von den Präsidenten des Parlaments, des Rates und der Kommission erneut feierlich proklamiert und danach im Amtsblatt veröffentlicht (ABl. EG C 303, 1). Hierdurch sollte der besondere Charakter der Charta hervorgehoben und ihre Wahrnehmung in der Öffentlichkeit verbessert werden.

214 Zur europäischen Grundrechtscharta, siehe ausführlich *Eickmeier*, DVBl 1999, 1026; *Pache*, EuR 2001, 475; *Schwarzer*, DVBl 1999, 1677; *Däubler-Gmelin*, EuZW 2000, 1; *Weber*, NJW 2000, 537.

215 *DSB-Konferenz*, 7./8.10.1999.

216 Vertrag von Lissabon zur Änderung des Vertrages über die Europäische Union und des Vertrages zur Gründung der Europäischen Gemeinschaft vom 8.10.2008 (BGBl. 2008 II, 1038).

217 Bekanntmachung vom 13.11.2009 (BGBl. 2009 II, 1223).

218 Zur Frage, ob Deutschland seine Staatlichkeit zu stark zugunsten der EU durch den Vertrag von Lissabon aufgebe, vgl. BVerfG, NJW 2009, 2127. In Reaktion auf das Urteil sind vier sog. Begleitgesetze in Kraft getreten: Gesetz über die Ausweitung und Stärkung der Rechte des Bundestages und des Bundesrates in Angelegenheiten der EU (BGBl. 2009 I, 3022), Gesetz zur Umsetzung der GG-Änderungen für die Ratifizierung des Vertrages von Lissabon (BGBl. 2009 I, 3822), Gesetz zur Änderung des Gesetzes über die Zusammenarbeit von Bundesregierung und Deutschen Bundestag in Angelegenheiten der EU (BGBl. 2009 I, 3026), Gesetz zur Änderung des Gesetzes über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der EU (BGBl. 2009 I, 3031).

219 *Pache/Rösch*, NVwZ 2008, 475.

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 (ABl. EG L 281, 31).

221 Zur EG-Datenschutzrichtlinie allgemein vgl. etwa *Brühann/Zerdick*, CR 1996, 429; *Weber*, CR 1995, 297. Der Zweck der Richtlinie geht insbesondere aus Art. 7 und 8 der Erwägungsgründe hervor.

der Datenschutzrichtlinie ist nach Art. 3 jede Verarbeitung von personenbezogenen Daten erfasst, soweit sie automatisiert erfolgt oder wenn es sich um Daten handelt, die in Dateien gespeichert sind oder werden sollen. In den Art. 5 bis 17 werden die verschiedenen Verarbeitungsgrundsätze formuliert. Die Verarbeitung von besonders sensitiven Daten gestattet die Richtlinie in Art. 8 nur unter bestimmten Voraussetzungen. In Art. 10, 11 und 12 sind die Rechte der Betroffenen enthalten. Besondere Bedeutung kommt den Vorschriften der Art. 25 und 26 zu, die die Zulässigkeit der Datenübermittlung in Drittländern regeln. Nach Art. 32 Abs. 1 musste die Richtlinie in einem Zeitraum von drei Jahren, also bis zum 24.10.1998, umgesetzt werden.[222] Dem blieben die deutschen Bundes- und Landesgesetzgeber jedoch zunächst säumig. Das BDSG wurde erst mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18.5.2001[223] an die Vorgaben der Datenschutzrichtlinie angepasst. In Rheinland-Pfalz ist das Landesdatenschutzgesetz mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 8.5.2002 an die Richtlinie angepasst worden.[224] Wie noch zu sehen sein wird, ist der Datenschutz in den Verfahrensordnungen nur rudimentär geregelt.[225] Dem BDSG und dem LDSG kommen daher in der elektronischen Justiz eine große Bedeutung zu. Vor diesem Hintergrund sind auch die Vorgaben der EG-Richtlinie von Bedeutung.

Die Richtlinie des Europäischen Rates und des Europäischen Parlaments über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen trat am 19.1.2000 in Kraft.[226] Mit der Richtlinie sollte ein vergleichbarer Standard für elektronische Signaturen geschaffen werden.[227] Die Richtlinie musste nach dessen Artikel 13 Abs. 1 bis zum 19.7.2001 in nationales Recht umgesetzt werden. In Deutschland ist die Richtlinie mit dem Signaturgesetz vom 16.5.2001, welches am 22.5.2001 in Kraft getreten ist,[228] umgesetzt worden. Aufgrund des § 24 SigG erging des Weiteren eine Signaturverordnung. Diese trat am 16.11.2001 in Kraft.[229] Die hier einschlägigen Verfahrensordnungen schreiben den Einsatz der elektronischen Signatur an verschiedenen Stellen vor.[230] Aus diesem Grund sind daher auch die Vorgaben dieser Richtlinie von Bedeutung.

---

222 Vgl. hierzu Art. 10 EGV: „Die Mitgliedstaaten treffen alle geeigneten Maßnahmen allgemeiner oder besonderer Art zur Erfüllung der Verpflichtungen, die sich aus diesem Vertrag oder aus Handlungen der Organe der Gemeinschaft ergeben. Sie erleichtern dieser die Erfüllung ihrer Aufgabe. Sie unterlassen alle Maßnahmen, welche die Verwirklichung der Ziele dieses Vertrags gefährden könnten."

223 BGBl. 2001 I, 904.

224 GVBl. 2002, 177.

225 Siehe hierzu Kapitel 5.

226 ABl. EG L 13, 12. Hierzu vgl. etwa *Roßnagel*, MMR 1999, 261; *Kilian*, BB 2000, 733; zur Umsetzung in den einzelnen EU-Ländern vgl. etwa *Dumortier/Rinderle*, CRi 2001, 5.

227 *Yildirim*, 2004, 87.

228 BGBl. 2001 I, 876. Durch dieses Gesetz wurde das bereits seit 1.8.1997 geltende SigG 1997 abgelöst.

229 BGBl. 2001 I, 3074. Mit dieser wurde die seit 1.11.1997 geltende SigV 1997 abgelöst.

230 Vgl. hierzu Abschnitt 4.3.4.4.

4.2 Das Grundgesetz und die Landesverfassung

4.2.1 Das Grundgesetz

Obgleich der Datenschutz ein Grundrecht ist, wird er im Grundgesetz nicht erwähnt. Juristischer Ausgangspunkt und verfassungsrechtlicher Ort des Datenschutzes war ursprünglich das allgemeine Persönlichkeitsrecht.[231] Das allgemeine Persönlichkeitsrecht schützt „die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen“. Seine Grundlage ist Art. 2 Abs. 1 i.V.m. Art. 1 GG.[232] Eine Beeinträchtigung des Persönlichkeitsrechts lag vor, wenn ein Grundrechtsverpflichteter im Sinne des Art. 1 Abs. 3 GG belastende Regelungen traf oder es sich um faktische Eingriffe von gewissem Gewicht handelte. Absoluten Schutz vor Beeinträchtigungen in das allgemeine Persönlichkeitsrecht genoss die Intimsphäre. In diese durfte nicht eingegriffen werden. In die Privatsphäre durfte nur nach einer Abwägung zwischen der grundsätzlichen Unantastbarkeit der Persönlichkeit einerseits und dem Informationsinteresse anderer Menschen andererseits eingegriffen werden. Unter weniger strengen Anforderungen stand ein Eingriff in die äußerste Sphäre, die Individualsphäre. Die Legitimationsanforderungen an die Rechtmäßigkeit eines Einriffs waren hier umso strenger, je näher die Maßnahme in den Kern des Persönlichkeitsrechts eingriff.[233]

Das Bundesverfassungsgericht hat in vielen Entscheidungen das Grundrecht konkretisiert und sich dabei mit dem Schutz der Privat- und Intimsphäre auseinandergesetzt. An dieser Stelle sei auf die Mikrozensus-Entscheidung[234] vom 16.7.1969, auf die Scheidungsakten-Entscheidung[235] vom 15.1.1970, auf die Patientenkarten-Entscheidung[236] vom 8.3.1972, auf die Lebach-Entscheidung[237] vom 5.6.1973, auf den Beschluss zur Suchtkrankenberatungsstelle[238] vom 24.5.1977, auf den Epplerbeschluss[239] vom 3.6.1980, auf die Selbstbezichtigungsentscheidung[240] vom 13.1.1981 und letztlich auf die Gegendarstellungsentscheidung[241] vom 8.2.1983 hingewiesen. Weil sich eine Abgrenzung nach den verschiedenen Sphären als schwierig erwies und weil die Deutung eines Datums nicht von diesem allein, sondern von dem Kontext seiner Entscheidung abhing, wurden die Entscheidungen in der Literatur vielfach kritisiert.[242]

---

231 *Liebscher*, 1994, 23.

232 BVerfGE 54, 148 (153).

233 Zu den einzelnen Sphären vgl. im Einzelnen *Liebscher*, 1994, 24 m.w.N.

234 BVerfGE 27, 1.

235 BVerfGE 27, 344.

236 BVerfGE 32, 373.

237 BVerfGE 35, 202.

238 BVerfGE 44, 353.

239 BVerfGE 54, 148.

240 BVerfGE 56, 37.

241 BVerfGE 63, 131.

242 Hierzu etwa *Steinmüller* et al., BT-Drs. 6/3826, 51: „Alle genannten Versuche haben gemeinsam, dass sie offenbar davon ausgehen, die jeweilige abstrakte Umschreibung ermögliche es, die Privatsphäre genau zu umgrenzen und somit Verletzungen scharf feststellen zu können. Das ist bisher nicht gelungen. (...) Was A zu seiner Privatsphäre zählt, muss B noch lange nicht dazu zählen und umgekehrt. Was aber A gegenüber C offenbaren will, das will B unter Umständen C gegenüber nicht geheimhalten und umgekehrt. Relativität

4.2.1.1 Das Volkszählungsurteil von 1983

Im Volkszählungsurteil von 1983 hat das Bundesverfassungsgericht klargestellt, dass nicht mehr auf die Art der Daten und die betroffenen Sphären abgestellt werden kann. Vielmehr seien die Nutzbarkeit und Verwendungsmöglichkeiten und der Verwendungszusammenhang maßgeblich.[243] In Überwindung der Sphärentheorie hat das Gericht aus Art. 2 Abs. 1 i.V.m. Art. 1 GG das Recht auf informationelle Selbstbestimmung abgeleitet. Das Bundesverfassungsgericht hat damit klargestellt, dass Datenschutz Verfassungsrecht besitzt.[244] Mit seiner Entscheidung hat das Gericht verfassungsrechtliche Grundlagen für die Fortentwicklung des Datenschutzrechts im öffentlichen und im nicht-öffentlichen Bereich festgelegt.[245]

Das Recht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[246] Diesen Anspruch bezeichnet das Bundesverfassungsgericht als Recht auf informationelle Selbstbestimmung.[247] Das informationelle Selbstbestimmungsrecht schützt den Bürger gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten.[248]

Mit dem informationellen Selbstbestimmungsrecht hat das Bundesverfassungsgericht kein neues Grundrecht erfunden. Es hat lediglich seine Rechtsprechung zum Persönlichkeitsrecht weiterentwickelt.[249] Es hat klargestellt, dass das Persönlichkeitsrecht nicht mehr in einzelne Sphären aufgeteilt wird. Vielmehr müsse der Erkenntnis Rechnung getragen werden, dass sich als Folge

---

der Privatsphäre heißt also: Privatsphäre gegenüber wem? Darum gilt der Grundsatz der Relativität der Privatsphäre und daraus folgt die Unmöglichkeit ihrer Definition."

243 Zu den Reaktionen auf das Volkszählungsurteil in der Literatur, vgl. etwa *Simitis*, NJW 1984, 394; *Podlech*, Leviathan 1984, 85; *Steinmüller*, DuD 1984, 85; *Benda*, DuD 1984, 86; *Hufen*, JZ 1984, 1072; *Krause*, JuS 1984, 268; *Baumann*, DVBl 1984, 612; *Busch*, DVBl 1984, 385.

244 *Büllesbach*, NJW 1991, 2595.

245 Der Entscheidung des Bundesverfassungsgerichts gingen damals zahlreiche Ausführungen in der Literatur voraus, vgl. hierzu *Steinmüller* et al., BT-Drs. 6/3826; *Podlech*, DVR 1972/73, 149; *Schmidt*, JZ 1974, 241.

246 BVerfGE 65, 1 (Leitsatz 1).

247 BVerfGE 65, 1 (Leitsatz 1).

248 In seinem Beschluss zur Vorratsspeicherung von Kontostammdaten vom 13.6.2007 hat das BVerfG auch die beschränkte Anwendung des informationellen Selbstbestimmungsrechts auf juristische Personen anerkannt. Vgl. hierzu BVerfGE 118, 168: „Staatliche informationelle Maßnahmen können Gefährdungen oder Verletzungen der grundrechtlich geschützten Freiheit juristischer Personen herbeiführen und einschüchternd auf die Ausübung von Grundrechten wirken. In dieser Hinsicht ergibt sich ein Schutzbedürfnis, das dem natürlicher Personen im Ansatz entspricht. Allerdings ergibt sich insoweit ein Unterschied, als der Tätigkeitskreis juristischer Personen anders als der natürlicher Personen in der Regel durch eine bestimmte Zielsetzung begrenzt wird. Die Unterschiede, die zwischen den Schutzbedürfnissen natürlicher und juristischer Personen im Hinblick auf das Recht auf informationelle Selbstbestimmung bestehen, sind bei der Bestimmung der grundrechtlichen Gewährleistung zu beachten."

249 Vgl. hierzu etwa *Simitis*, NJW 1984, 399: „Die Entscheidung zum Volkszählungsgesetz ist deshalb nicht die Geburtsstunde eines neuen Grundrechts. Konkret: Ein Grundrecht auf Datenschutz gibt es genauso wenig wie vorher. Mit dem Recht auf informationelle Selbstbestimmung bestätigt das BVerfG vielmehr: Das Grundgesetz garantiert nicht die Verarbeitungsfreiheit, sondern begründet Verarbeitungsbarrieren."

der automatisierten Verarbeitung die erhobenen Daten verselbstständigen könnten, ohne dass es noch auf den ursprünglichen Verwendungszusammenhang ankomme. Nach dem Bundesverfassungsgericht gibt es kein belangloses Datum mehr. Erst wenn Klarheit über die Verwendung besteht, lässt sich auch die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.[250]

Das Recht auf informationelle Selbstbestimmung ist nach dem Bundesverfassungsgericht jedoch nicht schrankenlos gewährleistet. Es gibt keine absolute Herrschaft über die eigenen Daten.[251] Die Teilnahme am Rechtsverkehr erfordert in vielen Fällen gerade die Offenlegung von bestimmten Daten an einen bestimmten Personenkreis. Eingriffe in das informationelle Selbstbestimmungsrecht sind daher in bestimmten Fällen möglich. Der Einzelne muss Einschränkungen aber nur im überwiegenden Allgemeininteresse hinnehmen.[252] Solche Beschränkungen bedürfen nach Art. 2 Abs. 1 GG einer gesetzlichen Grundlage.[253] Als gesetzliche Grundlage ist nicht immer ein Gesetz im formellen Sinn erforderlich. Auch Rechtsverordnungen oder Satzungen von autonomen öffentlich-rechtlichen Verbänden wie zum Beispiel einer Körperschaft, Stiftung oder Anstalt können ausreichen.[254] Zudem können Betriebsvereinbarungen oder Dienstvereinbarungen eine gesetzliche Grundlage in diesem Sinne sein.[255] Interne Regelungen wie Verwaltungsvorschriften, Richtlinien oder Erlasse reichen jedoch nicht aus.[256]

Die gesetzliche Grundlage muss weiter den Anforderungen der Normenklarheit genügen, d.h. Voraussetzung, Umfang und Zweck der Einschränkung müssen klar und für den Bürger erkennbar sein.[257] Die gesetzliche Grundlage muss des Weiteren dem Prinzip der Verhältnismäßigkeit genügen.[258] Eine Grundrechtseinschränkung muss von hinreichenden Gründen des Gemeinwohls gerechtfertigt sein, das gewählte Mittel muss zur Erreichung des Zwecks geeignet und erforderlich sein und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe muss die Grenze des Zumutbaren gewahrt sein.

In seiner Entscheidung hat das Bundesverfassungsgericht weiter den Zweckbindungsgrundsatz aufgestellt.[259] Dieser besagt, dass jede in das informationelle Selbstbestimmungsrecht eingreifende Rechtsnorm eine präzise Bestimmung des Verwendungszweckes enthalten muss. Jede Datenverarbeitung muss an einem von vornherein festgehaltenen Zweck ausgerichtet werden.

---

250 Hierzu wieder etwa *Simitis*, NJW 1984, 402: „Unter diesen Umständen sind Spekulationen darüber, welche Daten noch als harmlos qualifiziert werden können oder wie die Sensibilität personenbezogener Angaben zu gewichten ist, sinnlos, ja gefährlich. Aufschluss über die Verarbeitungskonsequenzen gibt niemals die einzelne Angabe, sondern immer nur der konkrete Verwendungszusammenhang."

251 BVerfGE 65, 1 (43).

252 BVerfGE 65, 1 (43).

253 BVerfGE 65, 1 (43).

254 Zur Frage, in welchen Fällen ein Gesetz im formellen Sinne erforderlich ist, hat das Bundesverfassungsgericht die Wesentlichkeitstheorie entwickelt. Vgl. hierzu etwa BVerfGE 34, 165; BVerfGE 40, 237; BVerfGE 41, 251; BVerfGE 45, 400; BVerfGE 48, 210.

255 BAG, NJW 1987, 674; LAG Düsseldorf, RDV 1989, 243; BAG, RDV 1996, 1985.

256 *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 4 Rn. 19.

257 BVerfGE 65, 1 (44).

258 BVerfGE 65, 1 (44).

259 BVerfGE 65, 1 (46).

Eine Übermittlung von Daten ist grundsätzlich an den Erhebungszweck gebunden. Hieraus folgt, dass eine Vorratsdatenspeicherung und eine Verwendung oder Verarbeitung entgegen gesetzlichen Zwecken verboten ist.[260]

Das Volkszählungsurteil hat eine wichtige Bedeutung für die hier zu untersuchenden Bereiche. Aufgrund der Vorgaben, die die Richter in dieser Entscheidung machten (Vorbehalt des Gesetzes), wurden das Schriftgutaufbewahrungsgesetz des Bundes und des Landes Rheinland-Pfalz[261] und das Justizmitteilungsgesetz[262] geschaffen. Zum anderen wurden die Vorschriften zum Schuldnerverzeichnis aufgrund einer Gesetzesänderung im Jahr 1994 überarbeitet und wesentlich enger gefasst.[263]

4.2.1.2 Die Entscheidung zur Online-Durchsuchung von 2008

Das Bundesverfassungsgericht erkannte am 27.2.2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme an.[264] In seiner Entscheidung hatte das Bundesverfassungsgericht über die Verfassungsmäßigkeit der sog. Online-Durchsuchung zu entscheiden.[265] Konkret ging es um Vorschriften des Verfassungsschutzgesetzes von Nordrhein-Westfalen, die Befugnisse der Verfassungsschutzbehörde zu verschiedenen Datenerhebungen insbesondere aus dem informationstechnischen Systemen sowie zum Umgang mit den erhobenen Daten regelten. Das Bundesverfassungsgericht hat dieses Grundrecht ebenfalls aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 GG abgeleitet.[266] Die Nutzung informationstechnischer Systeme ist nach dem Gericht für die Persönlichkeitsentfaltung vieler Bürger von zentraler Bedeutung, begründet gleichzeitig aber auch neuartige Gefährdungen der Persönlichkeit. In modernen IT-Systemen werden zum einen ununterbrochen vielfältige Daten in großem Umfang erzeugt, verarbeitet und gespeichert, die weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen.[267] Zum anderen ergeben sich neuartige Gefährdungen für den Benutzer, weil er darauf angewiesen ist, dass die IT-Systeme ihre Funktion integer und unmanipuliert erbringen. In diesem Zusammenhang stellte das Bundesverfassungsgericht Schutzlücken bei den bestehenden Grundrechten fest.[268] Art. 10 GG und Art. 13 GG seien nicht einschlägig. Auch das Recht auf informationelle Selbstbestimmung trägt den Persönlichkeitsgefährdungen nicht vollständig Rechnung. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere

[260] Vgl. hierzu Abschnitt 5.1.2.
[261] Vgl. hierzu Abschnitt 4.3.4.3
[262] Vgl. hierzu Abschnitt 4.3.4.4
[263] Vgl. hierzu Abschnitt 8.1.1
[264] BVerfG, NJW 2008, 822.
[265] Zum neuen IT-Grundrecht, vgl. etwa *Roßnagel/Schnabel*, NJW 2008, 3534; *Hoeren*, MMR 2008, 365; *Eifert*, NVwZ 2008, 521; *Bartsch*, CR 2008, 613; *Kutscha*, NJW 2008, 1042; *Leisner*, NJW 2008, 2902; *Gusy*, DuD 2009, 33; *Manssen* et al., 2009.
[266] BVerfG, NJW 2008, 824.
[267] BVerfG, NJW 2008, 824.
[268] BVerfG, NJW 2008, 824.

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.

Der Schutz des neuen Grundrechts beschränkt sich auf einzelne oder vernetzte IT-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 seiner Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf einen PC oder solche Mobiltelefone oder elektronischen Kalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können. Dagegen erstreckt sich der Schutz nicht auf Systeme, die nach ihrer technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen erhalten. Hierzu gehören etwa elektronische Steueranlagen der Haustechnik.

Das neue Grundrecht gewährleistet sowohl die Vertraulichkeit der Daten als auch die Integrität des IT-Systems. Damit ist zunächst das Interesse des Nutzers geschützt, dass die von einem vom Schutzbereich erfassten IT-System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.[269] Das Grundrecht verhindert des Weiteren, dass auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können. In diesem Fall ist nämlich die entscheidende technische Hürde für eine Ausspähung und Überwachung genommen.[270] Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätsprüfung besteht jedoch nur dann, wenn der Betroffene das IT-System als sein eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das IT-System selbständig verfügt.[271]

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Der Einzelne muss dabei nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen.

Die Entscheidung des Bundesverfassungsgerichts hat zu einem erheblichen Gewinn für den Datenschutz beigetragen. Durch das neue Grundrecht sind die Anforderungen an die Datensicherheit insgesamt gestiegen. Dies wirkt sich auch auf die hier zu untersuchenden Bereiche aus. So wird die Justiz in Zukunft in verstärktem Maße dafür sorgen müssen, dass etwa Angriffe von „eigenen“ Justizrechnern aus auf Rechner von Parteien, Verfahrensbeteiligten oder Anwälten zum Beispiel durch das Einschleusen von Schadsoftware durch Mitarbeiter oder Personen, die sich als solche ausgeben, ausgeschlossen werden.[272]

---

269 *Roßnagel/Schnabel*, NJW 2008, 3535.

270 *Roßnagel/Schnabel*, NJW 2008, 3535.

271 *Roßnagel/Schnabel*, NJW 2008, 3535.

272 Zu den Schutzpflichten von Grundrechten vgl. Abschnitt 4.2.3, zu den Anforderungen an die Datensicherheit vgl. Abschnitt 5.2.

Zum Teil wurde das Urteil des Bundesverfassungsgerichts kritisiert.[273] Diese Kritik bezog sich vor allem darauf, dass es angesichts des informationellen Selbstbestimmungsrechts keines neuen Grundrechts bedurft hätte. Mit dem Recht auf informationelle Selbstbestimmung stehe ein Grundrecht zur Verfügung, das die immer bedeutsamer werdende Persönlichkeitsentfaltung mittels informationstechnischer Systeme hinreichend schütze. Das Recht auf informationelle Selbstbestimmung werde in der Online-Entscheidung verkürzt. Umfassende Datenerhebungsmöglichkeiten seien als nicht mehr erfasst angesehen worden und die vermeintliche Schutzlücke sei durch das neue Grundrecht geschlossen worden.[274] Dem kann jedoch nicht zugestimmt werden. Der abwehrrechtliche Gehalt des Grundrechts wurde in der Vergangenheit von Rechtsprechung und Literatur überbetont.[275] Das Grundrecht auf informationelle Selbstbestimmung reagiert als Abwehrrecht nur punktuell auf eine Persönlichkeitsgefährdung. Der Betroffene ist auf die Nutzung eines informationstechnischen Systems heute in vielen Bereichen angewiesen. Bei der Benutzung eines IT-Systems vertraut er dem System vielfältige Daten an – allein schon dann, wenn er das System nur bedient. Ein Zugriff auf ein IT-System mit einem derartigen großen und aussagekräftigen Datenbestand würde über einzelne Datenerhebungen, die vom informationellen Selbstbestimmungsrecht geschützt sind, weit hinausgehen. Mit dem neuen Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme hat das Bundesverfassungsgericht auf die neuen Bedrohungen durch den Einsatz von IT-Systemen daher zutreffend reagiert.

4.2.1.3 Notwendigkeit einer Grundgesetzänderung

Mit dem Urteil zur Volkszählung und mit dem Urteil zur Online-Durchsuchung hat das Bundesverfassungsgericht dem Datenschutz Verfassungsrang eingeräumt. Dennoch ist der Datenschutz – im Unterschied zu anderen Staaten und den Verfassungen von verschiedenen Bundesländern[276] – nie als Grundrecht in das Grundgesetz aufgenommen worden. In der Vergangenheit gab es hierzu zwar mehrere Initiativen. Zuletzt hatte im Jahr 2008 die Fraktion Bündnis 90/Die Grünen einen Gesetzentwurf in den Deutschen Bundestag eingebracht,[277] welcher neben der grundrechtlichen Gewährleistungen auf Selbstbestimmung über persönliche Daten (Art. 2a) auch die Verankerung der Informationsfreiheit (Art. 5a) und den Schutz informationstechnischer Systeme sowie die Absicherung des absoluten Schutzes des Kernbereichs privater Lebensgestaltung im Wortlaut der Verfassung vorsah.[278] Durchsetzen konnten sich die Initiativen bislang jedoch noch nicht.[279]

[273] Vgl. hierzu etwa *Eifert*, NVwZ 2008, 521; *Hoeren*, MMR 2008, 365.
[274] *Eifert*, NVwZ 2008, 523.
[275] Vgl. hierzu *Bäcker*, in: *Manssen* at al. (Hrsg.), Computergrundrecht, 5 m.w.N.
[276] Vgl. hierzu etwa *Roßnagel*, KJ, 99 m.w.N.
[277] BT-Drs. 16/9607.
[278] *Künast*, ZRP 2008, 203.
[279] Weitere Initiativen waren zum Beispiel diejenige der Gemeinsamen Verfassungsreform von Bund und Ländern aus dem Jahr 1993. In der 17. Sitzung am 11.2.1993 verpasste diese Initiative jedoch die erforderliche Mehrheit von zwei Dritteln der Kommissionsmitgliedern, nachdem die Ergänzung von der Verfassungskommission des Bundesrates zuvor befürwortet war (BT-Drs. 12/6000, 61) und sich auch die

Gegen die Einführung eines Rechts auf informationelle Selbstbestimmung im Grundgesetz wird geltend gemacht, dass einfachgesetzliche Regelungen ausreichen würden, das Grundrecht zu schützen.[280] Auch wird argumentiert, dass die Privilegierung des Rechts auf informationelle Selbstbestimmung gegenüber den anderen, aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Rechten, nicht gerechtfertigt sei.[281] Zudem wird als Argument gegen die Aufnahme das Gebot der Zurückhaltung im Sinne einer verfassungsrechtlichen Kontinuität hervorgebracht.[282]

Dem ist jedoch entgegenzuhalten, dass eine formelle Verfassungsänderung im Hinblick auf das dann zu beachtende Zitiergebot einen rechtlichen Unterschied zum Status quo darstellen würde. Für die Bürger wäre mit einer Verfassungsänderung deutlicher erkennbar, dass unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte.[283] Außerdem würde der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie Rechnung getragen. Der Grundrechtskatalog würde dem technologischen Wandel angepasst und die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.[284]

Konferenz der Datenschutzbeauftragten des Bundes und der Länder dem angeschlossen hatte (vgl. hierzu *DSB-Konferenz*, 28.4.1992). Ein Jahr später hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder anlässlich der zehnjährigen Geburtsstunde des Volkszählungsurteils (*DSB-Konferenz*, 9./10.3.1994) ihre Forderung wiederholt: „Zwar ist die verfassungsrechtliche Dimension des Datenschutzes unbestritten. Gleichwohl fehlt der informationellen Selbstbestimmung das Fundament im Grundgesetz. Eine grundlegende Verbesserung könnte erreicht werden, wenn zehn Jahre nach der Anerkennung des Grundrechts auf Datenschutz durch das Bundesverfassungsgericht dieses Grundrecht auch ausdrücklich in das Grundgesetz aufgenommen werden würde. Dass die erforderliche Mehrheit im Bundesrat und Bundestag hierfür bisher nicht erreicht werden konnte, bedauert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich."

280 Vgl. hierzu BT-Drs. 12/6000, 62: „Die Feststellung des BVerfG (...) sei mit klaren Aufträgen an den Gesetzgeber einhergegangen. (...) Der Umfang des verfassungsrechtlich gewährleisteten Schutzes lasse keine regelungsbedürftige Lücke erkennen."

281 Vgl. hierzu BT-Drs. 12/6000, 63: „Zudem würde mit einer Grundgesetzänderung nur ein Teilbereich des allgemeinen Persönlichkeitsrechts ausdrücklich hervorgehoben, während andere ähnlich gewichtige Inhalte – wie z.B. die Ehre oder das Selbstdarstellungsrecht – unerwähnt blieben. Da Grundrechte immer auch zur objektiven Wertordnung der Verfassung beitragen, könnte die Nichterwähnung anderer Teilbereiche des allgemeinen Persönlichkeitsrechts für diese die Gefahr einer Abwertung mit sich bringen."

282 Vgl. hierzu grundsätzlich *Bryde*, 1982 und *Hesse*, 1959. Zudem BT-Drs. 12/6000, 63: „Verfassungsänderungen seien nur dann geboten, wenn neue Wertentscheidungen auf der Ebene der Verfassung festgeschrieben werden sollen, die bislang nicht erfasst sind. Diese treffen für das Recht auf informationelle Selbstbestimmung aber nicht zu."

283 *Künast*, ZRP 2008, 201.

284 Vgl. hierzu wiederum *Künast*, ZRP 2008, 201. Nach *Roßnagel*, KJ, 99 kommt es dagegen weniger auf die textliche Änderung des Datenschutzes im Grundgesetz als vielmehr auf eine Anpassung des Schutzkonzeptes an die künftigen Herausforderungen an.

4.2.2 Die Landesverfassung

In Rheinland-Pfalz ist der Datenschutz seit dem Jahr 2000 in Art. 4a[285] gesetzlich in der Landesverfassung (LV) verankert.[286] Neben Rheinland-Pfalz enthalten die Verfassungen der Länder Nordrhein-Westfalen (1978), Saarland (1985), Sachsen (1992), Sachsen-Anhalt (1992), Brandenburg (1992), Mecklenburg-Vorpommern (1993), Thüringen (1993), Berlin (1995) und Bremen (1997) das Grundrecht auf Datenschutz. Art. 4a LV formuliert ein für alle – Deutsche, Ausländer und Staatenlose – geltendes Menschenrecht. Grundrechtsträger sind alle natürlichen Personen. Art. 4a Abs. 1 Satz 1 LV enthält ein Abwehrrecht und schützt vor unberechtigter Erhebung und Verarbeitung personenbezogener Daten. Satz 2 der Vorschrift garantiert ein Auskunfts- und Akteneinsichtsrecht. Dieses ist eine notwendige verfahrensrechtliche Konsequenz, über die eigenen Daten selbst zu bestimmen.[287] Es ist für die Betroffenen von zentraler Bedeutung. Einfachgesetzlich findet sich dieses Recht in § 18 LDSG wieder.[288] Abs. 2 lässt Einschränkungen des Grundrechts zu, soweit überwiegende Interessen der Allgemeinheit dies erfordern. Dies hatte wie bereits gesehen das Bundesverfassungsgericht in seinem Volkszählungsurteil entschieden.[289] Danach bedürfen Beschränkungen einer gesetzlichen Grundlage, aus der sich Voraussetzungen und der Umfang der Beschränkung klar und für den Bürger erkennbar ergeben.[290] Aufgrund verfassungsmäßig ausreichender Ermächtigung erlassene Rechtsverordnungen reichen dabei aus, Verwaltungsvorschriften können einen Grundrechtseingriff jedoch nicht legitimieren.[291] Die Verankerung des Datenschutzes in der Landesverfassung stellt die Bedeutung des Datenschutzes nochmals in den Vordergrund. Der Verfassungsgeber auf Bundesebene sollte sich hieran orientieren. Anlässlich einer Änderung der Landesverfassung wäre zu überlegen, ob man Art. 4a LV um das neue Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ergänzt.

4.2.3 Schutzpflichten von Grundrechten

Grundrechte gelten gemäß Art. 1 Abs. 3 GG grundsätzlich nur im Verhältnis zwischen Bürger und Staat. Ihre eigentliche Aufgabe ist die Abwehr von und der Schutz vor staatlichen Eingriffen.[292] Grundrechte sind aber nicht nur subjektive Abwehrrechte gegen den Staat. Ih-

[285] Art. 4a hat folgenden Wortlaut: Jeder Mensch hat das Recht, über die Erhebung und weitere Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen. Jeder Mensch hat das Recht auf Auskunft über ihn betreffende Daten und auf Einsicht in amtliche Unterlagen, soweit diese solche Daten enthalten (Abs. 1). Diese Rechte dürfen nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern (Abs. 2).

[286] Vgl. hierzu 34. Änderungsgesetz vom 8.3.2000, GVBl. 2000, 65. Dieses Gesetz ist seit dem rheinland-pfälzischen Verfassungstag, dem 18.5.2000, gemäß Art. 2 Satz 1 in Kraft.

[287] *Rudolf*, in: *Grimm/Caesar*, Verfassung für Rheinland-Pfalz, 88 f.

[288] Vgl. hierzu Abschnitt 5.4.1.

[289] Vgl. hierzu Abschnitt 4.2.1.1.

[290] BVerfGE 65, 1 (44).

[291] *Rudolf*, in: *Grimm/Caesar*, Verfassung für Rheinland-Pfalz, 89.

[292] Vgl. etwa BVerfGE 7, 198 (204); BVerfGE 50, 290 (336); BGH, NJW 1975, 158.

nen kommt vielmehr auch eine schützende und staatliches Handeln leitende Funktion zu.[293] Staatliche Organe sind nicht nur zur Abwehr von Schäden, sondern auch zu einer aktiven umfassenden vorausschauenden Vorsorge für Freiheits- und Gleichheitsrechte verpflichtet. Sie haben dafür zu sorgen, dass die notwendigen rechtlichen und sonstigen wirtschaftlichen, sozialen und kulturellen Voraussetzungen für die Wahrnehmung der grundrechtlichen Freiheiten bestehen. Sie dürfen daher technische Systeme nicht ohne weiteres zulassen. Sie müssen vielmehr steuernd auf sie eingreifen, wenn deren Anwendung Grundrechten den Boden entziehen würde. Wenn technische Entwicklungen in der Lage sind, Sachzwänge zu schaffen, werden nachträgliche Korrekturen weitgehend wirkungslos sein. Um die normative Wirksamkeit der Grundrechte für die Zukunft zu sichern, bedarf es daher vorausschauender Untersuchungen grundrechtsbedrohender Entwicklungen.[294] Vor diesem Hintergrund hat der Gesetzgeber eine Schutzpflicht gerade auch im Bereich der IT. Der Staat muss die notwendigen Rahmenbedingungen dafür schaffen, dass die Bürger sicher im Internet kommunizieren können. Diesen Schutzpflichten ist der Gesetzgeber mit dem Signaturgesetz und der dazu ergangenen Signaturverordnung und dem Personalausweisgesetz nachgekommen. Es bleibt abzuwarten, ob auch das Bürgerportalgesetz verabschiedet werden wird. In diesem Kontext wird sich dann in Zukunft auch die Frage stellen, ob Elemente der IT-Ausstattung des Einzelnen (z.B. Versorgung mit einem Breitband-Internetanschluss oder die zum Einsatz des elektronischen Identitätsnachweises erforderliche Infrastruktur) zwingender Bestandteil einer sozio-kulturellen Grundversorgung der Bevölkerung sind und der Staat hier im Sinne einer E-Daseinsvorsorge zum steuernden Eingriff in den Markt verpflichtet ist.[295]

4.3 Das einfache Recht

4.3.1 Das Bundesdatenschutzgesetz

Das Datenschutzrecht ist durch drei, oder wenn man die Novellen des BDSG von 2009 hinzuzählen möchte, durch vier Phasen geprägt. Die erste Phase begann in den 70er Jahren mit der Verabschiedung der Datenschutzgesetze. Das BDSG trat hinsichtlich seiner wesentlichen Teile 1978 in Kraft.[296] Davor gab es bereits in Hessen[297] und in Rheinland-Pfalz[298] ein Datenschutzgesetz. Wesentlich waren dabei das Verbotsprinzip, d.h. der allgemeine Grundsatz, dass die Speicherung und weitere Verarbeitung personenbezogener Daten nur auf der Grundlage der

[293] Dabei richtet sich die Schutzpflicht vor allem an den Gesetzgeber. Nach dem Bundesverfassungsgericht steht ihm hierbei jedoch ein weiter Einschätzungs- und Gestaltungsspielraum zu (vgl. zum Beispiel BVerfGE 77, 170 (214); BVerfGE 79, 174 (202); BVerfGE 85, 191 (212)), der durch ein Untermaßverbot beschränkt ist, das ein Mindestmaß an Schutz gebietet (vgl. zum Beispiel BVerfGE 88, 203 (254)).

[294] Zu diesen Fragestellungen vgl. etwa schon *Roßnagel*, ZRP 1992, 55; *Roßnagel*, UPR 1986, 46.

[295] Zu dieser Fragestellung vgl. *Schulz/Schulz*, MMR 2009, 19.

[296] BGBl. 1977 I, 729. Zu den Einzelheiten des Gesetzgebungsverfahrens vgl. ausführlich *Liedtke*, 1980.

[297] GVBl. 1970 I, 625.

[298] GVBl. 1974 I, 31.

freiwillig erteilten Einwilligung des Betroffenen oder eines Gesetzes zulässig sein sollte.[299] Für die privaten Datenverarbeiter, die die elektronische Datenverarbeitung (EDV) geschäftsmäßig nutzten (für sonstige private Datenverarbeitungen galt und gilt das Datenschutzgesetz nicht), war maßgeblich, ob die Datenverarbeitung im Rahmen der Erfüllung der Geschäftszwecke lag und ob berechtigte Interessen an der Datenverarbeitung die schutzwürdigen Belange der Betroffenen überwogen. Begleitet wurden diese Grundregeln durch Ansprüche der Betroffenen auf Benachrichtigung, Auskunft, Berichtigung und Löschung, ggf. durch Schadensersatzansprüche, durch Meldepflichten der datenverarbeitenden Stellen, durch Pflichten der datenverarbeitenden Stellen zur Einrichtung von Datensicherungsmaßnahmen, durch die Überwachung durch externe Kontrollinstitutionen sowie durch Strafvorschriften für rechtswidrige Datenverarbeitungen.[300]

Wichtige Änderungen erfuhren die Datenschutzgesetze dann durch die zweite Phase.[301] In dieser wurde das Volkszählungsurteil umgesetzt, der Anwendungsbereich wurde auf die manuell in Akten gespeicherten Daten erweitert, der Zweckbindungsgrundsatz wurde betont und die Betroffenenrechte wurden ausgeweitet.[302]

Die dritte Phase[303] hatte die Anpassung an die Datenschutzrichtlinie zum Inhalt. Die Novelle enthielt im Wesentlichen Änderungen, die zur Anpassung an die EG-Datenschutzrichtlinie ohnehin unabdingbar waren. Man entschied sich hier für eine „kleine Lösung“. Dies waren u.a. die Aufnahme der Grundsätze der Datenvermeidung und Sparsamkeit, anonymes und pseudonymes Handeln und die Verankerung einer Regelung zum Datenschutzaudit, Regelungen zur Videoüberwachung, zu mobilen Speicher- und Verarbeitungsmedien, die Erweiterung des sachlichen Anwendungsbereiches des Gesetzes für die Privatwirtschaft, indem jede unter Einsatz von Datenverarbeitungsanlagen erfolgende Verarbeitung personenbezogener Daten erfasst wird, sowie Vorgaben zum grenzüberschreitenden Datenverkehr und die Erweiterung der Regelungen der Datenschutzkontrolle durch die Aufsichtsbehörde.[304]

Im Unterschied zu den vorherigen Novellen betrafen die drei Novellen von 2009 ausschließlich den Bereich des privaten Datenschutzrechts.[305] Mit der Datenschutznovelle I[306] hat der Gesetzgeber im Wesentlichen den Umgang mit personenbezogenen Daten in Auskunfteien modifiziert. In der Datenschutznovelle II[307] hat er den Datenschutz in der Werbung und in Beschäftigungsverhältnissen neu geregelt. In der Datenschutznovelle III[308] wurden in Umsetzung der EU-Verbraucherkreditrichtlinie Pflichten von Datenbankbetreibern geschaffen, denen

299 *Abel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 201.
300 Hierzu etwa *Abel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 196.
301 BGBl. 1990 I, 2955 (Bund); GVBl. 1994, 263 (Land Rheinland-Pfalz).
302 Hierzu etwa *Abel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 207 ff.
303 BGBl. 2001 I, 904 (Bund); GVBl. 2002, 177 (Land Rheinland-Pfalz).
304 Hierzu etwa *Abel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 212.
305 Zu diesen vgl. zum Beispiel *Roßnagel*, NJW 2009, 2716; *Abel*, RDV 2009, 147.
306 BGBl. 2009 I, 2254.
307 BGBl. 2009 I, 2814.
308 BGBl. 2009 I, 2384.

sich Darlehensgeber zur Bewertung der Kreditwürdigkeit potentieller Kunden bedienen. Anlass und Anstoß für diese Novellen waren jeweils konkrete Probleme.[309]

Da sich die Informationstechnik und ihre Nutzung in Wirtschaft und Verwaltung inzwischen qualitativ und quantitativ gewaltig verändert hat, wird seit mehr als zehn Jahren eine grundsätzliche Novellierung des Datenschutzrechts gefordert.[310] Es bleibt abzuwarten, ob sich diese Forderungen in naher Zukunft erfüllen werden. Der Koalitionsvertrag zur 17. Legislaturperiode enthält jedoch zumindest dahingehende Aussagen.[311]

4.3.1.1 Die Gesetzgebungskompetenz

Eine ausdrückliche Kompetenz zur Regelung des Datenschutzes ist im Grundgesetz weder dem Bund noch den Ländern zugewiesen. Die Gesetzgebungskompetenz des Bundesgesetzgebers für die Regelung des Datenschutzrechtes für den öffentlichen Bereich ergibt sich aus Art. 70 ff. i.V.m. Art. 84 Abs. 1, 85 Abs. 1 und Art. 86 GG.[312] Die Gesetzgebungskompetenz des Bundes für den privaten Bereich wird allgemein anerkannt. Die Begründungen hierfür sind jedoch verschieden: Teilweise wird die Kompetenz des Bundesgesetzgebers aus der Kompetenz zur Regelung des Bürgerlichen Rechts gemäß Art. 74 Nr. 1 GG abgeleitet.[313] Andere sehen sie in der Befugnis zur Regelung des Rechts der Wirtschaft gemäß Art. 74 Nr. 11 GG[314] oder in einer spezifischen Gesamtschau aller spezifischen Kompetenzen des Art. 74 GG.[315]

4.3.1.2 Der persönliche Anwendungsbereich des BDSG

Der Bundesgerichtshof als öffentliche Stelle des Bundes Der grundsätzliche Anwendungsbereich des BDSG für die Gerichte ergibt sich aus § 1 Abs. 2 Nr. 1 BDSG. Danach gilt das BDSG für öffentliche Stellen des Bundes. Nach § 2 Abs. 1 BDSG sind öffentliche Stellen des Bundes u.a. die Organe der Rechtspflege des Bundes. Zu den Organen der Rechtspflege des Bundes gehört im Bereich der ordentlichen Gerichtsbarkeit u.a. der Bundesgerichtshof.[316] Das BDSG findet auf den Bundesgerichtshof sowohl in seiner Eigenschaft als Justizverwal-

309 *Roßnagel*, NJW 2009, 2716.

310 Vgl. hierzu *Roßnagel*, NJW 2009, 2716 mit Verweis auf *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253; *Ahrend* et al., DuD 2003, 433; *Bizer*, DuD 2001, 274; *Bizer*, DuD 2004, 6; *Roßnagel*, MMR 2005, 71 sowie auf die 32. Sitzung des Innenausschusses am 5.3.2007, BT-Drs. 16/4882.

311 In *CDU, CSU und FDP*, Koalitionsvertrag, 97 heißt es hierzu: „Ein moderner Datenschutz ist gerade in der heutigen Informationsgesellschaft von besonderer Bedeutung. Wir wollen ein hohes Datenschutzniveau. Die Grundsätze der Verhältnismäßigkeit, der Datensicherheit und -sparsamkeit, der Zweckbindung und der Transparenz wollen wir im öffentlichen und privaten Bereich noch stärker zur Geltung bringen. Hierzu werden wir das Bundesdatenschutzgesetz unter Berücksichtigung der europäischen Rechtsentwicklung lesbarer und verständlicher machen sowie zukunftsfest und technikneutral ausgestalten."

312 BT-Drs. 7/1027, 16. Für eine Ergänzung des Grundgesetzes plädiert *Podlech*, DVR Beiheft 1 1973, 2.

313 *von Münch/Kunig*, GG, Art. 74 Rn. 5.

314 *Mallmann*, 1995, 115.

315 BT-Drs. 7/1027, 16.

316 Daneben zählen zu den Organen der Rechtspflege des Bundes unter anderem das Bundesverfassungsgericht und die Bundesgerichte sowie der Generalbundesanwalt beim Bundesgerichtshof und der Oberbun-

tungsbehörde als auch als Spruchkörper, also in seiner Funktion als rechtsprechende Gewalt, Anwendung. Rechtsanwälte sind zwar nach § 1 Bundesrechtsanwaltsordnung (BRAO) ebenfalls Organe der Rechtspflege. Sie sind jedoch kein Organ der Rechtspflege des Bundes.[317] § 1 Abs. 2 Nr. 1 BDSG erfasst daher nicht Rechtsanwälte.

Keine Anwendung des BDSG auf Gerichte von Rheinland-Pfalz § 1 Abs. 2 Nr. 2b BDSG bestimmt, dass das BDSG auf Landesorgane der Rechtspflege nur anwendbar ist, soweit keine landesrechtliche Regelungen existieren und soweit die Gerichte nicht in Verwaltungsangelegenheiten handeln. In Rheinland-Pfalz existiert mit § 2 Abs. 1 Nr. 2 LDSG eine landesrechtliche Regelung. Nach dieser Vorschrift ist das LDSG auf die Organe der Rechtspflege uneingeschränkt anwendbar und damit sowohl für den Bereich der Rechtspflege als auch für den der Justizverwaltung. Das rheinland-pfälzische LDSG gehört damit zu jenen Landesdatenschutzgesetzen, die das BDSG in ihrem Anwendungsbereich in vollem Umfang verdrängen. Für den Bereich der ordentlichen Gerichtsbarkeit bedeutet dies, dass die beiden Oberlandesgerichte, die Landgerichte und die Amtsgerichte von Rheinland-Pfalz vom Anwendungsbereich des BDSG ausgenommen sind.[318]

Neben dem rheinland-pfälzischen LDSG verdrängen außerdem die Landesdatenschutzgesetze von Baden-Württemberg,[319] Bayern,[320] Berlin,[321] Hamburg,[322] Hessen,[323] Niedersachsen,[324] Sachsen,[325] Sachsen-Anhalt,[326] Schleswig-Holstein[327] und Thüringen[328] das BDSG im gesamten Bereich der Rechtspflege.

Andere Landesdatenschutzgesetze regeln dagegen nur den Bereich der Justizverwaltung. Sie verdrängen das BDSG also nur im Bereich der Justizverwaltung, d.h. dass das BDSG auf den rechtsprechenden Teil in vollem Umfang anwendbar bleibt. Hierzu gehören die Landes-

desanwalt beim Bundesverwaltungsgericht. Vgl. hierzu *Schöttle*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 179; *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 2 Rn. 27.

317 *Gola/Schomerus*, BDSG, § 2 Rn. 12.

318 Des Weiteren sind selbstverständlich auch die hier nicht interessierenden Landesverfassungsgerichte, das Oberverwaltungsgericht, die Verwaltungsgerichte, das Landesarbeitsgericht, die Arbeitsgerichte und die Landes-(Sozialgerichte) sowie die Finanzgerichte, die Generalstaatsanwaltschaften und die Staatsanwaltschaften vom Anwendungsbereich ausgenommen.

319 § 2 Abs. 3 LDSG.

320 Art. 2 Abs. 1 BayDSG.

321 § 2 Abs. 1 BInDSG.

322 § 2 Abs. 1 Nr. 1 HmbDSG.

323 § 3 Abs. 1 HDSG.

324 § 2 Abs. 1 Nr. 1 NDSG.

325 § 2 Abs. 1 SächsDSG.

326 § 3 Abs. 1 DSG-LSA.

327 § 3 Abs. 1 LDSG.

328 § 2 Abs. 1 ThürDSG.

datenschutzgesetze von Bremen,[329] Brandenburg,[330] Mecklenburg-Vorpommern,[331] Nordrhein-Westfalen,[332] und dem Saarland[333].

Anwälte und Parteien als nicht-öffentliche Stellen Gemäß § 1 Abs. 2 Nr. 3 BDSG findet das Bundesdatenschutzgesetz auch auf nicht-öffentliche Stellen Anwendung. Nicht-öffentliche Stellen sind nach § 2 Abs. 4 BDSG natürliche und juristische Personen, Gesellschaften und – in der Regel – andere Personenvereinigungen des privaten Rechts. Im Bereich der Justiz kommen als nicht-öffentliche Stellen Rechtsanwälte, Parteien und Verfahrensbeteiligte in Betracht. Während bei Parteien und Verfahrensbeteiligten die Anwendbarkeit des BDSG unproblematisch ist, ergeben sich Probleme bei den Rechtsanwälten.

§ 1 Abs. 3 Satz 1 BDSG lautet: „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften des BDSG vor.“ Aus dieser Vorschrift könnte man schließen, dass § 203 StGB und § 43a Abs. 2 BRAO als andere Rechtsvorschriften des Bundes, die datenschutzrechtliche Fragen betreffen, dem Bundesdatenschutzgesetz vorgehen und allein die Probleme anwaltlicher Datenverarbeitung regeln.[334] In der Tat wird diese Auffassung in der Literatur vertreten.[335] Dem kann jedoch nicht zugestimmt werden. Bei § 203 StGB und bei § 43a Abs. 2 BRAO geht es lediglich um die Vertrauensbeziehung zwischen Anwalt und Mandant. Um diese Beziehung nicht zu gefährden, wird der Anwalt zur Verschwiegenheit verpflichtet. Das BDSG hat hingegen einen weiteren Anwendungsbereich. Geschützt werden nach dem BDSG nicht nur der Mandant, sondern auch Dritte, also zum Beispiel auch die gegnerische Partei. Über deren Schutz sagen die genannten Vorschriften aber nichts aus. Man kann daher sagen, dass wegen der eingeschränkten Sichtweise des § 203 Strafgesetzbuch (StGB) und des § 43a Abs. 2 BRAO diese Vorschriften nicht die gesamten Regelungen des Bundesdatenschutzgesetzes aufheben.[336] Auch § 1 Abs. 3 Satz 2 BDSG schließt im Übrigen die Anwendbarkeit des BDSG auf die anwaltliche Datenverarbeitung nicht aus. Diese Vorschrift dient nur der Klarstellung und besagt lediglich, dass Geheimhaltungspflichten standesrechtlicher Art stets beachtet werden müssen.[337] Das Bundesdatenschutzgesetz ist daher auf anwaltliche Datenverarbeitung anwendbar.[338]

Ungeachtet dessen ist jedoch zu beachten, dass es in Einzelfällen zu einer Konfliktsituation zwischen Mandantengeheimnis und Datenschutz kommen kann. Vor allem die Gegner eines Rechtsstreits könnten versuchen, über die Inanspruchnahme ihrer Datenschutzrechte ihre Po-

329 § 1 Abs. 4 BremDSG.
330 § 2 Abs. 1 BbDSG.
331 § 2 Abs. 4 DSG M-V.
332 § 2 Abs. 1 DSG NRW.
333 § 2 Abs. 1 SDSG.
334 *Redeker*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 44.
335 So *Rüpke*, 1995 und insbesondere *Rüpke*, NJW 2008, 1121; *Rüpke*, ZRP 2008, 87.
336 *Redeker*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 44.
337 *Schaffland/ Wiltfang*, BDSG, § 1 Rn. 35.
338 Die sog. Sphären- oder Schnittmengentheorie will dagegen im jeweiligen Einzelfall prüfen, ob die Vorschriften des BDSG anwendbar sind oder ob sie von § 43a BRAO oder § 203 StGB überlagert werden, vgl. *Abel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 1334.

sition zu verbessern.[339] Diese lassen sich jedoch allein durch eine saubere Subsumtion der Regelungen des BDSG lösen. Hierzu zwei Beispiele: § 34 Abs. 1 BDSG gibt dem Betroffenen gegenüber der verantwortlichen Stelle einen Auskunftsanspruch über die zu seiner Person gespeicherten personenbezogenen Daten. Mittels eines derartigen Anspruchs gegen den Rechtsanwalt könnte ein Gegner in einem Rechtsstreit versuchen, die Prozessstrategie und das beim Prozessgegner vorhandene Wissen auszuspionieren.[340] § 34 Abs. 7 BDSG gibt hierauf jedoch eine zufriedenstellende Antwort. So besteht nach § 34 Abs. 7 BDSG i.V.m. § 33 Abs. 2 Satz 1 Nr. 3 BDSG für die verantwortliche Stelle keine Pflicht zur Auskunftserteilung, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen. Diese Norm zielt ausdrücklich auf gesetzliche Geheimhaltungspflichten, z.B. die des Anwalts hinsichtlich seiner beruflichen Tätigkeit[341] und gibt daher eine ausreichende Antwort im Hinblick auf eine etwaige Konfliktsituation. Das nächste Beispiel: § 35 Abs. 1 BDSG gibt im Falle unrichtig gespeicherter Informationen einen Berichtigungsanspruch. Dieser könnte von einem Gegner dazu missbraucht werden, die Beweislage bezüglich inhaltlich bestrittener Sachverhalte außerprozessual zu beeinflussen.[342] Ein derartiger Berichtigungsanspruch aus Anwaltsakten durch Dritte kann in der Regel jedoch nicht erfolgreich durchgesetzt werden. Denn es ist anerkannt, dass die Dokumentation in einer Anwaltsakte kein Beleg für die Richtigkeit oder Unrichtigkeit eines Sachverhalts ist, sondern darüber, dass die Richtigkeit oder Unrichtigkeit dieses Sachverhaltes behauptet wird.[343]

4.3.1.3 Der sachliche Anwendungsbereich des BDSG

Definition Personenbezogene Daten sind in § 3 BDSG gesetzlich definiert als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.[344] Der Begriff findet sich auch in § 203 Abs. 2 Satz 2 StGB sowie in § 16 Abs. 1 des Gesetzes über die Statistik für Bundeszwecke.[345] Im Gegensatz zu diesen Vorschriften kommt es jedoch nicht darauf an, zu welchem Zweck die Daten erfasst wurden. Auch ist es gleichgültig, woher sie stammen. Der Begriff Angabe umfasst jede Information.[346] Notwendig ist lediglich ein finales, auf Vermittlung oder Aufbewahrung gerichtetes Element. Mit dem Begriff der Angaben zu den persönlichen und sachlichen Verhältnisse einer Person wollte der Gesetzgeber deutlich machen, dass er alle Informationen, die über die Bezugsperson etwas aussagen, erfassen will. Der Begriff ist daher außerordentlich weit zu verstehen. Tendenzen in der Literatur,[347] den Datenschutz auf einen bestimmten Teilbereich der personenbezogenen In-

339 *Weichert*, NJW 2009, 552.
340 *Weichert*, NJW 2009, 552.
341 *Weichert*, NJW 2009, 552.
342 *Weichert*, NJW 2009, 552.
343 *Weichert*, NJW 2009, 552.
344 Auch die DSRL enthält in Art. 2a eine ähnliche Definition.
345 *Gola/Schomerus*, BDSG, § 3 Rn. 2.
346 *Gola/Schomerus*, BDSG, § 3 Rn. 3.
347 Vgl. hierzu etwa *von Lewinski*, DuD 2000, 39.

formationen, etwa auf die Intim- und Privatsphäre, zu beschränken, ist der Gesetzgeber nicht gefolgt.[348] Auch hat der Gesetzgeber es zu recht abgelehnt, bestimmte elementare Angaben wie den Namen, die Anschrift, Geburtsdatum und Beruf zu sog. freien Daten zu erklären. Ein solcher Lösungsansatz ist für den Datenschutz ungeeignet, weil eine allgemeine Aussage zur Empfindlichkeit von Daten kaum möglich ist. So kann auch die Verarbeitung dieser Daten zu einer Störung der Privatsphäre des Betroffenen führen, wenn z.B. als Wohnort die Anschrift einer Strafvollzugsanstalt oder einer Nervenheilanstalt gespeichert ist.[349] Aus diesem Grund hat auch das Bundesverfassungsgericht in seinem Volkszählungsurteil festgestellt, dass es „unter den Bedingungen der modernen Datenverarbeitung kein belangloses Datum mehr gibt".[350]

Persönliche und sachliche Verhältnisse Was im einzelnen zu den Angaben über die persönlichen und sachlichen Verhältnisse einer Person gehört, ist im Gesetz nicht geregelt. Eine erschöpfende Aufzählung von Einzelangaben ist nicht möglich. Unter persönlichen Verhältnissen fallen aber zum Beispiel Angaben zu Namen, Anschrift, Geburtsdatum, Familienstand, Bankverbindung, Beruf, Gesundheitszustand.[351] Unstreitig sind auch die Darstellung von Verhaltensweisen, die Beziehungen von Personen zueinander oder auch Werturteile persönliche Verhältnisse im Sinne des § 3 BDSG.[352] Angaben über Eigentumsverhältnisse, vertragliche oder sonstige Beziehungen zu Dritten, Informationen über Kommunikations- und Nutzungsverhalten von Personen zählen dagegen zum Beispiel zu den sachlichen Verhältnissen einer Person.[353] Demnach handelt es sich also zum Beispiel bei den Aussagen eines Zeugen in einem Zivilverfahren um persönliche Verhältnisse. Um sachliche Verhältnisse würde es sich zum Beispiel bei den Vermögensverhältnissen in einem Prozesskostenhilfe-Verfahren handeln oder in der Zwangsvollstreckung oder im Insolvenzverfahren.

Einzelangaben In den Schutzbereich des BDSG fallen nur Einzelangaben. Den Gegensatz zu Einzelangaben bilden zusammengefasste Angaben, die in der Fachsprache der Statistik auch aggregierte Daten genannt werden. Von zusammengefassten Angaben kann nur dann gesprochen werden, wenn die Aussage nicht mehr einer Einzelperson zugeordnet werden kann. Dies ist in der Regel erst dann der Fall, wenn eine Gruppe, auf die sich eine Information bezieht, zumindest drei Personen umfasst, denn bei nur zwei Gruppenangehörigen besteht die

348 Vgl. hierzu BT-Drs. 7/5277, 5: „Abgelehnt hat der Ausschuss nach sorgfältiger Erörterung den aus den Kreis der Wirtschaft unterbreiteten Vorschlag, alle einer Geschäfts- oder gewerbliche Tätigkeit einer einzelnen Person betreffenden Daten aus dem Schutzbereich des Gesetzes auszunehmen. Eine solche Ausnahme scheitert nach Ansicht des Ausschusses am Fehlen eindeutiger Abgrenzungskriterien für reine geschäftliche oder private Daten."

349 BT-Drs. 7/5277, 5.

350 BVerfGE 65, 1 (45).

351 *Tinnefeld*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 490.

352 Die Existenz von Berichtigungsvorschriften steht dem nicht entgegen, sie besagt nur, dass es im Anwendungsbereich des BDSG berichtigungsfähige personenbezogene Daten geben muss, stützt aber nicht den Schluss, dass Angaben, die nicht an dem Kriterium der Richtigkeit gemessen werden können, vom Datenschutz schlechthin freigestellt werden.

353 *Tinnefeld*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 490.

Möglichkeit der Identifizierung durch Differenzbildung. Ausnahmsweise kann auch die Zusammenfassung von Angaben über mehr als drei Personen erforderlich sein, wenn die Angaben eines Gruppenangehörigen dominieren.[354] In der Justiz stellt sich die Frage der Abgrenzung von Einzelangaben und zusammengefassten Daten zum Beispiel bei der Erstellung von Statistiken über die Zahl der erledigten Verfahren in einem Referat.

Natürliche Personen § 3 Abs. 1 BDSG erfasst in seinem Schutzbereich nur Angaben, die sich auf eine natürliche Person beziehen. Angaben von Verstorbenen fallen daher nicht in den Schutzbereich des BDSG.[355] Nicht unter den Schutzbereich des BDSG fallen auch juristische Personen. Der Gesetzgeber hat bewusst darauf verzichtet, juristische Personen und Personenmehrheiten unter den Anwendungsbereich des BDSG aufzunehmen. So heißt es zum Beispiel schon in dem Gesetzentwurf der Bundesregierung von 1973: „Der Entwurf schützt nur Daten über natürliche Personen, obwohl nicht zu verkennen ist, dass auch juristische Personen oder nicht-rechtsfähige Personengruppen über einen Innenbereich verfügen, der gegenüber dem Informationsbedürfnis Dritter Schutz verdient. Weil aber dieser Bereich gesetzgeberisch kaum fassbar ist und die Praktikabilität des Entwurfs beeinträchtigen könnte, hat die Bundesregierung darauf verzichtet, diese Personengruppen als Schutzobjekt mit aufzunehmen.“[356] Zum Teil wird dies als positiv beurteilt.[357] So würden juristische Personen insbesondere aus Gründen des Konsumenten-, Anleger- und Gläubigerschutzes vielfältigen Pflichten zur Publizität und Rechnungslegung unterliegen und würden allein schon deswegen keines Schutzes bedürfen. Zudem seien Personenvereinigungen auch nicht schutzlos, da die zu einer Personenmehrheit gespeicherten Daten oft auch personenbezogene Daten der Mitglieder sein werden. Demgegenüber halten Roßnagel, Pfitzmann und Garstka in ihrem Gutachten zur Modernisierung des Datenschutzes die Einbeziehung von juristischen Personen für notwendig.[358] Dies begründen sie v.a. mit der Schwierigkeit bei der Abgrenzung der Daten von natürlichen Personen und juristischen Personen und damit, dass Art. 19 Abs. 3 GG grundsätzlich auch für juristische Personen gelte. Da also bislang zumindest juristische Personen vom Anwendungsbereich der Datenschutzgesetze ausgenommen sind, kann an dieser Stelle schon festgehalten werden, dass ein großer Teil der Daten, die in den oben beschriebenen elektronischen Handelsregister und Unternehmensregister veröffentlicht werden, nicht vom Schutzbereich der Datenschutzgesetze erfasst sind.

---

354 *Hartig/Klink/Eiermann*, LDSG, Erl. 2.2.2 zu § 3.

355 Zwar ist die Würde des Menschen nach Art. 1 Abs. 1 GG auch nach seinem Tod zu beachten; zudem gelten einzelne Datenschutzbestimmungen zeitlich über den Tod hinaus. Das Persönlichkeitsrecht erlischt jedoch mit dem Tod. Daher ist auch eine entsprechende Anwendung der Vorschriften des BDSG nicht gerechtfertigt. Vgl. hierzu *Dammann*, in: *Simitis*, BDSG, § 3 Rn. 17 und *Gola/Schomerus*, BDSG, § 3 Rn. 12. *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 3 Rn. 4 wollen hingegen auch den nasciturus und den Verstorbenen in den Schutz mit einbeziehen. Daten Verstorbener sollen für 30 Jahre Personenbezug haben.

356 BT-Drs. 7/1027, 18.

357 *Dammann*, in: *Simitis*, BDSG, § 3 Rn. 23.

358 *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 64.

Bestimmte und bestimmbare Person Die Person ist bestimmt, wenn sie mit Namen bezeichnet wird oder wenn ihre Identität auf andere Weise feststeht. Außer durch ihren Namen kann eine Person also beispielsweise durch ein Aktenzeichen oder durch eine sonstige unverwechselbare Kennzeichnung bestimmt sein.[359] Bestimmbar ist eine Person dann, wenn ihre Identität mittels Zusatzwissens festgestellt werden kann.[360] Es handelt sich dann um personenbeziehbare Daten. Zur Identitätsfeststellung geeignet sind alle Merkmale, die eine Person beschreiben wie zum Beispiel das Geburtsdatum, das Kfz-Kennzeichen oder die dynamische IP-Adresse.[361] Häufig wird eine Person auch durch Zusammenlegung mehrerer Merkmale bestimmbar, also zum Beispiel Staatsangehörigkeit, Alter und Geschlecht.[362] Da sich mit Hilfe der Angabe des Grundbuchblatts, der Größe und des Verkehrswertes des Grundstücks ermitteln lässt, wer Eigentümer des Grundstücks ist, handelt es sich zum Beispiel auch bei den Daten, die im Rahmen der Terminsbestimmung nach dem ZVG veröffentlicht werden, um personenbeziehbare Daten.

Anonyme und pseudonyme Daten Anonyme Daten sind nicht schutzwürdig und fallen deshalb auch nicht unter den Geltungsbereich des Gesetzes.[363] Eine Legaldefinition für die Anonymisierung findet sich in § 3 Abs. 6 BDSG. Danach ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.[364] Der Begriff der anonymen Daten hat daher zwei Varianten. Zum einen gelten solche Daten als anonym, bei denen eine Re-Identifizierung vollständig ausgeschlossen ist. Zum anderen sagt das Gesetz aber auch, dass der Ausschluss der vollständigen Re-Identifizierung nicht immer erforderlich ist. Ausreichend ist auch eine faktische Anonymisierung.[365] Bei dieser ist eine Re-Identifizierung zwar grundsätzlich möglich; diese wäre jedoch mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft verbunden.[366]

Nach § 3 Abs. 6a BDSG wird unter Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Einzelnen auszuschließen oder wesentlich zu erschweren, verstanden. Diese Legaldefinition wurde

[359] *Hartig/Klink/Eiermann*, LDSG, Erl. 2.3.3 zu § 3.

[360] *Gola/Schomerus*, BDSG, § 3 Rn. 10.

[361] Bezüglich der IP-Adresse streitig. So wie hier AG Berlin-Mitte, DuD 2007, 856. Anders jedoch AG München, CR 2009, 59.

[362] *Hartig/Klink/Eiermann*, LDSG, Erl. 2.3.4 zu § 3.

[363] *Schaffland/Wiltfang*, BDSG, § 3 Rn. 16.

[364] Von anonymen Daten sind Daten ohne Personenbezug zu unterscheiden. Während anonyme Daten mindestens eine Einzelangabe über eine Person enthalten (die allerdings nicht bekannt ist), enthalten Daten ohne Personenbezug keine Personenangaben. Vgl. hierzu *Yildirim*, 2004, 150.

[365] Bei den faktisch anonymisierten Daten treten schwierige Abgrenzungsfragen zu den personenbeziehbaren Daten auf. Vgl. hierzu im Einzelnen *Roßnagel/Scholz*, MMR 2000, 721.

[366] Zur Anonymisierung bei der Veröffentlichung von Gerichtsentscheidungen vgl. *Teschner*, SchlHA 2008, 191; *Mensching*, AfP 2007, 534; *Michel*, JurPC 1994, 2559; *Blümel*, DVBl 1966, 63.

erst mit der Novellierung des BDSG im Jahr 2001 eingefügt.[367] Davor wurde der Begriff des Pseudonyms im BDSG nirgendwo erwähnt. Daten werden pseudonymisiert, um den Inhalt nur einem kleinem Personenkreis zugänglich zu machen oder sie für einen gewissen Zeitraum zu „anonymisieren“. Zweck des Pseudonymisierens ist es also, den Inhalt der Daten zu einem bestimmten Zeitpunkt wieder erkennen zu können.[368] Im Unterschied zu den anonymen Daten werden daher pseudonyme Daten immer personenbezogene Daten bleiben.[369]

Allgemein zugängliche Daten Ob allgemein zugängliche Daten eines Schutzes bedürfen, war zunächst streitig. Im Gesetzentwurf der Bundesregierung von 1973 heißt es hier zum Beispiel: „Zur Diskussion stand weiterhin, ob aus allgemein zugänglichen Quellen entnommenen personenbezogenen Daten des gesetzlichen Schutzes bedürfen. Die Sachverständigen aus dem Bereich der Wissenschaft legten hierzu dar, dass auch die Verwendung von personenbezogenen Informationen, die aus allgemein zugänglichen Quellen entnommen worden seien, keinesfalls ungefährlich unter dem Blickwinkel des Schutzes der Privatsphäre zu sein bräuchten. (...) Von den Gegnern einer Einbeziehung der unmittelbar aus allgemein zugänglichen Quellen entnommenen Daten wurde vor allem auf die mit der Benachrichtigung der Betroffenen verbundenen Beschwernisse hingewiesen, durch die eine Speicherung, Verarbeitung und Auswertung von Literatur, Fachartikeln und Pressenotizen und anderen veröffentlichten Informationen unnötig erschwert werde. Dabei wurde die Frage gestellt, welchen Sinn es haben könnte, wenn zum Beispiel nach Veröffentlichungen im Bundesanzeiger über die Einleitung von Insolvenzverfahren gegen Personenhandelsgesellschaften die Betroffenen von allen diese Informationen speichernden Stellen nochmals davon unterrichtet werden müssten, dass diese Informationen zur Kenntnis genommen worden seien, obwohl die Veröffentlichung gerade der Unterrichtung der Öffentlichkeit diene.“[370] Nach weiteren kontroversen Diskussionen entschloss sich der Gesetzgeber dazu, die aus allgemein zugänglichen Quellen entnommenen Daten nicht generell aus dem Schutzbereich des BDSG auszunehmen.[371] Für die Verarbeitung von allgemein zugänglichen Daten gelten jedoch heute in vielen Bereichen erleichterte Vorgaben.[372] Insbesondere fällt auch der unbefugte Umgang mit allgemein zugänglichen Daten nicht unter einen Ordnungswidrigkeitentatbestand.

Nach § 10 Abs. 5 Satz 2 BDSG sind Daten allgemein zugänglich, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann. Um allgemein zugängliche Daten handelt es sich daher zum Beispiel bei den Daten aus dem elektronischen Handelsregister. Denn gemäß § 9 HGB kann das Handelsregister von jedermann zu Informationszwecken eingesehen werden. Anders ist dies dagegen bei den Schuldnerverzeich-

367 BT-Drs. 14/4329, 33.
368 *Schaffland/ Wiltfang*, BDSG, § 3 Rn. 13.
369 *Schaffland/ Wiltfang*, BDSG, § 3 Rn. 13.
370 BT-Drs. 7/5277, 4.
371 Anders jedoch die Vorschrift in § 2 Abs. 5 LDSG. Die Rechtsfolge – völliger Ausschluss der Schutzregelungen des LDSG – gebietet es jedoch, diese Regelung sehr zurückhaltend auszulegen. Vgl. hierzu *Hartig/ Klink/ Eiermann*, LDSG, Erl. 5.1 zu § 2.
372 Vgl. zum Beispiel: §§ 14 Abs. 2 Nr. 4, 28 Abs. 3 Nr. 1, 30 Abs. 2 Nr. 2, 33 Abs. 2 Nr. 7a BDSG.

nissen. Diese können gemäß § 915b Abs. 1 ZPO nur unter detailliert beschriebenen Voraussetzungen eingesehen werden. Auch bei den Daten im elektronischen Grundbuch handelt es sich nicht um allgemein zugängliche Daten. Das Grundbuch kann nur eingesehen werden, wenn ein berechtigtes Interesse gemäß § 12 GBO an den Informationen dargelegt wurde.

Verarbeitung in automatisierten Dateien und in Akten Im Rahmen des sachlichen Anwendungsbereiches ist zu differenzieren zwischen öffentlichen und nicht-öffentlichen Stellen:

Öffentliche Stellen Bis zur Novelle des BDSG im Jahr 1990 war der Anwendungsbereich – im öffentlichen wie im privaten Bereich – auf Dateien beschränkt.[373] Der Gesetzgeber wollte damit verhindern, dass etwa in Notizblöcken, Akten, Büchern und dergleichen gespeicherte Daten unter das Gesetz fallen.[374] Seit der Novelle von 1990 unterscheidet das Gesetz in § 1 Abs. 2 Nr. 1 und 2 bei öffentlichen Stellen jedoch nicht mehr danach, ob die Daten in einer Akte oder auf einem Medium der automatisierten Datenverarbeitung gespeichert sind oder werden sollen. Entscheidend für den sachlichen Anwendungsbereich ist allein, ob eine öffentliche Stelle personenbezogene Daten erhebt, verarbeitet oder nutzt. Dessen ungeachtet gelten heute für automatisierte Verarbeitungen jedoch besondere Bestimmungen im BDSG. So sind bei der automatisierten Datenverarbeitung spezielle technische und organisatorische Anforderungen ergänzend zu beachten. Auch gibt es besondere Formen der automatisierten Datenverarbeitung, deren Zulässigkeit von der Erfüllung besonderer Voraussetzungen abhängig ist.[375]

Nicht-öffentliche Stellen Bei nicht-öffentlichen Stellen ist nach § 1 Abs. 2 Nr. 3 BDSG erforderlich, dass der Umgang mit den Daten unter Einsatz von Datenverarbeitungsanlagen geschieht, oder dass – bei manueller Datenverarbeitung – nicht automatisierte Dateien die Datenquelle sind. Entscheidend ist die erleichterte Zugänglichkeit und Auswertbarkeit der Daten in einem Datenbestand.[376] Ausgenommen ist der Umgang mit Daten für ausschließlich persönliche oder familiäre Angelegenheiten gemäß § 1 Abs. 2 Nr. 3 letzter Hs. BDSG. Hierzu gehören zum Beispiel Datensammlungen, welche Adressen, Bilder oder Telekommunikationsnummern von Verwandten, Bekannten oder Vereinskollegen enthalten.[377] Auch Datensammlungen auf privat genutzten Festplatten oder auf privat genutzten Mobilfunkgeräten fallen hierunter.

---

[373] Vgl. § 2 Abs. 1 Satz 1 BDSG 1977: "Dieses Gesetz schützt personenbezogene Daten (...) soweit sie in Dateien gespeichert und sonst verarbeitet werden, es sei denn, dass die personenbezogenen Daten nicht für die Weitergabe an Dritte bestimmt sind."

[374] Vgl. BT-Drs. 7/1027, 17 und 19: „Hier war abzuwägen zwischen dem Interesse des Betroffenen an einem umfassenden Schutz seiner Daten und der Notwendigkeit, das Gesetz praktikabel zu gestalten. Ein Verzicht auf diese Beschränkung hätte zur Folge gehabt, dass auch Notizbücher, Akten und kleine nur zum persönlichen Gebrauch bestimmte Handkarteien unter das Gesetz gefallen wären. Dies ist jedoch bisher weder gefordert worden noch wäre es möglich, das Gesetz dann noch wirksam durchzuführen."

[375] Vgl. etwa §§ 4d, 4e, 4f, 9, 10 BDSG.

[376] Die Beschränkung im privaten Bereich kritisiert etwa *Dammann*, NJW 1991, 640.

[377] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 1 Rn. 21.

Soweit vertreten wird, dass bei Parteien und Verfahrensbeteiligten danach zu differenzieren sei, ob diese einen Rechtsstreit im privaten Bereich führen (mit der Folge der Unanwendbarkeit des BDSG) oder im geschäftlichen Bereich etwa als Unternehmen,[378] kann dem nicht gefolgt werden. Der Gesetzgeber hat die rein private Datenverarbeitung ausgenommen, um den Schutz der Privatsphäre zu verstärken.[379] Hier sollte zum Beispiel die staatliche Kontrolle durch die Aufsichtsbehörde nach § 38 BDSG nicht einsetzen.[380] Wenn eine Partei jedoch einen Rechtsstreit führt – sei es im privaten Bereich, etwa in einer Nachbarschaftsstreitigkeit, oder im geschäftlichen Bereich, zum Beispiel bei einer Honorarforderungsklage – hat sie den privaten Bereich, den der Gesetzgeber schützen wollte, verlassen. Sie muss sich deshalb auch an die Vorgaben des BDSG halten.

4.3.2 Das Landesdatenschutzgesetz

Nach Hessen[381] (1970) und Schweden (1973) war Rheinland-Pfalz weltweit das dritte Land, das den Datenschutz umfassend durch das Landesdatenschutzgesetz vom 24.1.1974[382] geregelt hat. Dies war eine der drei Pionierleistungen, die das Gesetz für die Anerkennung jenes Rechts gelegt haben, das vom Bundesverfassungsgericht neun Jahre später als Grundbedingung einer demokratischen, von der Selbstbestimmung und der Partizipation ihrer Mitglieder geprägten Gesellschaft apostrophiert und nach weiteren zwölf Jahren von der EU als konstitutives Element ihrer Grundrechtsordnung anerkannt wurde: das Recht jedes Einzelnen, selbst darüber zu befinden, wer welche seiner Daten für welche Zwecke verarbeiten darf.[383] In seinem Anwendungsbereich erfasst das LDSG – wie oben gesehen – die Gerichte von Rheinland-Pfalz, soweit diese personenbezogene Daten verarbeiten, unabhängig davon, ob diese die Daten in einer Akte in herkömmlicher Weise oder einem Medium der automatisierten Datenverarbeitung verarbeiten.[384]

Ursprünglich, d.h. in der Fassung des Landesdatenschutzgesetzes von 1974,[385] waren die Organe der Rechtspflege nicht ausdrücklich als öffentliche Stelle genannt. Mit der Novelle des LDSG von 1994[386] wurden sie in § 2 Abs. 1 aufgenommen. Damit sollte klargestellt werden, dass neben den Gerichten und den Behörden der Staatsanwaltschaft auch Notare und Schiedspersonen als öffentliche Stelle angesehen werden.

---

[378] *Schöttle*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 180.
[379] *Schaffland/ Wiltfang*, BDSG, § 1 Rn. 22.
[380] *Schaffland/ Wiltfang*, BDSG, § 1 Rn. 22.
[381] GVBl. 1970 I, 625.
[382] GVBl. 1974 I, 31.
[383] Vgl. hierzu *Simitis*, 1999.
[384] Vgl. hierzu § 3 Abs. 2 Satz 2 LDSG: „ungeachtet der dabei angewendeten Verfahren“. Diese Formulierung verdeutlicht, dass das LDSG für alle Formen des Umgangs mit personenbezogenen Daten anzuwenden ist. Vgl. hierzu *Hartig/Klink/Eiermann*, LDSG, Erl. 3.1 zu § 3.
[385] GVBl. 1974, 31.
[386] GVBl. 1994, 293.

Ob die Landesdatenschutzgesetze auf Notare anwendbar sind, war lange Zeit umstritten. Die Bundesnotarkammer hatte früher die Ansicht vertreten, dass das Landesdatenschutzgesetz für die Tätigkeit der Notare nicht gelten würde. Begründet hat sie dies damit, dass die Vorschriften der BNotO und des BeurkG den Vorschriften der Datenschutzgesetze der Länder vorgehe.[387] Dieser Ansicht hat der Bundesgerichtshof im Jahre 1990[388] jedoch eine Absage erteilt.[389] Ein Notar hatte es abgelehnt, bestimmte elektronische Verzeichnisse beim Landesbeauftragten für den Datenschutz anzumelden.[390] Nachdem der Landgerichtspräsident als Dienstherr des Notars diesen angewiesen hatte, die betreffenden Verfahren anzumelden, hob das Oberlandesgericht Köln[391] die Anweisung auf. Das Oberlandesgericht hielt die Bestimmungen zur Anmeldepflicht im Datenschutzgesetz nicht für einschlägig. Unter anderem würden Wortlaut und Entstehungsgeschichte der Datenschutzgesetze erkennen lassen, dass auch die Notare als Organe der Rechtspflege generell von den landesrechtlichen Vorschriften über den Datenschutz ausgenommen seien. Der Bundesgerichtshof hob die Entscheidung des Oberlandesgericht zu Recht auf. Die Ansicht des Oberlandesgerichts sei unzutreffend. Vom Datenschutzgesetz umfasst seien alle Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes. Dazu würden auch Notare gehören. Sie seien Träger eines öffentlichen Amtes,[392] die durch Hoheitsakt bestellt[393] worden seien und der Dienstaufsicht der Landesjustizverwaltung[394] unterliegen würden. Dabei sei es ohne Belang, dass die im Geltungsbereich des Datenschutzgesetzes Nordrhein-Westfalen bestehenden Notare nicht unmittelbar in die staatliche Organisation eingegliedert seien. Es reiche aus, dass sie auf der Grundlage einer Beleihung tätig werden würden. Nach dieser Entscheidung ist die Frage der Anwendbarkeit des Datenschutzgesetz auf die Notare geklärt.[395]

4.3.3 Die bereichsspezifischen Vorschriften

4.3.3.1 Der Grundsatz der Subsidiarität

Der Grundsatz der Subsidiarität findet sich im BDSG in § 1 Abs. 3 Satz 1 BDSG. Danach gehen, soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, dem BDSG vor. Eine fast gleichlautende Formulierung findet sich im LDSG. Zunächst haben Bundesspezialgesetze Vorrang vor dem LDSG.[396]

---

387 Mitteilung der Bundesnotarkammer, DNotZ 1989, 404.

388 Vgl. hierzu BGH NJW 1991, 568 sowie die Entscheidungsbesprechung *Rüpke*, NJW 1991, 568.

389 In diesem Fall ging es die Bestimmungen im nordrhein-westfälischen Datenschutzgesetz.

390 Vgl. § 27 Abs. 3 und § 23 Abs. 1 Satz 1 NRW DSG 1988.

391 OLG Köln, CR 1990, 144.

392 § 1 BNotO.

393 § 3 Abs. 1 BNotO.

394 §§ 92 ff. BNotO.

395 Von dieser Frage zu unterscheiden ist jedoch, ob und inwieweit Notare auch der Kontrolle des Landesbeauftragten für den Datenschutz unterliegen. Vgl. hierzu Abschnitt 6.2.3.

396 *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 1 Rn. 23.

Daneben erstreckt § 2 Abs. 7 LDSG die subsidiäre Anwendung – wie alle anderen Landesdatenschutzgesetze – auf Rechtsvorschriften des Landes.[397]

Unter Rechtsvorschriften fallen nicht nur Gesetze im formellen Sinne. Auch Rechtsverordnungen und autonome Satzungen von bundesunmittelbaren Körperschaften, Anstalten und Stiftungen zählen hierzu.[398] Nicht vorrangig sind jedoch Verwaltungsvorschriften, Erlasse und Richtlinien, also Normen ohne unmittelbare Außenwirkung. Nicht vorrangig ist auch die Rechtsprechung. Sie spielt zwar bei Gesetzeslücken oder hinsichtlich der Gesetzesauslegung eine dominierende Rolle, die Entscheidungen der Gerichte sind jedoch nicht den Rechtsvorschriften gleichzusetzen.[399] Für die subsidiäre Anwendung des BDSG und des LDSG ist es unbeachtlich, wann die vorrangige Norm entstanden ist. So können etwa Regelungen der ZPO oder der GBO das BDSG bzw. das LDSG verdrängen, obgleich diese schon lange vor den Datenschutzgesetzen in Kraft getreten sind.[400]

Vorrangwirkung kann immer nur einer einzelnen Rechtsvorschrift zukommen und nie einem ganzen Gesetz. Damit kann z.B. nicht die ZPO als Normengefüge das BDSG oder das LDSG verdrängen. Es stellt sich allein die Frage, ob etwa § 299 ZPO (Einsicht in Zivilakten) den jeweiligen Normen des BDSG und des LDSG vorgeht.[401] Der Vorrang der speziellen Norm gilt dabei nur, wenn von ihr der gleiche Sachverhalt wie von der entsprechenden Norm der Datenschutzgesetze geregelt wird. D.h. die bereichsspezifische Norm muss deckungsgleich sein. Dies geht aus der Formulierung „soweit“ in § 1 Abs. 3 Satz 1 BDSG und § 2 Abs. 7 LDSG hervor. Ob dies der Fall ist, lässt sich nicht immer leicht feststellen. Erst durch eine Interpretation des Gesetzestextes kann in der Regel erkannt werden, welche Verarbeitungsphasen betroffen sind. Regelt das Spezialgesetz nur teilweise die Datenverarbeitung, also zum Beispiel die Zulässigkeit der Datenübermittlung, nicht aber das Auskunftsrecht des Betroffenen, so sind hinsichtlich letzterem neben der speziellen Norm die Datenschutzgesetze anzuwenden.[402]

Das BDSG von 1977 enthielt noch in § 45 BDSG a.F. beispielhaft eine Einzelaufzählung von vorrangigen Normen. Mit der Novellierung des BDSG im Jahr 1990 wurde § 45 BDSG a.F. aufgehoben. Beispielhaft aufgeführt waren in § 45 BDSG a.F. unter anderem bestimmte Normen über die Beschränkung der Einsicht in Unterlagen durch Dritte, Bestimmungen über in öffentlichen Registern geführte personenbezogene Daten wie § 12 GBO und einige Vorschriften aus der ZPO, so §§ 299 und 760 über Akteneinsichtsrechte und §§ 383, 384 über Zeugnisverweigerungsrechte.[403]

---

397 Die ausdrückliche Erwähnung der Veröffentlichung in den beiden Regelungen hat keine eigenständige Bedeutung. Sie hat nur klarstellenden Charakter, da die Veröffentlichung ohnehin eine Übermittlung nach §§ 3 Abs. 5 Satz 2 Nr. 3a BDSG und § 3 Abs. 2 Nr. 4 LDSG darstellt, vgl. hierzu *Walz*, in: *Simitis*, BDSG, § 1 Rn. 22.

398 *Liebscher*, 1994, 54.

399 *Liebscher*, 1994, 54.

400 *Liebscher*, 1994, 55.

401 *Prütting*, ZZP 1993, 438.

402 *Liebscher*, 1994, 56.

403 *Liebscher*, 1994, 57.

4.3.3.2 Verfahrensordnungen

Die Verfahrensordnungen enthalten Datenschutzbestimmungen, die den allgemeinen Datenschutzgesetzen vorgehen. Diese Vorschriften verstehen sich oft auch nicht als klassische Datenschutzregelung. In ihnen kommen vielmehr die verschiedenen Verfahrensgrundsätze, die mit dem informationellem Selbstbestimmungsrecht in einem Spannungsverhältnis stehen, zum Ausdruck. Zum Beispiel ist den Parteien nach Art. 103 Abs. 1 GG rechtliches Gehör zu gewähren. Bestandteil des Anspruchs auf rechtliches Gehör ist das Akteneinsichtsrecht der Parteien (einfachgesetzlich etwa in §§ 299 Abs. 1, 760 ZPO und § 42 ZVG verankert). Dieses Recht darf nicht unter Berufung auf ein etwaiges informationelles Selbstbestimmungsrecht des Gegners versagt werden.[404] Und: Nach § 169 Satz 1 GVG haben gerichtliche Verhandlungen und Verkündungen von Entscheidungen öffentlich zu erfolgen. In diesem Grundsatz der Öffentlichkeit kommt das Prinzip einer demokratischen Rechtspflege zum Ausdruck. Hiervon darf nur in gesetzlich bestimmten Ausnahmefällen (§§ 171b Abs. 1, 172, 173 GVG), in denen der Privatsphäre des einzelnen ein höherer Schutz zukommt, abgewichen werden.[405] Oder weiter: Der Amtsermittlungsgrundsatz begründet die Verpflichtung der Gerichte, den Sachverhalt von Amts wegen zu untersuchen. Dieser Grundsatz findet sich nicht nur in der Strafprozessordnung (§ 244 Abs. 2 StPO). Er gilt vielmehr auch im Verfahren der freiwilligen Gerichtsbarkeit (§ 26 FamFG) oder im Insolvenzverfahren (§ 4 InsO). Er ist mit weitgehenden Mitwirkungspflichten beim Betroffenen verbunden, die sein Recht auf informationelle Selbstbestimmung tangieren können. Neben diesen Vorschriften, die die Prozessmaximen in den Verfahrensordnungen einfachgesetzlich verankern, hat der Gesetzgeber im Zuge der Elektronisierung von Verfahrensabläufen aber auch technische Anforderungen an die Datensicherheit in den Prozessordnungen geregelt. So enthalten manche Vorschriften etwa Vorgaben zur sicheren elektronischen Übermittlung von Schriftsätzen (§ 174 Abs. 3 Satz 3 ZPO), zur Einrichtung eines automatisierten Abrufverfahren (§ 133 GBO) oder zu Veröffentlichungen von gerichtlichen Informationen im Internet (§ 9 Abs. 2 Satz 3 InsO).[406]

4.3.3.3 Verfahrensübergreifende Mitteilungen von Amts wegen nach §§ 12 ff. EGGVG

In Straf- und Zivilsachen sowie in Verfahren der freiwilligen Gerichtsbarkeit sind während eines gerichtlichen Verfahrens zahlreiche Mitteilungen von Amts wegen an öffentliche Stellen wie Gerichte, Behörden und öffentlich-rechtliche Körperschaften zu machen. Diese Stellen benötigen die Mitteilungen der Gerichte zur Erfüllung ihrer Aufgaben. Lange Zeit waren der Inhalt, Zeitpunkt und der Empfänger der Mitteilungen in Verwaltungsanordnungen geregelt, die zwischen den Justizministern der Länder und dem Bundesminister der Justiz bundes-

404 *Wullweber*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 163.
405 *Wullweber*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 163.
406 Vgl. hierzu ausführlich Teil 3.

einheitlich vereinbart worden waren.[407] Als Rechtsgrundlage für die Mitteilungsanordnungen wurde früher der Amtshilfegrundsatz des Art. 35 GG herangezogen.[408] Diese Auffassung ließ sich jedoch seit dem Volkszählungsurteil des Bundesverfassungsgerichts nicht mehr aufrechterhalten. Aus diesem Grund hat der Gesetzgeber das Justizmitteilungsgesetz[409] geschaffen.[410] Die Datenschutzbeauftragten des Bundes und der Länder forderten eine gesetzliche Grundlage für das Mitteilungswesen der Justiz schon seit 1984.[411]

Das Gesetz enthält eine auf den ersten Blick nicht leicht zu überschauende Systematik: In den Art. 2-32 des Justizmitteilungsgesetzes hat der Gesetzgeber besondere, bereichsspezifische Anwendungsgebiete des Justizmitteilungswesens normiert, wie zum Beispiel im Beamtenrechtsrahmengesetz. Wenn diese speziellen Vorschriften nicht einschlägig sind,[412] kommen die Mitteilungsermächtigungen nach § 13 Abs. 1 Nr. 2-5 EGGVG zur Anwendung. Erst wenn auch die Voraussetzungen dieser Vorschriften nicht vorliegen, ist die Einschlägigkeit des Katalogs der Mitteilungsermächtigungen in den §§ 14-17 EGGVG zu prüfen.[413]

Die oben genannten bereichsspezifischen Vorschriften sind zum Teil als Mitteilungspflichten ausgestaltet worden, zum Teil aber auch nur als Mitteilungsbefugnisse. Wenn in ihnen – wie in §§ 14-17 EGGVG – keine Mitteilungspflichten enthalten sind, können Mitteilungspflichten – wie früher – in Verwaltungsvorschriften festgelegt werden. Derartige Verwaltungsvorschriften stellen heute die Mitteilungen in Zivilsachen (MiZi) und die Mitteilungen in Strafsachen (MiStra) dar.

Außer den Mitteilungsermächtigungen sind im EGGVG auch Regelungen zu organisatorischen und verfahrensrechtlichen Vorkehrungen enthalten (§ 18), zum Zweckbindungsgrundsatz (§ 19), zu Nachberichtigungs- und Unterrichtungspflichten (§ 20), zum Auskunfts- und Benachrichtigungsanspruch (§ 21) und zum Rechtsschutz (§ 20 EGGVG), welche in weiten Teilen den Vorschriften des BDSG und des LDSG nachgebildet sind und welche auch für das bereichsspezifischen Mitteilungswesen gelten.

Wenngleich das Justizmitteilungsgesetz erst 13 Jahre nach dem Volkszählungsurteil erlassen wurde,[414] ist es dennoch als positiv zu beurteilen, dass das Mitteilungswesen nunmehr auf eine gesetzliche Grundlage gestellt wurde. Verbesserungsbedarf besteht jedoch noch bei den Benachrichtigungspflichten. So sieht § 21 Abs. 2 EGGVG eine Benachrichtigung an die Betroffenen nur vor, wenn sie an dem Verfahren, in dem die Daten entstanden, nicht beteiligt sind. Dies ist aber unzureichend. Eine Benachrichtigung der Mitteilungen ist auch für dieje-

[407] BT-Drs. 13/4709, 16. Das waren die Mitteilungen in Zivilsachen (MiZi) und die Mitteilungen in Strafsachen (MiStrA).

[408] BT-Drs. 13/4709, 16.

[409] BGBl. 1997 I, 1430.

[410] Vertiefend hierzu *Golembiewski*, 2000. Einen Überblick über das Gesetz geben *Wullweber*, SchlHA 1999, 69; *Wollweber*, NJW 1997, 2488; *Wullweber*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 165; *Bär*, CR 1998, 767; *Schnupp*, PersV 1998, 110.

[411] *DSB-Konferenz*, 6./7.6.1984; *DSB-Konferenz*, 13.9.1985.

[412] Vgl. § 13 Abs. 1 Nr. 1 EGGVG.

[413] Die Vorschriften in §§ 14-17 EGGVG begründen jedoch keine Mitteilungspflichten.

[414] Zur Entwicklung bis 1993 vgl. *Krumsiek*, DVBl 1993, 1229.

nigen Personen erforderlich, die an dem Verfahren beteiligt waren. Die Betroffenen werden in der Regel die vielfältigen Vorschriften des Justizmitteilungswesens nicht kennen. Sie sind daher auf eine Benachrichtigung angewiesen. Erst dann können sie wirksam von ihren Rechtsschutzmöglichkeiten nach § 20 EGGVG Gebrauch machen.[415]

4.3.3.4 Gesetz zur Aufbewahrung von Schriftgut der Justiz

Inzwischen gibt es sowohl im Bund wie auch im Land Rheinland-Pfalz ein Schriftgutaufbewahrungsgesetz. Außer Rheinland-Pfalz verfügen des Weiteren auch die Länder Baden-Württemberg,[416] Bayern,[417] Berlin,[418] Brandenburg,[419] Nordrhein-Westfalen,,[420] Saarland,[421] Sachsen-Anhalt,[422] Schleswig-Holstein,[423] und Thüringen[424] über eine derartige Regelung. In den anderen Bundesländern sind die Fristen zur Aufbewahrung von Akten – wie auch zuvor im Bund und in Rheinland-Pfalz und in den anderen genannten Bundesländern – noch in Verwaltungsvorschriften geregelt. Weil diese die vom Bundesverfassungsgericht in seinem Volkszählungsurteil geforderte Außenwirkung nicht haben, hat die Rechtsprechung[425] eine gesetzliche Grundlage schon lange angemahnt. Ebenso taten dies die Datenschutzbeauftragten des Bundes und der Länder in den folgenden Entschließungen:

- „Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.“[426]

- „Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.“[427]

- „Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten

[415] So etwa auch *Wullweber*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 165; *Wollweber*, NJW 1997, 2489.
[416] GBl. 2008, 254.
[417] GVBl. 2009, 632.
[418] GVBl. 2008, 410.
[419] GVBl. 2008, 273.
[420] GV. NRW 2008, 128.
[421] Amtsblatt 2008, 1879.
[422] GVBl. 2008, 236.
[423] GVBl. 2009, 503.
[424] GVBl. 2008, 587.
[425] OLG Frankfurt, NJW 1989, 47; OLG Frankfurt, NJW 1995, 1102; OLG Frankfurt, NJW 1999, 73.
[426] *DSB-Konferenz*, 26./27.9.1994.
[427] *DSB-Konferenz*, 9./10.3.1995.

nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb (...) ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz."[428]

- „Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen."[429]

Die beiden Schriftgutaufbewahrungsgesetze des Bundes und des Landes Rheinland-Pfalz sind vor diesem Hintergrund erfreulich. Mit ihnen ist der Gesetzgeber den Forderungen der Rechtsprechung und der Datenschutzbeauftragten nachgekommen und hat die Regelungen über die Aufbewahrung von Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden nach Beendigung des Verfahrens endlich auf eine gesetzliche Grundlage gestellt. Im Detail gilt Folgendes:

Das SchrAG des Bundes Die Aufbewahrung von Schriftgut der Justiz wurde mit dem Justizkommunikationsgesetz[430] von 2005 auf eine gesetzliche Grundlage gestellt. Das Schriftgutaufbewahrungsgesetz (SchrAG) ist nach § 1 Abs. 1 nur für das Schriftgut des Bundes und das des Generalbundesanwalts anwendbar. Der Regierungsentwurf hatte den Anwendungsbereich noch auf das Schriftgut der Gerichte der Länder erstreckt.[431] Aufgrund aufkommender Zweifel über die Gesetzgebungskompetenz des Bundes zur Schaffung eines einheitlichen Aktenaufbewahrungsgesetzes für Bund und Länder wurde hiervon im weiteren Gesetzgebungsverfahren jedoch wieder abgesehen.[432] In sachlicher Hinsicht werden von dem Gesetz nur Akten oder Aktenbestandteile erfasst, denen ein justizförmiges Verfahren zugrunde lag. Das bedeutet, dass z.B. Akten der Justizverwaltung, etwa Personalakten und Beschaffungsakten, nicht hierunter fallen.[433] Das SchrAG ist nicht auf Papierakten beschränkt. Vielmehr folgt aus § 1 Abs. 2 Satz 2 SchrAG, dass auch elektronisch geführte Akten und Dateien vom Anwendungsbereich des Gesetzes erfasst werden.

