Speichern – Verwerten – Löschen: Zur zeitlichen Dimension des Informationsmanagements in Unternehmen

DISSERTATION
der Universität St. Gallen,
Hochschule für Wirtschafts-,
Rechts- und Sozialwissenschaften
sowie Internationale Beziehungen (HSG)
zur Erlangung der Würde eines
Doktors der Rechtswissenschaft

vorgelegt von

Patrick Eggimann

von

Zürich

Genehmigt auf Antrag der Herren

Prof. Dr. Thomas Geiser

und

Prof. Dr. Florent Thouvenin

Dissertation Nr. 4346

J.E. Wolfensberger AG, Birmensdorf 2015

Die Universität St. Gallen, Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften sowie Internationale Beziehungen (HSG), gestattet hiermit die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

St. Gallen, den 22. Oktober 2014

Der Rektor:

Prof. Dr. Thomas Bieger

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	anderer Ansicht
ABl	Amtsblatt der Europäischen Union
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AJP	Aktuelle Juristische Praxis, Zürich/St. Gallen
a.M.	anderer Meinung
aOR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 14. Juni 1981, SR 220
Art.	Artikel
Aufl.	Auflage
AuG	Bundesgesetz vom 16. Dezember 2005 über die Ausländerinnen und Ausländer, SR 142.20
BAR	Schweizerisches Bundesarchiv
BAWI	Bundesamt für Aussenwirtschaft
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
Bd.	Band
BDSG	Bundesdatenschutzgesetz vom 20. Dezember 1990, Deutschland
BezGer	Bezirksgericht
BGA	Bundesgesetz über die Archivierung vom 26. Juni 1998, SR 152.1
BGB	Bürgerliches Gesetzbuch, vom 18. August 1896, Deutschland
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BGer	Bundesgericht
BGH	Bundesgerichtshof, Deutschland
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 17. Dezember 2004, SR 152.3
BPDV	Verordnung über den Schutz von Personendaten des Bundespersonals vom 26. Oktober 2011, SR 172.220.111.4
BPG	Bundespersonalgesetz vom 24. März 2000, SR 172.220.1
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000, SR 780.1
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
BVerfG	Bundesverfassungsgericht, Deutschland

BVerfGE	Entscheide des (deutschen) Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997, SR 120
bzw.	beziehungsweise
CNIL	Commission Nationale de l'Informatique et des Libertés
CR	Computer und Recht, Köln
CRM	Customer-Relationship-Management
DBG	Bundesgesetz über die direkte Bundessteuer vom 14. Dezember 1990, SR 642.11
DBW	Die Betriebswirtschaft, Stuttgart
ders.	derselbe
d.h.	das heisst
digma	Zeitschrift für Datenrecht und Informationssicherheit, Zürich
DIN	Deutsches Institut für Normung
Diss.	Dissertation
DOMEA	Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1
DVR	Datenverarbeitung im Recht, München
E.	Erwägung
E BÜPF	Entwurf BÜPF, BBl 2013 2683
Ed(s).	Editor(s)
ed.	Edition
éd.	édition
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EIDI-V	Verordnung des EFD über elektronische Daten und Informationen vom 11. Dezember 2009, SR 641.201.511
Einl.	Einleitung
ENISA	European Network and Information Security Agency
Erw.	Erwägung
ESOMAR	European Society for Opinion and Marketing Research
et al.	*et alii*
etc.	*et cetera*
EuGH	Europäischer Gerichtshof

f./ff.	folgende/fortfolgende
FAZ	Frankfurter Allgemeine Zeitung
FDV	Verordnung über Fernmeldedienste vom 9. März 2007, SR 784.101.1
FMedV	Fortpflanzungsmedizinverordnung vom 4. Dezember 2000, SR 810.112.2
FMG	Fernmeldegesetz vom 30. April 1997, SR 784.10
FTC	Federal Trade Commission
GeBüV	Verordnung über die Führung und Aufbewahrung der Geschäftsbücher vom 24. April 2002, SR 221.431
GmbH	Gesellschaft mit begrenzter Haftung
GPS	Global Positioning System
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil, München
Hrsg.	Herausgeber
IAO	Frauenhofer-Institut für Arbeitswirtschaft und Organisation
ID	Identifikator
IP	Internet Protocol
IPRG	Bundesgesetz über das Internationale Privatrecht vom 18. Dezember 1987, SR 291
ISO	International Organization for Standardization
i.V.m.	in Verbindung mit
JIPITEC	Journal of Intellectual Property, Information Technology and E-Commerce Law
KGTG	Bundesgesetz über den internationalen Kulturgütertransfer vom 20. Juni 2003, SR 444.1
LaaS	Law as a Service
LugÜ	Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen vom 30. Oktober 2007, SR 0.275.12
m.H.	mit Hinweis(en)
MMR	Multimedia und Recht, München
MoReq	Model Requirements for the Management of Electronic Records
m.w.H.	mit weiteren Hinweisen
MWSTG	Bundesgesetz über die Mehrwertsteuer vom 12. Juni 2009, SR 641.20
N	Note
NASA	National Aeronautics and Space Administration

NBibG	Bundesgesetz über die Schweizerische Nationalbibliothek vom 18. Dezember 1992, SR 432.21
NJW	Neue Juristische Wochenschrift, München
No.	Number
Nr.	Nummer
NZZ	Neue Zürcher Zeitung
OAIS	Offenes Archiv-Informations-System
OECD	Organisation for Economic Co-Operation and Development
OJ	Official Journal of the European Union (Amtsblatt)
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220
o.S.	ohne Seitenangabe
PET	Privacy Enhancing Technologies
PNAS	Proceedings of the National Academy of Sciences of the United States of America, Washington, DC
resp.	Respektive
RL	Richtlinie
Rn.	Randnote
RSDA	Revue suisse de droit des affaires, Zürich
RTVG	Bundesgesetz über Radio und Fernsehen vom 24. März 2006, SR 784.40
Rz.	Randziffer
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs vom 11. April 1889, SR 281.1
SECO	Staatssekretariat für Wirtschaft
SHAB	Schweizerisches Handelsamtsblatt
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht, Zürich
SIGOIS	Special Interest Group on Office Information Systems
SJZ	Schweizerische Juristen-Zeitung, Zürich
sog.	sogenannt
SR	Systematische Sammlung des Bundesrechts
SRG	Schweizerische Radio- und Fernsehgesellschaft
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
StHG	Bundesgesetz über die Harmonisierung der direkten Steuern der Kantone und Gemeinden vom 14. Dezember 1990, SR 642.14
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007, SR 312.0

SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht, Zürich
u.a.	unter anderem
UEK	Unabhängige Expertenkommission Schweiz – Zweiter Weltkrieg
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte vom 9. Oktober 1992, SR 231.1
URL	Uniform Resource Locator
USC	Code of Laws of the United States of America
USD	US-Dollar
UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986, SR 241
v./vs.	*versus*
VBGA	Verordnung zum Bundesgesetz über die Archivierung vom 8. September 1999, SR 152.11
VE	Vorentwurf
VGG	Bundesgesetz über das Bundesverwaltungsgericht vom 17. Juni 2005, SR 173.32
Vol.	Volume
VPB	Verwaltungspraxis der Bundesbehörden
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001, SR 780.11
VZV	Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr vom 27. Oktober 1976, SR 741.51
WM	Zeitschrift für Wirtschafts- und Bankrecht, Frankfurt am Main
ZBJV	Zeitschrift des Bernischen Juristenvereins, Bern
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210
zit.	zitiert
ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008, SR 272
ZSR	Zeitschrift für Schweizerisches Recht, Basel
ZUM	Zeitschrift für Urheber- und Medienrecht, Baden-Baden
ZVW	Zeitschrift für Vormundschaftswesen, Zürich

Literaturverzeichnis

AEBI-MÜLLER REGINA E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Bern 2005

ALBERS MARION, Grundlagen des Verwaltungsrechts, Hoffmann-Riem Wolfgang/Schmidt-Assmann Eberhard/Vosskuhle Andreas (Hrsg.), Band 2, München 2006 (zit.: Grundlagen)

ALBERS MICHAEL J., Human–Information Interaction and Technical Communication: Concepts and Frameworks, Hershey, PA 2012 (zit.: Human-Information)

ALDERMAN ELLEN/KENNEDY CAROLINE, The right to Privacy, New York 1995

ALLEN ANITA L., Privacy in American Law, in: Rössler Beate (Ed.) Privacies: Philosophical Evaluations, Stanford University Press 2004, 19-39

ALTMAN IRWIN, The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding, Monterey, CA 1975

AMBROSE MEG LETA, It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten, Stanford Technology Law Review, Vol. 16, No. 2, 2013, 369-422

AMELUNG ULRICH, Der Schutz der Privatheit im Zivilrecht: Schadenersatz und Gewinnabschöpfung bei Verletzung des Rechts auf Selbstbestimmung über personenbezogene Informationen im deutschen, englischen und US-amerikanischen Recht, Tübingen 2002

AMMANN MARTIN, Datenschutz im Bank- und Kreditbereich: Eine Studie zu einem Schweizer Datenschutzgesetz unter Berücksichtigung ausländischer Erfahrungen – insbesondere in der BRD und in den USA, Zürich 1987

ANDERSON SIMON P., Advertising on the Internet, in: Peitz Martin/Waldfogel Joel (Eds.), The Oxford Handbook of the Digital Economy, Oxford University Press 2012, 355-396

ARNET RUTH, Freiheit und Zwang beim Vertragsschluss: Eine Untersuchung zu den gesetzlichen Kontrahierungspflichten und weiteren Schranken der Vertragsabschlussfreiheit im schweizerischen Recht, Bern 2008

ASSMANN ALEIDA, Der lange Schatten der Vergangenheit, München 2006 (zit.: Vergangenheit)

ASSMANN JAN, Das kulturelle Gedächtnis: Schrift, Erinnerung und politische Identität in frühen Hochkulturen, 6. Aufl., München 2007 (zit.: Gedächtnis)

ATKINSON JOHN W., Erwartungstheorie und Utilitätstheorie, in: Thomae Hans (Hrsg.), Die Motivation menschlichen Handelns, 5. Aufl., Köln/Berlin 1969, 462-473

AUER ANDREAS/MALINVERNI GIORGIO/HOTTELIER MICHEL, Droit constitutionnel suisse, 3e éd., Vol. 2, Les droits fondamentaux, Berne 2013

AUGUSTIN SIEGFRIED, Information als Wettbewerbsfaktor: Informationslogistik – Herausforderung an das Management, Zürich 1990

AZZABI SOFIAN, L'identification numérique: preuve et responsabilité, Publications de l'Institut suisse de droit comparé, L'individue face aux nouvelles technologies: Surveillance, identification et suivi, Genève/Zurich/Bâle 2005

BÄCHLI MARC, Das Recht am eigenen Bild: Die Verwendung von Personenbildern in den Medien, in der Kunst, der Wissenschaft und in der Werbung aus Sicht der abgebildeten Person, Basel 2002

BACKHAUS KLAUS/BLECHSCHMIDT BORIS, Fehlende Werte und Datenqualität: Eine Simulationsstudie am Beispiel der Kausalanalyse, DBW 2/2009, 265-287

BAERISWYL BRUNO, PET – ein Konzept harrt der Umsetzung, digma 1/2012, 18-21

BÄHLER REGULA, Ungefragte Momentaufnahmen, Medialex (2) 2012, 55-62

BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2e éd., Berne 2011

BASTON-VOGT MARION, Der sachliche Schutzbereich des zivilrechtlichen allgemeinen Persönlichkeitsrechts, Tübingen 1997

BAUKNECHT KURT/FORSTMOSER PETER/ZEHNDER CARL AUGUST (Hrsg.), Rechtsinformatik: Bedürfnisse und Möglichkeiten, Zürich 1984 (zit.: BAUKNECHT, in: ders./Forstmoser/Zehnder)

BAUMAN ZYGMUNT, Identity: Conversations with Benedetto Vecchi, Cambridge 2004

BAUMANN ROBERT, Mehr Datenschutz in Europa, digma 3/2013, 116-121

BEGLINGER JACQUES/BURGWINKEL DANIEL/LEHMANN BEAT/NEUENSCHWANDER PETER/WILDHABER BRUNO, Records Management: Leitfaden zur Compliance bei der Aufbewahrung von elektronischen Dokumenten in Wirtschaft und Verwaltung mit Checklisten, Mustern und Vorlagen, 2. Aufl., Zollikon 2008

BELSER EVA MARIA/EPINEY ASTRID/WALDMANN BERNHARD (Hrsg.), Datenschutzrecht, Bern 2001 (zit.: Autor, in: Belser/Epiney/Waldmann)

BELSER URS, Die Technikneutralität des Datenschutzgesetzes, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing: 20 Jahre Datenschutz in der Schweiz, Zürich/Basel/Genf 2012, 1-18

BENKLER YOCHAI, Siren Songs and Amish Children: Autonomy, Information and Law, New York University Law Review, Vol. 76, No. 1, 2001, 23-113

BERANEK ZANON NICOLE, Datenaufbewahrungspflichten vs. Datenlöschungspflichten: Kollision von BÜPF und DSG?, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 131-156

BERNSTEIN PETER L., Against the Gods: The Remarkable Story of Risk, New York 1996

BIAGGINI GIOVANNI, Bundesverfassung der Schweizerischen Eidgenossenschaft, Kommentar, Zürich 2007

BIAGGINI GIOVANNI/GÄCHTER THOMAS/KIENER REGINA (Hrsg.), Staatsrecht, Zürich/St.Gallen 2011 (zit: Autor, in: Biaggini/Gächter/Kiener)

BICK WOLFGANG/MÜLLER PAUL J., Informationssysteme und Informationsverhalten: soziologische Grundlagenforschung für eine Informationspolitik, Bundesministerium für Forschung und Technologie: Forschungsbericht ID 79-01, Eggenstein-Leopoldshafen 1979

BIRNHACK MICHAEL, Reverse Engineering Informational Privacy Law, Yale Journal of Law & Technology, Vol. 15, No. 2, 2013, 24-91

BONDALLAZ STÉPHANE, La protection des personnes et de leurs données dans les télécommunications: Analyse critique et plaidoyer pour un système en droit suisse, Zürich 2007

BONDOLFI ALBERTO, Zur «Privatsphäre» in sozialethischer Sicht: Einige Grundsatzüberlegungen zur ethischen Dimension des Datenschutzes, in: Baeriswyl Bruno/Rudin Beat (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, 127-141

BONFIELD LLOYD, American Law and the American Legal System, St. Paul, MN 2006

BORGHOFF UWE M./RÖDIG PETER/SCHEFFCZYK JAN/SCHMITZ LOTHAR, Langzeitarchivierung: Methoden zur Erhaltung digitaler Dokumente, Heidelberg 2003

BOSCHETTI PIETRO, Les Suisses et les Nazis: Le rapport Bergier pour tous, Carouge-Genève 2004

BOSTON CONSULTING GROUP, The Value of our Digital Identity, Liberty Global 2012

BRADSHAW SIMON/MILLARD CHRISTOPHER/WALDEN IAN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary University of London, Legal Studies Research Paper No. 63/2010

BRANDES HELMUT, Die Rechtsprechung des Bundesgerichtshofes zur GmbH, WM 1998, 1-19

BREITSCHMID PETER/KAMP ANNASOFIA, Persönlichkeitsschutz Verstorbener – Urheberpersönlichkeitsschutz im Besonderen, Successio 1/2011, 19-29

BRIDGELAND DAVID M./ZAHAVI RON, Business Modeling: A Practical Guide to Realizing Business Value, Burlington, MA 2009

BRIN DAVID, The Transparent Society, Reading, MA 1998

BRÜCKNER CHRISTIAN, Das Personenrecht des ZGB, Zürich 2000

BRÜHWILER JÜRG, Kommentar zum Einzelarbeitsvertrag, 2. Aufl., Bern 1996

BRUNNER ALEXANDER/GASSER DOMINIK/SCHWANDER IVO, Schweizerische Zivilprozessordnung (ZPO): Kommentar, Zürich/St. Gallen 2011 (zit.: Autor, in: Brunner/Gasser/Schwander)

BRUSATTI ALOIS, Was heisst Firmengeschichte?, in: Mosser Alois (Hrsg.), Corporate Identity und Geschichtsbewusstsein, Wien 1994

BUCHER ANDREAS, Natürliche Personen und Persönlichkeitsschutz, 4. Aufl., Basel 2009 (zit.: Persönlichkeitsschutz)

BUCHER EUGEN, Die Ausübung der Persönlichkeitsrechte: insbesondere die Persönlichkeitsrechte des Patienten als Schranke der ärztlichen Tätigkeit, Diss. Zürich 1956 (zit.: Persönlichkeitsrechte)

BÜCHLER ANDREA, Persönlichkeitsgüter als Vertragsgegenstand?, Von der Macht des Faktischen und der dogmatischen Ordnung, in: Honsell Heinrich/Portmann Wolfgang/Zäch Roger/Zobl Dieter (Hrsg.), Aktuelle Aspekte des Schuld- und Sachenrechts: Festschrift Rey, Zürich 2003, 177-195 (zit.: Persönlichkeitsgüter)

BÜCHLER ANDREA, Die Kommerzialisierung von Persönlichkeitsgütern: Zur Dialektik von Ich und Mein, in: Bork Reinhard/Taupitz Jochen/Wagner Gerhard (Hrsg.), Archiv für die civilistische Praxis, Band 206, Tübingen 2006, 300-351 (zit. Kommerzialisierung)

BULL HANS PETER, Gefühle der Menschen in der «Informationsgesellschaft» – Wie reagiert das Recht?, Baden-Baden 2011

BUNGARTEN THEO, Die Schwierigkeiten der Betriebswirtschaftslehre mit der Identität und Kultur, in: Janich Nina (Hrsg.), Unternehmenskultur und Unternehmensidentität: Wirklichkeit und Konstruktion, Wiesbaden 2005, 236-239

VON BÜREN ROLAND/MARBACH EUGEN/DUCREY PATRIK, Immaterialgüter- und Wettbewerbsrecht, 3. Aufl., Bern 2008

BURGSTALLER PETER/MINICHMAYR GEORG, E-Commerce-Recht, 2. Aufl., Wien 2011

BURKERT HERBERT, The Information Law Approach: An Exemplification, in: Gasser Urs (Ed.), Information Quality Regulation: Foundations, Perspectives, and Applications, Baden-Baden, 2004, 75-90 (zit.: Approach)

BURKERT HERBERT, Von künftigen Aufgaben des Informationsrechts, in: Meier-Schatz Christian J./Schweizer Rainer J. (Hrsg.), Recht und Internationalisierung, Zürich 2000, 155-173 (zit.: Aufgaben)

BURKERT HERBERT, Privacy-Enhancing Technologies: Typology, Critique, Vision, in: Agre Philip E./Rotenberg Marc (Eds.), Technology and Privacy: The New Landscape, Cambridge, MA 1997, 125-142 (zit.: PET)

BURT RONALD S., Structural Holes: The Social Structure of Competition, Cambridge, MA 1992

BYDLINSKI FRANZ, Fundamentale Rechtsgrundsätze: Zur rechtsethischen Verfassung der Sozietät, Wien 1988

BYFORD KATRIN SCHATZ, Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment, Rutgers Computer & Technology Law Journal, Vol. 24, No. 1, 1998, 1-74

BYSTRÖM KATRIINA/JÄRVELIN KALERVO, Taks complexity affects inforamtion seeking and use, Information Processing and Management, Vol. 31, No. 2, 1995, 191-213

CABRAL LUIS, Reputation on the Internet, in: Peitz Martin/Waldfogel Joel (Eds.), The Oxford Handbook of the Digital Economy, Oxford University Press 2012, 343-354

CAMP JEAN L., Web Security and Privacy: An American Perspective, The Information Society, Vol. 15, No. 4, 1999, 249-256

CARROLL SEAN, From Eternity to Here: The Quest for the Ultimate Theory of Time, New York 2010

CAVOUKIAN ANN, Privacy by Design: Leadership, Methods, and Results, in: Gutwirth Serge/de Hert Paul/Poullet Yves (Eds.), European Data Protection: Coming of Age, Dordrecht 2013, 175-202

CHAOUCHI HAKIMA, The Internet of Things: Connecting Objects to the Web, London 2010

CHERPILLOD, IVAN, Information et protection des intérêts personnels: Les publications des médias, ZSR 1999 II, 87-197

CHOU HAN-LIN, Wissen und Vergessen bei juristischen Personen, Basel 2002

CICHON CAROLINE, Internet-Verträge: Verträge über Internet-Leistungen und E-Commerce, 2. Aufl., Köln 2005

COHEN ADAM I., Social Media: Legal Risk & Coroprate Policy, New York 2013

CORTADA JAMES W., The Digital Flood: The Diffusion of Information Technology Across the U.S., Europe, and Asia, Oxford University Press 2012 (zit.: Flood)

CORTADA JAMES W., Information and the Modern Corporation, Cambridge, MA 2011 (zit.: Corporation)

CORTADA JAMES W., How Societies Embrace Information Technology: Lessons for Management and the Rest of Us, New Jersey 2009 (zit.: Technology)

COUTAZ GILBERT/HUBER RODOLFO/KELLERHALS ANDREAS/PFIFFNER ALBERT/ROTH-LOCHNER BARBARA, Archivpraxis in der Schweiz, Baden 2007 (zit.: Autor, in: Coutaz et al.)

CROSSON FREDERICK J./SAYRE KENNETH M. (Eds.), Philosophy and Cybernetics, Notre Dame, Indiana 1967, (zit.: Autor, in: Philosophy and Cybernetics)

CUKIER KENNETH, Data, Data everywhere: Special Report, The Economist, February 27, 2010, 3-5

DAIGLE BRADLEY, Stewardship and curation in a digital world, in: Fieldhouse Maggie/Marshall Audrey (Eds.), Collection Development in the Digital Age, London 2012, 93-107

DAMMANN ULRICH/KARHAUSEN MARK/MÜLLER PAUL/STEINMÜLLER WILHELM, Datenbanken und Datenschutz, Frankfurt 1974

DAMMANN ULRICH/MALLMANN OTTO/SIMITIS SPIROS (Hrsg.), Die Gesetzgebung zum Datenschutz: Eine internationale Dokumentation, Frankfurt am Main 1977

DÄSSLER ROLF, Medien und Technologien für die digitale Langzeitarchivierung, in: Rasch Manfred/Dörnemann Astrid (Hrsg.), Filmarchivierung: Sammeln – Sichern – Sichten – Sehen, Essen 2011

DECEW JUDITH WAGNER, In Pursuit of Privacy: Law, Ethics and the Rise of Technology, Cornell University Press, Ithaca NY 1997

DE GIORGI RAFFAELE, Das Gedächtnis des Rechts, in: Kiesow Rainer Maria/Ogorek Regina/Simitis Spiros (Hrsg.), Summa: Dieter Simon zum 70. Geburtstag, Frankfurt am Main 2005, 99-116

DESCHENAUX HENRI/STEINAUER PAUL-HENRI, Personnes physiques et tutelle, 4e éd., Berne 2001

DEVINE JANE/EGGER-SIDER FRANCINE, Going Beyond Google Again: Strategies for Using and Teaching the Invisible Web, London 2014

DÖRING NCOLA, Sozialpsychologie des Internet: Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen, Göttingen 1999

DOWDING MARTIN R., Privacy: Defending an Illusion, Lanham/Toronto/Plymouth 2011

DRAAISMA DOUWE, Das Buch des Vergessens, 2. Aufl., Berlin 2013

DRETSKE FRED I., Knowledge and the Flow of Information, Oxford 1981

DRUCKER PETER F., The Essential Drucker: Selections from the Management Works of Peter F. Drucker, London/New York 2007

DRUEY JEAN NICOLAS, Information als Gegenstand des Rechts, Zürich 1995 (zit.: Information)

DRUEY JEAN NICOLAS, Interessenabwägung – Eine Methode?, in: Beiträge zur Methode des Rechts, St. Galler Festgabe zum Schweizerischen Juristentag 1981, Bern 1981, 131-152 (zit.: Interessenabwägung)

DUBACH SPIEGLER ERICA, Application and Implication of User-Generated Content in Retail, Diss. Zürich 2011

DUDEN, Das Grosse Wörterbuch der deutschen Sprache, Band 6, 2. Aufl., Mannheim 1994

DUMAS BARRY M., Diving into the Bitstream: Information Technology meets Society in a Digital World, New York 2013

EDWARDS LILIAN/BROWN IAN, Information Security, Law, and Data- Intensive Business Models, in: Matwyshyn Andrea M. (Ed.), Harboring Data: Information Security Law and the Corporation, Stanford University Press 2009, 203-227

EGGER RAHEL, Vertragliche Pflichten der Betreiber von unentgeltlichen Web-Suchmaschinen, AJP 11/2008, 1339-1366.

EGGIMANN PATRICK/HARASGAMA REHANA, Online Dispute Resolution – Streitbeilegung in der Cyberwelt, in: Taeger Jürgen (Hrsg.), Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter, Edewecht 2013, 937-954

EGGIMANN PATRICK/TAMÒ AURELIA, European Data Protection Authorities Investigating Google's Privacy Policy – A Case Study, in: Brändli Sandra/Schister Roman/Tamò Aurelia (Hrsg.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft, Bern 2013, 57-79

EGLI URS, Soziale Netzwerke und Arbeitsverhältnis: Über die Auswirkungen von Facebook, Xing & Co auf den betrieblichen Alltag, Jusletter 17. Januar 2011

EHLERS DIRK (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 2. Aufl., Berlin 2005 (zit.: Autor, in: Ehlers)

ELIXMAN ROBERT, Datenschutz und Suchmaschinen, Berlin 2012

EVANS PHILIP/WURSTER THOMAS S., Blown to bits: How the New Economics of Information Transforms Strategy, Boston, MA 2000

FAIRFIELD JOSHUA, Do Not Track as Contract, Vanderbilt Journal of Entertainment and Technology Law, Vol. 14, No. 3, 2012, 101-158

FÄSSLER LUKAS, Records Management, Sorgfaltspflichten für Führungskräfte, Rheinfelden 2006

FELDMANN, THORSTEN, Das «Recht auf Vergessenwerden», in: Taeger Jürgen (Hrsg.), IT und Internet – mit Recht gestalten, Edewecht 2012, 675-685

FERLE CHRISTOPH H., Marktstudie Digitale Langzeitarchivierung: Im Spannungsfeld zwischen Digital Preservation und Enterprise Information Archiving, in: Spath Dieter/Weisbecker Anette (Hrsg.), Frauenhofer-Institut für Arbeitswirtschaft und Organisation IAO, Stuttgart 2012

FIDEL RAYA, Human Information Interaction: An Ecological Approach to Information Behavior, Cambridge, MA 2012

FIDEL RAYA/GREEN MAURICE, The Many Faces of Accessibility: Engineers' Perception of Information, Information Processing and Management, Vol. 40, No. 3, 2004, 563-581

FINN RACHEL L./WRIGHT DAVID/FRIEDEWALD MICHAEL, Seven Types of Privacy, in:, Gutwirth Serge/de Hert Paul/Poullet Yves (Eds.), European Data Protection: Coming of Age, Dordrecht 2013, 3-32

FISHER WILLIAM W. III, Promises to Keep: Technology, Law and the Future of Entertainment, Stanford, CA 2004

FORD HENRY, My Life and Work, New York 1923

FORSTMOSER PETER, 10 Jahre Gesetz – 30 Jahre Diskussion: Von den Anfängen des Datenschutzes in der Schweiz, digma 2/2003, 3-9

FRANKS PATRICIA C., Records & Information Management, Chicago 2013

FRANZ ECKART G., Einführung in die Archivkunde, 3. Aufl., Darmstadt 1989

FRECH PHILIPP, Zivilrechtliche Haftung von Internet-Providern bei Rechtsverletzungen durch ihre Kunden, Zürich 2009

FRICK KARIN, Das Zeitalter der Transparenz, Gottlieb Duttweiler Institute, Studie Nr. 36, Rüschlikon 2011

FRÖHLICH SUSANNE, Kostenfragen in digitalen Archiven: Erfahrungen des Digitalen Archivs Österreich, in: Keitel Christian/Naumann Kai (Hrsg.), Digitale Archivierung in der Praxis, Stuttgart 2013, 31-49

GALOUYE DANIEL F., Simulacron-3, 2. Aufl., München 1983

GANDY OSCAR H., Consumer Protection in Cyberspace, tripleC, Vol. 9, No. 2, 2011, 175-189

GASSER URS, What is Information Law – and what could it be?, in: ders. (Hrsg.), Informationsrecht in «e»-Umgebungen, Zürich 2002, 7-24 (zit.: Law)

GASSER URS, Variationen über «Informationsqualität», in: ders./Schweizer Rainer J./Burkert Herbert (Hrsg.), Festschrift Druey, Zürich 2002, 727-754 (zit.: Variationen)

GASSER URS, Kausalität und Zurechnung von Information als Rechtsproblem, Diss. St. Gallen 2001 (zit.: Kausalität)

GASSER URS, Zu den Möglichkeiten einer rechtlichen Erfassung von Medien- und Informationsqualität, in: ZSR 2000 I, 379-412 (zit.: Informationsqualität)

GASSER URS/HÄUSERMANN DANIEL, Beweisrechtliche Hindernisse bei der Digitalisierung von Unternehmensinformationen, AJP 3/2006, 305-316

GASSER URS/THURMAN JAMES, Themen und Herausforderungen der Regulierung von Suchmaschinen, in: Machill Marcel/Beiler Markus (Hrsg.), Die Macht der Suchmaschinen, Köln 2007, 44-64

GAUCH PETER/SCHLUEP WALTER R./EMMENEGGER SUSAN, Schweizerisches Obligationenrecht Allgemeiner Teil, Bd. 2, 9. Aufl., Zürich 2008

GEAMBASU ROXANA/KOHNO TADAYOSHI/KRISHNAMURTHY ARVIND/LEVY AMIT/LEVY HENRY/GARDNER PAUL/MOSCARITOLO, New Directions for Self-Destructing Data Systems, Technical Report, UW-CSE-11-08-01, University of Washington, August 2011

GEISSBÜHLER PASCAL, Eine Marke ist mehr als ihr guter Ruf, Kommunikationsmanager, 15. März 2011, 2-4

GEISER THOMAS, Die medizinisch-therapeutische Behandlung und Zwangsmassnahmen im Lichte der geltenden Rechtslage und besonderer Berücksichtigung von vormundschaftlichen Fragestellungen, ZVW 6/2001, 225-243 (zit.: Zwangsmassnahmen)

GEISER THOMAS, Die Persönlichkeitsverletzung insbesondere durch Kunstwerke, Basel 1990 (zit.: Persönlichkeitsverletzung)

GIESEN THOMAS, Imperiale und totalitäre Züge des Kommissionsentwurfs für eine europäische Datenschutzverordnung, Computer und Recht, 8/2012, 550-556

GLAUS BRUNO, Nachführungs- oder Säuberungspflicht in Archiven?, Medialex 4/2008, 199-200 (zit.: Nachführungspflicht)

GLAUS BRUNO, Das Recht auf Vergessen und das Recht auf korrekte Erinnerung, Medialex 4/2004, 193-202 (zit.: Vergessen)

GLAUS BRUNO, Das Recht am eigenen Wort, Bern 1997 (zit.: Wort)

GLAZER RASHI H., Measuring the Value of Information: The Information-Intensive Organization, IBM Systems Journal, Vol. 32, No. 1, 1993, 99-110

GLEICK JAMES, The Information: A History, a Theory, a Flood, New York 2011

GOLA PETER/KLUG CHRISTOPH/KÖRFFER BARBARA, BDSG, Bundesdatenschutzgesetz: Kommentar, 11. Aufl., München 2012

GOLDSMITH JACK/WU TIM, Who Controls the Internet?: Illusions of a Borderless World, New York 2006

GOLLWITZER PETER M., Abwägen und Planen, Bewusstseinslagen in verschiedenen Handlungsphasen, Göttingen/Toronto/Zürich, 1991

GÖTTING HOSRT-PETER/SCHERTZ CHRISTIAN/SEITZ WALTER (Hrsg.), Handbuch des Persönlichkeitsrechts, München 2008 (zit.: Autor, in: Götting/Schertz/Seitz)

GREVE WERNER, Handlungserklärung, Die psychologische Erklärung menschlicher Handlungen, Bern et al. 1994

GRIMMELMANN JAMES, Saving Facebook, Iowa Law Review, Vol. 94, No. 4, 2009, 1137-1206

HAAS RAPHAËL, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Zürich 2007

HÄFELIN ULIRCH/HALLER WALTER/KELLER HELEN, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich 2012

HÄFELIN ULRICH/MÜLLER GEORG/UHLMANN FELIX, Allgemeines Verwaltungsrecht, 6. Aufl., Zürich/St. Gallen 2010

HALLIER WILLI CHRISTINE, Corporate Identity Online: Wie Online-Kommunikation die Wahrnehmung des Unternehmens beeinflusst, in: Münch Peter/Ziese Hella (Hrsg.), Corporate Identity: Wie Unternehmensidentität aufgebaut, entwickelt und rechtlich abgesichert wird, Zürich/Basel/Genf 2012, 34-49

HANSEN MARIT, Datenschutz im Cloud Computing, in: Borges Georg/Schwenk Jörg (Hrsg.), Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, Berlin 2012, 79-95

HANSEN URSULA/BODE MATTHIAS, Marketing & Konsum: Theorie und Praxis von der Industrialisierung bis ins 21. Jahrhundert, München 1999

HARTUNG JÜRGEN, Neue Regulierungsaspekte in der EU-Datenschutzreform, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 31-54

HAUSER ROBERT, Das Prinzip der Öffentlichkeit der Gerichtsverhandlung und der Schutz der Persönlichkeit, in: Meier Isaak/Riemer Hans Michael/Weimar Peter (Hrsg.), Recht und Rechtsdurchsetzung, Festschrift Walder, Zürich 1994, 165-192

HÄUSERMANN DANIEL MARKUS, Vertraulichkeit als Schranke von Informationsansprüchen, Zürich 2009

HAUSHEER HEINZ/AEBI-MÜLLER REGINA E., Das Personenrecht des Schweizerischen Zivilgesetzbuches, 3. Aufl., Bern 2012

HAUSHEER HEINZ, Neuere Entwicklungen zum Persönlichkeitsrecht, in: Bucher Eugen/Canaris Claus-Wilhelm/Honsell Heinrich/Koller Thomas (Hrsg.), Norm und Wirkung, Festschrift Wiegand, Bern 2005

HAUSMANINGER HERBERT/SELB WALTER, Römisches Privatrecht, 9. Aufl., Wien/Köln/Weimar, 2001

VON HAYEK FRIEDRICH AUGUST, The use of Knowledge in Society, in: *idem*, Individualism and Economic Order, London 1948, 77-91

HECKHAUSEN JUTTA/HECKHAUSEN HEINZ, Motivation und Handeln, 4. Aufl., Berlin 2010 (zit.: Autor, in: Heckhausen/Heckhausen)

HELLER CHRISTIAN, Post-Privacy: Prima leben ohne Privatsphäre, München 2011

HETCHER STEVEN, Anonymity, Pseudonymity & Online Privacy, in: Dörr Dieter/Weaver Russel L. (Eds.), The Right To Privacy in the Light of Media Convergence: Perspectives from three Continents, Media Convergence, Vol. 3, Berlin/Boston 2012, 276-297

HILTY LORENZ/OERTEL BRITTA/WÖLK MICHAELA/PÄRLI KURT, Lokalisiert und identifiziert: Wie Ortungstechnologien unser Leben verändern, Zürich 2012

HILTY RETO M., Unübertragbarkeit urheberrechtlicher Befugnisse: Schutz des Urheberrechts oder dogmatisches Ammenmärchen?, in: Becker Jürgen/Hilty Reto M./Jean-Fritz Stöckli (Hrsg.), Recht und Wandel seines sozialen und technologischen Umfeldes, Festschrift Rehbinder, München/Bern 2002, 259-284 (zit. Unübertragbarkeit)

HILTY RETO M., Lizenzvertragsrecht, Systematisierung und Typisierung aus schutz- und schuldrechtlicher Sicht, Bern 2001 (zit. Lizenzvertragsrecht)

HOFFMANN BERNHARD, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes: Das Zweckproblem aus theoretischer und praktischer Sicht, Baden-Baden 1991

HOFSTADTER DOUGLAS R., Gödel, Escher, Bach: Ein Endloses Geflochtenes Band, 11. Aufl., München 2007

HOLENSTEIN CHRISTOPH, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, Bern 2002

HOLZNAGEL DANIEL, Notice and Take-Down-Verfahren als Teil der Providerhaftung, Tübingen 2013

HONSELL HEINRICH/VOGT NEDIM PETER/GEISER THOMAS (Hrsg.), Basler Kommentar, Zivilgesetzbuch I, Art. 1-456 ZGB, 4. Auflage, Basel 2010 (zit.: Autor, in: Honsell/Vogt/Geiser)

HONSELL HEINRICH/VOGT NEDIM PETER/WIEGAND WOLFGANG (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 5. Aufl., Basel 2011 (zit.: Autor, in: Vogt/Honsell/Wiegand)

HÖRA NIELS, Haftung für fehlerhafte Informationen gegenüber Nichtvertragspartnern, Frankfurt am Main 2008

HOTZ KASPAR ERNST, Zum Problem der Abgrenzung des Persönlichkeitsschutzes nach Art. 28 ZGB, Zürich 1967

HUBER MICHAEL, Erinnern, Vergessen und Falsch-Erinnern, in: Auchter Thomas/Schlagheck Michael (Hrsg.), Theologie und Psychologie im Dialog über Erinnern und Vergessen, Paderborn 2004, 93-112 (zit. Erinnern)

HUBER RENÉ, Die Teilrevision des Eidg. Datenschutzgesetzes – ungenügende Pinselrenovation, recht 6/2006, 205-221 (zit.: Teilrevision)

HUBMANN HEINRICH, Das Persönlichkeitsrecht, 2. Aufl., Köln 1967 (zit. Persönlichkeitsrecht)

HUBMANN HEINRICH, Grundsätze der Interessenabwägung, Archiv für die civilistische Praxis 2/1956, 85-134 (zit. Interessenabwägung)

HUBMANN HEINRICH, Das Recht des schöpferischen Geistes, Berlin 1954 (zit. Recht)

HUGUENIN CLAIRE/HILTY RETO M. (Hrsg.), Schweizer Obligationenrecht 2020: Entwurf für einen neuen allgemeinen Teil, Zürich 2013 (zit.: Autor, in: Huguenin/Hilty)

HUGUENIN CLAIRE/THOUVENIN FLORENT, Verjährung und Reform in der Schweiz, in: Remien Oliver (Hrsg.), Verjährungsrecht in Europa – zwischen Bewährung und Reform, Tübingen 2011, 303-323

HUI KAI-LUNG/PNG IVAN, The Economics of Privacy, in: Hendershott Terrence (Ed.), Economics and Information Systems, Handbooks in Information Systems, Vol. 1, Amsterdam 2006, 471-497

HÜRLIMANN DANIEL, Suchmaschinenhaftung: zivilrechtliche Verantwortlichkeit der Betreiber von Suchmaschinen aus Urheber-, Marken-, Lauterkeits-, Kartell- und Persönlichkeitsrecht, Bern 2012

HUVILA ISTO, Mining qualitative data on human information behaviour from the Web, in: Griesbaum Joachim/Mandl Thomas/Womser-Hacker Christa (Hrsg.), Information und Wissen: global, sozial und frei?, Boizenburg 2011

INDERKUM MATTHIAS, Schadenersatz, Genugtuung und Gewinnherausgabe aus Persönlichkeitsverletzung: Art. 28a Abs. 3 ZGB, Zürich 2008

JAAG TOBIAS/LIENHARD ANDREAS/TSCHANNEN PIERRE, Ausgewählte Gebiete des Bundesverwaltungsrechts, 7. Aufl., Basel 2009

JÄGGI PETER, Fragen des privatrechtlichen Schutzes der Persönlichkeit, ZSR 1960 II, 135a-261a

JESTAEDT MATTHIAS, Richterliche Rechtsetzung statt richterliche Rechtsfortbildung: Methodologische Betrachtungen zum sog. Richterrecht, in: Bumke Christian (Hrsg.), Richterrecht zwischen Gesetzesrecht und Rechtsgestaltung, Tübingen 2012, 49-69

JUNGKIND THILO, Risikokultur und Störfallverhalten der chemischen Industrie: Gesellschaftliche Einflüsse auf das unternehmerische Handeln von Bayer und Henkel seit der zweiten Hälfte des 20. Jahrhunderts, Stuttgart 2013

KANG JERRY, Information Privacy in Cyberspace Transactions, Stanford Law Review, Vol. 50, No. 4, 1998, 1193-1194

KATSH ETHAN M., Law in a Digital World, Oxford University Press 1995

KEITEL CHRISTIAN/SCHOGER ASTRID (Hrsg.), Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644, Berlin 2013

KIESER ALFRED, Organisationstheoretische Ansätze, München 1981

KILLIAS MARTIN, Unternehmensstrafrecht und Produktsicherheit, Zürich 2013

KINDT ANNE, Die Grundrechtliche Überprüfung der Vorratsdatenspeicherung: EuGH oder BVerfG – wer traut sich?, MMR 2009, 661-666

KLAS BENEDIKT, Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, Edewecht 2012

KOHLER JOSEF, Das Eigenbild im Recht, Berlin 1903

KOSCHEL KAY-VOLKER, Zur Rolle der Marktforschung in der Konsumgesellschaft, in: Schrage Dominik/Friederici Markus R. (Hrsg.), Zwischen Methodenpluralismus und Datenhandel: Zur Soziologie der kommerziellen Konsumforschung, Wiesbaden 2008, 29-50

KOSINSKI MICHAL/STILLWELL DAVID/GRAEPEL THORE, Private traits and attributes are predictable from digital records of human behavior, PNAS, Vol. 110, No. 15, 2013, 5802-5805

KRASSER RUDOLF, Verpflichtung und Verfügung im Immaterialgüterrecht, GRUR Int. 6/7/1973, 230-238

KREIS GEORG, Die Schweiz im Zweiten Weltkrieg, 4. Aufl., Innsbruck 2011

KUHLEN RAINER, Informationsmarkt: Chancen und Risiken der Kommerzialisierung von Wissen, Konstanz 1995

KUUTTI KARI/BANNON LIAM, Remembering past, present and future – articulating dimensions of «organizational memory» for organizational learning, SIGOIS Bulletin, Vol. 17, No. 3, 1996, 33-37

LANDWEHR WILFRIED, Das Recht am eigenen Bild, Diss. Zürich 1955

LANE FREDERICK S., American Privacy: The 400-Year History of Our Most Contested Right, Boston 2009

LANG WILHELM, Ton- und Bildträger: materielle Prozesse und prozessuale Grundfragen in persönlichkeitsrechtlicher Sicht, Bielefeld 1960

LANGER DIRK, Le droit à l'oubli à l'épreuve d'Internet, Jusletter, 12. März 2012

LANGHEINRICH MARC, Privacy in Ubiquitous Computing, in: Krumm John (Ed.), Ubiquitous Computing Fundamentals, Boca Raton 2010, 95-160

LANIER JARON, Who owns the future?, New York 2013

LEENES RONALD, Do They Know Me? Deconstructing Identifiability, University of Ottawa Law & Technology Journal, Vol. 4, No. 1-2, 2007, 135-161

LEHNER FRANZ, Digitale Identität und Unternehmensidentität aus der Perspektive von Informatik und Wirtschaftsinformatik, in: Scholz Christian (Hrsg.), Identitätsbildung: Implikationen für globale Unternehmen und Regionen, München/Mering 2005, 27-44

LESSIG LAWRENCE, Code and Other Laws of Cyberspace, New York 1999

LEU DANIEL/VON DER CRONE CASPAR, Übermässige Bindung und die guten Sitten: Zum Verhältnis von Art. 27 ZGB und Art. 20 OR, SZW/RSDA 4/2003, 221-228

LÉVY VANESSA, Le droit à l'image, Définition, Protection, Exploitation: étude de droit privé suisse, Zurich 2002

LIEDTKE WERNER, Das Bundesdatenschutzgesetz: eine Fallstudie zum Gesetzgebungsprozess, München 1980

LINDE FRANK, Ökonomie der Information, Göttingen 2005

LINDSAY DAVID, Digital Eternity or Digital Oblivion, in: Dörr Dieter/Weaver Russel L. (Eds.), The Right To Privacy in the Light of Media Convergence: Perspectives from three Continents, Media Convergence, Vol. 3, Berlin/Boston 2012, 322-344

LODGE JULIET/MAYER TERRI, Security and Privacy in Estonia, May 23, 2006, abrufbar unter: http://www.libertysecurity.org/article959.html, abgerufen am 12.2.2013

LONDON ECONOMICS, Study on the economic benefits of privacy-enhancing technologies (PET), Final Report to The European Commission DG Justice, Freedom and Security, London, July 2010

LOTZ CHRISTIAN, Versprechen – Verzeihen, Erinnern – Vergessen, in: Angehrn Emil/Baertschi Bernard (Hrsg.), Gedächtnis und Voraussicht, studia philosophica 60/2001, 78-93

LUBICH HANNES P., Unternehmensweite Datenschutz- und Datensicherheitskonzepte, in Baeriswyl Bruno/Rudin Beat (Hrsg.), Perspektive Datenschutz, Zürich/Baden-Baden/Wien 2002

LÜCHINGER ADOLF, Der privatrechtliche Schutz der Persönlichkeit und die Massenmedien, SJZ 70/1974, 321-327

LUHMANN NIKLAS, Grundrechte als Institution, 4. Aufl., Berlin 1999

LUTTER MARCUS, Haftung von Vorständen, Verwaltungs- und Aufsichtsräten, Abschlussprüfern und Aktionären, ZSR 2005 II, 415-463

LYRE HOLGER, Quantentheorie der Information, Wien 1998

MAASS CHRISTIAN/SKUSA ANDRE/HESS ANDREAS/PIETSCH GOTTHARD, Der Markt für Internet-Suchmaschinen, in: Lewandowski Dirk (Hrsg.), Handbuch Internet-Suchmaschinen, Nutzerorientierung in Wissenschaft und Praxis, Heidelberg 2009, 3-17

MACLEAN MARGRET/DAVIS BEN H. (Eds.), Time & Bits: Managing Digital Continuity, Los Angeles, CA 1998

MACLEOD DON, How to find out Anything, New York 2012

MADOW MICHAEL, Private Ownership of Public Image: Popular Culture and Publicity Rights, California Law Review, Vol. 81, No. 3, 1993, 125-240

MADRIAN BRIGITTE C./SHEA DENNIS F., The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior, Quarterly Journal of Economics, Vol. 118, No. 4, 2001, 1149-1187

MAISSEN THOMAS, Verweigerte Erinnerung: Nachrichtenlose Vermögen und Schweizer Weltkriegsdebatte 1989-2004, 2. Aufl., Zürich 2005

MALIK YOGESH/NIEMEYER ALEX/RUWADI BRIAN, Building the supply chain of the future, McKinsey Quarterly, January 2011

MANKIW GREGORY N./TAYLOR MARK P., Grundzüge der Volkswirtschaftslehre, 5. Aufl., Stuttgart 2012

MANTELERO ALESSANDRO, U.S. Concern about the European Right to Be Forgotten and Free Speech: Much Ado About Nothing?, Contratto e Impresa, 2/2012, 727-740

MARKOWITSCH HANS J., Gedächtnisstörungen, Stuttgart/Berlin/Köln, 1999

MASLOW ABRAHAM H., A Theory of Human Motivation, Psychological Review, Vol. 50, No. 4, 1943, 370-396

MASTRONARDI PHILIPPE, Der Verfassungsgrundsatz der Menschenwürde in der Schweiz: ein Beitrag zu Theorie und Praxis der Grundrechte, Berlin 1978

MATHER TIM/KUMARASWAMY SUBRA/SHAHED LATIF, Cloud Security and Privacy, Sebastopol, CA 2009

MATIS HERBERT, «Corporate Identity» und «Corporate Culture», in: Mosser Alois (Hrsg.), Corporate Identity und Geschichtsbewusstsein, Wien 1994, 75-111

MATTERN FRIEDEMANN, in: Kirchschläger Peter G./Kirchschläger Thomas/Belliger Andréa/Krieger David J. (Hrsg.), Menschenrechte und Terrorismus, Bern 2004, 315-335 (zit.: Menschenrechte)

MATTERN FRIEDEMANN, Total vernetzt: Szenarien einer informatisierten Welt, Berlin 2003 (zit.: vernetzt)

MAURER-LAMBROU URS/VOGT NEDIM PETER (Hrsg.), Basler Kommentar zum Datenschutzgesetz, 2. Aufl., Basel/Genf/München 2006 (zit.: Autor, in: Maurer-Lambrou/Vogt)

MAYER-SCHÖNBERGER VIKTOR, Delete: Die Tugend des Vergessens in digitalen Zeiten, Princeton University Press 2009

MAYER-SCHÖNBERGER VIKTOR/CUKIER KENNETH, Big Data: A Revolution that will Transform how we Live, Work, and Think, Boston/New York 2013

MCBARNET DOREEN, Corporate Social Responsibility beyond Law, through Law, for Law: the new corporate accountability, in: *idem*/Voiculescu Aurora/Campbell Tom (Eds.), The New Corporate Accountability: Corporate Social Responsibility and the Law, Cambridge University Press 2007, 9-58

MCCLELLAND DAVID C., Die Definition eines spezifischen Motivs, in: Thomae Hans (Hrsg.), Die Motivation menschlichen Handelns, 5. Aufl., Köln/Berlin 1969, 175-180

MCDONAGH MAEVE, The Uneasy Relationship between Data Protection and Freedom of Information, Publications de l'Institut suisse de droit comparé, L'individue face aux nouvelles technologies: Surveillance, identification et suivi, Genève/Zurich/Bâle 2005

MCDONALD ALEECIA M./CRANOR LORRIE FAITH, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society, Vol. 4, No. 3, 2008, 540-565

MCKEEN JAMES D./SMITH HEATHER A., IT Strategy: Issues and Practices, 2nd ed., New Jersey 2012

MCKINSEY GLOBAL INSTITUTE, Big Data: The next frontier for innovation, competition, and productivity, 2011

MEIER CORDULA, Kunst und Gedächtnis: Zugänge zur aktuellen Kunstrezeption im Licht digitaler Speicher, München 2002

MEIER-SCHATZ CHRISTIAN J.: Funktion und Recht des Handelsregisters als wirtschaftliches Problem, ZSR 1989 I, 433-463

MEILI ANDREAS, Kann man das Persönlichkeitsrecht im Internet durchsetzen?, Plädoyer 5/2009, 29

MEISTER HERBERT, Datenschutz im Zivilrecht: Das Recht am eigenen Datum, 2. Aufl., Bergisch Gladbach 1981

MELCHIOR ANNETT, CRM und Datenschutz, Berlin 2005

MELLEWIGT THOMAS/DECKER CAROLIN, Wissensmanagement (Sammelrezension), DBW 5/2009, 613-631

METZGER MIRIAM J., Effects of site, vendor, and consumer characteristics on web site trust and disclosure, Communiacation Research, Vol. 33, No. 3, 2006, 155-179

MEYER CAROLINE B., Privatrechtliche Persönlichkeitsrechte im kommerziellen Rechtsverkehr, Basel 2008 (zit.: Persönlichkeitsrechte)

MEYER CONRAD, Finanzielles Rechnungswesen, Zürich 2008 (zit.: Rechnungswesen)

MILLARD CHRISTOPHER (Ed.), Cloud Computing Law, Oxford University Press 2013 (zit.: Autor, in: Millard)

MOEREL LOKKE, Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers, Oxford University Press 2012

MOSER PATRICK/NEBIKER REGULA/OTHENIN-GIRARD MIREILLE, Lebenszyklus von Dokumenten im Zentrum, digma 2/2005, 66-71

MOSSER ALOIS, Management by History?, in: ders. (Hrsg.), Corporate Identity und Geschichtsbewusstsein, Wien 1994, 11-18

MÜLLER GEORG, Elemente einer Rechtssetzungslehre, 2. Aufl., Zürich/Basel/Genf 2006 (zit.: Rechtssetzungslehre)

MÜLLER PAUL J., Elemente einer schweizerischen Grundrechtstheorie, Bern 1982 (zit.: Grundrechtstheorie)

MÜLLER PAUL J., Funktionen des Datenschutzes aus soziologischer Sicht, DVR 1975, 107-118 (zit.: Funktionen)

MÜLLER PAUL J., Soziale Kontrolle durch Datenbanken, in: Krauch Helmut (Hrsg.), Erfassungsschutz – Der Bürger in der Datenbank: zwischen Planung und Manipulation, Stuttgart 1975, 141-152 (zit.: Kontrolle)

MULLIGAN DEIRDRE K./KING JENNIFER, Bridging the Gap between Privacy and Design, Journal of Constitutional Law, Vol. 14, No. 4, 2012, 989-1034

NABHOLZ LILI, Entstehung und Grundanliegen des Datenschutzgesetzes, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes, Zürich 1993, 1-7

NEBEN GERALD, Triviale Personenberichtserstattung als Rechtsproblem: Ein Beitrag zur Grenzziehung zwischen Medienfreiheit und Persönlichkeitsschutz, Berlin 2001

NEERACHER CHRISTOPH, Das arbeitsvertragliche Konkurrenzverbot, Bern 2001

NISSENBAUM HELEN, A Contextual Approach to Privacy Online, Daedalus, Vol. 140, No. 4, 2011, 32-48 (zit.: Approach)

NISSENBAUM HELEN, From Preemption to Circumvention: If Technology Regulates Why Do We Need Regulation (And Vice Versa)?, Berkeley Technology Law Journal, Vol. 26, No. 3, 2011, 1367-1386 (zit.: Preemption)

NISSENBAUM HELEN, Privacy as Contextual Integrity, Washington Law Review, Vol. 79, No. 1, 2004, 119-158 (zit.: Integrity)

NOBEL PETER, Leitfaden zum Presserecht, 2. Aufl., Zofingen 1983

NOBEL PETER/WEBER ROLF H., Medienrecht, 3. Aufl., Bern 2007

NONAKA IKUJIRO/TAKEUCHI HIROTAKA, The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation, Oxford University Press, 1995

OHM PAUL, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, Vol. 57, No. 6, 2010, 1701-1777

OHNO TAIICHI, Das Toyota-Produktionssystem, Frankfurt 1993

ONUF RACHEL/HYRY THOMAS, Take it Personally: The Implications of Personal Records in Electronic Form, in: Lee Christopher A. (Ed.), I, Digital: Personal Collections in the Digital Era, Chicago 2011, 241-256

OPPLIGER ROLF, Digitale Dokumente – Alte und neue Herausforderungen sowie Lösungsansätze, Jusletter, 8. November 2004

PAINE SCHOFIELD CARINA B./JOINSON ADAM N., Privacy, Trust, and Disclosure Online, in: Barak Azy (Ed.), Psychological Aspects of Cyberspace: Theory, Research, Applications, Cambridge University Press 2008, 13-31

PARKIN ALAN J., Gedächtnis, Weinheim 1996

PAZZINI KARL-JOSEF, in: Hedinger Johannes M./Gossolt Marcus (Hrsg.), Kunst, öffentlicher Raum, Identiät: Mocmoc, das ungeliebte Denkmal, Sulgen 2004, 42-46

PEDRAZZINI MARIO M., Versuch einer Nominalisierung des Lizenzvertrages, in: Forstmoser Peter/Tercier Pierre/Zäch Roger (Hrsg.), Innominatverträge: Festgabe Schluep, 413-422

PEDRAZZINI MARIO M./OBERHOLZER NIKLAUS, Grundriss des Personenrechts, 4. Aufl., Bern 1993

PEIFER KARL-NIKOLAUS, Individualität im Zivilrecht: Der Schutz persönlicher, gegenständlicher und wettbewerblicher Individualität im Persönlichkeitsrecht, Immaterialgüterrecht, und Recht der Unternehmen, Tübingen 2001

PEPELS WERNER, Lexikon Marktforschung, 2. Aufl., Düsseldorf 2011

PERELMAN CHAIM, Juristische Logik als Argumentationslehre, Freiburg/München 1979

PETER HANSJÖRG, Texte zum römischen Obligationenrecht mit Verweisen zum schweizerischen Recht, Zürich 1997 (zit.: Obligationenrecht)

PETER JAMES T., Das Datenschutzgesetz im Privatbereich: unter besonderer Berücksichtigung seiner motivationalen Grundlage, Zürich 1994 (zit.: Datenschutzgesetz)

PETERHANS MARKUS, Informationsmanagement: Theoretische Grundlagen & Führungskonzept, Diss. Zürich 1995

PETHIG RÜDIGER, Information als Wirtschaftsgut in wirtschaftswissenschaftlicher Sicht, in: Fiedler Herbert/Ullrich Hanns (Hrsg.), Information als Wirtschaftsgut: Management und Rechtsgestaltung, Köln 1997, 1-28

PEUKERT ALEXANDER, Persönlichkeitsbezogene Immaterialgüterrechte?, ZUM 8/9/2000, 710-721

PEYROT ROBERT PAUL, Informationspflichten der Konzernobergesellschaft gegenüber der Konzernuntergesellschaft, Diss. St. Gallen 2003

PICOT ARNOLD (Hrsg.), Information als Wettbewerbsfaktor, Stuttgart 1997 (zit.: Autor, in: Picot)

PICOT ARNOLD/FRANCK EGON, Die Planung der Unternehmensressource Information (I), in: Wirtschaftsstudium, 10/1988, 544-549

PICOT ARNOLD/MAIER MATTHIAS, Information als Wettbewerbsfaktor, in: Pressmar Dieter B. (Hrsg.), Informationsmanagement, Schriften zur Unternehmensführung, Band 49, Wiesbaden 1993, 31-53

PIERENKEMPER TONI (Hrsg.), Unternehmensgeschichte, Basistexte Geschichte, Band 7, Stuttgart 2011

PINKAS DANIEL, À propos d'une citation célèbre: «Those who cannot remember the past are condemned to repeat it», in: Angehrn Emil/Baertschi Bernard (Hrsg.), Gedächtnis und Voraussicht, studia philosophica 60/2001, 115-125

POLZER GEORG, Big Data – eine Einführung, digma 1/2013, 6-9

POPP CHRISTOPH, Das «Organisationskonzept Elektronische Verwaltungsarbeit» als Überarbeitung und Nachfolgerin des DOMEA-Konzepts, Archivar 1/2013, 54-57

POSNER RICHARD A., The Right of Privacy, Georgia Law Review, Vol. 12, No. 3, 1978, 393-422

PROBST THOMAS, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht: Personendaten und anonymisierte Einzeldaten in der globalisierten Informationsgesellschaft – Quo vaditis?, AJP 10/2013, 1423-1436

PROSSER WILLIAM L., Privacy, California Law Review, Vol. 48, No. 3, 1960, 383-423

PURI COLIN/SOON KIM DOO/ZEH PETER Z./VERMA KUNAL, Implementing a Data Lineage Tracker, in: Cuzzocrea Alfredo/Dayal Umeshwar (Eds.), Data Warehousing and Knowledge Discovery, Heidelberg 2012, 390-403

PURTOVA NADEZHDA, Property Rights in Personal Data: A European Perspective, Alphen aan den Rijn 2012

RADIN MARGARET JANE, Property Evolving in Cyberspace, Journal of Law and Communications, Vol. 15, No. 2, 1996, 509-526

RALLO ARTEMI/MARTINEZ RICARD, Data Protection, Social Networks and Online Mass Media, in: Gutwirth Serge/de Hert Paul/Poullet Yves (Eds.), European Data Protection: Coming of Age, Dordrecht 2013, 407-430

REAGLE JOSEPH/CRANOR LORRIE FAITH, The platform for privacy preferences, Communications of the Association for Computing Machinery, Vol. 42, No. 2, 1999, 48-55

RECK HANS ULRICH, Archive, Inszenierungen, Einschnitte, Verzweigungen: Sammeln im Zeitalter digitaler elektronischer Medien, in: Breuer Gerda (Hrsg.), summa summarum: Sammeln heute, Frankfurt am Main 1999, 73-91

REHBINDER MANFRED, Schweizerisches Urheberrecht, 3. Aufl., Bern 2000

RHINOW RENÉ/SCHEFER MARKUS, Schweizerisches Verfassungsrecht, 2. Aufl. Basel 2009

RICHLI PAUL, Interdisziplinäre Daumenregeln für eine faire Rechtsetzung: Ein Beitrag zur Rechtsetzungslehre im liberalen sozial und ökologisch orientierten Rechtsstaat, Basel/Genf/München 2000

RICOEUR PAUL, La mémoire, l'histoire, l'oubli, Éditions du Seuil 2000

RIEDER PETER, Interessenabwägung in der Rechtsprechung des BGH zum Namens- und Bezeichnungsschutz, zum Recht am Gewerbebetrieb und zum allgemeinen Persönlichkeitsrecht, Diss. Erlangen-Nürnberg 1971

RIEMER HANS MICHAEL, Personenrecht des ZGB, 2. Aufl., Bern 2002 (zit.: Personenrecht)

RIEMER HANS MICHAEL, Persönlichkeitsrechte und Persönlichkeitsschutz gemäss Art. 28 ff. ZGB im Verhältnis zum Datenschutz-, Immaterialgüter- und Wettbewerbsrecht, sic! 2/1999, 103-110 (zit.: Persönlichkeitsrechte)

RIKLIN FRANZ, Der Schutz der Persönlichkeit gegenüber Eingriffen durch Radio und Fernsehen nach schweizerischem Privatrecht, Freiburg i.Üe. 1968

ROBERTO VITO/HRUBESCH-MILLAUER STEPHANIE, Offene und neue Fragestellungen im Bereich des Persönlichkeitsschutzes, in: Schweizer Rainer J./Burkert Herbert/Gasser Urs (Hrsg.), Festschrift Druey, Zürich 2002, 229-241

RODRIGUES RUBEN, Privacy on Social Networks: Norms, Markets, and Natural Monopoly, in: Levmore Saul/Nussbaum Martha C. (Eds.), The Offensive Internet: Speech, Privacy and Reputation, Cambridge, MA/London 2010, 237-256

ROSEN JEFFREY, The Right To Be Forgotten, Stanford Law Review Online, Vol. 64, February 12, 2012, 88-92 (zit.: Forgotten)

ROSEN JEFFREY, The Web means the End of Forgetting, The New York Times, July 21, 2010 (zit.: Forgetting)

ROSEN JEFFREY, The Unwanted Gaze: The Destruction of Privacy in America, New York 2000 (zit.: Gaze)

ROSENTHAL DAVID, Datenschutz-Compliance im Unternehmen: Umsetzung in der Praxis und Handlungsbedarf des Gesetzgebers, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 157-187 (zit.: Datenschutz-Compliance)

ROSENTHAL DAVID, Das Bauchgefühl im Datenschutz, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing: 20 Jahre Datenschutz in der Schweiz, Zürich/Basel/Genf 2012, 69-91 (zit.: Bauchgefühl)

ROSENTHAL DAVID, «Logistep»: Offenbar ein Einzelfallentscheid, digma, 1/2011, 40-43 (zit.: Logistep)

ROSENTHAL DAVID, Wenn Datenschutz übertrieben wird oder: Hard cases make bad law, in: Jusletter, 27. Oktober 2010 (zit.: Datenschutz)

ROSENTHAL DAVID, Manche werden süchtig: Die Datenflut überfordert mittlerweile viele Manager, DIE ZEIT, 17/1998 (zit.: süchtig)

ROSENTHAL DAVID/JÖHRI YVONNE (Hrsg.), Handkommentar zum Datenschutzgesetz: sowie weiteren ausgewählten Bestimmungen, Zürich 2008 (zit.: Autor, Handkommentar DSG)

ROSENZWEIG ROY, Clio Wired: The Future of the Past in the Digital Age, New York 2011

RÖSSLER BEATE (Ed.), Privacies: Philosophical Evaluations, Stanford University Press 2004

ROUVINEZ JULIEN, La license des droits de la personnalité: Étude de droit privé suisse, Diss. Zürich 2011

RUBINSTEIN IRA S./GOOD NATHANIEL, Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, Berkeley Technology Law Journal, Vol. 28, No. 2, 2013, 1333-1414

RUDIN BEAT, Kollektives Gedächtnis und informationelle Integrität: Zum Datenschutz im öffentlichen Archivwesen, AJP 1998, 247-260

SALADIN PETER, Grundrechte und Privatrechtsordnung: Zum Streit um die sog. «Drittwirkung» der Grundrechte, SJZ 84 (1988), 373-384

SAMUELSON PAMELA, Privacy as Intellectual Property?, Stanford Law Review Vol. 52, No. 5, 2000, 1125-1174

SAMUELSON WILLIAM/ZECKHAUSER RICHARD, Status Quo Bias in Decision Making, Journal of Risk and Uncertainty, Vol. 1, No. 1, 1988, 7-59

SARVARY MIKLOS, Gurus and Oracles: The Marketing of Information, Cambridge, MA 2012

SAYRE KENNETH M., Cybernetics and the Philosophy of Mind, London 1976

SCHAAR PETER, Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft, München 2009

SCHENK DIETMAR, «Aufheben, was nicht vergessen werden darf»: Archive vom alten Europa bis zur digitalen Welt, Stuttgart 2013

SCHIEDERMAIR STEPHANIE, Der Schutz des Privaten als internationales Grundrecht, Tübingen 2012

SCHIRRMACHER FRANK, Ego: Das Spiel des Lebens, 3. Aufl., München 2013

SCHMID JÖRG, Persönlichkeitsschutz bei der Bearbeitung von Personendaten durch Private, ZBJV 12/1995, 809-832

SCHMIDT-BENS JOHANNA, Cloud Computing Technologien und Datenschutz, Edewecht 2012

SCHMITT KARLHEINZ, Kosten der digitalen Archivierung: Ein mögliches Vorgehensmodell und erste Erfahrungen, in: Keitel Christian/Naumann Kai (Hrsg.), Digitale Archivierung in der Praxis, Stuttgart 2013, 19-29

SCHNEIDER HOLGER, Digitale Amnesie: Langzeitarchivierung digitaler Dokumente im betrieblichen Umfeld, Norderstedt 2012 (zit.: Amnesie)

SCHNEIDER NORBERT F., Konsum und Gesellschaft, in: Rosenkranz Doris/ders. (Hrsg.), Konsum – Soziologische, ökonomische und psychologische Perspektiven, Wiesbaden 2000, 9-22 (Konsum)

SCHNEIDER JOCHEN, Datenschutzrechtliche Anforderungen an die Sicherheit der Kommunikation im Internet, in: Borges Georg/Schwenk Jörg (Hrsg.), Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, Berlin 2012, 21-42 (zit: Anforderungen)

SCHNEIDER JÜRG/SOMMER UELI/CARTIER MICHAEL, Chapter 5.25, Switzerland, in: Noorda Catrien/Hanloser Stefan (Eds.), E-Discovery and Data Privacy: A Practical Guide, Alphen aan den Rijn 2011, 277-293

SCHÖNPFLUG WOLFGANG/SCHÖNPFLUG UTE, Psychologie, 4. Aufl., München 1997

SCHUMACHER RAINER, Die Presseäusserung als Verletzung der persönlichen Verhältnisse: insbesondere ihre Widerrechtlichkeit, Freiburg i.Üe. 1960

SCHWANDER VERENA, Grundrecht der Wissenschaftsfreiheit: im Spannungsfeld rechtlicher und gesellschaftlicher Entwicklungen, Diss. Bern 2002

SCHWARTZ PAUL M./SOLOVE DANIEL J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information, New York University Law Review, Vol. 86, No. 6, 2011, 1814-1894

SCHWEIZER RAINER J., The Right to Access Personal Data and the Quality of Information, in: Gasser Urs (Ed.), Information Quality Regulation: Foundations, Perspectives, and Applications, Baden-Baden 2004, 125-133 (zit.: Access)

SCHWEIZER RAINER J., Grundsatzfragen des Datenschutzes, Basel 1985 (zit.: Grundsatzfragen)

SCHWEIZER RAINER J./BAUMANN JÉRÔME, Rechtsfragen der Archivierung digitaler Dokumente: Die Erfahrungen der Schweizerischen Nationalbibliothek und des Bundesarchivs, in: Wunderlich Werner/Schmid Beat (Hrsg.), Die Zukunft der Gutenberg-Galaxis, Bern 2008

SCHWENZER INGEBORG, Schweizerisches Obligationenrecht, Allgemeiner Teil, 6. Aufl., Bern 2012

SEARLS DOC, The Customer as a God, The Wall Street Journal, July 20, 2012, abrufbar unter: http://online.wsj.com/article/SB10000872396390444873204577535352521092154.html, abgerufen am 13.2.2013 (zit.: Customer)

SEARLS DOC, The Intention Economy, Boston, MA 2012 (zit.: Economy)

SEIDEL ULRICH, Die durchlöcherte Privatsphäre, in: Krauch Helmut (Hrsg.), Erfassungsschutz – Der Bürger in der Datenbank: zwischen Planung und Manipulation, Stuttgart 1975, 38-47 (zit.: Privatsphäre)

SEIDEL ULRICH, Datenbanken und Persönlichkeitsrecht, Köln 1972 (zit.: Datenbanken)

SEITEL FRASER P./DOORLEY JOHN, Rethinking Reputation: How PR Trumps Marketing and Advertising in the New Media World, New York 2012

SENN MARCEL, Rechtswissenschaft ohne reflexiven Habitus?, in: Sethe Rolf/Heinemann Andreas/Hilty Reto M./Nobel Peter/Zäch Roger (Hrsg.), Kommunikation, Festschrift Weber, Bern 2011, 913-929

SHAPIRO CARL/VARIAN HAL R., Information Rules: A Strategic Guide to the Network Economy, Boston 1999

SIEBER ULRICH, Informationsrecht und Recht der Informationstechnik, NJW 1989, 2569-2580

SIEGFRIED FELIX HEINZ, Internationaler Kulturgüterschutz in der Schweiz: Das Bundesgesetz über den internationalen Kulturgütertransfer (Kulturgütertransfergesetz, KGTG), Frankfurt am Main 2006

SIFRY MICAH L., WikiLeaks and the Age of Transparency, Yale University Press 2011

SILVER NATE, The signal and the noise: why so many predictions fail – but some don't, New York 2012

SIMITIS SPIROS (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011 (zit.: Autor, in: Simitis)

SIMITIS SPIROS, Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung, NJW 2009, 1782-1786 (zit.: Vorratsdatenspeicherung)

SIMITIS SPIROS, Datenschutz – eine notwendige Utopie, in: Kiesow Rainer Maria/Ogorek Regina/ders. (Hrsg.), Summa: Dieter Simon zum 70. Geburtstag, Frankfurt am Main 2005, 511-527 (zit.: Utopie)

SIMITIS SPIROS, «Sensitive Daten» – Zur Geschichte und Wirkung einer Fiktion, in: Brem Ernst/Druey Jean Nicolas/Kramer Ernst A./Schwander Ivo (Hrsg.), Festschrift Pedrazzini, Bern 1990, 469-493 (zit.: Daten)

SIMITIS SPIROS, Programmierter Gedächtnisverlust oder reflektiertes Bewahren: Zum Verhältnis von Datenschutz und historischer Forschung, in: Fürst Walther/Herzog Roman/Umbach Dieter C. (Hrsg.), Festschrift Zeidler, Bd. 2, Berlin 1987, 1475-1506 (zit.: Gedächtnisverlust)

SOLOVE DANIEL J., The Future of Reputation: Gossip, Rumor, and Privacy on the Internet, New Haven/London, 2007 (zit.: Reputation)

SOLOVE DANIEL J., A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3, 2006, 477-560 (zit.: Privacy)

SOLOVE DANIEL J., The Digital Person: Technology and Privacy in the Digital Age, New York University Press 2004 (zit.: Person)

SPÄRCK JONES KAREN, Privacy: What's different now?, Interdisciplinary Science Reviews, Vol. 28, No. 4, 2003, 287-292

SPECHT LOUISA, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, Köln 2012

SPECKER KARL, Die Persönlichkeitsrechte mit besonderer Berücksichtigung der Ehre im schweizerischen Privatrecht, Aarau 1911

STEINBUCH KARL, Die informierte Gesellschaft: Geschichte und Zukunft der Nachrichtentechnik, Stuttgart 1968

STEINMÜLLER WILHELM et al., Grundfragen des Datenschutzes: Gutachten im Auftrag des Bundesministeriums des Innern, Deutscher Bundestag, Drucksache VI/3828, Bonn 1972, 5-224

STIER MANUELA/HERBST DIETER, Corporate Identity Management: Wie Unternehmen ein Gesicht erhalten, in: Münch Peter/Ziese Hella (Hrsg.), Corporate Identity: Wie Unternehmensidentität aufgebaut, entwickelt und rechtlich abgesichert wird, Zürich/Basel/Genf 2012, 1-16

STRAUS FLORIAN/HÖFER RENATE, Entwicklungslinien alltäglicher Identitätsarbeit, in: Keupp Heiner/Höfer Renate (Hrsg.), Identitätsarbeit heute. Klassische und aktuelle Perspektiven der Identitätsforschung, Frankfurt am Main 1997, 270-307

STREMMEL RALF, Richard Ehrenberg als Pionier der Unternehmensgeschichtsschreibung oder: Wie unabhängig kann Unternehmensgeschichte sein?, in: Buchsteiner Martin/Viereck Gunther (Hrsg.), Richard Ehrenberg (1857 - 1921), «Ich stehe in der Wissenschaft allein.», Norderstedt 2008, 143-188

STROWEL ALAIN, Quand Google défie le droit: Plaidoyer pour un Internet transparent et de qualité, Bruxelles 2011

SUNSTEIN CASS R., On Rumors: How Falsehoods Spread, Why We Believe Them, What Can be Done, London 2009

SWEENEY LATANYA/ABU AKUA/WINN JULIA, Identifying Participants in the Personal Genome Project by Name, Harvard University, Data Privacy Lab, White Paper 1021-1, April 24, 2013

SWIRE PETER P./LITAN ROBERT E., None of your business: world data flows, electronic commerce, and the European Privacy Directive, Washington 1998

SZUBA DOROTHEE, Vorratsdatenspeicherung: Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, Baden-Baden 2011

TASIDOU AIMILIA/EFRAIMIDIS PAVLOS S., Using Personal Portfolios to Manage Customer Data, in: Joaquin Garcia-Alfaro/Navarro-Aribas Guillermo/Cuppens-Boulahia Nora/De Capitani di Vimercati Sabrina (Eds.), Data Privacy Management and Autonomous Spontaneous Security, Berlin 2012, 141-154

TEITLER MIRJAM, Der rechtskräftig verurteilte Straftäter und seine Persönlichkeitsrechte im Spannungsfeld zwischen öffentlichem Informationsinteresse, Persönlichkeitsschutz und Kommerz, Zürich 2008

TENE OMER/POLONETSKY JULES, Privacy in the Age of Big Data: A Time for Big Decicions, Stanford Law Review Online, Vol. 63, 2012, 63-69

TERCIER PIERRE, Le nouveau droit de la personnalité, Zürich 1984

THÖMEL JENS-ARNE, Datenbankverträge – Rechtsnatur und Haftung für fehlerhafte Information, Frankfurt am Main 2002

TREIBLMAIR HORST, Datenqualität und individualisierte Kommunikation: Potenziale und Grenzen des Internets bei der Erhebung und Verwendung kundenbezogener Daten, Wiesbaden 2006

TREYER TOBIAS, Das «Recht auf Vergessen» im digitalen Zeitalter, Medialex 2/2013, 61-62

TROLLER KAMEN, Grundzüge des schweizerischen Immaterialgüterrechts, 2. Aufl., Basel 2005

TRUDEL PIERRE, Law in Pursuit of Information Quality, in: Gasser Urs (Ed.), Information Quality Regulation: Foundations, Perspectives, and Applications, Baden-Baden, 2004, 91-105

TSCHENTSCHER AXEL, Das Grundrecht auf Computerschutz, AJP 4/2008, 383-393

TUTEN TRACY L./SOLOMON MICHAEL R., Social Media Marketing, Boston 2013

UHLIG KAI-PETER, Persönlichkeitsrecht im Film, AJP 3/2013, 327-335

UNSELD FLORIAN, Die Kommerzialisierung personenbezogener Daten, München 2010

VALLENDER KLAUS A., Kommentierung BV, 7. Abschnitt, in: ders./Ehrenzeller Bernhard/Schweizer Rainer J./Mastronardi Philippe (Hrsg.), Die Schweizerische Bundesverfassung: Kommentar, Art. 94-197, 2. Aufl., Zürich/St.Gallen 2008

VESTER FREDERIC, Denken, Lernen, Vergessen: Was geht in unserem Kopf vor, wie lernt das Gehirn, und wann lässt es uns im Stich?, 35. Aufl., München 2012

VESTING THOMAS, Das Internet und die Notwendigkeit der Transformation des Datenschutzes, in: Karl-Heinz Ladeur (Hrsg.), Innovationsoffene Regulierung des Internet, Baden-Baden, 2003, 155-190

VOGT WALTER, Vergessen und Erinnern, Werkausgabe, Dritter Band, Romane III, Zürich/Frauenfeld 1996

VON LEWINSKI KAI, Geschichte des Datenschutzes von 1600 bis 1977, in: Freiheit – Sicherheit – Öffentlichkeit, 48. Assistententagung Öffentliches Recht, Baden-Baden 2009, 196-220

WALDO JAMES/LIN S. HERBERT/MILLETT LYNETTE I., Engaging Privacy and Information Technology in a Digital Age, Washington, D.C. 2007

WANG RICHARD Y./STRONG DIANE M., Beyond Accuracy: What Data Quality Means to Data Consumers, Journal of Management Information Systems, Vol. 12, No. 4, 1996, 5-33

WARNER JEREMY, The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, University of Ottawa Law and Technology Journal, Vol. 2, No. 1, 2005, 75-104

WARREN SAMUEL D./BRANDEIS LOUIS D., The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, 1890, 193-220

WATZLAWICK PAUL/BEAVIN JANET H./JACKSON DONALD DALE: Menschliche Kommunikation: Formen, Störungen, Paradoxien, 8. Aufl., Bern/Stuttgart 1990

WEBER KARSTEN, Moral und Suchmaschinen, in: Lewandowski Dirk (Hrsg.), Handbuch Internet-Suchmaschinen, Nutzerorientierung in Wissenschaft und Praxis, Heidelberg 2009, 301-325 (zit.: Moral)

WEBER ROLF H., Neue Grundrechtskonzeptionen zum Schutz der Privatheit, in: ders./Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 7-29 (zit.: Grundrechtskonzeptionen)

WEBER ROLF H., The Right to Be Forgotten: More Than a Pandora's Box?, JIPITEC, Vol. 2., No. 2, 2011, 120-130 (zit.: Forgotten)

WEBER ROLF H., E-Commerce und Recht, 2. Aufl., Zürich 2010 (zit.: E-Commerce)

WEBER ROLF H., Shaping Internet Governance: Regulatory Challenges, Zürich 2009 (zit.: Governance)

WEBER ROLF H., Rundfunkrecht: Bundesgesetz vom 24. März 2006 über Radio und Fernsehen (RTVG), Bern 2008 (zit.: Rundfunkrecht)

WEBER ROLF H., Elektronische Aufbewahrung und Archivierung, recht 2004, 67-77 (zit.: Aufbewahrung)

WEBER ROLF H., Governance of Information Quality in Enterprises, in: Gasser Urs (Ed.), Information Quality Regulation: Foundations, Perspectives, and Applications, Baden-Baden 2004, 165-186 (zit.: Quality)

WEBER ROLF H., Persönlichkeitsrecht als Immaterialgut?, in: Honsell Heinrich/Zäch Roger/Hasenböhler Franz/Harrer Friedrich/Rhinow René (Hrsg.), Privatrecht und Methode: Festschrift Kramer, Basel/Genf/München 2004, 411-427 (zit.: Persönlichkeitsrecht)

WEBER ROLF H., Rechtsfragen rund um Suchmaschinen, Zürich 2003 (zit.: Suchmaschinen)

WEBER ROLF H., Information und Schutz Privater, ZSR 1999 II, 1-86 (zit.: Schutz)

WEBER ROLF H., Zivilrechtliche Haftung auf dem Information Highway, in: Hilty Reto M. (Hrsg.), Information Highway, Beiträge zu rechtlichen und tatsächlichen Fragen, Bern/München 1996 (zit.: Haftung)

WEBER ROLF H./FERCSIK SCHNYDER ORSOLYA, «Was für 'ne Sorte von Geschöpf ist euer Krokodil?» – zur datenschutzrechtlichen Qualifikation von IP-Adressen, sic! 9/2009, 577-589

WEBER ROLF H./SOMMERHALDER MARKUS, Das Recht der personenbezogenen Information, Zürich 2007

WEBER ROLF H./WILLI ANNETTE, IT-Sicherheit und Recht: Grundlagen eines integrativen Gestaltungskonzepts, Zürich 2006

WEICHERT THILO, Datenschutz bei Suchmaschinen, in: Lewandowski Dirk (Hrsg.), Handbuch Internet-Suchmaschinen, Nutzerorientierung in Wissenschaft und Praxis, Heidelberg 2009, 285-300

WELZER HARALD, Das kommunikative Gedächtnis: Eine Theorie der Erinnerung, 2. Aufl., München 2008

WERRO FRANZ, The Right to Inform vs. The Right to be Forgotten: A Transatlantic Clash, in: Colombi Ciacchi Aurelia/Godt Christine/Rott Peter/Smith Leslie Jane (Hrsg.), Haftungsrecht im Dritten Millennium, Baden-Baden 2009, 285-300

WESTIN ALAN F., Computers, health records, and citizen rights, Washington 1976 (zit.: Computers)

WESTIN ALAN F., Privacy and Freedom, 6th Ed., New York 1970 (zit.: Privacy)

WESTIN ALAN F./BAKER MICHAEL A., Databanks in a Free Society: Computers, Record-Keeping and Privacy, New York 1972

WHITE GARRY L./MÉNDEZ MEDIAVILLA FRANCIS A./SHAH JAYMEEN R., Information Privacy: Implementation and Perception of Laws and Corporate Policies by CEOs and Managers, in: Nemati Hamid R., Privacy Solutions and Security Frameworks in Information Protection, Hershey, PA 2013, 52-69

WILDHABER BRUNO, Privacy: Die Rolle von IT-Sicherheit und IT-Revision, in: Baeriswyl Bruno/Rudin Beat (Hrsg.), Perspektive Datenschutz, Zürich/Baden-Baden/Wien 2002

WILLI ERNST, «Master your past and you will master the future»: Die Bedeutung der Unternehmensarchive für die Unternehmen, in: Schweizerisches Wirtschaftsarchiv/Verein Schweizerischer Archivarinnen und Archivare (Hrsg.), Baden 2006, 32-37

WILLIAMS CAROLINE, Records and archives: concepts, roles and definitions, in: Brown Caroline (Ed.), Archives and Recordkeeping: Theory into practice, London 2014, 1-29

WILLKE HELMUT, Systemisches Wissensmanagement, 2. Aufl., Stuttgart 2001

WITSCHI PETER, Öffentliche Archive und regionale Unternehmenswelten: Strukturanalyse, Dokumentationsprofil und Bewertungsmodell, in: Schweizerisches Wirtschaftsarchiv/Verein Schweizerischer Archivarinnen und Archivare (Hrsg.), Baden 2006, 79-87

WOERTGE HANS-GEORG, Die Prinzipien des Datenschutzrechts und ihre Realisierung im geltenden Recht, Heidelberg 1984

WORLD ECONOMIC FORUM, Unlocking the Value of Personal Data: From Collection to Usage, Cologny/Geneva 2013 (zit. Value)

WORLD ECONOMIC FORUM, Rethinking Personal Data: Strengthening Trust, Geneva 2012 (zit.: Data)

ZEDER MARIANNE, Haftungsbefreiung durch Einwilligung des Geschädigten: eine rechtsvergleichende Betrachtung unter Einschluss des Handelns auf eigne Gefahr im Bereich des Sports, Zürich 1999

ZEHNDER CARL AUGUST, Datenschutz aus der Sicht eines Informatikers – seit es Datenbanken gibt, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing: 20 Jahre Datenschutz in der Schweiz, Zürich/Basel/Genf 2012, 147-155

ZEUNERT CHRISTIAN/ROSENTHAL DAVID, E-discovery and data protection: Challenges and solutions for multinational companies, Jusletter IT, Juni 2012

ZIKOPOULOS PAUL C./EATON CHRIS/DEROOS DIRK/DEUTSCH THOMAS/LAPIS GEORGE, Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data, New York, 2012

ZIMMERMANN REINHARD, Comparative foundations of a European law of set-off and prescription, Cambridge 2010

ZIPPELIUS REINHOLD, Geschichte der Staatsideen, 10. Aufl., München 2003

ZITTRAIN JONATHAN, The Future of the Internet: And How to Stop It, New Haven 2008

ZIMBRADO PHILIP/BOYD JOHN, Die neue Psychologie der Zeit, Heidelberg 2009

ZÖLLNER WOLFGANG, Rechtsgüterschutz im Rahmen sinnvoller Informationsordnung, in: Wilhelm Rudolf (Hrsg.), Information, Technik, Recht: Rechtsgüterschutz in der Informationsgesellschaft, Darmstadt 1993, 35-45

ZÜND ANDRÉ, Unternehmensgeschichte: Bedeutung – Forschung – Quellen, Schweizer Treuhänder 9/2005, 666-671

Materialienverzeichnis

Schweiz

Bericht des Bundesrates, Kollektiver Rechtsschutz in der Schweiz – Bestandesaufnahme und Handlungsmöglichkeiten, Bern, 3. Juli 2013 (zit.: Bericht des Bundesrates, Kollektiver Rechtsschutz)

Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335 ff. (zit.: BBl 2012)

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003 2101 ff. (zit.: BBl 2003)

Botschaft zur Totalrevision des Bundesgesetzes über Radio und Fernsehen (RTVG) vom 18. Dezember 2002, BBl 2003 III 1569 ff. (zit. BBl 2003 III)

Botschaft über das Bundesgesetz über die Archivierung vom 26. Februar 1997, BBl 1997 II 941 ff. (zit.: BBl 1997 II)

Botschaft über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 1 ff. (zit. BBl 1997 I)

Botschaft zum Bundesgesetz über den Datenschutz vom 23. März 1988, BBl 1988 II 413 ff. (zit.: BBl 1988 II)

Botschaft über die Änderung des Schweizerischen Zivilgesetzbuches vom 5. Mai 1982, BBl 1982 II 636 ff. (zit.: BBl 1982 II)

Bundesbeschluss betreffend die historische und rechtliche Untersuchung des Schicksals der infolge der nationalsozialistischen Herrschaft in die Schweiz gelangten Vermögenswerte vom 13. Dezember 1996, AS 1996 3487 (zit.: AS 1996, 3487)

Europäische Union

Der Europäische Datenschutzbeauftragte, Stellungnahme des Europäischen Datenschutzbeauftragten zur Stärkung des Vertrauens in die Informationsgesellschaft durch die Förderung des Schutzes von Daten und Privatsphäre, Brüssel 16.10.2010, ABl C 280/1 (zit.: Stellungnahmen, ABl C 280/1)

Erläuterungen zur Charta der Grundrechte, Brüssel 14.12.2007, ABl C 303/02 (zit.: ABl C 303/02)

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Gesamtkonzept für den Datenschutz in der Europäischen Union, Brüssel 4.11.2010, KOM(2010) 609 endgültig (zit.: Europäische Kommission, KOM(2010) 609 endgültig)

Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Brüssel 25.1.2012, KOM(2012) 11 endgültig (zit.: Europäische Kommission, KOM(2012) 11 endgültig)

Zusammenfassung

Das Informationsmanagement umfasst die Bearbeitung von Informationen in Unternehmen. Das übergeordnete Ziel des Informationsmanagements besteht in der Gestaltung und Nutzung von Information als Ressource für das unternehmerische Denken und Handeln. In zeitlicher Hinsicht orientiert sich das Informationsmanagement an den normativen Vorgaben, die sich in explizit und implizit zeitbezogene Normen unterteilen lassen. Die explizit zeitbezogenen Normen beziehen sich hauptsächlich auf die Aufbewahrung relevanter Informationen über einen definierten Zeitraum. Den implizit zeitbezogenen Normen liegt dagegen der Schutz subjektiver Rechte zugrunde.

Sowohl die explizit zeitbezogenen Normen als auch die implizit zeitbezogenen Normen weisen einen Konfliktbezug auf. Der zeitbezogene Schwerpunkt des Konflikts liegt in den gegensätzlichen Interessen am Erhalt und der Nutzung von Daten einerseits und an der Vernichtung und Unterlassung weiterer Bearbeitungen andererseits. Das Recht erfasst diesen Konflikt in zeitlicher Hinsicht nur begrenzt. So sehen die explizit zeitbezogenen Normen keine Pflicht zum Erhalt von Daten über den gesetzlich definierten Zeitraum hinweg vor. Allfällige Interessen an einer späteren Bearbeitung solcher Daten finden unter Privaten grundsätzlich keine Berücksichtigung. Die implizit zeitbezogenen Normen sehen dagegen im Rahmen des Persönlichkeits- und Datenschutzrechts umfassende Abwehrrechte seitens des Betroffenen gegenüber dem Bearbeiter personenbezogener Daten vor. Die Grenze dieser Normen liegt in der mangelnden Konkretisierung.

Die Konfliktfälle werden im Rahmen dieser Arbeit durch eine Integration zeitbezogener Aspekte in bestehende und zusätzliche Normen, die den Umgang mit personenbezogenen Daten durch Unternehmen regeln, gelöst. Im Rahmen eines mehrdimensionalen Ansatzes wird die zeitliche Dimension mit qualitativen und quantitativen Aspekten von Daten in Bezug gesetzt. Im Bereich der explizit zeitbezogenen Normen werden anhand dieses integrativen Ansatzes die rechtlichen Ausgestaltungsmöglichkeiten für einen langfristigen Erhalt von historisch und wissenschaftlich relevanten Unternehmensdaten geprüft. Der Bereich der implizit zeitbezogenen Normen umfasst dagegen eine Konkretisierung der Anwendung bestehenden Rechts sowie einen Vorschlag für eine mögliche Anpassung des Datenschutzrechts.

Abstract

Information Management covers the processing of data within corporations. The major goal of Information Management is to structure and to make use of information as a resource for entrepreneurial thinking and action. In terms of time, Information Management is oriented on the normative guidelines, which can be categorized in explicitly and implicitly time-related legal provisions. Explicitly time-related legal provisions are mainly related to storage requirements for relevant information over a defined period of time. Implicitly time-related legal provisions on the other hand are mainly focused on personal rights.

