Zulässigkeit des Einsatzes von Email-Filtersoftware in Deutschland und den USA

INAUGURAL-DISSERTATION

zur

Erlangung des Grades eines Doktors des Rechts

am Fachbereich Rechtswissenschaft

der

Freien Universität Berlin

vorgelegt von

Carolin Schug
Rechtsanwältin in Taufkirchen
2007

Erstgutachter:	Priv.-Doz. Dr. Lothar Determann
Zweitgutachter:	Univ.-Prof. Dr. Klaus Rogall
Tag der mündlichen Prüfung:	30.01.2009

Für meine Eltern und Matthias

Danksagung
Ich bedanke mich bei Herrn Priv.-Doz. Dr. Determann für seine engagierte Unterstützung, die zahlreichen Anregungen und Denkanstöße sowie die zeitnahe Korrektur.

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

2d	Second
3d	Third
4th	Fourth
a.A.	anderer Ansicht
a.a.O.	am angegebenen Ort
ABl.	Amtsblatt der EG
Abschn.	Abschnitt
a.E.	am Ende
AfP	Archiv für Presserecht
A.L.R. Fed.	American Law Reports, Federal
Am. Bus. L. J.	American Business Law Journal
Am. Crim. L. Rev.	American Criminal Law Review
Am. J. Int´l L.	American Journal of International Law
Am. U. Int´l L. Rev.	American University International Law Review
Anh.	Anhang
Anm.	Anmerkung
AöR	Archiv für öffentliches Recht
APT	Archiv für Post und Telekommunikation
Ark. L. Rev.	Arkansas Law Review
Art.	Artikel
Aufl.	Auflage
BAG	Bundesarbeitgericht
BB	Betriebsberater

BayVBl.	Bayerische Verwaltungsblätter
BDSG	Bundesdatenschutzgesetz
Berkeley Tech. L. J.	Berkeley Technology Law Journal
BFH	Bundesfinanzhof
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BNA	Bureau of National Affairs, Inc., (hier: Ausgabe Electronic Commerce & Law)
BR-Drs.	Bundesratsdrucksache
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des BVerfG
BVerfGG	Bundesverfassungsgerichtsgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des BVerwG
Cal.	California Reports (Entscheidungssammlung)
Cal. App.	California Appelate Reports (Entscheidungssammlung)
Cal. L. Rev.	California Law Review
Cal. Rptr.	West´s California Reporter (Entscheidungssammlung)
CAN-SPAM Act	Controlling the Assault of Non-Solicited Pornography and Marketing Act
Cath. U.L. Rev.	Catholic University Law Review
CML Rev.	Common Market Law Review
CR	Computer und Recht
DÖV	Die öffentliche Verwaltung

DSRL	Datenschutzrichtlinie
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
ECHR	The European Convention on Human Rights
ECPA	Electronic Communications Privacy Act
ECRL	E-Commerce-Richtlinie
E.D.	Eastern District
EG	Europäische Gemeinschaften
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der EG
Einf.	Einführung
Einl.	Einleitung
EK-DSRL	Datenschutzrichtlinie für Elektronische Kommunikation
EKMR	Europäische Kommission für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EuG	Gericht erster Instanz
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte Zeitschrift
EuR	Europarecht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht

EWR	Europäischer Wirtschaftsraum
F., F.2d, F.3d	Federal Reporter (Entscheidungssammlung US-Bundesgerichte)
FARL	Fernabsatzrichtlinie
FAZ	Frankfurter Allgemeine Zeitung
Fed. Comm. L. J.	Federal Communications Law Journal
Fordham Int´l L. J.	Fordham International Law Journal
Form.	Formular
F. Supp., F. Supp.2d	Federal Supplement (Entscheidungssammlung US-Bundesgerichte)
FTC	Federal Trade Commission
G 10	Artikel 10-Gesetz, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
Geo. Wash. L. Rev	George Washington Law Review
GG	Grundgesetz
GRC	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
Harv. Int´l L.J.	Harvard International Law Journal
Harv. L. Rev.	Harvard International Law Journal
HdStR	Handbuch des Staatsrechts
h.L.	herrschende Lehre
h.M.	herrschende Meinung

IPbürgPR	Internationale Pakt über bürgerliche und politische Rechte
IuR	Informatik und Recht
J. Marshall J. Computer & Info. L.	John Marshall Journal of Computer and Information Law
J. Small & Emerging Bus. L.	Journal of Small and Emerging Business Law
Jura	Juristische Ausbildung
Jurimetrics J.	Jurimetrics Journal
JuS	Juristische Schulung
JZ	Juristenzeitung
Kap.	Kapitel
K&R	Kommunikation und Recht
L.Ed.	Lawyer´s Edition (Entscheidungssammlung US-Supreme Court)
LG	Landgericht
L. Rev.	Law Review
L. J.	Law Journal
MDR	Monatsschrift für deutsches Recht
MDStV	Mediendienste-Staatsvertrag
Misc.	New York Miscellaneous Reports
M.J.	Military Journal (Entscheidungssammlung)
MMR	Multimedia und Recht
N.E., N.E. 2d	North Eastern Reporter (Entscheidungssammlung)
N. Eng. L. Rev.	New England Law Review
NJW	Neue Juristische Wochenschrift

NJW-CoR	Neue Juristische Wochenschrift - Computerrecht
NJW-RR	Neue Juristische Wochenschrift-Rechtsprechungsreport
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
N.W., N.W. 2d	North Western Reporter (Entscheidungssammlung)
N.Y.	New York Reports (Entscheidungssammlung)
N. Y. S. 2d	West´s New York Supplement (Entscheidungssammlung)
NZA	Neue Zeitschrift für Arbeitsrecht
OECD	Organization for Economic Cooperation and Development
OLG	Oberlandesgericht
P., P. 2d	Pacific Reporter (Entscheidungssammlung)
PC	Personal Computer
PLI/Pat	Practising Law Institute. Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series
Pub. L.	Public Law
RDV	Recht der Datenverarbeitung (Entscheidungssammlung)
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Request for Comment (Serie von Dokumenten die verschiedene Gewohnheiten und Standards im Internet beschreibt)
RIW	Recht der Internationalen Wirtschaft
Rn.	Randnummer

Rs.	Rechtssache
Rspr.	Rechtsprechung
S.	Seite
S. Ct.	Supreme Court Reporter (Entscheidungssammlung U.S. Supreme Court)
S. D.	Southern District
S.E.	South Eastern Reporter (Entscheidungssammlung)
Slg.	Sammlung der Rechtsprechung des Gerichtshofes
So.	Southern Reporter (Entscheidungssammlung)
SMU L.Rev.	Southern Methodist Law Review
S. REP.	U.S. Senate Report
st. Rspr.	ständige Rechtsprechung
Stan. L. Rev.	Stanford Law Review
StGB	Strafgesetzbuch
Stan. J. Int´l L.	Stanford Journal of International Law
S.W.	South Western Reporter (Entscheidungssammlung)
TDG	Teledienstegesetz
TDDSG	Gesetz über den Datenschutz bei Telediensten
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
U. Ill. L. Rev.	University of Illinois Law Review
Unix	ursprünglich UNICS für Uniplexed Information and Computing System (Bezeichnung für ein Betriebssystem)

U.S.	United States Reports (Entscheidungssammlung)
U.S.C.	United States Codes
U.S.C.A.	United States Codes Annotated (Kommentierte Textsammlung der US-Bundesgesetze)
U.S.C.C.A.N.	U.S. Code Congressional & Administrative News
UWG	Gesetz gegen den unlauteren Wettbewerb
Vand. J. Ent. L. & Prac.	Vanderbilt Journal of Entertainment Law & Practice
verb. Rs.	verbundene Rechtssachen
Vill. L. Rev.	Villanova Law Review
Vorbem.	Vorbemerkungen
VVDStRL	Veröffentlichungen der Vereinigung der deutschen Staatsrechtler
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WRP	Wettbewerb in Recht und Praxis
WÜV	Wiener Vertragsrechtskonvention
Yale L. J.	Yale Law Journal
ZfDG	Zollfahndungsdienstgesetz
Ziff.	Ziffer
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber und Medienrecht

Einleitung

Das Kommunikationsmedium Email wird von Millionen Menschen weltweit genutzt. Sowohl aus dem privaten Bereich, wie auch aus dem Geschäftsleben ist die elektronische Post nicht mehr wegzudenken. Vorzüge der Kommunikation per Email gegenüber der traditionellen Briefpost oder Telefax sind vor allem die distanzunabhängige Geschwindigkeit und Kostengünstigkeit des Versands sowie die Möglichkeit, Nachrichten jederzeit weltweit von jedem Internetanschluss aus abrufen zu können.

Allerdings hat auch die Werbewirtschaft das Medium für sich entdeckt. Durch das Aufkommen an elektronischen Werbe-Nachrichten entstehen einerseits Kosten für den Empfänger und die Email-Service-Provider, andererseits resultieren die Emails in einer Belastung des Netzwerks, wodurch die Geschwindigkeit des Datenstroms und damit die Funktionstüchtigkeit des Internet als Ganzes beeinträchtigt werden. Hinzu kommt der Zeitaufwand, den Email-Nutzer täglich für das Aussortieren der unverlangten Nachrichten aufwenden müssen. Für die Versender kommerzieller Emails ist das Medium hingegen aufgrund des geringen Kostenaufwands und der Möglichkeit, eine einmal erstellte Werbebotschaft millionenfach ohne zusätzliche Kosten zu versenden, äußerst attraktiv. Folglich ist ein stetiger Anstieg des Aufkommens an solchen Nachrichten zu verzeichnen.
Um die störungsfreie Email-Kommunikation auch in Zukunft zu gewährleisten, wurde deshalb in den letzten Jahren Filtersoftware entwickelt, die dazu dient, unerwünschte kommerzielle elektronische Nachrichten abzuwehren. Der Einsatz solcher Software erfolgt entweder beim Email-Service-Provider selbst oder beim Kunden. Dabei ist ihre Verwendung durch die Diensteanbieter rechtlich problematisch. Die Filterprogramme überprüfen die in den betroffenen Emails enthaltenen Daten und Informationen. Wird die Nachricht als kommerzielle Email identifiziert, so verfährt die eingesetzte Software je nach Einstellung dergestalt, dass sie die Nachricht blockiert, löscht, entsprechend markiert oder in einen speziellen Quarantäne-Ordner in der Mailbox des Empfängers umleitet.
Gegenstand der Arbeit ist die Frage nach der rechtlichen Zulässigkeit der verschiedenen Maßnahmen, die der Filtereinsatz zum Zweck der automatisierten Identifizierung und Abwehr unverlangter elektronischer Werbenachrichten mit sich bringt. Da zahlreiche US-amerikanische Unternehmen Filtersoftware entwickeln, soll hier neben der deutschen auch die Rechtslage in den USA beleuchtet werden.

Um ein Verständnis der Vorgänge zu ermöglichen, die bei dem Einsatz von Filtersoftware stattfinden, wird in Kapitel 1 zunächst ein Einblick in die Terminologie und technischen Grundlagen in Bezug auf das Internet, das Kommunikationsmedium der elektronischen Post sowie die Funktionsweise von Spamfiltersoftware gegeben.

Im Rahmen der Frage nach der rechtlichen Beurteilung des Einsatzes der Filtersoftware ist von Bedeutung, ob bzw. unter welchen Voraussetzungen die abzuwehrenden Werbe-Emails als zulässig anzusehen sind. Die im Raum stehenden Filtermethoden stellen die Reaktion auf das Versenden unverlangter kommerzieller Emails dar. Die Widerrechtlichkeit der abgewehrten Nachrichten könnte folglich mögliche Abwehrmaßnahmen rechtfertigen. Deshalb soll in Kapitel 2 Teil 1 dieser Arbeit darauf eingegangen werden, ob bzw. unter welchen Voraussetzungen der Versand solcher Emails nach Maßgabe des deutschen Rechts als rechtmäßig anzusehen ist. Kapitel 2 Teil 2 behandelt einerseits die Frage nach der Zulässigkeit der Überprüfung von Inhalt und Headerinformationen eingehender Emails durch die zur Filterung eingesetzte Software nach deutschem Recht. Andererseits wird dargestellt, ob als kommerzielle Emails identifizierte Nachrichten blockiert, gelöscht, durch Hinzufügen

einer zusätzlichen Headerzeile oder Veränderung der Subjekt-Zeile markiert oder in spezielle Ordner umgeleitet werden dürfen.

Im dritten Kapitel wird die Rechtslage in den USA beleuchtet. Auch hier stellt sich einerseits die Frage nach der Zulässigkeit kommerzieller Emails. Sie wird in Kapitel 3 Teil 1 beantwortet.
Andererseits ist zu klären, ob die mit dem Einsatz von Spamfiltern verbundene Überprüfung von in der Email enthaltenen Daten und Informationen sowie das weitere Vorgehen in Bezug auf als kommerzielle Emails identifizierte Nachrichten als rechtmäßig anzusehen ist. Hierauf wird in Kapitel 3 Teil 2 der Arbeit eingegangen.

Eine weitere Bedrohung des Kommunikationsmediums Email resultiert daraus, dass diese unter Umständen mit Computerviren infiziert sind. Diese können beim Empfänger Störungen auslösen, zum Verlust von Daten führen, im schlimmsten Fall die Festplatte des Rechners völlig neu formatieren sowie das System des Providers beschädigen. Auch zum Schutz vor Viren wird Filtersoftware eingesetzt. In Kapitel 4 dieser Arbeit wird kurz in einem Exkurs darauf eingegangen, wie der Einsatz von Virenfiltersoftware nach deutschem und US-amerikanischem Recht zu beurteilen ist.

In Kapitel 5 werden die in den beiden Rechtsordnungen getroffenen Regelungen miteinander verglichen. Dabei wird jeweils zunächst auf die Unterschiede und Gemeinsamkeiten der verschiedenen Vorschriften eingegangen, sodann auf die Gründe, die hierfür verantwortlich sind. Im Anschluss erfolgt eine wertende Gegenüberstellung der unterschiedlichen Lösungen und der dadurch erzielten tatsächlichen Folgen. Schließlich wird dargestellt, welche rechtspolitischen Folgerungen sich aus dem Vergleich der beiden Rechtsordnungen ergeben.

1. Kapitel: Terminologie, technische Grundlagen und Funktionsweise von Spam-Filtern

Im Folgenden werden die für das Verständnis der Arbeit relevante Terminologie, die technischen Grundlagen (Teil 1) sowie die Funktionsweise von Spam-Filtern (Teil 2) dargestellt.

Teil 1: Terminologie und technische Grundlagen

In diesem Teil wird auf die Terminologie und die technischen Grundlagen zunächst in Bezug auf das Internet (A.) und anschließend speziell für den Bereich der elektronischen Post (B.) eingegangen.

A. Das Internet - Beteiligte und Terminologie

Das Internet ist das weltweit größte Computernetzwerk, das aus vielen miteinander verbundenen lokalen und nationalen Netzwerken besteht und auf Grundlage des so genannten *Transport Control Protocol/Internet Protocol (TCP/IP)* funktioniert.[1] Hierbei existiert keine zentrale Steuerung, vielmehr ist jedes Teilnetz technisch und organisatorisch unabhängig.[2] Neben internen sowie externen Netzwerken ist das Internet einer der Hauptübertragungswege für Email.[3]

I. Technische Grundlagen und Terminologie

Nachfolgend werden die für das Verständnis der Arbeit erforderlichen Begriffe und technischen Grundlagen dargestellt.

1. Server und Client

Computer, die im Internet einen Dienst anbieten, werden *Server* genannt, solche, die einen Dienst in Anspruch nehmen, *Client*.[4]

2. OSI-Schichten-/Referenzmodell

Das *OSI-Schichten-/Referenzmodell* ist ein Modell für die Architektur von Rechnernetzen, das aus sieben Schichten besteht und festlegt, welche Protokolle und Dienste in den einzelnen Schichten verwendet werden können.[5] Die Abkürzung OSI steht für „**O**pen **S**ystems **I**nterconnection“, das bedeutet „Verbindung offener Systeme“.[6] Dem OSI-Schichtenmodell liegt die Unterteilung der Netzwerkkommunikation in übereinander geordnete Schichten

---

[1] *Art. 29 Datenschutzgruppe*, WP 37, S. 4; *Brockhaus*, Stichwort „Internet“; *Eckert*, S. 84 f.; *IETF*, RFC 2026, a.a.O.; *Irlbeck*, Stichwort „Internet“; *Klußmann*, Stichwort „Internet“; *Lipinski*, Stichwort „Internet“

[2] *Art. 29 Datenschutzgruppe*, WP 37, S. 4; *Brockhaus*, Stichwort „Internet“; *Eckert*, S. 76; *Lipinski*, Stichwort „Internet“

[3] *Brockhaus*, Stichwort „E- Mail“; *Eckert*, S. 135; *Lipinski*, Stichwort „E- Mail, Electronic Mail (Elektronische Post)“; *Rojas*, Stichwort „Electronic Mail“

[4] *Art. 29 Datenschutzgruppe*, WP 37, S. 6; *Brockhaus*, Stichwörter „Client“, „Server“; *Klußmann*, Stichwort „Server“; *Lipinski*, Stichwörter „Client“, „Server“;

[5] *Brockhaus*, Stichwort „OSI- Schichtenmodell“; *Irlbeck*, Stichwort „OSI- Schichtenmodell“; *Klußmann*, Stichwort „IP“

[6] *Brockhaus*, Stichwort „OSI- Schichtenmodell“; *Klußmann*, Stichwort „OSI- Referenzmodell“; *Rojas*, Stichwort „Open Systems Interconnection Reference Model“

zugrunde.[7] Dabei stellt jede Schicht bestimmte Dienstleistungen zur Verfügung, die der darüber liegenden Schicht angeboten und auf Grundlage darunter liegender Schichten erbracht werden.[8] Es übernimmt somit jede Ebene einen Teil der Kommunikationsaufgabe, die erst in der obersten Schicht vollständig abgeschlossen ist.[9]
Man unterscheidet die folgenden Schichten:[10]

Anwendersystem
Schicht 7: **Anwendungsschicht** (Application Layer)
Ausführung von Programmen
Schicht 6: **Darstellungsschicht** (Presentation Layer)
Benutzer- und geräteunabhängige Kommunikation
Schicht 5: **Kommunikationssteuerungsschicht** (Session Layer)
Logische Verbindung zwischen den Kommunikationspartnern
Transportsystem
Schicht 4: **Transportschicht** (Transport Layer)
Festlegen der für die Datenübertragung erforderlichen Funktionen
Schicht 3: **Vermittlungsschicht** (Network Layer)
Vermittlung und Aufbau des Übertragungswegs
Schicht 2: **Sicherungsschicht** (Data-Link Layer)
Gesicherte Übertragung auf einzelne Teilstrecken
Schicht 1: **Bitübertragungsschicht** (Physical Layer)
Festlegung des physikalischen Übertragungswegs

3. IP- und TCP Protokoll; IP- und Domain-Adressen

Das *Internet Protocol (IP-Protokoll)* entspricht der dritten Schicht des OSI-Referenzmodells.[11] Es spielt eine Vermittlerrolle zwischen der Transportschicht und den physikalischen Schichten und leistet verschiedene Dienste, die es den höheren Schichten zur Verfügung stellt.[12] Es teilt unter anderem die zu übermittelnden Daten in einzelne Pakete auf, wobei jedes Paket nicht nur die eigentlichen Nutzdaten beinhaltet, sondern auch einen Header, der Verwaltungsdaten enthält.[13] Nutzdaten sind dabei diejenigen Daten eines Datenpaktes, die keine Auswirkungen auf seine Steuerung oder Interpretation haben, die also allein der Information dienen.[14] Im Gegensatz dazu werden unter dem Begriff der Verwaltungsdaten allgemein solche Informationen verstanden, die unabhängig von den Abfragedaten angelegt und gespeichert werden, so etwa im Bereich der Email-

[7] *Brockhaus*, Stichwort „OSI- Schichtenmodell"; *Irlbeck*, Stichwort „OSI- Schichtenmodell"; *Klußmann*, Stichwort „OSI- Referenzmodell"; *Lipinski*, Stichwort „OSI- Referenzmodell (OSI Reference Modell)"; *Rojas*, Stichwort „Open Systems Interconnection Reference Model"
[8] *Brockhaus*, Stichwort „OSI- Schichtenmodell"; *Irlbeck*, Stichwort „OSI-Schichtenmodell"; *Klußmann*, Stichwort „OSI- Referenzmodell"; *Lipinski*, Stichwort „OSI- Referenzmodell (OSI Reference Model)
[9] *Brockhaus*, Stichwort „OSI-Schichtenmodell"; *Rojas*, Stichwort „Open Systems Interconnection Reference Model"
[10] *Irlbeck*, Stichwort „OSI-Schichtenmodell"; *Klußmann*, Stichwort „OSI- Referenzmodell"; *Lipinski*, Stichwort „OSI- Referenzmodell (OSI Reference Model); *Rojas*, Stichwort „Open Systems Interconnection Reference Model"
[11] *Brockhaus*, Stichwort „TCP/IP"; *Eckert*, S. 85; *Irlbeck*, Stichwort „TCP/IP"; *Lipinski*, Stichwort "IP, Internet Protocol (IP- Protokoll)"
[12] *Brockhaus*, Stichwort „TCP/IP"; *Eckert*, S. 85; *Irlbeck*, Stichwort „TCP/IP"; *Klußmann*, Stichwort „IP"; *Lipinski*, Stichwort "IP, Internet Protocol (IP- Protokoll)"
[13] *Brockhaus*, Stichwort „TCP/IP"; *Irlbeck*, Stichwort „TCP/IP"; *Klußmann*, Stichwort „IP"; *Lipinski*, Stichwort "IP, Internet Protocol (IP- Protokoll)"; *Rojas*, Stichwort "IP Address"
[14] *Brockhaus*, Stichwort „Nutzdaten"; *Klußmann*, Stichwort „Nutzdaten"; *Lipinski*, Stichwort „Nutzdaten"

Kommunikation Absender- sowie Empfängeradresse, Subjektzeile, Paketnummer, Senderkennung und Paketstatus.[15]

Die Abkürzung *TCP* steht für **T**ransmission **C**ontrol **P**rotocol.[16] Das *TCP* übernimmt die Aufgaben der vierten Schicht des OSI-Referenzmodells, indem es eine logische Verbindung zwischen Sender und Empfänger herstellt und dafür sorgt, dass die Daten korrekt und in der richtigen Reihenfolge über das Netz transportiert werden.[17] Es erkennt auch Datenverluste und veranlasst gegebenenfalls die Neuübertragung von Datenpaketen.[18] Die Datenübertragung in TCP/IP-Netzwerken geschieht dabei nicht dergestalt, dass zwischen den einzelnen miteinander kommunizierenden Rechnern eine Verbindung über eine Leitung hergestellt wird, vielmehr besteht eine rein virtuelle, so genannte logische Verbindung.[19] An der Übertragung der Datenpakete sind die so genannten *Router* entscheidend beteiligt. Router verbinden einzelne Teile des Netzwerks oder vollständige Netzwerke miteinander und steuern die Datenübertragung.[20]

Jeder einzelne mit dem Internet verbundene Computer wird durch eine einmalige so genannte *IP-Adressnummer*, auch *IP-Adresse*, in der Form A.B.C.D. identifiziert, wobei A, B, C und D Zahlen zwischen 0 und 255 sind, die jeweils durch einen Punkt voneinander getrennt sind, zum Beispiel „213.96.4.187".[21] Bisher sind für jede der vier Zahlen acht Bit reserviert, insgesamt also 32 Bit, womit sich etwa vier Milliarden Computer adressieren lassen.[22] Um eine größere Zahl an Adressierungsmöglichkeiten zu erhalten, werden die IP-Adressen in Zukunft auf Basis einer 128-Bit-Zahl vergeben werden, was dazu führt, dass 340 000 000 Quintillionen Rechner adressiert werden könnten.[23] Das entsprechende Protokoll wird *IP Next Generation* oder *IPv6* (Version Nr. 6) genannt, während die aktuellen Adressen zur *IPv4* gehören.[24]
Computer, die direkt mit dem Netzwerk verbunden sind, besitzen gewöhnlich eine feste, so genannte *statische IP-Adresse*, während den lediglich zeitweilig mit dem Internet verbundenen Rechnern so genannten *dynamische IP-Adressen* zugewiesen werden, die aus einem Pool momentan nicht genutzter Adressen entnommen werden, nach Verbindungstrennung jedoch wieder dorthin zurück wandern.[25] Mit der Umstellung auf das IPv6 können zukünftig alle Rechner, von denen aus Zugriff auf das Internet genommen wird mit einer eindeutigen statischen IP-Adresse ausgestattet werden.[26]
IP-Adressen werden in Europa mittels eines internationalen Verfahrens an Internet-Zugangsanbieter vergeben, die sie sodann ihren Kunden bereitstellen. Die Vergabe von IP-

---

[15] *Brockhaus*, Stichwort „Verwaltungsdaten"; *Klußmann*, Stichwort „Header"; *Lipinski*, Stichwort „Header"
[16] *Eckert,* S. 75; *IETF*, RFC 793; *Klußmann*, Stichwort „TCP";
[17] *Brockhaus*, Stichwort „TCP/IP"; *Eckert*, S. 88; *IETF*, RFC 793; *Irlbeck*, Stichwort „TCP/IP"; *Klußmann*, Stichwort „TCP"
[18] *Brockhaus*, Stichwort „TCP/IP"; *Eckert*, S. 88; *IETF*, RFC 793; *Irlbeck*, Stichwort „TCP/IP"; *Klußmann*, Stichwort „TCP"
[19] *Art. 29 Datenschutzgruppe*, WP 37, S. 5; *Klußmann*, Stichwort „TCP"; *Schaar*, Datenschutz im Internet, Rn. 7
[20] *Art. 29 Datenschutzgruppe*, WP 37, S. 5; *Brockhaus*, Stichwort „Router"; *Irlbeck*, Stichwort „Router"; *Lipinski*, Stichwort „Router"; *Rojas*, Stichwort „Router"
[21] *Eckert*, S. 86; *Klußmann*, Stichwort „IP"; *Rojas*, Stichwort „IP Address"
[22] *Brockhaus*, Stichwort „IP-Adresse"; *Eckert*, S. 86; *Irlbeck*, Stichwort „IP- Adresse"; *Lipinski*, Stichwort „IP-Adresse"; *Rojas*, Stichwort „IP Address"
[23] *Brockhaus*, Stichwort „IP-Adresse"; *Irlbeck*, Stichwort „IP- Adresse"; *Klußmann*, Stichwort „IP"; *Lipinski*, Stichwort „IP- Adresse"; *Rojas*, Stichwort „IP Address"
[24] *Brockhaus*, Stichwort „IP-Adresse"; *IETF*, RFC 1752, RFC 2460; *Irlbeck*, Stichwort „IP-Adresse"; *Lipinski*, Stichwort „IP-Adresse"; *Rojas*, Stichwort „IP Address"
[25] *Art. 29 Datenschutzgruppe*, WP 37, S. 4; *Bizer*, DuD 2003, S. 10; *Brockhaus*, Stichwort „IP-Adresse"; *BSI*, „Das Ende der Anonymität?, Abschn. 4; *Köhntopp/Köhntopp*, Datenspuren im Internet, S. 1; *Irlbeck*, Stichwort „IP-Adresse"; *Lipinski*, Stichwort „IP-Adresse";
[26] *Bizer*, DuD 2003, S. 10; *Schaar*, Datenschutz im Internet, Rn. 176

Adressen an Internet-Nutzer erfolgt durch den Verwalter eines mit dem Internet verbundenen lokalen Netzwerks, eines so genannten **L**ocal **A**rea **N**etwork (LAN) (a), durch einen Internet-Zugangsanbieter (b) oder durch den Inhaber eines Bereichsnamens bzw. einer Domain (c).[27]

a) Vergabe durch den Verwalter eines Local Area Network (LAN)

Unter dem Begriff Local Area Network sind lokale Netze mit einer Ausdehnung von 10 Metern bis hin zu 10 Kilometern zu verstehen, wobei eine Anzahl von lediglich zwei bis zu einigen hundert Stationen an das Netz angeschlossen sein können.[28] Local Area Networks sind beispielsweise Netze innerhalb einer Organisation, etwa einer Firma oder Universität, oder eines bestimmten Gebäudes, beispielsweise eines Bürokomplexes.[29]
LAN-Verwalter verwenden in der Regel ein festes Adressierschema und verwalten ein Verzeichnis der Entsprechungen zwischen den Computern der Teilnehmer und den IP-Adressen. Im Fall der dynamischen Vergabe der IP-Adressen führt der LAN-Verwalter ein Logbuch, anhand dessen die einzelnen Computer im Netzwerk identifiziert werden können.[30]

b) Vergabe durch einen Internet-Zugangsanbieter bzw. Access-Provider

Die Internet-Zugangsanbieter, auch Access-Provider genannt, treffen vertragliche Vereinbarungen mit den Internet-Teilnehmern. Hierfür ist die Angabe personenbezogener Daten, insbesondere des Namens und der Adresse des Nutzers erforderlich.[31] Der Internet-Zugangsanbieter führt ein Logbuch mit der zugewiesenen IP-Adresse, der Identität des Teilnehmers, dem Datum, der Dauer und dem Zeitpunkt der Adresszuweisung.[32] Durch die

---

[27] *Art. 29 Datenschutzgruppe*, S. 4; *Schaar*, Datenschutz im Internet, Rn. 172; *Wikipedia*, Stichwort „IP-Adresse“, a.a.O.
[28] *Irlbeck*, Stichwort „Lokales Netzwerk“; *Klußmann*, Stichwort „LAN“; *Lipinski*, Stichwort „LAN, Local Area Network (Lokales Netz)“; *Rojas*, Stichwort „Local Area Network“; *Wikipedia*, Stichwort „IP-Adresse“, a.a.O.
[29] *Brockhaus*, Stichwort „lokales Netzwerk“; *Klußmann*, Stichwort „LAN“; *Rojas*, Stichwort „Local Area Network“
[30] *Art. 29 Datenschutzgruppe*, WP 37, S. 4; *Schaar*, Datenschutz im Internet, Rn. 171 f.
[31] *Art. 29 Datenschutzgruppe*, WP 37, S. 7; vgl. etwa: *1 & 1* Datenschutzhinweise, (Erheben von Name, Anschrift, Email-Adresse und Bankverbindung, einsehbar unter: http://www.1und1.de (letzter Abruf: 29.04.2007); *Arcor*, Datenschutzhinweise, AGB und Downloads (Erheben von Adresse und anderen persönlichen Informationen; Hinweis, dass der Kunde nach der Registrierung für Arcor nicht mehr anonym ist), einsehbar unter: http://i.arcor.de/pdf/arcor/privat/preise_und_leistungen/arcor_pre_dsl_preise_leistungen.pdf (letzter Abruf: 29.04.2007) sowie http://www.arcor.de/hilfe/neu/index.php?sid=aktion=anzeigen&rubrik=010005001&id=49 (letzter Abruf: 29.04.2007); *AOL*, „Welche Daten erhebt AOL von AOL-Kunden zu welchem Zweck?“, (Erheben von Name, Anschrift, Bankverbindung), einsehbar unter: http://www.aol.de/index.jsp?cid=1255476409&pageId=3&sg=Poralkontakt_Datenschutz (letzter Abruf: 29.04.2007)
[32] *Art. 29 Datenschutzgruppe*, WP 37, S. 4; *BSI*, Das Ende der Anonymität?, Abschn. 4.2.; *Gnirck/Lichtenberg*, DuD 2004, 599; *Golembiewski* in Bäumler/von Mutius, S. 108; *Ruess/Patzak*, RDV 2003, 170; *Schuster* in Bäumler, S. 87; vgl. allerdings zu Löschungsverpflichtungen der Provider: LG Darmstadt, MMR 2006, 330 ff.; vgl. zu künftig gesetzlich durch die EU-Mitgliedstaaten anzuordnenden Speicherfristen: Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, Abl. EG 2006, L 105, S. 54 ff.; vgl. zur Speicherpraxis der Provider: *1& 1*, Datenschutzhinweise, (Speicherung von Datum und Uhrzeit sowie Zeitzone des Beginns und Endes der Nutzung, des Umfangs in Bytes, der Nutzer-IP-Adresse, der Art des in Anspruch genommenen Dienstes sowie für die Abrechnung erforderlicher Verbindungsdaten), abrufbar unter http://www.1und1.de (letzter Abruf: 29.04.2007); *AOL*, Datenschutzhinweise, (Speicherung für die Erbringung und Abrechnung erforderlicher Daten, so etwa genutzte Online-Zeit, IP-Adresse sowie übertragenes Datenvolumen), abrufbar unter: http://www.aol.de/index.jsp?cid=1255476409&pageId=3&sg=Portalkontakt_Datenschutz (letzter Abruf: 29.04.2007)

Richtlinie 2006/24/EG[33] besteht nun sogar eine Verpflichtung der Mitgliedstaaten, im Interesse der Prävention und Verfolgung von Straftaten[34] bis Ablauf der Umsetzungsfrist[35] sicherzustellen, dass Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste bestimmte Daten für einen Zeitraum von mindestens sechs Monaten bis zu höchstens zwei Jahren speichern.[36] Der Speicherpflicht unterliegen die zugewiesenen Benutzerkennungen von Absender und vorgesehenem Empfänger einer Email sowie die IP-Adresse des Absenders und die Namen und Anschriften der Teilnehmer oder registrierten Benutzer.[37] Auch der Zeitpunkt der An- und Abmeldung beim Email- oder Internetzugangsdienst sind vom Provider zusammen mit der zugewiesenen dynamischen oder statischen IP-Adresse bzw. Benutzerkennung zu speichern.[38] Schließlich sind auch die zur Bestimmung der Endeinrichtung erforderlichen Daten, so etwa Rufnummer des anrufenden Anschlusses oder des digitalen Teilnehmeranschlusses (DSL) festzuhalten.[39]

c) Vergabe durch den Inhaber eines Bereichsnamens bzw. einer Domain

Da sich die aus einer Reihe von Zahlen bestehenden IP-Adressen auf der Anwendungsebene nur schwer handhaben und einprägen lassen, wird über eine IP-Adresse identifizierten Computern über das so genannte Bereichsnamensystem DNS (**D**omain **N**ame **S**ystem) eine so genannte Domain-Adresse zugewiesen.[40] Solche Namen haben die Form <Name>.<übergeordneter Bereich>. Der übergeordnete Bereich ist dabei die Top-Level-Domain, der Name besteht dagegen in einer Zeichenfolge.[41] Eine *Domain*, deutsch Domäne, ist dabei eine Gruppe von Computern mit gemeinsamen Namensbestandteilen. Unterschieden werden Top-Level-Domains, zum Beispiel das Länderkürzel „de“ oder das Kürzel „com“ und Unter-Domains, die man Second-Level-Domains und Third-Level-Domains nennt.[42]

4. Der finger-Befehl, die Problematik der Selbstidentifikation des Nutzers und Cookies

Im Bereich des Datenschutzrechts wird die Frage Bedeutung gewinnen, inwieweit bestimmte Informationen einer individualisierbaren Person zuordenbar sind. Einige der Identifikation des Nutzers dienende Daten können durch den so genannten *finger-Befehl* vom Server des

---

[33] vgl. dazu: Fn. 32
[34] vgl.: Erwägungsgrund Nr. 7, Art. 1 Abs. 1 RL 2006/24/EG
[35] Die Richtlinie ist von den Mitgliedstaaten bis spätestens 15.09.2007 umzusetzen, Art. 15 Abs. 1 der Richtlinie, wobei bis 15.03.2009 jeder Mitgliedstaat die Anwendung der Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-Email aufschieben kann, Art. 15 Abs. 3 S. 1 der Richtlinie. Deutschland hat eine Erklärung dahingehend abgegeben, sich das Recht vorzubehalten, die Anwendung der Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-Email für einen Zeitraum von 18 Monaten ab dem in Art. 15 Abs. 1 S. 1 genannten Zeitpunkt zurückzustellen.
[36] Art. 3 Abs. 1 in Verbindung mit Art. 6 RL 2006/24/EG; zu verfassungsrechtlichen Bedenken im Hinblick auf die Richtlinie: *Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland*, DuD 2004, S. 603 ff. unter Verweis insbesondere auf das Volkszählungsurteil, BVerfGE 65, S. 1 ff., 43, BVerfGE 107, S. 299 ff., 321 sowie einen Verstoß gegen Art. 8 EMRK; *Westphal*, EuZW 2006, S. 555 ff.; zur Unzulässigkeit der Vorratsdatenspeicherung: BVerfG, MMR 2006, S. 531 ff.
[37] Art. 5 Abs. 1 lit. a) Nr. 2 i) und iii), Art. 5 Abs. 1 lit. b) Nr. 2 ii) 2006/24/EG
[38] Art. 5 Abs. 1 lit .c) Nr. 2 i) und ii) 2006/24/EG
[39] Art. 5 Abs. 1 lit. e) Nr. 3 i) und ii)
[40] *Art. 29 Datenschutzgruppe*, WP 37, S. 4 f.; *Eckert*, S. 86; *IETF*, RFC 1034, RFC 1035; *Irlbeck*, Stichwort „DNS“; *Klußmann*, Stichwort „Domain“; *Rojas*, Stichwort „Domain Name System“; *Wikipedia*, Stichwort „Domain-Name-System“, a.a.O.
[41] *Art. 29 Datenschutzgruppe*, WP 37, S. 4 f.; *Irlbeck*, Stichwort „DNS“; *Wikipedia*, Stichwort „Domain-Name-System“, a.a.O.
[42] *Brockhaus*, Stichwort „Domäne“; *Eckert*, S. 109; *Irlbeck*, Stichwort „DNS“; *Klußmann*, Stichwort „Domain“

Internet-Access- oder -Service-Providers heruntergeladen werden (a).[43] Daneben nimmt der Nutzer bisweilen selbst die Zuordnung zu einer zunächst faktisch anonymen IP-Adresse vor, und zwar häufig, ohne sich dessen bewusst zu sein (b).[44] Durch den Einsatz so genannter *Cookies* lassen sich Rückschlüsse auf bestimmte Gewohnheiten des jeweiligen Nutzers ziehen (c), die unter Heranziehung weiterer Informationen einer bestimmten Person zugeordnet werden können.[45]

a) Der finger-Befehl

Viele Internet-Provider verwenden das Betriebssystem Unix als Basisplattform für ihr Dienstangebot.[46] Auf Unix-Systemen werden Benutzerinformationen wie Login- und Benutzernamen, Anmeldezeitpunkt sowie das Terminal, von dem sich der Benutzer angemeldet hat, in einer Datei namens „passwd" gespeichert.[47] Mit dem Befehl „finger" kann sich grundsätzlich jedermann diese Informationen besorgen.[48]

b) Selbstidentifikation

Daneben kommt es häufig dazu, dass ein Nutzer, der zunächst an sich faktisch anonym im Internet agiert, selbst die Zuordnung bestimmter Daten zu seiner Person vornimmt, ohne dass er sich dessen notwendigerweise bewusst ist.[49] Beispielsweise erfolgt eine Selbstidentifikation des Nutzers, wenn dieser im Rahmen einer Anfrage oder Bestellung einem Diensteanbieter personenbezogene Angaben mitteilt, so etwa durch Ausfüllen eines Formulars.[50]
Teilweise wird der Nutzer durch den Browser identifiziert; einige ältere Browser lassen sich durch eine „http_from"-Anfrage dazu bewegen, die Email-Adresse des Nutzers automatisch an den anfragenden Server zu übermitteln.[51]

c) Cookies

Der Einsatz von Cookies ermöglicht es, ein Profil des jeweiligen Nutzers zu erstellen.[52] Unter einem Cookie wird eine kleine Datei verstanden, die beim Surfen im Internet auf Veranlassung einer besuchten Seite auf der Festplatte des Besuchers gespeichert wird.[53] Das Setzen eines Cookies geschieht dadurch, dass beim erstmaligen Besuch einer Web-Seite der Web-Server, über den die Internetverbindung läuft, die Benutzerdaten empfängt und sie an

---

[43] *BSI*, Das Ende der Anonymität?, a.a.O., Abschn. 4.4.
[44] *Bizer*, DuD 2003, S. 10
[45] *Art. 29 Datenschutzgruppe*, WP 37, S. 17; *BSI,* Das Ende der Anonymität? Abschn. 4.3.; *Eichler*, K & R 1999, S. 78; *Ihde*, CR 2000, S. 421; *Irlbeck*, Stichwort „Cookie"; *Klußmann*, Stichwort „Cookie"; *Lipinski*, Stichwort „Cookie"; *Schaar*, Datenschutz im Internet, Rn. 697
[46] *BSI*, Das Ende der Anonymität?, a.a.O., Abschn. 4.4.
[47] *BSI*, Das Ende der Anonymität?, a.a.O., Abschn. 4.4.; *Wikipedia*, Stichwort „Finger (Internetprotokoll)", a.a.O.
[48] *BSI*, Das Ende der Anonymität?, a.a.O., Abschn. 4.4.; *Eckert*, S. 140; *IETF*, RFC 1288; *Wikipedia*, Stichwort „Finger (Internetprotokoll)", a.a.O.
[49] *Bizer*, DuD 2003, S. 10; *Roessler* in Bäumler, S. 208 f.
[50] *Bizer*, DuD 2003, S. 10; *Roessler* in Bäumler, 208 f.
[51] *Spiegel*, DuD 2003, S. 266
[52] *BSI*, Das Ende der Anonymität?, a.a.O., Abschn. 4.3.; *Eichler*, K & R 1999, S. 78; *Ihde*, CR 2000, S. 421; *Irlbeck*, Stichwort „Cookie"; *Klußmann*, Stichwort „Cookie"; *Lipinski*, Stichwort „Cookie"; *Roessler* in Bäumler, S. 207 f.; *Schaar*, Datenschutz im Internet, Rn. 697; *Spiegel*, DuD 2003, S. 266
[53] *BSI*, Das Ende der Anonymität?, a.a.O., Abschn. 4.3.; *Eichler*, K & R 1999, S. 78; *Ihde*, CR 2000, S. 421; *Irlbeck*, Stichwort „Cookie"; *Klußmann*, Stichwort „Cookie"; *Lipinski*, Stichwort „Cookie; *Schaar*, Datenschutz im Internet, Rn. 697; *Spiegel*, DuD 2003, S. 266

den Web-Browser, das Navigationsprogramm für das Internet, schickt, wo sie als kleine Textdatei gespeichert werden.[54] Ruft der Nutzer später die Seite erneut auf, so wird der Cookie an den Web-Server zurückgesandt, von diesem ausgewertet, möglicherweise verändert und wieder an den Web-Browser übertragen.[55] So kann die entsprechende Web-Seite in Zukunft erkennen, dass sie von dem betroffenen Nutzer bereits zuvor besucht wurde.[56]

Mittels des so genannten *Data-Mining,* das bedeutet der Anwendung mathematischer Methoden auf einen Datenbestand mit dem Ziel der Mustererkennung, können so durch den Einsatz künstlicher Intelligenz und mathematischer Statistik die Vorlieben, Bedürfnisse und Kaufgewohnheiten einzelner Verbraucher prognostiziert werden.[57] Dabei ist das Nutzerprofil um so genauer, um so mehr Cookies sich auf der Festplatte des Nutzers befinden.[58] Mittels Cookies ist es möglich, bestimmte Nutzer auch bei wechselnden IP-Adressen wiederzuerkennen und ihr Profil zu erstellen.[59] Mittlerweile ermöglichen so genannte Clickstream-Techniken es sogar, das gesamte Klickverhalten eines Internet-Nutzers aufzuzeichnen.[60]

II. Akteure im Internet

Bei der Kommunikation im Internet sind mehrere Akteure beteiligt, welche die im Folgenden genannten Aufgaben wahrnehmen.

1. Carrier

Der Begriff *Carrier* bezeichnet den Betreiber eines Telekommunikationsdienstes und wird synonym mit der Bezeichnung *Netzbetreiber* verwendet.[61] Der Carrier stellt die technische Basis für Verbindungen zwischen verschiedenen Rechnern zur Verfügung, die im Internet kommunizieren.[62] Carrier sind beispielsweise die Deutsche Telekom[63] oder Arcor.[64]

2. Internet-Access-Provider

Internet-Access-Provider (IAP) ermöglichen den Zugang zum Netz, indem sie Zugangsknoten bereithalten, die von den Nutzern aus öffentlichen Telekommunikationsnetzen angewählt werden können.[65] Sobald eine Verbindung zwischen dem Nutzer und einem Zugangsknoten

---

[54] *Eichler*, K & R 1999, S. 78; *Ihde*, CR 2000, S. 421; *Klußmann*, Stichwort „Cookie"; *Lipinski*, Stichwort „Cookie"; *Schaar*, Datenschutz im Internet, Rn. 697;
[55] *Brockhaus*, Stichworte „Browser", „Cookie"; *Ihde*, CR 2000, S. 414; *Klußmann*, Stichwort „Cookie"; *Lipinski*, Stichworte „Browser", „Cookie"
[56] *Brockhaus*, Stichworte „Browser", „Cookie"; *Ihde*, CR 2000, S. 414; *Klußmann*, Stichwort „Cookie"; *Lipinski*, Stichworte „Browser", „Cookie"
[57] *Brockhaus*, Stichwort „Datenfilterung"; *Schaar*, Datenschutz im Internet, Rn. 699; *Wikipedia*, Stichwort „Data-Mining", a.a.O.
[58] *Spiegel*, DuD 2003, S. 266
[59] *Ruess/Patzak*, RDV 2003, S. 170
[60] *Spiegel*, DuD 2003, S. 266 ff.; *J. Weber*, DuD 2003, S. 626; *Wiese* in Bäumler, S. 12
[61] *Art. 29 Datenschutzgruppe*, WP 37, S. 7; *Brockhaus*, Stichwort „Carrier"; Rn. 20 f.; *Klußmann*, Stichwort „Carrier"; *Schaar*, Datenschutz im Internet, Rn. 20 f.
[62] *Art. 29 Datenschutzgruppe*, WP 37, S. 7; *Brockhaus*, Stichwort „Carrier"; *Schaar*, Datenschutz im Internet, Rn. 20 f.
[63] Homepage einsehbar unter: http://www.telekom3.de (letzter Abruf: 29.04.2007)
[64] Homepage einsehbar unter: http://www.arcor.de (letzter Abruf: 29.04.2007)
[65] *Brockhaus*, Stichwort „Internet- Provider"; *Irlbeck*, Stichwort „Internet- Provider"; *Klußmann*, Stichwort „ISP"; *Lipinski*, Stichwort „ISP (Internet Service Provider)"; *Rojas*, Stichwort „Internet Service Providers"

aufgebaut ist, stellt der Internet-Access-Provider auf Basis des *TCP/IP* eine logische Verbindung zum Internet her und weist dem Nutzer eine *IP-Adresse* zu.[66] So kann sich der Nutzer über eine Software, die der Provider in der Regel mitliefert, beim Zugangsknoten des Providers, dem so genannten *POP* einwählen. Der POP ist per Standleitung mit dem Internet verbunden.[67] Einzelpersonen wählen sich mittels ISDN, dem Integrated Services Digital Network,[68] oder eines Modems in das Internet ein.[69] Dabei erhalten sie eine dynamische oder statische IP-Adresse.[70] Um eine Verbindung herstellen zu können, müssen die Teilnehmer einen Vertrag mit dem Internet-Access-Provider abschließen und zwar auch dann, wenn die Teilnahme kostenfrei ist.[71]

Hierfür ist die Angabe personenbezogener Daten, insbesondere des Namens und der Adresse erforderlich.[72] Wie oben bereits ausgeführt wurde halten Internet-Access-Provider Datum, Zeitpunkt und Dauer der Zuweisung der betreffenden IP-Adresse in einem Protokoll fest.[73] Beispiele für Internet-Zugangsanbieter sind die T-Online[74], AOL[75], Arcor[76] und 1&1.[77]

3. Internet-Service-Provider

Unter der Bezeichnung *Internet-Service-Provider (ISP)*, deutsch Internet-Diensteanbieter, werden Anbieter verschiedener Dienste zusammengefasst. Internet-Service-Provider bieten Einzelpersonen oder Unternehmen Dienstleistungen an.[78] Sie besitzen oder mieten TCP/IP-Verbindungen und nutzen Server, die ständig mit dem Internet verbunden sind.[79] Ein typischer von ISP erbrachter Dienst ist *Email*, die elektronische Post.[80]
Häufig übernehmen Internet-Access-Provider auch die Funktion eines Internet-Service-Providers. Aus diesem Grund wird der Begriff ISP häufig verwendet, um sowohl Zugangs- als

---

[66] *Brockhaus*, Stichwort „Internet- Provider"; *Irlbeck*, Stichwort „Internet- Provider"; *Lipinski*, Stichwort „ISP (Internet Service Provider)"
[67] *Brockhaus*, Stichwort „Internet- Provider"; *Irlbeck*, Stichwort „Internet- Provider"; *Lipinski*, Stichwort „ISP (Internet Service Provider)"
[68] *Brockhaus*, Stichwort „ISDN"; *Klußmann*, Stichwort „ISDN"; *Lipinski*, Stichwort „ISDN"
[69] *Art. 29 Datenschutzgruppe*, WP 37, S. 7
[70] vgl.: 1. Kap. Teil 1 A. I. 3.
[71] *Art. 29 Datenschutzgruppe*, WP 37, S. 7
[72] *Art. 29 Datenschutzgruppe*, WP 37, S. 7; vgl. zur Praxis der Erhebung von Daten durch Provider: *1&1*, Datenschutzhinweise, (Erhebung von Name, Anschrift, Email-Adresse und Bankverbindung) abrufbar unter: http://www.1und1.de (letzter Abruf: 29.04.2007); *AOL*, Datenschutzhinweise, (Erheben von Name, Anschrift, Bankverbindung), abrufbar unter: http://www.aol.de/index.jsp?cid=1255476409&pageId=3&sg=Poralkontakt_Datenschutz (letzter Abruf: 29.04.2007); *Arcor*, Datenschutzhinweise, (Erheben von Name, Adresse und anderen persönlichen Informationen des Kunden und Speicherung dieser Informationen; Hinweis, dass nach Registrierung bei Arcor keine Anonymität mehr besteht), abrufbar unter: http://www.arcor.de/hilfe/neu/index.php?sid=aktion=anzeigen&rubrik=010005001&id=49 (letzter Abruf: 29.04.2007)
[73] vgl.: 1. Kap. Teil 1 A. I. 3. b)
[74] Homepage einsehbar unter: http://www.t-online.de (letzter Abruf: 29.04.2007)
[75] Homepage einsehbar unter: http://www.aol.com (letzter Abruf: 29.04.2007)
[76] Homepage einsehbar unter: http://www.arcor.de (letzter Abruf: 29.04.2007)
[77] Homepage einsehbar unter: http://www.1und1.de (letzter Abruf: 29.04.2007)
[78] *Art. 29 Datenschutzgruppe*, WP 37, S. 8; *Klußmann*, Stichwort „ISP"; *Schaar*, Datenschutz im Internet, Rn. 25 f.; *Wikipedia*, Stichwort „Internetdienstanbieter", a.a.O.
[79] *Art. 29 Datenschutzgruppe*, WP 37, S. 8; *Klußmann*, Stichwort „ISP"; *Schaar*, Datenschutz im Internet, Rn. 25 f.; *Wikipedia*, Stichwort „Internetdienstanbieter", a.a.O.
[80] *Art. 29 Datenschutzgruppe*, WP 37, S. 8; *Schaar*, Datenschutz im Internet, Rn. 25 f.; *Wikipedia*, Stichwort „Internetdienstanbieter", a.a.O.

auch Diensteanbieter zu bezeichnen. Konzeptionell gesehen handelt es sich aber um unterschiedliche Aufgaben.[81]

4. Nutzer

Nutzer sind diejenigen Personen, die im Internet angebotene Dienste in Anspruch nehmen. Der Nutzer wird üblicherweise Kunde eines Carriers sein, es sei denn, er wählt sich von einem fremden Anschluss, zum Beispiel von einem Hotel aus, in das Internet ein.[82] Dabei ist zu beachten, dass selbst in den Fällen, in denen der Teilnehmer eine falsche Identität oder die Identität eines anderen Nutzers angibt, unter Heranziehung des Logbuchs des Internet Access Providers stets der eigentliche Nutzer über den zur Einwahl benutzten Rechner ermittelt werden kann.[83] Entsprechendes gilt für Nutzer, die sich über ein LAN einwählen.[84]

B. Elektronische Post

Die *Elektronische Post (Email)* ist derzeit der wichtigste Dienst zur Individualkommunikation über das Netz.[85]

I. Akteure und Funktionsweise

Am Vorgang des Versendens einer elektronischen Nachricht sind mehrere Akteure beteiligt und zwar der Absender, der Empfänger und der Email-Diensteanbieter.[86] Ein Teilnehmer, der eine Email versenden möchte, benötigt ein so genanntes Email-Client-Programm, das auf seinem Rechner installiert ist, daneben eine Email-Adresse und eine Verbindung zum Internet.[87] Als Beispiele für Email-Client-Programme sind etwa Eudora,[88] Pegasus,[89] sowie Outlook[90] zu nennen.[91] Dabei ist es beim Vertragsschluss mit dem Email-Service-Provider in aller Regel erforderlich, bestimmte Daten, wie den Namen oder die geschäftliche Adresse anzugeben.[92]

Möchte der Nutzer eine Nachricht versenden, schreibt er den entsprechenden Text in sein Email-Client-Programm und füllt das Adressfeld mit der Email-Adresse des Empfängers

---

[81] *Art. 29 Datenschutzgruppe*, WP 37, S. 8; *Brockhaus*, Stichwort „Internet- Provider"; *Lipinski*, Stichwort „Provider"; *Stadler* in Hoeren/Sieber, Handbuch Multimediarecht, 12.1, Rn. 44
[82] *Art. 29 Datenschutzgruppe*, WP 37, S. 8 f.; *Schaar*, Datenschutz im Internet, Rn. 29 f.
[83] *Art. 29 Datenschutzgruppe*, WP 37, S. 8 f.; *Dammann* in Simitis, § 3 BDSG, Rn. 63; *Schaar*, Datenschutz im Internet, Rn. 29 f.
[84] *Art. 29 Datenschutzgruppe*, WP 37, S. 8 f.; *Schaar*, Datenschutz im Internet, Rn. 29 f.
[85] *Brockhaus*, Stichwort „E- Mail"; *Eckert*, S. 135; *Lipinski*, Stichwort „E- Mail, Electronic Mail (Elektronische Post)"; *Rojas*, Stichwort „Electronic Mail"
[86] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Brockhaus*, Stichwort „E-Mail"; *Lipinski*, Stichwort „E-Mail, Electronic Mail (Elektronische Post)"; *Rojas*, Stichwort „Electronic Mail"; *Schaar*, Datenschutz im Internet, Rn. 12
[87] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Brockhaus*, Stichwort „E-Mail"; *Lipinski*, Stichwort „E-Mail, Electronic Mail (Elektronische Post)"; *Rojas*, Stichwort „Electronic Mail"
[88] Homepage einsehbar unter: http://www.eudora.com (letzter Abruf: 29.04.2007)
[89] Homepage einsehbar unter: http://www.pmail.com/index.htm (letzter Abruf: 29.04.2007)
[90] Homepage einsehbar unter: http://www.outlook-net.de (letzter Abruf: 29.04.2007)
[91] *Brockhaus*, Stichwort „E-Mail", „Eudora","Pegasus", „Outlook"; *Rojas*, Stichwort „Electronic Mail";Homepage einsehbar unter: http://www.eudora.com (letzter Abruf: 29.04.2007)
[92] vgl. zur Praxis der Provider: *AOL*, Network Privacy Policy, abrufbar unter http://about.aol.com/aolnetwork/aol_pp (letzter Abruf: 29.04.2007); *Microsoft*, Onlinedatenschutzbestimmungen (Angabe des Namens, der Adresse und des Geburtsdatums), abrufbar unter: http://privacy.microsoft.com/de-de/fullnotice.aspx#collection (letzter Abruf: 29.04.2007)

aus.[93] Er betätigt sodann die Sendefunktion in seinem Programm, wonach der Email-Client die Email an den Mail-Server des Empfängers oder an das Email-Konto des Nutzers übersendet, das dieser bei einem Internet-Diensteanbieter führt.[94] Dabei wird beim Versenden grundsätzlich lediglich eine Kopie an den Adressaten übersandt, während das Original beim Absender gespeichert wird bzw. gespeichert werden kann.[95]
Die Email kann der Empfänger sodann auf zwei Arten erhalten. Entweder er ist direkt mit einem Mail-Server verbunden oder er muss erst eine Verbindung herstellen, um die Email zu erhalten.[96] Die an den Empfänger adressierten Emails werden dabei auf dem Mail-Server des Email-Service-Providers in der so genannten *Mailbox* zum Abruf bereitgehalten.[97] Befindet sich der Empfänger im jeweiligen Netz und ist sein Email-Programm aktiv, wird er meist durch ein Tonsignal über das Eintreffen neuer Emails informiert.[98] Er kann sie dann vom Mail-Server herunterladen und später auch ohne bestehende Internet-Verbindung lesen.[99]

II. Terminologie

Nachfolgend werden die für das Verständnis der Arbeit erforderlichen Begriffe hinsichtlich der Email-Kommunikation erläutert.

1. Header

Eine Email besteht aus der Steuerungsinformation dem so genannten *Header* und dem Nachrichteninhalt.[100] Dabei stellt die Email-Adresse des Empfängers die wichtigste im Header enthaltene Steuerungsinformation dar.[101] Des Weiteren enthält der Header die IP- und Email-Absenderadresse, Angaben über den Zeitpunkt der Erstellung bzw. der Versendung der Nachricht und die Kurzbezeichnung des Nachrichteninhaltes, den Betreff und die Namen der angehängten Dateien.[102] Die im Header enthaltenen Steuerungsinformationen werden von der Software benutzt, um die Datei zu übertragen.[103] Sie ermöglichen es für die an der Übertragung der Datenpakete beteiligten Transferrechner, Herkunft und Ziel der übertragenen Daten zu erkennen.[104]

---

[93] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Schaar*, Datenschutz im Internet, Rn. 12
[94] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Lipinski*, Stichwort „E-Mail, Electronic Mail (Elektronische Post); *Schaar*, Datenschutz im Internet, Rn. 12
[95] vgl.: *Gmx*, (Möglichkeit, gesendete Nachrichten in einem speziellen Ordner zu speichern), siehe http://gmx.net/de/produkte/mail/funktionen/mailbox/speicher/280490.html (letzter Abruf: 29.04.2007); *Hotmail*, (Möglichkeit, ein Kästchen mit der Bezeichnung „Gesendete Nachrichten im Ordner „Gesendete Nachrichten" speichern zu aktivieren), siehe www.hotmail.com, (letzter Abruf: 29.04.2007)
[96] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Brockhaus*, Stichwort „E-Mail"; *Klußmann*, Stichwort „E-Mail"; *Rojas*, Stichwort „Electronic Mail"; *Schaar*, Datenschutz im Internet, Rn. 12
[97] *Brockhaus*, Stichwort „E-Mail"; *Imhof* in Weitnauer, Form. A.1., Anm. 6; *Klußmann*, Stichwort „E-Mail"; *Rojas*, Stichwort „Electronic Mail"
[98] *Brockhaus*, Stichwort „E-Mail"
[99] *Lipinski*, Stichwort „POP-Protokoll, (POP, Post Office Protocol)"; *Klußmann*, Stichwort „POP3"
[100] *Art. 29 Datenschutzgruppe*, WP 37, S. 30; *Brockhaus*, Stichwort „E-Mail"; *IETF*, RFC 2822; *Lipinski*, Stichwort „E-Mail, Electronic Mail (Elektronische Post)"; *Rojas*, Stichwort „Electronic Mail"; *Schaar*, Datenschutz im Internet, Rn. 12; *Klußmann*, Stichwort „Header"
[101] *Art. 29 Datenschutzgruppe*, WP 37, S. 30; *Klußmann*, Stichwort „Header"; *Schaar*, Datenschutz im Internet, Rn. 12; *Wikipedia*, Stichwort „Header (E-Mail)", a.a.O.
[102] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Klußmann*, Stichwort „Header"; *Rojas*, Stichwort „Electronic Mail"
[103] *Brockhaus*, Stichwort „Header"; *Eckert*, S. 87; *Klußmann*, Stichwort „TCP/IP"; *Rojas*, Stichwort „Electronic Mail", „TCP/IP"
[104] *Brockhaus*, Stichwort „Header", „TCP/IP"; *Eckert*, S. 87; *Klußmann*, Stichwort „TCP/IP"; *Rojas*, Stichwort „TCP/IP"

2. SMTP- und POP-Protokoll

Für elektronische Post werden neben dem TCP/IP-Protokoll zwei weitere Protokolle verwendet und zwar das **S**imple **M**ail **T**ransport **P**rotocol (SMTP) und das **P**ost **O**ffice **P**rotocol (*POP-Protokoll)*.[105] SMTP wird benutzt, um eine elektronische Nachricht von einem Client zum Mail-Server des Empfängers zu übersenden.[106] Das POP-Protokoll ermöglicht es dem Empfänger, eine Verbindung zum Mail-Server herzustellen, auf dem die an ihn übersandten elektronischen Nachrichten gespeichert werden.[107] Die aktuelle Version dieses Programms ist *POP3*.[108] In der Regel enthalten Email-Client-Programme beide Protokolle, da der Absender einer Email in aller Regel auch eine Antwort erhalten möchte.[109]

3. Email-Adresse

Eine *Email-Adresse*, die für den Transport im SMTP-Protokoll benutzt wird, besteht aus zwei Teilen, die durch das Zeichen"@" getrennt sind.[110] Dabei identifiziert der rechte Teil das elektronische Postamt bzw. den Mail-Server des Adressinhabers, während der linke Teil in seiner einmaligen Kennung besteht.[111] Es handelt sich dabei um den Namen, unter dem der Adressinhaber bei dem Email-Server bekannt ist.[112] Dies muss nicht notwendigerweise der wirkliche Name des Adressinhabers sein, vielmehr kann der vor dem Zeichen „@" befindliche Teil der Email-Adresse auch ein vom Adressinhaber ausgesuchtes Pseudonym oder ein Zufallscode sein.[113]
Beim Versenden von unerbetenen Werbenachrichten verwendet der Absender häufig kein Email-Konto, sondern hat unmittelbaren Zugang zum SMTP-Protokoll, was ihm erlaubt, seine Email-Adresse zu löschen oder zu ändern.[114] Da es sich bei SMTP um ein textbasiertes Programm handelt und die Absenderadresse nicht geprüft wird, ist es möglich, von Hand eine Absenderadresse einzutragen, die mit der wirklichen Adresse nicht übereinstimmt.[115] Dieser Vorgang wird *Spoofing* genannt.[116] Der wahre Absender kann also über seine Identität

---

[105] *Art. 29 Datenschutzgruppe*, WP 37, S. 29; *Brockhaus*, Stichwort „SMTP"; *Klußmann*, Stichwort „SMTP"; *Lipinski*, Stichwort „SMTP"
[106] *Art. 29 Datenschutzgruppe*, WP 37, S. 29; *Brockhaus*, Stichwort „SMTP"; *IETF*, RFC 821 und 822; *Klußmann*, Stichwort „SMTP"; *Lipinski*, Stichwort „SMTP"
[107] *Art. 29 Datenschutzgruppe*, WP 37, S. 29; *Brockhaus*, Stichwort „POP3"; *IETF*, RFC 1725; *Klußmann*, Stichwort „SMTP", „POP3"; *Lipinski*, Stichwort „POP- Protokoll"
[108] *Art. 29 Datenschutzgruppe*, WP 37, S. 29; *Brockhaus*, Stichwort „POP3"; *Klußmann*, Stichwort „POP3"; *Lipinski*, Stichwort „POP- Protokoll"
[109] *Art. 29 Datenschutzgruppe*, WP 37, S. 29; *Brockhaus*, Stichwort „POP3"; *Lipinski*, Stichwort „POP-Protokoll"
[110] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Brockhaus*, Stichwort „E-Mail-Adresse"; *Lipinski*, Stichwort „E-Mail- Adresse"; *Rojas*, Stichwort „Electronic Mail"; *Schaar*, Datenschutz im Internet, Rn. 12; *Wikipedia*, Stichwort „E-Mail-Adresse", a.a.O.
[111] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Brockhaus*, Stichwort „E-Mail-Adresse"; *Lipinski*, Stichwort „E-Mail-Adresse"; *Rojas*, Stichwort „Electronic Mail"; *Schaar*, Datenschutz im Internet, Rn. 12; *Wikipedia*, Stichwort „E-Mail-Adresse", a.a.O.
[112] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Lipinski*, Stichwort „E-Mail-Adresse"; *Rojas*, Stichwort „Electronic Mail"; *Schaar*, Datenschutz im Internet, Rn. 12
[113] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Lipinski*, Stichwort „E-Mail-Adresse"; *Schaar*, Datenschutz im Internet, Rn. 12; *Wikipedia*, Stichwort „E-Mail-Adresse", a.a.O.
[114] *Art. 29 Datenschutzgruppe*, WP 37, S. 28; *Lipinski*, Stichwort „E-Mail- Adresse"; *Ruess/Patzak*, RDV 2003, S. 172; *Schaar*, Datenschutz im Internet, Rn. 12; *Wikipedia*, Stichwort „Simple Mail Transfer Protocol","Mail-Spoofing", a.a.O.
[115] *BSI*, Vortäuschen eines falschen Absenders, a.a.O.; *Ohne Autor*, Spoofed/Forged Email, abrufbar unter http://www.cert.org/tech_tips/email_spoofing.hmtl (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Simple Mail Transfer Protocol", a.a.O.
[116] *Brockhaus*, Stichwort „Spoofing"; *Ernst*, NJW 2003, S. 3234; *Klußmann*, Stichwort „Spoofing"; *Lipinski*, Stichwort „Spoofing"

täuschen und eine beliebige Email-Adresse als Absender angeben.[117] Allerdings ist die Anonymität des Absenders hierbei nicht vollständig gewährleistet, da -wie bereits dargestellt wurde-[118] die IP-Adresse des absendenden Rechners im Header der Email übermittelt wird, die -zumindest für den Provider oder LAN-Verwalter, der sie vergeben hat- Rückschlüsse auf den Absender zulässt.[119] Die IP-Adresse lässt sich jedoch im Gegensatz zur Email-Adresse nur sehr schwer fälschen.[120]

Bei Kenntnis der Email-Adresse einer Person lassen sich unter Zuhilfenahme bestimmter Informationen und Techniken durch Beobachtung ihrer Kommunikation auch ohne inhaltliche Wahrnehmung ihres Email-Verkehrs Rückschlüsse auf die Kommunikationsgewohnheiten des Adressinhabers ziehen. Dies geschieht, indem Verbindungsdaten in einer Kommunikationsmatrix abgespeichert werden, die dann mit verschiedenen automatischen Verfahren ausgewertet wird.[121] Als Resultat ergibt sich zunächst, ob zwei Personen keinen, einen asymmetrischen oder einen wechselseitigen Kontakt haben.[122] Eine weitere, über dieses Ergebnis hinausgehende Auswertungsmöglichkeit besteht darin, die Grenze der Paaranalyse zu verlassen und die Informationsflüsse zwischen mehreren Personen darzustellen.[123] Auf diese Weise kann sogar die Zugehörigkeit einer Person zu einer bestimmten sozialen Gruppe bestimmt und festgestellt werden, ob der Betroffene zu den führenden Köpfen dieser Gruppe gehört oder nicht.[124]

4. Spammail, Unsolicited Commercial Email und ähnliche Bezeichnungen

Der Begriff *Spamming* erfasst den massenhaften Versand von Emails durch Unternehmen oder Tendenzorganisationen mit dem Ziel, den Empfängerkreis durch ihre politischen Botschaften oder Werbemitteilungen in ihrem Sinne zu beeinflussen.[125] Der Begriff der Spammail leitet sich von einem in den USA verbreiteten Dosengericht mit der Bezeichnung „**S**piced **P**ork and H**am**“ ab, das in den Sketchen der Komikertruppe Monty Python als Sinnbild für Dinge, denen man nicht entkommen kann, Berühmtheit erlangte.[126] So wurde das Gericht in einem Sketch jedem Restaurantbesucher unaufgefordert vorgesetzt.[127] Später wurde der Begriff in die Phrase „**S**end **P**henomenal **A**mount of **M**ail“ umgedeutet.[128]
Neben dem Begriff Spammail existieren zahlreiche weitere verwandte Bezeichnungen, wie *Junkmail*, *Unsolicited Commercial Email (UCE)*, *Unsolicited Bulk Email (UBE), Cold Mail, Excessive Multi Posting (EMP)* oder *Massen- Email*,[129] die teilweise synonym, teilweise in nicht völlig mit dem Begriff der Spammail übereinstimmender Art und Weise gebraucht werden. Die Terminologie ist nicht einheitlich. Unter einer *Unsolicited Bulk Email (UBE)*, deutsch unverlangten Massen-Email, werden Emails verstanden, die unangefordert an eine große Anzahl von Empfängern verschickt werden, so etwa Kettenbriefe oder Marketing-

[117] *Ruess/Patzak*, RDV 2003, S. 172
[118] vgl.: 1. Kap. Teil 1 B. II. 1.
[119] *Dammann* in Simitis, § 3 BDSG, Rn. 62; *Ruess/Patzak*, RDV 2003, S. 172
[120] *Ruess/Patzak*, RDV 2003, S. 172
[121] *Lepperhoff/Tinnefeld*, RDV 2004, S. 9
[122] *Lepperhoff/Tinnefeld*, RDV 2004, S. 9
[123] *Lepperhoff/Tinnefeld*, RDV 2004, S. 10
[124] *Lepperhoff/Tinnefeld*, RDV 2004, S. 10
[125] *Brockhaus*, Stichwort „Spamming“; *Fritzmeyer/Lab*, K & R 2005, S. 50; *Klußmann*, Stichwort „Spam“; *Lipinski*, Stichwort „Spam Mail“; *Rojas*, Stichwort „Spam“
[126] *Brockhaus*, Stichwort „Spamming“; *Irlbeck*, Stichwort „Spam-Mail“; *Rojas*, Stichwort „Spam“; *Wikipedia*, Stichwort „Spam“, a.a.O.
[127] *Brockhaus*, Stichwort „Spamming“; *Irlbeck*, Stichwort „Spam-Mail“; *Rojas*, Stichwort „Spam“; *Wikipedia*, Stichwort „Spam“, a.a.O.
[128] *Brockhaus*, Stichwort „Spamming“; *Irlbeck*, Stichwort „Spam-Mail“
[129] *Brockhaus*, Stichwort „Spamming“; *Fritzmeyer/Lab*, K & R 2005, S. 50; *Irlbeck*, Stichwort „Spam-Mail“

Aktionen.[130] Der Begriff Unsolicited Commercial Email (UCE) bezeichnet hingegen Emails mit werbenden Inhalten, welche unaufgefordert an Empfänger -auch einzelne oder wenige- versandt werden.[131] Häufig sind Emails zugleich als Unsolicited Bulk Email und als Unsolicited Commercial Email zu qualifizieren; es handelt sich in diesem Fall um massenhaft versandte Werbe-Emails.[132] Die Begriffe Werbe-Email und Junkmail werden häufig synonym mit dem der Spammail gebraucht.[133] In der Umgangssprache existieren weder klare Abgrenzungen, noch feststehende Definitionen der verschiedenen Begriffe. Allerdings enthält das am 01.03.2007 in Kraft getretene Telemediengesetz[134] eine Definition der Bezeichnung der kommerziellen Kommunikation.[135] Auf den Begriff und seine Definition nimmt jedoch bisher lediglich das TMG Bezug. Demnach existiert auch nach Erlaß des TMG keine einheitliche Terminologie oder eine klare Abgrenzung zwischen den oben genannten verschiedenen Bezeichnungen.
Im Rahmen dieser Arbeit werden die Begriffe Spammail, kommerzielle Email, Werbe-Email, elektronische Werbenachricht, Werbung mittels elektronischer Post und Email-Werbung synonym verwendet. Etwas anderes gilt lediglich im Bereich des US-amerikanischen CAN-SPAM Act,[136] der nur Regelungen hinsichtlich kommerzieller Emails trifft. Folglich wird hier auch im Rahmen dieser Arbeit dort lediglich dieser Begriff gebraucht.

Anzumerken ist, dass Werbe-Emails nicht stets für alle Empfänger unerwünscht sind. Denn während möglicherweise eine Person Emails mit bestimmten Inhalten als belästigend empfindet, sind unter Umständen bestimmte Bevölkerungsgruppen am Erhalt solcher Nachrichten durchaus interessiert.