[428] *DSB-Konferenz*, 5./6.10.1998.
[429] *DSB-Konferenz*, 7./8.10.1999.
[430] BGBl. 2005 I, 852.
[431] BT-Drs. 15/4067.
[432] Vgl. BT-Drs. 15/4952, 50: „Mit Rücksicht auf die zwischenzeitliche Entwicklung der Rechtsprechung des Bundesverfassungsgerichts, Urteil vom 26.1.2005, 2 BvF 1/03 – Studiengebühren – nach der sich die Gesetzgebungskompetenz des Bundes für ein einheitliches Aktenaufbewahrungsgesetz des Bundes und der Länder im Hinblick auf Art. 72 Abs. 2 GG nicht mehr zweifelsfrei bejahen lässt, ist der Anwendungsbereich des Gesetzes auf das Schriftgut der Gerichte des Bundes und des Generalbundesanwalts beschränkt worden."
[433] Vgl. BT-Drs. 15/4067, 55.

Das SchrAG regelt in § 1 Abs. 1 die grundsätzliche Befugnis der Gerichte, die Akten auch noch nach Beendigung des Verfahrens aufzubewahren.[434] Konkrete Aufbewahrungsfristen sind im Gesetz selbst jedoch nicht genannt. § 2 SchrAG enthält insoweit eine Ermächtigung, diese in einer Rechtsverordnung näher zu bestimmen. Bei den Aufbewahrungsfristen handelt es sich um Höchstfristen, d.h. das Gericht muss die Akten nach Fristablauf zwingend vernichten oder an ein Archiv abgeben. Dies ergibt sich aus § 1 Abs. 1 SchrAG, wo es heißt: „Schriftgut (...) darf (...) nur solange aufbewahrt werden (...).“ Der Fristbeginn selbst ist in § 2 Abs. 3 SchrAG geregelt, welcher bestimmt, dass die Aufbewahrungsfristen mit Ablauf des Jahres, in dem nach Beendigung des Verfahrens die Weglegung der Akten angeordnet wurde, beginnen.

In § 2 Abs. 2 SchrAG hat der Gesetzgeber exemplarisch Kriterien genannt, die bei der Bemessung der Fristen zu beachten sind. Demnach ist zum einen das Interesse einer Person zu berücksichtigen, dass ihre in den Prozessakten befindlichen personenbezogenen Daten nicht länger als erforderlich gespeichert werden.[435] Des Weiteren bestimmen § 2 Abs. 2 Nr. 2 und 3 SchrAG, dass auch das Interesse eines ehemaligen Verfahrensbeteiligten und eines Dritten beachtet werden muss, auch nach Beendigung des Verfahrens noch auf Akten zurückgreifen zu können. Ein solches Interesse kann etwa bei einem Verfahrensbeteiligten bestehen, wenn ein Urteil berichtigt oder ergänzt werden muss[436] oder wenn im Falle einer Rechtsnachfolge ein Titel umgeschrieben werden muss.[437] § 2 Abs. 2 Nr. 4 SchrAG berücksichtigt darüber hinaus, dass das Verfahren auch z.B. im Fall der Unwirksamkeit eines Vergleiches fortgesetzt werden kann. Nr. 4 stellt insofern auch klar, dass öffentliche Interessen eine Aufbewahrung rechtfertigen können.[438]

Das LSchrAG Rheinland-Pfalz Auf Landesebene ist die Aufbewahrung von Schriftgut im LSchrAG vom 29.4.2008 gesetzlich geregelt.[439] Das Gesetz ist am 1.8.2008 in Kraft getreten.[440] Bei der Schaffung des LSchrAG hat sich der Landesgesetzgeber eng am Bundesgesetz orientiert. Auch das LSchrAG enthält dementsprechend in § 2 eine Ermächtigung, die konkreten Aufbewahrungsfristen in einer Rechtsverordnung zu regeln. Die in § 2 Abs. 2 Nr. 1 bis 4 LSchrAG enthaltenen Kriterien für die Bemessung der Fristen stimmen dabei wörtlich mit der bundesgesetzlichen Regelung überein.[441] Insoweit kann auf die Ausführungen von oben verwiesen werden. Auch bei diesen Fristen handelt es sich um Höchstfristen. Dies ergibt sich zum einen

[434] Vgl. BT-Drs. 15/4067, 55 und Wortlaut des § 1 Abs. 1 SchrAG „darf“.

[435] Vgl. § 2 Abs. 2 Nr. 1 SchrAG. Nach der Gesetzesbegründung sind Betroffene nicht nur Verfahrensbeteiligte im engeren Sinne, sondern nach § 3 Abs. 1 BDSG alle natürlichen Personen, deren personenbezogene Informationen in den Akten enthalten sind.

[436] Vgl. §§ 319, 321 ZPO.

[437] Vgl. § 727 ZPO.

[438] Die Gesetzesbegründung nennt den Fall, dass die Akten auch zu verfahrensübergreifenden Zwecken anderen öffentlichen Stellen zur Verfügung gestellt werden müssen, etwa zum Zweck der Rechtsfortbildung oder der Rechtsvereinheitlichung, vgl. BT-Drs. 15/4067, 56.

[439] GVBl. 2008, 77.

[440] Mit Ausnahme der Verordnungsermächtigung in § 2 LSchrAG, welche bereits zum 30.4.2008 in Kraft getreten ist.

[441] Vgl. § 2 Abs. 2 Nr. 1 bis 4 SchrAG.

aus dem Wortlaut des § 1 Abs. 1 LSchrAG, welcher mit dem Bundesgesetz übereinstimmt. Zum anderen lässt sich dies aber auch an zwei Stellen der Gesetzesbegründung entnehmen. So heißt es einmal auf Seite 5 der amtlichen Begründung „Diese dem § 1 Abs. 1 SchrAG entsprechende Formulierung impliziert zugleich das Verbot, Akten länger als notwendig aufzubewahren“,[442] und weiter auf Seite 6: „In der Rechtsverordnung werden für alle Aktentypen Fristen benannt werden, nach deren Ablauf das Schriftgut zu vernichten ist. Bei diesen Fristen handelt es sich nicht um Mindest-, sondern um Höchstfristen“.[443] Der sachliche Anwendungsbereich des Gesetzes stimmt ebenfalls mit dem Bundesgesetz überein. Insbesondere wird das Schriftgut der Justiz auch nach dem LSchrAG „unabhängig von seiner Speicherungsform“ erfasst. Damit wollte der Landesgesetzgeber sicherstellen, dass neben den derzeitigen Archivierungsmethoden Papierlagerung, Mikroverfilmung und elektronische Archivierung auch zukünftige Innovationen abgedeckt werden.[444] Lediglich der persönliche Anwendungsbereich ist weiter gefasst. Denn das LSchrAG ist nicht nur auf das Schriftgut der Gerichte und der Staatsanwaltschaften beschränkt. Erfasst wird vielmehr auch das Schriftgut von Justizvollzugsanstalten und das der Justizverwaltung.[445] Mit der Einbeziehung des Schriftgutes der Justizverwaltung wollte der Gesetzgeber schwierige Abgrenzungsfragen von reinen Justizverwaltungssachen und Verwaltungssachen, die trotz des verwaltenden Charakters der Rechtspflege im weitesten Sinne zuzuordnen sind, verhindern.[446]

4.3.4 Signaturgesetz

In der elektronischen Justiz kommt vor allem dem Signaturgesetz eine große Bedeutung zu.[447] Das Signaturgesetz regelt nicht die Anwendung von elektronischen Signaturen. Das Gesetz beschränkt sich vielmehr darauf, deren Sicherheit und die damit zusammenhängenden Fragen zu klären. Am 1.8.1997 trat in der Bundesrepublik Deutschland als erstem Staat der Welt ein Signaturgesetz (SigG) in Kraft.[448] Nur in Utah/USA war zuvor eine vergleichbare Regelung erlassen worden, die sich aber nur auf diesen Bundesstaat erstreckte. Die Bundesregierung regelte bereits damals sehr detailliert die technischen Anforderungen in einer zum SigG gehörenden Signaturverordnung. Das SigG war Bestandteil des Informations- und Kommunikationsdienste-Gesetzes (IuKDG), welches erstmals die rechtlichen Rahmenbedingungen des elektronischen Handels – zum Beispiel über das Internet – festlegte. Ursprünglich war geplant, im IuKDG auch die Regelungen des Bürgerlichen Gesetzbuches bezüglich Formvorschriften für die Erfordernisse des elektronischen Rechtsverkehrs anzupassen. Dies wurde

442 LT-Drs. 15/1909, 5.
443 LT-Drs. 15/1909, 6.
444 Vgl. LT-Drs. 15/1909, 5.
445 Vgl. § 1 Abs. 1 Satz 1 und 2 LSchrAG.
446 LT-Drs. 15/1909, 5.
447 Zu weiteren Einsatzmöglichkeiten der qualifizierten elektronischen Signatur vgl. etwa *Klink/Straub*, D-A-CH, 130.
448 BGBl. 1997 I, 1870. Die nachstehenden Ausführungen zur Entwicklung des Signaturgesetzes beruhen auf *Baier/Klink/Straub*, 2003, 13. Zum Signaturgesetz von 1997 vgl. im Einzelnen *Roßnagel*, RDV 1998, 5; *Roßnagel*, DuD 1997, 287; *Roßnagel*, NJW 1999, 1591; *Roßnagel*, DuD 1997, 75.

jedoch vom Gesetzgeber für eine rein technische Erprobungsphase zurückgestellt, so dass die digitale Signatur zunächst keine Rechtswirkungen entfaltete.

Das SigG in seiner heute gültigen Form ist eine grundlegende Neufassung, die am 22.5.2001 als Umsetzung der EU-Signaturrichtlinie in Kraft trat.[449] Eine Vereinheitlichung auf europäischer Ebene war nötig geworden, da die Mitgliedsstaaten unterschiedliche Signaturgesetze erlassen hatten. Nicht alle Staaten wollten wie die Bundesrepublik ein behördlich geprüftes Sicherheitsniveau zwingend vorschreiben. Als Kompromiss wurde dieses hohe Sicherheitsniveau als freiwillige Option neben niedrigeren Stufen formuliert. Mit Ausnahme des 1. Signaturänderungsgesetzes von 2005[450] hat das Signaturgesetz seit 2001 keine großen Änderungen erfahren.

4.3.4.1 Die verschiedenen Stufen

Bekanntlich definiert das Signaturgesetz in § 2 und § 15 vier aufeinander aufbauende Stufen von elektronischen Signaturen. Sog. einfache elektronische Signaturen sind nach § 2 Nr. 1 SigG Daten in elektronischer Form, die anderen Daten beigefügt sind und zur Authentifizierung dienen. Dies ist die schwächste Form. Mit ihr ist keinerlei Sicherheitswert verbunden. Sie kann beliebig oft kopiert werden und unter beliebig viele andere elektronische Dokumente gesetzt werden.[451] Zu denken ist hier etwa an die Fallgestaltung, dass ein Rechtsanwalt eine Klageschrift in einem Textverarbeitungsprogramm schreibt und die eingescannte handschriftliche Unterschrift als Grafik in den Text einfügt und die Datei als Anhang zu einer E-Mail an das Gericht versendet.[452]

Sog. fortgeschrittene elektronische Signaturen sind nach § 2 Nr. 2 SigG einfache elektronische Signaturen, die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, seine Identifizierung ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Die fortgeschrittene elektronische Signatur unterliegt höheren Anforderungen als die einfache. Gleichwohl erfüllt sie nicht die Anforderungen an digitale Signaturen nach dem Signaturgesetz. Sie kann daher als „Zwischenstufe“ im Verhältnis zu den einfachen elektronischen Signaturen und den qualifizierten elektronischen Signaturen bezeichnet werden.[453] Eine derartige Signatur liegt z.B. vor, wenn der Rechtsanwalt seine Klageschrift im Textverarbeitungsprogramm erstellt und als Datei speichert. Diese wird nun von einem weiteren Programm mit Hilfe des privaten Signaturschlüssels – dem Private Key des Anwalts – signiert. Dadurch werden die signierten Daten so miteinander verknüpft, dass spätere unbemerkte Änderungen am Text nicht möglich sind.[454]

[449] BGBl. 2001, 876. Vgl. hierzu im Einzelnen *Roßnagel*, BB 2002, 261; *Roßnagel*, NJW 2001, 1817; *Roßnagel*, MMR 2001, 201; *Roßnagel*, MMR 2000, 451.
[450] BGBl. 2005 I, 2. Vgl. hierzu *Roßnagel*, NJW 2005, 385.
[451] BT-Drs. 14/4662, 18.
[452] *Baier/Klink/Straub*, 2003, 14.
[453] BT-Drs. 14/4662, 18.
[454] *Baier/Klink/Straub*, 2003, 14.

Qualifizierte elektronische Signaturen sind nach § 2 Nr. 3 SigG fortgeschrittene Signaturen, die zusätzlich auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden. In diesem Fall ist der Ablauf derselbe wie bei der fortgeschrittenen Signatur. Zum Erstellen der Signatur wird aber eine spezielle Soft- und Hardware, etwa ein Lesegerät mit Chipkarte eingesetzt. Der Rechtsanwalt aktiviert diese durch Eingabe seiner geheimen PIN. Die Verwendung der Karte bietet einen erhöhten Schutz, da sie zum Signieren zwingend benötigt wird. Darüber hinaus ist der hinterlegte Signaturschlüssel besonders geschützt und kann auch nicht ausgelesen werden, wenn die Karte in falsche Hände gerät. Um diese Signaturen zu erstellen, muss sich der Sender allerdings bei einem Zertifizierungsdiensteanbieter registrieren lassen, um eine persönliche Karte und ein so genanntes qualifiziertes Zertifikat zu erhalten.[455]

Qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung nach § 15 SigG beruhen auf qualifizierten Zertifikaten, die von einem Zertifizierungsdiensteanbieter ausgestellt wurden, der sich einer freiwilligen Akkreditierung unterworfen hat. In diesem Fall bezieht der Rechtsanwalt sein Zertifikat von einem Zertifizierungsdiensteanbieter, dessen Sicherheit den Anforderungen des § 15 SigG genügt.[456]

Das SigG enthält bis auf § 14 Abs. 3 SigG nur materielle Anforderungen an qualifizierte elektronische Signaturen. Mit der Aufzählung der verschiedenen Stufen wollte der Gesetzgeber lediglich zum Ausdruck bringen, dass auch die Anwendung von anderen Stufen möglich und nicht ausgeschlossen ist.[457] Die beiden ersten Stufen werden auch als die „sonstigen“ oder „nicht signaturgesetzkonformen Verfahren“ bezeichnet.[458]

Im Vergleich zum qualifizierten elektronischen Signaturverfahren und dem akkreditierten Signaturverfahren unterliegen die sonstigen Signaturverfahren hinsichtlich ihrer organisatorischen Sicherheit keiner Kontrolle. Auch werden an die einzusetzenden technischen Komponenten keine speziellen Anforderungen gestellt. Im Unterschied zum qualifizierten Signaturverfahren und dem akkreditierten Signaturverfahren erfüllen sie zudem nicht die Anforderungen an die gesetzliche Schriftform nach §§ 126, 126a BGB und dem Signatur-Schlüsselinhaber einer sonstigen Signatur kommt zudem auch keine Beweiserleichterung im Sinne des § 371a ZPO zu. Da ausgestellte und gesperrte Zertifikate nicht in einem Verzeichnisdienst zur Nachprüfung zur Verfügung gehalten werden müssen, ist eine langfristige Prüfbarkeit in einem sonstigen Signaturverfahren nicht gewährleistet. Für sonstige Signaturverfahren gibt es letztlich keine rechtlichen Anforderungen zur Dokumentation der Vergabe und Sperrung von Zertifikaten. Ob in einem Rechtsstreit also auf eine solche Dokumentation zurückgegriffen werden kann, ist völlig unsicher.[459]

---

455 *Baier/Klink/Straub*, 2003, 15.
456 *Baier/Klink/Straub*, 2003, 15.
457 BT-Drs. 14/4662, 17.
458 *Roßnagel*, in: *ders.* (Hrsg.), Handbuch Datenschutzrecht, 1218.
459 Zu den Unterschieden vgl. im Einzelnen *Roßnagel*, MMR 2002, 215.

4.3.4.2 Der Zertifizierungsdiensteanbieter

Nach § 4 Abs. 1 SigG ist der Betrieb eines Zertifizierungsdiensteanbieters genehmigungsfrei.[460] Er muss gemäß § 4 Abs. 3 SigG lediglich angezeigt werden. Mit der Anzeige hat der Zertifizierungsdiensteanbieter darzulegen, dass er die in § 4 Abs. 2 SigG genannten Anforderungen erfüllt. So muss er die für den Betrieb erforderliche Zuverlässigkeit[461] und Fachkunde[462] besitzen, eine Deckungsvorsorge[463] nachweisen und ein Sicherheitskonzept[464] mit einer Erläuterung seiner praktischen Umsetzung vorlegen. Die Anzeige ist erforderlich, damit die Behörde ggf. von ihren Überwachungs- und Aufsichtsrechten nach §§ 19, 20 SigG Gebrauch machen kann.

Der Zertifizierungsdiensteanbieter kann Aufgaben auch an Dritte übertragen. Dies folgt aus § 4 Abs. 5 SigG. Dritte Personen können etwa ein Unternehmen, eine Behörde, Berufskammern oder privatwirtschaftliche oder kommunale Träger sein.[465] Der Gesetzgeber wollte mit dieser Regelung den Zertifizierungsdiensteanbietern bei der Ausgestaltung ihrer innerbetrieblichen Organisation einen großen Gestaltungsspielraum einräumen.[466] Selbstverständlich ändert die Übertragung auf Dritte aber nichts daran, dass er, der Zertifizierungsdiensteanbieter, und nicht der Dritte für etwaige Schäden haftet, wie sich aus § 11 Abs. 4 SigG ergibt.

Wenn der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt, muss er dies der zuständigen Stelle nach § 13 Abs. 1 Satz 1 SigG unverzüglich anzeigen. In diesem Fall muss er gemäß § 13 Abs. 1 Satz 2 und 3 SigG dafür Sorge tragen, dass ein anderer Zertifizierungsdiensteanbieter das qualifizierte Zertifikat übernimmt, anderenfalls muss er es sperren lassen. Was die Dokumentation betrifft, zu welcher er nach § 10 SigG verpflichtet ist, hat er diese dem nachfolgenden Anbieter zu übergeben. Wenn dieser sie nicht übernimmt, hat er sie gemäß § 13 Abs. 2 SigG der zuständigen Stelle zu übergeben.

Einem Zertifizierungsdiensteanbieter steht es frei, sich akkreditieren zu lassen. Für eine Akkreditierung muss er nach § 15 Abs. 1 Satz 2 SigG nachweisen, dass er die nach dem SigG und der Rechtsverordnung vorausgesetzten Sicherheitsanforderungen erfüllt. Mit der Akkreditierung erhält der Zertifizierungsdiensteanbieter entsprechend § 15 Abs. 1 Satz 3 SigG ein Gütezeichen. Dieses wird ihm von der zuständigen Stelle nach einer umfassenden Prüfung der genannten Anforderungen ausgehändigt. § 15 Abs. 2 Satz 2 SigG sieht vor, dass die zuständige Stelle die Einhaltung der Anforderungen in regelmäßigen Zeitabständen und nach einer sicherheitserheblichen Veränderung wiederholen muss. § 15 Abs. 4 und 5 SigG bestimmt, unter

---

460 Dies war jedoch nicht immer so. Das Signaturgesetz von 1997 enthielt noch ein Genehmigungsvorbehalt für Zertifizierungsdiensteanbieter. Die Änderung wurde aufgrund Art. 3 Abs. 1 EGSRL erforderlich.

461 Die Begründung zum Gesetzentwurf nennt als Beispiel den Auszug aus dem Bundeszentralregister, vgl. BT-Drs. 14/4662, 20.

462 Hier ist an die Vorlage von Zeugnissen gedacht, vgl. BT-Drs. 14/4662, 20.

463 Gemeint sind Versicherungspolicen und Bankbürgschaften, vgl. BT-Drs. 14/4662, 20.

464 Aus diesem muss hervorgehen, dass die eingesetzten Produkte und die Ablauforganisation den Anforderungen des Signaturgesetzes und der Rechtsverordnung nach § 24 SigG entsprechen, vgl. BT-Drs. 14/4662, 20.

465 BT-Drs. 14/4662, 20.

466 BT-Drs. 14/4662, 20.

welchen Voraussetzungen die Akkreditierung zurückzunehmen, zu widerrufen oder zu versagen ist.[467]

4.3.4.3 Die Registrierung der Nutzer und die Vergabe von Zertifikaten

Nach § 5 Abs. 1 Satz 1 SigG hat der Zertifizierungsdiensteanbieter die antragstellenden Personen zuverlässig zu identifizieren. Auf welche Weise dies zu erfolgen hat, ergibt sich aus § 3 Abs. 1 Satz 1 Signaturverordnung (SigV). Demnach hat der Zertifizierungsanbieter die Identifizierung anhand des Personalausweises, des Reisepasses oder anhand von Dokumenten, die die gleiche Sicherheit gewährleisten, vorzunehmen. Mit dem Personalausweisgesetz[468] wurde zudem § 3 Abs. 1 Satz 2 SigV eingefügt, welcher in Zukunft auch eine Identifizierung durch die Funktion des elektronischen Personalausweises ermöglicht. Optional gestattet das Gesetz seit der sog. kleinen Novelle von 2005 darüber hinaus dem Zertifizierungsanbieter, die Identifizierung anhand von Altdaten vorzunehmen. Hierzu ist allerdings gemäß § 5 Abs. 1 Satz 2 SigG die Einwilligung des Nutzers erforderlich. Flankierend dazu hat der Zertifizierungsdiensteanbieter nach § 6 SigG i.V.m. § 6 SigV bestimmte Belehrungspflichten zu erfüllen.

Nach der Identifizierung ordnet der Zertifizierungsdiensteanbieter der antragstellenden Person einen Signaturprüfschlüssel zu. Hierüber erteilt er ein qualifiziertes Zertifikat. § 7 Abs. 1 SigG regelt sodann im Einzelnen, welchen Inhalt das Zertifikat haben muss. Optional kann das Zertifikat – wie sich aus § 5 Abs. 2 SigG ergibt – auch Attribute enthalten. Eine Legaldefinition für den Begriff der Attribute enthält § 5 Abs. 2 Satz 1 SigG: Gemeint sind Angaben über eine Vertretungsmacht des Antragstellers, berufsbezogene Angaben und sonstige Angaben. Die letzten beiden Punkte hatte der Gesetzgeber auf Bitte der Berufskammern in das Gesetz aufgenommen. Damit kann das Zertifikat auch sog. potentiell relevante Angaben wie die Zugehörigkeit zu einer bestimmten Person, deren Aufgabenbereich, die Berufsbezeichnung und berufsrechtliche Zulassungen enthalten.[469] Dabei ist es wichtig zu wissen, dass Vertretungsrechte gemäß § 5 Abs. 2 Satz 2 SigG nur aufgenommen werden dürfen, wenn die Einwilligung des Dritten nachgewiesen wurde. Im gleichen Sinne erfordert § 5 Abs. 2 Satz 2 SigG auch, dass berufsbezogene oder sonstige Angaben zur Person durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle zu bestätigen ist.[470] § 5 Abs. 3 SigG bestimmt zudem, dass optional im Zertifikat ein Pseudonym aufgenommen werden kann. Will der Nutzer dieses jedoch mit einem Attribut versehen, so sieht § 5 Abs. 3 Satz 2 SigG vor, dass hierzu eine Einwilligung der oben genannten Personen vorliegen muss. D.h. diese müssen auch gerade mit der Verwendung eines Pseudonyms einverstanden sein. Auch die Aufnahme dieses Erfordernisses

[467] Zwischen qualifizierten und akkreditierten Signaturverfahren gibt es im Hinblick auf die administrative und technische Sicherheit sowie im Hinblick auf die langfristige Prüfbarkeit und Dokumentationspflicht Unterschiede, die hier nicht vertieft behandelt werden können. Diesbezüglich wird auf *Roßnagel*, MMR 2002, 215 verwiesen.

[468] Vgl. hierzu Abschnitt 4.3.5.

[469] BT-Drs. 14/4662, 21.

[470] Zuständige Stellen sind zum Beispiel Berufskammern. Diese müssen im Rahmen ihrer pflichtgemäßen Aufgabenerfüllung die Angaben bestätigen. Dagegen muss der Arbeitgeber dies nicht unbedingt tun.

beruhte auf einer Forderung der Kammern. Diese hatten nämlich befürchtet, dass durch die Verwendung eines Pseudonyms das Vertrauen in die berufsrechtliche Zulassung erschüttert werden würde.[471] Dies ist durch den Zustimmungsvorbehalt nunmehr ausgeschlossen.

Nach § 8 SigG kann der Zertifizierungsdiensteanbieter das Zertifikat unter bestimmten Voraussetzungen sperren. Als Gründe werden genannt: Das Verlangen des Signaturschlüssel-Inhabers oder seines Vertreters, das Zertifikat wurde aufgrund falscher Angaben ausgestellt,[472] der Zertifizierungsdiensteanbieter stellt seine Tätigkeit ein und diese wird nicht von einem anderen fortgeführt oder die zuständige Behörde hat die Sperrung angeordnet.

4.3.4.4 Bewertung

Das Signaturgesetz ist die Grundlage für einen sicheren elektronischen Rechtsverkehr. Nur mit Hilfe von qualifizierten elektronischen Signaturen können Integrität und Authentizität elektronischer Daten nachgewiesen werden. Als positiv sind insbesondere die Änderungen in § 3 Abs. 1 Satz 2 SigV hervorzuheben. Diese ermöglichen – über den etwas umständlichen Rückgriff auf Altdaten hinaus – die medienbruchfreie elektronische Beantragung eines qualifizierten Signaturzertifikats. Für den Bereich der elektronischen Justiz ist die elektronische Signatur überaus wichtig. In den hier zu untersuchenden Verfahrensordnungen spielt die elektronische Signatur eine große Rolle. Überall dort, wo der Gesetzgeber das Verfahren modernisiert hat, hat er auch die elektronische Signatur in seine Betrachtungen mit aufgenommen.

Die qualifizierte elektronische Signatur hat der Gesetzgeber in der ZPO an sechs Stellen erwähnt: § 130a Abs. 1 Satz 2 ZPO (Übermittlung von Dokumenten an das Gericht), § 130b ZPO (Ersatz für Schriftform im Binnenbereich), § 174 Abs. 4 ZPO (Übermittlung des Empfangsbekenntnisses an das Gericht mittels qualifizierter Signatur), § 299 Abs. 3 Satz 4 ZPO (Übermittlung von Dokumenten im Rahmen der Akteneinsichtsgewährung), § 317 Abs. 5 ZPO (Papierurteil kann als elektronisches Dokument zugestellt werden und muss qualifizierte elektronische Signatur enthalten), § 371a ZPO (Beweiskraft von elektronischen Dokumenten). An zwei Stellen hat er sich dagegen mit der sog. einfachen elektronischen Signatur zufrieden gegeben: nämlich bei § 174 Abs. 3 ZPO (Zustellung durch Gericht mittels elektronischer Signatur) und bei § 692 Abs. 2 ZPO (Mahnbescheid kann mit einfacher elektronischer Signatur versehen werden). Aufgrund des Gesetzes zur Reform der Sachaufklärung ist die qualifizierte elektronische Signatur in Zukunft zudem in § 802d Abs. 2 ZPO neu vorgesehen (Elektronische Übermittlung des Vermögensverzeichnisses an den Gläubiger mittels qualifizierter elektronischer Signatur).

---

[471] BT-Drs. 14/4662, 21.

[472] Im Signaturgesetz von 1997 befand sich noch das Wort „erwirkt“. Dieses wurde jedoch durch das Wort „ausgestellt“ ersetzt, da das erstere impliziert, dass absichtlich ein Zertifikat mit falschen Angaben herbeigeführt wurde; eine Sperrung sollte jedoch auch möglich sein, wenn in ein Zertifikat irrtümlich falsche Angaben aufgenommen wurden, vgl. hierzu BT-Drs. 14/4662, 23. Der Umstand, dass das Zertifikat mit falschen Angaben ausgestellt wurde, kann der Zertifizierungsdiensteanbieter nach § 8 Abs. 1 Satz 3 SigG, z.B. in Zertifikatsverzeichnisauskünften, seit 2001 kenntlich machen.

Im HGB ist die qualifizierte elektronische Signatur in § 9 Abs. 3 HGB erwähnt (Beglaubigung der Übereinstimmung von Daten aus dem Handelsregister und dem zugesandten elektronischen Dokument mittels qualifizierter elektronischer Signatur). Breite Anwendung wird die Signatur in Zukunft im neuen Grundbuchrecht finden. Der Gesetzgeber hat sie an drei Stellen vorgesehen. Einmal bei § 137 Abs. 3 GBO (qualifizierte elektronische Signatur als Ersatz für Schriftform für Erklärungen einer Behörde). Zum anderen in § 137 Abs. 1 Satz 2 GBO (Ersatz für elektronisches Zeugnis nach § 39a Beurkundungsgesetz bei einem Eintragungsantrag im Falle einer qualifizierten elektronischen Signatur mit Attributszertifikat) und in § 137 Abs. 2 GBO (Eintragungen aufgrund einer Erklärung oder des Ersuchens einer Behörde nur mittels qualifizierter elektronischer Signatur und Attributszertifikat), wobei hier jeweils ein Attributszertifikat erforderlich ist. Mit der einfachen elektronischen Signatur hat der Gesetzgeber sich wiederum an zwei Stellen zufrieden gegeben: in § 136 Abs. 1 Satz 4 GBO (Bestätigung des Eintragungsantrags mittels einfacher elektronischer Signatur) und in § 140 Abs. 2 GBO (Zustellungen von Entscheidungen, Verfügungen und Mitteilungen mittels einfacher elektronischer Signatur).

4.3.5 Personalausweisgesetz

Bedeutung für die vorliegende Untersuchung hat auch der neue elektronische Personalausweis. Er löst den herkömmlichen Personalausweis ab und dient als elektronischer Ausweis der Identifizierung im Internet. Die gesetzlichen Grundlagen für die Einführung des neuen Personalausweises wurden mit dem vom Bundestag am 18.12.2008 beschlossenen Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG) geschaffen.[473] Der Bundesrat stimmte am 13.2.2009 zu und das Gesetz wurde am 24.6.2009 verkündet.[474] Hinsichtlich seiner wesentlichen Regelungsinhalte tritt das Gesetz ab dem 1.11.2010 in Kraft.[475] Damit ist Einführungstermin für den neuen Personalausweis der 1.11.2010.[476] Der neue Personalausweis besitzt in Zukunft drei Funktionen, die nachfolgend beschrieben werden.[477]

[473] Durch die am 1.9.2006 in Kraft getretene Föderalismusreform (BGBl. 2006 I, 2034) ist die Gesetzgebungskompetenz für das Ausweiswesen gemäß Artikel 73 Abs. 1 Nr. 3 GG vollständig auf den Bund übergegangen.

[474] BGBl. 2009 I, 1346.

[475] Vgl. Artikel 7. Lediglich § 21 PAuswG, welcher die Vergabe der Berechtigungen regelt, tritt sechs Monate früher, nämlich ab dem 1.5.2010 in Kraft. Der Gesetzgeber wollte die Berechtigungen im Zusammenhang mit dem elektronischen Identitätsnachweis früher vergeben, damit im Zeitpunkt der Einführung des neuen Personalausweises die Anwendungen für die Bürger bereits offen stehen, BT-Drs. 16/10489, 49.

[476] Die bisherigen Ausweise bleiben jedoch bis zu ihrem Ablauf gültig.

[477] Vgl. hierzu näher *Reisen*, DuD 2008, 1.

4.3.5.1 Die drei Funktionen des elektronischen Personalausweises

Einmal enthält er – wie bislang schon – die hoheitliche Ausweisfunktion. Diese Funktion wird um biometrische Daten des Gesichts[478] und optional um Daten zweier Finger erweitert.[479] Nach § 9 Abs. 3 Satz 4 PAuswG hat der Ausweisinhaber schriftlich zu erklären, ob seine Fingerabdrücke im Verarbeitungsmedium gespeichert werden sollen. § 9 Abs. 3 Satz 5 PAuswG enthält zudem ein Verbot, den Ausweisinhaber, der sich gegen die Aufnahme von Fingerabdrücken entschieden hat, zu benachteiligen, flankiert mit einer hierauf bezogenen Informationspflicht.[480]

Nach § 22 PAuswG ist der Personalausweis als eine Signaturerstellungseinheit im Sinne des § 2 Nr. 10 SigG auszugestalten.[481] Hierzu soll jeder Ausweis zur optionalen Nutzung mit einem Chip ausgestaltet sein, der einen Signatur- und Prüfschlüssel erzeugen kann. Wenn sich der Ausweisinhaber nun dafür entscheidet, von der Signaturfunktion Gebrauch zu machen, kann er bei einem Zertifizierungsdiensteanbieter seiner Wahl einen Antrag stellen, auf dem Prüfschlüssel ein qualifiziertes Zertifikat auszustellen.[482] Die übrigen Regelungen des SigG bleiben unberührt, d.h. insbesondere, dass die Rechte und Pflichten der Zertifizierungsdiensteanbieter unverändert fortbestehen, dass das zwischen Signaturinhaber und Zertifizierungsdiensteanbieter bestehende Rechtsverhältnis nicht umgestaltet wird und dass die Vorgaben zu Datenschutz, Datensicherheit und Dokumentation unangetastet bleiben.[483]

Zum anderen besitzt der neue Ausweis die Möglichkeit, die Identität einer bestimmten Person in Online-Anmeldungen zu überprüfen. Die maßgeblichen Vorschriften sind diesbezüglich in den §§ 10-13 und 17-19 PAuswG zu finden. Für die elektronische Justiz ist insbesondere diese Anwendung von Bedeutung. Sie wird daher nachfolgend genauer betrachtet.[484]

4.3.5.2 Die Authentisierungsfunktion

Die Berechtigung zur Abfrage der Identität Eine Abfrage der Identität in Online-Anwendungen ist nach § 18 Abs. 4 PAuswG nur mit einer Berechtigung möglich. Eine Be-

[478] Hierzu soll der elektronische Personalausweis mit einem RFID (Radio Frequency Identification) Chip ausgestattet werden, auf dem die biometrischen Daten des Gesichts gespeichert werden können. Vgl. zu diesen Fragestellungen *Hornung*, 2005.

[479] Vgl. § 5 Abs. 9 Satz 1 PAuswG. Damit unterscheidet sich der elektronische Personalausweis vom elektronischen Reisepass, welcher die Speicherung der Fingerabdruckdaten obligatorisch vorsieht. Zu den Rechtsfragen des elektronischen Reisepasses, vgl. etwa *Zilkens*, RDV 2010, 14; *Hasse/Böhlke*, DuD 2009, 274; *Hornung*, DuD 2005, 69 sowie *Hornung*, DuD 2007, 181 und *Pallasky*, DuD 2007, 181.

[480] Der Regierungsentwurf vom 7.10.2008 (BT-Drs. 16/10489) enthielt eine derartige Regelung nicht. Die Regelung wurde erst im parlamentarischen Verfahren aufgenommen, vgl. hierzu Beschlussempfehlung und Bericht des Innenausschusses vom 17.12.2008 (BT-Drs. 16/11419).

[481] Vgl. allgemein zu den signaturrechtlichen Anforderungen beim elektronischen Personalausweis *Roßnagel/Gitter*, in: *Reichl/Roßnagel/Müller* (Hrsg.), Digitaler Personalausweis, 91 ff.; *Strasser* et al., in: *Reichl/Roßnagel/Müller* (Hrsg.), Digitaler Personalausweis, 243 ff. und *Hornung*, 2005, 319 ff.

[482] Hierzu sowie zu den Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung an eine kontaktlos genutzte Chipkarte, vgl. *Roßnagel*, DuD 2009, 403.

[483] *Schulz*, CR 2009, 267.

[484] Vgl. hierzu auch *Roßnagel/Hornung/Schnabel*, DuD 2008, 168.

rechtigung können zum einen sog. „zur Identitätsfeststellung berechtigte Behörden“ erhalten. Nach § 2 Abs. 2 PAuswG sind dies öffentliche Stellen, die befugt sind, zur Erfüllung ihrer gesetzlichen Aufgaben als hoheitliche Maßnahme die Identität von Personen festzustellen. Gemeint sind damit Behörden, die im Rahmen der Eingriffsverwaltung tätig werden und dabei, etwa auf der Grundlage des Polizeirechts, hoheitliche Funktionen ausüben. Nach § 2 Abs. 4 Satz 3 PAuswG erhalten diese Behörden sog. hoheitliche Berechtigungszertifikate. Nur diese Zertifikate ermöglichen den Zugriff auf biometrische Daten.

Daneben können aber auch sog. Diensteanbieter eine Berechtigung erhalten. Diensteanbieter sind nach § 2 Abs. 3 PAuswG natürliche und juristische Personen, die zur Wahrnehmung von Aufgaben der öffentlichen Verwaltung oder zur Erfüllung eigener Geschäftszwecke den Nachweis der Identität oder einzelner Identitätsmerkmale benötigen. Diensteanbieter können nach dem Personalausweisgesetz also sowohl öffentliche als auch nicht-öffentliche Stellen sein. Im Unterschied zu den oben genannten „zur Identitätsfeststellung berechtigten Behörden“ handelt es sich bei den öffentlichen Stellen nach § 2 Abs. 3 PAuswG um solche, die nicht im Rahmen der Eingriffsverwaltung tätig werden, sondern die Identität etwa im Rahmen der Leistungsverwaltung nachprüfen. In diesen Fällen erfolgt der Identitätsnachweis nur als Voraussetzung für die Leistungsgewährung.

Die zuständige Stelle erteilt nach § 21 Abs. 2 Satz 1 Nr. 1-5 PAuswG Dienstanbietern eine Berechtigung, wenn der angegebene Zweck nicht rechtswidrig ist, der Zweck nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen, der antragstellende Diensteanbieter die Erforderlichkeit der zu übermittelnden Angaben für den beschriebenen Zweck nachgewiesen hat, die Anforderungen, insbesondere an den Datenschutz und die Datensicherheit nach der Rechtsverordnung erfüllt sind und keine Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung vorliegen. § 21 Abs. 3 Satz 1 PAuswG sieht dabei vor, die Berechtigung zu befristen; sie darf gemäß § 21 Abs. 3 Satz 2 PAuswG einen Zeitraum von drei Jahren nicht überschreiten. In § 21 Abs. 5 PAuswG ist geregelt, unter welchen Voraussetzungen die Berechtigung zurückgenommen oder widerrufen werden kann.[485] Diese Regelungen gehen den §§ 48 und 49 VwVfG vor und schließen – anders als die subsidiären §§ 48 und 49 VwVfG – ein Ermessen der Behörde aus. Entscheidungen über Widerruf und Rücknahme sind gemäß § 30 PAuswG sofort vollziehbar.

Freie Wahl des Personalausweisinhabers Die Funktion des elektronischen Identitätsnachweises wird im elektronischen Speicher- und Verarbeitungsmedium standardmäßig bereitgestellt. Dennoch kann der Nutzer selbst darüber entscheiden, ob er diese grundsätzlich in Anspruch nehmen will oder nicht. Nach § 10 Abs. 3 PAuswG ist der Nutzer an diese Entschei-

[485] Die Berechtigung soll gemäß § 21 Abs. 5 Satz 2 PAuswG zurückgenommen oder widerrufen werden, wenn die zuständige Datenschutzaufsichtsbehörde es verlangt oder weil Tatsachen die Annahme rechtfertigen, dass der Diensteanbieter die erhaltenen personenbezogenen Daten in unverhältnismäßiger Weise verarbeitet oder nutzt.

dung nicht gebunden. Während der Gültigkeitsdauer des elektronischen Personalausweises kann er seine Entscheidung jederzeit ändern. Bei der Antragstellung hat die Personalausweisbehörde nach § 11 Abs. 2 PAuswG den Nutzer über diese Möglichkeiten zu unterrichten, ihm Informationsmaterial zur Verfügung zu stellen und ihm gemäß § 11 Abs. 3 PAuswG auch schriftlich mitzuteilen, welche Maßnahmen erforderlich sind, um die Sicherheit der Nutzung des elektronischen Identitätsnachweises zu gewährleisten. Nach § 11 Abs. 4 PAuswG muss der Antragstellung schriftlich bestätigen, dass er von der zuständigen Behörde entsprechend unterrichtet wurde. Nach der Antragstellung übersendet der Ausweishersteller dem Antragsteller entsprechend § 13 PAuswG eine Geheimnummer, die Entsperrnummer und das Sperrkennwort des Personalausweises. § 10 Abs. 1 PAuswG bestimmt, dass der Antragsteller bei der Aushändigung schriftlich gegenüber der Personalausweisbehörde zu erklären hat, ob er den Identitätsnachweis nutzen möchte oder nicht. Entscheidet er sich dagegen, teilt er dies bei Abholung seines neuen Ausweises mit. In diesem Fall übergibt er den noch verschlossenen PIN-Brief der Behörde und diese schaltet diese Funktion nach § 10 Abs. 1 Satz 3 PAuswG aus. Dies wird im Personalausweisregister dokumentiert.

Der Vorgang der Übermittlung personenbezogener Daten In § 18 Abs. 4 PAuswG ist der Vorgang der Übermittlung von personenbezogenen Daten genauer beschrieben. Zunächst muss der Diensteanbieter ein Berechtigungszertifikat an den Personalausweisinhaber übermitteln.[486] Dem Berechtigungszertifikat muss der Inhaber nach § 18 Abs. 4 Satz 2 Nr. 1 bis 5 PAuswG zumindest Angaben über die Identität des Diensteanbieters, die angefragten Datenkategorien, den Zweck, für den die Daten verwendet werden sollen, einen Verweis auf die Regeln, nach denen die Daten verarbeitet werden und die im Streitfall zuständige Datenschutzaufsicht entnehmen können sowie den letzten Tag der Gültigkeitsdauer des Berechtigungszertifikats. Auf der Grundlage dieser Informationen kann nun der Inhaber prüfen, ob er personenbezogene Daten an den Diensteanbieter freigibt. Dabei ist es ihm nach § 18 Abs. 5 Satz 2 PAuswG auch möglich, nur einen Teil der angeforderten Daten mitzuteilen.[487] Der eigentliche Übermittlungsvorgang wird dann nach § 18 Abs. 4 PAuswG durch die Eingabe einer Geheimnummer in Gang gesetzt.

4.3.5.3 Bewertung

Der herkömmliche Personalausweis hatte vor allem große Bedeutung für die Eingriffsverwaltung. Durch die neuen Funktionen wird der elektronische Personalausweis in Zukunft auch eine große Bedeutung bei der Leistungsverwaltung und im elektronischen Geschäftsverkehr haben. Immer mehr Bereiche des Wirtschafts-, des Verwaltungs- und des gesellschaftlichen Lebens verlagern sich in das Internet. Im E-Commerce wird der neue Ausweis daher vor allem im Internethandel, etwa bei Plattformen wie eBay und anderen Anbietern und im Dienst-

[486] Vgl. zu den technischen Fragen hierzu *BMI*, 2008, 57 ff., speziell zu den Sicherheitsmechanismen *Bender* et al., DuD 2008, 173.

[487] So kann er zum Beispiel nur die Angabe des Wohnortes oder die Angabe „volljährig“ mitteilen.

leistungsbereich, zum Beispiel beim Online-Banking, weite Verbreitung finden. Auch bei den sog. sozialen Netzwerken wie StudiVZ, XING oder facebook kann der elektronische Personalausweis zum Einsatz kommen. Ein weiteres wichtiges Anwendungsfeld wird der Bereich des E-Government sein. Hier kann der Ausweis zum Beispiel für das Ausfüllen von Formularen oder für das elektronische Genehmigungsverfahren benutzt werden. Im Bereich der elektronischen Justiz wird der Ausweis vor allem bei der elektronischen Akteneinsicht (§ 299 Abs. 3 ZPO) und bei der künftigen elektronischen Einsicht in das Schuldnerverzeichnis (§ 882f ZPO neu) zum Einsatz kommen können.[488]

Die Regelungen im PAuswG können als vorbildlich bezeichnet werden. Positiv hervorzuheben ist vor allem die Ausgestaltung der Authentisierungsfunktion. Der Bürger kann selbst darüber entscheiden, ob er diese Funktion überhaupt nutzen möchte oder nicht. Der Diensteanbieter ist nur dann berechtigt, bestimmte Daten abzufragen, wenn ihm zuvor ein Berechtigungszertifikat in einem Verwaltungsverfahren erteilt worden ist. Bei der Übermittlung von personenbezogenen Daten ist der Diensteanbieter verpflichtet, ebenfalls seine staatlich geprüfte Identität zu übermitteln. Damit wird der Vorgang der Datenübermittlung für den Bürger transparent.[489] Der Bürger kann zudem eine Beschränkung hinsichtlich einzelner Daten vornehmen und der eigentliche Übermittlungsvorgang wird erst durch die Eingabe einer Geheimnummer vorgenommen.[490] Der elektronische Personalausweis kann daher als Vertrauensanker für ein Identitätsmanagement bezeichnet werden. Er gewährleistet, dass Internetnutzer persönliche Daten gezielt, bewusst und sparsam weitergeben. Die Signaturfunktion auf dem Ausweis kann für den Bürger einen zusätzlichen Nutzen bringen. Mit dem Ausweis ist damit nicht nur eine sichere Identifizierung, sondern auch die Abgabe von Willenserklärungen möglich, die gemäß § 126 Abs. 3 und § 126a BGB einer eigenhändigen Unterschrift gleichkommen und mit denen nach § 371a ZPO darüber hinaus ein Anscheinsbeweis oder die Beweisvermutung für die Echtheit des Dokuments verbunden ist. Aufgrund dieser optionalen Kombinationsmöglichkeit wird sich in Zukunft auch die qualifizierte elektronische Signatur verbreiten.

4.3.6 Entwurf eines Bürgerportalgesetzes

Das Bürgerportalprojekt ist Teil der High-Tech-Strategie des Bundes und des E-Government-Programms 2.0.[491] Am 11.11.2008 hat das Bundesinnenministerium des Innern einen Entwurf eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften[492]

[488] Vgl. Abschnitte 7.4 und 8.1.

[489] Damit handelt sich auch nicht um eine Einbahnstraße oder um eine einseitige Authentisierung zwischen Bürger und Diensteanbieter.

[490] Die Mitwirkung des einzelnen Inhabers ist also durch die Elemente Besitz und Willen geschützt. Deshalb sieht § 1 Abs. 1 Satz 3 PAuswG auch vor, dass vom Ausweisinhaber nicht mehr verlangt werden kann, den Ausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam an diesem aufzugeben.

[491] Vgl. hierzu *Stach*, DuD 2008, 184; *Knopp* et al., MMR 2008, 723; *Werner/Wegener*, CR 2009, 310; *Roßnagel* et al., DuD 2009, 728; *Warnecke*, MMR 2010, 227; *Probst*, DSB 2009, 16; *Lappe*, DuD 2009, 651.

[492] Im Folgenden als BPG-E bezeichnet.

veröffentlicht. Vom 20.11. bis zum 12.12.2008 hatte sodann eine Online-Konsultation unter `www.e-konsultation.de` stattgefunden. Während dieser Zeit war es jedem Bürger möglich, sich zu dem Gesetzentwurf zu äußern. Im Anschluss an die Anhörungsphase wurde der Entwurf überarbeitet und am 4.2.2009 hatte das Bundeskabinett den Gesetzentwurf beschlossen. Wegen des erheblichen Zeitmangels wurde das Gesetz jedoch in der 16. Legislaturperiode nicht mehr verabschiedet. Allerdings soll es nach der Durchführung eines am 8.10.2009 gestarteten Pilotprojekts in Friedrichshafen[493] in der nächsten Legislaturperiode beschlossen werden. Im Koalitionsvertrages heißt es hierzu: „Wir werden ein De-Mail-Gesetz verabschieden und dabei die Erfahrungen aus dem Pilotprojekt und die Stellungnahmen der Datenschutzbeauftragten des Bundes und der Länder berücksichtigen. Hierdurch wollen wir den Unternehmen die Möglichkeit geben, Geschäftsprozesse elektronisch abzuwickeln.“[494]

Das Bürgerportal stellt eine elektronische Kommunikationsplattform im Internet dar, welche nach § 1 Abs. 2 Satz 2 BPG-E von einem akkreditierten Diensteanbieter betrieben wird. Dieser weist gemäß § 5 Abs. 1 Satz 2 BPG-E unter bestimmten Voraussetzungen einem Nutzer eine sog. De-Mail-Adresse, also eine Bürgerportaladresse zu, die bei natürlichen Personen aus dem Vor- und Nachnamen und bei juristischen Personen aus dem Namen besteht. Also zum Beispiel: `hermann-gustav.mueller.123@BP-Domain.de-mail.de` bei einer natürlichen Person oder `harry.mustermann@dachdecker-mueller.de-mail.de` bei einer juristischen Person. Der Diensteanbieter ist dabei auch zur Erbringung von pseudonymen Bürgerportaladressen nach § 5 Abs. 2 BPG-E verpflichtet.

4.3.6.1 Die Akkreditierung des Diensteanbieters

Ein Bürgerportalkonto kann nach § 3 BPG-E nur bei einem akkreditierten Diensteanbieter beantragt werden. Wann ein Diensteanbieter akkreditiert werden kann, ist in §§ 17 und 18 BPG-E geregelt. Nach § 17 Abs. 1 BPG-E ist hierfür Voraussetzung, dass der Diensteanbieter nachweist, dass er die Voraussetzungen nach § 18 BPG-E erfüllt und die Aufsicht über die zuständige Stelle gewährleistet ist. § 18 Abs. 1 Nr. 1-4 BPG-E setzt für eine Akkreditierung voraus, dass der Diensteanbieter die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde besitzt, eine geeignete Deckungsvorsorge trifft, seine Pflichten nach dem BPG-E zuverlässig und sicher erbringt und das Zusammenwirken mit den anderen akkreditierten Diensteanbietern gewährleistet und bei Gestaltung und Betrieb der Bürgerportale die Belange des Verbraucherschutzes und die des Datenschutzes beachtet. § 18 Abs. 2 BPG-E enthält Regelungen dazu, wie diese Voraussetzungen nachgewiesen werden können. Die Akkreditierung ist als solche ein Verwaltungsakt, der aufgrund einer bindenden Entscheidung ergeht, d.h. der Antragsteller hat einen Rechtsanspruch auf Akkreditierung, wenn er die Erfüllung der Voraussetzungen des § 18 BPG-E nachweisen kann. Nach erfolgter Akkreditierung soll der Diensteanbieter nach § 17 Abs. 2 BPG-E bei wesentlichen Änderungen, spätestens nach drei Jahren erneut überprüft werden.

493 Vgl. hierzu: `http://www.fn.de-mail.de/` (Zugriff am 20.5.2010).

494 *CDU, CSU und FDP*, Koalitionsvertrag, 94.

4.3.6.2 Die Registrierung der Nutzer

Nach § 3 Abs. 2 Satz 1 BPG-E hat ein akkreditierter Diensteanbieter von einer Person, die ein Bürgerportalkonto beantragt, zuverlässig deren Identität festzustellen. Bei einer natürlichen Person erhebt er dazu nach § 3 Abs. 2 Satz 2 Nr. 1 BPG-E die folgenden Angaben: Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift. Bei einer juristischen Person hat der Anbieter nach § 3 Satz 2 Nr. 2 BPG-E die Angaben Firma, Name oder Bezeichnung, Rechtsform, Registernummer, Anschrift des Sitzes oder der Hauptniederlassung und Namen der Mitglieder des Vertretungsorgangs oder der gesetzlichen Vertreter zu erheben. § 3 Abs. 3 Satz 1 BPG-E schreibt vor, dass der Diensteanbieter die Identität mittels folgender Dokumente überprüfen kann: bei natürlichen Personen durch einen Personalausweis, auch den elektronischen Personalausweis, durch einen Pass oder ein Dokument mit gleichwertiger Sicherheit und bei einer juristischen Person oder Personengesellschaft mittels eines Auszuges aus dem Handels- und Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in die Register- oder Verzeichnisdaten. Abweichend hiervon gestattet der Gesetzentwurf dem Dienstanbieter nach § 3 Abs. 3 Satz 2 BPG-E auch, die Identität anhand von Altdaten festzustellen, sofern diese zuverlässig überprüft worden waren und der Nutzer hiermit einverstanden ist.

4.3.6.3 Die verschiedenen Bürgerportaldienste

Der Entwurf des Bürgerportalgesetzes sieht in den §§ 5 bis 8 BPG-E verschiedene Dienste vor. Der wichtigste Dienst ist der Postfach- und Versanddienst nach § 5 BPG-E. Mit ihm muss der Diensteanbieter seinen Nutzern nach § 5 Abs. 1 BPG-E ein sicheres elektronisches Postfach und einen sicheren Versanddienst für elektronische Nachrichten anbieten. Das sichere elektronische Postfach zeichnet sich durch die vorherige zuverlässige Identifizierung durch den Bürgerportalanbieter aus, durch eine sichere Anmeldung von Sender und Empfänger beim Zugang zu diesem Dienst (also nicht nur Name und Passwort, sondern auch Elemente von Besitz und Wissen[495]) und durch eine Kommunikation über verschlüsselte Leitungen. Dabei sieht der Dienst keine Ende-zu-Ende-Verschlüsselungen vor, da die Nachrichten auf den Servern des sendenden und des empfangenden Bürgerportals im Klartext vorliegen.[496] Diese Sicherungsmaßnahme wird von dem Dienst jedoch unterstützt. § 5 Abs. 6 BPG-E verpflichtet den akkreditierten Diensteanbieter des Weiteren dazu, elektronische Nachrichten förmlich zuzustellen. In diesem Zusammenhang soll in § 174 Abs. 3 ZPO ein weiterer Satz eingefügt werden, nachdem die Übermittlung auch durch ein Bürgerportalkonto erfolgen kann. Im Verwaltungszustellungsgesetz (VwZG) soll ein neuer § 5a eingefügt werden, der die Zustellung über ein Bürgerportal neben den dort genannten Zustellungen als weitere Zustellungsart vor-

[495] Hintergrund hierfür ist die Rechtsprechung zum Anscheinsbeweis. Vgl. etwa OLG Köln, CR 2003, 55; LG Bonn, CR 2002, 293; LG Konstanz, CR 2002, 609.

[496] Zur Kritik hieran vgl. *DSB-Konferenz*, 16.4.2009.

sieht. Da es sich bei dem Diensteanbieter um ein privates Unternehmen handelt, soll dieses für die Vornahme von förmlichen Zustellungen beliehen werden. Hierfür bedarf es jedoch keines Beleihungsaktes. Vielmehr reicht nach § 5 Abs. 6 BPG-E die Akkreditierung des Diensteanbieters aus. Wenn Nachrichten nicht förmlich zugestellt werden, so ermöglicht es der Dienst nach § 5 Abs. 7 BPG-E darüber hinaus, im Verbund der Bürgerportale eine Nachricht zu versenden und entsprechende Bestätigungen darüber zu erlangen, ob die Nachricht angekommen ist.

Mittels des Verzeichnisdienstes nach § 7 BPG-E soll dem Nutzer die Möglichkeit verschafft werden, seine Daten freiwillig so zu veröffentlichen, dass Dritte die Möglichkeit haben, sich über seine Identitäts- und Attributsdaten zu informieren. Der Identitätsbestätigungsdienst nach § 6 BPG-E ist der einzige Dienst, den der Diensteanbieter nicht anzubieten braucht. Wird er bereit gestellt, so ermöglicht er es dem Nutzer die nach § 3 hinterlegten Identitätsdaten Dritten gegenüber zu verwenden. Der Speicherplatzdienst nach § 8 BPG-E soll dem Nutzer schließlich ein Mittel zur langfristigen Ablage und Verwaltung von elektronischen Dokumenten bieten.

4.3.6.4 Verhältnis zum Projekt S.A.F.E.

Bei S.A.F.E. handelt es sich um einen übergreifenden Registrierungs- und Identitätsdienst für föderiertes Identitätsmanagement für Justizanwendungen und E-Governmentanwendungen, der von den Bundesländern Baden-Württemberg und Rheinland-Pfalz federführend entwickelt wird.[497] Die Abkürzung S.A.F.E. steht für Secure Access to Federated eJustice/eGovernment. Ziel ist es, eine Reihe von Standards (gemäß OSCI) vorzugeben, gemäß derer sogenannte Identity Provider, sog. Attribute Services und sog. Service Provider zusammenwirken. Bei den Identity Providern handelt es sich um Dienste, bei denen sich die Teilnehmer registrieren und die gegenüber dem Service Provider die geprüfte Identität des Nutzers bescheinigen. Attribute Services sind Dienste, die einzelnen Nutzern bestimmte Eigenschaften und Berechtigungen zuordnen und diese auf Anforderung des Service Providers oder des Nutzers, bescheinigen. Die Service Provider sind schließlich Dienste, die die eigentlichen Fachanwendungen bereitstellen.

S.A.F.E. geht auf mehrere Beschlüsse unterschiedlicher Gremien zurück. Zunächst wurde das Vorhaben Registrierungsverzeichnis für Kommunikationsdienste (RVKD) genannt. Im Jahr 2006 hatte die Bund-Länder-Kommission ein Deutschland-Online-Projekt „Einheitliche Kommunikationsinfrastruktur für den elektronischen Rechtsverkehr“ initiiert. Sie hat die AG-IT beauftragt, das vorgeschlagene Deutschland-Online-Projekt nach Verabschiedung durch die Justizministerkonferenz zu betreuen und der Bund-Länder-Kommission zu berichten. Auf ihrer Sitzung am 30.11.2006 in Brüssel hat die Justizministerkonferenz den Vorschlag für ein Deutschland-Online-Projekt gebilligt und es an die Ministerpräsidentenkonferenz angemeldet. Die Staatssekretärsrunde hatte sodann 2007 das Projekt ebenfalls gebilligt und der Ministerpräsidentenkonferenz vorgeschlagen, es offiziell als Deutschland-Online-Projekt der Justiz-

[497] Vgl. hierzu *Bund-Länder-Kommission*, 2007 und Projektwebseite `http://www.deutschland-online.de/DOL_Internet/broker.jsp?uMen=404209ab-8d40-9114-fbf1-b1ac0c2f214a` (Zugriff am 10.2.2010).

ministerkonferenz aufzunehmen. Die Ministerpräsidentenkonferenz ist diesem Vorschlag 2007 gefolgt.

Bei S.A.F.E. handelt es sich um eine rein technische Anwendung. Es geht allein darum, eine technische Spezifikation für das Zusammenwirken der genannten Dienste herzustellen. Rechtliche Gesichtspunkte werden nicht thematisiert. Zum Beispiel wird nicht diskutiert, welche Berechtigungen vorliegen müssen, um eine bestimmte Fachanwendung nutzen zu können.

Die Projekte S.A.F.E. und Bürgerportale haben unterschiedliche Zielrichtungen. Ziel der Bürgerportale ist es, sicher im Internet per E-Mail kommunizieren zu können. Hierzu sieht das Konzept eine vorherige zuverlässige Registrierung durch einen Diensteanbieter vor. Gleichzeitig soll die Rechtssicherheit elektronischer Kommunikation durch verbesserte Beweismöglichkeiten sowie die Anerkennung einer rechtssicheren Zustellung von elektronischen Dokumenten gestärkt werden. Ziel des Projektes S.A.F.E ist dagegen, dem Nutzer bestimmte staatliche Fachanwendungen zu ermöglichen, ohne dass er sich mehrmals registrieren muss. S.A.F.E. basiert – im Unterschied zu den Bürgerportaldiensten – nicht auf E-Mail. Um eine bestimmte Fachanwendung nutzen zu können, rufen Nutzer eine Webseite auf.

Der Bundesrat hatte bemängelt, dass sich der Entwurf zum Bürgerportalgesetz mit dem Projekt S.A.F.E nicht auseinandersetzen würde.[498] Der Bundesrat forderte, dass man bei der Konzeption des Bürgerportals auf am Markt etablierte Technologien setzen solle, damit die Bürgerportaldienste auch später noch erweiterbar seien. Dem ist grundsätzlich zuzustimmen. Obwohl – oder gerade weil – die beiden Projekte unterschiedliche Zielrichtungen verfolgen, kann es sinnvoll sein, diese miteinander zu verbinden. Wie sich aus der Stellungnahme der Bundesregierung ergibt, ist die Konzeption S.A.F.E. mit der Konzeption Bürgerportale jedoch eng abgestimmt worden, so dass Verzeichnisdienste der Bürgerportale nach § 7 BPG-E mit den sog. Vertrauensdomänen von S.A.F.E eng zusammenarbeiten können. Auch der Austausch von elektronischen Identitäten ist möglich.[499]

4.3.6.5 Bewertung

Die Bürgerportale sind mit den qualifizierten elektronischen Signaturen und dem neuen elektronischen Personalausweis die dritte Anwendung, mit denen der elektronische Rechtsverkehr auf eine vertrauenswürdige Grundlage gestellt werden kann. Für den Bereich der elektronischen Justiz ist der Gesetzentwurf von Bedeutung, da er die rechtlichen Grundlagen dafür schaffen kann, dass elektronische Dokumente sicher zwischen Parteien und den Gerichten ausgetauscht werden können und förmliche Zustellungen rechtswirksam erfolgen können. Zum Teil wird behauptet, für das BPG-E bestehe keine Notwendigkeit. Der elektronische Personalausweis, die digitale Signatur und Verschlüsselungstechniken würden ausreichen, um den elektronischen Rechtsverkehr auf eine vertrauenswürdige Grundlage zu stellen.[500] Dem kann jedoch nicht zu-

498 BR-Drs. 174/09.
499 BT-Drs. 16/12598, 46.
500 Vgl. hierzu *Deutscher Anwaltsverein*, 2008, 3. In diese Richtung auch *Deutscher Notarverein*, 2008, 1.

gestimmt werden. Der elektronische Personalausweis ist lediglich ein Ausweisdokument. Mit seiner Hilfe soll der Internetnutzer seine Identität in der virtuellen Welt nachweisen können. Der elektronische Personalausweis stellt nur den Ersatz für den herkömmlichen Personalausweis dar.[501] Und die qualifizierte elektronische Signatur stellt den Ersatz für die eigenhändige Unterschrift dar. Dem Internetnutzer ist es mit Hilfe von beiden Anwendungen nicht möglich, nachzuweisen, ob und wann ein Dokument zugegangen ist. Zudem ist es Behörden bislang nicht möglich, die elektronische Zustellung von amtlichen Dokumenten nachzuweisen. Die Vorschriften, die eine elektronische Zustellung in der Prozessordnung ermöglichen, sehen lediglich eine freiwillige Empfangsbestätigung des Adressaten vor und weisen zudem teilweise einen beschränkten Personenkreis auf.[502]

Als problematisch bei der elektronischen Zustellung wird es angesehen, Diensteanbieter mit hoheitlichen Funktionen zu beleihen.[503] Dies führe zu einer Vermengung von hoheitlichen Aufgaben und kommerziellen Interessen. Der Bürger bleibe damit im Unklaren darüber, ob er einem hoheitlich handelnden Beliehenen gegenüberstehe oder einem kommerziellen Anbieter.[504] Dem ist jedoch entgegenzuhalten, dass auch andere Beliehene neben hoheitlichen Aufgaben kommerzielle Tätigkeiten ausüben. Zudem müssen Anbieter im Abstand von drei Jahren zertifiziert werden und werden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) überwacht. Auch die herkömmlichen Zustellungen werden an Private ausgelagert. So sieht § 168 ZPO vor, dass die Geschäftsstelle einen nach § 33 Postgesetz (PostG) beliehenen Unternehmer mit der Zustellung beauftragen kann. Nur in den wenigsten Fällen nimmt die Geschäftsstelle oder der Gerichtswachtmeister die Zustellung heute noch selbst vor. Ebenso wie § 35 PostG enthält auch der Entwurf des Bürgerportalgesetzes eine Haftungsregelung für Pflichtverletzungen im Zusammenhang mit der Durchführung von förmlichen Zustellungen. Missbräuchen des Diensteanbieters bei der Vornahme der Zustellung kann daher wirksam begegnet werden.

Zudem wird geltend gemacht, dass die Vorschriften zur elektronischen Zustellung als Ausübung einer hoheitlichen Gewalt einen grundrechtsrelevanten Eingriff darstellen würden. Die herkömmlichen Zustellungsarten seien dadurch gekennzeichnet, dass der Anspruchssteller aktiv werden müsse, um die Zustellung zu bewirken. So müsse dieser das Schriftstück in den Machtbereich des Empfängers bringen und die Zustellung nachweisen. Bei den hier vorgesehenen Zustellungen sei dies nicht mehr der Fall. Denn hier müsse sich der Nutzer erst in das Portal einloggen und eine technische Infrastruktur bereithalten. Nicht der Anspruchssteller, sondern er, der Gegner, müsse also aktiv werden. Dies führe zu einer Verschiebung des prozessualen Gleichgewichts zwischen Anspruchssteller und Anspruchsgegner, der der breiten Masse nicht zugänglich sei.[505] Probleme würden insbesondere auch dann bestehen, wenn der Diensteanbieter das Portal gesperrt habe. In diesem Fall habe der Bürger gar keine Möglichkeit, von

501 *Roßnagel/Hornung*, DÖV 2009, 305.
502 Vgl. im Einzelnen Abschnitt 7.2.
503 Vgl. hierzu *Deutscher Notarverein*, 2008, 4.
504 *Deutscher Notarverein*, 2008, 4.
505 *Deutscher Notarverein*, 2008, 15.

der elektronischen Zustellung zu erfahren.[506] Diesen Bedenken ist jedoch entgegenzuhalten, dass auch bei dem vorgesehenen BPG-E der Nachweis der elektronischen Zustellung bei der zustellenden Behörde verbleibt. Diese muss das elektronische Dokument nach wie vor in den Machtbereich des Empfängers bringen. Dies ist eben nicht mehr der herkömmliche Briefkasten, sondern ein neuer „elektronischer Briefkasten“. Genauso wie der Empfänger seinen herkömmlichen Briefkasten mit einem Schlüssel öffnen muss, muss er sich beim Bürgerportal eben entweder durch Name und Passwort oder durch weitere Sicherheitsmerkmale einloggen. Sollte der Diensteanbieter das Konto tatsächlich gesperrt haben, müsste die zustellende Behörde hierüber informiert werden und in diesem Fall wäre nicht von einer wirksamen Zustellung auszugehen.[507]

4.4 Zusammenfassung

Das Volkszählungsurteil des Bundesverfassungsgerichts hat das informationelle Selbstbestimmungsrecht in der Justiz gestärkt. So sind – wenngleich zum Teil mit großer Verspätung – eine Reihe bereichsspezifischer Gesetze und Vorschriften für die Justiz erlassen worden. Zu diesen gehören das Justizmitteilungsgesetz, das Schriftgutaufbewahrungsgesetz des Bundes und eines Teils der Länder sowie die Überarbeitung von Vorschriften zum Schuldnerverzeichnis. Mit dem Urteil zur Online-Durchsuchung wurde ein weiteres Grundrecht aus dem allgemeinen Persönlichkeitsrecht abgeleitet – das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Angesichts dessen, dass das Bundesverfassungsgericht nunmehr zwei neue Grundrechte basierend auf dem allgemeinen Persönlichkeitsrecht formuliert hat, wäre es an der Zeit, diese Grundrechte auch im Grundrechtskatalog des GG zu verankern. Dies würde auch für den Datenschutz in der elektronischen Justiz einen Gewinn bringen. Grundrechte sind nicht nur Abwehrrechte gegenüber dem Staat. Zur effektiven Ausübung von Grundrechten hat der Staat auch Schutzpflichten. Er hat dafür zu sorgen, dass die Bürger sicher und datenschutzkonform im Internet kommunizieren können. Vor diesem Hintergrund kommt auch dem Signaturgesetz und in Zukunft dem Personalausweisgesetz eine bedeutende Funktion zu. Es ist zu hoffen, dass in dieser Legislaturperiode auch das Bürgerportalgesetz verabschiedet werden wird. Die nachfolgende Tabelle zeigt noch einmal die Normenhierarchie im Datenschutz in der elektronischen Justiz.

[506] *Deutscher Notarverein*, 2008, 19.
[507] So wie hier *Roßnagel* et al., DuD 2009, 133. A.A. jedoch *Lappe*, DuD 2009, 651.

EU:

- Grundrechtscharta der EU (Art. 8)
- EG-Datenschutzrichtlinie

Verfassungsrecht:

- Volkszählungsentscheidung des BVerfG (Recht auf inform. Selbstbestimmung)
- Entscheidung des BVerfG zur Online-Durchsuchung
- Art. 4a LV Rheinland-Pfalz

BDSG:

- Organe der Rechtspflege des Bundes § 2 Abs. 1: BGH
- nicht-öffentliche Stellen § 2 Abs. 4: Rechtsanwälte, Parteien, Verfahrensbeteiligte, sofern Umgang mit Datenverarbeitungsanlagen oder automatisierten Dateien

LDSG:

- Organe der Rechtspflege des Landes § 2 Abs. 1 Nr. 2: OLG, LG, AG
- ebenso: Notare (BGH, NJW 1991, 568)

Bereichsspezifische Gesetze:

- SchrAG (2005)
- LSchrAG (2008)
- JuMiG (1998)

Bereichsspezifische Vorschriften:

- § 299 Abs. 2 ZPO: „rechtliches Interesse“
- § 12 GBO: „berechtigtes Interesse“
- § 915b Abs. 1 ZPO: „Darlegung näher bezeichneter Voraussetzungen“
- § 9 HGB: „jedem zu Informationszwecken“

Datensicherheit:

- SigG
- PAuswG
- BPG-E

Tabelle 3: Normenhierarchie.

Kapitel 5

Anforderungen des Datenschutzes an die elektronische Justiz

Nachdem der Rechtsrahmen beleuchtet wurde, werden in diesem Kapitel die Anforderungen des Datenschutzes an die elektronische Justiz aufgezeigt. Zunächst werden die tragenden Grundsätze des Datenschutzes vorgestellt. Sodann wird geprüft, unter welchen Voraussetzungen personenbezogene Daten in der Justiz verarbeitet werden können. Im Anschluss hieran werden die Vorgaben für die Datensicherheit in der elektronischen Justiz beschrieben. Schließlich werden die Rechte des Betroffenen betrachtet.

5.1 Allgemeine Datenschutzgrundsätze

Zu den allgemeinen Datenschutzgrundsätzen gehören der Grundsatz der Verhältnismäßigkeit, der Grundsatz der Zweckbindung, der Grundsatz der Datenvermeidung und Datensparsamkeit, der Grundsatz des Verbots mit Erlaubnisvorbehalt und der Grundsatz der Transparenz.

5.1.1 Grundsatz der Verhältnismäßigkeit

Es wurde bereits festgestellt,[508] dass das informationelle Selbstbestimmungsrecht nicht schrankenlos gewährleistet wird. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über seine Daten, er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Um ein gemeinschaftliches Zusammenleben zu ermöglichen, muss in das informationelle Selbstbestimmungsrecht eingegriffen werden. Der Staat benötigt seine Daten zur Aufgabenerfüllung und auch die Privatwirtschaft ist, etwa um Vertragsschlüsse abzuwickeln, ebenfalls auf die Verarbeitung von personenbezogenen Daten angewiesen.[509] Da sich Gefahren für die Persönlichkeitsrechte von

[508] Vgl. hierzu Abschnitt 4.2.1.1.
[509] *Gola/Klug*, 2003, 46.

Betroffenen am wirksamsten dadurch vermeiden lassen, dass ihre Verarbeitung und Nutzung auf das notwendige Maß beschränkt wird, hat der Gesetzgeber bei der Ausgestaltung einer verfassungsgemäßen gesetzlichen Grundlage den Grundsatz der Verhältnismäßigkeit zu beachten. Der Grundsatz der Verhältnismäßigkeit besagt, dass eine Verarbeitung von personenbezogenen Daten nur zulässig ist, wenn die Informationen für die Erreichung eines bestimmten Zwecks geeignet und erforderlich sind.[510] Wie noch zu sehen sein wird, finden sich für den Bereich der elektronischen Justiz vielfältige Konkretisierungen dieses Grundsatzes in den allgemeinen Datenschutzgesetzen und in den Verfahrensordnungen.[511]

5.1.2 Grundsatz der Zweckbindung

In engem Zusammenhang mit dem Grundsatz der Verhältnismäßigkeit steht der Grundsatz der Zweckbindung. Dieser Grundsatz besagt, dass ein Zwang zur Abgabe personenbezogener Daten voraussetzt, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Zum Schutz gegen Zweckentfremdung sind Weitergabe- und Verwertungsverbote erforderlich. In Konkretisierung dieses Grundsatzes hat der Gesetzgeber zum Beispiel in § 915 ZPO festgelegt, unter welchen Voraussetzungen ein Verzeichnis von Schuldnern angelegt werden und unter welchen Voraussetzungen dieses von Dritten eingesehen werden darf. Der Grundsatz der Zweckbindung, der im Übrigen ebenfalls in vielfältigen Vorschriften in den allgemeinen Datenschutzgesetzen und in den Verfahrensordnungen zum Ausdruck kommt, bedeutet weiter, dass eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder nicht bestimmbaren Zwecken unzulässig ist.[512] Es wäre daher zum Beispiel unzulässig, wenn die Gerichte – um nach dem Eingang einer Klageschrift Zeit bei der Erfassung der Angaben der Parteien einzusparen – eine Sammlung von Daten solcher Personen anlegen würden, die häufig in einen Rechtsstreit verwickelt sind.

5.1.3 Grundsatz der Datenvermeidung und Datensparsamkeit

Für die technische Gestaltung der Datenverarbeitungssysteme wird der Grundsatz der Verhältnismäßigkeit durch den Grundsatz der Datenvermeidung und Datensparsamkeit, welcher in § 3a Satz 1 BDSG und in § 1 Abs. 3 Satz 1 LDSG zum Ausdruck kommt, konkretisiert. Er stellt einen Programmsatz dar[513] und besagt, dass bereits bei Gestaltung und Auswahl der Datenverarbeitungssysteme darauf zu achten ist, dass bei ihrer Anwendung der Umfang der zu erhebenden, zu verarbeitenden oder zu nutzenden personenbezogenen Daten auf ein Minimum beschränkt wird. Um diesen Anforderungen gerecht zu werden, soll zum Beispiel gemäß § 3a Satz 2 BDSG und § 1 Abs. 3 Satz 2 LDSG von den Möglichkeiten der Anony-

510 *Gola/Klug*, 2003, 46.
511 Vgl. hierzu Abschnitt 5.2.
512 *Bergmann/Möhrle/Herb*, Datenschutzrecht, Systematik Ziff. 2.3.3.5.
513 *Gola/Klug*, 2003, 47.

misierung und Pseudonymisierung Gebrauch gemacht werden. Auch dieser Grundsatz spielt in der elektronischen Justiz eine bedeutsame Rolle. Zum Beispiel besagt § 12 GBO, dass eine Grundbucheinsicht nur gestattet ist, wenn ein berechtigtes Interesse dargelegt wurde. Damit nicht mehr Daten als nötig abgefragt werden, bestimmt § 133 Abs. 1 Nr. 1 GBO, dass ein automatisierter Abruf von Grundbuchdaten nur vorgenommen werden darf, wenn in technischer Hinsicht sichergestellt ist, dass die nach § 12 GBO zulässige Einsicht nicht überschritten wird.

5.1.4 Verbotsprinzip mit Erlaubnisvorbehalt

Das Verbotsprinzip mit Erlaubnisvorbehalt besagt, dass die Verarbeitung von personenbezogenen Daten grundsätzlich verboten und nur ausnahmsweise erlaubt ist. Vor diesem Hintergrund trifft das Gesetz Aussagen und legt Voraussetzungen fest, nach denen die Datenverarbeitung zulässig ist.[514] Die grundsätzlichen Erlaubnistatbestände finden sich in den allgemeinen Datenschutzgesetzen, sofern nicht vorrangige Spezialregelungen, hier insbesondere die Verfahrensordnungen, vorgehen.

5.1.5 Grundsatz der Transparenz

Nach dem Volkszählungsurteil des Bundesverfassungsgerichts wäre mit dem Recht auf informationelle Selbstbestimmung eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß. Es gehört zu den datenschutzrechtlichen Grundpositionen eines Betroffenen, dass die Verarbeitung seiner Daten nicht hinter seinem Rücken stattfinden darf. Dies setzt voraus, dass der Betroffene ordnungsgemäß und umfassend über die Bedingungen der ihn betreffenden Datenverarbeitung und -nutzung informiert wird. Die Transparenz soll insbesondere durch den Grundsatz der Direkterhebung und den damit verbundenen Unterrichtungspflichten gewährleistet sein.[515] Zudem sind ergänzend Benachrichtigungs- und Auskunftspflichten vorgesehen.[516]

5.2 Zulässigkeit der Datenverarbeitung in der elektronischen Justiz

Da nun die allgemeinen Grundsätze des Datenschutzrechts bekannt sind, wird im Folgenden darauf eingegangen, unter welchen Voraussetzungen eine Verarbeitung von personenbezogenen Daten in der elektronischen Justiz zulässig ist. Wie bereits festgestellt wurde, gilt im Datenschutzrecht der Grundsatz des Verbots mit Erlaubnisvorbehalt. Eine Verarbeitung von

514 *Bergmann/Möhrle/Herb*, Datenschutzrecht, Systematik Ziff. 3.2.1.
515 Vgl. hierzu Kapitel 5.2.
516 *Gola/Klug*, 2003, 49.

personenbezogenen Daten ist deshalb nach § 4 Abs. 1 BDSG und § 5 Abs. 1 LDSG nur zulässig, wenn der Betroffene eingewilligt hat oder sie durch eine Rechtsgrundlage gedeckt ist. Obwohl die Begriffe der Erhebung und Nutzung nicht Teil der Datenverarbeitung sind und damit nicht vom Wortlaut der genannten Vorschriften erfasst sind, gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt auch für diese Phasen des Datenumgangs. Dies folgt aus der Eingriffsqualität von Datenerhebung und -nutzung in das Datenschutzgrundrecht.[517]

5.2.1 Einwilligung des Betroffenen

Bei der Einwilligung handelt es sich um die aktive Ausübung des Grundrechts auf informationelle Selbstbestimmung. Das Bundesverfassungsgericht hat dies in seinem Volkszählungsurteil als die Befugnis des Einzelnen bezeichnet, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen.[518] Die Einwilligung ist daher nicht nur Ermächtigungsgrundlage, vielmehr ist ihre Erteilung oder Nichterteilung selbst die Ausübung des Rechts auf informationelle Selbstbestimmung, also ein Instrument der datenschutzrechtlichen Selbstbestimmung.[519] Die Einwilligung ist gemäß § 184 BGB die vorherige Zustimmung. Die Zustimmung ist eine empfangsbedürftige Willenserklärung. Diese muss den Anforderungen der §§ 104 ff. BGB entsprechen und vor der Vornahme des Rechtsgeschäfts erklärt werden.[520] Durch das BDSG und das LDSG ist sie außerdem an weitere Formalitäten gebunden worden. So muss die Einwilligung schriftlich[521] erfolgen oder nach § 126a BGB mittels einer qualifizierten elektronischen Signatur. Eine einfache elektronische Form genügt nicht den Anforderungen an eine wirksame Einwilligung.[522] Nur wenn besondere Umstände vorliegen, ist ausnahmsweise eine andere Form als die Schriftform zulässig.[523] Solche besonderen Umstände liegen zum Beispiel vor, wenn eine schriftliche Erteilung der Einwilligung nicht mehr rechtzeitig eingeholt werden kann oder sie den Verarbeitungszweck verfehlen würde.[524] Zusätzlich muss die Einwilligung weitere Spezifizierungen enthalten. So muss die Einwilligungserklärung im äußeren Erscheinungsbild besonders hervorgehoben werden, wenn sie zusammen mit anderen Erklärungen schriftlich erteilt wird[525] und es gelten besondere Hinweis- und Aufklärungspflichten, vor allem hinsichtlich des Zwecks der vorgesehenen Datenverarbeitung.[526]

---

517 *Globig*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 641.

518 BVerfGE 65, 1 (48).

519 *Geiger*, NVwZ 1989, 35; *Simitis*, in: *ders.*, BDSG, § 4 a, Rn. 1; *Weichert*, in: *Kilian/Heussen* (Hrsg.), Computerrechtshandbuch, Rn. 150. Anders dagegen *Robbers*, JuS 1985, 925, welcher die Einwilligung als Grundrechtsverzicht bewertet.

520 Eine nachträgliche Einwilligung verhilft der Datenverarbeitung nicht zu ihrer Rechtmäßigkeit. Vgl. hierzu *Auernhammer*, BDSG, § 4a Rn. 11.

521 Vgl. § 4a Abs. 1 Satz 3 BDSG und 5 Abs. 3 Satz 1 LDSG.

522 Anders *Schaar*, MMR 2001, 644. Wie hier *Yildirim*, 2004, 167 mit zutreffender Begründung.

523 Vgl. § 4a Abs. 1 Satz 3 2. Hs. BDSG und § 5 Abs. 3 Satz 1 2. Hs. LDSG.

524 *Simitis*, in: *ders.*, BDSG, § 4a Rn. 45.

525 Vgl. § 4a Abs. 1 Satz 4 BDSG und § 5 Abs. 3 Satz 2 LDSG.

526 Vgl. § 4a Abs. 1 Satz 2 BDSG und § 5 Abs. 2 Satz 2 und 3 LDSG.

Vereinzelt finden sich in den Verfahrensordnungen bereichsspezifische Einwilligungserklärungen. So bestimmt § 117 Abs. 2 Satz 2 ZPO etwa, dass die Erklärung über die persönlichen und wirtschaftlichen Verhältnisse samt den Belegen der gegnerischen Partei nur dann zugänglich gemacht werden dürfen, wenn der Antragsteller dem vorher zugestimmt hat.[527] § 127 Abs. 1 Satz 3 ZPO enthält eine vergleichbare Regelung für den Ablehnungsbeschluss des Prozesskostenhilfe-Antrags. Wenn dieser auch Angaben zu den persönlichen und wirtschaftlichen Verhältnissen erhält, dürfen diese dem Gegner nur mit Zustimmung der Partei zugänglich gemacht werden.[528] Oder: Bei der Gewährung von Akteneinsicht ist in § 299 Abs. 2 ZPO geregelt, dass der Vorstand des Gerichts, also etwa der Amtsgerichtsdirektor oder der Landgerichtspräsident, die Einsicht in die Akten ohne Einwilligung der Parteien nur gestatten darf, wenn ein rechtliches Interesse dargetan wurde.[529] Und weiter: Gemäß § 97 InsO ist der Schuldner etwa verpflichtet, bestimmten Personen und Einrichtungen Auskunft zu geben. Nach Satz 3 der Vorschrift dürfen diese Informationen aber nur mit seiner Zustimmung in einem Strafverfahren oder Ordnungswidrigkeitenverfahren verwendet werden. Und um ein letztes Beispiel zu nennen, sei auf § 133 Abs. 4 GBO hingewiesen. Dieser bestimmt, dass eine automatisiere Bearbeitung von Anträgen auf Auskunft aus dem Grundbuch u.a. nur dann zulässig ist, wenn der Berechtigte einer solchen zugestimmt hat. Diese bereichsspezifischen Einwilligungserklärungen gehen denen der allgemeinen Datenschutzgesetze vor.

5.2.2 Allgemeine Erlaubnisnormen

5.2.2.1 Das Erheben von personenbezogenen Daten

Eine Legaldefinition der Erhebung personenbezogener Daten findet sich in § 3 Abs. 3 BDSG und in § 3 Abs. 2 Satz 2 Nr. 1 LDSG. Danach ist das Erheben das Beschaffen von personenbezogenen Daten. Die Einbeziehung der Erhebung in den Regelungsbereich des BDSG und des LDSG beruht auf der Rechtsprechung des Bundesverfassungsgerichts, das im Volkszählungsurteil diese Phase als besonders bedeutsam und eingriffsintensiv hervorgehoben hat.[530] Der Begriff der Erhebung verlangt immer ein irgendwie geartetes aktives Tun. Damit liegt ein Erheben personenbezogener Daten nicht vor, wenn der verantwortlichen Stelle personenbezogene Daten nicht ohne konkretes oder generelles Auskunftsersuchen mitgeteilt werden oder wenn sie auf andere Weise zufällig Kenntnis von persönlichen oder sachlichen Verhältnissen des Betroffenen erlangt.[531] Zulässig ist das Erheben personenbezogener Daten, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.[532] Die Definition der jeweiligen Aufgabe ist den Gesetzen und Rechtsvorschriften zu entnehmen, durch die die Existenz

[527] Vgl. hierzu Abschnitt 7.4.
[528] Vgl. hierzu Abschnitt 7.4.
[529] Vgl. hierzu Abschnitt 7.4.
[530] BVerfGE 65, 1 (43).
[531] Eine Erhebung liegt daher nicht vor, wenn der Konkursverwalter zufällig Patientendaten beim Öffnen der Post des Gemeinschuldners zur Kenntnis nimmt. Vgl. hierzu OLG Bremen, NJW 1993, 798.
[532] § 13 Abs. 1 BDSG und § 12 Abs. 1 LDSG.

und die Tätigkeit der jeweiligen öffentlichen Stelle rechtlich begründet wird. Voraussetzung hierfür sind die örtliche und die sachliche Zuständigkeit. In § 4 Abs. 2 Satz 1 BDSG und in § 12 Abs. 2 Satz 1 LDSG findet sich der Grundsatz, dass die Daten beim Betroffenen selbst zu erheben sind. Nur wenn dies nicht praktikabel oder sonst unangemessen ist, ist zu prüfen, ob eine andere Erhebungsform zulässig ist. Das BDSG und das LDSG sehen als weitere Erhebungsform gemeinsam die Datenerhebung bei Dritten[533] vor und – das LDSG darüber hinaus – die Datenerhebung beim Betroffenen ohne dessen Kenntnis bzw. Mitwirkung.[534]

In den Verfahrensordnungen kommt den allgemeinen Erhebungsregeln in den Datenschutzgesetzen nur eine geringe Bedeutung zu. Dies liegt daran, dass sie durch die allgemeinen Verfahrensgrundsätze, insbesondere durch den Amtsermittlungsgrundsatz „überlagert“ werden. So werden die Zwangsvollstreckung und die Zwangsversteigerung auf Antrag eines Gläubigers von Amts wegen durchgeführt.[535] Gemäß § 4 InsO und gemäß § 26 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) gilt im Insolvenzverfahren, in der Grundbuchordnung und im Handelsgesetzbuch der Grundsatz der Amtsermittlung. Damit verbunden sind vielfältige Formen der Datenerhebung, die in den einzelnen Verfahrensordnungen – zum großen Teil schon vor Erlass der allgemeinen Datenschutzgesetze – speziell geregelt wurden. Mit dem weitestgehenden Eingriff in das informationelle Selbstbestimmungsrecht gehen dabei sicherlich die verschiedenen Formen der Datenerhebungen beim Schuldner in einem Zwangsvollstreckungs- oder Zwangsversteigerungsverfahren oder in einem Insolvenzverfahren[536] einher. Sicherlich ist dabei zu berücksichtigen, dass der Justizgewährungsanspruch des Staates zu einer wirkungsvollen Durchsetzung von Gläubigerforderungen verpflichtet.[537] Dessen ungeachtet muss der mit den Datenerhebungen verbundene Eingriff in das informationelle Selbstbestimmungsrecht jedoch verhältnismäßig sein. Hieran bestehen Zweifel, wenn man sich vergegenwärtigt, mit welchen weitreichenden Ermittlungsbefugnissen zum Beispiel der Gerichtsvollzieher nach dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung ausgestattet worden ist. Man kann dessen zukünftige Rolle mit Fug und Recht fast mit einem Staatsanwalt in einem strafrechtlichen Ermittlungsverfahren vergleichen:

---

533 § 4 Abs. 2 Satz 2 BDSG und § 12 Abs. 4 LDSG.

534 § 12 Abs. 3 LDSG.

535 *Zöller*, ZPO, Vor § 704 Rn. 20.

536 In der Insolvenzordnung sieht § 20 Abs. 1 InsO im Falle der Zulässigkeit des Antrags auf Eröffnung eines Insolvenzverfahrens zum Beispiel vor, dass der Schuldner dem Insolvenzgericht die Auskünfte zu erteilen hat, die zur Entscheidung über den Antrag erforderlich sind. § 97 Abs. 1 InsO bestimmt des Weiteren, dass der Schuldner verpflichtet ist, dem Insolvenzgericht, dem Insolvenzverwalter, dem Gläubigerausschuss und auf Anforderung des Gerichts der Gläubigerversammlung über alle das Verfahren betreffenden Verhältnisse Auskunft zu geben. Dies gilt insbesondere auch für solche Tatsachen, die geeignet sind, eine Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit herbeizuführen. Schließlich regeln die §§ 21 Abs. 2 Nr. 4 und 99 Abs. 1 InsO die Möglichkeit der Anordnung einer Postsperre. So kann das Insolvenzgericht, wenn es erforderlich erscheint, für die Gläubiger nachteilige Prozesshandlungen des Schuldners aufklären und anordnen, dass näher bezeichnete Unternehmen bestimmte oder alle Postsendungen für den Schuldner an den Verwalter zuzuleiten haben.

537 BVerfG, NJW 1988, 3141.

So ermöglicht § 802l Abs. 1 Satz 1 Nr. 1 ZPO neu zum Beispiel in Zukunft eine Abfrage des Gerichtsvollziehers bei einem Träger der Rentenversicherung[538] mit dem Ziel der Ermittlung des Arbeitgebers des Schuldners, um ggf. eine Lohnpfändung durchführen zu können.[539] § 802l Abs. 1 Satz 1 Nr. 2 ZPO neu ermöglicht dem Gerichtsvollzieher etwa die Ermittlung von Konten und Depots des Schuldners bei Kreditinstituten. Die Kontostammdatenabfrage hat über das Bundeszentralamt für Steuern zu erfolgen. § 802l Abs. 1 Satz 1 Nr. 3 ZPO neu gestattet dem Gerichtsvollzieher auch die Erhebung von Fahrzeug- und Halterdaten des Schuldners beim Kraftfahrtbundesamt. Diese Einholung von Fremdauskünften stehen – abgesehen davon, dass die Abrufe zur Vollstreckung erforderlich sein müssen – gemäß § 802l Abs. 1 Satz 1 und 2 ZPO neu lediglich unter der Bedingung, dass „sich der zu vollstreckende Anspruch des Gläubigers auf mindestens 500 EUR beläuft“, und „der Schuldner die Vermögensauskunft nicht abgibt oder eine Vollstreckung in die in dem Vermögensverzeichnis aufgeführten Vermögensgegenstände voraussichtlich nicht zu einer vollständigen Befriedigung des Gläubigers führt“. Hält man sich vor Augen, dass es sich bei dem Betrag von 500 EUR, der sich nicht nur aus der eigentlichen Forderung des Gläubigers, sondern auch aus den Kosten der Zwangsvollstreckung zusammensetzt,[540] um eine eher geringe Summe handelt und berücksichtigt man zudem, dass die Datenerhebungen auch ohne ein „Verschulden“ des Schuldners möglich sind, nämlich einfach dann, wenn sich aus dem Vermögensverzeichnis ergibt, dass der Schuldner mittellos ist, dürften nach einer sorgfältigen Interessenabwägung die Grenzen eines zulässigen Eingriffs in das informationelle Selbstbestimmungsrecht wohl überschritten sein.

Im Unterschied zu den bereits genannten Verfahrensordnungen gilt im Zivilverfahren nicht der Amtsermittlungsgrundsatz, sondern der Beibringungsgrundsatz. Dieser wird auch als Verhandlungsgrundsatz bezeichnet. Er besagt, dass das Gericht bei der Beschaffung des Prozessstoffes seiner Entscheidung nur das Tatsachenmaterial zugrunde legen darf, das von den Parteien vorgetragen wurde.[541] Folglich übermitteln also die Parteien zunächst einmal dem Gericht den aus ihrer Sicht relevanten Tatsachenstoff. Die ZPO legt hier fest, auf welche Art und Weise dies zu erfolgen hat. So hat etwa ein Kläger nach § 253 Abs. 4 i.V.m. § 130 Nr. 1 ZPO mit der Klageerhebung für sich und den Beklagten den Namen, den Stand oder das Gewerbe, den Wohnort und die Parteistellung anzugeben. Des Weiteren sind etwa gemäß §§ 373, 359 Nr. 2 ZPO die Zeugen und Sachverständigen mit Namen und ladungsfähiger Anschrift genau zu bezeichnen. Etwaige Datenerhebungen des Gerichts finden nur soweit statt, soweit die Parteien dem Gericht das Tatsachenmaterial geliefert haben und sich das Gericht über die Wahrheit

538 § 147 Abs. 1 SGB VI.

539 Vgl. hierzu BT-Drs. 16/10069, 32. Der Gerichtsvollzieher hat den zuständigen Rentenversicherungsträger nicht erst zu ermitteln. Sofern der Rentenversicherungsträger für den Schuldner nicht zuständig ist, soll dieser das Gesuch einfach an den zuständigen Rentenversicherungsträger weiterreichen und dieser soll dem Gerichtsvollzieher sodann die Daten übermitteln.