The explicitly time-related and the implicitly time-related legal provisions are essentially oriented towards situations of conflict. The time-related core area of the conflict lies in opposing interests regarding data preservation and usage on the one side as well as the destruction and omission of further processing on the other side. The law addresses this conflict only partially with regard to time. In accordance with that finding, the explicitly time-oriented laws do not entail a duty to retain data beyond the stated time frame. Legitimate interests in a later processing of such data are excluded from consideration among private parties. The implicitly time-related norms on the other hand provide for extensive individual rights of defence as a part of personal rights and data protection law. The limitation of these laws lies in the absence of concretisation.

The dissertation provides a solution for the conflicts mentioned above by integrating time-related aspects of personal data processing into existing regulation and by proposing a new framework. Within a multidimensional approach, time is being correlated with qualitative and quantitative aspects of data. In the area of explicitly time-related legal provisions, possible legal regulation for a long-term preservation of scientifically or historically relevant company data is being assessed by means of the multidimensional approach. In contrast, the area of implicitly time-related laws is addressed by concretising the application of existing legal rules and by proposing a possible amendment of data protection law.

Sommaire

La gestion de l'information a pour objet le traitement des informations au sein des entreprises. La gestion de l'information consiste à formuler et à diffuser l'information en tant qu'elle constitue une ressource utile à la réflexion et à l'action au sein de l'entreprise. Sous l'angle temporel, la gestion de l'information repose sur une législation qui se divise en dispositions se rapportant explicitement et implicitement au temps. Les dispositions de nature explicitement temporelles ont principalement pour objet la conservation des informations objectivement pertinentes sur une période définie. Les normes de nature implicitement temporelles tendent en revanche à protéger les droits subjectifs.

Tant les normes de natures explicitement temporelles que celles de nature implicitement temporelles peuvent entrer en conflit. Le point de conflit temporel se situe entre d'une part l'intérêt à la conservation et à l'utilisation de données et, d'autre part, l'intérêt à leur destruction et partant à l'abandon de leur utilisation prolongée. Le droit ne tient compte de ce conflit d'ordre temporel que de manière limitée. Les normes de nature explicitement temporelles ne prévoient ainsi pas l'obligation de conserver des données au-delà de la durée définie par la législation applicable en la matière. Un intérêt éventuel à un traitement ultérieur de telles données ne rencontre en principe que peu d'écho auprès des particuliers. En revanche, en matière de protection de la personnalité et des données, les normes de nature implicitement temporelles prévoient pour les personnes lésées la mise œuvre de droits de défense contre tout tiers ayant traité des données personnelles. Ces normes ne sont toutefois guère appliquées.

Dans le cadre de cette contribution, les cas de conflit sont résolus en intégrant les éléments d'ordre temporel dans des dispositions légales existantes ou complémentaires et qui régissent le traitement des données personnelles par les entreprises. Plusieurs solutions sont proposées dans une approche pluridisciplinaire dans laquelle la dimension temporelle est mise en relation avec les aspects qualitatifs et quantitatifs des données. En matière de normes explicitement temporelles, les possibilités de donner un cadre légal pour permettre une conservation prolongée des données d'importance historique et scientifique pour les entreprises sont examinées à l'aune de cette approche. Les normes implicitement temporelles sont en revanche de nature à concrétiser l'application du droit en vigueur et à offrir des possibilités d'adaptation du droit de la protection des données.

Einführung

Aktion, Interaktion und Kommunikation werden durch die Entwicklung neuer Technologien zunehmend zum Gegenstand digitaler Systeme. Die dadurch entstehenden Informationsquellen prägen das kulturelle, politische und wirtschaftliche Umfeld. Im Zuge dieser Entwicklung spielen Unternehmen als Informationsbearbeiter eine zentrale Rolle. In der vorliegenden Arbeit wird im Wesentlichen auf die spezifischen Aspekte des Informationsmanagements in Unternehmen und deren zeitliche Dimension eingegangen. Im Vordergrund stehen die Prozesse des Speicherns, Verwertens und Löschens von (personenbezogenen) Daten. Die unternehmensseitigen Ziele und Interessen an der Bearbeitung werden jenen der Individuen und der Öffentlichkeit gegenübergestellt und hinsichtlich der sich daraus ergebenden Konflikte untersucht. Im Zentrum steht die Frage, in welcher Weise das Recht den Umgang mit Informationen durch Unternehmen in zeitlicher Hinsicht ordnet und ob vor dem Hintergrund der technologischen Entwicklung eine Konkretisierung dieser Ordnung angezeigt ist. Auch der einzelne Mensch als Subjekt von Erinnerung und Gedächtnis steht in Abhängigkeit zu den Rahmenbedingungen, die sein Erinnern und Vergessen organisieren[1]. In einem grösseren Kontext stehen Speichern und Löschen der linearen Datenbearbeitung in digitalen Systemen somit in einem Zusammenhang mit den komplexen Vorgängen des menschlichen Erinnerns und Vergessens.

An dieser Ausgangslage orientiert sich die *Methodik der Arbeit*[2]. Diese ist sowohl interdisziplinär als auch phänomenologisch geprägt[3]. Die Prägung ist im Wesentlichen durch den informationsrechtlichen Ansatz bedingt[4]. Überall dort, wo das Recht eine Steuerung anstrebt, müssen gleichzeitig Informationen gesteuert werden. Informationsrecht entsteht folglich im Rahmen dieser Steuerungsziele[5]. Der informationsrechtliche Ansatz bildet eine spezifische Betrachtungsweise auf Erscheinungen an der Schnittstelle gesellschaftlicher Teilsysteme von Recht, Technologie, Ökonomie und Politik[6]. Das

---

1 ASSMANN, Gedächtnis, 36; RECK, 78; HUBER, Erinnern, 111. Eine Annäherung an die Phänomene der Erinnerung, der Geschichte und des Vergessens findet sich bei RICOEUR, 643-656.

2 Methodisch ist ein Vorgehen dann, wenn es überprüfbaren Regeln folgt und einen rational nachvollziehbaren Prozess aufweist. Auch in der Rechtssetzung ist heute die Existenz einer Methodik unbestritten; siehe MÜLLER, Rechtssetzungslehre, Rn. 50.

3 Siehe zur Notwendigkeit der Interdisziplinarität und zur Klärung der bestehenden Verhältnisse MÜLLER, Rechtssetzungslehre, Rn. 2, m.w.H.; RICHLI, 6; zum Begriff, ders., 8 ff.

4 Vgl. dazu die Hinweise bei GASSER, Law, 24.

5 DRUEY, Information, 40; siehe auch LIEDTKE, 269, wonach Informationsrecht die Aufklärung des Informationsbegriffs und seiner Bedeutung für das Recht zum Gegenstand hat.

6 BURKERT, Aufgaben des Informationsrechts, 156.

Informationsrecht setzt sich im Rahmen dieser Betrachtung hauptsächlich mit der Identifikation und Analyse informationeller Sachverhalte auseinander[7].

Die technischen Möglichkeiten haben den Trend der Informationserhaltung und Informationsverknüpfung wesentlich verstärkt. Ökonomische Faktoren, beispielsweise in Form von sinkenden Kosten für Speichermedien oder neuen Unternehmensstrategien, sind ein weiterer Grund für eine verstärke Nutzung und die gesellschaftliche Integration dieser Technologien. Die Frage, ob das Recht die informationellen Phänomene in ihrer zeitlichen Wirkung zureichend erfasst, kann ohne Rücksicht auf diese Gebiete nicht beantwortet werden. In Bezug auf die Ausgestaltung der Normen bleibt die Perspektive weitgehend auf die aktuellen Verhältnisse und den Nachvollzug des bereits eingetretenen Wandels beschränkt. Die Gestaltung künftiger Entwicklungen steht bei der Rechtssetzung nicht im Vordergrund[8]. Aufgrund der querschnittartigen Materie der zeitlichen Dimension erscheinen die Abstraktion und die Selektion ausgewählter Problemstellungen als angemessene Mittel zur Durchdringung der Materie. Für ein besseres Verständnis der zeitlichen Aspekte des Informationsmanagements sind insbesondere folgende Fragen auf unterschiedlichen Abstraktionsstufen von Bedeutung: Welche Vorgänge führen zu einer Aufnahme von Informationen durch Unternehmen? Aus welchen Gründen und für wie lange bleiben die Informationen im Unternehmen erhalten? Wer hat Zugriff auf die Informationen und wie werden diese durch das Unternehmen bzw. durch Dritte genutzt? Werden die Informationen zu einem bestimmten Zeitpunkt gelöscht oder bleiben sie «ewig» erhalten? Die Darstellung der rechtlichen Normen konzentriert sich auf die Analyse ihrer zeitlichen Dimension. Im Vordergrund steht die Frage, inwiefern die Bearbeitung von Daten in zeitlicher Hinsicht von den bestehenden Normen erfasst wird und ob die Wahrung der unterschiedlichen Interessen eine Konkretisierung der bestehenden bzw. neue Normen erfordert.

Der *Aufbau der Arbeit* gliedert sich in fünf Teile: *Im ersten Teil* wird der Gegenstand der Betrachtung definiert. Gegenstand der Betrachtung ist die Information im Kontext technologischer und ökonomischer Entwicklungen. In Bezug auf das Recht wird eine Unterteilung in explizit und implizit zeitbezogene Normen vorgenommen, die durch eine Auswahl an relevanten Gesetzen reflektiert wird. *Im zweiten Teil* folgt eine Darstellung der zeitbezogenen Normen im geltenden Recht, die im Grundsatz der genannten Unterteilung in explizit und implizit zeitbezogene Normen folgt. *Im dritten Teil* wird das Informationsmanagement vor dem Hintergrund der im zweiten Teil darge-

---

7 GASSER, Law, 13.

8 MÜLLER, Rechtssetzungslehre, Rn. 17 ff.

stellten Normen zum Umgang mit Informationen als Konfliktgegenstand betrachtet. Die konfliktbezogene Betrachtungsweise fusst auf der Erkenntnis, dass Normen und insbesondere das Recht auf die Lösung bzw. Vermeidung von Konflikten ausgelegt sind und sich das Informationsmanagement an diesen Konflikten orientiert. *Im vierten Teil* folgt eine Auseinandersetzung mit den Grenzen der relevanten Normen im Hinblick die Lösung der beschriebenen Konflikte. Nebst den im zweiten Teil dargelegten explizit und implizit zeitbezogenen Normen des Rechts wird auch auf organisationsbasierte Konkretisierungen zeitlicher Normen eingegangen. *Im fünften Teil* wird unter Berücksichtigung der Grenzen bisheriger Ansätze ein mehrdimensionaler Lösungsansatz aufgezeigt, dessen Konkretisierung sowohl unter Ausschluss von Anpassungen der Rechtsordnung als auch unter Einschluss solcher Anpassungen erfolgen kann.

A. Grundlagen und Eingrenzung

I. Gegenstand der Betrachtung

1. Information

1.1 Begriff und Eigenschaften

Der Begriff der Information umfasst im Wesentlichen zwei Merkmale: Einen Informationsvorgang als Voraussetzung der Entstehung und einen interpretationsbedürftigen Sinngehalt der Informationsgrundlage[9]. Das Datum als kleine Teileinheit der Information stellt eine mögliche Informationsgrundlage dar und dient entsprechend zur Erfassung des Sinngehalts von Information[10]. «Digitale» Daten sind in Form einer Zeichenfolge codiert[11]. Informationen können auch als Resultat eines Wissenszuwachses, als Wissensinhalt oder als Zustand der Kenntnis bezeichnet werden[12]. Das aus der Information resultierende Wissen ist demnach etwas, das gegenüber Daten einen Mehrwert aufweist[13]. Diese Deutung legt nahe, dass Informationen nicht Gegenstand objektiver Existenz sind, sondern der Wahrnehmung und Interpretation ihres Empfängers bedürfen[14]. Die Information ist Bestandteil der Kommunikation, die neben einem Inhalts- auch einen Beziehungsaspekt aufweist[15]. Die zentrale Bedeutung dieser Vorgänge spiegelt sich im Zwiegespräch und auf globaler Ebene gleichermassen. Der Austausch von Information und Wissen ist ein Fundament der menschlichen Existenz. Vor diesem Hintergrund ist es wenig erstaunlich, dass Adressat, Gegenstand und Vorgang der Kommunikation und der Zugriff auf Informationen schon lange kontrovers diskutiert werden[16].

---

9 SPECHT, 23; siehe auch DRETSKE, 44: «[...] *information is that commodity capable of yielding knowledge, and what information a signal carries is what we can learn from it.*».

10 DRUEY, Information, 20.

11 BORGHOFF et al., 11.

12 DRUEY, Information, 5 f.; zur Wissensdefinition ders., 25; KUHLEN, 344; ASSMANN, Vergangenheit, 210; siehe zu den Bedeutungsvarianten von Information GASSER, Kausalität, 31 f.; zur Problematischen Gleichsetzung von Information und Wissen (im Sinn von Kennen) ROSEN, Gaze, 201; NONAKA/TAKEUCHI, 58, grenzen Wissen und Information wie folgt ab: «[...] *information is a flow of messages, while knowledge is created by that very flow of information, anchored in the beliefs and commitment of its holder*.».

13 LINDE, 6; WILLKE, 7 ff.; KUHLEN, 82.

14 ALBERS, Grundlagen, § 22 Rn. 12; DRUEY, Information, 356; LINDE, 7; so auch Art. 3 lit. a. FMG in dem Informationen als «für den Menschen, andere Lebewesen oder Maschinen bestimmte Zeichen, Signale, Schriftzeichen, Bilder, Laute und Darstellungen jeder anderen Art» definiert werden.; siehe zur Wahrnehmung eingehend SAYRE, 153 ff.

15 WATZLAWICK/BEAVIN/JACKSON, 53.

16 DUMAS, 2.

Das Wesen der Information als ein vielfältiger Vorgang zeigt sich darin, dass ihre Qualität und die entsprechenden Mängel in einer Vielzahl von Formen auftreten können[17]. Das Spektrum reicht von falscher und richtiger Information über weitere Eigenschaften wie Klarheit, Verständlichkeit, Zugänglichkeit, Vollständigkeit und Zeitnähe[18]. Mängel der Information wie Unwahrheit, Unvollständigkeit oder fehlende Aktualität entwerten die Information nicht nur, sie können unter Berücksichtigung des Aufwands der Informationsbeschaffung auch zu einem Negativwert führen[19]. In der empirischen Datenanalyse wird trotz fehlender Werte von einer hohen Datenqualität ausgegangen, wenn ein Kompensationsverfahren zu einer angemessenen bzw. zu einer nicht verzerrten Schätzung führt[20].

Die Möglichkeit der Verknüpfung einer Information mit weiteren Informationen beeinflusst den Informationsgehalt entscheidend, das Bedürfnis nach weiteren Informationen kann daher als unerschöpflich erachtet werden[21]. Bereits in den Neunzigerjahren ergab eine Studie des Finanzinformationsdienstleistungsunternehmens Reuters, dass Informationen zur neuen Droge werden könnten[22]. Die Problematik der Informationsüberlastung bestand jedoch schon lange vor der Entwicklung elektronischer Medien[23]. Informationen weisen grundsätzlich eine spiegelbildliche Eigenschaft auf; die wachsende Konzentration von Daten widerspiegelt die zunehmende Komplexität gesellschaftlicher Verhältnisse[24].

Ein Teil der Verknüpfung einer Information mit weiteren Informationen bildet der Kontext. Der Kontext ist selbst Information und auch ein Aspekt der Informationsqualität. Informationen bilden oft eine kontextuelle Einheit, eine Mischung aus wahren, falschen, präzisen und weniger präzisen Informationsteilen. In Abhängigkeit zur Verteilung ergibt sich daraus die Richtigkeit oder Unrichtigkeit der gesamten Information bzw. der Nachricht[25].

---

17 Eingehend TREIBLMAIER, 31 ff.

18 DRUEY, Information, 66; ALBERS, Human-Information, 146 f.; LYRE, 211.

19 DRUEY, Information, 66.

20 BACKHAUS/BLECHSCHMIDT, 266.

21 DRUEY, Information, 9; vgl. auch SAYRE, 23, der Information als erhöhte Wahrscheinlichkeit definiert.

22 Glued to the Screen: An Investigation into Information Addiction Worldwide, Reuters 1997; siehe dazu ROSENTHAL, süchtig, o.S.; siehe auch SHAPIRO/VARIAN, 6.

23 Siehe dazu die historische Darstellung bei GLEICK, 401 ff.

24 SEIDEL, Datenbanken, 159.

25 Vgl. DRUEY, Information, 243.

1.2 Zuordnung

a) Information als Gemeingut

Die traditionelle Haltung gegenüber Information an sich kann dahingehend zusammengefasst werden, dass Information grundsätzlich als nicht zuordenbar und besitzbar erachtet wird[26]. In der Ökonomie entspricht die eigentumsrechtliche Zuordnung von Information nicht einer Grundannahme, Information gilt als Gemeingut. Sie wird als nicht knappes und damit nicht als Wirtschaftsgut betrachtet. Diese Zuordnung gründet auf der Annahme, dass sie unbeschränkt verbreitet werden und vom Informanten gleichzeitig behalten werden kann[27]. Aus ökonomischer Sicht steht dieser Zuordnung aber gerade die Werthaltigkeit von Information durch ihre verhältnismässige Ausschliesslichkeit und der für ihre Erlangung notwendige Aufwand entgegen[28]. Diese Zuordnung orientiert sich jedoch nicht an der Information selbst, sondern an den spezifisch wertgenerierenden Faktoren[29].

b) Information als Wirtschaftsgut

Informationen stehen in einer Wechselbeziehung mit der Wirtschaft[30]. Die wirtschaftliche Tätigkeit ist geprägt von einer zunehmenden Informationsdichte, die wiederum zu neuen Bedürfnissen in Bezug auf die Bewältigung der zusätzlichen Informationen führt[31]. Die Verdinglichung der Information ist nicht nur in der Technologie, sondern vor allem auch in der Ökonomie erfolgt[32]. Daten sind zum Rohstoff, zum Wettbewerbsfaktor[33] und zu einem eigenständigen Wirtschaftsgut geworden[34]. Information wird zum knappen Gut, wenn zu ihrer Beschaffung Arbeit und Kapital aufgewendet

---

26 LINDE, 14 ff. Auch die Gewährung exklusiver Rechte für Immaterialgüter in Form von Patenten, Urheberrechten, Marken und Designs gewährt keine umfassende Kontrolle über Informationen, da die Durchsetzung dieser Rechte durch die einfache Kopier- und Übertragbarkeit gefährdet ist, SHAPIRO/VARIAN, 4; ähnlich LINDE, 19, der auf den häufig grossen Aufwand zur Durchsetzung von Rechten des geistigen Eigentums und die unsichere Durchsetzung des Ausschlussprinzips bei der Verteilung von Wissen auf mehrere Individuen verweist.

27 DRUEY, Information, 100; DRUCKER, 63 f.

28 DRUEY, Information, 100; VON HAYEK, 80, weist grundlegend darauf hin, dass die wertvolle Information inhaltlich oft spezifisch ist und die Suchkosten entsprechend steigen.

29 DRUEY, Information, 100.

30 LINDE, 12 f.

31 EVANS/WURSTER, 11 f.

32 GASSER, Informationsqualität, 380 ff.

33 PICOT/MAIER, 33 ff.; AUGUSTIN, 185, 205; SIEBER, 2569; MAYER-SCHÖNBERGER/CUKIER, 182.

34 PICOT/MAIER, 45; PETHIG, 2.

werden müssen[35]. Die Produktion von Information ist dabei kostspielig, die Reproduktion dagegen ist billig[36].

Rechtlich ist die Begründung eines eigentumsrechtlichen Anspruchs aufgrund des Einsatzes von Arbeit und Kapital im Institut der Verarbeitung in Art. 726 ZGB angelegt[37]. Ein konkretes Beispiel für die Aufwendung von Arbeit und Kapital zur Generierung von Information ist die Marktforschung[38]. Gegen Ende des 19. Jahrhunderts wurde die Markteinschätzung aufgrund der Entstehung anonymer Massenmärkte für die Unternehmen zunehmend schwieriger. Mitte des 20. Jahrhunderts verschob sich dann auch die Vermittlerrolle des Handels zwischen Produzenten und Konsumenten immer mehr in Richtung der Marktforschungsinstitute. In einem engen Zusammenhang mit der Entwicklung der Markforschung standen zudem die zunehmende Bedeutung der Werbung und die Entwicklung des Markenartikelsystems[39]. Ähnlich der Werbung kann die Markforschung als Mittlerin zwischen Angebot und Nachfrage bezeichnet werden, die zur Überbrückung von Informationslücken dient[40]. Der Konsum ist im Laufe dieser Entwicklung auch begrifflich über seine lateinische Wurzel *cum sumere* (aufnehmen, verbrauchen, verzehren) hinausgewachsen und umfasst aus konsumsoziologischer Perspektive einen dynamischen Prozess mit mehreren Phasen, der bei der Entstehung von Bedürfnissen anfängt, über die Informationsgewinnung, die Entscheidung über den

---

35 DRUEY, Information, 99; WEBER, Quality, 179. Siehe grundlegend PICOT/FRANCK, 545, die als weiteres Kriterium den Aspekt der Nutzung von Information anführen. Siehe zur Notwendigkeit von Arbeit und Kapital in Bezug auf Suchmaschinen MAASS et al., 10, m.w.H. Google beispielsweise benötigt ca. 450'000 Server zur Erbringung des Suchangebots; siehe ferner WEBER, Moral, 317, der auf die unentgeltliche Leistung von Suchmaschinen trotz hoher Kosten hinweist. Anders LINDE, 21, der nur geheim gehaltene oder rechtlich geschützte Informationsgüter den knappen Gütern zuordnet und Güter bei denen das Ausschlussprinzip nicht angewandt werden kann oder bei denen keine Rivalität im Konsum vorliegt als sogenannte «Mischgüter» bezeichnet.

36 SHAPIRO/VARIAN, 3; LINDE, 14.

37 DRUEY, Information, 99; vgl. auch SAMUELSON, 1133, mit Hinweisen darauf, dass einige Unternehmen aus dem Einsatz von Kapital und Arbeit in die Sammlung, Organisation und Verarbeitung von Daten einen entsprechenden Eigentumsanspruch ableiten.

38 Treffend in Hinblick auf den Informationsbedarf GALOUYE, 10: «Nun, sehen Sie, Miss Ford, wir leben in einer komplizierten Gesellschaft, die es vorzieht, dem Wettbewerb alle Risiken zu nehmen. Deshalb gibt es auch mehr Meinungsforschungsinstitute als ein normaler Sterblicher zu zählen vermag. Bevor wir ein Produkt auf den Markt bringen, wollen wir erfahren, wer es kaufen wird, wie oft und was man dafür anlegen will; welche Gründe für Bekenntniswechsel massgebend sind; welche Chancen Gouverneur Stone hat, wieder gewählt zu werden; welche Waren besonders viel verlangt werden; ob Tante Bessie in der nächsten Modesaison Blau oder Rosa vorzieht.».

39 KOSCHEL, 34; HANSEN/BODE, 33 ff.

40 Vgl. BURT, 1 ff.; siehe auch PEPELS, 161, der Markforschung als «systematische Sammlung, Aufbereitung, Analyse und Interpretation von Daten über Märkte und Marktbeeinflussungsmöglichkeiten zum Zweck der Informationsgewinnung für Marketing-Entscheidungen» definiert.

Erwerb zur Nutzung resp. zum Verbrauch führt und mit der Entsorgung endet[41]. Im Jahr 2012 generierte die Marktforschungsindustrie gemäss einem von der European Society for Opinion and Marketing Research (ESOMAR) erstellten Bericht einen weltweiten Umsatz von 33,5 Milliarden US-Dollar. Das inflationsbereinigte Wachstum betrug 0,4 Prozent[42]. Diese geringe Zuwachsrate kann einerseits auf die ökonomischen und politischen Turbulenzen im Euroraum zurückgeführt werden[43], andererseits hat die Ausweitung internetbasierter Angebote zu einem direkteren Informationsaustausch zwischen Konsumenten und Produzenten geführt[44]. Bedeutend sind ferner Angebote, die eine direkte Auswertung von Nutzerinformationen zulassen[45]. Auch die internetbasierte Auswertung ändert indessen wenig an der Tatsache, dass für die Informationsbeschaffung Arbeit und Kapital aufgewendet werden müssen[46]. Die Informationsbeschaffung durch die Kommunikation zwischen Unternehmen und Individuen erfordert das Bereitstellen und Unterhalten einer entsprechenden Infrastruktur. Die genannten Erfordernisse zur Qualifikation als knappes Gut können entsprechend auch im Hinblick auf personenbezogene Daten grundsätzlich als erfüllt erachtet werden.

Information wird aufgrund unterschiedlicher Kriterien nicht nur als knappes Gut und damit als Wirtschaftsgut bewertet, sondern als eigenständiges Produkt[47]. SHAPIRO/VARIAN definieren Informationsprodukte als Produkte, die kodifiziert oder digitalisiert werden können[48]. SARVARY hält diese Definition für zu weit, da sie beispielsweise die Musikindustrie und die medizinische Diagnostik gleichermassen umfassen könne, ohne dass diese mehr gemeinsam hätten, als dass ihre Produkte in Form digitaler Codes transportiert werden können. SARVARY grenzt den informationellen Produktbegriff entsprechend ein und geht nur von Informationen aus, die für Entscheidungen genutzt

41 SCHNEIDER, Konsum, 11.

42 ESOMAR, Industry Report, Global Market Research 2012, 6.

43 ESOMAR, Industry Report, Global Market Research 2012, 6.

44 KOSCHEL, 48 f.; BOSTON CONSULTING GROUP, 26.

45 Siehe KOSCHEL, 48, der auf das Internet als öffentlichen Raum verweist und die verbesserte Informationslage für die Marktforschung hervorhebt.

46 In Anbetracht des wirtschaftlichen Wettbewerbs ist im Gegenteil sogar eher von steigenden Kosten auszugehen, sofern der relative Informationsanteil berücksichtigt wird.

47 LINDE, 8, 13, 37, 83; KUHLEN, 83 f.; AUGUSTIN, 53 ff., 72.

48 Siehe SHAPIRO/VARIAN, 3, die als Beispiele Baseballresultate, Bücher, Datenbanken, Magazine, Filme, Musik, Aktienkurse und Websites anführen.

werden und für die der Entscheidungsträger eine Zahlungsbereitschaft signalisiert[49]. Eine physische Komponente weist Information insofern auf, als dass sie Systeme nutzbar macht und damit Werkerzeugnisse erst ermöglicht[50]. Ein weiterer Aspekt findet sich bei LINDE, der in Bezug auf den Wert von Informationsgütern auf die von den Wirtschaftssubjekten vermutete Nützlichkeit der Daten verweist[51]. Indessen sind Märkte für Daten noch immer in der Experimentierphase und die Bewertungsmodelle müssen sich erst noch entwickeln[52].

1.3 Wertschöpfung

a) Informationswert

(1) Verarbeitung

Historisch ist die Stärke einer Wirtschaft eng mit ihrer Fähigkeit physische Güter zu transportieren verbunden. Die Seidenstrasse, die römischen Strassen und die britische Flotte bildeten das ökonomische Rückgrat, das weitrechende Gebiete verband. Diese Perspektive lässt sich auf Daten übertragen. Daten müssen fliessen, um Wert zu generieren[53]. Ein wachsendes Datenangebot erhöht aber nebst der Menge an ungebrauchter und unbrauchbarer Information auch die Gefahr der falschen Selektion[54]. Die vorhandenen Daten müssen dem Verständnis des Empfängers angepasst und entsprechend diesem Ziel verarbeitet werden. Die Erforderlichkeit der Verarbeitung ist mit jedem Datum verbunden und umfasst insbesondere die Verknüpfung mit anderen Daten zur Erschliessung des Verständnisses und des Nutzens[55]. Die Verbindung mehrerer Infor-

---

49 SARVARY, introduction. Siehe auch TENE/POLONETSKY, 63, die Daten als Rohmaterial der Produktion bezeichnen. Demnach wären die unverarbeiteten Daten Bestandteil des Informationsprodukts. JOB, in: Picot, 80, unterscheidet zunächst zwischen Information und Unterhaltung. Ein wesentlicher Unterschied zu anderen Produkten liegt für ihn in der Möglichkeit Informations-Produkte durch Computer personalisieren zu können, was ein wesentlicher Faktor zur Steigerung der Leistungsfähigkeit des Einzelnen sei.

50 CARROLL, 189; GLEICK, 355 ff.; LINDE, 12 f.; AUGUSTIN, 72.

51 LINDE, 7: «Ein Informationsgut ist eine inhaltlich definierbare Menge an Daten, die von Wirtschaftssubjekten als nützlich vermutet wird.».

52 MAYER-SCHÖNBERGER/CUKIER, 121 f.; siehe zur Entwicklungsstufe SIEGERT, in: Picot, 128; grundlegend KUHLEN, 105: «Dem Problem der Instabilität des Informationsmarktes kann man in einem Buch über den Informationsmarkt wohl nur dadurch entgehen, dass auf Strukturen und Metainformationsformen des Informationsmarktes als auf dessen reale Ausprägungen eingegangen wird.». Siehe zur Handelbarkeit personenbezogener Daten The Economist, Shameless self-promotion, September 1, 2012; SIMONITE TOM, If Facebook Can Profit from Your Data, Why Can't You?, MIT Technology Review, July 30, 2013; siehe zum generellen Problem der Bewertung MCKEEN/SMITH, 79.

53 WORLD ECONOMIC FORUM, Data, 7.

54 KIESER, 134.

55 LINDE, 7; DRUEY, Information, 120.

mationen wiederum generiert weitere Informationen; daraus ergeben sich neue Erkenntnisse und Nutzungsmöglichkeiten, jedoch auch neue Risiken[56]. Nebst der Verbindung mit anderen Informationen hängt der Wert der verarbeiteten Information vom Konkretisieren oder Weglassen weiterer Informationen ab[57]. Der Schlüssel zur Macht im digitalen Zeitalter resultiert entsprechend nicht aus den Daten an sich, sondern aus dem Wissen, das aus ihnen gezogen wird[58].

Die Kosten für die Datenverarbeitung haben durch die gesteigerte Rechenleistung über die letzten zehn Jahre um mehr als den Faktor hundert abgenommen[59]. Und auch die Kosten für die Datenspeicherung als Grundlage der Datenverarbeitung sind stark gesunken. Die Ökonomie der Datenerhaltung wurde damit umgekehrt: Früher wurden Daten gelöscht oder zumindest auf einen Sekundärspeicher mit erschwertem Zugang verschoben, sobald sie nicht mehr gebraucht wurden. Mit der Weiterentwicklung von Primärspeichern sind die Auswahl der zu löschenden Daten und die Umsetzung heute oft teurer als der Datenerhalt. Gleichzeitig können die wachsenden Speichermengen immer schneller abgerufen werden[60].

(2) Übertragung und Nutzung

Informationen sind immaterielle Güter, die auch durch die mehrfache Verwendung nicht verbraucht werden. Käufer von Informationen erhalten Kopien, wobei in Bezug auf die Information kein Besitzwechsel erfolgt. Der Wert von Informationen ist abhängig von der zeitlichen Verwendung und vom Kontext[61]. Das Verhältnis zwischen Wert und Kosten unterliegt dem Bewertungsparadoxon: Eine Information kann wirtschaftlich erst bewertet werden, wenn sie bekannt ist. Ist sie bekannt, hat bereits eine Aneignung stattgefunden. Der Wert kann durch Ergänzung, Selektion und Erläuterung gesteigert werden[62]. In Bezug auf mögliche Entscheidungen ergibt sich der Informationswert aus der Reduktion der mit einer Entscheidung verbundenen Ungewissheit[63].

---

56 WORLD ECONOMIC FORUM, Data, 7; WESTIN/BAKER, 7, weisen darauf hin, dass der Computer erstmals Informationen nicht nur nutzt, um Eingaben automatisch zu befolgen, sondern auch die Resultate seiner eigenen Operationen berücksichtigt.

57 PICOT/FRANCK, 545.

58 SOLOVE, Person, 74.

59 WALDO/LIN/MILLETT, 90.

60 WALDO/LIN/MILLETT, 91; so weisen beispielsweise Phasenwechselspeicher eine verhältnismässig kurze Latenzzeit auf.

61 PICOT/FRANCK, 545.

62 PICOT/FRANCK, 545. Die Computerisierung führte zu Beginn nicht zu einer Erhöhung der erfassten und gespeicherten Datenmenge, sondern zu einer Auswahl der objektivsten und der am häufigsten benutzten Daten; siehe dazu WESTIN/BAKER, 121.

63 Im Filmgeschäft beispielsweise durch das Angebot kostenloser Trailer, SHAPIRO/VARIAN, 5.

Information hat dabei nur dann einen Wert, wenn sie potentiell zu einer anderen Entscheidung führt, als zu jener, die der Entscheidungsträger ohne die Information getroffen hätte[64]. Für den Entscheidungsträger ist daher relevant, ob die Information das Potential besitzt seine Entscheidung zu ändern[65]. Die Bestimmung des Informationswerts setzt auch in diesem Zusammenhang die Kenntnis der für die Entscheidung relevanten Einzelheiten voraus[66]. Vertragstheoretisch unterscheiden COOTER/ULEN hierbei zwischen produktiver und umverteilender Information. Produktive Information kann wertvermehrend eingesetzt werden. Dabei handelt es sich insbesondere um methodenbezogene Informationen oder um die Entdeckung wertgenerierender Ressourcen. Umverteilende Informationen generieren dagegen einen Verhandlungsvorteil, der zur Umverteilung von Vermögen zu Gunsten der besser informierten Partei führen kann[67]. Darüber hinaus unterscheiden die Autoren zwischen Information, die durch Investitionen erlangt wurde und solcher, die durch Zufall erlangt wurde. Im Resultat plädieren COOTER/ULEN nur dort für eine Durchsetzung von Verträgen, wo produktive Information durch Investition erlangt worden ist[68]. Diese Perspektive deckt sich mit dem zivilrechtlichen Institut der Verarbeitung in Art. 726 ZGB[69].

(3) Verfügbarkeit

Das Kriterium der Verfügbarkeit von Information ist hinsichtlich des Informationswerts in zweierlei Hinsicht relevant: Einerseits muss die Information dann verfügbar sein, wenn sie verwertet werden kann. Andererseits muss sie in der notwendigen Konzentration vorliegen, d.h. die erforderliche kritische Masse für eine wirtschaftliche Nutzung muss erreicht werden[70]. Das bedingt den Zugang zu den Nutzern. Eine Suchanfrage beispielsweise bringt Werbungen zu verwandten Produkten und Websites, die Werbungen und Links zu weiteren verwandten Angeboten zeigen. Die Konsumenten blenden aufgrund der ausufernden Werbeangebote viele Informationen aus[71]. Für die

64 Subjektiv könnte hier auch der Wert einer eine Entscheidung bekräftigenden Information angeführt werden. Da Entscheidungen formal betrachtet aber nur für oder gegen etwas erfolgen können, generiert die Bekräftigung objektiv keinen Mehrwert.

65 SARVARY, 10.

66 SARVARY, 11.

67 COOTER/ULEN, 357.

68 COOTER/ULEN, 358.

69 Siehe dazu vorne A.I.1.2 b).

70 EVANS/WURSTER, 158.

71 ANDERSON, 387 f.

Werbenden besteht die Herausforderung somit darin, ihre Information wahrnehmbar zu machen und von anderen Mitteilungen abzugrenzen[72].

(4) Zeitabhängigkeit

Tendenziell wird sich der Wert von Informationen über die Zeit eher verringern[73], insbesondere, wenn kein Zugang zu zusätzlichen neuen Informationen gegeben ist[74]. Bei natürlichen Personen spielt die Zeitspanne, die zwischen Aufnahme und Abruf einer Information verstreicht zur Rekonstruktion des Wissens eine zentrale Rolle[75]. Die Zeitabhängigkeit der Speicherkapazität hängt mit der Hirnstruktur und dem Zusammenspiel von Kurz- und Langzeitgedächtnis zusammen[76]. Wichtige resp. wertvolle Informationen bleiben regelmässig besser und dauerhafter im Gedächtnis erhalten als unwichtige[77]. Für Unternehmen verlieren jedoch die meisten Daten über die Zeit an Nutzen und damit an Wert. Unter solchen Umständen können alte Daten nicht nur keine Wertsteigerung leisten, sondern auch den Wert neuer Daten beeinträchtigen. Das ist beispielsweise dann der Fall, wenn Werbung auf veralteten Bestellinformationen basiert und die heutigen Interessen des Nutzers nicht mehr – oder durch einen Teil veralteter Daten nur bedingt – widerspiegelt. Dieser wird entsprechende Anzeigen unter Umständen nachhaltig nicht mehr beachten[78]. Nicht alle Daten verlieren jedoch im gleichen Tempo oder auf die gleiche Weise an Wert und die Entscheidung über den Erhalt kann selten ausschliesslich auf den zeitlichen Faktor gestützt werden. Das erklärt, weshalb einige Unternehmen Daten so lange wie möglich speichern wollen, auch wenn die Gesetzgebung oder die Öffentlichkeit die Löschung bzw. Anonymisierung nach einer bestimmten Zeit fordert[79].

---

72 ANDERSON, 388 ff.

73 KATHS, 228; GLAZER, 101.

74 AMBROSE, 405 f.; siehe auch den Kriminalfall bei LODGE/MAYER, o.S.

75 BRANDES, 12. CROSSON, in: Philosophy and Cybernetics, 198, führt die Unterscheidung zwischen Wissen und Erinnern auf das Bewusstsein über den Zeitablauf zurück. So erinnert man sich beispielsweise nicht seines eigenen Namens, man weiss ihn. Deutlich wird die Grenze auch dadurch, dass das Vergessen solcher Informationen wie dem eigenen Namen eindeutig psychopathologisch ist. Die Erinnerung setzt bei solchen Informationen erst nach dem Vergessen ein. Man erinnert sich, einen Namen haben zu müssen, weiss ihn aber nicht mehr. Der Vorgang ist hier gerade umgekehrt; normalerweise geht man davon aus, etwas vergessen zu haben, nachdem man sich daran hatte erinnern können bzw. hätte erinnern können.

76 MARKOWITSCH, 14; siehe zum Ganzen auch VESTER, 57 ff.

77 CHOU, Rn. 487.

78 MAYER-SCHÖNBERGER/CUKIER, 110.

79 MAYER-SCHÖNBERGER/CUKIER, 111; der Wert hängt entscheidend von der beabsichtigten und im Einzelfall möglichen Nutzung ab.

b) Kontext der Verwertung

(1) Planung, Steuerung und Kontrolle

Information ist zugleich Gegenstand und Mittel der Planung, Steuerung und Kontrolle von Vorgängen. Betriebswirtschaftlich ist die Planung der Ressource Information dann sinnvoll, wenn ein den Planungsaufwand übersteigender Nutzen generiert werden kann[80]. Taiichi Ohno, der Erfinder des Toyota-Produktionssystems stellte Anfang der Neunzigerjahre die kritische Frage, ob es wirtschaftlich sei, Informationen schneller und in grösserem Umfang zu liefern, als diese gebraucht würden. Er verglich die Überversorgung mit dem Kauf einer grossen Hochleistungsmaschine, die zu viel produziere und deren Produkte dann gelagert werden müssten, was die Kosten erhöhe[81]. Kernstück des Toyota-Produktionssystems ist das *kanban*[82], dessen wichtigste Funktion in der Lieferung von Informationen besteht, die auf jeder Ebene die einzelnen Arbeitsschritte koordinieren. Die Planung von informationellen Prozessen ist eng mit damit zusammenhängenden weiteren Abläufen verbunden. Die Produkte werden vom *kanban* grundsätzlich auf dem Produktionsweg begleitet, es stellt das wesentliche Kommunikationsmittel für die Just-in-Time-Fertigung dar[83]. Die Just-in-Time-Fertigung sollte nur das liefern, was tatsächlich gebraucht wird und auch Informationen sollten nur dann anfallen, wenn sie tatsächlich gebraucht werden[84]. Die Verarbeitung von Kundenaufträgen und Informationen über Marktwünsche und Bedürfnisse per Computer wird in diesem Zusammenhang als sinnvoll erachtet, Informationen für Produktionszwecke würden aber nicht bereits zehn oder zwanzig Tage im Voraus benötigt[85].

Ebenfalls Anfang der Neunzigerjahre führte die Matsushita Electric Industrial Co., Ltd. ein neues Kommunikationssystem namens *Market-Oriented Total Management System* ein. Durch die Online-Verbindung von Forschungs- und Entwicklungseinheiten, Fabriken und Einzelhändlern konnten übermässige Lagerbestände und Lieferengpässe ver-

---

80 PICOT/FRANCK, 548.

81 OHNO, 75.

82 Ein *kanban* ist ein Schildchen, das nach der Idee von OHNO zwischen den einzelnen Arbeitsgängen zirkulieren sollte, um die Produktionsmenge (benötigte Menge) zu kontrollieren. Das Schildchen bestand meistens aus einem Stück Papier in einer Plastikhülle. Die darauf enthaltenen Informationen lassen sich in drei Kategorien unterteilen: (1) Entnahmeinformationen, (2) Transportinformationen, (3) Produktionsinformationen. Das *kanban* übermittelt diese Informationen sowohl vertikal als auch horizontal innerhalb des Unternehmens und an dessen Zulieferer; siehe dazu OHNO, 32, 54.

83 OHNO, 70.

84 OHNO, 76; AUGUSTIN, 112 f.; siehe zu den Kosten überflüssiger Informationen ferner DRUCKER, 93.

85 OHNO, 76.

mieden werden[86]. Aus einer Wissensperspektive bestand die grösste Auswirkung des Systems jedoch im freien Informationsfluss und im Teilen von Information unter verschiedenen Funktionsgruppen. Dadurch konnten die Verkaufs- und Fertigungseinheiten ihre Perspektiven hinsichtlich des Produktionsplans austauschen, was zu einer höheren Effizienz führte[87]. Ein ähnliches Konzept verfolgte die Handelskette Walmart. Durch die umfangreiche Sammlung von Informationen, was wo und wann produziert werden kann, was wo und wann transportiert werden kann und wer was wann zu welchem Preis kaufen wird, erlangte Walmart ein globales Bild der relevanten Handelskette. Für weitere Konkurrenten kam die Erkenntnis über den Nutzen einer umfangreichen Datenbearbeitung zu spät; Walmart hatte die Versorgungskette bereits für die eigenen Bedürfnisse optimiert[88].

Die Suche nach zusätzlichen Verbesserungen in Produktionsprozessen hält an[89] und findet heute vor dem Hintergrund einer erhöhten Rechenleistung sowie geringerer Speicherkosten statt. An künftige Versorgungsketten werden vier zentrale Anforderungen gestellt: Die erste Anforderung besteht in der Entwicklung nachfrageorientierter Versorgungsnetze[90]. Diese umfassen Informationen, die den Bedarf genau vorhersagen. Relevant für die Entwicklung solcher Netzwerke ist die Frage, wie die Daten in die Unternehmensprozesse eingebunden werden müssen, damit die Ressourcen vom Produktionsbeginn bis zur Verteilung in der notwendigen Menge und am richtigen Ort zur Verfügung stehen. Ein weiteres Erfordernis besteht in einer erhöhten Transparenz, die nicht nur die Erfassung von Vorgängen in Echtzeit, sondern auch eine offene und effiziente Zusammenarbeit gewährleisten muss. Drittens wird unter dem Begriff der Nachhaltigkeit die Nutzung von Informationen zur Feststellung von Kosten und Effizienz gefordert. Das vierte Erfordernis besteht im Risikomanagement im Zusammenhang mit unvorhersehbaren Ereignissen wie beispielsweise Naturkatastrophen. Dieses beinhaltet die Nutzung von Informationen zum Schutz der Versorgungskette und des Unternehmens[91]. Die Analyse grosser Datenmengen kann dabei ganze Geschäftsmodelle und auch die Interaktion zwischen verschiedenen Unternehmen transformieren. So konnte

86 NONAKA/TAKEUCHI, 120.

87 NONAKA/TAKEUCHI, 120 f.

88 LANIER, 63 f.

89 MALIK/NIEMEYER/RUWADI, 1, verweisen darauf, dass viele internationale Versorgungsketten nicht für die Zukunft gerüstet seien. Den Grund dafür sehen sie in der Ausrichtung dieser Versorgungsketten auf die Produktion grosser Mengen in Tieflohnländern.

90 Die Komplexität nimmt zu, da einzelne Produkte in einer deutlich höheren Anzahl von Varianten auf den Markt gebracht werden, um die Kundenbedürfnisse bestmöglich abdecken zu können; siehe dazu MALIK/NIEMEYER/RUWADI, 3.

91 CORTADA, Corporation, 39 f.

ein grosser europäischer Automobilhersteller durch die Nutzung von Verbrauchsdaten die kommerziellen Beziehungen mit einem Zulieferer neu gestalten, dem die entsprechenden Daten fehlten[92].

(2) Kommerzialisierung

In Abgrenzung zu den für die Planung, Steuerung und Kontrolle von Prozessen relevanten Daten erfasst die Kommerzialisierung Daten direkt beim Konsumenten und reicht entsprechend über eine reine Prozessgestaltung hinaus. Nutzerdaten sind beispielsweise ein wichtiger Bestandteil des Geschäftsmodells von Suchmaschinen und weiteren Anwendungen[93]. Die Kriterien des Arbeits- und Kapitalaufwandes zeigen aber deutlich, dass der Wert dieser Daten nicht bereits durch das Kundtun von Bedürfnissen seitens des Konsumenten entsteht. Bei diesem fallen – abgesehen von der weit vorgelagerten Tatsache des allgemeinen Aufwands zur Lebensführung – hinsichtlich der Generierung von Daten gerade keine Kosten an. Die konkrete Marktnachfrage, die einen ökonomisch nachweisbaren Nutzen generiert, bezieht sich damit erst auf eine kritische Masse an gehäuften und verarbeiteten Daten, die dann in Form relevanter Informationen auch wieder an die Konsumenten zurückfliessen.

Die Nutzung personenbezogener Daten wirkt aus ökonomischer Sicht als Treiber in der Marktordnung. Sie verschaffen dem Träger nach aussen die Möglichkeit, seine Individualität und seine Präferenzen kundzutun, sei dies im zwischenmenschlichen Kontakt oder gegenüber Unternehmen. Das Wissen um die persönlichen Verhältnisse oder Vorzüge einer Person schafft aber noch keinen Mehrwert; es schafft einzig die Möglichkeit eines gezielten Angebots. Die Wahrnehmung dieses Angebots und die Disposition über die zur Anschaffung der Güter und Dienstleistungen notwendigen Vermögenswerte unterliegen letztlich noch immer dem Willen des Individuums[94].

---

92 Siehe das Beispiel bei MAYER-SCHÖNBERGER/CUKIER, 133 f.: Der Autohersteller stellte bei der Auswertung von Sensordaten fest, dass der Sensor eines bestimmten Zulieferers oft falsche Daten lieferte und implementierte ein aufwendiges Analyseprogramm. Dieses resultierte in einer verbesserten Technologie, für die der Autohersteller ein Patent erhielt, das dann an den Zulieferer verkauft werden konnte.

93 Siehe WEBER, Moral, 317.

94 So auch BULL, 13 f., mit der Feststellung, dass sich einige offenbar «moralisch» verpflichtet fühlten und sich einem «psychologischen Kaufzwang» unterworfen sähen. Siehe zum Zusammenhang zwischen der Verbreitung von Informationen und dem menschlichen Bewusstsein SILVER, 218.

2. Informationsmanagement

2.1 Zeitliche Dimension

Zeit ist keine objektive Grösse, «Zeit ist ein historisch relativ junges, sozial erzeugtes Orientierungsmittel», das vom Menschen aufgrund seiner Abstraktion und Verdinglichung hauptsächlich als ein regulierendes und strukturierendes Element wahrgenommen wird und Veränderung dokumentiert[95]. Die zeitliche Dimension des Informationsmanagements erfasst die Ursachen und Wirkungen des Erhalts von Information über die Zeit. Die Informationsprozesse sind dabei Teil einer die Gegenwart prägenden Veränderung, die als digitale Revolution bezeichnet werden kann[96]. Die gegenwärtigen und zukünftigen Auswirkungen dieser Veränderungen sind unklar und werden sehr unterschiedlich eingeschätzt. Die groben Prognosen reichen vom Ende des Vergessens durch eine umfassende Datenspeicherung[97] bis hin zur Befürchtung, dass wichtige Informationen aufgrund der mangelnden Haltbarkeit digitaler Daten in verhältnismässig kurzer Zeit verloren gehen[98]. Der Erhalt von Daten ist hierbei für das Unternehmen nicht nur funktional relevant, sondern trägt auch zur Begründung einer Unternehmensidentität bei[99]. Die Identität von Organisationen wird durch das organisatorische Gedächtnis definiert. Bedeutend beeinflusst wird diese Identitätsbildung einerseits durch die (heute computergestützte) Vernetzung und durch den Erhalt prägender Geschichten in einem Unternehmen[100].

2.2 Informationsprozesse

Neue Erkenntnisse können beim Menschen unmittelbar den verfügbaren Informationen zugeordnet werden. Sinneseindrücke werden augenblicklich verarbeitet und in verfügbares Wissen umgewandelt[101]. Bei Unternehmen ist die Verarbeitung oft schwerfälliger. Die Sinneswahrnehmungen der einzelnen Wissensvermittler müssen erst in das Unternehmenssystem eingespeist werden[102], beispielsweise durch die manuelle Daten-

---

95 WELZER, 114.

96 Siehe zur digitalen Revolution SCHENK, 194; zum Ende der Epoche des Papiers MÜLLER LOTHAR, Weisse Magie. Die Epoche des Papiers, München 2012.

97 So insbesondere MAYER-SCHÖNBERGER, 52, der zumindest davon ausgeht, dass das Vergessen seine Normalität verloren hat.

98 SCHENK, 194, 202 f.

99 LEHNER, 36; STREMMEL, 155.

100 LEHNER, 37. Siehe zum Gedächtnis als Funktion von Systemen am Beispiel des Rechtssystems, DE GIORGI, 107 f.

101 CHOU, Rn. 506.

102 Siehe dazu PETERHANS, 223.

erfassung. Erst dann stehen sie den Entscheidungsträgern zur Verfügung[103]. Die zunehmende Automatisierung dieser Prozesse durch elektronische Vorgänge verkürzt hingegen auch in Unternehmen die zur Nutzbarmachung der Daten benötigte Zeit. In diesem Zusammenhang spielen Datenbanken eine zentrale Rolle. Die Bezeichnung Datenbank soll sprachlich auf eine Geldbank hinweisen, auf der anstelle von Geld Daten angelegt und beliebig wieder abgerufen werden können[104]. Eine Datenbank ist jedoch kein blosses Depot, sie grenzt sich von diesem dadurch insofern ab, als dass sie eine beliebige Kombinier- und Auswertbarkeit grosser Datenmengen ermöglicht[105]. Datenbanken im Sinne von computergestützten Einrichtungen zum organisierten Speichern und Abrufen grosser Datenmengen durch mehrere Benutzer gibt es seit ca. 1970[106]. In den letzten Jahren wurde das Paradigma einer selektiven Speicherung und Analyse von Daten jedoch zunehmend durch neue Entwicklungen überholt. Unternehmen begannen zunächst damit, nicht mehr nur Geschäftsprozesse, sondern die gesamte Interaktion mit den Kunden vom Marketing bis zum Verkauf elektronisch abzuwickeln. Diese Interaktion hat zu einer neuen Quantität und Qualität unternehmensrelevanter Daten geführt[107]. Die sinkenden Kosten für Speicherplatz ermöglichen die Verbreitung zeitintensiver und inhaltsreicher Ressourcen in neuen Ausmassen[108]. Diese Entwicklungen verstärken die Notwendigkeit einer gezielten Gestaltung von Informationsprozessen.

2.3 Informationsmanagement als Prozessgestaltung

a) Historische Perspektive

Grundlegend weist das Informationsmanagement eine historische Perspektive auf. In ihrer gegenwärtigen Form sind Unternehmen das Resultat eines historischen Prozesses. Die Kenntnis über den Verlauf und das Ergebnis dieser Entwicklung ist eine notwendige Voraussetzung für das Handeln in der Gegenwart[109]. Archive erfüllen hierbei eine Gedächtnisfunktion und «Archivierung ist Informationsmanagement»[110]. Die gezielte Aufbewahrung von Information bildet die Grundlage für die Geschichte eines Unter-

103 CHOU, Rn. 507.
104 SEIDEL, Datenbanken, 2; STEINBUCH, 207.
105 SEIDEL, Datenbanken, 3.
106 ZEHNDER, 147.
107 POLZER, 6.
108 SIFRY, 49 f.
109 Siehe DANIEL VASELLA, Von Basel in die Welt: Die Entwicklung von Geigy, Ciba und Sandoz zu Novartis, Zürich 2012, Vorwort, 7. Siehe zur Relevanz der Zeitstrukturen in Unternehmen in Bezug auf Entscheide MOSSER, 15 f.
110 MOSER/NEBIKER/OTHENIN-GIRAD, 67.

nehmens[111]. Die Unternehmensgeschichte beleuchtet ein Unternehmen aus historischer Sicht und verfolgt dabei hauptsächlich drei Ziele[112]: Ein erstes Ziel besteht in der Rechtfertigung früheren Handelns; anhand des historischen Materials wird aufgezeigt, weshalb nur so und nicht anders gehandelt werden konnte. Ein zweites Ziel besteht in der Lösung gegenwärtiger Probleme durch die Entwicklung eines Verständnisses für ihre Entstehung und ihren Verlauf. Ein drittes Ziel besteht in der historischen Erkenntnis an sich[113]. Vor diesem Hintergrund kann hinsichtlich der Entstehung zwischen zwei Arten von Unternehmensgeschichte unterschieden werden, die unterschiedlich motiviert sind: Die Erfassung der Unternehmensgeschichte kann durch das Unternehmen selbst oder durch Dritte (z.B. für wissenschaftliche oder ideologische Zwecke) initiiert sein[114]. Die Rechtfertigung früheren Handelns und die Lösung gegenwärtiger Probleme sind dabei intrinsische Motive zur Pflege der Unternehmensgeschichte, die historische Erkenntnis an sich liegt eher im Interesse Aussenstehender und ist Teil eines allgemeinen Interesses im Rahmen eines Geschichtsverständnisses im grösseren Kontext.

Geschichte ist vergänglich, sie lebt nur in Form von Erfahrungen und Erinnerungen in den Menschen weiter und muss daher in irgendeiner Form festgehalten werden[115]. Die Entwicklung und die Geschichte eines Unternehmens sind Teil der Gesellschaft und Teil der Verantwortung gegenüber dieser Gesellschaft[116]. Unternehmen agieren stets in einem geschichts- und kulturgeprägten Kontext und funktionieren nicht universal[117]. Darin besteht eine entscheidende Aufgabe von Unternehmensarchiven[118]. Dem Begriff des Archivs kommt dabei eine allgemeine und eine rechtlich definierte Bedeutung

---

111 Zur Entstehung und Vorgehensweise der Disziplin siehe PIERENKEMPER, 10 ff.

112 ZÜND, 666 f.; zur Entwicklung ders., 667 ff.

113 Kritisch gegenüber der Geschichte als «Lehrmeisterin des Lebens», ZÜND, 667, da sich die Geschichte nicht wiederhole; mit Verweis auf die Notwendigkeit eines kritischen Verständnisses der Vergangenheit PINKAS, 125.

114 BRUSATTI, 114; ZÜND, 666, unterscheidet zwischen auftragsgebundener Firmenfestschriftliteratur und wissenschaftlicher Firmengeschichtsschreibung.

115 WILLI, 32. Die Speicherung von Fakten und die menschliche Erinnerung sind indessen nicht gleichzusetzen; treffend hierzu VOGT, 122: «Vermutlich trügt meine Erinnerung. Die Ärztin hebt die Schultern. Meine Erinnerung sagt sie, sei nicht falsch. Höchstens anders als die damalige Realität! Ich muss sagen, die Psychiater haben für alles ein Argument.»; vgl. auch RECK, 78, wonach Gedächtnis nicht im Dienst der Erinnerung steht und die umfassende Konstitution dessen ist, woran sich der Mensch niemals erinnern kann. Siehe zur psychologischen Theorie und Beispielen zur individuellen Erinnerung WELZER, 185 ff.; HUBER, Erinnern, 101 ff.; siehe zur individuellen Erinnerung im Kontext normativ sozialer Rahmenbedingungen ASSMANN, Vergangenheit, 153 ff.

116 WILLI, 37.

117 JUNGKIND, 303.

118 WILLI, 32.

zu[119]. Allgemein werden sämtliche Stellen und Einheiten, die der systematischen Erfassung, Verwaltung und Bereitstellung von Schrift-, Bild-, und Tonträgern dienen und eine dokumentarische Funktion erfüllen, als Archiv bezeichnet[120]. Die rechtliche Definition ist enger und bezieht sich auf die Archivierung von Akten (z.B. Protokolle und Urteile)[121].

Die Relevanz von Unternehmensarchiven rückte im Jahr 1996 mit der Einsetzung einer Kommission zur historischen und rechtlichen Untersuchung des Schicksals der infolge nationalsozialistischer Herrschaft in die Schweiz gelangten Vermögenswerte durch die Eidgenössischen Räte[122] verstärkt ins Bewusstsein der Öffentlichkeit[123]. Diese wirtschaftshistorische Offensive des Bundesrates war primär politisch motiviert[124]. Die Schweiz wurde damals mit Sammelklagen amerikanisch-jüdischer Organisationen konfrontiert[125]. Als Reaktion darauf wurde zur aussenpolitischen Entlastung und zur innenpolitischen Klärung die Unabhängige Expertenkommission Schweiz – Zweiter Weltkrieg (UEK) eingesetzt[126]. Die Aufgabe der UEK bestand darin, das Verhalten von rund vierzig Schweizer Banken, Versicherungen und Industrieunternehmen im Zweiten Weltkrieg zu untersuchen. Forschungsschwerpunkte waren die Vermögensverschiebungen in und über die Schweiz, Bankgeschäfte mit dem Dritten Reich, nachrichtenlose Vermögen sowie die Beziehung zwischen schweizerischen Muttergesellschaften und ausländischen Tochtergesellschaften[127]. Von Bedeutung im vorliegenden Zusammenhang ist der unterschiedliche Umgang mit diesen Vermögenswerten über die Zeit[128]. Wo unter Anwendung anderer Gesetzgebungen (z.B. in den USA) solche ruhenden Vermögenswerte nach einer bestimmten Zeit an den Staat fallen[129], wurden sie in der Schweiz und beispielsweise in Israel unbedacht und ohne Suche nach den Anspruchsberechtigten weitergeführt[130]. Im Rahmen der juristischen Auseinandersetzung um die-

119 SCHWEIZER/BAUMANN, 238.
120 FRANZ, 2.
121 SCHWEIZER/BAUMANN, 238.
122 AS 1996 3487.
123 ROTH-LOCHNER/HUBER, in: Coutaz et al., 39; RUDIN, 247.
124 ZÜND, 668.
125 Siehe dazu MAISSEN, 244 ff.
126 ZÜND, 668, die UEK wird nach ihrem Vorsitzenden Jean-François Bergier im Volksmund «Bergier-Kommission» genannt.
127 ZÜND, 668; siehe zur Rolle des Finanzplatzes auch BOSCHETTI, 89 ff.
128 Die ausserbilanziellen Bestände der Banken beliefen sich auf über 20 Milliarden Schweizer Franken, BOSCHETTI, 91.
129 Die Vermögenswerte können vom Staat zurückgefordert werden, siehe dazu: http://usgovinfo.about.com/od/moneymatters/a/unclaimedstates.htm, abgerufen am 27.01.2014.
130 KREIS, 92.

se Vermögenswerte zogen auch die Banken selbst Historiker bei, um sich über die Inhalte ihrer Archivbestände in Kenntnis zu setzen[131].

Das unternehmenshistorische Potential in der Schweiz ist gross, es gibt viele alte Unternehmen, die keiner Kriegszerstörung und keinen Naturkatastrophen zum Opfer fielen. Zudem haben Übernahmen und Fusionen kleiner und mittlerer Unternehmen auch zu Zusammenschlüssen von Unternehmensarchiven geführt[132]. Trotz der hohen Unternehmensdichte sind Unternehmensarchive in der Schweiz jedoch unterentwickelt[133]. Die Quellen zur Unternehmensgeschichte sind gefährdet, da viele nicht erschlossen sind und häufig nicht erhalten bleiben[134]. Eine Ursache liegt – trotz einiger Zusammenschlüsse – im nach wie vor hohen Anteil an kleinen und mittleren Unternehmen[135]. Eine weitere Ursache liegt im fehlenden Bewusstsein um den kulturellen Wert der Unternehmensarchive[136].

b) Technologische Perspektive

Die wesentlichste Rolle der Technologie besteht darin, die Grundlagen für den Informationsfluss zu schaffen. Ohne diesen Informationsfluss bleibt die Information verschlossen, unerreichbar und entsprechend wertlos[137]. Das Informationsmanagement ist von der Informationstechnologie insofern abzugrenzen, als letztere die Technik, die Organisation und die Methoden zur Verarbeitung umfasst, durch die Daten zu Informationen verdichtet werden[138]. Das Informationsmanagement bezieht sich hingegen auf die Gestaltung des Umgangs mit diesen Informationen[139].

c) Betriebswirtschaftliche Perspektive

In der Betriebswirtschaftslehre wird die Information hauptsächlich im Hinblick auf ihren Nutzen für das Unternehmen untersucht[140]. Dabei werden Informationen grundsätzlich in zwei Kategorien unterteilt: Einerseits sind Informationen eine Ressource für das

131 MAISSEN, 253.
132 ZÜND, 669.
133 Das Gleiche gilt für die Unternehmensgeschichte als Disziplin, ZÜND, 668.
134 ZÜND, 669.
135 ROTH-LOCHNER/HUBER, in: Coutaz et al., 38.
136 ZÜND, 669, der im privaten Sektor insbesondere eine «geschichtslose» Managementausbildung als ursächlich erachtet.
137 DUMAS, 2, sieht sogar die Existenz der Information erst durch ihre Wahrnehmung begründet; siehe auch WORLD ECONOMIC FORUM, Data, 5: «*Just as tradable assets like water and oil must flow to create value, so too must data.*».
138 BEGLINGER et al., 34; siehe zur Abgrenzung vorne A.I.1.1.
139 BEGLINGER et al., 34.
140 AUGUSTIN, 62.

Unternehmen; dazu gehören das einsetzbare Wissen (Know-how) und die Immaterialgüter des Unternehmens. Andererseits sind Informationen ein Führungsinstrument[141]. Die personenbezogene Information kann nach hier vertretener Auffassung in Abhängigkeit zum Verwendungszweck sowohl der ersten als auch der zweiten Kategorie zugeordnet werden[142]. Die prozessorientierte Information, die insbesondere zur Gestaltung von Produktionsprozessen dient, ist hierbei ein Führungsinstrument[143]. Die für die Unternehmensidentität (Corporate Identity) relevanten Informationen sind ebenfalls dieser Kategorie zuzuordnen[144]. In der betriebswirtschaftlich strategischen Ausrichtung umfasst die Corporate Identity die Planung und operative Umsetzung von Massnahmen der erfolgsorientierten Unternehmensstrategie und sämtlicher kommunikativer Bereiche[145].

Der Trend im Laufe der letzten hundert Jahre zeigt eine steigende Abhängigkeit des Managements von verschiedenen Daten- und Informationsformen[146]. Vor dem Hintergrund sich verändernder Marktverhältnisse, insbesondere der Sättigung der Märkte, einer erhöhten Austauschbarkeit der Produkte und eines wachsenden Wettbewerbs, wird die Kundenorientierung und damit das Wissen um die inhaltlichen, örtlichen sowie zeitlichen Präferenzen der Konsumenten zunehmend bedeutender[147]. Gleichzeitig erfordert der wachsende Wert von Informationen umgekehrt auch die Bewirtschaftung dieser Ressource[148]. Die gezielte Aufbewahrung soll relevante Daten für die künftige Nutzung erhalten. Die Auswahl, Erstellung, Verwaltung und Erhaltung von Inhalten fällt wesentlich einfacher, wenn Klarheit über die Zielsetzung dieser Vorgänge besteht[149]. Bei der Umsetzung ist vorweg zu entscheiden, welche Informationen aufbewahrt werden sollen. Anschliessend müssen ein entsprechendes Informationssystem aufgebaut und die Speichermedien bestimmt werden. Daraus ergeben sich vielfältige

---

141 PEYROT, 3; siehe auch WEBER, Aufbewahrung, 72.

142 Siehe zur Verwertung vorne A.I.1.3 b).

143 Siehe zur prozessorientierten Information vorne A.I.1.3 b)(1).

144 Der Begriff *Corporate Culture* wird häufig synonym verwendet; siehe dazu MATIS, 75.

145 BUNGARTEN, 235.

146 CORTADA, Corporation, 127 f.

147 MELCHIOR, 133; DRUCKER, 111.

148 CAVOUKIAN, 193; CORTADA, Corporation, 76, geht davon aus, dass Unternehmen in den kommenden Jahren mehr Zeit darauf verwenden werden zu lernen, wie Informationen gesammelt, gehandhabt und genutzt werden können.

149 DAIGLE, 103. Siehe in Bezug auf die Archivierung KELLERHALS, in: Coutaz et al., 329.

Anforderungen und Probleme[150]. In grösseren Unternehmen muss zudem die Koordination mit anderen Einheiten sichergestellt werden[151]. In zeitlicher Hinsicht ist heute insbesondere nicht klar, ob der Datenerhalt durch digitale Speichermedien langfristig überhaupt gewährleistet werden kann[152]. Ursächlich für den Datenverlust sind beispielsweise die Alterung und der Verschleiss der Datenträger sowie die Bindung an spezifische Lesegeräte[153]. Im Aussenverhältnis sind die Vertraulichkeit der Informationen, intakte Überlieferungsmöglichkeiten und der Schutz Dritter relevant[154].

Die weitere Entwicklung deutet auf eine zunehmende Vernetzung grosser Informationsmengen hin. Verschiedene Arten von Informationen aus neuen Quellen werden sich in deutlich kürzeren Zeitabständen als heute gegenseitig beeinflussen[155]. Das Wissen um die informationellen Vorgänge in den Abteilungen des eigenen Unternehmens und in anderen Unternehmen wird für das Management an Bedeutung gewinnen. Die Bewirtschaftung von Datenbeständen in Form des Wissens- und Informationsmanagements wird dadurch vermehrt Bestandteil organisatorischer und normativer Kontrollmechanismen[156]. Verbunden mit dem Problem, wie die wachsenden Datenmengen kontrolliert werden können, ist die Frage, was die «richtige» Information zur Führung eines Unternehmens ausmacht[157].

d) Kommunikative Perspektive

Die Unternehmenskommunikation besteht aus einer Vielzahl direkter und indirekter Informationsübermittlungen[158], die insbesondere das Marken- und Reputationsmanage-

150 Siehe eine Übersicht bei WEBER, Aufbewahrung, 72 f., der u.a. darauf hinweist, dass die zu hinterlegenden Daten unabhängig vom Informationsträger sein müssen. Nach hier vertretener Auffassung sind aber gerade elektronische Daten grundsätzlich an einen Informationsträger gebunden. Vielmehr ist durch die – ebenfalls erwähnte – Datenmigration sicherzustellen, dass die Daten bei Bedarf auf jeweils neue Datenträger übertragen werden. Siehe ferner zu den allgemeinen Grundsätzen der elektronischen Aufbewahrung WILDHABER, 421, 433, 435 f.; LUBICH, 444.

151 DAIGLE, 103.

152 Beispielsweise kann die NASA die Daten der ersten Mondmissionen nicht mehr rekonstruieren, da die Datenträger nicht mehr lesbar sind, The Economist, Digital data: Big rot, April 28, 2012; siehe auch den Hinweis bei KEITEL/SCHOGER, 8. Siehe ferner die Beispiele bei BORGHOFF et al.: Die Satellitenbilder aus den Siebzigerjahren, die Aufschluss über die Entwicklung des brasilianischen Regenwaldes geben könnten, sind in elektronischer Form verloren gegangen. Die Daten der amerikanischen Volkszählung aus den Sechzigerjahren konnten mit viel Aufwand nach drei Jahren rekonstruiert werden, zehntausend Datensätze blieben jedoch verloren.

153 DÄSSLER, 75, 82.

154 WEBER, Aufbewahrung, 73.

155 CORTADA, Corporation, 128.

156 CORTADA, Corporation, 145 f.

157 CORTADA, Corporation, 44.

158 HALLIER WILLI, 39, unterteilt in kontrollierte, unkontrollierte und indirekte Kommunikation.

ment umfassen. Die Reputation geht dabei über die Kommunikation hinaus und zielt auf ein langfristig berechenbares Verhalten des Unternehmens, das Vertrauen schafft. Die Marke dient dagegen zur Vermittlung eines differenzierten Profils, das den Anspruchsgruppen ein über das Vertrauen und den guten Ruf hinausgehendes Bild vermittelt[159]. Die Unternehmensgeschichte ist ein zentraler Teil der Unternehmensidentität. Diese wird analog zur individuellen Persönlichkeit durch den Zusammenhang von Erscheinung, Worten und Taten greifbar[160]. Taten vermögen hierbei mehr als Worte[161]. Managementseitig liegt dem Entwicklungsprozess der Unternehmensidentität die systematische und langfristige Analyse, Gestaltung, Vermittlung und Überprüfung des Selbstverständnisses eines Unternehmens zugrunde[162]. Insbesondere bei Fusionen kommt der Unternehmensgeschichte eine wichtige Orientierungsfunktion zu[163]. Darüber hinaus wird die Unternehmensidentität in Anbetracht zunehmend gesättigter Märkte künftig deutlich stärker dazu beitragen müssen, eine Marke systematisch und langfristig zu führen[164].

Die Reputation im Internet ist aus mehreren Gründen ein eigenständiges Gebiet. Das Wachstum des Internets ist vom Wachstum formaler und systematisierter Bewertungssysteme begleitet, die sowohl online als auch offline Marktteilnehmer erfassen. Reputation wird dadurch mess- und analysierbar, die digitalen Bewertungssysteme bieten einen umfangreichen Informationspool[165]. Obwohl insbesondere in Bezug auf die Ausgestaltung von Bewertungsmechanismen noch viele ungelöste Probleme bestehen[166], ermöglicht das Internet eine rasche und umfangreiche Verbreitung kritischer Informationen. Diese Möglichkeit wird insbesondere auch für die weltweite Erfassung von Verstössen gegen die Datensicherheit genutzt und führt zu umgehenden Reaktionen[167].

---

159 GEISSBÜHLER, 2.

160 MATIS, 77 f.; siehe auch die umfassende Darstellung bei HALLIER WILLI, 39; kritisch ZÜND, 666, der auf die Gefahr einseitiger Darstellungen verweist, sofern die Unternehmensgeschichte ausschliesslich zu Zwecken der Public-Relations gebraucht werde.

161 MATIS, 78, 83.

162 STIER/HERBST, 9; kritisch zur Reduktion der Geschichte auf eine «erfolgsrelevante Ressource» STREMMEL, Fn. 36, m.w.H.

163 ZÜND, 667.

164 STIER/HERBST, 1.

165 CABRAL, 343.

166 CABRAL, 352.

167 Siehe beispielsweise www.privacyrights.org; www.attrition.org. Insbesondere multinationale Grossunternehmen stehen unter ständiger Beobachtung; siehe dazu MCBARNET, 15.

e) Rechtliche Perspektive

Betriebsinterne Daten und Informationen mit Geschäftsrelevanz werden als *Records* bezeichnet[168]. Der Begriff «*Records Management*» umschreibt im Allgemeinen eine Teildisziplin des Managements, die sich ursprünglich auf physische Dokumente bezog (z.B. Briefe, Verträge, Sitzungsprotokolle etc.)[169] und beinhaltet im Besonderen das Planen, Steuern und Kontrollieren der zur ordnungsgemässen Aufbewahrung von geschäftsrelevanten Daten erforderlichen Vorgänge[170]. Die Ordnungsmässigkeit und die Geschäftsrelevanz sind die für die Zuordnung zur rechtlichen Perspektive massgeblichen Kriterien. In den Siebzigerjahren kam der Begriff «Informationsmanagement» für die Beschreibung einer computerisierten Umwelt, in der strukturierte Informationen elektronisch gespeichert werden, auf. Da *Records* sowohl elektronisch als auch in Papierform existieren, wird heute auch von «*Records*- und Informationsmanagement» gesprochen[171].

Das *Records Management* beinhaltet das Erfassen, Erschliessen bzw. Indexieren, die Nutzung sowie die Verwaltung, Sicherung und Bewirtschaftung der *Records*[172]. *Records* dürfen einerseits nicht kürzer und müssen andererseits aber auch nicht länger als notwendig aufbewahrt werden[173]. Dadurch soll die Nachvollziehbarkeit von Vorgängen in der Vergangenheit sichergestellt werden. Normativ sind insbesondere die gesetzlichen und vertraglichen Aufbewahrungsfristen relevant. Eine Aufbewahrung über die gesetzlichen Fristen hinaus kann durch die gesellschaftsrechtliche oder geschäftspolitische Relevanz der Unterlagen begründet sein. Dabei handelt es sich beispielsweise um Gesellschaftsakten (Urkunden, Protokolle), interne Weisungen und Reglemente, Organigramme, Immaterialgüterrechte und Publikationen. Die Aufbewahrung dieser Dokumente ist durch interne Weisungen zu regeln[174].

Im Unterschied zum *Records Management* wird der Begriff der Archivierung meistens in einem historisch wissenschaftlichen Kontext verwendet[175]. In Abgrenzung zu diesem historisch wissenschaftlichen Kontext steht der Begriff der Archivierung im Han-

168 BEGLINGER et al., 36 f.; TOEBAK, in: Coutaz et al., 253.

169 FRANKS, 32.

170 BEGLINGER et al., 37.

171 FRANKS, 32.

172 Ein zentrales Resultat bzw. Ziel dieser Vorgänge besteht in der zeitnahen Auffindbarkeit relevanter *Records*; vgl. BEGLINGER et al., 37, wo dieser Faktor als zentrales Element des *Records Management* erwähnt wird; TOEBAK, in: Coutaz et al., 253.

173 TOEBAK, in: Coutaz et al., 257.

174 WILLI, 32 f. Siehe zur strategischen Entscheidfindung im Aufbewahrungsprozess WITSCHI, 80 ff.

175 Eine klare Unterscheidung ist indessen nicht möglich, WILLIAMS, 9; vgl. zum Begriff auch bereits vorne A.I.2.3 a).

delsrecht für die Trennung von Dokumenten des Tagesgeschäfts gegenüber solchen, die aufgrund der handelsrechtlichen Aufbewahrungspflicht weiter aufbewahrt werden[176]. Das *Records Management* beschränkt sich auf die Verwaltung und Bewirtschaftung von Datenbeständen in der dynamischen Phase, die einen Zeitraum von 0-5 Jahren umfasst. Die Archivierung umfasst dagegen eine statische Phase von mindestens 20 Jahren[177]; grundsätzlich sollen Archive die Daten jedoch zeitlich unbegrenzt sichern[178]. Im deutschen Sprachgebrauch hat sich hierfür der Begriff «Langzeitarchivierung» etabliert, wobei Archivare darauf hinweisen, dass schon immer unbegrenzt archiviert worden sei und der Begriff somit dem sprichwörtlichen weissen Schimmel entspreche[179]. Für die so verstandene Archivierung besteht rechtlich grundsätzlich keine Pflicht und öffentliche Institutionen können nur dort tätig werden, wo sie dazu rechtlich legitimiert sind. Indessen sieht das Recht die passive Übernahme historisch bedeutender Privatarchive vor[180]. Der Erhalt und die Nutzung personenbezogener Daten erfordert unter Berücksichtigung des Datenschutzrechts grundsätzlich auch in diesem Kontext die Möglichkeit den Zugang und den Verwertungsumfang zu beschränken[181]. Die Nutzung von archivierten Bildern oder das Abrufen von Bildmaterial aus einer Datenbank kann beispielsweise im Hinblick auf das Recht am eigenen Bild beschränkt sein. Eine einmal erteilte Einwilligung, die grundsätzlich als Rechtfertigungsgrund dient, umfasst nicht automatisch auch irgendwelche künftigen Nutzungen. Dies gilt insbesondere, wenn das Bildmaterial in einem völlig anderen Kontext verwertet wird[182].

f) Schlussfolgerungen

Das Informationsmanagement umfasst die Bearbeitung von Informationen in einem Unternehmen, unabhängig davon wie und zu welchen Zwecken diese Informationen eingesetzt werden. Das übergeordnete Ziel des Informationsmanagements besteht in der Gestaltung und Nutzung von Information als Ressource für das unternehmerische

---

176 Vgl. BEGLINGER et al., 210.

177 TOEBAK, in: Coutaz et al., 257 f.

178 DÄSSLER, 73; SCHWEIZER/BAUMANN, 238; siehe zu den verschiedenen Auffassungen über die Dauer der Aufbewahrung FRANKS, 272.

179 FERLE, 4. Der Begriff «Langzeitarchivierung» wird daher in der Branche mehr als Kommunikationsbegriff nach aussen genutzt, während intern differenzierte Bezeichnungen gewählt werden wie beispielsweise «Digitale Bestandeserhaltung».

180 Siehe auf Bundesebene Art. 17 Abs. 2 Bundesgesetz über die Archivierung (BGA); siehe auf kantonaler Ebene beispielsweise Art. 3 der Verordnung über das Archivwesen des Kantons Appenzell Ausserhoden. Kantonale Denkmalpflegegesetze können hingegen unter Umständen ein Bauwerk auch gegen den Willen von Eigentümern unter Schutz stellen.

181 SIMITIS, Gedächtnisverlust, 1493 ff.

182 BÄHLER, 61 f.

Denken und Handeln[183]. Da Unternehmen und Individuen Entscheidungen auf der Grundlage unvollständiger Informationen treffen müssen, hat sich insbesondere auch die Unternehmensidentität als Hoffnungsträger für den unternehmerischen Erfolg entwickelt[184]. Vor diesem Hintergrund kann grundsätzlich jegliche Nutzung von Informationsressourcen als Teil einer auf den Unternehmenserfolg ausgerichteten Handlungsweise betrachtet werden. In Abgrenzung zu dieser allgemeinen Nutzenorientierung weist das Informationsmanagement eine rechtliche Perspektive auf, der insbesondere die nachstehend zu betrachtende Risikoorientierung zugrunde liegt.

3. Risiko als Grundlage des Informationsmanagements

3.1 Risiko und Zeit

Risiko und Zeit sind die entgegengesetzten Seiten der gleichen Münze, da es ohne Zukunft auch kein Risiko gibt. Die Zeit transformiert das Risiko und die Art des Risikos wird durch den Zeithorizont beeinflusst[185]. Auch das Informationsmanagement ist von der Zeit geprägt. Zeit ist dann am wichtigsten, wenn Entscheidungen irreversible Folgen nach sich ziehen. Und doch müssen viele Entscheide auf der Basis unvollständiger Information getroffen werden[186], da sie eben zukünftige und damit grundsätzlich ungewisse Umstände mitumfassen.

Als Risiko wird der mögliche negative Ausgang eines Vorhabens mit dem Nachteile, Verluste oder Schäden verbunden sind bezeichnet[187]. Wer Risiken eingeht, wettet auf einen Ausgang, der aus den entsprechenden Handlungen resultiert, obwohl keine Gewissheit über diesen Ausgang besteht[188]. Die Speicherung, Verwertung und Löschung von Daten spielt in diesem Zusammenhang eine entscheidende Rolle. Die Essenz des Risikomanagements besteht in der Maximierung der Bereiche, in denen eine gewisse Kontrolle über den Ausgang ausgeübt werden kann und in der Minimierung jener Bereiche, die sich einer Kontrolle entziehen und in denen die Verbindungen zwischen Ursache und Wirkung verborgen bleiben[189]. Das Herstellen einer Verbindung zwischen

183 Vgl. BEGLINGER et al., 34; MCKEEN/SMITH, 73.

184 Kritisch dazu BUNGARTEN, 236 f., der darin die Entwicklung einer «esoterischen Heilslehre» erkennt und für einen analytischen Ansatz plädiert, der sich von marktstrategischen Interessen des Unternehmens distanziert.

185 BERNSTEIN, 15.

186 BERNSTEIN, 15.

187 DUDEN, 2792.

188 BERNSTEIN, 197.

189 BERNSTEIN, 197.

Ursache und Wirkung erfordert die nötigen Informationen[190]. Die Schaffung von Informationsgrundlagen zur Kontrolle von Bereichen und zur Minimierung des Risikos ist daher ein Grundmotiv der Informationsverarbeitung[191]. Gleichzeitig ist jedoch auch die dazu erforderliche Datenbearbeitung als Vorhaben zu bezeichnen das – entsprechend dem Risikobegriff – an sich zu einem negativen Ausgang führen kann. Nachstehend werden diese durch die Datenbearbeitung hervorgerufenen Risiken in Bezug auf den Informationszugang, die Informationsverwertung und die Informationslöschung hinsichtlich ihrer rechtlichen Auswirkungen überblickartig dargestellt. Nicht Gegenstand der Untersuchung ist der Umgang mit unmittelbar technisch bedingten Risiken[192].

3.2 Information als Risikogegenstand

a) Informationszugang

(1) Kontrollverlust

In Unternehmen wird Information häufig nicht als Wert wahrgenommen, der umfassend verwaltet werden sollte[193]. Entsprechend sind Unternehmensinformationen auf unterschiedlichsten Datenträgern über das ganze Unternehmen und auf einzelne Mitarbeiter verteilt[194]. Zudem werden grosse Datenmengen ohne Verschlüsselung oder andere Sicherheitsvorkehren übertragen[195]. Diese Vorgänge begünstigen den Verlust über die Kontrolle der Daten. Bedeutende Risiken dieses Kontrollverlusts sind Reputationsschäden und Kostenfolgen durch Rechtsverstösse[196].

Die Übertragung der Verfügungsmacht auf Dritte ist insbesondere bei der Nutzung von Cloud-Diensten relevant. Unternehmen können dadurch Investitionen in Informationsverarbeitungssysteme einsparen und die Nutzung flexibel anpassen. Die Cloud-Anbieter sind jedoch grundsätzlich den gleichen Risiken ausgesetzt wie die datenüber-

---

190 Ein Beispiel hierfür ist das Rechnungswesen, dessen Aufgabe in der Erfassung und Abbildung der finanziellen Konsequenzen der abgeschlossenen Verträge besteht; siehe dazu MEYER, Rechnungswesen, Rn. 24 ff.

191 FRANKS, 29 f.

192 Siehe dazu u.a. BRUNNSTEIN, in: Picot, 265 ff.

193 MCKEEN/SMITH, 79.

194 PURI et al., 390. Die Verteilung der Information wird insbesondere durch die geschäftliche Nutzung privater Geräte verschärft; siehe zu dieser Entwicklung u.a. FRANKS, 188.

195 CORTADA, Corporation, 23. Die wertorientierte Perspektive verdeutlicht das Problem, da Unternehmen im Regelfall beispielsweise über den Bestand und die Verwendung finanzieller Mittel stets sehr genau im Bilde sein werden.

196 FRANKS, 33.

tragenden Unternehmen selbst[197]. Ein zusätzliches Risiko aus Sicht des datenübertragenden Unternehmens besteht in der Verbreitung der Daten durch zusätzliche Personen, die einem innerhalb des Unternehmens definierten Nutzerkreis nicht angehören. Die Zugangskontrolle beim Cloud-Dienst ist hier ein wesentliches Kriterium für die Auslagerung von Daten. Die Zugangskontrollen sollten indessen mindestens jenen des datenübertragenden Unternehmens entsprechen und die Angestellten des Cloud-Anbieters sollten anhand des gleichen Standards überprüft und geschult werden, wie die Angestellten des datenübertragenden Unternehmens[198]. Im Weiteren kann ein Kontrollverlust durch den illegalen Zugriff Dritter erfolgen[199]. Die Erfahrung zeigt, dass Datenpannen zu einer Kettenreaktion führen können. Wenn ein Unternehmen die Kontrolle über Personendaten verliert, wirken sich die Folgen des Verlusts letztlich (direkt oder indirekt) beim Nutzer aus[200]. Ein weiterer Aspekt des Kontrollverlusts aus Sicht von Unternehmen entwickelte sich zu Beginn des 21. Jahrhunderts. Bis zum Ende des 20. Jahrhunderts dienten elektronische Systeme hauptsächlich zur Abwicklung und Erfassung geschäftsrelevanter Vorgänge in Unternehmen. Mit der Entwicklung kollaborativer Systeme können die Nutzer nun zunehmend eigene Inhalte erstellen und verbreiten, die Unternehmen verfügen entsprechend nicht mehr über die alleinige Kontrolle der Inhalte[201].

(2) Begründung einer Rechtsverletzung

Generell wird man zwar davon ausgehen können, dass Daten an sich weder Wert schaffen noch Probleme verursachen und nur durch die Verwertung Nutzen und Risiken generiert werden[202]. Vorhandene Daten sind jedoch Voraussetzung eines möglichen Missbrauchs und schaffen ein Grundrisiko[203]. Dieses weist in Bezug auf den Zugang zu Daten eine qualitative und eine quantitative Seite auf. In qualitativer Hinsicht begründet die Art der zugänglichen Daten das Risiko einer Rechtsverletzung. Der Zugang zu personenbezogenen Daten beispielsweise kann Haftungsfolgen aus Persönlichkeitsverletzungen nach sich ziehen[204]. In quantitativer Hinsicht kann der Zugang zu relevanten Informationen durch die Menge an verfügbaren Daten erschwert werden. Die Speiche-

197 FRANKS, 237 f.
198 FRANKS, 119.
199 FRANKS, 237.
200 MATHER/KUMARASWAMY/LATIF, 150.
201 FRANKS, 13.
202 WORLD ECONOMIC FORUM, Value, 12.
203 MELCHIOR, 139.
204 BGer vom 14.1.2013, 5A_792/2011; zur Datensicherheit ROSENTHAL, Handkommentar DSG, Art. 7 N 4 ff.

rung wachsender Datenmengen birgt daher das Risiko, dass tatsächlich benötigte Daten aufgrund der Datenmenge nicht mehr gefunden oder nicht mehr aufgenommen werden können. Im ersten Fall kommt es zum Konfusionseffekt: Angesichts der Masse an verfügbarer Information verliert der Empfänger den Überblick. Im zweiten Fall kommt es zum Kassandra-Effekt: Aufgrund der unüberblickbar grossen Menge an Informationen verweigert der Empfänger die Kenntnisnahme[205]. Die durch die Speicherung hervorgerufene Einschränkung einer effektiven Zugänglichkeit von Informationen kann auf diese Weise die Verwertung negativ beeinflussen bzw. im Extremfall faktisch verunmöglichen[206]. Hierdurch begründete Rechtsverletzungen ergeben sich daher insbesondere aus der mangelnden Kenntnisnahme bzw. korrekten Einhaltung von Normen[207].

b) Verwertung von Informationen

(1) Fehlerhafte oder unzulässige Verwertung

Der Vorgang des Verwertens ist auf die Erzielung eines unmittelbaren Nutzens ausgerichtet und damit eine Ausprägung der Verwendung, die die Umsetzung von Information in ein Verhalten generell umfasst[208]. Die Fortschritte der Informationstechnologie in der Aggregation und Analyse von Daten haben zu einer Systematisierung der Verwertung geführt. Daraus sind neue Unternehmen hervorgegangen, die Daten sammeln und nach der Aufbereitung ihren Kunden direkt zugänglich machen. Suchmaschinenanbieter beispielsweise speichern Suchanfragen oft länger, als dies zur Erbringung der eigentlichen Suchdienstleistung nötig wäre. Die gesammelten Daten werden insbesondere zu Marketingzwecken und zur Verbesserung des Suchmechanismus verwendet[209]. Die Verbesserung des Suchmechanismus resultiert wiederum in mehr Suchanfragen und einer erhöhten Relevanz für die Nutzung zu Marketingzwecken.

Ein wesentliches Risiko bei der Verwertung von Daten ergibt sich aus der möglichen Mangelhaftigkeit einer Schlussfolgerung und den daraus resultierenden Entscheidungen bzw. Verhaltensweisen – aus falschen oder unvollständigen Daten werden falsche Schlüsse gezogen[210]. Informationen können ungenau, unvollständig, aus dem Zusam-

---

205 WEBER, Aufbewahrung, 67. Siehe zum Problem überfordernder Datenmengen auch MCKEEN/SMITH, 203; KUHLEN, 83; GASSER, Law, 19 ff.; zur Relevanz der Kommunikation bei steigenden Informationsmengen DRUCKER, 202.

206 TUTEN/SOLOMON, 176.

207 Siehe zum Relevanzgewinn der Datenbearbeitung für das Recht SIMITIS SPIROS, Informationskrise des Rechts und Datenverarbeitung, Karlsruhe 1970.

208 DRUEY, Information, 12.

209 WALDO/LIN/MILLETT, 102.

210 PURTOVA, 47.

menhang gerissen, veraltet, nicht erklärt, falsch gewichtet oder schlicht nicht wahrheitsgetreu sein[211]. Die Fehlerhaftigkeit wird einerseits durch bewusste Manipulation erreicht. Andererseits können Fehlinformationen aber auch auf der Art der Datensammlung und Auswertung beruhen[212]. Eine Fortschreibung von Daten, die zum gegebenen Zeitpunkt nicht benötigt werden, verursacht Kosten, denen kein unmittelbarer Nutzen gegenübersteht[213]. So werden Daten aufgrund ihres potentiellen Werts erhalten und gegebenenfalls nicht mehr auf ihre Qualität überprüft. Die heutigen Methoden zur Analyse grosser Datenmengen versprechen hierbei neue Einsichten und präzise Prognosen diverser Vorgänge. Diese werden massgeblich durch die Zusammenführung verschiedener Daten in einem System erzielt. Systeme gegenseitiger Bestätigung und Ausdifferenzierung, die bestimmte Sachverhalte erfassen, weisen jedoch eine bedeutende Störanfälligkeit auf[214]. Die serielle Sammlung von Daten aus verschiedenen Quellen, die anschliessend kombiniert und verwertet werden, führt dazu, dass sich fehlerhafte Daten entscheidend auf das Resultat der Auswertung auswirken. In einem System von voneinander abgegrenzten Bereichen, wirken sich solche Störanfälligkeiten nur innerhalb dieser isolierten Bereiche aus. Fehlerhafte Informationen haben hier nur eine begrenzte Ausbreitungsmöglichkeit[215]. Bei fehlerhaften Daten ist die Verwertung insofern als fehlerhaft zu betrachten, als dass die Verarbeitung die Fehlerhaftigkeit der Daten nicht aufzuzeigen vermag[216].

