*Stefan Drackert*

# Die Risiken der Verarbeitung personenbezogener Daten

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

# Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

in Fortführung der Reihe
„Beiträge und Materialien aus dem Max-Planck-Institut
für ausländisches und internationales Strafrecht Freiburg“
begründet von Albin Eser

Band S 149

Max-Planck-Institut für ausländisches
und internationales Strafrecht

# Die Risiken der Verarbeitung personenbezogener Daten

## Eine Untersuchung zu den Grundlagen des Datenschutzrechts

Stefan Drackert


Duncker & Humblot · Berlin

Bibliografische Information der Deutschen Nationalbibliothek

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

DOI https://doi.org/10.30709/978-3-86113-806-8


Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany

ISSN 1860-0093
ISBN 978-3-86113-806-8 (Max-Planck-Institut)
ISBN 978-3-428-14730-4 Duncker & Humblot)
Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706

„Derjenige, welcher der Sichtbarkeit unterworfen ist und dies weiß,
übernimmt die Zwangsmittel der Macht und spielt sie gegen sich selber aus;
er internalisiert das Machtverhältnis, in welchem er gleichzeitig
beide Rollen spielt; er wird zum Prinzip seiner eigenen Unterwerfung.“

*Michel Foucault*, Überwachen und Strafen, S. 260

“I do not want to live in a world where everything I do and say is recorded.”

*Edward Snowden* im Interview des Guardian vom 10. Juni 2013

# Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2014 von der Rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg als Dissertation angenommen. Sie entstand überwiegend während meiner Zeit am Max-Planck-Institut für ausländisches und internationales Strafrecht neben meiner Tätigkeit als Referatsleiter für die Nordischen Länder und Lehrassistent im Öffentlichen Recht an der Universität. Gesetzgebung, Literatur und Rechtsprechung sind auf dem Stand vom 25. Juli 2013; einzelne Aktualisierungen konnten noch zum 24. Mai 2014 eingearbeitet werden.

Mein Dank gilt dem Betreuer dieser Arbeit, Herrn Prof. Dr. Dr. h.c. mult. *Ulrich Sieber*, für die zahlreichen Anregungen, die Förderung des Projekts und die hervorragenden Arbeitsbedingungen am Institut. Herrn Prof. Dr. Dr. h.c. *Hans-Jörg Albrecht* danke ich für die schnelle Erstellung des Zweitgutachtens.

Herzlich danke ich meinen Kollegen am Max-Planck-Institut für ausländisches und internationales Strafrecht, insbesondere Herrn Dr. *Emmanouil Billis*, LL.M., Frau Dr. *Brigitte Michel*, Herrn Rechtsanwalt *Nikolas von zur Mühlen*, Frau Dr. *Svetlana Paramonova*, LL.M. und Herrn Rechtsanwalt Dr. *Harald Weiß*, Maître en Droit. Besonderer Dank gilt auch meinen Kollegen aus den Länderreferaten, dem gesamten Bibliotheksteam des Instituts und auch meinen Kollegen im Lehrassistententeam der Universität und von den Lehrstühlen, insbesondere Frau Assessorin *Sabine Stampf* und Herrn Dr. *Nikolaus Marsch*, D.I.A.P. (ENA) für die hervorragende Arbeitsatmosphäre sowie den fachlichen und persönlichen Austausch.

Frau *Anastasia Mozgalina*, Herrn Assessor *Simon Lauck* und Herrn Rechtsanwalt Dr. *Harald Weiß* danke ich zusätzlich für die Durchsicht von Manuskriptauszügen und die hierzu gegebenen Anregungen. Herrn *Matthias Rawert* danke ich für die sorgfältige Arbeit als Lektor und die gute Zusammenarbeit bei der Drucklegung.

Ich widme diese Arbeit aus ganzem Herzen meinen Eltern, meinem Bruder und meiner Verlobten, *Anastasia Mozgalina*, für all ihre Liebe und Unterstützung.

Berlin, im Mai 2014 *Stefan Drackert*

# Inhaltsübersicht

# Inhaltsverzeichnis

## Teil 3
## Deutsches Recht

# Abkürzungsverzeichnis

| | |
|---|---|
| a.A. | anderer Ansicht |
| a.D. | außer Dienst |
| a.F. | alte Fassung |
| a.M. | am Main |
| ABl. | Amtsblatt |
| Abs. | Absatz |
| AcP | Archiv für die civilistische Praxis |
| ADHS | Aufmerksamkeitsdefizit-/Hyperaktivitätsstörung |
| AEMR | Allgemeine Erklärung der Menschenrechte (Resolution 217 A (III) der Generalversammlung der VN vom 10.12.1948) |
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union (in der Fassung der Bekanntmachung vom 9.5.2008; ABl. 2008 Nr. C 115 S. 47) |
| AFAPDP | Association francophone des autorités de protection des données |
| Anm. | Anmerkung |
| APEC | Asia-Pacific Economic Cooperation |
| APIS | Advanced Passenger Information System |
| App. | Application |
| AöR | Archiv des öffentlichen Rechts |
| Art. | Artikel |
| ASEAN | Association of South East Asian Nations |
| ASNEF | Asociación Nacional de Entidades de Financiación |
| ATDG | Antiterrordateigesetz |
| BBG | Bundesbeamtengesetz |
| BBK | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe |
| Bd. | Band |
| BDSG | Bundesdatenschutzgesetz |
| BeckRS | Beck'sche Rechtsprechungssammlung |
| BfLE | Bundesanstalt für Landwirtschaft und Ernährung |
| BGB | Bürgerliches Gesetzbuch |
| BGHZ | Entscheidungen des Bundesgerichtshofs in Zivilsachen |

| | |
|---|---|
| BITKOM | Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. |
| BMI | Bundesministerium des Innern |
| bpb | Bundeszentrale für politische Bildung |
| BrB | Brottsbalken |
| BRD | Bundesrepublik Deutschland |
| BStU | Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik |
| BvR | Registerzeichen des BVerfG |
| BVerfG | Bundesverfassungsgericht |
| BVerfGE | Entscheidung des Bundesverfassungsgerichts |
| CBPR | Cross-Border Privacy Rules |
| CERN | Conseil Européen pour la Recherche Nucléaire |
| CLSR | Computer Law & Security Review |
| CM/Rec | Committee of Ministers/Recommendation |
| CoE | Council of Europe |
| CR | Computer und Recht |
| DARPA | Defense Advanced Research Projects Agency |
| D.C. | District of Columbia |
| DDR | Deutsche Demokratische Republik |
| d.h. | das heißt |
| DH./Exp. | Registerzeichen |
| DJT | Deutscher Juristentag |
| DNA | deoxyribonucleic acid |
| Doc. | Document |
| DÖV | Die öffentliche Verwaltung |
| DR | Decisions and Reports / Recueil des arrêts et décisions |
| Dr. | Doktor |
| Drs. | Drucksache |
| dt. | deutsch |
| DuD | Datenschutz und Datensicherheit |
| DVBl. | Deutsches Verwaltungsblatt |
| ebd. | ebenda |
| EG | Europäische Gemeinschaft |
| EGMR | Europäischer Gerichtshof für Menschenrechte |

| | |
|---|---|
| EGV | Vertrag zur Gründung der Europäischen Gemeinschaft (in der Fassung des Vertrags von Athen; ABl. C 321 E/2 vom 29.12.2006) |
| Einl. | Einleitung |
| EKMR | Europäische Kommission für Menschenrechte |
| E-KOM | Elektronische Kommunikation |
| E-Kom-Richtlinie | Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) |
| EMRK | Konvention zum Schutze der Menschenrechte und Grundfreiheiten des Europarats vom 4.11.1950, in Kraft getreten am 2.9.1953 (ETS No. 005) |
| ENISA | European Network and Information Security Agency |
| et al. | et alii |
| ETS | European Treaty Series |
| EU | Europäische Union |
| EU-DSGVO-E | Entwurf einer Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012. KOM(2012) 9 endgültig, S. 19 ff. |
| EU-DSRL-E | Entwurf einer Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr vom 25.1.2012 KOM(2012) 10 |
| eucrim | European Criminal Law Associations' Forum |
| EuG | Gericht der Europäischen Union |
| EU-GRC | Charta der Grundrechte der Europäischen Union (ABl. 2007 Nr. C 303 S. 1) |
| EuGRZ | Europäische Grundrechte-Zeitschrift |
| EuR | Europarecht |
| EuRat | Europarat |
| EUV | Vertrag über die Europäische Union (in der Fassung des Vertrags von Lissabon; ABl. 2008 Nr. C 111 S. 56 und ABl. 2009 Nr. C 290 S. 1) |
| EUV a.F. | Vertrag über die Europäische Union (in der Fassung des Vertrags von Athen; ABl. C 321 E/2 vom 29.12.2006). |
| FES | Friedrich-Ebert-Stiftung |
| FS | Festschrift |

| | |
|---|---|
| G 10 | Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) |
| GA | Generalanwalt/-anwältin, Goltdammer's Archiv |
| GASP | Gemeinsame Außen- und Sicherheitspolitik |
| GATT | General Agreement on Tarifs and Trade |
| GATS | General Agreement on Trade in Services |
| gem. | gemäß |
| Gestapo | Geheime Staatspolizei |
| GG | Grundgesetz |
| ggf. | gegebenenfalls |
| GPS | Global Positioning System |
| GRCh | Charta der Grundrechte der Europäischen Union |
| GV-Vorschlag | Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11 endgültig vom 25.01.2012. |
| Harv. L. Rev. | Harvard Law Review |
| HCR | UN Human Rights Committee |
| HEG | Handbuch der Europäischen Grundrechte |
| HRRS | Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht |
| Hrsg. | Herausgeber |
| i.Br. | im Breisgau |
| IKT | Informations- und Kommunikationstechnologie |
| ILO | International Labour Organization |
| ILS | International Labour Office |
| IM | Inoffizieller Mitarbeiter des Ministeriums für Staatssicherheit der DDR |
| insb. | insbesondere |
| IntKommEMRK | Internationaler Kommentar zur Europäischen Menschenrechtskonvention |
| IPBürg | Internationaler Pakt über bürgerliche und politische Rechte (Resolution 2200A (XXI) der Generalversammlung der VN vom 16.12.1966. In Kraft getreten am 23.2.1976; von Deutschland ratifiziert am 17.12.1973, BGBl. 1973 II 1553) |
| IP-Adresse | Auf dem Internetprotokoll basierende Netzwerkadresse |
| IPv6 | Internet Protocol Version 6 |
| i.S.v. | im Sinne von |

| | |
|---|---|
| ITRB | IT-Rechtsberater |
| i.V.m. | in Verbindung mit |
| Jahrb. f. Dogm. | Jahrbücher für die Dogmatik des heutigen römischen und deutschen Privatrechts |
| JFT | Tidskrift utgiven av Juridiska Föreningen i Finland |
| JherJb. | Jherings Jahrbücher für die Dogmatik des heutigen römischen und deutschen Privatrechts |
| JIM | Jugend, Information, (Multi-) Media |
| JurisAnwZert ITR | Juris AnwaltZertifikatOnline IT-Recht |
| JurisPK-Internetrecht | Juris PraxisKommentar Internetrecht |
| JurisPR-IT-Recht | Juris PraxisReport Internetrecht |
| JuS | Juristische Schulung |
| JZ | Juristenzeitung |
| Kap./kap. | Kapitel/kapitel |
| KOM | Kommission |
| Konvention 108 | Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981, ETS No. 108 |
| KuR | Kommunikation und Recht |
| LDSG-BW | Landesdatenschutzgesetz Baden-Württemberg |
| LIBE | Ausschuss für bürgerliche Freiheiten, Justiz und Inneres |
| lit. | litera |
| MfS | Ministerium für Staatssicherheit |
| MMR | Multimedia und Recht |
| m.w.N. | mit weiteren Nachweisen |
| N.C.J.L. & Tech | North Carolina Journal of Law & Technology |
| NfD | Nachrichten für Dokumentation |
| NJOZ | Neue Juristische Online Zeitschrift |
| NJW | Neue Juristische Wochenschrift |
| Nr., No. | Nummer, Number |
| NSA | National Security Agency |
| NStZ | Neue Zeitschrift für Strafrecht |
| NVwZ | Neue Zeitschrift für Verwaltungsrecht |
| NZA | Neue Zeitschrift für Arbeitsrecht |
| NZM | Neue Zeitschrift für Miet- und Wohnungsrecht |

| | |
|---|---|
| OECD | Organisation for Economic Co-operation and Development |
| o.g. | oben genannt |
| ORF | Österreichischer Rundfunk |
| OSI | Other Service Request |
| PC | Personal Computer |
| PJZS | Polizeiliche und justizielle Zusammenarbeit in Strafsachen |
| PNAS | Proceedings of the National Academy of Sciences of the United States of America |
| PNR | Passenger Name Record |
| PUL | Personuppgiftslagen; SFS 1998:204 i.d.F.vom 29.4.1998, zuletzt geändert durch SFS 2010:1969 vom 16.12.2010 |
| RAF | Rote Armee Fraktion |
| RDV | Recht der Datenverarbeitung |
| RFID | Radiofrequencyidentification |
| RiVASt | Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten |
| RL | Richtlinie |
| Rn. | Randnummer |
| Rs. | Rechtssache |
| S. | Satz, Seite |
| SFS | Svensk författningssamling |
| SMS | Short Message Service |
| sog. | sogenannt |
| SSI | Special Service Information |
| SSR | Special Service Request |
| SZ | Süddeutsche Zeitung |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| TF | Tryckfrihetsförordningen, SFS 1949:105 |
| TKG | Telekommunikationsgesetz |
| TMG | Telemediengesetz |
| T-PD | Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data |

| | |
|---|---|
| u.a. | und andere, unter anderem |
| UN | United Nations |
| UN-Charta | Charta der Vereinten Nationen vom 26.6.1945 in der Fassung des Beschl. der UN-Generalversammlung vom 20.12.1963. In Kraft getreten am 12.6.1968 (UNTS Bd. 638 S. 308; BGBl. 1973 II S. 430, dt. Übersetzung BGBl. 1980 II S. 1252) |
| UN-Doc. E/CN | Registerzeichen |
| UrhG | Gesetz über Urheberrecht und verwandte Schutzrechte |
| US | United States |
| USA | United States of America |
| US-Verfassung | Verfassung der Vereinigten Staaten von Amerika vom 17.9.1787 |
| v. | von |
| v.a. | vor allem |
| Var. | Variante |
| verb. | verbunden |
| vgl. | vergleiche |
| vMKS | v. Mangoldt, Hermann/Klein, Friedrich/Starck, Christian |
| VN | Vereinte Nationen |
| WRV | Weimarer Reichsverfassung vom 14.8.1919 |
| Yale L. J. | Yale Law Journal |
| z.B. | zum Beispiel |
| ZD | Zeitschrift für Datenschutz |
| ZD-Aktuell | Zeitschrift für Datenschutz aktuell |
| ZIS | Zollinformationssystem |
| zit. | zitiert |
| ZPO | Zivilprozessordnung |
| ZRP | Zeitschrift für Rechtspolitik |
| ZStW | Zeitschrift für die gesamte Strafrechtswissenschaft |

# Einleitung

## I. Entwicklung des Datenschutzrechts

Das beklemmende Gefühl, nicht zu wissen, wer was über einen weiß und welche Folgen dies haben könnte, beschreibt *Franz Kafka* in seinem Roman „Der Proceß“:[1] Der unbescholtene Josef K. findet sich plötzlich als Angeklagter in einem undurchsichtigen und fremdartigen Gerichtswesen wieder, dessen unterschwelliges Verfahren langsam sein Leben durchsetzt und zerstört. Josef K. kennt weder den Anklagegrund noch weiß er, wer dem Gericht angehört und wie das Verfahren abläuft. Das Gericht hingegen scheint alles über Josef K. zu wissen und ihn permanent zu beobachten. Diese „kafkaeske“ Situation einer völligen „Informationsohnmacht“ ist eine der Bedrohungen, die durch den Schutz personenbezogener Daten verhindert werden sollen. Sie wurde mit den Datensammlungen der ca. 624.000 „inoffiziellen Mitarbeiter“ der Stasi[2] und der 31.000 Mitarbeiter der Gestapo[3] in den beiden deutschen Unrechtsregimes des 20. Jahrhunderts zur bitteren Realität. Inwieweit die mindestens 30.000 Mitarbeiter der NSA[4] in diesem Zusammenhang zu nennen sind, wird sich erst in Zukunft beurteilen lassen.[5] Explizit werden solche „kafkaesken“ Bedrohungen im *Volkszählungsurteil* des Bundesverfassungsgerichts (BVerfG) vom 15. Dezember 1983 aufgegriffen:

> „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“[6]

Um eine derartige Gesellschaftsordnung zu verhindern, müssen Informationen wegen der von ihrem Missbrauch betroffenen Personen geschützt werden. Informationen sind Sinngehalte, die sich bei Empfängern bilden, und regulatorisch schwer fassbar. Der Schutz knüpft deshalb an Daten an. Daten sind vergegenständlichte

---

[1] *Kafka*, Der Proceß.

[2] Hochgerechnet für den Zeitraum von 1950 bis 1989. Für das Jahr 1988 gelten 173.081 IM als gesichert, vgl. *Müller-Enbergs*, Die inoffiziellen Mitarbeiter, S. 36 f.

[3] *Kohlhaas*, in: Paul/Mallmann (Hrsg.), Gestapo, S. 221. Zur Zahl der Informanten fehlen aussagekräftige Studien, vgl. *Mallmann*, in: Paul/Mallmann (Hrsg.), Gestapo, S. 271 ff.

[4] Die Zahl stammt aus National Security Agency, 60 Years of Defending Our Nation, 2012, http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf [Stand: 28.3.2014], S. 3.

[5] Zu den Veröffentlichungen von *Edward Snowden* vgl. z.B. http://www.heise.de/thema/NSA [Stand: 28.3.2014].

[6] BVerfG Urteil vom 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83; BVerfGE 65, 43.

Zeichen und durch ihre physikalische Dimension leichter zu steuern.[7] Im Folgenden soll es bei dieser pragmatischen juristischen Definition der Begriffe „Daten" und „Informationen" bleiben.[8] Das Datenschutzrecht lässt sich damit definieren als Summe der rechtlichen Normen, die den Schutz des Betroffenen vor den Folgen der Datenverarbeitung bezwecken.[9] Der Begriff „Verarbeitung" von Daten erfasst als Oberbegriff das Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.[10]

Die verfassungsrechtliche Anerkennung des Datenschutzes im Rahmen des allgemeinen Persönlichkeitsrechts, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, stellt einen Meilenstein in der deutschen Rechtsentwicklung dar. Diese Entwicklung ist keineswegs abgeschlossen, sondern noch in vollem Gange. Sie setzt sich mittlerweile auf europäischer Ebene fort, insbesondere mit den Vorschlägen der Europäischen Kommission für zwei neue Datenschutzregelwerke,[11] mit Art. 8 EU-GRC, mit der Fortbildung des Datenschutzes in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR), des Europäischen Gerichtshofs (EuGH) und des BVerfG.

Die negativen Folgen der Verarbeitung personenbezogener Informationen und die Forderung nach einem Recht auf Selbstbestimmung über diese Informationen sind freilich erheblich älter als das Volkszählungsurteil. Ihre Wurzeln liegen im Schutz spezieller Berufsgeheimnisse, wie beispielsweise dem Arztgeheimnis oder dem Beichtgeheimnis, die bereits vor mehreren Tausend Jahren existierten.[12] Doch auch die engere Konzeption eines Selbstbestimmungsrechts gab es schon lange vor dem Volkszählungsurteil. Bereits im Jahr 1880 entwickelte *Josef Kohler* gestützt auf englische und französische Rechtsprechung aus der actio injuriarum[13] ein zivilrechtliches Persönlichkeitsrecht, dessen Begründung die Forderung nach informationeller Selbstbestimmung vorwegzunehmen scheint:

---

[7] Vgl. *Hoffmann-Riem*, in: ders. (Hrsg.), Offene Rechtswissenschaft, S. 526.

[8] Andere Definitionen sind in informationstheoretischen und informationstechnischen Kontexten gebräuchlich. Zum Informationsbegriff übergreifend: *Sieber*, NJW 1989, 2569 ff.; *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, § 20; *Albers*, Rechtstheorie Nr. 33 (2002), 61 ff.

[9] In Anlehnung an Simitis-*Simitis*, Einl. Rn. 2.

[10] In den Rechtsquellen des Datenschutzrechts wird das Erheben teilweise aus dem Verarbeitungsbegriff ausgegrenzt, vgl. § 3 Abs. 3 und 4 BDSG, teilweise wird es darunter gefasst, vgl. § 3 Abs. 2 LDSG-BW. In diesem Werk wird „Verarbeitung" als Oberbegriff verstanden.

[11] Mitteilung KOM (2012) 9 endgültig vom 25.1.2012.

[12] So wurde bereits 800 vor Christus in Indien von einem ethischen Schweigegebot der Ärzte berichtet. Der Hippokratische Eid datiert auf das 5. Jahrhundert vor Christus, und die Verletzung des Beichtgeheimnisses wurde bereits in der Spätantike mit besonderen Kirchenstrafen geahndet, vgl. *Rudolf*, in: Merten/Papier (Hrsg.), Handbuch Grundrechte III, § 90, S. 235.

[13] Zur actio injuriarum *Maass*, Zivilrecht, S. 6 m.w.N. Zu Genese und internationaler Wirkung der Positionen *Kohlers* ebd., S. 12–14.

„Somit ist es ein unveräußerliches Individualrecht des Autors, zu bestimmen, ob eine Gedankenäußerung den Rubiko überschreiten, aus dem Geheimnis seines Innenlebens wie ein Strahl aus dunkler Wolke hervorbrechen soll, oder nicht."[14]

Dieses Recht sollte die Geheimnisse des „Innenlebens" vor „unbefugter Publizität" schützen und verhindern, dass die verwundbaren Seiten des Privatlebens in „Pöbelwitz" und „Skandalklatsch" herabgezogen wurden.[15] Dieses „Individualrecht" sei verletzt, wenn „vertrauliche Äußerungen" veröffentlicht werden.[16] Zehn Jahre später griffen *Louis Brandeis* und *Samuel Warren* diesen Gedanken auf und entwickelten auf Grundlage des common law das bis heute wirkmächtige right to privacy:

"The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. […], he generally retains the power to fix the limits of the publicity which shall be given them."[17]

Ähnlich wie *Kohler* entwerfen auch *Warren/Brandeis* ihre Rechtsposition zur Abwehr einer als verwerflich empfundenen Berichterstattung[18] in Abgrenzung von nahestehenden Rechtsinstituten[19] unter Auseinandersetzung mit dem Eigentumsbegriff[20] sowie mit rechtsvergleichenden Methoden.[21] Im Unterschied zu *Kohler* bezogen sich *Warren/Brandeis* jedoch ausdrücklich auf Risiken neuer Technologien:

"the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion […] by […] the possessor of any other modern device for recording or reproducing scenes or sounds".[22]

Dieser Aspekt wurde in den ausgehenden 1960er-Jahren zum entscheidenden Merkmal der aufkommenden Datenschutzdiskussion und ist aufgrund der sich seit

---

[14] *Kohler*, 18 Jahrb. f. Dogm. (1880), 280.

[15] Ebd., 272 f.

[16] Ebd., 271. Das Individualrecht wurde von *Kohler* später als ein die Geheimsphäre schützendes Persönlichkeitsrecht bezeichnet, *Kohler*, Urheberrecht, S. 441.

[17] *Warren/Brandeis*, 4 Harv. L. Rev. 5 (1890), 198; deutsche Übersetzung mit Anmerkung bei *Hansen/Weichert*, Das Recht auf Privatheit, https://www.Datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html [Stand: 28.3.2014].

[18] "Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.", *Warren/Brandeis*, 4 Harv. L. Rev. 5 (1890), 196; *Kohler* entwickelt sein Recht anhand Veröffentlichungen „zum Zwecke des Gewinnes, […], zum Zweck des Klatsches und des Skandals", *Kohler*, 18 Jahrb. f. Dogm. (1880), 271.

[19] *Warren/Brandeis*, 4 Harv. L. Rev. 5 (1890), 200: "entirely independent of the copyright laws"; *Kohler*, 18 Jahrb. f. Dogm. (1880), 274: „vollkommen unabhängig von der Autorrechtsqualität".

[20] *Kohler*, 18 Jahrb. f. Dogm. (1880), 226 ff.; *Warren/Brandeis*, 4 Harv. L. Rev. 5 (1890), 200 ff.

[21] *Maass* weist darauf hin, dass *Brandeis* auch in den USA über die deutsche Rechtsliteratur informiert war und insoweit, obwohl er ihn nicht zitiert, von *Kohler* angeregt worden sein könnte, *Maass*, Zivilrecht, Fn. 63. Vgl. ebd. auch zu französischen Einflüssen.

[22] *Warren/Brandeis*, 4 Harv. L. Rev. 5 (1890), 206.

damals sprunghaft fortentwickelnden Informations- und Kommunikationstechnologie (IKT) bis heute die zentrale Forderung an den Datenschutz.[23] Während *Kohler* und *Warren/Brandeis* die negativen Auswirkungen der Publizität persönlicher Informationen noch ausschließlich aus dem Blickwinkel des „geistigen Innenlebens" und öffentlichen Ansehens betrachteten, folgte nun eine zunehmend gesellschaftskritische und demokratietheoretische Überformung der Diskussion. Die IKT erschien als undurchsichtige Großtechnologie. Sie befand sich in der Hand von Staat, Industrie und Banken, was durch Wissensakkumulation eine faktische Machtverschiebung zugunsten dieser Institutionen zu bewirken drohte.[24] In der Folgezeit entstanden die ersten nationalen Datenschutzgesetze; wenige Jahre später Empfehlungen der OECD, eine Konvention des Europarats, nationales Datenschutz-Verfassungsrecht, europäisches Sekundärrecht und schließlich auch Primärrecht.[25] Eine europaweit einheitliche Datenschutzrechtsordnung ist mit den im Januar 2012 vorgestellten Entwürfen einer neuen allgemeinen Datenschutzgrundverordnung sowie einer Datenschutzrichtlinie für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in greifbare Nähe gerückt.[26]

Dabei zieht sich eine Grundfrage wie ein roter Faden durch sämtliche Stufen der Rechtsentwicklung des Datenschutzes: Welches Maß an inhaltlicher Genauigkeit von Regulierung wird den Zielen von Datenschutz gerecht? Diese Frage zeigt sich in den Auseinandersetzungen auf den verschiedenen Ebenen des Rechts: So werden auf der Ebene des einfachgesetzlichen Datenschutzrechts Komplexität und Verrechtlichung scharf kritisiert. Immer noch aktuell ist der Befund des Reformgutachtens von *Roßnagel/Pfitzmann/Garstka* aus dem Jahr 2001, der das deutsche Datenschutzrecht als „Normenflut immer feiner differenzierender Normen für nahezu jeden Spezialbereich, die das inhaltliche Ziel, die Verarbeitung personenbezogener Daten auf die wirklich unabdingbaren Fälle einzuschränken, weitgehend verfehlt hat", beschreibt. Das Programm des Volkszählungsurteils sei in einer Weise „erfüllt", „die geradezu das Gegenteil von dem hervorbrachte, was beabsichtigt

---

[23] Zu den technischen Aspekten heutiger IKT *Sieber*, in: Hoeren/Sieber (Hrsg.), Handbuch MMR, Teil 1 sowie *Heckmann* (Hrsg.), juris PK-Internetrecht, Kapitel 9 Rn. 68 ff. Zur Geschichte der Kommunikationsmedien *Kittler*, in: Stroemfeld/Roter Stern/Museum für Gestaltung Zürich (Hrsg.), Kommunikationsmedien, S. 169–188.

[24] *Abel*, in: Roßnagel/Abel (Hrsg.), Handbuch, S. 197.

[25] Siehe unten Teil 2.

[26] Siehe unten Teil 2, III.F. und G.; KOM (2012) 11 endgültig sowie KOM (2012) 10 endgültig; dazu *Masing*, Ein Abschied von den Grundrechten, SZ vom 9.1.2012, S. 10; *Ehmann*, JurisPR-IT-Recht 4/2012, Anm. 2 [Stand: 28.3.2014]; vgl. auch die Stellungnahme und weitere aktuelle Informationen des Berichterstatters des Innenausschusses des Europaparlaments *Jan Philip Albrecht*, http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html [Stand: 28.3.2014]. Dem federführenden LIBE-Ausschuss lagen ca. 4000 Änderungsanträge vor, die Abstimmung erfolgte am 12.3.2014; der nächste Schritt im Gesetzgebungsverfahren ist der sog. „Trilog" zwischen Kommission, den Berichterstattern des Parlaments und der Ratspräsidentschaft. http://europa.eu/rapid/press-release_MEMO-14-60_en.htm?locale=en [Stand: 28.3.2014].

war".[27] Diese Sichtweise wird vielfach geteilt.[28] Entsprechend häufig ist die Forderung nach Reformen des Datenschutzrechts.[29]

Auf Verfassungsrechtsebene wird seit dem Volkszählungsurteil um die Konkretisierung des Grundrechts auf informationelle Selbstbestimmung gestritten: Wegen des hohen Abstraktionsgrades erscheint dieses vielen als „konturlos"[30] bzw. „nicht gegenstandsgerecht".[31] Entsprechend vielfältig sind die Vorschläge zur Begrenzung und Präzisierung.[32] Vorläufiger „Höhepunkt" in der Entwicklung des allgemeinen Persönlichkeitsrechts ist die „Abschichtung" eines Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) durch das BVerfG.[33] Dieses „neue Grundrecht" kann auch als Versuch der „dogmatischen Entlastung"[34] und Präzisierung des Grundrechts auf informationelle Selbstbestimmung verstanden werden.[35] Zu größeren Verwerfungen führt die Diskussion um die Reichweite des grundrechtlichen Schutzes im Verhältnis zu privaten Datenverarbeitern.[36]

Auf EU-Ebene sind die im Januar 2012 erfolgten Vorschläge für ein neues „Datenschutzpaket"[37] Ergebnis einer jahrelangen Reformarbeit.[38] Die Kompetenz-

---

[27] *Roßnagel/Pfitzmann/Garstka*, Gutachten, S. 29.

[28] Die Datenschutzbeauftragten bezeichneten das Datenschutzrecht auf ihrer 79. Konferenz als „selbst für Fachleute nur noch schwer verständlich", Anlage zur Pressemitteilung vom 18.3.2010, Zusammenfassung, Nr. 8. *Hoffmann-Riem*, AöR Nr. 123 (1998), 516 f. beschreibt die Lage wie folgt: „Komplizierte Anwendungsregeln, verschachtelte Verweisungen, vielfältige Bereichssonderregeln und offen formulierte Abwägungsermächtigungen prägen das Bild." Sehr kritisch auch *Kühling/Bohnen*, JZ 2010, 600 f. Zu den strukturellen Defiziten des BDSG *Weichert*, DuD 2010, 12. Zuletzt griff auch der vormalige Bundesdatenschutzbeauftragte *Schaar* in seinem Blog die Kritik an der Vielfalt bereichsspezifischer Regelungen auf: https://www.bfdi.bund.de/bfdi_forum/showthread.php?3211-Strre-meine-Kreise-nicht [Stand: 28.3.2014].

[29] *Weichert*, DuD 2010, 7 ff.; *Roßnagel/Pfitzmann/Garstka*, Gutachten, S. 22 ff., 34; *Masing*, NJW 2012, 2305 ff.; für das Europäische Datenschutzrecht z.B. *Rogall-Grothe*, ZRP 2012, 193 ff.

[30] *Ladeur*, DÖV 2009, 45 sowie 49 m.w.N.

[31] *Albers*, Informationelle Selbstbestimmung, S. 280 (zweite Aufl. in Vorbereitung). Zur Kritik im Einzelnen ebd., S. 174 ff. sowie die Nachweise bei *Bull*, Informationelle Selbstbestimmung, S. 16, Fn. 24. Auch *Hoffmann-Riem*, in: ders. (Hrsg.), Offene Rechtswissenschaft, S. 541: „ohne Kraft zur rechtsdogmatischen Begrenzung"; a.A. (hinreichend bestimmt) *Kutscha*, DuD 2011, 462. *Grimm* spricht von einer „Entgrenzung" des Datenschutzrechts, *Grimm*, JZ 2013, 585 (585 f.).

[32] Vgl. u.a. die Zusammenstellung bei *Rogall*, Informationseingriff, S. 49 ff.

[33] Urteil vom 27.2.2008, 1 BvR 370, 595/07 *(Online-Durchsuchung)* = BVerfGE 120, 274.

[34] *Bäcker*, in: Rensen/Brink (Hrsg.), Internetkommunikation, S. 124.

[35] Das Grundrecht auf informationelle Selbstbestimmung soll nun „einzelne Datenerhebungen" erfassen, während der Gesamtzugriff auf das System durch das IT-Grundrecht geschützt wird, BVerfGE 120, 313.

[36] Statt vieler: *Masing*, NJW 2012, 2305 ff. sowie *Grimm*, JZ 2013, 585 ff.

[37] Siehe oben Fn. 11.

vorschrift des Art. 16 AEUV ermöglicht diese Neuregelungen, auch unter Einbeziehung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Die Reformen werfen – ebenso wie die Konkretisierung des Datenschutzes nach Art. 8 EMRK und des Datenschutz-Grundrechts in Art. 8 EU-GRC – zahlreiche Fragen auf, insbesondere für den Bereich des Sicherheitsrechts.[39]

Auf der Ebene des internationalen Rechts manifestiert sich die Grundfrage nach der „Normierungstiefe" in den Datenschutz-Konflikten zwischen EU und USA: Das sektorale, auf Selbstregulierung und durchsetzbare Verhaltenskodizes setzende Datenschutzrecht der USA stellt dort einen Gegensatz zum europäischen Konzept umfassender gesetzlicher Verarbeitungsregelungen dar.[40] Die grenzüberschreitende Natur der IKT zwingt dabei zur Interoperabilität regionaler und internationaler Datenschutzinstrumente.[41]

Die Suche nach dem „richtigen Maß" an Datenschutzrecht auf der „richtigen Ebene" wird in jüngster Zeit durch drei Entwicklungen erschwert. Dabei handelt es sich erstens um den erneuten *qualitativen und quantitativen Wandel der IKT* in den letzten Jahren. Die Entwicklung ist geprägt durch eine zunehmend ubiquitäre, mobile und sozial-vernetzte Internetnutzung. Globale Unternehmen wie Facebook und Google haben staatliche Stellen als Inhaber der umfangreichsten Datensammlungen abgelöst. Zum Zweck der Generierung von Werbeeinahmen setzen sie mittels attraktiver Dienste vielfältige Anreize zur Preisgabe personenbezogener Daten. Die Nutzer profitieren einerseits von innovativen Anwendungen und neuen Formen von Kommunikation und Information. Andererseits machen sie sich selbst transparent und überwachbar. Das derzeit drängendste Beispiel sind soziale Netzwerke.[42] Sie sind die zurzeit erfolgreichste Ausprägung des Web 2.0.[43] Der Marktführer Facebook hatte Ende 2013 durchschnittlich mehr als 1,23 Milliarden aktive Nutzer im Monat.[44] Einer Untersuchung aus dem Jahr 2011 zufolge haben 74 % der Internet-

---

[38] Europäische Kommission, KOM (2010) 609, S. 4 f. sowie befürwortend: Konferenz der Europäischen Datenschutzbeauftragten, Entschließung, 5.4.2011, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/EuDSK/EntschliessungEUDSK_deutsch.pdf?__blob=publicationFile [Stand: 28.3.2014].

[39] Vgl. *Spiecker gen. Döhmann*, JZ 2011, 176 f.; *Britz*, EuGRZ 2009, 3 ff.; *Rogall-Grothe*, ZRP 2012, 193 ff.

[40] Zu den unterschiedlichen Ansätzen aus US-amerikanischer Sicht: *Schwartz*, 118 Yale L. J. (2009), 902 ff. sowie *Zimmer*, in: Szoka/Marcus (Hrsg.), The Next Digital Decade, S. 479 ff. m.w.N. Aus deutscher Sicht *Abel*, in: Roßnagel/Abel (Hrsg.), Handbuch, S. 198.

[41] *Gürtler*, RDV 2012, 126 (132 f.).

[42] Der Begriff „soziale Netzwerke" wird im Folgenden für die bekannten Internetplattformen wie Facebook und Google+ verwendet; zu alternativen Begriffen und zum Konzept sozialer Netzwerke in der Soziologie vgl. *Ebersbach/Glaser/Heigl*, Social Web, S. 29 und 81.

[43] Zum Begriff „Web 2.0", vgl. *O'Reilly*, What Is Web 2.0?, 2005, http://oreilly.com/web2/archive/what-is-web-20.html [Stand: 28.3.2014] sowie *Alby*, Web 2.0, S. 15 ff.

[44] https://newsroom.fb.com/company-info/ [Stand: 28.3.2014].

nutzer in Deutschland ein Profil bei mindestens einem der sozialen Netzwerke, 66 % sind aktive Nutzer. Bei der Gruppe der unter 30-Jährigen haben 92 % der Nutzer ein Profil, 85 % sind aktive Nutzer. Die meisten Nutzer (59 %) sind täglich in dem Netzwerk aktiv.[45] Bei aktiven Nutzern läuft ein großer Teil der alltäglichen Kommunikation und der virtuellen Selbstdarstellung über das soziale Netzwerk. Die dabei anfallenden Informationen umfassen potenziell alle Lebensbereiche. Sie enthalten neben Bild- und Videomaterial auch Ortsangaben und Informationen über Kontaktpersonen, politische und religiöse Überzeugungen, Freizeitbeschäftigungen, Wohn- und Arbeitsverhältnisse.[46] Zunehmend werden die Netzwerke auch mit anderen Web 2.0- und *cloud computing*-Angeboten unter einem gemeinsamen Portal verbunden und z.B. zur Datei- und E-Mail-Verwaltung eingesetzt.[47] Durch mobile Internetnutzung sind die sozialen Netzwerke jederzeit präsent.

Das Potenzial einer virtuellen Rekonstruktion nahezu des gesamten Lebens macht den Zugriff für Sicherheitsbehörden höchst attraktiv.[48] Es sind die Nutzer selbst, die durch ihr Kommunikations- und Informationsverhalten umfassende Überwachungsmöglichkeiten für alle Interessierten, private wie staatliche Stellen schaffen. Die Veröffentlichungen des ehemaligen NSA-Mitarbeiters *Snowden* bestätigen dieses Interesse eindrucksvoll.[49] Dass die neuen Dienste trotz mangelhaften Datenschutzes so populär sind, kann auf fehlendes Risikobewusstsein oder aber, soweit die Nutzung auf einer tauglichen Einwilligung beruht, auf geänderte Einstellungen im Hinblick auf Privatheit und Transparenz hinweisen.

Dies deutet die zweite Entwicklung im Bereich des Datenschutzes an: den *sorglosen Umgang vieler Nutzer mit ihren personenbezogenen Daten*. Artikuliert wird dies z.B. in der Debatte um *post privacy*-Konzepte. Danach sind Datenschutz und Privatsphäre in der digitalen Welt weder technisch erreichbar noch gesellschaftlich erstrebenswert. Stattdessen soll weitestgehende Transparenz die Isolation des Privaten, gesellschaftliche Tabus und Missstände aufbrechen. Das eigentliche Problem sei nicht die unvermeidliche Informationstransparenz; vielmehr seien lediglich Informationsungleichgewichte zu verhindern, indem die Transparenz auf alle ausgedehnt werde.[50] Inwieweit dieser Ansatz rechtlich haltbar ist, wird zu prüfen sein.

---

[45] BITKOM (Hrsg.), Soziale Netzwerke, S. 4.

[46] Eine Liste der bei facebook verfügbaren Informationen in ihrer „Rohfassung" ist auf der Internetseite von *Max Schrems* einsehbar: http://www.europe-v-facebook.org/DE/Datenbestand/datenbestand.html [Stand: 28.3.2014].

[47] Ein Beispiel hierfür ist das soziale Netzwerk Google+, mit dem andere Dienste des Anbieters wie z.B. eine Dokumentenverwaltung, ein virtuelles Laufwerk und das freemail-Angebot unter einem Portal verbunden sind, vgl. http://www.sueddeutsche.de/digital/google-drive-kommt-online-speicher-bietet-fuenf-gigabyte-kostenlos-1.1341139 [Stand: 28.3.2014].

[48] Vgl. *Drackert*, eucrim 2011, 122 ff. m.w.N.

[49] Vgl. hierzu http://www.heise.de/thema/NSA [Stand: 28.3.2014].

[50] Vgl. *Köhntopp*, Blogeintrag, 12.5.2011, http://blog.koehntopp.de/archives/3073-Von-der-Spackeria,-von-Aluhueten-und-vom-Kontrollverlust.html [Stand: 29.10.2011]. Kritisch:

Die geänderten Rahmenbedingungen zeigen jedenfalls, dass die „Idee Datenschutz“ vor fundamentalen Herausforderungen steht.

Die dritte Entwicklung kann als *qualitativer und quantitativer Wandel der Sicherheitspolitik* beschrieben werden. Technische, wirtschaftliche und politische Veränderungen der „Weltrisikogesellschaft“ haben in vielen Ländern den sicherheitspolitischen Fokus vorverlagert, weil es nunmehr möglich scheint, Verbrechen und Gefahren früher zu erkennen und somit zu verhindern. Diese politische Entwicklung geht einher mit der Erweiterung präventiver Überwachungskonzepte und verstärkten Mitwirkungspflichten Privater im Vorfeld und außerhalb von Strafverfahren.[51] Der Einsatz von IKT zur Verringerung der Aufklärungs- und Nachweisschwierigkeiten einer derart auf Prävention ausgerichteten Sicherheitspolitik betrifft unmittelbar den Bereich des Datenschutzes und birgt die Gefahr des Abbaus von Freiheitsrechten.[52] Es ist deshalb nicht verwunderlich, wenn sich die politische und juristische Diskussion um Freiheit und Sicherheit vielfach am Datenschutz entzündet.[53]

Diese drei Entwicklungen – Wandel der IKT, sorgloser Umgang mit personenbezogenen Daten sowie Verlagerung der Sicherheitspolitik auf die „Sicherheitsvorsorge“ –[54] machen es erforderlich, das Thema Datenschutz in einen größeren Untersuchungszusammenhang zu stellen und die Frage nach dessen Legitimation neu aufzuwerfen. Die Suche nach dem „richtigen Maß“ von Datenschutzrecht auf der „richtigen Ebene“ setzt Klarheit über die negativen Folgen, vor denen das Datenschutzrecht per definitionem schützen will, voraus. Weil Datenschutzrecht in der Phase des Vorfelds von Schäden eingreift,[55] sind diese Folgen als Risiken zu beschreiben.[56] Die Identifikation von Risiken ist die Voraussetzung zur Legitimation eines Vorfeldschutzes.[57] Die genannten Entwicklungen und der im Folgenden zu skizzierende Forschungsstand zeigen jedoch, dass hierüber keine Klarheit besteht. Die Grundlagenforschung im Bereich des Datenschutzrechts erfordert deshalb die Identifikation relevanter Risiken.

---

*Leutheusser-Schnarrenberger*, Artikel auf der Internetseite der FAZ, 25.4.2011, http://www.faz.net/-01sy3l [Stand: 28.3.2014]; *Koch*, ITRB 2011, 161 f.

[51] *Sieber*, ZStW 119 (2007), 4 ff.

[52] Dies zeigen die kritischen Äußerungen zum Datenschutz bei *Nehm*, NJW 2002, 2665 (2671); vgl. auch *Graulich*, in: ders./Simon (Hrsg.), Terrorismus, S. 407; zugespitzt *Düx*, ZRP 2003, 189 ff.

[53] Statt vieler: *Masing*, JZ 2011, 756 ff. und *Bull*, Informationelle Selbstbestimmung, S. 4 ff.

[54] Zum Begriff „Sicherheitsvorsorge“ vgl. die Nachweise bei *Masing*, JZ 2011, 756, Fn. 23.

[55] Vgl. *von Lewinski*, in: Arndt u.a. (Hrsg.), Freiheit-Sicherheit-Öffentlichkeit, S. 199.

[56] Zum Begriff „Risiko“ siehe unten IV.A.

[57] Für das Strafrecht vgl. *Sieber*, NStZ 2009, 353 (357).

# II. Stand der Forschung

„Risikoadäquanz“ wird im Datenschutzrecht häufig eingefordert.[58] Es findet sich aber in neuerer Zeit keine systematische Analyse und konzentrierte Zusammenstellung, die sich explizit den Risiken der Verarbeitung personenbezogener Daten widmet. Die oben beschriebene Umbruchsituation im Datenschutzrecht macht dies jedoch als Voraussetzung einer rationalen rechtspolitischen Diskussion und zur Absicherung der im Datenschutzrecht häufig erforderlichen Abwägung zwischen Datenverarbeitungsrechten und Persönlichkeitsrecht nötig. Die Risiken der Verarbeitung personenbezogener Daten werden im Schrifttum insbesondere im verfassungsrechtlichen Kontext thematisiert. Dabei enthalten die breiter angelegten Arbeiten von *Albers*[59] und *Britz*[60] zur informationellen Selbstbestimmung bzw. zum Allgemeinen Persönlichkeitsrecht im Rahmen ihrer jeweiligen Grundlagenteile für die vorliegende Untersuchung relevante Erkenntnisse, die später in der Analyse aufgegriffen werden. Exemplarisch für den datenschutzrechtlichen Reformdiskurs sind zwei von *Roßnagel* mit- bzw. verfasste Gutachten, die an entscheidender Stelle ebenfalls mit einschlägigen Risiken argumentieren, wobei auch hier die Risiken im ersten Gutachten überhaupt nicht und im zweiten nur unter dem Blickwinkel ubiquitärer Datenverarbeitung zum Gegenstand der Untersuchung wurden.[61] Aufschlussreich ist zudem die grundlegende Untersuchung von *Mallmann* zu den „Zielfunktionen des Datenschutzrechts“ aus dem Jahr 1977, die aufgrund ihrer soziologischen Bezüge und rechtspolitischen Ausrichtung eine Sonderstellung einnimmt. Die Arbeit beeinflusste den datenschutzrechtlichen Diskurs maßgeblich und wird deshalb trotz ihres Alters ebenfalls in die vorliegende Untersuchung einfließen.

Ansonsten existieren zwar ältere Arbeiten zu den Grundlagen des Datenschutzes; diese werden jedoch dem Stand der technischen und gesellschaftlichen Entwicklung nicht mehr gerecht.[62] Weiterhin scheint aus vielen älteren Arbeiten eine

---

[58] *Rogall-Grothe*, ZRP 2012, 193 (195); *Roßnagel/Pfitzmann/Garstka*, Gutachten, S. 13; vgl. auch *Bull*, Informationelle Selbstbestimmung, S. 68 ff.; *ders.*, ZRP 2008, 234; *Hoffmann-Riem*, AöR Nr. 123 (1998), 529 f. Für den Datenschutz im nicht-öffentlichen Sektor *Gurlit*, NJW 2010, 1040.

[59] *Albers*, Informationelle Selbstbestimmung, 2005 sowie *dies*., in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, 2008.

[60] *Britz*, Selbstdarstellung, 2007 sowie *dies*., in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft.

[61] Siehe unten Teil 3, III.C. und D.

[62] Literaturübersicht bei *Albers*, Informationelle Selbstbestimmung, S. 113–123, vgl. auch *dies.*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II Rn. 35, Rn. 25. Besonders hervorzuheben sind: *Steinmüller* u.a., Gutachten; *Mallmann*, Zielfunktionen; *Benda*, in: Leibholz u.a. (Hrsg.), FS Geiger; *Heussner*, in: Gitter/Thieme/Zacher (Hrsg.), FS Wannagat; *Ehmann*, AcP 188 (1988), 230–380 sowie *Roßnagel* u.a., Digitalisierung, die aber einen beachtenswerten Ansatz in Bezug auf technischen Wandel verfolgen.

grundsätzlich misstrauische oder sogar ablehnende Haltung gegenüber moderner Informationstechnologie zu sprechen. So sei z.B. der Computer ein „multifunktionaler unsichtbarer Manipulator im Dienst seines Herrn“ oder: „Computerkommunikation ist [...] der Grundtyp der ‚vertikalen Kommunikation' die wir als ‚hoheitliche Kommunikation' alle kennen“.[63] Dieser Linie der älteren Literatur wurde der Vorwurf gemacht, den „Interessengegensatz zwischen Besitzenden und Nichtbesitzenden durch den Interessengegensatz zwischen Wissenden und Unwissenden, zwischen Datenverarbeitern und davon Betroffenen“ zu ersetzen, um so eine „neue Rechtfertigung für die Fortführung des Klassenkampfes zur Herstellung einer klassen- und autoritätslosen Gesellschaft abzuleiten“.[64] Derartige postmarxistische Begründungsansätze sind ideologisch geprägt und können nicht überzeugen. Im Gegensatz dazu steht neben der bereits oben genannten Studie von *Mallmann* ein wirkkräftiger Aufsatz von *Schmidt* aus dem Jahr 1974, der aufgrund seiner richtungsweisenden Abhandlung der Entscheidungsfreiheit näher zu beleuchten ist.[65]

In der neueren Literatur verringern sich die oben genannten, eher ideologisch geprägten Verwerfungen. An deren Stelle ist bisher jedoch keine rationale, pragmatische und zugleich aktuelle juristische Arbeit zu einschlägigen Risiken getreten. Eine gewisse Sonderrolle im Schrifttum nehmen dabei die kleineren eigentumsanalogen Konzeptionen von *Ladeur* und *Kilian* zum Recht auf informationelle Selbstbestimmung ein, die aufgrund ihrer dezidierten Gegenposition zum „Mainstream“ des Schrifttums mit Blick auf die systematische Zuordnung von Risiken aufschlussreich sind.[66]

Im Übrigen wird in der neueren wie älteren Literatur das Bestehen von „Datenschutz-Risiken jedoch vielfach unbestimmt vorausgesetzt oder angedeutet, sodass daraus für die Frage, welche Risiken der Datenverarbeitung bestehen, nichts folgt.[67] Exemplarisch ist der – sonst wegweisende – Aufsatz von *Hoffmann-Riem,* der abstrakt von „neuen Risiken“ spricht, ohne diese zu erläutern. Das greifbarste Risiko, das *Hoffmann-Riem* nennt, ist die Befürchtung, dass erweiterte Eingriffsbefugnisse für Überwachungsmaßnahmen in erster Linie zur Bekämpfung von einfacher und alltäglicher Kriminalität herangezogen werden.[68] Ohne konkrete Benennung spricht auch *Trute* lediglich von „neue[n] Gefährdungen infolge weit-

---

[63] *Steinmüller*, NfD 1993, 222.

[64] *Ehmann*, 188 AcP (1988), 261.

[65] *Schmidt*, JZ 1974, 241.

[66] *Ladeur*, DuD 2000, 1; *Kilian*, CR 2002, 921.

[67] In den datenschutzrechtlichen Lehr- und Handbüchern sowie Kommentaren finden sich lediglich knappe Hinweise auf Risiken bzw. einschlägige Ziele des Datenschutzrechts: *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 1–4; *Roßnagel*, in: ders./Abel (Hrsg.), Handbuch, S. 2–6; Simitis-*Simitis*, Einl. Rn. 8–13; Taeger/Gabel-*Schmidt*, § 1 Rn. 8; keine Ausführungen dagegen bei *Kühling/Seidel/Sivridis*, Datenschutzrecht; in dieser Hinsicht auch nicht ergiebig *Gola/Schomerus*, § 1 Rn. 6–8.

[68] *Hoffmann-Riem*, AöR Nr. 123 (1998), 517 ff.

reichender Möglichkeiten der Dokumentation und Manipulation digitalisierter personenbezogener Informationen".[69] Hier müssten konkretere Fälle bezeichnet werden. Nur überblickartige Ausführungen bieten die Voraufl age des Lehrbuchs von *Tinnefeld/Ehmann/Gerling* und die Monografie von *Gridl*.[70] Die Monografie von *Griese* aus dem Jahr 1987 erörtert Risiken kurz, jedoch beschränkt auf den arbeitsrechtlichen Kontext.[71] Auch in den hinsichtlich ihres Grundlagenteils ergiebigeren neueren Arbeiten zum Grundrecht auf informationelle Selbstbestimmung werden Risiken eher im Rahmen des jeweiligen Modells vorausgesetzt und wegen der dogmatischen Zielsetzung weniger konkret gefasst und nicht selbst zum Gegenstand der Untersuchung gemacht.[72]

Die Unsicherheit, die durch das Fehlen einer Untersuchung zu den Risiken der Verarbeitung personenbezogener Daten entsteht, verdeutlichen die zahlreichen kritischen Stimmen zum Grundrecht auf informationelle Selbstbestimmung, das wegen seiner Unklarheit als Stück „Grundrechtstheologie" oder „Bergpredigt des Datenschutzes" kritisiert wird.[73] Es habe sich in der Kommentarliteratur „eingenistet", ohne dass dem Wort „irgendeine grundrechtssteigernde oder tatbestandspräzisierende Bedeutung" zukäme.[74] Unklar ist auch der Schutzbereich von Art. 8 EU-GRC. Hierzu führt *Britz* aus, dass man zunächst einmal wissen müsse, welches Gut überhaupt zu schützen sei. Dies bleibe momentan „vergleichsweise dunkel". Frage man sich, „was und wogegen" das europäische Datenschutzgrundrecht eigentlich schütze, so finde man keine schnelle Antwort.[75] An anderer Stelle verlangt sie die Herausarbeitung von Kriterien, „mittels derer man Grundrechtseingriffe von rechtlich irrelevanten Informationsvorgängen abgrenzen" könne.[76]

So erstaunt es denn auch nicht, dass die Klärung des Schutzguts von weiten Teilen der Literatur und den betroffenen Praktikern zunehmend eingefordert wird.[77]

---

[69] *Trute*, JZ 1998, 823 f.

[70] *Tinnefeld/Ehmann/Gerling*, Einführung, S. 63–73; *Gridl*, Datenschutz, S. 25–29.

[71] *Griese*, Persönlichkeitsschutz, S. 35–43.

[72] Konkrete Risiken werden bei *Albers* nur zum Teil genannt, vgl. *Albers*, Informationelle Selbstbestimmung, S. 416 f.; bei *Britz* finden sich zwar „Fallgruppen erhöhter Gefährdungslagen", diese bleiben jedoch eher abstrakt und deuten die implizierten Risiken nur an, vgl. *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 579. Auch in ihrer Monografie zum Allgemeinen Persönlichkeitsrecht weist sie zunächst nur auf die Notwendigkeit der Identifikation von „Gefahrpunkten" durch Verfassungsinterpretation hin, *Britz*, Selbstdarstellung, S. 40. Diese Arbeiten werden jedoch im Folgenden als Ausgangspunkt für die vorliegende Untersuchung fruchtbar gemacht.

[73] *Meister* und *Ladeur*, zit. nach *Bull*, Informationelle Selbstbestimmung, S. 45.

[74] vMKS-*Starck*, Art. 2 Abs. 1 Rn. 114.

[75] *Britz*, EuGRZ 2009, 8 f.

[76] *Britz*, Selbstdarstellung, S. 64.

[77] Vgl. insb. die Äußerungen von *Stentzel* und *Osthaus* in den Verhandlungen des 69. DJT in München, Ständige Deputation des Deutschen Juristentages (Hrsg.), DJT-Sitzungsberichte, O 202 f. sowie O 193 f.; *Schneider*, ITRB 2012, 180 (185).

Voraussetzung hierfür sind an den Folgen der Verarbeitung orientierte verfassungsrechtliche Vorgaben.[78] „Gefahrpunkte" seien erst noch zu identifizieren.[79] Pointiert verdeutlicht die Unklarheit auch die abweichende Meinung von Richterin des Bundesverfassungsgerichts *Haas* zur *Rasterfahndungsentscheidung* des BVerfG:[80]

> „Wenn die Senatsmehrheit raumgreifend eine Vielzahl einzelner Umstände der Datenverwertung meint anführen zu müssen, um die besondere Intensität des Eingriffs zu begründen, so dürfte dies wohl den Schluss erlauben, dass auch die Senatsmehrheit der Überzeugungskraft der einzelnen Argumente nicht ganz vertraut."[81]

Dies zeigt, dass die Risiken keineswegs evident und konsentiert sind. Schon die oben angesprochene *post privacy*-Debatte und das andere Datenschutzempfinden und Überwachungsverhalten in den USA verdeutlichen, auf welch unsicheren Grundlagen Datenschutzrecht basiert. So weist etwa *Bull* darauf hin, dass sich das Datenschutzrecht bloß dem Risiko der „Verdatung" im weitesten Sinne widme und diese Ungenauigkeit zu korrigieren sei:

> „Erfolgreiche Risikoabwehr setzt genaue Kenntnis voraus; ängstliche ‚Rundum-Verteidigung' ist Energievergeudung."[82]

Auch vonseiten des Bundesministeriums des Innern wurde unter Minister a.D. *Friedrich* die Auffassung vertreten, dass das Datenschutzrecht nur noch „risikobehaftete" Datenverarbeitungen regeln solle.[83] Was hierunter zu verstehen ist, bleibt bislang jedoch im Dunkeln.

## III. Forschungsziele und Forschungsfragen

Ziel der Arbeit ist die Identifikation und Klassifizierung von Risiken der Verarbeitung personenbezogener Daten. Hiermit sollen Indikatoren für datenschutzrechtliche Reformen benannt werden, die in der Diskussion um Legitimation, inhaltliche Genauigkeit und normenhierarchische Verortung von Datenschutzregelungen bislang fehlen. Die Identifikation einschlägiger Risiken führt damit

---

[78] Simitis-*Simitis*, Einl. Rn. 243; ähnlich in Anlehnung an BVerfGE 101, 361 (380) auch *Britz*, Selbstdarstellung, S. 49.

[79] *Britz*, Selbstdarstellung, S. 84.

[80] Abweichende Meinung der Richterin am Bundesverfassungsgericht a.D. *Haas* zum Beschluss des Ersten Senats vom 4.4.2006, 1 BvR 518/02 *(Rasterfahndung II)* = BVerfGE 115, 320.

[81] BVerfGE 115, 320 (371).

[82] *Bull*, Informationelle Selbstbestimmung, S. 69

[83] http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2012/10/datenschutzkonferenz.html [Stand: 28.3.2014]. Vgl. auch http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2012/23_DatenschutzVoranbringenUndNichtAbwickeln.html [Stand: 28.3.2014].

zugleich zur Präzisierung der im Moment noch unklaren datenschutzrechtlichen Schutzgüter. Vereinfacht ausgedrückt lässt sich das Ziel der Untersuchung folgendermaßen zusammenfassen: „Wovor schützt der Datenschutz?“

Bereits absehbar ist die Kritik an der Aufstellung einer Klassifikation bestimmter Datenschutzrisiken: Aufgrund der Natur von Informationen könne es kein belangloses Datum geben. Jede Datenverarbeitung stelle ein Risiko dar, weshalb sich eine Systematisierung erübrige. Richtig daran ist, dass sich Nachteile für das Individuum aus unterschiedlichsten Verwendungszusammenhängen ergeben können und diese wegen der Vielgestaltigkeit des Lebens niemals abschließend beschreibbar sind. Daraus folgt jedoch nicht, dass typische Risiken und typische Verwendungszusammenhänge nicht identifiziert werden könnten. Der von weiten Teilen der Literatur eingenommene resignative Standpunkt ist überholt.

Ohne einen Katalog einschlägiger Risiken und ohne eine präzise Vorstellung von Schutzgütern besteht die Gefahr, dass das Datenschutzrecht im Zustand der Überregulierung und des Vollzugsdefizits verharrt. Die Identifikation einschlägiger Risiken ist die notwendige Vorbedingung für die sinnvolle Abgrenzung von Erlaubtem und Verbotenem im Bereich der Verarbeitung personenbezogener Daten.

Das Erkenntnisinteresse gilt somit Risikokonzeptionen und Schutzgütern,[84] die den Datenschutzregelungen im Mehrebenensystem zugrunde liegen. Die Prämisse ist, dass einschlägige Risiken ihren Niederschlag bereits in den zahlreichen datenschutzrechtlichen Normen und Entscheidungen gefunden haben und demnach mit rechtswissenschaftlichen Methoden identifiziert werden können. Weil die Aussagen mutmaßlich in engem Zusammenhang mit Ausführungen zu den jeweiligen Schutzgütern stehen, werden diese in die Analyse einbezogen.

Das Forschungsziel lässt sich durch zwei Fragen konkretisieren: Die erste richtet sich darauf, welche Risikokonzeptionen und Schutzgüter datenschutzrechtlichen Normen zugrunde liegen. Hierzu sind „Steuerungsnormen“, wie beispielsweise Zielbestimmungen und Eingrenzungen des Anwendungsbereichs, aber auch Erwägungsgründe und Motive des Regelungsgebers zu untersuchen. Daneben werden die im normativen Material enthaltenen Datenschutzkonzepte, wie etwa das Recht auf Vergessen oder das Konzept der normativen Zweckbegrenzung, analysiert, um aufzuzeigen, welchen Risiken damit begegnet werden soll. Von besonderem Interesse ist hier die Frage, ob gemeinsame Risikokonzeptionen und Schutzgüter identifiziert werden können, obwohl die Regelungen auf unterschiedlichen Ebenen angesiedelt und in unterschiedlicher Weise verbindlich sind. Das Spektrum reicht dabei von bloßen Empfehlungen internationaler Zusammenschlüsse wie der OECD und dem Asiatisch-Pazifischen Wirtschaftsforum (APEC) bis hin zu rechtsverbindlichen Regelungen auf europäischer und nationaler verfassungsrechtlicher Ebene.

---

[84] Zu den Begriffen siehe unten IV.A.

Die zweite Forschungsfrage zielt auf eine Klassifikation der Risiken als Grundlage des Datenschutzrechts: Wie kann aus den identifizierten Risiken ein System gewonnen werden? Die Funktion einer solchen Klassifikation ist ähnlich derjenigen der Rechtsgutslehre für das Strafrecht: Es geht um Steuerung des Schutzumfangs und der Schutztechnik.[85] Im Unterschied zur Begrenzungsfunktion der strafrechtlichen Rechtsgutslehre ist das Ziel der vorliegenden Untersuchung jedoch offener: Die Klassifikation wird nicht mit dem Ziel der Rechtfertigung eines „Mehr" oder „Weniger" an Datenschutzrecht vorgenommen, sondern um eine rationalere Begründung des Datenschutzrechts zu erreichen und die weitere wissenschaftliche Befassung sowie die Reform des Datenschutzrechts in diese Richtung anzustoßen. Aus der Ausrichtung des Datenschutzrechts auf das Vorfeld konkreter Schäden folgt sodann die Verlagerung des Klassifikationsziels aus dem Bereich des Schutzguts in den des Risikos.

## IV. Methodik

Die Beantwortung der ersten Forschungsfrage (Identifikation von Risiken) erfolgt durch Gesetzesauslegung sowie Analyse von Rechtsprechung und juristischer Literatur. Dabei wird die Rechtslage in den ersten drei Teilen der Arbeit vorrangig *de lege lata* untersucht, wobei sich der besondere Forschungsertrag durch die Analyse unterschiedlicher Rechtsquellen (Gesetzesmaterialien, soft law, Gesetze, unionsrechtliche Rechtsakte, Rechtsprechung) auf verschiedenen Ebenen des Rechts unter dem einheitlichen Gesichtspunkt des Aufgreifens von Risiken ergeben soll. Das einfachgesetzliche Datenschutzrecht wird dabei nur in den für die jeweils untersuchten Konzeptionen relevanten Teilaspekten behandelt.[86]

Weil auch die Rechtsverbindlichkeit gerade im Datenschutzrecht kein für das hier verfolgte grundlegend-reformorientierte Ziel der Risiko-Identifikation maßgebliches Kriterium sein kann,[87] müssen Literaturkonzeptionen nicht schon dann aus der Untersuchung ausscheiden, wenn sie einen „überschießenden" rechtspolitischen Gehalt aufweisen. Maßgebliche Auswahlkriterien für die Literatur sind stattdessen ein enger Bezug zum geltenden Datenschutzrecht und die Ergiebigkeit im Hinblick auf Risiken. Diese dürfte vor allem bei solchem Schrifttum vorliegen, das eine in sich geschlossene Konzeption darstellt oder das – soweit es sich um ältere Werke handelt – von einer besonderen Wirkkraft auf die nachfolgende Verrechtlichung des Datenschutzes war.

---

[85] Zu diesem Ziel der Rechtsgutslehre des Strafrechts vgl. Kindhäuser/Neumann/Paeffgen-*Hassemer*, Vorbemerkungen zu § 1 Rn. 112.

[86] Zu den hierfür tragenden Erwägungen siehe unten IV.B.

[87] Andernfalls müsste das für das Datenschutzrecht so wichtige soft law unberücksichtigt bleiben, näher dazu Teil 1, I.

Die Untersuchungsreihenfolge innerhalb der Rechtsprechungsteile erfolgt historisch-systematisierend, einschlägige Entscheidungen werden also zunächst grundsätzlich in chronologischer Reihenfolge dargestellt. Sobald eine maßgebliche Risikokonzeption erstmals auftritt, wird die chronologische Darstellung jedoch durchbrochen und die weitere „Verzweigung" des Risikos in nachfolgenden Entscheidungen nachvollzogen. Diese Vorgehensweise ermöglicht die zusammenhängende Behandlung gleichartiger Risiken auch in der zeitlichen Entwicklungsdimension und wird damit sowohl der richterlichen Arbeitsweise gerecht, die auf Herstellung einer gefestigten Rechtsprechung bedacht ist, als auch dem Umstand, dass viele Risiken erst im Laufe der Zeit Gegenstand der Rechtsprechung wurden. Die Darstellungsreihenfolge der Literaturkonzeptionen folgt (absteigend) von deren jeweiliger Nähe zu geltendem Datenschutzrecht und der Aussagekraft im Hinblick auf Risiken.

Die zweite Forschungsfrage (Klassifikation) wird durch eine Systematisierung der in den Teilen 1 bis 3 gewonnenen Risiken verfolgt. Hierbei muss aufgrund der dargestellten Kontextabhängigkeit von Informationen „typisierend", also gerade nicht umfassend und abschließend vorgegangen werden. Die zu klassifizierenden Risiken sind jedoch – ähnlich wie auch Rechtsgüter im Strafrecht – keine „bloßen Abstraktionen", „gedanklichen Gebilde" oder „ideellen Werte", sondern „in der Wirklichkeit vorkommende soziale Interaktionsvorgänge".[88] Deshalb müssen auch Untersuchungen aus anderen Disziplinen und aktuelle tagespolitische Phänomene aufgegriffen werden, wobei hier aufgrund der umfänglichen und disziplinmäßigen Beschränkungen einer Einzeldissertation, anders als womöglich bei Dissertationen im Rahmen von Gemeinschaftsarbeiten (vgl. § 15 Abs. 2 Promotionsordnung der Rechtswissenschaftlichen Fakultät der Universität Freiburg i.d.F. vom 18.3.2000), kein vollständiger und fachgerechter Einbezug von Disziplinen wie beispielsweise der Sozialpsychologie erfolgen kann. Der umfassende Einbezug von Schrifttum aus Bereichen wie Soziologie oder Psychologie wäre mit wissenschaftlichem Anspruch nur im Rahmen einer Forschungsgruppe durch Mitarbeiter aus den jeweiligen Fachdisziplinen zu leisten. Gleichwohl liegt mittlerweile eine Reihe spezialisierter Untersuchungen und Überblickswerke vor,[89] welche die Klassifizierung bereichern und eine vertiefte Auseinandersetzung in den genannten Disziplinen anstoßen können. Darin liegt gerade kein „Eklektizismus", sondern eine durch die Zielsetzung gebotene Notwendigkeit interdisziplinären Vorgehens. Ein auf die reine Dogmatik beschränkter Ansatz würde die Untersuchung gleichsam „blind" für die Fragen der Realität werden lassen.[90] Die Kombination der empirischen und rechtsdogma-

---

[88] So für die in dieser Hinsicht vergleichbaren strafrechtlichen Rechtsgüter *Roxin*, AT I, S. 34 unter Verweis auf die Normentheorie von *Binding*.

[89] Siehe unten Teil 4, I.

[90] In Anlehnung an das Wort *Jeschecks*, wonach Strafrecht ohne Kriminologie blind ist und Kriminologie ohne Strafrecht grenzenlos ist, erfordert die Untersuchung von Grundlagenfragen auch hier das interdisziplinäre Vorgehen, vgl. *Jescheck*, Lehrbuch, S. 36.

tischen Methode ist überdies in der Grundlagenforschung anerkannt.[91] Im Rahmen der Systematisierung sind deshalb auch empirische Studien und Befragungen eingebracht worden, die im Zusammenhang mit dem normativen Gehalt des jeweiligen Risikos diskutiert werden. So wird z.B. hinterfragt, inwieweit der von der Rechtsprechung häufig angeführte „Überwachungsdruck“[92] bereits Gegenstand sozialpsychologischer Untersuchungen war.

## A. Schutzgut, Risiko, Risikokonzeption

Der Begriff „Schutzgut“ wird in Anlehnung an die Begriffsverwendung im Kontext des Bevölkerungsschutzes definiert. Ein Schutzgut ist demzufolge alles, was wegen seines ideellen oder materiellen Werts vor Schaden bewahrt werden soll. Unter einem „Schaden“ ist die negativ bewertete Auswirkung eines Ereignisses auf ein Schutzgut zu verstehen.[93] Der Begriff „Risiko“ wird bei dieser Untersuchung nicht als mathematisch darstellbares Produkt aus Ausmaß und Eintrittswahrscheinlichkeit eines Schadens[94] bzw. als Maß für die Wahrscheinlichkeit des Eintritts eines Schadens an einem Schutzgut[95] verstanden, sondern als Sachverhalt, indem ein Schadenseintritt an einem Schutzgut möglich ist und eine darauf bezogene normative Regelung zur Abwehr dieses Schadens besteht. Diese rechtliche Regelung zur Abwehr des ungewissen Schadens wird dementsprechend als „Risikokonzeption“ definiert. Solche Risikokonzeptionen lassen sich in allen normativen (präskriptiven) Texten identifizieren.

## B. Eingrenzung des Untersuchungsgegenstands

Das einfachgesetzliche Datenschutzrecht wird, wie oben angemerkt, nur in den für die jeweils untersuchten Konzeptionen relevanten Teilaspekten behandelt. Diese Eingrenzung ist durch das übergreifende Forschungsziel gerechtfertigt. Die Grundlagen, Ziele und wesentlichen Risiko- und Schutzgutkonzeptionen sind aufgrund der vollharmonisierenden unionsrechtlichen Vorgaben[96] und im Übrigen wegen Ausstrahlung und Vorrang des deutschen Verfassungsrechts auf diesen

---

[91] Vgl. *Sieber*, in: Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. (Hrsg.), Jahresbericht 2011, S. 40.

[92] Vgl. etwa BGH, Urteil vom 16.3.2010, VI ZR 176/09 = NZM 2010, 374.

[93] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.), BBK-Glossar, Einträge „Schutzgut“, „Schaden“.

[94] Vgl. *Ulbig/Hertel/Böl* (Hrsg.), Risikokommunikation, S. 8.

[95] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.), BBK-Glossar, Eintrag „Risiko“.

[96] EuGH Urteil vom 24.11.2011, verb. Rs. C-468/10 und C-469/10, ASNEF Rn. 28–32.

Ebenen ausreichend präsent: Dem nationalen Verfassungsrecht kommt darüber hinaus eine Stabilisierungsfunktion zu, die es im Hinblick auf einschlägige Risikokonzeptionen gegenüber dem z.T. widersprüchlichen und kurzlebigen einfachgesetzlichen Datenschutz zu einem für die hier verfolgten Forschungsziele geeigneteren Untersuchungsgegenstand macht.[97]

Von einer gesonderten Literaturanalyse nur des internationalen oder nur des europäischen Schrifttums wurde abgesehen, da die ausgewählten deutschen Literaturkonzeptionen bereits eine exemplarische und auch für den internationalen Diskurs repräsentative Auswahl darstellen.[98] Weiterhin musste angesichts der extremen Fülle des Schrifttums eine Eingrenzung vorgenommen werden. Besonders einschlägiges internationales Schrifttum wird zudem im Rahmen der Diskussion der gewonnenen Risiken im vierten Abschnitt einbezogen.

Der Schwerpunkt auf die für den europäischen Raum maßgeblichen Rechts- und Rechtserkenntnisquellen ist durch deren Wirkung auf die deutsche Rechtsentwicklung und ihr Potenzial zur Schaffung internationaler Mindeststandards für den Bereich des Datenschutzes begründet.

## C. Verwendung von Definitionen und Zitierweise

Begriffsdefinitionen erfolgen an der jeweils einschlägigen Stelle. Bei Zitaten wird „vgl." eingesetzt, wenn zwischen der entsprechenden Stelle der Dissertation und der Referenzstelle zwar größere Abweichungen bestehen bzw. eigene Anfügungen enthalten sind, diese jedoch für das Weglassen eines Nachweises als noch nicht ausreichend erachtet werden. „Vgl." wird ebenfalls eingesetzt, soweit lediglich auf einen ähnlichen Gedankengang verwiesen wird. Bei längeren paraphrasierten Stellen wird z.T. erst am Ende des Abschnitts ein Zitat gesetzt, wobei sich der wiedergebende Charakter durch Verwendung indirekter Rede, aus dem Kontext oder dem Zusatz „zum Ganzen" in der Fußnote ergibt. Der Zusatz „zum Ganzen" kann dabei auch eine nachfolgende paraphrasierte Stelle einleiten.

# V. Gang der Darstellung

Die Untersuchung besteht aus vier aufeinander aufbauenden Teilen. Die Teile 1 bis 3 folgen der Vorstellung eines rechtlichen Mehrebenensystems[99] und enthalten

---

[97] Zur Stabilisierungsfunktion von Verfassungsrecht *Gärditz*, Prävention, S. 25 ff.

[98] Dies dürfte auch daran liegen, dass in Deutschland sowohl die Einführung von Datenschutzgesetzen als auch die wissenschaftliche Befassung damit bereits sehr früh erfolgten, vgl. oben I.

[99] *Ast*, in: Bergmann (Hrsg.), Handlexikon EU.

die normative Analyse zur Identifikation der Risiken. Hiermit wird die Beantwortung der ersten Forschungsfrage vorgenommen. Teil 1 behandelt das Internationale Recht unter Einbeziehung der im Datenschutzrecht besonders wichtigen Spezialinstrumente und der Menschenrechtskataloge. Teil 2 analysiert das Recht der Europäischen Union (Primär- und Sekundärrecht) inklusive der datenschutzrechtlichen Reformvorschläge des Jahres 2012. Teil 3 betrifft die Ebene des nationalen deutschen Rechts, wobei zwischen Rechtsprechung des BVerfG und Literaturkonzeptionen untergliedert wird. Innerhalb der Ebenen wird nach Regelungsinstrumenten bzw. Konzeptionen differenziert. Innerhalb der Regelungsinstrumente bzw. Konzeptionen erfolgt die Prüfung von Risikokonzeptionen und Schutzgütern. Die Untersuchungsreihenfolge innerhalb der Rechtsprechungsteile erfolgt historisch-systematisierend.[100] Die Literaturkonzeptionen werden in absteigender Reihenfolge nach Maßgabe ihrer Nähe zu geltendem Datenschutzrecht und ihrer Aussagekraft im Hinblick auf Risiken bearbeitet. Überblicksabschnitte zu Beginn der Kapitel sowie Zwischenbetrachtungen werden verwendet, soweit dies zur Kontextualisierung erforderlich ist. Den Abschluss der Unterkapitel und Abschnitte bildet jeweils die Darstellung der (Zwischen-)Ergebnisse.

Teil 4 der Untersuchung enthält die typisierende Systematisierung der Risikokonzeptionen in Form einer vergleichenden Diskussion. Als Ergebnis wird eine Klassifikation bzw. ein Katalog von Risiken entwickelt. Dabei greifen Inhalt und Systematisierung die drei vorangegangenen Teile auf. Nach einer methodischen Vorbemerkung folgt die Diskussion struktureller Risiken auf einer Makroebene, danach die Besprechung individueller Risiken auf der Mikroebene und im Anschluss daran ein Abschnitt zu Risiken, die beide Ebenen betreffen. Den Abschluss bilden die Abschnitte zu Grenzfällen und Nicht-Risiken, die Schlussfolgerungen für Schutzgüter und ein Ausblick.

---

[100] Siehe oben IV.

*Teil 1*

# Internationales Recht

## I. Überblick

Datenschutzrecht hat sich auf mehreren Rechtsebenen und in verschiedenen Regionen der Welt als juristische Antwort auf unterstellte Risiken moderner Datenverarbeitung entwickelt.[1] Unterschiede bestehen im Hinblick auf kulturelle und politische Voraussetzungen.[2] Deshalb ist zu erwarten, dass aus den Rechtsquellen auf unterschiedlichen Regelungsebenen gemeinsame Risikokonzeptionen und Schutzgüter gewonnen werden können, welche dann im vierten Teil der Untersuchung klassifiziert und mit außerrechtlichen Bezügen und Prämissen diskutiert werden. Insofern nähert sich die Untersuchung dem zu schützenden Lebensbereich (Normbereich/Regelungsbereich) über das „Normprogramm" einschlägiger Regelungen.[3] Der Schwerpunkt liegt dementsprechend auf stärker „zielvorgebenden" Regelungen, insbesondere den „prinzipienartigen Vorrangnormen"[4] der Datenschutzgrundrechte.[5] Auf der Ebene des internationalen Rechts bestehen dabei Regelungen, denen für das Datenschutzrecht eine Vorläufer- und Modellfunktion[6] zukommt. Regelungen wie das Datenschutzübereinkommen des Europarats (Konvention 108)[7] und datenschutzrechtliche Spezialinstrumente, die dem soft law[8] zu-

---

[1] Zur „Frühgeschichte" des Datenschutzes *von Lewinski*, in: Arndt/Betz/Farahat/Goldmann u.a. (Hrsg.), Freiheit-Sicherheit-Öffentlichkeit; zur internationalen Gesetzgebungsentwicklung Simitis-*Simitis*, BDSG, Einl. Rn. 127–150.

[2] So legt man etwa in Schweden traditionell mehr Gewicht auf die Informationsfreiheit und Kommunikationsgrundrechte, was sich z.B. in dem Zurücktreten von Datenschutz hinter den Regelungen zum Aktenzugang niederschlägt, vgl. § 7 PUL. Nachvollziehen lässt sich dies auch an den starken Einwänden gegen die Einführung des Datenschutzgesetzes in Schweden, vgl. *Seipel*, in: Blume/Saarenpää (Hrsg.), Nordic Data Protection Law, S. 126 ff. sowie an der Erklärung Schwedens zu Transparenz und Informationszugang beim Beitritt zur EU, ABl. C 241 vom 29.8.1994, S. 397. Bestätigt wird dies zudem durch die in Umfragen deutlich werdenden geringeren Bedenken hinsichtlich übermäßiger Informationszugänglichkeit in Schweden, vgl. Europäische Kommission (Hrsg.), Eurobarometer 359, S. 60, 70 f., 75, 147.

[3] Zur hermeneutischen Differenzierung von Normprogramm und Normbereich vgl. *Hufen*, Staatsrecht II, S. 72 ff.

[4] *Mehde*, in: Heselhaus/Nowak (Hrsg.), HEG, S. 610.

[5] Zur Verankerung des Datenschutzes in den gemeinsamen Verfassungstraditionen der EU-Mitgliedstaaten *Mähring*, EuR 1991, 373.

[6] Simitis-*Simitis*, BDSG, Einl. Rn. 151 m.w.N.

[7] Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.1.1981, ETS No. 108, amtliche dt. Übersetzung: http://conventions.coe.int/Treaty/ger/Treaties/Html/108.htm [Stand: 28.3.2014].

zuordnen sind, stehen deshalb am Beginn der Untersuchung. Zum besseren Verständnis ist zunächst die historische Entwicklung der internationalen Instrumente nachzuzeichnen.

Die Entwicklung der Informations- und Kommunikationstechnologie (IKT) führte zwar zunächst auf nationaler Ebene zu Datenschutzgesetzen, die verschiedenen Phasen zugeordnet werden können und dabei jeweils bestimmten Regelungsmodellen folgten.[9] Der massive Anstieg von – auch grenzüberschreitenden – Datenverarbeitungen löste jedoch schon bald ein Bedürfnis nach international wirksamen Schutzinstrumenten aus.[10] Ein Recht auf Datenschutz war allerdings zu dieser Zeit in den internationalen Menschenrechtsverträgen noch nicht enthalten. Zwar konnte das Recht auf Achtung des Privatlebens als Anknüpfungspunkt dienen – dieses war in Art. 12 AEMR (1948), Art. 8 EMRK (1953) und Art. 17 IPBürg (1966) garantiert. Eine entsprechende Interpretation hatte sich allerdings noch nicht verfestigt.[11] Jedoch bestand damals der politische Wille, die sich abzeichnenden datenschutzrechtlichen Prinzipien international abzustimmen, um unnötige Unterschiede zwischen zukünftigen nationalen Gesetzen zu vermeiden.[12] Dies geschah dann in erster Linie mit dem Datenschutzübereinkommen des Europarats vom 28.1.1981 (Konvention 108)[13] und einer Reihe von parallel dazu entstehenden bzw. daran anschließenden datenschutzrechtlichen Spezialinstrumenten internationaler Organisationen. Erst im Anschluss an diese Rechtsquellen, die zum Teil dem soft law[14] zuzuordnen sind, folgte die interpretative Rezeption des Datenschutzes innerhalb der Menschenrechtsverträge und insbesondere im Rahmen der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR).[15] Im Folgenden werden die Spezialinstrumente, die Menschenrechtskataloge und im Anschluss die Rechtsprechung des EGMR untersucht, um damit die Entwicklung der Verrechtlichung

---

[8] Zum Begriff „soft law“: *Schwarze*, EuR 2011, 3 ff. sowie *Ehricke*, NJW 1989, 1906, kritisch: *Ipsen*, Völkerrecht, S. 251. Im Datenschutzrecht sind dies z.B. die Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten der OECD vom 23.9.1980, OECD – Dokument C (80) 58 (final), abgedruckt bei *Simitis* u.a., BDSG-Dok., D 12.1, oder die Empfehlungen des Europarats im Anschluss an die Konvention 108. Hierzu Simitis-*Simitis*, BDSG, Einl. Rn. 178.

[9] Diese Modelle reagierten auf empirische Bedingungen, deren Wandel sie schließlich nicht mehr gerecht wurden. So scheiterte etwa das insbesondere in Schweden und Norwegen verfolgte Regelungskonzept eines umfassenden Genehmigungsvorbehalts für jede Verarbeitung personenbezogener Daten an dem massiven Anstieg von Datenverarbeitungen, vgl. Simitis-*Simitis*, BDSG, Einl. Rn. 127 ff.

[10] *Siemen*, Grundrecht, S. 38 f.

[11] Für Art. 8 EMRK Simitis-*Simitis*, BDSG, Einl. Rn. 151.

[12] *Ellger*, Datenschutz, S. 461; vgl. auch *Siemen*, Grundrecht, S. 39.

[13] Siehe unten II.A.

[14] Siehe oben Anm. 8, zur Begriffsdefinition insbesondere *Ehricke*.

[15] Umfassend zur Entwicklung des Datenschutzes in der EMRK *Siemen*, Grundrecht, S. 51–211.

(von soft law zu verbindlicher Rechtsprechung des EGMR) nachzuvollziehen. Innerhalb der Spezialinstrumente richtet sich die Reihenfolge nach deren praktischer Bedeutung, wobei die Empfehlungen des Europarats (B., C.) – trotz ihrer, verglichen mit den OECD-Leitlinien, geringeren Bedeutung – unmittelbar im Anschluss an die Datenschutzkonvention des Europarats dargestellt werden, um den Sachzusammenhang zu wahren.

# II. Datenschutzrechtliche Spezialinstrumente

## A. Datenschutzkonvention des Europarats

### 1. Überblick

Die Datenschutzkonvention des Europarats vom 28.1.1981 (Konvention 108)[16] ist das erste rechtsverbindliche internationale Instrument speziell für den Bereich des Datenschutzes. Gegenwärtig ist sie von 43 der 47 Mitgliedstaaten des Europarats ratifiziert.[17] In Deutschland geschah dies am 19.6.1985. Sie trat am 1.10.1985 nach Erreichen der erforderlichen Mindestzahl von fünf Ratifikationen in Kraft.[18] Die Konvention 108 ist gem. Art. 4 Abs. 1 bindend für die Vertragsstaaten. Der Einzelne kann sich jedoch nur dann auf sie berufen, wenn sie in nationales Recht umgesetzt wurde (non self-executing treaty).[19] Die Konvention ist gem. Art. 23 offen für den (bisher allerdings noch nicht erfolgten) Beitritt von Nichtmitgliedstaaten des Europarats.[20] Ihr Ursprung geht auf das Jahr 1968 zurück. Die Parlamentarische Versammlung hatte das Ministerkomitee dazu aufgefordert, zu prüfen, ob die EMRK und die nationalen Rechtsordnungen ausreichenden Schutz des Persönlichkeitsrechts gegen Verletzungen durch „moderne wissenschaftliche und technische Methoden" bieten.[21] Nachdem in einem Zwischenbericht des Expertenausschusses für Menschenrechte Handlungsbedarf festgestellt worden war,[22] entstanden nach weiteren Vorarbeiten zwei Empfehlungen und danach die Konven-

---

[16] Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.1.1981, ETS No. 108.

[17] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=30/10/2011&CL=GER [Stand: 28.3.2014], deutsche Zitate beziehen sich auf die hier verlinkte amtliche Übersetzung. Zur rechtlichen Verbindlichkeit *Siemen*, Grundrecht, S. 40.

[18] Für Deutschland BGBl. II 1985, S. 538; Bekanntmachung S. 1134.

[19] *Gridl*, Datenschutz, S. 190 f.

[20] Zu Bestrebungen hinsichtlich einer Ausweitung der Konventionsmitglieder vgl. *Greenleaf*, CLSR 2009, 41.

[21] Rec. Nr. 509 vom 31.1.1968, http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta68/EREC509.htm [Stand: 28.3.2014].

[22] CoE DH./Exp (73) 17, S. 14 f.

tion.[23] In ihrem Art. 5 wurden erstmals allgemeine Verarbeitungsgrundsätze auf internationaler Ebene verbindlich festgeschrieben. Diese Grundsätze sind bis heute von überragender Bedeutung und haben sich auf alle nachfolgenden Datenschutzregelungen ausgewirkt.[24]

Die Bedeutung der Konvention zeigt sich neben den mit ihr eingeführten allgemeinen Verarbeitungsgrundsätzen auch daran, dass Rechtsakte der Europäischen Union auf sie Bezug nehmen, wenn zwar eine Harmonisierung erstrebt wird, jedoch die Übernahme der deutlicheren und schärferen Vorgaben der EG-Datenschutzrichtlinie politisch nicht durchsetzbar ist. So etwa beim Schengener Durchführungsübereinkommen, der Europol-Konvention und dem Eurojust-Beschluss.[25] Die Konvention wurde in der Folgezeit durch eine Vielzahl von Empfehlungen bereichsspezifisch ergänzt: so 1987 zur polizeilichen Tätigkeit,[26] 1995 zu Telekommunikationsdiensten, 1999 zum Internet.[27] 2001 folgte ein Zusatzprotokoll über Kontrollstellen und Drittstaatenweitergabe, das eine Anpassung an die entsprechenden Regelungen des EU-Datenschutzes brachte.[28] 2010 entstanden Empfehlungen zu Profiling und Datenschutz.[29] 2009 wurde eine Arbeitsgruppe mit der Überarbeitung der Konvention befasst.[30] Reformvorschläge wurden u.a. im Juni und September 2012 veröffentlicht.[31] Die Modernisierung soll an den Grundprinzipien festhalten und deren technikneutrale Natur sowie die Kohärenz und Kompatibilität mit dem Rechtsrahmen der Europäischen Union sicherstellen. Dabei soll der offene Charakter das Potenzial zur Schaffung globaler Mindeststandards ermöglichen.[32] Im Folgenden werden die materiellen Regelungsgehalte der Konvention auf einschlägige Risikokonzeptionen und Schutzgüter untersucht.

---

[23] Zum Ganzen *Siemen*, Grundrecht, S. 41 f.; zur Entstehungsgeschichte auch *Ellger*, Datenschutz, S. 460 ff.; *Mengel*, EuGRZ 1981, 376; Simitis-*Simitis,* BDSG, Einl. Rn. 151.

[24] Siehe unten II.A.2.d).

[25] Simitis-*Simitis,* BDSG, Einl. Rn. 183. Für Eurojust, Art. 14 Abs. 2 Beschluss 2002/187/JI vom 28.2.2002, ABl. Nr. L 063 vom 6.3.2002, S. 1–13.

[26] Siehe unten II.B.

[27] Simitis-*Simitis,* BDSG, Einl. Rn. 178 ff.; *Siemen*, Grundrecht, S. 41 sowie Fn. 92 zu weiteren Bereichen.

[28] Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, ETS 181 vom 8.11.2001. http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm [Stand: 28.3.2014].

[29] Siehe unten II.C.

[30] Zur Modernisierung *Gürtler*, RDV 2012, 126 (128).

[31] Final document on the modernisation of Convention 108 T-PD (2012)04Mos, vom 15.6.2012 sowie final document on the modernisation of Convention 108 T-PD(2012)04 rev en vom 17.9.2012, abrufbar unter http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp [Stand: 28.3.2014].

[32] T-PD (2012)04Mos, vom 15.6.2012, S. 5. Zum aktuellen Stand der Modernisierungsbestrebungen vgl. den Entwurf vom 18.12.2012, T-PD (2012)04 Rev4 E, abrufbar unter

## 2. Risikokonzeptionen und Schutzgüter

### *a) Vorwandfunktion des Grundrechtsschutzes*

Die Präambel der Konvention 108 beginnt mit einem Verweis auf das allgemeine Ziel des Europarats, eine auf Rechtsstaatlichkeit und Grundrechtsschutz beruhende engere Verbindung zwischen seinen Mitgliedern herbeizuführen. Sodann wendet sie sich den Schutzgütern zu. Nach Abs. 3 soll das Übereinkommen vor allem das Recht auf Achtung der Privatheit[33] („right to the respect for privacy" bzw. „le droit au respect de la vie privée") „erweitern". Die Erweiterung sei „wünschenswert" angesichts des „zunehmenden grenzüberschreitenden Verkehrs automatisch verarbeiteter personenbezogener Daten". Abs. 4 bekräftigt das Eintreten für die Informationsfreiheit „ohne Rücksicht auf Staatsgrenzen". In Abs. 5 wird die Notwendigkeit anerkannt, die „grundlegenden Werte der Achtung der Privatheit und des freien Informationsaustausches" in Einklang zu bringen.

Die materiellen Regelungen der Konvention beginnen in ihrem ersten Artikel mit Ausführungen zu „Gegenstand und Zweck". Danach dient das Übereinkommen insbesondere dem Schutz des „Rechts auf Privatheit" bei der automatischen Verarbeitung personenbezogener Daten. Der Schutz soll einzelnen Personen im Hoheitsgebiet der Vertragsstaaten unabhängig von Staatsangehörigkeit und Wohnort zukommen.

Die Aufzählungen in der Präambel, der erste Artikel und die Entstehungsgeschichte der Konvention verdeutlichen, dass der Schutz von Art. 8 EMRK im Vordergrund des Übereinkommens steht. Die Konvention selbst konkretisiert den geschützten Wert zwar nicht weiter, ein dahingehender Versuch findet sich allerdings in dem vorbereitenden Bericht des Expertenausschusses für Menschenrechte.[34] Darin beschreibt der Ausschuss zunächst optische und akustische Überwachungsmethoden und weist auf deren schnellen Wandel hin.[35] Sodann folgt eine rechtliche Analyse, die in der Feststellung mündet, dass es abgesehen von einzelnen Elemen-

---

http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp [Stand: 28.3.2014], siehe auch dort zum jeweils aktuellen Stand der Reformbestrebungen.

[33] Der Begriff „privacy" lässt sich am ehesten mit „Privatheit" übersetzen. Der teilweise in Übersetzungen verwendete Begriff „Privatsphäre" greift dabei mit der Voraussetzung von „Sphären" ein schon zu Beginn der US-amerikanischen Begriffsbildung kontroverses Konzept (Sphärentheorie) auf und ist deshalb ungeeignet, vgl. die Anmerkungen von *Weichert* zur Übersetzung des oben genannten Artikels von *Warren/Brandeis* (siehe oben Einleitung, I. Anm. 17), https://www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html [Stand: 28.3.2014]. Alternativ könnte man „privacy" auch mit „Persönlichkeit" übersetzen. Dies begegnet jedoch dem Einwand, dass hierfür bereits der Begriff „personality" existiert. Mittlerweile hat auch im US-amerikanischen Recht die Differenzierung zwischen Persönlichkeitsrecht und Datenschutzrecht eingesetzt, vgl. *Zimmer*, in: Szoka/Marcus (Hrsg.), The Next Digital Decade, S. 479, mit Verweisen in Fn. 14 auf Untersuchungen zu unterschiedlichen privacy-Ansätzen den USA einerseits und in der EU und Kanada andererseits.

[34] CoE DH./Exp (73) 17.

[35] Ebd., S. 6.

ten weder in internationalen noch in nationalen Rechtserkenntnisquellen eine allgemein akzeptierte Definition des Begriffs „Privatleben" i.S.v. Art. 8 Abs. 1 EMRK gibt.[36] Hierauf stützt die Kommission ihre Empfehlung zur Fortsetzung der Harmonisierungsbestrebungen und untersucht sodann Prinzipien für einen gemeinsamen Ansatz.[37] Anschließend folgen Ausführungen zu dem Wert („value"), der vom Recht auf Privatleben zu schützen ist. Hierzu zähle das Interesse des Einzelnen an einem Schutz gegen das Eindringen in das Intimleben einerseits („intrusion into his intimate life") sowie andererseits in jeden Teil der Existenz, welchen das Individuum in legitimer Weise für sich behalten möchte. Ein legitimes Interesse liege vor bei persönlicher Kommunikation und Beziehungen sowie – zirkelschlüssig – bei allen Ereignissen, die das Privatleben beeinträchtigen („all happenings that affect private life"). Als Beispiele werden genannt: Vorlieben, Stimme, Wohnung und Besitztümer, die zur persönlichen Sphäre („personal sphere") gehören.[38] Es folgt eine Aufzählung von gesetzwidrigen Beeinträchtigungen („unlawful interferences"), die sich an den anfangs beschriebenen Überwachungsmethoden orientiert und in „unlawful observation", „unlawful recording" sowie „utilisation of observations and recordings" gruppiert wird.[39] Die Erläuterungen des Ausschusses bleiben damit relativ vage. Zumindest kann daraus jedoch auf das Risiko der Offenbarung intimer Sachverhalte geschlossen werden. Aufgrund der Anbindung des legitimen Interesses an *alle* das Privatleben beeinträchtigenden Ereignisse wird die Risikokonzeption jedoch über den Intimbereich hinaus in denkbar weiter Weise ausgedehnt. Weiterhin bleiben die Erläuterungen zirkelschlüssig, da sie die zu klärende Frage nach der Beeinträchtigung des Rechts auf Privatleben mit dem Interesse bei „Ereignissen, die das Privatleben beeinträchtigen" definieren.

Die Entstehungsgeschichte der Präambel lässt zudem Zweifel an der zentralen Rolle des Persönlichkeitsrechts in den Konventionszielen aufkommen: Ursprünglich sollte die Präambel eine Passage enthalten, wonach die Beschränkung des grenzüberschreitenden Datenverkehrs nicht nur wegen grundrechtlicher Schutzgüter, sondern auch zum Schutz „wesentlicher Interessen" („essential interests") zulässig sein sollte. Diese wurde gestrichen, um sicherzustellen, dass wirtschaftliche Interessen nicht dem Persönlichkeitsrecht gleichgestellt und somit nicht Gegenstand des Datenschutzes werden können.[40] Der hohe Wert des Persönlichkeitsrechts wird hier offenbar nicht um seiner selbst willen herangezogen: Motiv ist vielmehr die durchscheinende Gefahr der „protektionistischen Zweckentfremdung" des Datenschutzes zum Schutz nationaler Wirtschaftsinteressen.[41] In diesem Zu-

---

[36] Ebd., S. 9 (Nr. 24).

[37] Ebd., S. 10 (Nr. 25 f.).

[38] Ebd., S. 11 (Nr. 32).

[39] Ebd., S. 17 (Nr. 24).

[40] *Henke*, Datenschutzkonvention, S. 50 f.

[41] Auch nach *Siemen*, Grundrecht, S. 45, handelt es sich „unverkennbar um ein Dokument einer internationalen Wirtschaftsorganisation".

sammenhang ist auch der Bezug der Präambel auf die Informationsfreiheit und auf den nötigen Ausgleich zwischen den Werten „Achtung des Persönlichkeitsbereichs“ und „freier Informationsaustausch“ zu sehen. Damit soll ausweislich des Erläuternden Berichts[42] klargestellt werden, dass andere Motive, insbesondere die Schaffung nicht tarifärer Handelshemmnisse oder eine Verringerung des Austauschs wissenschaftlicher und kultureller Informationen, nicht beabsichtigt waren und der Schutz nationaler Wirtschaftsinteressen nicht in die Abwägung eingestellt werden kann. Auch Art. 12 Nr. 2 und der Erläuternde Bericht hierzu bestätigen dieses implizit verfolgte Ziel: Der grenzüberschreitende Datenverkehr soll durch Mindestharmonisierung gegen nationale Handelsbarrieren „unter dem Vorwand“ des Persönlichkeitsrechtsschutzes gesichert werden.[43] Ausdrücklich stellt Nr. 20 des Erläuternden Berichts fest, dass diese Implementation verhindern soll, dass der freie Informationsfluss durch jedwede Art von Protektionismus beeinträchtigt wird: „that the principle of free flow of information would be jeopardised by any form of protectionism“. Für das Schutzgut folgt daraus, dass der genannte Schutz des Art. 8 EMRK konturlos bleibt und eher deklaratorische Züge erhält. Auch das nur angedeutete Risiko der Offenbarung intimer Sachverhalte wirkt neben dem ausführlicher behandelten Schutz vor Handelsbeeinträchtigungen nachrangig.

*b) Übergang von Persönlichkeitsrechtsschutz zu Datenschutzrecht*

Ein differenzierteres Bild entsteht bei Einbeziehung der Modernisierungsvorschläge vom 17.9.2012.[44] Diese sehen eine Veränderung hinsichtlich der Aufzählung von Schutzgütern in der Präambel vor. Der Bezug zum Recht auf Privatheit wird durchgehend durch das Recht auf Datenschutz ersetzt. Die Intensivierung von Datenverarbeitung und Datenaustausch erfordere es, die Menschenwürde, die Menschenrechte und Grundfreiheiten sowie insbesondere das „Recht zur Kontrolle der eigenen Daten und der Verwendung solcher Daten“ zu garantieren. Die Ersetzung des Rechts auf Privatheit durch das Recht auf Datenschutz wird konsequent an allen diesbezüglichen Stellen der Konvention durchgehalten. Weiterhin sehen die Modernisierungsvorschläge eine differenziertere Fassung der Gegeninteressen vor: Das Recht auf den Schutz personenbezogener Daten sei in seiner gesellschaftlichen Rolle zu sehen und mit anderen Menschenrechten und Grundfreiheiten, inklusive der Meinungsfreiheit, auszugleichen.[45]

---

[42] Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, Nr. 25 sowie Nr. 67. http://conventions.coe.int/Treaty/en/Reports/Html/108.htm [Stand: 28.3.2014]; vgl. auch *Henke*, Datenschutzkonvention, S. 52 f.

[43] Explanatory Report, Nr. 67.

[44] Siehe oben Anm. 31.

[45] T-PD (2012)04 Rev4 E S. 2 sowie T-PD (2012)04Mos, S. 8.

An den Modernisierungsvorschlägen zeigt sich somit die Verselbstständigung des Datenschutzrechts im Vergleich zum ursprünglich gewählten Anknüpfungspunkt des Rechts auf Privatheit, das in deutscher Terminologie dem Persönlichkeitsrecht zugeordnet werden kann. Dies bestätigen auch die Vorschläge zur Reform des Erläuternden Berichts,[46] in denen die Herausbildung im Rahmen von Art. 8 EMRK und Art. 8 EU-GRC angesprochen wird.[47] Hinsichtlich des Inhalts erlauben die Modernisierungsvorschläge dagegen, wie auch schon die Materialien zur Entstehung der Konvention, nur wenige Aussagen. Einschlägige Risikokonzeptionen werden allenfalls angedeutet, wenn hinsichtlich des Schutzgutes der Menschenwürde und der Ausübung von Kontrolle über die eigenen Daten an die Risiken von Würdeverletzungen und Kontrollverlust angeknüpft wird. In dem Entwurf zum Erläuternden Bericht wird zudem der Vorfeldcharakter des Datenschutzrechts betont: Diesem komme ein „ermöglichender" Charakter zu („not an isolated right but an enabling one"); ohne es könnten andere Rechte nicht in gleicher Weise ausgeübt werden.

Der Entwurf für die Modernisierung des Erläuternden Berichts bestätigt diese Befunde. Zunächst unterstreicht er das Risiko von Verletzungen der Menschenwürde durch Behandlung des Menschen als bloßes Objekt. In diesem Zusammenhang wird in Nr. 7 betont, dass Entscheidungen, die allein aufgrund automatisierter Datenverarbeitung erfolgen, nicht ohne das Recht der Betroffenen zur Stellungnahme („right to express their views") möglich sein sollen. Nr. 8 und 9 unterstreichen dagegen die Bedeutung der Meinungsäußerungsfreiheit, die mit dem Internet eine neue Dimension erhalten habe. Keinesfalls solle Datenschutz so ausgelegt werden, dass er Barrieren für Informationsflüsse errichte oder den Informationsaustausch und die Innovation behindere.

### *c) Informationsmacht*

Ein weiteres Risiko thematisiert der Erläuternde Bericht in seiner Fassung vor der Modernisierung, während die Modernisierungsvorschläge dazu keine Stellung mehr nehmen: In Nr. 2 des Berichts wird auf die mit „Informationsmacht" („information power") einhergehende soziale Verantwortung Bezug genommen. Weil in modernen Gesellschaften eine Vielzahl von Entscheidungen über das Individuum mittels in Computern gespeicherter Daten erfolge, müsse sichergestellt werden, dass die Vorteile dieser Form von Datenverarbeitung nicht zugleich zu einer Schwächung der Betroffenen führten.[48] Zwar bestünden auf der Ebene der Mitgliedstaaten bereits Vorschriften aus anderen Regelungsbereichen, die zu diesem Ziel beitrügen („laws on privacy, tort, secrecy or confidentiality of sensitive infor-

---

[46] T-PD (2012)04Mos, S. 31 f.

[47] Ebd., S. 32.

[48] Explanatory Report, Nr. 2.

mation“). Was hingegen fehle, seien allgemeine Regelungen über die Speicherung und Verwendung personenbezogener Informationen, die es dem Einzelnen erlaubten, Kontrolle über auf ihn bezogene und von anderen gespeicherte Informationen auszuüben.[49] Neben dem hier angesprochenen Schutzgut der Selbstbestimmung wird das Risiko von Machtverschiebungen und Manipulationsmöglichkeiten am Begriff „Informationsmacht“ deutlich.

*d) Allgemeine Regelungskonzeptionen und Grundsätze*

Kernstück der Konvention 108 sind die in Art. 5 erstmals auf internationaler Ebene verbindlich festgeschriebenen allgemeinen Datenschutzgrundsätze. Sie stellen neben den Vorschriften über besondere Arten von Daten (Art. 6), den Betroffenenrechten (Art. 8) und der Sanktionierung von Verstößen (Art. 10) den „harten Kern“ des Datenschutzrechts in Europa dar.[50] Das bis heute andauernde Festhalten an diesen Grundsätzen wurde zuletzt in einer umfassenden rechtsvergleichenden Studie im Auftrag der Europäischen Kommission bestätigt, der zufolge die wesentlichen Datenschutzgrundsätze „keiner größeren Änderung“ angesichts neuer Herausforderungen bedürften.[51] Die Modernisierungsvorschläge aus dem Jahr 2012[52] sehen zwar verschiedene Veränderungen und Ergänzungen vor, lassen jedoch die Grundsätze bestehen. Bedeutend ist vor allem die für Art. 2 lit. c) vorgesehene Erweiterung des Verarbeitungsbegriffs auf die Phase der Daten*erhebung*, die zuvor in der Konvention nur punktuell einbezogen worden war. Bei den Grundsätzen sieht die Modernisierung zunächst die Veränderung der Überschrift des Art. 5 von „Qualität der Daten“ zu „Legitimität der Datenverarbeitung und Qualität der Daten“ vor. Der neu vorgeschlagene erste Absatz des Art. 5 stellt einen Verweis auf die Notwendigkeit des fairen Ausgleichs zwischen den beteiligten Interessen und Rechten in allen Phasen der Verarbeitung voran. Ein zweiter Absatz sieht die Notwendigkeit der eindeutigen, spezifischen und informierten Einwilligung (a) sowie einen informationellen Gesetzesvorbehalt für die verbleibenden Fälle vor, in denen keine Einwilligung vorliegt (b). Der vorgeschlagene dritte Absatz stimmt im Wesentlichen mit dem bestehenden Art. 5 überein. Dieser fasst unter den Grundsatz der Datenqualität die rechtmäßige, nach Treu und Glauben erfolgende Beschaffung und Verarbeitung personenbezogener Daten, den Zweckbegrenzungsgrundsatz, den Grundsatz der sachlichen Richtigkeit und Aktualität sowie den Grundsatz der frühestmöglichen Depersonalisierung der Daten. Die Modernisierung bringt hier verschiedene Präzisierungen und Klarstellungen an.

---

[49] Explanatory Report, Nr. 3.

[50] Simitis-*Simitis*, BDSG, Einl. Rn. 146 und 158.

[51] *Korff/Brown*, in: Europäische Kommission (Hrsg.), Vergleichende Studie, S. 2.

[52] T-PD(2012)04 rev en sowie T-PD(2012)04 rev4 E.

Der in Art. 5 lit. a) der geltenden Fassung festgeschriebene Grundsatz einer nach Treu und Glauben erfolgenden Beschaffung in rechtmäßiger Weise ist im Sinne einer Grundsatzentscheidung für die Verrechtlichung der Datenverarbeitung zu verstehen. Bereits nach geltender Fassung kann daraus das Erfordernis der grundsätzlichen Beteiligung der Betroffenen an Verarbeitungsvorgängen sowie das Verbot der Erhebung von Daten, die durch Drohung oder Täuschung erlangt wurden, abgeleitet werden. Die Datenverarbeitung ist prinzipiell nicht rechtmäßig, wenn sie ohne Kenntnis des Verarbeitungssubjekts geschieht. Dabei werden jedoch Ausnahmen für den Bereich der polizeilichen Ermittlungstätigkeit anerkannt.[53] Dieser Grundsatz dürfte bei Übernahme des Einwilligungs- und Gesetzlichkeitsprinzips der Modernisierungsvorschläge an Bedeutung verlieren.

Sowohl das modernere Konzept der Einwilligung und Gesetzlichkeit als auch das ältere Prinzip der Rechtmäßigkeit der Verarbeitung nach Treu und Glauben verdeutlichen das Schutzgut der Selbstbestimmung. Indem der Einzelne informiert wird und ggf. auch der Verarbeitung zustimmen muss, soll er vor Fremdbestimmung geschützt werden. Auch im Fall der gesetzlichen Erlaubnis der Datenverarbeitung tritt diese Konzeption hervor, da der Zweck von Gesetzesvorbehalten auch und gerade in der Schaffung von Vorhersehbarkeit von Entscheidungen für das davon betroffene Individuum liegt. Weiterhin deutet die Konzeption auch auf das Risiko eines Überwachungsdrucks hin. Ein solcher kann entstehen, wenn sich das Recht aus der staatlichen Informationstätigkeit zurückzieht und der Einzelne nicht weiß, welche Informationen über ihn auf welchem Wege dem Staat zugänglich sind. Dieses Risiko wird auch von Art. 8 aufgegriffen, der Informations- und Berichtigungsrechte für Betroffene bereitstellt. Diese Rechte, die auch unter dem Stichwort der Transparenz zusammengefasst werden können, werden in den Modernisierungsvorschlägen ausgeweitet und präziser beschrieben.

Der in Art. 5 lit. b) und c) fixierte Grundsatz der normativen Zweckbegrenzung besagt, dass personenbezogene Daten nur zu festgelegten und rechtmäßigen Zwecken gespeichert und nicht in damit unvereinbarer Weise verwendet werden dürfen. Außerdem müssen die Daten für diese spezifischen Zwecke erheblich sein und dürfen nicht darüber hinausgehen. Weiter aufteilen lässt sich der Grundsatz somit in Teilbereiche wie Zweckfestlegung, Zweckentsprechung, Zweckrelevanz, Verwendungsbegrenzung und Erhebungsbegrenzung. Das zugrunde liegende Risiko scheint zunächst ebenfalls der Überwachungsdruck zu sein, der entstehen kann, wenn durch Informationen ein „virtuelles Abbild" sozialer Beziehungen in ihrer Gesamtheit hergestellt wird. Voraussetzung für die Vermeidung eines Gesamtbildes ist zunächst die Identifikation einzelner sozialer Beziehungen und anschließend deren Trennung. Diese Steuerung soll durch den Grundsatz der normativen Zweckbegrenzung erreicht werden.[54] Soweit man in die Konvention die Pflicht zur Mittei-

---

[53] *Henke*, Datenschutzkonvention, S. 100 f.

[54] *von Zezschwitz*, in: Roßnagel (Hrsg.), Handbuch, S. 221.

lung der Zwecke hineinliest,[55] tritt der Schutz des Individuums vor dem Risiko der Fremdbestimmung hervor.

Jedoch lässt sich aus der Verwendungsbegrenzung präziser auf ein anderes Risiko schließen. So können Informationen aus einem Bereich – beispielsweise zu riskantem oder verpöntem Freizeitverhalten – in einem anderen Bereich – beispielsweise Berufsleben – zu negativen Auswirkungen führen. Das so umrissene Risiko kann als *Entkontextualisierung* beschrieben werden.

Weiterhin etabliert Art. 5 lit. d) der geltenden Fassung der Konvention das Prinzip der sachlichen Richtigkeit und Aktualität der Daten. Das durch dieses Prinzip betroffene Risiko sind die Fehlerhaftigkeit von Informationen und daraus resultierende Schäden bei Verwendung der Informationen im Rahmen von Entscheidungen. Das in Art. 5 lit. e) vorgesehene Prinzip der frühestmöglichen Depersonalisierung verdeutlicht ebenfalls das Risiko des Überwachungsdrucks. Der Depersonalisierung kommt jedoch zudem die Funktion zu, einerseits eine zeitliche Grenze zu etablieren und damit das Risiko der Informationspermanenz, also einer dauerhaften Verfügbarkeit der Daten ohne Löschungsmöglichkeit, zu vermeiden. Weiterhin können Daten durch unbefugte Dritte erlangt werden und in diesem Fall zu Missbräuchen – etwa zu Erpressungen oder zur Inanspruchnahme von Internet-Dienstleistungen mittels Erstellung von Scheinidentitäten – verwendet werden. Das Prinzip betrifft somit auch das Risiko der *individuellen Verletzlichkeit* durch Verfügbarkeit personenbezogener Informationen.

Art. 6 der Konvention enthält einen Katalog besonderer Arten von Daten, die nur automatisch verarbeitet werden dürfen, wenn das innerstaatliche Recht geeigneten Schutz gewährleistet. Die Aufzählung umfasst die rassische Herkunft, politische Anschauungen, religiöse oder sonstige Überzeugungen, gesundheits- oder sexualbezogene Daten sowie Daten über Strafurteile. Die Modernisierungsvorschläge sehen eine Veränderung der Überschrift zu „Verarbeitung sensibler Daten“ vor und formulieren den Wortlaut neu. Neben einer präziseren Regelungstechnik wird auch der Katalog erweitert. Demnach dürfen personenbezogene Daten nicht verarbeitet werden, um die rassische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit sowie religiöse oder sonstige Glaubensvorstellungen aufzudecken. Ferner dürfen sie nicht zur Gewinnung biometrischer Informationen verarbeitet werden. Das grundsätzliche Verbot wird neben den in der geltenden Fassung genannten Kategorien auch auf genetische Daten ausgeweitet sowie auf solche, die Straftaten oder damit zusammenhängende Sicherheitsmaßnahmen betreffen. Weiterhin sieht der Vorschlag eine Generalklausel für Daten vor, die ein ernsthaftes Risiko für die Interessen, Rechte und Grundfreiheiten des Betroffenen, insbesondere durch das Risiko der Diskriminierung, begründen.

---

[55] So *Henke*, Datenschutzkonvention, S. 103.

Das Konzept des Schutzes sensibler Daten lässt bereits in der geltenden Fassung – und explizit nach Maßgabe der Reformvorschläge – auf das Risiko der Diskriminierung schließen. Der Begriff „Diskriminierung" kann als kategoriale Behandlung einer Person und eine damit verbundene negative Bewertung (Devaluation) verstanden werden. Unter einer kategorialen Behandlung ist die Verwendung einer sozialen Kategorie zur Bezugnahme auf eine Person oder deren Herkunft zu verstehen.[56] Die genannten Datenkategorien ermöglichen die nähere Eingrenzung der so verstandenen Diskriminierung. Zum einen handelt es sich um Daten, deren Bezugspunkt eine besondere Polarisierung hervorruft, wie etwa bei Daten zu politischen Anschauungen oder religiösen Vorstellungen. Die zweite Gruppe lässt sich unter dem Stichwort „Schambesetzung" zusammenfassen. Hierunter fallen die auf Sexualität bezogenen Daten und bis zu einem gewissen Grad auch Gesundheits- und Strafurteilsdaten. Bei den beiden letzteren kann neben der negativen Bewertung auch die Benachteiligung im Arbeitskontext als eigenständiges Risiko, das nicht zwangsläufig mit einer Devaluation einhergehen muss, festgehalten werden. Dieses Merkmal lässt sich als *Leistungsindikation* beschreiben.

Genetische und biometrische Daten betreffen hingegen Informationen, die eine eindeutige Identifizierung ermöglichen und darüber hinaus eine besondere Aussagekraft zu weiteren Persönlichkeitsmerkmalen aufweisen. Dieser Effekt kann als *Informationsemergenz* charakterisiert werden. Unter dem Begriff „Emergenz" wird das Auftreten neuer, nicht voraussagbarer Qualitäten beim Zusammenwirken mehrerer Faktoren verstanden.[57] Genau dieser Effekt „überschießender" Rückschlüsse kann auch im Fall der Kombination von Daten auftreten und charakterisiert deshalb das Risiko der Informationsemergenz. So ermöglichen etwa bestimmte genetische Daten Rückschlüsse auf Erbkrankheiten. Mittels biometrischer Daten lassen sich im Internet vorhandene Bilddaten personalisieren und dann beispielsweise durch Kombination mit einer Auswertung sozialer Netzwerke Rückschlüsse auf das Verhalten erbkranker Personen gewinnen. Bis zu einem gewissen Grad trifft diese Generierung neuer Aussagen zwar auf alle personenbezogenen Daten zu, bei genetischen und biometrischen Daten ist sie jedoch aufgrund der eindeutigen Identifizierbarkeit und hohen Aussagekraft besonders hervorzuheben.

Art. 7 der Konvention betrifft technische Sicherungsmaßnahmen gegen unbefugte Verwendung und zufälligen Verlust. Hier tritt wiederum das Merkmal der individuellen Verletzlichkeit besonders hervor.

Weiterhin sieht Art. 8 des Modernisierungsvorschlags das Recht vor, nicht Adressat einer allein auf automatisierter Datenverarbeitung gestützten erheblichen Entscheidung zu sein, ohne dass die Ansichten des Betroffenen dabei berücksich-

---

[56] Definitionen in Anlehnung an *Wagner* u.a., Diskriminierungen, S. 3.

[57] http://www.duden.de/rechtschreibung/Emergenz [Stand: 20.2.2013].

tigt werden. Hiermit wird, wie bereits oben dargestellt,[58] auf das Risiko der Objektmachung abgezielt. Das einschlägige Schutzgut ist somit die Menschenwürde.

### 3. Zwischenergebnis

Hinsichtlich der Schutzgüter knüpft die Konvention zwar an das Recht auf Achtung des Privatlebens, Art. 8 Abs. 1 EMRK an; diesem kam jedoch zur Zeit der Entstehung der Konvention noch kein über eine vage Vorstellung von optischen und akustischen Überwachungsmaßnahmen hinausgehender materieller Gehalt zu. Das einzige in dieser Frühphase angedeutete Risiko ist die Offenbarung intimer Sachverhalte. Im Übrigen stellt sich das Schutzgut als relativ unscharfe Vorstellung verschiedener Sphären dar. Wesentlich besser fassbar und anhand der Entstehungsgeschichte nachzuvollziehen ist das Risiko der „protektionistischen Zweckentfremdung" des Datenschutzes, d.h. der vorgeschobenen Berufung auf Datenschutzgründe zum Schutz nationaler Wirtschaftsinteressen durch nichttarifäre Handelshemmnisse. Hieraus folgt das paradoxe Ergebnis, dass die Datenschutzkonvention – bis zu einem gewissen Grad – auch der Verhinderung von Datenschutzrecht dient. Das Risiko nichttarifärer Handelshemmnisse ist jedoch ein spezifisch wirtschaftspolitisches (Außenhandelsbeschränkung). Der Freihandel wäre hier das einschlägige – jedoch nicht datenschutzspezifische – Schutzgut. Das Datenschutzrecht verfolgt bei einer derartigen Konzeption den Schutz von Individuen nur beiläufig-mittelbar, der Grundrechtsschutz wird bloßer Vorwand.[59]

Als zweites Zwischenergebnis ist der begriffliche Übergang vom (unklaren) persönlichkeitsrechtlichen Schutzgut hin zur Einbeziehung der Datenschutzgrundrechte im Rahmen der Modernisierungsvorschläge des Jahres 2012 festzustellen. Hiermit wird die Verselbstständigung bzw. „Konstitutionalisierung" des Datenschutzes als grundrechtliche Schutzposition auf europäischer Ebene nachvollzogen.[60]

Das eher aus übergreifender, gesellschaftlicher Perspektive zu sehende Risiko informationeller Machtverschiebungen wird durch die Anknüpfung des Erläuternden Berichts an den Schutz vor „Informationsmacht" und die damit einhergehende soziale Verantwortung der verarbeitenden Stellen angedeutet. Ein entsprechendes Schutzgut wären insoweit die Selbstbestimmung und die Handlungsfreiheit.[61]

Die ergiebigsten Rückschlüsse folgen aus der Untersuchung der allgemeinen Regelungskonzeptionen, insbesondere der Datenschutzgrundsätze, die mit der Konvention erstmals auf internationaler Ebene normiert wurden und auch im Rahmen der anstehenden Modernisierung in ihren Grundaussagen unverändert bleiben sol-

---

[58] Siehe oben II.A.2.b).

[59] Siehe oben II.A.2.a).

[60] Siehe oben II.A.1.

[61] Siehe oben II.A.2.c).

len. Sie lassen auf die Schutzgüter der Selbstbestimmung und der Menschenwürde schließen. Einschlägige Risiken sind neben der Fremdbestimmung vor allem der Überwachungsdruck durch unregulierte Informationsverarbeitung und umfassende Verfügbarkeit. Neben diesem Risiko verdeutlicht insbesondere die normative Zweckbegrenzung das Risiko der Entkontextualisierung von Informationen, womit die Schadensmöglichkeit aus bereichsübergreifender Informationsverfügbarkeit, beispielsweise Freizeit/Arbeitsleben gemeint ist. Ein weiteres in diesem Zusammenhang betroffenes Risiko ist die Erhöhung individueller Verletzlichkeit durch unbefugte Nutzung personenbezogener Daten. Daneben wird das Risiko der Diskriminierung aufgegriffen, das in Form einer kategorialen Behandlung und negativen Bewertung (Devaluation) von Personen auftritt. Aus den in der Konvention normierten Kategorien konnte eine Bestimmung gemeinsamer Kriterien sensibler Daten gewonnen werden. Diese Daten werden demnach durch eine besondere Polarisierung, Schambesetzung, Leistungsindikation oder *Informationsemergenz* charakterisiert. Letzteres ist ein eigenständiges Risiko, das bei der Möglichkeit „überschießender" Rückschlüsse aus bestimmten Daten auftritt. Von den allgemeinen Regelungskonzeptionen lediglich angedeutet wird hingegen das Risiko der *Informationspermanenz*, das aus der dauerhaften Verfügbarkeit von Informationen und dadurch ermöglichten Missbrauchspotenzialen resultiert.[62]

## B. Empfehlungen des Europarats zur polizeilichen Tätigkeit

### 1. Überblick

Die Empfehlungen des Ministerkomitees des Europarats über die Regulierung der Verwendung personenbezogener Daten im Polizeibereich vom 17.9.1987[63] stellen den ersten Versuch der Angleichung der Datenverarbeitung im Sicherheitsbereich dar. Sie sind damit ein Beispiel für das bereits früh verfolgte Ziel der Ergänzung der allgemeinen Datenschutzkonvention durch bereichsspezifische Regelungen. Dieses Ziel wird auch in den Modernisierungsvorschlägen zur Konvention festgehalten.[64] Die Empfehlungen sehen im Einzelnen Aufsichtsbehörden vor (Principle 1) und enthalten allgemein gefasste Vorschriften über die Datenerhebung. Sie bauen dabei auf der Konvention 108 auf und sehen u.a. die Prinzipien der Erforderlichkeit (Principle 2.1, Principle 7), der normativen Zweckbegrenzung (Principle 4), der Datenrichtigkeit (Principle 5.5.ii., 7.2), der Datensicherheit (Principle 8) sowie Informationspflichten (Principle 2.2) vor. Einen besonderen Augenmerk legen die Empfehlungen auf die Anregung zur gesetzlichen Normierung von

---

62 Siehe oben II.A.2.d).

63 Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector.

64 T-PD (2012)04Mos, S. 89 f.

Verarbeitungsbefugnissen (insb. Principle 2.1, 2.3, 5.2.i., 5.3.i., 5.4.a.) sowie auf grenzüberschreitende Mitteilungen (5.4). Das Hauptziel ist damit der Anstoß zur Verrechtlichung der informationellen Polizeitätigkeit.

### 2. Risikokonzeptionen und Schutzgüter

Rückschlüsse auf Risiken oder Schutzgüter, die über das hinausgehen, was bereits aus den allgemeinen Regelungskonzeptionen der Konvention folgt,[65] erlauben die Empfehlungen nur in geringem Ausmaß. Beachtlich ist jedoch, dass Umstände aufgegriffen werden, die für den Informationswert der Daten relevant sind. So enthält das dritte Prinzip (3.2) die Empfehlung, zwischen verschiedenen Kategorien von Daten, vor allem hinsichtlich deren Grad von Genauigkeit und Glaubhaftigkeit zu differenzieren. Im Einzelnen soll u.a. eine kategoriale Trennung erfolgen zwischen Daten, die sich auf Fakten stützen, und solchen, die auf bloßen Meinungen und persönlichen Wertungen basieren. Entsprechend empfiehlt dann auch Prinzip 5.5.ii. die Überprüfung von Informationen, die auf persönlichen Ansichten oder Wertungen beruhen, vor allem hinsichtlich ihrer Genauigkeit und Glaubhaftigkeit, bevor sie Behörden anderer Länder mitgeteilt werden. Hierin scheint das Risiko der Entkontextualisierung auf, welches im internationalen Informationsaustausch zwischen Strafverfolgungsbehörden zu besonderen Gefahren führt, wenn beispielsweise Auslieferungsentscheidungen oder freiheitsentziehende Maßnahmen auf diese Angaben gestützt werden. Das Entkontextualisierungsrisiko manifestiert sich insoweit nicht schon durch die bloße Übernahme in einen anderen Kontext – was hier in Anlehnung an eine medizinische Begriffsverwendung[66] als *Kontextinfiltration* bezeichnet wird –, sondern vielmehr durch die Nichtübernahme von Informationen aus dem ursprünglichen Kontext wie beispielsweise hinsichtlich der Glaubwürdigkeit von Zeugenaussagen, die für den Verdachtsgrad erforderlich sein können. Diese Facette der Entkontextualisierung lässt sich als *Kontextdefizit* beschreiben.

### 3. Zwischenergebnis

Die Empfehlungen lassen damit Rückschlüsse auf das Risiko der Entkontextualisierung in Form eines Kontextdefizits zu, das von dem Risiko der Kontextinfiltration zu unterscheiden ist.

---

[65] Siehe oben II.A.2.d).

[66] http://de.wikipedia.org/wiki/Infiltration_%28Medizin%29 [Stand: 28.3.2014].

## C. Empfehlungen des Europarats zu Profiling und Datenschutz

Die vom Ministerkomitee des Europarats am 25.11.2010 verabschiedeten Empfehlungen zu Profiling und Datenschutz[67] sind als Ergänzung der Konvention 108 zu sehen und übernehmen im Wesentlichen deren Regelungskonzeptionen für den Bereich des „Profiling". Zwar lassen sich aufgrund der Übernahme aus den materiellen Regelungen keine über die Konzeptionen der Datenschutzkonvention[68] hinausgehenden Rückschlüsse auf Risiken und Schutzgüter ziehen; etwas anderes gilt jedoch für die Definitionen der Begriffe „Profiling" und „Profil" sowie insbesondere für die mit der Empfehlung verfolgten Zwecke.

Unter „Profiling" wird entsprechend der Definition in Nr. 1 e) des Appendix die Anwendung eines Profils auf ein Individuum verstanden, wenn dadurch insbesondere eine die Person betreffende Entscheidung getroffen werden soll oder wenn sie zur Analyse oder zur Vorhersage persönlicher Präferenzen, Verhaltensweisen oder Einstellungen erfolgt. Unter einem „Profil" wird gem. Nr. 1 d) des Appendix eine Gruppe von Daten verstanden, die eine Kategorie von Individuen charakterisieren und dafür vorgesehen sind, auf ein Individuum angewendet zu werden. In der Präambel werden die Risiken beschrieben, welche die Grundlage der Empfehlung bilden: Die zunehmend konvergente Technik erlaube den Einsatz von Profilen, um Individuen durch die Verknüpfung einer großen Anzahl von Beobachtungen in vorgefertigte Kategorien einzuordnen und sei deshalb in der Lage, sich auf deren Leben auszuwirken. Dabei werden insbesondere die fehlende Transparenz, die Unkenntnis der Betroffenen und die mangelhafte Genauigkeit der Profile thematisiert. Soweit zur Profilbildung besondere Arten von Daten im Sinne des Art. 6 der Konvention 108 eingesetzt würden, könnten durch Profiling neue sensible Daten ohne das Wissen der betroffenen Personen erstellt werden. Diese Daten gingen mit einem besonders hohen Risiko für Diskriminierungen und Angriffen auf das Persönlichkeitsrecht sowie auf die Würde der Betroffenen einher. Wiederholt stellt die Präambel den Bezug des Profiling zur Menschenwürde und zu verschiedenen Formen der Diskriminierung her (Diskriminierung aufgrund von Geschlecht, rassischer oder ethnischer Herkunft, Religion oder Glaube, Behinderung, Alter, sexueller Orientierung). Einen eigenen Akzent setzt auch die Pressemitteilung, welche neben dem Menschenwürdebezug und den Diskriminierungsrisiken auch das Risiko der Stigmatisierung aufführt. Der Bezug auf die Menschenwürde wird aus dem „ungerechtfertigten Entzug des Zugangs zu bestimmten Gütern oder Dienstleistungen" gefolgert.[69]

---

[67] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

[68] Siehe oben II.A.2.d).

[69] Pressemitteilung 892 (2010); https://wcd.coe.int/ViewDoc.jsp?id=1711857&Site=COE [Stand: 28.3.2014].

Allein der ungerechtfertigte Entzug des Zugangs begründet jedoch noch keine Menschenwürde-Relevanz. Das Schutzgut der Menschenwürde ist jedoch dann berührt, wenn man in den beschriebenen, für die Betroffenen unvorhersehbaren und unkontrollierbaren Profilingmethoden eine Behandlung des Menschen als bloßes Objekt sieht. Neben dieses Schutzgut tritt das Risiko der Diskriminierung, das im Fall des Profilings aus einer unzureichenden „Konstruktion" der Profile folgen kann. Derartig konstruierte Profile selektieren einseitig und diskriminieren damit entsprechend der oben dargestellten Definition des Diskriminierungsbegriffs, nämlich im Sinne einer kategorialen Behandlung von Personen und der damit einhergehenden Devaluation.[70] Die Devaluationskomponente könnte in diesen Fällen zwar fraglich sein. Zumindest dann, wenn ein Zugangsentzug *und* das Anknüpfen an eines der genannten besonderen Merkmale auftritt, liegt die Annahme der Devaluation jedoch nahe. Dafür spricht insbesondere auch die Schwierigkeit der Übertragung des an Individuen entwickelten subjektiven Elements der Devaluation auf eine institutionelle Ebene.

Die in der Pressemitteilung angesprochene „Stigmatisierung" stellt dagegen ein mit der Diskriminierung verwandtes Phänomen dar und ist hiervon abzugrenzen. Im Vergleich zu Diskriminierungen haben Stigmatisierungen einen stärker konventionalen bzw. habituellen Charakter, indem die jeweilige Bewertung mit einem Stigmasymbol verbunden wird. Unter einem Stigma wird in Anlehnung an *Goffman* eine Beziehung zwischen einem Stigmasymbol und einem Stereotyp verstanden. Die Einordnung eines Merkmals als Stigmasymbol folgt aus einer großen Verbreitung und gesellschaftlichen Sichtbarkeit des Merkmals. Weiterhin muss die gesellschaftliche Verbreitung auch für das Stereotyp gelten.[71] So gesehen, kann die Stigmatisierung als besonders schwere und in der Bevölkerung verbreitete Diskriminierung betrachtet werden. Die beschriebenen Profilingmethoden betreffen demnach zunächst das Risiko der Diskriminierung. Bei bestimmten gesellschaftlichen Merkmalstypen kann hieraus jedoch eine Stigmatisierung werden – z.B. die als „Hartz-IV-Empfänger".

## D. OECD-Leitlinien

### 1. Überblick

Parallel zur Entstehung der Datenschutzkonvention des Europarats befasste sich die OECD mit dem Datenschutz. Nach einer Reihe von Vorstudien ab 1969[72] be-

---

[70] Siehe oben II.A.2.d).

[71] Zum Ganzen *Wagner* u.a., Diskriminierungen, S. 5 f.

[72] Die Vorstudien erschienen in der Reihe „OECD informatics studies", vgl. OECD, Digital Economy Paper No. 176, 2011, http://dx.doi.org/10.1787/5kgf09z90c31-en [Stand: 28.3.2014], S. 9 sowie *Hondius*, Emerging, S. 58.

auftragte sie im Anschluss an ein Seminar (1974) und ein Symposium (1977) eine Expertengruppe mit der Prüfung, wie sich Anforderungen an den Umgang mit personenbezogenen Daten auf den grenzüberschreitenden Datenaustausch auswirken.[73] Die Befassung führte 1980 zum Erlass der rechtlich unverbindlichen „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten".[74] Diese Leitlinien wurden zwischen 2011 und 2013 anlässlich ihres dreißigjährigen Jubiläums und wegen geänderter Technologien, Märkte und Nutzerverhalten sowie der wachsenden Bedeutung digitaler Identitäten unter Federführung der Arbeitsgruppe Informationssicherheit und Datenschutz der OECD überarbeitet.[75] Sie enthalten acht Verarbeitungsgrundsätze (Nr. 7–14), die sich im Wesentlichen mit denen der Konvention 108 decken. Für deren Umsetzung wird neben nationaler Gesetzgebung ausdrücklich die Anregung und Unterstützung von Selbstregulierungsmaßnahmen vorgeschlagen (Nr. 19 Buchstabe d). Am 11.4.1985 wurden die Leitlinien in einer Deklaration durch das Ministerkomitee der OECD bekräftigt.[76] Abgesehen von den Aktualisierungen des Jahres 2013, befasste sich die OECD in der Folgezeit immer wieder mit einzelnen Aspekten des Datenschutzes:[77] So folgten 1992 Leitlinien zur Informationssicherheit,[78] 1997 Leitlinien zur Kryptografie,[79] 1998 eine Deklaration zum Datenschutz in Globalen Netzwerken,[80] 2000 der „Privacy-Statement-Generator"[81] sowie seit 2006 verschiedene Maßnahmen zur Unterstützung der Zusammenarbeit bei der Durchsetzung von Datenschutzgesetzen.[82]

---

[73] Zu den Ergebnissen des Seminars und Symposiums OECD, Digital Economy Paper No. 176, 2011, http://dx.doi.org/10.1787/5kgf09z90c31-en [Stand: 28.3.2014], S. 9 f.; vgl. auch Simitis-*Simitis*, BDSG, Einl. Rn. 184.

[74] Annex zur Empfehlung des Rats vom 23.9.1980; abgedruckt in OECD, Guidelines.

[75] C(80)58/FINAL, geändert am 11.7.2013, C(2013)79, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf; Überblick über die Änderungen: http://www.oecd.org/sti/ieconomy/privacy.htm [Stand: 28.3.2014], vgl. auch *Gürtler*, RDV 2012, 126 (127).

[76] OECD, Declaration on Transborder Data Flows, http://www.oecd.org/internet/ieconomy/declarationontransborderdataflows.htm [Stand: 28.3.2014].

[77] Vgl. auch *Bygrave*, in: Rule/Greenleaf (Hrsg.), Global Privacy Protection, S. 28.

[78] Guidelines for the Security of Information Systems (C(92)188/FINAL). Ersetzt durch die OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security vom 25.7.2002; zum diesbezüglichen Reformprozess siehe OECD Digital Economy Paper No. 210, DSTI/ICCP/REG(2012)6/FINAL.

[79] Guidelines for Cryptography Policy (C(97)62/FINAL).

[80] Ministerial Declaration on the Protection of Privacy on Global Networks, DSTI/ICCP/REG(98)10/FINAL vom 18.12.1998.

[81] Dabei handelt es sich um eine mittlerweile eingestellte Webseite mit Anleitungen und Hilfestellungen für die Durchführung eines internen „Datenschutz-Audits", vgl. http://www.oecd.org/sti/ieconomy/oecdprivacystatementgenerator.htm [Stand: 28.3.2014].

[82] http://www.oecd.org/document/25/0,3746,en_2649_34255_37571993_1_1_1_1,00.html [Stand: 28.3.2014]. Dazu OECD, Digital Economy Paper No. 178, 2011, http://dx.doi.org/10.1787/5kgdpm9wg9xs-en [Stand: 28.3.2014].

### 2. Risikokonzeptionen und Schutzgüter

Nach Art. 1 Buchstabe a) der OECD-Konvention[83] widmet sich die Organisation insbesondere der Förderung des Wirtschaftswachstums. Diese Aufgabe liegt auch den Datenschutzleitlinien zugrunde. Sie stellen deshalb die Vermeidung möglicher Handelsbarrieren durch Datenschutzvorschriften ausdrücklich neben die persönlichkeitsrechtlichen Aspekte und verfolgen damit eine dualistische Zielsetzung.[84] Besonders deutlich wird dies in der Bezugnahme auf die ökonomischen und sozialen Vorteile der extensiven Nutzung personenbezogener Daten in der Präambel der 2013 überarbeiteten Fassung der Leitlinien. Auch verweist die Empfehlung vom 23.9.1980, deren Annex die ursprünglichen Leitlinien sind, zwar zunächst auf das gemeinsame Interesse am Schutz von Privatheit[85] und Grundfreiheiten („privacy and individual liberties"), zugleich jedoch auf den Ausgleich der konkurrierenden Werte „Privatheit" und „freier Informationsfluss" („privacy and the free flow of information"). Sodann wird unmittelbar der wirtschaftliche und soziale Nutzen freier Informationsflüsse betont und vor den möglichen Hindernissen durch nationale Datenschutzgesetzgebungen gewarnt. Den Mitgliedstaaten wird aus diesem Grund empfohlen, die im Annex aufgeführten Prinzipien in ihrer nationalen Gesetzgebung zu berücksichtigen. Die Schutzgüter werden dort also nicht über die abstrakten Begriffe „Privatheit" und „Grundfreiheiten" hinaus konkretisiert. Gleiches gilt für die Situation nach der Änderung der Konvention im Jahr 2013. Auch hier greift bereits der erste Absatz der Präambel die dualistische Zielsetzung auf.