540 Vgl. hierzu § 802l Abs. 1 Satz 2 2. Hs. ZPO neu: „(...) Kosten der Zwangsvollstreckung und Nebenforderungen sind bei der Berechnung nur zu berücksichtigen, wenn sie allein Gegenstand der Vollstreckung sind.“

541 *Zöller*, ZPO, Vor § 128 Rn. 10.

oder Unwahrheit der betreffenden Behauptungen ein Bild machen muss. So hat ein Richter etwa nach §§ 395 Abs. 2, 402 ZPO bei der Beweisaufnahme zur Feststellung von Identität und Eidesfähigkeit von Zeugen oder Sachverständigen diese über Namen, Vornamen, Alter, Stand, Gewerbe und den Wohnort zu befragen. Im Ermessen des Gerichts steht es dabei, den Zeugen zwecks Überprüfung seiner Glaubwürdigkeit über weitere Umstände, insbesondere über seine Beziehungen zu den Parteien zu erfragen.[542]

Nur wenn sich das Gericht aufgrund des vorgebrachten Tatsachenmaterials kein vollständiges Bild über den Sachverhalt machen kann, gestattet das Gesetz dem Gericht in bestimmten Fällen auch ohne Antrag der Parteien weitere Aufklärungsmaßnahmen.[543] Hierzu gehören etwa die Einnahme des Augenscheins sowie die Begutachtung durch Sachverständige gemäß § 144 ZPO, die Vorlage von Urkunden oder Akten nach §§ 142, 143 ZPO, die Anordnung von ergänzenden Vernehmungen einer oder beider Parteien nach § 448 ZPO sowie die Einholung von amtlichen Auskünften aufgrund von § 273 Abs. 2 Nr. 2 ZPO. In diesen Fällen stößt der Beibringungsgrundsatz jedoch an seine Grenzen.[544]

Weitere wichtige Datenerhebungen durch die Gerichte gehen schließlich mit der Beantragung eines Prozesskostenhilfeverfahrens einher. Mit dem Prozesskostenhilfeverfahren soll verhindert werden, dass Parteien aus wirtschaftlichen Gründen daran gehindert werden, ihr Recht vor Gericht durchzusetzen.[545] Art. 3 Abs. 1 GG erfordert ein derartiges Verfahren. Wie sich aus § 114 ZPO ergibt, ist das Prozesskostenhilfeverfahren ein Antragsverfahren. Mit dem Antrag hat die Partei gemäß § 117 Abs. 2 ZPO einen Vordruck auszufüllen. § 118 Abs. 2 Satz 2 ZPO gestattet es nun dem Gericht zur Prüfung der Bedürftigkeit weitere Erhebungen anzustellen, insbesondere kann es die Vorlage von Urkunden anordnen und Auskünfte einholen. Um hierdurch jedoch nicht den im Zivilprozess geltenden Beibringungsgrundsatz außer Kraft zu setzen, sollte davon zurückhaltend Gebrauch gemacht werden.[546]

5.2.2.2 Das Speichern und Nutzen von personenbezogenen Daten

Nach § 3 Abs. 4 Satz 2 Nr. 1 BDSG und nach § 3 Abs. 2 Satz 2 Nr. 2 LDSG ist unter dem Begriff des Speicherns das Erfassen, Aufnehmen oder Aufbewahren von personenbezogenen Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung oder Verwendung zu verstehen. Nutzen ist gemäß § 3 Abs. 5 BDSG und § 3 Abs. 2 Satz 2 Nr. 3 LDSG dabei jede sonstige Verwendung personenbezogener Daten. In welchen Fällen personenbezogene Daten gespeichert und genutzt werden dürfen, ist in § 14 BDSG und in § 13 LDSG bestimmt. Nach § 14 Abs. 1 BDSG und nach § 13 Abs. 1 LDSG ist eine Speicherung und Nutzung zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist und wenn die mit der Speicherung oder Nutzung

542 *Zöller*, ZPO, § 395 Rn. 3.
543 *Zöller*, ZPO, Vor § 128 Rn. 11.
544 *Zöller*, ZPO, Vor § 128 Rn. 11.
545 *Zöller*, ZPO, Vor § 114 Rn. 1.
546 *Zöller*, ZPO, § 118 Rn. 20.

verfolgten Zwecke mit den Erhebungszwecken identisch sind. Damit kommt der Grundsatz der Zweckbindung zum Ausdruck.[547]

Abweichungen von einem festgelegten Zweck stellen stets Eingriffe in das informationelle Selbstbestimmungsrecht dar. Sie sind nicht mehr von dem ursprünglich geltenden Zweck gedeckt, sondern stellen eine neue Datenverarbeitung dar.[548] Nach § 14 Abs. 2 BDSG und § 13 Abs. 2 LDSG sind sie nur zulässig, wenn der Betroffene eingewilligt hat oder die verantwortliche Stelle aufgrund einer gesetzlichen Ermächtigung dazu befugt ist.[549]

Nach den Vorgaben des § 14 Abs. 1 BDSG und des 13 Abs. 1 LDSG dürfen also Gerichte personenbezogene Daten im Grundsatz immer dann speichern und nutzen, wenn sie sie zur Erfüllung ihrer Aufgaben benötigen. Im Unterschied zu den Erhebungsregeln gibt es in den vorliegend zu untersuchenden Verfahrensordnungen jedoch keine speziellen Regelungen, die dem Gericht die Speicherung oder Nutzung gesondert gestatten würden.[550]

5.2.2.3 Das Übermitteln von personenbezogenen Daten

Das Übermitteln von Daten ist sowohl im BDSG in § 3 Abs. 4 Nr. 3 als auch im LDSG, dort in § 3 Abs. 2 Nr. 4 legaldefiniert. Danach ist unter einem Übermitteln das Bekanntgeben personenbezogener Daten an einen Dritten in der Weise zu verstehen, dass die Daten entweder an einen Dritten weitergegeben werden[551] oder der Dritte bereitgehaltene Daten einsieht oder abruft.[552] Unter dem Begriff Bekanntgeben wird die auf einem Handlungswillen beruhende Weitergabe von Daten verstanden. Die übermittelnde Stelle muss also wollen, dass der Dritte die Daten zur Kenntnis nimmt. In welcher Form die Bekanntgabe erfolgt, spielt dabei keine Rolle. Unter dem Begriff der Bekanntgabe fallen daher etwa briefliche oder mündliche Mitteilungen, das Gewähren von Einsicht in Aufzeichnungen oder öffentliche Bekanntmachungen im Internet. Ob der Empfänger die Information tatsächlich zur Kenntnis nimmt oder nehmen will, ist unbeachtlich.[553] Dritte sind alle Stellen oder Personen, die nicht betroffene Personen oder verantwortliche Stellen sind.[554] Die Weitergabe innerhalb der verantwortlichen Stellen stellt daher keine Datenübermittlung dar. Vielmehr liegt in diesem Fall eine Nutzung von Daten vor. Der Begriff der Weitergabe[555] entspricht dabei dem der Bekanntgabe.[556] Mit dem Begriff des Einsehens oder Abrufens bereitgehaltener Daten[557] ist gemeint, dass ein Dritter aktiv auf personenbezogene Daten der verantwortlichen Stelle zugreift. Gedacht ist an automatisierte Zugriffsverfahren im Rahmen von Online-Übermittlungen. Das BDSG und das LDSG unter-

[547] Vgl. hierzu auch Abschnitt 5.1.2.
[548] *Yildirim*, 2004, 180.
[549] *Yildirim*, 2004, 180.
[550] Für das Zivilverfahren vgl. *Werner*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 1427.
[551] Vgl. § 3 Abs. 4 Nr. 3a BDSG und § 3 Abs. 2 Nr. 4a LDSG.
[552] Vgl. § 3 Abs. 4 Nr. 3b BDSG und § 3 Abs. 2 Nr. 4b LDSG.
[553] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.5.2 zu § 3.
[554] *Hartig/Klink/Eiermann*, LDSG, Erl. 5.2 zu § 3.
[555] Vgl. § 3 Abs. 4 Nr. 3a BDSG und § 3 Abs. 2 Nr. 4a LDSG.
[556] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.5.5 zu § 3.
[557] Vgl. § 3 Abs. 4 Nr. 3b BDSG und § 3 Abs. 2 Nr. 4b LDSG.

scheiden im Hinblick auf die Zulässigkeit der Übermittlung danach, ob die personenbezogenen Daten an eine öffentliche Stelle[558] oder an eine nicht-öffentliche Stelle[559] übermittelt werden.

Übermittlung an öffentliche Stellen Die Übermittlung von personenbezogenen Daten an öffentliche Stellen ist gemäß § 15 BDSG und § 14 LDSG zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist oder wenn die Voraussetzungen vorliegen, die eine Nutzung zulassen würde. § 15 BDSG und 14 LDSG kommen insbesondere dann zur Anwendung, wenn es um die Einsichtgewährung von Akten im Rahmen einer Rechts- oder Amtshilfe geht. § 299 ZPO ist hier nämlich nicht einschlägig und auch Art. 35 GG stellt keine Rechtsgrundlage für eine Datenübermittlung an eine Behörde dar, so dass auf die allgemeinen Datenschutzregeln zurückgegriffen werden muss.

In der Justiz finden sich eine Vielzahl von bereichsspezifischen Übermittlungsvorschriften. Am bedeutsamsten sind die bereits dargestellten Regelungen in den §§ 12-22 EGGVG mitsamt der MiZi, die gerade dafür geschaffen wurden, dem informationellen Selbstbestimmungsrecht des Betroffenen nach den Vorgaben des Volkszählungsurteils Rechnung zu tragen. Von Bedeutung ist weiter auch § 116 Abs. 1 Abgabenordnung (AO), welche die Anzeige von Steuerstraftaten durch Gerichte und Behörden regelt. Da diese Vorschrift hinsichtlich der Datenübermittlung durch Gerichte und Behörden an die Finanzbehörden nicht nach der Schwere des Verdachts und der Schutzwürdigkeit der Geheimhaltungsinteressen der Verfahrensbeteiligten differenziert hatte, wurde sie zuweilen in ihrer alten Fassung für verfassungswidrig gehalten.[560] An dieser Auffassung dürfte sich heute wohl nichts geändert haben. Im Gegenteil: Früher musste für die Anzeige von Steuerstraftaten von Gerichten oder Behörden nämlich noch der Verdacht einer Straftat bestehen. In seiner heutigen Fassung müssen Tatsachen nur noch auf eine Steuerstraftat schließen lassen, d.h. ein Anfangsverdacht nach § 152 Abs. 2 Strafprozessordnung (StPO) ist nicht mehr erforderlich. Dennoch: Bei § 116 Abs. 1 a.F. dürfte es sich um eine verfassungsgemäße Norm gehandelt haben und auch § 116 AO in seiner jetzigen Fassung dürfte verfassungsgemäß sein. Adressat der Übermittlungen war und ist ein eingeschränkter Personenkreis (Gerichte, Behörden von Bund, Ländern und kommunalen Trägern der öffentlichen Verwaltung – seit 2006 nur noch solche, die nicht Finanzbehörden sind). Diese Stellen dürfen die Informationen nicht ohne weiteres mitteilen. Früher war ein Anfangsverdacht erforderlich und auch heute geht es der Formulierung „auf eine Straftat schließen lassen“ immerhin hervor, dass die Tatsachen zumindest mit einer gewissen Wahrscheinlichkeit für eine Straftat sprechen müssen.[561] Ob der Gesetzgeber durch die Neufassung, die als alleinigen Adressat der Mitteilungen von Steuerstraftaten nicht mehr die Finanzbehörden, sondern das Bundeszentralamt

[558] § 15 BDSG und § 14 LDSG.

[559] § 16 BDSG und § 16 LDSG.

[560] Wortlaut des § 116 AO in der Fassung bis 12.9.2006: „Gerichte und die Behörden von Bund, Ländern und kommunalen Trägern der öffentlichen Verwaltung haben Tatsachen, die sie dienstlich erfahren und die den Verdacht einer Steuerstraftat begründen, der Finanzbehörde mitzuteilen.“ Zur Verfassungswidrigkeit der Norm, vgl. *Vultejus*, ZRP 1996, 329; *Vultejus*, ZRP 1997, 386. Dagegen *Klos*, ZRP 1997, 50; *Bilsdorfer*, ZRP 1997, 137.

[561] BT-Drs. 16/814, 24.

für Steuern vorsieht, allerdings das Mitteilungsverfahren wesentlich effektiver gestaltet hat, mag bezweifelt werden. Dies ist jedoch eine andere Frage, die hier nicht vertieft behandelt werden soll.[562] Auch bei § 183 GVG (Übermittlung des Sitzungsprotokolls bei Begehung einer Straftat in der Sitzung) handelt es sich um eine spezielle Übermittlungsregelung im Bereich der Justiz. Die Vorschrift ist als Muss-Vorschrift ausgestaltet. So heißt es in § 183 GVG: „das Gericht hat den Tatbestand festzustellen“ und das Gericht „hat der zuständigen Behörde das darüber aufgenommene Sitzungsprotokoll mitzuteilen“. Die Vorschrift kommt jedoch entgegen dem etwas zu weit gefassten Wortlaut nur zur Anwendung, wenn gerade die Protokollierung eines strafrechtlichen Geschehens zur Beweissicherung erforderlich ist. Klassische Fälle hierfür sind etwa in der Sitzung begangene Beleidigungen gemäß § 185 StGB oder Körperverletzungen nach §§ 223 ff. StGB. Nicht hierunter werden jedoch Aussagedelikte nach §§ 153 ff. StGB oder Prozessbetrügereien nach §§ 263 ff. StGB fallen. Denn der Inhalt der Aussagedelikte ist gemäß § 160 Abs. 3 Nr. 4 ZPO ohnehin im Protokoll festzuhalten und der Tatsachenstoff ergibt sich bereits aus den Akten. Bei diesen Delikten wird regelmäßig keine Verpflichtung des Gerichts nach § 183 GVG zu einer gesonderten Protokollierung zwecks Beweissicherung bestehen. In diesen Fällen steht die Anzeige des Gerichts in seinem Ermessen.[563]

Übermittlung an nicht-öffentliche Stellen § 16 BDSG und § 16 LDSG bestimmen, unter welchen Voraussetzungen eine öffentliche Stelle Daten an Private übermitteln darf.[564] In diesem Zusammenhang sind vor allem die Vorschriften des § 16 Abs. 1 Nr. 2 BDSG und des § 16 Abs. 1 Nr. 3 LDSG von Bedeutung, wonach personenbezogene Daten an nicht-öffentliche Stellen übermittelt werden dürfen, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse (so die Regelung im BDSG) oder ein rechtliches Interesse (so die Regelung im LDSG) an der Kenntnis der zu übermittelnden Daten glaubhaft dargelegt hat. Bei telefonischen Auskünften an Dritte sind an eine solche Glaubhaftmachung besonders strenge Anforderungen zu stellen.[565] § 16 Abs. 4 BDSG und § 16 Abs. 4 LDSG verpflichten den privaten Datenempfänger dazu, die Daten nur zu dem Zweck zu übermitteln, zu dem sie ihm selbst übermittelt wurden. Damit kommt wiederum der oben genannte Zweckbindungsgrundsatz zum Ausdruck. Die öffentliche Stelle kann die Einhaltung der Zweckbindung durch Auflagen sichern. Eine spezialgesetzliche Norm findet sich diesbezüglich etwa in § 82 Abs. 1 Grundbuchverfügung (GBV). Danach ist der abrufberechtigten Person beim automatisierten Abrufverfahren zur Auflage zu machen, dass das Codezeichen nur von der Leitung und berechtigten Mitarbeitern verwendet werden

[562] Vgl. hierzu *Weyand*, Information StW 2007, 397. Zur Fragen der Strafbarkeit im Zusammenhang mit der Norm, vgl. *Bülle*, NStZ 2009, 57. Speziell zur mangelnden Bekanntheit der Vorschrift *Löwe-Krahl*, PStR 2005, 235.

[563] *Nierwetberg*, NJW 1996, 432.

[564] Die Vorschrift regelt nicht, ob Private ihrerseits die Daten auch erheben dürfen. Diese Frage ist für den Fall der geschäftsmäßigen Datenerhebung in § 28 BDSG geregelt. Liegt keine geschäftsmäßige Datenerhebung vor, so ergibt sich die Zulässigkeit der Datenerhebung aus Art. 5 GG bzw. aus Art. 2 GG.

[565] Vgl. hierzu etwa *LfD Bayern*, 17. Tätigkeitsbericht, Tz. 7.6.1.1. Hier hatte eine Rechtspflegerin einem Dritten, der sich als neuer Eigentümer eines versteigerten Grundstücks ausgab, am Telefon mitgeteilt, wie hoch sich der Auszahlungsbetrag, welcher dem Schuldner als überschießender Betrag ausbezahlt wurde, beläuft. Hier wären weitere Anforderungen an eine Glaubhaftmachung erforderlich gewesen.

darf; ein Wechsel der Mitarbeiter ist mitzuteilen. Außerdem muss sich die abrufberechtigte Stelle dazu verpflichten, das Codezeichen sicher aufzubewahren.

Vorschriften, die die Übermittlung von personenbezogenen Daten durch Gerichte an Private vorsehen, sind zahlreich. Hierzu gehören etwa die Regelungen über die Akteneinsicht nach § 299 ZPO, § 760 ZPO, § 13 FamFG oder § 42 ZVG oder diejenigen, die die Einsicht in öffentliche Register regeln, wie zum Beispiel § 12 GBO, § 9 HGB oder § 915b ZPO. Übermittlungsregelungen stellen des Weiteren die Vorschriften über die Bekanntmachungen von gerichtlichen Entscheidungen nach §§ 187, 948, 950, 956, 1014, 1017 Abs. 2, 1020 und 1022 Abs. 1 ZPO sowie die nicht anonymisierten Veröffentlichungen von Gerichtsentscheidungen oder Auskünfte des Gerichts an die Presse dar.[566] Auch § 36 Abs. 2 BRAO ist eine derartige Regelung.[567]

5.3 Anforderungen an die Datensicherheit in der elektronischen Justiz

Datenschutzrechtliche Maßnahmen zielen darauf ab, die Betroffenen vor den Folgen einer unberechtigten Verarbeitung ihrer personenbezogenen Daten zu schützen. Demgegenüber hat die Datensicherheit zum Ziel, Daten und Datenverarbeitungsprozesse gegen den Zugriff Unberechtigter zu schützen.[568] Datenschutz und Datensicherheit ergänzen einander und weisen eine bedeutende Schnittmenge auf. Für den Datenschutz ist die Datensicherheit ein Werkzeug dafür, Datenschutzziele zu erreichen. Umgekehrt betrachtet die Datensicherheit den Datenschutz als eine wesentliche Quelle für die Anforderungen, die sie umzusetzen hat.[569] Dabei bilden die technisch-organisatorischen Maßnahmen in § 9 BDSG und in § 9 LDSG die „Teilmenge, die dem Schutz des informationellen Selbstbestimmungsrechts dient“.[570] Wie sich aus § 9 Satz 2 BDSG und § 9 Abs. 1 Satz 2 LDSG ergibt, sind technisch-organisatorische Maßnahmen unter dem Gesichtspunkt der Verhältnismäßigkeit zu treffen. Sie sind nur dann erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Dies macht eine Abwägung erforderlich, die auf der Grundlage einer Bedrohungs- und Risikoanalyse erfolgt.[571] Die technisch-organisatorischen Anforderungen gelten nicht nur für die automatisierte Datenverarbeitung, sondern auch für die herkömmliche Datenverarbeitung in Akten.[572] Die Anlagen zu § 9 Satz 1 BDSG und § 9 Abs. 2 LDSG enthalten jedoch die nachfol-

[566] Für den Umgang von personenbezogenen Daten von Ermittlungsbehörden an die Presse vgl. *DSB-Konferenz*, 9./10.11.1995.

[567] Vgl. hierzu etwa *LfD Baden-Württemberg*, 19. Tätigkeitsbericht, Tz. 2.2: Ein Landgericht hatte eine Klageschrift gegen einen Anwalt aus Anwaltshaftung der Rechtsanwaltskammer mitgeteilt. Die Voraussetzungen des § 36a BRAO a.F. lagen jedoch nicht vor, da in dem vorliegenden Fall berufsrechtliche Pflichtverletzungen ersichtlich nicht einschlägig waren.

[568] *Ernestus*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 270.

[569] *Hartig/Klink/Eiermann*, LDSG, Erl. 1.1 zu § 9.

[570] *Hartig/Klink/Eiermann*, LDSG, Erl. 1.1 zu § 9.

[571] *Roßnagel/Schnabel*, NJW 2008, 3538.

[572] Vgl. hierzu § 9 Abs. 1 BDSG und § 9 Abs. 4 LDSG.

gend aufgeführten verschiedenen Gebote, die nur bei einer automatisierten Datenverarbeitung zu erfüllen sind.

Nach dem Urteil des Bundesverfassungsgerichts zum neuen IT-Grundrecht kommt den Datensicherungsmaßnahmen ein höherer Stellenwert zu als bisher. Datensicherungsmaßnahmen sind nun verhältnismäßig, die es früher vielleicht nicht waren.[573] Die Notwendigkeit angemessener und effektiver Maßnahmen darf dabei auch vor dem Hintergrund der Sensibilität der personenbezogenen Daten, die in der elektronischen Justiz verarbeitet werden, nicht unterschätzt werden.

5.3.1 Zutrittskontrolle

Ziel der Zutrittskontrolle[574] ist es zu verhindern, dass unbefugte Personen die Möglichkeit irgendeiner Bedienung der Datenverarbeitungsanlagen bekommen. Der Begriff des Zutritts erfasst dabei ausschließlich die räumliche Annäherung an eine Datenverarbeitungsanlage. Als Maßnahmen kommen zum Beispiel in Betracht allgemeine Sicherung der Räume während und nach der Dienstzeit, Zutrittsberechtigungsregelungen für unterschiedliche Bereiche oder besondere Zutrittssicherungen für Räume, in denen sich Datenverarbeitungsanlagen befinden.[575] IT wird heute in den Gerichten sowohl in den Geschäftsstellen als auch in den Büros der Richter eingesetzt. Im Rahmen der Zutrittskontrolle ist es daher erforderlich, dass diese Zimmer verschlossen sind. Über einen Schlüssel sollten für die Räumlichkeiten der Geschäftsstellen nur die dort arbeitenden Personen, deren Vertreter sowie der für diese Geschäftsstelle zuständige Richter verfügen. Einen Schlüssel für das Richterzimmer sollten neben dem dort arbeitenden Richter nur der zuständige Geschäftsstellenbeamte und der jeweilige Richtervertreter erhalten.

5.3.2 Zugangskontrolle

Die Zugangskontrolle[576] besagt, dass alles Erforderliche getan werden muss, um zu verhindern, dass unbefugte Personen in Datenverarbeitungssysteme eindringen und dabei die Möglichkeit haben, personenbezogene Daten zur Kenntnis zu nehmen, sie zu ändern und zu löschen.[577] Als Maßnahmen der Zugangskontrolle kommen in Betracht Benutzerkennung, Festlegung der Benutzerberechtigungen, Benutzer-Identifikationsroutinen, Reduzierung der Benutzerzahl, Zuordnung einzelner Datenendgeräte, Vergabe und Sicherung von Benutzerpasswörtern, Passwortschutz, Dunkelschaltung des Bildschirms mit Passwortschutz oder Wechsel der Passwörter und Trennung von Bearbeitungs- und Publikumszonen.[578] In der Justiz stellen solche Anlagen ein besonderes Problem dar, die in Räumen stehen, die gerichtsexternen Besuchern zugänglich

[573] *Roßnagel/Schnabel*, NJW 2008, 3538.
[574] Nr. 1 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 1 LDSG.
[575] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.2 zu § 9.
[576] Nr. 2 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 2 LDSG.
[577] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.3 zu § 9.
[578] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.3 zu § 9.

sind. Dies sind insbesondere die Räumlichkeiten der Geschäftsstellen. Bezüglich dieser Anlagen sind erhöhte Anforderungen an eine Zugangskontrolle zu stellen.

5.3.3 Zugriffskontrolle

Der Zugriff in diesem Sinne[579] erfasst die Tätigkeit innerhalb des EDV-Systems durch einen grundsätzlichen Berechtigten außerhalb seiner Berechtigung.[580] Der Umfang des Zugangs ist dabei auf das für die Aufgabenerfüllung Erforderliche zu beschränken. Es kommen in Betracht: Berechtigungskonzept, Protokollierung schreibender und lesender Zugriffe, Zugriffsschutz auf der Benutzerebene (Benutzerkennung, Passwort), auf der Dateiebene (verwaltungsinterne und verwaltungsexterne Dateizugriffe) und auf der Zugriffsebene (Lesen, Schreiben, Löschen).[581] Der Zugriff auf Dateien in der Justiz hat sich dabei am Geschäftsverteilungsplan auszurichten. In diesem bestimmt das jeweilige Präsidium gemäß § 21e GVG die Besetzung der Spruchkörper, regelt die Vertretung und verteilt die Geschäfte. Zugriff auf die jeweiligen Verfahren sollten daher der bearbeitende Richter, der Vertreter und die zuständigen Geschäftsstellenbeamten haben. Es sollte zudem bedacht werden, dass Urteilsentwürfe und eigene Anmerkungen der Richter nicht für die Richterkollegen einsehbar sind.

5.3.4 Weitergabekontrolle

Die Weitergabekontrolle[582] umfasst die Übermittlungskontrolle und die Transportkontrolle.[583] Zur Übermittlungskontrolle gehören Maßnahmen, die gewährleisten, dass bei der Übertragung von personenbezogenen Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert, gelöscht oder entwendet werden können. Zur Übermittlung gehören vor allem das Versenden von elektronischer Post oder Datenübermittlungen im Wege des automatisierten Übermittlungsverfahrens.[584] Maßnahmen sind vor allem die Verschlüsselung personenbezogener Daten bei ihrer Übermittlung.[585] Unter einer Transportkontrolle ist die physische Weitergabe von Bändern, Platten oder Papieraufzeichnungen zu verstehen. Als Maßnahmen kommen etwa die Bestimmung der zum Transport bestimmten Personen oder der Versand von verschlossenen Behältern in Betracht.[586] Die Weitergabekontrolle spielt in der Justiz v.a. bei der Übermittlung von Schriftsätzen eine Rolle.[587]

[579] Nr. 3 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 3 LDSG.
[580] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.4 zu § 9.
[581] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.4 zu § 9.
[582] Nr. 4 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 4 LDSG.
[583] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.5 zu § 9.
[584] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.5 zu § 9.
[585] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.5 zu § 9.
[586] *Hartig/Klink/Eiermann*, LDSG, Erl. 3.5 zu § 9.
[587] Vgl. hierzu insbesondere Abschnitt 7.1.1.

5.3.5 Eingabekontrolle

Mit der Eingabekontrolle[588] soll gewährleistet werden, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.[589] Geeignete Maßnahmen sind vor allem automatisierte Aufzeichnungen.[590] Die Protokollierung rein lesender Zugriffe, d.h. von Zugriffen, die nicht mit einer Eingabe, Änderung oder Löschung von Daten verbunden sind, wird von der Eingabekontrolle dagegen nicht erfasst.[591] Die Eingabekontrolle ist im Falle der Einführung der elektronischen Akte in der Justiz besonders wichtig.

5.3.6 Auftragskontrolle

Zur Auftragskontrolle[592] gehören Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der auftraggebenden Stelle verarbeitet werden können. Die Verfahrensordnungen gestatten den ordentlichen Gerichten an verschiedenen Stellen eine Datenverarbeitung im Auftrag.[593] Die Gerichte müssen daher die genannten Maßnahmen und Vorkehrungen zur Auftragskontrolle ergreifen. Elemente einer Vertragsgestaltung im Rahmen einer Datenverarbeitung im Auftrag sind etwa möglichst genaue Bezeichnung des Gegenstandes des Vertrages, Umfang und Grenzen der übertragenen Tätigkeiten oder Weisungs- Prüfungs- und Kontrollrechte des Auftraggebers.[594]

5.3.7 Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle[595] dient in Umsetzung von Art. 17 der EG-Datenschutzrichtlinie dem Schutz personenbezogener Daten vor zufälliger und unrechtmäßiger Zerstörung und Verlust durch besondere Ereignisse. Neben der Vertraulichkeit, Integrität und Authentizität stellt die Verfügbarkeit von Systemen, Programmen und Daten ein Grundziel der informationstechnischen Sicherheit dar.[596] Von Bedeutung ist hierbei vor allem eine ordnungsgemäße Datensicherung, um die Wiederherstellung von Datenbeständen im Bedarfsfall zu gewährleisten.[597] In der Justiz ergeben sich bei den Maßnahmen der Verfügbarkeitskontrolle keine Besonderheiten.

---

588 Nr. 5 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 5 LDSG.
589 *Heibey*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 582.
590 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.6 zu § 9.
591 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.6 zu § 9.
592 Nr. 6 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 6 LDSG.
593 § 126 Abs. 3 GBO, § 802k Abs. 3 Satz 3 ZPO.
594 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.7 zu § 9.
595 Nr. 7 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 7 LDSG.
596 *Heibey*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 548.
597 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.8 zu § 9.

5.3.8 Zweckbindungskontrolle

Das Zweckbindungsgebot[598] beinhaltet ein grundsätzliches Trennungsgebot für die zu unterschiedlichen Zwecken erhobenen Daten. Die Zweckbindungskontrolle soll damit die materiellrechtlichen Bestimmungen zur Datennutzung technisch abbilden. Als Maßnahmen kommt vor allem eine physikalische Trennung der Datenbestände durch eine getrennte Speicherung, eine logische Trennung über ein Mandantenkonzept oder eine zweckbezogene Kennzeichnung der jeweiligen Daten in Betracht.[599] Bei den ordentlichen Gerichten werden eine Vielzahl von personenbezogenen Daten zu unterschiedlichen Zwecken erhoben. Die Daten in den einzelnen Verfahren müssen daher getrennt gespeichert werden.

5.3.9 Dokumentations- und Verarbeitungskontrolle

Die Dokumentations- und Verarbeitungskontrolle ist nur in § 9 Abs. 2 Nr. 9 und 10 LDSG enthalten, nicht aber im BDSG. Die Dokumentationskontrolle soll eine Prüfung ermöglichen, inwieweit eine ordnungsgemäße Nutzung der eingesetzten IT-Systeme erfolgt. Sie umfasst im Wesentlichen eine Übersicht der zugelassenen Benutzer und deren Zugriffsrechte, die Dokumentation der eingesetzten IT-Systeme und deren Systemkonfiguration.[600] Maßnahmen der Verarbeitungskontrolle zielen darauf ab, die einzelnen Datenverarbeitungsprozesse auch hinsichtlich der verarbeitungsberechtigten Personen oder Personengruppen unter Beachtung des Grundsatzes der Verhältnismäßigkeit überprüfen zu können.[601] Die Protokollierungspflicht erstreckt sich dabei auf alle Phasen der Datenverarbeitung. Anders als die Eingabekontrolle erfasst sie auch rein lesende Zugriffe auf personenbezogene Daten. Diesen Anforderungen haben die rheinland-pfälzischen Gerichte nachzukommen.

Mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften von 2009[602] hat der Gesetzgeber in der Anlage zu § 9 BDSG nach Satz 2 folgenden Satz eingefügt: „Eine Maßnahme nach Satz 2 Nr. 2-4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsmaßnahmen.“ Obgleich Verschlüsselungsverfahren bereits jetzt zu den technischen und organisatorischen Maßnahmen zur Zugangs-, Zugriffs- und Weitergabekontrolle gehören, wollte der Gesetzgeber mit dieser Formulierung die Bedeutung von Verschlüsselungsverfahren hervorheben. Verschlüsselungsverfahren würden in der Praxis noch nicht in nennenswertem Umfang eingesetzt werden. Deshalb sollen sie gesondert im Gesetz als geeignete Maßnahme erwähnt werden.[603] Die Formulierung „dem Stand der Technik entsprechende“ bringe zum Ausdruck, dass fortschrittliche Verfahren gemeint sind, sie sich in der Praxis bewährt haben.[604] Die Änderung ist als positiv zu bewerten. Durch sie wird der Stel-

598 Nr. 8 der Anlage zu § 9 Satz 1 BDSG und § 9 Abs. 2 Nr. 8 LDSG.
599 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.9 zu § 9.
600 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.10 zu § 9.
601 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.11 zu § 9.
602 BGBl. 2009 I, 2814.
603 BT-Drs. 16/13657, 23.
604 BT-Drs. 16/13657, 23.

lenwert von Datensicherungsmaßnahmen nochmals hervorgehoben, was angesichts des Urteils des Bundesverfassungsgerichts zum Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme auch erforderlich ist.[605]

5.4 Die Rechte des Betroffenen

5.4.1 Benachrichtigungs- und Auskunftsrechte

§ 19a BDSG und § 18 Abs. 1 LDSG sehen eine Pflicht für eine Benachrichtigung für den Fall vor, dass eine öffentliche Stelle Daten ohne Kenntnis des Betroffenen erhoben hat. Unter bestimmten Voraussetzungen kann die verantwortliche Stelle von der Benachrichtigung auch absehen, so insbesondere dann, wenn sie gemäß § 19a Abs. 2 Nr. 2 BDSG und § 18 Abs. 2 Satz 1 Nr. 3 LDSG einen unverhältnismäßigen Aufwand erfordern würde. Diese Regelung soll der Verwaltungsvereinfachung dienen und geht zurück auf Art. 11 Abs. 1 Satz 1 EG-Datenschutzrichtlinie.

§ 19 Abs. 1 BDSG und § 18 Abs. 3 LDSG geben dem Betroffenen auf seinen Antrag hin einen unentgeltlichen Anspruch auf Auskunft über die über ihn gespeicherten Daten.[606] Ihrem Wortlaut nach verlangen § 19 Abs. 1 BDSG und § 18 Abs. 3 LDSG, dass dem Betroffenen die zu seiner Person gespeicherten Daten mitzuteilen sind. Von diesem Anspruch sind einmal „harte“ Informationen wie Geburtsdatum, Adresse, Namensbeschreibung, Beurteilungsnote umfasst, zum anderen aber auch Wertungen, Vermutungen oder sonstige Hinweise, die in den Akten oder in einem Medium der automatisierten Datenverarbeitung gespeichert sind.[607] Ebenfalls ist die Herkunft der Daten[608] mitzuteilen sowie der Empfänger[609] und der Zweck der Speicherung[610].

Grundsätzlich muss der Betroffene sein Auskunftsverlangen nicht begründen. Wenn die Daten jedoch nur noch zur Erfüllung von Aufbewahrungspflichten vorgehalten werden oder wenn die Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, muss der Betroffene ein berechtigtes Interesse darlegen.[611] In bestimmten Fällen kann die verantwortliche Stelle die Auskunft auch verweigern.[612] § 19 Abs. 5 BDSG und § 18 Abs. 6 LDSG kann entnommen werden, dass die verantwortliche Stelle die Verweigerung grundsätzlich zu begründen hat. Im Fall der Verweigerung kann sich der Betroffene an den Bundesbeauf-

605 Vgl. hierzu auch Abschnitt 4.2.1.2.

606 *Simitis/Fuckner*, NJW 1990, 2713; *Knemeyer*, JZ 1992, 348; *Gallwas*, NJW 1992, 2785 sind der Ansicht, dass die Auskunft selbst aus dem Recht auf informationelle Selbstbestimmung herleitbar ist. Dies lehnen *Ehmann*, CR 1988, 575; *Gola/Schomerus*, BDSG, § 19 Rn. 2 ab.

607 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.4.1 zu § 18.

608 § 19 Abs. 1 Nr. 1 BDSG und § 18 Abs. 3 Nr. 1 LDSG.

609 § 19 Abs. 1 Nr. 2 BDSG und § 18 Abs. 3 Nr. 2 LDSG.

610 § 19 Abs. 1 Nr. 3 BDSG und § 18 Abs. 3 Nr. 3 LDSG.

611 § 19 Abs. 2 BDSG und § 18 Abs. 4 LDSG.

612 § 19 Abs. 3 BDSG und § 18 Abs. 5 LDSG.

tragten für den Datenschutz bzw. an den Landesbeauftragten für den Datenschutz wenden. Diesem hat die verantwortliche Stelle die Auskunft zu erteilen. Allerdings ist es ihm dann nicht gestattet, dem Betroffenen die Informationen zu erteilen. Vielmehr beschränken sich die Handlungsmöglichkeiten auf eine Mitteilung an den Betroffenen, dass die Verweigerung der Auskunft für rechtswidrig gehalten wird.[613]

In Rheinland-Pfalz gelten die genannten Rechte gemäß § 18 Abs. 8 LDSG jedoch gegenüber Gerichten und dem Rechnungshof nur dann, wenn diese in Verwaltungsangelegenheiten tätig werden.[614] Auch gegenüber den Staatsanwaltschaften können sie nur geltend gemacht werden, wenn diese strafvollstreckend tätig werden sowie in Gnadensachen. Das BDSG enthält keine derartige Einschränkung, so dass die Ansprüche auf Bundesebene auch dann gegenüber den Gerichten geltend gemacht werden können, wenn diese nicht in Verwaltungsangelegenheiten tätig sind.[615] In diesem Fall ist der Richter grundsätzlich selbst für die Auskunftserteilung zuständig.[616] Dieser wird jedoch genau zu prüfen haben, ob er den Auskunftsanspruch nicht nach § 19 Abs. 4 BDSG ablehnen kann.

Unabhängig von den allgemeinen Auskunftsansprüchen in den Datenschutzgesetzen gibt es wiederum spezialgesetzliche Auskunftsansprüche. So etwa in § 21 Abs. 1 EGGVG. Dieser Anspruch kann mit dem Antrag auf gerichtliche Entscheidung nach §§ 23 ff. EGGVG geltend gemacht werden. Zuständig für die Entscheidung sind nach § 25 Abs. 1 Satz 1 1. Alt. EGGVG die Zivilsenate der Oberlandesgerichte. Wie oben bereits erläutert,[617] kann ein Betroffener den Auskunftsanspruch insofern aber nur schwer ausüben, als dass er, wenn er am Verfahren beteiligt war, nach der derzeitigen Ausgestaltung des § 21 Abs. 2 EGGVG nicht über etwaige Datenübermittlungen unterrichtet wird. Ein weiterer speziell geregelter Auskunftsanspruch ist zum Beispiel auch in § 133 Abs. 5 Satz 2 GBO i.V.m. § 83 Abs. 2 Satz 2 GBV zu finden (Auskunft des Eigentümers über Protokolldaten).

5.4.2 Berichtigung

§ 20 Abs. 1 BDSG und § 19 Abs. 1 LDSG bestimmt, dass personenbezogene Daten zu berichtigen sind, wenn sie unrichtig sind. Unrichtig sind die Daten dann, wenn feststeht, dass sie unzutreffend sind, dass sie die Realität nicht zutreffend wiedergeben oder auf unzutreffenden Voraussetzungen gründen.[618] Auch Wertungen können unrichtig sein, wenn keine genügenden tatsächlichen Erkenntnisse vorhanden sind, um die gespeicherte wertende Information zu be-

613 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.11 zu § 18.
614 Zum Begriff der Verwaltungsangelegenheiten vgl. Abschnitt 6.1.2 und 6.2.2.
615 *Werner*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 1439.
616 *Werner*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 1439.
617 Vgl. hierzu Abschnitt 4.3.3.3.
618 *Hartig/Klink/Eiermann*, LDSG, Erl. 1.1 zu § 19.

gründen.[619] Unrichtige Daten sind bereits von Amts wegen zu berichtigen.[620] Im automatisierten Verfahren erfolgt die Berichtigung dadurch, dass die unrichtige Information gelöscht und durch die richtige ersetzt wird oder sie als unrichtig gekennzeichnet und die richtige Information hinzugefügt wird.[621] Sind unrichtige Daten in Akten gespeichert, ist eine Vernichtung der entsprechenden Aktenteile unzulässig. Die Berichtigung erfolgt vielmehr dadurch, dass kenntlich gemacht wird, zu welchem Zeitpunkt und aus welchem Grund sie unrichtig waren oder unrichtig geworden sind.[622]

Im Bereich der Rechtsprechung der Justiz dürfte der Berichtigungsanspruch nicht in Betracht kommen. Im Zivilverfahren liefern die Parteien dem Gericht den Tatsachenstoff. Oft werden die von den Parteien vorgetragenen Informationen streitig sein. Der Richter hat deshalb hierüber Beweis zu erheben. Um die Aufklärung eines Sachverhaltes geht es auch im Zwangsvollstreckungs- und Zwangsversteigerungsverfahren, dem Grundbuchverfahren, dem Insolvenzverfahren und dem Handelsgesetzbuch. Die Dokumentation in einer gerichtlichen Akte ist daher kein Beleg für die Richtigkeit oder Unrichtigkeit eines Sachverhalts, sondern – so wie bei einer Anwaltsakte – darüber, dass die Richtigkeit oder Unrichtigkeit behauptet wird.[623]

5.4.3 Löschung, Sperrung, Widerspruchsrecht

Das Löschen wird in § 3 Abs. 4 Satz 2 Nr. 5 BDSG und in § 3 Abs. 2 Satz 2 Nr. 6 LDSG definiert als das Unkenntlichmachen gespeicherter personenbezogener Daten.[624] Das Gesetz schreibt vor, dass personenbezogene Daten zu löschen sind, wenn ihre Speicherung unzulässig[625] oder ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.[626] Unzulässig ist eine Datenspeicherung, wenn sie nicht durch ein Gesetz oder die Einwilligung des Betroffenen gerechtfertigt ist.[627] Der Wegfall der Erforderlichkeit kann auf verschiedenen Gründen beruhen. In erster Linie entfällt er, wenn die Aufgabe erledigt ist.[628]

---

619 *Hartig/Klink/Eiermann*, LDSG, Erl. 1.1 zu § 19.

620 Dies geht aus dem Wortlaut „sind zu berichtigen, wenn sie unrichtig sind“ in § 20 Abs. 1 BDSG und § 19 Abs. 1 LDSG hervor. Diese Handlung der Behörde ist dann kein Verwaltungsakt, sondern ein Realakt, vgl. hierzu BVerfG, MDR 1992, 419.

621 *Auernhammer*, BDSG, § 20 Rn. 5.

622 Insofern ist der Wortlaut der rheinland-pfälzischen Regelung, es sei ausreichend die Berichtigung zu vermerken missverständlich, vgl. hierzu *Hartig/Klink/Eiermann*, LDSG, Erl. 1.3 zu § 19.

623 Vgl. hierzu auch Abschnitt 4.3.1.2.

624 Auch ist die Abgabe an ein zuständiges Archiv als Löschung im Sinne der Datenschutzgesetze anzusehen.

625 § 20 Abs. 2 Nr. 1 BDSG und § 19 Abs. 2 Nr. 1 LDSG.

626 § 20 Abs. 2 Nr. 2 BDSG und § 19 Abs. 2 Nr. 2 LDSG.

627 *Yildirim*, 2004, 189.

628 Durch die Formulierung in § 19 Abs. 2 Nr. 2 2. Hs. LDSG, dass sich die Erforderlichkeit nach den für die verantwortliche Stellen getroffenen allgemeinen Regelungen über die Aufbewahrung von personenbezogenen Daten handelt, wollte der Gesetzgeber klarstellen, dass nicht nur Gesetze bei der Beurteilung der Erforderlichkeit eine Rolle spielen, sondern auch Verwaltungsvorschriften oder Dienstanweisungen. Der Zeitpunkt, wann die Verwaltung ihre Dokumentation erfüllt hat, ist grundsätzlich nicht eindeutig nach

Wie lange beispielsweise Akten an rheinland-pfälzischen Gerichten aufbewahrt werden dürfen, ergibt sich aus dem LSchrAG[629] in Verbindung mit der dazu ergangenen Verordnung.[630] Für die hier interessierenden Bereiche sind der Abschnitt I B[631] und der Abschnitt I D[632] von Bedeutung. Nach Abschnitt I B sind etwa Akten über ein allgemeines Zivilverfahren fünf Jahre lang aufzubewahren.[633] Die fünfjährige Aufbewahrungsfrist gilt auch für Akten über ein Zwangsvollstreckungsverfahren.[634] Für den Bereich der Zwangsversteigerung[635] wird bei der Aufbewahrungsfrist danach unterschieden, ob der Zuschlag erteilt wird oder nicht. Wird er erteilt, beträgt die Aufbewahrungsdauer fünf Jahre. Wird er nicht erteilt, sind die Akten zwei Jahre lang aufzubewahren. Abschnitt I D bestimmt, dass Grundbücher – wie sich im Übrigen auch aus § 10 GBO ergibt – dauernd aufzubewahren sind. Dies gilt auch für das dazugehörige Schriftgut an Akten oder Urkunden. Eine Ausnahme gilt nur für Sonderhefte mit den Schriften von vorübergehender Bedeutung (diese sind zwei Jahre lang aufzubewahren) und für Sammelakten mit den Anträgen auf Erteilung von Grundbuchabschriften. Die Aufbewahrungsfrist beträgt hier jeweils sechs Monate. Dauernd aufzubewahren sind auch Handelsregister. Die Aufbewahrungsdauer von Handelsregisterakten und für die zum Handelsregister einzureichenden Jahresabschlüsse und andere Unterlagen der Rechnungslegung beträgt dagegen zehn Jahre.

Alle Unterlagen, die zur Aufgabenerfüllung nicht mehr benötigt werden, sind nach § 2 Abs. 1 Bundesarchivgesetz (BArchG)[636] und nach § 7 Landesarchivgesetz (LArchG)[637] dem Archiv anzubieten.[638] Die Archive übernehmen Unterlagen von bleibendem Wert. Die Entscheidung, ob die Übernahmevoraussetzungen vorliegen, treffen die Archive innerhalb von sechs Monaten nach der Anbietung. Unterlagen, die nicht durch ein Archiv übernommen werden, müssen unter Beachtung der gesetzlichen Bestimmungen gelöscht werden und wenn dies zulässig ist, gesperrt werden.

---

objektiv feststehenden Kriterien berechenbar, er ist vielmehr unter einer Reihe von jeweils bereichsspezifischen Gesichtspunkten festzulegen.

629 Vgl. hierzu Abschnitt 4.3.3.4.

630 Landesverordnung zur Ausführung des Landesgesetzes zur Aufbewahrung von Schriftgut der Justiz, GVBl. 2008, 238.

631 Zivilprozess-, Insolvenz-, Konkurs- und Vergleichssachen.

632 Freiwillige Gerichtsbarkeit.

633 C-Sachen.

634 M-Sachen. Allerdings wird in der Verordnung darauf hingewiesen, dass § 915a ZPO besondere Löschungsregelungen für Eintragungen in einem Schuldnerverzeichnis vorsieht. § 915a ZPO geht damit den Bestimmungen der Verordnung zur Aufbewahrung von Schriftgut der Justiz vor.

635 K-Sachen.

636 Für das Schriftgut des Bundesgerichtshofes.

637 Für das Schriftgut der Oberlandesgerichte, der Landgerichte und der Amtsgerichte.

638 Der Begriff der Archivierung ist von dem der Aufbewahrung zu unterscheiden. Die Aufbewahrung umfasst jede Form der Erhaltung eines Dokuments unabhängig davon ob eine Speicherung im Datenmanagementsystem oder im Datenarchiv erfolgt, ob der Gesamtvorgang, zu dem das einzelne Dokument gehört, in der Bearbeitung abgeschlossen ist oder nicht oder ob eine bestimmte Aufbewahrungsfrist festgelegt ist. Von Archivgut wird dann gesprochen, wenn das Schriftgut bei der zuständigen Behörde ausgesondert, vom Archiv als archivwürdig eingestuft worden ist und ewig verwahrt wird. Vgl. hierzu *Roßnagel/Fischer-Dieskau/Jandt*, 2007, 9.

Nach § 3 Abs. 4 Satz 2 Nr. 4 BDSG und § 3 Abs. 2 Satz 2 Nr. 5 LDSG ist das Sperren das Kennzeichnen personenbezogener Daten, um ihre weitere Verwendung einzuschränken. In erster Linie sind Daten dann zu sperren, wenn die Richtigkeit der Daten von dem Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.[639] Der Anspruch auf Sperrung ist schon dann begründet, wenn der Betroffene die Richtigkeit der gespeicherten Daten ohne nähere Begründung bestreitet und die verantwortliche Stelle die Richtigkeit der Daten nicht beweisen kann. Aufgrund der oben genannten Überlegungen zum Berichtigungsanspruch dürfte der Anspruch auf Sperrung im Bereich der Rechtsprechung jedoch keine große Rolle spielen.

§ 20 Abs. 5 BDSG und § 19 Abs. 4 LDSG wurden in Anpassung an die EG-Datenschutzrichtlinie aufgenommen.[640] Die beiden Vorschriften stimmen wörtlich überein. Sie geben dem Betroffenen das Recht, einer – auch rechtmäßigen – automatisierten Verarbeitung seiner Daten zu widersprechen.[641] Der Betroffene hat den Widerspruch bei der verantwortlichen Stelle zu erheben. Der Widerspruch ist dabei an keine Form gebunden; auch ein mündlicher Widerspruch ist daher ausreichend. Auch kann der Betroffene die Reichweite seines Widerspruches selbst bestimmen, d.h. er kann den Widerspruch beispielsweise auf bestimmte Daten oder Datenarten und/oder Teile der Verarbeitung, etwa auf die Übermittlung an bestimmte Empfänger, beschränken. Wenn der Betroffene der automatisierten Verarbeitung seiner Daten widerspricht, hat die verantwortliche Stelle zu prüfen, ob das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an der Verarbeitung überwiegt.[642] Dabei ist eine Interessenabwägung vorzunehmen, die die Konsequenzen einer Erhebung, Verarbeitung oder Nutzung für den Betroffenen etwaigen öffentlichen Interessen oder privaten Interessen Dritter gegenüberstellt. Nach der Gesetzesbegründung ist ein derartiges Interesse nur im Einzelfall gegeben, wenn aus der weiteren Verarbeitung der personenbezogenen Daten eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann.[643] Aus diesem Grund wird daher auch in der elektronischen Justiz ein Widerspruch gegen die automatisierte Datenverarbeitung in der Regel erfolglos bleiben.

Wenn die verantwortliche Stelle Daten berichtigt, gelöscht oder gesperrt hat, so hat sie dies den Stellen[644] mitzuteilen, an welche sie die Daten übermittelt hat.[645] Hiermit wollte der Gesetzgeber sicherstellen, dass die schutzwürdigen Interessen der Betroffenen auch bei der empfangenden Stelle angemessen berücksichtigt werden. Eine Unterrichtung kann jedoch dann unterbleiben, wenn der Aufwand zu groß wäre und im Verhältnis dazu die Belange des Betroffenen zurückstehen können.[646]

---

639 § 20 Abs. 4 BDSG und § 19 Abs. 3 Satz 1 Nr. 1 LDSG.
640 Vgl. Art. 14a DSRL.
641 *Gola*, DuD 2001, 278, speziell zur Einordnung des Widerspruchsrechts *Schomerus*, ZRP 1981, 291.
642 *Yildirim*, 2004, 191.
643 BT-Drs. 14/4329, 41.
644 Dies können sowohl öffentliche als auch private Stellen sein.
645 § 20 Abs. 8 BDSG und § 19 Abs. 6 LDSG.
646 Dies ist nicht der Fall, wenn die Information diskriminierende Wirkung hat.

5.5 Zusammenfassung

Die Anforderungen des Datenschutzes an die elektronische Justiz ergeben sich nicht allein aus den Verfahrensordnungen. Vielmehr wirken die Verfahrensordnungen und das Datenschutzrecht zusammen. In den Verfahrensordnungen finden sich vor allem spezielle Erhebungsvorschriften. Hier tritt das Spannungsverhältnis der Verfahrensordnungen zum Datenschutz besonders zu Tage. Auch die allgemeinen datenschutzrechtlichen Übermittlungsregelungen spielen eher eine untergeordnete Rolle. Denn auch hier finden viele Spezialregelungen Anwendung. Diese sind oft älter als die Datenschutzgesetze und haben ganz unterschiedliche Zielrichtungen – zum Beispiel die Gewährung des rechtlichen Gehörs oder die Verlautbarung von wichtigen gerichtlichen Entscheidungen für die Allgemeinheit. Für das Speichern und das Nutzen von Daten gibt es dagegen keine speziellen Vorschriften. Hier gelten die allgemeinen Vorschriften.

Aufgrund der Entscheidung des Bundesverfassungsgerichts von 2008 werden die Anforderungen an die Datensicherheit steigen. Da der Datensicherheit ein höherer Stellenwert zukommt, kommen auf die durch § 9 BDSG und § 9 LDSG verpflichteten Gerichte erhöhte Anforderungen zu. Die Notwendigkeit angemessener und effektiver Maßnahmen darf dabei gerade auch vor dem Hintergrund der Sensibilität der personenbezogenen Daten, die in der elektronischen Justiz verarbeitet werden, nicht unterschätzt werden.

Kapitel 6

Datenschutzkontrolle

Der Betroffene ist nicht allein in der Lage, im Rahmen individueller Eigenkontrolle seine Rechte wahrzunehmen. Daher bedarf es der Beteiligung unabhängiger Datenschutzkontrolleinrichtungen, die den Betroffenen bei der Durchsetzung seiner Rechte behilflich sind und die die Einhaltung von Datenschutzbestimmungen beobachten und überwachen.[647] Vor diesem Hintergrund widmet sich dieses Kapitel der Datenschutzkontrolle. Zunächst werden die Entwicklung, die Rechtsstellung und die Befugnisse des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und des Landesbeauftragten für den Datenschutz dargestellt. Sodann wird geprüft, inwieweit diese die Einhaltung von Datenschutzbestimmungen bei den Gerichten, den Rechtsanwälten und den Notaren kontrollieren dürfen. Im Anschluss daran wird auf den gerichtlichen Datenschutzbeauftragten eingegangen.

6.1 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

6.1.1 Entwicklung, Rechtsstellung und Befugnisse

Das Amt des Bundesbeauftragten für den Datenschutz wurde mit dem ersten Bundesdatenschutzgesetz vom 27.1.1977 eingeführt.[648] Obgleich man sich schon von Beginn an einig war, dass ein etwaiges Bundesdatenschutzgesetz auch eine angemessene Kontrolle und Überwachung seiner Datenschutzregeln vorsehen sollte, war zunächst unklar, wie man diese ausgestalten sollte.[649] Zum Teil wurde vorgeschlagen, nach dem Vorbild des Hessischen Datenschutzgesetzes einen Datenschutzbeauftragten vorzusehen oder einen unabhängigen Ausschuss mit der Kontrolle zu beauftragen.[650] Als weitere Möglichkeiten wurden die Einrichtung einer zentralen Kontrollbehörde oder/und die Einrichtung einer besonderen Gerichtsbarkeit für den Daten-

[647] *Heil*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 749.
[648] BGBl. 1977 I, 207.
[649] BT-Drs. 7/1027, 18.
[650] BT-Drs. 7/1027, 18.

schutz vorgeschlagen.[651] Der Regierungsentwurf von 1973[652] entschied sich jedoch für keine der genannten Möglichkeiten. Vielmehr hielt er „auf der Grundlage des Prinzips der Selbstverantwortung ein System abgestufter Selbstkontrolle“ für ausreichend. Begründet wurde dies damit, dass für den Bereich der öffentlichen Verwaltung der Grundsatz der Rechtmäßigkeit des Verwaltungshandelns gelte und die Einhaltung dieses Grundsatzes durch zahlreiche Kontrollinstanzen überwacht werde (Parlament, Minister, unabhängige Rechnungshöfe).[653] Dies wurde vom Innenausschuss jedoch nicht mitgetragen. Dieser war sich darin einig, dass es auch zur Kontrolle der Einhaltung der für Behörden und sonstige Stellen geltenden datenschutzrechtlichen Bestimmungen einer unabhängigen Instanz bedürfe.[654] Schließlich entschied man sich für das Modell des Hessischen Datenschutzbeauftragten, womit man auch Forderungen aus der Wissenschaft und der Öffentlichkeit nachgekommen ist.[655]

Der Bundesdatenschutzbeauftragte überwacht die Einhaltung des Datenschutzes im öffentlichen Bereich des Bundes. Zur Überwachung des Datenschutzes in der Länderverwaltung oder gar im nicht-öffentlichen Bereich ist er nicht befugt.[656] Seit dem 1.1.2006 führt der Bundesbeauftragte für den Datenschutz die Bezeichnung Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Nach §§ 12 und 15 des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes (IFG)[657] ist ihm nämlich ab diesem Datum zusätzlich die Funktion eines Ombudsmanns in diesem Bereich übertragen worden. Der Bundesbeauftragte für den Datenschutz ist weder Beamter noch Angestellter. Er steht gemäß § 22 Abs. 4 Satz 1 BDSG in einem öffentlich-rechtlichen Amtsverhältnis eigener Art. Er unterliegt nach § 22 Abs. 4 Satz 3 BDSG der Rechtsaufsicht der Bundesregierung und gemäß § 22 Abs. 5 Satz 2 BDSG der Dienstaufsicht des Bundesministeriums des Innern. Bei der Ausübung seines Amtes ist er jedoch entsprechend § 22 Abs. 4 Satz 2 BDSG wie ein Richter unabhängig und nur dem Gesetz unterworfen.[658]

Die Aufgaben des Bundesbeauftragten für den Datenschutz können in drei Gruppen unterteilt werden. Einmal hat er nach § 24 BDSG die Aufgaben als Kontrollorgan der Exekutive bzw. – in beschränktem Umfang – auch der Judikative und nach § 21 BDSG die Aufgaben eines Ombudsmanns. Zum anderen hat er entsprechend § 26 Abs. 3, Abs. 2 Satz 1 BDSG verschiedene Beratungsfunktionen gegenüber Exekutive und Legislative wahrzunehmen.[659] In den hier interessierenden Bereichen kommt der zuletzt genannten Funktion sicherlich die größte Bedeutung zu. Bei der ZPO, dem ZVG, der InsO, der GBO und dem HGB handelt es sich

651 BT-Drs. 7/1027, 18.

652 BT-Drs. 7/1027, 18.

653 Für den nicht-öffentlichen Bereich sah der Entwurf dagegen die Bestellung eines der Unternehmensleitung unmittelbar verantwortlichen Datenschutzbeauftragten und örtliche Kontrollen vor, vgl. BT-Drs. 7/1027, 18.

654 BT-Drs. 7/5277, 5.

655 Vgl. hierzu ausführlich *Heil*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 747.

656 *Schaffland/ Wiltfang*, BDSG, § 22 Rn. 2.

657 BGBl. 2005 I, 2722.

658 Zu den Einzelheiten der Rechtsstellung des Bundesdatenschutzbeauftragten wird verwiesen auf *Schaffland/ Wiltfang*, BDSG, § 22 Rn. 5 ff.

659 Hierzu etwa *Werner*, RDV 1996, 234.

um Bundesrecht. Der Bundesdatenschutzbeauftragte hat daher Gesetzesänderungen in diesem Bereich zu beobachten und muss auf Anforderung von Regierung oder Parlament zu datenschutzrechtlichen Fragestellungen Auskunft geben. Seine Kontrollaufgaben und Aufgaben als Ombudsmann treten demgegenüber nicht zuletzt aufgrund seiner beschränkten Kompetenz in diesem Bereich bei den Gerichten in den Hintergrund.[660]

6.1.2 Die Kontrollkompetenz beim Bundesgerichtshof

Nach § 21 Satz 2 BDSG unterliegen die Bundesgerichte der Kontrolle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nur, soweit sie in Verwaltungsangelegenheiten tätig werden. § 21 Satz 2 BDSG korrespondiert insofern mit § 24 Abs. 3 BDSG, wonach bei Bundesgerichten nur die „unmittelbar der Rechtsprechung dienende Tätigkeit der Richter“ von der Kontrolle ausgenommen ist.[661] Der Begriff der Gerichtsverwaltung findet sich etwa im Deutschen Richtergesetz (DRiG) in den §§ 4 Abs. 2 Nr. 1, 42.[662] Die Gerichtsverwaltung ist darauf gerichtet, die finanziellen, organisatorischen und personellen Voraussetzungen für die Tätigkeit der Rechtspflege zu schaffen und zu unterhalten. Zur Gerichtsverwaltung zählen daher etwa die Personalverwaltung, die Bewirtschaftung der Haushaltsmittel, Beschaffung sowie Liegenschaftsverwaltung, die Bearbeitung von Eingaben und Amtshilfeersuchen, die Wahrnehmung der Belange des Staates als Verwaltungsträger und Rechtsperson nach außen, die Ausübung von Dienstaufsicht, die Erstellung von Statistiken und die Ausbildung des juristischen Nachwuchses.[663] Reine Rechtsprechungstätigkeit unterliegt dagegen nicht der Kontrolle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Zu reinen Rechtsprechungsangelegenheiten gehören alle Tätigkeiten, die von der richterlichen Unabhängigkeit umfasst sind, also etwa Termins- und Fristbestimmungen, Ladungen, Sitzungen, Einzelrichterbestellung, prozessleitende Maßnahmen, Durchführung von Beweisaufnahmen und Berichtigungen von Entscheidungen.[664] Eine Kontrolle des Bundesbeauftragten in diesem Bereich wäre nach Art. 92, 97 GG, 4 Abs. 1, 25 DRiG verfassungsrechtlich unzulässig. Auf Länderebene hat sich gezeigt, dass Unsicherheiten dahingehend bestehen, ob Tätigkeiten, die zwar keine Spruchtätigkeit darstellen, diese aber vorbereiten und unterstützen, Verwaltungstätigkeiten darstellen oder nicht. Da diese Frage bislang nur bei den Landesdatenschutzbeauftragten eine Rolle gespielt hat, soll sie erst dort behandelt werden.[665]

---

660 Vgl. hierzu den folgenden Abschnitt.
661 *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 21 Rn. 21.
662 Zu diesem Begriff vgl. auch *Zöller*, ZPO, Einl. GVG Rn. 10.
663 *Hartig/Klink/Eiermann*, LDSG, Erl. 3.18 zu § 18.
664 *Wullweber*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 159.
665 Vgl. hierzu Abschnitt 6.2.2.

6.2 Der Landesbeauftragte für den Datenschutz

6.2.1 Entwicklung, Rechtsstellung und Befugnisse

Bereits vor dem Amt des Bundesdatenschutzbeauftragten gab es in Rheinland-Pfalz einen Ausschuss für Datenschutz. Dieser wurde mit dem Gesetz gegen missbräuchliche Datennutzung vom 24.1.1974[666] eingeführt. Bei diesem Ausschuss handelte es sich um ein weisungsfreies Kollegialorgan, dem drei Abgeordnete des Landtags sowie je ein vom Landtag und von der Landesregierung entsandter Beamter angehörte.[667] Mit dem Landesgesetz zum Schutz des Bürgers bei der Verarbeitung personenbezogener Daten vom 21.12.1978,[668] welches in Reaktion auf das Bundesdatenschutzgesetz vom 27.1.1977 verabschiedet wurde, wurde der Ausschuss in Datenschutzkommission umbenannt. Damit sollte verdeutlicht werden, dass es sich bei diesem Gremium nicht um einen Parlamentsausschuss handelte.[669] Mit der Änderung des Landesdatenschutzgesetzes von 1991 trat ein erneuter Wechsel ein. Die Aufgabe der Datenschutzkontrolle wurde dem Landesbeauftragten für den Datenschutz übertragen.[670] Durch diese Änderung wollte der Gesetzgeber die Unabhängigkeit der Datenschutzkontrolle hervorheben, die das Bundesverfassungsgericht in seinem Volkszählungsurteil gefordert hatte.[671] Nach § 24 Abs. 1 Satz 1 LDSG kontrolliert der Landesbeauftragte für den Datenschutz die Einhaltung des Datenschutzes im öffentlichen Bereich. Mit dem Zweiten Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 17.6.2008[672] wurde ihm mit Wirkung vom 1.10.2008 auch die Aufsicht im nicht-öffentlichen Bereich gemäß § 24 Abs. 1 Satz 2 LDSG übertragen. Davor hatte diese Aufgabe die Aufsichts- und Dienstleistungsdirektion (ADD) in Trier wahrgenommen.[673]

Die Rechtsstellung des Landesbeauftragten für den Datenschutz gleicht dem des Bundesdatenschutzbeauftragten. Auch er wird nach § 23 Abs. 1 Satz 1 LDSG in ein öffentlich-rechtliches Amtsverhältnis berufen. Im nicht-öffentlichen Bereich untersteht er nach § 24 Abs. 1 Satz 2 LDSG der Rechtsaufsicht der Landesregierung.[674] Die Dienstaufsicht über ihn führt gemäß § 23 Abs. 1 Satz 2 LDSG der Präsident des Landtags. Ebenso wie der Bundesdatenschutzbeauftragte hat der Landesdatenschutzbeauftragte nach § 24 LDSG Aufgaben als Kontrollorgan der Exekutive und – wiederum in beschränktem Umfang – auch der Judikative wahrzuneh-

666 GVBl. 1974, 31.
667 *Hartig/Klink/Eiermann*, LDSG, Erl. 1 zu § 22.
668 GVBl. 1978, 749.
669 *Hartig/Klink/Eiermann*, LDSG, Erl. 1 zu § 22.
670 *Hartig/Klink/Eiermann*, LDSG, Erl. 1 zu § 22.
671 BVerfGE 65, 1 (46).
672 GVBl. 2008, 99.
673 *Hartig/Klink/Eiermann*, LDSG, Erl. 1 zu § 24.
674 Zur Vereinbarkeit der Staatsaufsicht im nicht-öffentlichen Bereich mit der DSRL, vgl. EuGH, EuZW 2010, 296. Der EuGH hatte hier entschieden, dass die Angliederung der Innenministerien der Länder in der BRD einen Verstoß gegen die vollkommene Unabhängigkeit der Datenschutzstellen nach Art. 28 der Datenschutzrichtlinie darstelle. Mit Blick hierauf fordert *Roßnagel*, EuZW 2010, 299 eine Neuorganisation der Kontrollstellen.

men. Er ist – wie sich aus § 29 LDSG ergibt – Ombudsmann und hat zudem nach § 24 Abs. 4 und 5 LDSG verschiedene Beratungsfunktionen gegenüber Exekutive und Legislative wahrzunehmen.

6.2.2 Kontrollkompetenz bei den Gerichten

Nach § 24 Abs. 2 LDSG unterliegen die Gerichte der Kontrolle des Landesdatenschutzbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Die Regelung entspricht der vieler Bundesländer. Oben wurde klargestellt, dass Tätigkeiten der Gerichtsverwaltung der datenschutzrechtlichen Kontrolle unterliegen. Ebenso wurde festgehalten, dass reine Rechtsprechungsangelegenheiten nicht der datenschutzrechtlichen Kontrolle unterfallen. In manchen Bundesländern[675] und so auch in Rheinland-Pfalz[676] bestand jedoch Unsicherheit, ob auch Tätigkeiten, die die Spruchtätigkeit lediglich vorbereiten, unter den Begriff der Verwaltungsangelegenheiten fallen. So verneint das Ministerium der Justiz in Rheinland-Pfalz ein Kontrollrecht in diesem Graubereich. Es legt den Begriff der Verwaltungstätigkeiten eng aus und subsumiert Tätigkeiten, die die Spruchtätigkeit vorbereiten, nicht unter den Begriff der Verwaltungsangelegenheiten. Die Justizministerien der anderen Bundesländer vertreten die gleiche Auffassung.[677] Mit diesem Argument haben sie beispielsweise ein Kontrollrecht beim Einsatz von neuen IT-Systemen verneint. Aus dem gleichen Grund sahen sie auch keine Notwendigkeit, IT-Verfahren bei den Landesdatenschutzbeauftragten anzumelden. Der Landesbeauftragte für den Datenschutz in Rheinland-Pfalz bejaht dagegen ein Kontrollrecht in diesem Bereich.[678] Tätigkeiten, die die Spruchtätigkeit vorbereiten, würden nicht unter den Begriff der Verwaltungsangelegenheiten fallen. Seine Haltung stimmt mit der Haltung der Datenschutzbeauftragten des Bundes und der Länder überein. Diese hatten auf einer Konferenz im Jahr 1998 betont, dass eine Kontrolle bei den Gerichten nur nicht im Bereich der richterlichen Unabhängigkeit bestehen würde. Wohl würde sie sich aber u.a. darauf erstrecken, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden. Die Datenschutzbeauftragten forderten insoweit eine gesetzliche Klarstellung.[679]

675 Vgl. etwa *LfD Baden-Württemberg*, 20. Tätigkeitsbericht, Tz. 1.1.

676 Vgl. hierzu etwa *LfD Rheinland-Pfalz*, 15. Tätigkeitsbericht, Tz. 7; *LfD Rheinland-Pfalz*, 16. Tätigkeitsbericht, Tz. 7.

677 Vgl. hierzu *DSB-Konferenz*, 5./6.10.1998.

678 Vgl. hierzu etwa *LfD Rheinland-Pfalz*, 15. Tätigkeitsbericht, Tz. 7; *LfD Rheinland-Pfalz*, 16. Tätigkeitsbericht, Tz. 7.

679 Vgl. hierzu *DSB-Konferenz*, 5./6.10.1998: „Die Beschränkung der Prüfkompetenz bei den Gerichten hat einzig und allein den Zweck, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten. Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u.a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung. Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.“

Am 23.4.2002 brachte die Fraktion Bündnis 90/Die Grünen einen Änderungsantrag zum Gesetzentwurf der Landesregierung und zur Beschlussempfehlung des Innenausschusses ein.[680] Dieser sah vor, § 24 in seinem Abs. 2 dahingehend zu ergänzen, dass die Gerichte und der Rechnungshof der Kontrolle des Landesbeauftragten für den Datenschutz nur unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden. Begründet hat sie dies mit den angesprochenen Meinungsverschiedenheiten vom Landesbeauftragten für den Datenschutz und der Justiz bei der Wahrnehmung von Kontrollaufgaben.[681] Der Begriff der Verwaltungsangelegenheiten habe die Kompetenzen bislang nicht klar abgegrenzt. Die Neufassung stelle klar, dass eine Beschränkung der Prüfkompetenz nur den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten. In der Sitzung am 24.4.2002 wurde der Antrag jedoch mit den Stimmen der SPD, der CDU und der FDP gegen die Stimmen von Bündnis 90/Die Grünen abgelehnt.[682]

In der Tat ist die Formulierung in den Landesdatenschutzgesetzen, dass eine Kontrolle nur in Verwaltungsangelegenheiten besteht, unglücklich gewählt. So muss berücksichtigt werden, dass es Sinn der Regelungen nur sein kann, die rechtsprechende Tätigkeit der Gerichte wegen der verfassungsrechtlich garantierten Unabhängigkeit der Richter von der Datenschutzkontrolle auszunehmen. Damit sind aber nur die reinen Rechtsprechungsangelegenheiten der Datenschutzkontrolle entzogen. Die Ausstattung von EDV der Gerichte gehört dagegen zu den Verwaltungsangelegenheiten. Für Verwaltungsangelegenheiten ist charakteristisch, dass die Gerichte insoweit den Vorgaben und Weisungen des Justizministeriums unterliegen. Bei der Ausstattung von IT ist dies der Fall. Die Hard- und Software wird von der Landesjustizverwaltung ausgesucht und die Gerichte haben sie einzusetzen.

680 LT-Drs. 14/1015.
681 LT-Drs. 14/1015.
682 Protokoll der 22. Sitzung des 14. Landtags Rheinland-Pfalz, PlPr. 14/22.

In den Bundesländern Berlin,[683] Bremen,[684] Hamburg,[685] Hessen[686] und Schleswig-Holstein[687] finden sich in den Landesdatenschutzgesetzen Regelungen, die die Kontrolle nicht auf Verwaltungstätigkeiten beschränken. Diese könnten als Vorbild für das rheinland-pfälzische Landesdatenschutzgesetz dienen.[688]

6.2.3 Kontrollkompetenz bei den Notaren

In der Literatur wird zum Teil ein Kontrollrecht der Landesbeauftragten für den Datenschutz bei den Notaren abgelehnt. Dies wird damit begründet, dass ein Kontrollrecht mit einem Risiko für den Notar verbunden sei. So bestünde die Gefahr, dass der Notar gegen § 18 Abs. 1 Satz 1 BNotO, welcher zur Verschwiegenheit über dienstlich erlangte Informationen verpflichtet, verstoßen würde, wenn er dem Landesbeauftragten für den Datenschutz Auskunft erteilen oder ihm Akteneinsicht gewähren würde.[689] Wie bereits erläutert, ist das LDSG auf Notare aber anwendbar. Der Bundesgerichtshof hatte dies im Jahr 1990 entschieden.[690] Damit verbunden ist nach § 24 LDSG auch eine Kontrolltätigkeit durch den Landesdatenschutzbeauftragten mit entsprechenden gesetzlichen Auskunftspflichten in § 28 LDSG. Nach § 24 Abs. 2 LDSG ist eine Kontrolle des Landesbeauftragten für den Datenschutz nur bei den Gerichten nicht möglich, wenn diese nicht in Verwaltungsangelegenheiten tätig sind. Für Notare hat der Gesetzgeber

683 § 24 Abs. 2 BlnDSG: Ausgenommen von Absatz 1 sind die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Setzen Gerichte zur Erfüllung ihrer gesetzlichen Aufgaben automatische Datenverarbeitungsanlagen ein, so unterliegt unbeschadet der richterlichen Unabhängigkeit die Ordnungsmäßigkeit und Rechtmäßigkeit der Verfahren der Kontrolle des Datenschutzbeauftragten.

684 § 27 Abs. 1 BrDSG: Gerichte unterliegen der Überwachung durch den Landesbeauftragten für den Datenschutz nur, wenn sie in Verwaltungsangelegenheiten tätig werden, die Gerichte darüber hinaus beim Einsatz automatisierter Datenverarbeitung hinsichtlich organisatorischer und technischer Maßnahmen der Datensicherung, unbeschadet der verfassungsrechtlich gewährleisteten Unabhängigkeit.

685 § 23 Abs. 1 HmbDSG: Die Bürgerschaft, die Gerichte und der Rechnungshof unterliegen der Überwachung durch die Hamburgische Datenschutzbeauftragte bzw. den Hamburgischen Datenschutzbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden; die Einschränkung gilt nicht für Gerichtsvollzieherinnen und Gerichtsvollzieher. Bei den Gerichten und beim Rechnungshof überwacht die bzw. der Hamburgische Datenschutzbeauftragte darüber hinaus, ob die erforderlichen technischen und organisatorischen Maßnahmen getroffen und eingehalten werden.

686 § 24 Abs. 1 HSDG: Die Gerichte unterliegen der Kontrolle des Hessischen Datenschutzbeauftragten nur, soweit sie nicht in richterlicher Unabhängigkeit tätig wurden.

687 § 39 Abs. 1 LDSG Schleswig-Holstein: Die Gerichte unterliegen der Kontrolle, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

688 Dagegen dienen die Regelungen im BDSG nicht als Vorbild. Vgl. hierzu *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 24 Rn. 40: „Zwar sind die Richter nach Art. 97 GG unabhängig und nur dem Gesetz unterworfen, aber § 21 Satz 2 formuliert für die Anrufung der Gerichte ‚soweit diese in Verwaltungstätigkeiten tätig werden'. Von einer Präzisierung kann also keine Rede sein. Vielmehr wird in § 24 Abs. 3 nur die Ausnahme als andere Seite der Medaille dargestellt: Die Regel ergibt sich durch einen Umkehrschluss aus § 24 Abs. 3 und aus § 21 Satz 2 BDSG. Die Kontrolle des BfD bei den Gerichten findet somit in Verwaltungsangelegenheiten statt."

689 *Seiler*, DNotZ 2002, 693; *Rüpke*, NJW 1991, 568; *Bohrer*, 1991, Rn. 137; *Arndt/Lerch/Sandkühler*, Bundesnotarordnung, § 18 Rn. 3; *Seiler*, DNotZ 2002, 693.

690 BGH, NJW 1991, 568.

aber keine entsprechende Ausnahmeregelung getroffen. Auch in den Gesetzesbegründungen zu § 24 Abs. 2 LDSG findet sich kein Hinweis auf eine Einbeziehung von Notaren in diese Regelung. In manchen Landesdatenschutzgesetzen[691] und auch im Bundesdatenschutzgesetz[692] gibt es Bestimmungen, nach denen Kontrollrechte ungeachtet besonderer Amts- und Berufsgeheimnisse bestehen. In Rheinland-Pfalz wie auch in den Bundesländern Bremen, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Saarland, Sachsen-Anhalt existiert eine derartige Regelung nicht.[693] Allein aus dem Fehlen einer derartigen Regelung kann man jedoch nicht schließen, dass in diesen Ländern wegen § 18 Abs. 1 Satz 1 BNotO ein Kontrollrecht bei Notaren nicht besteht. Der Gesetzgeber hat die Gerichte weitgehend von den datenschutzrechtlichen Bestimmungen ausgenommen, weil sie aufgrund ihrer spezifischen Eigenorganisation eine hinreichende Sicherheit dafür bieten, dass das Persönlichkeitsrecht des Betroffenen gewahrt bleibt.[694] An einer derartigen Eigenorganisation fehlt es aber bei den Notaren.[695] Die Notare unterstehen – im Gegensatz zu den Richtern – nach den §§ 92 ff. BNotO einer staatlichen Aufsicht, welche sich auf deren ordnungsmäßige Erledigung der Amtsgeschäfte (§ 93 Abs. 1 Satz 1 BNotO) erstreckt. Das Recht der Aufsicht steht nach § 92 Nr. 1-3 BNotO dem Präsidenten des Landgerichts über die Notare und Notarassessoren des Landgerichtsbezirks, dem Präsidenten des Oberlandesgerichts über die Notare und Notarassessoren des Oberlandesgerichtsbezirks und der Landesjustizverwaltung über sämtliche Notare und Notarassessoren des Landes zu. Der Bundesgerichtshof[696] hat entschieden, dass ein Notar zur Anmeldung eines Verfahrensverzeichnisses beim Landesdatenschutzbeauftragten verpflichtet sei. Die Dienstaufsicht der Landesjustizverwaltungen über die Notare und die Anmeldung zum Dateienregister würden sich nicht gegenseitig die Grundlage entziehen.[697] Der Bundesgerichtshof betrachtete die Anmeldepflicht nach § 23 Abs. 1 Satz 1 DSG NRW 1988 als eine nicht als mit der notariellen Verschwiegenheitspflicht kollidierende Regelung. Die Anmeldepflicht beim Landesdatenschutzbeauftragten macht aber nur dann Sinn, wenn dieser auch ein Kontrollrecht gegenüber den Notaren hat. Folglich kann aus der Entscheidung des Bundesgerichtshofes nicht nur geschlossen werden, dass die Landesdatenschutzgesetze auf Notare Anwendung finden.[698] Vielmehr besagt die Entscheidung zugleich, dass eine Kontrolle bei den Notaren durch den Landesdatenschutzbeauftragten möglich ist.[699] Soweit geltend gemacht wird, dass der Entscheidung des Bundesgerichtshof keine generelle Aussage zu einer etwaigen Kontrollkompetenz entnommen

691 Baden-Württemberg (§ 28 Abs. 2 Satz 1 LDSG), Bayern (Art. 30 Abs. 2 Satz 1 BayDSG), Berlin (§ 28 Abs. 2 BInDSG), Brandenburg (§ 23 Abs. 8 BbDSG), Hamburg (§ 23 Abs. 5 Satz 3 HmbDSG), Nordrhein-Westfalen (§ 22 Abs. 2 Satz 2 DSG NRW), Sachsen (§ 24 Abs. 1 Satz 2 SächsDSG), Schleswig-Holstein (§ 41 Abs. 1 Satz 2 Nr. 1 LDSG), Thüringen (§ 37 Abs. 2 Satz 1 ThürDSG).

692 § 24 Abs. 2 Nr. 2 BDSG.

693 Vgl. hierzu auch *Seiler*, DNotZ 2002, 696.

694 BGHZ 112, 178 ff.

695 *Seiler*, DNotZ 2002, 695.

696 BGH, NJW 1991, 568.

697 BGH, NJW 1991, 568.

698 Vgl. hierzu Abschnitt 4.3.2.

699 So wie hier *Mihm*, NJW 1998, 1595. Anders jedoch *Seiler*, DNotZ 2002, 693; *Rüpke*, NJW 1991, 568; *Bohrer*, 1991, Rn. 137; *Arndt/Lerch/Sandkühler*, Bundesnotarordnung, § 18 Rn. 3.

werden kann,[700] da die Pflicht, Einsicht in alle Unterlagen zu gewähren, mit Blick auf die notarielle Schweigepflicht ein ungleich höheres Kollisionspotential in sich berge als die Pflicht zur Anmeldung von Dateien, über die der Bundesgerichtshof zu entscheiden hatte, kann dem nicht gefolgt werden. Denn der Landesdatenschutzbeauftragte ist gemäß § 26 Abs. 1 Satz 1 LDSG verpflichtet, über amtlich bekannt gewordene Angelegenheiten Verschwiegenheit zu wahren. Aufgrund dessen kann es bei der Wahrnehmung der Kontrollaufgaben zu einer Kollision von Verschwiegenheitspflicht und Auskunfts- oder Einsichtsrechten nicht kommen.

6.2.4 Kontrollkompetenz bei den Rechtsanwälten

Nach § 24 Abs. 1 Satz 2 LDSG ist der Landesbeauftragte für den Datenschutz auch Aufsichtsbehörde nach dem Bundesdatenschutzgesetz für die Datenverarbeitung nicht-öffentlicher Stellen. Nach § 38 Abs. 1 BDSG hätte er daher grundsätzlich auch die Ausführung des BDSG bei Rechtsanwälten zu kontrollieren. Mit Blick auf deren Verschwiegenheitspflicht nach § 43a BRAO ist jedoch auch hier – genauso wie bei den Notaren – umstritten, ob dem Landesdatenschutzbeauftragten Kontrollkompetenzen zukommen.[701] Eine Kontrollkompetenz ist jedoch auch bei den Anwälten richtigerweise zu bejahen. Nach § 24 Abs. 2 Nr. 2 BDSG erstreckt sich die Kontrolle des Bundesdatenschutzbeauftragten im öffentlichen Bereich auf personenbezogene Daten, die einem Berufs- oder Amtsgeheimnis unterliegen. § 38 Abs. 4 Satz 3 i.V.m. § 26 Abs. 6 BDSG ordnet nun dessen entsprechende Anwendung für den Bereich des Betretungs- und Prüfungsrechts bei den Aufsichtsbehörden im nicht-öffentlichen Bereich ausdrücklich an.

Wenn aber der Gesetzgeber für das weitreichende Betretungs- und Prüfungsrecht der Aufsichtsbehörden eine entsprechende Anwendung festgelegt hat, stehen den Aufsichtsbehörden ungeachtet gesetzlicher Verschwiegenheitspflichten erst recht die weniger einschneidenden Auskunftsrechte nach § 38 Abs. 3 BDSG zu. Dem BDSG kann daher entnommen werden, dass die Aufsichtsbehörden auch gegenüber den Rechtsanwälten ihre Kontrollrechte wahrnehmen können. Zu einer Kollision von Verschwiegenheitspflicht und Wahrnehmung der Aufsichtsrechte kann es nicht kommen, da – wie schon festgestellt wurde – der Landesdatenschutzbeauftragte gemäß § 26 Abs. 1 Satz 1 LDSG zur Verschwiegenheit in amtlichen Angelegenheiten verpflichtet ist. Mit Blick auf § 43a BRAO sind insbesondere die Rechtsanwaltskammern,[702] aber auch ein Teil der Literatur[703] der Ansicht, die datenschutzrechtliche Kontrolle solle besser von den Kammern wahrgenommen werden. Unabhängig davon, dass eine Kollision zwischen Datenschutzkontrolle und Verschwiegenheitspflicht nicht festgestellt werden kann, spricht hiergegen aber allein schon Art. 28 Abs. 1 Satz 1 DSRL. Dieser fordert die Unabhängigkeit der Datenschutzkontrollbehörde. Da die Rechtsanwaltskammern nach § 62 Abs. 2 Satz 1 BRAO aber der Aufsicht des Staates unterliegen, sind sie keine unabhängige Behörde. Zudem schreibt Art. 28

700 So etwa *Seiler*, DNotZ 2002, 697.

701 Dagegen etwa *Bundesrechtsanwaltskammer*, 2006, 1; *Rüpke*, ZRP 2008, 87. Für eine Kontrollkompetenz plädiert etwa *BfDI*, 21. Tätigkeitsbericht, Tz. 9.7.

702 *Bundesrechtsanwaltskammer*, 2006.

703 *Rüpke*, ZRP 2008, 87.

Abs. 5 DSRL vor, dass jede Kontrollstelle regelmäßig einen Bericht über ihre Tätigkeit vorlegen muss, der zu veröffentlichen ist. Die Rechtsanwaltskammern erfüllen diese Verpflichtung aber nicht. Es kommt hinzu, dass Art. 28 DSRL Prüfungen ohne besonderen Anlass von Amts wegen vorsieht. Wie die Rechtsanwaltskammern diese Prüfungen jedoch erfüllen wollen, bleibt unklar.

6.3 Der gerichtliche Datenschutzbeauftragte

6.3.1 Erfordernis einer Bestellung

Für den Bereich des Bundesgerichtshofes ergibt sich die Notwendigkeit der Bestellung eines Datenschutzbeauftragten aus § 4f Abs. 1 BDSG.[704] § 4f Abs. 1 BDSG unterscheidet beim Erfordernis der Bestellung danach, ob personenbezogene Daten automatisiert verarbeitet werden oder nicht. Im ersten Fall ist gemäß § 4f Abs. 1 Satz 1 BDSG zwingend ein Datenschutzbeauftragter zu bestellen.[705] Wenn personenbezogene Daten konventionell verarbeitet werden, kommt es auf die Zahl der Personen an, die mit der Verarbeitung beschäftigt sind. § 4f Abs. 1 Satz 3 BDSG setzt diesbezüglich eine Zahl von regelmäßig 20 Personen voraus. Beim Bundesgerichtshof dürften beide Voraussetzungen vorliegen, so dass von der Notwendigkeit einer Bestellung auszugehen ist.

§ 11 LDSG bestimmt, dass öffentliche Stellen, bei denen mindestens zehn Beschäftigte regelmäßig personenbezogene Daten verarbeiten, einen Datenschutzbeauftragten zu bestellen haben. Bei der Mindestzahl von zehn Beschäftigten spielt es keine Rolle, ob diese die Daten automatisiert verarbeiten oder in herkömmlichen Verfahren.[706] Auch Bedienstete, die papiergebundene Akten bearbeiten, zählen hierzu.[707] Nach § 11 Abs. 6 LDSG haben Gerichte einen Datenschutzbeauftragten nur dann zu bestellen, wenn sie in Verwaltungsangelegenheiten tätig werden. Wie oben gesehen,[708] ist die Frage, was unter Verwaltungsangelegenheiten zu subsumieren ist, umstritten. Aus den genannten Gründen ist jedoch der weiten Auffassung zu folgen. Dies bedeutet, dass es bei der Anzahl von Personen, die personenbezogene Daten verarbeiten, nicht nur auf diejenigen ankommt, die mit Personalangelegenheiten etc. betraut sind. Mitzuzählen sind vielmehr auch jene, die zum Beispiel in den Geschäftsstellen arbeiten und die Spruchtätigkeit des Richters vorbereiten. Vor diesem Hintergrund dürften die Voraussetzungen für die Bestellung eines gerichtlichen Datenschutzbeauftragten in den meisten Amts- und Landgerichten und auch bei den beiden Oberlandesgerichten in Rheinland-Pfalz vorliegen.

---

704 Zum behördlichen Datenschutzbeauftragten allgemein vgl. etwa *Abel*, MMR 2002, 289; *Schild*, DuD 2001, 31; *Engelien-Schulz*, BWV 2001, 241.

705 Vgl. aber § 4f Abs. 1 Satz 4 BDSG, der bestimmt, dass, soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, die Bestellung eines Datenschutzbeauftragten für mehrere Bereiche genügt.

706 *Hartig/Klink/Eiermann*, LDSG, Erl. 2.1 zu § 11.

707 *Hartig/Klink/Eiermann*, LDSG, Erl. 2.1 zu § 11.

708 Vgl. hierzu Abschnitt 6.2.2.

6.3.2 Rechtsstellung und Aufgaben

Voraussetzungen für die Bestellung zum Datenschutzbeauftragten sind nach § 4f Abs. 2 BDSG und § 11 Abs. 1 Satz 3 LDSG Fachkunde und Zuverlässigkeit. Der Datenschutzbeauftragte ist dabei gemäß § 4f Abs. 3 Satz 1 BDSG und § 11 Abs. 1 Satz 2 LDSG unmittelbar der Behördenleitung zu unterstellen. Bei den Gerichten sind dies der jeweilige Gerichtspräsident bzw. die Direktoren der Amtsgerichte.

Die Datenschutzbeauftragten sind in Ausübung ihrer Tätigkeit auf dem Gebiet des Datenschutzes weisungsfrei.[709] Die Änderungen, die § 4f BDSG mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009[710] zum grundsätzlichen Kündigungsverbot des Datenschutzbeauftragten erfahren hat,[711] wirken sich in erster Linie für den Datenschutzbeauftragten in einer Kanzlei oder – falls in das LDSG eine entsprechende Regelung eingeführt werden würde – in einem Notariat aus, denn die Datenschutzbeauftragten in den Gerichten werden in der Regel beamtet sein. Für diese ist hinsichtlich der Änderungen auf Bundesebene jedoch § 4f Abs. 3 Satz 7 BDSG von Bedeutung, der nunmehr bestimmt, dass die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen hat.

Die Aufgaben des gerichtlichen Datenschutzbeauftragten ergeben sich aus § 4g BDSG und aus § 11 Abs. 3 LDSG. Zu den Aufgaben eines Datenschutzbeauftragten gehört es daher etwa, die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Bestimmungen des Datenschutzrechts vertraut zu machen, gesetzlich vorgeschriebene Verfahrensverzeichnisse zu führen und zur Einsicht bereitzuhalten oder die Durchführung von Vorabkontrollen. Im Unterschied zu § 4g Abs. 1 BDSG bestimmt § 11 Abs. 3 LDSG lediglich, dass der Datenschutzbeauftragte die Aufgabe hat, die öffentlichen Stellen bei der Ausführung des LDSG sowie anderer Vorschriften über den Datenschutz zu „unterstützen“. Nach § 11 Abs. 3 LDSG besitzt der Datenschutzbeauftragte also lediglich eine Beratungsfunktion und keine Kontrollfunktion. Ungeachtet dessen steht es jedoch der Behördenleitung frei, dem Datenschutzbeauftragten ergänzend auch Kontrollaufgaben zuzuweisen.[712] Die Wahrnehmung von Kontrollaufgaben des gerichtlichen Datenschutzbeauftragten findet jedoch ihre Grenze, wenn die in Art. 97 GG garantierte richterliche Unabhängigkeit tangiert ist. Während eines laufenden Verfahrens kann der gerichtliche Datenschutzbeauftragte daher nicht etwa den Eingaben von Petenten nachgehen. Die richterliche Unabhängigkeit ist jedoch nicht schon dann tangiert, wenn es um die technischen und organisatorischen Sicherheitsmaßnahmen von IT geht, die der Richter für seine Arbeit benutzt. Wenn der Richter zu Hause arbeitet, ergibt sich jedoch allein schon wegen Art. 13 GG (Unverletzlichkeit der Wohnung) eine Grenze der Datenschutzkontrolle.[713] Hier

[709] Ausdrücklich geregelt in § 4f Abs. 3 Satz 2 BDSG. Für § 11 LDSG vgl. *Hartig/Klink/Eiermann*, LDSG, Erl. 2.6 zu § 11.

[710] BGBl. 2009 I, 2814.

[711] § 4f Abs. 3 Satz 5 und 6 BDSG.

[712] *Hartig/Klink/Eiermann*, LDSG, Erl. 4.1 zu § 11.

[713] *Bäumler/Nordmann*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 145.

ist es notwendig, dass der Richter auf die Einhaltung des Datenschutzes vom Datenschutzbeauftragten gesondert hingewiesen wird.[714]

6.4 Zusammenfassung

Bereits vor dem Amt des Bundesdatenschutzbeauftragten gab es in Rheinland-Pfalz – wie auch in Hessen – eine Datenschutzkontrolle. Sowohl der Bundesdatenschutzbeauftragte als auch der Landesdatenschutzbeauftragte haben die Aufgaben als Kontrollorgan der Exekutive, die Aufgaben eines Ombudsmanns und Beratungstätigkeiten gegenüber dem Parlament und der Exekutive wahrzunehmen. Die Datenschutzkontrolle steht in einem Spannungsfeld zur richterlichen Unabhängigkeit. Der Gesetzgeber sollte diesbezüglich für eine Klarstellung dahingehend sorgen, dass nur die Tätigkeiten von einer Datenschutzkontrolle ausgenommen sind, die auch die richterliche Unabhängigkeit tangieren. Kontrollkompetenzen besitzt der Landesdatenschutzbeauftragte auch gegenüber Notaren und Rechtsanwälten.

[714] *Bäumler/Nordmann*, in: *Abel* (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 145.

Teil III

Datenschutzprobleme und Verbesserungsvorschläge

In Teil I wurden die Grundlagen dargestellt, die für den Datenschutz in der elektronischen Justiz von Bedeutung sind. Sodann wurde der Rechtsrahmen in Teil II vorgestellt und aufgezeigt, welche Anforderungen an den Datenschutz in der elektronischen Justiz zu beachten sind. Aufbauend darauf wird in diesem Teil nun untersucht, welche konkreten datenschutzrechtlichen Probleme bei der Anwendung von elektronischen Abläufen im Zivilverfahren, dem Zwangsvollstreckungsverfahren, dem Zwangsversteigerungsverfahren, dem Insolvenzverfahren, der Grundbuchordnung und dem Handelsgesetzbuch bestehen. Die Untersuchung folgt am Beispiel dieser Verfahrensordnungen, weil der Modernisierungsprozess in diesen Bereichen aufgrund der bereits vorgestellten gesetzgeberischen Aktivitäten besonders weit fortgeschritten ist. Zunächst erfolgt eine detaillierte Darstellung der elektronischen Abläufe aufgrund des Prozessrechts. Sodann wird bewertet, ob der Gesetzgeber den Datenschutz bei der Ausgestaltung seiner Verfahrensabläufe hinlänglich berücksichtigt hat. Dort, wo erforderlich, werden konkrete Verbesserungsvorschläge gemacht.

Kapitel 7

Zivilverfahren

Es wurde bereits festgestellt, dass die ZPO im Zivilverfahren die elektronische Einreichung von Schriftsätzen, elektronische Zustellungen, formlose elektronische Mitteilungen des Gerichts an Parteien, Verfahrensbeteiligte oder Dritte, eine elektronische Akteneinsicht, elektronische Bekanntmachungen und eine elektronische Aktenführung zulässt. Darüber hinaus ist das Mahnverfahren automatisiert worden. Zudem gab es ein Pilotprojekt, dass sich mit der Einbindung des ELENA-Verfahrens in das Prozesskostenhilfeverfahren beschäftigt hat. Schließlich machen bereits verschiedene Amts- und Landgerichte in der Bundesrepublik davon Gebrauch, Daten aus einem von der Europäischen EDV-Akademie des Rechts betriebenen zentralen Schutzschriftenregister abzurufen. Im Folgenden werden diese Verfahrensabläufe und Projekte im Hinblick auf datenschutzrechtliche Fragestellungen geprüft und bewertet.

7.1 E-Schriftsätze an das Gericht

Der Zivilprozess beginnt mit der Einreichung einer Klageschrift bei Gericht. Bei den an das Gericht übersandten Daten handelt es sich um personenbezogene Daten nach § 3 BDSG. In der Klageschrift sind entsprechend § 130 Nr. 1 bis 3 ZPO zumindest der Name, der Vorname, die Anschrift der Parteien, die Bezeichnung des Streitgegenstands, die Anträge und tatsächliche Ausführungen zum Vortrag der Parteien enthalten. Gegebenenfalls hat die Partei oder der Anwalt nach § 130 Nr. 5 ZPO noch Zeugen mit Vorname, Namen und Adresse in der Klageschrift genannt. In diesem Fall geht es also nicht nur um personenbezogene Daten der Parteien selbst, sondern auch um die Daten von Dritten, die nicht am Prozess beteiligt sind. Wenn die Partei oder der Anwalt die Klage mit einem Antrag auf Prozesskostenhilfe verbindet, sind in der Klageschrift zudem weitere sensible Daten enthalten. § 117 Abs. 2 ZPO schreibt insofern vor, dass dem Antrag auf Prozesskostenhilfe eine Erklärung der Partei über ihre persönlichen und wirtschaftlichen Verhältnisse, also Familienverhältnisse, Beruf, Vermögen, Einkommen und Lasten, mit den entsprechenden Belegen beizufügen ist. Aufgrund dieser Angaben hat das Gericht die Bedürftigkeit nach § 114 ZPO zu prüfen. Bei der Einreichung von elektronischen Dokumenten im Sinne des § 130a ZPO können sich aus datenschutzrechtlicher Sicht Probleme

ergeben, wenn diese nicht verschlüsselt und ohne qualifizierte elektronische Signatur an das Gericht geschickt werden.

7.1.1 Verschlüsselung

Werden elektronische Dokumente nicht verschlüsselt an das Gericht verschickt, könnten sie von Unbefugten mitgelesen werden. Daran würde sich auch nichts ändern, wenn die Partei oder der Anwalt das Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 SigG versehen hat. Denn diese gewährleistet lediglich die Authentizität und die Integrität des Dokuments, nicht aber die Vertraulichkeit. § 130a ZPO enthält keine Regelung, die den Absender verpflichten würde, elektronische Dokumente verschlüsselt an das Gericht zu schicken. Gemäß der Begründung zum Regierungsentwurf ist eine derartige Regelung zwar bei der Erarbeitung des Entwurfs in Erwägung gezogen worden. Hiervon ist – so weiter – jedoch wieder abgesehen worden, da es einerseits den Absendern überlassen bleiben sollte, ob sie ihre Dokumente verschlüsseln wollen und andererseits den Verordnungsgebern vorbehalten bleiben sollte, auch mit Blick auf die erforderliche technische Ausstattung bei den Gerichten Verschlüsselungstechniken zuzulassen.[715]

7.1.1.1 Pflicht zur Verschlüsselung

Die Begründung des Entwurfs geht damit ohne nähere Ausführungen davon aus, dass es den Absendern selbst überlassen ist, ob sie ihre Dokumente verschlüsselt an das Gericht senden wollen.