(2) Begründung einer Rechtsverletzung

Die Fehlerhaftigkeit der Verwertung kann rechtliche Folgen zeitigen, wo Daten an Dritte[217] oder an Vertragspartner[218] übermittelt werden und aus der Fehlerhaftigkeit ein Schaden entsteht[219]. Die Unzulässigkeit der Verwertung ist rechtlich weiter von Bedeutung, wo eine Verletzung relevanter Schutzvorschriften gegeben ist. Dabei kann es sich insbesondere um persönlichkeitsrechtliche, datenschutzrechtliche oder immaterialgüterrechtliche Normen handeln. Am Beispiel des Rechts am eigenen Bild lässt sich zeigen, dass die Verwertung an sich die wesentliche Verletzungsform eines sich aus der

211 SEIDEL, Datenbanken, 121.
212 SEIDEL, Datenbanken, 122.
213 SEIDEL, Privatsphäre, 45.
214 BICK/MÜLLER, 307.
215 BICK/MÜLLER, 307.
216 Auch bei richtigen Daten sind es fehlerhafte Verwertungsvorgänge, die zu falschen Schlüssen führen.
217 Siehe dazu HÖRA, 70 ff.
218 Siehe zur Haftung für fehlerhafte Rechercheergebnisse aus Datenbanken THÖMEL, 72 ff.; für sachlich fehlerhafte Daten dies., 123 ff.
219 WEBER, Haftung, 542.

Speicherung ergebenden Risikos darstellt. Die blosse Aufnahme stellt normalerweise nur eine Gefährdung der Persönlichkeit, jedoch keine Persönlichkeitsverletzung dar[220], der mit der Unterlassungsklage und ergänzend mit vorsorglichen Massnahmen begegnet werden kann[221]. Anderes ergibt sich jedoch im Datenschutzrecht, das insbesondere bei einer Verletzung der in Art. 4 Abs. 1-4 DSG enthaltenen Grundsätze von der unwiderlegbaren Vermutung einer Persönlichkeitsverletzung ausgeht[222]. Eine mögliche Konkretisierung dieses Risikos besteht u.a. im Zusammenhang mit der Stellensuche. Arbeitgeber nutzen im Bewerbungsprozess zunehmend soziale Netzwerke zur Recherche von Informationen über Stellenbewerber. Die rechtliche Zulässigkeit dieses Verfahrens ist umstritten[223]. Für die auf persönlichen Websites dargestellten Informationen wurde bisher von einer zulässigen Verwertung ausgegangen[224]. Nach hier vertretener Auffassung ist nicht ersichtlich, weshalb das nicht auch für die übrigen Medien gelten soll. Die öffentlich zugänglichen Informationen sind auch dort Teil einer willkürlichen Darstellung der eigenen Person[225]. Ungeachtet der Rechtsbehelfe setzt der eigentliche Kontrollverlust indessen bereits dort ein, wo Informationen für Dritte zugänglich werden[226]. Insbesondere im Zusammenhang mit Datenbanken kann die blosse Aufzeichnung von Daten in Abhängigkeit zum jeweiligen Umfang aufgrund spezifischer Missbrauchsmöglichkeiten bereits als selbständige Verletzungsquelle erachtet werden[227]. Jedoch erscheint ein Verweis auf die Missbrauchsmöglichkeiten unter Anknüpfung an

---

220 GEISER, Persönlichkeitsverletzung, Rz. 2.22, m.H. auf die gegenteilige Lehrmeinung; so auch AEBI-MÜLLER, Rn. 825; differenzierend unter Verweis auf «sensible» Daten und unter Berücksichtigung der Entwicklung der Informationstechnologie, HAUSHEER/AEBI-MÜLLER, Rz. 12.136, allgemein ablehnend für zufällige Aufnahmen, Rz. 13.29; so auch MEILI, in: Honsell/Vogt/Geiser, Art. 28 N 20; vgl. ferner JÄGGI, 230a; HOFFMANN, 21; a.A. LÉVY, 197; BUCHER, Persönlichkeitsschutz, Rn. 454, weist darauf hin, dass bereits die Aufnahme des Bildes oder der Stimme insbesondere das Risiko einer «ausgedehnten und nicht kontrollierbaren Verbreitung» begründe und entsprechend persönlichkeitsverletzend sein könne; RIKLIN, 204, verweist auf die übermässige Bedrohung durch den Eingriff und die Folgen auf das Gefühlsleben des Bedrohten und bejaht das Vorliegen eines Eingriffs bei blosser Fixierung ebenfalls; so auch MEILI, in: Honsell/Vogt/Geiser, Art. 28 N 19; In BGE 138 II 360 stützt das Bundesgericht die Ansicht, wonach bereits die blosse Aufnahme eine Persönlichkeitsverletzung bedeuten kann; siehe dahingehend auch bereits WARREN/BRANDEIS, 193 ff.

221 AEBI-MÜLLER, Rn. 825.

222 ROSENTHAL, Handkommentar DSG, Art. 4 N 2; siehe auch MEISTER, 153, das Recht am eigenen Datum knüpft bei der Erhebung an und bereits die Sammlung stellt eine Verwendung dar, die das Selbstbestimmungsrecht des Betroffenen tangiert.

223 EGLI, 8, m.w.H.; AMBROSE, 406, weist darauf hin, dass hier alte Daten zu schlechten Entscheiden führen könnten, da sie möglicherweise den aktuellen Status überschatten würden.

224 HOLENSTEIN, 141.

225 KLAS, 32 ff., plädiert für einen differenzierten Ansatz.

226 Siehe dazu vorne A.I.3.2 a)(1).

227 SEIBEL, 116.

die Datenmenge an sich als fragwürdig[228]. Auch eine einzelne Fotografie kann bei entsprechendem Sujet ein erhebliches Missbrauchspotential in sich bergen und über eine blosse Indiskretion hinausgehen[229].

c) Löschung von Informationen

(1) Löschen und Vergessen

Für den Menschen stellt das Vergessen eine tatsächliche Schranke dar; das verfügbare Wissen wird durch die beschränkte Aufnahmefähigkeit und durch die bewusste Unterteilung in relevante und unwichtige Informationen zeitlich limitiert[230]. In Unternehmen ist zwischen dem gespeicherten Wissen und der aktuellen Kenntnis in Form des tatsächlich genutzten Wissens zu unterscheiden[231]. Letzteres lässt ein Vergessen ohne Löschung zu, wenn beispielsweise noch vorhandene Daten nicht mehr genutzt werden. Von einer Löschung ist aber nur dann auszugehen, wenn die gespeicherten Inhalte nicht mehr rekonstruiert werden können[232]. In diesem Fall wird die juristische Person auch von den Folgen der Unkenntnis befreit. Die Zurechnung des verlorenen Wissens unterbleibt, sofern kein Verschulden der Organisation gegeben ist. Zulässig ist hier beispielsweise die Beseitigung von Akten nach Ablauf der Aufbewahrungsfrist. Auch bei Diebstählen, unverschuldeten Bränden oder dem Eindringen von Computerviren wird das Unternehmen regelmässig nicht haftbar, sofern die erforderlichen Schutzvorkehren getroffen wurden[233].

In einem erweiterten Kontext kann bereits dem Versuch des Löschens bzw. Vergessens ein gewisses immanentes Risiko zugeschrieben werden: «Was einmal in der Welt ist,

---

228 Das DSG differenziert entsprechend nicht einzig anhand der Menge der bearbeiteten Daten, sondern berücksichtigt auch die Qualität und verlangt gemäss Art. 4 Abs. 5 DSG eine ausdrückliche Einwilligung für die Bearbeitung von Persönlichkeitsprofilen. Bei Persönlichkeitsprofilen handelt es sich gemäss Art. 3 lit. d DSG um eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person ermöglicht; vgl. dazu das Urteil der Eidgenössischen Datenschutzkommission vom 27. Januar 2000, VPB 65.48, I. 2. b., wo ergänzend auf die Bedeutung der zeitlichen Dimension hingewiesen wird.

229 Ähnlich HOFFMANN, 21, der auf die einem Entscheid nicht zugängliche Frage nach der Sensibilität eines Datums hinweist; a.M. SEIBEL 116.

230 CHOU, Rn. 604.

231 CHOU, Rn. 606 f.

232 Siehe die Legaldefinition in BDSG § 3 Abs. 4 Satz 2 Nr. 5, wonach Löschen «das Unkenntlichmachen gespeicherter personenbezogener Daten» ist; vgl. dazu SIMITIS, in: ders., § 3 N 174: «Der Begriff „Unkenntlichmachen" trifft auf jede Handlung zu, die irreversibel bewirkt, dass eine Information nicht länger aus gespeicherten Daten gewonnen werden kann.»; siehe ferner GOLA/KLUG/KÖRFFER, § 3 N 40, wonach der grundbuchrechtliche Löschungsbegriff dieser Anforderung nicht entspricht, da der Text dort unverändert erhalten bleibe und die Ungültigkeit lediglich durch rotes Unterstreichen angezeigt werde.

233 CHOU, Rn. 637 ff. m.w.H.

kann man nur formal negieren. Und die Negation, die macht es stark, vielleicht sogar stärker als ohne Negation, die Negation lädt es mit Energie auf.»[234] Man kann nicht willentlich vergessen. Die Aufmerksamkeit lässt sich nicht ins Negative kehren und was man zu vergessen sucht, bleibt umso mehr in ihrem Fokus[235]. So ist nicht nur die Speicherfähigkeit thematisch kaum eingrenzbar, sondern eng damit verbunden auch die Automatisierung der Löschung von Erinnerung unüberschaubar und die Folgen nicht abzusehen[236].

(2) Begründung einer Rechtsverletzung

Der datenschutzrechtliche Begriff des Bearbeitens umfasst nach Art. 3 lit. e DSG jeden Umgang mit Personendaten. Die Aufzählung ist beispielhaft. Insbesondere ist auch das Vernichten von Personendaten eingeschlossen[237]. In der Lehre wird der Einschluss des Vernichtens hauptsächlich auf den Aspekt der Vertraulichkeit zurückgeführt[238]. Werden sensitive Unterlagen im Abfall entsorgt und vorher nicht unlesbar gemacht, oder elektronische Daten auf einer Festplatte nur scheinbar gelöscht, da der Löschbefehl im Computer die Daten normalerweise nur als gelöscht markiert, diese aber nicht überschreibt, wird die Persönlichkeit der Betroffenen allenfalls verletzt[239]. Problematisch ist in diesem Zusammenhang auch, dass insbesondere umfangreiche Datenbestände oft ausserhalb des Kontrollbereichs des ursprünglichen Dateninhabers gelöscht werden[240]. Doch auch das tatsächliche Vernichten von Personendaten kann die Persönlichkeit einer Person verletzen, da unter Umständen in ihre Privatsphäre eingegriffen und zudem ihr informationelles Selbstbestimmungsrecht verletzt wird[241].

---

234 PAZZINI, 42; siehe auch Michel De Montaigne: «Nichts hält etwas intensiver in der Erinnerung fest, als den Wunsch es zu vergessen.».

235 DRAAISMA, 18, die Griechen haben uns nur die *ars memoriae,* keine *ars oblivionis* hinterlassen; siehe ferner zum Vergessen als nicht aktiven Akt LOTZ, 88 f.

236 MEIER, 31.

237 ROSENTHAL, Handkommentar DSG, Art. 3 N 64.

238 BELSER, in: Maurer-Lambrou/Vogt, Art. 3 N 28.

239 ROSENTHAL, Handkommentar DSG, Art. 3 N 65.

240 BEGLINGER et al., 116.

241 ROSENTHAL, Handkommentar DSG, Art. 3 N 65, nennt hier beispielhaft den Arbeitgeber, der von sich aus sämtliche privaten E-Mails eines Arbeitnehmers in dessen Posteingang auf dem E-Mail-Server oder auf der Festplatte löscht. Die Verletzung besteht auch dann, wenn er keine Einsicht in die Nachrichten nimmt.

3.3 Information als Gegenstand der Risikosteuerung

a) Wissenstransfer und Geheimhaltung

Das Wissen umfasst sämtliche «Informationen, Kenntnisse und Fähigkeiten, die einem Menschen bei der Bewältigung von Aufgaben und Problemen zur Verfügung stehen»[242]. Unternehmen verfügen über die notwendigen Strukturen, um Informationen an zukünftige Mitglieder der Organisation weiterzugeben und relevantes Wissen über einen längeren Zeitraum zu bewahren[243]. Die globale und dezentrale Struktur wirtschaftlicher Vorgänge lässt Dokumente mit relevanten Wissensinhalten nicht mehr nur an einem Ort, sondern an einer Vielzahl von Orten entstehen. Die Geschwindigkeit dieser Prozesse erhöht das Risiko der Lücke[244]. Die Rolle der Risikosteuerung kommt hierbei der Metainformation über die Vorgänge zur Aufbewahrung von Informationen zu. Die Information darüber, was in welcher Weise wo aufzubewahren ist, schafft den Rahmen für den Erhalt und den Zugang zu Daten[245], die sowohl rechtlich als auch wirtschaftlich relevant sein können[246]. Elektronische Akten- und Archivsysteme gewährleisten die Nachvollziehbarkeit der Unternehmenstätigkeit und dienen als Wissensquellen für künftige Geschäftsvorgänge[247]. Die Schutzwürdigkeit der vorhandenen Daten liegt einerseits in ihrem Inhalt und andererseits in der Vertraulichkeit generell begründet. Im ersten Fall sollen für das Unternehmen nützliche bzw. schädliche Informationen geschützt werden, im zweiten Fall steht dagegen die Wahrung der Treuepflicht gegenüber dem Geheimnisherrn im Vordergrund[248].

b) Erhalt und Vernichtung von Beweisen

Die handelsrechtliche Aufbewahrungspflicht soll sicherstellen, dass Geschäftsbücher und weitere relevante Dokumente im Falle einer Auseinandersetzung zugänglich und

---

242 MELLEWIGT/DECKER, 614.

243 LEHNER, 36.

244 WILLI, 34.

245 SCHNEIDER, Amnesie, 36, 219.

246 Vgl. FÄSSLER, 64.

247 WEBER/WILLI, 208; SCHNEIDER, Amnesie, 36.

248 DRUEY, Information, 366; siehe dazu HÄUSERMANN, 146, rational agierende Unternehmen halten Informationen geheim, wenn die mit einer Preisgabe einhergehende Nutzenminimierung die Kosten für die Geheimhaltung übersteigt. Das Recht kann die Geheimhaltungskosten senken, indem es jenen Personen, die einen Geheimnisbruch begehen können, die Anreize dafür nimmt. Dieses Ziel wird klassischerweise durch die Strafandrohung erreicht. In allgemeiner Weise ist das Fabrikations- oder Geschäftsgeheimnis in Art. 162 StGB und Art. 6 i.V.m. Art 23 UWG enthalten. In Art. 47 Abs. 4 des Bankengesetzes wird der Geheimnisschutz im Rahmen des Bankgeheimnisses konkretisiert.

als Beweismittel verwendbar sind[249]. Ungeklärte Fragen im Zusammenhang mit der Aufbewahrung von Dokumenten können zu grossen wirtschaftlichen Schäden führen. Wenn ein Unternehmen plötzlich mit Altlasten konfrontiert wird, muss nachvollzogen werden können, wie diese entstanden sind und ob sie überhaupt am richtigen Ort sind. Solche Fälle zeigen die Schnittstelle zwischen Aufbewahrung und Archivierung[250], die einen Übergang zwischen dem Ende der gesetzlich geforderten Erhaltung von Daten und einem unternehmenseigenen Interesse zum längerfristigen Erhalt der Daten aufzeigt. Die Möglichkeit der historischen Erfassung unternehmensinterner Aufzeichnungen durch Dritte stellt aus Sicht des Unternehmens dagegen ein Risiko dar. Die Möglichkeit einer späteren Platzierung interner Dokumente in einem öffentlichen Archiv und die damit potentiell verbundene kritische Analyse durch Historiker können sich entsprechend negativ auf die Qualität der Aktenführung und den Informationsgehalt auswirken. Die Aufzeichnung von Informationen erfolgt hierbei unter Einfluss der Möglichkeit späterer Vorhaltungen[251]. Bei einem dahingehenden Bewusstsein kann wohl davon ausgegangen werden, dass heikle Inhalte gar nicht erst aufgeschrieben, rasch wieder vernichtet oder nur verklausuliert festgehalten werden[252].

4. Schlussfolgerungen

Die heutige Nutzung von Information verkörpert das neuste Stadium der ökonomischen Entwicklung. Seit dem Beginn des 20. Jahrhunderts als Henry Ford erklärte, dass jeder Kunde ein Fahrzeug in jeder gewünschten Farbe haben könne, solange diese schwarz sei[253], hat eine Verschiebung vom Primat der Produktion hin zum Primat der Informa-

249 BEGLINGER et al., 47.

250 WILLI, 34.

251 SCHENK, 201.

252 SCHENK, 201; siehe zur Vernichtung im Hinblick auf negative Folgen FRANKS, 100 f. Darüber hinaus ist, sofern die Daten doch erhalten bleiben, nachgelagert auch die Einschränkung der Verwertung relevant. Die Androhung haftungsrechtlicher Folgen kann die Qualität der Auswertung vermindern. Die Schweizerische Gesellschaft für Geschichte beispielsweise weist darauf hin, dass das Staatssekretariat für Wirtschaft (seco) Historikern «routinemässig» mit Klagen wegen der Verletzung von Fabrikations- oder Geschäftsgeheimnissen gemäss Art. 162 StGB und wegen der Verletzung des Verbots des wirtschaftlichen Nachrichtendienstes drohe, sollten sie bei der Auswertung von Daten der ehemaligen Handelsabteilung bzw. des Bundesamtes für Aussenwirtschaft (BAWI) die Namen von Unternehmen nennen. Die Schweizerische Gesellschaft für Geschichte erachtet dies als nicht annehmbar, da Forschungsprojekte, die sich auf Entscheidungsprozesse- und Strukturen konzentrierten oder «Akteure und informelle Netzwerke» untersuchten, ohne die Identifikation der Hauptakteure nicht durchführbar seien; siehe Schweizerische Gesellschaft für Geschichte, Ethik-Kodex und Grundsätze zur Freiheit der wissenschaftlichen historischen Forschung und Lehre, Bern 2004 (ergänzt 2012), Nr. 19.

253 FORD, 72.

tion bzw. Personalisierung stattgefunden[254]. Die mit dem steigenden Wettbewerb einhergehende Notwendigkeit zur Differenzierung von Produkten und Dienstleistungen setzt die Anbieter unter Druck, die Bedürfnisse der Kunden bestmöglich zu kennen und ihre Aufmerksamkeit zu gewinnen. Im Rahmen der Bedienung dieser Kundenbedürfnisse bzw. der Erzeugung neuer Bedürfnisse ist der Vorgang der Informationsverarbeitung von entscheidender Bedeutung. Im Weiteren dient Information zur Ausgestaltung der Produktions- und Dienstleistungsprozesse, wo sie insbesondere als Führungsinstrument eingesetzt wird. Unternehmen werden auch weiterhin vermehrt zu informationszentrierten Organisationen, da Information zunehmend als Mittel zur Reduktion von Unsicherheiten und zur Beschränkung von Risiken einerseits sowie zur Generierung von Profit andererseits eingesetzt wird[255].

Informationen werden auf jeder Stufe der Wertschöpfung generiert, verarbeitet und übermittelt. Entsprechend sind die rechtlichen Rahmenbedingungen auf all diesen Stufen zu beachten[256]. Die Verschiedenheit der Regulierung in den einzelnen Ländern erschwert die Einhaltung der Gesetze für multinationale Unternehmen[257]. Auf der Basis eines tragenden Informationsmanagements, dessen Ausgestaltung den potentiell anwendbaren nationalen Gesetzen von Beginn weg Rechnung trägt, können für das Unternehmen Vorteile generiert und Risiken verringert werden. Die Vorteile umfassen den Schutz sensitiver und historisch bedeutsamer Daten, die Erhaltung der Unternehmensgeschichte und Identität sowie die effektive Kontrolle der Informationsvorgänge im Unternehmen[258]. Risikoseitig sind ausserrechtliche Reputationsschäden[259], die Wahrung der unternehmerischen Kontinuität und der Schutz von Geschäftsgeheimnissen sowie mögliche Kostenfolgen aus Rechtsverletzungen relevante Faktoren des Informationsmanagements.

254 Vgl. POLZER, 9; SCHAAR, 186 f.

255 CORTADA, Corporation, 149.

256 BEGLINGER et al., 35.

257 WHITE/MÉNDEZ MEDIAVILLA/SHAH, 66.

258 FRANKS, 48.

259 POLZER, 7, verweist auf die Gefahr einer Schädigung der Unternehmensmarke durch die Verletzung der Privatsphäre von Kunden.

II. Beschränkung auf zeitbezogene Aspekte

1. Expliziter und impliziter Zeitbezug in der Rechtsordnung

1.1 Zeitbezogene Abgrenzung

Das *Records Management* erfasst regelmässig Daten, für die die Rechtsordnung einen expliziten Zeitbezug in Form eindeutig definierter Aufbewahrungsfristen vorsieht. In Abgrenzung dazu richtet sich die Aufbewahrung von Dokumenten, die nicht Gegenstand dieser explizit zeitbezogenen Normen sind sowie die langfristige, über die gesetzlich explizit statuierte Frist hinausgehende Archivierung von Unterlagen[260] für Personen des privaten Rechts nach den Normen, die einen impliziten Zeitbezug aufweisen. Ein solcher findet sich beispielsweise im Persönlichkeitsrecht in Form der Unzulässigkeit einer übermässigen Bindung nach Art. 27 Abs. 2 ZGB oder im Datenschutzrecht in Form einer unverhältnismässigen Datenbearbeitung nach Art. 4 Abs. 2 DSG.

1.2 Auswahl relevanter Gesetze

Im Bereich der explizit zeitbezogenen Normen sind insbesondere die Bestimmungen des Obligationenrechts über die Führung und Aufbewahrung von Geschäftsbüchern und Buchungsbelegen relevant. Darüber hinaus bestehen zahlreiche weitere Vorschriften, die eine Dokumentation und Aufbewahrung verlangen, durch die insbesondere die Einhaltung von Normen in spezifischen Bereichen nachgewiesen wird[261]. Im Rahmen dieser Arbeit wird nur auf einige wenige explizit zeitbezogene Normen im nationalen Recht eingegangen. Anhand dieser sollen die unterschiedlich motivierte Normierung eines zeitlichen Erhalts und die entsprechende Systematik aufgezeigt werden. Für international tätige Unternehmen ist an dieser Stelle auf die zahlreichen zusätzlichen ausländischen und internationalen Regelungen zu verweisen[262]. Für Private ebenfalls relevant ist das Registerrecht, das in zeitlicher Hinsicht häufig eine sehr lange oder gar eine «ewige» Aufbewahrungsdauer vorsieht. Aufgrund seiner Zugehörigkeit zum öffentlichen Recht und der unternehmensexternen Informationsverwaltung ist das Registerrecht im vorliegenden Zusammenhang jedoch nicht von Bedeutung.

Bei den implizit zeitbezogenen Normen liegt der Schwerpunkt der Betrachtung auf dem Persönlichkeits- und Datenschutzrecht, da diese Normen als Fundament weiterer dahingehend motivierter Regelungen dienen. Sofern personenbezogene Daten bearbeitet werden ist das DSG grundsätzlich anwendbar. Die datenschutzrechtliche Kompo-

---

260 Siehe dazu vorne A.I.2.3 a).

261 BEGLINGER et al., 62 f.

262 Siehe die graphische Übersicht bei SCHNEIDER, Amnesie, 34.

nente ist damit Teil des *Records Managements*, sofern Personendaten bearbeitet werden[263]. Die Aufbewahrung von Daten und Unterlagen ist eine Bearbeitung nach Art. 3 lit. e DSG und unterliegt entsprechend den Datenschutzgrundsätzen in Art. 4 DSG. Die Aufbewahrung und Archivierung von Daten kann insbesondere aufgrund ihres Umfangs oder ihrer Dauer eine Persönlichkeitsverletzung begründen[264].

Das Strafrecht weist im Unterschied zum Privatrecht einen engeren Persönlichkeitsschutz auf. Sofern eine Persönlichkeitsverletzung einen Straftatbestand erfüllt, der den Schutz der Persönlichkeit bezweckt, ist die Handlung auch zivilrechtlich widerrechtlich[265]. Gleiches gilt im Verhältnis zwischen DSG und StGB, ein Datenbearbeiter ist beiden Gesetzen gleichermassen unterworfen[266]. Diese Normen des StGB werden entsprechend nicht gesondert behandelt. Daneben gibt es einige strafrechtliche Bestimmungen, die für sich selbst stehen und im jeweiligen Zusammenhang dargestellt werden.

2. Fazit

Das Informationsmanagement orientiert sich in zeitlicher Hinsicht an den normativen Vorgaben, die sich in explizit und implizit zeitbezogene Normen unterteilen lassen. Die explizit zeitbezogenen Normen beziehen sich hauptsächlich auf die Aufbewahrung von Informationen über einen vordefinierten Zeitraum. Den implizit zeitbezogenen Normen liegt dagegen nicht der Schutz des Informationsbestands an sich, sondern der Schutz subjektiver Rechte zugrunde.

263 BEGLINGER et al., 37, 41.
264 BEGLINGER et al., 114.
265 GEISER, Persönlichkeitsverletzung, Rz. 1.12.
266 BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, § 8 Rn. 74.

B. Zeitbezogene Normen im geltenden Recht

I. Explizit zeitbezogene Normen

1. Obligationenrecht

Die Buchführungs- und Aufbewahrungsvorschriften des Obligationenrechts und die darauf basierende Geschäftsbücherverordnung (GeBüV) können als die wesentlichste gesetzliche Grundlage im Bereich der Buchführung und Aufbewahrung bezeichnet werden und bilden gewissermassen einen «Allgemeinen Teil» des Aufbewahrungsrechts[267]. Die Aufbewahrung von geschäftsrelevanten Informationen ist in Art. 957 ff. OR und in den auf Art. 958f Abs. 4 OR gestützten Ausführungsbestimmungen der Geschäftsbücherverordnung geregelt. Die Verletzung dieser Vorschriften ist strafbar[268]. Im Wesentlichen müssen die geschäftsrelevanten Bücher nach kaufmännischen Grundsätzen ordnungsgemäss geführt werden. Die der GeBüV unterstehenden Dokumente müssen nach Art. 958f Abs. 1 OR während zehn Jahren aufbewahrt werden[269]. Die Dokumente können dabei gemäss Art. 958f Abs. 2 OR elektronisch oder in vergleichbarer Weise aufbewahrt werden, soweit die zugrunde liegenden Geschäftsvorfälle und Sachverhalte unverändert dokumentiert sind und jederzeit wieder lesbar gemacht werden können[270]. Indessen gilt der Grundsatz der Unveränderbarkeit nicht absolut, Art. 3 GeBüV trägt dem Umstand Rechnung, dass sich im Nachhinein ein Berichtigungsbedarf ergeben kann; dieser muss aber nachvollziehbar bleiben[271].

Die Organisation von Unterlagen unterliegt gemäss Art. 7 GeBüV einem zeitlichen Argument. Die Bestimmung sieht in Art. 7 Abs. 1 GeBüV entweder die Trennung von archivierten und aktuellen Informationen oder eine entsprechende Kennzeichnung vor[272]. Die Wahl des jeweiligen Verfahrens hängt vom einzelnen Unternehmen sowie insbe-

---

267 BEGLINGER, et al., 46.

268 Gemäss Art. 325 StGB wird mit Busse bestraft «[...] wer vorsätzlich oder fahrlässig der gesetzlichen Pflicht, Geschäftsbücher, Geschäftsbriefe und Geschäftstelegramme aufzubewahren, nicht nachkommt.».

269 Mit dem neuen Rechnungslegungsrecht das am 1. Januar 2013 in Kraft trat, muss nicht mehr die gesamte Geschäftskorrespondenz aufbewahrt werden. Die neue Bestimmung in Art. 958f Abs. 1 OR enthält den Begriff «Geschäftskorrespondenz» nicht mehr, sondern beschränkt sich auf Geschäftsbücher und Buchungsbelege.

270 Siehe zur elektronischen Aufbewahrung BEGLINGER et al., 206 ff.; FÄSSLER, 29 f.; WEBER, Aufbewahrung, 1 ff.

271 BEGLINGER et al., 53; siehe dort auch Ausführungen zu den weiteren Grundsätzen der GeBüV.

272 Der Zeitpunkt der Archivierung wird in modernen Archivsystemen mittels Zeitstempel festgehalten. Technisch betrachtet handelt es sich dabei um digitale Signaturen; BEGLINGER et al., 222; zu den digitalen Signaturen siehe u.a. eingehend SCHLAURI SIMON, Elektronische Signaturen, Diss. Zürich 2002; SCHNEIDER, Amnesie, 47 ff.

sondere von organisatorischen und finanziellen Aspekten ab[273]. Sofern die dem Archivsystem zugeordneten Dokumente noch der handelsrechtlichen Aufbewahrungspflicht unterstehen, muss das System die Anforderungen von Art. 8 GeBüV erfüllen, wonach der Schutz vor unbefugtem Zugriff gewährleistet und Zugriffe bzw. Zutritte aufgezeichnet werden müssen[274]. Abgesehen von den gesetzlichen Erfordernissen bringt eine klare Trennung von aktuellen und archivierten Unterlagen auch operationelle Vorteile[275]: Erstens ist die Frage nach dem Lebenszyklus der einzelnen Daten eindeutig zu beantworten, dieser Prozess erhöht den Nutzen des *Records Management*. Darüber hinaus wird aus betriebswirtschaftlicher Sicht weniger Speicherplatz gebunden und die Flexibilität bezüglich der benutzten Applikationen bleibt gewahrt, da andernfalls immer wieder die Lesbarkeit und Systemkonformität der alten Daten überprüft und sichergestellt werden müssen. Schliesslich werden Unternehmensverkäufe und Übernahmen vereinfacht, da zu jedem Zeitpunkt Klarheit über die relevanten Daten besteht. Nebst diesen operationellen Aspekten muss die Verantwortung für die Informationen klar geregelt sein und dokumentiert werden. Die Pflicht des Verwaltungsrates zur Sicherstellung der Einhaltung gesetzlicher Vorgaben ergibt sich in der Aktiengesellschaft aus Art. 716a Abs. 1 Ziff. 5 OR.

Sofern auf Gesetzes- und Verordnungsstufe (insbesondere OR und GeBüV) nichts anderes vorgesehen ist, richtet sich die Ordnungsmässigkeit der Führung und Aufbewahrung der Bücher gemäss Art. 2 Abs. 3 GeBüV nach den anerkannten Standards zur Rechnungslegung. Die technischen und organisatorischen Einzelheiten werden durch das Gesetz nicht geregelt, da insbesondere die technische Entwicklung einem starken Wandel unterliegt. Die *best practice* richtet sich in diesem Zusammenhang nach Normen und Standards, denen durch die ausdrückliche Bezugnahme in der GeBüV grosse Bedeutung zukommt[276]. Unabhängig von spezifischen Standards im Bereich der Rechnungslegung, besteht mit dem ISO-Standard 15489 seit 2001 eine internationale Normierung, die allgemeine Leitlinien zur Verwaltung von Schriftgut in öffentlichen und

273 Siehe zum Ganzen BEGLINGER et al., 241 ff.

274 BEGLINGER et al., 210.

275 Siehe dazu BEGLINGER et al., 245 f.

276 FÄSSLER, 53 ff., verweist auf die ISO-Norm 15489, die Model Requirements for the Management of Electronic Records – MoReq, das Konzept DOMEA – Dokumentenmanagement und elektronische Archivierung und den Standard ISO 14721 – OAIS-Referenzmodell. Das DOMEA-Konzept wurde 2012 durch das Organisationskonzept elektronischer Verwaltungsarbeit ersetzt; siehe dazu die Einschätzung bei POPP, 54 ff.

privaten Organisationen umfasst[277]. Darüber hinaus sind Dossiers für die öffentliche Verwaltung ein wichtiger Bestandteil der Arbeitsabläufe in Behörden. Die lange Tradition des *Records Management* in diesem Sektor hat zu etablierten nationalen und internationalen Standards geführt[278]. Eine Tendenz zur Entwicklung solcher Standards ist auch auf der Ebene einzelner multinationaler Unternehmen zu beobachten[279]. Darüber hinaus können zudem ausländische Aufbewahrungsvorschriften relevant sein. Diese sind insbesondere zu beachten, wenn Teile eines Unternehmens, z.B. in Form von Tochtergesellschaften oder in Form einer sog. Betriebsstätte, im Ausland liegen. Entsprechend können bereits im Ausland betriebene Server über die Teile der Geschäftstätigkeit abgewickelt werden, die Berücksichtigung spezifischer Anforderungen begründen[280].

2. Steuerrecht

In Abweichung zu den handelsrechtlichen Aufbewahrungsvorschriften kann eine Veranlagung der Mehrwert- und der Einkommenssteuer in Bund und Kantonen bis fünfzehn Jahre nach Ablauf der jeweiligen Steuerperiode vorgenommen werden[281]. Die relevanten Daten sind entsprechend über die handelsrechtliche Aufbewahrungsfrist hinaus aufzubewahren. Aus datenschutzrechtlicher Sicht begründen die steuerrechtlichen Normen eine Rechtsgrundlage nach Art. 4 Abs. 1 i.V.m. Art. 13 Abs. 1 DSG, wonach eine Aufbewahrung personenbezogener Daten durch Gesetz legitimiert wird. Nebst den allgemeinen Aufbewahrungsvorschriften besteht im Mehrwertsteuerrecht in Form der Verordnung des Eidgenössischen Finanzdepartements über elektronisch übermittelte Daten und Informationen (EIDI-V) eine Sonderregelung für elektronische Daten[282].

3. Telekommunikations- und Rundfunkrecht

3.1 Fernmeldegesetzgebung

Wer mit fernmeldedienstlichen Aufgaben betraut ist oder betraut war, darf gemäss Art. 43 Fernmeldegesetz (FMG) Dritten grundsätzlich keine Angaben über den Fernmelde-

277 BEGLNGER et al., 37; TOEBAK, in: Coutaz et al., 252.; siehe eingehend LUTZ ALEXANDRA (Hrsg.), Schriftgutverwaltung nach DIN ISO 15489-1: Ein Leitfaden zur qualitätssicheren Aktenführung, Berlin 2012; KOS PATRICK, Rechtliche Anforderungen an die elektronische Schriftgutverwaltung in der Privatwirtschaft und Zertifizierungen nach ISO 15489-1 und ISO/IEC 27001, Zürich 2011.

278 Siehe die Übersicht bei BEGLINGER et al., 289.

279 Eingehend MOEREL, 87 ff.

280 Vgl. BEGLINGER et al., 180.

281 Art. 49 Abs. 4 MWSTG, Art. 120 Abs. 4 und Art. 152 Abs. 3 DBG, Art. 47 Abs. 1 StHG.

282 Siehe dazu WEBER/WILLI, 209.

verkehr von Teilnehmerinnen und Teilnehmern machen und niemandem Gelegenheit geben, solche Angaben weiterzuleiten. Gegenüber ihren Kunden müssen die Fernmeldedienstanbieterinnen gemäss Art. 45 FMG jedoch Auskünfte über die für die Rechnungsstellung verwendeten Daten geben können. Standortdaten von Kunden dürfen nur für die Fernmeldedienste und ihre Abrechnung bearbeitet werden. Die Bearbeitung für andere Dienste erfordert nach Art. 45b FMG die Einwilligung des Kunden oder die Anonymisierung der Daten. In der Verordnung zum Fernmeldegesetz (FDV) finden sich weitere Bestimmungen zum Fernmeldegeheimnis und zum Datenschutz. In zeitlicher Hinsicht ist insbesondere Art. 80 FDV relevant, der vorsieht, dass persönliche Kundendaten nur soweit und solange bearbeitet werden dürfen, wie dies für den Verbindungsaufbau resp. für die Erfüllung der im BÜPF statuierten Pflichten erforderlich ist.

Der Zugriff auf Informationen des Fernmeldegeheimnisses bzw. der Privatsphäre bedarf einer gesetzlichen Grundlage, der Verhältnismässigkeit und eines öffentlichen Interesses[283]. Dem Erfordernis einer gesetzlichen Grundlage entsprechend wurde im Jahr 2000 das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und im folgenden Jahr dessen Ausführungsverordnung (VÜPF) erlassen. Im Jahr 2007 kam die eidgenössische Strafprozessordnung hinzu. Gesetz und Verordnung regeln die Echtzeitüberwachung und die rückwirkende Überwachung (Art. 16, 24a, 24b VÜPF) des Fernmeldeverkehrs sowie die Auskunftserteilung über Teilnehmer (Art. 19, 27 VÜPF) zum Zwecke der Strafverfolgung. Im Rahmen der Fernmeldegesetzgebung müssen alle Fernmeldedienstanbieter Verkehrs- und Randdaten speichern. Die Speicherfrist beträgt gemäss Art. 15 Abs. 3 BÜPF (Anbieter Fernmeldeverkehr) aktuell noch sechs Monate, im Rahmen der Revision des BÜPF soll die Frist auf zwölf Monate erhöht werden (Art. 23 E BÜPF)[284]. Die zeitlich über die unternehmensnotwendige Da-

283 Art. 36 BV; eine Erläuterung der Erfordernisse findet sich u.a. in HÄFELIN/MÜLLER/UHLMANN, Rn. 307 ff.

284 In der Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens über den Bericht und den Vorentwurf zur Änderung des Bundesgesetzes vom 6. Okober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), Bern, Mai 2011, 13, wird hinsichtlich der Verlängerung eine breite Ablehnung der Teilnehmer festgestellt. Teilweise wird dabei auf die vom deutschen Bundesverfassungsgericht im Zusammenhang mit der Vorratsdatenspeicherung entwickelten Kriterien verwiesen. Das Bundesverfassungsgericht stellte im Volkszählungsurteil vom 15. Dezember 1983 insbesondere folgendes fest: «Eine vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate ist unter anderem deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiss nicht, was welche staatliche Behörde über ihn weiss, weiss aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können.», BVerfGE 65, 1, 43 f.

tenspeicherung hinausreichende Frist könnte sich grundsätzlich durch das Ziel der Gefahrenabwehr rechtfertigen lassen[285]. Indessen ist nicht klar, ob ohne diesen Erhalt überhaupt eine Schutzlücke entstehen würde[286].

Das Fernmelderecht der EU wies in Bezug auf die Speicherung von Verbindungsdaten eine mit der schweizerischen Gesetzgebung vergleichbare Regelung auf. Die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung bezweckte gemäss Art. 1 I RL die Harmonisierung der Vorschriften der Mitgliedstaaten zur Vorratsdatenspeicherung. Das Ziel bestand darin, sicherzustellen, dass die Daten für Ermittlungszwecke und die Feststellung und Verfolgung schwerer Straftaten (nach nationalem Recht) zur Verfügung stehen. Die Speicherdauer war in Art. 6 RL geregelt. Danach hatten die Mitgliedstaaten dafür zu sorgen, dass die in Art. 5 der RL angegebenen Datenkategorien[287] für mindestens sechs Monate und höchstens zwei Jahre ab dem Zeitpunkt des Kommunikationsvorgangs auf Vorrat gespeichert werden. Entgegen dem eindeutigen Wortlaut in Bezug auf die Speicherdauer sah Art. 12 RL bei besonderen Umständen die Möglichkeit einer Verlängerung der maximalen Speicherdauer durch die Mitgliedstaaten für einen begrenzten Zeitraum vor. Die besonderen Umstände wurden nicht konkretisiert[288]. Auch eine Angabe über die maximale Verlängerung der Speicherfrist fehlte[289]. Im April 2014 hat der Europäische Gerichtshof die Richtlinie zur Vorratsdatenspeicherung aufgrund ihrer Unverhältnismässigkeit im Hinblick auf den Schutz der Privatsphäre und den Datenschutz als ungültig erklärt[290].

3.2 Radio und Fernsehen

Veranstalter schweizerischer Programme müssen gemäss Art. 20 Abs. 1 des Bundesgesetzes über Radio und Fernsehen (RTVG) alle Sendungen aufzeichnen und die Auf-

---

285 ALLEN, 30; WEBER, Governance, 240.

286 Zu diesem Schluss kommt eine Studie des Max-Planck-Instituts: ALBRECHT HANS-JÖRG/KILCHLING MICHAEL (Hrsg.), Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten. Kriminologische Forschungsberichte aus dem Max-Planck-Institut, Bd. K 160, Berlin 2012.

287 Die Aufzählung in Art. 5 RL 2006/24/EG ist abschliessend, SZUBA, 52 f.; nach Art. 5 I lit. a-f sind folgende Datenkategorien auf Vorrat zu speichern: «zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten»; «zur Identifizierung des Adressaten einer Nachricht benötigte Daten»; «zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten»; «zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten»; «zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten» und «zur Bestimmung des Standorts mobiler Geräte benötigte Daten».

288 Kritisch dazu SZUBA, 57; SIMITIS, Vorratsdatenspeicherung, 1786.

289 Kritisch dazu SZUBA, 57; KINDT, 664.

290 EuGH vom 8. April 2014, C-293/12 und C-594/12.

zeichnungen sowie die einschlägigen Materialien und Unterlagen während mindestens vier Monaten aufbewahren. Sofern innert vier Monaten gegen eine oder mehrere Sendungen eine Beanstandung eingereicht, eine Beschwerde erhoben oder von Amtes wegen ein Aufsichtsverfahren eröffnet wird, müssen die Aufzeichnungen, Materialien und Unterlagen gemäss Art. 20 Abs. 2 RTVG bis zum Abschluss des Verfahrens aufbewahrt werden. Die Pflicht zur Aufzeichnung von Programmen ist eine notwendige Voraussetzung für die Kontrolle der Einhaltung von Vorschriften von Programmen und zur Durchführung entsprechender Verfahren[291]. Die Aufzeichnungs- und Aufbewahrungspflicht in Art. 20 RTVG gilt ausschliesslich gegenüber der Aufsichtsbehörde. Aufzeichnungen und Aufbewahrungen zu anderen Zwecken unterliegen den Einschränkungen im Urheberrechtsgesetz (URG)[292], da Sendungen unter den Werkbegriff nach Art. 2 URG fallen[293].

Im Rahmen der Erhaltung von Programmen kann der Bundesrat schweizerische Programmveranstalter gemäss Art. 21 Abs. 1 RTVG verpflichten, Aufzeichnungen ihrer Programme zur Verfügung zu halten, damit diese der Öffentlichkeit dauerhaft erhalten bleiben (*dépot légal*)[294]. Art. 21 RTVG «trägt der bedeutenden Rolle von Radio und Fernsehen für die gesellschaftliche Entwicklung Rechnung»[295]. Dabei wird vor allem den Sendungen der öffentlichen Programmveranstalter eine «hohe und dauerhafte politische, kulturelle und historisch-wissenschaftliche Bedeutung»[296] zugemessen. Die SRG hat sich bereits vor dieser gesetzlichen Verpflichtung um den Erhalt historisch bedeutender Informationssendungen bemüht und wird durch den Verein Memoriav, das Schweizerische Bundesarchiv (BAR), die Schweizerische Landesphonothek und die Schweizerische Landesbibliothek unterstützt[297]. Die privaten Veranstalter verfügen über keine mit jener der SRG vergleichbaren Archivstrategie. Ursächlich dafür sind primär die Kosten für eine professionelle Archivierung. Die systematische und professionelle Auswahl sowie der langfristige Erhalt von Sendungen durch Private erfordert daher eine öffentliche Unterstützung[298]. Das Gesetz sieht in Art. 21 Abs. 1 Satz 2 RTVG im Gegensatz zur alten Version (Art. 69 Abs. 3 RTVG vom 24. März 2006) eine Entschädigung für den Aufwand zur Erhaltung der Programme vor, die nach Art. 21

---

291 BBl 2003 III 1684.
292 BBl 2003 III 1684 f.
293 WEBER, Rundfunkrecht, Art. 20 RTVG, Rn. 8.
294 BBl 2003 III 1685.
295 BBl 2003 III 1685.
296 BBl 2003 III 1685.
297 BBl 2003 III 1685.
298 BBl 2003 III 1685 f.

Abs. 3 RTVG hauptsächlich aus dem Ertrag für die Einsichtnahme und die Weiterverbreitung der Inhalte sowie gemäss Art. 22 RTVG aus dem Konzessionsertrag finanziert werden soll. Ergänzend ist eine Finanzierung aus allgemeinen Bundesmitteln vorgesehen. Darüber hinaus kann der Bundesrat für die Erhaltung der Lesegeräte nach Art. 21 Abs. 4 RTVG Unterstützungsmassnahmen treffen. Der Erfolg dieser Strategie hinsichtlich des langfristigen Erhalts der Daten und den dadurch entstehenden Kosten kann zum jetzigen Zeitpunkt nicht beurteilt werden.

4. Arbeitsrecht

Im Bereich des Arbeitsrechts weist das Konkurrenzverbot nach Art. 340 ff. OR in Art. 340a Abs. 1 OR einen expliziten Zeitbezug auf, indem eine grundsätzliche Beschränkung des Verbots auf drei Jahre vorgesehen ist, die nur unter besonderen Umständen überschritten werden darf. Die Konkurrenzabrede zwischen Arbeitgeber und Arbeitnehmer soll vermeiden, dass der Arbeitnehmer den ehemaligen Arbeitgeber unter Ausnutzung bestimmter im Arbeitsverhältnis erworbener Kenntnisse schädigt[299]. Dem Schutzinteresse des Arbeitgebers steht das Interesse des Arbeitnehmers an der Möglichkeit einer uneingeschränkten beruflichen Entfaltung entgegen[300]. Aufgrund der zentralen Bedeutung einer freien Berufswahl des Arbeitnehmers untersagt Art. 340a OR nicht erst die komplette Aufhebung der wirtschaftlichen Entscheidungsfreiheit, sondern bereits eine unbillige Erschwerung des wirtschaftlichen Fortkommens[301]. Generelle Voraussetzung für ein Konkurrenzverbot ist gemäss Art. 340 Abs. 2 OR, dass das Arbeitsverhältnis dem Arbeitnehmer Einblick in den Kundenkreis[302] oder in Fabrikations- und Geschäftsgeheimnisse[303] gewährt hat und die Verwendung dieser Kenntnisse den Arbeitgeber erheblich schädigen könnte[304].

Die in Art. 340a Abs. 1 OR geforderten besonderen Umstände liegen bereits in der Art der zu schützenden Kenntnisse, weitere Besonderheiten müssen nicht gegeben sein[305]. Bei einer Überschreitung der in Art. 340a Abs. 1 Satz 2 OR festgelegten Dauer des Konkurrenzverbots von drei Jahren stellt das Gesetz die Vermutung einer unangemes-

---

299 NEERACHER, 3.

300 PORTMANN, in: Vogt/Honsell/Wiegand, Art. 340a N 1 ff.; NEERACHER, 4; ausserhalb des Arbeitsrechts stehen der Beschränkung der Wettbewerbsfreiheit einer Partei die Wirtschaftsfreiheit nach Art. 27 BV und der Schutz der Persönlichkeit vor übermässiger Bindung nach Art. 27 ZGB entgegen; siehe zum Prinzip des freien Wettbewerbs BGE 82 II 302; BGE 86 II 376.

301 PORTMANN, in: Vogt/Honsell/Wiegand, Art. 340a N 4; Neeracher, 4; BGE 95 II 535.

302 Siehe dazu NEERACHER, 20 ff.

303 Siehe dazu NEERACHER, 27 ff.

304 Siehe dazu NEERACHER, 31 ff.

305 NEERACHER, Fn. 336.

senen Abrede auf. Auch kürzere Abreden können unangemessen sein[306]. Das entscheidende Kriterium zur Festsetzung der Höchstdauer kann und darf einzig die Art der zu schützenden Kenntnis sein[307], da sich das Konkurrenzverbot auf die wettbewerbsrelevante Wirkung dieser Kenntnis stützt[308]. Im Resultat orientiert sich die Grenze der vertraglichen Bindung in zeitlicher Hinsicht an der Information.

5. Verjährung im Besonderen

5.1 Konzeption

Das Institut der Verjährung geht auf das spätere römische Recht und die jüngere Zeit zurück[309]. Zwei wesentliche Zwecke der Verjährung liegen in der Gewährleistung des Rechtsfriedens und der Rechtssicherheit der Beteiligten[310]. Dem gleichen Zweck dienen die Regeln über die Ersitzung von Grundstücken in Art. 661 f. ZGB, von beweglichen Sachen gemäss Art. 728 ZGB sowie die Begrenzung des Rückforderungsrechts gemäss Art. 934 ZGB[311]. Die Ersitzung soll ein anhaltendes Auseinanderfallen von Besitz und Eigentum sowie eine daraus hervorgehende Rechtsunsicherheit vermeiden[312]. Im Privatrecht soll die Verjährung im Wesentlichen den Schuldner nach einer gewissen Zeit von der Ungewissheit über die Geltendmachung einer Forderung durch den Gläubiger befreien[313]. Im Weiteren trägt die Verjährung zur Vermeidung von zeitlich bedingten Beweisschwierigkeiten bei, die zu aufwendigen Beweisverfahren und Fehlurteilen führen können[314].

---

306 NEERACHER, 52.

307 BRÜHWILER, Art. 340a OR N2.

308 NEERACHER, 52. Der Einblick in Geschäftsgeheimnisse rechtfertigt im Allgemeinen längere Fristen als der Einblick in den Kundenkreis, BGE 91 II 381. Die wettbewerbsrelevante Wirkung liegt insbesondere in der Gefahr des Kundenverlusts; siehe dazu PORTMANN, in: Vogt/Honsell/Wiegand, Art. 340a N 3.

309 PETER, Obligationenrecht, 137 ff.

310 BGE 90 II 437; BGE 137 III 18; siehe u.a. GAUCH/SCHLUEP/EMMENEGGER, Rn. 3279; DÄPPEN, in: Vogt/Honsell/Wiegand, Vor Art. 127-142 N 1; THOUVENIN/PURTSCHERT, in: Huguenin/Hilty, Vor Art. 148-162 N 1; siehe ferner KILLIAS, 54, wonach es sich kein Rechtssystem leisten könne, allfällig besseren Rechtsansprüchen beliebig lange die Durchsetzung zu erhalten.

311 Bei Kulturgütern beträgt die absolute Frist gemäss Art. 728 Abs. 1bis bzw. Art. 934 Abs. 1bis OR nicht fünf, sondern 30 Jahre; siehe dazu SIEGFRIED, 76.

312 HAUSMANINGER/SELB, 153.

313 HUGUENIN/THOUVENIN, 304, m.w.H.; BGE 90 II 437 f.; BGE 134 III 297.

314 GAUCH/SCHLUEP/EMMENEGGER, Rn. 3280; BGE 90 II 437 f.; siehe auch CHOU, Rn. 470 f., der die Verjährungsbestimmungen in einen Zusammenhang mit dem menschlichen Erinnerungsvermögen stellt.

Die Verjährung bezieht sich im Privatrecht auf die Geltendmachung vertraglicher, bereicherungsrechtlicher und deliktischer Ansprüchen[315]. Die Verjährung vertraglicher Ansprüche ist grundsätzlich in Art. 127 ff. OR geregelt und die ordentliche Verjährungsfrist beträgt nach Art. 127 OR zehn Jahre. Bei den bereicherungsrechtlichen Ansprüchen gelten nach Art. 67 Abs. 1 OR eine relative Frist von einem Jahr und eine absolute Frist von 10 Jahren. Die relative Frist knüpft an die Kenntnis des Verletzten an. Die gleiche Regelung findet sich in Art. 60 Abs. 1 OR für deliktische Ansprüche[316]. Eine abweichende absolute Frist von 30 Jahren findet sich in Art. 9 Abs. 4 des Bundesgesetzes über den internationalen Kulturgütertransfer (KGTG)[317]. Im Strafrecht wird zwischen der Verfolgungs- und der Vollstreckungsverjährung unterschieden (Art. 97 und 99 StGB). Bei der Verfolgungsverjährung orientiert sich die Frist gemäss Art. 97 Abs. 1 StGB an der Dauer der für die Tat angedrohten Höchststrafe. Bei der Vollstreckungsverjährung sind gemäss Art. 99 Abs. 1 StGB Art und Dauer der tatsächlich ausgesprochenen Strafe massgeblich. Die Verjährung tritt in beiden Fällen nach längstens 30 Jahren ein.

5.2 Entwicklung

a) Tendenzen zur Verlängerung

Im Bereich der strafrechtlichen Verjährung haben sich während der letzten zwanzig Jahre die Forderungen verstärkt, die Verjährung als Ganzes abzuschaffen oder die Fristen stark zu verlängern[318]. Nebst den Entwicklungen in der Schweiz und Europa gerät die Verjährung auch durch den Einfluss des amerikanischen Rechtsdenkens unter Druck. Bereits der Streit um die nachrichtenlosen Vermögen[319] kann als «Kulturschock» zwischen der kontinentaleuropäischen Perspektive über die Verjährung zivilrechtlicher Ansprüche und der amerikanischen Sichtweise über deren Unverjährbarkeit gewertet werden[320]. Im Weiteren sieht auch der Entwurf für einen neuen allgemeinen Teil des OR (OR 2020) teilweise eine Verlängerung der Verjährungsfristen vor. Im Zivilrecht soll die relative Frist gemäss Art. 149 Abs. 1 OR 2020 neu 3 Jahre betragen. Die absolute Frist von 10 Jahren bleibt gemäss Art. 149 Abs. 2 OR 2020 im Rahmen

315 Kritisch zu dieser Ausgestaltung im Rahmen eines Vorschlags zur Neukonzeption HUGUENIN/THOUVENIN, 322.

316 Siehe zu den zahlreichen weiteren Sondernormen HUGUENIN/THOUVENIN, 307 ff.

317 Siehe dazu SIEGFRIED, 26.

318 KILLIAS, 56, mit Verweis auf die Verjährungsinitiative in der Schweiz, die in der Volksabstimmung vom 30. November 2008 angenommen wurde. Der Verfassungstext wurde in Art. 101 Abs. 1 lit. e StGB umgesetzt.

319 Siehe dazu vorne A.I.2.3 a).

320 KILLIAS, 57.

eines zweistufigen Systems erhalten[321]. Als Ausnahme innerhalb eines einheitlichen Fristenregimes ist für Körper- und Umweltschäden in Art. 150 OR 2020 ausschliesslich «eine relative, subjektiv anknüpfende Frist von 3 Jahren» vorgesehen[322]. Die in Art. 151 OR 2020 generell vorgesehene Höchstfrist von 30 Jahren soll indessen auch hier gelten[323]. Auch diese verlängerte Frist wird bestimmte Schäden mit äusserst langen Latenzzeiten wohl nicht zu erfassen vermögen[324]. Im Fall eines Asbestopfers hat der EGMR Anfang 2014 diesbezüglich festgestellt, dass die Revisionsbestrebungen im schweizerischen Recht zu keiner gerechten Lösung des Problems führen werden[325].

b) Bewertung

Die Verjährung dient primär dem Schutz der Rechtssubjekte, nach einer bestimmten Zeit nicht mehr belangt zu werden. Diese Gewissheit erlaubt insbesondere auch die Entsorgung von älteren Akten, deren mögliche Relevanz in einem künftigen Verfahren ohne die Verjährung nicht abschliessend beurteilt werden kann[326]. Der Entfall der zivil- und strafrechtlichen Verjährung wäre für die Archivierung eine grosse Herausforderung[327], da dann die Erhaltung von Unterlagen über potentiell rechtsrelevante Tatsachen auch über die gesetzlichen Aufbewahrungsfristen hinaus sichergestellt werden müsste. Hinzu kommt, dass sich die Massstäbe zum adäquaten Verhalten über die Zeit entscheidend verschieben können. Wer erst spät für ein früheres Verhalten zur Rechenschaft gezogen wird, droht an Massstäben gemessen zu werden, die zur damaligen Zeit eine gänzlich andere Bedeutung hatten[328]. Im Weiteren erscheint eine Verlängerung der Verjährungsfristen auch im Hinblick auf die Prozessökonomie als problematisch, da

---

321 THOUVENIN/PURTSCHERT, in: Huguenin/Hilty, Art. 149 N 2.

322 THOUVENIN/PURTSCHERT, in: Huguenin/Hilty, Art. 149 N 4.

323 THOUVENIN/PURTSCHERT, in: Huguenin/Hilty, Vor Art. 148-162 N 13. Für Körper- und/oder Umweltschäden bestehen im deutschen und im französischen Recht bereits längere Fristen: In Deutschland beträgt die Frist für Schadenersatzansprüche aus der Verletzung von Leben, Körper, Gesundheit und Freiheit gemäss § 199 Abs. 2 BGB 30 Jahre; in Frankreich gilt gemäss Art. L 152.-1 Code de l'Environnement eine Frist von 30 Jahren für Schadenersatzansprüche bei Umweltschäden; siehe eingehend THOUVENIN/PURTSCHERT, in: Huguenin/Hilty Art. 150 N 1 ff., Art. 151 N 1 ff.

324 THOUVENIN/PURTSCHERT, in: Huguenin/Hilty, Art. 150 N 10.

325 EGMR vom 11. März 2014, Nr. 52067/10 und 41072/11, E. 75. KILLIAS, 67, schlägt als mögliche Alternative zur Verlängerung der Verjährungsfrist im Umgang mit Langzeitfolgen die Schaffung einer Art «Sozialversicherung» vor, die eine Entschädigung unabhängig von jeglichen persönlichen Schuldvorwürfen ermöglichen soll. Die Finanzierung könnte durch obligatorische Einzahlungen in einen Fonds erfolgen.

326 Ähnlich KILLIAS, 61.

327 KILLIAS, 61.

328 KILLIAS, 63 f.; vgl. zur zeitlich differenzierten Festlegung des Kenntnisstandes im Zusammenhang mit Asbest BGE 140 II 11 ff.

die Gerichte nicht mehr unter Druck stehen, Verfahren rasch abzuschliessen, um der Verjährung zuvorzukommen[329].

Insgesamt ist vor dem Hintergrund des kürzlich ergangenen EGMR-Urteils zum jetzigen Zeitpunkt nicht von einer grossflächigen Tendenz zur Unverjährbarkeit auszugehen. In Bereichen, wo gravierende Spätfolgen auftreten können, steht die Höchstfrist jedoch in Frage. Dem Urteil des EGMR, wonach die Revisionsbestrebungen zu keiner gerechten Lösung des Problems führen würden, ist unter alleiniger Bezugnahme auf die ausgleichende Gerechtigkeit, die für erlittene Schäden einen vollen Ausgleich fordert, zuzustimmen[330]. Aus einer zeitlichen Perspektive ist aber nebst den praktischen Problemen im Umgang mit lange zurückliegenden Schäden auch anzuerkennen, dass das Interesse am Rechtsfrieden und an der Rechtssicherheit als zentrale Aspekte der Verjährung die Forderung nach der ausgleichenden Gerechtigkeit irgendwann wieder zu überwiegen vermögen.

Anhand des Konflikts um die nachrichtenlosen Vermögen lässt sich aufzeigen, dass die vermeintliche Gewissheit über die fehlende Relevanz von Daten nicht nur deren Vernichtung, sondern – zumindest solange die Unkenntnis über die Relevanz besteht – auch deren Erhalt begünstigen kann. Eine Vernichtung historischer Dokumente, für die keine gesetzliche Aufbewahrungspflicht mehr besteht, erscheint als wesentlich drängender, wenn die Gefahr juristischer Konsequenzen gegeben ist.

6. Fazit

Die Rahmenbedingungen zum Informationsmanagement dienen insgesamt nicht nur Zwecken unter Privaten. Ein wesentlicher Zweck des Staates besteht in der Gewährleistung von Sicherheit. Dazu gehören nicht nur Sicherheit und Ordnung in einem polizeirechtlichen Sinn, sondern auch die soziale Sicherheit und die Wohlfahrt. Die Vorgaben über die Bearbeitung personenbezogener Daten durch Private sind für den Staat ein Mittel zur Erreichung dieses Zwecks[331]. Im nicht polizeilichen Bereich dient beispielsweise die Rechnungslegung insbesondere steuerrechtlichen Zwecken und damit dem Ziel der Wohlfahrt. Die Vorschriften zur Datenspeicherung in der Fernmeldegesetzge-

329 KILLIAS, 58, mit Verweis auf den sprunghaften Anstieg der Dauer von Rechtsmittelverfahren um 50 Prozent im Jahr 2002 nach jahrzehntelanger relativer Stabilität. Im Zuge der Revision des StGB-AT wurde u.a. die Regel eingeführt, dass nach einem erstinstanzlichen Urteil Straftaten grundsätzlich nicht mehr verjähren (Art. 97 Abs. 3 StGB). Die Verjährung ist nun auch für Vergehen auf 10 Jahre angehoben worden (Art. 97 Abs. 1 lit. c StGB). Siehe zur Prozessökonomie im Sinne einer Entlastung der Gerichte durch weniger aufwendige Beweisverfahren HUGUENIN/THOUVENIN, 304.

330 Siehe zur Gerechtigkeit ZIPPELIUS, 35 ff.

331 VON LEWINSKI, 201.

bung sind dagegen sicherheitspolitisch motiviert. In zeitlicher Hinsicht entfällt der Rechtfertigungsgrund einer gesetzlichen und explizit zeitbezogenen Grundlage gemäss Art. 28 Abs. 2 ZGB bzw. Art. 13 Abs. 1 DSG, sobald die gesetzliche Aufbewahrungspflicht erfüllt ist.

II. Implizit zeitbezogene Normen

1. Persönlichkeitsrecht

1.1 Konzeption

Der Persönlichkeitsschutz greift sowohl auf der Ebene des öffentlichen Rechts als auch auf der Ebene des Privatrechts[332]. Die verfassungsrechtliche Seite des Persönlichkeitsschutzes bildet das Recht auf persönliche Freiheit gemäss Art. 10 Abs. 2 BV[333]. Wo keine Beziehung zwischen Bürger und Staat betroffen ist, kommt der privatrechtliche Persönlichkeitsschutz zur Anwendung[334]. Die Abgrenzung von öffentlich-rechtlichen und privatrechtlichen Verhältnissen kann sich im Einzelfall schwierig gestalten[335], ist jedoch relevant, da in einem öffentlich-rechtlichen Verhältnis der privatrechtliche Persönlichkeitsschutz nicht greift[336]. Im Bereich der Verfassungsrechte ergibt sich ein Spannungsverhältnis mit der ebenfalls geschützten Meinungsäusserungsfreiheit, die in Art. 16 BV allgemein und in Art. 17 BV durch die Presse- sowie in Art. 20 und 21 BV in Form der Wissenschafts- und Kunstfreiheit geschützt ist. Eine Konkretisierung der Konzeption des Privatlebens erfordert die Güterabwägung zwischen den individuellen Schutzinteressen und den öffentlichen Interessen an Transparenz[337]. Gemäss Art. 35 Abs. 3 BV[338] sind die verfassungsrechtlichen Garantien im Rahmen der indirekten

---

332 Zur Notwendigkeit und Natur der Unterscheidung zwischen privatrechtlichem und verfassungsrechtlichem Persönlichkeitsschutz siehe BASTON-VOGT, 115 ff.

333 Das Bundesgericht hat den Schutzbereich in BGE 127 I 6 folgendermassen konkretisiert: «Die persönliche Freiheit im Sinne von Art. 10 Abs. 2 BV stellt [...] eine Grundgarantie zum Schutze der Persönlichkeit dar. Sie umfasst [...] all jene Freiheiten, die elementare Erscheinungen der Persönlichkeitsentfaltung darstellen und ein Mindestmass an persönlicher Entfaltungsmöglichkeit erlauben. Was im Einzelnen dazugezählt werden kann, ist im Einzelfall unter Auslegung und Fortbildung des Verfassungstextes zu entscheiden». Der Gedanke eines ungeschriebenen und umfassenden Rechts auf persönliche Freiheit hat sich mit BGE 90 I 34 ff. durchgesetzt; siehe dazu PEDRAZZINI/OBERHOLZER, 115.

334 HAUSHEER/AEBI-MÜLLER, Rz. 10.34.

335 Siehe die Beispiele bei HAUSHEER/AEBI-MÜLLER, Rz. 10.36 ff.

336 BGE 98 Ia 521.

337 WEBER, Grundrechtskonzeptionen, 13.

338 Vgl. dazu BBl 1997 I 191 ff.

Drittwirkung auch unter Privaten wirksam[339]. Obwohl die wesentlichen Schutzgüter der Persönlichkeit gegen Eingriffe durch Private ebenso zu bewahren sind, wie gegen staatliche, besteht hinsichtlich der Legitimation von Eingriffen in den Schutzbereich der persönlichen Freiheit ein bedeutender Unterschied zwischen der verfassungsrechtlichen und der privatrechtlichen Ebene. Der Staat ist an das Legalitätsprinzip gebunden und das staatliche Interesse ist auf die Erfüllung der an den Staat übertragenen Aufgaben beschränkt[340].

Die Rechtsfolgen einer Persönlichkeitsverletzung sind in Art. 28a ZGB geregelt. Sofern kein Rechtfertigungsgrund besteht, bleibt eine Verletzung widerrechtlich und der Betroffene kann die entsprechenden Rechtsbehelfe des Persönlichkeitsschutzes ergreifen. Passivlegitimiert sind nach dem Wortlaut von Art. 28 Abs. 1 ZGB alle, die an der Verletzung mitwirken, d.h. Allein- und Mittäter, Anstifter sowie Gehilfen[341]. Aktivlegitimiert ist gemäss Art. 28 Abs. 1 ZGB jede Person, die direkt, unmittelbar und persönlich von der Verletzung betroffen ist[342]. Das Bundesgericht hat eingehend dargelegt, dass der allgemeine Persönlichkeitsschutz grundsätzlich auch den juristischen Personen zusteht[343]. Das Persönlichkeitsrecht der juristischen Person findet gemäss Art. 53 ZGB allerdings dort seine Grenze, wo die darin enthaltenen Ansprüche Eigenschaften voraussetzen, die ihrem Wesen nach nur den natürlichen Personen zukommen.

1.2 Entwicklung

Im Privatrecht enthielt bereits das Obligationenrecht von 1881 den Schutz vor Verletzungen der persönlichen Verhältnisse und die damit verbundenen Rechtsfolgen[344]. Eine eigenständige Stellung erhielt das Persönlichkeitsrecht jedoch erst durch die Neuregelung im ZGB von 1907. Die seit der Revision von 1985 geltende Fassung ist jene in

339 Siehe SALADIN, 373 ff; HAUSHEER/AEBI-MÜLLER, Rz. 10.34; AUER/MALINVERNI/HOTTELIER, Rn. 124 ff.; grundlegend BGE 111 II 253 ff; siehe auch BGE 118 Ia 56; BGE 116 IV 40; BGE 101 IV 172; siehe ferner BGE 120 II 225, in dem das Bundesgericht feststellte, dass die Kunstfreiheit – damals Teil der Meinungsäusserungsfreiheit – als Rechtfertigungsgrund für eine Persönlichkeitsverletzung dienen könne.

340 Siehe Art. 36 Abs. 1 BV; BGE 118 Ia 73. Siehe ferner FORSTMOSER, 5 f., wonach man sich beim DSG von Beginn weg bewusst war, dass der Ansatz im privaten Bereich von jenem im öffentlichen Bereich wird abweichen müssen: Im Privatrecht ist erlaubt, was nicht verboten ist, öffentliche Stellen müssen sich dagegen auf eine gesetzliche Grundlage stützen können – das gilt auch für die Datenbearbeitung. Siehe für dahingehende Überlegungen in den Anfängen des deutschen Datenschutzrechts STEINMÜLLER et al., 59, 144.

341 AEBI-MÜLLER, Rn. 281; BGE 131 III 29; BBl 1982 II 656 f.

342 TERCIER, Rn. 799.

343 BGE 95 II 488; vgl. auch BGE 96 IV 148, wonach die juristischen Personen den strafrechtlichen Ehrenschutz beanspruchen können.

344 Art. 50 und 55 aOR sind die Vorgänger von Art. 41 und 49 des geltenden OR, PEDRAZZINI/OBERHOLZER, 115.

Art. 28 ZGB[345]. Es handelt sich dabei um eine Generalklausel, eine abstrakte und umfassende Beschreibung der Persönlichkeit ist nicht möglich[346]. Annäherungsweise können Persönlichkeitsrechte als jene subjektiven Rechte umschrieben werden, die dem Menschen um seiner selbst willen zustehen und «untrennbar mit seiner Person verknüpft» sind[347]. Die Rechtsprechung hat den Inhalt des Persönlichkeitsschutzes gemäss Art. 28 ZGB durch die Beurteilung im Einzelfall zu bestimmen[348]. Ein wesentlicher Vorteil der Generalklausel liegt in den flexiblen Anpassungsmöglichkeiten an veränderte Umstände im Allgemeinen und an technologische Entwicklungen im Speziellen. Dieser Vorteil bringt gleichzeitig den Nachteil einer gewissen Rechtsunsicherheit mit sich, wenn die Rechtsprechung für neue Probleme noch keine Lösungen formuliert hat[349]. Ausführungen zu einzelnen Schutzgütern können beispielhaft erfolgen und gegebenenfalls zur Rechtssicherheit beitragen[350]. Die Unmöglichkeit einer objektiven Umschreibung persönlichkeitsrechtlicher Informationsschranken hat zu einer Aufteilung in einzelne Sachverhalte geführt, die zumindest eine objektive Zuteilung ermöglichen[351]. So entstanden einzelne Fallgruppen wie das Recht auf einen eigenen Namen, auf geistige und körperliche Unversehrtheit, auf Freiheit, auf Privat- und Intimsphäre und auf Ehre[352]. Diese beispielhafte Konkretisierung trägt entscheidend zur Rechtssicherheit bei und macht die Persönlichkeitsgüter für das Rechtssubjekt erkennbar[353].

1.3 Zeitliche Dimension im Allgemeinen

a) Vorbemerkungen

Die folgende Darstellung über die zeitliche Dimension der Persönlichkeitsrechte umfasst eine Auswahl an Aspekten des Persönlichkeitsrechts, die in einem zeitlichen Zusammenhang als relevant erscheinen. Die zeitliche Dimension tritt hierbei unterschiedlich stark hervor. Deutlich erkennbar ist sie beim Schutz vor übermässiger Bindung nach Art. 27 ZGB. Diese Bestimmung trägt der Freiheit als fundamentalem Grundsatz

345 Siehe zur Revision BBl 1982 II 636 ff.

346 BRÜCKNER Rn. 380; PEDRAZZINI/OBERHOLZER, 116, 132.

347 BGE 84 II 573.

348 BGE 95 II 492; siehe für eine Übersicht zur älteren Rechtsprechung SCHMID, 813 ff.

349 BUCHER, Persönlichkeitsschutz, Rn. 436.

350 HAUSHEER/AEBI-MÜLLER, Rz. 12.40.

351 DRUEY, Information, 359; PEDRAZZINI/OBERHOLZER, 132 ff., weisen darauf hin, dass auch die Kategorisierung in Abhängigkeit zu den jeweiligen Sichtweisen und Gegebenheiten steht. Wesentlich sei dagegen, dass Art. 28 ZGB das Schutzobjekt der Persönlichkeit nicht begrenze.

352 RIEMER, Personenrecht, Rn. 293.

353 PEDRAZZINI/OBERHOLZER, 133.

des schweizerischen Privatrechts Rechnung und wahrt die Autonomie des Einzelnen[354]. Bei den weiteren Schutzgütern des Persönlichkeitsrechts tritt der Zeitbezug weniger deutlich hervor. Der Zeitbezug besteht hier in der Regelung des Erhalts (Speicherung) und der Verbreitung (Verwertung) persönlichkeitsrelevanter Schutzgüter. Hierzu gehören insbesondere Informationen, die der Privatsphäre zuzuordnen sind, das Recht am eigenen Bild, an der eigenen Stimme, am eigenen Namen und der Schutz der Ehre. Diese wie sämtliche Aspekte des Persönlichkeitsrechts sind insofern zeitbezogen, als dass der Rechtsordnung im Hinblick auf die Persönlichkeit des Menschen die Einsicht zu Grunde liegt, dass der Mensch «einer eigenen Berufung fähig ist, die in der Verwirklichung des eigenen Ichs besteht, und dass er deswegen den Anspruch erhebt, personal leben zu dürfen, d.h. in einer Art und Weise, die diesen Vollzug des eigenen Ichs erlaubt»[355]. Die Begriffe «Verwirklichung» und «Vollzug» deuten an, dass die Entfaltung der persönlichen Freiheit als Schutzgegenstand eines zeitlichen Kontinuums bedarf, das vor übermässigen Beeinträchtigungen durch die Rechtsordnung zu schützen ist.

b) Zeitbezug der Persönlichkeitsrechte

(1) Schutz vor übermässiger Bindung

Im Unterschied zu Art. 28 ZBG, der die Persönlichkeit vor Angriffen durch Dritte schützt, beschränkt Art. 27 ZGB die Möglichkeiten der Selbstbindung bzw. die Entäusserung von Persönlichkeitsgütern in der Interaktion mit Dritten[356]. Dadurch wahrt Art. 27 ZGB die Entscheidungsfreiheit und damit die Grundlage für die zukünftige Entfaltung der Persönlichkeit[357]. Die in Art. 27 ZGB umrissenen Schranken implizieren gleichzeitig der Verfügung zugängliche Teilbereiche der Persönlichkeit, so beispielsweise die Einwilligung zur Verwendung eines Bildes für Werbezwecke mittels Lizenzvertrag, den Abschluss eines Arbeitsvertrages etc.[358]. Ein Aspekt der persönlichen Freiheit besteht dabei gerade darin, auch verbindlich auf die Ausübung von eigenen Rechten verzichten zu können. Das Eingehen eines Arbeitsverhältnisses beinhaltet

354 PEDRAZZINI/OBERHOLZER, 118 f.; BRÜCKNER, Rn. 765

355 PEDRAZZINI/OBERHOLZER, 113.

356 PEDRAZZINI/OBERHOLZER, 119 f., Art. 27 schützt natürliche und juristische Personen vor übermässiger Selbstbindung. Die bundesgerichtliche Rechtsprechung bezieht den Schutz für juristische Personen in BGE 114 II 162 und BGE 106 II 377 ff. allerdings nur auf die wirtschaftliche Bewegungsfreiheit; BRÜCKNER, Rn. 765, hält die Formulierung «Schutz der Persönlichkeit vor sich selber» als verfehlt und verweist darauf, dass auch Art. 27 ZGB den Schutz vor Dritten zum Ziel habe; so auch TERCIER, Rn. 143.

357 AEBI-MÜLLER, Rn. 12; JÄGGI, 199a f.

358 AEBI-MÜLLER, Rn. 13.

grundsätzlich den Verzicht, während der Arbeitszeit eigenen Interessen nachzugehen[359]. Der Grundsatz *pacta sunt servanda* findet seine Grenze im Schutzbereich der persönlichen Freiheit[360].

Das Übermass einer Bindung kann sich aus dem Gegenstand der Bindung bzw. aus deren Dauer oder aus der Kombination dieser Faktoren ergeben[361]. Einerseits kann eine an sich unproblematische Bindung durch ihre Dauer übermässig werden, andererseits kann eine im Hinblick auf die Dauer problemlose Bindung durch den Gegenstand der Beeinträchtigung unzulässig sein[362]. Eine übermässige Einschränkung der Selbstbestimmung wirkt sich nur dann aus, wenn der Betroffene sich darauf beruft[363]. Bindungen, die den Kernbereich einer Person betreffen und aufgrund ihres Inhalts nicht Gegenstand vertraglicher Verpflichtungen sein können, sind dagegen von Beginn weg ungültig[364]. So kann beispielsweise nicht gültig in die Tötung oder in eine offensichtlich nicht medizinisch angezeigte Behandlung mit gesundheitsschädigenden Folgen eingewilligt werden[365]. In zeitlicher Hinsicht sind solche unzulässigen Vertragsgegenstände durch ihre Irreversibilität gekennzeichnet.

(2) Schutz vor Persönlichkeitsverletzungen

In Bezug auf die Bearbeitung personenbezogener Daten erscheint hauptsächlich der *Schutz der Privatsphäre* als vom Persönlichkeitsrecht geschütztes Gut relevant. In der Lehre und Rechtsprechung kommt häufig die sog. Sphärentheorie zur Anwendung, die eine Trennung in eine geheime, eine private und eine öffentliche Sphäre vorsieht[366]. Die Privatsphäre umfasst grundsätzlich jene Lebensbereiche, die nur mit einem be-

359 LEU/VON DER CRONE, 222.

360 LEU/VON DER CRONE, 223; nach BRÜCKNER, Rn. 765 stellt nicht die Verpflichtung an sich eine Verletzung dar, sondern das Beharren des Vertragspartners auf Einhaltung.

361 LEU/VON DER CRONE, 224; BUCHER, Persönlichkeitsschutz, Rn. 402 ff., ergänzt zur Dauer das Kriterium der Intensität, wobei damit wohl das Ausmass der Beeinträchtigung der persönlichen Freiheit gemeint ist. Die Intensität kann aber auch aus der Kombination von Dauer und Gegenstand resultieren.

362 LEU/VON DER CRONE, 223.

363 BGE 129 III 214; HAUSHEER, 340 f.

364 BGE 129 III 213 f.; AEBI-MÜLLER, Rn. 221, weist darauf hin, dass Vertragsgegenstände die aufgrund ihres Inhalts nach objektiven Punkten als sittenwidrig zu qualifizieren sind (beispielsweise die Verpflichtung zur Begehung einer Straftat) nicht in Anwendung von Art. 27 ZGB, sondern nach Art. 20 OR zu lösen seien; siehe zum Ganzen HAUSHEER, 340 f.

365 GEISER, Zwangsmassnahmen, 231, m.w.H.

366 BGE 97 II 100 f., BGE 109 II 357; BGE 118 IV 45; siehe dazu auch RIEMER, Personenrecht, Rn. 351 ff.; WEBER, Schutz, 69 ff.; VESTING, 175. Die Idee wurde in der Habilitation von HUBMANN, Persönlichkeitsrecht, 268 ff., erstmals dargestellt.

stimmten Kreis von relativ nahestehenden Personen geteilt werden[367]. Indessen soll der Schutzbereich von Art. 28 ZGB auch dort wirken, wo Tatsachen des Privatlebens mit Personen geteilt werden, die nicht dem Freundes- oder Bekanntenkreis zugehören[368]. Das Recht auf Achtung der Privatsphäre soll verhindern, dass jede private Lebensäusserung, die in der Öffentlichkeit stattfindet, der Allgemeinheit zugänglich wird[369]. Zusammenfassend besteht die Privatsphäre als Teil des Persönlichkeitsschutzes in der Macht, darüber zu bestimmen, was andere über ein Individuum in Erfahrung bringen können[370]. Nebst dieser informationellen Seite besteht auch eine physische Seite der Privatsphäre, die den Zugang zu einer Person umfasst und es Individuen erlaubt, zu bestimmen, für wen sie durch Sinneswahrnehmung in Form von Beobachtung oder Körperkontakt zugänglich sein wollen[371]. Von der durch Art. 28 ZGB geschützten Privatsphäre ist die Gemeinsphäre zu unterscheiden, die alle persönlichen Tatsachen umfasst, die jedermann zugänglich sind und entsprechend nicht zum Schutzbereich von Art. 28 ZGB gehören. Die Unterscheidung gründet auf objektiven Kriterien, jedoch ist sie nicht für jede Person gleich[372]. Der Umfang des Gemeinbereichs ist von den Umständen abhängig und die öffentliche Zugänglichkeit einer Information impliziert nicht ihre uneingeschränkte Verbreitung[373]. Die Abgrenzung zwischen Privat- und Gemeinsphäre kann sich über die Zeit verändern und eine Information, die dem Gemeinbereich zugeordnet wurde, kann in Vergessenheit geraten und in den Privatbereich der betroffenen Person übergegangen sein[374].

---

367 Siehe BGE 97 II 97 ff., 101; BRÜCKNER, Rn. 484; PEDRAZZINI/OBERHOLZER, 138;

368 BUCHER, Persönlichkeitsschutz, Rn. 453. Nach hier vertretener Auffassung ist dabei die individuell zugemessene Schutzwürdigkeit einer Information massgebend.

369 BÄCHLI, 43.

370 Vgl. KATSH, 228; siehe auch WESTIN, Privacy, 7, der die Privatsphäre als Anspruch definiert, wonach Individuen, Gruppen oder Institutionen darüber bestimmen können, wann, wie und in welchem Umfang Informationen über sie an andere weitergegeben werden; ALTMAN, 18, definiert die Privatsphäre aus psychologischer Sicht als selektive Kontrolle über den Zugang zum Selbst oder zur Gruppe.

371 DECEW, 76 f.; ALTMAN, 6, sieht die zentrale Rolle der Privatsphäre in einem interpersonalen Grenzprozess, anhand dem eine Person oder eine Gruppe ihre Interaktion mit Dritten steuert.

372 BUCHER, Persönlichkeitsschutz, Rn. 457, mit Hinweis auf die Unterscheidung einer absoluten und einer relativen Person der Zeitgeschichte in BGE 127 III 481 ff., 488 ff.

373 BUCHER, Persönlichkeitsschutz, Rn. 458, mit Verweis auf die Verbreitung durch Zeitungen; siehe auch die Formulierung bei BRÜCKNER, Rn. 485, wonach die Gemeinsphäre die Tatsachen umfasst, «die jedermann zugänglich sind und auch zugänglich sein sollen».

374 BUCHER, Persönlichkeitsschutz, Rn. 459; ALTMAN, 11, 23 ff.

Die Schwächen der Sphärentheorie wurden in der Literatur umfassend erörtert[375]. Ein zentrales Problem besteht in der ergebnisorientierten Anknüpfung am Ausschluss Dritter (geheim, privat, öffentlich), die sich nicht an der Schutzwürdigkeit der Information orientiert[376]. Dieses Problem wird durch die elektronische Datenbearbeitung verschärft. Die Speicherung und Verknüpfung zahlreicher Einzelinformationen, die für sich genommen der Gemeinsphäre zugeordnet werden können, lassen sich potentiell zu schützenswerten Persönlichkeitsprofilen verdichten[377]. Der zeitliche Faktor ist hier insofern relevant, als dass eine entsprechende Sammlung über die Zeit erfolgt und potentiell unabhängig vom Kontext erhalten bleibt. Im Weiteren ist die Unterscheidung zwischen öffentlich und privat grundsätzlich Gegenstand von Konventionen, die nicht statisch sind, sondern einem Wandel unterliegen[378]. Das Datenschutzrecht sieht entsprechend eine von der Sensitivität der Information weitgehend unabhängige Kontrolle vor[379]. Die intuitive Grundidee, dass man bestimmte Informationen in ihrer Gesamtheit je nach Inhalt mit den einen teilen will und mit den anderen nicht, bleibt hingegen auch unter diesen Vorzeichen anwendbar[380]. Die Artikel 28 ff. ZGB dienen dem Schutz der Persönlichkeit. In Bezug auf den Zugang zu vertraulichen Informationen ist daher das Bedürfnis des Betroffenen nach Geheimhaltung bestimmter Informationen relevant[381]. Daher ist die Sphärentheorie an sich weder überholt noch abzulehnen[382]. Indessen muss dem individualisierten Verständnis (subjektives Element) der einzelnen Sphären im Hinblick auf die konkrete Information (objektives Element) Rechnung getragen werden. Allgemeingültige Zuordnungen können durch die dynamischen Prozesse häufig nicht mehr gemacht werden. Relevant ist letztlich, ob der Wille zur Geheimhaltung tat-

375 Siehe AEBI-MÜLLER; Rn. 512 ff.; HAUSHEER/AEBI-MÜLLER, Rz. 12.123; DRUEY, Information, 354 ff.; WEBER, Schutz, 96; ders./SOMMERHALDER, 36; GEISER, Persönlichkeitsverletzung, Rz. 2.36; CHERPILLOD, 101 f. Siehe zur Privatsphäre im Besonderen PETER, Datenschutzgesetz, 50 ff.

376 WEBER, Grundrechtskonzeptionen, 13, m.w.H.

377 Indessen hat das Bundesgericht in BGE 97 II 106 früh erkannt, dass auch eine vermeintlich geringfügige Beeinträchtigung des Privatlebens wie die Publikation über eine Vereinszugehörigkeit dem rechtlichen Schutz der Privatsphäre zugehört und kein besonderes Geheimhaltungsinteresse bzw. Nichtverbreitungsinteresse nachzuweisen ist. Dem liegt die Annahme zu Grunde, dass sich das Privatleben aus einer Vielzahl von einzelnen Tatsachen zusammensetzt, die – isoliert betrachtet – nicht bedeutend erscheinen mögen. Eine isolierte Beurteilung der Schutzwürdigkeit dieser einzelnen Tatsachen würde die Privatsphäre jedoch grösstenteils ihres Inhalts berauben und den Schutz gegenstandslos werden lassen.

378 RÖSSLER, 5.

379 HAUSHEER/AEBI-MÜLLER, Rz. 12.123.

380 DRUEY, Information, 356; siehe auch MEISTER, 105, der grundsätzlich auf die Bedeutung verweist, die das Individuum der personenbezogenen Information beimisst.

381 GEISER, Persönlichkeitsverletzung, Rz. 2.37.

382 So auch SCHNEIDER, Anforderungen, 25.

sächlich gegeben ist. Fehlt dieses subjektive Element, vermag die Geheimhaltungswürdigkeit der Information an sich keine Persönlichkeitsverletzung zu begründen[383]. Die datenschutzrechtliche Betrachtungsweise führt zu einem anderen Schluss: Verdichten sich Informationen zu einem Persönlichkeitsprofil, sieht das Datenschutzgesetz gemäss Art. 4 Abs. 5 DSG eine ausdrückliche Einwilligung in die Datenbearbeitung durch den Betroffenen vor. Im Verhältnis zur Sphärentheorie würde das Datenschutzgesetz damit die Zuordnung zu einer schützenswerten Sphäre begründen[384].

Das *Recht am eigenen Bild* schützt als Selbstbestimmungsrecht vor einer widerrechtlichen Verkörperung des eigenen Erscheinungsbildes[385]. Es umfasst einen Abwehranspruch gegen das gezielte Erstellen von Fotografien und Videoaufzeichnungen[386]. Die Veröffentlichung eines individualisierten Bildes ohne die Einwilligung des Betroffenen begründet immer eine Persönlichkeitsverletzung, unabhängig von der Rechtmässigkeit der Aufnahme an sich[387]. Nebst dem Recht am eigenen Bild sind in diesem Zusammenhang oftmals auch die Ehre und die Privatsphäre einer Person betroffen[388]. Der *Schutz des Namens* fällt ebenfalls unter Art. 28 ZGB, sofern keine Namensanmassung im Sinne von Art. 29 ZGB vorliegt[389]. Relevant ist insbesondere die Verwendung der Namen von Prominenten zu Werbezwecken[390]. Die Aufnahme der *Stimme* unter Verletzung von Art. 179bis und 179ter StGB begründet einerseits einen Verstoss gegen die genannten Strafnormen und andererseits eine Persönlichkeitsverletzung[391]. Die *Ehre* umfasst das Ansehen, das einer Person in der Gesellschaft zukommt[392]. Im Unterschied zum Begriff der Ehre im Strafrecht[393] ist der zivilrechtliche Begriff weiter und umfasst nicht nur die Geltung ein achtenswerter Mensch zu sein, sondern beinhaltet auch das

383 GEISER, Persönlichkeitsverletzung, Rz. 2.37.

384 Siehe den Hinweis auf das weitgehend unklare Verhältnis bei HAUSHEER/AEBI-MÜLLER, Rz. 12.123.

385 BÄCHLI, 30 f.

386 Auch wenn die verwendeten Mittel nicht verpönt sind, kann bereits das systematische Auskundschaften des Privatlebens eine Persönlichkeitsverletzung begründen, PEDRAZZINI/OBERHOLZER, 140; BGE 44 II 319; BRÜCKNER, Rn. 628, präzisiert dahingehend, dass sich der Abwehranspruch auf ein gezieltes, auf «Identifikation und Ausforschung» gerichtetes Erstellen beziehe.

387 HAUSHEER/AEBI-MÜLLER, Rz. 13.30.

388 BÄCHLI, 59 ff.

389 BUCHER, Persönlichkeitsschutz, Rn. 477.

390 BRÜCKNER, Rn. 635.

391 BRÜCKNER, Rn. 632.

392 BGE 127 III 487; BGE 129 III 51; BGE 129 III 722. Die Unterscheidung in eine innere Ehre (Ehrgefühl) und eine äussere Ehre (Ruf in der Gemeinschaft) hat blosse Ordnungsfunktion, Art. 28 ZGB schützt beide Teile, HAUSHEER/AEBI-MÜLLER, Rz. 12.84.