Die Leitlinien verdeutlichen in der Präambel der neuen Fassung jedoch nunmehr explizit die Bedeutung des Risikobezugs im Datenschutzrecht: „RECOGNISING the importance of risk assessment in the development of policies and safeguards to protect privacy". Darüber hinaus lassen sie im Abschnitt über den Anwendungsbereich Rückschlüsse auf das Schutzgut zu. Demnach gelten die Leitlinien lediglich für personenbezogene Daten, die aufgrund ihrer Verarbeitungsweise, ihrer Eigenart oder dem Kontext, in dem sie verwendet werden, ein Risiko für Privatheit und Grundfreiheiten darstellen (Teil 1 Nr. 2). Während die ursprünglichen Leitlinien es ermöglichen sollten, personenbezogene Daten, die offensichtlich kein Risiko für Privatheit und Grundfreiheiten darstellen, vom Anwendungsbereich auszunehmen (Teil 1 Nr. 3 Buchstabe b a.F.), entfiel dieser Passus mit der Überarbeitung. Wäh-

---

[83] Convention on the Organisation for Economic Co-operation and Development vom 14.12.1960, http://www.oecd.org/document/7/0,3746,en_2649_201185_1915847_1_1_1_1,00.html [Stand: 28.3.2014].

[84] „twin concerns about threats to privacy from more intensive use of personal data and the risk to the global economy of restrictions on the flow of information", OECD, Digital Economy Paper No. 176, 2011, http://dx.doi.org/10.1787/5kgf09z90c31-en [Stand: 28.3.2014], S. 2; vgl. auch Simitis-*Simitis,* BDSG, Einl. Rn. 184 f.

[85] Die offizielle Übersetzung (abgedruckt bei *Dix*, Datenschutz, Nr. 60) spricht insoweit von „Persönlichkeitsbereich". Zur hier verwendeten Übersetzung des Begriffs „privacy" siehe oben Anm. 33.

rend sich also an der alten Fassung deutlicher festmachen lässt, dass die Leitlinien nicht von dem im deutschen Verfassungsrecht[86] kontrovers diskutierten kontextunabhängigen Schutz und der Ablehnung „belangloser Daten" ausgingen, sondern die Existenz „trivialer Daten" anerkannten[87], ist dies nach der Änderung nicht mehr so klar. Gleichwohl bleibt es aber bei dem in Teil 1 Nr. 2 genannten Risikobezug, der die Existenz nicht risikobehafteter Verarbeitungen voraussetzt. Stark akzentuiert sind zudem auch nach der Überarbeitung die Empfehlungen zur Sicherung des freien Informationsflusses in Teil 4 der Leitlinien. Auch hier wird nun explizit eine Anbindung an Risiken eingefordert. Nach Nr. 18 sollen alle Beschränkungen im Verhältnis zu den jeweiligen Risiken der Verarbeitung stehen. Die ursprüngliche Fassung setzte dagegen einen anderen Akzent, da sie in Nr. 18 a.F. empfahl, keine Beschränkungen „im Namen des Schutzes des Persönlichkeitsbereichs" zu schaffen, die den freien Informationsfluss stärker als erforderlich einschränken (Teil 3 Nr. 18 a.F.). Hier zeigte sich also deutlicher die auch der Datenschutzkonvention des Europarats[88] zugrunde liegende Befürchtung einer „protektionistischen Zweckentfremdung" des Datenschutzes mit dem Freihandel als damit verbundenem Schutzgut.

Die weitere Entwicklung der OECD-Leitlinien weist nun – differenzierter – eine an den Risiken der Datenverarbeitung orientierte Fassung des Schutzkonzepts auf. Beachtenswert ist auch, dass Beschränkungen für bestimmte Kategorien von Daten, die aufgrund ihrer Eigenart durch nationales Recht einiger Mitgliedsstaaten geschützt wurden und für die andere Mitgliedstaaten keinen gleichwertigen Schutz vorsahen, ursprünglich möglich waren (Teil 3 Nr. 17 S. 2 a.F.). In der neuen Fassung wird dem Harmonisierungsziel jedoch durch eine auf das Schutzniveau des anderen Staates pauschal abstellende Fassung Rechnung getragen. Nach Teil 4 Nr. 17 der überarbeiteten Richtlinie sollen die Mitgliedsstaaten nunmehr von Beschränkungen des zwischenstaatlichen Datenverkehrs dann absehen, wenn das jeweils andere Land die Leitlinien im Wesentlichen beachtet oder wenn die verarbeitende Stelle hinreichende Sicherungsmaßnahmen zur Aufrechterhaltung eines mit den Leitlinien konformen Schutzstandards getroffen hat. In Teil 4 Nr. 18 der überarbeiteten Fassung wird dann postuliert, dass jede Beschränkung des zwischenstaatlichen Datenverkehrs im Verhältnis zu den jeweiligen Risiken stehen soll und hierbei Sensibilität der Daten, sowie Zweck und Kontext der Verarbeitung zu beachten sind. Während die ursprünglichen OECD-Leitlinien damit insgesamt den Vorrang der wirtschaftlichen Motive stärker herausstellten,[89] liegt nun eine differenziertere Fassung durch ein – allerdings nicht näher ausgeführtes, also implizit vorausgesetztes – Verständnis von Datenschutzrisiken vor.

---

[86] Siehe unten Teil 3, I.

[87] Zur Diskussion um die „belanglosen Daten" statt vieler *Bull*, NJW 2006, 1618.

[88] Siehe oben II.A.2.a).

[89] Vgl. auch *Trute*, JZ 1998, 830.

Die Anerkennung trivialer Daten wies dagegen in der ursprünglichen Fassung auf ein weniger am Kontext und Verarbeitungszusammenhang ausgerichtetes Risikokonzept hin.[90] Die in dem OECD-Seminar von 1974 noch geäußerten starken rechtspolitischen Forderungen hinsichtlich der „gesellschaftlichen Kontrolle" moderner Informationstechnologie sowie einer „sozialen Software" in Form von Gesetzen, Regelungen und Ethikcodes zur Sicherung einer im Ergebnis positiven Auswirkung der Technikentwicklung[91] mündeten somit in einen Kompromiss, der insbesondere in der Einigung auf die auch in der aktuellen Fassung unverändert gebliebenen acht Verarbeitungsgrundsätze besteht. Die Schwierigkeit in der Umsetzung des ursprünglichen rechtspolitischen Programms verdeutlicht eine Aussage von *Michael Kirby*, dem Vorsitzenden der Expertengruppe, die den ursprünglichen Entwurf ausarbeitete. Ihm zufolge grenze es an ein Wunder, dass eine Einigung auf die Leitlinien überhaupt zustande gekommen sei. Diese Aussage begründet er mit dem Konflikt zwischen Informationsfreiheit und Datenschutz:

> "there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth."[92]

Die allgemeinen Datenschutzgrundsätze finden sich in Teil 2 Nr. 7–14. Sie entsprechen im Wesentlichen denen der Datenschutzkonvention des Europarats und erlauben insoweit auch die dazu erfolgten Rückschlüsse auf Risiken.[93] Expliziter als die Datenschutzkonvention folgen die Leitlinien einer Selbstbestimmungskonzeption durch Verweis auf das Einwilligungserfordernis (Nr. 7, Nr. 10 a) und die Mitteilungs- und Beteiligungsrechte (Nr. 13).

### 3. Zwischenergebnis

Die OECD-Leitlinien lassen kaum Rückschlüsse auf einschlägige Schutzgüter zu. Explizit genannt werden lediglich „Privatheit" und „Grundfreiheiten", ohne diese näher zu beschreiben. Stattdessen verfolgten die Leitlinien ursprünglich entsprechend der Zielsetzung der OECD einen stärker wirtschaftsorientierten Ansatz, wie dies (allerdings eher implizit) auch bei der Konvention 108 der Fall ist. Das – insoweit jedoch nicht datenschutzspezifische – Schutzgut ist der Freihandel. Nach einer Revision der Leitlinien im Jahr 2013 liegt eine differenziertere Fassung mit einem stärker an den Risiken der Datenverarbeitung orientierten Schutzkonzept

---

[90] Dieser Aspekt wird von *Simitis* scharf kritisiert, Simitis-*Simitis,* BDSG, Einl. Rn. 186 und § 1 Rn. 65 ff.

[91] Zu diesen Forderungen vgl. den Synthesis Report des OECD Sekretariats von 1976, zit. nach OECD, Digital Economy Paper No. 176, 2011, S. 9, http://dx.doi.org/10.1787/5kgf09z90c31-en [Stand: 28.3.2014].

[92] Ebd., S. 10.

[93] Siehe oben II.A.2.d).

vor. Die Risiken werden dabei jedoch – wie dies häufig der Fall ist – nicht expliziert, sondern stillschweigend vorausgesetzt. Im Übrigen gilt für die Leitlinien aufgrund der weitgehenden Übereinstimmung der Grundprinzipien mit denen der Konvention 108 das dort zu Risikokonzeptionen und Schutzgütern Ausgeführte.[94] Etwas stärker betont wird jedoch die Selbstbestimmungskonzeption.

## E. UN-Richtlinien

Die Vereinten Nationen befassten sich bereits seit den späten 1960er-Jahren mit der Ausarbeitung von Datenschutzgrundsätzen. Ihre Motive ähneln denen des Europarats. Sie stützen sich auf die Befürchtung, dass die technische Entwicklung die Menschenrechte beeinträchtigen könnte. Die Generalversammlung forderte deshalb am 19.12.1968 den Generalsekretär dazu auf, einen Bericht über relevante Auswirkungen anzufertigen und diesen auch an die UN-Menschenrechtskommission weiterzuleiten.[95] Dieser Bericht wurde 1974 vorgelegt.[96] Nach mehreren Resolutionsentwürfen der Menschenrechtskommission legte der u.a. für die wissenschaftlich-technische Entwicklung zuständige Unterausschuss 1985 einen Entwurf für Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien vor.[97] Daraus resultierten schließlich die am 4.12.1990 von der Generalversammlung gem. Art. 10 UN-Charta verabschiedeten Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien.[98] Die Richtlinien enthalten allgemeine Verarbeitungsgrundsätze, die an die Konvention 108[99] und die OECD-Leitlinien angelehnt sind. Enthalten sind u.a. die folgenden Grundsätze: Rechtmäßigkeit und Ehrlichkeit der Verarbeitung (Nr. 1), Datenrichtigkeit (Nr. 2), normative Zweckbegrenzung (Nr. 3), Einsichtsmöglichkeiten des Betroffenen (Nr. 4), Nichtdiskriminierung (Nr. 5) sowie Datensicherheit (Nr. 7). Der Katalog des Diskriminierungsgrundsatzes führt neben bekannten Kategorien auch die Hautfarbe explizit auf. Dies dürfte jedoch angesichts der ebenfalls in Nr. 5 erfassten Merkmale rassischer und ethnischer Herkunft eher deklaratorisch zu verstehen sein. Das bereits oben im Rahmen der Konvention 108 zu Risikokonzeptionen und Schutzgütern Ausgeführte lässt sich entsprechend auf die Richtlinien der UN übertragen. Eine Besonderheit

---

[94] Siehe oben II.A.2.d).

[95] United Nations, Resolution 2450 (XXIII) vom 19.12.1968. http://www.un.org/documents/ga/res/23/ares23.htm [Stand: 28.3.2014].

[96] United Nations, Economic and Social Council, Human Rights and Scientific and Technological Developments, Uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society, Report of the Secretary-General vom 31.1.1974, UN-Doc. E/CN. 4/1142.

[97] Zu diesen Dokumenten Simitis-*Simitis*, BDSG, Einl. Rn. 193 f. m.w.N.

[98] United Nations, Guidelines for the regulation of computerized personal data files, Resolution 44/132 vom 14.12.1990, UN. Doc. E/CN.4/Sub.2/1988/22.

[99] Siehe oben II.A.2.d).

der UN-Richtlinien besteht aber darin, dass sie sich nicht nur an Staaten richten, sondern auch die Datenverarbeitung in internationalen staatlichen Organisationen betreffen. Trotzdem blieben sie bisher im Vergleich zu den Instrumenten des Europarats und der OECD von geringerer praktischer Bedeutung.[100] Da sie keine eigenständigen, über die Gehalte der Instrumente des Europarats und der OECD hinausgehenden Konzepte enthalten, erübrigt sich eine eingehendere Prüfung. Allerdings ist anzumerken, dass ein vielfach geforderter globaler Datenschutzrahmen auf Ebene der UN angesiedelt sein müsste.

In diesem Zusammenhang ist auch die im Dezember 2013 von der Vollversammlung der Vereinten Nationen einstimmig beschlossene Resolution „The right to privacy in the digital age" zu sehen.[101] Die von Deutschland und Brasilien als Reaktion auf die NSA-Affäre angestoßene unverbindliche Resolution bezieht sich ausdrücklich auf den Privatlebensschutz des Art. 17 IPBürg[102] und ruft alle Staaten zum Schutz der Privatheit im Kontext digitaler Kommunikation, zur Beendigung von Rechtsverletzungen in diesem Kontext und zur Überarbeitung bestehender Praktiken und Regelungen der Kommunikationsüberwachung und der Sammlung personenbezogener Daten auf (Nr. 4 a–c). Weiterhin soll die staatliche Aufsicht von Überwachungsmaßnahmen gestärkt werden (Nr. 4 d). Ein Bericht des United Nations High Commissioner for Human Rights zum Schutz des Rechts auf Privatheit wird angefordert. Obwohl die Resolution, die im Vorfeld auf Betreiben der USA entschärft wurde, eher von symbolischer Bedeutung sein dürfte,[103] weist sie dennoch in ihrer Präambel auf eine durch massenhafte Überwachung hervorgerufene Einschränkung in der Ausübung von Freiheitsrechten hin.[104] Damit wird das Risiko von konformistisch motivierten Verhaltensanpassungen aufgegriffen.

## F. APEC Privacy Framework

### 1. Überblick

Ende der 1990er-Jahre griff das Asiatisch-Pazifische Wirtschaftsforum (APEC) das Thema Datenschutz auf. Dies ist angesichts der heterogenen Mitgliederstruktur des APEC (u.a. China, USA und Russland) bemerkenswert, auch wenn die Be-

---

[100] Zum Ganzen Simitis-*Simitis*, BDSG, Einl. Rn. 195 ff. sowie *Bygrave*, in: Rule/Greenleaf (Hrsg.), Global Privacy Protection, S. 29 f.

[101] A/C.3/68/L.45/Rev.1.

[102] Siehe unten III.B.2.

[103] Zur Einordnung und zu den Entschärfungsbestrebungen vgl. http://www.heise.de/newsticker/meldung/NSA-Affaere-UN-Resolution-fuer-mehr-Datenschutz-einstimmig-angenommen-2053841.html sowie http://www.heise.de/newsticker/meldung/NSA-Affaere-UN-Generalversammlung-beschliesst-Resolution-fuer-mehr-Datenschutz-2070221.html [Stand: 28.3.2014].

[104] A/C.3/68/L.45/Rev.1, Präambel, Abs. 11.

schlüsse des auf dem Konsensprinzip und ohne Vertragsgrundlage agierenden Forums lediglich unverbindliche Empfehlungen darstellen.[105] 1998 erklärten die Führer der APEC-Staaten im Rahmen des „APEC Blueprint for Action on Electronic Commerce", dass Regierungen und Unternehmen das Thema Datenschutz gemeinsam angehen sollten. Dabei bezogen sie sich auch auf die Tätigkeit der OECD.[106] Im November 2004 folgten die 2005 finalisierten APEC-Datenschutz-Rahmenbedingungen.[107] Sie enthalten neun Datenschutzprinzipien, die sich an den OECD-Leitlinien orientieren, jedoch schwächer als diese ausgestaltet sind.[108] Nach den Rahmenbedingungen folgte im Jahr 2007 das „Privacy Pathfinder Project", mit dem im Wege einer teilweisen Selbstregulierung durch die betroffenen Unternehmen Vorschriften für den grenzüberschreitenden Datenverkehr („cross border privacy rules") entwickelt werden sollen.[109] Im Juli 2010 wurde daraufhin ein Abkommen über die Zusammenarbeit der regionalen Datenschutzbehörden bei der Durchsetzung von Datenschutzgesetzen („Cross-Border Privacy Enforcement Arrangement") geschlossen.[110] Daneben wurden 2011 „Cross-Border Privacy Rules" (CBPR) geschaffen. Unternehmen innerhalb der APEC-Region erhalten damit die Möglichkeit, auf Grundlage der CBPR Daten auszutauschen. Das CBPR-System erkennt dabei Datenschutzregeln von privaten Unternehmen an, sofern gewisse Mindeststandards und Compliance-Strukturen eingehalten werden. Neben diesen Kernstücken schafft das Framework einen institutionellen Rahmen, der die Kontrolle der Regelungen sicherstellen soll, sich derzeit aber noch im Aufbau befindet.[111]

### 2. Risikokonzeptionen und Schutzgüter

Die Zielsetzung des APEC Privacy Framework weicht von den bisher untersuchten Regelungen ab und weist Parallelen zu Erwägungsgründen der EU-Datenschutzrichtlinie auf.[112] Die Präambel verweist auf den APEC Blueprint for Action

---

[105] Zum Status der APEC-Beschlüsse *Greenleaf*, CLSR 2009, 29.

[106] APEC Blueprint for Action on Electronic Commerce, Nr. 5, Nr. 6. http://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998_aelm/apec_blueprint_for.aspx [Stand: 28.3.2014].

[107] APEC (Hrsg.), APEC Privacy Framework, 2005. http://publications.apec.org/publication-detail.php?pub_id=390 [Stand: 28.3.2014].

[108] *Greenleaf*, CLSR 2009, 28; *Bygrave*, in: Rule/Greenleaf (Hrsg.), Global Privacy Protection, S. 44.

[109] APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised, 2009/SOM1/ECSG/SEM/027, S. 2. http://aimp.apec.org/Documents/2009/ECSG/SEM1/09_ecsg_sem1_027.doc [Stand: 28.3.2014].

[110] APEC (Hrsg.), Fact Sheet, 2010, http://www.apec.org/About-Us/About-APEC/Fact-Sheets/~/media/Files/AboutUs/Factsheet/FS_CPEA_020710.ashx [Stand: 28.3.2014].

[111] Hierzu im Einzelnen *Gürtler*, RDV 2012, 126 (128).

[112] Siehe unten Teil 2, III.A.

on Electronic Commerce[113] und führt aus, dass das Potenzial des elektronischen Handels nicht ohne die Schaffung von Vertrauen in die neuen Kommunikationstechnologien verwirklicht werden könne. Fehlendes Vertrauen der Verbraucher in den Schutz des Persönlichkeitsrechts könne die Mitgliedstaaten daran hindern, alle Vorteile des elektronischen Handels zu nutzen. Eine Schlüsselstellung in den Bemühungen der Mitgliedstaaten zur Herstellung dieses Vertrauens habe die Kooperation zum Ausgleich und zur Förderung des Persönlichkeitsrechtsschutzes als auch der Informationsfreiheit.[114] Nr. 2 der Präambel konzentriert sich zunächst auf die Darstellung der Vorteile moderner Technologien, greift jedoch dann den Begründungsstrang über das Verbrauchervertrauen wieder auf: Neue Formen der Datenverarbeitung seien für die Individuen nicht erschließbar („undetectable"). Deshalb sei es für sie schwieriger, ein gewisses Maß an Kontrolle („measure of control") über ihre personenbezogenen Informationen aufrechtzuerhalten. Das Ergebnis sei eine Besorgnis über die Folgen, die ein Missbrauch ihrer Informationen hervorrufen könne. Aus diesem Grund bestehe das Bedürfnis, einen ethischen und vertrauenswürdigen Informationsumgang sowohl in online- als auch in offline-Kontexten herzustellen.

Das damit angesprochene Schutzgut des Vertrauens wird hier zwar in seiner rein wirtschaftlichen Dimension dargestellt, besitzt jedoch – anders als der Bezug zum Freihandel – eine Offenheit gegenüber grundrechtlichen Schutzgutkonkretisierungen, wie auch die Rechtsprechung des EGMR zu Art. 8 EMRK und die in den USA und Deutschland entwickelten vertrauensbasierten Schutzgutkonzepte zeigen werden.[115] Im Übrigen verdeutlichen die Ausführungen in der Präambel die Nähe des Vertrauenskonzepts zu Kontrollkonzeptionen und damit zum Schutzgut der Selbstbestimmung.

Nr. 3 der Präambel beschreibt sodann die Abhängigkeit der globalen Wirtschaft von ständig verfügbaren Informationen. Regelungen, die unnötigerweise diesen freien Informationsfluss einschränken oder Hürden aufstellen, hätten negative Auswirkungen auf die globale Wirtschaft. Deshalb bestehe ein Bedarf an Datenschutzsystemen („systems for protecting information privacy"), die diese neuen Realitäten berücksichtigten.

Nr. 5 der Präambel bestimmt schließlich, dass das Framework konsistent mit den Werten der OECD-Leitlinien sei. Nr. 8 der Präambel enthält eine Liste von Zielen, die unter Anerkennung ihrer Bedeutung („in recognition of the importance of") aufgezählt werden. Dort werden insbesondere der Schutz vor schädlichen Konsequenzen ungewollter Privatheitsverletzungen und vor Missbräuchen personenbezogener Informationen genannt („harmful consequences of unwanted intrusions and

---

[113] Siehe oben II.F.1.

[114] APEC (Hrsg.), APEC Privacy Framework, 2005. http://publications.apec.org/publication-detail.php?pub_id=390 [Stand: 28.3.2014], Präambel Nr. 1.

[115] Siehe unten IV.B.5. sowie Teil 3, II.B.7.

the misuse of personal information“). Diese Anknüpfung an Schädigungen greift das Framework in seinem ersten Prinzip, „Preventing Harm“ (part iii.I.14), auf, das allerdings weder in der Konvention 108 noch in den OECD-Leitlinien ausdrücklich als eigenes Prinzip aufgeführt wird. Es bestimmt, dass der Schutz personenbezogener Informationen angesichts legitimer Privatheitserwartungen der Einzelnen so gestaltet sein soll, dass Missbrauch verhindert wird. Spezielle Verpflichtungen sollen sich an den mit Missbräuchen einhergehenden Risiken orientieren („specific obligations should take account of such risk“); Abhilfemaßnahmen sollen verhältnismäßig in Bezug auf die Wahrscheinlichkeit und Schwere eines Schadens durch Sammlung, Verwendung und Weiterleitung personenbezogener Informationen sein. Der Kommentar zu diesem Prinzip führt aus, dass die Verhinderung von Missbräuchen und daraus resultierenden Schäden eines der primären Ziele des Framework ist. Alle Umsetzungsmaßnahmen seien daran auszurichten.[116] In besonderer Weise verdeutlicht das Framework an dieser Stelle somit das Risiko der individuellen Verletzlichkeit.

### 3. Zwischenergebnis

Die Zielbestimmungen in der Präambel des APEC Framework sind konsequent auf wirtschaftliche Auswirkungen ausgerichtet. Menschenrechtliche Erwägungen finden dort keine eigenständige Erwähnung. Der Schutz personenbezogener Informationen dient dem Abbau von Ängsten unter den Verbrauchern, die negative Auswirkungen auf den elektronischen Handel haben könnten. Es sind somit nicht die Folgen für das Individuum, die den Schutz personenbezogener Informationen begründen, sondern die durch das Individuum als Konsument vermittelten wirtschaftlichen Auswirkungen. Auch das erste Prinzip, welches die legitimen Privatheitserwartungen des Individuums und das Bestehen von Risiken durch Missbrauch personenbezogener Informationen ausdrücklich anerkennt, spricht nicht gegen diese Feststellung. Zwar sieht der Kommentar zur Vorschrift in der Verhinderung von Missbräuchen und Schäden des Individuums ein zentrales Ziel des Framework;[117] dies widerspricht jedoch nicht der zuvor in der Präambel vorgenommenen Zielbestimmung, die den Schutz des Individuums gerade mit den wirtschaftlichen Auswirkungen begründet und insoweit ein übergeordnetes Ziel etabliert. Insbesondere Nr. 3 der Präambel ermöglicht eine weitere Differenzierung der wirtschaftlichen Risiken: Der dort hergestellte Bezug zur Abhängigkeit der globalen Wirtschaft von frei verfügbaren Informationen erinnert an das auch in den Materialien zur Datenschutzkonvention identifizierte Risiko von Handelshemmnissen durch Datenschutzrecht.[118]

---

[116] APEC (Hrsg.), APEC Privacy Framework, S. 11 Rn. 14.

[117] Ebd., S. 11 Rn. 14.

[118] Siehe oben II.A.2.a); 3.

## G. Weitere internationale Instrumente

Zahlreiche internationale Organisationen und Vereinigungen haben soft law im Bereich des Datenschutzes erlassen. Die Instrumente blieben jedoch von geringem Einfluss und sollen im Folgenden ohne Anspruch auf Vollständigkeit genannt werden. Über die bereits aus den Datenschutzinstrumenten des Europarats und der OECD gewonnenen Ergebnisse gehen sie nicht hinaus.

Zu nennen ist zunächst das Allgemeine Abkommen über den Handel mit Dienstleistungen (GATS)[119] der Welthandelsorganisation, die 1994 aus dem GATT hervorging. Das Abkommen enthält mit Artikel XIV a) ii) GATS eine Vorschrift zum Datenschutz. Sie bestimmt, dass das Abkommen von den Mitgliedstaaten nicht derart auszulegen ist, dass der Schutz des Persönlichkeitsbereichs in Bezug auf Verarbeitung und Verbreitung personenbezogener Daten und den Schutz der Vertraulichkeit individueller Aufzeichnungen und Konten verhindert wird.

Die Internationale Arbeitsorganisation (ILO) befasste sich ebenfalls mit dem Datenschutz – entsprechend ihren Kompetenzen jedoch beschränkt auf den Arbeitnehmerdatenschutz. Im November 1996 verabschiedete der Verwaltungsrat der ILO einen Datenschutz-Verhaltenskodex.[120] Dieser lehnt sich an die Datenschutzkonvention des Europarats an und bezieht im Rahmen von Bewerbungen eingeschaltete externe Stellen mit ein (13.1). Daneben enthält der Verhaltenskodex Regelungen zu arbeitnehmerdatenschutzrechtlichen Themen wie u.a. technische Überwachung der Arbeitnehmer (6.14), Gen- und Persönlichkeitstests (6.12, 6.11) sowie Vorschriften zum Schutz vor Erhebung sensibler Daten (6.5) – diese auch unabhängig von einer Einwilligung der Arbeiter.[121]

Weitere internationale Organisationen, die sich mit dem Datenschutz befassen, die jedoch ebenfalls keine mit den zuvor beschriebenen Instrumenten von Europarat und OECD vergleichbaren Normen hervorgebracht haben, sind u.a. der Verband Südostasiatischer Nationen (ASEAN) sowie verschiedene regionale Zusammenschlüsse von Datenschutzbehörden, wie beispielsweise das Ibero-amerikanische Datenschutznetzwerk und die Vereinigung der französischsprachigen Datenschutzbehörden (AFAPDP).[122]

---

[119] General Agreement on Trade in Services; Annex 1B zu "The Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations" vom 15.4.1994, abrufbar unter http://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm [Stand: 28.3.2014].

[120] ILO, Protection of workers' personal data. An ILO Code of practice, 1997.

[121] Insbesondere zu letzterem Aspekt Simitis-*Simitis*, BDSG, Einl. Rn. 202.

[122] Zu diesen Organisationen *Greenleaf*, CLSR 2009, S. 40 m.w.N.

## H. Zwischenergebnis

Die untersuchten datenschutzrechtlichen Spezialinstrumente lassen zwei Begründungslinien erkennen: eine persönlichkeitsrechtliche und eine wirtschaftspolitische. Die Datenschutzkonvention des Europarats knüpft an Art. 8 Abs. 1 EMRK an. Der Inhalt dieses Rechts war jedoch zur Zeit der Entstehung unklar. Die Untersuchung hat ergeben, dass bei näherer Betrachtung der Konventionsziele dem grundrechtlichen Schutzgut eine eher deklaratorische Bedeutung zukommt, da es sich allenfalls vage auf den Schutz eines Intimbereichs zurückführen lässt. In dieser Frühphase des Datenschutzrechts ist dagegen der Freihandel besser zu fassen. Er soll vor einer „protektionistischen Zweckentfremdung" durch nationales Datenschutzrecht geschützt werden.[123] Dabei handelt es sich jedoch um kein spezifisch datenschutzrechtliches Schutzgut, weswegen der Datenschutzkonvention – bis zu einem gewissen Grad – die paradoxe Funktion zukommt, Datenschutzrecht zu verhindern. An den Modernisierungsvorschlägen des Jahres 2012 zur Datenschutzkonvention lässt sich sodann der Übergang von der persönlichkeitsrechtlichen Komponente zu den neu entstandenen Datenschutzgrundrechten auf europäischer Ebene erkennen, womit die Aufwertung des Datenschutzes auf Ebene des Unionsrechts[124] nachvollzogen wird. Zudem wird das Schutzgut der Menschenwürde und das ihm zugeordnete Risiko von Objektmachungen in rein automatisierten Verarbeitungsprozessen im Rahmen der Modernisierungspläne herausgestellt. Abgesehen von dieser neueren Entwicklung tritt vor allem die wirtschaftspolitische Ausrichtung hervor. Diese ist im Vergleich zur Datenschutzkonvention deutlicher in der Entwicklung der OECD-Leitlinien erkennbar. Die Weiterentwicklung und Ergänzung der wirtschaftlichen Ausrichtung lässt sich am asiatisch-pazifischen APEC Privacy Framework nachvollziehen. Dort ist das Verbrauchervertrauen zentrales Schutzgut. Eine in der Untersuchung weiterzuverfolgende Vermutung spricht dafür, dass die Vertrauenskonzeption im Gegensatz zum Freihandel hinsichtlich der Datenschutzgrundrechte offener und „anschlussfähiger" ist.

Ein eigenständiger, jedoch nur in Ansätzen erkennbarer Begründungsstrang innerhalb der Datenschutzkonvention bezieht sich auf die Vorstellung von Informationsmacht und damit einhergehender sozialer Verantwortung. Damit lässt sich das Risiko informationeller Machtverschiebungen verbinden.

Rückschlüsse auf einschlägige Risiken ergeben sich sodann vor allem aus den – mit Ausnahme des APEC Privacy Framework – in allen untersuchten Instrumenten enthaltenen allgemeinen datenschutzrechtlichen Regelungskonzeptionen und Grundsätzen. Diese finden unter den geprüften Instrumenten ihre verbindlichste

---

[123] Dies deckt sich in gewisser Weise mit dem Befund von *Trute*, demzufolge das Einfügen institutioneller Anforderungen in einen vereinheitlichten Ordnungsrahmen weniger vom Schutz des Allgemeinen Persönlichkeitsrechts her gedacht ist, als von der weltweiten wirtschaftlichen Harmonisierung, vgl. *Trute*, JZ 1998, 822 (823).

[124] Siehe unten Teil 2, II.

und umfassendste Ausprägung in der Konvention 108. Darin treten die Schutzgüter „Selbstbestimmung“ und „Menschenwürde“ hervor. Einschlägiges Risiko ist neben der Fremdbestimmung insbesondere der Überwachungsdruck durch ungeregelte Informationsverarbeitung.

Daneben wird auf das Risiko der Entkontextualisierung von Informationen eingegangen. Hierunter wird die Schadensmöglichkeit aus bereichsübergreifender Informationsverfügbarkeit, beispielsweise Freizeit/Arbeitsleben, verstanden. Diesem Risiko konnten in Zusammenschau mit den Europaratsempfehlungen zur polizeilichen Tätigkeit zwei Teilaspekte entnommen werden, die als Kontextinfiltration und Kontextdefizit bezeichnet wurden.[125]

Ein weiteres mit den allgemeinen Regelungskonzeptionen aufgegriffenes Risiko ist die Erhöhung individueller Verletzlichkeit durch unbefugte Informationsnutzung.[126]

Eine nähere Aufschlüsselung erfolgte bezüglich des Risikos der Diskriminierung, das als kategoriale Behandlung und Devaluation von Personen bestimmt wurde. Aus enthaltenen Katalogen sensibler Daten können gemeinsame Merkmale gewonnen werden. Diese sind durch eine besondere Polarisierung, Schambesetzung, Leistungsindikation oder Informationsemergenz charakterisiert. Von den allgemeinen Regelungskonzeptionen bloß angedeutet wird das Risiko der Informationspermanenz, also der dauerhaften Verfügbarkeit von Informationen und daraus resultierenden Missbrauchspotenzialen.[127]

Übergreifend zeichnen sich damit in den untersuchten Schutzgütern und Risikokonzeptionen zentrale datenschutzrechtliche Konfliktfelder ab. Wie relevant die wirtschaftspolitische Zielsetzung ist, zeigen etwa der Streit zwischen Europäischer Kommission und den USA um europäische Datenschutzbestimmungen im Hinblick auf die Vereinbarkeit mit den Regelungen des GATS und die mit den Drittstaatenregelungen des Safe-Harbour-Abkommens verbundenen Probleme.[128] Auch die subjektivierte wirtschaftspolitische Begründungslinie über den Vertrauensschutz ist zunehmend bedeutsam; dies verdeutlicht etwa das mit dem Auftreten des sozialen Netzwerks Google+ zusammenfallende Bemühen von Google und Facebook um stärkere Datenschutzkonformität trotz wirtschaftlich gegenteiliger Anreize und ohne dazu beispielsweise in den USA rechtlich verpflichtet zu sein.[129] Die grundrechtliche Begründungslinie wird in den bisher untersuchten Regelungen dagegen.

---

[125] Siehe oben II.B.

[126] Siehe oben II.A.2.d); F.2.

[127] Siehe unten II.A.2.d).

[128] *Bygrave*, in: Rule/Greenleaf (Hrsg.), Global Privacy Protection, S. 40 f. m.w.N.

[129] Zwar sind die Datenschutzregelungen der beiden „Internetgiganten“ in vielfacher Hinsicht ungenügend; angesichts ihrer Marktmacht ist es gleichwohl bemerkenswert, dass überhaupt Datenschutzmaßnahmen getroffen werden, so fadenscheinig diese auch sein mögen, vgl. http://www.sueddeutsche.de/digital/datenschutz-bei-google-und-facebook-siemachen-was-sie-wollen-1.1272375-2 [Stand: 28.3.2014].

nur wenig konturiert. Die Bedeutung dieser Ebene wächst jedoch in jüngerer Zeit, wie die Revision der OECD-Leitlinien des Jahres 2012 und die Resolution der UN zum Privatheitsschutz im digitalen Zeitalter zeigen. Letztere lässt das Risiko der Beeinträchtigung von Freiheitsrechten aufscheinen.[130] Dieser Entwicklung folgend, sind nun die datenschutzrechtlichen Gehalte der Menschenrechtsverträge zu untersuchen

## III. Menschenrechtskataloge

### A. Überblick

Vor der Kodifikation der Grundrechtecharta der Europäischen Union befand sich in keinem der internationalen und regionalen Menschenrechtskataloge ein ausdrückliches Grundrecht auf Datenschutz. Datenschutzrechtliche Sachverhalte können jedoch vom Recht auf Achtung des Privatlebens erfasst sein. Dieses Recht war bereits seit 1948 in Art. 12 AEMR enthalten. Zudem ist es in Art. 17 IPBürg von 1976 sowie in Art. 8 EMRK von 1953, dem für die Untersuchung gewählten regionalen Menschenrechtskatalog, enthalten. Geht man noch weiter zurück, so zeigt sich, dass der grundrechtliche Schutz der Privatheit gegenüber dem Staat zu Beginn der rechtlich-politischen Verankerung von Menschenrechten in Verfassungsurkunden noch kein zentrales Thema war. Er gewann seine Bedeutung erst im Übergang vom liberalen zum sozialen Rechtsstaat. Vor dieser Entwicklung, also im späten 19. Jahrhundert, wurde der Schutz der Privatsphäre dadurch verwirklicht, dass sich der Staat auf seine Kernaufgaben, den Schutz von Leben, Freiheit und Eigentum, beschränkte.[131] Je weiter der Staat jedoch aus sozialen Motiven das Leben der Individuen zu beeinflussen suchte, desto größer wurde das Bedürfnis nach einem Schutz der freien persönlichen Lebensgestaltung als einem der zentralen grundrechtlichen Autonomieansprüche.[132] Die Erhöhung des Steuerungs- und Manipulationspotenzials staatlicher Verwaltung durch den Einsatz moderner IKT sowie deren Überwachungspotenzial, das die heutige präventive Sicherheitspolitik erst ermöglichen, verstärken dieses Schutzbedürfnis und führten zur Anerkennung des Datenschutzes als eigenständiger Schutzdimension im Rahmen des Privatlebensschutzes. Im Folgenden werden die einschlägigen Vorschriften AEMR, IPBürg und EMRK zur Präzisierung der Schutzgüter und zur Ableitung datenschutztypischer Risiken untersucht.

---

130 Siehe oben II.E.

131 *Marauhn/Meljnik*, in: Grote/Marauhn (Hrsg.), EMRK/GG, Kap. 16 Rn. 3.

132 Zur Fundierung menschenrechtlicher Autonomieansprüche vgl. *Hofmann*, JZ 1992, 168 f.

## B. Risikokonzeptionen und Schutzgüter

### 1. Art. 12 AEMR

Art. 12 AEMR hat folgenden Wortlaut:

> Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.[133]

Bei der AEMR handelt es sich um eine rechtlich nicht bindende Resolution der Generalversammlung der Vereinten Nationen.[134] Weil die AEMR keinen internationalen Schutzmechanismus vorsieht, werden bei der Auslegung des AEMR durch die einzelnen Staaten die Rechtsprechung zur EMRK und die Äußerungen des Menschenrechtsausschusses zum IPBürg als Interpretationshilfe herangezogen.[135] Dementsprechend wird aus Art. 12 AEMR der Schutz vor staatlicher Sammlung, Speicherung und Weitergabe personenbezogener Daten abgeleitet.[136] Mangels konkreten Fallmaterials und Problembewusstseins zur Zeit der Entstehung der AEMR erschöpft sich die Prüfung von Risikokonzeptionen und Schutzgütern im Verweis auf die oben genannten Menschenrechtsinstrumente, die Auslegungshilfen der AEMR darstellen und nachfolgend untersucht werden. Art. 12 AEMR wird damit im Datenschutzrecht allenfalls die Schaffung einer absoluten Grenze im Sinne eines Willkürschutzes zugebilligt. Im Übrigen bleibt seine datenschutzrechtliche Bedeutung jedoch gering.[137] Eigenständige Rückschlüsse auf Risikokonzeptionen und Schutzgüter sind nicht möglich.

### 2. Art. 17 IPBürg

Art. 17 IPBürg hat folgenden Wortlaut:

> (1) Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.
>
> (2) Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.[138]

---

[133] Resolution 217 A (III) der Generalversammlung vom 10.12.1948, in der Fassung des Deutschen Übersetzungsdienstes der Vereinten Nationen, http://www.un.org/depts/german/gruendungsres/grunddok/ar217a3.html [Stand: 28.3.2014].

[134] Vgl. Maunz/Dürig-*Durner,* Art. 10 Rn. 28 f.

[135] *Gridl*, Datenschutz, S. 168; so etwa bei *Rehof*, in: Eide u.a. (Hrsg.), Article 12, S. 193 ff.

[136] *Rehof*, in: Eide u.a. (Hrsg.), Article 12, S. 187.

[137] Zum Ganzen *Gridl*, Datenschutz, S. 168 ff.

[138] Amtliche Übersetzung, BGBl. 1973 II 1553; http://www.auswaertiges-amt.de/cae/servlet/contentblob/360794/publicationFile/3613/IntZivilpakt.pdf [Stand: 28.3.2014].

Der Internationale Pakt über bürgerliche und politische Rechte ist ein völkerrechtlicher Vertrag zum Schutz der Menschenrechte, der am 19.12.1966 abgeschlossen wurde und am 23.2.1976 in Kraft trat. Mittlerweile haben ihn 167 Staaten ratifiziert.[139] Der im Rahmen der Vereinten Nationen erarbeitete Vertrag ist für die beigetretenen Staaten bindendes Völkerrecht. Er enthält in Teil III einen Grundrechtskatalog und sieht über ein Zusatzprotokoll die Möglichkeit von Individualbeschwerden vor.[140]

In Art. 17 IPBürg wird der Datenschutz nicht wörtlich aufgeführt, kann jedoch ggf. unter den Begriff des Privatlebens subsumiert werden. Bei der Auslegung des Paktrechts besteht die Besonderheit, dass der Menschenrechtsausschuss (HCR) allgemeine Bemerkungen als rechtlich unverbindliche Interpretationshilfen erlässt und sich in der Bemerkung Nr. 16 schon früh für eine umfängliche Erfassung des Datenschutzes ausgesprochen hat.[141] Demnach erfordert Art. 17 IPBürg die rechtliche Regulierung staatlicher und privater automatischer Informationsverarbeitung und verbürgt zentrale datenschutzrechtliche Grundsätze wie die normative Zweckbegrenzung, die Datenrichtigkeit und das Recht auf Einsicht, Berichtigung und ggf. Löschung personenbezogener Daten. Dabei bezieht die Interpretationshilfe explizit auch Verletzungen durch Private in den Schutzbereich ein:

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."

Weiterhin sieht die Interpretationshilfe die Staaten zur Ergreifung effektiver Maßnahmen verpflichtet, um sicherzustellen, dass Informationen, die das Privatleben betreffen („information concerning a person's private life"), nicht an unberechtigte Dritte gelangen.[142] Erforderlich ist somit ein Bezug der Informationen zum Privatleben. Das Risiko individueller Verletzlichkeit durch unbefugte Nutzung der Daten wird damit an dieser Stelle angedeutet. Unklar bleibt jedoch, welche Kriterien für das Vorliegen eines Privatlebensbezugs maßgeblich sein sollen.[143] Der Wortlaut des IPBürg deutet auf einen weiten Schutzbereich hin, da die Formulierungen „niemand darf […] ausgesetzt werden" und „Jedermann hat Anspruch" darauf hinweisen, dass die Vorschrift nicht als reines Abwehrrecht konzipiert wurde und auch – wie die Interpretationshilfe explizit feststellt – im Verhältnis der Bürger untereinander gilt. Mithin begründet Art. 17 eine staatliche Schutzpflicht. Ein Leis-

---

[139] http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en [Stand: 28.3.2014].

[140] *Gridl*, Datenschutz, S. 154.

[141] HCR, CCPR General Comment No. 16: Article 17 (Right to Privacy) vom 8.4.1988. Hierzu *Gridl*, Datenschutz, S. 157 ff.; vgl. auch *Bygrave*, in: Rule/Greenleaf (Hrsg.), Global Privacy Protection, S. 45 f.

[142] HCR, CCPR General Comment No. 16, Article 17 (Right to Privacy) vom 8.4.1988.

[143] Kritisch deshalb *Gridl*, Datenschutz, S. 159.

tungsrecht soll daraus jedoch nicht abzuleiten sein.[144] Bemerkenswert ist, dass die Verpflichtung laut Bemerkung Nr. 16 „effective measures" umfasst und damit nicht allein auf rechtlichen Schutz beschränkt ist, sondern auch die Datensicherheit beinhaltet.[145] Weiterhin ist Art. 17 IPBürg so auszulegen, dass der Schutz unabhängig vom verwendeten Kommunikationsmedium gewährleistet wird.[146] Die Bemerkung spricht sich ferner für ein Verbot des Abhörens privater Kommunikation aus:

> "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[147]

Hieraus kann jedoch nur auf die Verpflichtung des Staates zum grundsätzlichen Verbot der Überwachung Privater durch andere Private geschlossen werden.[148] Der Verbürgung liegt damit vorrangig das Risiko der individuellen Verletzlichkeit durch unbefugte Datennutzung zugrunde. Der Verweis auf die Abhörmaßnahmen lässt sich im weiteren Sinne auch mit dem Risiko des Überwachungsdrucks und des Bekanntwerdens schambesetzter Informationen in Verbindung bringen; die Ausführungen hierzu müssten aber konkretisiert werden, um eine darauf bezogene Risikokonzeption darzustellen.

Die Bedeutung des IPBürg für den Datenschutz ist trotz der relativ modernen Schutzbereichsfassung gering, da es an wirksamen Kontroll- und Durchsetzungsmechanismen fehlt. Ob hieran die als Reaktion auf die NSA-Affäre im Dezember 2013 von der Vollversammlung der Vereinten Nationen einstimmig beschlossene und auf Art. 17 IPBürg abzielende Resolution „The right to privacy in the digital age"[149] etwas ändert, ist derzeit noch nicht abzusehen.[150] So besteht derzeit zwar die Möglichkeit von Individualbeschwerden an den Menschenrechtsausschuss gem. dem ersten Fakultativprotokoll zum Pakt. Die Ergebnisse dieses Verfahrens erschöpfen sich jedoch in Berichten und Veröffentlichungen.[151] Die Mitteilungen haben zwar durch die Publizitätswirkung, insbesondere im Rahmen des 1990 eingeführten Follow-Up-Verfahrens, ein gewisses Potenzial, Missstände anzuprangern, bleiben jedoch ebenso unverbindlich wie die Möglichkeiten des Ausschusses gem. Art. 40, 41 IPBürg, Berichte einzufordern und zu verfassen.[152] Entsprechend selten befasste sich der Ausschuss mit datenschutzrechtlichen Sachverhalten im

---

144 Ebd., S. 157 f.

145 Ebd, S. 159.

146 Ebd., S. 161 f.

147 HCR, CCPR General Comment No. 16: Article 17 (Right to Privacy) vom 8.4.1988.

148 *Gridl*, Datenschutz, S. 159.

149 A/C.3/68/L.45/Rev.1.

150 Siehe oben II.E.

151 *Schäfer*, Individualbeschwerde, S. 48 ff.

152 *Gridl*, Datenschutz, S. 155 f. Zum Follow-Up-Verfahren *Schäfer*, Individualbeschwerde, S. 49 ff.

Individualbeschwerdeverfahren. Die entsprechenden Stellungnahmen sollen gleichwohl im Folgenden analysiert werden.

Die erste Äußerung zu einer datenschutzrechtlichen Konstellation erfolgte in der Entscheidung *I.P. gegen Finnland*.[153] Darin bestätigt der Ausschuss, dass für steuerliche Abzüge relevante Informationen nicht willkürlich an einen privaten Arbeitgeber weitergegeben werden dürfen und dass hierfür grundsätzlich eine Rechtsgrundlage erforderlich ist. Die Beschwerde war jedoch wegen Nichterschöpfung des innerstaatlichen Rechtswegs unzulässig. Eine genaue Analyse des materiellen Paktrechts unterblieb.[154] In der Entscheidung *Van Hulst gegen die Niederlande* prüft der Ausschuss Maßnahmen der Telekommunikationsüberwachung anhand von Art. 17 IPBürg, ohne näher auf den Schutzbereich einzugehen. Er bejaht schließlich die Rechtmäßigkeit aufgrund einschlägiger Rechtsgrundlagen.[155]

2007 äußerte sich der Ausschuss in der Entscheidung *Sayadi u.a. gegen Belgien* erneut zum Datenschutz.[156] Die Entscheidung hatte einen Eintrag in den öffentlich zugänglichen Listen terrorverdächtiger Personen verschiedener Institutionen und Staaten zum Gegenstand. Der Ausschuss bejahte ohne weitere Erörterung die Verletzung von Art. 17 IPBürg aufgrund des auch nach Einstellung des Strafverfahrens fortdauernden Eintrags in den Listen.[157]

Rückschlüsse auf das Schutzgut und auf betroffene Risiken erlauben die bisherigen Berichte des Menschenrechtsausschusses somit aufgrund fehlender Erörterung des Schutzbereichs nicht. Einen im Vergleich hierzu erheblich größeren Einfluss auf die datenschutzrechtliche Rechtsentwicklung und Ausprägung des Schutzguts kommt der im Folgenden zu untersuchenden EMRK zu.

### 3. Art. 8 EMRK

Art. 8 EMRK verbürgt laut der amtlichen Überschrift das „Recht auf Achtung des Privat- und Familienlebens". Er hat folgenden Wortlaut:

> Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
>
> Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die

---

[153] UN Menschenrechtsausschuss, Communication No. 450/1991 vom 26.7.1993, *I.P. ./. Finnland.*

[154] Ebd.; *Gridl*, Datenschutz, S. 158 f. m.w.N.

[155] UN Menschenrechtsausschuss, Communication No. 903/2000 vom 1.11.2004, *Van Hulst ./. Niederlande* = A/60/40 (Vol. II.), S. 29 ff. Zur Prüfung von Eingriffen und Rechtfertigung im Rahmen des IPBürg vgl. ebd., S. 160.

[156] UN Menschenrechtsausschuss, Communication No. 1472/2006, vom 22.10.2008, *Sayadi et al. ./. Belgium* = A/64/40 (Vol. II).

[157] UN Menschenrechtsausschuss, Communication No. 1472/2006, vom 22.10.2008, *Sayadi et al. ./. Belgium* = A/64/40 (Vol. II), S. 262.

nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.[158]

Im ersten Absatz wird somit der aus vier Gewährleistungen zusammengesetzte Schutzbereich umschrieben. Garantiert werden neben der hier relevanten Gewährleistung auf Achtung des Privatlebens auch das Familienleben, die Wohnung und die Korrespondenz. Art. 8 Abs. 2 EMRK enthält den Schrankenvorbehalt. Der Wortlaut des Art. 8 Abs. 1 EMRK benennt den Datenschutz zwar nicht ausdrücklich, zentrale datenschutzrechtliche Grundsätze können jedoch durch Auslegung des Privatlebensbegriffs[159] und ggf. auch der Korrespondenz erfasst werden.[160] Methodisch ermöglicht dies die sog. „evolutive Auslegung". Dadurch sollen bereits enthaltene, aber veränderliche Konventionsgehalte im Lichte heutiger Bedingungen interpretiert werden.[161] Der EGMR versteht die Konvention dementsprechend als „living instrument", welches zeitgemäß auszulegen ist.[162] Das reichhaltige Fallmaterial erfordert die Untersuchung in einem eigenen Abschnitt.

## C. Zwischenergebnis

Die Menschenrechtskataloge der AEMR, des IPBürg und der EMRK enthalten Grundrechte, die das Privatleben im weiteren Sinne schützen. Art. 12 AEMR bleibt insbesondere mangels Schutzmechanismus unbestimmt und unbedeutend.[163] Bei Art. 17 IPBürg stellt sich die Lage anders dar: In der Bemerkung Nr. 16 des Menschenrechtsausschusses und einer Reihe von Individualbeschwerden wird die Erfassung des Datenschutzes bestätigt. Die Bemerkung Nr. 16 verdeutlicht dabei in erster Linie das Risiko der individuellen Verletzlichkeit durch unbefugte Nutzung der Daten. Bloß angedeutet wird das Risiko des Überwachungsdrucks, indem auf spezifische Abhörmaßnahmen eingegangen wird. Die geringe Anzahl und die inhaltliche Tiefe der Äußerungen im Rahmen der Individualbeschwerden erlauben hingegen keine Rückschlüsse auf Risiken und Schutzgüter.[164]

---

158 In der Fassung des Protokolls Nr. 11, http://conventions.coe.int/Treaty/ger/Treaties/Html/005.htm [Stand: 28.3.2014].

159 *Bygrave*, in: Rule/Greenleaf (Hrsg.), Global Privacy Protection, S. 45 f.

160 Zum Ganzen *Siemen*, Grundrecht, S. 52-63.

161 EGMR Urteil vom 29.5.1986, *Deumeland ./. Deutschland*, App. Nr. 9384/81, [24]; vgl. auch *Wildhaber/Breitenmoser*, in: Karl (Hrsg.), IntKommEMRK Rn. 17 f. m.w.N.

162 EGMR Urteil vom 25.4.1978, *Tyrer ./. Vereinigtes Königreich*, App. Nr. 5856/72, [31].

163 Siehe oben III.B.1.

164 Siehe oben III.B.2.

In Art. 8 EMRK können datenschutzrechtliche Schutzgehalte an den Merkmalen „Privatleben“ und „Korrespondenz“ festgemacht werden.[165] Anders als die zuvor genannten Menschenrechtsinstrumente verfügt die EMRK mit dem EGMR über einen verbindlichen Durchsetzungsmechanismus und Spruchkörper, dessen reichhaltiges Fallmaterial im Folgenden untersucht wird.

# IV. Rechtsprechung des EGMR

## A. Überblick: Prüfungsabfolge des EGMR

Bei der Prüfung einer Verletzung von Art. 8 Abs. 1 Var. 1 EMRK geht der Gerichtshof in verschiedenen Schritten vor.[166]

### 1. Schutzbereich und Eingriff

Zunächst untersucht er, ob ein Eingriff in das Privatleben der betroffenen Person vorliegt, und danach, ob dieser gerechtfertigt ist. Weil sich in der Rechtsprechung des EGMR noch keine differenzierte Eingriffsdogmatik und keine klare Konstruktion des Schutzguts entwickelt hat, wird die im Anschluss vorzunehmende Auswertung der Rechtsprechung des EGMR nach einschlägigen Schutzgütern und Risikokonzeptionen den Untersuchungsfokus auf die Sachverhalts-, Schutzbereichs und Eingriffsebene legen.[167] Die Abgrenzung von Schutzbereich und Eingriff kann im Rahmen des Art. 8 Abs. 1 Var. 1 EMRK noch nicht als dogmatisch gefestigt angesehen werden,[168] weswegen die Untersuchung hier ansetzen muss. Als Grundlage sind hierzu jedoch zunächst die weiteren Prüfungsschritte des EGMR darzustellen.[169]

### 2. Rechtfertigungsebene

Im Rahmen der Rechtfertigung prüft der Gerichtshof, ob der Eingriff gesetzlich vorgesehen ist, ob er einen in Art. 8 Abs. 2 EMRK genannten legitimen Zweck erfüllt und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft notwendig ist. Dabei sind die in Art. 8 Abs. 2 EMRK genannten Voraussetzungen eng

---

[165] Siehe oben III.B.3.

[166] Zum Ganzen GA *Leger*, Schlussanträge vom 22.11.2005 zu EuGH Urteil vom 30.5.2006 verb. Rs. C-317/04 u. C-318/04 (*Fluggastdaten*-Schlussanträge) Rn. 210 ff.

[167] Ergänzend kann auf die umfassende Untersuchung von *Siemen* verwiesen werden, die auch für die nachfolgende Prüfung als Ausgangspunkt herangezogen wurde, vgl. *Siemen*, Grundrecht, insb. S. 63–132.

[168] *Esser*, in: Wolter u.a. (Hrsg.), Alternativentwurf, S. 283 f.

[169] Zum Ganzen ebd., S. 286–307.

auszulegen. Ebenfalls rechtfertigend wirkt die Einwilligung des Betroffenen, die vom EGMR unter strengen Voraussetzungen als Grundrechtsverzicht gewertet wird.[170]

### *a) Grundlage des Eingriffs*

Das Merkmal „gesetzlich vorgesehen" („in accordance with the law") erfordert nach ständiger Rechtsprechung zunächst eine gesetzliche Grundlage im nationalen Recht („some basis in domestic law"), umfasst jedoch auch die Qualität des zu prüfenden Gesetzes: Das Gesetz muss für die Bürger zugänglich („accessible") sowie bestimmt und in seinen Wirkungen voraussehbar („foreseeable") sein. Hierzu müssen die Voraussetzungen und Modalitäten der Beschränkungen so genau festgelegt sein, dass der Bürger sein Verhalten, ggf. nach Einholung sachkundigen Rates, danach ausrichten und geeigneten Schutz vor Willkür in Anspruch nehmen kann. Dabei wird aber eine gewisse „Vagheit" aufgrund der Notwendigkeit, mit aktuellen Entwicklungen Schritt zu halten, hingenommen.[171] Jedoch muss sich der den Rechtsanwendern eingeräumte Spielraum und die Weise seiner Ausfüllung mit hinreichender Klarheit aus der Gesetzesgrundlage ergeben. Bei der Prüfung des erforderlichen Maßes an Bestimmtheit sind der Inhalt der Norm, das Rechtsgebiet sowie die Art und Anzahl der Adressaten zu berücksichtigen.[172] Eine gefestigte Rechtsprechung („settled case-law of this kind") kann die Verwendung unbestimmter Rechtsbegriffe konkretisieren.[173] Auch gewohnheitsrechtliche Grundlagen können, sofern sie diese Voraussetzungen erfüllen, „gesetzlich vorgesehen" i.S.v. Art. 8 Abs. 2 EMRK sein.[174] Bei Überwachungsmaßnahmen werden diese Anforderungen dahingehend konkretisiert, dass aufgrund der Gefahr der Befugnisüberschreitung bei verdeckten Maßnahmen schon das nationale Recht und nicht erst die behördliche Praxis Schutzvorkehrungen gegen willkürliche und missbräuchliche Eingriffe aufstellen muss („measure of protection", „adequate safeguards against various possible abuses").

### *b) Bestimmtheit*

Die Vorschrift muss so präzise formuliert sein, dass die Betroffenen die mit dem Eingriff verbundenen Folgen erkennen und ihr Verhalten danach ausrichten kön-

---

170 Ebd., S. 286 f.

171 EGMR Urteil vom 24.3.1988, *Olsson ./. Schweden*, App. Nr. 10465/83, [61 f.].

172 EGMR Entscheidung vom 4.12.2008, S. *u. Marper ./. Vereinigtes Königreich*, App. Nr. 30562/04 u. 30566/04 [95 f.].

173 *Esser*, in: Wolter u.a. (Hrsg.), Alternativentwurf, S. 287 (mit Verweis auf Entscheidungen *Kruslin, Huvig* und *Kopp*).

174 EGMR Entscheidung vom 26.4.1979, *The Sunday Times ./. Vereinigtes Königreich,* App. Nr. 6538/74, [47].

nen. Der Einsatz hochentwickelter Überwachungstechnologien verlangt detaillierte Regelungen („clear, detailed rules"), die dem Individuum aufzeigen, unter welchen Voraussetzungen die Maßnahmen ergriffen werden („adequate indication as to the circumstances and conditions"). Eine für sich betrachtete unklare Rechts- bzw. Gesetzeslage kann nur durch Rechtsprechung konkretisiert werden, wenn sie sich auf „settled case-law" stützen kann und nicht auf eine erweiternde Auslegung des Rechts („wide construction") hinausläuft. Insbesondere kann eine Generalklausel für Ermittlungszwecke keine Grundlage für verdeckte Überwachungsmaßnahmen bilden. Den durchführenden Stellen darf kein unbegrenzter Ermessensspielraum („unfettered power") eingeräumt werden.[175]

### *c) Ziel und Verhältnismäßigkeit*

Im nächsten Schritt prüft der EGMR das Vorliegen eines legitimen Ziels („legitimate aim") i.S.v. Art. 8 Abs. 2 EMRK. Dabei können der Schutz der nationalen Sicherheit bzw. öffentlichen Ordnung und insbesondere die Verhinderung von Straftaten die Verarbeitung personenbezogener Daten gebieten.[176] Im Anschluss an die Zweckprüfung untersucht der EGMR die Verhältnismäßigkeit. Dabei wird zunächst geprüft, ob der Eingriff in einer demokratischen Gesellschaft notwendig ist. „Notwendig" setzt nach der Rechtsprechung des EGMR ein „zwingendes gesellschaftliches Bedürfnis" („pressing social need") voraus. Zudem muss die Maßnahme in einem angemessenen Verhältnis zum verfolgten Zweck stehen („proportionate to the legitimate aim pursued"), wobei der Beurteilungsspielraum der nationalen Stellen sowohl von der Zielsetzung der Maßnahme als auch von dem Wesen des betroffenen Rechts abhängig ist.[177] Bei der Nachprüfung des Beurteilungsspielraums erörtert der EGMR zunächst, ob der Eingriff ausreichend begründet ist, und sodann, ob er in einem angemessenen Verhältnis zum verfolgten Zweck steht. Anschließend prüft der EGMR, ob eine Abwägung zwischen dem Allgemeininteresse und den Individualinteressen stattgefunden hat. Aus dieser Vorgehensweise hat man den Schluss gezogen, dass der Verhältnismäßigkeitsgrundsatz das wichtigste Element der Nachprüfung des nationalen Beurteilungsspielraums ist.[178] Innerhalb der Abwägung räumt der Gerichtshof den Staaten einen beschränkten Beurteilungsspielraum ein und hält eine strengere gerichtliche Nachprüfung für erforderlich, soweit das betroffene Recht die Intimsphäre des Einzelnen berührt, wie beispielsweise im Urteil *Z. gegen Finnland* das Recht auf Wahrung der Ver-

---

[175] Eingehend *Esser*, in: Wolter u.a. (Hrsg.), Alternativentwurf, S. 288 ff.

[176] Ebd., S. 295.

[177] EGMR Entscheidung vom 24.11.1986, *Gillow ./. Vereinigtes Königreich*, App. Nr. 9063/80, [55]; vgl. auch *Esser*, in: Wolter u.a. (Hrsg.), Alternativentwurf, S. 295.

[178] GA *Leger*, Schlussanträge vom 22.11.2005 zu EuGH Urteil vom 30.5.2006 verb. Rs. C-317/04 u. C-318/04 (*Fluggastdaten*-Schlussanträge) Rn. 227 m.w.N.

traulichkeit personenbezogener Gesundheitsdaten.[179] Ein größerer Beurteilungsspielraum („fairly wide margin of appreciation") wird hingegen bei den Zielen „Kampf gegen den Terrorismus" und „Schutz der nationalen Sicherheit" zugebilligt.[180] Eine anlasslose explorative und generelle Überwachung („exploratory or general surveillance") ist jedoch nicht mit dem Kriterium der Notwendigkeit vereinbar.[181]

### *d) Folgerungen für die weitere Untersuchung*

Für die Konturierung betroffener Risiken ist folglich zunächst relevant, wie der EGMR den Schutzbereich fasst und in welchen Konstellationen er von einem Eingriff in das Privatleben ausgeht. Näher zu betrachten ist dabei zuerst die Definition des Begriffs „Privatleben".[182] Der EGMR hat in mehreren Entscheidungen betont, dass sich dieser Begriff nicht abschließend definieren lasse.[183] Stattdessen dominiert eine kasuistische Betrachtungsweise. Diese Grundfeststellung teilt auch die überwiegende Literatur.[184] Obwohl sich unter den unzähligen Versuchen der Begriffsbestimmung und Fallgruppenbildung keine einheitliche Linie erkennen lässt, hat sich mittlerweile die Ansicht durchgesetzt, wonach der Datenschutz durch Art. 8 Abs. 1 EMRK gewährleistet wird.[185] Ein Teil der Literatur differenziert zwischen zwei Schutzgutkonzeptionen: Zum einen enthalte die Gewährleistung ein negatives Element der Privatsphäre, das vor Beeinträchtigungen durch die Öffentlichkeit schützen soll. Daneben bestehe ein Element der Selbstbestimmung, das nicht negativ auf die Abwehr von Öffentlichkeit, sondern positiv auf Interaktion

---

[179] GA *Leger*, Schlussanträge vom 22.11.2005 zu EuGH Urteil vom 30.5.2006 verb. Rs. C-317/04 u. C-318/04 (*Fluggastdaten*-Schlussanträge) Rn. 229, insb. Fn. 107 und die dort genannten Verfasser; EGMR Urteil vom 25.2.1997, *Z ./. Finnland*, App. Nr. 22009/93; kritisch gegenüber dem Konzept des Beurteilungsspielraums dagegen die teilweise abweichende Ansicht von *Judge de Meyer* im Anhang des Urteils.

[180] GA *Leger*, Schlussanträge vom 22.11.2005 zu EuGH Urteil vom 30.5.2006 verb. Rs. C-317/04 und C-318/04 (*Fluggastdaten*-Schlussanträge) Rn. 230.

[181] *Esser*, in: Wolter u.a. (Hrsg.), Alternativentwurf, S. 296.

[182] Zum Ganzen *Siemen*, Grundrecht, S. 58-63.

[183] EGMR Urteil vom 25.9.2001, *P.G. und J.H. ./. Vereinigtes Königreich*, App. Nr. 44787/98, [56]; EGMR Urteil vom 25.3.1993, *Costello-Roberts ./. Vereinigtes Königreich*, App. Nr. 13134/87, [36]; EGMR Urteil vom 16.12.1992, *Niemietz ./. Deutschland*, App. Nr. 13710/88, [29].

[184] Statt vieler *Wildhaber/Breitenmoser*, in: Karl (Hrsg.), IntKommEMRK Rn. 98 ff., der zudem auf die methodische Ähnlichkeit zum Vorgehen amerikanischer Gerichte bei der Konkretisierung des Begriffs „privacy" hinweist.

[185] *Grabenwarter*, Europäische Menschenrechtskonvention, S. 201; *Meyer-Ladewig*, Europäische Menschenrechtskonvention, Art. 8 Rn. 7, 40; *Bygrave*, in: Rule/Greenleaf (Hrsg.), Global Privacy Protection, S. 45 f. *Esser*, in: Wolter u.a. (Hrsg.), Alternativentwurf, S. 282 ff. Für die ältere Literatur *Breitenmoser*, Art. 8 EMRK, S. 43 ff. sowie S. 239 ff.

gerichtet sei.[186] Der erste Bereich spiegelt die Vorstellung privater „Geheimsphären" wider, welche die deutsche und amerikanische Rechtswissenschaft des späten 19. Jahrhunderts aus der römisch-rechtlichen actio injuriarum und vergleichbaren Rechtsinstituten des common law entwickelte.[187] Einflüsse dürften auch aus dem französischen Recht stammen, wo die Vorstellung räumlicher Rückzugsbereiche in denen das innere und geistige Leben als „hinter geschlossenen Türen" ablaufend beschrieben wird, ebenfalls geläufig ist.[188] Diese Konzeption, welche im deutschen Recht in der Sphärendogmatik des BVerfG[189] ihre stärkste Ausprägung findet, geht davon aus, dass sich um einen Kern der persönlichen Lebensgestaltung verschiedene Kreise ziehen lassen, die durch einen (räumlich oder thematisch) immer stärkeren Öffentlichkeitsbezug geprägt sind. Das andere Element lässt die Selbstbestimmung über Informationen in den Vordergrund treten und ist rechtsgeschichtlich ebenfalls spätestens seit *Josef Kohler* und *Warren/Brandeis* präsent.[190] Das Selbstbestimmungs-Element wird häufig als spätere Entwicklungsstufe des Grundrechts angesehen, wobei eine solche Entwicklung auch der EMRK in Aussicht gestellt wird.[191] Die besondere Stärke des Selbstbestimmungselements liegt in der Möglichkeit, dynamisch und unabhängig von objektiven, sich ändernden Bedingungen auf unterschiedliche Verwendungskontexte von Informationen einzugehen. Gleichwohl birgt es die Gefahr der Uferlosigkeit des Schutzbereichs und bedarf genauer Kenntnis vorhandener Risiken. Im Folgenden soll überprüft werden, welche Risiken das bisherige Fallrecht zum Gegenstand hatte, insbesondere, wie Schutzbereich und Eingriff konstruiert wurden.

## B. Risikokonzeptionen und Schutzgüter

### 1. Überwachungsbedrohung und Willkür

Die ältere Rechtsprechung des EGMR und der EKMR kannte den Datenschutz noch nicht als eigenständigen Schutzgehalt. Der Schutz personenbezogener Daten konnte sich zwar als Nebeneffekt zu einer Überwachungshandlung oder dem Ort der Aufbewahrung von Informationen ergeben, nicht jedoch aus der Natur der personenbezogenen Daten selbst.[192] So wurde etwa in der *Entscheidung Klass gegen Deutschland* das maßgebliche Risiko der durch das G10-Gesetz a.F. zugelassenen

---

186 *Siemen*, Grundrecht, S. 75 f. im Anschluss an *Peters*, Einführung, S. 156 ff.

187 *Maass*, Zivilrecht, S. 3 sowie oben Einleitung, I.

188 „La vie privée, c'est la vie familiale, personnelle de l'homme, sa vie intérieur, spirituelle, celle qu'il mène lorsqu'il vit derrière sa porte fermèe", *Martin*, zit. nach *Siemen*, Grundrecht, S. 59, Fn. 37.

189 Siehe unten Teil 3, II.B.1. sowie Maunz/Dürig-*DiFabio*, Art. 2 Rn. 157–162.

190 Siehe oben Einleitung, I.

191 *Siemen*, Grundrecht, S. 60 ff. m.w.N.

192 Ebd., S. 90; *Esser*, in: Wolter u.a. (Hrsg.), Alternativentwurf, S. 283.

Überwachungsmaßnahmen nicht in der Art der betroffenen Informationen, sondern in einer abstrakten Überwachungsbedrohung („menace of surveillance") gesehen.[193] Bemerkenswert ist, dass der Gerichtshof den Eingriff schon aufgrund der bloßen Existenz der Gesetzgebung bejaht. Er beurteilt das Risiko nicht auf den konkreten Einzelfall bezogen, sondern aus „Makrosicht" hinsichtlich eines sich auf die gesamte Bevölkerung erstreckenden Überwachungsgefühls. Da es für den Eingriff nicht erforderlich ist, dass der Betroffene tatsächlich überwacht wurde, wird der Charakter eines Vorfeldschutzes besonders unterstrichen.[194] Im Rahmen der Rechtfertigung führt der Gerichtshof aus, dass die geheimen Überwachungsmaßnahmen typisch für Polizeistaaten seien und insoweit eine strenge Prüfung des Kriteriums der Notwendigkeit zu erfolgen habe („strictly necessary for safeguarding the democratic institutions").[195] Die Überwachungsgesetze begründeten die Gefahr einer Schwächung oder gar Zerstörung der Demokratie im Namen ihres Schutzes.[196] Bei der Erörterung der Anordnungsvoraussetzungen wird das Risiko willkürlicher oder leichtfertiger Anwendung der Überwachungsmaßnahmen herausgestellt.[197] Der Gerichtshof stellt damit einen Zusammenhang zwischen dem Risiko der Überwachungsbedrohung, insb. durch mögliche Willkürmaßnahmen, und dem Demokratieprinzip her.

Die Kommissionsentscheidung *McVeigh gegen das Vereinigte Königreich* betraf das Einbehalten von Fingerabdrücken und Fotografien, die bei polizeilichen Untersuchung erhoben und anschließend in einem Polizeiregister gespeichert wurden.[198] Die Speicherung dauerte an, auch nachdem sich der für die Erfassung ursächliche Verdacht nicht bestätigt hatte. Die Kommission lehnte in dieser Entscheidung ohne nähere Begründung eine Verletzung von Art. 8 EMRK ab, weil sie Erhebung und Speicherung als gerechtfertigt ansah. Mangels geheimer Überwachungsmaßnahmen zog sie nicht den Vergleich zum Fall *Klass*.[199] Zwar werden im Entscheidungstext keine Ausführungen zu einschlägigen Risiken gemacht, die Entscheidung enthält jedoch eine abweichende Meinung des Kommissionsmitglieds *Klecker*, in der Zweifel an der Rechtmäßigkeit der Speicherung nach Wegfallen des Verdachts dargelegt werden.[200] *Klecker* bezieht sich darin auf die Stellungnahme eines englischen Datenschutzkomitees, in der mangelhafte Schutzmechanismen für die in Polizeiregistern erfassten Personen kritisiert werden.[201] Außer einem Verweis auf die fehlende

---

193 EGMR Urteil vom 6.9.1978, *Klass ./. Deutschland*, App. Nr. 5029/71, [41].

194 Ebd., [41].

195 Ebd., [42].

196 Ebd., [49].

197 Ebd., [51].

198 EKMR Entscheidung vom 18.3.1981, *McVeigh / Vereinigtes Königreich*, App. Nr. 8022/77, 8025/77, 8027/77; zum Ganzen *Siemen*, Grundrecht, S. 83 ff.

199 EKMR Entscheidung vom 18.3.1981, *McVeigh / Vereinigtes Königreich*, App. Nr. 8022/77, 8025/77, 8027/77, S. 64 ff.

200 Ablehnende Meinung *Klecker*, ebd., S. 72.

201 Ebd.

Erforderlichkeit der Speicherung nennt er jedoch keine Argumente. Gleichwohl zeigt die abweichende Meinung, dass sich ein Bewusstsein für die aufkommenden datenschutzrechtlichen Fragestellungen in der Kommission bildete.[202]

Die Entscheidung *Malone gegen das Vereinigte Königreich* hatte die mehrjährige Überwachung von Briefverkehr und Telefongesprächen eines Beschuldigten zum Gegenstand.[203] Der Gerichtshof differenzierte in dieser Entscheidung erstmals zwischen der Registrierung von Verbindungsdaten und anderen Maßnahmen der Kommunikationsüberwachung. Er wich jedoch der Frage aus, ob diese Verbindungsdaten in den Bereich des Privatlebens fallen. Stattdessen betrachtete er sie als Bestandteil der Telefongespräche.[204] Der Gerichtshof ging nicht näher auf den Schutzbereich von Art 8 Abs. 1 EMRK ein, sondern bejahte einen Eingriff schon aufgrund der Existenz geheimer Telefonüberwachungen und bezog sich wiederum auf die abstrakte Überwachungsdrohung unter Verweis auf die Entscheidung *Klass*.[205] Ausführlicher widmet sich der Gerichtshof der Rechtfertigung gem. Art. 8 Abs. 2 EMRK. Eine Verletzung bejaht er schließlich mangels tauglicher Rechtsgrundlage.[206] Im Rahmen der Rechtfertigung führt der Gerichtshof unter Verweis auf die *Klass*-Entscheidung aus, dass geheime Überwachungen ein evidentes Risiko für Willkür darstellen: „Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident".[207] Diese Risikokonzeption wurde auch in späteren Entscheidungen aufgegriffen.[208]

### *a) Vergleich mit Orwells „Big Brother"*

Obwohl der Fall *Malone* eine nähere Analyse des Schutzbereichs des Privatlebens und der Risiken vermissen lässt, ist er aufgrund der zustimmenden Meinung des Richters *Pettiti* für die Untersuchung von besonderer Bedeutung. *Pettiti* befasst sich darin ausführlich mit den Risiken, die dem Datenschutz zugrunde liegen. Da es sich hierbei um die erste eigenständige und ausführliche Erörterung einschlägiger Risiken durch den EGMR handelt, ist diese näher zu analysieren.[209] *Pettiti* beschreibt zunächst den Anreiz für den Staat, Einblick „in das Leben" seiner Bürger zu nehmen. Dieser erfolge zu allgemeinen Planungszwecken, insbesondere in den

---

202 *Siemen*, Grundrecht, S. 84.

203 EGMR Urteil vom 2.8.1984, *Malone ./. Vereinigtes Königreich*, App. Nr. 8691/79; zum Ganzen *Siemen*, Grundrecht, S. 86 ff.

204 EGMR Urteil vom 2.8.1984, *Malone ./. Vereinigtes Königreich*, App. Nr. 8691/79, [84].

205 Ebd., [64].

206 Ebd., [66–80].

207 Ebd., [67].

208 So etwa EGMR Urteil vom 30.7.1998, *Valenzuela Contreras ./. Spanien*, App. Nr. 58/1997/842/1048, [46]; EGMR Urteil vom 16.2.2000, *Amann ./. Schweiz*, App. Nr. 27798/95, [56].

209 Vgl. auch *Siemen*, Grundrecht, S. 87 f.

Bereichen der Sozial- und Steuerpolitik. Die Ausweitung staatlicher Interessen bewirke eine Vermehrung und Computerisierung persönlicher Datensätze. In einem späteren Stadium würden „Profile" der Bürger erstellt, welche zum Zwecke statistischer Erhebungen und bei Entscheidungsprozessen eingesetzt würden. *Pettiti* wendet sich sodann der Telefonüberwachung zu. Er beschreibt, wie diese in Verbindung mit den Möglichkeiten moderner Informationstechnologie immer effektiver ausgestaltet wird, um letztlich dazu beizutragen, ein komplettes Bild der Lebensführung eines Menschen durch viele kleine „Mosaiksteine" zu erstellen. Die neuen Techniken könnten nicht nur zur Strafverfolgung, sondern auch zur Überwachung von Journalisten und von Geheimdiensten eingesetzt werden. Dabei rügt *Pettiti* vor allem die mangelnde demokratische Kontrolle. Er plädiert für die Trennung exekutiver und judikativer Befugnisse, indem derartige Überwachungsmaßnahmen umfassend der richterlichen Anordnung und nachträglichen Kontrolle unterstellt werden.

Näher zu betrachten sind die Risiken, die *Pettiti* zur Begründung heranzieht: Polizeiliche Telefonüberwachungen führten zur Existenz sog. „prosecution files", welche die Regeln der Verfahrensfairness des Art. 6 EMRK unterlaufen würden, indem sie eine Schuldvermutung aufstellten. *Pettiti* nennt sodann verschiedene Rechtspositionen, die den Betroffenen zu gewähren seien. Dazu zählt er u.a. das Recht auf Zugang zu den Informationen nach Verfahrenseinstellungen oder Freispruch, Löschungsrechte und die vertrauliche Behandlung des Vorgangs. Erstmals findet sich ein expliziter und ausführlicher Verweis auf die Datenschutzkonvention des Europarats. *Pettiti* sieht die „Mission" des Europarats und seiner Organe in der Verhinderung eines Systems, wie es demjenigen des „Big Brother" aus *George Orwells* Roman „1984" entspricht. Weiterhin hält er Telefonüberwachungen für vergleichbar mit der im Roman beschriebenen optischen Überwachung von Privaträumen. Er führt schließlich aus, dass sich Natur und Auswirkungen automatisierter Datenverarbeitung völlig von denen manueller Datenverarbeitungen unterschieden. Schließlich verweist *Pettiti* auf das Volkszählungsurteil des Bundesverfassungsgerichts und plädiert für eine enge Auslegung der Schranken des Art. 8 Abs. 2 EMRK. Geheime Überwachungsmaßnahmen seien charakteristisch für Polizeistaaten und im Rahmen der EMRK nur zu tolerieren, wenn sie wirklich notwendig zum Schutz demokratischer Institutionen sind. Hinsichtlich der Abfrage von Verbindungsdaten weist *Pettiti* darauf hin, dass dabei auch Informationen zugänglich würden, die über den Zweck der Abfrage hinausgehen. Zudem hält er die automatisierte Verarbeitung neutraler Daten für genauso „enthüllend" wie diejenige von sensiblen Daten. *Pettiti* beendet sein Votum mit der Feststellung, dass das „right to be let alone" von Art. 8 EMRK umfasst sei.[210]

---

[210] Zustimmende Meinung von Richter *Pettiti*, EGMR Urteil vom 2.8.1984, *Malone ./. Vereinigtes Königreich*, App. Nr. 8691/79, [Anhang].

Die Entscheidung *Weber und Saravia gegen Deutschland*[211] steht exemplarisch für den in der Folgezeit stattfindenden Eingang der Risikokonzeption in die ständige Rechtsprechung. Sie erging infolge des zweiten Urteils des Bundesverfassungsgerichts zur Telekommunikationsüberwachung.[212] Gegenstand der Entscheidung waren die Vorschriften des G 10 zur strategischen Telekommunikationsüberwachung. Der Gerichtshof bejaht die Anwendbarkeit von Art. 8 Abs. 1 EMRK aufgrund der zuvor in *Klass* und *Malone* ermöglichten Erfassung der Telekommunikation von den Begriffen „Privatleben" und „Korrespondenz". Das maßgebliche Risiko sei die durch ein System geheimer Kommunikationsüberwachungen geschaffene abstrakte Überwachungsdrohung.[213] Die Entscheidung ist insofern bedeutend, als der EGMR darin nicht nur die Argumentation der Fälle *Klass* und *Malone* bekräftigt, sondern auch explizit das Risiko benennt, dass der Betroffene durch Weitergabe von Informationen an andere Behörden Ermittlungen ausgesetzt wird. Aufgrund dieses Risikos stellen Weitergabe und Nutzung von Daten durch die Behörde einen eigenständigen Eingriff in Art. 8 Abs. 1 EMRK dar.[214] Mit dieser Argumentation stimmt der EGMR mit dem BVerfG überein und übernimmt, wie sich zeigen wird, ein entscheidendes Merkmal modernen Informationsschutzes – nämlich den vor innerstaatlicher Informationsweitergabe. An gleicher Stelle bestätigt der EGMR darüber hinaus den Eingriffscharakter der Löschung und Nicht-Benachrichtigung der Betroffenen, weil dies dazu dienen kann, die Eingriffe in Art. 8 Abs. 1 EMRK zu verschleiern. Hiermit knüpft der EGMR an die schon im Sondervotum von Richter *Pettiti* entwickelte Forderung[215] an und übernimmt diese. In darauffolgenden Entscheidungen zu Telekommunikationsüberwachungsmaßnahmen wurde der Schutzbereich in vergleichbarer Weise eröffnet, so etwa in *Association for European Integration and Human Rights und Ekimdzhiev gegen Bulgarien*, *Liberty u.a. gegen Vereinigtes Königreich* sowie *Iordachi u.a. gegen Moldau*.[216]

---

[211] EGMR Entscheidung vom 29.6.2006, *Weber u. Saravia ./. Deutschland*, App. Nr. 54934/00 = NJW 2007, 1433.

[212] BVerfG Urteil vom 14.7.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, BVerfGE 100, 313; dazu unten Dritter Teil, II.B.5. sowie 9.a).

[213] EGMR Entscheidung vom 29.6.2006, *Weber u. Saravia ./. Deutschland*, App. Nr. 54934/00, [77].

[214] Ebd., [79]. Die herangezogenen Verweise auf *Leander*, *Amann* und *Rotaru* sind dabei jedoch nicht zielführend und verschleiern lediglich, dass der EGMR hier eine manifeste Erweiterung des Schutzes vorgenommen hat. Gerechtfertigt wäre hingegen ein Verweis auf BVerfGE 100, 313.

[215] Siehe oben IV.B.1.a).

[216] EGMR Entscheidung vom 28.6.2007, *Association for European Integration and Human Rights und Ekimdzhiev ./. Bulgarien*, App. Nr. 62540/00; EGMR Entscheidung vom 1.7.2008, *Liberty u.a. ./. Vereinigtes Königreich*, App. Nr. 58243/00; EGMR Entscheidung vom 10.2.2009, *Iordachi u.a. ./. Moldau*, App. Nr. 25198/02.

*b) Zwischenergebnis*

Die besprochenen Entscheidungen nehmen insgesamt gesehen somit nur eingeschränkt Stellung zu einschlägigen Risiken. Gleichwohl lässt sich anhand der Entscheidung *Klass* und der zustimmenden Meinung des Richters *Pettiti* zur Entscheidung *Malone* das Risiko einer Überwachungsbedrohung deutlich nachvollziehen. Dieses Risiko korrespondiert mit dem „Überwachungsdruck", der in Zusammenhang mit den oben untersuchten datenschutzrechtlichen Spezialinstrumenten an verschiedenen Stellen zumindest angedeutet wurde. Insbesondere in *Klass* wird die Nähe dieses Risikos zum Demokratieprinzip herausgestellt. Die zustimmende Meinung von *Pettiti* verdeutlicht die gesellschaftliche „Makro"-Perspektive indem ein Eingriff unabhängig von der konkreten Anordnung im Einzelfall bejaht wird. Beide Entscheidungen nennen die aus mangelnder Transparenz folgende Möglichkeit zu willkürlichem Behördenhandeln als weiteren Bestandteil des Risikos verdeckter Überwachungsmaßnahmen. Der Fall *Weber* und *Saravia* führt zu einer Ergänzung dieses Befundes um das Risiko von Anschlussermittlungen, das bei behördlichem Datenaustausch entsteht.

### 2. Flexibilisierung der Schutzgutkonzeption

*Pettitis* Appell steht am Beginn einer Rechtsprechungsänderung, die seit dem Urteil *Leander gegen Schweden*[217] den Schutzbereich stärker an die Information als solche statt an die Erhebungsmodalitäten und Sphärencharakteristika knüpft.[218] Dem Fall lag die Beschwerde des schwedischen Museumstechnikers *Leander* zugrunde, der nach einer Sicherheitsüberprüfung durch die Polizei entlassen wurde. Die Prüfung war angeordnet worden, da sich das Museum auf militärischem Sperrgebiet befand. Der Museumstechniker müsse sich frei auf dem Gelände bewegen können und sei deshalb zu überprüfen, lautete die Begründung. *Leander* wurde weder Einsicht in das geheime Polizeiregister noch eine Möglichkeit zur Stellungnahme eingeräumt.

Der EGMR übernimmt in der Entscheidung zunächst einen an das allgemeine Datenschutzrecht angelehnten Eingriffsbegriff, indem er sowohl in der Speicherung als auch in der Weitergabe von Informationen einen Eingriff sieht („both the storing and the release of such information, […] amounted to an interference").[219] Zentral für das Vorliegen des Eingriffs ist ein neues Prüfungsmerkmal: der Bezug der Informationen zum Privatleben („information relating to Mr. Leander's private life").[220] Sofern man die Ausführungen im Kommissionsbericht hinzunimmt, be-

---

[217] EGMR Urteil vom 26.3.1987, *Leander ./. Schweden*, App. Nr. 9248/81.

[218] Vgl. auch *Siemen*, Grundrecht, S. 90 f.

[219] EGMR Urteil vom 26.3.1987, *Leander ./. Schweden*, App. Nr. 9248/81, [48].

[220] Ebd.

steht dieser Bezug dann, wenn Informationen über Handlungen, Verbindungen und Meinungen Rückschlüsse auf das Verhalten oder die Persönlichkeit des Einzelnen zulassen. Dagegen soll ein Register mit bloßen Namens- und Adressangaben „normalerweise" keine Beeinträchtigung von Art. 8 EMRK darstellen.[221] Eine Auslegung entsprechend der Datenschutzkonvention des Europarats – wo gem. Art. 2 a) bereits „jede Information über eine bestimmte oder bestimmbare natürliche Person" den Anwendungsbereich und damit das Schutzkonzept eröffnet – konnte sich noch nicht durchsetzen. Das *Leander*-Urteil beinhaltet dennoch eine erhebliche Annäherung an das Schutzkonzept der Konvention 108 und stellt damit einen wichtigen Schritt zur Verselbstständigung des Merkmals „Information" als Anknüpfungspunkt für rechtlichen Schutz dar.[222] Eine solche abstraktere Betrachtung ist notwendig in der Entwicklung vom Schutz des Individuums gegen bestimmte Überwachungsmaßnahmen hin zu einem Schutz gegen „Informationsverwendungsfolgen", der bereits im Vorfeld greift. Im Rahmen des Prüfungspunktes Vorhersehbarkeit („foreseeability") wird zudem das Risiko der Willkür bei verdeckten, keiner Kontrolle zugänglichen Maßnahmen erneut herausgestellt, auf das sich bereits die Entscheidungen *Klass* und *Malone* bezogen.[223] Verwiesen wird außerdem im Rahmen der Notwendigkeit auf das Risiko einer „Verringerung oder Zerstörung der Demokratie unter dem Vorwand ihrer Verteidigung", das ebenfalls bereits in *Klass* entwickelt wurde.[224]

Die Erfassung des Datenschutzes vom Schutzbereich des Art. 8 Abs. 1 Var. 2 EMRK wurde sodann in der Zulässigkeitsentscheidung *Lundvall gegen Schweden* bestätigt.[225] Der Fall betraf die Aufnahme des Steuerschuldners *Lundvall* in ein spezielles Register unter Verwendung der schwedischen Personen-Identifizierungsnummer („personnummer"). Der Umstand, dass *Lundvall* ein Rechtsmittel gegen die Zahlungsverpflichtung eingelegt hatte, welches jedoch keine aufschiebende Wirkung besaß, war nicht im Register vermerkt. Ein Problem für *Lundvall* resultierte daraus, dass es in Schweden grundsätzlich möglich ist, derartige Informationen innerhalb des allgemeinen Rechts auf Informationszugang einzusehen.[226] Dies führte im vorliegenden Sachverhalt dazu, dass *Lundvall* als nicht kreditwürdig eingestuft wurde. Die Kommission bestätigte in ihrem Bericht zunächst, dass Datenschutz in den Anwendungsbereich von Art. 8 Abs. 1 EMRK fällt, und hält es deshalb für möglich („conceivable"), dass der Abgleich verschie-

---

221 EKMR Bericht vom 17.5.1985, *Leander ./. Schweden*, App. Nr. 9248/81 [56]; *Siemen*, Grundrecht, S. 89.

222 *Siemen*, Grundrecht, S. 90 f., sieht in diesem Wandel eine Aufwertung des Schutzbereichs als eigenen Prüfungspunkt.

223 EGMR Urteil vom 26.3.1987, *Leander ./. Schweden*, App. Nr. 9248/81, [50].

224 Ebd., [60].

225 EKMR Entscheidung vom 11.12.1985, *Lundvall ./. Schweden*, App. Nr. 10473/83.

226 Dies erklärt sich mit dem verfassungsrechtlichen Öffentlichkeitsprinzip *(offentlighetsprincipen)* gem. 2 kap. 1 § TF.

dener Register unter Verwendung einheitlicher Identifizierungsnummern im Rahmen von Art. 8 Abs. 1 EMRK zu berücksichtigen sei. Sie bricht dann jedoch eine eingehende Auseinandersetzung mit den Risiken ab, um die Beschwerde ratione personae für unzulässig zu erklären.[227] Der Fall verdeutlicht, dass die Übertragung von Informationen aus einem Bereich (Steuerschulden) auf einen anderen (private Kreditaufnahme) als Risiko erkannt wurde. Das Risiko eines „Durchbrechens" informationeller Ebenen ist bereits aus der Untersuchung der Spezialinstrumente bekannt und dort als Entkontextualisierung, genauer als „Kontextinfiltration" bezeichnet worden.[228] Die Entscheidung stellt ein weiteres Beispiel für diese Risikogruppe dar. Die negativen Auswirkungen bestehen dabei hinsichtlich der Inanspruchnahme von Dienstleistungen, was im Fall von Kreditvergaben besonders einschneidend sein kann. Hier liegt aber auch ein Aspekt des Risikos „Kontextdefizit" vor. Die Information, dass *Lundvall* ein Rechtsmittel gegen die Zahlungsverpflichtung eingelegt hatte, wurde in den zweiten Kontext, also in die Kreditwürdigkeitsprüfung, nicht einbezogen. Zwar hatte das Rechtsmittel keine aufschiebende Wirkung hinsichtlich der Zahlung, gleichwohl hätte die Information womöglich positive Auswirkungen auf den Scoringwert (der z.B. in Prozent der Erfüllungswahrscheinlichkeit angegeben werden kann)[229] gehabt.

Eine gewisse Bedeutung für die Risikokonzeption kommt dabei auch dem systematischen Verfahren durch Verwendung übergreifender Identifikationsnummern zu. So wurden etwa in der Kommissionsentscheidung *Reyntjens gegen Belgien* Personalausweisdaten ohne eine solche Identifikationsnummer als nicht relevant für Art. 8 Abs. 1 EMRK angesehen.[230]

In einer Reihe weiterer Fälle bestätigten die Kommission und der Gerichtshof die grundsätzliche Erfassung des Datenschutzes vom Anwendungsbereich des Art. 8 Abs. 1 EMRK, ohne jedoch näher auf zugrundeliegende Risiken einzugehen.[231] Dabei wurde allerdings deutlich, dass die aus der frühen Rechtsprechung stammende räumlich-sphärenartige Konzeption des Schutzguts zunehmend ausgeweitet wurde: Art. 8 Abs. 1 EMRK umfasst demnach nicht lediglich einen „inneren Kreis", sondern auch das Recht, soziale Beziehungen aufzunehmen.[232] Andererseits

---

[227] EKMR Entscheidung vom 11.12.1985, *Lundvall ./. Schweden*, App. Nr. 10473/83, S. 130.

[228] Siehe oben II.B.

[229] Vgl. z.B. das „Infoblatt Scoreübersicht" der Schufa, http://www.schufa.de/media/teamwebservices/wissenswertes/downloads_11/scoringinfo/schufa_infoblatt_scoreuebersicht_100120final.pdf [Stand: 16.6.2013].

[230] EKMR Entscheidung vom 9.9.1992, *Reyntjens ./. Belgien*, App. Nr. 16810/90, S. 152; *Siemen*, Grundrecht, S. 93.

[231] EKMR Entscheidung vom 12.5.1988, *P.H. u. H.H. ./. Vereinigtes Königreich*, App. Nr. 12175/86; EKMR Entscheidung vom 13.10.1988, *L. ./. Deutschland*, App. Nr. 12793/87.

[232] EGMR Urteil vom 16.12.1992, *Niemietz ./. Deutschland*, App. Nr. 13710/88, [29]; EKMR Entscheidung vom 19.5.1994, *Friedl ./. Österreich*, App. Nr. 15225/89, [44]; Ähn-

zeigen die Kommissionsentscheidungen *Lupker gegen die Niederlande*[233] und *Friedl gegen Österreich*,[234] dass bestimmte Anknüpfungspunkte aus der Öffentlichkeitssphäre den Bezug zum Privatleben entfallen lassen können:[235] Im Fall *Lupker* wurden Fotografien, die für den Führerschein bzw. Personalausweis erstellt wurden, im Rahmen strafrechtlicher Ermittlungen verwendet. Die Kommission hielt diese Praxis für zulässig, da die Fotografien „freiwillig" an die Behörden gegeben wurden.[236] Zudem führt die Kommission aus, dass die Bilder nicht der Allgemeinheit zugänglich gemacht wurden und nur zum Zwecke der Identifizierung Verwendung fanden. Dies spricht für ein eher sphärenartiges Verständnis, wonach Informationen, die einmal in die Öffentlichkeitssphäre entäußert wurden, frei verwendet werden können. Nach diesem Verständnis läge das Risiko weniger in den Folgen der Informationsverwendung als in der Verletzung einer privaten Sphäre. Die bereits in der Datenschutzkonvention des Europarats enthaltene Berücksichtigung von Zweckänderungen wurde im Fall *Lupker* somit nicht aufgegriffen, obwohl insbesondere das Risiko der Entkontextualisierung in den Kommissionsentscheidungen *Lundvall* und *Reyntjens* bereits identifiziert worden war. Auch der Hinweis in *Lupker* auf „bloße Identifizierungszwecke" blendet das Risiko der Entkontextualisierung, das aus der Übernahme von Meldedaten in strafrechtliche Kontexte entsteht, aus.

Der Fall *Friedl* betraf die Erstellung polizeilicher Fotografien eines Demonstrationsteilnehmers nach Auflösung der Kundgebung und seine anschließende Befragung zur Identitätsfeststellung. Die Fotografien dienten der Vorsorge späterer Strafverfolgung, wurden letztlich jedoch nicht verwendet. Zwar wurden die Bilder nicht mit den Personendaten des Abgebildeten zusammengeführt, auch nicht in ein elektronisches Datenverarbeitungssystem eingegeben und lediglich in einer Akte zu der betreffenden Demonstration abgelegt; gleichwohl verdeutlicht die mit einem Vergleich endende Entscheidung[237] eine Relativierung räumlicher Schutzgutkonzeptionen, ohne dass sich jedoch ein konsequenter Übergang zu einer das Risiko der Entkontextualisierung aufgreifenden Konzeption durchsetzen konnte: Die Kommission trennt zunächst zwischen den Bildaufnahmen und der Befragung. Hinsichtlich der Bildaufnahmen entwickelt sie aus der bisherigen Rechtsprechung, insbesondere den Fällen *Leander* und *McVeigh*, vier Prüfungskriterien. Das erste

---

lich, aber mit stärkerer Betonung der Sphärenkonzeption EKMR Entscheidung vom 12.7.1977, Brüggemann, *Scheuten ./. Deutschland*, App. Nr. 6959/75, [55-57].

233 EKMR Entscheidung vom 7.12.1992, *Lupker ./. Niederlande*, App. Nr. 18395/91.

234 EKMR Entscheidung vom 19.5.1994, *Friedl ./. Österreich*, App. Nr. 15225/89.

235 *Siemen*, Grundrecht, S. 103 f.

236 Zwar enthält die Entscheidung keine nähere Erörterung der so verstandenen „Freiwilligkeit", gleichwohl scheint nicht das Konzept der Einwilligung im Vordergrund zu stehen. Eine Einwilligung wäre mangels Kenntnis der späteren Verwendung bzw. mangels Aufklärung über derartige Verwendungszwecke unwirksam.

237 EGMR Entscheidung vom 31.1.1995, *Friedl ./. Österreich*, Entscheidung Nr. 28/1994/475/556.

Kriterium ist das Eindringen in den privaten Bereich des Individuums („intrusion into the individual's privacy"). Zweitens wird geprüft, ob sich dieses Eindringen auf private oder öffentliche Umstände bezieht („related to private matters or public incidents"). Das dritte Kriterium bezieht sich auf die Zugänglichmachung des Materials („whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public"). Zuletzt verweist die Kommission auf das Kriterium der freiwilligen Preisgabe.[238] Diese Kriterien sollen alternativ die Eröffnung des Schutzbereichs von Art. 8 Abs. 1 EMRK ermöglichen. Weil die Bildaufnahmen nicht mit Namen versehen und nicht aus dem „inneren Kreis", etwa der Wohnung, erhoben wurden, konnte die Kommission keinen Eingriff erkennen. Bezüglich der Befragung bejaht sie zwar einen Eingriff, sieht diesen jedoch als gerechtfertigt an.

Der Fall zeigt damit, wie die Kommission verschiedene Konzeptionen aus den vorangegangenen Entscheidungen – Sphärenbetrachtung, inhaltlicher Bezug und Selbstbestimmungskonzeption – kombiniert, ohne jedoch zur Frage von Informationsverwendungsfolgen Stellung zu nehmen und ohne auf das Schutzkonzept der Datenschutzkonvention zurückzugreifen, welche die Betroffenheit personenbezogener Daten in der Regel als Anlass für ihre Schutzgewährleistungen ausreichen lässt. Auch das zuvor bereits in *Reyntjens* und *Lupker* durchscheinende Risiko der Entkontextualisierung wird nicht aufgegriffen. Bedeutsam ist jedoch, dass entsprechend den *Friedl*-Kriterien Art. 8 Abs. 1 EMRK grundsätzlich auch bei der Überwachung öffentlicher Orte einschlägig sein kann und somit die Fortentwicklung des Sphärenverständnisses hin zu einer flexibleren, auf Risiken abstellenden Konzeption begünstigt wird. In kurzer Folge wurde diese Flexibilisierung mehrfach durch die EKMR bestätigt. So stellte die Kommission in der Entscheidung *Tsavachidis gegen Griechenland* fest, dass auch Aktivitäten, die an öffentlichen Orten stattfinden und nicht mittels besonderer Geheimhaltungsmaßnahmen vor Kenntnisnahme geschützt werden, in den Anwendungsbereich des Art. 8 Abs. 1 EMRK fallen können.[239]

Relativiert wird diese Entwicklung durch Einbeziehung eines Publizitätskriteriums (Zugänglichmachung für einen größeren Personenkreis). So wird in der Entscheidung *Campion gegen Frankreich* die Aufnahme eines Fotos bei einer Geschwindigkeitsmessung unter Verwendung der *Friedl*-Kriterien deshalb abgelehnt, weil die Aufnahme keinem größeren Personenkreis bekanntgemacht wurde.[240] Diese Beschränkung findet sich sodann in der Entscheidung *Herbecq gegen Belgien* wieder.[241] Der Fall betrifft die Videoüberwachung öffentlicher Plätze in Belgien.

---

238 EKMR Bericht vom 19.5.1994, *Friedl ./. Österreich*, App. Nr. 15225/89, [48].

239 EKMR Bericht vom 28.10.1997, *Tsavachidis ./. Griechenland*, App. Nr. 28802/95, [47]; vgl. auch *Siemen*, Grundrecht, S. 107 f.

240 EKMR Entscheidung vom 6.9.1995, *Campion ./. Frankreich*, App. Nr. 25547/94.

241 EKMR Entscheidung vom 14.1.1998, *Herbecq ./. Belgien*, App. Nr. 32200/96 und 32201/96; vgl. auch *Siemen*, Grundrecht, S. 108 f.

Die Kommission führt darin aus, dass eine Situation, in der Videoaufnahmen von der Überwachungskamera nicht gespeichert und lediglich von den auf den Monitor blickenden Personen gesichtet werden, mit einer Situation identisch sei, in der die Überwachungsperson selbst vor Ort ist und die Geschehnisse verfolgt. Der Beschwerdeführer habe darüber hinaus nicht geltend gemacht, dass etwaige private Handlungen an öffentlichen Orten überwacht würden.[242] Die Kommission hält somit am Kriterium des Inhaltsbezugs aus der Entscheidung *Leander* fest. Sie aktiviert jedoch durch das Kamerabeispiel ein Argument, das als „bloße Raumüberwindung" umschrieben werden kann. Die bloße Effizienzsteigerung durch Technikeinsatz soll insoweit also gerade kein eigenständiges Risiko darstellen. Die im Zuge der *Niemietz*-Entscheidung ermöglichte Ausdehnung des Privatlebensbegriffs über den „inner circle" hinaus wird durch die *Friedl*-Kriterien im Ergebnis also nur leicht verstärkt. Das Publizitätskriterium markiert weiterhin die Grenze.[243] Gleichwohl erfolgte mit dem Kriterium der freiwilligen Preisgabe die Öffnung hin zu einem flexibleren Verständnis und zu einer Anknüpfung an Risiken und Folgen der Informationsverarbeitung.

Der Fall *Amann gegen die Schweiz*[244] markiert sodann die nächste Stufe der Annäherung von Konventionsgarantie und Datenschutzübereinkommen.[245] Die Entscheidung betrifft die Aufnahme personenbezogener Informationen eines Schweizer Epiliergerätehändlers in ein geheimes Polizeiregister. Der Händler wurde darin als Kontakt zur russischen Botschaft geführt, weil eine seiner Kundinnen eine telefonische Bestellung aus der russischen Botschaft vorgenommen hatte. Das Telefonat wurde abgehört. Der Gerichtshof stellt fest, dass entsprechend den Fällen *Leander* und *Niemietz* eine weite Auslegung von Art. 8 EMRK zu erfolgen habe. Zudem sei die Speicherung von auf das Privatleben bezogenen Daten auch im beruflichen Kontext erfasst. Sodann merkt das Gericht an, dass diese Auslegung mit der Datenschutzkonvention übereinstimme und referiert deren Zwecke und Anwendungsbereich.[246] Zu einem völligen Gleichlaufen kam es dabei aber noch nicht, weil die Konvention einerseits allein das Vorliegen eines personenbezogenen Datums ausreichen lässt und der Gerichtshof andererseits an seinen Kriterien aus den Fällen *Leander* und *Friedl* festhalten wollte.[247]

---

[242] EKMR Entscheidung vom 14.1.1998, *Herbecq ./. Belgien*, App. Nr. 32200/96 und 32201/96, DR 92, 97.

[243] *Siemen*, Grundrecht, S. 109 f., sieht insbesondere in der *Herbecq*-Entscheidung einen Rückschritt zum Inhaltskriterium.

[244] EGMR Urteil vom 16.2.2000, *Amann ./. Schweiz*, App. Nr. 27798/95.

[245] Vgl. auch *Siemen*, Grundrecht, S. 110 f.

[246] EGMR Urteil vom 16.2.2000, *Amann ./. Schweiz*, App. Nr. 27798/95, [65]; *Siemen*, Grundrecht, S. 110 ff.

[247] *Siemen*, Grundrecht, S. 112, sieht in dem Verweis auf die Konvention keine inhaltliche Übernahme der in ihr enthaltenen Definitionen.

Weiterhin zeigt sich die zunehmende Flexibilisierung an dem in der Rechtsprechung des EGMR erstmals vorgenommenen Verweis auf die Datenschutzkonvention im Urteilstext in der Entscheidung *Z gegen Finnland*, die sogleich eingehender zu untersuchen ist.[248] Bestätigt wird diese Flexibilisierung in der Entscheidung *L.L. gegen Frankreich*: In diesem im Zusammenhang mit Medizindaten ergangenen Urteil nennt das Gericht den Bezug zum Privatleben zwar noch, verweist dann jedoch ohne weitere Erörterung auf die Datenschutzkonvention.[249]

### 3. Systematische Erhebung und Informationspermanenz

An die *Amann*-Entscheidung schloss sich eine Reihe datenschutzrechtlicher Urteile des EGMR an, die das Risiko der Permanenz erhobener Informationen veranschaulichen und dabei das systematische Zusammentragen von Informationen als eigenständiges Risikomerkmal herausbilden. Die Entscheidungen *Rotaru gegen Rumänien*,[250] *Sidabras gegen Litauen*,[251] *Turek gegen Slowakei*[252] und *Haralambie gegen Rumänien*[253] betreffen die Verwendung von Geheimdienstinformationen.

Diese Informationen wurden noch unter den vormaligen sowjetischen Regierungen der genannten osteuropäischen Staaten zusammengetragen. Die Nachfolgestaaten verwendeten die teilweise über 50 Jahre alten Informationen in unterschiedlichen Zusammenhängen. Die alten Informationen werfen Fragen in verschiedenen Kontexten auf, so etwa bei Entschädigungs- und Rückübereignungsfragen mit Bezug zu politischer Verfolgung *(Haralambie)*, bei der Löschung fehlerhaft gespeicherter Informationen zu nationalsozialistischen Bestrebungen *(Rotaru)* oder bei Lustrationsverfahren[254] *(Sidabras, Turek)*. Beachtlich ist der an diesen Geheimdienst-Entscheidungen entwickelte Schutz vor systematischer Erhebung von Informationen. Dieses Kriterium wurde im Fall *Rotaru* als neues Merkmal für die Eröffnung des Anwendungsbereichs von Art. 8 EMRK eingeführt. Informationen, selbst wenn diese öffentlich sind („public information"), können in den Anwendungsbereich fallen, soweit sie systematisch gesammelt und in Dateien der Behör-

---

248 EGMR Urteil vom 25.2.1995, *Z. ./. Finnland*, App. Nr. 22009/93, [95]; vgl. *Siemen*, Grundrecht, S. 100.

249 EGMR Entscheidung vom 10.10.2006, *L.L. ./. Frankreich*, App. Nr. 7508/02, [32].

250 EGMR Urteil vom 4.5.2000, *Rotaru ./. Rumänien*, App. Nr. 28341/95.

251 EGMR Urteil vom 27.10.2004 (final), *Sidabras und Dziautas ./. Litauen*, App. Nr. 55480/00 und 59330/00.

252 EGMR Urteil vom 13.9.2006 (final), *Turek ./. Slowakei*, App. Nr. 57986/00.

253 EGMR Entscheidung vom 27.1.2010 (final), *Haralambie ./. Rumänien*, App. Nr. 21737/03.

254 Der Begriff „Lustration" bezeichnete in der römischen Religion die feierliche kultische Reinigung und wird heute für die Entfernung politisch vorbelasteter Staatsbediensteter nach Systemwechseln verwendet, vgl. http://de.wikipedia.org/wiki/Lustration [Stand: 28.3.2014].

den gespeichert werden.[255] Dies habe erst recht zu gelten, wenn sich die Informationen auf die weit zurückliegende Vergangenheit des Betroffenen beziehen.[256] Das Urteil nimmt damit zugleich zu dem Risiko der Informationspermanenz Stellung. Einmal erhobene und gespeicherte Informationen können auch nach langen Zeiträumen (im Fall *Rotaru* waren es über 50 Jahre) erneut Bedeutung erlangen und verwendet werden. Dabei liegt die Fehleranfälligkeit aufgrund des hohen Alters auf der Hand; hiergegen richten sich Löschungs- und Berichtigungspflichten.[257]

*a) Exkurs: Informationsverjährung als Rechtsinstitut*

Hinzu kommt jedoch der aus der Verjährungsdogmatik bekannte Gedanke des Rechtsfriedens. Aufschlussreich ist in diesem Zusammenhang die Begründung des zivilrechtlichen Rechtsinstituts der Verjährung in den Motiven des BGB: Dort heißt es, dass der Verpflichtete nicht mit veralteten Ansprüchen behelligt werden soll, die in der Regel „innerlich unbegründet oder bereits erledigt" sind. Gewisse tatsächliche Zustände, die längere Zeit unangefochten bestanden haben, sollen im Interesse von Rechtsfrieden und Rechtssicherheit als bestehend anerkannt werden.[258] Auch die strafrechtliche Verjährung basiert auf dem Gedanken des Rechtsfriedens. Der Zeitablauf hat das durch die Tat erschütterte Rechtsgefühl der Allgemeinheit beruhigt, ein Prozess ist dann aus spezialpräventiven Gründen vielfach nicht mehr erforderlich.[259]

Dieses allgemeine Rechtsprinzip lässt sich auch auf den Kontext des Informationsrechts übertragen. Sofern die Informationserhebung lange zurückliegt, kann es – ähnlich wie im Zivilrecht – geboten sein, die Verjährung anzunehmen, die dann konsequenter Weise „Informationsverjährung" heißen müsste. Aufgrund der Eigenart der Kategorie „Information",[260] kann diese Verjährung nicht ein absolutes Verarbeitungsverbot begründen, womöglich jedoch dem Betroffenen ein Gegenrecht einräumen, das sich gegen Entscheidungen richtet, die auf der verjährten Information basieren und daran nachteilige Wirkungen für den Betroffenen knüpfen.

Exemplarisch für die Folgen derartiger Verwendungen sind die Ausführungen des Gerichtshofs im Fall *Sidabras*: Informationen über die vergangene Zusammenarbeit mit dem sowjetischen Geheimdienst beeinträchtigten nicht nur die Reputation der Antragsteller, sondern darüber hinaus ihre Möglichkeit private oder beruf-

---

255 *Siemen*, Grundrecht, S. 112 sowie 123 ff.

256 EGMR Urteil vom 4.5.2000, *Rotaru ./. Rumänien*, App. Nr. 28341/95, [43-44].

257 Hinsichtlich der Löschungsverpflichtung vgl. ebd., [57, 60].

258 MüKo-*von Feldmann*, § 194 Rn. 6.

259 Vgl. *Roxin*, AT I, § 23 Rn. 56.

260 Zum Informationsbegriff vgl. *Sieber*, NJW 1989, 2569 ff.

liche Beziehungen zu anderen Menschen aufzunehmen.[261] Das Gericht vermied zwar eine eingehendere Prüfung von Art. 8 Abs. 1 EMRK, weil es bereits eine Verletzung von Art. 14 EMRK i.V.m. Art. 8 EMRK (Diskriminierungsverbot) bejahte.[262] Die Erfassung systematisch gespeicherter, vor langer Zeit erhobener Informationen in Polizeiregistern wurde jedoch schließlich in der Entscheidung *Segerstedt-Wiberg u.a. gegen Schweden* unter Verweis auf die Entscheidungen *Amann* und *Rotaru* ohne weitere Erörterung bejaht.[263] Die Entscheidung *Jarnea gegen Rumänien*[264] bejaht den Eingriff, auch wenn dem Betroffenen nicht der vollständige Zugang zu den Informationen eingeräumt wird. In der Entscheidung *Antunes Rocha gegen Portugal*[265] führt der Gerichtshof aus, dass es bei einer systematischen Erhebung für die Frage des Eingriffs auch nicht darauf ankomme, ob die Erhebung dem Antragsteller bekannt war oder – etwa aufgrund einer unklaren Einwilligungserklärung – bekannt sein musste. Die Kenntnis und ggf. Einwilligung sei erst im Rahmen der Rechtfertigung zu untersuchen.[266]

### *b) Zwischenergebnis*

Festzuhalten bleibt somit, dass der Gerichtshof in den dargestellten Entscheidungen zwei Aspekte angeht: zum einen die systematische Erhebung durch den Staat, zum anderen das Risiko der Informationspermanenz. Letzteres gibt Anlass zu Überlegungen hinsichtlich einer „Informationsverjährung" als eigenständiges Rechtsinstitut des Informationsrechts in Anlehnung an die hergebrachten zivil- und strafrechtlichen Verjährungszwecke. Dabei wären Löschungsrechte angesichts der dezentralen Internetkommunikation technisch kaum umsetzbar.[267] Deshalb könnte sich das Rechtsinstitut auch insoweit an der zivilrechtlichen Verjährung orientieren, als die Rechtsfolgen rein innerrechtlich und in Abhängigkeit von der Ausübung des Betroffenen konstruiert werden. Eine so verstandene Informationsverjährung würde dem Einzelnen das Recht geben, Entscheidungen mit Regelungswirkung für ihn abzuwehren, soweit die dafür herangezogenen Informationen derart alt sind, dass ihre Verwendung den Rechtsfrieden gefährden würde. Sicherlich wäre es dann jedoch erforderlich, Ausnahmen und ggf. weitere Voraussetzungen zu entwickeln, da

---

[261] EGMR Urteil vom 27.10.2004 (final), *Sidabras und Dziautas ./. Litauen*, App. Nr. 55480/00 und 59330/00, [49].

[262] Ebd., [63].

[263] EGMR Urteil vom 6.6.2006 (final 6.9.2006), *Segerstedt-Wiberg u.a. ./. Schweden*, App. Nr. 62332/00, [72].

[264] EGMR Entscheidung vom 19.6.2011, *Jarnea ./. Rumänien*, App. Nr. 41838/05.

[265] EGMR Urteil vom 31.5.2005, *Antunes Rocha ./. Portugal*, App. Nr. 64330/01, [62-65].

[266] Ebd., [62-65].

[267] Fragwürdig ist deshalb das neue „Recht auf Vergessen" im Rahmen der Reformpläne zur Datenschutzrichtlinie der EU, dazu siehe unten Teil 2, III.F.2.a).

das Recht an Informationen höchst relativ und abhängig vom jeweiligen Kontext ist.

### 4. Publizitätsschäden und Schamgefühl

Eine Reihe z.T. neuerer Entscheidungen betrifft das Risiko von Publizitätsschäden und insbesondere die Auslösung von Schamgefühl bei Bekanntwerden von Informationen. Dabei wird der Anwendungsbereich des Art. 8 Abs. 1 EMRK entsprechend der *Leander*-Entscheidung weit gefasst, indem die Datenspeicherung ohne weiteren Inhaltsbezug für die Eröffnung des Anwendungsbereichs genügt.[268] In diese Gruppe fallen die Entscheidungen *Adamson gegen Vereinigtes Königreich*, *Gardel, Bouchacourt, M.B. (jeweils gegen Frankreich)* und *Dimitrov-Kazakov gegen Bulgarien*.[269] Diese Fälle hatten die Registrierung von tatsächlichen oder mutmaßlichen Sexualstraftätern zum Gegenstand. In den Entscheidungen wird an verschiedenen Stellen das Risiko von Publizitätsschäden deutlich, die aus der besonderen gesellschaftlichen Verachtung gegenüber Sexualstraftätern resultieren. Im Fall *Adamson* sieht der Gerichtshof jedoch keine Anhaltspunkte für ein besonderes Risiko öffentlicher Demütigung oder Verletzung durch die Registrierungspflicht, da diese lediglich gegenüber der Polizei gelte.[270] In *Gardel* wird die besondere Eingriffstiefe langfristiger Speicherung angesprochen, diese dann jedoch aufgrund der Schwere der Vorwürfe und angesichts gesetzlicher Begrenzung der Verarbeitung und bestehender Verfahrensgarantien als zulässig erachtet.[271] Ebenfalls in den Kontext des Publizitätsschadens ist der Fall *Khelili gegen die Schweiz* einzuordnen: Die Antragstellerin wurde über Jahre hinweg in einem Polizeiregister als Prostituierte geführt, weil eine Visitenkarte mit der Aufschrift: „Gentille, jolie femme fin trentaine attend ami pour prendre un verre de temps en temps ou sortir. Tel. (...)“[272] aufgefunden wurde. Auch nach der Bestätigung durch die Polizeibehörde, dass die Berufsangabe durch „couturière“ (Schneiderin) ersetzt wurde, verblieb die Antragstellerin in anderen Datenbanken der Justizverwaltung immer noch unter dem Eintrag „Prostituierte“. Der Gerichtshof bejahte den Eingriff ohne weitere

---

[268] Vgl. *Siemen*, Grundrecht, S. 121.

[269] EGMR Entscheidung vom 26.1.1999, *Adamson ./. Vereinigtes Königreich*, App. Nr. 42293/98; EGMR Entscheidungen vom 17.12.2009, *Gardel ./. Frankreich*, App. Nr. 16428/05, *Bouchacourt ./. Frankreich*, App. Nr. 5335/06, *M.B. ./. Frankreich*, App. Nr. 22115/06; EGMR Entscheidung vom 20.2.2011, *Dimitrov-Kazakov ./. Bulgarien*, App. Nr. 11379/03.

[270] EGMR Entscheidung vom 26.1.1999, *Adamson ./. Vereinigtes Königreich*, App. Nr. 42293/98, [2].

[271] EGMR Entscheidungen vom 17.12.2009, *Gardel ./. Frankreich*, App. Nr. 16428/05, [67–71], *Bouchacourt ./. Frankreich*, App. Nr. 5335/06, [67–70], *M.B. ./. Frankreich*, App. Nr. 22115/06, [60–62].

[272] „Liebe, hübsche Frau Ende dreißig sucht Freund, um ab und zu ein Glas zu trinken oder auszugehen, Tel. (…).“

Erörterung.[273] Auch hier ist das Auslösen eines Schamgefühls aufgrund der gesellschaftlichen Ablehnung des Prostitutionsgewerbes als Risiko festzuhalten. Die Auslösung von Schamgefühl ist zudem als Risiko der unter 2. und 5. thematisierten Entscheidungen zu Medizindaten einschlägig.

Die Entscheidung *Casuneanu gegen Rumänien*[274] betrifft neben dem Risiko von Publizitätsschäden durch Reputationsverletzungen auch die strafrechtliche Unschuldsvermutung: In der Entscheidung waren Informationen aus einer Telefonüberwachung an die Presse gelangt, noch bevor diese nach rumänischem Strafprozessrecht ohnehin öffentlich wurden. Der Gerichtshof bejahte unter Verweis auf die zu diesem Zeitpunkt fortbestehende Vertraulichkeitserwartung einen Eingriff und führte aus, es sei Sache der Staaten, das Verfahren derart zu organisieren bzw. das Personal so zu schulen, dass ein effektiver Schutz der Reputation erfolge.[275]

### 5. Sekundäreffekte enttäuschter Vertraulichkeitserwartungen

Der Fall *Halford gegen das Vereinigte Königreich*[276] verdeutlicht einen neuen Ansatz zur Bestimmung des Schutzguts. Die Entscheidung betraf die Überwachung des dienstlichen und privaten Telefons im Büro einer britischen Polizistin sowie des Privattelefons in ihrer Wohnung. Die Polizistin hatte sich wegen unterstellter Diskriminierung in einem Bewerbungsverfahren bei der zuständigen Stelle beschwert und vermutete, dass die Überwachungsmaßnahmen – obwohl sie offiziell mit Dienstvergehen begründet wurden – in Wirklichkeit auf das von ihr verfolgte Diskriminierungsverfahren zurückgingen. Hinsichtlich des Büroanschlusses war fraglich, inwieweit der Öffentlichkeitsbezug eines Büroraums den Schutz von Art. 8 Abs. 1 EMRK entfallen lassen könnte. Die Regierung argumentierte mit dem Fehlen einer berechtigten Vertraulichkeitserwartung („reasonable expectation of privacy"). Diese Argumentationsfigur entstammt der amerikanischen Rechtsprechung zum 4. Zusatzartikel der US-Verfassung. Sie besagt, dass öffentlich zugängliche Räume dann vom Vertraulichkeitsschutz der Vorschrift erfasst sind, wenn eine Person ihre subjektive Vertraulichkeitserwartung nach außen kenntlich gemacht hat und wenn diese subjektive Erwartung aus Sicht der Gesellschaft als „vernünftig" anzuerkennen ist.[277] Der EGMR macht sich diese Argumentation im Rahmen des Schutzbereichs zu eigen und führt aus, dass die Polizistin ein eigenes Büro nutzte und einer der beiden Apparate speziell für ihre Privatgespräche bestimmt war. Weiterhin wurde ihr bestätigt, dass sie ihre beiden Büro-Telefone für

---

273 EGMR Entscheidung vom 18.10.2011, *Khelili ./. Schweiz*, App. Nr. 16188/07, [56].

274 EGMR Entscheidung vom 16.4.2013, *Casuneanu ./. Rumänien*, App. Nr. 22018/10.

275 Ebd., [80–87].

276 EGMR Urteil vom 25.6.1997, *Halford ./. Vereinigtes Königreich*, App. Nr. 20605/92.

277 Concurring Opinion von Justice *Harlan*, US Supreme Court, Urteil vom 18.12.1967, *Katz v. U.S.,* 389 U.S. 347, 361 (1967).

das Diskriminierungsverfahren nutzen könne. Eine berechtigte Vertraulichkeitserwartung habe deshalb bestanden.[278] Der Gerichtshof bejahte die Anwendung von Art. 8 Abs. 1 EMRK und äußerte sich anschließend in der Rechtfertigungsprüfung zu den Risiken geheimer Überwachungsmaßnahmen: Das Recht der Mitgliedstaaten müsse einen Schutz gegen willkürliche Eingriffe in Art. 8 Abs. 1 EMRK aufgrund des Mangels an öffentlicher Überprüfung und aufgrund des Risikos von Machtmissbrauch gewähren.[279]

Der Fall zeigt zunächst, dass der Gedanke objektiv zu bestimmender Vertraulichkeitssphären dort Schwierigkeiten bereitet, wo „Vertraulichkeitsenklaven" in öffentlichen Bereichen bestehen. Für diese Fälle kann auf die Konzeption einer Vertraulichkeitserwartung zurückgegriffen werden. Der Vertrauensschutz dient insoweit der Flexibilisierung durch Abstraktion. Eine Verletzung der Vertraulichkeitserwartung führt zu einer Enttäuschung, was sich auf das künftige Verhalten auswirken kann. Der Gerichtshof übernimmt diese Schutzgutkonzeption jedoch nicht auch bei dem Merkmal „in Übereinstimmung mit dem Gesetz" („in accordance with the law"). Vielmehr bestärkt er dort erneut die Prinzipien aus *Klass*, wobei er aufgrund der Rüge einer konkreten Überwachung den Eingriff nicht in der abstrakten Überwachungsbedrohung durch Existenz von Überwachungsgesetzen sehen will, sondern eine angemessene Wahrscheinlichkeit („reasonable likelihood") der Durchführung im Einzelfall verlangt. Diese habe *Halford* nicht vorgetragen.[280] Die Argumentation ist wenig überzeugend, da nicht ersichtlich ist, weshalb die allein auf den Einzelfall beschränkte Rüge die Eingriffsqualität der Gesetzgebung entfallen lassen soll. Konsistenter wäre insoweit auch hier der Übergang zum Schutzgut der Vertraulichkeitserwartung, wie von der Regierung angeführt. Dieses hätte eine flexible, am Betroffenen ausgerichtete Abstufung der Eingriffsqualität ermöglicht.

Das Risiko enttäuschter Vertraulichkeitserwartungen wird dann jedoch in zwei Leitentscheidungen des EGMR aus dem Jahr 1997 aufgegriffen. Die Urteile *Z. gegen Finnland und M.S. gegen Schweden* hatten die Verwendung von Medizindaten im Rahmen gerichtlicher Verfahren zum Gegenstand.[281] Die problematischen Folgen von Vertrauensverlust treten dort als spezifisches, mit der Preisgabe medizinischer Daten verbundenes Risiko hervor. In *Z. gegen Finnland* handelte es sich um die besonders sensible Information über eine HIV-Infektion der Beschwerdeführerin. Der Gerichtshof führte aus, dass der Datenschutz von fundamentaler Bedeutung für das Recht auf Achtung des Privatlebens sei und im Fall von Medizindaten ein besonderes Risikopotenzial hinsichtlich des Vertrauens in das Gesundheitssys-

---

[278] EGMR Urteil vom 25.6.1997, *Halford ./. Vereinigtes Königreich*, App. Nr. 20605/92, [45].

[279] Ebd., [49].

[280] Ebd., [56 f.].

[281] Vgl. *Siemen*, Grundrecht, S. 98 f.

tem bestehe. Eindringlich beschreibt er die Konsequenzen von Vertrauensverlust, die in einer Abschreckung der Kranken von der Preisgabe intimer Informationen bei der Inanspruchnahme medizinischer Hilfe liegt. Das hieraus folgende Informationsdefizit der Ärzte kann dann zu einer unzureichenden Behandlung führen. Im schlimmsten Fall nehmen die Kranken überhaupt keine ärztliche Hilfe an, weil sie fürchten, dass dabei anfallende intime Informationen an die Öffentlichkeit gelangen. Dies kann nicht nur zu Schäden an der Gesundheit der Betroffenen, sondern im Fall übertragbarer Krankheiten auch zu einer Verringerung der Volksgesundheit führen.[282]

Das so umrissene Risiko besteht bei näherer Betrachtung aus mehreren Komponenten. Zum einen liegt der Schaden in der Auslösung von Schamgefühl als solchem. Andererseits besteht bei Gesundheitsdaten das Risiko der Kontextinfiltration,[283] soweit beispielsweise Daten über psychiatrische Behandlungen oder Suchterkrankungen im Berufsleben bekannt werden. Das spezifisch mit der Vertrauenskonzeption aufgenommene Risiko liegt jedoch nicht in diesen unmittelbaren Schäden, sondern – wie der Vergleich mit der Verbrauchervertrauenskonzeption des APEC Framework[284] zeigt – in den Auswirkungen auf das Verhalten der Betroffenen. Die Sekundäreffekte von Vertrauensverlust können insoweit sowohl in Konsumrückgang als auch in der Nichtinanspruchnahme medizinischer Dienstleistungen liegen. Verbindet man die Argumentation mit dem in der Entscheidung *Klass* entwickelten Bezug zum Demokratieprinzip, so weist dies auf das Risiko von Auswirkungen auf das Wahlverhalten hin, was noch näher zu untersuchen sein wird.[285]

### 6. Fortbildung der Vertraulichkeitserwartung

Die unter 5. besprochene, auf Vertraulichkeitserwartungen basierende Schutzgutskonzeption wird in einer Reihe daran anschließender Entscheidungen aufgegriffen und fortgebildet. Dabei kommt es insbesondere zu einer Zusammenführung des Risikos systematischer Erhebungen öffentlicher Informationen und weiterer Kriterien aus der älteren Rechtsprechung mit der Vertraulichkeitserwartung.

Das Urteil *P.G. und J.H. gegen das Vereinigte Königreich* steht am Beginn dieser Entscheidungsreihe.[286] Der Fall hatte die verdeckte Aufzeichnung einer Stimmprobe auf einer Polizeiwache zum Gegenstand. Ein Polizist verwickelte den inhaf-

---

[282] EGMR Urteil vom 25.2.1995, *Z. ./. Finnland*, App. Nr. 22009/93, [95] sowie bestätigt in EGMR Urteil vom 27.8.1997, *M.S. ./. Schweden*, App. Nr. 20837/92, [41].

[283] Siehe oben II.B.

[284] Siehe oben II.F.2.

[285] Siehe unten Teil 4, II.A.2.b).

[286] EGMR Urteil vom 25.9.2001, *P.G. u. J.H. ./. Vereinigtes Königreich*, App. Nr. 44787/98.

tierten und in Verhören schweigenden Verdächtigen in ein Gespräch über Fußball, um so an seine Stimmprobe zu gelangen. Die Stimmprobe wurde verwendet, um Gesprächsinhalte aus einer Tonbandaufzeichnung einer abgehörten Wohnung zuzuordnen. Das Gericht bestärkt im Urteil seine Auffassung, wonach auch im öffentlichen Bereich eines Polizeireviers („public context"), eine Privatheitsenklave bestehen könne („zone of interaction […] which may fall within the scope of ‚private life'").[287] Sodann rekurriert der Gerichtshof auf die Vertraulichkeitserwartung, wobei das Kriterium der wissentlichen oder absichtlichen Aktivität in der Öffentlichkeit nicht allein ausschlaggebend sei. Vielmehr könne auch in diesen Fällen die systematische oder permanente Aufzeichnung mit technischen Mitteln einen Eingriff in Art. 8 Abs. 1 EMRK darstellen.[288] Insoweit führt der Gerichtshof den Schutz berechtigter Vertraulichkeitserwartungen mit dem Aspekt der systematischen oder permanenten Aufzeichnung, wie im Fall *Rotaru* entwickelt, zusammen. Im Umkehrschluss weist er auf die Vergleichbarkeit mit der Speicherung von Bilddateien in der *Friedl*-Entscheidung hin. Dort war gerade der Umstand, dass die Bilder nicht zur Identifikation verwendet wurden für die Ablehnung des Eingriffs maßgeblich. Weiter bezieht sich das Gericht auf die Fälle „gewöhnlicher" Telefonüberwachungen und hält es wegen Vergleichbarkeit für „nicht ausgeschlossen", dass auch die Stimmidentifikation in den Schutzbereich des Art. 8 Abs. 1 EMRK fällt.[289] Eine weitere Besonderheit des Falls liegt im Verzicht auf jeglichen Bezug zum Inhalt des Gesprächs. Statt dieses überkommene Kriterium heranzuziehen, verweist der Gerichtshof wie in der *Amann*-Entscheidung auf Art. 2 der Datenschutzkonvention. Die Stimmprobe wird damit als personenbezogenes Datum betrachtet. Darin ist eine weitere Annäherung an das Schutzkonzept der Datenschutzkonvention zu sehen.[290]

Die Referenz auf die Vertraulichkeitserwartung wird in der Entscheidung *Peck gegen Vereinigtes Königreich* fortgebildet.[291] In dem Fall wurde das Verhalten von *Peck* nach einem nächtlichen Suizidversuch auf einer verlassenen Straße von einer Überwachungskamera aufgezeichnet und anschließend an die Medien weitergeleitet. Der Gerichtshof bejahte die Anwendbarkeit von Art. 8 Abs. 1 EMRK und verwies auf die Entscheidung *P.G.* und *J.H.* Angesichts der Umstände war es unschädlich, dass es sich um eine öffentliche Straße handelte. Den maßgeblichen Unterschied zu dem zuvor im Fall *Herbercq* gebildeten Argument der „hypothetischen Ersatzsichtbarkeit", d.h. der potenziellen Sichtbarkeit für jedermann bei Überwachungen des öffentlichen Raums, sieht das Gericht in der Speicherung und Weiter-

---

287 Ebd., [56].

288 Ebd., [57].

289 Ebd., [58 f.].

290 Vgl. zum Ganzen auch *Siemen*, Grundrecht, S. 116, die den Verzicht auf das Bezugskriterium herausstellt.

291 Vgl. ebd., S. 117 f.

gabe an die Medien.[292] Zur Abgrenzung wird das Kriterium der Vorhersehbarkeit bezüglich der Veröffentlichungsweise entwickelt.[293] Hier wird also das Risiko von Publizitätsschäden und Schamgefühl mit dem Konzept der Vertraulichkeitserwartung zusammengeführt und diese mittels des Kriteriums der Vorhersehbarkeit begrenzt.

Die Vertraulichkeitskonzeption wird sodann in einer Reihe von Entscheidungen aus den Jahren 2003 und 2007 aufgegriffen. So hatte die Entscheidung *Perry gegen Vereinigtes Königreich*[294] die heimliche Erstellung einer Videoaufnahme eines, die Mitwirkung an einer Gegenüberstellung verweigernden, Beschuldigten zum Zwecke der Identifizierung in einem Strafverfahren zum Gegenstand. *Perry* wurde in einer Polizeistation mit einer speziell für diesen Zweck modifizierten Überwachungskamera aufgenommen. Der Gerichtshof verweist wieder auf die Entscheidungen *Herbercq* sowie *P.G.* und *J.H.*: Allein das Beobachten öffentlicher Orte mithilfe von Überwachungskameras soll danach zwar noch keine Beeinträchtigung von Art. 8 Abs. 1 EMRK darstellen; etwas anderes gilt jedoch, wenn die Aufnahme gespeichert wird bzw. wenn weitere Umstände hinzukommen, die eine vernünftige Vertraulichkeitserwartung („reasonable expectation of privacy") begründen.[295] Weil *Perry* der Gegenüberstellung widersprochen hatte und nichts von der speziell für ihn umgestellten Videokamera wusste, bestand nach Ansicht des Gerichts eine solche Vertraulichkeitserwartung. Nichts anderes sei aus dem bloßen Identifizierungszweck zu folgern, da anders als in der *Lupker*-Entscheidung, das Bildmaterial nicht freiwillig abgegeben wurde.[296] Die Vertrauenskonzeption kann also durch Einwilligung begrenzt werden.

Ausdrücklich hervorgehoben wird die Bedeutung des „reasonable expectation of privacy test" auch im Fall *Peev gegen Bulgarien*.[297] In diesem Fall wurde das Büro eines Justizangestellten durchsucht. Trotz der Belegenheit der Räumlichkeiten konnte der Angestellte sich zumindest hinsichtlich seines Schreibtischs und seiner Ablage auf Art. 8 Abs. 1 EMRK berufen, weil er mit der Verwahrung privater Gegenstände eine Vertraulichkeitserwartung bekundet hatte und diese mangels entgegenstehender Weisungen auch als rechtlich schützenswert erachtet wurde. Der Gerichtshof spricht ausdrücklich von dem „reasonable expectation of privacy *test*"

---

[292] EGMR, Urteil vom 28.1.2003 (final 28.4.2003), *Peck ./. Vereinigtes Königreich*, App. Nr. 44647/98, [62].

[293] Ebd., [60–62].

[294] EGMR Urteil vom 17.7.2003, *Perry ./. Vereinigtes Königreich*, App. Nr. 63737/00; Siemen, Grundrecht, S. 118 ff.

[295] EGMR Urteil vom 17.7.2003, *Perry ./. Vereinigtes Königreich*, App. Nr. 63737/00, [37 f.].

[296] Ebd., [40 ff.]. Wobei auch im *Lupker*-Fall angesichts der Zweckänderung keine wirksame Einwilligung vorlag, siehe oben IV.B.2., Anm. 233.

[297] EGMR Urteil vom 26.7.2007, *Peev ./. Bulgarien*, App. Nr. 64209/01.

und erkennt damit das aus dem US-amerikanischen Recht stammende Institut[298] als solches an.[299]

In den Entscheidungen *Uzun gegen Deutschland* und *Shimovolos gegen Russland*[300] wird die Vertraulichkeitskonzeption bei der Erstellung von Bewegungsprofilen thematisiert. Im Fall *Uzun* wurde ein GPS-Sender in das Auto eines Komplizen eingebaut, um die Bewegungen von *Uzun* zu rekonstruieren. Bei der Prüfung des Anwendungsbereichs kombiniert das Gericht die Frage nach der berechtigten Vertraulichkeitserwartung mit den Konzepten der „hypothetischen Ersatzsichtbarkeit" aus *Herbercq* als Einschränkung und mit dem Kriterium systematisch-permanenter Speicherung aus *Rotaru* als Erweiterung.[301] Weitere zu berücksichtigende Kriterien seien die Zusammenführung von Daten über einen Betroffenen („compilation of data on a particular individual"), die Verarbeitung personenbezogener Daten sowie die Frage, ob das Material in einer unvorhersehbaren Weise und in unvorhersehbaren Umfang veröffentlicht wurde („publication of the material concerned in a manner or degree beyond that normally foreseeable"). Die genaue Einordnung dieses Abwägungsmaterials wird hingegen nicht erläutert.[302]

Bei der Übertragung der Prinzipien auf den konkreten Fall bejaht der Gerichtshof den Anwendungsbereich mittels des Kompilationsmerkmals und des Kriteriums der systematisch-permanenten Sammlung und Speicherung. Dabei sei das Erstellen von Bewegungsprofilen jedoch abzugrenzen von anderen Überwachungsmethoden, die einen größeren Einblick in Verhalten, Meinungen und Gefühle erlaubten. Zwar wird der Eingriff bejaht,[303] allerdings werden die Anforderungen an die Rechtfertigung gegenüber Telekommunikationsüberwachungen reduziert.[304] Die Möglichkeit, an die Positionsdaten weitere Ermittlungsmaßnahmen anzuschließen, wird in dem Kriterium systematisch-permanente Erhebung herausgestellt.[305] Die mit dem Bewegungsprofil ermöglichten Anschlussmaßnahmen werden damit als eigenes Risiko für nachfolgende Eingriffe verstanden. Im Rahmen der qualitativen Anforderungen an das einschränkende Gesetz fordert der Gerichtshof Vorkehrungen gegenüber unkoordinierten Ermittlungstätigkeiten durch verschiedene Behörden, die eine Totalüberwachung („total surveillance") verhindern sollen.[306] Dieses Risiko wird auch in der Verhältnismäßigkeitsprüfung aufgegriffen. Dort wird insbesonde-

---

298 Siehe unten IV.B.5.

299 EGMR Urteil vom 26.7.2007, *Peev ./. Bulgarien*, App. Nr. 64209/01, [39].

300 EGMR Entscheidung vom 2.9.2010, *Uzun ./. Deutschland*, App. Nr. 35623/05; EGMR Entscheidung vom 28.11.2011, *Shimovolos ./. Russland*, App. Nr. 30194/09.