Der Nachteil von Werbe-Emails für die Empfänger liegt einerseits in den durch diese verursachten zusätzlichen externen und internen Kosten.[137] Andererseits kann die Zustellung einer Mehrzahl solcher Nachrichten zu überquellenden Mailboxen mit der Folge führen, dass erwünschte Kommunikation bisweilen nicht mehr empfangen werden kann.[138] Des Weiteren resultiert das Aufkommen an Werbe-Emails in einer Belastung des Netzwerks, das die Geschwindigkeit des Datenstroms und damit die Funktionstüchtigkeit des Internets als Ganzes beeinträchtigt.[139] Angesichts der technischen Entwicklung ist allerdings mit einem Zusammenbruch des Servers des Diensteanbieters aufgrund eingehender Werbe-Emails nicht zu rechnen, es sei denn es erfolgt ein gezielter Angriff durch ein Mailbombing.[140] Hierunter wird das Versenden eines großen Volumens an Emails mit dem Ziel verstanden, den Empfänger-Server zum Absturz oder eine Mailbox zum Überlaufen zu bringen.[141]

---

[130] *Brockhaus*, Stichwort „UBE"; *Spamhaus*, The Definition of Spam, abrufbar unter: http://www.spamhaus.org/definition.html (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Spam", a.a.O.
[131] *Coalition Against Unsolicited Commercial Email* (CAUCE), How do you define „spam"?, abrufbar unter: http://www.cauce.org/faq/ (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Spam", a.a.O.
[132] *Wikipedia*, Stichwort „Spam", a.a.O.
[133] *Brockhaus*, Stichwort „Junk Mail"; *Coalition Against Unsolicited Commercial Email* (CAUCE), About Junk Email/UCE/Spam, abrufbar unter: http://www.cauce.org/book/print/9 (letzter Abruf: 29.04.2007); *Klußmann*, Stichwort „Junk-Mail"
[134] Telemediengesetz vom 26.02.2007, BGBl. I, S. 179 ff.
[135] vgl. § 2 Nr. 5 TMG
[136] Controlling the Assault of Non- Solicited Pornography and Marketing Act, Pub. L. No. 108- 187 vom 16.12.2003; siehe: Anhang I
[137] *Fritzmeyer*, K & R 2005, S. 50; *Härting*/*Eckart*, CR 2004, S. 120; *Jankowski*, K & R 2000, S. 499; *Klußmann*, Stichwort „Spam"; *Rojas*, Stichwort „Spam"; *Wikipedia*, Stichwort „Spam", a.a.O.
[138] *Fritzmeyer*, K & R 2005, S. 50; *Härting*/*Eckart*, CR 2004, S. 120; *Jankowski*, K & R 2000, S. 499; *Rojas*, Stichwort „Spam"; *Wikipedia*, Stichwort „Spam", a.a.O.
[139] *Irlbeck*, Stichwort „Spam-Mail"; *Rojas*, Stichwort „Spam"; *Wendlandt*, MMR 2004, S. 365 *Wikipedia*, Stichwort „Spam", a.a.O.
[140] *BSI*, Antispam-Strategien, 6.3.1.; *Koecher*, DuD 2005, S. 165
[141] *Wikipedia*, Stichwort „E-mail bomb"

Externe Kosten aufgrund von Werbe-Emails sind solche, die durch Leistungen Dritter entstehen, beispielsweise die Telefon-, Provider- und Stromkosten, die während des Lesens und des Löschens der betreffenden Nachricht anfallen.[142] Interne Kosten resultieren aus dem Einsatz eigener Mittel und beinhalten beispielsweise die Blockade von Speicherplatz auf dem Rechnersystem, die Rechnerleistung, den Zeitaufwand für die Datenübernahme vom Server des Providers auf das eigenen System und für das Aussortieren der unverlangten Werbe-Emails.[143] Den Email-Service-Providern entstehen Kosten vor allem dadurch, dass Werbe-Emails die Speicherkapazitäten der Server belegen, was Systemerweiterungen erforderlich machen kann.[144] Der gesamte durch Spammails verursachte Schaden geht jährlich in die Milliarden.[145] Studien schätzen die durch Spammails hervorgerufenen Kosten von Unternehmen pro Arbeitnehmer und Jahr auf $ 1.934.[146] Allein der Gesamtschaden durch Spam in den USA wird jährlich auf $ 10 Mrd. beziffert, in Europa auf $ 2,5 Mrd.[147]

Dabei wächst der Anteil von Spammails am gesamten Email-Aufkommen stetig an.
Allein zwischen November 2002 und Oktober 2003 war ein Anstieg der Menge von Werbe-Emails von 40 % auf 52 % zu verzeichnen.[148] Mittlerweile wird der Anteil auf zwischen 60 und 90 % geschätzt.[149] Auf Seiten der Versender von Spammails ist der Kostenaufwand äußerst gering.[150] Sie können Emails erstellen und millionenfach ohne zusätzliche Kosten verschicken.[151] Da das Kommunikationsmedium Email durch die große Anzahl versandter Spammails stark beeinträchtigt ist, wurden in den letzten Jahren verschiedene Filterverfahren entwickelt, die dazu dienen, sich vor unerwünschten Werbe-Emails zu schützen.[152] In den USA ansässige Unternehmen, die Spam- und Virenfiltersoftware herstellen, sind etwa McAfee,[153] Postini[154] sowie Symantec,[155] deutsche Hersteller sind unter anderem Avira,[156] Softwin,[157] Astaro[158] und Optisoft[159].

---

[142] *Härting*/*Eckart*, CR 2004, S. 120; *Jankowski*, K & R 2000, S. 499; *Wikipedia*, Stichwort „Spam“, a.a.O.
[143] *Brockhaus*, Stichwort „Spamming“; *Coalition Against Unsolicited Commercial Email* (CAUCE), Cost Shifting, abrufbar unter: http://www.cauce.org/problem/costshifting (letzter Abruf: 29.04.2007); *Härting*/*Eckart*, CR 2004, S. 120; *Jankowski*, K & R 2000, S. 499
[144] *Coalition Against Unsolicited Commercial Email* (CAUCE), Cost Shifting, abrufbar unter: http://www.cauce.org/problem/costshifting (letzter Abruf: 29.04.2007); *Spiegel*, DuD 2003, S. 266; *Wendlandt*, MMR 2004, S. 365; *Wikipedia*, Stichwort „Spam“, a.a.O.
[145] *BSI*, Antispam- Strategien, a.a.O., 2.; *Wikipedia*, Stichwort „Spam“, a.a.O.
[146] *BSI*, Antispam- Strategien, a.a.O., 3.3.1.; *Nucleus Research*, a.a.O., S. 1
[147] *BSI*, Antispam- Strategien, a.a.O., 3.3.1.; Heise Online News vom 04.01.2003, Spam belastet Europas Unternehmen, abrufbar unter: http://www.heise.de/newsticker/meldung/33417 (letzter Abruf: 29.04.2007)
[148] *Heidrich*/*Tschoepe*, MMR 2004, S. 75
[149] *BSI*, Antispam- Strategien, a.a.O., 1., 2.; *Wendlandt*, MMR 2004, S. 365
[150] *Brockhaus*, Stichwort „Spamming“; *Coalition Against Unsolicited Commercial Email* (CAUCE), Rubrik „Cost Shifting“, abrufbar unter: http://www.cauce.org/problem/costshifting (letzter Abruf: 29.04.2007); *Miller*, 2 Vand. J. Ent. L. & Prac., 127 f.; *Rojas*, Stichwort „Spam“; *Spiegel*, DuD 2003, S. 265 ff., 266; *Wendlandt*, MMR 2004, S. 365
[151] *Miller*, 2 Vand. J. Ent. L. & Prac., 127 f.
[152] *BSI*, Antispam- Strategien, a.a.O., 1.; *Heidrich*/*Tschoepe*, MMR 2004, S. 75; *Irlbeck*, Stichwort „Spam-Mail“; *Rojas*, Stichwort „Spam“
[153] Homepage einsehbar unter: http://www.mcafee.com (letzter Abruf: 29.04.2007)
[154] Homepage einsehbar unter: http://www.postini.com (letzter Abruf: 29.04.2007);
[155] Homepage einsehbar unter: http://www.symantec.com (letzter Abruf: 29.04.2007)
[156] Homepage einsehbar unter: http://www.avira.com/de (letzter Abruf: 29.04.2007)
[157] Homepage einsehbar unter: http://www.bitdefender.de (letzter Abruf: 29.04.2007)
[158] Homepage einsehbar unter: http://www.astaro.de (letzter Abruf: 29.04.2007)
[159] Homepage einsehbar unter: http://www.optisoft.de (letzter Abruf: 29.04.2007)

Die Möglichkeit, durch Eintrag in eine so genannte Robinson-Liste[160] dem Zusenden unerwünschter Email entgegenzuwirken,[161] führte nicht zu einer Lösung der Spamproblematik. In die Robinson-Listen können sich nach Maßgabe der europäischen ECRL[162] natürliche Personen eintragen, die keine kommerziellen Emails erhalten möchten, vgl. Art. 7 Abs. 2 ECRL. Die FTC hat eine Studie durchgeführt, wonach eine Robinson-Liste, auch Do-not-Email-Registry genannt, das Aufkommen an kommerziellen Emails nicht positiv beeinflussen würde.[163]

5. Computerviren

Computerviren sind Programme, die sich selbständig vervielfältigen und dabei in aller Regel Dateien oder Systembereiche verändern oder schädigen.[164] Viren können sich dabei auf kleinere Störungen beschränken, allerdings auch die Funktion des Computers beeinträchtigen, Daten sowie ganze Dateien vernichten sowie im schlimmsten Fall die Festplatte des Rechners neu formatieren, was zu einem Wegfall sämtlicher dort befindlicher Daten führt.[165] Neben dem Rechner der Nutzer können Viren das System des Providers beschädigen.[166] Häufig werden Viren auch dazu benutzt, vertrauliche Daten des Nutzers des betroffenen Rechners auszuspähen.[167] Viren werden oft als Anhang von Emails versandt bzw. verschicken sich teilweise selbst an alle Email-Adressen, die in den Adressbüchern des befallenen Rechners zu finden sind.[168] Ähnlich wie Viren funktionieren die so genannten Würmer; der Unterschied zwischen den beiden Schädlingen besteht darin, dass Viren zu ihrer Verbreitung anderer Programme bedürfen, des sogenannten Wirts, während Würmer sich ohne Wirt verbreiten können.[169]

---

[160] Robinson-Listen sind Listen mit Kontaktdaten von Personen, die keine unaufgeforderte Werbung erhalten wollen. Der Name „Robinson-Liste“ ist im Anklang an die Geschichte der Romafigur des Robinson Crusoe gewählt, der viele Jahre einsam auf einer abgelegenen Insel, verbrachte, ohne Verbindung zur Außenwelt zu haben, vgl.: http://de.wikipedia.org/wiki/Robinsonliste (letzter Abruf: 29.04.2007)

[161] vgl. hierzu im Bereich des Gemeinschaftsrechts Art. 7 Abs. 2 ECRL, wonach die Mitgliedstaaten dafür zu sorgen haben, dass Diensteanbieter, die Werbe-Emails versenden, regelmäßig Robinson-Listen konsultieren.

[162] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG Nr. L 178 v. 17.7.2000, S. 1 ff.

[163] *Federal Trade Commission*, National Do Not Email Registry, A Report To Congress, 15 ff., abrufbar unter: http://www.ftc.gov/reports/dneregistry/report.pdf (letzter Abruf: 29.04.2007)

[164] *Brockhaus*, Stichwort „Virus“; *BSI*, Computer-Viren. Definition und Wirkungsweise, a.a.O.; *Eckert*, S. 45 ff.; *Ernst*, NJW 2003, S. 3233 ff.; *Gravenreuth*, NStZ 1989, S. 201 ff.; *Koch*, NJW 2004, S. 801 ff.; *Libertus*, MMR 2005, S. 507 ff.; *Lipinski*, Stichwort „Virus“; *Rother*, a.a.O.

[165] *Brockhaus*, Stichwort „Virus“; *BSI*, Computer-Viren. Definition und Wirkungsweise, a.a.O.; *Eckert*, S. 45 ff.; *Ernst*, NJW 2003, S. 3233 ff.; *Gravenreuth*, NStZ 1989, S. 201 ff.; *Koch*, NJW 2004, S. 801 ff.; *Libertus*, MMR 2005, S. 507 ff.; *Lipinski*, Stichwort „Virus“

[166] *Art. 29 Datenschutzgruppe*, WP 118, S. 5; *BSI*, Computer-Viren. Definition und Wirkungsweise, a.a.O.; *Electronic Commerce Forum, Verband der deutschen Internetwirtschaft e.V.*, Whitepaper, a.a.O. S. 21; *Ernst*, NJW 2003, S. 3233 ff.; *Gravenreuth*, NStZ 1989, S. 201 ff.; *Koch*, NJW 2004, S. 801 ff.; *Libertus*, MMR 2005, S. 507 ff.

[167] *BSI*, Computer-Viren. Definition und Wirkungsweise, a.a.O.; *Eckert*, S. 52; *Ernst*, NJW 2003, S. 3233 ff.; *Gravenreuth*, NStZ 1989, S. 201 ff.; *Koch*, NJW 2004, S. 803; *Libertus*, MMR 2005, S. 507 ff.

[168] *Brockhaus*, Stichwort „Virus“; *Eckert*, S. 52; *Ernst*, NJW 2003, S. 3233 ff.; *Koch*, NJW 2004, S. 801 ff.; *Libertus*, MMR 2005, S. 507 ff.; *Lipinski*, Stichwort „Virus“

[169] *Eichelberger*, MMR 2004, Fn. 1; *Ernst*, NJW 2003, S. 3224 f.; *Ders*., Hacker, Cracker & Computerviren, Rn. 107 ff.; *Sieber* in Hoeren/Sieber, Handbuch Multimediarecht, 19, Rn. 67 ff.; vgl. zu den Auswirkungen von Würmern: *Eichelberger*, MMR 2004, S. 594; *Rother*, Die Geschichte der Computerviren, abrufbar unter: http://www.securitymanager.de (letzter Abruf: 29.04.2007): so führte „Sasser“ dazu, dass Delta Airlines aus Angst vor Flugzeugabstürzen Flüge strich, die englische Küstenwache mit gedruckten Seekarten anstatt computergestützt navigieren musste und fast der gesamte Sendebetrieb des Hessischen Rundfunkts lahmgelegt wurde, vgl. näher: *Eichelberger*, MMR 2004, S. 594. Der „I-Love-You“-Wurm ließ zahlreiche Mailserver

6. RFC- Konformität

Im Rahmen der rechtlichen Würdigung bestimmter Maßnahmen in Bezug auf eingehende Emails wird es von Bedeutung sein, wann diese Nachrichten in technischer Hinsicht als rechtmäßigerweise in Verkehr gebracht zu qualifizieren sind. Hier kann die so genannte *RFC-Konformität* einer Email relevant werden. Die Bezeichnung *RFC* steht für „**R**equest **f**or **C**omments“ und bezeichnet eine durchnummerierte Serie von Dokumenten, die verschiedene tatsächliche und vorgeschlagene Gewohnheiten beschreiben, die einen Bezug zum Internet haben und von der der **I**nternet **E**ngineering **T**ask **F**orce (IETF) herausgegeben werden.[170] *RFC-konform* ist eine Email dann, wenn sie den technischen Kriterien, die von der Internet Engineering Task Force aufgestellt wurden, entspricht.[171] In Bezug auf die Kommunikation per Email mittels SMTP gilt der RFC 821.[172]

Teil 2: Technische Funktionsweise von Spam-Filtern

Im Folgenden wird dargestellt, welche tatsächlichen Vorgänge beim Einsatz von Spam-Filter-Programmen stattfinden. Werbe-Emails werden dabei aufgrund bestimmter Eigenschaften oder Besonderheiten der Versendung identifiziert. Beispielsweise erfolgt der Versand von Spammails häufig über selbst betriebene Mail-Server, über so genannte *Open Proxies* oder *offene Relays*.[173] Unter einem Open Proxy versteht man einen Mail-Server, der fehlerhaft konfiguriert ist und deshalb die Nutzung von außerhalb des eigenen LAN zulässt.[174] Offene Relays sind solche Mail-Server, die Emails beliebiger Absender zur Beförderung annehmen.[175] Neben der Tatsache, dass sich Spammails bisweilen durch Besonderheiten bei der Versendung auszeichnen, weisen sie häufig typische inhaltliche Merkmale auf. Sie enthalten oft bestimmte Wörter oder Satzbestandteile wie „Viagra“ oder „Make Money Fast“ oder aber Begriffe, die auf einen pornographischen Inhalt hindeuten.[176]

Der Einsatz der speziellen Filter- Software, mittels derer man sich vor Spammails schützen kann, erfolgt entweder beim Provider selbst, also „server-based“ oder „client-based“, das bedeutet beim Kunden.[177] Der Unterschied zwischen den beiden Einsatzorten besteht darin, dass der jeweilige Anwender im Fall der kundenbasierten Filterung die Filterregeln in seinem Email-Programm selbst definieren kann.[178] Wird die Filtersoftware hingegen durch den Provider eingesetzt, so ordnet das Programm in der Regel für alle Kunden des Providers deren Emails nach Maßgabe derselben Kriterien und sortiert -teilweise bereits vor dem Zugriff des eigentlichen Empfängers- solche Nachrichten aus, die es als Spammails ansieht.[179] Rechtlich

---

abstürzen, vgl. näher: *Rother*, Die Geschichte der Computerviren, abrufbar unter: http://www.securitymanager.de (letzter Abruf: 29.04.2007).

[170] *Heidrich*/*Tschoepe*, MMR 2004, S. 75 ff., Fn. 33; *Henning*, Taschenbuch Multimedia, S. 343; *IETF*, RFC 821; *Irlbeck*, Stichwort „RFC“; *Klußmann*, Stichwort „RFC“

[171] *Heidrich*/*Tschoepe*, MMR 2004, S. 75 ff., Fn. 33; *Henning*, Taschenbuch Multimedia, S. 343; *IETF*, RFC 821; *Klußmann*, Stichwort „RFC“

[172] *Heidrich*/*Tschoepe*, MMR 2004, S. 75 ff., Fn. 33; *Henning*, Taschenbuch Multimedia, S. 343; *IETF*, RFC 821; *Klußmann*, Stichwort „RFC“

[173] *BSI*, Antispam- Strategien, a.a.O., 4.2.1., 4.2.3.; *Hoeren*, NJW 2004, S. 3513; *Wikipedia*, Stichwort „Offenes Mail-Relay“, a.a.O.

[174] *BSI*, Antispam- Strategien, a.a.O., 4.2.3.

[175] *Hoeren*, NJW 2004, S. 3513; *Wikipedia*, Stichwort „Offenes Mail-Relay“, a.a.O.

[176] *BSI*, Antispam- Strategien, a.a.O., 9.14.

[177] *Spindler*/*Ernst*, CR 2004, S. 437; die Filterung kann auch manuell durch Personen erfolgen. Gegenstand dieser Arbeit soll jedoch lediglich der Einsatz von automatischen Filtern, also von Spam- Filtersoftware zur Abwehr von Spam-Mails sein.

[178] *Spindler*/*Ernst*, CR 2004, S. 438

[179] *Spindler*/*Ernst*, CR 2004, S. 438

problematisch ist damit der Einsatz der Programme durch den Provider, während die client-basierte Filterverwendung grundsätzlich rechtlich unbedenklich ist, da der Empfänger selbst entscheiden kann, welche Emails er erhalten möchte und welche nicht.

Im Folgenden wird zunächst beschrieben, auf welche Art und Weise eingehende Emails als Spam-Nachrichten qualifiziert werden (A.) und wie sodann mit Emails verfahren wird, die unter Spam-Verdacht stehen (B.).

A. Qualifikation eingehender Emails als Spam-Nachrichten

Es wurden verschiedene Verfahrensweisen entwickelt, die es ermöglichen, eingehende Emails darauf zu überprüfen, ob es sich um Spam-Nachrichten handelt. Zu nennen sind einerseits das so genannte Black- und Whitelistverfahren (I.), die Header- und Text-Analyse (II.) und die Berechnung der Spam-Wahrscheinlichkeit unter Anwendung statistischer Methoden (III.). Dies sind die bekanntesten Verfahren der Spam-Filterung. Daneben wurden jedoch noch weitere Vorgehensweisen entwickelt, auf die ebenfalls kurz eingegangen werden soll (IV.).

I. Black- und Whitelisting

Das so genannte Black- und Whitelisting beruht auf der Erfahrung, dass IP- und Email-Adressen, von denen aus bereits Spammails versandt wurden, mit hoher Wahrscheinlichkeit wieder als Spam-Quelle in Erscheinung treten werden, während umgekehrt solche Adressen, von denen bisher nur legitime Emails verschickt wurden, grundsätzlich auch weiterhin nur dem Versand solcher Nachrichten dienen werden.[180] Diese Tatsache führte zur Entwicklung des Black- und Whitelisting. Dabei werden Listen solcher Adressen geführt, die als Ausgangspunkt entweder von Spammails oder aber legitimer elektronischer Post bekannt sind.[181] Je nach Art der Liste kann diese entweder die IP-Adresse des sendenden Rechners, die Absender-Email-Adresse oder die gesamte Absender-Domain enthalten.[182]

Beim Blacklisting wird die IP- oder Email-Adresse des Absenders aller eingehenden Nachrichten ständig mit der Liste unerwünschter Versender abgeglichen.[183] Zeitlich setzt die Methode des Blacklisting bereits beim Verbindungsaufbau zwischen SMTP-Sender und -Empfänger an. Der Server des Empfängers führt den Verbindungsaufbau nicht vollständig durch, sondern bricht die Verbindung unter Abgabe einer Fehlermeldung ab, sobald festgestellt wird, dass die Nachricht von einer auf der Liste befindlichen Adresse stammt.[184] Werden ganze IP-Bereiche blockiert, so wird die Verbindung bereits vor der Übertragung von Header und Text der Email unterbrochen, während in den Fällen, in denen lediglich

---

[180] *BSI*, Antispam- Strategien, a.a.O., 8.1.1.; *Wikipedia*, Stichwort „Realtime Blackhole List“, a.a.O.

[181] *BSI*, Antispam- Strategien, a.a.O., 8.1.1.; *GFI*, Programmbeschreibung, Stichwort „DNS-Blacklists (DNSBL) von Drittanbietern“, abrufbar unter: http://www.gfisoftware.de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Realtime Blackhole List“, a.a.O.

[182] *BSI*, Antispam- Strategien, a.a.O., 9.3.; *Heidrich*, MMR 2005, S. 182; *Postini*, Email Security & Management for Small and Midsize Businesses, Stichwort „Allowed and Blocked Sender, Domain and IP-Adress Lists“, abrufbar unter: http://www.postini.com/overviews/index.php?src=GWT (letzter Abruf: 29.04.2007); *Spindler*/*Ernst*, CR 2004, S. 437; *Wikipedia*, Stichwort „Realtime Blackhole List“, a.a.O.

[183] *Dietrich*/*Pohlmann*, DuD 2005, S. 548 ff., S. 549; *Spamhaus*, Frequently Asked Questions, abrufbar unter http://www.spamhaus.org/faq/answers.lasso?section=DNSBL (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Realtime Blackhole List“, a.a.O.

[184] *Dietrich*/*Pohlmann*, DuD 2005, S. 549; *Kerio MailServers*, Programmbeschreibung, abrufbar unter: http://www.kerio.com/kms_antispam.html (letzter Abruf: 29.04.2007); *Spamhaus*, Frequently Asked Questions, abrufbar unter http://www.spamhaus.org/faq/answers.lasso?section=DNSBL (letzter Abruf: 29.04.2007)

bestimmte Email-Adressen blockiert werden sollen, zumindest der Header der Email übertragen sein muss.[185] Im letztgenannten Fall wird jedoch die Verbindung in aller Regel spätestens vor Übermittlung des Inhalts abgebrochen, da hierdurch Ressourcen, wie Personal, Speicherplatz und Rechnerleistung gespart werden.[186]
Da die Versender von Spammails häufig ihre Adressen und Server ändern oder die Absender-Email-Adressen fälschen, ist der Nutzen statischer schwarzer Listen nur beschränkt; demgemäß werden in der Praxis grundsätzlich nur so genannte dynamische, also stets auf dem neusten Stand gehaltene schwarze Listen eingesetzt.[187] Ein schneller Zugriff auf schwarze Listen ist über das Domain Name System möglich. So kann über eine bestimmte DNS-Anfrage nahezu in Echtzeit festgestellt werden, ob eine IP-Adresse unter Spam-Verdacht steht oder nicht.[188] Als Oberbegriff für solche Listen werden die Bezeichnungen „*DNSBL*“ (**D**omain **N**ame **S**ystem **B**lacklist), „*Blackhole List*“ oder „*Blocking List*“ verwendet.[189] Gängig sind auch die Bezeichnungen „*Realtime Blacklist*“ oder „*Realtime Blackhole List*“.[190] Erstellt und gepflegt werden die schwarzen Listen entweder durch Email-Anbieter selbst oder durch spezielle Mitarbeiter und Organisationen, die solche Listen entgeltlich oder unentgeltlich zu Verfügung stellen.[191]

Häufig werden die Verfahren des Black- und des Whitelisting miteinander kombiniert. Das Whitelist-Verfahren nutzt Listen vertrauenswürdiger Absender.[192] Mit Hilfe solcher Listen lässt sich zuverlässige, gewünschte Kommunikation von der Überprüfung auf Spammails ausnehmen.[193] Auf diese Weise kann der ergänzende Einsatz des Whitelisting-Verfahrens vor Fehlentscheidungen der schwarzen Liste schützen.[194]

---

[185] *Dietrich*/*Pohlmann*, DuD 2005, S. 549; *Heidrich*, MMR 2005, S. 182; *Spamhaus*, Why use a DNSBL? abrufbar unter: http://www.spamhaus.org/faq/answers/lasso?section=DNSBL Technical (letzter Abruf: 29.04.2007)
[186] *Dietrich*/*Pohlmann*, DuD 2005, S. 549
[187] *BSI* Antispam- Strategien, a.a.O., 9.3.; *Dietrich*/*Pohlmann*, DuD 2005, S. 550 f.; *SpamEater*, Programmbeschreibung, abrufbar unter: http://www.hms.com/sep-features.asp (letzter Abruf: 29.04.2007)
[188] *BSI*, Antispam- Strategien, a.a.O., 9.4., *FAZ* v. 15. 07.1997, abrufbar unter: http://joergo.de/faz_spam.htm (letzter Abruf: 29.04.2007); *Spindler*/*Ernst*, CR 2004, S. 438; *Wikipedia*, Stichwort „Realtime Blackhole List“, a.a.O.; Beispiele für Listenbetreiber: *Mail Abuse Prevention System*, inzwischen von TrendMicro übernommen, erreichbar unter: http://www.mail-abuse.com (letzter Abruf: 29.04.2007) sowie http://www.trendmicro.com/kelkea (letzter Abruf: 29.04.2007); *Spam and Open Relay Blocking System* (SORBS), erreichbar unter: http://www.sorbs.net/ (letzter Abruf: 29.04.2007); *Spamhaus Block List* (SBL), erreichbar unter: http://www.spamhaus.org/ (letzter Abruf: 29.04.2007)
[189] *BSI*, Antispam- Strategien, a.a.O., 9.4.; *Spamhaus*, Frequently Asked Questions, abrufbar unter: http://www.spamhaus.org/faq/answers.lasso?section=DNSBL (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Realtime Blackhole List“, a.a.O.
[190] *BSI*, Antispam- Strategien, a.a.O., 9.4.; *Dietrich*/*Pohlmann*, DuD 2005, S. 551; *FAZ* v. 15. 07.1997, abrufbar unter: http://joergo.de/faz_spam.htm (letzter Abruf: 29.04.2007); *Spindler*/*Ernst*, CR 2004, S. 438; *Wikipedia*, Stichwort „Realtime Blackhole List“, a.a.O.
[191] *FAZ* v. 15. 07.1997, abrufbar unter: http://joergo.de/faz_spam.htm (letzter Abruf: 29.04.2007); *Spindler*/*Ernst*, CR 2004, S. 438
[192] *Dietrich*/*Pohlmann*, DuD 2005, S. 549; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *SpamEater*, Programmbeschreibung, abrufbar unter: http://www.hms.com/sep-features.asp (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Weiße Liste“, a.a.O.
[193] *Dietrich*/*Pohlmann*, DuD 2005, S. 549; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *SpamEater*, Programmbeschreibung, abrufbar unter: http://www.hms.com/sep-features.asp (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Weiße Liste“, a.a.O.
[194] *Dietrich*/*Pohlmann*, DuD 2005, S. 549; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Weiße Liste“, a.a.O.

Zu beachten ist, dass durch das Blacklisting einerseits keinesfalls sämtliche Spammails ausgefiltert werden können, da sich grundsätzlich nicht alle Server, von denen solche Nachrichten versandt werden, auf den schwarzen Listen befinden werden. Die unerbetenen Nachrichten, die den Filter passieren, werden *false negatives* genannt. Die stets vorhandene Quote von false negatives ergibt sich daraus, dass die Versender von Spammails die Server häufig wechseln oder ihre Absenderadresse fälschen.[195] Andererseits ist es möglich, dass bestimmte Nachrichten, die an sich erwünscht sind, fälschlicherweise ausgefiltert werden, so genannte *false positives*.[196] In der Vergangenheit wurden sogar bekannte Provider, die an sich nur den Versand legitimer Emails zulassen, auf schwarze Listen gesetzt.[197] Beispielsweise wurde ein Server des Email-Anbieters „web.de" im Jahr 2002 auf eine schwarze Liste aufgenommen, was zur Folge hatte, dass Kunden dieses Email-Dienstes zeitweise keine Emails mehr versenden konnten.[198] Die Gefahr auch als legitimer Provider auf solche Listen zu gelangen, ist stets gegeben, denn angesichts der Anzahl der Kunden dieser Provider kann es geschehen, dass die Dienste des Anbieters für die Versendung von Spam missbraucht werden.[199] Da weltweit eine große Anzahl von schwarzen Listen existiert, ist es den Administratoren der betroffenen Anbieter auch nicht möglich, sämtliche dieser Listen ständig darauf zu überprüfen, ob sie eigene Server als Versender von Spam-Mails auflisten.[200] Deshalb erfahren die Administratoren häufig erst von der Eintragung in einer schwarzen Liste, wenn sich Kunden darüber beschweren, dass sie ihre Emails nicht mehr versenden können.[201]

II. Header- und Textanalyse

Die Header- und Textanalyse macht sich die Tatsache zu Nutze, dass Spammails oft bestimmte typische Elemente oder Schlüsselwörter im Header oder Text der Nachricht enthalten. Deshalb werden eingehende Emails durch die entsprechende Filter-Software auf solche werbebezogenen Textbausteine überprüft. Dieser Vorgang, der abgeleitet vom englischen Begriff *scannen* genannt wird, betrifft sowohl den Header der Nachricht, als auch deren Inhalt.[202] Um nach einschlägigen Elementen innerhalb des Nachrichtentextes zu suchen, muss das Filterprogramm „Kenntnis" vom Inhalt der Nachricht nehmen, indem es diese virtuell öffnet.[203] Hierzu werden die Nachrichten zwar momentan in den Zwischenspeicher geladen, aber zu diesem Zweck nicht dauerhaft gespeichert oder für den Provider oder seine Mitarbeiter lesbar abgelegt.[204] Es finden damit lediglich Zwischenspeichervorgänge statt, wie sie bei der Datenübermittlung ständig durchgeführt werden. Eine dauerhafte Fixierung der Daten auf einem Speichermedium erfolgt hingegen nicht.[205] Somit steht derjenige, dessen Daten von der Filtermaßnahme erfasst sind hinsichtlich der Vertraulichkeit der ihn betreffenden Informationen nicht anders, als dies ohne den Filtereinsatz der Fall sein würde. Denn die in der Email enthaltenen Informationen werden während des Filtereinsatzes nicht durch eine natürliche Person wahrgenommen und mit dem Betroffenen in Verbindung gebracht. Dies kann auch nicht später nachgeholt werden, da die Daten nicht infolge des Filtereinsatzes dauerhaft gespeichert bleiben.

---

[195] *BSI*, Antispam-Strategien, a.a.O., 9.3.
[196] *Art. 29 Datenschutzgruppe*, WP 118, S. 8; *BSI*, Antispam- Strategien, 9.5.; *Spindler*/*Ernst*, CR 2004, S. 438
[197] *BSI*, Antispam- Strategien, a.a.O., 9.4.4.
[198] *FAZ* v. 15. 07.1997, abrufbar unter: http://joergo.de/faz_spam.htm (letzter Abruf: 29.04.2007)
[199] *BSI*, Antispam- Strategien, a.a.O., 9.4.4.
[200] *BSI*- Antispam- Strategien, a.a.O., 9.4.4.
[201] *BSI*- Antispam- Strategien, a.a.O., 9.4.4.
[202] *BSI*, Antispam- Strategien, a.a.O., 8.1.3.; *Spindler*/*Ernst*, CR 2004, S. 438
[203] *Spindler*/*Ernst*, CR 2004, S. 438
[204] *Spindler*/*Ernst*, CR 2004, S. 438
[205] *Spindler*/*Ernst*, CR 2004, S. 438

Ebenso wie das Verfahren des Black- und Whitelisting existiert auch hier eine gewisse Fehlerquote, da teilweise legitime Emails werbetypische Textbausteine enthalten oder aber die Versender von Spammails, so etwa durch falsche Schreibweisen, erreichen, dass die versandten Nachrichten den Filter passieren.[206]

III. Statistische Methoden

Schließlich kann durch Anwendung statistischer Methoden die Wahrscheinlichkeit dafür berechnet werden, dass es sich bei einer bestimmten Nachricht um eine Spammail handelt.[207] Das hierzu angewandte Verfahren baut auf dem Bayes-Wahrscheinlichkeitstheorem auf und wird auch Bayesscher Filter genannt.[208] Ihren Namen verdankt die Filtermethode dem Mathematiker Thomas Bayes.[209]

Der Filter analysiert zunächst alle Wörter einer Email und ordnet anschließend jedem Wort einen bestimmter Wert zu, aus dem sich dann die Wahrscheinlichkeit ermitteln lässt, mit der es sich bei der Nachricht um eine Spammail handelt.[210] Voraussetzung für die Funktionstüchtigkeit des Filters ist, dass er über eine Statistik der Worthäufigkeit einzelner Wörter in erwünschten sowie in unerwünschten Nachrichten verfügt.[211] Demnach muss der Filter vor seinem Einsatz erst konfiguriert werden. Er erhält dabei Informationen darüber, welche Wörter vor allem in erwünschten Emails vorkommen und welche in Spammails.[212] Hierdurch wird eine exakt angepasste Begriffsdatenbank erstellt, in der jedem Wort oder jedem so genannten Token, so etwa Dollar-Zeichen, IP-Adresse oder Domäne, eine bestimmte Wahrscheinlichkeit zugewiesen wird.[213] Die Zuordnung der Wahrscheinlichkeiten wird dabei individuell den Email-Korrespondenzgewohnheiten einer bestimmten Person oder eines spezifischen Unternehmens angepasst.[214] Der Filter wird ständig anhand neuer Werbe-Nachrichten und legitimer Emails aktualisiert, so dass die Erkennungsquote im Laufe der Zeit ansteigt.[215] Unter Zugrundelegung der verschiedenen Werte, die der Filter einzelnen Wörtern und Token zugewiesen hat, berechnet er sodann die Wahrscheinlichkeit, dass es sich bei einer

---

[206] *BSI*, Antispam-Strategien, a.a.O., 8.1.3
[207] *GFI*, Programmbeschreibung des GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Spaminhilators*, Programmbeschreibung, abrufbar unter: http://www.superspamkiller.de/, (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Bayessscher Filter", a.a.O.
[208] *Wikipedia*, Stichwort „Bayesscher Filter, a.a.O.
[209] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *Spaminhilator*, Programmbeschreibung, abrufbar unter: http://www.superspamkiller.de/ (letzter Abruf: 29.04.2007); *Wikipedia*, Stichwort „Bayessscher Filter", a.a.O.
[210] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Wikipedia*, Stichwort „Bayesscher Filter", a.a.O.
[211] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Wikipedia*, Stichwort „Bayesscher Filter", a.a.O.
[212] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Wikipedia*, Stichwort „Bayesscher Filter", a.a.O.
[213] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Wikipedia*, Stichwort „Bayesscher Filter", a.a.O.
[214] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Wikipedia*, Stichwort „Bayesscher Filter", a.a.O.
[215] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Wikipedia*, Stichwort „Bayesscher Filter", a.a.O.

Nachricht um eine Werbe-Email handelt. Sie wird als Spammail qualifiziert, wenn die berechnete Wahrscheinlichkeit höher ist, als ein bestimmter definierter Schwellenwert.[216]
Um nach einschlägigen Elementen innerhalb des Nachrichtentextes zu suchen, muss das Filterprogramm auch hier „Kenntnis" vom Inhalt der Nachricht nehmen, indem es diese virtuell öffnet.[217]

Der besondere Vorteil der Methode ist die Anpassung an das Anwenderprofil und die Lernfähigkeit des Filters. So kann er sich -insbesondere in den Fällen, in denen er für eine homogene Anwendergruppe eingesetzt wird- auch an veränderte Korrespondenzgewohnheiten anpassen.[218] Daneben kann das Bayes-Verfahren für jede Sprache eingesetzt werden, während gängige Stichwortkataloge meist nur in Englisch verfügbar sind und sich deshalb für andere Sprachen nicht eignen.[219] Der Bayes-Filter ist zudem schwerer zu umgehen, als herkömmliche Stichwortfilter. Denn da er auf die Bedürfnisse des jeweiligen Unternehmens bzw. Empfängers angepasst ist, können Versender von Spammails ihn nur überlisten, wenn sie die Korrespondenzgewohnheiten potentieller Empfänger kennen. Diese Informationen über die individuellen Empfänger kann der Versender jedoch kaum erlangen. So kann er den Bayes-Filter weder durch Verwendung spam-neutraler Begriffe, noch durch Aufteilung der Wörter oder andere Schreibweisen überlisten. [220]

Eine Fortentwicklung des Bayesschen Filters ist der so genannte Markow-Filter.[221] Während beim Bayesschen Filter die Wahrscheinlichkeit einzelner Wörter errechnet wird, zieht der Markow-Filter Wortketten zur Ermittlung der Wahrscheinlichkeit heran und gewichtet die einzelnen Kombinationsmöglichkeiten.[222]

IV. Weitere Verfahren

Neben den genannten Filterverfahren gibt es weitere Möglichkeiten, Spammails zu erkennen. Insbesondere werden protokollbasierte Maßnahmen zur Spam-Filterung verwendet, so etwa die Überprüfung auf einen Verstoß gegen das auf die Email-Versendung anzuwendenden Protokolls RFC 821 oder auf eine leere Mail-From-Adresse.[223] Des Weiteren wird die so genannte Frequenzanalyse zur Spam-Filterung eingesetzt.[224] Dabei wird eine Email anhand bestimmter Merkmale, so etwa der IP-Adresse bewertet.[225] Es werden für eine definierte Zeitspanne bei allen ankommenden Emails die Merkmale gezählt, auf deren Basis die spätere Beurteilung erfolgen soll.[226] Die gefundenen statistischen Werte werden einzeln oder in

---

[216] *BSI*, Antispam- Strategien, a.a.O., 9.15.
[217] *Spindler*/*Ernst*, CR 2004, S. 438
[218] *BSI*, Antispam- Strategien, a.a.O., 9.15.; *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007); *Graham*, A Plan for Spam, a.a.O.; *Wikipedia*, Stichwort „Bayessscher Filter", a.a.O.
[219] *GFI*, Programmbeschreibung GfiMailEssentials, abrufbar unter: http://www.gfi.software.de/de/mes/mesbrochure_de.pdf#search=%22whitelist%20mi%C3%9Fbra (letzter Abruf: 29.04.2007)
[220] *Spaminhilators*, Programmbeschreibung, abrufbar unter: http://www.superspamkiller.de/ (letzter Abruf: 29.04.2007); Wikipedia, Stichwort „Bayessscher Filter", a.a.O.
[221] *Wikipedia*, Stichwort „Markow-Filter", a.a.O.
[222] *Wikipedia*, Stichwort „Markow-Filter", a.a.O.
[223] *BSI*, Antispam-Strategien, a.a.O., 9.2.; *KerioMailServer*, Programmbeschreibung, Stichwort „Custom filtering by address, subject, content or size", abrufbar unter: http://www.kerio.com/kms_antispam.html (letzter Abruf: 29.04.2007)
[224] *BSI*, Antispam-Strategien, a.a.O., 9.5.; *KerioMailServer*, Programmbeschreibung, Stichwort: „Sent email per hour"quota, abrufbar unter: http://www.kerio.com/kms_antispam.html (letzter Abruf: 29.04.2007)
[225] *BSI*, Antispam-Strategien, a.a.O., 9.5.; *KerioMailServer*, Programmbeschreibung, Stichwort: „Sent email per hour"quota, abrufbar unter: http://www.kerio.com/kms_antispam.html (letzter Abruf: 29.04.2007)
[226] *BSI*, Antispam-Strategien, a.a.O., 9.5.

Kombination zur Beurteilung des enstprechenden Merkmals, so etwa der IP-Adresse eines sendenden Servers benutzt.[227] Überschreitet die dieser zugeordnete Frequenz einen bestimmten Schwellenwert, so wird die von dieser Adresse eingehende Email als Spam angesehen.[228]

Es lässt sich festhalten, dass Folge des Einsatzes von Filtersoftware unter Anwendung der soeben beschriebenen Methoden ist, dass im Header der Email enthaltene Informationen automatisiert durchsucht werden.

B. Weiteres Vorgehen bei Spam-Verdacht

Es gibt mehrere Möglichkeiten, mit einer als Spam bewerteten Email zu verfahren. So kann die Nachricht gelöscht, blockiert, mit einer Markierung versehen zugestellt oder aber in eine spezielle so genannte Quarantäne- Mailbox zugestellt werden.[229]

Ist die Software so eingestellt, dass spam-verdächtige Emails gelöscht oder gar nicht erst zugestellt werden, so ist der Vorgang in der Regel unwiderruflich. Eine andere Möglichkeit besteht darin, positiv gescannte Emails nicht zu löschen, sondern sie als unzustellbar zurückzuweisen.[230] Dem Empfänger wird die Email demnach nicht zugestellt. Der Absender erhält in aller Regel eine entsprechende Fehlermeldung.[231]

Teilweise sind die Filter so konfiguriert, dass positiv gescannte Emails weder gelöscht, noch zurückgewiesen, sondern lediglich als spam-verdächtig markiert werden. Die Kennzeichnung erfolgt dabei entweder durch eine Veränderung der Subjekt-Zeile oder durch eine zusätzlich eingefügte Header-Zeile.[232] Hierbei wird durch Anfügen einer bestimmten Anzahl von Sternchen oder anderen Symbolen die Spam-Wahrscheinlichkeit angezeigt.[233]

Schließlich werden positiv gescannte Emails teilweise in speziellen Ordnern abgelegt, die in der Regel die eingestellten Emails bis zu einem zuvor bestimmten Verfallstag oder einer bestimmten Höchstmenge aufnehmen.[234] Dabei sortiert das Filterprogramm eingehende Emails automatisch nach der Überprüfung in den Posteingang oder einen Quarantäne-Ordner ein. Die hier abgelegten Emails werden in der Regel nach einigen Tagen gelöscht.[235] Grundsätzlich weisen die Email-Service-Provider darauf hin, dass es sich nicht bei sämtlichen in den Quarantäne-Ordnern eingestellten Emails um Spam handelt.[236]

---

[227] *BSI*, Antispam-Strategien, a.a.O., 9.5.
[228] *BSI*, Antispam-Strategien, 9.5.; *KerioMailServer*, Programmbeschreibung, Stichwort: „Sent email per hour"quota, abrufbar unter: http://www.kerio.com/kms_antispam.html (letzter Abruf: 29.04.2007)
[229] *BSI*, Antispam- Strategien, a.a.O., 8.6., *Proofpoint*, Programmbeschreibung, (Einteilung eingehender Nachrichten in „Commercial Spam", „Pornographic Spam" und „Valid Emails"), abrufbar unter: http://www.proofpoint.com/products/spam.php (letzter Abruf: 29.04.2007); *Postini Solutions*, Programmbeschreibung, (Filterung nach nutzerdefinierten Kriterien wie „sexually explicit", „get rich quick", „special offers" sowie „racially insensitive"), abrufbar unter: http://www.postini.com/overviews/index.php?src=GWT (letzter Abruf: 29.04.2007); *Spindler*/*Ernst*, CR 2004, S. 438
[230] *Koecher*, DuD 2004, S. 273
[231] *Koecher*, DuD 2004, S. 273
[232] *BSI*, Antispam- Strategien, a.a.O., 8.6.4.; *Hoeren*, NJW 2004, S. 3515
[233] *BSI*, Antispam- Strategien, a.a.O., 8.6.4.
[234] *BSI*, Antispam- Strategien, a.a.O., 8.6.5.; *Spindler*/*Ernst*, CR 2004, S. 438
[235] *Spindler*/*Ernst*, CR 2004, S. 443
[236] vgl. *AOL*, Hinweise, abrufbar unter: http://www.aol.de/Webmail-Vorteile/Kostenloser-Spam-Virenschutz-508408064-2.html (letzter Abruf: 29.04.2007); *Hotmail*, Hinweise, abrufbar unter: http://msn.de//hilfecenter/ratgeber/spamschutz/prevention/ (letzter Abruf: 29.04.2007)

2. Kapitel: Rechtslage in Deutschland

Gegenstand dieser Arbeit ist die Frage nach der rechtlichen Zulässigkeit der verschiedenen Maßnahmen, die zur automatisierten Identifizierung und Abwehr von Werbe-Emails vorgenommen werden. Der Einsatz von Filtersoftware stellt die Reaktion auf das Versenden unverlangter kommerzieller Emails dar. Die Widerrechtlichkeit der abgewehrten Nachrichten könnte folglich mögliche Abwehrmaßnahmen rechtfertigen. Deshalb wird nachfolgend zunächst darauf eingegangen, ob bzw. unter welchen Voraussetzungen der Versand solcher Emails nach Maßgabe des deutschen Rechts als zulässig anzusehen ist (Teil 1). Anschließend wird dargestellt, wie technische Maßnahmen zur Identifizierung und Vermeidung unerbetener Werbe-Emails rechtlich zu beurteilen sind (Teil 2).

Teil 1: Zulässigkeit von Werbe-Emails

Die Frage nach der Zulässigkeit von Werbe-Emails wird zuerst am Maßstab des einfachen Rechts gemessen (A.). Im Anschluss wird die Rechtslage darauf überprüft, ob sie im Einklang mit verfassungs- und gemeinschafts- sowie völkerrechtlichen Vorgaben steht (B.).

A. Einfaches Recht

Die Unzulässigkeit unverlangter Werbe-Emails könnte sich aus straf- (I.), wettbewerbs- (II.) oder deliktsrechtlichen Vorschriften (III.) ergeben.

I. Strafrecht

Bewirkt das Volumen eingehender Werbenachrichten, dass legitime Emails nicht mehr zugestellt werden können oder der Empfänger nicht in der Lage ist, in seiner Mailbox befindliche erwünschte Nachrichten aufzufinden, so könnte der Straftatbestand des § 303 a Abs. 1 StGB[237] verwirklicht sein, der das Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten im Sinne des § 202 a Abs. 2 StGB sanktioniert.[238]
Voraussetzung ist, dass derjenige, der Werbe-Emails verschickt, den objektiven (1.) und subjektiven Tatbestand (2.) des § 303 a Abs. 1 StGB erfüllt und rechtswidrig (3.) handelt.

1. Objektiver Tatbestand

Der objektive Tatbestand des § 303 a Abs. 1 StGB ist erfüllt, wenn die legitimen Emails, die durch das Volumen zustellter Werbenachrichten beeinträchtigt werden, Daten im Sinne des § 202 a Abs. 2 StGB sind (a), die nach h.M.[239] fremd sein müssen (b). Daneben ist erforderlich, dass in den jeweiligen Maßnahmen eine Tathandlung im Sinne des § 303 a Abs. 1 StGB zu sehen ist (c).

---

[237] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998, BGBl. I. S. 3322

[238] Dabei soll nur auf mögliche Strafnormen eingegangen werden, die das Zusenden unverlangter Emails sanktionieren. Zu Straftatbeständen, die der Täter möglicherweise zusätzlich verwirklicht, so etwa, wenn er elektronische Nachrichten zur Verschleierung seiner Identität über fremde Rechner leitet oder Absender-Email-Adressen fälscht, vgl. Frank, CR 2004, S. 123 ff.

[239] BayObLG, JR 1994, S. 476 mit Anmerkung *Hilgendorf*, JR 1994, S. 478 ff.; *Kitz*, CR 2005, S. 454; *Koecher*, DuD 2004, S. 274; *Lenckner*/*Winkelbauer*, CR 1986, S. 829; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 3; Tröndle/Fischer, § 303 a StGB, Rn. 4

a) Daten im Sinne des § 202 a Abs. 2 StGB

Im Rahmen des § 202 a Abs. 2 StGB ist von einem weiten Datenbegriff auszugehen, der entsprechend dem allgemeinen Sprachgebrauch alle durch Zeichen oder kontinuierliche Funktionen dargestellten Informationen erfasst, die sich als Gegenstand oder Mittel der Datenverarbeitung für eine Datenverarbeitungsanlage kodieren lassen oder die das Ergebnis eines Datenverarbeitungsvorgangs sind.[240] Nicht erforderlich ist, dass es sich um personenbezogene Daten handelt, auch ein Geheimnis braucht ihnen nicht zu Grunde zu liegen.[241] Der Begriff erfährt allerdings eine Einschränkung dahingehend, dass die Daten nicht unmittelbar wahrnehmbar sein dürfen, § 202 a Abs. 2 StGB. An der unmittelbaren Wahrnehmbarkeit fehlt es, wenn sprachlich oder in Bildern kodierte Informationen nicht ohne weiteres mit den Sinnen, sondern erst mittels Instrumenten wie Verstärkern, Sensoren, Bildschirm, Drucker, also künstlich wahrnehmbar sind.[242] Emails enthalten in ihrem Text und Header durch Zeichen dargestellte Nutz- und Verwaltungsdaten.[243] Diese sind Gegenstand bzw. Ergebnis eines Datenverarbeitungsvorgangs. Da sie nur mittels eines Bildschirms oder nach dem Ausdrucken des Textes gelesen werden können, sind sie nicht unmittelbar wahrnehmbar.
Des Weiteren sind nur solche Informationen Daten im Sinne der Vorschrift, die gespeichert sind oder übermittelt werden, vgl. § 202 a Abs. 2 StGB. Gespeichert sind Daten, wenn sie zum Zweck ihrer weiteren Verwendung erfasst, aufgenommen oder aufbewahrt werden, § 3 Abs. 4 Nr. 1 BDSG.[244] Übermittelt werden Daten, wenn sie durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, insbesondere zum Abruf, bereitgehalten werden, daneben aber auch während des Datenflusses.[245] So ist insbesondere die Weiterleitung der Daten von Rechner zu Rechner innerhalb eines Netzwerkes oder über Fernmeldewege als Übermittlung im vorgenannten Sinne anzusehen.[246] Noch nicht eingegangene elektronische Nachrichten werden gerade weitergegeben. Sie sind demnach Daten, die übermittelt werden. Emails, die bereits in die Mailbox des Empfängers eingestellt sind, werden zum Zweck ihrer weiteren Verwendung aufbewahrt, weshalb sie sich als gespeicherte Daten qualifizieren lassen. Vor dem Herunterladen der Emails durch den Empfänger greift hier auch die Definition der Übermittlung, da die Daten zum Abruf bereitgehalten werden. Letztlich macht es für die Anwendung des Tatbestands keinen Unterschied, unter welche der beiden Tatbestandsoptionen die Nachrichten gefasst werden. In jedem Fall handelt es sich sowohl bei den eingehenden, als auch bei in die Mailbox eingestellten Emails um Daten im Sinne des § 202 a Abs. 2 StGB.

---

[240] *Kargl* in Kindhäuser/Neumann/Paeffgen, § 202 a StGB, Rn. 4; *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 3; *Schünemann* in Leipziger Komm., § 202 a StGB, Rn. 3; *Welp*, Iur 1988, S. 444

[241] *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 3; *Ders./Winkelbauer*, CR 1986, S. 485 f.; *Möhrenschlager*, wistra 1986, S. 140; *Schünemann* in Leipziger Kommentar, § 202 a StGB, Rn. 3; *Welp*, Iur 1988, S. 444

[242] *Lenckner*/*Winkelbauer*, CR 1986, S. 484; *Schünemann* in Leipziger Kommentar, § 202 a StGB, Rn. 4; *Tröndle*/*Fischer*, § 202 a StGB, Rn. 4; *Welp*, IuR 1988, S. 444 f.

[243] vgl.: 1. Kap. Teil 1 A. I. 3.

[244] *Kargl* in Kindhäuser/Neumann/Paeffgen, § 202 a StGB, Rn. 6; *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 4; *Tröndle*/*Fischer*, § 202 a StGB, Rn. 5; krit. zur Verwendungsklausel: *Welp*, IuR 1988, S. 446; vgl. zum BDSG: Neubekanntmachung des BDSG in der Form des Bekanntmachung v. 20.12.1990, BGBl. I, S. 2954 ff., in der ab 28.08.2002 geltenden Fassung

[245] *Hoyer* in Systematischer Kommentar, Rn. 3 f.; *Joeckl*, § 202 a StGB, Rn. 5; *Kargl* in Kindhäuser/Neumann/Paeffgen, § 202 a StGB, Rn. 6; *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 4; *Welp*, IuR 1988, S. 446

[246] *Ernst* in Ders., Hacker, Cracker & Computerviren, Rn. 272; *Tröndle*/*Fischer*, § 202 a StGB, Rn. 6; *Welp*, IuR 1988, S. 445 f.

b) Fremdheit der Daten

Zwar setzt der Wortlaut des § 303 a Abs. 1 StGB lediglich voraus, dass es sich bei den von der Tathandlung betroffenen Informationen um Daten im Sinne des § 202 a Abs. 2 StGB handelt. Jedoch verlangt die h.M. zusätzlich, dass die Daten fremd sind, das bedeutet, dass an ihnen ein unmittelbares Recht einer anderen Person auf Verarbeitung, Löschung oder Nutzung besteht, da nur durch diese Beschränkung in einer Art. 103 Abs. 2 GG genügenden Weise ein hinreichend bestimmtes Verhalten beschrieben werde.[247] Dabei wird das Kriterium der Fremdheit entweder als ungeschriebenes Tatbestandsmerkmal[248] oder als Voraussetzung der Rechtswidrigkeit[249] angesehen. Fraglich ist demnach, ob die betroffenen im Stadium der Übermittlung befindlichen oder bereits in die Mailbox eingestellten legitimen Nachrichten als fremd im vorgenannten Sinne anzusehen sind. Es ist somit zu prüfen, wem die Verfügungsberechtigung an den in den Emails enthaltenen Daten zusteht. Diese Frage gewinnt nicht nur an dieser Stelle, sondern auch im Hinblick auf die Berechtigung Bedeutung, den Strafantrag nach § 303 c StGB zu stellen.[250] Hinzu kommt, dass lediglich der Interessensträger der Tat durch seine Einwilligung die Rechtswidrigkeit nehmen kann.[251]

Im Rahmen der Kommunikation mittels Email lassen sich drei Phasen unterscheiden, in denen die Frage nach der Fremdheit der Daten möglicherweise unterschiedlich zu beurteilen ist und zwar der Zeitraum vor dem Absenden, zwischen Absenden und Einstellen der Nachricht in die Mailbox des Empfängers und danach.

Im Hinblick auf die erst- und letztgenannten Zeiträume besteht Einigkeit.
So soll die Verfügungsberechtigung zunächst demjenigen zukommen, der die Daten in einem Skripturakt erzeugt, also ihre Speicherung selbst unmittelbar bewirkt hat.[252] Dies bedeutet, dass der Absender zumindest so lange Verfügungsberechtigter über die in der Email enthaltenen Daten ist, bis er die Email durch Adressieren und Absenden aus seinem Einflussbereich entlässt.
Nach dem Einstellen der Email in das Postfach des Empfängers oder in einen Quarantäne-Ordner, auf den der Empfänger Zugriff hat, steht die Verfügungsberechtigung nach einhelliger Meinung dem Empfänger zu.[253]

Umstritten ist, wem die Verfügungsberechtigung über die Email in der Phase zwischen dem Versenden der Nachricht durch den Absender und ihrem Einstellen in der Mailbox des Empfängers zukommt. Hier werden im Wesentlichen drei Auffassungen vertreten. Einerseits soll ab dem Zeitpunkt des Absendens der Empfänger Verfügungsberechtigter sein,[254] andererseits wird davon ausgegangen, dass während des Übermittlungsvorgangs weder

---

[247] *Haft*, NStZ 1987, S. 10; *Hilgendorf*, JR 1994, S. 478; *Hoyer* in Systematischer Kommentar, § 303 a StGB, Rn. 5 f.; *Koecher*, DuD 2004, S. 274; *Lenckner*/*Winkelbauer*, CR 1986, S. 829; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 3; *Tolksdorf* in Leipziger Kommentar, § 303 a StGB, Rn. 5; *Tröndle*/*Fischer*, § 303 a StGB, Rn. 4; *Welp*, IuR 1988, S. 448; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 4
[248] *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 3; *Tröndle*/*Fischer*, § 303 a StGB, Rn. 4
[249] *Frommel*, JuS 1987, S. 667 f.; *Kitz*, CR 2005, S. 453
[250] *Stree* in Schönke/Schröder, § 303 c StGB, Rn. 3; *Tröndle*/*Fischer*, § 303 c StGB, Rn. 6; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 c StGB, Rn. 4
[251] *Lenckner*/*Winkelbauer*, CR 1986, S. 829; *Stree* in Schönke/Schröder, § 303 c StGB, Rn. 6; *Tolksdorf* in Leipziger Kommentar, § 303 a StGB, Rn. 37; *Tröndle*/*Fischer*, § 303 a StGB, Rn. 13
[252] BayObLG, JR 1994, S. 477; *Kitz*, CR 2005, S. 454
[253] *Hilgendorf*, JuS 1997, S. 325; *Jüngel*/*Schwan*/*Neumann*, MMR 2005, S. 824; *Tröndle*/*Fischer*, § 303 a StGB, Rn. 7
[254] *Kitz*, CR 2005, S. 454

Absender, noch Empfänger eine Verfügungsberechtigung zukommt,[255] während diese von einer dritten Auffassung dem Absender[256] zugewiesen wird.

Die erste Meinung, die den Empfänger als verfügungsberechtigt ansieht, beruft sich auf die Tatsache, dass das Verfügungsrecht ein eigentümerähnliches Interesse abbildet und stellt deshalb auf einen Vergleich mit der Rechtslage bei der Briefpost ab.[257] Dort sei für den Fall, dass der Übermittler Geheißperson sowohl des Absenders, als auch des Empfängers des versandten Briefes ist, von einem Eigentumserwerb des Empfängers bereits im Zeitpunkt der Einlieferung beim Postdienstleister auszugehen.[258] Gleiches gelte für die Kommunikation mittels Email; hier habe es der Empfänger in der Hand, durch entsprechende Anweisung an den Übermittler die Daten schon vor Zustellung seiner ausschließlichen Verfügungsgewalt zu unterwerfen.[259] Eine Verfügungsberechtigung des Absenders sei hingegen abzulehnen und lasse sich auch nicht daraus ableiten, dass der Absender in der Regel die Herrschaft über die Originaldaten behält, da beim Versenden grundsätzlich lediglich eine Kopie an den Adressaten übersandt wird,[260] während das Original beim Absender gespeichert bleibt.[261]
Für einen Übergang der Verfügungsberechtigung auf den Empfänger bereits im Zeitpunkt des Absendens der Email spricht daneben, dass ab diesem Zeitpunkt das Interesse des Absenders nicht mehr dahin geht, dass die Unversehrtheit der Daten gewährleistet sein soll. Denn grundsätzlich besteht für den Absender die Möglichkeit, die ausgehende Email in einem Ordner, der gesendete Nachrichten enthält, zu speichern.[262] In aller Regel geschieht dies sogar automatisch.[263] Ab dem Zeitpunkt, in dem der Absender die Email aus seiner Verfügungsbefugnis entlassen hat, kommt diesem damit kein Interesse mehr an der Unversehrtheit der Daten zu. Das Interesse ist vielmehr darauf gerichtet, dass die Email ordnungsgemäß zugestellt wird. Dieses von § 303 a StGB nicht erfasste Interesse wird durch § 206 Abs. 2 Nr. 2 StGB geschützt. Folglich spricht einiges dafür, dass die Verfügungsbefugnis bereits zu dem Zeitpunkt auf den Empfänger übergeht, zu dem der Absender die Email durch Adressieren und Absenden aus seinem Herrschaftsbereich entlässt.

Die Konstruktion über den Geheißerwerb ist allerdings problematisch. Es ist nicht ersichtlich, warum der Empfänger -selbst wenn er im Voraus Kenntnis davon hat, dass eine bestimmte Nachricht an in abgesandt wurde- den Übermittler als seine Geheißperson bezeichnen sollte. Denn letztlich liegt sein Interesse nicht in einer Übergabe an den Übermittler, sondern in einer Zustellung an ihn selbst. Erst Recht wird der Empfänger in der Regel kein Interesse an der Zusendung von Spammails haben und deshalb den Übermittler zumindest in diesen Fällen grundsätzlich nicht zu seiner Geheißperson machen.
Die Argumentation, die lediglich dem Empfänger der Daten ein geschütztes Interesse zugesteht, ist ebenfalls nicht zwingend. Zwar ist es richtig, dass für die Frage der Zuordnung darauf abzustellen ist, wer an der Unversehrtheit der Daten ein unmittelbares Interesse

---

[255] *Tröndle*/*Fischer*, § 303 a StGB, Rn. 7
[256] *Ernst*, Hacker, Cracker & Computerviren, Rn. 272; *Hilgendorf*, JuS 1997, S. 325; *Jüngel*/*Schwan*/*Neumann*, MMR 2005, S. 822
[257] *Kitz*, CR 2005, S. 454; zum Schutz eines eigentümerähnlichen Interesses: BT-Drs. 10/5058, S. 34; *Möhrenschlager*, wistra 1986, S. 141; *Stree* in Schönke/Schröder, Vorbem. §§ 303 ff. StGB, Rn. 1; *Tröndle*/*Fischer*, § 303 a StGB, Rn. 2; *Welp*, IuR 1988, 448; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 2
[258] *Kitz*, CR 2005, S. 454; vgl. auch: BGH, NJW 1973, S. 142; BGH, NJW 1974, S. 1133; BGH, NJW 1982, S. 2372; OLG Frankfurt, NJW-RR 1986, S. 471
[259] *Kitz*, CR 2005, S. 454
[260] *Kitz*, CR 2005, S. 454
[261] vgl.: 1. Kap. Teil 1 B. I.
[262] vgl.: 1. Kap. Teil 1 B. I.
[263] vgl.: 1. Kap. Teil 1 B. I.

besitzt.[264] Allerdings erschließt sich nicht, wieso ein solches lediglich dem Adressaten der Email vorbehalten sein soll. Denn zwar ist dieser als Empfänger der Daten vorgesehen, jedoch erlangt er bis zur Zustellung der Nachricht grundsätzlich keinerlei Rechtsposition an der an ihn adressierten Email.[265] Des Weiteren wird der Empfänger häufig kein Interesse am Erhalt der Email und in der Folge auch an der Unversehrtheit der Daten haben, so insbesondere bei unverlangter Werbepost. Insofern ist nicht ersichtlich, wieso einzig dem Adressaten ein Interesse an der Unversehrtheit der Daten zugesprochen werden soll. Hinzu kommt, dass hinsichtlich der Daten, die Gegenstand der Handlung des Täters sind, auf die konkrete Form der Speicherung abzustellen ist,[266] was dazu führt, dass das Vorhandensein inhaltsgleicher Daten auf anderen Datenträgern die Tatbestandsmäßigkeit gerade nicht ausschließt.[267] Folglich kann dem Absender der Nachricht auch nicht deshalb ein Interesse an der Unversehrtheit der in der versandten Version der Email enthaltenen Daten abgesprochen werden, weil er das Original der Email in seinem Einflussbereich behält. Es ist demnach nicht ersichtlich, wieso die Verfügungsberechtigung während der Übermittlungsphase bereits dem Empfänger zugewiesen werden soll.[268]

Die zweitgenannte Auffassung geht davon aus, dass weder der Absender noch der Adressat der Email im fraglichen Zeitraum verfügungsbefugt ist.[269]
Gegen diese Annahme spricht jedoch der Vergleich mit der in § 303 StGB geregelten Sachbeschädigung. § 303 a Abs. 1 StGB wurde erlassen, um diese Vorschrift zu ergänzen.[270] Im Rahmen des § 303 StGB entfällt das Tatbestandsmerkmal der Fremdheit lediglich dann, wenn die betroffene Sache herrenlos ist oder dem Täter selbst gehört.[271] Eine Sache, die gerade versandt wird, ist fremd im Sinne des § 303 StGB, da das Eigentum ursprünglich dem Absender zusteht und grundsätzlich erst mit Übergabe an den Empfänger übergeht, § 929 S. 1 BGB. Eine Phase, während der die Sache herrenlos ist, besteht demzufolge nicht. Dies spricht dafür, auch im Bereich des § 303 a StGB davon auszugehen, dass die Daten bereits fremd sind, bevor sie in die Mailbox des Empfängers eingestellt werden.
Hierfür lässt sich auch der in § 303 a Abs. 1 StGB enthaltene Verweis auf die Legaldefinition des Begriffs der Daten in § 202 a Abs. 2 StGB anführen. Dieser umfasst gespeicherte sowie übermittelte Informationen. Würde man Daten, die gerade übermittelt werden, stets mit dem Argument der fehlenden Fremdheit aus dem Tatbestand des § 303 a Abs. 1 StGB ausnehmen, so liefe der Verweis auf § 202 a Abs. 2 StGB teilweise leer. Denn letztlich könnten so übermittelte Daten niemals in den Anwendungsbereich des § 303 a Abs. 1 StGB fallen.
Demnach ist nicht davon auszugehen, dass das Kriterium der Fremdheit davon abhängt, dass die Nachricht bereits in die Mailbox des Empfängers eingestellt wurde.[272]

Schließlich besteht die Möglichkeit, die Verfügungsberechtigung während der Übermittlungsphase dem Absender zuzuweisen. Teilweise wird das Fortbestehen der Verfügungsberechtigung des Absenders auch nach Versenden der Nachricht damit begründet,

---

[264] BT-Drs. 10/5058, S. 34; *Bühler*, MDR 1987, S. 455; *Lenckner*/*Winkelbauer*, CR 1986, S. 829; *Möhrenschlager*, wistra 1986, S. 141; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 3; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 5
[265] *Jüngel*/*Schwan*/*Neumann*, MMR 2005, S. 822
[266] *Lenckner*/*Winkelbauer*, CR 1986, S. 829; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 7
[267] *Heidrich/Tschoepe*, MMR 2004, S. 79
[268] so im Ergebnis auch: *Jüngel/Schwan/Neumann*, MMR 2005, S. 822
[269] *Tröndle/Fischer*, § 303 a StGB, Rn. 7
[270] BT-Drs. 10/5058, S. 34
[271] *Tröndle/Fischer*, § 303 StGB, Rn. 4; *Stree* in Schönke/Schröder, § 303 StGB, Rn. 2; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 StGB, Rn. 4
[272] *Ernst*, NJW 2003, S. 3238; im Ergebnis: *Hoeren*, NJW 2004, S. 3516, *Spindler/Ernst*, CR 2004, S. 439; aA.: *Koecher*, DuD 2004, S. 274; *Tröndle/Fischer*, § 303 a StGB, Rn. 7

die Betreiber der Zwischenserver, welche die Email auf ihrem Weg zum Empfänger passiert, stünden „im Lager“ des Absenders.[273] Aufgrund der bestehenden Zugriffsmöglichkeit der Betreiber sei von einer Verfügungsberechtigung des Absenders auszugehen.[274] Diese Argumentation ist allerdings fragwürdig. Denn es ist nicht ersichtlich, warum die Betreiber der Zwischenserver gerade im Lager des Absenders stehen sollen, obwohl es sich hierbei um für diesen völlig Fremde handelt. Ebenso fehlt eine Begründung dafür, wieso diese Betreiber nicht umgekehrt der Sphäre des Empfängers zugeordnet werden sollen.
Aufgrund der Eigentumsähnlichkeit des Interesses ist vielmehr der Vergleich mit § 303 StGB entscheidend. Dort entfällt das Tatbestandsmerkmal wie erwähnt lediglich dann, wenn die betroffene Sache herrenlos ist oder dem Täter selbst gehört. Demnach ist auch eine Sache, die gerade versandt wird, fremd im Sinne des § 303 StGB. Sie steht bis zur Übereignung an den Empfänger im Eigentum des Absenders. Dies spricht dafür, auch im Bereich des § 303 a StGB davon auszugehen, dass die Daten der Verfügungsberechtigung des Absenders so lange unterliegen, bis sie in die Mailbox des Empfängers eingestellt werden. Schließlich würde der Verweis des § 303 a Abs. 1 StGB auf § 202 a Abs. 2 StGB teilweise leerlaufen, wenn übermittelte Daten dem Anwendungsbereich stets unter Hinweis auf die fehlende Fremdheit entzogen würde.
Aus den genannten Gründen ist davon auszugehen, dass die Verfügungsberechtigung während der Übermittlungsphase dem Absender zusteht.[275]
Im Ergebnis sind Emails auch in der Übermittlungsphase fremd.

c) Tathandlung

Fraglich ist, ob das Zustellen unverlangter Werbe-Emails als Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern der betroffenen legitimen Nachrichten qualifiziert werden kann, die deshalb nicht mehr zugehen oder vom Empfänger in der Mailbox nicht mehr aufgefunden werden.

In dem faktischen Blockieren der Nachrichten durch das Auffüllen der Mailbox könnte ein Unterdrücken von Daten liegen. Unterdrücken von Daten bedeutet, dass sie dem Zugriff des Berechtigten auf Dauer oder zeitweilig entzogen werden und er sie deshalb nicht verwenden kann.[276]
Hier wird zwar verhindert, dass der Empfänger auf die eingehende Email Zugriff nehmen kann. Allerdings kommt es im Hinblick auf die Zugriffsbefugnis nicht auf die Person des Empfängers, sondern auf die des Absenders an, da diesem, wie oben gezeigt,[277] bis zum Einstellen der Email in die Mailbox des Empfängers die Verfügungsberechtigung über die Daten zukommt.[278] Dem Absender wird die Verfügungsbefugnis jedoch nicht durch einen Dritten entzogen, vielmehr entlässt er die Email selbst durch das Versenden aus seinem Einflussbereich. Die Möglichkeit der Verwendung der konkret versandten Daten ist ihm somit ab diesem Zeitpunkt genommen und zwar unabhängig davon, ob die Email letztlich zugestellt wird oder nicht. Deshalb besteht auch, wie oben ausgeführt,[279] die Möglichkeit für den Absender, die Email im Ordner gesendete Nachrichten zu speichern.

---

[273] *Jüngel/Schwan/Neumann*, MMR 2005, S. 822
[274] *Jüngel/Schwan/Neumann*, MMR 2005, S. 822
[275] so auch im Ergebnis: *Ernst*, Hacker, Cracker & Computerviren, Rn. 272; *Hilgendorf*, JuS 1997, S. 325; *Jüngel/Schwan/Neumann*, MMR 2005, S. 822
[276] BT-Drs. 10/5058, S. 35; *Gravenreuth*, NStZ 1989, S. 206; *Hoyer*, Systematischer Kommentar, § 303 a StGB, Rn. 9; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tolksdorf* in Leipziger Kommentar, § 303 a StGB, Rn. 27; *Tröndle/Fischer*, § 303 a StGB, Rn. 10; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 8
[277] vgl.: 2. Kap. Teil 1 A. I. 1. b)
[278] *Ernst*, Hacker, Cracker & Computerviren, Rn. 272; *Hilgendorf*, JuS 1997, S. 325
[279] vgl.: 1. Kap. Teil 1 B. I.