393 Siehe dazu BGE 105 IV 111 ff.; BGE 119 IV 47; BGE 121 IV 80; BGE 122 IV 314.

Ansehen in beruflichen, sportlichen und politischen Lebensbereichen[394]. Daneben schützt Art. 28 ZGB den Kredit in Form des Rufs einer Person zahlungsfähig und zahlungswillig zu sein[395]. Die Informationsgegenstände Bild, Name und Stimme werden durch das Recht in zeitlicher Hinsicht in Form der Normierung von Speicherung und Verwertung implizit erfasst.

c) Zeitbezug der Rechtfertigung von Persönlichkeitsverletzungen

Eine Persönlichkeitsverletzung kann unabhängig von ihrem Ausmass aufgrund eines Rechtfertigungsgrundes nicht widerrechtlich sein und entsprechend rechtlich folgenlos bleiben[396]. Grundsätzlich ist dabei nach Art. 28 Abs. 2 ZGB und nach Art. 13 Abs. 1 DSG jede Persönlichkeitsverletzung widerrechtlich, sofern kein Rechtfertigungsgrund vorliegt[397]. Die Beweislast für das Vorliegen eines Rechtfertigungsgrundes trägt der Verletzer[398]. Eine Verletzung ist gemäss Art. 28 Abs. 2 ZGB nicht widerrechtlich, wenn sie durch Einwilligung des Verletzten, durch überwiegende private oder öffentliche Interessen oder durch Gesetz gerechtfertigt wird[399]. Ein Zeitbezug besteht bei allen drei Rechtfertigungsgründen. Bei der Rechtfertigung durch Gesetz ist in zeitlicher Hinsicht massgebend, ob im Zeitpunkt der Persönlichkeitsverletzung ein Gesetz in Kraft ist, das die Datenbearbeitung rechtfertig. Die Rechtfertigung durch das Gesetz ist nach Massgabe von Art. 52 OR grundsätzlich durch Notwehr, Notstand und Selbsthilfe möglich[400]. Im Weiteren kann eine gesetzliche Rechtfertigung in Form von Amtspflichten oder weiteren Gesetzesbestimmungen vorliegen[401]. Bei der Rechtfertigung durch ein überwiegendes Interesse ist in zeitlicher Hinsicht entscheidend, dass dieses zum Zeitpunkt der Verletzung gegenüber dem Interesse des von der Datenbearbeitung Betroffenen überwiegt. Die Einwilligung weist einen differenzierten Zeitbezug auf und

394 BGE 107 II 4; BGE 111 II 210 f.; BGE 129 III 722; GEISER, Persönlichkeitsverletzung, Rz. 2.49 ff.; PEDRAZZINI/OBERHOLZER, 136 ff.; TERCIER, Rn. 686.

395 HAUSHEER/AEBI-MÜLLER, Rz. 12.92, mit Hinweis auf BGE 120 II 20, in dem das Bundesgericht – indessen ohne Berufung auf Art. 28 ZGB – den Anspruch auf negative Feststellungsklage in Bezug auf einen ungerechtfertigten Eintrag im Betreibungsregister bestätigte.

396 RIEMER, Personenrecht, Rn. 369.

397 AEBI-MÜLLER, Rn. 167 ff.; MEILI in: Honsell/Vogt/Geiser § 28 N 45.

398 AEBI-MÜLLER, Rn. 182 ff.

399 Wird die Persönlichkeitsverletzung in einem ersten Schritt bejaht, ist diese grundsätzlich widerrechtlich und in einem zweiten Schritt auf einen rechtfertigenden Umstand zu prüfen, siehe dazu statt vieler HAUSHEER/AEBI-MÜLLER, Rz. 12.13.

400 RIEMER, Personenrecht, Rn. 374; nach PEDRAZZINI/OBERHOLZER, 145 f., 149, ist nur die Selbsthilfe gemäss Art. 52 Abs. 3 OR der gesetzlichen Rechtfertigung zuzuordnen, da Notwehr und Notstand als Fälle eines überwiegenden privaten oder öffentlichen Interesses zu qualifizieren seien; so auch HAUSHEER/AEBI-MÜLLER, Rz. 12.23; vgl. zu Notwehr und Notstand im Strafrecht Art. 16 und 17 StGB.

401 Siehe die Beispiele bei RIEMER, Personenrecht, Rn. 375 ff.

ist Ausdruck einer individuellen Wahrnehmung der Persönlichkeitsrechte, die sowohl eine vergangenheits- als auch eine zukunftsbezogene Wirkung entfalten kann.

In der Lehre wird zum Teil davon ausgegangen, dass die Einwilligung kein Rechtfertigungsgrund ist, sondern bereits den Tatbestand der Persönlichkeitsverletzung ausschliesst[402]. Das Bundesgericht und die herrschende Lehre ordnen die Einwilligung jedoch in ständiger Praxis den Rechtfertigungsgründen zu[403]. Von vornherein nicht von einer Persönlichkeitsverletzung und entsprechend auch nicht vom Erfordernis eines Rechtfertigungsgrundes kann dann ausgegangen werden, wenn die Einschränkung aus der Freiheit der allgemeinen Selbstbestimmung des Betroffenen resultiert[404]. Ungeachtet dieser allgemeinen Selbstbestimmung werden bestimmte Persönlichkeitsbereiche, wie beispielsweise die körperliche Integrität, *per se* geschützt, wodurch hier wieder eine rechtfertigende Einwilligung erforderlich ist[405]. Bei der informationellen Selbstbestimmung steht grundsätzlich die Autonomie des Individuums im Vordergrund. AEBI-MÜLLER ordnet diesen Bereich entsprechend der tatbestandsausschliessenden Kategorie der Selbstbestimmung zu[406]. Sowohl diese tatbestandsausschliessende als auch die rechtfertigende Einwilligung sind nach dem Vertrauensprinzip auszulegen und können jederzeit widerrufen werden, sofern keine rechtsgeschäftliche Verpflichtung zur Duldung des Eingriffs besteht[407].

Die Einwilligung in eine Persönlichkeitsverletzung muss vorgängig erfolgen[408]. Sie kann ausdrücklich oder stillschweigend erteilt werden[409]. In der Literatur wurde in diesem Zusammenhang die Frage aufgeworfen, ob die Einwilligung Rechtsgeschäft oder Zustand bzw. Realakt sei[410]. Sofern eine Handlung oder Unterlassung dem Willen des Betroffenen entspricht und innerhalb der Grenzen seiner Selbstbestimmung liegt, ist

---

402 So HOTZ, 45 ff.; ROBERTO/HRUBESCH-MILLAUER, 232 ff.; BUCHER, Persönlichkeitsrechte, 103 ff.; siehe in Bezug auf das Recht am eigenen Bild, BÄCHLI, 86.

403 Siehe BGE 117 Ib 200; BGE 136 III 413; PEDRAZZINI/OBERHOLZER, 145; HAUSHEER/AEBI-MÜLLER, Rz. 12.18; RIEMER, Personenrecht, Rn. 635; TERCIER, Rn. 635; BUCHER, Persönlichkeitsschutz, Rn. 497; ferner MEILI in: Honsell/Vogt/Geiser § 28 N 47 f.

404 Siehe AEBI-MÜLLER, Rn. 186 f., die insbesondere die Einschränkung der Bewegungsfreiheit von Passagieren im Rahmen einer (freiwilligen) Flugreise anführt.

405 AEBI-MÜLLER, Rn. 194.

406 AEBI-MÜLLER, Rn. 760, die als Beispiele insbesondere die Teilnahme an Talkshows, die Zustimmung für Fotografien und das Erstellen einer frei zugänglichen Website anführt.

407 AEBI-MÜLLER, Rn. 763; RAMPINI, in: Maurer-Lambrou/Vogt, Art. 13 N 14. Der Widerruf gilt für die Zukunft, ROSENTHAL, Handkommentar DSG, Art. 4 N 104.

408 AEBI-MÜLLER, Rn. 225, 762, im Nachhinein kann der Betroffene auf eine Klage verzichten; DESCHENAUX/STEINAUER, Rn. 588a; Ammann, 309; a.A. RIEMER, Personenrecht, Rn. 371.

409 AEBI-MÜLLER, Rn. 226; RIEMER, Personenrecht, Rn. 371.

410 Siehe u.a. ZEDER, 26 ff.; GEISER, Persönlichkeitsverletzungen, Rz. 9.4, m.w.H.; BUCHER, Persönlichkeitsschutz, Rn. 519; AEBI-MÜLLER, Rn. 203 ff.

davon auszugehen, dass der Wille nicht rechtsgeschäftlich kundgetan werden muss[411] und es sich entsprechend um einen Realakt handelt[412]. Entgegen dem Wortlaut muss der Betroffene den Eingriff in seine Persönlichkeitsgüter somit nicht wollen, sondern diesen nur dulden[413]. Es bestehen keine Formvorschriften, die Beweislast für die erteilte Einwilligung liegt jedoch beim Verletzer und entsprechend empfiehlt sich im Zweifelsfall eine schriftliche Einwilligung[414]. Die Widerrechtlichkeit gemäss Art. 28 Abs. 1 ZGB kann indessen trotz der rechtfertigenden Einwilligung aus Art. 28 Abs. 2 ZGB durch Art. 27 ZGB begründet werden, wenn die Einwilligung in zeitlicher Hinsicht übermässig ist. Die Schranken von Art. 27 ZGB können insbesondere überschritten sein, wenn die Zustimmung unwiderruflich oder zeitlich unbegrenzt erteilt wird[415]. Die Einwilligung ist nur gültig, wenn sich der Betroffene hinsichtlich der Tragweite seines Handelns bewusst war und die möglichen Folgen in seine Abwägungen einzubeziehen vermochte[416]. Massgebend ist hierbei einzig, was der Betroffene im Zeitpunkt einer möglichen Verletzung seiner Selbstbestimmung gewollt hat[417].

d) Zeitbezug der Rechtsansprüche aus Persönlichkeitsverletzung

(1) Unterlassungsanspruch

Art. 28a Abs. 1 Ziff. 1 ZGB ermöglicht es dem Kläger, eine drohende Verletzung präventiv abzuwenden. Die Gefahr der bevorstehenden Verletzung bzw. die Gefahr einer Wiederholung muss eine gewisse Wahrscheinlichkeit aufweisen resp. ernstlich zu befürchten sein[418]. Die Unterlassungsklage bezweckt damit, dem Beklagten unter Strafandrohung gemäss Art. 292 StGB (Ungehorsam gegen amtliche Verfügungen) die Vornahme einer persönlichkeitsverletzenden Handlung gerichtlich zu verbieten[419]. Die

---

411 AEBI-MÜLLER, Rn. 203; siehe dazu auch GEISER, Persönlichkeitsverletzungen, Rz. 9.5, der darauf hinweist, dass das Recht auf Selbstbestimmung in einem bestimmten Bereich nicht verletzt ist, sofern jemand einem dazu gehörenden Aspekt seiner Persönlichkeit gegenüber gleichgültig ist.

412 Siehe AEBI-MÜLLER, Rn. 203.

413 AEBI-MÜLLER, Rn. 181; zur Erörterung der dogmatischen Fragen nach der Rechtsnatur der Einwilligung Rn. 182 ff.

414 In Bezug auf die Formvorschriften ist demnach das im Online-Bereich verbreitete Erfordernis des Setzens von Häkchen ebenfalls nicht erforderlich und erklärt sich durch die genannte Beweisfunktion.

415 RIEMER, Personenrecht, Rn. 371 ff.

416 DESCHENAUX/STEINAUER, Rn. 588; siehe auch BGE 136 III 407, wobei die rechtswirksame und irrtumsfreie Einwilligung hier nicht strittig war; siehe dazu auch UHLIG, 331 f.; siehe zur Urteilsfähigkeit eingehend HAAS, Rn. 259 ff.

417 AEBEI-MÜLLER, Rn. 203.

418 BGE 95 II 500; BGE 97 II 92 ff.; BGE 97 II 107 f.

419 PEDRAZZINI/OBERHOLZER, 155.

Schwierigkeit dieses Anspruchs liegt in der auf die Zukunft gerichteten, möglichst genauen Umschreibung des verbotenen Handelns[420].

(2) Beseitigungsanspruch

Art. 28a Abs. 1 Ziff. 2 ZGB ermöglicht es dem Kläger, eine bestehende Verletzung beseitigen zu lassen. Im Unterschied zur Unterlassungsklage muss entsprechend bereits eine Persönlichkeitsverletzung eingetreten sein[421]. Die Beseitigungsklage dient insbesondere dazu, Material, das bereits zur Anwendung gekommen ist und dessen Verwertung noch andauert oder Material, das zur Verwertung vorbereitet worden ist, beseitigen zu lassen[422]. Auch scheinbar vergessene Äusserungen können sich noch während Jahren auswirken[423]. Birgt eine bestehende Störung die Drohung einer künftigen widerrechtlichen Verletzung in sich, kann die Abgrenzung zwischen der Beseitigungs- und der Unterlassungsklage im Einzelfall schwierig sein[424]. Die Unterscheidung ist indessen nicht von zentraler Bedeutung, da nach Art. 28a Abs. 1 ZGB im Grundsatz beide Klagen möglich sind[425].

(3) Feststellungsanspruch

Die Feststellungsklage in Art. 28a Abs. 1 Ziff. 3 ZGB ist die am häufigsten genutzte Klagemöglichkeit des Persönlichkeitsschutzes[426]. Der Kläger kann dadurch die Widerrechtlichkeit einer Verletzung gerichtlich feststellen lassen, wenn sich diese weiterhin störend auswirkt. Die Klage zielt darauf ab, den Inhalt des Persönlichkeitsrechts des Klägers in einem bestimmten Kontext zu klären und bezieht sich damit auf ein Rechtsverhältnis, nicht auf Tatsachen[427]. Das Feststellungsurteil ist einer Vollstreckung nicht zugänglich, der Anspruch wird bereits durch die gerichtliche Feststellung erfüllt[428]. Die

---

420 Siehe dazu BGer vom 20. Juni 2012, 5A_888/2011, E. 8.3.

421 GEISER, Persönlichkeitsverletzung, Rz. 10.18.

422 RIEMER, Personenrecht, Rn. 387; JÄGGI, 231a, der Anspruch auf Beseitigung umfasst bei einer Fotografie die Vernichtung des Negativs und der allenfalls hergestellten Kopien, nicht dagegen die Herausgabe dieser Gegenstände, es soll einzig der frühere Zustand wieder hergestellt werden. Im elektronischen Bereich müsste demnach zumindest eine Löschung oder – und unter Berücksichtigung der Wiederherstellbarkeit gelöschter Daten – eine Vernichtung des Datenträgers erfolgen.

423 BGE 95 II 497; SCHUMACHER, 178; JÄGGI, 249a.

424 HAUSHEER/AEBI-MÜLLER, Rz. 14.22; siehe auch BGE 95 II 500, wonach die in Art. 28 Abs. 1 ZGB vorgesehene Klage auf Beseitigung der Störung zugleich die Klage auf Unterlassung drohender Störungen umfasst.

425 GEISER, Persönlichkeitsverletzung, Rz. 10.18.

426 HAUSHEER/AEBI-MÜLLER, Rz. 14.27; RIEMER, Personenrecht, Rn. 390.

427 PEDRAZZINI/OBERHOLZER, 156.

428 HAUSHEER/AEBI-MÜLLER, Rz. 14.35.

Feststellungsklage enthält durch die gerichtliche Feststellung auch einen Beseitigungsaspekt[429]. Das Unrecht kann zwar durch die zeitliche Gebundenheit aller Ereignisse nicht ungeschehen gemacht werden, doch kann es durch das Gerichtsurteil nicht nur zeitlich, sondern auch inhaltlich überlagert und dadurch neutralisiert werden.

(4) Anspruch auf Berichtigung oder Urteilsveröffentlichung

Die gerichtliche Anordnung einer Berichtigung oder Urteilsveröffentlichung gemäss Art. 28a Abs. 2 ZGB erfolgt, sofern dadurch die Folgen einer Persönlichkeitsverletzung in geeigneter Weise beseitigt werden können[430]. Dabei handelt es sich um nicht selbständige Rechtsbehelfe, d.h. die Berichtigung oder Urteilsveröffentlichung gelangt nur im Zusammenhang mit einer Klage auf Unterlassung, Beseitigung oder Feststellung zur Anwendung[431]. Der Beseitigungsaspekt der Feststellungsklage wird durch die Urteilspublikation konkretisiert. Die Publikation des Urteils beseitigt das zuvor erweckte falsche Gedankenbild, was insbesondere bei ehrverletzenden Publikationen im Medienbereich relevant ist[432].

(5) Anspruch auf Schadenersatz, Genugtuung und Gewinnherausgabe

Für die Ansprüche auf Schadenersatz, Genugtuung und Gewinnherausgabe verweist Art. 28a Abs. 3 ZGB auf die entsprechenden Bestimmungen im OR. Schadenersatzansprüche richten sich nach Art. 41 ff. OR, Genugtuungsansprüche nach Art. 49 OR und Ansprüche auf Gewinnherausgabe nach Art. 423 OR[433].

In zeitlicher Hinsicht beziehen sich der Schadenersatz- und der Genugtuungsanspruch und der Anspruch auf Gewinnherausgabe auf die Vergangenheit, sie sollen einen Verlust bzw. einen durch den Schädiger erzielten Gewinn, der in der Vergangenheit entstanden ist, ausgleichen. In Abgrenzung dazu besteht das Ziel der Beseitigungsklage darin, zu verhindern, dass eine Persönlichkeitsverletzung in der Zukunft andauert. Beeinträchtigungen der Vergangenheit sind dagegen nicht Gegenstand der Beseitigungs-

429 RIEMER, Personenrecht, Rn. 390.

430 PEDRAZZINI/OBERHOLZER, 157.

431 HAUSHEER/AEBI-MÜLLER, Rz. 14.37; PEDRAZZINI/OBERHOLZER, 157; RIEMER, Personenrecht, Rn. 391.

432 RIEMER, Personenrecht, Rn. 392; so können die beklagten Zeitungen zur Publikation entsprechender Urteile verpflichtet werden; siehe dazu BGE 95 II 481 ff.; BGE 100 II 180; BGE 103 II 166; BGE 104 II 1 f.

433 HAUSHEER/AEBI-MÜLLER, Rz. 14.44 ff.; PEDRAZZINI/OBERHOLZER, 159 ff.; RIEMER, Personenrecht, Rn. 398 ff.

klage[434]. Auch der Unterlassungsanspruch ist auf die Zukunft gerichtet, wobei hier eine Persönlichkeitsverletzung vorweg verhindert werden soll[435].

e) Zeitliche Wirkung der Kommerzialisierung vermögenswerter Persönlichkeitsrechte

(1) Faktische Kommerzialisierung

Der Wortlaut von Art. 28 Abs. 1 ZGB unterscheidet nicht zwischen ideellen und vermögenswerten Bestandteilen des Persönlichkeitsrechts[436]. In Art. 28a Abs. 3 ZGB sind jedoch die vermögensrechtlichen Ansprüche, die sich aus einer Verletzung der Persönlichkeitsrechte ergeben können, enthalten[437]. Dies kann dahingehend interpretiert werden, dass der Gesetzgeber das Vorliegen verwertbarer Positionen und die aus dem Zugriff auf die Persönlichkeitsgüter resultierende wirtschaftliche Verwertung anerkennt[438]. Die Vermarktung der Persönlichkeit hat eine lange Geschichte. International geht die Entwicklung bis ins 18. Jahrhundert zurück[439]. Auch das von WARREN/BRANDEIS ursprünglich als ein Gegengewicht zur journalistischen Zudringlichkeit entwickelte «*right to be let alone*»[440] erhielt seine rechtliche Bedeutung erstmals im Zusammenhang mit der unautorisierten Nutzung von Namen und Ähnlichkeiten[441].

(2) Annäherung an die Immaterialgüterrechte

DRUEY merkt an, dass ungeachtet der rechtspolitischen Haltung gegenüber einer dem Immaterialgüterrecht nahestehenden Eigentumsanalogie auf jeden Fall eine Entkoppelung persönlichkeitsbezogener Aspekte vom Persönlichkeitsrecht, das keine Monopolisierung von sozialen Kontakten erlaube, erfolgt sei[442]. Die Qualifikation als Immaterialgüterrecht oder Quasi-Immaterialgüterrecht wird teilweise insbesondere für das Recht am eigenen Bild und auch generell für vermögenswerte Bestandteile des Persönlichkeitsrechts gefordert[443]. Dabei erfolgt meistens eine Anlehnung an das Urheberrecht,

---

434 GEISER, Persönlichkeitsverletzung, Rz. 10.19.

435 Vgl. GEISER, Persönlichkeitsverletzung, Rz. 10.18.

436 MEYER, Persönlichkeitsrechte, Rn. 673.

437 Siehe auch zum historischen Gesetzestext MEYER, Persönlichkeitsrechte, Rn. 663 ff., m.w.H.

438 BÜCHLER, Kommerzialisierung, 313 f.

439 MADOW, 148.

440 WARREN/BRANDEIS, 195 f.; WERRO, 292; siehe zum Entstehungshintergrund des Artikels LANE, 61 ff.

441 MADOW, 167.

442 DRUEY, Information, 360 f; siehe auch BÜCHLER, Persönlichkeitsgüter, 180, die für die kommerziell nutzbaren Elemente von Persönlichkeitsrechten eine faktische Entwicklung hin zu den Immaterialgüterrechten feststellt.

443 MEYER, Persönlichkeitsrechte, Rn. 738.

dem in einem gewissen Umfang eine Wesensverwandtschaft zugeschrieben wird[444]. Der Ausdruck eines Persönlichkeitsguts begründet jedoch kein urheberrechtlich geschütztes Werk[445]. Das Urheberrecht regelt den Schutz von Werken der Literatur und Kunst. Als Werke gelten gemäss Art. 2 Abs. 1 URG unabhängig von ihrem Zweck oder Wert geistige Schöpfungen der Literatur und Kunst, die individuellen Charakter haben[446]. Urheber ist gemäss Art. 6 URG die natürliche Person, die das Werk geschaffen hat. Im schweizerischen Urheberrecht gilt das Schöpferprinzip; das Urheberrecht entsteht immer originär bei der schöpfenden Person. Aus Art. 6 URG ergibt sich auch, dass Urheberrechte nur menschlichen Schöpfungen zugesprochen werden[447]. Der Begriff der «Schöpfung» impliziert, dass etwas geschaffen worden ist, ein Werk liegt nach diesem Verständnis somit nur dann vor, wenn ein schöpferischer Akt gegeben ist. Auch das blosse Finden und anschliessende Präsentieren des Gefundenen ist urheberrechtlich nicht geschützt[448].

Im Unterschied zu den Persönlichkeitsrechten, die ein individuelles Wesen schützen und das Verhältnis desselben zu anderen Personen rechtlich umfassen, schützen die Immaterialgüterrechte bestimmte Rechtsobjekte, die Gegenstand einer umfassenden Nutzung sein können[449]. Persönlichkeitsaspekte sind mit einer Person verbunden, Immaterialgüter existieren nach ihrer Entstehung dagegen ausserhalb und unabhängig von der Person[450]. Der wesentliche Unterschied zwischen Persönlichkeits- und Immaterialgüterrechten besteht demnach in der Selbständigkeit des geschützten Immaterialguts im Verhältnis zur Person, der es zugeordnet ist[451]. Indessen geniessen Identitätskennzeichen und die Identität selbst einen den Urheberrechten teilweise ähnlichen Rechtsschutz[452].

---

444 MEYER, Persönlichkeitsrechte, Rn. 738 ff., m.w.H.; RIEMER, Persönlichkeitsrechte, 103; UHLIG, 332, mit Verweis auf den verbotsrechtlichen Charakter und dem Hinweis, dass bei den Immaterialgüterrechten die Einräumung von Nutzungsrechten entsprechend ihrem Zweck der wirtschaftlichen Verwertbarkeit überwiege.

445 REHBINDER, § 5 N 30.

446 Siehe zum Begriff des urheberrechtlich geschützten Werks VON BÜREN/MARBACH/DUCREY, Rn. 230 ff.

447 VON BÜREN/MARBACH/DUCREY, Rn. 277.

448 VON BÜREN/MARBACH/DUCREY, Rn. 231.

449 PEIFER 273; TROLLER, 17.

450 KRASSER, 230; PEIFER, 273; MEISTER, 104.

451 HUBMANN, Recht, 85 f.; PEIFER, 141; MEISTER, 104; PEUKERT, 714.

452 REHBINDER, § 6 N 37.

Relevant im Hinblick auf die Abgrenzung zu den Immaterialgüterrechten erscheint die Unterscheidung zwischen Vermögens- und Persönlichkeitsrechten[453]. Im Schnittbereich stellt sich die Frage, ob vermögenswerte Bestandteile von Persönlichkeitsrechten eine neue Form von Immaterialgüterrechten darstellen. Grundsätzlich ist aber das Schutzobjekt ein anderes; während das Urheberrecht am Werk als Schutzobjekt anknüpft, steht beim Persönlichkeitsrecht die Person als Schutzobjekt im Zentrum[454]. In Bezug auf das unterschiedliche Schutzobjekt merkte bereits KOHLER an, dass die eigene Schöpfung die Verfügungsmacht über das Geschaffene zu begründen vermag, dies jedoch bei der eigenen Person gerade nicht gegeben sei, da die einzelne Person nicht Urheber ihrer eigenen Körperlichkeit sei[455]. Das Urheberrecht ist entsprechend bezüglich all jener Aspekte übertragbar, die von der Sache her übertragen werden können und der Urheber unterliegt weder einer im immaterialgüter- noch im sachenrechtlichen Vertragsrecht angelegten Verfügungsbeschränkung. Zwingend geschützt wird er hingegen – wie bereits dargelegt – im Rahmen von Art. 28 ZGB[456]. Eine umfassende Zuordnung der Persönlichkeitsrechte zu den Immaterialgüterrechten ist trotz einer möglichen Annäherung durch bestimmte Entwicklungen abzulehnen[457]. AEBI-MÜLLER und BRÜCKNER ordnen den Persönlichkeitsschutz ebenfalls den Abwehrrechten zu, bei dem die Wahrung der Autonomie und Integrität im Vordergrund stehen und nicht die Verwertung[458].

(3) Übertragbarkeit

Unabhängig von ihrem Vermögenswert bzw. der Zuordnung zu den Immaterialgüterrechten gehören gewisse Elemente des Persönlichkeitsrechts nicht zum Kernbereich der menschlichen Existenz und können daher nach einem Teil der Lehre Gegenstand

453 Vgl. dazu JÄGGI, 205a; VON BÜREN/MARBACH/DUCREY, Rn. 832 f.

454 MEYER, Persönlichkeitsrechte, Rn. 741.

455 KOHLER, 8 f.

456 HILTY, Lizenzvertragsrecht, 25.

457 WEBER, Persönlichkeitsrecht, 421 ff.; MEYER, Persönlichkeitsrechte, Rn. 764; BÄCHLI, 153 f., 162; siehe ferner BÜCHLER, Kommerzialisierung, 320 ff.; BÜCHLER, Persönlichkeitsgüter, 195; siehe zum deutschen Recht UNSELD, 283 ff., m.w.H.

458 AEBI-MÜLLER, Rn. 112; BRÜCKNER, Rn. 405 f.

von vertraglichen und weitgehend unwiderruflichen Verpflichtungen sein[459]. Ein anderer Teil der Lehre geht dagegen von der freien Widerrufbarkeit der Einwilligung mit allfälligen Schadenersatzansprüchen unter analoger Anwendung von Art. 404 Abs. 2 OR aus[460]. Generell folgt aus den unterschiedlichen Positionen im Hinblick auf die Ausgestaltung der Persönlichkeitsgüter nicht, dass diese dem Rechtsverkehr nicht zugänglich sind[461]. Gemäss Art. 19 Abs. 1 OR gilt die Vertragsfreiheit; innerhalb der gesetzlichen und sittlichen Schranken kann der Inhalt eines Vertrages beliebig bestimmt werden[462]. HILTY stellt fest, dass die Wahrnehmung legitimer wirtschaftlicher Interessen vom Recht möglichst nicht zu behindern sei und ein «griffiges Vertragsrecht» einen besseren Schutz biete als die Nichtigkeit von Verträgen, die die Übertragung von verwertbaren Persönlichkeitsgütern zum Inhalt hätten[463]. Hinsichtlich der Übertragbarkeit vermögenswerter Persönlichkeitsrechte ist dieser Auffassung zuzustimmen[464].

Sofern eine effektive Übertragbarkeit im veräusserungsrechtlichen Sinn nicht möglich ist, steht die Nutzung mittels Lizenzvertrag im Vordergrund[465]. Der Lizenzvertrag ist

---

459 Siehe zur Unterscheidung zwischen ideellen und vermögenswerten Persönlichkeitsrechten INDERKUM, Rn. 57 ff.; nach BRÜCKNER, Rn. 449, gehören Bild, Name und Stimme nicht zum Kernbereich menschlicher Existenz, weshalb entsprechende Lizenzverträge weder gegen die guten Sitten verstossen, noch eine übermässige Bindung im Sinne von Art. 27 Abs. 2 ZGB begründen würden; differenzierend hinsichtlich der Motive des Widerrufs BÜCHLER, Persönlichkeitsgüter, 187 f.; HAUSHEER/AEBI-MÜLLER, Rz. 10.24, verweisen aufgrund von Art. 27 Abs. 2 ZGB auf die grundsätzliche Widerrufbarkeit der Übertragung; unter Verweis auf die arbeitsrechtlichen Bestimmungen des Art. 337d und 337 OR stellt AEBI-MÜLLER, Rn. 220, fest, dass dem Anliegen von Art. 27 ZGB Genüge getan sei, wenn die Verpflichtung aus wichtigem Grund widerrufen werden könne; siehe auch GEISER, Persönlichkeitsverletzung, Rz. 9.25, dem es unter Verweis auf Arbeitsverträge falsch erscheint, jede vertragliche Bindung im Bereich der Persönlichkeit abzulehnen; siehe ferner UHLIG, 335, der sich am Beispiel des Persönlichkeitsrechts im Film ebenfalls für eine verbindliche und unwiderrufliche Einwilligung ausspricht.

460 TERCIER, Rn. 638 ff., weist einschränkend darauf hin, dass die Unverzichtbarkeit des Widerrufsrechts dort nicht unproblematisch sei, wo der Eingriff nicht ausschliesslich im Interesse des Betroffenen erfolge und für den Verletzenden mit erheblichen ideellen oder materiellen Investitionen verbunden sei; siehe dazu auch BÄCHLI, 92 f.; HAAS, Rn. 559-566; zur Anwendung von Art. 404 Abs. 2 OR statt vieler HAAS, Rn. 559, m.w.H.; GEISER, Persönlichkeitsverletzung, Rz. 9.25, Fn. 108, weist darauf hin, dass Schadenersatz nach Art. 404 Abs. 2 OR im Allgemeinen nicht genüge, da mit dem Rückzug zur Unzeit auch Persönlichkeitsrechte verletzt werden könnten.

461 BÜCHLER, Kommerzialisierung, 327.

462 HUGUENIN, in: Vogt/Honsell/Wiegand, Art. 19/20 N 12 ff.

463 HILTY, Unübertragbarkeit, 279 f.; a.A. PEUKERT, 718, der darin insbesondere eine Stärkung der Position professioneller Verwerter sieht, die sich alle erdenklichen geldwerten Positionen exklusiv einräumen lassen würden und weiter auf den drohenden Verlust des Selbstbestimmungsrechts verweist.

464 So auch INDERKUM, Rn. 58, 75.

465 BUCHER, Persönlichkeitsschutz, Rn. 442; BRÜCKNER, Rn. 449; WEBER, Persönlichkeitsrecht, 423 f.; HILTY, Lizenzvertragsrecht, 28; BÜCHLER, Persönlichkeitsgüter, 185; MEYER, Persönlichkeitsrechte, Rn. 789 ff; siehe zu den Formen BÄCHLI, 128; a.A. HAAS, Rn. 182.

ein Innominatvertrag *sui generis*[466]. In Anbetracht der vielfältigen Ausgestaltungsmöglichkeiten von Lizenzverträgen und der unterschiedlichen Vertragsgegenstände handelt es sich beim Lizenzvertrag um einen weiten Begriff[467]. Eine allgemeine Definition dafür findet sich bei PEDRAZZINI, der den Lizenzvertrag folgendermassen umschreibt: «Durch den Lizenzvertrag verpflichtet sich der Lizenzgeber, dem Lizenznehmer die Benutzung eines gesetzlich geschützten oder eines nur faktisch gesicherten Immaterialgutes zu gestatten, und der Lizenznehmer dem Lizenzgeber, hierfür in der Regel eine Gebühr zu bezahlen[468].» Daraus resultiert an sich insbesondere keine Entäusserung der Freiheit im Sinne von Art. 27 Abs. 2 ZGB[469]. Dauerschuldverhältnisse sind im Allgemeinen zudem aus wichtigem Grund kündbar[470]. Die fehlende Zuordnung der Persönlichkeitsrechte zu den Immaterialgüterrechten, steht einer lizenzvertraglichen Ausgestaltung somit nicht entgegen[471]. WEBER spricht sich für eine «Doppelnatur der Rechtsinhaberschaft in persönlichkeits- und vermögensrechtlicher Hinsicht» aus und verweist auf das Lizenzvertrags- und das Leistungsschutzrechtskonzept[472].

Das Bundesgericht bestätigt diese Rechtsauffassung, wenn wirtschaftliche Interessen im Vordergrund stehen und stellt zu Recht fest, dass in Anbetracht der Bedeutung, die die Vermarktung des eigenen Bildes, des Namens oder der Stimme in den letzten Jahrzehnten erlangt hat, die Einwilligung zur Abtretung spezifischer Rechte an diesen Elementen möglich sein muss[473]. Es wäre realitätsfern, diese Einwilligung als einer rechtlichen Bindung nicht zugängliches Geschäft zu erachten und einem umfassenden Recht auf freien Widerruf den Vorrang zu geben[474]. Ebenfalls nicht ersichtlich ist, weshalb

---

466 AMSTUTZ/MORIN/SCHLUEP, in: Vogt/Honsell/Wiegand, Einl. vor Art. 184 ff. N 242; BGE 92 II 299.

467 Siehe dazu umfassend HILTY, Lizenzvertragsrecht, 5 ff.

468 PEDRAZZINI, 414.

469 WEBER, Persönlichkeitsrecht, 423; siehe auch UHLIG, 334.

470 AEBI-MÜLLER, Rn. 337 f.; BÜCHLER, Persönlichkeitsgüter, 185 f.; BÜCHLER, Kommerzialisierung, 329 f., 347; MEYER, Persönlichkeitsrechte, Rn. 796; ROUVINEZ, Rn. 929 ff.

471 BÜCHLER, Persönlichkeitsgüter, 184 f.

472 WEBER, 422, m.w.H.

473 Siehe BGE 136 III 405, wo indessen ein entgeltliches Widerrufsrecht vereinbart war. Auch werden die wirtschaftlichen Interessen hier nicht konkretisiert. Nach BARRELET/WERLY, Rn. 1527, kann aus dem Urteil höchstens gefolgert werden, dass der Widerruf in besonderen Fällen an Bedingungen geknüpft werden kann; siehe auch die Kritik bei ROUVINEZ, Rn. 569; siehe ferner das Urteil des BGH 1 ZR 149/97 vom 1. Dezember 1999, wo im Fall Marlene Dietrich die verbesserten technischen Möglichkeiten von Bild- und Tonaufnahmen und das noch nie dagewesene Ausmass der wirtschaftlichen Nutzbarmachung hervorgehoben werden.

474 BGE 136 III 405; siehe unter Verweis auf eine «minimale Rechtssicherheit» BÜCHLER, Persönlichkeitsgüter, 187.

dieses Recht auf bekannte Persönlichkeiten, die beispielsweise ihren Namen oder ihr Bild mit Lizenzverträgen kommerziell nutzen, beschränkt sein soll[475].

Auf die Vererbbarkeit soll hier nur kurz eingegangen werden. Die Persönlichkeit geht mit dem Tod gemäss Art. 31 Abs. 1 ZGB unter und kann entsprechend ab diesem Zeitpunkt nicht mehr verletzt werden[476]. Die Persönlichkeitsrechte bleiben auch erbrechtlich nicht erhalten[477], die Persönlichkeit und mit ihr der Persönlichkeitsschutz enden mit dem Tod[478]. Trotzdem berücksichtigt das Bundesgericht ein «Nachwirken der Persönlichkeit des Verstorbenen» und ermöglicht den Hinterbliebenen die Geltendmachung bestimmter Abwehrrechte[479]. Der Schutzbereich ist indessen mit jenem von lebenden Personen nicht identisch[480]. Die Klagelegitimation setzt kein rechtlich relevantes Verhältnis zum Verstorbenen voraus und muss im Einzelfall ermittelt werden. Grundsätzlich stehen die Rechtsmittel aus Art. 28 ZGB zur Verfügung; so kann insbesondere auf Unterlassung oder Beseitigung geklagt werden. Der Anspruch auf Genugtuung hat nur bei erheblichen Eingriffen Aussicht auf Erfolg[481]. Eine Ausnahme vom Grundsatz der Unvererblichkeit bildet Art. 11 Abs. 2 URG, der den Schutz vor Entstellungen als Teil der Werkintegrität vorsieht und im Verhältnis zu Art. 28 ZGB *lex specialis* ist[482]. Im Weiteren sind die Urheberrechte aus Art. 16 Abs. 1 URG übertragbar und vererblich. Der Gegensatz kann mit der Nähe von Urheberpersönlichkeitsrechten zu vermögensrechtlichen Ansprüchen erklärt werden[483]. Der weit gefasste Werkbegriff[484] erleichtert die Berufung auf den Urheberrechtsschutz, dieser ist gegenüber dem persönlichkeitsrechtlichen Andenkenschutz im Vorteil[485].

(4) Schlussfolgerungen

Insgesamt nimmt der Schutz der Persönlichkeit in der schweizerischen Rechtsordnung einen hohen Stellenwert ein[486], so wird dem Persönlichkeitsrecht bisweilen auch eine

475 BGE 136 III 405 f.
476 BGE 129 I 302; BGE 129 III 209.
477 BGE 101 II 191; PEDRAZZINI/OBERHOLZER, 171.
478 BGE 104 II 235 f.
479 BGE 70 II 127; BGE 101 II 191; BGE 104 II 236; BGE 118 IV 323; HAUSHEER/AEBI-MÜLLER, Rz. 10.27.
480 BREITSCHMID/KAMP, 22.
481 BREITSCHMID/KAMP, 24.
482 RIEMER, Persönlichkeitsrechte, 108.
483 BREITSCHMID/KAMP, 27.
484 Vgl. dazu vorne B.II.1.3 e)(2).
485 BREITSCHMID/KAMP, 27;
486 AEBI-MÜLLER, Rn. 262.

Vorrangstellung gegenüber reinen Vermögensinteressen zugesprochen[487]. Eine Zuordnung zu den Immaterialgüterrechten würde daher weniger zu einer Erweiterung des Persönlichkeitsschutzes und mehr zu einer verbesserten Verkehrsfähigkeit der entsprechenden Persönlichkeitsaspekte führen[488]. Insbesondere in der US-amerikanischen Literatur wurde eingewendet, dass das Eigentum zur Kommodifizierung, Vermarktung und Monetarisierung von Beziehungen führen könnte, die einen ganz anderen Wertgehalt hätten und dadurch eine weitere Lebenssphäre dem Markt zugeführt würde[489]. Obwohl personenbezogene Daten von Unternehmen vermarktet werden, lässt sich dieser Vorgang nicht auf einen sozialen Kontext übertragen[490]. In diesem Zusammenhang ist auch festzustellen, dass ein kommerzieller Ansatz die Probleme der zwischenmenschlichen Interaktion gerade nicht zu lösen vermag[491].

Zweifelhaft erscheint zudem, ob ein zu schaffendes Eigentumsrecht durch die Eigentümer tatsächlich wahrgenommen werden könnte. Generell ist die Bewertung von Persönlichkeitsrechten stark subjektiv geprägt[492]. Handelsbasierte Lösungen, die personenbezogene Informationen dem handelbaren Eigentum zuordnen, hängen aber wesentlich von der Fähigkeit der Individuen ab, ihre Daten möglichst genau bewerten zu können[493]. Eigentumsrechte könnten den personenbezogenen Daten somit nur insofern einen Wert zuführen, als dass sie für die betroffene Person überhaupt einen solchen darstellen[494]. Der Wert bemisst sich dann nach der Höhe der Kompensation, die für die Aufgabe der Daten gefordert wird. Aus der Tatsache, dass die Anbieter routinemässig

---

487 TERCIER, Rn. 598; BGer vom 28.10.2003, 5P.308/2003. Im Bereich der Grundrechte wird innerhalb des Persönlichkeitsschutzes rein finanziellen Angaben über eine Person ein geringerer Schutz zugemessen. Mit BGE 104 Ia 53 wurde die höchstrichterliche Praxis begründet, wonach dem Bankgeheimnis nicht die Stellung eines verfassungsmässigen Rechts zukommt; vgl. auch BGE 123 II 160; BGE 125 II 84.

488 Indessen mit allen Konsequenzen; so erscheint ein jederzeitiges Rücktrittsrecht bei übertragenen Persönlichkeitsrechten als mit einer eigentumsrechtlichen Ausgestaltung unvereinbar; a.M. PURTOVA, 258; kritisch in Bezug auf die freie Übertragbarkeit insbesondere an Dritte und ohne Zweckbindung, SAMUELSON, 1138.

489 RADIN, 524 ff.; siehe im Zusammenhang mit *Big Data* auch die Modellkritik bei SCHIRRMACHER, 190 ff.

490 In Deutschland hat das BVerfG in einer Entscheidung zum Privatversicherungsrecht folgendes festgestellt: «Gerade im Verkehr zwischen Privaten lässt sich dem allgemeinen Persönlichkeitsrecht allerdings kein dingliches Herrschaftsrecht über bestimmte Informationen entnehmen.», BVerfGE JZ 2007, 576; siehe dazu grundlegend bereits das Volkszählungsurteil vom 15. Dezember 1983: «Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über „seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit.», BVerfGE 65, 1, 43 f.

491 Siehe GRIMMELMANN, 1188.

492 RODRIGUES, 247.

493 SOLOVE, Person, 87.

494 BYFORD, 56; HUI/PNG, 486 ff., mit Hinweis auf die Notwendigkeit entsprechender Studien.

Daten für Einkaufsrabattkarten, Zugang zu Webdiensten und sogar ganz ohne Gegenleistung preisgeben, kann zumindest geschlossen werden, dass dieser Wert im Allgemeinen sehr tief liegt[495]. Diese Annahme wird durch den tatsächlichen Umgang mit personenbezogenen Daten bestätigt[496]. Nach hier vertretener Auffassung erübrigt sich die Diskussion um einen funktionierenden Markt[497] indessen aus ökonomischer Sicht bereits deshalb, da personenbezogene Daten mangels der Aufwendung von Arbeit und Kapital auf Seiten des Individuums nicht den knappen Gütern zuzuordnen sind[498]. Relevant erscheint hierbei auch, dass eine eigentumsrechtliche Ausgestaltung primär jenen Organisationen zugute kommt, die die entsprechenden Datenbestände im grossen Umfang nutzen können[499]. Diese sind gegenüber kleineren Organisationen und gegenüber Individuen im Vorteil[500]. Im Resultat können die Immaterialgüterrechte aus rechtlicher Sicht kein Ordnungskriterium für persönliche Daten sein, da die Immaterialgüterrechte den Vermögensrechten zugeordnet sind[501]. Diesen können die Persönlichkeitsrechte wie dargelegt nicht umfassend zugeteilt werden. Der Abtretung spezifischer vermögenswerter Bestandteile von Persönlichkeitsrechten sowie lizenzanalogen Ausgestaltungen steht diese Wertung indessen nicht entgegen. In zeitlicher Hinsicht wird dadurch eine weitgehend rechtssichere Nutzung persönlichkeitsbezogener Aspekte über einen bestimmten Zeitraum hinweg möglich.

1.4 Recht auf Vergessen im Besonderen

a) Konzeption

Das Recht auf Vergessen ist in der Schweiz vom Bundesgericht bereits vor vielen Jahren im Rahmen der Konkretisierung von Art. 28 ZGB entwickelt worden[502]. Das Bun-

---

495 Vgl. LANE, 261.

496 SOLOVE, Person, 87. Es bestehen klare Anzeichen, dass viele Nutzer den Schutz ihrer Privatsphäre nicht sehr hoch gewichten; siehe dazu das Beispiel bei SAMANI RAJ, How much do you value your personal data?, The Telegraph, October 14, 2012, abrufbar unter: http://www.telegraph.co.uk/technology/internet-security/9605078/How-much-do-you-value-your-personal-data.html, abgerufen am 31.5.2014; danach kann bereits die Verteilung kostenloser Schokoladenriegel jegliche Vorbehalte in den Hintergrund treten lassen.

497 Siehe zur Problematik von Informationsmärkten grundlegend LINDE, 14 ff.

498 Siehe zur aufwandgenerierenden Verarbeitung durch Unternehmen vorne A.I.1.2 b); siehe auch die Feststellung bei MEISTER, 104: «Dass ein persönliches Datum nicht vom Betroffenen „geschaffen“ wird, bedarf keiner näheren Begründung».

499 Siehe dazu bereits in Bezug auf die Kommerzialisierung von Information vorne A.I.1.3 b)(2).

500 BENKLER, 103.

501 MEISTER, 105.

502 GLAUS, Vergessen, 193. Siehe zu den Ursprüngen in Europa in Form des französischen *droit à l'oubli* die umfassenden Verweise auf die Rechtsprechung bei MANTELERO, 728, Fn. 3; siehe zur US-amerikanischen Rechtsprechung ders., 730 ff.

desgericht entschied im Fall Irniger, dass bei einem Straftäter allein schon das Ziel der Resozialisierung eines dem «normalen Lauf der Dinge entsprechenden Vergessens» bedürfe, auch wenn dieses nie vollständig sein könne[503]. Ein generelles, von der Pressefreiheit losgelöstes «Recht auf Vergessen» wird vom Bundesgericht hingegen abgelehnt[504].

Das öffentliche Interesse an der Information durch die Presse kann insbesondere dann hinter das private Interesse einer Person zurücktreten, wenn ein Vorkommnis schon lange zurück liegt und sich eine Persönlichkeitsverletzung entsprechend nicht mehr durch das öffentliche Informationsinteresse rechtfertigen lässt[505]. Dabei ist auch eine wahrheitsgemässe Berichterstattung über vergangene Verurteilungen persönlichkeitsverletzend und ohne Rechtfertigungsgrund widerrechtlich[506]. Das Recht auf Vergessen trägt in seiner bisherigen Form dem Umstand Rechnung, dass sich die Grenze zwischen Privat- und Gemeinsphäre im Laufe der Zeit verschieben kann[507]. Ob die Pressefreiheit und das öffentliche Interesse eine erneute Berichterstattung über Ereignisse der Vergangenheit rechtfertigen, kann nicht abstrakt festgestellt werden und ist im Einzelfall zu prüfen[508]. Ein möglicher Rechtfertigungsgrund besteht in einer Berichtserstattung, die dem Schutz der Öffentlichkeit dient[509]. Entscheidend ist nebst der Berichterstattung an sich auch, dass diese verhältnismässig erfolgt[510]. Die Notwendigkeit der einzelfallbezogenen Interessenabwägung legt nahe, dass es sich beim Recht auf Vergessen um ein ebenso einprägsames wie unscharfes Instrument handelt, das aus rechtlicher Sicht der Präzisierung bedarf: «Es geht nicht um das Vergessen – dieses entzieht sich der rechtlichen Einflussnahme – sondern um die Unterlassung des öffentlichen In-Erinnerung-Rufens. Im privaten Rahmen ist die Erwähnung zurückliegender Verurtei-

503 BGE 109 II 353; siehe auch BARRELET/WERLY, Rn. 1536.; eingehend TEITLER, 82 ff.; WERRO, 290.

504 BGE 111 II 213 f.

505 AEBI-MÜLLER, Rn. 778; BGE 122 III 449 ff.; HAUSER, 170 ff.; siehe ferner zur Gerichtsberichterstattung BGE 129 III 529 ff., wo darauf hingewiesen wird, dass die Gerichtsberichterstattung einer verlängerten Gerichtsöffentlichkeit diene. Unter Verweis auf BGE 126 III 307 sowie BGE 127 III 489 wird die Namensnennung im Zusammenhang mit dem Verdacht auf eine begangene Straftat bei Personen der Zeitgeschichte – zu denen auch relativ prominente Personen gehören – je nach Interessenlage als gerechtfertigt erachtet. BARRELET/WERLY, Rn. 1538, weisen generell darauf hin, dass umgekehrt auch das Schutzinteresse des Betroffenen über die Zeit abnehmen kann.

506 BRÜCKNER, Rn. 498.

507 HAUSHEER/AEBI-MÜLLER, Rz. 12.118; BGE 122 III 454; GLAUS, Wort, 55; AMBROSE, 381; WEBER, Forgotten, Rn. 3.

508 MEILI, in: Honsell/Vogt/Geiser, Art. 28 N 52; BARRELET/WERLY, Rn. 2252.

509 BRÜCKNER, Rn. 498.

510 LÜCHINGER, 326.

lungen zulässig, sofern nicht die Schranke der Ehrverletzung gemäss Art. 173 ff. StGB überschritten wird[511].»

b) Verjährung als vergleichbares Konzept

Der Informatikprofessor FRIEDEMANN MATTERN wies darauf hin, dass bei der Verjährung die «Gnade der Zeit» von Bedeutung sei und Vergessen auch mit Verzeihen zu tun habe[512]. Dieser Bezug ist zu relativieren, denn wer vergessen hat, kann nicht mehr verzeihen und wer verziehen hat, muss nicht vergessen. Aus rechtlicher Sicht besteht zwischen dem Recht auf Vergessen und der Verjährung trotz der unterschiedlichen Ausgestaltung eine deutliche Parallele; beide Mechanismen haben letztlich zum Ziel, die Nutzung bzw. Geltendmachung noch bestehender und an sich auch richtiger Informationen zu begrenzen[513]. Aus der normativen Umsetzung der Konzepte lässt sich indessen auch ein deutlicher Unterschied ableiten. Das Recht auf Vergessen ist Ausfluss des allgemeinen Persönlichkeitsrechts in Art. 28 ZGB und nicht explizit im materiellen Recht geregelt. Die Verjährung dagegen ist Bestandteil des materiellen Rechts und beansprucht nach Massgabe ihres materiellen Gehalts absolute Geltung[514]. Eine solche kann das Recht auf Vergessen nicht beanspruchen, es unterliegt der richterlichen Interessenabwägung im Einzelfall. Vor diesem Hintergrund ist auch die Durchsetzbarkeit beider Konzepte unterschiedlich. Die Durchsetzung der Verjährung gestaltet sich verhältnismässig einfach, da das zuständige Gericht (vorbehältlich erfolgreicher Einreden der Gegenpartei) diese unmittelbar durchsetzen und einen Anspruch als verjährt beurteilen kann. Beim Recht auf Vergessen richtet sich der Anspruch dagegen an die Verfahrenspartei bzw. im Hinblick auf die Möglichkeit der weiteren Verbreitung von Inhalten an beliebige Dritte. Eine Identität mit der rechtsanwendenden Instanz besteht nicht. Die effektive Durchsetzung des Rechts auf Vergessen kann daher im Unterschied zur Verjährung nicht absolut gewährleistet werden.

511 BRÜCKNER, Rn. 498, Fn. 60.

512 MATTERN, Menschenrechte, 332.

513 HUGUENIN/THOUVENIN, 306, die Forderung erlischt mit Eintritt der Verjährung nicht, sondern verliert ihre Durchsetzbarkeit entgegen dem Willen des Schuldners; anders die Verwirkung; siehe dazu BGE 133 III 6 ff.; GAUCH/SCHLUEP/EMMENEGGER, Rn. 3386; DÄPPEN, in: Vogt/Honsell/Wiegand, Vor Art. 127-142 N 3. Zum Recht auf Vergessen: Sofern eine Information nicht korrekt ist, nimmt Art. 5 DSG die Anwendung des Rechts auf Vergessen vorweg.

514 Im kontinentalen Zivilrecht besteht – anders als in England – ein weitgehender Konsens, dass die Verjährung materiell- und nicht formellrechtlicher Natur ist; siehe dazu ZIMMERMANN, 69 ff.; HUGUENIN/THOUVENIN, 306, m.w.H.

2. Datenschutzrecht

2.1 Konzeption

a) Ausgestaltung

Das DSG bezweckt gemäss Art. 1 DSG den Schutz der Persönlichkeit und der Grundrechte der Personen, über die Daten bearbeitet werden. Entsprechend regelt das DSG sowohl die Datenbearbeitung im öffentlich-rechtlichen (Grundrechtsschutz) als auch im privatrechtlichen Bereich (Persönlichkeitsschutz)[515]. Der 2. Abschnitt des DSG enthält allgemeine Datenschutzbestimmungen, die sowohl für Private als auch für Bundesorgane gelten. Die wichtigsten Bestimmungen finden sich wie bereits erwähnt in Art. 4 Abs. 1-4 DSG, da sich die anderen Bearbeitungsgrundsätze von diesen ableiten lassen[516]. Der privatrechtliche Teil des Datenschutzgesetzes stellt im Verhältnis zu Art. 28 ZGB eine Ergänzung und Konkretisierung dar[517]. Im Zentrum steht der verstärkte Persönlichkeits- und Individualrechtsschutz[518]. Im Unterschied zum Schutz der Persönlichkeit gemäss Art. 28 ZGB begründet das Datenschutzgesetz ein Recht auf «informationelle Selbstbestimmung»[519]. Die Autonomie hinsichtlich der Verbreitung individualisierter Information soll unabhängig von ihrem konkreten Inhalt gestärkt werden, der Persönlichkeitsschutz wird dadurch gewissermassen vorverlagert[520]. Der Berührungspunkt der Schutzbereiche ist die Persönlichkeit, deren Entstehung in Form der Indivi-

---

515 ROSENTHAL, Handkommentar DSG, Art. 1 N 1.

516 ROSENTHAL, Handkommentar DSG, Art. 4 N 1.

517 BBl 1988 II 458, Ziff. 221.3; siehe auch Art. 15 Abs. 1 DSG; BGE 127 III 493; RIEMER, Persönlichkeitsrechte, 104 f.

518 Grundrechtlich ist die persönliche Freiheit (Art. 10 Abs. 2 und 13 Abs. 2 BV) sowie das Recht auf Privatsphäre und das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 1 und 2 BV) gemeint; siehe dazu MAURER-LAMBROU/KUNZ, in: Maurer-Lambrou/Vogt, Art. 1 N 15 ff., m.w.H.; kritisch AEBI-MÜLLER; Rn. 46 ff., 344 ff., 371 ff.

519 HAUSHEER/AEBI-MÜLLER, Rz. 12.123 f. Der Begriff der informationellen Selbstbestimmung wurde vom Bundesverfassungsgericht im Volkszählungsurteil BVerfG 65, 42 ff. geprägt, erst später wurde dieses Recht auch auf den zivilrechtlichen Persönlichkeitsschutz übertragen; siehe dazu AMELUNG, 30 ff.; siehe zur Entwicklung aus dem deutschen Recht WEBER, Grundrechtskonzeptionen, 15 ff. m.w.H.; kritisch im Hinblick auf den umfassenden Schutzbereich und die undifferenzierte Übernahme aus dem deutschen Recht AEBI-MÜLLER, Rn. 595 ff.; siehe ferner die Kritik zum Begriff bei RUDIN, 248 f., der auf den falschen Eindruck der beliebigen Verfügungsmöglichkeit über die eigenen Daten verweist und den Schutz der «informationellen Integrität» als zutreffender erachtet; siehe im deutschen Recht u.a. die Kritik bei BULL, 28, m.w.H., der den breiten Ansatz trotz der «ständigen Wiederholung» des Verfassungsgerichts als nicht zielführend erachtet.

520 Der Wortlaut des Zweckartikels im BDSG ist hierbei im Vergleich zu jenem des DSG aufschlussreicher, § 1 Abs. 1 BDSG: «Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.». Verhindert werden soll damit die Beeinträchtigung, nicht die Verletzung; siehe dazu VON LEWINSKI, 199; kritisch BULL, 26.

dualität von der Art und den Möglichkeiten der Selbstdarstellung abhängt[521]. Die betroffene Person soll nicht nur darüber entscheiden, ob, wann und in welchem Umfang die persönlichen Lebenssachverhalte an die Öffentlichkeit gelangen, sondern generell über den Gegenstand und den Umfang der Datenbearbeitung durch Dritte[522]. Dabei handelt es sich wie dargelegt nicht um absolute, uneingeschränkte Herrschaftsrechte im Sinne eines Eigentumsrechts, sondern um eine Verfügungsmacht über die persönlichen Daten, die als der betroffenen Person eigen erachtet werden können[523]. Im Gegensatz zum Persönlichkeitsschutz gemäss Art. 28 ZGB bildet entsprechend nicht die Persönlichkeitsverletzung die Grenze für erlaubte Datenbearbeitungen, sondern das Resultat einer in Bezug auf die Eingriffsintensität deutlich tieferen und pauschaleren Interessenabwägung[524].

b) Relevanz des Personenbezugs

Die Bundesverfassung sieht in Art. 13 Abs. 2 BV vor, dass jede Person vor dem Missbrauch ihrer persönlichen Daten zu schützen ist. Der Verfassungs- und entsprechend auch der Gesetzgeber hat damit den Begriff des Personendatums zur Voraussetzung der Anwendbarkeit des Datenschutzgesetzes gemacht[525]. Trotz dieser Relevanz handelt es sich beim Personenbezug um ein Kriterium mit unscharfen Konturen[526]. Die Bestimmbarkeit einer Person ist abhängig vom jeweiligen Kontext und kann nicht abstrakt definiert werden[527]. Eine eindeutige Kategorisierung von Personendaten kann zudem nicht mit der technologischen Entwicklung Schritt halten[528]. Das Problem besteht im stetigen Wachstum dieser Kategorie. So ist beispielsweise vor einigen Jahren niemand davon ausgegangen, dass Filmbewertungen zu Personendaten werden könnten[529]. Eine mögliche Lösung besteht in einem grundsätzlich umfassenden Verständnis des Personenbe-

521 Siehe dazu LUHMANN, 48 ff.

522 Vgl. WEBER, Schutz, 74, m.w.H.

523 WEBER, Schutz, 74 f.

524 AEBI-MÜLLER, Rn. 595 ff.; VON LEWINSKI, 199; vgl. im Zusammenhang mit dem deutschen Gesetzgebungsprozess LIEDTKE, 131, sowie kritisch ders., 194 f.

525 PROBST, 1424, zu weiteren Rechtsordnungen ders., 1427 ff.; siehe auch BGE 136 II 522; vgl. ferner die Regelung in der EU, wonach gemäss. Art. 16 AEUV jede Person das Recht «auf Schutz der sie betreffenden personenbezogenen Daten» hat.

526 Vgl. dazu PROBST, 1425, 1427; siehe für einen differenzierten Ansatz LEENES, 147 ff.

527 Siehe beispielsweise im Zusammenhang mit Suchmaschinen Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, April 4, 2008, 9, wonach IP-Adressen und Cookies, die eine personenbezogene Zuordnung von Suchen ermöglichen, als personenbezogene Daten zu behandeln sind. Siehe zu den IP-Adressen ferner SOLOVE, Reputation, 147; LEENES, 143 f.; zu den Cookies ROSENTHAL, Handkommentar DSG, Art. 3 N 23, N 40; LEENES, 142 f.

528 MAYER-SCHÖNBERGER/CUKIER, 192.

529 OHM, 1742.

zugs. Im Rahmen dieser Betrachtung weisen Daten, die letztlich von Menschen in irgendeiner Weise als Informationen interpretiert werden[530] oder mit ihnen irgendwie in Verbindung stehen, immer einen Personenbezug auf. Eine Verbindung ist auch bei rein sachlichen Daten gegeben, die zumindest die Aussage zulassen, dass sie von jemandem erstellt oder wahrgenommen worden sind[531]. Im Rahmen einer solchen umfassenden Interpretation wäre jedoch die Anwendbarkeit von auf diesem Kriterium basierenden Datenschutzgesetzen *immer* gegeben[532].

Für Daten, die als personenbezogen qualifiziert werden, ist der Vorgang der Anonymisierung von entscheidender Bedeutung[533]. Durch die Anonymisierung werden die personenbezogenen Merkmale entfernt, danach soll die Herstellung eines Personenbezugs für niemanden mehr möglich sein – auch für den Datenbearbeiter nicht[534]. Das Konzept der Anonymisierung wird teilweise als gescheitert kritisiert. Gemäss SCHWARTZ/SOLOVE gründet der Mythos der Anonymisierung auf einer Vermischung von momentaner Anonymität und der tatsächlichen Unmöglichkeit der Nachvollziehbarkeit[535]. Das Problem stellt sich für die Autoren insbesondere bei der Onlinenutzung. Wo die anonyme Nutzung von Onlinediensten noch relativ einfach gewährleistet werden kann, ist es sehr viel schwieriger, nicht verfolgt zu werden. Ein zentraler Aspekt dieser Verfolgbarkeit liegt für die Autoren in der Zuordnung statischer IP-Adressen zu bestimmten Computern, wodurch die Identifikation des Nutzers sehr viel wahrscheinlicher wird[536]. Mittels dieser IP-Adressen wird zwar eine Zuordnung der über das Internet versendeten Datenpakete zu einem bestimmten Computer möglich, auf die Identität des jeweiligen Nutzers kann aus diesen Adressen aber an sich nicht geschlossen wer-

---

530 Vgl. zur Feststellung wonach Informationen nicht Gegenstand objektiver Existenz sind, sondern stets der Wahrnehmung und Interpretation ihres Empfängers bedürfen vorne A.I.1.1.

531 GIESEN, 551; auf eine beachtenswerte Umkehrung kann aus der Argumentation bei BULL, 26, geschlossen werden, der zumindest eine flüchtige menschliche Wahrnehmung von Information als Voraussetzung ihrer Wirkung gegenüber einem von der Informationsbearbeitung Betroffenen anführt.

532 Kritisch in Bezug auf die Ausweitung, PROBST, 1436 f.; siehe zur Ausweitung des Begriffs auch EGGIMANN/TAMÒ, 64 f., 76.

533 Siehe zur Bedeutung der Anonymität und Pseudonymität im Allgemeinen HETCHER, 288 f.

534 ROSENTHAL, Handkommentar DSG, Art. 3 N 35. Ein typisches Beispiel für solche Daten sind Forschungsergebnisse und Statistiken. Tatsächlich unmöglich ist die Anonymisierung, wenn sich die involvierten Personen gut kennen und aus dem Inhalt auf den Einzelnen geschlossen werden kann; siehe HÄUSERMANN, 59, mit Verweis auf BGE 122 I 153.

535 SCHWARTZ/SOLOVE, 1837.

536 SCHWARTZ/SOLOVE, 1814 ff., 1837 f. Statische IP-Adressen sind einem bestimmten Computer auf Dauer zugeordnet, dynamische IP-Adressen werden dagegen bei jeder Verbindung, die der Computer zum Internet herstellt durch den Provider neu zugewiesen; siehe dazu BGE 136 II 514 f.; eingehend WEBER/FERCSIK SCHNYDER, 579 f.

den[537]. Für den Provider sind auch die dynamischen IP-Adressen zuordenbar[538]. Darüber hinaus werden bei dynamischen IP-Adressen andere Schlüsseldaten wie beispielsweise die E-Mailadresse für eine Identifikation herangezogen[539].

Trotz dieser Vorzeichen, so OHM, war das Vertrauen in die Anonymisierung bis vor kurzem weitgehend intakt[540]. Auch wenn einige Anonymisierungsverfahren die Datenintegrität noch schützen können, ist das Konzept *per se* nicht mehr einfach als wirksam zu erachten. Selbst Spezialisten, die an der Umgehung von Anonymisierungen arbeiten und darin laufend besser werden[541], sind von den Unzulänglichkeiten der Anonymisierung überrascht worden[542]. AOL beispielsweise veröffentlichte Suchanfragen von 650'000 Nutzern. Vor der Veröffentlichung versuchte AOL die Daten durch Entfernung von Namen und IP-Adressen zu anonymisieren. Um den Nutzen für wissenschaftliche Zwecke zu erhalten, wurden die personenbezogenen Daten durch Identifikationsnummern ersetzt, die die Herstellung von Korrelationen erlauben sollten[543]. Dieses Verfahren ermöglichte jedoch auch die Identifikation einzelner Nutzer[544]. Ein weiterer Grund, weshalb die Anonymisierung häufig nicht mehr wirksam ist, liegt entsprechend in der zunehmenden Quantität und Vielfalt vorhandener Daten. Die Kombination und Analyse dieser Daten vereinfachen die Re-Identifikation[545]. OHM plädiert daher für eine Risikoanalyse unter Berücksichtigung der in Frage stehenden Interessen[546]. Die Schwierigkeit einer solchen Analyse besteht in der zielführenden Definition der zu anonymisierenden Daten. So konnte nachgewiesen werden, dass auch vermeintlich nicht zu anonymisierende Daten durch Verbindung eine präzise Bestimmung persönli-

537 PROBST, 1426.

538 Vgl. BVerwG vom 27. Mai 2009, A-3144/2008, E. 2.2.4.

539 ROSEN, Gaze, 163, Fn. 7.

540 OHM, 1701 ff., 1710 ff., 1716; kritisch in Bezug auf die fehlende Schutzwirkung CAVOUKIAN ANN/EL EMAM KHALED, Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy, Information and Privacy Commissioner, Ontario, Canada, June 2011, abrufbar unter: http://www.ipc.on.ca/images/Resources/anonymization.pdf, abgerufen am 24.5.2014.

541 SCHWARTZ/SOLOVE, 1814 ff., 1841 f.

542 OHM, 1701 ff., 1711.

543 Entsprechend den obigen Ausführungen würde es sich hierbei aufgrund der möglichen Identifizierung durch AOL selbst um eine Pseudonymisierung handeln, die Möglichkeit zur internen Re-Identifikation war jedoch im Aussenverhältnis in diesem Fall nicht relevant.

544 Siehe BARBARO MICHAEL/ZELLER TOM JR., A Face is Exposed for AOL Searcher No. 4417749, The New York Times, August 9, 2006, A1; vgl. dazu LEENES, 144.

545 MAYER-SCHÖNBERGER/CUKIER, 154 f.

546 OHM, 1701 ff., 1710 ff., 1776.

cher Merkmale erlauben[547]. Abgesehen von den technischen Grenzen läuft die Anonymisierung häufig auch den sicherheitspolitischen Bestrebungen, insbesondere der Bekämpfung der Internetkriminalität, entgegen[548].

Im Unterschied zur Anonymisierung werden die personenbezogenen Merkmale bei der Pseudonymisierung nicht entfernt, sondern durch eine Zeichenfolge ersetzt, die anhand bestimmter Regeln den ursprünglichen personenbezogenen Daten zugeordnet werden kann. Pseudonymisierte Daten stellen für den Bearbeiter, der die Zuordnungsregel bzw. den Schlüssel kennt, weiterhin personenbezogene Daten dar. Ob und inwieweit der Personenbezug bei bestimmten Verwendungen der Daten im Einzelfall ausgeschlossen werden kann, ist von der konkreten technischen Umsetzung abhängig[549].

2.2 Entwicklung

a) Hintergrund

Der Schutz der Achtung des Privatlebens bzw. der Privatsphäre ist durch Art. 13 Abs. 1 BV gewährleistet. Der Einzelne soll grundsätzlich selbst darüber entscheiden können, was er als Privatsache ansieht und nicht der Öffentlichkeit zugänglich machen will[550]. Die Grundrechtskonzeption geht auf das in den USA von WARREN/BRANDEIS entwickelte «*right to be let alone*» zurück[551]. Nach heutigem Verständnis ist dieser Anspruch der «*Privacy*» zuzuordnen. Der Begriff «*Privacy*» beschreibt einen umfassenden Schutzgegenstand, der den Datenschutz einschliesst, wobei der Begriff teilweise auch synonym für den Datenschutz verwendet wird[552]. Nach anderer Ansicht ist der Begriff der «*Privacy*» jedoch nicht mit dem Datenschutz gleichzusetzen[553]. Im deutschen Sprachraum weit verbreitet ist der Oberbegriff «Privatheit», der zur Erfassung der informationellen Aspekte weiter einer «informationellen Privatheit» zugeordnet werden

547 KOSINSKI/STILLWELL/GRAEPEL, 5802 ff.; siehe zur Verknüpfung anonymisierter Gesundheitsdaten mit Daten aus öffentlichen Registern SWEENEY/ABU/WINN, 1, 4.

548 AZZABI, 51 f.

549 ROSENTHAL, Handkommentar DSG, Art. 4 N 36.

550 Vgl. WEBER, Grundrechtskonzeptionen, 13.

551 WEBER, Grundrechtskonzeptionen, 13; siehe dazu WARREN/BRANDEIS, 205, mit Verweis auf MCINTYRE COOLEY THOMAS, A Treatise on the Law of Torts, 2 ed., 1888, 29. Bereits 1834 hielt der U.S. Supreme Court in *Wheaton v. Peters*, 33 U.S. 591, 634 (1834) fest: «The defendant asks nothing – wants nothing, but to be let alone until it can be shown that he has violated the rights of another».

552 SCHIEDERMAIR, 17.

553 SCHWARTZ/SOLOVE, 1814. Der Supreme Court wiederum hielt in *Doe v. City of New York*, 15 F.3d 264 (1994) einstimmig fest, dass er zwischen zwei verschiedenen Seiten der Privatsphäre unterscheidet: Eine ist das Recht grundlegende Entscheidungen ohne übermässige externe Einflüsse treffen zu können. Die zweite Seite betrifft Rechte, Herrschaft und Verpflichtungen in Bezug auf die Vermeidung der Offenlegung von Daten; siehe dazu BRIN, 72.

kann, der wiederum der Datenschutz zuzuordnen ist[554]. In der Schweiz hat das in den Neunzigerjahren aufgekommene Bedürfnis im Bereich des Datenschutzes zu einem verfassungsrechtlichen Schutz gegen den Missbrauch persönlicher Daten gemäss Art. 13 Abs. 2 BV geführt[555]. Dieses Grundrecht schützt das Recht des Einzelnen, darüber zu entscheiden, wann, wem gegenüber und in welchem Umfang er auf seine Person bezogene Informationen offenbaren möchte[556]. Dieses Recht schützt die – in der Schweiz begrifflich uneinheitlich verwendete – informationelle Selbstbestimmung[557].

Die wichtigsten Faktoren für das Aufkommen gesetzlicher Regelungen zum Datenschutz in Europa sind die technologischen Entwicklungen, veränderte Geschäftsmodelle, der historische Missbrauch von Datensammlungen und Bedenken hinsichtlich der Blockade grenzüberschreitender Datenflüsse[558]. Insbesondere die digitalisierte Speicherung und Verarbeitung von Personendaten und die damit potentiell verbundenen Risiken haben den Schutz des Privatlebens verstärkt in den Fokus gerückt und zur Entwicklung des Datenschutzgesetzes beigetragen[559]. Die aktuellen und potentiellen Bedrohungen durch die Nutzung von Personendaten haben im Zuge dieser Entwicklung in quantitativer und qualitativer Hinsicht zugenommen. In der Schweiz hat der Gesetzgeber diesen Bereich 1993 daher ergänzend durch das Datenschutzgesetz geregelt, das sowohl die Datenbearbeitung durch private Personen als auch durch Bundesorgane erfasst[560]. Die Regelung des Datenschutzes für den privaten und den öffentlichen Sektor im gleichen Gesetz war dabei nicht von Beginn weg gegeben[561]. Historisch betrachtet blieb das informationelle Gleichgewicht zwischen Privaten anders als im öffentlichen Bereich auch nach Beginn der Neuzeit vorerst unverändert. Bedingt durch die Verfügungsmacht über Produktionsmittel waren die Ungleichgewichte unter Privaten sozia-

554 Siehe dazu AEBI-MÜLLER, Rn. 489, 506 ff., 546; HÄUSERMANN, 88, Fn. 63.

555 WEBER, Grundrechtskonzeptionen, 14.

556 WEBER, Schutz, 74 f.

557 WEBER, Grundrechtskonzeptionen, 14, mit Verweis auf BGE 120 II 118; BGE 122 I 153; BGE 127 III 481; siehe zum Begriff vorne B.II.2.1 a).

558 MCDONAGH, 147.

559 Der Datenschutz überträgt die von WARREN/BRANDEIS entwickelten Ideen gewissermassen ins Computerzeitalter, HELLER, 74. Siehe eingehend zur Entstehung des Datenschutzgesetzes SEETHALER, in: Maurer-Lambrou/Vogt, Entstehungsgeschichte des Datenschutzgesetzes, N 1 ff.; VON LEWINSKI, 196 ff. Siehe zum Gesetzgebungsprozess in der Schweiz PETER, Datenschutzgesetz, 59 ff.

560 BBl 1988 II 444; NABHOLZ, 1 ff.

561 Siehe FORSTMOSER, 5 f., wonach die Zusammenführung der ursprünglich separaten Gesetzesentwürfe für den privaten und den öffentlichen Bereich nicht aus systematischen Gründen erfolgt sei, sondern aus dem politischen Kalkül, wonach sich ein Gesetz einfacher durch das Parlament bringen lasse als zwei. Siehe zur Geltung des Gesetzes im privaten und im öffentlichen Bereich ferner AMMANN, 239.

ler und wirtschaftlicher Natur. Erst ab 1900 führten der Distanzhandel und die Erschliessung von Massengeschäften zu Informationsproblemen im Handel[562]. Die Unternehmen waren nicht mehr in der Lage ihre Geschäfte und das unternehmerische Risiko durch die Kenntnis ihrer Geschäftspartner zu steuern[563]. Zur Überbrückung dieser Informationsdefizite wurden Informationssysteme geschaffen, deren sich Lieferanten und Kreditgeber bedienen konnten[564]. In den USA führte die Entwicklung von Kreditdaten zwischen 1965 und 1970 zu umfassenden Debatten hinsichtlich der Gefährdung der Privatsphäre. Aufgrund dieser Befürchtungen wurde 1968 der *Fair Credit Reporting Act* erlassen, der nebst einem Einsichtsrecht die Möglichkeit zur Korrektur, Löschung oder, bei umstrittenen Einträgen, die Möglichkeit der Anbringung eines Vermerks vorsieht[565]. Auch in Deutschland bestand eine wesentliche Neuerung gegenüber den damals vorliegenden Datenschutzgesetzen darin, dass der Entwurf zum BDSG von 1973 auch Vorschriften für private und insbesondere kommerzielle Datenverarbeitungen vorsah. Diese Erweiterung des Anwendungsbereichs wurde zur Gewährleistung eines umfassenden Schutzes der Bürger als unerlässlich erachtet[566]. Einerseits wurde davon ausgegangen, dass die von Unternehmen bewirtschafteten Datensammlungen die Privatsphäre im gleichen Umfang gefährden würden, wie jene durch Einrichtungen des öffentlichen Rechts. Andererseits wurde befürchtet, dass die öffentlichen Stellen auf privatwirtschaftliche Organisationsformen ausweichen würden, falls dadurch die einschränkenden Vorschriften umgangen werden könnten[567].

b) Reformbestrebungen

(1) Schweiz

In der Schweiz wurde das DSG Ende 2011 einer Evaluation unterzogen[568]: In seinem Bericht stellt der Bundesrat fest, dass sich die Bedrohungen für den Datenschutz aufgrund der technologischen und gesellschaftlichen Entwicklungen verschärft hätten. Als zentral werden insbesondere die Zunahme der Datenbearbeitungen, die Intransparenz und die grenzüberschreitende Datenbearbeitung angesehen. Im Weiteren sei es zunehmend schwieriger, die Kontrolle über einmal bekannt gegebene Daten zu behalten. Die

562 VON LEWINSKI, 213.
563 MEISTER, 55 ff.
564 VON LEWINSKI, 213.
565 WESTIN/BAKER, 134 ff.
566 DAMMANN et al., 143, mit Verweis auf den Entwurf zum BDSG nach dem Stand vom 25.5.1973, Bundesrats-Drucksache 391/73.
567 DAMMANN et al., 143 f.
568 BBl 2012 335 ff.

einklagbaren Rechte werden als nur beschränkt wirksam erachtet, da sie von den Betroffenen nur selten genutzt würden. Mögliche Erklärungen dafür werden in der eher geringen Bekanntheit der Durchsetzungsmöglichkeiten sowie im beträchtlichen Aufwand einer Klage, der einem «diffusen und nicht gesicherten Nutzen» gegenübersteht gesehen. Die Schaffung einer Aufsichtsbehörde (EDÖB) wird grundsätzlich als wirksames Instrument eingestuft, die Wirksamkeit wird allerdings in verschiedener Hinsicht als begrenzt erachtet. Die Ergebnisse der Evaluation veranlassten den Bundesrat einen allfälligen Handlungsbedarf für die Verbesserung des Vollzugs bzw. für Anpassungen am DSG zu prüfen. Die Entwicklungen in der EU sollten berücksichtigt werden.

(2) Europäische Union

Auf europäischer Ebene wird das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation in Art. 7 der Europäischen Grundrechtscharta statuiert, währen Art. 8 der Grundrechtscharta eine spezielle Regelung zum Schutz personenbezogener Daten enthält[569]. Art. 7 der Grundrechtscharta soll den gleichen Schutzumfang wie Art. 8 der Europäischen Menschenrechtskonvention aufweisen[570]. Ferner sieht Art. 16 Abs. 1 AEUV vor, dass jede Person das Recht auf einen Schutz der sie betreffenden personenbezogenen Daten hat. Am 25. Januar 2012 veröffentlichte die EU-Kommission einen Vorschlag für einen neuen Rechtsrahmen zum Schutz personenbezogener Daten (E-DSVO)[571]. Die EG-Datenschutzrichtlinie RL 95/46/EG soll damit durch eine Datenschutz-Grundverordnung ersetzt werden, die in den Mitgliedstaaten unmittelbar anwendbar ist. Auf Basis der bisherigen Zielsetzungen des europäischen Datenschutzrechts wird eine verstärkte Harmonisierung des Rechts in den einzelnen Mitgliedstaaten angestrebt. Die Grundverordnung soll die Wirkung des Datenschutzes durch verschiedene neue Instrumente verbessern. Einige der wichtigsten Vorschläge der Kommission gründen auf der Annahme, dass der Datenschutz in Anbetracht der wachsenden Sammlung und Zugänglichkeit personenbezogener Daten der Stärkung bedarf.

In zeitlicher Hinsicht sind zwei Vorschläge relevant: Erstens das Recht auf «Vergessenwerden und auf Löschung» in Art. 17 E-DSVO, das den Betroffenen einen Anspruch auf Unterlassung der Datenbearbeitung bzw. auf Löschung gewähren soll, wenn die Daten nicht mehr für einen rechtmässigen Zweck gebraucht werden. Das ist nach Ansicht der Kommission beispielsweise dann der Fall, wenn die Datenbearbeitung

569 LAUBER-RÖNSBERG, in: Götting/Schertz/Seitz, § 62 N 7.

570 Erläuterungen zur Charta der Grundrechte, ABl C 303/02, 20.

571 Europäische Kommission, KOM(2012) 11 endgültig.

durch Zustimmung legitimiert ist und die betroffene Person ihre Zustimmung zurückzieht oder wenn die Pflicht zur Speicherung abgelaufen ist[572]. Zweitens soll die Übertragbarkeit von Daten durch das «Recht auf Datenübertragbarkeit» gemäss Art. 18 E-DSVO gewährleistet werden. Nutzer sollen ihre Daten uneingeschränkt von einem Dienst zurückholen und auf eine andere Anwendung übertragen können[573]. Damit würde eine längerfristige Bearbeitung von Daten durch den gleichen Anbieter über ein identisches Individuum gegebenenfalls seltener. Eine dahingehende Wirkung der Regelung ist zum jetzigen Zeitpunkt aber weitgehend ungewiss.

2.3 Zeitliche Dimension im Allgemeinen

a) Zeitbezogene Aspekte der Bearbeitung

(1) Verhältnismässigkeit

Gemäss Art. 4 Abs. 2 DSG muss die Bearbeitung von Personendaten nach Treu und Glauben erfolgen und verhältnismässig sein. Der in Art. 4 Abs. 2 DSG enthaltene Grundsatz, wonach jede Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen hat, dient als Generalklausel. Relevant wird diese Bestimmung beispielsweise bei Datenschutzpannen in Form von Datenverlusten oder ungewollten Offenlegungen[574]. Von zentraler Bedeutung ist das Verhältnismässigkeitsgebot, wonach Personendaten nur insoweit bearbeitet werden dürfen, wie dies für einen bestimmten Zweck nach objektiven Kriterien geeignet und effektiv erforderlich ist[575]. Der Grundsatz für staatliches Handeln aus Art. 5 Abs. 2 BV ist damit im Anwendungsbereich des DSG auch für Private verbindlich[576]. In der Datenschutzrichtlinie ist dieser Grundsatz in Art. 6 lit. e) RL weiter konkretisiert worden. Danach dürfen personenbezogene Daten nicht länger aufbewahrt werden, als es für die Erfüllung des Zwecks, für den sie erhoben oder weiterverarbeitet werden, erforderlich ist. Die zeitliche Beschränkung dieser Aufbewahrung gilt im Sinne der Definition personenbezogener Daten in Art. 2 lit. a) RL

572 Europäische Kommission, KOM(2010) 609 endgültig, 8.

573 Europäische Kommission, KOM(2010) 609 endgültig, 8; kritisch zum Konzept der freien Datenübertragbarkeit im Zusammenhang mit sozialen Netzwerken GRIMMELMANN, 1194 ff., der im Wesentlichen feststellt, dass die Daten dort auch andere Nutzer betreffen würden und eine autonome Übertragung der Daten durch einzelne Nutzer auch eine Ablösung von den rechtlichen, technischen und sozialen Rahmenbedingungen der ursprünglichen Plattform zur Folge habe.

574 ROSENTHAL, Handkommentar DSG, Art. 4 N 14 ff.

575 ROSENTHAL, Handkommentar DSG, Art. 4 N 19 ff.

576 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 23, m.w.H.; siehe auch BBl 1988 II 450, wonach durch das DSG «das im öffentlich-rechtlichen Bereich ohnehin geltende Verhältnismässigkeitsprinzip auch für den privaten Bereich als anwendbar erklärt» wird.

jedoch nur für Formen, die auch eine Identifizierung der betroffenen Personen ermöglichen.

(2) Zweckbindung

Der Zeitbezug der Zweckbindung besteht in der Fixierung eines zum Zeitpunkt der Datenerfassung erkennbaren Zwecks. Der Zweckbindungsgrundsatz nach Art. 4 Abs. 3 DSG gilt als wesentlichste Voraussetzung für die Wirksamkeit des Datenschutzes[577]. Der Grundsatz ist Ausfluss von Treu und Glauben im Rechtsverkehr[578]. Die Zweckbindung in Art. 4 Abs. 3 DSG sieht vor, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde oder aus den Umständen ersichtlich ist. Dadurch soll sichergestellt werden, dass bereits aus der Datenbeschaffung klar hervorgeht, wofür die entsprechenden Daten verarbeitet werden[579]. Das Sammeln von Daten auf Vorrat ist daher sowohl unverhältnismässig als auch ein Verstoss gegen die Zweckbindung[580]. Dem Konzept liegen zwei Prinzipien zugrunde: Personendaten dürfen nur für spezifische, explizite und legitime Zwecke gesammelt und in keiner mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden[581]. Eine Konkretisierung des Zweckbindungsgebots erfolgt beispielsweise im Arbeitsrecht. Nach Art. 328b OR darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, wenn sie die Eignung für das Arbeitsverhältnis betreffen oder im Rahmen der Erfüllung des Arbeitsvertrages erforderlich sind. Für abweichende Zwecke darf der Arbeitgeber Personendaten seiner Arbeitnehmer nicht bearbeiten, auch wenn dadurch keine Persönlichkeitsverletzung begangen wird[582].

(3) Transparenz und Erkennbarkeit

Der Grundsatz der Erkennbarkeit der Datenbeschaffung gemäss Art. 4 Abs. 4 DSG soll die Transparenz und entsprechend die Entscheidungsgrundlage im Hinblick auf die Zu-

577 SIMITIS, Daten, 484; BBl 1988 II 433, 449, 459. Die Zweckbindung entstammt der von KAMLAH im Nachgang zu zwei Entscheiden des BVerfG formulierten «Entfremdungsregel»; siehe dazu STEINMÜLLER et al., 37 f., die im Rahmen allgemeiner Grundsätze für das private Datenschutzrecht indessen nur vorsehen, dass durch Vertrag und Einwilligung auch Individualdaten verarbeitet werden dürfen, die zur Abwicklung des Vertrags notwendig bzw. von der Einwilligung umfasst sind; siehe STEINMÜLLER et al., 142. Siehe für den Zusammenhang mit dem Erfordernis der Normenklarheit im öffentlichen Recht HOFFMANN, 18 ff., insbesondere mit Hinweis auf BVerfGE 65, 1, 46; kritisch hinsichtlich einer Übertragung der Zweckbindung ins private Recht WOERTGE, 141 f.

578 BBl 1988 II 451.

579 ROSENTHAL, Handkommentar DSG, Art. 4 N 31 ff.

580 ROSENTHAL, Handkommentar DSG, Art. 4 N 31.

581 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, April 2, 2013.

582 BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, § 8 Rn. 73.

stimmung oder Ablehnung einer Datenbearbeitung verbessern. In zeitlicher Hinsicht muss die Beschaffung grundsätzlich dann erkennbar sein, wenn sie effektiv stattfindet[583]. Dieser Grundsatz gilt jedoch nicht absolut, es genügt, wenn die Beschaffung für die betroffene Person in Bezug auf den Zeitpunkt und die Umstände absehbar ist[584]. Im Einzelfall kann eine vorgängige Ankündigung genügen. Diesen Aspekt hat das Bundesgericht im Entscheid zu Google Street View konkretisiert[585]. In formaler Hinsicht stellt das Bundesgericht fest, dass die Ankündigung im Internet eine Woche im Voraus die erforderliche Erkennbarkeit nicht gewährleiste. Mit der Vorinstanz geht das Bundesgericht davon aus, dass die Bekanntgabe in den lokalen Medien hätte erfolgen müssen[586]. Obwohl diese Anforderungen relativ hoch sind, dienen sie meines Erachtens auch den Datenbearbeitern. Einerseits wird dadurch das Vertrauen in eine transparente und erkennbare Datenbearbeitung gefördert. Andererseits können Konflikte und damit verbundene Kosten für die juristische Klärung derselben vermieden werden. Die Zeitspanne zwischen Ankündigung und Beschaffung steht in Abhängigkeit zur Sensitivität der Daten; je heikler die Daten, desto zeitnäher muss informiert werden[587]. Das gilt meines Erachtens aber nur, wenn die Zeitnähe der Erinnerung dient. Ein überraschender und unerwarteter Hinweis auf die Beschaffung von Personendaten würde der Transparenz und Erkennbarkeit zuwiderlaufen. Von dieser zeitlich formalen Perspektive ist die zeitlich materielle Perspektive zu unterscheiden, die die Transparenz über die tatsächliche Speicherdauer zum Inhalt hat[588].

(4) Datenrichtigkeit

Die Richtigkeit von Daten lässt sich nur anhand objektiv feststellbarer Tatsachen beurteilen; subjektive Werturteile lassen sich kaum als richtig oder falsch einordnen[589]. Der in Art. 5 DSG enthaltene Grundsatz verpflichtet den Datenbearbeiter zur Überprüfung der Richtigkeit der Daten. Ferner müssen alle angemessenen Massnahmen zur Vernichtung oder Berichtigung unrichtiger oder unvollständiger Daten getroffen werden. Im Weiteren sieht Art. 5 Abs. 2 DSG einen Anspruch des Betroffenen auf Berichtigung

583 ROSENTHAL, Handkommentar DSG, Art. 4 N 52.

584 BBl 2003 2124. Unter welchen Umständen die betroffene Person als ausreichend informiert gelten kann ist ein grundlegendes Problem. Der Grenzziehung von SEIDEL, Privatsphäre, 40, wonach «eine wohlverstandene Aufklärung nicht in einer fachgerechten Erklärung technischer Details liegen kann» ist aber zuzustimmen.

585 BGE 138 II 375.

586 BGE 138 II 361.

587 ROSENTHAL, Handkommentar DSG, Art. 4 N 53.

588 Die Dauer der Speicherung kann sich dabei insbesondere aus dem Zweck ergeben und muss verhältnismässig sein; siehe dazu vorne B.II.2.3 a)(1).

589 MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 9.

unrichtiger Daten vor. Unklar ist hier, ob der Datenbearbeiter Dritte, an die er die Daten übermittelt hat, von sich aus auf die Unrichtigkeit der übermittelten Daten hinweisen muss[590]. Diese Frage ist meines Erachtens unter Berücksichtigung der Beziehung zur empfangenden Partei und damit der Verhältnismässigkeit einer Benachrichtigungspflicht zu beantworten.

Die Richtigkeit von Personendaten beurteilt sich im Rahmen von Art. 5 DSG nach dem Zeitpunkt jeder Bearbeitung und nicht nur nach dem Zeitpunkt ihrer Beschaffung. Personendaten, die einst richtig waren, können zu einem späteren Zeitpunkt falsch sein, sofern sich erhebliche Tatsachen geändert haben[591]. Sind solche Daten indessen als historische Daten erkennbar (beispielsweise mittels Datierung) und ohne Anspruch auf die gegenwärtige Richtigkeit bearbeitet worden, liegen im Sinne des Datenschutzgesetzes keine falschen Personendaten vor[592]. Ob und in welchem Umfang Massnahmen gemäss Art. 5 Abs. 1 DSG zu ergreifen sind, bemisst sich nach dem Risiko einer Persönlichkeitsverletzung, das aus der Bearbeitung falscher Daten resultiert[593]. Die Berichtigung von Personendaten hat in einer hinsichtlich ihrer künftigen Verwendung angemessenen Form zu erfolgen. Bei elektronischen Pressearchiven beispielsweise bietet sich eine Verlinkung von Originalbericht und Berichtigung an[594]. In anderer Form kann eine Berichtigung auch durch Komplettierung oder durch teilweise bzw. vollständige Löschung der Daten erfolgen. Ein genereller Löschungsanspruch kann jedoch auch aus Art. 5 Abs. 2 DSG nicht abgeleitet werden[595]. Ein solcher würde im Geschäftsverkehr insbesondere mit den handelsrechtlichen Aufbewahrungspflichten kollidieren[596].

---

590 ROSENTHAL, Handkommentar DSG, Art. 5 N 8, lehnt eine generelle Informationspflicht ausserhalb eines Auftragsverhältnisses mangels Grundlage ab; übereinstimmend mit HUBER, Teilrevision, 208, wird eine Informationspflicht mit strengen Anforderungen an die Verhältnismässigkeit im Einzelfall insbesondere dort bejaht, wo ein erhöhtes Schädigungspotential besteht.

591 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 46; BBl 1988 II 416; BGE 106 Ia 33 ff.

592 ROSENTHAL, Handkommentar DSG, Art. 5 N 2; anders MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 6, wonach eine Korrektur von falschen Einzeltatsachen immer möglich sein muss; siehe dazu auch BGer vom 2.5.2001, 1A.6/2001.