301 EGMR Entscheidung vom 2.9.2010, *Uzun ./. Deutschland*, App. Nr. 35623/05, [44].

302 Ebd., [45].

303 Ebd., [49–52].

304 Ebd., [66, 72].

305 Ebd., [51].

306 Ebd., [73].

re die Kombination aus unterschiedlichen qualitativen Überwachungsmaßnahmen (optisch, akustisch, Ortung) in Verbindung mit der Anordnung derselben Überwachungsmaßnahmen durch zwei Behörden (Bundeskriminalamt und Verfassungsschutzbehörde) als Kriterium für die besondere Eingriffstiefe angeführt. Insbesondere werde dadurch der Kreis der Personen, die Zugang zu den Daten haben, erhöht. Aufgrund der zeitlichen Kürze der GPS-Überwachung und der schwerwiegenden Gründe für die Anordnung (es ging um terroristische Anschläge durch eine Nachfolgeorganisation der RAF) sah der Gerichtshof die Maßnahme gleichwohl als verhältnismäßig an.[307] Aufgegriffen wurde damit die – vom Beschwerdeführer auch im Verfahren vor dem BVerfG gerügte – „Überwachungskumulation". Das durch Totalüberwachung ausgelöste Risiko stimmt mit dem bereits erörterten Überwachungsdruck überein. Die „Überwachungsdoppelbefugnis" von BKA und Bundesverfassungsschutz stellt einen Teilaspekt dieses Risikos dar, in dem eine „Überwachungskumulation" erfolgt.

Die Entscheidung *Shimovolos* betrifft ebenfalls die Erstellung von Bewegungsprofilen, enthält jedoch keine weitergehende Auseinandersetzung mit Vertraulichkeitserwartung und einschlägigen Risiken. Gegenstand war die Registrierung eines Menschenrechtsaktivisten in einer „Überwachungsdatenbank" für Extremisten. Infolge der Registrierung wurde der Kauf von Flug- und Bahnkarten dokumentiert. Örtliche Polizeibehörden führten daraufhin zahlreiche Kontrollmaßnahmen durch, als der Antragsteller zu einer Protestveranstaltung im Rahmen eines EU-Russland-Summits reiste. Der Gerichtshof bejaht den Eingriff ohne weitere Erörterung, aber unter Bezug auf die Entscheidung *Uzun*.[308] Obwohl die Ausführungen des Gerichtshofs wenig Substanz enthalten, verdeutlicht der Sachverhalt das Risiko einer möglichen Beeinträchtigung politischen Engagements durch Überwachungsmaßnahmen.

### 7. Verhältnis zu Korrespondenz- und Wohnungsschutz

Mit der zunehmenden Ablösung des Rechts auf Achtung des Privatlebens von dem Kriterium des inhaltlichen Bezugs stellte sich verstärkt die Frage nach dem Verhältnis der Privatlebensvariante zu der ebenfalls von Art. 8 Abs. 1 EMRK erfassten Korrespondenz und der Wohnung. In Zweifelsfällen lässt der Gerichtshof eine Abgrenzung zwar dahinstehen; es ist jedoch nicht ausgeschlossen, dass die Untersuchung einschlägiger Entscheidungen unter dem Aspekt des Verhältnisses der Schutzbereichsvarianten zueinander Rückschlüsse auf das Schutzgut erlaubt.

In zahlreichen Entscheidungen mit Telekommunikationsbezug hält der Gerichtshof das Recht auf Privatleben *und* Korrespondenz für einschlägig und differenziert

---

307 Ebd., [79 f.].

308 EGMR Entscheidung vom 28.11.2011, *Shimovolos ./. Russland*, App. Nr. 30194/09, [65 f.].

damit inhaltlich nicht zwischen den beiden Varianten. So etwa in *Klass gegen Deutschland*,[309] *Malone gegen Vereinigtes Königreich*,[310] *Halford gegen Vereinigtes Königreich*,[311] *Lambert gegen Frankreich*,[312] *Amann gegen Schweiz*,[313] *Taylor-Sabori gegen Vereinigtes Königreich*[314] *und Iordachi u.a. gegen Moldau.*[315] Die Entscheidung *Copland gegen Vereinigtes Königreich*[316] lässt sich zunächst in diese Reihe einordnen. Privatleben und Korrespondenz werden gemeinsam behandelt. Der Fall geht jedoch darüber hinaus, weil darin auch die Überwachung des E-Mail-Verkehrs und des Surfverhaltens ausdrücklich in den Schutz des Privatlebens und der Korrespondenz miteinbezogen werden.[317] Die Entscheidung betraf die Speicherung von E-Mail- und Telefonverbindungsdaten im Arbeitskontext. Begründet wurde der Schutz wiederum mit der vernünftigen Vertraulichkeitserwartung („reasonable expectation as to the privacy"), die auf den E-Mail- und Internetverkehr ausgedehnt wurde.[318] Der Gerichtshof trennt in der Entscheidung zwischen Anwendungsbereich von Art. 8 Abs. 1 EMRK und Eingriff. Den Eingriff bejaht er ohne Weiteres aufgrund der Erhebung und Speicherung der Informationen.[319]

Während die Entscheidung *Petri Sallinen gegen Finnland*[320] in Bezug auf eine Festplattenbeschlagnahme die Wohnungsvariante mit der Korrespondenz gemeinsam und ohne nähere Ausführung zum Verhältnis der verschiedenen Varianten prüft, präzisierte der Gerichtshof dieses Verhältnis in der Entscheidung *Wieser und Bicos Beteiligungen GmbH gegen Österreich*.[321] Dieser Fall betrifft die Speicherung elektronischer Daten im Rahmen einer Hausdurchsuchung. Der Gerichtshof bejahte die Anwendbarkeit der Korrespondenzvariante von Art. 8 Abs. 1 EMRK und hielt es deshalb für nicht erforderlich, zu prüfen, inwieweit auch die Privat-

---

309 EGMR Urteil vom 6.9.1978, *Klass ./. Deutschland*, App. Nr. 5029/71, [41].

310 EGMR Urteil vom 2.8.1984, *Malone ./. Vereinigtes Königreich*, App. Nr. 8691/79.

311 EGMR Urteil vom 25.6.1997, *Halford ./. Vereinigtes Königreich*, App. Nr. 20605/92, [42–44].

312 EGMR Entscheidung vom 24.8.1998, *Lambert ./. Frankreich*, App. Nr. 872/1084. In dieser Entscheidung wird der Eingriff auch gegenüber dem Gesprächspartner des überwachten Anschlusses bejaht.

313 EGMR Urteil vom 16.2.2000, *Amann ./. Schweiz*, App. Nr. 27798/95, [44].

314 EGMR Entscheidung vom 22.10.2002, *Taylor-Sabori ./. Vereinigtes Königreich*, App. Nr. 47114/99, [18].

315 EGMR Entscheidung vom 10.2.2009, *Iordachi u.a. ./. Moldau*, App. Nr. 25198/02.

316 EGMR Entscheidung vom 3.4.2007, *Copland ./. Vereinigtes Königreich*, App. Nr. 62617/00.

317 Ebd., [41].

318 Ebd., [42].

319 Ebd., [44].

320 EGMR Entscheidung vom 27.9.2005, *Petri Sallinen u.a. ./. Finnland*, App. Nr. 50882/99, [70 ff.].

321 EGMR Entscheidung vom 16.10.2007, *Wieser und Bicos Beteiligungen GmbH ./. Österreich*, App. Nr. 74336/01.

lebensvariante einschlägig war.[322] Die hierdurch angedeutete Spezialität des Korrespondenzkriteriums wird jedoch in der Entscheidung *Van Vondel gegen Niederlande*[323] wieder infrage gestellt. Gegenstand war der Mitschnitt eines Telefonats durch einen V-Mann. Der Gerichtshof bejahte den Eingriff in das Privatleben und/oder die Korrespondenz: „interference with the applicant's private life and/or correspondence".[324] In der Entscheidung *Robathin gegen Österreich*,[325] die ebenfalls die Durchsuchung und Beschlagnahme von Daten zum Gegenstand hatte, hält der Gerichtshof wiederum nur die Korrespondenzvariante für einschlägig und verweist auf die Entscheidung *Bicos Beteiligungen GmbH gegen Österreich*.[326] In der Entscheidung *Draksas gegen Litauen* werden beide Varianten angeführt.[327]

Eine einheitliche Linie in Bezug auf die Abgrenzung der Schutzbereichsvarianten ist somit derzeit nicht erkennbar. Hinsichtlich des Schutzguts ist jedoch die Ausdehnung der Vertraulichkeitskonzeption auf E-Mail- und Internetkommunikation festzuhalten.

### 8. Integritäts- und Identitätsschutz

Beginnend mit der Entscheidung *S. und Marper gegen Vereinigtes Königreich*,[328] welche die Erhebung und fortlaufende Speicherung von Zellproben, DNA-Profilen und Fingerabdrücken nach Beendigung von Strafverfahren (Freispruch und Einstellung) zum Gegenstand hatte, zieht der Gerichtshof auch in datenschutzrechtlichen Konstellationen abstraktere, d.h. vom Einzelfall stärker abgehobene, zugleich aber noch individuelle – also nicht etwa kollektive – Schutzgüter heran. Die Entscheidung stellt die Verbindung zwischen allgemein persönlichkeitsrechtlichen Schutzgütern und spezifisch datenschutzrechtlichen Risiken her. In zahlreichen Entscheidungen zu nicht datenschutzrechtlichen Sachverhalten hatte der Gerichtshof bereits zuvor die physische und psychologische Integrität sowie die physische und soziale Identität einer Person als Schutzgut des Persönlichkeitsrechts anerkannt.[329] In der Entscheidung *S. und Marper* werden diese Schutzgüter erst-

---

322 Ebd., [45].

323 EGMR Entscheidung vom 25.10.2007, *Van Vondel ./. Niederlande*, App. Nr. 38258/03.

324 Ebd., [49].

325 EGMR Entscheidung vom 3.7.2012, *Robathin ./. Österreich*, App. Nr. 30457/06, [39].

326 EGMR Entscheidung vom 16.10.2007, *Wieser und Bicos Beteiligungen GmbH ./. Österreich*, App. Nr. 74336/01.

327 EGMR Entscheidung vom 31.7.2012, *Draksas ./. Litauen*, App. Nr. 36662/04, [52].

328 EGMR Entscheidung vom 4.12.2008, *S. u. Marper ./. Vereinigtes Königreich*, App. Nr. 30562/04 und 30566/04.

329 Z.B. EGMR Entscheidung vom 29.4.2002, *Pretty ./. Vereinigtes Königreich*, App. Nr. 2346/02, [61] m.w.N. zu den älteren Entscheidungen; vgl. hierzu auch *Siemen*, Grundrecht, S. 74 f.

mals auch in einem spezifisch datenschutzrechtlichen, die Verarbeitung personenbezogener Daten betreffendem Fall herangezogen. Dabei setzt sich der Gerichtshof in beachtlicher Ausführlichkeit mit den Risiken dieser Informationen auseinander.

Zunächst führt er aus, dass die physische und psychische *Integrität* vom Konzept des Privatlebens (concept of „private life") umfasst wird und deshalb mehrere Aspekte der physischen und psychischen *Identität* einbezieht. Darunter seien nicht nur Elemente wie Geschlechtszugehörigkeit, sexuelle Orientierung und der Name zu verstehen, sondern auch andere Methoden zur Identifikation und Verknüpfung mit Familienbezügen („means of personal identification and of linking to a family"). Dabei zieht der Gerichtshof zunächst den „*Leander*-Grundsatz" heran, wonach bereits die Speicherung von Informationen mit Bezug zum Privatleben einen Eingriff in Art. 8 EMRK darstellen kann. Der Gerichtshof differenziert sodann aber zwischen Zellproben und DNA-Profilen auf der einen Seite sowie Fingerabdrücken auf der anderen.[330] Er bestätigt und erweitert damit einen zuvor bereits in der Entscheidung *Van der Velden gegen die Niederlande*[331] angerissenen Begründungsstrang, demzufolge die systematische Sammlung von Zellproben aufgrund möglicher Nutzungen in der Zukunft, insbesondere angesichts der rapiden Entwicklung der Gen- und Informationstechnologie, den Eingriff begründet. Den Einwand der Regierung, dass zukünftige hypothetische Nutzungen als bloße Spekulation auszuklammern seien, weist der Gerichtshof unter Verweis auf den schnellen Wandel der Technik und damit möglicher neuer Nutzungsweisen zurück. Ergänzend stützt er sich auf die zahlreichen durch Auswertung zellularen Materials zugänglichen Informationen, z.B. über den Gesundheitszustand des Probanden und die Bedeutung auch für Verwandte. Wegen der potenziellen künftigen Nutzung und des Informationsgehalts der Zellproben stelle deshalb schon die Erhebung, nicht erst die spätere Nutzung, einen Eingriff dar.[332] Auch hinsichtlich der aus den Proben gewonnenen DNA-Profile wird ein Eingriff bereits bei deren Erstellung bejaht. Den Grund sieht der Gerichtshof in der möglichen automatischen Auswertung z.B. nach ethnischer Zugehörigkeit oder Verwandtschaftsverhältnissen. Diese Möglichkeit erlaube es den Behörden, weit über die bloße Identifikation hinauszugehen.[333] Die Erhebung der Fingerabdrücke wird unter Verweis auf die Möglichkeit der exakten Identifikation ebenfalls als Eingriff angesehen. Der Gerichtshof bestätigt zwar die unterschiedliche Eingriffsintensität der Erhebung von Zellproben, DNA-Profilen und Fingerabdrücken. Die Notwendigkeit einer diesbezüglichen Differenzierung sieht

---

330 EGMR Entscheidung vom 4.12.2008, *S. u. Marper ./. Vereinigtes Königreich*, App. Nr. 30562/04 u. 30566/04, [66–68].

331 EGMR Entscheidung vom 7.12.2006, *Van der Velden ./. Niederlande*, App. Nr. 29514/05.

332 EGMR Entscheidung vom 4.12.2008, S. u. *Marper ./. Vereinigtes Königreich*, App. Nr. 30562/04 und 30566/04, [69 ff., 73 zum Eingriff].

333 Ebd., [75 ff.].

er jedoch erst auf der Rechtfertigungsebene.[334] Dieses weite Verständnis des Schutzbereichs hält er für vereinbar mit den vorgängigen Entscheidungen *McVeigh*, *Kinnunen*, *Friedl* sowie *P.G. und J.H.*[335]

Der Gerichtshof zieht somit drei Arten von Risiken heran: erstens die Unabsehbarkeit der Verwendung durch technische Entwicklung, zweitens den umfassenden Einblick in die Persönlichkeit des Probanden und drittens die Möglichkeit automatischer Auswertung nach prima facie nicht zugänglichen Informationskategorien wie beispielsweise Verwandtschaftsverhältnissen. Letzteres Risiko entspricht dem bereits oben aus den allgemeinen Regelungskonzeptionen der Datenschutzkonvention abgeleiteten Risiko der Informationsemergenz.[336] Den Risiken liegt nach dieser Konzeption der Schutz der individuellen psychischen Integrität zugrunde. Ein so verstandener Integritätsschutz bedeutet demnach also Schutz auch vor künftigen Verwendungsmöglichkeiten, Schutz vor umfassendem Einblick und Schutz vor massenhaft-automatisierter Auswertung.

Ein weiteres abstrakt-individuelles Risiko spricht der Gerichtshof erst bei der Prüfung der Verhältnismäßigkeit an: Die Speicherung unterschied nicht danach, ob sich ein anfänglicher Verdacht nach Abschluss des Verfahrens erhärtet hat oder nicht. Alle Informationen zu den erhobenen Spuren wurden gemeinsam in einer Datenbank gespeichert. Hierin erkennt das Gericht das Risiko der Stigmatisierung Unschuldiger und knüpft damit – freilich ohne Verweis – an die von Richter *Pettiti* gemachten Ausführungen zur Schuldvermutung aus dem Sondervotum zur Entscheidung *Malone* an.[337] Die angegriffene Speicherpflicht stelle insoweit keinen angemessenen Ausgleich zwischen den widerstreitenden privaten und öffentlichen Interessen her.[338]

Die physische und psychische Integrität als Schutzgut des Art. 8 Abs. 1 EMRK wird erneut in der Entscheidung *Gillberg gegen Schweden* aufgegriffen.[339] Dem Fall lag die Weigerung eines schwedischen Professors zur Herausgabe sensibler Patientendaten aus einer ADHS-Studie zugrunde. Der Professor berief sich auf eine zugunsten der Patienten abgeschlossene Vertraulichkeitsverpflichtung sowie auf ethische Grundsätze. Die Herausgabe sollte zum Zwecke wissenschaftlicher Forschung erfolgen, die Interessenten konnten sich bei ihrer Forderung auf das in Schweden besonders stark ausgeprägte verfassungsrechtliche Recht auf Zugang zu öffentlichen Informationen gem. 2 kap. 1 § TF berufen. Der Professor wurde schließlich wegen Dienstverfehlung, ein in Schweden gem. 20 kap. 1 § BrB straf-

---

334 Ebd., [84 ff.]

335 Ebd., [79–83].

336 Siehe oben II.A.2.d).

337 Siehe oben IV.B.1.a).

338 EGMR Entscheidung vom 4.12.2008, *S. u. Marper ./. Vereinigtes Königreich*, App. Nr. 30562/04 und 30566/04, [122, 125].

339 EGMR Entscheidung vom 3.4.2012, *Gillberg ./. Schweden*, App. Nr. 41723/06.

bares Delikt, verurteilt. Die Große Kammer des EGMR war lediglich mit der Frage befasst, ob durch die Strafverurteilung eine Verletzung von Konventionsrecht vorlag, und konnte sich wegen Verfristung nicht mit den Entscheidungen der schwedischen Verwaltungsgerichte auseinandersetzen, die das Zurückhalten der Informationen als solches geprüft hatten.[340] Der Gerichtshof verweist bei der Prüfung zunächst wieder auf die Erfassung des Schutzguts der physischen und psychischen Integrität und den möglichen Schutz verschiedener Aspekte der physischen und sozialen Identität. Weiterhin rekurriert er auf den persönlichkeitsrechtlichen Gehalt des Art. 8 Abs. 1 EMRK in Form eines Rechts auf persönliche Entwicklung und auf Beziehung zu anderen Menschen. *Gillberg* berief sich darauf, dass schon der mit der Verurteilung einhergehende Reputationsverlust eine Beeinträchtigung des Privatlebens i.S.v. Art. 8 Abs. 1 EMRK darstelle. Hiergegen wendet sich die Große Kammer mit dem Argument, dass die Norm nicht vor Reputationsverlusten schütze, die eine vorhersehbare Konsequenz eigenen Verhaltens darstellen. Aus diesem Grund lehnt sie die Betroffenheit von Art. 8 Abs. 1 EMRK durch Strafurteile grundsätzlich ab, auch wenn mit der Verurteilung persönliche, soziale, psychische und ökonomische Einbußen verbunden sind. Diese seien im Übrigen vom Antragsteller nicht hinreichend konkretisiert worden.[341]

Die Entscheidung verdeutlicht nochmals die abstrakte Fassung der Integritäts- und Identitätsschutzgüter und deren Nähe zur persönlichkeitsrechtlichen Komponente des Art. 8 Abs. 1 EMRK. Weiterhin zeigt das aufgestellte Erfordernis der Spezifikation persönlicher, sozialer, psychischer und ökonomischer Einbußen den Zusammenhang mit der Identifikation konkreter Risiken bzw. Informationsverwendungsfolgen, die den genannten Lebensbereichen zugeordnet werden können. Der Verweis auf vorhersehbare Konsequenzen bestätigt die Eingrenzungsfunktion der Eigenverantwortlichkeit, wie sie auch im Kriterium der Freiwilligkeit bereits zuvor in verschiedenen Entscheidungen[342] hervortrat.

## C. Zwischenergebnis

Art. 8 EMRK benennt den Datenschutz zwar nicht ausdrücklich, doch wurde er bei der Auslegung des Begriffs „Privatleben“ in der Rechtsprechung des EGMR kontinuierlich in einer Vielzahl von Entscheidungen als eigene Schutzdimension konturiert, wobei sich eine differenzierte Prüfungsabfolge herausgebildet hat. Der Privatlebensbegriff wird vom EGMR offen formuliert und kasuistisch konkretisiert. In der Literatur wurde bislang noch keine Systematisierung der Schutzgüter und

---

[340] Ebd., [64–67] sowie die vorangegangene Entscheidung vom 2.11.2010, *Gillberg ./. Schweden*, App. Nr. 41723/06, [97, 103].

[341] EGMR Entscheidung vom 3.4.2012, *Gillberg ./. Schweden*, App. Nr. 41723/06, [64–67].

[342] Siehe oben IV.B.2.

Risikokonzeptionen vorgenommen. Zum Teil sieht die Literatur in der Rechtsprechung zwei Schutzgutkonzeptionen: ein auf Abwehr gerichtetes Sphärenelement und ein auf Interaktion gerichtetes Selbstbestimmungselement.[343]

In der umfassenden Prüfung der Entscheidungen konnten sodann sowohl Risiken als auch Schutzgüter näher bestimmt werden: Eine Reihe von Entscheidungen zu technischen Überwachungsmaßnahmen bezieht sich auf das Risiko einer Überwachungsbedrohung („menace of surveillance"), die sich mit dem Risiko eines Überwachungsdrucks überschneidet, wie es den Spezialinstrumenten zugrunde liegt.[344] Dabei stellen die Entscheidungen des EGMR die Nähe dieser Risikokonzeption zur Abwehr willkürlichen Handelns bei mangelnder Kontrolle und zu Gefährdungen des Demokratieprinzips heraus. Letzteres zeigt die Anbindung an unterstellte Verhaltensauswirkungen in Bezug auf Wahlentscheidungen. Deutlich nimmt der Gerichtshof bei der Argumentation eine „Makroperspektive" ein, aus der gesamtgesellschaftliche Auswirkungen beschrieben werden.[345]

Beginnend mit der Entscheidung *Leander* erfolgt eine Flexibilisierung der Schutzgutkonzeption, indem Begleitumstände und Informationsinhalt an Bedeutung für die Eröffnung des Anwendungsbereichs verlieren und zudem eine Annäherung an das Schutzkonzept der Datenschutzkonvention des Europarats erfolgt. Verschiedene Entscheidungen dieser Phase betreffen das Risiko der Entkontextualisierung in Form der bereits im Rahmen der Spezialinstrumente entwickelten „Kontextinfiltration". Ein weiterer Teil der Entscheidungen verdeutlicht die langsame Ablösung von räumlich aufgebauten Schutzgutkonzeptionen und ermöglicht unter Einschränkungen auch den Privatlebensschutz an öffentlichen Orten, womit insgesamt eine Flexibilisierung und Differenzierung der Schutzgutkonzeption erfolgt.[346]

Das Risiko systematischer Informationserhebungen und das der langfristigen Permanenz von Informationen wurden in einer Reihe von Entscheidungen zu Geheimdiensttätigkeiten ehemals sowjetischer Staaten deutlich. Der Schutz vor systematischen Erhebungen wird dabei insbesondere auch auf öffentlich zugängliche Informationen erstreckt.[347] Im Rahmen eines Exkurses konnte gezeigt werden, dass das Risiko der Informationspermanenz Anlass zu einem spezifisch informationsrechtlichen Rechtsinstituts der Informationsverjährung gibt.[348]

---

343 Siehe oben IV.A.

344 Siehe oben II.A.2.d).

345 Siehe oben IV.B.1.

346 Siehe oben IV.B.2.

347 Siehe oben IV.B.3.

348 Siehe oben IV.B.3.a).

Eine Reihe von Entscheidungen, insbesondere zu Registern über Sexualstraftäter, greift die Risiken von Publizitätsschäden und der Auslösung von Schamgefühlen auf.[349]

Die Flexibilisierung der Schutzgutkonzeption führte schließlich in verschiedenen neueren Entscheidungen zur Übernahme der aus dem US-amerikanischen Recht stammenden Schutzgutkonzeption der Vertraulichkeitserwartung („reasonable expectation of privacy"). Dabei werden anhand mehrerer Entscheidungen zu Medizindaten Sekundäreffekte enttäuschter Vertraulichkeitserwartungen herausgearbeitet. Die Enttäuschung der Erwartung führt nach diesem Verständnis zu negativen Auswirkungen in einem anderen Bereich – in den untersuchten Entscheidungen handelte es sich um die Inanspruchnahme gesundheitlicher Dienstleistungen.[350] Das Schutzgutkonzept der Vertraulichkeitserwartung wird in darauffolgenden Entscheidungen fortgebildet. Dabei werden die Risiken von systematisch-permanenten Erhebungen, von Publizitätsschäden und Schamgefühl sowie von Bewegungsprofilen mit der Konzeption der Vertraulichkeitserwartung zusammengeführt. Die Entscheidungen zu Bewegungsprofilen verdeutlichen das Risiko eines durch Totalüberwachung ausgelösten Überwachungsdrucks, das durch die „Überwachungskumulation" bei „Überwachungsdoppelbefugnissen", wie zwischen Bundeskriminalamt und Bundesverfassungsschutz, verschärft wird.[351]

Weiterhin wurde das Verhältnis der Korrespondenz- und Wohnungsvariante zur Privatlebensvariante untersucht. Diesbezüglich besteht keine einheitliche Linie in der Rechtsprechung des EGMR. Gleichwohl hat die Untersuchung ergeben, dass die E-Mail- und Internetkommunikation in die Schutzgutkonzeption der Vertraulichkeitserwartung einbezogen wird.[352]

Die neuesten Entscheidungen übernehmen die persönlichkeitsrechtlichen Schutzgüter der physischen und psychologischen Integrität sowie der physischen und sozialen Identität. Integritäts- und Identitätsschutzgüter werden anhand des Risikos der Informationsemergenz entwickelt, das die spezifischen Charakteristika von DNA-Daten beschreibt. Die Integritäts- und Identitätskonzeption ist dabei offen für das Aufgreifen neuer Risiken, wie das in der Entscheidung *Gillberg* aufgestellte Erfordernis der Spezifikation persönlicher, sozialer, psychologischer und ökonomischer Einbußen als Informationsverwendungsfolgen zeigt.[353]

---

[349] Siehe oben IV.B.4.

[350] Siehe oben IV.B.5.

[351] Siehe oben IV.B.6.

[352] Siehe oben IV.B.7.

[353] Siehe oben IV.B.8.

# V. Ergebnis

Die Untersuchung der internationalrechtlichen Datenschutznormen hat eine Reihe von Risiken identifiziert, die mit den jeweiligen Regelungen aufgegriffen werden. Die Einbeziehung der Entstehungsgeschichte der Normen, insbesondere in Form von Präambeln und Begründungen sowie einschlägiger Entscheidungen – soweit das normative Material von Spruchkörpern angewendet wird –, ermöglichte zugleich die Benennung einschlägiger Schutzgüter, die durch den engen Zusammenhang mit den identifizierten Risiken nun konkreter fassbar sind.

Im Einzelnen sind folgende Ergebnisse festzuhalten: Der mit der Datenschutzkonvention des Europarats verfolgte Schutz des Art. 8 Abs. 1 EMRK erfüllte zunächst zumindest auch eine Vorwandfunktion, da die Konvention das Risiko der Beeinträchtigung des internationalen Handels durch protektionistisch in Stellung gebrachtes nationales Datenschutzrecht in ihrer Entstehungsphase besonders unterstrichen hat. Das jüngste untersuchte Datenschutzinstrument – das APEC Privacy Framework – stellt eine Fortentwicklung dieser wirtschaftspolitischen Konzeption dar, indem es das Schutzgut des Verbrauchervertrauens in den Vordergrund rückt. Das insoweit einschlägige Risiko besteht in Konsumeinschränkungen der Verbraucher aufgrund von Datenschutzmisstrauen (Nachfragerückgang). Beachtlich an denwirtschaftspolitischen Begründungsansätzen ist die Unabhängigkeit von der zu erwartenden Anknüpfung an persönlichkeitsrechtliche Schutzgüter. Der Grundrechtsbezug soll jedoch im Rahmen der Pläne zur Modernisierung der Datenschutzkonvention durch Berücksichtigung der an anderer Stelle vollzogenen Konstitutionalisierung des Datenschutzes erfolgen.

Diese Pläne stellen insbesondere auch einen Bezug zum Schutzgut der Menschenwürde her, wobei sie das einschlägige Risiko als Kontrollverlust bei automatisierten Verarbeitungen und damit einhergehender Objektmachung des Menschen beschreiben. Die Begründung zur Konvention deutet daneben in ihrer ursprünglichen Fassung durch die Einbeziehung von „Informationsmacht“ auch auf das Schutzgut der Selbstbestimmung und das Risiko von Machtverschiebungen hin.

Die untersuchten allgemeinen Regelungskonzeptionen und Grundsätze des Datenschutzrechts, wie beispielsweise das Konzept der normativen Zweckbegrenzung, sind in jeweils unterschiedlicher Ausprägung auch in den meisten anderen Spezialinstrumenten enthalten. Ihre Untersuchung auf Risikokonzeptionen und Schutzgüter erwies sich als besonders ergiebig, womit das zunächst festzustellende Überwiegen der wirtschaftspolitischen Zielsetzung aus materieller Sicht relativiert wird. Hinsichtlich der konkret erfassten Risikokonzeptionen konnte zunächst das Risiko eines Überwachungsdrucks durch ungeregelte Informationsverarbeitung identifiziert werden. In engem Zusammenhang hiermit stehen Auswirkungen auf das Verhalten Betroffener und damit das Schutzgut der Selbstbestimmung. Das Risiko wird auch in der Rechtsprechung des EGMR näher bestimmt. Dort ist von einer Überwachungsbedrohung („menace of surveillance“) die Rede. Das Risiko

wird aus gesellschaftlicher Makroperspektive betrachtet und die Nähe zu Demokratieprinzip und Willkürschutz herausgestellt.

Der zweite große Risikokomplex kann mit dem Begriff Entkontextualisierung beschrieben werden. Dieses Risiko, dem das Konzept der normativen Zweckbegrenzung zugrunde liegt, beschreibt Situationen, in denen sich Informationen aus einem Lebensbereich in einem anderen Bereich nachteilig für den Betroffenen auswirken. Hierbei differenzierten die normativen Risikokonzeptionen zwischen nachteiligen Auswirkungen durch die Informationsübernahme einerseits (Kontextinfiltration) und nachteiligen Auswirkungen durch die Nichtübernahme von Informationen andererseits (Kontextdefizit). Die Rechtsprechung des EGMR hat sich für dieses Risiko erst mit einer beginnenden Flexibilisierung der Schutzgutkonzeption langsam geöffnet. Diese Flexibilisierung ermöglichte insbesondere den Schutz von Privatheitsenklaven in öffentlichen Bereichen.

Eine nur in der Rechtsprechung, nicht jedoch in den Spezialinstrumenten enthaltene Schutzgutkonzeption stellt berechtigte Vertraulichkeitserwartungen in den Vordergrund. Die an das US-amerikanische Recht angelehnte Konstruktion („reasonable expectation of privacy test“) wurde in der Rechtsprechung des EGMR zunächst anhand des Risikos von Sekundäreffekten auf Verhaltensebene entwickelt. So standen in einer Reihe von Entscheidungen insbesondere die Nichtinanspruchnahme medizinischer Dienstleistungen und damit verbundene Auswirkungen auf die Bevölkerungsgesundheit im Vordergrund. Hier zeigt sich die Nähe zur wirtschaftspolitisch motivierten Schutzgutkonzeption des APEC Privacy Framework. Auch dort sind die sekundären Verhaltenseffekte – allerdings in Bezug auf Konsumentscheidungen – tragendes Risiko der Schutzgutkonzeption. In der Rechtsprechung des EGMR wurde die Vertraulichkeitskonzeption mit weiteren Risiken kombiniert, womit die besondere „Anschlussfähigkeit“ der Konzeption unterstrichen wird.

Die mit der Vertraulichkeitskonzeption kombinierten Risiken waren zuvor bereits in den Spezialinstrumenten und zum Teil auch in älteren Entscheidungen des EGMR aufgegriffen worden. Es handelt sich dabei zunächst um das Risiko des Überwachungsdrucks, das jedoch eine Konkretisierung für den Fall der Erstellung von Bewegungsprofilen erhielt. Hier wurde insbesondere das Risiko einer Überwachungskumulation durch Überwachungsdoppelbefugnisse anhand eines Sachverhalts entwickelt, bei dem sowohl Geheimdienst als auch Polizei Überwachungsmaßnahmen gegenüber der gleichen Person einleiteten. Die Vertraulichkeitserwartung wurde in der Rechtsprechung auch auf die E-Mail- und Internetkommunikation ausgedehnt. Ein weiteres sowohl in der Rechtsprechung als auch in den Normen aufgegangenes Risiko ist die Informationspermanenz, d.h. das Potenzial von Informationen, nach langen Zeiträumen – u.a. auch gerade wegen des Zeitablaufs – noch Schäden auszulösen. Dieses Risiko war Anlass für einen Exkurs, in dem sich das Erfordernis eines informationsrechtlichen Rechtsinstituts der Informationsverjährung in Anlehnung an die zivil- und strafrechtlichen Verjährungsvor-

schriften herausgestellt hat. Die Rechtsprechung des EGMR hat an dieser Konzeption das systematische Sammeln von Informationen – auch solchen, die öffentlich zugänglich sind – als eigenständiges Risiko verselbstständigt.

Eine weitere naheliegende Risikokategorie, die sowohl in den Datenschutzvorschriften als auch in der Rechtsprechung verschiedentlich aufgegriffen und mit der Vertraulichkeitskonzeption kombiniert wird, ist die Auslösung von Publizitätsschäden, womit die negative Auswirkung auf den Betroffenen durch das Bekanntwerden als solches – nicht erst durch die weitere Verwendung der Informationen – gemeint ist. Dabei ergibt die normative Analyse, dass hier vor allem die Auslösung von Schamgefühl beim Betroffenen aufgegriffen wird. In engem Zusammenhang damit, gleichwohl aber nur in den Spezialinstrumenten eindeutig zu identifizieren, ist das Risiko der Erhöhung individueller Verletzlichkeit. Hiermit wird insbesondere die Möglichkeit zu unbefugten, missbräuchlichen Verwendungen der Informationen gefasst. Dieses Risiko lässt sich auch im Rahmen des Art. 17 IPBürg, zusammen mit dem Risiko des Überwachungsdrucks, nachvollziehen.

Gute Rückschlüsse auf das Risiko der Diskriminierung ermöglichen die allgemeinen Regelungskonzeptionen der Spezialinstrumente. Dieses wurde näher bestimmt als kategoriale Behandlung und Devaluation von Personen. Dabei konnten aus verschiedenen Arten sensibler Daten die Charakteristiken der jeweiligen Datenkategorien herausgearbeitet werden. Diese bestehen in der besonderen Polarisierung, Schambesetzung, Leistungsindikation oder Informationsemergenz. Mit Letzterem ist der überschießende Charakter bestimmter Informationen gemeint. Diese wohnt zwar allen Informationen bis zu einem gewissen Grade inne, ist jedoch bei bestimmten Kategorien besonders naheliegend und aussagekräftig. So ermöglichen beispielsweise Gendaten nicht nur eine eindeutige Identifizierung des Betroffenen, sondern auch Rückschlüsse auf Verwandtschaftsverhältnisse und ggf. auch auf Erbkrankheiten. Ein weiteres Beispiel emergenter Informationen sind biometrische Daten, mit denen sich in zunehmender Weise über das reichhaltige Bildmaterial im Internet umfassende Personalisierungen und dann auch Rückschlüsse zu Aufenthaltsorten, politischen Einstellungen usw. vornehmen lassen. Das Risiko der Informationsemergenz wird auch von der Rechtsprechung des EGMR aufgegriffen und anhand des Beispiels „Gendaten“ durchdekliniert.

Die Rechtsprechung hat in Entscheidungen jüngeren Datums eine beachtliche „dogmatische Öffnung“ der Schutzgüter vorgenommen, die es ermöglicht, die einschlägigen Risiken umfassend abzudecken. Als Anknüpfungspunkt dienten die bereits in älteren persönlichkeitsrechtlichen Entscheidungen entwickelten Schutzgüter der physischen und psychologischen Integrität sowie der physischen und sozialen Identität. Diese Schutzgüter werden in datenschutzrechtlichen Kontexten herangezogen und sind hinreichend offen, um die bis dahin aufgegriffenen Risiken zu umfassen. Eine genauere Bestimmung, insbesondere des Verhältnisses der Varianten zueinander, nimmt der EGMR jedoch nicht vor.

*Teil 2*

# Recht der Europäischen Union

## I. Überblick

### A. Rechtsgrundlage und Reformvorhaben

Bevor der Vertrag von Lissabon[1] die aus den Europäischen Gemeinschaften, der Gemeinsamen Außen- und Sicherheitspolitik und der Zusammenarbeit im Bereich Justiz und Inneres gebildete Säulenstruktur der Europäischen Union auflöste, bildete Art. 286 EGV die einzige explizit datenschutzrechtliche Gesetzgebungsgrundlage. Die Vorschrift betraf jedoch lediglich die Datenverarbeitung durch Gemeinschaftsorgane und -einrichtungen. Im Übrigen waren die Kompetenzgrundlagen innerhalb der Säulenstruktur umstritten. Im Bereich der ersten Säule wurde das Sekundärrecht auf die Binnenmarktkompetenz des Art. 95 EGV a.F. (vormals Art. 100a EGV a.F., jetzt Art. 114 AEUV) gestützt. Die Dritte Säule (PJZS) ermöglichte Datenschutzregelungen im Rahmen von Art. 31 Abs. 1 lit. c i.V.m. Art. 34 Abs. 2 lit. b und Art. 24 sowie Art. 38 EUV a.F.[2]

Der Vertrag von Lissabon wertete den Datenschutz auf: Das Datenschutzgrundrecht des Art. 8 EU-GRC ist mit dem Reformvertrag gem. Art. 6 Abs. 1 EUV rechtsverbindlich geworden. Mit Art. 16 AEUV besteht nunmehr eine Kompetenzgrundlage, die eine Überführung des Datenschutzrechts der unterschiedlichen Politikfelder der Union in einen einheitlichen Rechtsrahmen ermöglicht. Der Datenschutz wird damit von seiner zweifelhaften Begründung über den Binnenmarkt befreit.[3] Am 25.1.2012 legte die Kommission dann auch zwei Entwürfe zur Neuregelung des Datenschutzes mit dem Ziel der umfassenden Harmonisierung[4] vor: Eine Datenschutzgrundverordnung (EU-DSGVO-E) für den Bereich der bisherigen ersten Säule und eine Datenschutzrichtlinie (EU-DSRL-E) für die Datenverarbeitung bei Polizei und Justiz. Die beiden Entwürfe sollen die derzeit gültige

---

[1] Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13.12.2007, ABl. 2007/C 306/01.

[2] Zum Ganzen *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2. Aufl., S. 14 ff.

[3] *Grimm*, JZ 2013, 585 (589).

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

Datenschutzrichtlinie aus dem Jahr 1995 und einen Rahmenbeschluss für den Bereich Justiz und Inneres aus dem Jahr 2008 ablösen.[5]

Die auf umfangreiche Vorarbeiten zurückgehenden Entwürfe der Kommission sind in der deutschen Literatur auf ein geteiltes Echo gestoßen. Während die anstehende Vereinheitlichung teilweise als Fortschritt begrüßt wird,[6] kritisiert Verfassungsrichter *Masing* die Pläne als „Abschied von den Grundrechten".[7] Verantwortlich für einen solchen „Abschied" ist der Anwendungsvorrang des europäischen Rechts, der – mit unterschiedlicher Begründung und Reichweite – von europäischer und nationaler Rechtsprechung und Literatur grundsätzlich anerkannt wird.[8] Anwendungsvorrang bedeutet, dass nationales Recht nicht angewendet werden darf, wenn es gegen Unionsrecht verstößt.[9] Der Anwendungsvorrang ist unabhängig vom Normrang innerhalb der jeweiligen Rechtsordnung und gilt deshalb auch zwischen europäischem Sekundärrecht und nationalem Verfassungsrecht. In Bereichen, in denen der Union von den Mitgliedstaaten Hoheitsrechte übertragen wurden, findet grundsätzlich keine Kontrolle anhand deutschen Rechts statt.[10] Während der Anwendungsvorrang nach Rechtsprechung des EuGH absolut gilt, bestehen davon nach Rechtsprechung des BVerfG jedoch Ausnahmen: Der wegen der Befürchtung einer „Vertragsänderung im Gewand von Vertragsauslegung" rechtspolitisch hoch brisante Streit zwischen EuGH und BVerfG hat mit den Entscheidungen des EuGH in der Sache *Åkerberg Fransson*[11] und des BVerfG zum *Antiterrordateiengesetz*[12] einen neuen vorläufigen Höhepunkt erreicht.[13] Da sich der Streit immer wieder an datenschutzrechtlichen Fragen entwickelt, soll hierzu kurz Stellung bezogen werden: Ausgangspunkt ist Art. 51 Abs. 1 EU-GRC, wonach die EU-GRC „ausschließlich bei der Durchführung des Rechts der Union" gilt. Die Kompetenz des Art. 16 Abs. 2 AEUV beschränkt sich zunächst ebenfalls auf die Verarbeitung durch Organe der Union, erstreckt sich dann aber auf die „Ausübung von Tätigkeiten" der Mitgliedstaaten, die in den „Anwendungsbereich" des Unionsrechts fallen.

---

[5] Dem federführenden LIBE-Ausschuss lagen ca. 4000 Änderungsanträge vor; die Abstimmung erfolgte am 12.3.2014, der nächste Schritt im Gesetzgebungsverfahren ist der sog. Trilog zwischen der Kommission, den Berichterstattern des Parlaments und der Ratspräsidentschaft. Zum aktuellen Stand (28.3.2014): http://europa.eu/rapid/press-release_MEMO-14-60_en.htm?locale=en; vgl. ZD-Aktuell 2013, 03628. Zur Bearbeitung durch den Berichterstatter des Innenausschusses des Europaparlaments *Jan Philip Albrecht* vgl. http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html [Stand: 28.3.2014].

[6] *von Lewinski*, DuD 2012, 564 (567, 570).

[7] *Masing*, SZ vom 9.1.2012.

[8] Statt vieler *Streinz*, Europarecht, S. 73 ff.

[9] *Polzin*, JuS 2012, 1.

[10] *von Lewinski*, DuD 2012, 564 (568); *Britz*, EuGRZ 2009, 1 (3).

[11] EuGH Urteil vom 26.2.2013 Rs. C-617/10 *(Åkerberg Fransson)* = JZ 2013, 613.

[12] BVerfG, Urteil vom 24.4.2013, 1BvR1215/07 *(Antiterrordateigesetz)* = JZ 2013, 621.

[13] Zum Ganzen *Grimm*, JZ 2013, 585 (589–592).

Auch die Erläuterungen zur EU-GRC sprechen unter Verweis auf die Rechtsprechung des EuGH vom „Anwendungsbereich" des Unionsrechts.[14] Bereits vor Inkrafttreten der EU-GRC zog der EuGH nämlich das Kriterium des „Anwendungsbereichs des Gemeinschaftsrechts" heran, um den Geltungsbereich der damals noch ungeschriebenen Unionsgrundrechte gegenüber den Mitgliedstaaten zu bestimmen.[15]

Wie weit die Auffassung des EuGH den Anwendungsbereich des europäischen Rechts ausdehnte, zeigte dann das Urteil in der Rechtssache *Österreichischer Rundfunk*.[16] Gegenstand des Verfahrens war eine Vorschrift, nach der die Bezüge von bestimmten Angestellten im öffentlichen Dienst veröffentlicht werden mussten. Der Gerichtshof prüfte das Gesetz zunächst am Maßstab der EU-DSRL und bejahte wegen deren Anwendbarkeit die Eröffnung des Unionsrechts ohne (über die Anwendbarkeit der Richtlinie hinaus) einen Binnenmarktbezug zu fordern. Anschließend prüfte er das Gesetz am Maßstab der europäischen Grundrechte. Diese weite Auslegung erlaubte eine umfassende Kontrolle nationaler Datenverarbeitungen am Datenschutzgrundrecht.[17] Weil praktisch jeder rechtlich relevante Vorgang auch ein Daten- und Informationsverarbeitungsvorgang ist, wurde diese Auslegung vielfach als zu weit in innerstaatliche Vorgänge hineinragend kritisiert. Dies gelte insbesondere aufgrund der Einbeziehung von Privatrechtsverhältnissen, die ebenfalls von der Richtlinie umfasst sind. Nationalen Grundrechten würde somit auch in diesem – ohnehin grundrechtsuntypischen – Bereich der Anwendungsvorrang entzogen.[18] Nach einer vermittelnden Auffassung konnte bei Umsetzungsspielräumen dem Prinzip des Höchststandards gefolgt werden, ähnlich der Zweischrankentheorie im europäischen Kartellrecht.[19] Unabhängig davon, welcher Auffassung man folgte, zeigte sich, dass die Grenzen zulässiger Datenverarbeitung bereits zu diesem Zeitpunkt in erster Linie von den Unionsgrundrechten gesetzt wurden.[20] Die kurz darauf ergangene – ebenfalls datenschutzrechtliche – Entscheidung in der Rechtssache *Lindqvist*[21] unterstrich die extensive Auslegung des „Anwendbarkeitskriteriums" nochmals: Der EuGH hielt es unter Verweis auf die ORF-Entscheidung nicht für erforderlich, dass der Anwendungsbereich des Unionsrechts im jeweiligen Einzelfall eröffnet ist, sondern nahm vielmehr eine extensive, generelle Betrachtungsweise ein.[22] Im Ergebnis fasste der EuGH damit den Anwendungsbereich des

---

[14] Erläuterung zu Art. 51, ABl. C 310/454 vom 16.12.2004.

[15] EuGH Urteil vom 18.6.1991 C-260/89 (ERT) Rn. 42 ff.; vgl. auch EuGH Urteil vom 13.7.1989 C-5/88 (Wachauf) Rn. 19 (dort jedoch „Durchführung").

[16] EuGH Urteil vom 20.5.2003 verb. Rs. C 465/00, C-138/01 und C-139/01 *(Österreichischer Rundfunk)*.

[17] *Britz*, EuGRZ 2009, 1 (4 ff.).

[18] Ebd., 1 (4) m.w.N.

[19] *Michael/Morlok*, Grundrechte Rn. 104.

[20] Vgl. *Bäcker/Hornung*, ZD 2012, 152.

[21] EuGH Urteil vom 6.11.2003 Rs. C-101/01 *(Lindqvist)*.

[22] Ausführlich zu dieser Rechtssache unten II.B.2.c).

Unionsrechts bereits vor der Entscheidung *Åkerberg Fransson* weit. Eine Bindung besteht nach seiner Auffassung bereits, wenn das Unionsrecht Ermessensspielräume eröffnet und wenn nationales Recht in Zusammenhang mit der Umsetzung von Richtlinien steht.[23]

Das Bundesverfassungsgericht hatte demgegenüber seinen Prüfungsanspruch in den beiden *„Solange"*-Entscheidungen[24] aufrechterhalten, aber ruhen lassen, solange sich der europäische Grundrechtsschutz nicht verschlechtern würde. Diesen Prüfungsanspruch hat es sodann in der *Lissabon*-Entscheidung[25] aufrechterhalten und mittels dreier Kontrollpunkte näher ausgestaltet: Dabei handelt es sich um Grundrechtskontrolle, Verfassungsidentitätskontrolle und Ultra-vires-Kontrolle. Der Prüfungsvorbehalt wird jedoch vom BVerfG aufgrund des Kooperationsverhältnisses zwischen BVerfG und EuGH nur zurückhaltend konstruiert und erfordert z.B. für den Fall der Grundrechtskontrolle ein dauerhaftes Absinken des Grundrechtsstandards der EU unter die Anforderungen des Grundgesetzes. Eine derartige Absenkung steht derzeit nicht zu befürchten.[26] Das BVerfG akzeptiert damit zwar, dass innerstaatliche Rechtsakte und Vollzugsvorschriften, die Unionsrecht gem. Art. 51 Abs. 1 Satz 1 EU-GRC durchführen, nicht mehr an den Grundrechten zu messen sind, doch wollte es den Anwendungsvorrang auf den Fall zwingender Vorgaben des Unionsrechts beschränken. Deshalb war es dem BVerfG beispielsweise möglich, die Umsetzungsgesetze zur Vorratsdatenspeicherung an deutschen Grundrechten zu messen, soweit diese über die Vorgaben der Richtlinie 2006/24/EG hinausgingen. Eine weitere Zurücknahme der Kontrolldichte erfolgte sodann in dem ein Jahr darauf ergangenen *Honeywell*-Beschluss,[27] der besonders hohe Anforderungen an die Annahme eines Ultra-Vires-Akts der Union stellt.[28]

Mit der Entscheidung *Åkerberg Fransson*[29] hat der EuGH nun erneut eine äußerst extensive Fassung des unionsrechtlichen Anwendungsbereichs an den Tag gelegt: Die Entscheidung erging auf Vorlage eines schwedischen Gerichts und bezog sich auf das Verbot der Mehrfachbestrafung, ne bis in idem, in einer Steuerstrafsache. Der EuGH greift zwar das Kriterium der Durchführung des Unionsrechts aus Art. 50 Abs. 1 EU-GRC auf, legt dieses aber – unter Rückgriff auf seine vorangegangene Rechtsprechung und die Erläuterungen zur Charta – äußerst weit aus: Es sei keine Fallgestaltung denkbar, die vom Unionsrecht erfasst würde, ohne

---

[23] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 51 GRCh Rn. 8 f.

[24] BVerfG Beschl. vom 29.5.1974, BvL 52/71 *(Solange I)* = BVerfGE 37, 271; BVerfG Beschl. vom 22.10.1986, 2 BvR 197/83 *(Solange II)* = BVerfGE 73, 339.

[25] BVerfG Urteil vom 30.6.2009, 2 BvE 2, 5/08, 2 BvR 1010, 1022, 1259/08, 182/09 *(Lissabon)* = BVerfGE 123, 267.

[26] *Polzin*, JuS 2012,1 ff.

[27] BVerfG Beschl. vom 6.7.2010, 2 BvR 2661/06 *(Honeywell)* = BVerfGE 126, 286.

[28] Zu den Einzelheiten *Grimm*, JZ 2013, 585 (591).

[29] EuGH Urteil vom 26.2.2013 Rs. C-617/10 *(Åkerberg Fransson)* = JZ 2013, 613.

dass die (Unions-)Grundrechte anwendbar seien. Ausreichend für diesen Zusammenhang sieht das Gericht sodann verschiedene unionsrechtliche Regelungen mit Bezug zum Mehrwertsteueraufkommen der Mitgliedstaaten, insbesondere das Erfordernis einer wirksamen Betrugsbekämpfung. Jedes Versäumnis bei der Erhebung der Mehrwertsteuer führe darüber hinaus zu einer Verringerung der Bereitstellung von Mehrwertsteuermitteln für den Haushalt der Union.[30] Diese Auffassung wird von der Literatur als zu weitgehend kritisiert.[31] *Grimm* meint, damit sei die Eingrenzung des Anwendungsbereichs der Unionsgrundrechte in Art. 51 Abs. 1 EU-GRC unterlaufen worden, die nationalen Grundrechte stünden zur Disposition der EU. Dem EuGH sei „kein Faden zu dünn", um eine Verbindung zum Unionsrecht zu erkennen.[32]

Das BVerfG ließ mit einer Stellungnahme auf das Urteil nicht lange auf sich warten und führt dann im Urteil zum *Antiterrordateiengesetz* aus, dass der Entscheidung *Åkerberg Fransson* keine „Lesart" unterlegt werden dürfe, nach der sie „offensichtlich als Ultra-vires-Akt zu beurteilen wäre oder Schutz und Durchsetzung der mitgliedstaatlichen Grundrechte in einer Weise gefährdete (Art. 23 Abs. 1 Satz 1 GG), dass dies die Identität der durch das Grundgesetz errichteten Verfassungsordnung in Frage stellte". Insofern dürfe die Entscheidung nicht in einer Weise verstanden und angewendet werden, „nach der für die Bindung der Mitgliedstaaten durch die in der Grundrechtecharta niedergelegten Grundrechte der Europäischen Union jeder sachliche Bezug einer Regelung zum bloß abstrakten Anwendungsbereich des Unionsrechts oder rein tatsächliche Auswirkungen auf dieses ausreiche".[33]

In der Folge prüft es das Antiterrorgesetz am Maßstab des Grundrechts auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[34]

Aus der soeben dargestellten Rechtslage auf Ebene der EU ergibt sich das nun folgende Prüfungsprogramm: Zunächst sind die gem. Art. 6 Abs. 1 EUV nunmehr rechtsverbindlichen Art. 7 und Art. 8 der EU-GRC auf die ihnen zugrunde liegenden Risikokonzeptionen und Schutzgüter zu untersuchen. Weil Art. 52 Abs. 3 Satz 1 EU-GRC bestimmt, dass die Rechte der Charta, die denjenigen der EMRK entsprechen, dieselbe Bedeutung und Tragweite wie diese haben sollen, bleibt zu überprüfen, ob die Rechtsprechung des EuGH eigenständige datenschutzrechtliche Risikokonzeptionen entwickelt hat. Hierzu ist zunächst der rechtliche Rahmen der „Grundrechtskorrespondenz" gem. Art. 52 Abs. 3 Satz 1 EU-GRC zu skizzieren. Sodann müssen die einschlägigen Charta-Grundrechte analysiert werden. In einem

---

30 EuGH Urteil vom 26.2.2013 Rs. C-617/10 *(Åkerberg Fransson)* Rn. 24–27.

31 *Dannecker*, JZ 2013, 616 (618) m.w.N.

32 *Grimm*, JZ 2013, 585 (591).

33 BVerfG, Urteil vom 24.4.2013, 1 BvR 1215/07 *(Antiterrordateigesetz)* Rn. 91.

34 Zu der Entscheidung siehe unten Teil 3, II.B.17 sowie *Grimm*, JZ 2013, 585 (591 f.) und *Gärditz*, JZ 2013, 633 ff.

dritten Schritt sind die Motive hinter den sekundärrechtlichen Regelungen auf Risikokonzeptionen zu überprüfen. Hierbei werden von den geltenden Rechtsquellen die RL 95/46/EG sowie der Rahmenbeschluss 2008/977/JI untersucht, um sodann zu den korrespondierenden Kommissionsentwürfen überzugehen.

## B. Grundrechtskorrespondenz von EMRK und Charta

Mit Art. 52 Abs. 3 Satz 1 EU-GRC wird eine „Korrespondenz" von Charta- mit EMRK-Grundrechten ermöglicht.[35] Die durch Art. 8 EMRK garantierten Rechte „entsprechen" den in Art. 7 und Art. 8 EU-GRC garantierten Rechten, auch wenn hinsichtlich der jeweils verwendeten Formulierungen und Begriffe Unterschiede bestehen. Diese Grundrechtskorrespondenz und der Umstand, dass Art. 6 Abs. 1 Unterabs. 1 EUV die rechtliche Gleichrangigkeit von Charta und Verträgen klarstellt, führen dazu, dass unionsrechtliche Materien künftig im Hinblick auf die Charta und nicht hinsichtlich der EMRK zu prüfen sind. Gleichzeitig wird die EMRK jedoch in die Charta bis zu einem gewissen Grade „inkorporiert", womit ihre fortwährende Bedeutung insbesondere für die Rechtsfindung auf unionaler Ebene belegt ist.[36]

Diese „Grundrechtskorrespondenz" konnte bis zu einem gewissen Grad auch vor Inkrafttreten des Lissabonner Vertrages erreicht werden: Art. 6 Abs. 2 EUV a.F. bestimmte, dass die Union die Grundrechte achtet, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben. Die EU-GRC – das „Kondensat eines rechtsvergleichenden Status quo" – wurde vom EuGH als Rechtserkenntnisquelle herangezogen.[37] Mangels expliziter normativer Ausgangsgrundlage hatte der EuGH das Datenschutzgrundrecht als allgemeinen Rechtsgrundsatz anerkannt, hierzu jedoch noch keine umfangreiche Rechtsprechung entwickelt.[38] Gleichwohl erfolgte bereits eine Orientierung an der EMRK als Minimalstandard.[39] Neben den pragmatischen Gründen sprachen dafür insbesondere der Grundsatz der Gemeinschaftstreue des Art. 10 EGV[40] sowie bestehende sekundärrechtliche Verweisungen auf Art. 8 EU-GRC. Insbesondere die letztgenannten Verweisungen konnten als normative Anknüpfungspunkte herangezogen werden.[41]

---

[35] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 52 GRCh Rn. 21.

[36] Zum Ganzen GA *Villalón*, Schlussanträge vom 14.4.2011 Rs. C-70/10 *(Scarlet Extended)* Rn. 30–34.

[37] *Kühling*, in: Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht, S. 666 f.

[38] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2. Aufl., S. 13.

[39] Gegen die Annahme eines „Minimalstandards" spricht jedoch die vom EuGH verschiedentlich angedeutete Auffassung, wonach die zur Grundrechtskonkretisierung herangezogene Datenschutzrichtlinie die Konflikte zwischen freiem Verkehr personenbezogener Daten und Datenschutz abschließend regelt, vgl. *Britz*, EuGRZ 2009, 1 (6 f.).

[40] *Kühling*, in: Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht, S. 673.

[41] *Britz*, EuGRZ 2009, 1 (2).

# II. Primärrecht

## A. Art. 7 EU-GRC

Art. 7 EU-GRC hat den Titel „Achtung des Privat- und Familienlebens“ und lautet: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation“.[42]

Die Vorschrift entspricht in ihrem Wortlaut damit teilweise Art. 8 Abs. 1 EMRK. Der Europäische Konvent, der den Wortlaut formulierte, bejaht insoweit auch die Entsprechung gem. Art. 52 Abs. 3 EU-GRC.[43] In seiner Entscheidung zu Agrarbeihilfen bestätigte dies der EuGH.[44] Die hier relevanten Merkmale des sachlichen Schutzbereichs sind das Privatleben und die Kommunikation. Der Begriff der Kommunikation entspricht dem der Korrespondenz bei Art. 8 EMRK.[45] Der Begriff „Korrespondenz“ wurde ersetzt, um der technischen Entwicklung Rechnung zu tragen.[46] Beeinträchtigungen der Kommunikation liegen vor, wenn die Kenntnisnahme von Inhalten oder Umständen der Kommunikation ermöglicht wird. Dabei fallen auch moderne Formen der Kommunikation wie E-Mail und SMS in den Schutzbereich. Kommunikationsdaten (Inhalts- und Verkehrsdaten) fallen jedoch als personenbezogene Daten in den Schutzbereich des Art. 8 EU-GRC.[47] Leitentscheidungen des EuG bzw. EuGH zur Schutzbereichsvariante „Kommunikation“ liegen nicht vor.[48] Deshalb konnte sich zunächst noch keine Abgrenzung ähnlich dem deutschen Recht herausbilden, das den Schutz des Art. 10 Abs. 1 GG auf laufende Kommunikation beschränkt, während die im Herrschaftsbereich der Teilnehmer verbleibende Kommunikation durch den insoweit spezielleren Art. 13 GG für den Bereich der Wohnung und darüber hinaus durch die einschlägigen Ausprägungen des Allgemeinen Persönlichkeitsrechts[49] gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt werden.[50]

Der Schutzbereich des Privatlebens muss danach die Entscheidung darüber umfassen, inwieweit die persönliche Lebensführung zum Gegenstand öffentlicher

---

[42] ABl. 2007 Nr. C 303 S. 4.

[43] Erläuterungen des Präsidiums des Europäischen Konvents, ABl. 2004, Nr. C 310, S. 456.

[44] EuGH Urteil vom 9.11.2010, Rs. C-92/09 und C-93/09 *(Agrarbeihilfeempfänger)* Rn. 51 f., 59, 72, 87.

[45] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 7 GRCh Rn. 10.

[46] Erläuterungen des Präsidiums des Europäischen Konvents, ABl. 2004, Nr. C 310/456.

[47] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2. Aufl., S. 16.

[48] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 6 GRCh Rn. 13.

[49] Im Folgenden wird in Abgrenzung vom zivilrechtlichen Allgemeinen Persönlichkeitsrecht vom Grundrecht auf Schutz der Persönlichkeit gesprochen, vgl. *Bäcker*, in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung, Fn. 7.

[50] BVerfGE 120, 274 (307 ff.) sowie näher dazu unten Teil 3, I.A. In diese Richtung auch *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 7 GRCh Rn. 10.

Kenntnis und Erörterung gemacht wird. Von Teilen der Literatur wird der Schutzbereich in drei Ausprägungen konkretisiert: Recht auf Selbstbestimmung, Recht auf Selbstbewahrung und Recht auf Selbstdarstellung. Insoweit wird von *Kingreen* der Schutz personenbezogener Daten gem. Art. 8 EU-GRC als besondere Ausprägung des Rechts auf Selbstbewahrung betrachtet.[51] Der EuGH hält im Fall der namentlichen Veröffentlichung von Agrarbeihilfeempfängern sowohl Art. 7 als auch Art. 8 EU-GRC für einschlägig und sieht einen engen Zusammenhang von Art. 7 und Art. 8 EU-GRC.[52] Hier wäre jedoch eine klare Stellungnahme für die Spezialität von Art. 8 EU-GRC wünschenswert gewesen, zumal der Gerichtshof die tragenden Gründe aus Urteilen des EGMR zieht, die zu dem datenschutzrechtlichen Schutzgehalt von Art. 8 EMRK ergangen sind.[53] Auch die Literatur geht von der Spezialität des Art. 8 EU-GRC aus. Eine Ausnahme hiervon wird allerdings für Telekommunikationsdaten erörtert.[54] Im zweiten Urteil des EuGH zur Vorratsdatenspeicherung vom 8.4.2014 werden ebenfalls Art. 7 und Art. 8 EU-GRC zum Maßstab gemacht, wobei der Gerichtshof dort davon ausgeht, dass das Privatleben und die durch Art. 7 EU-GRC „garantierten Rechte" betroffen seien. Weil die Vorratsdatenspeicherung eine Verarbeitung personenbezogener Daten im Sinne des Art. 8 EU-GRC darstellt, müssten „zwangsläufig die ihm zu entnehmenden Erfordernisse des Datenschutzes" erfüllt werden.[55]

Der Gerichtshof geht zudem davon aus, dass „der Schutz personenbezogener Daten, zu dem Art. 8 Abs. 1 der Charta ausdrücklich verpflichtet, für das in ihrem Art. 7 verankerte Recht auf Achtung des Privatlebens von besonderer Bedeutung ist".[56] Differenzierter ist die Abgrenzung von GA *Villalón* in seinen Schlussanträgen zur zweiten Vorratsdatenspeicherungsentscheidung.[57] Er grenzt beide Rechte nach der Art der betroffenen Daten ab, wobei er Art. 8 EU-GRC für Daten anwenden will, „die als solche personenbezogen sind, d. h. insofern, als sie eine Person individualisieren", und Art. 7 EU-GRC für „Daten, die gewissermaßen mehr als personenbezogen sind".[58] Dabei handele es sich „um Daten, die sich in qualitativer Hinsicht im Wesentlichen auf das Privatleben – auf das Geheimnis des Privatlebens, einschließlich der Intimität – beziehen" und bei denen sich bereits dann ein Problem stelle, wenn die Umstände des Privatlebens überhaupt Datenform ange-

---

[51] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 7 GRCh Rn. 3–5 und 12.

[52] EuGH Urteil vom 9.11.2010 Rs. C-92/09 und C-93/09 *(Agrarbeihilfeempfänger)* Rn. 47, 52 ff.

[53] Ebd. Rn. 48–52.

[54] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2. Aufl., S. 17.

[55] EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* Rn. 29.

[56] Ebd. Rn. 53.

[57] GA *Villalón*, Schlussanträge vom 12.12.2013 zu EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* Rn. 60–66.

[58] Ebd. Rn. 64 f.

nommen haben.[59] Ein dahingehender vorgelagerter Schutz werde in erster Linie durch Art. 7 EU-GRC gewährleistet. *Villalón* konterkariert seine eigene Abgrenzung dann jedoch, indem er ausführt, dass auch dieser Schutz „in zweiter Linie" anhand von Art. 8 EU-GRC zu prüfen sei.[60]

Da insoweit weder in den Schlussanträgen des GA noch in den Entscheidungen des EuGH eine gesicherte Abgrenzung zwischen Art. 7 und Art. 8 EU-GRC vorgenommen wurde und sich insbesondere in der zweiten Vorratsdatenspeicherungsentscheidung des EuGH eher der Eindruck einer „Parallelführung mit Tendenz zur Spezialität des Art. 8 EU-GRC" aufdrängt, wird die folgende Analyse anhand der Rechtsprechung zu Art. 8 EU-GRC aufgebaut. Soweit bei den untersuchten Urteilen und Schlussanträgen dort auch Ausführungen zu Art. 7 EU-GRC getroffen werden, ist es für die Zielsetzung dieser Untersuchung unschädlich, die einschlägigen Passagen in der Zusammenschau mit Art. 8 EU-GRC zu analysieren. Wegen der vom EuGH angenommenen besonderen Bedeutung des Schutzes personenbezogener Daten auch für Art. 7 EU-GRC werden mit diesem Untersuchungszuschnitt alle relevanten Entscheidungen einbezogen.

## B. Art. 8 EU-GRC und EuGH-Rechtsprechung

### 1. Überblick: sekundärrechtliche Prägung

Art. 8 EU-GRC ist überschrieben mit „Schutz personenbezogener Daten" und lautet:

> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.[61]

Der Artikel normiert somit im ersten Absatz das Recht auf Schutz personenbezogener Daten. Der zweite Absatz bestimmt die Voraussetzungen, unter denen die Verarbeitung dieser Daten rechtmäßig ist, indem er die Anforderungen der RL 95/46/EG in Art. 8 Abs. 2 Satz 1 EU-GRC übernimmt: Die Daten dürfen demnach nur nach Treu und Glauben für festgelegte Zwecke verarbeitet werden, vgl. Art. 6 Abs. 1 a) und b) RL 95/46/EG. Weiterhin ist gem. Art. 8 Abs. 2 Satz 2 EU-GRC die Einwilligung der betroffenen Person oder eine sonstige gesetzlich geregelte legitime Grundlage erforderlich. Das Erfordernis der Einwilligung findet sich in Art. 7 a) RL 95/46/EG. Bereits hier deutet sich eine Manifestation der Selbst-

---

[59] Ebd. Rn. 65.

[60] Ebd. Rn. 66.

[61] ABl. 2007 Nr. C 303 S. 4.

bestimmung als Schutzgut an.[62] Der datenschutzrechtliche Gesetzesvorbehalt als weitere Verarbeitungsvoraussetzung verweist auf die Anforderungen des Art. 7 b), c) RL 95/46/EG. Eine stärkere Einschränkung der Verarbeitungsanforderungen gegenüber der Richtlinie ist in den Abweichungen des Textes der Charta von der entsprechenden Regelung der Richtlinie nicht zu sehen.[63] Das Auskunftsrecht des Art. 8 Abs. 2 Satz 2 EU-GRC findet sich in Art. 10-12 der Richtlinie, die Überwachung durch eine unabhängige Stelle verweist auf Art. 28 RL 95/46/EG und war bereits in Art. 286 EGV a.F. enthalten.

Die enge Orientierung an der RL 95/46/EG bestätigen die Erläuterungen des Grundrechtskonvents zu Art. 8 EU-GRC, die gem. Art. 52 Abs. 7 EU-GRC und Art. 6 Abs. 1 Satz 3 EUV „gebührend" zu berücksichtigen sind: Art. 8 EU-GRC stützt sich danach auf die RL 95/46/EG. Diese enthalte zusammen mit der Verordnung über die Verarbeitung von Daten durch Organe und Einrichtungen der Union 45/2001/EG „Bedingungen und Beschränkungen für die Wahrnehmung des Rechts auf den Schutz personenbezogener Daten".[64] Auch die Rechtsprechung des EuGH bestätigt diese Konkretisierung anhand des Sekundärrechts, was wiederum in der Literatur aufgrund normsystematischer Unstimmigkeit kritisiert wird.[65] Die Befürchtung geht dahin, dass die sekundärrechtliche Vorprägung verhindert, dass das Grundrecht als Kontrollmaßstab gegenüber dem Sekundärrecht angewendet wird.[66] Diese Problematik zeigt sich in der Rechtssache *Bavarian Lager*.[67] Der Fall betraf den Antrag auf Zugang zu einem Kommissionsdokument, der auf den Verhaltenskodex über den Zugang der Öffentlichkeit zu Kommission- und Ratsdokumenten gestützt wurde. Der Antrag wurde u.a. aus Gründen des Datenschutzes abgelehnt. Es ging also um den Konflikt zwischen Datenschutz und Zugang zu Gemeinschaftsdokumenten.

Im Einzelnen: Der Bierimporteur Bavarian Lager verlangte Einsicht in das Protokoll eines Treffens im Rahmen eines von ihm angestoßenen Vertragsverletzungsverfahrens. Der vollständige Zugang wurde ihm jedoch verwehrt, da in dem Dokument personenbezogene Daten von Interessenvertretern enthalten waren, deren Einwilligung zur Veröffentlichung nicht erlangt werden konnte. Fraglich war nun, ob die Datenschutzregelungen der Zugangsverordnung 1049/2001/EG oder der Datenschutzverordnung 45/2001/EG anzuwenden waren und in welchem Verhält-

---

62 *Bernsdorff*, in: Meyer (Hrsg.), Charta, Art. 8 Rn. 21.

63 Ebd., Art. 8 Rn. 22.

64 Erläuterungen des Präsidiums des Europäischen Konvents, ABl. 2004, Nr. C 310, S. 431.

65 EuGH Urteil vom 14.9.2000 Rs. C-369/98 *(Agrardaten)* Rn. 31 ff. Anders jedoch die unten II.B.2.e), angesprochene Entscheidung *Österreichischer Rundfunk*; vgl. auch *Britz*, EuGRZ 2009, 1 (7) sowie *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II Rn. 44.

66 *Britz*, EuGRZ 2009, 1 (7).

67 EuGH Urteil vom 29.6.2010 Rs. C-28/08 P *(Bavarian Lager)*.

nis sie zueinander stehen. Das EuG als Vorinstanz wendete Art. 4 Abs. 1 b) VO 1049/2001/EG an und kontrollierte diese Vorschrift am Maßstab des Art. 8 EU-GRC. Das Grundrecht legt es allerdings – unter Berufung auf die ältere Rechtsprechung des EGMR – restriktiv aus und forderte einen Bezug zur Privatsphäre im engeren Sinne. Der EuGH sieht hierin einen Verstoß gegen den Wortlaut des Art. 4 Abs. 1 b) VO 1049/2001/EG, der „eine nicht aufspaltbare Bestimmung" darstelle und verlangt, dass „etwaige Beeinträchtigungen der Privatsphäre oder der Integrität des Einzelnen stets nach den Unionsvorschriften über den Schutz personenbezogener Daten, insbesondere der Verordnung Nr. 45/2001, geprüft und beurteilt werden". Weil die VO 45/2001/EG gerade den Schutz der Grundrechte und Grundfreiheiten zum Gegenstand habe, sei es unzulässig, die Verarbeitungsfälle in zwei Gruppen zu unterteilen und nur diejenigen Daten, die eine Beeinträchtigung im Sinne von Art. 8 Abs. 1 EMRK darstellen, auch am Maßstab der VO 45/2001/EG zu messen.[68] Beizupflichten ist dem EuGH zunächst deshalb, weil die Ansicht des EuG dazu führt, dass aufgrund der Rechtsprechung des EGMR dem Sekundärrecht ein geringeres Schutzniveau entnommen wird, womit nicht nur die Ausgestaltungsfunktion des Sekundärrechts einseitig verneint wird. Diese Auffassung führt überdies zu einer Konfusionslage im Hinblick auf die Funktion der EMRK. Anstatt die Grundrechtsverbürgungen als Schutzverstärkung anzuwenden, werden sie faktisch zur Eingriffsbegründung in Form der Zugangsgewährung herangezogen: Erst der Rekurs auf die Rechtsprechung des EGMR führt zu einer Nichtanwendung der VO 45/2001/EG. Die Entscheidung verdeutlicht damit die Relevanz unterschiedlicher Schutzbereichskonzeptionen auch auf Ebene des Unionsrechts. Zugleich zeigt sie die Gefahr der Grundrechtskonfusion in Privatrechtsverhältnissen. Die Untersuchung von Risikokonzeptionen muss somit in normsystematisch korrekter Weise erfolgen. Weiterhin ergibt sich aus der faktischen Ausgestaltungsfunktion des Sekundärrechts hinsichtlich Art. 8 EU-GRC die Notwendigkeit, die wichtigsten sekundärrechtlichen Regelungen in die Analyse einzubeziehen.

### 2. Risikokonzeptionen und Schutzgüter

Entgegen einer in der Literatur vertretenen Auffassung[69] lassen sich aus der älteren Rechtsprechung des EuGH, insbesondere aus den Rechtssachen *Stauder*[70] und *Adams*[71] noch keine Anhaltspunkte für die Anerkennung eines Datenschutzgrundrechts entnehmen.[72] Erstmals thematisiert wird der Datenschutz in einer Entschei-

---

[68] Ebd. Rn. 59 ff.

[69] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 16 AEUV Rn. 3.

[70] EuGH Urteil vom 12.11.1969 Rs. 29/69 *(Stauder)*.

[71] EuGH Urteil vom 7.11.1985 Rs. 145/83 *(Adams)*. Der Fall betrifft den Informantenschutz und dem Schutz beruflicher Geheimnisse, vgl. Rn. 34.

[72] So zu *Stauder* und *Adams* auch *Siemen*, Grundrecht, S. 214 und 220.

dung zu *Agrarsubventionsdaten* aus dem Jahr 2000.[73] Das Urteil betrifft die Frage, ob der neue Inhaber eines landwirtschaftlichen Betriebs von einer Behörde Angaben über die vom Vorbesitzer angebauten Pflanzen erhalten kann, die der neue Inhaber zur Beantragung bestimmter Zahlungen und zur Vermeidung von Sanktionen benötigte. Die Entscheidung enthält noch keine Auseinandersetzung mit einschlägigen Risiken. In der Folgezeit häufen sich dann jedoch Rechtssachen zu spezifisch datenschutzrechtlichen Fragen, die näher zu analysieren sind.

### *a) Personales Substrat und Gefährdungslagen*

Hinweise auf die Schutzgüter ergeben sich zunächst aus der Frage nach dem persönlichen Schutzbereich von Art. 8 EU-GRC. Hier wird teilweise vertreten, dass dieser für juristische Personen wegen des Bezugs des Rechts auf informationelle Selbstbestimmung zur Menschenwürde i.d.R. ausgeschlossen sei.[74] Jedoch darf nicht ohne weiteres von deutschen Besonderheiten auf die Auslegung des Art. 8 EU-GRC geschlossen werden. In der Entscheidung zu *Agrarbeihilfeempfängern* führt der EuGH aus, dass sich juristische Personen dann auf das Grundrecht berufen können, wenn ihr Name eine oder mehrere natürliche Personen bestimmt.[75] Es ist nicht klar, was das Gericht damit genau meint. Soweit es lediglich Personengesellschaften als erfasst ansieht, spricht hiergegen die Erwägung, dass Art. 8 EU-GRC ausdrücklich „Personen" und nicht – wie an anderer Stelle – „Menschen" erfasst und dass der Datenschutz nicht nur für den engeren Bereich von Intim- und Privatsphäre Bedeutung hat, sondern auch für Unternehmen. Insoweit besteht dann auch kein legitimer Anlass für eine Differenzierung zwischen Personen- und Kapitalgesellschaften.[76] Der EuGH führt zudem aus, dass die Verletzung des Rechts auf Schutz personenbezogener Daten bei juristischen Personen ein anderes Gewicht hat als bei natürlichen Personen, da juristische Personen bereits einer erweiterten Verpflichtung zur Veröffentlichung von Daten unterlägen. Für den Fall der Anwendbarkeit bekennt er sich deshalb zu einem geringeren Schutzstandard und hält die Veröffentlichung im konkreten Fall für mit der Charta vereinbar. Die Argumentation mit dem unterschiedlichem „Gewicht" der Eingriffe wird jedoch nicht näher präzisiert. Sie lässt zwar zunächst auf einen der Rechtsprechung zugrunde liegenden Würdebezug schließen; dieser wird allerdings dadurch relativiert, dass der EuGH die weitergehenden Veröffentlichungsvorschriften als Ursache des geringeren Schutzes ansieht. Dabei wird unzulässig von einer faktischen Gefährdungslage durch Veröffentlichungspflichten auf die weitergehende Zulässigkeit von Schutz-

---

[73] EuGH Urteil vom 14.9.2000 Rs. C-369/98 *(Agrarsubventionsdaten)*.

[74] *Bernsdorff*, in: Meyer (Hrsg.), Charta, Art. 8 Rn. 18.

[75] EuGH Urteil vom 9.11.2010 Rs. C-92/09 und C-93/09 *(Agrarbeihilfeempfänger)* Rn. 53.

[76] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 8 GRCh Rn. 11.

bereichsausnahmen geschlossen. Ein höherer Rang von Transparenzbestimmungen wird dabei wohl unterstellt, nicht jedoch begründet.

Fragwürdig sind sodann die ergänzenden Hinweise des EuGH, wonach die Prüfung, inwieweit der Name „natürliche Personen bestimmt", den Behörden eine unverhältnismäßige Verwaltungslast aufbürde.[77] Diese Argumentation wird von *Kühling* als „dogmatisch unausgereift" kritisiert. Zutreffend weist er darauf hin, dass ein Grundrechtseingriff nicht mit dem Argument gerechtfertigt werden könne, dass grundrechtskonformes Handeln der Verwaltung zu viel Aufwand bedeute.[78] Festzuhalten bleibt, dass der EuGH bezüglich des Schutzguts zwischen natürlichen und juristischen Personen differenziert und sich im Ergebnis der zu Art. 19 Abs. 3 GG vertretenen Theorie des personalen Substrats annähert.[79]

### *b) Ablösung vom Binnenmarktbezug*

Der sachliche Schutzbereich umfasst die Verarbeitung personenbezogener Daten. Fraglich ist, ob dies nur für Daten mit Binnenmarktrelevanz gilt. Hiergegen spricht jedoch der Verweis des Präsidiums des Grundrechtekonvents auf die Rechtstexte des Europarats.[80] Eine vergleichbare Voraussetzung wird dort nicht aufgestellt. Auch spricht die Aufnahme der Grundrechtecharta in das Primärrecht der Union für eine Akzentverschiebung in den Zielen der Union, in deren Konsequenz das Individuum und nicht mehr allein der Binnenmarkt im Zentrum des Unionshandelns steht.[81] Hiermit wird die bereits in den oben untersuchten Spezialinstrumenten[82] festzustellende wirtschaftspolitische Ausrichtung des Datenschutzes mit dem Schutzgut des freien Handels relativiert. Diese Ablösung vom Binnenmarktbezug wird im Folgenden insbesondere bei Zusammenschau mit Art. 16 AEUV deutlich.[83]

### *c) Risiken privater Datenverarbeitungen*

Die Rechtssachen *Lindqvist*,[84] *Promusicae*,[85] *Scarlet*,[86] *Netlog*,[87] und *Google Spain*[88] verdeutlichen, wie das Datenschutzgrundrecht zur Abwehr von Risiken

---

[77] EuGH Urteil vom 9.11.2010 Rs. C-92/09 und C-93/09 *(Agrarbeihilfeempfänger)* Rn. 87.

[78] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2. Aufl., S. 17 f.

[79] *Michael/Morlok*, Grundrechte Rn. 458.

[80] Erläuterungen des Präsidiums des Europäischen Konvents, ABl. 2004, Nr. C 310/431.

[81] *Bernsdorff*, in: Meyer (Hrsg.), Charta, Art. 8 Rn. 15a.

[82] Siehe oben Teil 1, II.A.2.d).

[83] Siehe unten II.C.

[84] EuGH Urteil vom 6.11.2003 Rs. C-101/01 *(Lindqvist)*.

[85] EuGH Urteil vom 29.1.2008 Rs. C-275/06 *(Promusicae)*.

privater Datenverarbeitungen dienen kann. Sie betreffen damit die in dogmatischer Hinsicht besonders problematische Frage nach der Privatrechtsgeltung bzw. Drittwirkung von Grundrechten.[89]

In der Rechtssache *Lindqvist*[90] hatte eine ehrenamtlich für eine Kirchengemeinde im Rahmen der Konfirmandenausbildung tätige Schwedin nach dem Besuch eines Informatikkurses eine Internetseite mit Informationen für Konfirmanden veröffentlicht. Darin nannte sie verschiedene Kollegen namentlich. Bei einigen bezeichnete sie Familienverhältnisse und Telefonnummer. Bei einer Kollegin wies sie darauf hin, dass sie sich am Fuß verletzt habe und krankgeschrieben sei. Eine Einwilligung der Betroffenen lag nicht vor, Frau *Lindqvist* hatte ihr Vorgehen auch nicht der schwedischen Datenschutzbehörde gemeldet. Nachdem sie erfahren hatte, dass ihre Kolleginnen die Seite missbilligten, entfernte sie diese sofort wieder. Gleichwohl leitete die Staatsanwaltschaft ein Strafverfahren gegen Frau *Lindqvist* wegen Verstoßes gegen das schwedische Datenschutzgesetz *(Personuppgiftslagen)* ein, was schließlich zur Verurteilung zu einer Geldstrafe führte. Der EuGH befasste sich in erster Linie mit der Frage, ob die Datenverarbeitungen in Form der Internetseite aus dem Anwendungsbereich der Richtlinie gem. Art. 3 Abs. 2 RL 95/46/EG herausfällt. Hinsichtlich der Variante des Art. 3 Abs. 2 erster Gedankenstrich folgt er dabei der bereits in der Entscheidung zum *Österreichischen Rundfunk* vertretenen Auffassung, wonach eine Beeinträchtigung des freien Marktes im Einzelfall nicht geprüft werden muss und hier eine generelle Betrachtungsweise zu einem weiten Anwendungsbereich des Gemeinschaftsrechts führt.[91] Auch die Ausnahme des Art. 3 Abs. 2 zweiter Gedankenstrich (Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten) hält der Gerichtshof bei einer Veröffentlichung im Internet für nicht erfüllt.[92] Eine der Vorlagefragen betraf den Widerspruch des Datenschutzes zum Grundsatz der Meinungsfreiheit. Der Gerichtshof löst diesen Konflikt durch einen Verweis auf das Regelungsgeflecht von Richtlinie, nationalen Regelungen und behördlicher Rechtsanwendungspraxis. Hierbei komme den Grundrechten eine besondere Bedeutung bei der Abwägung der Meinungsfreiheit von Frau *Lindqvist* mit dem Schutz der Privatsphäre betroffener Personen zu. Weil die Richtlinie genügend Spielraum für eine Umsetzung unter Wahrung des Verhältnismäßigkeitsgrundsatzes biete, läge kein Widerspruch zum Grundrecht der Meinungs-

---

[86] EuGH Urteil vom 29.11.2011 Rs. C-70/10 *(Scarlet)*.

[87] EuGH Urteil vom 16.2.2012 Rs. C-360/10 *(Netlog)*.

[88] EuGH Urteil vom 13.5.2014 Rs C-131/12 *(Google Spain)*.

[89] Dazu statt vieler *Badura*, Staatsrecht, C Rn. 22 f.

[90] EuGH Urteil vom 6.11.2003 Rs. C-101/01 *(Lindqvist)*.

[91] EuGH Urteil vom 6.11.2003 Rs. C-101/01 *(Lindqvist)* Rn. 42; EuGH Urteil vom 20.5.2003 verb. Rs. C 465/00, C-138/01 und C-139/01 *(Österreichischer Rundfunk)* Rn. 42.

[92] EuGH Urteil vom 6.11.2003 Rs. C-101/01 *(Lindqvist)* Rn. 47.

freiheit vor.[93] In der *Lindqvist*-Entscheidung nimmt der Gerichtshof damit keine eigene Abwägungsentscheidung vor und äußert sich deshalb auch nicht zu der Problematik, welche Risiken die datenschutzwidrige Veröffentlichung der Internetseite betrifft. Auch macht er – obwohl der Sachverhalt dies nahelegt – keine Ausführungen zur Grundrechtsgeltung im Privatrechtsverhältnis.

In der Rechtssache *Promusicae*[94] forderte ein Verband von Urheberrechtsinhabern von einem Internetanbieter die Herausgabe von (vorrätig gespeicherten) IP-Adressen zur Verfolgung von Urheberrechtsverletzungen. Der Internetanbieter lehnte die Offenlegung aus Gründen des Datenschutzes ab. Aussagekräftig, insbesondere hinsichtlich der Ausdehnung des Grundrechtsschutzes auf Privatrechtsverhältnisse durch Berufung auf den Anwendungsbereich des Sekundärrechts, ist der Schlussantrag der Generalanwältin *Kokott*. Darin führt sie aus, dass das Sekundärrecht grundrechtliche Vorgaben für den Datenschutz konkretisiert und sie in bestimmtem Umfang auf Einzelne ausdehnt. Damit verwirkliche und konkretisiere die Gemeinschaft ein aus dem Grundrecht auf Datenschutz folgendes Schutzziel.[95] Im Anschluss prüft *Kokott* die Rechtmäßigkeit von Ausnahmeregelungen zu den einschlägigen Verarbeitungsverboten gem. Art. 5 Abs. 1 und Art. 6 Abs. 1 der für die Bereitstellung elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen einschlägigen RL 2002/58/EG. Hierbei äußert sie sich an mehreren Stellen zu spezifischen Risiken, die aus der Verbindung staatlicher Informationssammlung und Erhebung durch private Stellen resultieren. So verweist sie zunächst unter Berufung auf die Rechtsprechung des BVerfG auf Zweifel an der Grundrechtsvereinbarkeit einer „Speicherung von Verkehrsdaten aller Nutzer gewissermaßen auf Vorrat", die dem Informationsersuchen der Urheberrechtsinhaber zugrunde lagen. Sie lässt die Frage nach der Rechtmäßigkeit der Vorratsdatenspeicherung jedoch offen.[96] Im Rahmen der Frage, ob Art. 15 Abs. 1 RL 2002/58/EG, der insbesondere Ausnahmeregelungen für die nationale und öffentliche Sicherheit sowie zur Verhütung von Straftaten und unzulässigem Gebrauch der Kommunikationssysteme ermöglicht, eng oder weit auszulegen ist, bezieht sich *Kokott* auf das Risiko des „gläsernen Bürgers". Eine weite Auslegung des Merkmals „unzulässiger Gebrauch", die darunter nicht nur einen Gebrauch fasst, der die Intaktheit oder Sicherheit des Systems infrage stellt, sondern auch den Gebrauch für unzulässige Zwecke, würde den Schutz des Kommunikationsgeheimnisses entleeren. Eine diesbezügliche Prüfung erfordere die Speicherung der gesamten Kommunikation und eine intensive Inhaltskontrolle. Der „gläserne Bürger" würde damit Realität. *Kokott* kommt zu dem Ergebnis, dass der unzulässige Gebrauch deshalb nur den systemwidrigen Gebrauch, nicht aber den Gebrauch zu unzulässigen Zwecken erfasst.[97]

---

[93] Ebd. Rn. 87–90.

[94] EuGH Urteil vom 29.1.2008 Rs. C-275/06 *(Promusicae)*.

[95] GA *Kokott*, Rs. C-275/06, Schlussanträge zur Rechtssache *Promusicae* Rn. 57.

[96] Ebd. Rn. 82.

[97] Ebd. Rn. 92–98.

Der Gerichtshof hat sich dieser auch von der Kommission vertretenen Auffassung angeschlossen.[98] Hier zeigt sich nun, wie das spezifische Risiko individueller Transparenz durch häufige und umfassende Inhaltskontrollen – ein Risiko, das mit dem oben erarbeiteten Überwachungsdruck zu verbinden ist – der Richtlinienauslegung zugrunde gelegt wird: Zwar steht dabei noch das Risiko staatlicher Datenerhebungen im Vordergrund. Bei der Frage, inwieweit es den Mitgliedstaaten gestattet wäre, in Ausfüllung des Art. 15 Abs. 1 Var. 3 und 4 RL 2002/58/EG die Weitergabe personengebundener Verkehrsdaten zu ermöglichen, widmet sich *Kokott* jedoch dem spezifisch aus einem staatlich-privaten Informationsverbund folgenden Risiko. Sie führt aus, dass die unmittelbare Weitergabe an staatliche Stellen ein milderes Mittel im Vergleich zur Weitergabe an die Urheberrechtsinhaber sein kann, da staatliche Stellen zum einen unmittelbar an die Grundrechte gebunden seien und Verfahrensrechte garantieren müssen und ihnen zum anderen ein objektiveres Aufklärungsinteresse zukomme. So hätten im Fall des infrage stehenden „filesharing" Private kein Interesse daran, aufzuklären oder auch nur zu berücksichtigen, ob tatsächlich eine andere Person – beispielsweise durch unbefugte Nutzung eines WLAN – die Datei heruntergeladen hat.[99] *Kokott* weist damit auf das Risiko mangelnder Objektivität und Gewinnorientierung Privater hin, wie es sich beispielsweise auch in vergleichbaren Abmahnfällen in Deutschland manifestiert hat.[100] Dieses Risiko lässt sich auch als Risiko individueller Verletzlichkeit durch Missbrauch – im Beispielsfall die aufgrund des Gewinnstrebens zumindest in Kauf genommene Rechtsverfolgung gegenüber Nichtstörern – beschreiben. *Kokotts* Argumentation müsste indes insoweit ergänzt werden, als auch eine durch Private angestoßene Verfolgung von Urheberrechtsverletzungen sowohl im Zivil- als auch im Strafrecht letztlich vor den objektiven staatlichen Stellen durchgesetzt wird. Die Risiken mangelnder Verfahrensvorschriften und gewinnorientierter Rechtsverfolgung liegen somit nicht schon in der Einbindung Privater als solcher, sondern in einer mangelhaften verfahrensmäßigen Ausgestaltung, die beispielsweise Anreize zu undifferenziertem und massenhaftem Abmahnen setzt.[101] Die Entscheidung des Gerichtshofs enthält im Gegensatz zu den Schlussanträgen der GA keine im Hinblick auf die Konturierung des Schutzguts relevante Erörterung von Risiken.

Die Entscheidungen *Scarlet*[102] und *Netlog*[103] betreffen die Verpflichtung von Diensteanbietern zur Einrichtung eines Filter- und Sperrsystems, um urheber-

---

98 EuGH Urteil vom 29.1.2008 Rs. C-275/06 *(Promusicae)* Rn. 52.

99 GA *Kokott*, Rs. C-275/06, Schlussanträge zur Rechtssache Promusicae Rn. 113–116.

100 Vgl. *Möller*, NJW 2011, 2560 ff. sowie zu Reformvorschlägen zur Minderung des „Abmahnunwesens"; vgl. http://www.heise.de/newsticker/meldung/Justizministerin-erlaeutert-Vorstoss-gegen-das-Abmahnunwesen-1468162.html [Stand: 28.3.2014].

101 Sinnvoll sind deshalb Vorschriften wie § 97a Abs. 2 UrhG, der die Höhe der Abmahnkosten begrenzt.

102 EuGH Urteil vom 29.11.2011 Rs. C-70/10 *(Scarlet)*.

103 EuGH Urteil vom 16.2.2012 Rs. C-360/10 *(Netlog)*.

rechtsverletzenden Dateiaustausch zu verhindern. Die belgische Verwertungsgesellschaft *Sabam* wollte die Anbieter im Wege einer gerichtlichen Anordnung hierzu verpflichten. In dem der Entscheidung *Scarlet* zugrunde liegenden Sachverhalt ging die *Sabam* gegen einen Internetzugangsanbieter vor, im Fall *Netlog* handelte es sich um ein soziales Netzwerk.

Der EuGH hält derartige Anordnungen zum einen für unvereinbar mit Art. 15 Abs. 1 RL 2000/31/EG, der die Verpflichtung von Hosting-Betreibern zu genereller Überwachung gespeicherter Informationen verbietet.[104] Weiterhin beeinträchtige eine derartige Verpflichtung die unternehmerische Freiheit der Diensteanbieter gem. Art. 17 EU-GRC sowie Art. 3 Abs. 1 RL 2004/48/EG, wonach Maßnahmen zur Durchsetzung geistiger Eigentumsrechte gerecht und verhältnismäßig und nicht übermäßig kostspielig sein dürfen.[105] Auch Art. 8 EU-GRC hält der EuGH für einschlägig: Die Ausführungen des Gerichtshofs beschränken sich jedoch in der *Scarlet*-Entscheidung auf die Feststellung, dass die Einrichtung eines derartigen Filtersystems eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen der Nutzer bedeuten würde, wobei er in den IP-Adressen aufgrund der Möglichkeit einer „genauen Identifizierung" personenbezogene Daten sieht.[106] In der *Netlog*-Entscheidung ist es die systematische Prüfung und Verarbeitung der Nutzerprofile des sozialen Netzwerks, die als Risiko bezeichnet wird. Die Nutzerprofile werden ebenfalls als personenbezogene Daten angesehen.[107] Die Entscheidungen enthalten im Übrigen keine nähere Auseinandersetzung mit einschlägigen Risiken und nehmen auch zu dem sich aufdrängenden Problem der Grundrechtsgeltung zwischen Privaten nicht Stellung. Insgesamt bleibt die Befassung des EuGH mit den Risiken privater Datenverarbeitungen damit begrenzt. Die substanziellsten Ausführungen sind im Schlussantrag der GA *Kokott* enthalten und beziehen sich einerseits auf die Auslösung eines Überwachungsdrucks und andererseits auf die aus der fehlenden Objektivität folgende Erhöhung individueller Verletzlichkeit im Fall eines „Abmahnmissbrauchs".

Risiken privater Datenverarbeitungen greifen auch die Schlussanträge des GA *Jääskinen* in der Rechtssache *Google Spain SL* auf.[108] Das Verfahren hat die Frage von Löschungspflichten des Suchmaschinenbetreibers Google wegen einer nachträglichen Online-Veröffentlichung zweier Zeitungsartikel, die personenbezogene Daten enthielten, zum Gegenstand. In den verlinkten Zeitungsartikeln wurde auf die Versteigerung des Grundstücks des Klägers wegen einer Pfändung aufgrund von Sozialversicherungsforderungen hingewiesen.

---

[104] EuGH Urteil vom 29.11.2011 Rs. C-70/10 *(Scarlet)* Rn. 40; EuGH Urteil vom 16.2.2012 Rs. C-360/10 *(Netlog)* Rn. 38.

[105] EuGH Urteil vom 29.11.2011 Rs. C-70/10 *(Scarlet)* Rn. 43, 48; EuGH Urteil vom 16.2.2012 Rs. C-360/10 *(Netlog)* Rn. 41, 46.

[106] EuGH Urteil vom 29.11.2011 Rs. C-70/10 *(Scarlet)* Rn. 51.

[107] EuGH Urteil vom 16.2.2012 Rs. C-360/10 *(Netlog)* Rn. 49.

[108] GA *Jääskinen*, Schlussanträge vom 25.6.2013 zur Rechtssache C-131/12 *(Google Spain)*.

Die Schlussanträge befassen sich in erster Linie mit der Frage der Anwendbarkeit der Datenschutzrichtlinie, der datenschutzrechtlichen Verantwortlicheneigenschaft von Google und dem Löschungsrecht in Art. 12 b) der Datenschutzrichtlinie. *Jääskinen* plädiert für eine relativ enge Auslegung des Begriffs des „für die Verarbeitung Verantwortlichen" im Sinne des Art. 2 d) der Datenschutzrichtlinie.[109] Im Übrigen wird das Risiko der Profilbildung und der Informationspermanenz lediglich am Rande und ohne weitere Vertiefung angesprochen.[110] GA *Jääskinen* plädiert wegen der Gefahren für die Grundrechte der Meinungs- und Informationsfreiheit der Suchmaschinenbetreiber und deren auf die bloße Vermittlung zwischen Urheber und Betroffenem beschränkten Rolle gegen ein aus Art. 7 EU-GRC abzuleitendes „Recht auf Vergessen".[111] Darüber hinaus spricht er sich gegen eine weite Auslegung der Löschungspflicht aus und betont die Notwendigkeit der Abwägung mit Gegenrechten der verarbeitenden Stellen.[112]

In dem darauffolgenden Urteil zur Rechtssache *Google Spain*[113] folgt der Gerichtshof nicht den Schlussanträgen und stuft Google als Verantwortlichen im Sinne von Art. 2 d) ein, da ein anderes Ergebnis weder mit dem Wortlaut der Vorschrift noch mit deren umfassendem Schutzzweck zu vereinbaren sei.[114] Der Gerichtshof verweist sodann auf den strukturierten Überblick in Form eines detaillierten Profils, das sich durch eine Namenssuche gewinnen lasse, und folgert hieraus eine erhebliche Beeinträchtigung von Art. 7 und Art. 8 EU-GRC.[115] Daran ändere sich nichts durch den fehlenden Einsatz bestimmter Techniken, mit denen der Seitenbetreiber der Suchmaschine den automatisierten Zugang verwehren könnte, da Art. 2 d) der Datenschutzrichtlinie nicht auch denjenigen als Verantwortlichen einstuft, der gemeinsam mit anderen über die Mittel der Verarbeitung entscheidet.[116] Der Gerichtshof befasst sich sodann ausführlich mit den Fragen des räumlichen Anwendungsbereichs der Richtlinie.[117] Hinsichtlich einschlägiger Risiken bleiben die Entscheidungsgründe dagegen zunächst eher oberflächlich: Der Gerichtshof verweist auf seine Ausführungen zur Namenssuche und darauf, dass die „im Internet zu findenden Informationen" „potenziell zahlreiche Aspekte des Privatlebens" betreffen. Diese wären ohne die Suchmaschine nicht oder nur sehr schwer miteinander verknüpfbar. Die Wirkung des Eingriffs würde zudem durch die „Rolle des Internets und der Suchmaschinen in der modernen Gesellschaft ge-

---

109 Ebd. Rn. 81, 89.

110 Ebd. Rn. 44.

111 Ebd. Rn. 109, 133 f.

112 Ebd. Rn. 119 ff.

113 EuGH Urteil vom 13.5.2014 Rs C-131/12 *(Google Spain)*.

114 Ebd. Rn. 33 f.

115 Ebd. Rn. 37 f.

116 Ebd. Rn. 39 f.

117 Ebd. Rn. 42–60.

steigert", was der Ergebnisliste „Ubiquität" verleihe.[118] Im Ergebnis bejaht der Gerichtshof dann grundsätzlich die Pflicht zur Entfernung entsprechender Links.[119]

Beachtenswert ist dann jedoch die am Ende zu den Vorschriften über die normative Zweckbegrenzung, Art. 6 Abs. 1 c)–e), der Datenschutzrichtlinie getroffene Feststellung, wonach „auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entsprechen kann, wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet worden sind, nicht mehr erforderlich sind". Dies sei insbesondere der Fall, „wenn sie diesen Zwecken in Anbetracht der verstrichenen Zeit nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen".[120] Die Rechte des Betroffenen überwiegen danach „grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit daran, die Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche zu finden". Dies sei nur dann nicht der Fall, „wenn sich aus besonderen Gründen – wie der Rolle der betreffenden Person im öffentlichen Leben – ergeben sollte, dass der Eingriff in die Grundrechte dieser Person durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt" sei.[121]

Das Urteil betrifft damit in erster Linie das Risiko der Informationspermanenz. Die zugrunde liegenden Erwägungen stützen dabei das oben anhand der Rechtsprechung des EGMR entwickelte Konzept einer Informationsverjährung.[122] Außerdem konkretisiert die Entscheidung das Risiko der Informationspermanenz für das hierfür sicherlich charakteristischste Beispiel der Namenssuche im Internet. Dabei wird auf den später noch näher zu besprechenden Argumentationstopos der Profilbildung eingegangen. Weiterhin deutet der EuGH mit den Verknüpfungsmöglichkeiten zu den anderweitig nicht auffindbaren „potenziell zahlreichen Aspekten des Privatlebens" das Risiko der Entkontextualisierung an.

#### *d) Staatliche Nutzung privater Datenbestände*

Die Risiken der staatlichen Nutzung privater Datenbestände werden zuerst im Zusammenhang mit *Fluggastdaten*, dann im Kontext der *Vorratsspeicherung* in Urteilen des EuGH und Schlussanträgen der Generalanwälte thematisiert. Am Beginn der Analyse steht deshalb der Schlussantrag des GA *Leger* zum *Fluggast-*

---

118 Ebd. Rn. 80.

119 Ebd. Rn. 88.

120 Ebd. Rn. 93.

121 Ebd. Rn. 97.

122 Siehe oben Teil 1, IV.B.3.a).

*daten*-Urteil des EuGH.[123] Diese Entscheidung betrifft ein zunächst bis Oktober 2006 gültiges Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Departement of Homeland Security.[124] Dieses Abkommen wurde in Folge der New Yorker Anschläge vom 11.9.2001 im Jahr 2004 geschlossen, um dem Zugangswunsch der USA zum Zweck der Terrorabwehr in einer mit europäischen Datenschutzvorstellungen konformen Weise nachzukommen. Die Passagierdaten umfassen Angaben, die Fluggäste üblicherweise im Zusammenhang mit der Reisebuchung der Fluggesellschaft bzw. dem Reisebüro anvertrauen. Die Informationen werden als Passenger Name Record (PNR) gespeichert. Neben Name, Anschrift, Telefonnummer und Kreditkartennummer enthalten die Datensätze auch Informationen über die Inanspruchnahme von Zusatzdienstleistungen an Bord des Flugzeugs und weitere Informationen zur Reise, wie beispielsweise Buchungen von Mietwagen oder Hotels. Die Informationen können dabei nicht nur die Reiseplanung offenbaren, sondern auch Rückschlüsse auf Religion, Weltanschauung und Gesundheitszustand zulassen (beispielsweise bestimmte Essenspräferenzen, Erfordernis von Rollstuhlplätzen im Flugzeug etc.). Das ursprüngliche Abkommen von März 2004 wurde infolge des EuGH-Urteils zu den Fluggastdaten am 31.7.2007 durch ein Interimsabkommen vom 16.10.2006[125] abgelöst. Dieses Abkommen lief am 31.7.2007 aus und wurde am 4.8.2007 durch ein weiteres ersetzt.[126] Im November 2011 wurde ein neues Abkommen verhandelt – das Europaparlament stimmte am 19.4.2012 zu,[127] was erneut zu heftiger Kritik vonseiten der Datenschützer führte.[128] Das geltende Abkommen ist am 1.7.2012 in Kraft getreten.[129]

---

[123] GA *Leger*, Schlussanträge vom 22.11.2005 zu EuGH Urteil vom 30.5.2006 Rs. C-317/04, C-318/04 (*Fluggastdaten*-Schlussanträge) Rn. 145 ff.

[124] ABl. 2004 L 183, S. 83, berichtigt im ABl. 2005, L 255, S. 168.

[125] ABl. 2006 L 298, S. 27.

[126] ABl. 2004 L 204, S. 16. Zum Ganzen http://www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/DerGlaesernePassagier.html?nn=409532 [Stand: 28.3.2014].

[127] Legislative Entschließung des Europäischen Parlaments vom 19.4.2012 zu dem Entwurf eines Beschlusses des Rates über den Abschluss des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security (17433/2011 – C7-0511/2011 – 2011/0382(NLE)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0134&language=DE&ring=A7-2012-0099 [Stand: 28.3.2014].

[128] http://www.zeit.de/digital/datenschutz/2012-04/fluggastdaten-usa-eu-parlament [Stand: 28.3.2014].

[129] Joint Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, SEC(2013) 630 final, S. 2.

Die Schlussanträge des GA *Leger* betreffen das erste Abkommen von 2004. Obwohl sie sich ganz überwiegend mit kompetenziellen Fragestellungen beschäftigen, verdeutlichen sie an verschiedenen Stellen einschlägige Risiken. Zunächst befasst sich *Leger* mit den Zielen des Abkommens, um zu prüfen, ob Art. 95 EGV a.F. als Rechtsgrundlage gewählt werden konnte. Dabei nimmt er zunächst Bezug auf die beiden im Abkommen ausdrücklich genannten Ziele des Kampfes gegen den Terrorismus und des Schutzes personenbezogener Daten, um dann zu klären, in welchem Verhältnis das vom Rat genannte Ziel der Verhinderung von Wettbewerbsverzerrungen zwischen den Fluggesellschaften hierzu steht. Dabei stellt *Leger* fest, dass ein solches Ziel allenfalls akzessorischer Natur sei und im Vergleich zu den beiden Hauptzielen im Hinblick auf Art. 95 EGV a.F. zurückzutreten habe.[130]

Hier zeigt sich, dass die mittelbaren und jeder Regulierung immanenten Einflüsse auf den Wettbewerb nicht zur Aktivierung des Art. 95 EGV a.F. herangezogen werden konnten. Daraus kann hingegen nicht der Schluss gezogen werden, dass bloß mittelbare Auswirkungen auf den Wettbewerb als eigenständig erfasstes Datenschutzrisiko ausscheiden. Die Argumentation des GA bezieht sich allein auf die Auslegung des Art. 95 EGV a.F. und steht nicht im Zusammenhang mit materiellem Datenschutzrecht. Etwas anderes gilt jedoch für die Ausführungen, in denen *Leger* die Stellungnahme des Datenschutzbeauftragten aufgreift. Dieser ging davon aus, dass sechs der insgesamt 34 Datenelemente eine Verletzung des Rechts auf Privatsphäre bewirken, weil hierdurch die Erstellung von Persönlichkeitsprofilen möglich sei. Bei den gerügten Datenelementen handelt es sich um die Einträge: Vielflieger-Eigenschaften (u.a. abgeflogene Meilen), allgemeine Bemerkungen, spezielle Service-Anforderungen OSI und SSR,[131] Zahl der Reisenden im PNR und APIS-Einträge.[132] Die Informationen erlauben weitreichende Rückschlüsse über sozioökonomischen Status, Religionszugehörigkeit und Reiseverhalten. Der Rat räumt dies indirekt ein, indem er auf die Notwendigkeit hinweist, „das Profil potenzieller Terroristen zu erstellen". Dies setze den Zugang zu einer größeren Anzahl von Daten voraus.[133] Leger bejaht in seiner Würdigung den Eingriff in das Privatleben durch die PNR-Datenelemente, auch wenn er bei einzelnen keine Beeinträchtigung erkennen kann. Die Liste der PNR-Datenelemente sei als Ganzes zu betrachten, der Abgleich erlaube die Bildung von Persönlichkeitsprofilen. Sodann folgt *Leger* jedoch der Ansicht des Rats und unterstreicht im Rahmen der Verhält-

---

130 GA *Leger*, Schlussanträge vom 22.11.2005 zu EuGH Urteil vom 30.5.2006 Rs. C-317/04, C-318/04 (*Fluggastdaten*-Schlussanträge*)* Rn. 150.

131 Hierunter werden Informationen zu besonderen Eigenschaften, wie „Reisende mit Kind" bzw. zu besonderen Anforderungen, wie „Essen ohne Schweinefleisch", erfasst, vgl. http://www.passagierrecht.de/html/fluggastdaten-pnr-21-30.html [Stand: 28.3.2014].

132 U.a. beim Check-In erfasste Vorab-Daten, insb. der Ausweispapiere, können aber z.B. auch die erste Adresse bei einer Reise in die USA enthalten, vgl. http://www.passagierrecht.de/html/fluggastdaten-pnr-31-34.html [Stand: 28.3.2014].

133 GA Leger, Schlussanträge vom 22.11.2005 zu EuGH Urteil vom 30.5.2006 Rs. C-317/04, C-318/04 (*Fluggastdaten*-Schlussanträge) Rn. 203.

nismäßigkeitsprüfung die Bedeutung und den Ermittlungsnutzen der Informationen.[134]

Neben der Anerkennung der Profilbildung als Risiko bleibt er somit hinsichtlich der Notwendigkeit eines Persönlichkeitsbezugs der Daten zunächst unbestimmt; indem er auf die Gesamtbetrachtung abstellt, bejaht er diesen aber indirekt. In seiner Entscheidung geht der EuGH nicht weiter auf einschlägige Risiken ein, da die angefochtene Angemessenheitsentscheidung der Kommission und der Beschluss des Rates bereits aus kompetenziellen Gründen nichtig waren.[135] Festzuhalten ist damit die Einbeziehung des Risikos der Erstellung von Persönlichkeitsprofilen. Die Fluggastdaten stehen dabei beispielhaft für die Vielfalt von Informationen, die bei privaten Dienstleistungsunternehmen zur Verfügung stehen. Bedient sich der Staat aus diesem Informationsfundus, so potenziert sich das Risiko durch den massiven Anstieg der Aussagekraft der erlangten Informationen. Hierin liegt das spezifische Risiko staatlicher Nutzung privater Datenbestände.

In Zusammenhang mit diesem Risiko ist auch der Komplex *Vorratsspeicherung von Telekommunikationsverbindungsdaten* zu sehen. In dem hierzu am 8.4.2014 ergangenen Urteil des EuGH[136] wird das Risiko jedoch nur in Ansätzen behandelt: Der Gerichtshof entschied, dass die – im Abschnitt über das Sekundärrecht noch näher zu analysierende[137] – Vorratsspeicherungsrichtlinie[138] den Verhältnismäßigkeitsgrundsatz in Bezug auf Art. 7, 8 und 52 EU-GRC verletzt und deshalb ungültig ist.

Das Urteil geht zurück auf die Vorabentscheidungsersuchen des irischen High Court und des österreichischen Verfassungsgerichtshofs. In beiden Ausgangsverfahren wurden nationale Umsetzungsakte angegriffen. Der Gerichtshof prüfte die Richtlinie hauptsächlich anhand von Art. 7 und Art. 8 EU-GRC,[139] wobei er zu deren Konkretisierung auch auf Entscheidungen des EGMR zurückgreift.[140] Die Freiheit der Meinungsäußerung, Art. 11 EU-GRC, wird zwar ebenfalls als Maßstab genannt, die Prüfung dieses Grundrechts unterbleibt dann jedoch, da der Gerichtshof bereits eine Verletzung der Verhältnismäßigkeit in Bezug auf Art. 7, 8 und 52

---

134 Ebd. Rn. 238 ff.

135 EuGH Urteil vom 30.5.2006 Rs. C-317/04, C-318/04 *(Fluggastdaten)* Rn. 58–61 sowie Rn. 67–70.

136 EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* = BeckRS 2014, 80686.

137 Siehe unten III.D.

138 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105/54.

139 EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* Rn. 23.

140 Ebd. Rn. 35.

EU-GRC annimmt.[141] Zu dem Ergebnis der Ungültigkeit wegen Unverhältnismäßigkeit kommt der Gerichtshof, nachdem er zunächst die „Relevanz" der Art. 7, 8 und 11 EU-GRC bejaht, weil aus den gespeicherten Daten „sehr genaue Schlüsse" auf das Privatleben Betroffener gezogen werden könnten.[142] Es sei nicht auszuschließen, dass sich die Vorratsspeicherung auf die Ausübung der Meinungsfreiheit auswirke.[143] In der Verpflichtung Privater zur Vorratsspeicherung liege ein Eingriff in Art. 7 EU-GRC; ein weiterer liege in dem Zugang der nationalen Behörden zu den Daten.[144] Da die Richtlinie eine Verarbeitung personenbezogener Daten vorsehe, liege auch ein Eingriff in Art. 8 EU-GRC vor.[145] Der Eingriff sei wegen des Umstands, dass die Teilnehmer nicht darüber informiert würden, auch als besonders schwerwiegend anzusehen. Hierbei verweist der EuGH auf die zum Rechtsstreit ergangenen Schlussanträge von Generalanwalt *Villalón* vom 12.12.2013:[146] Die Vorratsspeicherung sei dazu geeignet, ein Gefühl der ständigen Überwachung des Privatlebens auszulösen. *Villalón* relativiert diese Aussage in seinen Schlussanträgen jedoch: Es sei „darauf hinzuweisen, dass – abgesehen davon, dass der Gerichtshof nicht über genügend Informationen verfügt, um sich hierzu äußern zu können – dieser Effekt nur eine Nebenfolge eines Eingriffs in das Recht auf Achtung des Privatlebens" sei.[147] An einer späteren Stelle begründet er seine Annahme eines „diffusen Gefühls des Überwachtwerdens" mit der Möglichkeit vergangenheitsbezogener Auswertungen der Daten und verweist hierbei auf die Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung,[148] aus der dieses Argument übernommen wurde. Das Argument, das in seinem Risikogehalt im Rahmen des Dritten Teils noch näher analysiert wird,[149] enthält aufgrund der Enthüllungen von *Edward Snowden* hinsichtlich der NSA-Überwachungsprogramme „Mystic" und „Retro" einen besonderen Stellenwert. Denn mit diesen Programmen soll die NSA die Fähigkeit erprobt haben, alle Telefongespräche eines Landes für einen Zeitraum von 30 Tagen aufzuzeichnen, um damit eine vergangenheitsbezogene Auswertung vorzunehmen.[150] Der Unterschied zu der Überwachung nach der Vorratsspeicherungsrichtlinie liegt jedoch darin, dass sich die Speicherungspflicht der Richtlinie nicht auf die Inhaltsdaten bezog. Doch auch die Erfassung der in Art. 5 der Vorratsspeicherungsrichtlinie genannten Daten stellt nach Villalón einen

---

141 Ebd. Rn. 69 f.

142 Ebd. Rn. 27.

143 Ebd. Rn. 28.

144 Ebd. Rn. 34 f.

145 Ebd. Rn. 36.

146 GA *Villalón*, Schlussanträge vom 12.12.2013 zu EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* Rn. 52, 72.

147 Ebd. Rn. 52.

148 BVerfGE 125, 260.

149 Siehe unten Teil 3, II.B.9.a).

150 http://www.heise.de/tp/artikel/41/41280/1.html [Stand: 11.5.2014].

qualifizierten Eingriff dar, da „deren Auswertung es ermöglichen kann, eine ebenso zuverlässige wie erschöpfende Kartografie eines erheblichen Teils der Verhaltensweisen einer Person, die allein ihr Privatleben betreffen, oder gar ein komplettes und genaues Abbild der privaten Identität dieser Person zu erstellen".

Wegen der Nichterfassung des Kommunikationsinhalts kommt der EuGH dann zum Ergebnis, dass der Wesensgehalt (Art. 52 Abs. 1 EU-GRC) des Art. 7 EU-GRC nicht angetastet werde. Für Art. 8 EU-GRC folge dies daraus, dass die speichernden Stellen bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssten, und darüber hinaus daraus, dass „geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen".[151] Der Verhältnismäßigkeitsverstoß folgert der EuGH dann aus fehlenden Einschränkungen für Personen, „bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte" sowie für Berufsgeheimnisträger.[152] Weiterhin erfordere die Richtlinie keinen Zusammenhang zwischen den gespeicherten Daten und der Bedrohung der öffentlichen Sicherheit, insbesondere erfordere sie keinen dahingehenden zeitlichen, örtlichen oder personalen Zusammenhang.[153] Darüber hinaus genüge auch die Regelung des Zugangs der nationalen Behörden und der Speicherungsdauer nicht dem Erforderlichkeitsgrundsatz, insbesondere mangels „objektiver Kriterien" zur Beschränkung des zugangsberechtigten Personenkreises und der Speicherdauer.[154] Explizit beanstandet wird sodann das Fehlen von Garantien zum Schutz vor „Missbrauchsrisiken", zur Sicherstellung der unwiderruflichen Vernichtung nach Ablauf der Speicherungsfrist und der Belassung der Daten im Unionsgebiet zur Sicherstellung der unabhängigen Überwachung.[155]

Urteil und Schlussanträge betreffen damit zwar die staatliche Nutzung privater Datenbestände, greifen einschlägige Risiken jedoch nur in Ansätzen auf. Einbezogen werden etwa die Informationspermanenz[156] oder das Risiko informationsbedingter Verhaltensänderungen.[157] Im weiteren Sinne lässt sich auch aus der allgemeinen Argumentation mit „Missbrauchsrisiken"[158] auf das Risiko der indivi-

---

[151] EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* Rn. 40.

[152] Ebd. Rn. 58.

[153] Ebd. Rn. 59.

[154] Ebd. Rn. 60–64.

[155] Ebd. Rn. 66–68.

[156] Ebd. Rn. 67; GA *Villalón*, Schlussanträge vom 12.12.2013 zu EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* Rn. 72.

[157] Ebd. Rn. 52.

[158] EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* Rn. 66.

duellen Verletzlichkeit Betroffener schließen. Abgesehen von dem Verweis auf „Überwachungsgefühle“ in den Ausführungen des Generalanwalts bleibt die Annahme der besonderen Eingriffsschwere im Urteil jedoch unbegründet. Gleiches gilt für die Verneinung der Wesensgehaltsantastung, die lediglich mit der fehlenden Inhaltsüberwachung und der grundsätzlichen Existenz von Datenschutzvorschriften begründet wird.[159] Die dortigen Ausführungen bezüglich des Schutzes der Daten gegen zufällige oder unrechtmäßige Zerstörung sind hingegen nicht nachzuvollziehen, da die Zerstörung (also Löschung) von zu Überwachungszwecken gespeicherten Daten offensichtlich für die von der Überwachung betroffenen Bürger nicht nachteilig ist.

Risiken durch die staatliche Nutzung privater Datenbestände werden somit in der Rechtsprechung des EuGH und den Schlussanträgen in Sachen Fluggastdaten und Vorratsspeicherung erst in Ansätzen thematisiert, wobei teilweise auf Risikokonzeptionen anderer Rechtsebenen zurückgegriffen wird (wie z.B. durch den Verweis von GA *Villalón* auf die Entscheidung des BVerfG zur Vorratsdatenspeicherung. Insgesamt zeigt sich, dass die Einschaltung privater Stellen aufgrund der Vielzahl und Aussagekraft der dort vorhandenen Daten (man denke nur an Suchmaschinenbetreiber oder Telekommunikationsanbieter) weniger ein eigenständiges Risiko als vielmehr einen Potenzierungsfaktor für andere Risiken darstellt.

### *e) Grenzen der Transparenz*

Die Rechtssachen *Österreichischer Rundfunk*,[160] *Satamedia*,[161] *Bavarian Lager*[162] und *Agrarbeihilfeempfänger*[163] betreffen Konstellationen, in denen der Datenschutz Transparenzbestimmungen und der Ausübung der Meinungsfreiheit eine Grenze setzt und damit das Risiko von Publizitätsschäden im weiteren Sinne aufgreift.

In den bereits oben[164] angesprochenen Fällen *Österreichischer Rundfunk* und *Bavarian Lager* befassen sich die europäischen Gerichte und Generalanwälte jedoch nur in geringem Maße mit Risiken, die sich aus dem Transparenzanliegen ergeben. So bejaht der EuGH im Fall *Österreichischer Rundfunk*, in dem es um die Publikation von Gehaltsdaten bestimmter Spitzenbeamter bei der Kontrolltätigkeit des Rechnungshofes ging, den Eingriff in knapper Form: Dieser liege zwar nicht schon in der bloßen Speicherung durch den Arbeitgeber; die Weitergabe der Ge-

---

159 Ebd. Rn. 37, 39 f.

160 EuGH Urteil vom 20.5.2003 Rs. C-465/00, C-138/01, C-139/01 *(Österreichischer Rundfunk)*.

161 EuGH Urteil vom 16.12.2008 Rs. C-73/07 *(Satamedia)*.

162 EuGH Urteil vom 29.6.2010 Rs. C-28/08 P *(Bavarian Lager)*.

163 EuGH Urteil vom 9.11.2010 Rs. C-92/09 und C-93/09 *(Agrarbeihilfeempfänger)*.

164 Siehe I.A.

haltsdaten an die Behörde begründe jedoch den Eingriff unabhängig von der Frage, ob die Informationen sensibel seien.[165] In der Notwendigkeitsprüfung widmet sich der Gerichtshof der Schwere der Beeinträchtigung des Rechts auf Achtung des Privatlebens. Hierzu führt er jedoch lediglich an, dass sich die Veröffentlichung des beruflichen Einkommens negativ auf die Einstellungsmöglichkeiten bei anderen Unternehmen, die nicht der Kontrolle des Rechnungshofes unterliegen, auswirken könne.[166] Die Schlussanträge des GA *Tizzano* verweisen zudem auf die Abschreckungswirkung der Transparenzbestimmungen gegenüber den Angehörigen anderer Mitgliedstaaten, die einen Arbeitsplatzwechsel zu den der Rechnungshofkontrolle unterliegenden Einrichtungen anstreben.[167]

In der Entscheidung *Bavarian Lager,* die den ungekürzten Zugang zu Protokollen aus einem Treffen von Interessen- und Kommissionsvertretern im Rahmen eines Vertragsverletzungsverfahrens zum Gegenstand hatte, finden sich keine substantiierten Ausführungen zu betroffenen Risiken. Auch die Frage nach dem Privatlebensbezug – die eine Stellungnahme zu einschlägigen Risikokonzeptionen erwarten lässt – führt vorliegend nicht weiter: Der EuGH verlangt, wie auch schon in der ORF-Entscheidung, jedoch anders als das vorinstanzliche EuG, keinen Privatlebensbezug im engeren Sinne mehr und sieht die Vorschriften der VO 45/2001/EG, die den Datenschutz bei Datenverarbeitungen durch die Unionsorgane regelt, als zwingend an.[168] In der Vorinstanz bezog sich das EuG dagegen umfassend auf die ältere Rechtsprechung des EGMR zu Art. 8 Abs. 1 EMRK, um zu begründen, dass nicht bereits alle personenbezogenen Daten Art. 8 Abs. 1 EMRK beeinträchtigen, und formuliert besondere Anforderungen hieran: „personal data that are capable of actually and specifically undermining the protection of privacy".[169] Dies sei hingegen bei den Namen der Interessenvertreter aufgrund ihrer rein beruflich motivierten Anwesenheit bei dem Treffen, das dem gegenständlichen Protokoll zugrunde lag, nicht der Fall. Das EuG gesteht zwar zu, dass berufliche Tätigkeiten nach der Rechtsprechung des EGMR nicht zwangsläufig aus dem Schutzbereich des Art. 8 Abs. 1 EMRK herausfielen, gleichwohl sieht es im vorliegenden Fall keine hinreichend „tatsächliche" und „spezifische" („actually and specifically") Betroffenheit. Nähere Erläuterungen, was unter einer solchen Betroffenheit zu verstehen sein soll, macht das EuG freilich nicht. Aus dem Urteil wurde gelegentlich der Rückschluss gezogen, dass nicht mit Sicherheit feststehe, dass die Gerichte der Europäischen Union künftig – trotz des weitergehenden Sekundär-

---

[165] EuGH Urteil vom 20.5.2003 verb. Rs. C 465/00, C-138/01 und C-139/01 *(Österreichischer Rundfunk)* Rn. 74, 75.

[166] Ebd. Rn. 89.

[167] GA *Tizzano*, Schlussanträge vom 14.11.2002 zu EuGH Urteil vom 20.5.2003 verb. Rs. C 465/00, C-138/01 und C-139/01 *(Österreichischer Rundfunk)* Rn. 47, 32.

[168] EuGH Urteil vom 29.6.2010 Rs. C-28/08 P *(Bavarian Lager)* Rn. 52, 58 f.

[169] EuG Urteil vom 8.11.2007 Rs. T-194/04 *(Bavarian Lager)* Rn. 117–120.

rechts – auf einen Privatlebensbezug i.e.S. verzichten werden.[170] Mit der Entscheidung des EuGH wurde diese Vermutung zwar nicht bestätigt, jedoch auch nicht widerlegt, da sich der EuGH nicht mit der Grundrechtsauslegung befasste, sondern den Fall anhand der weitergehenden sekundärrechtlichen Maßgaben entschied.

Lediglich anzumerken ist der Versuch von GA *Sharpston* in den Schlussanträgen, durch eine restriktive Auslegung des Anwendungsbereichs der VO 45/2001/EG das Problem des Verhältnisses von Transparenz- und Datenschutzregelungen zu umgehen. Die Verordnung, die nach Art. 3 Abs. 2 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten und für die nicht automatisierte Verarbeitung personenbezogener Daten in einer Datei gilt, erfasse „nicht andere Formen der Verarbeitung von Daten wie z.B. die Gewährung des Zugangs zu Dokumenten".[171] Die Ansicht von *Sharpston* kann nicht überzeugen, da in den Protokollen personenbezogene Daten enthalten sind und die Gewährung von Zugang gerade eine Weitergabe solcher Daten und damit eine Verarbeitung im Sinne von Art. 2 VO 45/2001/EG darstellt. Auch aus dem bei nicht automatisierter Verarbeitung auf Dateien beschränkten Anwendungsbereich des Art. 3 Abs. 2 Var. 2 VO 45/2001/EG folgt nichts anderes, da die Protokolle mit den personenbezogenen Daten in einer strukturierten Sammlung erfasst und nach bestimmten Kriterien zugänglich sind, Art. 2 c) RL 45/2001/EG. Der für *Sharpston* tragende Umstand, dass die personenbezogenen Daten nur „beiläufig" in den Protokollen erfasst sind,[172] ändert hieran nichts, da der Anwendungsbereich der RL ansonsten ausgehöhlt würde. Auch die von *Sharpston* vorgeschlagene Differenzierung nach unterschiedlichen Kategorien von Dokumenten, solche die personenbezogene Daten nur beiläufig und solche, die eine große Anzahl von personenbezogenen Daten enthalten,[173] ist wenig überzeugend. Hier bleibt *Sharpston* die Begründung schuldig, weshalb Personen, deren Daten in einer Sammlung mit hauptsächlich sachbezogenen Angaben stehen, weniger schutzwürdig sein sollen, als solche, deren personenbezogene Daten sich in Sammlungen mit einer Vielzahl anderer Betroffener finden. Dies kann allenfalls ein politisches Argument im Rahmen der Einführung solcher Dateien darstellen, nicht jedoch bei der Auslegung des in diesem Punkt klaren Sekundärrechts, das gerade auch dem Schutz der Grundrechte Einzelner dienen soll. Aus der Perspektive des Einzelnen macht es jedoch keinen Unterschied, ob neben ihm noch eine Vielzahl anderer Personen von einem Eingriff betroffen ist. *Sharpston* hätte an dieser Stelle erklären müssen, weshalb Risiko und Schwere des Grundrechtseingriffs bei „beiläufiger" Erwähnung andere sind als bei „absichtlicher". Dies ist jedoch alles andere als evident; die Antwort auf diese Fra-

---

[170] *Britz*, EuGRZ 2009, 1 (9).

[171] GA *Sharpston*, Schlussanträge vom 15.10.2009 zu EuGH Urteil vom 29.6.2010 Rs. C-28/08 P (*Bavarian Lager*-Schlussanträge) Rn. 101.

[172] Ebd. Rn. 137.

[173] Ebd. Rn. 159 ff.

ge bleibt sie schuldig. So ist denn auch der Gerichtshof zu Recht nicht ihrer Ansicht gefolgt und hielt es auch nicht für erforderlich, sich mit den diesbezüglichen Ausführungen von *Sharpston* auseinanderzusetzen.[174] Die Schlussanträge verdeutlichen damit erneut die Notwendigkeit einer Argumentation anhand von Schutzgütern und einschlägigen Risiken, die in der Entscheidung jedoch zugunsten einer – nicht überzeugenden – rein formellen Argumentation versäumt wurde.

Während sich also den Entscheidungen *Österreichischer Rundfunk* und *Bavarian Lager* nur wenig zu einschlägigen Risiken entnehmen lässt, ist dies in den Entscheidungen *Satamedia* und *Agrarbeihilfedaten* – insbesondere aufgrund der ergiebigen Schlussanträge der Generalanwälte – anders.

In der Rechtssache *Satamedia* befasste sich der Gerichtshof mit der Publikation von in Finnland gem. § 5 des Gesetzes über die Öffentlichkeit und Geheimhaltung von Steuerdaten[175] öffentlich zugänglichen Steuerinformationen. Ein finnisches Unternehmen veröffentlichte in einer eigens dafür herausgegebenen Zeitschrift Steuerinformationen von ca. 1,2 Millionen natürlichen Personen. Die Daten umfassten den Vor- und Nachnamen sowie auf 100 Euro genau Informationen über das Einkommen aus Erwerbstätigkeit und Kapital und über das Vermögen. Die Informationen wurden in regionalen Publikationen veröffentlicht und waren alphabetisch nach Gemeinde und Einkommenskategorie geordnet. Die Angaben wurden jedoch nur bei Überschreiten einer – je nach Gemeinde unterschiedlichen – Untergrenze (für Helsinki 360.000 €) in die Liste aufgenommen. Weiterhin ermöglichten die Herausgeber in Kooperation mit weiteren Unternehmen die Abfrage der Steuerdaten per SMS. Eine Streichung aus den Dateien konnte gegen Entgelt vorgenommen werden.

Das vorlegende Gericht stellte insbesondere die Frage, inwieweit die Ausnahmevorschrift des Art. 9 RL 95/46EG einschlägig ist. Diese Vorschrift erlaubt Abweichungen, wenn eine Verarbeitung „allein zu journalistischen" Zwecken erfolgt. Weiterhin wurde die Frage aufgeworfen, ob das Schutzprogramm der Richtlinie auch dann gilt, wenn Informationen bereits in Medien veröffentlicht wurden.[176] Das Urteil des EuGH kommt mit nur knapper Begründung zu dem Ergebnis, dass es Sache des nationalen Gerichts ist, zu prüfen, ob die oben beschriebenen Verarbeitungen „allein zu journalistischen Zwecken" erfolgt sind, dass dies aber grundsätzlich möglich sei. Weiterhin lehnt es – ebenfalls nur knapp begründet – eine Ausnahme vom Anwendungsbereich aufgrund bereits erfolgter Publikation mangels einschlägiger Ausnahmevorschrift in der RL und aufgrund der Gefahr des Leerlaufens der RL ab. Das Urteil selbst ist zwar für die vorliegende Untersuchung wenig ergiebig, der Gerichtshof verweist darin jedoch an mehreren Stellen auf die Schluss-

---

[174] EuGH Urteil vom 29.6.2010 Rs. C-28/08 P *(Bavarian Lager)* Rn. 63.

[175] Laki verotustietojen julkisuudesta ja salassapidosta.

[176] EuGH Urteil vom 16.12.2008 Rs. C-73/07 *(Satamedia)* Rn. 25–34.

anträge, die wieder von GA *Kokott* stammen. Darin werden, im Gegensatz zum Urteil, eine umfassende und ausführliche Auseinandersetzung mit einschlägigen Risiken und eine Abwägung jeweiliger Schutzgüter vorgenommen.[177] Zwar kommt auch *Kokott* zum Ergebnis, dass es Sache der Mitgliedstaaten sei, die Anwendbarkeit des Art. 9 RL 95/46/EG zu prüfen; sie zeichnet jedoch die hierfür notwendige Abwägung zwischen den kollidierenden Schutzgütern der Meinungsfreiheit und der Privatsphäre umfassend nach.[178] *Kokott* äußert sich zunächst zu den maßgeblichen Grundrechten und Auslegungsmaßstäben. Das „Grundrecht auf Privatsphäre" macht sie dabei an Art. 8 Abs. 1 EMRK sowie an Art. 7 und Art. 8 EU-GRC fest. Sie stellt zunächst fest, dass die Weitergabe personenbezogener Daten unabhängig von der späteren Verwendung einen Eingriff darstellt und bejaht unter Verweis auf die Rechtsprechung des EGMR die positive Verpflichtung des Staates zum Schutz vor Risiken privater Datenverarbeitungen, welche sich in der RL 95/46/EG auf Ebene der Union manifestiere.[179] Die Allgemeinheit der RL erlaube es dabei, die Konfliktlage zwischen den betroffenen Grundrechten der Meinungsfreiheit und des Datenschutzes angemessen auszugleichen. Insoweit bestehe eine innerstaatliche Einschätzungsprärogative, welche bei der Auslegung zu berücksichtigen sei.[180]

Bei der eigentlichen Prüfung des Art. 9 RL 95/46/EG legt *Kokott* das Merkmal „journalistische Zwecke" funktional aus und sieht diese als gegeben an, wenn die Verarbeitung darauf abzielt, Informationen und Ideen über Fragen des „öffentlichen Interesses" zu vermitteln.[181] Zu untersuchen ist nun, wie *Kokott* das öffentliche Interesse konkretisiert und wo sie dessen – durch den grundrechtlichen Datenschutz gesetzte – Grenzen sieht. Zur Konkretisierung des öffentlichen Interesses zieht sie zunächst inhaltliche Kriterien heran: Bei personenbezogenen Daten komme es auf den Bezug zu einer öffentlichen Funktion der betroffenen Person an; dieser fehle, wenn Details aus dem Privatleben veröffentlicht werden, allein um die Neugier eines bestimmten Publikums zu befriedigen, sofern dadurch kein Beitrag zu „irgendeiner Diskussion von allgemeinem Interesse für die Gesellschaft" geleistet werde. Im Rahmen dieser Grenze sei die „berechtigte Erwartung" eines Betroffenen, dass seine Privatsphäre respektiert werde, von „besonderer Bedeutung".[182] Dabei verweist *Kokott* auf die Rechtsprechung des EGMR in Sachen *Halford, P.G. und J.H.* sowie *Copland*.[183] Sowohl die öffentliche Natur bestimmter

---

[177] GA *Kokott*, Schlussanträge vom 8.5.2008 zu EuGH Urteil vom 16.12.2008 Rs. C-73/07 (*Satamedia*-Schlussanträge).

[178] Ebd. Rn. 86–105.

[179] Ebd. Rn. 40 f.

[180] Ebd. Rn. 44 sowie 52 f.

[181] Ebd. Rn. 68.

[182] Ebd. Rn. 74, 77.

[183] Ebd., Fn. 48. Bei der Beurteilung entfalle ein solches Interesse jedoch nur in offensichtlichen Fällen, da staatliche Stellen das Vorliegen nicht „streng überprüfen" könnten

Informationen als auch die berechtigte Erwartung des Respekts der Privatsphäre seien jedoch sehr stark abhängig von der innerstaatlichen Rechtslage, von gesellschaftlichen Wertvorstellungen und von konkret existierenden öffentlichen Debatten. Es sei hingegen Aufgabe der zuständigen Stellen in den Mitgliedstaaten, diese Elemente zu prüfen. Der Gerichtshof habe insoweit nur auf die relevanten Umstände hinzuweisen. Im Fall der Steuerdaten sei zu beachten, dass lediglich einige Mitgliedstaaten diese als vertraulich ansähen. In diesen Staaten komme den Betroffenen folglich eine berechtigte Vertraulichkeitserwartung zu. Aufgrund der umfassenden Transparenzgesetzgebung in Finnland sei „vermutlich" davon auszugehen, dass bei finnischen Bürgern keine berechtigte Erwartung vertraulicher Behandlung ihrer Steuerdaten bestehe.[184]

Festzuhalten ist somit zunächst die von *Kokott* vorgenommene Konkretisierung der aus der Rechtsprechung des EGMR bekannten Konzeption schutzwürdiger Vertraulichkeitserwartung.[185] Das Neue daran ist die Konkretisierung aus übergreifender, gesellschaftlicher Perspektive durch den Bezug auf die finnischen Normen zur Informationsfreiheit. Bei einer derart „normgeprägten" bzw. „normativen" Konkretisierung der Schutzgutkonzeption drängt sich jedoch die Frage nach den Grenzen der Ausgestaltungsbefugnis der mitgliedstaatlichen Gesetzgeber auf. Dabei wird nämlich aus dem fehlenden rechtlichen Schutz auf Ebene der Mitgliedstaaten auf ein reduziertes Schutzniveau des Datenschutzgrundrechts geschlossen. Diese Vorgehensweise führt jedoch zu dem unhaltbaren Ergebnis, dass der Grundrechtsschutz umso reduzierter ist, je stärker die Mitgliedstaaten ihn einschränken. Letztlich steht eine Grundrechtskonkretisierung, die sich *allein* aus der übergreifenden Perspektive der rechtlichen Gegebenheiten orientiert, mit dem Sinn und Zweck der Grundrechte und insbesondere mit deren Abwehrfunktion in Widerspruch.[186]

*Kokott* fährt damit fort, das Bestehen eines öffentlichen Interesses nach den dargelegten Maßgaben zu prüfen. Beachtenswert sind dabei die Ausführungen in Bezug auf die Art des eingesetzten Mediums: Die Form der Zeitungsveröffentlichung spreche *prima facie* zwar für das Vorliegen eines öffentlichen Interesses, dies sei jedoch nicht zwingend, da durch die Steuerpublikation gerade auch private Neugier befriedigt werden könne. Bei der Anforderung von Steuerinformationen per SMS sei dieser Aspekt viel stärker ausgeprägt. Hier spreche die konkrete Anforderung von Informationen über eine bestimmte Person gegen das Vorliegen eines öffentlichen Interesses. Jedoch sei es nicht möglich, allein aufgrund der Informations-

---

und es zum Teil auch gerade erst durch die Vermittlung der Medien geschaffen werde, vgl. Rn. 78.