Rechtsanwalt Für den Anwalt ergibt sich jedoch eine Verpflichtung, das Dokument verschlüsselt an das Gericht zu schicken, bereits aus § 43a Abs. 2 BRAO.[716] Nach § 43a Abs. 2 Satz 1 BRAO ist der Anwalt zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich nach Satz 2 der Vorschrift auf alles, was ihm in Ausübung seines Amtes bekannt geworden ist. Von der Verschwiegenheitspflicht umfasst sind danach alle Mandantengeheimnisse, die dem Rechtsanwalt – vom Mandanten oder Dritten – anvertraut worden sind und darüber hinaus alle Informationen, die ihm im Rahmen seiner anwaltlichen Tätigkeit bekannt geworden sind und die nicht offenkundig sind.[717] Von der Verschwiegenheitspflicht umfasst sind danach jedenfalls auch die Informationen in einer Klageschrift, die der Rechtsanwalt von seinem Mandanten erhalten hat. Die Verschwiegenheitspflicht des Rechtsanwalts gilt auch bei einer Online-Kommunikation.[718]

[715] BT-Drs. 14/4987, 24.

[716] Nach § 1 Abs. 3 Satz 2 BDSG geht § 43a Abs. 2 BRAO insofern § 9 BDSG vor.

[717] *Feuerich/ Weyland*, BRAO, § 43a Rn. 16.

[718] Vgl. hierzu etwa *Knopp* et al., MMR 2008, 725; *Miedbroth*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 726; *Klett/ Sang-Woon*, CR 2008, 647; *Feuerich/ Weyland*, BRAO, § 43a Rn. 25. Eine Pflicht zur Verschlüsselung lehnen ab *Härting*, MDR 2001, 62; *Härting*, NJW 2005, 1248; *Degen*, NJW 2008, 1479; *Axmann/ Degen*, NJW 2006, 1457 f.; *Lindloff*, 2005, 75 ff.

Der Anwalt kann seiner Funktion als Organ der Rechtspflege nur nachkommen, wenn die elektronische Kommunikation zwischen ihm und seinem Mandanten vertraulich bleibt. Bei der Kommunikation mittels einer einfachen E-Mail ist dies nicht der Fall. Sender und Empfänger einer gewöhnlichen E-Mail benötigen einen Provider. Auf diesen sind die E-Mails abgespeichert. Die Inhalte in der E-Mail können von Mitarbeitern der Provider, die Zugriff auf die Server haben, mitgelesen werden. Außerdem sind Eingriffe von außen technisch möglich. So können Datenleitungen von Externen angezapft werden. Vor diesem Hintergrund hat der Anwalt Dokumente mit mandatsrelevanten Informationen – und damit auch die Klageschrift – verschlüsselt zu versenden.[719] Die Verschwiegenheitspflicht verpflichtet den Rechtsanwalt dabei, solche Verschlüsselungstechniken einzusetzen, die eine Einsichtnahme von Dritten – auch von Diensteanbietern – ausschließt.[720]

Eine Pflicht zur Verschlüsselung entfällt nur dann, wenn der Mandant im Vorfeld in eine unverschlüsselte Kommunikation eingewilligt hat.[721] Eine derartige Einwilligung kann auch konkludent erfolgen. Sie liegt zum Beispiel vor, wenn der Mandant seinem Anwalt die betreffenden Informationen selbst unverschlüsselt per E-Mail mitgeteilt hat. In diesem Fall kann davon ausgegangen werden, dass der Mandant mit einer entsprechenden Verfahrensweise des Anwalts einverstanden ist.[722]

Von einem Teil der Literatur wird zwar eine Pflicht zur Verschlüsselung bei der Online-Kommunikation des Anwalts abgelehnt.[723] Wie im Folgenden gezeigt wird, ist diese Auffassung jedoch nicht zutreffend.

Vergleich mit klassischen Kommunikationsmitteln Die Argumentation stützt sich zum einen auf den Vergleich klassischer Kommunikationsmittel und der E-Mail. Bei letzterer sei das Risiko des Verlustes der Vertraulichkeit nicht höher zu bewerten als bei den herkömmlichen Kommunikationsmitteln.[724] Dem kann jedoch nicht gefolgt werden. Die Übermittlung der Daten im Internet ähnelt einer mit Bleistift geschriebenen Postkarte, wenn keine technischen Schutzvorkehrungen getroffen werden.[725]

Die Übermittlung per Post findet dagegen in einem verschlossenen Umschlag statt, so dass der Inhalt von Dritten nicht zur Kenntnis genommen werden kann. Und die Übermittlung per Fax findet in einer geschlossenen Leitung statt. Wenn man bei der Übermittlung eines Faxes versehentlich die falsche Nummer anwählt, dann ist die Wahrscheinlichkeit hoch, dass eine normale Telefonnummer angewählt wird. In diesem Fall bricht das Faxgerät mit einer Fehlermeldung

719 *Knopp* et al., MMR 2008, 725; *Miedbroth*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 726; *Klett/Sang-Woon*, CR 2008, 647; *Feuerich/Weyland*, BRAO, § 43a Rn. 25.

720 Damit ist der Rechtsanwalt auch zu einer Ende-zu-Ende-Verschlüsselung verpflichtet. So auch *Roßnagel* et al., DuD 2009, 730. Zu den damit einhergehenden praktischen Problemen vgl. Abschnitt 7.1.1.3.

721 *Feuerich/Weyland*, BRAO, § 43a Rn. 25.

722 Vgl. hierzu *Feuerich/Weyland*, BRAO, § 43a Rn. 25 m.w.N.

723 *Härting*, MDR 2001, 62; *Härting*, NJW 2005, 1248/1249; *Degen*, NJW 2008, 1479; *Axmann/Degen*, NJW 2006, 1457 f.; *Lindloff*, 2005, 75 ff.

724 *Lindloff*, 2005, 105.

725 Vgl. hierzu *Yildirim*, 2004, 59.

ab und übermittelt keine Daten. Bei der Übermittlung per E-Mail ist dies hingegen anders. Wenn versehentlich eine falsche E-Mail Adresse eingegeben wird (z.B. `poststelle@ag-kl.de` statt `poststelle@ag-ka.de`), ist es sehr wahrscheinlich, dass eine andere gültige Adresse getroffen wird. Dies hat zur Folge, dass die Daten anderen Personen zur Kenntnis gelangen. Und selbst wenn keine gültige Adresse getroffen wurde, dann kann es sein, dass beim Provider die E-Mail trotzdem angenommen wird und eine Datenübermittlung stattfindet.

Wortlaut des § 43a BRAO Zum anderen beruft sich die Literaturmeinung auf den Wortlaut des § 43a BRAO, welcher den Anwalt nur zum Schweigen verpflichtet. Damit seien aktive Handlungen wie eine Verschlüsselung von der Verschwiegenheitspflicht ausgenommen.[726] Dem kann jedoch ebenfalls nicht zugestimmt werden. Folgt man dieser Argumentation, so würde der Rechtsanwalt auch dann nicht gegen seine Pflicht zur Verschwiegenheit verstoßen, wenn er etwa offen geschützte Schriftstücke wie Akten oder Briefe herumliegen lassen würde oder aus Bequemlichkeit darauf verzichten würde, seinen Schreibtisch aufzuräumen oder seinen PC vor Zugriffen zu schützen. In diesen Beispielsfällen wird – zu Recht – nicht in Frage gestellt, dass der Anwalt seine Pflicht zur Verschwiegenheit verletzt hat.[727] Denn für eine Pflichtverletzung nach § 43a BRAO spielt es keine Rolle, ob diese durch aktives Tun oder durch Unterlassen geschieht.[728]

Schutz durch die Strafrechtsordnung Weiter wird geltend gemacht, dass das Strafrecht ausreichend Sorge dafür getragen hat, dass der Betreiber der Übertragungseinrichtungen, ihre Beschäftigten oder Dritte keinen Zugriff auf die Daten nehmen dürfen.[729] In der Tat ist zutreffend, dass der Gesetzgeber bestimmte Handlungen der genannten Personen unter Strafe gestellt hat. Teilen der Inhaber oder Beschäftigte eines Unternehmens, das geschäftsmäßig Post- und Telekommunikationsdienste erbringt, Tatsachen, die dem Post- oder Fernmeldegeheimnis unterliegen, unbefugt an eine andere Person mit, so unterfällt diese Handlung unter den Straftatbestand des § 206 Abs. 1 StGB.[730] Dritte, die sich Kenntnis vom Kommunikationsvorgang mittels E-Mail verschaffen, machen sich – wenn die Daten verschlüsselt versandt

[726] Vgl. hierzu *Härting*, MDR 2001, 62; *Härting*, NJW 2005, 1248 f.; *Lindloff*, 2005, 105.

[727] *Feuerich/ Weyland*, BRAO, § 43a Rn. 19.

[728] Vgl. hierzu auch *von Lewinski*, DuD 2000, 15: „Insbesondere in der Strafrechtswissenschaft ist anerkannt, dass die ‚Wahrung des Geheimnisses' mehr ist als ‚bloßes Schweigen'. Die anwaltliche Schweigepflicht verbietet deshalb nicht nur eine Tätigkeit (‚Ausplaudern'), sie kann auch durch ein Nichthandeln verletzt werden (unechtes Unterlassungsdelikt, § 13 StGB)."

[729] Vgl. hierzu *Härting*, MDR 2001, 62; *Härting*, NJW 2005, 1248 f.; *Lindloff*, 2005, 105.

[730] Zur Anwendung des § 206 Abs. 1 auf E-Mails vgl. *Holznagel*, 2003, § 7 Rn. 46; *Ernst*, MDR 2003, 3237, OLG Karlsruhe, MMR 2005, 178.

werden – nach § 202a StGB strafbar.[731] Erfolgt die Übermittlung unverschlüsselt, erfüllen sie den Tatbestand des § 202b StGB.[732]

Doch muss berücksichtigt werden, dass der Täter, wenn er eine der Straftaten nach §§ 202a, b StGB begeht, keine hohen Sanktionen zu erwarten hat. Der Strafrahmen des § 202a StGB beträgt Geldstrafe oder Freiheitsstrafe bis zu drei Jahren, der des § 202b Geldstrafe oder Freiheitsstrafe bis zu zwei Jahren. Ein Ersttäter wird aufgrund dieses Strafrahmens daher wohl mit einer Einstellung des Verfahrens nach §§ 153 ff. StPO rechnen können. Es kommt hinzu, dass die Aufklärungsquote dieser Tatbestände ohnehin nicht hoch ist. Mit 29,0 Prozent im Jahr 2008[733] und 22,4 Prozent im Jahr 2009[734] liegt sie deutlich unter dem Durchschnitt.[735] Die Aufklärungsrate bei § 206 StGB wird nicht veröffentlicht. Bei § 206 StGB dürfte der Täter eher von der Begehung einer Straftat abgehalten werden. Dies zum einen aufgrund des etwas höheren Strafrahmens (Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe). Zum anderen aber auch vor allem deswegen, weil der Inhaber eines Anbieters mit dem Widerruf seiner Gewerbeerlaubnis und der Mitarbeiter des Diensteanbieters mit arbeitsrechtlichen Konsequenzen zu rechnen hat. Allerdings ist § 206 Abs. 2 Nr. 1 bis 3 StGB auf die E-Mail nicht anwendbar. Dies folgt aus dem Wortlaut des § 206 Abs. 2 Nr. 1 bis 3 StGB, welcher eine verschlossene Sendung – und damit einen körperlichen Gegenstand – verlangt.[736] Nur § 206 Abs. 1 findet auf die E-Mail Anwendung. Damit können Inhaber und Beschäftigte eines Diensteanbieters

[731] Vgl. § 202a StGB: „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, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“ § 202a StGB wurde mit dem 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7.8.2007 neu gefasst (BGBl. 2007 I, 1786). Der Gesetzgeber hat mit der Neufassung zum einen klargestellt, dass auch das bloße Hacking unter die Strafvorschrift fällt. Zum anderen hat der Gesetzgeber den Tatbestand aber auch dahingehend eingeschränkt, dass das Verschaffen unter „Überwindung einer Zugangssicherung“ zu erfolgen hat. Daten sind gegen unberechtigten Zugang besonders gesichert, wenn Vorkehrungen getroffen sind, den Zugriff auf Daten auszuschließen, oder wenigstens nicht unerheblich zu erschweren (vgl. dazu BT-Drs. 16/3656, 10). Derartige Zugangssicherungen stellen zum Beispiel Verschlüsselungstechniken beim Versand von E-Mail Nachrichten dar.

[732] § 202b StGB bestimmt, dass – soweit die Tat nicht nicht in anderen Vorschriften mit schwererer Strafe bedroht ist – derjenige mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft wird, der sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. § 202b StGB wurde mit dem 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7.8.2007 neu eingefügt. § 202b StGB stellt das Pendant zu dem Abhören und Aufzeichnung von Telefongesprächen dar. Von der Norm werden alle Formen der elektronischen Datenübermittlung erfasst, damit auch die E-Mail. Nach § 201 StGB ist lediglich das illegale Abhören von Telefongesprächen strafbar, nach § 148 i.V.m. § 89 TKG das Abhören von Nachrichten mittels einer Funkanlage und § 202a erfasst nur solche Daten, die verschlüsselt versandt werden. Mit § 202b StGB hat der Gesetzgeber damit eine Regelungslücke geschlossen. Vgl. hierzu im Einzelnen BT-Drs. 16/3656, 11.

[733] Vgl. hierzu *BMI*, 2009, 49, Schlüsselzahl 678000.

[734] Vgl. hierzu *BMI*, 2010, 44, Schlüsselzahl 678000.

[735] Die durchschnittliche Aufklärungsquote lag im Jahr 2008 bei 54,8 Prozent und im Jahr 2009 bei 55,6 Prozent. Vgl. hierzu *BMI*, 2010, 16.

[736] Vgl. hierzu *Lindloff*, 2005, 102 m.w.N.

zwar dann bestraft werden, wenn sie Dritte vom Inhalt oder vom Versand oder Empfang einer E-Mail unterrichten, nicht aber dann, wenn sie eine Datei löschen, fehlleiten oder unterdrücken. In diesen Fällen ist auch der Straftatbestand des § 246 StGB nicht einschlägig, da dieser eine fremde bewegliche Sache voraussetzt. Lediglich § 274 Nr. 2 StGB könnte herangezogen werden. Bei den Dokumenten an das Gericht würde es sich um beweiserhebliche Daten nach § 202a Abs. 2 StGB handeln. Der Täter müsste aber auch mit Nachteilszufügungsabsicht handeln, was in der Regel nicht einfach zu beweisen ist. Ob Dritte, der Inhaber oder der Beschäftigte einer Übertragungseinrichtung also letzten Endes mit einer strafrechtlichen Verurteilung zu rechnen haben, bleibt zumindest zweifelhaft. Im Übrigen spricht auch allein der Umstand, dass die Strafrechtsordnung die Vertraulichkeit der elektronischen Kommunikation ausreichend geschützt hat, nicht per se gegen eine Pflicht zur Verschlüsselung.

Naturparteien Eine Pflicht zur Verschlüsselung ergibt sich nicht nur für Anwälte. Auch Naturparteien sind nach § 9 BDSG zur Verschlüsselung verpflichtet. Auch sie müssen solche Verschlüsselungstechniken einsetzen, die eine Einsichtnahme von Dritten, d.h. auch von Diensteanbietern, ausschließen. Es wurde bereits festgestellt,[737] dass das BDSG und damit auch § 9 BDSG auf Naturparteien Anwendung findet. Nach § 9 Satz 1 BDSG sind öffentliche und auch nicht-öffentliche Stellen verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Anforderungen des BDSG sicherzustellen. Hierzu gehört nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG auch eine Weitergabekontrolle. Diese beinhaltet unter anderem die Sicherung der Übertragungswege, welche durch eine Verschlüsselung erreicht werden kann. Mit § 9 Satz 2 BDSG hat der Gesetzgeber alle Datensicherungsmaßnahmen unter den Grundsatz der Verhältnismäßigkeit gestellt.[738] So sind nach § 9 Satz 2 BDSG solche Maßnahmen erforderlich, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck besteht. Nach diesem Grundsatz sind E-Mails verschlüsselt an das Gericht zu verschicken. Verschlüsselungstechnologien sind geeignet, die Vertraulichkeit einer E-Mail zu gewährleisten.[739] Sie sind auch erforderlich, da es technisch nicht möglich ist, auf andere Weise die Vertraulichkeit einer E-Mail zu gewährleisten. Überdies steht der Einsatz einer Verschlüsselungstechnologie ihrem Aufwand nach nicht außer Verhältnis zum Zweck ihres Einsatzes.[740] Der Einsatz einer Verschlüsselungstechnologie ist heutzutage mit relativ geringen Anschaffungskosten und einem geringen Organisationsaufwand zu realisieren.[741] Die Sensibilität der an das Gericht zu übermittelnden Daten kann auf der anderen Seite jedoch sehr hoch sein.

Zum Teil wird vertreten, dass § 9 BDSG für die hier behandelnde Frage nicht einschlägig ist.[742] Begründet wird dies damit, dass eine Übermittlung im Sinne des § 3 Abs. 4 Satz 2 Nr. 3 BDSG nur das finale Handeln umfasse, nicht aber die unbefugte oder berechtigte Kennt-

[737] Vgl. hierzu Abschnitt 4.3.1.2.
[738] *Heibey*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 577.
[739] *Klett/Sang-Woon*, CR 2008, 647.
[740] *Klett/Sang-Woon*, CR 2008, 647.
[741] *Klett/Sang-Woon*, CR 2008, 647.
[742] So *von Lewinski*, BRAK-Mitt. 2004, 14 für die anwaltliche Kommunikation per E-Mail.

nisnahme Dritter. Diese Auffassung ist nicht verständlich, da die unbefugte Kenntnisnahme von Daten durch Dritte – und nur hierauf kommt es an – nicht zielgerichtet erfolgt. Ziel- und zweckgerichtet erfolgt die Übermittlung zwischen den Kommunikationspartnern. Damit dieser Vorgang vertraulich bleibt, sind technisch-organisatorische Maßnahmen im Sinne einer Weitergabekontrolle erforderlich.

Wenn Anwälte und Parteien nun verpflichtet sind, Verschlüsselungstechniken einzuführen, erscheint es angebracht, auch § 130a ZPO klarstellend dahingehend zu ergänzen, dass Dokumente so an das Gericht zu schicken sind, dass sie gegen unbefugte Kenntnisnahme Dritter geschützt sind. Für den umgekehrten Weg, der Ausgangsseite, sieht § 174 Abs. 3 ZPO eine derartige Verpflichtung vor. Was die Sensibilität der Daten angeht, bestehen zwischen Eingangs- und Ausgangsseite jedoch keine Unterschiede. Mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften von 2009[743] hat der Gesetzgeber in der Anlage zu § 9 Satz 1 BDSG in Satz 3 für die Zugangs-, Zugriffs- und Weitergabekontrolle die Bedeutung von Verschlüsselungsverfahren gesondert hervorgehoben. Er hielt dies für erforderlich, da Verschlüsselungsverfahren in der Praxis noch nicht in nennenswertem Umfang eingesetzt werden würden.[744] Da der Gesetzgeber Verschlüsselungstechniken schon für eine allgemeine Kommunikation für erforderlich hält, ist es erst recht notwendig, diese Techniken bei einer elektronischen Übermittlung von Daten einzusetzen, die aufgrund der Vertrauensbeziehung zwischen Anwalt und Mandat eines besonderen Schutzes bedürfen.

7.1.1.2 Flexibilität für den Verordnungsgeber

Die Begründung sieht weiter vor, dass es dem Verordnungsgeber überlassen bleiben sollte, ob er Verschlüsselungstechniken einführt oder nicht. Der Gesetzgeber wollte damit dem Verordnungsgeber wohl eine gewisse flexible Handhabung ermöglichen. Auf der Ausgangsseite, bei § 174 Abs. 3 ZPO, hat er jedoch den Landesjustizverwaltungen zu Recht keine Wahlmöglichkeit eingeräumt.[745] Wenn der Staat die elektronische Kommunikation zulässt, hat er auch dafür zu sorgen, dass die Kommunikation vertraulich ist und mit keinen Gefahren für das Recht auf informationelle Selbstbestimmung einhergeht. Dies gilt erst recht, wenn es – wie hier – um den Schutz von Mandantengeheimnissen geht.

7.1.1.3 Praktische Probleme

Gegen eine Pflicht zur Verschlüsselung könnten praktische Probleme angeführt werden. So könnte angeführt werden, dass dem Anwalt oder den Parteien der öffentliche Schlüssel des

743 BGBl. 2009 I, 2814.

744 BT-Drs. 16/13657, 23.

745 Die Gesetzesbegründung zu § 174 ZPO geht auf diesen Punkt nicht ein. Vgl. hierzu BT-Drs. 14/4554, 19. Dort heißt es lediglich: „Um die Vertraulichkeit der Übermittlung und den Schutz darin enthaltener Daten zu sichern, ist das elektronische Dokument daher in geeigneter Weise gegen unbefugte Kenntnisnahme zu schützen."

Gerichts oft nicht bekannt sei. Auch könnte es sein, dass sich dieser ändere, ohne dass der Anwalt oder die Parteien hiervon erfahren. Dabei ist jedoch zu berücksichtigen, dass es derzeit schon Verfahren gibt, bei denen die Schlüsselverwaltung vereinfacht wird. Hierzu gehört das bereits beschriebene Verfahren der Klageeinreichung über ein elektronisches Gerichtspostfach[746] oder – künftig – das Projekt S.A.F.E.[747]

Es würde sich zudem – falls das Bürgerportalgesetz verabschiedet werden würde – in Zukunft anbieten, dass sich Gerichte, Anwälte und Parteien bei einem Bürgerportaldiensteanbieter registrieren. Der Entwurf zum Bürgerportalgesetz sieht einen Postfach- und Versanddienst vor, in welchem die Vertraulichkeit von Nachrichten standardmäßig gewährleistet wird.[748] Eine manuelle Beschaffung des öffentlichen Schlüssels (etwa aus einem Verzeichnisdienst) wäre hierbei nicht erforderlich, da die Kenntnis der entsprechenden De-Mail-Adresse genügte. Allerdings handelt es sich bei dieser Variante – anders als bei den o.g. Verfahren – hier nur um eine Leitungsverschlüsselung der Transportwege zwischen Teilnehmern und Bürgerportaldiensteanbietern. Während bei einer Ende-zu-Ende-Verschlüsselung lediglich Sender und Empfänger die Information im Klartext kennen, gilt dies hier auch für den Bürgerportaldiensteanbieter.

Wesentlich ist, dass die Information zwischenzeitlich bei einem Dritten im Klartext vorliegt und dort prinzipiell eingesehen werden kann – sofern nicht entsprechende Schutzmaßnahmen vorgesehen sind. Vor diesem Hintergrund ist eine Ende-zu-Ende-Verschlüsselung erforderlich. Der Postfach- und Versanddienst eines Bürgerportaldiensteanbieters wird die Ende-zu-Ende-Verschlüsselung zulassen, diesen Dienst aber nicht selbst anbieten.[749] Die Anwender haben sich in diesem Fall selbst um die Erzeugung und Beschaffung kryptographischer Schlüssel zu kümmern. Zur Unterstützung soll der Diensteanbieter jedoch nach § 7 BPG-E auf ausdrückliches Verlangen des Nutzers die für die Verschlüsselung von Nachrichten an den Nutzer notwendigen Informationen in einem Verzeichnisdienst veröffentlichen müssen. Es bleibt also festzuhalten, dass einer Ergänzung des § 130a ZPO nichts im Wege stehen würde.

7.1.2 Qualifizierte elektronische Signatur

§ 130a Abs. 1 Satz 2 ZPO schreibt vor, dass die Klageschrift mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen werden soll. Sie soll also der elektronischen Form des § 126a BGB entsprechen.

---

[746] Vgl. hierzu Abschnitt 2.3.1.1.

[747] Vgl. hierzu *Bund-Länder-Kommission*, 2007.

[748] Vgl. § 5 Abs. 3 BPG-E: Nach der Begründung wird die Vertraulichkeit der Nachricht derart gewährleistet, dass die Nachricht vom Diensteanbieter verschlüsselt übermittelt wird, so dass sie auf dem Transportweg nicht ausgespäht und auch nicht spurenlos verändert werden kann. Vgl. hierzu auch Abschnitt 4.3.6.

[749] *Roßnagel* et al., DuD 2009, 230.

7.1.2.1 Rechtsprechung zum Schriftformerfordernis

Mit der Soll-Vorschrift hat sich der Gesetzgeber an § 130 Nr. 6 ZPO und der dazu ergangenen Rechtsprechung zum Unterschriftserfordernis bei bestimmenden Schriftsätzen orientiert.[750] Die §§ 129, 130 Nr. 6 ZPO sehen für bestimmende[751] und vorbereitende Schriftsätze[752] vor, dass sie die Unterschrift der Person, die den Schriftsatz verantwortet hat, enthalten soll. Entgegen dem Wortlaut „soll“ hat die Rechtsprechung schon früh bei bestimmenden Schriftsätzen die eigenhändige und handschriftliche Unterschrift der Partei oder ihres Prozessbevollmächtigten als zwingendes Wirksamkeitserfordernis erachtet.[753] Von diesem Unterschriftserfordernis hat sie jedoch im Laufe der Zeit wiederum zahlreiche Ausnahmen zugelassen. Zunächst hat sie Telegramme[754] und Telex[755] zugelassen, dann das Fax[756] und schließlich das Computerfax.[757] Bei Telegrammen und Telex ließ sie die maschinenschriftliche Wiedergabe des Namenszuges am Ende des Textes genügen. Bei der Übermittlung per Fax erachtete die Rechtsprechung die Wiedergabe der Unterschrift in der bei Gericht ankommenden Kopie als ausreichend an und beim Computerfax ließ sie eine eingescannte Unterschrift genügen. Weil die Rechtsprechung zu Wertungswidersprüchen und einer völligen Schieflage bei den Formerfordernissen geführt hat, wurde sie von einem Großteil der Literatur kritisiert.[758]

Mit dem Formvorschriftenanpassungsgesetz hat der Gesetzgeber den Wertungswiderspruch bedauerlicherweise nicht aufgelöst. Im Gegenteil: Er hat den Widerspruch sogar noch vertieft. Statt sich zu entscheiden, ob für bestimmende Schriftsätze die Schriftform eine zwingende Wirksamkeitsvoraussetzung sein soll oder nicht, hat er es bei dem bisherigen Wortlaut des § 130 Nr. 6 1. Hs. ZPO (soll) belassen und in § 130 Nr. 6 2. Hs. ZPO bestimmt, dass bei Telekopien die Wiedergabe der Unterschrift in der Kopie genügt. Den Begriff der Telekopie hat er dabei definiert als die Übermittlung durch einen Telefaxdienst. Hierunter soll sowohl die Übermittlung per Fax als auch die per Computerfax fallen.[759] Damit besteht also nach wie vor die eigenartige Situation, dass nach § 130 Abs. 6 1. Hs. ZPO in Verbindung mit der

---

750 *Dästner*, NJW 2001, 3470.

751 Bestimmende Schriftsätze sind Schriftsätze, welche ein Verfahren einleiten, z.B. § 253 Abs. 2 ZPO, fortsetzen, z.B. § 250 ZPO, inhaltlich ändern, z.B. §§ 261 Abs. 2, 263 ZPO oder beenden, z.B. § 269 ZPO.

752 Vorbereitende Schriftsätze sind im Gegensatz zu bestimmenden Schriftsätzen schriftliche Erklärungen der Parteien, welche ohne unmittelbar prozessgestaltende Wirkung der Vorbereitung und der Erleichterung dienen.

753 Hierzu umfassend *Vollkommer*, 1973, 146 ff.; *Vollkommer*, in: *Brambring/Medicus/Vogt* (Hrsg.), Festschrift für Horst Hagen, 49 ff.

754 RGZ 139, 45 (48); BSGE 1, 243 (245); BAG, NJW 1971, 2190 (2191); BGH, NJW 1981, 1618; BGH, NJW 1983, 1498; BGH, NJW 1982, 1470.

755 BGH, GRUR 1955, 29.

756 LAG Hamm, NJW 1988, 3286; BAG, NJW 1989, 1822.

757 GmS-OGB, NJW 2000, 2340.

758 *Zöller*, ZPO, § 130 Rn. 5; *Heinemann*, 2002, 338 f.; *Stadler*, ZZP 2002, 418.

759 Vgl. hierzu BT-Drs. 14/4987, 23. Zur Kritik an dieser missverständlichen Formulierung *Stadler*, ZZP 2002, 413. Folglich ist für die Frage, ob eine „Telekopie“ vorliegt, der Übertragungsweg, nämlich die Benutzung des öffentlichen Telekommunikationsnetzes und nicht die Benutzung eines bestimmten Geräts beim Absender oder Empfänger maßgeblich. Dazu *Dästner*, NJW 2001, 3470.

dazu ergangenen Rechtsprechung bei schriftlicher Einreichung grundsätzlich eine eigenhändige Unterschrift erforderlich ist, bei der Übermittlung per Fax oder Comupterfax dagegen die Wiedergabe der Unterschrift in Kopie genügt.

7.1.2.2 Folgerungen für § 130a ZPO

Entsprechend § 130 Nr. 6 1. Hs. ZPO hat der Gesetzgeber im Formvorschriftenanpassungsgesetz dann auch § 130a ZPO als Soll-Vorschrift ausgestaltet. In einer Erklärung des Vermittlungsausschusses,[760] die in der abschließenden Beratung des Bundesrates vom Berichterstatter zu Protokoll gegeben wird, heißt es hierzu: „Der Vermittlungsausschuss geht davon aus, dass auch die Formvorschrift in § 130a Abs. 1 ZPO und in den anderen Prozessordnungen für bestimmende Schriftsätze als Muss-Vorschrift zu interpretieren ist und lediglich in besonderen Fällen – wie bei der höchstrichterlichen Rechtsprechung zu § 130 ZPO herausgebildet – von einer qualifizierten elektronischen Signatur abgesehen werden kann, insbesondere um flexibel auf technische Entwicklungen reagieren zu können.“[761] Das heißt also, dass § 130a ZPO grundsätzlich als Muss-Vorschrift auszulegen ist.[762]

Mit dem Formvorschriftenanpassungsgesetz hätte der Gesetzgeber für eine Klarstellung sorgen müssen. Dabei hätte er richtigerweise sowohl § 130 Nr. 6 als auch § 130a ZPO – zumindest für bestimmende Schriftsätze – als Muss-Vorschrift ausgestalten sollen und § 130 Nr. 6 2. Hs. ZPO nicht einfügen dürfen.

Die Rechtsprechung, die Ausnahmen von dem Schriftformerfordernis zugelassen hat, will sich Kommunikationstechniken nicht verschließen, dem Rechtssuchenden die volle Ausschöpfung der Frist ermöglichen und ihm einen möglichst gleichen Zugang zum Recht gewähren.[763] Um den Urheber einer schriftlichen Prozesshandlung zu identifizieren und dessen unbedingten und verantwortungsrechtlichen Einreichungswillen zu dokumentieren, erachtet sie bei modernen Kommunikationsmitteln die oben genannten Anforderungen (bei einem Fax die Wiedergabe der Unterschrift auf der Kopie und bei einem Computerfax die eingescannte Unterschrift) für

760 Auch der Bundesrat wollte in § 130a ZPO die Ausgestaltung als Muss-Vorschrift. Er hatte deswegen den Vermittlungsausschuss angerufen.

761 Niederschrift der 765. Sitzung des Bundesrates vom 22.6.2001, PlPr. 765, 322.

762 In diesem Sinne ist auch der Entscheidung des Bundesgerichtshofes vom 14.1.2010 (BGH, MDR 2010, 653) zuzustimmen. Der Bundesgerichtshof stellt mit seiner Entscheidung klar, dass § 130a Abs. 1 Satz 2 ZPO für bestimmende Schriftsätze nicht nur eine Ordnungsvorschrift enthält. Bestimmende Schriftsätze müssen vielmehr zwingend mit einer qualifizierten elektronischen Signatur versehen sein. So heißt es in der Entscheidung des Bundesgerichtshofes etwa: „(...) Die Rechtsbeschwerde übersieht, dass qualifizierte elektronische Signaturen neben den sonstigen Funktionen der Unterschrift insbesondere auch gewährleisten soll, dass elektronische Dokumente nicht spurenlos manipuliert werden. Auch das spricht in erheblichem Umfang dafür, § 130a Abs. 1 Satz 2 ZPO bei bestimmenden Schriftsätzen grundsätzlich als Muss-Vorschrift zu verstehen (...).“ Für eine Auslegung als Muss-Vorschrift plädieren des Weiteren *Heinz* et al., ZPO, § 130a Rn. 2; *Dästner*, NJW 2001, 3470. Dagegen allerdings *Zöller*, ZPO, § 130 Rn. 5; *Heinemann*, 2002, 338 f.; *Stadler*, ZZP 2002, 418.

763 GemS-OGB, NJW 2000, 2340.

ausreichend.[764] Diese Anforderungen sind aber weder geeignet, eine sichere Identifizierung zu ermöglichen, noch lässt sich mit ihnen ein Einreichungswille dokumentieren.[765] Konsequenterweise müsste man daher auf diese Vorgaben ganz verzichten. Für den hier interessierenden Bereich der E-Mail-Kommunikation würde dies bedeuten, dass jede Klage mittels einfacher E-Mail eingereicht werden könnte. E-Mails sind heute zu einem Massenkommunikationsmittel geworden. Die überwiegende Zahl der Haushalte verfügt heute über einen Internetanschluss.[766] Wenn man einfache E-Mails als Wirksamkeitserfordernis für bestimmende Schriftsätze ausreichen lassen würde, würde man dem Bürger zwar schnell Zugang zum Recht gewähren. Um anderen Personen zu schaden oder um sich einen Spass zu machen, könnten Klageschriften aber leicht unter einem falschen Namen bei Gericht eingehen.[767] Damit würden nicht nur erhebliche Kosten für den Betroffenen entstehen; das informationelle Selbstbestimmungsrecht der Bürger wäre auch beeinträchtigt. Die Gerichte würden eine Akte anlegen und die Daten an den vermeintlich bezeichneten Gegner weiterübermitteln. Zum Teil wird geltend gemacht, dass eine etwa versehentlich eingereichte oder in böser Absicht eingereichte Klage dann unbeachtet bleiben kann, wenn das Gericht Anhaltspunkte für eine fehlende Authentizität oder Ernsthaftigkeit der Eingabe erkennt.[768] In diesem Fall könnte der scheinbare Urheber benachrichtigt werden und die Kosten könnten dem tatsächlichen Urheber aufgebürdet werden. Hiergegen spricht jedoch zum einen, dass in diesem Fall der Schaden bereits eingetreten ist und zum anderen, dass es fast ausgeschlossen ist, den wahren Urheber ausfindig zu machen.

Vor diesem Hintergrund ist es erforderlich, § 130a ZPO zumindest für bestimmende Schriftsätze als Muss-Vorschrift auszugestalten und andere Formen als die Schriftform und die qualifizierte elektronische Signatur nicht zuzulassen. Dies würde sich positiv auf den Datenschutz in der Justiz auswirken und würde mit Blick auf die unterschiedliche Rechtsprechung letzten Endes auch zu mehr Rechtssicherheit beitragen. Der Zugang zu Gericht würde überdies auch nicht gesondert erschwert. Immer mehr Anwälte verfügen über eine qualifizierte elektronische Signatur. Der elektronische Personalausweis wird zudem in Zukunft über eine Signaturfunktion verfügen.[769] Die qualifizierte elektronische Signatur wird sich daher langfristig in der Bevölkerung verbreiten. Zudem wäre als Alternative auch noch die Einreichung mittels des herkömmlichen – unterschriebenen – Schriftsatzes möglich.

---

764 BVerwG, NJW 1995, 2121; BSG, NJW 1997, 1254; BGH, NJW 1994, 2097.

765 Der Bundesgerichtshof (BGH, MDR 2010, 653) sieht hierin jedoch wohl keinen Widerspruch.

766 Im Jahr 2008 haben 68,7 Prozent der deutschen Haushalte über einen Internetzugang verfügt, vgl. *Statistisches Bundesamt*, Private Haushalte in der Informationsgesellschaft – Nutzung der Informations- und Kommunikationstechnlogie, H 1.2.

767 Aufgrund der Gefahr von Fälschungen erachten *Laghzaoui/ Wirges*, AnwBl 1999, 259 eine Klageerhebung per einfacher E-Mail nicht für zulässig.

768 Vgl. hierzu *Zöller*, ZPO, § 130 Rn. 21 für Brief und Fax.

769 Vgl. hierzu Abschnitt 4.3.5.1.

7.2 E-Zustellungen des Gerichts

Wenn eine Klageschrift eingereicht ist, hat sie der Richter gemäß § 271 Abs. 1 ZPO zuzustellen.[770] Die ZPO sieht eine „konfrontative“ elektronische Zustellung derzeit nicht vor. § 174 Abs. 3 und 1 ZPO gestattet lediglich eine „kooperative“ elektronische Zustellung, also eine solche gegen Empfangsbekenntnis. Es handelt sich hier um eine vereinfachte Form der Zustellung ohne die Inanspruchnahme eines Postunternehmens, des Gerichtsvollziehers oder einer Behörde.[771] Die Zustellung ist bewirkt, wenn der Zustellungsempfänger ein Empfangsbekenntnis zurückgesandt hat.[772] Eine kooperative elektronische Zustellung kann nach § 174 Abs. 3 und 1 ZPO an einen Anwalt, einen Notar, einen Gerichtsvollzieher, einen Steuerberater, eine Behörde, eine Körperschaft oder eine Anstalt des öffentlichen Rechts erfolgen. Darüber hinaus ist nach § 174 Abs. 3 und 1 ZPO auch eine elektronische Zustellung gegen Empfangsbekenntnis an eine sonstige Person zulässig, bei welcher aufgrund ihres Berufes von einer erhöhten Zuverlässigkeit ausgegangen werden kann. Mit dieser Formulierung wollte der Gesetzgeber es der gerichtlichen Praxis überlassen, welche weiteren Berufsgruppen an dieser Zustellungsform teilnehmen können.[773] Hierunter dürften Berufsgruppen gehören, die wie die ausdrücklich in § 174 Abs. 1 ZPO genannten Personen standesrechtlich gebunden sind, wozu etwa Wirtschaftsprüfer, Patentanwälte oder die in § 5 Abs. 2 VwZG aufgeführten Personen und Gesellschaften gehören.[774] Neben den in Abs. 1 Genannten kann eine elektronische Zustellung auch an andere Verfahrensbeteiligte erfolgen. Voraussetzung hierfür ist, dass sie der Übermittlung ausdrücklich zugestimmt haben. Diese Vorschrift überrascht, vergleicht man sie mit der postalischen Zustellung nach § 174 Abs. 1 ZPO und der Zustellung mittels Telefax nach § 174 Abs. 2 ZPO. Denn während die Zustellung nach § 174 Abs. 1 und 2 ZPO mittels Empfangsbekenntnis nur bei einem zuverlässigen Personenkreis möglich ist, sieht § 174 Abs. 3 ZPO vor, dass eine Zustellung an jedermann erfolgen kann, sofern er nur damit einverstanden ist. Die Erweiterung wurde aufgrund einer Anregung des Bundesrates eingefügt.[775] Damit sollte der Rechtsverkehr gefördert werden und eine Gleichstellung mit § 130a ZPO, welcher auf der Eingangsseite einem unbeschränkten Personenkreis eine elektronische Übermittlung gestattet, erreicht werden.[776] In der Kommentarliteratur wird die weite Fassung des § 174 Abs. 3 ZPO kritisiert.[777] Sie führe dazu, dass die Empfangsbekenntnisse häufig nicht an das Gericht zurückgesandt werden würde. Den Gerichten wird daher empfohlen, von der Vorschrift keinen Gebrauch zu machen.[778] Bei der Zustellung eines Richters auf elektronischem Wege ergeben sich aus datenschutzrechtlicher Sicht wiederum Fragestellungen, die die Vertraulichkeit,

[770] Erst dann ist die Sache rechtshängig, §§ 261 Abs. 1, 253 Abs. 1 ZPO.
[771] *Zöller*, ZPO, § 174 Rn. 1.
[772] *Schmieszek*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 31.
[773] BT-Drs. 14/4554, 18.
[774] *Stein/Jonas*, ZPO, § 174 Rn. 4.
[775] BT-Drs. 14/4554, 31.
[776] Eine ausdrückliche Zustimmung ist nicht in der bloßen Angabe einer E-Mail Adresse auf dem Briefkopf des betreffenden Verfahrensbeteiligten zu sehen. Siehe hierzu *Hess*, NJW 2002, 2420.
[777] *Baumbach* et al., ZPO, § 174 Rn. 17; *Kampen/Engelhardt*, ArbuR 2003, 244.
[778] *Stein/Jonas*, ZPO, § 174 Rn. 32.

die Authentizität und die Integrität der zu versendenden Daten angehen. Da § 174 Abs. 3 ZPO eine elektronische Zustellung – nach einer Zustimmung – aber an jedermann gestattet, können sich zudem Probleme im Zusammenhang mit der missbräuchlichen Nutzung einer falschen E-Mail-Adresse ergeben.[779]

7.2.1 Verschlüsselung

Im Gegensatz zu § 130a ZPO hat der Gesetzgeber Fragen der Vertraulichkeit bei der Zustellung von elektronischen Dokumenten in der ZPO zufriedenstellend gelöst. § 174 Abs. 3 Satz 3 ZPO schreibt vor, dass das Dokument gegen unbefugte Kenntnisnahme durch Dritte zu schützen ist.[780] Der durch diese Vorschrift geforderte Schutz des elektronischen Dokuments erfordert die geeignete Verschlüsselung des Dokuments.[781] In der Literatur wird diese Regelung kritisiert.[782] Auch einfache unverschlüsselte E-Mails würden den gleichen Schutz wie Brief oder Telefax bieten. Die Regelung hemme den elektronischen Rechtsverkehr. § 174 Abs. 3 Satz 3 ZPO würde ein den Begriffsdschungel des § 130a ZPO und des SigG noch undurchdringlich machender Auswuchs deutscher Überperfektion darstellen.[783] Dass dem nicht entsprochen werden kann, wurde bereits oben dargelegt.

Zudem wird in praktischer Hinsicht geltend gemacht, dass das Gericht zur Zustellung per E-Mail über den öffentlichen Schlüssel des Empfängers verfügen muss und ein allgemeines öffentliches Verzeichnis nicht existiere.[784] Das Anwaltsverzeichnis nach § 31 Abs. 1 BRAO sei in der heutigen Form nicht auf die Aufnahme der öffentlichen Schlüssel vorbereitet.[785] Und die Anbieter von elektronischen Signaturen, die die Verschlüsselungsfunktionen auf der Signaturkarte integrieren würden, würden keine Schlüssel veröffentlichen.[786] Eine Verschlüsselung bei der elektronischen Zustellung sei daher nicht praxistauglich. Auch hierbei würde ein Bürgerportalgesetz jedoch wiederum einen Gewinn bringen. Der Postfach- und Versanddienst nach § 5 BPG-E sieht standardmäßig vor, dass der Transport zwischen den akkreditierten Diensteanbietern verschlüsselt erfolgt. Damit der Bürgerportaldiensteanbieter keine Kenntnis vom Inhalt der Daten nehmen kann, wäre zwar eine Ende-zu-Ende-Verschlüsselung erforderlich. Wie gesehen, wird der Postfach- und Versanddienst eine solche jedoch unterstützen. Um eine Ende-zu-Ende-Verschlüsselung vorzunehmen, könnte dann auf die Daten zurückgegriffen

779 Zur Kritik einer – den Datenschutz nicht tangierenden – fehlenden Hinweispflicht bei § 174 Abs. 3 ZPO vgl. *Lindloff*, 2005, 203 m.w.N.

780 In der Gesetzesbegründung heißt es hierzu: „Das elektronische Dokument belässt den zu übermittelnden Text selbst unverschlüsselt, er bleibt aber auch während der Übermittlung frei leserlich. Um die Vertraulichkeit der Übermittlung und den Schutz darin enthaltener personenbezogener Daten zu sichern, ist das elektronische Dokument in geeigneter Weise gegen unbefugte Kenntnisnahme Dritter zu sichern.“ Siehe hierzu BT-Drs. 14/4554, 19.

781 *Stein/Jonas*, ZPO, § 174 Rn. 31.

782 Vgl. hierzu *Lindloff*, 2005, 206 ff. m.w.N.

783 Vgl. hierzu *Lindloff*, 2005, 206 ff. m.w.N.

784 *Lindloff*, 2005, 206.

785 *Lindloff*, 2005, 207.

786 *Lindloff*, 2005, 207.

werden, die in dem in § 7 BPG-E genannten Verzeichnis enthalten sind. Auch das Projekt S.A.F.E. sieht im Übrigen standardmäßig eine Ende-zu-Ende-Verschlüsselung vor, so dass sich das Gericht den öffentlichen Schlüssel des Empfängers nicht aufwändig beschaffen muss.

7.2.2 Qualifizierte elektronische Signatur

Für die elektronische Zustellung vom Gericht an die Verfahrensbeteiligten schreibt § 174 Abs. 3 Satz 3 ZPO vor, dass das Dokument für die Übermittlung mit einer elektronischen Signatur zu versehen ist. Der Gesetzgeber wollte es mit dieser Formulierung der absendenden Stelle überlassen, welche der drei Arten der in § 2 SigG genannten elektronischen Signaturen gewählt wird. Nach der Gesetzesbegründung[787] soll sich die Auswahl nach der Art des zu übermittelnden Dokuments richten. An dieser Vorschrift ist zu kritisieren, dass sie zum einen dem Geschäftsstellenbeamten eine hohe Verantwortung auflädt. So muss er bei jedem einzelnen Dokument prüfen, welche Form die richtige ist. Im Zweifel wird er sich – da schneller und einfacher zu handhaben – für die einfache Signatur entscheiden. Mit dieser kann aber nicht einmal die Authentizität des elektronischen Dokuments nachgewiesen werden. Es wäre daher wünschenswert, wenn § 174 Abs. 3 Satz 3 ZPO vorsehen würde, dass das Dokument mit einer qualifizierten elektronischen Signatur zu versehen ist.

7.2.3 Zuverlässige Identifizierung

Damit die zuzustellenden Schriftstücke, etwa die Klageschrift, nicht an Unbefugte übermittelt werden, ist es notwendig, dass das Gericht seine Kommunikationspartner kennt. Eine E-Mail-Adresse kann auf einfache Weise verfälscht werden. In der elektronischen Welt und insbesondere auch im elektronischen Gerichtsverfahren sind daher erhöhte Anforderungen an eine vorherige zuverlässige Registrierung der Kommunikationspartner zu stellen. Für eine zuverlässige Registrierung kommt einmal wiederum die Kommunikation innerhalb eines Bürgerportals in Betracht. Einen De-Mail-Account bekommen nämlich nur diejenigen, die sich im Rahmen einer Erstregistrierung zuverlässig identifiziert haben. Die Voraussetzungen für eine zuverlässige Registrierung ergeben sich aus § 3 Abs. 2 und 3 BPG-E und wurden bereits dargestellt.[788] Der Regierungsentwurf zum Bürgerportalgesetz vom 20.2.2008[789] sieht in Artikel 2 unter anderem[790] auch eine Änderung bei der Zustellung in der ZPO vor.[791] So ist vorgesehen, in § 174 Abs. 3 ZPO folgenden Satz anzufügen: „Die Übermittlung kann auch über ein Bürgerportal im Sinne von § 1 Bürgerportalgesetz erfolgen.“ Diese Änderung wäre erfreulich, da mit ihr das Bürgerportal als Übertragungsweg für die Übermittlung elektronischer

787 BT-Drs. 14/4554, 19.
788 Vgl. hierzu Abschnitt 4.3.6.2.
789 BT-Drs. 16/12598.
790 Darüber hinaus sollen nach Artikel 3 Zustellungen von Bundesbehörden durch die Einfügung eines § 5a VwZG über Bürgerportale ermöglicht werden.
791 BT-Drs. 16/12598, 12.

Dokumente ausdrücklich anerkannt werden würde.[792] Die amtliche Zustellbestätigung durch den beliehenen akkreditierten Bürgerportalbetreiber wäre dabei ein öffentliches Dokument, dessen Echtheit und dessen Inhalt nach §§ 371a Abs. 2, 415 und 437 ZPO vermutet werden würde.[793] Weiter kommt eine Registrierung nach dem S.A.F.E.-Konzept, ggf. in Verbindung mit dem Bürgerportaldienst in Betracht. Letztlich ist auch eine Registrierung mittels des elektronischen Personalausweises möglich. In diesem Fall wäre das entsprechende Gericht selbst Diensteanbieter nach dem PAuswG.[794] Das Gericht würde dem Anwalt oder der Naturpartei ein Berechtigungszertifikat übermitteln, um Zugriff auf die im elektronischen Personalausweis gespeicherten Daten zu erlangen.[795] In diesem müsste das Gericht Angaben über seine Identität, also zum Beispiel Amtsgericht Mainz, machen.[796] Außerdem müsste es die begehrten Datenkategorien mitteilen.[797] Für eine zuverlässige Registrierung wäre es hier ausreichend, wenn das Gericht um die Übermittlung des Vor- und Nachnamen[798] und des Wohnortes[799] ersucht. Als Zweck müsste das Gericht die elektronische Zustellung in einem näher bezeichneten Verfahren mit Aktenzeichen angeben.[800] Letztlich müsste es auch die im Streitfall zuständige Datenschutzaufsicht benennen[801] sowie den letzten Tag der Gültigkeitsdauer des Berechtigungszertifikats.[802] Wenn der Personalausweisinhaber nach § 18 Abs. 4 PAuswG nun die begehrten Informationen freigibt durch die Eingabe einer Geheimnummer wäre zumindest sichergestellt, dass die Klageschrift an den zutreffend ermittelten Verfahrensgegner übermittelt wird.

Erfolgt die elektronische Zustellung verschlüsselt, mittels einer qualifizierten elektronischen Signatur und wurde der Empfänger zuvor zuverlässig registriert, wäre dies im Vergleich zu einer papiergebundenen sogar datenschutzfreundlicher. So kam es in der Vergangenheit etwa vor, dass die Post der Amtsgerichte unverschlossen oder unzureichend verklebt zugestellt wurde.[803]

---

792 BT-Drs. 16/12598, 32.

793 *Roßnagel* et al., DuD 2009, 732.

794 § 2 Abs. 3 PAuswG.

795 § 2 Abs. 4 Satz 1 und 2 PAuswG.

796 § 18 Abs. 4 Satz 2 Nr. 1 PAuswG.

797 § 18 Abs. 4 Satz 2 Nr. 2 PAuswG.

798 § 18 Abs. 3 Satz 2 Nr. 1 und 2 PAuswG.

799 § 18 Abs. 3 Satz 2 Nr. 6 PAuswG.

800 § 18 Abs. 4 Satz 2 Nr. 3 PAuswG.

801 § 18 Abs. 4 Satz 2 Nr. 4 PAuswG.

802 § 18 Abs. 4 Satz 2 Nr. 4 PAuswG.

803 Vgl. etwa *LfD Baden-Württemberg*, 18. Tätigkeitsbericht, Tz. 4.3, wonach ein Amtsgericht einer Petentin immer wieder Schreiben, in denen es unter anderem um die Unterbringung ihres Sohnes in einer geschlossenen Anstalt ging, durch die Post in unverschlossenen oder unzureichend verschlossenen Umschlägen zustellen ließ.

7.3 E-Mitteilungen des Gerichts

Wie bereits gesehen,[804] erachtet die ZPO an verschiedenen Stellen die formlose Mitteilung an die Verfahrensbeteiligten als ausreichend. Hierbei ist anerkannt, dass auch eine elektronische Übermittlung zulässig ist. In der ZPO findet sich an keiner Stelle eine Regelung, wie die Übermittlung von derartigen Dokumenten zu erfolgen hat. In der Literatur wird vertreten, dass in diesen Fallgestaltungen die Übermittlung durch eine einfache, d.h. unverschlüsselte und unsignierte E-Mail, erfolgen könne.[805] So sei die Wahrscheinlichkeit, dass eine vom Gericht an die Verfahrensbeteiligten abgesandte E-Mail von Dritten abgefangen und verändert werde, als gering einzustufen. Auch handele es sich bei den formlosen Erklärungen um weniger bedeutsame, die für einen Dritten in der Regel uninteressant und inhaltlich kaum nachvollziehbar seien. Letztlich sei auch die Gefahr einer Identitätstäuschung denkbar gering und der Schaden überdies auch nicht irreparabel.[806] Dieser Ansicht dürfte jedoch zu widersprechen sein. Auch die formlosen Mitteilungen können sensible Inhalte haben. Zum Beispiel kann ein Richter nach § 273 Abs. 2 Nr. 1 ZPO den Parteien die Ergänzung oder die Erläuterung ihrer Vorträge aufgeben.[807] Je nachdem, wie die Fragen des Richters ausgestaltet sind, kann man allein schon anhand daran auf den Tatsachenstoff, den die Parteien dem Gericht mitgeteilt haben, schließen. Hinsichtlich der Sensibilität der in formlosen und förmlichen Mitteilungen des Gerichts enthaltenen personenbezogenen Daten dürfte daher kein großer Unterschied bestehen. Von daher gesehen sind auch für diese Übermittlungen die oben genannten – für förmliche Zustellungen – herausgearbeiteten Anforderungen nötig.

7.4 E-Akteneinsicht

Die Gewährung der Akteneinsicht des Gerichts stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Sie bedarf daher einer gesetzlichen Grundlage. Als Rechtsgrundlage könnte § 16 LDSG einschlägig sein. Der Anwendungsbereich des LDSG ist auf den ersten Blick zwar eröffnet: Eine öffentliche Stelle, nämlich das Gericht, übermittelt personenbezogene Daten nach § 3 LDSG. Allerdings ist der Grundsatz der Subsidiarität zu beachten. §299 ZPO stellt eine Spezialregelung[808] zu den allgemeinen Vorschriften im LDSG dar.[809] Somit ist § 299 ZPO die richtige Ermächtigungsgrundlage für die Gewährung der Akteneinsicht durch das Gericht und nicht § 16 LDSG. § 299 Abs. 3 ZPO regelt die Art und Weise der elektronischen Akteneinsicht. Hinsichtlich der Voraussetzungen

[804] Vgl. hierzu Abschnitt 2.3.1.3.
[805] *Krüger/Bütter*, MDR 2003, 186.
[806] *Krüger/Bütter*, MDR 2003, 186.
[807] Wenn der Richter der Partei hierfür keine Frist gibt, ist eine formlose Mitteilung möglich. Siehe hierzu *Zöller*, ZPO, § 273 Rn. 5.
[808] § 2 Abs. 7 LDSG.
[809] *Stein/Jonas*, ZPO, § 299 Rn. 1.

und des Umfangs der elektronischen Akteneinsicht kann auf das zurückgegriffen werden, was für die herkömmliche Akteneinsicht gilt:

So gibt § 299 Abs. 1 ZPO den Parteien[810] grundsätzlich einen uneingeschränkten Anspruch auf Akteneinsicht.[811] Parteien müssen für eine Einsichtsgewährung kein bestimmtes Interesse darlegen oder glaubhaft machen.

Sie haben auch grundsätzlich einen Anspruch darauf, die gesamten Prozessakten einzusehen.[812] Zu den Prozessakten gehört dabei alles, was in ihnen enthalten ist und was das Gericht im Prozess verwerten will, darf, soll oder zulässig verwertet hat.[813] Damit umfasst das Akteneinsichtsrecht insbesondere auch die beigezogenen Akten des Richters. Entwürfe zu Urteilen, Beschlüssen und Verfügungen, die zu ihrer Vorbereitung gelieferten Arbeiten sowie die Dokumente, die Abstimmungen betreffen, sind dagegen nicht Bestandteil der Akte. Das Einsichtsrecht erstreckt sich daher nicht hierauf. Dies ist in § 299 Abs. 4 ZPO ausdrücklich gesetzlich geregelt. Hinsichtlich des Umfangs des Akteneinsichtsrechts ist zu beachten, dass datenschutzrechtliche Gesichtspunkte keine Aussonderung von bestimmten Teilen einer Prozessakte begründen können. Die Aussonderung von bestimmten Aktenteilen hätte zur Folge, dass diese wegen Art. 103 Abs. 2 GG nicht im Prozess verwendet werden dürften. Eine Verweigerung der Akteneinsicht führt automatisch zur Unverwertbarkeit der entsprechenden Informationen im Prozess.[814] Dementsprechend geht Liebscher zu Recht davon aus, dass den Parteien sämtliche Unterlagen, die zur Entscheidungsgrundlage werden könnten – und damit die gesamte Prozessakte – zugänglich gemacht werden müssen.[815]

Das Einsichtsrecht darf jedoch nicht die Angaben zu den persönlichen und wirtschaftlichen Verhältnissen der gegnerischen Partei im Prozesskostenhilfe-Verfahren umfassen. Früher war diese Frage streitig. Zum Teil wurde vertreten, dass auch diese Unterlagen dem Gegner zur Einsicht zu gewähren sind. So würden die Angaben zu den persönlichen oder wirtschaftlichen Verhältnissen oft einen Sachvortrag enthalten. Art. 103 Abs. 2 GG verbiete es, diesen dem Gegner vorzuenthalten.[816] Auch wurde angeführt, dass der Gegner die wirtschaftlichen Verhältnisse überprüfen können müsse, da mit Hilfe der Prozesskostenhilfe gegen ihn schließlich ein Prozess angestrengt werden könne. Wenn sich ergebe, dass die Angaben zu den persönlichen und wirtschaftlichen Verhältnisse unzutreffend seien, könne der Gegner das Gericht hierauf hinweisen, was zur Verweigerung der Prozesskostenhilfe führen würde. Eine Vertraulichkeit der Prozesskostenhilfe-Unterlagen sei ohnehin nicht gegeben, wenn der Antrag

[810] Hierzu gehören auch der gesetzliche Vertreter, der Verfahrensbevollmächtigte und der Streithelfer nach § 66 ZPO, nicht aber der Streitverkündungsempfänger.

[811] Damit kommt der Gedanke der Parteiöffentlichkeit zum Ausdruck, § 357 ZPO. Im Übrigen dient die Vorschrift vor allem aber auch dem rechtlichen Gehör nach Art. 103 Abs. 2 GG, der Rechtssicherheit und der Prozesswirtschaftlichkeit. Vgl. hierzu *Baumbach* et al., ZPO, § 299 Rn.2.

[812] KG Berlin, NJW 1988, 1738.

[813] *Baumbach* et al., ZPO, § 299 Rn. 9.

[814] BGH, NJW 1952, 305.

[815] *Liebscher*, 1994, 104 ff.

[816] LAG Hamburg, MDR 1982, 527.

auf Prozesskostenhilfe mangels Bedürftigkeit abgewiesen werden würde. Denn spätestens der Ablehnungsbeschluss, der begründet werden müsse, würde dem Gegner zugehen.[817]

Die herrschende Meinung und so auch das Bundesverfassungsgericht und der Bundesgerichtshof waren dagegen der Ansicht, dass das Einsichtsrecht nicht die Unterlagen zu den persönlichen und wirtschaftlichen Verhältnissen umfasse. Denn das Prozesskostenhilfe-Verfahren betreffe nur das Verhältnis zwischen dem Staat und dem Antragsteller. Der Gegner sei in diesem Verfahren keine Partei. Deshalb könne auch kein Verstoß gegen Art. 103 Abs. 2 GG vorliegen. Das Grundrecht der Partei aus Art. 2 Abs. 1 i.V.m. Art. 1 GG verbiete es vielmehr, dem Gegner Einblick in das Beiheft zu gewähren.[818]

Der Gesetzgeber ist der herrschenden Meinung gefolgt. Er hat mit dem Prozesskostenhilfeänderungsgesetz im Jahr 1994[819] in § 117 Abs. 2 Satz 2 ZPO geregelt, dass die Erklärungen zu den persönlichen und wirtschaftlichen Verhältnissen mit den Belegen dem Gegner nur mit Zustimmung der Partei zugänglich gemacht werden dürfen.[820] Gleichzeitig hat er auch mit § 127 Abs. 2 Satz 3 ZPO bestimmt, dass, soweit die Gründe einer Entscheidung Angaben über die persönlichen und wirtschaftlichen Verhältnisse enthalten, sie dem Gegner nur mit Zustimmung der Partei zugänglich gemacht werden dürfen. Der bisherige Streit ist damit überholt. Aufgrund der Änderungen durch das Prozesskostenhilfeänderungsgesetz von 1994 werden die Erklärungen der Partei über ihre persönlichen und wirtschaftlichen und die Vorgänge der Abwicklung der Prozesskostenhilfe heute nicht in die Prozessakte genommen, sondern in ein Beiheft. Bei einer elektronischen Aktenführung, bei der es kein sog. Beiheft gibt, muss beachtet werden, dass das Dokument mit den Prozesskostenhilfe-Unterlagen für den anderen nicht sichtbar ist. Neben den Prozesskostenhilfe-Unterlagen sind vom Akteneinsichtsrecht auch Akten ausgenommen, die der Richter beigezogen hat, wenn die Behörde diese lediglich unter der Bedingung der Vertraulichkeit übersandt hat oder wenn es sich um Akten eines Strafverfahrens handelt, bei denen das Ermittlungsverfahren noch nicht abgeschlossen ist.[821]

Dritte, d.h. Antragsteller die weder Parteien, beigetretene Streithelfer noch Prozessbevollmächtigte sind, haben grundsätzlich keinen Anspruch auf Akteneinsicht. Nur wenn die Parteien eingewilligt haben oder der Dritte ein rechtliches Interesse nach § 294 ZPO glaubhaft gemacht hat, kann der Vorstand des Gerichts (Präsident des Oberlandesgerichts, Landgerichtspräsident oder Amtsgerichtsdirektor) ihnen die Einsicht in die Akten nach § 299 Abs. 2 ZPO gestatten. Rein wirtschaftliche oder gesellschaftliche Interessen stellen dabei kein rechtliches Interesse im Sinne von § 299 Abs. 2 ZPO dar. Erforderlich ist vielmehr ein Bezug zum

817 OLG Celle, MDR 1982, 761; OLG Frankfurt, JurBüro 1982, 1259.

818 BGHZ 89, 65; BVerfG, NJW 1991, 2078. Davor wurde diese Ansicht etwa auch vertreten vom OLG Düsseldorf, FamRZ 1984, 388 oder vom OLG Köln, MDR 1985, 328.

819 Prozesskostenhilfeänderungsgesetz vom 10.10.1994, BGBl. 1994 I, 364.

820 In der Praxis kommt es vor, dass der Schriftsatz des Antragstellers neben der nach § 117 Abs. 1 Satz 2 ZPO erforderlichen Darstellung des Streitverhältnisses auch Angaben zu den persönlichen und wirtschaftlichen Verhältnissen enthält. In diesem Fall darf der Schriftsatz an den Gegner versandt werden, da dann von einer Einwilligung in die Weiterleitung an den Gegner ausgegangen werden kann.

821 *Baumbach* et al., ZPO, § 299, Rn. 9.

Streitstoff der Akten.[822] Bei seiner Ermessensentscheidung hat der Vorstand des Gerichts auch das informationelle Selbstbestimmungsrecht der Parteien zu beachten.[823] Insbesondere ist in diesem Zusammenhang zu prüfen, ob dem rechtlichen Interesse nicht durch eine auf bestimmte Aktenteile begrenzte Einsicht entsprochen werden kann.[824]

Bei papiergebundener Aktenführung ist anerkannt, dass die Akten grundsätzlich in der Geschäftsstelle eingesehen werden können.[825] Die Aufsicht hierüber führt der Urkundsbeamte der Geschäftsstelle. Ein Anspruch auf Zusendung der Akte besteht nicht.[826] § 299 Abs. 3 Satz 1 und 2 ZPO nennen statt dessen nun verschiedene Varianten für eine elektronische Akteneinsicht: Erteilung eines Aktenausdrucks, Wiedergabe auf einem Bildschirm, Übermittlung von elektronischen Dokumenten und die Online-Einsicht von zu Hause aus. Mit der Erteilung eines Aktenausdrucks ist gemeint, dass der Geschäftsstellenbeamte das gewünschte Dokument ausdruckt und es der Partei dann übergibt. Dabei kann es sich um ein einzelnes Dokument, etwa eine per E-Mail eingegangene Replik der gegnerischen Partei handeln oder um den ganzen Inhalt der elektronisch geführten Akte. Bei der Variante „Wiedergabe auf einem Bildschirm“ werden bei dem aktenführenden Gericht Rechner aufgestellt, an denen die elektronischen Dokumente eingesehen werden können. Die Übermittlung von elektronischen Dokumenten meint das Übermitteln per E-Mail.[827] Die Online-Einsicht umfasst den gesamten Inhalt der Akten und ermöglicht eine Einsichtnahme von zu Hause aus. Da § 299 ZPO bei der elektronischen Akteneinsicht nicht nach Parteien und Dritten unterscheidet und in dieser Vorschrift auch keine anderweitigen Möglichkeiten für eine elektronische Akteneinsichtsgewährung genannt werden, gelten die genannten Varianten sowohl für Parteien als auch für Dritte.[828]

7.4.1 Aktenausdruck und Wiedergabe auf einem Bildschirm

Aus datenschutzrechtlicher Sicht ist die Einsichtsgewährung durch einen Aktenausdruck als positiv zu beurteilen. Denn sie erlaubt es, dass nur bestimmte Teile einer Akte ausgedruckt und weitergegeben werden, nämlich die, die die Partei oder Dritte gerade benötigen. Bei der herkömmlichen Aktenführung ist dies nicht möglich. Die Papierakte ist zusammengebunden. Der Partei oder Dritten muss daher bei der herkömmlichen Aktenführung immer die ganze Akte zur Einsicht überlassen werden. Insofern kann diese Form der Akteneinsicht als datenschutzfreundlicher angesehen werden als die herkömmliche.

Bei der Wiedergabe auf einem Bildschirm ist es aus datenschutzrechtlicher Sicht erforderlich, dass die Parteien immer nur diejenigen Teile auf dem Bildschirm einsehen können, die nicht den oben genannten Beschränkungen unterliegen. Hierzu ist es notwendig, dass der

822 Vgl. hierzu *Zöller*, ZPO, § 299 Rn. 6 b m.w.N.
823 Vgl. hierzu *Zöller*, ZPO, § 299 Rn. 6 b m.w.N.
824 Vgl. hierzu *Zöller*, ZPO, § 299 Rn. 6 b m.w.N.
825 BSG, MDR 1977, 1051; OLG Brandenburg, FamRZ 2004, 388.
826 OLG Stuttgart, MDR 1958, 43.
827 BT-Drs. 15/4067, 33.
828 Anders wohl *Schmieszek*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 40.

Geschäftsstellenbeamte die jeweiligen Stellen, etwa die Klageschrift, vor der Einsichtnahme auf dem Bildschirm aufruft. Ein Blättern in der elektronischen Akte selbst darf der Partei oder Dritten nur dann erlaubt werden, wenn sichergestellt ist, dass sie nicht auf andere – nicht für sie bestimmte – Dokumente, etwa das Beiheft im Prozesskostenhilfe-Verfahren, zugreifen können und den Akteninhalt nicht verändern können.[829] Sind diese Voraussetzungen nicht gegeben, darf nur der jeweils zuständige Geschäftsstellenbeamte in der elektronischen Akte blättern.

Bei der Gewährung der Akteneinsicht durch Aktenausdruck und durch Wiedergabe auf einem Bildschirm wäre zu überlegen, ob es zulässig ist, einen bestimmten Geschäftsstellenbeamten im Gericht damit zu betrauen, allen Parteien oder Dritten, die vor Ort in die elektronisch geführten Akten Einsicht nehmen wollen, Einsicht durch Wiedergabe auf einem Bildschirm zu ermöglichen. Man würde also bei Gericht eine zentrale Stelle schaffen, bei welcher Akteneinsicht durch Wiedergabe auf einen Bildschirm gewährt werden könnte. Dafür würde sprechen, dass dadurch die für die Bearbeitung des Verfahrens zuständigen Geschäftsstellenbeamten entlastet würden und der Publikumsverkehr bei einer Stelle konzentriert werden könnte. Dagegen spräche jedoch, dass man dem jeweiligen Geschäftsstellenbeamten, welcher die Akteneinsicht gewährt, Zugriffsrechte auf alle elektronisch geführten Akten erteilen müsste, was mit großen Missbrauchsrisiken verbunden wäre. Außerdem würden sich bei den Terminals Warteschlangen bilden, was nicht bürgerfreundlich und mit den Zielen der elektronischen Justiz nicht vereinbar ist. Eine derartige Form der Akteneinsichtsgewährung sollte daher nicht gestattet werden.

Der Gesetzesbegründung ist zu entnehmen, dass die Wiedergabe auf einem Bildschirm nicht notwendig in den Räumen der aktenführenden Stelle gewährt werden muss. Vielmehr – so heißt es weiter – kann dem Betroffenen, wenn er nicht im Einzugsbereich dieser Stelle wohnt, eine Akteneinsicht auch dadurch gewährt werden, dass die entsprechenden elektronischen Dokumente an die in seinem Wohnsitz nächstgelegene Verwaltungsbehörde oder an das nächstgelegene Gericht übermittelt werden und die Akteneinsicht durch Wiedergabe auf einem Bildschirm dort gewährt wird.[830] Auch das Grundbuchrecht sieht die Wiedergabe auf einem Bildschirm in das elektronisch geführte Grundbuch vor. § 132 GBO bestimmt diesbezüglich, dass die Einsicht auch bei einem anderen als dem Grundbuchamt genommen werden kann, das dieses Grundbuch führt. Aus datenschutzrechtlicher Sicht wäre es nun wünschenswert gewesen, der Gesetzgeber hätte auch in der ZPO entsprechendes im Gesetzestext selbst zum Ausdruck gebracht, zumal die Gesetzesbegründung in der ZPO weiter geht als § 132 GBO. Während § 132 GBO nämlich nur die Einsichtnahme bei einem Grundbuchamt gestattet, sieht die amtliche Begründung zu § 299 ZPO vor, dass eine Einsichtnahme bei jedem anderen Gericht und auch bei einer Verwaltungsbehörde möglich ist.[831] Angesichts dessen, dass die Entfernung zum nächstgelegenen Amts- oder Landgericht nicht größer sein dürfte als die zur nächstgelegenen Verwaltungsbehörde und demgegenüber das Missbrauchspotential mit einer Einsichtnahme in

[829] Bei der Grundbucheinsicht ist die Gewährung durch Aktenausdruck und Wiedergabe auf einem Bildschirm in § 79 GBV gesondert geregelt.

[830] BT-Drs. 15/4067, 33.

[831] BT-Drs. 15/4067, 33.

jeder möglichen Verwaltungsbehörde sehr hoch sein dürfte, ruft die Regelung jedoch unter dem Gesichtspunkt der informationellen Gewaltenteilung[832] ohnehin Bedenken hervor. Wenn man sich trotz dieser Bedenken jedoch für eine derartige Form der Einsichtgewährung entscheidet, wäre es zumindest notwendig, die Bediensteten, die bei den Verwaltungsbehörden dafür zuständig sind, vorher genau zu bestimmen und ihnen eine elektronische Kennung zu geben.

Missbrauchsrisiken sind bei den beiden dargestellten Formen der Akteneinsicht zudem dergestalt denkbar, dass jemand vortäuscht, selbst Partei oder ein zur Akteneinsicht befugter Dritter zu sein und sich so einen Aktenausdruck oder die Einsicht auf den Inhalt der Akten am PC des Geschäftsstellenbeamten erschleicht. Diese Missbrauchsrisiken sind im Wesentlichen identisch zu denen der herkömmlichen papiergebundenen Akteneinsicht. Sie können verhindert werden, wenn sich der jeweilige Geschäftsstellenbeamte vor der Einsichtsgewährung den Personalausweis vorzeigen lässt oder ein anderes Dokument, mit welchem die Identität der jeweiligen Person überprüft werden kann.

7.4.2 Übermitteln von elektronischen Dokumenten

Die Übermittlung von elektronischen Dokumenten meint, wie oben gesehen, das Übermitteln per E-Mail.[833] § 299 Abs. 3 Satz 4 ZPO schreibt diesbezüglich vor, dass für die Übermittlung die Gesamtheit der Dokumente mit einer qualifizierten elektronischen Signatur zu versehen ist und gegen unbefugte Kenntnisnahme zu schützen ist. Die unbefugte Kenntnisnahme kann dabei durch eine Verschlüsselung verhindert werden. Die qualifizierte Signatur gewährleistet, dass erkannt werden kann, von wem das Dokument stammt. Auch ist gewährleistet, dass ersichtlich ist, wenn ein Dokument verändert wird. Aus datenschutzrechtlicher Sicht ist dies als positiv zu bewerten. Der Vorgang der Übermittlung ist vertraulich. Die Authentizität und Integrität wird gewährleistet. Allerdings ist nicht berücksichtigt, ob das Dokument zur richtigen Person gelangt. Bei der Einsichtnahme durch Wiedergabe auf einem Bildschirm bei Gericht und bei der Erteilung eines Aktenausdrucks wurde festgestellt, dass sich Missbrauchsrisiken durch die Vorlage des Personalausweises vermeiden lassen. Dies gilt auch für die elektronische Übermittlung des Akteninhalts. Für eine elektronische Legitimationsprüfung einer Partei oder eines Dritten bieten sich hierfür wieder der elektronische Personalausweis und Bürgerportale ggf. in Verbindung mit dem Projekt S.A.F.E. an.

7.4.3 Online-Abruf

§ 299 Abs. 3 Satz 2 ZPO gestattet Rechtsanwälten den Online-Abruf auf den Inhalt der elektronisch geführten Akten. Die Entscheidung hierüber trifft der Vorsitzende. Satz 3 bestimmt, dass sicherzustellen ist, dass der Zugriff nur durch einen Bevollmächtigten erfolgt. Die Geset-

[832] Zum Grundsatz der informationellen Gewaltenteilung vgl. *Roßnagel/Laue*, DÖV 2007, 547 m.w.N.
[833] BT-Drs. 15/4067, 33.

zesbegründung gibt keine Auskunft darüber, wie dies erfolgen solle. Hier kommen wiederum die bereits oben beschriebenen Möglichkeiten in Betracht: nämlich der elektronische Personalausweis oder das Bürgerportal ggf. in Verbindung mit dem Projekt S.A.F.E. Bei dieser Variante wäre der Einsatz des elektronischen Personalausweises sehr sinnvoll. Denn dieser verfügt, wie gesehen, auch über eine Signaturfunktion. Anhand eines Berufsattributs könnte dann zugleich die Zugehörigkeit zu einer Rechtsanwaltskammer überprüft werden.[834] Die Variante der Online-Einsicht kann praktisch umgesetzt werden, indem der Anwalt entweder direkt auf die auf dem Gerichtsserver befindliche Akte zugreift oder indem eine Kopie ausgelagert wird.[835] Aus Datenschutzgründen ist die Auslagerung von Kopien dem Zugriff des Rechtsanwalts auf den Gerichtsserver der Vorzug zu geben. Ansonsten bestünde nämlich die Gefahr, dass sich Unbefugte einschleichen, sich Kenntnis von vertraulichen Daten verschaffen oder Daten manipulieren oder zerstören.[836]

7.4.4 Entscheidung über die elektronische Akteneinsicht

§ 299 Abs. 3 Satz 1 ZPO lautet, dass bei elektronischer Akteneinsichtsgewährung „die Geschäftsstelle die Akteneinsicht gewährt“. Über den Online-Abruf von Rechtsanwälten entscheidet dagegen das erkennende Gericht nach § 299 Abs. 3 Satz 2 ZPO nach pflichtgemäßem Ermessen. Wie sich aus § 299 Abs. 2 ZPO ergibt, entscheidet auch der Richter über die elektronische Gewährung von Akteneinsicht an Dritte. § 299 Abs. 2 ZPO geht in dieser Hinsicht den Regelungen in § 299 Abs. 3 ZPO vor.

§ 299 Abs. 3 Satz 1 ZPO gibt dem Urkundsbeamten für die elektronische Akteneinsicht durch Parteien mehr Befugnisse als bislang. Bislang, also bei herkömmlicher Aktenführung, entscheidet über die Gewährung der Akteneinsicht von Parteien der Urkundsbeamte der Geschäftsstelle. Wenn die Akten allerdings versendet werden sollen, ist eine Entscheidung des Richters erforderlich. Bei der Ermessensentscheidung hat der Richter die Interessen der Prozessparteien und der Prozessbevollmächtigten sowie die Erfordernisse eines geordneten Geschäftsgangs gegeneinander abzuwägen. Auch datenschutzrechtliche Gesichtspunkte hat er bei seiner Ermessensentscheidung mit einzubeziehen.[837] Nunmehr kann der Geschäftsstellenbeamte auch über die elektronische Übermittlung des Akteninhalts an die Parteien entscheiden, also dann, wenn die Akte nach außen geht. Dies ist als kritisch zu beurteilen. Der Geschäftsstellenbeamte kennt die Akte nicht so gut wie der Richter, der sie bearbeitet. Zwar ist es zutreffend, dass eine Entscheidung des Richters nicht mehr deshalb entbehrlich wird, weil der Richter nicht mehr zu prüfen hat, ob die Akte im Gericht noch gebraucht wird.[838] Allerdings

[834] *Holin*, 2008, 130.
[835] *Holin*, 2008, 130.
[836] *Holin*, 2008, 130.
[837] Während bei Rechtsanwälten grundsätzlich von deren persönlichen Zuverlässigkeit und der Einhaltung von Datenschutzbestimmungen ausgegangen wird, wird dies bei Naturparteien nicht vertreten. Deshalb ist bei Rechtsanwälten die Übersendung der Akten an die Kanzlei die Regel, nicht dagegen bei Parteien. Vgl. hierzu etwa OLG Frankfurt, MDR 1989, 465; LG Köln, RPfleger 1989, 334.
[838] Zu diesem Argument vgl. etwa *Lindloff*, 2005, 214.

hat der Richter auch immer datenschutzrechtliche Gesichtspunkte bei seiner Entscheidung mit zu berücksichtigen. Es wäre daher sinnvoll gewesen, diese Befugnis beim Richter zu belassen.

7.5 E-Bekanntmachungen nach der ZPO

Es wurde bereits beschrieben,[839] dass mit dem Justizkommunikationsgesetz bestimmt wurde, dass, soweit Veröffentlichungen im Bundesanzeiger erfolgen, diese im elektronischen Bundesanzeiger vorzunehmen sind. Ferner wurde mit dem Gesetz die Möglichkeit geschaffen, öffentliche Bekanntmachungen der Gerichte in einem vom Gericht bestimmten elektronischen Informations- und Kommunikationssystem zu veröffentlichen. Bei diesen Bekanntmachungen werden personenbezogene Daten nach § 3 LDSG übermittelt. Zum Beispiel bestimmt § 186 Abs. 2 Satz 3 Nr. 1 bis 4 ZPO für die öffentliche Zustellung, dass die Benachrichtigung über eine Zustellung die Person, für die zugestellt wird, den Namen und die letzte bekannte Anschrift des Zustellungsadressaten, das Datum, das Aktenzeichen des Schriftstücks und die Bezeichnung des Prozessgegenstands sowie die Stelle, wo das Schriftstück eingesehen werden kann, erkennen lassen muss. Mit den mit den Bekanntmachungen einhergehenden Datenübermittlungen wird in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 GG eingegriffen. Dieser Eingriff ist zwar vom Grundsatz her aufgrund des mit den verschiedenen Bekanntmachungen in Zusammenhang stehenden jeweiligen Unterrichtungsinteresses gerechtfertigt. So hat zum Beispiel ein Betroffener die öffentliche Zustellung in Kauf zu nehmen, da er sich aus seinem Lebenskreis entfernt hat, ohne die Möglichkeit geschaffen zu haben, dass ihn Zustellungen erreichen.[840] Könnte man Klageschriften oder Urteile oder vergleichbare Schriftsätze nicht öffentlich zustellen, wäre es einem Kläger oder Antragsteller unmöglich, Ansprüche titulieren oder Rechtsverhältnisse gestalten zu lassen.[841]

Die Veröffentlichungen im elektronischen Bundesanzeiger und die Veröffentlichungen in einem vom Gericht bestimmten Informations- und Kommunikationssystem stellen jedoch, verglichen mit den im herkömmlichen Bundesanzeiger oder an einer Gerichtstafel erfolgten Bekanntmachungen, einen ungleich intensiveren Grundrechtseingriff dar. Aufgrund dessen sind zum Schutz des informationellen Selbstbestimmungsrechts Vorkehrungen zu treffen. Die amtliche Begründung setzt sich mit der Problematik des Datenschutzes bei diesen Veröffentlichungen hingegen nicht auseinander.[842]

Bei der Veröffentlichung von Insolvenzinformationen im Internet hat der Gesetzgeber mit § 9 Abs. 2 InsO i.V.m. der dazu ergangenen Rechtsverordnung immerhin bestimmte – wenngleich

[839] Vgl. hierzu Abschnitt 2.3.1.5 .

[840] *Liebscher*, 1994, 137.

[841] *Liebscher*, 1994, 137.

[842] So heißt es etwa bei der Begründung zu § 186 lediglich: „Die Ergänzung schafft die zusätzliche Möglichkeit einer öffentlichen Zustellung durch Einstellung in das Internet auf der Homepage des Gerichts. Damit wird ein mittlerweile weit verbreitetes Medium genutzt, um eine zeitgemäße Möglichkeit der Kenntnisnahme der öffentlichen Zustellung zu schaffen.“ Vgl. hierzu BT-Drs. 15/4067, 32.

auch nicht ausreichende[843] – Schutzmaßnahmen für das informationelle Selbstbestimmungsrecht getroffen. So hat er Löschfristen für die bekannt zu machenden Daten definiert und vorgesehen, dass die Veröffentlichungen unversehrt, vollständig und aktuell bleiben müssen und jederzeit ihrem Ursprung nach zugeordnet werden können. Auch bei den Bekanntmachungen nach der ZPO hätte er sich daher mit diesen Vorgaben auseinandersetzen müssen.

Angesichts der Gefahren des Internets hätte der Gesetzgeber darüber hinaus neu prüfen müssen, ob die Inhalte der jeweiligen Bekanntmachungen unter dem Gesichtspunkt der Datensparsamkeit nach § 1 Abs. 3 LDSG im jeweiligen Einzelfall eingeschränkt werden müssen. So besteht zum Beispiel der Zweck einer öffentlichen Zustellung alleine darin, dem Gegner rechtliches Gehör zu verschaffen. Die Bekanntmachung richtet sich allein an ihn. Deshalb ist es zum Beispiel nicht erforderlich, dass § 186 Abs. 2 Satz 3 Nr. 2 ZPO vorsieht, dass auch die letzte bekannte Anschrift des Gegners zwingend anzugeben ist. Der Verfahrensgegner weiß, wo er gewohnt hat. Dass er mit der öffentlichen Zustellung gemeint ist, kann er auch anhand der anderen oben mitzuteilenden Daten (Person, für die zugestellt wird, sein Name, das Datum, das Aktenzeichen des Schriftstücks und die Bezeichnung des Prozessgegenstandes) gut erkennen. Wenngleich § 186 Abs. 2 ZPO mit dem Zustellungsreformgesetz[844] im Vergleich zu seinen vorherigen Fassungen[845] aus datenschutzrechtlicher Sicht eine Verbesserung erfahren hat, wäre angesichts der neuen Veröffentlichungsformen eine neue Bewertung angesagt gewesen. Dies gilt auch für die übrigen vorgesehenen Bekanntmachungen in den Verfahrensordnungen.

7.6 E-Akte

In § 298a Satz 1 ZPO ist bestimmt, dass die Prozessakten auch elektronisch geführt werden können. In der noch zu erlassenden Rechtsverordnung nach § 298a Satz 2 ZPO für die elektronische Aktenführung in Zivilsachen vor dem Bundesgerichtshof und der ordentlichen Gerichtsbarkeit in Rheinland-Pfalz werden vor allem auch datenschutzrechtliche Gesichtspunkte Beachtung finden müssen. Neben den Besonderheiten, die für das Scannen von Papierdokumenten in eine elektronische Akte gelten[846] wird der Verordnungsgeber auch die bereits beschriebenen Vorgaben nach § 9 BDSG und § 9 LDSG, insbesondere zu den Zutritts, Zugangs- und Zugangskontrollen, zu beachten haben. Mit der Einführung der elektronischen Akte werden sich diese Anforderungen verstärken.[847] Besondere Bedeutung kommt bei der elektronischen

[843] Siehe hierzu Abschnitt 9.1.

[844] BGBl. 2001 I, 1206.

[845] Wortlaut von § 204 Abs. 2 Satz 1 ZPO a.F. in der Fassung der Vereinfachungsnovelle, BGBl. 1976 I, 3281: „Die öffentliche Zustellung erfolgt durch Anheftung der zuzustellenden Ausfertigung oder einer beglaubigten Abschrift des zuzustellenden Schriftstückes an die Gerichtstafel.“ Wortlaut von § 204 Abs. 2 Satz 1 ZPO a.F. in der Fassung des Rechtspflegevereinfachungsgesetzes, BGBl. 1990 I, 2847: „Zur öffentlichen Zustellung wird ein Auszug des zuzustellenden Schriftstückes und eine Benachrichtigung darüber, wo das Schriftstück eingesehen werden kann, an die Gerichtstafel angeheftet.“

[846] Hierzu wird verwiesen auf *Roßnagel* et al., 2007; *Roßnagel/Jandt*, 2008.

[847] In diesem Sinne auch *Berlit*, JurPC Web-Dok. 2008, Abs. 122.

Aktenführung insbesondere aber auch der Problematik der dauernden Verfügbarkeit und Integrität von elektronisch gespeicherten Daten zu.

Oben wurde festgestellt,[848] dass Akten in Zivilverfahren grundsätzlich fünf Jahre lang aufzubewahren sind. Erscheint eine Aufbewahrungsfrist im Einzelfall aus besonderen Gründen zu kurz oder zu lang, kann auch eine längere oder kürzere Aufbewahrungsfrist verfügt werden.[849] Die Aufbewahrungsfrist beginnt nach § 2 Abs. 3 SchrAG und nach § 2 Abs. 3 LSchrAG mit Ablauf des Jahres, in dem nach Beendigung des Verfahrens die Weglegung der Akte verfügt worden ist. Die Aufbewahrung erfolgt sowohl im Interesse von Verfahrensbeteiligten und Dritten, auch nach Beendigung des Verfahrens noch Auskünfte oder Ausfertigungen, Auszüge oder Abschriften aus den Akten erhalten zu können oder ein Wiederaufnahmeverfahren einleiten zu können. Aber auch öffentliche Interessen können eine Aufbewahrung rechtfertigen. Zum Beispiel können Gerichte und Justizbehörden ein Interesse daran haben, dass der Aktenbestand auch nach Beendigung des Verfahrens zur Fortbildung des Rechts, zur Wahrung der Rechtseinheit oder sonst für verfahrensübergreifende Zwecke der Rechtspflege zur Verfügung steht.[850] Um diese Zwecke zu erfüllen, muss die Integrität, die Authentizität und die Lesbarkeit der Daten während der Aufbewahrungsdauer sichergestellt werden. Angesichts dessen, dass sich ein Zivilverfahren über Jahre hinweg hinziehen kann und die fünfjährige Aufbewahrungsfrist mit Ablauf des Jahres beginnt, in dem die Weglegung der Akten angeordnet wurde, ergibt sich die Notwendigkeit, elektronische Dokumente sicher und datenschutzkonform für einen längeren Zeitraum aufzubewahren.

Bei elektronisch signierten Dokumenten erweist sich dies jedoch als problematisch. Elektronisch signierte Dokumente verlieren im Laufe der Zeit an Sicherheit und mithin an Beweiswert. Die Ursache hierfür liegt in der bei fortschreitender Technikentwicklung abnehmenden Sicherheitseignung der ursprünglich verwendeten kryptographischen Verfahren und Schlüssel.[851] Der Verlust an Sicherheitseignung kann zur Folge haben, dass sowohl die Integrität als auch die Authentizität nicht mehr nachgewiesen werden kann.[852] Wie lange die mathematischen Verfahren sicher sind, kann nicht auf Dauer, sondern nur für einen bestimmten Zeitraum bestimmt werden. Die Bundesnetzagentur (vormals: Regulierungsbehörde für Telekommunikation und Post), die für die Beurteilung der Sicherheitseignung nach Anlage 1 I Nr. 2 zur Signaturverordnung zuständig ist,[853] bestimmt unter Hinzuziehung eines Fachkreises aus Wissenschaft und Wirtschaft jährlich sowie nach Bedarf die Eignung der Algorithmen und ihrer Parameter für die jeweils nächsten sechs Jahre und veröffentlicht diese im Bundesanzeiger.[854]

---

848 Vgl. hierzu Abschnitt 5.4.3.

849 § 2 Abs. 2 der Landesverordnung zur Ausführung des Landesgesetzes zur Aufbewahrung von Schriftgut der Justiz, GVBl. 2008, 139.

850 § 2 Abs. 2 Satz 2 Nr. 1-4 SchrAG und § 2 Abs. 2 Satz 2 Nr. 1-4 LSchrAG.

851 Vgl. hierzu *Brandner* et al., DuD 2002, 97.

852 *Roßnagel* et al., CR 2003, 301.

853 Vgl. § 3 SigG i.V.m. § 66 TKG.

854 *Fischer-Dieskau*, in: *Hering/Schäfer* (Hrsg.), Digitales Verwalten – Digitales Archivieren, 35.

7.6.1 Langzeitarchvierung

Als geeignete Vorkehrung, dem Verlust der Sicherheitseignung der eingesetzten Algorithmen und zugehörigen Parametern entgegenzuwirken, kommt eine Neusignierung nach § 17 SigV in Betracht.[855] Nach § 17 Satz 2 SigV sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen und der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Satz 3 verlangt darüber hinaus, dass diese erneute Signatur mit geeigneten neuen Algorithmen und Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen muss.[856] Die erneute Signatur stellt keine Willens- oder Wissenserklärung dar, die eine vorherige Prüfung der erneuten Signatur erfordert. Aus diesem Grund ist es unbeachtlich, wer die erneute Signatur vornimmt.[857] Die erneute Signatur ist rechtzeitig vor Ablauf der Sicherheitseignung vorzunehmen. Hierfür verlangt das Gesetz die Verwendung eines qualifizierten Zeitstempels. Nach § 2 Nr. 14 SigG stellt ein qualifizierter Zeitstempel eine elektronische Bescheinigung eines qualifizierten Zertifizierungsdiensteanbieters darüber dar, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Hierdurch soll eine Missbrauchsmöglichkeit durch Vordatierung der erneuten Signatur auf einen Zeitpunkt, zu dem der Sicherheitswert der früheren Signatur möglicherweise so gering geworden ist, dass Fälschungen möglich sind, ausgeschlossen werden. Die Daten müssen entsprechend der fehlenden Eignung des Sicherungsmittels, d.h. der eingesetzten Algorithmen und Parameter, neu signiert werden. Wenn lediglich der verwendete Signaturalgorithmus in seiner Sicherheit bedroht ist, reicht es aus, allein die Signaturen des elektronischen Dokuments mit einem Zeitstempel zu versehen und neu zu signieren. Nur wenn auch der verwendete Hashalgorithmus nicht mehr sicherheitsgeeignet ist, muss ein neuer Hashwert der gesamten Daten berechnet werden, der einen neuen sicherheitsgeeigneten Hashalgorithmus und einen erneuten Zeitstempel enthält.[858] Bei der Neusignierung können beliebig viele signierte Dokumente und Signaturen einbezogen werden. Es muss nicht jedes einzelne Dokument und nicht jedes einzelne Verfahren neu signiert werden. Dies wird aus der Gesetzesformulierung „Daten“ und „frühere Signaturen“ im Plural deutlich.[859]

Die Problematik, dass elektronisch signierte Dokumente im Laufe der Zeit an Beweiskraft verlieren, hat der Gesetzgeber mit der Signaturerneuerung zufriedenstellend gelöst. Mit ihr kann die Integrität und Authentizität eines elektronischen Dokuments langfristig sichergestellt werden. Erforderlich ist jedoch zur Sicherung der Authentizität weiter, dass das der Signaturerneuerung zugrunde liegende qualifizierte Zertifikat noch gültig und nicht gesperrt ist.[860] Für eine langfristige beweiskräftige Aufbewahrung ist deshalb auch die langfristige Verfügbarkeit

---

855 *Brandner* et al., DuD 2002, 98.

856 *Fischer-Dieskau*, in: *Hering/Schäfer* (Hrsg.), Digitales Verwalten – Digitales Archivieren, 38.

857 *Fischer-Dieskau*, in: *Hering/Schäfer* (Hrsg.), Digitales Verwalten – Digitales Archivieren, 39. Zur Zulässigkeit der automatisiert erstellten Signatur vgl. *Roßnagel/Fischer-Dieskau*, MMR 2004, 133.

858 *Roßnagel* et al., CR 2003, 304.

859 *Brandner* et al., DuD 2002, 305.

860 *Yildirim*, 2004, 135.

der Verifikationsdaten erforderlich.[861] Nach §§ 4 Abs. 1, 5 Abs. 2 SigV sind qualifizierte Zertifizierungsdiensteanbieter jedoch nur verpflichtet, die von ihnen ausgestellten Zertifikate für eine Dauer von mindestens fünf Jahren nach Ablauf des Jahres ihrer Gültigkeit im Verzeichnis nachprüfbar zu halten. Auch die Dokumentation ist gemäß §§ 8 Abs. 3, 4 Abs. 1 SigV nur für diesen Zeitraum vom Zertifizierungsdiensteanbieter aufzubewahren. Bei Geschäftsaufgabe oder Insolvenz des Zertifizierungsdiensteanbieters ist selbst diese Aufbewahrungsdauer der Zertifikate nicht gewährleistet. Für akkreditierte Zertifizierungsdiensteanbieter gilt dagegen für die Dokumentation ein Aufbewahrungszeitraum von mindestens 30 Jahren nach §§ 8 Abs. 3, 4 Abs. 2 SigV. Zertifikate sind nach §§ 8 Abs. 3, 4 Abs. 2 SigV mindestens 30 Jahre nach Ablauf des Jahres der Gültigkeit eines Zertifikats im Verzeichnisdienst nachprüfbar zu halten. Aus diesem Grund empfiehlt sich der Einsatz von akkreditierten Signaturen.[862] Werden diese Vorgaben erfüllt, ist eine sichere langfristige Archivierung elektronischer Dokumente möglich. Zu diesem Ergebnis kommt auch das Projekt ArchiSig, das Verfahren für eine rechtssichere und beweiskräftige Langzeitarchivierung entwickelt hat.[863]

7.6.2 Transformation

Neben dem Problem, dass elektronisch signierte Dokumente im Laufe der Zeit ihre Beweiskraft verlieren, ist zudem zu berücksichtigen, dass die benutzte Hard- und Software veralten kann. Selbst wenn die Daten der elektronischen Akte auf den Speichermedien für einen längeren Zeitraum erhalten geblieben sind, kann die Lesbarkeit daran scheitern, dass sie mit den aktuellen Lesegeräten nicht mehr sichtbar gemacht werden können.[864] Zur Lösung der Risiken, die aus dem drohenden Verlust der Lesbarkeit von elektronischen Dokumenten folgen, stehen unterschiedliche Konzepte zur Verfügung. Einmal kommt das Aufbewahren der alten Soft- bzw. Hardware in Betracht. Da die jeweils genutzte Hard- und Software aber regelmäßig vorgehalten werden muss, kann diese Lösung nur für kurz- oder mittelfristige Aufbewahrungsvorhaben empfohlen werden. Zum anderen kommt die Übertragung der Daten in ein anderes Format in Betracht, die sog. Transformation.[865] Auch dies erweist sich jedoch als nicht völlig unproblematisch. Denn durch die Übertragung in ein anderes Format wird die zur Integritätssicherung angebrachte elektronische Signatur zerstört und kann deshalb ihren Zweck nicht mehr erfüllen.[866]

Um den drohenden Verlust der Lesbarkeit durch eine Transformation entgegenzuwirken und gleichzeitig den rechtlichen Wert des signierten Dokuments zu erhalten, hat der Gesetzgeber

[861] Zu den Verifikationsdaten gehören auch das Nutzerzertifikat sowie weitere zur Gültigkeitsprüfung dieses Zertifikats erforderlichen Informationen wie das Wurzelzertifikat, Gültigkeitsabfragen bei Zertifizierungsdiensteanbietern und angebrachte Zeitstempel zur Ermittlung des spätesten Signaturerstellungszeitpunktes.