593 ROSENTHAL, Handkommentar DSG, Art. 5 N 9.

594 Siehe dazu La Corte Suprema Di Cassazione, 5525 / 2012.

595 ROSENTHAL, Handkommentar DSG, Art. 5 N 13.

596 ROSENTHAL, Handkommentar DSG, Art. 5 N 13. Wobei dies für die Geschäftskorrespondenz im Rahmen des neuen Rechnungslegungsrechts nur noch dann gilt, wenn diese die Funktion eines Buchungsbeleges hat; siehe dazu hinten E.II.2.2 a).

b) Zeitbezug der Rechtfertigung

(1) Rechtfertigung im Allgemeinen

Im Grundsatz gilt das Gleiche wie bei der Rechtfertigung von Persönlichkeitsverletzungen[597]. Die Besonderheit des Datenschutzgesetzes liegt in den Bearbeitungsgrundsätzen von Art. 4 DSG[598]. Die Verletzung der Bearbeitungsgrundsätze würde nach dem Wortlaut von Art. 12 Abs. 2 lit. a DSG die Möglichkeit einer Rechtfertigung ausschliessen. Nach der herrschenden Lehre und der Rechtsprechung kann die Datenbearbeitung indessen trotzdem im Rahmen von Art. 13 Abs. 1 DSG gerechtfertigt werden[599]. Nach der Rechtsprechung des Bundesgerichts kann das Vorliegen von Rechtfertigungsgründen nur mit grosser Zurückhaltung bejaht werden[600]. Auch in Bezug auf die Erforderlichkeit eines Rechtfertigungsgrundes bestehen unterschiedliche Sichtweisen. Einerseits wird aus Art. 4 Abs. 1 DSG gefolgert, dass jede Bearbeitung von Personendaten durch Private einen Rechtfertigungsgrund erfordert[601]. Als Grund wird angeführt, dass jede Bearbeitung von Personendaten eine Persönlichkeitsverletzung darstelle und daher ohne Rechtfertigungsgrund unrechtmässig sei. Dass dem nicht so ist, kann aus der differenzierten Formulierung der Bearbeitungsgrundsätze durch den Gesetzgeber geschlossen werden[602]. Der rechtliche Zweck von Art. 4 DSG besteht allgemein einzig darin, einer Person den Schutz ihrer Persönlichkeit zu erleichtern, indem die unwiderlegbare Vermutung aufgestellt wird, dass wer gegen die Grundsätze verstösst, die Persönlichkeit der betroffenen Person verletzt hat[603]. Im Weiteren widerspricht die Annahme, wonach jede Datenbearbeitung eine Persönlichkeitsverletzung darstellt, auch der Praxis des Bundesgerichts[604] und jener des Bundesverwaltungsgerichts[605].

---

597 Siehe dazu vorne B.II.1.3 c).

598 Siehe dazu vorne B.II.2.3 a).

599 BGE 138 II 358; BGE 136 II 520 f.; RAMPINI, in: Maurer-Lambrou/Vogt, Art. 13 N 3, m.w.H. Der geltende Wortlaut entstand offenbar durch eine versehentliche Änderung der Formulierung von Art. 12 Abs. 2 DSG durch das Parlament; siehe dazu ROSENTHAL, Datenschutz, Rz. 5; ders., Handkommentar DSG, Art. 12 N 16 ff.; a.A. EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 5 ff., m.w.H., die insbesondere auch der Einwilligung keine rechtfertigende Wirkung zuspricht, da ein öffentliches Interesse an einem ausreichenden und effektiven Datenschutz bestehe und dem Staat eine Schutzpflicht im Hinblick auf Beeinträchtigungen des Grundrechts von Art. 13 Abs. 2 BV zukomme.

600 BGE 138 II 358; BGE 136 II 521.

601 So beispielsweise im Einzelfall wiederholt vom EDÖB vertreten, siehe Tätigkeitsbericht EDÖB 2006/2007, 62; Tätigkeitsbericht EDÖB 2007/2008, 143.

602 ROSENTHAL, Handkommentar DSG, Art. 4 N 12.

603 ROSENTHAL, Handkommentar DSG, Art. 4 N 2.

604 BGE 138 II 357.

605 BVerwG vom 26. Februar 2008, A-4086/2007, E. 5.4.

In zeitlicher Hinsicht besonders relevant ist auch im Bereich des DSG der Rechtfertigungsgrund der Einwilligung. Der datenschutzrechtliche Begriff der Einwilligung ist in Art. 4 Abs. 5 DSG enthalten. Die Bestimmung findet nur dort Anwendung, wo das DSG eine Einwilligung überhaupt erfordert[606]. Grundsätzlich ist eine Einwilligung nicht erforderlich. Das DSG verwirklicht das Konzept der informationellen Selbstbestimmung durch die Definition bestimmter Grundsätze und indem es der betroffenen Person Transparenz-, Widerspruchs- und Korrekturrechte einräumt[607]. Die rechtlich gültige Einwilligung setzt gemäss Art. 4 Abs. 5 DSG eine auf angemessener Information beruhende, freiwillige Zustimmung voraus[608]. Das Erfordernis der angemessenen Information soll sicherstellen, dass die betroffene Person über Gegenstand, Zweck und Umfang der Datenbearbeitung informiert ist[609]. Nach anderer Auffassung ist die Gültigkeit der Einwilligung bereits dann gegeben, wenn sich die betroffene Person bewusst ist, in was sie einwilligt und insbesondere auch die möglichen negativen Folgen ihrer Einwilligung abschätzen kann[610]. Eine angemessene Information ist gegeben, wenn die betroffene Person über alle Informationen, die zu einer freien Entscheidung notwendig sind, verfügt[611]. Entsprechend muss die Einwilligung vor der jeweiligen Datenbearbeitung erfolgen[612].

Die Einwilligung ist nicht an eine bestimmte Form gebunden und kann stillschweigend bzw. durch konkludentes Handeln erfolgen, sofern es nicht um die Bearbeitung besonders schützenswerter Daten oder von Persönlichkeitsprofilen geht[613]. Gemäss dem Verhältnismässigkeitsgrundsatz ist davon auszugehen, dass die Anforderung an die Eindeutigkeit der Zustimmung steigt, je sensibler die Personendaten sind[614]. In der Praxis sind Einwilligungen häufig in Allgemeinen Geschäftsbedingungen und Formularverträgen enthalten, durch deren Annahme die Einwilligung gültig erfolgt[615].

606 BBl 2003 2127.

607 ROSENTHAL, Handkommentar DSG, Art. 4 N 66.

608 RAMPINI, in: Maurer-Lambrou/Vogt, Art. 13 N 4, m.w.H.; ROSENTHAL, Handkommentar DSG, Art. 4 N 67 ff.

609 RAMPINI, in: Maurer-Lambrou/Vogt, Art. 13 N 4; EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 17.

610 ROSENTHAL, Handkommentar DSG, Art. 4 N 72.

611 BBl 2003 2127; ROSENTHAL, Handkommentar DSG, Art. 4 N 67, m.w.H.

612 AEBI-MÜLLER, Rn. 762; siehe auch ROSENTHAL, Handkommentar DSG, Art. 4 N 91.

613 BBl 2003 2127; a.A. ROSENTHAL, Handkommentar DSG, Art. 4 N 77.

614 BBl 2003 2127.

615 ROSENTHAL, Handkommentar DSG, Art. 4 N 90.

(2) Globale Einwilligung und Widerspruchsrecht im Besonderen

Unter Berücksichtigung der dargestellten Anforderungen an eine informierte Einwilligung im Sinne der Kenntnis von Gegenstand, Zweck und Umfang der Datenbearbeitung wäre eine allgemeine Einwilligung in sämtliche künftigen, zum Zeitpunkt der Einwilligung noch nicht bekannten Bearbeitungen nicht möglich. Jedoch soll auch hier eine globale Einwilligung gültig sein, wenn sie informiert und bewusst erteilt wird und Klarheit hinsichtlich ihrer Grenzen besteht[616]. Im Weiteren sind auch hier die Grenzen von Art. 27 Abs. 2 ZGB zu beachten; diese können überschritten sein, wenn keine sachliche Begrenzung erfolgt. Relevant sind insbesondere die Art und Dauer der Bearbeitung[617]. In zeitlicher Hinsicht ist weiter von Bedeutung, wie weit Information und Einwilligung auseinanderliegen dürfen. Dabei sind insbesondere die Umstände und die Schwere der möglichen Folgen massgebend. Abgestellt wird auf zwei Aspekte: Zum einen darf die Zeitspanne nicht so lange sein, dass sich die betroffene Person nicht mehr an die Information erinnert[618]. Zum anderen muss genügend Bedenkzeit zur Erfassung der Information gegeben werden[619]. Hinsichtlich des Widerspruchsrechts ist Art. 12 Abs. 2 lit. b DSG massgeblich, wonach Personendaten ohne Rechtfertigungsgrund nicht gegen den ausdrücklichen Willen des Betroffenen bearbeitet werden dürfen.

c) Zeitbezug der Rechtsansprüche

Die Rechtsansprüche richten sich im Grundsatz nach Art. 28 Abs. 2 ZGB. Soweit das DSG den Persönlichkeitsschutz gemäss Art. 28 ZGB konkretisiert, sind die Normen des DSG und des ZGB kumulativ anwendbar. Das DSG weicht von Art. 28 ZGB insbesondere insofern ab, als dass Art. 15 Abs. 1 DSG auch Ansprüche auf Datenvernichtung und Datensperrung vorsieht[620]. Diese Ansprüche umfassen in Bezug auf den Bestand bzw. die Verbreitung der Daten einen impliziten Zeitbezug.

---

616 RAMPINI, in: Maurer-Lambrou/Vogt, Art. 13 N 5. Im Rahmen von Einwilligungen bei AGB sind die Regeln über deren Auslegung zu beachten, ROSENTHAL, Handkommentar DSG, Art. 4 N 90; zurückhaltend in Bezug auf Einwilligungen im Rahmen von AGB AEBI-MÜLLER, Rn. 764.

617 ROSENTHAL, Handkommentar DSG, Art. 4 N 93.

618 Siehe dazu BBl 1988 II 416, mit Hinweis auf die Bedeutung des Überblicks für eine von der Datenbearbeitung betroffenen Person sowie auf das Urteil des deutschen Bundesverfassungsgerichts vom 15. Dezember 1983, BVerfGE 65, 43; ROSENTHAL, Handkommentar DSG, Art. 4 N 76.

619 ROSENTHAL, Handkommentar DSG, Art. 4 N 76.

620 BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, § 8 Rn. 71.

2.4 Löschung von personenbezogenen Daten im Besonderen

a) Im öffentlichen Bereich

Im öffentlichen Recht gibt es eine Vielzahl von Normen, die explizit eine Löschung personenbezogener Daten vorsehen[621]. Auf Bundesebene ist in diesem Zusammenhang das Bundesgesetz über die Archivierung (BGA) zu beachten. Gemäss Art. 6 BGA i.V.m. Art. 1 BGA sind die Daten vor ihrer Vernichtung regelmässig dem Bundesarchiv zur Archivierung anzubieten. Die entsprechende Verordnung sieht in Art. 6 Abs. 2 VBGA vor, dass Unterlagen im Zweifelsfall zu archivieren sind. Im Unterschied zum privaten Bereich gilt im öffentlichen Sektor das in Art. 5 Abs. 1 BV enthaltene Legalitätsprinzip, wodurch bereits die Beschaffung von Personendaten entscheidend eingeschränkt wird[622].

b) Unter Privaten

Anders als im öffentlichen Recht, gibt es im Privatrecht keine zeitlich definierten Vorgaben, wann Daten zu löschen sind und somit keinen expliziten Zeitbezug. Der implizite Zeitbezug ergibt sich dagegen aus den erwähnten Rechtsansprüchen auf Sperrung, Vernichtung oder Berichtigung gemäss Art. 15 Abs. 1 DSG. Da die Aufbewahrung und Archivierung von Personendaten Formen des Bearbeitens im Sinne von Art. 3 lit. e DSG darstellen, kann im Rahmen von Art. 12 Abs. 2 lit. b DSG mit dem Widerspruchsrecht die vollständige oder teilweise Löschung von Personendaten gefordert werden[623]. Die Vernichtung als Teil der Beseitigung kann jedoch nur verlangt werden, wenn und soweit für den Beklagten überhaupt noch eine Möglichkeit dazu besteht[624]. Sind die Daten bereits unrechtmässig an einen Dritten weitergegeben worden, kann vom Beklagten immerhin noch verlangt werden, dass er allfällige vertragliche Ansprüche auf Löschung oder Herausgabe geltend macht[625]. Falls das Ziel in der Löschung *falscher* Daten in einer Datensammlung besteht, ist Art. 5 Abs. 2 DSG aus Sicht des Betroffenen vorteilhaft, da sich ein Unternehmen hier, anders als beim Widerspruch,

---

621 Vgl. u.a. Art. 20 Abs. 2 FMedV; Art. 369 StGB; Art. 261 Abs. 3 und 4 StPO; Art. 15 Abs. 1 und 5 BWIS; Art. 149a Abs. 3 SchKG; Art. 25 BPDV; Art. 27b Abs. 7 BPG; Art. 111i Abs. 5 AuG; Art. 123 Abs. 2 VZV.

622 WINTERBERGER-YANG, in: Maurer-Lambrou/Vogt, Art. 21 N 6. Vgl. im US-amerikanischen Recht die Bestimmung des *US Privacy Act* von 1974 zum Erhalt von Daten in Section (o)(F), die vorsieht, dass für Daten die an andere Behörden übermittelt und durch Computer verarbeitet werden, Massnahmen für die Speicherung und die zeitgerechte Löschung zu treffen sind.

623 ROSENTHAL, Handkommentar DSG, Art. 12 N 32.

624 ROSENTHAL, Handkommentar DSG, Art. 15 N 33. Siehe zur Beseitigung generell MEILI, in: Honsell/Vogt/Geiser, Art. 28a N 4.

625 ROSENTHAL, Handkommentar DSG, Art. 15 N 33.

nicht auf einen Rechtfertigungsgrund berufen kann – der Anspruch auf Berichtigung besteht uneingeschränkt[626]. Die Bearbeitung falscher Personendaten kann zu erheblichen Persönlichkeitsverletzungen führen[627].

Im zweiten Satz von Art. 5 Abs. 1 DSG wird der Bearbeiter von Daten, die in Bezug auf ihren Zweck, ihre Bearbeitung oder ihre Beschaffung unrichtig oder unvollständig sind, verpflichtet, alle angemessenen Massnahmen zur Vernichtung oder Berichtigung der Daten zu treffen. Die Bestimmung hängt wiederum mit den Bearbeitungsgrundsätzen aus Art. 4 DSG zusammen[628], da die Beachtung der Grundsätze letztlich die Richtigkeit der bearbeiteten Daten bedingt[629]. Obwohl die Formulierung dies nicht eindeutig zum Ausdruck bringt, ist von einer Pflicht zur Vernichtung auch in jenen Fällen auszugehen, in denen die Daten für den Bearbeitungszweck nicht mehr benötigt werden[630]. Diese Verpflichtung resultiert darüber hinaus auch aus dem Verhältnismässigkeitsgrundsatz[631]. Die bisherige Praxis des Bundesgerichts ist zurückhaltender: «Mangels Vorliegens von unrichtigen Daten erweist es sich von vornherein nicht als erforderlich, gewisse Aktenstücke vernichten zu lassen»[632]. Die Zurückhaltung ist begründet; auch bei einer weitgehend zweckgebundenen Verarbeitung gemäss Art. 4 Abs. 3 DSG lässt sich auf Daten im Einzelfall nicht einfach verzichten, sobald der ursprüngliche Bearbeitungszweck erreicht ist[633]. Dies bereits deshalb, da oft nur anhand der aufbewahrten Daten Vorgänge rekonstruier- und beweisbar bleiben[634].

c) Ansätze zur Konkretisierung

(1) Datenschutzrechtliches Recht auf Vergessen in der EU

Im Hinblick auf das Recht auf Vergessen stellte der Generalanwalt des Europäischen Gerichtshofes Niilo Jääskinen in der Empfehlung vom 25. Juni 2013 an den Gerichtshof fest, dass die Europäische Datenschutzrichtlinie kein allgemeines Recht auf Ver-

---

626 ROSENTHAL, Handkommentar DSG, Art. 5 N 12; MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 2 f.

627 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 45; BBl 1988 II 450; AEBI-MÜLLER, Rn. 542.

628 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 45; MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 2.

629 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 45.

630 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 49; wobei wohl der ursprüngliche Bearbeitungszweck relevant sein dürfte.

631 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 49.

632 BGer vom 2.5.2001, 1A.6/2001, E. 2c.

633 Siehe dagegen PETER, Datenschutzgesetz, 128, wonach die Zweckgebundenheit grundsätzlich eine Vernichtung oder Anonymisierung der Daten nach Erfüllung des Bearbeitungszwecks mit sich bringe.

634 SIMITIS, Gedächtnisverlust, 1488.

gessen enthalte[635]. Gleiches gelte unter Berücksichtigung der Grundrechtscharta[636]. Hintergrund war das Begehren eines Klägers, wonach die elektronischen Versionen zweier Zeitungsberichte über ihn im Suchindex von Google nicht mehr angezeigt werden sollten. Entsprechend klagte er vor dem zuständigen Gericht in Spanien auf ein Recht auf Vergessen gegenüber dem Suchmaschinenbetreiber[637]. Der Europäische Gerichtshof folgte dieser Empfehlung nicht und legte Art. 12 lit. b RL 95/46/EG (Ansprüche auf Berichtigung, Löschung und Sperrung) sowie Art. 14 Abs. 1 lit. a RL (allgemeines Widerspruchsrecht) dahingehend aus, dass der Suchmaschinenbetreiber zu einer Entfernung der Links auf die von Dritten veröffentlichten Internetseiten zu verpflichten ist. Dies auch dann, wenn die Informationen dort nicht gelöscht werden und gegebenenfalls auch, wenn die Veröffentlichung dort rechtmässig ist[638]. Grundlagen des Anspruchs bilden Art. 7 und 8 der Grundrechtscharta[639].

Das «Recht auf Vergessenwerden und auf Löschung» in Art. 17 der neuen E-DSVO ist in einem weiten Sinn zu verstehen. Der Kern dieses Rechts besteht im bereits bekannten Löschungsanspruch gegenüber dem Datenbearbeiter[640]. Entscheidend ist die Rechtsfolge des Normvorschlags in Form der zu unterlassenden Datenbearbeitung. Unter Berücksichtigung der abweichenden Formulierung in Art. 19 Abs. 3 E-DSVO, ist davon auszugehen, dass Art. 17 Abs. 1 E-DSVO einen Unterlassungsanspruch im rechtstechnischen Sinn schafft[641]. Die Unterlassung soll hierbei nach Art. 17 Ziff. 2 E-DSVO auch bei Dritten durch eine Informationspflicht seitens des für die Verarbeitung Verantwortlichen sichergestellt werden. Neu im Vergleich zur bisherigen Tradition des Rechts auf Vergessen und zur Praxis des Bundesgerichts ist die Ausweitung des Anspruchs auf Bereiche ausserhalb des medialen Bereichs, wo sich entsprechend auch der rechtliche Anspruch auf Vergessen bzw. Löschen nicht mehr auf den Verlust des öffentlichen Interesses stützen muss[642]. Nebst der Durchsetzbarkeit der Norm[643] bestehen

635 Opinion of Advocate General Jääskinen, 25 June 2013, Case C-131/12, Nr. 108 ff.

636 Opinion of Advocate General Jääskinen, 25 June 2013, Case C-131/12, Nr. 126 ff.

637 Opinion of Advocate General Jääskinen, 25 June 2013, Case C-131/12, Nr. 5.

638 EuGH vom 13. Mai 2014, C-131/12, Ziff. 3.

639 EuGH vom 13. Mai 2014, C-131/12, Ziff. 4.

640 HARTUNG, 45; MANTELERO, 734 f.; FELDMANN, 675 ff.

641 FELDMANN, 676.

642 Siehe dazu MANTELERO, 736. In Bezug auf die Abgrenzung von Vergessen und Löschen stellt AMBROSE, 386, fest, dass das Recht auf Vergessen gemäss E-DSVO als Spektrum verstanden werden könne, dass auch die Löschung umfasse.

643 Siehe dazu ENISA, The Right to be forgotten – between expectations and practice, 18.10.2011.

insbesondere Bedenken über die Reichweite im Hinblick auf das Recht auf freie Meinungsäusserung[644].

(2) Löschungsanspruch für Minderjährige in Kalifornien

Ein Ansatz der Konkretisierung von Löschungsansprüchen im privaten Sektor lässt sich am Beispiel eines neuen Gesetzes, das in Kalifornien anfangs 2015 in Kraft treten soll, aufzeigen[645]. Nutzer unter 18 Jahren sollen gegenüber Betreibern von Websites und Applikationen, die sich an Minderjährige richten oder von denen der Betreiber weiss, dass Minderjährige sie benutzen, die von ihnen öffentlich verbreiteten Inhalte löschen bzw. die Löschung verlangen können. Eine bedeutende Einschränkung der Anwendbarkeit des Gesetzes liegt neben der Beschränkung auf den Staat Kalifornien und einer allfälligen Verletzung der *Dormant Commerce Clause*[646] sowie dem Recht auf freie Meinungsäusserung darin, dass der Löschungsanspruch nur dann besteht, wenn keine Gegenleistung seitens des Betreibers erfolgt ist. Sofern bereits die Erbringung von Marketing und Vertrieb als Gegenleistungen gelten, wird das Gesetz kaum je Anwendung finden. Eine grosse Gefahr für die Nutzer besteht in der Illusion der Kontrolle über ihre Inhalte. Diese beschränkt sich indessen auf durch die Minderjährigen Nutzer selbst verbreiteten Inhalte und erfasst nicht die Verbreitung der Kopien Dritter, die gerade bei problematischen Inhalten häufig weiterverbreitet werden. Ein zusätzliches Problem besteht in der möglichen Löschung einzelner Inhalte innerhalb eines Gesamtzusammenhangs, beispielsweise bei Diskussionsforen[647].

2.5 Schlussfolgerungen

Das datenschutzrechtliche Konzept der informationellen Selbstbestimmung lässt sich in Anlehnung an die Sphärentheorie inhaltlich unterschiedlich interpretieren. DRUEY wertet die informationelle Selbstbestimmung dahingehend, dass sie «bloss in neuer und etwas zu radikalisierender Weise» die Gestalt des «Geheimnisherrn» ausdrücke, die

644 ROSEN, Forgotten, 89 ff. Hierzu ist anzumerken, dass der Entwurf in Art. 17. Ziff. 3 lit. a E-DSVO Daten, die zur Ausübung des Rechts auf freie Meinungsäusserung erforderlich sind, von der Löschung ausnimmt. Wie diese Grenze zu ziehen sein wird, ist indessen unklar. Siehe zum Ganzen auch die Rechtsvergleichung zwischen dem Recht auf Vergessen in Europa und den USA bei WERRO, 298 ff.

645 Siehe *Senate Bill No.* 568, *an Act to add Chapter* 22.1 (*commencing with Section* 22580) *to Division* 8 *of the Business and Professions Code, relating to the Internet*.

646 Nach dieser Verfassungsdoktrin dürfen die Gliedstaaten der USA keine Regulierung vorsehen, die den interstaatlichen Handel übermässig beeinträchtigen. Die Regulierung dieses Bereichs ist grundsätzlich dem Kongress vorbehalten; siehe dazu BONFIELD, 37 f.

647 GOLDMAN ERIC, California's New «Online Eraser» Law Should Be Erased, Forbes, September 24, 2013, abrufbar unter: http://www.forbes.com/sites/ericgoldman/2013/09/24/californias-new-online-eraser-law-should-be-erased/, abgerufen am 29.01.2014.

auch in die Sphärentheorie eingegangen sei[648]. AEBI-MÜLLER sieht hingegen die Gemeinsphäre als Teil der Sphärentheorie durch das Recht auf informationelle Selbstbestimmung als vollständig aufgelöst, da es grundsätzlich keine Daten mehr gebe, die unabhängig vom Willen des Betroffenen bearbeitet werden könnten[649]. Ungeachtet der Frage nach der Reichweite der informationellen Selbstbestimmung an sich statuiert das Datenschutzgesetz aufgrund seiner Vermutungstatbestände über das Vorliegen einer Persönlichkeitsverletzung (hauptsächlich Art. 4 DSG) insofern ein umfassendes Abwehrrecht, als dass darin zugleich eine Beweislasterleichterung angelegt ist[650]. Auf der Gegenseite müssen insbesondere jene, die den Daten einen wirtschaftlichen Wert zumessen und diesen auch umsetzen können, die Datenbearbeitung unabhängig vom konkreten Umfang der Datenbearbeitung gegebenenfalls rechtfertigen[651]. Insbesondere der Grundsatz der Zweckbindung, der die Zustimmung zu einer klar vordefinierten Datenbearbeitung statuiert, läuft hierbei in Anbetracht einer zunehmend umfangreicheren Datenbearbeitung vermehrt ins Leere[652]. Darin zeigt sich der Konflikt zwischen einem umfassenden Abwehrrecht und dem Ideal der tatsächlichen Selbstbestimmung. Die Einschränkung der Entscheidung des Individuums, Daten auf der Grundlage klarer, unklarer oder nicht vorhandener Informationen über die Verwendung zu übermitteln, erscheint in diesem Zusammenhang als grundsätzlich fragwürdig[653]. In zeitlicher Hinsicht erscheint hierbei beachtenswert, dass personenbezogene Daten nicht nur für Unternehmen, sondern auch aus Sicht des Individuums über die Zeit an Relevanz verlieren können.

Der Ansatz zur Konkretisierung von Löschungsansprüchen im europäischen Recht ist gegenüber dem kalifornischen Ansatz dahingehend zu relativieren, dass ersterer offenbar primär den bereits bestehenden Unterlassungsanspruch konkretisiert. In Bezug auf die Verbreitung von Daten erscheint die Notwendigkeit einer dahingehenden Konkretisierung aufgrund der neusten Rechtsprechung des EuGH indessen als fragwürdig.

---

648 DRUEY, Information, 92 f.

649 AEBI-MÜLLER, Rn. 611.

650 Siehe unter Verweis auf den Vernehmlassungsentwurf BBl 1988 II 427. Siehe zum Problem der Beweislage im allgemeinen Persönlichkeitsrecht und im Rahmen der Entstehung des deutschen Datenschutzgesetzes STEINMÜLLER et al., 136.

651 Vgl. HAUSHEER/AEBI-MÜLLER, Rz. 12.124; siehe auch den Hinweis bei ROSENTHAL, Datenschutz-Compliance, 176, wonach die materiellen Regelungen im Datenschutzrecht auch Bearbeitungen erfassen, die «als selbstverständlich und normal erachtet werden».

652 MELCHIOR, 142; siehe zu diesem Problem auch ROSENTHAL, Datenschutz-Compliance, 165.

653 Siehe WEBER, Moral, 322 f; ROSENTHAL, Bauchgefühl, 81 ff. Siehe in Bezug auf Persönlichkeitsrechte im Allgemeinen BÄCHLI, 127; BÜCHLER, Kommerzialisierung, 347; MEYER, Persönlichkeitsrechte, Rn. 148 ff.; TERCIER, Rn. 621.

3. Ausgewählte weitere Rechtsnormen

3.1 Vertragsrecht

Das Auftragsrecht beinhaltet nach Art. 400 Abs. 1 OR insbesondere eine allgemeine und jederzeitige Rechenschaftspflicht des Beauftragten. Diese Norm dient der Dokumentation gegenüber dem Auftraggeber und ermöglicht diesem die Kontrolle der in Art. 398 OR geforderten, getreuen Ausführung[654]. Sämtliche Informationen, die für den Auftraggeber von Bedeutung sein können, müssen rechtzeitig, wahrheitsgetreu und vollständig an diesen übermittelt werden[655]. In Art. 363 OR als Teil des Werkvertragsrechts findet sich entsprechend keine solche Regelung, dort legt gewissermassen das Werk an sich über die Ausführung Rechenschaft ab.

3.2 Prozessrecht

Abgesehen vom allgemeinen Prinzip von Treu und Glauben im Verfahren sind die Parteien in der Schweiz nicht verpflichtet, potentiell relevante Daten im Hinblick auf ein vernünftigerweise zu erwartendes Verfahren bzw. eine Untersuchung zu erhalten[656]. Die aufgrund der handelsrechtlichen Vorschriften aufzubewahrenden Dokumente sind dagegen eine wichtige Informationsquelle sowohl für zivile Kläger als auch für Behörden. Entsprechend kann ein Gericht oder eine Behörde anordnen, dass solche Daten in einer lesbaren Form eingereicht werden[657]. Die Verweigerung der Mitwirkung wird vom Gericht nach Art. 164 ZPO zum Nachteil der Partei gewürdigt[658].

Insbesondere das US-amerikanische Prozessrecht sieht im Unterschied zum schweizerischen Prozessrecht umfassende Herausgabepflichten vor, die bereits vor Prozessbeginn einsetzen (*Pretrial Discovery*)[659]. Gemäss der US-amerikanischen Zivilprozessordnung (*US Rules of Civil Procedure*) müssen die Parteien eines gerichtlichen Verfahrens ab dem Zeitpunkt, ab dem ein Gerichtsverfahren wahrscheinlich ist, alle potentiell relevanten Informationen aufbewahren[660]. Bei elektronischen Datenbeständen handelt es sich hierbei um die *Electronic Discovery* (*E-Discovery)*. Kritisch sind hier insbeson-

---

654 WEBER, in: Honsell/Vogt/Wiegand, Art. 400 N 2 f.

655 WEBER, in: Honsell/Vogt/Wiegand, Art. 400 N 4, m.w.H.; BGE 112 III 95; BGE 110 II 182.

656 SCHNEIDER/SOMMER/CARTIER, 290; siehe zum Prinzip von Treu und Glauben im Zivilprozess Art. 52 ZPO sowie im Allgemeinen Art. 2 ZGB.

657 SCHNEIDER/SOMMER/CARTIER, 290.

658 HIGI, in: Brunner/Gasser/Schwander, Art. 164 N 7.

659 COOTER/ULEN, 383.

660 ZEUNERT/ROSENTHAL, Rn. 44, bereits die telefonische Androhung eines Gerichtsverfahrens kann zu einer unternehmensinternen Anordnung führen, wonach keine im jeweiligen Zusammenhang relevanten Daten verändert oder vernichtet werden dürfen.

dere die Übermittlung sensitiver Informationen[661] und mögliche Verletzungen lokaler Datenschutzbestimmungen sowie technische und organisatorische Machbarkeitsfragen bei grossen Datenmengen[662]. Aus datenschutzrechtlicher Sicht stehen durch die längere Aufbewahrung der Daten Fragen zur Zweckbindung, zur Transparenz und zur Verhältnismässigkeit der Datenbearbeitung im Vordergrund[663]. Die Erfahrung zeigt jedoch, dass durch die Anwendung von Verfahren, durch die nur für den jeweiligen Zweck tatsächlich benötigte Daten übermittelt werden und die gleichzeitig eine Entfernung oder Redaktion der Daten nur dann vorsehen, wo dies zum Schutz von Angestellten, Kunden oder Dritten tatsächlich notwendig ist, ein Kompromiss möglich ist[664]. In organisatorischer Hinsicht sollte ein multinational tätiges Unternehmen interne Strukturen, Verfahren und Verantwortlichkeiten schaffen, die die *E-Discovery* als grundlegende Unternehmensfunktion unabhängig von einer spezifischen Rechtssache zum Gegenstand haben. Dadurch können die Kosten gesenkt und die *E-Discovery* gegebenenfalls als taktischer Vorteil genutzt werden[665].

4. Fazit

Durch das Persönlichkeitsrecht können der Bestand und die Verbreitung von Informationen über die eigene Person beeinflusst werden. Diese Abwehrrechte werden im Datenschutzgesetz insbesondere durch Vermutungstatbestände hinsichtlich persönlichkeitsverletzender Datenbearbeitungen erweitert. In zeitlicher Hinsicht kann aus dem Verhältnismässigkeits- und dem Zweckbindungsgebot eine implizite Begrenzung der Bearbeitung und des Datenbestands abgeleitet werden. Von einer Rechtfertigung persönlichkeitsverletzender Datenbearbeitungen ist im Rahmen der bundesgerichtlichen Rechtsprechung allgemein und entsprechend auch in Bezug auf die Verletzung der genannten Grundsätze nur mit grosser Zurückhaltung auszugehen. Uneingeschränkt gilt indessen einzig der Anspruch auf die Berichtigung falscher Daten. Dieser beinhaltet in zeitlicher Hinsicht jedoch nicht zwingend einen Anspruch auf Löschung. Eine Anspruchsgrundlage für die Vernichtung richtiger Informationen, die die Persönlichkeit des Betroffenen verletzen, besteht dagegen im Rahmen des persönlichkeitsrechtlichen Unterlassungsanspruchs.

---

661 Insbesondere zu beachten sind in diesem Zusammenhang die Straftatbestände der Handlungen für einen fremden Staat gemäss Art. 271 StGB sowie der wirtschaftliche Nachrichtendienst gemäss Art. 273 StGB.

662 FERLE, 7; ZEUNERT/ROSENTHAL, Rn. 15 ff., 55 ff.

663 ZEUNERT/ROSENTHAL, Rn. 45.

664 ZEUNERT/ROSENTHAL, Rn. 144.

665 ZEUNERT/ROSENTHAL, Rn. 145.

C. Informationsmanagement als Konfliktgegenstand

I. Darstellung des Konflikts

1. Interessen des Unternehmens

1.1 Daten als Wirtschaftsfaktor

Die Speicherung und Verwertung von Daten ist zum Motor der sozialen und wirtschaftlichen Wertschöpfung geworden und die aus der Verbindung unabhängiger Datenelemente gewonnenen Erkenntnisse haben sich zu einem wichtigen Innovationsfaktor entwickelt[666]. In Reaktion auf das veränderte Geschäftsumfeld haben Unternehmen einen tiefgreifenden Wandel vollzogen und mit den neuen Geschäftsmodellen sowie operationellen Strukturen veränderten sich auch die Ansprüche an das Informationsmanagement. Der Marktdruck hat insbesondere die Technologie, die Datenverarbeitung, die Globalität sowie die Flexibilität und Innovation in den Vordergrund gerückt[667]. Im Onlinebereich profitieren die Nutzer von zahlreichen und oft kostenlosen Dienstleistungen (Suchmaschinen, E-Mail, soziale Netzwerke etc.), die vorher entweder nicht existierten oder die in anderer, nicht digitaler Form beachtliche Kosten verursachen[668]. Tatsächlich sind diese Angebote jedoch auch in elektronischer Form nicht kostenlos, da sie durch die Verwertung von Nutzerdaten in Form personalisierter Werbung direkt oder indirekt finanziert werden[669]. Je zahlreicher die erfassten Aktivitäten, desto zielgerichteter können die Anbieter ihre Offerten platzieren[670]. Viele der übermittelten Daten sind grundsätzlich oder notwendigerweise nicht verschlüsselt und können durch ihre umfassende Übertragbarkeit von einigen wenigen oder von vielen, von autorisierten oder nicht autorisierten Personen gelesen werden[671].

---

666 WORLD ECONOMIC FORUM, Value, 7; BOSTON CONSULTING GROUP, 21 ff.. Im virtuellen Raum können personenbezogene Daten besonders einfach, umfassend und kostengünstig gesammelt werden, KANG, 1198 f., 1220 ff.

667 CAVOUKIAN, 179.

668 A.A. offenbar SAMUELSON, 1134, die den Ärger der Amerikaner bezüglich des Kontrollverlusts über ihre Personendaten hauptsächlich darauf zurückführt, dass diese keinerlei Vorteile erhalten würden.

669 WORLD ECONOMIC FORUM, Data, 9; BOSTON CONSULTING GROUP, 22; siehe auch die häufig verwendete Notion von ANDREW LEWIS: «If you are not paying fot it, you're not the customer; you're the product being sold.»; abrufbar unter: http://www.metafilter.com/95152/Userdriven-discontent#3256046, abgerufen am 24.1.2012.

670 DUMAS, 40.

671 SPÀRCK JONES, 292.

1.2 Zuordnung anhand des Geschäftsmodells

a) Zuordnungskriterien

Unternehmen haben Ziele. Nach aussen manifestieren sich diese Ziele in Form von Produkten und Dienstleistungen. Im Innern liegt der unternehmerischen Tätigkeit in der Regel das Streben nach Gewinn zugrunde[672]. Dazwischen gibt es viele weitere Ziele, die sich auf einzelne Produkte oder Dienstleistungen beziehen. So kann ein mögliches Ziel in der Produktion formschöner und funktionaler Gegenstände oder in der Herstellung qualitativ hochstehender Mahlzeiten bestehen. Der Kreis schliesst sich am Markt, wo das Angebot auf die Nachfrage trifft und Unternehmensgewinne erwirtschaftet werden[673]. Das Erreichen der gesetzten Ziele setzt Aktion voraus. Die Handlungen können dabei in Strategien und Taktiken unterteilt werden. Strategien sind umfangreicher und schwieriger zu ändern. Taktiken sind kompakter und einfacher anzupassen. Strategien und Taktiken kanalisieren die Anstrengungen auf ein bestimmtes Ziel hin[674].

b) Datenbearbeitung als Gegenstand der Zielsetzung

Die Erreichung jedes Ziels erfordert die Bearbeitung bestimmter Daten. Entscheidend ist jedoch, in welchem Verhältnis die Datenbearbeitung zum übergeordneten Ziel des Gewinnstrebens steht. In einem Industrieunternehmen dienen letztlich alle benötigten Informationen dazu, die Abwicklung der für das Erreichen der Unternehmensziele notwendigen Prozesse zu ermöglichen[675]. Dagegen besteht bei rein informationsbasierten Diensten das Ziel in der Datenbearbeitung an sich. Bereits in den Neunzigerjahren waren Internet-Angebote im Allgemeinen kostenlos, jedoch gab es zu Beginn noch keine nennenswerten Werbeeinnahmen, mit denen die Kosten hätten gedeckt werden können. Bereits damals erschien es jedoch als wahrscheinlicher, dass sich die Nutzer weiterhin den kostenlosen Angeboten zuwenden werden und selbst bekannte Anbieter ihr Angebot nicht gegen Bezahlung würden erhalten können[676]. Hotmail offerierte schliesslich einen kostenlosen E-Mail-Dienst für Nutzer, die einen Fragebogen zu demografischen Daten und Interessen ausfüllten. Anhand dieser personenbezogenen Angaben konnte Hotmail nebst den versandten Nachrichten auch personalisierte Werbung an die Nutzer übermitteln. Dieses eins-zu-eins Marketing wurde als für beide Seiten

672 So sind gemäss Art. 706 Abs. 2 Ziff. 4 OR Beschlüsse der Generalversammlung, die die Gewinnstrebigkeit der Gesellschaft ohne Zustimmung sämtlicher Aktionäre aufheben, anfechtbar.

673 Siehe zum Ganzen, BRIDGELAND/ZAHAVI, 44 ff.

674 BRIDGELAND/ZAHAVI, 50 f.

675 AUGUSTIN, 85.

676 JOB, in: Picot, 80; SOLOMON/TUTEN, 12.

vorteilhaft erachtet. Der Werbende kann genau jenen Markt erreichen, den er will und die Nutzer müssen ihre Aufmerksamkeit nur auf solche Anzeigen richten, die für sie potentiell von Interesse sind[677]. Das gewinnorientierte Ziel wird damit nicht durch den Betrieb eines E-Mail-Dienstes an sich erreicht, sondern einerseits mit der Auswertung der durch dieses Angebot generierten personenbezogenen Daten sowie andererseits durch die Übermittlung entsprechender Werbung an die einzelnen Nutzer.

Werbeeinnahmen sind heute eine der Haupteinnahmequellen in der Internetbranche, wobei die Suchmaschinenwerbung momentan zu den beliebtesten Werbeformen zählt. Das Erlösmodell basiert auf der Definition von bestimmten Schlüssel- bzw. Suchwörtern durch die Werbetreibenden, die bei entsprechenden Suchanfragen der Nutzer Werbeanzeigen in Form von Links generieren. Werden diese dann durch den Nutzer angewählt, ist ein Preis pro Klick an den Suchmaschinenbetreiber zu entrichten[678].

c) Datenbearbeitung als Gegenstand der Strategie

Generell kann nicht mehr davon ausgegangen werden, dass die allgemeine Unternehmensstrategie automatisch auch die informationstechnologische Strategie prägt[679]. Gerade das Umgekehrte kann der Fall sein, die Möglichkeiten neuer Technologien prägen die strategische Richtung des Unternehmens[680]. Einige Unternehmen bewirtschaften auch die Daten, die im Rahmen ihrer Zielsetzung anfallen gezielt strategisch[681]. Google beispielsweise sammelt Tippfehler von Suchanfragen und nutzt diese Informationen für ein Rechtschreibprüfprogramm[682]. Auch das Übersetzungsprogramm basiert auf den Eingaben unzähliger Nutzer. Wird eine Übersetzungsanfrage eingegeben, wird diese mit den gesammelten Daten korreliert. Dabei besteht fast immer eine Ähnlichkeit zu vorherigen Eingaben und eine entsprechende Zusammenstellung führt zu brauchbaren Resultaten[683].

d) Datenbearbeitung als Gegenstand der Taktik

Die Verwertung personenbezogener Daten wird zunehmend zur Individualisierung des Angebots genutzt. Der Informationsfilter bei Amazon «Kunden, die diesen Artikel gekauft haben, kauften auch» beispielsweise schlägt verwandte Waren vor, die der Kunde

677 SHAPIRO/VARIAN, 7; in Bezug auf Suchmaschinen MAASS et al., 7.
678 MAASS et al., 6 f.
679 Siehe dahingehend beispielsweise noch PETERHANS, 202 f.
680 MCKEEN/SMITH, 13.
681 Davon zu unterscheiden ist die Analyse von Daten zum Erkennen neuer Unternehmensstrategien, siehe dazu MCKEEN/SMITH, 203.
682 MAYER-SCHÖNBERGER/CUKIER, 132.
683 LANIER, 16.

sonst möglicherweise nicht entdeckt hätte. Im Vergleich zu Google ist Amazon stärker auf die Primärnutzung von Daten fokussiert und greift nur marginal auf die Sekundärnutzung zurück[684]. Darin widerspiegelt sich eine wesentliche Unterscheidung zwischen Nutzer und Kunde: Bei Google ergibt sich der Wert des Nutzers hauptsächlich aus seinen Daten, während die Kunden (Werbung) primär eine Geldquelle darstellen[685]. Die Nutzung von Daten muss indessen nicht für alle Zwecke auf den Einzelnen zurückgeführt werden können. So hat der Detailhandelskonzern Walmart ein Managementsystem implementiert, das es den Lieferanten ermöglicht, zu jedem Zeitpunkt die genaue Menge ihrer Produkte in jedem Gestell und in jedem Laden festzustellen[686]. Welcher Konsument was kauft, ist für den Lieferanten hier nicht ersichtlich und wohl auch nicht erheblich.

e) Schlussfolgerungen

Die Gliederung unternehmerischer Tätigkeit in Ziel, Strategie und Taktik verdeutlicht in Bezug auf die Datenbearbeitung die Unterschiede der unternehmerischen Ausrichtung. Erstaunlicherweise konkurrieren die internetbasierten Dienste trotz deutlich unterschiedlicher Angebote für die Nutzer mit einem weitgehend identischen Angebot um die gleichen (Werbe-)Kunden. LANIER sieht hierin eine deutliche Beschränkung des Entwicklungshorizonts internetbasierter Angebote und geht von einem schrumpfenden Werbekuchen aus, der sich langfristig auf die Zielsetzung der konkurrierenden Unternehmen auswirken wird[687].

2. Interessen des Individuums

2.1 Vorbemerkungen

Die Zeit geht in vielerlei Hinsicht nicht spurlos am Menschen vorbei. Die Fähigkeit des Erinnerns ermöglicht es uns zu vergleichen, zu lernen und den Wandel der Zeit wahrzunehmen. Genauso wichtig ist die Fähigkeit des Vergessens und des Loslassens für ein Leben in der Gegenwart. Menschen wandeln sich über die Zeit, Ideen entwickeln und Ansichten verändern sich[688]. In Unternehmen erscheinen diese Prozesse mehr als Resultat der individuellen Vorgänge. Der Wandel der Zeit und die veränderte Wahr-

684 MAYER-SCHÖNBERGER/CUKIER, 132. Diese geringe Nutzung von Sekundärdaten ist nach hier vertretener Auffassung daher der Taktik zuzuordnen und weder Bestandteil der Zielsetzung, die im Verkauf von Waren besteht, noch Bestandteil der Strategie, die darin besteht, diesen Verkauf im Vergleich zu den klassischen Händlern online abzuwickeln.

685 LANIER, 165.

686 TENE/POLONETSKY, 65.

687 LANIER, 330.

688 MAYER-SCHÖNBERGER, 196.

nehmung reflektieren sich in den Entscheidungen der Unternehmensführung, die dann unter anderem das beschriebene Marken- und Reputationsmanagement beeinflussen[689]. Im Gegensatz zum Menschen reagiert ein Unternehmen nicht direkt auf seine Umwelt, sondern durch den Filter jener Menschen, die für das Unternehmen handeln. Hinsichtlich der Aussenwirkung dieses Handelns ist der individuelle Bereich indessen durchaus mit der Situation von Unternehmen vergleichbar. Die traditionelle Bedeutung des Rufs als eines der kostbarsten Güter und als Vertrauensbasis wird durch die Beschränkung der Anonymität wieder gestärkt[690]. Dahingehende Tendenzen lassen sich anhand der steigenden Nachfrage nach einem professionellen Reputationsmanagement beobachten[691].

2.2 Handlung und Motivation

a) Grundlagen

Der Sinn menschlicher Handlungen kann nicht durch Kausalgesetze erfasst werden, sondern bedarf einer Analyse der zugrundeliegenden Ziele und Absichten[692]. Ursache des Handelns sind individuelle Anreize und Motive, wie beispielsweise soziale Interaktion, Leistung und Status[693]. Dem Abwägen und Planen einer Handlung liegen unterschiedliche Bewusstseinszustände mit einer abweichenden Informationsverarbeitung zugrunde. Beim Abwägen stehen die objektive Analyse der Information im Hinblick auf positive und negative Anreize sowie die entsprechenden Folgen im Vordergrund. Bei der Planung dagegen verschiebt sich die Betrachtungsweise zu Gunsten jener Informationen, die den geplanten Verlauf einer Handlung unterstützen, bekräftigen oder rechtfertigen[694]. In der Konsequenz führt eine identische Information in Abhängigkeit zum jeweiligen Bewusstseinszustand zu abweichenden Handlungen[695]. Die Wirkung der Kenntnisnahme von mit der Informationsübertragung verbundenen Gefahrenhinweisen kann entsprechend durch die eine geplante Handlung fördernden Informationen

689 Siehe dazu vorne A.I.2.3 d).

690 BRIN, 333.

691 Für die Tendenz dieser Professionalisierung des Reputationsmanagements privater Personen im Internet siehe beispielsweise www.reputation.com, ein Unternehmen das 2006 gegründet wurde und heute über eine Million Nutzer hat.

692 GREVE 21 f., 49 f.

693 Grundlegend MCCLELLAND, 175; ATKINSON, 462 ff.

694 GOLLWITZER, 189 ff.; siehe zu Handlungsphasen und Bewusstseinslagen allgemein ACHTZIGER/GOLLWITZER, in: Heckhausen/Heckhausen, 314 ff.

695 Vgl. GASSER, Kausalität, 84.

verdrängt werden[696]. Die auf einem Handlungsplan basierenden Handlungen laufen zudem automatisiert und routinemässig ab, der Handelnde muss sich die Handlungen zu ihrer Ausführung nicht mehr bewusst machen[697].

b) Kontext

(1) Funktionaler Kontext

Mit neuen Informationstechnologien kommen neue Probleme, Hoffnungen mischen sich mit Zweifeln[698]. All diesen Neuerung ist indessen die fortschreitende Adaption und Nutzung gemein. Einige Komponenten des menschlichen Verhaltens mögen unveränderbar sein[699], im Übrigen passt sich der Mensch einer veränderten Umwelt durch entsprechende Änderungen seines Verhaltens an[700]. Die dafür erforderliche Bereitschaft zur Adaption ist an bestimmte Voraussetzungen geknüpft. Insbesondere die Einflussfaktoren auf die Entscheidung darüber, ob eine neue Technologie genutzt wird oder nicht, wurden in verschiedenen Modellen untersucht. Diese zeigen, wie Individuen auf Technologien reagieren und wie diese Reaktionen die Entscheidung und die Art der Benutzung dieser Technologien beeinflussen. Wesentlich sind dabei vor allem die Bedienfreundlichkeit und der erzielbare Nutzen[701].

(2) Sozialer Kontext

Informationen sind Teil der Kommunikation, die auch ein Beziehungselement umfasst[702]. Das individuelle Gedächtnis entwickelt sich in einer bestimmten Person durch ihre Teilnahme an kommunikativen Prozessen[703]. Diese Prozesse haben sich vermehrt

---

696 Siehe beispielsweise die Challenger-Katastrophe vom 28. Januar 1986, wo die Ingenieure auf die für gewisse Dichtungsringe aus Gummi problematisch tiefen Aussentemperaturen hinwiesen. Der Start war zu diesem Zeitpunkt bereits um sechs Tage verzögert und wurde trotz der Warnungen durchgeführt; siehe dazu: http://www.history.com/topics/challenger-disaster, abgerufen am 11.4.2014.

697 SCHÖNPFLUG/SCHÖNPFLUG, 312.

698 GLEICK, 411 f; SCHENK, 197; BULL, 8.

699 SCHENK, 197, stellt fest, dass selbst wenn alle Lebensbereiche von den aktuellen Veränderungen durch die technischen Medien erfasst würden, nicht nur diese wirksam wären. Stets gebe es menschliche Eigenschaften, die durch neue Gegebenheiten zwar modifiziert, jedoch nicht vollständig beseitigt würden.

700 STEINBUCH, 243.

701 ALBERS, Human-Information, 173. Siehe auch VENKATESH VISWANATH et al., User acceptance of Information Technology: Toward a unified view, Management Information Systems Quarterly, 27(3), 425-478 und die Kritik bei BAGOZZI RICHARD P., The legacy of the technology acceptance model and a proposal for a paradigm shift, Journal of the Association for Information Systems (8) 2007, 244-254.

702 Siehe dazu WATZLAWICK/BEAVIN/JACKSON, 53; MEISTER, 105.

703 ASSMANN, Gedächtnis, 36 f.; WELZER, 70 ff.

in den elektronischen Raum verlagert und hinterlassen dort entsprechende Spuren[704]. Das Gedächtnis bleibt durch die Kommunikation erhalten, wenn diese abbricht oder der jeweilige Bezugsrahmen verschwindet, ist Vergessen die Folge[705]. Die Aufnahme von Information resultiert oft aus der Interaktion zwischen Menschen[706]. Dabei wenden sich Individuen auf Informationssuche nicht nur am häufigsten, sondern auch zuerst an andere Menschen[707]. Das Teilen des erlangten Wissens ist entsprechend ein integraler und komplementärer Bestandteil menschlicher Interaktion[708]. Das Web ist längst keine passive, einzig auf den Konsum von Inhalten ausgerichtete Umgebung mehr, sondern ein dynamisches Umfeld, in dem die Nutzer interagieren und sich ausdrücken können[709]. Aufgrund dieser Eigenschaften ist das Web heute auf eine intimere Weise in das Leben der Menschen eingebunden als andere Medien, es verbindet Menschen mit Orten und Menschen untereinander[710]. Der Kreis sozialer und weiterer Kontakte wird dadurch jenseits zeitlicher und örtlicher Schranken ausgeweitet. Permanenz und Art der Verfügbarkeit dieser kommunikativen Räume tragen entscheidend zum Mitteilungsbedürfnis der Nutzer bei[711]. Soziale Netzwerke beispielsweise basieren darauf, dass Nutzer Informationen über sich preisgeben und sich mit anderen Nutzern austauschen. Im Zuge dieser Entwicklung hat sich die befürchtete Hemmung des persönlichen Ausdrucks in den neuen digitalen Medien nicht bestätigt[712].

(3) Individueller Kontext

Jedes Individuum entwickelt in der Interaktion mit anderen multiple Identitäten, die den unterschiedlichen sozialen Kontexten angepasst und in Teilen auch gegeneinander abgeschirmt werden müssen[713]. Wo das traditionelle Identitäts-Verständnis auf Dauerhaftigkeit und Einheit ausgerichtet war, stehen bei neueren Konzepten die Veränderung und die Vielfalt im Mittelpunkt. Identität wird als komplexe Struktur einer Vielzahl einzelner Elemente aufgefasst[714]. Auf die Entwicklung kohärenter Identitätskerne muss

704 LINDSAY, 324.
705 ASSMANN, Gedächtnis, 37.
706 FIDEL, 37.
707 BYSTRÖM/JÄRVELIN 191 ff.; FIDEL/GREEN 563 ff.
708 FIDEL, 37, 39.
709 RALLO/MARTINEZ, 412 f.
710 PAINE SCHOFIELD/JOINSON, 16.
711 RALLO/MARTINEZ, 412 f.
712 ONUF/HYRY, 249.
713 DÖRING, 258; MEISTER, 106.
714 DÖRING, 255, m.w.H.

trotz der Komplexität dieser modernen Subjektivität nicht verzichtet werden[715]. Diese Kohärenz wird insbesondere durch die folgenden zwei Methoden erreicht[716]: Einerseits durch die mittels Erzählung geschaffene kohärente Selbstkonstruktion, der die verschiedenen Teilidentitäten zugeordnet werden. Andererseits durch die Konzentration auf wenige Teilidentitäten während bestimmter Lebensphasen. Die darauf basierende Erfahrung von Konsistenz und Kontinuität begründet das Gefühl einer Einheitlichkeit über die Zeit. Durch digitale Identitäten werden diese Erfahrungen vermeintlich oder tatsächlich erweitert, was nicht nur stabilisierend, sondern auch destabilisierend wirken kann[717]. Im Zuge dieser Entwicklung wird das Subjekt vermehrt zu einem Subjektivitäts-Konzept, das nicht mehr als ursprüngliche, konstante Verfassung des Menschen verstanden wird, die sich aus dem festen Bestand individueller Erinnerung bildet, sondern als Resultat bestimmter Praktiken, durch die das Individuum sich selbst konstruiert[718].

Der Bezug dieser Bedürfnisse zum Recht lässt sich anhand der soziologischen Perspektive aufzeigen. Hinsichtlich des Datenschutzes umfasste diese insbesondere die Erkenntnis, dass Institutionen nur über jene (unterschiedlichen) personenbezogenen Informationen verfügen sollten, die sie zur Wahrnehmung ihrer jeweiligen Funktion benötigen. Das Nebeneinander der sich daraus ergebenden unterschiedlichen Bilder über das Individuum schafft die Autonomie für ein individuelles Handeln und verhindert einen «Normendruck zur generellen Konformität»[719]. Dieses auf den öffentlichen Bereich bezogene Verständnis ist grundsätzlich auch unter Privaten gültig[720].

c) Informationsübermittlung

(1) Explizite Übermittlung

Im Kontakt zwischen Unternehmen und Individuen werden zahlreiche Informationen explizit übermittelt. Anders als im Verhältnis zum Staat besteht hier keine Pflicht für diese Übermittlung. Grundsätzlich stellt sich somit die Frage, ob und inwiefern der Einzelne vor sich selber geschützt werden muss[721]. Nach hier vertretener Ansicht recht-

715 DÖRING, 259.
716 Siehe dazu STRAUS/HÖFER, 296 ff.
717 LEHNER, 33.
718 MEIER, 41; BAUMAN, 15 f., 48 f.
719 MÜLLER, Funktionen, 109.
720 MEISTER, 112.
721 BONDOLFI, 131, argumentiert, dass die Bestimmung der Privatsphäre durch das Individuum unzureichend sei, da der Einzelne gegen seine objektiven Interessen über die Privatsphäre verfügen könne und auch Dritte durch die subjektive Grenzziehung beeinträchtigt werden könnten.

fertigt sich ein Eingriff bei explizit übermittelten Daten nur dort, wo die Urteilsfähigkeit des Nutzers nicht gegeben ist bzw. das Bewusstsein über die möglichen Folgen einer Handlung nicht abgeschätzt werden können. Bei einigen Angeboten im Onlinebereich kann diese Wertung freilich schwer fallen. So stellt sich beispielsweise die Frage, inwiefern in sozialen Netzwerken übermittelte Informationen auch gegenüber Dritten als explizit übermittelt gelten.

(2) Implizite Übermittlung

Von einer impliziten Übermittlung ist dann auszugehen, wenn sich der Nutzer zumindest bewusst ist, dass seine Daten nicht nur dem von ihm unmittelbar beabsichtigten Zweck dienen, sondern auch von Unternehmen und weiteren Dritten für deren Zwecke genutzt werden können. Die meisten Vorgänge im Netz umfassen heute eine implizite Übermittlung personenbezogener Daten. Suchen, Bestellen, Bewerten, Kommentieren usw. lassen eine Auswertung und eine zielgerichtete Verwertung der erlangten Daten zu[722].

(3) Unbewusste Übermittlung

Noch weitgehend unbewusst verläuft die Übermittlung von Daten durch Cookies, GPS-Systeme und weitere Technologien[723]. Und erst am Anfang steht die Entwicklung neuer und immer kleiner werdender Geräte zur Datensammlung. Diese erbringen ohne Zweifel wertvolle Dienste, stellen aber gleichzeitig auch eine Gefahr für die Privatsphäre dar[724]. Aus Sicht des Individuums ergibt sich in diesem Zusammenhang ein entscheidender Unterschied zwischen tatsächlicher und bloss empfundener Privatsphäre, die oft in einem Ungleichgewicht stehen. Die empfundene Privatsphäre kann beispielsweise bei der Übermittlung persönlicher Daten an einen Onlinehändler als stark eingeschätzt werden. Die tatsächliche Privatsphäre kann dagegen aufgrund der unauffälligen (automatischen) Sammlung von Daten des Onlineverhaltens und der möglichen zukünftigen Nutzung der Daten durch unbekannte Dritte sehr schwach ausgeprägt sein[725].

---

722 DUMAS, 40; siehe auch die Ausführungen bei ZIKOPOULOS et al., 24 ff.

723 Siehe zur unbewussten Übermittlung BOSTON CONSULTING GROUP, 40 f.

724 DUMAS, 242; WALDO/LIN/MILLETT, 89, 256 ff.

725 PAINE SCHOFIELD/JOINSON, 15.

3. Interessen der Öffentlichkeit

Im öffentlichen Interesse liegt insbesondere «was der Staat zum Gemeinwohl vorkehren muss, um eine ihm obliegende Aufgabe zu erfüllen»[726]. Die umfassende Datenbearbeitung als Strategie zur Erfüllung der Interessen beschränkt sich dabei nicht auf private Unternehmen. Auch die staatlichen Organe sind am Zugriff auf immer mehr personenbezogene Informationen interessiert[727]. Das Ziel der Datensammlung durch staatliche Organe liegt insbesondere in der verstärkten Überwachung der Einhaltung von Normen[728]. Die technologischen Fortschritte haben zu einer laufenden Verbesserung der Überwachungstechniken geführt[729]. Diese Technologien dienen den staatlichen Organen zur direkten Informationsbeschaffung – beispielsweise durch geheimes Durchsuchen von Datenverarbeitungssystemen[730]. Die gesetzlichen Grundlagen verpflichten auch private Anbieter zur Duldung einer Überwachung[731]. Wie in der Privatwirtschaft besteht darüber hinaus innerhalb der Bundesverwaltung ein Interesse, die Nutzung der Informations- und Kommunikationsmittel zur Sicherstellung des Betriebs und zur Verhinderung von Missbräuchen zu kontrollieren[732]. Dieses Ziel wird hauptsächlich durch die Auswertung von bei der Nutzung anfallenden Daten (sog. Randdaten) realisiert. Diese zeigen, welche IP-Adresse wann wie lange mit welcher URL (*Uniform Resource Locator,* Adresse einer Internetseite) in Verbindung gestanden hat. Auf Basis dieser Daten kann die Benutzung des Internets durch den einzelnen Mitarbeiter ausgewertet werden. Im Resultat mag das Ziel der Bearbeitung ein anderes sein, in Bezug auf die Datenerhebung und Verwertung an sich sind hingegen kaum nennenswerte Unterschiede zu erkennen. Das Sammeln von Daten wird auch im öffentlichen Sektor mit dem Glauben an eine verbesserte Kontrolle von Vorgängen verknüpft[733].

Macht über Daten ist darüber hinaus nicht nur mehr ein Mittel des modernen Staates zur Gewährleistung öffentlicher Sicherheit oder zur Erreichung weiterer im öffentli-

---

726 HÄFELIN/HALLER/KELLER, Rn. 315.

727 WEBER, Grundrechtskonzeptionen, 10.

728 Siehe für eine Übersicht aufzuzeichnender Daten im Rahmen des BÜPF BERANEK ZANON, 142 ff. Im Jahr 2012 sind die von Strafverfolgungsbehörden zur Aufklärung schwerer Straftaten angeordneten Fernmeldeüberwachungen um rund 20 Prozent angestiegen, Generalsekretariat EJPD, News, Bern, 7.2.2013. Siehe zum Problem der Schattenwirtschaft in der EU und digitalen Lösungsansätzen zur Überwachung von Steuerzahlungen BOSTON CONSULTING GROUP, 83 f.

729 Siehe für eine detaillierte Analyse über die entsprechende Gefährdungslage TSCHENTSCHER, 383 ff.

730 WEBER, Grundrechtskonzeptionen, 10.

731 BERANEK ZANON, 141.

732 Siehe zum ganzen Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 19. Tätigkeitsbericht 2011/2012, Bern 2012, 51.

733 HELLER, 105.

chen Interesse liegender Ziele durch staatliches Handeln. Die Macht der Öffentlichkeit selbst über Daten begrenzt die politische und wirtschaftliche Autonomie. Diese Aufgabe obliegt vor allem den Medien[734]. Die Medienfreiheit schützt Medienschaffende (Journalisten, Kameraleute usw.)[735]. Indessen sieht die schweizerische Bundesverfassung keine geschlossene Kommunikationsordnung vor und berücksichtigt die wirtschaftlichen, gesellschaftlichen und technischen Entwicklungen, indem neben den klassischen Medien (Presse, Radio, Fernsehen) auch weitere «Formen der öffentlichen fernmeldetechnischen Verbreitung» Erwähnung finden[736]. Sie ist primär ein gegen den Staat gerichtetes Abwehrrecht und entfaltet keine unmittelbare Wirkung im Privatsektor. Die rechtsetzenden und rechtsanwendenden Behörden müssen nach Art. 35 Abs. 3 BV aber sicherstellen, dass insbesondere die Grundgehalte des Art. 17 BV auch unter Privaten wirksam werden[737].

4. Schlussfolgerungen

Eine grosse Vielfalt an unterschiedlichen Daten wird heute in zunehmender Anzahl und in unterschiedlichen Kontexten bearbeitet[738]. Auch die klassischen Sektoren nutzen vermehrt personenbezogene Daten nicht mehr nur in Form von Kontaktinformationen[739]. In Bezug auf den Erhalt von Daten läuft die Löschung personenbezogener Daten der Zielsetzung und der Strategie von Unternehmen vielfach entgegen. Suchmaschinenbetreiber beispielsweise können durch die Aufbewahrung dieser Daten die Werbung ihrer Kunden wesentlich gezielter platzieren[740]. Die klassische Werbung generiert dabei generell einen grösseren Effekt auf die Verkaufszahlen als nutzergenerierte Inhalte, wie sie beispielsweise innerhalb von sozialen Netzwerken in Form von Beschreibungen durch einzelne Nutzer gegeben sind. Das Erfassen solcher Beschreibungen stellt höhere kognitive Ansprüche, die von den Konsumenten aufgrund zeitlicher Restriktionen oft nicht erbracht werden können[741]. Zudem ermöglicht die Speicherung personenbezogener Daten die Verbindung mit weiteren Daten, was zu einem detaillier-

---

734 VON LEWINSKI, 217. Siehe zum stetigen Verweis der Medien auf ein überwiegendes öffentliches Interesse als Rechtfertigungsgrund für Persönlichkeitsverletzungen AEBI-MÜLLER, Rn. 789 ff.

735 BGE 121 III 367; BGE 131 II 258.

736 NOBEL/WEBER, 2 Rn. 2.

737 BIAGGINI, Art. 17 N 7.

738 PAINE SCHOFIELD/JOINSON, 16.

739 BOSTON CONSULTING GROUP, 55, 71 ff.; siehe auch die Übersicht in LONDON ECONOMICS, 133. Die technologische Entwicklung hat die Sekundärnutzung von Personendaten und die Weitergabe an Partnerunternehmen vereinfacht, WHITE/MÉNDEZ MEDIAVILLA/SHAH, 62.

740 STROWEL, 209.

741 DUBACH, 152 f., 164 f.

ten Profil der einzelnen Person führt[742]. Die anhand dieses Profils übermittelten Daten können individuell ausgerichtet werden und sollen der betroffenen Person möglichst nur für sie relevante Inhalte liefern.

Das Individualinteresse liegt hauptsächlich in der Nutzung der angebotenen Dienste als Mittel zur individuellen Entfaltung und sozialen Interaktion. Identität, Beziehung und Kommunikation sind grundlegende Elemente sozialer Interaktion[743]. Die explizite Übermittlung von Daten dient entsprechend nicht primär der Interaktion mit dem jeweiligen Unternehmen. Diese ist mehr Teil einer impliziten oder sogar unbewussten Übermittlung von Informationen.

5. Gegenstand resultierender Konflikte

5.1 Ausgangslage

Das Aufkommen sozialer Netzwerke und des Cloud-Computing sowie die Weiterentwicklung internetbasierter Technologien haben die Nutzung des Internets durch Individuen und Unternehmen stark erhöht[744]. Diese gesteigerte Nutzung internetbasierter Angebote und der globale E-Commerce haben in Kombination mit den Fortschritten im Bereich der elektronischen Datensammlung und des Marketings zu neuen potentiellen Bedrohungen für die Privatsphäre geführt, die vielen Nutzern verborgen bleiben[745]. Die Betrachtung des Konflikts umfasst die Auseinandersetzung mit den divergierenden Positionen von Unternehmen und Individuen.

Vor dem Hintergrund der oben beschriebenen Prozesse ergeben sich dort Konflikte, wo der Mensch mit digitalen Systemen interagiert und eine dauerhafte Erfassung ohne wirksame Anonymisierung erfolgt. Rein technische Vorgänge, wie beispielsweise mit Sensoren ausgestattete Produktionsanlagen oder Flugzeugturbinen[746], sind in diesem Kontext unproblematisch[747]. Die neue Grenze verläuft bei der Erhebung persönlicher Daten im Bereich menschlicher Beziehungen, Erfahrungen und Stimmungen[748]. Die Entwicklung deutet auf eine vermehrte Erfassung menschlichen Verhaltens hin, wodurch auch eine Analyse des sozialen Verhaltens auf allen Ebenen möglich wird[749].

---

742 STROWEL, 209; BOSTON CONSULTING GROUP, 35 f.

743 Siehe dazu MASLOW, 372 ff.

744 WHITE/MÉNDEZ MEDIAVILLA/SHAH, 53.

745 CAMP, 256, m.w.H.

746 POLZER, 6, eine Flugzeugturbine sammelt während eines Fluges Daten, die direkt an eine Auswertungsstelle am Boden übermittelt werden.

747 MAYER-SCHÖNBERGER/CUKIER, 152; SCHWEIZER, Grundsatzfragen, 5.

748 MAYER-SCHÖNBERGER/CUKIER, 91.

749 MAYER-SCHÖNBERGER/CUKIER, 93 f.

Im Unterschied zu analogen Daten bieten digitale Daten mehr Möglichkeiten und erlauben Bearbeitungen, die nicht mehr durchschaubar sind[750]. Zwei zentrale Probleme dieser Datenbearbeitungen liegen in der mangelnden Transparenz und in der fehlenden Kontrolle für die Betroffenen[751]. Nachstehend werden diese zwei Faktoren als massgebliche Konfliktpunkte untersucht.

5.2 Transparenz

a) Inhaltliche Transparenz

Der Grundsatz der Transparenz führt im Verhältnis zwischen dem Individuum und dem Unternehmen zur zentralen Frage nach dem Umfang der Aufklärungspflicht resp. dem Aufklärungsanspruch. Diese Frage ist im Einzelfall zu klären und kann nicht generell beantwortet werden[752]. Indessen machte das deutsche Bundesverfassungsgericht – für den öffentlichen Bereich – in seinem Volkszählungsurteil die wesentliche Aussage, dass nicht die Datenmacht an sich eine Beeinträchtigung der Freiheit bewirke, sondern die Unsicherheit über den Bestand eines Informationsgefälles[753]. Zumindest in Anbetracht einer gewissen Zugriffsmöglichkeit staatlicher Stellen auf private Datensammlungen erscheint die Transparenz über die bearbeiteten Daten auch im privaten Sektor als relevant[754]. In den USA wird unter Verweis auf das Fehlen eines nationalen Gesetzes zum Schutz der Vertraulichkeit von Gesundheitsdaten und genetischen Daten ferner auf das Problem der Diskriminierung im Arbeits-, Versicherungs-, Schul- und Mietverhältnis hingewiesen[755].

b) Transparenz über die Verwertung

In der Regel besteht für die Betroffenen kaum Transparenz über die Datenerhebung und -verarbeitung, da die Verwertungsmechanismen und das vollständige Ergebnis dieser Prozesse nicht kommuniziert werden[756]. Durch die heutige Technologie finden die-

---

750 BAUMANN, 116.

751 Diese Faktoren sind auch im Bericht des Bundesrates über die Evaluation des DSG hervorgehoben; siehe BBl 2012 350.

752 MELCHIOR, 134.

753 BVerfGE 65, 46; VON LEWINSKI, Fn. 18.

754 Siehe dazu beispielsweise den Google Transparenzbericht, abrufbar unter: http://www.google.com/transparencyreport/?hl=de, abgerufen am 14.2.2014; kritisch in Bezug auf die Effizienz dieses Vorgehens BULL, 14 f.

755 ALLEN, 28; WESTIN, Computers, 212 f. Siehe ferner zur Diskriminierung von Konsumenten, GANDY, 175 ff.

756 Insbesondere beim Cloud-Computing besteht das Risiko einer unzureichenden Information darüber, wie, wo und durch wen Daten bearbeitet werden; siehe dazu Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, July 1, 2012, 2.

se Vorgänge ohne eine unmittelbar wahrnehmbare Verbindung zwischen den Betroffenen und den Verwertenden statt. Die beliebige Verfügbarkeit wachsender Datenmengen und ihre Auswertung führen zum Abbild eines Individuums, das an diesem Vorgang nicht aktiv beteiligt, sondern eben nur das Ergebnis desselben ist[757]. Für Unternehmen gibt es sowohl Gründe, die für als auch solche die gegen diese Intransparenz sprechen. So kann einerseits das Auskunftsrecht des Betroffenen mit dem Geschäftsgeheimnis des Unternehmens kollidieren[758]. Andererseits können Unternehmen durch eine transparente und sorgfältige Nutzung personenbezogener Daten Folgeprobleme vermeiden und die Partizipationsbereitschaft der Nutzer fördern oder zumindest nicht wesentlich beeinträchtigen[759].

5.3 Kontrolle

a) Kontrolle über den Inhalt

Die direkte Kontrolle über den Inhalt von Information bezieht sich nicht primär auf einzelne Daten, sondern auf die Kontrolle über die aus diesen Daten gewonnen Erkenntnisse[760]. Darüber hinaus ist die Kontrolle ein entscheidender Faktor für die Informationsqualität. Der direkte Informationszugriff der betroffenen Person ermöglicht zumindest die Sicherstellung der relativen Genauigkeit von Daten und führt zu einer besseren Datenqualität als die indirekte Überprüfung anhand der Bewertung von Datenbearbeitungsvorgängen[761]. Neuere Forschungsergebnisse weisen darauf hin, dass Entwicklungen im Umgang mit über das Internet verbreiteten Daten eine Kontrolle generell begünstigen[762]. Wo die Nutzer nicht über die für eine umfassende Kontrolle ihrer Daten notwendigen Kenntnisse verfügen oder diese Kontrolle gar nicht wollen, vertrauen sie auf die Reputation und die Unternehmenspraktiken der Datenbearbeiter[763]. Datenschutzverletzungen bergen aus Sicht des Unternehmens entsprechend das Risiko von Reputationsschäden, einem damit einhergehenden Vertrauensverlust und einer Abnahme an verfügbaren Daten.

---

757 Vgl. SPÀRCK JONES, 293.

758 MELCHIOR, 134.

759 DUBACH, 146.

760 Vgl. FRICK, 58.

761 SCHWEIZER, Access, 133; siehe auch DRUEY, Information, 394: «Das Interesse des Betroffenen richtet sich darum auch nicht notwendig auf die Beschränkung der Informationsvorgänge, sondern auf die Teilhabe daran, um allenfalls von sich aus die Qualität sicherzustellen.».

762 Siehe dazu u.a. die Studie des Pew Research Center, Teens, Social Media and Privacy, Berkman Center, May 21, 2013, abrufbar unter: http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx, abgerufen am 18.8.2013.

763 CAVOUKIAN, 179; siehe zur ökonomischen Relevanz des Vertrauens und insbesondere als Wettbewerbsfaktor BOSTON CONSULTING GROUP, 111 ff.

Angebotsseitig werden insbesondere im Bereich der Kontrollmöglichkeiten neue Ansätze in Form von persönlichen Datenspeichern verfolgt. Diese ermöglichen dem Individuum eine zentrale Datenspeicherung und die Kontrolle über die Verwendung von Kopien der Daten[764]. Ein entscheidender Faktor für die Autonomie der Nutzer liegt hierbei in der freien Übertragbarkeit ihrer Daten. Insbesondere im Bereich der sozialen Medien wurde die verbesserte Übertragbarkeit der Nutzerdaten als möglicher Treiber für mehr Wettbewerb unter den Anbietern angeführt. Dieser würde möglicherweise auch den Schutz der Privatsphäre umfassen; vorausgesetzt, es handelt sich dabei aus Sicht der Nutzer um einen wettbewerbsrelevanten Faktor[765]. Zur Erreichung dieses Ziels werden häufig gemeinsame Industriestandards vorgeschlagen. Damit der Aufwand für einen Angebotswechsel aber tatsächlich reduziert werden kann, müssten sich alle namhaften Anbieter dazu verpflichten und sich auf einen umfassenden Standard einigen. Unter Berücksichtigung der ökonomischen Anreize für die exklusive Beanspruchung der Nutzerdaten erscheint ein solcher Standard konkurrierender Unternehmen als unwahrscheinlich[766]. Zudem zeigt sich bei den Suchmaschinen, dass die Wahl für Alternativen wohl einer Gesamtabwägung des Nutzers unterliegt. Der Verzicht auf die Speicherung personenbezogener Daten und der damit potentiell einhergehende bessere Schutz der Privatsphäre ist nur ein Teilaspekt und gegenüber der Funktionalität und Leistungsfähigkeit eines Angebots abzuwägen. Im Weiteren wird der Nutzen einer verbesserten Übertragbarkeit der Daten durch die Schwierigkeit eines Markeintritts neuer Konkurrenten relativiert. Am Beispiel von Suchmaschinen lassen sich zwei wesentliche Eintrittsbarrieren aufzeigen: Einerseits bedingt die Bewältigung einer wachsenden Datenmenge technische Kenntnisse und Ressourcen, die mit entsprechend hohen Kosten einhergehen. Andererseits verfügen neue Wettbewerber noch nicht über die notwendige Reichweite, um für den Werbemarkt attraktiv zu sein, was die Bereitstellung finanzieller Reserven erfordert[767].

b) Kontrolle über die Verbreitung

Verbreiten umfasst die Übermittlung von Informationen an wenigstens einen Dritten[768]. Die Fixierung des menschlichen Handelns schafft eine deutlich grössere Gefahr

764 WORLD ECONOMIC FORUM, Value, 13.

765 Dem ist eher nicht so; siehe dazu insbesondere SOLOVE, Person, 82.

766 RODRIGUES, 247 f.

767 MAASS et al., 10 f., sehen darin einen der Gründe, weshalb Lycos und AOL ihre Suchergebnisse von Google beziehen. Auch die Suchmaschine Duck Duck Go verfügt über keine eigene Bildersuche.

768 RIKLIN, 205.

der Verbreitung als die blosse Kenntnisnahme[769]. Wer bestimmte Handlungen eines anderen aufzeichnet, gewinnt Macht über diesen[770]. Hinsichtlich der Kontrolle über die Verbreitung lassen sich zwei Faktoren unterscheiden: Einerseits besteht ein Interesse an der Kontrolle über die örtliche Verbreitung; diese umfasst das Medium und den Adressatenkreis. Andererseits besteht ein Interesse an der Kontrolle über die zeitliche Verbreitung, die den Zeitpunkt und die Dauer umfasst.

Die zeitbezogenen Aspekte waren insbesondere Gegenstand einer Studie von HOOFNAGLE, KING LI und TUROW über die Unterschiede zwischen jungen Erwachsenen und älteren Menschen hinsichtlich der Wahrnehmung von Kontrollmöglichkeiten. Auf die Frage, ob Websitebetreiber und Werbeunternehmen rechtlich verpflichtet werden sollten, alle gespeicherten Informationen über ein Individuum zu löschen, antworteten 92 Prozent, dass sie ein solches Gesetz begrüssen würden. Zwischen den ältesten und den jüngsten Teilnehmern bestand nur ein kleiner Unterschied von 2 Prozent, wobei die jüngeren Teilnehmer etwas seltener zu Gunsten eines solchen Gesetzes antworteten[771].

Die ortsbezogenen Aspekte umfassen sowohl das Medium als auch den damit zusammenhängenden Adressatenkreis, da sich dieser häufig über das Medium definiert. Zusätzlich von Bedeutung im Zusammenhang mit dem Geheimnisschutz ist der Geheimhaltungswille des Betroffenen. Gemäss der negativen Abgrenzung der Privatsphäre resp. des Privatlebens fallen Äusserungen und Handlungen, die öffentlich erkenn- und einsehbar sind und an denen kein Interesse an ihrer Geheimhaltung besteht nicht unter den Schutzbereich des Privatlebens[772]. Sofern indessen ein Geheimhaltungsinteresse besteht, fallen Äusserungen und Handlungen gemäss der Praxis des EGMR auch dann in den Bereich des Privatlebens, wenn sie in der Öffentlichkeit geäussert werden[773]. Die Information über den Inhalt einer Äusserung und Handlung wird hier grundsätzlich unabhängig vom Forum der Kundgabe qualifiziert.

---

769 RIKLIN, 203; LANDWEHR, 40 f.; siehe zur Verbreitung im Internet ZITTRAIN, 225.

770 LANG, 16: «Der Machtgewinnung auf der einen Seite steht eine Entmachtung auf der andern gegenüber.»; RIKLIN, 204, sieht dadurch die These bestätigt, dass bereits die Aufnahme die Privatsphäre beeinträchtigt; siehe unter Verweis auf die Missbrauchsmöglichkeiten auch BULL, 11.

771 Siehe HOOFNAGLE CHRIS JAY/KING JENNIFER/LI SU/TUROW JOSEPH, How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?, April 14, 2010, abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864, abgerufen am 18.8.2013; siehe zur Relevanz der Kontrolle über die Verbreitung auch SOLOVE, Reputation, 170.

772 NOBEL/WEBER, 4 Rn. 12 f.

773 EGMR vom 25. September 2001, Nr. 44787/98, Nr. 56.

c) Schlussfolgerungen

Konflikte ergeben sich dort, wo der Einzelne die Kontrolle über die ihn betreffenden Inhalte verliert und seine Reputation bzw. Identität angegriffen wird[774]. In zeitlicher Hinsicht stehen Informationen aus der Vergangenheit, die der gegenwärtigen Selbstkonstruktion einer (Teil-)Identität entgegenstehen, im Vordergrund[775]. Zwar kann mit Recht festgestellt werden, dass eine provozierende oder verletzende Verhaltensweise auch in vielen anderen Situationen menschlicher Kommunikation auftritt[776]; die besondere Problematik solcher Handlungen im digitalen Umfeld liegt jedoch in ihrer potentiellen Reichweite und ihrem zeitlichen Fortbestand[777].

Klärungsbedarf besteht indessen bereits bei unproblematischen Inhalten. So darf das Bild einer Person nicht ausserhalb des von ihr definierten Bereichs verbreitet werden. Aus Unternehmenssicht stellt sich im digitalen Umfeld die Frage, wie dieser Bereich für eine frei zugängliche Website zu definieren ist. Wenn auf einer Website nebst dem Bild auch der Name des Abgebildeten vorkommt, dürfte die konkludente Einwilligung eine Aufnahme der Abbildung in die Trefferliste bei einer entsprechenden Namenssuche mitumfassen[778]. Nach der hier vertretenen Auffassung muss sowohl der Betreiber der Website als auch der Abgebildete damit rechnen, dass die Website über die Textsuche erschlossen wird. Die Einwilligung des Abgebildeten in die allgemeine Auffindbarkeit umfasst zugleich die Einwilligung zur Aufnahme des Bildes in die Bildersuche[779]. Der Arbeitnehmer, der in die Veröffentlichung seines Bildes auf der Unternehmenswebsite zugestimmt hat, willigt damit auch in die Erfassung durch Suchmaschinen und damit in eine allgemeine Zugänglichkeit ein[780].

---

774 So beispielsweise durch die ungewollte Verbreitung über Videoportale durch Dritte; siehe dazu die Beispiele bei SOLOVE, Reputation, 43 ff., 170 ff. DÖRING, 270, weist darauf hin, dass die Anonymität und die physische Distanz im Netz die sozialen Kontrollen reduzieren und die Handlungen nicht mehr vor anderen gerechtfertigt werden müssten.

775 Siehe dazu vorne C.I.2.2 b)(3).

776 So DÖRING, 270.

777 Dabei müssen keine umfassenden Informationen mehr vorhanden sein. Jede Wahrnehmung eröffnet immer auch implizite Aspekte, die zu bestimmten Schlussfolgerungen führen, CROSSON, in: Philosophy and Cybernetics, 189.

778 Siehe HÜRLIMANN, 91.

779 Gemäss Urteil des LG Köln vom 22. Juni, 28 O 819/10 2011, Rn. 19, gelten die im Urteil des BGH vom 29. April 2010, I ZR 69/08 (Vorschaubilder) genannten Grundsätze zur Einwilligung auch im Persönlichkeitsrecht, da es stets um das Selbstbestimmungsrecht geht.

780 Siehe dazu das Urteil des LG Hamburg vom 16. Juni 2010, 325 O 448/09, Rn. 22.

5.4 Veranschaulichung anhand ausgewählter Dienstleistungen

a) Cloud-Computing

Die Kontrolle von Cloud-Angeboten gestaltet sich für den Nutzer aufgrund mangelnder Transparenz hinsichtlich der Datenverarbeitung und der Sicherheitsmassnahmen generell schwierig. Viele Anbieter informieren nur oberflächlich über die Funktionsmechanismen und vernebeln den Blick hinter die Wolke. Regelmässig hat der Nutzer nur Einblick in den ihn betreffenden Teil der Datenverarbeitung, jedoch nicht in Teile, die auch andere Nutzer betreffen. Eine Auswertung aller administrativen Tätigkeiten im System darf nicht erfolgen, sofern dadurch auch Informationen über andere Kunden des Anbieters offenbart werden könnten[781].

In Bezug auf den zeitlichen Bestand von Daten bestehen grundsätzlich zwei Probleme: Einerseits ist fraglich, wie lange der Nutzer nach Beendigung des Nutzungsverhältnisses noch Zugriff auf die Daten hat und ob andererseits die Daten nach diesem Zeitraum tatsächlich gelöscht werden[782]. Bei vielen Cloud-Angeboten ist insbesondere nicht gewährleistet, dass die Daten vollständig gelöscht werden. Abhängig von der Funktionsweise der Cloud können Kopien von Daten auf vielen Servern und Backup-Systemen erhalten bleiben. Dieser Umstand ist insbesondere im Zusammenhang mit sensiblen Daten zu beachten, die beispielsweise dem Berufs- oder Amtsgeheimnis unterliegen[783]. Die tatsächliche Löschung ist hingegen dann problematisch, wenn Unklarheit über die Beendigung des Nutzungsverhältnisses besteht und die Daten entgegen dem Willen des Nutzers nicht mehr zugänglich sind[784]. Darüber hinaus bewahren sich viele Anbieter das Recht vor, auf die gespeicherten Daten zuzugreifen und diese auch zu löschen oder den Account zu sperren, wenn sie von der Regelwidrigkeit von Inhalten ausgehen[785].

Ein weiteres Problem ergibt sich im Hinblick auf die durch die Nutzung von Cloud-Diensten entstehenden Metadaten. Daraus lassen sich allenfalls zusätzliche schützenswerte Informationen ableiten, wenn beispielsweise analysiert wird, wer, wann, mit wem an welchem Dokument gearbeitet hat[786]. Aus rechtlicher Sicht ist zudem der Verlust der Ortsgebundenheit relevant. Im Datenschutzrecht bezieht sich die Einschätzung über ein angemessenes Datenschutzniveau grundsätzlich auf den Ort der Verarbei-

781 HANSEN, 89.
782 BRADSHAW/MILLARD/WALDEN, 23.
783 HANSEN, 90.
784 BRADSHAW/MILLARD/WALDEN, 23 f.
785 HANSEN, 92.
786 HANSEN, 90; siehe zur fehlenden Vereinbarung bezüglich dem Umgang mit Metadaten HON/MILLARD/WALDEN, in: Millard, 131.

tung[787]. In Abhängigkeit zum jeweiligen Rechtssystem des Cloud-Anbieters können Zugriffsrechte bestehen, über die sich der Nutzer nicht bewusst ist[788].

b) Suchmaschinen

Die schnelle, umfassende und kostengünstige Erhältlichkeit von Informationen hat das Bedürfnis nach der Suche, Filterung und Übermittlung in den Vordergrund gerückt[789]. Die Informationssuche im Internet erfolgt meistens mit Hilfe von Suchmaschinen, die entsprechend spezifischer Suchanfragen der Nutzer eine Auswahl der verfügbaren Daten vornehmen und übersichtsartig zur Verfügung stellen[790]. Die Suchresultate werden durch Hyperlinks zugänglich gemacht. Dieser rein mechanisch-technische Vorgang nähert die Suchmaschinen an die Access-Provider an[791]. Werden dagegen eigene Inhalte generiert, wird der Betreiber zum Content-Provider[792].

Die Zielsetzung vieler Suchmaschinen hängt in Teilen von der Sammlung grosser Mengen an nutzerspezifischen Informationen ab[793]. Dazu gehören beispielsweise IP-Adressen, Suchverläufe und personenbezogene Angaben bei der Registrierung für bestimmte Dienstleistungen. Die Speicherung der Suchanfragen ermöglicht Rückschlüsse hinsichtlich der Interessen, Verbindungen und Absichten der Nutzer. Die Suchverläufe können daher umfassende und sensitive Personendaten enthalten[794]. In zeitlicher Hinsicht speicherte beispielsweise Google Suchanfragen für 18 Monate mit folgenden Angaben: IP-Adresse, von welcher die Suche durchgeführt wurde, Domain, über die die Suche gestartet wurde, Tag und Uhrzeit der Suchanfrage, der eingegebene Suchbegriff, Informationen über den Browser und die ID-Nummer des Cookies, über die festgestellt werden kann, ob und wie der Dienst bereits einmal benutzt wurde[795]. Nachdem sich das Unternehmen der Forderung nach der Löschung der vollständigen IP-Adressen von alten Suchanfragen lange widersetzt hatte, werden nun die letzten Ziffern nach neun Monaten gelöscht. Die Daten können dadurch noch immer über die Jahre hinweg verglichen werden, jedoch nicht mehr auf individueller, sondern nur noch auf regionaler Basis[796]. Ein weiterer Konflikt ergab sich zwischen der französischen Datenschutzbehör-

787 HANSEN, 90.
788 HANSEN, 91; eingehend WALDEN, in: Millard, 285 ff.
789 SHAPIRO/VARIAN, 6.
790 SHAPIRO/VARIAN, 6; WEBER, E-Commerce, 391.
791 BURGSTALLER/MINICHMAYR, 162.
792 BURGSTALLER/MINICHMAYR, 163.
793 Siehe zur Zielsetzung vorne C.I.1.2 b).
794 STROWEL, 209; WEICHERT, 286.
795 WEICHERT, 287.
796 MAYER-SCHÖNBERGER/CUKIER, 111.

de (Commission Nationale de l'Informatique et des Libertés, CNIL) und Google im Zusammenhang mit der Konsolidierung der Nutzungsbestimmungen verschiedener Dienste[797]. Zentral sind hier die Fragen nach der Erhebung und Kombination von Daten über verschiedene Dienste hinweg sowie die Kontrollmöglichkeiten über diese Daten seitens der Nutzer[798]. Problematisch gestaltet sich im Weiteren die Kontrolle über persönlichkeitsverletzende Inhalte, die durch Suchmaschinen erhalten bleiben[799]. Wie erwähnt anerkannte der EuGH jedoch in seinem kürzlich ergangenen Urteil den Anspruch auf ein Recht auf Vergessen gegenüber Suchmaschinen[800]. Zudem wurde darin ausdrücklich festgehalten, dass die Datenbearbeitung durch Suchmaschinen die Kriterien in Art. 2 lit. b RL 95/46/EG erfüllt und die Vorgänge als «Verarbeitung» einzustufen sind[801]. Darüber hinaus wurde auch die Verantwortlichkeit aus Art. 2 lit. d RL 95/46/EG bejaht[802].

c) Soziale Netzwerke

Soziale Netzwerke stehen emblematisch für den Wandel von Kommunikationsformen im digitalen Zeitalter. Sie umfassen Kommunikationsplattformen, die dem Individuum den Beitritt zu oder die Erstellung von Netzwerken Gleichgesinnter erlauben[803]. Soziale Netzwerke und auch Videoportale basieren darauf, dass Nutzer Informationen mit anderen teilen[804]. Die Informationen können sich hierbei auf den Nutzer selbst oder auf Dritte beziehen[805]. Hinsichtlich der ausgetauschten Daten bestehen verschiedene Konfliktpotentiale, so beispielsweise die Verbreitung persönlichkeitsverletzender oder ur-

797 Die französische Datenschutzbehörde wurde durch die Artikel 29-Datenschutzgruppe mit der Untersuchung beauftragt. Diese wiederum wurde im Rahmen der RL 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr eingerichtet; siehe dazu RL 95/46/EG, E. 65.