184 GA *Kokott*, Schlussanträge vom 8.5.2008 zu EuGH Urteil vom 16.12.2008 Rs. C-73/07 (*Satamedia*-Schlussanträge) Rn. 86–89.

185 Siehe oben Teil 1, IV.B.5. und 6.

186 Zu den Grundrechtsfunktionen *Jarass/Pieroth*, Grundgesetz, Vorb. vor Art. 1, Rn. 3 ff. sowie *Pieroth* u.a., Grundrechte, § 4.

vermittlung unter Einsatz von Telekommunikation das öffentliche Interesse auszuschließen. Diese ergänze vielmehr zunehmend traditionelle Verteilungsformen.[187] Als inhaltliche Kriterien für private Interessen nennt *Kokott* neben der „persönlichen Neugier" auch die naheliegenden kommerziellen Interessen hinsichtlich zielgerichteter Werbung und Bonitätsprüfungen. Ob hierin ein eigenständiges Risiko – etwa bei Versagung von Vertragsschlüssen nach Bonitätsprüfung durch Steuerdaten – zu sehen ist, erörtert *Kokott* nicht. Das Risiko fehlerhafter Daten deutet sie im Zusammenhang mit der Möglichkeit, die eigenen Daten aus der Liste streichen zu lassen an.[188]

Das vorlegende Gericht stellte zudem die Frage, ob bereits in den Medien veröffentlichtes Material aus dem Anwendungsbereich der Richtlinie herausfällt. Dieser Aspekt ist auch für die vorliegende Untersuchung relevant, weil er die Benennung etwaiger Risiken voraussetzt und die Frage aufwirft, inwieweit erneute Verarbeitungen eine Erhöhung der Risiken oder Vertiefung von Schäden bewirken. *Kokott* betont jedoch lediglich, dass die RL keine ungeschriebenen Ausnahmen enthält und dass bei einer derartigen Ausnahme insbesondere die Zweckbindung gem. Art. 6 Abs. 1 b) RL 95/46/EG leerliefe. Bei der sich anschließenden Abwägung von grundrechtlicher Meinungsfreiheit und Datenschutz sei jedoch davon auszugehen, dass der „Schutzanspruch der Privatsphäre" bei bereits veröffentlichten Informationen „in der Regel" von geringerem Gewicht sei. Dies stünde jedoch einer Vertiefung und Perpetuierung von Eingriffen durch weitere Verarbeitungen nicht entgegen. Als Beispiele nennt *Kokott* Fehlinformationen, Beleidigungen und die Intimsphäre betreffende Informationen.[189] Einen mitgliedstaatlichen Gestaltungsspielraum für Ausnahmen bejaht *Kokott* hinsichtlich Art. 13 Abs. 1 g) RL 95/46/EG (Ausnahme u.a. zum Schutz der Freiheiten anderer Personen) zwar grundsätzlich, führt hierzu jedoch aus, dass offensichtlich unverhältnismäßige Beeinträchtigungen des Rechts auf Privatsphäre nicht auf Art. 13 gestützt werden können. So könne die Weiterverarbeitung bewiesenermaßen falscher personenbezogener Informationen nicht damit gerechtfertigt werden, dass sie veröffentlicht wurden.[190] *Kokott* mildert damit die oben kritisierte Problematik des Leerlaufens grundrechtlichen Datenschutzes durch eine „Normprägung" ab, indem sie die Grenze einer offensichtlichen Unverhältnismäßigkeit aufstellt.

---

[187] GA *Kokott*, Schlussanträge vom 8.5.2008 zu EuGH Urteil vom 16.12.2008 Rs. C-73/07 (*Satamedia*-Schlussanträge) Rn. 90–95. Die Argumentation der GA nähert sich hier der im medienrechtlichen Zusammenhang häufig eingeforderten „Technikneutralität", wonach Regelungen funktional und nicht abhängig von dem raschen Wandel eingesetzter Techniken sein sollen, vgl. *Sieber*, NJW-Beil. 2012, 89.

[188] GA *Kokott*, Schlussanträge vom 8.5.2008 zu EuGH Urteil vom 16.12.2008 Rs. C-73/07 (*Satamedia*-Schlussanträge) Rn. 97.

[189] Ebd. Rn. 122.

[190] Ebd. Rn. 124.

In der Entscheidung zu *Agrarbeihilfeempfängern*[191] geht es um die Gültigkeit von Vorschriften der EU, nach denen im Rahmen der Gemeinsamen Agrarpolitik gezahlte Beihilfen zusammen mit dem Namen des Empfängers, der jeweiligen Gemeinde und der Postleitzahl offengelegt wurden. Zwei betroffene Landwirte wendeten sich gegen die Veröffentlichungen der Daten auf der Internetseite der Bundesanstalt für Landwirtschaft und Ernährung (BfLE), die auf Grundlage der einschlägigen Verordnungen 1290/2005/EG und 259/2008/EG erfolgt waren. Das vorlegende Verwaltungsgericht Wiesbaden stellte u.a. die Frage, ob die Rechtsgrundlagen gültig sind, da es die Datenverarbeitungen der BfLE ansonsten für rechtswidrig erachten müsse. Aufschlussreich hinsichtlich einschlägiger Risiken sind die Ausführungen von GA *Sharpston* in ihren Schlussanträgen.[192] *Sharpston* stellt zunächst die widerstreitenden Ziele dar. Diese sind auf der einen Seite das Recht auf Zugang zu Informationen im Interesse der Transparenz und auf der anderen Seite das Recht auf Schutz der Privatsphäre.[193] Letzteres unterteilt sie in das „klassische" Recht des Schutzes der Privatsphäre nach Art. 8 Abs. 1 EMRK und das „eher moderne" Recht aus den Datenschutzbestimmungen der Konvention 108. In der EU-GRC knüpft sie sowohl an Art. 7 als auch an Art. 8 EU-GRC an und verweist auf den engen Zusammenhang beider Rechte nach Ansicht des EuGH. Unter Verweis auf die Rechtssachen *Österreichischer Rundfunk* und *Satamedia* bejaht *Sharpston* einen Eingriff sowohl in das Recht auf Schutz der Privatsphäre als auch in das Recht auf den Schutz personenbezogener Daten.[194] Ein maßgebliches Risiko sieht sie in der Kombination aus Postleitzahlen, Namen und den Unterstützungsbeträgen. In Verbindung mit anderen online leicht zugänglichen Informationsquellen ermöglichten diese Informationen die Ermittlung der genauen Adresse einer Person. Rückschlüsse auf das Einkommen der Begünstigten seien besonders aussagekräftig, da die Beihilfen bis zu 70 % des Einkommens der Landwirte ausmachen könnten.[195]

Im Anschluss an die Prüfung, inwieweit das Transparenzprinzip eine legitime Grundlage i.S.v. Art. 8 Abs. 2 EU-GRC darstellt, widmet sich *Sharpston* knapp den Auswirkungen der Veröffentlichung im Internet, bei denen eine Befassung mit Risiken der Internetnutzung nahegelegen hätte. Sie führt dann jedoch lediglich aus, dass die leichte Zugänglichkeit, die Suchmöglichkeiten und die „bequeme Nutzung" dazu führten, dass Veröffentlichungen in diesem Medium potenziell stärker in die Rechte auf Schutz der Privatsphäre eingreifen. Bei der Prüfung, ob die Veröffentlichung von personenbezogenen Daten mit einem besonderen „Maß an Detailgenauigkeit" einen gerechtfertigten und verhältnismäßigen Eingriff darstellt,

---

[191] EuGH Urteil vom 9.11.2010 Rs. C-92/09 und C-93/09 *(Agrarbeihilfeempfänger)*.

[192] GA *Sharpston*, Schlussanträge vom 17.6.2010 zu EuGH Urteil vom 9.11.2010 Rs. C-92/09 und C-93/09 (*Agrarbeihilfeempfänger*-Schlussanträge).

[193] Ebd. Rn. 65.

[194] Ebd. Rn. 89–91.

[195] Ebd. Rn. 92, 83.

müsse man sich des „Wesens und der Folgen“ einer Veröffentlichung im Internet bewusst sein.[196] *Sharpston* führt dieses Argument zwar nicht weiter aus. Sie deutet damit jedoch das Risiko der Informationspermanenz und allgemeinen Zugänglichkeit von im Internet veröffentlichten Informationen zumindest an. Das auf die Schlussanträge folgende Urteil des EuGH widmet sich sodann vor allem Erforderlichkeitsaspekten und enthält keine weiteren Informationen zu betroffenen Risiken. Festzuhalten bleibt somit insbesondere der Bezug zum Risiko von Publikationsschäden durch Veröffentlichung präziser Einkommensinformationen.

### 3. Zwischenergebnis

Die Untersuchung von Art. 8 EU-GRC hat zunächst die besondere Relevanz des Sekundärrechts und der Rechtsprechung des EGMR zu Art. 8 EMRK bei der Konkretisierung des Schutzgehalts erwiesen. Dabei treten normsystematische Probleme auf, da das Sekundärrecht Gegenstand und nicht Maßstab der grundrechtlichen Verbürgung ist. Das Problem ist insbesondere dann relevant, wenn mehrere Private beteiligt sind und es deshalb zu Überschneidungen beim anwendbaren Sekundärrecht kommen kann (z.B. gleichzeitige Anwendbarkeit von Datenschutz- und Informationsfreiheitsvorschriften).

In einer solchen Konstellation nahm das EuG in der Entscheidung *Bavarian Lager* unter Berufung auf die Rechtsprechung des EGMR eine restriktive Auslegung von Art. 8 EU-GRC vor, indem es einen Privatlebensbezug i.e.S. einforderte. Der EuGH löste die Konfliktlage allein auf der Ebene des Sekundärrechts.[197]

Bei der Untersuchung der Risikokonzeptionen wurde mit dem persönlichen Schutzbereich begonnen. Hier differenziert der EuGH zwischen natürlichen und juristischen Personen und nähert sich der zu Art. 19 Abs. 3 GG vertretenen Theorie des personalen Substrats an. Die Differenzierung entbehrt jedoch bisher einer tragfähigen Begründung. Die an dieser Stelle eigentlich gebotene Analyse der Gefährdungslage juristischer Personen – aus der Rückschlüsse auf maßgebliche Risiken hätten folgen können – unterlässt der EuGH und schließt in fragwürdiger Weise von bestehenden Veröffentlichungspflichten auf eine weitergehende Zulässigkeit von Schutzbereichsausnahmen.[198] Im sachlichen Schutzbereich verlangt der EuGH eine besondere Binnenmarktrelevanz betroffener Daten nicht mehr, worin in der Literatur eine Akzentverschiebung in den Zielen der Union – von der Binnenmarktzentralität zum Individuum – gesehen wird.[199] Hiermit deutet sich eine ähnliche Entwicklung hinsichtlich der Schutzgüter wie im Rahmen der Modernisierungsvorschläge zur Datenschutzkonvention des Europarats an.[200]

---

196 Ebd. Rn. 96.

197 Siehe oben II.B.1.

198 Siehe oben II.B.2.a).

199 Siehe oben II.B.2.b).

200 Siehe oben Teil 1, II.A.2.b).

Eine Reihe von Entscheidungen des EuGH befasste sich sodann mit privaten Datenverarbeitungen. Eine umfassende inhaltliche Auseinandersetzung mit einschlägigen Risiken und Schutzgütern findet sich jedoch zunächst weniger in den Urteilen – diese verweisen häufig auf den Umsetzungsspielraum der Mitgliedstaaten, lösen die Problematik allein kompetenzrechtlich oder verbleiben undifferenziert –, sondern vielmehr in den Schlussanträgen der Generalanwälte. So bejaht GA *Kokott* in den Schlussanträgen zur Entscheidung *Promusicae* ein aus dem Datenschutzgrundrecht folgendes Schutzziel bei privaten Datenverarbeitungen und dessen sekundärrechtliche Konkretisierung. *Kokott* beruft sich auf die Rechtsprechung des BVerfG zur Vorratsdatenspeicherung und erörtert das Risiko „gläserner Bürger", das mit dem oben erörterten Überwachungsdruck korreliert. Ein besonderes Risiko bei Weitergabe an Private folge zudem aus dem rein ökonomisch motivierten und damit einseitigen Ermittlungsinteresse der Privaten in „Abmahnkonstellationen". Dieses Risiko lässt sich in die Gruppe der Erhöhung individueller Verletzlichkeit einordnen.[201] Die staatliche Nutzung privater Datenbestände thematisiert zunächst GA *Leger* in den Schlussanträgen zur *Fluggastdaten*-Entscheidung des EuGH. Das maßgebliche Risiko wird hier in der Bildung von Persönlichkeitsprofilen gesehen, wobei *Leger* zwar in einzelnen PNR-Datenelementen keine Beeinträchtigung des Privatlebens sieht, bei der gebotenen Gesamtbetrachtung den Eingriff jedoch bejaht. Das am Beispiel der Fluggastdaten entwickelte Risiko der Nutzung privater Datenbestände durch den Staat betrifft die Kategorie „Persönlichkeitsprofile". Wie jedoch die Schlussanträge des GA *Villalón* und das zweite Urteil des EuGH zur Vorratsdatenspeicherung zeigen, werden auch andere Risiken wie beispielsweise die Informationspermanenz oder informationsbedingte Verhaltensanpassungen aufgegriffen.[202] Charakteristisch ist die Potenzierung des Risikos durch den massiven Anstieg der Aussagekraft und die Vielfalt vorhandener Informationen gerade auch bei privaten Stellen. Das Zusammenwirken von Staat und privaten Stellen zu Überwachungszwecken ist damit weniger eine eigenständige Risikokategorie als vielmehr ein Potenzierungsfaktor für andere Risiken. Aussagekräftig sowohl für die Potenzierung verschiedener Risiken als auch für das Risiko der Informationspermanenz ist hingegen das Urteil des EuGH in der Rechtssache *Google Spain*.[203]

Eine Reihe weiterer Entscheidungen des EuGH betrifft die Grenzen, die der Datenschutz staatlicher Transparenz setzt. Dabei wird z.T. eine stark formale Erörterung ohne substanzielle Auseinandersetzung mit Risiken und Schutzgütern vorgenommen. In den Schlussanträgen der GA *Kokott* zur Entscheidung *Satamedia* findet sich jedoch eine Fortbildung des aus der EGMR-Rechtsprechung bekannten Schutzguts der Vertraulichkeitserwartung. Vorgeschlagen wird die Anbindung der Erwartung an die jeweils bestehende mitgliedstaatliche Rechtslage, an gesellschaft-

---

[201] Siehe oben II.B.2.c).

[202] Siehe oben II.B.2.d).

[203] Siehe oben II.B.2.d).

lichen Wertvorstellungen und konkret existierende öffentliche Debatten. Dies läuft jedoch zumindest hinsichtlich der „normgeprägten" Auslegung dem Schutzziel der Grundrechte entgegen, da der Schutzstandard in die Disposition des einfachen Gesetzgebers gestellt wird und der Ausgestaltungsbefugnis keine materiellen Grenzen gesetzt werden.[204] Angedeutet wird ferner das Risiko fehlerhafter Daten durch willkürliche Löschungspflichten sowie die Vertiefung und Perpetuierung von Eingriffen als Risiken bezüglich bereits veröffentlichter Informationen. In den Schlussanträgen zur Entscheidung *Agrarbeihilfedaten* wird zudem das Risiko von Publizitätsschäden bei Veröffentlichung von Gehaltsdaten aufgenommen.[205]

## C. Art. 16 AEUV und Art. 39 EUV

Art. 16 AEUV lautet:

> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.
>
> Die auf der Grundlage dieses Artikels erlassenen Vorschriften lassen die spezifischen Bestimmungen des Artikels 39 des Vertrags über die Europäische Union unberührt.

Der erste Absatz hat somit den gleichen Inhalt wie Art. 8 Abs. 1 EU-GRC und verbürgt ein Datenschutzgrundrecht. Der zweite Absatz enthält eine gegenüber der vorangegangenen Rechtslage erheblich erweiterte Gesetzgebungskompetenz und ordnet die Überwachung der Vorschriften durch unabhängige Behörden an.

Der im letzten Unterabsatz angesprochene Art. 39 EUV betrifft den Datenschutz im Rahmen der GAS; er lautet:

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

Die beiden mit dem Vertrag von Lissabon eingeführten Vorschriften unterstreichen den hohen Stellenwert, der dem Datenschutz auf Ebene des Unionsrechts mittlerweile zukommt. Im Vergleich zu der davor bestehenden Rechtslage erfuhr der Datenschutz eine Aufwertung, da die bisherige Akzessorietät zwischen Binnenmarkt und Datenschutz durch Art. 16 Abs. 2 Unterabs. 1 Satz 1 Hs. 1 AEUV

---

[204] Siehe oben II.B.2.e).

[205] Siehe oben II.B.2.e).

aufgelöst wurde.[206] Die zuvor äußerst weite und deshalb fragwürdige Auslegung des Art. 95 EGV a.F. hat sich damit erübrigt.[207] Das Sekundärrecht ist damit nicht mehr auf die Binnenmarktkompetenz angewiesen.[208] Daneben tritt nun eine – nach alter Rechtslage noch nicht bestehende – Rechtsetzungszuständigkeit auch im Bereich der polizeilichen und justiziellen Zusammenarbeit. Die Bezugnahme zum „freien Datenverkehr" in Art. 16 Abs. 2 Unterabs. 1 Satz 1 Hs. 2 AEUV verdeutlicht die Ambivalenz der Regelungsmaterie „Datenschutz", bei der immer auch der freie Informationsaustausch als teilweise kollidierendes Schutzgut mitgedacht werden muss. Da Art. 16 Abs. 1 AEUV nicht über den Schutz des Art. 8 EU-GRC hinausgeht[209] und auch noch keine Rechtsprechung zur Vorschrift besteht, können daraus keine eigenständigen Risikokonzeptionen oder Schutzgüter abgeleitet werden. Die Wirkung beschränkt sich neben einer Vergegenwärtigung des Datenschutzanliegens bereits im Legislativprozess auf die Möglichkeit, Art. 16 AEUV i.V.m. Art. 8 EU-GRC als datenschutzrechtliche Schutzpflicht auszulegen.[210] Da das Bestehen einer solchen, wie oben dargestellt, bereits vor Einführung des Art. 16 AEUV anerkannt war, folgt hieraus keine materielle Erweiterung des Schutzes. Problematisch erscheint dagegen, dass Art. 16 AEUV im Gegensatz zu Art. 8 EU-GRC nicht unter Schrankenvorbehalt steht. Die Transferklausel des Art. 52 Abs. 2 EU-GRC zielt jedoch darauf ab, bei einer Doppelung von Rechten, Divergenzen zu vermeiden. Mithin dürfen die Charta-Rechte nicht abweichend von den Vertragsrechten eingeschränkt werden. Um zu vermeiden, dass die Schrankenregelung des Art. 8 Abs. 2 EU-GRC leerläuft, ist Art. 52 Abs. 2 EU-GRC, wie es auch der überwiegenden Ansicht in der Literatur entspricht, ausnahmsweise teleologisch zu reduzieren.[211] Aufgrund dieser neuen Kompetenzen und wegen der oben dargestellten „quasi normgeprägten" Grundrechtsauslegung des EuGH[212] ist das datenschutzrechtliche Sekundärrecht im Folgenden zu analysieren.

## D. Zwischenergebnis

Die Rechtsprechung des EuGH zu Art. 8 EU-GRC orientiert sich einerseits an der Rechtsprechung des EGMR und andererseits an dem europäischen Sekundär-

---

[206] *Kingreen*, in: Callies/Ruffert (Hrsg.), EUV/AEUV, Art. 16 AEUV Rn. 5; Streinz-*Herrmann*, Art. 16 AEUV Rn. 4; *Spiecker gen. Döhmann*, JZ 2011, 169 (172).

[207] Zu „taktischen" Erwägungen der Akteure (Vermeidung des Einstimmigkeitsprinzips) im Kontext der Kompetenzdebatte vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie, S. 64 f.

[208] Vgl. auch *Grimm*, JZ 2013, 585 (589).

[209] Streinz-*Herrmann*, Art. 16 AEUV Rn. 5.

[210] *Spiecker gen. Döhmann*, JZ 2011, (169), 172.

[211] Ebd. 169 (172).

[212] Siehe oben I.B. sowie II.B.2.e).

recht. Die Orientierung an der EMRK ist normsystematisch gut begründbar. Die Konkretisierung anhand des Sekundärrechts hat dagegen zu Kritik geführt, da die Charta Maßstab des Sekundärrechts und nicht umgekehrt das Sekundärrecht Maßstab der Charta ist.[213] Art. 7 EU-GRC ist bislang zwar hinsichtlich der erfassten elektronischen Kommunikation für die hiesige Untersuchung von Relevanz; darauf beschränkte und aussagekräftige Leitentscheidungen liegen jedoch nicht vor. Weil der EuGH im Übrigen von einer besonderen Bedeutung des Art. 8 EU-GRC für Art. 7 EU-GRC ausgeht und die Prüfung parallel führt, wurde die Risikoanalyse anhand der Leitentscheidungen zu Art. 8 EU-GRC aufgebaut. Die partielle Einbeziehung entsprechender Passagen zu Art. 7 EU-GRC konnte dabei gleichwohl erfolgen, womit die bislang vom EuGH nicht vorgenommene Abgrenzung beider Rechte aufgegriffen wurde.[214] Die Analyse der Rechtsprechung des EuGH zu Art. 8 EU-GRC zeigte dabei zunächst einen Schwerpunkt auf kompetenziellen und verfahrensrechtlichen Fragen. Gleichwohl wurde mit der Binnenmarktfokussierung eine Parallele zur wirtschaftspolitischen Ausrichtung der Spezialinstrumente gefunden, deren Bedeutung jedoch durch die mit dem Lissabonner Vertrag geschaffenen Kompetenznormen und einer gewissen individualrechtlichen Akzentverschiebung zurücktritt.[215] Hierin zeigen sich ähnliche Tendenzen wie im Rahmen der Modernisierungsvorschläge zur Datenschutzkonvention, wonach das Schutzgut unabhängiger von wirtschaftspolitischen Erwägungen gefasst wird. Bei der Frage nach dem persönlichen Schutzbereich hinsichtlich juristischer Personen gelingt dies jedoch nicht überzeugend. Feststellbar ist allein eine Annäherung an die in der deutschen Grundrechtsdogmatik vertretene Theorie vom personalen Substrat.[216] Fälle zu privaten Datenverarbeitungen und staatlicher Nutzung privater Datensammlungen lassen einerseits die durch Qualität und Quantität privater Verarbeitungen erfolgende Potenzierung der Risiken konformistischer Verhaltensanpassungen, Profilbildungen und Informationspermanenz erkennen und verdeutlichen andererseits das Risiko individueller Verletzlichkeit u.a. am Beispiel des Abmahnmissbrauchs.[217] Eine beachtenswerte Fortbildung der Schutzgutkonzeption der Vertraulichkeitserwartung versucht diese aus gesamtgesellschaftlicher Perspektive zu begreifen und damit „quasi normgeprägt“ aufzuladen. Dies begegnet schwerwiegenden Einwänden, soweit nicht zugleich materielle Ausgestaltungsgrenzen etabliert werden.[218]

---

213 Siehe oben II.B.1.

214 Siehe oben II.A.

215 Siehe oben II.B.2.b).

216 Siehe oben II.B.2.a).

217 Siehe oben II.B.2.c) und d).

218 Siehe oben II.B.2.e).

# III. Sekundärrecht

## A. Datenschutzrichtlinie (95/46/EG)

### 1. Überblick: Entstehung, Ziele und Inhalt

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995[219] (im Folgenden: Datenschutzrichtlinie) ist bis zu einer möglichen Ablösung im Zuge der Reformvorschläge vom 25.1.2012 der wichtigste Teil des datenschutzrechtlichen Sekundärrechts. Nachdem das Parlament bereits ab 1975 mehrfach Datenschutzregelungen auf Unionsebene eingefordert hatte, präsentierte die Kommission erst 1990 ein erstes und 1992 ein überarbeitetes zweites Maßnahmenpaket, das schließlich 1995 zum Erlass der allgemeinen EG-Datenschutzrichtlinie führte.[220] Wie schon bei dem Datenschutzübereinkommen des Europarats und den OECD-Richtlinien waren dabei zunächst wirtschaftspolitische Gründe ausschlaggebend – die Richtlinie diente der Vollendung des gemeinsamen Marktes. Fünf Mitgliedstaaten – Belgien, Griechenland, Italien, Spanien und Portugal – verfügten bis dahin über keine Datenschutzgesetze. Damit hätten diese Länder z.B. angesichts der damals bereits bestehenden deutschen Landesdatenschutzgesetze vom Austausch personenbezogener Daten ausgeschlossen werden müssen.[221] Die inkompatiblen nationalen Datenschutzgesetze stellten somit eine Gefahr für den freien Waren- und Dienstleistungsverkehr dar. Der Lösungsansatz der Richtlinie kann als „dualistisch" beschrieben werden.[222] Kernstück ist Art. 1 Abs. 2, der einen einheitlichen europäischen Informationsmarkt schafft, indem er Information als Wirtschaftsgut in das europarechtliche Diskriminierungsverbot einbezieht.[223] Der Weg dahin liegt in einem durch die Richtlinie harmonisierten grundrechtlichen Schutzniveau für personenbezogene Daten. Die Richtlinie wurde deshalb „insbesondere" auf die Kompetenz zur Harmonisierung des Binnenmarktes[224] gestützt, gleichzeitig zielt sie jedoch gem. Art. 1 Abs. 1 auf den „Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen".[225] Bereits die Überschrift verdeutlicht diese zweifache Zielsetzung: Statt das Regelwerk naheliegend als „Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezo-

---

219 ABl. L 281 vom 23.11.1995, S. 31–50.

220 *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2. Aufl., S. 23.

221 17. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Landtags-Drs. 12/4040 vom 2.2.1989, S. 16; Simitis-*Simitis*, BDSG, Einl. Rn. 205.

222 *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Einl. Rn. 4.

223 Ebd., Art. 1 Rn. 3, 5.

224 Die Wahl der Binnenmarktkompetenz des Art. 100a EGV a.F. (und nicht beispielsweise des Art. 235 EGV a.F.) hatte wohl vor allem strategische Gründe (Mehrheitsbeschlüsse ausreichend), vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie, Einl. Rn. 6.

225 Zum Ganzen auch *Kübler*, Säulen, S. 60.

gener Daten“ zu bezeichnen, fügte die Kommission den Zusatz „und zum freien Datenverkehr“ hinzu und beschränkte die Überschrift auf den Schutz „natürlicher Personen“.[226] Die Erwägungsgründe Nr. 1, 3, 10 und 11 unterstreichen hingegen den grundrechtlichen Bezug. So soll die Harmonisierung laut Erwägungsgrund Nr. 10 nicht durch eine Verringerung nationaler Schutzvorschriften erfolgen, sondern im Gegenteil darauf abzielen, in der Gemeinschaft „ein hohes Schutzniveau sicherzustellen“. Dies betont auch der EuGH in ständiger Rechtsprechung.[227] Insbesondere in den Schlussanträgen des GA *Tizzanzo* zu den Rechtssachen *Österreichischer Rundfunk*[228] und *Lindqvist*[229] wird jedoch die gegenteilige Auffassung und damit die Problematik der Zielsetzung „Grundrechtsschutz“ angesichts der überkommenen Kompetenznorm des Art. 95 EG a.F. nochmals deutlich herausgearbeitet. Nach Ansicht von *Tizzano* könne die Wahrung der Grundrechte kein eigenständiges Ziel darstellen, da die Gemeinschaft dadurch die ihr im Rahmen des Art. 95 EGV a.F. eingeräumten Befugnisse überschreiten würde. Der Gerichtshof schließt sich dem jedoch nicht an und lässt die „mittelbare“ Zielsetzung des Grundrechtsschutzes genügen.[230]

Die Richtlinie knüpft den Inhalt des Grundrechtsschutzes ausweislich des zehnten Erwägungsgrunds ausdrücklich an Art. 8 EMRK und führt diesen als Mindeststandard auf, den die Rechtsangleichung durch die Richtlinie nicht unterschreiten dürfe. Erwägungsgrund Nr. 11 sieht sodann in der Richtlinie eine Konkretisierung und Erweiterung der Grundsätze der Konvention 108 des Europarats. Begrifflich spricht die Richtlinie an mehreren Stellen (Erwägungsgründe Nr. 2, 7, 9, 10, 11, 33, 34, 68, Art. 1 Abs. 1, Art. 9, Art. 13 Abs. 2, Art. 25 Abs. 6, Art. 26 Abs. 2, Abs. 3) von der „Privatsphäre“, was angesichts des Bezugs zum Recht auf „Privatleben“ des Art. 8 EMRK inkonsequent ist und einmal mehr die begriffliche Unklarheit, die auch in anderen Datenschutznormen herrscht, unterstreicht.[231]

Inhaltlich regelt die Richtlinie die Datenqualität (Art. 6), die Zulässigkeitsvoraussetzungen für Datenverarbeitungen (insb. Art. 7) und den Umgang mit sensiblen Daten (Kapitel II, Abschnitt III). Daneben führt sie Benachrichtigungspflichten der informationsverarbeitenden Stelle ein und gibt Betroffenen Auskunfts- und Widerspruchsrechte (Kapitel II, Abschnitte IV-VII). Abschnitt VIII des zweiten Kapitels betrifft die Vertraulichkeitspflicht von Dritten sowie technisch-organisatorische Sicherungen.

---

226 Simitis-*Simitis*, BDSG, Einl. Rn. 206.

227 Zuletzt: EuGH Urteil vom 9.3.2012 Rs. C-518/07 *(Datenschutzaufsicht)* Rn. 22.

228 GA *Tizzano*, Schlussanträge vom 14.11.2002 zu EuGH Urteil vom 20.5.2003 verb. Rs. C-465/00, C-138/01 und C-139/01 *(Österreichischer Rundfunk)* Rn. 52 f.

229 GA *Tizzano*, Schlussanträge vom 19.9.2002 zu EuGH Urteil vom 6.11.2003 Rs. C-101/01 *(Lindqvist)* Rn. 41.

230 Zum Ganzen *Siemen*, Grundrecht, S. 257 f.

231 Zur begrifflichen Abgrenzung von Privatsphäre und Privatheit siehe oben Teil 1, II.A.2.a).

Die Richtlinie schuf im Vergleich mit den zuvor bestehenden nationalen Datenschutzgesetzen kein komplett neues Regelungssystem, sondern kombiniert Leitprinzipien der verschiedenen nationalen Datenschutzgesetze.[232] Sie kann deshalb als das gemeinsame „Erbe" oder „Substrat" der Früh- und Mittelphase der nationalen Datenschutzgesetzgebung in Europa bezeichnet werden. Es verwundert deshalb nicht, dass sich die Richtlinie zu einem international genutzten Regelungsmodell entwickelt hat, das beispielsweise mit den Regelungen zum Drittstaatenaustausch nur bei „angemessenem Datenschutzniveau" großen rechtspolitischen Einfluss ausübt.[233] Beispiele für in der Richtlinie aufgegangenen nationalen Konzepte sind die BDSG-Vorschriften über betriebliche Datenschutzbeauftragte und die Sondervorschriften zur Verarbeitung sensibler Daten, die aus dem französischen Datenschutzrecht übernommen wurden.[234] Der Forderung nach kontrollierter Selbstregulierung (Art. 27) liegen wiederum britische und niederländische Konzepte zugrunde. Der Prozess der Kombination führte dabei zu einer Verfeinerung und Fortentwicklung der Ursprungskonzepte, wie es sich beispielsweise in der deutsch-französischen Kontroverse um generelle Meldepflichten zeigt. Weil die Bundesrepublik diese als überflüssige Bürokratisierung ansah und das Modell betrieblicher Datenschutzbeauftragter bevorzugte, wurde den Mitgliedstaaten die Wahl zwischen dem verfahrensorientierten französischen Konzept der Meldepflichten und dem individualorientierten deutschen Ansatz der Bestellung betrieblicher Datenschutzbeauftragter gelassen, Art. 18 Abs. 2 RL 95/46/EG.[235] Neben den besonders kontroversen Regelungen des vierten Kapitels über die Übermittlung personenbezogener Daten an Drittländer (Erfordernis eines angemessenen, adäquaten Schutzniveaus) sieht die Richtlinie Rechtsbehelfe, Haftungs- und Sanktionsvorschriften (Kapitel III) sowie die Errichtung von unabhängigen Kontrollstellen (Kapitel VI) und eines Beratungsgremiums (Artikel-29-Datenschutzgruppe) vor. Letzteres hat die Aufgabe, durch verschiedene Stellungnahmen zur einheitlichen Auslegung der Richtlinie beizutragen und insbesondere das Schutzniveau in Drittländern zu prüfen, Art. 30 Abs. 1 RL 95/46/EG.

### 2. Risikokonzeptionen und Schutzgüter

Obwohl die Aussagekraft der Richtlinie aufgrund ihrer notwendigen Abstraktheit[236] in Bezug auf Risikokonzeptionen eingeschränkt ist, lassen sich gerade aus den allgemeinen Regelungsanforderungen, die eine Synthese nationaler Ansätze darstellen, Rückschlüsse auf Risiken und Schutzgüter entnehmen. Dabei wird

---

232 Simitis-*Simitis*, BDSG, Einl. Rn. 219.

233 Ebd. Rn. 149 f.

234 Ebd. Rn. 210.

235 *Dammann/Simitis*, EG-Datenschutzrichtlinie, Einl. Rn. 11 f.

236 Gerade im Bezug auf die Datenschutzrichtlinie jedoch relativierend *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Einleitung Rn. 12.

– entsprechend der ständigen Rechtsprechung des EuGH – die Richtlinie im Hinblick auf ihre Ziele und das mit ihr eingeführte System ausgelegt.[237]

*a) Anwendungsbereich und Bereichsausnahme*

Die Richtlinie unterscheidet nicht zwischen Datenverarbeitung im öffentlichen und im privaten Bereich und zeigt damit bereits die gestiegene Bedeutung privater Datenverarbeitungen. Sie symbolisiert auf diese Weise die Abkehr von der Konzeption des Datenschutzes als einem reinen Abwehrrecht gegenüber dem Staat hin zu einem umfassenderen Recht.[238] Risiken, die ursprünglich allein staatlicher Herkunft waren, werden durch die staatliche Verwendung privater Datensammlungen auf die private Datenerhebung vorverlagert; konsequenterweise müssen die Datenschutzregelungen dieser Verlagerung folgen. Insoweit wird das in der Rechtsprechung zu Art. 8 EU-GRC konturierte Risiko der privaten Datenverarbeitungen und der staatlichen Nutzung privater Datenbestände aufgegriffen.[239] Weiterhin sind auch nicht automatisierte Verarbeitungen einbezogen, wenn personenbezogene Daten in einer Datei gespeichert und damit nach bestimmten Kriterien zugänglich sind, Art. 3 Abs. 1 i.V.m. Art. 2 c). Erwägungsgrund 27 nennt in diesem Zusammenhang die Gefahr der Umgehung anderer Regelungen. Daneben wird in den Kriterien der „Strukturiertheit" und der „Zugänglichkeit nach bestimmten personenbezogenen Merkmalen" das Risiko einer fehlerhaften Selektivität angedeutet, welches bestimmte Merkmale absolut setzt, ggf. ohne andere relevante Umstände zu berücksichtigen.

Näher zu betrachten ist des Weiteren die Bereichsausnahme des Art. 3 Abs. 2 Spiegelstrich 2. Diese nimmt Verarbeitungen vom Anwendungsbereich der Richtlinie aus, die „von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" vorgenommen werden. Die Ausnahme findet in der Konvention 108 keine Entsprechung. Im zwölften Erwägungsgrund wird als Beispiel „Schriftverkehr" oder die „Führung von Anschriftenverzeichnissen" genannt. Die Begründung zur Richtlinie vom 15.10.1992 nennt als Beispiel das Führen eines „elektronischen Notizbuchs". Nach Ansicht der Literatur gehören zu den persönlichen Tätigkeiten private Korrespondenz sowie Datenverarbeitungen im Rahmen persönlichen Konsums, der Freizeit und des Hobbys. Der Umfang sei dabei nicht entscheidend.[240] Im deutschen Recht findet sich die Bereichsausnahme gleichlautend in § 1 Abs. 2 Nr. 3 BDSG. Die Beurteilung dessen, was als persönlich bzw. familiär anzusehen ist, richte sich dort nach der Verkehrsanschauung. Darunter zu fassen seien Datenverarbeitungen unabhängig vom verwendeten Me-

---

237 EuGH Urteil vom 16.12.2008 Rs. C-73/07 *(Satamedia)* Rn. 51.

238 *Siemen*, Grundrecht, S. 242.

239 Siehe oben II.B.2.c) und d).

240 *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 3 Rn. 8.

dium, die typischerweise zu Freizeit, Liebhabereien, Urlaub, privatem Konsum, Sport, Hobby und Unterhaltung gehören.[241] In der europarechtlichen Literatur wird die Ausnahmevorschrift teilweise als *de-minimis-Regelung*[242] bezeichnet, die davon ausgeht, dass derartige Verarbeitungen keine Risiken für den Schutz der Privatsphäre der betroffenen Personen mit sich bringen.[243] Nach anderer Ansicht ist die Ausnahmeregelung aus dem Gesichtspunkt konkurrierender Grundrechtspositionen dogmatisch zu rechtfertigen.[244] Die Artikel-29-Datenschutzgruppe setzte sich im Rahmen der Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke mit der Bereichsausnahme auseinander.[245] Sie befasst sich darin zunächst mit den Risiken sozialer Netzwerke und zählt hierzu die Erstellung von detaillierten Persönlichkeitsprofilen und Gefahren, die aus der Nutzung personenbezogener Daten durch Unbefugte entstehen. Aufgeführt werden: Identitätsdiebstahl, finanzielle Einbußen, Nachteile für Geschäfts- oder Erwerbsmöglichkeiten und Beeinträchtigungen der körperlichen Unversehrtheit.[246] Die Datenverarbeitungen der Nutzer sozialer Netzwerke seien jedoch – anders als diejenigen der Anbieter – in der Regel als ausschließlich persönliche und familiäre Tätigkeiten von der Ausnahme des Art. 3 Abs. 2 Spiegelstrich 2 erfasst. Festgestellt wird dann allerdings ein zunehmender Trend zur Nutzung des Web 2.0 zu Produktivitäts- und Dienstleistungszwecken, in dessen Rahmen, z.B. bei Nutzung für Vereins- oder Unternehmenszwecke, die Anwendbarkeit gegeben sei. Auch könne eine hohe Anzahl von Drittkontakten ein Anhaltspunkt dafür sein, dass die Ausnahmeklausel nicht anwendbar sei.[247] Gerade die letztere Feststellung wird auch in den Kommentaren zur Datenschutzrichtlinie aufgegriffen. Eine sehr umfangreiche Datenverarbeitung könne demnach darauf hindeuten, dass die Tätigkeiten die Grenze vom Privaten zum Gewerblichen überschreite.[248] Die Datenschutzgruppe nennt als weiteren Faktor für die Überschreitung „ausschließlich persönlicher oder familiärer" Nutzung Zugriffsmöglichkeiten, die über die vom Nutzer selbst ausgewählten Kontakte hinausreichen, z.B. bei Zugriffsberechtigung aller Mitglieder des sozialen Netzwerks oder wenn Daten von externen Suchmaschinen indexiert werden können. Weiterhin kämen „alle Aufgaben und Pflichten des für die Verarbeitung Verantwortlichen zur Geltung, wenn ein Nutzer in voller Kenntnis der Sachlage die Entscheidung trifft, die Zugriffsmög-

---

241 Simitis-*Dammann*, BDSG, § 1 Rn. 151.

242 Nach lat. de minimis non curat praetor (um Kleinigkeiten kümmert sich der Prätor nicht), vgl. http://de.wikipedia.org/wiki/De_minimis [Stand: 28.3.2014].

243 Grabitz/Hilf-*Brühann*, A 30 Art. 3 Rn. 13.

244 *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 3 Rn. 22; *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 3 Rn. 7.

245 Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009, 01189/09/DE WP 163, angenommen am 12.6.2009.

246 Ebd., S. 4.

247 Ebd.

248 *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 3 Rn. 8; Grabitz/Hilf-*Brühann*, Art. 3 Rn. 13.

lichkeit über den Kreis der von ihm selbst ausgewählten ‚Freunde' hinaus auszudehnen".

In diesen Fällen bestehe eine Parallele zu sonstigen Internetveröffentlichungen. Unter Verweis auf die Entscheidung *Satamedia* stellt der EuGH sodann fest, dass der Mangel an Zugriffsbeschränkungen in mehreren Mitgliedsstaaten dazu führe, dass der jeweilige Nutzer die Pflichten des für die Verarbeitung Verantwortlichen erhalte.[249] Der EuGH hatte in dieser Entscheidung nämlich unter Verweis auf die Entscheidung *Lindqvist* ausgeführt, dass Tätigkeiten, die zum Privat- oder Familienleben „offensichtlich" dann nicht vorlägen, wenn Daten einer unbegrenzten Zahl von Personen zur Kenntnis gebracht werden sollen.[250] Im Übrigen verdeutlicht die Auseinandersetzung um die Reichweite der Ausnahmebestimmung die bereits entwickelten Risiken von Überwachungsdruck und individueller Verletzlichkeit durch missbräuchliche Datenverwendung, die insbesondere in der Stellungnahme der Datenschutzgruppe konkretisiert werden. Zweifelhaft erscheinen allerdings die argumentativen Bemühungen um die Ausscheidung der ausschließlich persönlichen oder familiären Datenverarbeitungen. Hier wird angesichts der geänderten technischen Ausgangsbedingungen, insbesondere angesichts des Risikos der staatlichen Nutzung privater Datenbestände, kein geringeres Risiko anzunehmen sein. Dies spricht im Übrigen auch gegen die Einordnung als *de-minimis-Regelung*. Die Risiken von Internetpublikationen und der Verwendung sozialer Netzwerke können im Rahmen des Art. 3 Abs. 2 Spiegelstrich 2 auch deshalb nicht ausschlaggebend sein, da nicht der Umfang oder die Betroffenheit relevant ist, sondern der Zweck. Würde man – wie dies in der Literatur teilweise vertreten wird und in den Äußerungen der Datenschutzgruppe sowie in den Entscheidungen *Satamedia* und *Lindqvist* zumindest anklingt – den Umfang der Datenverarbeitung zum Maßstab machen, so würde dies dem Wortlaut widersprechen, der klar den Zweck der Verarbeitung in den Vordergrund stellt. Überdies würde die Bereichsausnahme angesichts der mittlerweile ubiquitären Datenverarbeitung – gerade zu persönlichen Zwecken – leerlaufen. Vorzugswürdig ist demnach die oben angesprochene Ansicht, die in der Vorschrift keine *de-minimis-Regelung* sondern die Berücksichtigung konkurrierender Grundrechtspositionen ansieht. Eine eigenständige Risikokonzeption sowie Rückschlüsse auf Schutzgüter erlaubt Art. 3 Abs. 2 Spiegelstrich 2 RL 95/46/EG somit nicht unmittelbar. Gleichwohl hat der Streit um die Auslegung die Risiken des Überwachungsdrucks und der Erhöhung individueller Verletzlichkeit weiter bestätigen und konkretisieren können.

---

[249] Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009, 01189/09/DE WP 163, angenommen am 12.6.2009, S. 7.

[250] EuGH Urteil vom 16.12.2008 Rs. C-73/07 *(Satamedia)* Rn. 44; EuGH Urteil vom 6.11.2003 Rs. C-101/01 *(Lindqvist)* Rn. 47.

*b) Allgemeine Regelungskonzeptionen*

Soweit die Richtlinie Regelungskonzepte enthält, die bereits zuvor in der Konvention 108 bzw. in den OECD-Richtlinien enthalten waren, sind hieraus grundsätzlich die vergleichbaren Rückschlüsse auf Risikokonzeptionen und Schutzgüter zu ziehen wie dort. So verweisen die Qualitätsgrundsätze des Art. 6 (Rechtmäßigkeit der Verarbeitung, normative Zweckbegrenzung, Datenrichtigkeit, Erforderlichkeit) auf die folgenden Risiken: Überwachungsdruck durch rechtlich ungesteuerte Datenverarbeitungen, Entkontextualisierung (Kontextinfiltration, Kontextdefizit) bei Datenverwendung zu nicht vorhersehbaren Zwecken, Risiken der individuellen Verletzlichkeit insbesondere bei fehlerhaften Daten und Überwachungsdruck, der bei einer über das Erforderliche hinausgehenden Datensammlung auftreten kann.[251] Darüber hinaus lässt sich das Konzept der normativen Zweckbegrenzung mit dem Risiko der Informationspermanenz verbinden.[252] Art. 7 legt zunächst den Grundstein für das datenschutzrechtliche Prinzip des grundsätzlichen Verbots der Datenverarbeitung und der Erlaubnis im Einzelfall. Der Katalog des Art. 7 a)–f) enthält Erlaubnistatbestände, aus denen mittelbar auf die betroffenen Risiken geschlossen werden kann, da der Unionsgesetzgeber in diesen Fällen offenbar von einem geringeren oder nicht vorhandenen Risiko ausging: Zuerst zielen hier das Konzept der Einwilligung, Art. 7 a)–c), die Informationspflichten der verarbeitenden Stelle, Art. 10, Art. 11 sowie die Auskunfts- und Widerspruchsrechte, Art. 12–14, auf eine Stärkung der Autonomieposition der von der Datenverarbeitung Betroffenen. Soweit keine Einwilligung vorliegt oder die Voraussetzung einer informierten Einwilligung nicht gegeben ist, besteht das Risiko von Fremdbestimmung.

Dieses wird mit der in Art. 7 a)–c) bezweckten Schaffung von Handlungsoptionen in Bezug auf Datenverarbeitung angegangen. Neben dem so aufgegriffenen Risiko von Fremdbestimmung wird zugleich auch das diesem zuzuordnende Schutzgut der Selbstbestimmung – insbesondere aus dem Ziel einer informierten Einwilligung – deutlich. Die Grundsätze des Art. 7 c)–f) nennen hingegen bestimmte Fallgruppen, für die eine Erforderlichkeit und damit Zulässigkeit nicht aus dem Fehlen des Risikos der Fremdbestimmung folgt, sondern sich erst als Abwägungsposition ergibt, z.B. wegen rechtlicher Verpflichtung des Betroffenen, Art. 7 c), oder zur Wahrung lebenswichtiger Interessen der jeweiligen Person, Art. 7 d). Alle Varianten zeigen jedoch durch den Bezug zur Erforderlichkeit, dass auch dort ein bestimmtes Risikopotenzial gesehen wird. Hierin kann aber allenfalls ein grober Verweis auf ein eher diffus verstandenes Risiko des Überwachungsdrucks erkannt werden. Der dritte Abschnitt des ersten Kapitels betrifft besondere Kategorien der Verarbeitung und ist für Rückschlüsse auf konkrete Risiken besser geeig-

---

[251] Siehe oben Teil 1, II.A.2.d).

[252] Siehe oben zur Rechtssache *Google Spain*, II.B.2.d).

net. So verpflichtet Art. 8 die Mitgliedstaaten zur grundsätzlichen Untersagung der Verarbeitung personenbezogener Daten, die sich den folgenden Kategorien zuordnen lassen: rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Art. 8 Abs. 5 enthält Sonderregelungen für Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen. Die Absätze 2–4 enthalten Ausnahme- und Zulässigkeitsregelungen, Abs. 6 Mitteilungspflichten. Absatz 7 etabliert nationale Kennziffern oder andere Kennzeichen allgemeiner Bedeutung als besondere Kategorie. Hierunter dürften beispielsweise Personenkennzahlen und Sozialversicherungsnummern fallen. Mit diesen Vorschriften wird in klarer Weise auf das oben herausgearbeitete Risiko von Diskriminierungen,[253] aber auch auf das Risiko der Auslösung von Schamgefühl abgezielt. Zugleich werden diese Risiken durch die Vorschriften präzisiert.

Erwägungsgrund 33 spricht von „Daten, die aufgrund ihrer Art geeignet sind, die Grundfreiheiten oder die Privatsphäre zu beeinträchtigen". Die Begründung[254] zu Art. 8 weist darauf hin, dass im Allgemeinen nicht der Inhalt personenbezogener Daten, sondern deren Verarbeitungskontext die Gefährdung für das Recht auf Privatsphäre ausmache. Gleichwohl gebe es bestimmte Kategorien von Daten, die aufgrund ihres Inhalts das Risiko mit sich brächten, das Recht der betroffenen Person auf Privatsphäre zu verletzen. In der Etablierung besonderen Schutzes für solche auch als „sensible Daten" bezeichneten Informationen folgt die Richtlinie der Datenschutzkonvention, präzisiert jedoch den Katalog bei den Strafdaten. Weiterhin entwickelt sie den Schutz fort, indem sie nicht nur wie Art. 6 der Konvention einen „geeigneten Schutz" durch innerstaatliches Recht vorsieht, sondern die zulässige Verarbeitung detailliert materiell regelt.[255] Unter diesen materiellen Regelungen findet sich etwa eine Qualifikation der Einwilligung (d.h. ausdrückliche Einwilligung); weiterhin die genaue Umschreibung von Situationen, in denen die Verarbeitung (allein) erforderlich ist, sowie Ausnahmeregelungen zum grundsätzlichen Verarbeitungsverbot. Wie bereits bei der Konvention greifen die Regelungen neben dem Diskriminierungsrisiko auch das Risiko von Publizitätsschäden auf, das entsteht, wenn bestimmte Informationen, die in der Regel schamhaft besetzt sind, veröffentlicht werden.

Besondere Kategorien von Daten werden auch in Art. 18 Abs. 2 behandelt. Die Vorschrift ermöglicht eine Lockerung von Meldepflichten bei belanglosen Daten als Gegenstück zu sensiblen Daten. Weil jedoch der Verarbeitungskontext, also die Zusammenführung mit anderen Informationen, gerade auch die auf den ersten Blick belanglosen Daten, wie beispielsweise die Anwesenheit an einem Ort zu

---

253 Siehe oben Teil 1, II.A.2.d).

254 Begründung abgedruckt bei *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 8, S. 156.

255 Ebd., Art. 8 Rn. 1.

einer bestimmten Zeit, zu Persönlichkeitsprofilen zusammensetzen kann, ist eine derartige Qualifikation eigentlich erst im Nachhinein möglich. „Belanglose" Daten sind somit kaum normativ fassbar. Art. 20 sieht dann – im gleichen Kontext der Meldepflichten – die Möglichkeit von Vorabkontrollen bei spezifischen Risiken vor. Der zugehörige Erwägungsgrund 53 definiert die spezifischen Risiken näher als Verarbeitungen, die aufgrund ihrer Art, Tragweite oder Zweckbestimmungen besondere Risiken im Hinblick auf die Rechte und Freiheiten der jeweiligen Person aufweisen. Als Beispiele werden das Ausschließen einer betroffenen Person von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags sowie die „besondere Verwendung einer neuen Technologie" genannt. Die Begründung[256] verweist hinsichtlich des Merkmals „Art" auf Art. 8 RL 96/46/EG. Hinsichtlich des Merkmals „Tragweite" wird eine Makroperspektive eingenommen, indem die Betroffenheit der gesamten nationalen Bevölkerung genannt wird. Beim Merkmal „Zweckbestimmung" wird der Ausschluss von einer Begünstigung durch ein Recht, eine Leistung oder einen Vertrag als Beispiel genannt („schwarze Listen"). Für die Risikokonzeptionen folgt zunächst aus dem Merkmal „Art" der Daten nichts anderes als im Zusammenhang mit Art. 8 RL 95/46/EG. Die Einnahme der Makroperspektive im Rahmen der Tragweite erinnert an den im Rahmen des Risikos Überwachungsdruck von der Rechtsprechung des EGMR herausgestellten Bezug zum Demokratieprinzip, das durch eine breit angelegte Verunsicherung der Wahlbevölkerung beeinträchtigt werden könnte,[257] bleibt jedoch vage. Der Verweis auf die große Anzahl von Personen ist hingegen zu relativieren, sofern er als „Streubreite" eine besondere Eingriffsintensität markieren soll. Aus grundrechtlicher Sicht wiegt jede individuelle Verletzung gleich schwer, die „Streubreite" stellt insoweit lediglich ein rechtspolitisches Argument dar.[258] Die Ausführungen zum Merkmal „Zweck" korrespondieren wiederum mit den Entkontextualisierungsrisiken, gehen jedoch durch eine offenere Fassung darüber hinaus. So bleibt es unbenommen, hierunter auch Fälle fehlerhafter Selektivität zu fassen, die auf Informationen aus den gleichen Lebensbereichen zurückgehen.

Die Richtlinie enthält ferner in Art. 16 und 17 Vorschriften über Vertraulichkeitspflichten von an Verarbeitungen beteiligten Personen und über technisch-organisatorische Schutzmaßnahmen bei Datenverarbeitungen. Hiermit wird das Risiko der Verletzlichkeit des Einzelnen durch missbräuchliche Verwendung der Daten aufgegriffen. Darüber hinaus werden jedoch keine Anknüpfungspunkte für eine materiell-rechtliche Konkretisierung des Schutzguts gegeben. Hierzu deuten allenfalls die Wörter „Schutzniveau" und „Art der zu schützenden Daten" eine Richtung an, bleiben jedoch vage.[259] Die Regelungen des Kapitel III betreffen

---

256 Begründung abgedruckt ebd., Art. 20, S. 250 f.

257 Siehe oben Teil 1, IV.B.1.

258 Siehe bereits oben II.B.2.e).

259 *Schneider*, ITRB 2012, 180 (185).

Rechtsbehelfe, Haftungs- und Sanktionsvorschriften, die zum Ausgleich materieller, aber insbesondere auch immaterieller Schäden[260] und zur Durchsetzung der übrigen Regelungen geschaffen wurden. Sie verdeutlichen damit erneut das Risiko der Verletzlichkeit Einzelner.

Insgesamt bestätigen die Allgemeinen Regelungskonzeptionen viele der bereits in den speziellen datenschutzrechtlichen Instrumenten und der Rechtsprechung des EGMR herausgebildete Risikokonzeptionen, gestalten diese jedoch näher aus und konkretisieren sie.

### *c) Ausschließlich automatisierte Einzelentscheidungen*

Eine Risikokonzeption, die nicht bereits in der (ursprünglichen Fassung) der Datenschutzkonvention enthalten ist, sieht Art. 15 Abs. 1 vor. Die Vorschrift gewährleistet das Recht,[261] keinen erheblich beeinträchtigenden Entscheidungen sowie Entscheidungen, die rechtliche Folgen nach sich ziehen, unterworfen zu werden, wenn diese ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte der Person erfolgen. Als Beispiele für solche „Aspekte der Person" nennt Art. 15 Abs. 1 die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit und das Verhalten. Abs. 2 enthält jedoch Ausnahmen für Entscheidungen im privaten Rechtsverkehr und bei gesetzlicher Zulassung, soweit bestimmte Garantien zur Wahrung berechtigter Interessen bestehen. Der zugehörige zweite Erwägungsgrund betont den dienenden Charakter von Datenverarbeitungssystemen gegenüber dem Menschen sowie die Grundrechte. In der Begründung[262] wird auf scheinbare Objektivität und Unbestreitbarkeit informationstechnischer Entscheidungen verwiesen. Der Anschein könne dazu führen, dass der Informatik gegenüber menschlichen Entscheidungsträgern übermäßige Bedeutung beigemessen wird und die Entscheidungsträger dadurch ihrer Verantwortung nicht nachkommen. Als Beispiel für einen Widerspruch mit dem Grundsatz wird die allein auf Ergebnisse eines „psychotechnischen" Computertests basierte Ablehnung einer Einstellung verwiesen. Derartige Verarbeitungen würden ein Standardprofil auf die Persönlichkeit anwenden und damit Fälle ausschließen, in denen das System über keine Definition des Persönlichkeitsprofils verfügt. Der in früheren Fassungen verwendete Begriff „Persönlichkeitsprofil" wurde wegen seiner Unschärfe zugunsten der Verarbeitung „zum Zwecke der Bewertung" aufgegeben.[263]

---

[260] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 23 Rn. 5.

[261] Umstritten ist, ob es sich bei Art. 15 Abs. 1 um ein Verbot handelt, da der Wortlaut lediglich die Einräumung eines Rechts und nicht einen Verbotstatbestand vorsieht. Weil aber hinsichtlich der Risikokonzeptionen und Schutzgüter daraus keine Unterschiede folgen und auch die Begründung von einem Verbot ausgeht, wird es im Folgenden als solches bezeichnet, vgl. *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 15 Rn. 5 ff.

[262] Begründung abgedruckt bei *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 15, S. 216.

[263] Ebd., Art. 15 Abs. 6.

Eine vorgeschlagene Zulassung der rein automatisierten Entscheidung bei Vorliegen einer Einwilligung wurde nicht aufgenommen, da eine Einwilligungslösung keine hinreichenden Garantien biete, wenn ein „ungünstiges Machtverhältnis" besteht, wie dies beispielsweise bei der Arbeitssuche der Fall sei. Die Ausnahmen des Abs. 2 sollen hingegen Fälle des credit scoring zulassen, wenn die positive Kreditvergabeentscheidung lediglich auf Grundlage automatischer Risikobewertung ergeht. Bei negativer Punktzahl seien hingegen die berechtigten Interessen – beispielsweise durch eine zwischengeschaltete, nicht automatische Prüfung – zu wahren. In der Literatur werden der Vorschrift zwei Ziele entnommen: Zum einen solle die ausreichende Beteiligung des Betroffenen sichergestellt werden, zum anderen bezwecke die Regelung die Herstellung persönlicher Verantwortung für zu treffende Entscheidungen. Das Risiko einer nur automatisierten Entscheidung liege in der Ignoranz der Individualität der Person und ihrer Degradierung zum bloßen Objekt einer Computeroperation.[264] Maßgeblich ist dabei die inhaltliche Letztverantwortung eines Menschen, die nicht bloß formal sein darf. Das Verbot greift daher nicht, wenn der Technikeinsatz lediglich Vorschläge für Entscheidungen produziert oder diese in anderer Weise unterstützt.[265] Die Vorschrift soll den Menschen davor bewahren, angesichts einer zunehmenden Schematisierung der Lebenssachverhalte im Interesse einer gesteigerten Leistungsfähigkeit nur noch als Teil einer von Experten nach bestimmten scheinbar objektiven und scheinbar „sachgerechten", in Wirklichkeit aber einseitig an Effizienzzielen ausgerichteten Merkmalen definierten Gruppe behandelt zu werden.[266]

Indem die Vorschrift verhindern will, dass Menschen zu bloßen Objekten und „Nummern" einer von Maschinen gesteuerten Wirklichkeit degradiert werden, betrifft sie sämtliche Konstellationen, in denen die Betroffenen als bloßes Mittel zum Zweck betrachtet und dadurch in ihrer Würde als Menschen verletzt werden. Folglich kann die Menschenwürde als Schutzgut identifiziert werden. Das maßgebliche Risiko ist eine Situation, in der Persönlichkeitsprofile zu einem Verantwortungsdefizit führen.

### 3. Zwischenergebnis

Die Datenschutzrichtlinie als praktisch wichtigster Teil des Sekundärrechts kann als gemeinsames „Erbe" bzw. „Substrat" nationaler Datenschutzkonzeptionen der Früh- und Mittelphase der Datenschutzgesetzgebung gesehen werden. Problematisch ist ihre dualistische Zielsetzung aus Grundrechtsschutz und Binnenmarktharmonisierung. Diese Kombination führte zu kompetenzrechtlichen Zerwürfnissen, die jedoch nunmehr durch Art. 16 AEUV beseitigt werden. Inhaltlich knüpft die

---

264 Ebd., Art. 15 Rn. 2.

265 Ebd., Art. 15 Rn. 3.

266 Grabitz/Hilf-*Brühann*, A 30 Art. 15 Rn. 1.

Richtlinie an Art. 8 EMRK und an die Datenschutzkonvention des Europarats an. Hinsichtlich der Risikokonzeptionen und Schutzgüter weist die gemeinsame Regelung von privater und öffentlicher Datenverarbeitung auf die gestiegene Bedeutung der privaten Datenverarbeitung hin, da in ihr alle Risiken der öffentlichen Datenverarbeitung aufgehen, wenn sich der Staat privater Datensammlungen bedient. Näher analysiert wurde zunächst die Bereichsausnahme des Art. 3 Abs. 2 Spiegelstrich 2 für ausschließlich private und familiäre Datenverarbeitungen. Die Ansicht, welche hierin eine Ausnahme aufgrund fehlender Risiken sieht, ist abzulehnen, da die Risiken privater Datenverarbeitungen mittlerweile insbesondere durch soziale Netzwerke stark gestiegen sind. Die für das Vorliegen eines geringeren Risikos gegebenen Begründungen der Materialien und des Schrifttums sind nicht mehr stichhaltig. Vorzugswürdig ist die Auffassung, wonach es sich um eine Vorschrift zum Ausgleich kollidierender Rechte der verarbeitenden Stellen handelt. Die Grenze zwischen zulässiger privater Verarbeitung und gewerblicher Nutzung wird teilweise am Umfang der Verarbeitung festgemacht, wobei insbesondere von der Artikel-29-Datenschutzgruppe auf die Risiken der Nutzung sozialer Netzwerke hingewiesen wird. Die Auseinandersetzung um die Rechtsnatur der Bereichsausnahme hat auch die Risiken des Überwachungsdrucks und der Erhöhung individueller Verletzlichkeit verdeutlicht, insbesondere durch die Ausführungen der Datenschutzgruppe. In die Kategorie der individuellen Verletzlichkeit fallen damit insbesondere Identitätsdiebstahl, finanzielle Einbußen, Nachteile für Geschäfts- oder Erwerbsmöglichkeiten und Beeinträchtigungen der körperlichen Unversehrtheit.[267]

Allgemeine Regelungskonzeptionen, die sich mit denen der Datenschutzkonvention des Europarats überschneiden, greifen auch die dort zugrunde liegenden Risiken auf und entwickeln den Schutz partiell weiter, wie beispielsweise bei den Regelungen zu sensiblen Daten im Rahmen des Art. 18 Abs. 2 RL 95/46/EG. Betroffene Risikokonzeptionen sind Überwachungsdruck, Entkontextualisierung, Erhöhung der individuellen Verletzlichkeit, Fremdbestimmung, Publizitätsschäden durch Schamgefühl sowie insbesondere Diskriminierungen.[268]

Besondere Rückschlüsse auf das Schutzgut der Menschenwürde erlaubt das in Art. 15 Abs. 1 RL 95/46/EG vorgesehene Recht gegen automatisierte Einzelentscheidungen, das die Risiken der Nutzung von Persönlichkeitsprofilen zur Verantwortungsnegation bei nachteiligen Entscheidungen aufgreift und damit eine Situation voraussetzt, in der der Mensch nicht mehr als Selbstzweck sondern nur noch als Mittel zum Zweck behandelt wird.[269]

---

[267] Siehe oben II.B.2.a).

[268] Siehe oben II.B.2.b).

[269] Siehe oben II.B.2.c).

## B. Zwischenbetrachtung: weiteres Sekundärrecht

Neben der Datenschutzrichtlinie wird die gegenwärtige Rechtslage vor allem von zwei Richtlinien geprägt: zum einen die Richtlinie vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (RL 2002/58/EG, im Folgenden: E-Kom-Richtlinie)[270] und zum anderen die Richtlinie vom 15.2.2006 über die „Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“ (RL 2006/24/EG, im Folgenden: Vorratsspeicherungsrichtlinie).[271] Darüber hinaus besteht mit der Verordnung 45/2001/EG „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr“ vom 18.12.2000 (im Folgenden: Datenschutzverordnung) eine Regelung, die den Datenschutz auch gegenüber dem Unionshandeln gewährleistet. Eine nähere Untersuchung dieser Verordnung erübrigt sich allerdings, da die Regelungen abgesehen von dem Adressatenkreis weitgehend parallel zu denen der RL 95/46/EG verlaufen.[272] Die anderen beiden Richtlinien enthalten dagegen an verschiedenen Stellen Regelungskonzepte, die Rückschlüsse auf Risikokonzeptionen und Schutzgüter erwarten lassen, und sind deshalb im Folgenden zu prüfen.

## C. E-Kom-Richtlinie (2002/58/EG) und E-Privacy-Richtlinie (2009/136/EG)

### 1. Überblick

Die RL 2002/58/EG (im Folgenden: E-Kom-Richtlinie) ist eine selbstständige Ergänzung, die neben der allgemeinen Datenschutzrichtlinie (RL 95/46/EG) steht und sektorspezifische Vorgaben für den Bereich der elektronischen Kommunikation enthält.[273] Die Ziele entsprechen denen der allgemeinen Datenschutzrichtlinie. Bezüglich des Grundrechtsschutzes knüpft die E-Kom-Richtlinie jedoch an Art. 7 und Art. 8 EU-GRC an sowie an die „internationalen Menschenrechtsübereinkünfte“, insbesondere die Datenschutzkonvention des Europarats. Schutzgut ist die „Vertraulichkeit der Kommunikation“.[274] Anlass für die Schaffung der Richtlinie war der technische Wandel, der die Vorgängerrichtlinie (97/66/EG) überholte. In-

---

[270] ABl. 2002 L 201/37; zuletzt geändert durch RL 2009/136/EG.

[271] ABl. 2006, L 105/54.

[272] Vgl. EuGH Urteil vom 9.11.2010 Rs. C-92/09 *(Agrarsubventionsdaten)* Rn. 106.

[273] Erwägungsgrund 4.

[274] Erwägungsgrund 2 und 3.

haltlich enthält die Richtlinie technisch-organisatorische Schutzmaßnahmen zur Gewährleistung der Netzwerksicherheit, Art. 4, Regelungen zur Vertraulichkeit der Inhalte von in Kommunikationsnetzen und –diensten übertragenen Nachrichten, Art. 5, sowie Regelungen zu Verkehrs- und Standortdaten, Art. 6, 8, 9. Geregelt werden zudem Spezialbereiche wie der Einzelgebührennachweis, Art. 7, Rufnummernunterdrückung, Art. 8, automatische Anrufweiterschaltungen, Art. 11, Teilnehmerverzeichnisse, Art. 12 sowie unerbetene Nachrichten, Art. 13.[275]

Aufschlussreich hinsichtlich betroffener Risikokonzeptionen und Schutzgüter sind die Erwägungsgründe einschließlich derer der RL 2009/136/EG[276] (im Folgenden: E-Privacy-Richtlinie). Die E-Privacy-Richtlinie (mitunter auch als Cookie-Richtlinie bezeichnet) modifizierte die E-Kom-Richtlinie, um spezifische Risiken zu aufzugreifen. Sie ist deshalb im Zusammenhang mit der E-Kom-Richtlinie in die Untersuchung einzubeziehen. Ferner ist Art. 5 der E-Kom-Richtlinie[277] näher zu untersuchen. Er enthält Regelungen zur Vertraulichkeit der Kommunikation.

## 2. Risikokonzeptionen und Schutzgüter

### *a) Spähsoftware*

Ausdrücklich spricht Erwägungsgrund 24 der E-Kom-Richtlinie betroffene Risiken an. Gegenstand der Äußerung sind Informationen, die in den Endgeräten der Nutzer elektronischer Kommunikationsnetze gespeichert sind. Diese unterlägen als „Teil der Privatsphäre“ der Datenschutzkonvention. Als Beispiel für Risiken wird „Spyware“ genannt. Die Aufzählung, die dann folgt, ist eigenwillig: „Web-Bugs“, „Hidden Identifiers“ und „ähnliche Instrumente“. Dies seien „Instrumente“, die ohne das Wissen des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen oder die Nutzeraktivität zurückzuverfolgen. Sie führten zu einer ernsthaften Verletzung der Privatsphäre. In erster Linie dürften unter diese Beschreibung „trojanische“ Viren fallen. Die eigenwillige Begriffswahl ist wohl dem Anliegen technikneutraler Formulierung geschuldet. Unter dem Blickwinkel einschlägiger Risiken ist mit der unwissentlichen Informationserhebung und Zurückverfolgung vor allem der Einsatz von Überwachungssoftware gemeint. Deren Risiken werden in Erwägungsgrund Nr. 20 als Gegenstand von Aufklärungspflichten der Diensteanbieter genannt, jedoch nicht näher ausgeführt. Die mit Spähsoftware einhergehenden Risiken liegen vor allem in der Erhöhung der Verletzlichkeit des Einzelnen gegenüber missbräuchlicher Datennutzung sowie gegenüber technischen Schäden am betroffenen Gerät. Weiterhin sind sowohl Überwachungsdruck

---

[275] Zum Ganzen *Ohlenburg*, MMR 2003, 82 ff.

[276] ABl. 2009 L 337/11.

[277] Die Änderungen des Art. 5 der E-Kom-Richtlinie durch die E-Privacy-Richtlinie sind für die hiesige Fragestellung unerheblich.

als auch Publizitätsschäden einschlägig, da der Einsatz der Software typischerweise mit Kenntniserlangung gespeicherter intimer Inhalte einhergeht.

### *b) Abgrenzung zu informationstechnischen Schutzgütern*

In Erwägungsgrund 53 der die E-Kom-Richtlinie modifizierenden E-Privacy-Richtlinie (2009/136/EG) werden „Störungen oder unrechtmäßige böswillige Eingriffe“ in Informationssysteme näher umschrieben: Diese beeinträchtigten die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten. Hiermit sind spezifisch informationstechnische Schutzgüter angesprochen. Diese überschneiden sich teilweise mit den hier interessierenden datenschutzrechtlichen Schutzgütern und sind deshalb im Folgenden davon abzugrenzen: In der IT-Sicherheit werden unter dem Schutzgut „Verfügbarkeit“ die Risiken gefasst, dass Daten, Programme oder Hardware verschwinden, nicht zugreifbar oder nicht funktionsfähig sind. Das Schutzgut „Integrität“, also die Verlässlichkeit, wendet sich gegen Datenverfälschungen, gegen die Verarbeitung falscher Daten sowie gegen die Verfälschung von Programmen oder Hardware, die (auch unbemerkt) zu fehlerhaften Ergebnissen oder Funktionsstörungen führen. Das Schutzgut der „Authentizität“ betrifft die Verbindlichkeit vor allem von Daten, insbesondere in Form von Dokumenten und Urkunden, die elektronisch übertragen werden und bei denen die Herkunft gesichert sein muss. Darunter fällt aber auch die Authentizität von Programmen und von Hardware, soweit sie z.B. im elektronischen Zahlungsverkehr eingesetzt werden. Das Schutzgut der „Vertraulichkeit“ wendet sich insbesondere gegen den Zugriff auf Daten durch Unbefugte.[278] Die Vertraulichkeit nimmt eine Sonderstellung ein, indem sie die Inhalte der Nachrichten betrifft. Hierbei handelt es sich um ein vom Datenschutzrecht erfasstes Schutzgut, dessen Doppelfunktion in IT-Sicherheit und im Datenschutz näher zu betrachten ist. Es wird von Art. 5 der E-Kom-Richtlinie aufgegriffen und nachfolgend genauer untersucht.

### *c) Der Begriff der Vertraulichkeit*

Art. 5 E-Kom-Richtlinie verpflichtet die Mitgliedstaaten zur Sicherstellung der Vertraulichkeit von Nachrichten und Verkehrsdaten, die in öffentlichen Kommunikationsnetzen übertragen werden. Es folgt eine Aufzählung von Beispielen, in denen diese Vertraulichkeit verletzt wird: „Abhören, Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten“, jedoch nur soweit diese Handlungen vorgenommen werden durch „andere Personen als die Nutzer“ oder wenn keine Einwilligung der betroffenen Nutzer vorliegt. Die Vertraulichkeit kann damit als Schutz vor unbefugter inhaltli-

---

[278] http://www.datenschutz-berlin.de/content/technik/begriffsbestimmungen/verfuegbarkeit-integritaet-vertraulichkeit-authentizitaet [Stand: 28.3.2014].

cher Kenntnisnahme verstanden werden. Eine weitere Ausnahme bildet die gesetzliche Ermächtigung zu Beschränkungen nach Art. 15 Abs. 1 E-Kom-Richtlinie aus Gründen der nationalen Sicherheit. Nicht entgegen steht zudem eine Speicherung, die aus technischen Gründen für die Weiterleitung erforderlich ist. Art. 5 Abs. 2 E-Kom-Richtlinie enthält eine weitere Ausnahme für rechtlich zulässiges Aufzeichnen von Nachrichten und Verkehrsdaten im Rahmen einer „Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Nachricht". Abs. 3 wird durch die E-Privacy-Richtlinie neu gefasst, betrifft auf dem Endgerät gespeicherte Informationen und stellt deren Speicherung und Zugriff unter Informations- und Einwilligungsvorbehalt, wobei wiederum Ausnahmen für technische Erfordernisse oder bei Erforderlichkeit zur Erbringung eines vom Nutzer ausdrücklich gewünschten Dienstes bestehen. Neben den bereits in Erwägungsgrund 24 hervortretenden Risiken des Einsatzes von Spähsoftware[279] lassen sich in Zusammenschau mit Art. 15 Abs. 1 E-Kom-Richtlinie Rückschlüsse auf das Risiko staatlicher Nutzung privater Daten gewinnen. Die Beschränkung der Vertraulichkeit kann erfolgen, wenn sie sich gem. Art. 13 Abs. 1 RL 95/46/EG auf Gründe der „nationalen Sicherheit", (verstanden als „Sicherheit des Staates"), der „Landesverteidigung", der „öffentlichen Sicherheit", der „Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten" oder des „unzulässigen Gebrauchs von elektronischen Kommunikationssystemen" stützen kann. Weiterhin muss die Verarbeitung „notwendig, angemessen und verhältnismäßig sein". Mit der Einbeziehung der Angemessenheit und Verhältnismäßigkeit geht die Richtlinie über Art. 13 Abs. 1 RL 95/46/EG hinaus, der lediglich das Erfordernis der „Notwendigkeit" aufstellt. Die Ausweitung greift damit die Anforderungen des EGMR an Eingriffe in Art. 8 Abs. 1 EMRK auf und nennt ausdrücklich die vom EGMR im Rahmen der Notwendigkeit geprüften Aspekte der Angemessenheit und Verhältnismäßigkeit.[280] Durch die Begrenzung und rechtliche Steuerung werden die Risiken willkürlicher staatlicher Überwachung, insbesondere der Überwachungsdruck sowie das damit einhergehende Machtpotenzial, aufgegriffen und der Versuch unternommen, diese rechtlich einzuhegen.

#### *d) Allgemeine Regelungskonzeptionen*

Explizit angesprochen werden Risiken im Rahmen des Erwägungsgrundes Nr. 61 E-Privacy-Richtlinie (2009/136/EG), der eine Begründung dafür liefert, weshalb Betreiber nach Bekanntwerden einer Verletzung der Datenschutzvorschriften die nationale Aufsichtsbehörde und ggf. die Betroffenen unterrichten sollen (Privacy-Breach-Notification, durch die E-Privacy-Richtlinie angefügter Art. 4 Abs. 3 der E-Kom-Richtlinie). Die Verletzung könne zu erheblichen wirtschaft-

---

279 Siehe oben III.C.2.a).

280 Siehe oben Teil 1, IV.A.

lichen Schäden und sozialen Nachteilen einschließlich des Identitätsbetrugs führen, sofern nicht rechtzeitig und angemessen reagiert werde. Die Auswirkungen seien nachteilig, „wenn sie z.B. Identitätsdiebstahl oder -betrug, physische Schädigung, erhebliche Demütigung oder Rufschaden in Verbindung mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in der Gemeinschaft zur Folge haben".

Auf diesen Erwägungen baut der ebenfalls durch die E-Privacy-Richtlinie neu gefasste Art. 2 h) auf, der die Verletzung des Schutzes personenbezogener Daten als eine Sicherheitsverletzung definiert, durch die personenbezogene Daten bei ihrer Verarbeitung unbeabsichtigt oder unrechtmäßig vernichtet, verloren, verändert oder unbefugt weitergegeben bzw. zugänglich gemacht werden. Die in den Erwägungsgründen beschriebenen Folgen lassen sich unter dem Risiko der individuellen Verletzlichkeit zusammenfassen und verdeutlichen dessen verschiedene Komponenten. Zeitliche Begrenzungen der Speicherpflicht, wie sie beispielsweise in den Erwägungsgründen 26 und 27 vorgesehen sind, unterstreichen diese Risikokonzeption.

Aus den inhaltlichen Regelungen lassen sich hingegen lediglich einige allgemeine Rückschlüsse ziehen: Die einschränkenden Regelungen zu Verkehrs- und Standortdaten sowie zu Einzelverbindungsnachweisen sind maßgeblich für das zugrunde liegende Risiko der Bildung von Persönlichkeitsprofilen bzw. dem damit einhergehenden Überwachungsdruck. Erwägungsgrund 33 E-Kom-Richtlinie spricht zwar recht unbestimmt von einer „Gefahr für die Privatsphäre"; die Berechtigung zum opt-out hinsichtlich Einzelverbindungsnachweisen, Art. 7 Abs. 1, sowie die in Art. 8 vorgesehene Möglichkeit der Rufnummernunterdrückung gewährleisten die anonyme Nutzung z.B. telefonischer Seelsorgedienste und Beratungshotlines. Letztere werden in Erwägungsgrund Nr. 34 E-Kom-Richtlinie explizit angesprochen. Das mit einer nicht anonymisierten Nutzung einhergehende Schamgefühl (Publizitätsschaden) und mögliche Diskriminierungen stehen als Risiken hinter den Regelungen. Erwägungsgrund 35 E-Kom-Richtlinie expliziert dies hinsichtlich von Standortdaten; diese sind teilweise genauer, als es zur Nachrichtenübertragung erforderlich wäre. In diesen Fällen soll eine zeitweise Untersagung durch die Nutzer auf einfache Weise möglich sein. Hierin ist wiederum die Auswirkung des Kontrollparadigmas zu sehen, wonach der Nutzer selbstbestimmt über die Datenverwendung entscheiden können soll. Die in Art. 12 festgelegten Einschränkungen der Aufnahme personenbezogener Daten in Teilnehmerverzeichnisse begründet Erwägungsgrund Nr. 38 E-Kom-Richtlinie mit deren weiter Verbreitung und Öffentlichkeit. Das verbundene Risiko sind Publizitätsschäden, die aus dem großen Wirkungskreis entstehen. Art. 13 E-Kom-Richtlinie wurde durch die E-Privacy-Richtlinie neu gefasst und betrifft unerbetene Nachrichten, die insbesondere zur Direktwerbung erfolgen. Das hiermit verbundene Geschehen ist die Belästigung durch Werbesendungen, Spamnachrichten und Anrufe, wobei noch zu klären ist, ob es sich dabei wirklich um ein Risiko im hier zu beschreibenden Sinne handelt.

### 3. Zwischenergebnis

Die E-Kom-Richtlinie (2002/58/EG) sowie deren Änderungen und Ergänzungen im Rahmen der E-Privacy-Richtlinie (2009/136/EG) sind hinsichtlich der Ziele an die allgemeine Datenschutzrichtlinie 95/46/EG angelehnt.[281] Die erste relevante Risikokonzeption folgt aus der Einbeziehung des Einsatzes von Spähsoftware. Hiermit verbunden sind die Risiken der Verletzlichkeit des Einzelnen gegenüber missbräuchlicher Datennutzung und technischen Schäden sowie der allgemeine Publizitätsschaden durch Offenlegung typischerweise intimer Informationen.[282]

Die informationstechnischen Schutzgüter der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten werden in Erwägungsgrund 53 E-Privacy-Richtlinie aufgegriffen und damit die spezifischen Risiken, welche in der IT-Sicherheit damit verbunden sind, einbezogen.[283] Von besonderer Bedeutung ist das Schutzgut der Vertraulichkeit, welches mit Art. 5 E-Kom-Richtlinie eine tragende Regelung der Richtlinie darstellt. Es richtet sich gegen unbefugte inhaltliche Kenntnisnahme und wird so dem Risiko der Erhöhung individueller Verletzlichkeit zugewiesen. Dem Schutzgut kommt eine „Doppelrolle“ mit Bedeutung sowohl im Rahmen der IT-Sicherheit als auch der datenschutzrechtlichen Schutzgüter zu. Die Ausnahmevorschriften des Art. 15 Abs. 1 E-Kom-Richtlinie deuten auf das Risiko staatlicher Verwendung privater Datenbestände hin. Dieses wird jedoch nur eingeschränkt und in erster Linie gegen willkürliche und übermäßige Eingriffe unter Anknüpfung an die Rechtsprechung des EGMR zu Art. 8 EMRK in Stellung gebracht.[284]

Aus den übrigen, allgemeinen Regelungskonzepten der Richtlinien lassen sich Rückschlüsse auf das Risiko der individuellen Verletzlichkeit folgern, das mit einer Reihe von Beispielen, u.a. dem Identitätsdiebstahl und Identitätsbetrug angereichert wird. Das Risiko von Publizitätsschäden wird durch die Topoi „erhebliche Demütigungen“ und „Rufschädigung“ konkretisiert. Weiterhin zielen die Richtlinien auf die Risiken „Überwachungsdruck“ sowie „Diskriminierung“, jedoch ohne hier über die auch aus den anderen Instrumenten gezogenen Folgerungen hinauszugehen. Eine Besonderheit liegt im Bezug auf unerwünschte Direktwerbung, die womöglich eher als Belästigung denn als Risiko anzusehen ist.[285]

---

281 Siehe oben III.C.1.

282 Siehe oben III.C.2.a).

283 Siehe oben III.C.2.b).

284 Siehe oben III.C.2.c).

285 Siehe oben III.C.2.d).

## D. Vorratsspeicherungsrichtlinie (2006/24/EG)

### 1. Überblick

Die am 8.4.2014 vom EuGH für ungültig erklärte[286] Richtlinie 2006/24/EG über die „Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG" wurde im Zuge der Terroranschläge von London (7.7.2005) unter britischer und österreichischer Ratspräsidentschaft verabschiedet. Zuvor war ein von Frankreich, Irland, Schweden und Großbritannien eingebrachter Entwurf eines Rahmenbeschlusses in Folge der Terroranschläge von Madrid (11.2.2004) an massivem Widerstand des Europäischen Parlaments und unter Kritik seitens des Rats und der Kommission bezüglich der Rechtsgrundlage gescheitert. Daraufhin legte die Kommission Ende September 2005 den auf Art. 95 EG a.F. gestützten Richtlinienentwurf vor.[287] Er verpflichtete Anbieter von Telekommunikations- und Internetdiensten zur anlass- und verdachtlosen Speicherung von Verkehrsdaten für Sicherheitsbehörden in erheblichem Umfang. Die Richtlinie war von Beginn an in der Öffentlichkeit und Fachpublizistik heftig umstritten und wurde als Fall der „Politikwäsche" (policy laundering) betrachtet. Hierunter wird der Versuch verstanden, auf nationaler Ebene politisch nicht akzeptierte Regelungen über den „Umweg Europa" durchzusetzen und dabei die bislang nicht vorhandene europäische Öffentlichkeit auszunutzen, indem auf die Umsetzungspflicht verwiesen wird, um auf diese Weise nationaler Kritik zu entgehen.[288]

Gegen die Richtlinie klagte die Republik Irland erfolglos vor dem EuGH.[289] Entsprechend den Anträgen befasste sich der EuGH in dieser ersten Entscheidung zur Vorratsdatenspeicherung allein mit der formellen Rechtmäßigkeit und klammerte die Frage der Grundrechtsverletzung aus.[290] Er entschied, dass die Richtlinie zu Recht auf die Binnenmarktkompetenz gestützt wurde und begründete dies mit den tiefgreifenden Unterschieden zwischen den nationalen Vorratsdatenspeicherungsregelungen. Die Unterschiede beeinträchtigten den Wettbewerb zwischen den Mitgliedstaaten, insbesondere weil sie zu erheblichem finanziellen Mehraufwand führten.[291] In der Literatur stieß diese Argumentation wegen der rein negativen Binnenmarktwirkung (Generalisierung der Speicherpflicht) und der bloßen Akzessorietät des Ziels „Binnenmarktharmonisierung" im Vergleich zum Hauptziel

---

[286] EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* = BeckRS 2014, 80686; siehe oben II.B.2.d).

[287] *Westphal*, EuR 2006, 706 (707).

[288] Ebd., 706 (718).

[289] EuGH Urteil vom 10.2.2009 Rs. C-301/06 *(Vorratsdatenspeicherung I)*.

[290] Ebd. Rn. 57.

[291] Ebd. Rn. 63–68.

„Strafverfolgungsvorsorge“ auf Ablehnung.[292] Die Umsetzungsfrist endete bereits am 15.9.2007. Ein Zwischenbericht der Kommission offenbarte jedoch die Bedenken der Mitgliedstaaten hinsichtlich der Rechtmäßigkeit der Richtlinie.[293] Im Jahr 2010 erklärte das BVerfG das deutsche Umsetzungsgesetz für verfassungswidrig.[294] Die Richtlinie wurde auch in den übrigen Mitgliedstaaten nur teilweise umgesetzt bzw. von nationalen Verfassungsgerichten für rechtswidrig erklärt.[295] Gleichwohl strengte die Kommission noch Ende Mai 2012 ein Vertragsverletzungsverfahren gegen Deutschland an und beantragte die Zahlung eines täglichen Zwangsgeldes in Höhe von 315.036,54 €.[296] Am 8.4.2014 hat der EuGH dann entschieden, dass die Richtlinie den Verhältnismäßigkeitsgrundsatz in Bezug auf Art. 7, 8 und 52 EU-GRC verletzt und deshalb ungültig ist.[297]

### 2. Fehlende Risikosensibilität

Weil die umfassende Speicherung von den in Art. 5 der Vorratsspeicherungs-RL genannten Daten – insbesondere Rufnummern, Name und Anschrift der Teilnehmer und Zeit des Kommunikationsvorgangs – eine potenziell vollständige Rekonstruktion aller Kommunikationsvorgänge mit Ausnahme der Inhalte ermöglicht, wird allgemein und auch in der Rechtsprechung des EuGH von einer erheblichen Eingriffstiefe ausgegangen.[298] Dies erklärt sich nicht nur aus der Möglichkeit zur Erstellung von Bewegungsprofilen und der Aufklärung des Bekanntenkreises, sondern auch aus der Nähe zu einer Inhaltsüberwachung durch die Speicherung aufgerufener Internetseiten.[299] Die Richtlinie behandelt den Datenschutz dagegen lediglich in Art. 7 sowie hinsichtlich der Kontrolle der Datensicherheit in Art. 9 und stellt dort überwiegend Anforderungen an den technisch-organisatorischen Schutz. Nicht enthalten sind insbesondere eine nähere Zweckbestimmung, eine hinreichend bestimmte Definition des Begriffs „schwere Straftaten“, Art. 1 Abs. 1 sowie Regelungen zur Sicherstellung der Erforderlichkeit und Angemessenheit des Ein-

---

[292] Vgl. *Klesczewski*, HRRS 2009, 250 (251).

[293] „Geleakt“ von der Bürgerrechtsorganisation „Quintessenz“: http://quintessenz.at/doqs/000100011699/2011_12_15,Eu_Commission_data_retention_reform.pdf [Stand: 13.9.2012].

[294] BVerfGE 125, 260, siehe unten Teil 3, II.B.8.

[295] Zum Ganzen *Albrecht/Kilchling*, Gutachten Vorratsdatenspeicherung, S. 181 ff.

[296] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/530&format=HTML&aged=0&language=DE&guiLanguage=en [Stand: 28.3.2014].

[297] EuGH Urteil vom 8.4.2014 Rs. C-293/12, C-594/12 *(Vorratsdatenspeicherung II)* = BeckRS 2014, 80686 Rn. 69 f.; siehe oben II.B.2.d).

[298] Zur Einschätzung von GA *Villalón* siehe oben II.B.2.d).

[299] Statt vieler *Westphal*, EuR 2006, 706 (714 ff.) sowie die interaktive Demonstration der Einsatzmöglichkeiten von Verkehrsdaten auf http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten [Stand: 28.3.2014].

griffs.[300] Die fehlenden Regelungen zur Wahrung der Verhältnismäßigkeit führten dementsprechend auch zur Ungültigerklärung der Richtlinie durch den EuGH am 8.4.2014.[301]

### 3. Zwischenergebnis

Aus dem normativen Programm der Richtlinie 2006/24/EG können aufgrund der mangelhaften Perzeption von Risiken für die vorliegende Untersuchung keine Rückschlüsse folgen. Die Risiken der Vorratsdatenspeicherung werden auf Ebene des Primärrechts im Rahmen des Urteils des EuGH zur Vorratsspeicherungsrichtlinie[302] sowie auf Ebene des nationalen Verfassungsrechts untersucht.[303]

## E. Rahmenbeschluss Datenschutz polizeiliche/justizielle Zusammenarbeit (2008/977/JI)

### 1. Überblick

Der am 19.1.2008 in Kraft getretene Rahmenbeschluss 2008/977/JI[304] über den „Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden" (im Folgenden Rahmenbeschluss) stützt sich auf Art. 30, 31 e) und Art. 34 Abs. 2 b) EUV a.F. Mit ihm wurden die zuvor nur in einzelnen Rechtsakten geregelten Datenschutzanforderungen für den Bereich der ehemaligen Dritten Säule vereinheitlicht. Von einer Untersuchung der einzelnen Rechtsakte der ehemals Dritten Säule, insbesondere Europol, Eurojust, ZIS und Prümer Vertrag, kann deshalb abgesehen werden.[305] Rahmenbeschlüsse waren ein bis zum Inkrafttreten des Vertrags von Lissabon für die polizeiliche und justizielle Zusammenarbeit in Strafsachen in den Art. 29–42 EUV a.F geregeltes Instrument, das sich am ehesten mit Richtlinien vergleichen lässt. Rahmenbeschlüsse waren hinsichtlich des zu erreichenden Ziels für die Mitgliedstaaten verbindlich; die genaue Art und Weise der Umsetzung wurde jedoch den innerstaatlichen Stellen überlassen. Sie sind – anders als Richtlinien unter bestimmten Voraussetzungen – nicht unmittelbar anwendbar. Nach dem Vertrag von Lissabon ersetzt das „ordentliche Gesetzgebungsverfahren" nunmehr das Instru-

---

300 Ebd., 706 (714 ff.).

301 Siehe oben II.B.2.d).

302 Siehe oben II.B.2.d).

303 Siehe unten Teil 3, II.B.8.

304 ABl. L 350 vom 30.12.2008, S. 60.

305 Überblick zu diesen Regelungen bei *Eisele*, in: Sieber u.a. (Hrsg.), Europäisches Strafrecht, S. 781. Die Regelungen erschöpfen sich zumeist in Verweisen auf die Datenschutzkonvention oder auf innerstaatliches Recht, vgl. Erwägungsgrund Nr. 40.

ment der Rahmenbeschlüsse. Für den Bereich der Verarbeitungsregelungen (auch in Bezug auf die ehemalige Dritte Säule) folgt die Kompetenz u.a. aus Art. 16 Abs. 2 AEUV. Die Regelungsinstrumente ergeben sich aus Art. 289 Abs. 1 AEUV.[306] Die alten Rahmenbeschlüsse gelten bis zu einer Änderung durch Regelungsinstrumente des derzeit gültigen Vertragswerks fort.[307]

Als Ziel nennt Art. 1 Abs. 1 Rahmenbeschluss die Grundrechtskonformität der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen und „gleichzeitig" die Gewährleistung eines „hohen Maßes" an öffentlicher Sicherheit. Inhaltlich orientiert sich der Beschluss an den Grundsätzen der Datenschutzrichtlinie und den übrigen Datenschutzregelungen der Rechtsakte der ehemals Dritten Säule.[308] Vielfach kritisiert wurde jedoch die „verwässerte" Umsetzung mittels allgemeiner Formulierungen und zahlreicher Ausnahmevorschriften, insbesondere den Durchbrechungen des Zweckbindungsgrundsatzes.[309]

### 2. Risikokonzeptionen und Schutzgüter

Zugrunde liegende Risikokonzeptionen entstammen den abgeschwächt umgesetzten Regelungsmodellen anderer Datenschutzinstrumente, namentlich der Datenschutzkonvention des Europarats und der Richtlinie 95/46/EG. Auf diese wurde bereits oben eingegangen.[310] Beachtenswert ist, dass neben den Rückschlüssen auf die Risiken der Entkontextualisierung, des Überwachungsdrucks und der Selektionsschäden auch das Risiko der Verantwortungsnegation aufgegriffen wird, indem Art. 7 Schutz vor ausschließlich automatisiert erfolgenden Einzelentscheidungen bietet. Aus dem im Einzelnen geringeren Schutzstandard durch allgemeinere Formulierungen und Ausnahmeregelungen[311] ist hingegen nicht auf eine abweichende Risikokonzeption zu schließen. Dieser erklärt sich vielmehr mit dem politischen Entstehungsprozess des Instruments: Die „beschränkten Konsensmöglichkeiten" des Rates illustrieren insoweit die einseitige Berücksichtigung von Verarbeitungsinteressen.[312] Darüber hinaus werden spezifische Risiken zwar an zwei Stellen erwähnt, jedoch nicht näher ausgeführt – so in Erwägungsgrund 32, der lediglich auf

---

306 Zum Ganzen Simitis-*Simitis*, Einl. Rn. 242; Bericht der Kommission vom 25.1.2012, KOM 2012 (12) endgültig, S. 2.

307 Art. 9 und 10 der Übergangsbestimmungen, Protokoll Nr. 36 zum Vertrag von Lissabon, ABl. Nr. C-115 vom 9.5.2008, S. 1-388.

308 *Eisele*, in: Sieber u.a. (Hrsg.), Europäisches Strafrecht, S. 784.

309 Simitis-*Simitis*, Einl. Rn. 240; sowie Europäischer Datenschutzbeauftragter, Stellungnahme vom 23.6.2007, ABl. C 139/1 S. 5.

310 Siehe oben Teil 1, II.A.2.d) und Teil 2, III.A.2.b).

311 Vgl. auch Erwägungsgrund Nr. 40 sowie, als Beispiel für den geringeren Schutzstandard, die Durchbrechungen des Zweckbindungsgrundsatzes in Art. 11.

312 Simitis-*Simitis*, Einl. Rn. 241 f.

die Verarbeitung mithilfe „neuer Technologien, Mechanismen oder Verfahren“ als Risiko verweist. Die Regelung über technisch-organisatorische Schutzmaßnahmen, Art. 22 Rahmenbeschluss, spricht in Abs. 1 Satz 2 lediglich allgemein von Risiken, die von der Verarbeitung ausgehen. Abs. 2 nennt dann einen Katalog verschiedener Schutzmaßnahmen, der auf die Verhinderung unbefugter Verarbeitung (Schutzgut der Vertraulichkeit, Risiko der individuellen Verletzlichkeit) durch eine Reihe von Kontrollen und Sicherungspflichten abzielt und zuletzt auch auf das informationstechnische Schutzgut der Integrität eingeht. Einen weiterführenden Aspekt verdeutlicht die Vorschrift über die Vertraulichkeit, Art. 21 Abs. 2 Rahmenbeschluss. Hiernach werden die Pflicht zur allein dienstlichen Nutzung der Daten sowie sämtliche behördlichen Datenschutzbestimmungen auf Personen erstreckt, „die beauftragt werden, für eine zuständige Behörde eines Mitgliedstaats zu arbeiten“. Hiermit wird das Risiko des Einsatzes privater Stellen in der polizeilichen Datenverarbeitung angesprochen. Ein solcher Einsatz kann insbesondere zur Erhöhung des Überwachungsdrucks führen, wenn die nichtstaatlichen Akteure nicht den gleichen Verarbeitungsregelungen unterworfen werden wie die staatlichen Stellen. Hierdurch können jedoch prinzipiell auch die Risiken von Publizitätsschäden und individueller Verletzlichkeit gesteigert werden, soweit bei Privaten von geringeren Schutzstandards ausgegangen wird. Insgesamt handelt es sich somit um ein spezifisches Umgehungsrisiko.

### 3. Zwischenergebnis

Der Rahmenbeschluss 2008/977/JI ist an den Regelungen der Datenschutzkonvention und der Richtlinie 95/46/EG orientiert und verweist insoweit auf deren Risikokonzeptionen. Der schwächere Schutzstandard ist dem politischen Entstehungsprozess geschuldet und lässt nicht auf eine veränderte Risikowahrnehmung schließen. Als eigenständige Risikokonzeption verweist Art. 21 Abs. 2 auf das Risiko der Umgehung von Schutzvorschriften durch den Einsatz privater Stellen bei polizeilichen Datenverarbeitungen.

## F. Reformvorschlag vom 25.1.2012: Grundverordnung

### 1. Überblick

Die umfassende Neuregelung des Datenschutzes auf Unionsebene wurde ab Mitte 2009 durch das unter schwedischer Ratspräsidentschaft entstandene Stockholmer Programm[313] und den daran anknüpfenden Aktionsplan[314] forciert. Dieses Fünf-

---

[313] Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger. KOM (2009) 262 endgültig vom 10.6.2009.

Jahresprogramm mit Richtlinien zur gemeinsamen Innen- und Sicherheitspolitik der Mitgliedstaaten sieht vor, dass die Union eine „umfassende Regelung zum Schutz personenbezogener Daten schaffen muss, die für sämtliche Zuständigkeitsbereiche der Union gleichermaßen gilt", und dass sie zudem für die „konsequente Anwendung des Grundrechts auf Datenschutz" zu sorgen hat.[315] Im Anschluss hieran erfolgten öffentliche Anhörungen sowie Gespräche mit Interessenvertretern. Am 4.11.2010 wurde eine Mitteilung über das Gesamtkonzept durch die Kommission veröffentlicht, zwischen September und Dezember 2011 folgte die Erörterung mit den nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten.[316] Am 25.1.2012 wurden sodann die Reformvorschläge zum „Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert" veröffentlicht.[317] Das Kernstück der Reform ist die auf Art. 16 AEUV gestützte Datenschutz-Grundverordnung (GV-Vorschlag).[318] Die Verordnung wäre im Fall des Inkrafttretens gem. Art. 288 AEUV unmittelbar anwendbar. Ziel ist die „Stärkung der Wirksamkeit des Grundrechts auf Datenschutz und die Übertragung der Kontrolle über die Daten an die Betroffenen, insbesondere vor dem Hintergrund der technologischen Entwicklungen und der zunehmenden Globalisierung."

Weiterhin soll die Verordnung zu einer „Vertiefung der Binnenmarktdimension" des Datenschutzes beitragen, indem sie Unterschiede in den Regelungen abbaut, Kohärenz verstärkt, das Regelungsumfeld vereinfacht, dadurch unnötige Kosten vermeidet und den Verwaltungsaufwand verringert.[319] In der Literatur stoßen die Reformvorschläge aufgrund ihrer Allgemeinheit und Unbestimmtheit überwiegend auf Kritik.[320] Die Verordnung baut in wesentlichen Teilen auf den Regelungskonzepten der Richtlinien 95/46/EG und 2002/58/EG auf, enthält jedoch auch neue Regelungen und Weiterentwicklungen. Die Richtlinie 95/46/EG soll mit der Grundverordnung abgelöst, die Richtlinie 2002/58/EG geändert werden. Zu der in der Richtlinie 95/46/EG bereits enthaltenen Regelungskonzeption gehören insbesondere die Verarbeitungsgrundsätze, Art. 5 GV-Vorschlag, die – etwas bestimmter gefasste – Regelung der Einwilligung, Art. 7 GV-Vorschlag, das Konzept sensibler

---

[314] Aktionsplan zur Umsetzung des Stockholmer Programms. KOM (2010) 171 endgültig vom 20.4.2010.

[315] KOM (2009) 262 endgültig, S. 33; KOM (2010) 171, S. 3.

[316] Näher zu den Vorarbeiten KOM (2012) 11 endgültig, S. 2.

[317] KOM (2012) 9 endgültig.

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

[319] KOM 2012 (11), S. 116.

[320] *Tinnefeld/Schild*, DuD 2012, 312 (317); *Schneider/Härting*, ZD 2012, 199 (203); *Schneider*, ITRB 2012, 180 (185 f.). Verhalten positiv dagegen *von Lewinski*, DuD 2012, 564 (569 f.).

Daten, Art. 9 GV-Vorschlag, sowie Informationspflichten, Abschnitt 2 GV-Vorschlag.[321] Bei der nun folgenden Prüfung der Risikokonzeptionen und Schutzgüter wird das Augenmerk deshalb auf darüber hinausgehende und eigenständige Gehalte des Verordnungsvorschlags gelegt.

### 2. Risikokonzeptionen und Schutzgüter

Die Einleitung zum Vorschlag der Grundverordnung bezieht sich zunächst auf die wirtschaftlichen Aspekte des Datenschutzes: Die Möglichkeit zur Kontrolle persönlicher Informationen und ein hohes Datenschutzniveau seien nötig, um zu verhindern, dass die Verbraucher ihr Vertrauen in Online-Dienste verlieren, weil dadurch das Potenzial der digitalen Wirtschaft nicht ausgeschöpft werden könne. Erforderlich seien moderne kohärente Regeln für den freien Datenverkehr, um den Verwaltungsaufwand der Unternehmen auf ein Mindestmaß zu begrenzen. Hierdurch würde auch das Wirtschaftswachstum „angekurbelt".

Zur Illustration der Binnenmarktaspekte verweist die Einleitung auf Umfragen zum gefühlten Kontrollverlust hinsichtlich personenbezogener Daten und nennt verschiedene Beispiele, darunter das vergebliche Bemühen um Auskunft und Löschung von Daten in einem sozialen Netzwerk sowie die Datenverluste infolge des Hackings von Kundendatenbanken und die uneinheitliche Reaktion der Datenschutzbehörden auf Online-Kartierungssysteme. Art. 8 und Art. 16 EU-GRC werden dagegen in der Einleitung lediglich kurz angedeutet.[322]

Auch die Begründung des Verordnungsentwurfs bezieht sich zunächst auf das Schutzgut des Vertrauens in die „Online-Umgebung" als Grundlage für Online-Einkäufe sowie auf die schnelle Entwicklung und Nutzung innovativer neuer Technologien. Unterstrichen wird dies durch Erwägungsgrund Nr. 6, der explizit die Notwendigkeit einer „Vertrauensbasis" für die „digitale Wirtschaft" benennt. Der Weg zu dieser Vertrauensbasis führe über die Kontrolle, die jede Person über die „eigenen Daten" besitzen solle. An dieser Stelle überschneidet sich die Begründung mit der wirtschaftspolitischen Ausreichung der Datenschutzkonvention und den OECD-Leitlinien:[323] Der Erwägungsgrund vermittelt den Eindruck, dass es nicht die Grundrechtsaspekte sind, welche die Einräumung von Kontrolle an die Betroffenen erfordern, sondern vielmehr der ökonomische Nutzen, der aus dem zu wahrenden Kundenvertrauen folgt. Sodann wird jedoch die Grundrechtsverankerung von der Begründung einbezogen. Angeknüpft wird hierzu an Art. 8 EU-GRC, Art. 16 AEUV und Art. 8 Abs. 1 EMRK. Ein enger Zusammenhang bestehe mit

---

321 Zur diesbezüglichen Analyse der Risikokonzeptionen und Schutzgüter siehe oben III.A.2.b).

322 KOM (2012) 9 endgültig, S. 1 ff.

323 Siehe oben Teil 1, II.A.2.a) sowie D.2.

Art. 7 EU-GRC.[324] Unterstrichen wird dies auch durch Erwägungsgrund Nr. 1, der klarstellt, dass der Schutz natürlicher Personen bei der Datenverarbeitung ein Grundrecht ist und gem. Art. 8 Abs. 1 EU-GRC und Art. 16 Abs. 1 AEUV jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Erwägungsgrund Nr. 2 verdeutlicht die aufrechterhaltene „dualistische" Zielrichtung, die der Richtlinie 95/46/EG entspricht. Neben dem Grundrechtsbezug soll die Datenverarbeitung auch zur Vollendung der Wirtschaftsunion zum wirtschaftlichen Fortschritt und dem Zusammenwachsen der Volkswirtschaften im Binnenmarkt beitragen. Erwägungsgrund Nr. 5 nennt den technologischen Fortschritt als Anlass und bezieht sich insbesondere auf die Veröffentlichung personenbezogener Daten im Internet. Die Erwägungsgründe Nr. 3 und 7 bestätigen die fortwährende Gültigkeit der Grundsätze der Richtlinie 95/46/EG und deren Ziel der Grundrechtsharmonisierung.

Die Verordnung gliedert sich in 11 Kapitel. Die „Allgemeinen Bestimmungen" (Kapitel 1) sowie die „Grundsätze" (Kapitel 2) enthalten nur geringe Abweichungen von den Regelungen der Richtlinien 95/46/EG und 2002/58/EG.[325] Das dritte Kapitel enthält – allgemein formulierte – Transparenzanforderungen sowie Informationspflichten, Auskunfts- und Berichtigungs- bzw. Löschungsrechte. In persönlicher Hinsicht ist der Verordnungsvorschlag auf den Schutz natürlicher Personen begrenzt, Art. 1 Abs. 1 und Abs. 2 sowie Erwägungsgrund Nr. 12. Bemerkenswert ist dabei die Übernahme eines Konzepts verschiedener Identitäten, die sich in der Definition der „betroffenen Person", Art. 4 Abs. 1, zeigt. Betroffener ist demnach, wer mit Mitteln bestimmt werden kann. Zu diesen „Mitteln" gehört auch die Zuordnung zu „besonderen Merkmalen", die Ausdruck der „physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität" sind. Hiermit wird an die in der neueren Rechtsprechung des EGMR verfolgte Schutzgutkonzeption angeknüpft.[326] Die „untere" Grenze des Anwendungsbereichs stellt weiterhin die „Ausnahme für Privathaushalte" dar. Verarbeitungen rein persönlicher oder familiärer Natur, die natürliche Personen zu nichtgewerblichen Zwecken vornehmen, werden wie schon bei der Vorgängerrichtlinie nicht erfasst, Art. 2 Abs. 2 d), Erwägungsgrund 15.[327]

### *a) Recht auf Vergessen*

Näher zu betrachten ist zunächst der aus neun Absätzen bestehende Art. 17, der in öffentlichkeitswirksamer Weise ein „Recht auf Vergessen" garantiert. Die Neuerung im Vergleich zu „gewöhnlichen" Löschungsrechten, wie beispielsweise be-

---

[324] KOM (2012) 11 endgültig, S. 7.

[325] Vgl. KOM (2012) 11 endgültig, S. 7 f.

[326] Siehe oben Teil 1, IV.B.8.

[327] Siehe oben III.A.2.a).

reits in Art. 12 b) der Richtlinie 95/46/EG enthalten, besteht in der Kombination aus Einwilligungswiderruf, Art. 17 Abs. 1 b), und an Folgeverarbeiter gerichtete Informationspflichten. Der Datenverarbeiter wird gem. Art. 17 Abs. 2 Satz 1 verpflichtet, „alle vertretbaren Schritte, auch technischer Art" zur Information Dritter über das Verlangen des Betroffenen zur Löschung „aller Querverweise" und „Kopien oder Replikationen" der Daten zu ergreifen. Wenn die ursprüngliche verarbeitende Stelle einem Dritten die Verarbeitung gestattet, bleibt die Verantwortung bei der ersten Stelle, Art. 17 Abs. 2 Satz 2. Einschränkungen u.a. zur Ausübung des Rechts auf freie Meinungsäußerung und aus Gründen des öffentlichen Interesses enthält Abs. 3.

Die Vorschrift spiegelt die seit langem bestehende Forderung nach einem „digitalen Radiergummi", die jedoch bisher aufgrund der technischen Eigenschaften des Internets als nicht umsetzbar galt. Die Idee eines „right to be forgotten" wurde, soweit ersichtlich, erstmals in einem Arbeitspapier von *Viktor Mayer-Schönberger* im Jahr 2007 formuliert. Dieses mündete dann in seine zwei Jahre darauf erschienene Monografie „Delete – The Virtue of Forgetting in the Digital Age".[328] Zu den Bemühungen, eine Lösung für die technischen Schwierigkeiten zu finden, gehörte sogar ein mit 5000 € dotierter Wettbewerb des BMI, der jedoch ebenfalls keine durchbrechenden Lösungsvorschläge erbrachte.[329] Die Problematik ergibt sich aus der Digitalisierung von Objekten, dem sprunghaften Anstieg der Speicherkapazitäten und der dezentralen Struktur des Internets. Die dadurch erreichte Ausfallsicherheit und Verfügbarkeit der Daten macht zugleich deren Löschung in vielen Fällen praktisch unmöglich, da kein umfassender Zugriff auf die zahlreichen Server besteht, auf denen die Daten „gespiegelt" werden. Alternative Konzepte, die auf ein „Verfallsdatum" durch Verschlüsselung setzen, sind technisch schwer zu implementieren und leicht (beispielsweise durch Screenshots) zu umgehen.[330]

Hinter dem Regelungskonzept des „Rechts auf Vergessen" steht das Risiko der Informationspermanenz, wie es bereits oben angesprochen wurde.[331] Die dauerhafte Verfügbarkeit der Informationen ermöglicht deren missbräuchliche Nutzung in der Zukunft und – im Fall von Persönlichkeitsrechtsverletzungen – eine Perpetuierung des Schadens. Besonders naheliegend ist dieses Risiko in Situationen, in denen ein Betroffener noch im Kindesalter, als er die damit verbundenen Gefahren nicht in vollem Umfang absehen konnte, in eine Verarbeitung eingewilligt hat, die später im Internet zugänglich ist. Das Risiko wird von Erwägungsgrund 53 explizit angesprochen. Im Rahmen eines Exkurses wurde oben die Schaffung eines informationsrechtlichen Rechtsinstituts der Informationsverjährung angeregt. Dieses

---

328 Arbeitspapier zit. nach *Nolte*, ZRP 2011, 236; *Mayer-Schönberger*, Delete.

329 http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2012/05/acatech.html [Stand: 28.3.2014].

330 *Nolte*, ZRP 2011, 236 (237).

331 Siehe oben Teil 1, II.A.2.d); IV.B.3.

könnte, indem es in Anlehnung an die zivilrechtliche Verjährung lediglich eine Verwendungshemmung auf Entscheidungsebene vorsieht, das Problem der technischen Umsetzbarkeit vermeiden.[332]

### *b) Datenportabilität*

Art. 18 GV-Vorschlag sieht ein Recht auf Datenportabilität vor. Portabilität bedeutet in diesem Zusammenhang die Möglichkeit zur Überführung der Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System, ohne Verhinderung durch die verarbeitenden Stellen. Die Daten müssen daher in einem strukturierten, gängigen elektronischen Format zur Verfügung gestellt werden. Erwägungsgrund Nr. 55 nennt die Ziele der Portabilität. Diese sei nötig, „damit die betroffenen Personen eine bessere Kontrolle über ihre eigenen Daten haben und ihr Auskunftsrecht besser ausüben können". Explizit angesprochen wird das Beispiel soziale Netzwerke. Hinter diesem Konzept steht der Gedanke, dass insbesondere bei sozialen Netzwerken einzelne große Anbieter eine Monopolstellung für bestimmte Dienste innehaben, wodurch die Wahlfreiheit der Nutzer eingeschränkt wird. Die Regelung ist damit ihrer Natur nach jedoch nicht datenschutzrechtlich, sondern dem Wettbewerbsrecht zuzuordnen. Auch lässt sie sich nicht auf die Schutzkonzeption der Selbstbestimmung und Transparenz zurückführen, wie dies Erwägungsgrund 55 nahelegt: Für diese Ziele ist das Recht auf Einsicht und Löschung ausreichend, eine Mitnahme zu anderen Anbietern ist hierzu gerade nicht notwendig. Zwar mag die anschließende Verwendung der Daten im Rahmen eines ggf. datenschutzfreundlicheren Anbieters dazu führen, dass dem Betroffenen hieraus ein Nutzen entsteht, indem er das über ihn gefertigte „Profil" anderweitig nutzen kann. Damit würde jedoch gerade die wirtschaftliche Eigenleistung des Erstanbieters entwertet; es bestünde dann mangels wirtschaftlicher Verwertbarkeit der Daten kaum mehr ein Anreiz zu innovativen Entwicklungen wie beispielsweise den angesprochenen sozialen Netzwerken. Das für die mangelnde Datenschutz-Compliance ursächliche Risiko liegt in der Monopolstellung des Verarbeiters und ist deshalb nicht spezifisch datenschutzrechtlich.[333]

### *c) Schutz vor Profiling*

Art. 20 GV-Vorschlag enthält das Recht, nicht einer auf rein automatisierter Datenverarbeitung basierenden Maßnahme unterworfen zu werden. Die Vorschrift beruht damit auf Art. 15 der Richtlinie 95/46/EG, die Schutz vor bestimmten, allein auf automatisierter Datenverarbeitung gestützten Entscheidungen bietet. Den Rege-

---

[332] Siehe oben Teil 1, IV.B.3.a).

[333] Hieraus ergeben sich insbesondere kompetenzrechtliche Probleme, da die Regelung aufgrund ihrer Zuordnung zum Wettbewerbsrecht nicht von Art. 16 AEUV umfasst ist.

lungsinhalt fasst Erwägungsgrund 58 zusammen: „Eine natürliche Person braucht sich keiner Maßnahme unterwerfen lassen, die auf Profiling im Wege der automatischen Datenverarbeitung basiert." Ausnahmen sind jedoch die gesetzliche Zulassung oder die Einwilligung des Betroffenen. In Bezug auf die Risikokonzeptionen gilt das zu Art. 15 RL 95/46/EG Ausgeführte.[334] Zugrunde liegt das Risiko der Verantwortungsnegation und der Behandlung von Menschen als Objekte. Bemerkenswert ist jedoch die Ausweitung der Beispiele. Während Art. 15 RL 95/46/EG nur die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit und das Verhalten nennt, bezieht sich Art. 20 GV-Vorschlag zusätzlich auf den Aufenthaltsort, den Gesundheitszustand und persönliche Vorlieben. Darüber hinaus wird in der Überschrift der Begriff „profiling" als Oberbegriff gewählt. Damit bezieht sich der GV-Vorschlag auf die oben besprochenen Empfehlungen des Europarats zum Profiling.[335] Wiederum gilt das dort Ausgeführte in Bezug auf Risikokonzeptionen und Schutzgüter.[336] Eine Präzisierung findet sich in Erwägungsgrund 21. Dort wird erwogen, dass die Frage, „ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von Personen gilt", daran festgemacht werden sollte, ob „Internetaktivitäten mithilfe von Datenverarbeitungstechniken nachvollzogen werden, durch die einer Person ein Profil zugeordnet wird". Ein derartiges Profil liege vor, wenn es Grundlage für sie betreffende Entscheidungen bildet oder es ermöglicht, „persönliche Vorlieben, Verhaltensweisen oder Gepflogenheiten" zu analysieren oder vorauszusagen. Wie schon bei den Empfehlungen des Europarats zum Profiling tritt auch hier wieder das Risiko von Menschenwürdeverletzungen hervor, soweit derartige Profile intransparent und „rein funktional" ohne Einflussmöglichkeiten des Betroffenen konstruiert sind. Auch kann die unzureichende Konstruktion das Risiko der fehlerhaften Selektivität hervorrufen.

#### *d) Risikoprognosen im Rahmen von Meldepflichten*

Der GV-Vorschlag sieht in bestimmten Fällen Meldepflichten bei Datenschutzverstößen vor. Das schon ansatzweise in der Richtlinie 2002/58/EG verwirklichte Konzept der „privacy breach notifications"[337] wurde ausgeweitet und um differenzierte Regelungen zu Risikoprognosen ergänzt. Hieraus können Rückschlüsse auf Risikokonzeptionen gezogen werden. Unterschieden wird zunächst zwischen Meldepflichten gegenüber der Aufsichtsbehörde (Art. 31 GV-Vorschlag) und gegenüber den Betroffenen (Art. 32 GV-Vorschlag). Art.79 Abs. 6 h) sanktioniert Verstöße gegen Meldepflichten mit einer Geldbuße von bis zu 2 % des weltweiten Jahresumsatzes. Angeknüpft wird an die Verletzung des Schutzes personenbezoge-

---

334 Siehe oben Teil 1, II.C.

335 CM/Rec (2010) 13 vom 23.11.2010.

336 Siehe oben III.A.2.c).

337 Art. 4 Abs. 3 RL 2002/58/EG.

ner Daten, die in Art. 4 Abs. 9 gleichlautend mit Art. 2 h) RL 2002/58/EG[338] definiert wird. Die nähere Beschreibung der Verletzung erfolgt in den Erwägungsgründen Nr. 67 und 68. Erwägungsgrund 67 weist auf die erheblichen wirtschaftlichen Schäden und sozialen Nachteile von Verletzungen hin und nennt als Beispiele neben „Identitätsbetrug" und „Identitätsdiebstahl" auch physische Schädigungen, erhebliche Demütigungen und Rufschädigungen. Eine Unterrichtung soll gem. Erwägungsgrund 68 erfolgen, „bevor persönliche oder wirtschaftliche Interessen Schaden nehmen können". Dabei sind „Art und Schwere der Verletzung" sowie deren „negative Folgen" zu berücksichtigen. Die Meldepflicht besteht gem. Art. 31 Abs. 1 gegenüber der Aufsichtsbehörde schon bei Vorliegen der Verletzung, wobei die Kommission gem. Abs. 5 dazu ermächtigt wird, delegierte Rechtsakte nach Maßgabe von Art. 86 zu erlassen, um Kriterien und Anforderungen an die Feststellung der Verletzung näher zu bestimmen. Die Meldepflicht gegenüber den jeweiligen Personen erfordert als weitere Voraussetzung gem. Art. 32 Abs. 1 die Vornahme einer Risikoprognose. Die Meldung hat demnach zu erfolgen, „wenn die Wahrscheinlichkeit besteht, dass der Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Person durch eine festgestellte Verletzung des Schutzes personenbezogener Daten beeinträchtigt wird".

Auch für diese Konstellation soll gem. Art. 31 Abs. 5 die nähere Ausgestaltung durch delegierte Rechtsakte der Kommission vorgenommen werden. Hierbei soll die Kommission „Kriterien und Anforderungen" in Bezug auf die Verletzung sowie die „konkreten Umstände" der Meldepflicht festgelegen.

Die Literatur verweist für die Konkretisierung dieser allgemein gehaltenen Regelungen auf ähnliche Vorschriften im BDSG.[339] Sie finden sich dort in § 42a BDSG, der sich auf Risikodatenkategorien bezieht. Neben den in § 3 Abs. 9 BDSG aufgeführten besonderen Arten von Daten (u.a. Angaben mit Bezug zu Herkunft, politischer Einstellung, Sexualleben) werden hierunter Daten gefasst, die einem Berufsgeheimnis unterliegen, sich auf strafbare Handlungen oder Ordnungswidrigkeiten bzw. einen entsprechenden Verdacht beziehen, sowie personenbezogene Daten zu Bank- oder Kreditkartenkonten. Weitere Tatbestandsmerkmale sind die unrechtmäßige Kenntniserlangung eines Dritten sowie eine Gefahrenprognose. Ausreichend für das Merkmal „Kenntniserlangung" ist eine hohe Wahrscheinlichkeit der Kenntnisnahme Dritter.[340] Für die Gefahrenprognose soll kein zu enger Maßstab angelegt werden. Erhebliche materielle Schäden oder soziale Nachteile werden gerade nicht gefordert. Reine Vermögensschäden sollen in die Prognose einbezogen werden. Außer Betracht bleiben sollen dagegen rechtliche Widerspruchs- oder Rückbuchungsmöglichkeiten, die beispielsweise im Lastschriftverfahren häufig

---

338 Siehe oben III.C.2.d).

339 *Kaufmann*, ZD 2012, 358 (360).

340 Simitis-*Dix*, § 42a Rn. 8.

dazu führen, dass im Ergebnis keine Beeinträchtigung vorliegt.[341] Bemerkenswert ist zudem die Regelung des § 42a Satz 5 BDSG: Soweit die Benachrichtigung aufgrund der Vielzahl der Fälle unverhältnismäßig ist, tritt an deren Stelle die Information der Öffentlichkeit durch mindestens halbseitige Anzeigen in zwei bundesweit erscheinenden Tageszeitungen.

Diese Gegenüberstellung zeigt das größere Maß an Bestimmtheit der deutschen Regelungen. Entsprechend werden auch die Ausgestaltung der Art. 31 und 32 GV-Vorschlag in der Literatur kritisiert: Der Meldepflicht mangele es an der Benennung von Risikodatenkategorien entsprechend § 42a BDSG.[342]

Die Vorschriften zu den Meldepflichten basieren damit zunächst allein auf dem Risiko der individuellen Verletzlichkeit, wie die Anknüpfung an persönliche und wirtschaftliche Interessen in Erwägungsgrund 68 unterstreicht. Die Notwendigkeit einer genaueren Spezifizierung zeigt die kritische Befassung in der Literatur, die hierfür den Vergleich mit § 42a BDSG vornimmt. Die dort näher umschriebenen Kategorien berücksichtigen das Risiko von Diskriminierung explizit durch Einbezug der in § 3 Abs. 9 BDSG aufgeführten besonderen Arten personenbezogener Daten.

### *e) Datenschutz-Folgenabschätzung*

Ein Novum stellt die ebenfalls im vierten Kapitel geregelte Datenschutz-Folgenabschätzung dar. Hiermit sollen die verantwortlichen Stellen dazu verpflichtet werden, vor einer „risikobehafteten Datenverarbeitung“[343] deren Konsequenzen für die Betroffenen zu eruieren. Damit werden die nachgelagerten Meldepflichten der Art. 31 f. um einen Vorfeldschutz ergänzt. Bei Vorliegen einer „risikobehafteten“ Datenverarbeitung im Sinne des Vorschlags muss die Aufsichtsbehörde informiert werden. In bestimmten Fällen kann sie dann die Verarbeitung verbieten. Von besonderem Interesse für die vorliegende Untersuchung ist die Frage, was unter einer „risikobehafteten Datenverarbeitung“ im Sinne des Vorschlags zu verstehen ist. Hierzu enthält Art. 33 Abs. 1 GV-Vorschlag eine Generalklausel und Abs. 2 einen daran anschließenden Beispielkatalog. Die Verarbeitungsvorgänge müssen gem. Art. 33 Abs. 1 aufgrund ihres „Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten“ der jeweiligen Person darstellen. Dies sei gem. Art. 33 Abs. 2 a) insbesondere bei systematischer und umfassender Auswertung persönlicher Aspekte einer natürlichen Person der Fall. Als Beispiel wird die Analyse der wirtschaftlichen Lage, des Aufenthaltsorts oder des Verhaltens genannt. Weiterhin liege ein Risiko im Sinne des Vorschlags vor, wenn Vo-

---

341 Ebd. Rn. 9.

342 Weiterhin werden die „Flut von Meldungen“ und der erhebliche bürokratische Aufwand für die Unternehmen kritisiert, *Kaufmann*, ZD 2012, 358 (360).

343 KOM (2012) 11 endgülig, S. 11.

raussagen auf Grundlage automatisierter Verarbeitung getroffen werden und diese als Basis für Maßnahmen mit Rechtswirkung gegenüber dem Betroffenen dienen oder sonstige erhebliche Auswirkungen haben. Nach Erwägungsgrund 69 sollen für Verletzungsmeldungen die „Umstände der Verletzung hinreichend berücksichtigt werden"; als Beispiel wird das Vorhandensein geeigneter technischer Sicherheitsvorkehrungen, die sich gegen Identitätsbetrug oder andere Formen des Datenmissbrauchs richten und diese „wirksam verringern", aufgeführt. Das mit Art. 33 Abs. 1 aufgegriffene Risiko im Sinne dieser Untersuchung liegt somit zum einen in der individuellen Verletzlichkeit, wie es sich im Merkmal „Aufenthaltsort" und in den Angaben in Erwägungsgrund 69 niederschlägt; daneben jedoch auch in dem mit umfassender Ausforschung verbundenen Überwachungsdruck, wie die Aufführung von „systematischer und umfassender" Auswertung in Abs. 2 a) verdeutlicht.

Art. 33 Abs. 2 b) dehnt die „Risikobehaftung" im Sinne des Vorschlags auf besondere Kategorien von Daten aus, wobei neben den üblichen Inhalten (Sexualleben, Gesundheitszustand, Rasse oder ethnische Herkunft) auch die Verarbeitung von Daten für Gesundheitsdienste, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder ansteckende Krankheiten genannt werden. In diesen Fällen soll die Risikobehaftung im Sinne des Vorschlags jedoch nur vorliegen, soweit die Daten „in großem Umfang im Hinblick auf Maßnahmen oder Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen". Zunächst wird damit wiederum das Risiko der individuellen Verletzlichkeit, vor allem aber das Risiko der Diskriminierung unterstrichen. Fraglich ist jedoch, was die letzten beiden Halbsätze ausdrücken sollen. Sofern damit allein die Anzahl der Betroffenen („großer Umfang") gemeint ist, erscheint dies aufgrund des individuellen Schutzziels inkonsequent. Überflüssig ist auch die zweite Ergänzung, welche die Risikobehaftung im Sinne des Vorschlags auf solche Daten beschränkt, die sich auf spezifische Einzelpersonen beziehen. Hier würde die Klarstellung, dass es sich um personenbezogene Daten handelt, genügen.

Art. 33 Abs. 2 c) nennt die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere in Fällen der Videoüberwachung. Hier wird das Risiko des Überwachungsdrucks aufgegriffen. Art. 33 Abs. 2 d) stellt die Risikobehaftung im Sinne des GV-Vorschlags bei der Datenverarbeitung „aus umfangreichen Dateien" sowie von Daten über Kinder, von genetischen und biometrischen Daten fest. Die letzten drei Varianten betreffen dabei wieder die individuelle Verletzlichkeit, wobei diese im Fall der Kindsdaten aus dem noch wenig ausgeprägten Problembewusstsein und damit der geringeren Selbstbestimmungsfähigkeit von Kindern folgt. Was mit einer Verarbeitung „aus umfangreichen Dateien" gemeint ist, bleibt dagegen völlig unklar. Das Merkmal kann sowohl quantitativ (Vielzahl von Betroffenen) als auch qualitativ (Aussagekraft und Umfang der Informationen) verstanden werden. Nur im letzteren Fall fügt es sich in das auf dem Schutz vor individueller Verletzlichkeit ausgerichtete Schutzkonzept ein.

Die letzte Variante, Art. 33 Abs. 2 e), verweist für die Risikobehaftung im Sinne des Vorschlags auf Art. 34 Abs. 2 b). Hierbei handelt es sich um Fälle, in denen die Aufsichtsbehörde gem. Art. 34 Abs. 4 bestimmte Verarbeitungsvorgänge auf einer Liste als risikobehaftet kennzeichnet. Inhaltliche Maßgaben resultieren lediglich aus dem Verweis auf „konkrete Risiken" des Art. 34 Abs. 2 b). Diese sollen offenbar von den „hohe[n] konkreten Risiken" unterschieden werden, die gem. Art. 34 Abs. 2 a) die Pflicht zur vorherigen Zurateziehung begründen. Erwägungsgrund Nr. 74 befasst sich dagegen mit „großen konkreten Risiken". Hierzu wird das Risiko (im Sinne des GV-Vorschlags), „infolge des Rückgriffs auf neue Technologien" vom Datenschutzrecht keinen Gebrauch machen zu können, gefasst. Auch unter Berücksichtigung des Erwägungsgrunds bleiben die Risikobegriffe des Entwurfs unklar und allgemein gehalten. Sie unterstreichen damit das Erfordernis der vorliegenden Untersuchung, da sie den verarbeitenden Stellen, abgesehen von den „Listenfällen", keinen praktikablen Abgrenzungsmaßstab zur Hand geben. Die Literatur bemüht an dieser Stelle wiederum den Vergleich mit der deutschen Rechtslage, der zur Vervollständigung im Folgenden dargestellt wird:

Das BDSG enthält in § 4 d Abs. 5 das Gebot der Vorabkontrolle. Eine solche ist vorzunehmen, wenn Daten gem. § 3 Abs. 9 BDSG verarbeitet werden oder wenn die Verarbeitung zu einer Bewertung der Persönlichkeit des Betroffenen einschließlich dessen Fähigkeiten, seiner Leistung oder des Verhaltens bestimmt ist. Nach überwiegender Ansicht soll die Vorabkontrollpflicht auch für Videoüberwachungen in öffentlich zugänglichen Bereichen i.S.v. § 6 b BDSG gelten. Der Unterschied zur Regelung des Art. 33 GV-Vorschlag liegt jedoch in der Zuständigkeit zur Vorabkontrolle. Gem. § 4 d Abs. 6 BDSG obliegt diese dem betrieblichen Datenschutzbeauftragen. Nur in Ausnahmefällen hat dieser sich an die Aufsichtsbehörde zu wenden.[344] Nach europäischem Vorschlag löst die Folgenabschätzung hingegen im Rahmen des Art. 34 Abs. 2 GV-Vorschlag eine Genehmigungspflicht der Aufsichtsbehörde aus, sofern sich aus der Folgenabschätzung „hohe konkrete Risiken" ergeben oder wenn es die Behörde für erforderlich hält. Diese Regelung wird wiederum in der Literatur aufgrund der damit verbundenen Kosten und Bürokratie kritisiert: *Kaufmann* spricht insoweit von „unendlich viele[n] Verfahren", die aufgrund der weiten Fassung der Risikobehaftung der jeweiligen Aufsichtsbehörde vorzulegen wären.[345] Rückschlüsse auf die Auslegung der „konkreten Risiken" bzw. der „hohen konkreten Risiken" in Art. 34 Abs. 2 GV-Vorschlag lassen sich aus dem Vergleich jedoch nicht ohne Weiteres gewinnen. Mangels klarer Fassung der Risikobehaftung könnte allenfalls dann ein Rückschluss auf das Risiko der Individualverletzlichkeit erfolgen, wenn der (normsystematisch unzulässige) Vergleich mit den deutschen Bestimmungen des BDSG angestrengt wird. In diesem Fall müsste jedoch auch das Risiko des Überwachungsdrucks erfasst sein, da die

---

344 *Kaufmann*, ZD 2012, 358 (361).

345 Ebd., 361.

Vorabkontrolle im deutschen Recht nach herrschender Auffassung auch für Videoüberwachung in öffentlich zugänglichen Bereichen gilt.[346] Überzeugender ist jedoch die systematische Auslegung. Demnach muss es sich bei den Risiken des Entwurfs um solche handeln, die nicht schon in den Varianten a)–c) erfasst sind. Da sich diese Varianten bereits auf die Risiken der individuellen Verletzlichkeit sowie des Überwachungsdrucks beziehen, liegt es nahe, der Variante d) eine Auffangfunktion zuzusprechen und darunter die übrigen Risiken des Entwurfs, wie sie unten entwickelt werden, zu erfassen.[347]

### 3. Zwischenergebnis

Der Vorschlag zur Datenschutzgrundverordnung baut im Wesentlichen auf bekannten Konzepten der Datenschutzrichtlinie 95/46/EG und der E-Kom-Richtlinie 2002/58/EG auf, setzt daneben jedoch eigene Akzente und enthält Neuerungen, die Rückschlüsse auf Risikokonzeptionen und Schutzgüter erlauben. Was die Schutzgüter angeht, teilt der Entwurf die „dualistische" Konzeption der Richtlinie 95/46/EG. Obwohl er an prominenter Stelle wiederholt den Bezug zu Art. 8 EU-GRC und Art. 16 AEUV betont, wird weiterhin der Eindruck vermittelt, Daten würden nicht um der Grundrechte willen, sondern wegen der Schaffung einer „Vertrauensbasis" für die „IT-Wirtschaft" geschützt.[348] Beachtlich ist die Anknüpfung an die Schutzgutkonzeption des Verbrauchervertrauens, die insbesondere an das APEC Privacy Framework[349] erinnert. Die Vertrauenskonzeption ist ein geeignetes Schutzgut, um wirtschaftliche Risiken mit den übrigen Risiken zu vereinen.

Von den eigenständigen Gehalten des Vorschlags ist das in Art. 17 GV-Vorschlag geregelte und wohl von einer Monografie *von Mayer-Schönberger* inspirierte „Recht auf Vergessen" auf das Risiko der Informationspermanenz bezogen.[350] Dafür erscheint jedoch das bereits oben angestoßene Rechtsinstitut der Informationsverjährung geeigneter.[351] Die Regelungen zur Datenportabilität, Art. 18 GV-Vorschlag, greifen dagegen kein spezifisch datenschutzrechtliches Risiko auf und sind dem Wettbewerbsrecht zuzuordnen.[352] Eine Weiterentwicklung des Schutzes gegen allein auf automatisierter Datenverarbeitung gestützte Einzelentscheidungen stellt der Schutz vor Profiling des Art. 20 GV-Vorschlags dar. Die damit verbundenen Risikokonzeptionen gleichen denen des Art. 15 RL 95/46/EG und der Europaratsempfehlungen zum Profiling. Die Zusammenschau verdeutlicht

---

346 *Gola/Schomerus*, § 4d Rn. 13.