Insofern verwirklicht der Täter nicht die Tathandlung des Unterdrückens im Sinne des § 303 a Abs. 1 StGB.[280]

Es könnte jedoch ein Unbrauchbarmachen von Daten im Sinne des § 303 a Abs. 1 StGB vorliegen.
Dies wird angenommen, wenn Daten in ihrer Gebrauchsfähigkeit so beeinträchtigt werden, dass sie nicht mehr ordnungsgemäß verwendet werden können und damit ihren bestimmungsgemäßen Zweck nicht mehr zu erfüllen vermögen.[281] Eine solche Wirkung kann auch durch Hinzufügen weiterer Daten erreicht werden.[282] Demnach werden die bereits in der Mailbox befindlichen Emails unbrauchbar gemacht, wenn es dem Nutzer aufgrund der Anzahl der elektronischen Werbenachrichten nicht mehr möglich ist, die legitimen und gewünschten Nachrichten herauszusuchen.[283] Allerdings wird dies eher selten und bei einer extrem hohen Anzahl an unerbetenen Nachrichten der Fall sein, die dem Empfänger innerhalb eines kurzen Zeitraums zugehen.

d) Kausalität

Fraglich ist, ob das Zustellen von Werbe-Emails kausal für die dargestellte Beeinträchtigung legitimer Nachrichten ist. Zweifel daran bestehen deshalb, da der einzelnen Nachricht die beschriebenen Auswirkungen nicht zukommen. Vielmehr ergeben sich die dargestellten Konsequenzen erst bei Zusammentreffen einer Vielzahl von Werbe-Emails.

Allerdings ist vom Vorliegen der erforderlichen Kausalität auszugehen, wenn mehrere unabhängig voneinander vorgenommene Handlungen den Erfolg erst durch ihr Zusammenwirken herbeiführen, wobei diese Konstellation als kumulative Kausalität bezeichnet wird.[284] Insofern ist vom Vorliegen der Kausalität auszugehen.

2. Subjektiver Tatbestand

Der für die Verwirklichung des subjektiven Tatbestands erforderliche Vorsatz könnte deshalb fehlen, weil die Mailbox nicht bereits durch die -möglicherweise einzige- durch den Täter versandte Nachricht überfüllt wird.[285] Allerdings ist davon auszugehen, dass der Täter den Umstand, dass neben seiner auch noch zahlreiche weitere Werbe-Nachrichten zugestellt werden, nicht nur für möglich hält, sondern hiermit angesichts des hohen Aufkommens solcher Nachrichten auch grundsätzlich rechnet.[286] Der Versender kennt somit die Konsequenzen seines Tuns. Demnach ist zumindest dolus eventualis zu bejahen, da der Täter den von ihm erkannten Erfolg billigend in Kauf nimmt.[287]

---

[280] im Ergebnis a.A.: *Frank*, CR 2004, S. 125
[281] BT Drucksache 10/5058, S. 35; *Gravenreuth*, NStZ 1989, S. 206; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4
[282] *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tröndle/Fischer*, § 303 a StGB, Rn. 11; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 9
[283] *Marberth- Kubicki*, Computer- und Internetstrafrecht, Rn. 88
[284] BGHSt 37, 131; *Lenckner* in Schönke/Schröder, Vorbem. §§ 13 StGB, Rn. 83; *Otto*, Jura 1992, S. 96; *Tröndle/Fischer*, vor § 13 StGB, Rn. 18
[285] *Frank*, CR 2004, S. 125; *Marberth- Kubicki*, Computer- und Internetstrafrecht, Rn. 88
[286] *Frank*, CR 2004, S. 125; zum Aufkommen an solchen Nachrichten: 1. Kap. Teil 1 B. II. 4.
[287] im Ergebnis auch: *Frank*, CR 2004, S. 125

3. Rechtswidrigkeit

Die Rechtswidrigkeit der Tat fehlt, wenn eine Einwilligung des Verfügungsberechtigten über die Daten vorliegt.[288] Diese muss den im Strafrecht geltenden Einwilligungserfordernissen genügen, insbesondere muss sie erklärt, das bedeutet nach außen kundbar gemacht worden sein, wobei nicht notwendig ist, dass die Erklärung an den Täter gerichtet und erst recht nicht, dass sie diesem im zivilrechtlichen Sinn zugegangen ist.[289]

4. Antragserfordernis, § 303 a StGB

§ 303 a StGB unterliegt dem Antragserfordernis des § 303 c StGB. Antragsberechtigt ist der Empfänger, da ihm die Verfügungsberechtigung hinsichtlich der in der Mailbox befindlichen Daten zukommt.

5. Zwischenergebnis

Als Ergebnis lässt sich festhalten, dass das Versenden unverlangter Werbe-Emails eine Verwirklichung des Tatbestands des § 303 a Abs. 1 StGB darstellt, wenn der Empfänger in kurzer Zeit so viele solche Nachrichten erhält, dass er diese nicht mehr von den legitimen Nachrichten unterscheiden kann.

II. Wettbewerbsrecht

Der Zulässigkeit unverlangter Email-Werbung könnten die §§ 3, 7 Abs. 1, Abs. 2 Nr. 3 des am 08.07.2004 in seiner Neufassung in Kraft getretenen UWG[290] entgegenstehen.[291]

Sollte der Versand von Werbe-Emails als Wettbewerbsverstoß anzusehen sein, so stünden anspruchsberechtigten Empfängern Schadensersatz- und Unterlassungsansprüche gegen den Absender[292] sowie gegebenenfalls dessen Auftraggeber[293] oder das Recht zu, den erzielten Gewinn abzuschöpfen, vgl. §§ 8 Abs. 1, 9, 10 Abs. 1 UWG. Anspruchsberechtigt sind dabei nach Maßgabe des § 8 Abs. 3 UWG nur Mitbewerber und bestimmte Verbände, während konkret betroffenen Gewerbetreibenden, die nicht in einem Wettbewerbsverhältnis zum Werbenden stehen, als mögliche Anspruchsgrundlagen lediglich die allgemeinen deliktsrechtlichen Vorschriften zur Verfügung stehen.[294]

---

[288] *Lenckner/Winkelbauer*, CR 1986, S. 829; *Tolksdorf* in Leipziger Kommentar, § 303 a StGB, Rn. 37; *Tröndle/Fischer*, § 303 a StGB, Rn. 13; *Stree* in Schönke/Schröder, § 303 c StGB, Rn. 6

[289] BGH, NJW 1956, S. 1106; BayObLG, NJW 1968, S. 665; OLG Oldenburg, NJW 1966, S. 2132; *Lenckner* in Schönke/Schröder, § Vorbem. §§ 32 ff. StGB, Rn. 43; *Tröndle/Fischer*, vor § 32 StGB, Rn. 3; a.A.: *Zitelmann*, AcP 1999, S. 1

[290] Gesetz gegen den unlauteren Wettbewerb, BGBl. I, S. 1414

[291] Die Vorschrift findet auch neben § 6 Abs. 1 und 2 des am 01.03.2007 in Kraft getretenen Telemediengesetzes, BGBl. 2007 I, S. 179 ff., Anwendung, wie sich aus § 6 Abs. 3 TMG ergibt. § 6 Abs. 1 TMG legt bestimmte Informationspflichten fest, Abs. 2 verbietet des Verschleiern oder Verheimlichen des kommerziellen Charakters einer Email in Kopf- und Betreffzeile.

[292] BGH, GRUR 2004, S. 517 ff.

[293] BGH, GRUR 1997, S. 315 - Architektenwettbewerb; BGH, GRUR 2002, S. 619- Meißner Dekor

[294] BT-Drs. 15/1487, S. 22; *OLG Oldenburg*, GRUR-RR 2004, S. 210; *Köhler* in Baumbach/Köhler/Bornkamm, § 1 UWG, Rn. 34; *Köhler*, GRUR 2003, S. 267; *Leistner/Pothmann*, WRP 2003, S. 815; *Lettl*, GRUR 2004, S. 460

Bereits vor Inkrafttreten der Neufassung des UWG waren von der unterinstanzlichen Rechtsprechung Grundsätze zur Zulässigkeit der Email-Direktwerbung entwickelt worden.[295] Das erste Urteil des Bundesgerichtshofs zu dieser Frage erging jedoch erst im Jahr 2004.[296] Zuvor hatte der Gerichtshof lediglich zur Zulässigkeit herkömmlicher Mittel des Direktmarketings Stellung genommen.[297] Allerdings ging die herrschende Meinung in der Literatur und unterinstanzlichen Rechtsprechung bereits vor dem Urteil des Bundesgerichtshofs aus dem Jahr 2004 davon aus, dass ohne das vorherige ausdrückliche oder stillschweigende Einverständnis des Adressaten abgesandte elektronische Werbenachrichten wettbewerbswidrig sind.[298] In seinem Urteil aus dem Jahr 2004, das noch vor Inkrafttreten der Neufassung des UWG erging, führte der Gerichtshof aus, dass unverlangte Email-Werbung gegen § 1 UWG in seiner alten Fassung verstößt.[299] Diese Feststellung begründete das Gericht damit, dass elektronische Werbenachrichten extrem kostengünstig versandt werden können und deshalb auf ein immer weiteres Umsichgreifen angelegt sind.[300] Daneben verwies der Bundesgerichtshof auf die gemeinschaftsrechtliche Vorschrift des Art. 13 Abs. 1 EK-DSRL,[301] die vorsieht, dass die Verwendung von elektronischer Post für Zwecke der Direktwerbung durch die Mitgliedstaaten nur bei vorheriger Einwilligung des Empfängers gestattet werden darf und stellte auf den durch solche Nachrichten anfallenden Zeit- und Kostenaufwand des Empfängers ab.[302]

Explizite Regelungen zur Email-Werbung finden sich seit der Neufassung des UWG in §§ 3, 7 Abs. 1 in Verbindung mit Abs. 2 Nr. 3.
§ 3 UWG erklärt unlautere Wettbewerbshandlungen, die geeignet sind, den Wettbewerb zum Nachteil der Mitbewerber, der Verbraucher oder der sonstigen Marktteilnehmer nicht nur unerheblich zu beeinträchtigen, für unzulässig. Nach § 7 Abs. 1 UWG handelt derjenige unlauter im Sinne des § 3 UWG, der einen Marktteilnehmer in unzumutbarer Weise belästigt. Eine unzumutbare Belästigung ist nach § 7 Abs. 2 Nr. 3 UWG insbesondere bei Werbung mittels elektronischer Post anzunehmen, die ohne Einwilligung des Adressaten erfolgt. Allerdings enthält § 7 Abs. 3 UWG eine Ausnahmeregelung, bei deren Eingreifen die Email-Werbung nicht als unzumutbare Belästigung anzusehen ist.
Neben der Unlauterkeit der Wettbewerbshandlung setzt § 3 UWG voraus, dass diese geeignet ist, den Wettbewerb zum Nachteil der Mitbewerber, der Verbraucher oder der sonstigen Marktteilnehmer nicht nur unerheblich zu beeinträchtigen. Da Werbe-Emails für den Empfänger in einem Zeit- und Kostenaufwand resultieren und zum Überlaufen seiner Mailbox führen können, ist davon auszugehen, dass diese Form der Direktwerbung geeignet

[295] LG Traunstein, NJW 1998, S. 1648 ff.; LG Hamburg, WRP 1999, S. 250; LG Braunschweig, NJW-CoR 2000, S. 235 f.
[296] BGH, GRUR 2004, S. 517, 518- Email- Werbung
[297] BGH, GRUR 1970, S. 523 ff.- Telefonwerbung I; BGH, GRUR 1973, S. 211- Telex – Werbung; BGH, NJW 1973, S. 1120; BGH, NJW 1988, S. 1671 f. - Btx- Werbung; BGH, GRUR 1989, S. 226- Handzettel-Wurfsendung; BGH, GRUR 1989, S. 753 ff. - Telefonwerbung II; BGH, GRUR 1990, S. 280 ff.- Telefonwerbung III; BGH, GRUR 1991, S. 764 ff.- Telefonwerbung IV; BGH, NJW 1992, S. 1109, 1110- Postwurfsendung; BGH, GRUR 1995, S. 220 ff.- Telefonwerbung V; BGH, WRP 1996, S. 102 = NJW 1996, S. 661 - Telefax- Werbung; BGH, NJW 1999, S. 1864 ff.; BGH, GRUR 2000, S. 818 ff. – Telefonwerbung VI
[298] BGH, GRUR 2004, S. 517, 518 - Email-Werbung; LG Traunstein, NJW 1998, S. 1648; LG Hamburg, WRP 1999, S. 250; *Gummig*, ZUM 1996, S. 583; *Hoeren*, WRP 1997, S. 994 f.; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 85; *Lange,* WRP 2002, S. 787 f.; a.A.: LG Braunschweig, NJW-CoR 2000, S. 235 f.; *Busche/Kraft*, WRP 1998, S. 1145 f. *Reichelsdorfer*, GRUR 1997, S. 197
[299] BGH, GRUR 2004, S. 518 -Email-Werbung
[300] BGH, GRUR 1988, S. 616 - Btx- Werbung; BGH, GRUR 2004, S. 518 - Email-Werbung
[301] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 105, S. 54 ff.
[302] BGH, GRUR 2004, S. 519 - Email-Werbung

ist, den Wettbewerb auf dem Markt nicht nur unerheblich zum Nachteil der Adressaten zu beeinträchtigen.[303]
Email-Werbung ist im Ergebnis nach § 7 Abs. 2 Nr. 3 UWG als unzumutbare Belästigung und damit gemäß §§ 3, 7 Abs. 1 UWG als unzulässig anzusehen, es sei denn der Adressat hat zuvor seine Einwilligung erklärt oder es liegt die in § 7 Abs. 3 UWG genannte Ausnahmekonstellation vor. Das Gesetz schreibt somit in § 7 Abs. 2 Nr. 3 UWG für den Bereich der Email-Werbung das Opt-In-Prinzip fest. § 7 Abs. 2 Nr. 3 UWG setzt Art. 13 Abs. 1 EK- DSRL in deutsches Recht um.[304]
§ 7 Abs. 3 UWG sieht vor, dass abweichend von Abs. 2 Nr. 3 eine unzumutbare Belästigung bei Werbung unter Verwendung elektronischer Post nicht anzunehmen ist, wenn ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, Abs. 3 Nr. 1, der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet, Abs. 3 Nr. 2, der Kunde der Verwendung nicht widersprochen hat, Abs. 3 Nr. 3 und dieser bei der Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere, als die Übermittlungskosten nach den Basistarifen entstehen, Abs. 3 Nr. 4. Somit legt § 7 Abs. 3 UWG für die in der Vorschrift genannten Fälle das Opt-Out-Prinzip fest. Diese Regelung entspricht weitgehend Art. 13 Abs. 2 EK- DSRL,[305] in deren Umsetzung sie erging und ist richtlinienkonform auszulegen.[306] Dabei hat der deutsche Gesetzgeber von der in Art. 13 Abs. 5 S. 2 EK-DSRL eröffneten Möglichkeit Gebrauch gemacht, die Regelung auch auf Direktwerbung gegenüber juristischen Personen zu erstrecken.

Als Ergebnis lässt sich festhalten, dass wettbewerbsrechtliche Vorschriften der Versendung unverlangter Email-Werbung entgegenstehen. Derjenige, der Email-Direktwerbung verschickt, handelt unlauter im Sinne der §§ 7 Abs. 1, Abs. 2 Nr. 3 in Verbindung mit § 3 UWG. Etwas anderes gilt nur dann, wenn der Empfänger der Nachricht zuvor seine Einwilligung erklärt hat oder wenn die in § 7 Abs. 3 UWG genannte Ausnahmekonstellation vorliegt.

III. Deliktsrecht

Dem uneingeschränkten Versand unverlangter kommerzieller Emails könnten darüber hinaus deliktsrechtliche Vorschriften, insbesondere § 823 Abs. 1 sowie Abs. 2 BGB in Verbindung mit § 249 Abs. 1 BGB bzw. § 1004 Abs. 1 BGB entgegenstehen.

---

[303] BGH, GRUR 1996, S. 209 zur Telefax-Werbung; BGH, GRUR 2004, 519-Email-Werbung; OLG Stuttgart, WRP 1995, S. 255; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 85; *Leupold*, WRP 1998, S. 270, 272; *Ohly* in Piper/Ohly, § 7 UWG, Rn. 63

[304] vgl. UWG, BGBl. I, S. 1414

[305] Nach Art. 13 Abs. 2 EK-DSRL gilt die Opt-Out-Lösung, wenn die Email-Adresse durch eine natürliche oder juristische Person im Zusammenhang mit dem Verkauf eines Produktes oder einer Dienstleistung gemäß der DSRL erlangt wurde, die Adresse zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwendet wird, der Kunde klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung seiner elektronischen Kontaktinformation bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, jedoch diese Nutzung nicht von vorneherein abgelehnt hat.

[306] *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 86; *Ohly* in Piper/Ohly, § 7 UWG, Rn. 14; allgemein zum Gebot der richtlinienkonformen Auslegung: EuGH, Rs. 14/83, Slg. 1984, S. 1909 - von Colson und Kamann/Land Nordrhein-Westfalen; EuGH, Rs. 79/83, Slg. 1984, S. 1942 - Harz/Deutsche Tradax; EuGH, Rs. 222/84, Slg. 1986, S. 1690 - Johnston/Chief Constable of the Royal Ulster Constabulary; EuGH, Rs. 31/87, Slg. 1988, S. 4655, 4662 - Beentjes/Niederlande; EuGH, Rs. C-106/89, Slg. 1990, S. I-4158 - Marleasing/La Commercial Internacional de Alimentación SA; EuGH, Rs. C-334/92, Slg. 1993, S. I-6932 - Wagner Miret/Fondo de garantía salarial; EuGH, Rs. C-91/92, Slg. 1994, S. I-3357 - Faccini Dori/Recreb

Hinsichtlich der Frage nach der deliktsrechtlichen Zulässigkeit unverlangter elektronischer Nachrichten stehen Emails karitativer oder politischer Organisationen der kommerziellen Direktwerbung gleich, da hier nicht auf den Inhalt der Email, sondern auf die Folgen für den Empfänger abgestellt wird.[307]

Bei einer Verletzung der durch die deliktischen Vorschriften geschützten Rechtsgüter bzw. Interessen können sich Schadensersatz- und Unterlassungsansprüche des Adressaten gegen das Unternehmen, das die Nachricht versandt hat, sowie gegebenenfalls dessen Auftraggeber ergeben.[308]

1. §§ 823 Abs. 1, 1004 Abs. 1 BGB

Das Versenden unverlangter Emails könnte nach dem Maßstab der §§ 823 Abs. 1, 1004 Abs. 1 BGB als unzulässig anzusehen sein. Dabei ist zu beachten, dass § 1004 Abs. 1 BGB zwar seinem Wortlaut nach nur das Eigentum schützt, nach einhelliger Auffassung allerdings auch sämtliche absoluten Rechte erfasst sind.[309]

Die genannten Vorschriften würden dem Versand elektronischer Direktwerbung entgegenstehen, wenn hierdurch ein durch § 823 Abs. 1 BGB geschütztes Rechtsgut verletzt würde (a), die Handlung für die Rechtsgutsverletzung haftungsbegründend kausal (b) sowie rechtswidrig wäre (c), bestimmte weitere Voraussetzungen wie Verschulden bzw. Wiederholungsgefahr vorlägen und keine Duldungspflicht bestünde (d).

a) Rechtsgutsverletzung

Der Versand elektronischer Direktwerbung könnte einerseits das allgemeine Persönlichkeitsrecht des Empfängers (aa), andererseits sein Recht auf den eingerichteten und ausgeübten Gewerbebetrieb (bb) verletzen.

aa) Verletzung des allgemeinen Persönlichkeitsrechts

Das allgemeine Persönlichkeitsrecht ist als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anerkannt.[310] Durch das Zusenden unerwünschter elektronischer Post könnte in dieses Recht eingegriffen werden. Zur Frage der Verletzung des allgemeinen Persönlichkeitsrechts durch Mittel der Direktwerbung nahm der Bundesgerichtshof bisher lediglich im Bereich herkömmlicher Werbeformen Stellung.[311] So verneint er im Fall der Briefkastenwerbung eine

---

[307] BVerfG, NJW 2002, S. 2938 f.; LG München, NJW-RR 2003, S. 764; KG, NJW 2002, S. 380; AG Rostock, NJW-RR 2003, S. 1282; Fritzemeyer, K & R 2005, S. 57; *Rixecker* in Münchener Kommentar, Anhang zu § 12 BGB, Rn. 97

[308] zur Person des Störers beim Anspruch aus § 1004 Abs. 1 BGB: BGH, NJW 1983, S. 751; BGH, NJW 2000, S. 2902; BGH, NJW-RR 2001, S. 232; *Bassenge* in Palandt, § 1004 BGB, Rn. 16 f.; *Gursky* in Staudinger, § 1004 BGB, Rn. 93; *Medicus* in Münchener Kommentar, § 1004 BGB, Rn. 53

[309] RGZ 60, S. 9; RGZ 61, S. 369; RGZ 116, S. 153; *Bassenge* in Palandt, § 1004 BGB, Rn. 3; *Gursky* in Staudinger, § 1004, Rn. 15 f.

[310] BGH, NJW 1954, S. 1404 f.; BGH, NJW 1956, S. 1555; BGH, NJW 1957, S. 1315; BGH, NJW 1958, S. 827; BGH, NJW 1958, S. 1344

[311] BGH, GRUR 1970, S. 524 - Telefonwerbung I; BGH, GRUR 1973, S. 211- Telex-Werbung; BGH, NJW 1973, S. 1120 - Briefkastenwerbung; BGH, NJW 1988, S. 1671 f. - Btx- Werbung; BGH, GRUR 1989, S. 225 - Handzettel-Wurfsendung; BGH, GRUR 1989, S. 754 - Telefonwerbung II; BGH, GRUR 1990, S. 281 - Telefonwerbung III; BGH, GRUR 1992, S. 617 - Briefkastenwerbung; BGH, NJW 1992, S. 1110 - Postwurfsendung; BGH, WRP 1996, S. 100 = NJW 1996, S. 660 - Telefax- Werbung; BGH, GRUR 2000, S. 819 - Telefonwerbung V; das Urteil BGH, CR 2004, S. 446 ff. - Email-Werbung betrifft lediglich den geschäftlichen Bereich

Verletzung des allgemeinen Persönlichkeitsrechts, da sich der Betroffene der Werbung relativ leicht entledigen könne.[312] Eine Persönlichkeitsrechtsverletzung liegt im Fall der Briefkastenwerbung lediglich dann vor, wenn ein auf dem Briefkasten angebrachter Vermerk, Werbung sei unerwünscht, nicht beachtet wird.[313] Gleiches gilt für unerwünschte politische Werbung.[314] Die Telefonwerbung wertet der Bundesgerichtshof hingegen als Eingriff in das allgemeine Persönlichkeitsrecht, da sich der Angerufene unter Überwindung relativ hoher psychologischer Barrieren des Anrufers entledigen muss und der Belästigungsgrad durch die unmittelbare Kontaktaufnahme höher ist, als im Fall der Briefkastenwerbung.[315] Da im Bereich der übrigen herkömmlichen Werbeformen in der Regel geschäftliche Anschlüsse betroffen waren, nahm der Bundesgerichtshof zur Frage der Persönlichkeitsrechtsverletzung in diesem Bereich nicht Stellung.

Die Beantwortung der Frage danach, ob Email-Werbung als Persönlichkeitsverletzung zu werten ist, hängt entscheidend davon ab, mit welcher herkömmlichen Werbeform die Email-Werbung am ehesten vergleichbar ist.
Gegen die Beeinträchtigung des Persönlichkeitsrechts durch Email-Werbung spricht einerseits die fehlende Vergleichbarkeit mit der Telefonwerbung, die sich daraus ergibt, dass eine einem Telefonanruf ähnelnde direkte Ansprache hier gerade nicht vorliegt.[316] Insofern könnte davon ausgegangen werden, dass Email-Werbung eher mit der Briefkastenwerbung vergleichbar ist,[317] die ausweislich der soeben zitierten Rechtsprechung des Bundesgerichtshofs vom Betroffenen grundsätzlich hinzunehmen ist. Allerdings führen auch Werbe-Emails dazu, dass der Empfänger mit Werbung konfrontiert wird, die er möglicherweise gar nicht erhalten möchte und mit der er sich dennoch auseinandersetzen muss.[318] Er wird daran gehindert, seine Zeit wie gewünscht zu verbringen, da er sich mit dem Aussortieren der elektronischen Werbepost beschäftigen muss. Hinsichtlich der Vergleichbarkeit mit der Briefkastenwerbung bestehen Bedenken. Denn Email-Werbung kann unverhältnismäßig leichter realisiert werden, als die herkömmliche Brief- oder Handzettelwerbung.[319] Diese Werbemittel erfordern einen erheblich größeren finanziellen und zeitlichen Aufwand, als die Email-Werbung, bei der das Werbemittel nur einmal erstellt zu werden braucht, um es anschließend kostengünstig, automatisiert und in beliebiger Anzahl zu versenden.[320] Auch ist zu beachten, dass die einschlägige Rechtsprechung zur Brief- und Handzettel-Werbung darauf abstellt, dass der Adressat mittels Aufkleber auf dem Briefkasten den Einwurf verhindern kann.[321] Gerade dies ist aber im Bereich der Email-Werbung nicht möglich.[322] Schließlich spricht auch die

---

[312] BGH, NJW 1973, S. 1120 - Briefkastenwerbung; BGH, GRUR 1989, S. 225 - Handzettel-Wurfsendung; BGH, GRUR 1992, S. 617 - Briefkastenwerbung; BGH, NJW 1992, S. 1110 - Postwurfsendung
[313] BGH, NJW 1973, S. 1120 - Briefkastenwerbung; BGH, GRUR 1989, S. 225 - Handzettel-Wurfsendung; BGH, GRUR 1992, S. 617 - Briefkastenwerbung; BGH, NJW 1992, S. 1110 - Postwurfsendung
[314] OLG Bremen, NJW 1990, S. 2140 f.
[315] BGH, GRUR 1970, S. 524 - Telefonwerbung I; BGH, GRUR 1989, S. 754 - Telefonwerbung II; BGH, GRUR 1990, S. 281 - Telefonwerbung III, BGH, GRUR 2000, S. 819 - Telefonwerbung V; *Spindler/Schmittmann*, MMR 2001/Beilage 8, S. 12
[316] *Spindler/Schmittmann*, MMR 2001/Beilage 8, S. 12
[317] *Leupold/Bräutigam/Pfeiffer*, WRP 2000, S. 592 f.; *Reichelsdorfer*, GRUR 1997, S. 197
[318] LG Kiel, MMR 2000, S. 706; LG Berlin, MMR 2003, S. 420; AG Brakel, MMR 1998, S. 492; *Ernst/Seichter*, MMR 2006, S. 780; *Spindler/Schmittmann*, MMR 2001, Beilage 8, S. 13 f.;*Wendlandt*, MMR 2004, S. 366; für die SMS-Werbung: *Schmittmann*, MMR 1998, 348
[319] BGH, CR 2004, S. 447- Email-Werbung; LG Kiel, MMR 2000, S. 706; LG Berlin, NJOZ 2001, S. 202 f.; KG, NJOZ 2002, S. 2204; *Ernst/Seichter*, MMR 2006, S. 780; *Spindler/Schmittmann*, MMR 2001/Beilage 8, S. 13; *Wendlandt*, MMR 2004, S. 36
[320] BGH, CR 2004, S. 447 - Email-Werbung ; LG Kiel, MMR 2000, S. 706; *Spindler/Schmittmann*, MMR 2001/Beilage 8, S. 13; vgl. auch: 1. Kap. Teil 1 B. II. 4.
[321] BGH, NJW 1973, S. 1119 ff. - Briefkastenwerbung; BGH, GRUR 1989, S. 225 ff.- Handzettel-Wurfsendung; BGH, NJW 1992, S. 1109 ff. - Postwurfsendung; BGH, GRUR 1992, S. 617 ff. - Briefkastenwerbung
[322] *Spindler/Schmittmann*, MMR 2001/Beilage 8, S. 13

Tatsache, dass die unverlangte Werbung mittels elektronischer Post nach der Neufassung des UWG grundsätzlich als unzumutbare Belästigung zu qualifizieren ist, § 7 Abs. 2 Nr. 3 UWG, für eine Persönlichkeitsverletzung. Denn es ist kein Grund ersichtlich, die Situation im allgemeinen Deliktsrecht anders zu behandeln, als im Wettbewerbsrecht.

Demnach ist davon auszugehen, dass unverlangte Werbung mittels Email einen Eingriff in das allgemeine Persönlichkeitsrecht des Empfängers darstellt. Dieses Ergebnis entspricht auch der nahezu einhelligen Rechtsprechung der Instanzengerichte und der Literatur.[323] Etwas anderes gilt allerdings aufgrund der gebotenen richtlinienkonformen Auslegung unter Berücksichtigung des Art. 13 Abs. 2 EK-DSRL, dem im Wettbewerbsrecht § 7 Abs. 3 UWG entspricht, im Rahmen bestehender Kundenbeziehungen im Sinne der genannten Vorschriften.[324]

bb) Verletzung des Rechts auf den eingerichteten und ausgeübten Gewerbebetrieb

Durch die Zustellung unverlangter Email-Werbung an Gewerbetreibende könnte in deren Recht auf den eingerichteten und ausgeübten Gewerbebetrieb eingegriffen werden. Dieses Recht ist als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anerkannt.[325] Es handelt sich um einen offenen Auffangtatbestand,[326] der eine sonst bestehende Lücke insbesondere im gewerblichen Rechtsschutz schließen soll.[327] Inhalt und Grenzen des Schutzes einschließlich der Rechtswidrigkeit des Eingriffs ergeben sich aber entsprechend der Natur als offener Tatbestand erst aus einer Interessens- und Güterabwägung mit der im Einzelfall kollidierenden Interessenssphäre.[328] Das Recht schützt den Betriebsinhaber gegen Beeinträchtigungen der bisher rechtmäßig ausgeübten Tätigkeit.[329] Es umfasst dabei alles, was in seiner Gesamtheit den wirtschaftlichen Wert des Betriebs ausmacht, also Bestand, Erscheinungsform, Tätigkeitskreis und Kundenstamm.[330]

Die Rechtsprechung begründet das Vorliegen eines Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb durch Email-Direktwerbung häufig mit einem Hinweis auf den für das Aussortieren anfallenden Zeit- und Kostenaufwand.[331] Jedoch wird das

---

[323] LG Berlin, MMR 2000, S. 571; LG Berlin, MMR 2000, S. 704; LG Kiel, MMR 2000, S. 706; LG Berlin, NJOZ 2001, S. 202 f.; LG Berlin, MMR 2003, S. 420; KG, NJOZ 2002, S. 2204; AG Brakel, MMR 1998, S. 492 unter Verweis auf BGH, NJW 1989, S. 902; *Brömmelmeyer*, GRUR 2006, S. 289; *Ernst/Seichter*, MMR 2006, S. 780; *Spindler/Schmittmann*, MMR 2001, Beilage 8, S. 13 f.; *Wendlandt*, MMR 2004, S. 366; für die SMS-Werbung: *Schmittmann*, MMR 1998, S. 348; aA.: AG Kiel, K & R 2000, S. 201; *Ohly* in Piper/Ohly, § 7 UWG, Rn. 19; *Rixecker* in Münchener Kommentar, Anh. § 12 BGB, Rn. 99

[324] vgl. dazu: 2. Kap. Teil 1 A. II.

[325] BGHZ 69, S. 138 f.; BGHZ 90, S. 123; OLG Nürnberg, MDR 1983, S. 667

[326] BGH, NJW 1957, S. 1315; BGH, NJW 1963, S. 531; BGH, NJW 1979, S. 1351; *Hager* in Staudinger, BGB Kommentar, § 823 BGB, Rn. D 2; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 104; *Sprau* in Palandt, § 823 BGB, Rn. 126

[327] BGH, NJW 1966, S. 1618; BGH, NJW 1977, S. 2265; BGH NJW 2003, S. 1041; *Hager* in Staudinger, BGB Kommentar, § 823 BGB, Rn. D 2; *Sprau* in Palandt, BGB Kommentar, § 823 BGB, Rn. 126

[328] BGH, NJW 1984, S. 1607; BGH, NJW 1998, S. 2141; BGH, NJW 2005, S. 2770; *Hager* in Staudinger, BGB Kommentar, § 823 BGB, Rn. D 4; *Mertens* in Münchener Kommentar, § 823 BGB, Rn. 481; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 112; *Sprau* in Palandt, BGB Kommentar, § 823 BGB, Rn. 126

[329] BGH, NJW 1969, S. 1207 f.; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 105; *Sprau* in Palandt, § 823 BGB, Rn. 127; *Teichmann* in Jauernig, § 823 BGB, Rn. 97

[330] BGH, NJW 1952, S. 660; BGH, NJW 1953, S. 297; BGH, NJW 1957, S. 630; BGH, NJW 1959, S. 479; BGH, NJW 1987, S. 2225; BGH, NJW 1990, S. 52; *Hager* in Staudinger, § 823 BGB, Rn. D 9; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 105; *Sprau* in Palandt, § 823 BGB, Rn. 127

[331] LG Berlin, CR 1998, S. 623; LG Berlin, MMR 1999, S. 43; AG Charlottenburg, MMR 2000, S. 775; im Bereich des Wettbewerbsrechts: BGH, CR 2004, S. 445 -Email-Werbung; LG Traunstein, MMR 1998, S. 54; LG Berlin, NJW 2002, S. 2570; LG München I, MMR 2003, S. 484

Kostenargument teilweise als fragwürdig angesehen, da in Folge dieser Argumentation die an sich deliktsrechtlich nicht schutzfähige[332] Vermögensverletzung ersatzfähig wird.[333] Allerdings ist das Kostenargument durchaus schlagkräftig, wie auch der europäische Gesetzgeber in Erwägungsgrund Nr. 30 ECRL anerkennt und sind die entstehenden Kosten nicht die einzigen negativen Folgen des Direktmarketings mittels Email.[334] Denn, wie bereits angemerkt, kann es hierdurch auch zu Datenverlusten kommen.[335] Daneben haben der Empfänger oder seine Angestellten Zeit für das Aussortieren und Löschen der Nachrichten aufzuwenden, während der sie für andere Arbeiten im Betrieb nicht zur Verfügung stehen.[336] Daher ist davon auszugehen, dass die Gesamtheit der aus der werblichen Ansprache mittels elektronischer Post folgenden Nachteile in einem Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb resultiert.[337]

Dieser muss jedoch, um eine Beeinträchtigung der §§ 823 Abs. 1, 1004 Abs. 1 BGB zu bewirken, betriebsbezogen sein.[338] Das Merkmal der Betriebsbezogenheit erfordert, dass der Eingriff „irgendwie“ gegen den Betrieb gerichtet ist bzw. die Grundlagen des Betriebs bedroht oder gerade den Funktionszusammenhang der Betriebsmittel auf längere Zeit aufhebt.[339] Mittelbare Beeinträchtigungen verletzen das Recht hingegen nicht.[340]
Zwar wird durch das Zustellen von unerbetenen Werbenachrichten die betriebliche Email-Kommunikation verlangsamt, wenn sie nicht sogar durch Überquellen des elektronischen Briefkastens unmöglich gemacht wird. Auch verlieren Angestellte durch das Aussortieren der Nachrichten Zeit.[341] Allerdings lässt sich der Eingriff -selbst wenn das Zustellen einer großen Anzahl solcher Nachrichten dazu führen würde, dass die betriebliche Kommunikation deutlich verlangsamt oder teilweise sogar blockiert wird- nicht als betriebsbezogen qualifizieren. Dies ergibt sich daraus, dass selbst in der Unterbrechung der betrieblichen Telefonleitung[342] oder Stromzufuhr durch Kabelverletzungen[343] nach der Rechtsprechung kein betriebsbezogener Eingriff zu sehen ist. Ein solcher ist folglich auch nicht deshalb anzunehmen, weil Angestellte ihre Arbeitszeit für das Aussortieren aufwenden müssen oder weil sich die betriebliche Kommunikation verlangsamt oder blockiert wird.[344]

---

[332] RGZ 51, S. 93; RGZ 52, S. 366; RGZ 58, S. 28; RGZ 62, S. 317; RGZ 95, S. 174; BGHZ 27, S. 140; BGHZ 41, S. 126 f.; BGH, NJW 1978, S. 2028; BGH, NJW 1992, S. 1512; OLG München, NJW 1980, S. 1582; *Hager* in Staudinger, Vorbem. §§ 823 ff. BGB, Rn. 20, § 823 BGB, Rn. B 192; *Teichmann* in Jauernig, § 823 BGB, Rn. 19; *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 176 ff.
[333] *Ayad*, CR 2001, S. 540
[334] *Ayad*, CR 2001, S. 540
[335] vgl.: 1. Kap. Teil 1 B. II. 4.
[336] vgl.: 1. Kap. Teil 1 B. II. 4.
[337] OLG Düsseldorf, MMR 2006, S. 682; LG Berlin, CR 1998, S. 623; LG Berlin, MMR 1999, S. 43; LG Berlin, NJW 2002, S. 2570; LG München I, MMR 2003, S. 484; AG Charlottenburg, MMR 2000, S. 775; *Ernst/Seichter*, MMR 2006, S. 780; *Köhler* in Baumbach/Köhler/Bornkkamm, UWG, § 7 UWG, Rn. 84; *Leistner/Pohlmann*, WRP 2003, S. 817; *Spindler/Schmittmann*, MMR 2001, Beilage 8, S. 15; *Wendlandt*, MMR 2005, S. 366 f.
[338] RGZ 132, S. 316; RGZ 158, S. 379; RGZ 163, S. 32; BGH, NJW 1951, S. 644; BGH, NJW 1952, S.661; BGH, NJW 1959, S. 481; BGH, NJW 1964, S. 720; *Hager* in Staudinger, § 823 BGB, Rn. D 11; *Sprau* in Palandt, § 823 BGB, Rn. 126 ff.; *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 185
[339] BGHZ 29, S. 72; BGHZ 55, S. 161; BGH, NJW 1983, S. 813; OLG Oldenburg, NJW-RR 2005, S. 614; AG Tauberbischofsheim, NJW-RR 1993, S. 482; *Hager* in Staudinger, BGB Kommentar, § 823 BGB, Rn. D 11; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 105 ff.; *Teichmann* in Jauernig, § 823 BGB, Rn. 98
[340] RGZ 132, S. 316; RGZ 158, S. 379; RGZ 163, S. 32; BGH, NJW 1959, S. 481
[341] vgl.: 1. Kap. Teil 1 B. II. 4.
[342] LG Hamburg, NJW-RR 2004, S. 23
[343] BGH, NJW 1959, S. 479 f.; BGH, NJW 1964, S. 722; BGH, NJW 1968, S. 1280; BGH, BB 1977, S. 1419
[344] AG München, CR 2004, S. 379; AG Dresden, NJW 2005, S. 2562; *Baetge*, NJW 2006, S. 1039; *Reichelsdorfer*, GRUR 1997, S. 197; im Bereich der Telefonwerbung: *Böhm*, MMR 1999, S. 644; a.A. die h.M. in der Rspr. u. Lit.: LG Traunstein, NJW 1998, S. 1648; LG Berlin, CR 1998, S. 623; LG Berlin, MMR 1999, S. 43; LG Berlin, NJW-RR 2000, S. 1230; LG Berlin, NJW-RR 2001, S. 628 f.; AG Charlottenburg, MMR 2000,

Demnach stellt das Zustellen von unverlangter Email-Werbung keinen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb dar.[345]

b) Haftungsbegründende Kausalität

Es stellt sich die Frage nach der haftungsbegründenden Kausalität. Da der Absender an den Empfänger möglicherweise nur eine einzige elektronische Werbenachricht versandt hat, bestehen Zweifel am Vorliegen dieses Merkmals. Allerdings besteht die Gefahr von elektronischer Werbepost oder anderen massenhaft versandten Emails gerade darin, dass diese an eine nicht überschaubare Anzahl von Empfängern versandt wird, was die beschriebenen Beeinträchtigungen der Empfänger sowie des Internet zur Folge hat. Insofern muss es möglich sein, jeden einzelnen Mitverursacher für die Gesamtwirkung verantwortlich zu machen, da ansonsten keine Handhabe gegen diese Art von Belästigung bestünde.[346]

Dogmatisch lässt sich die Haftung der einzelnen Mitverursacher begründen, indem man die allgemeinen für die Kausalität geltenden rechtlichen Grundsätze heranzieht. Denn für die haftungsbegründende Kausalität ist Mitursächlichkeit grundsätzlich ausreichend.[347] Dies bedeutet, dass ein Zurechnungszusammenhang auch dann gegeben ist, wenn die Handlung des Schädigers nicht allein, sondern nur im Zusammenwirken mit dem Handeln eines Anderen die Rechtsgutsbeeinträchtigung herbeiführen konnte, wobei diese Konstellation als Gesamtkausalität bzw. kumulative Kausalität bezeichnet wird.[348] Hier ist ein Fall der Gesamtkausalität gegeben. Denn eine einzelne Werbe-Email verursacht zwar noch nicht die genannten negativen Auswirkungen. Jedoch werden diese durch das Zusammentreffen mehrerer elektronischer Nachrichten bewirkt. Demnach ist davon auszugehen, dass die Handlung jedes einzelnen Versenders von Email-Werbung kausal für die jeweils eintretende Rechtsgutsbeeinträchtigung ist.[349]

S. 775; *Hoeren*, NJW 2004, 3513 f.; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 84; *Leistner/Pothmann*, WRP 2003, S. 817; *Wendlandt*, MMR 2005, S. 366 f.

[345] AG München, CR 2004, S. 379; AG Dresden, NJW 2005, S. 2562; *Baetge*, NJW 2006, S. 1039 f.; *Brömmelmeyer*, GRUR 2006, S. 289 f.; *Ohly* in Piper/Ohly, § 7 UWG, Rn. 22; für die Telefonwerbung: *Schricker*, GRUR Int. 1998, S. 549 unter Verweis auf BGH, NJW 1977, S. 2264 ff.; a.A. die h.M. in der Rspr. u. Lit.: OLG Düsseldorf, MMR 2006, S. 682; LG Traunstein, NJW 1998, S. 1648; LG Berlin, CR 1998, S. 623; LG Berlin, MMR 1999, S. 43; AG Charlottenburg, MMR 2000, S. 775; LG Berlin, NJW-RR 2000, S. 1230; LG Berlin, NJW-RR 2001, S. 628 f.; *Hoeren*, NJW 2004, S. 3513 f.; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 84; *Leistner/Pothmann*, WRP 2003, S. 817; *Wendlandt*, MMR 2005, S. 366 f.

[346] im Ergebnis: LG Berlin, MMR 1999, S. 44; LG Berlin, MMR 2000, S. 571; LG Berlin, MMR 2000, S. 704; LG Kiel, MMR 2000, S. 706; LG Berlin, NJOZ 2001, S. 202 f.; LG Berlin, MMR 2003, S. 420; KG, NJOZ 2002, S. 2204; AG Brakel, MMR 1998, S. 492 unter Verweis auf BGH, NJW 1989, S. 902; *Ernst/Seichter*, MMR 2006, S. 780; *Spindler/Schmittmann*, MMR 2001, Beilage 8, S. 13 f.; *Wendlandt*, MMR 2004, S. 366; für die SMS-Werbung: *Schmittmann*, MMR 1998, S. 348; aA.: OLG Düsseldorf, MMR 2006, S. 682; LG Traunstein, NJW 1998, S. 1648; LG Berlin, CR 1998, S. 623; LG Berlin, MMR 1999, S. 43; LG Berlin, NJW-RR 2000, S. 1230; LG Berlin, NJW-RR 2001, S. 628 f.; AG Kiel, K & R 2000, S. 201; AG Charlottenburg, MMR 2000, S. 775; *Hoeren*, NJW 2004, S. 3513 f.; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 84; *Leistner/Pothmann*, WRP 2003, S. 817

[347] BGH, NJW-RR 1999, S. 819; BGH, NJW 2000, S. 3424; BGH, NJW 2002, S. 2709; BGH, NJW-RR 2005, S. 897; BGH, NJW-RR 2006, S. 673

[348] BGH, NJW 1990, S. 2884; BGH, NJW 2002, S. 2708 f.

[349] LG Berlin, MMR 1999, S. 44; LG Berlin, MMR 2000, S. 571; LG Berlin, MMR 2000, S. 704; LG Kiel, MMR 2000, S. 706; LG Berlin, NJOZ 2001, S. 202 f.; LG Berlin, MMR 2003, S. 420; KG, NJOZ 2002, S. 2204; AG Brakel, MMR 1998, S. 492 unter Verweis auf BGH, NJW 1989, S. 902; *Ernst/Seichter*, MMR 2006, S. 780; *Spindler/Schmittmann*, MMR 2001, Beilage 8, S. 13 f.; *Wendlandt*, MMR 2004, S. 366; für die SMS-Werbung: *Schmittmann*, MMR 1998, S. 348; aA.: OLG Düsseldorf, MMR 2006, S. 682; LG Traunstein, NJW 1998, S. 1648; LG Berlin, CR 1998, S. 623; LG Berlin, MMR 1999, S. 43; LG Berlin, NJW-RR 2000, S. 1230; LG Berlin, NJW-RR 2001, S. 628 f.; AG Kiel, K & R 2000, S. 201; AG Charlottenburg, MMR 2000, S. 775;

c) Rechtswidrigkeit

Im Rahmen der Rechtfertigung der Eingriffe werden zwei Aspekte relevant und zwar zum einen das Erfordernis der Widerrechtlichkeit (aa), zum anderen die Frage nach Rechtfertigungsgründen für den Eingriff (bb).

aa) Widerrechtlichkeit

Voraussetzung eines Abwehr- oder Ersatzanspruchs ist, dass der Eingriff widerrechtlich ist. Da es sich beim allgemeinen Persönlichkeitsrecht um einen so genannten offenen Tatbestand handelt, gilt hier nicht der Grundsatz, dass die Tatbestandsmäßigkeit die Rechtswidrigkeit indiziert.[350] Vielmehr muss in jedem Einzelfall unter sorgsamer Würdigung aller Umstände festgestellt werden, ob der Eingriff befugt war oder nicht, was durch eine Güter- und Interessenabwägung festzustellen ist.[351] Dabei fällt auf Seiten des Empfängers sein allgemeine Persönlichkeitsrecht ins Gewicht. Auf Seiten des Versenders bzw. seines Auftraggebers ist hingegen zu berücksichtigen, dass ein Interesse daran besteht, für Produkte oder Dienstleistungen zu werben bzw. werben zu lassen.
Allerdings besteht kein Grund, die Zustellung unverlangter Werbepost uneingeschränkt, das bedeutet ohne vorheriges Einverständnis des Empfängers, als zulässig anzusehen. Im Rahmen der Interessens- und Güterabwägung ist auch den gemeinschaftsrechtlichen Vorschriften, insbesondere Art. 13 EK- DSRL Rechnung zu tragen.[352] Folglich ist von Bedeutung, dass Art. 13 Abs. 1 EK- DSRL eine -wenngleich abgeschwächte- Opt-In-Lösung vorschreibt. Demnach ist von einem widerrechtlichen Eingriff auszugehen, wenn Email-Direktwerbung versandt wird, ohne dass der Adressat zuvor seine Einwilligung erklärt hat.

bb) Rechtfertigungsgründe

Das Zusenden einer Werbe-Email ist gerechtfertigt, wenn der Empfänger zuvor seine Einwilligung erklärt hat.

d) Weitere Voraussetzungen

Fraglich ist, ob das im Rahmen des § 823 Abs. 1 BGB erforderliche Verschulden gegeben ist. Hier gilt grundsätzlich das Gleiche, wie im Bereich des Strafrechts,[353] weshalb in der Regel von Vorsatz, zumindest jedoch von Fahrlässigkeit auszugehen ist. Verschulden im Sinne des § 276 Abs. 1 BGB liegt demnach vor.

§ 1004 Abs. 1 BGB setzt das Bestehen einer Wiederholungsgefahr sowie das Fehlen einer Duldungspflicht voraus. Dabei besteht eine tatsächliche Vermutung der Wiederholungsgefahr im Sinne des § 1004 Abs. 1 BGB, die bereits durch die vorangegangene rechtswidrige Beeinträchtigung begründet wird.[354] Im Übrigen ist zu erwarten, dass sich die Versender des

---

Hoeren, NJW 2004, S. 3513 f.; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 84; *Leistner/Pothmann*, WRP 2003, S. 817

[350] BGH, NJW 1959, S. 526; BGH, NJW 1978, S. 753; BGH, NJW 1987, S. 2668; *Hager* in Staudinger, § 823 BGB, Rn. C 17; *Sprau* in Palandt, BGB Kommentar, § 823 BGB, Rn. 95

[351] BGH, NJW 1959, S. 526; BGH, NJW 1978, S. 753; BGH, NJW 1987, S. 2668; *Hager* in Staudinger, § 823 BGB, Rn. C 17; *Sprau* in Palandt, BGB Kommentar, § 823 BGB, Rn. 95

[352] BGHZ 13, S. 338; BGHZ 24, S. 80; *Eckhardt*, MMR 2003, S. 561; *Günther*, CR 1999, S. 180; *Hager* in Staudinger, § 823 BGB, Rn. C 16; *Sprau* in Palandt, § 823 BGB, Rn. 95, 126

[353] vgl. dazu: 2. Kap. Teil 1 A. I. 2.

[354] *Bassenge* in Palandt, § 1004 BGB, Rn. 32; *Medicus* in Münchener Kommentar, § 1004 BGB, Rn. 95

Kommunikationsmittels aufgrund seines Zeit- und Kostenvorteils auch weiter bedienen werden. Vom Vorliegen der Wiederholungsgefahr ist folglich auszugehen.
Der Anspruch ist auch nicht nach § 1004 Abs. 2 BGB ausgeschlossen. Eine Duldungspflicht besteht grundsätzlich nicht, es sei denn der Empfänger hat zuvor eingewilligt.[355]

2. §§ 823 Abs. 2, 1004 Abs. 1 BGB

Daneben könnten auch die §§ 823 Abs. 2, 1004 Abs. 1 BGB der Zulässigkeit unverlangter Email-Werbung entgegenstehen. Es wurde bereits dargestellt, dass § 1004 Abs. 1 BGB zwar seinem Wortlaut nach nur das Eigentum schützt, nach einhelliger Auffassung allerdings auch die durch § 823 Abs. 2 BGB geschützten Rechtsgüter von der Vorschrift erfasst sind. [356] § 823 Abs. 2 BGB setzt die Verletzung eines Schutzgesetzes voraus. Schutzgesetz im Sinne des § 823 Abs. 2 BGB ist jede Rechtsnorm im Sinne des Art. 2 EGBGB,[357] die gezielt dem Individualschutz dient.[358] Dabei muss der Individualschutz nicht alleiniges Anliegen der Norm sein, ausreichend ist vielmehr, dass die Vorschrift neben der Allgemeinheit auch den Einzelnen schützen möchte.[359] Die Schutzgesetzeigenschaft wird sogar dann bejaht, wenn das Gesetz in erster Linie Allgemein- und lediglich daneben auch Individualinteressen schützt.[360] Unabdingbare Voraussetzung der Schutzgesetzeigenschaft ist, dass dem Einzelnen die Möglichkeit gegeben wird, seine Rechtspositionen unmittelbar mit Mitteln des Privatrechts gegen den Störer zu verteidigen.[361]

Als Schutzgesetze kommen hier völker- und gemeinschaftsrechtliche Vorschriften (a) oder Regelungen des einfachen deutschen Gesetzesrechts (b) in Betracht.

a) Völker- und gemeinschaftsrechtliche Vorschriften

Zwar können grundsätzlich auch unmittelbar geltende Vorschriften des Europäischen Primärrechts Schutzgesetze im Sinne des § 823 Abs. 2 BGB sein,[362] allerdings ist Voraussetzung, dass die jeweilige Norm die Befugnis enthält, die Verletzung einer Verhaltensnorm mit den Mitteln des Privatrechts zu ahnden.[363] Dies bedeutet, dass die Eröffnung eines individuellen, auf dem Zivilrechtsweg zu verfolgenden Schadensersatzanspruchs erkennbar vom Gesetzgeber erstrebt oder zumindest im Rahmen des haftpflichtrechtlichen Gesamtsystems liegen muss.[364]

---

[355] *Bassenge* in Palandt, § 1004 BGB, Rn. 38; *Gursky* in Staudinger, § 1004 BGB, Rn. 187
[356] RGZ 60, S. 9; RGZ 61, S. 369; RGZ 116, S. 153; *Bassenge* in Palandt, § 1004 BGB, Rn. 3; *Gursky* in Staudinger, § 1004, Rn. 15 f.
[357] *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 147; *Sprau* in Palandt, § 823 BGB, Rn. 56; *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 322
[358] BGHZ 28, S. 365; BGHZ 39, S. 368; BGHZ 64, S. 237; BGHZ 66, S. 390; BGHZ 69, S. 16; BGH, NJW 1991, S. 419; *Hager* in Staudinger, § 823 BGB, Rn. G 19; *Sprau* in Palandt, § 823 BGB, Rn. 57
[359] RGZ 128, S. 300; RGZ 138, S. 231; BGHZ 29, S. 102; BGHZ 29, S. 350; BGHZ 66, S. 355; BGH, NJW 1970, S. 1876 f.; BGH, NJW 1973, S. 1548 f.; BGH, NJW 1975, S. 48 f.; BGH, NJW 1992, S. 242 f.
[360] BGHZ 29, S. 350; BGHZ 66, S. 355; BGHZ 100, S. 14 f.; BGHZ 106, S. 206; BGH, NJW 1992, S. 242 f.; *Hager* in Staudinger, § 823 BGB, Rn. G 19; *Sprau* in Palandt, § 823 BGB, Rn. 57
[361] BGHZ 40, S. 307; BGHZ 100, S. 19; BGHZ 106, S: 206; *Hager* in Staudinger, § 823 BGB, Rn. G 21; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 156; *Sprau* in Palandt, § 823 BGB, Rn. 57; *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 345
[362] BGH, WuW 1980, S. 191; BGH, GRUR 1999, S. 277; *Köhler*, GRUR 2004, S. 100; *Kremer*, EuR 2003, S. 696; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 147; *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 327; *Weiß* in Calliess/Ruffert, Art. 82 EGV, Rn. 73
[363] BGH, NJW 1964, S. 396; BGH, NJW 1987, S. 1819; BGH, NJW 1989, S. 974; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 156; *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 345; kritisch: *Hager* in Staudinger, § 823 BGB, Rn. G 21
[364] BGH, NJW 1989, S. 974

Die in der Europäischen Verfassung[365] statuierten Gemeinschaftsgrundrechte entfalten jedoch bisher keine bindende Rechtswirkung und können bereits deshalb nicht auf dem Privatrechtweg verfolgt werden. Eine privatrechtliche Ahndung von Verstößen kommt auch deshalb nicht in Betracht, weil eine unmittelbare Drittwirkung der Gemeinschaftsgrundrechte ganz überwiegend abgelehnt wird.[366] Gleiches gilt für die EMRK-Rechte.[367] Demnach kann der Einzelne die genannten Rechte nicht im Rahmen des Privatrechtswegs geltend machen. Vielmehr handelt es sich um Rechte, die gegen den Staat gerichtet sind.[368] Somit sind Vorschriften des Völkerrechts und europäischen Primärrechts bereits aus diesem Grund nicht als Schutzgesetze im Sinne des § 823 Abs. 2 BGB anzusehen.

Im Übrigen kommt ein Rückgriff auf die genannten Vorschriften auch deshalb nicht in Betracht, weil nach der Rechtsprechung und herrschenden Lehre davon auszugehen ist, dass ein deliktischer Schutz nach § 823 Abs. 2 BGB im Grundsatz entbehrlich ist, wenn dieselben Belange des Geschädigten bereits anderweitig abgesichert sind.[369] Dies ist hier der Fall, da der Betroffene bereits durch § 823 Abs. 1 BGB bzw. durch die §§ 3, 7 Abs. 1, Abs. 2 Nr. 3 UWG geschützt ist. Aus dem letztgenannten Grund entfällt auch eine Anwendung des europäischen Sekundärrechts, insbesondere des Art. 13 Abs. 1 EK-DSRL, als Schutzgesetz.

Ansprüche aus den §§ 823 Abs. 2, 1004 Abs. 1 BGB in Verbindung mit völker- und gemeinschaftsrechtlichen Vorschriften scheiden somit aus.

b) Vorschriften des einfachen Gesetzesrechts

Fraglich ist, ob die Vorschriften des einfachen deutschen Gesetzesrechts als Schutzgesetze herangezogen werden können.

Allerdings gilt auch hier der Grundsatz, dass ein deliktischer Schutz nach § 823 Abs. 2 BGB entbehrlich ist, wenn dieselben Belange des Geschädigten bereits anderweitig abgesichert sind.[370] Deshalb ist davon auszugehen, dass die Vorschriften des UWG nicht als Schutzgesetze eingreifen können und zwar unabhängig von der strittigen Frage, ob das im UWG statuierte Klagesystem einer Schutzgesetzeigenschaft der Vorschriften dieses Gesetzes entgegensteht.[371]
Die Subsidiarität gilt allerdings nur außerhalb strafbewehrter Normen,[372] so dass Straftatbestände als Schutzgesetze in Betracht kommen. § 303 a StGB schützt eigentümerähnliche Positionen und in der Folge Individualinteressen.[373] Daher ist davon

[365] Die in der Charta der Grundrechte der Europäischen Union enthaltenen Rechte wurden ohne inhaltliche Änderung in die europäische Verfassung übernommen, *Walter* in Ehlers, § 1, Rn. 32; *Th. Schmitz*, EuR 2004, S. 694 f.
[366] *Borowsky* in Meyer, Art. 51 GRC, Rn. 31; *Calliess* in Ders./Ruffert, Art. 1 GRC, Rn. 14; *Suerbaum*, EuR 2003, S. 416
[367] *Kingreen* in Calliess/Ruffert, Art. 51 GRC, Rn. 18; *Meyer-Ladewig*, Art. 1 EMRK, Rn. 7; vgl. zur EMRK: Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten, BGBl. II 1952, S. 686, 953
[368] *Borowsky* in Meyer, Art. 51 GRC, Rn. 31; *Calliess* in Ders./Ruffert, Art. 1 GRC, Rn. 14; *Kingreen* in Calliess/Ruffert, Art. 51 GRC, Rn. 18; *Meyer-Ladewig*, Art. 1 EMRK, Rn. 7; *Suerbaum*, EuR 2003, S. 416
[369] BGHZ 84, S. 317; BGHZ 116, S. 14; BGHZ 125, S. 374; BGH, NJW 1980, S. 1793
[370] vgl.: 2. Kap. Teil 1 A. III. 2. a)
[371] dagegen: BGH, GRUR 1975, S. 150 - Prüfzeichen; *Köhler* in Baumbach/Baumbach, Einl., Rn. 7.5; dafür: *Sack*, NJW 1975, S. 1305 f.; *Schricker*, GRUR 1975, S. 118
[372] BGH, NJW 1982, S. 2780; BGH, NJW 1992, S. 241; *Spindler* in Bamberger/Roth, BGB Kommentar, § 823 BGB, Rn. 155
[373] BT-Drs. 10/5058, S. 34; *Möhrenschlager*, wistra 1986, S. 141; *Stree* in Schönke/Schröder, Vorbem. §§ 303 ff. StGB, Rn. 1; *Tröndle/Fischer*, § 303 a StGB, Rn. 2; *Welp,* IuR 1988, S. 448; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 2

auszugehen, dass § 303 a StGB ein Schutzgesetz im Sinne des § 823 Abs. 2 BGB ist.[374] Eine Schutzgesetzverletzung und damit Ansprüche nach Maßgabe der §§ 823 Abs.2, 1004 Abs. 1 BGB sind demnach in den Fällen gegeben, in denen der Empfänger in kurzer Zeit so viele Werbe-Emails erhält, dass er die erwünschten Emails von den Werbenachrichten nicht mehr unterscheiden kann.

3. Zwischenergebnis

Die §§ 823 Abs. 1, 2 BGB, 1004 Abs. 1 BGB stehen dem uneingeschränkten Versand unverlangter Werbe-Emails entgegen. Zum einen verletzt der Versender den Empfänger der Email-Werbung durch das Zusenden der Nachricht in seinem allgemeinen Persönlichkeitsrecht, wenn nicht die in § 7 Abs. 3 UWG genannte Konstellation vorliegt. Zum anderen ist der Straftatbestand des § 303 a Abs. 1 StGB, der als Schutzgesetz im Sinne der §§ 823 Abs. 2, 1004 Abs. 1 BGB zu qualifizieren ist, verwirklicht, wenn der Empfänger innerhalb Zeit so viele Werbe-Emails erhält, dass er die erwünschten Emails von den Werbenachrichten nicht mehr unterscheiden kann. Gerechtfertigt werden kann die Zusendung der Werbe-Email, wenn zuvor die Einwilligung des Empfängers eingeholt wird.

IV. Ergebnis

Das Versenden unverlangter Email-Werbung ist nach deutschem Recht grundsätzlich unzulässig, sofern nicht zuvor die Einwilligung des Empfängers eingeholt wurde. Dies ergibt sich aus §§ 7 Abs. 1, Abs. 2 Nr. 3 in Verbindung mit § 3 UWG und aus §§ 823 Abs. 1, 1004 Abs. 1 BGB. Es gilt somit das Opt-In-Prinzip. Dieser Grundsatz wird im Bereich des Wettbewerbs- und Deliktsrechts durch die in § 7 Abs. 3 UWG genannte Ausnahmekonstellation abgeschwächt. Bewirkt das Zusenden der Werbe-Emails -auch im Zusammenwirken mit anderen derartigen Nachrichten- dass der Empfänger erwünschte Emails nicht mehr von Werbenachrichten unterscheiden kann, so ist die Tätigkeit auch strafrechtlich sanktioniert, § 303 a StGB. Über §§ 823 Abs. 2, 1004 Abs. 1 BGB ergeben sich in diesem Fall auch zivilrechtliche Ansprüche.

B. Völker-, Gemeinschafts- und Verfassungsrecht

Im Folgenden soll überprüft werden, ob die einfachgesetzliche Rechtslage mit verfassungs-, gemeinschafts- sowie völkerrechtlichen Vorschriften im Einklang steht. Ist dies nicht der Fall, so kann daraus -abhängig davon, gegen welche Norm verstoßen wird- die Ungültigkeit des Gesetzes, eine Verpflichtung des Gesetzgebers zur Aufhebung der Norm, der Anwendungsvorrang der verletzten Vorschrift oder aber die unmittelbare Anwendbarkeit bzw. eine Verpflichtung zu einer Umsetzung oder richtlinienkonformen Auslegung folgen.[375]

I. Verfassungsrecht

Fraglich ist, ob die Vorschriften des einfachen Gesetzesrechts, welche eine Einschränkung der Zulässigkeit von Email-Werbung bewirken, gegen Grundrechte des Grundgesetzes verstoßen. Ein Grundrechtsverstoß würde wie jede Verfassungswidrigkeit eines Gesetzes dazu führen, dass dieses von Anfang an ipso jure nichtig ist.[376] Eine Ausnahme von der

[374] im Ergebnis: Wuermeling, CR 1994, S. 591
[375] zu den Folgen des Verstoßes gegen höherrangige Vorschriften: 2. Kap. Teil 1 B. I und II
[376] BVerfGE 84, S. 20 f.; BVerfGE 91, S. 27, 34 ff.; BVerfGE 92, S. 27; BVerfGE 93, S. 25; BVerfGE 93, S. 376; *Battis* in Isensee/Kirchhof, Band VII, § 165, Rn. 1 ff., 30; *Hartmann*, DVBl. 1997, S. 1264 ff.; *Herzog* in Maunz/Dürig, Art. 20 Abs. VI GG, Rn. 12; *Menzel*, DVBl. 1997, S. 642 ff.; *Ossenbühl*, NJW 1986, S. 2906;

Verfassungswidrigkeit ergibt sich nur, wenn das Bundesverfassungsgericht dies ausdrücklich zulässt, so etwa durch eine Unvereinbarkeitserklärung, vgl. §§ 31 Abs. 2 S. 2, 3, 79 Abs. 1 BVerfGG.[377] In diesem Fall bleibt die verfassungswidrige Norm wirksam, der Gesetzgeber ist jedoch verpflichtet, die Rechtslage zu ändern.[378]

Fraglich ist allerdings, ob die Grundrechte des Grundgesetzes hier überhaupt Anwendung finden. Zweifel daran bestehen insoweit, als § 7 Abs. 2 Nr. 3 UWG in Umsetzung des Art. 13 Abs. 1 EK-DSRL erlassen wurde.[379] Nach ständiger Rechtsprechung wird jedoch weder Gemeinschaftsrecht am Maßstab deutscher Grundrechte überprüft,[380] noch nationales Recht, das in Umsetzung sekundären Gemeinschaftsrechts erlassen wurde, soweit die Normsetzung diesem zwingend folgt.[381] Vielmehr unterliegt das Gesetz in diesem Fall allein dem auf Gemeinschaftsebene gewährleisteten Grundrechtsschutz.[382] Besteht hingegen bei der Umsetzung in mitgliedstaatliches Recht ein Spielraum des nationalen Gesetzgebers, so ist dieser an die nationalen Grundrechte gebunden.[383]
Art. 13 Abs. 1 EK-DSRL sieht vor, dass elektronische Post zum Zweck der Direktwerbung nur bei vorheriger Einwilligung des Empfängers versandt werden darf. Insofern besteht bei Umsetzung der Regelung kein Spielraum. Die Grundrechte des Grundgesetzes finden demnach keine Anwendung, soweit das deutsche Recht durch Art. 13 Abs. 1 EK- DSRL determiniert ist. Im Übrigen sind sie jedoch Prüfungsmaßstab. Eine Anwendbarkeit kommt damit einerseits in dem Bereich in Betracht, der nicht zwingend durch die Richtlinie vorgegeben ist, das bedeutet, im Hinblick auf Direktwerbung gegenüber anderen als natürlichen Personen, vgl. Art. 13 Abs. 5 EK-DSRL. Andererseits wurden auch die §§ 823 Abs. 1, 2, 1004 Abs. 1 BGB und § 303 a Abs. 1 StGB nicht in Umsetzung von Gemeinschaftsrecht erlassen, so dass auch in diesem Bereich die nationalen Grundrechte Anwendung finden. Soweit dies der Fall ist, ist die Frage zu beantworten, ob ein Eingriff in den Schutzbereich eines Grundrechts (1.) vorliegt und wenn ja, ob dieser verfassungsrechtlich gerechtfertigt werden kann (2.).

Pietzcker, AöR 101 (1976), S. 381

[377] *Battis* in Isensee/Kirchhof, Band IV, § 165, Rn. 33 ff.; *Seer*, NJW 1996, S. 285 ff.; *Schulze-Fielitz* in Dreier, Art. 20 GG, Rn. 89; *Schuppert*, AöR 120 (1995), S. 93 ff.; vgl. zum BVerfGG: Gesetz über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 11.08.1993, BGBl. I, S. 1473

[378] BVerfGE 33, S. 305; BVerfGE 37, S. 218, 262 ff.; BVerfGE 61, S. 321, 356 f.; BVerfGE 72, S. 333; BVerfGE 93, S. 178 f.; BVerfGE 102, S. 98; BVerfGE 103, S. 270; BVerfGE 109, S. 211, 235 ff.; BVerfGE 111, S. 306

[379] vgl.: 2. Kap. Teil 1 A. II.

[380] BVerfG, NJW 1987, S. 577 - Solange II; BVerfG, NJW 1993, S. 3049 - Maastricht; BVerfG, NJW 2000, S. 3125- Bananenmarkt; *Hirsch*, NJW 1996, S. 2463 ff.; *Nicolaysen/Nowak*, NJW 2001, S. 1233 ff.

[381] BVerfG, NJW 2001, S. 1268; BVerfG, NVwZ 2004, S. 1347; BVerwG, NVwZ 2005, S. 1181; *Classen* in von Mangoldt/Klein/Starck, Art. 23 GG, Rn. 67; *Ehlers* in Ehlers, § 13, Rn. 30; *Gerstner/Goebel*, Jura 1993, S. 632; *Jarass*, EU- Grundrechte, § 4, Rn. 12; *Kingreen,* JuS 2000, S. 864; *Masing*, NJW 2006, S. 265; *Pernice* in Dreier, Art. 23 GG, Rn. 30; *Pieroth/Schlink*, Staatsrecht II, Rn. 191; *Rengeling/Szczekalla*, Rn. 313; *Starck* in von Mangoldt/Klein/Starck, Art. 1 GG, Rn. 225, 237; *A. Weber*, NJW 2000, S. 542

[382] BVerfG, NJW 2001, S. 1268; BVerfG, NVwZ 2004, S. 1347; BVerwG, NVwZ 2005, S. 1181; *Classen* in von Mangoldt/Klein/Starck, Art. 23 GG, Rn. 67; *Ehlers* in Ehlers, § 13, Rn. 30; *Gerstner/Goebel*, Jura 1993, S. 632; *Jarass*, EU- Grundrechte, § 4, Rn. 12; *Kingreen,* JuS 2000, S. 864; *Masing*, NJW 2006, S. 265; *Pernice* in Dreier, Art. 23 GG, Rn. 30; *Pieroth/Schlink*, Staatsrecht II, Rn. 191; *Rengeling/Szczekalla*, Rn. 313; *Starck* in von Mangoldt/Klein/Starck, Art. 1 GG, Rn. 225, 237; *A. Weber*, NJW 2000, S. 542

[383] BVerfG, EuGRZ 1989, S. 340; BVerfG, NVwZ 1993, S. 883; BVerfG, EuGRZ 2001, S. 152; BVerfG, NVwZ 2004, S. 1346 f.; *Ehlers* in Ders., § 13, Rn. 30; *Gerstner/Goebel*, Jura 1993, S. 632; *Jarass*, EU-Grundrechte, § 4, Rn. 12; *Ders*. in Jarass/Pieroth, Art. 23 GG, Rn. 38; *Kingreen*, JuS 2000, S. 864; *Pieroth/Schlink*, Staatsrecht II, Rn. 191; *Rengeling/Szczekalla*, Rn. 313; *Scholz*, NJW 1990, S. 941; *Streinz* in Isensee/Kirchhof, Band VII, § 182, Rn. 33; *A. Weber*, NJW 2000, S. 542

1. Grundrechtseingriff

Die Vorschriften des einfachen Gesetzesrechts, die in einer Beschränkung der Zulässigkeit von Email-Werbung resultieren, könnten in Grundrechte der Werbetreibenden (a) sowie in diejenigen solcher Personenkreise eingreifen, die am Erhalt von Email-Werbung interessiert sind (b).

a) Verfassungsrechtlicher Schutz der Werbetreibenden

Die genannten Normen könnten einen Eingriff in den Schutzbereich des Grundrechts der Meinungsfreiheit der Werbetreibenden nach Art. 5 Abs. 1 GG (aa) oder in denjenigen der Berufsfreiheit gemäß Art. 12 Abs. 1 GG (bb) darstellen. Ein Eingriff liegt nicht nur in Rechtsakten, die final und unmittelbar das Grundrecht beschränken, so die „klassische" Eingriffsdefinition,[384] sondern in jeder Beeinträchtigung des Schutzbereichs eines Grundrechts durch die öffentliche Gewalt, unabhängig davon, ob diese durch Rechtsakt oder bloß faktisches Handeln, ob final und unmittelbar erfolgt.[385]

aa) Meinungsfreiheit, Art. 5 Abs. 1 GG

Es stellt sich die Frage, ob die genannten Vorschriften des einfachen deutschen Rechts in den Schutzbereich der Meinungsäußerungsfreiheit des Werbetreibenden eingreifen.

Dazu müsste sich kommerzielle Werbung unter den Begriff der Meinung im Sinne des Art. 5 Abs. 1 GG einordnen lassen. Dieser ist weit zu verstehen.[386] Er umfasst Werturteile und Tatsachenbehauptungen, letztere allerdings lediglich weil und soweit sie Voraussetzung für die Bildung von Meinungen sind.[387] Werturteile sind durch ein Element der „Stellungnahme, des Dafürhaltens oder Meinens" im Rahmen einer geistigen Auseinandersetzung oder einer sonstigen sozialen Kommunikation gekennzeichnet.[388] Tatsachenbehauptungen sind hingegen mit Mitteln des Beweises überprüfbar.[389] Werbebotschaften enthalten grundsätzlich Fakten über das Produkt bzw. die Dienstleistung, in der Regel jedoch auch subjektive Äußerungen, also Elemente der Stellungnahme, des Dafürhaltens und des Meinens, die der Absatzförderung dienen.[390] Soweit in der Werbebotschaft Tatsachen genannt werden, sind diese Grundlage der Meinungsbildung über das beworbene Produkt. Danach enthält Werbung

---

[384] BVerfGE 105, S. 299 f.; *Herdegen* in Maunz/Dürig, Art. 1 Abs. 3 GG, Rn. 39; *Jarass* in Ders./Pieroth, Vorbem. Art. 1, Rn. 25; *Pieroth/Schlink*, Staatsrecht II, Rn. 238 f.