798 Siehe eingehend zu diesem Konflikt EGGIMANN/TAMÒ, 58 ff.

799 MEILI, 29.

800 Siehe vorne B.II.2.4 c)(1).

801 EuGH vom 13. Mai 2014, C-131/12, Rn. 28.

802 EuGH vom 13. Mai 2014, C-131/12, Rn. 32 ff. Nach Ansicht des EuGH ändert daran auch die Möglichkeit von Websitebetreibern den Ausschluss vom Suchindex beispielsweise mit Hilfe von Ausschlussprotokollen wie «robot.txt» zu signalisieren nichts. In Zusammenhang mit dieser Argumentation ist die Feststellung in Rn. 84 des Urteils zu sehen, wonach auf einer Website veröffentliche Informationen einfach auf andere Websites übertragen werden könnten und der Betroffene aufgrund der dann notwendigen Durchsetzung gegenüber den einzelnen Websitebetreibern nicht mehr wirksam geschützt werden könne.

803 Siehe die Definition der Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 12 June 2009, 4.

804 MULLIGAN/KING, 994.

805 Siehe LINDSAY, 324, der indessen nur auf Informationen hinweist, die Nutzer über sich teilen.

heberrechtlich geschützter Inhalte[806]. In zeitlicher Hinsicht steht in Bezug auf die Datenbearbeitung in Unternehmen auch hier der Erhalt von Daten im Vordergrund. Informationen, die in sozialen und anderen Netzwerken geteilt worden sind, können über einen unbekannt langen Zeitraum hinweg fortbestehen[807]. Dieser Fortbestand ergibt sich einerseits dadurch, dass einmal verbreitete Daten durch Dritte einfach kopiert werden können. Andererseits kann es auch im Interesse der Anbieter liegen, die Daten nicht umgehend zu löschen.

Im Hinblick auf die Löschung von Nutzerprofilen wird insbesondere das soziale Netzwerk Facebook kritisiert. Ursächlich sind hierbei nicht technische Probleme bei der Löschung der Daten, sondern wirtschaftliche Anreize; der Erhalt der Daten aus dem Nutzerprofil ermöglicht ehemaligen Nutzern, die sich für eine Rückkehr entscheiden, eine einfache Wiederherstellung ihres Profils[808]. Die aktuellen Datenschutzbestimmungen von Facebook[809] unterscheiden zwischen der Deaktivierung und der Löschung des Profils. Die Deaktivierung dient dem erwähnten Ziel einer möglichen Reaktivierung des Profils. In diesem Fall erfolgt ausdrücklich keine Löschung der Daten. Bei der Löschung wird darauf hingewiesen, dass diese normalerweise einen Monat in Anspruch nimmt und einige Informationen bis zu 90 Tage in Backups oder Logfiles erhalten bleiben könnten[810].

5.5 Das zeitliche Argument im Besonderen

Übergeordnet führt die technologische Entwicklung in der heutigen Zeit zu einer verstärkten Schriftlichkeit der Kommunikation; vieles wird trotz seines flüchtigen und beiläufigen Charakters in Form digitalen Texts übermittelt und bleibt dadurch erhalten[811]. Durch diesen Erhalt bleiben die Inhalte in ihrer ursprünglichen Form wahrnehmbar, wobei sich die Wahrnehmung selbst und die mit ihr einhergehenden Wertungen verschieben können. Aufgrund der Abhängigkeit zwischen Information und Wahrnehmung verschiebt sich die (wahrgenommene) Qualität einer Information über die Zeit. Eine ursprünglich wenig relevante Information kann so, in einem anderen Kontext oder

806 WEBER, E-Commerce, 479.

807 Siehe EDWARDS/BROWN, 211.

808 Siehe The New York Times, «How Sticky Is Membership on Facebook? Just Try Breaking Free», February 11, 2008.

809 Abrufbar unter: http://www.facebook.com/about/privacy/your-info, abgerufen am 29.44.2014.

810 Dass dem möglicherweise nicht so ist und die Daten trotz Löschung längerfristig erhalten bleiben, lässt der Fall von Max Schrems vermuten. Dieser erhielt auf Anfrage eine PDF im Umfang von 1'222 Seiten mit persönlichen Daten, die er bereits gelöscht glaubte; siehe FAZ, «Auf Facebook kannst du nichts löschen», 25. Oktober 2011.

811 SCHENK, 202.

einem anderen Adressatenkreis, plötzlich eine grosse Relevanz erlangen. Die Qualität der Information ist auch aus individueller Sicht nicht konstant. Entscheidend ist die Einstellung gegenüber dem Vergangenen, unabhängig davon, ob diese Einstellung auf zutreffenden Erinnerungen beruht[812]. Das Individuum ist seiner Vergangenheit grundsätzlich nicht einfach ausgeliefert. Selbst bei sehr traumatischen Erlebnissen in der Vergangenheit ist die Deutung der rekonstruierten Erinnerung entscheidend[813]. In Abgrenzung zu dieser «Deutungshoheit» kann auch dem tatsächlichen, individuellen Vergessen eine wichtige Funktion zukommen. Das menschliche Gedächtnis kann Erinnerungen unzugänglich machen, um mit beunruhigenden und beängstigenden Erfahrungen fertig zu werden. Die dafür verantwortlichen Mechanismen sind jedoch nur schwer fassbar[814]. Die Macht über das Abrufen und die Wertung der Vergangenheit ist dem Individuum gegenüber Dritten entzogen. Im Vordergrund einer rechtlichen Bewertung steht daher das Interesse des Individuums an einer Beschränkung sowohl des Erhalts als auch der Verbreitung von Informationen der Vergangenheit. In Bezug auf die Verbreitung von Inhalten knüpft hier das Recht auf Vergessen an[815].

6. Schlussfolgerungen

Im Zeitalter der Individualisierung sind Identitäten Fluch und Segen zugleich, sie schwanken zwischen Traum und Albtraum, ohne dass gesagt werden kann, wann sich das eine ins andere verkehrt[816]. Der Konflikt entsteht im Einzelfall und drängt dann Individuen in unterschiedlichem Ausmass aus der Komposition des eigenen Bildes hinaus; sei das im Verhältnis zu sich selbst, zu einzelnen Dritten oder zur Öffentlichkeit. Gleichzeitig ist die Interaktion mit Dritten Voraussetzung der Erschaffung der eigenen Identität[817]. Dieser kontinuierliche Vorgang findet zunehmend im Dreiecksverhältnis zwischen den jeweiligen Individuen und Unternehmen statt, die den Rahmen für diese Interaktion bieten[818]. Eine Komplikation des Konflikts liegt im verschwommenen Grenzverlauf der Interessen. Das Verhalten von Konsumenten und Nutzern zeigt, dass diese Angebote, die ihre Privatsphäre beeinträchtigen, nicht immer ablehnen. Im Gegenteil, den Bedürfnissen nach dem Schutz der Privatsphäre und nach Kontrolle über personenbezogene Daten stehen Bedürfnisse nach Annehmlichkeit, Effizienz und den

812 ZIMBRADO/BOYD, 103.
813 ZIMBRADO/BOYD, 109.
814 PARKIN, 105.
815 Siehe dazu vorne B.II.1.4.
816 BAUMAN, 32.
817 BAUMAN, 68.
818 MULLIGAN/KING, 991.

zahlreichen weiteren Vorteilen «kostenloser» Angebote im Austausch gegen persönliche Daten entgegen[819]. Den beschriebenen Sachverhalten liegt kein autoritäres oder gar totalitäres Überwachungsregime zugrunde, der Fall liegt wesentlich weniger dramatisch[820]. Die Daten werden in den meisten Fällen freiwillig zu irgendwelchen Zwecken an irgendwelche Stellen übermittelt. Das Problem besteht aus einer zeitlichen Perspektive darin, dass im Einzelfall häufig nicht mehr klar ist, wozu die Daten später tatsächlich verwendet werden und welche Konsequenzen sich aus der Übermittlung letztlich ergeben können[821]. In Anbetracht der grossen Abhängigkeit der gesellschaftlichen Entwicklung von der Informationstechnologie sollte die Perspektive hierbei nicht nur auf die aktuellen Probleme, sondern auch in die Zukunft gerichtet sein[822]. Die weitergehenden Entwicklungen zeigen, dass nicht mehr nur das, was gesagt wird und was andere über einen sagen in einen digitalen Speicher übergeht, sondern zunehmend auch das, was getan wird[823]. Daraus resultiert indessen nicht automatisch ein generell erhöhter Missbrauch von Daten[824]. Ein solcher ist vielmehr immer anhand des einzelnen Konfliktfalls zu beurteilen[825].

II. Konfliktbezug explizit zeitbezogener Normen

1. Normierung der Speicherung

1.1 Ausgangslage

Die explizit zeitbezogenen Normen weisen einen mittelbaren Konfliktbezug auf. Die Aufbewahrung über eine vordefinierte Zeitspanne dient nebst unmittelbaren Dokumentations- und Beweiszwecken – beispielsweise in Form der Berechnungsgrundlage für die geschuldete Steuerschuld – der Lösung antizipierter Konflikte, für die die aufzubewahrenden Daten potentiell von Relevanz sind[826]. Aus Unternehmenssicht sind in Bezug auf diese potentiellen Konflikte entsprechende organisatorische Massnahmen zu

819 CAVOUKIAN, 179; ROSEN, Gaze, 196.

820 Siehe zur «Überängstlichkeit» in Bezug auf die Datenbearbeitung durch Staat und Wirtschaft BULL, 17.

821 SPÄRCK JONES, 293.

822 CORTADA, Technology, 186.

823 Vgl. ROSEN, Forgetting, o.S., der feststellte, dass wir erst anfangen würden zu verstehen, welche Folgen ein Zeitalter hat, in dem so vieles von dem was wir sagen und von dem was andere über uns sagen in einen permanenten und öffentlich digitalen Speicher übergeht. Siehe zur Erfassung auch vorne C.I.5.1.

824 Vgl. dazu BULL, 16.

825 Ähnlich Bull, 12, mit Verweis auf die verbreitete Vorstellung, wonach aus dem potentiellen Missbrauch auf den Missbrauch als Normalfall geschlossen werde.

826 Siehe dazu vorne B.II.3.2.

treffen. Die Archivierung von historisch oder wissenschaftlich relevanten Daten ist für Private dagegen grundsätzlich nicht verbindlich geregelt[827]. Art. 17 Abs. 2 BAG sieht einzig vor, dass sich das Bundesarchiv für die Sicherung von Archiven und Nachlässen von Personen des öffentlichen und privaten Rechts einsetzt und zur Übernahme solcher Archive Verträge abschliessen kann. Die Anbieterpflicht in Art. 6 BAG bezieht sich nur auf die in Art. 1 Abs. 1 BAG genannten Stellen. Auch die Ablieferung gedruckter oder elektronischer Publikationen erfolgt in der Schweiz gemäss Art. 3 Abs. 2 Nationalbibliothekgesetz (NBibG) auf Bundesebene ausschliesslich gestützt auf Vereinbarungen mit Verbänden der Verleger und der Hersteller selbst[828]. Der sich hieraus ergebende Konflikt liegt im Interesse am Erhalt der Daten insbesondere für historische oder wissenschaftliche Zwecke und in der Nichterhaltung bzw. Löschung dieser Daten[829].

1.2 Aufbewahrungspflichten

a) Organisation der Gesellschaft

Entsprechend den Grundregeln der *Corporate Governance* muss der Verwaltungsrat ein internes Kontroll-System aufbauen[830]. Die Sicherstellung der Compliance ist nach Art. 716a Abs. 1 Ziff. 5 OR eine Kernaufgabe des Verwaltungsrates, wobei die konkreten Massnahmen zur Umsetzung eines solchen Systems im Einzelfall an den entsprechenden Risiken auszurichten sind[831]. Die Revisionsstelle prüft nach Art. 728a Abs. 1 Ziff. 3 OR, ob ein solches System besteht und bestätigt dies gemäss Art. 728b Abs. 1 OR im Revisionsbericht. Zudem obliegt es dem Verwaltungsrat ein Verfahren zur Beurteilung der Risiken im Unternehmen zu implementieren. Die Durchführung dieser Risikobeurteilung ist gemäss Art. 961c Abs. 2 Ziff. 2 OR im Lagebericht zu dokumentieren. Die informationsbezogenen Risiken betreffen insbesondere den Verlust, die Veränderung, die Preisgabe an Unberechtigte oder auch die mangelnde Beweisqualität vorhandener Informationen[832]. Auch aufsichtsrechtlich bestehen in vielen weiteren Gesetzen Aufbewahrungsvorschriften[833]. Das Eigentum und die Verantwortung für *Records* liegen bei der Gesamtorganisation, nicht beim einzelnen Mitarbeiter[834]. Die

827 Eine Ausnahme bildet die Pflicht zur Erhaltung von Programmen in Art. 21 RTVG; siehe dazu vorne B.I.3.2.

828 SCHWEIZER/BAUMANN, 241, 252, mit Verweis auf die abweichende Regelung in Deutschland und Frankreich.

829 Dieser Aspekt ist in Teil E. wieder aufzunehmen.

830 BEGLINGER et al., 39; LUTTER, 437.

831 BEGLINGER et al., 39.

832 BEGLINGER et al., 29.

833 Siehe eine Auswahl bei WEBER, Aufbewahrung, 71.

834 TOEBAK, in: Coutaz et al., 260.

nachhaltige Umsetzung des *Records Management* in einer Organisation bedingt jedoch von Beginn weg die Definition von Verantwortlichkeiten, die von der Unternehmensleitung genehmigt und durchgesetzt werden müssen[835]. Entsprechend wird die Verantwortung in Bezug auf die Umsetzung der beschlossenen Massnahmen im Innenverhältnis auf einzelne Mitarbeiter übertragen.

b) Haftung

Das Konzept der Haftung weist eine Steuerungsfunktion auf und ist Teil der *Corporate Governance*[836]. Organe der Gesellschaft haften dieser und Dritten gegenüber für Schäden, die durch die Verletzung von Sorgfaltspflichten entstanden sind[837]. Die zivilrechtliche Verantwortlichkeit des Managements richtet sich in der Schweiz nach Art. 716 ff. OR. In der Beurteilung der nach den Umständen angemessenen Sorgfaltspflicht kommt zudem insbesondere auch den internationalen Normen und Standards ein grosser Stellenwert zu. Der Verwaltungsrat und die Geschäftsleitung müssen diese international oder national anerkannten Normen sowie die branchenspezifischen Standards kennen und anwenden, um sich nicht einem erhöhten Haftungsrisiko auszusetzen[838].

Ein weiteres Feld, das zunehmend an Bedeutung gewinnt, ist die Produkthaftung. Unternehmen können im Schadensfall vertraglich oder ausservertraglich für Sach- und Personenschäden haftbar gemacht werden. Die Anforderungen an die Sorgfalt der Unternehmen sind hoch und im Zuge einer Untersuchung muss gegebenenfalls nachgewiesen werden können, dass nach dem massgebenden Stand der Technik in der Entwicklung und Herstellung eines Produkts keine Fehler gemacht wurden. Die Beweisführung erfordert eine möglichst vollständige Dokumentation[839]. Die Haftung ergibt sich hier im Gegensatz zur Verletzung zeitrelevanter Normen indessen nicht direkt aus der Datenbearbeitung, sondern indirekt, indem der Sorgfaltsbeweis an der mangelhaften Datenerhaltung scheitert. Eine unmittelbare Haftung kann sich dagegen auch aus der Aufbewahrung der Daten an sich ergeben, sofern diese einen Personenbezug aufweisen[840]. Die langfristige Archivierung von Daten in übermässiger Menge oder während einer unverhältnismässig langen Dauer kann eine Persönlichkeitsverletzung begründen. In diesem Zusammenhang erscheint auch die handelsrechtliche Aufbewah-

835 HAGMANN, in: Coutaz et al., 275.
836 LUTTER, 417.
837 FÄSSLER, 19; LUTTER, 433 f.
838 FÄSSLER, 53.
839 SCHNEIDER, Amnesie, 36.
840 Vgl. Art. 3 lit. e DSG.

rungsdauer nach Art. 958f Abs. 1 OR über zehn Jahre als lang. Diese ist jedoch auf die Verjährungsfrist in Art. 127 OR abgestimmt[841].

2. Normierung der Verwertung

Bei den explizit zeitbezogenen Normen lassen sich im Hinblick auf die Verwertung der Daten zwei Kategorien unterscheiden: Entweder wird die Verwertung im jeweiligen Gesetz ausdrücklich beschränkt oder sie bleibt dort offen. Der ersten Kategorie sind u.a. die handelsrechtlichen Aufbewahrungsvorschriften zuzuordnen. So dürfen die gemäss Art. 958f Abs. 1 OR während zehn Jahren aufzubewahrenden Geschäftsbücher und Buchungsbelege sowie der Geschäfts- und Revisionsbericht wohl grundsätzlich auch zu anderen als den in Art. 958 OR umschriebenen Zwecken der Rechnungslegung genutzt werden. Indessen ist davon auszugehen, dass das DSG auch im Rahmen der kaufmännischen Buchführung anwendbar ist[842]. Sofern daher Personendaten bearbeitet werden, ist nebst sämtlichen anderen relevanten Bestimmungen des DSG insbesondere auch der datenschutzrechtliche Grundsatz der Zweckbindung gemäss Art. 4 Abs. 3 DSG zu beachten. Demnach wäre eine über den gesetzlich vorgesehenen Zweck hinausgehende Bearbeitung durch eine erneute Einwilligung bzw. durch ein überwiegendes privates Interesse gemäss Art. 13 Abs. 1 DSG zu rechtfertigen. Eine dahingehende ausdrückliche Beschränkung findet sich in der zweiten Kategorie von Normen. So wird in Art. 45b FMG darauf hingewiesen, dass Anbieter von Fernmeldediensten die Standortdaten ihrer Kunden nur bei Einwilligung oder Anonymisierung zu einem anderen Zweck als für die Fernmeldedienste und ihre Abrechnung bearbeiten dürfen[843].

III. Konfliktbezug implizit zeitbezogener Normen

1. Normierung der Speicherung

1.1 Ausgangslage

Die implizit zeitbezogenen Normen des Persönlichkeits- und Datenschutzrechts weisen im Gegensatz zu den explizit zeitbezogenen Normen einen unmittelbaren Konfliktbezug auf. Sie räumen den Betroffenen im Konfliktfall umfassende Abwehransprüche ein. Von diesen konfliktbezogenen Normen zu unterscheiden sind implizit zeitbezogene Normen, die der Dokumentation dienen. Auf diese ist im folgenden Zusammenhang nicht weiter einzugehen.

---

841 BEGLINGER et al., 114; siehe dazu vorne B.I.5.1.

842 BEGLINGER et al., 108.

843 Siehe vorne B.I.3.1.

Das Bewusstsein über die Problematik des Datenerhalts geht bereits auf Empfehlungen des Europarates in den Siebzigerjahren zurück. Zu dieser Zeit war einerseits klar, dass die Speicherung und Nutzung von Daten bestimmten Verboten unterliegen müsste; andererseits hatte der Europarat seine hauptsächliche Rechtfertigung für die Harmonisierung definiert, die insbesondere darin bestand, dass Individuen vor den Schäden einer übermässig langen Datenspeicherung zu schützen sind[844]. Im erklärenden Bericht zur Resolution 73 (22) wurde zudem vorgeschlagen, dass die Regeln über die Dauer des Datenerhalts durch Computer umgesetzt werden könnten, die so zu programmieren wären, dass sie die Daten nach Ablauf der vorgesehen Zeitspanne automatisch löschen[845].

1.2 Persönlichkeitsverletzung

a) Datenspeicherung als Ursache der Verletzung

Sowohl aus Sicht des Persönlichkeitsschutzes als auch aus Sicht des Datenschutzes vermag regelmässig bereits die Erfassung bzw. Speicherung von Daten eine Persönlichkeitsverletzung zu begründen. Anders als im Datenschutzrecht enthält das Persönlichkeitsrecht keine unwiderlegbaren Vermutungstatbestände, wann die Persönlichkeit verletzt ist[846]. Im allgemeinen Persönlichkeitsrecht sind im Hinblick auf die Erfassung von Daten insbesondere das Recht am eigenen Bild[847], an der eigenen Stimme[848], am eigenen Wort[849] sowie der Schutz der Privat- und Geheimsphäre[850] relevant. Im Bereich des Datenschutzes ist im Zusammenhang mit der Erfassung von Daten insbesondere der Grundsatz der Verhältnismässigkeit bedeutend.

b) Massgeblichkeit des Verhältnismässigkeitsgrundsatzes

Voraussetzung für die Beurteilung der Verhältnismässigkeit der Datenbearbeitung ist ein gewisses Mass an Transparenz über die Bearbeitungsvorgänge. Eine erhöhte Transparenz hinsichtlich der Datenbearbeitung verbessert sowohl die Position der rechtsanwendenden Behörden und Gerichte als auch jene der betroffenen Individuen. Die Verbesserung der Transparenz und der Aufsicht an sich können eine materiell zu-

844 WARNER, 83.

845 Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, Adopted by the Committee of Ministers on 26 September 1973, Explanatory Report, Principle 4, No. 23.

846 Siehe dazu vorne B.II.2.3 b)(1).

847 Siehe dazu vorne B.II.1.3 b)(2).

848 Siehe dazu BGE 110 II 419; NOBEL/WEBER, 4 Rn. 76; BUCHER, Persönlichkeitsschutz, Rn. 454;

849 Siehe dazu umfassend GLAUS, Wort, 27 ff.; siehe ferner die Gleichsetzung von Wort und Stimme bei BARRELET/WERLY Rn. 1513.

850 Siehe dazu BGE 118 IV 45; BGE 97 II 101; BGE 119 II 225.

lässige Datenmacht grundsätzlich nicht einschränken[851], sind für die Beurteilung und Kontrolle der Verhältnismässigkeit aber zentral. Wesentlich für die Beurteilung der Verhältnismässigkeit ist insbesondere die Transparenz über die mit der Datenbearbeitung verfolgten Zwecke, da es sich bei der Verhältnismässigkeit um eine Zweck-Mittel-Beziehung handelt[852]. Daraus kann indessen nicht geschlossen werden, dass bei einer Verletzung des Verhältnismässigkeitsgrundsatzes auch eine Verletzung der Zweck*bindung* vorliegt. Der Verhältnismässigkeitsgrundsatz bewertet die Mittel unter Berücksichtigung *eines* Zwecks, wohingegen der Zweckbindungsgrundsatz die Fixierung und Erkennbarkeit *des* Zwecks vorsieht. Der zu betrachtende Zweck muss nach hier vertretener Auffassung nicht identisch sein. Entsprechend kann eine Datenbearbeitung gegen den Zweckbindungsgrundsatz verstossen und dennoch verhältnismässig sein. Der Zweckbindungsgrundsatz ist hier in Bezug auf die Speicherung von Daten vielmehr deshalb nicht relevant, da dieser – abgesehen von einer angemessenen Bekanntgabe – erst bei weiteren Bearbeitungen von Daten zu anderen als den ursprünglich angegebenen Zwecken verletzt wird.

Die Anwendung des Verhältnismässigkeitsgrundsatzes ist auf ein hoheitliches Verhalten ausgerichtet und auch seine Entstehung kann darauf zurückgeführt werden[853]. Fraglich ist, ob dem Prinzip unter Privaten die gleiche Bedeutung wie im öffentlichen Sektor zukommen soll[854]. EPINEY bejaht diese Frage insbesondere unter Verweis auf fehlende Hinweise dafür, dass dem Verhältnismässigkeitsgrundsatz nach Art. 4 Abs. 2 DSG gegenüber Behörden eine andere Tragweite zukommen soll. Trotz dieser Voraussetzung wird festgehalten, dass die «notwendigerweise einzelfallbezogene Anwendung» des Verhältnismässigkeitsgrundsatzes anders ausfallen könne, je nachdem ob Private oder Behörden betroffen seien – wobei das Prinzip als solches gleichermassen gelten soll[855]. Obwohl die Anwendung des Grundsatzes unter Privaten nach wie vor als fragwürdig erscheint, ist dieser Auffassung in Anbetracht des geltenden materiellen Rechts zuzustimmen. Möglich bleibt eine weite Auslegung im Einzelfall.

---

851 VON LEWINSKI, 216.

852 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 24.

853 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 26.

854 PETER, Datenschutzgesetz, 132 ff.

855 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 26.

1.3 Rechtswidrigkeit

a) Interessenabwägung

(1) Relevante Interessen

Eine Persönlichkeitsverletzung kann durch die Interessen des Verletzers selbst gerechtfertigt werden[856]. Der Verletzer kann entsprechend jene Vorteile zur Rechtfertigung der Persönlichkeitsverletzung anführen, die ihm selber aus der persönlichkeitsverletzenden Handlung erwachsen[857]. Der Verletzer kann aber nicht nur seine eigenen Interessen geltend machen[858]. Die Lehre anerkennt, dass der Verletzer seine Handlung auch mit den Interessen des Verletzten rechtfertigen kann[859]. In diesem Fall stehen sich die Interessen am Ausbleiben sowie jene an der Vornahme der verletzenden Handlung gegenüber. Das Interesse an der Verminderung der Verletzung vermag den Eingriff selbst jedoch nicht zu rechtfertigen[860]. Die Verminderung einer im Interesse des Geschädigten selbst erfolgten Verletzung ist nach hier vertretener Auffassung vielmehr als Gebot der Verhältnismässigkeit ohnehin anzustreben. Die Relevanz der Interessen privater Dritter zur Rechtfertigung einer persönlichkeitsverletzenden Handlung kann sowohl aus Gesetz als auch aus Vertrag begründet werden[861]. Der Verletzte kann entsprechend Art. 28 ZGB gegen jeden klagen, der an der Persönlichkeitsverletzung mitgewirkt hat[862]. Entsprechend dazu muss der Beklagte die Interessen all dieser Mitwirkenden auch zu seinen Gunsten geltend machen können[863]. Darüber hinaus können auch Interessen von Dritten geltend gemacht werden, die nicht an der Persönlichkeitsverletzung mitgewirkt haben[864].

Nebst überwiegenden privaten Interessen können unter Anwendung von Art. 28 ZGB auch öffentliche Interessen eine Persönlichkeitsverletzung rechtfertigen. Dazu zählen einerseits die (bereits durch Art. 6 Abs. 1 ZGB abgedeckten) öffentlich-rechtlichen

---

856 TERCIER, Rn. 677 ff.

857 GEISER, Persönlichkeitsverletzungen, Rz. 9.32; siehe zu den Interessen vorne C.I.

858 Siehe zur älteren Lehre, nach der grundsätzlich nur die eigenen Interessen des Verletzers relevant waren TERCIER, Rn. 682.

859 TERCIER, Rn. 673 ff.

860 GEISER, Persönlichkeitsverletzungen, Rz. 9.38.

861 Siehe zur gesetzlichen und vertraglichen Grundlage TERCIER, Rn. 684; zur Ausweitung insbesondere auf die Geschäftsführung ohne Auftrag gemäss Art. 422 Abs. 1 OR GEISER, Persönlichkeitsverletzungen, Rz. 9.35.

862 Siehe dazu hinten D.II.2.3 b).

863 GEISER, Persönlichkeitsverletzungen, Rz. 9.36; vgl. auch BGE 101 II 199.

864 GEISER, Persönlichkeitsverletzung, Rz. 9.36, mit Verweis auf BGE 101 II 199, wo das Bundesgericht den Ärzten, die trotz fehlender Zustimmung der Angehörigen eine Organentnahme vornahmen, der Berufung auf das Interesse des Organempfängers folgte.

Normen, wozu beispielsweise das Handeln von Strafverfolgungsbehörden zählt[865]. Andererseits erfasst Art. 28 Abs. 2 ZGB das private Handeln des Einzelnen im Interesse einer Personenmehrheit oder der Allgemeinheit[866]. Dabei handelt es sich nicht um Interessen im technischen Sinn[867].

(2) Überwiegendes Interesse

Gemäss Art. 28 Abs. 2 ZGB dient das überwiegende private oder öffentliche Interesse der Rechtfertigung einer Persönlichkeitsverletzung. Die Rechtfertigung einer Persönlichkeitsverletzung durch ein überwiegendes privates oder öffentliches Interesse erfordert die Schutzwürdigkeit der verfolgten Ziele und der dazu verwendeten Mittel[868]. Die Interessenabwägung im Einzelfall bestimmt sich nach dem jeweiligen Schwerpunkt der Betrachtung und ist geprägt von kulturellen und sozialen Anschauungen[869]. Das private Interesse besteht um der Einzelperson oder um einiger weniger Einzelpersonen willen, das öffentliche Interesse um einer Vielzahl von Personen oder um der Allgemeinheit willen[870]. Die Unterscheidung ist prinzipiell unbedeutend, Art. 28 Abs. 2 ZGB schützt beide Interessen gleichermassen[871].

Ein anerkanntes öffentliches Interesse besteht im Informationsbedürfnis, das aus den Grundrechten der Meinungsäusserungs- und der Pressefreiheit hervorgeht[872]. Für das Verbreiten von Unwahrheiten besteht dagegen kein Rechtfertigungsgrund, da ein öffentliches Interesse an der Unwahrheit nicht begründet werden kann[873]. In der Rechtsprechung wurde das Informationsbedürfnis soweit indessen nur als Rechtfertigungsgrund im Rahmen der Presseberichterstattung über Personen des öffentlichen Lebens

865 TERCIER, Rn. 691; GEISER, Persönlichkeitsverletzungen, Rz. 9.40.
866 GEISER, Persönlichkeitsverletzungen, Rz. 9.41.
867 TERCIER, Rn. 692.
868 PEDRAZZINI/OBERHOLZER, 145; BGer vom 27.5.2003, 5C.26/2003.
869 Siehe dazu NEBEN, 180 ff.
870 TERCIER, Rn. 686; AEBI-MÜLLER, Rn. 246.
871 GEISER, Persönlichkeitsverletzung, Rz. 9.29.
872 BRÜCKNER, Rn. 458; HAUSHEER/AEBI-MÜLLER Rz. 12.31; PEDRAZZINI/OBERHOLZER, 147 f.; NOBEL, 27 f.
873 BGE 120 II 227; BGE 111 II 214; BGE 91 II 406.

angeführt[874]. Im Weiteren können nach bundesgerichtlicher Rechtsprechung auch wirtschaftliche Interessen die Beeinträchtigung von Persönlichkeitsrechten rechtfertigen[875].

b) Bewertung der Interessen

(1) Relevanter Zeitpunkt

In zeitlicher Hinsicht ist nicht nur der Moment der persönlichkeitsverletzenden Handlung, sondern auch die Entstehung des Interessenkonflikts und die mögliche Einflussnahme der Parteien relevant[876]. Die Abwägung kann nicht allein abstrakt erfolgen, die Bedeutung der Interessen für die Parteien muss im Einzelfall bewertet werden[877].

(2) Wertordnung

Die Wertordnung ergibt sich aus der Gesamtheit der Rechtsordnung[878]. Zu beachten ist hierbei, dass die gesetzlichen Entscheide auf bestimmten Konfliktsituationen beruhen und entsprechend nicht nur den Wertunterschied der Interessen, sondern meistens auch weiterer Faktoren, wie beispielsweise die Rechtssicherheit und die Praktikabilität einer Lösung, miteinbeziehen[879]. Klare Lösungen können dort erzielt werden, wo sich isolierte Interessen gegenüberstehen[880].

(3) Rangordnung der Güter

Grundsätzlich ist davon auszugehen, dass die Rechtsordnung die Persönlichkeit höher bewertet als die wirtschaftlichen Güter[881]. Darüber hinaus können auch wirtschaftliche Interessen für die Interessenabwägung bedeutend sein[882]. Innerhalb der Persönlich-

---

874 BGE 127 III 481; BGE 126 III 212; BGE 126 III 307; BGE 122 III 449; BGE 97 II 97; zum Ganzen HAUSHEER/AEBI-MÜLLER, Rz. 12.23 ff.

875 Siehe BGE 136 III 410, wo die Observation durch eine Versicherungsgesellschaft zu beurteilen war. Das Bundesgericht stellt in E. 2.2.3 fest, dass die Zulässigkeit der Observation insbesondere vom betroffenen Persönlichkeitsrecht und von der Schwere des Eingriffs abhängt. Als entscheidend wird u.a. die Art der Versicherungsleistung bzw. die Höhe der Forderung erachtet. Im Rahmen der Interessenabwägung wurde einerseits das überwiegende private Interesse der Versicherungsgesellschaft als auch das überwiegende öffentliche Interesse der Versichertengemeinschaft anerkannt. Siehe zum Ganzen auch GEISER, Persönlichkeitsverletzungen, Rz. 9.31 ff., der höchstens ein anderes absolutes subjektives Recht als höherwertig erachtet.

876 GEISER, Persönlichkeitsverletzungen, Rz. 9.53. Vgl. ferner Art. 3 Abs. 1 lit. b. Raumplanungsverordnung vom 28. Juni 2000, SR 700.1.

877 GEISER, Persönlichkeitsverletzungen, Rz. 9.52; Vgl. auch die explizite Anordnung in Art. 3 Abs. 1 der Raumplanungsverordnung vom 28. Juni 2000, SR 700.1.

878 GEISER, Persönlichkeitsverletzungen, Rz. 954; HUBMANN, Interessenabwägung, 101.

879 GEISER, Persönlichkeitsverletzungen, Rz. 9.54.

880 GEISER, Persönlichkeitsverletzungen, Rz. 9.54; HUBMANN, Interessenabwägung, 101.

881 TERCIER, Rn. 598; siehe bereits vorne B.II.1.3 e)(4).

882 TERCIER, Rn. 681.

keitsaspekte lassen sich der Leib und die Menschenwürde, die insbesondere die Freiheit und die Ehre umfasst, als Kernbereiche definieren[883]. Innerhalb der wirtschaftlichen Güter ergibt sich die Rangordnung aufgrund einer Gegenüberstellung der entsprechenden Geldwerte[884].

(4) Öffentliche Interessen im Besonderen

Bei der generellen Wertung einzelner Rechtsgüter sind die öffentlichen Interessen bereits mitberücksichtigt. Die höhere Gewichtung des Kernbereichs des Persönlichkeitsrechts gegenüber wirtschaftlichen Werten entspricht einer gesellschaftlichen Wertung, die das Interesse der Allgemeinheit an der Entfaltung der Persönlichkeit umfasst[885]. Generell konnten die öffentlichen Interessen gegenüber den privaten Interessen als vorrangig erachtet werden[886]. Von diesem generellen Vorrang ist heute nicht mehr auszugehen, massgeblich ist entsprechend stets das Verhältnis zwischen dem angestrebten Ziel und der Schwere der Verletzung[887]. In Abgrenzung zur Wertverschiebung aufgrund eines bestimmten Rechtsguts kann sich die Wertverschiebung auch aus dem konkreten Sachverhalt ergeben. Besonders zu berücksichtigen sind hierbei Handlungen, die die Ausübung von Grundrechten betreffen[888].

(5) Interessennähe

Überwiegend ist das Interesse nur dann, wenn die Vorteile für die handelnde Person im Gegensatz zu den Nachteilen des Betroffenen als wichtiger erscheinen[889]. Die Interessennähe ist sowohl nach objektiven als auch nach subjektiven Kriterien zu bewerten. Objektiv ist entscheidend, wie stark sich die Verletzung nach aussen manifestiert[890]. Die Verletzung ist beispielsweise nicht gleich intensiv, wenn die Indiskretion von der nächsten Umgebung des Betroffenen oder von einem ihm vollkommen unbekannten Personenkreis wahrgenommen wird; je grösser die Zahl der Empfänger und je näher ihre Beziehung zum Betroffenen, desto schwerer wiegt der Eingriff[891]. In subjektiver Hinsicht ist relevant, wie viel dem Betroffenen tatsächlich am Schutz seiner Interessen

883 MASTRONARDI, 62; JÄGGI, 215a.
884 GEISER, Persönlichkeitsverletzungen, Rz. 9.56.
885 GEISER, Persönlichkeitsverletzungen, Rz. 9.58.
886 SPECKER, 250: «Besser der einzelne bringe zum Wohle der Gesamtheit ein Opfer, als dass das Ganze Not leidet und in der Entwicklung gehemmt wird.».
887 Das ergibt sich bereits aus Art. 5 Abs. 2 BV.
888 GEISER, Persönlichkeitsverletzungen, Rz. 9.58 f.
889 GEISER, Persönlichkeitsverletzungen, Rz. 9.62.
890 GEISER, Persönlichkeitsverletzungen, Rz. 9.63.
891 RIKLIN, 145.

liegt. Das heisst weder, dass auf individuelle Empfindlichkeiten abgestellt wird[892] noch dass von einem Verzicht auf die Geltendmachung des Persönlichkeitsschutzes auszugehen ist[893]. Die Wertung der Interessen verschiebt sich jedoch; wird eine Verletzung ohne relevante Gründe über eine längere Zeit untätig hingenommen, ist davon auszugehen, dass die Verletzung für den Betroffenen kein grosses Opfer darstellt[894].

(6) Ursache des Konflikts

Die Interessenabwägung erfolgt nicht statisch; im Rahmen einer sinnvollen Abwägung ist vielmehr zu berücksichtigen, wie es zum Konflikt gekommen ist[895]. «Aus dem Achtungsanspruch, den alle Werte mit sich führen, folgt, dass der Mensch sein Handeln so einrichten soll, dass daraus nicht eine Gefahr für fremde Güter entsteht»[896]. Im Umkehrschluss kann aus dieser Obliegenheit zur Reduktion bzw. Vermeidung von Gefahren keine Pflicht zum Schutz eigener Interessen abgeleitet werden, jedoch verschiebt sich die Wertung, sofern jemand eigene Güter einer Gefahr aussetzt[897]. Bei der Interessenabwägung ist somit stets zu berücksichtigen, wessen Verhalten zu einem Konflikt gegensätzlicher Interessen geführt hat[898]. Insbesondere Personen, die durch öffentliche Handlungen das Interesse der Allgemeinheit wecken, tragen damit zum Interessenkonflikt bei[899]. Das gilt sowohl für sogenannte absolute Personen der Zeitgeschichte[900], die das öffentliche Interesse durch bewusstes Handeln hervorrufen als auch für die sogenannten relativen Personen der Zeitgeschichte, die einmalig und möglicherweise ungewollt im Rampenlicht stehen[901].

Für den Anspruch eines Rechts auf Vergessen ist nicht nur die Handlung relevant, die Gegenstand der Veröffentlichung bildet, sondern auch das spätere Verhalten einer Person[902]. Der Anspruch auf Vergessen wiegt schwerer, wenn sich die Person von ihrem

892 TERCIER, Rn. 481; BGE 105 II 163.
893 BGE 109 II 361 f.
894 GEISER, Persönlichkeitsverletzungen, Rz. 9.63.
895 GEISER, Persönlichkeitsverletzungen, Rz. 9.70.
896 HUBMANN, Interessenabwägung, 119.
897 HUBMANN, Interessenabwägung, 120.
898 GEISER, Persönlichkeitsverletzungen, Rz. 9.70; HUBMANN, Interessenabwägung, 120; RIEDER, 35.
899 GEISER, Persönlichkeitsverletzungen, Rz. 9.71.
900 Siehe zum Begriff LANDWEHR, 66 f., 92 f.
901 GEISER, Persönlichkeitsverletzungen, Rz. 9.71; RIKLIN, 227 f.; NOBEL, 156.
902 BARRELET/WERLY, Rn. 1538.

früheren Verhalten distanziert, als wenn sie ihr späteres Handeln als Fortsetzung auffasst und dieses für die Gegenwart von Bedeutung bleibt[903].

c) Interessenabwägung im Datenschutzrecht

Gemäss Art. 4 Abs. 1 DSG verletzt die Bearbeitung von Personendaten die Persönlichkeit der betroffenen Person immer dann, wenn der Bearbeitung ein unrechtmässiges Verhalten zugrunde liegt. Ein Verhalten ist unrechtmässig, wenn ohne Rechtfertigung gegen eine Norm der schweizerischen Rechtsordnung verstossen wird[904]. Ausserhalb des DSG sind nur Verletzungen von Verhaltensnormen erfasst, die den Schutz der Persönlichkeit einer Person direkt oder indirekt bezwecken[905]. Das Vorliegen einer Rechtfertigung beurteilt sich nach den für die jeweilige Verhaltensnorm relevanten Regeln. Innerhalb der Anwendbarkeit des DSG ist die Bearbeitung von Personendaten gemäss Art. 13 Abs. 1 DSG nur dann widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist[906]. Art. 13 Abs. 1 DSG wiederum statuiert, was für das Persönlichkeitsrecht sowieso gilt. Der Wortlaut und der Sinn der Norm entsprechen Art. 28 Abs. 2 ZGB[907].

2. Normierung der Verwertung

2.1 Medienrechtlicher Hintergrund

Vor dem Hintergrund der Erfindung des Rotationsdrucks und der mit diesem aufkommenden Boulevardpresse stellten bereits WARREN/BRANDEIS fest, dass sich der Schaden aus der Verwertung persönlicher Details nicht auf jene beschränken würde, die dem Journalismus oder anderen Unternehmungen unmittelbar ausgesetzt seien. Vielmehr gelte hier wie in anderen Handelszweigen, dass das Angebot die Nachfrage schaffe. Jede Verwertung werde zur Saat für neue Hechelei und senke in direkter Proportionalität die sozialen Standards sowie die Moral. Zudem stellten sie fest, dass auch scheinbar harmlose Gerüchte durch eine weitrechende und fortwährende Streuung grossen Schaden anrichten könnten[908]. POSNER hält dem aus ökonomischer Warte ent-

---

903 GEISER, Persönlichkeitsverletzungen, Rz. 9.71; WERRO, 291; BGE 111 II 213 f.

904 ROSENTHAL, Handkommentar DSG, Art. 4 N 6.

905 ROSENTHAL, Handkommentar DSG, Art. 4 N 7.

906 ROSENTHAL, Handkommentar DSG, Art. 4 N 3. Werden die Bearbeitungsgrundsätze eingehalten, ist eine vorgängige Einwilligung («opt-in») grundsätzlich nicht erforderlich; siehe dazu ROSENTHAL, Handkommentar DSG, Art. 12 N 25.

907 ROSENTHAL, Handkommentar DSG, Art. 13 N 1.

908 WARREN/BRANDEIS, 195 f.

gegen, dass das Angebot nie die Nachfrage schaffe und der Anstieg von Klatschkolumnen vielmehr auf das steigende Einkommen zurückzuführen sei. Das Beobachten in wohlhabenden Gesellschaften sei aufgrund der stärker entwickelten Privatsphäre und der (zeitlich bedingten) höheren Opportunitätskosten im Vergleich zu ärmeren Gesellschaften teurer[909]. In der Wohlstandsgesellschaft sei entsprechend nach alternativen Methoden gesucht worden, um sich über die Lebensweise der anderen zu informieren und die Presse sei dieser Nachfrage nachgekommen. POSNER sieht in der dahingehenden Informationsbeschaffung eine legitime und wichtige Spezialisierung der Presse, da die Kosten zur Beschaffung für den Einzelnen zu hoch wären[910].

Im virtuellen Raum erlangt die Diskussion um die Verwertung von Daten eine neue Dimension, da die erwähnte Funktionsweise der Presse nicht mehr nur von dieser, sondern von einer Vielzahl von Akteuren wahrgenommen werden kann. Die Verbindung und Verbreitung von Daten mittels moderner Technologien erfolgt zudem zu noch tieferen Kosten und reduziert auch den zur Verbreitung notwendigen Zeitaufwand. Aus gesellschaftlicher Sicht erscheinen diese Möglichkeiten vor allem dort problematisch, wo der Datenbearbeiter unbekannt ist und nicht in unmittelbarer Beziehung mit dem betroffenen Individuum steht[911]. Die Entwicklung eines gemeinsamen Normverständnisses und die gezielte Normdurchsetzung werden durch diese Globalität und Anonymität erschwert.

2.2 Verwertungsbeschränkung durch das Recht auf Vergessen

a) Massgeblichkeit der Verwertung

Die rechtliche Beurteilung einer Wiederverbreitung von Inhalten kann sich nicht auf die Feststellung beschränken, dass die Erstverbreitung durch ein öffentliches Interesse gerechtfertigt war. Die Interessenabwägung muss unter Berücksichtigung eines sich über die Zeit vermindernden öffentlichen Interesses an der Information erfolgen, die mit der Zeit wieder dem Schutzbereich der Privatsphäre zugehörig werden kann[912]. Die Anwendung dieses Konzepts bleibt zwangsläufig unscharf, da sich der Anspruch auf Vergessen im Spannungsfeld zwischen der Verhältnismässigkeit, dem Recht auf freie Meinungsäusserung, der Medienfreiheit sowie spezifischen Interessen des Datenbear-

909 Siehe zur historischen Entwicklung der Privatsphäre FRICK, 18 ff.
910 POSNER, 396 f.
911 WORLD ECONOMIC FORUM, Value, 8.
912 LANGER, 4.

beiters befindet[913]. Die Festsetzung einer allgemeingültigen Frist für den Erhalt von Daten erscheint aus dieser Perspektive weder praktikabel noch wünschenswert[914]. Das eigentliche Problem besteht vielmehr im Zugang zu Informationen, der im digitalen Zeitalter grösstenteils ortsunabhängig und gezielt erfolgen kann. So wurden vor dem Zeitalter der Informations- und Kommunikationstechnik Zeitungen in öffentlichen Bibliotheken archiviert, eine automatisierte Suche nach bestimmten Personen oder Ereignissen gab es nicht. In diesem Sinn begünstigte die papierbelassene Aufbewahrung das Vergessen[915].

b) Schlussfolgerungen

Im Bereich der klassischen Medien wird die Verbreitung persönlichkeitsverletzender Inhalte unter Berücksichtigung des öffentlichen Interesses gegebenenfalls durch das Recht auf Vergessen eingeschränkt. Die Rechtsprechung in diesem Bereich zeigt, dass nicht der Erhalt der Daten, sondern die Verbreitung im Vordergrund steht. Im Rahmen der digitalen Medien erscheint dieser Ansatz grundsätzlich unverändert, jedoch kommt hier dem Erhalt der Daten aufgrund des grösseren Verbreitungspotentials eine erhöhte Bedeutung zu[916]. In Bezug auf die Haftung für Persönlichkeitsverletzungen stellt sich bei der Datenverwertung durch Suchmaschinen, soziale Netzwerke und Cloud-Anbieter das generelle Problem einer deutlich eingeschränkten Erfolgsaussicht bei der Geltendmachung von Schadenersatzansprüchen. Der Nachweis eines durch die Datenbearbeitung resultierenden Schadens, für den Geldersatz verlangt wird, dürfte in der Praxis regelmässig schwierig zu erbringen sein[917]. Die in Art. 42 Abs. 2 OR vorgesehene Möglichkeit, wonach ein ziffernmässig nicht nachweisbarer Schaden nach richterlichem Ermessen abzuschätzen ist[918], führt nur zu einer Erleichterung der Beweislast ohne diese gänzlich zu beseitigen[919]. Lässt sich die für einen Geldersatz notwendige Vermögenseinbusse nicht bestimmen, kann die Forderung nach Naturalrestitution unter

913 Zu den spezifischen Interessen des Datenbearbeiters zählen insbesondere die wirtschaftlichen Interessen; siehe dazu EuGH vom 13. Mai 2014, C-131/12, Nr. 97.

914 Siehe auch die Schlussfolgerung bei LANGER, 18.

915 BAUMANN, 119; siehe auch das Urteil des EGMR vom 16. Juli 2013, Nr. 33846/07, wo in E. 58, wo auf die erhöhte Kapazität des Internets in Bezug auf die Speicherung und Verbreitung von Informationen im Vergleich zu den Printmedien hingewiesen und zudem festgestellt wird, dass das Internet möglicherweise nie der gleichen Regulierung und Kontrolle unterliegen wird.

916 Siehe BBl 1988 II 416: «Eine Person kann ein Leben lang mit einem Makel behaftet bleiben, wenn Daten mit negativen Angaben über sie auf unbestimmte Zeit aufbewahrt und immer wieder benutzt werden.» Daraus kann geschlossen werden, dass auch die Erhaltung an sich – die Voraussetzung der Verbreitung ist – und nicht nur die Verbreitung als problematisch erachtet wird.

917 ROSENTHAL, Handkommentar DSG, Art. 15 N 40.

918 So der Hinweis bei RAMPINI, in: Maurer-Lambrou/Vogt, Art. 15 N 21, m.w.H.

919 ROSENTHAL, Handkommentar DSG, Art. 15 N 40.

Anwendung von Art. 43 Abs. 1 OR sinnvoller sein[920]. Der Naturalersatz kann auch einen Kontrahierungszwang umfassen[921]. Wird der Vertragsschluss für eine öffentlich angebotene Leistung aufgrund von Feststellungen, die auf einer unrechtmässigen Datenbearbeitung beruhen, verweigert, und trifft das Unternehmen ein Verschulden, kann der Richter den Vertragsschluss somit gegebenenfalls erzwingen[922].

2.3 Weitere Verwertungsbeschränkungen

a) Verhältnismässigkeit

Die Verhältnismässigkeit ist ein entscheidendes Kriterium bei der Beurteilung des zulässigen Umfangs der Informationsverwertung und kommt auch ausserhalb des Datenschutzrechts, wo sie in Art. 4 Abs. 2 DSG ausdrücklich als Datenbearbeitungsgrundsatz genannt wird, zur Anwendung. Danach muss das gewählte Mittel zur Erreichung des beabsichtigten Ziels geeignet sein, die mildeste Massnahme zur Erreichung des Ziels darstellen und das Interessengleichgewicht wahren (Verhältnismässigkeit im engeren Sinn)[923]. Aus dem Grundsatz der Verhältnismässigkeit wird ferner auch die Pflicht abgeleitet, personenbezogene Daten nach einer gewissen Zeit wieder zu löschen[924].

Im medienrechtlichen Bereich wurde beispielsweise der Hinweis auf verbüsste Zuchthausstrafen eines Betroffenen, der zwischenzeitlich in einem ganz anderen Zusammenhang Teil einer medialen Berichterstattung wurde, als unverhältnismässig erachtet[925]. Der Zweck der Medienberichterstattung, in deren Rahmen vom geschäftstätigen Gebaren des Betroffenen hätte gewarnt werden sollen, vermag die Verwertung der zurückliegenden und offenbar zusammenhangslosen Zuchthausstrafen nicht zu rechtfertigen und stellt ein im Verhältnis zu diesem Zweck unzulässiges Mittel dar[926]. Auch eine in der Öffentlichkeit stehende Person braucht nicht zu dulden, dass die Medien mehr über

---

920 ROSENTHAL, Handkommentar DSG, Art. 15, N 40. Naturalrestitution kann unabhängig vom Vorliegen eines Vermögensschadens gemäss Differenztheorie verlangt werden, BGE 129 III 334. In der Praxis spielt die Naturalrestitution gemäss SCHWENZER, Rz. 15.01, jedoch nur eine geringe Rolle.

921 SCHWENZER, Rz. 15.02.

922 ROSENTHAL, Handkommentar DSG, Art. 15 N 40; siehe zum Kontrahierungszwang aufgrund eines Verstosses gegen den allgemeinen privatrechtlichen Grundsatz der guten Sitten BGE 129 III 47; eingehend zur allgemeinen Kontrahierungspflicht ARNET, 241 ff.

923 Siehe u.a. BGE 130 II 438 f.

924 SCHMID, 823, mit dem Hinweis, dass diese Pflicht wohl bereits aus dem Gebot von Treu und Glauben folge; vgl. zum öffentlichen Recht BGE 113 Ia 8; BGE 113 Ia 265; siehe auch bereits vorne B.II.2.4 b).

925 BGE 122 III 457.

926 Vgl. zur Zweck-Mittel-Beziehung der Verhältnismässigkeit vorne C.III.1.2 b).

sie berichten, als durch ein legitimes Informationsbedürfnis gerechtfertigt werden kann[927].

Im arbeitsrechtlichen Bereich wurde der Einsatz eines GPS-Systems in Mitarbeiterfahrzeugen einer im Verkauf und Unterhalt von Feuerlöschern tätigen Unternehmung im Rahmen einer sporadischen Überwachung als verhältnismässig beurteilt. Massgeblich waren das Verwertungsziel der Unternehmung, im Falle einer Funktionsstörung eines Feuerlöschers den Nachweis über die Anwesenheit des Mitarbeiters beim Kunden erbringen zu können und das Mittel einer nicht permanenten Überwachung. Eine permanente Echtzeit-Überwachung wäre hingegen nicht ohne Weiteres als verhältnismässig zu beurteilen[928].

b) Zweckbindung

Die Normierung der Datennutzung erfolgt im Rahmen der implizit zeitbezogenen Normen insbesondere durch das DSG. Bei personenbezogenen Daten kann aus dem Grundsatz der Zweckbindung gemäss Art. 4 Abs. 3 DSG eine Beschränkung abgeleitet werden. Durch die zunehmende Analyse grosser Datenmengen wird der Nutzen jedoch nicht mehr nur im primären Zweck der Datenspeicherung und damit im Zeitpunkt der Datenerfassung definiert, sondern auch durch die weitere Nutzung der Daten[929]. Diese Weiterverwendung von Daten zu anderen Zwecken steht dem Prinzip der an den Zeitpunkt der Datensammlung anknüpfenden Zweckbindung und der dahingehenden Einwilligung entgegen[930]. Das Gleiche gilt für Daten, die für einen gesetzlich definierten Zweck gespeichert werden. Die Durchbrechung der Zweckbindung ist nur durch eine entsprechende Zustimmung des Betroffenen oder durch eine von Beginn weg offene und damit nicht mehr zweckgebundene Einwilligung zu erreichen. Das Einholen einer erneuten Zustimmung scheitert spätestens bei der Frage nach der Praktikabilität. Die zweckoffene Zustimmung ist dagegen ab einem bestimmten Punkt mit dem Prinzip der informierten Zustimmung nicht mehr vereinbar[931]. Das Konzept der Zweckbindung über die Zeit ist damit im Hinblick auf die Nutzung des latenten Werts von Daten zu restriktiv und zum Schutz des Individuums (gegebenenfalls) zu weit[932]. Das Problem

927 BGE 126 III 307; BGE 126 III 212.

928 BGE 130 II 425. Der Grundsatz der Verhältnismässigkeit der Datenbearbeitung ergibt sich im arbeitsrechtlichen Verhältnis spezifisch aus Art. 328 OR und Art. 328b OR sowie aus Art. 26 der Verordnung 3 zum Arbeitsgesetz.

929 MAYER-SCHÖNBERGER/CUKIER, 153.

930 Siehe zur Zweckbindung als Grundprinzip der Datenschutzgesetzgebung vorne B.II.2.3 a)(2).

931 Siehe zur Zustimmung vorne B.II.2.3 b)(2).

932 MAYER-SCHÖNBERGER, 154.

der Verletzung des Zweckbindungsgrundsatzes lässt sich behelfsweise durch die Interessenabwägung auf der Rechtfertigungsebene lösen[933].

3. Normierung der Löschung

Nach Art. 5 Abs. 1 Satz 2 DSG wird der Bearbeiter von Daten, die in Bezug auf ihren Zweck, ihre Bearbeitung oder ihre Beschaffung unrichtig oder unvollständig sind, verpflichtet, alle angemessen Massnahmen zur Vernichtung oder Berichtigung der Daten zu treffen[934]. Die RL 95/46/EG macht im Vergleich zum DSG weitergehende Angaben zur Löschung und verbindet diese mit dem Zweckbindungsgrundsatz. Artikel 6 Abs. 1 lit. b RL 95/46/EG sieht vor, dass personenbezogene Daten «für festgelegte eindeutige und rechtmässige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen». Artikel 6 Abs. 1 lit. e RL 95/46/EG konkretisiert in zeitlicher Hinsicht dahingehend, dass personenbezogene Daten «nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden». Das deutsche BDSG sieht im Vergleich zum schweizerischen DSG unter § 35 BDSG eine dahingehende Konkretisierung des Löschungsanspruchs vor[935].

4. Schlussfolgerungen

Eine wesentliche Eigenschaft von Daten ist ihr unbegrenztes Potential für ihre Wiederverwendung, ihr optionaler Wert. Die Speicherung bildet nur die Voraussetzung zur Realisierung des informationellen Wertpotentials; entscheidend ist letztlich die tatsächliche Nutzung[936]. Die explizit zeitbezogenen Normen statuieren hierbei eindeutige und verbindliche Regeln in Bezug auf den Datenerhalt und implizieren immer auch einen konkreten Zweck. Die Verletzung der explizit zeitbezogenen Normen führt zu einer entsprechenden Verantwortlichkeit. Der Konfliktbezug dieser Normen ist indirekt, da

933 Siehe zum Interessenausgleich durch Sachgerechte Auslegung und ablehnend im Hinblick auf eine weitere Generalklausel bereits WOERTGE, 142.

934 Siehe vorne B.II.2.3 a)(4).

935 Siehe dazu SIMITIS, in: ders., § 35 N 19 ff.; GOLA/KLUG/KÖRFFER, § 35 N 10 ff.; siehe zum Begriff der Löschung vorne A.I.3.2 c)(1).

936 MAYER-SCHÖNBERGER/CUKIER, 122.

die zu erhaltenden Daten nur zur Lösung potentieller Konflikte herangezogen werden. Im Unterschied dazu weisen die persönlichkeits- und datenschutzrechtlichen Bestimmungen einen direkten Konfliktbezug auf, der sich insbesondere in der Interessenabwägung widerspiegelt.

D. Grenzen der Konfliktlösung

I. Grenzen explizit zeitbezogener Normen

1. Endliche Aufbewahrung

1.1 Erfüllung der Aufbewahrungspflicht

Die Grenze explizit zeitbezogener Normen liegt in der Erfüllung der entsprechenden Aufbewahrungspflicht[937]. Die Erfüllung stellt im Rahmen der für den privaten Sektor geltenden Normen in zeitlicher Hinsicht keine nennenswerten Probleme. Die als explizit zeitbezogene Norm zu verstehende Zielsetzung eines «ewigen» Datenerhalts stösst dagegen auf faktische Grenzen[938]. Die Aufbewahrung immenser elektronischer Datenmengen stellt heute ein grosses Problem dar. Bis jetzt bestehen keine sinnvollen technischen Lösungen zur langfristigen Speicherung und Reproduzierbarkeit dieser Daten[939]. Entsprechend wird noch immer auf Papier archiviert[940].

1.2 Löschung

Die explizit zeitbezogenen Normen machen keine Aussagen über die Löschung. Eine allfällige Pflicht dazu kann einzig aus dem Zweckbindungsgebot bzw. aus dem Verhältnismässigkeitsgrundsatz abgeleitet werden[941]. In der Literatur wurden in Bezug auf die Löschung von Daten bereits mehrere Lösungsansätze genannt. ZITTRAIN schlug 2008 einen Reputationsbankrott (*Reputational Bankruptcy*) vor, bei dem bestimmte Kategorien von Daten, insbesondere sensitive Daten, nach ca. 10 Jahren gelöscht werden[942]. Ähnlich ist der Vorschlag von SUNSTEIN, der sich für ein Recht auf Entfernung von falschen und schädlichen Informationen aussprach und insbesondere für Informationen im Internet ein Recht auf *Notice and Take Down* gegenüber Content-Provider ähnlich dem Modell des *Digital Millenium Copyright Act* anregte[943]. MAYER-SCHÖNBERGER setzt dagegen unmittelbar bei den Daten an und sprach sich 2009 in Anlehnung an das menschliche Vergessen für Verfallsdaten aus, die durch die Nutzer

937 FRANKS, 37.

938 SCHENK, 199, verweist darauf, dass sich dieses Problem für Archive schon immer gestellt habe, da das unmittelbare Ziel der im Alltag erstellten Dokumente meistens nicht im langfristigen Erhalt liege und entsprechend keine dauerhaften Materialen und Techniken verwendet würden.

939 SCHNEIDER, Amnesie, 199; siehe zur Dauer ders., 223, wonach Zusagen über die Haltbarkeit von digitalen Archivmechanismen von über 30 Jahren «spekulativ und schlicht unseriös» seien; siehe dagegen BORGHOFF et al., 139, wo 100 Jahre noch als kürzerer Zeitraum bezeichnet werden.

940 WILLI, 34.

941 Siehe dazu vorne C.III. 2.3.

942 ZITTRAIN, 228 ff.

943 SUNSTEIN, 78 f.

selbst gesetzt werden könnten[944]. Die Umsetzung dieses Ansatzes würde durch einen entsprechenden Rechtsrahmen erfolgen[945]. Mit Ausnahme der von SUNSTEIN angeregten Lösung weisen die vorgeschlagenen Ansätze einen expliziten Zeitbezug auf.

Die in der Theorie vermeintlich einfachen Lösungen täuschen über die Komplexität des Vorgangs im Einzelfall hinweg. Die Umsetzung und die Art des Löschens stellen Unternehmen vor grosse Herausforderungen[946]. Unregelmässigkeiten können beispielsweise entstehen, wenn nur die einzelnen Objekte selbst und nicht die Metadaten[947] (oder umgekehrt)[948] gelöscht werden[949]. Eine Möglichkeit der unkoordinierten Löschung entgegenzuwirken ist die Erstellung von Löschungsplänen, die genau festlegen, wann welche Daten zu vernichten sind[950]. Insbesondere im Rahmen von Automatismen müsste sehr genau definiert werden, welche Daten zu löschen sind. So stellt sich beispielsweise auch die Frage, ob die Tatsache, dass Daten gelöscht wurden – und von wem – festzuhalten ist.

2. Schlussfolgerungen

Die Konfliktlösung durch Zeitbezug erfolgt im Rahmen der explizit zeitbezogenen Normen indirekt, indem die potentiell relevanten Daten über eine gewisse Zeit aufzubewahren sind. Dieses Ziel der explizit zeitbezogenen Normen widerspiegelt sich im Handelsrecht in der Übereinstimmung zwischen der zehnjährigen Aufbewahrungsdauer gemäss Art. 958f Abs. 2 OR und der zehnjährigen Verjährungsfrist in Art. 127 OR. Diese zeitliche Grenze der Aufbewahrungspflicht wird stets für bestimmte Datenkategorien definiert, wodurch gleichzeitig eine Konkretisierung der Menge an aufzubewahrenden Daten erfolgt. In zeitlicher Hinsicht lassen sich über den Bestand von Daten daher zwei Aussagen machen: Einerseits besteht keine Pflicht, wonach Daten über den explizit definierten Zeitrahmen hinaus weiter aufzubewahren wären. Andererseits kann nicht davon ausgegangen werden, dass sämtliche Daten mit Überschreitung dieser zeitlich explizit definierten Grenzen auch tatsächlich gelöscht werden. Dieses Ziel könnte im Rahmen der aufgezeigten Vorschläge allenfalls durch den von MAYER-

944 MAYER-SCHÖNBERGER, 169-195.

945 MAYER-SCHÖNBERGER, 330. Relevant erscheint nach hier vertretener Auffassung ein rechtlicher Schutz der entsprechenden technischen Massnahmen; vgl. dazu Art. 39a f. URG).

946 FRANKS, 37.

947 Hierbei handelt es sich um Angaben über das Dokument, beispielsweise in Form von Angaben zum Autor, Fachgebiet, Speicherort, der Codierung oder zur Urheberrechtsangaben, siehe dazu BORGHOFF et al., 10 f.

948 Siehe dazu und zur Bedeutung von Metadaten im Finanzsektor PURI et al., 390 f.

949 FERLE, 30.

950 FRANKS, 100 ff., mit Hinweis auf die Probleme im Zusammenhang mit elektronischen Daten.

SCHÖNBERGER verfolgten Ansatz erreicht werden, wo der Zeitablauf dem einzelnen Datum von Beginn weg eingeschrieben und dadurch explizit definiert wird. Im Gegensatz zum Reputationsbankrott und zum Recht auf *notice and takedown* ergibt sich bei dieser Lösung auch ein geringeres Konfliktpotential in Bezug auf die freie Meinungsäusserung, da der Zeitablauf eines Datums nur vom jeweiligen Urheber für von ihm selbst erstellte Daten gesetzt werden kann[951].

II. Grenzen implizit zeitbezogener Normen

1. Eingrenzung

Die Betrachtung der Grenzen zeitbezogener Normen beschränkt sich auf die Darstellung des Persönlichkeits- und Datenschutzrechts. Bei den weiteren ausgewählten Bestimmungen mit implizitem Zeitbezug ergeben sich im Hinblick auf die Normen selbst keine im vorliegenden Zusammenhang relevanten Problemstellungen. Die Grenzen liegen hier im impliziten Zeitbezug und der dadurch bedingten fehlenden Konkretisierung.

2. Persönlichkeits- und Datenschutzrecht

2.1 Konzeptionelle Grenzen

Die Ausführungen zum schweizerischen Recht haben gezeigt, dass sich der Umfang des Persönlichkeitsschutzes kaum anhand allgemeingültiger Kriterien definieren lässt. Auch innerhalb der Europäischen Union weist der Persönlichkeitsschutz deutliche Unterschiede auf[952]. In Anbetracht der globalen Ausbreitung des Internets und der zunehmenden Verflechtung von Medienunternehmen stellt sich die Frage nach einer Vereinheitlichung der rechtlichen Rahmenbedingungen. Indessen kann weder aus den Grundrechten der Union noch aus der Grundrechtscharta (vgl. Art. 51 Grundrechtscharta) eine dahingehende Kompetenzgrundlage abgeleitet werden. Harmonisierungsmassnahmen können entsprechend nur im Rahmen von Massnahmen zur Gewährleistung der Funktionsfähigkeit des Binnenmarkts legitimiert werden, deren Rechtsgrundlagen im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) enthalten sind. In An-

951 Die Beurteilung von Urheberrechtsverletzungen im Rahmen von *Notice and Take Down* gestaltet sich im Gegensatz zu jener über Persönlichkeitsverletzungen insofern einfacher, als dass erstere keine Interessenabwägung hinsichtlich eines allfälligen Informationsinteresses der Öffentlichkeit und weiterer Dritter umfasst. Die Umsetzung des Reputationsbankrotts würde – abgesehen von den auch hier relevanten Informationsansprüchen – ein Inventar der erfassten Informationen und allenfalls ein entsprechendes Register bedingen. Spätestens bei der Geltendmachung des Bankrotts würden entsprechende Spekulationen sowie das Bedürfnis an der Kenntnis der davon erfassten Informationen geweckt. Vgl. hierzu vorne A.I.3.2 c)(1).

952 Siehe dazu eingehend GÖTTING/SCHERTZ/SEITZ, § 63-68.

betracht der kulturellen, rechtspolitischen und rechtsdogmatischen Unterschiede gestaltet sich eine substantielle Harmonisierung generell schwierig[953]. Eine harmonisierende Wirkung lässt sich dagegen im Rahmen der Rechtsprechung erkennen[954].

In den USA hat PROSSER die Klage aus der Verletzung der Privatsphäre im Rahmen einer Analyse 1960 in vier Kategorien unterteilt: Die erste Kategorie umfasst Eingriffe in die Abgeschiedenheit, Einsamkeit oder privaten Angelegenheiten des Klägers. Die zweite Kategorie umfasst die Veröffentlichung peinlicher privater Informationen. Die dritte Kategorie umfasst Veröffentlichungen, die den Kläger in ein falsches öffentliches Licht rücken. Und die vierte Kategorie umfasst die Aneignung des Namens oder der Gestalt des Klägers durch den Beklagten. Bemerkenswerterweise waren Klagen wegen Verletzungen der Privatsphäre vor 1960 relativ selten. Nachdem jedoch PROSSERS Artikel an Einfluss gewann, folgte eine Klagewelle[955]. Ein weiterer zentraler Beitrag veröffentlichte WESTIN, der die Privatheit auf zwei verschiedene Weisen auslegte. Die allgemeine Definition umfasste den Anspruch des Einzelnen, von Gruppen und Institutionen, autonom darüber bestimmen zu können, wann, wie und in welchem Umfang Informationen über sie verbreitet werden. Nebst dieser allgemeinen Umschreibung definierte er die Privatheit in Bezug auf das Verhältnis des Individuums zu seiner sozialen Partizipation mit der Möglichkeit des bewussten Rückzugs in die Einsamkeit oder in eine kleine Gruppe[956]. Darüber hinaus definierte WESTIN vier Funktionen der Privatheit in einer demokratischen Gesellschaft, in Form persönlicher Autonomie, emotionaler Entlastung, Selbstreflexion und begrenzter sowie geschützter Kommunikation[957]. SOLOVE kommt zum Schluss, dass sowohl PROSSERS als auch WESTINS Ansatz die verschiedenen Dimensionen der Privatheit nicht erfasse[958]. In Anbetracht dieser Vielschichtigkeit entwickelt er ein Bezugssystem, das zum Verständnis der vielseitigen Probleme der Privatheit und deren Ursachen beitragen soll[959].

Beim Datenschutz zeigen sich die konzeptionellen Grenzen noch deutlicher. So ist bereits der Kernbegriff der informationellen Selbstbestimmung in Bezug auf den implizierten Schutzumfang problematisch[960]. Im Resultat sind die konzeptionellen Grenzen

953 Vgl. LAUBER-RÖNSBERG, in: Götting/Schertz/Seitz, § 62 N 18.
954 LAUBER-RÖNSBERG, in: Götting/Schertz/Seitz, § 62 N 20.
955 BRIN, 73.
956 WESTIN, Privacy, 7.
957 WESTIN, Privacy, 31 f.
958 SOLOVE, Privacy, 482.
959 SOLOVE, Privacy, 560; siehe auch FINN/WRIGHT/FRIEDEWALD, 7 ff., die 7 Typen der Privatheit unterscheiden.
960 Siehe dazu vorne B.II.1.4 a).

aufgrund offener und gesellschaftlich geprägter Inhalte überaus weit und bedürfen insbesondere einer Konkretisierung durch die Gerichte.

2.2 Grenzen der Anwendbarkeit

a) Systematische Grenzen

Auf Verfassungsebene liegt ein wesentliches Problem in der praktischen Umsetzung von Grundrechten in ihrer möglichen Kollision untereinander sowie mit anderen Zielsetzungen der Verfassung. Die Erzielung eines Ausgleichs durch Abwägen der sich gegenüberstehenden Positionen ist primär Aufgabe der Gesetzgebung[961]. Wo beispielsweise dem Auskunftsrecht Geheimhaltungsinteressen von Drittpersonen gegenüberstehen, sind die Interessen der Geheimhaltung gegenüber jenen an der Einsicht abzuwägen[962]. Im Bereich der Grundrechte sind im Zusammenhang mit dem Persönlichkeits- und Datenschutz hauptsächlich die Meinungs- und Informationsfreiheit (Art. 16 BV), die Medienfreiheit (Art. 17 BV) und die Kunstfreiheit (Art. 21 BV) relevant. Weniger relevant erscheint der verfassungsrechtliche Grundsatz der Wirtschaftsfreiheit, deren individualrechtlicher Gehalt in Art. 27 BV festgelegt und in Art. 94 BV konkretisiert wird. Die Wirtschaft soll im Grundsatz nicht durch den Staat, sondern durch den Markt gesteuert werden. Der private Wettbewerb ist ein zentrales Koordinationsprinzip[963]. Einschränkungen in den Nutzungsmöglichkeiten von Personendaten sind wettbewerbstechnisch jedoch insofern nicht relevant, als dass sich alle Marktteilnehmer daran zu halten haben. Auch im Hinblick auf die programmatischen Bestimmungen in Art. 94 Abs. 2 und Abs. 3 BV ergibt sich kein Konfliktpotential[964]. Darüber hinaus kommt den ideellen Grundrechtsgehalten, wie sie insbesondere beim Persönlichkeitsschutz im Vordergrund stehen, gegenüber wirtschaftlichen Interessen, wie sie insbesondere von der Wirtschaftsfreiheit erfasst werden, ein gewisser Vorrang zu[965]. Auf der Gesetzesebene ergeben sich die rechtssystematischen Grenzen aus der Möglichkeit der Rechtfertigung einer Persönlichkeitsverletzung durch Gesetz[966].

---

961 MÜLLER, Grundrechtstheorie, 119.

962 RHINOW/SCHEFER, § 14 Rn. 1386; vgl. auch BGE 128 I 78.

963 UHLMANN, in: Biaggini/Gächter/Kiener, § 35 N 6.

964 Siehe dazu VALLENDER, Art. 94 N 10 ff.

965 RHINOW/SCHEFER, § 11 Rn. 1013; siehe zu entsprechenden Ansätzen in der Rechtsprechung BGE 126 I 140; BGE 96 I 592; siehe zur Vorrangstellung des Persönlichkeitsrechts gegenüber reinen Vermögensinteressen vorne B.II.1.3 e)(4).

966 Art. 28 Abs. 2 ZGB; Art. 13 Abs. 1 DSG.

b) Materielle Grenzen

Die Grenze der Anwendbarkeit des DSG verläuft im Individualbereich. Art. 2 Abs. 2 DSG enthält eine abschliessende Aufzählung von Einschränkungen des Geltungsbereiches des DSG[967]. Art. 2 Abs. 2 lit. a DSG nennt Bearbeitungen zum ausschliesslich persönlichen Gebrauch. Wenn eine natürliche Person Daten zu ihrem ausschliesslich persönlichen Gebrauch bearbeitet, kann das Datenschutzgesetz ohnehin kaum mehr Geltung beanspruchen[968]. Mit dem ausschliesslich persönlichen Gebrauch ist vor allem eine Verwendung der Informationen im engeren Privat- und Familienleben gemeint. Niemand soll beispielsweise verpflichtet werden, Einsicht in private Notizen zu gewähren. Gleichermassen sind Privatgespräche im Familien- und Freundeskreis, private Briefsammlungen etc. dem DSG entzogen. Auch Notizen, die jemand zwar bei der Ausübung seines Berufs, jedoch nur als Arbeitshilfe zum persönlichen Gebrauch macht, fallen nicht unter das Gesetz. Kommt es im Rahmen der Datenbearbeitung zum persönlichen Gebrauch dennoch zu Persönlichkeitsverletzungen – beispielsweise wenn ein persönlicher Brief liegen geblieben und Dritten zur Kenntnis gelangt ist –, steht dem Betroffenen die Geltendmachung der Rechtsbehelfe gemäss Art. 28 ZGB offen[969].

Im internationalen Verhältnis verläuft die Grenze der Wirksamkeit des materiellen Datenschutzrechts insofern etwas weiter, als dass die Übermittlung von Daten ins Ausland an bestimmte Voraussetzungen geknüpft sind. Die Voraussetzungen einer grenzüberschreitenden Bekanntgabe sind in Art. 6 DSG geregelt. Diese Bestimmung ist bei einer entsprechenden Übermittlung der Daten kumulativ zu beachten[970]. Auch Art. 25 der RL 95/46/EG sieht vor, dass personenbezogene Daten nur dann in ein Drittland übermittelt werden dürfen, wenn dort ein angemessener Schutz gewährleistet ist. Die Beurteilung erfolgt durch eine Angemessenheitsprüfung, wobei die ausländische Regelung nicht identisch, sondern im Hinblick auf die fundamentalen Schutzmassnahmen bloss gleichwertig sein muss[971]. Das Resultat ist eine weiche Normglobalisierung: Das Recht breitet sich global aus, jedoch nicht in einer bindenden Art[972]. In den USA haben bis jetzt zwei Regulierungen den Status einer adäquaten Lösung erhalten. Die erste ist das Safe Harbor Programm, das eine freiwillige Rahmenvereinbarung für amerikanische

967 ROSENTHAL, Handkommentar DSG, Art. 2 N 20.

968 So auch der Eigengebrauch gemäss Art. 19 URG.

969 BBl 1988 II 440.

970 ROSENTHAL, Handkommentar DSG, Art. 6 N 2.

971 Siehe Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, July 24, 1998, 5.

972 BIRNHACK, 42.

Unternehmen vorsieht, nach der diese erklären können, dass sie die europäischen Datenschutzregelungen einhalten. Die Kontrolle über die Einhaltung unterliegt dann der Federal Trade Commission (FTC). Die zweite Regulierung umfasst das Abkommen zur Übermittlung von Fluggastdaten von der EU an die USA im Rahmen der Terrorbekämpfung[973].

c) Prozessuale Grenzen

Eine Konsequenz der Nutzung globaler Informationsnetze besteht darin, dass Unternehmen Nutzerdaten ohne grosse Zeitverzögerung zwischen verschiedenen Rechtsordnungen verschieben können[974]. Insbesondere bei internetbezogenen Streitigkeiten ist damit regelmässig ein internationaler Sachverhalt gegeben, der die Prüfung der gerichtlichen Zuständigkeit und des anwendbaren Rechts im Einzelfall erfordert. Die Zuständigkeit entscheidet sich aus nationaler Sicht anhand des schweizerischen internationalen Privatrechts (IPRG) oder nach völkerrechtlichen Verträgen, insbesondere nach dem Lugano-Übereinkommens (LugÜ)[975]. Für Art. 29 DSG als öffentlich-rechtliche Bestimmung gilt das Territorialitätsprinzip[976].

Da die widerrechtliche Datenbearbeitung durch Private eine Persönlichkeitsverletzung begründet, steht dem Geschädigten gemäss Art. 139 IPRG eine Rechtswahl zu, die insbesondere das Recht seines gewöhnlichen Aufenthalts umfasst[977]. Dadurch sollte verhindert werden, dass sich der Datenbearbeiter durch die Wahl seines Domizils zu Lasten des Betroffenen datenschutzrechtliche Vorteile verschafft[978]. Im europäischen Raum relativieren sich die prozessrechtlichen Hürden zumindest teilweise durch die Angleichung der materiellen Rechtsgrundlagen und Rechtsprechung. Die EMRK bildet einen multilateralen völkerrechtlichen Vertrag zugunsten Dritter und begründet entsprechende Verpflichtungen unter den Vertragsstaaten. Die EMRK und die damit verbundene Rechtsprechung des EGMR wirken hierbei als Orientierungshilfe für die nationalstaatliche Rechtsanwendung[979]. Darüber hinaus hat der EuGH in seiner Rechtsprechung spezifische Grundrechte zum Schutz der Persönlichkeit als Teilgehalt des Schut-

973 *Passenger Name Record;* BIRNHACK, 42.

974 WHITE/MÉNDEZ MEDIAVILLA/SHAH, 53.

975 ROSENTHAL, Handkommentar DSG, Art. 15 N 66 ff.

976 Siehe ROSENTHAL, Handkommentar DSG, Art. 29 N 6 f.; BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, § 7 Rn. 59.

977 BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, § 7 Rn. 60.

978 BBl 1988 II 489.

979 SCHIEDERMAIR, 162 f., 349; SCHWEIZER, Grundsatzfragen, 67.

zes des Privatlebens gemäss Art. 8 EMRK entwickelt[980]. Dazu gehört insbesondere auch das Recht auf den Schutz personenbezogener Daten[981].

Eine Erweiterung der prozessualen Grenzen wurde im nationalen Recht angeregt. Die Anwendbarkeit der persönlichkeits- und datenschutzrechtlichen Normen könnte demnach durch die Stärkung des kollektiven Rechtsschutzes verbessert werden[982]. Für die Durchsetzung von Ansprüchen gegen eine oder wenige Gegenparteien, die auf einer vergleichbaren Rechts- und Tatsachenlage beruhen, soll der kollektive Rechtsschutz eine im Vergleich zum Individualrechtsschutz effizientere und effektivere Rechtsdurchsetzung gewährleisten[983].

2.3 Problematik der zeitlichen Normkomponente

a) Wirkungsgrad *ex ante*

Die Wirkung *ex ante* ist im Rahmen der Voraussetzung einer informierten Einwilligung sowohl im Persönlichkeits- als auch im Datenschutzrecht enthalten. Die Befunde über das menschliche Handeln zeigen jedoch, dass Warnhinweise selbst bei unmittelbar drohenden Gefahren jegliche Wirkung verlieren können, sofern sich das Bewusstsein bereits auf das Planen einer Handlung fokussiert hat[984]. Die Berücksichtigung weit in der Zukunft liegender Nachteile kann entsprechend umso weniger vorausgesetzt werden. In diesem Zusammenhang ist aber auch festzustellen, dass die Gefahr der Datenverarbeitung für den Betroffenen bisweilen zu hoch eingeschätzt wird[985]. Die Fokussierung auf mögliche Gefahren führt zu einem umfassenden und absoluten Anspruch an die informationelle Selbstbestimmung, die in diesem Grad sowohl der sozialen Interaktion im Allgemeinen als auch der Kommunikation im Besonderen zuwiderläuft[986]. Das sich Aufhalten und Verhalten führt im sozialen Umfeld immer zu einer gewissen Exposition und einer entsprechenden Wahrnehmung Dritter, die häufig nur einen kleinen Ausschnitt einer Persönlichkeit umfasst – sei dieser nun positiv oder ne-

980 SCHORKOPF, in: Ehlers, § 15 N 20.

981 SCHIEDERMAIR, 379 ff., 381; SCHORKOPF, in. Ehlers, § 15 N 39 ff.

982 Bericht des Bundesrates, Kollektiver Rechtsschutz, 6.

983 Bericht des Bundesrates, Kollektiver Rechtsschutz, 9.

984 Siehe dazu vorne C.I.2.2 a).

985 Siehe ZÖLLNER, 42; dahingehend auch ROSENTHAL, Datenschutz-Compliance, 177. SCHENK, 194, verweist darauf, dass die aktuelle Situation des Umbruchs insbesondere zu Unsicherheit und Übertreibung führe.

986 Siehe eingehend AEBI-MÜLLER, Rn. 609 f.

gativ – und auch in zeitlicher Hinsicht von weitgehender Dauer sein kann[987]. In diesem Zusammenhang erscheint eine gänzliche Kontrolle dieser kommunizierten Persönlichkeitsaspekte weder wünschenswert noch umsetzbar.

b) Wirkungsgrad *ex post*

Im Sachenrecht wird im Gegensatz zum Persönlichkeitsrecht durch die Dereliktion und den Untergang der Sache ein finaler Untergang der rechtlichen Ansprüche an dieser Sache begründet. Dereliktion ist die Besitzaufgabe an einer Sache in der erkennbaren Absicht der Preisgabe des Eigentums. *Res derelictae* werden zur herrenlosen Sache. Ein Untergang der Sache liegt vor, wenn sie zerstört oder verbraucht worden ist. Gleichzusetzen ist der Fall, in dem eine Sache der menschlichen Beherrschung so entzogen wird, dass keine Aussicht auf Wiedererlangung besteht[988]. Im Rahmen der informationellen Selbstbestimmung kann bewusst auf den Schutz personenbezogener Daten verzichtet werden, eine Dereliktion im sachenrechtlichen Sinn ist für Persönlichkeitsrechte aber nicht möglich[989]. Aus der bisweilen unüberschaubaren Verbreitung personenbezogener Daten kann im Einzelfall auch eine faktische Unmöglichkeit der Wiedererlangung der Kontrolle resultieren. Die persönlichkeitsrechtlichen Ansprüche bleiben aber ungeachtet dieser faktischen Unmöglichkeit bestehen.

Liegt klarerweise eine Persönlichkeitsverletzung vor, besteht das Problem nicht mehr darin, dass Daten aus datenschutzrechtlicher Sicht unrechtmässig bearbeitet werden, sondern in der Zuordnung der Verantwortlichkeit für die Persönlichkeitsverletzung und in der damit zusammenhängenden Wiedererlangung der Kontrolle über die Verbreitung. Fraglich ist hier, wie weit der Kreis der Verantwortung zu ziehen ist. Diese Frage ist letzlich rechtspolitischer Natur. Im Grundsatz definiert Art. 28 Abs. 1 ZGB einen umfassenden Verantwortlichkeitsbereich und verpflichtet potentiell *jeden*, der an der Verletzung mitwirkt. Entsprechend hat das Bundesgericht festgehalten, dass auch der Host-Provider, der als Anbieter eines Blogs die Technik zur Verfügung stellt und den Blog auf dem eigenen Server betreibt, für persönlichkeitsverletzende Blogbeiträge zi-

---

987 Siehe auch HAUSHEER/AEBI-MÜLLER, Rz. 12.131, wonach das gesellschaftliche Zusammenleben grundsätzlich und unweigerlich zu einem gewissen Einblick in das Privatleben Dritter führe. Diese Kenntnisnahme allein stelle indessen noch keine Persönlichkeitsverletzung dar. Eine Verletzung der informationellen Privatsphäre setze einen qualifizierten Eingriff voraus.

988 HAUSMANINGER/SELB, 165.

989 PEUKERT, 714.

vilrechtlich haftbar wird[990]. In einem früheren Urteil stellte das Bundesgericht fest, dass der in seiner Persönlichkeit Verletzte nicht zwingend gegen den hauptsächlich für die Verletzung Verantwortlichen – im konkreten Fall ein Presseunternehmen – vorgehen muss und stattdessen auch gegen einen nur sekundär Beteiligten – hier ein Kiosk – vorgehen kann[991]. Das Urteil des EuGH zum Recht auf Vergessen gegenüber Suchmaschinenbetreibern deckt sich mit dieser Argumentation[992].

c) Gesellschaftlicher Wandel als übergeordneter Zeitfaktor

Die Trennung zwischen Sozial- und Rechtsnormen ist insoweit unvermeidbar, als dass der Ende des 18. Jahrhunderts im Westen eingeführten Zweiteilung von Recht und Sitte gefolgt wird[993]. Aus der formalen Trennung der beiden Normgefüge resultiert indessen keine Isolation. Die sozialen Normen reflektieren sich im Recht und die Interpretation des Rechts erfolgt innerhalb der sozialen Kognition[994]. Ein Vergleich zwischen Europa und den USA zur Privatsphäre zeigt diese Wechselwirkung deutlich auf. In den USA lässt sich eine verhältnismässig geringe Sorge um den Schutz der Privatsphäre im Rahmen kommerzieller Transaktionen beobachten. In Bezug auf die Integrität des menschlichen Körpers im öffentlichen Raum gehen die soziale und die rechtliche Wertung dagegen über jene in Europa hinaus[995]. Für den Rechtsstaat ergibt sich daraus insbesondere die Folgerung, «dass die Gesellschaft kein abstrakt-soziales, sondern ein nach den Gesetzen der individuellen Verhaltens- und Einstellungsmuster entstandenes und sich weiterentwickelndes Kunstgebilde darstellt»[996]. Diese Entwicklung ist massgeblich durch eine ökonomisch motivierte Technologieentwicklung und eine entspre-

990 BGer vom 14. Januar 2013, 5A_792/2011. FRECH, 349, plädiert dafür dass, wer fremde Informationen nur bereithält bzw. durchleitet nicht haftbar wird, wenn sich diese als rechtswidrig erweisen. Schadenersatzansprüche sollten hierbei nur gegenüber dem ursprünglichen Verletzer und nicht gegenüber dem Provider geltend gemacht werden können. Auch Unterlassungsansprüche erforderten eine differenzierte Lösung. Host- und Access-Provider sollten nicht auf Unterlassung in Anspruch genommen werden können, da sie dieser Verpflichtung nur durch den Einsatz von Filtertechnologien Folge leisten könnten. Die entsprechende vorbeugende Überwachung ihrer Kunden durch die Betreiber erscheine unverhältnismässig; siehe dahingehend FRECH, 42 f., 349. Siehe zum abweichenden deutschen Recht HOLZNAGEL, 119.

991 BGer vom 12. September 2002, 5P.254/2002, E. 2.5; vgl. zu einem ähnlichen Sachverhalt im Internet BGer vom 28. Oktober 2003, 5P.308/2003, E. 2.4 f.

992 EuGH vom 13. Mai 2014, C-131/12, Nr. 85, 88; siehe dazu vorne B.II.2.4 c)(1).

993 SENN, 924.

994 Vgl. dazu MULLIGAN/KING, 1017. Ein einheitlicher Begriff der sozialen Normen besteht nicht. Ein mögliches Verständnis umfasst die normativen Erwartungen, «die von einer grösseren Bezugsgruppe geteilt und ausserrechtlich sanktioniert werden», HÄUSERMANN, 183 f., m.w.H.

995 ALLEN, 28, mit Hinweis auf die geringe Akzeptanz öffentlicher Nacktheit in den USA und den möglichen rechtlichen Folgen.

996 SEIDEL, Privatsphäre, 47.

chende gesellschaftliche Kognition geprägt[997]. Eine fehlende oder unzureichende Gesetzgebung ist unter anderem auch Resultat einer Macht- und Deutungshoheit über die Risiken umfassender Datenbearbeitungen durch Unternehmen, die um die Schaffung einer gesellschaftlich akzeptierten Normalität bemüht sind. Diese Normalität resultiert schliesslich in einem kollektiven Gedächtnis der Menschen, das diese Risiken insbesondere in Anbetracht der mit dem unternehmerischen Handeln verknüpften Vorteile als annehmbar erscheinen lässt[998]. Vieles von dem, was Verantwortungsträger in Unternehmen und im öffentlichen Sektor heute tun, wird die Gesellschaft in den kommenden Jahrzehnten begleiten[999].

Exemplarisch für den Wandel der gesellschaftlichen Kognition lässt sich die Rechtsprechung des Supreme Court im Bereich der Telekommunikation anführen. In *Olmstead v. United States* hielt der Supreme Court fest, dass niemand ein Recht auf Privatsphäre bei Telefongesprächen habe[1000]. Das Gericht argumentierte, dass die Privatsphäre bei der Kommunikation durch das Telefon bewusst aufgegeben werde, da die entsprechende Technologie inhärent ohne Sicherheit sei. Weiter hielt das Gericht fest, dass den Gesprächspartnern bewusst sei, dass die Signale ihre Wohnungen verlassen würden und nur die Naivsten vom Erhalt der Privatsphäre ausgehen würden. Die Argumentation kann heute auf internetbasierte Dienste übertragen werden[1001]. In *Katz v. United States* kam der Supreme Court dann jedoch zu einem anderen Ergebnis und stellte fest, dass eine begründete Erwartung auf Privatsphäre bei Telefongesprächen bestehe[1002]. In den Jahrzehnten zwischen *Olmstead v. United States* und *Katz v. United States* statuierte das Recht in Bezug auf den Zugang zu Telefongesprächen, dass aufgrund der Offenheit des Systems keine Privatsphäre zu erwarten sei. Obwohl es im Zeitraum zwischen den beiden Urteilen zu technischen Änderungen im Telefonsystem kam, änderte sich am logischen Argument in Bezug auf das Netz grundsätzlich nichts. Die Signale wurden noch immer ausserhalb der Wohnung übertragen und Telefone konnten auch 1967 einfach angezapft werden. Was sich jedoch geändert hatte, war die

997 Vgl. zur gesellschaftlichen Wahrnehmung von Überwachung und Technologie, KANG, 1285.
998 Siehe in Bezug auf die chemische Industrie JUNGKIND, 97.
999 CORTADA, Technology, 186.
1000 *Olmstead v. United States*, 277 U.S. 438 (1928).
1001 CAMP, 255.
1002 *Katz v. United States*, 389 U.S. 347 (1967).

soziale Kognition, die sich zumindest auf der gerichtlichen und legislativen Ebene widerspiegelt[1003].