347 Siehe unten Teil 4.

348 Siehe oben F.2.

349 Siehe oben Teil 1, II.F.

350 Siehe oben III.F.2.a).

351 Siehe oben Teil 1, IV.B.3.

352 Siehe oben III.F.2.b).

die Herausbildung des Rechtsbegriffs „Profiling“. Zugrunde liegende Risiken sind Selektivitätsschäden, Verantwortungsnegation und Menschenwürdeverletzungen.[353]

Die in Art. 31 f. geregelten „privacy breach notifications“ setzen differenzierte Risikoprognosen voraus. Die Bestimmungen geben den verarbeitenden Stellen hierzu jedoch lediglich unzureichende Maßstäbe an die Hand. Aus diesem Grund wird teilweise auf vergleichbare deutsche Regelungen des § 42a BDSG zurückgegriffen. Die Risikokonzeptionen des Art. 31 f. GV-Vorschlag basieren auf dem Risiko der individuellen Verletzlichkeit. Das Risiko des Überwachungsdrucks lässt sich durch einen – allerdings normsystematisch unstimmigen – Vergleich mit den Regelungen des BDSG einbeziehen.[354] Am stärksten ausgeprägt ist die „Risikodogmatik“ bei den Vorschriften zur neu eingeführten Datenschutz-Folgenabschätzung. Hier kommt dem Begriff „Risiko“ schon explizit durch den Vorschlag zentrale Bedeutung zu. Dieser spricht von verschiedenen Arten von Risiken: „konkrete Risiken“, „hohe konkrete Risiken“ und „große konkrete Risiken“, ohne diese allerdings näher zu präzisieren. Inhaltlich lassen sich aus der Generalklausel keine über die Beurteilungskriterien „Wesen“, „Umfang“, „Zweck“ hinausgehenden Maßstäbe gewinnen. Der in Art. 33 Abs. 2 a)–c) enthaltene Katalog risikobehafteter Datenverarbeitungen (im Sinne des Vorschlags) ist auf das Risiko der individuellen Verletzlichkeit ausgerichtet. Das Risiko des Überwachungsdrucks wird lediglich angedeutet. Art. 33 Abs. 2 e) enthält eine Verweisung auf Fälle, in denen die Aufsichtsbehörde Risiken (im Sinne des Vorschlags) listenmäßig festhalten. Inhaltliche Maßstäbe für derartige Aufnahmen lassen sich kaum finden. Die systematische Auslegung legt nahe, dass die dort angesprochenen Fälle andere Risiken als die bereits in Art. 33 Abs. 2 a)–c) geregelte individuelle Verletzlichkeit erfassen sollen. Der Vorschrift kommt damit eine Auffangfunktion zu.[355]

## G. Reformvorschlag vom 25.1.2012: Richtlinie Polizei und Justiz

### 1. Überblick

Die Reformvorschläge vom 25.1.2012 beinhalten einen ebenfalls auf Art. 16 Abs. 2 AEUV gestützten Vorschlag einer Richtlinie für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (RL-Vorschlag). Der Vorschlag soll den Rahmenbeschluss 2008/977/JI ablösen und im Gegensatz zu diesem auch die innerstaatliche Datenverarbeitung regeln. Damit soll das Problem behoben werden, dass Strafverfolgungsbehörden aufgrund der gestiegenen Transnationalität

---

353 Siehe oben III.F.2.c).

354 Siehe oben III.F.2.d).

355 Siehe oben III.F.2.e).

häufig nicht mehr zwischen rein innerstaatlichen und grenzübergreifenden Verarbeitungen unterscheiden können; insbesondere kann ein grenzüberschreitender Informationsaustausch auch noch in späteren Phasen des Verfahrens notwendig werden. Auch der große Umsetzungsspielraum des Rahmenbeschlusses und die fehlenden Durchführungsbefugnisse der Kommission werden zur Begründung der Reform herangezogen.[356] Im Anhang zur Schlussakte der Regierungskonferenz zum Vertrag von Lissabon stellen die Mitgliedstaaten deshalb fest, dass auf Art. 16 AEUV gestützte Vorschriften aufgrund des „spezifischen Charakters" des polizeilich-strafprozessualen Bereichs erforderlich sein könnten.[357] Insbesondere die Einbeziehung der innerstaatlichen Datenverarbeitung führte jedoch auf nationaler Ebene zur Befürchtung eines „Abschleifens" deutscher Grundrechtsstandards auf ein niedrigeres EU-Niveau.[358] Nicht zuletzt deshalb sind die aktuellen Entwicklungen der EU-Datenschutzreform für die Frage der Risikoperzeption durch das geltende Recht von besonderer Bedeutung. Diese Einschätzung teilt auch der Europäische Datenschutzbeauftragte *Hustinx*. Zwar steht er der Erfassung innerstaatlicher Datenverarbeitung grundsätzlich positiv gegenüber, eine Verbesserung folge daraus jedoch nur bei einer spürbaren Anhebung des Schutzniveaus, was mit dem RL-Vorschlag nicht geschehe.[359] Auch wird die Anmahnung eines zu großen mitgliedstaatlichen Umsetzungsspielraums nach geltender Rechtslage (Rahmenbeschluss) dadurch relativiert, dass der RL-Entwurf im Gegensatz zu einer im November bekannt gewordenen Vorversion stark „entschärft" wurde. Die „Entschärfung" betraf insbesondere die materiellen Mindestanforderungen an mitgliedstaatliche Erlaubnistatbestände, was in der Literatur teils scharf kritisiert wird. So meinen *Bäcker/Hornung*, dass der Richtlinienentwurf die Verarbeitungsbefugnisse fast vollständig in das Belieben der Mitgliedstaaten stelle, was Folge einer massiven Intervention zur Verhinderung der Begrenzung informationeller Befugnisse der Kriminalbehörden sei.[360] Entsprechend äußerte sich auch der Europäische Datenschutzbeauftragte in seiner Stellungnahme vom 7.2.2012 zum Reformpaket: Er sei „ernsthaft enttäuscht" über das gewählte Rechtsinstrument, dieses biete im Vergleich zum GV-Vorschlag ein „unangemessenes Schutzniveau".

Dem Richtlinienentwurf ging eine Reihe von Anhörungen und Workshops voraus. Auch das Europäische Parlament unterstützte in einer Entschließung vom

---

356 KOM (2012) 10 endgültig, S. 2.

357 Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte der Regierungskonferenz, die den am 13.12.2007 unterzeichneten Vertrag von Lissabon annahm; vgl. auch Erwägungsgrund Nr. 10.

358 http://www.taz.de/Schaar-ueber-EU-Richtlinie-zum-Datenschutz/!88245/ [Stand: 28.3.2014]. In Bezug auf beide Reformvorschläge auch *Tinnefeld*, DuD 2012, 364.

359 ABl. C 192/7 vom 30.6.2012.

360 *Bäcker/Hornung*, ZD 2012, 147 (149 f.).

6.7.2011 das Konzept der Kommission zur Reform der Datenschutzregelung.[361] Weiterhin wurde eine Folgenabschätzung vorgenommen, in der mehrere Optionen überprüft wurden und insbesondere eine „minimalistische" Option für unzureichend befunden wurde.[362] Das Reformvorhaben befindet sich nun im Gesetzgebungsprozess und wird dabei u.a. im Innenausschuss des Europaparlaments beraten.[363]

Die Regelungen sind an denen des GV-Vorschlags angelehnt, an zahlreichen Stellen sind jedoch die Ausnahmetatbestände offen formuliert und ergeben ein im Vergleich mit dem GV-Vorschlag geringeres Schutzniveau. So etwa in Art. 11 Abs. 4 b) RL-Vorschlag, der in unbestimmter und offener Weise ein Absehen von der Benachrichtigung des Betroffenen ermöglicht. Die Nichtbenachrichtigung sei möglich, um zu gewährleisten, dass die „Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten nicht beeinträchtigt" wird.[364] Ähnlich auch Art. 13 Abs. 1 RL-Vorschlag, der einen Katalog von Ausnahmen zu den Auskunftsrechten der Betroffenen u.a. für die Fälle der „Behinderung" behördlicher oder gerichtlicher Ermittlungen, Untersuchungen und Verfahren enthält und es in Abs. 2 auch ermöglicht, Datenverarbeitungskategorien festzulegen, in denen die Ausnahmeregelungen des ersten Absatzes zur Anwendung kommen. Auch wird der Zweckbindungsgrundsatz, wie auch vom Europäischen Datenschutzbeauftragten gerügt,[365] sehr unklar formuliert: Art. 4 enthält keinerlei materielle Begrenzungen der Zweckfestlegung. Erwägungsgrund Nr. 19 verweist auf die Notwendigkeit der kontextübergreifenden Verarbeitung zur Erstellung von Lagebildern und Trends. Es fehlen zentrale Regelungen, wie beispielsweise eine Bestimmung darüber, dass die Übermittlung personenbezogener Daten an andere Behörden oder private Stellen nur unter bestimmten Voraussetzungen zulässig ist, oder eine Darlegung der Gründe des öffentlichen Interesses, bei deren Vorliegen ein Abrücken vom Grundsatz der Zweckbindung zulässig ist.[366]

Im Übrigen stützt sich der RL-Vorschlag jedoch (in abgeschwächter Weise) auf die hergebrachten datenschutzrechtlichen Regelungskonzepte der Verarbeitungsgrundsätze, der Rechtmäßigkeit der Verarbeitung, dem Schutz besonderer Kategorien von Daten, Profilingschutz (Kapitel II), Betroffenenrechte (Kapitel III), Regelungen zu Auftragsdatenverarbeitung und Datensicherheit sowie zum Daten-

---

361 KOM (2012) 10 endgültig, S. 3 f.

362 KOM (2012) 10 endgültig, S. 4.

363 Vgl. zum aktuellen Stand die Internetseite des Berichterstatters des Innenausschusses http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html sowie der Kommission http://europa.eu/rapid/press-release_MEMO-14-60_en.htm?locale=en [Stand: 28.3.2014].

364 Kritisiert wird hieran insbesondere, dass die Einschränkung auch aus Gründen unabhängig von der Anlasstat möglich ist, vgl. *Bäcker/Hornung*, ZD 2012, 147 (150).

365 ABl. C 192/8 vom 30.6.2012.

366 Vgl. ABl. C 192/13 vom 30.6.2012.

schutzbeauftragten (Kapitel IV). Weiterhin sind Vorschriften zu Aufsichtsbehörden (Kapitel VI), zur Amtshilfe (Kapitel VII) und zur Durchsetzung (Kapitel VIII) enthalten. Ein Schwerpunkt der Regelungen betrifft die Übermittlung in Drittländer oder an internationale Organisationen (Kapitel V). Problematisch ist jedoch, dass spezifische Datenschutzinstrumente der ehemals Dritten Säule, wie beispielsweise der Prümer Beschluss und die Vorschriften über Europol und Eurojust unangetastet bleiben, was eine „Hauptschwäche" des Vorschlags darstellt.[367]

### 2. Risikokonzeptionen und Schutzgüter

Die Ziele des RL-Entwurfs werden – ähnlich wie bei den anderen EU-Datenschutzinstrumenten – in „dualistischer", sich teilweise widersprechender Weise formuliert. Art. 1 a) bezieht sich auf den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Datenschutzgrundrecht. Art. 1 b) nennt dagegen das Ziel, den Austausch personenbezogener Daten zwischen Behörden in der Union nicht aus Gründen des Datenschutzes einzuschränken oder zu verbieten. Der Grundrechtsbezug wird in Erwägungsgrund Nr. 1 unterstrichen, der Art. 8 Abs. 1 EU-GRC und Art. 16 Abs. 1 AEUV anspricht. Die Erwägungsgründe Nr. 3 und 4 enthalten den Rückschluss von gestiegenem Datenverarbeitungsumfang durch Behörden auf die Notwendigkeit stärker abgestimmter unionaler Datenschutzbestimmungen. Erwägungsgrund Nr. 7 beinhaltet das Ziel, einen unionsweit hohen Schutz zu gewährleisten. Erwägungsgrund Nr. 80 fasst den Grundrechtsbezug nochmals zusammen, nennt jedoch neben dem Datenschutzgrundrecht auch das Recht auf Privat- und Familienleben sowie die Garantie des fairen Verfahrens.

#### *a) Personale Risikofaktoren bei Betroffenenkategorien*

Eine Besonderheit stellt die Differenzierung zwischen verschiedenen Kategorien von Betroffenen dar. Dabei handelt es sich um ein weder in der Richtlinie 95/46/EG noch im Rahmenbeschluss 2008/977/JI enthaltenes Konzept, das die Kommission jedoch ursprünglich für den Rahmenbeschluss vorgeschlagen hatte. Vergleichbare Vorschriften gelten bereits für die Datenverarbeitung von Europol (Art. 14 Europol-Beschluss 2009/371/JI) und Eurojust (Art. 15 Eurojust-Beschluss 2009/426/JI).[368]

Erwägungsgrund Nr. 23 benennt dieses Ziel: Es soll – „soweit wie möglich" – zwischen Verdächtigen, verurteilten Straftätern, Opfern und Dritten, beispielsweise Zeugen oder Sachverständigen, sowie Informanten unterschieden werden. Art. 5 RL-Vorschlag führt diese Differenzierung ein. Überraschenderweise knüpfen die

---

[367] So der Europäische Datenschutzbeauftragte in seiner Stellungnahme, ABl. C 192/7 vom 30.6.2012.

[368] KOM (2012) 10 endgültig, S. 8.

Vorschläge jedoch keinerlei Rechtsfolgen an die Unterscheidung. Allein aus der Trennung lassen sich allerdings Rückschlüsse auf unterschiedliche Risikokonzepte ziehen. So könnte die Unterscheidung mit dem Risiko der Diskriminierung (und damit der Gefährdung der Resozialisierung von Straftätern) oder auch mit dem Risiko der individuellen Verletzung – etwa im Zuge von „Lynch-Mobs" und Anwohnerinitiativen – begründet werden. Weiterhin kann die Offenbarung der Opferrolle Schamgefühle auslösen. Im Fall von Polizeiinformanten liegt das Risiko der persönlichen Verletzlichkeit bei Offenlegung ihrer Rolle auf der Hand. Die besondere Schutzwürdigkeit der Verdächtigen ergibt sich aus der Unschuldsvermutung, die gebietet, dass die Rechtsfolgen der Strafe nicht durch Publizität vorweggenommen werden. Zwar deutet die Übernahme der Trennung auf diese Risikokonzepte hin, jedoch fehlt es an materiellen Regelungen, die der besonderen Schutzbedürftigkeit beispielsweise durch Weitergabeschwellen oder Verarbeitungsverbote Rechnung tragen.

### *b) Faktentrennung*

Erwägungsgrund Nr. 21 beinhaltet die Überlegung, dass Aussagen, die personenbezogene Daten enthalten, in Gerichtsverfahren häufig auf subjektiver Wahrnehmung basieren und dass deshalb der Grundsatz der sachlichen Richtigkeit in diesen Fällen zu modifizieren sei. Dieser dürfe sich nicht auf die Richtigkeit einer Aussage, sondern allein auf deren Existenz beziehen. Erwägungsgrund Nr. 24 unterstreicht dies, indem er die Trennung zwischen Fakten und persönlichen Einschätzungen für geboten hält. Das Konzept lehnt sich an die Empfehlung des Europarats zum Profiling, Nr. R (87)15 an, zu den Risiken gilt das dort Angeführte.[369] So lässt sich aus der Trennung auf das Risiko der Entkontextualisierung in Form von Kontextdefiziten schließen. Dies kann insbesondere in grenzüberschreitenden Sachverhalten von großer Bedeutung sein, wenn beispielsweise Auslieferungsentscheidungen oder freiheitsentziehende Maßnahmen auf übermittelte Informationen eines anderen Landes gestützt werden.

### *c) Risikoprognosen im Rahmen der Zurateziehung*

Der RL-Vorschlag enthält keine Regelungen zu Datenschutzfolgeabschätzungen. Art. 26 bestimmt jedoch, dass in gewissen Fällen die Aufsichtsbehörde zu Rate zu ziehen ist. Die Zurateziehung soll neben der Verarbeitung sensibler Daten gem. Art. 8 auch in solchen Fällen erfolgen, die „wegen der Art der Verarbeitung, insbesondere der Verarbeitung mit neuen Technologien, Mechanismen oder Verfahren, andernfalls spezifische Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere für den Schutz ihrer personenbezogener Daten"

---

[369] Siehe oben Teil 1, II.C.

schaffen. Eine Präzisierung der Risikofälle erfolgt in dem RL-Vorschlag jedoch im Gegensatz zur „Risikodogmatik" der GV-Vorschläge[370] nicht.

#### *d) Kontrollsystematik im Bereich Datensicherheit*

Von Relevanz sind sodann die Regelungen zur Datensicherheit im zweiten Abschnitt des vierten Kapitels der Vorschläge. Neben der Anknüpfung des Schutzniveaus an die „von der Verarbeitung ausgehenden Risiken", Art. 27 Abs. 2, enthält Abs. 3 einen Katalog von zehn Kontrollkonzepten, die der für die Verarbeitung Verantwortliche nach einer Risikobewertung anzustreben hat. Darunter fallen die Zugangskontrolle und die Datenträgerkontrolle, die sich gegen den Zutritt bzw. die Kenntnisnahme oder Veränderung von Daten durch Unbefugte richten. Die Variante c) erstreckt dies neben den Datenträgern auch auf Speicher (Speicherkontrolle), wobei der Unterschied zwischen Datenträger und Speicher nicht ersichtlich ist. Variante d) richtet sich gegen die unbefugte Nutzung mit „Einrichtungen zur Datenübertragung" (Benutzerkontrolle). Die Varianten e) und f) betreffen ebenfalls die Verhinderung unbefugten Zugriffs (Zugriffs- und Übermittlungskontrolle). Nach Variante g) ist sicherzustellen, dass nachträglich festgestellt werden kann, welche Daten wann und von wem eingegeben worden sind. Die Varianten h)–i) schützen die informationstechnischen Schutzgüter der Verfügbarkeit, Zuverlässigkeit und Integrität und sind damit nicht über das bereits oben hierzu Festgestellte relevant.[371] Die Varianten a)–h) verdeutlichen hingegen unterschiedliche Aspekte der unbefugten Nutzung von Daten und sind damit exemplarisch für das Risiko der individuellen Verletzlichkeit bei missbräuchlicher Verwendung von Daten.

#### *e) Exkurs: enforced accountability in den Vereinigten Staaten*

Auffällig ist, dass die besonders naheliegenden Missbrauchsmöglichkeiten aus dem Umfeld der Datenverarbeiter nicht explizit angesprochen werden. So hätte es sich beispielsweise angeboten, das in den USA zum Teil bereits praktizierte Konzept der *enforced accountability* zu übernehmen. Dieses Konzept basiert auf der Möglichkeit, das Überwachungs- und Kontrollpotenzial der neuen Technologien zum Schutz der Betroffenen einzusetzen, indem es auf die Verarbeiter angewendet wird. Es lässt sich unter dem Motto „watch the watchers" zusammenfassen. Zentral sind dabei die Zugriffsdokumentation und die Möglichkeit, bei Abweichungen von vorher festgelegten legitimen Nutzungen Meldungen an Aufsichtsstellen oder die jeweils betroffene Person zu senden bzw. den Verarbeitern besondere Erklärungspflichten aufzuerlegen. Das Konzept wurde erstmals im US-Präsidentschaftswahlkampf 2008 bekannt, als unberechtigte Zugriffe auf Meldedaten des Kandidaten *Obama* und eines Kritikers der Demokraten bereits kurz nach den Zugriffen

---

370 Siehe oben III.G.2.d), e).

371 Vgl. bereits oben III.C.2.b).

aufgeklärt und den unbefugt nutzenden Beamten zugeordnet werden konnten.[372] Der Katalog des Art. 27 und insbesondere die starke Begrenzung von Benachrichtigungspflichten durch den Verweis des Art. 29 Abs. 4 auf Art. 11 Abs. 4 RL-Vorschlag bleibt dagegen weit hinter einem derartigen Konzept zurück.

### 3. Zwischenergebnis

Die Regelungen des RL-Vorschlags sind im Vergleich zum GV-Vorschlag und zu einer im November 2012 bekannt gewordenen Vorversion stark zugunsten der Verarbeitungsinteressen eingeschränkt und werden hierfür in der Literatur kritisiert.[373] Ziel des RL-Vorschlags ist die Sicherstellung eines einheitlichen (grundrechtlichen) Schutzniveaus zur Verhinderung von Verarbeitungsbeschränkungen im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.[374] Die Regelungskonzeptionen überschneiden sich mit denen des GV-Vorschlags. Rückschlüsse auf Risikokonzeptionen sind deshalb nur begrenzt möglich. Eigenständiger Regelungsgehalt ist die Unterscheidung verschiedener Kategorien von Betroffenen. Hierin deuten sich die Risiken der Diskriminierung, Stigmatisierung und individuellen Verletzlichkeit, aber auch der Gefährdung der Resozialisierung, der Gefährdung der Unschuldsvermutung und der Auslösung von Schamgefühlen an. Schamgefühl und Resozialisierungshindernisse können dabei dem Spektrum der Publizitätsschäden zugeordnet werden. Die Aussagekraft des RL-Vorschlags ist hier jedoch beschränkt, da er zwar die Differenzierung einführt, jedoch keinerlei materielle Regelungen daran anknüpft.[375] Das Risiko des Kontextdefizits verdeutlichen die Regelungen zur Trennung von Fakten und persönlichen Einschätzungen, die an die Vorschläge des Europarats Nr. R (87)15 angelehnt sind.[376] Aus den Vorschriften zur Zurateziehung von Aufsichtsbehörden lassen sich aufgrund der Allgemeinheit der Regelungen keine Aussagen zu betroffenen Risiken treffen.[377] Im Abschnitt zur Datensicherheit findet sich ein Katalog verschiedener Kontrollmaßnahmen, die auf das Risiko der individuellen Verletzlichkeit durch missbräuchliche Datennutzung bezogen sind. Daneben werden die informationstechnischen Schutzgüter der Verfügbarkeit, Zuverlässigkeit und Integrität geschützt.[378] Das in den USA teilweise umgesetzte Datenschutzkonzept der *enforced accountability* wird, obwohl dies naheliegt, von dem RL-Vorschlag nicht aufgegriffen.[379]

---

372 *Baker*, in: Szoka/Marcus (Hrsg.), The Next Digital Decade, S. 501 ff.

373 Siehe oben III.G.1.

374 Siehe oben III.G.2.

375 Siehe oben III.G.2.a).

376 Siehe oben III.G.2.b).

377 Siehe oben III.G.2.c).

378 Siehe oben III.G.2.d).

379 Siehe oben III.G.2.e).

## H. Zwischenergebnis

Die Analyse des Sekundärrechts hat damit die bereits zuvor identifizierten Risiken von Überwachungsdruck, Entkontextualisierung, Erhöhung der individuellen Verletzlichkeit, Fremdbestimmung, Publizitätsschäden durch Schamgefühl sowie Diskriminierungen bestätigt und konturiert.[380] Dabei sind insbesondere die Risiken durch soziale Netzwerke im Rahmen der Auseinandersetzung um die Bereichsausnahme für rein persönliche und familiäre Datenverarbeitungen klarer hervorgetreten. Sie bestehen – korrespondierend mit einem diesbezüglichen Bericht der Datenschutzgruppe – u.a. in Identitätsdiebstahl, finanziellen Einbußen, Nachteilen für Geschäfts- oder Erwerbsmöglichkeiten und Beeinträchtigungen der körperlichen Unversehrtheit und sind damit Teil der Risikokategorie „Erhöhung individueller Verletzlichkeit".[381] Genau diese Kategorie fasst auch die Richtlinie 2002/58/EG konkreter. Neben „Identitätsdiebstahl" verwendet sie den Begriff „Identitätsbetrug" und bezieht physische Schädigungen ein. Näher umschrieben werden zudem die unterschiedlichen Möglichkeiten des Einsatzes von Spähsoftware, die ebenfalls in die Kategorie der Verletzlichkeit – genauer in die Variante der missbräuchlichen Datennutzung durch Dritte – einzuordnen sind. Darüber hinaus wird mit dem – typischerweise intime Inhalte betreffenden – Einsatz von Spähsoftware auch auf das Risiko von Publizitätsschäden abgezielt. Die Richtlinie ergänzt dieses Risiko um die Varianten „erhebliche Demütigungen" und „Rufschäden".[382] Dem Risiko der Erhöhung individueller Verletzlichkeit durch missbräuchliche Datennutzung ordnet die Richtlinie das Schutzgut der Vertraulichkeit zu, welches zudem von einer Reihe in anderen Disziplinen anerkannten informationstechnischen Schutzgütern abgegrenzt wurde.[383] Im Rahmen der allgemeinen Regelungskonzeptionen werden ferner einzelne Fallgruppen zu den Risiken von Überwachungsdruck und Publizitätsschäden konkretisiert. Die Richtlinie betrifft daneben unerwünschte Direktwerbung, wobei noch zu klären ist, ob dies ein eigenständiges Risiko oder eine bloße Belästigung darstellt.[384] Weitgehende Übereinstimmung mit zuvor erörterten Risikokonzeptionen hat die Untersuchung des Rahmenbeschlusses 2008/977/JI ergeben, wobei der Einsatz Privater im Rahmen der Strafverfolgung aufgegriffen und das Risiko der Umgehung von Schutzstandards einbezogen wird.[385]

Die Reformvorschläge zur Schaffung einer Datenschutzgrundverordnung gehen zunächst von einer auf dem Verbrauchervertrauen basierenden Schutzgutkonzeption aus, die an die Entsprechungen im APEC Privacy Framework erinnert.[386] Da-

---

380 Siehe oben III.A.2.b) sowie insbesondere C. und F.

381 Siehe oben III.A.2.a).

382 Siehe oben III.C.2.a).

383 Siehe oben III.C.2.b).

384 Siehe oben III.A.2.c).

385 Siehe oben III.E.2.

386 Siehe oben III.F.2. zum APEC Privacy Framework, siehe oben Teil 1, II.F.

bei wird jedoch die Einräumung von Kontrolle als Mittel zur Schaffung von Vertrauen betont. Sodann erfolgt eine bemerkenswerte Anbindung der Schutzgutkonzeption an die Identitätskonzeption, die in der neueren EGMR-Rechtsprechung verwendet wird.[387] Insgesamt basiert der Verordnungsentwurf damit auf einer dualistischen Schutzgutkonzeption (wirtschaftspolitische Zielsetzung und Grundrechtsschutz), die in der auf dem Vertrauensbegriff aufbauenden Schutzgutkonzeption ihre beste Entsprechung findet. Unter den neuen Regelungskonzepten lässt sich das Recht auf Vergessen dem Risiko der Informationspermanenz zuordnen, wobei eine Verjährungskonzeption vorteilhafter wäre.[388] Dem Recht auf Datenportabilität liegt dagegen das Risiko von Verstößen gegen die Datenschutzcompliance aufgrund von Marktmacht zugrunde. Es handelt sich hierbei um eine Regelung, die auch im Wettbewerbsrecht verortet werden könnte.[389]

Das Schutzgut der Menschenwürde konnte gut anhand des Abwehrrechts gegen ausschließlich automatisierte Einzelentscheidungen, Art. 15 Abs. 1 RL 95/46/EG, nachvollzogen werden. Dabei hat sich die Verantwortungsnegation als eigenständiges Risiko herauskristallisiert.[390] Dieses Risiko greift auch der GV-Entwurf auf und weitet die Regelungen hierzu aus. Insbesondere erfolgt eine begriffliche Veränderung, wonach es sich bei den Tätigkeiten um Profiling handelt. Damit wird an die bestehenden Empfehlungen des Europarats angeknüpft und die diesbezüglichen Risikokonzeptionen einbezogen.[391]

Die Meldepflichten im Rahmen des GV-Vorschlags und die Zurateziehung bei dem RL-Vorschlag setzen ein Verständnis einschlägiger Risiken voraus. Der GV-Vorschlag bezieht sich dort auf die Kategorie der individuellen Verletzlichkeit und verbindet damit Elemente, die bereits zuvor insbesondere im Rahmen der Richtlinie 2002/58/EG beschrieben wurden. Die zur Auslösung der Meldepflicht erforderliche Risikoprognose wird jedoch nicht näher konkretisiert, dies soll durch delegierte Rechtsakte der Kommission erfolgen. In der Literatur wird aufgrund dieses unbefriedigenden Ergebnisses – systematisch zweifelhaft – auf entsprechende Regelungen des BDSG verwiesen. Am stärksten ausgeprägt ist die Risiko-Begrifflichkeit im Rahmen der neu eingeführten Datenschutzfolgenabschätzung. Die Regelungen sind dort offener für andere Risiken als dasjenige der individuellen Verletzlichkeit. Gleichwohl bleiben die Formulierungen abstrakt und setzen ein Vorverständnis für relevante Risiken voraus. Insgesamt belegt die vielfältige Verwendung der Risikobegrifflichkeiten die Notwendigkeit einer Klärung, wie sie in dieser Untersuchung vorgenommen wird.[392]

---

[387] Siehe oben III.F.2. zur Identitätskonzeption in der EGMR-Rechtsprechung, siehe oben Teil 1, IV.B.8.

[388] Siehe oben III.F.2.a).

[389] Siehe oben III.F.2.b).

[390] Siehe oben III.E.2.

[391] Siehe oben III.F.2.c); zu den Europaratsempfehlungen siehe oben Teil 1, II.C.

[392] Siehe oben III.F.2.d), e).

Der Vorschlag für eine Datenschutzrichtlinie für die Bereiche Polizei und Justiz hat trotz der vielfach kritisierten Allgemeinheit und der starken Abschwächung im Rahmen des Entwurfsprozesses auf verschiedene Risiken und Schutzgutkonzeptionen verwiesen. So deutet das Konzept der Differenzierung nach Betroffenenkategorien (Verdächtiger, Opfer, Informant) auf unterschiedliche Bedrohungslagen hin. Die Rückschlüsse bleiben jedoch von geringer Aussagekraft, da der Entwurf keine materiellen Folgen an die Differenzierung knüpft.[393] Ähnliche Rückschlüsse wie aus den Empfehlungen des Europarats zur polizeilichen Tätigkeit folgen sodann aus der Abstufung hinsichtlich der Glaubwürdigkeit von Informationen, der im strafprozessualen Zusammenhang insbesondere bei grenzüberschreitendem Austausch aufgrund des Entkontextualisierungsrisikos besondere Bedeutung zukommt.[394] Unergiebig waren hingegen die Regelungen zur Zurateziehung von Aufsichtsbehörden.[395] Näher ausgestaltet und insbesondere an informationstechnische Maßstäbe angebunden wird dagegen das Risiko der individuellen Verletzlichkeit im Rahmen der Systematik verschiedener Kontrollen zur Datensicherheit.[396] Auf die naheliegende Übernahme des Konzepts der *enforced accountability* kommen die Richtlinienvorschläge dagegen nicht.[397]

## IV. Ergebnis

Die Analyse des Rechts der Europäischen Union hat Parallelen zu den im internationalrechtlichen Abschnitt identifizierten Risiken und Schutzgütern aufgezeigt. Hierzu ist etwa die Binnenmarktorientierung des Sekundärrechts zu nennen. Insbesondere überschneiden sich jedoch die Risiken, wobei die europarechtlichen Quellen zu einer weiteren Konturierung beitragen konnten. Die Entscheidungen des EuGH und die Schlussanträge zu Art. 8 EU-GRC haben insbesondere anhand privater Datenverarbeitung die Risikokategorien Überwachungsdruck, individuelle Verletzlichkeit, Fehlerhaftigkeit der Daten, Publizitätsschäden und Persönlichkeitsprofile aufgegriffen, wobei zum Teil eine problematische normgeprägte Auslegung des Schutzguts der Vertraulichkeitserwartung vorgenommen wurde.[398]

Im Rahmen des Sekundärrechts wurde von der RL 95/46/EG das Risiko der individuellen Verletzlichkeit durch Identitätsdiebstahl, finanzielle Einbußen, Nachteile bei Erwerbs- und Geschäftsmöglichkeiten sowie Beeinträchtigungen der kör-

---

393 Siehe oben III.G.2.a).
394 Siehe oben III.G.2.b).
395 Siehe oben III.G.2.c).
396 Siehe oben III.G.2.d).
397 Siehe oben III.G.2.e).
398 Siehe oben II.B.2.e) und 3.

perlichen Unversehrtheit verdeutlicht. Weiterhin werden die Risiken des Überwachungsdrucks, der Entkontextualisierung, Fremdbestimmung, Publizitätsschäden (insbesondere Auslösung von Schamgefühl), Diskriminierungen und das Schutzgut der Menschenwürde aufgegriffen.[399] Der Richtlinie 2002/58/EG konnte dagegen zur Klarlegung des Risikos der Verletzlichkeit des Einzelnen über den Einsatz von Spähsoftware herangezogen werden. Daneben wurde dort der Anschluss an informationstechnische Schutzgüter (Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit) hergestellt. Zur näheren Beschreibung des Risikos der individuellen Verletzlichkeit wird neben dem Topos „Identitätsdiebstahl" auch „Identitätsbetrug" verwendet. Das Risiko von Publizitätsschäden wird als erhebliche Demütigung und Rufschädigung konkretisiert. Ebenfalls aufgegriffen werden Diskriminierungen und Überwachungsdruck.[400]

Der Rahmenbeschluss 2008/977/JI weist auf das Risiko der Umgehung von Schutzvorschriften beim Einsatz Privater bei polizeilicher Datenverarbeitung hin.[401] Der Vorschlag einer Grundverordnung greift das Schutzgut des Verbrauchervertrauens auf, über Vertrauenskonzeptionen können auch wirtschaftliche Risikokonzeptionen einbezogen werden. Daneben wird insbesondere das Risiko der Informationspermanenz im Rahmen des Rechts auf Vergessen aufgegriffen, wobei die Datenportabilität eher auf wettbewerbsrechtliche Risiken verweist. Selektivitätsschäden werden ebenso angegangen wie Verantwortungsnegation, individuelle Verletzlichkeit und Überwachungsdruck. Im Rahmen der Datenschutzfolgenabschätzung wird explizit eine Risikoterminologie eingeführt, die jedoch nicht konkretisiert wird.[402] Der RL-Vorschlag richtet sich gegen Selektivitätsschäden und ermöglicht dadurch die Zuordnung der Topoi Beeinträchtigung von Resozialisierung und Unschuldsvermutung zum Risiko der Publizitätsschäden. Daneben werden die Risiken Entkontextualisierung und individuelle Verletzlichkeit im Fall von Datensicherheitsverletzungen aufgegriffen.[403]

---

399 Siehe oben III.A.2.

400 Siehe oben III.C.2.

401 Siehe oben III.E.2.

402 Siehe oben III.F.2.

403 Siehe oben III.G.2.

*Teil 3*

# Deutsches Recht

## I. Überblick

### A. Thematische Eingrenzung einschlägiger Grundrechte

Datenschutzrechtliche Gewährleistungen können auf nationaler deutscher Ebene an mehreren Grundrechtspositionen festgemacht werden. Zu nennen sind das Fernmeldegeheimnis, Art. 10 Abs. 1 Var. 3 GG, der Schutz der Wohnung, Art. 13 Abs. 1 GG, sowie das Grundrecht auf Schutz der Persönlichkeit,[1] Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, das in weitere, sogleich zu besprechende Einzelverbürgungen ausdifferenziert ist. Bevor mit der Analyse der Risikokonzeptionen und Schutzgüter in Literatur und Rechtsprechung begonnen werden kann, müssen diese einschlägigen Grundrechtsgarantien hinsichtlich ihrer Konkurrenzen näher eingegrenzt werden.

Das Fernmeldegeheimnis des Art. 10 Abs. 1 Var. 3 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mithilfe des Telekommunikationsverkehrs. Dabei werden beliebige elektromagnetische und andere unkörperliche Formen der Übermittlung erfasst. Insbesondere erstreckt sich der Schutzbereich auf Internet und E-Mail.[2] Der Schutz bezieht sich jedoch nur auf den Übermittlungsvorgang und endet mit dessen Abschluss. Nur insoweit besteht die spezifische Gefahr der räumlich distanzierten Kommunikation, die im Einsatz eines Dritten beim Übermittlungsvorgang liegt. Die im Herrschaftsbereich eines Kommunikationsteilnehmers verbleibenden Daten sind deshalb nicht vom Fernmeldegeheimnis geschützt. Der Teilnehmer ist nach diesem Verständnis darauf verwiesen, dort eigene Vorkehrungen gegen ungewollten Datenzugriff zu treffen.[3]

Nicht von Art. 10 Abs. 1 Var. 3 GG geschützt ist zudem das Vertrauen der Kommunikationspartner zueinander. Risiken, die nicht in der Einschaltung eines Dritten bei der Übermittlung liegen, sondern im Kommunikationspartner begründet sind, fallen deshalb nicht in den Schutzbereich.[4] Erfasst werden hingegen neben dem

---

[1] Diese Bezeichnung wird in Abgrenzung vom zivilrechtlichen Allgemeinen Persönlichkeitsrecht vorgeschlagen, vgl. *Bäcker*, in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung, Fn. 7.

[2] *Jarass/Pieroth*, Grundgesetz, Art. 10 Rn. 5.

[3] BVerfGE 115, 166 (184).

[4] BVerfG Beschluss vom 9.10.2002, 1 BvR 1611/96, 805/98 *(Mithöreinrichtung)* = BVerfGE 106, 28 (37).

Kommunikationsinhalt auch die Kommunikationsumstände.[5] Hierunter fällt, „ob, wann und wie oft zwischen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder dieser versucht wurde".[6] Als problematisch hat sich in diesem Zusammenhang die Einordnung von IP-Adressen herausgestellt. Ausgangspunkt des BVerfG ist die Feststellung, dass eine bloße Zuordnung einer Nummer zu einem Anschlussinhaber die Vertraulichkeit des konkreten Kommunikationsvorgangs unberührt lässt, ein Eingriff in Art. 10 Abs. 1 GG in diesen Fällen nicht vorliege.[7] Lediglich die „identifizierende Zuordnung" dynamischer, also dem Teilnehmer nicht dauerhaft zugeordneter IP-Adressen wird am Maßstab des Art. 10 Abs. 1 GG gemessen, da das Gericht dort eine besondere Nähe zu konkreten Telekommunikationsvorgängen erkennt.[8] Entscheidend sei, dass die Telekommunikationsunternehmen zur Identifizierung der dynamischen Adressen „in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten müssen".[9] Dieser Zugriff auf die Telekommunikationsverbindungen falle unter das Telekommunikationsgeheimnis, unabhängig von der Grundlage, auf der die Diensteanbieter agieren (vertraglich oder gesetzlich), eine Verpflichtung zum Rückgriff auf diese Daten begründe den Eingriff in Art. 10 Abs. 1 GG.[10]

Art. 13 Abs. 1 GG lässt sich als Ergänzung dieses Schutzbereichszuschnitts von Art. 10 Abs. 1 GG verstehen, der die im Herrschaftsbereich des Kommunikationsteilnehmers verbleibenden Daten ausnimmt. Die Garantie der Unverletzlichkeit der Wohnung schützt die Privatheit als „räumliche Sphäre" der Entfaltung des Privatlebens. Unter den Begriff „Wohnung" fallen alle Räume, die der allgemeinen Zugänglichkeit durch räumliche Abschirmung entzogen sind und zur Stätte privaten Lebens und Wirkens gemacht wurden.[11] Art. 13 Abs. 1 GG schützt auch Maßnahmen, durch die sich staatliche Stellen mit besonderen Hilfsmitteln Einblick in die Vorgänge innerhalb einer Wohnung verschaffen, soweit diese Vorgänge der natürlichen Wahrnehmung von außen entzogen sind. Erfasst werden damit insbesondere technische Überwachungsmaßnahmen.[12] Auch dieser Schutz bleibt jedoch in seiner räumlichen Bezogenheit auf den Begriff der Wohnung fragmentarisch.

Das Potenzial für einen umfassenderen Schutz bietet das bereits oben angesprochene[13] Grundrecht auf informationelle Selbstbestimmung, das in der Volkszählungsentscheidung des BVerfG als Einzelverbürgung des Grundrechts auf Schutz

---

5 BVerfGE 115, 166 (183).

6 Epping/Hillgruber-*Baldus*, Art. 10 Rn. 8.

7 BVerfGE 130, 151 (180 f.).

8 Ebd., (181).

9 Ebd.

10 Ebd., (181 f.).

11 *Jarass/Pieroth*, Grundgesetz, Art. 13 Rn. 1, 4.

12 BVerfGE 120, 274 (310).

13 Siehe oben Einleitung, I.

der Persönlichkeit, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelt wurde.[14] Das Grundrecht auf Schutz der Persönlichkeit war zu Beginn der maßgeblichen Rechtsentwicklung der geeignete Anknüpfungspunkt für die Implementierung des Datenschutzes, da es auf Elemente abzielt, die nicht bereits Gegenstand spezieller Freiheitsverbürgungen sind, diesen jedoch in ihrer konstituierenden Bedeutung für die Persönlichkeit des Menschen nicht nachstehen.[15] Durch die vom BVerfG betonte Entwicklungsoffenheit ist es in der Lage, aktuelle Entwicklungen und neuartige Risiken aufzugreifen.[16] Der grundrechtliche Schutz der informationellen Selbstbestimmung ist in diesem Zusammenhang zu verstehen. Er garantiert dem Einzelnen die Befugnis, selbst über Preisgabe und Verwendung persönlicher Daten zu bestimmen. Er garantiert ferner die „aus dem Gedanken der Selbstbestimmung" folgende Entscheidungshoheit über die Offenbarung persönlicher Lebenssachverhalte.[17] Der Schutz ist dabei weder auf automatische Datenverarbeitung noch auf Daten mit Bezug zu Privat- oder Intimsphäre beschränkt.[18] Diese sich an der Auffangfunktion des Art. 2 Abs. 1 GG[19] orientierende Konzeption ist Anlass für fortdauernde Kritik an der „Konturlosigkeit"[20] und Ausuferung der Verbürgung.[21] Die vielfältigen Vorschläge zur Begrenzung und Präzisierung sind kaum mehr überschaubar.[22] Die Ausdifferenzierung des Grundrechts auf Schutz der Persönlichkeit in zahlreiche Einzelverbürgungen schafft darüber hinaus das Problem, deren Verhältnis zueinander zu bestimmen. Die Einzelverbürgungen überschneiden sich dabei teilweise. Hierzu gehören insbesondere die Grundrechte auf Schutz des eigenen Bildes, des eigenen Wortes, der Privatsphäre in räumlicher und thematischer Hinsicht sowie das neue Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme.[23]

Die Abgrenzung des Grundrechts auf Schutz der Persönlichkeit zu Art. 10 Abs. 1 GG und Art. 13 Abs. 1 GG lässt sich im Wege der Spezialität relativ einfach durchführen: [24] So ist Art. 10 Abs. 1 GG beispielsweise dann gegenüber dem Recht auf informationelle Selbstbestimmung spezieller, wenn Telefonverbindungsdaten an Strafverfolgungsbehörden weitergegeben werden. Art. 13 Abs. 1 GG ist grundsätz-

---

[14] BVerfGE 65, 1 (43).

[15] Maunz/Dürig-*Di Fabio*, Art. 2 Rn. 127.

[16] Ebd. Rn. 147.

[17] BVerfGE 65, 1 (42 f.).

[18] *Jarass/Pieroth*, Grundgesetz, Art. 2 Rn. 42 f.

[19] BVerfGE 6, 32 (36).

[20] *Ladeur*, DÖV 2009, 45 sowie 49 m.w.N.

[21] *Albers*, Informationelle Selbstbestimmung, S. 280. Zur Kritik im Einzelnen ebd., S. 174 ff. sowie die Nachweise bei *Bull*, Informationelle Selbstbestimmung, S. 16, Fn. 24.

[22] Vgl. etwa die Zusammenstellung bei *Rogall*, Informationseingriff, S. 49 ff.

[23] *Hoffmann-Riem*, in: ders. (Hrsg.), Offene Rechtswissenschaft, S. 539. Eingehend und weiter differenzierend Maunz/Dürig-*Di Fabio*, Art. 2 D.

[24] Zum Ganzen *Frenz*, DVBl. 2009, 333 (338 f.).

lich spezieller, soweit die Daten aus der Wohnung erhoben werden. Eine Ausnahme hiervon besteht jedoch, wenn eine nur partielle Überschneidung des Grundrechts auf informationelle Selbstbestimmung mit einem spezielleren Freiheitsrecht vorliegt bzw. wo sich ein eigenständiger Freiheitsbereich mit festen Konturen herausgebildet hat. Dies soll etwa der Fall sein, wenn eine Wohnungsdurchsuchung zur Erlangung von auf Endgeräten gespeicherten Telekommunikationsverbindungsdaten durchgeführt wird. In diesem Fall gehe es nicht nur um die Überwindung der räumlichen Grenzen, vielmehr sei der Schutzgehalt der Daten von einigem (eigenständigem) Gewicht.[25] So wird dann auch in der Entscheidung des BVerfG zur Durchsuchung einer Richterwohnung (*Bargatzky*-Entscheidung)[26] auf diese Ergänzungsfunktion des Grundrechts auf informationelle Selbstbestimmung verwiesen.[27]

Schwieriger gestaltet sich dagegen die Abgrenzung der Einzelverbürgungen des Art. 2 Abs. 1 GG untereinander. Ein Weg, das Verhältnis zwischen Grundrecht auf informationelle Selbstbestimmung und Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) zu bestimmen, verdeutlicht das Urteil des BVerfG zur *Online-Durchsuchung* vom 27.2.2008.[28] Hiernach soll das Grundrecht auf informationelle Selbstbestimmung für den Zugriff auf einzelne Kommunikationsvorgänge oder gespeicherte Daten heranzuziehen sein, während das IT-Grundrecht den Gesamtzugriff auf das System – die „Infiltration" – erfasst.[29] Auch diese Anbindung des Schutzes an das System als solches soll nur insoweit erfolgen, als das System personenbezogene Daten des Betroffenen in einem Umfang und einer Vielfalt enthalten kann, die im Zugriffsfall einen Einblick in wesentliche Teile der Lebensgestaltung einer Person bzw. ein aussagekräftiges Bild der Persönlichkeit ermöglichen. Am Grundrecht auf informationelle Selbstbestimmung sollen dagegen auch Zugriffe auf Systeme gemessen werden, soweit diese lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich enthalten. Als Beispiel hierfür gibt das BVerfG eine vernetzte elektronische Steuerungsanlage der Haustechnik an.[30] Beispielhaft für die andere Kategorie von Systemen, die ein aussagekräftiges Bild der Persönlichkeit ermöglichen, sind soziale Netzwerke.[31] Das IT-Grundrecht verbindet damit die räumliche Schutzbereichskonzeption des Art. 13 Abs. 1 GG mit der inhaltlichen Dimension des Grundrechts auf informationelle Selbstbestimmung. So verstanden ist das IT-Grundrecht ein Schutz des „virtuellen Hauses" des modernen Menschen. Freilich liegt nach mo-

---

[25] Ebd.

[26] BVerfG Urteil vom 2.3.2006, 2 BvR 2099/04 *(Bargatzky)* = BVerfGE 115, 166.

[27] BVerfGE 115, 166 (188).

[28] Urteil vom 27.2.2008, 1 BvR 370, 595/07 *(Online-Durchsuchung)* = BVerfGE 120, 274.

[29] Zu diesem Risiko siehe unten II.B.15. und 16.

[30] BVerfGE 120, 274 (313 f.).

[31] *Drackert*, eucrim 2011, 122 (124, 126).

mentanem Stand der Technikentwicklung noch keine gleiche Angewiesenheit zwischen realer und virtueller Wohnung vor,[32] mit zunehmender Bedeutung informationstechnischer Systeme für das tägliche Leben verliert dieser Unterschied jedoch an Relevanz. Das Verhältnis der übrigen Einzelverbürgungen des Art. 2 Abs. 1 GG zueinander lässt sich dagegen nur im Einzelfall bestimmen, oftmals überschneiden sich die Verbürgungen auch.[33]

## B. Funktionale Eingrenzung nach Wirkmodus der Grundrechte

Die Entwicklungsoffenheit des Grundrechts auf Schutz der Persönlichkeit, Art. 2 Abs. 1 GG, ermöglicht die Ausdehnung des Schutzes auf Risiken, die aus neuen Techniken wie beispielsweise den sozialen Netzwerken[34] resultieren. Allein diese Öffnung des Schutzbereichs für neue Verarbeitungstechniken würde jedoch der spezifischen Charakteristik heutiger Datenverarbeitung zumindest dann nicht gerecht, wenn der Grundrechtsschutz allein klassisch als Abwehr staatlicher Eingriffe verstanden würde. Risiken durch private Datenverarbeitung könnten dann von vornherein nicht angemessen aufgegriffen werden. Bereits die Analyse der Rechtsprechung des EuGH und des europäischen Sekundärrechts haben darauf hingewiesen, dass ein spezifisch datenschutzrechtliches Risiko jedoch gerade aus der massiv angestiegenen Datenverarbeitung durch Private resultiert.[35] Dieses Risiko kann nicht nur aus der privaten Datenverarbeitung selbst folgen, sondern potenziert und wandelt sich durch den jederzeit möglichen Zugriff staatlicher Stellen auf die privaten Datenbestände.[36] Sofern der Datenschutz konsequent als Vorfeldschutz verstanden wird,[37] liegt die Ausdehnung des Schutzes auf diese Risiken nahe. Die hieraus resultierenden Probleme betreffen die allgemeinen Grundrechtslehren und wurden in letzter Zeit insbesondere von *Hoffmann-Riem* und *Masing* aufgegriffen. Dieser Diskurs ist für die vorliegende Untersuchung relevant, da er zeigt, wie über allgemeine Grundrechtslehren eine Verschiebung der verfassungsrechtlichen Risikoperzeption vorgenommen wird. So führt *Hoffmann-Riem* aus, dass die Gefahren durch Private unter heutigen Rahmenbedingungen die von Trägern der Staatsgewalt versursachbaren Gefährdungen übersteigen können. Dem Staat komme aufgrund der zunehmend privaten Informationsinfrastruktur eine Privatisierungsfolgenverantwortung zu. Gegebenenfalls könne diese die Form einer grundrechtlichen

---

32 Vgl. BVerfGE 113, 348 (391).

33 Maunz/Dürig-*Di Fabio*, Art. 2 Abs. 1 Rn. 148. Für eine Bestimmung des Verhältnisses der Einzelverbürgungen nach Maßgabe einer Selbstdarstellungskonzeption siehe *Britz*, Selbstdarstellung, S. 65 ff.

34 *Drackert*, eucrim 2011, 122 ff.

35 Vgl. oben Teil 2, II.B.2.c).

36 Vgl. oben Teil 2, II.B.2.d).

37 *Duttge*, JZ 1996, 558 (560 f.).

Schutzpflicht annehmen, zumindest führe sie jedoch zu einem Ausgestaltungsauftrag für den Bereich der Kommunikationsinfrastruktur. Die derzeitige Asymmetrie von privatem und öffentlichem Datenschutz entspreche nicht dem objektivrechtlichen Gehalt der Grundrechtsnormen.[38] Im Anschluss spricht sich *Hoffmann-Riem* nach einem Vergleich mit hinnehmbaren Risiken in anderen gesellschaftlichen Bereichen (Rauchen, Alkoholkonsum, Jugendschutz) für eine Neujustierung des Datenschutzes aus und schließt dabei eine Beschränkung gesetzlicher Schutzmaßnahmen im Zuge der Herstellung praktischer Konkordanz und der Angleichung des Schutzniveaus im privaten und staatlichen Bereich nicht aus.[39] Das Grundrecht auf informationelle Selbstbestimmung wandele sich von einem Abwehrrecht gegen staatliche Eingriffe zu einem Element der Sicherung einer mehrdimensionalen und mehrpoligen kommunikativen Entfaltung in der Informationsgesellschaft.[40]

Auch *Masing* sieht den privaten Datenschutz durch Schutzpflichten und mittelbare Drittwirkung zunehmend gegenüber dem Datenschutz in Staat-Bürger-Konstellationen in den Vordergrund treten: Im Verhältnis zwischen Privaten wirken die Grundrechte nur mittelbar und als objektive Prinzipien, dieser Wirkmodus verpflichte den Staat lediglich zu einem Ausgleich zwischen den gleichermaßen berechtigten Freiheitssphären der Bürger. Es gehe nicht um die Minimierung von Eingriffen, sondern um das Abfangen derjenigen Ungleichgewichte, die der Verwirklichung der Leitideen der Grundrechte auf der Ebene der Gleichheit zwischen Privaten entgegenstehen.[41] *Masing* spricht sich sodann für einen Perspektivenwechsel aus: Bei privater Datenverarbeitung sei nicht erst die Erlaubnis zur Verarbeitung rechtfertigungsbedürftig, sondern primär deren Einschränkung. Im Gegensatz zu den Regelungen im staatlichen Bereich müssten deshalb möglichst weite Gestaltungsräume offengehalten werden. Die privaten Datenverarbeitungsregelungen seien keine gesetzlichen Eingriffsgrundlagen und könnten nicht den gleichen Bestimmtheitsanforderungen unterliegen. Auch könne die Zweckbindung nicht ohne Weiteres auf Private übertragen werden. Zudem sei es irreführend, dort von einem Verbot mit Erlaubnisvorbehalt zu sprechen.[42] Stattdessen komme der Einwilligung eine zentrale Rolle zu, sie dürfe jedoch nicht als absolute Verfügungsbefugnis konstruiert werden. Der Datenschutz zwischen Privaten sei ein Ausgestaltungsauftrag an den Gesetzgeber, genau wie das übrige Zivilrecht. Hier könne jedoch auch eine mittelbare Grundrechtswirkung zu strengen Anforderungen an den Gesetzgeber führen. Erforderlich seien eine rechtlich differenzierte Absicherung von Vertraulichkeitserwartungen sowie die Chance auf Vergessen.[43] Hier wird

---

38 *Hoffmann-Riem*, AöR 123 (1998), 514 (524 f.).

39 Ebd., (528 f., 539).

40 Ebd., (538 f.).

41 *Masing*, NJW 2012, 2305 (2306).

42 Ebd., (2307).

43 Ebd., (2307 f.).

das Risiko privater Datenverarbeitungen relativiert und das datenschutzrechtliche Prinzip des grundsätzlichen Verbots von Datenverarbeitungen für den privaten Bereich hinterfragt.

Die beiden dargestellten Literaturstimmen verdeutlichen, dass bei der Auswertung der Rechtsprechung in Bezug auf Risikokonzeptionen und Schutzgüter das Augenmerk auch auf die funktionale Ebene zu legen ist, da sich auch an dieser „Stellschraube" die Perzeption insbesondere der Risiken durch private Datenverarbeitungen niederschlagen kann und künftig stärker auswirken wird.

## C. Zwischenbetrachtung: Analyse nach Konzeptionen

Für den Fortgang der Untersuchung sind damit die einschlägigen Grundrechtsgarantien thematisch und funktional eingegrenzt. Die bereits angeklungene starke Befassung der Rechtslehre mit dem verfassungsrechtlichen Datenschutz und insbesondere mit dem Grundrecht auf informationelle Selbstbestimmung rechtfertigt eine eigenständige Analyse der wichtigsten Konzeptionen der Literatur, die im Anschluss an die Prüfung der Rechtsprechung des BVerfG vorgenommen wird. Die Literaturkonzeptionen können trotz eines möglichen „rechtspolitischen Gehalts" Rückschlüsse auf hier interessierende Risikokonzeptionen und Schutzgüter vermitteln, da für die Auswahl des einbezogenen Schrifttums der enge Bezug und die Anbindung der Konzeption an das geltende Datenschutzrecht maßgeblich waren.[44]

Die Rechtsprechung wird entsprechend der oben vorgenommenen thematisch-funktionalen Eingrenzung historisch-zusammenfassend analysiert, um die Entwicklungslinien nachzuzeichnen und damit insbesondere den kontinuierlichen Wandel der Schutzgüter und aufgegriffenen Risiken angemessen einzubeziehen. Bereits dieser Untersuchungsaufbau lässt eine Anlehnung an *Ehmanns* naheliegende Annahme aufscheinen, wonach sich die Rechtsprechung zur informationellen Selbstbestimmung als zunehmende „Entkörperlichung" des Schutzguts darstellt, die jedoch bei steigender Bedeutung der Privatrechtswirkung in Ermangelung der objektiven Manifestation einschlägiger privater Willensbetätigungen an ihre Grenzen stößt.[45] Die mit dem IT-Grundrecht vorgenommene Rückbindung an das räumlich verstandene informationstechnische System könnte insoweit auf eine Rückkehr zur „gegenständlichen Verkörperung"[46] des Schutzguts hinweisen.[47] Freilich würde damit die seit den Anfängen der Datenschutzdiskussion von einem Teil der Literatur angestrebte Abkehr von der „Sphärentheorie" relativiert.[48]

---

[44] Näher zu Forschungszielen und Methode oben Einleitung III. und IV.

[45] Vgl. *Ehmann*, AcP 188 (1988), 306 ff.

[46] *Ehmann* bezieht diese freilich auf die geschützte Willensmacht, vgl. ebd., 306.

[47] Befürwortet wird eine Rückkehr zu Sphärenkonzeptionen insbesondere durch *Böckenförde*, JZ 2008, 938 f.

[48] Zu dieser Abkehr vgl. Simitis-*Simitis*, § 1 Rn. 35 ff.

Der kontinuitären Konzeption der Rechtsprechung stehen die Ansätze der Literatur gegenüber. Hiervon werden exemplarisch fünf besonders bedeutsame Ansätze herausgegriffen und näher untersucht.[49] Die Analyse wird abgeschlossen mit weiteren Konzeptionen der Literatur, die nicht in gleichem Maße umfassend wie die vorgenannten sind, sondern eher punktuelle Aspekte betreffen.[50] Die unüberschaubare Vielfalt der Einzelansichten zu Datenschutzfragen seit den 1970er-Jahren lässt sich im Rahmen dieser Untersuchung nicht erschöpfend behandeln, sodass eine selektive Eingrenzung auf wichtige Ansichten notwendig war, was insbesondere deshalb vertretbar ist, weil die neueren Literaturkonzeptionen die älteren Auffassungen würdigen und teilweise auf ihnen aufbauen bzw. sie einbeziehen.

# II. Rechtsprechung des BVerfG

## A. Überblick

Zur besseren Einordnung der folgenden Analyse nach Risiken und Schutzgütern sind zunächst Kontext und Vorbedingungen der untersuchten Entscheidungen und die verfassungsgerichtliche Prüfungsabfolge beim Recht auf informationelle Selbstbestimmung überblickartig darzustellen.

### 1. Kontext der kontinuitären Konzeption

Die hohe Aussagekraft der Rechtsprechung des BVerfG zu datenschutzrechtlichen Risikokonzeptionen und Schutzgütern speist sich aus drei Entwicklungen, die auch darüber hinaus maßgeblich für die überragende Bedeutung der Grundrechtsjudikatur in Deutschland sind. Dies ist zunächst der von *Dieter Grimm* als „wichtigster Markstein" grundrechtlicher Rechtsprechung bezeichnete Verhältnismäßigkeitsgrundsatz.[51] Diese aus dem Rechtsstaatsprinzip und dem „Wesen der Grundrechte selbst" abgeleitete Rechtsfigur verlangt als „Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat", dass Grundrechte „nur so weit beschränkt werden dürfen, als es zum Schutze öffentlicher Interessen unerlässlich ist".[52] Die Herausbildung des aus den vier Teilgeboten legitimer Zweck, Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit im engeren Sinne (bzw. Angemessenheit) aufgebauten Verhältnismäßigkeitsgrundsatzes setzte 1954 ein und trägt mittlerweile die Hauptlast des Grundrechtsschutzes.[53] Wie die nachfol-

---

[49] Siehe unten III.A.–E.

[50] Siehe unten III.F.

[51] *Grimm*, Verfassung II, S. 186.

[52] BVerfGE 19, 342 (348 f.); *Jarass/Pieroth*, Grundgesetz, Art. 20 Rn. 80.

[53] *Grimm*, Verfassung II, S. 186.

gende Analyse zeigt, finden sich die maßgeblichen Risikokonzeptionen und Schutzgüter neben der Stufe des Schutzbereichs[54] vor allem auf der Ebene der Verhältnismäßigkeit im engeren Sinne. Die dort vorzunehmende Abwägung erfordert in erster Linie eine Beurteilung der Eingriffsschwere,[55] bei der in verschiedenen datenschutzrechtlichen Entscheidungen etwa Intensitätskriterien[56] entwickelt wurden, welche die Identifikation von Risikokonzeptionen ermöglichen.

Die zweite Entwicklung liegt in der im *Elfes*-Urteil[57] vorgenommenen Ausweitung des punktuellen Grundrechtsschutzes zur Lückenlosigkeit, indem Art. 2 Abs. 1 GG als „Auffanggrundrecht" gedeutet wurde.[58] Hierin liegt eine der Vorbedingungen der Öffnung des Grundrechtsschutzes für neue Gefährdungslagen, die ebenfalls über Art. 2 Abs. 1 GG erfolgt ist und im Volkszählungsurteil[59] seine wirkkräftigste Bestätigung für den Fall des Datenschutzes fand. Die damit eintretende „informationsrechtliche Wende"[60] führte dazu, dass zahlreiche informationsbezogene polizeiliche Maßnahmen nicht mehr als schlichtes Verwaltungshandeln angesehen wurden und deshalb die allgemeinen Aufgabenzuweisungen und Generalermächtigungen keine tauglichen Eingriffsgrundlagen mehr darstellten.[61] Auch das Strafprozessrecht wurde durch die Vorgaben des Volkszählungsgesetzes stark geprägt – zahlreiche der nach den Terroranschlägen vom 11.9.2001 eingeführten strafprozessualen Überwachungsmaßnahmen wurden am Recht auf informationelle Selbstbestimmung gemessen.[62] Es sind vor allem diese Entscheidungen, welche den Ausgangspunkt für die folgende Analyse bilden und welche die zu untersuchenden Risikokonzeptionen und Schutzgüter näher ausgestalten.

Die dritte Entwicklung reicht ebenfalls bereits auf das Jahr 1958 zurück und ist in der Anerkennung einer objektiven Dimension der Grundrechte in der *Lüth*-Entscheidung zu sehen.[63] Die hiervon ausgehende Wirkung der Grundrechte auf die Anwendung des gesamten einfachen Rechts, insbesondere des Zivilrechts, war

---

[54] Eine Übernahme der in der Literatur teilweise vorgenommenen Unterscheidung zwischen Schutzbereich und Gewährleistungsgehalt ist für die Forschungsziele dieser Untersuchung nicht nötig, im Zweifel wird von dem weiteren Verständnis ausgegangen. Zur Unterscheidung vgl. *Jarass/Pieroth*, Grundgesetz, Vorb. Vor Art. 1 Rn. 21.

[55] Näher zu diesem Teilgebot ebd., Art. 20 Rn. 86, 86a.

[56] Siehe unten II.B.9.a).

[57] BVerfG, Urteil vom 16.1.1957, 1 BvR 253/56 *(Elfes)* = BVerfGE 6, 32.

[58] *Grimm*, Verfassung II, S. 186.

[59] BVerfG, Beschluss vom 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83 *(Volkszählung)* = BVerfGE 65, 1.

[60] Einen ähnlichen Begriff verwendet *Amelung*, allerdings erst für die Entscheidung zum zweiten *G-10*-Gesetz, vgl. *Amelung*, ZStW 123 (2011), 595 (602).

[61] *Menzel/Müller-Terpitz* (Hrsg.), Verfassungsrechtsprechung, S. 370 f.

[62] Ebd., S. 371.

[63] BVerfG Urteil vom 15.1.1958, 1 BvR 400/51 *(Lüth)* = BVerfGE 7, 198.

Grundlage für die in der ersten Abtreibungsentscheidung von 1975[64] erfolgte Ergänzung der grundrechtlichen Handlungsschranken um staatliche Handlungspflichten im Fall der Bedrohung verfassungsrechtlich geschützter Freiheiten von Dritten.[65] Im Rahmen der oben vorgenommenen funktionalen Eingrenzung wurde bereits festgestellt, dass diese Drittkonstellation im Hinblick auf datenschutzrechtliche Risiken wegen der Bedeutung privater Kommunikationsdienste im Internet eine besondere Rolle einnimmt.[66]

Die drei beschriebenen Entwicklungen bilden auf einer übergeordneten Ebene die Vorbedingung und den Kontext für die Entwicklung des verfassungsrechtlichen Datenschutzes durch das BVerfG. Im Folgenden ist zur besseren Einordnung der sich anschließenden Analyse von Risiken und Schutzgütern ein auch für die anderen einschlägigen Grundrechte exemplarischer Überblick über die Schutzbereichs- und Eingriffsdogmatik des Rechts auf informationelle Selbstbestimmung zu geben.

### 2. Prüfungsabfolge Recht auf informationelle Selbstbestimmung

Kernelement des vom Verfassungsgericht als Befugnis zur Selbstbestimmung[67] umschriebenen Schutzbereichs des Rechts auf informationelle Selbstbestimmung ist ein relativ abstraktes und dadurch weitreichendes „abwehrrechtlich geschütztes individuelles Entscheidungsrecht“.[68] Der Schutzbereich setzt dabei lediglich den Personenbezug bzw. die Personenbeziehbarkeit der Daten voraus und erstreckt sich sachlich von der Preisgabe bis zu Verwendung der Daten, wobei die Reichweite prozess- und verarbeitungsorientiert bestimmt wird:[69] Grundsätzlich wird jeder Verarbeitungsschritt – wie beispielsweise Speicherung, Veränderung, Nutzung oder Übermittlung – als Eingriff angesehen, wobei sich diese Konzeption nicht auf derart klare Phasen beschränkt, sondern angesichts der „nicht-linearen, vernetzten und vielschichtigen Prozesse“ der Datenverarbeitung jeweils eigenständig herauskristallisiert werden muss, ob ein Eingriff vorliegt. Ein solcher kann beispielsweise auch in einem Abgleich mit Suchbegriffen oder einer Relevanzprüfung liegen[70] oder aber aufgrund technisch spurenloser Aussonderung unmittelbar nach der Erfassung abzulehnen sein.[71] Die daraus resultierende Ablösung vom traditionellen

---

[64] BVerfG Urteil vom 25.2.1975, 1 BvF 1, 2, 3, 4, 5, 6/74 *(Schwangerschaftsabbruch I)* = BVerfGE 39, 1.

[65] *Grimm*, Verfassung II, S. 186.

[66] Siehe oben I.B.

[67] BVerfGE 65, 1 (42 f.).

[68] *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, S. 139.

[69] Zum Ganzen ebd., S. 139–141.

[70] BVerfGE 100, 313 (366 f.).

[71] BVerfGE 120, 378 (399); näher dazu unten II.B.8.

Eingriffsverständnis dient der Abstimmung auf die Schutzbereichsbeschreibung.[72] Der so umschriebene abwehrrechtliche Gehalt wird flankiert durch Verpflichtungen zu organisations-, verfahrens- und technikbezogenen Schutzvorkehrungen und Kenntnisrechten der Betroffenen.[73] Aufgrund dieser auf einzelne Verarbeitungsschritte abgestimmten Eingriffskonzeption knüpft auch das Erfordernis von gesetzlichen Ermächtigungsgrundlagen an einzelne Verarbeitungsschritte an: Diese sind für jeden Verarbeitungsschritt erforderlich, Aufgaben- und Befugnisnormen decken den Umgang mit personenbezogenen Daten nicht ab.[74] Die Anforderungen an die Eingriffsgrundlagen werden in der Rechtsprechung des BVerfG ebenfalls eigenständig auf den datenschutzrechtlichen Kontext abgestimmt; neben dem Verhältnismäßigkeitsprinzip sind dies insbesondere die Grundsätze der Zweckfestlegung und Zweckbindung, wobei eine Vorratsdatenspeicherung zu unbestimmten oder nicht bestimmbaren Zwecken verfassungswidrig ist und auch Zweckänderungen eine eigenständige, normenklare gesetzliche Grundlage benötigen, die mit dem ursprünglichen Verwendungszweck vereinbar und durch überwiegende Allgemeininteressen gerechtfertigt sein muss.[75]

### 3. Konsequenzen für die weitere Prüfung

Die Rechtsprechung des BVerfG zu datenschutzrechtlichen Risiken und Schutzgütern lässt sich angesichts der Vorbedingungen und der Genese[76] als „kontinuitäre Rechtsentwicklung“ auffassen. Entsprechend ist die Analyse historisch-systematisierend aufgebaut, um auch ältere Entscheidungen einzubeziehen und damit die Risiken und Schutzgüter auch in ihrer Entstehung zu analysieren. Erste Hinweise auf datenschutzrechtliche Risiken und Schutzgüter finden sich bereits in frühen Entscheidungen zum Allgemeinen Persönlichkeitsrecht mit denen sich die nachfolgende Rechtsprechungsanalyse befasst.

## B. Risikokonzeptionen und Schutzgüter

### 1. Verwaltungstechnische Entpersönlichung

Die *Mikrozensus*-Entscheidung des BVerfG vom 16.7.1969[77] betraf Auskunftspflichten hinsichtlich durchgeführter Urlaubs- und Erholungsreisen. Bereits in dieser frühen Phase werden Risikokonzeptionen und Schutzgüter deutlich, die sich

---

72 *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, S. 140.

73 Ebd.

74 Ebd.

75 Umfassende Rechtsprechungsnachweise ebd., S. 141, Fn. 164.

76 Vgl. hierzu ebd., S. 141.

77 BVerfG, Beschluss vom 16.7.1969, 1 BvL 19/63 *(Mikrozensus)* = BVerfGE 27, 1.

auch in den Regelungen auf internationaler und europäischer Ebene, insbesondere zum Schutz vor Profiling,[78] finden. Das Gericht zieht Art. 1 Abs. 1 GG und Art. 2 Abs. 1 GG als Prüfungsmaßstab heran und führt aus, dass es mit der Menschenwürde nicht zu vereinbaren sei, Menschen zwangsweise in ihrer ganzen Persönlichkeit „zu registrieren und zu katalogisieren".[79] Sie würden damit wie eine Sache behandelt, die einer „Bestandsaufnahme in jeder Beziehung" zugänglich sei. Sodann zieht das Gericht die bereits seit *Josef Kohler*[80] geläufige Begründungsfigur eines „Innenraums" heran, „in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt".[81] Das Risiko des „psychischen Drucks" durch „öffentliche Anteilnahme" wird ebenfalls bereits explizit einbezogen. Hinsichtlich der Schutzgüter verweist die Entscheidung neben der Menschenwürde auf das „Selbstbestimmungsrecht im innersten Lebensbereich".[82] Der Schutzbereich wird jedoch entsprechend der sphärenartigen Konzeption auf den Bereich „menschlichen Eigenlebens" eingegrenzt, der „von Natur aus Geheimnischarakter" habe. Nur insoweit bestünden Sperren vor dem explizit herausgestellten Risiko einer „verwaltungstechnischen Entpersönlichung". Sofern das Verhalten den Außenbereich berühre, fehle in der Regel der notwendige Persönlichkeitsbezug. Das BVerfG sah aus diesem Grund im vorliegenden Fall keinen Verstoß gegen Art. 1 Abs. 1, Art. 2 Abs. 1 GG und betonte, dass sich die Informationen „ohne größere Schwierigkeiten" auch ohne Befragung hätten ermitteln lassen.[83]

Die im Anschluss ergangene Entscheidung vom 15.1.1970 hatte die Übersendung von *Ehescheidungsakten* im Rahmen eines Disziplinarverfahrens wegen des Verdachts eines Dienstvergehens durch ein „ehebrecherisches Verhältnis" zum Gegenstand.[84] Das Gericht prüft wie bereits im *Mikrozensus*-Beschluss Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, nimmt jedoch nicht in vergleichbar umfangreichem Ausmaß Stellung zu einschlägigen Schutzgütern. Gleichwohl tritt bei der Prüfung der Erforderlichkeit das Risiko der Entkontextualisierung in der oben beschriebenen Form der Kontextinfiltration[85] hervor: Das Gericht rügt die fehlenden Feststellungen des Fachgerichts zur Erforderlichkeit der Aktenübersendung. Die Auswirkung des Verhaltens im Lebensbereich der Familie auf den amtlichen Tätigkeitsbereich, der Gegenstand der disziplinarischen Beurteilung war, verstehe sich nicht von selbst. Wechselseitige Rückwirkungen lägen „keineswegs in allen Fällen

---

78 Siehe oben Teil 1, II.C., Teil 2, III.F.2.c).

79 BVerfGE 27, 1 (6).

80 Siehe oben Einleitung, I.

81 So unter Verweis auf *Wintrich* BVerfGE 27, 1 (6 f.).

82 BVerfGE 27, 1 (7).

83 Ebd., (7 f.).

84 BVerfG, Beschluss vom 15.1.1970, 1 BvR 13/68 *(Ehescheidungsakten)* = BVerfGE 27, 344.

85 Siehe oben Teil 1, II.

auf der Hand".[86] Zwar war die Beschwerde zu dem – für heutige Verhältnisse grotesk anmutenden – Verfahrensgegenstand wegen der Verletzung des Verhältnismäßigkeitsprinzips begründet; der Schutzbereich von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG wird jedoch im Gegensatz zu den komplexen Ausführungen des *Mikrozensus*-Beschlusses nicht weiter konkretisiert.

Die beiden Entscheidungen verdeutlichen damit die räumliche Schutzbereichskonzeption, welche die Risiken von Publizität und Entkontextualisierung aufgreift.

### 2. Frühe Vertraulichkeitskonzeptionen

In einer Reihe darauf folgender Entscheidungen wurde das Allgemeine Persönlichkeitsrecht in seiner Ausprägung als Privatsphärenschutz auf – aus heutiger Sicht – datenschutzrechtliche Sachverhalte angewendet. Ausführungen zu einschlägigen Risiken bleiben zwar punktuell, lassen sich aber der oben beschriebenen Vertraulichkeitskonzeption[87] zuordnen: So wird in einem Beschluss vom 8.2.1972 zur Beschlagnahme von Patientenkarteikarten[88] das Vertrauensverhältnis zwischen Arzt und Patient als Grundvoraussetzung ärztlichen Wirkens herausgestellt und über Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt.[89] An eine Vertrauensbeziehung knüpft auch die Entscheidung zum Zeugnisverweigerungsrecht für Sozialarbeiter vom 19.7.1972[90] an. Dort wird bereits deutlich mit der Rechtsfigur einer Vertraulichkeitserwartung operiert: Eine solche sei mit dem Berufsbild des Sozialarbeiters gerade nicht verbunden.[91] In den gleichen Kontext fällt die Entscheidung des BVerfG vom 24.5.1977,[92] welcher die Durchsuchung von Räumen einer Drogenberatungsstelle und die Beschlagnahme dort vorgefundener Unterlagen zugrunde lag. Dort wird die Wahrung des Geheimhaltungsinteresses als „Vorbedingung" eines funktionsnotwendigen Vertrauens in die Tätigkeit von Beratungsstellen bezeichnet. Geprüft wurden dabei eine Verletzung der allgemeinen Handlungsfreiheit, Art. 2 Abs. 1 GG, hinsichtlich der Beratungsstelle sowie das Grundrecht auf Achtung der Privatsphäre, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, bezüglich der betroffenen Kunden. Für die Tätigkeit der Beratungsstelle wurde zudem die im Sozialstaatsprinzip, Art. 20 Abs. 1, 28 Abs. 1 S. 1 GG, verankerte Gesundheitsfürsorge herangezogen.[93] Insgesamt zeichnet sich somit schon in diesen frühen Entschei-

---

[86] BVerfGE 27, 344 (354).

[87] Siehe oben Teil 1, IV.B.5. und 6.

[88] BVerfG, Beschluss vom 8.3.1972, 2 BvR 28/71 *(Patientenkartei)* = BVerfGE 32, 373.

[89] Ebd., (380).

[90] BVerfG, Beschluss vom 19.7.1972, 2 BvL 7/71 *(Sozialarbeiter)* = BVerfGE 33, 367.

[91] Ebd., (379).

[92] BVerfG, Beschluss vom 24.5.1977, 2 BvR 988/75 *(Beratungsstelle)* = BVerfGE 44, 353.

[93] Ebd., (375 ff.)

dungen das Risiko enttäuschter Vertraulichkeitserwartungen und dadurch bedingter Sekundäreffekte ab, ohne dass dies jedoch in der gleichen umfassenden Weise wie beispielsweise in der zeitlich späteren Rechtsprechung des EGMR[94] ausgearbeitet wird.

Ein etwas anders gelagertes, gleichwohl in diesen Zusammenhang fallendes Risiko wird in der Entscheidung des BVerfG vom 31.1.1973 zur Verwertung heimlich erstellter Tonbandaufnahmen deutlich.[95] Dort entwickelt das Gericht den Schutz der „Unbefangenheit der menschlichen Kommunikation" durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Diese würde erheblich geschmälert, sofern jeder mit dem Bewusstsein leben müsste, „daß jedes seiner Worte, eine vielleicht unbedachte oder unbeherrschte Äußerung, eine bloß vorläufige Stellungnahme im Rahmen eines sich entfaltenden Gesprächs oder eine nur aus einer besonderen Situation heraus verständliche Formulierung bei anderer Gelegenheit und in anderem Zusammenhang hervorgeholt werden könnte, um mit ihrem Inhalt, Ausdruck oder Klang gegen ihn zu zeugen".[96]

Hier wird also das in den vorangegangenen Entscheidungen ausgearbeitete Risiko der Funktionsauswirkungen enttäuschter Vertraulichkeitserwartungen abstrahiert und auf individuelle Handlungsauswirkungen durch Publizitätserwartungen übertragen. Diese Entscheidung bildet die Grundlage für die weitere Ausdifferenzierung dieser Abstraktion im sogleich zu prüfenden Volkszählungsurteil.

### 3. Volkszählungsurteil

Der größte Schritt in der Verselbstständigung des verfassungsrechtlichen Datenschutzes erfolgte mit dem Volkszählungsurteil.[97] Die Verfassungsbeschwerde richtete sich – im Fahrwasser einer starken Protestbewegung – gegen das „Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung" vom 25.2.1982.[98] Gleich zu Beginn des Urteils wird das Ausmaß der öffentlichen Betroffenheit beschrieben: So habe die durch das Volkszählungsgesetz ausgelöste Datenerhebung „Beunruhigung auch in solchen Teilen der Bevölkerung ausgelöst, die als loyale Staatsbürger das Recht und die Pflicht des Staates respektieren, die für rationales und planvolles staatliches Handeln erforderlichen Informationen zu beschaffen".[99]

---

[94] Siehe oben Teil 1, IV.B.5. und 6.

[95] BVerfG, Beschluss vom 31.1.1973, 2 BvR 454/71 *(Tonbandaufnahme)* = BVerfGE 34, 238.

[96] Ebd., (246 f.).

[97] BVerfG, Beschluss vom 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83 *(Volkszählung)* = BVerfGE 65, 1.

[98] BGBl. 1983 I S. 369.

[99] BVerfGE 65, 1 (3).

Die Entscheidung wird von vielen als eine der wichtigsten und folgenreichsten des BVerfG angesehen.[100]

### *a) Selbstbestimmung und Informationsemergenz*

Eine maßgebliche Risikokonzeption wird bereits zu Beginn des Urteils herausgestellt: die Furcht vor unkontrollierbarer Persönlichkeitserfassung als zentralem Risiko moderner Datenverarbeitung.[101] Die Beschwerdeführer beriefen sich auf ein aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG folgendes Gebot der Anonymität. Ohne dieses mache eine Befragung den Einzelnen „für beliebige fremdbestimmte Zwecke" verfügbar und beraube ihn der freien Selbstbestimmung, womit er zum „Gegenstand fremder Willensausübung und Kontrolle" werde.[102] Die gewandelten technologischen Bedingungen ermöglichten die Erstellung eines als umfassendes und detailliertes Bild der Person zu verstehenden Persönlichkeitsprofils auch im Intimbereich. Dadurch werde der Bürger zum „gläsernen Menschen".[103] Das Gericht zieht sodann – wie schon in der *Mikrozensus*-Entscheidung[104] – Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG als Prüfungsmaßstab heran und begründet die Offenheit für weitere Konkretisierungen des Allgemeinen Persönlichkeitsrechts mit Verweis auf „moderne Entwicklungen" und „neue Gefährdungen".[105] Im Anschluss greift es das von den Beschwerdeführern eingebrachte Schutzgut der Selbstbestimmung auf: Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfasse auch die „aus dem Gedanken des Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden".[106] Das BVerfG greift damit die auf *Josef Kohler* zurückgehende Selbstbestimmungskonzeption[107] auf und ergänzt sie sodann um den Aspekt des technischen Wandels, wie dies bereits *Warren/Brandeis*[108] taten: Die Befugnis bedürfe „unter den heutigen und künftigen Bedingungen automatischer Datenverarbeitung in besonderem Maße des Schutzes".[109] Zur Begründung verweist das Gericht auf zwei Eigenschaften des technischen Wandels: erstens die unbegrenzte Speicher- und Abrufbarkeit personenbezogener Daten sowie zweitens deren Kom-

---

[100] *Menzel/Müller-Terpitz* (Hrsg.), Verfassungsrechtsprechung, S. 366.

[101] BVerfGE 65, 1 (4).

[102] Ebd., (16 f).

[103] Ebd., (17).

[104] Siehe oben II.B.1.

[105] BVerfGE 65, 1 (41).

[106] Ebd., (42).

[107] Siehe oben, Einleitung I. Die Anbindung an das Schutzgut „Selbtbestimmung" wird auch im zivilrechtlichen Persönlichkeitsrecht nachvollzogen, vgl. BGHZ 13, 334 (338 f.) sowie *Enders*, Persönlichkeit, S. 174.

[108] Siehe oben Einleitung, I.

[109] BVerfGE 65, 1 (42).

binationsmöglichkeit. Hier greift das Gericht also zunächst das bereits bekannte Risiko der Informationspermanenz (unbegrenzte Speicherung und zeitlich unbegrenzte Abrufbarkeit) auf. Fraglich ist, ob sich die angeführten Kombinationsmöglichkeiten dem oben näher herausgearbeiteten Risiko der Informationsemergenz[110] zuordnen lassen. Eindeutig folgt dies aus der zitierten Urteilspassage nicht. Dagegen spricht, dass sich das Gericht im Anschluss nur auf die fehlende Kontrollierbarkeit von Richtigkeit und Verwendung der Daten bezieht. Andererseits ist jedoch gerade der Effekt eines überschießenden Erkenntnisgewinns in besonderer Weise geeignet, die oben referierten „Ängste" der Beschwerdeführer auszulösen.

Ferner bezieht sich das Gericht auf „bisher unbekannte Möglichkeiten einer Einsicht- und Einflussnahme".[111] Gerade die genuine Neuschöpfung von Informationen durch automatisierte Auswertung bestehender Bestände kann eine solche – bis dahin unbekannte Möglichkeit darstellen. Freilich gab es bereits zuvor die Chance auf Erkenntnisgewinn durch Auswertung von Informationen. Automatisierte Datenverarbeitung ist damit verglichen jedoch quantitativ und qualitativ andersartig, denn es ist keine der Erkenntniserlangung über die Person unmittelbar vorgeschaltete menschliche Denkoperation mehr nötig. Es fehlt insoweit an der bei menschlichen Denkprozessen – zumindest typischerweise – unbewussten Kontextmitberücksichtigung sowie an der Kritikfähigkeit und Verantwortlichkeit des menschlichen „Informationsschöpfers". Allerdings geht auch die automatisierte oder, wie man heute besser sagen würde, „informationstechnische" Datenverarbeitung auf menschliche Denkprozesse zurück: Es sind diejenigen des Programmierers. Doch sind dem Programmierer durch das Erfordernis der Formalisierung und die Antizipation von Problemen, Fragestellungen und Entscheidungen stärkere Grenzen gesetzt, als dies bei einem (kompetenten), nicht ausschließlich an informationstechnischen Entscheidungen orientierten Menschen der Fall ist. Insbesondere erweist sich der Programmierer als weniger „greifbar" und entfernter als ein unmittelbar vor der Informationsverarbeitung vorgeschalteter „menschlicher Datenverarbeiter". Dies dürfte die besondere Furcht erklären, die aus der stärkeren Entfernung des „Faktors Mensch" von der jeweiligen Entscheidung folgt.[112] So gesehen lässt sich der Verweis des Verfassungsgerichts auf die Kombinationsmöglichkeiten durchaus dem Risiko der Informationsemergenz zuordnen.

---

[110] Siehe oben Teil 1, II.A.2.d).

[111] BVerfGE 65, 1 (42).

[112] In die richtige Richtung gehen deshalb die Überlegungen des amerikanischen Verfassungsrechtlers *Lawrence Lessig*, der in einem berühmten Aufsatz die Aussage „code is law" prägte. *Lessig* meint damit die Verlagerung des freiheitsbedrohenden Potenzials von Regelungsmacht vom Gesetzgeber auf den Programmierer, vgl. http://harvardmagazine.com/2000/01/code-is-law-html [Stand: 28.3.2014]; vgl. auch *Lessig*, Code.

### *b) Konformismusrisiko*

Ein weiterer Begründungsstrang der Selbstbestimmungskonzeption der Volkszählungsentscheidung sind die vermuteten Auswirkungen öffentlicher Anteilnahme, die ihre Grundlage bereits in der Entscheidung zur Mithöreinrichtung finden.[113] Die Publizität wirke sich auf die Verhaltensfreiheit des Individuums in der Form eines „psychischen Drucks" aus. Dem Einzelnen müsse demgegenüber „auch unter den Bedingungen moderner Informationsverarbeitungstechnologien" Entscheidungsfreiheit verbleiben und zwar über „vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit […], sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten".[114] Dieser Vorstellung zufolge wirkt sich Unsicherheit über das Bekanntsein von Informationen in bestimmten Bereichen der „sozialen Umwelt" freiheitshemmend aus, da der Einzelne das Wissen seiner Kommunikationspartner nicht abschätzen kann.[115] Sodann wechselt das Gericht die Perspektive von der individuellen zu einer gesamtgesellschaftlichen Betrachtungsweise. Eine Gesellschaftsordnung, „in der die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß", sei mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.[116] Darauf folgt eine tragende Aussage, deren Prämisse, soweit ersichtlich, bisher nicht hinterfragt wurde:

> „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."[117]

Als Beispiel führt das Gericht die Teilnahme an einer „Versammlung oder einer Bürgerinitiative" an. Wer damit rechne, dass die Teilnahme „behördlich registriert" wird und dass ihm dadurch „Risiken entstehen könnten", verzichte womöglich auf die Ausübung seiner Grundrechte aus Art. 8 und Art. 9 GG.

Die Überzeugungskraft dieses Arguments hängt unmittelbar von dem staatlichen Selbstverständnis und der Einschätzung des Staates durch die Bürger ab. In einem autoritären Staat sind die geäußerten Befürchtungen nachvollziehbar und die Auswirkungen auf die Verhaltensfreiheit unmittelbar einsichtig. In einem liberalen Rechtsstaat wie der Bundesrepublik Deutschland erscheinen derartige Befürchtungen hingegen aufgrund der verfassungsrechtlichen Garantien des Grundgesetzes zunächst überzogen und wenig plausibel. Auch wenn seit den Aufdeckungen von *Edward Snowden* im Frühsommer 2013 Befürchtungen hinsichtlich der Überwachungstätigkeit in großem Ausmaß als begründet erscheinen mögen, fehlen in einem Rechtsstaat jedoch die zu erwartenden Repressalien, die an eine Registrierung anknüpfen. Erst bei deren Existenz wären Verhaltensänderungen zu erwarten.

---

113 Siehe oben I.A.

114 BVerfGE 65, 1 (42 f.).

115 Ebd., (43).

116 Ebd.

117 Ebd.

Von dieser Überlegung sind jedoch zwei Ausnahmen zu machen: Die mutmaßlichen Verhaltensauswirkungen sind zum einen dann zu erwarten, wenn den Bürgern das Vertrauen in die freiheitliche Grundordnung fehlt, auch wenn diese in Wirklichkeit gegeben ist und praktische Wirksamkeit entfaltet, d.h. wenn also tatsächlich auf die freiheitliche Grundordnung vertraut werden könnte. In diesem Fall würde das Recht also darauf abzielen, die Folgen irrationaler Ängste zu begrenzen. Für das Demonstrationsbeispiel heißt dies, dass die Demonstranten befürchten, durch ihre Teilnahme staatlichen Repressionen ausgesetzt zu werden, obwohl dies de facto nicht zu erwarten steht. Das Beispiel zeigt, dass auch dieser Argumentation nur wenig Überzeugungskraft zukommt, da einerseits die Aufklärung der Bürger (z.B. durch „vertrauensbildende Maßnahmen" und „Staatsbürgerkunde") naheliegendere Abhilfe zu bringen scheint. Andererseits liegt – zumindest in der heutigen, von keiner Diktatur geprägten Gesellschaft – die Angst vor staatlichen Repressionen nicht mehr ohne Weiteres auf der Hand und wäre jedenfalls zunächst empirisch zu belegen. Jedoch gibt es noch eine zweite Interpretation der Argumentation des Gerichts: Das BVerfG spricht nur von Risiken als Konsequenz behördlicher Registrierung. Nicht ausgeschlossen ist, dass unter den negativen Folgen nicht nur staatliche Repression, sondern allgemein alle nachteiligen Auswirkungen der behördlichen Verarbeitung zu fassen sind, auch wenn die Folgen erst durch Private hervorgerufen werden. Soziale Ausgrenzung und Diskriminierung sind Risiken, die sich – wie oben untersucht[118] – auch an anderen Datenschutzregelungen festmachen lassen und höchst naheliegend erscheinen.

Andererseits jedoch spricht das BVerfG nur von „behördlicher" Registrierung. Notwendiger Zwischenschritt zu einer derartigen Interpretation der Argumentation wäre also die Weitergabe staatlich erhobener Daten an Private. Diese erscheint – eingedenk der erst kürzlich wieder aufgebrochenen Diskussion um die Verwendung von Meldedaten durch Private[119] – durchaus plausibel. Auch führt das BVerfG die privaten Risiken an einer späteren Stelle – im Rahmen der Prüfung besonderer Anforderungen bei statistischer Erhebung – explizit an: Der Gesetzgeber müsse bei der Anordnung einer Auskunftspflicht prüfen, ob sie „insbesondere für den Betroffenen die Gefahr der sozialen Abstempelung (etwa als Drogensüchtiger, Vorbestrafter, Geisteskranker, Asozialer)" hervorrufe.[120] Bei beiden Interpretationen der Argumentation des BVerfG (irrationale Ängste/weites Folgenverständnis) bleiben jedoch zusätzlich die unterstellten tatsächlichen Verhaltensauswirkungen empirisch zu hinterfragen. Gerade in politischen Entscheidungen muss nicht jedes erwartete Risiko – etwa finanzielle Einbußen – zu einer Anpassungshandlung führen. Unberücksichtigt bleiben dabei insbesondere andere nahe-

---

118 Siehe oben Teil 1, II.A.2.d) sowie C.

119 http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/neues-meldegesetz-erst-durchgewinkt-dann-durchgefallen-11825532.html [Stand: 28.3.2014].

120 BVerfGE 65, 1 (48).

liegende Verhaltensweisen, die beispielsweise durch an ideellen Werten orientierte Entscheidungen in Wahlen, Abstimmungen oder sonstigen politischen Willensäußerungen motiviert sind. Denkbar ist auch, dass politische Handlungen – als eine Art Trotzreaktion – gerade als Symbol der Missbilligung und Nichtidentifikation mit erwarteten Sanktionen vorgenommen werden.

Die Argumentation mit konformitätsbildender Verhaltensauswirkung von Informationsverarbeitung überträgt das Gericht sodann wieder von der individuellen auf die gesellschaftliche Ebene: Betroffen seien nicht nur individuelle Entfaltungschancen, sondern auch das Gemeinwohl, da Selbstbestimmung eine „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich-demokratischen Gemeinwesens" sei. Das Gericht folgert hieraus, dass die freie Entfaltung der Persönlichkeit unter den Bedingungen moderner Datenverarbeitung Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der persönlicher Daten erfordere, und leitet diesen in Form der „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen", aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ab.[121]

### *c) Verwendungszweck als „Gradmesser"*

Das bei anderen Datenschutzinstrumenten eigenständig aufgegriffene Risiko der Entkontextualisierung lässt sich in den Entscheidungsgründen nicht unmittelbar identifizieren, obwohl der Verwendungszweck in einer tragenden Passage ausgiebig aufgegriffen wird. Er dient jedoch nur als „Gradmesser" für die Anforderungen an die Rechtfertigung bei zwangsweiser Informationserhebung: Dem Verwendungszusammenhang komme – neben den Verarbeitungs- und Verknüpfungsmöglichkeiten – eine entscheidende Rolle zu. Die Sensibilität von Informationen hänge nicht allein davon ab, ob intime Vorgänge betroffen seien; vielmehr sei es zur Feststellung der persönlichkeitsrechtlichen Bedeutung nötig, den Verwendungszusammenhang zu kennen. Insoweit gebe es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses Datum' mehr".[122] Zwangsweise Erhebungen seien nicht vereinbar mit dem Recht auf informationelle Selbstbestimmung, wenn sie „auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" erfolgten. Der Zweck müsse vielmehr bereichsspezifisch und präzise bestimmt werden, die Angaben hierfür geeignet und erforderlich sein.[123] Das Gericht greift hier jedoch nicht – wie es zunächst scheint – den Begründungsstrang der Furcht vor intransparenter Verarbeitung und auch nicht das Risiko der Entkontextualisierung auf, sondern will die Unmöglichkeit der Festlegung von Rechtfertigungsmaßstäben bei Unkenntnis des konkreten Verwendungszwecks feststellen:

---

[121] Ebd., (43).

[122] Ebd., (45).

[123] Ebd., (46).

„Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten."[124]

Bei der Konkretisierung der Anforderungen an statistische Erhebungen sieht das Gericht jedoch das Problem, dass es in der Natur von Statistiken liegt, dass die Verwendungszwecke dort nicht im Voraus bestimmbar sind. Stattdessen seien klar definierte Verarbeitungsvoraussetzungen zu schaffen, um zu verhindern, dass „der Einzelne unter den Bedingungen einer automatischen Erhebung und Verarbeitung der seine Person betreffenden Angaben nicht zum bloßen Informationsobjekt wird". Die Gefahr bestehe in einer „persönlichkeitsfeindlichen Registrierung und Katalogisierung".[125] Hier greift das Gericht also das bereits in der *Mikrozensus*-Entscheidung herausgearbeitete und auch von den Beschwerdeführern bezeichnete Risiko einer „verwaltungstechnischen Entpersönlichung" auf und verweist im Anschluss auch ausdrücklich auf das Schutzgut der Menschenwürde, wobei es davon ausgeht, dass die Erstellung bestimmter Teil- oder Gesamtabbilder der Persönlichkeit mit der Würde des Menschen unvereinbar ist.[126] Das Risiko informationeller Machtverschiebungen greift das Gericht dagegen nur knapp auf, wenn es die Trennung der Kommunalstatistik von anderen Gemeindeaufgaben als unerlässliche „informationelle Gewaltenteilung" auffasst.[127]

### *d) Funktionale Aspekte des Vertrauens*

Im Rahmen des „Besonderen Teils" der Ausführungen zu Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG – also bei den besonderen Anforderungen an Statistiken – bezieht sich das Gericht auf das Schutzgut des Vertrauens in seiner funktionalen Dimension, wie dies bereits in den oben geprüften Datenschutzinstrumenten[128] und in Ansätzen auch bei den frühen Entscheidungen des BVerfG[129] zu finden ist: Für die Funktionsfähigkeit der amtlichen Statistik sei ein möglichst hoher Grad an Genauigkeit und Wahrheitsgehalt der erhobenen Daten notwendig. Dieses Ziel könne nur erreicht werden, wenn der auskunftspflichtige Bürger das notwendige Vertrauen in die „Abschottung" seiner für statistische Zwecke erhobenen Daten hat. Andernfalls fehle es an der Bereitschaft, wahrheitsgemäße Angaben zu machen.[130] Auch hier greift das Gericht also die bereits oben in den frühen Entscheidungen zu Vertrau-

---

124 Ebd., (45).

125 Ebd., (48).

126 Ebd., (52 ff.).

127 Ebd., (69).

128 Siehe oben Teil 1, IV.B.5. und 6.

129 Siehe oben II.B.2.

130 BVerfGE 65, 1 (50) (unter Verweis auf die Begründung der Bundesregierung zum Entwurf des Volkszählungsgesetzes).

lichkeitskonzeptionen[131] dargestellten funktionalen Aspekte auf. Von dem Schutzgut „Vertraulichkeitserwartung" spricht das Gericht an dieser Stelle jedoch nicht.

*e) Fortbildung der Konzeption, insbesondere Einschüchterungseffekte*

In neueren Entscheidungen wurden die oben dargestellten Risikokonzeptionen und Schutzgüter des Volkszählungsurteils vielfach aufgegriffen und bestätigt. So übernimmt z.B. der Beschluss zur *Rasterfahndung* vom 4.4.2006[132] die Abschnitte zur Selbstbestimmungskonzeption wörtlich.[133] In anderen Entscheidungen weicht die Terminologie zwar ab, in der Sache werden jedoch die gleichen Risiken angesprochen. So ist im Beschluss zur *Rasterfahndung* vom 5.7.1995[134] von „Verhaltensanpassungen" und „Kommunikationsstörungen" die Rede.[135] Exemplarisch für die Fortführung der Risikokonzeptionen ist auch der Beschluss zur *Beschlagnahme von Anwaltsdatenträgern* vom 12.4.2005.[136] Ausdrücklich bezieht sich das Gericht dort auf das Konformismusrisiko, wenn es ausführt, dass das Grundrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG auch vor einem „Einschüchterungseffekt" schützt, der „entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen" kann, und sich dabei auf das Schutzgut der Selbstbestimmung und dessen mögliche Hemmung bezieht: „Fremdes Geheimwissen" müsse nicht nur im Interesse des Betroffenen vermieden werden, es beeinträchtige auch das Gemeinwohl, „weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens" sei.[137]

Im Anschluss knüpft es ebenso wie im Volkszählungsurteil an die funktionalen Aspekte des Vertrauens an, jedoch bezogen auf die „freie Advokatur": Die Sicherstellung und Beschlagnahme von Anwaltsdaten greife in das Grundrecht der Mandanten auf informationelle Selbstbestimmung ein und beeinträchtige damit auch Belange der Allgemeinheit. Die Mandanten würden an einer offenen, rückhaltlosen und vertrauensvollen Kommunikation mit ihren Verteidigern gehindert oder gar von der Mandatierung abgehalten. Die damit einhergehende Beeinträchtigung des Vertrauensverhältnisses zwischen Mandant und für sie tätig werdenden Berufsträgern laufe der fundamentalen, objektiven Bedeutung der freien Advokatur ent-

---

131 Siehe oben II.B.2.

132 BVerfG Beschluss vom 4.4.2006, 1 BvR 518/02 *(Rasterfahndung II)* = BVerfGE 115, 320.

133 Ebd., (342).

134 BVerfG Beschluss vom 5.7.1995, 1 BvR 2226/94 *(Rasterfahndung I)* = BVerfGE 93, 181.

135 Ebd., (188 f., 192 f.).

136 BVerfG Beschluss vom 12.4.2005, 2 BvR 1027/02 *(Anwaltsdaten)* = BVerfGE 113, 29.

137 Ebd., (46).

gegen.[138] Der maßgebliche „Einschüchterungseffekt“ und die abschreckende Wirkung „fremden Geheimwissens“ mit ihren nachteiligen Folgen für das Gemeinwesen werden in jüngeren Entscheidungen immer wieder thematisiert.[139] Auch das oben analysierte Risiko der Informationsemergenz wird in späteren Entscheidungen aufgegriffen, so etwa in der Entscheidung zur *Rasterfahndung* vom 4.4.2006: Das Zusammenführen und der Abgleich der erhobenen Daten öffentlicher und privater Einrichtungen ermöglichten die Gewinnung vielfältiger neuer Informationen.[140]

### *f) Zwischenergebnis*

Das Verfassungsgericht hat im Volkszählungsurteil die älteren Selbstbestimmungskonzeptionen mit Ideen von *Kohler* sowie *Warren/Brandeis* kombiniert und daraus das Schutzgut des Grundrechts auf Informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, konstruiert. Die Schutzgutkonzeption basiert auf zwei Aspekten technischen Wandels, die sich den bereits zuvor herausgearbeiteten Risiken von Informationspermanenz und Informationsemergenz zuordnen lassen. Die Anbindung an das Risiko der Informationsemergenz setzte eine Auslegung der vom Verfassungsgericht herangezogenen „Kombinationsmöglichkeiten“ voraus. Die in diesem Rahmen vorgenommene nähere Analyse der Informationsemergenz hat mit ihrem Hinweis auf Formalisierung und begrenzter Problemantizipation im Rahmen von Programmierung an den Befund von *Lessig* erinnert („code is law“).[141] Das spezifische Risiko, das in der Entscheidung nur implizit artikuliert wird, lässt sich damit auch als eine weitere „Entfernung“ der durch Programmierung antizipierten Entscheidung vom Betroffenen verstehen: Grundlage der auch vom Gericht einbezogenen „Angst“ des Einzelnen ist dann die vermutete Fehleranfälligkeit aufgrund im Vergleich mit menschlicher Informationsverarbeitung schwieriger zu implementierender Kontextmitberücksichtigung.

Einen besonderen Stellenwert räumt die Entscheidung dem Risiko der Konformismusförderung ein. Das tragende Beispiel des vorsorglichen Verzichts auf Grundrechtsausübung lässt bei genauerer Analyse zwei mögliche Interpretationen zu: Zum einen können dem Risiko Verhaltensauswirkungen zugrunde liegen, die in irrationalen Ängsten vor staatlicher Repression begründet sind; zum anderen Verhaltensauswirkungen bei negativen Folgen durch die Kenntnisnahme Privater von den durch staatliche Stellen erhobenen Informationen. Beide Möglichkeiten können weiter hinterfragt werden, da die konformistische Verhaltensänderung nicht in allen Fällen ohne Weiteres nachvollziehbar ist.[142]

---

138 Ebd., (47 ff.).

139 BVerfGE 115, 166 (188), BVerfGE 115, 320 (354).

140 BVerfGE 115, 320 (349).

141 Siehe oben II.B.3.b) sowie Teil 1, IV.B.3.

142 Siehe oben II.B.3.b).

Die Ausführungen zur Zweckbindung verweisen nicht wie zunächst zu erwarten auf das Risiko der Entkontextualisierung, sondern dienen lediglich der Anpassung der Rechtfertigungsanforderungen je nach Kontext. In diesem Zusammenhang wird jedoch das Risiko der „verwaltungstechnischen Entpersönlichung" mit seiner Grundlage im Schutzgut der Menschenwürde herangezogen.[143] Das Schutzgut der Vertraulichkeitserwartung wird zwar nicht explizit genannt, dessen funktionale Komponenten werden jedoch im Rahmen der Konkretisierung des Schutzbereichs für statistische Erhebungen aufgegriffen.[144] Neue Entscheidungen ergänzen insbesondere das Konformismusrisiko um einen stärkeren Bezug zur gesamtgesellschaftlichen Ebene und um den Topos „Einschüchterungseffekt".[145] Nur knapp angerissen wird dagegen das Risiko informationeller Machtverschiebungen bei der für unerlässlich gehaltenen „informationellen Gewaltenteilung".[146]

### 4. Informationspermanenz

In der Entscheidung zur *Bekanntmachung einer Entmündigung*[147] wird der Inhalt des Grundrechts auf informationelle Selbstbestimmung jenseits von Zwangserhebungen im Rahmen der Volkszählung konkretisiert: Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sei nicht nur dann betroffen, wenn der Staat vom Einzelnen die Bekanntgabe von Daten verlange oder wenn es sich um automatische Datenverarbeitung handele; vielmehr schütze das Recht generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten.[148] Im Rahmen der Verhältnismäßigkeitsprüfung greift das BVerfG zunächst auf das Risiko der Diskriminierung („soziale Abstempelung") und negativer Auswirkungen auf den Resozialisierungszweck zurück, um den Verstoß gegen die Verhältnismäßigkeit im engeren Sinne zu begründen. Dabei wird dann aber mit dem Erschwernis der Löschung nach öffentlicher Bekanntgabe das Risiko der Informationspermanenz an prominenter Stelle angeführt.[149] Diesem kam freilich zur damaligen Zeit, also vor Existenz des Internets, noch nicht die heutige Bedeutung zu. Deutlicher tritt dieses Risiko dann aber in der *Bargatzky*-Entscheidung[150] hervor: Mit der Nutzung digitaler Übertragungsgeräte habe Telekommunikation an „Flüchtigkeit" verloren und hinterlasse „beständige Spuren".[151]

---

143 Siehe oben II.B.3.c).

144 Siehe oben II.B.3.d).

145 Siehe oben II.B.3.e).

146 Siehe oben II.B.3.f).

147 BVerfG Beschluss vom 9.3.1988, 1 BvL 49/86 *(Entmündigungsbekanntgabe)* = BVerfGE 78, 77.

148 Ebd., (84).

149 Ebd., (87).

150 BVerfG Urteil vom 2.3.2006, 2 BvR 2099/04 *(Bargatzky)* = BVerfGE 115, 166.

151 Ebd., (189).

### 5. Gesamtgesellschaftliche Perspektive zur Verhaltensanpassung

Das Risiko von Verhaltensanpassungen aufgrund befürchteter Überwachungsnachteile, wie dies bereits in der Volkszählungsentscheidung aufgegriffen wird,[152] erhält im *zweiten Urteil des BVerfG zum G-10-Gesetz*[153] eine noch stärkere Anbindung an die gesamtgesellschaftliche Ebene. Zwar prüft das Verfassungsgericht die Befugnisse zur strategischen Fernmeldeaufklärung am Maßstab des Art. 10 Abs. 1 GG, gibt diesem jedoch weitgehend den gleichen Inhalt wie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[154] Damit geht eine erhebliche Erweiterung des Eingriffsbegriffs einher: Selbstständige Eingriffe liegen schon in jeder Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten durch den Staat, unter Ausschluss solcher Daten, die „technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden".[155] Darüber hinaus sollen auch Abgleiche und „Selektionsakte" eigenständige Informationseingriffe darstellen.[156] Bei der Prüfung der Verhältnismäßigkeit von § 1 Abs. 1, § 3 Abs. 1 G 10 a.F., die die Befugnis zur Erfassung, Aufzeichnung, Speicherung und den Abgleich der Informationen enthielten, bezieht sich das Gericht im Rahmen der Prüfung der Eingriffsintensität auf Nachteile, die den Grundrechtsträgern aufgrund der Überwachungsmaßnahme drohen „oder von ihnen nicht ohne Grund befürchtet werden".[157] Derartige objektiv zu erwartende oder subjektiv befürchtete Nachteile können „schon mit der Kenntnisnahme" eintreten. Die Befürchtung selbst könne bereits im Vorfeld zu einer „Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen" führen. Als Beispiel führt das Gericht die Vermeidung bestimmter Gesprächsinhalte oder Termini an.[158] Ein solches spezifisches Risiko kann auch in der Überführung von Daten in einen anderen Verwendungszusammenhang liegen, wenn dies zur Einleitung eines Ermittlungsverfahrens führt.[159] Neben diesem individuellen Anknüpfungspunkt unterstreicht das Gericht vor allem aber die Auswirkungen auf gesamtgesellschaftlicher Ebene: Die heimliche Überwachung betreffe die Kommunikation der Gesellschaft insgesamt. Dem Recht auf informationelle Selbstbestimmung sei gerade deshalb ein „über das Individualinteresse hinausgehender Gemeinwohlbezug" zuerkannt worden.[160] „Schwerekriterien" sieht das Gericht in der Anlasslosigkeit,

---

[152] Siehe oben II.B.3.b).

[153] BVerfG, Urteil vom 14.7.1999, 1 BvR 2226/94, 2420, 2437/95 *(G-10-Gesetz 2)* = BVerfGE 100, 313.

[154] Ebd., (359).

[155] Ebd., (366).

[156] Ebd., (367).

[157] Ebd., (376).

[158] Ebd., (381).

[159] Ebd., (360, 391 f.).

[160] Ebd., (381).

in der Nicht-Unterscheidung verschiedener Inhalte, der voll umfänglichen Erfassung und der Streubreite des Eingriffs.[161] Gerade letzteres Kriterium wurde bereits oben im Rahmen der RL 95/46/EG[162] untersucht und wirft besondere Rechtfertigungsprobleme auf; es wird in der Entscheidung jedoch nicht näher erläutert. Eine räumliche Eingrenzung der Überwachungsmaßnahmen soll die Eingriffsintensität verringern, war jedoch angesichts der im Vergleich zum *ersten G-10-Urteil*[163] geänderten Rechtslage nicht mehr gegeben.[164] Diese räumliche Eingrenzung der Überwachung war wohl zumindest mitursächlich für die im *ersten G-10-Urteil* weitgehende Ausblendung der gesamtgesellschaftlichen Perspektive.[165] Die dort geprüften Maßnahmen bezogen sich auf Kommunikation mit Stellen im Gebiet des Warschauer Pakts, während die im *zweiten G-10-Urteil* geprüften Befugnisse zur strategischen Fernmeldeaufklärung regional nicht eingegrenzte Risiken, wie den internationalen Terrorismus, zum Gegenstand hatten.

### 6. Selbstdarstellung und Publizitätsschäden

In enger Verbindung zum Schutzgut „Selbstbestimmung" steht die Selbstdarstellung. Diese wird bereits seit den oben beschriebenen historischen Wurzeln des zivilrechtlichen Allgemeinen Persönlichkeitsrechts gegen verletzende Medienberichterstattung vorgebracht.[166] Der Einzelne soll mittels des Selbstdarstellungsrechts vor Bloßstellung und Diskreditierung des gesellschaftlichen Ansehens durch mediale Berichterstattung geschützt werden. Die Risiken von Fremdzuschreibungen sind in einer Vielzahl zivilrechtlicher und verfassungsrechtlicher Entscheidungen ausdifferenziert worden – es handelt sich dabei jedoch um zivilrechtliche Fragen des Persönlichkeitsschutzes gegenüber Privaten.[167] Diese Entscheidungen werden nicht umfassend einbezogen, da die entsprechenden Risikokonzeptionen und Schutzgüter im Grundrecht auf informationelle Selbstbestimmung eine spezifisch datenschutzrechtliche Konkretisierung und Weiterentwicklung erfahren haben und darin zum größten Teil aufgehen. Selbst die Fragen der Geltung gegenüber Privaten und bei staatlichem Zugriff auf private Daten werden unter diesem Topos

---

161 Ebd., (380, 392).

162 Siehe oben Teil 2, III.A.2.b).

163 BVerfG Beschl. vom 20.6.1984, 1 BvR 1494/78 *(G-10-Gesetz 1)* = BVerfGE 67, 154.

164 BVerfGE 100, 313 (378).

165 Vgl. BVerfGE 67, 157 (174). Darauf nicht zurückzuführen ist allerdings die ansonsten bemerkenswert unkritische Haltung hinsichtlich betroffener Risiken, insbesondere BVerfGE 67, 157 (179), wo das „gelegentliche Lesen" von Briefen, das „Abhören und Mitschneiden von Ferngesprächen" als „Grundrechtseingriff von geringerer Intensität" bezeichnet wird.

166 Siehe oben, Einleitung I.

167 Zur Rechtsprechung im Einzelnen vgl. *Enders*, Persönlichkeit, S. 177 ff.

aufgegriffen.[168] Gleichwohl ist die *Caroline*-Entscheidung des BVerfG[169] aufgrund der dortigen Ausdifferenzierung des Schutzguts Selbstdarstellung und des Privatsphärenschutzes in die Untersuchung exemplarisch einzubeziehen und näher zu analysieren.

### *a) Caroline-Entscheidung*

Die Verfassungsbeschwerde betraf die Veröffentlichung verschiedener Fotografien, welche die im Ausgangsverfahren vor dem BGH als „absolute Person der Zeitgeschichte" eingestufte prominente Beschwerdeführerin (*Caroline von Monacco*) im Alltags- und Privatleben zeigten. Aufgrund der Einordnung als absolute Person der Zeitgeschichte wurde ihr ein auf §§ 823 Abs. 2 BGB, 22, 23 Abs. 2 KUG i.V.m. § 1004 BGB (analog) gestützter Unterlassungsanspruch verwehrt, soweit sie sich nicht an einem abgeschiedenen Ort aufgehalten hatte und in einem typisch privaten Charakter abgebildet wurde.

Das BVerfG hat im Rahmen der gem. § 23 Abs. 2 KUG vorzunehmenden Güterabwägung Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG im Vergleich zum BGH weiter ausgelegt und sich dabei auch mit betroffenen Risiken und Schutzgütern auseinandergesetzt. Das Verfassungsgericht prüft die Veröffentlichungsbefugnis anhand des Rechts am eigenen Bild *und* der Garantie der Privatsphäre als Konkretisierung des Allgemeinen Persönlichkeitsrechts. Ein allgemeines und umfassendes Verfügungsrecht über die Darstellung der eigenen Person folge daraus jedoch nicht. Unter Berufung auf ältere persönlichkeitsrechtliche Rechtsprechung wird ein Recht des Einzelnen „so von anderen dargestellt zu werden, wie er sich selber sieht oder gesehen werden möchte" abgelehnt.[170] Das Schutzbedürfnis folge aus der Möglichkeit, das „Erscheinungsbild eines Menschen in einer bestimmten Situation von diesem abzulösen und datenmäßig zu fixieren und jederzeit vor einem unüberschaubaren Personenkreis zu reproduzieren". Hierdurch könnten die „Formen der Öffentlichkeit", in denen der Einzelne erscheint, geändert werden.[171]

An diese Ausführungen, die zunächst auf dem Risiko der Informationspermanenz aufbauen, folgt die Einbeziehung des Entkontextualisierungsrisikos: Mit dem Wechsel des Kontextes ändere sich bewusst oder unbewusst auch der Sinngehalt der Bildaussage. Der Schutz ziele demnach „vor allem" auf Verfälschungen durch Kontextveränderung.[172]

---

168 Siehe oben Teil 2, II.B.2.c) und d).

169 BVerfG Urteil vom 15.12.1999, 1 BvR 653/96 *(Caroline)* = BVerfGE 101, 361.

170 Ebd., (380).

171 Ebd., (381).

172 Ebd., (382).

Die Ausführungen gehen jedoch über das Risiko der Entkontextualisierung im bereits eingegrenzten Sinne hinaus: Im Anschluss an die Passage werden die Ausführungen zum Recht am eigenen Bild zwar nicht weitergeführt, stattdessen widmet sich die Entscheidung jedoch der Privatsphäre als davon abzugrenzender Einzelverbürgung. Diese beziehe sich nicht speziell auf Abbildungen, sondern sei thematisch und räumlich bestimmt.[173] Umfasst seien Inhalte, die „typischerweise" als privat einzustufen seien, weil ihre öffentliche Erörterung oder Zurschaustellung als „unschicklich" gelte oder als „peinlich" empfunden werde. Bei fehlendem Schutz würden eine Reihe grundrechtlich geschützter Verhaltensweisen beeinträchtigt oder unmöglich gemacht, so die „Auseinandersetzung mit sich selbst", die „unbefangene Kommunikation unter Nahestehenden", die „sexuelle Entfaltung" und die „Inanspruchnahme ärztlicher Hilfe".[174] Neben dieser thematischen Eingrenzung erstrecke sich der Schutz auf einen „räumlichen Bereich", in dem der Einzelne „zu sich kommen, sich entspannen oder auch gehen lassen" könne.[175] Der Grund für diesen räumlichen Schutz liege darin, dass der Einzelne „psychisch überfordert" sei, wenn er ständig auf seine Wirkung gegenüber anderen oder die richtige Verhaltensweise achten müsse.[176]

Weiterhin erforderlich bleibt ein räumlicher Anknüpfungspunkt. Das BVerfG lockert diesen Bezug allerdings, indem es das Kriterium der „Abgeschiedenheit" des Rückzugsbereichs nicht „an den Hausmauern oder Grundstücksgrenzen" enden lässt, sondern es auch auf die „natürliche Umgebung" und auf solche Örtlichkeiten erstreckt, die zwar außerhalb des eigenen Hauses liegen, die jedoch „von der breiten Öffentlichkeit deutlich abgeschieden sind".[177] Notwendig bleibe das Kriterium der örtlichen Abgeschiedenheit, da erst darin das Bedürfnis, sich der ständigen Beobachtung zu entziehen und sich der mit Beobachtung einhergehenden Verhaltenskontrolle auszusetzen, der Entspannung und dem „Zu-sich-Kommen" weichen könne.[178] Schutz sei an diesen Orten dann gerade auch vor solchen Aufnahmetechniken geboten, die „die räumliche Abgeschiedenheit überwinden, ohne dass der Betroffene dies bemerken kann". Eine genaue Abgrenzung lasse sich zwar nur situativ vornehmen; nicht erfasst seien aber Plätze, an denen sich viele Menschen befinden. Diese könne der Einzelne auch nicht durch typischerweise privates Verhalten „in seine Privatsphäre umdefinieren".[179]

---

173 Ebd.
174 Ebd.
175 Ebd., (382 f.).
176 Ebd., (383).
177 Ebd., (383 f., 384).
178 Ebd., (394).
179 Ebd., (384).

*b) Zwischenergebnis*

Die *Caroline*-Entscheidung verdeutlicht damit zunächst den nur eingeschränkten Schutz der Selbstdarstellung. Gleichzeitig wird eine ganze Reihe schon untersuchter Risiken aufgegriffen. Dies ist zunächst die Entkontextualisierung, welche zur Konkretisierung des Schutzguts Selbstdarstellung dient. Die Entkontextualisierung wird in der Entscheidung jedoch in einer anderen Weise verstanden, als dies in den oben untersuchten Fällen[180] der Kontextinfiltration und des Kontextdefizits der Fall ist. Das Problem der Pressefotos ist die Änderung der „Form der Öffentlichkeit" und der damit einhergehende veränderte Sinngehalt der Abbildung. Berücksichtigt man die noch differenzierteren Ausführungen zur Privatsphäre, die – obgleich zu einer anderen Einzelverbürgung ergangen – doch argumentativ auf dem vorangehenden Abschnitt der Entscheidung aufbauen, so folgt das Risiko der geänderten Öffentlichkeitsform nicht allein aus dem anderen Stellenwert, der einer Information im Kontext der Medienöffentlichkeit zukommt. Vielmehr sind die unmittelbaren Auswirkungen des Sich-bewusst-Seins einer größeren Öffentlichkeit das spezifische Risiko. Auch insoweit werden also die aus der Volkszählungsentscheidung stammenden Konzeptionen der Verhaltensauswirkungen aufgegriffen. Das BVerfG geht in der *Caroline*-Entscheidung ebenso wie dort auf psychische Folgen und Verhaltensänderungen ein, nicht jedoch auf die Frage, wie die Informationen im Kontext der geänderten Öffentlichkeit verwendet werden. Das hier vom BVerfG aufgegriffene Risiko lässt sich damit der Kategorie „Publizitätsschaden" zuordnen. Für eben diese Kategorie weist das Urteil differenzierte Äußerungen auf, die sich auf psychische Folgen der öffentlichen Anteilnahme zurückführen lassen. Ebenso verweist das Urteil auf das Konformismusrisiko, jedoch ohne eine funktionaldemokratische Anbindung auf unterstellte Verhaltensauswirkungen. Festzuhalten ist auch der – im Rahmen der Einzelverbürgung „Privatsphäre" – weiterhin verbleibende räumliche Bezug, der mit der Ausdehnung auf „abgeschiedene Örtlichkeiten" eine nur zögerliche Ausweitung erfährt.

### 7. Vertraulichkeitserwartung

Die Entscheidung des BVerfG zu *Mithöreinrichtungen*[181] schließt in dogmatischer Hinsicht unmittelbar an die *Caroline*-Entscheidung an, thematisiert jedoch anders als diese explizit den Topos „Vertraulichkeitserwartung", wobei die Erwartung die Funktion eines Schutzguts einnimmt. Daneben betrifft der Beschluss das Verhältnis der Einzelverbürgungen des Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG zueinander. Der Entscheidung liegen zwei Zivilurteile zugrunde, die die Beschwerdeführer in ihrem Recht am gesprochenen Wort, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1

---

[180] Siehe oben Teil 1, II.B.

[181] BVerfG Beschluss vom 9.10.2002, 1 BvR 1611/96, 805/98 *(Mithöreinrichtung)* = BVerfGE 106, 28.

GG, verletzten. Die Zivilgerichte bejahten undifferenziert eine Einwilligung in das Mithören von Telefongesprächen, vernahmen daraufhin die Mithörer und verwerteten deren Aussagen. Das BVerfG lehnt zunächst die Eröffnung des Schutzbereichs von Art. 10 Abs. 1 GG ab, da der Gewährleistungsgehalt lediglich die Vertraulichkeit der Mediennutzung, nicht aber das Vertrauen der Kommunikationspartner zueinander schütze.[182] Zwar ende der Schutz nicht am Endgerät, erfasst seien beispielsweise Abhöreinrichtungen; keine Beeinträchtigung liege jedoch vor, wenn der Gesprächspartner einem privaten Dritten den Zugriff auf die Einrichtung gestatte. Es realisiere sich dann nicht die von Art. 10 Abs. 1 GG vorausgesetzte spezifische Gefährdungslage.[183]

Sodann prüft das BVerfG Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG. Hierbei bezieht es sich zunächst auf das Schutzgut der Selbstbestimmung, das nicht nur als Befugnis zur Entscheidung über die „Verdinglichung" der Sprache durch Aufnahmen verstanden wird, sondern sich auch gegen die heimliche Einbeziehung Dritter als Zuhörer richte.[184] Das Medium „Sprache" ist damit ausreichender, rein formeller Anknüpfungspunkt für die Eröffnung des Schutzes. Es komme nicht darauf an, ob es sich bei den ausgetauschten Informationen um personale Kommunikationsinhalte oder persönlichkeitssensible Daten handelt oder ob das Gespräch vertraulich war.[185] Das Gericht setzt hier also eine allein durch das formale Kriterium der „flüchtigen" Sprache ausgelöste Vertraulichkeitserwartung voraus. Vom Recht am eigenen Wort unterscheidet es den im Anschluss geprüften Schutz der Privatsphäre, der erst durch den Inhalt des Gesprächs ausgelöst werde. Hier sei der Schutz unabhängig davon, wie der Inhalt an den Gesprächspartner gelange. Die Privatsphäre sei auch dann betroffen, wenn der Gesprächspartner entgegen einer Vertraulichkeitserwartung des Sprechers einen Dritten über den Gesprächsinhalt in Kenntnis setze.[186] Hier wird also die Vertraulichkeitserwartung als eigenständiges Schutzgut betrachtet. Sie muss in diesen Fällen aus einem anderen objektiven Anknüpfungspunkt folgen. Hinsichtlich des Rechts am gesprochenen Wort argumentiert das BVerfG sodann wieder mit den negativen Auswirkungen des fehlenden Schutzes, im konkreten Fall aufgrund des zu erwartenden Verlusts an Unbefangenheit der mündlichen Kommunikation.[187] Weiterhin billigt das Gericht die Gewährleistung – aufgrund des rein formalen Anknüpfungspunkts des Rechts am eigenen Wort – auch juristischen Personen zu und bejaht insoweit die wesensmäßige Anwendbarkeit von Art. 19 Abs. 3 GG. Der Bezug zur Menschenwürde stehe dem nicht entgegen, da das Recht am gesprochenen Wort als besondere Ausprägung des All-

---

182 Ebd., (37).
183 Ebd., (38).
184 Ebd., (40).
185 Ebd., (41).
186 Ebd.
187 Ebd., (42).

gemeinen Persönlichkeitsrechts nicht von einem besonderen personalen Kommunikationsinhalt abhänge. Die Gefährdungslage sei grundrechtstypisch, da sich die juristische Person zur Kommunikation natürlicher Personen bediene. Die verfassungsrechtliche Grundlage des Schutzes liege insoweit allein in Art. 2 Abs. 1 GG.[188]

Dem Schutzgut „Vertraulichkeitserwartung" kommt beim Recht am eigenen Wort darüber hinaus eine besondere Rolle im Rahmen der Einwilligung zu. Diese sei Ausdruck des in Art. 2 Abs. 1 GG geschützten Selbstbestimmungsrechts und könne den Schutz der Vertraulichkeit aufheben. Jedoch stellt das BVerfG hohe Anforderungen an das Vorliegen einer konkludenten Einwilligung. Gerügt wird insbesondere der Schluss des Oberlandesgerichts von der tatsächlichen Verbreitung der Mithöreinrichtungen auf eine stillschweigende Billigung des Mithörens. Diese würde das Selbstbestimmungsrecht in verfassungsrechtlich nicht hinnehmbarer Weise einengen. Erforderlich für eine konkludente Einwilligung seien zunächst die Anforderungen, wie sie die fachgerichtliche Rechtsprechung herausgebildet hat. Danach muss ein bestimmtes Verhalten in einem solchen Maße üblich und geradezu selbstverständlich sein, dass „entsprechend dem Grundgedanken des § 157 BGB nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte vernünftigerweise nur von einer Zustimmung des Betroffenen ausgegangen werden könne".[189] Das bloße „faktische Verbreitetsein" oder die „faktisch häufig[e]" oder „gar weitgehend[e]" Üblichkeit reichten gerade nicht aus.[190] Weiterhin müsse die technische Nutzungsmöglichkeit aufgrund des Selbstbestimmungsrechts für die Annahme einer konkludenten Einwilligung so zu verstehen sein, „dass Dritten ohne Zustimmung sämtlicher Gesprächspartner das heimliche Zuhören des Gesprächs ermöglicht werden darf, sofern nicht vorsorglich von allen widersprochen wird."[191] Auch wenn „Vertraulichkeitserwartungen" infolge tatsächlicher Nutzungsveränderungen vielfach entgegenstünden, seien die Feststellungen zu den Anforderungen an konkludente Einwilligungen nicht entbehrlich.[192] Diese Stelle ist hinsichtlich der Funktion der Vertraulichkeitserwartung nicht ganz klar; sie kann zumindest so verstanden werden, dass das Fehlen einer Vertraulichkeitserwartung nicht als pauschale Behauptung dienen darf, sondern dass darüber hinaus die Anforderungen an konkludente Einwilligungen weiterhin zu prüfen und festzustellen sind.

Neben diesen Anknüpfungspunkten führt insbesondere die Entscheidung zur *Rasterfahndung* aus dem Jahr 2006 die dogmatische Einbindung der „Vertraulichkeitserwartung" fort. Im Rahmen der Kriterien für die Eingriffsintensität[193] komme

---

188 Ebd., (46).

189 Ebd., (45 f.).

190 Ebd., (46).

191 Ebd., (47).

192 Ebd., (47).

193 Siehe unten II.B.9.a).

der Persönlichkeitsrelevanz große Bedeutung zu. Wann eine solche Relevanz vorliegt, bestimmt das Gericht unter Verweis auf die Vertraulichkeitserwartung, es handele sich um einen besonders intensiven Eingriff, wenn Informationen betroffen sind, „bei deren Erlangung Vertraulichkeitserwartungen verletzt werden". Vor allem sei dies der Fall, wenn Informationen unter dem Schutz besonderer Grundrechte wie Art. 3 Abs. 3 GG, Art. 13 GG und Art. 10 GG stehen. Hierbei sei auch auf die einfachgesetzliche Kategorie „besonderer Arten personenbezogener Daten" gem. § 3 Abs. 9 BDSG abzustellen.[194] Die Vertraulichkeitserwartung wird also als Schutzgut verstanden und normativ aufgeladen, um durch den Bezug zu Einzelgrundrechten und zur Kategorie sensibler Daten zumindest im Ansatz eine inhaltliche Konkretisierung zu erreichen.

Die Entscheidungen belegen damit die zentrale Stellung des Topos „Vertraulichkeitserwartung": Einerseits bildet die Vertraulichkeitserwartung ein Schutzgut der Privatsphäre, andererseits aber kommt ihr auch im Rahmen des rein formalen, mediengebundenen Rechts am eigenen Wort Bedeutung zu, da bei Fehlen dieser Erwartung – unter den strengen Voraussetzungen der konkludenten Einwilligung – der Schutzbereich nicht eröffnet sein soll. Daneben zeigt die Rasterfahndungsentscheidung eine Möglichkeit zur normativen Konkretisierung der Vertraulichkeitserwartung mittels der Einzelgrundrechte. Eher am Rande verweist die Entscheidung zu Mithöreinrichtungen auch auf das Risiko von Verhaltensänderungen (Verlust der unbefangenen Kommunikation), welches dem Recht am eigenen Wort ebenso wie dem Recht am eigenen Bild zugrunde liegt.

### 8. Persönlichkeitsprofile und Informationskonvergenz

Das Risiko der Erstellung von Persönlichkeitsprofilen wird insbesondere in der Entscheidung zur *automatischen Kennzeichenerfassung* aufgegriffen.[195] Das Gericht prüfte die Eingriffsgrundlagen nicht nur hinsichtlich der Rückschlüsse, welche die Erfassung „punktuell", also unmittelbar auf das Bewegungsverhalten bei der konkreten Vorbeifahrt an einer Überwachungskamera ermöglichte, sondern auch im Hinblick auf ein „Mehr" an Informationen, das etwa aus der Nähe des Angetroffenen zu einer bestimmten Veranstaltung (beispielsweise Antreffen auf Zufahrtswegen) geschlossen werden kann oder das aus der Zusammenstellung von Einzelfahrten zu einem Bewegungsprofil folgt.[196] Diese Arten der Nutzung von Kennzeichendaten seien als funktionale Äquivalente zu anderen Eingriffen zu werten und könnten ähnlich einer gezielten Notierung von Veranstaltungsteilnahmen verhaltenssteuernde Wirkung entfalten. Bezüglich der beeinträchtigten Kommuni-

---

[194] BVerfGE 115, 320 (348).

[195] BVerfG Urteil vom 11.3.2008, 1 BvR 2074/05, 1254/07 (*Kennzeichenerfassung)* = BVerfGE 120, 378; dazu: *Kenzel*, Kennzeichenfahndung, 2013.

[196] BVerfGE 120, 378 (405 f.).

kationsfreiheiten liege in diesem Fall eine eingriffsgleiche Maßnahme vor.[197] Die Zusammenstellung der Einzelfahrten zu einem Bewegungsprofil lasse die Kennzeichenerfassung als Mittel der technischen Observation und nicht lediglich als Schlüssel zu Folgeeingriffen erscheinen. Es liege dann nicht bloß eine Effektivierung des bisherigen „Eingriffsinstrumentariums", sondern eine „neuartige Eingriffsmöglichkeit mit potenziell hoher Persönlichkeitsrelevanz" vor.[198] Durch längerfristigen oder weiträumigen Einsatz und anschließende Verknüpfung mit weiteren Informationen könne sich die Intensität des Eingriffs „der Erstellung eines Persönlichkeitsbilds annähern".[199] Hier wird also eine Situation beschrieben, die in engem Zusammenhang zur Informationsemergenz steht, aber dennoch davon unterschieden werden kann. Es handelt sich um die Gesamterfassung. Eine genauere Beschreibung weist die Entscheidung jedoch nicht auf.

In der Entscheidung zur *Vorratsdatenspeicherung*[200] wird die Aussagekraft von Verbindungsdaten mit dem Risiko der Profilbildung verbunden: Die Daten ermöglichten „tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers". Obwohl gerade keine Inhaltsdaten gespeichert würden, erlaube eine umfassende und automatisierte Auswertung inhaltliche Rückschlüsse „bis in die Intimsphäre". Die Kombination der Daten gestatte „detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen". Mit zunehmender Dichte der Telekommunikation ermögliche die Speicherung die Erstellung „aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers".[201] Noch stärker gewichtet das Gericht die Rückschlüsse auf Kommunikationsinhalte bei IP-Adressen: Schon aufgrund des Umfangs der Kontakte, die durch das Aufrufen von Internetseiten hergestellt würden, sei die Speicherung von IP-Adressen aussagekräftiger als eine Telefonnummernabfrage. Die „Kenntnis einer Kontaktaufnahme mit einer Internetseite" habe eine andere inhaltliche Bedeutung. Aufgrund der elektronischen Fixierung und längeren Abrufbarkeit lasse sich vielfach verlässlich rekonstruieren, „mit welchem Gegenstand sich der Kommunizierende auseinander gesetzt hat". Die IP-Adresse gebe damit zugleich Auskunft über den Inhalt der Kommunikation. Die für Telefonnummern geltende „Unterscheidung von äußerlichen Verbindungsdaten und Gesprächsinhalten" löse sich bei IP-Adressen auf.[202] Deutlicher wird hier das Risiko der Informationsemergenz („überschießende" Inhaltsrückschlüsse)[203] vorausgesetzt und mit dem Risiko der Informationspermanenz (Fixierung der Daten)

---

197 Ebd., (406).

198 Ebd.

199 Ebd., (407).

200 BVerfG Urteil vom 2.3.2010, 1 BvR 256, 263, 586/08 *(Vorratsdatenspeicherung)* = BVerfGE 125, 260.

201 BVerfGE 125, 260 (319).

202 Ebd., (342).

203 Siehe oben Teil 1, II.A.2.d).

verbunden. Zwar findet sich im Anschluss an die Passage kein weiterer Verweis auf die Profilerstellung, gleichwohl präzisiert das Gericht hier ersichtlich das Risiko der zuvor genannten „aussagekräftigen Persönlichkeitsprofile". Beachtlich ist zudem die Übertragung der Risikokonzeption auch auf „Gruppen und Verbände", bei denen die Telekommunikationsdaten Rückschlüsse auf „interne Einflussstrukturen" und Entscheidungsabläufe ermöglichten.[204]

Das Risiko von „Bewegungs- oder Sozialprofilen" greift auch Richter *Eichelberger* in seiner abweichenden Meinung zur Vorratsdatenentscheidung auf.[205] Seine Kritik an der Senatsmehrheit betrifft jedoch nicht die dargestellten inhaltlichen Aspekte der Risikokonzeption, sondern vielmehr deren Funktion und Stellenwert in der Urteilsbegründung: Die Senatsmehrheit gehe bei ihrer Abwägung im Rahmen der Verhältnismäßigkeitsprüfung „stets von dem größtmöglichen Eingriff eines umfassenden, letztlich auf ein Bewegungs- oder Sozialprofil abzielenden Datenabrufs aus". Hierin könne zwar ein Eingriff liegen, der „in seiner Schwere dem eines gewichtigen Zugriffs auf die Telekommunikationsinhalte des Bürgers gleichkommt". Außer Betracht bleibe jedoch, dass viele Abfragen nur auf einzelne Ereignisse abzielten und daher eher von geringerem Gewicht seien.[206] Was *Eichelberger* hier kritisiert ist also nicht die Risikokonzeption der Profilbildung an sich – diese bestätigt er sogar –, sondern die abstrakte Betrachtungsweise, die auf „befürchtete Nachteile", sozusagen auf die Gefühle der Grundrechtsberechtigten, abstellt, und nicht auf ein objektives Merkmal. Er kritisiert hier also einen Aspekt der Subjektivierung und Abstrahierung der Risikokonzeptionen.

Die Bezüge von IP-Adressen zur Profilbildung greift auch die Entscheidung des BVerfG zu *TKG-Abfragen* auf.[207] Im Unterschied zur Vorratsdatenspeicherung betrifft die Entscheidung nicht die Speicherung sämtlicher Telekommunikationsverkehrsdaten, sondern lediglich Speicherpflichten bei Telekommunikationsnummern.[208] Diese Daten umfassten weder höchstpersönliche Informationen noch sei mit ihnen die Erstellung von Persönlichkeits- oder Bewegungsprofilen möglich.[209] Insbesondere umfasse die Norm, welche die privaten Anbieter zur Erhebung und Speicherung auch über das betrieblich Erforderliche verpflichtet, § 111 TKG, nicht dynamische IP-Adressen. Statische IP-Adressen seien jedoch „unter den derzeitigen technischen Bedingungen" nur sehr begrenzt und in der Regel „institutionellen Großnutzern" zugewiesen, weshalb keine weitreichende Zuordnung von Internet-

---

204 BVerfGE 125, 260 (319).

205 Ebd., (380 ff.).

206 Ebd., (383 f.).

207 BVerfG Beschluss vom 24.1.2012, 1 BvR 1299/05 *(TKG-Abfragen)* = BVerfGE 130, 151.

208 Hierunter fallen Rufnummern, Anschlusskennungen, Mobilfunkendgerätenummern und Kennungen elektronischer Postfächer, BVerfGE, ebd., (153).

209 Ebd., (190).

kontakten möglich sei.[210] Beachtlich ist der explizite Verweis auf ein womöglich „deutlich größeres Eingriffsgewicht" im Fall der weiteren Verbreitung der IPv6, welche das Problem der IP-Nummernknappheit der IPv4 behebt und damit einer umfassenden Verwendung statischer IP-Adressen Vorschub leistet.[211] Für die Frage des Eingriffsgewichts der IP-Adressenidentifizierung komme es nicht primär darauf an, ob eine IP-Adresse technisch dynamisch oder statisch zugeteilt wird, sondern auf die „tatsächliche Bedeutung" der Auskunftspflicht. Der umfassende Gebrauch der IPv6 könne insoweit zu einer dauerhaften Deanonymisierung von Nutzern und Kommunikationsvorgängen im Netz führen.[212] Für sich genommen (also ohne die Kombinationsmöglichkeit bei Erfassung sämtlicher Verkehrsdaten oder eine Nutzung von IPv6 in größerem Umfang) komme den Daten eine bloß begrenzte Aussagekraft zu. Sie ermöglichten allein Auskunft über die Zuordnung einzelner Telekommunikationsnummern zum jeweiligen Anschlussinhaber.[213] Bezüglich weiterer Rückschlüsse im Sinne des Risikos der Informationsemergenz verweist das Gericht auf die Vorschriften zur Erhebung anderer Daten: Soweit sich „im Rahmen konkreter Erhebungszusammenhänge daraus sensible Informationen ergeben" könnten, richte sich die Beurteilung der Rechtmäßigkeit nach den Vorschriften, auf deren Grundlage die anderen Informationen erhoben wurden.[214] Die Entscheidung deutet damit zumindest darauf hin, dass das Risiko von „Persönlichkeits- oder Bewegungsprofilen" im Fall der Umstellung auf IPv6 für die Eingriffsart „individualisierende Zuordnung von Telekommunikationsnummern" aufleben wird.

Einen Hinweis auf die materiellen Anforderungen an das Vorliegen eines Persönlichkeitsprofils enthält die Zulässigkeitsprüfung in der Entscheidung zu strafprozessualen *Verwertbarkeit rechtswidrig erhobener Informationen*.[215] Der Entscheidung lag die akustische Wohnraumüberwachung zugrunde. Das BVerfG lehnte das Zulässigkeitserfordernis der substantiierten und schlüssigen Darlegung einer Rechtsverletzung in der Beschwerdebegründung gem. § 23 Abs. 1 S. 2, § 92 BVerfGG ab, weil die Eignung der verdeckten Ermittlungsmaßnahmen zur Erstellung eines Persönlichkeitsprofils nicht dargelegt worden sei. Maßgeblich hierfür war die nicht bestrittene fachgerichtliche Feststellung der Aufzeichnungsdauer von lediglich 8,4 % des Gesamtüberwachungszeitraums.[216]

---

210 Ebd., (190, 198).

211 http://de.wikipedia.org/wiki/Ipv6 [Stand: 28.3.2014].