[385] BVerfGE 105, S. 273; BVerfGE 105, S. 300 f.; *Gallwas*, a.a.O., S. 49 ff.; *Herdegen* in Maunz/Dürig, Art. 1 Abs. 3 GG, Rn. 39; *Lübbe-Wolff*, a.a.O., S. 25 ff.; *Jarass* in Ders./Pieroth, Vorbemerkung zu Art. 1 GG, Rn. 26

[386] BVerfGE 61, S. 9; BVerfGE 71, S. 179; *Herzog* in Maunz/Dürig, Art. 5 Abs. 1, 2 GG, Rn. 55; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 3; *Leibholz/Rinck*, Art. 5 GG, Rn. 26; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 8

[387] std. Rspr. seit BVerfGE 61, S. 1, 8 f.; vgl. etwa: BVerfGE 65, S. 41; BVerfGE 94, S. 7; vgl. auch: *Herdegen* in Maunz/Dürig, Art. 5 Abs. 1, 2 GG, Rn. 55 a; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 3; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 26; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 10

[388] BVerfGE 7, S. 210; BVerfGE 61, S. 8 f.; BVerfGE 65, S. 41; BVerfGE S. 71, 179; BVerfGE 90, S. 247; BGHZ 130, S. 5, S. 11; *Bethge* in Sachs, Art. 5 GG, Rn. 25; *Hösch*, WRP 2003, S. 937; *Leibholz/Rinck*, Art. 5 GG, Rn. 26; *Säcker*, WRP 2004, S. 1203; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 22; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 8

[389] BVerfG, NJW 1983, S. 1416; BVerfG, NJW 1992, S. 1440; BGHZ, 132, S. 13; BGH, NJW-RR 1999, S. 1251; BGH, NJW 2005, S. 281 f.; *Hösch*, WRP 2003, S. 937; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 3; *Leibholz/Rinck*, Art. 5 GG, Rn. 27

[390] BVerfGE 11, S. 238; BVerfGE 30, S. 352; BVerfGE 71, S. 162 ff., 175; *Friauf/Höfling*, AfP 1985, S. 253 f.; *Jarass*, NJW 1982, S. 1834 f.; *Ders.* in Jarass/Pieroth, Art. 5 GG, Rn. 3; *Lerche*, a.a.O., S. 77 f., 83 f.; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 25; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 11; a.A.: *Faßbender*, GRUR Int. 2006, S. 972

Werturteile und der Meinungsbildung zugrundeliegende Tatsachen, weshalb sie vom Schutzbereich der Meinungsäußerungsfreiheit umfasst ist.[391] Daran ändert auch die wirtschaftliche Zielsetzung der Äußerung nichts.[392]
Geschützte Tätigkeiten sind das Äußern und Verbreiten der Meinung, also ihre Abgabe und der Vorgang der Informationsübertragung.[393] Dabei nennt Art. 5 Abs. 1 GG die Äußerung in Wort, Schrift und Bild, wobei hierin jedoch keine abschließende Aufzählung zu sehen ist.[394] Demnach sind auch Werbung sowie sonstige Meinungsäußerungen mittels Email in den Schutzbereich des Grundrechts miteinzubeziehen.
Grundrechtsträger sind natürliche Personen, auch Ausländer,[395] sowie inländische juristische Personen und Personenvereinigungen.[396]

Das Grundrecht wird durch jede Anordnung der öffentlichen Gewalt beeinträchtigt, die die Meinungsäußerung oder -verbreitung verbietet, behindert oder gebietet.[397] Hier wird die Meinungsäußerung dadurch behindert, dass der Äußernde zur Vermeidung eines wettbewerbs-, delikts- bzw. strafrechtlichen Vorwurfs verpflichtet ist, vor dem Versenden der Email die Einwilligung des Adressaten einzuholen. Etwas anderes gilt im Bereich des Wettbewerbs- und Deliktsrechts, sofern die Ausnahmevorschrift des § 7 Abs. 3 UWG eingreift.[398] Insofern ist die gesetzliche Regelung dahingehend, dass die Werbe-Emails erst versandt werden darf, wenn ein Dritter seine Einwilligung erklärt hat, als Eingriff anzusehen.

bb) Berufsfreiheit, Art. 12 Abs. 1 GG

Fraglich ist, ob die Einschränkungen der Zulässigkeit kommerzieller Emails durch die Vorschriften des Delikts-, Wettbewerbs- und Strafrechts daneben als Eingriff in das Grundrecht der Berufsfreiheit der Werbetreibenden nach Art. 12 Abs. 1 GG zu qualifizieren sind.

Art. 12 Abs. 1 GG enthält ein einheitliches Grundrecht, das die Freiheit der Berufswahl und der Berufsausübung umfasst.[399] Zur Berufsfreiheit gehört auch die berufliche

---

[391] BVerfGE 11, S. 238; BVerfGE 30, S. 352; BVerfGE 71, S. 162 ff., 175; *Friauf/Höfling*, AfP 1985, S. 253 f.; *Jarass*, NJW 1982, S. 1834 f.; *Ders.* in Jarass/Pieroth, Art. 5 GG, Rn. 3; *Lerche*, a.a.O., 77 f., 83 f.; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 25; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 11; a.A.: *Faßbender*, GRUR Int. 2006, S. 972

[392] BVerfGE 11, S. 238; BVerfGE 30, S. 352; BVerfGE 53, S. 99; BVerfGE 71, S. 175; BVerfGE 95, S. 182; BVerfGE 102, S. 359; BGHZ 130, S. 203; *Friauf/Höfling*, AfP 1985, S. 253 f.; *Jarass*, NJW 1982, S. 1834 f.; *Ders.* in Jarass/Pieroth, Art. 5 GG, Rn. 3; *Lerche*, a.a.O., 77 f., 83 f.; *Schmitt Glaeser*, AöR 113 (1988), S. 72; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 25; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 11; a.A.: *Faßbender*, GRUR Int. 2006, S. 972

[393] *Bethge* in Sachs, Art. 5 GG, Rn. 44; *Herzog* in Maunz/Dürig, Art. 5 Abs. 1, 2 GG, Rn. 56 f.; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 6; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 16

[394] *Bethge* in Sachs, Art. 5 GG, Rn. 44; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 7; a.A.: *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 16

[395] *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 8; *Schulze-Fielitz* in Dreier, Art. 5 Abs. 1, 2 GG, Rn. 86; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 178; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 4

[396] BVerfGE 95, S. 34 f. zu Pressefreiheit; *Herzog* in Maunz/Dürig, Art. 5 Abs. 1, 2 GG, Rn. 17; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 8; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 181; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 6

[397] BVerfGE 86, S. 128; *Degenhardt* in Bonner GG Kommentar, Art. 5 GG, Rn. 51; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 9; *Schulze-Fielitz* in Dreier, Art. 5 GG, Rn. 124; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 189; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 18

[398] vgl. dazu bereits: 2. Kap. Teil 1 A. II.

[399] BVerfGE 9, S. 344; BVerfGE 17, S. 276; BVerfGE 50, S. 363; BVerfGE 58, S. 364; BVerfGE 68, S. 267; BVerfGE 85, S. 104; BVerfGE 94, S. 389; BVerfGE 105, S. 266; BVerfGE 106, S. 192; BVerfGE 106, S. 298; BVerfGE 111, S. 373; BVerwGE 105, S. 219; BVerwGE 114, S. 189 f.; BGHZ 147, S.74; *Gubelt* in von Münch/Kunig, Art. 12 GG, Rn. 38, 40; *Jarass* in Ders./Pieroth, Art. 12 GG, Rn. 8; *Manssen* in von

Außendarstellung des Grundrechtsträgers, einschließlich der Möglichkeit, für seine beruflichen Leistungen zu werben.[400]
Grundrechtsträger sind alle Deutschen im Sinne des Art. 116.[401] Erfasst sind auch inländische juristische Personen im Sinne des Art. 19 Abs. 3 GG sowie nicht-rechtsfähige Personenvereinigungen des bürgerlichen Rechts.[402]

Ein Eingriff in das Grundrecht der Berufsfreiheit ist gegeben, wenn die fragliche Regelung sich unmittelbar auf einen oder mehrere Berufe bezieht oder eine berufsregelnde Tendenz aufweist.[403] Letzteres ist der Fall, wenn schwerpunktmäßig Tätigkeiten von der Vorschrift erfasst sind, die typischerweise beruflich ausgeübt werden.[404] Akte mit berufsneutraler Zielsetzung sollen dagegen nicht Art. 12 Abs. 1 GG unterfallen.[405] Es genügt also nicht, dass eine Vorschrift oder ihre Anwendung unter bestimmten Umständen Auswirkungen auf die Berufstätigkeit hat.[406] Werbebeschränkungen für berufliche Tätigkeiten stellen Eingriffe in das Grundrecht der Berufsfreiheit dar, da sie den beruflichen Bereich betreffen.[407] Die Tatsache, dass dem betroffenen Grundrechtsträger nur ein einziges Werbemedium genommen wird, schadet hierbei nicht, da das Bundesverfassungsgericht auch bereits die Beeinträchtigung einzelner Aspekte der Außendarstellung als Eingriffe in die Berufsfreiheit ansieht.[408]

Ein Eingriff in das Grundrecht der Berufsfreiheit ist daneben auch unter dem Gesichtspunkt zu bejahen, dass Unternehmen, deren berufliche Tätigkeit darin besteht, Werbe-Emails zu versenden, in ihrer Tätigkeit eingeschränkt werden.

cc) Sonderfall: Politische Email-Werbung

Einen Sonderfall stellt politische Email-Werbung dar. Durch die Beschränkung dieser Form von Werbung durch die oben genannten delikts- und strafrechtlichen Normen könnte Art. 21 Abs. 1 GG verletzt sein.

Mangoldt/Klein/Starck, Art. 12 Abs. 1 GG, Rn. 2, 68; *Meesen*, JuS 1982, S. 400; *Scholz* in Maunz/Dürig, Art. 12 GG, Rn. 14; *Schwabe*, DÖV 1969, S. 737 f.

[400] BVerfGE 40, S. 382 f.; BVerfGE 53, S. 97 ff.; BVerfGE 85, S. 256; BVerfGE 94, S. 388; BVerfGE 105, S. 266; BVerfGE 111, S. 373; BGHZ 147, S. 74; BVerwGE 105, S. 363; *Faßbender*, GRUR Int. 2006, S. 965 ff.; *Ders*., NJW 2006, S. 1465; *Gubelt* in von Münch/Kunig, Art. 12 GG, Rn. 38; *Hofmann* in Schmidt-Bleibtreu/Klein, Art. 12 GG, Rn. 64; *Jarass* in Ders./Pieroth, Art. 12 GG, Rn. 8

[401] für eine Einbeziehung von EU-Bürgern: *Breuer* in Isensee/Kirchhof, Band VI, § 147, Rn. 21; gegen eine Einbeziehung: *Manssen* in von Mangoldt/Klein/Starck, Art. 12 GG, Rn. 265; *Scholz* in Maunz/Dürig, Art. 12 GG, Rn. 97; *Tettinger* in Sachs, Art. 12 GG, Rn. 18 ff.

[402] BVerfGE 97, S. 253; BVerfGE 102, S. 212 f.; BVerfGE 105, S. 265; BVerwGE 97, S. 23; *Dürig* in Maunz/Dürig, Art. 19 Abs. 3 GG, Rn. 29 f.; *Jarass* in Jarass/Pieroth, Art. 12 GG, Rn. 10; *Scholz* in Maunz/Dürig, Art. 12 GG, Rn. 98

[403] BVerfGE 13, S. 185; BVerfGE 37, S. 17 unter Verweis auf BVerfGE 13, S. 181 ff., 185 f.; BVerfGE 16, S. 162; BVerfGE 29, S. 333; BVerfGE 70, S. 214; BVerfGE 82, S. 224; BVerfGE 97, S. 254; BVerfGE 98, S. S. 258; BVerfGE 111, S. 213; BAGE 103, S. 251; *Gubelt* in von Münch/Kunig, Art. 12 GG, Rn. 43; *Jarass* in Ders./Pieroth, Art. 12 GG, Rn. 11; *Tettinger* in Sachs, Art. 12 GG, Rn. 71, 73; a.A.: *Manssen* in v. Mangoldt/Klein/Starck, Art. 12 GG, Rn. 74

[404] BVerfGE 97, S. 254

[405] BVerfGE 10, S. 363; BVerfGE 32, S. 63 f.; BVerfGE 41, S. 241; BVerfGE 49, S. 48; BVerfGE 54, S. 270

[406] BVerfGE 95, S. 301 unter Bezugnahme auf BVerfGE 70, S. 191 ff., 214; BVerfGE 95, S. 302; *Gubelt* in von Münch/Kunig, Art. 12 GG, Rn. 43; *Jarass* in Ders./Pieroth, Art. 12 GG, Rn. 12 ff.; *Tettinger* in v. Mangoldt/Klein/Starck, Art. 12 GG, Rn. 74

[407] BVerfGE 65, S. 245; BVerfGE 71, S. 172 f.; BVerfGE 76, S. 205 f.; BVerfGE 82, S. 26 ff.; BVerfGE 85, S. 256 f.; BVerwGE 89, S. 33; *Faßbender*, GRUR Int. 2006, S. 965 ff.; *Ders*., NJW 2006, S. 1465

[408] BVerfGE 82, S. 26

Die Vorschrift weist den politischen Parteien die Aufgabe zu, an der politischen Willensbildung des Volkes mitzuwirken. Diese Mitwirkung erfolgt nach § 1 Abs. 2 PartG insbesondere dadurch, dass die Parteien auf die Gestaltung der öffentlichen Meinung Einfluss nehmen, die aktive Teilnahme der Bürger am politischen Leben fördern, sich durch Aufstellung von Bewerbern den Wahlen in Bund, Ländern und Gemeinden beteiligen, die von ihnen erarbeiteten politischen Zielen in den Prozeß der staatlichen Willensbildung einführen und für eine ständige lebendige Verbindung zwischen dem Volk und den Staatsorganen sorgen.[409]

Die politische Werbung dient, auch wenn sie außerhalb von Wahlkampfzeiten stattfindet, der Einflussnahme auf die politische Willensbildung und ist damit von der Betätigungsfreiheit der politischen Parteien umfasst.[410] In den Schutzbereich der Parteifreiheit fällt danach etwa die Werbung mit Plakaten und Informationsständen sowie das Verteilen und Zusenden von Flugblättern und anderem Werbematerial.[411] Ebenso ist das Verbreiten politischer Ansichten mittels des Internet durch Art. 21 Abs. 1 GG geschützt.[412] Die genannten Einschränkungen politischer Werbung stellen somit einen Eingriff in Art. 21 Abs. 1 GG dar.

dd) Zwischenergebnis

Die Grundrechte der Meinungsäußerungs- und Berufsfreiheit, in deren Schutzbereich hier eingegriffen wird, haben eine unterschiedliche Schutzrichtung. Ebenso kommt Art. 21 Abs. 1 GG ein vom Gewährleistungsgehalt der Grundrechte verschiedener Bedeutungsgehalt zu. Insofern tritt keines der Rechte hinter die anderen zurück. Sie stehen daher in Idealkonkurrenz.[413]

b) Verfassungsrechtlicher Schutz an Email-Werbung interessierter Personenkreise

Diejenigen Personenkreise, die am Erhalt von Email-Werbung interessiert sind, könnten durch die im deutschen Recht aufgrund der genannten Vorschriften des Wettbewerbs-, Delikts- und des Strafrechts bestehenden Beschränkung der Zulässigkeit dieses Mittels des Direktmarketing in ihrem Recht auf Informationsfreiheit nach Art. 5 Abs. 1 GG verletzt sein.[414] Zwar wird denjenigen Personen, die gerne Email-Werbung erhalten möchten, an sich durch die Möglichkeit, sich für und gegen diese zu entscheiden, eine weitere Option eingeräumt. Allerdings wird aufgrund des Einwilligungsvorbehalts der Versand von Werbe-Emails von einer zusätzlichen Voraussetzung abhängig gemacht. So kann unter Umständen bewirkt werden, dass der Zugang der Werbenachrichten im Vergleich zum Versand ohne Einholen der Zustimmung verzögert wird. In einigen Fällen wird die Zustellung der Email-Werbung aufgrund des Zustimmungsverbehalts möglicherweise sogar verhindert. Hierin könnte ein Eingriff in das Recht auf Informationsfreiheit nach Art. 5 Abs. 1 GG liegen.

Nach Art. 5 Abs. 1 S. 1 GG hat jeder das Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Allgemein zugänglich sind Informationsquellen, wenn sie geeignet und bestimmt sind, der Allgemeinheit, also einem individuell nicht bestimmbaren

[409] für die Briefkastenwerbung: *Löwisch*, NJW 1990, S. 437 f.
[410] BVerfG, NJW 2002, S. 2938
[411] BVerfG, NJW 1991, S. 910; BVerfG, NJW 2002, S. 2938
[412] LG München I, MMR 2003, S. 283
[413] *Gubelt* in von Münch/Kunig, Art. 12 GG, Rn. 95; *Ipsen* in Sachs, Art. 21 GG, Rn. 44; *Massen* in v. Mangoldt/Klein/Starck, Art. 12 Abs. 1, 2 GG, Rn. 279; *Tettinger* in Sachs, Art. 12 GG, Rn. 167
[414] vgl. dazu bereits: 2. Kap. Teil 1 A.

Personenkreis, Informationen zu beschaffen.[415] Auch die öffentliche Wirtschaftswerbung wird als allgemein zugängliche Quelle angesehen.[416] Ob Werbe-Emails als solche zu qualifizieren sind, könnte allerdings deshalb fraglich sein, weil Sendungen, die an bestimmte Personen übersandt werden, ausweislich der Rechtsprechung grundsätzlich keine allgemein zugänglichen Quellen sind.[417] Allerdings sollen Flugblätter und Handzettel als allgemein zugängliche Quellen anzusehen sein.[418] Werbe-Emails sind in aller Regel nicht einem Privatbrief vergleichbar, da sie grundsätzlich nicht lediglich an einen einzelnen individualisierten Adressaten, sondern massenhaft anhand von Adresslisten an einen großen Empfängerkreis versandt werden. Demnach besteht bei Massen-Emails eine Vergleichbarkeit zu Flugblättern, so dass sie als allgemein zugängliche Quelle anzusehen sind. Etwas anderes gilt, wenn Werbe-Emails individualisiert und in geringen Mengen versandt werden. Solche Nachrichten können nicht als allgemein zugängliche Quelle qualifiziert werden, mit der Folge, dass hier nicht Art. 5 Abs. 1 GG eingreift, sondern die subsidiäre allgemeine Handlungsfreiheit, Art. 2 Abs. 1 GG.[419]
Die Unterrichtung aus den allgemein zugänglichen Quellen ist nicht nur auf aktives Handeln zugeschnitten, auch die schlichte Entgegennahme von Informationen zählt dazu, ebenso wie die Chance des ungehinderten Empfangs unbestellter Informationen.[420] Daher ist das Interesse der an Werbung interessierten Personenkreise durch Art. 5 Abs. 1 GG geschützt.

Fraglich ist, ob in dem Erfordernis der vorherigen Einwilligung, der aufgrund wettbewerbs-, delikts- und teilweise auch strafrechtlicher Vorschriften gilt, ein Eingriff zu sehen ist. Als Eingriff in das Grundrecht der Informationsfreiheit werden alle Maßnahmen qualifiziert, die die Informationsaufnahme verbieten oder durch Gebote behindern.[421] Aufgrund des Wortlauts des Art. 5 Abs. 1 GG „ungehindert“ geht die Rechtsprechung davon aus, dass bereits in einer Verzögerung der Information ein Eingriff in das Grundrecht der Informationsfreiheit liegt.[422] Durch das Einholen der Einwilligung des Adressaten wird der Zugang der Werbe-Nachrichten im Vergleich zum Versand ohne Einholen der Zustimmung verzögert, im Hinblick auf einige Grundrechtsträger möglicherweise sogar verhindert. Insofern ist von einem Eingriff in den Schutzbereich des Grundrechts durch das UWG, das Deliktsrecht und die strafrechtliche Vorschrift, welche die Zulässigkeit der Email-Direktwerbung wie oben ausgeführt einschränken, auszugehen.

2. Verfassungsrechtliche Rechtfertigung

Es stellt sich die Frage, ob die Beeinträchtigung der Schutzbereiche verfassungsrechtlich gerechtfertigt werden kann.

---

[415] BVerfGE 27, S. 71 ff., 83; BVerfGE 33, S. 52 ff., 65; BVerfGE 90, S. 27 ff., 30; BVerfGE 103, S. 44 ff., 60; BVerwGE 47, S. 247 ff., 252; *Herzog* in Maunz/Dürig, Rn. 90; *Lerche*, Jura 1995, S. 565 f.; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 16; *Schmid-Jortzig* in Isensee/Kirchhof, Band VI, § 141, Rn. 32; *Schmitt Glaeser*, Jura 1987, S. 570 f.; *Schulze-Fielitz* in Dreier, Art. 5 Abs. 1, 2 GG, Rn. 58; *Wendt* in v. Münch/Kunig, Art. 5 GG, Rn.23

[416] *Kresse*, WRP 1985, S. 540 f.; *Oppermann*, a.a.O., S. 405 f.; *Schulze-Fielitz* in Dreier, Art. 5 Abs. 1, 2 GG, Rn. 57

[417] BVerfGE 18, S. 315; BVerfGE 35, S. 315

[418] *Schulze-Fielitz*, in Dreier, Art. 5 Abs. 1, 2 GG, Rn. 58; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 45; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 23

[419] BVerfGE 6, S. 37; BVerfGE 67, S. 171; BVerfGE 83, S. 194; BVerfGE 89, S. 13

[420] BVerfGE 27, S. 82 f.; BayVerfGH, DÖV 1986, S. 73; *Bethge* in Sachs, Art. 5 GG, Rn. 53; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 17; *Wendt* in von Münch/Kunig Kommentar, Rn. 26

[421] BVerfGE 15, S. 295; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 19; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 189

[422] BVerfGE 27, S. 98 f.

a) Voraussetzungen der Grundrechtsschranken

Weder Art. 5 Abs. 1 GG, noch Art. 12 Abs. 1 GG sind schrankenlos gewährleistet. Vielmehr nennt Art. 5 Abs. 2 GG als Schranke des Art. 5 Abs. 1 GG die allgemeinen Gesetze. Art. 12 Abs. 1 S. 2 GG sieht vor, dass die Berufsausübung durch Gesetz oder aufgrund eines Gesetzes geregelt werden kann.

Allgemeine Gesetze im Sinne des Art. 5 Abs. 2 GG sind solche Normen, die sich weder gegen die Meinungsfreiheit an sich, noch gegen bestimmte Meinungen richten, sondern dem Schutz eines schlechthin, ohne Rücksicht auf eine bestimmte Meinung zu schützenden Rechtsgutes dienen.[423] Die Begrenzung der Zulässigkeit der Email-Werbung zielt nicht darauf ab, die Äußerung einer bestimmten Meinung zu verhindern, sondern dient dem Schutz der Empfänger vor den Folgen der massenhaft versandten Email-Werbung.[424] Die fraglichen Vorschriften[425] erfüllen demnach das Kriterium der allgemeinen Gesetze.

Art. 12 Abs. 1 S. 2 GG sieht vor, dass die Berufsausübung nur durch Gesetz oder aufgrund eines Gesetzes geregelt werden kann. Erforderlich ist ein formelles Gesetz,[426] wobei die Rechtsprechung jedoch nicht fordert, dass sich alle einschlägigen Vorgaben aus dem Wortlaut des Gesetzes ergeben, sondern es ausreichen lässt, wenn sie sich mit Hilfe allgemeiner Auslegungsgrundsätze erschließen lassen.[427] Die Beschränkung erfolgt hier durch formelle Gesetze. Soweit sich die gesetzlichen Vorgaben nicht aus dem Gesetzeswortlaut ergeben,[428] existiert eine umfangreiche Rechtsprechung,[429] anhand derer sich diese durch Auslegung konkretisieren lassen.

b) Schranken-Schranken

Allerdings sind dem Gesetzgeber im Rahmen der Beschränkungen der Grundrechte wiederum Schranken gesetzt, die so genannten Schranken-Schranken.[430]

aa) Verhältnismäßigkeit

Die Grundrechtseinschränkungen lassen sich nur dann rechtfertigen, wenn sie verhältnismäßig sind. Dies ist der Fall, wenn die fraglichen Maßnahmen geeignet sowie erforderlich sind, das gewünschte Ziel zu erreichen und das Kriterium der Verhältnismäßigkeit im engeren Sinne gegeben ist.[431] Im Rahmen des Art. 5 GG hat das Bundesverfassungsgericht die so genannte Wechselwirkungstheorie geprägt, die jedoch lediglich eine besondere Ausprägung des Verhältnismäßigkeitsgrundsatzes ist.[432] Danach entsteht eine Wechselwirkung dahingehend, dass die allgemeinen Gesetze zwar dem

[423] BVerfGE 97, S. 146; BVerfGE 71, S. 175; BVerfGE 95, S. 235; BVerfGE 111, S. 155; BVerwGE 93, S. 325; *Degenhardt* in Bonner GG Kommentar, Art. 5 GG, Rn. 66; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 56; *Kannengießer* in Schmidt/Bleibtreu/Klein, Art. 5 GG, Rn. 22; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 199; *Wendt* in von Münch/Kunig, Art. 5 GG, Rn. 69
[424] BT-Drs. 15/1487, S. 20 f.; Erwägungsgrund Nr. 40 EK-DSRL
[425] vgl.: 2. Kap. Teil 1 A. und B. I.
[426] BVerfGE 59, S. 364; BVerfGE 65, S. 258
[427] BVerfGE 80, S. 279; BVerfGE 82, S. 224 f.
[428] vgl.: 2. Kap. Teil 1 A. III. 1.
[429] vgl.: 2. Kap. Teil 1 A. III. 1.
[430] vgl. dazu: Pieroth/Schlink, Staatsrecht II, Rn. 274
[431] BVerfGE 59, S. 265; BVerfGE 65, S. 54; BVerfGE 67, S. 173; BVerfGE 70, S. 286; BVerfGE 71, S. 181; BVerfGE 77, S. 75; BVerfGE 104, S. 347 ff.; BVerwGE 109, S. 191
[432] BVerfGE 67, S. 172 f.; *Bethge* in Sachs, Art. 5 GG, Rn. 146; *Jarass* in Ders./Pieroth, Vorbem. Art. 1 GG, Rn. 44

Grundrecht Schranken setzen, sie aber aufgrund der Bedeutung der Meinungsfreiheit im freiheitlichen demokratischen Staat ausgelegt und so in ihrer das Grundrecht begrenzenden Wirkung wieder eingeschränkt werden müssen.[433]

Geeignet ist der Einsatz solcher Mittel, mit deren Hilfe der gewünschte Erfolg gefördert werden kann, die also die Zweckerreichung ermöglichen.[434] Die Einschränkung der Möglichkeit der Email-Direktwerbung wird rechtstreue Unternehmen und Personen davon abhalten, ohne Einwilligung des Adressaten solche Nachrichten zu versenden. Gegen nicht rechtstreue Unternehmen bestehen zivilrechtliche Ansprüche und unter Umständen strafrechtliche Sanktionen.[435] Die Geeignetheit ist damit gegeben.

Die Maßnahme ist erforderlich, wenn sie nicht über das zum Erreichen ihres Zwecks notwendige Maß hinausgeht.[436] Keine Erforderlichkeit liegt danach vor, wenn das gleiche Ergebnis auch durch ein genauso wirksames, das Grundrecht weniger einschränkendes Mittel, erzielt werden kann.[437] Dabei darf das mildere Mittel Dritte und die Allgemeinheit nicht stärker belasten.[438] Auf den ersten Blick erscheint die Opt-Out-Lösung weniger eingriffsintensiv, als das Einwilligungserfordernis, das im deutschen Recht aufgrund wettbewerbs-, delikts- und strafrechtlicher Vorgaben gilt und so zu einer rechtsgebietsübergreifenden Opt-In-Lösung führt. Denn im ersten Fall dürfen die Werbetreibenden so lange Werbe-Emails versenden, bis der Adressat widerspricht. Insofern erhalten auch an Werbung interessierte Adressaten ungehindert Informationen, während im Fall der Opt-In-Lösung zumindest die rechtstreuen Werbetreibenden lediglich den Empfängern Nachrichten zustellen werden, deren Einwilligung ihnen vorliegt. Allerdings besteht im Bereich der Opt-Out-Lösung das Problem, dass angesichts der hohen Anzahl eingehender Werbe-Emails der Betroffene sehr viel Zeit aufwenden muss, um der Zustellung sämtlicher solcher Nachrichten zu widersprechen. Des Weiteren ist zu berücksichtigen, dass die Empfänger durch ihren Widerspruch den Absendern der Nachrichten zu erkennen geben, dass die Email-Adresse, an welche die ursprüngliche Nachricht versandt wurde, existent ist und noch benutzt wird. Auch deshalb werden die Empfänger von Email-Werbung häufig davon Abstand nehmen, ihren Widerspruch zu erklären, da die Absender hierdurch die Existenz der Adresse verifizieren können. Insofern werden Adressaten unerwünschter Email-Werbung durch das Opt-In-Prinzip effektiver geschützt, als durch die Opt-Out-Lösung. Das alternative Mittel ist somit nicht genauso wirksam, wie das eingesetzte.
Die deutschen Bestimmungen sind folglich erforderlich.

Fraglich ist, ob sie im engeren Sinne verhältnismäßig sind. Die Verhältnismäßigkeit im engeren Sinne fordert eine adäquate Zweck-Mittel-Relation, zielt also auf einen angemessenen Ausgleich zwischen der Schwere der grundrechtlichen Beeinträchtigung und der Bedeutung des mit der Maßnahme verfolgten öffentlichen Belangs ab.[439] Der Betroffene

---

[433] BVerfGE 7, S. 208 f.; BVerfGE 66, S. 150; BVerfGE 71, S. 214; *Degenhardt* in Bonner Kommentar, Art. 5 GG; Rn. 157; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 57; kritisch: *Schmidt-Jortzig* in Isensee/Kirchhof, Band VI, § 141, Rn. 42 f.
[434] BVerfGE 30, 316; BVerfGE 33, 187; BVerfGE 67, S. 173, 175; BVerfGE 96, S. 23
[435] vgl.: 2. Kap. Teil 1 A. I.
[436] BVerfGE 53, S. 145 f.; BVerfGE 67, S. 177; BVerfGE 68, S. 219; BVerfGE 92, S. 273; ähnlich: BVerfGE 102, S. 217
[437] BVerfGE 53, S. 145 f.; BVerfGE 67, S. 177; BVerfGE 68, S. 219; BVerfGE 92, S. 273; ähnlich: BVerfGE 102, S. 217
[438] BVerfGE 77, S. 110 f.; BVerfGE 81, S. 91 f.; *Jarass* in Ders./Pieroth, Art. 20 GG, Rn. 85; *Manssen* in von Mangoldt/Klein/Starck, Art. 20 GG, Rn. 181; *Sachs* in Ders., Art. 20 GG, Rn. 152
[439] BVerfGE 30, S. 316 f.; BVerfGE 59, S. 355; BVerfGE 77, S. S. 111 ff.; *Jarass* in Ders./Pieroth, Art. 20 GG, Rn. 86; *v. Münch* in Ders./Kunig, Vorbem. Art. 1-19 GG, Rn. 55; *Sachs* in Ders., Art. 20 GG, Rn. 154

darf nicht übermäßig belastet werden.[440] Im Rahmen der Verhältnismäßigkeit im engeren Sinne sind auch die kollidierenden Rechtsgüter abzuwägen und in Ausgleich zu bringen.[441]
Es ist folglich eine Güterabwägung zwischen der Kommunikations- und Berufsfreiheit auf der einen Seite und den Grundrechten derjenigen Personenkreise durchzuführen, die solche Informationen nicht erhalten möchten.

Dieses Interesse könnte durch Art. 5 Abs. 1 GG erfasst sein. Literatur und Rechtsprechung gehen teilweise davon aus, dass Art. 5 Abs. 1 GG auch die negative Informationsfreiheit beinhaltet.[442] Diese soll dem Grundrechtsträger das Recht einräumen, sich aufgedrängten Informationen zu verschließen, nicht hinzuhören, sich nicht zu informieren und in Ruhe gelassen zu werden.[443] Auch vor unerwünschter Werbung soll er durch das Recht auf negative Informationsfreiheit geschützt sein.[444]
Aus dem Wortlaut des Art. 5 Abs. 1 GG lässt sich ein solches Recht nicht ableiten, da hier nur von der positiven Informationsfreiheit die Rede ist. Jedoch wird teilweise der Wortlaut des Art. 5 Abs. 1 GG „sich…zu unterrichten" dahingehend aufgefasst, dass das Grundrecht auf selbsttätige und selbständige Information, also auf eine eigene Auswahlentscheidung gerichtet ist.[445] Hierzu ist anzumerken, dass es zwar richtig ist, dass das Bundesverfassungsgericht den Aspekt des Auswählenkönnens als Bestandteil der Informationsfreiheit ansieht,[446] allerdings betraf diese Aussage die positive Informationsfreiheit. Der Rechtsprechung des Gerichtshofs lässt sich nicht entnehmen, dass der Betroffene auch die Möglichkeit haben muss, bestimmte Informationen noch vor deren Erhalt abzulehnen. Gegen eine Einbeziehung dieses Aspekts in den Schutzbereich des Art. 5 Abs. 1 GG spricht auch, dass das Grundrecht der Zielsetzung dient, die geistige Auseinandersetzung, den Kampf der Meinungen, zu ermöglichen.[447] Ein Verschließen vor Informationen fördert den Meinungskampf gerade nicht, was dafür spricht, dass die Auswahlfreiheit nur im Hinblick auf den Wunsch sinnvoll ist, sich aus bestimmten Quellen zu informieren.[448] Daneben ist zu berücksichtigen, dass das Bundesverfassungsgericht das Recht, in Ruhe gelassen zu werden, in Art. 1 Abs. 1 GG später in dem von dieser Gewährleistung beeinflussten allgemeinen Persönlichkeitsrecht verankert hat.[449] Der Verweis auf die Verwendung der Reflexivform des Verbs „unterrichten" überzeugt schließlich deshalb nicht, weil dieser auch lediglich die Bedeutung zukommen kann, den Adressaten der Information festzulegen, so dass sich hieraus nicht

---

[440] BVerfGE 16, S. 201 ff.; BVerfGE 22, S. 218 ff.; BVerfGE 30, S. 316 ff., 323; BVerfGE 33, S. 171; BVerfGE 67, S. 178 ff.; BVerfGE 81, S. 194 ff.; BVerfGE 83, S. 19; BVerfGE 90, S. 183
[441] *Gentz*, NJW 1968, S. 1600 ff.; *Grabitz*, AöR 98 (1973), S. 568 ff.; *Huster*, JZ 1994, 542 f.; *Schnapp*, JuS 1983, 850 ff.; *Wittig*, DÖV 1968, 817 ff.
[442] *Bethge* in Sachs, Art. 5 GG, Rn. 57 a; *Degenhardt* in Bonner Kommentar, Art. 5 Abs. 1; *Fenchel*, a.a.O., S. 76 ff.; *Fikentscher/Möllers*, NJW 1998, S. 1340; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 17; *Pieroth/Schlink*, Staatsrecht II, Rn. 566; *Wendt* in v. Münch/Kunig, Art. 5 GG, Rn. 26; a.A.: *Faber*, a.a.O., S 62 ff.; *Hoffmann-Riem in Alternativkommentar,* 3. Aufl., Art. 5 GG, Rn. 109 und 1. Aufl., Rn. 97
[443] BVerwG, NJW 1999, S. 806; *Fikentscher/Möllers*, NJW 1998, S. 1340; *Herzog* in Maunz/Dürig/Herzog, Art. 5 Abs. 1, 2 GG, Rn. 40; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 17; *Pieroth-Schlink*, Staatsrecht II, Rn. 566; *Schmidt-Jortzig* in Isensee/Kirchhoff, Band VI, § 141, Rn. 27; *Wendt* in v. Münch/Kunig, Art. 5 GG, Rn. 26; a.A. (Verankerung in (Art. 2 Abs. 1 i.V.m.) Art. 1 Abs. 1 GG: BVerfGE 27, S. 1 6 f.; - Mikrozensus; BVerfGE 44, S. S. 203 f.
[444] BVerwG, NJW 1999, S. 805 f.; *Degenhardt* in Bonner Kommentar, Art. 5 Abs. 1, 2 GG, Rn. 309; *Fikentscher/Möllers*, NJW 1998, S. 1337 ff., 1340
[445] Fenchel, a.a.O., S. 78; im Anschluss daran: *Fikentscher/Möllers*, NJW 1998, S. 1340
[446] BVerfGE 15, S. 295; BVerfGE 27, S. 83; BVerfGE 34, S. 402; zur Freiheit der Informationsauswahl: *Schmidt-Jortzig* in Isensee/Kirchhof, Band VI, § 141, Rn. 29; *Starck* in von Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 40
[447] BVerfGE 7, S. 208; BVerfGE 62, S. 247; BVerfGE 76, S. 208 f.
[448] ähnlich: *Hoffmann-Riem* in Alternativkommentar, 1. Aufl., Art. 5 Abs. 1, 2 GG, Rn. 95
[449] BVerfGE 27, S. 6- Mikrozensus; BVerfGE 44, S. 203

notwendigerweise ein Recht auf alleinige Beherrschung des Unterrichtungsvorganges ableiten lässt.[450]
Im Übrigen hindert der Zwang, bestimmte Informationen entgegenzunehmen grundsätzlich nicht an der Entgegennahme anderer Informationen und beeinträchtigt demzufolge nicht das Recht des Betroffenen, sich ungehindert zu unterrichten.[451] Dem lässt sich auch nicht entgegenhalten, dass die massenhaft versandten Werbe-Emails teilweise einen derartigen Raum in der Mailbox des Empfängers einnehmen, dass die legitimen an den Empfänger gesandten Emails durch diesen nicht mehr wahrgenommen werden können. Denn legitime Nachrichten werden in aller Regel individualisiert übersandt, so dass es sich, wie oben bereits dargestellt wurde, nicht um allgemein zugängliche Quellen handelt.
Deshalb ist davon auszugehen, dass die negative Informationsfreiheit von Art. 5 Abs. 1 GG nicht erfasst wird.

Im Rahmen seiner Schutzpflichtdimension,[452] könnte das verfassungsrechtlich geschützte allgemeine Persönlichkeitsrecht den Gesetzgeber dazu verpflichten, Email-Werbung zu beschränken, um die Rechte der hieran nicht interessierten Adressaten zu sichern.
Grundlage dieses Rechts ist Art. 2 Abs. 1 GG, wobei es durch Art. 1 Abs. 1 GG beeinflusst wird.[453] Das Grundrecht schützt die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen.[454] Vielfach wird das Recht, nicht zuhören oder bestimmte Informationen bzw. Meinungen nicht aufnehmen zu müssen, als Bestandteil des allgemeinen Persönlichkeitsrechts angesehen.[455] Für diese Auffassung spricht, dass das allgemeine Persönlichkeitsrecht den Bürger in einer Sphäre privater Lebensgestaltung zu schützen sucht.[456] In dieser Sphäre kommt ihm ein Recht auf Ruhe und Einsamkeit zu.[457] Insofern kann der Grundrechtsträger Aktivitäten entgegentreten, die in seine Privatsphäre eindringen und so versuchen, Einfluss auf seine Konsumentscheidungen zu gewinnen.[458] Das Recht, das im Rahmen der Abwägung miteinzubeziehen ist, folgt demnach aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG.
Grundrechtsträger des allgemeinen Persönlichkeitsrechts sind natürliche Personen, auch Ausländer.[459] Umstritten ist jedoch die Anwendbarkeit auf juristische Personen und Personenvereinigungen.[460] Dem steht entgegen, dass das allgemeine Persönlichkeitsrecht, wie eben dargestellt, durch Art. 1 Abs. 1 GG mitgeprägt wird, juristischen Personen jedoch ein

---

[450] dies räumt auch *Fenchel* ein, a.a.O., S. 78 f.
[451] *Fenchel*, a.a.O., S. 78
[452] BVerfGE 34, S. 281; BVerfGE 96, S. 64; BVerfGE 99, S. 194 f.; *Di Fabio* in Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 135, 189; *Jarass* in Ders./Pieroth, Art. 2 GG, Rn. 57; *Kunig* in von Münch/Kunig, Art. 2 GG, Rn. 40
[453] BVerfG, NJW 1980, S. 2072; BVerfG, NJW 1986, S. 1859; BVerfG, NJW 1995, S. 3303; BVerfG, NJW 1997, S. 1769; BVerfG, NJW 2006, S. 595; BVerfG, NJW 2006, S. 1415; *Di Fabio* in Maunz/Dürig, Art. 2 GG, Rn. 128; *Jarass*, NJW 1989, S. 857; *Ders*. in Jarass/Pieroth, Art. 2 GG, Rn. 39; *Kunig* in von Münch/Kunig, Art. 2 GG Rn. 30
[454] BVerfGE 54, S. 153; BVerfGE 72, 170
[455] BVerfG, NJW 1991, S. 911; VGH Mannheim, NJW 1990, S. 2147; *Götzfried*, NJW 1961, S. 1963; *Hoffmann-Riem* in Alternativkommentar, 3. Aufl., Art. 5 Abs. 1, 2 GG, Rn. 109; *Kimminich*, Der Staat 3 (1964), S. 75 ff.; im Bereich des Deliktsrechts: *Alt*, NJW 1986, S. 1598
[456] BVerfGE 6, S. 41 - Ausreisefreiheit
[457] BVerfGE 27, S. 6 - Mikrozensus; BVerfGE 44, S. 203; *Steindorff*, a.a.O., S. 23
[458] *Götzfried*, NJW 1963, S. 1962 f.; *Hellermann*, a.a.O., S. 183 ff.; *Hoffmann-Riem* in Alternativkommentar, 3. Aufl., Art. 5 Abs. 1, 2 GG, Rn. 109; *Kimminich*, Der Staat 3 (1964), S. 75 ff.; kritisch: *Fikentscher/Möllers*, NJW 1998, S. 1339 f.; vgl. zur politischen Beeinflussung: BVerfGE 44, S. 197 ff., 203
[459] *Jarass* in Ders./Pieroth, Art. 2 GG, Rn. 51; *Kunig* in von Münch/Kunig, Art. 2 GG, Rn. 39
[460] bejaht: BVerfGE 106, S. 28 ff., 42; BGHZ 98, S. 94 ff., 97 f.; vgl. auch: BGHZ 81, S. 75 ff., 78; BVerwGE 82, S. 76 ff., 78; verneint: BVerfGE 95, S. 220 ff., 242; *Hirte*, NJW 1988, S. 1704; *Jarass*, NJW 1989, S. 859 f.; *Kunig* in von Münch/Kunig, Art. 2 GG, Rn. 39; *Schmitt-Glaeser* in Isensee/Kirchhof, Band VI, § 129, Rn. 88; offengelassen: BVerfGE 106, S. 28 ff., 44

Recht auf Menschenwürde nicht zukommt.[461] Inländische juristische Personen und Personengesamtheiten können sich jedoch auf das subsidiäre Recht auf allgemeine Handlungsfreiheit, Art. 2 Abs. 1 GG berufen.[462]

Denkbar ist, dass Art. 14 Abs. 1 GG im Rahmen seiner Schutzpflichtdimension[463] eingreift. Allerdings gewährt Art. 14 GG nur Bestands-, keinen Erwerbsschutz.[464] Eingriffe in die Erwerbstätigkeit sind an Art. 12 GG zu messen.[465] Werbe-Emails bewirken zwar eine Verzögerung betrieblicher Abläufe, da Mitarbeiter Zeit für das Aussortieren aufwenden müssen und sich möglicherweise auch die Netzgeschwindigkeit verringert.[466] Auch kann es trotz größerer Speicherkapazitäten in Einzelfällen zu einem Überlaufen von Mailboxen kommen.[467] Allerdings wird der Bestand des Betriebs hierdurch nicht gefährdet, sondern allenfalls die Erwerbstätigkeit.
Diese ist, wie soeben dargestellt, an Art. 12 Abs. 1 GG zu messen. Allerdings wird durch das Zustellen der Werbe-Emails der Betroffene nicht daran gehindert, seine berufliche Tätigkeit auszuüben; lediglich die Tatsache, dass Zeit für das Aussortieren von Emails verwendet werden muss, bedingt noch keine Regelung der Berufsausübung. Denn im Fall eines Eingriffs wäre hier eine berufsregelnde Tendenz abzulehnen, da das Zustellen der Werbe-Emails berufsneutral ist und sich nur mittelbar auf die Berufstätigkeit auswirkt.[468] Gleiches hat zu gelten, soweit die Schutzpflichtdimension des Grundrechts betroffen ist. Danach ist davon auszugehen, dass das Interesse, von Werbung verschont zu bleiben auch nicht durch Art. 12 Abs. 1 GG geschützt ist.

Gegeneinander abzuwägen sind demnach das Recht der Werbetreibenden auf Meinungs- und Berufsfreiheit, Art. 5 Abs. 1, 12 Abs. 1 GG sowie der Informationsfreiheit der an Werbung interessierten Personenkreise auf der einen Seite und das allgemeine Persönlichkeitsrecht bzw. die allgemeine Handlungsfreiheit der Adressaten, Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG auf der anderen Seite.
Hierbei kommt den Freiheiten des Art. 5 Abs. 1 GG zwar grundsätzlich ein hoher Rang zu.[469] Etwas anderes gilt jedoch, wenn die Äußerung keine Sachverhalte betrifft, die von öffentlichem Interesse sind.[470] So wird der Meinungsfreiheit im Bereich der kommerziellen Werbung ein eher geringeres Gewicht zugebilligt, da lediglich die Förderung privater Wettbewerbsinteressen betroffen ist.[471] Aufgrund der Tatsache, dass die Informationsfreiheit Voraussetzung der Meinungsbildung ist,[472] muss Gleiches auch im Verhältnis zum Rezipienten gelten, der die Werbung erhalten möchte.

---

[461] *Jarass*, NJW 1989, S. 860; *Kunig* in von Münch/Kunig, Art. 1 GG, Rn. 11, Art. 2 GG, Rn. 39
[462] BVerfGE 10, S. 99; BVerfGE 20, S. 336; BVerfGE 70, S. 26; BVerwG, NJW 1991, S. 713; OLG Koblenz, NJW 1985, S. 2032; *Kunig* in von Münch/Kunig, Art. 2 GG, Rn. 7; *Starck* in v. Mangoldt/Klein/Starck, Art. 2 Abs. 1 GG, Rn. 46; vgl. auch: 2. Kap. Teil 1 B. I. 1. b)
[463] BVerfG, NJW 2005, S. 2365; BVerfG, NJW 2006, S. 1784; BVerwG, NVwZ 1999, S. 541
[464] BVerfG, NJW 1966, S. 1211; BVerfG, NJW 1977, S. 2027; BVerfG, NJW 1985, S. 1289; BVerfG, NJW 1993, S. 2036; BVerwGE 95, S. 348 f.
[465] BVerfGE 30, S. 334 f.; BVerfGE 65, S. 248; BGHZ 34, S. 190; BGHZ 92, S. 46; BGHZ 98, S. 351; BGHZ 111, S. 357 f.; BGH, DVBl. 1996, S. 799
[466] vgl.: 1. Kap. Teil 1 B. II. 4.
[467] vgl.: 1. Kap. Teil 1 B. II. 4.
[468] vgl.: 2. Kap. Teil 1 B. I. 1. a) bb)
[469] BVerfGE 7, S. 208; BVerfGE 35, S. 221 f.; BVerfGE 71, S. 219 f.
[470] BVerfGE 54, S. 137
[471] BVerfGE 64, S. 118 f.; BGH, NJW 1985, S. 62; BGH NJW 1987, S. 1082 f.; BGHZ 130, S. 11; Jarass, JZ 1983, S. 281
[472] *Herzog* in Maunz/Dürig, Art. 5 Abs. 1, 2 GG, Rn. 82; *Schmidt-Jortzig* in Isensee/Kirchhof, Band VI, § 141, Rn. 29; *Schulze-Fielitz* in Dreier, Art. 5 Abs. 1, 2 GG, Rn. 56; *Starck* in v. Mangoldt/Klein/Starck, Art. 5 Abs. 1, 2 GG, Rn. 37

Im Rahmen des Art. 12 Abs. 1 GG ist die vom Bundesverfassungsgericht entwickelte so genannte Stufenlehre zu beachten,[473] die vor allem bei der Verhältnismäßigkeit im engeren Sinne sowie der Erforderlichkeit eine Rolle spielt.[474] Die Stufenlehre unterscheidet drei Arten von Beeinträchtigungen der Berufsfreiheit und zwar objektive und subjektive Berufswahl- sowie Berufsausübungsbeschränkungen.[475] Hier ist nicht das „Ob" der Berufstätigkeit betroffen, sondern das „Wie", da ein Einwilligungsvorbehalt des Empfängers von Email-Werbung dem Betroffenen nicht den Zugang zum Beruf verwehrt, sondern ihm lediglich Modalitäten seiner Berufstätigkeit vorschreibt. Demnach liegt eine bloße Berufsausübungsbeschränkung vor. Selbst im Hinblick auf solche Unternehmen, deren berufliche Tätigkeit darin besteht, Werbe-Emails zu versenden, ist nicht die Berufswahl betroffen, sondern lediglich die Berufsausübung. Dies ergibt sich daraus, dass nicht der Zugang zum Beruf, also das „Ob" beschränkt wird, sondern lediglich die Tätigkeit an die Voraussetzung gebunden wird, dass vor dem Versenden der Nachrichten die Einwilligung des Versenders eingeholt wird. Insofern ist die Berufswahl nicht betroffen.
Im Bereich bloßer Berufsausübungsregelungen kommt dem Gesetzgeber ein erheblicher Beurteilungs- und Gestaltungsspielraum zu.[476] Im Rahmen der Prüfung der Verhältnismäßigkeit im engeren Sinne hat das Bundesverfassungsgericht die Formel geprägt, dass reine Berufsausübungsbeschränkungen durch jede vernünftige Erwägung des Allgemeinwohls legitimiert werden können.[477]

Dabei ist zu berücksichtigen, dass Werbung ein unverzichtbares Instrument für den Marktzugang darstellt und ohne sie bestehende Konsumgewohnheiten festzementiert würden.[478] Dieser Nachteil relativiert sich jedoch, da Email-Werbung zwar möglicherweise das kostengünstigste, keineswegs aber das einzige Medium ist, mittels dessen geworben werden kann. So steht den Werbetreibenden beispielsweise immer noch die Möglichkeit offen, durch Wurfzettel oder Werbeanzeigen in Zeitungen zu werben.
Seitens der Adressaten, die keine Werbung erhalten möchten, gewinnt die Tatsache Bedeutung, dass die versandten Werbe-Emails, deren Volumen stetig ansteigt,[479] einen immer größeren Zeitaufwand für die Empfänger verursachen und diese mit immer mehr unerwünschten Themen konfrontieren. Insofern wird die Beeinträchtigung, die darin liegt, dass die Betroffenen ihre Zeit nicht wie gewünscht verbringen können und sich einer unerwünschten Beeinflussung ausgesetzt sehen, mit steigendem Werbe-Email-Aufkommen immer tiefgreifender.
Schließlich ist zu berücksichtigen, dass die Beschränkung der Werbemöglichkeit nicht besonders schwerwiegend ist. Zum einen nimmt die Ausnahmevorschrift des § 7 Abs. 3 UWG solche Adressaten vom Anwendungsbereich der wettbewerbs- und deliktsrechtlichen Opt-In-Lösung aus, zu denen bereits zuvor ein geschäftlicher Kontakt bestand. Zum anderen kann der Werbetreibende die Einwilligung des Adressaten einholen und anschließend rechtmäßig Email-Werbung an diesen versenden. Insofern werden die Rechte der Werbetreibenden und der interessierten Adressaten nicht vollständig zurückgedrängt. Allerdings wird diese Form der Werbung auch nicht uneingeschränkt zugelassen, was zu einem einseitigen Zurücktreten der Rechte derjenigen Adressaten führen würde, die Email-Werbung nicht empfangen möchten. Diese sind dadurch geschützt, dass ihnen Email-Werbung nur zugestellt werden

[473] BVerfG, NJW 1958, S. 1039 f.; BVerfG, NJW 1969, S. 499
[474] BVerfG, NJW 1958, S. 1038
[475] BVerfG, NJW 1958, S. 1035 ff.; BVerfG, NJW 1978, S. 313 f.
[476] BVerfGE 46, S. 256 f.; BVerfGE 77, S. 332; BVerfGE 88, S. 262; BVerfGE 102, S. 218; BVerfGE 110, S. 157
[477] BVerfGE 7, S. 405 f.; BVerfGE 16, S. 297; BVerfGE 65, S. 125; BVerfGE 70, S. 28; BVerfGE 78, S. 162; BVerfGE 85, S. 259; BVerfGE 103, S. 10
[478] *Lüder*, EuZW 1996, S. 615
[479] vgl.: 1. Kap. Teil 1 B. II. 4.

darf, wenn sie zuvor ihre Einwilligung erklärt haben. Insofern werden durch das im deutschen Recht geltende Opt-In-Prinzip die kollidierenden Grundrechte in einen angemessenen Ausgleich gebracht, dergestalt, dass keines zugunsten des jeweils anderen zu weitgehend eingeschränkt wird. Die Verhältnismäßigkeit im engeren Sinne ist danach gegeben.

bb) Weitere Schranken-Schranken

Den Garantiebereichen der Grundrechte der Meinungsäußerungs- und Berufsfreiheit unterfallen auch dann noch hinreichend wichtige Schutzgüter, wenn die Email-Direktwerbung von der Einwilligung des Adressaten bzw. von einem bereits zuvor existenten Geschäftskontakt abhängig gemacht wird[480] und es liegt wie oben[481] gezeigt auch keine übermäßige Einschränkung der Schutzbereiche vor.[482] Der Wesensgehalt der im Raum stehenden Grundrechte ist demnach weder unter Zugrundelegung der absoluten,[483] noch der relativen[484] Theorie angetastet. Das Zitiergebot des Art. 19 Abs. 1 S. 2 GG findet auf die allgemeinen Gesetze des Art. 5 Abs. 2 GG keine Anwendung.[485] Auch im Bereich der Berufsfreiheit gilt es nicht.[486]

c) Sonderfall: Politische Werbung

Es wurde bereits dargestellt, dass die durch das Delikts- und Strafrecht bewirkten Beschränkungen der Möglichkeit, politische Email-Werbung zu versenden, als Eingriffe in den Schutzbereich des Art. 21 Abs. 1 GG anzusehen sind.[487] Allerdings sind auch im Bereich der politischen Email-Werbung die Interessen derjenigen Empfänger zu berücksichtigen, die solche Werbung nicht erhalten möchten.[488] Die Rechte der Adressaten sind gegenüber dem Interesse der Parteien abzuwägen, politische Werbung zu versenden.[489] Im Bereich der Briefkastenwerbung fällt diese Abwägung zugunsten solcher Empfänger aus, die kundgetan haben, keine Werbung erhalten zu wollen.[490]

Fraglich ist, ob Gleiches für die Email-Werbung gilt. Das Anbringen eines Hinweises dahingehend, dass Werbe-Emails unerwünscht sind, ist nicht möglich. Auch hier ist jedoch das Problem der Kostenverlagerung auf den Empfänger zu berücksichtigen, das bereits angesprochen wurde.[491] Darüber hinaus ist zu beachten, dass die in dem Aufdrängen von unerwünschtem Werbematerial liegende Beeinträchtigung nicht nur bei kommerziellen Äußerungen, sondern auch dann gegeben ist, wenn es sich um Werbematerial einer politischen Partei handelt.[492] Ob es sich um eine zu duldende sozialadäquate Beeinträchtigung handelt, hängt insofern nicht vom Inhalt der Werbung, sondern von dem Ausmaß ab, das die Werbung nach Quantität und Intensität erreicht hat.[493] Schließlich wird die Parteienwerbung

---

[480] dies fordern die Vertreter der absoluten Theorie: *G. Dürig*, AöR 81 (1956), S. 156; *Krüger*, DÖV 1955, S. 597
[481] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[482] auf dieses Kriterium stellen die Vertreter der relativen Theorie ab: BVerwGE 2, S. 94; *Alexy*, a.a.O., S. 272; *Häberle*, a.a.O., S. 64; *v. Hippel*, a.a.O., S. 56 ff.; *Maunz* in Ders./Dürig, Art. 19 Abs. 2 GG, Rn. 29
[483] vgl. dazu: Fn. 517
[484] vgl. dazu: Fn. 519
[485] BVerfGE 28, S. 289, 291 ff.; BVerfGE 33, S. 77 f.; BVerfGE 44, S. 201 f.; BVerfGE 64, S. 80
[486] BVerfGE 7, S. 404; BVerfGE 13, S. 122; BVerfGE 28, S. 46; BVerfGE 64, 80 f.
[487] vgl.: 2. Kap. Teil 1 B. I. 1. a) cc)
[488] BVerfG, NJW 2002, S. 2939
[489] BVerfG, NJW 2002, S. 2939
[490] BVerfG, NJW 2002, S. 2939
[491] vgl.: 1. Kap. Teil 1 B. II. 4.
[492] OLG Bremen, NJW 1990, S. 2140 f.
[493] OLG Bremen, NJW 1990, S. 2140 f. unter Verweis auf BGH, NJW 1989, S. 902 f.

nicht dadurch in Frage gestellt, dass die Parteien bestimmte Werbemittel nur an solche Empfänger versenden dürfen, die dem Erhalt er Werbung zuvor zugestimmt haben,[494] da immer noch an interessierte Adressaten Werbung versandt sowie auf alternative Werbeformen zurückgegriffen werden kann. Im Übrigen entspricht dem Recht der Parteien, ihrer politischen Tätigkeit ungehindert nachgehen zu dürfen keine Pflicht des Bürgers, sich von den Parteien informieren lassen zu müssen.[495]

Nach alledem besteht kein Anlass die Bürger in ihrem Recht in Ruhe gelassen zu werden gegenüber politischer Parteiwerbung einzuschränken, da das Ausmaß der Störung und Beeinträchtigung das Gleiche ist, wie im Fall der kommerziellen Werbung.[496] Danach kann von den Parteien verlangt werden, entweder vor Zusenden des Werbematerials das Einverständnis des Empfängers einzuholen oder aber auf eingriffsärmere Möglichkeiten, wie Plakate, Informationsstände sowie Zusendung oder Verteilung von Flugblättern auszuweichen.[497]

3. Zwischenergebnis

Es lässt sich festhalten, dass die angesprochenen Normen des Wettbewerbs-, Delikts- und Strafrechts verfassungsgemäß sind.

II. Völkerrecht und Gemeinschaftsrecht

Fraglich ist, ob die Vorschriften des deutschen einfachen Rechts, welche eine Beschränkung der Zulässigkeit der Email-Werbung bewirken, im Einklang mit dem Völker- und Gemeinschaftsrecht stehen.

1. Gemeinschaftsrecht

Es könnte ein Verstoß gegen primäres Gemeinschaftsrecht vorliegen. Dies würde zwar nicht zur Nichtigkeit der Vorschriften des gemeinschaftsrechtswidrigen einfachen Gesetzesrechts führen, jedoch wären in diesem Fall sämtliche staatlichen Stellen, insbesondere Gerichte und Behörden dazu verpflichtet, dem Gemeinschaftsrecht den Vorrang einzuräumen und die gemeinschaftswidrige nationale Norm außer Anwendung zu lassen.[498] Im Falle eines Verstoßes gegen Sekundärrecht könnte sich die unmittelbare Wirkung[499] der Richtlinie bzw.

---

[494] OLG Bremen, NJW 1990, S. 2140 f.
[495] KG, NJW 2002, S. 380
[496] OLG Bremen, NJW 1990, S. 2140 f.; KG, NJW 2002, S. 380; LG München I, MMR 2003, S. 283; aA.: *Löwisch*, NJW 1990, S. 437 f.
[497] LG München I, MMR 2003, S. 283
[498] EuGH, Rs. 6/64, Slg. 1964, S. 1251 ff., 1270 - Costa/E.N.E.L; EuGH, Rs. 11/70, Slg. 1970, S. 1125, Rn. 3 - Internationale Handelsgesellschaft; EuGH, Rs. 106/77, Slg. 1978, S. 629, Rn. 13 ff. - Simmenthal II; EuGH, Rs. 103/88, Slg. 1989, S. 1839, Rn. 28 ff. - Costanzo; EuGH, Rs. C-184/89, Slg. 1991, S. I-297, Rn. 19 - Nimz; EuGH, Rs. C-431/92, Slg. 1995, S. I-2189, Rn. 37 ff. - Großkrotzenburg; BVerfGE 73, S. 366 ff.-Solange II; BVerfGE 75, S. 235 ff.- Kloppenburg; BVerfGE 89, S. 155, 190 – Maastricht; *Hatje* in Schwarze, Art. 10 EGV, Rn. 21 f.; *Hetmeier* in Lenz/Borchardt, Art. 249 EGV, Rn. 23 f.; *Schroeder* in Streinz, Art. 249 EGV, Rn. 43; *Wegener* in Calliess/Ruffert, Art. 220 EGV, Rn. 23
[499] EuGH, Rs. 41/74, Slg. 1974, S. 1337, Rn. 12 - van Duyn/Home Office; EuGH, Rs. 51/76, Slg. 1977, S. 113, Rn. 20/24 - Nederlandse Ondernemingen; EuGH, Rs. 21/78, Slg. 1978, S. 2327, Rn. 18/21 - Delkvist; EuGH, Rs. 148/78, Slg. 1979, S. 1629, Rn. 20 - Ratti; EuGH, Rs. 8/81, S. 53, Rn. 22 - Becker; EuGH, Rs. 152/84, Slg. 1986, S. 723, Rn. 47 - Marshall II; EuGH, Rs. 71/85, Slg. 1986, S. 3855 - Federatie Nederlandse Vakbeweging; EuGH, Rs. 286/85, Slg. 1987, S. 1453, Rn. 12 - McDermott und Cotter; EuGH, Rs. 80/86, Slg. 1987, S. 3969, Rn. 8 - Kolpinhuis Nijmegen; EuGH, Rs. C- 208/90, Slg. 1991, S. I- 4269, Rn. 20 - Emmott; BVerwGE 70, S. 49; BVerwGE 74, S. 247

eine Verpflichtung zur richtlinienkonformen Auslegung[500] der im Raum stehenden nationalen Vorschrift ergeben.

Im Folgenden wird das deutsche Recht am Maßstab des europäischen Sekundär- (a) und Primärrechts (b) überprüft.

a) Sekundärrecht

Auf der Ebene des Sekundärrechts könnten die EK-DSRL[501] (aa), die E-Commerce-Richtlinie[502] (bb) und die Fernabsatz-Richtlinie[503] eingreifen. Es ist zu prüfen, ob die deutsche Regelung im Einklang mit diesen Richtlinien steht.

aa) EK-DSRL

Den entscheidenden Einfluss auf die nationale Rechtslage übt die EK-DSRL aus. Art. 13 Abs. 1 EK-DSRL lässt elektronische Direktwerbung nur bei vorheriger Einwilligung des Empfängers zu. Diese strikte Opt-In-Regelung wird allerdings für den Bereich der elektronischen Post unter den Voraussetzungen des Art. 13 Abs. 2 EK- DSRL insgesamt zu einem so genannten „Soft-Opt-In“.[504] Die Vorschrift wurde in Deutschland durch § 7 Abs. 2 Nr. 2 und Abs. 3 UWG umgesetzt und enthält nahezu den gleichen Wortlaut.[505] Ein Verstoß der deutschen Regelung gegen Art. 13 Abs. 1 EK-DSRL kommt danach nicht in Betracht.

Fraglich ist, ob die §§ 823 Abs. 1, 1004 Abs. 1 BGB nebst der dazu ergangenen Rechtsprechung mit Art. 13 Abs. 1 EK-DSRL im Einklang stehen. Die Vorschriften sprechen bei Verletzung bestimmter Rechtsgüter Schadensersatz- und Unterlassungsansprüche zu. Art. 13 Abs. 1 EK-DSRL war bis 31.Oktober 2003 in deutsches Recht umzusetzen, Art. 17 Abs. 1 EK-DSRL. Allerdings wurden die soeben genannten Vorschriften durch den Gesetzgeber nicht abgeändert oder ergänzt. Es stellt sich die Frage, ob die Vorschriften richtliniengemäß sind. Email-Werbung greift nach nahezu einhelliger Rechtsprechung der Instanzengerichte in das allgemeine Persönlichkeitsrecht des Empfängers ein, das als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anerkannt ist, und dessen Verletzung auch im Rahmen des § 1004 Abs. 1 BGB zu einem Unterlassungsanspruch führt.[506] Daneben wird überwiegend ein Eingriff in das Recht auf den eingerichteten und ausgeübten Gewerbebetrieb bejaht.[507] Bei der Prüfung der Verletzung des allgemeinen Persönlichkeitsrechts und des Rechts auf den eingerichteten und

---

[500] EuGH, Rs. 14/83, Slg. 1984, S. 1909 - von Colson und Kamann/Land Nordrhein-Westfalen; EuGH, Rs. 79/83, Slg. 1984, S. 1942 - Harz/Deutsche Tradax; EuGH, Rs. 222/84, Slg. 1986, S. 1690 - Johnston/Chief Constable of the Royal Ulster Constabulary; EuGH, Rs. 31/87, Slg. 1988, S. 4655, 4662 - Beentjes/Niederlande; EuGH, Rs. C-106/89, Slg. 1990, S. I-4158 - Marleasing/La Commercial Internacional de Alimentación SA; EuGH, Rs. C-334/92, Slg. 1993, S. I-6932 - Wagner Miret/Fondo de garantía salarial; EuGH, Rs. C-91/92, Slg. 1994, S. I-3357 - Faccini Dori/Recreb

[501] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 105, S. 54 ff.

[502] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG Nr. L 178 v. 17.7.2000, S. 1 ff.

[503] Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABl. EG Nr. L 144/19

[504] *Eckhardt*, MMR 2003, S. 558; *Ohlenburg*, MMR 2003, S. 84; *Weiler*, MMR 2003, S. 227; vgl. auch: 2. Kap. Teil 1 A. II.

[505] vgl.: 2. Kap. Teil 1 A. II.

[506] vgl.: 2. Kap. Teil 1 A. III. 1. a) aa)

[507] vgl.: 2. Kap. Teil 1 A. III. 1. a) bb)

ausgeübten Gewerbebetrieb trägt die Rechtsprechung dabei im Rahmen der Interessens- und Güterabwägung, die zur Begründung der Widerrechtlichkeit vorzunehmen ist,[508] auch den gemeinschaftsrechtlichen Vorschriften Rechnung.[509] Die Rechtslage entspricht demnach bereits den gemeinschaftsrechtlichen Vorgaben, indem von der Unzulässigkeit von Email-Werbung ausgegangen wird, sofern der Empfänger nicht zuvor seine Einwilligung erklärt hat bzw. wird hierauf schon explizit Bezug genommen.[510] Die in Deutschland bestehende Rechtslage steht danach nicht im Widerspruch zu den Vorgaben der EK-DSRL. Angesichts der Tatsache, dass der EuGH für die Umsetzung einer Richtlinie in innerstaatliches Recht nicht notwendig verlangt, dass ihre Bestimmungen förmlich oder wörtlich in einer ausdrücklichen, besonderen Gesetzesvorschrift wiedergegeben werden, sondern dass auch ein allgemeiner rechtlicher Rahmen genügen kann,[511] ist auch die in der Literatur geäußerte Auffassung, die Richtlinie sei mangelhaft umgesetzt worden,[512] zurückzuweisen. Zwar ist es richtig, dass im Rahmen des UWG keine individuellen Schadensersatzansprüche bestehen,[513] allerdings kann sich der Betroffene auf §§ 823, 1004 BGB berufen und so zivilrechtlich seine Ansprüche verfolgen. Diese sind durch die Rechtsprechung der Instanzengerichte und des Bundesgerichtshofs mittlerweile hinreichend konkretisiert, indem Werbung ohne vorherige Zustimmung grundsätzlich als unzulässig erachtet sowie bereits explizit auf die Vorgaben der EK-DSRL Bezug genommen wird.[514] Die Umsetzung der Vorgaben der Richtlinien ist demnach gewährleistet; der Einzelne kann seine Rechte nach den Vorgaben von UWG sowie der zu den §§ 823, 1004 BGB ergangenen Rechtsprechung einschätzen und diese auch gerichtlich durchsetzen. Die im deutschen Recht bestehende Rechtslage entspricht den Vorgaben der Richtlinie.
§ 303 a Abs. 1 StGB verstärkt den auf zivilrechtlicher Ebene bestehenden Schutz sogar noch, indem bestimmte Fälle strafrechtlich sanktioniert werden. Da § 303 a Abs. 1 StGB ein Schutzgesetz im Sinne des § 823 Abs. 2 BGB ist, bestehen dann auch zivilrechtliche Ansprüche des Adressaten.[515] Diese Regelung verstößt nicht gegen die EK-DSRL, denn auch hier gilt das gemeinschaftsrechtlich festgeschriebene Opt-In-Prinzip, da der Empfänger dem Tatbestand durch seine Einwilligung die Rechtswidrigkeit nehmen kann.[516]

Ein Verstoß gegen die EK-DSRL liegt daher nicht vor.

bb) E-Commerce-Richtlinie

Der geltende Rechtslage könnte jedoch die E-Commerce-Richtlinie entgegenstehen, die zeitlich vor der EK-DSRL erlassen wurde und ebenfalls den Bereich der Email-Werbung betrifft. Die Richtlinie enthält in Art. 7 Abs. 1 eine Regelung, welche die Mitgliedstaaten, die nicht angeforderte Email-Werbung zulassen, zu Maßnahmen verpflichtet, die sicherstellen, dass solche Nachrichten als Werbung erkennbar sind. Darüber hinaus haben die Mitgliedstaaten nach Art. 7 Abs. 2 ECRL dafür zu sorgen, dass Diensteanbieter, die Werbe-

[508] vgl.: 2. Kap. Teil 1 A. III. 1. c) aa)
[509] BGH, NJW 2004, S. 1657- Email-Werbung
[510] BGH, NJW 2004, S. 1655 ff., 1657- Email-Werbung
[511] EuGH, Slg. 1985, S. 1661, Leitsatz 1- Kommssion/Deutschland; EuGH, Slg. 1987, S. 173, Leitsatz- Kommission/Italien; EuGH, Slg. 1989, S. 143- Kommission/Italien; EuGH, Rs. 339/87, Slg. 1990, S. I-851 ff.- Kommission/Niederlande
[512] *Brömmelmeyer*, GRUR 2006, S. 291 f.
[513] so die Kritik von *Brömmelmeyer*, GRUR 2006, S. 291 f.
[514] vgl.: 2. Kap. Teil 1 A. III. 1.; vgl. auch: BGH, NJW 2004, S. 1657- E-Mail-Werbung ; vgl. zur Umsetzungspflicht trotz bereits bestehender richtlinienkonformer Auslegung durch mitgliedstaatliche Gerichte bei fehlender Klarheit und Bestimmtheit: EuGH, EuZW 2001, S. 438
[515] vgl.: 2. Kap. Teil 1 A. III. 2. b)
[516] vgl.: 2. Kap. Teil 1 A. II.

Emails versenden, regelmäßig so genannte Robinson-Listen konsultieren, in denen sich solche natürlichen Personen eintragen können, die keine derartige kommerzielle Kommunikation erhalten möchten.