Ob jene Generation, die mit neuen Medien aufwächst und heute vielfach freimütig persönliche Daten preisgibt, zu einer Generation heranwächst, die versiert mit den Möglichkeiten der Datenkontrolle umgeht und die entsprechenden Probleme auf diese Art lösen wird, ist ungewiss[1004]. Eine Thematisierung der mit der Nutzung verbundenen Möglichkeiten und Gefahren ist aber sicher angezeigt[1005].

2.4 Ausgestaltung im Nutzungs- und Vertragsverhältnis

a) Abgrenzung

Viele Dienstleistungen im Internetsektor werden unentgeltlich angeboten und es stellt sich die Frage, ob bei solchen Angeboten von einem Vertragsverhältnis auszugehen ist[1006]. Für die Beurteilung der Frage, ob ein Vertrag oder ein Gefälligkeitsverhältnis vorliegt, ist das Vorhandensein eines Rechtsbindungswillens massgelblich[1007]. Für die Annahme eines Rechtsbindungswillens können die Verwendung von Allgemeinen Geschäftsbedingungen seitens des Anbieters, das gewinnorientierte Handeln und ein wirtschaftliches Interesse im Hinblick auf den Erfolg der Tätigkeit angeführt werden[1008]. Gegen einen Rechtsbindungswillen spricht einerseits, dass die unentgeltlichen Angebote nicht durch die Nutzer, sondern durch Dritte finanziert werden[1009] und andererseits ein vorgängiges Rechtsverhältnis nicht besteht, die Bindung zwischen den Parteien mithin sehr lose ist[1010]. Übereinstimmend dazu wird insbesondere bei Suchmaschinen hinsichtlich der Richtigkeit oder Vollständigkeit der Verweise kein besonderes Vertrauen erweckt[1011]. Die herrschende Lehre geht hierbei entsprechend von einem Gefälligkeitsverhältnis aus[1012]. Von einem Vertragsverhältnis wird dagegen ausgegangen, sofern sich der Nutzer registriert, bestimmte Präferenzen und Kontakte offenlegt und

---

1003 CAMP, 256, führt in diesem Zusammenhang die Watergate-Affäre an. Diese ereignete sich jedoch erst in den Siebzigerjahren. Entscheidender dürfte der ebenfalls erwähnte zunehmend verbreitete Gebrauch von Telefonen im privaten Umfeld und nicht mehr nur in Unternehmen gewesen sein.

1004 EDWARDS/BROWN, 227; siehe in Bezug auf die gegenteilige aktuelle Situation LONDON ECONOMICS, 78.

1005 Siehe dahingehend GRIMMELMANN, 1203 ff.

1006 Vgl. in Bezug auf Suchmaschinen WEBER, Suchmaschinen, 125.

1007 Siehe WEBER, in: Vogt/Honsell/Wiegand, Art. 394 N 18.

1008 Siehe am Beispiel von Suchmaschinen EGGER, 1346 f.

1009 EGGER, 1346.

1010 WEBER, E-Commerce, 391.

1011 CICHON, Rn. 691.

1012 EGGER, 1347; CICHON, Rn. 691 f., mit Verweisen auf die deutsche Literatur und Rechtsprechung.

AGB akzeptiert[1013]. Weiter soll es für die Begründung eines Vertragsverhältnisses ausreichen, falls die AGB eine Klausel enthalten, wonach mit der Nutzung der Dienste die AGB als angenommen gelten und diese vom Nutzer zur Kenntnis genommen werden können. Fehlt eine solche Klausel, wird bei einer erhöhten Nutzerbindung (beispielsweise durch dauerhafte Einstellungen von Filtern oder Sprachtools) im Allgemeinen ebenfalls von einem beidseitigen Rechtsbindungswillen ausgegangen[1014].

b) Massgeblichkeit der Nutzungsbestimmungen

Ungeachtet der Frage, ob die Nutzungsbestimmungen nun Teil eines bestimmten vertraglichen Verhältnisses sind oder nicht, beanspruchen sie grundsätzlich Geltung und finden sich bald auf jeder Website[1015]. Problematisch an diesen Erklärungen sind teilweise die Länge und die fehlende Klarheit. Die Verständlichkeit wird durch den Umfang häufig negativ beeinflusst[1016].

Ein wesentlicher Zweck der Nutzungs- und Datenschutzbestimmungen liegt in der Information des Nutzers auf deren Basis er in die Datenbearbeitung einwilligt. Indessen stellt sich das Problem eines asymmetrischen Informationsverhältnisses bei diesen einseitigen Erklärungen mindestens im gleichen Umfang wie bei Vertragsabschlüssen. Langfristig wird jene Partei mit den besten Informationen den grössten ökonomischen Nutzen generieren können. Das Recht setzt dabei durch Offenlegungspflichten oder Verbote für die Nutzung von Informationen gewisse Schranken; im Datenschutzrecht in Form der Verhältnismässigkeit (Art. 4 Abs. 2 Satz 2 DSG), der Zweckbindung (Art. 4 Abs. 3 DSG) und des Auskunftsrechts (Art. 8 DSG). Auch Garantieerklärungen können zur Überbrückung von Informationsasymmetrien genutzt werden[1017]. In der Praxis werden den Nutzern jedoch kaum Haftungsansprüche und häufig keine umfassenden Kontrollmöglichkeiten in Bezug auf die personenbezogenen Daten eingeräumt[1018]. Gerade bei standardisierten Verträgen und allgemeinen Geschäftsbedingungen reflektiert sich die grössere Verhandlungsmacht in der Autonomie über die Gestaltung des Vertragsinhalts[1019]. In Anbetracht der fehlenden Notwendigkeit einer individualisierten

---

1013 EGGER, 1347.

1014 EGGER, 1347; a.M. und ohne Begründung HÜRLIMANN, 27.

1015 Siehe die Übersicht zu den sozialen Medien bei COHEN, 127 ff.

1016 DOWDING, 39, m.w.H. Die Datenschutzerklärung von Facebook beispielsweise ist von 1'004 Wörtern im Jahr 2005 auf 5'830 Wörter im Jahr 2010 angewachsen, GATES GUILBERT, Facebook Privacy: A Bewildering Tangle of Options, New York Times, May 21, 2010.

1017 Siehe COOTER/ULEN, 297 f.; in Bezug auf ein angemessenes Datenschutzniveau SCHMIDT-BENS, 59.

1018 SIMITIS, in: ders., § 4c N 48.

1019 Siehe KATSH, 115; EDWARDS/BROWN, 222.

Abstimmung der Nutzungsbedingungen erscheint die Verwendung standardisierter Bestimmungen als effizienteste und einfachste Form der Übereinkunft. Die technologische Entwicklung hat damit bisher zumindest im Verhältnis zwischen Anbietern und Nutzern nicht zu einem dynamischen Vertragsverhandlungsverhältnis geführt[1020].

Insbesondere in Bezug auf den Datenerhalt sehen einzelne Nutzungsbestimmungen indessen die individuelle Einflussnahme oder einen automatisierten Vorgang vor. Die Möglichkeit der Einflussnahme nach der Nutzung sowie die Variante eines vordefinierten Mechanismus lassen sich anhand von zwei Beispielen veranschaulichen. Am Beispiel der Plattform Tillate[1021] lässt sich die Ausgestaltung der Einflussnahme nach Veröffentlichung der Bilder aufzeigen: Die Plattform stellt die an ausgewählten Events gemachten Bilder ab dem folgenden Tag zur Ansicht ins Netz. Die Publikation beschränkt sich gemäss den AGB nicht auf die Website von Tilllate[1022]. Unter der Rubrik «Datenschutz» folgt die Erklärung: «Deine Bilder werden auf Tilllate.com veröffentlicht. Die schönsten Bilder können auch bei unseren Partnermedien oder auf Mobildiensten erscheinen». Bilder können vom zukünftigen Gebrauch mittels Löschbegehren per Telefon oder E-Mail jederzeit ausgenommen werden. Zudem besteht immer ein Einsichtsrecht und auch unabhängig von der Nutzung die Möglichkeit Bilder löschen zu lassen[1023]. Es ist davon auszugehen, dass durch diese Regelung auch die Datenweitergabe an Dritte erfasst wird. Eine vordefinierte Lösung über den Umgang mit Daten findet sich bei der Plattform Doodle, die die Terminsuche erleichtert. Die Datenschutzbestimmungen sehen einerseits vor, dass veraltete oder abgeschlossene Terminumfragen jederzeit manuell gelöscht werden können. Zudem wird darauf hingewiesen, dass die Daten auch in den Datenbanken von Doodle gelöscht werden. Andererseits – und hierin besteht der vordefinierte Mechanismus – sollen Umfragen von Zeit zu Zeit au-

1020 Siehe die Darlegungen einer solchen Entwicklung bei KATSH, 120 ff.; ferner SAMUELSON, 1172, mit dem Hinweis darauf, dass paradoxerweise gerade der virtuelle Raum solche konsensbasierten Lösungen vereinfachen würde.

1021 Tilllate ist ein auf Eventfotografie spezialisiertes Unternehmen, das 2001 gegründet wurde; siehe die Unternehmensinformationen unter: http://ch.tilllate.com/de/information/company/?ref=footer, abgerufen am 4.12.2013.

1022 Das Unternehmen Tilllate gehört heute zu hundert Prozent der Tamedia-Gruppe und ist dem Medienverbund 20-Minuten angeschlossen, das wiederum über 70 Titel umfasst; siehe dazu BÄHLER, 62.

1023 Siehe http://ch.tilllate.com/DE/about/privacy, abgerufen am 30.1.2013.

tomatisch, jedoch frühestens nach dreissig Tagen seit dem neusten Datum in einer Umfrage oder dreissig Tage nach dem letzten Zugriff, gelöscht werden[1024].

c) Exkurs: Ökonomische Analyse

(1) Vorbemerkungen

Für den Gesetzgeber stellt sich regelmässig die Frage nach den Auswirkungen von Gesetzen auf die Betroffenen. Die Wirtschaftswissenschaften bieten eine Verhaltenstheorie zur Bestimmung der durch die Gesetze hervorgerufenen Reaktionen. Diese sind im Hinblick auf den Erlass, die Revision, die Aufhebung und die Interpretation von Gesetzen relevant. Nebst Fragen der Effizienz zeigt die wirtschaftswissenschaftliche Perspektive auch auf, wer die Kosten einer Regulierung letztlich trägt[1025].

(2) Auswirkungen der Datenschutzregulierung

Während eine Eigentums- oder Lizenzanalogie im Rahmen der Kommerzialisierung von Persönlichkeitsrechten, wo der Nachfrager und die Informationsinhaber einen Vertrag aushandeln können, zur Lösung von Interessenkonflikten beitragen können, gibt es viele Situationen in denen derartige Vertragsverhältnisse überhaupt nicht oder nicht ohne grössere Hürden zu erreichen sind. Diese Situationen bedürfen einer allgemeinen Regulierung bzw. einer Schadenersatzordnung. Solche Regelungen sind der ökonomischen Analyse zugänglich[1026]. Die Ausgangslage der aktuellen Regulierung ist nicht überall dieselbe. Im US-amerikanischen Raum weist der Datenschutz im Vergleich zur Schweiz und zu Europa generell eine andere Form und Intensität auf. Die ökonomischen Effekte bleiben jedoch vergleichbar.

HUI und PNG argumentieren, dass Datenschutzregulierungen am besten geeignet sind, wenn viele Informationsanbieter vorhanden sind und diese sich um die Bearbeitung ihrer persönlichen Daten sorgen. Unter diesen Voraussetzungen sei die Regulierung effizient und führe zu einer Maximierung des allgemeinen Wohlstandes, da die Informationsanbieter die Kosten, die zum Verständnis der Datenschutzbestimmungen der einzelnen Datensammler aufgebracht werden müssten, vermeiden könnten[1027]. Für die Regulierung spricht auch eine verbesserte Durchsetzbarkeit und eine breite Anwend-

---

1024 Siehe die Rubrik «*Outdated and completed polls*», abrufbar unter: http://www.doodle.com/about/policy.html, abgerufen am: 18.5.2014. Sofern sämtliche Daten gelöscht werden, ist davon auszugehen, dass auch die auf Umfrageinhalten basierte Werbung nicht mehr auf die gelöschten Umfragen Bezug nimmt.

1025 COOTER/ULEN, 3.

1026 Siehe grundlegend WALDO/LIN/MILLETT, 74.

1027 HUI/PNG, 488; siehe zu den Kosten MCDONALD/CRANOR, 540 ff.

barkeit, die zu einer allgemeingültigen Anwendung führt[1028]. Und auch für den Datenbearbeiter kann eine allgemeingültige Regulierung vorteilhaft sein, da ein gesetzlich statuierter Schutz personenbezogener Daten zur Förderung des Vertrauens in die Datenbearbeitung beiträgt[1029]. Niemand hat die Zeit oder die Geduld, sich durch sperrige Bestimmungen zu lesen, die vielfältige und unklare Regeln über die Kontrolle der Daten enthalten[1030].

(3) Verhaltensökonomische Analyse

Die Mikroökonomie ging lange von der uneingeschränkten Annahme eines rationalen Verhaltens der Teilnehmer aus (*rational choice theory*). In den letzten dreissig Jahren kam dieses Konzept jedoch aufgrund empirischer Erkenntnisse zunehmend unter Druck[1031]. Im Jahr 2004 erschienen erste Publikationen über verhaltensökonomische Aspekte des Datenschutzes. Die Verhaltensökonomie versucht Erkenntnisse aus der Psychologie mit neoklassischen Theorien der Ökonomie zu verbinden. Dadurch sollen die ökonomischen Auswirkungen erklärt werden, die nicht dem kalkulierenden, nicht emotional handelnden, nutzenmaximierenden Verhalten des *homo oeconomicus* entsprechen[1032]. In verschiedenen Studien wurde eine grosse Diskrepanz zwischen der Wahrnehmung des Datenschutzes durch Individuen und ihrem tatsächlichen Verhalten festgestellt[1033]. Das tatsächliche Verhalten ist geprägt von mangelnder Selbstkontrolle und anderen Verzerrungen[1034]. Ohne eine entsprechende Nachfrage wird der Markt für Angebote zum Schutz der Privatsphäre jedoch klein bleiben und auch andere Mechanismen zur Selbstregulierung, die vom Verhalten der Konsumenten abhängen, werden unter diesen Vorzeichen keinen ausreichenden Schutz bieten können[1035]. Zudem weisen die psychologische und die verhaltensökonomische Forschung darauf hin, dass die meisten Individuen dazu neigen, Voreinstellungen zu akzeptieren, die in ihrem Namen gemacht und als vermeintliche Entscheidung wahrgenommen werden, anstatt diese zu ändern. Das gilt auch, wenn eine Änderung gegenüber der Voreinstellung vorteilhaft wäre[1036]. Im Gegensatz dazu gibt es jedoch auch Hinweise darauf, dass bei der Nut-

1028 WALDO/LIN/MILLETT, Fn. 29.
1029 Siehe BOSTON CONSULTING GROUP, 22.
1030 LESSIG, 160; SOLOVE, Person, 82; GRIMMELMANN, 1181.
1031 COOTER/ULEN, 50.
1032 WALDO/LIN/MILLETT, 75.
1033 Siehe dazu die Hinweise bei HUI/PNG, 489.
1034 WALDO/LIN/MILLETT, 76.
1035 WALDO/LIN/MILLETT, 76, m.H. auf ACQUISTI, Privacy, Economics, and Immediate Gratification: Why Protecting Privacy is easy, But Selling it Is Not, Presentation.
1036 SAMUELSON/ZECKHAUSER, 7 ff.; MADRIAN/SHEA, 1184 ff.

zung von Online-Angeboten jeweils die damit verbundenen Vor- und Nachteile durchaus nach objektiven Kriterien abgewogen werden[1037]. Für die Vertrauensbildung entscheidend sind hierbei nicht nur die einzelnen Datenschutzbestimmungen eines Anbieters, sondern auch seine Reputation[1038]. Diese Entscheidungsgrundlage wird durch die Übertragung von Personendaten an Dritte stark beeinträchtigt, da die Informationen im Nachgang für eine unbestimmt lange Zeit an eine unbestimmte Anzahl Dritter weitergeleitet werden können[1039]. Die Nutzer unterschätzen die mit der Offenlegung persönlicher Daten verbundenen Risiken und enthüllen entsprechend zu viele Daten. Entscheidend ist hierbei die schwache Verbindung zwischen Aktion (Offenlegung der Daten) und Konsequenz (belästigende E-Mail, Betrug, Diebstahl, Profilierung etc.)[1040].

d) Grenzen der Wirksamkeit

Der Beitrag von Nutzungs- und Vertragsverhältnissen zur Konfliktlösung ist in zweifacher Hinsicht zu relativieren: Einerseits reflektieren die Nutzungs- und Vertragsbestimmungen in der heutigen Form primär die Interessen der Anbieter und kaum die individuellen Nutzerpräferenzen[1041]. In Anbetracht der fehlenden Notwendigkeit einer Individualisierung erscheint die dahingehende Praxis der Unternehmen nachvollziehbar und sinnvoll. Zudem erstreckt sich der Konflikt aufgrund des Erhalts und der Weitergabe von Daten auch auf Verhältnisse ausserhalb der unmittelbaren Nutzungsverhältnisse. Obwohl das Vertragsrecht die Privatsphäre innerhalb der Beziehung der Vertragsparteien schützen kann, löst es die Probleme von Persönlichkeitsverletzungen im ausservertraglichen Verhältnis nicht[1042].

3. Schlussfolgerungen

Anders als zum Zeitpunkt der Ausarbeitung der OECD-Richtlinien vor 30 Jahren kann die Frage, wer Personendaten bearbeitet und wo sich diese befinden, heute kaum mehr beantwortet werden[1043]. Der traditionelle Ansatz im Datenschutzrecht geht von informationstechnologischen Strukturen aus, wo Regierungen und Grossunternehmen isoliert operierten und das Individuum gezielt in die Datenbearbeitung einwilligen sowie den genauen Zeitpunkt der Datenerfassung bestimmen konnte. Die Daten wurden dann für einen bestimmten, von der Zustimmung des Kunden erfassten Zweck verwendet

1037 METZGER, 156.
1038 METZGER, 169.
1039 WALDO/LIN/MILLETT, 76.
1040 LONDON ECONOMICS, 60 f.
1041 NISSENBAUM, Approach, 35.
1042 SOLOVE, Person, 81.
1043 WORLD ECONOMIC FORUM, Value, 3.

und später gelöscht. Die Datenbearbeitung erfolgte hier häufig in Bezug auf eine bestimmte Dienstleistung, ein bestimmtes Unternehmen oder einen einmaligen Zweck und ausserhalb hochgradig vernetzter Systeme[1044]. Bereits der beschränkte Speicherplatz und die begrenzte Rechenleistung erforderten eine deutlich stärkere Selektion und Zweckorientierung.

In Bezug auf die verhaltensökonomischen Aspekte misst SOLOVE dem Recht dort eine grosse Rolle zu, wo Dritte die Persönlichkeitsrechte von Betroffenen verletzen und weniger, wo der Einzelne bloss selbst persönliche Daten bekanntgibt[1045]. LANIER spricht den reinen Abwehransprüchen dagegen insgesamt die Wirksamkeit weitgehend ab und hält kommerzielle Rechte für zielführender[1046]. Die Notwendigkeit einer rechtlichen Durchsetzung würde hierbei nicht entfallen, jedoch durch die mit dem kommerziellen Ansatz verknüpfte Aussicht auf Kompensation seitens der Betroffenen einen verstärkten Anreiz zur Geltendmachung aufweisen[1047]. Die Nachweisbarkeit der Verletzung von Rechten würde durch die Registrierung von Dateneinheiten sichergestellt[1048]. Auch LESSIG geht von der Notwendigkeit eines rechtlichen Impulses aus und beschreibt eine eigentumsrechtliche Ausgestaltung, die vor jeder Beanspruchung der Privatsphäre eine Einigung bedingen würde[1049]. In Anbetracht der bewertungsbezogenen Probleme in Bezug auf einen eigentumsrechtlichen Ansatz müsste der rechtliche Impuls nach hier vertretener Ansicht insbesondere in der Schaffung einer transparenten Bewertungsgrundlage für die Nutzungsentschädigung bestehen. Die Notwendigkeit für dahingehende Anpassungen in der schweizerischen und in der europäischen Rechtsordnung wird durch den hohen materiellen Wirkungsgehalt des Persönlichkeitsrechts indessen in Frage gestellt.

Ungeachtet des Lösungspotentials rechtlicher Normkonzepte an sich, unterliegt das klassische Gerichtsverfahren als Mittel zur Streitbeilegung im Konfliktfall einer gewissen Schwerfälligkeit, die sich insbesondere in zeitlicher und örtlicher Hinsicht äus-

---

1044 WORLD ECONOMIC FORUM, Value, 11.

1045 SOLOVE, Reputation, 196.

1046 LANIER, 295, 303.

1047 LANIER, 301 ff.

1048 LANIER, 304, führt hierzu das Beispiel von Fotografien an und verweist zur Vermeidung von Fälschungen auf duplizierte Datensätze.

1049 LESSIG, 160.

sert[1050]. Das Problem liegt demnach mehr in der konkreten Ausgestaltung der Wahrnehmungsmöglichkeiten von Rechten und weniger in ihrem materiellen Gehalt[1051]. Ausserhalb gerichtlicher Konfliktlösungen verlangen Regulatoren, Datenschutzbehörden und Interessengruppen zunehmend nach Nachweisen, dass die bestehenden datenschutzrechtlichen Prinzipien tatsächlich umgesetzt werden und dass auch eine entsprechende Prüfung erfolgt (*Due Diligence*). Die wachsende Anzahl von Datenschutzverantwortlichen in Unternehmen verdeutlicht das Bestreben der Unternehmen diesen Anforderungen gerecht zu werden[1052].

III. Grenzen organisationsbasierter Konkretisierungen

1. Vorbemerkungen

Die organisationsbasierten Konkretisierungen orientieren sich in unterschiedlicher Stärke und auf verschiedene Weise an den normativen Vorgaben einzelstaatlicher und supranationaler Regulierungen. Bedeutende Mittel dieser Konkretisierung sind die Selbstregulierung in Form normativer Vorgaben sowie technische Lösungen, die der Einhaltung dieser Vorgaben dienen oder eigenständige Funktionen erfüllen.

2. Selbstregulierung

Die Selbstregulierung wird nach anfänglicher Kritik im Hinblick auf ihre demokratische Legitimation mittlerweile als Chance für einen Ausgleich einer ausschliesslich durch staatliche Regelungen definierten Ordnung betrachtet[1053]. Die Selbstregulierung lässt sich in eine reine Selbstregulierung und in eine staatlich gelenkte Selbstregulierung (auch regulierte Selbstregulierung) unterteilen. Die reine Selbstregulierung umfasst privatrechtliche Normierungen durch Verträge, Statuten oder Beschlüsse seitens

---

1050 Vgl. BUCHER, Persönlichkeitsschutz, Rn. 436: Die «Flexibilität in der Entwicklung des Rechts des Persönlichkeitsschutzes bringt andererseits eine gewisse Rechtsunsicherheit mit sich, insofern als es für ein neu auftretendes Problem oft noch keine in der Rechtsprechung enthaltene Lösung gibt. Die dem Gerichtsverfahren eigene Langsamkeit und Umständlichkeit lassen diesen Nachteil als noch schwerer erscheinen». Im Zusammenhang mit der Durchsetzung rechtlicher Ansprüche stellt sich mittel- bis langfristig wohl generell die Frage, ob die Gerichte als Institution mit der sich beschleunigenden Realität im Onlinebereich Schritt halten können (und müssen) und inwiefern die rechtlichen Prozesse – insbesondere für persönlichkeits- und datenschutzrechtliche Streitigkeiten – verstärkt online erfolgen könnten; siehe dazu EGGIMANN/HARASGAMA, 937 ff., 948-952. Das Tätigwerden staatlicher Gerichte an sich wäre auch in diesem Rahmen nicht ausgeschlossen, jedoch hier Teil eines institutionellen Wandels, der noch grösseren zeitlichen Dimensionen unterliegt.

1051 Indessen wird eine wirksamere Durchsetzung bisweilen auch durch schärfere Sanktionen erwartet, siehe u.a. BELSER, 17.

1052 CAVOUKIAN, 192.

1053 MÜLLER, Rechtssetzungslehre, Rn. 37; der Ausgleich kann insbesondere im Sinne einer Ergänzung verstanden werden, siehe dahingehend WEBER, Governance, 23.

privatrechtlicher Organisationen, wohingegen die gelenkte Selbstregulierung öffentlich-rechtlicher Natur ist[1054]. Im Datenschutz überwiegt bis jetzt eine wenig griffige Form der reinen Selbstregulierung. Viele multinationale Unternehmen haben zur Reduktion der datenschutzrechtlichen Risiken für sämtliche Unternehmen innerhalb der Gruppe globale Datenschutzbestimmungen eingeführt. Diese Unternehmen haben einen *top-down* Ansatz gewählt, anstatt den Datenschutz (*bottom-up*) auf der Basis einzelner Staaten umzusetzen. Durch diese globalen Datenschutzbestimmungen haben sie ihre eigenen auf den generellen Prinzipien der OECD und der Datenschutzrichtlinie beruhenden Schutzbestimmungen umgesetzt. In Anbetracht des administrativen Aufwands ignorieren zudem viele internationale Unternehmen die Datentransferregeln und verschieben ihre Daten innerhalb der Konzerngesellschaften weltweit[1055]. Zudem ist die vollumfängliche Einhaltung der einzelnen Datenschutzgesetze aufgrund der abweichenden und sich teils widersprechenden Inhalte praktisch unmöglich[1056]. Vor diesem Hintergrund ersuchten einzelne Unternehmen bei den Datenschutzbehörden um Anerkennung ihrer Bestimmungen als alternatives Instrument zur Einhaltung der Datenschutzprinzipien auf Ebene der Europäischen Union[1057].

Darüber hinaus bestehen branchenspezifische Ansätze, beispielsweise in der Online-Werbeindustrie[1058]. Die Digital Advertising Alliance hat im Jahr 2013 Prinzipien zur Selbstregulierung im Mobilbereich veröffentlicht[1059]. Diese widerspiegeln die allgemeinen Datenschutzprinzipien und gehen partiell auf Aspekte der Transparenz, der Zweckbindung und der Datensicherheit ein. Hintergrund dieser Initiative war die generelle Haltung der Marktteilnehmer, wonach eine Selbstregulierung gegenüber einer zentralen staatlichen Kontrolle zu bevorzugen ist. Darüber hinaus sollte die Angst der Nutzer bezüglich möglicher Verletzungen ihrer Privatsphäre nicht in Aktivismus umschlagen. Es liegt im Interesse der Unternehmen, den Bedenken der Nutzer Rechnung zu tragen, bevor sich diese aktiv gegen die Datenbearbeitung zur Wehr setzen[1060].

Die Selbstregulierung kann als Mittel zur Konkretisierung von gesetzlichen Zielen genutzt werden[1061]. Insbesondere im Datenschutz, der im Vergleich zu den klassischen

---

1054 MÜLLER, Rechtssetzungslehre, Rn. 38. f.

1055 Siehe zur Problematik der Implementierung, MCKEEN/SMITH, 79 f.

1056 MOEREL, 91 f.

1057 MOEREL, 99.

1058 TUTEN/SOLOMON, 73.

1059 Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment, July 2013.

1060 TUTEN/SOLOMON, 73.

1061 MÜLLER, Rechtssetzungslehre, Rn. 47.

Persönlichkeitsrechten eine Ergänzung darstellt, wären solche Konkretisierungen denkbar[1062]. Der Selbstregulierungsansatz der Digital Advertising Alliance beispielsweise weist einige Konkretisierungen auf, die sich explizit auf die Werbung im mobilen Umfeld beziehen. Entscheidende Schwächen des Selbstregulierungsansatzes liegen jedoch in der fehlenden Gewährleistung der Transparenz und der damit einhergehenden Rechtssicherheit sowie der Entstehung eines unübersichtlichen Regelwerks[1063]. Zudem ist die heutige Datenschutzgesetzgebung auch Resultat der Erkenntnis, dass der als ungenügend erachtete Rechtsschutz gerade nicht durch die Selbstregulierung entscheidend hatte verbessert werden können[1064].

3. Technische Lösungen

3.1 Schutzlösungen

Der Aufbau und die Eigenschaften digitaler Systeme lassen sich in zeitlicher Hinsicht in drei Ebenen unterteilen: Auf der ersten Ebene steht die Zeitlichkeit digitaler Systeme an sich. Ohne konstante Migration[1065] sind Datenformate und Datenträger innert verhältnismässig kurzer Zeit nicht mehr lesbar[1066]. Die Ursache liegt in der binären Codierung von digitalen Daten, die aus nur zwei Zuständen besteht[1067]. Die Entschlüsselung der binär codierten Information ist ohne technische Hilfsmittel und ohne Dekodier-Anleitung nicht möglich, die Daten sind dadurch an physische Datenträger gebunden und ihre Entzifferung ist von Rechenprogrammen abhängig[1068]. Entsprechend führt

---

1062 Ähnlich MÜLLER, Rechtssetzungslehre, Rn. 48, der explizit auf das Umweltrecht verweist.

1063 MÜLLER, Rechtssetzungslehre, Rn. 47; siehe auch die Aufzählung bei WEBER, Governance, 22 f., der im Weiteren insbesondere auf die fehlende Verbindlichkeit und das Problem der Durchsetzbarkeit verweist.

1064 Siehe dazu bereits AMMANN, 224 ff.; vgl. auch BBl 1988 II 419 mit Verweis auf die «Berufsethischen Normen» der Schweizerischen Institutsleiterkonferenz, dem Verband Schweizerischer Marktforscher, dem Verband für Wirtschaftsauskunfteien und der Schweizerischen Vereinigung für Direktwerbung; die «Neuen Grundsätze für Vertrauensärzte» und die «Grundsätze für Betriebsärzte» der Schweizerischen Ärztekammer; die Vereinbarung zwischen dem Arbeitgeberverband Schweizerischer Metallindustrieller und dem Schweizerischen Metall- und Uhrenarbeitnehmerverband; die Mustervereinbarung der Angestelltenkommission des Schweizerischen Gewerkschaftsbundes über «Neue Techniken und Datenschutz im Betrieb».

1065 Zum Begriff siehe SCHNEIDER, Amnesie, 134, wonach es sich bei der Migration nicht um eine einheitliche Methode, sondern um einen Oberbegriff für eine Vielzahl verschiedener Übergangstechniken handle; dahingehend auch BORGHOFF et al., 38; siehe zu den Techniken, ders., 37 ff., 59 ff., 137 ff.

1066 Vgl. BEGLINGER et al., 287.

1067 Der Binärcode besteht hierbei aus Nullen und Einsen; siehe zu den binären Datenformaten BORGHOFF et al., 12.

1068 DÄSSLER, 74; BORGHOFF et al., 5; ROSENZWEIG, 9, mit dem zusätzlichen Hinweis, dass die zur Interpretation notwendigen Trägermedien und die Software aufgrund technischer Innovation und kompetitiver Märkte ständig wechseln würden.

beispielsweise auch der Untergang eines Unternehmens nach einer gewissen Zeit zum Datenverlust, da die datenerhaltenden Massnahmen unterbrochen werden[1069]. Ohne entsprechende Schutzlösungen werden die Daten damit langfristig durch Unterlassen faktisch gelöscht[1070]. Dieses Problem stellt sich bei einer physischen Aufbewahrung grundsätzlich nicht; Akten können einfach gelesen und Mikrofilme notfalls mit Kerze und Lupe entziffert werden[1071].

Auf der zweiten Ebene kann ein System auf die Vermeidung der Datensammlung angelegt sein[1072]. Der dritten Ebene sind Systeme zuzuordnen, die Daten nach einer gewissen (vordefinierten) Zeit automatisch löschen[1073]. Sowohl die zweite als auch die Dritte Ebene können aus datenschutzrechtlicher Sicht der *Privacy by Design* zugeordnet werden[1074]. Nach diesem Grundsatz werden Probleme im Bereich des Datenschutzes umfassend bereits im Zeitpunkt der Entwicklung von neuen Technologien eruiert und geprüft, wodurch die lediglich nachträgliche Korrektur von Datenschutzproblemen vermieden werden soll[1075]. Die Mechanismen werden – häufig in Reaktion auf neue Bedrohungen – konstant weiterentwickelt[1076]. Der Europäische Datenschutzbeauftragte wies die Kommission 2010 in einer Stellungnahme darauf hin, dass die Umsetzung dieses Grundsatzes mindestens in zweifacher Weise in den Rechtsrahmen eingebettet werden müsse: Erstens durch die Aufnahme als allgemeinverbindlicher Grundsatz und zweitens durch Einbindung in spezifische Bereiche der Informations- und Telekommunikationstechnologie, die besondere Risiken für die Privatsphäre und den Datenschutz bergen und die sich durch eine Anpassung der technischen Gestaltung verringern las-

1069 Siehe zum Verlust durch äussere Einflüsse und zu den entsprechenden Gegenmassnahmen FRANKS, 216 ff.

1070 SCHNEIDER, Amnesie, 14.

1071 SCHENK, 204.

1072 Dazu kann bereits die Oberflächengestaltung beitragen, PAINE SCHOFIELD/JOINSON, 26; SOLOVE, Reputation, 200 f.; siehe zu möglichen Entwicklungstendenzen im Bereich von Nutzeroberflächen u.a. LANIER, 344; siehe zur Wirkung eines solchen Vorgehens auch die Anekdote bei ROSEN, Gaze, 198, wonach eine altmodische Apotheke in Georgetown mit dem Verkauf von Antidepressiva, Viagra und anderen intimen Medikamenten ein lukratives Geschäft mache, da es zur Unternehmenspolitik gehöre, alle Rezepte nur handschriftlich zu erfassen und keine Computerdateien anzulegen.

1073 Siehe dazu MAYER-SCHÖNBERGER, 169 ff.

1074 In diesem Zusammenhang ist die Feststellung relevant, dass sich die Technologie nicht selbst entwickelt, sondern der menschlichen Gestaltungsmacht unterliegt; siehe dazu LANIER, 311 f.

1075 BBl 2012 346, Fn. 11. Empirisch ist die Wirksamkeit dieses Ansatzes bis jetzt jedoch kaum nachgewiesen; siehe dazu RUBINSTEIN/GOOD, 1335.

1076 LONDON ECONOMICS, ix; siehe für einen möglichen Umsetzungsprozess im Unternehmen RUBINSTEIN/GOOD, 1353.

sen. Diesen Bereichen sind nach Ansicht des Datenschutzbeauftragten die Funkfrequenzkennzeichnung, soziale Netzwerke und Browser-Anwendungen zuzuordnen[1077].

Die Nutzung der Technologie zum Schutz der Privatsphäre ist indessen nicht neu und geht bereits in die Zeit der Entstehung der ersten Datenbanken in den Sechzigerjahren zurück[1078]. Zentral erscheint in diesem Zusammenhang auch die Möglichkeit der Verschlüsselung, die vor allem dort relevant ist, wo Daten an Dritte übertragen werden[1079]. Daten in einer Cloud beispielsweise können verschlüsselt gespeichert und übertragen werden. Eine komplett verschlüsselte Verarbeitung der Daten ist jedoch oft nicht möglich. Entsprechend würden die Daten zumindest während ihrer Verarbeitung in einem nicht verschlüsselten Zustand vorliegen[1080].

3.2 Transaktionslösungen

Ein entscheidender Vorteil vertraglich vereinbarter Datenschutzbestimmungen liegt in ihrer Flexibilität und der Möglichkeit unterschiedlichen Interessen Rechnung zu tragen[1081]. Die Verarbeitungskosten von Datenschutzerklärungen sind für die Nutzer jedoch, wie dargelegt, oft zu hoch[1082]. Zudem entsteht die Vereinbarung nicht durch Verhandlung, sondern durch die einseitige Annahme einer vorgefertigten Erklärung. In Anlehnung an die Überlegungen zur Kommerzialisierung personenbezogener Daten, könnten individuell abgestimmte Datenschutzpräferenzen – unabhängig von einem monetären Ausgleich – durch Verhandlung verwirklicht werden[1083]. Manuell ausgeführt generiert dieser Vorgang offensichtlich sowohl auf Seiten des Unternehmens als auch für die Nutzer einen übermässigen Mehraufwand. Der Verhandlungsprozess müsste entsprechend automatisiert erfolgen[1084]. Erforderlich wäre ein Verhandlungsprotokoll das zwischen den involvierten Computern ausgeführt wird. Der Nutzer definiert seine Präferenzen einmalig und sobald eine Internetseite aufgerufen wird, erfolgt ein Abgleich der Präferenzen, bis eine Einigung entsteht. Erst dann werden die Personendaten zugänglich[1085]. Dieser Mechanismus könnte durchaus auch eine Angebots-

---

1077 Europäischer Datenschutzbeauftragter, Stellungnahmen, ABl C 280/1, Nr. 6.

1078 LANGHEINRICH, 128.

1079 Siehe RUBINSTEIN/GOOD, 1355 f. Die Wirksamkeit von Verschlüsselungen wird durch die steigende Rechenleistung indessen langfristig immer wieder gefährdet und muss entsprechend auf dem neusten Stand gehalten werden.

1080 HANSEN, 90.

1081 SAMUELSON, 1172.

1082 Siehe vorne D.II.2.4 c)(2).

1083 Siehe insbesondere dahingehend auch NISSENBAUM, Preemption, 1385.

1084 LESSIG, 160.

1085 REAGLE/CRANOR 48. Die Idee wurde auch von SEARLS, Customer, o.S., aufgegriffen.

diskriminierung umfassen. Die Umsetzung einer solchen Lösung wäre innerhalb der bestehenden rechtlichen Rahmenbedingungen möglich, erscheint aber aufgrund mangelnder Anreize für die Unternehmen als unwahrscheinlich. Insbesondere dürfte die Bereitschaft zur Tragung möglicher Kosten für eine Implementierung notwendiger Systemanpassungen kaum gegeben sein. Andererseits sind das wachsende Angebot und die zunehmende Nutzung internetbasierter Dienste noch immer junge Erscheinungen und der grösste Teil der Entwicklung hat sich bis jetzt auf die Angebotsseite konzentriert[1086]. Die Kunden und Nutzer profitierten davon, ihre technische Autonomie gegenüber den Anbietern wurde jedoch nicht gestärkt[1087]. Das wachsende Bewusstsein auf der Nachfrageseite könnte daher langfristig auch ohne rechtliche Intervention zu einer Kehrtwende führen[1088]. Erste Lösungsansätze in diese Richtung sind in Form von Erweiterungspaketen zur Blockade von Werbung und *Do Not Track* Einstellungen bereits vorhanden[1089]. Im Weiteren bestehen Lösungsansätze im Rahmen alternativer Datenbearbeitungsmodelle, bei denen dem Nutzer die Kontrolle über seine Daten gänzlich übertragen wird[1090].

3.3 Grenzen technischer Lösungen

a) Technologische Entwicklung

Die Informationstechnologie dringt in immer mehr Lebensbereiche vor[1091]. Seit den Siebzigerjahren haben drei aufeinanderfolgende Veränderungen stattgefunden, die zu günstigen Prozessoren, günstigen Netzwerken und günstigen Sensoren geführt haben. Die dritte Entwicklung hat mit Hilfe der vorangehenden zwei zu neuen und beachtenswerten Auswirkungen auf die Privatsphäre geführt[1092]. Die vom Menschen hervorgebrachte und empfangene Information kann heute zumindest potentiell umfassend aufgezeichnet und festgehalten werden[1093]. Fortschritte in der Datensuche und Datenanalyse sowie die massive Zunahme der Rechenleistung und Speicherkapazität haben die Masse an verfügbaren Daten für Unternehmen, Regierungen und Individuen stark er-

---

1086 SEARLS, Economy, 44, 71 ff.; AMBROSE, 396.
1087 SEARLS, Economy, 153 ff.
1088 SEARLS, Economy, 249 f.
1089 SEARLS, Customer, o.S.; FAIRFIELD, 141 ff.
1090 TASIDOU/EFRAIMIDIS, 141 ff., m.w.H. zu anderen Projekten; siehe auch SEARLS, Economy, 194 ff.
1091 MATTERN, vernetzt, 2; BONDALLAZ, Rn. 85.
1092 ZITTRAIN, 205; siehe auch CORTADA, Corporation, 85.
1093 GLEICK, 396 f.; SIMITIS, Utopie, 524; SCHMID, 810.

weitert[1094]. Und auch die Filterung der vorhandenen Informationen erfolgt zunehmend durch entsprechende Algorithmen[1095]. Bei einem Algorithmus handelt es sich um eine spezifische Beschreibung, wie eine Aufgabe ausgeführt werden muss. Typischerweise enthält jeder Algorithmus eine Mischung von bestimmten durchzuführenden Operationen und Kontrollbefehlen[1096]. Die Berücksichtigung datenschutzrechtlicher Aspekte bei der Ausgestaltung solcher Programme hat sich in Abhängigkeit vom jeweiligen Rechts- und Kulturkreis anders entwickelt. So wurde der europäische Ruf nach der *Privacy by Design* beispielsweise bei der Entwicklung von *E-Discovery* Software bis anhin weitgehend ignoriert[1097]. Die Technologie definiert die Grenzen zur Lösung von informationellen Konflikten ohne eine gestaltende Einflussnahme des Rechts entsprechend durch ihre tatsächliche Entwicklung.

Das Beispiel der Anonymisierung zeigt, dass die technologische Entwicklung auch andere Schutzmassnahmen unterlaufen kann[1098]. Anonymisierend wirkt eine Verschlüsselung von Personendaten erst dann, wenn die Daten nicht mit einem Schlüssel oder auf andere Weise wieder lesbar gemacht werden können[1099]. Ähnlich wie bei der Pseudonymisierung kann durch Anwendung des korrekten Schlüssels der Personenbezug wieder hergestellt bzw. auf die Daten zugegriffen werden. Auch hier muss sichergestellt werden, dass nur befugte Personen Zugang zum Entschlüsselungscode haben und die Verschlüsselung möglichst nicht zu knacken ist[1100]. Obwohl insbesondere im Geschäftsverkehr viele Daten nach einigen Jahren an Risikopotential verlieren, gibt es Informationen, die auch nach langer Zeit noch zum Schaden eines Unternehmens verwendet werden können. Sofern diese in verschlüsselter Form bei Dritten aufgezeichnet worden sind, besteht die Gefahr, dass die einst sichere Verschlüsselung durch eine erhöhte Rechenleistung oder neue Analyseverfahren umgangen werden kann[1101].

b) Vernetzung

In den Zwanziger- und Dreissigerjahren des 20. Jahrhunderts entstanden in verschiedenen Laboratorien in den USA und Europa computerähnliche Technologien. Diese wurden in den Vierzigerjahren zu den heute bekannten digitalen Computern, wobei die

1094 CUKIER, 3 ff.
1095 FIDEL, 40.
1096 HOFSTADTER, 440; vgl. auch HOFFMANN, 147.
1097 ZEUNERT/ROSENTHAL, Rn. 78.
1098 Siehe in Bezug auf die Kombination von Daten vorne B.II.2.1 b).
1099 ROSENTHAL, Handkommentar DSG, Art. 4 N 39.
1100 ROSENTHAL, Handkommentar DSG, Art. 4 N 39.
1101 BRIN, 282 f.

kommerzielle Nutzung erst Mitte der Fünfzigerjahre begann. In den Sechziger- und Siebzigerjahren wurden Grossrechner und die Telekommunikation in integrierten Systemen zusammengeführt[1102]. Seit den Achtzigerjahren traten immer mehr Vernetzungsmöglichkeiten von unterschiedlichen und unabhängigen Computern auf. Von internationaler Tragweite war die Entstehung des Internets, zuerst unter Hochschulangehörigen[1103], ab 1993 mit der weiteren Verbreitung dann für alle[1104].

Da Informationen auf Computern gespeichert werden und das Internet definitionsgemäss aus der weltweiten Verbindung einer gewissen Anzahl dieser Computer besteht[1105], ist es schwieriger geworden Inhalte dem Zugang über das Internet zu entziehen. Durch E-Mails versendete Daten beispielsweise werden auf Servern gespeichert, deren geographische Lage den Nutzern häufig gänzlich unbekannt ist[1106]. Die potentiell erhältlichen Informationen beschränken sich dabei nicht auf die Reichweite der führenden Suchmaschinen. Die Datenbanken, die sich der oberflächlichen Suche entziehen, umfassen weitaus mehr Informationen als die einfach auffindbaren Datensätze[1107]. Obwohl keine genauen Angaben verfügbar sind, wird dieser verborgene Datenbestand auf ein Mehrfaches der direkt publizierten und den Suchmaschinen zugänglichen Inhalte geschätzt[1108]. Die grossen Suchmaschinenbetreiber sind sich dieser Einschränkung bewusst und versuchen dieses Problem zu lösen[1109].

Ein schwieriges Problem in der Informatik stellt ferner das Auffinden von Bildern aufgrund von Merkmalen abgebildeter Inhalte dar. Wird beispielsweise bei Google ein Name in der Bildersuche eingegeben, erscheinen jene Bilder, in deren Zusammenhang der Name im Text vorkommt. Die Suche im Netz erfolgt nicht anhand des Inhalts (*by content*), sondern nach dem Zusammenhang (*by context*)[1110]. Die inhaltsbasierte Bild-

---

1102 CORTADA, Technology, 167.

1103 Der wichtigste Dienst des Internets ist das World Wide Web. Der Grundstein dafür wurde 1989 am schweizerischen Kernforschungsinstitut (CERN) gelegt, wo man zur Förderung des Informationsaustausches zwischen Wissenschaftlern elektronische Dokumente miteinander verknüpfen wollte, MAASS et al., 4.

1104 ZEHNDER, 154; siehe zur Organisation des Internets GOLDSMITH/WU, 29 ff.

1105 WEBER, Governance, 5.

1106 SARVARY, 96; SCHAAR, 230.

1107 Die Reichweite von Suchmaschinen wird indessen laufend weiterentwickelt und Informationen, die vormals zum *Invisible Web* bzw. *Deep Web* gezählt worden sind, werden heute durch gebrauchsübliche Suchmaschinen gefunden und können nicht mehr dem *Invisible Web* zugeordnet werden, DEVINE/EGGER-SIDER, 3 f.

1108 Siehe die Übersicht zu der dahingehenden Literatur und die entsprechenden Schätzungen bei DEVINE/EGGER-SIDER, 15 f.

1109 MACLEOD, 35 ff.

1110 HILTY et al., 25; siehe zu damit einhergehenden Einschränkungen bei der Auffindbarkeit von Personen, MACLEOD, 130 ff.

suche wird laufend weiterentwickelt. Häufig wird dabei die Suche durch Beispiel verwendet. Das Verfahren beruht auf Ähnlichkeitsmassen für Gesichter. Eine grössere Menge an Beispielen verbessert die Trefferquote, jedoch führt ein grösserer Bildbestand gleichzeitig zu einer Verschlechterung der Trennschärfe. Die Zuordnungsquote nimmt daher mit einem grösseren Bildbestand ebenso zu, wie die Verwechslungsgefahr[1111]. Im Weiteren werden biometrische Lesegeräte vermehrt bei üblichen Endgeräten eingesetzt. Für Onlineanbieter wird es daher in Zukunft einfacher, eine eindeutige und unverfälschte Identifikation der Nutzer zu erhalten[1112]. Durch die zunehmende Vernetzung von Informationsressourcen steigt die Dichte an vorhandenen Personendaten an[1113]. Die Zugänglichkeit und mögliche Verwertung dieser Daten ist insbesondere im Hinblick auf Verstösse gegen das Datenschutzgesetz relevant[1114].

c) Konvergenz von Datenbeständen

(1) Ursachen

Die informationellen Vorgänge unterliegen einer zunehmenden Konvergenz[1115]. Der Begriff ist ursprünglich gesellschaftspolitischer Natur und umfasst das Zusammenlaufen verschiedener Bereiche auf der Basis von Prinzipien, die sich nach und nach als gemeinsam herausstellen[1116]. Im technologischen Bereich führte Ende des zwanzigsten Jahrhunderts bereits die Konvergenz zwischen der Informationstechnologie und der Telekommunikation zu Veränderungen in der Arbeits- und Freizeitgestaltung[1117]. Konvergenz bedeutet in diesem Zusammenhang, dass mehr als eine Technologie im gleichen Gerät verwendet wird. Ein Beispiel hierfür ist ein portabler Computer, der automatisch das Telefon bedient, um eine Internetverbindung herzustellen; darin vereinen sich die Informationstechnologie in Form von Computern und Prozessoren mit der Te-

---

1111 HILTY et al., 26; von diesem Verfahren zu unterscheiden ist die eigentliche Gesichtserkennung (*Face Recognition*), die der möglichst zuverlässigen Erkennung von Personen dient und mit biometrischen Authentifizierungsverfahren wie beispielsweise Fingerabdrücken oder Iriserkennung funktioniert. Diese Verfahren erreichen eine hohe Zuverlässigkeit und sind der menschlichen Gesichtserkennung überlegen.

1112 ZITTRAIN, 228.

1113 Siehe CHAOUCHI, 217 f., wonach die zunehmende Verwendung von Sensoren zur Automatisierung alltäglicher Lebensräume (*Internet of Things*) in Zukunft zu einer noch grösseren Ansammlung von Daten führen wird. Diese dürften insbesondere durch Kombination mit anderen Daten häufig auch Rückschlüsse auf bestimmte Personen zulassen. Durch die Kombination steigt ferner die Aussagekraft über die einzelne Person und damit die Datenqualität; siehe dazu SCHAAR, 190.

1114 ELIXMAN, 25.

1115 CORTADA, Corporation, 85 f.; SPÄCK JONES, 291.

1116 KUHLEN, 111.

1117 CORTADA, Flood, 585.

lekommunikation[1118]. Parallel dazu erfolgte eine Konvergenz der Wirtschaftssysteme mit welcher ein verstärktes Tätigwerden der Regierungen einherging, die um die Sicherung der nationalen Sicherheit, der Wohlfahrt und des Wirtschaftswachstums besorgt waren[1119].

Auf der Unternehmensebene erfolgt die Konvergenz vor dem Hintergrund einer erleichterten Übertragbarkeit von Daten. Einerseits wollen Unternehmen nicht leichtfertig auf Informationen verzichten, die Ihnen Wettbewerbsvorteile verschaffen könnten. Andererseits ist der Aufwand einer umfassenden Datensammlung für alle Fälle regelmässig zu gross bzw. für einzelne Unternehmen gar nicht möglich. Entsprechend muss eine optimale Informationsauswahl getroffen werden. Die Auswahl der relevanten Information richtet sich nach dem einzelnen Unternehmen[1120]. Sich daraus ergebende Unterschiede im Informationsbestand können im Rahmen der Vernetzung durch den Informationsfluss zwischen verschiedenen Unternehmen und Unternehmenseinheiten ausgeglichen werden[1121]. Dieser Ausgleich kann auf einer höheren Ebene auch über ganze Sektoren (zum Beispiel öffentlich und privat) hinweg stattfinden[1122], wodurch sich im Hinblick auf das Geflecht an informationsverarbeitenden Stellen eine Komplexitätssteigerung für den Betroffenen ergibt[1123]. Die Konvergenz stellt den nächsten Schritt dieser Entwicklung dar und umfasst den Zusammenschluss ganzer Systeme. Ein weiterer Faktor der Konvergenz liegt in diesem Zusammenhang in der Konzentration von Marktanteilen einzelner Unternehmen. Im Internetsektor beispielsweise verteilen sich die Marktanteile trotz der weitgehend offenen Strukturen des Netzes an sich auf einige wenige Grossunternehmen[1124]. Die Marktkonzentration kann hierbei zwar auch für den Nutzer problematisch sein, tatsächlich gebunden aufgrund von Netzwerkeffekten ist aber der Werbetreibende als Kunde dieser Dienste[1125].

(2) Vorgang

Die technologische Entwicklung fördert die Konvergenz zwischen Netzen, Endgeräten und Dienstleistungen. Durch die Digitalisierung können verschiedene Prozesse vermehrt in einheitlicher Form (beispielsweise dem *Internet Protocol*) übertragen wer-

1118 CORTADA, Technology, 168.
1119 CORTADA, Flood, 585.
1120 HOCH, in: Picot, 10 f.
1121 MÜLLER, Kontrolle, 142.
1122 Siehe dazu die Darstellung bei MÜLLER, Kontrolle, 143.
1123 Siehe in Bezug auf den öffentlichen Sektor MÜLLER, Kontrolle, 145.
1124 The Economist, Battle of the internet giants: Survival of the biggest, December 1, 2012.
1125 LANIER, 166; siehe zur Unterscheidung von Kunde und Nutzer vorne C.I.1.2 d).

den[1126]. Die Verbreitung schnellerer Anschlüsse und die Weiterentwicklung des *Internet Protocol* als umfassendes Netz für Kommunikationsdienste ermöglichen die Übertragung grosser Datenmengen in kurzer Zeit[1127]. Die technologischen Entwicklungen führen zu einer verbesserten Erfassung und Auswertung von on- und offline Vorgängen[1128]. Insbesondere das Konsumentenverhalten wird dadurch ein Teil der Wertschöpfungskette. Die fortschreitende Miniaturisierung verschiedener Technologien bietet zahlreiche neue Möglichkeiten und führt zu einer zunehmenden Durchdringung der Umwelt[1129]. Die dieser Entwicklung zugrundeliegenden Technologien befinden sich indessen teilweise noch in einem frühen Stadium[1130]. Der Blick auf den heutigen Stand der Technik sollte daher immer auch deren zukünftige Entwicklung und die damit einhergehende Verstärkung der Auswirkungen berücksichtigen. Obwohl Prognosen mit Vorsicht zu stellen sind, ist zu erwarten, dass der Trend zunehmender Datenquellen und deren Verknüpfung anhalten wird. Zentrale Felder dieser Konvergenz sind insbesondere die Nanotechnologie, die Medizin und die Neurowissenschaften[1131].

(3) Informationstheoretische Probleme aktueller Entwicklungen

Eine aktuelle Entwicklung lässt sich am Phänomen *Big Data* beobachten[1132]. Der Begriff umfasst Informationen, die nicht mit traditionellen Prozessen verarbeitet oder analysiert werden können[1133]. Daten waren immer Teil der informations- und telekommunikationstechnischen Entwicklung. Umfang und Tragweite von *Big Data* übersteigen jedoch das bisherige Mass und führen zu einem Wendepunkt, der sich durch die weitere Vernetzung und Konvergenz nicht nur von Informationen, sondern technologischer Entwicklungen an sich akzentuieren wird[1134]. Bei der Analyse von Daten ergibt sich hierbei im Zusammenhang mit der Zusammenführung der Datenquellen ein spezifi-

1126 WEBER, E-Commerce, 6.
1127 WEBER, E-Commerce, 6 f.
1128 Einschränkend HUVILA, 324, insbesondere in Bezug auf die Herstellung eines individuellen Kontexts von öffentlich zugänglichen Daten; kritisch in Bezug auf den mit der Datensammlung verbundenen Datenüberfluss, BRIN, 330.
1129 Siehe dazu beispielsweise NZZ Folio, Der Kunde, Mai 2013, Nr. 262, 20-64.
1130 CORTADA, Technology, 239 f.
1131 CORTADA, Technology, 241.
1132 Siehe zur Entstehungsgeschichte ZIKOPOULOS et al., 40 ff.
1133 ZIKOPOULOS et al., 3.
1134 MCKINSEY, 2.

sches informationstheoretisches Problem[1135]: In Bezug auf den *Inhalt* von Informationen macht eine Betrachtung des mittleren Informationsgehalts mehrerer Nachrichten bzw. Signale keinen Sinn. Eine solche Betrachtung macht nur dort Sinn, wo Aussagen über die durchschnittliche *Menge* an Information aus mehreren Nachrichten gemacht werden können. Der Inhalt einer Nachricht ist keine Grösse, die gemittelt werden kann. Gemittelt werden kann nur die Menge der Inhalte. Entscheidend ist aber die Information, die in bestimmten Nachrichten enthalten ist, da nur diese einen Inhalt aufweist[1136]. SAYRE beschrieb in diesem Zusammenhang einen grundsätzlichen Unterschied zwischen der Informationstheorie und der Semantik. Erstere befasst sich mit den Umständen der Kommunikation im Allgemeinen, wohingegen sich die Semantik mit dem Inhalt einer bestimmten Nachricht auseinandersetzt[1137]. *Big Data* basiert auf einem quantitativen Ansatz und zeigt Korrelationen, nicht Kausalitäten[1138]. Im Kern quantifiziert eine Korrelation die statistische Beziehung zwischen zwei Datenwerten[1139]. Die Korrelationen zeigen entsprechend nicht, weshalb etwas passiert, sie zeigen bloss, dass etwas passiert[1140]. *Big Data* ist aus informationstheoretischer Sicht entsprechend ein Phänomen, bei dem sich die Erkenntnis aus der Menge an Inhalten und nicht aus diesen selbst ergibt. Tritt nun ein bestimmtes Ereignis mit einem anderen bestimmten Ereignis auf, kann durch die Beobachtung des einen Ereignisses auf das andere geschlossen werden[1141]. Durch diese Analysen werden auch Aussagen über die Zukunft möglich[1142]. Bereits vor dieser Entwicklung ging STEINBUCH Ende der Sechzigerjahre davon aus, dass für die Beurteilung gegenwärtigen Verhaltens weniger die Vergangenheit relevant sein wird, sondern stärker die in der Zukunft liegenden, durch das Verhalten hervorgerufenen Konsequenzen[1143]. Daraus folgerte er die zukünftige Gesetzmässigkeit wonach

---

1135 Siehe zum Ganzen, DRETSKE, 47 f., der folgendes Beispiel anführt: X wird, während er in der Zeitung liest, dass seine Aktien gesunken sind, mitgeteilt, dass Y auf ihn wartet. X hat zwei Dinge erfahren: Seine Aktien sind gefallen und Y wartet auf ihn. Es gibt keinen Durchschnitt davon, was er erfahren hat. Hingegen kann allenfalls ein Durchschnitt der Menge an Informationen, die er erfahren hat gebildet werden.

1136 DRETSKE, 48.

1137 SAYRE, in: Philosophy and Cybernetics, 11.

1138 MAYER-SCHÖNBERGER/CUKIER, 2, 13 f., 19.

1139 MAYER-SCHÖNBERGER/CUKIER, 52.

1140 MAYER-SCHÖNBERGER/CUKIER, 14.

1141 Die Kausalität ist dagegen viel stärker mit der Erklärung verbunden. Die Bestimmung einer Ursache für ein Ereignis umfasst zumindest eine Teilerklärung desselben. Umgekehrt umfasst die Erklärung zumindest die Identifikation einer Teilursache, SAYRE, 69.

1142 MAYER-SCHÖNBERGER/CUKIER, 53.

1143 STEINBUCH, 243: «Das zukünftig zu erwartende Informiertsein über die Konsequenzen menschlichen Verhaltens ermöglicht es, spezielle Verhaltensmuster an deren Konsequenzen zu bewerten, nicht – wie es bisher üblich war – durch Vergleich mit der Tradition. Der kritische Blick orientiert sich dann weniger an der Vergangenheit, mehr an der Zukunft.»

Zukunft vor Vergangenheit gehen werde[1144]. Die Verflechtung der Daten sowie die fehlenden Kausalzusammenhänge sind jedoch entscheidende Gründe für die Einschränkung von Transparenz und Kontrolle[1145]. Jene Daten über einen Nutzer, die beispielsweise Facebook zum kommerziellen Gebrauch für Dritte zugänglich macht, würden für den aussenstehenden Betrachter meistens keinen Sinn ergeben[1146]. Die kommerziellen Korrelationen bleiben fast immer komplett verborgen und die Loslösung einzelner Aspekte ist kaum aussagekräftig[1147]. Problematisch erscheint dieser Umstand vor allem dann, wenn die Resultate entsprechender Auswertungen nicht mehr hinterfragt werden bzw. aufgrund der Intransparenz der Bearbeitungsvorgänge gar nicht mehr sinnvoll hinterfragt werden können.

3.4 Schlussfolgerungen

Grundsätzlich kann nicht abschliessend gesagt werden, welches Mittel zur Lösung von durch Datenbearbeitungen hervorgerufenen Konflikten am besten geeignet ist[1148]. Technologische Ansätze werden gesetzliche Vorgaben wohl kaum ersetzen[1149]. In Bezug auf die zahlreichen, aus dem Datenerhalt potentiell hervorgehenden Probleme, dürften Anpassungen an der Software gegenüber anderen Lösungen und insbesondere gegenüber konsensbasierten Vertrags- und Nutzungsbestimmungen jedoch deutlich effektiver sein[1150]. Daten, die nicht gesammelt, gespeichert oder veröffentlicht werden, sind Daten, die nicht geschützt, verwaltet und verantwortet werden müssen. Auf Daten, die gar nicht erst existieren, kann auch nicht zugegriffen werden, sie können nicht verändert, kopiert und verteilt werden oder verloren gehen[1151]. Das dem Datenschutzrecht entstammende Prinzip der Datenminimierung, kann durch die Gestaltung von Systemen grundsätzlich gezielt umgesetzt werden[1152]. In der Praxis hat sich die datenschutzfreundliche Gestaltung der Technik indessen bis anhin nicht etablieren können[1153]. Die

---

1144 STEINBUCH, 243.

1145 Siehe dazu vorne C.I.5.2, 5.3.

1146 Demnach stellen sie für diesen keine Informationen dar; siehe dazu vorne A.I.1.1.

1147 LANIER, 105 f.

1148 LESSIG, 85 ff.

1149 SIMITIS, Utopie, 524; NISSENBAUM, Preemption, 1386.

1150 EDWARDS/BROWN, 223.

1151 CAVOUKIAN, 181. Und sie können nicht für irgendwelche anderen, zu einem späteren Zeitpunkt nützlich erscheinenden Zwecke (legitim oder nicht) benützt werden; siehe dazu das Beispiel bei SCHAAR, 219, wonach in Deutschland bei der Autobahnmaut auf ein System verzichtet wurde, das die zurückgelegten Strecken nicht registriert und stattdessen versucht wird die Verwertung der nun vorhandenen Daten durch gesetzliche Schranken einzugrenzen.

1152 Siehe dazu RUBINSTEIN/GOOD, 1377, 1397 f., 1406.

1153 BAERISWYL, 19.

hohen Kosten und die Akzeptanz der gegebenen Verhältnisse seitens der Nutzer sind bei Grossunternehmen die häufigsten Gründe für die eingeschränkte Nutzung dieser Technologien. Bei Klein- und Mittelunternehmen besteht der wichtigste Faktor darin, dass sie die Anwendung dieser Technologien für ihre Geschäftstätigkeit als nicht relevant erachten[1154]. Die technologische Innovation bedingt eine entsprechende soziale Innovation, die insbesondere durch das Recht wahrgenommen werden muss[1155]. Genauso wie die Technologie aber nicht die gesellschaftlichen und rechtlichen Gegebenheiten ausblenden soll, soll das Recht die Technologie nicht auf der Basis eines isolierten Schutzgedankens und ungeachtet weiterer zentraler Faktoren zu steuern suchen. So besteht beispielsweise der Zweck sozialer Netzwerke gerade darin, dass sich die Nutzer grundsätzlich ohne technische Hürden austauschen können[1156]. Eine Regulierung oder softwarebasierte Einstellungen, die dem sozialen Kontext und den menschlichen Bedürfnissen nicht Rechnung tragen, sind hier nicht zielführend[1157].

IV. Interpretation der Grenzen

Auf Basis der Analyse über die Grenzen zeitbezogener Normen und organisationsbasierter Konkretisierungen lassen sich die in Teil C. dargestellten Konflikte in zwei für die weitere Betrachtung massgebende Aspekte unterteilen. Die explizit zeitbezogenen Normen weisen, wie dargelegt, einen indirekten Konfliktbezug auf, indem sie die Informationsgrundlage für mögliche künftige Konflikte schaffen. Dieser Vorgang umfasst allenfalls praktische Probleme im *Records Management* und ist nicht weiter zu vertiefen. Hinsichtlich der explizit zeitbezogenen Normen relevant erscheint hingegen die Tatsache, dass die Pflicht zum Erhalt von Daten mit der Erfüllung der Aufbewahrungsfrist endet. Daraus ergibt sich das folgend als *Konflikt im weiteren Sinn* zu behandelnde Problem, wonach Daten, die möglicherweise auch nach der Erfüllung der expliziten Aufbewahrungsfrist noch relevant sein könnten (beispielsweise für die historisch-wissenschaftliche Forschung), gegebenenfalls verloren gehen.

Die implizit zeitbezogenen Normen weisen einen direkten Konfliktbezug auf, indem sie Lösungen für sich unmittelbar widersprechende Interessen im Hinblick auf die Bearbeitung von Daten vorsehen. Dieser Konflikt ist weiter als *Konflikt im engeren Sinn* zu behandeln. Der zeitliche Aspekt dieses Konflikts bezieht sich auf das Interesse der

---

1154 LONDON ECONOMICS, 144.

1155 BURKERT, PET, 140; MULLIGAN/KING, 1033, verweisen in diesem Zusammenhang auf die notwendige Veränderung der rechtlichen Perspektive selbst, die zu stark auf eine datenschutzrechtliche Kontrolle über Daten und zu wenig auf den Schutz der Privatsphäre ausgerichtet sei.

1156 GRIMMELMANN, 1186 f.

1157 GRIMMELMANN, 1185 ff., 1206; NISSENBAUM, Integrity, 155.

Betroffenen an einer Löschung ihrer persönlichen Daten bzw. an der Unterlassung einer weiteren Bearbeitung und dem Interesse der Datenbearbeiter, die aufgrund eines aktuellen oder potentiellen Nutzens an der weiteren Bearbeitung der Daten interessiert sind. Im Rahmen des geltenden materiellen Rechts lassen sich dahingehende Konflikte weitgehend lösen. Bereits das allgemeine Persönlichkeitsrecht weist einen hohen Schutzumfang auf. Durch das DSG wird dieser noch erweitert[1158]. Die Grenze der entsprechenden implizit zeitbezogenen Normen ist daher insbesondere in der fehlenden Konkretisierung zu sehen.

Darüber hinaus ist festzustellen, dass die Abwehrrechte unabhängig von ihrem materiellen Gehalt im Konfliktfall immer erst *ex post* wirken. Eine effektiv vorgängig wirksame Einschränkung des Konfliktpotentials in Bezug auf die Verwertung von Daten müsste daher auf Ebene der Löschung erfolgen.

[1158] Vgl. dazu AMBROSE, 388.

E. Mehrdimensionaler Lösungsansatz

I. Ansatz

Das einleitend formulierte Ziel der Arbeit besteht in der Ausarbeitung von Vorschlägen für die Integration zeitbezogener Aspekte in bestehende oder zusätzliche Normen, die den Umgang mit (personenbezogenen) Daten durch Unternehmen regeln. Die bisherigen Ausführungen haben gezeigt, dass sich die bestehenden Normen grundsätzlich in explizit und implizit zeitbezogene Normen unterteilen lassen. Beide Normtypen unterliegen im Hinblick auf die Lösung von Konflikten gewissen Grenzen, anhand denen sich der Konflikt in einen im weiteren Sinn und einen im engeren Sinn unterteilen lässt. Innerhalb beider Normtypen bestehen nebst der zeitlichen auch eine qualitative und eine quantitative Dimension. Vor diesem Hintergrund verfolgt der mehrdimensionale Ansatz zwei Ziele: In einem ersten Schritt sollen die Dimensionen Zeit, Quantität und Qualität für beide Normtypen anhand ihrer wesentlichen Inhalte dargestellt werden[1159]. In einem zweiten Schritt soll der mehrdimensionale Ansatz dann anhand der zwei genannten Konfliktsituationen konkretisiert werden. Die jeweilige Konkretisierung erfolgt sowohl innerhalb der bestehenden Normen als auch in Bezug auf neue Normen.

Insbesondere das digitale Umfeld ist äusserst dynamisch und Regulierungen, die zu einer bestimmten Zeit als notwendig erscheinen, können innert kürzester Zeit obsolet werden[1160]. Die Geschichte der Technikregulierung ist geprägt von zeitlich und inhaltlich überholten Gesetzen[1161]. Vor diesem Hintergrund orientiert sich der mehrdimensionale Ansatz an der tatsächlichen Bearbeitung der Daten[1162]. Die Technikneutralität des Datenschutzrechts ist insofern beizubehalten, als dass das Recht nicht jede Innovation sogleich aufnehmen soll[1163]. Dies nicht zuletzt deshalb, da sich neue Probleme häufig sachgerecht mittels bestehender Instrumente lösen lassen und neue Rechtsnormen nicht nur neue Lösungen, sondern auch neue Probleme schaffen können[1164]. Ande-

---

1159 Die drei Dimensionen spiegeln sich auch bei *Big Data* in Form der Grössen *volume, variety* und *velocity* wider, siehe dazu ZIKOPOULOS et al., 5 ff.

1160 GASSER/THURMAN, 52; RODRIGUES, 247; LIEDTKE, 5 f.; SOLOVE, Reputation, 205; siehe zum Problem der Überforderung der Rechtssetzung grundlegend MÜLLER, Rechtssetzungslehre, Rn. 35; diesem Umstand wird im Technologierecht und anderen Rechtsgebieten zunehmend mit sog. «*sunsetlaws*» begegnet, die vom Gesetzgeber mit einem Ablaufdatum versehen werden und zu einem bestimmten Zeitpunkt ausser Kraft treten und/oder einem Evaluationsprozess unterzogen werden, BURKERT, Aufgaben, 165.

1161 FISHER, 83 ff.

1162 Siehe den Verweis auf die Wesentlichkeit dieser Orientierung bei SIMITIS, Utopie, 526.

1163 BURKERT, Approach, 80; siehe das Argument einer weitgehend technikneutralen Ausgestaltung bei BELSER, 17.

1164 In Bezug auf die zivilrechtliche Haftung von Internet-Providern FRECH, 344.

rerseits muss das Recht seine Umwelt und die damit verbundenen Konflikte reflektieren, um anerkannt zu werden[1165]. Eine wichtige Orientierung in der Frage nach der Ausgestaltung von Rechtsnormen bietet insbesondere eine umfassende Sichtweise auf den Normzweck. Gerade im Bereich des Datenschutzes besteht die Rolle des Rechts auch in der Schaffung eines Vertrauenssystems, das durch die Generalisierung und Stabilisierung der Erwartungen in einem unsicheren Umfeld die Interaktion fördert sowie einen Ausgleich der erwarteten Risiken und Möglichkeiten schafft[1166]. Das Regelungsziel der Schaffung einer Vertrauensgrundlage, auf deren Basis Informationen fliessen können, ist in Anbetracht der Bedeutung des Regelungsgegenstandes für Wirtschaft und Gesellschaft zentral und schafft eine über den Schutzgedanken hinausreichende Perspektive[1167]. Diese zeigt nebst den Gefahren einer fehlgeleiteten Datenbearbeitung ein deutliches Potential für eine erweiterte Nutzung von Daten durch technologische Fort- und Neuentwicklungen.

II. Dimensionen

1. Zeitliche Dimension

Die zeitliche Dimension ist systematisch in die Betrachtung der qualitativen und quantitativen Dimension eingebunden. Sie ist entsprechend als immanenter Bestandteil der nachfolgend dargestellten Dimensionen zu betrachten und nicht als eigenständige Grösse. Einer zeitlichen Betrachtung zugänglich sind nur gegenständlich definierte Grössen – hier qualitativ und quantitativ, auf die sich die Zeit beziehen kann. Dies ergibt sich bereits aus der nachstehend beizubehaltenden Unterteilung in explizit und implizit zeitbezogene Normen, die stets qualitativ und quantitativ definierbare Informationsgrössen zum Gegenstand haben. Der Zusammenhang zeigt sich auch bei der Beschaffung von Informationen. Die datenschutzrechtliche Bestimmbarkeit einer Person hängt von der Quantität und Qualität der vorhandenen Daten ab, die wiederum durch den finanziellen und zeitlichen Aufwand zu ihrer Beschaffung bestimmt werden[1168].

1165 BURKERT, Approach, 80.

1166 BURKERT, Approach, 78. Zentral erscheint in diesem Zusammenhang vor allem auch die Schaffung von Transparenz; siehe dazu ROSENTHAL, Datenschutz-Compliance, 164 ff.

1167 Die Interessen am Individualschutz (Persönlichkeitsschutz) und am Systemschutz (Wirtschaft) stehen sich damit nicht nur entgegen; vgl. PETER, Datenschutzgesetz, 25.

1168 Siehe PROBST, 1425.

2. Qualitative Dimension

2.1 Eingrenzung

Noch in den Neunzigerjahren fehlte ein Massstab für die Beurteilung der Qualität von Informationen weitgehend. Im Vordergrund standen rein quantitative Grössen und damit Aspekte der Informationsverarbeitungskapazitäten sowie die Möglichkeiten der Informationstechnologie[1169]. Generell ist die Informationsqualität abhängig vom jeweiligen Kontext und kann unterschiedliche Bedeutungen haben[1170]. Weiter ist sie abhängig von der jeweiligen Perspektive, wobei die Bewertung aus der Sicht des Senders, des Übermittlers, des Empfängers oder einer Drittperson erfolgen kann[1171]. In einem sozialpolitischen Kontext stehen insbesondere die Objektivität, Verständlichkeit, Relevanz und die Transparenz im Vordergrund[1172]. In einem rechtlichen Kontext erscheinen dagegen richterliche Beurteilungskriterien wie die Richtigkeit, Vollständigkeit, Verlässlichkeit, Klarheit, Kohärenz, Nützlichkeit und Verständlichkeit als zentral[1173]. Ein besonderes Bewusstsein für die Qualität von Informationen zeigt sich auch bei den Archivwissenschaften, deren konstantes Ziel die Vermittlung von zuverlässiger Information aus eindeutig erkennbaren Quellen ist[1174]. Für Unternehmen ist die Datenqualität in den letzten Jahren zunehmend wichtiger geworden, da diese Informationen vermehrt zentralisieren und für verschiedene Steuerungs- und Überwachungsfunktionen nutzen[1175]. In Unternehmen wird sich ein Bezugssystem für die Datenqualität hauptsächlich an den gesetzlichen Anforderungen ausrichten, da das Bezugssystem hier in einer Struktur entsteht, die selbst substantiell durch das Recht geprägt worden ist[1176]. Anhand der explizit und der implizit zeitbezogenen Normen lassen sich einige relevante Qualitätsaspekte aufzeigen.

1169 HOCH, in: Picot, 9.

1170 TRUDEL, 96.

1171 GASSER, Variationen, 735 f.

1172 WEBER, Quality, 168.

1173 WEBER, Schutz, 43 f.; GASSER, Variationen, 743 f.

1174 KELLERHALS, in: Coutaz et al., 354. SCHENK, 208, geht davon aus, dass diese Funktion von Archiven aufgrund der Veränderbarkeit und Kombinierbarkeit digitaler Datenbestände in Zukunft noch wichtiger wird.

1175 Nach MCKEEN/SMITH, 220, ist Datenqualität ohne Datenmanagement möglich, Datenmanagement ohne Datenqualität dagegen nicht.

1176 WEBER, Quality, 169.

2.2 Explizit zeitbezogene Normen

a) Eindeutigkeit der Information

Sämtliche explizit zeitbezogenen Normen weisen eine eindeutige und relativ enge Kategorisierung der aufzubewahrenden Daten auf. Im Rahmen der Revision des Rechnungswesens wurde im Handelsrecht der Gegenstand der zehnjährigen Aufbewahrungsfrist zusätzlich konkretisiert. Danach muss die Geschäftskorrespondenz unter Vorbehalt spezialrechtlicher Bestimmungen nur noch aufbewahrt werden, wenn sie die Funktion eines Buchungsbelegs hat[1177]. Zugleich wird mit der Aufbewahrungspflicht ein eindeutiger Zweck verfolgt, der wiederum zur Bestimmung der relevanten Daten herangezogen werden kann.

b) Echtheit und Unveränderbarkeit der Information

Für herkömmliche Dokumente haben sich in Form von optischen Erkennungsmerkmalen oder physikalischen Dokumenteneigenschaften verschiedene Verfahren zur Sicherung der Integrität[1178], Authentizität[1179], und Verbindlichkeit[1180] herausgebildet. Aus rechtlicher Perspektive sind hierbei an elektronische Dokumente mindestens ebenso hohe Anforderungen zu stellen wie an herkömmliche Dokumente[1181]. Im Vordergrund steht dabei im Grunde genommen nicht die Speicherung von Dokumenten, sondern deren Wiedergabe. Diese muss in qualitativer Hinsicht in einer Form gewährleistet sein, die die Beweisqualität des Dokuments nicht in Frage stellt[1182]. Bei digitalen Dokumenten wird die Integrität und der Nachweis der Urheberschaft heute durch digitale Signaturen sichergestellt[1183]. Die Voraussetzungen gehen indessen nicht soweit, dass archivierte Objekte auf ewig in der ursprünglichen Form aufbewahrt werden müssen. Bei einer langen Aufbewahrungsdauer ist damit zu rechnen, dass Übertragungen (Migrati-

---

1177 Siehe Der Bundesrat, Medienmitteilungen, Neues Rechnungslegungsrecht tritt am 1. Januar 2013 in Kraft, 22.11.2012.

1178 Siehe die Definition bei KEITEL/SCHOGER, 57, wonach eine Repräsentation integer ist, «die weder durch einen technischen Defekt noch durch böswillige Eingriffe manipuliert wurde und der weder Daten hinzugefügt noch entzogen wurden.»; BEGLINGER et al., 252 f. definieren die Unveränderbarkeit eines Dokuments dahingehend, dass ein in einer definierten Form archiviertes Dokument nicht mehr verändert werden kann, ohne dass dies am Dokument selbst feststellbar ist.

1179 Siehe die Definition bei KEITEL/SCHOGER, 59, wonach ein «Informationsobjekt inhaltlich genau das ist, was es zu sein vorgibt». Massgeblich für die Authentizität ist der Erhalt der kennzeichnenden Eigenschaften; vgl. zu den entsprechenden Metadaten PURI et al., 391.

1180 Die Verbindlichkeit ergibt sich aus der Integrität und Authentizität eines Dokuments.

1181 OPPLIGER, Rn. 11 f.

1182 BEGLINGER et al., 180.

1183 BEGLINGER et al., 178 f.; SCHNEIDER, Amnesie, 48.

onen) und Veränderungen (Transformationen) stattfinden[1184], die Definition eindeutiger Integritätsanforderungen muss daher von der Speicherung über die Aufbewahrung bis zur Wiedergabe gewährleistet sein[1185].

Bedeutend sind die Erfordernisse der Authentizität und Integrität einerseits, wo der Verkehrsschutz eine zentrale Rolle spielt – so beispielsweise im Wertpapierrecht[1186]. Andererseits sind die Echtheit und Unveränderbarkeit bei beweisrelevanten Dokumenten unabdingbar. Im Zivilverfahren wird in Art. 168 lit. b. ZPO die Urkunde als zulässiges Beweismittel genannt. Dabei gelten nach Art. 177 ZPO auch «elektronische Dateien und dergleichen» als Urkunden. Aus dem Recht auf Beweis folgt, dass digitalisierte Dokumente gleichermassen zum Beweis zuzulassen sind[1187]. Die Echtheit der Urkunde ist von jener Partei zu beweisen, die sich auf sie beruft, sofern die andere Partei die Echtheit bestreitet. Eine pauschale oder vorsorgliche Bestreitung reicht nicht aus, es müssen konkrete Umstände genannt werden, die das Gericht ernsthaft an der Echtheit zweifeln lassen[1188]. Im Mehrwertsteuerrecht sind die Voraussetzungen für die Beweiskraft elektronischer Dokumente in Art. 3 der Verordnung des Eidgenössischen Finanzdepartements über elektronische Daten und Informationen (EIDI-V) geregelt[1189]. Die Integrität und der Zugang zu den relevanten Daten werden durch die Anforderungen an die Datensicherheit, die Überprüfbarkeit, die Wiedergabe und Verfügbarkeit sowie zum Einbezug Dritter und zur Aufbewahrung sichergestellt (Art. 4-10 EIDI-V). Die Gewährleistung der Integrität erfolgt in der EIDI-V gemäss Art. 3 Abs. 1 lit. a EIDI-V durch das Erfordernis einer elektronischen Signatur[1190].

Im Weitern spielt die Authentizität in der Archivierung historisch bedeutsamer Dokumente eine entscheidende Rolle[1191]. Sofern die Authentizität nicht als wesentliches Merkmal gilt, können Überlieferungen leicht für bestimmte Zwecke der Erinnerungs-

---

1184 KEITEL/SCHOGER, 2, weisen auf die Gefahr der Korrumpierung und Manipulation von Daten bei diesen Vorgängen hin; ähnlich SCHNEIDER, Amnesie, 134; ferner BORGHOFF et al., 56. Siehe auch die philosophische Perspektive bei RECK, 74: «Es gibt in den digitalen Archiven keine Referenz auf das Original mehr, keinen ontologischen Unterschied zwischen dem Authentischen und den Fälschungen, dem Ursprünglichen und den Replikationen: alles wird zum Original, auch Irreführung, Fälschung, Zitat, ob man das will oder nicht.»; MOSER/NEBIKER/OTHENIN-GIRARD, 67, verweisen ebenfalls darauf, dass es im elektronischen Archiv keine Originaldokumente im traditionellen Sinn mehr gebe; ähnlich SCHENK, 205 f.

1185 BEGLINGER et al., 179 f.; KEITEL/SCHOGER, 57.

1186 SCHWEIZER/BAUMANN, 247.

1187 BEGLINGER et al., 173.

1188 BEGLINGER et al., 174; siehe auch GASSER/HÄUSERMANN, 305 ff.

1189 WEBER/WILLI, 209.

1190 WEBER/WILLI, 209.

1191 SCHWEIZER/BAUMANN, 239; OPPLIGER, Rn. 23.

kultur instrumentalisiert werden[1192]. Mit der Authentizität der Objekte eng verknüpft ist die Vertrauenswürdigkeit der handelnden Institution[1193]. Seit der digitalen Revolution[1194] stellt sich die Frage der Vertrauenswürdigkeit nebst den klassischen Gedächtnisinstitutionen wie Archive, Bibliotheken oder Museen auch für Unternehmen, Verbände und zahlreiche andere Einrichtungen[1195]. Digitale Daten können im Gegensatz zu analogen Objekten vom Datenträger getrennt werden und Manipulationen am Inhalt sind nicht mehr am Zustand des Mediums an sich erkennbar. Die Authentizität der archivierten Aufzeichnungen ist dadurch in Gefahr und mit ihr die Vertrauenswürdigkeit der verwaltenden Institution[1196]. Die Bewahrung authentischer Aufzeichnungen als Ziel historischer Archive wäre nicht realisierbar, wenn der zeitliche Fortbestand unzähliger Informationsteile mit ständigen Änderungen kombiniert würde. Die Stabilität elektronischer Daten ist jedoch problematisch[1197]. Die Qualität und der Nutzen des Erhalts werden damit in Frage gestellt. Die archivarische Tätigkeit der Sicherung originaler, authentischer Dokumente und der zugehörigen Informationen über Kontexte hat im digitalen Umfeld entsprechend eine mindestens ebenso wichtige Funktion, wie bei herkömmlichen Dokumenten[1198].

c) Richtigkeit und Wesentlichkeit der Information

Wo die Richtigkeit der zu erhaltenden Informationen für die Erfüllung des Aufbewahrungszwecks relevant ist, macht das Recht konkrete Vorgaben. So schreibt beispielsweise Art. 957a Abs. 2 lit. a OR die vollständige, wahrheitsgetreue und systematische Erfassung der Geschäftsvorfälle und Sachverhalte vor.

Bei der Archivierung, stellt sich grundsätzlich die Frage, ob diese dynamisch oder statisch erfolgen soll. Die Dokumentation des Vergangenen kann neuen Erkenntnissen angepasst und aktualisiert werden. Dieser Ansatz umfasst insbesondere die Präzisie-

1192 SCHENK, 82.
1193 KEITEL/SCHOGER, 20.
1194 Siehe vorne A.I.2.1.
1195 KEITEL/SCHOGER, 1.
1196 KEITEL/SCHOGER, 2 ff., mit Verweis und Kommentierung der Norm DIN 31644, die die Vertrauenswürdigkeit der digitalen Langzeitarchivierung anhand eines vollständigen Kriterienkatalogs objektiv bestimmbar und überprüfbar machen soll. Die Norm basiert auf einer seit über zwanzig Jahren international geführten Fachdiskussion zur digitalen Langzeitarchivierung.
1197 SCHENK, 203.
1198 SCHENK, 203.

rung, die Nachschreibung und gegebenenfalls auch die Korrektur[1199]. Umgekehrt fragt sich, inwiefern die Archivierung selbst Teil der Gegenwart sein soll. Heute wird befürwortet, dass Archivare bereits im Vorfeld des Endarchivs tätig werden und in Bezug auf das *Records Management* eine beratende Rolle einnehmen oder sogar selbst aktiv mitwirken[1200]. Die Beurteilung der Richtigkeit und der Wesentlichkeit der Information erfolgt so fortlaufend und ergibt sich nicht mehr aus dem (historischen) Bestand eines Dokuments an sich. Trotz berechtigter Kritik an diesem Vorgehen besteht bei digitalen Dokumenten das Problem, dass ihre Erhaltung aktiv betrieben werden muss. Die Frage nach dem Wert des Aufhebens stellt sich damit praktisch bereits kurz nach der Erstellung eines Dokuments[1201]. Und auch die Frage der Richtigkeit sowie allfälliger Aktualisierungen, die im Gegensatz zu physischen Dokumenten bei digitalen Datenbeständen wesentlich einfacher realisiert werden können, stellt sich in verhältnismässig kurzen Zeitabständen immer wieder von Neuem.

In der spärlichen Bundesgerichtspraxis zu Archivdaten findet sich insbesondere der Hinweis auf die Richtigkeit vorhandener Informationen[1202]. Der Entscheid vom 2.5.2001 setzte sich mit Versicherungsakten auseinander, die keiner breiten Öffentlichkeit zugänglich waren[1203]. Darin stellte das Bundesgericht fest, dass die Gesamtheit der Informationen die tatsächlichen Umstände richtig wiedergeben, obwohl einzelne In-

1199 So GLAUS, Vergessen, 192, der die Nachschreibung befürwortet; siehe zur korrigierenden Anmerkung im Archiv auch die Rechtsprechung des EGMR vom 10. März 2009, Nr. 3002/03 und 23676/03, die im Entscheid vom 16. Juli 2013, Nr. 33846/07 bestätigt wurde und wonach bei (potentiell) diffamierendem Material ein entsprechender Hinweis auf die (mögliche) Unwahrheit normalerweise genügt.

1200 Kritisch dazu SCHENK, 201, der auf den Quellenwert der Unabsichtlichkeit und die Eigenschaft der Dokumente «Überrest» zu sein verweist; grundlegend dazu FRANZ, 2: «Was die Archive von Bibliotheken, Museen und anderen Dokumentationsinstituten abhebt, ist nicht die gelegentlich etwas grobschlächtig angewandte Scheidung nach handschriftlichen, gedruckten und materiellen Dokumenten, eher schon der besondere funktionale Zusammenhang des organisch erwachsenen Archivguts, das nur zu einem kleinen Teil von vornherein als dauerndes Zeugnis rechtlicher Vorgänge angelegt wurde. Die Masse des Archivguts entsteht bei Behörden, Einrichtungen oder Einzelpersonen in Erfüllung verwaltungsmässiger, rechtlicher, geschäftlicher oder sonstiger Aufgaben, um dann erst später [...] zur Quellengrundlage für historische und andere Forschungen zu werden.»; ähnlich MOSER/NEBIKER/OTHENIN-GIRARD, 67: «Archivdokumente unterscheiden sich von Dokumentations- oder Bibliotheksgut: Sie entstehen unmittelbar aus einem Handlungskontext heraus, sie sind in der Regel nicht publiziert und haben oft Beweis- oder Nachweischarakter.»; siehe ferner RECK, 84: «Archivalien sind also nicht mehr adressiert auf Vergangenheit, sondern sind eingebunden in eine Logistik, deren Koordinaten quer zu der Differenz von Gegenwart / Vergangenheit verlaufen.».

1201 BORGHOFF et al., 140.

1202 GLAUS, Nachführungspflicht, 199.

1203 BGer vom 2.5.2001, 1A.6/2001; siehe dazu bereits vorne B.II.2.4 b).

formationen offensichtlich falsch sind[1204]. Weiter geht das Bundesgericht im entsprechenden Fall davon aus, dass auch bei «Momentaufnahmen», die sich nachträglich als falsch herausstellen, keine Nachführungspflicht besteht. MAURER-LAMBROU geht dagegen nur dann nicht von einer Pflicht zur Nachführung aus, wenn Momentaufnahmen zum Zeitpunkt in der Vergangenheit richtig waren und sich auch unter Berücksichtigung neuerer Erkenntnisse bezogen auf diesen zurückliegenden Zeitpunkt als richtig herausstellen[1205]. Im Resultat seien Datensammlungen daher grundsätzlich nachzuführen[1206]. Ein Recht auf nachträgliche Berichtigung kann auch gegeben sein, wenn die nur einen Ausschnitt wiedergebenden Daten für einen anderen Zweck oder in einem anderen Kontext verwertet werden[1207]. Im öffentlichen Recht ist die Vernichtung oder Berichtigung von Archivdaten grundsätzlich ausgeschlossen[1208]. Nach Art. 15 Abs. 3 BGA können die betroffenen Personen keine Berichtigung oder Vernichtung von Daten verlangen, sondern lediglich den strittigen oder unrichtigen Charakter vermerken lassen. Grundsätzlich falsch sind Daten, die an sich und unabhängig von ihrem jeweiligen Kontext unrichtig sind (zum Beispiel falsche Schreibweise von Namen oder falsche Geburtsdaten)[1209]. Ebenfalls als falsch können richtige Personendaten erachtet werden, die in Verbindung mit anderen Daten zu einem falschen Gesamtbild führen[1210]. Entsprechend sind der Zweck und die Art der Bearbeitung von Personendaten entscheidende Kriterien, die für jede Bearbeitung stets berücksichtigt werden müssen[1211].