212 BVerfGE 130, 151 (198).

213 Vgl. ebd., (197).

214 Vgl. ebd.

215 BVerfG Beschluss vom 7.12.2011, 2 BvR 2500/09, 1857/10 *(Verwertbarkeit rechtswidrig erhobener Informationen)* = BVerfGE 130, 1.

216 Ebd., 1 (24).

Von den älteren Entscheidungen bezieht sich die Kammerentscheidung zur *molekulargenetischen Untersuchung von Körperzellen* zum Zwecke der Strafverfolgungsvorsorge[217] auf die fehlende Möglichkeit zur Profilerstellung bei der Verwendung „nicht codierender" Abschnitte der DNA, um die Betroffenheit des von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG absolut geschützten Kernbereichs der Persönlichkeit zu verneinen.[218] Das Risiko der Stigmatisierung („soziale Abstempelung") und die Auswirkung auf das Rehabilitationsinteresse des Betroffenen wird am Rande angesprochen.[219] Im Übrigen werden weder Risiken noch Schutzgüter näher erörtert, obwohl der Sachverhalt Anlass zur Einbeziehung des Risikos Informationsemergenz geboten hätte.

In der *Bargatzky*-Entscheidung[220] wird hingegen der Aspekt der Informationskonvergenz mit der Risikokonzeption von Persönlichkeitsprofilen zusammengeführt: Unter Informationskonvergenz wird die mit der Überschneidung von Übertragungswegen, Diensten und Endgeräten einhergehende „Komprimierung des Informationsflusses" verstanden. Das (ggf. mobile) Endgerät diene nicht nur dem persönlichen Austausch, sondern zunehmend der „Abwicklung von Alltagsgeschäften" und der „Inanspruchnahme vielfältiger Dienste". Die Ausweitung der durch moderne Kommunikationsmittel gestalteten Lebensbereiche führe dabei zu quantitativer und qualitativer Erhöhung des Aussagegehalts. Am Ende der Argumentationskette steht sodann das Risiko der Erstellung von Persönlichkeitsprofilen, das jedoch nicht vertieft wird.[221]

Auch in der Entscheidung zur *Rasterfahndung* bezieht sich das Gericht auf die Möglichkeit der Erstellung eines „teilweise oder weitgehend vollständigen" Persönlichkeitsbildes, welches durch Menge und Vielfalt der im Rahmen der Rasterfahndung zugänglichen Informationen zumindest naherücke. Das Gericht unterstreicht die Ausführungen mit dem Verweis auf die Daten privater Stellen, wie beispielsweise aus Kundenkartensystemen von Kaufhäusern, die im Rahmen der Rasterfahndung ebenfalls zugänglich werden.[222]

Von den analysierten Entscheidungen geht somit vor allem die Entscheidung zu Vorratsdaten näher auf die Charakteristika von Persönlichkeitsprofilen ein. Festzuhalten bleibt dabei die charakteristische Verbindung mehrerer Risiken (Informationsemergenz und Informationspermanenz). Die Zusammenschau mit der *Bargatzky*-Entscheidung ergänzt dieses Bild um den Aspekt der Informationskonvergenz. Die Entscheidung zur Abfrage von Telekommunikationsnummern nach

---

[217] BVerfG Beschluss vom 13.12.2000, 2 BvR 1741/99, 276,2061/00 *(Genetischer Fingerabdruck)* = BVerfGE 103, 21.

[218] Ebd., (31).

[219] Ebd., (34).

[220] BVerfGE 115, 166.

[221] Ebd., (190, 193).

[222] BVerfGE 115, 320 (350 f.).

dem TKG deutet auf das Profilrisiko bei Umstellung auf IPv6 hin. Darüber hinaus fällt auf, dass die Profilbildung eine Risikokategorie darstellt, die nicht nur mehrere bereits identifizierte Risiken in spezifischer Weise verbindet, sondern in den Entscheidungen üblicherweise am Ende einer Argumentationskette, sozusagen als schwerstes Risiko, auftritt. Die Anbindung an Schutzgüter erfolgt dabei, wie insbesondere die Entscheidung zur *Kennzeichenfahndung* zeigt, wiederum über die vorausgesetzten Auswirkungen auf die Verhaltensfreiheit und den Grundrechtsgebrauch.

### 9. Individuelle Überwachungsnachteile

In der Entscheidung vom 12.3.2003[223] befasste sich das BVerfG mit der Erhebung von *Telekommunikationsverbindungsdaten* mehrerer Journalisten. Die Strafverfolgungsbehörden wollten damit den Aufenthaltsort von Beschuldigten ermitteln.[224] Aufgrund der Berichterstattung gingen sie davon aus, dass die Journalisten persönlichen Kontakt mit den Beschuldigten unterhielten. Beachtlich ist die Entscheidung insbesondere wegen der Aufstellung von Intensitätskriterien bei Informationseingriffen und der Auseinandersetzung mit Risiken für unbeteiligte Dritte, die von der Erhebung der Verbindungsdaten beeinträchtigt werden.

Zunächst bestätigt das Gericht die Erfassung von Kommunikationsumständen und zieht Art. 10 Abs. 1 GG als alleinigen Maßstab heran.[225] Wiederum stehen mögliche Auswirkungen auf das Verhalten der Betroffenen im Vordergrund: Es solle verhindert werden, dass Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen aufgrund des Bewusstseins staatlicher Kenntniserlangung „unterbleibt oder nach Form und Inhalt verändert verläuft".[226] Herausgehoben wird dabei die Möglichkeit zur Rekonstruktion von Aufenthaltsorten durch Kenntnis von Mobilfunkdaten.[227] Auch inhaltlich komme dem Kommunikationsverhalten insbesondere durch das Internet eine gestiegene Bedeutung zu. In immer mehr Lebensbereichen seien personenbezogene Daten über das Kommunikationsverhalten der Menschen verfügbar, wodurch „erhebliche Rückschlüsse" auf das „Kommunikations- und Bewegungsverhalten" möglich seien.[228] Die Zusammenführung der Verbindungs- mit den ebenfalls verfügbaren Kundendaten ermögliche über den dadurch oftmals bekannten Beruf des Gesprächspartners auch „begrenzte Rückschlüsse" auf die Art der Gesprächsinhalte. Hierin lägen, ebenso wie in der Mit-

---

[223] BVerfG Urteil vom 12.3.2003, 1 BvR 330/96, 348/99 – *Telekommunikationsverbindungsdaten* = BVerfGE 107, 299.

[224] Es handelte sich um den Immobilienbetrüger *Schneider* und den Terroristen *Klein*.

[225] BVerfGE 107, 299 (312).

[226] Ebd., (313).

[227] Ebd., (314).

[228] Ebd., (319 f.).

betroffenheit der großen Anzahl von Kommunikationspartnern, Kriterien für die Schwere des Eingriffs. Insbesondere sei das Gewicht der Beeinträchtigung abhängig von der Anonymität der Gesprächsteilnehmer, der Art der erfassten Kommunikationsumstände und von Nachteilen, die den Gesprächspartnern „auf Grund der Überwachungsmaßnahmen drohen oder von ihnen nicht ohne jeden Grund befürchtet werden". In diesem Zusammenhang wird dann auch das Kriterium der „erheblichen Streubreite" herangezogen.[229] Die Erfassung der Kommunikation Unverdächtiger schaffe das Risiko, „einem unberechtigten Verdacht ausgesetzt zu werden". Insoweit liege bereits in dem Bekanntwerden durch die Sicherheitsbehörden ein Eingriff. „Spezifische Risiken", entstünden, da sich Einzelne erst dann rechtlich wehren können, wenn der Eingriff bereits vollzogen sei.[230] Neben dieser materiellen Beschreibung individueller Überwachungsnachteile bestätigt der in der Entscheidung besonders hervorgehobene „Grundrechtsschutz durch Verfahren" die Selbstbestimmungskonzeption, die insbesondere im Volkszählungsurteil vorangebracht wurde:[231] Wegen der – mangels Kenntnis – regelmäßig fehlenden Möglichkeit von Rechtsschutz durch die Betroffenen selbst müsse eine unabhängige, auch die Interessen der Betroffenen wahrnehmende Stelle in solchen Fällen entscheiden, in denen nicht bereits eine sofortige Löschung nach der Aufzeichnung erfolgt. Insoweit forderte das BVerfG neben einem qualifizierten Richtervorbehalt auch weitere verfahrensrechtliche Absicherungen bestehender Beweisverwertungsverbote.[232]

Die dargestellten Abschnitte präzisieren damit die bereits im Volkszählungsurteil und in der *zweiten G-10*-Entscheidung[233] entwickelte Eingriffskonzeption, die auf individuelle Nachteile und Verhaltensauswirkungen durch Überwachung abstellt. Dabei wird nicht nur die Möglichkeit, Gegenstand von Ermittlungen zu werden, sondern bereits die bloße Kenntniserlangung durch Sicherheitsbehörden als einschlägiges Risiko betrachtet. Festzuhalten ist insbesondere die weitere Ausdifferenzierung der subjektiven Risikokonzeption im Hinblick auf „nicht ohne jeden Grund" befürchtete Nachteile. Bestätigt wird diese Konzeption in der Entscheidung zur *präventiven Telekommunikationsüberwachung*:[234] Im Rahmen der Verhältnismäßigkeitsprüfung führt das Gericht dort an, dass der Einblick in das Kommunikationsverhalten die Freiheit der Bürger „mittelbar beeinträchtigt". Die Furcht vor Überwachung könne unbefangene Kommunikation verhindern. Insbesondere er-

---

229 Ebd., (320), mit Verweis auf BVerfGE 100, 313 (376) bezüglich des Kriteriums der drohenden oder befürchteten Nachteile.

230 BVerfGE 107, 299 (321).

231 Siehe oben II.B.3.a).

232 BVerfGE 107, 299 (316, 333); *Peilert*, in: Menzel/Müller-Terpitz (Hrsg.), Verfassungsrechtsprechung, S. 736.

233 Siehe oben II.B.5.

234 BVerfG Urteil vom 27.7.2005, 1 BvR 668/04 *(präventive Telekommunikationsüberwachung)* = BVerfGE 113, 348.

mögliche die Standortkennung eingeschalteter Mobilfunkendeinrichtungen die Erstellung eines Bewegungsbildes, über das Gewohnheiten der betroffenen Personen oder Abweichungen hiervon aufgedeckt würden. Im Folgenden wird wieder die „Streubreite" des Eingriffs hinsichtlich unbeteiligter Kommunikationspartner aufgegriffen.[235] Die bereits angesprochene *Bargatzky*-Entscheidung stellt derartige Rückschlüsse ebenfalls in den Vordergrund und ergänzt den durch Art. 10 Abs. 1 GG vermittelten Schutz während der Übertragung auf die im Herrschaftsbereich des Teilnehmers verbleibenden Daten, die von Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG geschützt werden.[236]

In der Entscheidung zu *Kontostammdaten*[237] werden neben dem Persönlichkeitsbezug und den antizipierten Folgen die Abwehrmöglichkeiten des Betroffenen stärker in den Vordergrund gerückt: Das Gewicht nachteiliger Wirkungen informationsbezogener Maßnahmen sei abhängig von den Möglichkeiten des Einzelnen, die „Grundrechtsbeeinträchtigung oder jedenfalls weitere Folgen des Eingriffs abwehren zu können". Im Fall der Stammdatenabfrage verhinderte die Heimlichkeit der Maßnahme einen wirkungsvollen Schutz.[238] Im Ergebnis wurden die untersuchten Abfragen jedoch vor allem deshalb als wenig intensiv und damit nicht unangemessen beurteilt, weil die geprüften Eingriffsgrundlagen keinen Einblick in die Kontoinhaltsdaten erlaubten. Auch das Risiko von Folgeeingriffen, die dann etwa zur Erhebung der Kontobewegungen führen könnten, wurde angesichts bestehender Eingriffsschwellen, verfolgter Gemeinwohlbelange und den erforderlichen eigenständigen Eingriffsgrundlagen für Folgeeingriffe nicht beanstandet.[239]

### *a) Intensitätskriterien und Einschüchterungseffekte*

Bereits im Beschluss zur *Rasterfahndung* wird die Betroffenheit mit einer einen Grundrechtseingriff auslösenden Qualität mit Folgeverarbeitungen begründet, die sich an den ersten Datenabgleich anschließen. Dabei führt eine unmittelbar erfolgende spurenlose Löschung, wie bereits in der *zweiten G-10*-Entscheidung, dazu, dass die Eingriffsqualität entfällt.[240] Die im Rahmen der Verhältnismäßigkeitsprüfung aufgegriffenen Intensitätskriterien verbinden dann jedoch wieder die individuelle mit der gesamtgesellschaftlichen Ebene: Maßgebend soll neben der „Intensität der individuellen Beeinträchtigung" auch die Zahl der Betroffenen sein. Die Intensität der individuellen Beeinträchtigung wird – wie schon in BVerfGE 100, 313

---

235 Ebd., (382 f.).

236 BVerfGE 115, 166 (183 f.). Siehe oben I.A.

237 BVerfG Beschluss vom 13.6.2007, 1 BvR 1550/03, 2357/04, 603/05 *(Kontostammdaten)* = BVerfGE 118, 168.

238 Ebd., (197 f.).

239 Ebd., (199 f.).

240 BVerfGE 115, 320 (343 f.).

und BVerfGE 109, 279 – durch die Merkmale Veranlassung, Anonymität, Persönlichkeitsbezug der Information sowie drohende oder nicht ohne Grund befürchtete Nachteile konkretisiert. Darüber hinaus werden die Kriterien jedoch näher ausgebreitet. Das BVerfG stellt zunächst fest, dass sie auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG übertragbar sind, da Art. 10 GG und Art. 13 GG, anhand derer sie entwickelt wurden, „spezielle Ausprägungen" des Grundrechts auf informationelle Selbstbestimmung seien.[241]

Unter den individuellen Nachteilen versteht das Gericht sodann erneut das Risiko, Gegenstand staatlicher Ermittlungen zu werden, „das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden". Ausdrücklich thematisiert wird dann jedoch auch die „stigmatisierende Wirkung" des Bekanntwerdens informationsbezogener Ermittlungsmaßnahmen und damit die Erhöhung des mittelbaren Risikos, im Alltag oder Berufsleben diskriminiert zu werden.[242] Als Beispiel für das Risiko von Anschlussermittlungen wird die Vorladung von 140 ausländischen Studenten zu „Gesprächen" mit der Polizei genannt, die im Anschluss an die nach dem 11.9.2001 erfolgte Rasterfahndung durchgeführt wurde.[243] Bei Nichterscheinen wurden die Personen „auf andere Weise überprüft", wozu z.B. auch Umfelderkundigungen gehörten.[244] Die stigmatisierende Wirkung sieht das Gericht in dem Anknüpfen an besondere persönlichkeitsbezogene Merkmale im Sinne von Art. 3 Abs. 3 GG bzw. Art. 140 GG i.V.m. Art. 136 Abs. 3 WRV. Maßgeblich für die Schwere des Eingriffs war in der Entscheidung also die Zielrichtung der Fahndung (Ausländer bestimmter Herkunft bzw. muslimischen Glaubens). Diese bringe das Risiko der Reproduktion von Vorurteilen und Stigmatisierung von Bevölkerungsgruppen in der öffentlichen Wahrnehmung mit sich.[245]

Im Beschluss zur *Videoüberwachung des öffentlichen Raums* vom 23.2.2007[246] greift das BVerfG diese Konzeption auf und stellt neben den Kriterien Anlasslosigkeit und Streubreite unter Verweis auf *Geiger*[247] auch auf die Abschreckungswirkung von Überwachungskameras und deren Ziel einer „Verhaltenslenkung" als Schwerekriterien ab.[248]

---

241 Ebd., (347).

242 Ebd., (351).

243 Ebd., (352).

244 Ebd.

245 Ebd., (353).

246 BVerfG Beschluss vom 23.2.2007, 1 BvR 2368/06 *(Videoüberwachung)* = NVwZ 2007, 688.

247 *Geiger*, Video-Überwachungstechnologie.

248 BVerfG Beschluss vom 23.2.2007, 1 BvR 2368/06 *(Videoüberwachung)* Rn. 38, 51 f.

Die Entscheidung zur *automatischen Kennzeichenerfassung*[249] lässt sich in diese Rechtsprechungslinie einordnen. Stärker als in den anderen Entscheidungen wird hier zunächst der Charakter eines Vorfeldschutzes im Rahmen des Grundrechts auf informationelle Selbstbestimmung hervorgehoben: Die Schutzgüter Verhaltensfreiheit und Privatheit werden bereits auf der „Stufe der Persönlichkeitsgefährdung" aufgegriffen. „Bereits im Vorfeld konkreter Bedrohungen von Rechtsgütern" könne eine maßgebliche Gefährdungslage entstehen.[250] Anschließend wird das Risiko von Folgeeingriffen unter Verweis auf BVerfGE 100, 313 sowie BVerfGE 115, 320 aufgegriffen: Auch wenn die Erfassung eines größeren Datenbestandes „letztlich nur Mittel zum Zweck für eine weitere Verkleinerung der Treffermenge ist", könne ein Eingriff bereits in der Informationserhebung liegen, soweit die Informationen den Behörden verfügbar gemacht werden und sie dadurch „die Basis für einen nachfolgenden Abgleich mit Suchkriterien" bilden können.[251]

Im konkreten Fall der automatischen Kennzeichenerfassung differenziert das Gericht ebenso wie in der *zweiten G-10-Entscheidung* und der *Verbindungsdatenentscheidung* nach Trefferfällen.[252] Nur wenn das Kennzeichen nach der Erfassung unmittelbar „technisch wieder spurenlos, anonym und ohne die Möglichkeit einen Personenbezug herzustellen" ausgesondert werde, liege kein „Gefährdungstatbestand" und damit auch kein Eingriff in das Recht auf informationelle Selbstbestimmung vor.[253] Die „spezifische Persönlichkeitsgefährdung für Verhaltensfreiheit und Privatheit", die den Schutz des Grundrechts auslöse, beginne erst in einem Trefferfall, also wenn das Kennzeichen als Treffer im Speicher festgehalten und „gegebenenfalls Grundlage weiterer Maßnahmen werden kann".[254]

Im Übrigen greift die Entscheidung wieder die bekannten Intensitätskriterien auf, namentlich die Persönlichkeitsrelevanz, Zurechenbarkeit und Heimlichkeit der Maßnahme.[255] Im Rahmen der Zurechenbarkeit, also der Frage, ob der Betroffene einen zurechenbaren Anlass – beispielsweise durch eine Rechtsverletzung – geschaffen hat, wechselt die Entscheidung in die gesamtgesellschaftliche „Makro-Perspektive": Sofern eine große Anzahl von Personen in den Wirkungsbereich einer Maßnahme einbezogen wird, ohne selbst einen Erhebungsanlass gegeben zu haben, könnten hieraus „allgemeine Einschüchterungseffekte" folgen, die grundrechtsausübungsrelevant sein könnten. Es folgt der Verweis auf die gefährdete Unbefangenheit des Verhaltens, indem breit streuende Maßnahmen Missbrauchsrisi-

---

[249] BVerfG Urteil vom 11.3.2008, 1 BvR 2074/05, 1254/07 *(Kennzeichenerfassung)* = BVerfGE 120, 378; dazu *Kenzel*, Kennzeichenfahndung, 2013.

[250] BVerfGE 120, 378 (397).

[251] Ebd., (398).

[252] Zu diesen beiden Entscheidungen siehe oben II.B.5. und 8.

[253] BVerfGE 120, 378 (399).

[254] Ebd., (399 f.).

[255] Ebd., (401 ff.).

ken schaffen und das Überwachungsgefühl auslösen.[256] Die Intensitätskonzeption wird dabei quasi „dynamisiert", indem sie an das Risiko von Folgeeingriffen gebunden wird:

> „Die Schwere des Eingriffs nimmt mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe in Grundrechte der jeweiligen Personen zu sowie mit der Möglichkeit der Verknüpfung mit anderen Daten, die wiederum andere Folgemaßnahmen auslösen können".[257]

Das „Gefühl des Überwachtwerdens" greift die Entscheidung nochmals im Rahmen der Verhältnismäßigkeit im engeren Sinne auf: Treffe die automatisierte Kennzeichenerfassung unterschiedslos jeden nur deshalb, weil er mit dem Fahrzeug die Erfassungsstelle passiert, so vermittele dies den „Eindruck ständiger Kontrolle". Es stelle sich ein „Gefühl des Überwachtwerdens" mit Beeinträchtigung der Grundrechtsausübung ein.[258]

Das so entwickelte Konzept wird in gleicher Weise auch in der einstweiligen Anordnung zum *Bayerischen Versammlungsgesetz* aufgegriffen.[259] Dort waren die Eingriffsgrundlagen für die Aufzeichnung von Übersichtsaufnahmen (Kamera-Monitor-Übertragungen) Gegenstand der negativen Folgenabwägung im Rahmen des § 32 Abs. 1 BVerfGG. Trotz der Bezeichnung als „Übersichtsaufnahme" waren Einzelpersonen individualisierbar.[260] Die Eingriffsgrundlagen erlaubten neben den Aufnahmen auch z.T. die zeitlich unbegrenzte Speicherung und verschiedene Anschlussverwendungen. Sie sollten sogar auf Veranstaltungen in geschlossenen Räumen anwendbar sein.[261] Das Gericht bezieht sich zur Begründung der stattgebenden Entscheidung wieder auf Einschüchterungseffekte, Folgen für die Grundrechtsausübung, Gefahr von Folgeeingriffen und Überwachungsgefühl.[262] Besonderes Augenmerk legt die Anordnung auf die Ermöglichung einer anlasslosen Datenbevorratung der Aufzeichnungen: Diese führe zu im Rahmen des § 32 BVerfGG durchgreifenden Nachteilen, da sie allein an die Wahrnehmung des Versammlungsrechts und damit an den Gebrauch eines für die demokratische Meinungsbildung elementaren Grundrechts anknüpfte. Die Einschüchterungseffekte überwogen im Rahmen der Folgenabwägung deshalb die Nachteile des teilweisen Verzichts auf Übersichtsaufzeichnungen.[263]

---

256 Ebd., (402).

257 Ebd., (403).

258 Ebd., (430).

259 BVerfG Beschluss vom 17.2.2009, 1 BvR 2492/08 *(Bayerisches Versammlungsgesetz)* = BVerfGE 122, 342.

260 Ebd., (368).

261 Vgl. ebd., (369 ff.).

262 Ebd., (369 ff.).

263 Ebd., (371).

Ein Fall, in dem das Gericht keine relevante Gefährdungslage und damit auch keinen Eingriff wegen spurloser technischer Aussonderung von „Nichttreffern“[264] erkannte, stellt die *Mikado*-Entscheidung[265] dar. Der Nichtannahmebeschluss hatte ein Ermittlungsverfahren zu § 184b StGB zum Gegenstand. Die Staatsanwaltschaft hatte Kenntnis über den genauen Abbuchungsbetrag, der für den Zugang zu bestimmten kinderpornografischen Inhalten per Kreditkarte bezahlt worden war. Sie forderte daher alle Institute, die in Deutschland an ihre Kunden Mastercard- und Visa-Kreditkarten ausgeben, zur Überprüfung relevanter Umsätze mittels Überweisungsbetrag, Empfänger und einer „Merchant-ID“ auf. Die Unternehmen führten einen automatischen Suchlauf durch und übermittelten die erfragten Informationen, was schließlich zur Ermittlung von 322 Karteninhabern führte. Die Beschwerdeführer rügten insbesondere die fehlende Eingriffsgrundlage; § 161 StPO könne nicht für „personenbezogene Datenfahndungen“ herangezogen werden. Die Maßnahme stünde vielmehr der Rasterfahndung nahe und müsse deshalb die Anforderungen des § 98 StPO erfüllen. Gerügt wurde ferner eine „Flucht ins Privatrecht“ durch Abfrage der Daten bei privaten Kreditinstituten und ein daraus resultierender Einschüchterungseffekt, der Bürger von der Nutzung von Kreditkarten abschrecke. Weiterhin bestehe ein Missverhältnis zwischen der Zahl der 22 Millionen überprüften Kreditkarteninhaber und den schließlich ermittelten 322 Verdächtigen.[266]

Das BVerfG sah jedoch in der Maßnahme keinen Eingriff, da die Kreditkartendaten nicht „durch eine staatliche Stelle oder auf deren Veranlassung erhoben, gespeichert, verwendet oder weitergegeben“ wurden. Die bei den Instituten gespeicherten Daten seien nicht an die Strafverfolgungsbehörden übermittelt oder dort zur weiteren Verwendung gespeichert worden. Im Rahmen des automatischen Suchlaufs, den die Kreditkartenunternehmen nur „auf Veranlassung der Staatsanwaltschaft“ durchführten, wurden die Daten der Beschwerdeführer lediglich maschinell geprüft, jedoch mangels Erfüllung der Suchkriterien schon bei den Unternehmen als Nichttreffer angezeigt. Ihre Daten seien daher nie an die Staatsanwaltschaft weitergegeben worden. Zudem habe auch die Staatsanwaltschaft keine Möglichkeit gehabt, den Datenbestand für eigene Abfragen zu nutzen. Der maschinelle Suchlauf sei für die Annahme eines Eingriffs nicht ausreichend, da die Daten „anonym und spurenlos aus diesem Suchlauf ausgeschieden wurden und nicht im Zusammenhang mit dieser Ermittlungsmaßnahme behördlich zur Kenntnis genommen wurden“.[267] Auch entspreche die Maßnahme hinsichtlich Wirkung und Eingriffsintensität nicht der Rasterfahndung, da sie insbesondere kein „Hinarbeiten“ auf Personen, die ein „nach kriminalistischen Erfahrungen“ festgelegtes „Ver-

---

[264] Siehe auch oben II.B.2.

[265] BVerfG Beschluss vom 17.2.2009, 2 BvR 1372/07 *(Mikado)* = http://www.bverfg.de/entscheidungen/rk20090217_2bvr137207.html [Stand: 28.3.2014].

[266] Ebd. Rn. 12.

[267] Ebd. Rn. 19.

dächtigenprofil“ erfüllen, darstelle, sondern, weil vielmehr ein gezieltes Kriterium verwendet wurde, dessen Erfüllung mit hinreichender Wahrscheinlichkeit auf die Verwirklichung der strafbaren Handlung schließen ließ.[268] Indirekt bestätigt die Entscheidung damit die Risikokonzeption der Informationspermanenz: Da keine Daten zurückbleiben, liegt kein Risiko und deshalb auch kein Eingriff vor. Die durch die Beschwerdeführer gerügten Einschüchterungseffekte, die auch aufgrund der bloßen Verarbeitungspraxis auftreten könnten, greift das BVerfG nicht auf.

In der Entscheidung zur *Vorratsdatenspeicherung*[269] nehmen Einschüchterungseffekt und Überwachungsgefühl dagegen wieder einen hohen Stellenwert bei der Prüfung der Verhältnismäßigkeit im engeren Sinne ein: Die Schwere des Eingriffs einer anlasslosen sechsmonatigen Speicherung aller Telekommunikationsverkehrsdaten begründet das Gericht unter anderem damit, dass sie ein „Gefühl des ständigen Überwachtwerdens“ hervorrufen könne und „tiefe Einblicke in das Privatleben“ ermögliche, „ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich“ sei. Dem Einzelnen sei nicht bekannt, was welche staatliche Behörde über ihn weiß, wohl aber, dass die Behörden „vieles, auch Höchstpersönliches über ihn wissen können“. Hierdurch könne die Speicherung eine „diffuse Bedrohlichkeit“ erhalten. Aus dem Nichtwissen um die Relevanz der Daten ergebe sich eine „Bedrohlichkeit“, welcher ebenso wie „verunsichernde[n] Spekulationen“ entgegenzuwirken sei.[270]

Auch die übrigen Kriterien des Intensitätskatalogs werden in der Vorratsdatenentscheidung aufgegriffen und fortentwickelt: So spricht die Entscheidung von einem „diffus bedrohliche[n] Gefühl des Beobachtetseins, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen“ beeinträchtigen könne.[271] Auch das Risiko von Folgeeingriffen wird thematisiert und um ein Beispiel ergänzt: Die bloße Anwesenheit in einer Funkzelle genüge, um in weitem Umfang Ermittlungen ausgesetzt zu sein.[272] Superlative gebraucht das Gericht in Bezug auf die Breitenwirkung. Es handele sich bei der Vorratsdatenspeicherung um einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Die Speicherung beziehe sich auf „Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar“ sei.[273]

Zusammenfassend liegt den Entscheidungen ein an einem Katalog von Intensitätskriterien orientiertes Konzept zur Prüfung der Eingriffsschwere zugrunde. Das

---

[268] Ebd. Rn. 24.

[269] BVerfG Urteil vom 2.3.2010, 1 BvR 256, 263, 586/08 *(Vorratsdatenspeicherung)* = BVerfGE 125, 260.

[270] BVerfGE 125, 260 (335).

[271] Ebd., (320).

[272] Ebd., (320).

[273] Ebd., (318 f.).

Ergebnis der näheren Untersuchung der Intensitätskriterien fügt sich in die Risikokonzeption von Verhaltensanpassungen und Beeinträchtigung des Grundrechtsgebrauchs durch Einschüchterungseffekte sowie Risiken von Folgeeingriffen ein. Die Risiken lassen sich dabei zwar in erster Linie der individuellen Ebene zuordnen, enthalten aber – insbesondere im Rahmen des Intensitätskriteriums „Streubreite" und „Missbrauchsgefahren" – auch Bezüge zu Risiken auf gesamtgesellschaftlicher Ebene.

*b) Sondervoten Haas, Schluckebier, Eichelberger*

Eine pointierte Gegenposition zu dieser Konzeption von Eingriffsintensität, Einschüchterungseffekt und unterstellten Verhaltensanpassungen nimmt Richterin am Bundesverfassungsgericht a.D. *Haas* in ihrer abweichenden Meinung zur *Rasterfahndungsentscheidung* ein: Ihr zufolge widerspricht die Feststellung einer besonderen Eingriffsintensität der gleichzeitig als Schwerefaktor herangezogenen Unkenntnis der Betroffenen von der durchgeführten Maßnahme.[274] Weiterhin argumentiert Haas mit der öffentlichen Bekanntheit der Suchkriterien. Diese lägen wie etwa im Fall der Merkmale Geschlecht, Wohnsitz oder Studienrichtung „ohnehin für jedermann offen zutage".[275] Einer stigmatisierenden Wirkung tritt sie mit dem Argument entgegen, dass diese mangels öffentlicher Durchführung der Rasterfahndung nicht bestehe. Hierbei hält sie die Rasterfahndung für vergleichbar mit der Suche nach einem weiblichen Täter. Auch dort käme niemand „ernsthaft" auf den Gedanken, dass die Geschlechtsvorgabe zu einer Stigmatisierung führe. In der großen Zahl der jeweils betroffenen Personen sieht sie ebenfalls keine Erhöhung der Intensität, sondern geht aufgrund einer dadurch bestehenden „faktischen Anonymität" sogar von einer geringeren Eingriffsschwere bei Massenerhebungen aus.[276] Des Weiteren argumentiert sie mit der Sicherheitsgewährleistung des Staates und entsprechenden Schutzverpflichtungen. Verhaltensanpassungen und Einschüchterungen folgten nicht aus der Datenerhebung durch den Staat, sondern vielmehr aus der terroristischen Bedrohung.[277] Auch das Kriterium eines fehlenden Nähebezugs des Individuums zur Überwachung (Anlasslosigkeit) hält sie für „weder von Verfassungs wegen veranlasst noch systemgerecht". Die Rasterfahndung sei nämlich gerade für Konstellationen geschaffen, in denen ein Nähebezug erst noch zu klären sei. Insgesamt wertet sie den Eingriff als „nicht schwer". Er habe deshalb hinter dem Sicherheitsinteresse aller Bürger zurückzutreten. Hinsichtlich der übrigen Personen, die nicht als Treffer angezeigt wurden, lehnte sie die Grundrechtsbetroffenheit ab.[278]

---

274 BVerfGE 115, 320 (371 f.).

275 Ebd., (372).

276 Ebd., (373 f.).

277 Ebd., (375 f.).

278 BVerfGE 115, 320 (378 f.).

Unter einem anderen Gesichtspunkt wenden sich die Richter *Schluckebier* und *Eichberger* in ihren abweichenden Meinungen zur Vorratsdatenentscheidung gegen die dargestellte Konzeption.[279] Zum einen kritisieren sie die besondere Schwere aufgrund der Speicherung bei privaten Stellen, denen die Betroffenen ein „Grundvertrauen" entgegenbrächten,[280] zum anderen die Heranziehung des „größtmöglichen Eingriffs" einer Profilerstellung als allgemeinem Abwägungsmaßstab.[281]

### *c) Zwischenergebnis*

Die besprochenen Entscheidungen präzisieren die subjektive, auf Einschüchterungseffekten aufbauende Risikokonzeption durch die Formulierung von Intensitätskriterien. Sie beziehen sich zwar vorwiegend auf individuelle Überwachungsnachteile, erhalten jedoch insbesondere mit dem Kriterium „Streubreite" auch Bezüge auf die gesamtgesellschaftliche Ebene. Diese Differenzierung verkennt *Haas* in ihrer abweichenden Meinung: Die von ihr herangezogene Unkenntnis der jeweiligen Personen liegt nur vor, wenn von einer einengenden Betrachtung zum Zeitpunkt der Maßnahme ausgegangen wird. Aus der Urteilsperspektive sind jedoch auch diejenigen Effekte zu berücksichtigen, die sich zeitlich erst nach dem Ende der Überwachungsmaßnahme einstellen, und auch solche, die bereits durch die abstrakte Kenntnis von der Existenz der Überwachungsmaßnahme auftreten.

Die Schwächen von *Haas'* Argumentation zeigen sich weiterhin bei konsequenter Fortführung ihres Gedankengangs: Demzufolge müsste die absolute und dauerhafte Geheimhaltung von Überwachungsmaßnahmen den minimalsten Eingriff darstellen. In einer offenen Gesellschaft mit freier Presse wird dieses Geheimhaltungspostulat nicht zu verwirklichen sein. Vor allem widerspricht es jedoch dem auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesen, wie es das BVerfG seit der Volkszählungsentscheidung immer wieder hervorhebt.[282] *Haas'* Konzeption weist eine bedenkliche Nähe zum Modell eines autoritären Arkanstaats auf, dessen Bürgern mangels eigener Entscheidungsbefugnis auch kein Bedürfnis nach Transparenz zugesprochen wird. Aus diesem Grund gehen auch ihre Argumente bezüglich der nicht offenen Durchführung der Maßnahme ins Leere. Die Annahme der „faktischen Anonymität" durch die große Zahl der Betroffenen ignoriert zum einen die gesamtgesellschaftliche Ebene maßgeblicher Risiken, zum anderen die Möglichkeit schneller und einfacher Individualisierung auch extrem großer Datenbestände durch heutige Informationstechnologie. Schon die Durchführung der Maßnahme, die auf Gewin-

---

[279] BVerfGE 125, 260 (364 ff. und 380 ff.).

[280] Ebd., (366). Vgl. auch unten II.B.13.

[281] BVerfGE 125, 260 (383). Zu Profilen bereits oben Teil 1, II.C.

[282] BVerfGE 65, 1 (43).

nung verwertbarer personenbezogener Daten zielt, zeigt, dass von einer Anonymität gerade nicht die Rede sein kann.

Bedenklich ist insbesondere auch ihr Vergleich mit der Zugänglichkeit der in die Rasterfahndung einbezogenen Merkmale für jedermann. Zum einen ignoriert *Haas* damit das entscheidende Risiko der Informationsemergenz – die Gewinnung neuer, bislang unbekannter Aussagen aus vorhandenen Beständen. Im Fall der Rasterfahndung handelt es sich hierbei um die bei Vorliegen der spezifischen Merkmalskombination erhöhte Wahrscheinlichkeit, dass es sich bei der geprüften Person um einen verdeckt lebenden Terroristen (Schläfer) handelt. Zum anderen sind jedoch bereits die von *Haas* beschriebenen Situationen nicht vergleichbar: Die Kenntnisnahme durch staatliche Ermittlungsbehörden ist gerade nicht vergleichbar mit der Kenntnisnahme durch Private. Es handelt sich dabei um zwei verschiedene Risiken. Während es Privaten aufgrund des Autonomieprinzips[283] unbenommen ist, Informationen anderer Privater zur Kenntnis zu nehmen, ist dies bei staatlichen Ermittlungsbehörden anders: Es realisiert sich gerade kein „allgemeines Lebensrisiko", sondern eine staatliche Ermittlungsmaßnahme.[284]

### 10. Schutzgut „Vertrauen der Allgemeinheit"

Die in den älteren Entscheidungen stärker gesamtgesellschaftlich ausgerichtete Risikokonzeption findet neben der im Urteil zu *Telekommunikationsverbindungsdaten* enthaltenen individuellen Perspektive ebenfalls Berücksichtigung. Sie wird in der Angemessenheitsprüfung aufgegriffen. Ausgangspunkt ist die große Zahl betroffener Personen bei einer Zielwahlsuche. Unter Verweis auf die zweite *G-10*-Entscheidung wird sodann die gesamtgesellschaftliche Risikokonzeption mit der individuellen Ebene kombiniert: maßgeblich sei, wie viele Personen wie intensiven Beeinträchtigungen ausgesetzt werden.[285] An dieser Stelle wechselt das Urteil dann jedoch wieder auf die individuelle Ebene und grenzt die weite Eingriffskonzeption ein, indem es den Nicht-Treffern der Zielwahlsuche aus individueller Sicht keine Eingriffsqualität zuspricht. Eine solche hätte der oben dargestellten Risikokonzeption zufolge eigentlich gegeben sein müssen, da auch den Nicht-Treffern eine negative Aussage über die Herstellung einer Verbindung entnommen werden kann. Als Grund für die Einschränkung wird auch hier die rein maschinelle, anonyme, spurenlose und ohne Erkenntnisinteresse für die Strafverfolgungsbehörden erfolgende Verarbeitung im Fall der Nicht-Treffer angeführt.[286] Gleichwohl bleibe die „gesamtgesellschaftliche Bedeutung". Die Streubreite von Ermittlungsmaßnahmen

---

283 Siehe oben Teil 1, III.B.1.

284 Zu diesem Argument im Kontext des informationsrechtlichen Gesetzesvorbehalts vgl. *Mahlstedt*, Verdeckte Befragung, S. 183.

285 BVerfGE 107, 299 (327).

286 Ebd., (328).

trage zur Entstehung von Missbrauchsrisiken und des Gefühls des Überwachtwerdens bei. Explizit bezieht sich das Gericht dann auf das Schutzgut des Vertrauens der Allgemeinheit,[287] das sich den oben dargestellten gesamtgesellschaftlichen Risiken[288] zuordnen lässt.

### 11. Kernbereichslehre

Die Entscheidung des BVerfG zum *„großen Lauschangriff"*[289] hatte die Einführung der akustischen Wohnraumüberwachung zu Strafverfolgungszwecken zum Gegenstand. Sie befasst sich mit Änderungen des Art. 13 GG und mit Vorschriften der StPO zur Durchführung der Wohnraumüberwachung. Das Urteil hat übergreifende Bedeutung für datenschutzrechtliche Fragestellungen, da der Prüfungsmaßstab die Menschenwürde, Art. 1 Abs. 1 GG, war.[290]

Die maßgebliche Kernaussage liegt in der Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung, bei dessen Betroffenheit keine Abwägung nach Maßgabe des Verhältnismäßigkeitsprinzips durchgeführt werden dürfe, auch wenn hochrangige Gemeinwohlinteressen, wie die Effektivität der Strafrechtspflege, betroffen seien.[291] Hierzu etabliert das Gericht ein abgestuftes Schutzkonzept, wonach dem Schutz des Kernbereichs in allen Phasen der Informationsverarbeitung Rechnung getragen werden muss.[292] Die Risiken für das Schutzgut Menschenwürde werden in Anlehnung an das Volkszählungsurteil und die oben im Rahmen des Abschnitts zu Persönlichkeitsprofilen genannten Entscheidungen[293] beschrieben: Eine nahezu lückenlose, alle Bewegungen und Lebensäußerungen umfassende Registrierung könne Grundlage für ein Persönlichkeitsprofil werden und verletze deshalb die Menschenwürde.[294] Jenseits des absolut geschützten Kernbereichs wird die Eingriffsintensität in Anlehnung an das Urteil zu *Telekommunikationsverbindungsdaten* bestimmt. Insbesondere werden Einschüchterungseffekte und Befangenheit der Kommunikation genannt.[295] Aber auch die Kommunikation in ihrer „gesamtgesellschaftlichen Bedeutung" wird laut Entscheidung vom objektivrechtlichen Gehalt des Art. 13 GG umfasst.[296] Im Übrigen ist auf

---

287 Ebd., (328).

288 Siehe oben II.B.5.

289 BVerfG Urteil vom 3.3.2004, 1 BvR 2378/98, 1084/99 *(Großer Lauschangriff)* = BVerfGE 109, 279.

290 Ebd., (311).

291 Ebd., (313 f.).

292 Ebd., (318 f.).

293 Siehe oben II.B.8.

294 BVerfGE 109, 279 (323).

295 Ebd., (353 f.).

296 Ebd., (354 f.).

die Ausführungen zu Schutzgütern und Risikokonzeptionen des Urteils zu *Telekommunikationsverbindungsdaten* zu verweisen.[297]

In dem noch am gleichen Tag ergangenen Beschluss zum *Zollkriminalamt* bzw. zur *Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz*[298] übernimmt das BVerfG die Grundsätze aus dem Urteil zu *Telekommunikationsverbindungsdaten* und befasst sich daneben umfassend mit den Bestimmtheitsanforderungen an Überwachungsmaßnahmen.[299] Risiken und Schutzgüter werden zwar als abwägungsrelevant dargestellt, jedoch nicht näher präzisiert: Die Einschätzung der „Schwere der dem Schutzgut drohendenden Gefahr" setze Klarheit „nicht nur über das gefährdete Rechtsgut, sondern auch über die dieses gefährdende Handlung" voraus.[300] In der Entscheidung zur *präventiven Telekommunikationsüberwachung* wird das Schutzkonzept schließlich auch auf Art. 10 Abs. 1 GG übertragen.[301]

Auffällig an der Kernbereichslehre ist die Rückkehr zu einem räumlichen, sphärenartigen Schutzkonzept, dessen Umschreibung an die Wesensgehaltsgarantie der Grundrechte, Art. 19 Abs. 2 GG, erinnert.

### 12. Überwachungskumulation

Der kumulative Einsatz verschiedener Überwachungsmaßnahmen war Gegenstand der Entscheidung des Bundesverfassungsgerichts zu *GPS-Beweiserhebungen*.[302] Der Ausgangsfall wurde auch vom EGMR überprüft, der Sachverhalt und das maßgebliche Risiko der „Überwachungskumulation" bereits oben analysiert.[303] Das BVerfG sieht das Risiko in der Ausgangsentscheidung ebenfalls, hält jedoch eine gesonderte gesetzliche Regelung für den Einsatz mehrerer Ermittlungsmaßnahmen zur selben Zeit nicht für erforderlich: Eine „stets unzulässige Rundumüberwachung", welche die Erstellung eines umfassenden Persönlichkeitsprofils ermögliche, könne durch allgemeine verfahrensrechtliche Sicherungen ausgeschlossen werden.[304] Das BVerfG bezeichnet die erforderlichen Kooperations- und Abstimmungserfordernisse deshalb einprägsam als „grundrechtssichernde Abstimmung der Ermittlungstätigkeit".[305]

---

297 Siehe oben II.B.8.

298 BVerfG Beschluss vom 3.3.2004, 1 BvF 3/92 *(Zollkriminalamt)* = BVerfGE 110, 33.

299 BVerfGE 110, 33 (53 ff.).

300 Ebd., (55).

301 BVerfGE 113, 348 (390 f.).

302 BVerfG Urteil vom 12.4.2005, 2 BvR 581/01 *(GPS-Daten)* = BVerfGE 112, 304.

303 Siehe oben Teil 1, IV.B.1.a).

304 BVerfGE 112, 304 (319).

305 Ebd., (320).

Die hier verfolgte Risikokonzeption folgt der „Nadelstich-Theorie", wonach viele kleine Stiche letztlich auch zu einer größeren Schutzgutverletzung führen und damit auch in ihrer Gesamtheit eine andere Qualität erreichen können. Eine ähnliche Argumentation wurde auch im Rahmen der oben dargestellten Entscheidungen zur Kategorie Persönlichkeitsprofile vom Verfassungsgericht verfolgt.[306]

### 13. Risiken privater Datenverarbeitungen

In dem Kammerbeschluss vom 23.10.2006 befasst sich das BVerfG mit einer versicherungsvertraglichen Obliegenheit zur *Schweigepflichtentbindung*.[307] Wie bereits oben angesprochen, kommt der Frage der Privatrechtsgeltung des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG unter den derzeitigen Bedingungen der Datenverarbeitung besondere Bedeutung und auch erhebliches wissenschaftliches Interesse zu.[308]

Der Entscheidung lag die von einer Berufsunfähigkeitsversicherung geforderte Abgabe einer Schweigepflichtentbindung zur Einholung „sachdienlicher Auskünfte" u.a. bei Ärzten, Behörden und früheren Arbeitgebern zugrunde. Beachtenswert ist zunächst die ausdrückliche Anerkennung einer staatlichen Schutzpflicht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG mit objektiver Wirkung auch für das Privatrecht.[309] In der Entscheidung führt das Gericht aus, dass sich dem Allgemeinen Persönlichkeitsrecht zwar kein „dingliches Herrschaftsrecht über bestimmte Informationen" entnehmen lasse und die Gestaltung der Kommunikationsbeziehungen in Privatrechtsverhältnissen auch grundsätzlich dem Einzelnen selbst obliege. Staatliche Verantwortung hinsichtlich der Gewährleistung der „Voraussetzungen selbstbestimmter Kommunikationsteilhabe" liege jedoch dort vor, wo informationeller Selbstschutz nicht möglich sei.[310] Eben dieser Selbstschutz – etwa durch abweichende Vertragsgestaltung – war der Versicherungsnehmerin aufgrund der faktisch einseitigen Bestimmbarkeit des Vertragsinhalts durch den weit überlegenen Vertragspartner ‚Versicherung' verwehrt. Die Überlegenheit ergab sich zudem daraus, dass die von der Versicherung angebotene Leistung von erheblicher Bedeutung zur Sicherung der persönlichen Lebensführung war. Das Gericht führt hierzu die Bedeutung von Berufsunfähigkeitsversicherungen aufgrund der unzureichenden gesetzlichen Absicherung an. Der Verzicht auf einen Vertragsschluss zur Vermeidung der Preisgabe von Informationen sei der Versicherungsnehmerin deshalb unzumutbar.[311]

---

306 Siehe oben II.B.8.

307 BVerfG Beschluss vom 21.10.2006, 1 BvR 2027/02 *(Schweigepflichtentbindung)* = MMR 2007, 93.

308 Dazu bereits oben I.B.

309 BVerfG Beschluss vom 21.10.2006, 1 BvR 2027/02 *(Schweigepflichtentbindung)* Rn. 31.

310 Ebd. Rn. 32 f.

311 Ebd. Rn. 35–39.

Die Entscheidung nimmt damit zwar keine Stellung zu einschlägigen Risiken privater Datenverarbeitungen, verdeutlicht jedoch mit der Forderung nach der selbstbestimmungsermöglichenden Gestaltung von Kommunikationsbeziehungen erneut die Bedeutung, die das Verfassungsgericht dem Schutzgut Selbstbestimmung zumisst.

In der Entscheidung des BVerfG zur *Vorratsdatenspeicherung*[312] werden Risiken privater Datenverarbeitungen zwar aufgegriffen, eine wirklich vertiefte Auseinandersetzung fehlt aber auch dort. Mangels Handlungsspielraum der speicherungspflichtigen privaten Anbieter wird zunächst der mit der Speicherung verbundene Eingriff dem Gesetzgeber unmittelbar zugerechnet.[313] Die Verteilung der Speicherpflichten auf zahlreiche private Diensteanbieter wird zudem als Argument für die Verhältnismäßigkeit im engeren Sinne herangezogen, da der Staat keinen unmittelbaren Zugriff auf die Daten hat.[314] Die Gefahr des Missbrauchs und illegalen Zugriffs thematisiert die Entscheidung im Rahmen der Überprüfung der konkreten Ausgestaltung, wobei die „Bedingungen von Wirtschaftlichkeit und Kostendruck" und damit die nur „begrenzten Anreize zur Gewährleistung von Datensicherheit" als Risikofaktoren für die Notwendigkeit eines höheren Datensicherheitsniveaus genannt werden.[315]

Unter dem gegenteiligen Aspekt einer Risikoverminderung wird hingegen die private Speicherung in der abweichenden Meinung von *Schluckebier* betrachtet: Es fehle „jede objektivierbare Grundlage für die Annahme eines eingriffsintensivierenden Einschüchterungseffekts"; und auch das in der Entscheidung herangezogene Gefühl „des ständigen Überwachtwerdens" und einer „diffusen Bedrohlichkeit" lehnt *Schluckebier* gerade wegen der privaten Speicherung ab. Die Betroffenen brächten den privaten Stellen „das bei Vertragsschlüssen solcher Art vorauszusetzende Grundvertrauen" entgegen. Dem Erfordernis eines höheren Datensicherheitsniveaus stimmt er gleichwohl zu.[316] Dieser Sichtweise schließt sich auch *Eichberger* in seiner abweichenden Meinung an. Bemerkenswert dabei ist die Einforderung eines empirischen Belegs für den von der Senatsmehrheit angenommenen Einschüchterungseffekt.[317]

Die Risiken privater Datenverarbeitungen haben damit in der Rechtsprechung bisher in zwei Ausprägungen ihren Niederschlag gefunden: einerseits in Form einer Gefährdung selbstbestimmter Kommunikationsteilhabe Kommunikationsteilhabe in Privatrechtsverhältnissen, bei denen die Verhandlungsmacht einer Partei voll-

---

[312] BVerfG Urteil vom 2.3.2010, 1 BvR 256, 263, 586/08 *(Vorratsdatenspeicherung)* = BVerfGE 125, 260.

[313] BVerfGE 125, 260 (311).

[314] Ebd., (321).

[315] Ebd., (325).

[316] Ebd., (366).

[317] Ebd., (380 f.).

kommen überwiegt – exemplarisch hierfür ist die Entscheidung zur Schweigepflichtentbindung. Die andere Ausprägung basiert auf dem Risiko individueller Verletzlichkeit, welches durch die Funktionslogik privater Akteure als besonders hoch eingestuft wird. Beachtenswert ist zudem die Ablehnung eines Einschüchterungseffekts aufgrund der privaten Speicherung durch die beiden abweichenden Meinungen zur Vorratsdatenentscheidung, wobei insbesondere die Einforderung empirischer Nachweise festzuhalten ist.

### 14. Einschüchterungseffekt bei juristischen Personen

In der bereits angesprochenen Entscheidung zu *Kontostammdaten*[318] wird auch die Gefährdungslage juristischer Personen thematisiert. Hierbei führt das Gericht aus, dass sich für das Allgemeine Persönlichkeitsrecht nicht allgemein angeben lasse, ob es seinem Wesen nach auf juristische Personen anwendbar sei. Staatliche informationelle Maßnahmen könnten jedoch „Gefährdungen oder Verletzungen der grundrechtlich geschützten Freiheit juristischer Personen herbeiführen und einschüchternd auf die Ausübung von Grundrechten wirken".[319] Hier wird also – unter Verweis auf die Entscheidung zu Anwaltsdaten – das Risiko von Einschüchterungen und Hemmung des Grundrechtsgebrauchs von der Individualebene konformistischer Verhaltensanpassungen auf die Ebene juristischer Personen übertragen. Diese Übertragung wurde in der zitierten Entscheidung zu den Anwaltsdaten noch nicht in gleicher Weise vollzogen.[320] Der Transfer erscheint insbesondere deshalb bemerkenswert, da in wirtschaftlichen Zusammenhängen aufgrund des *rational choice*-Paradigmas der Wirtschaftswissenschaft[321] von einer relativen Rationalität der Akteure ausgegangen wird und bei „rein theoretischer" Betrachtung aufgrund des unterstellten rechtmäßigen staatlichen Gebrauchs der Eingriffsgrundlagen und des rechtmäßigen Verhaltens der Unternehmen einer Einschüchterungswirkung der Boden entzogen wäre. Das Verhalten kann jedoch – durchaus bei Beibehaltung des o.g. Paradigmas – auch mit dem ggf. irrationalen Verhalten der Kunden erklärt werden. Beschwerdeführer waren u.a. ein Kreditinstitut und eine Anwaltskanzlei. So betrachtet verweisen die Ausführungen des Gerichts wieder auf die bereits oben besprochenen funktionalen Aspekte des Vertrauensbegriffs.[322]

Inkonsequent sind dann allerdings die Ausführungen des BVerfG im Anschluss an die Annäherung an funktionale Aspekte der Vertraulichkeitsbeeinträchtigung: Der Tätigkeitskreis juristischer Personen sei „anders als der natürlicher Personen"

---

318 Siehe oben II.B.9.

319 BVerfGE 118, 168 (203).

320 BVerfGE 113, 29 (46).

321 *Diekmann/Voss*, Rational Choice, 2003, http://www.uni-leipzig.de/~sozio/mitarbeiter/m27/content/eigene_site/prof.voss.public_2003b.pdf [Stand: 28.3.2014].

322 Siehe oben Teil 1, IV.B.5. und 6 sowie Teil 3, II.B.3.d).

in der Regel durch eine bestimmte Zwecksetzung begrenzt, woraus zu folgern sei, dass Unterschiede „zwischen den Schutzbedürfnissen" juristischer und natürlicher Personen bei der Bestimmung des Gewährleistungsgehalts zu beachten seien. Das Gericht konkretisiert diese Ausführungen, indem es die Beachtlichkeit der Gefährdungslage an die Zwecksetzung der juristischen Person knüpft, im Fall der Bank also an die kreditwirtschaftliche Tätigkeit. Es lehnt sodann die Gefährdung ab, da nur die Kunden betroffen seien und nicht das Kreditinstitut selbst.[323] Den naheliegenden Rückschluss von der wirtschaftlichen Beeinträchtigung des Kreditinstituts durch gesunkenes Kundenvertrauen bei Durchbrechung des Bankgeheimnisses vollzieht das BVerfG damit inkonsequenterweise nicht.

Fadenscheinig ist sodann auch die Begründung, mit der eine Beeinträchtigung des Mandantenverhältnisses im Fall des beschwerdeführenden Anwalts abgelehnt wird. Dieser verfüge über keine tatsächlichen Einflussmöglichkeiten auf die kontoführenden Kreditinstitute, und folglich realisiere sich im Fall des Zugriffs ein Offenbarungsrisiko, das der Anwalt „von vornherein nicht beherrschen kann".[324] Das Gericht verlässt insoweit die an den realen Auswirkungen des Informationseingriffs orientierte Grundrechtsauslegung und präsentiert stattdessen ein wenig überzeugendes dogmatisches Scheinargument. Dies erscheint auch deshalb überraschend, da in der Entscheidung zur *Vorratsdatenspeicherung* sogar das Risiko der Erstellung von Persönlichkeitsprofilen[325] auf „Gruppen und Verbände" ausgedehnt wird; maßgeblich sei dabei die Aufdeckung interner „Einflussstrukturen" und Entscheidungsabläufe.[326]

### 15. Informationstechnische Systeme

Das Urteil zur *Online-Durchsuchung* vom 27.2.2008[327] hat die Verwendung von Überwachungsprogrammen zu Ermittlungszwecken zum Gegenstand. Es enthält die bereits oben angesprochene Neuschöpfung eines Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme.[328] Die Entscheidung widmet sich damit dem hochaktuellen und nicht nur auf staatliche Datenverarbeitung beschränkten Risiko des Einsatzes von Spähsoftware (trojanische Viren).[329] Sie eignet sich auch hinsichtlich der zugrunde liegenden Risikokonzeption für eine nähere

---

323 BVerfGE 118, 168 (204 f.).

324 Ebd., (206 f.).

325 Siehe oben II.B.8.

326 BVerfGE 125, 260 (319).

327 Urteil vom 27.2.2008, 1 BvR 370, 595/07 *(Online-Durchsuchung)* = BVerfGE 120, 274.

328 Siehe oben I.A.

329 Zu Funktionen und Risiken derartiger Programme *Kaspersky*, Malware, S. 63 ff.

Analyse.[330] Hierzu ist im Folgenden die „Konstruktion" der Bedrohungslage durch das Gericht kurz nachzuvollziehen, da diese den Ausgangspunkt der gerichtlichen Risikoperzeption darstellt.

Das Gericht sieht das zentrale Risiko in einem durch die trojanischen Viren ermöglichten „Gesamtzugriff" auf die „äußerst großen und aussagekräftigen" Datenbestände informationstechnischer Systeme wie PCs, Laptops und Smartphones.[331] Es führt als Grundlage hierfür zunächst aus, dass informationstechnische Systeme „allgegenwärtig" und ihre Nutzung „für die Lebensführung vieler Bürger von zentraler Bedeutung" sei.[332] Hervorgehoben wird neben der Verbreitung auch die Leistungsfähigkeit der Systeme und ihre Verwendung für eine „Vielzahl unterschiedlicher Zwecke". Weiterhin verweist das Gericht auf informationstechnische Komponenten, die in Telekommunikationsgeräten sowie anderen elektronischen Geräten in Wohnungen und Kraftfahrzeugen enthalten sind und die zunehmende Bedeutung für die Persönlichkeitsentfaltung bei deren Vernetzung. Aufgrund der Internetnutzung weiter Teile der Bevölkerung erkennt das Gericht diese Vernetzung mittlerweile als Normalfall an. Bedeutung misst es auch der Möglichkeit des aktiven Aufbaus und der Pflege sozialer Verbindungen mittels neuer Kommunikationsdienste und dabei auftretender Konvergenzeffekte zu. Als Beispiel für diese Konvergenz führt es die Verlagerung der Sprachtelefonie auf das Internet an.[333] Risiken sieht das Gericht nicht nur in der bewussten Anlage und Speicherung von Daten durch den Nutzer, sondern auch in den selbsttätig durch das informationstechnische System generierten Daten im Rahmen von Datenverarbeitungsprozessen. Solche Daten könnten ebenso wie bewusst angelegte im Hinblick auf Verhalten und Eigenschaften des Nutzers ausgewertet werden. Diese Passage verweist mit dem Risiko von Kontrollverlust auf ein Verständnis der informationellen Selbstbestimmung als Schutzgut. Mit Bezug auf das Volkszählungsurteil stellt es sodann auf die Möglichkeit weiterreichender Rückschlüsse auf die Persönlichkeit des Nutzers „bis hin zur Profilbildung" ab. Als Beispiel für unbewusst erzeugte Daten führt das Gericht Daten im Arbeitsspeicher und auf den Speichermedien des Systems zu persönlichen Verhältnissen, sozialen Kontakten und ausgeübten Tätigkeiten des Nutzers an. In der Vernetzung, insbesondere über das Internet, sieht es sodann eine Vertiefung der Gefährdungen, die aus der größeren Vielzahl und Vielfalt der Daten folge.[334]

---

330 Zum Ganzen auch *Drackert*, eucrim 2011, 122 ff.

331 BVerfGE 120, 274 (313 f.)

332 Ebd., (303).

333 Ebd., (304).

334 Ebd., (305).

### *a) Risiko technischer Infiltration*

Die bis dahin im Urteil behandelten Risiken ließen sich auch anderen Informationseingriffen zuordnen. Ein spezifisches, mit dem Einsatz von Spähsoftware verbundenes Risiko thematisiert das Gericht jedoch im Anschluss unter dem Oberbegriff der Infiltration: Die Vernetzung des Systems eröffne Dritten eine technische Zugriffsmöglichkeit, mit der vorhandene Daten nicht nur ausgespäht, sondern auch manipuliert werden können.[335] Die Besonderheit von Eingriffen mittels trojanischer Viren bestehe nun darin, dass der Betroffene die Zugriffe teilweise nicht wahrnehmen und somit nur begrenzt abwehren könne. Aufgrund des hohen Komplexitätsgrads informationstechnischer Systeme bereite überdies der technische Selbstschutz erhebliche Schwierigkeiten, könne den durchschnittlichen Nutzer überfordern und zudem mit hohem Aufwand und Funktionseinbußen einhergehen. Auch würden Maßnahmen des Selbstschutzes wie beispielsweise die Verschlüsselung von Daten „weitgehend wirkungslos", wenn Dritten die Infiltration des Systems gelingt. Das Risiko der Infiltration wird deutlicher mittels Abgrenzung von der „Internetaufklärung", die das Gericht hiervon ausnehmen will: Demnach liegt eine Infiltration vor, wenn der Zugriff nicht auf dem technisch dafür vorgesehenen Weg erfolgt. Die Überwachung zugangsgesicherter Kommunikationsinhalte durch Nutzung oder Erhebung von Zugangsschlüsseln „ohne oder gegen den Willen" der Kommunikationsbeteiligten stellt eine Infiltration in diesem Sinne dar; wohingegen unter der Internetaufklärung die Erhebung von Daten verstanden wird, die der Inhaber des Systems für die Internetkommunikation bestimmt hat und die auf dem technisch dafür vorgesehenen Weg erhoben werden.[336] Das Gericht versteht unter der Infiltration also ausschließlich die „technische Infiltration".

### *b) Schutzgüter Vertraulichkeit und Integrität*

Neben der Infiltration als risikoauslösende Zugriffsmodalität geht das Gericht näher auf Schutzgüter ein, die es aus den Schutzbedürfnissen der Nutzer ableitet. Bemerkenswert ist, dass das BVerfG hier nicht nur auf das herkömmliche Schutzgut der „Vertraulichkeit" rekurriert, sondern auch die Integrität des informationstechnischen Systems miteinbezieht.[337] Hierzu führt das Gericht aus, dass die bisherigen Grundrechtsgarantien die beschriebenen Risiken nicht umfassend abdecken und deshalb eine neue Einzelverbürgung des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG – sozusagen als Kombination von alten und neuen Schutzgütern – anzuerkennen sei. Ergebnis dieser Kombination ist das Recht auf Vertraulichkeit und Integrität

---

[335] Ebd., (306).

[336] Ebd., (340 f., 344).

[337] Ebd., (306).

informationstechnischer Systeme.[338] Bei der Darstellung des Schutzbereichs der neuen Einzelverbürgung misst das Gericht der „Vertraulichkeits- und Integritätserwartung" des Nutzers besondere Bedeutung zu. Diese grundrechtlich anzuerkennende Erwartung bestehe unabhängig vom Zugriffsaufwand, solange das System eigengenutzt werde, wobei darunter auch ein gemeinschaftlicher berechtigter Gebrauch durch mehrere Personen zu sehen sei. Unschädlich sei es ferner, wenn die Nutzung des eigenen Systems „über informationstechnische Systeme stattfinde, die sich in der Verfügungsgewalt anderer befinden".[339]

### *c) Zwischenergebnis*

Das Urteil basiert damit auf zwei Risikokonzeptionen: Maßgebliches Risiko sind einerseits Rückschlüsse auf die Persönlichkeitsgestaltung des Einzelnen, die angesichts der quantitativen und qualitativen Veränderung der Nutzung informationstechnischer Systeme erneut an Bedeutung gewinnen. Des Weiteren weist das Gericht explizit darauf hin, dass das „Risiko einer Bildung von Verhaltens- und Kommunikationsprofilen" durch die Möglichkeit einer langfristigen Überwachung des Zielsystems erhöht wird und dass die damit ermöglichte weitgehende Ausforschung des Betroffenen einen Grundrechtseingriff „von besonders hoher Intensität" darstellt.[340] Diesem Risiko wird das Schutzgut der Vertraulichkeit zugeordnet.

Im Rahmen der Abgrenzung der Einzelverbürgungen informationelle Selbstbestimmung und Vertraulichkeit des Systems wird die Risikoänderung auf den Punkt gebracht: Es geht um den Gesamtzugriff – das Aufdecken weiter Teile der Persönlichkeitsgestaltung „auf einen Schlag".[341] Das Gericht greift damit den Nutzungsaspekt heutiger Informationstechnologie auf, der für viele plakativ eine „Auslagerung des Gehirns" darstellt. Zum anderen stützt sich das Gericht jedoch auch auf das Risiko der verdeckten Manipulation von Daten, welches dem Missbrauch gerade durch staatliche Stellen Tür und Tor öffnet. Es ist nicht nur „praktisch unvermeidbar", Informationen zur Kenntnis zu nehmen, bevor deren Kernbereichsbezug bewertet werden kann. Möglich ist sogar die Einspielung fingierten Beweismaterials aufgrund der technischen Öffnung des Systems.[342] Das Gericht sieht zwar die

---

338 Ebd., (305–315).

339 Ebd., (315).

340 Ebd., (324 f.).

341 Ebd., (313 f., 324).

342 Hierzu ist anzumerken, dass staatlichen Ermittlungsbehörden ein derartiges Verhalten nicht pauschal unterstellt werden darf. Hinsichtlich der Grundrechtsrelevanz müssen jedoch offensichtliche Missbrauchsmöglichkeiten einkalkuliert werden. Insbesondere der extrem weitgehende Funktionsumfang der von Ermittlungsbehörden eingesetzten Spähsoftware (beispielsweise die Nachladefunktion, die es dem Trojaner ermöglicht, weitere Software mit vielfachen Funktionen auf das System aufzuspielen) unterstreicht dieses Erfordernis. Zu den Funktionen vgl. http://www.sueddeutsche.de/digital/ueberwachungssoftware-ungeklaerte-fragen-der-staatstrojaner-affaere-1.1283378 [Stand: 28.3.2014].

Möglichkeit, den „vollständigen Kontrollverlust“ des Betroffenen durch „geeignete Verfahrensvorschriften“ abzuschirmen.[343] Die Anhörung der sachkundigen Auskunftspersonen in der Verhandlung ergab jedoch, dass es keinen „rein lesenden“ Zugriff beim Einsatz der Überwachungssoftware gibt und deshalb auch eine Verursachung von Schäden am Zielsystem nicht ausgeschlossen werden könne.[344] Dem damit umrissenen Infiltrationsrisiko lässt sich somit das zweite Schutzgut der neuen Einzelverbürgung – die Integrität des informationstechnischen Systems – zuordnen.

### 16. Aufklärung öffentlich zugänglicher Internetinhalte

Das Urteil zur *Online-Durchsuchung* vom 27.2.2008[345] widmet sich jedoch nicht nur den Fragen der Infiltration informationstechnischer Systeme durch Schadprogramme, sondern hat auch die sonstige heimliche Internetaufklärung zum Gegenstand. Obwohl die Ausführungen zur Internetaufklärung teilweise Züge eines *obiter dictum* tragen, verdienen sie aufgrund der Widersprüche zu den Übrigen Risikokonzeptionen des BVerfG und aufgrund der praktischen Relevanz, der ihnen insbesondere seitens der Strafverfolgungsbehörden zugemessen wird, eine nähere Analyse.

#### *a) Vertraulichkeitserwartung im Internet*

Unter der „Internetaufklärung“ versteht das BVerfG Maßnahmen, bei denen vom Systeminhaber für die Internetkommunikation bestimmte, also insbesondere öffentlich zugängliche Daten auf dem technisch dafür vorgesehenen Weg erhoben werden.[346] Das Gericht sieht hier keine Berührung der neuen Einzelverbürgung des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, da der Betroffene sein System für die Erhebungen „selbst technisch geöffnet“ habe.[347] In der Regel sei auch ein Eingriff in das Recht auf informationelle Selbstbestimmung zu verneinen, da es dem Staat „grundsätzlich nicht verwehrt“ sei, öffentlich zugängliche Informationen, wie beispielsweise die Informationen einer Internetseite, zur Kenntnis zu nehmen.[348] Die Grenze zieht das Gericht dort, wo Informationen, „die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden“, soweit

---

[343] Die praktischen Schwierigkeiten erkennt das Gericht zwar, sieht in ihnen aber kein grundsätzliches Erhebungshindernis, BVerfGE 120, (336 ff.).

[344] BVerfGE 120, 274 (325 f.)

[345] Urteil vom 27.2.2008, 1 BvR 370, 595/07 *(Online-Durchsuchung)* = BVerfGE 120, 274.

[346] Ebd., (344).

[347] Ebd.

[348] Ebd., (344 f.).

sich daraus eine „besondere Gefährdungslage für den Betroffenen“ ergibt.[349] Weiterhin führt das Gericht aus, dass ein Eingriff nicht schon dann vorliege, „wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt“. Erforderlich sei vielmehr ein „schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners“. Dieses Vertrauen müsse ausgenutzt werden, um persönliche Daten zu erheben, welche die Behörde andernfalls nicht erhalten würde.[350] Im Folgenden räsoniert das BVerfG über das Bestehen derartigen Vertrauens bei Nutzung der „Kommunikationsdienste des Internet“. Dort sei das Vertrauen in die Identität und Wahrhaftigkeit der Kommunikationspartner nicht schutzwürdig, da hierfür „keinerlei Überprüfungsmechanismen“ bereitstünden. Dies gelte selbst dann, wenn die Kommunikation über einen längeren Zeitraum erfolge und sich eine Art „elektronische Gemeinschaft“ gebildet habe. Auch in diesem Fall sei „jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann“. Das Vertrauen auf die Nichtkommunikation mit einer staatlichen Stelle sei deshalb nicht schutzwürdig.[351]

### *b) Öffentlich zugängliche Quellen*

Eine Bestätigung und nähere Ausgestaltung findet diese Ablehnung des Eingriffs bei allgemein zugänglichen Inhalten in der kurz darauf ergangenen Entscheidung zu Auskunftsansprüchen gegen das Bundesamt für Finanzen.[352] Dort verlangte der Antragsteller Auskunft über auf Grundlage von § 88a AO gespeicherte Informationen, die aus im Ausland öffentlich zugänglichen Quellen stammten und die den Finanzbehörden zur Beurteilung der steuerlichen Absetzbarkeit von Zahlungen an Auslandsgesellschaften dienen. Die maßgebliche Auseinandersetzung mit den Risiken findet sich im Rahmen der Eingriffsprüfung. Hier fällt zunächst auf, dass nicht wie in der Vorentscheidung von „allgemein zugängliche[n] Daten“,[353] sondern von Daten aus „öffentlich zugänglichen Quellen“[354] gesprochen wird. Auch wenn dies im konkreten Fall in der Sache keinen Unterschied macht, liegt es nahe, darin eine Modifizierung des Konzepts zu sehen: Während bei allgemein zugänglichen Daten tatsächlich jedermann zugriff haben müsste, kann bei öffentlich zugänglichen Daten nach Teilöffentlichkeiten unterschiedlicher Größe differenziert werden.

---

[349] Ebd., (345).

[350] Ebd.

[351] Ebd., (345 f.).

[352] BVerfG Beschluss vom 10.3.2008, 1 BvR 2388/03 *(Steuerdaten)* = BVerfGE 120, 351.

[353] BVerfGE 120, 274 (341).

[354] BVerfGE 120, 351 (361).

Eine nähere Bestimmung erfolgt sodann im Rahmen der Eingriffsprüfung. Ein Eingriff liege demnach bei Daten aus öffentlich zugänglichen Quellen – im Gegensatz zu Daten, die schon für sich genommen sensibel sind – nicht ohne Weiteres schon in der Erhebung.[355] Er könne dagegen auch bei öffentlich zugänglichen Daten vorliegen, wenn sie in eine Sammlung aufgenommen und systematisch erfasst werden. Dem Staat sei es nicht verwehrt, „von jedermann zugänglichen Informationsquellen unter denselben Bedingungen wie jeder Dritte Gebrauch zu machen".[356] „Grundrechtserhebliche Auswirkungen auf Privatheit und Verhaltensfreiheit" könnten jedoch auch bei Daten, die „für sich genommen keine besondere Relevanz" aufweisen, je nach dem „Ziel und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten" auftreten.[357] Ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung sei anzunehmen, wenn die aus öffentlich zugänglichen Quellen gewonnenen Daten durch „systematische Erfassung, Sammlung und Verarbeitung einen zusätzlichen Aussagewert erhalten, aus dem sich die für das Grundrecht auf informationelle Selbstbestimmung spezifische Gefährdungslage für die Freiheitsrechte oder die Privatheit des Betroffenen" ergebe. Als Beispiel führt das Gericht die Verbindung der öffentlichen mit anderen, bereits für sich genommen sensiblen Daten auf. In diesem Fall nehme der Aussagegehalt der verknüpften Daten insgesamt zu.[358]

### *c) Übertragbarkeit auf Inhalte sozialer Netzwerke*

Die Konzeption zu den allgemein zugänglichen bzw. aus öffentlichen Quellen stammenden Daten erweist sich bei näherer Überprüfung zumindest als unvollständig und in einem wichtigen Anwendungsfall sogar als untauglich.[359] Sie greift die tatsächlichen Eigenarten der Kommunikationsbeziehungen im Internet nicht hinreichend auf und steht damit in Widerspruch zu der im gleichen Urteil entwickelten Risikokonzeption sowie dem Schutzbedürfnis der Grundrechtsberechtigten. Darüber hinaus erweist sie sich auch offen für eine Lesart, die unvereinbar mit der Funktion des Gesetzesvorbehalts[360] im Bereich des Informationsrechts ist. Vonseiten der Exekutive und der Strafverfolgungsbehörden wird die Passage zur Internetaufklärung in BVerfGE 120, 274 verständlicherweise sehr positiv aufgenommen und für eine relativ weitgehende Zulässigkeit von Ermittlungen im Internet mangels „Grundrechtsrelevanz" herangezogen.[361]

---

355 Ebd., (361).

356 Ebd.

357 Ebd., (362).

358 Ebd.

359 Zum Ganzen *Drackert*, eucrim 2011, 122 ff.

360 Epping/Hillgruber-*Huster/Rux*, Art. 20 Rn. 159–167; Maunz/Dürig-*Herzog/Grzeszick*, Art. 20 Rn. 83 sowie Rn. 111–115.

361 Vgl. die Antwort der Bundesregierung auf eine kleine Anfrage der Fraktion „Die Linke", elektronische Vorabfassung, Deutscher Bundestag, 17. Wahlperiode, Drs. 17/6587

Eine vertiefte Auseinandersetzung muss zwar angesichts der auf die Risikokonzeptionen und Schutzgüter eingegrenzten Fragestellung dieser Arbeit einer eigenen Untersuchung vorbehalten bleiben;[362] gleichwohl sollen hier die wichtigsten Einwände dargestellt werden, da sie die Unvollständigkeit der Risikokonzeptionen des Urteils zur Online-Durchsuchung verdeutlichen. Besonders gut lassen sich die Schwächen der BVerfG-Konzeption zu Identitätsvertrauen und allgemein zugänglichen Informationen am Beispiel von Ermittlungen in sozialen Netzwerken zeigen. Diese Kommunikationsform ist aufgrund der erheblichen Nutzerzahlen besonders relevant und stößt auch auf erhebliches Ermittlungsinteresse bei Polizeibehörden.[363]

Die Ausführungen zum schutzwürdigen Identitätsvertrauen in der Entscheidung sind zunächst deshalb wenig aussagekräftig, da sie anhand herkömmlicher – „Web 1.0" – Internetseiten entwickelt wurden. Die zugrunde liegende, vom BVerfG auch im Urteilstext zitierte Literaturkonzeption von *T. Böckenförde*[364] wurde 2003 am Beispiel offener und geschlossener Chatgruppen entwickelt. Diese Gruppen waren jedoch hinsichtlich der Verfügbarkeit von Inhalten und ihrer Funktionen weit von den Möglichkeiten entfernt, welche soziale Netzwerke heute bieten. Die alten Chatgruppen dienten nicht primär der Identitätsdarstellung und enthielten nicht die typische Verbindung verschiedener Informationsarten – Bilder, Kommunikation, statische Informationen und tagebuchartigen Ausführungen – wie sie prägend für die sozialen Netzwerke ist. Zumindest auf diesen bedeutsamen Fall lassen sich die Ausführungen des BVerfG deshalb schon aufgrund anders gelagerter Risiken nicht übertragen. Dies wird besonders deutlich, wenn man die zuvor anhand der technischen Infiltration entwickelte Risikokonzeption eines „Gesamtzugriffs" gegenüberstellt. Gerade die Enthüllung wesentlicher Teile der Persönlichkeit „auf einen Schlag" wird auch – zwar nicht in gleichem Ausmaß, aber durchaus ähnlich zur technischen Infiltration – durch die Erhebung von Daten sozialer Netzwerke ermöglicht. Der auf Profilseiten verfügbare Datenbestand bietet insbesondere deshalb weitgehende Rückschlüsse auf Lebensgewohnheiten des Anwenders, da viele der eingestellten Inhalte mit Zeit- und Ortsangaben versehen sind und fortlaufend generiert werden. Weiterhin kann der Online-Status sichtbar sein und damit der aktuelle Aufenthaltsort nachvollzogen werden. Nutzbar sind zudem biometrische Auswertungsdienste der Netzwerke z.B. über „Markierungsvorschläge" für abgebildete Personen.[365] Gerade die hieraus folgenden Ermittlungsansätze sind in ihrer Bedeutung noch gar nicht erkannt worden. So verfügt Facebook über das weltweit größte

---

sowie vonseiten der Strafverfolgungsbehörden *Henrichs/Wilhelm*, Kriminalistik 2010, 30 (35) sowie *Rosengarten/Römer*, NJW 2012, 1764 (1766).

362 Vgl. auch *Drackert*, eucrim 2011, 122 ff.

363 *Henrichs/Wilhelm*, Kriminalistik 2010, 30 ff.; *dies.*, Deutsche Polizei Nr. 10 (2010), 6 ff.

364 *Böckenförde*, Die Ermittlung im Netz, zit. in: BVerfGE 120, 274 (344).

365 *Drackert*, eucrim 2011, 123 f.

Bildarchiv und macht dies – zumindest in den USA – auch der biometrischen Auswertung zugänglich. Ohne Weiteres könnten Strafverfolgungsbehörden Bilder verdächtiger Personen in einen eigens dafür kreierten Account einstellen, um so beispielsweise mögliche Verbindungen zu anderen Personen oder auch Teilnahmen an bestimmten Veranstaltungen, zu denen Fotos vorliegen, herauszufinden. Eine pauschale Ablehnung schutzwürdigen Identitätsvertrauens, wie sie bei einer bloßen Übertragung der BVerfG-Konzeption vorgenommen würde, würde die Offenheit des Art. 2 Abs. 1 i.V.m. Art. 1 Abs.1 GG für neue Gefährdungslagen gerade verhindern.

Auch die wesentlichen Argumente, welche für die Eingriffsablehnung bei Daten aus öffentlich bzw. allgemein zugänglichen Quellen sprechen, sind auf Informationen aus sozialen Netzwerken nicht übertragbar. Wie oben dargestellt,[366] zeichnen sich die vom BVerfG vorgestellten öffentlichen Quellen durch Nicht-Sensibilität der eingestellten Informationen aus. Dies ist bei Informationen in sozialen Netzwerken anders.[367] Weiterhin liegt aber auch gerade der eingriffsauslösende „Mehrwert" von Informationen, der aus der Verknüpfung und systematischen Speicherung folgt, wie dargestellt auch bei sozialen Netzwerken vor. Dass die Verknüpfung und Generierung von höheren Aussagewerten durch den Betreiber des sozialen Netzwerks und nicht durch unmittelbare Verarbeitung der Ermittlungsbehörden erfolgt, ist aus der allein maßgeblichen Perspektive des Grundrechtsbetroffenen belanglos.

Die Anbindung der Gewährleistung an überprüfbares Identitätsvertrauen[368] trägt darüber hinaus dem spezifischen Schutzbedürfnis von Fernkommunikation, insbesondere auch internetbasierter Kommunikation, nicht hinreichend Rechnung: Die Nichtkenntnis des Kommunikationsteilnehmers ist bei jeder Fernkommunikation möglich und liegt in der Natur dieser Kommunikationsweise. Sie taugt deshalb nicht als Abgrenzungskriterium auf der Ebene von Schutzbereich und Eingriff. Dies zeigt bereits der Vergleich mit herkömmlicher Mobiltelefonie. Auch dort kann trotz Vorlage eines Personalausweises bei der Anmeldung des Mobilfunkvertrags nicht ausgeschlossen werden, dass eine andere Person das Telefon nutzt. Darüber hinaus ist es gerade das Erfolgs- und Geschäftskonzept der Internetkommunikation, dass sie nicht abhängig von umständlichen Registrierungsprozessen wie beispielsweise dem Post-Ident-Verfahren oder einer Authentifizierung mit dem neuen Personalausweis ist.[369] Diese Einfachheit der Kommunikation ist nicht zuletzt auch aufgrund von Art. 5 Abs. 1 GG und Art. 12 Abs. 1 GG in besonderem Maße schützenswert. Darüber hinaus erweist sich die Argumentation mit „fehlendem Identi-

---

366 Siehe oben II.B.16.b).

367 *Drackert*, eucrim 2011, 122 ff.

368 So im Anschluss an das BVerfG auch *Seidl/Beyvers*, jurisAnwZert ITR Nr. 15 (2011), Anm. 3.

369 Zu diesen Verfahren *Möller*, NJW 2005, 1605 ff.; *Borges*, NJW 2010, 3334 ff.

tätsvertrauen“ auch als zirkelschlüssig, da zumindest nicht in allen Fällen eine wirkliche und absolute Anonymität vorliegt und häufig – wie das Ermittlungsinteresse zeigt – der tatsächliche Nutzer eben doch ermittelt werden kann.[370]

Zur Rechtfertigung des Postulats fehlender Schutzwürdigkeit wird vielfach, insbesondere auch von Praktikern, vorgebracht, es handele sich bei Ermittlungen in sozialen Netzwerken um Maßnahmen, die jedermann vornehmen könnte und die deshalb auch den Ermittlungspersonen nicht vorenthalten werden dürften.[371] Diesem auch im Urteil des BVerfG zur Online-Durchsuchung anklingenden[372] und im Beschluss zu den Steuerdaten explizierten[373] Postulat kommt indes bei genauerer Betrachtung zumindest dann keine rechtliche Überzeugungskraft zu, wenn die Informationserhebung wie im Fall der „virtuellen verdeckten Ermittler“ mittels kommunikativem Kontakt und unter bewusster Identitätstäuschung, also ohne Offenlegung des Ermittlungszwecks, erfolgt. Insbesondere laufen diese Maßnahmen der zentralen Funktion des Vorbehalts des Gesetzes entgegen. Der Grundsatz, wonach exekutivisches Handeln einer gesetzlichen Grundlage bedarf, dient vor allem der Sicherstellung von Transparenz und Voraussehbarkeit staatlichen Handelns.[374] In Verbindung mit dem allgemeinen Freiheits- bzw. Autonomieprinzip stellt er die Abkehr vom absolutistischen Wohlfahrts- und Polizeistaat sicher: Der Staat darf zwar die Freiheitsausübung der Menschen regeln; Ausgangspunkt und Normalfall bleiben aber stets die Begrenzung des Staatshandelns und das Erfordernis ausdrücklicher Befugniseinräumung.[375] Zwar wandelte sich der aus Gedanken der Aufklärung gewonnene Grundsatz des Vorbehalts des Gesetzes durch die umfassende demokratische Legitimation der Staatsgewalt unter der Ägide des Grundgesetzes; auch bewirkt das Erfordernis der Schutzgewährleistung gegenüber neuen Gefährdungen eine Zunahme der Exekutivbedeutung.[376] Ermittlungsmaßnahmen müssen gleichwohl für die Einzelnen vorhersehbar sein. Das BVerfG selbst sieht diese enge Verbindung zwischen Parlamentsvorbehalt und Bestimmtheitsgebot: Der Parlamentsvorbehalt habe sicherzustellen, dass Entscheidungen einer bestimmten Tragweite „aus einem Verfahren hervorgehen, das der Öffentlichkeit Gelegenheit bietet, ihre Auffassungen auszubilden und zu vertreten, und die Volksvertre-

---

370 Hierauf weisen zutreffend *Schulz/Hoffmann*, CR 2010, 131 (134), hin.

371 Der Verfasser hat diesen Einwand insbesondere bei seinen im Jahr 2012 auf Praktikertagungen der Katholischen Akademie Trier gehaltenen Vorträgen vorwiegend von Staatsanwälten und Kriminalbeamten häufig zu hören bekommen. Link zum Tagungsprogramm: http://cms.bistum-trier.de/bistum-trier/Integrale?MODULE=Frontend.Media&ACTION=ViewMediaObject&Media.PK=27873&Media.Object.ObjectType=full [Stand: 28.3.2014].

372 BVerfGE 120, 274 (344 f.): „[…] eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat gundsätzlich nicht verwehrt“.

373 BVerfGE 120, 351 (361).

374 Statt vieler Epping/Hillgruber-*Huster/Rux,* Art. 20 Rn. 160.

375 Vgl. *Hufen*, Staatsrecht II, § 1 Rn. 12, S. 6 f.

376 Vgl. Maunz/Dürig-*Herzog/Grzeszick,* Art. 20 Rn. 86 f.

tung dazu anhält, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären."[377]

Die Verwaltung muss „steuernde und begrenzende Handlungsmaßstäbe" vorfinden, der betroffene Bürger sich auf mögliche belastende Maßnahmen einstellen können.[378]

Dies scheint hier zunächst der Fall zu sein, da – wie das BVerfG ausführt – niemand darauf vertrauen kann, nicht mit staatlichen Stellen zu kommunizieren.[379] In der Tat entspricht es auch dem allgemeinen Lebensrisiko, sich in der Identität eines Kommunikationspartners im Internet zu täuschen. Wenn Ermittlungsbehörden informelle Informationserhebungen durchführen und sich dabei die Identitätstäuschung des Betroffenen zunutze machen bzw. diese erst hervorrufen, verwirklicht sich jedoch kein solches allgemeines Lebensrisiko, sondern eine staatliche Ermittlungsmaßnahme. Diese ist schon aufgrund des Risikos von Anschlussermittlungen und der in der Rechtsprechung anerkannten höheren Gefahr von Verhaltensbeeinträchtigungen bei staatlicher Informationskenntnisnahme[380] nicht vergleichbar mit Informationserhebungen Privater, sondern stellt ein Aliud hierzu dar. Mit verdeckten Ausforschungen muss in einem Rechtsstaat – anders als in einem Polizeistaat – grundsätzlich niemand rechnen. Entscheidend ist vielmehr die Frage, ob eine Ermächtigungsgrundlage für solche Informationserhebungen existiert. Erst wenn eine einschlägige Ermächtigungsgrundlage für derartige Täuschungen besteht, ist das Vertrauen in der Tat normativ nicht schutzwürdig.[381]

Anzumerken ist gleichwohl, dass hieraus noch keine Aussage über die Eignung bestehender Rechtsgrundlagen oder das rechtspolitische Erfordernis der Schaffung solcher Grundlagen getroffen ist. Aus rechtsstaatlichen Gründen scheint es jedoch geboten, Praktiken wie virtuelle verdeckte Ermittlungen in sozialen Netzwerken aus der exekutivischen Grauzone von zwischen den Entscheidungsträgern abgestimmten Praktiken und unter Verschluss gehaltenen, staatsanwaltschaftlichen Gutachten zu befreien und im Rahmen einer öffentlichen politischen Auseinandersetzung über Notwendigkeit und Grenzen derartiger Ermittlungen eine klare Rechtslage zu schaffen.

### *d) Täuschungsinfiltration*

Überzeugender als die diffuse Anknüpfung an Identitätsvertrauen scheint deshalb die konsequente Durchhaltung der Risikokonzeption des BVerfG und damit eine

---

377 So BVerfGE 120, 378 (408) unter Verweis auf BVerfGE 85, 386 (403 f.); 108, 282 (312).

378 Ständige Rechtsprechung, vgl. BVerfGE 120, 351 (366).

379 BVerfGE 120, 274 (346).

380 Siehe oben II.B.3.b).

381 Zum Ganzen *Mahlstedt*, Verdeckte Befragung, S. 183 ff.

Ergänzung des Schutzes vor technischer Infiltration durch den Schutz vor täuschender Infiltration. Die Wortbedeutung des Begriffs „Infiltration" legt dies ohnehin nahe: Unter Infiltration wird neben dem Eindringen und Einsickern auch die Unterwanderung verstanden.[382] Genau hierauf zielen polizeiliche Maßnahmen in sozialen Netzwerken ab. Es geht um verdeckte Informationserhebungen in bestimmten Bevölkerungsgruppen wie beispielsweise „Fußball-Hooligans" oder im Drogenmilieu. Hier können an dem äußeren Erscheinungsbild und dem Kommunikationsverhalten der Zielgruppe orientierte Scheinprofile erstellt und zur aktiven und passiven Informationserhebung, ggf. also auch zu Kommunikation mit einzelnen Betroffenen, eingesetzt werden. Technische Möglichkeiten dazu bieten beispielsweise Bildgeneratoren, die aus einer Vielzahl von Gesichtsporträts neue Gesichtsfotografien mit wahlweisen Merkmalen zusammensetzen.[383]

Die mit der Erstellung und Nutzung sogenannter Scheinprofile einhergehende Täuschung und Schaffung von Vertrauensverhältnissen lässt sich unter der Risikokategorie „Täuschungsinfiltration" zusammenfassen. Ob derartige Ermittlungsmaßnahmen bereits nach geltender Rechtslage zulässig sind, braucht hier nicht analysiert zu werden, scheint jedoch kaum denkbar. Problematisch sind neben der fehlenden einschlägigen Ermächtigungsgrundlage insbesondere der Vorfeldcharakter sowie ein möglicher Verstoß gegen das Täuschungsverbot und die Selbstbelastungsfreiheit. Die Frage überschreitet indes die Forschungsziele der vorliegenden Arbeit und muss deshalb einer eigenständigen Untersuchung überlassen bleiben.

#### *e) Zwischenergebnis*

Im zweiten Abschnitt des Urteils widmet sich das BVerfG der „Internetaufklärung" und erkennt hier nur sehr eingeschränkt Risiken, namentlich bei gezielter Zusammentragung, Speicherung und ggf. bei einer unter Hinzuziehung weiterer Daten erfolgenden Auswertung allgemein zugänglicher Informationen, soweit sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.[384] In der Entscheidung zu Steuerdaten wird das Konzept zu allgemein zugänglichen Daten auf öffentlich zugängliche Daten ausgedehnt und bestätigt.[385]

Eine Gefährdungslage bei allgemein zugänglichen Daten erkennt das BVerfG in der Entscheidung zur Online-Durchsuchung nicht ohne Weiteres bei einer legendierten Kommunikationsaufnahme durch staatliche Stellen. Das in der Entscheidung für erforderlich gehaltene Identitätsvertrauen lehnt das Gericht bei der Internetkommunikation ab, soweit keine Nachprüfungsmechanismen bestehen.[386] Die

---

382 *Munzinger/Duden*, Online-Ausgabe, Eintrag „Infiltration".

383 Beispiele: http://www.facegen.com/modeller.htm [Stand: 28.3.2014].

384 Siehe oben II.B.16.a).

385 Siehe oben II.B.16.b).

386 Siehe oben II.B.16.a).

Konzeption des BVerfG hat sich bei näherer Prüfung als wenig überzeugend erwiesen. Sie wird der heutigen Internetkommunikation nicht gerecht und begünstigt eine Lesart, die unstimmig mit der im vorangehenden Abschnitt des Urteils entwickelten Risikokonzeption ist. Anhand des Beispiels „Ermittlungen in sozialen Netzwerken" konnten die Probleme der unvollständigen Risikokonzeption dargestellt werden.[387] Naheliegender wäre die Ergänzung des Schutzes vor technischer Infiltration durch den Schutz vor täuschender Infiltration. Diese hat das Gericht freilich bislang noch nicht vorgenommen.[388]

### 17. Informationelles Trennungsprinzip

In der bereits oben angesprochenen[389] Entscheidung zum *Antiterrordateiengesetz*[390] befasst sich das BVerfG mit der Schaffung einer zentralen Verbunddatei der Sicherheitsbehörden, in der Daten verschiedener, abstrakt festgelegter Kategorien von Personen mit Verbindungen zum internationalen Terrorismus (§ 2 ATDG) aufgenommen werden. Die Inhalte umfassen dabei neben sogenannten Grunddaten (insbesondere Personalien, § 2 Abs. 1 Nr. 1 a) ATDG) eine Vielzahl von Informationen als „erweiterte Grunddaten" – u.a. zu genutzten Kommunikationsanschlüssen, Volks- und Religionszugehörigkeit, besonderen Fähigkeiten, Angaben zur Gefährlichkeit, zu besuchten Orten oder Gebieten und zu Kontaktpersonen; vgl. § 2 Abs. 1 Nr. 1 b) aa)–rr) ATDG. Auf diese Datei können insgesamt mehr als 60 Behörden, darunter Polizei- und Nachrichtendienstbehörden, im Rahmen ihrer Aufgabenerfüllung unter bestimmten Voraussetzungen mit unterschiedlicher Reichweite zugreifen. Von der Datei waren im August 2012 ca. 16.000 Personen erfasst, beinahe 3.000 davon lebten im Inland. Seit März 2007 wurden wöchentlich etwa 1.200 Anfragen gestellt, insgesamt ca. 350.000.[391]

Diese Entscheidung des BVerfG hatte mithin nicht die Begrenzung von Eingriffen auf der primären Erhebungsebene zum Gegenstand, sondern den sekundären Informationsaustausch zwischen Sicherheitsbehörden. Die Feinjustierung erfolgt im Rahmen der Bestimmtheit, wobei das ATDG in seinen „Grundstrukturen" mit dem Recht auf informationelle Selbstbestimmung für vereinbar gehalten wurde, zahlreiche Einzelbestimmungen jedoch mit dem Bestimmtheitsgebot unvereinbar waren.[392]

---

387 Siehe oben II.B.16.c).

388 Siehe oben II.B.16.d).

389 Siehe oben Teil 2, I.A.

390 BVerfG, Urteil vom 24.4.2013, 1 BvR 1215/07 *(Antiterrordateigesetz)* = NJW 2013, 1499 = JZ 2013, 621; zum Ganzen *Gärditz*, JZ 2013, 633.

391 *Giesecke/Wissenschaftlicher Dienst des Bundestages* (Hrsg.), Aktueller Begriff Nr. 18/13 (23.5.2013), S. 1.

392 BVerfG, Urteil vom 24.4.2013, 1 BvR 1215/07 *(Antiterrordateigesetz)* Rn. 1; *Gärditz*, JZ 2013, 633.

Hinsichtlich einschlägiger Risiken ist das Urteil nur mittelbar relevant. Die besondere Eingriffsschwere der Zusammenführung von Daten der Nachrichtendienste mit denen der Vollzugsbehörden folgert das Gericht aus den Eigenarten der jeweiligen Befugnisse: Die weitergehenden Möglichkeiten der Nachrichtendienste hinsichtlich Verdeckung und Vorfeldaufklärung rechtfertigten sich gerade durch deren nicht vorhandene Vollzugsbefugnisse. Eine Geheimpolizei, die verdeckte Ermittlungen im Vorfeld mit operativen Vollzugsbefugnissen kombiniert, sei verfassungsrechtlich nicht vorgesehen.[393] Um diese „Aufgabenteilung" nicht zu umgehen, entwickelt das BVerfG aus dem Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, ein informationelles Trennungsprinzip.[394] Es widmet sich in der Entscheidung somit nicht unmittelbar einzelnen thematischen Risiken, sondern – übergreifend – der spezifischen Konstellation einer Umgehung bestehender Schutzvorschriften durch Herstellung einer „Informationseinheit". Lediglich am Rande werden dagegen Aspekte der Profilbildung[395] und Diskriminierung[396] angesprochen.

## C. Zwischenergebnis

Ausgangspunkt der Rechtsprechungsentwicklung ist das räumliche Schutzkonzept des aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG folgenden Rechts auf Privatsphäre. Dieses richtet sich in den frühen Entscheidungen insbesondere gegen die Risiken von Publizitätsschäden und Entkontextualisierungen. In der älteren Rechtsprechung wird dabei der enge Bezug des Schutzguts Menschenwürde zum Risiko einer „verwaltungstechnischen Entpersönlichung" durch Registrierung und Katalogisierung deutlich.[397] In der Folgezeit knüpfen die Entscheidungen an mögliche Verhaltensauswirkungen bei Verletzung von Vertraulichkeitserwartungen an und gehen damit zu einer folgenorientierten Betrachtung über.[398] Darin kann eine Grundlage für die maßgeblich auf angenommenen Verhaltensänderungen basierende Risikokonzeption des *Volkszählungsurteils* gesehen werden.[399]

Die Selbstbestimmungskonzeption des *Volkszählungsurteils* basiert auf den Risiken Informationspermanenz und Informationsemergenz. Letzteres lässt sich allerdings erst durch eine Auslegung der im Entscheidungstext angeführten Kombina-

---

393 Ebd. Rn. 122.
394 Vgl. ebd. Rn. 123.
395 Ebd. Rn. 169 und 174.
396 Ebd. Rn. 189.
397 Siehe oben II.B.1.
398 Siehe oben II.B.2.
399 Siehe oben II.B.3.d).

tionsmöglichkeiten erkennen.[400] Grundlage der vom Gericht als Anknüpfungspunkt gewählten Befürchtungen der Betroffenen ist bei näherer Analyse die vermutete Fehleranfälligkeit, welche ihre Grundlage in der im Vergleich zu menschlicher Informationsverarbeitung schwieriger in Prozessen implementierbaren Kontextberücksichtigung findet.[401] Ein tragendes Risiko der *Volkszählungsentscheidung* sind zudem konformitätsbegünstigende Verhaltensanpassungen. Dieses Risiko weist bei näherer Analyse auf weiteren Forschungsbedarf hin: Verhaltensanpassungen durch Publizität sind nicht ohne Weiteres plausibel. Sie setzen entweder das tatsächliche Fehlen elementarer Rechtsstaatlichkeit oder eine irrationale Verhaltensweise der Betroffenen voraus. Größere Überzeugungskraft erlangt das Argument erst bei weiterer Interpretation auch unter Einbeziehung privater Risiken. Neben den problematischen Prämissen dieser individuell-folgenorientierten Risikokonzeption widmet sich die Entscheidung den Risiken aus Sicht einer gesamtgesellschaftlichen Makro-Perspektive, indem die Folgen der Datenverarbeitungen für die Funktionsvoraussetzungen des Demokratieprinzips einbezogen werden.[402] Dieses Makro-Risiko wird in der Folgezeit über den Topos „Einschüchterungseffekt" konkretisiert und setzt wiederum die Prämisse tatsächlich erfolgender Handlungsauswirkungen bei betroffenen Bürgern voraus. Das Risiko von Einschüchterungen sieht die Rechtsprechung jedoch nicht nur bei Individuen, sondern überträgt es in der Entscheidung zu Kontostammdaten auch – allerdings nicht konsequent – auf juristische Personen.[403] Das Risiko von individuellen Handlungsauswirkungen wird auch in jüngeren Entscheidungen zu privater Datenverarbeitung aufgegriffen, wobei Selbstschutzmöglichkeiten der Betroffenen maßgeblich für die Gewährung von Schutzpflichten gegenüber den Privaten sind. Darüber hinaus werden bei privaten Datenverarbeitungen aus den Bedingungen von Wirtschaftlichkeit und Kostendruck spezifische Risiken für das Schutzgut Datensicherheit erkannt, wobei die Annahme von Einschüchterungseffekten bei privater Datenverarbeitung in einem Sondervotum hinterfragt und empirische Belege eingefordert werden.[404]

Das Risiko der Informationspermanenz wird in der *Entmündigungsentscheidung* aufgegriffen, wobei man ihm jedoch einen eher geringen Stellenwert einräumt wird. Bemerkenswert ist allerdings, dass das Risiko überhaupt bereits zu dieser – vor der Existenz des Internets liegenden – Zeit präsent war.[405] Die Anbindung von Risiken an eine gesamtgesellschaftliche Makro-Ebene wird in den *G10*-Entscheidungen deutlich, wobei dort auch das Schutzziel einer Abwehr von „Befürchtun-

---

400 Siehe oben II.B.3.a).
401 Siehe oben II.B.3.f).
402 Siehe oben II.B.3.b).
403 Siehe oben II.B.14.
404 Siehe oben II.B.13.
405 Siehe oben II.B.4.

gen“ der Betroffenen deutlich hervorgehoben wird.[406] Dieser Konzeption lässt sich als Schutzgut das „Vertrauen der Allgemeinheit“ zuordnen.[407]

Das davon zu unterscheidende Schutzgut der Selbstdarstellung wird in der *Caroline*-Entscheidung aufgegriffen. Die maßgeblichen Risiken, die zur Konkretisierung dieses Schutzguts dienten, waren die Entkontextualisierung – jedoch verstanden als Veränderung der „Form der Öffentlichkeit“ – und das Risiko von Publizitätsschäden. Darüber hinaus verdeutlicht die analysierte Entscheidung die nur zögerliche Ausweitung des räumlichen Bezugs der Einzelverbürgung „Privatsphäre“.[408] Einen größeren Schritt bei der Ablösung von räumlich-thematischen Kriterien weist die Anknüpfung an das formale Kriterium der Sprache in der *Mithörentscheidung* auf. Dort erfüllt der Topos „Vertraulichkeitserwartung“ die zentrale Abgrenzungsfunktion für die Schutzgewährleistung und wird nach Maßgabe eines eigenen Schutzguts konstruiert. Einen Weg zur normativen Konkretisierung der Vertraulichkeitserwartung über thematische Einzelgrundrechte weist dann die *Rasterfahndungsentscheidung*.[409]

Mit dem Topos „Persönlichkeitsprofile“ setzen sich verschiedene Entscheidungen auseinander. Die Profilbildung erweist sich darin als spezifische Kombination der Risiken von Informationspermanenz und Informationsemergenz mit dem Phänomen der Informationskonvergenz.[410] Ein ähnliches Risiko stellt die Überwachungskumulation dar, worunter der verstärkende Effekt unterschiedlicher Überwachungsmaßnahmen zu verstehen ist.[411]

Risiken verschiedener individueller Überwachungsnachteile werden in einer Reihe jüngerer Entscheidungen aufgegriffen, wobei es genügen soll, wenn eine Befürchtung „nicht ohne jeden Grund“ vorliegt. Hierin ist eine manifeste Abstraktion und Subjektivierung der Risikokonzeption zu sehen.[412] Zahlreiche Entscheidungen widmen sich einschlägigen Risiken im Rahmen von Schwerekriterien, die bei der Prüfung der Verhältnismäßigkeit im engeren Sinne relevant sind. Dort werden insbesondere die Risiken von Anschlussermittlungen und Stigmatisierungen, z.B. bei Umfelderkundigungen, aufgegriffen.[413] Die Entscheidung zum Antiterrorgesetz lässt sich in diesen Kontext einordnen, bezieht sich jedoch auf den übergreifenden Aspekt der Umgehung rechtsstaatlicher Befugnisaufteilung durch Zusammenführung von Informationen.[414] Im Gegensatz zu diesen abstrakt-subjektiven

---

406 Siehe oben II.B.5.
407 Siehe oben I.B.10.
408 Siehe oben II.B.6.
409 Siehe oben II.B.7.
410 Siehe oben II.B.8
411 Siehe oben II.B.12.
412 Siehe oben II.B.9.
413 Siehe oben II.B.9.a).
414 Siehe oben II.B.17.

Risiken steht dann die Konzeption des Kernbereichsschutzes, die das Schutzgut der Menschenwürde konkretisiert und wiederum stark räumlichen Vorstellungen folgt.[415]

Die vielschichtigste Risikokonzeption findet sich in den Aussagen zu informationstechnischen Systemen und zu öffentlich zugänglichen Daten. Bei informationstechnischen Systemen werden zwei Risiken gesehen: zum einen der Gesamtzugriff auf vertrauliche Informationen, dem aufgrund der umfassenden Verwendung der Systeme besonderes Gewicht zukommt. Diesem Risiko kann das Schutzgut „Vertraulichkeit" zugeordnet werden. Daneben wird das Risiko technischer Infiltration und Manipulation bzw. Beschädigung des Systems aufgegriffen. Diesem Risiko lässt sich das Schutzgut Integrität zuordnen.[416] Bei der in diesem Zusammenhang maßgeblichen Internetaufklärung wird eine relativ weite Ausnahme von den genannten Risiken im Fall öffentlich zugänglicher Daten gemacht. Diese erwies sich bei näherer Untersuchung als lückenhaft und verdeutlichte die Notwendigkeit einer Ergänzung des Schutzes vor dem Risiko technischer Infiltration durch den Schutz vor dem Risiko einer Täuschungsinfiltration.[417]

Die anfangs dargestellte These *Ehmanns* zur Entkörperlichung des Schutzguts hat sich damit zum Teil bestätigt, wobei das Problem der fehlenden Anknüpfungspunkte der Willensmanifestation gerade bei der Internetkommunikation greifbar wird. Das nicht von der Rechtsprechung aufgegriffenen Risiko der Täuschungsinfiltration könnte bei näherer Analyse hier taugliche Abgrenzungsmaßstäbe erbringen. Insbesondere ist es möglich, in den Datenschutzeinstellungen der Nutzer – beispielsweise der Zuordnung von Nachrichten zu bestimmten Empfängerkreisen in sozialen Netzwerken – eine derartige Willensmanifestation zu sehen. Die Einzelheiten dieses Ansatzes weisen allerdings über die Forschungsfragen dieser Untersuchung hinaus und müssen einer künftigen Studie vorbehalten bleiben.

# III. Literaturkonzeptionen

## A. Zwei-Ebenen-Konzeption (Albers)

### 1. Überblick

Die ergiebigste und derzeit auch umfassendste Auseinandersetzung mit dem Datenschutzrecht hat *Marion Albers* in ihrer 2005 erschienenen Habilitationsschrift[418]

---

415 Siehe oben II.B.11.

416 Siehe oben II.B.15.c).

417 Siehe oben II.B.16.

418 *Albers*, Informationelle Selbstbestimmung, 2005.

vorgelegt und in einem Sammelbandbeitrag aus dem Jahr 2008[419] bekräftigt. In diesem jüngeren Beitrag beginnt *Albers* ihre Ausführungen mit der Ablehnung einer „verwaltungsrechtlichen Informationsordnung" im Sinne eines besonderen Rechtsgebiets.[420] Sie verfolgt stattdessen ein „neues übergreifendes Konzept, [...] das die Kategorien Kommunikation, Wissen und Information auf einer Grundlagenebene in das Verwaltungsrecht integriert". Durch das Verständnis informationsbezogener Normen aus dem Gesamtkontext will *Albers* damit „zu einer angemessenen Dogmatik" gelangen. Hierfür sei eine Emanzipation des Datenschutzes von seiner Entstehungsgeschichte und eine anschließende Neukonzeption nötig.[421] In diesem Zusammenhang hält sie sowohl die Reformulierung der Ziele des Datenschutzes als auch der bestehenden Schutzbedürfnisse seitens der Bürger für erforderlich.[422] Insbesondere Letzteres macht ihre Arbeit auch für die vorliegende Untersuchung relevant und rechtfertigt ihre Einbeziehung. Soweit möglich wird der kompaktere Beitrag von 2008 zugrunde gelegt, da dieser aktueller ist und an den entscheidenden Stellen auf der Habilitationsschrift basiert.

Ausgangspunkt von *Albers'* Neukonzeption ist die Unterscheidung zwischen Daten und Informationen, wobei sie unter Daten auf Datenträgern festgehaltene Zeichen versteht, die als Informationsgrundlagen dienen können. Als Informationen bezeichnet sie „Sinnelemente, die in einem bestimmten sozialen Kontext aus Beobachtungen, Mitteilungen oder Daten erzeugt und dann genutzt werden". Informationen misst sie eine „zweigliedrige Struktur" zu, da die Informationsinhalte einerseits u.a. an Daten anknüpften, andererseits aber erst durch eine Interpretationsleistung der empfangenden Person „vollendet" würden. Weil für *Albers* die Informationen mehr voraussetzen als die von ihr als „Informationsgrundlagen" beschriebenen Daten, seien Informationen und Daten keine Synonyme.[423]

### 2. Risikokonzeptionen und Schutzgüter

Eine erste Annäherung an relevante Risiken erfolgt bei *Albers* in der Begründung, weshalb der Umgang mit personenbezogenen Informationen und Daten eine eigenständige Dimension des Verwaltens ist. Dort differenziert sie zunächst in der Grundkategorie „Information" zwischen einer Struktur- und einer Prozessdimension.

---

419 *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II.

420 Ebd., S. 113.

421 Ebd.

422 Ebd., S. 114.

423 Ebd., S. 114 ff.

### *a) Unterstellungsrisiko*

Im Rahmen der Strukturdimension definiert sie den Begriff „Wissen" als „Faktor und Produkt des Kontexts, in dem sich der Umgang mit Informationen und Daten vollzieht". Das Wissen der Verwaltung wirke sich auf den Schutzbedarf derjenigen Personen aus, auf die die Informationen und Daten verweisen. Es beeinflusse die Deutung von „Beobachtungen, Mitteilungen oder Daten" und deren Informationsgehalt. Es bestehe aus „komplex aufgebauten kognitiven Erwartungen, die gegenüber einzelnen Ereignissen relativ zeitbeständig" seien. Insbesondere wirke es durch Erwartungen auf die Informationserzeugung ein, wobei auch das Ausbleiben einer erwarteten Beobachtung oder Mitteilung Informationsqualität gewinnen könne und ggf. zur Ausfüllung von Informationslücken mittels Unterstellungen führe.[424] Der Einfluss des Wissens führe dazu, dass personenbezogene Daten auch im Fall ihres Fehlens „nachteilige informatorische Effekte" verursachen könnten.[425]

Die an dieser Stelle von *Albers* beschriebenen Unterstellungen infolge des Fehlens bestimmter Informationen erinnern zunächst an das oben beschriebene Risiko des Kontextdefizits.[426] Auch dort wurde der Mangel an spezifischen Informationen als Risiko aufgegriffen. Das Risiko des Kontextdefizits unterscheidet sich jedoch von der Situation, die *Albers* beschreibt, durch den engen Zusammenhang des Kontextdefizits mit der Informationsübernahme durch die Verwaltung, während das Risiko von Unterstellungen dem zeitlich vorgelagert bereits durch das Verwaltungswissen ausgelöst werden kann. Dieses Risiko ist nicht von einer anderen, erfolgreichen Informationsbeschaffung abhängig. Die Hervorrufung von Unterstellungen weist damit auch auf die Unvollständigkeit hin, die eine reine Fokussierung von Risikokonzeptionen auf den Schutz vor Informationsbeschaffung mit sich bringt.

### *b) Technikspezifische Schutzerfordernisse*

In ihrem Abschnitt zur Grundkategorie „Information" beschreibt *Albers* die prägende Wirkung von Medien, Techniken und Netzen im Hinblick auf Daten- und Informationsumgang. Dort referiert sie technikspezifische Schutzerfordernisse anderer Literaturkonzeptionen und setzt sich mit deren Risikokonzeptionen auseinander.[427] Aus der frühesten Literatur greift sie insbesondere diejenigen Ansichten auf, die aus dem Macht-, Kontroll- und Überwachungspotenzial auf das Erfordernis datenschutzrechtlicher Regulierung wegen der Einschränkung von Verhaltensspielräumen schließen. Diese Ansichten, zu denen insbesondere die bereits oben ange-

---

424 Ebd., S. 117.

425 Ebd., S. 118.

426 Siehe oben Teil 1, II.B.

427 *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, S. 121–124.

sprochene von *Steinmüller* zu zählen ist,[428] verwirft sie als „teils pauschal und politisiert". Der „Erwerb von Wissen über andere" und die Orientierung an „Verhaltens- oder Erwartungserwartungen" seien ebenso wie „soziale Kontrolle" notwendig mit sozialen Beziehungen verbunden und begründeten keinen pauschalen Schutzbedarf des Betroffenen.[429] Eine präzisere Herausarbeitung sieht sie in den frühen Literaturstimmen, die auf Risiken „sachlich und zeitlich allumfassender Datenbanken mit ungesteuerten Zugriffsmöglichkeiten sämtlicher staatlicher Behörden, zunehmend datengestützter behördlicher Entscheidungen ohne jede Regulierung der Fehlerquellen rechnergestützter Datenverarbeitung, Wegfall auch der angemessenen Wissensschranken in sozialen Beziehungen" und „erwartungsvermittelte Selbstregulationen auch des effektiv grundrechtsgeschützten Verhaltens" abstellen. Diese verwiesen auf vielfältige Schutzerfordernisse, die differenziert zu entwickeln seien und durch die Technik ihrer Zeit ausgelöst, aber nicht vollständig geprägt würden.[430] Eine pauschale Differenzierung nach der eingesetzten Technik bei der Bestimmung des Schutzbedarfs hält *Albers* auch angesichts deren Veränderungen für verfehlt. Stattdessen fordert sie eine Orientierung an den jeweiligen Folgen des Umgangs mit Informationen und deren Untersuchung auf ihre rechtliche Relevanz hin. An Techniken orientierten Risiken komme gleichwohl eine bedeutende Rolle zu. Gefährdungspotenziale hätten sich um aktuelle Probleme wie die Datensammlung oder Profilbildung über Netze, die Authentizität von Kommunikationspartnern oder Manipulationsgefahren erweitert.[431] Im Übrigen fordert sie eine Rekonstruktion des Schutzbedarfs in Form einer „Aufschlüsselung" von Schutzerfordernissen und wendet sich gegen Abstraktionen wie das von *Hoeren* vorgeschlagene Leitziel einer „Informationsgerechtigkeit".[432]

Die von *Albers* referierten Risiken der älteren Literaturkonzeptionen gehen – abgesehen von einer z.T. höheren Abstraktion – nicht über die der oben untersuchten Normen und Entscheidungen hinaus. Zuzustimmen ist *Albers* in der Kritik der unspezifisch-pauschalen Annahme der Schutzbedürftigkeit in der älteren Literatur.[433]

### *c) Makrorisiken auf einer zweiten Ebene*

Unmittelbar bevor sie ihren eigenen Ansatz darstellt, identifiziert *Albers* eine Reihe von „Bruchlinien" und „Defizite[n]" des Rechts auf informationelle Selbstbestimmung, die sie auf eine mangelhafte Umstellung des Anknüpfungspunkts

---

[428] Siehe oben Einleitung II.

[429] *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, S. 122.

[430] Ebd., S. 123.

[431] Ebd.

[432] Ebd., S. 124.

[433] Siehe oben Einleitung, II.

(von Daten auf Informationen) für den Schutz und eine den neuen Inhalten nicht gerecht werdende Verhaftung der Rechtsprechung in Mustern traditioneller eigentumsanaloger Dogmatik zurückführt.[434] Das von ihr zur Abhilfe vorgeschlagene Modell einer Zwei-Ebenen-Konzeption basiert auf der Vorstellung, dass der Umgang mit personenbezogenen Daten ein neues Schutzgut betrifft, „das sich von traditionellen Schutzgütern wie Verhalten oder Eigentum unterscheidet".[435] *Albers* kritisiert die „auf Basis einer spezifischen Unterscheidung von Staat und Gesellschaft" individualistisch konzipierten Schutzgüter und verweist auf die Möglichkeit, Gewährleistungsinhalte aus überindividueller und übergreifender Perspektive zu formulieren.[436] Zwar benennt sie das ihr vorschwebende neue Schutzgut nicht explizit, sondern führt nur aus, dass sich der Schutz auf „Informationen und Daten" richtet; ihre Ebenenkonzeption lässt jedoch Rückschlüsse auf die Risikokonzeption zu: Sie unterscheidet zwischen Schutzpositionen, die in konkreten Konstellationen bestehen, von solchen, „die sich auf einer übergreifend-vorgelagerten Ebene auf eine Grundregulierung der Informations- und Datenverarbeitungen richten".[437] Auf der von dieser übergreifend-vorgelagerten Ebene unterschiedenen konkreteren ersten Ebene sollen thematische Einzelgrundrechte bestimmte Vorgaben für den Umgang mit Informationen und Daten hergeben. Dabei erachtet sie den Personenbezug als nicht ausreichend für die Auslösung des Schutzes. Vielmehr will sie durch „normorientierte Argumentation" die rechtliche Relevanz erwartbarer Nachteile nach den Kriterien des jeweils einschlägigen Grundrechts berücksichtigen. Als Beispiel nennt sie u.a. Art. 4 GG im Fall von Tagebüchern mit Gewissensauseinandersetzungen und Art. 5 Abs. 1 S. 1 GG bei Informationen zu in einer Bibliothek ausgeliehenen Büchern.[438] Art. 2 Abs. 1 GG sieht sie hingegen nur auf der zweiten Ebene für rein persönlichkeitsbezogene Bereiche bzw. die „Bündelung vielfältiger Situationen oder Folgen" vor.[439] Auf dieser zweiten, übergeordnet-vorgelagerten Ebene will sie Risiken angehen, die sie als „Allumfassende, unbegrenzte und intransparente Informations- und Datenverarbeitungen" beschreibt und als „kulturell verankert" und durch die Werke von *Orwell*, *Bentham* und *Kafka* „popularisiert" sieht.[440]

Eine der „Wurzeln der Schwierigkeiten" des Rechts auf informationelle Selbstbestimmung nach Konzeption des BVerfG sieht *Albers* in dem Versuch, die Schutzerfordernisse in konkreten Situationen (erste Ebene) und die übergreifend-vorgelagerten Schutzerfordernisse (zweite Ebene) über ein „einheitliches Recht" zu

---

[434] *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, S. 142 ff.

[435] Ebd., S. 145.

[436] Ebd.

[437] Ebd., S. 146.

[438] Ebd., S. 149 f.

[439] Ebd., S. 149.

[440] Ebd., S. 152.

bewältigen. In ihrer ersten Ebene will sie Unterlassungs- und Schutzansprüche aus thematisch spezifizierten Grundrechten herleiten; das Risiko unbegrenzter und intransparenter Informations- und Datenverarbeitungen will sie auf der den konkreten Fallkonstellationen vorgelagerten Ebene mittels Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG angehen.[441] Die Schutzerfordernisse auf der zweiten Ebene beschreibt sie in Anlehnung an *Saladin* als „essentielle, existentiale Voraussetzungen für die Ausübung jeglicher Freiheit".[442] Als Risiken bezieht sie sich dort auf die „allwissende Verwaltung" und den „gläsernen Bürger".

Insgesamt weist *Albers'* Konzeption damit auf die Risiken auf gesellschaftlicher Ebene hin, die auch der Rechtsprechung von BVerfG und EGMR zugrunde liegen.[443] Zu der von ihr vorgeschlagenen zweiten Ebene, auf welcher der Schutz über Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vermittelt würde, lassen sich Makrorisiken wie die Erstellung von Persönlichkeitsprofilen, gesamtgesellschaftliche Verhaltensanpassungen oder das im Volkszählungsurteil ausgearbeitete Konformismusrisiko rechnen.

### 3. Zwischenergebnis

Die Zwei-Ebenen-Konzeption von *Albers* enthält aufgrund der dogmatischen Zielsetzung der Entwicklung eines übergreifenden Konzepts zum Informations- und Datenumgang und dessen Integration in das Verwaltungsrecht auch hinsichtlich der Schutzgüter und Risikokonzeptionen relevante Aussagen. Ergiebig ist insbesondere die kompakte Fassung ihrer Konzeption im Sammelschriftbeitrag aus dem Jahr 2008, der zunächst auf das Risiko von Unterstellungen im Fall fehlender Informationen hinweist.[444] Darüber hinaus werden im Rahmen der Darstellung der technikspezifischen Schutzerfordernisse Risikokonzeptionen älterer Fachliteratur referiert, die jedoch – abgesehen von einer höheren Abstraktion – nicht über die aus der normativen Analyse, insbesondere der Rechtsprechung, hinausgehen.[445] *Albers'* Konzeption einer zweiten, vorgelagert-übergeordneten Ebene verdeutlicht insgesamt jedoch die Kategorie von Makro-Risiken, wie sie auch aus der Rechtsprechung von EGMR und BVerfG gefolgert werden konnten,[446] und die sich auf die im Vierten Teil vorzunehmende Systematisierung der Risiken auswirken wird.

---

441 Ebd., S. 153.

442 Ebd.

443 Vgl. insbesondere oben Teil 1, IV.B.1.a); Teil 3, II.B.1, 3.b), 5., 8., 10.

444 Siehe oben III.A.2.a).

445 Siehe oben III.A.2.b).

446 Siehe oben III.A.2.c).

## B. Selbstdarstellungskonzeption (Britz)

### 1. Überblick

Neben der Konzeption von *Albers* ist vor allem die maßgeblich in einer Monografie aus dem Jahr 2007[447] und einem Sammelbandbeitrag aus dem Jahr 2010[448] entwickelte Selbstdarstellungskonzeption der Gießener Professorin und heutigen Verfassungsrichterin *Gabriele Britz* in die Untersuchung einzubeziehen.

*Britz* widmet sich in ihrer Monografie der Rekonstruktion des Allgemeinen Persönlichkeitsrechts und dessen Teilbereich der Selbstdarstellung. Ausgehend von einer Wortlautauslegung des Art. 2 Abs. 1 GG greift sie auf ein vorrechtliches „Normativkonzept autonomer Freiheit" zurück und beschreibt hiermit Systematik und Gewährleistungsgehalt des „Rechts auf Selbstdarstellung" und weiterer Einzelausprägungen des Art. 2 Abs. 1 GG.[449]

Die von *Britz* herangezogene vorrechtliche Vorstellung autonomer Freiheit umfasst dabei einerseits ein Element äußerer Verhaltensfreiheit (verstanden als Möglichkeit zur Vornahme oder Unterlassung beliebiger Handlungen) und andererseits eine innere Komponente, die sie als „die auf einem gewählten Selbst gründende Selbstreflexivität" beschreibt.[450] Konkret soll dieses innere Element die Möglichkeit des Menschen erfassen, seine Entscheidungen und Handlungen in ein Verhältnis zu einem selbstgewählten Persönlichkeitsbild zu setzen. Autonomie habe nach dieser Konzeption neben der äußeren Verhaltensfreiheit die Voraussetzung einer „Möglichkeit der Selbstreflexivität".[451] An den Vorgang der „Selbst-Wahl" seien jedoch aufgrund der „zahlreichen Grenzen und Einflussfaktoren" der Identitätsbildung und deren Eigenschaft als „kommunikativer Vorgang" keine hohen Anforderungen in Form einer Identitätsleistung zu stellen. Vielmehr stehe die „Selbst-Wahl" unter den „Vorbehalt gradueller Verwirklichung".[452] Maßgeblich sei das Bestehen einer Wahlmöglichkeit, auch wenn sich diese lediglich „innerhalb einer Bandbreite äußerlich determinierter Optionen" abspiele. Das Individuum müsse zur Autonomie zwar nicht „Alleinentscheider", solle aber doch „Mitentscheider" sein. Voraussetzung hierfür sei die Möglichkeit der Einnahme einer kritischen Distanz zu dem interaktiv hervorgebrachten „Identitätskonglomerat aus fremden und eigenen Wahrnehmungen". Erst mittels dieser „Selbst-Distanzierung" sei die „wählende Selbstvergewisserung" möglich, die dem von *Britz* referierten Verständnis vor-

---

447 *Britz*, Selbstdarstellung.

448 *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft.

449 *Britz*, Selbstdarstellung, S. V und 4 f.

450 Ebd., S. 22, 7.

451 Ebd., S. 11.

452 Ebd., S. 11–15.

rechtlicher Autonomie entspreche.[453] Zusammenfassend erfordere die „Selbst-Wahl“ die Selbstdistanzierung, Selbstvergewisserung und erneute Selbstannahme.[454]

Diese Autonomiekonzeption ordnet sie einer Wortlautinterpretation des Begriffs „Entfaltung“ aus Art. 2 Abs. 1 GG zu. Entfaltung könne als ein realisierender Vorgang verstanden werden, worunter die Verhaltensfreiheit falle, die der äußeren Komponente des Autonomiekonzepts zuzuordnen sei.[455] Daneben gestatte der Wortlaut jedoch auch die Aufnahme der inneren Autonomiekomponente in Form des Verständnisses von „Entfaltung als konstituierendem Vorgang“.[456] *Britz* rekonstruiert im Anschluss an diese Weichenstellungen das Allgemeine Persönlichkeitsrecht über die Möglichkeit von Selbstdarstellung zum Zwecke der Autonomiewahrung und widmet sich neben dem Recht auf Selbstdarstellung auch der informationellen Selbstbestimmung, wobei sie immer wieder auch auf datenschutzrechtlich relevante Risiken und Schutzgüter eingeht.

In ihrem Sammelbandbeitrag aus dem Jahr 2010 ergänzt und erweitert sie die schon in der Monografie angelegten Ausführungen zum Recht auf informationelle Selbstbestimmung und bemüht sich dabei insbesondere um Anschlussfähigkeit an die Konzeption von *Albers* und diejenige des BVerfG.[457] Sie verfolgt deshalb nicht nur den Selbstdarstellungsansatz, sondern modifiziert auch die von ihr dem BVerfG zugeschriebene Konstruktion des Rechts auf informationelle Selbstbestimmung über das Schutzgut der Verhaltensfreiheit.[458] Im Folgenden werden die für Risikokonzeptionen und Schutzgüter relevanten Passagen analysiert.

### 2. Risikokonzeptionen und Schutzgüter

#### *a) Schutzgut innerer Reflexivitätsraum*

*Britz* geht an verschiedenen Stellen explizit auf das Schutzgut sowohl des Allgemeinen Persönlichkeitsrechts als auch des Rechts auf informationelle Selbstbestimmung ein. Ausgangspunkt hinsichtlich der Schutzgüterkonzeption ist die oben beschriebene innere Dimension der Entfaltungsfreiheit. Sowohl informationelle Selbstbestimmung als auch die von *Britz* ebenfalls auf das Recht auf Selbstbestimmung zurückgeführten Diskriminierungsverbote teilten das „auf die innere Dimension der Entfaltungsfreiheit zielende Schutzgut des Allgemeinen Persönlichkeits-

---

453 Ebd., S. 15 f.
454 Ebd., S. 27.
455 Ebd., S. 17.
456 Ebd., S. 18 ff.
457 *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 595.
458 Vgl. ebd., S. 582.

rechts“.[459] In Anlehnung an Raummetaphern des BVerfG lasse sich das Schutzgut als „innerer Freiraum“ beschreiben, was „ein Bild für die innere Komponente autonomer Freiheit“ und die dafür maßgebliche „Selbst-Wahl“ sei.[460] Das Recht auf Selbstdarstellung sei ein Instrument zur Absicherung des Schutzguts des Allgemeinen Persönlichkeitsrechts, das „anders als andere Teilbereiche des Allgemeinen Persönlichkeitsrechts“ dort ansetze, wo der zu schützende „innere Reflexivitätsraum gerade durch Fremdbilder“ bedrängt werde.[461]

Hinsichtlich des Rechts auf informationelle Selbstbestimmung führt *Britz* aus, dass die informationelle Selbstbestimmung kein eigenständiges Schutzgut sei; vielmehr bilde der Schutzgegenstand einer Datenverfügungsbefugnis das grundrechtliche Schutzgut nicht unmittelbar ab und werde nicht um seiner selbst willen geschützt. Als eigentliches Schutzgut sieht sie an dieser Stelle nicht nur die Entfaltungs-, sondern auch die Verhaltensfreiheit.[462] Dies dürfte insbesondere auf das Ziel der Herstellung einer „Anschlussfähigkeit“ an die von ihr über das Schutzgut „Verhaltensfreiheit“ ausgelegte Rechtsprechung des BVerfG zum Recht auf informationelle Selbstbestimmung zurückzuführen sein.

Festzuhalten bleibt das von *Britz* maßgeblich herangezogene Schutzgut eines „inneren Freiraums“, das sie aus ihrer eingangs beschriebenen Autonomiekonzeption gewinnt. Auffällig ist hierbei die Nähe zu den alten Konzeptionen von *Kohler* und *Warren/Brandeis,*[463] insbesondere hinsichtlich der bei *Britz* besonders stark ausgeschöpften räumlichen Konstruktion.

### *b) Fremdbildrisiko*

Das zentrale Risiko, das sich aus *Britz'* Konzeption ergibt, folgt der oben beschriebenen inneren Autonomiekonzeption als Prozess der Selbstvergewisserung und dem Schutzgut des „inneren Freiraums“. Der Prozess der Selbstreflexivität setze „private Rückzugsräume“ voraus. Das Individuum benötigte solche Räume nicht nur im wörtlichen Sinn, sondern auch in Form eines „mentalen Raum[s], der als innerer Freiraum im Sinne einer inneren Offenheit“ zur ernsthaften Infragestellung von Identitätsbeschreibungen und -erwartungen zu verstehen sei. Diese Offenheit sei in Abgrenzung zu an den Betroffenen gerichteten Identitätserwartungen anderer Personen zu wahren.[464] Das Risiko hierfür sieht sie in „allzu präzise[n] Identitätserwartungen“ anderer: Das Individuum sei davor zu schützen, sich „in Erwartung fremder Identitätserwartungen seines Optionenspielraums“ zu bege-

---

[459] *Britz*, Selbstdarstellung, S. 5.

[460] Ebd., S. 27.

[461] Ebd., S. 44.

[462] *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 582.

[463] Siehe oben Einleitung, I.

[464] *Britz*, Selbstdarstellung, S. 28 f.

ben.[465] Der innere Freiraum werde in besonderem Maße dadurch gefährdet, „dass sich das Individuum durch tatsächliche oder vermeintliche Identitätserwartungen der anderen gebunden“ sehe.[466] Fremdbilder seien dabei „potenziell doppelt relevant für die Persönlichkeitsentfaltung“: Neben der Verhinderung des Freiraums für die innere Auseinandersetzung seien sie dazu geeignet, dem Einzelnen die Aussicht zu nehmen „durch Formen der Selbstdarstellung Fremdbilder effektiv aufbrechen zu können“.[467] „Besondere Gefahren“ resultierten aus „besonders starken Fremdbildern, die eine effektive Wahrnehmung dessen, was das Individuum kommuniziert, von vornherein“ verhinderten.[468]

Bemerkenswert ist sodann die Anbindung dieser Risikokonzeption an privates Handeln: „Manipulative Bedingungen, unter denen sich Persönlichkeit entfaltet“, seien zum Großteil nicht staatlich gesetzt, sondern beruhten auf privatem Handeln bzw. „konkreten oder strukturellen Entfaltungshemmnissen“ in der Sphäre des Individuums selbst.[469] Das Recht auf informationelle Selbstbestimmung ordnet sie in diese Risikokonzeption ein als Schwächung vorgefertigter Identitätserwartungen und Schärfung des Blicks für die Selbstdarstellung der Person.[470] Als damit verbunden sieht *Britz* das Risiko von Diskriminierungen. Diese beruhten auf Stereotypen, die sich infolge der Fremdbildkonstruktion ergeben können. Derartige Stereotype könnten schon durch ein einziges Merkmal transportiert werden und ähnliche Folgen für die innere Autonomiekomponente hervorrufen wie die Verwendung umfangreicher, viele Merkmale erfassender Datenbestände. Hierzu verweist sie auf die Sensibilität bestimmter Daten.[471] Die Merkmale könnten ein undurchdringliches Erwartungsgeflecht erzeugen und dadurch die „Wahrnehmung dessen verhindern, als was eine Person sich tatsächlich darstellt“.[472]

*Britz'* zentrales Risiko besteht somit in Fremdbildern, die das Individuum in der für die (innere) Persönlichkeitsentfaltung als notwendig erachteten Selbstreflexivität beeinträchtigen. Hinzu kommt die in ähnlicher Weise vorgenommene Konstruktion des Risikos von Diskriminierungen über die Entfaltungsauswirkungen von Stereotypen. *Britz* geht in ihrer Konzeption dabei über das Risiko der Informationsfehlerhaftigkeit von Fremdbildern hinaus, da sie auch das Bestehen zutreffender Fremdbilder als ein Risiko einstuft, das zugunsten der Selbstdarstellung zu verhindern sei.[473] Deutlich wird damit die besonders konsequente Ausrichtung auf das betroffene Subjekt.

---

465 Ebd., S. 29.
466 Ebd., S. 37.
467 Ebd., S. 49 f.
468 Ebd., S. 50.
469 Ebd., S. 32.
470 Ebd., S. 53 f.
471 Ebd., S. 55.
472 Ebd.
473 Ebd., S. 57.

*c) Schutzgut Verhaltensfreiheit und verbundene Risiken*

Bereits in ihrer Monografie beschreibt *Britz* alternative (also nicht über die Entfaltungsfreiheit erfolgende) Herleitungen von Teilbereichen des Allgemeinen Persönlichkeitsrechts.[474] Hinsichtlich des Schutzes informationeller Selbstbestimmung führt sie aus, dass diese auch unmittelbar dem Schutz der allgemeinen Handlungsfreiheit diene: „Das Bewusstsein des Wissens anderer um das, was man tut oder nicht tut, beeinflusst das eigene Verhalten unmittelbar". Zahlreiche Handlungen würden nur vorgenommen, wenn man wisse, dass andere dies nicht bemerkten.[475] *Britz* arbeitet diesen alternativen Herleitungsweg über die Verhaltensfreiheit, den sie auch in der verfassungsgerichtlichen Rechtsprechung verwirklicht sieht, in ihrem Sammelbandbeitrag weiter aus. Zunächst greift sie zwar auch dort die Risikokonzeption der Fremderwartungen auf – bei der Begründung der Vernachlässigung der sozialen Dimension von Informationen führt sie aus, dass Freiheitsbeeinträchtigungen erst aus sozialer Interaktion und insbesondere aus der Antizipation von Fremderwartungen und Entscheidungen in Form einer Informationskontextualisierung des sozialen Gegenübers folgen.[476] Sie widmet sich dann jedoch dem Schutzgut der Verhaltensfreiheit und hält die Verankerung des Rechts auf informationelle Selbstbestimmung nach Maßgabe des BVerfG für missverständlich, denn Daten und Verfügungsbefugnis würden nicht um ihrer selbst willen geschützt. Die Regulierung fördere nur mittelbar materielle Selbstbestimmung.[477] Sodann befasst sie sich mit der These der Verhaltensauswirkungen des Volkszählungsurteils sowie mit dem Risiko von Einschüchterungseffekten und kommt zu dem Ergebnis, dass „informationelle Ungewissheit den (kommunikativen) Freiheitsgebrauch hemmt".[478]

Die Anknüpfung an das Schutzgut der Verhaltensfreiheit erfasst ihrer Ansicht nach jedoch die materielle Schutzrichtung nicht abschließend, da die Betroffenen in den entsprechenden Konstellationen der informationellen Ungewissheit nicht unmittelbar am Freiheitsgebrauch gehindert würden. Die Annahme von Verhaltensauswirkungen impliziere vielmehr die Unzumutbarkeit der Datenpreisgabe. Diesbezüglich müsse jedoch erst geklärt werden, in welchen Fällen der Wunsch, „von ungewollter Datenpreisgabe verschont zu bleiben", verfassungsrechtlich berechtigt sei.[479] Die Konkretisierung der Schutzwürdigkeit hält sie einerseits über die äußere Entfaltungsfreiheit („mit einer Offenbarung potenziell einhergehenden Nachteile") und andererseits über die Gewährleistung „innerer Entfaltungsfreiheit" für möglich.[480] Bei Letzterem verweist sie wieder auf das Risiko „heteronomer Fremdbil-

---

474 Ebd., S. 76–80.

475 Ebd., S. 77.

476 *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 567.