Früher wurde teilweise aus Art. 7 ECRL gefolgert, dass Email-Werbung auch ohne vorherige Zustimmung des Empfängers zulässig sein müsse, da andernfalls die Vorschrift leer laufe.[517] Diese Argumentation widerspricht jedoch dem Wortlaut der Richtlinie. Denn Erwägungsgrund Nr. 30 stellt klar, dass die ECRL keine Aussage zu der Frage trifft, ob der Empfänger einer unverlangten Email vorher seine Zustimmung erklären muss oder nicht.[518] Im Übrigen ist die mittlerweile ergangene Regelung des Art. 13 EK-DSRL zu beachten, die insofern Rechtsklarheit schafft.

cc) Fernabsatz-Richtlinie

Die Fernabsatz-Richtlinie stellte den ersten Versuch des europäischen Gesetzgebers dar, dem ungehemmten Einsatz von Email als Marketingsinstrument einen Riegel vorzuschieben.[519] Werden zum Zweck der Direktwerbung Automaten als Gesprächspartner oder Telefax eingesetzt, so gilt nach Art. 10 Abs. 1 FARL das Opt-In-Prinzip. Hinsichtlich nicht in Abs. 1 genannter Fernmeldekommunikationstechniken, die eine individuelle Kommunikation erlauben, verpflichtet Abs. 2 die Mitgliedstaaten, dafür Sorge zu tragen, dass sie nur dann verwendet werden dürfen, wenn der Verbraucher dies nicht offenkundig abgelehnt hat. Da Email-Werbung als individuelles Kommunikationsmittel der Opt-Out-Regelung des Abs. 2 unterfällt, ist sie im Anwendungsbereich der FARL demnach zulässig, sofern der Verbraucher ihre Verwendung nicht offenkundig abgelehnt hat.
Aufgrund dieser Regelung war lange Zeit umstritten, ob aus Art. 10 Abs. 2 FARL eine mitgliedstaatliche Verpflichtung resultiert, die werbliche Ansprache mittels Email gesetzlich zuzulassen, soweit der Empfänger dies nicht zuvor ausdrücklich abgelehnt hat. Der deutsche Gesetzgeber sah einen derartigen Umsetzungsbedarf allerdings nicht als gegeben an.[520] Teilweise wurde diese Haltung kritisiert und der Vorwurf erhoben, in Deutschland bestünde eine richtlinienwidrige Rechtslage.[521]

Mittlerweile hat sich der Streit jedoch durch den Erlass der EK-DSRL erledigt. Denn nach Art. 13 Abs. 1 EK-DSRL gilt grundsätzlich das -durch Abs. 2 der Vorschrift abgeschwächte- Opt-In-Prinzip. Aus Erwägungsgrund Nr. 17 der FARL ist erkennbar, dass im Bereich der unverlangten Kontaktaufnahme solche Garantien von der Richtlinie unberührt bleiben, die dem Verbraucher auf Grund gemeinschaftsrechtlicher Vorschriften über den Schutz der Privatsphäre und personenbezogener Daten zustehen. Daher ist davon auszugehen, dass die Vorschrift des Art. 13 EK-DSRL im Bereich der Email-Werbung das liberale Konzept des Art. 10 Abs. 2 FARL verdrängt.[522] Somit sind die vormals geäußerten Zweifel an der Zulässigkeit des Opt-In-Prinzips nunmehr ausgeräumt.[523]

---

[517] *Ziem*, MMR 2000, S. 134
[518] *Ayad*, CR 2001, S. 537; *Lettl*, GRUR 2000, S. 984; *Schrick*, MMR 2000, S. 404; *Spindler/Schmittmann*, MMR 2001/Beilage 8, S. 14
[519] *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 83; *Weiler*, MMR 2003, S. 223
[520] *Weiler*, MMR 2003, S. 224; *Zehentmeier*, BB 2000, S. 944
[521] *Lettl*, GRUR 2000, S. 982; *Vehslage*, GRUR 1999, S. 658; *Weiler*, MMR 2003, S. 224; *Zehentmeier*, BB 2000, S. 943; zweifelnd: LG Berlin, MMR 1999, S. 43 f.
[522] *Brömmelmeyer*, GRUR 2006, S. 287; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 83; *Weiler*, MMR 2003, S. 228; *Wendlandt*, MMR 2004, S. 366
[523] *Brömmelmeyer*, GRUR 2006, S. 287; *Köhler* in Baumbach/Köhler/Bornkamm, § 7 UWG, Rn. 83; *Weiler*, MMR 2003, S. 228; *Wendlandt*, MMR 2004, S. 366

dd) Zwischenergebnis

Im Ergebnis verstößt die Rechtslage in Deutschland weder gegen die Fernabsatz-Richtlinie, noch gegen die E-Commerce-Richtlinie oder die Datenschutzrichtlinie für elektronische Kommunikation.

b) Primärrecht

Fraglich ist, ob die Vorschriften des einfachen deutschen Rechts, die dazu führen, dass Email-Werbung nicht uneingeschränkt zulässig ist, im Einklang mit europäischem Primärrecht stehen. Ein Verstoß würde, wie oben dargestellt, zu einem Anwendungsvorrang der entsprechenden gemeinschaftsrechtlichen Norm führen.[524]

In diesem Zusammenhang ist auch die Frage der Rechtmäßigkeit des Sekundärrechts zu überprüfen, auf dessen Grundlage das nationale Recht erlassen wurde,[525] da primärrechtswidriges Sekundärrecht im Rahmen einer Nichtigkeitsklage für unwirksam erklärt werden kann, Art. 230, 231 EGV; dies hätte wiederum zur Folge, dass auch der nationale Umsetzungsakt förmlich außer Kraft zu setzen und soweit erforderlich durch neue rechtmäßige Maßnahmen zu ersetzen wäre.[526]

aa) Europäische Grundfreiheiten

Die Vorschriften des deutschen Rechts und die Regelung in Art. 13 Abs. 1 EK-DSRL könnten rechtswidrig in die Waren- oder Dienstleistungsfreiheit eingreifen, Art. 28 ff. bzw. 49 ff. EGV. Nicht die Grundfreiheiten, sondern das speziellere Sekundärrecht ist jedoch Prüfungsmaßstab für das nationale Recht, wenn bereits eine abschließende Rechtsharmonisierung erfolgt ist.[527] Art. 13 Abs. 1 und Abs. 2 EK-DSRL bewirken eine Harmonisierung der Frage nach der Zulässigkeit elektronischer Direktwerbung. Sie finden jedoch nur dann Anwendung, wenn der Adressat der Werbe-Email eine natürliche Person ist, vgl. Art. 13 Abs. 5 S. 1 EK-DSRL. Folglich ist nationales Recht, das die Frage der Email-Direktwerbung gegenüber natürlichen Personen betrifft, nicht am Maßstab der Grundfreiheiten des EGV, sondern nur auf seine Übereinstimmung mit dem einschlägigen Sekundärrecht, hier der EK-DSRL zu überprüfen.[528] Im Übrigen, das bedeutet hinsichtlich mitgliedstaatlicher Vorschriften, die Email-Direktwerbung gegenüber Adressaten betreffen, die keine natürliche Person sind, bleiben die Grundfreiheiten anwendbar. Daneben sind, wie soeben ausgeführt, die sekundärrechtlichen Regelungen an den Grundfreiheiten zu messen.

Der Schutzbereich der Waren- und Dienstleistungsfreiheit ist nur dann eröffnet, wenn ein grenzüberschreitender Sachverhalt vorliegt, das bedeutet der Waren- oder Dienstleistungsverkehr zwischen den Mitgliedstaaten betroffen ist.[529] Daneben muss die

---

[524] vgl.: 2. Kap. Teil 1 B. II. 1.
[525] vgl.: 2. Kap. Teil 1 A. II.
[526] *Borchardt* in Lenz, Art. 233 EGV, Rn. 6; *Cremer* in Calliess/Ruffert, Art. 233 EGV, Rn. 5; *Gaitanides* in v. d. Groeben/Schwarze, Art. 231 EGV, Rn. 5, Art. 233 EGV, Rn. 12
[527] EuGH, Slg. 1993, S. I- 4978, Rn. 9 - Strafverfahren gegen José Vanacker und André Lesage; EuGH, EuZW 2002, S. 91- Daimler Chrysler; EuGH, NJW 2004, S. 133- DocMorris; *Ehlers* in Ehlers, § 7 Rn. 7; *Frenz*, Handbuch Europarecht, Band 1, Rn. 350
[528] vgl. hierzu bereits: 2. Kap. Teil 1 B. II. 1. a) cc)
[529] zur Warenverkehrsfreiheit: EuGH, Slg. 1987, S. 823, Rn. 12 - Mathot; EuGH, Slg. 1987, S. 1002, Rn. 7 - Rousseau; *Becker* in Schwarze, Art. 28 EGV, Rn. 19 ff.; *Epiney* in Calliess/Ruffert, Art. 28 EGV, Rn. 43; *Schroeder* in Streinz, Art. 28 EGV, Rn. 20 f.; zur Dienstleistungsfreiheit: EuGH, Slg. 1980, S. 833, Rn. 9- Debauve; EuGH, Slg. 1991, S. I-727, Rn. 9-Kommission/Griechenland; EuGH, Slg. 1991, S. I-1979, Rn. 37-39-

fragliche Maßnahme eine Ware im Sinne des Art. 23 Abs. 2 EGV bzw. eine Dienstleistung im Sinne des Art. 50 Abs. 1 EGV betreffen.

Sind diese Voraussetzungen erfüllt, so stellt sich die Frage, ob die Möglichkeit, für Waren und Dienstleistungen kommerziell zu werben, Inhalt der Grundfreiheiten gemäß Art. 28 ff., 49 ff. EGV ist. Dabei ist zu berücksichtigen, dass die Produktwerbung Voraussetzung eines erfolgreichen Warenvertriebs ist.[530] Ohne Werbung würden Kunden auf unbestimmte Zeit einem bestimmten Produkt die Treue halten, da sie von dem neuen Produkt unter Umständen gar keine Kenntnis erlangen würden. Folglich stellt die Möglichkeit der Produktwerbung ein unverzichtbares Instrument für den Marktzugang dar, insbesondere für neue Wettbewerber.[531] Dies bedeutet, dass Werbebeschränkungen dazu beitragen, bestehende Einkaufsgewohnheiten der Verbraucher festzuzementieren und zugunsten der etablierten Anbieter den status quo zu erhalten.[532] Die Produktwerbung ist damit Voraussetzung eines erfolgreichen Warenvertriebs, weshalb sie als integraler Bestandteil der Warenverkehrsfreiheit anzusehen ist.[533] Das Gleiche hat im Bereich der Dienstleistungsfreiheit zu gelten, da die Sachlage hier identisch ist.

Grundfreiheitsträger sind natürliche Personen, die Staatangehörigen der Mitgliedstaaten sind sowie nach den Rechtsvorschriften eines Mitgliedstaats gegründete Gesellschaften mit satzungsmäßigem Sitz bzw. Hauptverwaltung oder -niederlassungen innerhalb der Gemeinschaft.[534] Für die Dienstleistungsfreiheit ergibt sich dies aus Art. 55 EGV, der auf Art. 48 EGV verweist. Diese Grundsätze werden auf den Bereich der Warenverkehrsfreiheit erstreckt.[535]

Fraglich ist, ob in den Vorschriften des einfachen deutschen Rechts eine Beschränkung des Schutzbereichs der Waren- und Dienstleistungsfreiheit zu sehen ist. Dies setzt einerseits voraus, dass die Maßnahme die Vorgaben der Dassonville-Formel bzw. der entsprechenden Umschreibung im Bereich der Dienstleistungsfreiheit erfüllt (1), andererseits darf keine bestimmte Verkaufsmodalität im Sinne der Keck-Rechtsprechung (2) und keine zulässige Beschränkung im Sinne der Cassis-Rechtsprechung (3) vorliegen.

Höfner und Elser; EuGH, Slg. 1994, S. I-4795, Rn. 14-TV 10; EuGH, Slg. 1995, S. I-6511, Rn. 14 - Reisebüro Broede; EuGH, Slg. 1997, S. I- 195, Rn. 19- USSL N° 47 di Biella; EuGH, Slg. 1997, S. I-3395, Rn. 38- Sodemare; *Holoubek* in Schwarze, Art. 49 EGV, Rn. 44 ff.; *Kluth* in Calliess/Ruffert, Art. 49 EGV, Rn. 23; *Müller-Graff* in Streinz, Art. 49 EGV, Rn. 31 ff.

[530] *Lüder*, EuZW 1996, S. 615

[531] Schlussanträge der Generalanwältin Stix-Hackl, Slg. 2003, S. 14887 ff., 14934, Rn. 177 f.; *Lüder*, EuZW 1996, S. 615

[532] EuGH, Slg. 1990, S. I-667, R. 8 ff.-GB-INNO; EuGH, Slg. 1990, S. I-4695, Rn. 29-SARPP; EuGH, Slg. 1993, S. I-2361, Rn. 23-Yves Rocher; *Lüder*, EuZW 1996, S. 615

[533] EuGH, Slg. 1990, S. I-667, R. 8 ff.-GB-INNO; EuGH, Slg. 1990, S. I-4695, Rn. 29-SARPP; EuGH, Slg. 1993, S. I-2361, Rn. 23-Yves Rocher; EuGH, Slg. 2003, S. 14939, Rn. 2- Doc Morris; Lüder, EuZW 1996, S. 615

[534] *Frenz*, Handbuch Europarecht, Band 1, Grundfreiheiten, Rn. 224 ff.; *Troberg/Tiedje* in von Groeben/Schwarz, Art. 48 EGV, Rn. 1

[535] EuGH, Slg. 1979, S. 649 - Cassis; *Frenz*, Handbuch Europarecht, Band 1, Rn. 224 ff.

(1) Vorgaben der Dassonville-Formel bzw. der entsprechenden Umschreibung im Bereich der Dienstleistungsfreiheit

Im Rahmen der Dienstleistungsfreiheit fasst der EuGH den Beschränkungsbegriff sehr weit.[536] Eine Beschränkung liegt danach nicht erst vor, wenn Dienstleistungen unterbunden oder behindert werden, sondern bereits dann, wenn ihre Erbringung durch die fragliche Regelung weniger attraktiv gemacht wird.[537] So sah der EuGH ein mitgliedstaatliches Verbot, mit potentiellen Kunden telefonisch oder persönlich in Verbindung zu treten, wenn diese nicht zuvor ausdrücklich schriftlich ihre Einwilligung erklärt haben, als Beschränkung der Dienstleistungsfreiheit an.[538] Dies begründete er damit, dass ein derartiges Verbot den Zugang zum Dienstleistungsmarkt in anderen Mitgliedstaaten beeinflusst und folglich geeignet ist, den innergemeinschaftlichen Dienstleistungsverkehr zu behindern.[539] Die gleiche Wirkung hat ein Verbot, Email-Werbung zu betreiben bzw. ein Erschwernis der Möglichkeit, sich dieses Instruments des Direktmarketing zu bedienen, weshalb sich die zitierte Rechtsprechung hierauf übertragen lässt. Die genannten Vorschriften des deutschen einfachen Rechts erfüllen demnach die Vorgaben, die der EuGH an den Beschränkungsbegriff stellt.

Im Bereich der Warenverkehrsfreiheit sind Ein- oder Ausfuhrbeschränkungen oder Maßnahmen gleicher Wirkung verboten, Art. 28, 29 EGV. Da die Warenein- und -ausfuhr nicht wie für die Annahme einer Ein- oder Ausfuhrbeschränkung erforderlich[540] der Menge oder dem Wert nach begrenzt bzw. völlig untersagt wird, liegt hier keine mengenmäßige Ein- oder Ausfuhrbeschränkung vor. Eine Maßnahme gleicher Wirkung wie eine Einfuhrbeschränkung ist nach der vom EuGH entwickelten so genannten Dassonville-Formel in jeder staatlichen Regelung zu sehen, die geeignet ist, den innergemeinschaftlichen Handel unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern.[541] Email-Werbung ist ein schnelles und kostengünstiges Mittel der Kontaktaufnahme; insofern wird der innergemeinschaftliche Handel durch nationale Gesetze, die diese Art des Direktmarketing restringieren zumindest mittelbar und potentiell behindert, da so die Produktwerbung organisatorisch schwieriger und kostenintensiver wird. Im Bereich der Einfuhrbeschränkungen sind die Voraussetzungen der Dassonville-Formel daher erfüllt.

In Bezug auf Ausfuhrbeschränkungen könnte die Sachlage hingegen anders zu beurteilen sein. Auch hier ist von der der Dassonville-Formel auszugehen.[542] Allerdings wird die Formel bei Ausfuhrbeschränkungen als zu weit angesehen und deswegen dahingehend eingeschränkt, dass nur solche Maßnahmen erfasst sind, die spezifische Beschränkungen der Ausfuhrströme bezwecken oder bewirken und damit unterschiedliche Bedingungen für den Binnenhandel eines Mitgliedstaats und seinen Außenhandel schaffen, so dass die nationale Produktion oder

---

[536] EuGH, Slg. 1996, S. I-6511 ff., Rn. 25-Reisebüro Broede; EuGH, Slg. 1997, S. I-3899, Rn. 18- Parodi; EuGH, Slg. 1999, S. I-8453 ff., Rn. 33- Arblade

[537] EuGH, Slg. 1996, S. I-6511 ff., Rn. 25-Reisebüro Broede; EuGH, Slg. 1997, S. I-3899, Rn. 18- Parodi; EuGH, Slg. 1999, S. I-8453 ff., Rn. 33- Arblade

[538] EuGH, Slg. 1995, S. I -1142 ff., 1178, Rn. 38 f.- Alpine Investments

[539] EuGH, Slg. 1995, S. I- 1142 ff., 1178, Rn. 38- Alpine Investments

[540] EuGH, Slg. 1977, S. 901- van den Hazel; EuGH, Slg. 1978, S. 2247- Thompson; EuGH, Slg. 1979, S. 3795, Rn. 12-Henn und Darby; EuGH, Slg. 1986, S. 3935, Rn. 3 ff.- Kommission/Griechenland; EuGH, Slg. 1987, S. 3883, Rn. 11-Nertsvoederfabrik; EuGH, Slg. 1992, S. I-3669, Rn. 13 f.- Delhaize/Promalvin; EuGH, Slg. 1996, S. I-2611, Rn. 17-Hedley Lomas; EuGH, Slg. 1998, S. I- 1281, Rn. 39 - World Farming; *Becker* in Schwarze, Art. 28 EGV, Rn. 33; *Epiney* in Ehlers, § 8, Rn. 19; *Dies.* in Calliess/Ruffert, Art. 28 EGV, Rn. 6 und Art. 29 EGV, Rn. 5; *Schroeder* in Streinz, Art. 28 EGV, Rn. 32 und Art. 29 EGV, Rn. 3

[541] EuGH, Slg. 1974, S. 837 ff., Rn. 5- Benoît und Gustave Dassonville

[542] *Müller-Graff* in von Groeben/Schwarze, Art. 29 EGV, Rn. 15; vgl. zur Dassonville-Formel: Fn. 541

der Binnenmarkt des betroffenen Staates einen besonderen Vorteil erlangt.[543] Unterschiedslos anwendbare Vorschriften, denen keine protektionistische Wirkung zukommt, sind danach keine Maßnahmen gleicher Wirkung wie eine mengenmäßige Ausfuhrbeschränkung.[544] Da die fraglichen Regelungen unterschiedslos Waren für den Binnen- und Außenhandel erfassen und auch nicht den inländischen Markt schützen, liegt hier unter Zugrundelegung der Rechtsprechung des EuGH keine Maßnahme gleicher Wirkung wie eine mengenmäßige Ausfuhrbeschränkung vor.[545] Sekundärrecht kann bereits deshalb keine spezifische Beschränkung zugunsten einzelner Märkte darstellen, weil es gemeinschaftsweit wirkt.

(2) Kein Vorliegen einer bestimmten Verkaufsmodalität im Sinne der Keck-Rechtsprechung

In den Bereichen, in denen eine Beschränkung an sich zu bejahen ist, könnte sich unter Zugrundelegung des Keck-Urteils[546] etwas anderes ergeben. Vor diesem Urteil sah der EuGH bestimmter Werbeformen als Maßnahmen gleicher Wirkung wie mengenmäßige Einfuhrbeschränkungen und damit als Beschränkungen der Warenverkehrsfreiheit an.[547] In seinem Keck-Urteil entschied der EuGH jedoch, dass nationale Rechtsvorschriften, die „bestimmte Verkaufsmodalitäten" beschränken oder verbieten, vom Schutzbereich des Art. 28 EGV ausgenommen sind, sofern sie für alle betroffenen Wirtschaftsteilnehmer gelten, die ihre Tätigkeit im Inland ausüben und den Absatz der inländischen Erzeugnisse und der Erzeugnisse aus anderen Mitgliedstaaten rechtlich wie tatsächlich in der gleichen Weise berühren.[548] Aus der Folgerechtsprechung ergibt sich, dass Maßnahmen, die die Vermarktung des Produktes betreffen, bestimmte Verkaufsmodalitäten im Sinne der Keck-Rechtsprechung sind.[549] Einschränkungen in Bezug auf Email-Werbung betreffen die Vermarktung und sind folglich als vertriebsbezogene Maßnahmen anzusehen. Nach der Keck-Rechtsprechung stellen

---

[543] EuGH, Slg. 1979, S. 3409 ff., 3415, Rn. 7 - Groenveld; EuGH, Slg. 1981, S. 1993 ff., 2009, Rn. 13-Oebel; EuGH, Slg. 1982, S. 1299 ff., 1313 –Holdijk; EuGH, Slg. 1983, S. 555 –Inter-Huiles; EuGH, Slg. 1984, S. 483, 503 ff.-Jongeneel Kaas; EuGH, Slg. 1984, S. 523 –Duphar; EuGH, Slg. 1984, S. 2171 ff., 2172-Denkavit; EuGH, Slg. 1984, S. 4277, 4278 –Haug Adrion; EuGH, Slg. 1986, S. 576, 589-Bulk Oil; EuGH, Slg. 1990, S. I-4625, Rn. 17 –Hennen Olie; EuGH, Slg. 1991, S. I-107 ff., 124, Rn. 14 -Alsthom Atlantique; EuGH, Slg. 1991, S. I-1027 ff., 1042, Ziff. 18 –Marchandise; EuGH, Slg. 1992, S. I-3669 ff., 3708, Rn. 12 –Delhaize; EuGH, Slg. 1994, S. I-1019 ff., 1035, Rn. 24 -Kommission/Belgien; EuGH, Slg. 1999, S. I-3845 ff., 3879, Rn. 10 –ED; EuGH, Slg. 2000, S. I-3123 ff., 3162, Rn. 41 -Belgien/Spanien

[544] EuGH, Slg. 1979, S. 3409 ff., 3415, Rn. 7-Groenveld; EuGH, Slg. 1981, S. 1993 ff., 2009, Rn. 13-Oebel; EuGH, Slg. 1982, S. 1299 ff., 1313 –Holdijk; EuGH, Slg. 1983, S. 555 –Inter-Huiles; EuGH, Slg. 1984, S. 483, 503 ff.-Jongeneel Kaas; EuGH, Slg. 1984, S. 523 –Duphar; EuGH, Slg. 1984, S. 2171 ff., 2172-Denkavit; EuGH, Slg. 1984, S. 4277, 4278 –Haug Adrion; EuGH, Slg. 1986, S. 576, 589-Bulk Oil; EuGH, Slg. 1990, S. I-4625, Rn. 17 –Hennen Olie; EuGH, Slg. 1991, S. I-107 ff., 124, Rn. 14 -Alsthom Atlantique; EuGH, Slg. 1991, S. I-1027 ff., 1042, Ziff. 18 –Marchandise; EuGH, Slg. 1992, S. I-3669 ff., 3708, Rn. 12 –Delhaize; EuGH, Slg. 1994, S. I-1019 ff., 1035, Rn. 24 -Kommission/Belgien; EuGH, Slg. 1999, S. I-3845 ff., 3879, Rn. 10 –ED; EuGH, Slg. 2000, S. I-3123 ff., 3162, Rn. 41 -Belgien/Spanien; Leible in Grabitz/Hilf, Art. 29 EGV, Rn. 4

[545] zustimmend: *Classen*, EuR 2004, S. 416 ff.; kritisch: *Becker* in Schwarze, Art. 29 EGV, Rn. 12; *Frenz*, Handbuch Europarecht, Band 1, Rn. 912; *Füller*, a.a.O., S. 244 ff.; *Leible* in Grabitz/Hilf, Art. 29 EGV, Rn. 4; *Pipkorn/Bardenhewer-Rating/Taschner* in v.d. Groeben/Schwarze, Art. 14 EGV, Rn. 30; *Schroeder* in Streinz, Art. 29 EGV, Rn. 5

[546] EuGH, Slg. 1993, S. I- 6097 ff- Keck und Mithouard

[547] EuGH, Slg. 1982, S. 4575 ff., Rn. 15- Oosthoek's Uitgeversmaatschappij BV;
EuGH, Slg. 1989, S. 1235 ff., Rn. 7 ff.- R. Buet und SARL Educational Business Services (EBS)/Ministère public; EuGH, Slg. 1990, S. S -I- 667 ff., Rn. 7, 8- GB-INNO-BM/Confédération du commerce luxembourgeois; EuGH, Slg. 1991, S. I- 1487 ff., Rn. 50- Delattre

[548] EuGH, Slg. 1993, I- S. 6097 ff., Rn. 13- Keck und Mithouard

[549] EuGH, Slg. 1994, I- S. 2199 ff., Rn. 12- Tankstation `t Heuske vof und J.B.E.Boermans; EuGH, EuZW 1994, S. 119 ff., Rn. 21- Ruth Hündermund u.a./Landesapothekenkammer Baden- Württemberg; EuGH, EuZW 1995, S. 250 ff., Rn. 19- Société d'Importation Édouard Leclerc-Siplec/TF 1 Publicité SA u. M6 Publicité SA; EuGH, Slg. 1995, S. I- 1621 ff., Rn. 13- Kommission/Griechische Republik;

sie folglich keine Beschränkung des freien Warenverkehrs dar. Da der EuGH die Keck-Formel auch im Bereich der Dienstleistungsfreiheit anwendet,[550] gilt Gleiches für diese.
Mittlerweile vertritt der EuGH allerdings wieder eine weitere Auslegung des Schutzbereichs der Grundfreiheiten.[551] Danach sind mitgliedstaatliche Anforderungen, die unmittelbar mit dem Produkt verbundene Werbung betreffen, als Maßnahme gleicher Wirkung anzusehen, da so erhebliche Mehrkosten in Bezug auf Darbietung und Werbung entstehen.[552] Darüber hinaus stellt nach der Rechtsprechung des EuGH ein Einwilligungsvorbehalt hinsichtlich der Telefonwerbung für Dienstleistungen in anderen Mitgliedstaaten eine Beschränkung der Dienstleistungsfreiheit dar.[553] Die Keck-Formel wandte der EuGH in der vorgenannten Konstellation nicht an; zur Begründung führt der Gerichtshof aus, Hintergrund der Keck-Rechtsprechung sei, dass vertriebsbezogene Maßnahmen den innergemeinschaftlichen Handel grundsätzlich nicht beeinträchtigen, da sie aus- und inländische Produkte in der selben Weise berühren.[554] Dies sei jedoch nur bei einem Verbot durch den Einfuhrmitgliedstaat der Fall, während der Marktzugang in der umgekehrten Konstellation sehr wohl beeinflusst würde, da die Werbeverbote den Wirtschaftsteilnehmern in diesem Fall ein schnelles und direktes Mittel der Kontaktaufnahme nähmen.[555] Dies bedeutet, dass Werbebeschränkungen, die vom Einfuhrmitgliedstaat ausgesprochen werden, weiterhin unter die Keck-Formel fallen, während diese auf vom Ausfuhrmitgliedstaat ausgesprochene Beschränkungen keine Anwendung findet.

(3) Keine tatbestandsausschließende Beschränkung durch die Cassis-Rechtsprechung

Etwaige Grundfreiheitsbeeinträchtigungen könnten unter Zugrundelegung der tatbestandsausschließenden Beschränkung durch die Cassis-Rechtsprechung dem Schutzbereich der Waren- und Dienstleistungsfreiheit entzogen sein.[556] Nach dieser Rechtsprechung sind auf innerstaatlichen Rechtsvorschriften, die unterschiedslos für einheimische, wie für eingeführte Erzeugnisse gelten,[557] beruhende Handelshemmnisse dann hinzunehmen, wenn sie notwendig sind, um zwingenden Erfordernissen gerecht zu werden, so etwa einer wirksamen steuerlichen Kontrolle, dem Schutz der öffentlichen Gesundheit, der Lauterkeit des Handelsverkehrs und des Verbraucherschutzes.[558] In späteren Urteilen hat der EuGH weitere zwingende Erfordernisse anerkannt, hierbei unter anderem den ordnungsgemäßen Betrieb eines öffentlichen Telekommunikationsnetzes und die Kommunikationsfähigkeit der Endgeräte.[559] Soweit Verbraucher betroffen sind, stellt hier daher der Verbraucherschutz ein zwingendes Erfordernis dar.[560] Daneben kommt -auch im Verhältnis zu Personen, die keine Verbraucher sind- der ordnungsgemäße Betrieb der

[550] EuGH, Slg. 1995, S. I-1176 ff., Rn. 36 - Alpine Inverstments
[551] EuGH, Slg. 1994, S. I- 337, Rn. 19 - Clinique; EuGH, Slg. 1995, S. I-1923, Rn. 13 - Mars; EuGH, Slg. 1995, S. I-1141 ff., Rn. 28 ff. - Alpine Investments
[552] EuGH, Slg. 1994, S. I- 337, Rn. 19- Clinique; EuGH, Slg. 1995, S. I-1923, Rn. 13 - Mars
[553] EuGH, Slg. 1995, I- S. 1141 ff., Rn. 28 ff.- Alpine Investments
[554] EuGH, Slg. 1995, I- S. 1141 ff , Rn. 38- Alpine Investments
[555] EuGH, Slg. 1995, I- S. 1141 ff , Rn. 37- Alpine Investments BV/Minister von Financiën
[556] EuGH, Slg. 1979, S. 649 ff. - Cassis de Dijon; Cassis-Rechtsprechung als immanenten Schranke: EuGH, Slg. 1982, S. 1625 ff., 1638 - Kommission/Irland; EuGH, Slg. 1982, S. 2349, 2360 - Robertson; EuGH, Slg. 1982, S. 3961 - Rau; Cassis-Rechtsprechung als Rechtfertigungsgrund: EuGH, Slg. 1997, S. I-3689, 3715, Rn. 18 - Familiapress
[557] EuGH, Slg. 1984, S. 3651 ff., 3662, Rn. 14 - Kohl/Ringelhan; EuGH, Slg. 1991, S. I - 4151 ff., 4184, Rn. 13 - Aragonesa; EuGH, Slg. 1992, S. I - 4431 ff., 4480, Rn. 34 - Abfälle
[558] EuGH, Slg. 1979, S. 649 ff., Rn. 8, 14 - Cassis de Dijon
[559] EuGH, Slg. 1991, S. I-1223 ff., 1268, Rn. 37- Frankreich/Kommission; EuGH, Slg. 1991, S. I-5941 ff., 5983, Rn. 31 - Régie des télégraphes et des téléphones/GB-Inno-BM SA; EuGH, Slg. 1994, S. I-3257 ff., 3277, Rn. 6 - Strafverfahren gegen François Rouffeteau und Robert Badia
[560] *Köhler* in Baumbach/Köhler/Bornkamm, UWG, § 7 UWG, Rn. 82

Telekommunikationsnetze und die Kommunikationsfähigkeit der Endgeräte als zwingendes Erfordernis in Betracht. Die Kommunikationsfähigkeit der Endgeräte und der ordnungsgemäße Betrieb der Telekommunikationsnetze werden durch die Email-Direktwerbung bedroht, da diese die Netzgeschwindigkeit verlangsamen und bisweilen den Empfang anderer Nachrichten durch Überfluten der Mailbox verhindern.[561] Die Beschränkung der Möglichkeit der Email-Werbung differenziert nicht danach, ob für einheimische oder ausländische Produkte geworben wird. Auch faktisch ergibt sich keine differenzierte Wirkung der Regelung des deutschen Rechts hinsichtlich einheimischer und ausländischer Produkte, denn beide können nicht mittels Email beworben werden, sofern nicht die Einwilligung des Adressaten vorliegt oder der genannte Ausnahmetatbestand[562] eingreift.

Weitere Voraussetzung der tatbestandsausschließenden Beschränkung durch die Cassis-Rechtsprechung ist, dass die mitgliedstaatlichen Maßnahmen geeignet, erforderlich und im engeren Sinn verhältnismäßig zur Sicherung der zwingenden Erfordernisse sind.[563]
Die Geeignetheit ergibt sich daraus, dass die Einschränkung der Möglichkeit der Email-Direktwerbung zumindest rechtstreue Unternehmen davon abhalten wird, weiterhin ohne Zustimmung des Adressaten solche Nachrichten zu versenden.
Die Erforderlichkeit setzt voraus, dass kein anderes gleich wirksames, aber weniger eingriffsintensives Mittel zur Verfügung steht.[564] Hinsichtlich des Vergleichs zu dem scheinbar weniger eingriffsintensiven Opt-Out-Prinzip gelten die Ausführungen zum Verfassungsrecht entsprechend.[565]
Die Verhältnismäßigkeit im engeren Sinne ist gegeben, wenn das eingesetzte Mittel in angemessener Relation zum angestrebten Ziel steht.[566] Das Erfordernis, zuvor die Einwilligung des Adressaten von Werbe-Emails einzuholen, steht nicht außer Verhältnis zum angestrebten Ziel, die Verbraucher zu schützen und den ordnungsgemäßen Betrieb der Telekommunikationsnetze zu gewährleisten. Denn einerseits ist in Betracht zu ziehen, dass bei einem bereits zuvor bestehenden geschäftlichen Kontakt Email-Werbung zugestellt werden darf, Art. 13 Abs. 2 EK-DSRL, § 7 Abs. 3 UWG. Diese Einschränkung gilt, wie bereits dargestellt wurde,[567] auch im Deliktsrecht. Andererseits wird den Versendern durch die wettbewerbs- und deliktsrechtlichen Vorschriften lediglich zugemutet, vor dem Zustellen der Nachricht die Einwilligung der Adressaten einzuholen, was allerdings angesichts der ansonsten erfolgenden Verlagerung der Werbekosten auf die Empfänger,[568] durchaus als zumutbar anzusehen ist.

[561] vgl.: 1. Kap. Teil 1 B. II. 4.
[562] vgl.: 2. Kap. Teil 1 II.
[563] EuGH, Slg. 1979, S. 649 ff., 664 - Cassis de Dijon; EuGH, Slg. 1990, S. I-4827 ff., 4848 - Pall; EuGH, Slg. 1995, S. I-1923 ff., 1942 - Mars; EuGH, Slg. 1997, S. I-3689 ff., 3716 - Familiapress
[564] EuGH, Slg. 1988, S. 4489, Rn. 15- Smanor; EuGH, Slg. 1992, S. I- 3351, Rn. 31- Ramrath; EuGH, Slg. 1998, S. I-8033, Rn. 35- Bluhme; *Jarass*, EuR 2000, S. 722; *Kingreen* in Calliess/Ruffert, Art. 28 ff. EGV, Rn. 93;
[565] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[566] EuGH, Slg. 1987, S. 1227, Rn. 28 - Kommission/Deutschland; EuGH, Slg. 1991, S. I-4151, Rn. 18- Aragonesa de la publicidad exterior; *Kingreen* in Calliess/Ruffert, Art. 28 ff. EGV, Rn. 98; *Schroeder* in Streinz, Art. 30 EGV, Rn. 55
[567] vgl.: 1. Kap. Teil 1 B. II. 4.
[568] vgl.: 1. Kap. Teil 1 B. II. 4.

(4) Zwischenergebnis

Die nach deutschem Recht geltenden Restriktionen der Möglichkeit, Email-Werbung zu versenden, stellen keine rechtswidrige Beschränkung der Warenverkehrs- und Dienstleistungsfreiheit dar. In den Vorschriften ist zwar eine Beschränkung der Dienstleistungsfreiheit und in Bezug auf die Warenverkehrsfreiheit eine Maßnahme gleicher Wirkung wie eine mengenmäßige Einfuhrbeschränkung zu sehen. Eine Maßnahme gleicher Wirkung wie eine mengenmäßige Ausfuhrbeschränkung der Warenverkehrsfreiheit ist hingegen nicht gegeben.
Durch den Einfuhrmitgliedstaat ausgesprochene Beschränkungen fallen nach der Keck-Rechtsprechung aus dem Anwendungsbereich der Grundfreiheiten. Darüber hinaus greifen zwingende Erfordernisse im Sinne der Cassis-Rechtsprechung ein, die tatbestandsausschließende Wirkung entfalten.

bb) Europäische Gemeinschaftsgrundrechte

Die Gemeinschaftsgrundrechte könnten den Vorgaben des deutschen einfachen Rechts und des Sekundärrechts entgegenstehen, welche die Zulässigkeit der Email-Werbung einschränken.

Grundvoraussetzung ist allerdings, dass diese überhaupt einschlägig sind.
Der Anwendungsbereich der Gemeinschaftsgrundrechte ist dabei einerseits gegenüber den Grundfreiheiten abzugrenzen. Soweit sich Grundfreiheiten und Gemeinschaftsgrundrechte im Anwendungsbereich überschneiden, sind nach der Rechtsprechung[569] und der überwiegenden Meinung in der Literatur[570] erstere als geschriebenes Recht speziell. Da die Gemeinschaftsgrundrechte jedoch nicht verdrängt sind, soweit die Grundfreiheiten mangels eines grenzüberschreitenden Sachverhalts keine Anwendung finden,[571] werden sie hier dennoch separat und nicht lediglich im Rahmen der Schrankenbestimmungen der Grundfreiheiten dargestellt.

Fraglich ist andererseits, ob mitgliedstaatliche Rechtsakte anhand der Gemeinschaftsgrundrechte überprüft werden können oder ob hier lediglich nationales Verfassungsrecht Anwendung findet. Adressatin der Gemeinschaftsgrundrechte ist die Europäische Union, das bedeutet deren Organe und Einrichtungen,[572] vgl. Art. 6 Abs. 2 EUV/Art. 51 Abs. 1 GRC.[573] Danach wäre nur das Sekundärrecht, hier Art. 13 EK-DSRL, an den Gemeinschaftsgrundrechten zu messen, nicht jedoch mitgliedstaatliche Regelungen. Eine Bindung der Mitgliedstaaten an die Gemeinschaftsgrundrechte wird über den Wortlaut der Art. 6 Abs. 2 EUV/Art. 51 Abs. 1 GRC hinaus ausnahmsweise dann angenommen, wenn diese im Anwendungsbereich des Gemeinschaftsrechts handeln.[574] Dies ist insbesondere dann

[569] Soweit der EuGH Gemeinschaftshandeln an den Grundfreiheiten überprüft erwähnt er die Grundrechte nur im Rahmen der Rechtfertigung mitgliedstaatlicher Eingriffe, prüft sie jedoch nicht als selbständige Tatbestände, vgl. EuGH, Slg. 1975, S. 1219, Rn. 26, 28 - Rutili; EuGH, Slg. 1991, S. I-2925, Rn. 43 - ERT; EuGH, Slg. 1997, S. I-3689, Rn. 24 - Familiapress
[570] *Rengeling* in Schwarze, Der Verfassungsentwurf des Europäischen Konvents, S. 343; *Ruffert* in Calliess/Ruffert, Art. 15 GRC, Rn. 26 f.; *Wunderlich*, a.a.O., S. 104; a.A. (Idealkonkurrenz): *Kingreen/Störmer*, EuR 1998, S. 263 ff., 286
[571] *Ehlers* in Ders., § 13, Rn. 12; *Frenz*, Handbuch Europarecht, Band 1, Rn. 61; *Jarass*, EU-Grundrechte, § 2, Rn. 10; *Rengeling/Szczekalla*, Rn. 785
[572] *Ehlers* in Ehlers, § 13, Rn. 28; *Rengeling/Szczekalla*, Rn. 269;
[573] Vertrag über die Europäische Union vom 07.02.1992, Abl. EG Nr. C 191, S. 1 ff.; Charta der Grundrechte der Europäischen Union, ABl. EG 2000, C 364/01
[574] EuGH, Slg. 1991, S. I-2964, Rn. 42 - ERT; EuGH, Slg. 1991, S. I-4043, Rn. 23- Gouda; EuGH, Slg. 1991, S. I-4740, Rn. 31- Grogan; EuGH, Slg. 1994, S. I-982 f. - Bostock;

der Fall, wenn die Mitgliedstaaten Gemeinschaftsrecht umsetzen,[575] sofern bei der Umsetzung kein Spielraum mehr verbleibt.[576] Besteht ein Umsetzungsspielraum, so ist der mitgliedstaatliche Gesetzgeber in erster Linie an die nationalen Grundrechte gebunden,[577] hat seinen Ermessensspielraum jedoch dennoch in gemeinschaftsgrundrechtskonformer Weise auszuüben, damit ein unionsweiter einheitlicher Grundrechtsmindeststandard gewährleistet ist.[578] Bei der Umsetzung von Richtlinien, bei denen den Mitgliedstaaten ein Spielraum verbleibt, finden demnach sowohl nationale, als auch Gemeinschaftsgrundrechte Anwendung.[579] Daneben legt der EuGH geschriebene und ungeschriebene Ausnahmen von Grundfreiheiten sowie Schutzbereichsbeschränkungen nach der Keck-Rechtsprechung unter Berücksichtigung der Gemeinschaftsgrundrechte aus.[580] Wie oben dargestellt determiniert Art. 13 Abs. 1 EK-DSRL den deutschen Gesetzgeber, soweit natürliche Personen Adressaten der Email-Werbung sind.[581] Auf diese Konstellation sowie auf das Sekundärrecht finden die Gemeinschaftsgrundrechte somit Anwendung. Im grenzüberschreitenden Verkehr fließen die Gemeinschaftsgrundrechte in die Prüfung der Grundfreiheiten ein, soweit Schutzbereichsbeschränkungen durch die Keck- und Cassis- Rechtsprechung betroffen ist.[582]

Soweit die Gemeinschaftsgrundrechte Anwendung finden, ist Voraussetzung der Gemeinschaftswidrigkeit, dass die zu überprüfenden Rechtsakte einen Grundrechtseingriff (1) darstellen, der nicht gerechtfertigt werden kann (2).

(1) Grundrechtseingriff

Hier könnten Grundrechte der Werbetreibenden (a) oder aber derjenigen Personenkreise beeinträchtigt sein, die am Erhalt der Email-Werbung interessiert sind (b).

(a) Gemeinschaftsrechtlicher Schutz der Werbetreibenden

Die Restriktion der Möglichkeit zur Direktwerbung mittels Email könnte eine unzulässige Beschränkung des europäischen Grundrechts auf Meinungsfreiheit darstellen, das wesentlich durch Art. 10 EMRK und die dazu ergangene Rechtsprechung des EGMR geprägt ist.[583]

---

zustimmend: *Ruffert*, EuGRZ 1995, S. 527; *Weiler/Lockhart*, CML Rev. 1995, S. 622; *Zuleeg*, EuGRZ 2000, S. 511; anders: *Beutler*, EuGRZ 1989, S. 188; *Pernice*, NJW 1990, S. 2417; kritisch: *Coppel/O´Neill*, CML Rev. 1992, S. 691 f.

[575] EuGH, Slg. 1988, 2609, Rn. 19- Wachauf; EuGH, Slg. 1994, I- 955, Rn. 16- Bostock; EuGH, Slg. 1996, I-569, Rn. 29 - Duff.; EuGH, Slg. 1997, I- 1961, Rn. 36 - Earl de Kerlast;
Ehlers in Ders., § 13, Rn. 30; *Ruffert*, EuGZR 1995, S. 527; *Störmer*, AöR 123 (1998), S. 567; *Weiler/Lockhart*, CML Rev. 1995, S. 74

[576] vgl.: 2. Kap. Teil 1 B. I.

[577] vgl.: 2. Kap. Teil 1 B. I.

[578] EuGH, Slg. 1989, S. 2609 ff., 2641, Rn. 22 f.-Wachauf; EuGH, Slg. 1994, S. I-955 ff., 982, Rn. 12 ff.-Bostock; *Ehlers* in Ders., § 13, Rn. 30; *Jarass*, EU-Grundrechte, § 4, Rn. 13; *Kühling* in v. Bogdandy, S. 608 f.; *Störmer*, AöR 123 (1998),S. 567 ff.

[579] *Kühling* in v. Bogdandy, S. 608 f.; a.A.(Anwendbarkeit lediglich der nationalen Grundrechte): *Gerstner/Goebel*, Jura 1993, S. 632; *Kingreen*, JuS 2000, S. 864; *Ders.* in Calliess/Ruffert, 2. Aufl., Art. 6 EUV, Rn. 59; *Pieroth/Schlink*, Staatsrecht II, Rn. 191; *A. Weber*, NJW 2000, S. 542

[580] EuGH, Slg. 1991, S. I-2964, Rn. 43 - ERT; EuGH, Slg. 1991, S. I-4043, Rn. 23 - Gouda; EuGH, Slg. 1991, S. I-3689, Rn. 24 - Familiapress; zustimmend: *Rengeling/Szczekalla*, Rn. 320; *A. Weber*, NJW 2000, S. 542; *Weiler/Lockhart*, CML Rev. 1995, S. 74; kritisch: *Coppel/O´Neill*, CML Rev. 1992, S. 678; *Kingreen*, JuS 2000, S. 864 f.

[581] vgl.: 2. Kap. Teil 1 B. I.

[582] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb)

[583] EuGH, Slg. 1992, S. I-5485, Rn. 38 - Strafverfahren gegen Ter Voort; EuGH, Slg. 1997, S. I-3689, Rn. 26 - Familiapress; EuGH, Slg. 2001, S. I-1611, Rn. 25 - Connolly/Kommission; EuGH, EuZW 2004, S. 439, Rn. 44, 48-52 - Karner; *Beutler* in von Groeben/Schwarze, Art. 6 EUV, Rn. 84; *Blanke/Kingreen* in Calliess/Ruffert, Art.

Ebenso wie das Konventionsrecht[584] umfasst das Gemeinschaftsgrundrecht auf freie Meinungsäußerung auch die kommerzielle Kommunikation.[585]
Das in der EMRK verankerte Recht schützt jede Form der Kommunikation im zwischenmenschlichen Bereich.[586] Es erfasst auch Werbung,[587] Informationen kommerzieller und geschäftlicher Natur[588] sowie Inhalte, die einen Teil der Bevölkerung verletzen, schockieren oder beunruhigen.[589] Art. 10 Abs. 1 EMRK möchte dabei in erster Linie davor schützen, dass die Meinungsäußerung bzw. der Informationsfluss verhindert wird,[590] beinhaltet also das Recht des Grundrechtsträgers, Tatsachenäußerungen und Meinungen mitzuteilen,[591] Informationen zu erhalten bzw. sich darum zu bemühen und sie weiterzugeben.[592] Demnach fällt die werbliche Ansprache mittels elektronischer Post in den Schutzbereich der Meinungsfreiheit und zwar selbst dann, wenn diese inhaltlich nicht für alle Empfänger akzeptabel ist. Da der EGMR auch in denjenigen Fällen einen Eingriff in das Recht auf freie Meinungsäußerung bejahte, in denen der Betroffene lediglich im Hinblick auf ein bestimmtes Äußerungsmedium beschränkt werden sollte,[593] kann ein Eingriff auch nicht mit dem Hinweis abgelehnt werden, dass dem Versender bzw. dessen Auftraggeber lediglich ein einziges Werbemedium genommen werde. Träger des Grundrechts sind natürliche sowie juristische Personen und Personenvereinigungen.[594] Aufgrund der Tatsache, dass das europäische Grundrecht wesentlich durch Art. 10 EMRK und die dazu ergangene Rechtsprechung des EGMR geprägt ist,[595] können die soeben dargestellten Grundsätze auf das Gemeinschaftsgrundrecht übertragen werden.

Daneben könnte die Einschränkung der Möglichkeit, Werbe-Emails zu versenden, einen Eingriff in das Grundrecht auf Korrespondenz darstellen. Auch im Bereich der

---

52 GRC, Rn. 24; *Faßbender*, GRUR Int. 2006, S. 974; *Schorkopf* in Ehlers, § 15, Rn. 59; vgl. auch: Art. 52 Abs. 3 GRC

[584] EGMR, NJW 1985, 2886 - Barthold; EGMR, Nr. 3/1988/147/201, Serie A/165, Rn. 26- markt intern; EGMR, Nr. 8/1993/403/481, Serie A/285-A, Rn. 35- Casado Coca; EGMR, NJW 2003, S. 497- Stambuk

[585] EuGH, EuZW 2004, S. 439 Rn. 48 ff.- Karner; *Calliess* in Ders./Ruffert, Art. 11 GRC, Rn. 6; *Grabenwarter*, § 23, Rn. 4; *Schorkopf* in Ehlers, § 15, Rn. 72

[586] *Frowein* in Ders./Peukert, Art. 10, Rn. 5; *Grabenwarter*, EMRK Studienbuch, § 23, Rn. 3 f.

[587] EGMR, NJW 1985, S. 2886- Barthold; EGMR, Nr. 8/1993/403/481, Serie A/285-A, Rn. 35- Casado Coca; EGMR, NJW 2003, S. 497- Stambuk; EKMR, EuGRZ 1991, S. 525- Hempfing/Bundesrepublik Deutschland; Calliess in Ders./Ruffert, Art. 11 GRC, Rn. 6; *Ovey/White*, ECHR, S. 286;

[588] EKMR, EuGRZ 1991, S. 525 - Hempfing/Bundesrepublik Deutschland; EGMR Urt. v. 24.02.1994- Casado Coca/Spanien

[589] EGMR, Nr. 3/1988/147/201, Serie A/165, Rn. 26 - markt intern; EGMR, Nr. 13/1994/460/541, Serie A/313, Rn. 38 - Prager und Oberschlick/Österreich; EGMR, EuGRZ 1996, S. 293- Handyside/Vereinigtes Königreich

[590] EGMR, EuGRZ 1979, S. 386- Sunday Times; EGMR, Nr. 10/1985/6/144, Rn. 74- Leander/Schweden; EGMR, Nr. 2/1988/146/200, Rn. 52 f.- Gaskin/Vereinigtes Königreich; *Bernsdorff* in Meyer, Art. 11 GRC, Rn. 12; *Meyer-Ladewig*, Art. 10 EMRK, Rn. 14; *Ovey/White*, ECHR, S. 276

[591] EGMR, EuGRZ 1979, S. 386 - Sunday Times; *Bernsdorff* in Meyer, Art. 11 GRC, Rn. 12; *Meyer-Ladewig*, Art. 10 EMRK, Rn. 14; *Ovey/White*, ECHR, S. 276

[592] EGMR, EuGRZ 1979, S. 386 - Sunday Times; EGMR, Nr. 10/1985/6/144, Rn. 74 - Leander/Schweden; EGMR, Nr. 2/1988/146/200, Rn. 52 f. - Gaskin/Vereinigtes Königreich; EGMR, NJW 1991, S. 620 ff.- Autronic/Schweiz; EGMR, NJW 1993, 773, Rn. 55 - Open Door and Dublin Well Woman/Irland; EGMR, EuGRZ 1995, S. 16, 20 - Observer and Guardian/Vereinigtes Königreich

[593] EGMR, EuGRZ 1996, S. 304- markt intern; EGMR, EuGRZ 1996, S. 307 - Jacubowski/Bundesrepublik Deutschland

[594] EGMR, EuGRZ 1979, S, 386 - Sunday Times; EGMR, NJW 1991, 621, Rn. 47- Autronic/Schweiz; EGMR, NJW 1991, S. 615- Groppera Radio AG/Schweiz; EGMR, EuGRZ 1996, S. 304- markt intern; *Calliess* in Ders./Ruffert, Art. 11 GRC, Rn. 9; *Jarass*, EU-Grundrechte, § 16, Rn. 13

[595] EuGH, Slg. 1992, S. I-5485, Rn. 38 - Strafverfahren gegen Ter Voort; EuGH, Slg. 1997, S. I-3689, Rn. 26 - Familiapress; EuGH, Slg. 2001, S. I-1611, Rn. 25 - Connolly/Kommission; EuGH, EuZW 2004, S. 439, Rn. 44, 48-52 - Karner; *Beutler* in von Groeben/Schwarze, Art. 6 EUV, Rn. 84; *Blanke/Kingreen* in Calliess/Ruffert, Art. 52 GRC, Rn. 24; *Faßbender*, GRUR Int. 2006, S. 974; *Schorkopf* in Ehlers, § 15, Rn. 59; vgl. auch: Art. 52 Abs. 3 GRC

Korrespondenz kann auf die entsprechende Gewährleistung in Art. 8 EMRK abgestellt werden.[596] Das Konventionsrecht richtet sich gegen das Anhalten und Verzögern von Briefen[597], das Öffnen[598], das Lesen und Kopieren,[599] das Löschen bestimmter Stellen,[600] Genehmigungsvorbehalte bzw. Verbote[601] sowie Beschränkungen der Zahl oder Länge von Briefen.[602] Aus den verschiedenen Urteilen zum Recht auf Korrespondenz lässt sich folgern, dass stets diejenigen Vorgänge in den Schutzbereich des Konventionsrechts eingreifen, die entweder eine inhaltliche Kontrolle des Briefverkehrs beinhalten, das Recht auf Versendung von Briefpost beschränken oder bewirken, dass der Betroffene nicht vollständig, verspätetet oder überhaupt nicht vom Inhalt der Nachricht Kenntnis nehmen kann. Hier wird das Recht eingeschränkt, elektronische Post mit werbendem Inhalt zu versenden. Insofern ist auch eine Beeinträchtigung des Schutzbereichs des Rechts auf Korrespondenz zu bejahen, zumal der EGMR in seinem Urteil in Sachen Golder ausgeführt hat, es stelle den radikalsten Eingriff in die Ausübung des Rechts auf Achtung des Briefverkehrs dar, wenn jemandem die Möglichkeit des Briefverkehrs genommen werde.[603] Insofern ist davon auszugehen, dass das Recht der kommerziellen Werbung auch durch Art. 8 Abs. 1 EMRK geschützt wird. Aufgrund der Bezugnahme des EuGH auf Art. 8 EMRK gelten die dargestellten Grundsätze auch für das Gemeinschaftsgrundrecht.

Fraglich ist, ob die Einschränkung der Zulässigkeit kommerzieller Email-Werbung als Eingriff in das Gemeinschaftsgrundrecht der Berufsfreiheit zu qualifizieren ist. Der sachliche Schutzbereich der Berufsfreiheit wurde zwar vom EuGH noch nicht abstrakt definiert,[604] doch lässt sich dieser aus einer Gesamtschau der bisherigen Rechtsprechung sowie der GRC gewinnen.[605] Danach umfasst die Berufsfreiheit die umfassende Gewährleistung der wirtschaftlichen Betätigungsfreiheit.[606] Das Grundrecht sichert die Berufswahl und die Berufsausübung umfassend.[607] Da das Grundrecht der Berufsfreiheit die gesamte wirtschaftliche Betätigung schützt, ist davon auszugehen, dass die Möglichkeit des Grundrechtsträgers, für die berufliche Tätigkeit zu werben, in den Schutzbereich des Grundrechts fällt. Da Email ein sehr effizientes und kostengünstiges Werbemittel ist, kann es hier ebenso wie im Bereich der nationalen Grundrechte nicht darauf ankommen, dass dem Betroffenen noch andere Werbemittel zur Verfügung stehen.[608] Grundrechtsträger sind natürliche und juristische Personen.[609]

---

[596] EuGH, Slg. 1980, S. 2033 ff., Rn. 19 - National Panasonic; EuGH, Slg. 1994, S. I- 4737 ff., Rn. 17 - X/Kommission; EuG, Slg. 1994, S. II- 179 ff., Rn. 47- A/Kommission; *Bernsdorff* in Meyer, Art. 7 GRC, Rn. 1; *Jarass*, EU-Grundrechte, § 12, Rn. 2; *Kingreen* in Calliess/Ruffert, Art. 7 GRC, Rn. 2; *Rengeling/Szczekalla*, Rn. 664; vgl. auch: Erläuterung des Präsidiums des Europäischen Konvents, ABl. 2004, Nr. C 310/456

[597] EGMR, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, Rn. 83 ff. - Silver u.a./Vereinigtes Königreich; EGMR, Nr. 4/1987/127/178, Rn. 23 ff. - Schöneberger und Durmaz/Schweiz

[598] EGMR, Nr. 28524/9, Rn. 79 ff. - Peers/Griechenland

[599] EGMR, Nr. 52/1990/243/314, Rn. 30 ff. - Campbell/Vereinigtes Königreich; EGMR, Nr. 33274/96, Rn. 27 ff. -Foxley/Vereinigtes Königreich

[600] EGMR, Nr. 54/1990/245/316, Rn. 40 ff. - Pfeifer und Plankl/Österreich

[601] EGMR, EuGRZ 1975, S. 98 - Golder/Vereinigtes Königreich

[602] *Wildhaber* in Karl, Art. 8 EMRK, Rn. 499

[603] EGMR, EuGRZ 1975, S. 98 - Golder/Vereinigtes Königreich

[604] *Ruffert* in Ehlers, § 15, Rn. 9; *Wunderlich*, a.a.O., S. 105

[605] *Ruffert* in Ehlers, § 15, Rn. 9

[606] *Ruffert* in Ehlers, § 15, Rn. 10; vgl. auch: EuGH, Slg. 1985, S. 2857 ff., Rn. 23 - Finsider; Art. 15 Abs. 1, 16 GRC

[607] EuGH, Slg. 1979, S. 3727, Rn. 32 - Liselotte Hauer/Land Rheinland Pfalz; EuGH, Slg. 1994, S. I-5555, Rn. 25 - SMW Winzersekt; *Feger*, RdA 1987, S. 16; *Notthoff*, RIW 1995, S. 543

[608] vgl.: 2. Kap. Teil 1 B. I. 1. a) bb)

[609] EuGH, Slg. 1974, S. 491 ff., 501, Rn. 12 ff. - Nold; EuGH, Slg. 1989, S. 2237 ff., Rn. 18 - Schräder; EuG, Slg. 1998, S. II-125, II-149 f., Rn. 72 ff. - Edouard Dubios et Fils/Rat und Kommission; *Jarass*, EU-Grundrechte, § 20, Rn. 9 ff., 10; *Ruffert* in Ehers, § 15, Rn. 24 ff.; *Wunderlich*, a.a.O., S. 120 f.

Eingriffe sind alle Maßnahmen, die sich unmittelbar auf die berufliche Betätigung beziehen.[610] Zwar hat der EuGH hierzu noch nicht Stellung genommen, es ist jedoch davon auszugehen, dass auch mittelbare belastende Maßnahmen als Eingriff anzusehen sind.[611] Insofern stellt die durch das einfache Recht statuierte Beschränkung der Zulässigkeit der Email-Werbung wie im Bereich der nationalen Grundrechte[612] einen Eingriff dar, da die Möglichkeit zur beruflichen Außendarstellung des Grundrechtsträgers in Gestalt der Gelegenheit, für seine beruflichen Leistungen zu werben, beeinträchtigt wird.

Im Ergebnis ist der Gehalt mehrerer Freiheitsrechte betroffen. Es ist mit dem EuGH davon auszugehen, dass diese in Idealkonkurrenz stehen.[613]

(b) Gemeinschaftsgrundrechtlicher Schutz an Email-Werbung interessierter Personenkreise

Die genannten Beschränkungen der Zulässigkeit der Email-Werbung könnten auch einen Eingriff in das Recht derjenigen Personenkreise darstellen, die am Erhalt von Email-Werbung interessiert sind.

Die Informationsfreiheit ist auch auf Ebene des europäischen Gemeinschaftsrechts gewährleistet. Ihre Auslegung lehnt sich an Art. 10 EMRK nebst der dazu ergangenen Rechtsprechung[614] an.[615] Sie umfasst das Recht, Informationen zu erhalten bzw. sich um Informationen zu bemühen.[616]

Das Grundrecht ist aus den im Bereich der nationalen Grundrechte genannten Argumenten beeinträchtigt.[617] Hinsichtlich der Grundrechtsträgerschaft kann auf die Ausführungen zur Meinungsäußerungsfreiheit verwiesen werden.[618]

---

[610] EuGH, Slg. 1990, S. I-4071, Rn. 27 f. - Marshall; EuGH, Slg. 1992, S. I-35, Rn. 16 - Kühn; EuGH, Slg. 1994, S. I-5555, Rn. 24 - SMW Winzersekt; EuGH, Slg. 1994, S. I-4973, Rn. 81 - Deutschland/Rat; EuGH, Slg. 1995, S. I-3115, Rn. 55 f. - Fishermen´s Organisations u.a.

[611] *Kingreen* in Calliess/Ruffert, 15 GRC, Rn. 10 f.; *Wunderlich*, a.a.O., S. 113 ff.

[612] vgl.: 2. Kap. Teil 1 B. I. 1. a) bb)

[613] EuGH, Slg. 1994, S. I-4973 ff., Rn. 67, 77, 81 - Deutschland/Rat; *Jarass*, EU-Grundrechte, Rn. 31; *Kingreen* in Calliess/Ruffert, 2. Aufl., Art. 6 EUV, Rn. 83; *Kugelmann*, EuGRZ 2003, S. 24

[614] EGMR, Nr. 15/1989/175/231, Serie A/178, Rn. 47 - Autronic AG/Schweiz; EGMR, Nr. 64/1991/316/387-388, Serie A/246-A, Rn. 55 - Open Door and Dublin Well Woman/Irland

[615] EuGH, Slg. 1989, S. 4285, Rn. 15 f.-Oyowe und Traore/Kommission; EuGH, Slg. 1997, S. 3698, Rn. 26-Familiapress; *Beutler* in von Groeben/Schwarze, Art. 6 EUV, Rn. 84; *Calliess* in Ders./Ruffert, Art. 11 GRC, Rn. 8; *Schorkopf* in Ehlers, § 15, Rn. 59

[616] EGMR, EuGRZ 1979, S. 386 ff., 386 - Sunday Times; EGMR, Nr. 10/1985/6/144, Rn. 74-Leander/Schweden; EGMR, Nr. 2/1988/146/200, Rn. 52 f. - Gaskin/Vereinigtes Königreich; EGMR, NJW 1991, S. 620 ff.- Autronic AG/Schweiz; EGMR, NJW 1993, S. 773, Rn. 55 - Open Door and Dublin Well Woman/Irland; EuGRZ 1995, S. 16, 20 - Observer and Guardian/Vereinigtes Königreich; *Beutler* in von Groeben/Schwarze, Art. 6 EUV, Rn. 84; *Bernsdorff* in Meyer, Art. 11 GRC, Rn. 12; *Calliess* in Ders./Ruffert, Art. 11 GRC, Rn. 8; *Meyer-Ladewig*, Art. 10 EMRK, Rn. 14; *Ovey/White*, ECHR, S. 276

[617] vgl.: 2. Kap. Teil 1 B. I. 1. b)

[618] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (1) (a)

(2) Rechtfertigung

Fraglich ist, ob die Eingriffe gerechtfertigt werden können.

(a) Schranken

Einschränkungen des Grundrechts auf Korrespondenz bzw. Meinungsäußerungs- und Informationsfreiheit lassen sich unter den in Art. 8 Abs. 2 bzw. 10 Abs. 2 EMRK genannten Voraussetzungen rechtfertigen.[619] Ein Eingriff ist danach nur möglich, wenn dieser gesetzlich vorgesehen und von tatsächlich dem Gemeinwohl dienenden Zielen der Gemeinschaft gedeckt ist.[620] Auch im Bereich der Berufsfreiheit ist eine gesetzliche Grundlage erforderlich.[621]

Zulässige Einschränkungsgründe im Hinblick auf die Meinungsfreiheit sind die von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen und der Schutz der Rechte und Freiheiten anderer, vgl. Art. 10 Abs. 2 EMRK, Art. 52 Abs. 3 GRC. Art. 8 Abs. 2 EMRK lässt Eingriffe in die Rechte des Abs. 1 zu, soweit diese gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale und öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Auch dem Grundrecht der Berufsfreiheit setzen dem Gemeinwohl dienende Ziele Schranken.[622] Hier sind die Rechte anderer betroffen, nämlich die der Empfänger, die Email-Werbung nicht erhalten möchten.

Die Voraussetzungen für eine Einschränkung liegen demnach vor.

(b) Schranken-Schranken

Zu den Schranken-Schranken zählen insbesondere der Verhältnismäßigkeitsgrundsatz (aa) und die Wesensgehaltsgarantie (bb).

(aa) Verhältnismäßigkeit/Übermaßverbot

Die Grundrechtseinschränkungen lassen sich nur dann rechtfertigen, wenn sie verhältnismäßig sind.[623] Dies ist der Fall, wenn die fraglichen Maßnahmen geeignet sowie erforderlich sind, das gewünschte Ziel zu erreichen und das Kriterium der Verhältnismäßigkeit im engeren Sinne gegeben ist.[624]

---

[619] EuGH, Slg. 1997, S. I-3689, Rn. 26 - Familiapress; EuGH, Slg. 2002, S. I-6279, Rn. 42 - Carpenter; EuGH, Slg. 2003, S. I-5659, Rn. 79 - Schmidberger; vgl. auch: Art. 52 Abs. 3 GRC

[620] EuGH, Slg. 1974, S. 491, Rn. 14 - Nold; EuGH, Slg. 1989, S. 2609, Rn. 18 - Wachauf

[621] EuGH, Slg. 1989, S. 2859, Rn. 19 - Hoechst/Kommission; EuGH, Slg. 1989, S. 3165 ff., Rn. 16 - Dow Chemical Ibérica u.a./Kommission; *Jarass*, EU-Grundrechte, § 20, Rn. 13; *Wunderlich*, a.a.O., S. 185 f.; vgl. auch: Art. 52 GRC

[622] EuGH, Slg. 1979, S. 3727 ff., Rn. 32 - Liselotte Hauer; EuGH, Slg. 1986, S. 2897, Rn. 14 - Keller unter Verweis auf EuGH, Slg. 1974, S. 491 ff., Rn. 14 - Nold

[623] EuGH, Slg. 1994, S. I-4973, Rn. 78 - Deutschland/Rat; EuGH, Slg. 1994, S. I-5555, Rn. 22 - SMW Winzersekt; *Jarass*, EU-Grundrechte, § 6, Rn. 45 ff.; *Kingreen* in Calliess/Ruffert, 2. Aufl., Art. 6 EUV, Rn. 73 ff.

[624] EuGH, Slg. 1989, S. 2237, Rn. 21 - Schräder

Zur Geeignetheit und Erforderlichkeit wurde bereits Stellung genommen.[625] Die Kriterien sind erfüllt.
Die gesetzgeberischen Maßnahmen dürften darüber hinaus keinen im Hinblick auf den verfolgten Zweck unverhältnismäßigen nicht tragbaren Eingriff darstellen.[626] Im Rahmen der Verhältnismäßigkeit im engeren Sinne sind die gegenläufigen Interessen abzuwägen und es ist anhand sämtlicher Umstände des jeweiligen Einzelfalls festzustellen, ob das rechtliche Gleichgewicht zwischen diesen Interessen gewahrt ist.[627] Daher sind die kollidierenden Rechtsgüter zu gewichten und in einen Ausgleich zu bringen. Es ist wie im Bereich der nationalen Grundrechte eine Abwägung zwischen den beeinträchtigten Rechten und denjenigen Interessen durchzuführen, die durch die nationalen Vorschriften und diejenigen des Sekundärrechts verfolgt werden.[628] Dabei ist zu berücksichtigen, dass sich im Bereich der EMRK in den Fällen, in denen die Ausübung der Meinungsfreiheit nichts zu einer Debatte von allgemeinem Interesse beiträgt und sie darüber hinaus in einem Kontext erfolgt, in dem die Staaten einen gewissen Entscheidungsspielraum haben, die Kontrolle auf die Prüfung beschränkt, ob der Eingriff in einem angemessenen Verhältnis zu den verfolgten Zielen steht.[629] Gleiches muss aufgrund der genannten Bezugnahmen des EuGH auf die Konventionsrechte und die dazu ergangene Rechtsprechung auch für das Gemeinschaftsgrundrecht gelten.
Hier gewinnen die Rechte derjenigen Personenkreise Bedeutung, die Email-Direktwerbung nicht erhalten möchten. Die Berechtigung, solche Nachrichten abzulehnen, könnte einerseits aus dem Recht auf Privatleben herzuleiten sein, das sich an Art. 8 EMRK anlehnt,[630] oder aus einer etwaigen negativen Komponente der Meinungs- und Informationsfreiheit, die sich an Art. 10 EMRK orientiert.[631] Bisher hat der EGMR den Begriff des Privatlebens im Sinne des Art. 8 Abs. 1 EMRK nicht definiert, aus der umfangreichen Kasuistik in diesem Bereich lassen sich jedoch Schlussfolgerungen hinsichtlich der Reichweite und Ausgestaltung des Schutzbereichs des Privatlebens ziehen.[632] Es ist eine Tendenz des EGMR erkennbar, das Recht auf Privatleben sehr weit auszulegen, um die freie Entfaltung der Persönlichkeit des Grundrechtsträgers zu gewährleisten.[633] So sind das Recht auf ein selbstbestimmtes Leben,[634]

---

[625] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[626] EuGH, Slg. 1992, S. I-35, Rn. 16 - Kühn/Landwirtschaftskammer Weser-Ems; EuGH, Slg. 1995, S. I-3115, Rn. 55 - The Queen/Minister of Agriculture, Fisheries and Food; EuGH, Slg. 1997, S. I-4315, Rn. 42 - Affish BV/Rijskdienst voor de keuring van Vee en Vlees; EuGH, Slg. 1998, S. I-7976, Rn. 79 - The Queen/The Licensing Authority; EuGH, Slg. 2003, S. I-5659, Rn. 80 - Schmidberger/Österreich
[627] EuGH, Slg. 2004, S. I-6911, Rn. 85 ff. - Di Lenardo; EuGH, Slg. 2005, S. I-3785, Rn. 130 ff. - Regione autonoma Friuli-Venezia Giulia und ERSA; EuGH, Slg. 2003, S. I-5659, Rn. 81 - Schmidberger/Österreich; *Blanke/Kingreen* in Calliess/Ruffert, Art. 52 GRC, Rn. 70 ff.; *Jarass*, EU-Grundrechte, § 6, Rn. 50
[628] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[629] EGMR, Serie A, Nr. 165, Rn. 33 - markt intern Verlag GmbH und Klaus Beermann; EGMR, Reports of judgements and decisions 2001 VI, Rn. 69 f.-VGT Verein gegen Tierfabriken/Schweiz; EuGH, Slg. 2004, S. I-03025, Rn. 51- Karner
[630] EuGH, Slg. 1980, S. 2056 f., Rn. 17 ff. - National Panasonic/Kommission; EuGH, Slg. 1994, S., I- 4789, Rn. 17 - X/Kommission; *Bengt/Beutler* in von der Groeben/Schwarze, Art. 6 EUV, Rn. 132; *Bernsdorff* in Meyer, Art. 7 GRC, Rn. 19; *Kingreen* in Calliess/Ruffert, Art. 7 GRC, Rn. 2; *Pernice/Mayer* in Grabitz/Hilf, Art. 6 EUV, Rn. 82
[631] EuGH, Slg. 1997, I-3689, Rn. 26 - Familiapress; EuGH, Slg. 2001, I-1611, Rn. 40 f. - Connolly/Kommission; *Calliess* in Ders./Ruffert, Art. 11 GRC, Rn. 5; *Schorkopf* in Ehlers, § 15, Rn. 59
[632] EGMR, NJW 1993, S. 718 ff. - Niemitz/Deutschland; EGMR, EuGRZ 2002, S. 234 - Pretty; *Ovey/White*, ECHR, S. 220 f.; *Uerpmann* in Ehlers, § 3, Rn. 3 ff.
[633] EGMR, Urt. v. 06.09.1978- Klass u.a. gegen Bundesrepublik Deutschland; EGMR, Nr. 10/1985/96/144 Leander gegen Schweden; EGMR NJW 1993, S. 718 ff. - Niemitz/Deutschland; EGMR, Nr. 13/1997/797/1000-Kopp gegen Schweiz; EGMR, 27798/95 - Amann gegen Schweiz; EGMR, 28341/95 - Rotaru gegen Rumänien; EGMR, 44787/98 - P.G. und J.H. gegen Vereinigtes Königreich; EGMR, EuGRZ 2002, S. 234 - Pretty; EGMR, 44647/98 - Peck gegen Vereinigtes Königreich; *Frowein* in Ders./Peukert, EMRK Kommentar, Art. 8, Rn. 3; *Grabenwarter*, § 22, Rn. 6; *Meyer-Ladewig*, Art. 8, Rn. 3; *Uerpmann* in Ehlers, § 3, Rn. 3 ff.
[634] EGMR, EuGRZ 2002, S. 234 - Pretty

berufliche Tätigkeiten und das Hinaustreten in die Öffentlichkeit[635], auf den Schutz persönlicher Daten,[636] vor dem Abhören und Aufzeichnen privater und geschäftlicher Telefon-[637] und sonstiger Gespräche[638] vom Schutzbereich des Rechts auf Privatleben erfasst. Des Weiteren stellt nach der Rechtsprechung des EGMR jegliche Registrierung und Weitergabe von Informationen einen Eingriff in das Recht auf Privatleben dar und zwar auch dann, wenn es sich um Informationen handelt, die der Betroffene selbst zu einem anderen Zeitpunkt veröffentlicht hat.[639] Da der EuGH auf das Konventionsrecht und die dazu ergangene Rechtsprechung des EGMR Bezug nimmt, ist davon auszugehen, dass das Gemeinschaftsgrundrecht einen deckungsgleichen Inhalt hat.
Aufgrund der hieraus resultierenden weiten Auslegung des Gemeinschaftsgrundrechts auf Privatleben und der Tatsache, dass unerwünschte Kommunikation den Empfänger dazu zwingt, sich mit Inhalten und der Durchsicht der Nachrichten auseinanderzusetzen, ist davon auszugehen, dass auch die Freiheit des Bürgers in den Schutzbereich fällt, Informationen, die er nicht erhalten möchte, nicht zu empfangen.[640]
Andererseits könnte die Freiheit, von Kommunikation frei zu bleiben, also die negative Informationsfreiheit, ähnlich wie dies im Bereich der deutschen Grundrechte vertreten wird,[641] vom Grundrecht auf freie Meinungsäußerung erfasst sein, das sich, wie bereits ausgeführt wurde,[642] in seiner Auslegung an Art. 10 EMRK nebst der dazu ergangenen Rechtsprechung anlehnt.
Der Wortlaut des Art. 10 Abs. 1 EMRK stellt auf die freie Meinungsäußerung und auf die freie Weitergabe und Entgegennahme von Informationen ab. Insofern scheint nach dem Wortlaut gerade die Verbreitung von Meinungen und Informationen durch das Grundrecht geschützt zu sein, nicht jedoch das Recht, vor fremden Meinungen frei zu bleiben. Art. 8 Abs. 1 EMRK wird hingegen durch den EGMR sehr weit ausgelegt, um die freie Entfaltung der Persönlichkeit bzw. des Grundrechtsträgers zu gewährleisten.[643] Fühlt sich eine Person durch das Zusenden unerwünschten Werbematerials gestört, so ist der persönlichkeitsrelevante Bereich betroffen, da die Person sich mit Informationen auseinandersetzen muss, die sie nicht erhalten möchte und sie insofern in ihrem Recht auf ein selbstbestimmtes Leben beeinträchtigt ist. Deshalb ist nach der hier vertretenen Auffassung das Recht auf Abwehr unerwünschter Email-Werbung dem Bereich des Privatlebens im Sinne des Art. 8 Abs. 1 EMRK zuzuordnen.[644] Aufgrund der Bezugnahmen des EuGH auf die Konventionsrechte und die dazu ergangene Rechtsprechung des EGMR hat Gleiches im Bereich der Gemeinschaftsgrundrechte zu gelten.