2.3 Implizit zeitbezogene Normen

a) Anknüpfungspunkt

Das DSG knüpft mit Ausnahme einer differenzierten, indessen schwach ausgeprägten, Behandlung von Persönlichkeitsprofilen ausschliesslich an das Kriterium des Perso-

---

1204 BGer vom 2.5.2001, 1A.6/2001, E. 2c.; ablehnend MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 6, der darauf verweist, dass eine Berichtigung falscher Einzeltatsachen immer möglich sein müsse.

1205 MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 7.

1206 BBl II 450; MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 8.

1207 So in Bezug auf Medienarchive GLAUS, Nachführungspflicht, 199 f.; siehe auch EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 46; MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 6; vgl. zudem die ausführliche Regelung in Art. 35 Abs. 6 BDSG.

1208 Siehe dazu bereits RUDIN, 256.

1209 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 47; MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 6.

1210 MALLMANN, in: Simitis, § 20 N 13.

1211 MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 6, mit dem Hinweis auf die relative Richtigkeit von Personendaten.

nenbezugs an[1212]. In den USA bestehen dagegen zahlreiche legislative Einzelakte, die in Reaktion auf bestimmte Probleme erlassen wurden[1213]. Ein anschauliches Beispiel liefert der *Video Privacy Act* von 1988. Als Robert H. Bork für den Supreme Court nominiert wurde, gelangten einige Journalisten 1987 an die Daten seiner Videoausleihen, was zum *Video Privacy Act* führte. Dieser verbietet den Verleihern, Daten über das Konsumverhalten ihrer Kunden offenzulegen[1214]. Das Gesetz beinhaltet insbesondere auch eine zeitliche Vorgabe zur Vernichtung der Daten[1215]. Der *Fair Credit Reporting Act* gewährleistet den individuellen Zugang zu den Aufzeichnungen und beschränkt die Offenlegung von Kreditdaten[1216]. Der *Telephone Consumer Protection Act* reguliert die Kundenanwerbung per Telefon und der *Driver's Privacy Protection Act* beschränkt die Freigabe von Daten aus dem Fahrzeugregister. Der *Children's Online Privacy Protection Act* enthält Regeln für den Umgang mit persönlichen Daten von Kindern unter 13 Jahren. Im Zusammenhang mit Krankenversicherungen ist der *Health Insurance Portability and Accountability Act* relevant. Dieser wurde im Jahr 2009 um den *Health Information Technology for Economic and Clinical Health Act* erweitert, der insbesondere eine Informationspflicht für Datenschutzverstösse sowie erhöhte Strafen von bis zu USD 50'000 für jeden Verstoss und bis zu USD 1.5 Millionen pro Kalenderjahr vorsieht[1217]. Insgesamt lässt sich die Gesetzeslage anhand dieser nicht abschliessenden Liste relevanter Gesetze dahingehend zusammenfassen, dass eine vielgestaltige Mischung von Einzelinteressen abgedeckt wird und sich die jeweiligen Gesetze auf bestimmte Datenkategorien beziehen. Die Gesamtheit der Bundesgesetze gleicht einem Puzzle in dem die einzelnen Teile nicht zusammenpassen[1218].

b) Richtigkeit der Information

(1) Zeitbezug

Die der japanischen Sprache inhärenten Eigenschaften offenbaren eine einzigartige Perspektive auf Zeit und Raum. In der japanischen Kultur wird Zeit als ein kontinuier-

---

1212 Siehe dazu vorne B.II.2.1 b).

1213 Vgl. die Übersicht bei BONDALLAZ, Rn. 749 ff.

1214 ROSEN, Gaze, 167; LANE, 224 f.

1215 Teil (e) des *Video Privacy Protection Act* von1988 hält fest: «*A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or persuant to a court order*.», *codified in* 18 USC § 2710. Ein vergleichbarer Schutz für Bücher oder Zeitschriften oder auch für medizinische Daten gibt es nicht, BRIN, 73.

1216 Siehe dazu vorne B.II.2.2 a).

1217 FRANKS, 231.

1218 ALDERMAN/KENNEDY, 154.

licher Fluss einer stets aktualisierten Gegenwart betrachtet. Der Westen hat dagegen eine sequentielle Perspektive auf die Zeit. Gegenwart und Zukunft werden dabei aus einer historischen Retrospektive gebildet[1219]. Ausgangspunkt und Kontext der Erinnerung ist die Gegenwart, in der das Erinnern stattfindet und die den Zweck des Erinnerns definiert. Die Handlung in einer gegenwärtigen Situation erfordert das Verstehen der Gegenwart im Lichte der Vergangenheit und im Hinblick auf die sich in der Zukunft ergebenden Folgen dieses Handelns[1220]. Indessen unterliegt auch die sequentielle westliche Perspektive in Bezug auf ihre gegenwärtige Betrachtung einem kontinuierlichen Fluss[1221]. Die Geschichte bildet faktisch auch hier eine aktualisierte Gegenwart (Repräsentation, Rekonstruktion), die die Vergangenheit bisweilen nur noch bruchstückhaft abzuzeichnen vermag[1222].

(2) Rechtliche Wertung

Das Bundesgericht unterstellt die Ehre und das Recht auf Wahrheit dem Persönlichkeitsschutz nur unvollkommen. Von einer Verletzung wird nur dann ausgegangen, wenn die Äusserung den Betroffenen in einem falschen Licht darstellt[1223]. Darüber hinaus räumt das Datenschutzrecht jenen, über die unrichtige Daten bearbeitet werden, in Art. 5 Abs. 2 DSG einen Anspruch auf Berichtigung ein[1224]. Der Berichtigungsanspruch ist eng mit der Datenqualität verknüpft. Der Datenbearbeiter muss sich über die Richtigkeit der Daten vergewissern und diese korrigieren oder löschen, sofern sie hinsichtlich des Zwecks ihrer Bearbeitung falsch oder unvollständig sind[1225]. Entsprechend kann aus Art. 5 Abs. 2 DSG nicht in jedem Fall ein Löschungsanspruch abgelei-

---

1219 Die Japaner sehen auch den Raum frei von einer fixen Perspektive, daher kommt bei japanischen Gemälden dem Zeichnen von Schatten keine zentrale Bedeutung zu, NONAKA/TAKEUCHI, 28.

1220 KUUTTI/BANNON, 34 f.

1221 Siehe dazu RECK, 78: «Das Gedächtnis ist immer aktuell, Geschichte immer eine Repräsentation der Vergangenheit, die eine problematische und unvollständige Rekonstruktion dessen ist, was nicht mehr existiert.».

1222 Siehe exemplarisch und im Kontext dazu den Fall Stacy Snyder, wo ein unvorteilhaftes Bild der Betroffenen zum Abbruch ihrer Karriere als Lehrerin geführt haben soll, vgl. statt vieler MAYER-SCHÖNBERGER, 1 f.; ROSEN, Forgetting, o.S. Aus der entsprechenden gerichtlichen Beurteilung *Stacey Snyder v. Millersville University,* No. 07-1660, December 3, 2008*,* geht dagegen hervor, dass einerseits die Leistungsanforderungen durch die Betroffene nicht erfüllt wurden und es bereits im Vorfeld zum Konflikt mit der Praktikumsbetreuerin kam, mithin das Bild nur ein Faktor von mehreren war. Mit Blick in die Zukunft wurde der Fall häufig in Zusammenhang mit einem materiellen Recht auf Vergessen angeführt; vgl. statt vieler WEBER, Forgotten, Rn. 2 ff., 42 f.

1223 BGE 107 II 6.

1224 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, § 11 Rn. 57; siehe vorne B.II.2.3 a)(4).

1225 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, § 11 Rn. 57.

tet werden[1226]. Die Berichtigung der Daten hat im Hinblick auf ihre künftige Verwendung in einer angemessenen Form zu erfolgen[1227] und umfasst nebst der Löschung auch Veränderungen und Ergänzungen[1228]. Die Prüf- oder Berichtigungspflicht wird ausgelöst, sobald konkrete Gründe für die Annahme einer Unrichtigkeit (insbesondere Berichtigungsanspruch) der Daten vorliegen[1229]. Im Zusammenhang mit der Geltendmachung der Ansprüche aus Art. 5 Abs. 2 DSG sind die Informationspflicht und das Auskunftsrecht von zentraler Bedeutung[1230]. Sofern der Datenbearbeiter seiner Pflicht zur Prüfung und gegebenenfalls Berichtigung nicht oder nur unzureichend nachkommt, ist das zukünftige Bearbeiten der mangelhaften Daten *per se* widerrechtlich[1231]. In Art. 6 Abs. 1 der RL 95/46/EG werden unter dem Titel «Grundsätze in Bezug auf die Qualität der Daten» sowohl Aspekte der Datenbearbeitung als auch solche der Information selbst zusammengefasst. Hinsichtlich der informationsbezogenen Kriterien werden auch hier die Richtigkeit und die Aktualität genannt (Art. 6 Abs. 1 lit. b. RL 95/46/EG), in Bezug auf die Informationsverarbeitung insbesondere die Zweckbindung und zeitliche Aspekte der Verhältnismässigkeit (Art. 6 Abs. 1 lit. b), c), e) RL 95/46/EG).

3. Quantitative Dimension

3.1 Bedeutung

Die quantitative Dimension ist ein fundamentaler Bestandteil der Aufzeichnung und Auswertung von Daten. Die Aufzeichnung wachsender Informationsmengen ermöglicht die Nachbildung von Aktivitäten und die Planung zukünftiger Handlungen[1232]. In Anbetracht der grossen Datenmengen, die durch die elektronische Informationsverarbeitung gespeichert werden können, kann die Quantität an vorhandenen Daten durchaus auch in Qualität umschlagen[1233]. Wachsende Datenmengen bedeuten umgekehrt aber auch, dass wesentliche Informationen (beispielsweise solche mit rechtlicher Rele-

---

1226 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, § 11 Rn. 59; ROSENTHAL, Handkommentar DSG, Art. 5 N 13; siehe vorne B.II.2.3 a)(4).

1227 ROSENTHAL, Handkommentar DSG, Art. 5 N 13.

1228 MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 17.

1229 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, § 11 Rn. 57.

1230 MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 16.

1231 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, § 11 Rn. 57.

1232 MAYER-SCHÖNBERGER/CUKIER, 79 ff.; DRUCKER, 83.

1233 MEISTER, 19.

vanz) in der Datenmasse untergehen können[1234]. Dem sollen neue Auswertungsverfahren entgegenwirken[1235].

3.2 Explizit zeitbezogene Normen

Die explizit zeitbezogenen Normen führen zumindest innerhalb der durch sie gezogenen Grenzen der Aufbewahrung zu einer weitgehend bestimmbaren Quantität an Daten. Aufgrund der Problematik, wonach nur Teile dieser Datenbestände vernichtet werden können, kann die Bestimmbarkeit der durch die explizit zeitbezogenen Normen definierten Quantität von Daten über die Zeit nachlassen[1236]. Anders ist dies im öffentlichen Sektor, wo aufgrund der generellen Anbieterpflicht und der an diese anknüpfende, eindeutige Entscheidung über die Vernichtung oder den Erhalt von Daten, die tatsächlich vorhandene Quantität durch die Archivbestände weitgehend bestimmbar sein sollte.

3.3 Implizit zeitbezogene Normen

Viele Daten, die heute generiert werden, sind personenbezogen und Unternehmen haben mannigfaltige Anreize, mehr davon zu speichern, sie länger aufzubewahren und häufiger wiederzuverwenden[1237]. Indessen führt auch eine wachsende Quantität an verfügbaren Daten über eine Person nicht zwingend zu einem ausgewogeneren Urteil über diese. Die Gefahr von Fehlurteilen auf Basis unvollständiger Informationen bleibt bestehen[1238]. Im Weiteren führt die Möglichkeit der Herstellung eines Personenbezugs zu einer quantitativ grösseren Anzahl an Daten, die im Sinne der Datenschutzgesetzgebung als personenbezogen zu qualifizieren sind[1239].

III. Konkretisierung

1. Vorgehen

Im Rahmen der Konkretisierung soll der mehrdimensionale Ansatz einerseits in Bezug auf den Konflikt im weiteren Sinn und andererseits in Bezug auf den Konfliktfall im engeren Sinn angewendet werden. Innerhalb dieser Kategorien wird sowohl eine An-

---

1234 ZIKOPOULOS et al., 6 f., verweisen hierbei auf ein inverses Verhältnis der wachsenden Datenmenge in Unternehmen und dem prozentualen Anteil an Daten, der durch das Unternehmen verarbeitet werden kann.

1235 Siehe dazu ZIKOPOULOS et al., 12 f.

1236 Auch daraus ergibt sich die Eigenschaft von Archivbeständen «Überrest» zu sein; siehe dazu vorne E.II.2.2 c).

1237 MAYER-SCHÖNBERGER/CUKIER, 152.

1238 SOLOVE, Reputation, 66.

1239 Siehe dazu vorne B.II.2.1 b).

wendung im Rahmen des geltenden Rechts als auch eine Anwendung im Rahmen neu zu schaffender Normen aufgezeigt. Unter dem Titel «Ausschluss gesetzlicher Anpassungen» finden jeweils jene Argumente Berücksichtigung, die gegen eine Änderung der bestehenden Normen sprechen. Beim «Einschluss gesetzlicher Anpassungen» folgt die Argumentation dagegen jenen Faktoren, die für entsprechende Änderungen sprechen.

2. Normbezogene Grundlagen

Im Rahmen der Anwendung des mehrdimensionalen Ansatzes auf neu zu schaffende Normen sind im Hinblick auf die Ausgestaltung zwei wesentliche Aspekte in Form der Verhältnismässigkeit bzw. Notwendigkeit der Norm und der Praktikabilität zu beachten: Unverhältnismässig ist eine Regelung dann, wenn sie nicht geeignet ist, das Ziel zu erreichen. Nicht erforderlich ist eine Regelung, wenn durch einen geringeren Eingriff in bestehende Rechtspositionen das gleiche Ziel gleich gut und gleich schnell erreicht werden kann[1240]. Die Chancen, dass eine Norm richtig und vollständig angewendet wird, steigen, wenn diese einfach zu handhaben ist[1241]. Die Kriterien der Praktikabilität lassen sich kaum abstrakt definieren. Wichtig ist, dass die Frage der Praktikabilität frühzeitig geprüft und insbesondere Erfahrungen im Vollzug mit ähnlichen Regelungen einbezogen werden[1242].

3. Anwendung auf den Konflikt im weiteren Sinn

3.1 Ausschluss gesetzlicher Anpassungen

a) Argumentation

(1) Datenerhalt

Die Nutzbarhaltung digitaler Publikationen, Datenbanken oder Websites über einen unbestimmt langen Zeitraum hinweg stellt Organisationen vor komplexe Aufgaben und Entscheidungen. Im Zentrum der Überlegungen steht vielfach die Frage nach der zuverlässigen Sicherung und langfristigen Aufbewahrung[1243]. Weitgehend unklar bleibt, welche Massnahmen in der Gegenwart getroffen werden müssen, um digitale Inhalte

1240 MÜLLER, Rechtssetzungslehre, Rn. 260.
1241 MÜLLER, Rechtssetzungslehre, Rn. 268.
1242 MÜLLER, Rechtssetzungslehre, Rn. 276.
1243 KELLERHALS, in: Coutaz et al., 350; siehe auch die Grundanforderungen an Archive bei BEGLINGER et al., 252 f.; SCHNEIDER, Amnesie, 14.

langfristig nutzbar zu erhalten[1244]. Die Erfahrung mit den klassischen Archiven zeigt, dass Objekte nur über einen sehr langen Zeitraum erhalten werden können, wenn eine Organisation mit der nötigen Struktur vorhanden ist, die diese Aufgabe nachhaltig erfüllen kann[1245]. Aus technischer Sicht ist festzustellen, dass für digitale Archive keine alltäglichen Geräte zur Anwendung kommen, sondern hoch technisierte mehrfach redundante Server und Speichermedien, deren Kosten nicht mit regulären Geräten zu vergleichen sind. Das geläufige Argument, wonach Speicherplatz heute nichts mehr koste, ist für den Archivbereich nicht haltbar[1246]. Die stark angestiegene und laufend billigere Speicherkapazität verleitet auf kurze Sicht dazu, wenig selektiv vorzugehen und alles aufzubewahren[1247]. Hinzu kommt, dass öffentliche Beiträge zur Sicherung von Unternehmensakten meist gering ausfallen[1248]. Ein weiteres Problem besteht in der Sichtung der immensen Datenfülle. So gestaltet sich die Frage, welche Informationen Bestandteil des Projekts e-Helvetica[1249] bilden sollen – und damit die Erfüllung des gesetzlichen Sammelauftrags – für die Nationalbibliothek als arbeitsintensives Unterfangen[1250]. Schliesslich sind auch die Ansprüche an den Kontexterhalt und die Datenqualität zu beachten. Beides kann den Speicherbedarf und die aus dem langfristigen Erhalt entstehenden Kosten weiter erhöhen[1251].

(2) Ziel und Umfang der Aufbewahrungspflicht

Das Bundesgesetz über die Archivierung regelt in Art. 2 Abs. 1 BGA die Aufbewahrung rechtlich, politisch, wirtschaftlich, historisch, sozial oder kulturell wertvoller Unterlagen des Bundes. Das der Öffentlichkeit zugängliche Archiv soll – ähnlich dem BGÖ[1252] – durch die Dokumentation ein bedeutendes Anliegen des demokratischen

1244 SCHMITT, 19; SCHWEIZER/BAUMANN, 239; implizit auch MOSER/NEBIKER/OTHENIN-GIRARD, 67. Eine Auswahl notwendiger Planungsschritte findet sich bei FERLE, 40 ff.

1245 KEITEL/SCHOGER, 5. Die Übertragung wird zudem durch die stetig wachsende Datenmenge laufend erschwert, BORGHOFF et al., 57.

1246 FRÖHLICH, 40; KEITEL/SCHOGER, 52, bezeichnen den Betrieb und die Weiterentwicklung eines digitalen Langzeitarchivs als «kostenintensive Daueraufgaben»; FERLE, 10, weist zudem darauf hin, dass auch die Marktsituation kritisch zu betrachten sei und die Abhängigkeit von einem bestimmten Anbieter zu einem schwer prognostizierbaren Kostenanstieg führen könne.

1247 BORGHOFF et al., 140.

1248 ZÜND, 669.

1249 Ziel des Projekts e-Helvetica ist die Definition von Kriterien für eine längerfristige Sammelpolitik, SCHWEIZER/BAUMANN, 246.

1250 SCHWEIZER/BAUMANN, 246; siehe dazu e-Helvetica, Lagebeurteilung, Strategische Planung 2009-2015, Eidgenössisches Departement des Innern, 7. Juli 2009, 10.

1251 BORGHOFF et al., 141 f.

1252 BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, § 7 Rn. 117. Die zunehmende Zahl an Öffentlichkeitsgesetzen zeigt, dass der Zugang zu Daten der öffentlichen Hand an Bedeutung gewinnt, KELLERHALS, in: Coutaz et al., 354.

Rechtsstaats erfüllen und staatliches Handeln für die Bürger überprüfbar machen[1253]. Der Nachweis über das demokratische Handeln des Staates soll zuverlässig und systematisch dauerhaft erbracht werden können[1254]. Ein weiteres Ziel besteht darin, eine umfangreiche historische und sozialwissenschaftliche Forschung zu ermöglichen[1255]. Auf Bundesebene sieht Art. 6 BGA eine globale Angebotspflicht vor[1256], der im Anschluss gemäss Art. 7 BGA die Ermittlung der Archivwürdigkeit und die Übernahme der Unterlagen folgt. Die wichtigste Kernkompetenz der Archive besteht generell in dieser Bestimmung der Archivwürdigkeit[1257].

Würde die globale Angebotspflicht in gleichem Umfang auf Private übertragen, müssten sämtliche Unterlagen erst durch die Unternehmen erhalten, dann durch das BAR bewertet und im Anschluss gegebenenfalls übertragen werden. Die öffentlichen Archive wären jedoch kaum in der Lage, den Bestand sämtlicher privater Archive zu übernehmen[1258]. Die Digitalisierung von Daten kann dem zwar entgegenwirken, zumindest die Frage nach der Finanzierung bleibt aber bestehen[1259]. Würde die Pflicht zur langfristigen Erhaltung der Datenbestände dagegen bei den Unternehmen verbleiben, müssten diese, damit die Daten nutzbar sind, auch die Bereithaltung und den Zugang zu den Informationen sicherstellen[1260]. Die Übertragung an ein öffentliches Archiv kann ebenfalls eine weitergehende Mitwirkungspflicht erfordern, da zumindest im öffentlichen Sektor auch nach der Ablieferung eine enge Zusammenarbeit zwischen der Verwaltung und dem Archiv stattfindet[1261].

1253 BBl 1997 II 942; siehe auch SEIDEL, Datenbanken, 161: «Die Veröffentlichung zeitgeschichtlicher Daten erfüllt eine demokratische Kontrollfunktion, da sie oftmals Missstände der politischen oder moralischen Führung deutlich macht.».

1254 MOSER/NEBIKER/OTHENIN-GIRARD, 67.

1255 BBl 1997 II 952.

1256 Durch das BGA wurde die als unrealistisch erachtete Ablieferungspflicht durch eine generelle Anbieterpflicht ersetzt, BBl 1997 II 942.

1257 MOSER/NEBIKER/OTHENIN-GIRARD, 67.

1258 Siehe den Verweis bei ZÜND, 669, auf ein Statement des Vereins Schweizerischer Archivarinnen und Archivare anlässlich der Gründung im Jahr 1993.

1259 Die Schweizerische Gesellschaft für Geschichte fordert eine Honorierung durch die öffentliche Hand, da die Errichtung von Privatarchiven eine wichtige kulturelle Dienstleistung an die Gesellschaft darstelle; siehe Schweizerische Gesellschaft für Geschichte, Ethik-Kodex und Grundsätze zur Freiheit der wissenschaftlichen historischen Forschung und Lehre, Bern 2004 (ergänzt 2012), Nr. 7.

1260 MOSER/NEBIKER/OTHENIN-GIRARD, 69, verweisen darauf, dass Archivierung nicht Selbstzweck sei und nebst der Sicherung und Aufbewahrung auch der Zugang und die Vermittlung gewährleistet sein müssten.

1261 MOSER/NEBIKER/OTHENIN-GIRARD, 68.

(3) Notwendigkeit

Die grundlegenden Elemente der Unternehmensgeschichte wurden einleitend bereits dargelegt[1262]. Rein pragmatisch gesehen, ist Unternehmensgeschichte das, was Unternehmenshistoriker tun – sie beschreiben primär die Geschichte von Unternehmen[1263]. Diese Tätigkeit unterliegt gewissen, indirekt auch rechtlich bedingten Grenzen. Ein bis heute bestehendes Problem für Unternehmenshistoriker liegt in der relativen Abhängigkeit von den untersuchten Unternehmen durch begrenzten Quellenzugang, Publikationsauflagen und finanzielle Abhängigkeiten[1264]. Diese Abhängigkeiten sind indessen nicht unüberwindbar[1265]. In Deutschland hat mittlerweile kaum ein namhaftes Unternehmen darauf verzichten können, eine an wissenschaftlichen Standards orientierte Geschichte der eigenen Unternehmung zu veröffentlichen[1266], wobei auch in Deutschland private Unternehmen nicht der Archivgesetzgebung unterliegen[1267].

(4) Haftungsrisiko aus Datenerhalt und Offenlegung

Im Ethik-Kodex leiten die Schweizer Historiker aus der Wissenschaftsfreiheit einen Informationsanspruch zu Forschungszwecken und eine unentgeltliche Akteneinsicht ab[1268]. Die Wissenschaftsfreiheit ist jedoch, wie die übrigen Grundrechte, hauptsächlich ein Abwehrrecht[1269]. Auch im öffentlichen Sektor besteht kein Anspruch auf Zugang zu den für die Forschung benötigten amtlichen Dokumenten[1270]. Darüber hinaus kann die Wissenschaftsfreiheit gegenüber Privaten nicht unmittelbar angerufen werden[1271]. Die bedeutendste Gefahr eines Anspruchs auf Zugang zu Information besteht aus Unternehmenssicht darin, dass das Unternehmen auf Grundlage dieser Informationen mit rechtlichen Ansprüchen konfrontiert werden könnte. Im öffentlichen Bereich wurde die Frage nach der Abwägung der durch die Archivierung betroffenen Interessen[1272] einerseits durch die Schaffung von Schutzfristen gemäss Art. 9, 11 und 12 BGA

1262 Siehe A.I.2.3 a).
1263 PIERENKEMPER, 15, m.w.H.
1264 PIERENKEMPER, 19.
1265 STREMMEL, 143 ff., 185 f.
1266 PIERENKEMPER, 14.
1267 PIERENKEMPER, 21. Siehe zu den Wirtschaftsarchiven des 20. Jahrhunderts in Deutschland und der Schweiz FRANZ, 28 ff.
1268 Schweizerische Gesellschaft für Geschichte, Ethik-Kodex und Grundsätze zur Freiheit der wissenschaftlichen historischen Forschung und Lehre, Bern 2004 (ergänzt 2012), Nr. 11, 14.
1269 SCHWANDER, 135, m.w.H.
1270 SCHWANDER, 139.
1271 SCHWANDER, 165, 169 f.
1272 Siehe dazu RUDIN, 255 f.

beantwortet[1273]. Andererseits wird für besonders sensitive Daten eine Pflicht zur Vernichtung bzw. Anonymisierung vorgesehen[1274]. Dem Problem allfälliger Rechtsfolgen für das Unternehmen aus dem Zugang zu unternehmensinternen Daten könnte durch eine auf die Verjährung abgestimmten Schutzfrist – ähnlich der Regelung des BGA – begegnet werden. Die umfassende Wirkung einer solchen Lösung steht aber in Anbetracht der neueren Rechtsprechung des EGMR zur Verjährung zumindest ansatzweise in Frage[1275].

Abschliessend sind allfällige Auswirkungen auf die Unternehmensidentität und den Ruf der einzelnen Unternehmen zu berücksichtigen[1276]. Aus Unternehmenssicht ist das Erfassen und Zugänglichmachen der Unternehmensgeschichte den Public Relations zuzuordnen, die heute dem Marketing im Allgemeinen und der Werbung im Besonderen als überlegen gelten[1277]. Wesentlich im vorliegenden Zusammenhang ist die Erkenntnis, dass der Ruf als Teil der Public Relations ein Wert ist, der durch das Unternehmen verwaltet und gepflegt werden muss[1278]. Dazu gehört meines Erachtens auch die Unternehmensgeschichte, zumal im 21. Jahrhundert die Wahrnehmung oft über die Realität siegt und selbst eine umsichtige Darstellung aller relevanten Tatsachen eine einseitige und negative Interpretation im Einzelfall nicht zu verhindern vermag[1279]. Der Ansicht, dass das individuelle Anliegen sich nur «im besten Lichte und Andenken» verewigen zu wollen Grenzen hat und Leistungen zumindest zu einem späteren Zeitpunkt gegebenenfalls anders bewertet werden, ist indessen durchaus zuzustimmen[1280]. Das Argument des Schutzes der Unternehmensreputation ist im Unterschied zu haftungsrechtlichen Fragen entsprechend geringer zu gewichtigen.

1273 MOSER/NEBIKER/OTHENIN-GIRARD, 69; siehe zur Abwägung zwischen absoluten und relativen Schutzfristen RUDIN, 258 ff.

1274 Kritisch zur raschen Vernichtung von Daten MOSER/NEBIKER/OTHENIN-GIRARD, 70, die gerade dort, wo der Staat stark in die Persönlichkeitsrechte eines Individuums eingreift, die Notwendigkeit zu einer Überprüfung des staatlichen Handelns auch nach langer Zeit sehen und darauf hinweisen, dass hier eine besonders lange Aufbewahrung aus beweisrechtlichen Gründen eher im Interesse des Betroffenen sein könnte. Siehe zur problematischen Löschungsaktion von Stasi-Akten in den Neunzigerjahren SCHAAR, 31 f.

1275 Siehe dazu vorne B.I.5.2.

1276 Siehe dazu vorne A.I.2.3 d).

1277 SEITEL/DOORLEY, 1.

1278 SEITEL/DOORLEY, 3, 107.

1279 SEITEL/DOORLEY, 172.

1280 BREITSCHMID/KAMP, 29.

(5) Datenschutzrechtliche Interessenabwägung

Eine gesetzliche Grundlage *de lege ferenda* für die Aufbewahrung von Informationen zu unternehmensgeschichtlichen Zwecken würde die damit verbundene Bearbeitung personenbezogener Daten nach Art. 13 Abs. 1 DSG legitimieren[1281]. Indessen ist die Legitimation dieser Datenbearbeitungen nicht an die Notwendigkeit der gesetzlichen Grundlage gebunden. Entscheidet sich ein Unternehmen *de lege lata* für die Wahrung seiner Geschichte und bearbeitet zu diesem Zweck personenbezogene Daten, ist unter Anwendung von Art. 13 Abs. 1 DSG zumindest ein überwiegendes privates Interesse zu berücksichtigen[1282]. Der Zweck einer historisch möglichst umfassenden Dokumentation vermag hier wohl auch einer entsprechenden Verhältnismässigkeitsprüfung standzuhalten[1283].

b) Anwendung innerhalb eines flexiblen Systems

Die explizit zeitbezogenen Normen bilden ein starres System in Bezug auf die Erhaltung von Daten und definieren nebst der minimalen Aufbewahrungsdauer deren Qualität und dadurch auch die Quantität der zu erhaltenden Daten. Diese sind nach der Erfüllung der Aufbewahrungspflichten einem auch auf die implizit zeitbezogenen Normen anwendbaren flexiblen System zuzuführen, das der qualitativen, quantitativen und zeitlichen Dimension integrativ Rechnung trägt. Zentrale Elemente dieses Systems sind der Verhältnismässigkeitsgrundsatz (Art. 4 Abs. 2 DSG) und die Interessenabwägung auf der Rechtfertigungsebene (Art. 13 Abs. 1 DSG).

Unter Anwendung des datenschutzrechtlichen Verhältnismässigkeitsprinzips sind Daten, die zur Erfüllung eines bestimmten Zwecks nicht mehr gebraucht werden grund-

---

1281 Ausdrücklich vorgesehen ist dieser Legitimationsgrund auch in Art. 17 Ziff. 3 (c) E-DSVO.

1282 EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 25, verweist darauf, dass Private grundsätzlich keine öffentlichen Interessen wahrnehmen; BEGLINGER et al., 115 verweisen auf die «Wahrung schutzwürdiger Interessen der aufbewahrungspflichtigen Stelle»; ROSENTHAL, Handkommentar DSG, Art. 13 N 20, verweist darauf, dass dort, wo ein hinreichendes öffentliches Interesse bestehe, häufig auch eine gesetzliche Grundlage gegeben sei. Insgesamt stellt das Informationsbedürfnis der Öffentlichkeit im Bereich des Persönlichkeitsschutzes ein wichtiges öffentliches Interesse dar; vgl. dazu u.a. BGE 132 III 644; BGE 129 III 529; BGE 127 III 481. Das öffentliche Informationsbedürfnis muss sich aber auch bei Archiven immer gegenüber dem Interesse der einzelnen, im Archiv erfassten Person messen; vgl. dazu im öffentlichen Bereich BBl 1997 II 957, wo die Abwägung dieser Interessen durch Schutzfristen gelöst wird. Nach Art. 9 Abs. 1 BGA beträgt die Schutzfrist für sämtliche Unterlagen, die gemäss Art. 9 Abs. 2 BGA nicht bereits vorher öffentlich waren 30 Jahre. Archivgut, das nach Personenname erschlossen ist und besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthält, unterliegt mangels gegenteiliger Einwilligung der betroffenen Person gemäss Art 11 Abs. 1 BGA einer Schutzfrist von 50 Jahren.

1283 BEGLINGER et al., 115; siehe zum Grundsatz der Verhältnismässigkeit EPINEY, in: Belser/Epiney/Waldmann, § 9 Rn. 23 ff.

sätzlich zu löschen[1284]. Dieser Mechanismus führt bei einem engen Zweckverständnis rasch zu einer Reduktion der Datenquantität und ist im Hinblick auf den potentiellen Nutzen verschiedener Auswertungsmöglichkeiten häufig nicht wünschenswert. Die Quantität und Qualität bearbeiteter Daten sollten demnach einerseits im Rahmen der Beurteilung der Verhältnismässigkeit und andererseits im Rahmen der Rechtfertigung in einem zeitlichen Kontext berücksichtigt werden.

3.2 Einschluss gesetzlicher Anpassungen

a) Argumentation

(1) Ausgangslage

Aus rechtlicher Sicht besteht *de lege lata* für Private nebst den beweisrechtlich motivierten gesetzlichen Fristen zur Aufbewahrung bestimmter Dokumente[1285] keine gesetzliche – und insbesondere keine historisch motivierte – Aufbewahrungspflicht[1286]. Eine Ausnahme bildete das Vernichtungsverbot für Akten aus der Zeit des Zweiten Weltkrieges[1287]. Dieses wurde vom Bundesrat durch einen dringlichen Bundesratsbeschluss erlassen und war bis zum 31. Dezember 2001 befristet[1288]. Den oben beschriebenen Problemen in Bezug auf den langfristigen Datenerhalt steht die unmittelbarere Gefahr eines Verlusts wichtigen Kulturguts entgegen, die zumindest ein Erproben verschiedener Lösungen im Gegensatz zu einer weitgehenden Untätigkeit nahelegt[1289].

(2) Sicherung des Informationsbestands

Die Frage des Datenerhalts stellt ein grundsätzliches Problem dar, das auch für Institutionen des öffentlichen Rechts zu lösen ist[1290]. Wie aufwändig und schwierig eine fortwährende technische Pflege digitaler Daten ist, wird sich erst noch zeigen müssen[1291].

1284 Siehe vorne C.III. 2.3.

1285 Siehe vorne A.I.3.3 a)(2).

1286 Das geht beispielsweise *e contrario* aus § 10 Abs. 2 der Archivverordnung des Kantons Zürich vom 9. Dezember 1998 hervor: «Fällt eine öffentliche Aufgabe durch die Auflösung des Organs oder seine Überführung ins Zivilrecht dahin, bietet das Organ die bis zu diesem Zeitpunkt entstandenen Akten dem Staatsarchiv an.».

1287 Siehe zum Hintergrund vorne A.I.2.3 a).

1288 AS 1996 3487.

1289 Vgl. BORGHOFF et al., 136.

1290 Siehe dazu die Hinweise auf die Forschungsergebnisse zum Datenerhalt bei AMBROSE, 372, 391 ff.

1291 SCHENK, 207, der in diesem Zusammenhang weiter feststellt: «Bereits eine kurze Unterbrechung der Wartung elektronischer Datenbestände, etwa in einer Zeit politischer Krise, könnte zu gravierenden Verlusten an Information führen, während Papier in einer Art von Dornröschenschlaf verharren und Jahrzehnte, wenn auch nicht immer ganz unbeschädigt überstehen kann.».

Im Unterschied zum öffentlichen Bereich unterliegen bei Privaten jedoch nebst den Datenträgern und den Lesegeräten auch die Inhaber dieser Geräte der Zeitlichkeit[1292]. Unternehmen sind dem Marktdruck, rechtlichen Eingriffen und politischen Einflüssen ausgesetzt, die Langlebigkeit einzelner Unternehmen ist ein entsprechend seltenes Phänomen[1293]. Der Erhalt digitaler Archive setzt einen verhältnismässig häufigen Wechsel des Speichermediums und eine ständige Wiederholung des Speichervorgangs voraus[1294]. Nach dem heutigen Stand der Technik lässt sich die Unternehmensgeschichte somit nicht einfach *en passant* digital festhalten und auch der Erhalt physischer Dokumente wird durch die Möglichkeit der Diskontinuität der Unternehmenstätigkeit gefährdet. Das Internet reflektiert diese Umstände. So werden die global vernetzten Rechner als grösste Kopiermaschine der Welt bezeichnet – wenn etwas kopiert werden kann, wird es auch kopiert. Der Erhalt über die Zeit ist dagegen nicht Teil dieses Vorgangs[1295].

(3) Verhältnismässigkeit

Unter Bezugnahme auf die normbezogenen Grundlagen erscheint ein Anbieterrecht seitens von Unternehmen und eine entsprechende Prüfpflicht seitens des BAR im Vergleich zu einer umfassenden Angebotspflicht als das mildere Mittel. Der Eingriff in die Rechtsposition der Unternehmen ist bei dieser Lösung geringer. Erst wenn dadurch wesentliche Bestände nicht gesichert werden können, wäre zur Erreichung des Ziels eine globale Angebotspflicht – wie sie im öffentlichen Bereich besteht – in Erwägung zu ziehen. Denkbar wäre ferner eine Beschränkung auf explizit definierte Inhalte, wie sie im Rahmen des RTVG vorgesehen ist.

b) Anwendung innerhalb eines starren Systems

Aus rechtlicher Sicht erscheinen für die Beantwortung der Frage, ob der langfristige Erhalt von Unternehmensdaten *de lege ferenda* aufgenommen werden sollte, folgende Aspekte relevant[1296]: Vorweg bestehen in Bezug auf den langfristigen Erhalt und die Reproduzierbarkeit von Daten erhebliche Ungewissheiten, die mit entsprechenden,

---

1292 Mit Verweis auf Facebook SCHENK, 203.

1293 Ein Drittel der Unternehmen im Fortune 500 von 1970 war bereits 1983 durch Fusionen und Übernahmen, Konkurs oder Aufspaltung wieder verschwunden, The Economist, The business of survival, December 18, 2004.

1294 SCHENK, 207.

1295 MACLEAN/DAVIS, 6, mit Verweis auf die Aussage von Kevin Kelly, Mitgründer und ehemaliger Chefredakteur des Technologiemagazins Wired.

1296 Siehe vorne E.III.3.1 a).

ebenfalls schwer abschätzbaren Kostenfolgen verbunden sind[1297]. Im Weiteren kommt der Dokumentation im öffentlichen Sektor eine fundamental andere Aufgabe als im Privatsektor zu. Anders als bei privaten Akteuren stellt das Archivwesen hier eine unverzichtbare und öffentliche Aufgabe für die Nachvollziehbarkeit, die Kontrolle und das Verstehen staatlichen Handelns dar[1298]. Für den öffentlichen *und* den privaten Sektor ist somit nur das Ziel einer umfangreichen historischen und sozialwissenschaftlichen Forschung beachtenswert. Darüber hinaus erscheint eine globale Anbieterpflicht seitens der Unternehmen als unverhältnismässig. Das RTVG, wo eine solche Pflicht für Private in Art. 21 RTVG statuiert wird, bezieht sich auf einen eng umgrenzten Bereich, aus dem gleichzeitig ein Finanzierungsbeitrag generiert werden kann[1299]. Die Funktion des mehrdimensionalen Ansatzes besteht demnach darin, übergeordnete Kriterien für die Eingrenzung einer Angebotspflicht zu definieren. Innerhalb eines solchen starren Systems wären demnach die Qualität und die Quantität der anzubietenden Daten möglichst genau zu definieren. Diese Herangehensweise liegt auch den weiteren explizit zeitbezogenen Normen zugrunde. Entsprechend könnte sich die Anbieterpflicht insbesondere auf Unterlagen beziehen, für die bereits eine (zeitlich begrenzte) explizite Aufbewahrungsfrist besteht.

3.3 Schlussfolgerungen

Die Unklarheiten im Hinblick auf den langfristigen Erhalt von Daten sowie die mit einer globalen Angebotspflicht verbundenen Risiken für die Unternehmen erscheinen als wesentliche Gründe dafür, von einer Ausweitung der Angebotspflicht auf Private abzusehen. Entsprechend dieser Sichtweise hält Art. 16 Abs. 1 BGA zu Recht am Grundsatz der Vertragsfreiheit fest und verweist für die Einsichtnahme in Nachlässe oder Depositen natürlicher oder juristischer Personen auf die Bestimmungen des jeweiligen Übernahmevertrags. Erst wenn solche Bestimmungen fehlen, kommen subsidiär die öffentlich-rechtlichen Bestimmungen des BGA zur Anwendung. Innerhalb dieses vertragsbasierten Ansatzes *de lege lata* führt der mehrdimensionale Ansatz zur Erkenntnis, dass die Wertung über die Qualität, Quantität und den zeitliche Bestand von Daten grundsätzlich beim Dateninhaber verbleibt, solange sich dieser nicht in Anbetracht der ge-

---

1297 Siehe vorne E.III.3.2 a)(1).

1298 RUDIN, 250; siehe vorne E.III.3.2 a)(2).

1299 Siehe zur ökonomischen Analyse von Normen BYDLINSKI, 286, der diese «zur Verdeutlichung der Konsequenzen, die sich aus der Knappheit der wirtschaftlichen Güter ergeben, und damit zur Bekämpfung der verbreiteten ideologisch-illusionären Vorstellungen, alles, was gut und teuer ist, sei ohne weiteres gleichzeitig voll machbar, wenn man nur die ans Ruder lässt, die allein die richtige Organisation der gemeinsamen menschlichen Aktivitäten wissen» für ein sehr wertvolles Instrument hält.

nannten Kriterien für eine – allenfalls «ewige» – Aufbewahrung dieser Datenbestände entscheidet.

Im Kontrast zu obigen Feststellungen stehen die Ängste eines langfristigen Verlusts historisch relevanter Daten und die entsprechende Argumentation für die Sicherung von Datenbeständen[1300]. Die Anwendung des mehrdimensionalen Ansatzes führt hier zur Erkenntnis, dass eine entsprechende Angebotspflicht innerhalb eines starren Systems auf klar umgrenzte Datenbestände zu beschränken wäre. Ergänzend oder zusätzlich kommt ein Anbieterrecht der Unternehmen mit gleichzeitiger Prüfpflicht seitens des BAR als verhältnismässigere Lösung in Betracht.

4. Anwendung auf den Konflikt im engeren Sinn

4.1 Ausschluss gesetzlicher Anpassungen

a) Argumentation

Die implizit zeitbezogenen Normen des Persönlichkeits- und Datenschutzrechts führen auf unterschiedliche Weise zu einer zeitlichen Beschränkung der Datenbearbeitung. Hinsichtlich der datenschutzrechtlichen Ansprüche auf Datenvernichtung und Datensperrung wird darauf hingewiesen, dass diese im Konfliktfall einerseits zu einer Einschränkung der in Art. 17 BV garantierten Medienfreiheit und andererseits zu einer «Verzerrung historisch relevanter Ereignisse» führen könnten[1301]. Für den Medienbereich wird in der Lehre daher einerseits für eine zurückhaltende Anwendung des DSG plädiert[1302] und andererseits auf die im Vergleich zu anderen Rechtsgebieten hier noch wichtigere Interessenabwägung hingewiesen[1303]. Diesen Bedenken über die Anwendung des Datenschutzrechts ist entgegenzuhalten, dass sich zumindest der Anspruch auf Löschung ohne die Möglichkeit einer Rechtfertigung im Rahmen von Art. 5 Abs. 2 DSG nur auf unrichtige Daten bezieht. Eine Erweiterung der materiellen Ansprüche auf die Beschränkung von Datenbearbeitungen – wie in der geplanten europäischen Datenschutzverordnung vorgesehen – führt hingegen zu einer relevanten Einengung des Anwendungsbereichs der einzelfallbezogenen Interessenabwägung. Dass durch die Datenbearbeitung in verschiedenen Bereichen zunehmend ein bedeutender Nutzen gezo-

1300 Kritisch hierzu RECK, 86 f.: «Die eigentliche Pathologie der Erinnerung besteht in dem durch das historisierende Sammeln heute sich aufdrängenden Verbot, irgendetwas zu zerstören. Das Feld des Erinnerungswürdigen wird seit einigen Jahrzehnten unterschiedslos und schamlos ausgeweitet. Der digitale Code verspricht fälschlich eine universale Registratur alles nur Formulierbaren.».

1301 MEILI, in: Honsell/Vogt/Geiser, Art. 28 N 10.

1302 MEILI, in: Honsell/Vogt/Geiser, Art. 28 N 10.

1303 BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, § 8 Rn. 71.

gen werden kann[1304], lässt sich im privaten Sektor sowohl als Argument für dahingehende Verschärfungen als auch dagegen anführen. Im Vergleich zur staatlichen Datenbearbeitung steht dem Nutzen indessen nicht das gleiche Missbrauchspotential entgegen. Unternehmen mögen in vielerlei Hinsicht mächtig sein, über die staatlichen Zwangsmassnahmen verfügen sie nicht[1305]. Im Resultat erscheint die Möglichkeit einer einzelfallbezogenen Interessenabwägung auch ausserhalb des Medienbereichs als wichtiges Instrument im Zusammenhang mit der Lösung informationsbezogener Konflikte. Fraglich ist, inwiefern dieser Prozess insbesondere unter Berücksichtigung der zeitlichen Dimension stärker strukturiert und systematisiert werden kann.

b) Interessenabwägung im Rahmen der Rechtfertigung

(1) Ausgangslage

Insbesondere bei der automatisierten Datenbearbeitung ist eine tatbestandsbegründende Interessenabwägung nicht hilfreich[1306]. Diese erfolgt entsprechend erst auf der Rechtfertigungsebene. In Bezug auf die Datenbearbeitung Privater soll das DSG den Datenbearbeitern und den Gerichten Orientierungspunkte dafür bieten, wann eine Datenbearbeitung die Persönlichkeit widerrechtlich verletzt[1307]. Die entsprechenden Vermutungen sind in Form der Datenbearbeitungsgrundsätze in Art. 4 DSG enthalten[1308]. Für die Rechtfertigung einer widerrechtlichen Persönlichkeitsverletzung werden in Art. 13 Abs. 2 DSG beispielhaft Situationen aufgeführt, bei denen ein überwiegendes Interesse des Bearbeiters gegeben sein kann[1309]. Entsprechend ihrer systematischen Stellung sind diese Beispiele im Gegensatz zu den Bearbeitungsgrundsätzen aus Art. 4 DSG subjektiv geprägt und orientieren sich an der Absicht des Datenbearbeiters. Wo die Verhältnismässigkeit im Grundsatz abgelehnt und daher von einer Verletzung der Persönlichkeit gemäss Art. 4 Abs. 2 DSG ausgegangen wird, ist auf der Rechtfertigungsebene gemäss Art. 13 DSG über die Widerrechtlichkeit dieser Bearbeitung zu entscheiden. So ist beispielsweise das Speichern von Daten auf Vorrat grundsätzlich unverhältnismässig, im Rahmen einer Betrachtung überwiegender öffentlicher oder privater Interessen kann im Einzelfall die Rechtswidrigkeit aber dennoch verneint werden.

1304 MAYER-SCHÖNBERGER/CUKIER, 192; zusammenfassend POLZER, 6 ff.; siehe auch vorne A.I.1.3 a).

1305 MAYER-SCHÖNBERGER/CUKIER, 156; BULL, 16.

1306 MEISTER, 137.

1307 JAAG/LIENHARD/TSCHANNEN, 240.

1308 PETER, Datenschutzgesetz, 161.

1309 ROSENTHAL, Handkommentar DSG, Art. 13 N 33.

Ein Beispiel hierfür bietet der potentielle Konflikt zwischen der Geltendmachung eines Anspruchs auf Löschung und der Archivierung von Daten[1310]. Werden Daten nur noch für archivarische Zwecke verwendet und in diesem Sinne aufbewahrt, weichen sie in ihrer Funktion von prozessorientierten Daten ab und sind hinsichtlich ihrer Qualität entsprechend anders zu beurteilen[1311]. Das Archivieren stellt aus datenschutzrechtlicher Sicht eine besondere Art der Datenbearbeitung dar, da es nicht um ein materielles Bearbeiten im Sinne eines inhaltlichen Änderns geht, sondern um den Erhalt für ein späteres Bearbeiten[1312]. Da das Bearbeiten archivierter Daten mit dem Zweckbindungsgebot in Konflikt geraten kann[1313], wurden im öffentlichen Bereich spezifische Rechtsgrundlagen für die Archivierung geschaffen, die sich in den entsprechenden kantonalen Archivierungsgesetzen finden[1314]. Auch hier zeigt sich indessen das Problem der Umschreibung eines angemessenen Bearbeitungszwecks; eine zu enge Umschreibung verhindert die Erfüllung künftiger Zwecke und eine zu weite Fassung kollidiert mit dem Verhältnismässigkeitsprinzip[1315]. Die Bestimmungen des Archivwesens im öffentlichen Bereich können generell vorbehalten sein oder die verantwortlichen Behörden dazu verpflichten, die nicht mehr benötigten Daten vor der Vernichtung den zuständigen öffentlichen Stellen zur Archivierung anzubieten[1316]. Die Abwägung zwischen dem Interesse an der Vernichtung der Daten und dem Archivierungsinteresse gestaltet sich aufgrund des ungewissen Nutzens einer retrospektiven Betrachtung der Daten schwierig[1317]. Im privaten Bereich besteht dagegen kein grundsätzliches Erfordernis für eine gesetzliche Grundlage[1318] und die Verletzung des Zweckbindungsgebots sowie der

---

1310 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, § 9 Rn. 59, verweisen auf den Konflikt im Zusammenhang mit Daten, für die eine Archivierungspflicht besteht (i.c. Art. 957 ff. OR). Hier erübrigt sich die Frage nach einer Interessenabwägung indessen bereits aufgrund der gesetzlichen Grundlage. Die Autoren verweisen entsprechend auf die Rechtswidrigkeit einer Veränderung bzw. Löschung solcher Daten.

1311 AMBROSE, 401.

1312 Vgl. RUDIN, 250, der jedoch bei der späteren Bearbeitung von einem materiellen und wohl inhaltlichen Verändern ausgeht; dahingehend auch zitiert bei WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, § 13 Rn. 114. Nach hier vertretener Ansicht ist der Erhalt nicht zwingend mit späteren inhaltlichen Bearbeitungen verbunden.

1313 MOSER/NEBIKER/OTHENIN-GIRARD, Fn. 6.

1314 WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, § 13 Rn. 114; RUDIN, 250 f.; siehe zu den in Ergänzung zum Datenschutz geregelten Inhalten MOSER/NEBIKER/OTHENIN-GIRARD, 69.

1315 RUDIN, 255, mit dem Hinweis, dass eine komplette Endarchivierung sämtlicher Personendaten insbesondere aus datenschutzrechtlicher Sicht unverhältnismässig wäre.

1316 WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, § 13 Rn. 114, mit Verweis auf die entsprechenden kantonalen Gesetze.

1317 WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, § 13 Rn. 114.

1318 Siehe vorne B.II.1.1.

restlichen Bearbeitungsgrundsätze kann im Rahmen der Interessenabwägung gerechtfertigt werden.

(2) Funktion des mehrdimensionalen Ansatzes

Der mehrdimensionale Ansatz ist auf der Rechtfertigungsebene im Rahmen der Interessenabwägung zu integrieren. Der Rechtfertigungsgrund eines überwiegenden privaten Interesses ist trotz seiner besonderen praktischen Relevanz aufgrund der wertenden Abwägung nicht einfach anzuwenden[1319]. Die Interessenabwägung ist «Gerechtigkeits-Optimierung», die auf die Berücksichtigung aller Einzelheiten des jeweiligen Falls abzielt[1320]. Das daraus hervorgehende Richterrecht erzeugt bei jedem Urteil individuell konkretes Recht und ist in dieser Funktion nichts Aussergewöhnliches, sondern Ausdruck rechtschöpfenden Charakters der Rechtsprechung[1321]. Problematisch ist dieser Vorgang nur dort, wo eine richterliche Rechtsfortbildung nicht mehr auf der Grundlage des positiven Rechts erfolgt[1322].

Die Funktion des mehrdimensionalen Ansatzes besteht nicht darin, eine formallogische Methode der subjektbezogenen Interessenabwägung im Persönlichkeits- und Datenschutzrecht zu schaffen. Argumentation findet notwendigerweise in einem psychosozialen Kontext statt und umfasst immer auch Elemente des praktischen Denkens, die ausserhalb einer rein formaltheoretischen Vernunft liegen[1323]. Vielmehr soll der vorliegende Ansatz daher eine integrale Betrachtung der datenbezogenen Kriterien Qualität, Quantität und Zeit fördern und in der Bewertung der Interessen einen argumentativen Orientierungspunkt bieten, der sowohl der Einzelfallgerechtigkeit als auch dem Prinzip der Rechtssicherheit[1324] Rechnung trägt[1325].

Im Zusammenhang mit Anfragen an Medienhäuser hinsichtlich der Löschung, Anonymisierung oder Fortschreibung alter Artikel besteht beispielsweise keine einheitliche Praxis[1326]. In Bezug auf online zugängliche Archive könnte nun der Zugriff in zeitli-

---

1319 ROSENTHAL, Handkommentar DSG, Art. 13 N 6.

1320 DRUEY, Interessenabwägung, 133; siehe zur Wesentlichkeit der Interessenabwägung im konkreten Einzelfall und kritisch in Bezug auf einebnende Verallgemeinerungen BULL, 30.

1321 JESTAEDT, 69.

1322 JESTAEDT, 67 ff.

1323 PERELMAN, 166.

1324 Im Zusammenhang mit der Rechtsprechung soll die Rechtssicherheit gewährleisten, dass auch Einzelfallentscheidungen gut vorhersehbar sind, BYDLINSKI, 293; zur Rechtssicherheit als Gerechtigkeitskriterium, RICHLI, 265.

1325 Ähnlich in Bezug auf die BGH-Rechtsprechung RIEDER, 145.

1326 TREYER, 62.

cher Hinsicht limitiert werden[1327]. Im Rahmen des mehrdimensionalen Ansatzes erfolgt die Beurteilung einer solchen Beschränkung unter Berücksichtigung qualitativer und quantitativer Aspekte. Sind Inhalte in persönlichkeitsrechtlicher Hinsicht beispielsweise unproblematisch, steht einem umfassenden und zeitlich unbegrenzten Zugriff nach hier vertretener Ansicht nichts entgegen[1328]. Gleichermassen kann unter Berücksichtigung quantitativer Aspekte argumentiert werden, sofern eine Persönlichkeit ausgewogen und umfassend dargestellt wird[1329]. Ist ein Beitrag dagegen nur fragmentarisch, undifferenziert und möglicherweise sogar persönlichkeitsverletzend, wäre der Zugriff in zeitlicher Hinsicht zu verkürzen. Einer gänzlichen Löschung stehen die zeithistorische Dokumentation und das Gedächtnis des Medienunternehmens an sich entgegen. In diesem Sinn knüpft der mehrdimensionale Ansatz an die Funktionsweise des Rechts auf Vergessen an, das nur die Verbreitung und nicht den Bestand von Informationen erfasst.

c) Hinweise in der Rechtsprechung

(1) Vorbemerkungen

Nachstehend sind dem mehrdimensionalen Ansatz im Rahmen einer Betrachtung der Rechtsprechung zum Informationsmanagement weitere Konturen zu verleihen. Das Ziel besteht nicht in der Objektivierung der ohnehin subjektiv geprägten Interessen an der Datenbearbeitung, sondern in der Auseinandersetzung mit den objektivierbaren argumentativen Elementen innerhalb konkreter Konfliktfälle.

(2) Der Fall «Logistep»

Dem Bundesgerichtsentscheid liegt eine Empfehlung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemäss Art. 29 Abs. 3 DSG zugrunde, nach der die Logistep AG ihre Datenbearbeitung unverzüglich hätte einstellen sollen[1330]. Nachdem die Logistep AG die Empfehlung abgelehnt hatte, gelangte der EDÖB gemäss Art. 29 Abs. 4 DSG i.V.m. Art. 35 lit. b VGG ans Bundesverwaltungsgericht. Dieses wies die Klage ab und hob die Empfehlung des EDÖB auf[1331]. Das Bundesgericht wiederum hob das Urteil der Vorinstanz auf.

1327 Siehe TREYER, 62, der als Beispiel zehn Jahre nennt.

1328 Siehe auch MAURER-LAMBROU, in: Maurer-Lambrou/Vogt, Art. 5 N 8, der für Daten, die laufend bearbeitet und publiziert werden, einen zeitlich befristeten Berichtigungsanspruch vorschlägt, der nach Ablauf dieser Frist durch die Möglichkeit von Ergänzungen ersetzt würde.

1329 Vgl. PEIFER, 270.

1330 BGE 136 II 508.

1331 BVerwG vom 27. Mai 2009, A-3144/2008.

Die Logistep AG suchte mittels der von ihr entwickelten Software in verschiedenen Peer-to-Peer-Netzwerken (P2P-Netzwerke) nach angebotenen, urheberrechtlich geschützten Werken. Beim Herunterladen dieser Werke wurden Übermittlungsdaten, wie beispielsweise der Benutzername des Nutzers im P2P-Netzwerk und die IP-Adresse, aufgezeichnet und in einer Datenbank abgespeichert. Die auf diese Weise erhobenen Daten wurden anschliessend innerhalb eines entgeltlichen Auftragsverhältnisses an die Urheberrechtsinhaber weitergegeben und von diesen zur Identifikation des Internetanschlussinhabers verwendet. Zur Erreichung dieses Ziels erstatteten die Urheberrechtsinhaber Strafanzeige gegen Unbekannt, um anschliessend via Akteneinsichtsrechts an die Identitätsdaten zu gelangen, die dann zur Geltendmachung von Schadenersatzansprüchen verwendet wurden[1332]. Das Bundesgericht kam in Bezug auf die von der Logistep AG erhobenen Daten zum Schluss, dass statische und dynamische IP-Adressen als Personendaten zu qualifizieren seien, da die Identität des Internetanschlussinhabers – ohne einen unverhältnismässigen Aufwand – nach Art. 3 lit. a DSG bestimmt werden könne[1333]. In subjektiver Hinsicht soll es bei einer Weitergabe der Daten ausreichen und eine Anwendbarkeit des DSG auch auf den Datenübermittler möglich sein, wenn der Empfänger der Daten (i.c. der Urheberrechtsinhaber) die betroffene Person identifizieren kann[1334].

Entscheidend ist, dass der Verstoss gegen die Bearbeitungsgrundsätze Erkennbarkeit und Zweckbindung in Art. 4 Abs. 3 und 4 DSG[1335] sowohl durch ein überwiegendes privates als auch durch ein überwiegendes öffentliches Interesse hätte gerechtfertigt werden können[1336]. Massgeblich ist hier das Qualitätsmerkmal der Daten[1337]: Es ging von Beginn an ausschliesslich um IP-Adressen von Raubkopierern, die zweifellos für eine Straftat benutzt worden waren und deren Sammlung im Rahmen eines Antragsdelikts notwendigerweise durch die Rechteinhaber erfolgen musste[1338].

1332 BGE 136 II 509 f.; ROSENTHAL, Logistep, 41, weist in diesem Zusammenhang zu Recht darauf hin, dass Art. 14 Abs. 4 BÜPF die Grundlage für dieses Vorgehen schafft. Danach müssen Internetanbieter bei über das Internet begangenen Straftaten der zuständigen Behörde alle Angaben machen, die eine Identifikation des Urhebers ermöglichen.

1333 BGE 136 II 513 ff.

1334 BGE 136 II 515; kritisch PROBST, 1429 f.; zustimmend ROSENTHAL, Logistep, 40 f.

1335 In BGE 136 II 518 stimmt das Bundesgericht mit der Vorinstanz überein, dass für die betroffenen Personen weder die Sammlung noch der Verwendungsweck ersichtlich waren.

1336 ROSENTHAL, Logistep, 41 ff.

1337 Die Aufbewahrungsdauer und die Quantität der erhobenen Daten sind durch die Verwertung im Verfahren definiert.

1338 ROSENTHAL, Logistep, 41.

(3) Der Fall «Google Street View»

Dem Bundesgerichtsentscheid liegt ebenfalls eine Empfehlung des EDÖB gemäss Art. 29 Abs. 3 DSG zugrunde, nach der Google zur Anonymisierung von Bildern in Google-Street-View, auf denen Personen und Fahrzeugkennzeichen erkennbar sind, aufgefordert worden war[1339]. Im Folgenden hat das Bundesverwaltungsgericht auf Klage gemäss Art. 29 Abs. 4 DSG i.V.m. Art. 35 lit. b VGG im Sinne des EDÖB entschieden[1340].

Die Rohbilder von Personen und die Abbildungen, die das Erkennen einer Person möglich machen, werden als Personendaten qualifiziert. Von der problemlosen Herstellung eines Personenbezuges ohne grossen Aufwand wird bei Fahrzeugkennzeichen und Häusern ausgegangen. Das Interesse Dritter an diesen Angaben und die Bereitschaft Dritter zur Vornahme einer Identifizierung werden ebenfalls bejaht[1341]. Den Persönlichkeitsschutz konkretisiert das Bundesgericht in Bezug auf das Recht am eigenen Bild insbesondere dahingehend, dass sich der Einzelne nicht dauernd beobachtet fühlen soll, sondern – mit gewissen Einschränkungen – selber soll bestimmen können, welche Informationen über ihn einer breiten Öffentlichkeit zugänglich sind. Im Weiteren wird ausgeführt, dass sich durch die elektronische Datenverarbeitung auch Informationen, die ohne Weiteres der Öffentlichkeitssphäre zurechenbar wären, durch Speicherung, Verknüpfung und Reproduktion zu schützenswerten Persönlichkeitsprofilen verdichten liessen[1342].

Im Rahmen der Interessenabwägung wird bestätigt, dass die Veröffentlichung eines individualisierenden, nicht rein zufälligen Bildes ohne Einwilligung des Betroffenen immer persönlichkeitsverletzend ist[1343]. Die Einschränkung wird jedoch gegen den Aufwand des Anbieters zur Anonymisierung der Daten abgewogen[1344]. Die Toleranzgrenze in Bezug auf die Identifizierbarkeit wird bei 1 Prozent angesetzt. Zudem werden verschiedene Bedingungen aufgestellt, wie beispielsweise die Einrichtung eines leicht zu handhabenden und kostenlosen Widerspruchsverfahrens, das zur Anonymisierung der betroffenen Person führt, die Verwendung neuster Technologien zur automatischen Anonymisierung, die Sicherstellung einer vollständigen Unidentifizierbarkeit von Personen im Zusammenhang mit sensitiven Einrichtungen (Gerichte, Gefängnisse, Spitä-

1339 BGE 138 II 346.
1340 BVerwG vom 30. März 2011, A-7040/2009.
1341 BGE 138 II 356.
1342 BGE 138 II 359.
1343 BGE 138 II 360.
1344 BGE 138 II 365 ff.

ler, ect.) und die Vermeidung von Aufnahmen geschützter Privatbereiche[1345]. Im Rahmen der Interessenabwägung anerkennt das Bundesgericht, dass nebst den wirtschaftlichen Interessen seitens Google auch das Interesse der Bevölkerung an der Nutzung dieses Angebots zu berücksichtigen ist[1346].

Massgeblich ist im vorliegenden Fall die Feststellung, dass die Interessen an der Bearbeitung eines qualitativ und quantitativ definierten Teils der Daten die Interessen der Betroffenen am Schutz dieser Daten nicht zu überwiegen vermögen. Für den im Interesse des Datenbearbeiters sowie Dritter liegenden Teil der bearbeiteten Daten ist die Erkennbarkeit personenbezogener Merkmale nicht erforderlich.

(4) Der Fall «Moneyhouse»

Das Bundesverwaltungsgericht erliess auf Antrag des EDÖB eine superprovisorische Zwischenverfügung, wonach die itonex AG als Betreiberin des Internet-Portals moneyhouse.ch angewiesen wurde, ihren Dienst zur Personensuche vorläufig einzustellen. Entscheidend war unter anderem, dass gemäss EDÖB gesperrte private Daten veröffentlicht wurden[1347]. Die itonex AG bezieht die Daten elektronisch vom SECO und ergänzt diese mit verschiedenen Suchfunktionen – insbesondere mit einer Personensuche mit den Parametern Name, Vorname und Heimatort.

Aus der Öffentlichkeit des Handelsregisters, dem Zweck der Publizität und insbesondere jenem der informationellen Erleichterung des Geschäftsverkehrs leitet das Bundesverwaltungsgericht ein generelles öffentliches Interesse an einer möglichst leichten Zugänglichkeit der Handelsregisterdaten ab[1348]. Dieses erfasse auch das Angebot privater Anbieter[1349]. In zeitlicher Hinsicht sind die auf der Website einmal veröffentlichten Handelsregistermeldungen der natürlichen und der juristischen Personen unbeschränkt verfügbar. Über die Online-Publikation des SHAB sind dagegen nur Handelsregistereinträge der letzten drei Jahre abrufbar. Das Bundesverwaltungsgericht stellt jedoch fest, dass für sämtliche Arten der Publikation von Handelsregisterdaten kein Raum für eine zeitliche Befristung bestehe. Ferner stellt das Bundesverwaltungsgericht fest, dass trotz einer zu erwartenden Abnahme der Publikumsinteressen an gewissen Handelsregisterinformationen über die Zeit die Fiktion der Kenntnis der entsprechenden Einträge

1345 BGE 138 II 367 ff.
1346 BGE 138 II 366 f.
1347 Siehe die Medienmitteilung des EDÖB vom 7.8.2012.
1348 Siehe dazu eingehend MEIER-SCHATZ, 435 ff.
1349 BverwG vom 28. Februar 2008, A-4086/2007, E. 5.2.3 f.

fortbestehe[1350]. Ein «Recht auf Vergessen» würde den Gesetzeszweck des Handelsregisters unterlaufen[1351]. Daran ändert nach Ansicht des Gerichts auch Art. 11 Abs. 2 der Verordnung zum SHAB nichts, der nur eine Onlineverfügbarkeit von drei Jahren vorsieht. Dies insbesondere deshalb, da Art. 11 Abs. 2 der Verordnung zum SHAB nicht speziell auf Handelsregisterdaten ausgerichtet sei und eine Verhältnismässigkeitsvorgabe für private Veröffentlichungen daraus entsprechend nicht abgeleitet werden könne[1352]. Im Resultat verstosse die zeitlich unbeschränkte Weitergabe von Handelsregisterinformationen nicht gegen das Zweckbindungsgebot aus Art. 4 Abs. 3 DSG und entsprechend liege keine Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 lit. a DSG vor[1353]. Im Weiteren stellte das Bundesverwaltungsgericht fest, dass das Verhältnismässigkeitsprinzip nicht verletzt sei und die Datenbearbeitung gemäss Art. 13 Abs. 1 DSG i.V.m. Art. 930 OR auf einer gesetzlichen Grundlage beruhe[1354]. Offen lässt das Bundesverwaltungsgericht, ob die Personensuche mit dem Persönlichkeits- bzw. Datenschutz vereinbar und vom handelsregisterrechtlichen Zweck der Publizität und der informationellen Erleichterung des Geschäftsverkehrs gedeckt. Auch die Frage, ob technische Massnahmen zur Einschränkung der Auffindbarkeit durch Suchmaschinen von der Anbieterin genutzt werden müssten, bleibt ungeklärt[1355].

Zentral ist hier die Feststellung, dass sämtliche Daten, die den qualitativen Kriterien von Handelsregisterdaten entsprechen zumindest in Bezug auf ihre Speicherung und wohl weitgehend auch in Bezug auf andere Bearbeitungen keinen zeitlichen Schranken unterliegen.

4.2 Einschluss gesetzlicher Anpassungen

a) Argumentation

Aus rechtlicher Sicht wird der etablierte Mechanismus von Information und Einwilligung durch die sekundäre Nutzung von Daten grundsätzlich in Frage gestellt. MAYER-SCHÖNBERGER und CUKIER sehen die Lösung in einem neuen System zum Datenschutz, das weniger auf die individuelle Zustimmung zur Datenbearbeitung im Zeit-

1350 BverwG vom 28. Februar 2008, A-4086/2007, E. 5.2.5.

1351 BverwG vom 28. Februar 2008, A-4086/2007, E. 5.2.6. Das Recht auf Vergessen weist in diesem Zusammenhang einen doppelten Sinn auf: Nebst dem fehlenden Anspruch auf Vergessen für den von der Datenbearbeitung Betroffenen, impliziert die Fiktion der Kenntnis auch für die relevanten Verkehrskreise eine Schranke des Vergessens.

1352 BverwG vom 28. Februar 2008, A-4086/2007, E. 5.2.7.

1353 BverwG vom 28. Februar 2008, A-4086/2007, E. 5.2.9.

1354 BverwG vom 28. Februar 2008, A-4086/2007, E. 7.2.

1355 BverwG vom 28. Februar 2008, A-4086/2007, E. 5.2.8.

punkt der Datenerfassung ausgerichtet ist und vermehrt die Verantwortlichkeit des Datennutzers für seine Handlungen zum Gegenstand hat[1356]. Im Zusammenhang mit dieser Zuordnung der Verantwortlichkeit steht die von den Autoren geforderte Nachvollziehbarkeit und Zurückverfolgbarkeit der Datenbearbeitung[1357]. Die Wahrnehmung dieser Aufgabe erfordert nach Ansicht der Autoren eine neue Gruppe von Experten, die die Funktionsweise und die Erfüllung zu schaffender Standards überprüfen soll[1358]. Der hier entwickelte Ansatz für die Elemente eines solchen Standards steht im Kontext der nationalen Gesetzgebung. Die grundsätzlichen Überlegungen lassen sich aber auch ausserhalb dieses Kontexts auf andere Rechtsordnungen übertragen[1359].

b) Erweiterung des mehrdimensionalen Ansatzes

(1) Datenintensitätsmodell als Ausgangspunkt

Ein neues System und neue Standards zum Datenschutz könnten durch ein allgemeines Datengesetz realisiert werden, das die informationelle Selbstbestimmung und den präventiven Schutzgedanken weitgehend ausklammert. Im Hinblick auf die zu schaffenden Standards wird der mehrdimensionale Ansatz hier zu einem Datenintensitätsmodell (DIM) erweitert, das die Zeit, die Quantität und die Qualität von Daten integral erfasst[1360]. Anstelle der wenig differenzierten Anknüpfung der Datenschutzgesetze am Begriff des personenbezogenen Datums[1361] knüpft das DIM an den drei zentralen Kri-

1356 MAYER-SCHÖNBERGER/CUKIER, 173, 193.

1357 MAYER-SCHÖNBERGER/CUKIER, 178 f.

1358 MAYER-SCHÖNBERGER/CUKIER, 179, 180 ff.

1359 Siehe zur Notwendigkeit global anwendbarer Prinzipien CAVOUKIAN, 192 f.; dahingehend in der Entstehungszeit der datenschutzrechtlichen Gesetzgebung auch bereits DAMMANN/MALLMANN/SIMITIS, 7. Dagegen besteht eine mögliche Entwicklung in der «Fragmentierung» des Internets, die nationale oder gar regionale Lösungen wieder verstärkt in den Fokus rücken könnte; siehe dazu GRASSEGGER HANNES, NZZ am Sonntag, Das Ende des Internets: Staaten steigen aus dem Web aus, 9. Februar 2014.

1360 Siehe dazu AMBROSE, 384, wonach jede Regulierung ältere Informationen und deren wechselnden Wert genau analysieren soll, um diesen dann gegenüber bestehenden Bedürfnissen und Werten abzuwägen.

1361 BULL, 23, sieht darin die eine Verrechtlichung sämtlicher Informationsbeziehungen, die jeden Gesetzgeber überfordere.

terien für eine differenzierte Kategorisierung der bearbeiteten Daten an[1362]. Unter Berücksichtigung der problematischen Fragmentierung von Datenschutzgesetzen im US-amerikanischen Recht schafft das DIM eine einheitliche Grundlage für die Konkretisierung[1363]. Die Bewertung der Datenqualität erfolgt anhand eines erweiterten Bezugssystems, das insbesondere die Perspektive der Datenbearbeiter integriert[1364]. Im Fall «Logistep» beispielsweise ist unter Berücksichtigung des Kriteriums «Mehrwert» festzustellen, dass die gewinnorientierte Zielsetzung der Datenbearbeitung erst durch die nachgelagerte Bestimmung der betroffenen Person im Strafverfahren möglich wird. Gleichzeitig wird hierbei deutlich, dass der Wert und die Relevanz der Daten für Logistep in diesem Zeitpunkt endet[1365]. Der Wert der Information verändert sich damit über die Zeit[1366]. Die Diskussion darüber, ob sich die bearbeiteten Daten auf eine bestimmte oder bestimmbare Person beziehen, erübrigt sich, da aus der tatsächlichen Zielsetzung und der konkreten Nutzung der Daten bestimmte Personen identifizierbar werden. Die entscheidende Frage ist demnach, was mit den Daten letztlich gemacht wird.

1362 Vgl. auch das Modell von SCHWARTZ/SOLOVE, 1865 ff., 1877, in dem Informationen einem Kontinuum zugeordnet werden, an dessen Anfang Informationen ohne Risiko einer Identifikation stehen und das mit identifizierten Individuen endet. Das Kontinuum wird in die drei Kategorien identifizierter, identifizierbarer und nicht identifizierbarer Personen unterteilt, auf deren jeweiligen Daten unterschiedliche Regulierungen anwendbar sein sollen. Unter Berücksichtigung der Ausführungen zum Fall «Logistep» erscheint eine abstrakte Kategorisierung von Daten im Hinblick auf eine mögliche Bestimmbarkeit als wenig hilfreich, da bei nicht identifizierenden Daten die Gefahr einer Persönlichkeitsverletzung immer abstrakter Natur ist und folglich im Konfliktfall immer nur die letzte Kategorie von Bedeutung sein wird.

1363 Vgl. SIMITIS, der die Abschaffung des BDSG anregt und an dessen Stelle ein Gesetz vorsieht, das die generellen Prinzipien umfasst. Die präzisierenden bereichsspezifischen Regelungen würden dann damit verbunden und zeitlich befristet; siehe dazu Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Interview mit Prof. Dr. Dr.h.c. Spiros Simitis, 1:03:44 ff., abrufbar unter: https://www.datenschutzzentrum.de/interviews/simitis/, abgerufen am 1.6.2014. Siehe zum Fehlen einer generellen Regulierung BONDALLAZ, Rn. 746 f.

1364 Siehe dazu das Konzept von WANG/STRONG, 20, wo die Datenqualität in die vier übergeordneten Kategorien intrinsisch (Richtigkeit, Objektivität, Glaubwürdigkeit, Reputation), kontextuell (Mehrwert, Relevanz, Aktualität, Vollständigkeit und hinreichender Umfang), gegenständlich (Deutbarkeit, Verständlichkeit, Konsistenz, Übersichtlichkeit) und Zugänglichkeit (Zugang und Zugangssicherheit) unterteilt wird.

1365 Siehe zur gesetzlich vorgesehenen Berücksichtigung des zeitbezogenen Werts von Daten die Bestimmung im BDSG: Nach § 35 Abs. 2 Nr. 4 BDSG werden Stellen, die Daten zum Zweck der Übermittlung und Vermarktung speichern, nach Ablauf von drei Jahren zur Prüfung der weiteren Erforderlichkeit einer Speicherung verpflichtet. Falls die Daten für eine Vermarktung weiterhin interessant sind und die Zulässigkeit der Speicherung gemäss § 29 Abs. 1 BDSG weiterhin gegeben ist, können sie weitere drei Jahre gespeichert werden; siehe dazu GOLA/KLUG/KÖRFFER § 35 N 14, besondere Löschungsvorschriften bleiben unberührt.

1366 AMBROSE, 398.

(2) Konkretisierung am Beispiel der Datenlöschung

Die Speicherung ist in Form der Vorschriften zur Aufbewahrung bereits Gegenstand explizit zeitbezogener Normen. Konzeptionell wäre hier nur noch eine Erweiterung in Form von Speicherungsverboten möglich. Solche würden indessen jedes Nutzungspotential von Beginn weg ausschliessen[1367]. Die zeitliche Normierung der Verwertung führt dagegen konzeptionell letztlich wieder zum datenschutzrechtlichen Zweckbindungsprinzip, das bezüglich seiner Anwendbarkeit unter Privaten grundsätzlich problematisch ist[1368]. Die Verwertung ist entsprechend gezielter durch die Aspekte Risiko und Haftung zu erfassen. Ein wirksamer Eingriff *ex ante*, der insbesondere der Notwendigkeit und den Schwächen einer gerichtlichen Durchsetzung nur im Ausnahmefall unterliegt, ist demnach auf der Ebene der Löschung zu integrieren.

Vernetzte Informationssysteme führen dazu, dass zeitlich voneinander abweichende und unterschiedliche Ereignisse in der Gegenwart gleichzeitig präsent sein können[1369]. Aufgrund der zunehmenden Speicherung von Daten über öffentliche und private Handlungen, wird die Kontrolle über den Lebenszyklus dieser Daten an Bedeutung gewinnen[1370]. Allen informationellen Konflikten ist die Abwägung der unterschiedlichen Interessen gemein, der Zeitablauf kann aber zu einer notwendigen Neubeurteilung führen[1371]. Hierbei sind u.a. die Informationseigenschaften in Form der Qualität und Quantität relevant. Im Rahmen des DIM sind entsprechend vorweg die bearbeiteten Daten zu bewerten. In einem zweiten Schritt werden in Bezug auf den einzelnen Sektor spezifische Regeln erlassen, die die Löschung einzelner Datenkategorien vorsehen[1372]. Der Löschvorgang selbst kann durch Datensysteme integriert werden und ist so auszugestalten, dass sämtliche Kopien einer Datei nach einer festgelegten Zeit nicht mehr lesbar sind[1373]. In Abgrenzung zum Recht auf Vergessen wird die Interessenabwägung hierbei vorweggenommen, was eine eindeutige und enge Kategorisierung der zu lö-

---

1367 Siehe dazu die Kritik bei BULL, 26 f., sowie den Verweis auf die Rasterfahndung, wo Daten zwischenzeitlich gespeichert und bei fehlender Relevanz – ohne menschliche Wahrnehmung – automatisch wieder gelöscht werden.

1368 Siehe dazu B.II.2.5.

1369 MÜLLER, Kontrolle, 146.

1370 GEAMBASU et al., 2.

1371 AMBROSE, 399.

1372 Auch aus ökonomischer Sicht erscheint eine spezifische Regulierung als vorteilhaft; siehe dahingehend HUI/PNG, 488.

1373 Siehe dazu GEAMBASU et al., 2 ff.; HON/MILLARD, in: Millard, 23.

schenden Daten bedingt[1374]. Unproblematisch dürfte die Löschung eindeutig falscher Daten sein[1375]. Aber auch bei richtigen Daten erscheint die generelle Vermutung über deren Wert als fragwürdig und ein automatisierter Löschmechanismus ist insbesondere unter Berücksichtigung der zeitlichen und qualitativen Dimension von Daten nicht rundweg abzulehnen[1376]. Vorteilhaft ist dieses Vorgehen insbesondere dort, wo Daten nicht willentlich, sondern automatisch in Backup-Systeme integriert werden.

c) Integration von Risiko und Haftung

Den Anreizen zur Sammlung und Verwertung personenbezogener Daten stehen kaum Risiken gegenüber[1377]. Ökonomisch betrachtet kann ein Unternehmen die Gewinne aus der Nutzung der Daten internalisieren und gleichzeitig einen Anteil der Kosten externalisieren – ein Umstand, der die übermässige Beanspruchung personenbezogener Daten fördert[1378]. Externalitäten führen generell dazu, dass der private und der soziale Nutzen bzw. die privaten und sozialen Kosten wirtschaftlichen Handelns auseinanderfallen[1379]. LANIER schlägt als Lösung eine Einbindung der Risikotragenden in den Wertschöpfungsprozess vor[1380]. Nebst dieser Partizipation der Risikotragenden am Nutzen der Datenverwertung sind auch Anpassungen im Bereich der Haftung für die Datenverwerter denkbar[1381]. Die technologische Entwicklung erweitert das Potential für Verlet-

1374 Siehe in Bezug auf das Recht auf Vergessen AMBROSE, 376, die veraltete, irrelevante, schädliche und/oder unrichtige Informationen nennt; vgl. zur vergleichbaren Ausgestaltung im öffentlichen Recht vorne BII.2.4 a). Zur Sicherstellung einer sachgerechten Anwendbarkeit können zudem die spezifischen Erlasse selbst zeitlich befristet werden; siehe vorne E.I.

1375 Siehe zur Bedeutung richtiger Daten u.a. BAUKNECHT, in. ders./Forstmoser/Zehnder, 14. Die Löschung falscher Daten ist allenfalls dort problematisch, wo es gerade darum geht, den Nachweis der Unrichtigkeit zu erbringen.

1376 A.A. MANTELERO, 739, der zumindest den kollektiven Informationsbestand des Internets generell als zu bewahrendes Wissen wertet. Siehe die Beispiele für eine auf zeitlichen und qualitativen Kriterien beruhende Informationsbewertung im US-amerikanischen Recht bei AMBROSE, 378.

1377 Siehe die Beispiele zur Netzwerkökonomie bei LANIER, 263 ff.; auch im Medienbereich wird selten Schadenersatz zugesprochen, siehe dazu STUDER PETER, NZZ, Schadenersatz erhält man Selten, 28. Mai 2013; siehe im Zusammenhang mit Persönlichkeitsverletzungen im Allgemeinen und im Rahmen der Entstehung des deutschen Datenschutzgesetzes STEINMÜLLER et al., 136.

1378 SWIRE/LITAN, 8. Die Kapitalbindung zur Vorhaltung von Daten nimmt durch sinkende Preise für Speicherplatz – mit Ausnahme der Kosten für eine langfristige Aufbewahrung – ab, womit hauptsächlich noch die mit der Erhaltung der Daten verbundenen Risiken für eine Reduktion der Informationsmenge sprechen; vgl. dazu AUGUSTIN, 72.

1379 MANKIW/TAYLOR, 245; LINDE, 46; LANIER, 264, verweist auf die strukturellen Ähnlichkeiten mit dem Finanzsektor und das Problem von *too obig to fail*, das durch das Eingehen von Risiken für Einzelne einen entsprechenden Nutzen generiert, ohne dass diese auch die Kosten für diese Risiken tragen müssten.

1380 LANIER, 265 ff., 268. Konzeptionell ist dieser Vorschlag von jenem mit KILLIAS im Zusammenhang mit der Verjährung vergleichbar; siehe vorne B.II.5.2 a).

1381 Siehe insbesondere dazu GANDY, 183 ff.

zungshandlungen laufend, der Erfolg für eine Verhaltenskontrolle anstelle der Erfolgskontrolle ist damit schon länger als sehr begrenzt zu erachten[1382]. Der mehrdimensionale Ansatz liefert die genannten objektivierbaren Kriterien in Bezug auf den Umfang einer möglichen Verantwortlichkeit. Im Rahmen der spezialgesetzlichen Konkretisierung des DIM könnten gewisse Datenkategorien nach einem bestimmten Zeitablauf einer verschärften Haftung zugeführt werden. Werden beispielsweise quantitativ umfangreiche und qualitativ hochstehende Daten bearbeitet, wären diese rascher wieder zu löschen. Erfolgt die Löschung dagegen nicht und steigt das Risiko eines Missbrauchs dadurch an, wäre die Haftung im Falle eines Missbrauchs der Daten zu verschärfen. Eine solche Verschärfung könnte beispielsweise durch eine Beweislasterleichterung zu Gunsten des Klägers erreicht werden. Die Haftung für Daten, die keiner besonderen Kategorie zugeordnet sind, richtet sich nach dem etablierten Rechtsbehelfen im Rahmen von Art. 28a Abs. 3 ZGB. Ein wesentlicher Faktor in Bezug auf die Haftung für den Datenmissbrauch ist die Möglichkeit der Einschränkung der Zugänglichkeit von Daten. Im virtuellen Raum können Daten durch die Schaffung spezieller Umgebungen mit Registrierfunktion und Zugriffsregeln geschützt werden[1383].

4.3 Schlussfolgerungen

Unter Verweis auf die Bedeutung der einzelfallbezogenen Interessenabwägung bietet der mehrdimensionale Ansatz im Rahmen des geltenden Rechts eine integrale Herangehensweise und einen argumentativen Orientierungspunkt. Die Anwendung eines gleichförmigen Ansatzes führt darüber hinaus auch innerhalb von Unternehmen zu einer Verbesserung der Transparenz und erleichtert damit die Einhaltung der gesetzlichen Vorgaben[1384]. In Anbetracht der wachsenden Datenvolumen und den erhöhten Anforderungen an den Persönlichkeits- und Datenschutz bedarf das unternehmensbezogene Informationsmanagement an sich einer Priorisierung und Fokussierung anhand eines objektiven Massstabs[1385]. Das Ziel des Ansatzes besteht in diesem Zusammenhang gerade nicht darin, unter Verweis auf formale Prinzipien wie die Zweckbindung

---

1382 AEBI-MÜLLER, Rn. 109; siehe auch den Hinweis bei GANDY, 184, wonach sich die Schaffung regulatorischer Grenzen für die Nutzung diskriminierender Technologien in den USA als äusserst schwierig erwiesen hat. SIMITIS, Utopie, 527, erachtet den Versuch, Regeln zu realisieren, die zu einer tatsächlichen Restriktion der Verarbeitung führen als «ungemein beschwerlich und fortwährend von Rückschlägen begleitet» aber dennoch notwendig.

1383 ONUF/HYRY, 253; AMBROSE, 380. Siehe einschränkend den Hinweis zum Digital Rights Management (DRM) bei GRIMMELMANN, 1187, wonach technische Vorkehren zur Kontrolle von Daten selten wirksam sind, sofern jemand Zugriff auf diese Daten hatte und entschlossen ist, diese zu verbreiten.

1384 HAGMANN, in: Coutaz et al., 278.

1385 MCKEEN/SMITH, 81 f., m.w.H.

oder die Verhältnismässigkeit, die Datenbearbeitung abstrakt einzuschränken. Die allgemeinen Kriterien sollen vielmehr die einzelfall- und argumentationsbezogene Betrachtungsweise fördern und insbesondere den zahlreichen Situationen Rechnung tragen, in welchen die Bearbeitung von Daten nicht nur erforderlich, sondern auch erwünscht ist[1386].

Unter Einschluss gesetzlicher Anpassungen und unter Berücksichtigung des Wirkungsgehalts des allgemeinen Persönlichkeitsrechts wäre eine Ablösung vom persönlichkeitsrechtlich geprägten Datenschutz zu einem allgemeineren Datenrecht als Grundlage für präzisierende und schutzmotivierte Einzelerlasse denkbar. Der Datenschutz ist nicht Selbstzweck, er bemisst sich an der konkreten Schutzbedürftigkeit im Einzelnen[1387]. Den gesetzlichen und allein am Personenbezug von Daten orientierten Vermutungstatbeständen von Persönlichkeitsverletzungen im geltenden Recht stehen zunehmend Bearbeitungspraktiken entgegen, die nach einer differenzierten Beurteilung verlangen. Zwar ist diese im Rahmen der Interessenabwägung wie dargelegt weitgehend möglich, aufgrund der bundesgerichtlichen Zurückhaltung in der Anerkennung von Rechtfertigungsgründen zumindest bis jetzt aber deutlich eingeschränkt. Unter Berücksichtigung des potentiellen Nutzens, den Dateninhaber aus ihren Datenbeständen ziehen, erscheint im Rahmen eines expliziten Zeitbezugs auch eine generelle Pflicht zur Löschung als problematisch[1388]. Selbst wenn ein Unternehmen seine Datenbestände selbst nicht umfassend nutzt, besteht die Möglichkeit die Nutzung in Lizenz an Dritte zu übertragen[1389]. Unter Bezugnahme auf das DIM wäre eine spezialgesetzliche Pflicht zur Löschung daher auf bestimmte Datenkategorien zu beschränken. Insbesondere unrichtige Daten könnten Gegenstand einer zwingenden und – nach Massgabe technischer Möglichkeiten – automatisierten Löschung sein. Unabhängig von einer gesetzlichen Pflicht

---

1386 Vgl. BULL, 29.

1387 Vgl. BONDOLFI, 140; BULL, 30; siehe zum Selbstzweck ROSENTAHL, Bauchgefühl, 91.

1388 STEINMÜLLER et al., 146, erachteten eine automatische Löschung für die gewerbliche Datennutzung in Anbetracht des Aufwandes zur Wiederbeschaffung erneut benötigter Daten in den Siebzigerjahren noch als «zu hart». Die beschleunigte Speicherung und Verarbeitung von Daten durch immer schnellere Prozessoren könnte in bestimmten Bereichen jedoch zu einer Verkürzung der Speicherdauer führen. Wo heute beispielsweise in der Medizin umfangreiche Patientendossiers angelegt werden, könnte künftig eine rasche und kostengünstige Analyse der körperlichen Verfassung die Relevanz dieser vergangenen Daten in Frage stellen. Aus der umfassenden Analyse der aktuellen Lage würde dann so viel Information bzw. Wissen gezogen werden können, dass eine – in diesem Zusammenhang rudimentär anmutende – Sammlung und Analyse alter Daten hauptsächlich noch für historische oder statistische Zwecke relevant erschiene; siehe dahingehend in Bezug auf operationelle Geschäftsdaten auch AMBROSE, 405.

1389 MAYER-SCHÖNBERGER/CUKIER, 121, mit Verweis auf Lizenzzahlungen an Autoren und die Verknüpfung von Lizenzzahlungen mit Erfindungen im Biotechnologiesektor, die auf der Technologie des Lizenzgebers beruhen.

und automatisierten Löschung ergibt sich, dass veraltete Daten häufig einen geringen Wert haben aber erhebliche Risiken bergen und sich der Bearbeiter dessen bewusst sein sollte. Darüber hinaus bedarf auch ein kommerzieller Lösungsansatz, wie ihn LANIER propagiert, einer präzisen (buchhalterischen) Erfassung bearbeiteter Daten, die eben gerade auch die «Abschreibung» negativer Datenbestände beinhalten sollte. Das DIM als Erweiterung des mehrdimensionalen Ansatzes bietet auch hier eine mögliche Bewertungsstruktur. Am anderen Ende des Spektrums steht der Erhalt historisch relevanter Daten, die ebenfalls entsprechend kategorisiert werden und durch Zugangsbeschränkungen geschützt erhalten werden können. Die Schwierigkeit besteht hier vor allem in der Vorhersage darüber, welche Informationen in Zukunft von Wert sein werden.

Patrick Eggimann

2014 - 2015	Praktika Zürich / London
2012 - 2014	Wissenschaftlicher Mitarbeiter / Geschäftsführer Forschungsstelle für Informationsrecht (FIR-HSG)
2012	Universität Zürich, Master of Law (Business Law)
2010	Universität Zürich, Bachelor of Law