477 Ebd., S. 568.

478 Ebd., S. 569.

479 Ebd., S. 570.

480 Ebd., S. 570 f.

der“, wie bereits oben beschrieben, konkretisiert dieses jedoch um zwei Fallgruppen, in denen „die grundrechtliche Relevanzgrenze“ überschritten sei. Zum einen handele es sich um intensive Persönlichkeitsausforschungen, „die an eine Erstellung von Persönlichkeitsprofilen heranreichte“, sowie zum anderen um „den Umgang mit thematisch besonderen Daten und Informationen“.[481]

Ähnlich bestimmt sie auch die (sich auf die Verhaltensfreiheit beziehende) Konkretisierung über die äußere Entfaltungsfreiheit. Hier komme es für die Relevanz eines informationsbedingten Nachteils darauf an, ob „anderweitig rechtlich geschützte Aspekte äußerer Entfaltungsfreiheit“ beeinträchtigt würden.[482] Diese Ausführungen weisen eine gewisse Ähnlichkeit zur ersten Ebene der Konzeption von *Albers* auf und zeigen eine mögliche Anschlussfähigkeit zu deren Konzeption.[483] Die Forderung nach einer Anknüpfung an die Verhaltensfreiheit unterstreicht *Britz* in ihrem Fazit: Die Notwendigkeit des Schutzes informationeller Selbstbestimmung lasse sich häufiger auf Aspekte der äußeren Entfaltungsfreiheit stützen, welche durch die allgemeine Handlungsfreiheit und die speziellen Freiheitsrechte geschützt sei; entsprechend greife eine ausschließliche Verankerung im Allgemeinen Persönlichkeitsrecht zu kurz. Der Grundrechtsschutz sei darüber hinaus akzessorisch, da ihn nicht bereits jeder Nachteil, sondern erst ein verfassungsrechtlich relevanter Nachteil auslöse. Das Recht auf informationelle Selbstbestimmung schütze die Unbefangenheit des Verhaltens deshalb nur mittelbar.[484] Die Verhaltensfreiheit müsse „funktional eingriffsäquivalent“ gehemmt werden, „wenn von bestimmten Verhaltensoptionen nur um den Preis ‚freiwilliger’ Offenbarungen Gebrauch gemacht werden könnte, vor denen die Betroffenen wegen der drohenden nachteiligen Entscheidungen anderer oder wegen der Bedrohung innerer Entfaltungsfreiheit gerade geschützt werden müssen“.[485]

*Britz* setzt ihre Ausführungen dann fort, indem sie untersucht, inwieweit auch Gefährdungen im Vorfeld einer konkret nachteiligen Informationsverwendung die von ihr geforderte Relevanz hinsichtlich des Schutzguts Verhaltensfreiheit erlangen können.[486]

Im Ergebnis beschränkt sie dann den Grundrechtsschutz auf besondere Gefährdungslagen und bildet sechs Fallgruppen, für die sie besondere Risiken annimmt. Hierzu zählt sie erstens die „Kombination der abstrakten Absehbarkeit realistischer Verwendungszusammenhänge einerseits und der Intensität des damit verbundenen Nachteils andererseits“; zweitens „Daten und Informationen, die inhaltlich von vornherein ein besonders hohes Risiko nachteiliger Verwendung bergen, ohne dass

---

481 Ebd., S. 572.

482 Ebd., S. 571.

483 Siehe oben III.A.1.

484 *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 573 f.

485 Ebd., S. 574.

486 Ebd., S. 577.

sich bereits eine konkrete Verwendungsabsicht abzeichnen müsste"; drittens heimliche Daten- und Informationserhebungen; viertens „die Verwendung von statistischen Annahmen und deren Kombination mit konkreten personenbezogenen Daten zur Gewinnung weitergehender Informationen über eine Person"; fünftens die elektronische Datenverarbeitung besonders großer Informationsbestände „mit für den Einzelnen nicht mehr überschaubaren Verwendungs- und Verknüpfungsmöglichkeiten" und sechstens den Bruch berechtigter Vertraulichkeitserwartungen.[487] Bei der fünften Fallgruppe sieht *Britz* besondere Gefahren „aus der Fehleranfälligkeit von Massenvorgängen, die das Risiko falscher Entscheidungen zum Nachteil der Betroffenen" mit sich bringen, eine intensivere Verhaltenskontrolle ermöglichen und wegen des Personenkreises die Wahrscheinlichkeit einer konkret nachteiligen Verwendung erhöhen.[488]

Insgesamt weisen die Ausführungen von *Britz* zum Schutzgut der Verhaltensfreiheit damit zutreffend auf die Problematik einer weitgehenden Unterstellung der rechtlichen Relevanz informationsbedingter Verhaltensauswirkungen in der Rechtsprechung des BVerfG und tragen damit zur Konturierung dieses Schutzguts bei. Die von Britz im Ergebnis herangezogenen Fallgruppen besonderer Gefährdungslagen bestätigen zum Teil die aus der Normen- und Rechtsprechungsanalyse gewonnenen Risikokonzeptionen der vorangegangenen Abschnitte. So lassen sich die Fallgruppen 1 bis 3 sowie 5 dem Risiko der Überwachungsbedrohung auf gesamtgesellschaftlicher Ebene zuordnen und konkretisieren dies insbesondere durch die nähere Beschreibung der fünften Fallgruppe. Die zweite Fallgruppe weist darüber hinaus auf die Diskriminierungs- und Stigmatisierungsrisiken hin. Fallgruppe 4 verdeutlicht dagegen die Risiken der „verwaltungstechnischen Entpersönlichung", der Fehlerhaftigkeit von Informationen und der Informationsemergenz. Im Rahmen der Systematisierung der Risiken in dieser Untersuchung bleibt zu klären, weshalb sich die Risiken (insb. hinsichtlich der Diskriminierung und Stigmatisierung) trotz der von *Britz* vorgenommenen Aussonderung konkret nachteiliger Informationsverwendungen auch auf individueller Ebene befinden. Dieser Umstand lässt darauf schließen, dass es Risiken gibt, die sich sowohl der individuellen, als auch der gesamtgesellschaftlichen Makroebene zuordnen lassen.

#### *d) Bruch von Vertraulichkeitserwartungen*

Näher zu betrachten ist die sechste der von *Britz* für besonders risikoreich angesehenen Fallgruppen, der Bruch berechtigter Vertraulichkeitserwartungen. Hierbei verweist sie auf den Privatsphärenschutz von Art. 10 und Art. 13 GG sowie auf das IT-Grundrecht. Es handele sich um Bereiche, in denen die Betroffenen auf die informationelle Abschirmung vertrauten und denen sie ihre nicht für die Öffentlich-

---

[487] Ebd., S. 580 f.

[488] Ebd., S. 580.

keit bestimmte Kommunikation anvertrauten. Besonderer Schutzbedarf folge aus der Konzentration geheimer Kommunikation in den extra dafür vorgesehenen Vertraulichkeitssphären.[489] Der Grundrechtsschutz werde „insoweit jedoch maßgeblich durch jene Grundrechte geleistet, die bestimmten Vertraulichkeitserwartungen eine verfassungsrechtliche Berechtigung zuordnen". Die bereichsspezifischen Regelungen seien insoweit Spezialregelungen zum Recht auf informationelle Selbstbestimmung.[490] Den Schutz der Vertraulichkeitserwartungen dehnt sie dann über eine Schutzpflichtkonzeption auch auf Risiken vonseiten Privater aus.[491]

*Britz* greift hier also die sich bereits in den Entscheidungen des BVerfG und des EuGH abzeichnende normative Konkretisierung[492] der Vertraulichkeitserwartung mit den oben beschriebenen Problemen auf.

### *e) Aussonderung von Nicht-Risiken*

In ihrem Aufsatz befasst sich *Britz* auch mit der Ergänzung der abwehrrechtlichen Dimension des Rechts auf informationelle Selbstbestimmung durch Schutzpflichten und geht dabei auf Grundrechtsgefährdungen privater Dritter ein. Hier sieht sie vor allem ein „grundrechtsrelevantes Nachteilspotenzial der informationsbedingten Verweigerung von Vertragsverhältnissen".[493] Weniger eindeutig positioniert sie sich zum „Nachteilspotenzial der kommerziellen Verarbeitung und Nutzung von Kundendaten" zu „Werbe-, Markt- und Meinungsforschungszwecken". Eine grundrechtsrelevante Freiheitsbeschränkung sieht sie hier nur bei „aggressiven Vertragsschlusspraktiken", bei denen „Kunden Verträge geradezu aufgenötigt werden". Dieses Verhalten sei jedoch auf das Vertragsanbahnungsverhältnis begrenzt und nicht auf die Informationsmaßnahme selbst. Beschränke sich diese auf „schlichte Werbung", sei von vornherein zu bezweifeln, dass die „Grenze zu bloß lästigem Verhalten" überschritten sei. Die Verarbeitung von Kundendaten hält sie für „unter Nachteilsvermeidungsaspekten" kaum angemessen durch den Gedanken der informationellen Selbstbestimmung erfassbar und verweist auf die Zuordnung kommerzieller Verwertungsbefugnisse als richtigen, jedoch in Art. 14 GG anzusiedelnden Weg.[494]

Festzuhalten bleibt somit die Aussonderung eines in der öffentlichen Diskussion besonders mit Datenschutzrecht verbundenen Bereichs – der Schutz vor privater kommerzieller Datenverarbeitung – aus der Risikokonzeption sowie die Zuordnung zu „bloß lästigem" Verhalten.

---

489 Ebd., S. 580.

490 Ebd., S. 580 f.

491 Ebd., S. 588 ff.

492 Vgl. oben Teil 2, II.B.2.e) sowie Teil 3, II.B.7.

493 *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 586.

494 Ebd., S. 586.

### 3. Zwischenergebnis

Die maßgeblich aus dem Gedanken der Selbstdarstellung entwickelte Konzeption von *Britz* verweist auf zwei Schutzgüter: erstens einen „inneren Freiraum", der auf das von ihr gewählte vorrechtliche Autonomiekonzept zurückzuführen ist und dem sie das maßgebliche Risiko von Fremdbildzuschreibungen und dadurch erfolgender Beeinträchtigung der inneren Komponente der Entfaltungsfreiheit entnimmt.[495] Daneben widmet sie sich zweitens auch dem Schutzgut der Verhaltensfreiheit und weist hier auf die Problematik informationsbedingter Verhaltensanpassungen hin. Die von ihr vorgeschlagenen Fallgruppen rechtlich relevanter Gefährdungslagen lassen sich den in den vorangegangenen Abschnitten dieser Untersuchung erarbeiteten Risiken zuordnen.[496] Das Risiko des Bruchs relevanter Vertraulichkeitserwartungen konstruiert *Britz* normativ und vergleichbar mit den Rechtsprechungskonzeptionen.[497] Daneben sieht sie in der kommerziellen Nutzung privater Daten kein grundrechtsrelevantes Risiko, sondern stuft diese Verarbeitungen als „bloß lästig" ein.[498]

## C. Reformgutachten (Roßnagel/Pfitzmann/Garstka)

### 1. Überblick

Eine sich dezidiert für die Identifikation einschlägiger Risiken aussprechende Arbeit stellt das im Oktober 2001 vorgelegte Reformgutachten der Professoren *Roßnagel/Pfitzmann/Garstka* dar.[499] Es entstand im Auftrag des BMI und zielte auf eine – freilich nie zustande gekommene – umfassende Neuregelung des einfachgesetzlichen Datenschutzrechts in Form einer zweiten Stufe zur BDSG-Reform des Jahres 2001. Anlass für die Reformbemühungen waren die Unübersichtlichkeit des bestehenden einfachgesetzlichen Datenschutzrechts, technische Entwicklungen, die seinerzeit mangelhafte Umsetzung der Europäischen Datenschutzrichtlinie sowie Anforderungen der Internationalisierung und Globalisierung.[500] Das unter Beteiligung weiter Kreise der Fachöffentlichkeit[501] entstandene Gutachten beginnt mit einer Analyse des faktischen und normativen Reformbedarfs des seinerzeitigen Datenschutzrechts und leitet daraus folgende vier Forderungen ab: Datenschutz-

---

495 Siehe oben III.B.2.a) und b).

496 Siehe oben III.B.2.c).

497 Siehe oben III.B.2.d).

498 Siehe oben III.B.2.e).

499 *Roßnagel/Pfitzmann/Garstka*, Gutachten, 2001. Dazu *Kilian*, CR 2002, 921 ff.

500 *Roßnagel/Pfitzmann/Garstka*, Gutachten, S. 10.

501 Ebd., S. 11.

recht müsse effektiver, risikoadäquat, verständlich und attraktiv werden.[502] Keinen Änderungsbedarf sieht das Gutachten hinsichtlich des Rechts auf informationelle Selbstbestimmung, welches es als Schutzgut des Datenschutzrechts versteht.[503] Für ein modernes Datenschutzrecht sei die größere technische Unterstützung der „normativen Ziele" des Datenschutzrechts geboten. Diese normativen Ziele sieht das Gutachten in Zweckbindung, Selbstbestimmung, Erforderlichkeit, Vermeidung von Personenbezug sowie der Wahrnehmung von Betroffenenrechten. Weiterhin soll über die Verarbeitung der personenbezogenen Daten, über zusätzliche Informationspflichten und Auskunftsrechte höhere Transparenz geschaffen werden. Der Personenbezug soll durch Anonymisierung und Pseudonymsierung vermieden, die Entscheidungsautonomie der Einzelnen und der Datenschutz in eine Informationsordnung eingegliedert werden, die aus den Elementen informationelle Grundversorgung, Informationsfreiheit und informationelle Selbstbestimmung bestehe. Die Umsetzung habe durch drei „Instrumente" zu erfolgen, die im Rahmen der Vorschläge zur Umsetzung genauer beschrieben werden. Es handelt sich dabei um 1) den Systemdatenschutz – hierunter wird eine von *Podlech* stammende Konzeption technikunterstützten Datenschutzes verstanden –, 2) den Selbstdatenschutz im Sinne der selbstbestimmten Nutzung technischer und organisatorischer Schutzinstrumente sowie 3) eine Anreizorientierung mittels Auditing und Zertifizierungen.[504]

### 2. Risikokonzeptionen und Schutzgüter

#### *a) Schutzgut informationelle Selbstbestimmung*

Relativ kurz befasst sich das Gutachten mit dem einschlägigen Schutzgut. Dieses sei in der informationellen Selbstbestimmung zu sehen, die in drei Ausprägungen zu berücksichtigen sei: Ihren „Kern" habe sie im Schutz der Persönlichkeit und der Menschenwürde. Sie dürfe jedoch nicht auf das Persönlichkeitsrecht aus Art. 2 Abs. 1 GG reduziert werden und gewinne ihre Kraft vielmehr durch ihre Bedeutung als „Grundlage einer freien und demokratischen Kommunikationsverfassung".[505] Das Schutzgut sei vom BVerfG als „risikoorientierte Ausprägung der Grundrechte in der Informationsgesellschaft entwickelt" worden.[506] Jede Datenverarbeitung gegen den Willen des Betroffenen sei ein Eingriff. Die Frage des Eingriffs sei nicht von der Person des Eingreifenden, sondern vom Schutzgut der informationellen Selbstbestimmung her festzustellen, weshalb „es für die Eingriffsqualität grundsätzlich keinen Unterschied" mache, ob die Datenerhebung durch eine staatliche Behörde oder ein privates Unternehmen erfolge. Die damit

---

[502] Ebd., S. 34.

[503] Ebd., S. 35.

[504] Ebd., S. 35–42 sowie zum Ganzen die Zusammenfassung bei *Kilian*, CR 2002, 921 (922) m.w.N.

[505] *Roßnagel/Pfitzmann/Garstka*, Gutachten, S. 59.

[506] Ebd., S. 14.

einhergehenden grundrechtsdogmatischen Brüche versucht das Gutachten zu lösen, indem es eine unmittelbare Abwehrfunktion nur gegenüber dem Staat begründet und bei Privaten die mittelbare Wirkung über den Charakter der informationellen Selbstbestimmung als Teil der „objektiven Wertordnung" heranzieht.[507]

Das Gutachten bleibt damit bei einer Gleichsetzung des Grundrechts mit dem Schutzgut stehen und verweist im Übrigen auf die übergeordnete Bedeutung der informationellen Selbstbestimmung als Grundlage einer Kommunikationsverfassung und Teil der objektiven Wertordnung sowie auf ein risikoorientiertes Grundrechtsverständnis des BVerfG. Die fehlende Hinterfragung des Rechts auf informationelle Selbstbestimmung als Schutzgut dürfte dabei auf die spezifisch einfachrechtliche Zielsetzung des Gutachtens zurückzuführen sein, erscheint gleichwohl angesichts der zahlreichen Kontroversen um das Recht auf informationelle Selbstbestimmung und der expliziten Anerkennung einer „risikoorientierten" Ausprägung inkonsequent.

### *b) Implizite Risikokonzeption*

Trotz des Verweises auf die „risikoorientierte" Ausprägung und die vom Gutachten immer wieder herausgehobene Forderung nach „Risikoadäquanz" des Datenschutzrechts findet eine Konkretisierung einschlägiger Risiken nur in geringem Maße statt. So deutet die erste zusammenfassende These des Gutachtens zwar die Makrorisiken für Demokratie und Wirtschaftsordnung an: „Teilhabe und Teilnahme an demokratischer Willensbildung" und freier Wirtschaftsverkehr seien „nur zu erwarten", „wenn jeder Teilnehmer sein Handeln auf freier Willensbildung gründen kann".[508] Die tatsächlichen Verhaltensauswirkungen werden an dieser Stelle aber nicht weiter belegt. Später gehen die Gutachter auf eine Studie ein, der zufolge Versicherungen hinsichtlich des Umgangs mit personenbezogenen Daten nur das Vertrauen von 30 % der deutschen Bevölkerung genießen, womit sie die wirtschaftlichen Auswirkungen des Vertrauensverlusts ansprechen: Ein moderner Datenschutz sei für „alle künftigen Ausprägungen der Informationsgesellschaft und Informationswirtschaft von herausragender Bedeutung." „Ohne ausreichenden Datenschutz" würden sich viele Bürger verweigern.[509] In ähnlicher Weise wie bei der im Rahmen des Vertrauensverlusts zugrundeliegenden Prämisse von Verhaltensänderungen wird das Risiko von „Datenmissbrauch" ebenfalls mittels einer die Befürchtungen der Bürger aufzeigenden Studie angesprochen.[510] Nicht thematisiert wird hingegen, was unter Datenmissbrauch zu verstehen sein soll und welche Folgen die Befürchtungen der Bürger haben. Im selben Abschnitt werden dann techni-

---

[507] Ebd., S. 46 f.
[508] Ebd., S. 13.
[509] Ebd., S. 21.
[510] Ebd., S. 22.

sche Potenziale moderner Informationstechnologie beschrieben, und es wird ausgeführt, dass interaktive Kommunikation auch sensible Bereiche wie Sexualität, Gesundheit und Religion betreffen kann, wobei auf den durch die gestiegene Bedeutung privater Datenverarbeitung bedingten „Rollenwechsel zwischen den Betroffenen der Datenverarbeitung einerseits und den Beteiligten an der Datenverarbeitung andererseits“ in interaktiven Medien hingewiesen wird.[511] Nur kurz erwähnt wird das Risiko der Informationspermanenz.[512] Im Übrigen verharrt das Gutachten bei einer impliziten Konzeption: Die im Volkszählungsurteil beschriebenen Risiken würden „noch immer bestehen“. Zitiert wird hierzu der Abschnitt des Urteils, das die Möglichkeiten von Verhaltensauswirkungen und psychischem Druck thematisiert.[513] Zum Beleg der „Verschärfung der Gefährdungen“ werden erneut technische Potenziale beschrieben, darunter der Einsatz von Globally Unique Identifiers (GUIDs) in von bestimmten Programmen erstellten Dokumenten sowie verdeckte „Histories“, mit denen der Entstehungsprozess eines Dokuments zurückverfolgt werden kann.[514]

Eine nähere Beschreibung des gefährdeten Guts oder der Auswirkungen des Technikeinsatzes findet nicht statt. Das Gleiche gilt für die im Anschluss vorgenommene Darstellung kommerzieller Datennutzungen. Dabei wird das credit scoring mit dem Risiko von Diskriminierungen in Zusammenhang gebracht, da die durch das Verfahren gewonnenen Werte nicht exakt seien und deshalb nur unsichere Informationen lieferten. Ohne nähere Bestimmung werden Risiken in der Kategorie von Kommunikationsdaten („wer, wann, von welchem Ort, wohin, mit wem kommuniziert“) gesehen, da damit die Frage beantwortet werden könne, wer sich wann an welchem Ort aufgehalten habe.[515] Hinsichtlich „digitaler Dokumente“ wird auf das durch die Intransparenz begünstigte Risiko von Manipulation sowie von Kopien und Weiterverbreitung verwiesen; in diesem Zusammenhang werden die Möglichkeiten der unbemerkten Marktforschung und nicht als solcher erkennbarer Internetwerbung genannt.[516] Unter anderem aus diesen Gründen wird abschließend auf die Notwendigkeit einer risikoorientierten Interpretation der Rechtsprechung des Bundesverfassungsgerichts geschlossen.[517]

Das Gutachten greift damit zwar Risiken auf, die sich auch in der Rechtsprechungsanalyse gezeigt haben; angesichts der Forderung nach einer risikoorientierten Interpretation und Neukonzeption bleiben diese jedoch zu undifferenziert. So verweist es neben den oben angesprochenen Risiken z.B. auch auf „immaterielle

---

511 Ebd., S. 23.
512 Ebd., S. 25.
513 Ebd., S. 26.
514 Ebd., S. 26.
515 Ebd., S. 27.
516 Ebd., S. 29.
517 Ebd., S. 54 f.

Schäden", die das eigentliche Risiko des Datenschutzrechts sein sollen, soweit sie auf schweren Verletzungen des Persönlichkeitsrechts beruhten.[518] Eine nähere Klassifizierung dieser Verletzungen oder des Schadens wird nicht vorgenommen. Insgesamt spricht das Gutachten, wie beispielsweise bei den Ausführungen zu neuen Technikpotenzialen und kommerzieller Datenverarbeitung, eine eher intuitive Ebene an. Dieser Ansatz kann deshalb aufgrund der Ausrichtung auf intersubjektive Überzeugungskraft auch als „intuitive Risikokonzeption" charakterisiert werden.

### *c) Profilbildung*

Von den eher intuitiven und lediglich angedeuteten Risiken heben sich die Ausführungen zu Profilbildungen ab, die als besondere Gefahr für die informationelle Selbstbestimmung angesehen werden.[519] Nach einer Beschreibung der gestiegenen Bedeutung privater Datenverarbeitung führen *Roßnagel/Pfitzmann/Garstka* aus, dass private Unternehmen „nicht selten über aussagekräftige Profile zu Kaufkraft, Kaufgewohnheiten und Kreditwürdigkeit" verfügten. Anhand von Bewertungsmodellen würde entschieden, „welcher Nutzen von dem Kunden für das Unternehmen noch zu erwarten sei". Profilhändler seien in der Lage, „spezifische Persönlichkeitsprofile" zu liefern. Dafür würden „hochsensitive Daten" aus der „privaten Lebenssphäre" erfasst, mit öffentlich zugänglichen Daten kombiniert und für Marketing- und andere Zwecke verwendet. Der Orwell'sche „Big Brother"-Staat ängstige die Bürger „mittlerweile weniger als der unüberschaubare Datenaustausch beim modernen Adresshandel".[520] Personenbezogene Daten werden als „Abbild der sozialen Beziehungen" beschrieben, wobei „Gesamtbilder" verfassungsrechtlich zu verhindern seien. Das „eigentliche Problem" bestehe in der „Erstellung von Profilstrukturen und der Einbindung einzelner Daten in diese Struktur". Das Risiko für die informationelle Selbstbestimmung liege nicht so sehr im einzelnen Datum, sondern in der Gesamtinformation, die die verantwortliche Stelle durch Kombination erlangen könne. Als Beispiel wird der Internethandel genannt, bei dem eine Vielzahl „von für sich genommen möglicherweise" harmlosen Einzelinformationen zur Entwicklung individueller „Nutzer- und Kundenprofile" führen könne, mit der sich „mit hoher Aussagekraft Präferenzen, Bedürfnisse, Kaufgewohnheiten und sonstige Verhaltensweisen" beschreiben ließen.[521]

Zwar bleibt auch hier unklar, worin das eigentliche Problem der kommerziellen Nutzung liegt, doch expliziert das Gutachten die zu erwartenden Folgen im anschließenden Abschnitt: Die „vielfältige Reproduzierbarkeit des Persönlichkeitsprofils" bewirke ein „Gefühl des Ausgeliefertsein" und ein „Wissen um Fremd-

---

518 Ebd., S. 19 und 182.

519 Ebd., S. 16.

520 Ebd., S. 24.

521 Ebd., S. 117.

beobachtung“. Beides könne zu Verhaltensanpassungen führen und stelle den Anspruch des Betroffenen, „als selbstverantwortliche und selbstbestimmte Persönlichkeit respektiert zu werden“, infrage. Es bliebe kein Raum für eine „eigene Rolleninterpretation in sozialen Zusammenhängen, wenn der Interaktionspartner schon umfassend informiert“ sei.[522]

Sodann werden die Risiken unter Verweis auf *Ladeur* relativiert, „da in der Praxis niemand an der Erstellung von Totalabbildern interessiert“ sei. „Die meisten Persönlichkeitsprofile“ seien mangels Eingriffsintensität nicht verfassungswidrig. Gleichwohl sei eine Regelung nötig, um ihren „spezifischen Risiken“ adäquat zu begegnen. Im Weiteren definiert das Gutachten den Begriff „Persönlichkeitsprofil“ im Anschluss an ältere Arbeiten: Ein Profil entstehe, „wenn über das Zusammenführen von Einzeldaten hinaus zusätzliche, bisher nicht vorhandene Erkenntnisse über die Persönlichkeit der betroffenen Person gewonnen und zu einem (Teil-) Abbild der Persönlichkeit zusammengeführt“ würden.[523] Auffällig hieran ist wiederum die Nähe zum Risiko der Entkontextualisierung. Im Anschluss spricht sich das Gutachten gegen ein Totalverbot von Profilen aus und macht deren Zulassung durch Einwilligung oder Erlaubnistatbestand von einer Reihe einschränkender Kriterien abhängig.[524]

Dem Topos „Persönlichkeitsprofil“ wird in dem Gutachten damit ein besonderer Stellenwert zugeordnet, wobei die damit verbundenen Risiken insbesondere in der durch ein Gefühl des „Ausgeliefertseins“ und der „Fremdbeobachtung“ vermuteten Verhaltensanpassung liegen sollen. Daneben wird ein Risiko für die Persönlichkeitsbildung im weiteren Sinne aufgegriffen, welches durch die fehlende Möglichkeit eigener Rolleninterpretationen in sozialen Kontexten ausgelöst werden soll. Mit diesen Bezügen zur Rollentheorie und der Vorstellung von Daten als Abbildern sozialer Beziehungen steht das Gutachten in der Tradition älterer Literaturkonzeptionen, insbesondere derjenigen von *Mallmann*[525] und *Steinmüller*.[526]

### 3. Zwischenergebnis

Das BMI-Gutachten von *Roßnagel/Pfitzmann/Garstka* zielt auf eine Modernisierung des einfachgesetzlichen Datenschutzrechts, wobei dessen fehlende Risikoadäquanz einen entscheidenden Grund für die Forderung nach umfassender Reform darstellt. Entsprechend der einfachgesetzlichen Zielrichtung wird das Recht auf informationelle Selbstbestimmung als Schutzgut des Datenschutzrechts verstanden

---

522 Ebd., S. 117 f.

523 Ebd., S. 118.

524 Ebd., S. 119 f.

525 Siehe unten III.E.

526 Vgl. *Steinmüller*, NfD 1993, 215 (217).

und nicht weiter hinterfragt.[527] Trotz der wichtigen Rolle, die der Identifikation von Risiken in der Konzeption von *Roßnagel* zufällt, konkretisiert das Gutachten einschlägige Risiken nur in geringem Umfang. Zwar werden Risiken, die bereits in der Rechtsprechungsanalyse identifiziert wurden, thematisiert; auffällig ist jedoch die mehr oder minder implizite Argumentationsweise, die auf eine eher gefühlsmäßig-intuitive Überzeugungskraft abzuzielen scheint.[528] Relativ umfassend beschäftigt sich das Gutachten dagegen mit dem Risiko der Profilbildung. Hier wird im Rahmen der Definition des Begriffs „Persönlichkeitsprofil" auf das Risiko der Entkontextualisierung eingegangen. Die beiden zentralen Risiken der Profilbildung sieht das Gutachten jedoch einerseits in Verhaltensanpassungen durch ein Gefühl des „Ausgeliefertseins" bzw. durch „Fremdbeobachtungen" sowie zweitens in Problemen der Persönlichkeitsentwicklung durch fehlenden Raum für Rolleninterpretationen. Insgesamt steht das Gutachten damit in der Tradition älterer Literaturkonzeptionen.[529]

## D. Ubiquitätskonzeption (Roßnagel)

### 1. Überblick

Eine spezifisch mit dem Phänomen des *ubiquitous computing* verbundene Arbeit hat *Alexander Roßnagel* in einem Gutachten für die Friedrich-Ebert-Stiftung (FES) aus dem Jahr 2007 vorgelegt. Es befasst sich in einem Kapitel explizit mit Datenschutzrisiken und steht darüber hinaus in der Tradition älterer, dem Topos „Informationsmacht" eine besondere Bedeutung zumessender Literaturkonzeptionen,[530] weshalb es hier neben den Konzeptionen von *Albers* und *Britz* eigenständig behandelt wird. Auch hebt es sich von dem ebenfalls von *Roßnagel* mitverfassten BMI-Gutachten ab, da es stärker als dieses auf bestimmte Kategorien von Risiken eingeht.

*Roßnagel* beginnt seine Untersuchung mit einer phänomenologischen Schilderung technischer Entwicklungspotenziale, Anwendungsfelder und Szenarien der unter dem Sammelbegriff *ubiquitous computing* zusammengefassten Veränderungen der Informations- und Kommunikationstechnologien.[531] Der auf den US-amerikanischen Wissenschaftler *Mark Weiser* zurückgehende Begriff *ubiquitous computing* steht dabei für Technologien, bei denen Daten nicht mehr nur in Computern im herkömmlichen Sinne, sondern in nahezu allen Alltagsdingen (z.B. Klei-

---

527 Siehe oben III.C.2.a).

528 Siehe oben III.C.2.b).

529 Siehe oben III.C.2.c).

530 Vgl. den Verweis auf *Steinmüller*, *Roßnagel*, Gutachten FES, S. 111 sowie *Roßnagel/Wedde/Hammer/Pordesch*, Digitalisierung, S. 38 ff., 118 ff., 164 ff.

531 *Roßnagel*, Gutachten FES, S. 9–81.

dung, Haushaltsgeräte oder Möbel) und damit allgegenwärtig verarbeitet werden.[532] Anschließend beschreibt *Roßnagel* Datenschutzrisiken in drei Kategorien mit verschiedenen Unterabschnitten. Weitere Kapitel betreffen den Schutz der informationellen Selbstbestimmung, Datenschutztechnik und Konzepte zur Modernisierung des Datenschutzrechts. Seine Ausführungen beziehen dabei zum Teil das Gutachten für das BMI zur Reform des Datenschutzrechts aus dem Jahr 2001 ein und entwickeln dortige Ansätze weiter.[533]

*Roßnagel* kommt zu dem Ergebnis, dass eine „Frontstellung" zwischen Datenverarbeitern und Betroffenen die Voraussetzung für die Eignung des normativen Schutzkonzepts des Datenschutzrechts de lege lata sei[534] und dass das *ubiquitous computing* das überkommene Schutzprogramm des Datenschutzrechts in jeder Hinsicht aushöhle oder überspiele.[535] Als Lösungsansatz schlägt er insbesondere Datenschutz durch Technik,[536] permanent zu beachtende Gestaltungsregelungen,[537] Vorsorgevorschriften für potenziell personenbeziehbare Daten[538] sowie die Einschränkung der Ausnahme vom Verarbeitungsverbot für private Datenverarbeitungen vor.[539] Übergreifend fordert er eine Reform zugunsten eines risikoadäquaten und einfachen Datenschutzrechts.[540] Im Folgenden werden die von ihm dafür vorgebrachten Risikokonzeptionen und Schutzgüter untersucht.

### 2. Risikokonzeptionen und Schutzgüter

#### *a) Verhaltensauswirkungen und implizite Risiken*

*Roßnagel* zufolge birgt die allgegenwärtige Datenverarbeitung Risiken für die informationelle Selbstbestimmung, die Entscheidungsfreiheit, die Entfaltungsfreiheit, „die Ausübung vieler anderer Grundrechte" und die demokratische Ordnung.[541] Er untergliedert sie in fünf Kategorien: „allgegenwärtige Datenverarbeitung", „allgegenwärtige Datenweitergabe und -nutzung", „Ausspähen von Daten", „Verhaltensbeeinflussungen" und „allgegenwärtige Überwachung".

---

532 *Weiser* beschrieb 1991 das *ubiquitous computing* als „calm technology, when technology recedes into the background of our lives" und als „computing, that does not live on a personal device of any sort, but is in the woodwork everywhere", zit. nach ebd., S. 10 f.

533 *Roßnagel/Pfitzmann/Garstka*, Gutachten, hierzu siehe oben Teil 3, III.C.

534 *Roßnagel*, Gutachten FES, S. 120.

535 Ebd., S. 155.

536 Ebd., S. 158 ff.; 172 ff.; 183 ff.

537 Ebd., S. 179 ff.

538 Ebd., S. 185 ff.

539 Ebd., S. 192 ff.

540 Ebd., S. 176.

541 Ebd., S. 85.

In der ersten Kategorie geht er zunächst auf die Intransparenz unbemerkter Datenerhebungen ein und verbindet diese Feststellung mit der Annahme von Verhaltensanpassungen: „Die Ahnung aber, dass jedes Verhalten irgendwo und irgendwie registriert werden könnte, wird zu Verhaltensanpassungen führen“.[542] Sodann greift er den Aspekt der automatischen Datenerhebung auf. Nach einer Beschreibung der zu erwartenden qualitativen und quantitativen Veränderung der Verarbeitungsweise geht *Roßnagel* auf die Unterschiede zur bisherigen Datenverarbeitung ein. Diese ermöglichte ein „Wahrnehmen und Erinnern“ und damit „Chancen, durch das eigene Verhalten im Voraus oder im Nachhinein darauf zu reagieren“. Die Mitwirkungsnotwendigkeit des Betroffenen erlaubte die Abgrenzung von anderen Handlungsvollzügen und damit „die Chance zu wissen, was sein Kommunikationspartner über ihn wissen kann“. Diese entfalle mit der neuen, durchgängig automatisierten „Datenerhebung potenziell jeder Handlung“, da es schon an dem Bewusstsein über die Momente der Erhebung mangele.[543] Fehlende Überschaubarkeit leitet er sodann auch aus dem Umfang allgegenwärtiger Datenverarbeitung ab („Fülle und Komplexität“). In dieser Fallgruppe benennt er jedoch die konkreten Nachteile für das Individuum nicht, sondern impliziert diese mit der Beschreibung technischer Potenziale. Nicht ganz deutlich wird dann auch der Unterschied zum nächsten von ihm beschriebenen Risiko der „Ständigen und ubiquitären Datenerhebung“. Auch hier erfolgt eine phänomenologische Beschreibung der Leistungsfähigkeit moderner Technologie, wobei er vor allem auf die zeitliche Komponente eingeht. Die eigentlichen konkreten Nachteile werden auch hier nur impliziert.[544] Das letzte Risiko der ersten Kategorie sieht *Roßnagel* in der erhöhten Aussagekraft der Daten, wobei auch hier die konkreten Nachteile nicht ausdrücklich dargestellt werden. Aus den fünf beschriebenen Eigenschaften der allgegenwärtigen Datenerhebungen (Heimlichkeit, Automatisierung, Umfang, zeitliche Komponente, Aussagekraft) folgert er zusammenfassend das Risiko der Ermöglichung einer „Alltagsüberwachung“.[545]

Die Risiken der Verhaltensauswirkung und Alltagsüberwachung greift *Roßnagel* auch in seiner vierten und fünften Risikokategorie auf. Die Eigenschaften allgegenwärtiger Datenverarbeitung ermöglichten es, „das Verhalten und die Präferenzen eines Menschen“ „(fast) immer“ vorherzusagen. Dies könnten die Dateninhaber zur Verhaltensbeeinflussung durch „Informationssteuerung“ benutzen.[546] Hier geht es *Roßnagel* also zunächst nicht nur um die unbewusste Anpassung im Sinne der Konformitätsthese des BVerfG, sondern vielmehr um eine aktive, informationsinduzierte Manipulation. Die Konformitätsthese wiederholt er im unmittelbaren

---

[542] Ebd., S. 86 f.
[543] Ebd., S. 88.
[544] Ebd., S. 90 f.
[545] Ebd., S. 94.
[546] Ebd., S. 100.

Anschluss daran jedoch am Beispiel von Kreditinformationen: Die Unsicherheit über das Wissen anderer führe dazu, dass man sich so verhalte, „wie man vermutet, dass es der andere erwartet". *Roßnagel* verweist auf die Konformitätsthese des BVerfG und führt aus, dass „allein durch die Überwachungsarchitektur das Verhalten von vielen Menschen gesteuert" werden könne. „Realistisch betrachtet" werde der Betroffene „in vielen Fällen sein allgemeines Persönlichkeitsrecht zurückstellen, um nicht finanzielle oder gesellschaftliche Nachteile in Kauf nehmen zu müssen". Das *ubiquitous computing* führe in „bestimmten Kontexten" zu einer Zwangslage und einer Beschränkung von „Entscheidungsalternativen".[547]

Im Anschluss an diese Ausführungen verbindet *Roßnagel* die Verhaltensauswirkungen mit dem Risiko der Informationspermanenz: Löschungsregelungen erfüllten die gesellschaftliche Entlastungsfunktion des Vergessens, und eben diese könnten bei Techniken der ubiquitären Datenverarbeitung unmöglich werden. Das dadurch ausgelöste Gefühl permanenter Kontrolle führe zu Verhaltensänderungen und zu einem nicht dem freien Willen, sondern den „vermuteten Erwartungshaltungen" entsprechenden Verhalten.[548]

In der fünften Risikokategorie beschreibt *Roßnagel* die Mittel des *ubiquitous computing* als „Überwachungstechnologie", die jedem zur Verfügung stehe. Vor allem ermöglichten Sensornetzwerke, also die Verbindung von Geräten zur technischen Erfassung physikalischer oder chemischer Eigenschaften in einem Netzwerk, die „unbemerkte, räumlich und zeitlich vollständige Überwachung". Nicht auszuschließen sei, dass sich auch die Pflicht zur Vorratsdatenspeicherung künftig auf die „Transaktionen allgegenwärtiger Datenverarbeitungen" bezöge.[549] Den Topos „Überwachung" beschreibt *Roßnagel* dabei sehr weitgehend: So führe „jede gewünschte und sinnvolle personalisierte Nutzung von Informationstechnik" „zwangsläufig" zu mehr Überwachung.[550] Wie dieses Risiko zu verstehen ist, beschreibt er im letzten Abschnitt der Untersuchung: Durch die umfassende Überwachung entstünde eine „Informationsmacht", die die „bestehende Machtverteilung in der Gesellschaft stark verändern" könne.[551]

Die Kategorien eins und zwei sowie vier und fünf von *Roßnagels* Risikokonzeption verweisen auf unterstellte Verhaltensanpassungen und basieren im Übrigen auf der impliziten Überzeugungskraft der Risikohaftigkeit von Potenzialen moderner Datenverarbeitungstechnik. Diese Art der Risikofassung wird jedoch, wie eingangs beschrieben,[552] zunehmend hinterfragt. So ließe sich beispielsweise gerade aus dem von *Roßnagel* beschriebenen fehlenden Bewusstsein für Datenverarbeitungsvor-

---

547 Ebd., S. 100 f.
548 Ebd., S. 101 f.
549 Ebd., S. 102 ff.
550 Ebd., S. 158.
551 Ebd., S. 201.
552 Siehe oben Einleitung, II.

gänge darauf schließen, dass diese mangels Kenntnis der Betroffenen keine Auswirkungen auf deren Verhalten haben. Die unterstellten Verhaltensauswirkungen müssten an dieser Stelle empirisch unterlegt werden. Fragwürdig erscheinen auch die pauschale Verbindung von „Überwachung" und „Nutzung der Informationstechnik" sowie der Verweis auf eine durch Überwachungstechnologie ausgelöste „Informationsmacht". Diese Argumentationsweise erinnert an die von *Ehmann* aufgezeigten Versuche älterer Literaturkonzeptionen, den Interessengegensatz zwischen Besitzenden und Nichtbesitzenden durch den Interessengegensatz zwischen Betroffenen und Datenverarbeitern zu ersetzen.[553]

### *b) Datenmissbrauch*

Die dritte Risikokategorie beschreibt Roßnagel als „allgegenwärtige Datenweitergabe und -nutzung". Die Risiken sieht er in dem „Austausch der Daten zwischen unterschiedlichen Systemen" und der „Profilierung des Nutzers".[554] Die „Interkonnektivität zwischen vielen kommunikationsfähigen Gegenständen" schaffe ein „kaum mehr zu überblickendes Datennetz". Die Datenströme seien mit „traditionellen Zugriffskontrollen" nicht mehr zu verwalten und führten zu einer „Proliferation" von Daten. Seine Argumentation mündet in der Feststellung, dass niemand im Voraus wissen oder im Nachhinein werde rekonstruieren können, welche Daten von den kommunikationsfähigen Gegenständen erhoben und zwischen ihnen kommuniziert werden.[555] Im Anschluss geht er auf Profilbildungen ein. Die Anwendungen allgegenwärtiger Datenverarbeitung erforderten die „ständig wiederholte Erhebung von Lebenssituationen des Nutzers" und ermöglichten die Erstellung sehr aussagekräftiger Profile. Diese könnten für unerwünschte Zwecke verwendet werden; als Beispiel nennt er u.a. die Interessen von Produktherstellern, Werbetreibenden, Arbeitgebern, Auskunfteien, staatlichen „Überwachungsbehörden", „des neugierigen Nachbarn" oder eines „eifersüchtigen Liebhabers".[556] Auffällig an dieser Zusammenstellung ist die Kombination legitimer gewerblicher Verarbeitungsinteressen mit zumindest sozial missbilligten Verarbeitungen durch Private.

In der nächsten Fallgruppe geht *Roßnagel* auf das Risiko von Datenmissbrauch durch das Ausspähen von Daten in Form des unerlaubten Abhörens, von „Datenlecks" und von „Einbruchsversuche[n]" in RFID-Systemen ein.[557]

Die dritte Risikokategorie ist damit im Vergleich zu den übrigen zwar konkreter, deutet jedoch auf eine Illegitimität kommerzieller Verarbeitungen hin, die aus einer Risikoperspektive erst zu belegen wäre.

---

553 Siehe ebd.

554 *Roßnagel*, Gutachten FES, S. 94.

555 Ebd., S. 96 f.

556 Ebd., S. 97 f..

557 Ebd., S. 98 ff.

*c) Subjektive und objektive Schutzgutkonzeption*

Im Anschluss an die Darstellung seiner Risikokategorien widmet sich *Roßnagel* auch dem Schutzgut der informationellen Selbstbestimmung. Sie sei „keine Frage des Schutzes von Verfügungsrechten, sondern der Freiheit".[558] Er referiert die Ausführungen des Volkszählungsurteils zur individuellen Selbstbestimmung und differenziert zwischen subjektivem Grundrecht und objektivem „Strukturprinzip einer Kommunikationsverfassung". Im Rahmen des subjektiven Grundrechts sieht er das Schutzgut in der „selbstbestimmten Entwicklung und Entfaltung des Einzelnen". Er verweist auf die Notwendigkeit der Selbstdarstellung in unterschiedlichen sozialen Rollen und auf das Erfordernis der Kontrolle von Informationspreisgaben.[559] Hinsichtlich privater Datenverarbeitungen verweist er auf die Abgrenzungsnotwendigkeit „konkurrierender Grundrechtssphären" durch den Gesetzgeber und bekräftigt das datenschutzrechtliche Verbot der Datenverarbeitung mit Erlaubnisvorbehalt für den Bereich privater Datenverarbeitungen.[560] Hinsichtlich der objektiv-rechtlichen Komponente eines Strukturprinzips bezieht er sich unter Verweis auf die *Volkszählungsentscheidung* auf die Eigenschaft der Selbstbestimmung als demokratische Funktionsbedingung und beschreibt die informationelle Selbstbestimmung als Element der „objektiven Wertordnung".[561] Im Folgenden greift er den Informationsbegriff *Steinmüllers* (Information als Modell der Wirklichkeit) auf und spricht sich für eine Kommunikationsordnung aus, in der bestimmt wird, „wer in welcher Beziehung befugt ist, mit dem Modell in einer bestimmten Weise umzugehen". Eine solche Ordnung müsse auf dem Prinzip der informationellen Selbstbestimmung basieren und Kommunikationsmöglichkeiten im überwiegenden Individual- oder Allgemeininteresse vorsehen.[562] Das „Prinzip der informationellen Selbstbestimmung" müsse beantworten, „wer über welche personenbezogenen Daten verfügen und diese in gesellschaftlicher Kommunikation verwenden können soll".[563]

### 3. Zwischenergebnis

Mit dem FES-Gutachten von *Roßnagel* liegt eine Konzeption vor, die in vielerlei Hinsicht auf dem von ihm mitverfassten BMI-Gutachten aufbaut. Es lässt sich wie das für das BMI erstellte Gutachten in die Linie älterer Literaturkonzeptionen einordnen, widmet sich jedoch im Unterschied zum BMI-Gutachten explizit verschiedenen Kategorien und Untergruppen von Risiken anhand des aktuellen Phänomens *ubiquitous computing*. Dabei werden Risiken zunächst über Verhaltensauswirkun-

---

[558] Ebd., S. 108, vgl. auch S. 111.
[559] Ebd., S. 109.
[560] Ebd., S. 109 f.
[561] Ebd., S. 110 f.
[562] Ebd., S. 111 f.
[563] Ebd., S. 119.

gen in Anlehnung an die Konformitätsthese des Verfassungsgerichts im Volkszählungsurteil konstruiert. Auffällig dabei ist jedoch, dass konkrete Nachteile für das Individuum im Vergleich zu den phänomenologischen Beschreibungen der Eigenschaften ubiquitärer Datenverarbeitung in den Hintergrund treten. Dieser Aspekt wurde bereits beim BMI-Gutachten deutlich, ist hier jedoch noch ausgeprägter. Nach der eingangs vorgenommenen Bestimmung des Begriffs „Risiko" müsste der Schaden viel konkreter bestimmt werden. Es handelt sich ebenfalls um Risiken, da *Roßnagel* diese Schäden implizit annimmt und sie zumindest bei seiner Beschreibung des Phänomens „Überwachung" etwas deutlicher als Verschiebung der Informationsmacht charakterisiert. Hier zeigen sich jedoch problematische Parallelen zu der am Beginn der Untersuchung dargestellten Kritik *Ehmanns* an den älteren Literaturauffassungen.[564] Die weiteren von *Roßnagel* beschriebenen Datenmissbräuche weisen ebenfalls Voraussetzungen auf, die deutlicher auszuführen wären; insbesondere deuten sie zum Teil auf eine zu hinterfragende Annahme einer Illegitimität kommerzieller Datenverarbeitungen hin.[565] Das Schutzgut der informationellen Selbstbestimmung beschreibt er dagegen zumindest in seiner subjektiven Ausprägung in eher konventioneller Weise. Die objektive Komponente konstruiert er hingegen als Strukturprinzip einer Kommunikationsverfassung und begünstigt damit ein hohes Maß an Regulierung.[566]

## E. Privatsphärenkonzeption (Mallmann)

### 1. Überblick

Der Frühphase des Datenschutzes lässt sich die Arbeit von *Otto Mallmann* zu Zielfunktionen des Datenschutzrechts aus dem Jahr 1977 zuordnen.[567] Der Ausgangspunkt seiner Untersuchung ist fortwährend aktuell: Es geht ihm um die Frage, „was also Datenschutz gegen welche Gefahren schützen soll". *Mallmann* unterscheidet hierbei zwischen „dem individuellen Interesse am Schutz der Privatsphäre" und dem Interesse „an der Gewährleistung korrekter Information" und untersucht dabei u.a. die „ideengeschichtliche Entstehungsbedingungen von Privatsphäre". Allerdings verweist er auf die Notwendigkeit einer weitergehenden Analyse von Konfliktsituationen in „einzelnen sozialen Bereichen", die er nur exemplarisch für den Bereich der Kreditinformationen vornimmt.[568] Ausgehend von einer historischen Analyse der außerrechtlichen und rechtlichen Entstehungsbedingungen von Privatsphäre beschreibt er zunächst zwei Risiken aus der Per-

---

564 Siehe oben III.D.2.a).

565 Siehe oben III.D.2.b).

566 Siehe oben III.D.2.c).

567 *Mallmann*, Zielfunktionen.

568 Ebd., S. 9 f.

spektive der soziologischen Rollentheorie. Diese versteht menschliches Verhalten als Rollenspiel, wobei Rollen „als vorgegebene Verhaltensmuster", Erwartungen und Ansprüche „der Gesellschaft oder einer Gruppe an den Inhaber einer sozialen Position" aufgefasst werden.[569]

### 2. Risikokonzeptionen und Schutzgüter

#### *a) Rollenfixierung und Entlastungsfunktion*

Das erste von *Mallmann* aufgegriffene Risiko liegt in einer „Rollenfixierung durch Computerdossiers" und steht damit in gewisser Nähe zu dem in der Rechtsprechungs- und Normenanalyse beschriebenen Risiko der Informationspermanenz: Der Einzelne komme „von der computerisierten Version seiner Vergangenheit nicht mehr los".[570] „Spielräume für aktive Rolleninterpretationen und spontane Ich-Leistungen" würden durch die präformierenden Vorinformationen Abhängigkeiten im Kommunikationsprozess schaffen. Zudem werde das Risiko von „Diskriminierung sozialer Randgruppen wie Vorbestrafter oder psychisch Kranker" verstärkt. „Freiräume bei der situativen Ausfüllung von Rollenerwartungen" würden beseitigt. Es drohe eine Beschränkung „individuelle[r] Lebenschancen in allen gesellschaftlichen Bereichen".[571] *Mallmann* geht dabei auch auf die Frage von Vorteilen für den Betroffenen durch allgemeine Offenheit und das „Entfallen eines doppelten moralischen Standards" ein. Dabei antizipiert er die oben angesprochenen[572] *post privacy*-Ideen. Den genannten Vorteilen erteilt er jedoch eine Absage unter Verweis auf „das gleichzeitige Nebeneinander unterschiedlicher Rollenanforderungen", die er als Folge „einer differenzierten, auf Arbeitsteilung beruhenden Sozialstruktur" ansieht.[573] Das zweite von ihm rollentheoretisch begründete Risiko liegt in der „Gefährdung der Entlastungsfunktion beschränkter Visibilität" im Sinne einer „Erholung von wechselnden Rollenanforderungen". Durch die Ausdehnung der „Darstellungsanforderungen der Wirtschafts- und Arbeitswelt" in das Privatleben werde die „Risikoschwelle bisher kaum sanktionsbeschwerter privater Kommunikation entscheidend verlagert".[574] Im Anschluss hieran beschreibt er jedoch die Unzulänglichkeiten der Rollentheorie, die er vor allem darin sieht, dass sich nicht alle Gefahren mit ihrer Hilfe erfassen ließen.[575]

---

569 Ebd., S. 36 f.
570 Ebd., S. 39 ff.
571 Ebd., S. 41 f.
572 Siehe oben, Einleitung I.
573 *Mallmann*, Zielfunktionen, S. 42.
574 Ebd., S. 43 f.
575 Ebd.

### *b) Schutzgutpaare*

Im Anschluss geht *Mallmann* kurz auf das Risiko des Bruchs von Vertraulichkeitserwartungen ein, wobei er die Handlungsauswirkungen verletzter Vertraulichkeit am Beispiel von Arztbesuchen und der Inanspruchnahme staatlicher Leistungen nennt.[576] Das Risiko entwickelt er anhand des Schutzgutpaares „Intimität und Distanz", neben dem er im Anschluss das Schutzgutpaar „Identität und Selbsteinschätzung" untersucht.[577]

Bei beiden Schutzgutpaaren rückbezieht er sich jedoch auch auf das Risiko von Fixierungen in Form von „Dossierinformationen". Die Festlegung auf Rollenmuster erschwere die „Möglichkeit abgestufter Distanzsetzung in intersubjektiven Kontakten" und wirke sich auf die „Skala intersubjektiver Beziehungen" und damit auf Intimität und Distanz als Grundlage von „Liebe, Freundschaft und Vertrauen" aus.[578] „Dossierinformationen" bestimmten darüber hinaus über die „Bewertungen der Interaktionspartner" die mit der Identität verbundene Selbsteinschätzung.[579] Auch die Unkenntnis der „Dossierinformationen" ändere nichts an der „indirekten Einwirkung gespeicherter Daten" auf das Selbstbild des Betroffenen. Darüber hinaus sei auch die Richtigkeit der Informationen kein Ausschlussfaktor für das Risiko, da die Identitätsbildung „normalerweise ein niemals abgeschlossener Prozeß" sei, der nicht auf einem bestimmten Stand festgeschrieben werden dürfe. Im Fall des Abweichens der Informationen vom Selbstbild könne es darüber hinaus zu einer Anpassung des Selbstbildes an die Einschätzungen anderer oder bei erheblich unrichtigen Angaben sogar zu schwerwiegenden Identitätskrisen bei der Internalisierung kommen.[580]

### *c) Autonomie, Apathie und Anpassung*

Nach einer historisch aufgebauten Analyse der Individualautonomie (insb. unter Abgrenzung von Isolation und Determination sowie unter Einbeziehung der frühliberalen Staats- und Gesellschaftstheorie) beschreibt *Mallmann* das Überwachungspotenzial polizeilicher Informationssysteme.[581] Einer zunehmenden Verhaltenskontrolle durch automatisierte Informationssysteme schreibt er sodann Auswirkungen auf Spontaneität und Kreativität und auf die Bereitschaft der Bürger zur Ausübung politischer Grundrechte zu, wobei er das Fehlen empirischen Materials rügt und lediglich auf eine Umfrage zum Problembewusstsein der britischen

---

576 Ebd., S. 45 f.
577 Ebd., S. 45 ff. sowie S. 47 ff.
578 Ebd., S. 45 f.
579 Ebd., S. 49.
580 Ebd., S. 49 f.
581 Ebd., S. 52 ff.

Bevölkerung verweist.[582] Nach einer weiteren Beschreibung von Überwachungstechnologien greift er auf eine empirische Untersuchung von *Jahoda/Cook*[583] über die sozialpsychologischen Konsequenzen des McCarthyismus[584] auf das Verhalten von Angehörigen des öffentlichen Dienstes in den USA zurück, um seine Risikokonzeption zu unterlegen. Zu den in der Studie beschriebenen Reaktionen auf das damalige „komplexe System formeller und informeller sozialer Kontrollen" gehörte die Herausbildung neuer „Verhaltenscodes" – u.a. „als Vorsichtsmaßnahme" die Kündigung von Mitgliedschaften in auf einer Liste des Justizministeriums geführten, als subversiv geltenden Organisationen, die Abbestellung von Abonnements der von ihnen herausgegebenen Schriften sowie der Verzicht auf Mitgliedschaften in nicht auf der Liste stehenden Organisationen aus Furcht vor einer Aufnahme in eben diese Liste.[585] *Mallmann* schließt daraus, dass das Bewusstsein intensiver politischer Überwachung „zur Einstellung oder jedenfalls starken Reduzierung politischer Aktivitäten" und zu „übervorsichtigem Verhalten und letztlich zur Vereinzelung des Individuums" führen kann. Er sieht diesen Befund sodann von lerntheoretischen Erkenntnissen bestätigt, wonach die Maximierung von Erfolgserwartungen wesentlich die Verhaltensselektion bestimme: „Überwachungsmechanismen" wirkten insoweit als „negative Verhaltensverstärker". Die Angst vor Sanktionen führe zu „übersteigerter Anpassung und politischer Apathie". Weiterhin komme es zu einer Internalisierung neuer Verhaltensstandards, deren Befolgung nach ausreichender Zeit als freiwillig angesehen werde.[586] Es komme nicht nur zu einer Verhaltensselektion, sondern auch zur Beeinflussung individueller Motivations- und Bedürfnisstrukturen. Die Überwachungsmechanismen führten zu „Apathie und Konformität", die „Bereitschaft zur Initiative im politischen und privaten Bereich" nehme tendenziell ab. „Freiräume zur Erprobung alternativer sozialer Modelle" fielen weg. Es werde ein Zwang zur Inkaufnahme sozialer Sanktionen statuiert, wenn der Einzelne nicht mehr über die Publizität von Ergebnissen selbst entscheiden könne. Der Preis sei soziale Stagnation.[587]

Die „Begrenzung von Verhaltensinformationen" verhindere dagegen, dass „die Zahnräder des normativen Verhaltenssystems allzu eng in die ungeschliffene Lebensrealität […] eingreifen". Sie ermögliche das Ausweichen, die Entdramatisierung und damit eine „Unschärfe-Relation des sozialen Lebens".[588] *Mallmann* wen-

---

582 Ebd., S. 57.

583 *Jahoda/Cook*, 61 Yale L.J. (1952), S. 295 ff.

584 Die McCarthy-Ära beschreibt einen Zeitabschnitt in der Geschichte der Vereinigten Staaten von Amerika (1947 bis ca. 1956), der sich durch starke Verfolgung echter und vermeintlicher Kommunisten auszeichnete, vgl. http://de.wikipedia.org/wiki/McCarthyism [Stand: 28.3.2014].

585 *Jahoda/Cook*, zit. nach *Mallmann*, Zielfunktionen, S. 60.

586 So unter Verweis auf *Jahoda/Cook* und eine Studie von *Bettelheim*, ebd., S. 62.

587 Ebd., S. 62 f.

588 Ebd., S. 63.

det sich im Anschluss gegen totale Transparenz und fordert die Schwerpunktsetzung bei der „Allokation von Kontrollressourcen". Die Aufmerksamkeit dürfe nicht" der Perfektionierung der Verfolgung von Bagatelldelikten" gelten; stattdessen müsse sich das Kontrollpotenzial dem hochgradig sozialschädlichen Verhalten zuwenden. Der Ausdehnung von Verhaltenstransparenz müsse deshalb eine „Analyse sämtlicher sozialer Implikationen vorangehen". Die Einschüchterungswirkung sei ein „sozialer Kostenfaktor", der „bei der Implementierung von Informationssystemen in Rechnung zu stellen" sei.[589]

### *d) Machtverschiebung*

Im nächsten Abschnitt wendet sich *Mallmann* „Planungsinformationssystemen" zu, womit er heutiges Datenmanagement und rechnerbasierte Modelle antizipiert.[590] Zwar sieht er hier bei einer Anonymisierung und bei geeignetem Schutz gegen Missbrauch der Daten nicht die oben beschriebenen Risiken der Dossiers, wendet sich jedoch stattdessen „Machtverschiebungen im politischen System" zu. Er hält die „vertikale Gewaltenbalance zwischen Bund, Ländern und Gemeinden" für ebenso gefährdet wie „die Chancen politischer Einflußnahme durch Parteien und Bürgerinitiativen". „Informationsmonopole und -oligopole" ermöglichten Machtkonzentrationen in erheblichem Umfang. So entstünden für Außenstehende nicht nachvollziehbare Entscheidungsabläufe; der „Anspruch wissenschaftlich abgesicherter Objektivität" lasse eine Problematisierung der mit den Instrumenten verfolgten Interessen kaum zu. Es entstehe eine verfassungswidrige Machtkonzentration, die den demokratischen Meinungs- und Willensbildungsprozess „nicht weniger bedrohe als eine intensive Datenüberwachung des Einzelnen und sozialer Gruppen."[591] Das Risiko weitet er auf den Privatsektor aus und beschreibt frühe Formen des Handels mit personenbezogenen Daten.[592]

### *e) Präjudizierung von Entscheidungen*

Im letzten Abschnitt seines „Allgemeinen Teils" widmet sich *Mallmann* der Informationsrichtigkeit und geht dabei auf das Problem fehlerhafter Information als Präjudizierung menschlicher Entscheidungen ein, sofern bestimmte Informationen über Kennzahlen und Punktsysteme komprimiert werden.[593] Daneben beschreibt er das Risiko der Verantwortungsnegation: Der Entscheider werde mittels des formalisierten, objektiven Entscheidungsprozesses „vom Legitimationsdruck" entlas-

---

589 Ebd., S. 63 f.

590 Näher zum Phänomen „Big Data" vgl. BITKOM (Hrsg.), Big Data.

591 *Mallmann*, Zielfunktionen, S. 65 f.

592 Ebd., S. 67.

593 Ebd., S. 71 f.

tet.[594] Es drohe die Verstärkung „partizipationsfeindlicher Entscheidungsprozesse“ und eine Potenzierung von Fehlern bei einer multifunktionaleren Verwendung der nur einmal erhobenen Daten.[595]

Abschließend nimmt er eine weitere Differenzierung der Informationsrichtigkeit in „Objektive Richtigkeit“, „Vollständigkeit“ und „Wahrung der Kontextgebundenheit“ vor. Im Rahmen der letzteren Kategorie beschreibt er das Risiko der Kontextinfiltration im Fall von Bewertungen; dort sei aufgrund der in unterschiedlichen Bereichen verschieden gesetzten Standards eine Abstrahierung nicht ohne Weiteres möglich. Als Beispiel nennt er psychologische Tests und Abiturnoten. Er verbindet die Entkontextualisierung mit einer Diskriminierung der Prüflinge. Die „Grenzen multifunktionaler Verwendung“ müssten dort verlaufen, „wo Mißverständnisse zulasten der Betroffenen drohen“.[596]

### 3. Zwischenergebnis

Die Arbeit von *Mallmann* weist trotz ihres Alters eine bemerkenswerte Aktualität auch im Hinblick auf Risikokonzeptionen und Schutzgüter auf. Während das Risiko der Rollenfixierung auf die eher konstruiert wirkende „Rollentheorie“ aufbaut, weist die Identifizierung der Schutzgutpaare „Intimität und Distanz“ sowie „Identität und Selbsteinschätzung“ auf die in der obigen Normen- und Rechtsprechungsanalyse herausgearbeiteten Risiken hin. Der besondere Wert seiner Untersuchung liegt jedoch in der Erfassung des Risikos von Verhaltensauswirkungen. Hier bleibt er im Gegensatz zu vielen neueren Arbeiten nicht auf der Stufe bloßer Unterstellungen stehen, sondern versucht diese durch Einbeziehung der Studie zu Verhaltensauswirkungen in der Zeit des McCarthyismus und mit Bezug auf lerntheoretische Ansätze zu belegen, was jedoch im Ergebnis aufgrund der sehr speziellen zeitgeschichtlichen Bedingungen für heutige Datenverarbeitungen nur begrenzt aussagekräftig ist, zumal es sich bei den damaligen Überwachungsmaßnahmen und Sanktionen um ein extremes und gerade auf politische Wirkung zielendes System handelte. Fraglich ist, ob auch an sich legitime, nicht auf politisches Verhalten bezogene (bzw. nur potenziell darauf beziehbare) Überwachungsmaßnahmen, etwa zu Strafverfolgungszwecken, die von ihm beschriebenen negativen Verhaltensauswirkungen auf politisches Engagement haben.

Die übrigen von *Mallmann* dargestellten Risiken der Machtverschiebung und Verantwortungsnegation weisen ebenfalls eher auf eine übergeordnete Perspektive hin und wurden bereits in der normativen Analyse, z.B. in dem erläuternden Bericht zur Datenschutzkonvention des Europarats, identifiziert.[597] Festzuhalten bleibt

---

[594] Vgl. ebd., S. 73.

[595] Ebd., S. 74.

[596] Ebd., S. 78 f.

[597] Siehe oben Teil 1, II.A.2.c).

jedoch die auch von *Mallmann* bejahte Notwendigkeit der Markierungs- und Indizierungsfunktion einer Identifikation maßgeblicher Risiken sowie deren Ergänzung um eine (bis heute) nicht geleistete umfassende Wirkungsanalyse.[598]

## F. Weitere Konzeptionen

### 1. Überblick

Von den mittlerweile nahezu unüberschaubaren kleinteiligeren und älteren Literaturkonzeptionen[599] soll im Folgenden nur eine exemplarische Auswahl einbezogen werden, wobei solche Arbeiten ausgewählt wurden, die sich von den bereits unter A. bis F. besprochenen Ansätzen deutlich unterscheiden. Die Konzeption von *Schmidt* entstammt dabei, wie die bereits besprochene Arbeit von *Mallmann*, der älteren Phase, setzt jedoch eigene Akzente. Die Arbeiten von *Ladeur* und *Kilian* stehen für eine neuere, den überkommenen Datenschutzkonzeptionen wegen deren Verrechtlichungsproblematik kritisch gegenüberstehende Strömung.

### 2. Risikokonzeptionen und Schutzgüter

#### *a) Entscheidungsfreiheit (Schmidt)*

Eine der frühesten Risikokonzeptionen findet sich in einem wirkkräftigen Aufsatz von *Walter Schmidt* aus dem Jahr 1974,[600] der an dieser Stelle exemplarisch für eine Reihe älterer, sich in Risikokonzeptionen und Schutzgütern ähnelnden „Pionierarbeiten" behandelt wird.[601] *Schmidt* befasst sich mit den Risiken der damals beginnenden elektronischen Datenverarbeitung bei staatlichen und privaten Stellen. Diese führe dazu, dass sich die Betroffenen beobachtet fühlten und sich entsprechend darauf einstellten: „Wer durchschaut worden ist, dessen Verhalten kann im voraus abgeschätzt, dessen Entscheidungen können vorweggenommen werden".[602] Gefahren bestünden in der Zusammenfügung von „Mosaiksteine[n]" zu einem „Lebensbild" oder „Persönlichkeitsprofil". „Unzulänglichkeiten der inneradministrativen Kommunikation" hätten bis dahin eine „ungeschriebene Gewal-

---

598 *Mallmann*, Zielfunktionen, S. 68.

599 Vgl. die Nachweise hierzu bei *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, S. 122, Fn. 70–77, 86 f.

600 *Schmidt*, JZ 1974, 241 ff.

601 *Benda*, in: Leibholz/Faööer/Mikat/Reis (Hrsg.), FS Geiger; *Podlech*, in: Brückner/Dalichau (Hrsg.), Festgabe Grüner; *Simitis*, NJW 1971, 673 ff.; *ders.*, in: Horn/Luig/Söllner (Hrsg.), FS Coing; *ders.*, NJW 1984, 394 ff.; *Steinmüller* u.a., Gutachten; *Steinmüller* (Hrsg.), Verdatet und vernetzt; *ders.*, NfD 1993, 215 ff.

602 *Schmidt*, JZ 1974, 241.

tenteilung innerhalb der Verwaltung“ begründet, deren Schutzwirkung durch die neuen Entwicklungen „zunichte“ würde.[603]

*Schmidt* differenziert sodann im Rahmen des Persönlichkeitsschutzes zwischen der allgemeinen Sicherung des „persönlichen Lebens- und Geheimbereichs“ sowie dem „Schutz vor Mißbrauch personenbezogener Daten“ und kritisiert in diesem Zusammenhang die „Sphären-Konstruktion“ des Persönlichkeitsschutzes in der damaligen Rechtsprechung. Dieser sei es nicht gelungen, „sichere Maßstäbe“ zu liefern, die „Inhalt und Umfang des Persönlichkeitsschutzes vorhersehbar machen“.[604] In Anlehnung an *Westin*[605] fordert er die Ergänzung des Persönlichkeitsschutzes vor „indiskrete[m] Eindringen“ durch ein Verfügungsrecht des Einzelnen über die ihn betreffenden personenbezogenen Informationen, um „selbst zu bestimmen, was davon anderen mitgeteilt werden soll und auf welche Weise“. Dadurch werde die Selbstdarstellung nach außen geschützt.[606] Er ergänzt seine Konzeption um das Schutzgut der Entscheidungsfreiheit. Die Datenverarbeitung ermögliche die „technische Reproduzierbarkeit des ‚inneren’ Persönlichkeitsprofils“ und die „Simulation des Konsumenten- und Wählerverhaltens“. Diese „Datenintegration“ schmälere die persönliche Entfaltungsmöglichkeit jedes Einzelnen und steigere dessen Abhängigkeit. Der Einzelne passe sich den Erwartungen an. Informationen würden zum Instrument privater und staatlicher Machtbildung. Die Entscheidungsfreiheit setze die Möglichkeit des „Auch-anders-Könnens“ voraus, was wiederum von der „Formulierung möglicher Entscheidungsalternativen“ abhänge. Hierfür sei neben der Informationsfreiheit auch eine unbehinderte Kommunikation erforderlich. Diese sei „verzerrt“, wenn ein Partner „schon alles über die Persönlichkeit des andern“ wisse und dieses „Wissen als Machtfaktor“ einsetze. Es bestehe dann ein durch rechtliche Schutzvorkehrungen vermeidbares „Informationsungleichgewicht“.[607] Von diesen Erwägungen schließt *Schmidt* auf die Unzulässigkeit bestimmter Arten von Datenverarbeitung und verweist dabei auch auf Gefahren für die „politische Entscheidungsfreiheit“ und das Risiko der „politische[n] Einschüchterung“ bei Sammlung und Speicherung von Daten aus dem Bereich der Öffentlichkeitssphäre.[608] Gefahren bestünden für „den einzelnen wie für das gesamte politische System“.[609]

---

603 Ebd., 242.

604 Ebd., 243 f.

605 *Westin*, Privacy and Freedom, 1967.

606 *Schmidt*, JZ 1974, 241 (244).

607 Ebd., 245 f.

608 Ebd., 247 f.

609 Ebd., 249.

### *b) Eigentumsanaloge Konzeptionen (Ladeur, Kilian)*

Eine dezidierte Gegenposition zu der herrschenden und auch den obigen Untersuchungen zugrunde liegenden Ablehnung einer eigentumsanalogen Interpretation des Rechts auf informationelle Selbstbestimmung findet sich in zwei Aufsätzen von *Ladeur*[610] und *Kilian*.[611] *Ladeur* kritisiert in erster Linie die Risikokonzeptionen des BVerfG: Die Erstellung von Persönlichkeitsbildern sei eine „Mystifikation", an der unter den Bedingungen westlicher Verfassungsstaaten niemand ernsthaft interessiert sei; der vom BVerfG formulierte psychische Druck durch öffentliche Anteilnahme und die Beeinträchtigung von „Entfaltungschancen" seien nur für „Daten über (i.w.S.) abweichendes Verhalten" „ohne weiteres einleuchtend". Das Gericht lasse „jede Konturierung der zulässigen Datensammlung vermissen"; die Darstellung der Schranken des Grundrechts sei inkonsequent und führe dazu, dass der Staat als „Miteigentümer über die Nutzung der Daten" entscheide.[612] Die Konzeption des BVerfG sei „jenseits eines durch wenige Beispiele plausibilisierten Bereichs der evidenten Gefährdung faktischer Grundrechtsausübung [...] substanzlos" und „im Bereich der Grundrechtstheologie" anzusiedeln.[613] Die mangelhafte Beschreibung der Gefährdungen der informationellen Selbstbestimmung und die „Anrufung des Gesetzesvorbehalts" hätten eine „bloße Problemverlagerung" bewirkt. *Ladeur* verweist stattdessen u.a. auf eine stärkere Selbstregulierung und Vorsorge gegen Ungleichgewichte durch „prozeduralen Datenschutz", um neuen Wissensformen gerecht zu werden. Unter „prozeduralem Datenschutz" versteht er unter anderem eine Auslegung des Rechts auf informationelle Selbstbestimmung, „als eine ‚vor die Klammer gezogene' Verfahrenskomponente, in der Form eines prozeduralen Rechts auf Information über gespeicherte Daten".[614]

Im Anschluss wendet er sich erneut gegen Befürchtungen, welche „die realen Risiken der Informationstechnologie übertreiben und auf die Möglichkeit ‚vollständiger Persönlichkeitsprofile' hinweisen". Der Nutzung von personenbezogenen Daten für Werbezwecke steht er insgesamt positiv gegenüber, wobei er Risiken für Flexibilität und Beweglichkeit von Wissensnetzwerken aufgreift und als Beispiel das „Einrasten" von „bestimmten Moden" bei überproportionaler Verstärkung durch Marketingstrategien und die Festlegung von Individuen auf negative Persönlichkeitsmerkmale nennt und sich grundsätzlich für eine „Zuordnung" zum Eigentum ausspricht.[615]

---

610 *Ladeur*, DuD 2000, 1.ff.
611 *Kilian*, CR 2002, 921 ff.
612 *Ladeur*, DuD 2000, 1 (13).
613 Ebd., 15.
614 Ebd., 16 f.
615 Ebd., 18 f.

Stärker noch als bei *Ladeur* ist die Anbindung an Marktprozesse auch in der Risikokonzeption *Kilians* ausgeprägt. In seinem Aufsatz kritisiert er das Gutachten von *Roßnagel/Pfitzmann/Garstka* zur Modernisierung des Datenschutzrechts hinsichtlich der dortigen bloß „technischen Effektivierung der Durchsetzung feststehender Verfügungsrechte"; notwendig sei stattdessen die „Konzeptualisierung und Begründung der Verfügungsrechte" selbst.[616]

Im Anschluss daran entwickelt *Kilian* aus dezidiert zivilrechtlichem Verständnis die These, dass „die überwiegende Zahl staatlicher Regulierungen im nichtöffentlichen Bereich [des Datenschutzrechts] überflüssig sind, wenn man das informationelle Selbstbestimmungsrecht [...] als eigentumsähnliche Position (property right) auffasst".[617] Obwohl *Kilian* im Wesentlichen die (phänomenologisch-implizite) Beschreibung von Risiken im Modernisierungsgutachten mitträgt,[618] entwickelt er aus seiner spezifisch marktorientierten Perspektive eine andere Risikokonzeption. Der Kommerzialisierung personenbezogener Daten müsse Grenzen gezogen werden, wenn es sich um „zweckunabhängige, allumfassende oder ausschließliche Nutzungsvereinbarungen" Einzelner handele, da sie sich dort der „informationellen Dispositionsmöglichkeiten eines Dritten ausliefern". Dies verstoße gegen die Menschenwürde oder die guten Sitten, für die er auf § 138 BGB verweist. „Exzessive, gefährdende oder menschenverachtende Informationsnutzungen" sollen seiner Ansicht nach durch das „Marktordnungs- und Strafrecht" bekämpft werden.[619] Er spricht sich gegen die These des Gutachtens hinsichtlich der Beeinträchtigung der Funktionsbedingung des demokratischen Gemeinwesens durch marktorientierte Interpretation des Allgemeinen Persönlichkeitsrechts aus.[620] Abschließend lässt er jedoch Raum für die Regulierung risikobehafteter Bereiche: „[A]ngemessene rechtliche Rahmenbedingungen" könnten „Marktprozesse für Risikobereiche begrenzen".[621]

### 3. Zwischenergebnis

Die drei beschriebenen Konzeptionen weisen jeweils eine eigene, von den obigen Arbeiten abweichende Perspektive auf Risiken und Schutzgüter auf. *Schmidt* weist neben den individualbezogenen Risiken für die Entscheidungsfreiheit bereits auf die gesamtgesellschaftlichen Risiken hin. Seine individuelle Risikokonzeption zur Entscheidungsfreiheit bleibt dabei jedoch intuitiv. Insgesamt ist sein Aufsatz

---

616 *Kilian*, CR 2002, 922.
617 Ebd., 922 f.
618 Ebd., 921.
619 Ebd., 928.
620 Ebd.
621 Ebd., 929.

exemplarisch für einen Teil der älteren Literatur, der insbesondere die Risikokonzeptionen des Volkszählungsurteils beeinflusste.

Die beiden Aufsätze von *Ladeur* und *Kilian* stehen hingegen für eine neuere, den Konzeptionen des Volkszählungsurteils ablehnend gegenüberstehende Strömung. Risiken und Schutzgüter werden in diesen Arbeiten zwar in geringerem Umfang aufgegriffen, insbesondere der Ansatz von *Kilian* zeigt jedoch, dass auch in einer eigentumsanalogen Konzeption insbesondere über Marktordnungsrecht und Strafrecht eine abgegrenzte Regulierung in risikobehafteten Bereichen möglich ist. Dies spricht gegen die Notwendigkeit des datenschutzrechtlichen Verbots mit Erlaubnisvorbehalt. Nicht geklärt wird jedoch, wie die risikobehafteten Bereiche von den übrigen abzugrenzen sind.

## G. Zwischenergebnis

Die Literaturkonzeptionen unterscheiden sich teilweise deutlich voneinander und setzen jeweils eigene Akzente auf einschlägige Risiken und Schutzgüter. Alle Konzeptionen greifen jedoch das Risiko informationsbedingter Verhaltensauswirkungen auf. Abgesehen von *Mallmann* bleiben die untersuchten Konzeptionen dabei jedoch auf einer eher intuitiv-impliziten Beschreibung des Risikos stehen. Besonders deutlich wird dies bei dem Reformgutachten von *Roßnagel/Pfitzmann/Garstka* und dem Gutachten für die FES von *Roßnagel*. Hier wird bereits der phänomenologischen Beschreibung bestimmter Technikpotenziale Risikocharakter zugesprochen. Verbunden mit einer Schutzgutkonzeption, die sich auf ein objektives, strukturell-kommunikatives Verständnis der informationellen Selbstbestimmung stützt, lässt sich damit eine weitgehende Regulierung begründen.[622] In den impliziten Risikokonzeptionen wird zum Teil ausdrücklich auch der Aspekt „informationeller Machtverschiebungen“[623] aufgegriffen, wobei dort die bei *Ehmann* vorgetragene Kritik an der Übertragung marxistischer Argumentationsmuster in Erinnerung kommt. Das Risiko wird dabei nicht nur auf individueller Ebene gesehen, sondern insbesondere bei *Schmidt* auch auf die gesamtgesellschaftliche Ebene des politischen Systems übertragen.[624]

Die Privatsphärenkonzeption von *Mallmann* greift das Risiko von Verhaltensauswirkungen ebenfalls auf, begründet dies jedoch mit einer Studie zu Überwachungsmaßnahmen zur Zeit des McCarthyismus. Das Problem an diesem grundsätzlich richtigen Ansatz liegt jedoch in der fraglichen Aussagekraft dieser Studie für die heute relevanten Fälle, bei denen es anders als zu Zeiten des McCarthyis-

---

622 Siehe oben III.C.3. und D.3.

623 Siehe oben III.D.2.a), auch E.2.d).

624 Siehe oben III.F.2.a).

mus – abgesehen von bestimmten Maßnahmen zur Terrorismusabwehr – gerade nicht um die Überwachung politischer Einstellungen geht.[625]

Im Übrigen legen die Literaturkonzeptionen Schwerpunkte auf bestimmte einzelne Risiken, wie z.B. Unterstellungen im Fall fehlender Informationen,[626] Datenmissbräuche,[627] Bruch von Vertraulichkeitserwartungen,[628] Entscheidungspräjudizierung[629] sowie die Erstellung von Persönlichkeitsprofilen.[630] Besonders kontrovers ist dabei die Beurteilung von Datenverarbeitungen zu kommerziellen (insb. Werbe-)Zwecken. Während *Roßnagel* hierin – mit fragwürdiger Begründung – ein Risiko sieht,[631] werden diese in der Konzeption von *Britz* überwiegend als bloß lästiges Verhalten ohne Risikocharakter eingestuft.[632] Die Konzeptionen von *Ladeur* und *Kilian* setzen sich von den vorgenannten durch eine eigentumsanaloge Schutzgutkonzeption ab, entwickeln jedoch keine aussagekräftigen Risikotypologien.[633]

Neben dem Risiko von Verhaltensanpassungen legen insbesondere *Mallmann, Britz* und *Schmidt* einen Schwerpunkt auf Persönlichkeitsauswirkungen im weiteren Sinne. *Mallmann* greift diesen Aspekt unter den Schutzgüterpaaren „Intimität und Distanz“ sowie „Identität und Selbsteinschätzung“ auf und sieht insbesondere das Risiko einer Rollenfixierung.[634] *Britz* entwickelt aus einem außerrechtlichen Autonomiekonzept das Risiko der Beeinträchtigung innerer Entfaltungsfreiheit durch Fremdbildzuschreibungen.[635]

## IV. Ergebnis

Die bereits in den ersten Teilen der Arbeit identifizierten Risiken von Entkontextualisierung, Publizitätsschäden, Informationspermanenz und Persönlichkeitsprofilen werden sowohl von der Rechtsprechung des BVerfG als auch von den Literaturkonzeptionen aufgegriffen. Das Risiko der Entkontextualisierung lässt sich mit der Rechtsprechung als Befürchtung der Informationsfehlerhaftigkeit mangels

---

625 Siehe oben III.E.3.
626 Siehe oben III.A.2.a).
627 Siehe oben III.D.2.b).
628 Siehe oben III.B.2.d).
629 Siehe oben III.C.2.c).
630 Siehe oben III.E.2.d), e).
631 Siehe oben III.D.2.b).
632 Siehe oben III.B.2.e) sowie C.2.b); D.2.a).
633 Siehe oben III.F.b).
634 Siehe oben III.B.2.a), b).
635 Siehe oben III.B.2.b).

Kontextmitberücksichtigung sowie in Zusammenhang mit der Änderung der „Form der Öffentlichkeit“ verstehen. Letzteres steht dem Schutzgut der Selbstdarstellung und dem Risiko von Publizitätsschäden nahe.

Das zentrale Risiko, das von Literatur und Rechtsprechung immer wieder aufgegriffen wird, ist die informationsbedingte Verhaltensänderung, wobei zwischen einer individuellen und einer gesellschaftlichen Ebene unterschieden werden kann. Hinsichtlich letzterer verweist sowohl die Rechtsprechung als auch die Literatur auf die Möglichkeit konformitätsbegünstigender Einschüchterungen durch die Informationsverfügbarkeit bei Dritten. Diese Annahme wird jedoch in der Literatur ebenso wie in der Rechtsprechung nicht genauer belegt. Verschiedenen Literaturansätzen liegt insoweit eine eher implizit-intuitive Risikokonzeption zugrunde. Eine Ausnahme bildet nur die Arbeit von *Mallmann*, in der zumindest den Versuch unternommen wird, die These mit empirischen Belegen zu untermauern. Der insoweit bestehende Klärungsbedarf wird auch von Sondervoten zu verschiedenen Entscheidungen bestätigt. Das später von der Rechtsprechung unter dem Topos „Einschüchterungseffekt“ behandelte Risiko von Verhaltensanpassungen zielt am ehesten auf den Schutz eines Sicherheitsgefühls bzw. Vertrauens der Allgemeinheit ab. In der früheren Rechtsprechung finden sich Entscheidungen, in denen das Risiko von Verhaltensänderungen auf einer individuellen Ebene aufgegriffen und dem Schutzgut bestimmter beruflicher Vertraulichkeitserwartungen zugeordnet wird. In späteren Entscheidungen operiert die Rechtsprechung explizit mit „Befürchtungen“ der Betroffenen, die im Fall verschiedener individueller Überwachungsnachteile sogar bereits dann erheblich sein sollen, wenn sie „nicht ohne jeden Grund“ bestehen. Das Schutzgut der Vertraulichkeitserwartung wird in der Rechtsprechung ebenfalls normativ konkretisiert, im Unterschied zum EU-Recht jedoch über die Einzelgrundrechte, was aus grundrechtsfunktionaler Sicht vorteilhaft ist.

Inwieweit kommerzielle Datenverarbeitungen zu Werbezwecken ein Risiko darstellen, wird in der Literatur kontrovers betrachtet, wobei eine eigentliche Begründung bei den Ansichten, die das Risikopotenzial betonen, fehlt. In der Rechtsprechung wird zumindest auf Risiken für die Datensicherheit durch Kostendruck verwiesen.

Im Übrigen wird sowohl von der Rechtsprechung als auch in der Literatur das Risiko von Persönlichkeitsprofilen aufgegriffen, wobei sich dies in der Rechtsprechung mit der Gefahr einer „verwaltungstechnischen Entpersönlichung“ und damit dem Schutzgut der Menschenwürde in Verbindung bringen lässt. Insbesondere können durch Profilbildungen die Risiken von Informationspermanenz und -emergenz durch Konvergenzeffekte kombinieren. In diesem Sinne lässt sich auch das im Urteil zum IT-Grundrecht genannte Risiko eines Gesamtzugriffs auf informationstechnische Systeme verstehen, wobei die Untersuchung gezeigt hat, dass die Fokussierung auf das Risiko technischer Infiltration unzureichend ist und das der Täuschungsinfiltration ebenfalls aufgegriffen werden sollte.

*Teil 4*

# Typisierende Systematisierung der Risiken

## I. Methodische Vorüberlegung

In der nun folgenden Systematisierung werden die Risiken, die in der normativen Analyse identifiziert wurden, in eine logische Ordnung gebracht und diskutiert. Wie bereits oben dargestellt, kommt dabei keine abschließende, sondern nur eine typisierende Systematisierung in Betracht.[1] Hierzu werden zunächst die in den rechtlichen Regelungen aufgegriffenen Risiken in bestimmte Kategorien gefasst und in eine Reihenfolge gebracht. Unter den Einträgen der einzelnen Risiken erfolgt dann die Diskussion. Dort werden nach Möglichkeit auch empirische Studien, demografische Daten und außerrechtliche Quellen berücksichtigt. Forschungsergebnisse aus anderen Fachbereichen und anderen Sprachen können jedoch nur punktuell und ohne Anspruch auf Vollständigkeit einbezogen werden. Die Systematisierung ist deshalb insgesamt als Vorschlag und möglicher Ausgangspunkt künftiger Reformen zu verstehen. Gleichwohl erleichtert die mittlerweile beachtliche Zahl an einschlägigen Untersuchungen die interdisziplinäre Diskussion. Zu nennen ist hier beispielsweise die empirische Studie zu Risiken des *life-logging* der *European Network and Information Security Agency* (ENISA).[2] Die Agentur befasste sich in dieser interdisziplinären Untersuchung aus dem Jahre 2011 mit der Frage, inwieweit neue Techniken, die unter dem Stichwort *life-logging* zusammengefasst werden, psychologische, ökonomische, soziale und rechtliche Risiken hervorrufen. Ein weiteres von ENISA herausgegebenes Werk behandelte die ökonomischen Aspekte des Datenschutzes aus der Perspektive des Individuums.[3] Anzuführen ist weiterhin die Befragung zum Datenschutzempfinden im Eurobarometer Nr. 359 von 2011[4] sowie die jährliche JIM-Studie des Medienpädagogischen Forschungsverbunds Südwest, die sich u.a. mit Gefahren im Internet und mit Datenschutz befasst.[5]

---

[1] Siehe oben Einleitung, IV.

[2] ENISA (Hrsg.), Life-logging-Studie.

[3] ENISA (Hrsg.), Monetising Privacy.

[4] Europäische Kommission (Hrsg.), Eurobarometer 359.

[5] Medienpädagogischer Forschungsverbund Südwest (Hrsg.), JIM 2011.

## II. Systematisierungsvorschlag

Die obige Analyse hat ergeben, dass auf den unterschiedlichen Ebenen des Datenschutzrechts vergleichbare Risikokonzeptionen bestehen und dass sich die darin untersuchten Risiken häufig überschneiden. Sie lassen sich somit zunächst nach dem Ort eines möglichen Schadens einteilen.[6] Demnach bestehen einerseits Risiken auf einer übergeordneten strukturellen Ebene (Makroebene). Hierzu gehören zum Beispiel informationsbedingte Auswirkungen auf die Ausübung politischer Grundrechte und angenommene Verschiebungen informationeller „Machtverhältnisse" bzw. „Informationsgleichgewichte". Diese Risiken können unter der Kategorie gesellschaftlich-politische Risiken gefasst werden. Der Makroebene ist allerdings auch eine Kategorie wirtschaftlicher Risiken zuzuordnen, die insbesondere durch die internationalen Spezialinstrumente und das europäische Sekundärrecht aufgegriffen werden. Neben dieser Makroebene betrifft die überwiegende Anzahl der Risikokonzeptionen jedoch die Ebene des Individuums (Mikroebene), wie etwa die Risiken von Publizitätsschäden oder der Erhöhung individueller Verletzlichkeit zeigen.

Obwohl die Risiken aufgrund der Eigenarten von Informationen immer in einem Wechselwirkungsverhältnis stehen, lässt sich doch aus der obigen Analyse eine weitere Kategorie von Risiken bilden, bei denen diese Wechselwirkung besonders groß ist, und die deshalb sowohl die Makro- als auch die Mikroebene betreffen. Hierzu zählt etwa das Risiko enttäuschter Vertraulichkeitserwartungen, das gleichermaßen bei möglichen individuellen Schäden (etwa Nichtinanspruchnahme von gesundheitlichen Dienstleistungen) und auf einer übergeordneten Ebene (Nachfragerückgänge in Folge von Vertrauensverlust bei Verbrauchern) auftritt. Im Anschluss lässt sich eine Kategorie von Verarbeitungen nennen, bei denen manche Autoren davon ausgehen, dass es sich nicht um Risiken handelt, während andere dies bestreiten. Zu dieser Kategorie der „Grenzfälle" und Nicht-Risiken zählen vor allem kommerzielle Datenverarbeitungen. Im Folgenden werden die Risiken diesen Kategorien zugeordnet und diskutiert.

---

[6] Eine vergleichbare Aufteilung hinsichtlich der „settings" von „privacy rights" findet sich bei *Westin*, 59 Journal of Social Issues 2 (2003), 431 f. (political, socio-cultural, personal), eine andere Aufteilung nach Subjekten ebd., 434; für eine andere Aufteilung der Risiken (individuals/commercial and economic interests/state/government and society) vgl. ENISA (Hrsg.), Life-logging-Studie.

# A. Makroebene: Strukturelle Risiken

## 1. Gesellschaftlich-politische Risiken

### *a) Informationsmacht*

Das erste Risiko der gesellschaftlich-politischen Ebene ist die von mehreren Konzeptionen aufgegriffene Verlagerung von „Informationsmacht". Während teilweise bloß auf eine damit einhergehende soziale Verantwortung und mögliche Nachteile für die Betroffenen[7] oder auch auf möglichen Machtmissbrauch[8] verwiesen wird, gehen andere Literaturkonzeptionen umfassender darauf ein: Staatliche Informationssysteme könnten Machtverschiebungen im politischen System bewirken und die vertikale Gewaltenteilung gefährden. „Informationsmonopole und -oligopole" führten zu einer Machtkonzentration und gefährdeten den demokratischen Meinungs- und Willensbildungsprozess.[9] Informationen seien Instrumente staatlicher und privater Machtbildung; sie könnten als Machtfaktor eingesetzt werden und Informationsungleichgewichte hervorrufen.[10] Das Volkszählungsurteil befasst sich mit diesem Risiko in eher geringem Umfang, wenn es die Trennung von Statistiken und anderen Gemeindeaufgaben als unerlässliche „informationelle Gewaltenteilung" beschreibt.[11] Besondere Aktualität erhielt dieser Gewaltenteilungsaspekt hingegen in der Entscheidung zum Antiterrordateigesetz. Darin etabliert das BVerfG explizit ein informationelles Trennungsprinzip, um zu verhindern, dass die rechtsstaatliche Aufteilung von weitreichenden, verdeckten Aufklärungsbefugnissen der Nachrichtendienste und operativen Vollzugsbefugnissen der Polizeibehörden auf der Informationsebene zunichte gemacht wird.[12] Auch dies ist ein Aspekt informationeller Machtausübung, der bei Berücksichtigung der durch *Snowden* enthüllten und in ihrer Tragweite noch nicht absehbaren Überwachungstätigkeit amerikanischer Sicherheitsbehörden[13] besondere Brisanz gewinnt.

Für ein besseres Verständnis dieser Risikokonzeptionen, muss zunächst der Begriff „Macht" definiert werden. Nach *Max Weber* bedeutet Macht „jede Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht".[14] Bei „Informationsmacht"

---

[7] Siehe oben Teil 1, II.A.2.c).

[8] Siehe oben Teil 1, IV.B.5.

[9] Siehe oben Teil 3, III.E.2.d); zu Machtverschiebungen siehe auch Teil 3, III.D.2.a).

[10] Siehe oben Teil 3, III.F.2.a).

[11] BVerfGE 65, 1 (69); zum Topos „informationelle Gewaltenteilung" vgl. auch *Trute*, JZ 1998, 826, Fn. 44 m.w.N.; *Tinnefeld*, MMR 2006, 23 ff. und *Gärditz*, Prävention, S. 203.

[12] Siehe oben Teil 3, II.B.17.

[13] Siehe oben Einleitung, I.

[14] *Weber*, Wirtschaft und Gesellschaft, S. 28.

beruht die Durchsetzungschance entsprechend auf Informationen,[15] die dann eine „Machtquelle" darstellen.[16] Ein Beispiel wäre die Nötigung gemäß § 240 Abs. 1 Hs. 1 Var. 2 StGB: Dort kann das Tatbestandsmerkmal „Drohung mit einem empfindlichen Übel" auch durch die Veröffentlichung von Informationen – etwa über ein außereheliches Verhältnis – verwirklicht werden.[17] Dieses Verständnis beschreibt allerdings lediglich Auswirkungen auf der individuellen Ebene. Es ist jedoch zweifelhaft, ob die Informationsmacht ein typisches Risiko des Umgangs mit personenbezogenen Daten darstellt. Wie *Albers* ausführt, geht der Wissenserwerb über andere notwendig mit sozialen Beziehungen einher und begründet kein pauschales Schutzbedürfnis.[18]

Der Vergleich mit der Nötigung zeigt, dass für die Risikohaftigkeit des Informationsumgangs ein Wertungselement hinzukommen muss – vgl. § 240 Abs. 2 StGB. Eben dies ermöglicht es jedoch, die individuelle Komponente der Informationsmacht auf der Mikroebene anderen spezielleren Risiken zuzuordnen. Das auf der Makroebene angesprochene Risiko „schädlicher Informationsungleichgewichte durch Machtausübung" besteht hingegen insbesondere in fehlendem Informationszugang.[19] Informationsmacht auf gesellschaftlich-politischer Ebene lässt sich darüber hinaus mit Techniken zur Massenbeeinflussung in Verbindung bringen, wie sie unter dem Oberbegriff der Propaganda beschreibbar sind. Propaganda in diesem Sinne ist die zur Beeinflussung, Manipulation und Herrschaftssicherung eingesetzte Werbetechnik.[20] Weiterhin kann Informationsmacht die Auswirkungen politischer Verfolgung und Überwachung ermöglichen und verstärken.

Problematisch an diesem in vielen Konzeptionen mitschwingenden Aspekt ist, dass zwischen dem Informationsumgang als solchem (Einsatz von Massenkommunikationsmitteln sowie Verwendung von Informationen über die Bevölkerung) und dem (illegitimen) Verwendungszweck in autoritären Staaten und Diktaturen[21] ein weiter Weg liegt. Zutreffend weist deshalb *Bull* darauf hin, dass informatorische Effizienzsteigerungen der Verwaltung zwar das Risiko von Missbräuchen durch

---

15 Zum Begriff „Information" bereits oben Einleitung, I.

16 Zur Verwendung der Begriffe „Informationsmacht" und „Machtquelle" in der Psychologie vgl. http://www.psychologie.uni-heidelberg.de/ae/allg/lehre/wct/m/M03/M0303mac.htm [Stand: 28.3.2014]; zur Vorstellung von Information als Macht vgl. auch *Schwan*, zit. nach *Rogall*, Informationseingriff, S. 30; *Heussner*, in: Gitter/Thieme/Zacher (Hrsg.), FS Wannagat, S. 199 f.; *Hatje*, Informationsaustausch, 2008; http://www.datenschutz.hessen.de/europa.htm [Stand: 28.3.2014], S. 5 sowie zum Machtmissbrauch auch *Hoffmann-Riem*, AöR 123 (1998), 514 ( 534).

17 Vgl. Schönke/Schröder-*Eser/Eisele*, § 240 Rn. 10.

18 Vgl. *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen II, S. 122.

19 *Tinnefeld*, MMR 2006, 23 (26).

20 http://de.wikipedia.org/wiki/Propaganda [Stand: 28.3.2014].

21 Zur Rolle der Datensammlungen in den NS- und Stasi-Regimen vgl. *Masing*, NJW 2012, 2305.

einen autoritären Staat steigern, in einer rechtsstaatlich gesicherten Ordnung wie der gegenwärtigen Bundesrepublik die Wahrscheinlichkeit einer Machtusurpation durch Kriminelle oder die eines Staatsstreichs dagegen sehr gering ist.[22] Zwar ist nicht ausgeschlossen, dass sich auch Rechtsstaaten „schleichend" ihrer Grundsätze begeben – doch bestehen hiergegen bereits mit Art. 1 Abs. 1, 3, Art. 79 Abs. 3 und Art. 20 GG starke Sicherungen. Damit dürfte sich auch erklären, dass das Risiko der Informationsmachtverschiebung eher geringen Niederschlag in den untersuchten Normen und Gerichtsentscheidungen gefunden hat, dafür jedoch umso stärker in der Literatur diskutiert wird. Es ist allerdings durchaus nicht ausgeschlossen, neben dem „Horrorszenario"[23] einer Diktatur auch in modernen, weniger „krassen" Propagandamitteln wie beispielsweise der gezielten Verwendung von Daten aus sozialen Netzwerken zu politischen Zwecken[24] oder in von Regierungsstellen vorgetäuschten Massenbewegungen in sozialen Netzwerken (Astroturfing) eben dieses Risiko zu sehen.[25] Dabei können etwa Socialbots, also Computerprogramme zur Kontrolle von Accounts sozialer Netzwerke, risikoverstärkend eingesetzt werden.[26]

Diese realistischeren Praktiken werden jedoch bereits durch die kompetenziellen Grenzen und die Neutralitätsgrenzen eingeschränkt, die das BVerfG der Öffentlichkeitsarbeit der Regierung in der Entscheidung vom 2.3.1977 gesetzt hat.[27] Zur Klarstellung könnten hier allerdings Regelungen geschaffen werden, die zur Offenlegung der (Regierungs-)Urheberschaft bei Kommunikation in sozialen Netzwerken, Blogs etc., verpflichten.[28] Die Enthüllungen der NSA-Überwachungstätigkeit[29] unterstreichen das Risiko, da sie die umfassende Verschaltung von Informationen privater Kommunikationsunternehmen mit dem Staat und damit die Nähe der beiden größten Informationsverarbeitungsbereiche belegen.

---

[22] *Bull*, Informationelle Selbstbestimmung, S.78 f.

[23] Ebd., S. 78.

[24] Übergreifend zu möglichen Einsatzfeldern *Punie* u.a. (Hrsg.), Social Computing, S. 131 f.; für ein Beispiel der Aussagekraft möglicher Analysen http://www.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence [Stand: 28.3.2014].

[25] http://de.wikipedia.org/wiki/Astroturfing [Stand: 28.3.2014].

[26] Zur Anfälligkeit sozialer Netzwerke für diese Methoden vgl. *Boshmaf* u.a., Socialbot Network, 2011, http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf [Stand: 28.3.2014].

[27] BVerfG Urteil vom 2.3.1977, 2 BvE 1/76 *(Öffentlichkeitsarbeit der Regierung)* = BVerfGE 44, 125. Dazu unter Berücksichtigung des Internets *Mandelartz/Grotelüschen*, NVwZ 2004, 647 ff.

[28] Zu ähnlichen Regelungen für den kommerziellen Bereich durch die amerikanische Verbraucherschutz- und Kartellbehörde FTC vgl. die „Guides Concerning the Use of Endorsements and Testimonials in Advertising", 16 CFR Part 255, http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-publishes-final-guides-governing-endorsements-testimonials/091005revisedendorsementguides.pdf; vgl. auch http://arstechnica.com/tech-policy/2009/10/more-transparency-coming-to-blog-reviews-under-new-ftc-rules/ [Stand: 28.3.2014].

[29] Siehe insb. oben Teil 2, II.B.d) sowie Teil 3, II.16.

*b) Konformistische Verhaltensanpassung durch Überwachungsdruck*

Ein Risiko, das von Rechtsquellen auf allen analysierten Ebenen häufig an tragender Stelle aufgegriffen wird, ist die konformistische Verhaltensanpassung durch Überwachungsdruck und deren Auswirkungen auf den demokratischen Staat. An dieses Risiko knüpft insbesondere das Volkszählungsurteil des BVerfG an: Die Unsicherheit über die Speicherung abweichenden Verhaltens führe dazu, dass der Betroffene versuche, „nicht durch solche Verhaltensweisen aufzufallen".[30] Das Beispiel des Gerichts, wonach Überwachung zu einem vorbeugenden Verzicht auf Grundrechtsausübung führt, wird in späteren Entscheidungen immer wieder aufgenommen und auch mit den Topoi „psychischer Druck" bzw. „Einschüchterungseffekte" umschrieben.[31]

Der spezifische Bezug von Überwachung und Demokratie wird auch auf anderen Regelungsebenen, insbesondere in der Rechtsprechung des EGMR gesehen: Dort wird das Risiko als Überwachungsbedrohung (menace of surveillance) bezeichnet, wobei auf die Volkszählungsentscheidung und das Ziel der Verhinderung eines *Orwell'schen* „big brother"-Systems verwiesen wird.[32] Auch in der Datenschutzkonvention des Europarats und der IPBürg finden sich Anklänge an dieses Risiko eines „Überwachungsdrucks".[33] Der spezifische Demokratiebezug wird jedoch dort, wie auch in den EU-Rechtsquellen, nicht eindeutig herausgestellt. Gleichwohl lässt sich auch im Europäischen Recht das Risiko „Überwachungsdruck" nachvollziehen, wobei die Metapher vom „gläsernen Bürger" allgegenwärtig ist.[34]

In den Literaturkonzeptionen ist der Bezug des Risikos zur Makroebene deutlicher: So zielt etwa die erste Ebene in *Albers* Konzeption auf die Fassung des Gewährleistungsgehalts aus einer überindividuellen, übergreifenden Perspektive. Hier sieht sie Risiken „allumfassender" Verarbeitung, die kulturell verankert seien. Sie verweist auf *Orwell* und das Risiko „gläserner Bürger".[35] Auch *Roßnagel* sieht Risiken für die demokratische Ordnung, wobei er insbesondere mit Verhaltensauswirkungen in Form von Anpassungen an vermutete Erwartungshaltungen argumentiert.[36] Nach *Mallmann* führten die Überwachungsmechanismen zu Apathie und Konformität, es fehle der Freiraum zur Erprobung alternativer Sozialmodelle. Politische Aktivitäten der Bürger könnten durch das Bewusstsein intensiver politischer Überwachung eingestellt oder stark reduziert werden.[37]

---

[30] Siehe oben Teil 3, II.B.3.b).
[31] Siehe oben Teil 3, II.B.3.e).
[32] Siehe oben Teil 1, IV.B.1. und 1.a).
[33] Siehe oben Teil 1, II.A.2.d) sowie III.B.1.
[34] Siehe oben Teil 2, II.B.2. c); III.A.2.b); C.2.a); E.2; F.2.e).
[35] Siehe oben Teil 3, III.A.2.c).
[36] Siehe oben Teil 3, III.D.2.a).
[37] Siehe oben Teil 3, III.E.2.c).

Inwieweit der Informationsumgang tatsächlich einen Schaden für die Demokratie bewirkt, hängt jedoch entscheidend von individuellen Verhaltensänderungen aufgrund der Informationsverfügbarkeit ab. Um hier zu einer wirklich tragfähigen Risikofassung zu gelangen, muss die Lücke zwischen der Verfügbarkeit personenbezogener Daten und den möglichen Verhaltensauswirkungen geschlossen werden. Dies wird von vielen Konzeptionen ganz offenbar als so selbstverständlich vorausgesetzt, dass sie hierzu keine Stellung beziehen. Angesichts der heutigen Normalität weitgehender Informationsverfügbarkeit lässt sich jedoch auch die entgegengesetzte These vertreten. Danach hat sich bei den meisten Bürgern gerade wegen der großen Anzahl und Komplexität der Informationsvorgänge kein Bewusstsein einer Überwachung gebildet; gerade der Umstand, dass die allermeisten Datenverarbeitungen ohne jede nachteilige Folge bleiben und im Gegenteil eine vielfältige Bereicherung des Lebens bewirkten, habe vielmehr das Vertrauen in Informationstechnologie gestärkt.[38] Dieses Vertrauen – sollte es tatsächlich bestehen – würde die Existenz eines Risikos konformistischer Verhaltensänderung stark infrage stellen.

Auf eine andere mögliche Fehlerquelle in der Verhaltensthese weist eine sozialpsychologische Studie von *Tripathi* hin, wonach eine große Diskrepanz zwischen Privatheitswunsch und Wirklichkeit nicht nur, wie zu erwarten, zu einer größeren Privatheitspräferenz führen kann, sondern – im Gegenteil – auch zu deren Abnahme (cognitive dissonance reduction).[39] Gerade dieser Einwand stellt eine besondere Schwäche der gängigen Risikokonzeption dar, da er selbst nach Bekanntwerden umfassender Überwachungstätigkeiten wie derjenigen der NSA nicht von der Hand zu weisen ist: Selbst die umfassendste Kommunikationsüberwachung kann mangels tatsächlich „spürbarer" nachteiliger Auswirkungen auf Seiten der Betroffenen statt zu einer konformistischen Verhaltensanpassung vielmehr zu Ignoranz oder Trotz führen.

Von den genannten Autoren erkennt allein *Mallmann* diese Problematik und verweist auf eine empirische Untersuchung zu den Auswirkungen politischer Überwachung in der Zeit des McCarthyismus.[40] Diese Untersuchung trifft aber nicht den Kern der Konformitätsthese, da damals tatsächlich mit dem Ziel einer politischen Steuerung überwacht und an die Befunde entsprechende Sanktionen geknüpft wurden. Parallelen dazu lassen sich heute allenfalls im Tätigkeitsbereich des Bundesamtes für Verfassungsschutz sehen, wo „Bestrebungen" gemäß § 4 Abs. 1 a)–c) BVerfSchG ebenfalls politisch bestimmt werden. Die Aufgaben des Verfassungsschutzes beziehen sich jedoch gemäß § 3 Abs. 1 Nr. 1–4 BVerfSchG

---

[38] Ähnliches legen Untersuchungen zu Leistungskontrollen am Arbeitsplatz nahe, die, sofern die Ziele des Arbeitgebers von den Arbeitnehmern positiv bewertet wurden (z.B. Belohnung von Leistungen), zur Akzeptanz der Kontrollmaßnahme führten, vgl. *Griffith*, zit. nach *Margulis*, 59 Journal of Social Issues 2 (2003), 255.

[39] *Tripathi*, Psychological Studies 55 (2010), 109.

[40] Siehe oben Teil 3, III.E.2.c).

auf die Informationssammlung zu gewaltbereitem Extremismus und sind insgesamt mangels Vollzugskompetenzen schwach ausgestaltet.[41] Zwar ist nicht auszuschließen, dass die Tätigkeit des eher „zahnlosen" Verfassungsschutzes verhaltensrelevante Auswirkungen hervorruft. Dies ändert jedoch nichts an dem Befund, dass die Vermutungen zu Verhaltensauswirkungen um Belege ergänzt werden müssen und dass auch alltägliche Datenverarbeitungen und Informationsverfügbarkeiten *unter den Bedingungen eines intakten Rechtsstaats, also ohne Elemente politischer Verfolgung*, eine konformistische Verhaltensdrift auslösen können. In diese Richtung geht bislang allerdings keine der dargestellten Konzeptionen.

Sicher lässt sich eine gewisse Plausibilität der Angst vor politischer Verfolgung angesichts der deutschen Vergangenheit nicht abstreiten. Auch soll eine mögliche Schutzbedürftigkeit wegen bestimmter Befürchtungen der Bürger vor ungerechtfertigten „informationsbedingten" Rechtsnachteilen nicht in Abrede gestellt werden. So können zum Beispiel auch in unserer Demokratie an spezifische Informationen bestimmte Nachteile durch den Staat geknüpft werden, die sogar – wie etwa bei Prüfungsentscheidungen oder beamtenrechtlichen Beurteilungen – nur eingeschränkter gerichtlicher Kontrolle[42] unterliegen. Gleichwohl zeigt die hier vorgenommene Analyse dieser Risiken, dass deren datenschutzrechtliche Erfassung auf eine bessere und gesichertere Grundlage gestellt werden muss. Auch die Desiderata in der Forschung dürften dafür verantwortlich sein, dass sich die Positionen der „Datenschutzbefürworter" und der „Datenverarbeitungsbefürworter" oftmals besonders unversöhnlich und emotional aufgeladen gegenüberstehen.

Leider kann an dieser Stelle nicht die psychologische oder auch ökonomische Forschung zum Thema „privacy" vollständig und fachlich qualifiziert (also vom Standpunkt der jeweils außerrechtlichen Fachdisziplin aus) einbezogen und ausgewertet werden. Jedoch lässt sich einschlägigen Überblicksartikeln entnehmen, dass die oben aufgeworfene Frage mit dem durchaus vorhandenen Forschungsmaterial zum Thema „privacy" im Rahmen eines interdisziplinären Forschungsprojekts untersucht werden sollte. Neben sozialpsychologischen Arbeiten im Anschluss an die einflussreichen privacy-Theorien von *Westin* und *Altmann*[43] hat insbesondere die empirische Wirtschaftsforschung das Potenzial, über den Zusammenhang von Privatheitspräferenzen und Kaufentscheidungen verallgemeinerungsfähige Aussagen zu Verhaltensauswirkungen des Informationsumgangs zu gewinnen.[44]

---

[41] Siehe aber zur Problematik der Antiterrordatei oben Teil 3, II.B.17.

[42] Jedoch ist auch bei Bestehen eines Beurteilungsspielraums gerichtlicher Schutz bei Überschreiten eben dieses Spielraums wegen „sachfremder Erwägungen" möglich, statt vieler BVerwG, Beschluss vom 13.5.2004 - 6 B 25/04 = NVwZ 2004, 1375 (1377).

[43] Zu einem Überblick über die Theorien von *Westin* und *Altmann* sowie darauf bezogene sozial-psychologische Forschungen vgl. *Margulis*, 59 Journal of Social Issues 2 (2003), 411 ff.

[44] Vgl. z.B. *Brown/Muchira*, 5 Journal of Electronic Commerce Research 1 (2004), 62 ff.; *Baumer/Brande Earp/Evers*, 4 N.C.J.L. & Tech (2002–2003), 217 ff.; *Boritz/No*, Behavior,

Im Ergebnis lässt sich die Notwendigkeit einer Verknüpfung der juristisch relevanten Frage von Verhaltensauswirkungen mit den Erkenntnissen sozialpsychologischer und wirtschaftswissenschaftlicher Forschung zum Zusammenhang von Privatheit und Verhalten feststellen. Der Zusammenhang ist bislang noch nicht hinreichend belegt. Diese Frage sollte deshalb durch ein interdisziplinäres Forschungsprojekt mit einer entsprechend besetzten Forschungsgruppe untersucht werden.

### *c) Verantwortungsnegation*

Ein weiteres Risiko der Makroebene – das der Verantwortungsnegation – lässt sich an dem Recht festmachen, keinen „erheblich beeinträchtigenden" und rechtserheblichen Entscheidungen unterworfen zu werden, sofern diese ausschließlich aufgrund automatisierter Datenverarbeitung zum Zwecke der Bewertung einzelner Aspekte der Person erfolgen. Das zugrunde liegende Risiko wird als übermäßige Bedeutungszumessung informationstechnischer Entscheidungen umschrieben, die eine scheinbare Objektivität und Unbestreitbarkeit erlangen könnten. Die Individualität des Einzelnen könne ignoriert, er selbst als bloßer Teil einer effizienzorientiert gewählten Gruppe behandelt werden. Deutlich wird dabei der Bezug zum Schutzgut der Menschenwürde.[45] Das Risiko findet seine Entsprechung in den Vorschlägen für eine Datenschutzgrundverordnung und wurde im nationalen Recht mit § 6a BDSG umgesetzt.

Eine ähnliche Regelung findet sich in § 114 BBG hinsichtlich der Personalakten von Beamten. Besonders deutlich sind die Bezüge im europäischen Sekundärrecht zum Topos „Persönlichkeitsprofile", wobei die Reformvorschläge zur Datenschutzgrundverordnung hierfür den Begriff „Profiling" wählen.[46] In der Literatur wird das Risiko insbesondere von *Mallmann* aufgegriffen und als Entlastung vom Legitimationsdruck einer Entscheidung sowie als Verstärkung „partizipationsfeindlicher Entscheidungsprozesse" bzw. als mögliche Quelle einer Potenzierung von Entscheidungsfehlern dargestellt.[47]

Inwieweit dieses Risiko begründet ist, lässt sich exemplarisch an § 62 BBG zeigen. Die Regelung bestimmt im ersten Absatz, dass Beamte für die Rechtmäßigkeit ihrer dienstlichen Handlungen die volle persönliche Verantwortung tragen. Bei Zweifeln sind sie auf die in den Absätzen 2 und 3 näher ausgestaltete Remonstration verwiesen, wobei die innerbehördlich letztverbindliche Entscheidung durch

---

2007, http://accounting.uwaterloo.ca/uwcisa/resources/eprivacy/Privacy%20Customer%20Paper%202008-01-19.pdf [Stand: 28.3.2014]; *Kim/Ferrin/Rao*, 44 Decision Support Systems (2008), 544 ff.

[45] Siehe oben Teil 2, III.A.2.c) sowie E.2.

[46] Siehe oben Teil 3, E.2.e).

[47] Siehe oben Teil 3, III.E.2.e).

Vorgesetzte und die Weisungspflicht der Untergegebenen sichergestellt wird. Der Remonstration vorgelagert und durch die Bindung an Gesetz und Recht, Art. 20 Abs. 3 GG, verfassungsrechtlich geschützt ist das Normprüfungsrecht des Beamten. Dieses dient der Neutralität und Gemeinwohlverpflichtung des Berufsbeamtentums.[48] Aus demokratietheoretischer Sicht ist die Exekutivgewalt den ausführenden Personen vom demokratischen Souverän lediglich übertragen und anvertraut worden. Die Legitimität der Verwaltungshandlung hängt deshalb davon ab, inwieweit die betroffenen Bürger die Entscheidungen nachvollziehen und kontrollieren können.[49] Die für die Akzeptanz und Legitimation des Verwaltungshandelns so wichtige Kontrolle und Nachvollziehbarkeit ist jedoch bei bestimmten, nicht nur untergeordneten, rechtserheblichen Entscheidungen in Gefahr, wenn diese allein automatisiert erfolgen. Auch hier ist das Risiko jedoch nicht in jedem Fall vorhanden, weshalb differenziertere Regelungen erforderlich sind. So wäre es denkbar, durch stark ausgestaltete Informationspflichten und zeitgleiche Interventionsmöglichkeiten der Betroffenen das Risiko zu verringern, indem beispielsweise von der betroffenen Person erreicht werden kann, dass sich ein Mensch mit dem Verwaltungsvorgang befasst. Voraussetzung wäre jedoch ein sehr hohes Maß an Funktionalität der E-Government-Mechanismen, um sicherzustellen, dass die Betroffenen tatsächlich Kenntnis von den jeweiligen Entscheidungen und den ihnen zukommenden Möglichkeiten haben. Als Beispiel dafür kann das zivilrechtliche Mahnverfahren gemäß §§ 688 ff. ZPO genannt werden.

### 2. Wirtschaftliche Risiken

Neben den gesellschaftlich-politischen Risiken bildeten bereits in der Frühphase des Datenschutzrechts wirtschaftliche Risiken eine Motivation zum Aufbau des Datenschutzrechts. Die wirtschaftlichen Risikokonzeptionen der analysierten Normen lassen sich dabei in zwei Gruppen unterteilen. Zum einen richten sie sich gegen Handelshemmnisse durch nichtharmonisiertes nationales Datenschutzrecht; zum anderen werden negative Effekte aufgegriffen, die sich aufgrund sinkenden Verbrauchervertrauens ergeben, das auf mangelndem Datenschutzrecht beruht. Beide Gruppen betreffen die Wirtschaft insgesamt, weshalb sie hier als Makrorisiko eingeordnet werden. Eine Unterscheidung zwischen volkswirtschaftlicher (Makro-) und betriebswirtschaftlicher (Mikro-)Ebene ist in diesem Kontext nicht erforderlich.

---

[48] *Battis*, BBG, § 63 Rn. 2.

[49] *Behnke*, in: Czerwick/Lorig/Treutner (Hrsg.), Responsivität, S. 53.

*a) Handelshemmnisse*

Verschiedene Normen aus der Frühphase des Datenschutzrechts beziehen sich zwar auf den Persönlichkeitsrechtsschutz, bleiben diesbezüglich aber ungenau und unspezifisch. Besser fassbar sind hingegen die dort enthaltenen Risikokonzeptionen, die sich gegen nicht tarifäre Handelshemmnisse durch nationales Datenschutzrecht richten. Teilweise erwecken die Normen dabei den Eindruck, das Risiko nicht nur in den faktischen Auswirkungen national unterschiedlichen (legitimen) Datenschutzes zu sehen, sondern gerade auch in der protektionistischen Zweckentfremdung des Datenschutzrechts. Problematisch ist der durch eine solche Risikokonzeption geschaffene rechtspolitische Anreiz zur Harmonisierung durch Abbau des Datenschutzrechts, der in der Frühphase der Datenschutzkonvention des Europarats anklingt.[50] Die Außenhandelsbeschränkung stellt insoweit ein spezifisch wirtschaftspolitisches Risiko dar, zu dessen Abwendung die Anpassung des Datenschutzrechts nur eine mittelbare Funktion erfüllt. Der Grundrechtsschutz wird insoweit zu bloßem Vorwand.

Das geringe Maß an Konkretisierung einschlägiger Grundrechte dürfte sich auch durch die Dominanz dieser Sichtweise in der Frühphase des Datenschutzrechts erklären. Der Zweck des Datenschutzrechts wird nämlich bereits dann durch ein „irgendwie" geartetes Regelungsgefüge erfüllt, sofern es nur zu einer Harmonisierung führt. Ein aktuelles Beispiel für ein derart „zahnlos-zweckentfremdetes" Datenschutzrecht ist das APEC Privacy Framework, das das Risiko von unnötigen Einschränkungen des Informationsflusses sowie die Abhängigkeit der Wirtschaft von Informationen beschreibt, sich im Vergleich dazu aber kaum anderen einschlägigen Risiken zuwendet. Entsprechend schwach ist die Ausgestaltung der Regelungen.[51]

Das Risiko von Handelsbeschränkungen tritt auch in den OECD-Leitlinien und im GATS hervor.[52] Ein besonderer Stellenwert kommt dem Risiko von Handelshemmnissen im EU-Recht zu, wo schon aus kompetenziellen Gründen – bis zum Vertrag von Lissabon – die Gefahr inkompatibler Datenschutzregelungen Grundlage einer auf die Binnenmarktharmonisierung beschränkten Union war. Trotz der nunmehr bestehenden datenschutzrechtlichen Kompetenztitel bleibt die „dualistische Konzeption" einer Grundrechtsharmonisierung zur Binnenmarktharmonisierung auch den aktuellen Reformvorschlägen immanent.[53]

Das beste Beispiel für das Risiko divergierender Datenschutzregelungen und die Gefahr einer „Verschleifung" des Datenschutzes auf niedrigem Niveau ist das Safe-Harbor-Abkommen in Bezug auf den Datenaustausch zwischen europäischer und

---

[50] Vgl. oben Teil 1, II.A.2.a) und 3.

[51] Vgl. oben Teil 1, II.F.1.

[52] Vgl. oben Teil 1, II.D.2. und G.

[53] Vgl. oben Teil 2, III.A.1. und III.F.2.

US-Rechtsordnung.[54] Nicht zuletzt deshalb ist das Risiko durchaus gut begründet. Die Folgen informationeller Barrieren aufgrund unterschiedlicher Datenschutzregelungen können sich dabei in den heutigen globalisierten und hoch technisierten Abläufen an allen Stellen der Wertschöpfungskette eines Unternehmens negativ auswirken. Zur Anschauung sei auf die betriebswirtschaftlichen Modelle zur integrierten Informationsverarbeitung in Unternehmen verwiesen.[55]

*b) Nachfragerückgang durch Vertrauensverlust*

Das zweite wirtschaftliche Risiko liegt in einem Nachfragerückgang durch Vertrauensverlust bei Verbrauchern. Es wird insbesondere vom APEC Privacy Framework aufgegriffen: Fehlendes Vertrauen in den Schutz des Persönlichkeitsrechts könne ein Hindernis bei der Nutzung der Vorteile des elektronischen Handels darstellen.[56] In der Rechtsprechung des EGMR klingt dieses Risiko lediglich in Bezug auf den Schutz von Medizindaten und die Möglichkeit der Nichtinanspruchnahme medizinischer Dienstleistungen im Fall von Vertrauensverlust an.[57] Den Bezug zum Vertrauen in Online-Dienste stellt hingegen insbesondere auch der Entwurf einer Datenschutzgrundverordnung her: Ohne die notwendige Vertrauensbasis könne das Potenzial der digitalen Wirtschaft nicht ausgeschöpft werden. Das Vertrauen sei Grundlage für Online-Einkäufe. Zum Beleg für das Risiko wird auf Umfragen zu gefühltem Vertrauensverlust unter den Bürgern, auf die Debatten um Online-Kartierungssysteme (Google Maps) und die Schwierigkeit der Löschung von Daten in sozialen Netzwerken verwiesen.[58]

In der Tat bringen Umfragen regelmäßig vorhandene Befürchtungen hinsichtlich fehlenden Datenschutzes an den Tag.[59] Allerdings könnte das Verbrauchervertrauen viel stärker von kulturellen als von Rechtsschutzaspekten abhängig sein. So wies eine Studie trotz unterschiedlicher Regulierungsstrukturen auf eine im Vergleich zu Deutschland höhere Nutzungsbereitschaft der Endkunden in China, Korea und den USA hin.[60] Insgesamt scheint derartigen Befragungen auch nur eine geringe Aussagekraft hinsichtlich des tatsächlichen Nutzungsverhaltens der Betroffenen zuzukommen. So ergab die BITKOM-Untersuchung zu sozialen Netzwerken zwar,

---

[54] Vgl. hierzu: http://www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html?nn=409532 [Stand: 28.3.2014]; *Reimer*, DuD 2010, 733; *Regan*, 59 Journal of Social Issues 2 (2003), 263 ff. und *Genz*, Datenschutz, 2004.

[55] *Mertens*, Informationsverarbeitung, S. 13–23.

[56] Vgl. oben Teil 1, II.F.2.

[57] Vgl. oben Teil 1, IV.B.5.

[58] Vgl. oben Teil 2, III.F.2.

[59] Vgl. etwa speziell zur Nutzung sozialer Netzwerke BITKOM (Hrsg.), Soziale Netzwerke, S. 28 f.; allgemein Europäische Kommission (Hrsg.), Eurobarometer 359, S. 137–145; Münchner Kreis (Hrsg.), Zukunftsbilder, S. 28.

[60] Münchner Kreis (Hrsg.), Zukunftsbilder, S. 28.

dass 62 % der Befragten Facebook misstrauen – gleichwohl waren 51 % dort angemeldet und immerhin 45 % aktive Nutzer (unter den 14- bis 29-Jährigen waren 71 % aktiv).[61] Angesichts der hohen monatlichen Nutzerzahlen in Deutschland – im Sommer 2013 ca. 26 Millionen[62] – dürfte der Nutzungsgrad seitdem weiter gestiegen sein.

Die Zukunftsstudie des Münchner Kreises zeigte auch, dass sich nur wenige der Befragten trotz ihres Misstrauens und der Angst vor Betrugsfällen davon abhalten ließen, im Internet zu bezahlen.[63] Andererseits ergab eine Umfrage des Verbraucherzentrale-Bundesverbands, dass 48,7 % der Privatpersonen, die beabsichtigen, ein Online-Kundenkonto zu löschen, sich um die Sicherheit ihrer Daten sorgten.[64] Auf ein weiteres mit dem Verlust von Verbrauchervertrauen eng verbundenes Risiko weist eine Erhebung von ConsumerReports.org hin, wonach die Zahl der Nutzer, die bewusst falsche Informationen auf Facebook angeben, im Zeitraum von 2010 bis 2012 von 2 % auf 25 % gestiegen ist.[65] Relativiert wird dieses Ergebnis jedoch von einer BITKOM-Befragung aus dem Jahr 2012, die ergab, dass 58 % der Mitglieder sozialer Netzwerke ihren vollen Vor- und Nachnamen angaben.[66]

Zweifel an der engen Verbindung zwischen Privatheitspräferenz und tatsächlicher Kaufentscheidung weckt dagegen ein Experiment, das von Forschern des Deutschen Instituts für Wirtschaftsforschung zusammen mit der Universität Cambridge (Vereinigtes Königreich) im Auftrag der europäischen IT-Sicherheitsagentur ENISA durchgeführt wurde: 443 Studenten der Berliner Technischen Universität konnten beim Kauf von Kinokarten zwischen zwei Anbietern wählen. Beide fragten nach Namen, Geburtsdatum und E-Mail-Adresse der Kunden, wobei einer zusätzlich entweder die Handynummer oder aber die Einwilligung verlangte, Werbung per E-Mail zusenden zu dürfen. Die Angaben wurden überprüft, sodass keine falschen Daten eingegeben werden konnten. Bei diesem Anbieter kosteten die Kinokarten 7 Euro, bei dem anderen 7,50 Euro. Obwohl 93 % der Teilnehmer in einer Befragung nach dem Experiment angaben, „interessiert“ oder „sehr interessiert“ an Datenschutz zu sein, entschieden sich nur 41 % für den Anbieter, der aus Datenschutzperspektive vorteilhafter war.[67]

---

61 BITKOM (Hrsg.), Soziale Netzwerke, S. 8.

62 http://allfacebook.de/userdata/ [Stand: 28.3.2014]. Seit dem 15.6.2013 wird die automatische Erfassung der Nutzungszahlen durch Drittanbieter unterbunden, sodass keine aktuelleren Zahlen verfügbar sind.

63 Münchner Kreis (Hrsg.), Zukunftsbilder, S. 60.

64 Verbraucherzentrale Bundesverband e.V. (Hrsg.), Accounts, S. 4.

65 Vgl. https://www.unwatched.org/20120504_Steigendes_Misstrauen_Besorgte_User_beluegen_Facebook?pk_campaign=twun&pk_kwd=20120504 [Stand: 28.3.2014].

66 http://www.bitkom.org/de/presse/74534_72558.aspx [Stand: 28.3.2014].

67 ENISA (Hrsg.), Monetising Privacy; Zusammenfassung bei Heise, http://www.heise.de/newsticker/meldung/Studie-Manche-Verbraucher-zahlen-fuer-Privatsphaere-1477662.html [Stand: 28.3.2014].

Das Verbrauchervertrauen könnte jedoch nicht nur wegen des Risikos von Nachfragerückgängen relevant sein: In einem Experiment der amerikanischen Psychologen *Brandimarte/Acquisti/Loewenstein* sollten Probanden Bögen mit teils sehr intimen Fragen ausfüllen, auf deren Grundlage angeblich ein Profil für ein neues universitäres soziales Netzwerk erstellt werden sollte. Soweit die Probanden einen – wenn auch nur geringen – Einfluss auf den Datenumgang hatten, erhöhte dies die Preisgabe von Informationen. Darüber hinaus zeigten sich Hinweise auf den Effekt der „Risiko-Homöostase", wonach Menschen zu besonders riskantem Verhalten neigen, wenn sie den Eindruck haben, selbst Kontrolle ausüben zu können: Das Preisgabeverhalten blieb auch dann abhängig vom Kontrollgefühl, wenn die Veröffentlichungswahrscheinlichkeit und damit das objektive Risiko verändert wurde.[68]

Festzuhalten bleibt, dass das Risiko von Nachfragerückgängen zwar plausibel ist, von den zitierten Umfragen und dem Experiment von ENISA allerdings relativiert wird, da der Wunsch nach Inanspruchnahme einer Leistung die eigenen Bedenken häufig zerstreut. Dieser Befund deckt sich auch mit der allgemeinen Lebenserfahrung. Dagegen liegt ein – von den untersuchten Instrumenten bisher noch nicht aufgegriffenes, gleichwohl in diesem Zusammenhang stehendes – Risiko in nachteiligen wirtschaftlichen Auswirkungen durch den Rückgang von Informationspreisgaben und Falschangaben bei geringem „Datenkontrollgefühl". Der Wunsch nach Leistungsinanspruchnahme kann dieses Risiko nur dann verringern, wenn die personenbezogenen Daten nicht in Form einer Individualisierung Bestandteil eben dieser Leistung sind.

## B. Mikroebene: Überwiegend individuelle Risiken

### 1. Erhöhung individueller Verletzlichkeit durch Straftaten

Das Risiko der Erhöhung individueller Verletzlichkeit durch den Umgang mit personenbezogenen Daten ist in fast allen untersuchten Instrumenten gegenwärtig und dürfte auch in der öffentlichen Debatte am deutlichsten präsent sein. Bereits auf der Ebene internationaler Datenschutzinstrumente beziehen sich darauf die Grundsätze der Datenrichtigkeit sowie die Anforderungen an technische Schutzmaßnahmen in der Datenschutzkonvention des Europarats.[69] Ausdrücklich formuliert das auch das APEC Privacy Framework mit dem Prinzip „preventing harm", dem Schutz vor schädlichen Konsequenzen von Privatheitsverletzungen und Miss-

---

[68] Vgl. *Brandimarte/Acquisti/Loewenstein*, Social Psychological and Personality Science (Online-Version, http://spp.sagepub.com/content/4/3/340) 2012, 1–8; Zusammenfassung bei *Herrmann*, SZ vom 14.8.2012 sowie unter http://www.sueddeutsche.de/digital/privatsphaere-im-social-web-wie-man-internetnutzer-zum-sprechen-bringt-1.1441039 [Stand: 28.3.2014].

[69] Siehe oben Teil 1, II.A.2.d).

bräuchen personenbezogener Informationen.[70] Festmachen lässt sich das Risiko auch an Art. 17 IPBürg.[71] In der Rechtsprechung des EGMR wird die Erhöhung individueller Verletzlichkeit bisher zwar nicht explizit herausgestellt; anders ist dies jedoch in den Schlussanträgen zu Entscheidungen des EuGH,[72] im europäischen Sekundärrecht[73] und in der Rechtsprechung des BVerfG,[74] wo es an jeweils verschiedenen Stellen ausdrücklich aufgegriffen wird. In der E-Kom-Richtlinie (RL 2002/58/EG) und in der Entscheidung des BVerfG zur Online-Durchsuchung wird das Risiko für die Fallgruppe technischer Infiltrationen weiter differenziert.

Die E-Kom-Richtlinie und die sie ergänzende E-Privacy-Richtlinie (RL 2009/136/EG) beziehen sich explizit auf den Einsatz von Spähsoftware und trojanischen Viren und verweisen zudem auf informationstechnische Schutzgüter. Die unbefugte inhaltliche Kenntnisnahme wird dabei dem Schutzgut der Vertraulichkeit zugeordnet. Als Beispiele für die individuelle Verletzlichkeit dienen Identitätsdiebstahl und Identitätsbetrug. Das Risiko dient weiterhin zur Begründung von Unterrichtspflichten bei Datenschutzverletzungen.[75] Der Vorschlag der Datenschutzgrundverordnung greift das Risiko ebenfalls bei Meldepflichten auf und nennt in Erwägungsgrund 68 „persönliche und wirtschaftliche Interessen“ bzw. in Erwägungsgrund 69 „Identitätsbetrug“ und andere Formen des Datenmissbrauchs, wobei im Rahmen der Folgenabschätzung eine aus Sicht der individuellen Verletzlichkeit inkonsequente Beschränkung auf Erhebungen in großem Umfang besteht.[76] Das Risiko lässt sich darüber hinaus auch an verschiedenen Konzeptionen des RL-Vorschlags festmachen.[77]

Von der analysierten Rechtsprechung des BVerfG ist für die Risikogruppe der Erhöhung individueller Verletzlichkeit vor allem das Urteil zur Online-Durchsuchung relevant. Hier wird – ähnlich wie bei der E-Kom-Richtlinie – das Schutzgut der Vertraulichkeit aufgegriffen und näher auf die Risiken von Infiltrationen informationstechnischer Systeme eingegangen. Daneben wird dem Schutzgut der Integrität die Möglichkeit von Schäden am Zielsystem zugeordnet. Das entscheidende Risiko der Infiltration liegt jedoch in der technischen Öffnung und den damit einhergehenden Datenmanipulations- und Ausspähungsmöglichkeiten – wiederum also in einer Erhöhung individueller Verletzlichkeit. Die insbesondere bei sozialen Netzwerken naheliegende Möglichkeit der Täuschungsinfiltration, die sich eben-

---

70 Siehe oben Teil 1, II.F.2.

71 Vgl. oben Teil 1, III.B.2.

72 Vgl. oben Teil 2, II.B.2.c)

73 Vgl. oben Teil 2, III.A.2.a), b); E.2.

74 Vgl. oben Teil 3, II. B.15.c).

75 Vgl. oben Teil 2, III.C.2.a)–d); 3.

76 Vgl. oben Teil 2, III.F.2.d), e).

77 Vgl. oben Teil 2, III.G.2.a), d).

falls als Erhöhung individueller Verletzlichkeit auffassen lässt, hat das Gericht nicht aufgegriffen.[78]

Im Rahmen der Analyse von Risiken sozialer Netzwerke verweist die Art.-29-Datenschutzgruppe ebenfalls auf die Kategorie „individuelle Verletzlichkeit". Ihr zufolge bestehen die Risiken insbesondere in Identitätsdiebstahl, finanziellen Einbußen, Nachteilen für Geschäfts- oder Erwerbsmöglichkeiten und Beeinträchtigungen der körperlichen Unversehrtheit.[79] Eine Ergänzung dieser durch private Verarbeitungen entstehenden Risiken ergibt sich bei Zusammenschau mit dem BVerfG-Urteil zur Vorratsdatenspeicherung: Hier wird die Gefahr von Missbrauch und illegalem Zugriff bei privater Datenverarbeitung mit den „Bedingungen von Wirtschaftlichkeit und Kostendruck" und den deshalb nur „begrenzten Anreize[n] zur Gewährleistung von Datensicherheit" begründet.[80] Überraschenderweise wird die Kategorie der Erhöhung individueller Verletzlichkeit in den untersuchten Literaturkonzeptionen kaum aufgegriffen. Lediglich die Ubiquitätskonzeption von *Roßnagel* deutet unter dem Topos „Datenmissbrauch" dieses Risiko an.[81]

Der Vergleich zeigt, dass die Fallgruppe der Erhöhung individueller Verletzlichkeit gut zu empirischen Beschreibungen wie dem *threat landscape* von ENISA passt. In dieser auf 120 Berichte relevanter Akteure (u.a. der Sicherheitsindustrie) gestützten Untersuchung werden 16 Bedrohungen für Internetnutzer beschrieben.[82] Die dort behandelten „top threats" setzen die Kenntnis personenbezogener Daten – häufig beispielsweise Zugangsdaten, Bankverbindungsdaten oder auch IP-Adressen[83] – voraus bzw. zielen wie im Fall von Phishing und Identitätsdiebstahl auf die Gewinnung weiterer personenbezogener Daten. Eine weitere phänomenologische Risikountersuchung von ENISA befasste sich 2011 mit den Risiken des *life-logging* und widmet sich auf individueller Ebene ebenfalls dem Betrugsrisiko.[84] Der Missbrauch von Profildaten sozialer Netzwerke, insbesondere zu Identitätsdiebstahl und Betrug wird auch im Rom-Memorandum der International Working Group on Data Protection in Telecommunications – einer Arbeitsgruppe der Internationalen Datenschutzkonferenz[85] – aufgegriffen.[86] Die Zusammenschau von phä-

---

[78] Siehe oben Teil 3, II.B.15.c); 16.e).

[79] Siehe oben Teil 2, III.A.2.a)

[80] Siehe oben Teil 3, II.B.13.

[81] Siehe oben Teil 3, III.D.2.b).

[82] ENISA (Hrsg.), Threat Landscape, S. 3.

[83] Die Einordnung der IP-Adresse als personenbezogenes Datum ist umstritten, vgl. *Spindler*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen, F 71 ff.

[84] Vgl. ENISA (Hrsg.), Life-logging-Studie, S. 7.

[85] Vgl. http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt [Stand: 28.3.2014].