[862] *Roßnagel*, MMR 2002, 218.

[863] Vgl. hierzu im Einzelnen die Webseite des Projekts `www.archisig.de`.

[864] *Roßnagel/Fischer-Dieskau/Wilke*, CR 2005, 903.

[865] *Roßnagel* et al., CR 2003, 305; *Hähnchen*, NJW 2005, 2259; *Redeker*, AnwBl 2005, 349.

[866] *Fischer-Dieskau*, 2006, 221.

mit § 33 Abs. 5 VwVfG[867] einen Weg aufgezeigt. § 33 Abs. 5 Satz 2 VwVfG sieht im Fall der Transformation eines qualifizierten Dokuments in ein neues Format vor, dass ein Beglaubigungsvermerk zu erstellen ist, der die Feststellungen enthalten muss, wen die Signaturprüfung als Inhaber der Signatur aufweist, welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur nennt und welche Zertifikate mit welchen Verfahren zugrunde lagen. Dieser Beglaubigungsvermerk muss den Namen des zuständigen Bediensteten und der vornehmenden Behörde nennen und mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur versehen werden. Anhand dieser Angaben soll die Geltung des Signaturschlüssels überprüft werden können.[868] Diese Vorschrift ist jedoch insofern nicht praktikabel, als dass es für die Transformation immer der Mitwirkung einer bestimmten Person bedarf. Sie verhindert damit die Automatisierung des Vorgangs, weshalb sich die Umformatierung in dieser Art und Weise für massenhaft zu transformierende Akten nicht eignet.[869]

Aus diesem Grund empfiehlt es sich nicht, eine entsprechende Vorschrift in die ZPO aufzunehmen. Vielmehr ist ein Verfahren erforderlich, in welchem elektronische Dokumente in einem automatisierten Vorgang konvertiert werden können. Ein derartiges Verfahren hat das Projekt „TransiDoc – Rechtssichere Transformation signierter Dokumente“ entwickelt, das Nachfolgeprojekt von ArchiSig.[870]

Nach dem TransiDoc-Konzept wird die elektronische Signatur unmittelbar vor der eigentlichen Konvertierung in einem Transformationssystem geprüft. Das Prüfergebnis wird sodann in einem Transformationsvermerk, der Bestandteil des Zieldokuments ist, festgehalten.[871] Um die Integrität und Authentizität des Ausgangsdokuments zu gewährleisten, wird in dem Prüfergebnis nicht nur die mathematische Korrektheit der Signatur festgehalten, im Transformationsvermerk befinden sich vielmehr auch Angaben über die Zertifikatskette bis hin zum Wurzelzertifikat.[872] Weiterhin enthält der Transformationsbericht die im Rahmen der Prüfung einer qualifizierten elektronischen Signatur automatisch eingeholte OCSP-Antwort, aus der sich die Gültigkeit des Nutzerzertifikats zum Zeitpunkt der Abfrage ergibt. Das Transformationssystem selbst befindet sich in einer sicheren Einsatzumgebung und ist durch eine Zugangskontrolle und z.B. eine Firewall gesichert.[873] Damit die Qualität des eingesetzten Systems für den Rechtsverkehr nachvollziehbar bleibt, werden die Hard- und Softwarekomponenten, die für die Transformation verwendet wurden, im Transformationsvermerk protokolliert.[874] Wenn die Transformation ordnungsgemäß erfolgt ist, bestätigt das System in dem Transformationsver-

867 Eingeführt durch das Dritte Verwaltungsverfahrensänderungsgesetz vom 21.8.2002, BGBl. 2002 I, 3322.
868 BT-Drs. 14/9000, 33.
869 *Holin*, 2008, 114.
870 Dieses Projekt wurde vom BMWi gefördert. An ihm waren das Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt, die Projektgruppe verfassungsverträgliche Technikgestaltung der Universität Kassel (provet), das Zentrum für Informations- und Medizintechnik des Uni-Klinikums Heidelberg (ZIM), die InterComponentWareAG (ICW), die Curiavant Internet GmbH sowie die Bundesnotarkammer als assoziierte Partnerin beteiligt.
871 *Wilke* et al., CR 2008, 609.
872 *Wilke* et al., CR 2008, 609.
873 *Wilke* et al., CR 2008, 609.
874 *Wilke* et al., CR 2008, 609.

merk die Übereinstimmung von Ausgangs- und Zieldokument. Um auch die Authentizität und die Integrität des Zieldokuments gegen Verfälschungen zu sichern, wird zudem gewährleistet, dass das Zieldokument einschließlich des Transformationsberichts unmittelbar nach Abschluss der Transformation mit einer qualifizierten elektronischen Signatur versehen wird.[875] Mit Hilfe der Langzeitarchivierung nach § 17 SigV und des TransiDoc-Konzeptes lässt sich also die beschriebene Problematik einer langen Aufbewahrung von elektronischen Dokumenten lösen.[876]

7.7 E-Mahnverfahren

Mit dem Mahnverfahren nach §§ 688 ff. ZPO soll dem Gläubiger einer Geldforderung schnell und einfach ohne mündliche Verhandlung ein Vollstreckungstitel verschafft werden. Wie bereits dargestellt wurde, bestehen bei den Gerichten auf der Grundlage von § 689 Abs. 3 ZPO zentrale Mahngerichte. Zentrale Mahngerichte sind aus mehreren Gründen von Vorteil: Zum einen werden mit ihrer Hilfe die Kosten für das Einrichten der elektronischen Infrastruktur auf ein Gericht beschränkt.[877] Zum anderen kann mit Hilfe eines zentralen Mahngerichts der Personaleinsatz innerhalb der Justiz effizient ausgestaltet werden.[878] Außerdem erweist sich die Kommunikation für Gläubiger mit lediglich einem Gericht als einfacher. Unter dem Gesichtspunkt des Datenschutzes bestehen gegen zentrale Mahngerichte keine Bedenken, sofern die in § 9 LDSG beschriebenen technisch-organisatorischen Anforderungen erfüllt sind. Was die Einreichung der Mahnanträge angeht, so bestimmt § 690 Abs. 3 ZPO, welche als spezielle Regelung der Vorschrift des § 130a ZPO vorgeht,[879] dass es für die Einreichung von Mahnanträgen einer handschriftlichen Unterzeichnung nicht bedarf, wenn in anderer Weise gewährleistet ist, dass der Antrag nicht ohne den Willen des Antragstellers übermittelt wird. Aus den oben genannten Gründen wäre jedoch auch für die Einreichung der Mahnanträge eine qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG erforderlich. Insbesondere im Mahnverfahren ist eine hinreichende Authentifizierung zum Schutz des Schuldners notwendig. Wenn dieser nämlich keinen Widerspruch gemäß § 694 ZPO einlegt, erlässt das Gericht nach § 699 ZPO einen Vollstreckungsbescheid, auf dessen Grundlage der Gläubiger sodann die Zwangsvollstreckung betreiben kann.

7.8 ELENA und Prozesskostenhilfe

Für die Prüfung der Bedürftigkeit nach § 114 ZPO hat das Gericht die Angaben über die Familienverhältnisse, zum Beruf, zum Vermögen, zum Einkommen und zu den Lasten des Antragstellers zu erheben. Hierzu hat dieser einen Vordruck auszufüllen und dem Gericht zu

875 *Wilke* et al., CR 2008, 609.
876 Zur rechtssicheren Transformation vgl. im Übrigen auch ausführlich *Roßnagel/Schmidt/Wilke*, 2009.
877 *Sujecki*, MMR 2006, 371.
878 *Sujecki*, MMR 2006, 371.
879 *Zöller*, ZPO, § 690 Rn. 22.

übermitteln. Nach den derzeitigen Planungen soll sich dieses Verfahren in Zukunft ändern. Vorgeschlagen wird die Einbindung von ELENA in das Prozesskostenhilfeverfahren.

Das ELENA-Verfahren geht auf eine Idee der Kommission zum Abbau der Arbeitslosigkeit und zur Umstrukturierung der Bundesanstalt für Arbeit (Hartz-Kommission) zurück. Die Hartz-Kommission schlug vor, eine Versicherungskarte, die sog. JobCard, als Signatur- oder Schlüsselkarte zu entwickeln, die für den Abruf von Verdienst- und Arbeitsbescheinigungen durch die jeweils zuständige Stelle nach Ermächtigung durch den Antragsteller zur Verfügung steht. Die Bundesregierung hatte diesem Vorschlag am 21.8.2002 zugestimmt, worauf das erste Pilotprojekt am 21.11.2002 startete. Das Bundesministerium für Wirtschaft und Arbeit hatte die Federführung für dieses Projekt. Dieses betraute die Spitzenverbände der Krankenkassen mit der technischen Umsetzung des Projekts, die ihrerseits den Projektauftrag an eine gemeinsame Tochtergesellschaft, die ITSG GmbH[880] vergaben. Das Bundesministerium für Wirtschaft und Arbeit legte seinen Bericht am 31.3.2003 vor. Von September 2003 bis April 2004 wurde das Verfahren – unter Einbeziehung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – am Beispiel der Arbeitsbescheinigung nach § 312 SGB III erprobt. In einem zweiten Modellvorhaben wurde das Verfahren auf Verdienst- und Auskunftsbescheinigungen ausgedehnt. Der ursprüngliche Begriff JobCard wurde dabei durch die Formulierung ELENA (elektronischer Einkommensnachweis) ersetzt.

Am 22.1.2009 hatte der Bundestag den Entwurf des ELENA-Verfahrensgesetzes beschlossen. Nicht wegen datenschutzrechtlicher Bedenken, sondern wegen der Einbeziehung des Wohngeldes in das Verfahren und der Finanzierung des Vorhabens hatte der Bundesrat am 13.3.2009 den Vermittlungsausschuss angerufen.[881] Nachdem dort eine Einigung erzielt werden konnte[882] hat der Bundestag am 6.3.2009 den Änderungen im Vermittlungsausschuss zugestimmt. Das Gesetz wurde sodann am 1.4.2009 verkündet[883] und trat nach dessen Artikel 11 hinsichtlich seiner wesentlichen Regelungen am 2.4.2009 in Kraft.[884] Inzwischen liegt dem Bundesverfassungsgericht eine „Sammelbeschwerde“ gegen das Gesetz vor.[885]

---

880 Die ITSG GmbH (Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH) ist die Clearingstelle für den Datenaustausch zwischen der gesetzlichen Kranken- und Rentenversicherung sowie den Arbeitgebern.

881 Im Laufe des Gesetzgebungsverfahrens wurden nur punktuelle datenschutzrechtliche Verbesserungen, zum Beispiel bei den Regelungen zur Löschung vorgenommen, vgl. hierzu Beschlussempfehlung des Ausschusses für Wirtschaft und Verkehr, BT-Drs. 16/11666.

882 Das Wohngeld wurde in das Verfahren einbezogen; die Kosten für die Anschubfinanzierung für das Vorhaben 2009 bis 2013 soll durch Bundesmittel erfolgen. Von 2014 an soll die Finanzierung von denjenigen Bundes- und Landesbehörden getragen werden, die über ELENA Daten aus der Zentralen Speicherstelle abrufen.

883 BGBl. 2009 I, 639.

884 Zum neuen Gesetz vgl. auch *Warga*, DuD 2010, 216; *Wedde*, ArbuR 2010, 94; *Kiesche/Wilke*, dbr 2010, 33; *Warga*, PersR 2010, 111; *Stüwe*, sj 2009, 45; *Wedde*, AiB 2010, 143; *Wedde*, SozSich 2010, 73.

885 Siehe `http://www.heise.de/newsticker/meldung/Datenschuetzer-uebergeben-Sammelbeschwerde-gegen-ELENA-968296.html` (Zugriff am 20.5.2010).

Nach § 95 Abs. 1 findet das ELENA-Verfahren in einem ersten Schritt zunächst nur Anwendung für die Bescheinigungen zur Leistungsberechnung für das Arbeitslosen-, das Wohn und das Elterngeld.[886]

Das ELENA-Verfahrensgesetz sieht folgenden Verfahrensablauf vor: Die Arbeitgeber übertragen monatlich sämtliche Daten, die für die Berechnung des Arbeitslosen-, des Wohn- oder des Elterngeldes relevant sind,[887] für jede bei ihnen beschäftigte Person an die Zentrale Speicherstelle. Sobald ein Nachweis erforderlich ist, haben sich die beschäftigten Personen nach § 98 Abs. 1 ELENA-Verfahrensgesetz am Verfahren anzumelden. Die Anmeldung erfolgt entsprechend § 98 Abs. 2 Satz 2 ELENA-Verfahrensgesetz bei einer sog. Registratur Fachverfahren oder über eine Anmeldestelle, die den Antrag unverzüglich an die Registratur Fachverfahren weiterleitet. Für die Anmeldung sind die Versicherungs- oder Verfahrensnummer und eine sog. Zertifikatsidentitätsnummer gemäß § 98 Abs. 2 Satz 1 ELENA-Verfahrensgesetz anzugeben. Wie sich aus § 98 Abs. 2 Satz 1 ELENA-Verfahrensgesetz ergibt, setzt sich die Zertifikatsidentitätsnummer aus der laufenden Nummer des Zertifikats, dem Namen des Zertifizierungsdiensteanbieters sowie seinem Niederlassungsstaat zusammen. Aufgabe der Registratur Fachverfahren ist es, die Zertifikatsidentitätsnummer des Teilnehmers mit der Versicherungs- oder Verfahrensnummer des Teilnehmers zu verknüpfen. Dieses Verfahren ist erforderlich, weil die Zentrale Speicherstelle die bei ihr gespeicherten Daten nicht unter der Versicherungsnummer speichern soll, um die Datensicherheit und den Grad der Pseudonymisierung zu erhöhen. Diejenigen Behörden, die die Daten benötigen, können diese bei der Zentralen Speicherstelle abrufen. Nach § 103 Abs. 1 ELENA-Verfahrensgesetz ist der Abruf jedoch nur zulässig, wenn

886 Vgl. § 95 Abs. 1 ELENA-Verfahrensgesetz: „Das Verfahren zur Erstellung und Verarbeitung des elektronischen Entgeltnachweises findet auf folgende Auskünfte, Bescheinigungen und Nachweise (erfasste Nachweise) Anwendung: 1. Arbeitsbescheinigung nach § 312 des Dritten Buches, 2. Nebeneinkommensbescheinigung nach § 313 des Dritten Buches, 3. Auskunft über die Beschäftigung nach § 315 Abs. 3 des Dritten Buches, 4. Auskünfte über den Arbeitsverdienst zum Wohngeldantrag nach § 23 Abs. 2 des Wohngeldgesetzes und 5. Einkommensnachweise nach § 2 Abs. 7 Satz 4 und § 9 des Bundeselterngeld- und Elternzeitgesetzes.“

887 Vgl. hierzu § 97 Nr. 1 ELENA-Verfahrensgesetz: „Der Arbeitgeber hat der Zentralen Speicherstelle für jeden Beschäftigten, Beamten, Richter oder Soldaten monatlich gleichzeitig mit der Entgeltabrechnung eine Meldung zu erstatten, welche die Daten enthält, die in die erfassten Nachweise (§ 95 Abs. 1) aufzunehmen sind. Das sind insbesondere 1. die Versicherungsnummer (§ 147 des Sechsten Buches) oder Verfahrensnummer (Absatz 4), Familienname, Vornamen, Tag der Geburt und Anschrift des Beschäftigten, Beamten, Richters oder Soldaten, 2. das erfasste Einkommen in Euro, Beginn und Ende des Zeitraums, für den das erfasste Einkommen erzielt worden ist, die Art des Einkommens, die Beitragsgruppen, falls vorhanden, und die laufende Nummer der Meldung sowie 3. Name und Anschrift des Arbeitgebers sowie die Betriebsnummer des Beschäftigungsbetriebs. Sonstige personenbezogene Daten darf die Meldung nicht enthalten. Zusätzlich zur monatlichen Meldung nach Satz 1 hat der Arbeitgeber der Zentralen Speicherstelle die Meldung zu den erfassten Nachweisen zu dem Zeitpunkt und mit dem Inhalt zu übermitteln, den das für den jeweiligen Nachweis geltende Gesetz bestimmt. Auf die Übermittlung und den Anspruch des Beschäftigten, Beamten, Richters oder Soldaten auf Auskunft über die zu seiner Person gespeicherten Daten ist auf der Entgeltbescheinigung hinzuweisen. Eine Meldepflicht des Arbeitgebers besteht nicht, wenn Entgelte ausschließlich aus einer geringfügigen Beschäftigung in einem Privathaushalt nach § 8a erzielt werden.“

der Teilnehmer mit seiner qualifizierten elektronischen Signatur sein Einverständnis erklärt hat. Damit die Behörde die Daten abrufen kann, bedarf sie einer Zulassung zum Verfahren gemäß § 99 Abs. 7 ELENA-Verfahrensgesetz. Die Zulassung erfolgt auf Antrag durch die Zentrale Speicherstelle. Nach § 119 Abs. 1 ELENA-Verfahrensgesetz hat die Zentrale Stelle zu gewährleisten, dass das Abrufverfahren am 1.1.2012 vollständig funktionsfähig ist. Wie sich aus § 119 Abs. 3 ELENA-Verfahrensgesetz ergibt, wurden die Arbeitgeber erst nach dem 31.12.2009 verpflichtet, die Nachweise elektronisch zu erbringen. Dessen ungeachtet hat der Arbeitgeber bis zum 31.12.2011 auch noch papierne Auskünfte und Bescheinigungen auszustellen. Diese Verpflichtung kann nach § 119 Abs. 4 ELENA-Verfahrensgesetz erst entfallen, wenn das ELENA-Verfahren ab dem 1.1.2012 voll einsatzbereit ist.

Eine Zugriffsmöglichkeit auf die Zentrale Speicherstelle ist auch für die Gerichte insbesondere im Prozesskostenhilfeverfahren von Interesse.[888] In einem Pilotprojekt wurde eine vorläufige Bescheinigung entwickelt, die die Daten erfasst, die bei der zentralen Stelle vorhanden sind und die für die Prüfung der Bedürftigkeit benötigt werden.[889] Die Planungen sehen vor, dass das Gericht den Antragsteller nach der Einreichung seines Prozesskostenhilfe-Antrags auffordert, seine Einwilligung zum Abruf der Daten zu erteilen. Auch wird vorgeschlagen, auf einem zentralen gerichtlichen Server ein elektronisches Formular vorzuhalten, auf welchem der Antragsteller sogleich sein Einverständnis zum Datenabruf erklären, dieses qualifiziert signieren und elektronisch übermitteln kann. Das von dem Antragsteller erteilte Einverständnis kann dann z.B. anhand des auf dem Formular als Pflichtangabe mitzuteilenden Aktenzeichens automatisch dem jeweiligen Verfahren zugeordnet werden. Das Gericht veranlasst die Abfrage bei der zentralen Speicherstelle, indem es die qualifizierte elektronische Signatur des Betroffenen und des entsprechenden Sachbearbeiters (Abrufagent) der zentralen Speicherstelle übermittelt. Diese antwortet mit der Übersendung der Prozesskostenhilfe-Bescheinigung im XML-Format. Die eingegangenen Daten werden in der Fachanwendung gespeichert und können automatisch in ein Berechnungsprogramm für Prozesskostenhilfe übergeben werden. Sofern es zur Leistungsgewährung, d.h. zur Prozesskostenhilfe-Bewilligung kommt, könne die Überwachung der Änderung der wirtschaftlichen Verhältnisse durch turnusmäßige und automatisierte Abfragen erfolgen.[890] Diskutiert wird darüber hinaus, auch dem Rechtsanwalt eine Zugriffsmöglichkeit auf die Daten aus der Zentralen Speicherstelle mit Einwilligung des Betroffenen zukommen zu lassen, damit dieser die Erfolgsaussichten des Prozesskostenhilfe-Antrags prüfen kann. Die Vorteile der Einbindung von ELENA werden zum einen darin gesehen, dass Manipulationsmöglichkeiten des Betroffenen ausgeschlossen werden können. Außerdem würde die Kontrolle der Änderung der wirtschaftlichen Verhältnisse im Prozesskostenhilfeverfahren nach § 120 Abs. 4 ZPO erleichtert. Schließlich wird geltend gemacht, dass hinsichtlich dieser Daten die Verpflichtung der Glaubhaftmachung durch Einreichung von Papierunterlagen

[888] Vgl. hierzu *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 172.
[889] Vgl. hierzu *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 172.
[890] Vgl. hierzu *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 174

nach § 118 Abs. 2 ZPO entfallen und so ein Medienbruch bei elektronischer Aktenführung verhindert werden kann.[891]

7.8.1 Generelle Kritik

Gegen die Einbeziehung von ELENA in das gerichtliche Verfahren spricht schon die grundsätzliche Struktur des ELENA-Verfahrens. Bei der Zentralen Speicherstelle werden millionenfach als sensibel zu bewertende Arbeitnehmerdaten gesammelt, ohne dass absehbar ist, ob diese Daten überhaupt einmal benötigt werden. Ziel von ELENA ist es, die Arbeitgeber von der Ausstellung mehrerer Bescheinigungen zu entlasten, eine medienbruchfreie Übertragung der Daten zu ermöglichen und Behörden den Zugang zu den Daten zu vereinfachen.[892] Langfristig sollen hierdurch unnötige Kosten sowohl bei den Arbeitgebern als auch in der Verwaltung vermieden werden.[893] Untersuchungen haben ergeben, dass sich die Kosten für eine auszustellende Bescheinigung auf rund 10 EUR, nach anderen Berechnungen auf etwa 5 Prozent der gesamten Kosten der Personalverwaltung belaufen.[894] Um das Ziel der Kostenminimierung zu verfolgen, hat der Gesetzgeber in das Recht auf informationelle Selbstbestimmung von Millionen Beschäftigten eingegriffen. Um das Recht auf informationelle Selbstbestimmung mit diesen Zielvorgaben zu einem verfassungsrechtlichen Ausgleich zu bringen, hat er insbesondere durch die Zwischenschaltung der Registratur Fachverfahren und der Mitwirkung des Betroffenen[895] verschiedene Schutzvorkehrungen im ELENA-Verfahrensgesetz verankert. Ob diese Schutzvorkehrungen jedoch ausreichend sind, wird sich erst noch zeigen. Aufgrund des vergleichsweise geringen Nutzens von ELENA hinsichtlich der Kosteneinsparungen und angesichts einer derartigen Datenvorhaltung dürften jedoch ungeachtet dessen erhebliche Zweifel an der Verhältnismäßigkeit der Regelungen im ELENA-Verfahrensgesetz bestehen. Es bleibt abzuwarten, wie das Bundesverfassungsgericht in dem derzeit anhängigen Verfassungsbeschwerdeverfahren gegen das Gesetz entscheidet.

7.8.2 Datenabruf durch die Gerichte

Eine Einbeziehung von ELENA dürfte jedoch zumindest bei den Gerichten abzulehnen sein. Der Antragsteller hat bisher schon die Verpflichtung nach § 117 Abs. 1 ZPO, dem Antrag eine Erklärung über seine persönlichen und wirtschaftlichen Verhältnisse, welche die Angaben über Familienverhältnisse, Beruf, Vermögen, Einkommen und Lasten betragen, beizufügen. Man könnte sich zwar überlegen, ob dann, wenn konkrete Zweifel an der Richtigkeit der Angaben des Betroffenen bestehen, eine Anfrage bei der Zentralen Speicherstelle mit Einverständnis

[891] Vgl. hierzu *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 173. Dieser sieht aufgrund dieser Vorteile mittelfristig sogar die Notwendigkeit, das ELENA-Verfahren flächendeckend bei Gericht einzuführen. Speziell zu den Vorteilen bei der Nachkontrolle *Schaefer*, ZRP 2006, 95.

[892] BR-Drs. 561/08, 10.

[893] BR-Drs. 561/08, 10.

[894] BR-Drs. 561/08, 10.

[895] Vgl. hierzu ausführlich BR-Drs. 561/08, 26.

des Betroffenen eingeholt werden darf. Sofern konkrete Zweifel an der Richtigkeit der Angaben bestehen, kann das Gericht aber nach § 118 Abs. 2 ZPO schon die Glaubhaftmachung der Angaben verlangen[896] und weitere Erhebungen anstellen, insbesondere die Vorlegung von Urkunden anordnen und Auskünfte einholen.[897] Vor diesem Hintergrund ist ein Datenabruf zur Vermeidung von Manipulationen nicht notwendig. Überdies ist auch zu berücksichtigten, dass der Antragsteller seinem Prozesskostenhilfe-Antrag Unterlagen beizufügen hat, die nicht bei der Zentralen Speicherstelle gespeichert sind. Hierzu gehört etwa der Mietvertrag oder der Kreditvertrag mit den Zins- und Tilgungsraten für den Hauskauf.[898] Aus diesem Grund werden Medienbrüche ohnehin solange nicht vermieden werden können, bis die elektronische Einreichung von Unterlagen verpflichtend eingeführt wird.

Ziel der Einbindung von ELENA in das Prozesskostenhilfeverfahren ist unter anderem auch, die Überprüfungen der Änderungen der wirtschaftlichen und persönlichen Verhältnisse des Rechtspflegers durch eine Abfrage des Gerichts bei der Zentralen Speicherstelle zu ersetzen. So wird geltend gemacht, dass die Ausgaben für die Prozesskostenhilfe dringend begrenzt werden müssten. Das derzeitige Verfahren der Nachkontrolle sei mit Mängeln behaftet und leide unter einem strukturellen Vollzugsdefizit.[899] Nach der derzeitigen Regelung hat der Antragsteller keine Anzeigepflicht bei einem nachträglich erhöhten Einkommen. Für die Nachkontrolle setzt der Rechtspfleger[900] dem Antragsteller deshalb eine Frist. Wenn der Antragsteller hierauf nicht reagiert, dann kann der Rechtspfleger die Prozesskostenhilfe aufheben.[901] An diesem Verfahren wird kritisiert, dass es umständlich ist und mit ihm eine effektive Nachkontrolle nicht möglich ist. Mit der Einbindung von ELENA in die Prozesskostenhilfe dagegen könnten routinemäßige Abrufe bei der Zentralen Speicherstelle durch das Gericht erfolgen, die eine Nachkontrolle effektiv machen würden. Damit sei ein erheblicher Rückfluss der im Rahmen der Prozesskostenhilfe verauslagten Gelder zu erwarten.[902] Dem kann jedoch nicht zugestimmt werden. Der Verfahrensablauf lässt sich auch mit dem ELENA-Verfahren nicht vereinfachen.

---

896 Vgl. zur Glaubhaftmachung § 294 ZPO. Das Gericht kann die Glaubhaftmachung sowohl für die Tatsachen verlangen, für die die Partei die Beweislast trifft, ferner für die Tatsachen, für die sie ihre Hilfsbedürftigkeit herleitet. Ob das Gericht die Glaubhaftmachung verlangt, steht in seinem Ermessen. Zur Hilfsbedürftigkeit sollte eine Versicherung an Eides Statt nur angefordert werden, wenn keine Belege beigebracht werden können. Vgl. hierzu im Einzelnen *Zöller*, ZPO, § 118 Rn. 16.

897 Das Gericht darf Erhebungen nur als letztes Mittel anstellen. Vgl. hierzu *Zöller*, ZPO, § 118 Rn. 18 mit Verweis auf die Parteimaxime.

898 In der Zentralen Speicherstelle befinden sich ausschließlich vom Arbeitgeber zur Verfügung gestellte Daten, also vor allem das Einkommen. Von diesem sind nach § 115 Satz 3 Nr. 3 ZPO aber unter anderem die Kosten der Unterkunft abzuziehen, soweit sie nicht in einem auffälligen Missverhältnis zu den Lebensverhältnissen der Parteien stehen. Aus diesem Grund ist der Mietvertrag oder der Kreditvertrag vorzulegen.

899 *Schaefer*, ZRP 2006, 94.

900 Zuständig ist der Rechtspfleger des Gerichts, das die Prozesskostenhilfe bewilligt hat, vgl. § 20 Nr. 4c RPflG.

901 Vgl. hierzu § 124 Nr. 2 ZPO. Die Gesetzesbegründung nimmt hierauf ausdrücklich Bezug, vgl. BT-Drs. 10/3054, 22.

902 *Schaefer*, ZRP 2006, 93; *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 173. Zur Begrenzung der Ausgaben für die Prozesskostenhilfe vgl. auch den Gesetzesantrag der

Um eine Mitwirkung des Betroffenen zu gewährleisten, sieht § 103 Abs. 1 Satz 1 ELENA-Verfahrensgesetz vor, dass ein Abruf bei der Zentralen Speicherstelle gespeicherten Daten nur zulässig ist, wenn der Teilnehmer sein Einverständnis (mit seiner qualifizierten Signatur) erklärt hat. Nach dieser Vorschrift sind also routinemäßige Kontrollen ohne Mitwirkung des Antragstellers gar nicht möglich. Vielmehr muss bei jedem Datenabruf ein Einverständnis eingeholt werden, was auch mit einem Aufwand verbunden ist.

Offenbar gehen die Befürworter der Einbindung von ELENA,[903] davon aus, dass sich das einmal erteilte Einverständnis zu einem Datenabruf zum Zweck einer Nachkontrolle – sogar bis zur Verjährung eines etwaigen Rückforderungsanspruchs[904] – auf weitere Datenabrufe zum Zweck von Nachkontrollen fortwirkt. Richtig daran ist nur, dass das einmal erteilte Einverständnis nach § 103 Abs. 1 Satz 2 ELENA-Verfahrensgesetz auch auf eine begrenzte Anzahl künftiger Abrufe ausgedehnt werden kann. Eine Einverständniserklärung auf unbestimmte Zeit oder eine unbegrenzte Zahl von Zugriffen ist jedoch nicht statthaft und führt zur Nichtigkeit der Erklärung.[905] Die Nachkontrolle hat der Rechtspfleger nach Verfahrensabschluss vorzunehmen. Zu diesem Zeitpunkt ist aber noch nicht absehbar, wie lange die Nachkontrolle dauert und wie viele Abrufe erforderlich sein werden. Das Einverständnis zu einem Datenabruf für die Nachkontrolle kann daher nicht auf weitere Abrufe ausgedehnt werden. Erst recht ist es nicht möglich, ein Einverständnis, das für die Überprüfungen der subjektiven Voraussetzungen der Prozesskostenhilfe bei der Antragstellung erteilt wurde, auf Datenabrufe für die spätere Nachkontrolle zu erstrecken.[906] Die Datenabrufe für die Überprüfung der subjektiven Voraussetzungen und die für spätere Nachkontrollen erfolgen zu unterschiedlichen Zwecken. Einmal geht es darum, das Vorliegen der Voraussetzungen des § 114 ZPO festzustellen, um dem Antragsteller den Zugang zu Gericht zu eröffnen. Diese Prüfung nimmt der Richter vor. Die Nachkontrolle, die vom Rechtspfleger vorgenommen wird, hat lediglich zum Ziel, Unbilligkeiten auszugleichen und die Ursprungsentscheidung zu ändern, falls sich herausstellt, dass sich die Vermögenslage wesentlich verändert hat.

Insgesamt bringt die hier anvisierte Einbeziehung von ELENA in das Prozesskostenhilfeverfahren also keinen großen Nutzen. Statt dessen wird der Datenschutz beim Prozesskostenhilfeverfahren erheblich verschlechtert. Der Betroffene wird vor die Wahl gestellt, sein Einverständnis zu einem Datenabruf zu erteilen oder ganz auf die Prozesskostenhilfe zu verzichten. Das derzeitige System der Prüfung der Bedürftigkeit ist durch ein abgestuftes System gekennzeichnet: Das Gericht prüft das Vorliegen der subjektiven Voraussetzungen zunächst auf der Grundlage der Angaben des Betroffenen.[907] Erst wenn Zweifel an der Richtigkeit der Angaben bestehen,

Länder Baden-Württemberg, Hessen, Niedersachen, Nordrhein-Westfalen, Schleswig-Holstein, Thüringen, BT-Drs. 16/1994.

903 *Schaefer*, ZRP 2006, 93; *Schaefer*, MMR 2006, X; *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 169.

904 Speziell hierzu *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 173

905 BR-Drs. 561/08, 51.

906 *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 173.

907 § 117 Abs. 2 ZPO.

kann das Gericht Erhebungen bei einer dritten Stelle anstellen.[908] Durch die Einbeziehung von ELENA in das Prozesskostenhilfeverfahren wird dieses System unterlaufen. Es wird sogleich um Auskunft bei einer dritten Stelle, der Zentralen Speicherstelle, ersucht, ohne die Daten vorher beim Betroffenen zu erfragen. Von den hier skizzierten Vorhaben sollte daher Abstand genommen werden. Sicherlich würde es für die Justiz eine Entlastung bringen, wenn die Daten elektronisch übermittelt werden würden und sogleich in ein Berechnungsprogramm eingetragen werden könnten. Für diesen Effekt bedarf es jedoch keines Datenabrufs bei einer Zentralen Speicherstelle. Hierzu würde es ausreichen, entsprechende Vorgaben und Datenformate im Zuge der Einführung einer elektronischen Akte zu entwickeln.

7.8.3 Datenabruf durch Rechtsanwälte

Soweit diskutiert wird, dass auch Rechtsanwälten der Zugriff auf ELENA gestattet werden muss,[909] ist dies erst recht abzulehnen. Das ELENA-Verfahren ist von seiner Zielsetzung und seiner derzeitigen Struktur her nicht für Abrufe von nicht-öffentlichen Stellen ausgelegt. Mit dem ELENA-Verfahren sollen Arbeitgeber und Verwaltung entlastet werden. Die Arbeitgeber sollen keine kostenträchtigen Papierbescheinigungen mehr ausstellen müssen und die Verwaltung soll Daten aus der Papierbescheinigung des Arbeitgebers nicht mehr manuell und fehleranfällig in elektronisch bearbeitete Vorgänge eingeben müssen.[910] Zugriff auf die Daten der Zentralen Speicherstelle haben nach dem ELENA-Verfahrensgesetz deshalb nur bestimmte öffentliche Stellen, die die Daten des Arbeitgebers zur Erfüllung ihrer Aufgaben benötigen. Diese öffentlichen Stellen müssen sich einem besonderen Zulassungsverfahren unterziehen,[911] sie müssen über die notwendigen technischen Einrichtungen verfügen und auch einen verantwortlichen Mitarbeiter benennen, der für die Verwaltung der Abrufbefugnisse dieser Behörde zuständig ist (sog. Abrufagent).[912]

Die Gerichte erledigen monatlich eine beträchtliche Zahl allein an Zivilverfahren. Davon sind viele Verfahren mit einem Antrag auf Prozesskostenhilfe verbunden. Eine hohe Zahl an Verfahren findet an den Landgerichten statt, wo Anwaltszwang besteht.[913] In vielen Zivilverfahren vor den Amtsgerichten lassen sich die Parteien von einem Anwalt vertreten. Wollte man – neben den Gerichten – nun auch jedem Anwalt, der einen Mandanten mit Prozesskostenhilfe vertritt, den Zugriff auf Daten aus der Zentralen Speicherstelle gestatten, würden die Missbrauchsrisiken erheblich steigen. Der Nutzen, der mit einem derartigen Datenabruf verbunden wäre, stünde in keinem Verhältnis zu den damit verbundenen Risiken für das Recht auf

908 § 118 Abs. 2 Satz 2 ZPO.

909 Vgl. hierzu *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 174, wonach der Rechtsanwalt ein vitales Interesse daran hat, vorab zu erfahren, welche Daten später an das Gericht übertragen werden, da er die Erfolgsaussichten des Prozesskostenhilfe-Antrags zur Frage der Bedürftigkeit nach §§ 114 ff. ZPO abschätzen muss.

910 BR-Drs. 561/08, 20 f.

911 Vgl. hierzu § 99 Abs. 7 ELENA-Verfahrensgesetz.

912 Vgl. § 102 ELENA-Verfahrensgesetz.

913 Vgl. § 78 Abs. 5 ZPO.

informationelle Selbstbestimmung der Betroffenen. Zwar ist es zutreffend, dass der Anwalt die Erfolgsaussichten des Prozesskostenhilfeantrags einschätzen können muss.[914] Vor der Einreichung des Prozesskostenhilfeantrags oder der Klageschrift findet jedoch eine persönliche Kontaktaufnahme, das Mandantengespräch, statt. Der Mandant selbst kann vor diesem Termin einen Auskunftsanspruch bei der Zentralen Speicherstelle stellen[915] und die entsprechenden Informationen dem Anwalt sodann samt den anderen Belegen zur Verfügung stellen.

7.9 E-Schutzschriftenregister

In einem Eilverfahren kann ein Richter einem Antrag auf Erlass einer einstweiligen Verfügung stattgeben, ohne dass er hierfür eine mündliche Verhandlung anberaumen muss. Der Richter entscheidet alleine aufgrund des Verfügungsantrages. Da der Antragsgegner vor Erlass der einstweiligen Verfügung nicht angehört wird,[916] wird dessen Grundrecht auf rechtliches Gehör nach Art. 103 Abs. 2 GG verkürzt.[917] Diese Verkürzung nimmt man jedoch in Fällen besonderer Dringlichkeit hin, um ein effektives Eilverfahren zu gewährleisten. Dennoch ist der Antragsgegner nicht ganz schutzlos gestellt: Wenn ein Antragsgegner davon ausgeht, dass gegen ihn eine einstweilige Verfügung beantragt wird, hat er die Möglichkeit, vorsorglich bei Gericht eine sog. Schutzschrift einzureichen.[918] Die Schutzschrift entspricht in ihrem Aufbau dem eines Verfügungsgesuchs.[919] Sie enthält Angaben zum Streitverhältnis und dem potentiellen Gegner. In diesem Schriftsatz wird die eigene Version des Streites dargelegt und glaubhaft gemacht.[920] Die Gerichte sind rechtlich verpflichtet, die Ausführungen in der Schutzschrift bei der Wahl ihres Verfahrens (Entscheidung durch Beschluss oder mündliche Verhandlung) und ihrer Entscheidungsfindung zu berücksichtigen.[921]

Die Schutzschrift ist bei dem Gericht einzureichen, das für den zu erwartenden Antrag auf Erlass einer einstweiligen Verfügung zuständig ist. In vielen Fällen sieht die ZPO für eine Streitigkeit jedoch verschiedene Gerichtsstände vor. Eine Schutzschrift muss deshalb bei allen in Betracht kommenden zuständigen Gerichten eingereicht werden. Dies geht für die Anwälte oder die Naturparteien mit einem großem Aufwand einher.[922] Auch für die Gerichte ist der Eingang einer Schutzschrift mit Belastungen verbunden. Wenn eine Schutzschrift eingereicht

914 So *Wahlmann*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 174.
915 § 103 Abs. 4 ELENA-Verfahrensgesetz.
916 Vgl. § 937 Abs. 2 ZPO.
917 *Zöller*, ZPO, § 937 Rn. 4.
918 Zur Schutzschrift vgl. etwa *Danckwerts*, GRUR 2008, 763; *Keller*, Jura 2007, 327; *Deutsch*, GRUR 1990, 327; *Schulz*, WRP 2009, 1472.
919 *Liebscher*, 1994, 91.
920 *Liebscher*, 1994, 91.
921 Vgl. hierzu *Zöller*, ZPO, § 937 Rn. 4. Die Schutzschrift ist in den 60er Jahren in Wettbewerbssachen entstanden, gesetzlich nicht geregelt, aber von der Rechtsprechung anerkannt. Vgl. hierzu *Liebscher*, 1994, 91.
922 Vgl. hierzu etwa `https://www.schutzschriftenregister.de/Informationen/Register.aspx` (Zugriff am 22.1.2010).

wird, muss sie zunächst dem Richter vorgelegt werden. Sodann wird sie in ein Register des Gerichts eingetragen. Sobald eine einstweilige Verfügung eingeht, muss geprüft werden, ob hierfür bereits eine Schutzschrift bei Gericht vorliegt.[923]

Um diesen Aufwand für Anwälte und Richter gering zu halten, hat die Europäischen EDV-Akademie des Rechts mit `www.schutzschriftenregister.de` ein zentrale Schutzschriftenregister entwickelt. Das Ziel dieses zentralen Schutzschriftenregisters wird wie folgt beschrieben:[924] „Im ZSR können Schutzschriften nebst Anlagen schnell und bequem elektronisch hinterlegt werden. Die Gerichte fragen das Register nur noch im konkreten Einzelfall online ab. Für den möglichen Antragsgegner eines Verfügungsantrages bzw. dessen Verfahrensbevollmächtigten entfällt damit die Notwendigkeit, bei allen in Betracht kommenden Gerichtsständen eine Schutzschrift einzureichen. Vor dem Hintergrund, dass z.B. in wettbewerbsrechtlichen Streitigkeiten jedes Landgericht zuständig sein kann, wird deutlich, dass die einmalige Hinterlegung eine erhebliche zeitliche und finanzielle Entlastung bietet. Die Gerichte haben die Möglichkeit, im ZSR etwa gespeicherte Schutzschriften abzurufen. Der Richter kommt dadurch erst bei Vorliegen des eigentlichen Verfügungsantrages mit der Schutzschrift in Berührung. So entfällt der Aufwand, die Schutzschriften entsprechend der Aktenordnung im Gericht zu registrieren, zu verwahren und zu archivieren. Dies bedeutet eine erhebliche Zeitersparnis, insbesondere, wenn man berücksichtigt, dass bei 95-98 Prozent der Schutzschriften kein Verfügungsantrag nachfolgt.“

Der Ablauf gestaltet sich folgendermaßen: Bevor erstmals eine Schutzschrift hinterlegt wird, muss sich der Prozessbevollmächtigte – ohne Identitätsprüfung – registrieren. Bei der Registrierung erhält der Nutzer ein Kennwort und ein Passwort. Wenn der Nutzer nun eine Schutzschrift hinterlegen will, muss er Angaben zu den potentiellen Verfahrensbeteiligten und zum Streitgegenstand machen und dann die Schutzschrift als elektronisches Dokument hochladen. Die Schutzschrift wird sodann 90 Tage in dem Register gespeichert. Sie wird nach den 90 Tagen automatisch gelöscht, wobei zu berücksichtigen ist, dass eine Speicherung um weitere 90 Tage bei einem entsprechenden Verlängerungsantrag möglich ist. Zudem kann die Schutzschrift jederzeit auch ganz aus dem Register gelöscht werden. Für die Speicherung einer Schutzschrift und für die Verlängerung der Speicherung fallen jeweils Gebühren in Höhe von 45 EUR zuzüglich Mehrwertsteuer an. Zur Begleichung dieser Gebühr mittels Bankeinzug muss der Nutzer seine Kontonummer und eine Einzugsermächtigung erteilen. Zum Abruf der Daten erhalten die Gerichte eine Kennung und ein Passwort. Bei der Suche nach einer Schutzschrift sind Angaben zu den Verfahrensbeteiligten und die Angabe des gerichtlichen Aktenzeichens zwingend. Die von den Rechtsanwälten eingereichten Schutzschriften werden bei der EEAR gGmbH gespeichert. Die Speicherung der Daten bei der gGmbH erfolgt weder im Auftrag der

[923] Vgl. hierzu etwa `https://www.schutzschriftenregister.de/Informationen/Register.aspx` (Zugriff am 22.1.2010).

[924] Vgl. hierzu etwa `https://www.schutzschriftenregister.de/Informationen/Register.aspx` (Zugriff am 22.1.2010).

Rechtsanwälte noch im Auftrag der Gerichte. Vielmehr ist die gGmbH selbst verantwortliche Stelle.[925]

7.9.1 Rechtsgrundlage für Speicherung bei der EEAR

Die Speicherung der Daten bei der EEAR ist insofern problematisch, als dass sich in der Schutzschrift Angaben zu dem potentiellen Gegner befinden. Neben dem Vor- und Nachnamen und der Anschrift werden in der Regel detaillierte Angaben zum Sachverhalt erfolgen, damit der Richter sich mit den Gegenargumenten auseinandersetzt und nicht sofort einen einstweiligen Verfügungsbeschluss erlässt. Die Speicherung der Daten über den potentiellen Gegner bei der gGmbH erfolgt ohne dessen Einwilligung. Ein Erlaubnistatbestand, der diese Formen der Datenverarbeitung rechtfertigen könnte, dürfte jedoch nicht vorhanden sein. Da die EEAR als juristische Person des Privatrechts eine nicht-öffentliche Stelle ist und die personenbezogenen Daten bei der EEAR unter Einsatz von Datenverarbeitungsanlagen gespeichert werden, kommen nach § 27 BDSG die Vorgaben der §§ 28, 29 BDSG zur Anwendung.

§ 28 BDSG regelt die Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke. Zu eigenen Geschäftszwecken im Sinne des § 28 Abs. 1 BDSG werden Daten gespeichert, wenn sie zum Beispiel für die Abwicklung eines Kauf- oder Dienstleistungsvertrages, eines Mitgliedschaftserwerbs und ähnlichen Rechtsgeschäften notwendig sind.[926] Unter diese Fallgestaltung fallen die Schutzschriften jedoch nicht. Die Schutzschriften werden nur deshalb bei der EEAR hinterlegt, damit die Gerichte diese später abrufen können. Die EEAR befasst sich nach ihrem Gesellschaftsvertrag mit der Durchführbarkeit und den Folgen der elektronischen Informationsverarbeitung in Recht und Verwaltung; sie soll Wissenschaft und Forschung fördern, insbesondere durch Förderung des Einsatzes von Informationstechnik im Rechtswesen und in der Verwaltung.[927] Somit könnte man sich überlegen, ob die Speicherung an den Vorgaben des § 28 Abs. 2 Nr. 3 BDSG, welche die Nutzung von Daten zu Forschungszwecken regelt, zu messen ist. Selbst wenn man jedoch die gGmbH als Forschungseinrichtung im Sinne dieser Vorschrift ansehen würde, würden die Daten nicht zur Durchführung der wissenschaftlichen Forschung gespeichert. Bei der Ausgestaltung des zentralen Schutzschriftenregisters handelt es sich nicht um ein Pilotprojekt. Für die Durchführung eines derartigen Projektes würden keine personenbezogenen Daten der potentiellen Antragsteller benötigt werden. Die Daten werden vielmehr für ein „normales“ Verfahren nach der ZPO gespeichert und mehrere Gerichte haben im Rahmen einer Selbstverpflichtung gegenüber der EEAR kundgetan, die Daten in diesem Verzeichnis abzurufen. § 28 Abs. 2 Nr. 3 BDSG ist daher nicht einschlägig.

§ 29 BDSG setzt voraus, dass personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert werden. Für die Speicherung einer Schutzschrift und für die Verlängerung der Speicherung verlangt die EEAR jeweils Gebühren in Höhe von 45 EUR zuzüglich Mehr-

[925] Vgl. hierzu etwa `https://www.schutzschriftenregister.de/Informationen/Register.aspx` (Zugriff am 22.1.2010).

[926] Vgl. hierzu *Schaffland/ Wiltfang*, BDSG, § 28 Rn. 3.

[927] 15. Deutscher EDV-Gerichtstag, Grußwort des Vorsitzenden.

wertsteuer. Damit liegt eine geschäftsmäßige Speicherung vor. Da die Schutzschriften nur deshalb bei der EEAR hinterlegt werden, damit die Gerichte diese später abrufen können, erfolgt die Speicherung zum Zweck der Übermittlung. Nach § 29 Abs. 1 Nr. 1 BDSG ist das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat. Hiervon kann jedoch nicht ausgegangen werden. Der mögliche Antragsteller einer einstweiligen Verfügung hat ein schutzwürdiges Interesse daran, dass seine Daten bei der EEAR nicht gespeichert werden. Im Vergleich zu der Hinterlegung einer Schutzschrift bei einem einzelnen Gericht ist das Missbrauchsrisiko und die Gefahr von Zweckänderungen durch die zentrale Datenhaltung und die Speicherung bei einer privaten Stelle erhöht. Bei der Anmeldung werden die Prozessbevollmächtigten nicht zuverlässig registriert. Für eine Registrierung reichen Angaben zu Vor- und Nachname und der Adresse des Prozessbevollmächtigten aus sowie die Angaben eines individuellen Kennwortes oder Passwortes. Es kommt hinzu, dass die Gerichte rechtlich nicht dazu verpflichtet sind, das Verzeichnis überhaupt einzusehen. Insofern werden personenbezogene Daten gespeichert, obwohl nicht feststeht, dass die Gerichte diese überhaupt in das Verfahren einbeziehen werden. Nach den derzeitigen Verfahren hat der potentielle Antragsteller – zumindest nach einer Meinung – auch das Recht, das Schutzschriftenregister bei Gericht in Analogie zu § 299 ZPO einzusehen.[928] Dieses Recht kann ein Antragsteller nicht wahrnehmen, wenn die Daten bei der EEAR gespeichert sind. Der für den Antragsteller noch verbleibende Auskunftsanspruch nach § 34 BDSG kann mit dem Recht auf Akteneinsicht nicht verglichen werden. Die einzige noch mögliche Rechtsgrundlage für eine Datenspeicherung, nämlich § 29 Abs. 1 Nr. 1 BDSG, ist daher auch nicht einschlägig.

7.9.2 Schutzschriftenregister als staatliche Aufgabe

Die Verwaltung von Schutzschriften ist eine ureigene staatliche Aufgabe. Sie muss daher bei den Gerichten verbleiben. Aus diesem Grund sollte das Projekt in dieser Form nicht weitergeführt werden. Zwar ist die Idee, ein zentrales Schutzschriftenregister einzuführen, durchaus sinnvoll. Die Schutzschriften sollten jedoch bei einem zentralen Gericht oder einer juristischen Person des öffentlichen Rechts im Auftrag der Justiz gespeichert werden. Bei dem Datenabruf durch die einzelnen Gerichte wäre dann darauf zu achten, dass der Zugang zu dem Verzeichnis nur einem beschränkten Kreis von Mitarbeitern möglich ist. Dieser Kreis müsste zuvor klar definiert sein. Zudem müsste ein unberechtigter Zugang durch Sicherungsmittel wie Benutzerkennung und Passwort ausgeschlossen werden. Des Weiteren müssten die Suche – wie das jetzt schon bei der EEAR der Fall ist – auf das Aktenzeichen und die Parteien des Verfügungsverfahrens beschränkt sein. Auch wäre eine zuverlässige Registrierung durch die Rechtsanwälte erforderlich. Diese könnte in Zukunft entweder über den elektronischen Personalausweis oder über Bürgerportale oder dem Projekt S.A.F.E. erfolgen.

[928] Zum Meinungsstand vgl. ausführlich *Liebscher*, 1994, 92 ff.

7.10 Zusammenfassung

Um ein elektronisches Zivilverfahren sicher gestalten zu können, ist für eine elektronische Klageeinreichung sowie für die Einreichung von Mahnanträgen der Einsatz von qualifizierten elektronischen Signaturen erforderlich. Der Gesetzgeber sollte dies an den entsprechenden Stellen im Gesetzestext zum Ausdruck bringen. Der Gesetzgeber hat im Zivilverfahren für gleiche Sachverhalte unterschiedliche Regelungen getroffen. So hat er bestimmt, dass im Rahmen des § 174 Abs. 3 ZPO Schriftstücke gegen unbefugte Kenntnisnahme zu schützen sind, bei § 130a ZPO hat er jedoch keine entsprechenden Vorgaben getroffen. Auch bei den öffentlichen Bekanntmachungen nach der ZPO hat sich der Gesetzgeber nicht an anderen Bestimmungen (§ 9 Abs. 2 InsO i.V.m. der dazu ergangenen Bekanntmachungsverordnung) orientiert. Insgesamt fällt also eine gewisse Inkonsistenz bei der Ausgestaltung der Modernisierungsformen auf, die zu Lasten des Datenschutzes geht.

Im Rahmen der elektronischen Akteneinsicht sowie bei den elektronischen Zustellungen erweisen sich der elektronische Personalausweis, die Bürgerportale und das Projekt S.A.F.E. als zukunftsträchtige Anwendungsformen, um den Datenschutz bei diesen Abläufen zufriedenstellend gestalten zu können. Bei der noch zu erlassenden Rechtsverordnung für eine elektronische Aktenführung im Zivilverfahren wird der Verordnungsgeber die genannten technisch-organisatorischen Anforderungen an den Datenschutz beachten müssen. Mit Hilfe einer Neusignierung und eines bereits erprobten Verfahrens für eine Transformation von elektronischen Dokumenten sind keine Probleme bei der Archivierung von elektronisch geführten Akten zu erwarten.

Abzulehnen ist die Einbeziehung von ELENA in das Prozesskostenhilfeverfahren. Gegen das ELENA-Verfahrensgesetz bestehen verfassungsrechtliche Bedenken und ein Datenabruf durch die Gerichte brächte ohnehin keinen besonders großen Nutzen – der Rechtsschutz eines Antragstellers auf Prozesskostenhilfe dagegen würde ohne Grund verkürzt werden. Ebenso abzulehnen ist die derzeitige Ausgestaltung eines zentralen Schutzschriftenregisters bei der EEAR gGmbH. Die Schutzschriften werden dort ohne Rechtsgrundlage gespeichert. Ein elektronisches zentrales Schutzschriftenregister macht zwar durchaus Sinn. Dieses sollte aber von den Gerichten selbst betrieben werden.

Kapitel 8

Zwangsvollstreckung und Zwangsversteigerung

Nachdem der Datenschutz bei den elektronischen Abläufen im Zivilverfahren betrachtet wurde, werden nun die datenschutzrechtlichen Aspekte bei den neuen Verfahrensabläufen im Zwangsvollstreckungs- und Zwangsversteigerungsverfahren herausgearbeitet. Zunächst wird das elektronische Schuldnerverzeichnis betrachtet. Im Anschluss daran folgen Ausführungen zum elektronischen Vermögensverzeichnis und zur vereinfachten elektronischen Antragstellung für einen Pfändungs- und Überweisungsbeschluss. Sodann folgen Untersuchungen zur elektronischen Akteneinsicht, zur elektronischen Bekanntmachung und zur Internetversteigerung. Die Untersuchungen zum Schuldnerverzeichnis, zum zentralen Vermögensverzeichnis und der vereinfachten Antragstellung erfolgen auf der Grundlage des bereits beschlossenen und zum 1.1.2013 in Kraft tretenden Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung.

8.1 E-Schuldnerverzeichnis

Die Auskunft aus einem Schuldnerverzeichnis stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 GG dar und bedarf daher einer gesetzlichen Grundlage. § 16 LDSG kann hierfür nicht einschlägig sein. Der Anwendungsbereich ist zwar auf den ersten Blick eröffnet: Die Schuldnerverzeichnisse werden bei einem Gericht[929] und damit einem Organ der Rechtspflege nach § 2 Abs. 1 Nr. 2 LDSG geführt. In ihnen werden auch personenbezogene Daten nach § 3 LDSG gespeichert.[930] Allerdings gehen die §§ 882b ff. ZPO neu den Datenschutzgesetzen als bereichsspezifische Regelungen vor.[931] Für eine direkte oder analoge Heranziehung der Datenschutzgesetze ist insoweit kein Raum.[932]

[929] Amtsgericht nach § 915 ZPO und in Zukunft zentrales Vollstreckungsgericht, § 882h Abs. 1 ZPO neu.
[930] § 1 Abs. 1 SchuVVO und § 882b Abs. 2 ZPO neu.
[931] Zu §§ 915 ff. ZPO vgl. etwa BGH VersR 1988, 38; OLG München, NJW 1982, 244 f.
[932] *Prütting*, ZZP 1993, 448.

Von den Schuldnerverzeichnissen sind die privatrechtliche Warndateien abzugrenzen. Die bekannteste Warndatei ist die Schufa. Sie wurde 1927 gegründet und verfügt über 440 Millionen Einzeldaten von 65 Millionen natürlichen Personen.[933] Geschäftszweck der Schufa ist es, ihren Vertragspartnern Informationen über die Kreditwürdigkeit von Kunden zu geben und sie so vor Verlusten zu schützen.[934] Da die Schufa eine nicht-öffentliche Stelle ist, richtet sich die Zulässigkeit ihrer Datenübermittlung und -erhebung nach den Vorgaben der §§ 28, 29 BDSG.[935] Die rechtliche Situation von staatlichen Schuldnerverzeichnissen und privaten Warndateien ist daher – um mit Prütting zu sprechen – vollkommen anders.[936]

Wie bereits beschrieben,[937] befanden sich bislang nur wenige Vorschriften zu automatisierten Verarbeitungen beim Schuldnerverzeichnis. Mit den Regelungen in den §§ 882b ff. ZPO, die aufgrund des Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung hinsichtlich ihres wesentlichen Inhalts zum 1.1.2013 in Kraft treten,[938] wird sich dies jedoch in Zukunft grundlegend ändern.[939] Nach § 882h Abs. 1 ZPO neu stellt das Schuldnerverzeichnis ab dem 1.1.2013 ein Internet-Register dar, welches durch ein zentrales Vollstreckungsgericht geführt werden wird. Damit sollen sämtliche anfallenden Daten dem Rechtsverkehr zeitnah, zuverlässig und kostengünstig zur Verfügung gestellt werden.[940] Der Inhalt des Schuldnerverzeichnisses kann über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden.[941] In dieses Schuldnerverzeichnis wird im Gegensatz zu § 915 ZPO nicht mehr eingetragen, wer die eidesstattliche Versicherung abgegeben oder gegen wen die Haft angeordnet worden ist. Eingetragen wird vielmehr derjenige, der seinen vollstreckungsrechtlichen Auskunftspflichten nicht mehr nachkommt oder gegen den die Vollstreckung erfolglos war. Im Einzelnen sind die Eintragungsgründe in dem künftig geltenden § 882c ZPO neu aufgezählt.

Die Auskunft aus dem Schuldnerverzeichnis wird in Zukunft in § 882f ZPO neu geregelt sein. Ebenso wie § 915b ZPO verlangt der künftige § 882f Satz 1 ZPO neu für eine Auskunft die Darlegung für Zwecke der Zwangsvollstreckung (Nr. 1),[942] um gesetzliche Pflichten zur Prüfung der wirtschaftlichen Zuverlässigkeit zu erfüllen (Nr. 2),[943] um die Voraussetzungen für die Gewährung von öffentlichen Leistungen zu prüfen (Nr. 3),[944] um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungspflichten nicht

933 *Rottwilm*, 2008.
934 Vgl. zur Schufa *Kamlah*, MMR 1999, 395, speziell zur Einwilligungserklärung *Hornung*, CR 2007, 753.
935 Vgl. hierzu im Einzelnen *Duhr*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 1157.
936 *Prütting*, ZZP 1993, 448.
937 Siehe hierzu Abschnitt 2.3.2
938 Zum Inkrafttreten vgl. Art. 6.
939 Zur Reform der Sachaufklärung insgesamt vgl. *Seip*, DGVZ 2008, 38; *Jäger*, Rbeistand 2008, 43; *Jäger*/*Schatz*, ZVI 2008, 143.
940 BR-Drs. 304/08, 90.
941 Vgl. § 882h Abs. 1 Satz 2 ZPO.
942 Ein vollstreckungsbedingtes Einsichtsrecht besteht insbesondere hinsichtlich der Entscheidung, ob ein Vollstreckungsversuch unternommen wird, BT-Drs. 16/10069, 41.
943 Voraussetzung ist also eine Prüfungspflicht, eine Prüfungsbefugnis genügt nicht, BT-Drs. 16/10069, 41.
944 Hierunter fallen insbesondere Anfragen von Sozialleistungsträgern, BT-Drs. 16/10069, 41.

nachkommen (Nr. 4)[945] oder für Zwecke der Strafverfolgung (Nr. 5). Neu wird nach § 882f Satz 1 Nr. 6 ZPO neu sein, dass der Schuldner auch Auskunft über ihn selbst betreffende Daten verlangen kann. Auf diese Weise wollte der Gesetzgeber sicherstellen, dass der Schuldner sich über ihn betreffende Eintragungen informieren und gegebenenfalls eine Löschung erwirken kann.[946] Im Übrigen wird der künftige § 882f Satz 1 ZPO neu – wiederum gleich wie § 915b ZPO – lediglich die „Darlegung", dass einer der aufgeführten Zwecke vorliegt, verlangen.

Die Kammern und bestimmte andere Personen[947] können trotz der verbesserten Einsichtsmöglichkeiten in Zukunft auch weiterhin Abdrucke aus dem Schuldnerverzeichnis erhalten. Die Vorschrift des § 882g ZPO neu entspricht fast vollständig[948] den bislang geltenden §§ 915d ff. ZPO. Sie wurde lediglich aus Gründen der Übersichtlichkeit in einem Paragraphen zusammengefasst.[949]

In einer Rechtsverordnung sollen nach § 882h Abs. 3 ZPO nähere Regelungen zu Form und Übermittlung der Eintragungsanordnungen, zum Inhalt des Schuldnerverzeichnisses und zur Ausgestaltung der Einsicht getroffen werden. Außerdem soll die Rechtsverordnung geeignete Maßnahmen zur Sicherung des Datenschutzes und der Datensicherheit vorsehen. Hierzu gehören insbesondere Maßnahmen, die sicherstellen, dass die Daten bei der elektronischen Übermittlung an das zentrale Vollstreckungsgericht sowie an eine andere Stelle gegen unbefugte Kenntnisnahme geschützt sind,[950] die Daten unversehrt und vollständig wiedergegeben werden,[951] jederzeit ihrem Ursprung nach zugeordnet werden können[952] und nur von registrierten Nutzern nach Angabe des Verwendungszweckes abgerufen werden können[953]. Überdies soll sichergestellt werden, dass jeder Abrufvorgang protokolliert wird und Nutzer im Fall des missbräuchlichen Datenabrufs oder einer missbräuchlichen Datenverwendung von der Einsichtnahme ausgeschlossen werden können[954]. Die Ermächtigung zum Erlass dieser Rechtsverordnung ist nach Art. 6 des Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung bereits am 1.8.2009 in Kraft getreten.

Bislang ist der Eintragungsinhalt in einer Verordnung, der SchuVVO,[955] enthalten. In Zukunft ist der Eintragungsinhalt nicht mehr in einer Rechtsverordnung geregelt, sondern – wie sich

---

945 Nach der amtlichen Begründung soll diese Regelung dem berechtigten Interesse des Geschäftsverkehrs Rechnung tragen, sich rechtzeitig und mit vertretbaren Aufwand der Kreditwürdigkeit seiner Geschäftspartner vergewissern zu können, BT-Drs. 16/10069, 41.

946 BR-Drs. 304/08, 88.

947 Zum Beispiel Handelsauskunfteien, wenn ihrem berechtigten Interesse durch Einzelauskünfte nicht hinreichend Rechnung getragen werden kann. Vgl. hierzu *Zöller*, ZPO, § 915e Rn. 4.

948 Zu den beiden Abweichungen vgl. BT-Drs. 16/10069, 42.

949 BR-Drs. 304/08, 89.

950 Abs. 3 Satz 3 Nr. 1.

951 Abs. 3 Satz 3 Nr. 2.

952 Abs. 3 Satz 3 Nr. 3.

953 Abs. 3 Satz 3 Nr. 4.

954 Abs. 3 Satz 4 Nr. 4.

955 Schuldnerverzeichnisverordnung vom 15.12.1994 (BGBl. 1994 I, 3822), zuletzt durch Artikel 3 des Gesetzes vom 13.12.2001 (BGBl. 2001 I, 3638) geändert. Zur Schuldnerverzeichnisverordnung vgl. etwa *Lappe*, NJW 1995, 1657.

aus § 882b Abs. 2 und 3 ZPO neu ergibt – im Gesetz selbst. Der Gesetzgeber hat dies mit der erhöhten Publizität begründet, die das neue Veröffentlichungsmedium Internet mit sich bringe. Insoweit sei es datenschutzrechtlich geboten, den Verzeichnisinhalt gesetzlich festzulegen.[956] Was den Eintragungsinhalt selbst betrifft, so ist festzustellen, dass dieser sinngemäß von § 1 SchuVVO übernommen wurde.[957] So werden einerseits eingetragen der Name und der Vorname des Schuldners.[958] Außerdem werden nach § 882b Abs. 2 Nr. 1 ZPO neu – so wie bislang auch[959] – gemäß § 882b Abs. 2 Nr. 2 der Geburtsname des Schuldners und – das ist neu – bei einem Kaufmann zusätzlich die Firma und die Handelsregisternummer eingetragen. Eine Verpflichtung, diese Angaben einzutragen, besteht nur, wenn sie bekannt sind. Damit will der Gesetzgeber verhindern, dass die Eintragung in das Schuldnerverzeichnis dadurch verzögert wird, dass der Schuldner diese Angaben verweigert.[960] Eine Bindung des Eintragungsinhalts durch § 1 Abs. 1 Nr. 1 SchuVVO an das Rubrum des Titels, der dem Vollstreckungsverfahren zugrunde liegt, entfällt in Zukunft. Künftig können sich mehrere Eintragungen im Schuldnerverzeichnis überlagern. Da sichergestellt werden soll, dass denselben Schuldner betreffende Eintragungen sicher identifiziert werden, sollen bereits bei Eintragung als überholt oder als unrichtig bekannte Titeldaten ausschließlich die richtigen Daten eingetragen werden.[961] Zudem wird, wie bislang auch,[962] das Geburtsdatum und der Geburtsort des Schuldners eingetragen, um Verwechslungen zu vermeiden. Eine Eintragung dieser Daten hat ebenfalls nur zu erfolgen, wenn sie bekannt sind, d.h. wenn sie sich etwa aus dem Vermögensverzeichnis oder aus dem Vollstreckungstitel entnehmen lassen. Nachforschungen des zuständigen Gerichts, des Gerichtsvollziehers oder der Vollstreckungsbehörde sind also nicht erforderlich.[963]

In das künftige Schuldnerverzeichnis werden nach § 882b Abs. 2 Nr. 3 ZPO neu auch die Wohnsitze des Schuldners eingetragen werden. Wenn die Wohnsitzangaben eines Schuldners aufgrund verschiedener Vollstreckungsanträge voneinander abweichen, dann sollen nach dem Willen des Gesetzgebers im Hinblick auf die Warn- und Informationsfunktion des Registers alle Wohnanschriften eingetragen werden. Wollte man dies verhindern, müsste man die Anschrift oder Anschriften des Schuldners jeweils aktuell halten. Der Gesetzgeber hat hiervon jedoch abgesehen, da er eine umfassende Überwachung des Schuldners während des Eintragungszeitraums zu gewährleisten hatte.[964] Zur Erleichterung der Identifikation des Schuldners und zur Vermeidung von Verwechslungen ist in § 882b Abs. 2 ZPO neu bestimmt, dass auch die Eintragung abweichender Personendaten möglich ist, wenn sie bekannt sind.[965] Dies können

[956] BR-Drs. 304/08, 75.
[957] BR-Drs. 304/08, 75.
[958] Nicht eingetragen wird, wie bislang in § 1 Abs. 3 SchuVVO schon vorgesehen, der gesetzliche Vertreter des Schuldners. Eine ausdrückliche gesetzliche Klarstellung erschien dem Gesetzgeber aufgrund des eindeutigen Wortlauts entbehrlich, BR-Drs. 304/08, 75.
[959] § 1 Abs. 1 Nr. 1 SchuVVO.
[960] BR-Drs. 304/08, 75 f.
[961] BR-Drs. 304/08, 76.
[962] § 1 Abs. 1 Nr. 2 SchuVVO.
[963] BR-Drs. 304/08, 75 f.
[964] BR-Drs. 304/08, 76.
[965] Vgl. etwa *LfD Bayern*, 17. Tätigkeitsbericht, Tz. 7.6.1.2, wonach ein Bediensteter im Zuge des Verfahrens zur Abnahme der eidesstattlichen Versicherung gegen einen Dritten mit gleichem Vornamen fehlerhaft den

zum Beispiel Alias- oder Künstlernamen oder ehemalige Namen von Geschiedenen sein.[966] Letztlich schreibt § 882b Abs. 3 Nr. 1 ZPO neu vor, dass das Aktenzeichen des Gerichts bzw. die Vollstreckungsbehörde der Vollstreckungssache oder des Insolvenzverfahrens anzugeben ist und § 882b Abs. 3 Nr. 2-4 ZPO neu bestimmt, dass das Datum der Eintragungsanordnung und der Grund, der zur Eintragung in das Schuldnerverzeichnis geführt hat, eingetragen werden.

8.1.1 Verfassungsmäßigkeit

Bei der Bewertung des elektronischen Schuldnerverzeichnisses muss sich zunächst gefragt werden, ob die Führung eines Schuldnerverzeichnisses überhaupt mit der Verfassung in Einklang steht. So ist das Schuldnerverzeichnis in erheblichem Maße dazu geeignet, eine Person abzustempeln und als nicht zahlungskräftig zu brandmarken. Wenn eine Person im Schuldnerverzeichnis eingetragen ist, wird sie sich in der Regel im Wirtschaftsleben schwer tun. Potentielle Geschäftspartner und Kreditgeber beziehen vor Abschluss eines Geschäftes oft Informationen über die Solidität ihres künftigen Vertragspartners. Für diesen Personenkreis stellt das Schuldnerverzeichnis eine interessante Informationsquelle dar. Es ist stets aktuell gehalten und verfügt über eine staatliche Richtigkeitsgewähr. Wenn der Gläubiger erkennt, dass ein Schuldner im Verzeichnis eingetragen ist, wird er in der Regel den Geschäftskontakt abbrechen. Die Eintragung in das Schuldnerverzeichnis geht daher mit einem intensiven Eingriff in das Recht auf informationelle Selbstbestimmung einher.

Auf der anderen Seite hat es der Schuldner hingegen selbst in der Hand, ob er in das Schuldnerverzeichnis eingetragen wird oder nicht. Denn: Eingetragen wird er nur, wenn gegen ihn ein Titel erstritten wurde und dazu weitere Voraussetzungen erfüllt sind.[967] Ohne eine Eintragung in die „amtliche schwarze Liste“ hätten Gläubiger keine Möglichkeit zu erfahren, ob es sich überhaupt lohnt, derzeit einen Titel gegen den Schuldner zu erwirken und ihn gegebenenfalls zwangsweise durchzusetzen. Ist der Schuldner nämlich zahlungsunfähig, besteht für den Gläubiger die Gefahr, dass er auf seinen bereits verauslagten Prozesskosten[968] und Kosten der Zwangsvollstreckung[969] sitzen bleibt. Zum anderen hätten auch zukünftige Vertragspartner keine Möglichkeiten, sich darüber zu informieren, ob sie es mit einem zahlungswilligen und zahlungsfähigen Schuldner zu tun haben. So besteht insbesondere bei den Kreditinstituten ein großes Bedürfnis danach, sich ein zuverlässiges Bild über die Zahlungsfähigkeit und Zahlungswilligkeit eines potentiellen Kunden zu machen. In diesem Sinne kommt dem Schuldnerverzeichnis also eine besondere Schutz- und Warnfunktion zu.[970]

Vornamen abgeändert hatte. Dem Betroffenen sind daraufhin Schwierigkeiten bei der Fremdfinanzierung eines Bauvorhabens entstanden.

966 BR-Drs. 304/08, 77.

967 Vgl. § 915 ZPO und § 882c ZPO neu.

968 § 91 ZPO.

969 § 788 ZPO.

970 *Musielak*, ZPO, § 915 Rn. 1. Das BVerfG (NJW 1988, 3010) will dem Schuldnerverzeichnis darüber hinaus noch eine weitere Funktion beimessen: Es trage auch zur Verringerung volkswirtschaftlicher Fehlentwicklungen und zur Abwehr der Wirtschaftskriminalität bei. Ein rechtlich geordneter, ziel- und zweckgebun-

Mit der Gesetzesänderung von 1994[971] wurden eine Reihe von Vorschriften eingeführt, die das informationelle Selbstbestimmungsrecht des Schuldners gestärkt haben: Wegfall eines unbeschränkten Einsichtsrechts in das Schuldnerverzeichnis,[972] Zweckbindung für alle Informationen aus dem Schuldnerverzeichnis,[973] Regelungen zur Gewährleistung der Aktualität und Richtigkeit gespeicherter Daten aus dem Schuldnerverzeichnis, Verwertungsverbote bei Beendigung des laufenden Bezuges, präzise Löschungsfristen,[974] Verpflichtung zur vertraulichen Behandlung der Daten,[975] Befugnis zum Bezug von Listen über Eintragungen nur aufgrund vorheriger Bewilligung sowie präzise Verwendungsbeschränkungen bei den aus den Listen erlangten Informationen.[976] Bei dieser Reform[977] hat der Gesetzgeber das informationelle Selbstbestimmungsrecht des Schuldners berücksichtigt und es in einen angemessenen Ausgleich mit dem Interesse der Allgemeinheit, sich über die Zahlungsfähigkeit und -willigkeit eines Vertragspartners informieren zu können, gebracht.[978] Mit dieser Reform kann die Ausgestaltung des Schuldnerverzeichnisses als verfassungsgemäß bezeichnet werden.[979]

Mit den neuen Gesetzesänderungen zum Internet-Schuldnerverzeichnis verfolgt der Gesetzgeber das Ziel, das Schuldnerverzeichnis zu modernisieren und die Zwangsvollstreckung durch eine Vernetzung der bislang lediglich örtlich bei den Amtsgerichten geführten Schuldnerverzeichnisse zu effektivieren.[980] Dass dies mit einem intensiveren Eingriff in das informationelle Selbstbestimmungsrecht der Schuldner einhergeht, hat der Gesetzgeber erkannt. Gleichwohl sah er ein Bedürfnis hierfür. Als Ausgleich hierfür hat er an verschiedenen Stellen Vorkehrungen getroffen. Man wird das Internet-Schuldnerverzeichnis daher wohl als verfassungskonform bezeichnen können. Dennoch wären aus datenschutzrechtlicher Sicht an verschiedenen Stellen Änderungen wünschenswert.[981]

---

dener Informationsfluss innerhalb des ökonomischen Prozesses diene dem Schutz letztlich aller Marktteilnehmer und damit einem überwiegendem Allgemeininteresse.

971 Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15.7.1994, BGBl. 1994 I, 1566.

972 § 915b Abs. 1 ZPO.

973 § 915 Abs. 3 ZPO.

974 § 915a ZPO.

975 § 915d Abs. 2 ZPO.

976 § 915f und g ZPO.

977 Vgl. hierzu *Schnigula*, 2001, 242 ff.; *Lappe*, NJW 1994, 3067; *Hornung*, Rpfleger 1995, 233.

978 In diese Richtung auch *BfD*, 15. Tätigkeitsbericht, Tz. 4.8.

979 Vor der Reform wurde das Schuldnerverzeichnis für verfassungswidrig gehalten von *Straub*, 1995; *Leue*, in: *Vollkommer* (Hrsg.), Datenverarbeitung und Persönlichkeitsschutz, 102; *Zabel*, RpflStud 1999, 66. Das Bundesverfassungsgericht hatte die Frage der Verfassungswidrigkeit jedoch verneint, vgl. BVerfG NJW 1988, 423 (für § 107 Abs. 2 KO). So auch OLG Frankfurt, NJW 1988, 310 (für § 915 ZPO). Diese Ansicht wurde etwa von *Prütting*, ZZP 1993, 449 geteilt.

980 BR-Drs. 304/08, 1.

981 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kritisierte die Ausgestaltung des Schuldnerverzeichnisses als Internet-Register, vgl. hierzu *BfDI*, 20. Tätigkeitsbericht, Tz. 7.1.4. Nach seiner Meinung dürfe es ein Internet-Register zahlungsunfähiger Schuldner nicht geben. Zur Begründung führte er aus, dass damit die Zahlungsunfähigkeit des Schuldners weltweit zugänglich werden würde und auch nicht sichergestellt werden könne, wie die Daten im Internet wieder gelöscht werden können. In seinem Tätigkeitsbericht schreibt er: „Zum anderen beobachte ich mit Sorge, dass das Schuldnerverzeichnis nach dem Vorschlag der Arbeitsgruppe als öffentliches Register im Internet ausgestaltet werden soll. Damit

8.1.2 Zentralisierung des Schuldnerverzeichnisses

Diese Änderungen betreffen weniger die Konzeption des zukünftigen Schuldnerverzeichnisses in Form eines zentralen Verzeichnisses. Zentrale Strukturen gehen zwar mit großen Datensammlungen einher und sind von daher als kritisch zu beurteilen. Gleichwohl besteht für eine Vernetzung der Schuldnerverzeichnisse ein Bedarf. So sind die Gerichtsvollzieher darauf angewiesen, schnell zu erfahren, ob eine bestimmte Person im Verzeichnis eingetragen ist oder nicht. Ist nämlich ein Schuldner im Verzeichnis eingetragen, hat dies zur Folge, dass der Gerichtsvollzieher ihn binnen zwei Jahren nicht nochmals zur Auskunft über sein Vermögen auffordern darf, wenn ein Gläubiger keine Tatsachen glaubhaft gemacht hat, die auf eine wesentliche Veränderung der Vermögensverhältnisse des Schuldners schließen lassen. Dies bestimmt der künftige § 802d ZPO neu.[982] Auch der Erlass eines Haftbefehls durch einen Richter zur Erzwingung einer Vermögensauskunft wäre unzulässig.[983]

Auch bislang hat die Eintragung des Schuldners in das Schuldnerverzeichnis zur Folge, dass der Gerichtsvollzieher den Schuldner mit Ausnahme des § 903 ZPO[984] binnen drei Jahren nicht nochmals zur Abgabe einer eidesstattlichen Versicherung auffordern darf und der Richter keinen Haftbefehl gegen ihn nach § 901 ZPO erlassen darf. Da die Schuldnerverzeichnisse derzeit noch dezentral bei den einzelnen Amtsgerichten geführt werden und dort die Daten von „fremden Schuldnern“, d.h. von Schuldnern, für die das Amtsgericht nicht zuständig ist, nicht gespeichert werden, kam es in der Praxis immer dann zu Problemen, wenn der Schuldner seinen Wohnsitz gewechselt hatte, nachdem er im Schuldnerverzeichnis eingetragen worden war.[985] Zuständig für die Abnahme der eidesstattlichen Versicherung ist nach § 899 ZPO nämlich der Gerichtsvollzieher bei dem Amtsgericht, in dessen Bezirk der Schuldner zum Zeitpunkt der Auftragserteilung des Gläubigers seinen Wohnsitz hat. Wenn der Schuldner vor der Auftragserteilung aber seinen Wohnsitz in einem anderen Amtsgerichtsbezirk hatte und deshalb dort eingetragen war, ging die Abfrage des Gerichtsvollziehers bei „seinem“ Amtsgericht ins Leere und für den Schuldner bestand die Gefahr, die eidesstattliche Versicherung nochmals abgeben zu müssen. Zudem war der Schuldner, wenn er nicht beim Pfändungsversuch anwesend war und auch zum Termin zur Abgabe der eidesstattlichen Versicherung nicht erschienen ist, der

würde die Zahlungsunfähigkeit des Schuldners weltweit zugänglich. Zudem stellt sich die Frage, ob und wie die im Internet veröffentlichten Angaben jemals wieder gelöscht werden können. Den Vorschlag eines Internetregisters kann ich daher nicht unterstützen. Ich werde die weitere Entwicklung der Reformarbeiten weiterhin kritisch begleiten.“

982 Der Gesetzentwurf sah ursprünglich noch drei Jahre vor, BT-Drs. 16/10069, 6. Im Laufe des Gesetzgebungsverfahrens wurde die Frist auf zwei Jahre verkürzt, BT-Drs. 16/13432, 10. Zur Forderung, die dreijährige Frist auf ein Jahr zu verkürzen, vgl. *Deutscher Gerichtsvollzieher Bund e.V.*, 2008.

983 Vgl. § 802g ZPO neu.

984 Nach § 903 ZPO darf der Gerichtsvollzieher den Schuldner zur erneuten Abgabe einer eidesstattlichen Versicherung binnen drei Jahren nach der ersten Erklärung auffordern, wenn glaubhaft gemacht wird, dass der Schuldner später Vermögen erworben hat oder dass ein bisher bestehendes Arbeitsverhältnis mit dem Schuldner aufgelöst ist.

985 *Diederich*, 2003.

Gefahr einer Verhaftung nach § 901 ZPO ausgesetzt.[986] Mit den künftig geltenden Regelungen werden vergleichbare Situationen nicht mehr vorkommen. In Zukunft wird es landesweit nur noch ein zentrales Vollstreckungsgericht geben. Der Inhalt des Schuldnerverzeichnisses kann über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden.[987]

Damit bleibt festzuhalten, dass ein Bedarf an einer Zentralisierung durchaus besteht.[988] Zwar hatte § 915h Abs. 2 ZPO bisher schon erlaubt, ein zentrales Register einzuführen. Hiervon haben bislang allerdings nur wenige Bundesländer Gebrauch gemacht.[989] Aus diesem Grunde wurde mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung die Ausgestaltung des Schuldnerverzeichnisses als ein zentrales Verzeichnis zwingend vorgeschrieben.

8.1.3 Eintragungsgründe

Im Unterschied zur grundsätzlichen Struktur des Schuldnerverzeichnisses als ein zentrales Register begegnen jedoch die Eintragungsgründe an manchen Stellen Bedenken. Nach der bislang geltenden Rechtslage wird in das Schuldnerverzeichnis nach § 915 ZPO eingetragen, wer die eidesstattliche Versicherung abgegeben hat oder gegen wen die Haft angeordnet worden ist. Der Schuldner ist zur Abgabe einer eidesstattlichen Versicherung verpflichtet, wenn eine Pfändung nicht zu einer vollständigen Befriedigung des Gläubigers geführt hat,[990] der Gläubiger glaubhaft macht, dass er durch die Pfändung seine Befriedigung nicht vollständig erlangen konnte,[991] wenn der Schuldner die Durchsuchung verweigert hat[992] oder der Gerichtsvollzieher den Schuldner wiederholt in seiner Wohnung nicht angetroffen hat[993]. Die Haft wird gemäß § 901 ZPO angeordnet, wenn der Schuldner in dem Termin zur Abgabe der eidesstattlichen Versicherung nicht erscheint oder die Abgabe der eidesstattlichen Versicherung ohne Grund verweigert.

In Zukunft sind Anknüpfungspunkte für eine Eintragung nicht mehr formale Tatbestände wie die Abgabe der eidesstattlichen Versicherung oder die Anordnung der Erzwingungshaft. Vielmehr wird in Zukunft derjenige eingetragen, der seinen vollstreckungsrechtlichen Auskunftspflichten nicht nachgekommen ist oder gegen den die Vollstreckung erfolglos ist.[994] Zur Auskunft über sein Vermögen ist der Schuldner dabei gemäß § 802c ZPO neu schon vor Einleitung einer Pfändung verpflichtet. Wenn diese unergiebig ist, hat der Gläubiger darüber hinaus nach § 802l ZPO neu die Möglichkeit, seine Informationen von dritter Seite zu beziehen. Man kann sich darüber streiten, ob die Möglichkeit, Sachaufklärungsmaßnahmen vor der eigentlichen Pfändung durchzuführen, mit dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit

986 *Diederich*, 2003.
987 § 882h Abs. 1 Satz 2 ZPO neu.
988 Vgl. hierzu *Grunow/Dressel*, ZRP 1989, 325; *Stamm*, InVo 2003, 51; *Stamm*, ZRP 2003, 95; *Stamm*, KKZ 2003, 154.
989 Vgl. hierzu Abschnitt 2.3.2.1.
990 § 807 Abs. 1 Nr. 1 ZPO.
991 § 807 Abs. 1 Nr. 2 ZPO.
992 § 807 Abs. 1 Nr. 3 ZPO.
993 § 807 Abs. 1 Nr. 4 ZPO.
994 BR-Drs. 304/08, 33.

im Einklang steht.[995] Zwar stellt die Vermögensauskunft gleich zu Beginn der Zwangsvollstreckung für den Schuldner einen sehr intensiven Eingriff in sein informationelles Selbstbestimmungsrecht dar. Allerdings ist zu berücksichtigen, dass auch ein Pfändungsversuch mit einem intensiven Eingriff in die Grundrechte eines Schuldners verbunden sein kann. Hier geht es vor allem um einen Eingriff in Art. 13 GG (Unverletzlichkeit der Wohnung). Die neue Rechtslage wird dazu führen, dass sich die meisten Gläubiger zunächst über die Vermögensverhältnisse des Schuldners informieren werden, bevor sie eine Pfändung vornehmen. Für den Schuldner kann dies von Vorteil sein, da so unnötige Kosten durch einen erfolglosen Pfändungsversuch vermieden werden können und die mit dem Besuch eines Gerichtsvollziehers verbundene Prangerwirkung entfällt. Von daher ist das grundsätzliche Anliegen des Gesetzgebers als vertretbar anzusehen.

Dennoch muss man sich fragen, ob Änderungen bei den einzelnen Eintragungsgründen nicht wünschenswert gewesen wären. Dies gilt zwar nicht für § 882c Abs. 1 Nr. 1 ZPO neu und § 882c Abs. 1 Nr. 3 ZPO neu. Nr. 1 ordnet an, dass der Schuldner eingetragen wird, wenn er seiner Pflicht zur Abgabe der Vermögensauskunft nicht nachkommt. Dieser Eintragungsgrund stellt die Strafe des Schuldners dafür dar, dass er seiner Mitwirkungspflicht nicht nachgekommen ist. Wenn er im Termin zur Abgabe der Vermögensauskunft unentschuldigt gefehlt hat oder wenn er die Abgabe der Vermögensauskunft oder deren eidesstattliche Bekräftigung grundlos verweigert hat oder wenn er die Abgabe der Vermögensauskunft durch Nichtvorlage von erforderlichen Dokumenten vereitelt, ist es gerechtfertigt, ihn in das Schuldnerverzeichnis einzutragen.[996] Nach § 882c Abs. 3 Nr. 3 ZPO neu wird weiter eingetragen, wer dem Gerichtsvollzieher die Befriedigung des Gläubigers nicht binnen einer Frist von einem Monat nachweist. Die Beweislast für die Befriedigung des Gläubigers liegt damit beim Schuldner.[997] Dies ist aber auch gerechtfertigt, da die Nichtleistung des geschuldeten Betrages in seine Verantwortung fällt. Die Frist von einem Monat erscheint auch gerechtfertigt.

Anders verhält es sich jedoch bei § 882c Abs. 1 Nr. 2 ZPO neu. Danach wird eingetragen, wenn eine Vollstreckung nach dem Inhalt des Vermögensverzeichnisses aussichtslos erscheint. Hierzu muss der Inhalt des Vermögensverzeichnis ausgewertet werden und geprüft werden, ob angesichts des Wertes der angegebenen Gegenstände voraussichtlich eine vollständige Befriedigung des Gläubigers erzielt werden kann.[998] Dieser Eintragungsgrund lässt sich daher in der Regel nur schwer feststellen. Er erfordert vom Gerichtsvollzieher eine Prognose und eine wertende Entscheidung, die sich in der Regel als sehr fehleranfällig erweisen kann. Dieser Eintragungsgrund hätte daher gestrichen werden sollen. Offensichtlich hat auch der Gesetzgeber diesen Eintragungsgrund als kritisch beurteilt, wenn er in der Gesetzesbegründung schreibt, dass „im Einzelfall eine Eintragungsanordnung auf der Grundlage von Nummer 2 zu unterbleiben hat“.[999] Die Rechte des Schuldners werden dabei auch nicht dadurch gestärkt, dass

[995] Dagegen *Münzberger*, Rpfleger 1987, 269. Dafür *Gaul*, ZZP 1995, 3; *Schilken*, Rpfleger 2006, 629.
[996] BR-Drs. 304/08, 78.
[997] BR-Drs. 304/08, 80.
[998] BR-Drs. 304/08, 79.
[999] BR-Drs. 304/08, 79.

der Schuldner gegen die Eintragung gemäß § 882d Abs. 1 Satz 1 ZPO Widerspruch einlegen kann. Denn dieser hat grundsätzlich nach § 882d Abs. 1 Satz 2 ZPO keine aufschiebende Wirkung. Nur auf gesonderten Antrag des Schuldners kann das Vollstreckungsgericht gemäß § 882d Abs. 2 Satz 1 ZPO anordnen, dass die Eintragung einstweilen ausgesetzt wird.

8.1.4 Online-Auskunft aus dem Schuldnerverzeichnis

Bedenken bestehen zudem bei der Online-Auskunft. Der Gesetzgeber hat das Schuldnerverzeichnis im Jahr 1994 zum Schutz des Schuldners bewusst als beschränkt öffentliches Register ausgestaltet.[1000] Mit der künftigen Ausgestaltung des Online-Schuldnerverzeichnisses wird das Schuldnerverzeichnis jedoch faktisch zu einem unbeschränktem öffentlichen Register. Zwar sind die Voraussetzungen für eine Online-Auskunft aus dem Schuldnerverzeichnis die gleichen wie beim herkömmlichen papiergebundenen Schuldnerverzeichnis. Erforderlich ist die Darlegung für bestimmte Zwecke.[1001] Bei der Online-Auskunft wird das Vorliegen der Voraussetzungen aber nicht mehr vor der Erteilung der Auskunft geprüft. Der jeweilige Nutzer soll durch das Anklicken von bestimmten Textfeldern oder Schlüsselzahlen auf elektronischem Wege mitteilen, für welchen Zweck er Informationen benötigt. Danach werden ihm – ohne weitere Prüfung – die begehrten Informationen erteilt.[1002]

§ 882h Abs. 3 Satz 3 Nr. 4 ZPO sieht vor, dass die Daten nur von registrierten Nutzern abgerufen werden dürfen. Nach der Begründung des Bundesrats-Entwurfs soll eine Registrierung durch ein Web-Formular oder über ein zum Download bereitgestelltes Antragsformular erfolgen. Die Identifizierung soll entweder durch eine Kreditkarte erfolgen oder – subsidiär – durch die Übersendung der Authentisierungsdaten auf dem Postweg.[1003] Dies ist aber nicht ausreichend. Zwar prüft das Kreditunternehmen bei der Ausstellung der Kreditkarte die Identität des Antragstellers. Bei jedem Zahlvorgang legt der Kreditkarteninhaber seine Daten aber offen und es besteht die Gefahr, dass diese Daten von Dritten gestohlen werden. Es ist damit keineswegs sichergestellt, dass durch die Angabe von Personenangaben und Kreditkartendaten Nutzer und Kreditkarteninhaber identisch sind. Eine sichere Identifizierung ist im Übrigen auch nicht durch eine Übersendung der Authentisierungsdaten auf dem Postweg sichergestellt. Hier besteht in gleichem Maße die Gefahr, dass der Brief mit den Authentisierungsdaten abhanden kommt. Durch die beschriebenen Maßnahmen kann also später nicht rückverfolgt werden, von wem die Daten tatsächlich abgerufen wurden.[1004]

[1000] Vgl. hierzu BT-Drs. 12/193, 9: „Es besteht kein berechtigtes oder schutzwürdiges Interesse daran, uneingeschränkt alle Eintragungen eines Schuldnerverzeichnisses durchzusehen und dabei auch über die Eintragung solcher Personen Kenntnis zu erlangen, mit denen keinerlei geschäftliche Beziehungen bestehen."

[1001] Vgl. § 882f ZPO neu und § 915b ZPO.

[1002] BR-Drs. 304/08, 88.

[1003] BR-Drs. 304/08, 93.

[1004] Vgl. hierzu auch BT-Drs. 16/13432, 49.

Eine zuverlässige Identifizierung wäre lediglich mit Hilfe des elektronischen Personalausweises oder auch der Bürgerportale möglich. Auch die Begründung der Beschlussempfehlung geht hiervon aus.[1005]

Allerdings ist angesichts der Sensibilität der Daten in einem Schuldnerverzeichnis eine zuverlässige Identifizierung nicht ausreichend. Vielmehr ist es erforderlich, dass eine regelmäßige Kontrolle der Rechtmäßigkeit der Abrufe stattfindet. Dies ist aber bei der vorliegenden Ausgestaltung des Schuldnerverzeichnisses nicht gewährleistet. Zwar wird jeder Abrufvorgang protokolliert werden.[1006] Die Justiz ist jedoch ohnehin überlastet und Ziel der Online-Auskunft ist ja gerade, die Gerichte zu entlasten. Von daher ist nicht damit zu rechnen, dass die Protokolldaten in regelmäßigen Abständen überprüft werden. Im Übrigen ist auch zu berücksichtigen, dass gar nicht klar ist, wie eine Kontrolle hier stattfinden kann. Wenn der Nutzer beispielsweise angegeben hat, die Daten zu benötigen, um wirtschaftliche Nachteile zu verhindern,[1007] wird es der Justizverwaltung schwer fallen, zu kontrollieren, ob diese Voraussetzungen tatsächlich auch vorlagen. Darlegen bedeutet das widerspruchsfreie und schlüssige Vortragen.[1008] Wenn der Nutzer nicht nur mündliche Verhandlungen mit seinem potentiellen Geschäftspartner geführt hat, muss er Dokumente vorlegen, zum Beispiel Korrespondenzen, aus welchen sich vorvertragliche Beziehungen ergeben. Dies tut er bei der elektronischen Abfrage aber gerade nicht. Allein aufgrund der elektronischen Angaben dürfte also eine Kontrolle nicht möglich sein. Aufgrund der Arbeitsbelastung des Justizpersonals ist auch nicht zu erwarten, dass diese Dokumente bei einer Stichprobenkontrolle angefordert werden. Auch mit einer Kontrolle durch die Datenschutz-Aufsichtsbehörden wird nicht in großem Maße zu rechnen sein. Diese sind personell unterbesetzt. Zu Recht wurde daher schon von den Datenschutzbeauftragten anlässlich der Novellierung der §§ 915 ff. ZPO im Jahr 1994 geltend gemacht, dass nicht einmal regelmäßige Kontrollen bei den privaten Beziehern von Abdrucken möglich seien.[1009] Auch durch die Zahlung einer Gebühr können missbräuchliche Abrufe nicht verhindert werden. Zutreffend geht Straub davon aus, dass sich derjenige, der sich von einem Missbrauch von den Daten einen Vorteil verspricht, von einer Gebühr nicht abhalten lassen wird.[1010] Als präventive Maßnahme kann die Zahlung einer Gebühr nicht dazu beitragen, das informationelle Selbstbestimmungsrecht des Schuldners zu schützen.[1011] § 882h Abs. 3 Satz 3 Nr. 4 ZPO schreibt vor, dass als repressive Maßnahme Nutzer im Fall eines missbräuchlichen Datenabrufs von der Einsicht-

[1005] Vgl. hierzu auch BT-Drs. 16/13432, 49: „Kreditkarten stellen grundsätzlich kein geeignetes Mittel zur Authentifizierung von Personen dar und entsprechend nicht den an den Datenschutz zu stellenden Anforderungen. Beim Erlass der Rechtsverordnung nach § 882h Abs. 3 Satz 1 ZPO-E wird das Bundesministerium der Justiz daher auf eine ausreichende Datensicherheit achten und die Möglichkeit der Nutzung eines elektronischen Personalausweises und/oder des Bürgerportals vorsehen."

[1006] § 882h Abs. 3 Satz 3 Nr. 4 ZPO neu.

[1007] § 882f Nr. 4 ZPO neu.

[1008] BT-Drs. 12/193, 11.

[1009] *Straub*, 1995, 138.

[1010] *Straub*, 1995, 138.

[1011] So aber die Begründung der Beschlussempfehlung, BT-Drs. 16/13432, 49: „Es ist davon auszugehen, dass die Auskünfte aufgrund landesrechtlicher Vorschriften kostenpflichtig sein werden. Dies stellt eine praktische Hemmschwelle gegen Abfragen dar, denen kein wirtschaftliches Interesse zu Grunde liegt."

nahme ausgeschlossen werden können. Der Ausschluss von der Einsichtnahme stellt jedoch ebenfalls keine große Hemmschwelle gegen eine missbräuchliche Nutzung dar.

Möglicherweise halten strafrechtliche Sanktionen davon ab, die Daten missbräuchlich abzurufen. Sollte jemand unter seinem richtigen Namen einen Account beantragt haben, dann aber Daten abrufen, obwohl er keine der genannten Zwecke für sich in Anspruch nehmen kann, könnte zwar § 37 Abs. 1 Nr. 2 Var. 1 LDSG einschlägig sein.[1012] Insbesondere würde es sich bei den Daten im Schuldnerverzeichnis um nicht offenkundige Daten im Sinne des § 37 LDSG handeln.[1013] Auch wäre § 37 Abs. 1 Nr. 2 Var. 4 LDSG einschlägig, wenn sich der Täter unter falschem Namen einen Account erschleicht und damit Schuldnerdaten aus dem Verzeichnis abruft. Eine Strafbarkeit nach § 37 LDSG setzt aber immer voraus, dass der Täter in Bereicherungsabsicht, gegen Entgelt oder in Schädigungsabsicht gehandelt hat. Ruft der Täter dagegen die Daten etwa nur aus Neugier ab, so ist keine Strafbarkeit gegeben. Unabhängig davon ist der Strafrahmen des § 37 LDSG (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) äußerst gering und die Taten werden auch nur von wenigen Strafverfolgungsorganen überhaupt verfolgt.[1014] Auch eine strafrechtliche Ahndung wird daher nicht wirksam vor Missbrauchsrisiken schützen. Daher ist es erforderlich, den Kreis der zum Abruf über das Internet berechtigten Personen einzuschränken.