---

[635] EGMR, NJW 1993, S. 718 ff. - Niemitz/Deutschland; EGMR, 44647/98 - Peck gegen Vereinigtes Königreich
[636] EGMR, Nr. 10/1985/96/144 Leander gegen Schweden; EGMR, 27798/95 - Amann gegen Schweiz; EGMR, 28341/95 - Rotaru gegen Rumänien
[637] EGMR, Urt. v. 06.09.1978- Klass u.a. gegen Bundesrepublik Deutschland; EGMR, Nr. 13/1997/797/1000- Kopp gegen Schweiz; EGMR, 27798/95 - Amann gegen Schweiz
[638] EGMR, 44787/98 - P.G. und J.H. gegen Vereinigtes Königreich
[639] EGMR, Nr. 10/1985/96/144 Leander gegen Schweden; EGMR, 28341/95 - Rotaru gegen Rumänien
[640] *Fikentscher/Möllers*, NJW 1998, S. 1344; *Kugelmann*, EuGRZ 2003, S. 24; vgl. auch: *Rüpke*, a.a.O., S. 84 und *Wildhaber/Breitenmoser* in Karl, Art. 8 EMRK, Rn. 109, die zwischen mehreren Kategorien unterscheiden: (1) dem Verbot des Aufzwingens von Kommunikation durch Eindringen in die private Geheimsphäre; (2) der Freiheit der Auswahl eigener Kommunikationspartner; (3) der Freiheit vor erzwungener Kommunikationsteilhabe; (4) Verbot der Isolierung von Information aus dem Kommunikationskontext.
[641] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[642] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (1) (a)
[643] EGMR NJW 1993, S. 718 ff. - Niemitz/Deutschland; *Frowein* in Frowein/Peukert, Art. 8 EMRK, Rn. 3; *Grabenwarter*, § 22, Rn. 6; *Meyer-Ladewig*, Art. 8 EMRK, Rn. 3; *Uerpmann* in Ehlers, § 3, Rn. 3 ff.
[644] im Ergebnis: *Fikentscher/Möllers*, NJW 1998, S. 1344; *Kugelmann*, EuGRZ 2003, S. 24; *Rüpke*, a.a.O., S. 84; *Wildhaber/Breitenmoser* in Karl, Art. 8 EMRK, Rn. 109

Im Rahmen der bestehenden Schutzpflichtdimension haben die Grundrechtsadressaten dem Gemeinschaftsgrundrecht auf Privatleben dadurch Rechnung zu tragen, dass sie den betroffenen Bürger vor Eingriffen durch Private schützen.[645]

Denkbar ist, dass darüber hinaus das Eigentumsgrundrecht den Gesetzgeber im Rahmen seiner Schutzpflichtdimension[646] zu einer Beschränkung verpflichtet. Voraussetzung wäre, dass das hier möglicherweise betroffene Recht auf den eingerichteten und ausgeübten Gewerbebetrieb von diesem Recht umfasst und hier betroffen ist. Ob das Recht auf den eingerichteten und ausgeübten Gewerbebetrieb als Bestandteil des Eigentumsgrundrecht auf Gemeinschaftsebene gewährleistet ist, ist zweifelhaft.[647] Der EGMR bejaht dies,[648] was jedoch auch daran liegen kann, dass die EMRK kein Grundrecht auf Berufsfreiheit kennt.[649] Jedenfalls ist der Schutzbereich nur eröffnet, wenn der Bestand des Betriebs betroffen ist.[650] Dies ist jedoch wie bereits dargestellt nicht der Fall.[651]
Aus den oben genannten Gründen liegt kein hinreichender Berufsbezug vor, wenn Emails an einen Unternehmer versandt werden, die dieser nicht erhalten möchte.[652] Daher fehlt der Maßnahme ein Berufsbezug. Ein Eingreifen der Berufsfreiheit scheidet daher aus.
Im Rahmen der Verhältnismäßigkeitsprüfung sind hier folglich auf Seiten der Werbetreibenden und der an Email-Werbung interessierter Personenkreise auf Meinungs- bzw. Informationsfreiheit, Art. 10 Abs. 1 GG sowie auf Seiten der nicht an Werbung interessierter Personen deren Recht auf Privatleben gemäß Art. 8 Abs. 1 EMRK in die Abwägung miteinzustellen. Diese wird nicht anders ausfallen, als im Bereich des Verfassungsrechts,[653] so dass auf die dortigen Ausführungen verwiesen werden kann. Demnach ist die Beschränkung verhältnismäßig.

(bb) Wesensgehaltsgarantie

Der Wesensgehalt der Gemeinschaftsgrundrecht ist nicht angetastet. Die Ausführungen zu den nationalen Grundrechten gelten entsprechend.

(3) Zwischenergebnis

Die Gemeinschaftsgrundrechte stehen den Beschränkungen im Bereich der Email-Werbung durch die Vorschriften des deutschen einfachen Rechts nicht entgegen.

---

[645] EGMR, EuGRZ 1979, S. 626, Nr. 32 f. - Airey/Irland; EGMR, Urt. v. 27.04.1979, Marckx; EGMR, Nr. 14327/88 Sibson/Vereinigtes Königreich; EGMR, Nr. 16/1993/411/490, Keegan/Irland; EMGR, Nr. 59320/00, Caroline von Hannover/Bundesrepublik Deutschland; *Bernsdorff* in Meyer, Art. 7 GRC, Rn. 16; *Borowsky* in Meyer, Art. 51 GRC, Rn. 31; *Bröhmer*, EuZW 2006, S. 75; *Holoubek*, DVBl. 1997, S. 1034; *Meyer-Ladewig*, Art. 8 EMRK, Rn. 20, 37, Art. 10 EMRK, Rn. 2; *Ohly*, GRUR Int. 2004, S. 909
[646] EGMR, Nr. 48 553/99, Rn. 96 ff. Sovtransavto Holding/Ukraine; *Jarass*, EU-Grundrechte, § 22, Rn. 36; *Meyer*, Art. 17 GRC, Rn. 18;
[647] *Jarass*, EU-Grundrechte, § 22, Rn. 13; *Kingreen* in Calliess/Ruffert, 2. Aufl., Art. 6 EUV, Rn. 145
[648] EGMR, EuGRZ 1988, S. 35 ff., Rn. 41 - van Marle u.a./Niederlande
[649] *Jarass*, EU-Grundrechte, § 22, Rn. 13; *Kingreen* in Calliess/Ruffert, 2. Aufl., Art. 6 EUV, Rn. 145
[650] so angedeutet in: EuGH, Slg. 1980, S. 907, Rn. 90 - Valsabbia/Kommission; vgl. auch: *Kingreen* in Calliess/Ruffert, 2. Aufl., Art. 6 EUV, Rn. 145; *Penski/Elsner*, DÖV 2001, S. 269
[651] vgl.: 2. Kap. Teil 1 B. 2. b) aa)
[652] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[653] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)

2. Völkerrecht

Fraglich ist, ob die Vorschriften des deutschen einfachen Rechts, die eine Beschränkung der Zulässigkeit der Email-Werbung bewirken, gegen Völkerrecht verstoßen.

Bedeutung gewinnen hier die EMRK und der IPbürgPR.[654] Völkerrechtlichen Verträgen kommt innerstaatlich Gesetzesrang zu, soweit ihnen nach Art. 59 Abs. 2 GG durch ein Parlamentsgesetz der Rechtsanwendungsbefehl erteilt wurde.[655] Verfassungsrang können völkerrechtliche Verträge nach deutschem Recht danach nicht für sich beanspruchen.[656] Etwas anderes würde sich nur dann ergeben, wenn die genannten Bestimmungen als allgemeine Regeln des Völkerrechts im Sinne des Art. 25 GG anzusehen wären. Hierunter sind Rechtsvorschriften zu verstehen, die allgemein gelten, das bedeutet, von der überwiegenden Mehrheit der Staaten, der weitaus größeren Zahl anerkannt werden.[657] Die allgemeinen Regeln des Völkerrechts gehen im Rang dem einfachen Bundesrecht vor.[658] Das Völkervertragsrecht zählt mangels allgemeiner Geltung jedoch nicht zu den allgemeinen Regeln des Völkerrechts und zwar auch dann nicht, wenn der Vertrag von der Mehrheit von Staaten abgeschlossen worden ist.[659] Insoweit ist Art. 59 Abs. 2 GG lex specialis.[660] Der EMRK und den weiteren Menschenrechtsgewährleistungen kommt demnach der Rang eines einfachen Bundesgesetzes zu.

a) EMRK

Die genannten Vorschriften könnten einen Eingriff in das Konventionsrecht der Meinungsfreiheit darstellen. Es gelten die bereits dargestellten Grundsätze zu den Gemeinschaftsgrundrechten,[661] da diese entscheidend durch Art. 8 Abs. 1, 10 Abs. 1 EMRK und die dazu ergangene Rechtsprechung des EGMR geprägt wurden.[662] Die Berufsfreiheit garantiert die EMRK nicht.
Auch hinsichtlich der Rechte derjenigen Personenkreise, die am Erhalt von Email-Werbung interessiert sind gelten obige Ausführungen.[663]
Im Rahmen der Abwägung sind die Rechte derjenigen Personenkreise zu berücksichtigen, die Email-Direktwerbung nicht erhalten möchten. Dieses resultiert nach der hier vertretenen

---

654 vgl. zur EMRK: BGBl. II 1952, S. 686, 953; zum IPbürgPR: BGBl. II 1973, S. 1534 ff.
655 BVerfGE 1, S. 396 ff., 410 f.; BVerfGE 29, S. 348 ff., 358; BVerfGE 90, S. 286 ff., 364; BVerfGE 99, S. 145 ff., 158; BVerfGE 104, S. 151 ff., 209; BVerwGE 110, S. 363 ff., 366; *Bernhardt* in Isensee/Kirchhof, Band VII, § 174, Rn. 28 f.; *Jarass* in Ders./Pieroth, Art. 59 GG, Rn. 17 ff.; *Streinz* in Sachs, Art. 59 GG, Rn. 60
656 BVerwGE 47, S. 365 ff., 378 f.; BVerwGE 110, S. 363 ff., 366; *Bernhardt* in Isensee/Kirchhof, Band VII, § 174, Rn. 29; *Jarass* in Jarass/Pieroth, Art. 59 GG, Rn. 19
657 BVerfGE 15, S. 25 ff., 34; BVerfGE 16, S. 27 ff., 33; BVerfGE 23, S. 288 ff., 316 f.; BVerfGE 94, S. 315 ff., 322; *Jarass* in Ders./Pieroth, Art. 25 GG, Rn. 5; *Pernice* in Dreier, Art. 25 GG, Rn. 17; *Streinz* in Sachs, Art. 25 GG, Rn. 22
658 BVerfGE 6, S. 309 ff., 316; BVerfGE 23, S. 288 ff., 316 f.; BVerfGE 36, S. 342 ff., 365; BVerfGE 37, S. 271 ff., 279; BVerwGE 72, S. 241 ff., 250 f.; *Jarass* in Ders./Pieroth, Art. 25 GG, Rn. 13; a.A.(Verfassungsrang): *Bleckmann*, DÖV 1996, S. 141; *Koenig* in von Mangoldt/Starck/Klein, Art. 25 GG, Rn. 49; *Steinberger* in Isensee/Kirchhof, Band VII, § 173, Rn. 61; *Streinz* in Sachs, Art. 25 GG, Rn. 85 ff., 88
659 BVerfGE 6, S. 309 ff., 363; BVerfGE 41, S. 88 ff., 120 f.; BVerfGE 100, S. 266 ff., 269; *Jarass* in Jarass/Pieroth, Art. 25 GG, Rn. 6
660 *Herdegen* in Maunz/Dürig, Art. 25 GG, Rn. 20; *Jarass* in Ders./Pieroth, Art. 25 GG, Rn. 6; *Koenig* in von Mangoldt/Klein/Starck, Art. 25 GG, Rn. 18; *Rojahn* in v. Münch/Kunig, Art. 25 GG, Rn. 10; *Steinberger* in Isensee/Kirchhof, Band VII, § 173, Rn. 9; *Tomuschat* in Isensee/Kirchhof, Band VII, § 172, Rn. 12
661 vgl.: 2. Kap. Teil 1 B. II. 1. b) bb)
662 vgl.: 2. Kap. Teil 1 B. II. 1. b) bb)
663 vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (1) (b)

Auffassung aus Art. 8 Abs. 1 EMRK.[664] Im Hinblick auf die Abwägung kann auf die obige Darstellung verwiesen werden.[665]

b) Weitere internationale Menschenrechtsgewährleistungen

Auch im IPbürgPR ist ein Recht auf Privatleben und Korrespondenz enthalten, vgl. Art. 17 IPbürgPR.[666] Eine die Vorschrift interpretierende „Rechtsprechung" des UN-Ausschusses für Menschenrechte ist zwar nicht existent, allerdings lassen die vorliegenden Entscheidungen darauf schließen, dass die den Schutzbereich der Bestimmung markierenden Begriff weit ausgelegt und Art. 17 IPbürgPR hinsichtlich seines personellen und sachlichen Anwendungsbereichs ähnliche Konturen verliehen werden, wie Art. 8 EMRK.[667] Daneben ist in Art. 19 IPbürgPR ein Recht auf freie Meinungsäußerungs- und Informationsfreiheit enthalten, Art. 19 IPbürgPR.[668] Vorbild der Vorschrift war Art. 19 AEMR, der allerdings keine rechtliche Verbindlichkeit zukommt.[669] Der Schutzbereich des Art. 19 IPbürgPR ist dabei weiter, als der des Art. 10 EMRK.[670]
Aufgrund des der EMRK entsprechenden bzw. über diese hinausgehenden Gewährleistungsgehalts der Rechte des IPbürgPR wird sich hier keine andere Beurteilung ergeben als im Rahmen der EMRK.[671]

c) Zwischenergebnis

Folglich liegt auch kein Verstoß gegen internationale Menschenrechtsgewährleistungen vor.[672]

---

[664] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)
[665] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)
[666] die Vorschrift lautet: *„1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
2. Everyone has the right to the protection of the law against such interference or attacks."
[667] *Bernsdorff* in Meyer, Art. 7 GRC, Rn. 4; *Seidel*, Handbuch, S. 74 ff., 83 f.; vgl. etwa: Entscheidung v. 09.04.1981, EuGRZ 1981, S. 391 - Maurizische Frauen/Mauritius; Entscheidung v. 29.10.1981, EuGRZ 1982, S. 13 - Pinkney/Kanada; Entscheidung v. 29.03.1989, EuGRZ 1984, S. 423 - Erstrella/Uruguay
[668] die Vorschrift lautet: *„1. Everyone shall have the right to hold opinions without interference.*
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
(a) For respect of the rights or reputations of others;
(b) For the protection of national security or of public order (ordre public), or of public health or morals."
[669] *Bernsdorff* in Meyer, Art. 11 GRC, Rn. 3; *Defeis*, 29 Stan. J. Int´l Law, S. 76 f.; *Determann*, a.a.O., S. 246 f.; *Kimminich*, S. 340; *Verdross/Simma*, S. 822
[670] *Bernsdorff* in Meyer, Art. 11 GRC, Rn. 3
[671] vgl.: 2. Kap. Teil 1 B. II. 2. a)
[672] Im Rahmen dieser Arbeit wird nur auf Verpflichtungen eingegangen, speziell gegen die Belästigung durch unerwünschte Email-Werbung vorzugehen. Verpflichtungen, die sich etwa zum Schutz der Ehre vor privaten Beeinträchtigungen, vgl. Art. 17 Abs. 1, 2 IPbürgR, zum Schutz vor Rassendiskriminierung, vgl. Art. 26 S. 2 IPbürgR sowie vor Kriegspropaganda und dem Eintreten für nationalen, rassischen oder religiösen Hass, durch das zu Diskriminierung, Feindseligkeit oder Gewalt aufgestachelt wird, vgl. Art. 20 IPbürgR oder vor Pornographie, vgl. Art. 34 c, Art. 19 Abs. 1 und Art. 4 des Übereinkommens über die Rechte des Kindes vom 20.11.1989, BGBl. 1992 II, S. 192, soll hier nicht eingegangen werden, weil das Eingehend auf spezielle Inhalte den Rahmen dieser Arbeit sprengen würde, vgl. hierzu *Determann*, a.a.O., S. 245 ff.

III. Ergebnis

Die geltenden Vorschriften des deutschen Rechts stehen mit verfassungs-, gemeinschafts- sowie völkerrechtlichen Vorschriften im Einklang. Die genannten Vorschriften sind deshalb weder ungültig, noch besteht eine gesetzgeberische Verpflichtung, die Normen aufzuheben oder ein Anwendungsvorrang einer widersprechenden internationalen bzw. gemeinschaftsrechtlichen Vorschrift.

C. Ergebnis

Nach deutschem Recht ist das Versenden unverlangter Email-Werbung unzlässig, sofern nicht zuvor die Einwilligung des Empfängers eingeholt wurde. Dies ergibt sich einerseits aus §§ 7 Abs. 1, Abs. 2 Nr. 3 in Verbindung mit § 3 UWG, andererseits aus §§ 823 Abs. 1, 1004 Abs. 1 BGB. Es gilt somit das Opt-In-Prinzip. Eingeschränkt wird dieses lediglich durch die in § 7 Abs. 3 UWG genannte Ausnahmekonstellation, wobei diese sowohl im Wettbewerbs-, als auch im Deliktsrecht Anwendung findet. Bewirkt das Zusenden der Werbe-Email -auch im Zusammenwirken mit anderen derartigen Nachrichten- dass der Empfänger erwünschte Emails nicht mehr von Werbenachrichten unterscheiden kann, so ist die Tätigkeit auch strafrechtlich sanktioniert, § 303 a StGB. Über §§ 823 Abs. 2, 1004 Abs. 1 BGB ergeben sich in diesem Fall auch zivilrechtliche Ansprüche.
Die dargestellten Vorgaben des einfachen deutschen Rechts verstoßen weder gegen deutsches Verfassungsrecht, noch gegen Gemeinschafts- oder Völkerrecht.

Teil 2: Zulässigkeit technischer Maßnahmen zur Identifizierung und Vermeidung unerbetener elektronischer Werbenachrichten

Gegenstand dieser Arbeit ist die Frage nach der rechtlichen Zulässigkeit der verschiedenen Maßnahmen, die der Filtereinsatz zum Zweck der automatisierten Identifizierung und Abwehr unverlangter elektronischer Werbenachrichten mit sich bringt. Die Filtersoftware bewirkt, wie bereits dargestellt,[673] dass Inhalt und Headerinformationen eingehender Emails durch das Programm überprüft werden. Positiv gescannte Nachrichten werden entweder gelöscht, blockiert, als verdächtig markiert oder in Quarantäne-Ordnern abgelegt.[674]
Der Einsatz von Filtersoftware stellt die Reaktion auf das Versenden unverlangter kommerzieller Emails dar. Die Widerrechtlichkeit der abgewehrten Nachrichten kann demnach mögliche Abwehrmaßnahmen rechtfertigen. Deshalb wurde in Kapitel 2 Teil 1 darauf eingegangen, ob bzw. unter welchen Voraussetzungen der Versand solcher Emails nach Maßgabe des deutschen Rechts als zulässig anzusehen ist. Nachdem diese Frage beantwortet wurde, kann nun das Hauptproblem der Arbeit dargestellt werden. Nachfolgend wird daher die Frage beantwortet, wie die Überprüfung von Inhalt und Headerinformationen eingehender Emails durch die zur Filterung eingesetzte Software rechtlich zu beurteilen ist und ob es zulässig ist, Emails im Rahmen von Spam-Filtermaßnahmen zu blockieren, zu löschen, durch Hinzufügen einer zusätzlichen Headerzeile oder Veränderung der Subjektzeile zu markieren oder in Quarantäne-Ordner umzuleiten.
Dabei wird zunächst auf den Maßstab des einfachen Rechts eingegangen (A.), im Anschluss daran wird überprüft, ob die Rechtslage im Einklang mit internationalen, gemeinschafts- und verfassungsrechtlichen Vorgaben steht (B.).

[673] vgl.: 1. Kap. Teil 2 A.
[674] vgl.: 1. Kap. Teil 2 B.

A. Einfaches Recht

Der Zulässigkeit der verschiedenen Maßnahmen in Bezug auf als Spam identifizierte Emails könnten das Datenschutzrecht und das einfachgesetzliche Fernmeldegeheimnis (I.) sowie straf- (II.) oder bürgerlich-rechtliche (III.) Vorschriften entgegenstehen.

I. Datenschutzrecht und einfachgesetzliches Fernmeldegeheimnis

Fraglich ist, ob die Vorschriften des bereichsspezifischen oder allgemeinen Datenschutzrechts (1.) oder das einfachgesetzliche Fernmeldegeheimnis (2.) eingreifen.

1. Allgemeines und bereichsspezifisches Datenschutzrecht

In dem Einsatz der Software mit den genannten Folgen könnte ein Verstoß gegen allgemeines oder bereichsspezifisches Datenschutzrecht liegen. Insbesondere könnten die Vorschriften des BDSG,[675] der §§ 91 ff. des TKG[676] bzw. der §§ 11 ff. des TMG[677] den Filtermaßnahmen entgegenstehen. Verstöße gegen allgemeine oder bereichsspezifische datenschutzrechtliche Regelungen können zu Löschungs-,[678] Berichtigungs-,[679] oder Schadensersatzansprüchen[680] führen. Andererseits stellen unzulässige Datenverarbeitungsvorgänge teilweise eine Straftat,[681] teilweise eine bußgeldbewehrte Ordnungswidrigkeit[682] dar.
Im Datenschutzrecht gilt der Grundsatz, dass die Erhebung, das Speichern, Verarbeiten und die Weitergabe personenbezogener Daten verboten ist,[683] soweit nicht der Betroffene seine Einwilligung erklärt hat oder ein gesetzlich geregelter Erlaubnistatbestand eingreift, vgl. §§ 4 Abs. 1 BDSG.[684]
Die verschiedenen Filterverfahren wurden oben bereits beschrieben.[685] Ihnen ist gemeinsam, dass eingehende Emails durch die Software auf bestimmte Merkmale in ihrem Text oder Header überprüft und so anhand der gefundenen Kriterien als erwünscht oder unerwünscht qualifiziert werden. Als unerwünscht erkannte Emails werden sodann von dem Programm gelöscht, blockiert, als kommerzielle Email markiert oder aber in spezielle Quarantäne-Ordner im Email-Postfach des Empfängers umgeleitet.
Es stellt sich die Frage, ob das durch den Filtereinsatz bedingte Durchsuchen von Inhalt und Headerinformationen eingehender Emails sowie das weitere Vorgehen hinsichtlich positiv gescannter Nachrichten wie das Blockieren, Löschen, Umleiten oder Einstellen in eine Quarantäne-Mailbox datenschutzrechtlich zulässig sind. Würde der Filtereinsatz datenschutzrechtlich unzulässige Verarbeitungsschritte mit sich bringen, so wäre dieser rechtswidrig, sofern kein gesetzlicher Erlaubnistatbestand eingreift oder sämtliche von der Datenverarbeitung Betroffenen ihre vorherige Einwilligung mit den entsprechenden

---

[675] Neubekanntmachung des BDSG in der Form des Bekanntmachung v. 20.12.1990, BGBl. I, S. 2954 ff., in der ab 28.08.2002 geltenden Fassung
[676] Telekommunikationsgesetz vom 22. Juni 2004, BGBl. I, S. 1190 ff.
[677] Telemediengesetz vom 26. Februar 2007, BGBl. I, S. 179 ff.
[678] vgl. § 35 Abs. 2 S. 2 BDSG; vgl. auch Art. 14 DSRL
[679] vgl. § 35 Abs. 1 BDSG; vgl. auch Art. 14 DSRL
[680] vgl. § 7, 8 BDSG
[681] vgl. § 43 Abs. 2 Nr. 1 BDSG in Verbindung mit § 44 Abs. 1 BDSG
[682] vgl. §§ 14 Abs. 1, 15 Abs. 1 S. 1, Abs. 8 S. 1, Abs. 8 S. 2 jeweils i. V. m. § 16 Abs. 2 Nr. 5 TMG; § 43 Abs. 2 Nr. 1 BDSG; § 149 Abs. 1 Nr. 16, 17 TKG
[683] *Helfrich* in Hoeren/Sieber, Handbuch Multimediarecht, 16.1, Rn. 33; *Sokol* in Simitis, § 4 BDSG, Rn. 2
[684] BVerfGE 65, S. 1 ff., 43; *Helfrich* in Hoeren/Sieber, 16.1, Rn. 34 f.; *Schmitz* in Spindler/Schmitz/Geis, Einführung TDDSG, Rn. 2 ff.; *Simitis*, DuD 2000, S. 720; *Walz* in Simitis, § 4 BDSG, Rn. 4 ff.; vgl. auch: § 12 Abs. 1 TMG, der allerdings nur solche Erlaubnistatbestände zulässt, die im TMG enthalten sind oder aber sich ausdrücklich auf Telemedien beziehen.
[685] vgl.: 1. Kap. Teil 2 A.

Vorgängen erklärt haben. Hierbei ist zu beachten, dass der Filtereinsatz bereits dann rechtswidrig ist, wenn dabei einzelne unzulässige Vorgänge vorgenommen werden.

Nachfolgend wird dargestellt, ob die im Rahmen des Filtereinsatzes stattfindenden Vorgänge als Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu qualifizieren sind (a) und, falls ja, in welchen Fällen diese durch eine Einwilligung der Betroffenen gedeckt sein wird bzw. ein gesetzlicher Erlaubnistatbestand eingreift (b).

a) Erhebung, Verarbeitung oder Nutzung personenbezogener Daten

Fraglich ist, ob in der Überprüfung von Inhalt und Headerinformationen eingehender Emails durch die zur Filterung eingesetzte Software sowie in dem Blockieren, Löschen oder durch Hinzufügen einer zusätzlichen Headerzeile oder Veränderung der Subjektzeile erfolgenden Markieren von Emails eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu sehen ist.

aa) Personenbezogene Daten

Es ist zu untersuchen, ob einzelne oder mehrere der bei der Überprüfung von Emails auf ihre Eigenschaft als Werbe-Email oder im Anschluss an eine positive Bewertung durchgeführten Verarbeitungsschritte datenschutzrechtlich unzulässig sind. Die Maßnahmen betreffen, wie bereits dargestellt wurde,[686] Informationen, die im Inhalt oder Header der Email enthalten sind oder aber die gesamte Email.

Somit stellt sich die Frage, ob die im Inhalt und Header der Email enthaltenen Informationen als personenbezogene Daten zu qualifizieren sind. Das bereichsspezifische Datenschutzrecht enthält keine Definition dieses Begriffs. Hier greift deshalb das BDSG ein, das ausweislich seines § 1 Abs. 3 S. 1 subsidiär auch dort Anwendung findet.
Nach Maßgabe des § 3 Abs. 1 BDSG umfasst der Begriff des personenbezogenen Datums Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Daten juristischer Personen oder anderer rechtsfähiger Personenmehrheiten werden hingegen nach der Definition des § 3 Abs. 1 BDSG nicht erfasst. Gleiches gilt im Bereich des Telemediengesetzes, das nach § 11 Abs. 1 TMG nur personenbezogene Daten der Nutzer miteinbeziehen möchte, wobei unter diesen Begriff lediglich natürliche Personen gefasst werden, vgl. § 11 Abs. 2 TMG. Das Telekommunikationsdatenschutzrecht findet hingegen nicht nur auf personenbezogene Daten natürlicher Personen Anwendung, sondern auch auf dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, falls sie mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, § 91 Abs. 1 S. 2 TKG.

Im Folgenden wird dargestellt, welche der von den Filtermaßnahmen betroffenen Daten als personenbezogen anzusehen sind. Es wird geprüft, ob die von der Filtermaßnahme erfassten Daten als Einzelangaben über persönliche oder sachliche Verhältnisse der betroffenen Person anzusehen sind (1) und in welchen Fällen der Betroffene bestimmt oder bestimmbar ist (2).

[686] vgl.: 1. Kap. Teil 2 A. II.

(1) Einzelangabe über persönliche oder sachliche Verhältnisse der betroffenen Person

Voraussetzung für das Vorliegen eines personenbezogenen Datums ist ausweislich der Definition des § 3 Abs. 1 BDSG, dass es sich bei der entsprechenden Information um eine Einzelangabe über persönliche oder sachliche Verhältnisse der betroffenen Person handelt. Zu prüfen ist folglich, ob im Inhalt oder Header einer Email solche Einzelangaben enthalten sind bzw. zumindest in Einzelfällen enthalten sein können. Eine Einzelangabe liegt dann vor, wenn sich die fragliche Information auf eine bestimmte natürliche Person bezieht oder wenn sie geeignet ist, einen Bezug zu dieser herzustellen, wie dies etwa bei dem Namen, der Ausweis- oder Versicherungs- sowie der Telefonnummer des Betroffenen der Fall ist.[687]

Im Inhalt einer Email werden häufig Informationen enthalten sein, die einen Bezug zur betroffenen Person herstellen können, wie etwa ihr Name oder ihre Telefonnummer. Somit wird durch Filtermaßnahmen, die den Inhalt einer Email durchsuchen, in aller Regel zumindest bisweilen auf Einzelangaben über persönliche oder sachliche Verhältnisse der betroffenen Person zugegriffen.

Einige Filtermethoden beschränken sich jedoch auf die Überprüfung von Headerinformationen und bringen damit keinen Zugriff auf Inhaltsdaten mit sich. Dies ist beim Black- und Whitelisting und der Frequenzanalyse der Fall, da hier die Verbindung bereits aufgrund bestimmter Headerdaten wie Email- oder IP-Absenderadresse unterbrochen oder aber ohne weitere inhaltliche Kontrolle durchgeführt wird.[688] Bei diesen Verfahren gewinnt die Frage Relevanz, ob auch den im Header enthaltenen Daten, die durch die Filtersoftware überprüft werden, ein Personenbezug zukommt. Voraussetzung ist, dass es sich bei den genannten Informationen um Einzelangaben über persönliche oder sachliche Verhältnisse der betroffenen Person handelt. Der Email-Header enthält die Email- und IP-Adresse von Absender und Empfänger, Angaben über den Zeitpunkt der Erstellung bzw. der Versendung der Nachricht, den Betreff und die Bezeichnung der angehängten Dateien.[689] Fraglich ist, welche dieser Daten sich als Einzelangaben qualifizieren lassen. Die Betreffzeile der Email kann Einzelangaben enthalten. Hingegen sind Informationen über den Zeitpunkt der Erstellung bzw. Versendung und die Bezeichnung der angehängten Dateien nicht auf die Person bezogen und können somit für sich genommen keinen Bezug zu ihr herstellen. Demnach handelt es sich dabei nicht um Einzelangaben. Etwas anderes könnte jedoch für die IP- und die Email-Adressen gelten, die ebenfalls Bestandteil des Email-Headers sind. Email-Adressen, die den Namen des Betroffenen enthalten, identifizieren ihn. Da IP- und auch solche Email-Adressen, die nicht den Namen oder Namensbestandteile einer natürlichen Person erfassen, wie oben dargestellt,[690] mit Hilfe des Providers dem Nutzer zugeordnet werden können, sind sie geeignet den Bezug zu der betroffenen Person herzustellen und fallen somit ebenso wie etwa die Wohnadresse oder die Telefonnummer unter den Begriff der

[687] BGH, NJW 1986, S. 2506 (Kreditdaten und Kontostände); BAG, NJW 1987, S. 676 f. (Telefonnummer einer betrieblichen Nebenstelle); BAG, RDV 1988, S. 197 f. (in Fahrtenschreibern festgehaltene Daten über Lenkzeiten als Einzelangaben); KG Berlin, Urteil vom 26.05.1983, Simitis/Dammann/Mallmann/Reh, BDSG-Dokumentation, § 2 Abs. 3, E 3 (momentaner Aufenthalt als Einzelangabe); *Auernhammer*, § 3 BDSG, Rn. 4; *Dammann* in Simitis, § 3 BDSG, Rn. 4 ff.; *Gola/Schomerus*, § 3 BDSG, Rn. 3; *Tinnefeld/Ehmann/Gerling*, S. 279

[688] vgl.: 1. Kap. Teil 2 A. II., IV.

[689] vgl.: 1. Kap. Teil 1 B. II. 1.

[690] vgl.: 1. Kap. Teil 1 A. I. 3.; 1. Kap. Teil 1 B. I.

Einzelangabe.[691] Über die genannten Einzelangaben können Inhalts- sowie weitere Informationen, die in der Email enthalten sind den Betroffenen zugeordnet werden.[692]

(2) Bestimmtheit oder Bestimmbarkeit des Betroffenen

Wie eben dargestellt wurde, können im Inhalt und der Betreffszeile der Email Einzelangaben über persönliche und sachliche Verhältnisse der betroffenen Person enthalten sein. Daneben fallen auch die im Header enthaltenen Email- und IP-Adressen unter den Begriff der Einzelangabe. Einzelangaben sind jedoch nur dann als personenbezogene Daten zu qualifizieren, wenn sie eine bestimmte oder bestimmbare Person betreffen, vgl. § 3 Abs. 1 BDSG. Deshalb ist im Folgenden zu überprüfen, ob sich die in der Email enthaltenen Einzelangaben auf eine bestimmte oder bestimmbare Person beziehen.

Eine Person ist bestimmt, wenn die Daten mit dem Namen des Betroffenen verbunden sind oder sich aus dem Inhalt oder dem Zusammenhang der Bezug unmittelbar herstellen lässt.[693] Häufig werden im Inhalt einer Email Informationen enthalten sein, die bestimmt sind, so der Name der betroffenen Person, der es zulässt, ihr etwaige weitere Inhaltsinformationen zuzuordnen.

Da einzelne Filterverfahren, wie das Black- und Whitelisting und die Frequenzanalyse nur Headerdaten betreffen, ist fraglich, ob die im Header enthaltenen Einzelangaben eine bestimmte Person betreffen. Im Fall von Email-Adressen kann es sich im Einzelfall um bestimmte Daten handeln. Von der Bestimmtheit der Person ist auszugehen, wenn die Adresse den Namen oder Namensbestandteile der betroffenen Person enthält. Andernfalls ist das Kriterium der Bestimmtheit nicht gegeben. Eine IP-Adresse wird nie den Namen der betroffenen Person enthalten, da es es sich bei diesen Adressen, wie oben dargestellt, um eine Zahlenfolge handelt.[694] Der Inhaber einer IP-Adresse ist demnach nie bestimmt.

Der Personenbezug liegt nicht nur dann vor, wenn die betroffene Person bestimmt ist, sondern auch wenn sie bestimmbar ist. Die Bestimmbarkeit wird bejaht, wenn der Personenbezug unter Zuhilfenahme von Kenntnissen und anderen Mitteln mittelbar hergestellt werden kann.[695]
Im Inhalt einer Email können Daten enthalten sein, welche die Herstellung des Personenbezugs zu der betroffenen Person ermöglichen. In diesem Fall ist von der Bestimmbarkeit der entsprechenden Informationen auszugehen. Daneben werden, wie eben dargestellt, häufig Daten enthalten sein, die bereits bestimmt sind.
Im Gegensatz hierzu ist bei Headerdaten grundsätzlich -von solchen Email-Adressen abgesehen, die den Namen des Betroffenen enthalten- keine Bestimmtheit gegeben, weshalb es hier für die Frage des Personenbezugs in aller Regel entscheidend auf die Bestimmbarkeit ankommt.

---

[691] vgl. zur Eigenschaft der Nummer einer betrieblichen Nebenstelle als personenbezogenes Datum: BAG, NJW 1987, S. 676 f.
[692] *Dammann* in Simitis, § 3 BDSG, Rn. 62
[693] *Dammann* in Simitis, § 3 BDSG, Rn. 21; *Gola/Schomerus*, § 3 BDSG, Rn. 9; *S. Meyer*, WRP 2002, S. 1029 f.; *Tinnefeld* in Roßnagel, 4.1., Rn. 20; *Tinnefeld/Ehmann/Gerling*, S. 279 f.
[694] vgl.: 1. Kap. Teil 1 A. I. 3.
[695] *Dammann* in Simitis, § 3 BDSG, Rn. 22; *Gola/Schomerus*, § 3 BDSG, Rn. 9; *Schmitz* in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 24; *Tinnefeld* in Roßnagel, 4.1., Rn. 21; *Tinnefeld/Ehmann/Gerling*, S. 280 ff., S. 280; vgl. auch: BGH, NJW 1991, S. 568 ff., 570; Art. 2 lit. a) sowie Erwägungsgrund Nr. 26 S. 2 der DSRL

Dabei ist der Personenbezug eines Datums nicht für sich festzulegen, also zu prüfen, ob einem Datum „als solchem“ ein Personenbezug zukommt, vielmehr kann eine Aussage lediglich dann getroffen werden, wenn das Datum im Kontext der jeweiligen Verarbeitung betrachtet wird.[696] Der Personenbezug hängt danach nicht von der Art des betroffenen Datums ab, sondern entscheidend vom Verarbeitungskontext. Deshalb kann es möglicherweise einen Unterschied machen, ob von den Maßnahmen bereits auf dem Empfängerserver gespeicherte Daten betroffen (a) oder aber Handlungen zu beurteilen sind, die nicht oder lediglich kurzfristig automatisch zwischengespeicherte Daten erfassen (b).

(a) Maßnahmen hinsichtlich bereits auf dem Empfängerserver gespeicherter Daten

Teilweise werden durch die Filtervorgänge Verarbeitungsschritte durchgeführt, die bereits auf dem Empfängerserver eingegangene und dort abgelegte Emails betreffen. Dies ist der Fall, wenn die Email nicht bereits aufgrund bestimmter vor dem endgültigen Abspeichern erkannter Merkmale als unerwünscht qualifiziert und blockiert, umgeleitet oder die bereits eingegangenen kurzfristig zwischengespeicherten Bestandteile wieder gelöscht werden. Maßnahmen hinsichtlich bereits auf dem Empfängerserver gespeicherter Daten betreffen danach Emails, die zwar als Spam erkannt, aber dennoch in die Mailbox des Empfängers oder einen speziellen Quarantäne-Ordner eingestellt wurden.
Dabei reicht es aus, wenn durch durch die Filtervorgänge in einzelnen Fällen personenbezogene Daten betroffen sind. Denn bereits dann führt die Software teilweise unzulässige Verarbeitungsvorgänge durch, wenn nicht die Einwilligung der Betroffenen vorliegt oder ein gesetzlich normierter Erlaubnistatbestand eingreift. Soweit nicht nach den eben dargestellten Grundsätzen bestimmte Daten betroffen sind, stellt sich die Frage nach der Bestimmbarkeit der im Inhalt und dem Header enthaltenen Informationen.

Wie bereits dargestellt wurde, müssen die Internetnutzer einen Vertrag mit einem Internet-Access-Provider abschließen, um eine statische oder dynamische IP-Adresse zugewiesen zu bekommen und zwar auch dann, wenn die Teilnahme kostenfrei ist.[697] Hierfür ist in aller Regel die Angabe personenbezogener Daten, insbesondere des Namens und der Adresse des Nutzers erforderlich.[698] Gleiches gilt für die Vergabe von Email-Adressen.[699] Auch Netzwerk-Administratoren liegen die genannten Informationen grundsätzlich vor, da sie die IP- und Email-Adressen an die Nutzer vergeben.[700] Danach kann der Inhaber einer Email-Adresse durch den Email-Service-Provider bzw. LAN-Verwalter identifiziert werden, der ihm die Adresse zur Verfügung gestellt hat.[701] Eine statische IP-Adresse kann der Internet-Service-Provider oder LAN-Verwalter, der diese zugewiesen hat, mit einem bestimmten Rechner in Verbindung bringen, denn, wie oben bereits ausgeführt wurde,[702] halten Provider und Administratoren Datum, Zeitpunkt und Dauer der Zuweisung der betreffenden IP-Adresse in einem Log-Protokoll fest. Auch bei der Vergabe dynamischer IP-Nummern können sie diese mittels Rückgriff auf das festgehaltene Log-Protokoll einzelnen Anschlüssen zuordnen.[703] In den Fällen, in denen der Internet-Nutzer über ein öffentliches Telekommunikationsnetz die Verbindung hergestellt hat, besitzt auch die Telefongesellschaft

[696] *Dammann* in Simitis, § 3 BDSG, Rn. 20; *Hornung*, DuD 2004, S. 430
[697] vgl.: 1. Kap. Teil 1 A. I. 3. b)
[698] vgl.: 1. Kap. Teil 1 A. I. 3. b)
[699] vgl.: 1. Kap. Teil 1 B. II. 3.
[700] vgl.: 1. Kap. Teil 1 A. I. 3. a)
[701] *Roßnagel/Scholz*, MMR 2000, S. 725; *Terwagne/Louveaux*, MMR 1998, S. 452.; vgl. auch: 1. Kap. Teil 1 A. I. 3.; 1. Kap. Teil 1 B. I.
[702] vgl.: 1. Kap. Teil 1 A. I. 3. b)
[703] vgl.: 1. Kap. Teil 1 A. I. 3. b)

Informationen, welche zur Bestimmung des Nutzers beitragen können und zwar die Nummer des Anrufers mit Datum, Stunde und Dauer der Verbindung.[704]
Im Ergebnis liegen somit bestimmten Personengruppen, insbesondere den Internet- sowie Email-Service-Providern und Netzwerk-Administratoren zusätzliche Informationen vor, mit deren Hilfe der Personenbezug hinsichtlich der IP- und Email-Adresse von Absender und Empfänger hergestellt werden kann.[705] Für Dritte besteht die Möglichkeit, diese Informationen zu erhalten, indem sie mittels des Befehls „finger" auf die „passwd"-Datei zugreifen.[706] Selbst im Fall von Maskerade-Emails, bei denen die Email-Adresse des Absenders gefälscht wird, ist eine Zuordnung in aller Regel unter Zuhilfenahme der IP-Adresse möglich.[707]
Etwas anderes gilt, wenn sich der Nutzer bei dem Provider nicht unter seinem wirklichen Namen und Angabe seiner Daten, sondern anonym angemeldet hat. In diesem Fall wird grundsätzlich keine Möglichkeit bestehen, die Adresse dem Inhaber bzw. Nutzer zuzuordnen.

Im Hinblick auf IP-Adressen wurde allerdings bisher nur festgestellt, dass sich diese mit Hilfe der bei den Internet-Access-Providern und LAN-Verwaltern gespeicherten Daten einem bestimmten Anschluss zuordnen lassen. Dies lässt jedoch noch nicht den Rückschluss auf eine bestimmte Person zu, da häufig mehrere Nutzer an einem Rechner arbeiten. Aus diesem Grund könnte der Personenbezug zu verneinen sein. Allerdings ist zu berücksichtigen, dass -soweit einmal der Anschluss des jeweiligen Nutzers identifiziert wurde- sich durch weitere Ermittlungen herausfinden lässt, um wessen Daten es sich handelt.[708] Es wird in aller Regel feststellbar sein, wer den fraglichen Rechner zu welchem Zeitpunkt genutzt hat, so etwa durch Nachfrage beim Netzwerkadministrator, Access Provider oder der Telefongesellschaft, über welche die Verbindung hergestellt wurde.[709] Demnach bedeutet die Tatsache, dass sich die IP-Adresse zunächst nur einem Rechner, nicht jedoch einer bestimmten Person zuordnen lässt, nicht, dass deshalb ein Personenbezug zu verneinen ist.[710] Im Ergebnis scheidet dieser somit nicht deshalb aus, weil einem Datum zunächst nicht mit Sicherheit eine einzelne Person, sondern lediglich eine Personengruppe zugeordnet werden kann, sofern sich -wie hier- durch zusätzliche Nachforschungen herausfinden lässt, auf welche Person sich das Datum bezieht.[711]

Demnach lässt sich festhalten, dass den Providern und Netzwerkverwaltern die für die Herstellung des Personenbezugs erforderlichen Informationen vorliegen. Etwas anderes gilt lediglich bei einer anonymen Anmeldung. Allerdings kann beim Filtereinsatz nicht ausgeschlossen werden, dass zumindest auch Emails von den Maßnahmen betroffen werden, deren Absender sich nicht anonym bei ihrem Email-Anbieter angemeldet haben. Insofern gilt der dargestellte Grundsatz, dass es für die Unzulässigkeit des Filtereinsatzes ausreicht, wenn

---

[704] *Schaar*, Datenschutz im Internet, Rn. 171; vgl. auch: 1. Kap. Teil 1 A. I. 3. b)
[705] *Köhler/Arndt/Fetzer*, Recht des Internet, S. 297; *Roßnagel/Scholz*, MMR 2001, S. 725; *Ruess/Patzak*, RDV 2003, S. 169; *Strömer*, Online-Recht, S. 274; vgl. auch: AG, Darmstadt, MMR 2005, S. 634 ff., 635: in dem Verfahren war zwischen den Parteien unstreitig, dass dynamische IP-Adressen dazu führen können, das Nutzerverhalten im Internet transparent zu machen und mit weiteren Daten einen Personenbezug herzustellen, mit der Folge, dass nachvollzogen werden kann, welche Aktivitäten bestimmte Personen im Internet entfaltet haben, ebenso ging die Folgeinstanz vom Personenbezug aus; vgl. dazu: LG Darmstadt, GRUR-RR, S. 173 ff.; BGH, Urteil vom 26.10.2006, III ZR 40/06
[706] vgl. dazu bereits: 1, Kap. Teil 1 A. I. 4. a)
[707] vgl.: 1. Kap. Teil 1 B. II. 3.
[708] *Schaar*, Datenschutz im Internet, Rn. 154
[709] *Schaar*, Datenschutz im Internet, Rn. 171
[710] *Schaar*, Datenschutz im Internet, Rn. 171
[711] *Helfrich* in Hoeren/Sieber, 16.1, Rn. 31; *Schaar*, Datenschutz im Internet, Rn. 154; ähnlich: *Tinnefeld/Ehmann/Gerling*, S. 281; für statische IP-Adressen: *Golembiewski* in Bäumler/von Mutius, S. 107 ff., 109

dieser in einzelnen Fällen dazu führt, dass unerlaubt personenbezogene Daten verarbeitet werden. Es ist nicht erforderlich, dass dies stets der Fall ist. Hier werden zumindest teilweise Emails von den Maßnahmen erfasst werden, deren Absender sich nicht anonym angemeldet haben. Werden Verarbeitungsvorgänge hinsichtlich bereits auf dem Empfängerserver gespeicherter Nachrichten vorgenommen, so sind danach stets auch bestimmbare Personen betroffen.
Mittels des „finger"-Befehls können sich auch Dritte Informationen besorgen, die den Personenbezug herzustellen vermögen. Die Bestimmbarkeit besteht folglich für den Provider des jeweiligen Nutzers stets, für Dritte bei Anwendung bestimmter Verfahren oder Kenntnisse bzw. dann, wenn der Provider die entsprechenden Information an sie weiter gibt.

(aa) Fehlende datenschutzrechtliche Relevanz von IP- und Email-Adressdaten?

Zwar ist der Inhaber einer Email- oder IP-Adresse unter Zuhilfenahme zusätzlicher Informationen und gegebenenfalls weiterer Nachforschungen bestimmbar.[712] Jedoch stellt sich die Frage, ob rein technischen Daten, wie IP- und Email-Adressen eine datenschutzrechtliche Relevanz nicht dennoch mit dem Argument abzusprechen ist, dass das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG herzuleitende informationelle Selbstbestimmungsrecht des Betroffenen, das Schutzgegenstand des Datenschutzrechts ist,[713] durch eine Kenntnis lediglich dieser Daten nicht tangiert wird.

Hiergegen lässt sich einerseits anführen, dass die DSRL, die auf das BDSG im Wege der richtlinienkonformen Auslegung Einfluss entfaltet,[714] ausdrücklich auch technische Angaben wie Kennummern in den Begriff der personenbezogenen Daten einbezieht, vgl. Art. 2 lit. a) DSRL.[715] Dies spricht dafür, auch im Bereich des BDSG den Personenbezug von Email- und IP-Adresse nicht deshalb auszuschließen, weil es sich lediglich um technische Angaben mit möglicherweise geringer Persönlichkeitsrelevanz handelt.
Daneben ist zu beachten, dass das Bundesverfassungsgericht bereits im Volkszählungsurteil aussprach, dass es unter der Bedingung der automatischen Datenverarbeitung kein „belangloses" Datum mehr geben könne, da entscheidend allein seine Nutzbarkeit und Verwendungsmöglichkeit sei.[716] Diese wiederum hängen nach Auffassung des Gerichts einerseits von dem Zweck ab, dem die Erhebung dient, andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten.[717] Das Gericht stellt also darauf ab, dass auch eine für sich unerhebliche Information in Verknüpfung mit anderen Daten Rückschlüsse auf den Betroffenen, seinen Lebensweg und seine

[712] vgl. dazu soeben: 2. Kap.Teil 2 A. I. 1. a) aa) (2) (a)
[713] BVerfGE 65, S. 1 ff., 41 ff.; *Denninger*, ZRP 1981, S. 231 ff.; *Gola/Schomerus*, § 1 BDSG, Rn. 6 ff.; *Meister*, DuD 1983, S. 163 ff.; *Simitis* in Ders., § 1 BDSG, Rn. 23 ff.; *Tinnefeld/Ehmann/Gerling*, S. 142 ff.; *Trute* in Roßnagel, 2.5, Rn. 1 ff., 7 ff.
[714] Allgemein zur richtlinienkonformen Auslegung: EuGH, Slg. 1984, S. 1891, Rn. 26 - von Colson und Kaman/Land Nordrhein-Westfalen; EuGH, Slg. 1984, S. I-1921, Rn. 26 - Harz/Deutsche Tradax; EuGH, Slg. 1987, S. 3969, Rn. 12 - Kolpinhuis Nijmegen; EuGH, Slg. 1988, S. 4635, Rn. 39 - Beentjes; EuGH, Slg. 1999, S. I-1103, Rn. 48 - Carbonari; EuGH, Slg. 2000, S. I-4619, Rn. 40 - Brinkmann Tabakfabriken; EuGH, Slg. 2000, S. I-4941, Rn. 30 - Océano Grupo; EuGH, Slg. 2000, S. I-6007, Rn. 16 - Centrosteel; EuGH, Slg. 2000, S. I-7881, Rn. 37 - Gozza; BVerfGE 75, S. 237; BAGE 61, S. 209; BAGE 70, S. 238; BGHZ 63, S. 264 f.; BGHZ 87, S. 61 f; BGHZ 138, S. 60 ff.; BVerwGE 49, S. 60; BFHE 132, S. 319; BFHE 140, S. 393; *Nettesheim* in Grabitz/Hilf, Art. 249 EUV, Rn. 153; *Ruffert* in Calliess/Ruffert, Art. 249 EGV, Rn. 115 ff.; speziell zur richtlinienkonformen Auslegung nach Maßgabe der DSRL: EuGH, Slg. 2003, S. I-04989, Rn. 93 - Rechnungshof u.a./Österreichischer Rundfunk; *Klug*, RDV 2001, S. 266 ff.; *Trosch*, DuD 1998, S. 724
[715] *Helfrich* in Hoeren/Sieber, 16.1, Rn. 31
[716] BVerfGE 65, S. 1 ff., 45
[717] BVerfGE 65, S. 1 ff., 45

Persönlichkeit ermöglichen kann.[718] Besonders die Herausbildung neuer Techniken spielt im Rahmen des Schutzes des allgemeinen Persönlichkeitsrechts eine Rolle.[719]
Ist die Email- oder IP-Adresse einer bestimmten Person zuordenbar, so ergeben sich vielfache Verarbeitungs- und Verknüpfungsmöglichkeiten, zu denen diese verwendet werden kann. Die genannten Daten lassen sich nutzen, um unter Zuhilfenahme zusätzlicher Kenntnisse und bestimmter Mittel Informationen über den Adressinhaber abzuleiten.
So können etwa durch den Einsatz von Cookies spezifische, den jeweiligen Nutzer betreffende Informationen gewonnen werden.[720] Unter Zuhilfenahme von Data-Mining-Techniken ist es so möglich, Vorlieben, Bedürfnisse und Kaufgewohnheiten des Betroffenen vorherzusagen.[721] Die erstellten Nutzerprofile können bei Kenntnis der IP-Adresse einem bestimmten Rechner und in aller Regel auch einer bestimmten Person zugeordnet werden.[722] Daneben ist es möglich, mittels Clickstreaming das gesamte Klickverhalten eines Internet-Nutzers aufzuzeichnen und dieses Verhalten einer bestimmten Person zuzuordnen.[723]
Bei Kenntnis der Email-Adresse eines Nutzers lassen sich unter Zuhilfenahme von Zusatzwissen Rückschlüsse auf die Kommunikationsgewohnheiten des Adressinhabers ziehen. So kann aus den bei der Email-Kommunikation angefallenen Daten ermittelt werden, ob zwei Personen keinen, einen asymmetrischen oder wechselseitigen Kontakt haben, wobei die Analyse letztlich sogar Hinweise auf den sozialen Status einer Person innerhalb einer bestimmten Gruppe geben kann.[724] Auch das Bundesverfassungsgericht hat mittlerweile ausgesprochen, dass Verbindungsdaten in zunehmendem Maß Rückschlüsse auf Art und Intensität von Beziehungen, auf Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den Kommunikationsinhalt zulassen und -je nach Art und Umfang der angefallenen Daten- Erkenntnisse vermitteln können, die an die Qualität eines Persönlichkeitsprofils heranzureichen vermögen.[725] Über die Email-Adresse lassen sich die gewonnenen Erkenntnisse den jeweiligen Nutzern zuordnen.[726] Nicht zuletzt ist zu beachten, dass sich die Inhaltsdaten einer Email über die Email- und IP-Adresse den Kommunikationspartnern zurechnen lassen.[727]

Im Ergebnis ist festzuhalten, dass Email- und IP-Adressen die datenschutzrechtliche Relevanz nicht aus dem Grund abgesprochen werden kann, weil sie die Bagatellgrenze nicht überschreiten.[728]

(bb) Zusatzwissen und Relativität des Personenbezugs

Bisher wurde lediglich festgestellt, dass bestimmte Stellen die im Raum stehenden Daten einer konkreten Person zuordnen können, weil und soweit sie über die hierfür erforderlichen

---

[718] zur Möglichkeit der Verknüpfung von Informationen: 1. Kap. Teil 1 A. 4.
[719] BVerfGE 78, S. 77 ff., 84; *Starck* in v. Mangoldt/Klein/Starck, Art. 2 Abs. 1 GG, Rn. 114
[720] vgl.: 1. Kap. Teil 1 A. I. 4.
[721] vgl.: 1. Kap. Teil 1 A. I. 4.
[722] vgl.: 1. Kap. Teil 1 A. I. 4.; vgl. auch: *Bizer*, DuD 2003, S. 10; *Dammann* in Simitis, § 3 BDSG, Rn. 65; *Helfrich* in Hoeren/Sieber, 16.1, Rn. 32; *Ruess/Patzak*, RDV 2003, S. 167 ff., 170; *J. Weber*, DuD 2003, S. 625 ff., 627; vgl. auch: AG Darmstadt, MMR 2005, S. 634 ff., 635; LG Darmstadt, GRUR-RR, 173 ff.; BGH, Urteil vom 26.10.2006, III ZR 40/06
[723] vgl.: 1. Kap. Teil 1 A. I. 4.
[724] vgl.: 1. Kap. Teil 1 B. II. 3.
[725] BVerfGE 2006, S. 976 ff., 980; zustimmend: *I.Geis/E.Geis*, K & R 2006, S. 279 f., 280
[726] vgl. dazu soeben: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a)
[727] *Dammann* in Simitis, § 3 BDSG, Rn. 62
[728] so auch im Ergebnis: RegPräs. Darmstadt, MMR 2003, S. 213 ff., LG Darmstadt, MMR 2006, S. 330 ff.; vgl. dazu: BGH, Urteil vom 26.10.2006, III ZR 40/06; vgl. auch: AG Darmstadt, MMR 2005, S. 634 ff., 635; *Schaar*, Datenschutz im Internet, Rn. 168 ff.; *Terwangne/Louveaux*, MMR 1998, S. 452; *Tinnefeld/Ehmann/Gerling*, S. 284 f.; *Tinnefeld* in Roßnagel, 4.1., Rn. 21

Angaben verfügen. Die Informationen, die den Personenbezug herzustellen vermögen, werden Zusatzwissen genannt.[729] Es zeigt sich, dass die Bestimmbarkeit nicht allein von der Art der Information abhängt, sondern auch davon, welches Zusatzwissen dem Datenverwender zur Verfügung steht.[730] Der Begriff des Personenbezugs ist damit relativ, das bedeutet, dass dasselbe Datum für einen Datenverwender personenbezogen sein kann, während es für einen anderen, der nicht über das für die Bestimmbarkeit erforderliche Zusatzwissen verfügt, keinen Personenbezug aufweist.[731] Folglich kann hinsichtlich ein- und desselben Datums die Anwendbarkeit der Datenschutzgesetze für einen Datenverwender zu bejahen, für einen anderen hingegen zu verneinen sein.[732]

In Bezug auf Daten, die einen Rückschluss auf eine bestimmte Person nicht oder nur eingeschränkt zulassen, wird in der juristischen Literatur zwischen anonymen[733] und pseudonymen[734] Daten unterschieden.[735] Die entsprechenden Maßnahmen, welche die Zuordnung der Daten ausschließen oder erschweren sollen, werden Anonymisieren bzw. Pseudonymisieren genannt, vgl. § 3 Abs. 6 und Abs. 6 a) BDSG.
Das Pseudonymisieren zeichnet sich im Vergleich zum Anonymisieren dadurch aus, dass die Bestimmung des Betroffenen erschwert werden soll, indem der Name oder das Identifikationsmerkmal durch ein Kennzeichen ersetzt wird, vgl. § 3 Abs. 6 a) BDSG, während in § 3 Abs. 6 BDSG hinsichtlich des Begriffs des Anonymisierens nicht von einem Ersetzen, sondern lediglich allgemein vom Verändern der Daten die Rede ist.
Email-Adressen, die keinen Namensbestandteil des Inhabers enthalten, ersetzen dessen Namen durch ein Kennzeichen, nämlich die Zeichen, aus denen sich die Adresse zusammensetzt. Hierdurch wird für Dritte die Bestimmung erschwert, jedoch kann diejenige Stelle, die das Pseudonym zugewiesen hat, den Betroffenen über das Kennzeichen und die hierzu abgespeicherten Daten identifizieren.[736] Dies ist grundsätzlich der Email-Service-Provider oder in einem Unternehmen der Netzwerkadministrator.
Im Fall von IP-Adressen verbirgt sich die Identität des Anschlussinhabers ebenfalls hinter einem Kennzeichen, nämlich einer vierstelligen Nummer,[737] das Dritten die Identifikation erschwert. Dem Internet-Service-Provider bzw. Netzwerkadministrator, der die Adresse

---

[729] *Dammann* in Simitis, § 3 BDSG, Rn. 29 ff.; *Dittrich/Schlörer*, DuD 1987, S. 31; *Louis*, a.a.O., Rn. 26; *Roßnagel/Scholz*, MMR 2000, S. 725; *Schaar*, Datenschutz im Internet, Rn. 168 ff.; *Terwagne/Louveaux*, MMR 1998, S. 452 ff.; *Tinnefeld* in Roßnagel, 4.1., Rn. 28; *Tinnefeld/Ehmann/Gerling*, S. 280 f.; vgl. auch: *Hammerbacher*, DVBl. 1978, S. 422 f.

[730] *Dammann* in Simitis, § 3 BDSG, Rn. 29 ff.; *Dittrich/Schlörer*, DuD 1987, S. 30 ff.; *Gola/Schomerus*, § 3 BDSG, Rn. 9; *Louis*, a.a.O., Rn. 26; *Roßnagel/Scholz*, MMR 2000, S. 723; *Schaar*, Datenschutz im Internet, Rn. 168 ff.; *Schulz*, Die Verwaltung 1999, S. 163; *Terwagne/Louveaux*, MMR 1998, S. 452 ff.; *Tinnefeld* in Roßnagel, 4.1., Rn. 22; *Tinnefeld/Ehmann/Gerling*, S. 280 f.

[731] *Dammann* in Simitis, § 3 BDSG, Rn. 35; *Gola/Schomerus*, § 3 BDSG, Rn. 9; *Louis*, a.a.O., Rn. 26; *Roßnagel/Scholz*, MMR 2000, S. 723; *Schulz*, Die Verwaltung 1999, S. 163; *Tinnefeld/Ehmann/Gerling*, S. 280; *Tinnefeld* in Roßnagel, 4.1., Rn. 22

[732] *Dammann* in Simitis, § 3 BDSG, Rn. 35; *Gola/Schomerus*, § 3 BDSG, Rn. 9; *Louis*, a.a.O., Rn. 26; *Roßnagel/Scholz*, MMR 2000, S. 723; *Schulz*, Die Verwaltung 1999, S. 163; *Tinnefeld/Ehmann/Gerling*, S. 280; *Tinnefeld* in Roßnagel, 4.1., Rn. 22; zur Entsprechung der Definitionen des Begriffs der personenbezogenen Daten im BDSG und der DSRL:
Roßnagel/Scholz, MMR 2000, S. 722; *Schaar*, Datenschutz im Internet, Rn. 148; *Saeltzer*, DuD 2004, S. 221; *Tinnefeld* in Roßnagel, Handbuch Datenschutzrecht, 4.1., Rn. 18

[733] Das Wort anonym steht im Griechischen für „namenlos“/“dem Namen nach unbekannt“, vgl. *Roßnagel/Scholz*, MMR 2000, S. 723; *Tinnefeld* in Roßnagel, 4.1., Rn. 23

[734] Pseudonym steht im Griechischen für „falscher Name“/“Deckname“, vgl. *Roßnagel/Scholz*, MMR 2000, S. 723; *Tinnefeld* in Roßnagel, 4.1., Rn. 23

[735] *Roßnagel/Scholz*, MMR 2000, S. 721; *Schaar*, Datenschutz im Internet, Rn. 155 ff.

[736] vgl.: 1. Kap. Teil 1 B. II. 3.

[737] vgl.: 1. Kap. Teil 1 A. I. 3.

zugewiesen hat, ist dieser Rückschluss hingegen möglich.[738] IP-Adressen sind daher ebenso wie Email-Adressen Pseudonyme.[739]

Auch bei Pseudonymen ist im Hinblick auf den Personenbezug darauf abzustellen, ob sie unter Zuhilfenahme von Zusatzwissen dem Betroffenen zugeordnet werden können.[740]
Für die Frage nach einem Personenbezug der fraglichen Informationen kommt es demnach entscheidend darauf an, ob das Zusatzwissen, das die Identifikation des Adressinhabers ermöglicht, bei demjenigen vorhanden ist, der die Daten erhebt, verwendet oder nutzt. Folglich ist hier zu klären, wer als verarbeitende Stelle anzusehen ist und ob das Zusatzwissen bei der fraglichen Person oder dem Rechtsträger präsent ist. Ist dies der Fall, so sind die Daten personenbezogen, andernfalls wird zu überprüfen sein, ob und in welchem Umfang das Zusatzwissen Dritter bei der Frage nach der Bestimmbarkeit der betroffenen Person Berücksichtigung finden kann.
Verantwortliche Stelle im Sinne des BDSG ist nach § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder die Tätigkeit durch andere im Auftrag vornehmen lässt. Die im Wege der richtlinienkonformen Auslegung zu berücksichtigende DSRL definiert den für die Verarbeitung Verantwortlichen als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Art. 2 lit. d) S. 1 DSRL.[741] Das maßgebliche Kriterium für die Bestimmung des für die Verarbeitung Verantwortlichen ist die Entscheidungsverantwortung über die Zwecke und Mittel der Verarbeitung, Art. 2 lit. d) DSRL.[742] Demnach ist derjenige Rechtsträger verantwortliche Stelle, der die Daten in eigener Verantwortlichkeit verarbeitet oder verarbeiten lässt.[743] Dies ist hier der Entscheidungsträger, der den Einsatz der entsprechenden Filtersoftware veranlasst, also der Provider oder LAN-Verwalter des Empfängers. Durch die beim Empfängerserver eingesetzte Filtersoftware werden Daten, die in der vom Absender versandten Email enthalten sind, überprüft. Über das Zusatzwissen hinsichtlich der in der Email enthaltenen Daten des Absenders verfügt, wie dargestellt,[744] sein Provider oder Netzwerkadministrator. Dieser wird in der Regel nicht mit der verantwortlichen Stelle im Sinne des BDSG, nämlich dem Provider oder Administrator auf Empfängerseite identisch sein, es sei denn Absender und Empfänger sind ausnahmsweise Kunden desselben Providers. Danach wird das für die Herstellung des Personenbezugs erforderliche Zusatzwissen zwar bei bestimmten Dritten vorliegen, in aller Regel jedoch nicht bei dem für den Filtereinsatz Verantwortlichen. Somit stellt sich die Frage, in welchem Umfang Zusatzwissen, das Dritten zur Verfügung steht, bei der Frage nach der Bestimmbarkeit einer Person durch die verantwortliche Stelle zu berücksichtigen ist. Dabei könnten Einschränkungen einerseits in personeller Hinsicht zu machen sein (α), andererseits kommt eine Beschränkung anhand des Beschaffungsaufwandes, der Wahrscheinlichkeit der Identifikation oder auf das auf legalem Weg erhältlichen Zusatzwissens in Betracht (β).

---

[738] vgl.: 1. Kap. Teil 1 A. I. 3. a) und b)
[739] *Tinnefeld* in Roßnagel, 4.1., Rn. 30; für dynamisch vergebene IP-Adressen: *Roßnagel/Scholz*, MMR 2000, S. 725
[740] *Dammann* in Simitis, § 3 BDSG, Rn. 61; *Roßnagel/Scholz*, MMR 2000, S. 725
[741] vgl. zur richtlinienkonformen Auslegung: 2. Kap. Teil 2 A. I. 1. aa) (2) (a) (aa)
[742] *Brühann* in Roßnagel, 2.4., Rn. 20; *Dammann/Simitis*, DSRL Kommentar, Art. 2 DSRL, Rn. 11; *Ehmann/Helfrich*, Art. 2 DSRL, Rn. 44
[743] *Gola/Schomerus*, § 3 BDSG, Rn. 48, 50
[744] vgl.: 1. Kap. Teil 1 A. I. 3.; 1. Kap. Teil 1 B. I.

(α) Beschränkung des Personenkreises?

Der Kreis derjenigen Personen und Rechtsträger, deren Zusatzwissen bei der Frage nach der Bestimmbarkeit des Betroffenen durch die für die Verarbeitung verantwortliche Stelle zu berücksichtigen ist, könnte anhand bestimmter Kriterien zu beschränken sein. Hier werden unterschiedliche Auffassungen vertreten.

Nach einer Auffassung soll der Personenbezug lediglich dann entfallen, wenn eine Identifizierung der betroffenen Person definitiv ausscheidet.[745] Umgekehrt ausgedrückt ist danach von einem Personenbezug stets auszugehen, wenn eine Identifizierung möglich ist.[746] Auf die Art oder Weise der Ermittlung oder Eingrenzung der betroffenen Person soll es nach der genannten Auffassung nicht ankommen.[747] Die Bestimmbarkeit ist auch dann gegeben, wenn sich die Identität des Betroffenen erst durch komplizierte Verarbeitungsvorgänge ermitteln lässt.[748] Letztlich bedeutet dies, dass sämtliche von Dritten erlangbare Informationen bei der Frage nach der Bestimmbarkeit der betroffenen Person miteinzubeziehen sind, ohne den Kreis derjenigen, deren Zusatzwissen bei der Frage nach der Bestimmbarkeit zu berücksichtigen ist, zu beschränken.
Eine andere Auffassung lässt nur die Berücksichtigung des Zusatzwissens zu, das sich die verantwortliche Stelle aus allgemein zugänglichen Quellen bzw. mit Mitteln beschafft, die ihm normalerweise zur Verfügung stehen.[749]
Des Weiteren wird vertreten, dass der Personenbezug stets dann zu bejahen sei, wenn die Möglichkeit bestehe, die Information der Person zuzuordnen.[750] Das Erkennen eines Personenbezugs durch einen imaginären oder potentiellen Dritten aufgrund eines ihm zur Verfügung stehenden Zusatzwissens soll jedoch nicht ausreichen, um den Personenbezug herzustellen.[751] Anders, als nach der erstgenannten Auffassung, ist also nicht entscheidend, ob eine Identifizierung definitiv ausscheidet, sondern es ist nur das von existenten und dem für die Verarbeitung Verantwortlichen bekannten oder zumindest erreichbaren Dritten erlangbare Zusatzwissen zu berücksichtigen.
Schließlich wird vertreten, dass nur das bei solchen Dritten vorhandene Zusatzwissen miteinzubeziehen sei, die eine Verbindung rechtlicher, institutioneller oder sonstiger Art zu dem für die Verarbeitung Verantwortlichen haben.[752]

Gegen eine Einschränkung des zu berücksichtigenden Zusatzwissens sprechen Wortlaut und Entstehungsgeschichte der DSRL, die auf das BDSG im Wege der richtlinienkonformen Auslegung Einfluss nimmt.[753] Nach Art. 2 lit. a) DSRL ist eine Person dann bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, wobei die Richtlinie keine Beschränkung auf ein bestimmtes Zusatzwissen enthält. Der Wortlaut der Richtlinie legt also nahe, keine Beschränkung auf bestimmte Personen vorzunehmen. Auch Erwägungsgrund Nr. 26 S. 3 DSRL spricht für diese Auslegung. Danach ist die Richtlinie nur dann unanwendbar, wenn Daten derartig anonymisiert sind, dass die betroffene Person nicht mehr identifiziert werden kann. Dies bedeutet, dass der Schutz der Daten durch die DSRL nach dem Willen des Richtliniengebers nur dann entfallen soll, wenn die Identifizierung unmöglich ist.