[86] International Working Group on Data Protection in Telecommunications (Hrsg.), Rome Memorandum, Nr. 7 und 8.

nomenologischen Risikobeschreibungen und normativen Risikokonzeptionen legt es nahe, dass die zu dieser Fallgruppe zählenden Verhaltensweisen bereits nach geltender Rechtslage weitgehend strafbares Verhalten in vielen Rechtsordnungen darstellen.[87] Zahlreiche der von ENISA geschilderten Bedrohungen wie beispielsweise Trojaner, Würmer, Phishing oder Rogueware sind mittlerweile hinlänglich beschrieben.[88] Untersuchungen zu Häufigkeit und Schäden bei Straftaten im Internet[89] verdeutlichen die Relevanz des Risikos. Hinsichtlich einschlägiger Schäden braucht für Deutschland nur auf die durchschnittliche Schadenssumme von 4.000 Euro pro Phishing-Fall und auf insgesamt ca. 25,7 Millionen Euro, die dem BKA zufolge 2011 angefallen sind, verwiesen werden.[90]

### 2. Schamgefühl und Publizitätsschäden

Risiken, bei denen zugrunde liegende Schäden ohne weitere, außerhalb der betroffenen Person liegende Umstände eintreten – also bereits mit der Publizität der Information – lassen sich der Kategorie „Schamgefühl und Publizitätsschäden" zuordnen. Dieses Risiko wurde in der EGMR-Rechtsprechung bei Informationen zu Sexualstraftätern, Prostituierten sowie in Bezug auf Medizindaten oder Suizidversuche aufgegriffen.[91] Die allgemeinen Regelungskonzeptionen des Sekundärrechts greifen Publizitätsschäden insbesondere bei Kategorien sensibler Daten auf. Davon erfasst werden – neben den noch zu besprechenden Datenkategorien, die sich auf Selektivitätsrisiken beziehen – insbesondere schambesetzte Informationen wie beispielsweise Sexual-, Gesundheitsinformationen oder solche bezüglich vergangener Straftaten.[92] Auch das aktuelle Reformpaket greift das Risiko bei der Differenzierung nach Betroffenenkategorien im RL-Vorschlag auf.[93] Der GV-Vorschlag bezieht sich vor allem im Rahmen der Notifikationspflichten darauf.[94] Weitere Topoi, die sich in den unionsrechtlichen Konzeptionen dem Risiko der Publizitätsschäden zuordnen lassen, richten sich gegen Spähsoftware (Kenntnis intimer Informationen auf den betroffenen IT-Systemen) sowie Einkommensinfor-

---

87 Für eine nähere Analyse der in Betracht kommenden Verhaltensweisen vgl. *Sieber*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen.

88 Für eine kurze Zusammenfassung der wichtigsten Bedrohungen vgl. http://www.bitkom.org/de/presse/30739_74922.aspx [Stand: 28.3.2014].

89 *Sieber*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen, C 27 und C 29 m.w.N.

90 Vgl. Bundeskriminalamt (Hrsg.), Cybercrime 2011, S. 11 f; vgl. auch die Zusammenfassung auf http://www.bitkom.org/de/presse/74534_73455.aspx [Stand: 28.3.2014]; zur Haftung der Kunden im Fall von Identitätsmissbräuchen siehe *Borges*, NJW 2012, 2385 ff.

91 Siehe oben Teil 1, IV.B.4. und 6.

92 Siehe oben Teil 2, III.A.2.b); C.2.d).

93 Siehe oben Teil 2, III.G.2.a) sowie 3.

94 Siehe oben Teil 2, III.G.2.d).

mationen (zu Letzterem vgl. die EuGH-Rechtsprechung).[95] In der Rechtsprechung des BVerfG ist neben dem Scheidungsaktenbeschluss[96] die *Caroline*-Entscheidung zu nennen, in der solche Inhalte der Privatsphäre zugeordnet werden, deren öffentliche Erörterung oder Zurschaustellung als „unschicklich" gilt oder die als „peinlich" empfunden werden.[97]

Die beschriebenen Publizitätsschäden beziehen sich in erster Linie auf Informationen, deren Bekanntwerden zu einem gesellschaftlichen Achtungsverlust führt. Der bei Veröffentlichung sensibler Informationen eintretende unmittelbare Schaden lässt sich darüber hinaus aber auch als Auslösung von Stress auffassen und wird mit verschiedenen nachteiligen physiologischen und psychologischen Effekten in Verbindung gebracht.[98] Die körperlichen Folgen des Schamgefühls können damit über das sprichwörtliche Erröten hinausgehen und sind ein unmittelbar einsichtiges Risiko.

### 3. Selektivitätsschäden

Die analysierten Konzeptionen richten sich häufig gegen Diskriminierung und Stigmatisierung. Bei näherer Betrachtung handelt es sich bei beiden Fällen um rechtlich oder politisch unerwünschte Informationsverwendungen in Auswahlprozessen. Die informationsbezogenen Risiken treten dabei nicht nur in institutionell-formellen Auswahlprozessen – wie beispielsweise Bewerbungsverfahren – auf, sondern auch in persönlich-individuellen, wie etwa bei der Auswahl von Vertragspartnern. Im Extremfall können bestimmte Informationen zur Ausgrenzung aus gesellschaftlichen Beziehungen in Form „sozialer Abstempelung" verwendet werden. Im Folgenden werden die Fallgruppen von Diskriminierung und Stigmatisierung besprochen.

#### *a) Diskriminierung*

Der Begriff Diskriminierung wurde definiert als kategoriale Behandlung einer Person und einer damit verbundenen negativen Bewertung (Devaluation), wobei unter einer kategorialen Behandlung die Verwendung einer sozialen Kategorie zur Bezugnahme auf eine Person oder deren Herkunft zu verstehen ist.[99] Die untersuchten Instrumente greifen dieses Risiko insbesondere im Rahmen von Verarbeitungs-

---

95 Siehe oben Teil 2, III.C.2.a) sowie II.B.2.e).

96 Siehe oben Teil 3, II.B.1.

97 Siehe oben Teil 3, II.B.6.

98 Vgl. *Stone-Romero/Stone/Hyatt*, 59 Journal of Social Issues 2 (2003), 346.

99 Siehe oben Teil 1, II.A.2.d).

regeln auf, die an Kataloge von sensiblen bzw. sensitiven[100] Daten anknüpfen. Die Sensibilität der Informationen wird von den Instrumenten in Anlehnung an das Diskriminierungspotenzial bestimmt und liegt beispielsweise dann vor, wenn sich die Informationen auf die rassische Herkunft, auf Glaubensvorstellungen oder Sexualität beziehen. Derartige Kataloge finden sich auf allen untersuchten Ebenen, so etwa in der Datenschutzkonvention des Europarats,[101] in den UN-Richtlinien[102] – dort wird explizit ein Grundsatz der Nichtdiskriminierung etabliert – sowie im geltenden und geplanten europäischen Sekundärrecht, wobei hier die ausgeprägtesten materiellen Verarbeitungsanforderungen existieren.[103] Ein gemeinsames Merkmal der sensiblen Daten ist ihre Polarisierungswirkung.[104] So können beispielsweise Informationen zu politischen Einstellungen bei deren Anhängern starke Zustimmung, bei den politischen Gegnern dagegen starke Ablehnung hervorrufen. Ähnliches gilt für bestimmte Glaubens- und Weltanschauungsüberzeugungen.

Das Risiko wird in der untersuchten Rechtsprechung allerdings nicht häufig aufgegriffen. Am deutlichsten nimmt das BVerfG im Rasterfahndungsbeschluss zu Diskriminierungen Stellung: Maßgeblich sei eine „Reproduktion" von Vorurteilen bei informationsbezogenen Ermittlungsmaßnahmen. Zugrunde lag die Vorladung ausländischer Studenten zu „Polizeigesprächen" kombiniert mit einer „Überprüfung auf andere Weise" bei Nichterscheinen.[105] Daneben betraf lediglich die Entmündigungsbekanntmachung[106] und am Rande auch die Antiterrordateientscheidung[107] das Diskriminierungsrisiko. *Britz* sieht eine Verbindung zwischen der inneren Entfaltungsfreiheit als Schutzgut von Selbstdarstellung und sonstigen Diskriminierungsverboten. Diskriminierungen könnten zu einem mit dem jeweiligen Stereotyp verbundenen „Erwartungsgeflecht" führen und dadurch die Entfaltungsfreiheit des Einzelnen beeinträchtigen.[108] Das Reformgutachten von *Roßnagel* bringt das Diskriminierungsrisiko mit Selektionsprozessen und credit scoring in Verbindung;[109] nicht vertieft wird es hingegen bei *Mallmann*.[110]

---

[100] Die Begriffe „sensibel" und „sensitiv" werden in der Literatur teilweise synonym verwendet. Vorzuziehen ist der Begriff „sensibel", da „sensitiv" „überempfindlich" bedeutet, vgl. http://www.duden.de/suchen/dudenonline/sensitiv [Stand: 28.3.2014], während der Begriff „sensibel" auch „besonders viel Sorgfalt" oder „Umsicht erfordernd" umfasst, vgl. http://www.duden.de/rechtschreibung/sensibel [Stand: 28.3.2014]. Entsprechend wurde in dieser Arbeit auch der Begriff „sensitive" aus dem Englischen jeweils mit „sensibel" übersetzt.

[101] Siehe oben Teil 1, II.A.2.d).

[102] Siehe oben Teil 1, II.E.

[103] Siehe oben Teil 2, III.A.2.b); C.2.d); F.2.d); G.2.a).

[104] Siehe oben Teil 1, II.A.2.d).

[105] Siehe oben Teil 3, II.B.9.a).

[106] Siehe oben Teil 3, II.B.4.

[107] Siehe oben Teil 3, II.B.17.

[108] Siehe oben Teil 3, III.B.2.b).

[109] Siehe oben Teil 3, III.C.2.b).

Das Diskriminierungsrisiko ist durch die Kataloge sensibler Daten und die an soziologische Arbeiten angelehnte Definition plausibel. Eine Problematik der Konzeptionen liegt allerdings in der Ausklammerung des Elements der Devaluation. Dieses ist zwar bei strukturell-institutionellen Diskriminierungen regulatorisch schwer fassbar, gleichwohl könnte durch dieses Element womöglich eine bessere Unterscheidung zwischen legitimen und nicht legitimen Verarbeitungen von Daten der betroffenen Kategorien gelingen. Die bislang verfolgte Alternative sind umfassende Verbote wie in Art. 9 Nr. 1 GV-Vorschlag, die aber zu pauschal sind und eine umfangreiche und komplexe Regelung von Erlaubnistatbeständen und Ausnahmen erforderlich machen. So enthält beispielsweise das zunächst klar wirkende Verbot des Art. 9 Nr. 1 GV-Vorschlag in Nr. 2 insgesamt 10 Erlaubnisregelungen, die ihrerseits wieder durch Rückausnahmen und Verweisungen ein hohes Maß an Komplexität erreichen. Die Ausnahmen sind zum Teil auch schwer bestimmbar und undifferenziert, wie im Fall des „offenkundigen Öffentlichmachens von Informationen", Art. 9 Nr. 2. e) GV-Vorschlag. Die kürzlich bekannt gewordene Möglichkeit, aus (wohl in diesem Sinne öffentlich gemachten) Twitter-Äußerungen Rückschlüsse auf Psychopathien zu gewinnen,[111] verdeutlicht exemplarisch die Unzulänglichkeit der Regelung. Besser greifbar erscheint dort zumindest der devaluierende Effekt. Ansatzpunkt für ein Verbot könnte also die Devaluationswirkung bei den Betroffenen (denen beispielsweise Psychopathien unterstellt werden) sein. Mögliche Ausnahmetatbestände könnten hieran zielgenauer ausgerichtet werden.

Ein gemeinsames Merkmal bestimmter Elemente der oben angesprochenen Kataloge besteht in der Leistungsindikation.[112] Diese kann insbesondere bei Informationen zu Gesundheit und Vorstrafen vorliegen. Bei leistungsindizierenden Daten ist das Devaluationselement nicht zwingend gegeben, die Benachteiligung kann unabhängig davon im Arbeitsverhältnis erfolgen. Das Risiko der Leistungsindikation wird dagegen stärker im hier nicht gesondert untersuchten einfachgesetzlichen Datenschutzrecht aufgegriffen, wobei die Reformbestrebungen um den Arbeitnehmerdatenschutz[113] darauf hindeuten, dass das Risiko vom BDSG bislang noch nicht hinreichend abgedeckt wird.[114]

---

[110] Siehe oben Teil 3, III.E.2.a).

[111] http://www.heise.de/newsticker/meldung/Twitter-Sprache-kann-auf-Psychopathien-hinweisen-1674182.html [Stand: 28.3.2014].

[112] Siehe oben Teil 1, II.A.2.d).

[113] Zum aktuellen Stand: http://www.bfdi.bund.de/DE/Themen/Arbeit/Arbeitnehmer datenschutz/Artikel/Beschaeftigtendatenschutz.html?nn=409756 [Stand: 28.3.2014].

[114] Zum Ganzen vgl. die Beiträge von *Däubler, Wolf* und *Perreng*, in: Schmidt/Weichert (Hrsg.), Datenschutz.

### *b) Stigmatisierung*

Die untersuchten Instrumente sprechen nur zum Teil von „Stigmatisierung". Sie unterscheidet sich von Diskriminierung durch Qualität und Quantität. Maßgeblich ist – in Anlehnung an soziologische Konzepte – die Beziehung zwischen einem Stigmasymbol und einem gesellschaftlich verbreitetem Stereotyp, wobei sich ein Stigmasymbol durch große Verbreitung und gesellschaftliche Sichtbarkeit des Merkmals auszeichnet.[115]

Die Pressemitteilung zu den Empfehlungen des Europarats zum Profiling bezieht sich auf „Stigmatisierungen".[116] In der Rechtsprechung des EGMR wird das Risiko im Zusammenhang mit Gendaten und der Unschuldsvermutung genannt,[117] was wiederum an die Unterscheidung von Betroffenenkategorien im RL-Vorschlag erinnert.[118] In der Rechtsprechung des BVerfG wird das Risiko ebenfalls in Bezug auf Gendaten und die Rasterfahndung aufgegriffen.[119] Im GV-Vorschlag lässt sich das Risiko im Rahmen der Meldepflichten erst durch Zusammenschau mit dem nationalen einfachgesetzlichen Datenschutzrecht konkretisieren; bei der Datenschutz-Folgenabschätzung wird jedoch wieder auf bestimmte Kategorien Bezug genommen, wobei der Schutz von Gesundheitsdaten stärker ausdifferenziert wird.[120] Von den Literaturkonzeptionen nähert sich *Britz* der Selektionsproblematik in einer ihrer Fallgruppen an.[121]

Das Risiko von Stigmatisierungen wird in einschlägiger Privatheitsforschung zur Beschreibung der Kosten von Privatheitsverletzungen herangezogen: *Margulis* differenziert unter Verweis auf weitere einschlägige Studien zwischen körperlichen (Missbildungen), charakterlichen (Homosexualität) und demografischen (Rasse) Stigmata. Mangels sozialer Akzeptanz würden die stigmatisierten Individuen entwertet, ihnen werde ein geringerer sozialer Status zugeschrieben, und sie würden zu Zielen von negativen Stereotypen, von Vorurteilen und Diskriminierung. Das soziale Kernproblem des Diskreditierten sei das Management seiner sozialen Interaktion. Für den Diskreditierbaren sei es das Management von Informationen über das Stigma.[122] Als Folge der Stigmatisierung trete das Gefühl der Scham und des Ungewolltseins auf.[123] Studien an HIV-Trägern ergaben, dass mit der Zunahme der Erwartung einer gesellschaftlichen Stigmatisierung die Neigung wächst, die Infor-

---

115 Siehe oben Teil 1, II.C.

116 Siehe oben Teil 1, II.C.

117 Siehe oben Teil 1, 4.B.8.

118 Siehe oben Teil 2, III.G.3.

119 Siehe oben Teil 3, II.B.8. sowie 9.a), b).

120 Siehe oben Teil 2, III. F.2.d) und e).

121 Siehe oben Teil 3, III. B.2.c).

122 *Margulis*, 59 Journal of Social Issues 2 (2003), 247 f.

123 *Archer*, zit. nach ebd., 248.

mation über die Infektion nicht den Eltern, Intimpartnern oder Freunden zu offenbaren.[124] Stigmatisierung trete dann auf, wenn Personen Eigenschaften zugeschrieben würden, die eine Basis dafür bilden, diese Menschen zu meiden oder auszuschließen.[125] Speziell in Bezug auf Gendaten wird gefordert, den Privatheitsschutz auf der Ebene sozialer Gruppen zu stärken, da auch dort Verletzungen – selbst bei Nichtidentifikation von Individuen – auftreten können.[126] Die Frage nach der Zuordnung zur Makro- oder Mikroebene tauchte bereits bei der Diskussion der Konzeption von *Britz* auf.[127] Der Schwerpunkt des Stigmatisierungsrisikos wird von den übrigen Konzeptionen jedoch der individuellen Ebene zugeordnet. Etwas anderes könnte für das dem Stigmatisierungsrisiko ähnelnde, unten diskutierte Phänomen der Profilbildungen gelten.[128]

Aktuelle Beispiele können das Risiko illustrieren: So versammelte sich 2012 ein über Facebook organisierter „Lynchmob" vor einer Polizeiwache in Emden, der die Tötung eines sich später als unschuldig herausstellenden Sexualstraftäters forderte.[129] Weniger spektakulär, gleichwohl gesellschaftlich verbreitet und schwerwiegend ist die Stigmatisierung von HIV-Infizierten.[130]

Wie *Alpert* am Beispiel einer aufgrund ihrer Homogenität intensiv erforschten Bevölkerungsgruppe, den aschkenasischen Juden, zeigt, sind entsprechende Stigmatisierungen auch auf Gruppenebene denkbar. In dem von ihr genannten Beispiel der starken medizinischen Beforschung der Gruppe liegt die Intensität einer Stigmatisierung im hier beschriebenen Sinne jedoch noch nicht vor. [131]

### 4. Informationspermanenz

Sehr viele der untersuchten Konzeptionen greifen das Risiko der Informationspermanenz auf. Damit sind nachteilige Effekte gemeint, die sich gerade aus der langfristigen Verfügbarkeit von Informationen ergeben. Bereits seit der Datenschutzkonvention des Europarats weisen Regelungen, die sich mit der frühestmöglichen Depersonalisierung von Daten befassen, auf eben dieses Risiko hin.[132] Der EGMR griff im Zusammenhang mit der Verwendung von teilweise über 50 Jahre

---

[124] *Derlega* u.a., zit. nach *Margulis*, 59 Journal of Social Issues 2 (2003), 248.

[125] Vgl. *Leary/Schreindorfer*, zit. nach *Alpert*, 59 Journal of Social Issues 2 (2003), 304.

[126] Vgl. ebd., 313 f., 319.

[127] Siehe oben Teil 3, III.B.2.c)

[128] Siehe unten II.C.2.

[129] http://www.faz.net/aktuell/gesellschaft/kriminalitaet/facebook-aufruf-zur-lynchjustiz-zwei-wochen-dauerarrest-fuer-18-jahre-alten-mann-11767938.html [Stand: 28.3.2014].

[130] http://www.avert.org/hiv-aids-stigma.htm [Stand: 28.3.2014].

[131] So *Alpert* am Beispiel der aschkenasischen Juden, vgl. *Alpert*, 59 Journal of Social Issues 2 (2003), 313 f. 319.

[132] Siehe oben Teil 1, II.A.2.d).

alten Geheimdienstinformationen das Risiko in mehreren Entscheidungen auf.[133] Während es auf Ebene des EuGH zunächst nur am Rande von GA *Sharpstone* und *Jääskinen* thematisiert wurde,[134] wird dieses Risiko in der Entscheidung zur Rechtssache *Google Spain* ausführlich aufgegriffen.[135]

Darüber hinaus widmet sich der GV-Vorschlag mit dem vorgesehenen Recht auf Vergessen in besonderer Weise der Informationspermanenz, wobei der Gedanke eines „digitalen Radiergummis" auf *Viktor Mayer-Schönberger* zurückgeht.[136]

Auf nationaler Ebene wurde das Risiko bereits vor der Verbreitung des Internets Gegenstand von Entscheidungen des BVerfG, wobei insbesondere im Volkszählungsurteil die zeitlich unbegrenzte Speicherbarkeit und Abrufbarkeit thematisiert wird.[137]

Charakteristisch für die Informationspermanenz ist in anderen Entscheidungen der Verlust der Flüchtigkeit von Telekommunikation, das Hinterlassen beständiger Spuren[138] sowie die Fixierung von Erscheinungsbildern mit der Möglichkeit der unüberschaubaren Reproduktion.[139] Eine solche Fixierung ermöglicht die Rekonstruktion von individuellem Verhalten.[140] In den Literaturkonzepten wird die Informationspermanenz bei *Roßnagel* behandelt.[141] Er spricht von einer gesellschaftlichen Entlastungsfunktion des Vergessens.[142] *Mallmann* thematisiert das Risiko unter dem Aspekt der Rollenfixierung: Der Einzelne komme von seiner Vergangenheit nicht los.[143]

Maßgeblich für das Risiko sind die Faktoren Digitalisierung, Speicherkapazität, Dezentralität und Redundanz der Speicherungen im Internet.[144] Die dadurch erreichte Ausfallsicherheit der verwendeten Systeme bringt die Schwierigkeit – in bestimmten Fällen auch die praktische Unmöglichkeit – der Löschung von Daten mit sich. Insbesondere bei Persönlichkeitsverletzungen kann dies zu einer Perpetuierung des Schadens führen. Ein gutes Beispiel zur Illustration des Permanenzrisikos ist der sogenannte „Streisand-Effekt". Der Versuch, eine Fotografie des Anwesens von *Barbara Streisand* entfernen zu lassen, führte zu gesteigerter öffentlicher

---

133 Siehe oben Teil 1, IV.B.3.
134 Siehe oben Teil 2, II.B.2.e).
135 Siehe oben Teil 2, II.B.2.d).
136 Siehe oben Teil 2, III.F.2.a).
137 Siehe oben Teil 3, II.B.3.a) und 4.
138 Siehe oben Teil 3, II.B.4.
139 Siehe oben Teil 3, II.B.6.a).
140 Siehe oben Teil 3, II.B.8.
141 Siehe oben Teil 3, III.C.2.b) sowie III.D.2.a).
142 Siehe oben Teil 3, III.D.2.a).
143 Siehe oben Teil 3, III.E.2.a).
144 Siehe oben Teil 2, III.F.2.a).

Aufmerksamkeit, als deren Folge das Foto mittlerweile überall verfügbar ist und es sogar einen entsprechenden Eintrag auf Wikipedia (inklusive Abbildung des Anwesens) gibt.[145] Die Löschung der Daten wird dadurch praktisch unmöglich. Die Permanenz der Informationen erhöht das Risiko von Missbräuchen auf der zeitlichen Ebene und führt bei persönlichkeitsverletzenden Informationen zu einer Schadensvertiefung. Aus soziologischer Perspektive spricht *Gräf* hier von einer „Verewigung" und betont die Vereitelung der Chance von Neuanfängen als maßgebliche Gefahr.[146] *Spindler* weist in seinem DJT-Gutachten auf die Permanenz von Informationen durch Archivierungsdienste im Internet hin.[147] Eine weitere Differenzierung der Informationspermanenz findet sich in der Risiko-Studie von ENISA, in der die Permanenz der Informationen als *life-logging* den Aufhänger für die Identifikation von Folgerisiken darstellt.[148]

Probleme wirft das Risiko der Informationspermanenz somit insbesondere durch die bis zur Unmöglichkeit reichende Schwierigkeit der Löschung von im Internet veröffentlichten Informationen auf. Neben einer bisher nicht absehbaren technischen Lösung bietet es sich deshalb an, das Problem nicht auf Ebene der Daten, sondern der Informationswirkungen anzugehen. In einem Exkurs wurde oben deshalb der Gedanke der *Informationsverjährung* entwickelt: Dem Einzelnen sollte grundsätzlich das Recht gegeben werden, Entscheidungen mit auf ihn bezogener Regelungswirkung abzuwehren, soweit die dafür benutzten Informationen derart veraltet sind, dass deren Verwendung den Rechtsfrieden gefährden würde.[149]

### 5. Entkontextualisierung

Die Relevanz des Kontexts einer Information wurde insbesondere durch eine prägnante Aussage im Volkszählungsurteil publik, wonach es unter den Bedingungen automatischer Datenverarbeitung kein belangloses Datum mehr gebe.[150] Die dieses Phänomen aufgreifende Vorstellung einer normativen Zweckbegrenzung von Daten hat Eingang in zahlreiche der untersuchten Konzeptionen gefunden und verweist auf das Risiko von negativen Auswirkungen, die dem Individuum bei der Übertragung von Informationen aus einem Lebensbereich in einen anderen entstehen können (Entkontextualisierung).[151] Die Rechtsprechung des BVerfG widmete sich dem Risiko bereits frühzeitig im *Scheidungsaktenbeschluss*, wo die in den Fäl-

---

145 http://de.wikipedia.org/wiki/Streisand-Effekt [Stand: 28.3.2014].

146 *Gräf*, Privatheit und Datenschutz, S. 221–231; hinsichtlich des „Neuanfangproblems" vgl. *Gridl*, Datenschutz, S. 26 f.

147 *Spindler*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen, F 15.

148 ENISA (Hrsg.), Life-logging-Studie.

149 Siehe oben Teil 1, IV.3.a), b).

150 Siehe oben Teil 3, II.B.3.c).

151 Siehe oben Teil 1, II.A.2.d); Teil 2, III.A.2.b); E.2.

len der Entkontextualisierung häufig zugrunde liegende These einer Übertragbarkeit der Verhaltensmaximen vom Privat- auf das Berufsleben (in Anlehnung an *Gräf* könnte hier von einem „Konsistenzzwang" gesprochen werden)[152] explizit infrage gestellt wurde.[153] Das Volkszählungsurteil geht indes bei genauerer Betrachtung weniger auf das Risikopotenzial des Kontexts als auf dessen Rolle bei der Bildung der Rechtfertigungsmaßstäbe für zwangsweise Informationserhebungen ein.[154] Auch in der *Caroline*-Entscheidung wird das Risiko der Entkontextualisierung nur mittelbar aufgegriffen.[155] Der dort beschriebene Kontextwechsel zur Medienöffentlichkeit deutet eher auf das Risiko von Schamgefühl und Publizitätsschäden hin.[156]

Konzeptionen auf internationaler und unionsrechtlicher Ebene verweisen stärker auf das Entkontextualisierungsrisiko und ermöglichen diesbezüglich eine weitere Systematisierung: Am Beispiel von Informationen mit Bezug zu Strafverfahren lässt sich zeigen, dass nicht nur die unmittelbaren Folgen der bereichsübergreifenden Informationsübernahme nachteilig sein können, sondern gerade auch die Nichtübernahme bestimmter Informationen, wie beispielsweise zur Glaubwürdigkeitsbeurteilung von Zeugenaussagen im (ggf. internationalen) Informationsaustausch.[157] Diese Risikokonzeption wird auch durch die aktuellen Reformvorschläge auf europäischer Ebene aufgegriffen.[158] Das Risiko von Entkontextualisierungen lässt sich deshalb in zwei Untergruppen einteilen.

#### *a) Kontextdefizit*

Die aus den Strafverfahrensdaten hergeleitete Untergruppe lässt sich als Kontextdefizit beschreiben: Der Schaden liegt dabei gerade in der Nichtübernahme von Informationen aus einem Lebensbereich in einen anderen.[159] Neben dem Strafverfahrenskontext lässt sich der Rechtsprechung des EGMR ein weiteres Beispiel entnehmen: So wurde etwa in der Entscheidung *Lundvall gegen Schweden* eine Information der Steuerbehörden im privatrechtlichen Kontext für eine nachteilige Kreditwürdigkeitsbeurteilung herangezogen, wobei allerdings der Umstand der Einlegung eines Rechtsmittels gegen den Akt der Steuerbehörden nicht berücksichtigt wurde.[160]

---

[152] *Gräf*, Privatheit und Datenschutz

[153] Siehe oben Teil 3, II.B.1.

[154] Siehe oben Teil 3, II.B.3.c).

[155] Siehe oben Teil 3, II.B.6.a).

[156] Siehe oben II.B.2.

[157] Siehe oben Teil 1, II.B. sowie Teil 2, III.G.2.a).

[158] Siehe oben Teil 2, III.G.2.a).

[159] Siehe oben Teil 1, II.B; zu einer ähnlichen Konzeption auf Makro-Ebene vgl. *Tinnefeld/Schmale*, MMR 2011, 790.

[160] Siehe oben Teil 1, IV.B.2.

Das Risiko des Kontextdefizits ist ohne weiteres plausibel und lässt sich aus einem übergreifenden Standpunkt auch an gesellschaftlichen Veränderungen verdeutlichen: Die Entwicklung von der Dorfgemeinschaft zur industriell-bürokratischen Massengesellschaft (*Forsthoff*) führt nach *Ehmann* dazu, dass der Mensch nur noch in Teilaspekten gekannt werden konnte. Isolierte Informationen können in weiten Wirkungsräumen größeren Schaden anstiften, da sie im Fall der Fehlerhaftigkeit nur schwer richtigzustellen sind und im Fall des Zutreffens nicht durch bekannte andere Aspekte der Persönlichkeit, beispielsweise als „einmalige schlimme Sache" bzw. als „persönlichkeitsfremder Ausrutscher", erkennbar werden. Dagegen ist eine engere Gemeinschaft stärker dazu in der Lage, Fehlverhalten durch „Mitleid und Liebe" zuzudecken.[161] Neben dieser zutreffenden Schlussfolgerung, die *Ehmann* bereits 1988 formulierte, stellt sich mittlerweile jedoch die Frage, ob die Entwicklung von der industriell-bürokratischen Massengesellschaft zur heutigen Informationsgesellschaft eine Chance auf Minderung des Risikos von Kontextdefiziten durch die Masse und Verfügbarkeit auch privater Daten ermöglicht. In genau diesem Zusammenhang sind die oben dargestellten Ideen der *post privacy*-Vertreter[162] zu sehen. Leider werden die anderen Risiken durch deren einseitige Verklärung der positiven Seiten der Informationsverfügbarkeit ausgeblendet.

### *b) Kontextinfiltration*

Die zweite Untergruppe der Entkontextualisierung lässt sich als „Kontextinfiltration" beschreiben. Der Begriff „Infiltration" bringt dabei das bereichsübergreifende „Einsickern" bzw. „Eindringen" von Informationen gut zum Ausdruck.[163] Eine Kontextinfiltration liegt dementsprechend bei der bereichsübergreifenden Nutzung von Informationen vor.[164] Nachteilige Effekte können hierbei insbesondere aus der überraschenden Wirkung und fehlenden Kontrollierbarkeit der Verwendung folgen. Der Sachverhalt der EGMR-Entscheidung *Lupker gegen Niederlande* (Verwendung von Führerscheinbildern für Strafermittlungen) lässt sich in diese Gruppe einordnen, wobei das Risiko dort entsprechend einer sphärenartigen Konzeption aufgrund des Öffentlichkeitsbezugs normativ nicht aufgegriffen wurde.[165] In den Literaturkonzeptionen wird die Kontextinfiltration in die Nähe der noch zu besprechenden Profilbildungen gerückt.[166] *Mallmann* weist darauf hin, dass durch die Übertragbarkeit von Informationen zwischen verschiedenen Bereichen auch Ver-

---

161 Zum Ganzen *Ehmann*, AcP 188 (1988), 245.

162 Siehe oben Einleitung, II.

163 *Munzinger/Duden*, Online-Ausgabe, „Infiltration".

164 Siehe oben Teil 1, II.B.

165 Siehe oben Teil 1, IV.B.2.

166 Siehe oben Teil 3, III.C.2.c).

haltensanforderungen aus dem jeweiligen Bereich in einen anderen übernommen werden könnten; Missverständnisse wirkten sich zulasten der Betroffenen aus.[167]

Die Kontextinfiltration stellt damit eines der typischen Informationsrisiken dar, das insbesondere durch die Regelungen zur normativen Zweckbegrenzung Gegenstand zahlreicher untersuchter Risikokonzeptionen wurde. Mit der zunehmenden Vernetzung und Kompatibilität von Informationen wird es zunehmend ineffizienter, Informationen in nur begrenzten Kontexten zu verwenden, da durch die multifunktionale Verwendung Informationserhebungskosten und Zeit (Transaktionskosten) eingespart werden können. Entsprechende Systeme sollten gleichwohl das Risiko der Entkontextualisierung berücksichtigen.

### 6. Informationsemergenz

Das Risiko der Informationsemergenz bezeichnet die Möglichkeit, aus verschiedenen Informationen automatisiert neue, bislang nicht vorhandene Rückschlüsse zu gewinnen.[168] Auch wenn dies ein Merkmal vieler Informationsverarbeitungen ist, lässt sich die Risikohaftigkeit dieses Effekts aus den untersuchten Konzeptionen näher bestimmen: Auf Ebene der Datenschutzkonvention[169] und in der Rechtsprechung des EGMR[170] werden in diesem Zusammenhang Gendaten aufgegriffen. Biometrische Daten fallen ebenfalls darunter. Bei beiden Datenkategorien liegt die Möglichkeit „überschießender" Informationsgewinne im Rahmen weiterer Abgleiche besonders nahe: So ermöglichen biometrische Informationen die Personalisierung von Bilddaten, die wiederum – beispielsweise bei Abgleich mit Daten sozialer Netzwerke – den Aufenthaltsort zu bestimmten Zeiten oder bestimmte politische Einstellungen offenbaren können. Im Fall der Gendaten lassen sich Informationen zu Verwandtschaftsverhältnissen, Erbkrankheiten oder genetisch bedingten (unterstellten) Verhaltensmustern gewinnen.

In der Rechtsprechung des BVerfG verdeutlicht das Volkszählungsurteil das Risiko der Informationsemergenz durch Kombinationsmöglichkeiten. Bei näherer Analyse der Entscheidungsgründe hat sich die Nähe dieser Risikogruppe zur Entkontextualisierungsfallgruppe gezeigt: Die im Urteil argumentationsleitende Betroffenenangst wird insbesondere durch die schwierige Kontextimplementation und Problemantizipation im Rahmen von Programmierungsprozessen ausgelöst.[171] Eine ähnliche Risikokonstruktion liegt auch der Rasterfahndungsentscheidung zugrunde.[172] Auch die IP-Adresse ermöglicht überschießende Informationsgewinnung

---

[167] Siehe oben Teil 3, III.E.2.e).
[168] Siehe oben Teil 1, II.A.2.d).
[169] Siehe oben Teil 1, II.A.2.d).
[170] Siehe oben Teil 1, IV.B.8.
[171] Siehe oben Teil 3, II.B.3.a).
[172] Siehe oben Teil 3, II.B.3.e).

durch Kombination mit Verbindungsdaten und – im Fall der IPv6 – eindeutigen Gerätedaten besonders gut, wobei hier insbesondere der Zusammenhang zum Risiko der Informationspermanenz charakteristisch ist.[173] In der Literaturkonzeption von *Britz* wird dieses Risiko ähnlich wie beim Volkszählungsurteil im Zusammenhang mit statistischen Daten aufgegriffen.[174]

Das Risiko hat in letzter Zeit insbesondere durch die Entwicklungen, die mit dem Begriff *big data* beschrieben werden, an Relevanz gewonnen. Darunter versteht man „die Analyse großer Datenmengen aus vielfältigen Quellen in hoher Geschwindigkeit mit dem Ziel, wirtschaftlichen Nutzen zu erzeugen".[175] Dies ermöglicht eine ganze Reihe erheblicher wirtschaftlicher Vorteile.[176] Probleme des *big data* kreisen insbesondere um die einfachgesetzlich vorgesehenen Erforderlichkeitsvoraussetzungen, die Einwilligung und die Befürchtungen unkontrollierter Überwachung.[177] Die Enthüllungen um die Überwachung durch die NSA unterstreichen diese Problematik besonders eindringlich.

Das Risiko der Informationsemergenz wird dabei auch in der außerrechtlichen Privatheitsforschung aufgegriffen. Zu nennen sind etwa die Versuche, von Twitter-Nachrichten auf psychische Erkrankungen[178] oder aus Facebook-Profilen auf die sexuelle Orientierung und Intelligenz zu schließen.[179] Eine Studie der Carnegie Mellon Universität verdeutlicht das Risiko der Informationsemergenz und weist auf die Möglichkeit der Rekonstruktion der in den Vereinigten Staaten von Amerika besonders sensiblen Sozialversicherungsnummern aus verschiedenen anderen Daten unter Einsatz von Gesichtserkennungssoftware hin.[180]

### 7. Informationsfehlerhaftigkeit

Ein Risiko, das sich vor allem aus unkontrollierten und intransparenten Verarbeitungsvorgängen ergeben kann, liegt in der Informationsfehlerhaftigkeit. Bereits in der Datenschutzkonvention wird es zusammen mit dem Prinzip der sachlichen Richtigkeit der Daten aufgegriffen.[181] Präsent ist es insbesondere auch auf unions-

---

173 Siehe oben Teil 3, II.B.8.

174 Siehe oben Teil 3, III.B.2.c).

175 BITKOM (Hrsg.), Big Data, S. 7.

176 Vgl. ebd., S. 15 sowie die Einsatzbeispiele S. 51 ff.

177 Ebd., S. 10.

178 *Sumner/Byers/Boochever/Park*, Predicting Dark Triad Personality Traits from Twitter usage and a linguistic analysis of Tweets, 2012, https://www.onlineprivacyfoundation.org/research_/Sumner_Predicting_Dark_Triad_Traits_from_Twitter_Usage_V5.pdf [Stand: 28.3.2014].

179 *Kosinski/Stillwell/Graepel*, 110 PNAS 15 (2013), 5802.

180 *Hoffmann-Riem*, in: ders. (Hrsg.), Offene Rechtswissenschaft, S. 546.

181 Siehe oben Teil 1, A.2.d).

rechtlicher Ebene.[182] Ein für die Fehlerhaftigkeit relevanter Ursachenkomplex sind „Datenverfälschungen", insbesondere durch Schadprogramme, die in der E-Kom-Richtlinie[183] und in der Rechtsprechung des BVerfG dem Schutzgut der Integrität zugeordnet werden.[184] In der Literatur wird von *Britz* das Risiko der Fehlerhaftigkeit von Informationen vor allem mit Massenvorgängen in Zusammenhang gebracht.[185] *Mallmann* weit auf die Möglichkeit der Präjudizwirkung fehlerhafter Informationen hin.[186]

Das Risiko der Informationsfehlerhaftigkeit und von Datenverfälschungen liegt beim Einsatz von Schadsoftprogrammen besonders nahe. Es stellt insoweit ein übergreifendes Risiko dar, als die Gründe für die Fehlerhaftigkeit vielfältig sein können. Ein Teilbereich ist dabei bereits vom Risiko des Kontextdefizits umfasst, das gerade aus dem Phänomen der mangelhaften Implementierung des Informationskontexts, insbesondere bei Massenvorgängen, resultieren kann. Die Verringerung fehlerhafter Informationen kann dabei vor allem durch Einbindung der Betroffenen sowie durch Kontroll- und Löschungsrechte erreicht werden.

## C. Makro- und Mikroebene: Risiken für Gesellschaft und Individuum

Neben den Risiken auf struktureller und individueller Ebene lassen sich in den untersuchten Konzeptionen auch solche identifizieren, die in etwa gleichem Maße Makro- und Mikroebene betreffen. Diese wurden zum Teil bereits bei den jeweiligen Ebenen in bestimmten Teilaspekten thematisiert, gewinnen ihr charakteristisches Risikopotenzial jedoch gerade in der Verbindung der Ebenen.

### 1. Behandlung des Menschen als bloßes Objekt

Die Verletzung der Menschenwürde ist eines der schwerwiegendsten Risiken, welche datenschutzrechtliche Konzeptionen in bestimmten Konstellationen aufgreifen. Die hierzu behandelten Fallgruppen stellen aufgrund der Eigenschaft der Menschenwürde als gemäß Art. 1 Abs. 1 GG oberstem (abwägungsfestem) Verfassungswert und tragendem Konstitutionsprinzip[187] ein besonderes Problem dar. Dabei spiegelt bereits die Dogmatik zu Art. 1 Abs. 1 GG die spezifische Kombination aus Makro- und Mikroebene: Die Menschenwürde lässt sich als „anthropo-

---

182 Siehe oben Teil 2, II.B.2.e) und III.A.2.b).

183 Siehe oben Teil 2, III.C.2.b).

184 Siehe oben Teil 3, II.B.15.a).

185 Siehe oben Teil 3, B.2.c).

186 Siehe oben Teil 3, E.2.e).

187 Statt vieler Epping/Hillgruber-*Hillgruber*, Art. 1 Rn. 1.

zentrische Relativierung des Staates“ durch den „Achtungsanspruch des selbstbestimmten Individuums“ nach Maßgabe einer „personalen Staatsidee“ verstehen.[188] Das Risiko ist deshalb sowohl der Makro- als auch Mikroebene zuzuordnen.

Die Konzeptionen greifen die „Verobjektivierung des Menschen“ und damit die „Objektmachung“, die der auf *Kant* zurückzuführenden[189] Formel der Menschenwürde zugrunde liegt, zunächst bei Regelungen auf, die sich gegen ausschließlich automatisierte Einzelentscheidungen richten.[190] Diese Konzeptionen, die auch Eingang in die aktuellen Reformentwürfe auf unionsrechtlicher Ebene gefunden haben,[191] gehen von der Prämisse aus, dass Entscheidungen, die ohne Einschaltung eines Menschen allein von Maschinen getroffen werden – sofern sie nicht ausschließlich vorteilhaft für den Betroffenen sind – mit der Menschenwürde unvereinbar sind. Es handele sich hierbei um eine „Herabdegradierung“ des Menschen zum „Objekt einer Computeroperation“.[192]

Auf europäischer Ebene werden die Gefahren über besondere Verarbeitungsthemen konkretisiert; die Regelungen richten sich damit insbesondere gegen ausschließlich automatisierte Entscheidungen bei Einstellungen, Prüfungen von Kreditwürdigkeit, Zuverlässigkeitsprüfungen.[193] Sicherzustellen sei die Letztentscheidung durch einen Menschen, womit das Risiko der Verantwortungsnegation[194] einbezogen wird. Der GV-Vorschlag bezieht die Themen Gesundheit und persönliche Vorlieben ein und verwendet für die rein automatisierten Abläufe den Überbegriff „Profiling“, wobei insbesondere internetbasierte Verfahren angesprochen werden.[195] Im *Mikrozensus*-Urteil des BVerfG wird herausgestellt, dass Menschen nicht wie Sachen einer „Bestandsaufnahme in jeder Beziehung“ zugänglich gemacht werden dürfen. Sie dürften – selbst in einer anonymen statistischen Erhebung – nicht in ihrer ganzen Persönlichkeit zwangsweise registriert und katalogisiert werden. Das Risiko wird als „verwaltungstechnische Entpersönlichung“ umschrieben.[196] Auch das Volkszählungsurteil greift diese Linie unter dem Stichwort „persönlichkeitsfeindlicher Registrierung und Katalogisierung“ auf.[197]

Fraglich erscheint allerdings, ob bereits aus der rein automatisierten Entscheidung als solcher eine Menschenwürdeverletzung folgt. Die Menschenwürde sollte aufgrund ihrer besonderen Wertigkeit und Stellung nicht „zu kleiner Münze“ ver-

---

188 Maunz/Dürig-*Herdegen*, Art. 1 Abs. 1 Rn. 1 und 2.

189 Ebd., Art. 1 Abs. 1 Rn. 12.

190 Siehe oben Teil 1, II.A.2.b) und d) sowie Teil 2, III.A.2.c).

191 Siehe oben Teil 2, F.2.c).

192 Siehe oben Teil 2, III.A.2.c).

193 Siehe oben Teil 2, III.A.2.c).

194 Siehe oben II.A.1.c).

195 Siehe oben Teil 2, F.2.c).

196 Siehe oben Teil 3, II.B.1. Vgl. auch *Ehmann*, AcP 188 (1988), 305.

197 Siehe oben Teil 3, II.B.3.c).

arbeitet werden, weshalb für den Rückgriff auf sie nicht allein der – wertfreie – Umstand des Einsatzes moderner Techniken zur Vereinfachung von Massenverfahren ausreichen sollte. Eine „Herabwürdigung des Menschen zum Informationsobjekt“[198] kann in der Informationsgesellschaft nicht bereits aus dem Technikeinsatz als solchem folgen. Hinzukommen muss noch ein außerhalb des bloßen Technikeinsatzes liegendes „Umstandsmoment“. Ein solches wäre z.B. im Fall eines automatisierten Scoringverfahrens zur Todeswahrscheinlichkeit auf Intensivstationen gegeben.[199] Hier liegt es auf der Hand, dass die Ressourcenverteilung, sofern Menschenleben davon abhängen, nicht allein automatisiert erfolgen kann. Dabei besteht eine besondere Nähe zum Risiko der Verantwortungsnegation.[200]

Auch im Rahmen des Strafverfahrens erscheint die Menschenwürderelevanz besonders naheliegend. Der Einsatz bestimmter Überwachungstechnologien und ggf. deren Kumulation[201] legen den Rückfall in ein quasi-inquisitorisches Verfahren nahe, da bestimmte Technologien die Selbstüberführung praktisch unausweichlich machen können. Mit dem Einsatz und der Kombination derartiger Technologien kann ein Zustand hergestellt werden, der demjenigen vor Einführung des reformierten Strafprozesses ähnelt. Dort war der Beschuldigte bloß materielles Beweisobjekt. Sein Geständnis (Selbstüberführung) galt es mit allen Mitteln zu erreichen. Heute kann der Technikeinsatz – wie beispielsweise die Enthüllungen um die NSA-Überwachungen zeigen – die Selbstüberführung unausweichlich machen und den Beschuldigten gerade dadurch zum Verfahrensobjekt degradieren.[202]

## 2. Exkurs: „Persönlichkeitsprofil“

In engem Zusammenhang mit dem Risiko von Verletzungen der Menschenwürde steht die Bildung von Persönlichkeitsprofilen. Der Topos „Persönlichkeitsprofil“ wird bereits auf international-rechtlicher Ebene mit den Empfehlungen des Europarats zum „Profiling“ aufgegriffen. Das Profiling wird dort als Anwendung einer kategorial-charakterisierenden Gruppe von Daten auf bestimmte Individuen verstanden.[203] Während auf Ebene der Datenschutzrichtlinie (RL 95/46/EG) der Begriff noch wegen seiner Unschärfe kritisiert wurde,[204] wird das Profiling im GV-Vorschlag als Oberbegriff für rein automatisierte Einzelentscheidungen verwendet

---

198 *Benda*, in: Leibholz/Faller/Mikat (Hrsg.), FS Geiger, S. 27, vgl. auch S. 39 f.

199 Beispiel nach *Trute*, JZ 1998, 829, Fn. 85.

200 Siehe oben II.A.1.c).

201 Zur Überwachungskumulation vgl. oben Teil 3, II.B.12.

202 Allgemein zu dieser These vgl. *Bosch*, zit. nach *Mahlstedt*, Verdeckte Befragung, S. 229, Fn. 410.

203 Siehe oben Teil 1, II.C.

204 Teil 2, III.A.2.c).

und auch im RL-Vorschlag aufgegriffen.[205] Auf Ebene der Rechtsprechung des EuGH wird das Profiling im Zusammenhang mit Fluggastdaten, also bei der Verwendung privater Daten durch staatliche Stellen, thematisiert.[206] Im Kontext sozialer Netzwerke verwendet es die Art.-29-Arbeitsgruppe.[207] Während sie im Volkszählungsurteil lediglich Argumentationstopos sind,[208] werden „Persönlichkeitsprofile" in verschiedenen anderen Entscheidungen des BVerfG in Zusammenhang mit den Risiken von Entkontextualisierung, Informationspermanenz und Informationsemergenz gebracht, wobei die Rekonstruierbarkeit, die Kombination verschiedener Daten und Techniken (Informationskonvergenz), typisch für die Beschreibung des Profilbildungsrisikos ist.[209]

Teilweise wird das Merkmal der Lückenlosigkeit der Überwachung bzw. der Kumulation verschiedener Überwachungstechniken als Merkmal für Menschenwürdeverletzungen durch Profile beschrieben.[210] In den Literaturkonzeptionen lässt sich das Profiling *Albers'* zweiter Ebene zuordnen. Bei *Britz* wird – in Anlehnung an die Rechtsprechung des BVerfG – das Erfordernis eines großen Umfangs an Informationen herausgestellt.[211] Ausführlicher widmet sich das Reformgutachten von *Roßnagel* u.a. den Persönlichkeitsprofilen, wobei dort der Schwerpunkt auf die wirtschaftliche Verwendung von Daten zur Einschätzung von Kaufkraft und Kreditwürdigkeit gelegt wird. Die meisten Profilbildungen werden von ihm dann jedoch mangels Eingriffsintensität für nicht verfassungswidrig erachtet. Die Definition der Profilbildung zeigt die Nähe zur Informationsemergenz: Maßgeblich sei das Gewinnen neuer unbekannter Informationen und das Zusammenführen von Abbildern der Persönlichkeit.[212]

Der risikohafte Teil des Topos „Persönlichkeitsprofil" lässt sich damit dem Risiko von Menschenwürdeverletzungen zurechnen und wird für umfangreiche und besonders aufschlussreiche Sammlungen personenbezogener Daten verwendet. Es handelt sich gleichwohl nicht um ein eigenständiges Risiko, sondern vielmehr um einen Argumentationstopos, da die Charakteristiken bereits anderen Risiken (neben den Menschenwürdeverletzungen sind dies Informationspermanenz, Informationsemergenz, Verantwortungsnegation und Entkontextualisierung, bei bestimmter Profilkonstruktion auch Selektivitätsschäden) zugeordnet werden können.

---

205 Siehe oben Teil 2, III.F.2.c), G.1.

206 Siehe oben Teil 2, II.B.2.d).

207 Teil 2, III.A.2.a).

208 Siehe oben Teil 3, II.B.3.a).

209 Siehe oben Teil 3, II.B.3.a) sowie 8. und, nur am Rande, dagegen 17.

210 Siehe oben Teil 3, II.B.11.; 12.

211 Siehe oben Teil 3, III.A.2.c) sowie B.2.c).

212 Siehe oben Teil 3, III.C.2.c).

### 3. Fremdbestimmung

Ein weiteres Risiko, das sich sowohl der Makro- als auch Mikroebene zuordnen lässt, ist das der Fremdbestimmung. Auf der individuellen Ebene können personenbezogene Daten zur Manipulation des individuellen Verhaltens eingesetzt werden, z.B. zu Erpressungen mit belastendem Fotomaterial. Es lässt sich insoweit auch der individuellen Verletzlichkeit zuordnen. Auf der Makroebene können sich diese Manipulationen bei hinreichender Häufung und bestimmter politischer Ausrichtung – folgt man der Konformitätsthese[213] – negativ auf demokratische Prozesse auswirken. Das Risiko verweist insoweit auf die oben dargestellten konformistischen Verhaltensanpassungen auf gesellschaftlich-politischer Ebene.[214] Dass es bereits sehr früh vom Datenschutzrecht aufgegriffen wurde, zeigen nicht nur die allgemeinen Regelungskonzeptionen auf internationaler und unionaler Ebene,[215] sondern auch die Schutzgutkonzeptionen, die auf informationeller Selbstbestimmung als Gegenstück zum Risiko von Fremdbestimmungen aufbauen.

### 4. Enttäuschung von Vertraulichkeitserwartungen

Bereits auf der Makroebene wurden die übergreifenden Aspekte gesunkenen (Verbraucher-)Vertrauens mangels wirksamen Datenschutzes diskutiert.[216] Die Enttäuschung von Vertraulichkeitserwartungen stellt jedoch zudem ein Querschnittsrisiko dar, da es sich auch auf individueller Ebene auswirkt. Dabei sind nicht nur die individuell nachteiligen Folgen der Nichtinanspruchnahme medizinischer Dienstleistungen, bestimmter Beratungsleistungen[217] und sonstiger Verhaltensoptionen[218] relevant.

Das Risiko weist darüber hinaus auch in seiner dogmatischen Ausgestaltung in den untersuchten Konzeptionen eine besondere Verknüpfung von individueller und struktureller Ebene mit dem Konzept der berechtigten Vertraulichkeitserwartung („reasonable expectation of privacy“) auf. Nach dieser Rechtsfigur, die in der US-amerikanischen Rechtsprechung zum vierten Zusatzartikel der Bundesverfassung entwickelt wurde, ist zunächst zu prüfen, inwieweit eine nach außen kenntlich gemachte subjektive Vertraulichkeitserwartung bestand. In einem zweiten Schritt wird nach der „Berechtigung“ bzw. „Vernünftigkeit“ dieser Erwartung aus Sicht der Gesellschaft gefragt.[219] Diese Rechtsfigur wurde vielfach auf internationaler,

---

213 Siehe oben A.1.b).

214 Ebd.

215 Siehe oben Teil 1, II.A.2.d); III.A.2.b); C.2.d).

216 Siehe oben II.A.2.b).

217 Siehe oben Teil 1, IV.B.5.

218 Zu möglichen Verhaltensauswirkungen bei Gentests vgl. *Margulis*, 59 Journal of Social Issues 2 (2003), 252.

219 Siehe oben Teil 1, IV.B.5.; vgl. auch *Harper/Spies*, Reasonable Expectation, S. 33.

unionaler und nationaler Ebene rezipiert.[220] Dabei zeigen sich zwei Möglichkeiten der Konkretisierung des „normativen" zweiten Schritts der Prüfung: Einerseits kann an das tatsächlich-rechtliche Umfeld in der jeweiligen Gesellschaft angeknüpft werden, wie beispielsweise an die extensiven Regelungen zur Informationsfreiheit in den skandinavischen Ländern.[221] Andererseits können bestehende (thematische) Spezialgrundrechte herangezogen werden und so eine dogmatisch geschlossenere Konkretisierung erfolgen.[222] Im letzteren Fall muss jedoch besonderer Wert darauf gelegt werden, dass der Schutz auch für neue Technologien offen ist.

Der Komplex Internetüberwachung und die hierzu bestehende verfassungsrechtliche Rechtsprechung ist ein Beispiel für einen Bereich, in dem durchaus mit der Vertraulichkeitserwartung als Rechtsfigur operiert werden kann, wobei nicht vorschnell von der (Teil-)Öffentlichkeit bestimmter Informationen auf die Absenz einer vernünftigen Vertraulichkeitserwartung geschlossen werden darf. Das Risiko von täuschungsbedingten Infiltrationen sozialer Netzwerke ist ein gutes Beispiel für einen Sachverhalt, in dem unter bestimmten Umständen berechtigte Vertraulichkeitserwartungen bestehen und der bislang noch nicht hinreichend rechtswissenschaftlich aufgearbeitet wurde. Während sich im nicht virtuellen Raum die rechtliche Anerkennung von Vertraulichkeitsenklaven auch in öffentlichen Bereichen immer stärker durchgesetzt hat, steht der Durchbruch dieser – hier befürworteten Sichtweise – für den virtuellen Raum noch bevor.[223] Dabei kann auch nicht allein aus faktischer Überwachungstätigkeit – wie sie etwa im Zuge der NSA-Überwachungen bekannt wurde – auf die Unvernünftigkeit von Vertraulichkeitserwartungen geschlossen werden, da es sich bei der „Vernünftigkeit" um einen wertend auszulegenden normativen Rechtsbegriff handelt. Andernfalls wäre der Schutzgehalt umso geringer, je stärker die Überwachungstätigkeit ausgeprägt ist.

## D. Grenzfälle und Nicht-Risiken

In den untersuchten Konzeptionen wurden eine Reihe von Informationsverarbeitungen aufgegriffen, bei denen prima facie nicht klar ist, ob es sich dabei wirklich um Risiken handelt, oder um bloß „mitgeregeltes", im Einzelfall womöglich lästiges, jedoch nicht schädigendes Verhalten. Hierunter fallen insbesondere kommerzielle Datenverarbeitungen. Dabei darf allerdings nicht übersehen werden, dass auch dabei Informationen gewonnen werden und diese – etwa im Fall mangelhafter Datensicherheit oder bei staatlichem Zugriff auf die Daten – wiederum eine der

---

220 Siehe oben Teil 1, IV.B.6.; Teil 2, II.B.2.e); Teil 3, III.B.2.c), d); B.2.c), d); E.2.b).

221 Siehe oben Teil 2, II.B.2.e).

222 Siehe oben Teil 3, II.B.7.

223 Siehe oben Teil 3, II.B.15. und 16; vgl. auch *Drackert*, eucrim 2011, 122 ff.

oben bereits besprochenen Risikokategorien auslösen können, z.B. die Kontextinfiltration bei staatlicher Nutzung oder die individuelle Verletzlichkeit. Notwendig ist dann jedoch ein Zwischenschritt, der es fraglich erscheinen lässt, bereits die kommerzielle Nutzung als eigenständiges Risiko und damit regulatorischen Anknüpfungspunkt für Verbote zu wählen. Bevor dies zu diskutieren ist, müssen die kommerziellen Informationsverarbeitungen weiter unterteilt werden.

Als Ausgangspunkt lassen sich die von *Lüke* in einem Sammelband der bpb vorgeschlagenen sechs nachteiligen Konsequenzen kommerzieller Datenverarbeitung nennen, die er im Zusammenhang mit der Forderung nach einer Ausweitung der Zustimmungslösung (Opt-in) bei kommerziellen Datenverarbeitungen bespricht.[224] Die von ihm dargestellten Fallgruppen sind: die ausschließliche Möglichkeit von Nachnahmezahlung im Versandhandel, die Verweigerung von Handyverträgen, die Verweigerung oder Verteuerung von Krediten, Ablehnung von Versicherungsabschlüssen, gezielte Internetwerbung und Differenzierung bei Spendenanfragen. Diese Liste kann erweitert werden um ungewünschte Postwurfsendungen und die Einblendung zielgruppenorientierter Bannerwerbung auf besuchten Internetseiten. Fraglich ist bei allen Fallgruppen, ob mit ihnen tatsächlich rechtspolitisch zu missbilligende individuelle Nachteile einhergehen. Aus datenschutzrechtlicher Sicht lassen sich die Verarbeitungen in drei Untergruppen der kommerziellen Informationsverarbeitung aufteilen. Die im Folgenden zu untersuchenden Fallgruppen sind Informationsverarbeitungen 1) zur Werbung und Zielgruppenpräzisierung, 2) zu Forderungsmanagement und Bonitätsprüfungen sowie 3) im Rahmen von Bewerbungsverfahren.

### 1. Werbung und Zielgruppenpräzisierung

In diese Kategorie fällt insbesondere die Informationsverarbeitung für unerbetene Direktwerbenachrichten, zielgruppenorientierte Werbung in Anzeigen, Postwurfsendungen, Werbespots und Banner-/Pop-up-Werbung sowie solche zur Präzisierung von Zielgruppen. Derartige Informationsverarbeitungen werden von den untersuchten Konzeptionen zum Teil aufgegriffen,[225] mitunter sind sie auch als Nicht-Risiko dem bloß lästigen Verhalten zuzuordnen.[226]

Bei ungewünschten Postwurfsendungen oder zielgruppenorientierter Werbung mag eine gewisse Belästigungswirkung vorliegen, da die ungewünschten Sendungen weggeworfen, die leidigen Werbeeinblendungen auf Internetseiten weggeklickt oder mittels einer Einstellung im Browser unterdrückt werden müssen. Darüber hinaus sind jedoch keine unmittelbar mit der kommerziellen Nutzung verbundenen nachteiligen Folgen ersichtlich. Auch intensivere oder umfangreichere kommerziel-

---

[224] *Lüke*, in: Schmidt/Weichert (Hrsg.), Datenschutz, S. 154.

[225] Siehe oben Teil 2, III.C.2.d); Teil 3, C.2.b).

[226] Siehe oben Teil 3, B.2.e); F.2.b).

le Datennutzungen[227] wie im Fall von „behavioral tracking“[228] oder kurioser Zielgruppenmodelle (beispielsweise die Zuordnung zum „prekären“, „traditionellen“ oder auch „adaptiv pragmatischen Milieu“)[229] ändern an der grundsätzlich geringen unmittelbaren Relevanz nichts, da niemand zur Inanspruchnahme der Dienstleistungen und Produkte, deren Vermarktung die Datennutzungen dienen, gezwungen ist. Zugleich steht es dem Verwender frei, seine wirtschaftliche Tätigkeit auf Zielgruppen zu fokussieren. Der Hersteller, der bestimmte Konsumenten von seinem Angebot ausschließt, wird von diesen auch keine Einnahmen erzielen. Er wird dies deshalb nicht leichtfertig tun, weil im Zweifel seine Mitbewerber schon zur Bedienung der Nachfrage bereitstehen. Die Ausscheidung ungewünschter Praktiken kann insoweit durch normale Marktprozesse erfolgen. Im Gegenteil liegen insbesondere Werbung und Produktinformation aufgrund der Konsumwünsche der Verbraucher häufig in deren Interesse und stellen insoweit ein völlig normales, wirtschaftspolitisch wünschenswertes und grundrechtlich durch die Art. 12, 14 sowie 2 Abs. 1 GG geschütztes Verhalten in einem funktionierenden Markt dar.[230] Niemand ist gezwungen, den Kaufempfehlungen der Werbung zu folgen. *Fiedler* verdeutlicht dies am Beispiel von Werbebriefen einer Wirtschaftszeitung und schließt vom Verhältnis der Widerspruchsraten zu positiven Antworten auf ein Überwiegen der Vorteile dieser Werbung.[231]

Auch wenn es schwierig erscheint, in diesem Bereich verallgemeinerungsfähige Aussagen zu treffen, so liegt doch in der kommerziellen Informationsnutzung als solcher (also abgesehen von der möglichen Relevanz anderer, oben besprochener Risikokategorien, insbesondere durch mittelbaren Zugriff des Staates) kein genuin datenschutzrechtliches Problem. Soweit den Werbepraktiken ein besonders hohes Maß an Belästigung zukommt, fallen sie vielmehr in die regulatorische Zuständigkeit des Wettbewerbsrechts, das mit § 7 Abs. 1 UWG eine passende und mit gegenüber dem Datenschutzrecht effizienteren Durchsetzungsmechanismen ausgestattete Abhilfemöglichkeit bereithält.

---

[227] Zum Umfang der Datenverarbeitungen vgl. http://www.tagesspiegel.de/medien/digitale-welt/vernetzung-einzelinformationen-fuer-gezielte-werbestrategien/7223236-2.html [Stand: 28.3.2014].

[228] Vgl. die Beispiele bei *Spindler*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen, F 13 f.; fragwürdig beispielsweise auch die Nutzerüberwachung durch eine Spielekonsole, http://www.spiegel.de/netzwelt/games/microsoft-konsole-xbox-one-kinect-kamera-schafft-datenschutz-probleme-a-900397.html [Stand: 6.7.2013].

[229] Einordnung nach den „Sinus-Milieus“, http://www.sinus-institut.de/de/loesungen/sinus-milieus.html [Stand: 28.3.2014].

[230] Zu den Einstellungen gegenüber Werbung vgl. http://www.bitkom.org/de/presse/74534_71795.aspx [Stand: 28.3.2014].

[231] *Fiedler*, in: Schmidt/Weichert (Hrsg.), Datenschutz, S. 169.

### 2. Bonitätsprüfungen, Forderungsmanagement

Im Gegensatz zu bloßen Belästigungen sind die nachteiligen Konsequenzen im Rahmen von Vertragsabschlüssen, also insbesondere deren Verweigerung oder Verteuerung nach Verarbeitung einschlägiger Informationen über den potenziellen Vertragspartner, durchaus einleuchtend, da sie sich wirtschaftlich beziffern lassen. Auch hierin kann jedoch – isoliert betrachtet – kein zu berücksichtigendes datenschutzrechtliches Risiko liegen, weil die Abschlussfreiheit und privatautonome Setzung von Vertragsmodalitäten einen wesentlichen Bestandteil eines marktwirtschaftlichen Wirtschaftssystems ausmacht (Vertragsfreiheit) und dies im Gegensatz zu planwirtschaftlichen Modellen gerade erwünscht ist. Die Vertragsfreiheit darf deshalb nicht mittelbar durch die Beschränkung der hierfür erforderlichen Informationsverarbeitungsfreiheit unverhältnismäßig beschränkt werden. Bei der Verteuerung oder dem Nichtzustandekommen von Verträgen handelt es sich nicht um ein datenverarbeitungsrechtliches Risiko, sondern um ein allgemeines Lebensrisiko. Die Notwendigkeit der Regulierung kann sich hier allenfalls in begrenzten Wirtschaftsbereichen ergeben, in denen aufgrund der fortwirkenden Effekte eines überkommenen Staatsmonopolismus faktisch noch kein funktionierender Markt besteht und auch ohne Rücksicht auf datenschutzrechtliche Fragen z.T. noch Kontrahierungszwänge bestehen. Zu denken ist hier insbesondere an den Infrastrukturbereich (Strom-, Wärme, Telekommunikation, Nahverkehr).

Im Übrigen ergeben sich Rechtfertigungsansätze für die Beschränkung nicht aus der kommerziellen Verarbeitung als solcher, sondern aus den anderen, oben beschriebenen Risiken, die in bestimmten Fällen – z.B. mangelhafter Datensicherheit oder permanenter Speicherung – mitbetroffen sein können. Als Beispiel für die Ausscheidung der kommerziellen Datenverarbeitung als spezifisch datenschutzrechtliches Risiko mag der von *Lüke* geschilderte Fall des geo scoring[232] bei Versandbuchhändlern dienen: Weshalb sollten diese das Risiko, mit ihren Forderungen auszufallen, nicht durch statistische Verfahren begrenzen und in bestimmten Ortsteilen nur Nachnahmezahlung anbieten? Dem nachteilig betroffenen Kunden steht es frei, einen anderen Versandhändler oder einen stationären Buchhändler zu wählen. Sofern das Scoring unzutreffende Ergebnisse liefert, also der als risikoreich eingeschätzte Kunde in Wirklichkeit ein geringes Ausfallrisiko aufweist, trägt doch gerade der Unternehmer den wirtschaftlichen Schaden, der sich aus dem geringeren Umsatz durch die im Vergleich zu Mitbewerbern oder dem stationären Buchhandel einseitige Zahlungsmöglichkeit ergibt.

---

[232] Zum geo-scoring (an statistischen Wohnortdaten orientiertes Verfahren zur Minimierung kaufmännischer Risiken) statt vieler *Helfrich*, in: Hoeren/Sieber (Hrsg.), Handbuch MMR, Teil 16.4 Rn. 3–29.

### 3. Exkurs: Arbeitsrechtlicher Kontext

Ein von den untersuchten Konzeptionen kaum thematisierter[233] Problemkreis sind Datenverarbeitungen im arbeitsrechtlichen Kontext. Lediglich aus Gründen der Vollständigkeit sollen auch diese Informationsverwendungen hier erwähnt werden, da sie in der Öffentlichkeit umstritten sind und mit den Vorschlägen einer Neuregelung des Arbeitnehmerdatenschutzes[234] auch rechtspolitische Aktualität besitzen. Bei dieser Nutzung von Informationen ist zu differenzieren zwischen Datenverarbeitung im Rahmen der Begründung eines Arbeitsverhältnisses auf der einen Seite und zur Arbeitnehmerüberwachung auf der anderen Seite. Bei der Datenverarbeitung im Rahmen der Begründung von Arbeitsverhältnissen ist insbesondere der von *Britz* angesprochene Fall der Verwendung von Informationen aus sozialen Netzwerken bei Bewerbungsverfahren relevant.[235] Diese Konstellation lässt sich – soweit es sich nicht um ein explizit dem Berufsleben zuzuordnendes Netzwerk handelt – den oben beschriebenen Risiken der Diskriminierung, Informationspermanenz und Entkontextualisierung zuordnen.[236] Daneben werden datenschutzrechtliche Fragen beim Einsatz von Informationstechnologie zur Arbeitnehmerüberwachung aufgeworfen, wobei weiter zwischen der Leistungsüberwachung und der Überwachung aus Gründen der Compliance unterschieden werden kann. Mit beiden Aspekten werden zahlreiche, insbesondere arbeitsrechtliche,[237] strafrechtliche[238] und rechtspolitische[239] Fragen aufgeworfen, deren Klärung über die hier verfolgten Forschungsziele hinausreicht und die einer eigenständigen Untersuchung vorbehalten bleiben müssen.

## III. Folgerungen für mögliche Schutzgüter

Die Konzeptionen beziehen sich trotz der gemeinsamen Zuordnung zum Datenschutzrecht auf eine Vielzahl unterschiedlicher Schutzgüter. Dabei zeigen vor allem die internationalen und unionsrechtlichen Komponenten einen starken Bezug zu den dem Datenschutz eher fernliegenden Schutzgütern des Freihandels und des

---

233 Insoweit nur *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 592 sowie der oben erwähnte Verhaltenscode der ILO, Teil 1, II.G.

234 Zum aktuellen Stand der Reformbestrebungen: http://www.bfdi.bund.de/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Beschaeftigtendatenschutz.html?nn=409756 [Stand: 24.5.2014].

235 *Britz*, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, S. 592; eingehend *Ernst*, NJOZ 2011, 953 ff.

236 Siehe oben II.B.3.a), 4., 5.

237 *Däubler*, in: Schmidt/Weichert (Hrsg.), Datenschutz, S. 188 ff.

238 *Maschmann*, NZA-Beilage 2012, 50 ff.; *Eisele*, Compliance, 2012.

239 *Rex*, ZD-Aktuell 2013, 03565.

Wettbewerbs. Letzteres wird sogar im Rahmen der aktuellen Reformvorschläge mit dem Vorschlag zur Datenportabilität verfolgt.[240] Dabei wandelten sich die vom Binnenmarktgedanken geprägten unionsrechtlichen Konzeptionen seit dem Lissabonner Vertrag zu einem stärkeren genuin datenschutzrechtlichen Konzept. In der deutschen Rechtsprechung und Literatur liegt hingegen der Schwerpunkt auf informationeller Selbstbestimmung, Selbstdarstellung, Menschenwürde und auf der Verhaltensfreiheit. Von besonderer Vielfalt sind die Schutzgüter in der Rechtsprechung des EGMR, wo neben der Vertraulichkeitserwartung auch physische und psychische Integrität sowie soziale Identität geschützt werden. In der Rechtsprechung des EGMR lässt sich darüber hinaus die Flexibilisierung der Schutzgüter nachvollziehen: durch eine Abkehr von der eher starren, abwehrenden Verteidigung bestimmter Intimitäts- und Geheimsphären hin zu einem flexiblen, ortsunabhängigeren Schutz von Vertraulichkeitserwartungen.

Der Vergleich der unterschiedlichen Schutzgutkonzeptionen auf den verschiedenen Ebenen zeigt, dass die aus dem US-amerikanischen Recht stammende Figur der Vertraulichkeitserwartung ein brauchbarer Ansatz ist. Hiermit operiert mittlerweile nicht nur der EGMR, das Schutzgut wird vielmehr auch auf Ebene der EuGH- und BVerfG-Rechtsprechung herangezogen. Die besondere Eignung des Schutzguts „Vertraulichkeitserwartung" ergibt sich daraus, dass es in der Lage ist, Risiken auf verschiedenen Ebenen aufzugreifen. Im Gegensatz zur Selbstbestimmung können durch den Schutz von Vertraulichkeitserwartungen auch gesamtgesellschaftliche Makro-Risiken und über den Umweg des Verbrauchervertrauens sogar wirtschaftliche Aspekte einfließen. Das bedeutet zwar nicht, dass die Vertraulichkeitserwartung als Schutzgut alle dargestellten Risiken umfasst. Sie kann jedoch dort tauglich sein, wo eine Anknüpfung an die Selbstbestimmung und Menschenwürde mangels faktischer Verhaltensauswirkung oder mangels besonderer Schwere zu pauschal ist. Der Nachvollzug bereichsspezifischer Vertraulichkeitserwartungen kann deshalb die Ausrichtung des Datenschutzrechts auf die dargestellten Risiken fördern. Ein weiterer Vorteil der Vertraulichkeitserwartung ergibt sich aus der internationalen Anschlussfähigkeit, da das Schutzgut in verschiedenen Rechtskreisen gebräuchlich ist. Auch begegnet der Erwartungsschutz im Gegensatz zum Schutz der Verhaltensfreiheit nicht dem Einwand der nicht hinreichend belegten informationsbedingten Verhaltensanpassungen.

Dabei muss eine „Vertraulichkeitserwartung" als Schutzgut jedoch mehr sein als die bloße Erwartung der Nichtweitergabe von Daten. Nicht das Vertrauen als solches ist bereits schützenswert, sondern erst die Vertraulichkeitserwartung, für die auch bestimmte vertrauensbegründende Umstände vorliegen müssen.[241] Sind diese gegeben, kann das Vorhandensein von Vertrauen – das sich z.B. in einer bestimm-

---

[240] Siehe oben Teil 2, F.2.b).

[241] Zu der insoweit vergleichbaren Diskussion um strafrechtliche Vertrauensrechtsgüter vgl. *Hefendehl*, GA 2007, 1 (12 f.).

ten Mediennutzung manifestieren kann – mit den Mitteln der empirischen Sozialforschung geprüft werden.

Eine Gefahr bei der stärkeren Ausrichtung auf dieses Schutzgut liegt jedoch in einer Umsetzungsweise, die sich nicht am Menschen, sondern pauschal an der Rechtslage orientiert. Es sollte nicht – wie es sich auf Ebene der Rechtsprechung des EuGH zumindest andeutet – undifferenziert durch Verweis auf die Rechtslage in einem Mitgliedstaat eine Vertraulichkeitserwartung für unberechtigt erklärt werden. Der verfassungsrechtliche Schutzumfang darf jedenfalls nicht vollends in die Disposition des Gesetzgebers verlagert werden. Andererseits darf auch nicht von faktischer Überwachungstätigkeit – wie beispielsweise durch die NSA – allgemein auf die Unvernünftigkeit jeder Vertraulichkeitserwartung geschlossen werden. Sinnvoll erscheint dagegen die sich in der Rechtsprechung des BVerfG abzeichnende Konkretisierung über Spezialgrundrechte. Auch hier muss jedoch eine Offenheit für die oben beschriebenen Risiken gewahrt werden. Die Risikokategorien sollten deshalb zur Konkretisierung von Vertraulichkeitserwartungen herangezogen werden.

Eine weitere Folgerung für Schutzgüter ergibt sich aus den Grundstrukturen der oben vorgenommenen Risikosystematisierung in Makro- und Mikroebene. Diese kann auch im Rahmen der – insbesondere für das einfachrechtliche Datenschutzrecht bedeutsamen – Einwilligung fruchtbar gemacht werden: So sind Makro-Risiken keiner Individualeinwilligung zugänglich, ähnlich wie dies bei Kollektivrechtsgütern im Strafrecht der Fall ist.

Es wird sich zeigen, inwieweit die vorgenommene Klassifizierung von Risiken und die Folgerungen für Schutzgüter bei kommenden Datenschutzreformen zu einem pragmatischen und kohärenten Datenschutzrecht beitragen können.

## IV. Ausblick

*Michel Foucault* erklärt die Existenz einer in die Tiefe gehenden Organisation von Überwachungen und Kontrollen als Antwort des Prinzips „Ordnung“ auf die Verwirrungen der Pestepidemie im 17. Jahrhundert; auf die Ängste vor einer todbringenden Vermischung und Vervielfältigung von Körpern, der Auslöschung von Verboten durch Furcht, Tod und Ausbreitung der Krankheit. Die nach dieser Vorstellung entwickelte Idee einer lückenlosen Überwachung des parzellierten Raums stellt für ihn das kompakte Modell einer Disziplinierungsanlage dar. Es mündet in dem Prinzip des Panopticons, einem auf *Jeremy Bentham* zurückgehenden Gefängnismodell, in dem jeder Gefangene von der Wärterposition aus sichtbar ist und

dadurch zum Prinzip seiner eigenen Überwachung gemacht wird.[242] Die in ihrer Tragweite noch nicht absehbaren Enthüllungen *Edward Snowdens*[243] werfen die Frage auf, welche Verwirrungen und Ängste dem von den beteiligten Regierungen geschaffenen Überwachungssystem zugrunde liegen. Ist es die legitime Furcht vor grenzüberschreitender Kriminalität und religiös oder nationalistisch motiviertem, internationalem Terrorismus oder der Vorbote einer überwunden geglaubten Totalisierung des Staates?

Die Grenzen staatlicher und staatlich-privater Informationsverwendung sind seit jeher zentraler Regelungsgegenstand des Datenschutzrechts. Die Enthüllungen um die amerikanisch-britische Internetüberwachung verdeutlichen dabei das auch in dieser Untersuchung aufgegriffene, von den untersuchten Konzeptionen jedoch erst in Ansätzen erfasste Problem der staatlichen Verwendung privater Daten zu Überwachungszwecken. Die „Verschmelzung von Staat und Markt" zu einem „Informationsstaat",[244] der seine Bürger in vielfältiger Weise überwacht, ist eine der offenen Flanken vieler Datenschutzkonzeptionen. Themenfelder wie die Vorratsspeicherung von Telekommunikationsverbindungsdaten oder die Auswertung von Fluggastdaten sind zwar bereits Gegenstand von Regelung und Rechtsprechung geworden, sie orientieren sich jedoch noch nicht hinreichend an den Risiken der Verarbeitung personenbezogener Daten. Die Sicherheitsgesetzgebung wie auch die hierzu ergehende Rechtsprechung sollte deshalb in datenschutzrechtlicher Hinsicht stärker auf die hier entwickelten Risiken ausgerichtet werden. Die staatliche Nutzung privater Datenbestände kann dabei aufgrund der Verschmelzung von staatlichen Eingriffsbefugnissen mit der Masse an privater Datenverarbeitung zu einer Potenzierung der dargestellten Risiken führen.

Trotz dieser Gefahr – einer staatlich-privaten „Informationstransgression" – darf nicht der Blick darauf verstellt werden, dass in einer von legitimen privaten und kommerziellen Informationsverarbeitungen geprägten und durchzogenen Gesellschaft einfache Verbote nach Maßgabe des überkommenen nationalen Polizeirechts oder die Idee einer Verringerung von Datenverarbeitung keine gangbaren Wege mehr sind. Es gilt stattdessen, Forschung, Gesetzgebung und Rechtsprechung auf die in dieser Untersuchung herausgearbeiteten Risiken auszurichten. Zu erwägen ist deshalb die (zumindest teilweise) Ablösung der überkommenen starren Verarbeitungsregelungen und Verbote durch einen eher am Vorbild des Deliktsrechts orientierten Ansatz. Gerade hierzu kann die vorgenommene Klassifizierung von Risiken beitragen.

---

242 *Foucault*, Überwachen und Strafen, S. 251 ff., 260.

243 Dazu oben Einleitung, I.

244 http://www.faz.net/aktuell/feuilleton/big-data-und-nsa-am-luegendetektor-12276531.html [Stand: 28.3.2014].

# Zusammenfassung

Die vorliegende Untersuchung hat sich aus einer grundlegend rechtsvergleichenden Perspektive mit dem Datenschutzrecht befasst und dabei die Frage gestellt, wovor das Datenschutzrecht eigentlich schützt. Diese Frage konnte durch eine systematische Erarbeitung von Risikokategorien und durch eine Präzisierung einschlägiger Schutzgüter, insbesondere der Vertraulichkeitserwartung, beantwortet werden. Dabei wurden die wichtigsten datenschutzrechtlichen Konzeptionen auf internationaler, unionsrechtlicher und nationaler Ebene herausgegriffen und in verschiedenen „Dimensionen" des Rechts (soft law, Völkerrecht, Unionsrecht, Rechtsprechung und Lehre) untersucht. Dabei wurde das einfachgesetzliche nationale Datenschutzrecht nur in den für die untersuchten Konzeptionen relevanten Teilaspekten aufgegriffen, da sich die wesentlichen Regelungskonzeptionen bereits auf internationaler und unionsrechtlicher Ebene wiederfinden.

Es wird nicht verkannt, dass sich dieser Ansatz von der bisherigen datenschutzrechtlichen Dogmatik unterscheidet: Er gibt sich nicht mit der pauschalen Behauptung zufrieden, dass jede automatisierte Informationsverarbeitung ein Risiko darstelle. Diese Aussage mag zwar von einem allgemeinen Standpunkt aus zutreffen, sie ist jedoch in einer von Informationsverarbeitung geprägten Welt kein taugliches Leitmotiv mehr und muss daher fortentwickelt werden. Ähnlich wie die Rechtsgutslehre im Strafrecht zur Begrenzung einer überbordenden strafrechtlichen Rechtsetzung erforderlich ist,[245] gilt es eine Schutzgüterlehre im Datenschutzrecht zur Verhinderung einer übertriebenen und gerade dadurch ihren Schutzauftrag verfehlenden Regulierung zu entwickeln. Dass dies erforderlich ist, lässt sich gut anhand datenschutzrechtlicher Diskurse nachvollziehen; so etwa in der Forderung von *Masing* nach einer Abschichtung von Vertraulichkeitserwartungen im zivilrechtlichen Datenschutzrecht[246] oder anhand der kontroversen Diskussion des datenschutzrechtlichen Verbotsprinzips[247] in der Literatur, zuletzt etwa bei *Bull*[248] und *Weichert*.[249] Die vorliegende Untersuchung soll als Diskussionsvorschlag und erster Schritt in diese Richtung verstanden werden.

Wie die Herausarbeitung der (zahlreichen und zum Teil schwerwiegenden) Risiken gezeigt hat, liegt in dem hier verfolgten risikoorientierten Ansatz gerade keine Verharmlosung von Informationsverarbeitung und auch keine pauschale Forderung nach einer Abkehr vom datenschutzrechtlichen Verbotsprinzip. Stattdessen wird

---

[245] Allgemein zur Rechtsgutslehre statt vieler: *Rönnau*, JuS 2009, 211 ff.; *Hefendehl*, GA 2007, 1 ff.

[246] *Masing*, NJW 2012, 2305 (2307).

[247] Kurzer Überblick über das Verbotsprinzip bei *Hartge*, in: Schmidt/Weichert (Hrsg.), Datenschutz, S. 280 ff.

[248] *Bull*, Netzpolitik, S. 136 ff.

[249] *Weichert*, DuD 2013, 246 ff.

ein pragmatischer Vorschlag zur stärkeren Ausrichtung und Ausdifferenzierung der rechtswissenschaftlichen Bemühungen auf *konkrete Verarbeitungsfolgen* unterbreitet. Aufgrund der nun vorliegenden Klassifizierung von Risiken der Verarbeitung personenbezogener Daten erscheint es aber durchaus möglich und diskussionswürdig, auch im Datenschutzrecht eine „kopernikanische Wende" zu vollziehen und das pauschale datenschutzrechtliche Verbotsprinzip – zumindest im Privatbereich – aufzugeben. An dessen Stelle könnten dann z.B. einzelne, an den Risiken der Verarbeitung personenbezogener Daten ausgerichtete Sanktionen, ggf. in Anlehnung an das Deliktsrecht, treten.

Mit den im vierten Abschnitt dieser Arbeit entwickelten Risikokategorien werden hierzu erstmals umfassend *Indikatoren* kenntlich gemacht, auf die weitere Untersuchungen aufbauen und die in künftigen Regelungen aufgegriffen werden können. Sie stellen das Substrat der untersuchten Regelungskonzeptionen des überkommenen Datenschutzrechts dar. Diese Risiken können zu einer besseren Systematik des Datenschutzrechts beitragen, in dem mit ihnen einschlägige Schutzgüter konkretisiert werden. Erste Überlegungen hierzu wurden für die Vertraulichkeitserwartung vorgenommen. Diese erscheint als Schutzgut tauglich, da es sowohl auf individueller also auch auf kollektiver Ebene greifen kann und sich durch Flexibilität, Offenheit und internationale Anschlussfähigkeit auszeichnet.

## Übersicht Risikokategorien

**A. Makroebene: Strukturelle Risiken**

1. Gesellschaftlich-politische Risiken
   a) Informationsmacht
   b) Konformistische Verhaltensanpassung durch Überwachungsdruck
   c) Verantwortungsnegation
2. Wirtschaftliche Risiken
   a) Handelshemmnisse
   b) Nachfragerückgang durch Vertrauensverlust

**B. Mikroebene: Überwiegend individuelle Risiken**

1. Erhöhung individueller Verletzlichkeit für Straftaten
2. Schamgefühl und Publizitätsschäden
3. Selektivitätsschäden
   a) Diskriminierung
   b) Stigmatisierung

## Summary

There is a contentious debate in German Constitutional Law on how to interpret and determine the limits of constitutional data protection. The concept of contemporary German and European data protection policy is a protection against the abuse of personal data which starts long before something happens. The citizens' concerns which triggered the development of this legal framework can roughly be traced back to the abuse of centralized registers by Nazi and Socialist regimes. They led to a situation in which data protection regulations cover nearly the entire data processing activity of state and private entities.

Because of technological changes and globalization the broad regulatory approach has failed. Legal scholars and practitioners nowadays tend to support modernization and demand a concept appropriate to „the risks“. However, it has not been clarified yet what hat these actual risks are. The fact that they reach beyond identity theft and reputation losses is illustrated by the view that data protection rules have to strengthen democracy and prevent conformism in elections and a possible chilling effect on freedom of speech. This thesis therefore systematizes risk conceptions in Data Protection Law as a prerequisite to a regulatory reform.

I reviewed International, European and German Data Protection norms as well as court rulings regarding underlying risk conceptions and protected values. The out-

come is a classification of data protection risks on different levels of regulation which are common to the analyzed normative rules. The classification enables a new approach to structuring future data protection policy.

Furthermore, these risk conceptions can help to specify the protected values in Data Protection law. The value that proved to be most appropriate as protected value is the expectation of privacy. It is flexible, open to new technologies and can easily be adapted in different legal systems. Thus, expectation of privacy can be specified by the developed risk categories and recognized on the individual and collective level.

## Overview of Categories of Risks

**A. Macro-level: Structural Risks**

1. Societal-Political Risks
   a) Informational Power
   b) Conformistic Behavioral Adjustment due to Surveillance Pressure
   c) Diffusion of Responsibility
2. Economic Risks
   a) Trade Restrictions
   b) Decrease in Demand due to the Loss of Trust

**B. Micro-level: Predominantly Individual Risks**

1. Increase in Individual Vulnerability to Criminal Offenses
2. Feeling of Shame and Showcase Damages
3. Damages due to Selectivity
   a) Discrimination
   b) Stigmatization
4. Permanence of Information
5. Decontextualization
   a) Shortfall of Context
   b) Infiltration of Context
6. Emergence of Information
7. Flawed Information

**C. Macro- and Micro-level: Societal and Individual Risks**

1. Treatment of Humans as mere Objects

2. Excourse: „Personality Profile“
3. Heteronomy
4. Deception of Expectations of Privacy

**D. Borderline and Non-Risks**

1. Advertisements and Specification of Target Groups
2. Solvency Checks and Accounts Receivable Management
3. Excourse: Labour Law Context

# Literaturverzeichnis


*Abel, Ralf-Bernd*, Geschichte des Datenschutzrechts. In: Alexander Roßnagel (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, S. 194–217.

*Albers, Marion*, Information als neue Dimension im Recht. Rechtstheorie 33 (2002), 61–89.

– Informationelle Selbstbestimmung. Baden-Baden 2005.

– Umgang mit personenbezogenen Informationen und Daten. In: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen. Berlin u.a. 2008, S. 107–220.

*Albrecht, Hans-Jörg/Kilchling, Michael*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten. Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht im Auftrag des Bundesamtes für Justiz zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung. 2., erweiterte Fassung. Freiburg Juli 2011.

*Alby, Tom*, Web 2.0. Konzepte, Anwendungen, Technologien. 3. Aufl. München 2008.

*Alpert, Sheri A.*, Protecting Medical Privacy: Challenges in the Age of Genetic Information. 59 Journal of Social Issues 2 (2003), 301–322.

*Amelung, Knut*, Buchbesprechung Jäger, Christian: Beweisverwertung und Beweisverwertungsverbote im Strafprozess. ZStW 123 (2011), 595–605.

APEC (Hrsg.), APEC Privacy Framework, Singapur 2005.

– Fact Sheet APEC Cross-border Privacy Enforcement Arrangement, 2010, abrufbar unter www.apec.org/About-Us/About-APEC/Fact-Sheets/~/media/Files/AboutUs/Factsheet/FS_CPEA_020710.ashx [Stand: 28.3.2014].

*Ast, Susanne*, Mehrebenenstruktur, Mehrebenensystem. In: Jan Bergmann (Hrsg.), Handlexikon der Europäischen Union. 4. Aufl. Baden-Baden 2012 (Beck-Online).

*Bäcker, Matthias*, Die Vertraulichkeit der Internetkommunikation. In: Harmut Rensen/Stefan Brink (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts. Berlin 2009, S. 99–136.

*Bäcker, Matthias/Hornung, Gerrit*, EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa. ZD 2012, 147–152.

*Badura, Peter*, Staatsrecht. Systematische Erläuterungen des Grundgesetzes. 5. Aufl. München 2012.

*Baker, Stewart*, The Privacy Problem: What's Wrong with Privacy? In: Berin Szoka/Adam Marcus (Hrsg.), The Next Digital Decade. Essays on the Future of the Internet. Washington D.C. 2010, S. 483–507.

*Battis, Ulrich*, Bundesbeamtengesetz. 4. Aufl. München 2009.

*Baumer, David L./Brande Earp, Julia/Evers, Pamela S.*, Tit for Tat in Cyberspace: Consumer and Website Responses to Anarchy in the Market for Personal Information. 4 N.C.J.L. & Tech (2002–2003), 217–273.

*Behnke, Nathalie*, Responsivität und Verantwortlichkeit der öffentlichen Verwaltung. In: Edwin Czerwick/Wolfgang Lorig/Erhard Treutner (Hrsg.), Die öffentliche Verwaltung in der Demokratie der Bundesrepublik Deutschland. Wiesbaden 2009, S. 45–64.

*Benda, Ernst*, Privatsphäre und „Persönlichkeitsprofil". In: Gerhard Leibholz/Hans Joachim Faller/Paul Mikat/Hans Reis (Hrsg.), Menschenwürde und freiheitliche Rechtsordnung. Festschrift für Willi Geiger zum 65. Geburtstag. Tübingen 1974, S. 23–44.

*Bernsdorff, Norbert*, Kommentierung zu Art. 8. In: Jürgen Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union. 3. Aufl. Baden-Baden u.a. 2011, S. 215–225.

BITKOM (Hrsg.), Soziale Netzwerke. Zweite, erweiterte Studie. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet. Berlin 2011.

– Big Data im Praxiseinsatz. Szenarien, Beispiele, Effekte. Berlin 2012.

*Böckenförde, Thomas*, Die Ermittlung im Netz. Tübingen 2003.

– Auf dem Weg zur elektronischen Privatsphäre – zugleich Besprechung von BVerfG, Urteil vom 27.2.2008 – „Online-Durchsuchung". JZ 2008, 925–939.

*Borges, Georg*, Der neue Personalausweis und der elektronische Identitätsnachweis. NJW 2010, 3334–3339.

– Haftung für Identitätsmissbrauch im Online-Banking. NJW 2012, 2385–2389.

*Boritz, Efrim/No, Won Gyun*, The Effect of Involvement and Privacy Policy Disclosure on Individuals' Privacy Behaviour. 2007, abrufbar unter http://accounting.uwaterloo.ca/uwcisa/resources/eprivacy/Privacy Customer Paper 2008-01-19.pdf [Stand: 28.3.2014].

*Boshmaf, Yazan/Muslukhov, Ildar/Beznosov, Konstantin/Ripeanu, Matei*, The Socialbot Network: When Bots Socialize for Fame and Money. 2011, abrufbar unter http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf [Stand: 28.3.2014].

*Brandimarte, Laura/Acquisti, Alessandro/Loewenstein, George*, Misplaced Confidences: Privacy and the Control Paradox. In: Social Psychological and Personality Science OnlineFirst, abrufbar unter http://spp.sagepub.com/content/4/3/340 [Stand: 9.8.2012].

*Breitenmoser, Stephan*, Der Schutz der Privatsphäre gemäss Art. 8 EMRK. Das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und des Briefverkehrs. Basel u.a. 1986.

*Britz, Gabriele*, Freie Entfaltung durch Selbstdarstellung. Tübingen 2007.

– Europäisierung des grundrechtlichen Datenschutzes? EuGRZ 2009, 1–11.

*Britz, Gabriele*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. In: Wolfgang Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft. Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen. Tübingen 2010, S. 561–596.

*Brown, Mark/Muchira, Rose*, Investigating the relationship between internet privacy concerns and online purchase behavior. 5 Journal of Electronic Commerce Research 1 (2004), 62–70.

*Bull, Hans Peter*, Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese? NJW 2006, 1617–1624.

– Neue Bewegung im Datenschutz – Missbrauchsbekämpfung oder Ausbau bereichsspezifischer Regelungen? ZRP 2008, 233–236.

– Informationelle Selbstbestimmung – Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit. Tübingen 2009.

– Informationelle Selbstbestimmung – Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit. 2. Aufl. Tübingen 2011.

– Netzpolitik: Freiheit und Rechtsschutz im Internet. Baden-Baden 2013.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.), BBK-Glossar. Ausgewählte zentrale Begriffe des Bevölkerungsschutzes. 2. Aufl. Bonn 2011.

Bundeskriminalamt (Hrsg.), Cybercrime. Bundeslagebild 2011. Wiesbaden 2011.

*Bygrave, Lee A.*, International agreements to protect personal data. In: James B. Rule/Graham Greenleaf (Hrsg.), Global Privacy Protection. The First Generation. Cheltenham u.a. 2008, S. 15–49.

*Dammann, Ulrich/Simitis, Spiros*, EG-Datenschutzrichtlinie. Kommentar. Baden-Baden 1997.

*Dannecker, Gerhard*, Anmerkung zu EuGH Urteil vom 26.2.2013 Rs. C 617/10. JZ 2013, 616–620.

*Däubler, Wolfgang*, Die kontrollierten Belegschaften. In: Jan-Hinrik Schmidt/Thilo Weichert (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn 2012, S. 188–197.

*Diekmann, Andreas/Voss, Thomas*, Die Theorie rationalen Handelns. Stand und Perspektiven, 2003, abrufbar unter www.uni-leipzig.de/~sozio/mitarbeiter/m27/content/eigene_site/prof.voss.public_2003b.pdf [Stand: 28.3.2014].

*Dix, Alexander*, Datenschutz und Informationsfreiheit. Landes-, Bundes-, Europa- und Völkerrecht. Baden-Baden 2011.

*Drackert, Stefan*, Die Verwendung fiktiver Identitäten für strafprozessuale Ermittlungen in sozialen Netzwerken. Überlegungen zur Grundrechtsrelevanz und Zulässigkeit nach deutschem Recht. eucrim 2011, 122–126.

*Duttge, Gunnar*, Strafprozessualer Einsatz von V-Personen und Vorbehalt des Gesetzes. JZ 1996, 556–565.

*Düx, Heinz*, Globale Sicherheitsgesetze und weltweite Erosion von Grundrechten. Statt „Feindstrafrecht" globaler Ausbau demokratischer Rechte. ZRP 2003, 189–195.

*Ebersbach, Anja/Glaser, Markus/Heigl, Richard*, Social Web. Konstanz 2008.

*Ehmann, Eugen*, Das „Datenschutz-Paket" der Europäischen Kommission – Beginn einer Zeitenwende im europäischen Datenschutz? JurisPR-ITR 4/2012 Anm. 2 [Stand: 28.3.2014].

*Ehmann, Eugen/Helfrich, Marcus*, EG-Datenschutzrichtlinie. Kurzkommentar. Köln 1999.

*Ehmann, Horst*, Informationsschutz und Informationsverkehr im Zivilrecht. AcP 188 (1988), 230–380.

*Ehricke, Ulrich*, „Soft law" – Aspekte einer neuen Rechtsquelle. NJW 1989, 1906–1908.

*Eisele, Jörg*, Datenschutz im Rahmen der PJZS. In: Ulrich Sieber/Franz-Hermann Brüner/Helmut Satzger/Bernd von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht. Baden-Baden 2011, S. 781–786.

– Compliance und Datenschutzstrafrecht. Strafrechtliche Grenzen der Arbeitnehmerüberwachung. Baden-Baden 2012.

*Ellger, Reinhard*, Der Datenschutz im grenzüberschreitenden Datenverkehr. Eine rechtsvergleichende und kollisionsrechtliche Untersuchung. Baden-Baden 1990.

*Enders, Christoph*, Schutz der Persönlichkeit und Privatsphäre. In: Detlef Merten/Hans-Jürgen Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band III: Grundrechte in Deutschland – Allgemeine Lehren II. Heidelberg 2009, S. 159–231.

ENISA (Hrsg.), To log or not to log? Risks and benefits of emerging life-logging applications (final report). Heraklion 2011.

– Study on monetising privacy. An economic model for pricing personal information. Heraklion 2012.

– Threat Landscape. Responding to the Evolving Threat Environment. Heraklion 2012.

*Epping, Volker/Hillgruber, Christian* (Hrsg.), Beck'scher Online-Kommentar GG [Stand: 5.5.2013, Edition 18]. München 2013 (zit. Epping/Hillgruber-*Bearbeiter*).

*Ernst, Stefan*, Social Networks und Arbeitnehmer-Datenschutz. NJOZ 2011, 953–957.

*Eser, Albin/Heine, Günter/Perron, Walter/Sternberg-Lieben, Detlev/Eisele, Jörg/Bosch, Nikolaus/Hecker, Bernd/Kinzig, Jörg*, Strafgesetzbuch – Kommentar. Begründet von Adolf Schönke, fortgeführt von Horst Schröder. Unter Mitarbeit von Ulrike Schittenhelm. 28. Aufl. München 2010 (zit. Schönke/Schröder-*Bearbeiter*).

*Esser, Robert*, Europäischer Datenschutz – Allgemeiner Teil – Mindeststandards der Europäischen Menschenrechtskonvention (EMRK). In: Jürgen Wolter/Wolf-Rüdiger Schenke/Hans Hilger/Josef Ruthig/Mark A. Zöller (Hrsg.), Alternativentwurf Europol und europäischer Datenschutz. Heidelberg 2008, S. 281–317.

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

– Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Gesamtkonzept für den Datenschutz in der Europäischen Kommission; KOM 2010 (609), 4.11.2010.

Europäische Kommission (Hrsg.), Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union. Brüssel 2011.

*Fiedler, Christoph*, Datenverarbeitung am Beispiel adressierter Werbung. In: Jan-Hinrik Schmidt/Thilo Weichert (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn 2012, S. 165–171.

*Foucault, Michel*, Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt a.M. 1994.

*Frenz, Werner*, Informationelle Selbstbestimmung im Spiegel des BVerfG. DVBl. 2009, 333–339.

*Gärditz, Klaus Ferdinand*, Strafprozess und Prävention. Entwurf einer verfassungsrechtlichen Zuständigkeits- und Funktionenordnung. Tübingen 2003.

– Anmerkung zu BVerfG, Urteil vom 24.4.2013, 1 BvR 1215/07. JZ 2013, 633–636.

*Geiger, Andreas*, Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie bei der Straftatbekämpfung. Berlin 1994.

*Genz, Alexander*, Datenschutz in Europa und den USA. Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung. Wiesbaden 2004.

*Giesecke, Bettina/Wissenschaftlicher Dienst des Bundestages* (Hrsg.), Aktueller Begriff: Die Entscheidung des Bundesverfassungsgerichts zum Antiterrordateigesetz. Berlin 2013.

*Gola, Peter/Klug, Christoph*, Grundzüge des Datenschutzrechts. München 2003.

*Gola, Peter/Klug, Christoph/Körffer, Barbara/Schomerus, Rudolf*, BDSG, Bundesdatenschutzgesetz. 11. Aufl. München 2012 (zit. *Gola/Schomerus*).

*Grabenwarter, Christoph*, Europäische Menschenrechtskonvention. Ein Studienbuch. 4. Aufl. München u.a. 2009.

*Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin/Wolf, Manfred* (Hrsg.), Das Recht der Europäischen Union, Band IV: Sekundärrecht. A: Verbraucher- und Datenschutzrecht. 40. Aufl. München 2009 (zit. Grabitz/Hilf-*Bearbeiter*).

*Gräf, Lorenz*, Privatheit und Datenschutz. Eine soziologische Analyse aktueller Regelungen zum Schutz privater Bereiche auf dem Hintergrund einer Soziologie der Privatheit. Köln 1993.

*Graulich, Kurt*, Terrorismus und Terrorismusbekämpfung. Folgt der Auflösung der rechtlichen Angriffsform die Auflösung der rechtlichen Verteidigungsform? In: Kurt Graulich/Dieter Simon (Hrsg.), Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Perspektiven. Berlin 2007, S. 389–410.

*Greenleaf, Graham*, Five years of the APEC Privacy Framework: Failure or promise? 25 CLSR (2009), 28–43.

*Gridl, Rudolf*, Datenschutz in globalen Telekommunikationssystemen: Eine völker- und europarechtliche Analyse der vom internationalen Datenschutzrecht vorgegebenen Rahmenbedingungen. Baden-Baden 1999.

*Griese, Thomas*, Zur Notwendigkeit und Effektivität eines verbesserten datenrechtlichen Persönlichkeitsschutzes im Arbeitsrecht. Berlin 1987.

*Grimm, Dieter*, Die Zukunft der Verfassung II. Auswirkungen von Europäisierung und Globalisierung. Berlin 2012.

– Der Datenschutz vor einer Neuorientierung. JZ 2013, 585–592.

*Gurlit, Elke*, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. NJW 2010, 1035–1041.

*Gürtler, Paul*, Baustelle Datenschutz – internationale Entwicklungen. RDV 2012, 126–135.

*Hansen, Marit/Weichert, Thilo*, Das Recht auf Privatheit, 2011, abrufbar unter www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html [Stand: 28.3.2014].

*Harper, Jim/Spies, Axel*, A Reasonable Expectation of Privacy? Data Protection in the United States and Germany. Washington D.C. 2006.

*Hartge, Dagmar*, Erlaubnisse und Verbote im Datenschutzrecht. In: Jan-Hinrik Schmidt/Thilo Weichert (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn 2012, S. 280–289.

*Hatje, Armin*, Informationsaustausch und Datenschutz in der Europäischen Union – primärrechtliche Grundlagen, Grundzüge und Probleme des aktuellen Sekundärrechts. In: Dokumentation der Fachtagung „Datenschutz in Deutschland nach dem Vertrag von Lissabon“ am 09. Dezember 2008, abrufbar unter www.datenschutz.hessen.de/europa.htm [Stand: 28.3.2014].

*Heckmann, Dirk* (Hrsg.), Juris PK-Internetrecht. 3. Aufl. Saarbrücken 2011.

*Hefendehl, Roland*, Der Begriff des Rechtsguts. GA 2007, 1–14.

*Helfrich, Marcus*, Scoring und Datenschutz. In: Thomas Hoeren/Ulrich Sieber/Bernd Holznagel (Hrsg.), Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs. München 2014 [Stand: 38. Erg. Lfg.], Teil 16.4.

*Henke, Ferdinand*, Die Datenschutzkonvention des Europarates. Frankfurt a.M. 1986.

*Henrichs, Axel/Wilhelm, Jörg*, Global vernetzen – lokal ermitteln. Polizeiliche Herausforderungen durch soziale Netzwerke. Deutsche Polizei 10 (2010), 6–12.

– Polizeiliche Ermittlungen in sozialen Netzwerken. Kriminalistik 2010, 30–37.

*Herzog, Roman/Herdegen, Matthias/Scholz, Rupert/Klein, Hans H.*, Grundgesetz Kommentar. Begründet von Theodor Maunz und Günter Dürig. Stand: 67. Erg.-Lfg. 2013. München 2013 (zit. Maunz/Dürig-*Bearbeiter*).

*Heussner, Hermann*, Zur Funktion des Datenschutzes und der Notwendigkeit bereichsspezifischer Regelungen. In: Wolfgang Gitter/Werner Thieme/Hans Zacher (Hrsg.), Im Dienst des Sozialrechts. Festschrift für Georg Wannagat. Köln u.a. 1981, S. 173–200.

*Hoffmann-Riem, Wolfgang*, Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Wege zu einem neuen Konzept des Datenschutzes. AöR 123 (1998), 513–540.

*Hoffmann-Riem, Wolfgang*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. In: Wolfgang Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft. Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen. Tübingen 2010, S. 525–559.

*Hofmann, Hasso*, Menschenrechtliche Autonomieansprüche. JZ 1992, 165–173.

*Hondius, Frits W.*, Emerging data protection in Europe. Amsterdam 1975.

*Hufen, Friedhelm*, Staatsrecht II. Grundrechte. 2. Aufl. München 2009.

ILO, Protection of workers' personal data. An ILO Code of practice. Genf 1997.

International Working Group on Data Protection in Telecommunications (Hrsg.), Report and Guidance on Privacy in Social Network Services – "Rome Memorandum". 43rd meeting, 3–4 March 2008, Rome (Italy). Rom 2008.

*Ipsen, Knut*, Völkerrecht, 5. Aufl. München 2004.

*Jahoda, Marie/Cook, Stuart W.*, Security measures and freedom of thought: An exploratory study of the impact of loyalty and security programs. 61 Yale L.J. (1952), 295–333.

*Jarass, Hans/Pieroth, Bodo*: Grundgesetz für die Bundesrepublik Deutschland. Kommentar. 12. Aufl. München 2012.

*Jescheck, Hans-Heinrich*, Lehrbuch des Strafrechts. Allgemeiner Teil. Berlin 1988.

*Kafka, Franz*. Der Proceß. Stuttgart 1998.

*Kaspersky, Eugen*, Malware. Von Viren, Würmern, Hackern und Trojanern und wie man sich vor ihnen schützt. München 2008.

*Kaufmann, Noogie C.*, Meldepflichten und Datenschutz-Folgenabschätzung. Kodifizierung neuer Pflichten in der EU-Datenschutz-Grundverordnung. ZD 2012, 358–362.

*Kenzel, Brigitte*, Die automatische Kennzeichenfahndung. Eine Überwachungsmaßnahme an der Schnittstelle zwischen präventivem und repressivem Einsatz. Hamburg 2013.

*Kilian, Wolfgang*, Informationelle Selbstbestimmung und Marktprozesse. CR 2002, 921–929.

*Kim, Dan J./Ferrin, Donald L./Rao, H. Raghav*, A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. 44 Decision Support Systems (2008), 544–564.

*Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich* (Hrsg.), Strafgesetzbuch. 4. Aufl. Baden-Baden 2013 (zit. Kindhäuser/Neumann/Paeffgen-*Bearbeiter*).

*Kingreen, Thorsten*, Kommentierung zu Art. 7, 8 und Art. 51 f. GRCh. In: Christian Callies/Matthias Ruffert (Hrsg.), EUV/AEUV Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta. 4. Aufl. München 2011, S. 2807–2819, S. 2812–2816 und S. 2955–2991.

*Kittler, Friedrich A.*, Geschichte der Kommunikationsmedien. In: Stroemfeld/Roter Stern/Museum für Gestaltung Zürich (Hrsg.), Interventionen 2 – Raum und Verfahren. Basel, Frankfurt a.M. 1993, S. 169–188.

*Klesczewski, Diethelm*, Binnenmarktförderung durch Speicherpflichten? HRRS 2009, 250–252.

*Koch, Frank A.*, Neue technische Formen der Persönlichkeitserfassung und die Frage der „PostPrivacy". ITRB 2011, 158–162.

*Kohler, Josef*, Das Autorrecht – eine zivilistische Abhandlung, zugleich ein Beitrag zur Lehre vom Eigenthum, vom Miteigenthum, vom Rechtsgeschäft und Individualrecht. 18 Jahrb. f. Dogm. (1880), 130–487.

– Urheberrecht an Schriftwerken und Verlagsrecht. Stuttgart 1907.

*Kohlhaas, Elisabeth*, Die Mitarbeiter der regionalen Staatspolizeistellen. Quantitative Befunde zur Personalausstattung der Gestapo. In: Gerhard Paul/Klaus-Michael Mallmann (Hrsg.), Die Gestapo. Mythos und Realität. Darmstadt 2003, S. 219–235.

*Köhntopp, Kristian*, Von der Spackeria, von Aluhüten und vom Kontrollverlust (Blogeintrag), 12.5.2011, http://blog.koehntopp.de/archives/3073-Von-der-Spackeria,-von-Aluhueten-und-vom-Kontrollverlust.html [Stand: 29.10.2011].

Konferenz der Europäischen Datenschutzbeauftragten, Entschließung über die Notwendigkeit eines umfassenden Rahmens für den Datenschutz, 5.4.2011, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/EuDSK/EntschliessungEUDSK_deutsch.pdf?__blob=publicationFile [Stand: 28.3.2014].

*Korff, Douwe/Brown, Ian*, Zusammenfassung. In: Europäische Kommission (Hrsg.), Vergleichende Studie über verschiedene Ansätze zur Bewältigung neuer Herausforderungen für den Schutz der Privatsphäre, insbesondere aufgrund technologischer Entwicklungen. 2010, S. 1–7.

*Kosinski, Michal/Stillwell, David/Graepel, Thore*, Private traits and attributes are predictable from digital records of human behavior. 110 PNAS 15 (2013), 5802–5805.

*Kübler, Johanna*, Die Säulen der Europäischen Union: einheitliche Grundrechte? Zur Grundrechtsdivergenz zwischen der ersten und dritten Säule am Beispiel des Datenchutzes. Baden-Baden 2002.

*Kühling, Jürgen*, Grundrechte. In: Armin von Bogdandy/Jürgen Bast (Hrsg.), Europäisches Verfassungsrecht – theoretische und dogmatische Grundzüge. 2. Aufl. Heidelberg u.a. 2009, S. 657–704.

*Kühling, Jürgen/Bohnen, Simon*, Zur Zukunft des Datenschutzrechts – Nach der Reform ist vor der Reform. JZ 2010, 600–610.

*Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios*, Datenschutzrecht. Frankfurt a.M. 2008.

– Datenschutzrecht. 2. Aufl. Heidelberg 2011.

*Kutscha, Martin*, Grundrechtlicher Persönlichkeitsschutz bei der Nutzung des Internet. DuD 2011, 461–464.

*Ladeur, Karl Heinz*, Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken. Zur „objektiv-rechtlichen Dimension" des Datenschutzes. DuD 2000, 12–19.

– Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion? DÖV 2009, 45–55.

*Lessig, Lawrence*, Code und andere Gesetze des Cyberspace. Berlin 2001.

*Lüke, Falk*, Datenschutz aus Verbrauchersicht. In: Jan-Hinrik Schmidt/Thilo Weichert (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn 2012, S. 154–164.

*Maass, Hans-Heinrich*, Information und Geheimnis im Zivilrecht. Eine rechtshistorische und rechtsvergleichende Kritik der privaten und der gewerblichen Geheimsphäre. Stuttgart 1970.

*Mahlstedt, Tobias*, Die verdeckte Befragung des Beschuldigten im Auftrag der Polizei. Informelle Informationserhebung und Selbstbelastungsfreiheit. Berlin 2011.

*Mähring, Matthias*, Das Recht auf informationelle Selbstbestimmung im europäischen Gemeinschaftsrecht. EuR 1991, 369–375.

*Mallmann, Klaus-Michael*, Die V-Leute der Gestapo. In: Gerhard Paul/Klaus-Michael Mallmann (Hrsg.), Die Gestapo. Mythos und Realität. Darmstadt 2003, S. 268–287.

*Mallmann, Otto*, Zielfunktionen des Datenschutzes – Schutz der Privatsphäre, korrekte Information. Mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen. Frankfurt a.M. 1977.

*Mandelartz, Herbert/Grotelüschen, Henning*, Das Internet und die Rechtsprechung des BVerfG zur Öffentlichkeitsarbeit der Regierung. NVwZ 2004, 647–650.

*Margulis, Stephen T.*, On the Status and Contribution of Westin's and Altman's Theories of Privacy. 59 Journal of Social Issues 2 (2003), 411–429.

– Privacy as a Social Issue and Behavioral Concept. 59 Journal of Social Issues 2 (2003), 243–260.

*Maschmann, Frank*, Compliance versus Datenschutz. NZA-Beilage 2012, 50–58.

*Masing, Johannes*, Die Ambivalenz von Freiheit und Sicherheit. JZ 2011, 753–758.

– Herausforderungen des Datenschutzes. NJW 2012, 2305–2312.

*Maurauhn, Thilo/Meljnik, Konstantin*, Kapitel 16: Privat- und Familienleben. In: Rainer Grote/Thilo Maurauhn (Hrsg.), EMRK/GG Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz. Tübingen 2006, S. 744–816.

*Mayer-Schönberger, Viktor*, Delete: The Virtue of Forgetting in the Digital Age. Princeton 2009.

Medienpädagogischer Forschungsverbund Südwest (Hrsg.), JIM 2011. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Stuttgart 2011.

*Mehde, Veith*, Datenschutz. In: Sebastian Heselhaus/Carsten Nowak (Hrsg.), Handbuch der Europäischen Grundrechte. München 2006, S. 608–630.

*Mengel, Hans-Joachim*, Die Datenschutzkonvention des Europarats vom 28. Januar 1981 – Einführung und Übersetzung. EuGRZ 1981, 376–381.

*Menzel, Jörg/Müller-Terpitz, Ralf* (Hrsg.), Verfassungsrechtsprechung. Ausgewählte Entscheidungen des Bundesverfassungsgerichts in Retrospektive. 2. Aufl. Tübingen 2011.

*Mertens, Peter*, Integrierte Informationsverarbeitung 1: Operative Systeme in der Industrie. 18. Aufl. Wiesbaden 2013.

*Meyer-Ladewig, Jens*, Europäische Menschenrechtskonvention – Handkommentar. 3. Aufl. Baden-Baden, Basel 2011.

*Michael, Lothar/Morlok, Martin*, Grundrechte, 2. Aufl. Baden-Baden 2010.

*Möller, Mirko*, Rechtsfragen im Zusammenhang mit dem Postident-Verfahren. NJW 2005, 1605–1609.

– Das Ende der urheberrechtlichen Massenabmahnungen? NJW 2011, 2560–2562.

*Müller-Enbergs, Helmut/BStU* (Hrsg.), Die inoffiziellen Mitarbeiter. Berlin 2008.

Münchner Kreis (Hrsg.), Zukunftsbilder der digitalen Welt. Nutzerperspektiven im internationalen Vergleich, abrufbar unter http://www.zukunft-ikt.de; [Stand: 28.4.2013]. 2011.

Munzinger/Duden, Großes Wörterbuch der deutschen Sprache, aktualisierte Online-Ausgabe 2009.

National Security Agency, 60 Years of Defending Our Nation, 2012, abrufbar unter http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf [Stand: 28.2.2014].

*Nehm, Kay*, Ein Jahr danach. Gedanken zum 11. September 2001. NJW 2002, S. 2665–2671

*Nolte, Norbert*, Zum Recht auf Vergessen im Internet. Von digitalen Radiergummis und anderen Instrumenten. ZRP 2011, 236–240.

*O'Reilly, Tim*, What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software, 2005, abrufbar unter http://oreilly.com/web2/archive/what-is-web-20.html (Stand: 28.3.2014).

OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2001.

– The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines. OECD Digital Economy Papers, No. 176, 2011, abrufbar unter http://dx.doi.org/10.1787/5kgf09z90c31-en [Stand: 29.2.2014].

– Report on the Implementation of the OECD Recommendation on Crossborder Co-operation in the Enforcement of Laws Protecting Privacy. OECD Digital Economy Papers No. 178, 2011, abrufbar unter http://dx.doi.org/10.1787/5kgdpm9wg9xs-en [Stand: 28.2.2014].

*Ohlenburg, Anna*, Die neue EU-Datenschutzrichtlinie 2002/58/EG. Auswirkungen und Neuerungen für elektronische Kommunikation. MMR 2003, 82–86.

*Peilert, Andreas*, BVerfGE 109, 279 – Großer Lauschangriff. Die Abwägungsfestigkeit des absolut geschützten Kernbereichs privater Lebensgestaltung gegenüber Strafverfolgungsinteressen. In: Jörg Menzel/Ralf Müller-Terpitz (Hrsg.), Verfassungsrechtsprechung. Ausgewählte Entscheidungen des Bundesverfassungsgerichts in Retrospektive. 2. Aufl. Tübingen 2011, S. 733–739.

*Perreng, Martina*, Datenschutz ist ein Grundrecht – auch im Arbeitsverhältnis. In: Jan-Hinrik Schmidt/Thilo Weichert (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn 2012, S. 206–213.

*Peters, Anne*, Einführung in die Europäische Menschenrechtskonvention. Mit rechtsvergleichenden Bezügen zum deutschen Grundgesetz. München 2003.

*Pieroth, Bodo/Schlink, Bernhard/Kingreen, Thorsten/Poscher, Ralf,* Grundrechte Staatsrecht II. Mit ebook: Lehrbuch, Entscheidungen, Gesetzestexte. 29. Aufl. Heidelberg 2013.

*Podlech, Adalbert*, Individualdatenschutz und Systemdatenschutz. In: Klaus Brückner/Gerhard Dalichau (Hrsg.), Beiträge zum Sozialrecht – Festgabe für Hans Grüner. Percha am Starnberger See, Kempfenhausen am Starnberger See 1982, S. 451–462.

*Polzin, Monika*, Das Rangverhältnis von Verfassungs- und Unionsrecht nach der neuesten Rechtsprechung des BVerfG. JuS 2012, 1–6.

*Punie, Yves/Lusoli, Wainer/Centeno, Clara/Misuraca, Gianluca/Broster, David* (Hrsg.), The Impact of Social Computing on the EU Information Society and Economy, 2009, abrufbar unter http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2819 [Stand: 28.2.2014].

*Reding, Viviane*, Sieben Grundbausteine der europäischen Datenschutzreform. ZD 2012, 195–198.

*Regan, Priscilla M.*, Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows. 59 Journal of Social Issues 2 (2003), 263–282.

*Rehof, Lars Adam*, Article 12. In: Asbjørn Eide/Gudmundur Alfredsson/Göran Melander/Lars Adam Rehof/Allan Rosas (Hrsg.), The Universal Declaration of Human Rights: A Commentary. Dordrecht 1992, S. 187–201.

*Reimer, Helmut*, Report. DuD 2010, 730–736.

*Rex, Constantin Graf von*, Gesetzgebung zum Beschäftigtendatenschutz in der BRD – Chronik einer langwierigen Suche nach der notwendigen Lösung. ZD-Aktuell 2013, 03565.

*Rogall, Klaus*, Informationseingriff und Gesetzesvorbehalt im Strafprozessrecht. Tübingen 1992.

*Rogall-Grothe, Cornelia*, Ein neues Datenschutzrecht für Europa. ZRP 2012, 193.

*Rönnau, Thomas*, Grundwissen – Strafrecht: Der strafrechtliche Rechtsgutsbegriff. JuS 2009, 209–211.

*Rosengarten, Carsten/Römer, Sebastian*, Der „virtuelle verdeckte Ermittler" in sozialen Netzwerken und Internetboards. NJW 2012, 1764–1768.

*Roßnagel, Alexander*, Einleitung. In: Alexander Roßnagel/Ralf-Bernd Abel (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, S. 2–40.

– Datenschutz in einem informatisierten Alltag – Gutachten im Auftrag der Friedrich-Ebert-Stiftung. Bonn 2007.

*Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen*, Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Innern. Berlin 2001.

*Roßnagel, Alexander/Wedde, Peter/Hammer, Volker/Pordesch, Ulrich*, Digitalisierung der Grundrechte. Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik. Opladen 1990.

*Roxin, Claus*, Strafrecht Allgemeiner Teil, Band I: Grundlagen. Der Aufbau der Verbrechenslehre. 4. Aufl. München 2006.

*Rudolf, Walter*, Informationelle Selbstbestimmung. In: Detlef Merten/Hans-Jürgen Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band III: Grundrechte in Deutschland: Allgemeine Lehren II. Heidelberg 2009, S. 233–289.

*Säcker, Franz Jürgen*, Münchener Kommentar zum Bürgerlichen Gesetzbuch. Band 1: Allgemeiner Teil. 3. Aufl. München 1993 (zit. MüKo-*Bearbeiter*).

*Schäfer, Bernhard*, Die Individualbeschwerde nach dem Fakultativprotokoll zum Zivilpakt. Ein Handbuch für die Praxis. 2. Aufl. Berlin 2007.

*Schmidt, Walter*, Die bedrohte Entscheidungsfreiheit. JZ 1974, 241–250.

*Schneider, Jochen*, Datenschutz-Grundverordnung. ITRB 2012, 180–186.

*Schneider, Jochen/Härting, Niko*, Wird der Datenschutz nun endlich internettauglich? Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht. ZD 2012, 199–203.

*Schulz, Sönke E./Hoffmann, Christian*, Grundrechtsrelevanz staatlicher Beobachtungen im Internet. CR 2010, 131–136.

*Schwartz, Paul M.*, Preemption and Privacy. 118 Yale L. J. (2009), 902–947.

*Schwarze, Jürgen*, Soft Law im Recht der Europäischen Union. EuR 2011, 3–18.

*Seidl, Alexander/Beyvers, Eva*, Virtuelle verdeckte Ermittler? – Überblick über polizeiliche Ermittlungen in sozialen Netzwerken. Juris AnwZert ITR 15/2011 Anm. 3.

*Seipel, Peter*, Sweden. In: Peter Blume/Ahti E. Saarenpää (Hrsg.), Nordic Data Protection Law. Uppsala 2001, S. VII, 244.

*Sieber, Ulrich*, Informationsrecht und Recht der Informationstechnik – Die Konstituierung eines Rechtsgebietes in Gegenstand, Grundfragen und Zielen. NJW 1989, 2569–2580.

– Grenzen des Strafrechts – Grundlagen und Herausforderungen des neuen strafrechtlichen Forschungsprogramms am Max-Planck-Institut für ausländisches und internationales Strafrecht. 119 ZStW 1 (2007), 1–68.

– Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im „Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten". NStZ 2009, 353–364.

– Technische Grundlagen. In: Thomas Hoeren/Ulrich Sieber (Hrsg.), Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs. München 2011 (30. Ergänzungslieferung), Teil 1.

– Cybercrime und Strafrecht in der globalen Informationsgesellschaft. In: Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. (Hrsg.), Jahresbericht 2011. München 2012, S. 37–42.

– Gutachten C: Straftaten und Strafverfolgung im Internet. In: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages. München 2012, C 9–C 157.

– Straftaten und Strafverfolgung im Internet. NJW-Beilage 2012, 86–90.

*Siemen, Birte*, Datenschutz als europäisches Grundrecht. Berlin 2006.

*Simitis, Spiros*, Chancen und Gefahren der elektronischen Datenverarbeitung. NJW 1971, 673–682.

– Datenschutz: Voraussetzung oder Ende der Kommunikation? In: Norbert Horn/Klaus Luig/Alfred Söllner (Hrsg.), Europäisches Rechtsdenken in Geschichte und Gegenwart. Festschrift für Helmut Coing zum 70. Geburtstag. München 1982, Band II, S. 495–520.

– Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. NJW 1984, 394–405.

– Bundesdatenschutzgesetz. 7. Aufl. Baden-Baden 2011 (zit. Simitis-*Bearbeiter*).

*Simitis, Spiros/Dammann, Ulrich/Geiger, Hansjörg/Mallmann, Otto/Reh, Hans-Joachim* (Hrsg.), Dokumentation zum Bundesdatenschutzgesetz. Bund – Länder – Kirchen – Ausland und Internationales: Rechts- und Verwaltungsvorschriften. Entscheidungssammlung. Beschlüsse der Datenschutzaufsichtsinstanzen, Band 2 D: Ausland und Internationales. 50. Lfg. Baden-Baden November 2010.

*Spiecker gen. Döhmann, Indra*, Kommt das „Volkszählungsurteil" nun durch den EuGH? – Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon. JZ 2011, 169–177.

*Spindler, Gerald*, Gutachten F, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung. In: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages. München 2012, F 9–F 132.

Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages München 2012. Bd. II/2. Sitzungsberichte: Diskussion und Beschlussfassung. München 2012.

*Steinmüller, Wilhelm* (Hrsg.), Verdatet und vernetzt – sozialökologische Handlungsspielräume in der Informationsgesellschaft. Frankfurt a.M. 1988.

– Informationswissenschaftliche und technische Voraussetzungen einer neuen Informationsordnung. NfD 1993, 215–226.

*Steinmüller, Wilhelm/Lutterbeck, Bernd/Mallmann, Christoph/Harbort, U./Kolb, G./Schneider, J.*, Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern. Anl. 1 zu Bundestags-Drs. VI/3826, 1971.

*Stone-Romero, Eugene/Stone, Dianna L./Hyatt, David*, Personnel Selection Procedures and Invasion of Privacy. 59 Journal of Social Issues 2 (2003), 343–368.

*Streinz, Rudolf*, Europarecht, 9. Aufl. Heidelberg u.a. 2012.

– EUV/AEUV. Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union. 2. Aufl. München 2012 (zit. Streinz-*Bearbeiter*).

*Sumner, Chris/Byers, Alison/Boochever, Rachel/Park, Gregory J.,* Predicting Dark Triad Personality Traits from Twitter usage and a linguistic analysis of Tweets, 2012, abrufbar unter: http://www.onlineprivacyfoundation.org/research_/Sumner_Predicting_Dark_Triad_Traits_from_Twitter_Usage_V5.pdf [Stand: 28.2.2014].

*Taeger, Jürgen/Gabel, Detlev*, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG. Frankfurt a.M. 2010 (zit. Taeger/Gabel-*Bearbeiter*).

*Tinnefeld, Marie-Theres*, Das Erbe Montesquieus, Europäisierung und Informationsgesellschaft. MMR 2006, 23–27.

– Datenschutz in der Union. DuD 2012, 364.

*Tinnefeld, Marie-Theres/Ehmann, Eugen/Gerling, Rainer W.*, Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht. 4. Aufl. München u.a. 2005.

*Tinnefeld, Marie-Theres/Schild, Hans-Hermann*: Datenschutz in der Union – Gelungene oder missglückte Gesetzesentwürfe? DuD 2012, 312–317.

*Tinnefeld, Marie-Theres/Schmale, Wolfgang*, Öffentlichkeit, Geheimhaltung und Privatheit. Sichtweisen im Raum der europäischen Geschichte und in Cyberia. MMR 2011, 786–791.

*Tripathi, Nachiketa*, Privacy and Control: Are They Related? Psychological Studies 55 (2010), 108–117.

*Trute, Hans-Heinrich*, Der Schutz personenbezogener Informationen in der Informationsgesellschaft. JZ 1998, 822–831.

*Ulbig, Ellen/Hertel, Rolf F./Böl, Gaby-Fleur* (Hrsg.), Kommunikation von Risiko und Gefährdungspotenzial aus Sicht verschiedener Stakeholder. Abschlussbericht. Berlin 2010.

Verbraucherzentrale Bundesverband e.V. (Hrsg.), Löschen von Accounts und Kundenkonten. Eine Untersuchung des Projekts „Verbraucherrechte in der digitalen Welt" des Verbraucherzentrale Bundesverbandes. Berlin 2011.

*Vesting, Thomas*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung. In: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen. Berlin u.a. 2008, S. 1–35.

*von Lewinski, Kai*, Geschichte des Datenschutzrechts von 1600 bis 1977. In: Felix Arndt/Nicole Betz/Anuscheh Farahat/Matthias Goldmann/Matthias Huber/Rainer Keil/Petra Lea Láncos/Jan Philip Schaefer/Maja Smrkolj/Franziska Sucker/Stefanie Valta (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Öffentliches Recht Heidelberg 2008. Baden-Baden 2009, S. 196–220.

– Europäisierung des Datenschutzrechts. DuD 2012, 564–570.

*von Mangoldt, Hermann/Klein, Friedrich/Starck, Christian*, Kommentar zum Grundgesetz, Band 1: Präambel, Art. 1–19. 6. Aufl. München 2010 (zit. vMKS-*Bearbeiter*).

*von Zezschwitz, Friedrich*, Konzept der normativen Zweckbegrenzung. In: Alexander Roßnagel/Ralf-Bernd Abel (Hrsg.), Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, S. 219–268.

*Wagner, Franc/Huerkamp, Matthias/Jockisch, Heike*/*Graumann, Carl F.*, Sprachlich realisierte soziale Diskriminierungen: empirische Überprüfung eines Modells expliziter Diskriminierung. Heidelberg, Mannheim 1990.

*Warren, Samuel/Brandeis, Louis*, The Right to Privacy. 4 Harv. L. Rev. 5 (1890), 193–220.

*Weber, Max*, Wirtschaft und Gesellschaft. Grundriß der verstehenden Soziologie. 5. Aufl. Tübingen 1972.

*Weichert, Thilo*, Dauerbrenner BDSG-Novellierung. DuD 2010, 7–14.

– Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz? Zugleich Besprechung von Bull, Hans Peter, Netzpolitik: Freiheit und Rechtsschutz im Internet. DuD 2013, 246–249.

*Westin, Alan F.*, Privacy and Freedom, New York 1967.

– Social and Political Dimensions of Privacy. 59 Journal of Social Issues 2 (2003), 431–453.

*Westphal, Dietrich*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten – Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft". EuR 2006, 706–723.

*Wildhaber, Luzius/Breitenmoser, Stephan*, Art. 8 EMRK. In: Wolfram Karl (Hrsg.), Internationaler Kommentar zur Europäischen Menschenrechtskonvention. 13. Erg. Lfg. Köln u.a. September 2010, S. 1–264.

*Wolf, Roland*, Beschäftigtendatenschutz ist Teil guter Unternehmensführung. In: Jan-Hinrik Schmidt/Thilo Weichert (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn 2012, S. 199–205.

*Zimmer, Michael*, Privacy Protection in the Next Digital Decade: "Trading Up" or a "Race to the Bottom"? In: Berin Szoka/Adam Marcus (Hrsg.), The Next Digital Decade. Essays on the Future of the Internet. Washington D.C. 2010, S. 477–482.

# Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht

Die zentralen Veröffentlichungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht werden in Zusammenarbeit mit dem Verlag Duncker & Humblot in den folgenden vier Unterreihen der „Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht“ vertrieben:

- „Strafrechtliche Forschungsberichte“,
- „Kriminologische Forschungsberichte“,
- „Interdisziplinäre Forschungen aus Strafrecht und Kriminologie“ sowie
- „Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung“.

Diese Publikationen können direkt über das Max-Planck-Institut unter <www.mpicc.de> oder über den Verlag Duncker & Humblot unter <www.duncker-humblot.de> erworben werden.

Darüber hinaus erscheinen im Hausverlag des Max-Planck-Instituts in der Unterreihe „research in brief“ zusammenfassende Kurzbeschreibungen von Forschungsergebnissen und in der Unterreihe „Arbeitsberichte“ Veröffentlichungen vorläufiger Forschungsergebnisse. Diese Veröffentlichungen können über das Max-Planck-Institut bezogen werden.

Detaillierte Informationen zu den einzelnen Publikationen des Max-Planck-Instituts für ausländisches und internationales Strafrecht sind unter <www.mpicc.de> abrufbar.

---

The main research activities of the Max Planck Institute for Foreign and International Criminal Law are published in the following four subseries of the “Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht” (Research Series of the Max Planck Institute for Foreign and International Criminal Law), which are distributed in cooperation with the publisher Duncker & Humblot:

- “Strafrechtliche Forschungsberichte” (Reports on Research in Criminal Law),
- “Kriminologische Forschungsberichte” (Reports on Research in Criminology),
- “Interdisziplinäre Forschungen aus Strafrecht und Kriminologie” (Reports on Interdisciplinary Research in Criminal Law and Criminology), and
- “Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung” (Collection of Foreign Criminal Laws in German Translation).

These publications can be ordered from the Max Planck Institute at <www.mpicc.de> or from Duncker & Humblot at <www.duncker-humblot.de>.

Two additional subseries are published directly by the Max Planck Institute for Foreign and International Criminal Law: “research in brief” contains short reports on results of research activities, and “Arbeitsberichte” (working materials) present preliminary results of research projects. These publications are available at the Max Planck Institute.

Detailed information on all publications of the Max Planck Institute for Foreign and International Criminal Law can be found at <www.mpicc.de>.

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aus dem strafrechtlichen Veröffentlichungsprogramm:

S 128.1.1 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
**National Criminal Law in a Comparative Legal Context**
Volume 1.1: Introduction to National Systems
2013 • 314 Seiten • ISBN 978-3-86113-822-8 € 40,00

S 128.1.2 Volume 1.2: Introduction to National Systems
2013 • 363 Seiten • ISBN 978-3-86113-826-6 € 43,00

S 128.1.3 Volume 1.3: Introduction to National Systems
2014 • 297 Seiten • ISBN 978-3-86113-818-1 € 40,00

S 128.1.4 Volume 1.4: Introduction to National Systems
2014 • 391 Seiten • ISBN 978-3-86113-810-5 € 43,00

S 128.2.1 *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
**National Criminal Law in a Comparative Legal Context**
Volume 2.1: General limitations on the application of criminal law
2011 • 399 Seiten • ISBN 978-3-86113-834-1 € 43,00

S 128.3.1 *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
**National Criminal Law in a Comparative Legal Context**
Volume 3.1: Defining criminal conduct
2011 • 519 Seiten • ISBN 978-3-86113-833-4 € 46,00

S 114.1 *Ulrich Sieber/Karin Cornils* (Hrsg.)
**Nationales Strafrecht in rechtsvergleichender Darstellung**
– Allgemeiner Teil –
Band 1: Grundlagen
2009 • 790 Seiten • ISBN 978-3-86113-849-5 € 55,00

S 114.2 Band 2: Gesetzlichkeitsprinzip – Internationaler Geltungsbereich – Begriff und Systematisierung der Straftat
2008 • 470 Seiten • ISBN 978-3-86113-860-0 € 41,00

S 114.3 Band 3: Objektive Tatseite – Subjektive Tatseite – Strafbares Verhalten vor der Tatvollendung
2008 • 490 Seiten • ISBN 978-3-86113-859-4 € 41,00

S 114.4 Band 4: Tatbeteiligung – Straftaten in Unternehmen, Verbänden und anderen Kollektiven
2010 • 527 Seiten • ISBN 978-3-86113-842-6 € 45,00

S 114.5 Band 5: Gründe für den Ausschluss der Strafbarkeit – Aufhebung der Strafbarkeit – Verjährung
2010 • 718 Seiten • ISBN 978-3-86113-841-9 € 55,00

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aktueller Publikationen aus dem kriminologischen Veröffentlichungsprogramm:

K 167 *Christopher Murphy*
**"Come in Spinner" – Money Laundering in the Australian Casino Industry**
Berlin 2014 • 152 Seiten • ISBN 978-3-86113-250-9 € 29,00

K 166 *Ramin Tehrani*
**Die „Smart Sanctions" im Kampf gegen den Terrorismus und als Vorbild einer präventiven Vermögensabschöpfung**
Berlin 2014 • 256 Seiten • ISBN 978-3-86113-247-9 € 35,00

K 165 *Daniela Cernko*
**Die Umsetzung der CPT-Empfehlungen im deutschen Strafvollzug**
Eine Untersuchung über den Einfluss des Europäischen Komitees zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe auf die deutsche Strafvollzugsverwaltung
Berlin 2014 • 455 Seiten • ISBN 978-3-86113-246-2 € 39,00

K 164 *Franziska Kunz*
**Kriminalität älterer Menschen**
Beschreibung und Erklärung auf der Basis von Selbstberichtsdaten
Berlin 2014 • 387 Seiten • ISBN 978-3-86113-244-8 € 35,00

K 163 *David Jensen*
**Maras**
A study of their origin, international impact, and the measures taken to fight them
Berlin 2013 • 245 Seiten • ISBN 978-3-86113-243-1 € 35,00

K 161 *Gunda Wößner, Roland Hefendehl, Hans-Jörg Albrecht* (Hrsg.)
**Sexuelle Gewalt und Sozialtherapie**
Bisherige Daten und Analysen zur Längsschnittstudie „Sexualstraftäter in den sozialtherapeutischen Abteilungen des Freistaates Sachsen"
Berlin 2013 • 274 Seiten • ISBN 978-3-86113-241-7 € 35,00

K 159 *Andreas Armborst*
**Jihadi Violence**
A study of al-Qaeda's media
Berlin 2013 • 266 Seiten • ISBN 978-3-86113-119-9 € 35,00

K 158 *Martin Brandenstein*
**Auswirkungen von Hafterfahrungen auf Selbstbild und Identität rechtsextremer jugendlicher Gewalttäter**
Berlin 2012 • 335 Seiten • ISBN 978-3-86113-118-2 € 35,00

K 157 *Ghassem Ghassemi*
**Criminal Policy in Iran Following the Revolution of 1979**
A Comparative Analysis of Criminal Punishment and Sentencing in Iran and Germany
Berlin 2013 • 265 Seiten • ISBN 978-3-86113-116-8 € 35,00