Lediglich einer bestimmten Personengruppe sollte es deshalb gestattet sein, Informationen aus dem Schuldnerverzeichnis ohne eine vorherige Prüfung des Einzelfalls zu beziehen. Bei dieser Personengruppe könnte dann vermutet werden, dass die Voraussetzungen für eine Einsicht in das Schuldnerverzeichnis vorliegen. Zu diesen könnten etwa der Gerichtsvollzieher und die Bediensteten der Vollstreckungsgerichte, die mit der Führung des Schuldnerverzeichnisses betraut sind, zählen. Zudem kämen öffentliche Stellen wie etwa Sozialleistungsträger,[1015] Staatsanwaltschaften oder die Polizei[1016] in Betracht. Bei den privaten Stellen ließe sich an den Personenkreis anknüpfen, der bislang zum Bezug von Abdrucken berechtigt ist. Das sind zum einen die Kammern, also die Industrie- und Handelskammern und die berufsständischen Selbstverwaltungskörperschaften.[1017] Zum anderen könnten dazu diejenigen Stellen gehören, die die Informationen aus dem Schuldnerverzeichnis zur Errichtung und Führung nicht-öffentlicher zentraler Schuldnerverzeichnisse verwenden[1018] und Antragsteller, deren berechtigtes Interesse durch Einzelauskünfte nicht hinreichend Rechnung getragen werden kann.[1019] Die Einsicht dieser Stellen könnte dabei durch ein automatisiertes Abrufverfahren ermöglicht werden.

Den anderen Personen hätte zwar ebenfalls eine Auskunft auf elektronischen Wege gestattet werden können. Hier hätte jedoch eine vorherige Einzelfallprüfung erfolgen sollen. Dabei

[1012] § 44 BDSG scheidet als Sanktionsnorm aus, da das Schuldnerverzeichnis von den Ländern geführt wird. Vgl. hierzu *Hartig/Klink/Eiermann*, LDSG, Erl. 1.1 zu § 37.
[1013] Vgl. hierzu *Meyer/Brocks/Nordmann*, RDV 2000, 11.
[1014] *Hartig/Klink/Eiermann*, LDSG, Erl. 1.2 zu § 37.
[1015] Vgl. § 882f Nr. 3 ZPO neu.
[1016] Vgl. § 882f Nr. 5 ZPO neu.
[1017] Vgl. § 915e Abs. 1a ZPO.
[1018] Vgl. § 915e Abs. 1b ZPO.
[1019] Vgl. § 915e Abs. 1c ZPO.

hätte der entsprechende Antrag zum Beispiel per E-Mail an das zentrale Vollstreckungsgericht übermittelt werden können. In diesem hätte dann dargelegt werden können, aus welchen Gründen Informationen aus dem Schuldnerverzeichnis benötigt werden. Der zuständige Mitarbeiter hätte sodann nach einer zuverlässigen Identifizierung prüfen können, ob die Voraussetzungen vorliegen. Falls dies der Fall gewesen wäre, hätte er diese Daten dann verschlüsselt und mit einer qualifizieren elektronischen Signatur an den Antragsteller übermitteln können.

Es ist nicht zu erwarten, dass der Gesetzgeber vor Inkrafttreten der eigentlichen Regelungen zum Schuldnerverzeichnis noch Änderungen seines bereits beschlossenen Gesetzes vornehmen wird. Von daher wird das Schuldnerverzeichnis – wie es § 882f ZPO neu vorsieht – jedermann offen stehen. Umso wichtiger wird es dann jedoch sein, dass in der noch zu errichtenden Rechtsverordnung zumindest strenge Vorgaben im Hinblick auf eine zuverlässige Registrierung, eine Protokollierung sowie die Festsetzung einer hohen Gebühr zum Abruf festgeschrieben werden.

8.1.5 Erteilung von Abdrucken

Nicht nur bei den Eintragungsgründen und der Online-Einsicht wären Änderungen des Gesetzgebers wünschenswert gewesen. Auch die Regelungen zur Abschriftenerteilung hätten anders ausgestaltet werden sollen. In dem künftigen § 882g ZPO neu hat der Gesetzgeber die bisherigen Regelungen der §§ 915d-g ZPO beibehalten und in einer Vorschrift zusammengefasst.[1020] Die Vorschriften zur Abschriftenerteilung hätten jedoch nicht beibehalten werden sollen. Der Gesetzgeber hat sich in § 882g ZPO neu dazu entschlossen, das Schuldnerverzeichnis für jedermann über das Internet durch eine zentrale länderübergreifende Abfrage einsehbar zu machen. Die §§ 915d-g ZPO haben zum Ziel, die Eintragungen im Schuldnerverzeichnis dem überregionalen Geschäftsverkehr zugänglich zu machen.[1021] Wenn zum 1.1.2013 die Regelungen zum Internet-Schuldnerverzeichnis in Kraft treten, besteht hierfür jedoch keine Notwendigkeit mehr. Der überregionale Geschäftsverkehr kann die Schuldnerdaten über das Internet durch eine zentrale und länderübergreifende Abfrage von da an direkt einsehen. Der Gesetzgeber hat die Weitergeltung der Vorschriften zur Abschriftenerteilung damit begründet, dass sich Kammern und andere Nutzer auf die Überlassung aufbereiteter Daten eingerichtet haben.[1022] Dabei ist jedoch zu berücksichtigen, dass die Regelungen zum neuen Schuldnerverzeichnis

[1020] Lediglich an zwei Stellen hat der Gesetzgeber kleine Änderungen vorgenommen. Einmal wurde in Abs. 4 im Interesse der Rechtseinheitlichkeit die Berechtigung zum Abruf aus Abdrucken des Schuldnerverzeichnisses abweichend von § 915e Abs. 2 ZPO an die gleichen Voraussetzungen geknüpft, die sich aus § 10 BDSG ergeben (BT-Drs. 16/10069, 42). Zum anderen wurde in Abs. 7 Satz 1 abweichend vom bisherigen § 915e Abs. 4 Satz 1 ZPO darauf verzichtet, die Aufsichtsbehörde nach § 38 BDSG zu ermächtigen, auch dann zu kontrollieren, wenn ihr keine hinreichenden Anhaltspunkte für eine Verletzung von Datenschutzvorschriften vorliegen. Diese Regelung ist überflüssig geworden, weil die Aufsichtsbehörde nach § 38 BDSG in seiner seit dem Jahr 2001 geltenden Fassung anlassfrei kontrollieren kann (BT-Drs. 16/10069, 42).

[1021] *Liebscher*, 1994, 156.

[1022] BR-Drs. 304/08, 89. Mittelfristig werde allerdings zu prüfen sein, inwieweit für die Erteilung von Abschriften noch ein Bedürfnis besteht. Vgl. hierzu BR-Drs. 304/08, 89.

erst zum 1.1.2013 in Kraft treten. Einer Übergangsphase für die Abschriftenbezieher hätte es daher nicht bedurft. Sie hätten noch lange genug Zeit gehabt, sich auf eine neue Situation einzustellen.

Die Regelungen zur Erteilung von Abschriften in den §§ 915d-g ZPO sind nach ihrer geltenden Rechtslage überdies auch als kritisch zu beurteilen. So leuchtete es bislang schon nicht ein, warum sich die Gläubiger nicht direkt beim Vollstreckungsgericht die erforderliche Auskunft beschaffen können. Zum Teil wurde geltend gemacht, dass die Abschriftenerteilung die Vollstreckungsgerichte entlasten solle.[1023] Dieses Argument ist jedoch nicht geeignet, eine solch breitgefächerte Verteilung von Informationen zu rechtfertigen. Zu Recht wurde daher geltend gemacht, dass die hohe Arbeitsbelastung nicht durch eine Abschriftenerteilung, sondern durch eine personelle Verstärkung der Dienststellen auszugleichen ist.[1024] In Zukunft macht die Abschriftenerteilung überhaupt keinen Sinn mehr. Einer Erteilung von Abdrucken bedarf es nicht mehr, wenn die Daten für jedermann im Internet abrufbar sind. Insofern hätten die Regelungen in §§ 915d-g ZPO nicht in das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aufgenommen werden sollen.

8.1.6 Löschung

Im Unterschied zu den Eintragungsgründen, der Online-Auskunft und den Vorschriften zur Abschriftenerteilung sind die Vorgaben zur Löschung nicht zu beanstanden. Im Gegenteil: Der künftige Beginn der Löschungsfrist ist sogar als positiv hervorzuheben. Nach § 882e Abs. 1 ZPO neu wird die Eintragung in Zukunft nach Ablauf von drei Jahren gelöscht. Die Frist beginnt mit dem Tag der Eintragungsanordnung.[1025] Auch nach dem bislang geltenden § 915a Abs. 1 ZPO wird die Eintragung nach drei Jahren gelöscht. Fristbeginn bei § 915a Abs. 1 ZPO ist im Unterschied zu § 882e Abs. 1 ZPO neu jedoch nicht der Tag der Eintragungsanordnung, sondern das Ende des Jahres, indem die eidesstattliche Versicherung abgegeben, die Haft angeordnet oder die sechsmonatige Haftvollstreckung beendet worden ist. Die jetzige Rechtslage hat zur Folge, dass der Schuldner noch im Schuldnerverzeichnis eingetragen sein kann, obwohl er möglicherweise schon vor mehr als drei Jahren seine eidesstattliche Versicherung abgegeben hat.[1026]

Den Fristbeginn zum Jahresende nach § 915a Abs. 1 ZPO hat der Gesetzgeber so gewählt, weil so die Löschung der Daten aus dem papiergebundenen Verzeichnis vereinfacht werden konnte. Um den Schuldner vor einer Auskunft über veraltete Daten zu schützen,[1027] musste der Gesetzgeber mit § 915b Abs. 2 ZPO eine datenschutzrechtliche Sonderregelung schaffen,

[1023] Vgl. hierzu *Straub*, 1995, 97 m.w.N.

[1024] *Straub*, 1995, 98.

[1025] Die Sperrfrist des § 802d Abs. 1 Satz 1 ZPO neu und die Frist zur Speicherung des Vermögensverzeichnisses betragen dagegen zwei Jahre.

[1026] § 903 ZPO.

[1027] Zum Schutz des Schuldners vor Auskunft über veraltete Eintragungen nach Abs. 2 vgl. *Stein/Jonas*, ZPO, § 915b Rn. 5.

welche die Löschung nach Ablauf von drei Jahren seit der Eintragung an fingiert hatte. D.h.: Wenn etwa die Eintragung am 5.5.2001 erfolgte, kann Auskunft nur bis zum 5.5.2004 gewährt werden; obwohl die Löschung erst zum 31.12.2004 erfolgte. In Zukunft wird das Verzeichnis elektronisch geführt werden. Der Gesetzgeber geht davon aus, dass die Daten deshalb einfacher als bislang gelöscht werden können.[1028] Dementsprechend hat er auf eine datenschutzrechtliche Sonderregelung zur Auskunfterteilung verzichtet und den Fristbeginn an den Tag der Eintragungsanordnung selbst angeknüpft und die Eintragungsfrist damit insgesamt verkürzt. In diesem Zusammenhang stellt die Elektronisierung des Schuldnerverzeichnisses aus datenschutzrechtlicher Sicht also einen Gewinn dar.

8.1.7 Auskunft des Schuldners

Mit der Reform der Sachaufklärung in der Zwangsvollstreckung hat der Gesetzgeber die Auskunft des Schuldners über ihn selbst betreffende Daten zufriedenstellend gelöst. Bislang ist das Auskunftsrecht des Schuldners nicht spezialgesetzlich in den §§ 915 ff. ZPO geregelt. Es ist jedoch anerkannt, dass dem Schuldner dessen ungeachtet nach den allgemeinen Datenschutzgesetzen ein Auskunftsanspruch zusteht.[1029] Nunmehr bestimmt § 882f Satz 1 Nr. 6 ZPO neu, dass die Einsicht in das Schuldnerverzeichnis jedem gestattet ist, der darlegt, Angaben nach § 882b zur Auskunft über ihn selbst betreffende Eintragungen zu benötigen. Mit der neuen Regelung hat der Gesetzgeber in den Vorschriften zum Schuldnerverzeichnis also einen spezialgesetzlichen Auskunftsanspruch normiert, was grundsätzlich als positiv zu beurteilen ist. Bezüglich der Auskunft des Schuldners darüber, ob und wann Daten an Dritte übermittelt wurden, verbleibt es mangels einer Spezialregelung dagegen bei dem allgemeinen Auskunftsanspruch in § 18 Abs. 3 Satz 1 Nr. 2 LDSG. Diesen Anspruch kann das zentrale Vollstreckungsgericht in Zukunft auf der Grundlage der nach § 882h Abs. 3 Satz 3 Nr. 4 ZPO neu zu erhebenden Protokolldaten erfüllen.

8.1.8 Datenverarbeitung im Auftrag

Die Auftragsdatenverarbeitung kann von Vorteil sein, da sie zu Kosteneinsparungen führen kann und der Auftragnehmer in der Regel über Spezialwissen im IT-Bereich verfügt. Mit der Auftragsdatenverarbeitung sind jedoch auch Risiken verbunden. So treten zusätzliche Akteure auf, die das Missbrauchspotential erhöhen. Zudem wird die Datenschutzkontrolle durch die Auslagerung kompliziert und verschlechtert und schutzwürdige personenbezogene Daten werden Serviceunternehmen bekannt.[1030]

Aus diesem Grund hat der Gesetzgeber an manchen Stellen bereichsspezifische Vorschriften geschaffen, die Beschränkungen bei der Auftragsdatenverarbeitung vorsehen.[1031] § 126 Abs. 3

[1028] BT-Drs. 16/10069, 40.
[1029] *Zöller*, ZPO, § 915b Rn. 7.
[1030] *LfD Niedersachsen*, 2002, 3.
[1031] Vgl. hierzu *Hartig/Klink/Eiermann*, LDSG, Erl. 9 zu § 4.

GBO bestimmt zum Beispiel, dass das zuständige Grundbuchamt die Datenverarbeitung im Auftrag nur auf den Anlagen einer anderen staatlichen Stelle oder auf den Anlagen einer juristischen Person des öffentlichen Rechts vornehmen kann, wenn die ordnungsgemäße Erledigung der Grundbuchsachen sichergestellt ist.

§ 882h Abs. 2 Satz 2 ZPO neu in Verbindung mit § 802k Abs. 3 Satz 3 ZPO neu, enthält – im Unterschied zu dem genannten Beispiel – keine derartigen Beschränkungen. Der Gesetzgeber hat dies damit begründet, dass die Kammern nach § 915e Abs. 3 ZPO auch bislang schon private Dritte mit der Zusammenfassung der Abdrucke beauftragen können. Zudem würden die Landesdatenschutzgesetze für die Beauftragung öffentlicher und nicht-öffentlicher Stellen umfangreiche Kontrollpflichten des Auftraggebers vorsehen.[1032]

Richtigerweise hätte der Gesetzgeber die Datenverarbeitung im Auftrag aber auf öffentliche Stellen beschränken sollen. Die personenbezogenen Daten im Schuldnerverzeichnis sind nicht weniger sensibel als die, die in einem Grundbuch enthalten sind.[1033] Zwar ist es zutreffend, dass die Kammern bislang schon nach § 915e Abs. 3 ZPO die Datenverarbeitung an private Dritte zur Erstellung von Listen „outsourcen“ können. Unabhängig von der Frage, ob die Entscheidung des Gesetzgebers damals zutreffend war, ist aber zu berücksichtigen, dass es sich bei der Führung und Verwaltung des Schuldnerverzeichnisses – im Unterschied zur Listenerstellung durch die Kammern – um eine hoheitliche Aufgabe handelt. Das LDSG von Rheinland-Pfalz sieht – ebenso wie die Datenschutzgesetze anderer Länder – zwar bestimmte Pflichten des Auftraggebers bei der Auswahl und der Kontrolle seines Auftragnehmers vor.[1034] Dennoch gibt es bestimmte Bereiche, die Privaten grundsätzlich nicht anvertraut werden sollten. Dies ergibt sich auch aus § 4 Abs. 4 Satz 2 LDSG. Nach dieser Vorschrift soll ein Auftrag an nicht-öffentliche Stellen nur vergeben werden, wenn überwiegende schutzwürdige Interessen, insbesondere Berufs- oder besondere Amtsgeheimnisse, nicht entgegenstehen. Zu diesen Bereichen gehören auch hoheitliche Tätigkeiten.[1035] Da die Kammern die Schuldnerdaten bislang dezentral bei den einzelnen Amtsgerichten beziehen müssen, ist zudem die Anzahl der Daten, die das zentrale Vollstreckungsgericht an Private outsourcen würde, um Unterschied zu den Daten, die die Kammern an Private outsourcen, im Zweifel viel größer. Eine Beschränkung der Datenverarbeitung im Auftrag auf öffentliche Stellen wäre daher erforderlich gewesen.

8.2 E-Vermögensverzeichnis

Auch die Auskunft von Daten aus einem elektronischen Vermögensverzeichnis geht mit einem Eingriff in das informationelle Selbstbestimmungsrecht nach Art. 1 i.V.m. Art. 2 GG einher. Da die Daten in einem elektronischen Vermögensverzeichnis bei einem Gericht[1036] und da-

[1032] BT-Drs. 16/10069, 31.
[1033] Zu den personenbezogenen Daten im Grundbuch vgl. Abschnitt 10.1.
[1034] Vgl. hierzu § 4 LDSG.
[1035] Vgl. hierzu *Hartig/Klink/Eiermann*, LDSG, Erl. 9 zu § 4.
[1036] Zentrales Vollstreckungsgericht, vgl. § 802k Abs. 1 ZPO neu.

mit einem Organ der Rechtspflege nach § 2 Abs. 1 Nr. 2 LDSG[1037] geführt werden und es sich dabei um personenbezogene Daten nach § 3 LDSG handelt, wäre eigentlich der Anwendungsbereich des LDSG eröffnet. Wie bei den Vorschriften zum Schuldnerverzeichnis, gehen jedoch auch die Bestimmungen des elektronischen Vermögensverzeichnisses den allgemeinen Datenschutzgesetzen vor.

Bei dem in einem elektronischen Vermögensverzeichnis gespeicherten personenbezogenen Daten handelt es sich nach § 802c Abs. 1 ZPO neu – im Interesse der eindeutigen Zuordnung der Vermögensangaben[1038] – zunächst um den Geburtsnamen, das Geburtsdatum und den Geburtsort des Schuldners. Die weiteren Angaben entsprechen im Wesentlichen der bislang noch geltenden Vorschrift des § 807 Abs. 1 und 2 ZPO zum papiergebundenen Vermögensverzeichnis. Wie das papiergebundene Vermögensverzeichnis wird auch das elektronische Vermögensverzeichnis nach § 802c Abs. 2 Satz 1 ZPO neu Angaben über die Vermögensgegenstände, die dem Schuldner gehören, enthalten. Hierunter fallen die einzelnen beweglichen Vermögenswerte, also etwa körperliche Sachen oder Forderungen und sämtliches unbewegliches Vermögen.[1039] § 802c Abs. 2 Satz 2 ZPO neu bestimmt, dass bei Forderungen auch der Grund des Anspruchs und die Beweismittel anzugeben sind. Um dem Gläubiger eine Pfändung der Forderungen zu ermöglichen, hat der Schuldner zudem den Drittschuldner mit Namen und Anschrift des Arbeitgebers oder der kontoführenden Bank und andere zur Identifikation erforderliche Daten anzugeben.[1040] Überdies schreiben § 802c Abs. 2 Satz 3 Nr. 1 und 2 ZPO neu vor, dass bestimmte entgeltliche[1041] und bestimmte unentgeltliche Veräußerungen des Schuldners an eine nahe stehende Person[1042] in das Verzeichnis eingetragen werden müssen.[1043]

Im Unterschied zum Schuldnerverzeichnis, das nur Angaben dazu enthält, ob die eidesstattliche Versicherung abgegeben oder die Haft angeordnet wurde[1044] und statt dessen in Zukunft, ob der Schuldner seinen vollstreckungsrechtlichen Auskunftspflichten nachgekommen ist oder ob gegen ihn die Vollstreckung erfolglos geblieben ist,[1045] sind im Vermögensverzeichnis also konkrete Angaben zu den Vermögensverhältnissen enthalten.

[1037] Vgl. hierzu *Hartig/Klink/Eiermann*, LDSG, Erl. 1.2 zu § 2.

[1038] BR-Drs. 304, 45.

[1039] BR-Drs. 304, 46.

[1040] BR-Drs. 304, 46.

[1041] Vgl. § 138 InsO.

[1042] Entgeltliche Veräußerungen an nahe stehende Personen sind nach § 802c Abs. 2 Satz 3 Nr. 1 anzugeben, wenn der Schuldner diese in den letzten zwei Jahren vor dem Termin nach § 802f Abs. 1 und bis zur Abgabe der Vermögensauskunft vorgenommen hat. Unentgeltliche Leistungen sind nach § 802c Abs. 2 Satz 3 Nr. 2 ZPO anzugeben, wenn der Schuldner diese in den letzten vier Jahren vor dem Termin nach § 802f Abs. 1 und bis zur Abgabe der Vermögensauskunft vorgenommen hat, sofern sie sich nicht auf gebräuchliche Gelegenheitsgeschenke geringen Wertes richteten.

[1043] Sachen, die der Pfändung nach § 811 Abs. 1 Nr. 1 und 2 ZPO offensichtlich nicht unterworfen sind, brauchen nach § 802c Abs. 2 Satz 4 ZPO nicht angegeben zu werden, es sei denn, dass eine Austauschpfändung nicht in Betracht kommt.

[1044] Vgl. § 915 Abs. 1 ZPO.

[1045] Vgl. im Einzelnen §§ 882b, c ZPO neu.

Das elektronische Vermögensverzeichnis wird errichtet, indem der Gerichtsvollzieher die mündlichen Erklärungen des Schuldners im Termin zur Abgabe der eidesstattlichen Versicherung[1046] in ein elektronisches Dokument überträgt.[1047] Vom Schuldner beigebrachte Anlagen können in ein elektronisches Dokument übertragen und in das Vermögensverzeichnis aufgenommen oder mit diesem untrennbar verbunden werden. Das Erfordernis einer Unterschrift des Schuldners unter das Vermögensverzeichnis entfällt.[1048] Die Einzelheiten der Form des Vermögensverzeichnisses einschließlich der Behandlung von Anlagen kann der Verordnungsgeber nach § 802k Abs. 4 ZPO festlegen. Nach § 802f Abs. 5 Satz 3 ZPO neu ist dem Schuldner auf Verlangen ein Ausdruck des Vermögensverzeichnisses zu erteilen. Er soll dem Schuldner die Feststellung ermöglichen, welche Daten bei dem zentralen Vollstreckungsgericht hinterlegt werden.[1049]

Der Gerichtsvollzieher hat das Vermögensverzeichnis nach § 802f Abs. 6 ZPO neu bei einem zentralen Vollstreckungsgericht zu hinterlegen. Das zentrale Vermögensverzeichnis wird gemäß § 802k Abs. 1 ZPO neu in Zukunft landesweit in elektronischer Form verwaltet. In dieses können Gerichtsvollzieher und bestimmte Vollstreckungsbehörden zu Vollstreckungszwecken Einsicht nehmen. Ansonsten sind Vollstreckungsgerichte, Insolvenzgerichte und Registergerichte sowie Strafverfolgungsbehörden im Rahmen ihrer Aufgabenwahrnehmung befugt, Einsicht zu nehmen. § 802k Abs. 3 ZPO ermächtigt die Landesregierungen durch Rechtsverordnung zu bestimmen, welches Gericht genau die Aufgaben des zentralen Vollstreckungsgerichts wahrzunehmen hat. Des Weiteren ist in § 802k Abs. 3 ZPO bestimmt, dass das zentrale Vollstreckungsgericht andere Stellen mit der Wahrnehmung der Datenverarbeitung beauftragen kann, wenn eine ordnungsgemäße Bearbeitung sichergestellt ist. § 802k Abs. 4 ZPO enthält eine Ermächtigung zum Erlass einer Rechtsverordnung. In dieser sollen gemäß § 802k Abs. 4 Satz 1 ZPO Form, Aufnahme, Übermittlung, Verwaltung und Löschung der Vermögensverhältnisse näher bestimmt werden. Außerdem sollen in der Rechtsverordnung nach § 802k Abs. 4 Satz 1 letzter Hs. ZPO die Einzelheiten der Einsichtnahme, insbesondere durch ein automatisiertes Verfahren geregelt werden. Schließlich sollen geeignete Regelungen zur Sicherung des Datenschutzes und der Datensicherheit nach § 802k Abs. 4 Satz 2 ZPO vorgesehen werden. § 802k Abs. 1 Satz 3 ZPO neu sieht vor, dass das Vermögensverzeichnis nach Ablauf von zwei Jahren seit der Abgabe der Auskunft oder bei Eingang eines neuen Vermögensverzeichnisses zu löschen ist.

8.2.1 Verfassungsmäßigkeit

Wie beim elektronischen Schuldnerverzeichnis stellt sich auch bei dem elektronischen Vermögensverzeichnis zunächst die Frage, ob dessen Führung mit der Verfassung, hier dem infor-

[1046] Zum Verfahren der eidesstattlichen Versicherung vgl. § 802f ZPO neu.

[1047] BR-Drs. 304/08, 51.

[1048] BR-Drs. 304/08, 51. Die Strafbarkeit der falschen eidesstattlichen Versicherung der Vollständigkeit und Richtigkeit der Auskunftserteilung an Eides Statt bleibt davon unberührt; auch eine mündlich abgegebene eidesstattliche Versicherung ist strafbar.

[1049] BR-Drs. 304, 52.

mationellen Selbstbestimmungsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, in Einklang steht. Dass das Vermögensverzeichnis einem legitimen Zweck dient, steht dabei jedoch außer Zweifel. Im Unterschied zum Schuldnerverzeichnis enthält nur das Vermögensverzeichnis konkrete Angaben zu den Vermögensverhältnissen des Schuldners. Diese Angaben benötigt der Gläubiger, um die Zwangsvollstreckung gegen den Schuldner erfolgreich betreiben zu können. So kann der Gläubiger durch die Einsicht in das Vermögensverzeichnis erkennen, welche weiteren Möglichkeiten einer Zwangsvollstreckung bestehen und ob etwaiges zugrifffreies Schuldnervermögen vorhanden ist.[1050] Den damit verbundenen Eingriff in das informationelle Selbstbestimmungsrecht muss der Schuldner hinnehmen, da er trotz des Vorliegens der allgemeinen Zwangsvollstreckungsvoraussetzungen den Gläubiger nicht befriedigt hat. Ein gleich geeignetes, aber weniger einschneidendes Mittel, dem Gläubiger die entsprechenden Informationen zukommen zu lassen, ist nicht ersichtlich. Bislang wird das elektronische Vermögensverzeichnis bei den einzelnen Amtsgerichten papiergebunden geführt. Künftig wird das Verzeichnis in den Ländern elektronisch bei einer Stelle geführt, was mit einem tieferen Grundrechtseingriff einhergeht. Dies belastet jedoch den Schuldner nicht unverhältnismäßig. So haben private Stellen keinen Zugriff auf das zentrale Vermögensverzeichnis. Der Zugriff ist vielmehr Gerichtsvollziehern, Vollstreckungsgerichten und bestimmten anderen Stellen in der Justiz vorbehalten.[1051] Damit diese Stellen die Daten nicht missbräuchlich abrufen können, hat der Gesetzgeber verschiedene Schutzmaßnahmen für den Datenschutz und die Datensicherheit vorgesehen. So hat er in § 802k Abs. 4 Satz 3 Nr. 1-4 ZPO neu bestimmt, dass die noch zu erlassende Rechtsverordnung insbesondere Vorgaben enthalten sollen, die sicherstellen, dass die Übermittlung von Daten an das zentrale Vollstreckungsgericht sowie bei der Weitergabe an die anderen Stellen gegen unbefugte Kenntnisnahme geschützt sind (Nr. 1), unversehrt und vollständig wiedergegeben werden (Nr. 2), jederzeit ihrem Ursprung nach zugeordnet werden können (Nr. 3) und nur von registrierten Nutzern abgerufen werden können und jeder Abrufvorgang protokolliert wird (Nr. 4). Alles in allem kann daher die künftige Ausgestaltung des elektronischen Vermögensverzeichnis als verfassungsgemäß angesehen werden. Genauso wie beim Schuldnerverzeichnis wären jedoch auch beim elektronischen Vermögensverzeichnis an manchen Stellen Änderungen wünschenswert gewesen, die nachfolgend diskutiert werden.

8.2.2 Zentrale Struktur

Wie beim elektronischen Schuldnerverzeichnis betreffen diese jedoch nicht die grundsätzliche Ausrichtung des elektronischen Vermögensverzeichnisses als zentrale Datei. Das Gesetzgeber wollte, dass das Vermögensverzeichnis im Interesse der Effektivität der Zwangsvollstreckung und der Aufwandsminimierung landesweit in elektronischer Form bei einem zentralen Vollstreckungsgericht verwaltet wird.[1052] Er hat damit das Ziel verfolgt, das Zwangsvollstreckungs-

[1050] *Liebscher*, 1994, 192.

[1051] Zur Frage der Verfassungsmäßigkeit des elektronischen Vermögensverzeichnisses vgl. auch BT-Drs. 16/13432, 48.

[1052] BR-Drs. 304, 57.

verfahren zu beschleunigen und kostengünstiger zu machen. Zentrale Strukturen sind aus datenschutzrechtlicher Sicht zwar grundsätzlich als kritisch zu beurteilen, da in ihnen eine Vielzahl von personenbezogenen Daten gespeichert werden, was vor allem das Risiko von zukünftigen Zweckänderungen mit sich bringt.[1053] Dass sich zentrale Strukturen in erster Linie negativ auf den Datenschutz auswirken, trifft jedoch in dieser grundsätzlichen Aussage nicht für das zentrale Vermögensverzeichnis zu. Mit dem künftigen elektronischen Vermögensverzeichnis kann der Gerichtsvollzieher bei Eingang eines Auftrages effizienter prüfen, ob der Schuldner bereits innerhalb der letzten zwei Jahre eine Vermögensauskunft abgegeben hat oder nicht.[1054] Dies entlastet auch den Schuldner,[1055] da so verhindert wird, dass der Schuldner das Vermögensverzeichnis mehrmals abgeben muss. Das zentrale Vermögensverzeichnis dient damit sowohl dem Schutz des Schuldners als auch der Entlastung der Justiz.

8.2.3 Online-Einsicht in das zentrale Vermögensverzeichnis

Auch gegen die Online-Einsicht bestehen keine Bedenken. Sie ist auf öffentliche Stellen begrenzt. Nach § 802k Abs. 2 Satz 1 ZPO neu können Gerichtsvollzieher und die in § 802k Abs. 2 Satz 2 ZPO neu bestimmten Vollstreckungsbehörden die Daten zu Vollstreckungszwecken zur Einsichtnahme abrufen. Dies ist sachgerecht. Denn dieser Personenkreis benötigt die Daten insbesondere deswegen, um bei Eingang des Auftrages auf Abgabe der Vermögensauskunft überprüfen zu können, ob der Schuldner bereits innerhalb der letzten zwei Jahre eine Vermögensauskunft[1056] abgegeben hat.[1057]

Die anderen in § 802k Abs. 2 Satz 3 ZPO neu genannten Stellen dürfen die Daten aus dem Vermögensverzeichnis abrufen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Auch diese Regelung ist nicht zu beanstanden. Durch das Merkmal der Erforderlichkeit wird dem datenschutzrechtlichen Interesse einer möglichst begrenzten Datenübermittlung Rechnung getragen.[1058] Satz 3 begründet auch keine neuen Einsichtsrechte, sondern führt lediglich die bestehenden Einsichtsrechte in einer Vorschrift zusammen.[1059] Bei den in Satz 3 genannten Vollstreckungsgerichten, die bislang schon unmittelbaren Zugriff auf die Daten in einem Vermögensverzeichnis hatten, kann die Erforderlichkeit zum Beispiel bejaht werden, wenn sie in Rechtsbehelfsverfahren das Verfahren zur Abnahme der Vermögensauskunft nach §§ 802c, 802d, 802f ZPO neu zu überprüfen haben.[1060] Die weiter in Satz 3 genannten Insolvenzgerichte, die auch bislang schon auf die Daten aus dem Vermögensverzeichnis zugegriffen haben, haben

[1053] Vgl. hierzu auch *BfDI*, 20. Tätigkeitsbericht, Tz. 7.1.4.: „Zum einen soll eine zentrale Datei eingerichtet werden, in der alle Vermögensauskünfte gespeichert werden. Zwar soll der Zugriff auf diese Vermögensauskunftsdatei nur Gerichtsvollziehern vorbehalten bleiben. Eine derartige Datei birgt aber das Risiko zukünftiger Zweckänderungen."

[1054] BT-Drs. 16/13432, 48.

[1055] BT-Drs. 16/13432, 48.

[1056] § 802d ZPO neu.

[1057] Vgl. hierzu im Einzelnen die zutreffende Gesetzesbegründung, BT-Drs. 16/10069, 29.

[1058] BT-Drs. 16/10069, 30.

[1059] BT-Drs. 16/10069, 30.

[1060] Vgl. hierzu im Einzelnen die zutreffende Gesetzesbegründung, BT-Drs. 16/10069, 30.

bei der Entscheidung über die Eröffnung des Insolvenzverfahrens die Vermögensverhältnisse des Schuldners festzustellen. Wenn dieser nicht nach § 20 InsO sein Vermögensverzeichnis vorlegt, sind die Insolvenzgerichte auf die Daten aus dem Vermögensverzeichnis angewiesen.[1061] Die Einsichtsmöglichkeit der ebenfalls in Satz 3 aufgeführten Registergerichte rechtfertigt sich aus dem Umstand, dass diese die Löschung von vermögenslosen Gesellschaften nach § 394 FamFG vorzunehmen haben. Hierfür ist die Kenntnis der Daten aus dem Vermögensverzeichnis erforderlich. Zu diesem Zweck haben sie bislang schon nach den Vorgaben der MiZi[1062] Abschriften der Vermögensverzeichnisse von Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung übersandt.[1063] Letztlich benötigen auch die in Satz 3 genannten Staatsanwaltschaften die Daten aus dem Vermögensverzeichnis, nämlich dann, wenn es etwa um Betrugs- und Insolvenzverfahren, Geldwäschedelikte, falscher Versicherung an Eides statt oder um die Verletzung der Unterhaltspflicht geht. Auch die Staatsanwaltschaften fordern derzeit schon Abschriften der Vermögensverzeichnisse von den Vollstreckungsgerichten an und erhalten Mitteilungen über die Abgabe der eidesstattlichen Versicherung von Handelsgesellschaften.[1064]

Vor diesem Hintergrund ist die Entscheidung des Gesetzgebers, den genannten öffentlichen Stellen eine Online-Einsicht einzurichten, durchaus nachvollziehbar. Um Missbräuche zu vermeiden, wäre es jedoch erforderlich, dass die Zahl der registrierten Nutzer nach § 802k Abs. 4 Satz 3 Nr. 4 ZPO neu bei den einzelnen öffentlichen Stellen überschaubar bleibt und die zum Abruf berechtigten Personen eine Kennung und ein Passwort erhalten. Außerdem ist es notwendig, dass im Rahmen der Protokollierung nach § 802k Abs. 4 Satz 3 Nr. 4 ZPO neu nicht nur festgestellt werden kann, welche Behörde die Abfrage getätigt hat. Es sollte vielmehr auch eine Protokollierung des Abrufs der einzelnen Mitarbeiter möglich sein. Entsprechendes sollte in der noch zu erlassenden Rechtsverordnung bestimmt werden.

8.2.4 Elektronische Zuleitung an Gläubiger

Wie oben gesehen, ist der Zugriff auf das elektronische Vermögensverzeichnis öffentlichen Stellen vorbehalten. Dessen ungeachtet benötigen jedoch auch private Stellen, insbesondere Gläubiger, die Daten aus dem Vermögensverzeichnis, um Art und Ausmaß der Vollstreckung zu bestimmen. Die diesbezüglich getroffenen Regelungen sind nicht zu beanstanden. Bislang bestimmt § 900 Abs. 5 ZPO, dass Gläubigern, die das Verfahren zur Abgabe der eidesstattlichen Versicherung als Partei betreiben, eine Abschrift des Vermögensverzeichnisses zuzuleiten ist. Außerdem haben sie die Möglichkeit, das Vermögensverzeichnis (nochmals) auf der Grundlage des § 299 Abs. 1 ZPO einzusehen.[1065] In Zukunft wird ihnen das Vermögensverzeichnis nach § 802f Abs. 6 ZPO neu vom Gerichtsvollzieher nach der Abnahme der Vermögensauskunft

[1061] BT-Drs. 16/10069, 30.
[1062] Unterabschnitt X/3 MiZi, § 15 Nr. 1 EGGVG.
[1063] BT-Drs. 16/10069, 30.
[1064] BT-Drs. 16/10069, 30.
[1065] *Liebscher*, 1994, 193.

unverzüglich zugeleitet. Der Gläubiger erhält einen Ausdruck und dieser muss den Vermerk enthalten, dass er mit dem Inhalt des Vermögensverzeichnisses übereinstimmt. Anstelle der Zuleitung eines Ausdrucks kann dem Gläubiger gemäß § 802f Abs. 6 Satz 2 i.V.m. § 802d Abs. 2 ZPO auf Antrag auch das Vermögensverzeichnis als elektronisches Dokument übermittelt werden, wenn dieses mit einer qualifizierten elektronischen Signatur versehen und gegen unbefugte Kenntnisnahme geschützt ist. Diese Vorschriften führen vor dem Hintergrund der dargestellten bisherigen Rechtslage zu keiner Verschlechterung des Datenschutzes. Im Gegenteil: In § 802f Abs. 6 Satz 2 i.V.m. § 802d Abs. 1 Satz 3 ZPO neu hat der Gesetzgeber sogar bestimmt, dass der Gläubiger die erlangten Daten nur zu Vollstreckungszwecken nutzen darf und sie nach Zweckerreichung zu löschen hat; hierauf hat ihn der Gerichtsvollzieher hinzuweisen. Diese Regelung entspricht § 16 Abs. 4 LDSG. Ihre Verankerung in der ZPO ist als positiv zu bewerten.

Auch die Vorgaben für die Kenntnisnahme der hier in Rede stehenden Daten durch andere Gläubiger begegnen keinen Bedenken. Zwar bezieht sich § 900 Abs. 5 ZPO nur auf Gläubiger, die das Verfahren zur Abgabe der eidesstattlichen Versicherung betreiben. Dessen ungeachtet haben diese richtigerweise bislang nach § 299 Abs. 1 ZPO schon einen Anspruch auf Akteneinsicht in das Vermögensverzeichnis. Zwar betreiben sie das Verfahren zur Abnahme der eidesstattlichen Versicherung nicht. Dennoch sind sie einer Partei im Sinne des § 299 Abs. 1 ZPO gleichzustellen, da die Vorschrift des § 903 ZPO ihnen gegenüber eine gesetzliche Sperrwirkung entfaltet. Die Norm wirkt für sie so, als hätten sie das Verfahren als Partei selbst betrieben.[1066] Vor diesem Hintergrund ist es daher gerechtfertigt, auch ihnen, wie es § 802d Abs. 1 Satz 2 und § 802d Abs. 2 ZPO neu vorsehen, einen Abdruck aus dem elektronischen Vermögensverzeichnis zukommen zu lassen. Mit § 802d Abs. 1 Satz 3 ZPO (Zweckbindung beim Gläubiger) und § 802d Abs. 1 Satz 4 ZPO (Benachrichtigung des Schuldners) hat der Gesetzgeber dem Datenschutz in ausreichender Weise Rechnung getragen.

8.2.5 Löschung

Die Vorgaben zur Löschung sind teilweise bedenklich. § 802k Abs. 1 Satz 3 ZPO neu bestimmt nunmehr zukünftig, dass ein Vermögensverzeichnis entsprechend der zweijährigen Sperrwirkung des § 802d Abs. 1 Satz 1 ZPO neu nach Ablauf von zwei Jahren seit der Abgabe der Auskunft oder bei Eingang eines neuen Vermögensverzeichnisses zu löschen ist. Die Löschung hat von Amts wegen zu erfolgen.[1067] Hieran ist zu kritisieren, dass eine Befriedigung des Schuldners nicht zu einer vorzeitigen Löschung im Vermögensverzeichnis führen kann. Der Gesetzgeber hat dies damit begründet, dass eine weitere Aufbewahrung dem Schutz des Schuldners vor einer erneuten Abgabe einer Vermögensauskunft und aus Gründen der Entlastung der Justiz nicht möglich sei.[1068] Letzteres Argument trägt jedoch schon angesichts des in § 13 Abs. 1 Nr. 1 LDSG allgemein zum Ausdruck kommenden Grundsatzes, dass eine Spei-

[1066] *Schmidt-Jortzig*, JurBüro 1970, 445; LG Konstanz, JurBüro 1984, 1587; KG Berlin, NJW 1989, 534.
[1067] BT-Drs. 16/10069, 29.
[1068] BT-Drs. 16/10069, 29.

cherung von personenbezogenen Daten bei einer öffentlichen Stelle nur solange möglich ist, wie sie zur rechtmäßigen Aufgabenerfüllung benötigt werden, nicht.[1069] Und zum Schutz des Schuldners vor einer erneuten Abgabe der eidesstattlichen Versicherung benötigt man nicht den Inhalt des Vermögensverzeichnisses. Es wäre hier ausreichend, zu dokumentieren, wann ein Vermögensverzeichnis abgegeben wurde. Vor diesem Hintergrund hätte der Gesetzgeber in § 802k Abs. 1 Satz 3 ZPO neu bestimmen sollen, dass eine Befriedigung des Gläubigers zu einer vorzeitigen Löschung führt. Zumindest aber wäre es erforderlich gewesen, vorzusehen, dass die Daten von Dritten nicht mehr abgerufen werden können und nach § 19 Abs. 3 LDSG gesperrt werden, wenn der Schuldner den Gläubiger befriedigt hat.

8.2.6 Auskunft des Schuldners

Was die Auskunft des Schuldners hinsichtlich über ihn selbst gespeicherte Daten im Vermögensverzeichnis angeht, hat der Gesetzgeber von einem derartigen Anspruch bewusst abgesehen. Von daher ist ein Rückgriff auf den allgemeinen datenschutzrechtlichen Auskunftsanspruch nach § 18 Abs. 3 Satz 1 Nr. 1 LDSG nicht möglich. Der Gesetzgeber hat seine Entscheidung damit begründet, dass der Schuldner gemäß § 802f Abs. 5 Satz 3 ZPO neu schon eine Abschrift seines Vermögensverzeichnisses erhalte. Somit könne er wissen, welche Daten das zentrale Vollstreckungsgericht über ihn speichert. Eines Auskunftsanspruches bedürfe es daher nicht mehr.[1070] Dies ist jedoch unzutreffend. Nach § 802k Abs. 1 Satz 3 ZPO neu ist ein Vermögensverzeichnis nach Ablauf von zwei Jahren seit Abgabe der Auskunft oder bei Eingang eines neuen Verzeichnisses zu löschen. Um zu prüfen, ob die Daten nach dieser Zeit auch gelöscht werden, bedarf es eines derartigen Auskunftsanspruches. Es wäre deshalb sachgerecht gewesen, wenn der Gesetzgeber entsprechend den Vorgaben zum Schuldnerverzeichnis nach § 882f Satz 1 Nr. 6 ZPO neu ebenfalls einen Auskunftsanspruch des Schuldners über ihn selbst betreffende Daten vorgesehen hätte. Zumindest hätte er jedoch einen Rückgriff auf den allgemeinen datenschutzrechtlichen Auskunftsanspruch durch seine Gesetzesbegründung[1071] nicht verschließen dürfen.

Wie gesehen,[1072] dürfen bestimmte Behörden die Daten aus dem Vermögensverzeichnis abrufen. Der Schuldner muss daher auch erfahren können, ob und falls ja, an welche Behörden seine Daten weitergegeben wurden. Bezüglich dieses Auskunftsanspruches kann auf § 18 Abs. 3 Satz 1 Nr. 2 LDSG zurückgegriffen werden. Diesen Anspruch kann das zentrale Vollstreckungsgericht in Zukunft auf der Grundlage der nach § 802k Abs. 4 Satz 3 Nr. 4 ZPO neu zu erhebenden Protokolldaten erfüllen.

[1069] Vgl. hierzu *Hartig/Klink/Eiermann*, LDSG, Erl. 2.1 zu § 13.
[1070] BT-Drs. 16/10069, 27.
[1071] BT-Drs. 16/10069, 27.
[1072] Vgl. hierzu Abschnitt 8.2.3.

8.2.7 Datenverarbeitung im Auftrag

Auch die Vorgaben zur Datenverarbeitung im Auftrag sind bedenklich. So wie beim elektronischen Schuldnerverzeichnis hat der Gesetzgeber auch beim elektronischen Vermögensverzeichnis in § 802k Abs. 3 Satz 3 ZPO neu keine Beschränkungen der Datenverarbeitung im Auftrag auf öffentliche Stellen vorgenommen. Aufgrund der Verweisung in § 882h Abs. 2 Satz 2 ZPO neu[1073] hat der Gesetzgeber eine einheitliche Übertragung des IT-Betriebs für das Schuldnerverzeichnis und für das Vermögensverzeichnis ermöglicht.[1074] Im elektronischen Vermögensverzeichnis sind konkrete Angaben zu den Vermögensverhältnissen des Schuldners enthalten, z.B. einzelne Forderungen und sämtliches unbewegliches Vermögen. Im Vergleich zum Schuldnerverzeichnis, aus welchem nur hervorgeht, ob und seit wann ein Schuldner eingetragen ist, ist die Schutzbedürftigkeit der im elektronischen Vermögensverzeichnis gespeicherten Daten höher zu bewerten. Eine Beschränkung der Auftragsdatenverarbeitung auf öffentliche Stellen wäre daher hier erst recht sachgerecht gewesen.

Der Gesetzgeber hat dies jedoch nicht so gesehen. Er hat die im elektronischen Vermögensverzeichnis enthaltenen Angaben mit den Daten verglichen, die bei einem Sozialleistungsträger gespeichert sind. Er hat die Schutzbedürftigkeit der im Vermögensverzeichnis gespeicherten Daten nicht so hoch bewertet wie die bei einem Sozialleistungsträger und daher eine Beschränkung, wie sie in § 80 Abs. 5 SGB X[1075] enthalten ist, abgelehnt. In seiner Begründung hat er ausgeführt: „Ein Aufgreifen der engeren Vorgaben für die Beauftragung nichtöffentlicher Stellen in § 80 Abs. 5 SGB X ist dagegen nicht veranlasst. Die besonderen Beschränkungen des § 80 Abs. 5 SGB X erklären sich aus dem erhöhten Schutzbedürfnis bei Sozialdaten. Da beim zentralen Vollstreckungsgericht nach § 802k Abs. 1 ZPO neu aber nicht die Ergebnisse der Fremdauskünfte nach § 802l Abs. 1 Satz 1 Nr. 1 ZPO-E, sondern nur die im Rahmen der Selbstauskunft des Schuldners errichteten Vermögenswerte gespeichert werden, besteht kein vergleichbares Schutzbedürfnis.“[1076] Zwar ist die Auffassung des Gesetzgebers zutreffend, dass bei den Sozialdaten und den Daten in einem elektronischen Vermögensverzeichnis nicht unbedingt das gleiche Schutzniveau gegeben ist. Der Gesetzgeber hat jedoch an mehreren Beispielen gezeigt, dass nicht nur bei Sozialdaten eine Beschränkung der Auftragsdatenverarbeitung sachgerecht ist, sondern auch bei anderen Daten. Oben[1077] wurde bereits auf die Vorschrift des § 126 Abs. 3 GBO eingegangen. Nach dieser kann die Datenverarbeitung im Auftrag des zuständigen Grundbuchamts auf den Anlagen einer anderen staatlichen Stelle oder auf den Anlagen einer juristischen Person des öffentlichen Rechts vorgenommen werden, wenn die ordnungsgemäße Erledigung der Grundbuchsachen sichergestellt ist. Im Meldegesetz ist in

[1073] Siehe Abschnitt 8.1.8.

[1074] So auch BT-Drs. 16/10069, 31.

[1075] Nach dieser Vorschrift ist die Beauftragung Privater nur zulässig, wenn beim Auftragnehmer sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Aufgaben beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst.

[1076] BT-Drs. 16/10069, 31.

[1077] Vgl. hierzu Abschnitt 8.1.8.

§ 37 Abs. 5 ausdrücklich vorgesehen, dass die Rechtsträger der Meldebehörden Dritte nur zur Erfüllung einzelner behördlicher Aufgaben beauftragen können. § 90a Landesbeamtengesetz (LBG) ermöglicht die Beauftragung von privaten Dritten nur im Rahmen einer Beleihung.[1078] Im Vergleich zu diesen Daten sind die Daten in einem elektronischen Vermögensverzeichnis schutzwürdiger. Vor diesem Hintergrund wäre daher eine Beschränkung sachgerecht gewesen.

8.3 E-Antragstellung für Pfändungs- und Überweisungsbeschluss

Mit dem Justizkommunikationsgesetz vom 22.3.2005[1079] wurde mit § 829 Abs. 4 ZPO die Möglichkeit geschaffen, Formulare für einen Antrag auf Erlass eines Pfändungs- und Überweisungsbeschlusses einzuführen, die elektronisch bearbeitet werden können.[1080] Der Gesetzgeber verfolgte damit das Ziel, die übermittelten Daten aufgrund einer einheitlich definierten Schnittstelle zu übernehmen und elektronisch weiterzubearbeiten.[1081] Später erkannte der Gesetzgeber, dass der mit dieser Möglichkeit verbundene Ressourcengewinn in der Praxis nicht ausgeschöpft werden kann, da dem Antrag die vollstreckbare Ausfertigung des Titels und gegebenenfalls weitere Urkunden beigefügt werden müssen, die in der Regel nur in Papierform vorliegen.[1082] Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung[1083] sollte der Medienbruch vermieden werden. Es sollte eine Vereinfachung und Beschleunigung des Zwangsvollstreckungsverfahrens erreicht werden, soweit die Pfändung von Geldforderungen auf der Grundlage von Vollstreckungsbescheiden betroffen ist.[1084] Um in Zukunft eine vollautomatische Auftragserteilung auch in praktischer Hinsicht zu erreichen,[1085] bestimmt der künftig geltende § 829a ZPO neu, dass bei einem Vollstreckungsbescheid, der keiner Vollstreckungsklausel bedarf,[1086] eine Ausfertigung entbehrlich ist, wenn die von ihm in § 829a Abs. 1 Satz 1 Nr. 1 bis 4 genannten Voraussetzungen vorliegen. Dies sind: Die Forderung aus dem Vollstreckungsbescheid darf nicht mehr als 5.000 EUR betragen (Nr. 1), wobei zu berücksichtigen ist, dass die Kosten der Zwangsvollstreckung und Nebenforderungen bei der Berechnung der Höhe der Forderung nur zu berücksichtigen sind, wenn sie allein Gegenstand des Vollstreckungsauftrages sind, die Vorlage anderer Urkunden als der Ausfertigung des Vollstreckungsbescheides darf nicht vorgeschrieben sein (Nr. 2), der Gläubiger muss eine Ausfertigung oder Abschrift des Vollstreckungsbescheides neben einer Zustellungsbescheinigung als elektronisches Dokument dem Auftrag beifügen (Nr. 3) und der Gläubiger muss versichern, dass eine Ausfertigung des Vollstreckungsbescheides und eine Zustellungsbescheinigung vor-

[1078] *Hartig/Klink/Eiermann*, LDSG, Erl. 9.5 zu § 4.
[1079] BGBl. 2005 I, 841.
[1080] Soweit Formulare eingeführt sind, muss sich der Antragsteller ihrer nach § 829 Abs. 4 Satz 2 ZPO bedienen.
[1081] BT-Drs. 15/4067, 36.
[1082] BT-Drs. 16/10069, 34.
[1083] BGBl. 2009 I, 2258.
[1084] BT-Drs. 16/10069, 34.
[1085] BT-Drs. 16/10069, 34.
[1086] Vgl. hierzu § 796 ZPO.

liegen und die Forderung in Höhe des Vollstreckungsauftrages noch besteht (Nr. 4). Wenn das Gericht an dem Vorliegen der Voraussetzungen Zweifel hat, so bestimmt § 829a Abs. 2 ZPO, dass es dies dem Gläubiger mitzuteilen hat und der Gläubiger die entsprechenden Bescheinigungen in Papierform dem Gericht vorzulegen hat.[1087]

8.3.1 Einscannen der vollstreckbaren Ausfertigung

Die Änderungen, die § 829a ZPO neu durch das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung erfahren hat, sind nicht datenschutzkonform und sicher. Sie sind mit erheblichen Missbrauchsrisiken verbunden. § 829a Abs. 1 Satz 1 Nr. 3 ZPO neu sieht vor, dass der Gläubiger die vollstreckbare Ausfertigung des Vollstreckungsbescheides einscannen kann. Dabei ist es leicht möglich, Änderungen am Originaldokument vorzunehmen. Dem eingescannten Dokument können diese Änderungen nicht entnommen werden. So ist es beispielsweise möglich, dass das Original des Titels derart geändert wird, als dass es dort heißt, dass ein Betrag von 5.000 EUR statt 3.000 EUR geschuldet wird. Auch kann es sein, dass der Gläubiger sich eine Kopie des Vollstreckungsbescheides in elektronischer Form macht und dann aber im Zeitpunkt des Vollstreckungsauftrages gar nicht im Besitz des Original-Vollstreckungsbescheides ist, weil dieser z.B. bei einem anderen Gerichtsvollzieher für dort laufende Vollstreckungsmaßnahmen vorliegt.[1088] Daneben sind noch weitere Missbrauchsrisiken möglich: So kann es etwa sein, dass der Gläubiger und ursprüngliche Titelinhaber seine Forderung an einen Dritten abgetreten hat. Der Gläubiger kann sich nun vor Übergabe des Titels eine Kopie machen und somit mit Hilfe von Vollstreckungsorganen versuchen, eine ihm nicht mehr gehörende Forderung zwangsweise durchzusetzen. Zwar braucht der Schuldner nach § 407 BGB nicht mehr an den neuen Gläubiger zu leisten. Dennoch ist die Situation für den neuen Gläubiger misslich: Für ihn besteht die Gefahr, dass er seinen Regressanspruch gegen den alten Gläubiger nicht mehr durchsetzen kann.[1089] Offenbar war es auch dem Gesetzgeber bei der Zulassung des vereinfachten Vollstreckungsauftrages unwohl. Ansonsten hätte er die Erteilung eines vereinfachten Vollstreckungsauftrages nicht an bestimmte Voraussetzungen geknüpft und auch nicht bestimmt, dass das Gericht bei Zweifeln weitere Prüfungen vorzunehmen hat. Vor diesem Hintergrund hätte auf diese Form der Antragstellung ganz verzichtet werden sollen.[1090]

[1087] Diese Regelung dient der weiteren Sicherung des Schuldners vor ungerechtfertigter Vollstreckung. Vgl. hierzu BT-Drs. 16/10069, 37.

[1088] Vgl. *Bundesrechtsanwaltskammer*, 2009, 4. Hier ändert sich im Übrigen nichts dadurch, dass der Gesetzgeber in § 829a Abs. 1 Satz 1 Nr. 4 das Wort „in“ eingefügt hat. So aber wohl BT-Drs. 16/13432, 53.

[1089] *Bundesrechtsanwaltskammer*, 2009, 5.

[1090] Zu diesem Ergebnis kommt auch *Bundesrechtsanwaltskammer*, 2009, 5.

8.3.2 Beseitigung des Medienbruchs

Der Gesetzgeber muss sich langfristig fragen, wie er den Medienbruch im Bereich des Zwangsvollstreckungsrechts beseitigen kann. Das Erkenntnisverfahren kann nach den Vorschriften der ZPO sowohl elektronisch als auch papiergebunden geführt werden. Da für das Zwangsvollstreckungsverfahren – mit Ausnahme der nicht als Vorbild dienenden Vorschrift des § 829a ZPO – eine Papierausfertigung erforderlich ist, muss im Fall der Durchführung eines elektronischen Zivilprozesses ein Medientransfer nach § 317 Abs. 3 ZPO erfolgen. § 317 Abs. 3 ZPO bestimmt diesbezüglich, dass Ausfertigungen von einem Urteilsausdruck nach § 298 ZPO erteilt werden können. Der Urteilsausdruck muss in diesem Fall den Vermerk enthalten, welches Ergebnis die Integritätsprüfung des Dokuments ausweist, wen die Signaturprüfung als Inhaber der Signatur ausweist und welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist.[1091] Dies erweist sich als zeitaufwändig und umständlich. Insofern ist zu prüfen, ob es Möglichkeiten gibt, ein elektronisches Zwangsvollstreckungsverfahren sicher und datenschutzkonform zu gestalten.

Einmal wird vorgeschlagen, dass im Zuge der künftigen Einführung eines elektronischen Titels von dem in § 733 ZPO normierten Grundsatz der Einmaligkeit des Titels abgewichen werden sollte.[1092] Gleichzeitig müsse in diesem Zusammenhang auch in § 757 ZPO das Erfordernis der Quittierung der Zahlungen auf dem Titel und dessen Aushändigung bei vollständiger Zahlung an den Schuldner aufgegeben werden. Um die Gefahr einer Doppelvollstreckung zu vermeiden, sei es insoweit ausreichend, dass dem Schuldner für geleistete Zahlungen eine Quittung durch den Gerichtsvollzieher erteilt werde, ohne dass zusätzlich die vollstreckbare Ausfertigung des Titels ausgehändigt werden müsse. Der Schuldner könne durch die erteilte Quittung erforderlichenfalls nachweisen, dass der Gläubiger wegen der titulierten Forderung ganz oder teilweise befriedigt ist und bei unberechtigten weiteren Vollstreckungsmaßnahmen Rechtsmittel einlegen.[1093]

Es ist jedoch nicht ausreichend, dem Schuldner eine Quittung zu erteilen. Die Zwangsvollstreckung ist ein staatliches Verfahren zur Durchsetzung einer privaten, zuvor im Erkenntnisverfahren erstrittenen Forderung. Aufgrund der Konzeption als staatliches Verfahren mit Zwangsbefugnissen obliegt es dem Vollstreckungsorgan, vor Beginn der Vollstreckungsmaßnahmen umfassend zu prüfen, ob die Voraussetzungen der Zwangsvollstreckung vorliegen. Dies beinhaltet auch die Prüfung, ob zuvor schon vollstreckt wurde. Im papiergebundenen Verfahren kann die Prüfung durch die körperliche Vorlage einer vollstreckbaren Ausfertigung des Titels erfolgen. Im elektronischen Zwangsvollstreckungsverfahren muss nach einem Äquivalent gesucht werden.

[1091] Vgl. hierzu *Schmieszek*, in: *Scherf/Schmieszek/Viefhues* (Hrsg.), Elektronischer Rechtsverkehr, 46; *Fischer-Dieskau*, MMR 2003, 701; *Krüger*, ZVI 2004, 162; *Viefhues*, CR 2003, 541.

[1092] *Krüger/Bütter*, MDR 2003, 181.

[1093] *Krüger/Bütter*, MDR 2003, 181.

Sicher und datenschutzkonform wäre es, wenn man ein Verfahren ähnlich dem von elektronischen Münzen wählen würde.[1094] Will der Gläubiger die Zwangsvollstreckung betreiben, dann stellt das Gericht – sofern erforderlich – keine vollstreckbare Ausfertigung mehr in Papierform her. Vielmehr signiert es den elektronischen Titel digital, gibt diesem eine eindeutige Seriennummer wie z.B. RP.AGKL.123-0 und übermittelt dem Gläubiger diesen Datensatz elektronisch. Der Gläubiger stellt nun beim Vollstreckungsorgan einen Antrag auf Zwangsvollstreckung. Diesem Antrag schickt der Gläubiger nicht mehr eine vollstreckbare Ausfertigung in Papierform, sondern er überliefert nur den Datensatz an das Vollstreckungsorgan mit einem Zustellungsnachweis. Das Vollstreckungsorgan nimmt vor Beginn der Zwangsvollstreckung eine Signaturprüfung vor, um sicherzustellen, dass das Dokument vom Gericht stammt. Zudem holt es eine Online-Auskunft beim Gericht ein, um sicherzustellen, dass noch nicht vollstreckt worden ist. Nach dieser Prüfung und der Prüfung des Zustellungsnachweises leitet das Vollstreckungsorgan die Zwangsvollstreckung ein. Kann der Schuldner nur teilweise erfüllen, teilt das Vollstreckungsorgan die teilweise Erfüllung dem Gericht mit. Dieses stellt daraufhin eine neue Seriennummer aus wie z.B. RP.AGKL.123-I und übermittelt diesen Datensatz wiederum dem Vollstreckungsorgan und auch dem Gläubiger. Die alte Seriennummer wird gespeichert, so dass diese nicht mehr verwendet werden kann. Zugleich erteilt es dem Schuldner eine Quittung über den bereits bezahlten Betrag. Wird der Gläubiger vollständig befriedigt, teilt das Vollstreckungsorgan dies dem Gericht mit. Das Gericht speichert wiederum die Seriennummer und übermittelt dem Schuldner eine Quittung über den nun vollständig gezahlten Betrag. Bei dieser Konstellation wird somit auf eine papiergebundene vollstreckbare Ausfertigung verzichtet. Die bisherige Unterscheidung von Titeln mit und ohne vollstreckbaren Ausfertigung fällt weg. Alle vom Gericht ausgestellten Titel bekommen eine nur einmal zu vergebende Seriennummer. Damit entfällt die Gefahr von Doppelvollstreckungen.

8.4 E-Akteneinsicht

§ 760 ZPO stellt das Gegenstück zu dem im Erkenntnisverfahren geltenden § 299 ZPO dar.[1095] Nach § 760 Satz 1 ZPO hat jeder Beteiligte einen Anspruch auf Einsicht in die Handakten des Gerichtsvollziehers.[1096] Zu diesen gehört der ganze Urkundsstoff mit Belegen einschließlich der Protokolle des Gerichtsvollziehers und der Dienstregister, soweit er die Zwangsvollstreckung betrifft.[1097] Beteiligter ist jeder, den eine Vollstreckungsmaßnahme irgendwie betrifft. Hierzu gehören in erster Linie die Parteien und deren Rechtsnachfolger. Daneben können aber etwa auch der Drittschuldner nach § 840 ZPO oder solche Personen, die nach § 805 ZPO zu ei-

[1094] Vgl. hierzu grundsätzlich *Breitscheid* et al., 2004; *Breitscheid* et al., 2006; *Kristoferitsch*, 1998.

[1095] *Baumbach* et al., ZPO, § 760, Rn. 1.

[1096] Nach *Baumbach* et al., ZPO, § 760, Rn. 2 stellt das Akteneinsichtsrecht nach § 760 ZPO eine Rechtmäßigkeitskontrolle dar. So diene § 760 ZPO wesentlich der Stärkung des Vertrauens auf die Korrektheit des staatlichen Vollstreckungsorgans in einem Verfahrensabschnitt, der anders als das Erkenntnisverfahren nicht der Kontrolle der Öffentlichkeit in Gestalt von Zuschauern unterliegen kann.

[1097] *Baumbach* et al., ZPO, § 299, Rn. 5.

ner vorzugsweisen Befriedigung berechtigt sind, Beteiligte im Sinne dieser Vorschrift sein.[1098] Das Akteneinsichtsrecht von Dritten bestimmt sich dagegen nach § 299 Abs. 2 ZPO. Über die Gewährung der Akteneinsicht entscheidet der Gerichtsvollzieher. Die Akten sind grundsätzlich in den Räumlichkeiten des Gerichtsvollziehers einzusehen. Der Beteiligte hat keinen Anspruch darauf, dass die Akten ihm zugesendet werden. Bezüglich des Vorrangs vor den Datenschutzgesetzen kann auf die Ausführungen zu § 299 ZPO verwiesen werden.[1099]

§ 760 Satz 2 ZPO regelt, wie § 299 Abs. 3 ZPO, Art und Weise der Akteneinsicht, wenn die Akten elektronisch geführt werden. Wie bei § 299 Abs. 3 ZPO ist hier eine Einsichtnahme durch Erteilung von Ausdrucken, durch Übermittlung von elektronischen Dokumenten oder durch Wiedergabe auf einem Bildschirm möglich. Im Unterschied zu § 299 Abs. 3 ZPO ist jedoch keine Akteneinsicht durch einen Online-Abruf möglich. Bezüglich der Einsichtnahme durch Erteilung eines Ausdrucks, durch Übermittlung von elektronischen Dokumenten und durch Wiedergabe auf einem Bildschirm kann auf das zurückgegriffen werden, was oben gesagt wurde. Sie bedürfen hier keiner gesonderten Erörterung.

8.5 E-Bekanntmachungen nach dem ZVG

Damit möglichst viele Interessenten für ein Zwangsversteigerungsverfahren gewonnen werden, bedarf es der Veröffentlichung von Terminen über Zwangsversteigerungen. Nach § 39 Abs. 1 ZVG muss die Terminsbestimmung im Zwangsversteigerungsverfahren durch einmalige Einrückung in das für Bekanntmachungen des Gerichts bestimmte Blatt oder in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem öffentlich bekannt gemacht werden. § 39 Abs. 1 ZVG sieht die Veröffentlichung im Amtsblatt oder Internet alternativ vor, nicht kumulativ. Die Veröffentlichung im Amtsblatt ist neben der Internetveröffentlichung (ebenso umgekehrt) nicht notwendig, als zusätzliche Bekanntmachung aber zulässig.[1100] Das Informations- und Kommunikationssystem und die Art der Veröffentlichung werden landesrechtlich bestimmt. Hierfür genügt eine allgemeine Verwaltungsverfügung.[1101] Ohne eine landesrechtliche Ermächtigung kann das Vollstreckungsgericht diese Bestimmung also nicht selbst treffen.[1102] Die Terminsbestimmung muss die Angaben nach § 37 ZVG enthalten. Hierzu gehören die Bezeichnung des Grundstücks, Zeit und Ort des Versteigerungstermins, die Angabe, dass die Versteigerung im Wege der Zwangsversteigerung erfolgt und die Aufforderung, Rechte, die zur Zeit der Eintragung des Versteigerungsvermerks aus dem Grundbuch nicht ersichtlich sind oder die einer Versteigerung entgegenstehen, anzumelden. Des Weiteren soll die Terminsbestimmung nach § 38 ZVG die Angabe des Grundbuchblatts, der Größe und des Verkehrswertes des Grundstücks enthalten sowie nach Satz 2 zusätzliche Angaben

[1098] *Baumbach* et al., ZPO, § 760 Rn. 2.
[1099] Auch § 760 ZPO war im Rahmen des § 45 BDSG a.F., der die Subsidiarität ausdrücklich anordnete, beispielhaft als vorrangige Norm genannt, vgl. hierzu *Liebscher*, 1994, 187.
[1100] Vgl. hierzu *Stöber*, ZVG, § 39 Rn. 2.4.
[1101] BGH, NJW 2008, 3708.
[1102] *Stöber*, ZVG, § 39 Rn. 2.3.

über frühere Grundstücksversteigerungen. Dieser Soll-Inhalt gehört zum Inhalt der Terminsbestimmung und ist daher zu veröffentlichen.[1103] § 38 Abs. 2 ZVG gestattet des Weiteren dem Gericht fakultativ, Wertgutachten und Abschätzungen in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem zu veröffentlichen.[1104]

Für geringwertige Grundstücke kann das Gericht nach § 39 Abs. 2 ZVG anordnen, dass die Amtsblatt- und die Internetveröffentlichung unterbleibt. In diesem Fall muss es dafür die Terminsbestimmung an der für amtliche Bekanntmachungen bestimmten Stelle, der Gemeindetafel, anheften lassen. Bei einer Veröffentlichung im Amtsblatt soll die Terminsbestimmung gemäß § 40 Abs. 1 Satz 1 ZVG an die Gerichtstafel angehängt werden. Bei einer Veröffentlichung in einem gerichtlichen Informations- und Kommunikationssystem kann die Anheftung an die Gerichtstafel dagegen nach § 40 Abs. 1 Satz 2 ZVG unterbleiben. Darüber hinaus kann das Gericht nach § 40 Abs. 2 ZVG noch „andere oder wiederholte“ Veröffentlichungen zulassen, wobei insbesondere auf den Ortsgebrauch Rücksicht zu nehmen ist. Möglich sind zum Beispiel Veröffentlichungen in örtlichen Tageszeitungen oder je nach der Eigenart des Objekts als landwirtschaftliches, gewerbliches oder zur Vermietung bestimmtes Haus in einer Fachverbandszeitschrift.[1105] Mit anderer Veröffentlichung ermöglicht § 40 Abs. 2 – ohne landesrechtliche Ermächtigung – bei Terminsbestimmungen im Amtsblatt auch die Terminsbestimmung im Internet.[1106]

8.5.1 Veröffentlichung von Terminsbestimmungen

Mit Hilfe der Angabe des Grundbuchblatts, der Größe und des Verkehrswertes des Grundstücks lässt sich ermitteln, wer Eigentümer des Grundstücks ist. Zwar haben Bietinteressenten nach zutreffender Auffassung kein berechtigtes Interesse an einer Grundbucheinsicht nach § 12 GBO.[1107] Gemäß § 42 ZVG kann jedoch jeder Einsicht in die Mitteilungen des Grundbuchsamtes, die erfolgten Anmeldungen und die eingeholten Gutachten nehmen. Hierzu muss er kein rechtliches Interesse geltend machen und zumindest aus diesen Unterlagen[1108] lassen sich die Namen der Eigentümer entnehmen.[1109] Bei den Angaben der Terminsbestimmung handelt es sich daher um personenbezogene Daten nach § 3 LDSG. Deren Veröffentlichung geht mit einem Eingriff in das informationelle Selbstbestimmungsrecht einher. § 39 ZVG stellt hierfür jedoch eine verfassungskonforme Rechtsgrundlage dar. Die Terminsveröffentlichung im

[1103] *Stöber*, ZVG, § 39 Rn. 2.5.
[1104] Eingefügt durch das 2. JustizModG (BGBl. 2006, I 3416), siehe Kapitel 2.
[1105] *Stöber*, ZVG, § 40 Rn. 3.2.
[1106] *Stöber*, ZVG, § 40 Rn. 3.2.
[1107] Vgl. hierzu *Liebscher*, 1994, 206.
[1108] Zu weiteren einfachen Möglichkeiten nach der derzeitigen Ausgestaltung der Plattform vgl. den folgenden Abschnitt und Abbildung 4.
[1109] Andere Nachweise und Unterlagen in den Vollstreckungsakten dürfen nicht eingesehen werden. Hierzu gehören etwa Vollstreckungstitel, Erbscheine, Abtretungsurkunden, Vollmachten, Zustellungsnachweise, Vollstreckungsschutzanträge, Verzeichnisse über Zubehör und Urkunden über eine Sicherheitsleistung. Siehe hierzu *Hintzen/Engels/Rellermeyer*, ZVG, § 42 Rn. 2.

Amtsblatt oder im Internet hat den Zweck, im Interesse einer bestmöglichen Verwertung des Grundstücks eine möglichst breite Öffentlichkeit über den Versteigerungstermin zu unterrichten und alle, deren Rechte von der Versteigerung berührt werden, zur Wahrung dieser Rechte zu veranlassen.[1110] Dass das Objekt bestmöglich verwertet wird, ist vor allem im Interesse des Schuldners. Gerade deshalb gestattet das ZVG dem Schuldner auch, selbst den Zwangsversteigerungstermin zu veröffentlichen. Für Dritte, deren Recht im Grundbuch nach § 37 Nr. 4 ZVG nicht vermerkt oder deren Recht später als der Versteigerungsvermerk eingetragen wurde, ist es wichtig, dass sie Kenntnis von der Versteigerung erlangen. Wenn sie ihr Recht nicht spätestens im Versteigerungstermin vor der Aufforderung zur Abgabe von Geboten anmelden und glaubhaft machen, wird – wenn der Gläubiger dem Antragsteller widerspricht – ihr Recht im geringsten Gebot nicht berücksichtigt und bei der Verteilung des Versteigerungserlöses dem Anspruch des Gläubigers und der übrigen Rechte nachgesetzt.[1111] Im Vergleich zu früher hat die Vorschrift des § 38 ZVG eine deutliche Verbesserung aus datenschutzrechtlicher Sicht erfahren: Während früher in § 38 ZVG noch bestimmt war, dass die Terminsbestimmung im Regelfall die Angabe des Namens des Grundstückseigentümers enthalten soll, wurde dieser Halbsatz durch das 1. Justizmodernisierungsgesetz[1112] aus datenschutzrechtlichen Gründen – wie es in der Gesetzesbegründung heißt[1113] – ersatzlos gestrichen.[1114] Zwar stellt die fakultativ mögliche Internetveröffentlichung im Vergleich zu einer Veröffentlichung im Amtsblatt einen intensiveren Grundrechtseingriff dar. Der Gesetzgeber hatte für die Zulassung dieses Mediums jedoch einen Grund, den es zu akzeptieren gilt: Er wollte den Zugang zu den Veröffentlichungen der Gerichte benutzerfreundlicher und kostengünstiger gestalten,[1115] den Personalaufwand bei der Aufbereitung der Veröffentlichungen für die verschiedenen Medien reduzieren und die Arbeitsabläufe vereinfachen und beschleunigen.

Obwohl von der Verfassungsmäßigkeit der Norm ausgegangen werden kann, stellt sich gleichwohl die Frage, wie man bei der Auslegung von bestimmten Vorschriften dem informationellen Selbstbestimmungsrecht Rechnung tragen kann. Hier ist zunächst festzustellen, dass die Gerichte bei der Wahl ihres Veröffentlichungsmediums das informationelle Selbstbestimmungsrecht des Schuldners berücksichtigen sollten. So bietet sich eine Internetveröffentlichung zum Beispiel an, wenn es um die Versteigerung eines gewerblichen Grundstücks geht, dagegen ist bei der Versteigerung eines Einfamilienhauses in einer kleinen Ortschaft eher zurückhaltender von diesem Medium Gebrauch zu machen. Nach § 40 Abs. 2 ZVG ist das Gericht befugt, noch andere oder wiederholte Veröffentlichungen zuzulassen. Auch hier sollte das informationelle Selbstbestimmungsrecht sorgfältig mit den Zielen, die mit einer Veröffentlichung einhergehen, abgewogen werden. Nur wenn Aussicht besteht, dass das Grundstück bei einer wiederholten Veröffentlichung tatsächlich besser verwertet werden kann, sollte eine wiederholte Veröffentlichung erfolgen. Nach § 36 Abs. 2 ZVG soll der Zeitraum zwischen der Anberaumung

[1110] *Stöber*, ZVG, § 39 Rn. 2.
[1111] Zu den Rechtsfolgen bei einem der Versteigerung entgegenstehenden Recht vgl. § 37 Nr. 5 ZVG.
[1112] BGBl. 2004 I, 2206.
[1113] BT-Drs. 15/1508, 36.
[1114] Zu diesem Punkt vgl. auch *LfD Baden-Württemberg*, 19. Tätigkeitsbericht, Tz. 2.4.
[1115] BT-Drs. 15/4067, 62.

des Termins und dem Termin, wenn nicht besondere Gründe vorliegen, nicht mehr als sechs Monate betragen. § 43 Abs. 1 ZVG bestimmt, dass die Terminsbestimmung mindestens sechs Wochen vorher bekanntgemacht werden muss.[1116] Aus datenschutzrechtlicher Sicht wäre es wünschenswert, wenn die Veröffentlichung des Termins möglichst kurz gehalten wird, d.h. sie sollte sich an der sechs-Wochen Frist orientieren. Durch eine verfrühte Bekanntgabe wird zum einen der Kredit des Schuldners gefährdet. Zum anderen vergessen die Leser – auch bei einer Veröffentlichung im Internet – den Termin wieder.[1117]

8.5.2 Veröffentlichung von Wertgutachten

Im Unterschied zu den Terminsbestimmungen ist für die Veröffentlichung von Wertgutachten keine Rechtsgrundlage vorhanden.[1118] Nach § 38 Abs. 2 ZVG kann das Gericht zwar Wertgutachten in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem öffentlich bekannt machen. Der Gesetzgeber verfolgte mit dieser Regelung das Ziel, die Verwertungsmöglichkeiten im Zwangsversteigerungsverfahren zu verbessern.[1119] Das Kommunikationssystem und die Art der Veröffentlichung werden jedoch landesrechtlich bestimmt. Eine solche landesrechtliche Bestimmung existiert derzeit in Rheinland-Pfalz nicht. Auch andere Rechtsgrundlagen kommen nicht in Betracht. § 40 Abs. 2 ZVG gestattet zwar dem Gericht, noch andere oder wiederholte Veröffentlichungen zu veranlassen. Die Vorschrift bezieht sich jedoch nur auf die Veröffentlichung von Terminsbestimmungen, ansonsten hätte der Gesetzgeber wie auch in § 38 Abs. 2 ZVG ausdrücklich die Worte Wertgutachten und Abschätzungen genannt. Auch § 42 ZVG ist nicht einschlägig. Zwar steht jedem ein Akteneinsichtsrecht ohne nähere Begründung zu. Voraussetzung dieses Rechts ist aber zumindest eine Antragstellung. Von dieser Bestimmung kann keinesfalls die Befugnis zur Veröffentlichung im Internet umfasst werden. Dass es für die Veröffentlichung von Wertgutachten einer Rechtsgrundlage bedarf, folgt aus dem Grundsatz des Vorbehalts des Gesetzes. Die Veröffentlichung von Wertgutachten geht – ebenso wie die Terminsbestimmungen – mit einem Eingriff in das informationelle Selbstbestimmungsrecht einher. Bei den Informationen in einem Wertgutachten handelt es sich um personenbezogene Daten nach § 3 LDSG. Zwar werden auf der Plattform der Name von Schuldner und Eigentümer der betroffenen Liegenschaft nicht genannt. Jedoch ist das Grundstück mit den Angaben zu Flurstück, Straße und Hausnummer so genau bezeichnet, dass für einen beliebig großen Personenkreis durch einfach zu erlangende Zusatzinformationen Bewohner und auch die Eigentümer der Liegenschaften leicht zu eruieren sind.[1120] Bei der Anzeige einzelner Datensätze erfolgt sogar schon eine direkte Verlinkung zu einem „GeoServer“, in der Regel ist dies Google Maps. Besonders problematisch ist dies, da Google Maps nicht nur die Adresse, sondern sofort auch die Google bekannten Personen und Firmen mit dieser Anschrift anzeigt wie aus Abbildung 4 auf Seite 215 ersichtlich.

[1116] Anderenfalls muss der Versteigerungstermin nach § 43 ZVG aufgehoben und von neuem bestimmt werden.
[1117] *Stöber*, ZVG, § 39 Rn. 2.8.
[1118] *Klink*, D-A-CH, 23. Vgl. auch *LfD Rheinland-Pfalz*, 22. Tätigkeitsbericht, Tz. 11.2.1.
[1119] BT-Drs. 16/3038, 42.
[1120] *LfD Rheinland-Pfalz*, 19. Tätigkeitsbericht, Tz. 7.1.3.

Folglich sollte auf diese Form der Veröffentlichung und erst recht auf die Übermittlung der Daten an die Firma hansen marketing e.K.[1121] verzichtet werden.

8.6 E-Versteigerungen

Nach § 814 Abs. 2 Nr. 2 ZPO kann die öffentliche Versteigerung gepfändeter Sachen auch im Rahmen einer allgemein zugänglichen Auktion im Internet erfolgen. Die Regelungen zur Internetversteigerung sind aus datenschutzrechtlicher Sicht als positiv zu bewerten. Sie enthalten sowohl Vorgaben zur Anonymisierung der Schuldnerdaten als auch zur Anonymisierung der Daten von Anbietern. So regelt § 814 Abs. 3 Nr. 6 ZPO, dass die Landesregierungen durch Rechtsverordnung zu bestimmen haben, dass die Angaben zur Person des Schuldners vor ihrer Veröffentlichung zu anonymisieren sind. Nach der Gesetzesbegründung ist die Veröffentlichung von Daten, die Rückschlüsse auf die Identität des Schuldners zulassen, zur Durchführung der Versteigerung nicht erforderlich und wäre daher ein unverhältnismäßiger Eingriff in dessen Persönlichkeitsrechte.[1122] Daneben ist in § 814 Abs. 3 Nr. 6 ZPO vorgesehen, dass auch die Angaben der Bieter zu anonymisieren sind.

8.7 Zusammenfassung

Die im Zwangsvollstreckungsverfahren gespeicherten personenbezogenen Daten enthalten vielfach konkrete Angaben zum Vermögenswert des Schuldners oder geben zumindest Auskunft über dessen Zahlungsfähigkeit und -willigkeit. Da der Schuldner damit für immer gebrandmarkt werden kann, kommt dem informationellen Selbstbestimmungsrecht in diesem Bereich eine große Bedeutung zu. Die zukünftigen Ausgestaltungen des elektronischen Schuldnerverzeichnisses und des elektronischen Vermögensverzeichnisses können trotz ihrer größeren jeweiligen Eingriffsintensität als verfassungsgemäß bezeichnet werden. Beide Register dienen einem legitimen Zweck, sind erforderlich und aufgrund verschiedener Schutzvorkehrungen auch verhältnismäßig. Auch die grundsätzliche Ausrichtung der beiden Verzeichnisse als zentrale landesweite Datei begegnet keinen Bedenken, da Gerichtsvollzieher auf überörtliche Verzeichnisse dringend angewiesen sind, um zu überprüfen, ob der Schuldner bereits eine Vermögensauskunft abgegeben hat. Dies schützt auch den Schuldner vor einer nochmaligen Abgabe der Vermögensauskunft.

Dessen ungeachtet sind jedoch insbesondere die Regelungen zur Online-Einsicht des Schuldnerverzeichnisses zu kritisieren. Sie gehen zu weit. Ein Internet-Schuldnerverzeichnis für jedermann ist abzulehnen. Die Vorgaben hätten dahingehend eingeschränkt werden sollen, dass nur bestimmten Stellen ein Online-Zugriff gestattet ist. Da jedoch nicht zu erwarten ist, dass der Gesetzgeber das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung vor

[1121] Vgl. hierzu Abschnitt 2.3.2.5.
[1122] BT-Drs. 12811, 11.

seinem Inkrafttreten am 1.1.2013 ändern wird, wird es umso wichtiger sein, dass in der noch zu errichtenden Rechtsverordnung zumindest strenge Vorgaben im Hinblick auf eine zuverlässige Registrierung, eine Protokollierung sowie die Festsetzung einer hohen Gebühr zum Abruf festgeschrieben werden.

Beim elektronischen Vermögensverzeichnis hat der Gesetzgeber die Online-Auskunft zufriedenstellend gelöst, wenngleich die Regelungen zur Löschung und Auskunft anders hätten ausgestaltet werden sollen. Bei beiden Registern fällt auf, dass der Gesetzgeber die Datenverarbeitung im Auftrag nicht auf öffentliche Stellen begrenzt hat. Angesichts der Sensibilität der in einem Zwangsvollstreckungsverfahren gespeicherten personenbezogenen Daten wäre hier jedoch eine entsprechende Beschränkung erforderlich gewesen.

Die Regelungen zur elektronischen Antragstellung für einen Pfändungs- und Überweisungsbeschluss in § 829a ZPO sind nicht gelungen. Sie sind mit erheblichen Missbrauchsrisiken verbunden. In Zukunft wird man ein Äquivalent für den herkömmlichen papiergebundenen Titel benötigen. Hier bietet sich ein Verfahren ähnlich der von elektronischen Münzen an.

Die Veröffentlichungen von Terminsbestimmungen im Zwangsversteigerungsverfahren begegnet ebenfalls keinen verfassungsrechtlichen Bedenken. Gleichwohl werden die Gerichte bei der Wahl ihres Veröffentlichungsmediums und der Frage einer wiederholten Veröffentlichung das informationelle Selbstbestimmungsrecht zu berücksichtigen haben. Im Unterschied zu den Terminsbestimmungen erfolgen die Veröffentlichungen von Wertgutachten dagegen ohne Rechtsgrundlage. Für diese Arten von Veröffentlichungen muss baldmöglichst eine entsprechende Grundlage geschaffen werden.

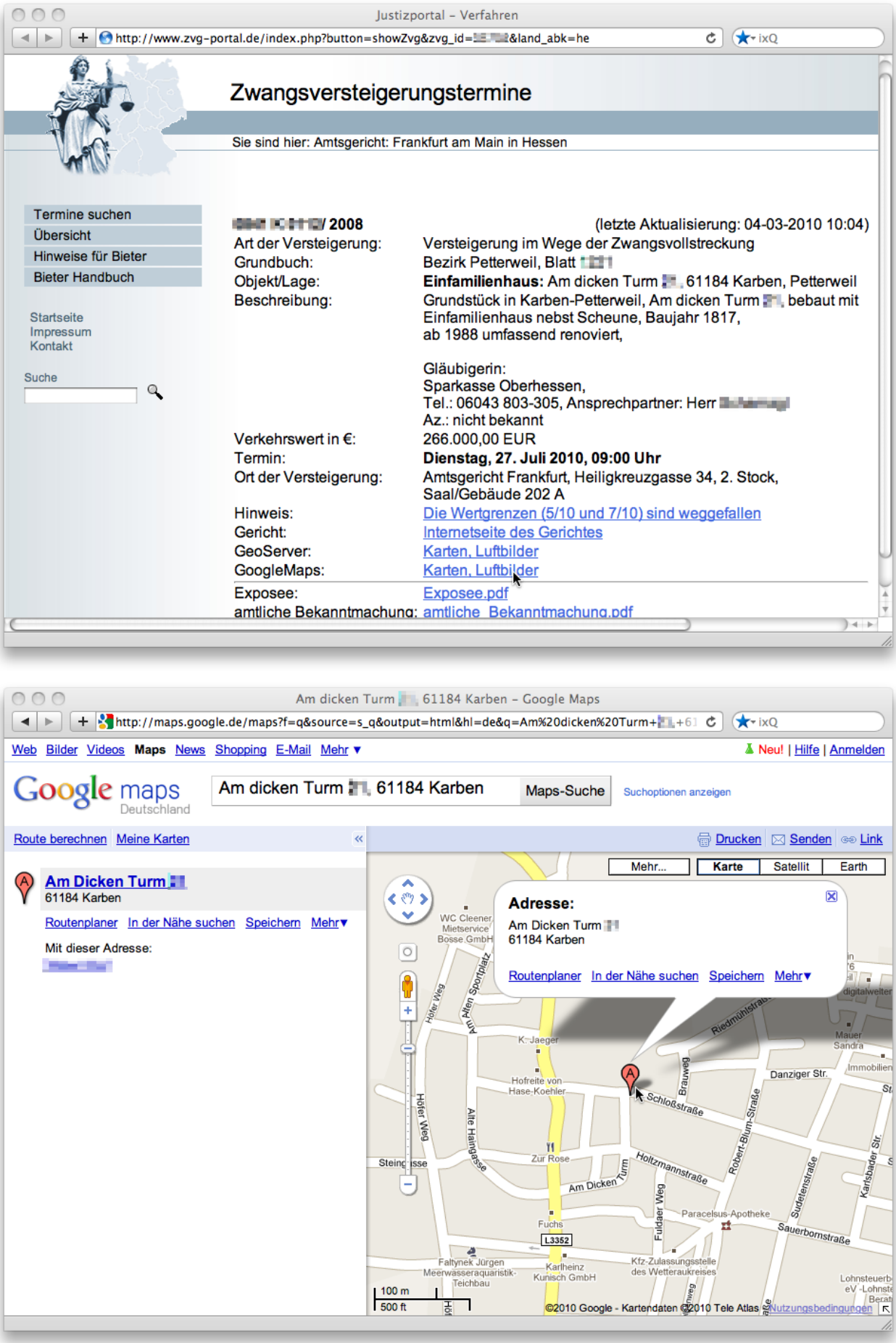

Abbildung 4: Verknüpfung von Geo- und Zwangsversteigerungsdaten.

Kapitel 9

Insolvenzverfahren

Für die Modernisierungen im Zivilverfahren, dem Zwangsvollstreckungs- und dem Zwangsversteigerungsverfahren wurde untersucht, wie der Datenschutz dort verbessert werden kann. Nun wird der Datenschutz bei den Modernisierungsformen im Insolvenzverfahren betrachtet. Der Schwerpunkt dieser Prüfung liegt bei den Veröffentlichungen von Insolvenzdaten im Internet. Im Anschluss daran folgen Ausführungen zu den elektronischen Tabellen und Verzeichnissen, zur elektronischen Forderungsanmeldung und zur allgemeinen elektronischen Kommunikation im Insolvenzverfahren entsprechend der Verweisungsvorschrift des § 4 InsO.

9.1 E-Bekanntmachungen im Internet

§ 9 Abs. 1 InsO bestimmt, dass die Bekanntmachungen im Insolvenzverfahren zwingend durch eine zentrale und länderübergreifende Veröffentlichung im Internet zu erfolgen haben.[1123] Was im Einzelnen öffentlich bekannt zu machen ist, ergibt sich nicht aus § 9 InsO. Vielmehr sind die Vorschriften im Zusammenhang mit der Regelung des Gegenstandes der Bekanntmachung zu suchen.[1124] Ihre Zahl in der Insolvenzordnung ist groß.[1125] Auch der Beschluss, mit dem ein Insolvenzantrag mangels Masse abgewiesen wird, ist seit 2007[1126] nach § 26 Abs. 1 Satz 3 InsO öffentlich bekannt zu machen. Das Gericht hat die Bekanntmachungen von Amts wegen zu veranlassen. Dies ergibt sich zwar nicht ausdrücklich aus dem Wortlaut des § 9 InsO.

[1123] Zunächst sah der RegE zum InsOÄndG von 2001 zunächst den Begriff „des elektronisch betriebenen Informationsverbreitungssystem“ vor, welche aus § 15 WpHG übernommen wurde. Von diesem Begriff wurde jedoch im weiteren Gesetzgebungsverfahren wieder Abstand genommen, weil von diesem System nicht das Internet umfasst sei, sondern ein nach außen abgeschottetes Bank- und Börseninformationssystem für eine geschlossene Benutzergruppe. Vgl. hierzu BT-Drs. 14/6468, 17.

[1124] *Nerlich/Römermann*, InsO, § 9 Rn. 3.

[1125] Vgl. hierzu §§ 23 Abs. 1 Satz 1, 25 Abs. 1, 26 Abs. 1 Satz 3, 30 Abs. 1 Satz 1, 34 Abs. 3 Satz 1, 64 Abs. 2 Satz 1, 74 Abs. 2 Satz 1, 78 Abs. 2 Satz 1, 177 Abs. 3 Satz 1, 188 Satz 3, 189 Abs. 1, 200 Abs. 2 Satz 1, 208 Abs. 2 Satz 1, 214 Abs. 1 Satz 1, 215 Abs. 1 Satz 1, 235 Abs. 2 Satz 1, 258 Abs. 3 Satz 1, 267 Abs. 1 und 2, 268 Abs. 2 Satz 1, 273, 277 Abs. 3 Satz 1, 289 Abs. 2 Satz 3, 300 Abs. 3 Satz 1, 303 Abs. 3 Satz 3 InsO.

[1126] BGBl. 2007 I, 509.

Ein Tätigwerden von Amts wegen ist jedoch die Konsequenz aus dem Amtsermittlungsgrundsatz nach § 5 Abs. 1 Satz 1 InsO. Die gesetzlich angeordnete öffentliche Bekanntmachung kann gemäß § 9 Abs. 1 Satz 1 2. Hs. InsO auch nur auszugsweise erfolgen. Nach § 9 Abs. 1 Satz 2 InsO ist der Schuldner jedoch genau zu bezeichnen, insbesondere sind seine Anschrift und sein Geschäftszweig anzugeben. Zudem wurde mit dem Gesetz zur Vereinfachung des Insolvenzverfahrens von 2007[1127] noch zusätzlich geregelt, dass der Eröffnungsbeschluss auch das Geburtsjahr des Insolvenzschuldners und die Nummer, unter der er im Handelsregister eingetragen ist, enthalten muss[1128] sowie einen Hinweis, ob der Schuldner einen Antrag auf Restschuldbefreiung gestellt hat.[1129]

§ 9 Abs. 2 Satz 1 InsO bestimmt, dass das Gericht weitere Veröffentlichungen veranlassen kann, sofern dies landesrechtlich bestimmt ist. Damit ist eine gleichzeitige oder spätere Veröffentlichung mittels eines anderen Mediums als desjenigen, mit dem die öffentliche Bekanntmachung zu bewirken ist, gemeint.[1130] Ob das Gericht hiervon Gebrauch macht, steht in seinem pflichtgemäßen Ermessen.[1131] Bei der Frage gegen oder für eine zusätzliche Bekanntmachung und bei der Auswahl der Medien wird es sich von der Frage leiten lassen, wie es den Betroffenen am besten erreicht. In Betracht kommen neben Tageszeitungen und Wochenzeitungen der Bundesanzeiger und andere Mitteilungsblätter, eine Anschlagstafel bei Gericht oder der Rundfunk. Allerdings kommt als Veröffentlichungsmedium nicht das Internet in Betracht. Insofern stellt § 9 Abs. 1 InsO eine Sonderreglung dar, neben der eine weitere Insolvenzveröffentlichung durch die Insolvenzgerichte auf einer nicht amtlichen Internetseite auch unter den Voraussetzungen des § 9 Abs. 2 Satz 1 InsO unzulässig ist.[1132]

Von den amtlichen Bekanntmachungen nach § 9 InsO sind Veröffentlichungen von privaten Betreibern zu unterscheiden, insbesondere von Verlagen, Auskunfteien und Wirtschaftsinformationsdiensten. Diese durchsuchen systematisch die jeweiligen Bekanntmachungen und veröffentlichen diese auf ihren Homepages im Internet.[1133] Die amtlichen Bekanntmachungen dürfen schließlich auch nicht mit der Internetveröffentlichung von einzelnen Insolvenzverwaltern[1134] verwechselt werden.

[1127] BGBl. 2007 I, 509.
[1128] § 27 Abs. 1 Nr. 1 InsO.
[1129] § 27 Abs. 1 Nr. 4 InsO.
[1130] *Nerlich/Römermann*, InsO, § 9 Rn. 13.
[1131] *Nerlich/Römermann*, InsO, § 9 Rn. 13.
[1132] So *Bundesregierung*, BT-Drs. 15/181, 3, a.A. *Nerlich/Römermann*, InsO, § 9 Rn. 17.
[1133] Vgl. hierzu Informationsdienst für Insolvenzverfahren (`http://www.insolnet.de`, Zugriff am 20.5.2010); WBDat Wirtschafts- und Branchendaten GmbH (`http://www.indat.info`, Zugriff am 20.5.2010).
[1134] Zum Beispiel der Rechtsanwaltschaftsgesellschaft Schultze & Braun GmbH, Achern, (`http://www.schubra.de`, Zugriff am 20.5.2010).