---

[745] *Gallwas*, § 2 BDSG, Rn. 8
[746] *Gallwas*, § 2 BDSG, Rn. 8
[747] *Gallwas*, § 2 BDSG, Rn. 8
[748] *Gallwas*, § 2 BDSG, Rn. 8
[749] *Schulz*, Die Verwaltung 1999, S. 163; *Saeltzer*, DuD 2004, S. 222
[750] *Hammerbacher*, DVBl. 1978, S. 424
[751] *Hammerbacher*, DVBl. 1978, S. 424
[752] *Terwangne/Louveaux*, MMR 1998, S. 452
[753] vgl.: 2. Kap. Teil 2 A. I. 1. aa) (2) (a) (aa)

Daneben spricht auch die Entstehungsgeschichte der Datenschutzrichtlinie für einen Einbezug sämtlichen Zusatzwissens. Hier ist zu beachten, dass anfangs geplant war, eine Regelung im Hinblick auf anonymisierte Daten in die Richtlinie aufzunehmen. Von der Vorschrift sollte der Fall erfasst sein, dass Daten derart verändert werden, dass die darin enthaltenen Angaben nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Arbeitskraft, Kosten und Zeit einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.[754] Allerdings wurde auf die Aufnahme einer Norm über anonymisierte Daten schließlich mit dem Argument verzichtet, dass eine derartige Vorschrift mit zunehmender technischer Entwicklung sinnentleert würde.[755] Im Bereich der elektronischen Datenverarbeitung sei der Begriff des unverhältnismäßig großen Aufwands, der ursprünglich in der Definition des Begriffs der Anonymisierung verwendet wurde, fehl am Platz.[756] Aus dem Umstand, dass die zunächst vorgesehene Regelung über anonymisierte Daten nicht in die Richtlinie aufgenommen wurde, lässt sich schließen, dass es für die Frage nach dem Personenbezug nicht darauf ankommt, bei welchen Dritten sich die verarbeitende Stelle das Zusatzwissen beschafft.

Für eine Einbeziehung sämtlichen Zusatzwissens spricht des Weiteren, dass durch eine personelle Beschränkung letztlich diejenigen Personen privilegiert würden, die Zusatzwissen durch längere Recherche oder auf undurchsichtigen Kanälen erhalten. Diese müssten die Datenschutzgesetze nicht beachten, während diejenigen verantwortlichen Stellen, die sich ihr Wissen aus allgemein zugänglichen Quellen oder mit normalerweise zur Verfügung stehenden Mitteln von bekannten Dritten beschaffen, hierzu verpflichtet wären.

Schließlich wird nicht immer abschätzbar sein, ob das erforderliche Zusatzwissen nur beim Provider oder auch bei Dritten vorhanden ist. So kann eine legale oder illegale Weitergabe durch die Person oder Personengruppe erfolgt sein, die ursprünglich über das Zusatzwissen verfügte. Gerade im Internet kann der Datenaustausch jederzeit grenzüberschreitend und in Sekundenschnelle erfolgen. Insofern würde eine Sichtweise, die nur bestimmte Personengruppen in den Kreis derjenigen einbezieht, deren Zusatzwissen bei der Frage nach dem Personenbezug zu berücksichtigen ist, hier zu kurz greifen.
Die Weitergabe von Zusatzwissen erfolgt in erster Linie an staatliche Behörden. Diesen stehen Auskunftsansprüche auf Mitteilung der „hinter“ einer IP- oder Email-Adresse stehenden Person gegen diejenigen Stellen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken aus § 113 Abs. 2 TKG bzw. §§ 100 g, h StPO zu.[757] Telefonverbindungsdaten müssen auch an Verfassungsschutzbehörden weitergegeben werden, § 2 Abs. 1 S. 3 G 10. Allerdings werden Provider nicht nur von staatlichen Stellen, sondern auch von Privatpersonen als Informationsquelle in Anspruch genommen. So entschied das AG Düsseldorf, dass ein Kind von einem Mobilfunktreiber Auskunft über die Daten eines Anschlussinhabers verlangen kann, wenn die betreffende Person als Kindsvater in Betracht

[754] *Ehmann/Helfrich*, Art. 2 DSRL, Rn. 23
[755] *Ehmann/Helfrich*, Art. 2 DSRL, Rn. 25 f.
[756] ABlEG Nr. C 159 vom 17.06.1991, S. 40; vgl. auch: *Ehmann/Helfrich*, Art. 2 DSRL, Rn. 25 f.
[757] Dabei ist im Bereich dynamischer IP-Adressen umstritten, welche der genannten Vorschriften als Rechtsgrundlage heranzuziehen ist. Die überwiegende Rechtsprechung wendet § 113 Abs. 1 TKG an und verlangt demgemäß keinen richterlichen Beschluss, LG Stuttgart, NStZ-RR 2005, S. 218; LG Stuttgart, MMR 2005, S. 624; LG Hamburg, MMR 2005, S. S. 712; LG Würzburg, NStZ-RR 2006, S. 46 f.. Nach einem Teil der Literatur und Rechtsprechung greifen hingegen die §§ 100 g, h StPO ein mit der Folge des Erfordernisses eines richterlichen Beschlusses, vgl. LG Ulm, MMR 2004, S. 187; LG Bonn, Beschluss vom 21.05.2004, Az.: 31 Qs 65/04; LG Hannover, Bschluss vom 08.08.2004, Az.: 46 Qs 138/04; *Bär*, MMR 2002, S. 358 ff.; *Gnirck/Lichtenberg*, DuD 2004, S. 598 ff.; *Köbele*, DuD 2004, S. 609 f.; *Kühling*, K & R 2004, S. 109; vgl. auch: Sankol, MMR 2006, S. 361 ff. Statische IP- und Email-Adressen sind Bestandsdaten und unterfallen demnach § 113 Abs. 1 TKG, vgl. *Hoeren*, Recht der Access-Provider, Rn. 192; *Ders*., wistra 2005, S. 4

kommt.[758] Das TMG sieht eine Ausweitung der Befugnisse der Provider zur Auskunfterteilung dahingehend vor, dass nun auch zur Durchsetzung der Rechte am geistigen Eigentum Auskunft erteilt werden darf.[759]
Hinzu kommt, dass in Zukunft Verbindungsdaten über einen Zeitraum von mindestens sechs Monaten gespeichert werden müssen, wie sich aus der Richtlinie zur Vorratsdatenspeicherung ergibt.[760] Durch die längere Speicherdauer erhöht sich die Gefahr einer Auskunfterteilung, einer Weitergabe oder eines illegalen Abrufs der gespeicherten Informationen. Zwar ist die Richtlinie in datenschutzrechtlicher Hinsicht bedenklich.[761] Denn es steht ein Verstoß gegen das sowohl auf gemeinschaftsrechtlicher, als auch auf nationaler Ebene geschützte Rechtes auf Privatleben im Raum,[762] dessen Verhältnismäßigkeit angesichts der Möglichkeit des in den USA praktizierten so genannten quick-freeze-Verfahrens[763] zweifelhaft ist.[764] Daneben ist die Verfassungsmäßigkeit der Maßnahme auch deshalb fraglich, weil die umfangreichen Datensammlungen die Gefahr bergen, dass durch Data-Mining-Techniken[765] Profilbildungen erleichert werden und daneben nachvollzogen werden kann, wer wann mit wem wie lange kommuniziert hat.[766] Auf Ebene des nationalen Verfassungsrechts kommt hinzu, dass das Bundesverfassungsgericht von einem grundsätzlichen Verbot der Vorratsdatenspeicherung ausgeht, sofern keine Datenerhebung für statistische Zwecke betroffen ist.[767] Allerdings sind die Mitgliedstaaten trotz der bestehenden Bedenken dazu verpflichtet, die Richtlinie in nationales Recht umzusetzen, soweit diese nicht zuvor für nichtig erklärt wird.[768]
Demnach ist aufgrund geänderter rechtlicher Rahmenbedingungen ein Anstieg des Gefährdungspotentials hinsichtlich der Weitergabe bzw. der Erhebung von Verbindungsdaten durch Dritte bei Providern zu verzeichnen. Dieser Umstand legt es nahe, der Gefährdung für die informationelle Selbstbestimmung durch eine weite Ausdehnung des Anwendungsbereichs der Datenschutzgesetze entgegenzuwirken.

Im Übrigen ist der technischen Entwicklung Rechnung zu tragen. Diese gewinnt hier in zweifacher Hinsicht Bedeutung. Einerseits bewirkt sie, dass das Erheben des für die Bestimmbarkeit erforderlichen Zusatzwissens durch Dritte immer einfacher und schneller möglich wird und insofern die Wahrscheinlichkeit der Zuordnung der Daten zu einer bestimmten Person steigt. Andererseits sind die Folgen der Kenntnis bestimmter Daten, wie der Email- und IP-Adresse gravierender, als dies vor der Entwicklung der dargestellten Methoden der Datenauswertung[769] der Fall war.
Die Tatsache, dass die Identifikation einfacher und schneller möglich ist und damit immer wahrscheinlicher wird, ist Folge der Entwicklung der Informationstechnologie, insbesondere des Internet. Diese bewirkt, dass schneller, grenzüberschreitend weltweit auf eine Fülle von Informationen zugegriffen werden kann. Hinzu kommt die Möglichkeit des

[758] AG Düsseldorf, RDV 2005, S. 176 f.
[759] *Gola/Klug*, NJW 2006, S. 2456; *Seichter*, WRP 2006, S. 398
[760] vgl.: 1. Kap. Teil 1 A. I. 3. b)
[761] kritisch: *Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland*, DuD 2004, S. 603 ff.; *Westphal*, EuZW 2006, S. 555 ff.
[762] vgl. hierzu: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)
[763] Hierunter ist das Einfrieren von Daten im Verdachtsfall zu verstehen, d.h. das Speichern wird von den TK-Anbietern bzw. Providern veranlasst, wenn das entsprechende behördliche Begehren richterlich genehmigt oder kraft Gesetzes erlaubt ist. Das Prinzip wurde auch in die Cybercrime-Konvention mitaufgenommen und als „fast freeze-quick thaw" bezeichnet, vgl. *Art. 29 Datenschutzgruppe*, WP 99, S. 4.
[764] *Westphal*, EuZW 2006, S. 558
[765] vgl.: 1. Kap. Teil 1 A. I. 4. c)
[766] *Westphal*, EuZW 2006, S. 559
[767] BVerfGE 65, S. 1 ff., 47; BVerfG, NJW 2006, S. 1939 ff., 1943
[768] EuGH, Slg. 1994, S. I-2646, Rn. 48 - Kommission/BASF; EuGH, EuR 2005, S. 757 f., Rn. 19 - Kommission/Griechenland; *Jarass*, DVBl. 1995, S. 960
[769] vgl.: 1. Kap. Teil 1 A. I. 4. c); 1. Kap. Teil 1 B. II. 3.

Informationsabrufs mittels des „finger"-Befehls[770] und die Tatsache, dass sich Nutzer teilweise -ohne hiervon Kenntnis zu haben- selbst identifizieren.[771] Bisweilen erfolgt auch eine Identifikation des Nutzers über den Browser, den er benutzt.[772] Es zeigt sich also, dass die Wahrscheinlichkeit der Identifikation des Nutzers mit fortschreitender technischer Entwicklung stetig ansteigt.
Auch die Folgen der Kenntnis bestimmter Daten, wie der Email- und IP-Adresse werden angesichts des Fortschritts der Internettechnologie gravierender. Dies wird erkennbar, wenn man sich die Möglichkeit vor Augen führt, unter Einsatz von Cookie-Dateien[773] und der Mittel des Data-Mining[774] Nutzerprofile zu erstellen. Clickstream-Techniken ermöglichen es sogar, das gesamte Klickverhalten eines Nutzers nachzuvollziehen.[775] Bei Kenntnis der Email-Adresse können unter den oben genannten Voraussetzungen Kommunikationsprofile erstellt und daraus weitere Rückschlüsse gezogen werden,[776] die teilweise sogar Schlussfolgerungen auf den Inhalt der Nachricht zulassen.[777]
Im Internet ist nach alledem eine faktische Anonymität, wie sie das Bundesverfassungsgericht im Bereich des Rechts auf informationelle Selbstbestimmung fordert,[778] nicht mehr gegeben,[779] es sei denn der Nutzer trifft spezielle Vorkehrungen.[780] Insofern ist die Befürchtung des Gerichts, dass auch unerhebliche Informationen in Verknüpfung mit anderen Daten Rückschlüsse auf den Betroffenen, seinen Lebensweg und seine Persönlichkeit ermöglichen,[781] dort mittlerweile Realität. Auch deshalb sollte von einem weiten Anwendungsbereich der Datenschutzgesetze ausgegangen werden. Bereits vor geraumer Zeit stellte Gallwas fest, dass der Fortschritt der Verarbeitungstechnik zu einer Ausweitung des Kreises derjenigen Angaben führt, die den Begriff der personenbezogenen Daten erfüllen.[782] Dieser Auffassung ist aufgrund der genannten Argumente zuzustimmen.

Im Ergebnis ist danach bei der Frage nach dem Personenbezug sämtliches verfügbares Zusatzwissen zu berücksichtigen, ohne den Kreis der Dritten, von denen dieses erlangt werden kann, in irgendeiner Art und Weise zu beschränken. Demnach fallen Diensteanbieter und Unternehmen, die Email-Filtersoftware einsetzen, nicht deshalb aus dem Anwendungsbereich der Datenschutzgesetze, weil sie über das zur Herstellung des Personenbezugs erforderliche Zusatzwissen nicht verfügen.

---

[770] vgl.: 1. Kap. Teil 1 A. I. 4. a)
[771] vgl.: 1. Kap. Teil 1 A. I. 4. b)
[772] vgl.: 1. Kap. Teil 1 A. I. 4. b)
[773] vgl.: 1. Kap. Teil 1 A. I. 4. c)
[774] vgl.: 1. Kap. Teil 1 A. I. 4. c)
[775] vgl.: 1. Kap. Teil 1 A. I. 4. c)
[776] vgl.: 1. Kap. Teil 1 B. II. 3.
[777] vgl. hierzu: 2. Kap. Teil 2 A. I. 1. aa) (2) (a) (aa)
[778] BVerfG, NJW 1987, S. 2805 ff., 2807; BVerfG, NJW 1988, S. 962 ff., 963
[779] ebenso: *Rötzer* in Bäumler, a.a.O., S. 27; *Schaar*, Datenschutz im Internet, Rn. 174; *Wiese* in Bäumler, a.a.O., S. 9 ff.; a.A.: *Schmitz* in Hoeren/Sieber, 16.4, Rn. 51; *Ders*. in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 26; vgl. auch: *Roßnagel/Pfitzmann/Garstka*, DuD 2001, S. 253 ff., 254; zu den Ermittlungsmöglichkeiten unter Heranziehung der IP-Adresse: *Dietrich*, NJW 2006, S. 809 ff.; http://www.ip-adress.com/ (letzter Abruf: 29.04.2007)
[780] vgl. etwa das Projekt AN.ON - Anonymität Online der Technischen Universität Dresden und der Universität Regensburg, abrufbar unter: http://anon.inf.tu-dresden.de/ (letzter Abruf: 29.04.2007); zu Annonymisierungsdiensten: *Diaz/Claessens/Preneel*, DuD 2003, S. 143 ff.; *Köpsell/Miosga*, DuD 2005, S. 403 ff.; *Spiekermann*, DuD 2003, S. 150 ff.; zu Verschlüsselungsverfahren: *Gerling*, DuD 1997, S. 197 ff.; zur Anonymisierung von Emails: *Möller*, DuD 2000, 267 ff.; *Ders*., DuD 2000, S. 344 ff.
[781] BVerfGE 65, S. 1 ff., 45
[782] *Gallwas*, § 2 BDSG, Rn. 8

(β) Beschränkung anhand des Beschaffungsaufwandes, der Wahrscheinlichkeit der Identifikation oder Berücksichtigung nur des auf legalem Weg erhältlichen Zusatzwissens ?

Das zu berücksichtigende Zusatzwissen könnte anhand bestimmter Kriterien einzuschränken sein. In der Literatur wurden verschiedene Ansätze entwickelt.
Eine Auffassung beschränkt das Zusatzwissen nach dem Grad der Wahrscheinlichkeit der Identifikation[783] oder dem Beschaffungsaufwand,[784] der für die Zuordnung zu betreiben ist. Teilweise wird bei der Frage nach der Bestimmbarkeit nur das auf legalem Wege erhältliche Zusatzwissen miteinbezogen.[785]
Demgegenüber ist ein Personenbezug nach anderer Auffassung nur dann abzulehnen, wenn eine Identifizierung definitiv ausscheidet.[786]

Für die beiden erstgenannten Auffassungen lässt sich anführen, dass angesichts der im Internet bei Vernachlässigung des Beschaffungsaufwandes stets möglichen Identifizierung der Person eine Grenze gesetzt werden muss, um ein Ausufern des Anwendungsbereichs der Datenschutzgesetze zu vermeiden.[787] Zudem wird argumentiert, es sei wünschenswert, durch die Ausnahme anonymer Daten vom Anwendungsbereich der Datenschutzgesetze oder zumindest bestimmter datenschutzrechtlicher Vorschriften einen Anreiz zur Anonymisierung von Daten zu schaffen.[788] Dieses Ziel könne jedoch nicht erreicht werden, wenn sämtliche anonymen Daten, unabhängig von der Wahrscheinlichkeit der (Re-)Identifizierung als personenbezogen angesehen würden.[789] Auch der Wortlaut des § 3 Abs. 6 und Abs. 6 a) BDSG spricht auf den ersten Blick für die beiden erstgenannten Auffassungen, denn das Gesetz lässt es für eine Anonymisierung ausreichen, dass die Einzelangabe nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können, § 3 Abs. 6 BDSG. Pseudonymisieren bedeutet nach § 3 Abs. 6 a) BDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Es sprechen jedoch auch gewichtige Gründe gegen eine Beschränkung des zu berücksichtigenden Zusatzwissens anhand der vorgenannten Kriterien.
Aus dem Wortlaut des § 3 Abs. 6 BDSG lässt sich kein Argument in Bezug auf die Frage gewinnen, ob im Rahmen der Bestimmbarkeit ein gewisser Aufwand für die Identifizierung oder eine festgesetzte Wahrscheinlichkeit der Herstellung des Personenbezugs zu fordern ist. Auch eine Begrenzung auf legal erlangtes Zusatzwissen lässt sich daraus nicht ableiten. Denn die Vorschrift sagt noch nichts darüber aus, ob anonyme Daten personenbezogen sein können. Nach den allgemeinen Grundsätzen zur Bestimmbarkeit, die bereits dargestellt wurden,[790] ist davon auszugehen, dass nur in der ersten Alternative des § 3 Abs. 6 BDSG der Personenbezug entfällt, während in der zweiten Alternative die Qualität der Daten als personenbezogen

[783] *Roßnagel/Scholz*, MMR 2000, S. 723; *Tinnefeld* in Roßnagel, 4.1., Rn. 22; *Tinnefeld/Ehmann/Gerling*, S. 280
[784] *Dammann* in Simitis, 1. Aufl., § 2 BDSG, Rn. 36 f.; *Gola/Schomerus*, § 3 BDSG, Rn. 9; *Ruess/Patzak*, RDV 2003, S. 174; *Schmitz* in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 24; *Schulz*, Die Verwaltung 1999, S. 137 ff., 163 f.
[785] *Tinnefeld* in Roßnagel, 4.1., Rn. 22
[786] *Gallwas*, § 2 BDSG, Rn. 8; *Hammerbach*, DVBl. 1978, S. 422; ähnlich: *Brühann* in Grabitz/Hilf, A 30, Rn. 8; *Louis*, a.a.O. Rn. 26
[787] *Roßnagel/Scholz*, MMR 2000, S. 726; *Ruess/Patzak*, RDV 2003, S. 174
[788] *Roßnagel/Scholz*, MMR 2000, S. 726
[789] *Roßnagel/Scholz*, MMR 2000, S. 726
[790] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2)

erhalten bleiben kann.[791] Gleiches gilt im Hinblick auf das Pseudonymisieren von Daten, das in § 3 Abs. 6 a) BDSG geregelt ist. Sofern hier eine Zuordnungsregel vorhanden ist, liegen personenbeziehbare Daten vor.[792]

Des Weiteren ist das nationale Recht richtlinienkonform auszulegen. Hier kann auf die oben dargestellte Argumentation verwiesen werden, aus der sich ergibt, dass es für die Frage nach dem Personenbezug nicht darauf ankommt, bei welchen Dritten sich die verarbeitende Stelle das Zusatzwissen beschafft und welcher Aufwand hierzu erforderlich ist.[793]
Ebenso greift auch das bereits genannte Argument dahingehend, dass nicht diejenigen Personen und Personengruppen privilegiert werden sollen, die Zusatzwissen durch längere Recherche oder auf undurchsichtigen Kanälen erhalten.[794] Eine solche Privilegierung würde aber insbesondere die Beschränkung auf legal erhaltenes Zusatzwissen bewirken.
Des Weiteren gewinnt das aufgrund der Veränderung der rechtlichen und technischen Rahmenbedingungen gestiegene Gefährdungspotential für personenbezogene Daten Bedeutung.[795] Um diesem Umstand Rechnung zu tragen, sollten die Vorschriften so ausgelegt werden, dass ein immer weiteres faktisches Aushöhlen der Rechtsposition des Betroffenen verhindert wird.
Die gegenteilige Auffassung würde darüber hinaus dazu führen, dass im Einzelfall eine Prognose zu stellen wäre, wie wahrscheinlich die Identifizierung bzw. welcher Beschaffungsaufwand dazu erforderlich ist. Dies ist äußerst schwierig.[796] Im Übrigen steht nicht fest, ab welcher Wahrscheinlichkeit bzw. unter Heranziehung welchen Beschaffungsaufwandes von einem Personenbezug ausgegangen werden kann, was letztlich zu einer nicht unerheblichen Rechtsunsicherheit führt.

Das Argument, durch die Ausnahme anonymer Daten vom Anwendungsbereich der Datenschutzgesetze oder zumindest bestimmter datenschutzrechtlicher Vorschriften solle ein Anreiz zur Anonymisierung geschaffen werden, dieses Ziel könne aber nicht erreicht werden, wenn sämtliche anonymen Daten, unabhängig von der Wahrscheinlichkeit der (Re-) Identifizierung als personenbezogen angesehen würden,[797] ist ebenfalls nicht zwingend. Dagegen lässt sich anführen, dass die Absonderung und getrennte Speicherung der zur Identifikation geeigneten Daten nur eine spezifische Sicherungsmaßnahme darstellt, aber das BDSG nach den allgemeinen Grundsätzen zur Bestimmbarkeit nicht unanwendbar macht, so lange eine Wiederzusammenführung möglich ist.[798] Insofern besteht jedenfalls kein Anreiz zur Anonymisierung von Daten, so lange ihre Zusammenführung mit dem Identifikationsmerkmal noch erfolgen kann.

Daher ist davon auszugehen, dass Daten, bei denen die Möglichkeit der (Re-)Identifizierung besteht, als personenbezogen zu qualifizieren sind. Demnach sind sowohl statische,[799] als

---

[791] *Dammann* in Simitis, § 3 BDSG, Rn. 196; a.A.: *Brühann* in Grabitz/Hilf, A 30, Rn. 8; *Hornung*, DuD 2004, S. 429; *Roßnagel/Scholz*, MMR 2000, S. 726
[792] *Dammann* in Simitis, § 3 BDSG, Rn. 217; a.A.: Roßnagel/Scholz, MMR 2000, S. 724 f.
[793] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a) (bb) (α)
[794] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a) (bb) (α)
[795] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a) (bb) (α)
[796] zur Berechnung der (Re-)Identifikation: *Paaß*, DuD 1985, S. 97 ff.; *Dittrich/Schlörer*, DuD 1987, S. 30 ff.
[797] *Roßnagel/Scholz*, MMR 2000, S. 726
[798] *Dammann* in Simitis, § 3 BDSG, Rn. 34; *Gola/Schomerus*, § 3 BDSG, Rn. 43 f.; *Tinnefeld* in Roßnagel, 4.1, Rn. 25; zur Bestimmbarkeit: 2. Kap. Teil 2 A. I. 1. a) aa) (2)
[799] für einen Personenbezug statischer IP- Adressen: *Eichler*, K & R 1999, S. 79; *Gundermann*, K & R 2000, S. 227; *Ihde*, CR 2000, S. 417; *Schmitz* in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 27; *Wohlgemuth/Gerloff*, S. 28; im Ergebnis auch: *Art. 29 Datenschutzgruppe*, WP 37, S. 17; differenzierend: *Helfrich* in Hoeren/Sieber, 16.1, Rn. 31 f.; *Schulz*, Die Verwaltung 1999, S. 166

auch dynamische[800] IP-Adressen personenbezogene Daten. Dasselbe gilt für Email-Adressen[801] und im Text und Betreff der betroffenen Email enthaltene Informationen, die unter Zuhilfenahme von Zusatzwissen einer bestimmten Person zugeordnet werden können. Über die Email- und IP-Adresse können auch Inhaltsinformationen und sonstige in der Email enthaltene Daten dem Betroffenen zugeordnet werden.[802]

(b) Maßnahmen hinsichtlich nicht oder lediglich kurzfristig automatisch zwischengespeicherter Daten

Soeben wurde dargestellt, dass im Inhalt einer Email personenbezogene Daten enthalten sein können und auch den IP- und Email-Absenderadressen, die Bestandteil des Email-Headers sind, ein Personenbezug zukommt.[803] Dabei wurde davon ausgegangen, dass die betreffenden Informationen nicht nur vorübergehend gespeichert sind. Da bei der Frage nach dem Personenbezug von Daten stets auf den jeweiligen Verarbeitungskontext abzustellen ist,[804] könnte etwas anderes in Bezug auf solche Daten gelten, die nicht oder lediglich kurzfristig zum Zweck der Email-Filterung zwischengespeichert, jedoch nicht dauerhaft festgehalten werden. Dies ist der Fall, wenn schon vor vollständigem Eingang bzw. der dauerhaften Speicherung auf dem Empfängerserver Emails durch die Filtersoftware auf bestimmte werbetypische Merkmale durchsucht werden.

Dabei spielt es für die Anwendung des Datenschutz- und des Datenschutzstrafrechts keine Rolle, ob Daten allein automatisch verarbeitet werden, vgl. § 1 Abs. 2 Nr. 3 BDSG. Entscheidend könnte hier allerdings sein, dass die Überprüfung des Inhalts und der elektronischen Kontaktinformationen durch den Einsatz von Software erfolgt, welche die Daten während des Vorgangs keiner bestimmten Person zuordnet.[805] Auch finden im Rahmen der Spamfilterung keine dauerhaften Speichervorgänge statt, mit der Folge, dass nach dem Filtereinsatz keine anderen Informationen festgehalten bleiben, als dies der Fall wäre, wenn keine Filtersoftware eingesetzt würde.[806] Es finden also lediglich Zwischenspeichervorgänge statt, die bei der Datenübermittlung ständig durchgeführt werden, jedoch letztlich nicht zu einer dauerhaften Fixierung der Daten auf einem Speichermedium führen.[807] Somit erfolgt weder während des Einsatzes der entsprechenden Software eine Zuordnung von Informationen zu einer konkreten Person und kann dies auch nicht später nachgeholt werden, da keine in der Email enthaltenen Informationen gespeichert bleiben. Es stellt sich daher die Frage, ob der von der Filtermaßnahme Betroffene bestimmt oder bestimmbar ist.

Der Zweck des Datenschutzrechts besteht darin, den Einzelnen davor zu schützen, durch den Umgang mit ihn betreffenden personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt zu werden, § 1 Abs. 1 BDSG. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG das Recht auf informationelle Selbstbestimmung

---

[800] *Eicheler*, K & R 2000, S. 79; im Ergebnis auch: *Art. 29 Datenschutzgruppe*, WP 37, S. 17; *Schaar*, Datenschutz im Internet, Rn. 174 f.; aA.: *Gundermann*, K & R 2000, S. 227; *Ihde*, CR 2000, S. 417; *Roßnagel/Scholz*, MMR 2000, 727; *Schmitz* in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 26 f.

[801] *Dammann* in Simitis, § 3 BDSG, Rn. 62; *Ruess/Patzak*, RDV 2002, S. 172; einschränkend: *Engels/Eimterbäumer*, K & R 1998, 197; *Schmitz* in Hoeren/Sieber, 16.4, Rn. 56 ; *Ders*. in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 29

[802] *Dammann* in Simitis, § 3 BDSG, Rn. 62

[803] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a)

[804] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2)

[805] vgl.: 1. Kap. Teil 2 A. II.

[806] vgl.: 1. Kap. Teil 2 A. II.

[807] vgl.: 1. Kap. Teil 2 A. II.

abgeleitet.[808] Dieses ist neben dem durch Art. 10 Abs. 1 GG geschützten Telekommunikationsgeheimnis Schutzgut des Datenschutzrechts.[809] Die informationelle Selbstbestimmung beinhaltet das Recht des Betroffenen, selbst über die Preisgabe und Verwendung ihn betreffender personenbezogenen Daten zu bestimmen und ist Grundlage der allgemeinen und bereichsspezifischen Datenschutzgesetzgebung.[810] Die Maßgaben, die für das Recht auf informationelle Selbstbestimmung entwickelt wurden,[811] gelten auch für das Fernmeldegeheimnis, das der Verarbeitung personenbezogener Daten in seinem Anwendungsbereich[812] Grenzen setzt.[813]

Fraglich ist allerdings, ob das Schutzgut des Datenschutzrechts hier überhaupt betroffen wird. Dabei sind die bereits gennannten technischen Grundlagen zu beachten.[814] Danach werden die Daten während des Filtervorgangs keiner bestimmten Person zugeordnet. Auch finden keine dauerhaften Speichervorgänge statt mit der Folge, dass der von den Filtermaßnahmen Betroffene nach dem Filtereinsatz im Hinblick auf in der Email enthaltene Daten nicht anders steht, als dies der Fall wäre, wenn keine Filtersoftware eingesetzt worden wäre. Insofern entsteht durch den Filtereinsatz nicht die Gefahr, dass die Zuordnung zu der Person später nachgeholt oder die Inhalte aufgrund des Filtervorgangs von natürlichen Personen gelesen werden. Demnach werden die Kommunikationspartner nicht in ihrem Recht beeinträchtigt, über die Preisgabe und Verwendung sie betreffender personenbezogener Daten zu bestimmen. Eine Gefahr für das Recht von Absender und Empfänger auf informationelle Selbstbestimmung besteht somit nicht.[815] Der Schutzzweck des Datenschutzrechts greift folglich nicht ein. Daher besteht keine Notwendigkeit den Filtervorgang als Verarbeitung personenbezogener Daten zu qualifizieren.

Auch aus dem Wortlaut des § 3 Abs. 1 BDSG ergibt sich nichts anderes. Dieser stellt darauf ab, ob Einzelangaben über bestimmte oder bestimmbare Personen betroffen sind. Wie eben gezeigt, werden die Kommunikationspartner jedoch während des Vorgangs der Email-Filterung nicht bestimmt und sind diese weder zu diesem Zeitpunkt, noch später anhand von Daten, die durch den Filtervorgang entstehen, bestimmbar. Auch aus dem Wortlaut des Art. 2 Abs. 2 DSRL, der hier im Wege der richtlinienkonformen Auslegung zu berücksichtigen ist,[816] ergibt sich nichts anderes. Die Vorschrift sieht solche Personen als bestimmbar an, die direkt oder indirekt identifiziert werden können. Dies ist jedoch, wie soeben dargestellt, aufgrund des blossen technischen Durchsuchens des Inhalts und Headers der Email nicht der Fall.

Für die Ausnahme der Überprüfungsmaßnahmen aus dem Anwendungsbereich des Datenschutzrechts spricht auch der hinter dem in § 1 Abs. 3 Nr. 1 BDSG 1990 enthaltenen Ausschluss temporärer Dateien aus dem Anwendungsbereich des BDSG stehende Gedanke.

---

[808] BVerfGE 65, S. 1 ff.
[809] *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 8 ff.; *Roßnagel/Pfitzmann/Garstka*, DuD 2001, S. 256; *Tinnefeld/Ehmann/Gerling*, S. 138 ff., 234 f.
[810] BVerfGE 65, S. 41 ff.; *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 8 ff.; *Helfrich* in Hoeren/Sieber, Kap. 16.1, Rn. 17; *Kunig* in v. Münch/Munig, Art. 2 GG, Rn. 38; *Roßnagel/Pfitzmann/Garstka*, DuD 2001, S. 256; *Schmitz* in Spindler/Schmitz/Geis, Einf. TDDSG, Rn. 2; *Simitis* in Ders., Einl., Rn. 27 ff.; *Tinnefeld/Ehmann/Gerling*, S. 138 ff.
[811] grundlegend: BVerfGE 65, S. 1 ff., 44 ff., 54
[812] vgl.: 2. Kap. Teil 2 A. I. 2. c) bb)
[813] BVerfGE 100, S. 313 ff., 359; BVerfGE 110, S. 33 ff., 53; BVerfG, NJW 2006, S. 976 ff., 979 f.
[814] vgl.: 1. Kap. Teil 2 A. II.
[815] im Ergebnis ebenso: *Art. 29 Datenschutzgruppe*, WP 37, S. 31, 38, die davon ausgeht, dass Emails auf bestimmte inhaltliche Merkmale überprüft werden dürfen, wenn dies automatisch erfolgt und die Nachrichten selbst wenn sie positiv gescannt wurden, niemandem gezeigt werden.
[816] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a) (aa)

Die Vorschrift normierte eine Einschränkung des Gesetzes für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung wieder gelöscht wurden. Für diese sollten lediglich die §§ 5 und 9 BDSG 1990 gelten, welche das Datengeheimnis und bestimmte zu treffende technische und organisatorische Maßnahmen betrafen. Den weiteren Anforderungen und Beschränkungen des BDSG unterfielen temporäre Dateien nicht. Als temporär wurden solche Dateien angesehen, die ausschließlich aus verarbeitungstechnischen Gründen und vorübergehend erstellt und nach der verarbeitungstechnischen Nutzung automatisch wieder gelöscht wurden.[817] Sofern also der Verarbeitungsvorgang „diskret" ablief, das bedeutet nicht an der Benutzeroberfläche der Ein- oder Ausgabegeräte sichtbar wurde, sondern intern blieb, wurde davon ausgegangen, dass Zwischen- und Hilfsdateien keine Gefahr für das allgemeine Persönlichkeitsrecht des Betroffenen darstellen.[818] Hintergrund der Aufnahme der Regelung in das BDSG 1990 war demnach die mangelnde Persönlichkeitsrelevanz der genannten Dateien.[819] Dies zeigt sich auch, wenn man berücksichtigt, dass Voraussetzung der Ausnahmeregelung war, dass keine Kenntnisnahme durch natürliche Personen erfolgen konnte. So sollte die Privilegierung in dem Fall nicht eingreifen, in dem die Ergebnisse der Hilfs- oder Zwischendatei ausgedruckt, angezeigt oder sonst festgehalten wurden, ebenso dann, wenn ein Zugriff von außen auf die Datei erfolgte, auch wenn dies nur zu Zwecken der Wartung geschah.[820] Denn in diesem Fall war der Grund der Ausnahmeregelung, nämlich der geringe Gefährdungsgrad interner Zwischendateien für das Persönlichkeitsrecht des Betroffenen, nicht mehr gegeben.[821] Die Aufnahme der Vorschrift in das BDSG 1990 zeigt somit, dass solche Vorgänge aus dem Anwendungsbereich des Datenschutzrechts fallen sollten, die mangels Kenntnisnahmemöglichkeit Dritter keine Gefahr für das allgemeine Persönlichkeitsrechts des Betroffenen darstellten.

Auf den ersten Blick lässt sich allerdings aus der Tatsache, dass die Ausnahmevorschrift des § § 1 Abs. 3 Nr. 1 im BDSG 1990 enthalten war, kein Argument herleiten, da die Norm im BDSG 2000 nicht mehr mitaufgenommen wurde. Allerdings ist zu berücksichtigen, dass diese lediglich deshalb aus dem BDSG 2000 gestrichen wurde, weil der Gesetzgeber sich in Umsetzung des Art. 3 Abs. 1 DSRL hierzu verpflichtet sah, da die Richtlinie eine entsprechende Einschränkung des Anwendungsbereichs nicht vorsieht.[822] Jedoch greift auch die Datenschutzrichtlinie nur dann ein, wenn dies zum Schutz der Grundrechte und Grundfreiheiten und insbesondere zum Schutz der Privatsphäre erforderlich ist, wie sie in Art. 8 EMRK sowie den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannt ist, Art. 1 Abs. 1 DSRL, Erwägungsgründe Nr. 10, 33 DSRL. Insofern waren in Umsetzung der Richtlinie nur solche Einschränkungen des Anwendungsbereichs zu beseitigen, die Gefährdungen oder Verletzungen der Privatsphäre betrafen. Demnach entfällt der hinter der ursprünglichen Ausnahme stehende Gedanke, dass Tatbestände, in denen eine Grundrechtsgefährdung ausgeschlossen ist, nicht dem Anwendungsbereich des BDSG zuzuordnen sind, durch die Aufhebung der Vorschrift nicht. Dieser Grundgedanke wurde auch bereits vor der ausdrücklichen Aufnahme der genannten Regelung im BDSG 1990 vertreten. Schon damals wurde die Auffassung geäußert, dass die genannten Dateien vom Anwendungsbereich des BDSG ausgenommen waren.[823]

---

[817] *Dörr/Schmidt*, 1. Aufl., § 1 BDSG, Anm. zu Abs. 3; *Geiger* in Simitis, 4. Aufl., § 1 BDSG, Rn. 231
[818] *Dörr/Schmidt*, 1. Aufl., § 1 BDSG, Anm. zu Abs. 3; *Geiger* in Simitis, 4. Aufl., § 1 BDSG, Rn. 230, 232, 234
[819] *Dörr/Schmidt*, 1. Aufl., § 1 BDSG, Anm. zu Abs. 3; *Geiger* in Simitis, 4. Aufl., § 1 BDSG, Rn. 230, 232, 234
[820] *Auernhammer*, § 1 BDSG, Rn. 19; *Geiger* in Simitis, 4. Aufl., § 1 BDSG, Rn. 238 f.; *Schaffland/Wiltfang*, § 1 BDSG, Rn. 23
[821] *Auernhammer*, § 1 BDSG, Rn. 19; *Geiger* in Simitis, 4. Aufl., BDSG 1990, Rn. 240
[822] BR-Drs. 461/00, S. 76; BT-Drs. 14/4329, S. 31; BT-Drs. 14/5793, S. 60
[823] *Geiger* in Simitis, 4. Aufl., § 1 BDSG, Rn. 230

Einzubeziehen sind danach lediglich solche Vorgänge, bei denen eine Gefährdung oder Verletzung des informationellen Selbstbestimmungsrechts zu befürchten ist. Der Grundgedanke, solche Umgangsweisen mit Daten aus dem Anwendungsbereich des Datenschutzrechts auszunehmen, die keine Gefährdung der Grundrechte der Betroffenen bewirken, gilt demnach nach wie vor. Zwar zeigte er sich besonders anschaulich in § 1 Abs. 3 Nr. 1 BDSG 1990, jedoch gilt der Gedanke, der hinter dieser Vorschrift stand, wie gezeigt, auch nach dessen Streichung fort.

Im Ergebnis lässt sich daher festhalten, dass ein Personenbezug der von der Filtermaßnahme betroffenen Daten im maßgeblichen Zeitpunkt des Zugriffs auf in der Email enthaltene Informationen zu verneinen ist. Dies gilt selbst dann, wenn die überprüften Daten normalerweise unter Zuhilfenahme entsprechender Zusatzinformationen der betroffenen Person zugeordnet werden könnten.[824] Ein Personenbezug kommt den Daten demnach erst dann zu, wenn sie nicht lediglich kurzfristig zwischengespeichert sind oder sogleich wieder gelöscht werden. Dann sind sie auch natürlichen Personen zugänglich, die auf legalem oder illegalem Weg auf sie Zugriff nehmen und die unter Zuhilfenahme bestimmten Zusatzwissens den Personenbezug herstellen und hieraus Schlussfolgerungen ziehen können.
Danach verstößt das Überprüfen eingehender Nachrichten auf werbebezogene Merkmale durch den Einsatz von Filtersoftware selbst dann nicht gegen das allgemeine oder bereichsspezifische Datenschutzrecht, wenn von der Maßnahme Daten oder Inhalte betroffen sind, die unter Zuhilfenahme bestimmter Zusatzinformationen der betroffenen Person zugeordnet werden könnten. Gleiches gilt für den Vorgang des Löschens, Markierens oder Umleitens eingehender Emails und der darin enthaltenen Daten, sofern die Maßnahmen vor Speichern der Nachricht auf dem Empfänger-Server oder in der Mailbox des Empfängers stattfinden.

Folge für den Filtereinsatz ist danach, dass Maßnahmen bereits dann keine personenbezogenen Daten betreffen, wenn eine rein technische Überprüfung eingehender Nachrichten erfolgt und keine in der Email enthaltenen Daten dauerhaft festgehalten werden. Filtermaßnahmen, die vor dem endgültigen Speichern von Daten auf dem Empfängerserver ansetzen sind danach datenschutzrechtlich unbedenklich. Etwas anderes gilt, wenn Daten betroffen sind, die endgültig oder für eine nicht nur unerhebliche Dauer gespeichert sind.

bb) Erhebung, Verarbeitung oder Nutzung

Eben wurde dargestellt, dass Maßnahmen, die durch die Filtersoftware durchgeführt werden, noch bevor die Emails endgültig auf dem Empfängerserver gespeichert sind, keine personenbezogenen Daten erfassen.[825] Solche Vorgänge sind das Untersuchen eingehender Emails sowie das Umleiten, Blockieren und Löschen der Nachricht noch vor einem nicht lediglich kurzfristigen Speichern auf dem Empfängerserver.[826] Die genannten Verarbeitungsschritte stellen demnach bereits keinen Umgang mit personenbezogenen Daten dar, weshalb sie unabhängig davon datenschutzrechtlich zulässig sind, ob sie den im BDSG niedergelegten Begriffen der Datenerhebung, -verarbeitung oder -nutzung unterfallen.[827]

---

[824] so im Ergebnis auch: *Art. 29 Datenschutzgruppe*, WP 118, S. 6, die zwar datenschutzrechtliche Fragestellungen aufwirft, es allerdings ausreichen lässt, wenn der Inhalt der Emails automatisch erfolgt und über den Adressaten hinaus keinem Dritten bekanntgegeben wird; die Datenschutzgruppe stellt in dem Arbeitspapier auch auf Art. 8 EMRK ab und merkt an, eine Überwachung und damit ein Eingriff in die Privatsphäre liege nur dann vor, wenn ein Dritter Zugang zum Inhalt oder den Verbindungsdaten erhält; vgl. auch: *Spindler/Ernst*, CR 2004, S. 440

[825] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[826] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[827] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

Ist die Filtersoftware hingegen so eingestellt, dass bereits gespeicherte Informationen bestimmten Verarbeitungsschritten unterzogen werden, so sind -wie bereits dargestellt wurde- möglicherweise im Inhalt der Email enthaltene Informationen als personenbezogene Daten zu qualifizieren.[828] Den im Header enthaltenen Email- und IP-Adressen der Kommunikationspartner kommt ebenfalls ein Personenbezug zu.[829] Über diese personenbezogenen Daten können weitere in der Email enthaltene Informationen den Betroffenen zugeordnet werden.
Spamfilter sind -wie oben gezeigt- teilweise so eingestellt, dass positiv gescannte Nachrichten zwar in der Empfänger-Mailbox gespeichert, jedoch nach einer gewissen Zeitspanne oder bei Überschreiten eines gewissen Datenvolumens wieder gelöscht werden.[830] Es stellt sich die Frage, ob in dem Entfernen der Email und damit der darin enthaltenen personenbezogenen Informationen ein datenschutzrechtlich relevanter Verarbeitungsvorgang zu sehen ist. Darin könnte ein dem Verbot mit Erlaubnisvorbehalt des § 4 Abs. 1 BDSG unterfallendes Löschen gemäß § 3 Abs. 4 S. 1, S. 2 Nr. 5 BDSG zu sehen sein. Löschen ist nach § 3 Abs. 4 S. 2 Nr. 5 BDSG das Unkenntlichmachen gespeicherter personenbezogener Daten. Wird eine Email aus der Mailbox entfernt, so werden damit auch die darin enthaltenen personenbezogenen Daten unkenntlich. Ein Löschen ist daher zu bejahen.

b) Einwilligung des Betroffenen oder Eingreifen eines Erlaubnistatbestands

Fraglich ist, wie eben dargestellt, ob das Löschen von Emails und damit der darin enthaltenen personenbezogenen Daten zulässig ist. Dies wäre der Fall, wenn die Einwilligung aller Betroffener vorläge oder eine Rechtsvorschrift dies erlauben oder anordnen würde, vgl. § 4 Abs. 1 BDSG.[831]

Betroffener ist nach § 3 Abs. 1 BDSG derjenige, über dessen persönlichen oder sachlichen Verhältnisse durch die Einzelangaben eine Aussage getroffen wird, hier also grundsätzlich Absender und Empfänger der Email in Bezug auf die Headerdaten oder gegebenenfalls ein Dritter im Hinblick auf im eigentlichen Text der Email enthaltene Informationen. Hieraus folgt bereits, dass eine Einwilligung sämtlicher Betroffener in die Löschung der Daten grundsätzlich nicht vorliegen wird, da zumindest der Absender damit nicht einverstanden sein wird, weil er die Email mit dem Ziel abschickt, dass der Empfänger sie auch erhält. Auch Dritte werden ihre Einwilligung zur Löschung grundsätzlich nicht erklärt haben.

Allerdings ist § 35 Abs. 2 S. 1 BDSG zu beachten. Die Vorschrift beinhaltet eine das allgemeine Verarbeitungsverbot aufhebende Zulässigkeitsregelung für das Löschen personenbezogener Daten.[832]

aa) Anwendbarkeit des § 35 Abs. 2 S. 1 BDSG

Fraglich ist allerdings, ob diese Norm hier Anwendung findet oder ob sie aufgrund der Subsidiarität des BDSG, die in § 1 Abs. 3 BDSG angeordnet ist, verdrängt ist. Vorrangige bereichsspezifische Datenschutzregelungen könnten sich einerseits aus den §§ 11 ff. TMG

[828] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2)
[829] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a)
[830] vgl.: 2. Kap. Teil 2 A. II.
[831] vgl. auch: § 12 Abs. 1 TMG, der allerdings nur solche Erlaubnistatbestände zulässt, die im TMG enthalten sind oder aber sich ausdrücklich auf Telemedien beziehen.
[832] *Bergmann/Möhrle/Herb*, § 35 BDSG, Rn. 55; *Dix* in Simitis, § 35 BDSG, Rn. 19; *Gola/Schomerus*, § 35 BDSG, Rn. 10

ergeben, andererseits aus den §§ 91 ff. TKG. Vorfrage ist, ob der Anwendungsbereich der genannten Gesetze hier überhaupt eröffnet ist.

Bevor das TMG in Kraft trat, war umstritten, ob ein Email-Dienstleister Telekommunikationsdienste im Sinne des § 3 Nr. 24 TGK oder Teledienste gemäß § 2 Abs. 1 TDG[833] erbringt. Die Abgrenzung war entscheidend für die Frage, ob das TKG oder die vor dem Inkrafttreten des TMG anwendbaren Vorschriften des TDG bzw. des TDDSG[834] Anwendung fanden. Unter den Begriff des Teledienstes fielen alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt waren und denen eine Übermittlung mittels Telekommunikation zugrunde lag, § 2 Abs. 1 TDG. Telekommunikation ist demgegenüber nach der nach wie vor gültigen Vorschrift des § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Telekommunikationsdienste sind nach § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdiensten in Rundfunknetzen. Teilweise fanden die Vorschriften beider Gesetze parallel Anwendung, wenn verschiedene Informationsschritte erfasst waren, die unterschiedlich zu beurteilen waren.[835]
Hinsichtlich der Abgrenzung der Gesetze in Bezug auf Email-Dienste wurden zwei Auffassungen vertreten. Nach einer Auffassung waren Email-Dienste vollständig als Telekommunikationsdienst anzusehen und folglich den Regelungen des TKG untergeordnet.[836] Nach anderer Auffassung waren im Bereich der Email-Kommunikation zwei verschiedene Ebenen zu unterscheiden und zwar zum einen die reine Übertragung der Nachricht, die als Telekommunikationsdienst eingeordnet wurde, und zum anderen die so genannte Anwendungsebene, die als Teledienst anzusehen sein sollte.[837] Der Vorgang der Übertragung der Email erfasste dabei nur die durch das TCP/IP-Protokoll realisierte Kommunikation.[838] Zur Anwendungsebene sollte hingegen die Darstellung und Verwaltung von Emails und der Vorgang des Versendens durch den Absender bzw. des Abrufs durch den Empfänger gehören.[839]
Während danach nach der ersten Auffassung der Vorgang bis einschließlich des Abrufs der Email als Telekommunikationsdienst anzusehen war,[840] unterfiel nach der anderen Auffassung dem Begriff lediglich die reine Übermittlung, also der Zeitraum ab dem Absenden bis zum Eintreffen auf dem Server des Empfängers, während der Vorgang des Absendens, das

---

[833] Gesetz über die Nutzung von Telediensten v. 22.07.1997, BGBl. I, S. 1870; Art. 5 des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer Geschäftsverkehr-Vereinheitlichungsgesetz, BGBl. 2007, I, S. 179 ff.) sah als Zeitpunkt des Inkrafttretens des TMG und des Außerkrafttretens des TDG und des TDDSG den Tag vor, an dem der Neunte Rundfunkänderungsstaatsvertrag der Länder in Kraft trat; der Tag des Inkrafttretens des TMG und Außerkrafttretens des TDG und des TDDSG war der 01.03.2007.
[834] Gesetz über den Datenschutz bei Telediensten vom 22. 07.1997, BGBl. I, S. 1870
[835] *Engel-Flechsig*, RDV 1997, S. 59 ff., 61
[836] *Ernst*, Vertragsgestaltung im Internet, Rn. 576; *Kieper*, DuD 1998, S. 584 f.; *Möller*, DuD 2000, S. 345; *Schaar*, Datenschutz im Internet, Rn. 248; *Spindler/Ernst*, CR 2004, S. 439; im Ergebnis auch: *Königshofen*, DuD 2001, S. 86; *Mengel*, BB 2004, S. 2014; *Moos* in Kröger/Gimmy, S. 411 ff., 420; *Schmidl*, MMR 2005, S. 344
[837] OLG Hamburg, MMR 2000, S. 611 ff.; *Schmitz* in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 14; *Ders*., MMR 2000, S. 616
[838] *Schmitz* in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 14; *Wuermeling/Felixberger*, CR 1997, S. 233
[839] OLG Hamburg, MMR 2000, S. 613 f.; *Schmitz* in Spindler/Schitz/Geis, § 1 TDDSG, Rn. 14
[840] *Ernst*, Vertragsgestaltung im Internet, Rn. 576; *Kieper*, DuD 1998, S. 584 f.; *Möller*, DuD 2000, S. 345; *Schaar*, Datenschutz im Internet, Rn. 248; *Spindler/Ernst*, CR 2004, S. 439; im Ergebnis auch: *Königshofen*, DuD 2001, S. 86; *Mengel*, BB 2004, S. 2014; *Moos* in Kröger/Gimmy, S. 411 ff., 420; *Schmidl*, MMR 2005, S. 343 ff., 344

Verwalten der Email auf dem Empfänger-Server und der Abruf durch den Adressaten als Teledienst zu qualifizieren sein sollte.[841]
Demnach fand nach beiden Auffassungen im Hinblick auf Maßnahmen, die eingehende Nachrichten betrafen das TKG Anwendung. Zu unterschiedlichen Ergebnissen kamen die Auffassungen demnach im Hinblick auf Maßnahmen, die bereits in die Mailbox des Empfängers eingestellte Nachrichten betrafen. Nach der ersten Ansicht war der gesamte Vorgang bis zum Abruf durch den Empfänger als Telekommunikation anzusehen, mit der Folge, dass das TKG auch hier Anwendung finden konnte. Nach der zweitgenannten Auffassung war hier nicht mehr der bloße Übermittlungsvorgang mittels TCP/IP[842] betroffen, sondern die Anwendungsebene, was dazu führte, dass der Provider bzw. das Unternehmen insofern einen Teledienst erbrachte.
Gegen die Aufspaltung des Vorgangs im Sinne der zweitgenannten Auffassung sprach dabei, dass der Kommunikationsvorgang mit dem Einstellen der Nachricht in die Mailbox noch nicht beendet ist, da der technische Bereich der Fernmeldeanlage dabei noch nicht verlassen wurde.[843] Das Speichermedium stellt einen Teil der Fernmeldeanlage dar, an die es angeschlossen ist.[844] Danach erfasst der Übermittlungsvorgang auch noch solche Nachrichten, die in einer Mailbox gespeichert aber noch nicht abgerufen sind.[845]
Der Schutz durch das Fernmeldegeheimnis endet erst in dem Moment, in dem die Nachricht sich im Herrschaftsbereich des Empfängers befindet und der Übertragungsvorgang beendet ist.[846] Vor diesem Zeitpunkt, also auch während des Zeitraums, während dessen die Nachricht in der Mailbox ruht und auf den Abruf wartet, ist sie jedoch gerade noch nicht im Herrschaftsbereich des Empfängers, da der Provider darauf zugreifen kann. Demnach ist der Vorgang der Telekommunikation zu diesem Zeitpunkt noch nicht beendet.[847] Die Nachricht befindet sich erst dann im alleinigen Herrschaftsbereich, wenn der Empfänger sie abgerufen hat.[848] In diesem Fall mag die Nachricht zwar auf dem Server des Empfängers gespeichert bleiben, allerdings besteht kein Unterschied mehr zu einer durch den Empfänger selbst angelegten Datei, da er es in der Hand hatte, die Email nach dem Lesen vom Server zu löschen.[849] Der Telekommunikationsvorgang ist folglich erst mit dem Abruf durch den Empfänger abgeschlossen.
Die Tatsache, dass die Übermittlung mit Einstellen der Nachricht in die Mailbox noch nicht beendet ist, spricht gegen eine Aufspaltung des einheitlichen Vorgangs und damit auch gegen eine Zuordnung der verschiedenen Übermittlungsphasen unter die Vorgaben verschiedener Gesetze.
Für die einheitliche Einordnung von Email-Diensten als Telekommunikationsdienstleistungen sprach auch, dass die Funktion des Übermittelns wesentlicher Bestandteil der Dienstleistung ist. Der Email-Server des Diensteanbieters dient lediglich als Zwischenspeicher, auf dem die Nachrichten abgelegt und automatisch auf Anfrage des Berechtigten an diesen weitergeleitet werden.[850] Da somit der Übermittlungsvorgang im Vordergrund steht, sprachen vor dem Inkrafttreten des TMG und dem damit verbundenen Außerkrafttreten von TDG und TDDSG

[841] OLG Hamburg, MMR 2000, S. 611 ff.; *Schmitz* in Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 14; Ders., MMR 2000, S. 616
[842] vgl.: 1 Kap. Teil 1 A. I. 3.
[843] BGH, NJW 1997, S. 1935; LG Hanau, NJW 1999, S. 3647; *Lührs*, wistra 1995, S. 19 f.
[844] BGH, NJW 1997, S. 1935; *Lührs*, wistra 1995, S. 19 f.
[845] BGH, NJW 1997, S. 1935; LG Hanau, NJW 1999, S. 3647; *Lührs*, wistra 1995, S. 19 f.
[846] BVerfG, NJW 2006, S. 976 ff.
[847] BGH, NJW 1997, S. 1935; LG Hanau, NJW 1999, S. 3647; *Sankol*, MMR 2006, Heft 12, S. XXX f.; *Ders*., JuS 2006, S. 700;
[848] BVerfG, NJW 2006, S. 978
[849] BVerfG, NJW 2006, S. 978 f.
[850] *Reg TP*, Mitteilung Nr. 11/2001, ABl. Reg TP 1/2001, S. 45; *Schaar*, Datenschutz im Internet, Rn. 266 f.

die besseren Argumente dafür, die gesamte Dienstleistung der Telekommunikation zuzuordnen.

Fraglich ist, ob die genannten Grundsätze auch für die Abgrenzung des TKG zum TMG gilt, welches das TDG und das TDDSG ersetzt.
Dabei könnten Unterschiede im Wortlaut von TMG und dem TKG dafür sprechen, beide Gesetze nebeneinander anzuwenden. Denn nach § 3 Nr. 24 TKG sind solche Dienste Telekommunikationsdienste, die „ganz oder überwiegend" in der Übertragung von Signalen über Telekommunikationsnetze bestehen. § 1 Abs. 1 TMG nimmt hingegen nur solche Vorgänge vom Anwendungsbereich des Telemediengesetzes aus, die „ganz" in der Übertragung von Signalen bestehen. Damit geht das Gesetz davon aus, dass ein Telekommunikationsdienst, der „überwiegend" in der Übertragung von Signalen besteht, zugleich Telekommunikations- und Telemediendienst sein kann.[851] Dies spricht dafür, dass in bestimmten Fällen auf einen Dienst sowohl das TKG, als auch das TMG Anwendung finden können.
Die Definition des Telekommunikationsdienstes in § 3 Nr. 24 TKG hat sich durch das Inkrafttreten des TMG nicht geändert. Insofern bleibt es bei der Aussage, dass Email-Dienste bis einschließlich der Phase des Abrufs der Email durch den Empfänger als Telekommunikationsdienst einzuordnen sind. Daneben könnte auch das TMG Anwendung finden. Hierfür spricht, dass vom Anwendungsbereich des Gesetzes lediglich solche Dienste ausgenommen werden, die „ganz" in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Allerdings werden durch Email-Dienstleister, wie eben dargestellt, nicht lediglich Signale übertragen, sondern auch andere Leistungen, wie das Verwalten und Vorhalten der Emails auch nach ihrem Abruf erbracht. Email-Dienste bestehen demnach nicht „ganz", sondern nur „überwiegend" in der Übertragung von Signalen über Telekommunikationsnetze.[852] Insofern unterfallen sie nunmehr auch dem TMG.[853]

Demnach könnten hier sowohl datenschutzrechtliche Vorschriften des TMG, als auch des TKG die allgemeine Zulässigkeitsregelung des § 35 Abs. 2 S. 1 BDSG verdrängen. Es stellt sich somit die Frage, ob die §§ 91 ff. TKG bzw. §§ 11 ff. TMG gegenüber § 35 Abs. 2 S. 1 BDSG speziell im Sinne des § 1 Abs. 3 S. 1 BDSG sind. Allerdings ist zu beachten, dass das BDSG nur insoweit subsidiär ist, als auf personenbezogene Daten anzuwendende Vorschriften des Bundes nach einem genauen inhaltlichen Vergleich eine abweichende Regelung für den exakt gleichen Sachverhalt treffen.[854] Das Fehlen der Deckungsgleichheit kann sich dabei vor allem daraus ergeben, dass ein Spezialgesetz nicht dieselben Phasen der Datenverarbeitung oder -nutzung oder aber unterschiedliche Datenarten betrifft.[855]
Sowohl in den datenschutzrechtlichen Vorschriften des TKG, als auch des TMG finden sich Vorschriften hinsichtlich des Löschens bestimmter Arten von personenbezogenen Daten. So ordnet § 13 Abs. 4 S. 1 Nr. 2 TMG an, dass der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden. Auch § 15 Abs. 8 S. 2 TMG enthält eine Löschungsverpflichtung des Diensteanbieters, die sich auf Daten bezieht, die dieser nach § 15 Abs. 8 S. 1 TMG gespeichert hat. § 15 Abs. 8 S. 1 TMG sieht vor, dass sofern dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vorliegen, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das

[851] BT-Drs. 16/3078, S. 17; *Hoeren*, NJW 2007, S. 802
[852] BT-Drs. 16/3078, S. 13
[853] BT-Drs. 16/3078, S. 13
[854] *Gola/Schomerus*, § 1 BDSG, Rn. 24; *Walz* in Simitis, § 1 BDSG, Rn. 170
[855] *Gola/Schomerus*, § 1 BDSG, Rn. 24; *Walz* in Simitis, § 1 BDSG, Rn. 170

Entgelt nicht oder nicht vollständig zu entrichten, er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorganges sowie die in Absatz 7 genannte Speicherfrist hinaus nur verwenden darf, soweit dies für Zwecke der Rechtsverfolgung erforderlich ist. Nach § 15 Abs. 8 S. 2 TMG hat der Diensteanbieter die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. § 35 Abs. 2 S. 1 BDSG nimmt jedoch weder auf personenbezogene Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung im Sinne des § 13 Abs. 4 S. 1 Nr. 2 TMG Bezug, noch sind solche Daten betroffen, die zum Zwecke der Rechtsverfolgung über die in § 15 Abs. 7 TMG genannte Speicherfrist hinaus gespeichert werden. Aufgrund des Subsidiaritätsvorbehalts des § 1 Abs. 3 BDSG findet § 35 Abs. 2 S. 1 BDSG demnach auf Vorgänge, die nicht mit den genannten Vorschriften des TMG deckungsgleich sind, weiterhin Anwendung. Ein solcher Vorgang ist auch das Löschen von Emails durch den Email-Diensteanbieter.
Die Anwendbarkeit des § 35 Abs. 2 S. 1 BDSG könnte jedoch deshalb entfallen, weil § 12 Abs. 1 TMG nur Vorschriften aus dem TMG sowie solche Normen als Erlaubnistatbestände zulässt, die sich ausdrücklich auf Telemedien beziehen. Insofern könnte die Anwendbarkeit eines allgemeinen Erlaubnistatbestandes aus dem BDSG hier ausgeschlossen sein. Allerdings finden die Vorschriften der §§ 11 ff. TMG bereits dann keine Anwendung wenn die Bereitstellung der Dienste im Dienst- oder Arbeitsverhältnis zu ausschließich beruflichen oder dienstlichen Zwecken erfolgt, § 11 Abs. 1 Nr. 1 TMG. Auch außerhalb dieser Konstellation ist zu beachten, dass gemäß § 11 Abs. 3 TMG soweit Telemedien betroffen sind, die „überwiegend“ in der Übertragung von Signalen über Telekommunikationsnetze bestehen lediglich einzelne Normen des im TMG verankerten Datenschutzes Anwendung finden. Es wurde bereits dargestellt, dass die Email-Übertragung überwiegend in der Übertragung von Signalen besteht.[856] Die Vorschrift des § 12 Abs. 1 TMG, die den Kreis der Erlaubnistatbestände einschränkt, findet auf Email-Dienste gemäß § 11 Abs. 3 TMG keine Anwendung und schließt folglich § 35 Abs. 2 S. 1 BDSG nicht aus.

Fraglich ist jedoch, ob die Norm durch Tatbestände des TKG verdrängt wird. Auch das TKG enthält Regelungen zur Löschungspflicht des Diensteanbieters für bestimmte personenbezogene Daten. So schreibt § 95 Abs. 3 TKG eine Löschungsverpflichtung hinsichtlich der Bestandsdaten, also der Daten des Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, § 3 Nr. 3 TKG, bei Vertragsbeendigung fest. § 96 Abs. 2 S. 2 TKG verpflichtet den Diensteanbieter zum Löschen gespeicherter Verkehrsdaten nach dem Ende der Verbindung. § 97 Abs. 3 S. 2 TKG beinhaltet eine Löschungsverpflichtung hinsichtlich Verkehrsdaten, die zum Zweck der Entgeltermittlung oder -abrechnung verwendet wurden. § 100 Abs. 3 S. 4 TKG enthält eine Löschungsverpflichtung hinsichtlich solcher Daten, die zum Aufdecken und Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen von Telekommunikationsnetzen und -diensten erhoben wurden, die jedoch Verbindungen betreffen, hinsichtlich derer kein Verdacht der Leistungserschleichung besteht. Keine der im TKG kodifizierten Löschungsverpflichtungen ist deckungsgleich mit § 35 Abs. 2 S. 1 BDSG. Weder werden Bestandsdaten aus Anlaß der Vertragsbeendigung gelöscht, § 95 Abs. 3 TKG, noch sind Verbindungsdaten betroffen, die nach dem Ende der Verbindung gelöscht werden oder die zum Zweck der Entgeltermittlung oder -abrechnung oder der Aufdeckung von Leistungserschleichungen erhoben oder verwendet wurden, §§ 96 Abs. 2 S. 2, 97 Abs. 3 S. 2, 100 Abs. 3 S. 4 TKG . Folglich findet § 35 Abs. 2 S. 1 BDSG Anwendung, soweit nicht die vorgenannten Tatbestände eingreifen, vgl. § 1 Abs. 3 S. 1 BDSG. Auf den Fall der Löschung

[856] vgl. auch: BT-Drs. 16/3078, S. 17; *Hoeren*, NJW 2007, S. 802

von Emails nebst der darin enthaltenen personenbezogenen Daten findet die Norm daher weiterhin Anwendung.

§ 35 Abs. 2 S. 1 BDSG ist somit nicht durch spezielle datenschutzrechtliche Vorschriften aus dem TMG oder dem TKG verdrängt.

bb) Voraussetzungen des § 35 Abs. 2 S. 1 BDSG

Nach § 35 Abs. 2 S. 1 BDSG ist das Löschen von Daten generell gestattet, sofern nicht gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, § 35 Abs. 2 S. 1 in Verbindung mit Abs. 3 Nr. 1 BDSG, oder Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden, § 35 Abs. 2 S. 1 in Verbindung mit Abs. 3 Nr. 2 BDSG.

Hier existieren jedoch keine gesetzlichen oder satzungsmäßigen Aufbewahrungsfristen. Auch enthalten die Nutzungsbedingungen der Email-Service-Provider im Allgemeinen keine Verpflichtung des Providers dahingehend, sämtliche eingehenden Emails, also auch solche, bei denen es sich ausweislich der Überprüfung um Spammails handelt, zuzustellen bzw. zu speichern. Vielmehr schließen die Provider in aller Regel die Haftung für den Fall des Löschens eingehender Emails durch den eingesetzten Spamfilter aus.[857] Auch Arbeitgeber werden grundsätzlich keine Verpflichtung zur Zustellung sämtlicher privater Emails übernehmen.[858] Insofern besteht keine vertragliche Aufbewahrungsfrist, die einem Löschen der Email bzw. der darin enthaltenen Daten entgegenstehen könnte.

§ 35 Abs. 2 S. 1 umfasst Fälle, in denen schutzwürdige Interessen des Betroffenen die Löschung verbieten. Fraglich ist, ob dies hier der Fall ist.
Sinn und Zweck der Erstreckung des in § 4 Abs. 1 BDSG enthaltenen Verbots mit Erlaubnisvorbehalt auf den Vorgang des Löschens ist es, die Funktion der Daten zu erhalten, bestimmte Kenntnisse zu vermitteln.[859] Das hier im Raum stehende Interesse der Kommunikationspartner betrifft allerdings nicht den Erhalt einzelner in der Email enthaltener personenbezogener Daten. Denn allenfalls steht dem Absender -zumindest in den Fällen, in denen legitime Nachrichten versandt werden- ein Interesse daran zu, dass die Email vollständig zugestellt und nicht vor Kenntnisnahme durch den Empfänger gelöscht wird. Ein spezielles Interesse daran, den Informationsgehalt der in Header und Inhalt der Nachrichten enthaltenen personenbezogenen Daten zu erhalten, ist jedoch nicht erkennbar. Der Absender wird grundsätzlich seine eigene Email- und IP-Adresse kennen, weshalb kein Interesse daran besteht, solche Daten zum Zweck der Sicherung des darin verkörperten Informationsgehalts zu speichern. Soweit im Inhalt enthaltene Informationen betroffen sind, ist zu beachten, dass das Original der Email in aller Regel beim Absender gespeichert bleibt,[860] so dass die Funktion der in der Email enthaltenen Daten, bestimmte Kenntnisse zu vermitteln, durch das Löschen nicht beeinträchtigt wird. Im Übrigen geht dem Betroffenen, also dem Absender, die Möglichkeit, die in der konkret versandten Version der Email enthaltene Daten zum Zweck der Kenntnisnahme zu verwenden, ohnehin durch das Versenden der Kopie verloren, da die versandte Kopie in diesem Fall seinem Einflussbereich entzogen wird. Das hier betroffene Interesse des Absenders ist danach darauf gerichtet, dass kein Eingriff in den

[857] vgl. etwa: *Hotmail*, Geschäftsbedingungen, abrufbar unter: http://privacy2.msn.com/tou/de-de/default.aspx (letzter Abruf: 29.04.2007); *Yahoo!*, Geschäftsbedingungen, abrufbar unter: http://de.docs.yahoo.com/info/utos.html (letzter Abruf: 29.04.2007)
[858] vgl. zu entsprechenden Empfehlungen: *Schmidl*, MMR 2005, S. 348; Tinnefeld/Ehmann/Gerling, S. 225
[859] *Dammann* in Simitis, § 3 BDSG, Rn. 173; *Tinnefeld/Ehmann/Gerling*, S. 304
[860] vgl.: 1. Kap. Teil 1 B. I.

Übermittlungsvorgang vorgenommen und die Email ordnungsgemäß aufbewahrt wird, bis der Adressat hiervon Kenntnis nimmt. Dieses Interesse ist unter Umständen durch Vorschriften außerhalb des BDSG geschützt, stellt jedoch wie eben gezeigt kein Schutzziel des BDSG dar. Auch ein der Löschung entgegenstehendes Interesse etwaiger Betroffener Dritter an der Speicherung ihrer personenbezogenen Daten gerade in der betreffenden Email ist nicht ersichtlich.

Aus den vorstehenden Ausführungen ergibt sich, dass § 35 Abs. 2 S. 1 in Verbindung mit Abs. 3 Nr. 2 BDSG der Löschung der entsprechenden Daten nicht entgegensteht. Demnach ist das Löschen von Emails datenschutzrechtlich nicht relevant. Dies bedeutet allerdings nicht, dass sich die Unzulässigkeit der fraglichen Maßnahmen nicht aus Rechtsvorschriften ergeben kann, die andere Interessen schützen, als das BDSG.

c) Zwischenergebnis

Die Überprüfung des Inhalts und der in einer Email enthaltenen elektronischen Kontaktinformationen durch den Einsatz von Filtersoftware begegnet datenschutzrechtlich keinen Bedenken. Auch das Blockieren, Löschen, Umleiten und Markieren positiv gescannter Nachrichten verstößt nicht gegen Vorschriften des BDSG.

2. Fernmeldegeheimnis

Den verschiedenen technischen Maßnahmen, die zur Identifizierung und Vermeidung unerbetener elektronischer Werbenachrichten vorgenommen werden, könnte das einfachgesetzliche in § 88 TKG normierte Fernmeldegeheimnis entgegenstehen.
Ein vorsätzlicher oder fahrlässiger Verstoß gegen das Fernmeldegeheimnis führt zu einem Schadensersatzanspruch des betroffenen Nutzers, § 44 Abs. 1 S. 1, 3 TKG.

Dem Fernmeldegeheimnis unterliegen gemäß § 88 Abs. 1 S. 1 TKG der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Den durch das Fernmeldegeheimnis verpflichteten Diensteanbietern ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen, § 88 Abs. 3 S. 1, Abs. 2 S. 1 TKG.

Ein Verstoß gegen das Fernmeldegeheimnis des § 88 TGK setzt einerseits voraus, dass das TKG auf die Erbringung von Email-Dienstleistungen Anwendung findet (a), andererseits muss derjenige, der die entsprechende Filtersoftware einsetzt, zum Adressatenkreis der Vorschrift gehören (b). Schließlich ist erforderlich, dass in dem Durchsuchen der Email auf werbebezogene Merkmale ein Verschaffen von Kenntnissen über den Inhalt oder die näheren Umstände der Telekommunikation im Sinne des § 88 Abs. 3 TKG zu sehen ist (c).

a) Anwendbarkeit des TKG

Eben wurde bereits dargestellt, dass Email-Dienstleister Telekommunikationsdienste erbringen.[861] Somit ist davon auszugehen, dass das TKG und damit auch das in § 88 Abs. 1, 3 TKG verankerte Fernmeldegeheimnis auf die Filtermaßnahmen Anwendung finden.