9.1.1 Verfassungsmäßigkeit

Die Veröffentlichung von gerichtlichen Bekanntmachungen als Sonderform staatlicher Datenübermittlung[1135] stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Allein die Kenntnis von der Eröffnung eines Insolvenzverfahrens kann sowohl im gesellschaftlichen Bereich als auch insbesondere in den Geschäftskreisen, denen der Schuldner angehört, einen allgemeinen Ansehensverlust zur Folge haben, der gleichsam wie ein Makel am Schuldner haftet.[1136] Auf die öffentliche Bekanntmachung von Insolvenzdaten kann jedoch nicht ohne weiteres verzichtet werden.[1137] Das Insolvenzverfahren ist ein Massenverfahren, bei dem der Kreis der Betroffenen groß ist und sich nicht immer von vornherein überschauen lässt. Mit der Eröffnung des Insolvenzverfahrens gehen verschiedene Rechtswirkungen einher, die sich für etwaige Gläubiger und Vertragspartner nachteilig auswirken können. Um hierauf entsprechend reagieren zu können, muss denjenigen Gläubigern, die keine Kenntnis von einem Insolvenzverfahren haben, die Möglichkeit gegeben werden, sich überhaupt ihrer Stellung als Insolvenzgläubiger bewusst zu werden. Dies ist insbesondere mit Blick auf §§ 174 ff. InsO von Bedeutung. Gemäß § 87 InsO können Insolvenzgläubiger ihre Forderungen nämlich nur nach den Vorschriften über das Insolvenzverfahren verfolgen. Eine Klage gegen den Insolvenzschuldner persönlich ist demnach ausgeschlossen. § 28 Abs. 1 Satz 1 InsO bestimmt, dass die Anmeldung zu dieser Forderung innerhalb der vom Insolvenzgericht im Eröffnungsbeschluss festgesetzten Frist unter Beachtung des § 174 InsO beim Insolvenzverwalter zu erfolgen hat. Wird eine Forderung erst nach dem Prüfungstermin angemeldet, sind für den Gläubiger nicht unerhebliche Nachteile verbunden. So hat das Gericht nach § 177 InsO auf Kosten des Säumigen entweder einen besonderen Prüfungstermin zu bestimmen oder die Prüfung hat im schriftlichen Verfahren zu erfolgen. Zudem zeigt sich die Notwendigkeit der Unterrichtung von Gläubigern auch an den Vorgaben zur Restschuldbefreiung nach § 301 Abs. 1 Satz 2 InsO. Diese Vorschrift bestimmt, dass von der erteilten Restschuldbefreiung auch diejenigen Insolvenzgläubiger betroffen sind, die ihre Forderung nicht angemeldet haben. Auch diesen Gläubigern muss die Möglichkeit gegeben werden, Kenntnis vom Restschuldbefreiungsverfahren erlangen zu können, damit sie die Versagung der Restschuldbefreiung im Schlusstermin[1138] oder während der Wohlverhaltensperiode[1139] beantragen können. Bereits die öffentliche Bekanntmachung der Ankündigung der Restschuldbefreiung soll den Gläubigern diese Rechte sichern.[1140] Daneben sind mit der Eröffnung des Insolvenzverfahrens noch weitere Rechtswirkungen verbunden. So kann ein Drittschuldner nach der Eröffnung des Insolvenzverfahrens nach § 82 InsO nur dann mit befreiender Wirkung an einen Schuldner leisten, wenn dieser zur Zeit der Leistung die Eröffnung des Insolvenzverfahrens nicht

[1135] BVerfG NJW 1988, 2031 f.
[1136] *Lepa*, 2002, 45.
[1137] LG Duisburg, NJW-RR 2005, 57.
[1138] § 290 InsO.
[1139] § 296 InsO.
[1140] *Keller*, ZIP 2003, 149.

kannte.[1141] Mit der Eröffnung des Insolvenzverfahrens verliert der Schuldner darüber hinaus die Befugnis, über sein Vermögen zu verfügen.[1142] Eine Leistung des Schuldners ist nur wirksam, wenn der Erwerber keine Kenntnis von der Eröffnung des Insolvenzverfahrens hatte. Die öffentliche Bekanntmachung trägt hier dazu bei, eine mögliche Gutgläubigkeit zu zerstören. Aufgrund dieser Folgen ist es sachgerecht, möglichst viele Personen über die Eröffnung des Insolvenzverfahrens zu unterrichten. Die Bekanntmachung zählt also zu den Instrumenten einer möglichst breiten Publizität. Sie stellt eine Kompensation für die mit dem Insolvenzverfahren verbundenen Beschneidungen individuellen Zugriffs auf das Schuldnervermögen dar.[1143] Das Verfahrensziel größtmöglicher Publizität ist dabei nicht nur beschränkt auf die Phase der Eröffnung des Insolvenzverfahrens. Den Verfahrensbeteiligten muss auch über das gesamte Insolvenzverfahren hinweg ermöglicht werden, sich über den jeweiligen Verfahrensstand hinreichend zu informieren. Neben dieser Publikationswirkung ist zu berücksichtigen, dass die öffentliche Bekanntmachung auch mit einer Verfahrensvereinfachung verbunden ist. Eigentlich müssten die Entscheidungen des Insolvenzgerichts, um wirksam zu sein, zugestellt werden. Hierauf kann jedoch nach § 9 Abs. 3 InsO verzichtet werden. Die öffentliche Bekanntmachung ersetzt die Zustellung.

Wägt man das informationelle Selbstbestimmungsrecht des Schuldners mit dem Unterrichtungsinteresse ab, so hat dieses – zumindest bei herkömmlichen Bekanntmachungen in Amtsblättern und Tageszeitungen – hinter das Unterrichtungsinteresse der Allgemeinheit zurückzutreten.[1144] § 9 InsO i.V.m. mit den Vorschriften, welche die Bekanntmachung anordnen, dient somit als verfassungsrechtliche Schranke. Der Insolvenzschuldner muss diesen Eingriff hinnehmen. Im Jahr 1988 hatte das Bundesverfassungsgericht eine Vorschrift zur Bekanntmachung der Entmündigung wegen Verschwendung oder wegen Trunksucht sowie die Wiederaufhebung einer solchen Entmündigung als verfassungswidrig angesehen.[1145] Das Bundesverfassungsgericht hat seine Entscheidung u.a. damit begründet, dass die öffentliche Bekanntmachung wegen einer Entmündigung keine Rechtswirkungen entfalte, sondern sich in einer breit gestreuten, nicht zweckgebundenen Warnung erschöpfen würde. Auf die Bekanntmachungen nach der Insolvenzordnung trifft dies jedoch nicht zu. Mit ihr sind, wie gesehen, Rechtswirkungen verbunden.

[1141] Vgl. hierzu BGH, ZIP 2010, 935: „Haben Unternehmen mit umfangreichen Zahlungsverkehr zur Erfüllung einer Verbindlichkeit an einen Insolvenzschuldner geleistet, ohne dass sie die Eröffnung des Insolvenzverfahrens kannten, hindert sie die Möglichkeit, diese Informationen durch eine Einzelabfrage aus dem Internet unter `http://www.insolvenzbekanntmachungen.de` zu gewinnen, nach Treu und Glauben nicht daran, sich auf ihre Unkenntnis zu berufen. Sie sind nicht gehalten, sich wegen der Möglichkeit der Internetabfrage beweismäßig für alle Mitarbeiter zu entlasten."

[1142] §§ 27, 80, 81 Abs. 1, 21 Abs. 2 Nr. 2, 24 Abs. 2 InsO.

[1143] *Nerlich/Römermann*, InsO, § 9 Rn. 2.

[1144] So *Nerlich/Römermann*, InsO, § 9 Rn. 2.

[1145] BVerfG NJW 1988, 2031. Die Vorschrift hatte allerdings nur geringe praktische Relevanz. In der Zeit vom 1.10.1985 bis zum 30.9.1987 ist zum Beispiel in Rheinland-Pfalz nur eine einzige Veröffentlichung erfolgt, die die Aufhebung der Trunksucht zum Gegenstand hatte. Vgl. hierzu *LfD Rheinland-Pfalz*, 11. Tätigkeitsbericht, Tz. 7.2.3.1.

Mit den Internetbekanntmachungen geht eine intensivere Gefährdung des informationellen Selbstbestimmungsrechts einher. So sind die Daten weltweit abrufbar und sie können auch nicht gelöscht werden.[1146] Der Gesetzgeber wollte mit den Internetbekanntmachungen die Publizität erhöhen und gleichzeitig die Druckkosten und damit die Verfahrenskosten senken.[1147] Insbesondere im Verbraucherinsolvenzverfahren ist dies von Bedeutung. Wegen der geringen Massen können hohe Veröffentlichungskosten dazu beitragen, dass diese Verfahren erst gar nicht eröffnet werden und dass dem Schuldner dadurch der Weg zur Restschuldbefreiung versperrt bleibt. Akzeptiert man dieses gesetzgeberische Ziel, müssen zum Schutz des Schuldners Vorkehrungen getroffen werden, um die Verhältnismäßigkeit des Grundrechts sicher zu stellen. Dies hat der Gesetzgeber mit der auf der Grundlage des § 9 Abs. 2 Satz 2 und 3 InsO erlassenen Rechtsverordnung getan, weshalb die Veröffentlichung von Insolvenzdaten im Internet verfassungsgemäß ist. Gleichwohl wären auch hier Änderungen wünschenswert.

9.1.2 Zentrale Struktur

Gemäß § 9 InsO erfolgt die öffentliche Bekanntmachung durch eine zentrale und länderübergreifende Veröffentlichung ausschließlich im Internet. Aufgrund der zentralen Struktur der Insolvenzbekanntmachungen sind zum Schutz des Schuldners in der Bekanntmachungsverordnung Einschränkungen bei den Suchkriterien enthalten. Sie konkretisieren den in § 1 Abs. 3 LDSG enthaltenen Grundsatz der Datensparsamkeit.[1148] § 2 Abs. 1 Nr. 3 InsoBekV bestimmt insofern, dass die Daten spätestens nach Ablauf von zwei Wochen nach dem ersten Tag der Veröffentlichung nur noch dann abgerufen werden können, wenn die Abfrage den Sitz des Insolvenzgerichts und mindestens den Familiennamen, die Firma, den Sitz oder Wohnsitz des Schuldners, das Aktenzeichen des Insolvenzgerichts oder die Registernummer und den Sitz des Registergerichts enthält.[1149] Diese beschriebenen Beschränkungen, also selektive Suchanfrage und zeitliche Komponente, führen zu einer datensparsamen Ausgestaltung der Insolvenzdatenbank. Mit ihnen werden die Suchmöglichkeiten für Dritte erschwert und dem Grundsatz der Datensparsamkeit wird in verhältnismäßiger Weise Rechnung getragen.

Vor dem Ablauf von zwei Wochen dürfen die Daten aber ohne jegliche Einschränkungen, also frei im Internet, zur Verfügung stehen. Eine solche selektionslose Darstellung im Internet lässt sich als offene Einsichtnahme bezeichnen.[1150] Den Gerichten steht es frei, ob sie die Daten während der ersten zwei Wochen uneingeschränkt zur Verfügung stellen oder ob sie schon vom ersten Tag der Veröffentlichung eine Beschränkung nach den genannten Kriterien vorneh-

[1146] Zu diesen Gefahren vgl. *DSB-Konferenz*, 24.4.2001.

[1147] Dabei hat er keine Erhebungen angestellt, wie hoch sich diese Kosten belaufen. Nach *Vallander/Fuchs*, NZI 2003, 292 machen die Veröffentlichungskosten im Insolvenz- und Restschuldbefreiungsverfahren natürlicher Personen durchschnittlich einen Betrag von ca. 70-400 EUR aus.

[1148] Vgl. hierzu Abschnitt 5.1.3.

[1149] Aus dem Begriff „mindestens“ folgt, dass die Suchkriterien auch kumulativ eingegeben werden können.

[1150] Vgl. hierzu *Riebeling*, 2005, 87 mit dem Verweis darauf, dass das Portal diese Suchmöglichkeit als „uneingeschränkte Suche“ bezeichnet.

men.[1151] Dieses sog. Optionsmodell[1152] ist jedoch zu kritisieren. Mit einer uneingeschränkten Suchmöglichkeit während der ersten zwei Wochen wird dem Grundsatz der Datenvermeidung und Datensparsamkeit nicht mehr in ausreichendem Maße Rechnung getragen. Der Verordnungsgeber ging zutreffend davon aus, dass er mit den Regelungen für die eingeschränkte Suchmöglichkeit eine Analogie zu den Veröffentlichungen in Printmedien erreicht hat.[1153] Die Suchkriterien bei einer eingeschränkten Suche sind nämlich schon so offen formuliert, dass bei ihrer Verwendung ein Interessent ohne größeren Aufwand sich über das für ihn relevante Insolvenzgeschehen informieren kann. Die Suche wird zudem dadurch erleichtert, dass die Kriterien nicht in vollständig korrekter Schreibweise eingegeben werden müssen, sondern auch eine Abfrage mittels unvollständiger Angaben zulässig ist, sofern diese noch Unterscheidungskraft besitzen.[1154] Mit Blick hierauf hat der Verordnungsgeber davon abgesehen, die insolvenzrechtlichen Daten erst mittels einer an enge Recherchekriterien gebundenen Suchfunktion wie zum Beispiel dem vollständigen Namen oder dem kompletten Aktenzeichen sichtbar zu machen.[1155] Diejenigen, die sich mit Blick auf eine erhöhte Publikationswirkung für eine obligatorische uneingeschränkte Suche von Anfang an aussprechen,[1156] verkennen, dass die mit einer uneingeschränkten Suche einhergehende Trefferquote letzten Endes so hoch ist, dass sie nicht mehr überschaubar ist und für den Gläubiger keinen großen Nutzen bringt. Einen Nutzen wird die Datenbank nur für die vielen Auskunfteien und Verlage bringen, welche die Daten nach einer uneingeschränkten Suche massenhaft herunterladen und nach beliebig vielen Kriterien auswerten können. Vor diesem Hintergrund hätte man von Anfang an lediglich eine – obligatorische – beschränkte Suche vorsehen sollen.

9.1.3 Inhalt der Bekanntmachung

Für die öffentliche Bekanntmachung gibt § 9 Abs. 1 Satz 2 InsO vor, dass der Schuldner genau zu bezeichnen ist, insbesondere sind seine Anschrift und sein Geschäftszweig anzugeben.[1157] Nähere Ausführungen, welche Daten für eine genaue Bezeichnung des Schuldners erforderlich sind, enthält § 9 InsO jedoch nicht. Auch die Bekanntmachungsverordnung bringt in § 1 Satz 2 InsoBekV lediglich die Selbstverständlichkeit zum Ausdruck, dass die Veröffentlichung nur die

[1151] Derzeit werden auf der Internetseite die Insolvenzdaten während der ersten zwei Wochen uneingeschränkt zur Verfügung gestellt. Vgl. hierzu `http://www.insolvenzbekanntmachungen.de` (Zugriff am 20.5.2010).

[1152] *Riebeling*, 2005, 92

[1153] BR-Drs. 1082/01, 6.

[1154] BR-Drs. 1082/01, 7.

[1155] BR-Drs. 1082/01, 6.

[1156] So *Riebeling*, 2005, 92. Er bemängelt, dass die Verordnung eine Beschränkung von Anfang an zulasse. Die Notwendigkeit eines zielgerichteten Agierens des Interessenten sperre die bei Printveröffentlichungen oder offenen Einsichtnahmen vorhandene Möglichkeit eines Interessenten, bei Durchsicht des aktuellen Insolvenzgeschehens ein für ihn relevantes Verfahren zu erblicken. Aus diesem Grunde solle die Bekanntmachungsverordnung das Optionsmodell mit der Wahl zwischen einer anfänglich offenen Einsichtnahme und einer später selektiven Einsichtnahme beseitigen und eine zunächst offene Einsichtnahme obligatorisch vorschreiben.

[1157] Zur Frage des Haftungsausschlusses bei fehlerhaften Bekanntmachungen vgl. OLG Düsseldorf, MMR 2009, 57.

personenbezogenen Daten enthalten darf, die nach der Insolvenzordnung oder nach anderen Gesetzen, die eine öffentliche Bekanntmachung in Insolvenzverfahren vorsehen, bekannt zu machen sind. Im Hinblick auf den mit einer Internetveröffentlichung einhergehenden tiefen Eingriff in das informationelle Selbstbestimmungsrecht wäre es jedoch erforderlich gewesen, im Gesetz selbst genau festzulegen, welche Daten des Insolvenzschuldners veröffentlicht werden dürfen. Lediglich im Falle der Eröffnung des Insolvenzverfahrens hat der Gesetzgeber in § 27 Abs. 2 InsO genaue Vorgaben getroffen.[1158] Insgesamt hätten also die verschiedenen Bekanntmachungen daraufhin überprüft werden müssen, welche Daten – bei möglichst schonendem Umgang mit dem informationellen Selbstbestimmungsrecht – zu veröffentlichen sind, um eine Verwechslung von Insolvenzschuldnern zu vermeiden. Für eine genaue Bezeichnung des Schuldners würden sich dabei der Vor- und Nachname des Insolvenzschuldners, sein Geschäftszweig, sein Geburtsdatum und die Nummer, unter der er im Handelsregister eingetragen ist, anbieten. Auf die Angabe des Wohnorts oder der Wohnanschrift könnte jedoch – entgegen § 9 Abs. 1 Satz 2 InsO – verzichtet werden. Diese Angaben tragen zur Identifizierung nicht viel bei, da sie sich schnell ändern können. Die Identifizierung einer bestimmten Person wird vielmehr durch die Angabe des Namens und des Geburtsdatums in ausreichendem Maße sichergestellt.[1159]

9.1.4 Löschung der Bekanntmachungen

Nach § 3 Abs. 1 Satz 1 InsoBekV werden die Daten spätestens nach Ablauf von einer Frist von sechs Monaten nach der Aufhebung oder der Rechtskraft der Einstellung des Insolvenzverfahrens gelöscht. Für das Restschuldbefreiungsverfahren hielt der Verordnungsgeber eine gesonderte Bestimmung erforderlich. Nach § 3 Abs. 2 InsoBekV gilt Absatz 1 Satz 1 für die Veröffentlichungen im Restschuldbefreiungsverfahren einschließlich des Beschlusses nach § 289 der Insolvenzordnung entsprechend mit der Maßgabe, dass die Frist mit Rechtskraft der Entscheidung über die Restschuldbefreiung zu laufen beginnt. Die sechsmonatige Löschfrist wurde erst mit dem Gesetz zur Vereinfachung des Insolvenzverfahrens im Jahr 2007[1160] eingefügt. Davor betrug sie einen Monat.[1161] Der Verordnungsgeber hat die Verlängerung der Frist damit begründet, dass die Löschfrist von einem Monat zu kurz sei, um die Öffentlichkeit zu informieren. Die kurze Frist würde dazu führen, dass entweder der mit der öffentlichen Bekanntmachung angestrebte Schutz nicht realisiert würde oder nach der Löschung noch zahlreiche Anfragen bei Gericht eingingen. Werde künftig noch die Abweisung mangels Masse öffentlich bekannt gemacht, so sei nochmals mit einem Anstieg der Anfragen zu rechnen. Der durch die Internetbekanntmachung erhoffte Entlastungseffekt bei den Gerichten würde somit vollständig

[1158] Die Angabe des Geburtsjahres und der Registernummer, unter der der Schuldner in das Handelsregister eingetragen ist und ein Hinweis darauf, ob der Schuldner einen Antrag auf Restschuldbefreiung gestellt hat, sind 2007 neu in § 27 Abs. 2 InsO aufgenommen worden. Die ersten beiden Angaben hielt der Gesetzgeber für erforderlich, um Verwechslungen zu vermeiden und eine größere Rechtssicherheit zu schaffen (BT-Drs. 16/3227, 16).

[1159] *Deutscher Anwaltsverein*, 2005, 6.

[1160] BGBl. 2007 I, 509.

[1161] BGBl. 2002 I, 677.

verfehlt werden.[1162] Dies überzeugt jedoch nicht. Nach den allgemeinen datenschutzrechtlichen Grundsätzen sind die personenbezogenen Daten dann zu löschen, wenn ihre Kenntnis zur Erfüllung der Aufgaben nicht mehr erforderlich ist.[1163] Damit wird der wesentliche Aspekt hervorgehoben, dass die mit der Datenspeicherung verbundene Aufgabe erfüllt ist.[1164] Die formelle Rechtskraft des Einstellungsbeschlusses oder des Beschlusses über die Restschuldbefreiung tritt nach Ablauf der zweiwöchigen Beschwerdefrist ein.[1165] Sobald Rechtskraft eingetreten ist, benötigt der Rechtsverkehr die Daten aber grundsätzlich nicht mehr. Mit der vormals einmonatigen Löschungsfrist hat der Verordnungsgeber an die Frist nach Rechtskraft noch eine Phase der Einsichtnahme geknüpft, was vom Grundsatz her vertretbar war. Die sechsmonatige Löschfrist ist jedoch zu lange. Insbesondere im Interesse von natürlichen Personen, die eine Restschuldbefreiung erlangt haben, muss gewährleistet sein, dass ihr wirtschaftlicher Neuanfang nicht durch die fortlaufende Publizität von Veröffentlichungen aus dem Insolvenzverfahren gestört wird.[1166] Aus der Formulierung „spätestens“ folgt zwar, dass auch eine frühere Löschung möglich ist. Die Gerichte haben hiervon jedoch keinen Gebrauch gemacht. Insofern sollte in der Verordnung geregelt werden, dass eine Löschung nach Rechtskraft der Einstellung des Insolvenzverfahrens zu erfolgen hat oder spätestens einen Monat danach.

Seit dem Inkrafttreten der Insolvenzordnung werden die Veröffentlichungen durch Verlage, durch Auskunfteien und Wirtschaftsinformationsdienste ausgewertet[1167] und über das Internet verbreitet. Die Weiterverbreitung von Insolvenzdaten erfolgt auf diese Weise außerhalb jeglicher staatlicher Kontrolle. Es liegen derzeit keine genaueren Erkenntnisse vor, in welchem Zeitraum diese die Daten löschen. Derzeit fällt die Verbreitung der Daten nach Ablauf einer Löschungsfrist weder unter einen Straftatbestand nach dem StGB noch unter einen Straf- bzw. Ordnungswidrigkeitentatbestand nach dem BDSG:[1168] Als Strafvorschriften nach dem StGB kämen lediglich §§ 187 (Verleumdung) oder 203 StGB (Verletzung des Privatgeheimnisses) in Betracht. § 187 StGB ist jedoch nicht einschlägig, da es an der Unwahrheit der verbreiteten Tatsachen fehlt und zwar unabhängig davon, ob die Daten vor oder nach dem Eintritt einer gesetzlichen Löschfrist weiterverarbeitet werden. Für eine Strafbarkeit nach § 203 StGB fehlt es schließlich an einem Geheimnis, denn die veröffentlichten Daten sind bis zur Löschung einer Vielzahl von Dritten erlaubterweise zur Kenntnis gelangt. Nach § 43 Abs. 2 Nr. 1 und 2 BDSG handelt ordnungswidrig, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt, verarbeitet oder mittels eines automatisierten Abrufverfahrens bereithält. Die auf den Internetseiten veröffentlichten Daten sind jedoch allgemein zugänglich. An dieser einmal eingetretenen Allgemeinzugänglichkeit ändert sich auch nichts, wenn die

[1162] BT-Drs. 16/3227, 21.
[1163] § 19 Abs. 2 Nr. 2 LDSG.
[1164] Vgl. hierzu Abschnitt 5.4.3.
[1165] §§ 216, 289 Abs. 2 Satz 1, 6 Abs. 2 InsO i.V.m. §§ 557, 569 Abs. 1 ZPO.
[1166] So auch die Begründung zur Verordnung von 2002, vgl. BR-Drs. 1082/01.
[1167] Das bloße Speichern von Insolvenzdaten unter Auswertung von staatlichen Internetbekanntmachungen ist nach § 29 Abs. 1 Nr. 1 bzw. zumindest nach Nr. 2 BDSG zulässig. Vgl. hierzu ausführlich *Riebeling*, 2005, 70 ff.
[1168] *Bundesregierung*, BT-Drs. 15/181, 6.

Daten aus dem gerichtlichen Informationssystem gelöscht wurden. Außer Frage steht dies, sofern die Daten zugleich in einem Printmedium veröffentlicht wurden, da die darin enthaltenen Informationen dauerhaft allgemein zugänglich bleiben. Aber auch bei einer ausschließlich im Internet vorgenommenen Veröffentlichung kann nichts anderes gelten. Dies zeigt ein Vergleich mit den Inhalten von Rundfunk- und Fernsehsendungen. Diese werden ebenfalls nicht in einer für jedermann jederzeit einsehbaren Form dokumentiert. Trotzdem bleiben sie allgemein zugänglich.[1169] Die Verbreitung der Daten nach Ablauf einer Löschfrist sollte daher mit einem Bußgeld bewehrt oder unter eine Strafe gestellt werden. Eine Möglichkeit wäre es dabei, zunächst § 29 BDSG dahingehend zu ergänzen, dass die Erhebung und Speicherung von Daten zum Zweck der Übermittlung und die Übermittlung dieser Daten im Internet nur unter Beachtung der von den öffentlichen Stellen festgesetzten Fristen zulässig sind. Sodann müsste in § 43 Abs. 2 Nr. 1 und 2 BDSG das Merkmal nicht allgemein zugänglich durch das Merkmal nicht oder nicht mehr allgemein zugänglich geändert werden.[1170] Würde man eine derartige Regelung einführen, würde sich dies auch positiv für den Datenschutz bei anderen zeitlich befristeten Veröffentlichungen auswirken.[1171]

9.1.5 Kopierschutzregelung

§ 9 Abs. 2 Satz 3 Nr. 3 InsO a.F. und § 2 Abs. 1 Satz 3 InsoBekV a.F. hatten Regelungen zu einem Kopierschutz enthalten. Damit sollte das massenhafte Herunterladen von Insolvenzdaten verhindert werden. Mit dem EHUG[1172] wurden die Vorschriften zum Kopierschutz jedoch wieder gestrichen.[1173] Dies erfolgte damals auf eine Prüfbitte des Bundesrates hin. Dieser hatte zu Bedenken gegeben, dass sich ein Kopierschutz in der Praxis nicht durchsetzen ließe und diese Vorschriften deshalb derzeit überflüssig seien.[1174] Die Bundesregierung stimmte damals dem Vorschlag des Bundesrates zu, die genannte Vorschrift zum Kopierschutz aufzuheben, da nach dem derzeitigen Stand der Technik und wohl auch in absehbarer Zukunft ein Schutz gegen ein Kopieren von Veröffentlichungen im Internet nicht erreicht werden könne. Die Frage, wie dem Schutzzweck der genannten Vorschriften auf andere Weise genügt werden könne, werde – so die Bundesregierung weiter – noch geprüft werden müssen; ggf. werde eine entsprechende Regelung auch in einem anderen Gesetzgebungsverfahren mit stärkerem Sachzusammenhang berücksichtigt werden können.[1175] Bislang ist dies jedoch nicht erfolgt. Die Streichung der Regelungen zum Kopierschutz war aus hiesiger Sicht ein Fehler. Der Kopierschutz gehört zu den wichtigsten Regelungen für natürliche Schuldner vor einer dauerhaften und unkontrollierbaren Wiedergabe ihrer Daten im Internet außerhalb des amtlichen Bekanntmachungssystems. Insofern besteht im Grundsatz ein erhebliches und berechtigtes Interesse, entsprechende Schutzvor-

[1169] *Schaffland/ Wiltfang*, BDSG, § 28 Rn. 134.
[1170] *Bundesregierung*, BT-Drs. 15/181, 6.
[1171] *Klink*, D-A-CH, 28.
[1172] BGBl. 2007 I, 2866.
[1173] Vgl. hierzu Abschnitt 2.3.3.1.
[1174] BR-Drs. 942/05, 30.
[1175] BT-Drs. 16/960, 95.

kehrungen vorzusehen, um eine Vervielfältigung so weit es geht, technisch zu unterbinden.[1176] Hätte man die Vorschrift zum Kopierschutz nicht gestrichen, wäre jedenfalls gewährleistet, dass ein nach dem derzeitigen Stand der Technik möglicher Kopierschutz bestehen würde. Die Daten in den oben genannten Seiten liegen derzeit als HTML-Dateien vor. Damit lassen sich die veröffentlichten Daten leicht extrahieren. Als Alternativen, welche das Kopieren zumindest erschweren, kommt einmal die Gestaltung der Dateien als verschlüsseltes PDF-Dokument in Betracht. Dieses kann zwar von Menschen mit Hilfe der zugehörigen Software betrachtet werden, es ist aber nicht ohne weiteres automatisch durchsuch- und auswertbar. Zum anderen wäre die Gestaltung der Dateien als Grafik denkbar. Auch hierdurch kann verhindert werden, dass die Dateien leicht durchsucht werden können. Letztlich ist auch Digital Rights Management eine Möglichkeit, welches z.B. bereits bei den sog. E-Books verwendet wird. Damit kann prinzipiell verhindert werden, dass Kopien von Dokumenten erstellt werden und einem Dokument kann eine Gültigkeitsdauer vergeben werden. Nach Ablauf der Gültigkeit wäre ein Zugriff auf die elektronischen Dokumente nicht mehr möglich.[1177]

9.2 E-Tabellen und E-Verzeichnisse

Bezüglich der bereits vorgestellten Vorschrift des § 5 Abs. 4 InsO gibt es im Unterschied zu den Insolvenzbekanntmachungen keine spezifischen datenschutzrechtlichen Punkte zu beachten. Erforderlich ist, dass die in § 9 LDSG an anderer Stelle dieser Arbeit bereits beschriebenen technisch-organisatorischen Schutzmaßnahmen beachtet werden. Diese Maßnahmen wären dann auch in die noch zu erlassende Rechtsverordnung aufzunehmen.

9.3 E-Forderungsanmeldungen

Wie bereits dargestellt, ermöglicht es § 174 Abs. 4 InsO den Gläubigern, ihre Forderungen elektronisch bei dem Insolvenzverwalter anzumelden. § 174 Abs. 4 InsO bestimmt insofern, dass die Anmeldung durch Übermittlung eines elektronischen Dokuments erfolgen kann, wenn der Insolvenzverwalter der Übermittlung elektronischer Dokumente ausdrücklich zugestimmt hat. In diesem Fall sollen die Urkunden, aus denen sich die Forderung ergibt, unverzüglich nachgereicht werden.

Weder aus dem Wortlaut der Vorschrift noch aus der Gesetzesbegründung lässt sich entnehmen, dass für die Anmeldung von Forderungen der Einsatz einer qualifizierten elektronischen Signatur erforderlich ist.[1178] Da jedoch die Forderungsanmeldung in ihrer rechtlichen Wirkung einem bestimmenden Schriftsatz gleichkommt,[1179] ist die elektronische Forderungsanmeldung

[1176] *Riebeling*, 2005, 111.
[1177] *Klink*, D-A-CH, 20.
[1178] *Riebeling*, 2005, 23.
[1179] *Riebeling*, 2005, 23.

entsprechend den oben genannten Ausführungen zu § 130a ZPO qualifiziert elektronisch zu signieren.[1180] Es wäre wünschenswert, wenn der Gesetzgeber dies im Gesetzestext zum Ausdruck bringen würde.[1181]

Was die Wirksamkeit einer elektronischen Forderungsanmeldung angeht, so reicht es aus, dass der Gläubiger die Originalurkunden einscannt und sie dann dem Insolvenzverwalter übermittelt.[1182] Dies ergibt sich aus dem Wortlaut des § 174 Abs. 4 Satz 2 InsO, welcher besagt, dass die Urkunden unverzüglich nachgereicht werden „sollen". § 174 Abs. 4 Satz 2 InsO ist weiter auch nicht so auszulegen, dass der Gläubiger zur Vorlage der Originalurkunden im Anschluss an die elektronische Forderungsanmeldung verpflichtet ist. Zum einen fordert auch § 174 Abs. 1 Satz 2 InsO (papiergebundene Forderungsanmeldung) nicht die Vorlage des Originals im Sinne des § 420 ZPO.[1183] Diese Vorschrift spricht vielmehr von einer „Abschrift". Und zum anderen besteht die Möglichkeit für den Schuldner, die Authentizität der elektronisch eingereichten und vorher eingescannten Unterlagen zu bestreiten.[1184] In diesem Fall hat der Gläubiger das Original der Urkunde im Prüfungstermin vorzulegen[1185] und für den Schuldner sind keine Nachteile verbunden. Dieses Verfahren ist daher ausreichend sicher.

9.4 E-Kommunikation nach § 4 InsO und E-Mitteilungen

Bei der elektronischen Kommunikation, die die Insolvenzordnung durch den Verweis des § 4 InsO auf die Vorschriften in der Zivilprozessordnung ermöglicht, kann auf die Ausführungen von oben verwiesen werden.[1186] Dies bedeutet, dass elektronische Dokumente nach § 4 InsO i.V.m. § 130a ZPO verschlüsselt an das Gericht versendet werden müssen und – soweit es sich um bestimmende Schriftsätze handelt – mittels einer qualifizierten elektronischen Signatur versehen sein müssen.[1187] Die Vornahme der elektronischen Zustellung nach § 4 InsO i.V.m. 174 Abs. 3 ZPO[1188] sowie die Vornahme der elektronischen Akteneinsicht nach Maßgabe des § 4 InsO i.V.m. § 299 Abs. 3 ZPO[1189] setzt eine vorherige zuverlässige Registrierung voraus. Für die dargestellten Anforderungen bieten sich wiederum der Einsatz von Bürgerportalen i.V.m. mit dem Projekt S.A.F.E. sowie der elektronische Personalausweis an.

[1180] Vgl. hierzu Abschnitt 7.1.2.

[1181] Anderer Ansicht ist *Riebeling*, 2005, 24. Er hält die einfache Signatur für ausreichend, da dem Gläubiger im Unterschied zu anderen bei Gericht einzureichenden Schriftsätze bei einer verspäteten Forderungsanmeldung allein Kostennachteile entstehen würden.

[1182] So auch *Riebeling*, 2005, 25.

[1183] *Riebeling*, 2005, 26.

[1184] *Riebeling*, 2005, 27.

[1185] *Riebeling*, 2005, 27.

[1186] Vgl. hierzu Abschnitt 7.1 bis 7.4.

[1187] Für weitere spezifische Fragen im Zusammenhang mit der Verweisung von § 4 InsO auf § 130a ZPO, die keinen datenschutzrechtlichen Bezug haben, wird auf *Riebeling*, 2005, 6 ff. verwiesen.

[1188] Für weitere spezifische Fragen im Zusammenhang mit der Verweisung von § 4 InsO auf § 174 Abs. 3 ZPO, die keinen datenschutzrechtlichen Bezug haben, wird auf *Riebeling*, 2005, 27 ff. verwiesen.

[1189] Für weitere spezifische Fragen im Zusammenhang mit der Verweisung von § 4 InsO auf § 299 ZPO, die keinen datenschutzrechtlichen Bezug haben, wird auf *Riebeling*, 2005, 34 ff. verwiesen.

9.5 Zusammenfassung

Die Bekanntmachungen von Insolvenzdaten sind nicht verfassungswidrig. Das Insolvenzverfahren ist ein Massenverfahren, bei denen der Kreis der Betroffenen groß ist und sich nicht immer überschauen lässt. Mit der Eröffnung des Insolvenzverfahrens gehen verschiedene Rechtswirkungen einher. Da sich diese für Gläubiger nachteilig auswirken, muss eine möglichst große Publizität erreicht werden. Von daher dienen die Bekanntmachungen einem legitimen Zweck und sind erforderlich. Im Vergleich zu den herkömmlichen Bekanntmachungen stellt die Internetbekanntmachung einen intensiveren Grundrechtseingriff dar. Zum Schutz des Schuldners hat der Gesetzgeber in § 9 Abs. 2 InsO jedoch verschiedene Vorkehrungen getroffen, aufgrund derer dem Schuldner der Grundrechtseingriff zumutbar ist. Dennoch besteht Nachbesserungsbedarf. So ist es zum einen erforderlich, auf eine uneingeschränkte Suche während der ersten zwei Wochen der Veröffentlichung zu verzichten. Zudem sollte in der Insolvenzordnung genau festgeschrieben werden, welche personenbezogenen Daten veröffentlicht werden dürfen. Die sechsmonatige Löschfrist in der Insolvenzbekanntmachungsverordnung ist überdies zu lange. Im Interesse von natürlichen Personen, die eine Restschuldbefreiung erlangt haben, muss gewährleistet sein, dass ihr wirtschaftlicher Neuanfang nicht durch die fortlaufende Publizität von Veröffentlichungen aus dem Insolvenzverfahren gestört wird. Auch war es ein Fehler, dass der Gesetzgeber die Regelungen zum Kopierschutz gestrichen hat. Bei den elektronischen Tabellen und Verzeichnisse ergeben sich keine spezifischen Datenschutzprobleme. Was die elektronische Forderungsanmeldung betrifft, so ist hier der Einsatz einer qualifizierten elektronischen Signatur erforderlich. Bei der elektronischen Kommunikation nach § 4 InsO und den elektronischen formlosen Mitteilungen kann auf das verwiesen werden, was zum Zivilverfahren gesagt wurde.

Kapitel 10

Grundbuchordnung

Für den Modernisierungsprozess im Grundbuchwesen ist zunächst das elektronische Grundbuch von Bedeutung. Die Untersuchung beginnt daher mit dem elektronischen Grundbuch. Im Jahr 2009 wurden die Rechtsgrundlagen für die Einführung der elektronischen Grundakte geschaffen und es wurde ermöglicht, dass Gerichte und Verfahrensbeteiligte im Grundbuchwesen miteinander elektronisch kommunizieren können. Vor diesem Hintergrund beschäftigt sich dieses Kapitel nach dem elektronischen Grundbuch mit der elektronischen Grundakte und mit der elektronischen Übermittlung von Schriftsätzen im Grundbuchwesen. Zuletzt wird auf die Problematik des Eigentümerverzeichnisses eingegangen.

10.1 E-Grundbuch

Das Grundbuch gibt Auskunft über den Grundstücksbestand, die Eigentumsverhältnisse, die dinglichen Belastungen, die Verfügungsbeschränkungen und die Rangverhältnisse.[1190] Es besteht aus dem Bestandsverzeichnis und den Abteilungen I-III. Das Bestandsverzeichnis weist Grundstücks- und Katasternummer, Gemarkung, Parzellennummer, Größe, Lage und Wirtschaftsart des Grundstücks aus. Abteilung I enthält Eintragungen über die Eigentumsverhältnisse am Grundstück, Abteilung II enthält dingliche Rechte wie beispielsweise Nießbrauch oder Wegerechte und Abteilung III enthält Grundpfandrechte, insbesondere Hypotheken und Grundschulden. Als Grundbuch versteht man nach § 3 Abs. 1 Satz 2 GBO das jeweilige ganze Blatt für ein Grundstück, das aus dem Bestandsverzeichnis und den drei Abteilungen besteht.[1191] § 12 Abs. 1 GBO bestimmt, dass die Einsicht in das Grundbuch nur jemandem gestattet ist, der ein berechtigtes Interesse darlegt. Darlegen ist weniger als Glaubhaftmachen, jedoch mehr als Behaupten.[1192] Darlegen kann damit als das Vorbringen von Tatsachen in der Weise bezeichnet werden, dass das Grundbuchamt von der Verfolgung berechtigter In-

[1190] *Liebscher*, 1994, 162.
[1191] *Liebscher*, 1994, 163.
[1192] *Kuntze* et al., GBO, § 12 Rn. 4.

teressen überzeugt ist.[1193] Ist das Grundbuchamt nicht überzeugt, kann es im Einzelfall bei begründeten Bedenken auch die Glaubhaftmachung oder den Nachweis des Interesses verlangen.[1194] Mit der Regelung des § 12 GBO hat der Gesetzgeber einen Mittelweg zwischen der strengen Vorschrift des § 299 Abs. 2 ZPO, die ein rechtliches Interesse verlangt, und dem Handelsregister, das gemäß § 9 HGB jedermann offen steht, gesucht.[1195] Wie sich §§ 53 Abs. 4 und 69 Abs. 2 BauGB ergibt, hat der deutsche Gesetzgeber die Regeln der Grundbucheinsicht auch in anderen Bereichen des Bodenverkehrs und der Bodenneuordnung als beispielhaft angesehen. Der Gesetzgeber hat sich damit nicht für ein „gläsernes Grundbuch“ entschieden, wie dies etwa in anderen westeuropäischen Staaten der Fall ist.[1196]

Bei der Auslegung des berechtigten Interesses in § 12 GBO ist das informationelle Selbstbestimmungsrecht zu berücksichtigen. Dabei ist unstreitig, dass der Begriff des berechtigten Interesses umfassender ist als der des rechtlichen Interesses. Hierfür ist es ausreichend, dass der Antragsteller ein verständiges, durch die Sachlage gerechtfertigtes Interesse verfolgt.[1197] Es genügt, dass sachliche Gründe vorgetragen werden, welche die Verfolgung unbefugter Zwecke oder Einsichtnahmen aus bloßer Neugier ausgeschlossenen erscheinen lassen.[1198] Auch wirtschaftliche Interessen können genügen. So kann etwa auch der Gläubiger, der die Zwangsvollstreckung des Grundbesitzes seines Schuldners beabsichtigt, das Grundbuch einsehen;[1199] auch kann der Mieter in das Grundbuch seines Vermieters einsehen.[1200] Kein berechtigtes Interesse haben aber etwa der Kaufinteressent, der durch die Grundbucheinsicht erst den Namen des Grundstückseigentümers erfahren will[1201] oder Auskunfteien oder Immobilienmakler.[1202] Das Oberlandesgericht Karlsruhe hatte des Weiteren sogar einer Tochter, die erfahren wollte, ob das Grundstück ihrer demnächst pflegebedürftigen Mutter zur Verwertung noch zur Verfügung steht, eine Einsichtnahme versagt.[1203]

Inwieweit die Presse ein Einsichtsrecht hat, ist umstritten. Während die Rechtsprechung[1204] ein derartiges Einsichtsrecht dann gestattet, wenn die presserechtlichen Voraussetzungen eines Auskunftsanspruches dargelegt sind und eine Interessenabwägung ergibt, dass das öffentliche Informationsinteresse das private Geheimhaltungsinteresse des Betroffenen überwiegt, wird in der Literatur ein derartiges Einsichtsrecht verneint. Eickmann[1205] etwa betont, dass das Grundbuch keine allgemeine Auskunfts- und Informationseinrichtung ist. Nur wer in Bezug

[1193] *Demharter*, GBO, § 12 Rn. 12.
[1194] *Demharter*, GBO, § 12 Rn. 12.
[1195] *Liebscher*, 1994, 163.
[1196] *Grziwotz*, MittBayNot 1995, 100.
[1197] OLG Stuttgart, Rpfleger 1983, 272; OLG Hamm, Rpfleger 1986, 128.
[1198] OLG Stuttgart RPfleger 1983, 272, OLG Hamm Rpfleger 1986, 128.
[1199] OLG Zweibrücken, NJW 1989, 531.
[1200] OLG Hamm, Rpfleger 1986, 128; LG Mannheim, Rpfleger 1992, 246; BayOblG, NJW-RR 1993, 1142.
[1201] Dieser hat erst ein Recht auf Einsichtnahme nach Eintritt in die Verkaufsverhandlungen mit dem Eigentümer. Vgl. hierzu BayOblG Rpfleger 1984, 351.
[1202] *Demharter*, GBO, § 12 Rn. 12.
[1203] OLG Karlsruhe, FamRZ 2009, 1773. Siehe hierzu auch die Anmerkung von *Böhringer*, ZEV 2009, 43.
[1204] BVerfG, Rpfleger 2001, 15; OLG Hamm, Rpfleger 1988, 473; LG Mosbach, Rpfleger 1990, 60; KG Berlin, Rpfleger 2001, 539.
[1205] *Kuntze* et al., GBO, § 12 Rn. 3 und 6.

auf das im Buch Verlautbarte rechtlich zu handeln beabsichtigt, bedürfe der Einsicht und habe ein Recht auf sie.

Wenn das Grundbuch elektronisch geführt wird, so kann es gemäß § 79 GBV entweder durch Wiedergabe auf einem Bildschirm oder durch die Erteilung eines Aktenausdrucks eingesehen werden. Zudem besteht nach § 133 GBO die Möglichkeit eines automatisierten Abrufverfahrens. Hierfür ist eine vorherige Genehmigung erforderlich.

Für die Zulassung müssen folgende Voraussetzungen erfüllt sein:

- Die Datenübermittlung muss unter Berücksichtigung der schutzwürdigen Interessen und der betroffenen dinglich Berechtigten wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen sein.
- Auf Seiten des Empfängers müssen die Grundsätze einer ordnungsgemäßen Datenverarbeitung eingehalten werden.
- Auf Seiten der grundbuchführenden Stelle müssen die technischen Möglichkeiten der Einrichtung und Abwicklung des Verfahrens gegeben sein und eine Störung des Geschäftsbetriebes des Grundbuchsamtes darf nicht zu erwarten sein.

Für das uneingeschränkte Abrufverfahren[1206] können Gerichte, Behörden, Notare und öffentlich bestellte Vermessungsingenieure zugelassen werden.[1207] Diese können die Einsicht in vollem Umfang ausüben. Dies bedeutet, dass sie jedes Grundbuchblatt einsehen können und zwar gemäß § 133 Abs. 7 Satz 1 GBO im gesamten Bundesland.[1208] Sobald die technischen Voraussetzungen dafür gegeben sind, ist auch ein bundesweiter Abruf möglich.[1209]

Beim eingeschränkten Abrufverfahren muss das Vorliegen eines Grundes für den Abruf angegeben werden. Es sind nur die folgenden Gründe zugelassen:

- Der Abrufende ist dinglich Berechtigter am Grundstück oder er ist vom dinglich Berechtigten beauftragt.
- Die Zustimmung des Eigentümers liegt vor.
- Es sollen Maßnahmen der Zwangsvollstreckung betrieben werden.
- Die abrufende Stelle ist ein Versorgungsunternehmen.

[1206] Der Begriff des uneingeschränkten Abrufverfahrens wird an keiner Stelle verwendet. Er folgt vielmehr im Umkehrschluss aus § 82 Abs. 2 GBV, der vom eingeschränkten Abrufverfahren spricht.

[1207] Dieser Personenkreis ist nach § 43 GBV auch von der Darlegung eines berechtigten Interesses befreit.

[1208] Wer also zum Abrufverfahren bei einem Grundbuchamt zugelassen ist, ist bei allen anderen Grundbuchämtern desselben Landes, bei denen die Voraussetzungen des § 133 Abs. 1, 2 Satz 3 Nr. 1, 2 GBO vorliegen, zugelassen.

[1209] Das BMJ stellt das Vorliegen dieser Voraussetzungen durch Rechtsverordnung fest, vgl. § 133 Abs. 7 Satz 3 GBO. Eine entsprechende Rechtsverordnung wurde noch nicht erlassen.

Auch die Berechtigten im eingeschränkten Abrufverfahren können das einzelne Grundbuch, mithin jedes Grundbuchblatt unbeschränkt einsehen. Die Kontrolle, ob beim Einsichtnehmer das berechtigte Interesse vorgelegen hat, erfolgt mit Hilfe einer Protokollierung der Abrufe. Das Grundbuchamt protokolliert gemäß § 83 Abs. 1 GBV alle Abrufe, sowohl im eingeschränkten wie auch im uneingeschränkten Abrufverfahren. Bei den zu erfassenden Daten handelt es sich um das Grundbuchamt, das Grundbuchblatt, den Abrufer und sein Geschäfts- und Aktenzeichen und überdies – im eingeschränkten Abrufverfahren – die kodierte Darlegungserklärung.

Die Protokolle werden vom Grundbuchamt für Stichprobenverfahren der aufsichtsführenden Stellen bereitgehalten. Auf der Grundlage der Protokolldaten kann der Eigentümer des jeweils betroffenen Grundstücks gemäß § 133 Abs. 5 Satz 2 GBO Auskunft darüber verlangen, wer Daten abgerufen hat; beim eingeschränktem Abruf kann er auch Auskunft über die Art des Abrufs verlangen. Für das automatisierte Abrufverfahren werden gemäß der Justizverwaltungskostenordnung Gebühren erhoben.

10.1.1 Verfassungsmäßigkeit

Das Einsichtsrecht kann die Geheimhaltungsinteressen des Eigentümers gefährden.[1210] So sind in den Grundbuchauszügen regelmäßig Angaben zu Name, Beruf, Geburtsdatum und Eigentumsanteil und Darlehensbelastungen aller Eigentümer enthalten.[1211] Gleichwohl unterliegt § 12 GBO keinen verfassungsrechtlichen Bedenken.[1212] Nach dem BGB hat das Grundbuch drei Funktionen: Die Übertragungswirkung ist das Erfordernis, dass die rechtsgeschäftliche Änderungen in den Verhältnissen an einem Grundstück eingetragen werden müssen (§§ 873, 875 BGB).[1213] Unter der Vermutungsfunktion versteht man die Annahme, dass derjenige der eingetragen ist, auch der Berechtigte ist (§ 891 BGB).[1214] Die dritte Funktion ist die Gutglaubensfunktion. Diese ermöglicht den Rechtserwerb von den im Grundbuch Eingetragenen, selbst wenn dieser nicht berechtigt ist.[1215] Diese Funktionen des Grundbuchs können nur erfüllt werden, wenn der Inhalt des Grundstücks dem Rechtsverkehr auch zugänglich ist. Die Zielrichtung des Rechts der Grundbucheinsicht geht also auf Publizität und nicht auf irgendeinen Geheimnisschutz. Dementsprechend gingen auch die Gesetzesmotive zur Grundbuchordnung davon aus, dass die materiell-rechtlichen Vermutungs- und Gutglaubensvorschriften des BGB (§§ 891 ff. BGB) „die Nothwendigkeit einer gewissen Oeffentlichkeit des Grundbuchs bedingen würden“.[1216] Vor diesem Hintergrund muss bei der Grundbucheinsicht nicht die gleiche Prüfung angestrengt werden wie beim Schuldnerverzeichnis, dem Vermögensverzeichnis und den öffentlichen Bekanntmachungen.

[1210] *Liebscher*, 1994, 163.
[1211] *Liebscher*, 1994, 164.
[1212] BVerfG, Rpfleger 2001, 15.
[1213] *Liebscher*, 1994, 163.
[1214] *Liebscher*, 1994, 163.
[1215] *Liebscher*, 1994, 163.
[1216] *Grziwotz*, MittBayNot 1995, 101.

10.1.2 Aktenausdruck und Wiedergabe auf einem Bildschirm

Die Erteilung eines Aktenausdrucks unterliegt keinen Bedenken. Der Ausdruck nach § 131 GBO kann dem Antragsteller zur Einsicht überlassen oder ihm ausgehändigt werden. Bei der Wiedergabe auf einem Bildschirm ist aus datenschutzrechtlicher Sicht zu verlangen, dass zumindest eine zuständige Person des Grundbuchamtes anwesend ist und das Grundbuchblatt aufruft. Dem wird grundsätzlich Rechnung getragen. § 79 Abs. 1 Satz 2 GBO enthält jedoch eine Ausnahme für den Fall, dass sichergestellt ist, dass nur das betreffende Grundbuchblatt eingesehen und der Inhalt nicht verändert werden kann. In diesem Fall gestattet § 79 Abs. 1 Satz 2 GBV darüber hinaus auch dem Antragsteller die Grundbucheinsicht ohne Beisein des zuständigen Grundbuchbeamten. Dies ist grundsätzlich nicht zu beanstanden. Allerdings muss sichergestellt werden, dass der Antragsteller bei dieser Form der Einsicht nicht von anderen in den Diensträumen herumliegenden Unterlagen Kenntnis nehmen kann.

Grundsätzlich ist das Grundbuch in den Diensträumen des Grundbuchamtes einzusehen. Wenn das Grundbuch jedoch elektronisch geführt wird, so gestattet § 132 GBO, dass dieses auch bei einem anderen als dem grundbuchführenden Grundbuchamt eingesehen werden kann. In diesem Fall ist es jedoch erforderlich, dass nur wenige Bedienstete Zugriff auf die Daten haben. Eine Regelung mit diesem Inhalt findet sich in § 79 Abs. 3 Satz 2 und 3 GBV. Danach müssen die hierfür zuständigen Bediensteten besonders bestimmt werden und sie müssen eine elektronische Kennung verwenden. Diese Regelung ist als positiv zu beurteilen. Mit der elektronischen Kennung wird verhindert, dass unbefugte Mitarbeiter Kenntnis erlangen.

Bei der Erteilung des Aktenausdrucks und der Wiedergabe auf einem Bildschirm fällt auf, dass diese Formen der Einsichtnahmen in das Grundbuch nicht dokumentiert werden. Eine Dokumentation ist nur für die Einsichtnahme im automatisierten Verfahren vorgesehen. Eine Dokumentation bei der Erteilung eines Aktenausdrucks und der Wiedergabe auf einem Bildschirm wäre jedoch erforderlich, um im Interesse der Betroffenen im Einzelfall feststellen zu können, wer personenbezogene Informationen über ihn erhalten hat und um unberechtigten Einsichtnahmen entgegenzuwirken.[1217] Nur durch eine Dokumentation kann der Betroffene seinen Auskunftsanspruch nach § 18 Abs. 3 LDSG wahrnehmen. Dabei ist auch zu berücksichtigen, dass der Eigentümer vor der Übermittlung der Grundstücksdaten an Dritte nicht angehört wird und ihm gegen die positive Entscheidung des Urkundsbeamten kein Be-

[1217] So etwa auch der Vorschlag des *LfD Bayern*, 16. Tätigkeitsbericht, 7.2.4

schwerderecht zusteht.[1218] Umso mehr ist es daher erforderlich, dass der Betroffene nachträglich erfahren kann, wem seine Daten vom Grundbuchamt mitgeteilt wurden.

10.1.3 Online-Auskunft

Im Vergleich zu einer Einsicht durch Aktenausdruck und Wiedergabe auf einem Bildschirm ist das automatisierte Abrufverfahren mit einer stärkeren Gefährdung für das informationelle Selbstbestimmungsrecht des Eigentümers verbunden. Allerdings benötigen die in § 133 Abs. 2 Satz 2 GBO genannten Stellen, insbesondere die Notare und Gerichte, die Angaben aus dem Grundbuch für ihre tägliche Arbeit. Sie sind auf eine zügige Übermittlung angewiesen. Für die Abfrage von Grundbuchdaten müssen diese Stellen eine besondere Genehmigung vorweisen, die nach den Vorgaben des § 133 Abs. 2 Satz 3 GBO an enge Voraussetzungen geknüpft ist. Mit der Genehmigung der Zulassung erhält der Abrufer ein Codezeichen, das ihn identifiziert. Dem Abrufer wird gemäß § 82 GBV zur Auflage gemacht, das Codezeichen sicher gegen Missbrauch zu verwahren. § 133 Abs. 6 GBO bestimmt weiter, dass der Empfänger die personenbezogenen Daten aus dem automatisierten Abrufverfahren nur für den Zweck verwenden kann, zu dessen Erfüllung sie ihm übermittelt worden sind. Zudem werden nach § 133 Abs. 1 Nr. 2 GBO und § 83 GBV alle Abrufe protokolliert und § 133 Abs. 5 Satz 2 GBO gibt dem Betroffenen einen umfassenden Auskunftsanspruch. Nur wenn durch die Bekanntgabe der Erfolg strafrechtlicher Ermittlungen gefährdet würde, kann der Auskunftsanspruch beschränkt werden. Vom Grundsatz her bestehen daher gegen das uneingeschränkte Abrufverfahren keine Bedenken.

Dies gilt ebenso für das eingeschränkte Abrufverfahren. Auch das eingeschränkte Abrufverfahren setzt nach § 133 Abs. 4 Satz 2 GBO eine besondere Genehmigung voraus. Zudem muss das Vorliegen eines der abschließend in § 133 Abs. 4 Satz 3 GBO genannten Gründe für einen Abruf dargelegt werden. Die Kontrolle erfolgt ebenfalls durch eine Protokollierung, insbesondere auch der codierten Darlegungserklärung. Über die in § 83 GBV genannten Vorgaben hinaus muss der eingeschränkte Abruf gemäß § 82 Abs. 2 Satz 1 GBV an die Verwendung eines weiteren Codezeichens geknüpft werden, das die Art des Abrufs bezeichnet. Auch beim eingeschränkten Abrufverfahren kann der Betroffene den Auskunftsanspruch nach § 133 Abs. 5 Satz 2 GBO wahrnehmen und der Datenempfänger darf nach Maßgabe des § 133 Abs. 6 GBO die abgerufenen Daten nicht zweckwidrig verwenden.

[1218] So die herrschende Meinung. Vgl. hierzu BGH, DNotZ 1982, 240; OLG Stuttgart, BWNotZ 1957, 197; OLG Stuttgart, Rpfleger 1992, 247; *Demharter*, GBO, § 12 Rn. 32. Sie begründet dies damit, dass sich bei der Prüfung des Einsichtsrechts nur das Grundbuchamt und der Antragsteller gegenüberstehen, der Eigentümer dagegen nicht beteiligt sei und diesem auch kein Anspruch auf Geheimhaltung zustünde. Die gegenteilige Auffassung hält ein Anfechtungsrecht solange für möglich, wie die Einsicht noch nicht vollzogen ist. So habe der Eigentümer häufig ein Interesse daran, seine sich im Grundbuch widerspiegelnden wirtschaftlichen Verhältnisse nicht der Allgemeinheit offenzulegen. Das Gesetz stelle auch ausdrücklich auf einen gerichtlich nachprüfbaren Rechtsbegriff ab und nicht auf das Ermessen des Gerichts. Vgl. hierzu BayOblG, Rpfleger 1975, 361; *Kuntze* et al., GBO, § 12 Rn. 12.

Gegen die grundsätzliche Unbedenklichkeit des Abrufverfahrens sprechen im Übrigen auch nicht die durch das ERVGBG[1219] erfolgten Gebührenermäßigungen bei den Abrufen.[1220] Die jeweils zuständige Stelle hat die beschriebenen Voraussetzungen für eine Genehmigung sorgfältig zu prüfen. Sofern sie dies tut, wird nicht damit zu rechnen sein, dass die Zahl von missbräuchlichen Abrufen allein durch die Gebührenermäßigungen steigen wird.

Obwohl gegen die grundsätzliche Ausgestaltung des Abrufverfahrens keine Bedenken bestehen, ist es jedoch zu kritisieren, dass Notare – im Falle des Erlasses einer entsprechenden Rechtsverordnung – gemäß § 133 Abs. 7 Satz 2 GBO die Daten aus dem Grundbuch bundesweit abrufen können. Nach § 10a Abs. 2 BNotO soll der Notar seine Urkundstätigkeit nur innerhalb seines Amtsbereichs ausüben. Nur wenn besonders berechtigte Interessen der Rechtssuchenden ein Tätigwerden außerhalb des Amtsbereichs gebieten, gestattet § 10a Abs. 2 BNotO eine Ausnahme. Urkundstätigkeiten außerhalb des Amtsbereichs hat der Notar der Aufsichtsbehörde oder nach deren Bestimmung der Notarkammer, der er angehört, nach § 10a Abs. 3 BNotO unverzüglich und unter Angabe der Gründe mitzuteilen. Vor diesem Hintergrund benötigt der Notar zur Erfüllung seiner Aufgaben nur in Ausnahmefällen Daten von anderen Amtsgerichtsbezirken. Das gleiche gilt auch für die Gemeinden. Gemäß § 2 GemO sind die Gemeinden in ihrem Gebiet Träger der gesamten Verwaltung. Sie nehmen also lediglich örtliche Aufgaben wahr. Vor diesem Hintergrund ist es nicht sachgerecht, Gemeinden einen bundesweiten Zugriff auf die Daten des elektronischen Grundbuchs zu gewähren.

10.1.4 Dauerhafte Verfügbarkeit und Integrität

Nach § 10 Abs. 1 Satz 1 GBO sind Grundbücher dauernd aufzubewahren. Eigentlich ergibt sich dies bereits aus dem Gesamtzusammenhang der Regelungen zur Grundbuch- und Grundaktenführung und aus den Aufbewahrungsbestimmungen der Landesjustizverwaltungen.[1221] Da der Gesetzgeber mit dem ERVGBG jedoch Ausnahmen von der Verpflichtung zur dau-

[1219] BGBl. 2009 I, 2713.

[1220] Die Einrichtungsgebühr für Notare betrug früher 500 EUR, ferner wurde eine Grundgebühr von 50 EUR für jeden vollen Kalendermonat erhoben, in dem das Abrufverfahren eingerichtet ist. Die Abrufgebühren betrugen bei jedem Abruf von Daten aus einem Grundbuchblatt 5 EUR, bei dem Abruf von Daten aus Verzeichnissen nach § 12a der Grundbuchordnung 2,50 EUR für jeden einzelnen Suchvorgang. Rief ein Teilnehmer in einer Angelegenheit innerhalb von sechs Monaten mehrmals Daten aus demselben Grundbuchblatt ab, so hat sich die Abrufgebühr für Folgeabrufe auf jeweils 2,50 EUR ermäßigt. Die Gebühren waren früher in § 133 Abs. 8 GBO i.V.m. § 85 GBV und § 1 GBAbVfG geregelt. Mit dem Inkrafttreten des ERVGBG wurden die genannten Vorschriften aufgehoben. Maßgeblich ist nunmehr die Anlage zu § 2 der JVKostO. Danach ist keine Gebühr mehr in Höhe von 500 EUR für die Einrichtung des uneingeschränkten Abrufverfahrens mehr zu zahlen. Lediglich für die Einrichtung des eingeschränkten Abrufverfahrens sieht die Anlage eine einmalige Gebühr von 50 EUR vor. Zudem ist die monatliche Grundgebühr abgeschafft und die Höhe der Gebühr für den Abruf von Grundbuch- und Registerdaten wurde auf einheitlich 8 EUR und für den Abruf von Dokumenten auf 1,50 EUR festgelegt. Der Gesetzgeber wollte damit das Abrufverfahren – insbesondere für Anwaltsnotare – attraktiver gestalten. Vgl. hierzu BT-Drs. 16/12319, 2.

[1221] BT-Drs. 16/12319, 19.

ernden Aufbewahrung der Originalgrundbücher gemacht hat, hielt er es für geboten, diesen Grundsatz ausdrücklich in die Grundbuchordnung aufzunehmen.[1222] Wie bereits gesehen,[1223] werden die Grundbücher in nunmehr fast allen Bundesländern elektronisch geführt. Vor diesem Hintergrund können sich die genannten Probleme hinsichtlich der Integrität und dauerhaften Verfügbarkeit der Daten ergeben. Aufgrund der Bedeutung des Grundbuchs ist die Sicherstellung der Integrität und Verfügbarkeit besonders wichtig. Mit Hilfe der vorgestellten Langzeitarchivierung nach § 17 SigV, den Vorgaben des ArchiSig-Verfahrens sowie mit Hilfe des TransiDoc-Modells lassen sich diese jedoch lösen.[1224]

10.2 E-Grundakte

Aus den Schriften zu dem einzelnen Grundbuchblatt wird die Grundakte gebildet.[1225] In den Grundakten sind die im Zusammenhang mit dem Grundbuch stehenden Urkunden und Vorgänge enthalten. Dazu gehören auch die bisher noch nicht erledigten Eintragungsanträge. Die in den Grundakten befindlichen notariellen Urkunden enthalten vielfach sehr sensible Daten. Die Einsichtnahme in die Grundakten kann daher das Geheimhaltungsinteresse des Grundstückseigentümers gefährden. So befinden sich in den Grundakten Hinweise auf persönliche, wirtschaftliche und finanzielle Verhältnisse von Beteiligten,[1226] z.B. Finanzierungsregelungen in Kaufverträgen, Gesellschafts- und Eheverträgen. § 12 Abs. 1 Satz 2 GBO bestimmt, dass diejenigen Urkunden, auf die im Grundbuch zur Ergänzung einer Eintragung Bezug genommen wird sowie die noch nicht erledigten Eintragungsanträge im Falle der Darlegung eines berechtigten Interesses eingesehen werden können. Darüber hinaus gestattet § 46 Abs. 1 GBV bei Vorliegen eines berechtigten Interesses Einblick in die Grundakten, auch soweit es sich nicht um die in § 12 Abs. 1 Satz 2 GBO genannten Urkunden handelt. Auf Verlangen hat das Grundbuchamt nach § 46 Abs. 3 GBV neben Abschriften der Grundakte auch solche von Urkunden zu erteilen, auf die sich das Einsichtsrecht erstreckt. Wie oben dargestellt, können die Grundakten gemäß § 135 Abs. 2 GBO nunmehr elektronisch geführt werden. In diesem Zusammenhang sind vor allem die neuen Vorgaben zur Einsicht in die Grundakte von Interesse. § 139 Abs. 1 und 2 GBO enthalten diesbezüglich Regelungen zum Aktenausdruck und zur Akteneinsicht und Abs. 3 ermöglicht – ebenso wie beim Grundbuch – ein automatisiertes Abrufverfahren nach den bereits beschriebenen Vorgaben des § 133 GBO.

10.2.1 Aktenausdruck und Akteneinsicht

§ 139 Abs. 1 GBO ist § 131 GBO nachgebildet und – genauso wie diese Vorschrift – als datenschutzrechtlich unkritisch zu beurteilen. Ebenfalls als unkritisch anzusehen ist die Vorschrift

[1222] BT-Drs. 16/12319, 19.
[1223] Vgl. hierzu Abschnitt 2.3.4.1.
[1224] Vgl. hierzu Abschnitt 7.6.1 und 7.6.2.
[1225] *Liebscher*, 1994, 172.
[1226] *Liebscher*, 1994, 172.

des § 139 Abs. 2 GBO. Diese Norm entspricht § 132 GBO. Der Datenbestand kann nunmehr vom zuständigen Bediensteten des Grundbuchamtes aufgerufen und die Einsicht kann über einen Bildschirm gewährt werden.[1227] Zudem kann die Einsicht in die elektronischen Grundakten auch bei einem anderen Grundbuchamt gewährt werden, das diese Grundakten führt. Dadurch sollen den Bürgern längere Anfahrtswege erspart werden.[1228] Über die Gestattung der Einsicht entscheidet in diesem Fall das Grundbuchamt, bei dem die Einsicht begehrt werden kann. Nach § 99 Abs. 2 GBV gilt die Vorschrift des § 79 GBO entsprechend. Die Ausführungen von oben gelten daher auch hier. Auch bei der Gestattung der elektronischen Grundakte wäre es jedoch wünschenswert, dass dokumentiert wird, wer die Daten wann eingesehen hat.

10.2.2 Online-Einsicht

In der amtlichen Begründung zu § 139 Abs. 3 GBO findet sich kein Hinweis für die Notwendigkeit eines automatisierten Abrufverfahrens für Daten aus der Grundakte. Die Begründung zu § 139 Abs. 3 GBO verweist lediglich auf die Vorschrift des § 133 GBO, die sich in der Vergangenheit im Verfahren über den Abruf von Grundbuchdaten bewährt hätte.[1229] Bei der Einsichtnahme des Grundbuchs ist aber anerkannt, dass dieses das gesamte Grundbuchblatt umfasst, also alle Abteilungen. Eine Beschränkung auf einzelne Abteilungen widerspricht dem eindeutigen Wortlaut des § 12 GBO.[1230] Bei der Einsichtnahme in die Grundakten ist hingegen keine Gesamteinsicht möglich. Da die Grundakte vielfach Informationen über die persönlichen, wirtschaftlichen und finanziellen Verhältnisse einer bestimmten Person enthält, ist hier anerkannt, dass eine Einsicht nur soweit zu gewähren ist, wie das berechtigte Interesse wirklich reicht.[1231] Angesichts dieser Unterschiede bei der Einsicht von Grundbuch und Grundakte hätte der Gesetzgeber hier die Erforderlichkeit der Abrufe von Grundaktendaten näher darlegen müssen. Vor diesem Hintergrund sollten die Landesjustizverwaltungen in Zukunft hohe Anforderungen an die Erteilung einer Genehmigung nach § 139 Abs. 3 i.V.m. § 133 GBO stellen und die Voraussetzungen hierfür sorgfältig nachprüfen. Da eine Gesamteinsicht der Grundakte nicht zulässig ist, sollte zudem bestimmt werden, dass sowohl beim eingeschränkten wie auch beim uneingeschränkten Abrufverfahren auch die Art der Datenabrufe kontrolliert wird, um so missbräuchlichen Abrufen entgegenwirken zu können.[1232]

10.2.3 Dauerhafte Verfügbarkeit und Integrität

Nach § 10 Abs. 1 Satz 1 GBO ist nicht nur das Grundbuch dauernd aufzubewahren, sondern auch die Grundakte. Für die dauernd aufzubewahrenden Grundakten besteht das Problem der mangelnden Beständigkeit von Datenformaten. Wiederum lässt sich dieses mit Hilfe der

[1227] BT-Drs. 16/12319, 32.
[1228] BT-Drs. 16/12319, 32.
[1229] BT-Drs. 16/12319, 32.
[1230] *Liebscher*, 1994, 171.
[1231] OLG Zweibrücken, NJW 1989, 531; *Böhringer*, Rpfleger 1987, 185; *Böhringer*, Rpfleger 1989, 311.
[1232] Bisher ist dies nur beim eingeschränkten Abrufverfahren der Fall, vgl. § 83 Abs. 2 Satz 2 GBV.

vorgestellten Langzeitarchivierung nach § 17 SigV, des ArchiSig-Verfahrens und des TransiDoc-Modells lösen.[1233]

10.3 E-Übermittlung von Schriftsätzen

§ 135 Abs. 1 Nr. 2 GBO sieht vor, dass in einer Rechtsverordnung bestimmt werden soll, dass Einzelheiten der Datenübermittlung und -speicherung zu regeln sind. Nr. 4a sieht vor, dass Notare Dokumente elektronisch zu übermitteln haben. Für Notare ergibt sich eine Verpflichtung zur Verschlüsselung der elektronischen Dokumente bereits aus § 18 BNotO. Nach § 18 BNotO ist der Notar zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm bei Ausübung seines Amtes bekannt geworden ist. Für andere Personen ergibt sich eine entsprechende Verpflichtung aus § 9 BDSG. Auch hier würde wiederum die Einrichtung eines Bürgerportals oder das Projekt S.A.F.E. einen Gewinn bringen. Ebenso wie § 174 Abs. 3 ZPO bestimmt § 140 Abs. 2 GBO nunmehr, dass Entscheidungen, Verfügungen und Mitteilungen durch die Übermittlung elektronischer Dokumente bekanntgegeben werden können. Der Personenkreis ist dabei der gleiche wie bei § 174 Abs. 1 ZPO. Ansonsten ist die Übermittlung elektronischer Dokumente zulässig, wenn der Empfänger dem ausdrücklich zugestimmt hat. Die Dokumente sind weiter gegen unbefugte Kenntnisnahme zu schützen. Bei der Übermittlung von Beschlüssen, die nicht bereits signiert sind, sind die Dokumente mit einer elektronischen Signatur zu versehen. Auch hier gilt das oben Gesagte,[1234] d.h. es ist erforderlich, dass der jeweilige Empfänger zuvor zuverlässig registriert wird und dass auch die Beschlüsse nicht nur mit einer einfachen, sondern mit einer qualifizierten elektronischen Signatur versehen werden.

10.4 E-Eigentümerverzeichnisse

Die Grundbuchämter führen zudem auch ein Eigentümerverzeichnis. Das Eigentümerverzeichnis führt in alphabetischer Reihenfolge alle Eigentümer mit dem entsprechenden Grundbuchblatt auf. Damit kann allein anhand des Verzeichnisses festgestellt werden, ob eine bestimmte Person Immobiliareigentum hat. Es wird geführt, um die schnelle Ermittlung der den einzelnen Personen gehörenden Grundstücke nach ihrer grundbuchmäßigen Bezeichnung zu erleichtern und damit die Tätigkeit der Behörde zu vereinfachen. Aufgrund seiner Ausrichtung als in erster Linie internes Verzeichnis steht es den Grundbuchämtern frei, ob sie es auch öffentlich

[1233] § 138 Abs. 2 GBO und § 97 GBV bestimmen diesbezüglich, dass der Inhalt der zur Grundakte genommenen elektronischen Dokumente in lesbarer Form zu erhalten ist. Hierzu können die Dokumente in ein anderes Format übertragen werden und in dieser Form anstelle der bisherigen Dateien in die Grundakte übernommen werden.

[1234] Vgl. hierzu Abschnitt 7.2.2 und 7.2.3.

zugänglich machen.[1235] Das Eigentümerverzeichnis ist nicht Bestandteil des Grundbuchs. Es ist daher nicht vom Einsichtsrecht nach § 12 GBO gedeckt. Vielmehr ergibt sich aus der speziellen Vorschrift des § 12a GBO, unter welchen Voraussetzungen Auskunft und Einsicht in das Verzeichnis erteilt werden darf.

Die Führung der Eigentümerverzeichnisse unterliegt unter dieser Prämisse grundsätzlich keinen datenschutzrechtlichen Bedenken. So ist es zunächst als positiv zu beurteilen, dass mit § 12a GBO eine gesetzliche Grundlage für die Führung dieser Verzeichnisse geschaffen wurde. Vor der Schaffung dieser Norm wurden sie nämlich lediglich auf der Grundlage der AktO geführt,[1236] was nach dem Volkszählungsurteil des Bundesverfassungsgerichts bedenklich war. Als positiv ist es auch zu beurteilen, dass in die Eigentümerverzeichnisse grundsätzlich nicht eingesehen werden kann und § 12a Abs. 1 Satz 3 GBO für die Auskunft detailliert beschriebene Anforderungen vorgibt. So muss das Verzeichnis zum einen öffentlich zugänglich sein. Zum anderen muss ein solches Verzeichnis der Auffindung der Grundbuchblätter dienen, zur Einsicht in das Grundbuch oder für den Antrag auf Erteilung von Abschriften erforderlich sein und die Voraussetzungen für die Einsicht in das Grundbuch müssen gegeben sein. Diese Auskunft, die grundsätzlich jedem zusteht, wird nicht elektronisch erteilt. Sie ist sinnvoll, da so vermieden werden kann, dass über das erforderliche Maß hinaus Einsicht in das Grundbuch selbst gewährt wird. Die Auskunft steht im pflichtgemäßen Ermessen des zuständigen Urkundsbeamten,[1237] welcher damit auch datenschutzrechtliche Gesichtspunkte prüfen kann. Sinnvoll ist auch die Vorschrift des § 12a Abs. 1 Satz 4 GBO, welche bestimmt, dass unabhängig davon – nämlich bei Vorliegen eines berechtigten Interesses – Auskunft auch dann gewährt werden kann, wenn dadurch eine Einsicht in das Grundbuch entbehrlich würde.[1238] Dadurch wird ebenfalls erreicht, dass auf eine Grundbucheinsicht unter Umständen verzichtet werden kann. Einsicht kann nach § 12a Abs. 1 Satz 5 GBO nur inländischen Gerichten, Behörden und Notaren erteilt werden. Diese Stellen können nach § 12a Abs. 7 i.V.m. § 133 GBO das Eigentümerverzeichnis auch im automatisierten Abrufverfahren einsehen. Im Hinblick auf die beim Grundbuch genannten Vorkehrungen, d.h. formelles Zulassungsverfahren sowie die Vergabe von Codewörtern und Protokollierung der Abrufe, erscheint ein automatisiertes Abrufverfahren unbedenklich.

10.5 Zusammenfassung

Mit der Regelung des § 12 GBO zur Einsichtnahme in das Grundbuch hat der Gesetzgeber einen Mittelweg zwischen der Vorschrift des § 299 Abs. 2 ZPO, die ein rechtliches Interesse an der Einsichtnahme verlangt, und der des § 9 HGB, nach welcher das Handelsregister voraussetzungslos eingesehen werden kann, gewählt. Das informationelle Selbstbestimmungsrecht ist bei der Auslegung der Frage des berechtigten Interesses in § 12 GBO zu berücksichtigen. Im

[1235] Letzteres ist aber nicht der Fall, wenn lediglich anderen Behörden der Zugang eröffnet wird. Vgl. hierzu *Demharter*, GBO, § 12a Rn. 5.
[1236] *Demharter*, GBO, § 12a Rn. 3.
[1237] § 12c Abs. 1 Nr. 2 GBO.
[1238] *Demharter*, GBO, § 12a Rn. 7.

Wesentlichen können die Vorschriften zum elektronischen Grundbuch als positiv bezeichnet werden. Auffällig ist lediglich, dass die GBO es mit Ausnahme der Protokollierung im automatisierten Abrufverfahren grundsätzlich nicht vorsieht, dass eine Dokumentation im Falle einer Übermittlung von Grundstücksdaten an Dritte zu erfolgen hat. Eine solche wäre jedoch erforderlich, damit der Dritte seinen Auskunftsanspruch nach § 18 Abs. 3 LDSG wahrnehmen kann. Außerdem fällt auf, dass die Möglichkeit eines bundesweiten Abrufes von Grundstücksdaten bei den Notaren und den Gemeinden mit Blick auf deren beschränkten Zuständigkeitsbereich zu weit geht. Die dauerhafte Verfügbarkeit und Integrität der Grundbuchdaten ist wegen der dauernden Aufbewahrungspflicht und aus Gründen der Rechtssicherheit von besonderer Bedeutung. In diesem Bereich wurde jedoch bereits geforscht und es wurden brauchbare Lösungen gefunden. Bei der elektronischen Grundakte hat der Gesetzgeber nicht dargelegt, warum auch hier ein automatisiertes Abrufverfahren erforderlich ist. Um Missbräuche zu verhindern, muss die jeweils zuständige Stelle das Vorliegen der Genehmigungsvoraussetzungen besonders streng prüfen. Bei den Vorschriften, mit denen der elektronische Rechtsverkehr im Grundbuchverfahren zugelassen wurde, ergeben sich keine spezifische Fragestellungen. Hier kann auf das zurückgegriffen werden, was bereits schon beim Zivilverfahren festgestellt wurde. Der Gesetzgeber hat die Voraussetzungen für eine Auskunft und eine Einsichtnahme aus einem elektronischen Eigentümerverzeichnis detailliert geregelt. Diese Regelungen unterliegen keinen Bedenken.

Kapitel 11

Handelsgesetzbuch

Nachdem der Datenschutz bei den neuen Anwendungen im Zivilverfahren, dem Zwangsvollstreckungs- und Zwangsversteigerungsverfahren, dem Insolvenzverfahren und dem Grundbuchwesen betrachtet wurde, beschäftigt sich dieses letzte Kapitel mit dem Datenschutz bei der Ausgestaltung von neuen Verfahrensabläufen im Handelsgesetzbuch. Im Vordergrund der Prüfung stehen das elektronische Handelsregister und das elektronische Unternehmensregister. Darüber hinaus werden jedoch auch die elektronischen Anmeldungen zum Handelsregister und die elektronischen Bekanntmachungen betrachtet.

11.1 E-Handelsregister

Das Handelsregister dient der Offenbarung der Zugehörigkeit oder Nichtzugehörigkeit gewerblicher Unternehmen zum Handelsstand[1239] und gibt Auskunft über die wichtigsten Rechtsverhältnisse der Unternehmen des Handelsstands.[1240] Die Informationen aus dem Handelsregister schaffen Klarheit über Rechtsvorgänge, die für die Wirtschaft besonders wichtig sind, sie dienen damit der Sicherheit des Rechtsverkehrs. Was in das Handelsregister eingetragen werden darf oder einzutragen ist, ergibt sich aus vielen Einzelvorschriften. Angaben wie die Errichtung eines kaufmännischen Unternehmens,[1241] die Erteilung einer Prokura,[1242] der Eintritt oder der Austritt von Gesellschaftern in der OHG[1243] müssen zwingend in das Handelsregister eingetragen werden. Andere Angaben wie die Vorschriften zum Kann-Kaufmann nach § 2 HGB oder Haftungsausschlüsse nach §§ 25, 28 HGB können dagegen freiwillig in das Handelsregister eingetragen werden. Ansonsten gilt, dass Dinge, die im Gesetz nicht als Gegenstand

[1239] *Baumbach/Hopt*, HGB, § 8 Rn. 1.
[1240] *Baumbach/Hopt*, HGB, § 8 Rn. 1.
[1241] § 29 HGB.
[1242] § 53 HGB.
[1243] §§ 107, 143 HGB.

des Handelsregister erwähnt sind, nicht eintragungsfähig sind.[1244] Das Handelsregister muss nicht mit der wirklichen Rechtslage übereinstimmen. Ein großer Teil der Eintragungen hat nur deklaratorische Wirkung, d.h. die Eintragung ist keine tatbestandliche Voraussetzung für die Rechtsänderung.[1245] Nur in manchen Fällen wirken Eintragungen konstitutiv, d.h. die Rechtsänderung tritt in diesen Fällen erst mit der Eintragung in das Handelsregister ein.[1246] Das Handelsregister genießt öffentlichen Glauben. Im Geschäftsverkehr wirken gemäß § 15 Abs. 2 HGB eingetragene und bekanntgemachte Tatsachen gegenüber Dritten. Andererseits kann einer dritten Person nach § 15 Abs. 1 HGB eine in das Handelsregister einzutragende Tatsache solange nicht entgegengehalten werden, wie sie nicht eingetragen oder bekanntgemacht worden ist. Das Handelsregister besteht aus zwei Abteilungen: In die Abteilung A werden eingetragen die Einzelkaufleute, die in § 33 des Handelsgesetzbuchs bezeichneten juristischen Personen sowie die offenen Handelsgesellschaften, die Kommanditgesellschaften und die Europäischen wirtschaftlichen Interessenvereinigungen. In die Abteilung B werden eingetragen die Aktiengesellschaften, die SE, die Kommanditgesellschaften auf Aktien, die Gesellschaften mit beschränkter Haftung und die Versicherungsvereine auf Gegenseitigkeit.[1247]

Nach § 9 Abs. 1 Satz 1 HGB ist die Einsichtnahme in das Handelsregister jedermann zu Informationszwecken gestattet.[1248] Im Unterschied zur Einsichtnahme in Akten (§ 299 Abs. 2 ZPO), dem Grundbuch (§ 12 GBO) und den Schuldnerverzeichnissen (§§ 915b ZPO bzw. 882f ZPO neu), ist das Handelsregister ohne Voraussetzungen einsehbar. Das Handelsregister ist also ein unbeschränktes öffentliches Register. Das unbeschränkte Einsichtsrecht gilt dabei nicht nur für den Inhalt des Handelsregisters. Auch die zum Handelsregister eingereichten Dokumente können unbeschränkt eingesehen werden.[1249] Dies ergibt sich ebenfalls aus § 9 Abs. 1 Satz 1 HGB. Zu diesen Schriftstücken, die zum Handelsregister einzureichen, aber nicht einzutragen sind, zählen insbesondere Satzungen und Gesellschaftsverträge, die Niederschrift der Verhandlungen einer Hauptversammlung, die GmbH-Gesellschafterliste oder Unternehmensverträge

[1244] Damit soll das Handelsregister übersichtlich gehalten werden. Nicht eintragungsfähig sind daher zum Beispiel die gesetzliche Vertretung von Minderjährigen oder die Anordnung einer Testamentsvollstreckung. Vgl. hierzu auch *Baumbach/Hopt*, HGB, § 8 Rn. 5.

[1245] Die Erteilung der Prokura nach § 48 Abs. 1 HGB ist zum Beispiel eine eintragungspflichtige Tatsache. Ob jemand aber Prokurist ist oder nicht mehr, bestimmt sich nach seinem Vertragsverhältnis mit dem Inhaber.

[1246] Zum Beispiel bezeugen Eintragungen nach §§ 2, 3 Abs. 2 Abs. 2 HGB nicht die Kaufmannseigenschaft, sondern machen erst zum Kaufmann. Oder: Die Eintragung einer AG oder einer GmbH bezeugt nicht ihre Entstehung, sondern lässt sie erst als solche entstehen. Vgl. hierzu *Baumbach/Hopt*, HGB, § 8 Rn. 11.

[1247] Vgl. hierzu § 3 HRV.

[1248] Der Begriff wurde aus datenschutzrechtlicher Sicht positivrechtlich formuliert, vgl. BT-Drs. 14/6855, 17.

[1249] Dass der Inhalt dieser Schriftstücke nicht in das Handelsregister eingetragen wird, hat unterschiedliche Gründe. Zum Teil eignet er sich nicht zur Eintragung, wie z.B. Unterschrifts- und Firmenbezeichnungen. Zum Teil würde die Eintragung aber auch zu einer Überlastung des Handelsregisters führen, weil der Inhalt der Schriftstücke so umfangreich ist (z.B. bei Unternehmensverträgen gemäß § 294 Abs. 1 Satz 1 AktG) oder weil es sich um häufig wechselnde Tatsachen handelt (wie zum Beispiel bei einer jährlichen GmbH-Gesellschafterliste nach § 40 Abs. 1 Satz 1 GmbHG). Vgl. hierzu *Kollhosser*, NJW 1988, 2417.

und Jahresabschlüsse.[1250] Diese Dokumente werden in einen Registerordner aufgenommen, der elektronisch geführt wird. Er tritt an die Stelle des Sonderordners der Papierregister.[1251] Die übrigen Dokumente wie z.B. der Schriftwechsel zwischen dem Registergericht und den Beteiligten, Gutachten oder Auskünfte der Industrie- und Handelskammern oder von Behörden, werden in den sog. Registerakten – dies war bislang der Hauptband – gesammelt. Diese Akten können nicht von jedermann eingesehen werden und müssen daher auch nicht elektronisch geführt werden.[1252]

Im Handelsregister finden sich vielfach Informationen über Vereine, Verbände, Körperschaften, Gesellschaften des Handelsrechts und anderer juristischer Personen. Den dort enthaltenen Daten fehlt es jedoch an der personenbezogenen Qualität nach § 3 LDSG. Sie sind daher vom Regelungsbereich der Datenschutzgesetze ausgenommen.[1253] Allerdings werden in das Handelsregister auch Daten von natürlichen Personen eingetragen. So stellen die Daten über Namen und Anschrift von Gesellschaftern oder Einzelkaufleuten personenbezogene Daten im Sinne der Datenschutzgesetze dar. Insbesondere sind auch die Angaben über die finanzielle Situation einer Gesellschaft, die als Teil der Angaben über die Person eines Gesellschafters gespeichert sind, personenbezogene Daten des Gesellschafters.[1254] Der Bezug dieser Daten zum Bereich gewerblicher Tätigkeit lässt ihren persönlichkeitsrechtlichen Gehalt nicht entfallen.[1255]

§ 8 Abs. 1 HGB bestimmt seit dem 1.1.2007, dass das Handelsregister von den Gerichten[1256] elektronisch geführt wird. § 1 HRV legt dabei fest, dass das Amtsgericht, in dessen Bezirk ein Landgericht seinen Sitz hat, für den Bezirk dieses Landgerichts ein Handelsregister führt. § 9 Abs. 1 Satz 1 HGB regelt die Einsichtnahme grundsätzlich ohne die Unterscheidung zwischen der herkömmlichen Papiereinsicht und der elektronischen Online-Einsicht. Für letztere finden sich in § 9 Abs. 1 Satz 2-5 HGB Spezialvorschriften.[1257]

Die Online-Abfrage der Daten ist gebührenpflichtig. Darüber hinaus ist gemäß § 10 HRV die kostenlose Einsichtnahme auf der Geschäftsstelle des Registergerichts während der Dienststunden möglich. Altdaten können entweder beim zuständigen Amtsgericht eingesehen werden.

[1250] *Noack*, BB 2001, 1263.

[1251] *Seibert/Wedemann*, GmbHR 2007, 17.

[1252] *Seibert/Wedemann*, GmbHR 2007, 17.

[1253] Zur Frage der Anwendbarkeit des informationellen Selbstbestimmungsrechts auf juristische Personen vgl. BVerfGE 118, 168. Siehe hierzu auch schon Abschnitt 4.2.1.1.

[1254] *Liebscher*, 1994, 179.

[1255] BVerfG, NJW 1988, 3010. In dem vom Bundesverfassungsgericht entschiedenen Fall ging es um die Größe des Betriebs, die Betriebsstruktur, die Einkünfte und den Schuldenstand von Betrieben der Landwirtschaft. Nach dem BVerfG ist kein Grund dafür ersichtlich, die den Gewerbetreibenden im Wirtschaftsleben betreffenden personenbezogenen Daten einem prinzipiell abgeschwächten grundrechtlichen Schutz zu unterstellen. Der regelmäßig gesteigerte Sozialbezug solcher Daten werde zwar bei der Prüfung der Einschränkbarkeit des Rechts auf informationelle Selbstbestimmung im Einzelfall berücksichtigt werden müssen. Er könne jedoch nicht dazu führen, dass diese Daten als dem Schutzbereich des Grundrechts von vornherein entzogen anzusehen sind.

[1256] Einer Übertragung der Handelsregisterführung auf die IHKs hat der Gesetzgeber mit dem EHUG eine Absage erteilt. Vgl. hierzu *Baumbach/Hopt*, HGB, § 8 Rn. 3.

[1257] *Baumbach/Hopt*, HGB, § 9 Rn. 3.

Darüber hinaus besteht nach § 9 Abs. 2 HGB auch die Möglichkeit, sich diese elektronisch übermitteln zu lassen. Dies setzt allerdings voraus, dass diese Schriftstücke weniger als zehn Jahre vor dem Zeitpunkt der Antragstellung zum Handelsregister eingereicht wurden. Es besteht gemäß § 9 Abs. 4 Satz 2 HGB auch die Möglichkeit, eine Abschrift zu verlangen. Die Glaubhaftmachung eines berechtigten Interesses ist dafür nicht nötig.[1258]

11.1.1 Verfassungsmäßigkeit

Die Vorschrift des § 9 HGB geht mit einem Eingriff in das informationelle Selbstbestimmungsrecht einher. Genauso wie beim Grundbuch[1259] ist jedoch auch beim Handelsregister eine etwaige Unvereinbarkeit mit Art. 2 Abs. 1 i.V.m. Art. 1 GG noch nicht ernsthaft diskutiert worden. Dies ergibt sich aus dem Zweck des Handelsregisters, zum Schutz des Rechtsverkehrs eine größtmögliche Publizität zu erreichen. Wer als Kaufmann oder in kaufmännischen Angelegenheiten im Register steht, hat über diese Daten keine Selbstbestimmung mehr. Die Daten sind bestimmungsgemäß solche des Rechtsverkehrs geworden.[1260]

11.1.2 Zentrale Struktur

Nach § 9 Abs. 1 Satz 2 HGB bestimmen grundsätzlich die Landesjustizverwaltungen das elektronische Informations- und Kommunikationssystem für den Datenabruf. Gemäß § 9 Abs. 1 Satz 4 HGB können die Länder aber auch ein länderübergreifendes, zentrales elektronisches Informations- und Kommunikationssystem bestimmen. Ein solches Portal ist bereits eingerichtet worden. Die Publizitätsrichtlinie sieht ein derartiges zentrales Abrufportal – im Unterschied zur elektronischen Führung des Handelsregisters – nicht vor. Dennoch sind die Gründe des Gesetzgebers hier zu akzeptieren. Der Gesetzgeber wollte mit der Zentralisierung die Zersplitterung der Handelsregister für Zwecke der Einsichtnahmen überwinden. Es sei dem Einsichtnehmenden in der heutigen Zeit nicht mehr zuzumuten, die jeweiligen lokalen Registergerichte ausfindig zu machen.[1261] Die Zentralisierung der örtlichen Handelsregister ist insbesondere für den europäischen Binnenmarkt von Vorteil. Mit Hilfe der Zentralisierung kann etwa der englische oder italienische Geschäftspartner die Prokuristeneigenschaft seines Geschäftspartners oder die Höhe des Grundkapitals der Gesellschaft innerhalb einer Minute verlässlich feststellen. Wenn nun diese Angaben über eine zentrale Datenbank verfügbar sind, ist – um mit Noack zu sprechen – dem Anliegen der Registerpublizität gerade zweckgerecht nachgeholfen worden.[1262]

[1258] Bis 1969 war dieses Recht auf Abschrift noch an das Vorliegen eines berechtigten Interesses geknüpft. Diese Einschränkung wurde jedoch beseitigt, um Art. 3 Abs. 3 der Ersten Publizitätsrichtlinie zu genügen. Nach dieser Richtlinie sind vollständige und auszugsweise Abschriften auf schriftliches Verlangen zuzusenden. Vgl. hierzu *Noack*, BB 2001, 1261.

[1259] Vgl. hierzu Abschnitt 10.1.1.

[1260] *Noack*, BB 2001, 1263.

[1261] BT-Drs. 16/960, 42.

[1262] *Noack*, BB 2001, 1263.

11.1.3 Online-Auskunft

Wenn man Teilen der Literatur folgen und entgegen dem Wortlaut des § 9 HGB verlangen würde, dass eine Auskunft ausnahmsweise beschränkt werden kann,[1263] müsste man sich fragen, ob man eine Online-Auskunft überhaupt zulassen kann, da eine vorherige Überprüfung nur schwer möglich ist. So wird von einem älteren Teil der Literatur vertreten, dass § 9 Abs. 1 HGB nur die Einsicht in konkrete Registerblätter, nicht aber die Durchsicht des gesamten Handelsregisters decke. Dahinter steht die Annahme, dass § 9 Abs. 1 HGB nicht die Verfolgung aller Interessen an der Auswertung der Daten umfasse (insbesondere nicht solche kommerzieller Natur), sondern nur bestimmte Interessen, etwa ein Individualinteresse einer bestimmten Person für eigene Zwecke. Diese Norm sei daher § 34 FGG a.F. anzunähern und eng auszulegen.[1264] Dem kann jedoch nicht zugestimmt werden.[1265] § 9 HGB meint das gesamte Handelsregister und nicht nur einzelne Registerblätter. Für den Rechtsverkehr ist das Handelsregister nur dann informativ, wenn die Eintragungen nicht geheim gehalten werden. Publizität ist der Grundbaustein für den kaufmännischen Rechtsverkehr. Zudem folgt auch aus § 10 HGB, dass keine Einschränkung der Auskunft auf bestimmte Registerblätter geboten ist.[1266] Schon § 12 Abs. 2 Satz 1 ADHGB lautete: „Das Handelsregister ist öffentlich." Dieser Satz wurde nicht ins HGB übernommen, weil der Gesetzgeber ihn neben dem umfassend gewährten Einsichtsrecht für überflüssig hielt.[1267] Von daher gesehen ist die Auskunft aus dem Register nicht auf einzelne Teile beschränkt. Eine Online-Auskunft der Registerblätter ist daher möglich.

Dessen ungeachtet muss jedoch verhindert werden, dass rechtsmissbräuchliche Abfragen erfolgen. Dies ergibt sich aus der Formulierung „zu Informationszwecken" und der amtlichen Begründung zum ERJuKoG.[1268] Dieser nennt als Beispiel für einen Rechtsmissbrauch den Komplettabruf der gesamten Registerdaten oder die Sabotage des gesamten Registerbetriebes.[1269] Bezüglich ersterem knüpft die Begründung an eine Entscheidung des Bundesgerichtshofes aus dem Jahr 1988 an.[1270] Hier hatte der Bundesgerichtshof entschieden, dass § 9 HGB kein Recht gibt auf eine kommerzielle Mikroverfilmung des gesamten Datenbestandes.[1271] Zum Schutz von rechtsmissbräuchlichen Abrufen hat der Gesetzgeber jedoch ausreichende Vorkehrungen getroffen. Wie oben gesehen,[1272] werden für den Online-Abruf Gebühren erhoben. Die Anlage zu § 2 Abs. 1 JVKostO bestimmt, dass der Abruf von Daten je Registerblatt 4,50 EUR und der Abruf von Dokumenten je Datei 1,50 EUR kostet. Zudem bestimmt § 53 HRV, dass die Abrufe protokolliert werden müssen. Im Protokoll dürfen das Gericht, die Nummer des Re-

[1263] Vgl. hierzu *Kollhosser*, NJW 1988, 2410 m.w.N.
[1264] Vgl. hierzu *Kollhosser*, NJW 1988, 2410 m.w.N.
[1265] So die herrschende Meinung. Vgl. hierzu *Kollhosser*, NJW 1988, 2413; *Windbichler*, CR 1988, 447; *Liebscher*, 1994, 180.
[1266] *Liebscher*, 1994, 180.
[1267] *Prütting*, ZZP 1993, 430.
[1268] BT-Drs. 14/6855, 18.
[1269] BT-Drs. 14/6855, 18.
[1270] BGHZ 108, 32.
[1271] Zur Kritik an der Entscheidung vgl. *Gustavus*, GmbHR 1990, 197; *Hirte*, CR 1990, 631.
[1272] Vgl. hierzu Abschnitt 11.1.

gisterblatts, die abrufende Person oder Stelle, ein Geschäfts-, Aktenzeichen oder eine sonstige Kennung des Abrufs, der Zeitpunkt des Abrufs sowie die für die Durchführung des Abrufs verwendeten Daten gespeichert werden.[1273] Diese Protokolldaten dürfen außer zu Zwecken der Abrechnung auch für die Sicherung der ordnungsgemäßen Datenverarbeitung verwendet werden.[1274] Im Unterschied zu den Abrufen bei den Schuldnerverzeichnissen scheinen diese Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechtes ausreichend zu sein. So ist zu berücksichtigen, dass das Handelsregister ein unbeschränktes öffentliches Register ist und von der Zweckbestimmung mehr auf Publizität ausgerichtet ist als das Schuldnerverzeichnis.

11.1.4 Inhalt des Handelsregisters

Aus dem Registerblatt und den Dokumenten, die zum Handelsregister einzureichen sind, lassen sich der Wohnort und oftmals auch die private Anschrift von Betroffenen ermitteln. Auf dem Registerblatt umfassen die Angaben zu den natürlichen Personen, die als Einzelkaufleute, Gesellschafter einer OHG oder KG, Geschäftsführer einer GmbH oder Prokuristen eingetragen werden, den Vornamen, den Familiennamen, das Geburtsdatum und den Wohnort.[1275] Als Wohnort wird der Name der politischen Gemeinde eingetragen, zusätzlich kann ein Ortsteil angegeben werden, wenn dies der näheren Identifizierung dient.[1276] Der Wohnort lässt sich auch dem Text der Handelsregisteranmeldung entnehmen.[1277] Über den Wohnort hinaus können auch private Anschriften zum Beispiel aus dem Beglaubigungsvermerk ermittelt werden. Dies ergibt sich aus §§ 40 Abs. 4, 10 Abs. 1 BeurkG i.V.m. § 26 Abs. 2 Satz 1 1. Hs. der Dienstordnungen für Notarinnen und Notare (DONot). Letztere Vorschrift bestimmt, dass bei der Bezeichnung der natürlichen Personen der Name, das Geburtsdatum, der Wohnort und die Wohnung anzugeben sind. Wohnung bedeutet dabei Angabe der Privatanschrift einschließlich der Straße und der Hausnummer. Des Weiteren kann die Privatanschrift zum Beispiel auch über das Gründungsprotokoll einer GmbH und einer AG ermittelt werden. Nach §§ 9 Abs. 1 Nr. 1, 10 Abs. 1 BeurkG müssen im Gründungsprotokoll die Personen der Beteiligten so genau bezeichnet werden, dass Zweifel und Verwechslungen ausgeschlossen werden. Diese Anforderungen werden wiederum durch § 26 Abs. 2 Satz 1 1. Hs. DONot konkretisiert.[1278]

Aus der Verfügbarkeit dieser Daten im Internet ergeben sich Möglichkeiten der Informations- und Datenverwendung, die über die bisherigen weit hinausgehen.[1279] Die Offenlegung des Wohnortes und der Privatanschrift im weltweit zugänglichen Netz setzt betroffene Personen der Gefahr von Drohungen, Erpressungen und Entführungen aus.[1280] Nach § 1 Abs. 3 LDSG haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurich-

[1273] § 53 Abs. 1 HRV.
[1274] § 53 Abs. 2 HRV.
[1275] § 40 HRV.
[1276] *Seibert/ Wedemann*, GmbHR 2007, 17.
[1277] *Seibert/ Wedemann*, GmbHR 2007, 17.
[1278] *Seibert/ Wedemann*, GmbHR 2007, 18.
[1279] *Deutscher Anwaltsverein*, 2005, 5.
[1280] *Deutscher Anwaltsverein*, 2005, 5.

ten, keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Vor diesem Hintergrund fragt man sich, ob die Veröffentlichung der Angaben des Wohnorts und der Privatanschrift tatsächlich notwendig ist. Der Wohnort oder die Wohnanschrift sollen dem Zweck der Identifizierung einer bestimmten Person dienen und, zum Teil, der Ermöglichung von Zustellungen an sie, entweder als Vertreter des Unternehmens (z.B. Aufsichtsratsmitglieder bei Anfechtungsklagen) oder wenn sie persönlich in Anspruch genommen werden.[1281] Die Angabe des Wohnorts mit oder ohne Wohnanschrift trägt jedoch zur Identifizierung nicht viel bei, da sich diese Angabe schnell ändern kann, wie bereits erwähnt.[1282] Die Identifizierung einer bestimmten Person wird vielmehr durch die Angabe des Namens und des Geburtsdatums in ausreichendem Maße sichergestellt. Der Wohnort und die Wohnanschrift müssen auch nicht zwingend zum Zweck der Ermöglichung von Zustellungen angegeben werden.[1283] So können Zustellungen genauso gut an eine Zustelladresse oder an einen Zustellrepräsentanten erfolgen. Deshalb sollte die Möglichkeit bestehen, auf die Angabe des Wohnorts und der Wohnanschrift zu verzichten, sofern diese durch die Angabe einer Zustelladresse oder eines Zustellrepräsentanten ersetzt wird.

Wenn man dem nicht folgt, sollte man zumindest aber bei den Vorschriften, die bislang Ausnahmen von der Angabe der Wohnanschrift zulassen, oder bei denen streitig ist, ob neben dem Wohnort auch die Privatanschrift anzugeben ist, im Sinne des informationellen Selbstbestimmungsrechts eine restriktive Auslegung bevorzugen. Bislang wurde zum Beispiel von der Ausnahmeregelung des § 26 Abs. 2 Satz 2 DONot nur selten Gebrauch gemacht.[1284] Nach dieser Regelung kann von der Angabe der Wohnanschrift abgesehen werden, wenn dies in besonders gelagerten Ausnahmefällen zum Schutz gefährdeter Beteiligter oder ihrer Haushaltsangehörigen erforderlich ist. Da sich durch die Veröffentlichung im Internet neuartige Gefährdungen ergeben, sollte von dieser Regelung künftig in verstärktem Maße Gebrauch gemacht werden. Bei der Anmeldung einer neu gegründeten GmbH sowie nach jeder Veränderung der Zusammensetzung der Gesellschafter einer GmbH ist beim Handelsregister eine Liste der Gesellschafter einzureichen. Dieser muss nach §§ 8 Abs. 1 Nr. 3, 40 Abs. 1 Satz 1 GmbHG der Name, Vorname, Geburtsdatum und Wohnort der Gesellschafter entnommen werden können. Ob darüber hinaus die Angabe der Wohnanschrift erforderlich ist, ist jedoch zum Beispiel streitig. Manche[1285] sind der Auffassung, dass die Angabe der Adresse zulässig, aber nicht nötig sei. Andere[1286] sind dagegen der Meinung, dass in großen Städten die Angabe des Wohnortes nicht genüge, sondern vielmehr auch die Angabe der Adresse erforderlich sei. Aufgrund der oben genannten Gründe sollte man hier für eine restriktive Sichtweise plädieren.

[1281] *Deutscher Anwaltsverein*, 2005, 5.
[1282] *Deutscher Anwaltsverein*, 2005, 6; siehe hierzu auch Abschnitt 9.1.3.
[1283] *Deutscher Anwaltsverein*, 2005, 6.
[1284] *Seibert/ Wedemann*, GmbHR 2007, 18.
[1285] Vgl. hierzu *Seibert/ Wedemann*, GmbHR 2007, 19 m.w.N.
[1286] Vgl. hierzu *Seibert/ Wedemann*, GmbHR 2007, 19 m.w.N.

11.2 E-Anmeldungen zum Handelsregister

Nach § 12 Abs. 2 Satz 1 HGB sind alle Dokumente zu den Anmeldungen zur Eintragung in das Handelsregister elektronisch einzureichen. Auch im Falle eines Schriftformerfordernisses genügt jedoch nach § 12 Abs. 2 Satz 2 1. Hs. HGB die Übermittlung einer elektronischen Aufzeichnung. Dies ist zu kritisieren. In der Gesetzesbegründung heißt es hierzu schlicht, dass es nicht notwendig erscheine, im Zuge der Umstellung auf die elektronische Kommunikation mit dem Registergericht in diesen Fällen zur Sicherung der Authentizität zu verlangen, dass das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen wird.[1287] Dies stellt jedoch einen Verstoß gegen den Grundsatz der Formäquivalenz dar. Auch hier hätte der Gesetzgeber den Einsatz einer qualifizierten elektronischen Signatur vorschreiben sollen, um etwaige Unrichtigkeiten im Handelsregister und damit einhergehende Schäden zu vermeiden.

11.3 E-Bekanntmachungen

Die Bekanntmachungen der Eintragungen in das Handelsregister sind gemäß § 10 HGB in dem von der Landesjustizverwaltung bestimmten elektronischen Informations- und Kommunikationssystem in der zeitlichen Abfolge ihrer Eintragungen nach Tagen geordnet bekannt zu machen. Nach dieser Vorschrift werden die Bekanntmachungen grundsätzlich über 16 Landessysteme verteilt. Durch einen Verweis auf die Vorschrift des § 9 Abs. 1 Satz 4 HGB wird den Ländern aber die Möglichkeit eröffnet, ein länderübergreifendes, zentrales elektronisches Informations- und Kommunikationssystem zu bestimmen. Hiervon wurde Gebrauch gemacht.[1288]

Nach den europarechtlichen Vorgaben wäre eine Bekanntmachung im Internet nicht erforderlich gewesen. Es wäre ebensowenig notwendig gewesen, dies in einem zentralen Informations- und Kommunikationssystem zu tun.[1289] Dessen ungeachtet ist die Entscheidung des Gesetzgebers nicht zu beanstanden. Das Recht, das Handelsregister einzusehen und der Anspruch auf Erteilung von Abschriften begründen zusammen mit der Bekanntmachung nach § 10 HGB die Öffentlichkeit des Handelsregisters.[1290] Genauso wie beim elektronischen Handelsregister hat auch bei den Bekanntmachungen das informationelle Selbstbestimmungsrecht des Betroffenen hinter das Interesse der Allgemeinheit an den bekannt zu machenden Daten zurückzutreten.

[1287] BT-Drs. 16/960, 45.

[1288] Nach einem Teil der Literatur verstößt der völlige Verzicht auf eine Bekanntmachung in Papierform gegen Art. 3 Abs. 1 GG und Art. 5 Abs. 1 GG, da die noch immer bestehende digitale Kluft, also der Unterschied zwischen technisch kundigen Internet-Nutzern und den diesbezüglichen Unkundigen, eine nicht zu rechtfertigende Ungleichbehandlung beim Informationszugang der Marktteilnehmer darstelle. Weitere Nachweise bei *Baumbach/Hopt*, HGB, § 10 Rn. 1.

[1289] Art. 3 Abs. 4 Unterabsatz 2 der Richtlinie 2003/58/EG bestimmt insofern, dass Bekanntmachungen im Amtsblatt durch eine ebenso wirksame Form der Veröffentlichung, die zumindest die Verwendung eines Systems voraussetzt, mit dem die offen gelegten Informationen chronologisch geordnet über eine zentrale elektronische Datei zugänglich gemacht werden, ersetzt werden können.

[1290] *Liebscher*, 1994, 175.

Daraus, dass die Daten nun im Internet bekannt zu machen sind, folgt nichts anderes. Hiermit kann der Publizität der Bekanntmachungen noch mehr als bislang Rechnung getragen werden. Aus den oben genannten Gründen wären jedoch Schutzvorkehrungen im Hinblick auf die Angaben des Wohnorts und der Wohnanschrift erforderlich.

11.4 E-Unternehmensregister

Das Unternehmensregister wird nach § 8b Abs. 1 HGB vom Bundesministerium der Justiz elektronisch geführt. Es kann diese Aufgabe jedoch nach § 9a HGB durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf, auf eine juristische Person des Privatrechts übertragen. Die Führung des Unternehmensregisters wurde auf die Bundesanzeiger Verlagsgesellschaft mbH als Beliehene übertragen. Das Unternehmensregister ist gemäß § 9 Abs. 6 Satz 1 i.V.m. § 9 Abs. 1 Satz 1 HGB für jedermann einsehbar. In § 8b Abs. 2 HGB wird enumerativ aufgeführt, welche Daten über das Unternehmensregister zugänglich sind.[1291] Zugänglich bedeutet, dass die Informationen nicht selbst im Unternehmensregister gespeichert sein müssen, vielmehr genügt eine Zugriffsmöglichkeit auf andere Register über das mit diesem vernetzte Unternehmensregister.[1292] Im letzteren Fall erfüllt das Unternehmensregister lediglich eine Portalfunktion.[1293] Hierzu gehören die Informationen aus den Handels-, Genossenschafts- und Partnerschaftsregistern[1294] und die Informationen aus den Insolvenzbekanntmachungen[1295] mit Ausnahme von Verfahren nach InsO Teil 9 (Verbraucherinsolvenzverfahren und sonstige Kleinverfahren). Der Abruf von Daten aus Handels-, Genossenschafts- und Partnerschaftsregistern kostet auch über das Unternehmensportal die bereits oben genannten Gebühren.

11.4.1 Unternehmensregister als Zugangsportal

Soweit in dem Unternehmensregister lediglich der Zugriff auf Daten aus dem Handelsregister und den Insolvenzbekanntmachungen mit Ausnahme von Verfahren nach InsO Teil 9 (Verbraucherinsolvenzverfahren und sonstige Kleinverfahren) ermöglicht wird, ergeben sich keine mit dem Unternehmensregister verbundenen spezifischen Fragestellungen. Diesbezüglich kann daher auf die obigen Ausführungen verwiesen werden.

[1291] Diese Aufzählung ist nicht abschließend. Das Unternehmensregister ist auch offen für weitere unternehmensrelevante Daten, vgl. *Baumbach/Hopt*, HGB, § 8b Rn. 2.

[1292] *Baumbach/Hopt*, HGB, § 8b Rn. 3.

[1293] Dies ist nicht nur einfacher und kostengünstiger als eine doppelte Datenhaltung, sondern vermeidet auch die Datenspiegelung im Unternehmensregister und dadurch mögliche Widersprüche zwischen den Original- und den gespiegelten Daten, vgl. hierzu *Baumbach/Hopt*, HGB, § 8b Rn. 3.

[1294] § 8b Abs. 2 Nr. 1-3 HGB.

[1295] § 8b Abs. 2 Nr. 11 HGB.

11.4.2 Veröffentlichung des Jahresabschlusses

Bezüglich der Daten, die im Unternehmensregister selbst gespeichert sind[1296] begegnet die Veröffentlichung des Jahresabschlusses nach § 8b Abs. 2 Nr. 4 HGB bei solchen GmbHs, die nur einen oder sehr wenige Gesellschafter haben, Bedenken.[1297] Über das elektronische Handelsregister lassen sich der Name, der Vorname, der Betrag der übernommenen Stammeinlage, Firma, Sitz, Unternehmensgegenstand, Höhe des Stammkapitals bzw. der Kommanditeinlagen sowie die Personen der Gesellschafter ermitteln.[1298] Aus dem Unternehmensregister kann zudem gebührenfrei der Lagebericht zum Geschäftsjahr, die Bilanz, die Gewinn- und Verlustrechnung mit Jahresüberschuss, die Pflicht zur Aufgliederung der Umsatzerlöse sowie Angaben über die Gesamtbezüge der Organwalter abgerufen werden.[1299] Die Kombination von diesen beiden Informationsquellen kann die Kenntnis des Vermögens und des Gewinns einer Gesellschaft und die Relation zwischen der Stammeinlage/Kommanditeinlage des einzelnen Gesellschafters zur Höhe des Stammkapitals/Kommanditkapitals der Gesellschaft ergeben, woraus sich in der Regel der Gewinnanteil des einzelnen Gesellschafters zumindest überschlägig errechnen lässt.[1300] Im Hinblick darauf könnte man der Ansicht sein, die Veröffentlichung dieser Informationen stehe nicht mit Art. 2 Abs. 1 i.V.m. Art. 1 GG in Einklang.[1301] Dieser Ansicht ist jedoch nicht zu folgen.[1302] Zweck der handelsrechtlichen Publizität ist es, Gläubiger zu schützen. Einblicke in das Handelsregister geben über die aktuelle Struktur der Gesellschaft und über Gewinne und Vermögen Auskunft.[1303] Damit kann eine Prognose über die zukünftige Zahlungsfähigkeit der Gesellschaft getroffen werden.[1304] Wägt man nun dieses Ziel mit den schutzwürdigen Interessen der Beteiligten ab, so ist ersterem der Vorrang zu geben. Für den Rechtsverkehr ist die Offenlegung der handelsrechtlichen Umstände von großer Bedeutung. Die Veröffentlichung der Jahresabschlüsse stellt das Äquivalent zur Haftungsbeschränkung der Gesellschaft dar. Jedermann soll sich ein Bild über die wirtschaftliche Lage der jeweiligen Kapitalgesellschaft machen können, um imstande zu sein, die aufgrund der Haftungsbeschränkung bestehenden Risiken abzuwägen. Um kleine und mittlere Gesellschaften zu schützen, hat der Gesetzgeber an mehreren Stellen auch Erleichterungen bei der Veröffentlichungspflicht normiert.[1305] Zwar

[1296] Vgl. hierzu § 8b Abs. 2 Nr. 4-10 HGB.
[1297] *Starck*, DStR 2008, 2036.
[1298] *Starck*, DStR 2008, 2035.
[1299] *Starck*, DStR 2008, 2036.
[1300] *Starck*, DStR 2008, 2036.
[1301] So *Starck*, DStR 2008, 2035.
[1302] Vgl. hierzu auch den Nichtannahmebeschluss des BVerfG vom 10.9.2009, 1 BvR 1636/09: „Die Anwendung von § 325 HGB verletzt betroffene Kapitalgesellschaften nicht in dem Recht auf informationelle Selbstbestimmung oder auf Berufsfreiheit. Durch die Offenlegung werden mit dem Schutz des Wirtschaftsverkehrs sowie der Kontrollmöglichkeit der betroffenen Gesellschaften Zwecke verfolgt, die in erheblichem Allgemeininteresse liegen. Mögliche Eingriffe in die genannten Grundrechte werden durch diese Zwecke jedenfalls gerechtfertigt.“ Und weiter die Entscheidungen des LG Bonn, BB 2008, 1728 und des LG Köln, BB 2009, 211.
[1303] LG Köln, BB 2009, 211.
[1304] LG Köln, BB 2009, 211.
[1305] §§ 326, 327, § 286 Abs. 2 HGB.

wurden früher, d.h. vor dem Inkrafttreten des EHUG, die Jahresabschlüsse beim Amtsgericht eingereicht und die Einsichtnahme war nur in Papierform möglich. Mit der Veröffentlichung im Unternehmensregister im Internet wird nunmehr eine breitere Öffentlichkeit erreicht. Diese Tatsache rechtfertigt jedoch keine andere Bewertung. Denn mit der Veröffentlichung im Internet wird gerade das Ziel verfolgt, dass sich jedermann schnell einen Überblick über die wirtschaftliche Lage einer Kapitalgesellschaft machen kann, was nicht zu beanstanden ist.[1306]

11.5 Zusammenfassung

Im Unterschied zu der Einsichtnahme in Akten (§ 299 Abs. 2 ZPO), dem Grundbuch (§ 12 GBO) und den Schuldnerverzeichnissen (§ 915b ZPO bzw. § 882f ZPO neu) ist das Handelsregister nach § 9 HGB ohne Voraussetzungen einsehbar. Im Handelsregister befinden sich vielfach personenbezogene Daten über natürliche Personen. Den mit der Veröffentlichung dieser Daten einhergehenden Eingriff in das informationelle Selbstbestimmungsrecht hat der Betroffene hinzunehmen. Wer als Kaufmann oder in kaufmännischen Angelegenheiten im Register steht, hat über diese Daten keine Selbstbestimmung mehr. Die Daten sind bestimmungsgemäß solche des Rechtsverkehrs geworden. Die Zentralisierung des Handelsregisters begegnet keinen Bedenken. Insbesondere für den europäischen Binnenmarkt ist sie sogar von Vorteil. Auch gegen eine Online-Auskunft ist nichts einzuwenden. § 9 HGB kennt – wie aus dem Wortlaut dieser Vorschrift folgt – keine Beschränkungen eines Einsichtsrechts und zum Schutz von rechtsmissbräuchlichen Abrufen hat der Gesetzgeber entsprechende Vorkehrungen getroffen. Unzureichend ist aber der Schutz der Privatanschrift geregelt. Wenn man auf die Veröffentlichung der Privatanschrift nicht ganz verzichten will, sollte man zumindest aber bei den Vorschriften, die bislang Ausnahmen von der Angabe der Wohnanschrift zulassen, oder bei denen streitig ist, ob neben dem Wohnort auch die Privatanschrift anzugeben ist, im Sinne des informationellen Selbstbestimmungsrechts eine restriktive Auslegung bevorzugen. Das gleiche gilt auch für die elektronischen Bekanntmachungen im Handelsrecht. Spezielle datenschutzrechtliche Fragestellungen im Zusammenhang mit dem Unternehmensregister treten nur insofern auf, als die Daten dort selbst gespeichert sind, das Unternehmensregister also nicht nur eine Portalfunktion erfüllt. Bei solchen GmbHs, die nur einen oder sehr wenige Gesellschafter haben, werden verfassungsrechtliche Bedenken im Hinblick auf die Veröffentlichung des Jahresabschlusses im elektronischen Unternehmensregister angeführt. Im Ergebnis kann diesen Bedenken jedoch nicht gefolgt werden.

[1306] LG Köln, BB 2009, 211.

Kapitel 12

Schlussbetrachtung

12.1 Zusammenfassung der Arbeit

Angesichts der insgesamt zu beobachtenden rasanten technischen Entwicklung wird auch der Modernisierungsprozess in der Justiz schnell voranschreiten. In diesem Zusammenhang wird dem Datenschutz und der Datensicherheit eine immer größere Bedeutung auch in der Justiz zukommen. In der öffentlichen Diskussion und in der Literatur steht vor allem der Datenschutz im Strafprozessrecht im Blickpunkt. Mit der Frage der Online-Durchsuchung, der KfZ-Kennzeichenerfassung und der Vorratsdatenspeicherung haben sich bereits viele Autoren beschäftigt. Von der Öffentlichkeit aufmerksam verfolgt werden auch die Entscheidungen des Bundesverfassungsgerichts zu diesen Themen. Der Datenschutz im Zivilverfahren, im Zwangsvollstreckungs- und Zwangsversteigerungsverfahren, dem Insolvenzverfahren, der Grundbuchordnung und dem Handelsgesetzbuch war dagegen in der Vergangenheit nur selten im Blickpunkt. Dass dieses Thema in der Literatur bislang nur stiefmütterlich behandelt wurde, ist jedoch nicht gerechtfertigt. Im Gegensatz zum strafrechtlichen Bereich spielen die genannten Verfahren in der täglichen Praxis eine viel bedeutendere Rolle. Die Sensibilität der Daten ist im Unterschied zum strafrechtlichen Bereich keinesfalls geringer. Man muss hier nur an die in dieser Arbeit ausführlich betrachteten Schuldnerdaten denken, an die im Zusammenhang mit einem Prozesskostenhilfeverfahren zu erhebenden Daten über die Vermögensverhältnisse eines Antragstellers oder an die vielen Informationen, die durch einen Blick in das Grundbuch ermittelt werden können.

Im Unterschied zum E-Government ist der Modernisierungsprozess in der Justiz bereits weiter gediehen. Erwähnt seien hier nur die jüngeren Gesetzesänderungen durch das Gesetz über das elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister aus dem Jahr 2007, das Gesetz zur Änderung weiterer grundbuch-, register- und kostenrechtlicher Vorschriften aus dem Jahr 2009 sowie das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung, ebenfalls aus dem Jahr 2009 stammend. Nicht nur aufgrund der Besonderheiten der Modernisierungsabläufe in der Justiz als dritte Gewalt, sondern gerade

auch aufgrund der vielen gesetzgeberischen Aktivitäten ist eine gesonderte Betrachtung des Datenschutzes in der Justiz notwendig.

Das Ziel dieser Arbeit war es, erstmals einen Gesamtüberblick über die technischen Neuerungen in der Justiz in den genannten Verfahrensabläufen zu geben und dabei die Aspekte des Datenschutzes zu beleuchten. Hierzu mussten zunächst die Grundlagen erarbeitet werden. So wurden in Teil I die Begriffe erklärt, die Entwicklung der elektronischen Justiz in den untersuchten Verfahrensordnungen aufgezeigt und deren Ziele erörtert. Sodann wurden die Herausforderungen für den Datenschutz aufgezeigt. In Teil II wurde der Rechtsrahmen beschrieben, die Anforderungen des Datenschutzes für die elektronische Justiz aufgezeigt und die Thematik der Datenschutzkontrolle betrachtet. Anhand der gewonnenen Erkenntnisse wurden die verschiedenen Modernisierungsformen in den Verfahrensordnungen in Teil III bewertet. Die Untersuchung erfolgte spiegelbildlich zu Teil I mit einem jeweils einheitlichen Vorgehen. Zunächst wurde der prozessuale Ablauf vorgestellt und sodann wurden entsprechende Verbesserungspotentiale aufgezeigt.

12.2 Leitsätze

Die Ergebnisse dieser Arbeit sind in den nachfolgenden sieben Leitsätzen festgehalten. Zusammenfassend lässt sich sagen, dass die elektronische Justiz durch den technischen Fortschritt dem Datenschutz teilweise enteilt ist. Diese Lücke muss vollständig geschlossen werden, wobei bereits positive Ansätze erkennbar sind.

1. Leitsatz	**Der Datenschutz ist bei herkömmlichen Verfahrensabläufen hinreichend beachtet worden.**

Vultejus[1307] hat in einem Aufsatz geschrieben, dass der Datenschutz nirgends so schlecht aufgehoben sei wie in der Justiz. Diese These ist provokant und kann für herkömmliche Verfahrensabläufe in der Justiz auch nicht bestätigt werden. Das Prozessrecht und der Datenschutz stehen zwar in einem spannungsreichen Verhältnis zueinander. So erfordern die verschiedenen Verfahrensgrundsätze wie der Amtsermittlungsgrundsatz und der Grundsatz des rechtlichen Gehörs vielfältige Datenerhebungen und -übermittlungen, die mit einem Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen einhergehen. Auch die in dieser Arbeit vorgestellten Register können ihre Aufgabe nur erfüllen, wenn die in ihnen enthaltenen Daten von Dritten eingesehen werden können.

Grundsätzlich kann jedoch weder auf die Einhaltung der Verfahrensgrundsätze oder die Publizität von Registern verzichtet werden, noch darf der Datenschutz im Prozessrecht vernachlässigt werden. Daher muss in jedem Einzelfall ein Ausgleich gefunden werden zwischen den Geheimhaltungsinteressen von Betroffenen einerseits und dem Informationsinteresse der Allgemeinheit andererseits.

[1307] *Vultejus*, ZRP 1996, 329.

Alles in allem ist dem Gesetzgeber dieser Ausgleich gut gelungen. So ist es zum Beispiel gerechtfertigt, dass Dritte Akten in einem Zivilverfahren nur dann einsehen dürfen, wenn sie gemäß § 299 Abs. 2 ZPO ein rechtliches Interesse glaubhaft machen. Auch ist es richtig, dass in das Grundbuch nur eingesehen werden kann, wenn ein berechtigtes Interesse nach § 12 GBO dargelegt wurde. Zudem ist es richtig, eine Einsichtnahme in das Schuldnerverzeichnis nur unter den in § 915b Abs. 1 ZPO näher bezeichneten Voraussetzungen zuzulassen und Daten aus einem Handelsregister nach § 9 HGB jedermann zu Informationszwecken zur Verfügung zu stellen.

2. Leitsatz **Die Modernisierung und Elektronisierung der Justiz lässt die Anforderungen an den Datenschutz steigen.**

Der Gesetzgeber hat vor allem in der ZPO, dem ZVG, der InsO, der GBO und dem HGB eine ganze Reihe von Vorschriften erlassen, die eine Elektronisierung von Verfahrensabläufen beinhalten. Diese betreffen vor allem die Einführung der elektronischen Kommunikation mit dem Gericht und die Umstellung der bislang papiergebunden geführten Register in elektronische Register.

Technisch bedingt gehen mit diesen Änderungen neuartige Gefährdungen für den Datenschutz einher. Um ein vergleichbares Datenschutzniveau wie bei herkömmlichen Verfahrensabläufen zu schaffen, sind deshalb weitergehende Anforderungen an den Datenschutz erforderlich.

Hier ist auch das Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung von 2008 von Bedeutung. Aufgrund dieses Urteils sind auch in der Justiz die Anforderungen an die Datensicherung gestiegen. Datensicherungsmaßnahmen sind nunmehr verhältnismäßig, die es früher vielleicht einmal nicht waren.

3. Leitsatz **Teilweise hat sich der Gesetzgeber dem Datenschutz für die neuen Technologien schon angenommen.**

Es wäre nun falsch zu sagen, der Gesetzgeber habe bei der Einführung der neuen Techniken datenschutzrechtliche Aspekte grundsätzlich vernachlässigt. Bei seinen Modernisierungsbestrebungen hatte der Gesetzgeber in manchen Gebieten die datenschutzrechtliche Problematik durchaus erkannt und – wenngleich nicht immer ausreichende – Schutzmaßnahmen im Gesetz bestimmt. Tabelle 4 führt einige Beispiele dazu auf.

Für das künftige zentrale Internet-Schuldnerverzeichnis hat der Gesetzgeber zum Beispiel bestimmt, dass die nach § 882h Abs. 3 ZPO zu erlassende Rechtsverordnung sicherzustellen hat, dass die Daten nur von registrierten Nutzern nach Angabe des Verwendungszwecks abgerufen werden können, dass jeder Abrufvorgang protokolliert wird und Nutzer im Falle des missbräuchlichen Datenabrufs oder einer missbräuchlichen Datenverwendung von der Einsichtnahme ausgeschlossen werden können.

1. Beispiel: Internet-Schuldnerverzeichnis (vgl. Abschnitt 8.1)
• Ermächtigung zur RVO (§ 882h Abs. 3 ZPO) • Inhalt: Registrierung von Nutzern, Angabe des Verwendungszwecks, Protokollierung der Abrufe, Ausschluss von Nutzern bei Missbrauch
2. Beispiel: Insolvenzbekanntmachungen (vgl. Abschnitt 9.1)
• § 9 Abs. 2 InsO i.V.m. InsBekVO • Inhalt: insbesondere Löschungsfrist (6 Monate)
3. Beispiel: Internetversteigerungen (vgl. Abschnitt 8.6)
• § 814 Abs. 3 Nr. 6 ZPO • Inhalt: Anonymisierung der Schuldnerdaten, Möglichkeit der Anonymisierung der Angaben der Anbieter
zahlreiche weitere Vorschriften:
• § 174 Abs. 3 Satz 3 ZPO • § 299 Abs. 3 Satz 3 ZPO • § 133 GBO

Tabelle 4: Bereits vorhandene Schutzmaßnahmen.

Bei der Veröffentlichung von Insolvenzbekanntmachungen im Internet hat der Gesetzgeber insbesondere vorgesehen, dass Insolvenzdaten nach § 9 Abs. 2 InsO i.V.m. InsBekVO spätestens 6 Monate nach der Rechtskraft der Einstellung des Insolvenzverfahrens gelöscht werden müssen.

Schutzmaßnahmen befinden sich darüber hinaus zum Beispiel auch bei den Internetversteigerungen. Nach § 814 Abs. 3 Nr. 6 ZPO haben die Landesregierungen in ihren Rechtsverordnungen Regelungen zur Anonymisierung von Schuldnerdaten und von Angaben der Anbieter zu bestimmen.

Darüber hinaus finden sich in den Verfahrensordnungen zahlreiche weitere Vorschriften, die sich mit dem Datenschutz und der Datensicherheit bei elektronischen Verfahrensabläufen auseinandersetzen. So schreibt etwa § 174 Abs. 3 Satz 3 ZPO vor, dass das Dokument bei einer elektronischen Zustellung gegen unbefugte Kenntnisnahme zu schützen ist. § 299 Abs. 3 Satz 3 ZPO ZPO besagt, dass bei einer Online-Einsicht in eine Zivilakte sichergestellt werden muss, dass der Zugriff nur durch den Prozessbevollmächtigten erfolgt und § 133 GBO lässt ein automatisiertes Abrufverfahren beim elektronischen Grundbuch nur unter ganz bestimmten Voraussetzungen zu. So ist für ein automatisiertes Abrufverfahren eine vorherige

Genehmigung durch die Landesjustizverwaltung erforderlich. Diese Genehmigung kann nur bestimmten Stellen erteilt werden. Zudem muss jeder Abrufvorgang protokolliert werden.

4. Leitsatz **Die derzeitige Gemengelage der datenschutzrechtlichen Vorschriften ist zu vereinheitlichen.**

Ungeachtet der bereits vorhandenen Schutzmaßnahmen ist jedoch festzustellen, dass derzeit eine Gemengelage an datenschutzrechtlichen Vorschriften existiert, die vereinheitlicht werden muss.

Obgleich im Hinblick auf die Sensibilität der Daten kein unterschiedlicher Schutzbedarf festgestellt werden kann, hat der Gesetzgeber nämlich für die neuen Anwendungen zum Teil kein gleiches Datenschutzniveau geschaffen, wie die folgenden Beispiele zeigen (vgl. auch Tabelle 5):

- Der Gesetzgeber hat es für notwendig erachtet, nach § 126 Abs. 3 GBO die Datenverarbeitung im Auftrag im Grundbuchwesen auf eine staatliche Stelle oder eine juristische Person des öffentlichen Rechts zu beschränken; bei den ab dem 1.1.2013 geltenden Vorschriften zum elektronischen Vermögensverzeichnis und zum elektronischen Schuldnerverzeichnis finden sich dagegen in § 802k Abs. 3 Satz 3 und in § 882h Abs. 2 Satz 2 ZPO keine vergleichbaren Anforderungen.

- Mit § 882f Satz 1 Nr. 6 ZPO neu hat der Gesetzgeber einen spezialgesetzlichen Auskunftsanspruch für den Schuldner geschaffen, damit dieser prüfen kann, welche Daten über ihn im Schuldnerverzeichnis gespeichert sind. Beim künftigen elektronischen Vermögensverzeichnis findet sich eine vergleichbare Regelung nicht. Auch der Rückgriff auf die allgemeinen Datenschutzgesetze ist nicht möglich, weil ein Auskunftsanspruch in der Gesetzesbegründung ausdrücklich abgelehnt worden ist.

- Bei der elektronischen Zustellung hat der Gesetzgeber mit § 174 Abs. 3 Satz 3 ZPO bestimmt, dass Dokumente gegen eine unbefugte Kenntnisnahme geschützt werden müssen. Bei der elektronischen Einreichung einer Klageschrift nach § 130a ZPO hat er dagegen keine vergleichbare Regelung getroffen.

- Darüber hinaus hat der Gesetzgeber Schutzvorkehrungen, insbesondere eine sechsmonatige Löschfrist, bei den öffentlichen Bekanntmachungen von Insolvenzdaten im Internet vorgesehen. Obwohl auch andere öffentliche Bekanntmachungen, zum Beispiel im Zivilverfahren, einen vergleichbar sensiblen Inhalt haben können, gibt es dort keine entsprechenden Schutzmaßnahmen.

Insgesamt müssten die Technikbestimmungen in den Verfahrensordnungen im Hinblick auf ihren datenschutzrechtlichen Gehalt also nochmals überprüft und vereinheitlicht werden.

Aspekt	⟵ enger **Regelungen** weiter ⟶	
Datenverarbeitung im Auftrag	nur staatliche Stellen (§ 126 Abs. 3 GBO)	auch private Stellen (§§ 802k Abs. 3 Satz 3, 882h Abs. 2 Satz 2 ZPO)
Auskunftsanspruch	für eigene Daten möglich (§ 882f Satz 1 Nr. 6 ZPO neu)	nicht für Vermögensverzeichnisse (BR-Drs. 16/10069, 27)
Sicherheit bei elektronischer Übermittlung von Schriftsätzen	Verschlüsselung gefordert (§ 174 Abs. 3 Satz 3 ZPO)	keine technischen Vorgaben (§ 130a ZPO)
Schutzvorkehrungen bei öffentlichen Bekanntmachungen	insb. Löschfrist (§ 9 Abs. 2 InsO i.V.m. InsBekV)	keine Vorgaben (Bekanntmachungen nach ZPO)

Tabelle 5: Beispiele für uneinheitliche Regelungen zum Datenschutz.

5. Leitsatz **Die elektronischen Verfahrensabläufe erfordern weitergehende rechtliche und technische Schutzmaßnahmen.**

Darüber hinaus sind aber auch weitergehende rechtliche und technische Schutzmaßnahmen erforderlich. Dies gilt vor allem für die Veröffentlichungen und Bekanntmachungen von Schuldnerdaten. Die hier untersuchten Internet-Register zeichnen sich durch eine Zentralisierung und eine länderübergreifende Abrufmöglichkeit unter Benutzung eines einzigen Zugangsportals aus. Zwar konnte die Verfassungsmäßigkeit der Veröffentlichung von Schuldnerdaten im Internet bejaht werden, da der Gesetzgeber bestimmte Schutzvorkehrungen vorgesehen hat. Auch für die jeweiligen Zentralisierungen der Internet-Register und Bekanntmachungsplattformen sprachen – im Zwangsvollstreckungsverfahren nicht zuletzt auch zum Schutz des Schuldners – gute Gründe. Allerdings wären an verschiedenen Stellen Änderungen wünschenswert gewesen.

So dürfen beschränkt einsehbare Register nicht faktisch zu unbeschränkt öffentlichen Registern werden. Vor diesem Hintergrund hätte zum Beispiel eine Online-Einsicht für jedermann in das künftige elektronische Schuldnerverzeichnis nicht ermöglicht werden dürfen. Da jedoch nicht zu erwarten ist, dass das bereits im Jahr 2009 beschlossene Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung vor seinem Inkrafttreten am 1.1.2013 nochmals geändert wird, ist es zumindest erforderlich, dass in der noch zu errichtenden Rechtsverordnung strenge Vorgaben im Hinblick auf eine zuverlässige Registrierung, eine Protokollierung sowie die Festsetzung einer hohen Gebühr zum Abruf bestimmt werden.

Da Insolvenzdaten von Auskunfteien, Wirtschaftsinformationsdiensten und Verlagen vielfach ausgewertet und im Internet verbreitet werden, muss v.a. auch das massenhafte Herunterladen dieser Daten und deren Weiterverbreitung nach Ablauf der amtlichen Löschfrist verhindert werden. Hierzu bedarf es zum Einen der (Wieder-) Einfügung einer Regelung zum Kopierschutz in § 9 Abs. 2 InsO und zum Anderen der Schaffung eines Straf- oder Bußgeldtatbestandes

im BDSG, der eine Weiterverbreitung von Daten durch Dritte nach Ablauf einer amtlichen Löschfrist verbietet.

6. Leitsatz **Verschlüsselungstechniken, qualifizierte elektronische Signaturen, der neue Personalausweis und Anwendungen wie Bürgerportale schaffen Rechtssicherheit in den elektronischen Verfahrensabläufen.**

Vorschriften zur Verschlüsselung und die Pflicht zum Einsatz qualifizierter elektronischer Signaturen werden oft als Hemmschuh und Hindernis betrachtet. Eine Verschlüsselung führe zu einer Überbelastung und sei daher nicht zu rechtfertigen. Auch der Einsatz von qualifizierten elektronischen Signaturen wird oft nur als deutsche Überperfektion ohne großen Nutzen empfunden. Diese Arbeit hat jedoch gezeigt, dass dem nicht zugestimmt werden kann. Eine vertrauenswürdige Kommunikation ist ohne den Einsatz dieser Techniken gar nicht möglich. Aber nicht nur die Beachtung dieser Techniken ist erforderlich. Für die elektronische Akteneinsicht und auch für andere Prozesse, welche eine zuverlässige Registrierung erfordern, wird langfristig auch der Einsatz des elektronischen Personalausweises in der Justiz unabkömmlich sein. In diesem Zusammenhang ist auch zu hoffen, dass der Entwurf eines Bürgerportalgesetzes verabschiedet wird. Die Möglichkeit, über verschlüsselte Leitungen mit Personen elektronisch kommunizieren zu können, die sich zuvor zuverlässig registriert haben, brächte gerade auch für die elektronische Justiz einen großen Nutzen, da hiermit auch ein Zustellungsnachweis verbunden wäre. Der elektronische Personalausweis und die Bürgerportale könnten dabei mit dem Projekt S.A.F.E. verbunden werden.

7. Leitsatz **Eine grundlegende Modernisierung der allgemeinen Datenschutzgesetze ist erforderlich.**

Unabhängig von den in dieser Arbeit speziell betrachteten datenschutzrechtlichen Problemen und den jeweils speziell beschriebenen Lösungsansätzen, muss man sich jedoch langfristig fragen, ob der Schutz von Inhaltsdaten im Internet nach den allgemeinen Datenschutzgesetzen überhaupt ausreichend ist. Als Beispiele seien an dieser Stelle nur etwa die Problematik um Google Earth, der Bewertungsplattformen von Lehrern im Internet oder die sozialen Netzwerke erwähnt. Diese Problematik anzugehen wird bei der ins Auge gefassten grundlegenden Modernisierung des Datenschutzrechts sicherlich eine der wichtigsten Aufgaben sein.

Literaturverzeichnis

Ralf B. Abel: Aktuelle Entwicklungen bei der geplanten Änderung der Schuldnerverzeichnisse. RDV, 1988, 185.

Ralf B. Abel: Schuldnerverzeichnisse in privater Hand. RDV, 1991, 233.

Ralf B. Abel: Der behördliche Datenschutzbeauftragte. MMR, 2002, 289.

Ralf B. Abel (Hrsg.)**:** Datenschutz in Anwaltschaft, Notariat und Justiz. 2. Auflage. München: C.H. Beck, 2003.

Ralf B. Abel: Datenschutz in Anwaltschaft und Notariat. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 1334.

Ralf B. Abel: Geschichte des Datenschutzes. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 194.

Ralf B. Abel: Die neuen BDSG-Regelungen. RDV, 2009, 147.

Volker Ahrend et al.**:** Modernisierung des Datenschutzes? DuD, 2003, 433.

Herbert Arndt/Klaus Lerch/Gerd Sandkühler: Bundesnotarordnung. 6. Auflage. Köln: Carl Heymanns Verlag, 2008.

Herbert Auernhammer: Bundesdatenschutzgesetz. 3. Auflage. Köln: Carl Heymanns Verlag, 1993.

Henning Aufderhaar/Gerold M. Jaeger: Gesetzliche Neuregelung zur Modernisierung des Grundbuchverfahrens. ZfIR, 2009, 681.

Mario Axmann/Thomas A. Degen: Kanzlei-Homepages und elektronische Mandatsbearbeitung – Anwaltsstrategien zur Minimierung rechtlicher Risiken. NJW, 2006, 1457.

Mathias Bäcker: Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen. In: **Gerrit Manssen** et al. (Hrsg.), Das neue Computergrundrecht. Berlin: LIT Verlag, 2009, 1.

Susanne Baer: Grundrechtecharta ante portas. ZRP, 2000, 363.

Harald Baier/Judith Klink/Tobias Straub: Digitale Signatur – Leitfaden zum Einsatz digitaler Signaturen. Wiesbaden: hessen-media, 2003.

Wolfgang Bär: Informationelle Selbstbestimmung und Justiz. CR, 1998, 767.

Michael Bartsch: Die Vertraulichkeit und Integrität informationstechnischer Systeme als sonstiges Recht nach § 823 Abs. 1 BGB. CR, 2008, 613.

Reinhold Baumann: Stellungnahme zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 15.12.1983 zum Volkszählungsgesetz 1983. DVBl, 1984, 612.

Adolf Baumbach/Klaus J. Hopt: Handelsgesetzbuch. München: C.H. Beck, 2010, 34. Auflage.

Adolf Baumbach et al.**:** Zivilprozessordnung. 68. Auflage. München: C.H. Beck, 2010.

Helmut Bäumler/Christine Nordmann: Die Aufgaben des gerichtlichen Datenschutzbeauftragten. In: **Ralf B. Abel** (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz. 2. Auflage. München: C.H. Beck, 2003, 129.

Ernst Benda: Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz. DuD, 1984, 86.

Jens Bender et al.**:** Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DuD, 2008, 173.

Lutz Bergmann/Roland Möhrle/Armin Herb: Datenschutzrecht. Stuttgart: Richard Boorberg Verlag, 2009.

Uwe Berlit: Richterliche Unabhängigkeit und Organisation effektiven Rechtsschutzes im „ökonomisierten“ Staat. In: **Helmuth Schulze-Fielitz/Carsten Schütz** (Hrsg.), Justiz und Justizverwaltung zwischen Ökonomisierungsdruck und Unabhängigkeit. Berlin: Duncker & Humblot, 2002, 135.

Uwe Berlit: E-Justice – Chancen und Herausforderungen in der freiheitlichen demokratischen Gesellschaft. JurPC Web-Dok. 2007, Nr. 171, Abs. 1–146.

Uwe Berlit: Die elektronische Akte – rechtliche Rahmenbedingungen der elektronischen Gerichtsakte. JurPC Web-Dok. 2008, Nr. 157, Abs. 1–132.

Wilfried Bernhard: E-Justice überwindet die Grenzen innerhalb Europas. JurPC Web-Dok. 2007, Nr. 75, Abs. 1–43.

Peter Bilsdorfer: Die Anzeige von Steuerstraftaten nach § 116 AO und das Recht auf informationelle Selbstbestimmung. ZRP, 1997, 137.

Johann Bizer: Ziele und Elemente der Modernisierung des Datenschutzrechts. DuD, 2001, 274.

Johann Bizer: Strukturplan modernes Datenschutzrecht. DuD, 2004, 6.

Willi Blümel: Zur Praxis der Veröffentlichung von Gerichtsentscheidungen. DVBl, 1966, 63.

Michael Bohrer: Das Berufsrecht der Notare. 1. Auflage. München: C.H. Beck, 1991.

Walter Böhringer: Informationelles Selbstbestimmungsrecht kontra Publizitätsprinzip bei § 12 GBO. Rpfleger, 1987, 181.

Walter Böhringer: Der Einfluss des informationellen Selbstbestimmungsrecht auf das Grundbuchverfahrensrecht. Rpfleger, 1989, 309.

Walter Böhringer: Kein Anspruch auf Grundbucheinsicht durch Angehörige auch bei zu erwartender Pflegebedürftigkeit des Grundstückseigentümers. ZEV, 2009, 43.

Günter Brambring/Dieter Medicus/Max Vogt (Hrsg.)**:** Festschrift für Horst Hagen. Köln: RWS Verlag Kommunikationsforum, 1999.

Ralf Brandner et al.**:** Langzeitarchivierung qualifizierter elektronischer Signaturen. DuD, 2002, 97.

Markus Breitscheid et al.**:** Sichere Zahlungsverfahren für E-Government. Regensburg: ibi research, 2004.

Markus Breitscheid et al.**:** Zahlungsabwicklung im Internet – Bedeutung, Status quo und zukünftige Herausforderungen. Regensburg: ibi research, 2006.

Gabriele Britz: Von der elektronischen Verwaltung zur elektronischen Verwaltungsjustiz – Realisierungsbedingungen und Realisierungsrisiken im Vergleich. DVBl, 2007, 993.

Ulf Brühann/Thomas Zerdick: Umsetzung der EG-Datenschutzrichtlinie. CR, 1996, 429.

Brun O Bryde: Verfassungsentwicklung: Stabilität und Dynamik im Verfassungsrecht der Bundesrepublik Deutschland. Baden-Baden: Nomos, 1982, 1. Auflage.

Walter Buggisch: Fälschung beweiserheblicher Daten durch Verwendung einer falschen E-Mail-Adresse? NJW, 2004, 3519.

Jens Bülle: Die Strafbarkeit des Amtsträgers wegen Strafvereitelung und Steuerhinterziehung bei Verletzung der Mitteilungspflicht aus § 116 Abs. 1 S. 1 AO. NStZ, 2009, 57.

Alfred Büllesbach: Das neue Bundesdatenschutzgesetz. NJW, 1991, 2593.

Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz, Arbeitsgruppe „IT-Standards in der Justiz“: SAFE Grobkonzept. 2007 ⟨URL: `http://www.deutschland-online.de/DOL_Internet/binarywriterservlet?imgUid=29710643-fa8a-9b11-d88e-f1ac0c2f214a&uBasVariant=22222222-2222-2222-2222-222222222222`⟩.

Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz, Arbeitsgruppe „Zukunft“: Welches Maß an IT-Zentralisierung verträgt die Dritte Gewalt? JurPC Web-Dok. 2009, Nr. 202, Abs. 1–126.

Bundesbeauftragter für den Datenschutz: 15. Tätigkeitsbericht. 1994.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: 19. Tätigkeitsbericht. 2002.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: 20. Tätigkeitsbericht. 2004.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: 21. Tätigkeitsbericht. 2006.

Bundesministerium des Innern: Einführung des elektronischen Personalausweises in Deutschland, Grobkonzept – Version 2.0. 2008 ⟨URL: `http://www.bmi.bund.de/cae/servlet/contentblob/122648/publicationFile/9169/Grobkonzept_Personalausweis.pdf`⟩.

Bundesministerium des Innern: Polizeiliche Kriminalstatistik 2008. 2009 ⟨URL: `http://www.bmi.bund.de/cae/servlet/contentblob/541740/publicationFile/26893/PKS2008.pdf`⟩.

Bundesministerium des Innern: Polizeiliche Kriminalstatistik 2009. 2010 ⟨URL: `http://www.bmi.bund.de/cae/servlet/contentblob/1069004/publicationFile/65239/PKS2009.pdf`⟩.

Bundesrechtsanwaltskammer: Datenaufsicht durch die Rechtsanwaltskammern. Schreiben des Präsidenten vom 27. September, 2006 ⟨URL: `http://www.brak.de/seiten/pdf/aktuelles/Schr_Datenaufsicht.pdf`⟩.

Bundesrechtsanwaltskammer: Stellungnahme durch den Ausschuss ZPO/GVG zur Reform der Sachaufklärung in der Zwangsvollstreckung. 2009 ⟨URL: `http://www.brak.de/seiten/pdf/Stellungnahmen/2009/Stn15.pdf`⟩.

Bundesregierung: Bericht der Bundesregierung über Daten- und Persönlichkeitsschutz bei der Veröffentlichung insolvenzrechtlicher Daten über das Internet. Drucksache 15/181, 2002.

Jost-Dietrich Busch: Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts. DVBl, 1984, 385.

CDU, CSU und FDP: Wachstum, Bildung, Zusammenhalt – Koalitionsvertrag zwischen CDU, CSU und FDP. 17. Legislaturperiode, 2009.

Mark R. Crispin: Internet Message Access Protocol, Version 4rev1. RFC 3501, 2003 ⟨URL: `http://www.ietf.org/rfc/rfc3501.txt`⟩.

Ulrich Dammann: Das neue Bundesdatenschutzgesetz. NJW, 1991, 640.

Rolf Nikolas Danckwerts: Die Entscheidung über den Eilantrag. GRUR, 2008, 763.

Christian Dästner: Neue Formvorschriften im Prozessrecht. NJW, 2001, 3469.

Herta Däubler-Gmelin: Eine Europäische Charta der Grundrechte. Beitrag zur gemeinsamen Identität. EuZW, 2000, 1.

Thomas A. Degen: Mahnen und Klagen per E-Mail – Rechtlicher Rahmen und digitale Kluft bei Justiz und Anwaltschaft? NJW, 2008, 1473.

Johann Demharter: Grundbuchordnung. 27. Auflage. München: C. H. Beck, 2010.

Volker Deutsch: Die Schutzschrift in Theorie und Praxis. GRUR, 1990, 327.

Deutscher Anwaltsverein: Stellungnahme durch den Handelsrechtsausschuss zum Entwurf eines Gesetzes über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister. 2005 ⟨URL: `http://anwaltverein.de/downloads/stellungnahmen/2005-31.pdf`⟩.

Deutscher Anwaltsverein: Stellungnahme durch den Ausschuss Informationsrecht zum Referentenentwurf des Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften. 2008 ⟨URL: `http://anwaltverein.de/downloads/Stellungnahmen-08/SN70.pdf`⟩.

Deutscher Gerichtsvollzieher Bund e.V.: Stellungnahme zur Reform der Sachaufklärung in der Zwangsvollstreckung. 2008 ⟨URL: `http://www.dgvb.de/archiv/stellungnahme-des-dgvb-zum-gesetz-zur-sachaufklaeru.php`⟩ – Zugriff am 20.1.2010.

Deutscher Notarverein: Stellungnahme zum Entwurf eines Gesetzes zur Regelung von Bürgerportalen. 2008 ⟨URL: `http://www.dnotv.de/_files/Dokumente/Stellungnahmen/STN-Brgerportale.pdf`⟩.

Ralf Diederich: Lösungswege elektronisches Schuldnerverzeichnis. 2003 ⟨URL: `http://www.gv24.de/032c7e98d70e0f01a/032c7e98d70e2ab20.php`⟩ – Zugriff am 20.1.2010.

Alfred Schramm Dietmar Jahnel/Elisabeth Staudegger (Hrsg.)**:** Informatikrecht. 2. Auflage. Wien: Springer, 2002.

Elisabeth Duhr: Datenschutz in Auskunfteien. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 1157.

Jos Dumortier/Regina Rinderle: Umsetzung der Signaturrichtlinie in den europäischen Mitgliedstaaten. CRi, 2001, 5.

Dieter Duursma/Henriette Duursma-Kepplinger: Funktionen und Wirkungen der österreichischen Insolvenzdatei. ZInsO, 2002, 913.

Dieter Duursma/Henriette Duursma-Kepplinger: Die Insolvenzdatei im Internet. In: **Oliver Plöckinger/Dieter Duursma/Günther Helm** (Hrsg.), Aktuelle Entwicklungen im Internet-Recht: Beiträge zur zivil-, straf- und verwaltungsrechtlichen Diskussion. Wien: Neuer Wissenschaftlicher Verlag, 2002, 89.

Claudia Eckert: IT-Sicherheit. 6. Auflage. München: Oldenbourg Wissenschaftsverlag, 2009.

Eugen Ehmann: Kriminalpolizeiliche Sammlungen und Auskunftsanspruch des Betroffenen. CR, 1988, 575.

Sylvia Eickmeier: Eine europäische Charta der Grundrechte. Bericht über das gemeinsame Forum des Bundesministeriums der Justiz und der Vertretung der Europäischen Kommission in Deutschland. DVBl, 1999, 1026.

Martin Eifert: Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchungen. NVwZ, 2008, 521.

Thomas Engelien-Schulz: Der behördliche Datenschutzbeauftragte – Rechtsstellung, Aufgaben und Befugnisse. BWV, 2001, 241.

Walter Ernestus: Konzept der Datensicherung. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 269.

Stefan Ernst: Beweisprobleme bei E-Mail und anderen Online-Willenserklärungen. MDR, 2003, 1091.

Wilhelm E. Feuerich/Dag Weyland: Bundesrechtsanwaltsordnung. München: Verlag Franz Vahlen, 2008, 7. Auflage.

Stefanie Fischer-Dieskau: Der Referentenentwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts. MMR, 2003, 701.

Stefanie Fischer-Dieskau: Elektronisch signierte Dokumente – Anforderungen und Maßnahmen für ihren dauerhaften Erhalt. In: **Rainer Hering/Udo Schäfer** (Hrsg.), Digitales Verwalten – Digitales Archivieren. Hamburg: Hamburg University Press, 2004, 33.

Stefanie Fischer-Dieskau: Das elektronische Dokument als Mittel zur Beweissicherung: Anforderungen an seine langfristige Aufbewahrung. Dissertation, Universität Kassel, 2006.

Ingo Fritsche: Die Einführung des elektronischen Rechtsverkehrs im Privatrecht – Eine Übersicht. NJ, 2002, 169.

Hans-Ullrich Gallwas: Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit. NJW, 1992, 2785.

Hans Friedhelm Gaul: Grundüberlegungen zur Neukonzipierung und Verbesserung der Sachaufklärung in der Zwangsvollstreckung. ZZP, 1995, 3.

Andreas Geiger: Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung. NVwZ, 1989, 35.

Hansjörg Geiger: Datenschutz bei Gerichten und Staatsanwaltschaften. CR, 1986, 37.

Gesellschaft für Informatik e.V./Informationstechnische Gesellschaft: Electronic Government als Schlüssel zur Modernisierung von Staat und Verwaltung. 2000 ⟨URL: `http://www.gi-ev.de/fileadmin/redaktion/Download/presse_memorandum.pdf`⟩.

Hartmut Gieselmann: Gegen das Vergessen. c't, 2005, Nr. 1, 44.

Klaus Globig: Zulässigkeit der Erhebung, Verarbeitung und Nutzung im öffentlichen Bereich. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 627.

Peter Gola: Informationelle Selbstbestimmung in Form des Widerspruchsrechts. DuD, 2001, 278.

Peter Gola/Christoph Klug: Grundzüge des Datenschutzrechts. München: C.H. Beck, 2003.

Peter Gola/Rudolf Schomerus: BDSG Kommentar. 9. Auflage. München: C.H. Beck, 2007.

Claudia Golembiewski: Mitteilungen durch die Justiz. Dissertation, Universität Hamburg, 2000.

Ulrich Graf/Irene Wunsch: Akteneinsicht im Insolvenzverfahren. ZIP, 2001, 1800.

Christoph Grimm/Peter Caesar: Verfassung für Rheinland-Pfalz. Baden-Baden: Nomos, 2001, 83.

Ursula Grunow/Gerd Dressel: Überlegungen zur zentralen Erfassung der Eintragungen in Schuldnerverzeichnisses. ZRP, 1989, 325.

Herbert Grziwotz: Grundbucheinsicht, allgemeines Persönlichkeitsrecht und rechtliches Gehör. MittBayNot, 1995, 97.

Eckhardt Gustavus: Handelsregister-Datenbanken: Pro und Contra. GmbHR, 1990, 197.

Christoph Gusy: Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. DuD, 2009, 33.

Jürgen Häfner: eGovernment in der Justiz – Sachstand und Ausblick. DRiZ, 2005, 151.

Susanne Hähnchen: Elektronische Akten bei Gericht – Chancen und Risiken. NJW, 2005, 2257.

Susanne Hähnchen: Einführung: Was ist „elektronischer Rechtsverkehr“? (Kapitel 1). JurPC Web-Dok. 2007, Nr. 151, Abs. 1–22.

Judith Hartig/Judith Klink/Helmut Eiermann: Landesdatenschutzgesetz Rheinland-Pfalz. 1. Auflage. Wiesbaden: Kommunal- und Schulverlag, 2009.

Niko Härting: Unveschlüsselte E-Mails im anwaltlichen Geschäftsverkehr – Ein Verstoß gegen die Verschwiegenheitspflicht? MDR, 2001, 61.

Niko Härting: IT-Sicherheit in der Anwaltskanzlei – Das Anwaltsgeheimnis im Zeitalter der Informationstechnologien. NJW, 2005, 1248.

Lutz Hasse/Katrin Böhlke: Factum nebulosum – Jus nebulosum. DuD, 2009, 274.

Hanns-Wilhelm Heibey: Datensicherung. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 570.

Helmut Heil: Datenschutzkontrolle. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 747.

Jörn Heinemann: Neubestimmung der prozessualen Schriftform. Dissertation, Universität Erlangen-Nürnberg, 2002.

Thomas Heinz et al.**:** Zivilprozessordnung. 30. Auflage. München: C.H. Beck, 2009.

Rainer Hering/Udo Schäfer (Hrsg.)**:** Digitales Verwalten – Digitales Archivieren. Hamburg: Hamburg University Press, 2004.

Burkhard Hess: Neues deutsches und europäisches Zustellungsrecht. NJW, 2002, 2417.

Konrad Hesse: Die normative Kraft der Verfassung. Tübingen: Mohr Siebeck, 1959.

Markus Hesseler: Auskunfts-/Akteneinsichtsrechte und weitere Informationsmöglichkeiten des Gläubigers im Regelinsolvenzverfahren. ZInsO, 2001, 873.

Udo Hintzen/Ralf Engels/Klaus Rellermeyer: Gesetz über die Zwangsversteigerung und die Zwangsverwaltung – einschließlich EGZVG und ZwVwV. Bielefeld: Verlag Ernst und Werner Gieseking, 2008, 13. Auflage.

Heribert Hirte: Kommerzielle Nutzung des Handelsregisters. CR, 1990, 631.

Thomas Hoeren: Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme? MMR, 2008, 365.

Constanze Holin: Der elektronische Ablauf des Zivilprozesses. Dissertation, Universität Münster, 2008.

Bernd Holznagel: Recht der IT-Sicherheit. München: C.H. Beck, 2003.

Anton Hornung: Änderungen zum Schuldnerverzeichnis. Rpfleger, 1995, 233.

Gerrit Hornung: Biometrische Daten in Ausweisen. DuD, 2005, 69.

Gerrit Hornung: Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren. Dissertation, Universität Kassel, 2005.

Gerrit Hornung: Fingerabdrücke statt Doktortitel: Paradigmenwechsel im Passrecht. DuD, 2007, 181.

Oliver Hornung: Erweiterung der Schufa-Klausel möglich? CR, 2007, 753.

Friedhelm Hufen: Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbstbestimmung – eine juristische Antwort auf „1984“? JZ, 1984, 1072.

Ulrich Jäger: Die Reform der Sachaufklärung in der Zwangsvollstreckung. Rbeistand, 2008, 43.

Ulrich Jäger/Jochen H Schatz: Etwas Licht und viel Schatten – Der Entwurf eines Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung. ZVI, 2008, 143.

Jens Jeep/Klaus Wiedemann: Die Praxis der elektronischen Registeranmeldung. NJW, 2007, 2439.

Wulf Kamlah: Das Schufa-Verfahren und seine datenschutzrechtliche Zulässigkeit. MMR, 1999, 395.

Alfried Kampen/Marc Engelhardt: Das Zustellungsreformgesetz – Eine Darstellung der neuen Rechtslage. ArbuR, 2003, 244.

Christoph Keller: Der einstweilige Rechtsschutz im Zivilprozess – 2. Teil. Jura, 2007, 327.

Rolf Keller: Die Automation des Mahnverfahrens. NJW, 1981, 1184.

Ulrich Keller: Auswirkungen des Zustellungsreformgesetzes auf das Insolvenzverfahren. NZI, 2002, 581.

Ulrich Keller: Die öffentlichen Bekanntmachungen im Insolvenzverfahren. ZIP, 2003, 149.

Eberhard Kiesche/Matthias Wilke: Elektronischer Entgeltnachweis (ELENA). dbr, 2010, 33.

Wolfgang Kilian: EG-Richtlinie über digitale Signaturen in Kraft. BB, 2000, 733.

Wolfgang Kilian/Benno Heussen (Hrsg.)**:** Computerrechtshandbuch. München: C.H. Beck, 2009.

John C. Klensin: Simple Mail Transfer Protocol. RFC 2821, 2001 ⟨URL: `http://www.ietf.org/rfc/rfc2821.txt`⟩.

Detlef Klett/Lee Sang-Woon: Vertraulichkeit des E-Mailverkehrs. CR, 2008, 644.

Judith Klink: Datenschutz bei Internetbekanntmachungen – Ein Modell für eGovernment? Tagungsband D-A-CH Security, 2008, 20.

Judith Klink/Tobias Straub: Rechtliche und technische Entwicklungen qualifizierter Signaturen. Tagungsband D-A-CH Security, 2005, 130.

Joachim Klos: Nochmals: Das Datengeheimnis des Richters. ZRP, 1997, 50.

Franz-Ludwig Knemeyer: Auskunftsanspruch und behördliche Auskunftsverweigerung – Ermessen oder Abwägung. JZ, 1992, 348.

Michael Knopp et al.**:** Grunddienste für die Rechtssicherheit elektronischer Kommunikation – Rechtlicher Bedarf für eine gewährleistete Sicherheit. MMR, 2008, 723.

Ralf Koebler: eJustice: Vom langen Weg in die digitale Zukunft der Justiz. NJW, 2006, 2089.

Helmut Kollhosser: Handelsregister und private Datenbanken. NJW, 1988, 2409.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Mitteilungen in Zivilsachen. Entschließung der 27. Konferenz am 6./7. Juni, 1984.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Mitteilungen in Zivilsachen. Entschlließung der 30. Konferenz am 13. September, 1985.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Grundrecht auf Datenschutz. Entschließung der 43a. Sonderkonferenz am 28. April, 1992.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Bestandsaufnahme über die Situation des Datenschutzes „10 Jahre nach dem Volkszählungsurteil“ zustimmend zur Kenntnis genommen. Entschließung der 47. Konferenz am 9./10. März, 1994.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz. Entschließung der 48. Konferenz am 26./27. September, 1994.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich. Entschließung der 49. Konferenz am 9./10. März, 1995.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien. Entschließung der 50. Konferenz am 9./10. November, 1995.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Fehlende bereichsspezifische Regelungen bei der Justiz. Entschließung der 56. Konferenz am 5./6. Oktober, 1998.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten. Entschließung der 56. Konferenz am 5./6. Oktober, 1998.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften. Entschließung der 58. Konferenz am 7./8. Oktober, 1999.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Zum Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der EU. Entschließung der 58. Konferenz am 7./8. Oktober, 1999.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Veröffentlichung von Insolvenzinformationen im Internet. Entschließung vom 24. April (zwischen der 61. und 62. Konferenz), 2001.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzgerechtes eGovernment. Orientierungshilfe der Arbeitsgruppe „eGovernment“, 2003 ⟨URL: `http://www.bfdi.bund.de/cae/servlet/contentblob/417388/publicationFile/25251/eGovernment.pdf`⟩.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutz bei Dokumentenmanagementsystemen. Orientierungshilfe des Arbeitskreises „eGovernment“, 2006 ⟨URL: `http://www.bfdi.bund.de/cae/servlet/contentblob/417368/publicationFile/25256/OrientierungshilfeDMS.pdf`⟩.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutz beim vorgesehenen Bürgerportal unzureichend. Entschließung vom 16. April (zwischen der 77. und 78. Konferenz), 2009.

Klaus König: Öffentliches Management und Governance als Verwaltungskonzepte. DÖV, 2001, 617.

Peter Krause: Das Recht auf informationelle Selbstbestimmung – BVerfGE 65, 1. JuS, 1984, 268.

Georg Kristoferitsch: Digital Money – Electronic Cash – Smart Cards – Chancen und Risiken des Zahlungsverkehrs via Internet. Wien: Ueberreuter, 1998.

Thomas Krüger: Das Justizkommunikationsgesetz – weitere Schritte zum ‚elektronischen Rechtsverkehr‘. ZVI, 2004, 162.

Thomas Krüger/Michael Bütter: Justitia goes online! – Elektronischer Rechtsverkehr im Zivilprozess. MDR, 2003, 181.

Rolf Krumsiek: Die unendliche Geschichte des Justizmitteilungsgesetzes. DVBl, 1993, 1229.

Renate Künast: „Meine Daten gehören mir“ – und der Datenschutz gehört ins Grundgesetz. ZRP, 2008, 201.

Joachim Kuntze et al.**:** Grundbuchrecht – Kommentar zur Grundbuchordnung und Grundbuchverfügung einschließlich Wohnungseigentumsgrundbuchverfügung. 6. Auflage. Berlin: De Gruyter, 2006.

Martin Kutscha: Mehr Schutz von Computerdaten durch ein neues Grundrecht? NJW, 2008, 1042.

Ralf Laghzaoui/Volkmar Wirges: Anwaltshaftung bei Verwendung von Internet und Telefax. AnwBl, 1999, 253.

Landesbeauftragter für den Datenschutz Baden-Württemberg: 18. Tätigkeitsbericht. 1997.

Landesbeauftragter für den Datenschutz Baden-Württemberg: 19. Tätigkeitsbericht. 1998.

Landesbeauftragter für den Datenschutz Baden-Württemberg: 20. Tätigkeitsbericht. 1999.

Landesbeauftragter für den Datenschutz Bayern: 16. Tätigkeitsbericht. 1994.

Landesbeauftragter für den Datenschutz Bayern: 17. Tätigkeitsbericht. 1996.

Landesbeauftragter für den Datenschutz Niedersachsen: Auftragsdatenverarbeitung – Orientierungshilfe und Checkliste. 2002 ⟨URL: `http://www.lfd.niedersachsen.de/ps/tools/download.php?file=/live/institution/dms/mand_48/psfile/docfile/76/C1333914_L4be914079fdcf.pdf`⟩.

Landesbeauftragter für den Datenschutz Rheinland-Pfalz: 11. Tätigkeitsbericht. 1987.

Landesbeauftragter für den Datenschutz Rheinland-Pfalz: 15. Tätigkeitsbericht. 1995.

Landesbeauftragter für den Datenschutz Rheinland-Pfalz: 16. Tätigkeitsbericht. 1997.

Landesbeauftragter für den Datenschutz Rheinland-Pfalz: 19. Tätigkeitsbericht. 2003.

Landesbeauftragter für den Datenschutz Rheinland-Pfalz: 22. Tätigkeitsbericht. 2009.

Friedrich Lappe: Das neue Schuldnerverzeichnis. NJW, 1994, 3067.

Friedrich Lappe: Die neue Schuldnerverzeichnisverordnung. NJW, 1995, 1657.

Thomas Lappe: Brauchen wir De-Mail und Bürgerportale? DuD, 2009, 651.

Walter Leisner: Das neue Kommunikationsgrundrecht – Nicht Alibi für mehr, sondern Mahnung zu weniger staatlicher Überwachung. NJW, 2008, 2902.

Brita Lepa: Insolvenzordnung und Verfassungsrecht: eine Untersuchung der Verfassungsmäßigkeit der InsO und der Einwirkung verfassungsrechtlicher Wertungen auf die Einwendungen dieses Gesetzes. Dissertation, Universität Bonn, 2002.

Jürgen Leue: Einsichtsrechte in öffentliche Register. In: **Max Vollkommer** (Hrsg.), Datenverarbeitung und Persönlichkeitsschutz. Erlangen: Universitätsbund Erlangen-Nürnberg, 1986, 83.

Kai von Lewinski: Kaufleute im Schutzbereich des BDSG. DuD, 2000, 39.

Kai von Lewinski: Anwaltliche Schweigepflicht und E-Mail. BRAK-Mitt. 2004, 12.

Brigitta Liebscher: Datenschutz bei der Datenübermittlung im Zivilverfahren. Dissertation, Universität Köln, 1994.

Werner Liedtke: Das Bundesdatenschutzgesetz: eine Fallstudie zum Gesetzgebungsprozess. Dissertation, Universität München, 1980.

Dirk Lindloff: E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten. Dissertation, Universität Münster, 2005.

Oliver Löwe-Krahl: § 116 AO: Eine zu Unrecht vergessene Vorschrift. PStR, 2005, 235.

Jörn von Lucke/Heinrich Reinermann: Speyerer Definition von Electronic Government. 2000 ⟨URL: `http://foev.dhv-speyer.de/ruvii/SP-EGov.pdf`⟩.

Otto Mallmann: Zielfunktionen des Datenschutzes – Schutz der Privatsphäre – Korrekte Information. Neuwied: Luchterhand Verlag GmbH, 1995.

Gerrit Manssen et al. (Hrsg.)**:** Das neue Computergrundrecht. Berlin: LIT Verlag, 2009.

Herbert Mayer: Die Automation des gerichtlichen Mahnverfahrens. NJW, 1983, 92.

Christian Mensching: Veröffentlichungspflicht und Veröffentlichungsanspruch bei gerichtlichen Entscheidungen. AfP, 2007, 534.

Regina Meyer/Holger Brocks/Christine Nordmann: Gericht kontra Datenschutz: Kein strafrechtlicher Schutz mehr für Fahrzeughalterdaten? RDV, 2000, 11.

Wolfgang Michel: Publikations- und Zitierverhalten bei Gerichtsentscheidungen. JurPC, 1994, 2559.

Anja Miedbroth: Besondere Datenschutzpflichten. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 715.

Katja Mihm: Datenschutzaufsicht durch den Landesbeauftragten für den Datenschutz und Aufsichtsbehörde im Notariat. NJW, 1998, 1591.

Franz Mohr: Die österreichischen Insolvenzen im Internet. ZIP, 2000, 997.

Ingo von Münch/Philip Kunig: Grundgesetz-Kommentar, Bd. 3: Art. 70 bis Art. 146 und Gesamtregister. 3. Auflage. München: C.H. Beck, 2003.

Wolfgang Münzberger: Reform der Zwangsvollstreckung in das bewegliche Vermögen. Rpfleger, 1987, 269.

Hans-Joachim Musielak: Kommentar zur Zivilprozessordnung. 7. Auflage. München: Franz Vahlen, 2009.

John G. Myers/Marshall T. Rose: Post Office Protocol – Version 3. RFC 1939, 1996 ⟨URL: `http://www.ietf.org/rfc/rfc1939.txt`⟩.

Jörg Nerlich/Volker Römermann: Kommentar zur Insolvenzordnung. 18. Auflage. München: C.H. Beck, 2010.

Rüdiger Nierwetberg: Strafanzeige durch das Gericht. NJW, 1996, 432.

Ulrich Noack: Online-Unternehmensregister in Deutschland und Europa – Bemerkungen zum Regierungsentwurf eines ERJuKoG. BB, 2001, 1261.

Ulrich Noack: Das EHUG ist beschlossen – elektronisches Handels- und Unternehmensregister ab 2007. NZG, 2006, 801.

Eckhard Pache: Die Europäische Grundrechtecharta. EuR, 2001, 475.

Eckhard Pache/Franziska Rösch: Der Vertrag von Lissabon. NVwZ, 2008, 473.

Ansgar Pallasky: Datenschutz in Zeiten globaler Mobilität. DuD, 2007, 181.

Gerhard Pape: Änderungen im eröffneten Verfahren durch das Gesetz zur Vereinfachung des Insolvenzverfahrens. NZI, 2007, 480.

Oliver Plöckinger/Dieter Duursma/Günther Helm (Hrsg.)**:** Aktuelle Entwicklungen im Internet-Recht: Beiträge zur zivil-, straf- und verwaltungsrechtlichen Diskussion. Wien: Neuer Wissenschaftlicher Verlag, 2002.

Adalbert Podlech: Verfassungsrechtliche Probleme öffentlicher Informationssysteme. DVR, 1972/73, 149.

Adalbert Podlech: Datenschutz in der Verwaltung. DVR Beiheft 1, 1973, 2.

Adalbert Podlech: Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeit unbegrenzter Informationsverarbeitung mittels Technik. Leviathan, 1984, 85.

Jon Postel: User Datagram Protocol. RFC 768, 1980 ⟨URL: `http://www.ietf.org/rfc/rfc768.txt`⟩.

Jon Postel: Internet Protocol. RFC 791, 1981 ⟨URL: `http://www.ietf.org/rfc/rfc791.txt`⟩.

Jon Postel: Transmission Control Protocol. RFC 793, 1981 ⟨URL: `http://www.ietf.org/rfc/rfc793.txt`⟩.

Jon Postel/Joyce Reynolds: File Transfer Protocol (FTP). RFC 959, 1985 ⟨URL: `http://www.ietf.org/rfc/rfc0959.txt`⟩.

Thomas Probst: Bürgerportale – geprüfte statt gefühlte Sicherheit. DSB, 2009, 16.

Hanns Prütting: Datenschutz und Zivilverfahrensrecht in Deutschland. ZZP, 1993, 427.

Helmut Redeker: Datenschutz und Mandantenschutz in der Anwaltskanzlei. In: **Ralf B. Abel** (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz. 2. Auflage. München: C.H. Beck, 2003, 43.

Helmut Redeker: Elektronische Kommunikation mit der Justiz – eine Herausforderung für die Anwaltschaft. AnwBl, 2005, 348.

Herbert Reichl/Alexander Roßnagel/Günter Müller (Hrsg.)**:** Digitaler Personalausweis. Wiesbaden: Deutscher Universitäts-Verlag, 2005.

Andreas Reisen: Digitale Identität im Scheckkartenformat. DuD, 2008, 1.

Jan Riebeling: Der Einsatz von Informations- und Kommunikationstechnologie im Insolvenzverfahren. Dissertation, Universität Kiel, 2005.

Gerhard Robbers: Der Grundrechtsverzicht. JuS, 1985, 925.

Alexander Roßnagel: Die rechtliche Verantwortung technischer Risiken. UPR, 1986, 46.

Alexander Roßnagel: Die parlamentarische Verantwortung für den technischen Fortschritt. ZRP, 1992, 55.

Alexander Roßnagel: Das Signaturgesetz. DuD, 1997, 75.

Alexander Roßnagel: Das Signaturgesetz jetzt verbessern und verabschieden. DuD, 1997, 287.

Alexander Roßnagel: Das Gesetz und die Verordnung zur digitalen Signatur – Entstehung und Regelungsgehalt. RDV, 1998, 5.

Alexander Roßnagel: Europäische Signaturrichtlinie und Optionen ihrer Umsetzung. MMR, 1999, 261.

Alexander Roßnagel: Das neue Signaturgesetz nach zwei Jahren. NJW, 1999, 1591.

Alexander Roßnagel: Auf dem Weg zu neuen Signaturregelungen. MMR, 2000, 451.

Alexander Roßnagel: Das neue Recht elektronischer Signaturen. NJW, 2001, 1817.

Alexander Roßnagel: Das neue Signaturgesetz – Grundlage des elektronischen Rechtsverkehrs. MMR, 2001, 201.

Alexander Roßnagel: Das neue Signaturgesetz. BB, 2002, 261.

Alexander Roßnagel: Rechtliche Unterschiede von Signaturverfahren. MMR, 2002, 215.

Alexander Roßnagel: Datenschutz im Signaturverfahren. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 1210.

Alexander Roßnagel (Hrsg.)**:** Handbuch Datenschutzrecht. München: C.H. Beck, 2003.

Alexander Roßnagel: Elektronische Signaturen mit der Bankkarte? NJW, 2005, 385.

Alexander Roßnagel: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung. MMR, 2005, 71.

Alexander Roßnagel (Hrsg.)**:** Recht der Multimedia-Dienste. 7. Auflage. München: C.H. Beck, 2005.

Alexander Roßnagel: Der elektronische Personalausweis als sichere Signaturerstellungseinheit. DuD, 2009, 403.

Alexander Roßnagel: Die Novellen zum Datenschutzrecht – Scoring und Adresshandel. NJW, 2009, 2716.

Alexander Roßnagel: Die Zukunft der informationellen Selbstbestimmung: Datenschutz ins Grundgesetz und Modernisierung des Datenschutzkonzepts. KJ, Beiheft 1 2009, 99.

Alexander Roßnagel: Verurteilung Deutschlands zur Neuorganisation seiner Datenschützer. EuZW, 2010, 299.

Alexander Roßnagel/Stefanie Fischer-Dieskau: Automatisiert erzeugte elektronische Signaturen. MMR, 2004, 133.

Alexander Roßnagel/Stefanie Fischer-Dieskau/Silke Jandt: Handlungsleitfaden zur Aufbewahrung elektronischer oder elektronisch signierter Dokumente. Bundesministerium für Wirtschaft und Technologie, 2007.

Alexander Roßnagel et al.**:** Scannen von Papierdokumenten – Anforderungen und Empfehlungen. Baden-Baden: Nomos, 2007.

Alexander Roßnagel et al.**:** Erneuerung elektronischer Signaturen – Grundfragen der Archivierung elektronischer Dokumente. CR, 2003, 301.

Alexander Roßnagel/Stefanie Fischer-Dieskau/Daniel Wilke: Transformation von Dokumenten – Zur Notwendigkeit einer Technik- und Rechtsgestaltung. CR, 2005, 903.

Alexander Roßnagel/Rotraud Gitter: Signaturrechtliche Anforderungen. In: **Herbert Reichl/Alexander Roßnagel/Günter Müller** (Hrsg.), Digitaler Personalausweis. Wiesbaden: Deutscher Universitäts-Verlag, 2005, 91.

Alexander Roßnagel/Gerrit Hornung: Ein Ausweis für das Internet. DÖV, 2009, 301.

Alexander Roßnagel et al.**:** De-Mail und Bürgerportale. DuD, 2009, 728.

Alexander Roßnagel/Gerrit Hornung/Christoph Schnabel: Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht. DuD, 2008, 168.

Alexander Roßnagel/Silke Jandt: Handlungsleitfaden zum Scannen von Papierdokumenten. Bundesministerium für Wirtschaft und Technologie, 2008.

Alexander Roßnagel/Philip Laue: Zweckbindung im Electronic Government. DÖV, 2007, 543.

Alexander Roßnagel/Andreas Pfitzmann: Der Beweiswert von E-Mails. NJW, 2003, 1209.

Alexander Roßnagel/Andreas Pfitzmann/Hans-Jürgen Garstka: Modernisierung des Datenschutzes. DuD, 2001, 253.

Alexander Roßnagel/Andreas Schmidt/Daniel Wilke: Rechtssichere Transformation signierter Dokumente – Anforderungen, Konzepte und Umsetzung. Baden-Baden: Nomos, 2009.

Alexander Roßnagel/Christoph Schnabel: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. NJW, 2008, 3534.

Alexander Roßnagel/Philip Scholz: Datenschutz durch Anonymität und Pseudonymität. MMR, 2000, 721.

Christoph Rottwilm: Die unheimliche Macht der Datendealer. Manager Magazin, 2008 ⟨URL: `http://www.manager-magazin.de/geld/geldanlage/0,2828,552042,00.html`⟩ – Zugriff am 20.1.2010.

Giselher Rüpke: Das spezifische Datenschutzrecht des Notars. NJW, 1991, 568.

Giselher Rüpke: Freie Advokatur, anwaltliche Informationsverarbeitung und Datenschutzrecht. München: C.H. Beck, 1995.

Giselher Rüpke: Datenschutz, Mandatsgeheimnis und anwaltliche Kommunikationsfreiheit. NJW, 2008, 1121.

Giselher Rüpke: Mehr Rechtssicherheit für anwaltliche Datenverarbeitung – Ein Vorschlag zur informationsrechtlichen Ergänzung der Bundesrechtsanwaltsordnung. ZRP, 2008, 87.

Peter Schaar: Datenschutzrechtliche Einwilligung im Internet. MMR, 2001, 644.

Christoph Schaefer: ELENA: Vorphase des Gesetzgebungsverfahrens für den Elektronischen Einkommensnachweis beginnt. MMR, 2006, X.

Christoph Schaefer: Verbesserter Grundrechtsschutz durch ein elektronisches Bescheinigungsverfahren. ZRP, 2006, 93.

Hans-Jürgen Schaffland/Noeme Wiltfang: Bundesdatenschutzgesetz. Berlin: Erich Schmidt, 2009.

Uwe J. Scherf/Hans-Peter Schmieszek/Wolfram Viefhues (Hrsg.)**:** Elektronischer Rechtsverkehr: Kommentar und Handbuch. Heidelberg: C.F. Müller Verlag, 2006.

Hans-Hermann Schild: Behördlicher Datenschutzbeauftragter. DuD, 2001, 31.

Eberhard Schilken: Zur Reform der Sachaufklärung in der Zwangsvollstreckung. Rpfleger, 2006, 629.

Jochen N. Schlotter: Das EHUG ist in Kraft getreten: Das Recht der Unternehmenspublizität hat eine neue Grundlage. BB, 2007, 1.

Walter Schmidt: Die bedrohte Entscheidungsfreiheit. JZ, 1974, 241.

Werner Schmidt: Die Grenzen datenschutzrechtlicher Kontrolle in der Rechtspflege. RDV, 1995, 215.

Edzard Schmidt-Jortzig: Die Gestattung der Einsichtnahme und die Erteilung von Abschriften des Vermögensverzeichnisses im Offenbarungsverfahren. JurBüro, 1970, 445.

Hans-Peter Schmieszek: Zivilprozessordnung. In: **Uwe J. Scherf/Hans-Peter Schmieszek/Wolfram Viefhues** (Hrsg.), Elektronischer Rechtsverkehr: Kommentar und Handbuch. Heidelberg: C.F. Müller Verlag, 2006, 24.

Jörn Schnigula: Das Offenbarungsverfahren – Darstellung und Reform der Sachaufklärung in der Zwangsvollstreckung. Dissertation, Universität Bonn, 2001.

Günther Schnupp: Übermittlung personenbezogener Daten durch die Justiz. PersV, 1998, 110.

Rudolf Schomerus: Datenschutz oder Datenverkehrsordnung. ZRP, 1981, 291.

Hendrik Schöttle: Datenschutz. In: **Uwe J. Scherf/Hans-Peter Schmieszek/ Wolfram Viefhues** (Hrsg.), Elektronischer Rechtsverkehr: Kommentar und Handbuch. Heidelberg: C.F. Müller Verlag, 2006, 176.

Andreas Schulz: Die Rechte des Hinterlegers einer Schutzschrift. WRP, 2009, 1472.

Anika D. Schulz/Sönke E. Schulz: eDaseinsvorsorge – Neuorientierung des überkommenen Rechtsbegriffs „Daseinsvorsorge“ im Zuge technischer Entwicklungen. MMR, 2009, 19.

Sönke E. Schulz: Der neue „E-Personalausweis“ – elektronische Identitätsnachweise als Motor des E-Government, E-Commerce und des technikgestützten Identitätsmanagement? CR, 2009, 267.

Helmuth Schulze-Fielitz/Carsten Schütz (Hrsg.)**:** Justiz und Justizverwaltung zwischen Ökonomisierungsdruck und Unabhängigkeit. Berlin: Duncker & Humblot, 2002.

Jürgen Schwarzer: Auf dem Weg zu einer europäischen Verfassung – Wechselwirkungen zwischen europäischem und nationalem Recht. DVBl, 1999, 1677.

Max Schwoerer: Die elektronische Justiz: Ein Beitrag zum elektronischen Rechtsverkehr und zur elektronischen Akte unter Berücksichtigung des Justizkommunikationsgesetzes. Dissertation, Universität Tübingen, 2005.

Ulrich Seibert/Daniela Decker: Das Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister – der Big Bang im Recht der Unternehmenspublizität. DB, 2006, 2446.

Ulrich Seibert/Frauke Wedemann: Der Schutz der Privatanschrift im elektronischen Handels- und Unternehmensregister. GmbHR, 2007, 17.

Wolfgang Seiler: Zur datenschutzrechtlichen Kontrolle notarieller Daten. DNotZ, 2002, 693.

Theo Seip: Zur geplanten Reform der Sachaufklärung in der Zwangsvollstreckung – Eine Betrachtung zum gegenwärtigen Sachstand. DGVZ, 2008, 38.

Spiros Simitis: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. NJW, 1984, 394.

Spiros Simitis: 25 Jahre rheinland-pfälzisches Landesdatenschutzgesetz. Gastvortrag beim Landesbeauftragten für den Datenschutz Rheinland-Pfalz, 1999 ⟨URL: `http://www.datenschutz.rlp.de/de/ds.php?submenu=hist&typ=Simitis`⟩ – Zugriff am 20.1.2010.

Spiros Simitis (Hrsg.)**:** Bundesdatenschutzgesetz. Baden-Baden: Nomos, 2006, 6. Auflage.

Spiros Simitis/Gerhard Fuckner: Informationelle Selbstbestimmung und „staatliches Geheimhaltungsinteresse". NJW, 1990, 2713.

Heike Stach: Mit Bürgerportalen für einfach sichere, vertrauliche und verbindliche elektronische Kommunikation. DuD, 2008, 184.

Astrid Stadler: Der Zivilprozess und neue Formen der Informationstechnik. ZZP, 2002, 413.

Josef Stamm: Das zentrale Schuldnerverzeichnis. ZRP, 2003, 95.

Josef Stamm: Das zentrale Schuldnerverzeichnis – ein dringender Bedarf. InVo, 2003, 51.

Josef Stamm: Das zentrale Schuldnerverzeichnis – ein dringender Bedarf. KKZ, 2003, 154.

Christian Starck: Bilanzpublizität und Datenschutz. DStR, 2008, 2035.

Statistisches Bundesamt: Private Haushalte in der Informationsgesellschaft – Nutzung der Informations- und Kommunikationstechnlogie. 2009 ⟨URL: `https://www-ec.destatis.de/csp/shop/sfg/bpm.html.cms.cBroker.cls?cmspath=struktur,vollanzeige.csp&ID=1025074`⟩.

Friedrich Stein/Martin Jonas: Kommentar zur Zivilprozessordnung. Tübingen: Mohr Siebeck, 2005, 22. Auflage.

Wilhelm Steinmüller: Das Volkszählungsurteil des Bundesverfassungsgerichts. DuD, 1984, 85.

Wilhelm Steinmüller et al.**:** Grundfragen des Datenschutzes – Gutachten im Auftrag des Bundesministerium des Innern. Drucksache 6/3826, 1971.

Werner Sternal: „Versteckte" Änderungen insolvenzrechtlicher Vorschriften. NZI, 2008, 158.

Kurt Stöber (Hrsg.)**:** Zwangsversteigerungsgesetz. München: C.H. Beck, 2009, 19. Auflage.

Moritz Strasser et al.**:** Kosten und Umsetzungsmodelle. In: **Herbert Reichl/Alexander Roßnagel/Günter Müller** (Hrsg.), Digitaler Personalausweis. Wiesbaden: Deutscher Universitäts-Verlag, 2005, 243.

Gabriele Straub: Das Schuldnerverzeichnis unter besonderer Berücksichtigung des Datenschutzes. Dissertation, Universität Regensburg, 1995.

Jürgen Stüwe: Elektronischer Entgeltnachweis (ELENA) kommt 2010. sj, 2009, 45.

Robert Suermann: Schöne (?) neue Welt – die elektronische Akte. DRiZ, 2001, 291.

Bartosz Sujecki: Das Online-Mahnverfahren in Deutschland. MMR, 2006, 369.

Andrew S. Tanenbaum: Computernetzwerke. 4. Auflage. München: Pearson Studium, 2003.

Armin Teschner: Die Veröffentlichung von Gerichtsentscheidungen. SchlHA, 2008, 191.

Marie-Theres Tinnefeld: Geschützte Daten. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 485.

Heinz Vallander/Karlhans Fuchs: Ein großer Wurf? Anmerkungen zum Diskussionsentwurf des BMJ. NZI, 2003, 292.

Wolfram Viefhues: Insolvenzmitteilungen aus Nordrhein-Westfalen im Internet. MMR, 2002, XIII.

Wolfram Viefhues: Referentenentwurf des Justizkommunikationsgesetzes – Auf dem Weg zur elektronischen Gerichtsakte. CR, 2003, 541.

Wolfram Viefhues: Grundzüge der elektronischen Kommunikation und der Aktenbearbeitung. In: **Uwe J. Scherf/Hans-Peter Schmieszek/Wolfram Viefhues** (Hrsg.), Elektronischer Rechtsverkehr: Kommentar und Handbuch. Heidelberg: C.F. Müller Verlag, 2006, 3.

Wolfram Viefhues: Justiz. In: **Uwe J. Scherf/Hans-Peter Schmieszek/Wolfram Viefhues** (Hrsg.), Elektronischer Rechtsverkehr: Kommentar und Handbuch. Heidelberg: C.F. Müller Verlag, 2006, 145.

Wolfram Viefhues/Karl-Heinz Volesky: Elektronischer Rechtsverkehr – Ziele, Probleme und Chancen. TKMR, 2003, 245.

Max Vollkommer: Formstrenge und prozessuale Billigkeit dargestellt am Beispiel der prozessualen Schriftform: Zur Überwindung des Formalismus in der Rechtsprechung. Dissertation, Universität München, 1973.

Max Vollkommer (Hrsg.)**:** Datenverarbeitung und Persönlichkeitsschutz. Erlangen: Universitätsbund Erlangen-Nürnberg, 1986.

Max Vollkommer: Formzwang und Formzweck im Prozessrecht: Zum Ruf nach einer Überprüfung und Neubestimmung der Erfordernisse der prozessualen Schriftlichkeit für alle Teilrechtsordnungen. In: **Günter Brambring/Dieter Medicus/Max Vogt** (Hrsg.), Festschrift für Horst Hagen. Köln: RWS Verlag Kommunikationsforum, 1999, 49.

Ulrich Vultejus: Das Datengeheimnis des Richters. ZRP, 1996, 329.

Ulrich Vultejus: Das Datengeheimnis des Richters. ZRP, 1997, 386.

Carsten Wahlmann: JobCard. In: **Uwe J. Scherf/Hans-Peter Schmieszek/Wolfram Viefhues** (Hrsg.), Elektronischer Rechtsverkehr: Kommentar und Handbuch. Heidelberg: C.F. Müller Verlag, 2006, 169.

Norbert Warga: Das Elena-Konzept. DuD, 2010, 216.

Norbert Warga: ELENA-Verfahren zum elektronischen Entgeltnachweis. PersR, 2010, 111.

Thomas Warnecke: Das Bürgerportalgesetz. MMR, 2010, 227.

Albrecht Weber: Die Europäische Grundrechtscharta – auf dem Weg zu einer europäischen Verfassung. NJW, 2000, 537.

Martina Weber: EG-Datenschutzrichtlinie. CR, 1995, 297.

Peter Wedde: ELENA. AiB, 2010, 143.

Peter Wedde: ELENA – Meilenstein zum Bürokratieabbau oder Stolperstein für das Persönlichkeitsrecht? ArbuR, 2010, 94.

Peter Wedde: Elena und Sozialleistungen – Funktionen und (rechtliche) Probleme des neuen Datenerhebungs-Verfahrens. SozSich, 2010, 73.

Thilo Weichert: Datenschutz. In: **Wolfgang Kilian/Benno Heussen** (Hrsg.), Computerrechtshandbuch. München: C.H. Beck, 2009, 130.

Thilo Weichert: Datenschutz auch bei Anwälten? NJW, 2009, 550.

Dennis Werner/Christoph Wegener: Bürgerportale. CR, 2009, 310.

Marcus Werner: Elektronische Datenverarbeitung und Zivilprozess: Datenschutz und Datensicherung bei der Anwendung elektronischer Datenverarbeitung im Zivilprozess. Dissertation, Universität Bonn, 1995.

Marcus Werner: Die Kontrolle des Datenschutzes bei den Zivilgerichten. RDV, 1996, 232.

Marcus Werner: Datenschutz im Zivil- und Verwaltungsprozess. In: **Alexander Roßnagel** (Hrsg.), Handbuch Datenschutzrecht. München: C.H. Beck, 2003, 1419.

Raimund Weyand: Anzeige einer Steuerstraftat durch öffentliche Stellen – Die aktuelle Fassung des § 116 Abs. 1 AO. Information StW, 2007, 397.

Daniel Wilke et al.**:** Eine Beweisführung von Format – Die Transformation signierter Dokumente auf dem Prüfstand. CR, 2008, 607.

Klaus Wimmerer: Gesetzentwurf zur Vereinfachung des Insolvenzverfahrens. DB, 2006, 233.

Christine Windbichler: Handelsrechtliche Publizität durch private Datenverbreiter. CR, 1988, 447.

Harald Wollweber: Iustitias langer Arm – Analyse und Kritik des Justizmitteilungsgesetzes. NJW, 1997, 2488.

Dietmar Wullweber: Justizmitteilungsgesetz (JuMiG) und Neufassung der Anordnung über Mitteilungen in Zivilsachen. SchlHA, 1999, 69.

Dietmar Wullweber: Datenschutz im Zivilprozess – einschließlich der Verfahren der freiwilligen Gerichtsbarkeit. In: **Ralf B. Abel** (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz. 2. Auflage. München: C.H. Beck, 2003, 157.

Nuriye Yildirim: Datenschutz im Electronic Government. Dissertation, Universität Kassel, 2004.

Michael Zabel: Datenschutz in der Justiz. RpflStud, 1999, 65.

Martin Zilkens: Datenschutz im Pass- und Personalausweiswesen. RDV, 2010, 14.

Richard Zöller: Zivilprozessordnung. 28. Auflage. Köln: Dr. Otto Schmidt, 2010.

Brigitte Zypries: 10 Punkte für eine bessere Justiz dank eJustice. Rede anlässlich der CeBIT, 2007 ⟨URL: `http://www.bmj.de/enid/6423c0bcbeae9f31c9bc6b3f4c1935eb,898fb56d6f6465092d09093a09636f6e5f6964092d0934303636/Pressemitteilungen_und_Reden/Pressemitteilungen_58.html`⟩.

Für die Justiz hat der Gesetzgeber jüngst zahlreiche Vorschriften zur Modernisierung von Verfahrensabläufen erlassen, die zu neuartigen Herausforderungen für den Datenschutz führen.

In dieser Arbeit werden erstmals datenschutzrechtliche Fragestellungen der elektronischen Justiz identifiziert und bewertet. Die Untersuchung erfolgt am Beispiel des Bundesgerichtshofs und der ordentlichen Gerichtsbarkeit von Rheinland-Pfalz. Sie berücksichtigt die neuen Verfahrensabläufe im Zivilverfahren, dem Zwangsvollstreckungsverfahren, dem Zwangsversteigerungsverfahren, dem Insolvenzverfahren, der Grundbuchordnung und dem Handelsgesetzbuch.

Es zeigt sich, dass besonderes Augenmerk auf die datenschutzkonforme Ausgestaltung gerichtlicher Veröffentlichungen und die Vertraulichkeit und Authentizität elektronischer Kommunikation im Internet zu richten ist.

ISBN 978-3-89958-962-7