[861] vgl.: 2. Kap. Teil 2 A. I. 1. b) aa)

b) Adressatenkreis des Fernmeldegeheimnisses

§ 88 TKG steht dem Einsatz der Filtersoftware nur dann entgegen, wenn diejenigen Personen oder Personengruppen, die die entsprechenden Filterprogramme einsetzen, Adressaten des einfachgesetzlichen Fernmeldegeheimnisses sind.
Zur Wahrung des Fernmeldegeheimnisses ist nach § 88 Abs. 2 S. 1 TKG jeder Diensteanbieter verpflichtet. Demnach stellt sich die Frage, ob diejenigen Personen und Personengruppen, welche die Software einsetzen, als Diensteanbieter im Sinne des TKG zu qualifizieren sind.
Diensteanbieter ist nach § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung der Dienste mitwirkt. Unter dem geschäftsmäßigen Erbringen von Telekommunikationsdienstleistungen ist nach § 3 Nr. 10 TKG das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht zu verstehen. Email-Service-Provider bieten nachhaltig für Dritte Telekommunikationsdienstleistungen mit Gewinnerzielungsabsicht an. Gewinn wird hierbei - insbesondere über Werbung- auch dann erzielt, wenn die Telekommunikationsdienstleistung kostenfrei zur Verfügung gestellt wird. Demnach ist der Email-Service-Provider als Diensteanbieter im Sinne des TKG zu qualifizieren.
Aufgrund der Formulierung des § 3 Nr. 6 TKG sind nicht nur solche Personen oder Rechtsträger als Diensteanbieter zu qualifizieren, die Telekommunikationsleistungen gegenüber jedermann erbringen, sondern auch solche, die Leistungen für so genannte geschlossene Benutzergruppen bereitstellen, also nur für bestimmte Dritte anbieten. Dies ist beispielsweise der Fall, wenn in Betrieben Telekommunikationsanlagen von den dort beschäftigten Personen privat genutzt werden dürfen,[862] wenn also die Privatnutzung entweder ausdrücklich gestattet oder stillschweigend geduldet ist.[863] Die Qualifikation dieser Personengruppe als Dritte im Sinne des § 3 Nr. 10 TKG ergibt sich daraus, dass sie die Telekommunikationsdienste außerhalb ihrer betrieblichen Verpflichtung zu eigenen Zwecken nutzen können.[864] Ist die private Nutzung hingegen untersagt, so liegt kein Angebot von

[862] Die Gewährung der Privatnutzung im Arbeitsverhältnis kann hierbei entweder durch eine ausdrückliche vertragliche Vereinbarung erfolgen oder durch betriebliche Übung. Selbst wenn der Arbeitgeber die Privatnutzung untersagt, kann ein von der Nutzungsordnung abweichendes Nutzungsverhalten des Arbeitnehmers auf Grund betrieblicher Übung zum Inhalt des Arbeitsvertrages werden, wenn der Arbeitgeber hiervon Kenntnis hat und der Arbeitnehmer darauf vertrauen konnte, dass es auch in Zukunft bei diesem Zustand bleibt, *Elschner* in Hoeren/Sieber, 22.1, Rn. 45. Die Länge der Zeitspanne, die verstreichen muss, bis von einem entsprechenden Vertrauenstatbestand auszugehen ist, lässt sich nicht pauschal festlegen. In der Literatur wird von einem Zeitraum von einem halben bis zu einem Jahr ausgegangen, *Däubler*, K & R 2000, S. 325; *Elschner* in Hoeren/Sieber, 22. 1, Rn. 48; *Huber* in Weitnauer, Form. J.1, Anm. 6. Ob der Arbeitgeber dem Arbeitnehmer die Privatnutzung gestattet, steht grundsätzlich in seinem freien Ermessen, da ihm die Dispositionsbefugnis über die Arbeitsmittel zukommt, *Huber* in Weitnauer, Form. J.1, Anm. 5 b). Ausweislich der <kes>Microsoft Sicherheitsstudie 2004 erlauben 72 % aller an der Studie teilnehmenden Unternehmen allen Mitarbeitern die private Online-Nutzung (Internet und E-Mail), 11 % beschränkten die Gestattung auf spezielle Mitarbeiter/Abteilungen, 5 % auf ausgewählte Arbeitsplätze. Lediglich 13 % gestatteten generell keine private Nutzung, vgl. Nr. 1.03. der vollständigen Studie, vgl. *Koch*, VersR 2006, S. 1433.
[863] OLG Karlsruhe, MMR 2005, S. 179 f.; ArbG Hannover NZA-RR 2005, S. 421; *Altenburg/von Reinersdorff/Leister*, MMR 2005, S. 136; *Dies.*, MMR 2005, S. 223; *Büchner* in Beck´scher TGK-Kommentar, § 88 TKG, Rn. 24; *Büttgen* in Hoeren/Sieber, 16.3, Rn. 40; *Heidrich/Tschoepe*, MMR 2004, S. 76; *Huber* in Weitnauer, Form. J.1, Anm. 10 c); *Koch*, VersR 2006, S. 1433; *Lindemann/Simon*, BB 2001, S. 1951; *Mengel*, BB 2004, S. 1450; *Nägele/Meyer*, K & R 2004, S. 314; *Rieß* in Roßnagel, 6.4, Rn. 27; *Ueckert*, ITRB 2003, 158 ff.; *Weißnicht*, MMR 2003, S. 449
[864] *Hassemer/Witzel*, ITRB 2006, S. 139 ff.; *Huber* in Weitnauer, Form. J.1, Anm. 10 c); *Post-Ortmann*, RDV 1999, S. 102 ff.; *Robert* in Beck´scher TKG-Kommentar, 2. Aufl., § 3 TKG, Rn. 19

Telekommunikationsdiensten vor.[865] In diesem Fall würde sich die Kontrolle der Emails allein nach den allgemeinen Vorschriften des BDSG richten.[866]

Demgemäß findet § 88 TKG auf Email-Service-Provider stets, im Fall von Unternehmen hingegen nur dann Anwendung, wenn den Angestellten die private Email-Nutzung erlaubt wurde.

c) Kenntnisverschaffen über den Inhalt oder die näheren Umstände der Telekommunikation

Ein Verstoß gegen § 88 Abs. 3 S. 1 TKG setzt voraus, dass in dem Filtereinsatz ein Kenntnisverschaffen im Sinne der Vorschrift liegt.
Der Einsatz der Filtersoftware kann, wie oben dargestellt,[867] dazu führen, dass eingehende Emails durch das Programm virtuell geöffnet werden oder die Verbindung bereits aufgrund bestimmter erkannter Merkmale etwa der Email-Adresse des Absenders unterbrochen, die Email gelöscht oder umgeleitet wird. Wie bereits dargestellt wurde,[868] kommt es jedoch durch den Filtereinsatz nicht zu anderen Speichervorgängen, als dies der Fall wäre, wenn die Software nicht verwendet würde.
Nachfolgend wird zwischen dem Vorgehen in Bezug auf positiv gescannte Nachrichten (aa) und der Überprüfung von Inhalts- und Headerdaten (bb) unterschieden.

aa) Vorgehen in Bezug auf positiv gescannte Nachrichten

Fraglich ist, ob das Vorgehen in Bezug auf positiv gescannte Nachrichten, also das Blockieren, Löschen, Markieren durch Hinzufügen einer zusätzlichen Headerzeile oder Verändern der Subjektzeile, sowie das Umleiten der Nachricht in einen speziellen Ordner als Kenntnisverschaffen im Sinne des § 88 TKG angesehen werden kann.

Der Wortlaut des § 88 Abs. 1 S. 1 TKG stellt lediglich auf das Verschaffen und Verwenden von Kenntnissen über den Inhalt oder die näheren Umstände der Telekommunikation ab. Das ebenfalls aus der Übermittlung durch Dritte resultierende Übermittlungsrisiko erwähnt die Vorschrift jedoch nicht. Aus der Formulierung des § 88 TKG wird deutlich, dass das Fernmeldegeheimnis verschiedene Maßnahmen des Diensteanbieters zu verhindern sucht und zwar einerseits das Kenntnisverschaffen, andererseits die Verwendung erlangter Kenntnisse. Insofern ist bereits nach dem Wortlaut der Vorschrift davon auszugehen, dass das Fernmeldegeheimnis dem Löschen, Blockieren, Markieren oder Umleiten elektronischer Nachrichten nicht entgegensteht.
Das Ergebnis wird bestätigt, wenn man sich vor Augen führt, dass das Fernmeldegeheimnis lediglich dem Schutz der Privatsphäre dient.[869] Hingegen fällt darunter nicht der Schutz vor

---

[865] OLG Karlsruhe, MMR 2005, S. 179 f.; ArbG Hannover NZA-RR 2005, S. 421; *Altenburg/von Reinersdorff/Leister*, MMR 2005, S. 136; *Dies.*, MMR 2005, S. 223; *Büchner* in Beck´scher TKG-Kommentar, § 88 TKG, Rn. 24; *Büttgen* in Hoeren/Sieber, 16.3, Rn. 40; *Heidrich/Tschoepe*, MMR 2004, S. 76; *Huber* in Weitnauer, Form. J.1, Anm. 10 c); *Koch*, VersR 2006, S. 1433; *Lindemann/Simon*, BB 2001, S. 1951; *Mengel*, BB 2004, S. 1450; *Nägele/Meyer*, K & R 2004, S. 314; *Rieß* in Roßnagel, 6.4, Rn. 27; *Ueckert*, ITRB 2003, 158 ff.; *Weißnicht*, MMR 2003, S. 449

[866] *Altenburg/von Reinersdorff/Leister*, MMR 2005, S. 136; *Heidrich/Tschoepe*, MMR 2004, S. 76; *Lindemann/Simon*, BB 2001, S. 1951; *Mengel*, BB 2004, S. 1450; *Weißnicht*, MMR 2003, S. 449 f.

[867] vgl.: 1. Kap. Teil 2 A.

[868] vgl.: Gliederungsziffer

[869] BVerfGE 33, S. 1 ff., 11; BVerfGE 67, S. 157 ff., 171 f.; BVerfGE 85, S. 386 ff., 396; BVerfGE 100, S. 313 ff., 366; BVerfG, NJW 2002, S. 3619 ff., 3620; BVerfG, NJW 2003, S. 1787 ff., 1789; BVerfG, NJW 2004, S. 2213 ff., 2215; BVerfG, NJW 2005, S. 2603 ff., 2604; BVerfG, CR 2005, S. 799 ff., 800; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 24; *Bizer* in Alternativkommentar, Art. 10 GG, Rn. 37

der Unterdrückung der Kommunikation, also der Entfernung aus dem gewöhnlichen Ablauf des Übermittlungsvorgangs oder dem Anhalten, da sich dies begrifflich nicht als Verletzung der Geheimnissphäre der Kommunikationspartner darstellt.[870] Das Übermittlungsrisiko ist demnach durch das Fernmeldegeheimnis nicht erfasst.[871]

Daher steht das Fernmeldegeheimnis dem Löschen, Blockieren, Markieren oder Umleiten elektronischer Nachrichten nicht entgegen.

bb) Überprüfung von Inhalts- und Headerdaten

Fraglich ist, ob das Überprüfen von Inhalts- und Headerdaten als Kenntnisverschaffen im Sinne des § 88 Abs. 3 S. 1 TKG zu qualifizieren ist.

Grundvoraussetzung ist, dass die vorliegende Konstellation in zeitlicher Sicht dem Fernmeldegeheimnis unterfällt. Der Schutz des Fernmeldegeheimnisses reicht bis zu dem Moment, in dem sich die Nachricht im Herrschaftsbereich des Empfängers befindet und der Übertragungsvorgang beendet ist.[872] Sämtliche Arbeitsschritte, die darauf ausgerichtet sind, eingehende Emails anhand bestimmter Merkmale als unerwünscht zu identifizieren, finden vor dem Einstellen in die Mailbox und demnach stets vor Abruf der Nachricht durch den Empfänger statt, da nur so der von der Providern verfolgte Zweck, nämlich die Ersparnis von Speicherplatz, Aufwand und Kosten realisiert werden kann. Demnach unterfällt der Filtereinsatz in zeitlicher Hinsicht dem Fernmeldegeheimnis.

Die durch die Filtersoftware durchgeführten Maßnahmen könnten unter den Begriff des Kenntnisverschaffens im Sinne des § 88 Abs. 3 S. 1 TKG fallen.
An dieser Stelle wird relevant, wie die eingesetzte Software technisch funktioniert. Wie bereits dargestellt wurde,[873] werden Inhalt und Headerinformationen eingehender Emails oder beides durch die Filtersoftware nach bestimmten Merkmalen durchsucht, anhand derer die Nachricht als erwünscht oder unerwünscht qualifiziert werden kann. Dabei nimmt das Filterprogramm „Kenntnis“ vom Inhalt der Nachricht, indem es diese virtuell öffnet.[874] Zu diesem Zweck werden die Nachrichten zwar momentan in den Zwischenspeicher geladen, allerdings nicht dauerhaft gespeichert oder für den Provider oder seine Mitarbeiter lesbar abgelegt.[875] Damit finden lediglich solche Zwischenspeichervorgänge statt, wie sie bei der Datenübermittlung ständig durchgeführt werden. Eine dauerhafte Fixierung der Informationen auf einem Speichermedium erfolgt hingegen nicht.[876] Zu einer Kenntnisnahme der in der Email enthaltenen Daten und Informationen durch kommunikationsfremde Dritte kommt es demnach nicht.[877] Da Emails oder Email-Bestandteile nicht infolge des Filtereinsatzes

[870] das Bundesverfassungsgericht prüft nur Art. 5 Abs. 1, 2 Abs. 1 GG: BVerfGE 35, S. 311 ff., 315; BVerfGE 42, S. 234 ff., 236; BVerfGE 57, S. 170 ff., 177; BVerfG, NJW 1995, S. 1477 f., 1478; vgl. auch: *Bizer* in Alternativkommentar, Art. 10 GG, Rn. 71; *Dürig* in Maunz/Dürig, Art. 10 GG, Rn. 17; *Hermes* in Dreier, Art. 10 GG, Rn. 83; *Jarass* in Ders./Pieroth, Art. 10 GG, Rn. 11; *Lengning*, a.a.O., S. 10; *Kämmerer/Eidenmüller*, § 5 PostG, Anm. 10; *Wollweber*, a.a.O., S. 25
[871] das Bundesverfassungsgericht prüft nur Art. 5 Abs. 1, 2 Abs. 1 GG: BVerfGE 35, S. 311 ff., 315; BVerfGE 42, S. 234 ff., 236; BVerfGE 57, S. 170 ff., 177; BVerfG, NJW 1995, S. 1477 f., 1478; vgl. auch: *Bizer* in Alternativkommentar, Art. 10 GG, Rn. 71; *Dürig* in Maunz/Dürig, Art. 10 GG, Rn. 17; *Hermes* in Dreier, Art. 10 GG, Rn. 83; *Jarass* in Ders./Pieroth, Art. 10 GG, Rn. 11; *Lengning*, a.a.O., S. 10; *Kämmerer/Eidenmüller*, § 5 PostG, Anm. 10; *Wollweber*, a.a.O., S. 25
[872] BVerfG, NJW 2006, S. 976 ff.; vgl. näher: 2. Kap. Teil 2 A. I. 2. a)
[873] vgl.: 1. Kap. Teil 2 A. II.
[874] vgl.: 1. Kap. Teil 2 A. II.
[875] vgl.: 1. Kap. Teil 2 A. II.
[876] vgl.: 1. Kap. Teil 2 A. II.
[877] vgl.: 1. Kap. Teil 2 A. II.

gespeichert bleiben, können Dritte auch nicht aufgrund des Filtervorgangs später von Kommunikationsdaten und -inhalten Kenntnis nehmen. Aufgrund dieser Tatsache könnten die Filtermaßnahmen nicht als Kenntnisverschaffen im Sinne des § 88 Abs. S. 1 TKG zu qualifizieren sein.

Für das Vorliegen eines Kenntnisverschaffens könnte jedoch sprechen, dass es für das Eingreifen des Fernmeldegeheimnisses als unerheblich angesehen wird, ob die Erfassung und Verarbeitung der geschützten Informationen maschinell gesteuert wird oder unmittelbar durch eine menschliche Handlung erfolgt.[878] Insofern könnte davon auszugehen sein, dass ein Kenntnisverschaffen im Sinne des § 88 Abs. 3 TKG unabhängig davon zu bejahen ist, ob die Gefahr der Kenntnisnahme durch kommunikationsfremde Dritte besteht.

Dagegen lässt sich jedoch anführen, dass der Begriff der Kenntnis beinhaltet, dass eine dem Kommunikationsvorgang fremde Person die maßgeblichen Inhalte optisch oder anderweitig wahrnimmt oder zumindest aufgrund einer Aufzeichnung später wahrnehmen kann. So wird nach dem Sprachgebrauch unter Kenntnis „das Wissen von etwas“, „das Bekanntsein mit bestimmten Fakten o.ä.“ verstanden.[879] „Verschaffen“ bedeutet „dafür sorgen, dass jemandem etwas zuteil wird, jemand etwas bekommt (was nicht ohne weiteres erreichbar ist)“.[880] Folglich bedeutet Kenntnisverschaffen, dass jemandem ein bestimmtes Wissen zuteil wird.
Dieses Verständnis ergibt sich auch aus dem übrigen Wortlaut des § 88 Abs. 3 TKG. Nach § 88 Abs. 3 S. 1 TGK ist es Diensteanbietern im Sinne des § 88 Abs. 2 TKG untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Somit stellt die Vorschrift eindeutig darauf ab, dass entweder der Telekommunikationsdienstleister selbst oder Dritte von den Inhalten oder den näheren Umständen der Telekommunikation erfahren. Vorgänge ohne Wahrnehmung der Inhalte oder näheren Umstände der Telekommunikation durch eine Person oder eine zumindest mögliche spätere Wahrnehmung sind demnach vom Wortlaut des § 88 Abs. 3 S. 1 TGK nicht erfasst. Eine Weitergabe an Dritte ist nach § 88 Abs. 3 S. 3 TGK nur unter bestimmten dort näher genannten Voraussetzungen zulässig. Auch hier sieht das Gesetz die Gefahr darin, dass Dritte durch die Weitergabe oder die Verwendung von den fraglichen Informationen Kenntnis erlangen. Somit wird auch insoweit auf die Kenntnisnahme oder Kenntnisnahmemöglichkeit als den Betroffenen gefährdenen Akt abgestellt.
Auch der Wortlaut des Art. 10 Abs. 1 GG, der auf verfassungsrechtlicher Ebene das Fernmeldgeheimnis schützt, spricht dafür, dass solche Vorgänge nicht unter das Fernmeldegeheimnis fallen, die nicht zu einer Kenntnisnahme durch Dritte oder zumindest zu einer späteren Kenntnisnahmemöglichkeit führen. Denn Art. 10 Abs. 1 GG spricht vom Fernmeldegeheimnis. Eine Verletzung eines Geheimnisses kann allerdings lediglich dann angenommen werden, wenn ein Dritter von der geheimzuhaltenden Tatsache Kenntnis erlangt bzw. zumindest Informationen vorliegen, die eine spätere Kenntnisnahme ermöglichen.
Für dieses Ergebnis spricht auch der Wortlaut der gesetzlichen Schranken des Art. 10 Abs. 1 GG. § 100 a S. 1 StPO ermöglicht die Überwachung und Aufzeichnung der Telekommunikation durch Strafverfolgungsbehörden. Das G 10[881] erlaubt es den Verfassungsschutzbehörden des Bundes und der Länder, dem militärischen Abwehrdienst sowie dem Bundesnachrichtendienst unter bestimmten Voraussetzungen, die

[878] *Bizer* in Alternativkommentar, Art. 10 GG, Rn. 73
[879] *Duden*, Bedeutungswörterbuch, Stichwort „Kenntnis“
[880] *Duden*, Bedeutungswörterbuch, Stichwort „verschaffen“
[881] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz, BGBl. I 2001, 1254, 2298

Telekommunikation zu überwachen und aufzuzeichnen und dem Brief- oder Postgeheimnis unterliegende Sendungen zu öffnen und einzusehen, vgl. § 1 Abs. 1 G 10. Auch das ZfDG[882] betrifft die Überwachung der Telekommunikation. Die genannten Schranken stellen folglich stets auf das Überwachen sowie auf das Aufzeichnen der Kommunikation ab.
Der Begriff der Überwachung umfasst dabei das Mitlesen der Kommunikation bzw. der Verbindungsdaten sowie die Übertragung auf einen Schriftträger.[883] Aufzeichnen bedeutet die Sicherung der Kommunikationsvorgänge auf speziellen Speichermedien.[884] Abgestellt wird somit stets auf die Wahrnehmung der betreffenden Informationen bzw. auf eine dauerhafte Fixierung mit der Folge der Möglichkeit einer späteren Kenntnisnahme.

Die Auslegung dahingehend, dass lediglich die Kenntnisnahme bzw. Gefahrschaffung der späteren Kenntnisnahme durch einen Dritten als Eingriff in das Fernmeldegeheimnis qualifiziert werden kann, ergibt sich auch, wenn man dessen Zielrichtung betrachtet. Das Fernmeldegeheimnis begegnet Gefahren für die Vertraulichkeit von Mitteilungen, die aus dem Übermittlungsvorgang einschließlich der Einschaltung fremder Übermittler entstehen.[885] Bei der Nutzung von Telekommunikationseinrichtungen ist die Kommunikation aufgrund der räumlichen Distanz der Gesprächspartner Gefährdungen in Gestalt der Kenntnisnahme durch Dritte ausgesetzt und unterliegt deshalb besonderem Schutz.[886] Grundrechtlich ist die Unverletzlichkeit des Fernmeldegeheimnisses in Art. 10 Abs. 1 GG verbürgt. Es soll vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikation deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.[887] Dabei umfasst das Fernmeldegeheimnis im Sinne des Art. 10 Abs. 1 GG den Kommunikationsinhalt,[888] darüber hinaus jedoch auch die Kommunikationsumstände, insbesondere die Frage, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist.[889] Im Interesse eines effektiven Grundrechtsschutzes sind zu den näheren Umständen auch die Angaben einer Person zu zählen, die ein Eindringen in eine vertrauliche Kommunikationsbeziehung ermöglichen, wie die Nummer oder Kennung eines Endgerätes oder die postalische Adresse, soweit sie nicht von den Betroffenen öffentlich zugänglich gemacht worden sind.[890] Art. 10 Abs. 1 GG garantiert demnach die Privatsphäre bei der Kommunikation auf räumliche Distanz.[891] Der Schutzbereich des Art. 10 Abs. 1 GG ist dabei

---

[882] Gesetz über das Zollkriminalamt und die Zollfahndungsämter, Zollfahndungsdienstgesetz, BGBl. 2002, 3202
[883] *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 325; *Meyer-Goßner*, § 100 a StPO, Rn. 3; *Pfeiffer*, § 100 a StPO, Rn. 4; *Schäfer* in Löwe-Rosenberg, § 100 a StPO, Rn. 60 ff.
[884] *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 326; *Schäfer* in Löwe-Rosenberg, § 100 a StPO, Rn. 60 f.
[885] BVerfG, NJW 2003, S. 1787 ff., 1789
[886] BVerfGE 67, S. 157 ff., 171 f.; BVerfGE 85, S. 386 ff., 396; BVerfG, NJW 2002, S. 3620 ff., 3620; BVerfGE 107, S. 299 ff., 312; OVG Bremen, CR 1994, S. 700 ff., 702; *Burghart* in Leibholz/Rinck, Art. 10 GG, Rn. 31; *Gusy* in von Magoldt/Klein/Starck, Art. 10 GG, Rn. 14 ff.; *Kubicek*, DuD 1995, S. 657
[887] BVerfGE 93, S. 181 ff., 188; BVerfGE 100, S. 313 ff., 359; BVerfG, NJW 2003, S. 1787 ff., 1789; BVerfG, NJW 2005, S. 2603 ff., 2604; BVerfG, CR 2005, S. 799 ff., 800; OVG Bremen, CR 1994, S. 700 ff., 702; *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 310; *Burghart* in Leibholz/Rinck, Art. 10 GG, Rn. 31; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 45
[888] BVerfGE 67, S. 157 ff., 172; BVerfGE 85, S. 386 ff., 396; BVerfGE 100, S. 313 ff., 358; BVerfGE 107, S. 299 ff., 312
[889] BVerfGE 67, S. 157 ff., 172; BVerfGE 85, S. 386 ff., 396; BVerfGE 100, S. 313 ff., 358¸ BVerfGE 107, S. 299 ff., 312 f.
[890] *Bizer* in Alternativkommentar, Art. 10 GG, Rn. 40
[891] BVerfGE 85, S. 386 ff., 395 f.; BVerfGE 100, S. 313 ff., 358; BVerfGE 106, S. 28 ff., 36; BVerfG, NJW 1992, S. 1875 ff., 1875; BVerfG, NJW 2003, S. 1787 ff., 1788; BVerfG, CR 2005, S. 799 ff.; *Burghart* in Leibholz/Rinck, Art. 10 GG, Rn. 31; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 19

auch betroffen, wenn zu befürchten ist, dass der Staat Kenntnisse von Fernmeldeumständen und -inhalten in anderen Zusammenhängen zum Nachteil der Kommunikationspartner verwertet.[892] Daher erfasst Art. 10 GG auch solche Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von den geschützten Kommunikationsvorgängen anschließen und den Gebrauch, der von der erlangten Kenntnis gemacht wird.[893] Das auf verfassungsrechtlicher Ebene verbürgte Fernmeldegeheimnis schützt also umfassend die Vertraulichkeit des Fernmeldeverkehrs und sieht die Wahrnehmung der fraglichen Informationen, deren Fixierung mit der Folge der möglichen späteren Kenntnisnahme durch Dritte sowie spätere Verarbeitungsvorgänge als Verletzungshandlungen an.
§ 88 TKG verfolgt das gleiche Ziel wie Art. 10 Abs. 1 GG, allerdings im Verhältnis zu privaten Übermittlungspersonen.[894] Die dargestellte Argumentation zu Art. 10 Abs. 1 GG lässt sich daher auf § 88 TKG übertragen. Zusammenfassend kann demnach festgehalten werden, dass es Ziel der das Fernmeldegeheimnis sichernden Vorschriften ist, vor der Kenntnisnahme von Inhalt und Kommunikationsumständen oder der Weitergabe bzw. weiteren Verwendung der hierbei erlangten Informationen zu schützen, um die Vertraulichkeit der räumlich distanzierten Kommunikation zu gewährleisten. Maßnahmen, die nicht in einer Kenntnisnahme oder einem Niederlegen der betreffenden Informationen mit der Folge der Möglichkeit der späteren Kenntnisnahme, Verwendung oder Weitergabe resultieren, beeinträchtigen jedoch nicht die Vertraulichkeit der räumlich distanzierten Kommunikation.[895] Es ist somit davon auszugehen, dass die Kommunikation nicht aufgrund solcher Handlungen inhaltlich oder der Form nach anders verläuft. Hieraus folgt, dass die entsprechenden Vorgänge nicht dem Fernmeldegeheimnis unterfallen.

Die zu Art. 10 GG sowie anderen die Privatsphäre schützenden Grundrechten ergangene Rechtsprechtung bestätigt dieses Ergebnis.
So wurde ein Eingriff in das Fernmeldegeheimnis stets in solchen Fällen bejaht, in denen sich staatliche Stellen ohne Zustimmung der Beteiligten Kenntnis vom Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschafften.[896] Ein Eingriff in Art. 10 Abs. 1 GG liegt insbesondere im Öffnen von Briefen und der Wahrnehmung von deren Inhalt.[897] Auch das Abhören, die Kenntnisnahme, das Erfassen der näheren Umstände, das Auswerten des Inhalts der Telekommunikation, die Verwendung der gewonnenen Daten sowie die Zuordnung eines bestimmten Telekommunikationsvorgangs zu den daran beteiligten Endgerätenutzern ist nach der Rechtsprechung als Eingriff in Art. 10 Abs. 1 GG anzusehen.[898] Ebenso soll der heimliche Zugriff auf die in der Mailbox eines Anschlussinhabers gespeicherten Daten in den Schutzbereich des Fernmeldegeheimnisses fallen.[899] Schließlich bejahte die Rechtsprechung in einem Fall des Erfassens von

[892] BVerfGE 100, S. 313 ff., 359 unter Hinweis auf BVerfGE 65, S. 1 ff., 42 f., BVerfGE 93, 181 ff., 188; BVerfGE 107, S. 299 ff., 313
[893] BVerfGE 100, 313 ff, S. 359; für das Recht auf informationelle Selbstbestimmung: BVerfGE 65, S. 1 ff., 46
[894] *Büchner* in Beck´scher TKG-Kommentar, § 88 TKG, Rn. 2
[895] ähnlich: BVerwG, NJW 1969, 1638, wonach das Postgeheimnis betriebsbedingten Maßnahmen, insbesondere der Prüfung, ob die Voraussetzungen für einen offenen Versand erfüllt sind, nicht entgegensteht, sofern über das Ergebnis dieser Prüfung keine Mitteilung nach außen gelangt.
[896] BVerfGE 100, S. 313 ff., 366; BVerfG, NJW 2002, S. 3619 ff., 3620; BVerfG, NJW 2003, S. 1787 ff., 1789; BVerfG, NJW 2004, S. 2213 ff., 2215; BVerfG, NJW 2005, S. 2603 ff., 2604; BVerfG, CR 2005, S. 799 ff., 800; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 57
[897] BVerfGE 33, S. 1 ff., 11; BVerfGE 67, S. 157 ff., 171 f.; BVerfG, NJW 2004, S. 2213 ff., 2215
[898] BVerfGE 67, S. 157 ff., 171 f.; BVerfGE 100, S. 313 ff., 358 ff.; BVerfGE 106, S. 28 ff., 37; BVerfG, NJW 2004, S. 2213 ff., 2215; LG Stuttgart, NJW 2005, S. 614 ff., 614
[899] BGH, NJW 1997, S. 1934ff., 1935

Ferngesprächen mittels einer Fangschaltung und Zählervergleichseinrichtung durch die Deutsche Bundespost einen Eingriff in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG.[900]
Auch im Bereich der Wohnraumüberwachung stellt die Rechtsprechung -allerdings im Rahmen des Art. 13 GG- auf die Kenntnisnahme bzw. weitere Verwendung der erlangten Informationen ab. Danach sind im Wege der akustischen Wohnraumüberwachung erlangte Kenntnisse über Äußerungen dem durch Art. 13 Abs. 1 in Verbindung mit Art. 1 Abs. 1 und Art. 2 Abs. 1 GG geschützten Kernbereich privater Lebensgestaltung zuzurechnen, weshalb sie im Strafverfahren einem absoluten Verwertungsverbot unterliegen.[901]
Soweit nach Abschluss des Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherte Verbindungsdaten betroffen sind, ergibt sich der grundrechtliche Schutz nicht aus Art. 10 GG, sondern aus dem Recht auf informationelle Selbstbestimmung.[902] Die Sicherstellung von Datenträgern, auf denen Telekommunikationsverbindungsdaten gespeichert sind, greift nach Rechtsprechung des Bundesverfassungsgerichts in das informationelle Selbstbestimmungsrecht ein.[903]
Ebenso werden heimliche Tonbandaufnahmen als rechtswidriger Eingriff in die Privatsphäre angesehen, wobei auch hier der Grundrechtsschutz des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG eingreift.[904] Das allgemeine Persönlichkeitsrecht im Sinne des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst nach der Rechtsprechung auch das Recht am gesprochenen Wort, das bedeutet die Befugnis, zu bestimmen, ob es allein dem Gesprächspartner oder auch Dritten oder sogar der Öffentlichkeit zugänglich sein soll, ferner ob es auf Tonträger aufgenommen werden darf.[905]
Aus der vorgenannten Rechtsprechung ergibt sich, dass Kommunikation sowie deren Begleitumstände umfassend vor der Kenntnisnahme durch Dritte geschützt wird, da den Grundrechtsträgern eine Sphäre der Privatheit zukommen soll, innerhalb deren sie sich frei äußern können. Soweit die Privatheit allerdings durch bestimmte Maßnahmen nicht beeinträchtigt wird, weil die Kenntnisnahme durch einen Dritten ausgeschlossen ist, besteht kein Bedürfnis, diese als Eingriff in die Privatsphäre, hier in Gestalt des Fernmeldegeheimnisses, anzusehen. Die zitierte Rechtsprechung zeigt, dass ein Eingriff in das Fernmeldegeheimnis oder andere Gewährleistungen der Privatsphäre stets die Kenntnisnahme oder zumindest die Kenntnisnahmemöglichkeit durch einen Dritten voraussetzt, so etwa bei der Verarbeitung erlangter Informationen oder deren Weitergabe. Hier ist eine solche Gefahr allerdings nicht gegeben.[906] Demnach ist ein Eingriff in das Fernmeldegeheimnis zu verneinen.

Dies wird durch ein Urteil des Bundesverfassungsgerichts bestätigt, in dem dieses ausführt, ein Eingriff in das Fernmeldegeheimnis scheide aus, soweit Fernmeldevorgänge zwischen Anschlüssen ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach Signalaufbereitung technisch wieder spurenlos ausgesondert würden.[907] Hingegen soll die Überwachung und Aufzeichnung von Telekommunikationsvorgängen auch dann einen Eingriff darstellen, wenn die erfassten Daten nicht sofort einer bestimmten Person zugeordnet

[900] BVerfGE 85, S. 386 ff., 396
[901] BGH, NJW 2005, S. 3295 ff., 3296 unter Bezugnahme auf BVerfGE 109, S. 279 ff., 311 ff.; BGH, NJW 1997, S. 1019 f.; vgl. auch: BGH, NJW 1998, S. 3285; SächsVerfGH, NVwZ 2005, S. 1314 f.
[902] BVerfG, NJW 2006, S. 976 ff., 979
[903] BVerfG, NJW 2006, S. 976 ff., 980
[904] BVerfGE 34, S. 245; BGHSt 27, S. 357; BGHSt 31, S. 306; BGHSt 34, S. 399; BGH, NJW 1988, S. 1016; BGH, NJW 1989, S. 2760; OLG Köln, NJW 1987, S. 262; *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 341
[905] BVerfGE 34, S. 245; BVerfGE 54, S. 154; BGHZ 27, S. 286; BGH, NJW 2002, S. 3619 ff., 3621 ; BAGE 41, S. 37; BAGE 80, S. 366
[906] vgl.: 1. Kap. Teil 2 A.
[907] BVerfGE 100, S. 313 ff., 366

werden können, sofern sich der Personenbezug später herstellen lässt.[908] Hier zeigt sich deutlich, dass hinsichtlich des Fernmeldegeheimnisses darauf abzustellen ist, ob eine Kenntnisnahme von Kommunikationsinhalt und -umständen durch einen Dritten möglich ist.[909] Ist dies nicht der Fall so liegt nach der soeben zitierten Rechtsprechung kein Eingriff in das Fernmeldegeheimnis vor. Auch dies spricht dafür, das Merkmal des Kenntnisverschaffens nur bei solchen Vorgängen zu bejahen, die zur Kenntnisnahme durch Dritte oder zu einer späteren Kenntnisnahmemöglichkeit führen.

Schließlich ist zu beachten, dass die im Bereich des informationellen Selbstbestimmungsrechts geltenden Vorgaben auch für das spezielle Fernmeldegeheimnis Anwendung finden.[910] Somit kann auch auf die im Bereich des Datenschutzrechts genannten Argumente und das dort gefundene Ergebnis verwiesen werden.[911]

Es wurde gezeigt, dass das Fernmeldegeheimnis lediglich vor der Kenntnisnahme bzw. Gefahrschaffung der späteren Kenntnisnahme durch einen Dritten schützt. Der Filtereinsatz bringt diese Gefahr, wie bereits dargestellt wurde, nicht mit sich. Deshalb liegt in dem Einsatz der Filtersoftware kein Verstoß gegen das Fernmeldegeheimnis.

d) Zwischenergebnis

Dem Einsatz von Filtersoftware mit der Folge der Überprüfung des Inhalts und der Headerinformationen eingehender Emails steht das in § 88 TKG normierte einfachgesetzliche Fernmeldegeheimnis nicht entgegen.
Auch die weitere Vorgehensweise in Bezug auf positiv gescannte Emails, also das Löschen, Blockieren, Markieren oder Umleiten elektronischer Nachrichten ist zulässig, da das Übermittlungsrisiko durch § 88 TKG nicht erfasst wird.

II. Strafrecht

Dem Überprüfen von Inhalt oder Headerinformationen eingehender Emails sowie dem Löschen, Markieren, Umleiten oder Blockieren elektronischer Nachrichten, die als Spam identifiziert wurden, könnten strafrechtliche Vorschriften entgegenstehen.
So könnte sich derjenige, der den Einsatz der Filtersoftware veranlasst, nach § 202 Abs. 1 StGB (1.), § 202 a Abs. 1 StGB (2.), § 206 StGB (3.), § 303 a StGB (4.) oder § 44 Abs. 1 BDSG (5.) strafbar machen.

1. § 202 Abs. 1 StGB

§ 202 Abs. 1 StGB sanktioniert die Verletzung des Briefgeheimnisses. Den Tatbestand verwirklicht derjenige, der einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück öffnet, das nicht zu seiner Kenntnis bestimmt ist oder sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft.

---

[908] BVerfGE 100, S. 366
[909] im Ergebnis: *Art. 29 Datenschutzgruppe*, WP 118, S. 3, die von einem Eingriff in die durch Art. 8 EMRK geschützte Privatsphäre nur dann annimmt, wenn ein Dritter Zugang zum Inhalt oder den Verbindungsdaten erhält
[910] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)
[911] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

Allerdings ist -unabhängig von der Frage, ob eine Email als Brief oder sonstiges Schriftstück im Sinne des § 202 StGB angesehen werden kann-[912] fraglich, ob eine solche Nachricht das Merkmal des Verschlossenseins im Sinne des § 202 StGB erfüllt. Verschlossen ist ein Schriftstück, wenn ein mit ihm unmittelbar verbundener Verschluss die Kenntnisnahme durch beliebige Dritte zumindest erschwert.[913] Mit einer Email kann jedoch kein Verschluss verbunden sein, da es sich nicht um einen körperlichen Gegenstand handelt. Fraglich ist, ob im Fall der Verschlüsselung der Email von einem Verschlossensein ausgegangen werden kann. Dabei ist das strafrechtliche Analogieverbot zu beachten, das in Art. 103 Abs. 2 GG verankert ist.[914] Danach ist die Anwendung einer Vorschrift auf einen auf Grund einer planwidrigen Regelungslücke nicht gesetzlich geregelten Sachverhalt sowie das Entwickeln neuer Rechtssätze aus ähnlichen bereits bestehenden zu Ungunsten des Täters ausgeschlossen.[915] Der Wortsinn als Grenze der Auslegung ist aus der Sicht des Bürgers zu bestimmen und darf sich nicht gänzlich vom allgemeinen Sprachgebrauch lösen, sondern muss voraussehbar bleiben.[916] Der Begriff „verschließen" bedeutet nach dem allgemeinen Sprachgebrauch „mit einem Schloß o.ä. zumachen, schließen, sichern; durch Zuschließen unzugänglich machen", „in etwas hineinlegen und es abschließen", „mit Hilfe eines Gegenstandes, einer Vorrichtung ö.ä. bewirken, dass etwas nach außen hin fest zu ist".[917] „Verschlüsseln" bedeutet hingegen „in Geheimschrift abfassen".[918] Da der Begriff verschlossen nach dem allgemeinen Sprachgebrauch auf das körperliche Unzugänglichmachen eines Gegenstandes abstellt, das Verschlüsseln hingegen eine völlig andere Zielrichtung hat, nämlich, den Bedeutungsgehalt einer Information durch Abfassen in Geheimschrift zu verbergen, können sie nach dem allgemeinen Sprachgebrauch nicht gleichgesetzt werden. Würde das Verschlüsseln unter den Begriff Verschlossen subsumiert, läge folglich ein Verstoß gegen das Analogieverbot vor. Es ist somit davon auszugehen, dass verschlüsselte Emails nicht verschlossen im Sinne des § 202 StGB sind.[919]

Aus den im Rahmen des § 88 TKG genannten Gründen fehlt es darüber hinaus an einem Kenntnisverschaffen.[920]

Somit ist § 202 Abs. 1 StGB nicht einschlägig. Der Versuch ist nicht strafbar, da die Mindeststrafdrohung unter einem Jahr liegt und eine Versuchsstrafbarkeit in der Vorschrift nicht angeordnet ist, §§ 23 Abs. 1, 12 Abs. 1, Abs. 2 StGB.

---

[912] vgl. dazu: *Barton*, CR 2003, S. 841
[913] RGSt 16, S. 288; *Lenckner* in Schönke/Schröder, § 202 StGB, Rn. 7; *Tröndle/Fischer*, § 202 StGB, Rn. 5
[914] *Kunig* in von Münch/Kunig, Art. 103 GG, Rn. 21; *Rudolphi* in Systematischer Kommentar, § 1 StGB, Rn. 22 ff.; *Schmidt-Aßmann* in Maunz/Dürig, Art. 103 GG, Rn. 231 ff.; *Schulze-Fielitz* in von Mangoldt/Klein/Starck, Art. 103 Abs. 2 GG, Rn. 41; *Tröndle/Fischer*, § 1 StGB, Rn. 10; *Wassermann* in Alternativkommentar, Art. 103 GG, Rn. 3
[915] BVerfGE 71, 115; BVerfGE 73, S. 235; BVerfGE 82, S. 269; BVerfGE 87, S. 225; BVerfGE 87, S. 411; BVerfGE 92, S. 13 f.; BVerfG, NJW 1993, S. 2524 f.; BVerfG, NJW 1995, S. 2587; BGHSt 7, S. 193; BGHSt 8, S. 70; BGH, NJW 1951, S. 809; BayObLG, AfP 1997, S. 526; *Amelung*, NJW 1995, S. 2587; *Schulze-Fielitz* in von Mangoldt/Klein/Starck, Art. 103 Abs. 2 GG, Rn. 41; *Tröndle/Fischer*, § 1 StGB, Rn. 10
[916] BVerfGE 71, S. 114 f.; BVerfGE 73, S. 244 f.; BVerfGE 82, S. 269; BVerfGE 87, S. 224; BVerfGE 92, S. 23; BVerfG, NJW 1995, S. 3051; *Degenhardt* in Sachs, Art. 103 GG, Rn. 70 a f.; *Scheffler*, Jura 1996, S. 505 ff.; *Schmidt-Aßmann* in Maunz/Dürig, Art. 103 Abs. 2 GG, Rn. 225 ff.; *Schulze-Fielitz* in von Mangoldt/Klein/Starck, Art. 103 Abs. 2 GG, Rn. 39
[917] Duden, Bedeutungswörterbuch, Stichwort „verschließen"
[918] Duden, Bedeutungswörterbuch, Stichwort „verschlüsseln"
[919] im Ergebnis: *Lenckner* in Schönke/Schröder, § 202 StGB, Rn. 7
[920] vgl.: 2. Kap. Teil 2 A. I. 2. c)

2. § 202 a Abs. 1 StGB

Durch den Einsatz des Filterprogramms mit der Folge der Überprüfung des Inhalts und der Headerinformationen eingehender Emails könnte jedoch der Tatbestand des § 202 a Abs. 1 StGB verwirklicht sein, der das Ausspähen von Daten strafrechtlich sanktioniert.
Die Vorschrift greift ein, wenn der Täter unbefugt Daten, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft.

Fraglich ist bereits, ob die durch das Programm überprüften Informationen gegen unberechtigten Zugang besonders gesichert sind. Das Merkmal liegt vor, wenn Vorkehrungen getroffen wurden, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren, wobei dies nicht der einzige Zweck der Vorkehrungen sein muss; erforderlich ist allerdings, dass der Berechtigte durch die Sicherung sein spezielles Interesse an der Geheimhaltung dokumentiert.[921] Bei im Übertragungsstadium befindlichen Daten kommt als Sicherungsmaßnahme nur die Datenverschlüsselung in Betracht.[922] Für einen Schutz verschlüsselt übertragener Daten durch § 202 a StGB spricht einerseits die Tatsache, dass diese andernfalls während des Übermittlungsvorgangs weitgehend schutzlos bleiben würden, andererseits lässt der Gesetzeswortlaut eine derartige Auslegung zu, da die Verschlüsselung den Zugang zu den versandten Daten verhindert.[923] Demnach kann die Verschlüsselung als eine den einzelnen Daten unmittelbar anhaftende Zugangssicherung angesehen werden.[924]
Daten, die verschlüsselt übermittelt werden, sind folglich gegen einen unberechtigten Zugang besonders gesichert. Bei unverschlüsselt versandten Emails fehlt es hingegen an einer besonderen Sicherung gegen unberechtigten Zugang.

Fraglich ist allerdings, ob derjenige, der den Filter einsetzt, die überprüften Inhalte sich oder einem anderen verschafft. Verschafft sind Daten, wenn der Täter bzw. der Dritte durch optische bzw. akustische Wahrnehmung von ihnen tatsächlich Kenntnis genommen hat, ferner ohne vorherige Kenntnisnahme dann, wenn der Täter den körperlichen Datenträger in seine oder des Dritten Verfügungsgewalt bringt oder wenn er die Daten auf einem solchen fixiert.[925] Dies ist allerdings nicht der Fall. Denn die Daten werden weder von einer Person während des Filtervorgangs zur Kenntnis genommen, noch ist dies später möglich, da die Ergebnisse und Zwischenschritte des Filtervorgangs nicht auf einem Datenträger gespeichert bleiben. Insofern kann derjenige, der den Filter einsetzt, weder im Augenblick der

---

[921] RGSt 16, S. 288; *Ernst*, NJW 2003, S. 3236; *Graf* in Münchener Kommentar, § 202 a StGB, Rn. 31; *Lackner/Kühl*, § 202 a StGB, Rn. 4; *Leicht*, IuR 1987, S. 74 ff.; *Lenckner/Winkelbauer*, CR 1986, S. 487; *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 7; *Schünemann* in Leipziger Kommentar, § 202 a StGB, Rn. 14 f.; *Tröndle/Fischer*, § 202 a StGB, Rn. 8

[922] *Lenckner/Winkelbauer*, CR 1986, S. 487; *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 8; *Tröndle/Fischer*, § 202 a StGB, Rn. 8

[923] *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 8; im Ergebnis auch: *Graf* in Münchener Kommentar, § 202 a StGB, Rn. 38; *Lackner/Kühl*, § 202 a StGB, Rn. 4; *Leicht*, IuR 1987, S. 51 f.; *Mehrings*, a.a.O., S. 185; *Schünemann* in Leipziger Kommentar, § 202 a StGB, Rn. 16; *Tröndle/Fischer*, § 202 a StGB, Rn. 8; a.A.: *Schmid*, a.a.O., S. 103 f.

[924] *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 8; im Ergebnis auch: *Graf* in Münchener Kommentar, § 202 a StGB, Rn. 38; *Lackner/Kühl*, § 202 a StGB, Rn. 4; *Leicht*, IuR 1987, S. 51 f.; *Mehrings*, a.a.O., S. 185; *Schünemann* in Leipziger Kommentar, § 202 a StGB, Rn. 16; *Tröndle/Fischer*, § 202 a StGB, Rn. 8; a.A.: *Schmid*, a.a.O., S. 103 f.

[925] *Ernst* in Ders., Hacker, Cracker & Computerviren, Rn. 234 f.; *Hoyer* in Systematischer Kommentar, § 202 a StGB, Rn. 11; *Jung* in Kindhäuser/Neumann/Paeffgen, § 202 a StGB, Rn. 9; *Lackner/Kühl*, § 202 a StGB, Rn. 5; *Lenckner/Winkelbauer*, CR 1986, S. 488; *Lenckner* in Schönke/Schröder, § 202 a StGB, Rn. 10; *Schünemann* in Leipziger Kommentar, § 202 a StGB, Rn. 6; *Spindler/Ernst*, CR 2004, S. 439; *Tröndle/Fischer*, § 202 a StGB, Rn. 10

Überprüfung, noch später erkennen, welche Daten der Header oder Inhalt der Email enthält. Da jedoch Voraussetzung des § 202 a StGB ist, dass der Täter die Daten liest oder so abspeichert, dass sie später gelesen werden können, wird der Tatbestand des § 202 a StGB durch den Einsatz des Filterprogramms nicht erfüllt.

3. § 206 StGB

Diejenige Person, die den Filtereinsatz anordnet, könnte sich nach § 206 StGB strafbar machen. Das Überprüfen des Inhalts und der Headerinformationen könnte dem Tatbestand des § 206 Abs. 2 Nr. 1 StGB unterfallen (a), während sich möglicherweise derjenige, der positiv gescannte Nachrichten blockiert, löscht, markiert oder umleitet, nach § 206 Abs. 2 Nr. 2 StGB strafbar macht (b).

a) Überprüfung des Inhalts und der Headerinformationen der elektronischen Nachricht

§ 206 Abs. 2 Nr. 1 StGB stellt denjenigen unter Strafe, der eine Sendung, die einem in Abs. 1 genannten Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, unbefugt öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft. Dabei muss der Täter Inhaber oder Beschäftigter des in Abs. 1 genannten Unternehmens sein.

Voraussetzung ist auch hier das Merkmal des Verschlossenseins. Eine Email kann jedoch, wie im Rahmen des § 202 StGB dargestellt, grundsätzlich nicht verschlossen sein.[926] Bereits deshalb wird der Tatbestand des § 206 Abs. 2 Nr. 1 StGB durch die Filtermaßnahme nicht verwirklicht. Im Übrigen fehlt es auch hier aus den im Rahmen des §§ 88 TKG genannten Gründen an einem Kenntnisverschaffen.[927]

b) Blockade, Löschen, Markieren oder Umleiten elektronischer Nachrichten

Die Person, die den Einsatz der Software veranlasst, könnte jedoch den Tatbestand des § 206 Abs. 2 Nr. 2 StGB verwirklichen, wenn das Filterprogramm bewirkt, dass positiv gescannte Nachrichten blockiert, gelöscht, markiert oder umgeleitet werden.
Nach § 206 Abs. 2 Nr. 2 StGB macht sich derjenige strafbar, der als Inhaber oder Beschäftigter eines in Abs. 1 bezeichneten Unternehmens unbefugt eine diesem zur Übermittlung anvertraute Sendung unterdrückt.

aa) Objektiver Tatbestand

Der objektive Tatbestand des § 206 Abs. 2 Nr. 2 StGB ist verwirklicht, wenn derjenige, der den Einsatz der entsprechenden Filter veranlasst, zum in Abs. 1 der Vorschrift genannten Täterkreis gehört (1), wenn eine Email sich als Sendung im Sinne der Vorschrift qualifizieren lässt (2) und die Sendung dem Täter anvertraut ist (3). Des Weiteren ist erforderlich, dass der Täter die Sendung unterdrückt (4) und dabei unbefugt handelt (5).

(1) Täterkreis

Voraussetzung ist zunächst, dass diejenigen Personen, die die Blockade, das Löschen, Markieren oder Umleiten spamverdächtiger Emails veranlassen, zum in § 206 Abs. 2 Nr. 2 StGB genannten Täterkreis gehören.

---

[926] vgl.: 2. Kap. Teil 2 A. II. 1.
[927] vgl.: 2. Kap. Teil 2 A. I. 2 c)

Von der Vorschrift werden Inhaber oder Beschäftigte eines in Abs. 1 bezeichneten Unternehmens erfasst. § 206 Abs. 1 StGB bezieht solche Unternehmen in den Täterkreis ein, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen. Der durch § 206 Abs. 1 StGB bezeichnete Personenkreis ist deckungsgleich mit demjenigen, der nach § 88 Abs. 2 TKG zur Wahrung des Post- bzw. Fernmeldegeheimnisses verpflichtet ist.[928] Oben wurde dargestellt, dass § 88 TKG auf Email-Service-Provider stets, im Fall von Unternehmen jedoch nur dann Anwendung findet, wenn den Angestellten die private Email-Nutzung erlaubt wurde.[929] Demgemäß gehören auch nur Inhaber oder Beschäftigte dieser Unternehmen zum geeigneten Täterkreis im Sinne des § 206 Abs. 1 StGB.

(2) Vorliegen einer Sendung

Weitere Voraussetzung des § 206 Abs. 2 Nr. 2 StGB ist, dass es sich bei der Email, die gelöscht, blockiert, markiert oder umgeleitet wird, um eine Sendung im Sinne der Vorschrift handelt.

Hierbei stellt sich die Frage, ob das Tatbestandsmerkmal „Sendung" das Merkmal der Körperlichkeit voraussetzt oder ob auch Emails unter den Begriff gefasst werden können.
Gegen ein Erfordernis der Körperlichkeit spricht einerseits der Regelungszweck der Vorschrift des § 206 StGB, der dahin geht, das Post- und Fernmeldegeheimnis im Sinne des Art. 10 GG zu schützen.[930] Vom Fernmeldegeheimnis im Sinne des Art. 10 GG wird jedoch auch die körperlose Übermittlung der Information,[931] mithin auch die Kommunikation mittels Email erfasst.[932]
Des Weiteren folgt aus dem Begriff der Sendung nach allgemeinem Sprachverständnis nicht notwendigerweise, dass diese eine Körperlichkeit aufzuweisen hat.[933]
Würde man die Körperlichkeit als Voraussetzung des Begriffs der Sendung ansehen, so ergäben sich im Übrigen Strafbarkeitslücken im Bereich der Email-Kommunikation. So würden bestimmte Eingriffe in die Kommunikation mittels elektronischer Post straffrei bleiben, während dieselbe Verhaltensweise im ähnlich gelagerten Fall der traditionellen Briefpost strafbar wäre.
Allgemein wird deshalb davon ausgegangen, dass der Begriff Sendung keine Körperlichkeit erfordert, jedoch das in § 206 Abs. 2 Nr. 1 StGB vorausgesetzte Merkmal des Verschlossenseins gerade nur bei körperlichen Sendungen vorliegen kann.[934]
Der unterschiedliche Wortlaut des § 206 Abs. 2 Nr. 1 StGB, der eine verschlossene Sendung voraussetzt, und des § 206 Abs. 2 Nr. 2 StGB, der nur auf das Vorliegen einer Sendung abstellt, basiert auf der verschiedenartigen Zwecksetzung der Vorschriften. Während bei § 206 Abs. 2 Nr. 1 StGB das Fernmeldegeheimnis, also das Verbot der Ausforschung des Inhalts der Kommunikation im Vordergrund steht, schützt § 206 Abs. 2 Nr. 2 StGB das

[928] BT- Drs. 13/8016, 29; *Heidrich/Tschoepe*, MMR 2004, S. 76; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 8
[929] vgl.: 2. Kap. Teil 2 A. I. 2. b)
[930] *Groß*, JZ 1999, S. 326; *Kindhäuser*, Lehr- und Praxiskommentar, § 206 StGB, Rn. 1; *Lackner/Kühl*, § 206 StGB, Rn. 2; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 2; *Welp*, ArchPF 1976, S. 764; *Tröndle/Fischer*, § 206 StGB, Rn. 1
[931] BVerfGE 46, S. 143
[932] *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 39; *Hermes* in Dreier, Art. 10 GG, Rn. 40; *Hofmann* in Schmidt-Bleibtreu/Klein, Art. 10 GG, Rn. 9; *Jarass* in Jarass/Pieroth, Art. 10 GG, Rn. 6, 8; *Kleine-Voßbeck*, a.a.O., S. 32; *Kudlich*, JuS 1998, S. 211; *Löwer* in von Münch/Kunig, Art. 10 GG, Rn. 18; *Pieroth/Schlink*, Staatsrecht II, Rn. 773
[933] vgl. Duden, Das Bedeutungswörterbuch, Stichwort „Sendung", wonach auch Übertragungen per Rundfunk oder Fernsehen als Sendung anzusehen sind.
[934] OLG Karlsruhe, MMR 2005, S. 180; *Schmidl*, DuD 2005, S. 268; *Spindler/Ernst*, CR 2004, S. 439

Vertrauen in die Störungsfreiheit der Übermittlung.[935] Aus diesem Grund ist es im Rahmen des § 206 Abs. 2 Nr. 1 StGB erforderlich, dass der Täter ein besonderes Hindernis überwindet, das ihm vom Versender entgegengestellt wird, um eine Kenntnisnahme zu verhindern.[936] Dies kann bei einer Email nicht der Fall sein. Selbst wenn eine elektronische Nachricht verschlüsselt wird, lässt sie sich, wie oben dargestellt, nicht unter den Begriff einer verschlossenen Sendung einordnen.[937] Da § 206 Abs. 2 Nr. 1 StGB somit im Telekommunikationssektor grundsätzlich keine Rolle spielt, würde die Verweisung in § 206 Abs. 3 Nr. 2 StGB auf Telekommunikationsdienste leer laufen, wenn auch § 206 Abs. 2 Nr. 2 StGB in diesem Bereich nicht anwendbar wäre.[938]

Demnach lässt sich festhalten, dass Emails zwar nicht das Merkmal des Verschlossenseins erfüllen, jedoch als Sendung im Sinne des § 206 Abs. 2 Nr. 2 StGB zu qualifizieren sind.[939]

(3) Anvertrautsein der Sendung

Weitere Voraussetzung des § 206 Abs. 2 Nr. 2 StGB ist, dass die Sendung dem Unternehmen oder den Personen, die die entsprechenden Filtermaßnahmen mit der Folge der Blockade, des Löschens, Umleitens oder Markierens der positiv gescannten Emails vornehmen, zu diesem Zeitpunkt bereits anvertraut ist.

Im Fall der Telekommunikation ist die Sendung anvertraut, wenn sie auf vorschriftsmäßige Weise in den Verkehr gelangt ist und sich im Gewahrsam des Unternehmens befindet.[940] Im Rahmen des Postverkehrs ist die Sendung ab dem Zeitpunkt des Einwerfens in den Briefkasten anvertraut.[941] Nicht erforderlich ist somit eine Annahme oder sonstige Bearbeitung durch die Post.[942] Dabei stellt sich insbesondere in zwei Fällen die Frage danach, ob die Email dem Provider des Empfängers oder dem Unternehmen, bei dem der Empfänger beschäftigt ist, bereits anvertraut ist. Dies ist einerseits der Fall, wenn es zu keiner vollständigen Übermittlung der Daten an den Empfänger kommt, weil die Verbindung zuvor unterbrochen wird (a), andererseits ist zweifelhaft, ob bei massenhaft versandten Spammails, die ohne vorherige Einwilligung der Adressaten versandt wurden, überhaupt davon gesprochen werden kann, dass diese dem Provider bzw. Unternehmen anvertraut sind (b).

(a) Unvollständige Datenübermittlungen

Problematisch ist, dass bei manchen der oben dargestellten Maßnahmen, insbesondere bei der Filterung mittels des Blacklist-Verfahrens, die Verbindung durch den Email-Empfänger-Server abgebrochen wird, sobald die eingehende Nachricht aufgrund bestimmter bereits übermittelter Daten als Spam identifiziert wird. Demnach kommt es hier grundsätzlich nicht zu einer vollständigen Übertragung der Email an den Provider des Empfängers. Fraglich ist, ob in diesem Fall bereits davon gesprochen werden kann, dass die Nachricht dem Email-

[935] *Hoyer* in Systematischer Kommentar, § 206 StGB, Rn. 3; *Lackner/Kühl*, § 206 StGB, Rn. 1; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 2; *Schmidl*, DuD 2005, S. 268; *Träger* in Leipziger Kommentar, § 206 StGB, Rn. 4; *Tröndle/Fischer*, § 206 StGB, Rn. 1; a.A.: *Altenhain* in Münchener Kommentar, § 206 StGB, Rn. 3 ff.
[936] *Schmidl*, DuD 2005, S. 269
[937] vgl.: 2. Kap. Teil 2 A. II. 1.
[938] *Spindler/Ernst*, CR 2004, S. 439
[939] so mittlerweile auch die Rspr.: OLG Karlsruhe, MMR 2005, S. 178 ff.
[940] OLG Karlsruhe, MMR 2005, S. 180; *Heidrich/Tschoepe*, MMR 2004, S. 77
[941] RGSt 22, S. 395; RGSt 28, S. 100 f.; *Lackner/Kühl*, § 206 StGB, Rn. 8; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 17; *Tröndle/Fischer*, § 206 StGB, Rn. 12
[942] *Lackner/Kühl*, § 206 StGB, Rn. 8; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 17

Service-Provider des Empfängers bzw. dem Unternehmen, bei dem der Empfänger beschäftigt ist, anvertraut war.

Diese Frage wurde bisher durch die Rechtsprechung nicht beantwortet. Das OLG Karlsruhe, das sich erstmalig mit der Frage der strafrechtlichen Relevanz der Blockade einer Email zu befassen hatte, entschied nicht, ab welchem Zeitpunkt von einem Anvertrautsein gesprochen werden kann. Es sprach lediglich aus, dass dies spätestens dann der Fall ist, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht hat und der versendende Mailserver die Daten dem empfangenden Server per SMTP-Protokoll übermittelt hat.[943]

Wird die Verbindung vor Übermittlung der vollständigen Email abgebrochen, so spricht gegen ein Anvertrautsein, dass diese noch nicht in den Einflussbereich des Email-Service-Providers bzw. Unternehmens gelangt ist. Es könnte davon auszugehen sein, dass ein Wechsel der Verantwortung für den Mailtransport erst zu dem Zeitpunkt vorliegt, in dem der empfangende Server den Erhalt der Email an den Absender-Client bestätigt, somit im Bereich der Übermittlung im Wege des SMTP-Protokolls erst nach der Übertragung der Kopfzeilen und des eigentlichen Inhalts der Email.

Dieser Interpretation lässt sich allerdings entgegenhalten, dass die in der Email enthaltenen Daten zur Zeit des Abbruchs der Verbindung bereits teilweise beim Email-Service-Provider oder Unternehmen angekommen sind. Denn zumindest ein Bestandteil der eigentlichen Sendung, nämlich die IP-Nummer des Absenders im Header, ist auch in diesem Fall bereits in den Bereich des empfangenden Mailservers gelangt.[944] Hier ist von Bedeutung, dass § 206 StGB, wie sich aus Abs. 5 ergibt, nicht nur der Inhalt, sondern auch die Umstände eines Kommunikationsvorgangs erfasst. Deshalb wird teilweise vertreten, die Sendung habe in dem Moment den Empfänger erreicht und sei ihm damit zur weiteren Übermittlung anvertraut, in dem ein Bestandteil der eigentlichen Sendung den empfangenden Mailserver erreicht hat.[945] Dieser Auffassung ist zuzustimmen. Denn die Verbindung wird durch den Empfänger-Server bewusst unterbrochen, nachdem die Daten ihn teilweise erreicht haben. Das Unterbrechen der Verbindung erfolgt mit dem Ziel, die Zustellung der Sendung zu verhindern. Daher liegt ein zielgerichteter und klassischer Fall des Eingriffs in die Zuverlässigkeit des Fernmeldeverkehrs vor. Der Wortlaut „anvertraut“ lässt dabei nicht zwingend darauf schließen, dass bereits die vollständige Email den Server des Empfängers erreicht haben muss. Dies lässt sich aus der Auslegung des entsprechenden Begriffs im Bereich des Postverkehrs ersehen. Hier ist eine Sendung ab dem Zeitpunkt des Einwerfens in den Briefkasten anvertraut.[946] Nicht erforderlich ist dagegen eine Annahme oder sonstige Bearbeitung durch die Post.[947] Demnach kann sich der Betreiber des Empfängerservers nicht dadurch seiner Verpflichtung entziehen, dass er die Email, wenn er sie positiv gescannt hat, nicht zur Bearbeitung annimmt und dies möglichst, bevor der vollständige Nachrichteninhalt übermittelt ist. Vielmehr ist auch hier das Vertrauen in die Zuverlässigkeit des Fernmeldeverkehrs zu schützen.

Deshalb ist davon auszugehen, dass § 206 Abs. 2 Nr. 2 StGB auch in den Fällen eingreift, in denen die Daten nur teilweise den Server erreicht haben.

---

[943] OLG Karlsruhe, MMR 2005, S. 180; so auch: *Heidrich/Tschoepe*, MMR 2004, S. 77
[944] *Heidrich/Tschoepe*, MMR 2004, S. 77 f.; *Schmidl*, DuD 2005, S. 269
[945] *Heidrich/Tschoepe*, MMR 2004, S. 78; *Lehnhardt*, DuD 2003, S. 488; im Ergebnis ebenso: *Cornelius/Tschoepe*, K & R 2005, S. 270
[946] vgl.: 2. Kap. Teil 2 A. II. 3. b) aa) (3)
[947] vgl.: 2. Kap. Teil 2 A. II. 3. b) aa) (3)

(b) Anvertrautsein einer Spammail

Im Bereich der Email-Werbung stellt sich eine weitere Frage und zwar, ob im Fall einer massenhaft versandten Spammail, die ohne vorherige Einwilligung des Adressaten versandt wurde, überhaupt davon gesprochen werden kann, dass diese dem Unternehmen anvertraut ist.

Dagegen lässt sich anführen, dass die Versender solcher rechtswidriger Nachrichten, anders als dies bei legitimen Emails der Fall ist, kein Vertrauen darauf entfalten können, dass die von ihnen massenweise versandten Emails bestimmte Empfänger oder eine bestimmte Anzahl von Empfängern erreichen. Das Versenden solcher Nachrichte ohne vorherige Einwilligung des Adressaten ist vielmehr -wie oben dargestellt- grundsätzlich rechtswidrig,[948] so dass für den Fall, dass diese nicht zugestellt werden, das durch § 206 Abs. 2 Nr. 2 StGB geschützte Rechtsgut, nämlich das Vertrauen der Allgemeinheit in die Sicherheit und Zuverlässigkeit des Post- und Telekommunikationsverkehrs,[949] nicht tangiert wird. Insofern wird argumentiert, dass der Schutzzweck des § 206 Abs. 2 Nr. 2 StGB konterkariert werde, wenn der Schutz der Vorschrift auch den Versendern von Spammails zugebilligt würde. Dem Tatbestandsmerkmal des Anvertrautseins wohne ein Element der berechtigten Zustellungserwartung inne, die bei Spam nicht gegeben sei.[950]

Dafür, dass auch Spammails im Sinne des § 206 Abs. 2 Nr. 2 StGB anvertraut sein können, spricht allerdings, dass die Vorschrift alle tatsächlichen Teilnehmer am Fernmeldeverkehr schützt, also nicht nur die berechtigten Inhaber von Fernmeldeanschlüssen.[951] Beim Merkmal des Anvertrautseins ist daher nicht auf die subjektiven Absichten des Absendenden, sondern nur auf objektive Kriterien abzustellen.[952] Ein geeignetes objektives Merkmal ist die RFC-Konformität[953] der versandten Email.[954]
Folglich ist davon auszugehen, dass Emails dann einem Unternehmen anvertraut sind, wenn sie RFC-konform versandt wurden.[955]

(4) Unterdrücken

Fraglich ist, ob in dem Löschen, Blockieren, Markieren oder Umleiten einer positiv gescannten Email ein Unterdrücken im Sinne des § 206 Abs. 2 Nr. 2 StGB zu sehen ist.
Dies wird im Telekommunikationsbereich angenommen, wenn in den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten mittels Telekommunikationsanlagen eingegriffen wird, mit der Folge, dass die Nachrichten ihr Ziel nicht oder nur noch verstümmelt oder unvollständig erreichen.[956] Im Postbereich wird von einem Unterdrücken gesprochen, wenn die Sendung dem ordnungsgemäßen Postverkehr entzogen wird und zwar auch dann, wenn der Gewahrsam des Postunternehmens bestehen

---

[948] vgl.: 2. Kap. Teil 1
[949] *Hoyer* in Systematischer Kommentar, § 206 StGB, Rn. 3; *Lackner/Kühl*, § 206 StGB, Rn. 1; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 2; *Träger* in Leipziger Kommentar, § 206 StGB, Rn. 4; *Tröndle/Fischer*, § 206 StGB, Rn. 1; a.A.: *Altenhain* in Münchener Kommentar, § 206 StGB, Rn. 3 ff.
[950] *Schmidl*, DuD 2005, S. 270
[951] *Heidrich/Tschoepe*, MMR 2004, S. 77; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 6
[952] für den ähnlichen Fall virenbehafteter Emails: *Lehnhardt*, DuD 2003, S. 488
[953] vgl. zum Begriff: 1. Kap. Teil 1 B. 6.
[954] *Heidrich/Tschoepe*, MMR 2004, S. 77
[955] ebenso: *Heidrich/Tschoepe*, MMR 2004, S. 77
[956] OLG Karlsruhe, MMR 2005, S. 180; *Heidrich/Tschoepe*, MMR 2004, S. 77; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 20; *Tröndle/Fischer*, § 206 StGB, Rn. 15

bleibt.[957] Ein nur vorübergehendes Entziehen genügt, so etwa ein kurzzeitiges Verstecken eines Briefs, um diesen nicht sofort, sondern erst am nächsten Morgen zustellen zu müssen.[958]

Durch ein Blockieren der Nachricht wird in den Vorgang des Empfangens eingegriffen, mit dem Ergebnis, dass die Nachricht ihr Ziel nicht erreicht. Demnach ist das Blockieren der Nachricht als ein Unterdrücken im Sinne des § 206 Abs. 2 Nr. 2 StGB anzusehen.[959]

Es stellt sich die Frage, ob auch das Löschen von Emails ein Unterdrücken im Sinne des § 206 Abs. 2 Nr. 2 StGB darstellt. Dabei sind zwei Fälle zu unterscheiden und zwar einerseits das Löschen auf dem Empfänger-Mailserver eingegangener, aber noch nicht in die Mailbox des Empfängers eingestellter Nachrichten, andererseits das Löschen solcher Nachrichten, die bereits an die Mailbox des Empfängers weitergeleitet wurden.
In der erstgenannten Konstellation ist von einem Unterdrücken der Nachricht auszugehen. Denn hier wird durch das Löschen in den Vorgang des Empfangens eingegriffen, mit dem Ergebnis, dass die Nachricht ihr Ziel nicht mehr erreicht.
Demgegenüber ist in den Fällen, in denen die Nachricht erst nach dem Speichern in der Mailbox des Empfängers, etwa in einem gesonderten Spam-Ordner, gelöscht wird, fraglich, ob hierin ein Unterdrücken im Sinne des § 206 Abs. 2 Nr. 2 StGB gesehen werden kann.

Dagegen spricht auf den ersten Blick, dass der Empfänger nach dem Einstellen der Nachricht in der Mailbox zumindest die theoretische Möglichkeit der Kenntnisnahme hat.[960] Es könnte folglich davon auszugehen sein, dass das Übermittlungsrisiko ab dem Einstellen in der Mailbox des Empfängers nicht mehr besteht, mit der Folge, dass bei einem Löschen bereits in die Mailbox eingestellter Nachrichten kein Unterdrücken mehr angenommen werden kann. Insofern könnte das Vorliegen eines Eingriffs in den Vorgang des Aussendens, Übermittelns und Empfangen von Nachrichten mit dem Argument abzulehnen sein, dass die Nachricht ihr Ziel mit Eingang in der Mailbox bereits erreicht hat. Dafür wird teilweise angeführt, Kern des Fernmeldeverkehrs sei nach dem natürlichen Sprachsinn die Bewegung.[961] Während der Phase des Ruhens einer Nachricht finde jedoch gerade keine Bewegung statt, so dass davon auszugehen sei, dass bei einem Zugriff auf die gespeicherten Daten nicht in den Fernmeldeverkehr eingegriffen werde.[962]

Gegen die soeben genannten Auffassung könnte allerdings die das Fernmeldegeheimnis betreffende Rechtsprechung zur zeitlichen Reichweite des Telekommunikationsvorgangs sprechen. Zwar ist hier nicht das Fernmeldegeheimnis, sondern das Übermittlungsrisiko betroffen. Allerdings spricht Einiges für eine deckungsgleiche Auslegung, da sowohl Eingriffe in die Vertraulichkeit der Kommunikation, als auch das Unterdrücken von Nachrichten aus dem Einsatz von Transportpersonen resultiert und insofern dieselbe Zeitspanne umfasst.

---

[957] RGSt 1, S. 115; RGSt 52, S. 249; RGSt 72, S. 197; BGHSt 19, S. 32; OLG Hamm, NJW 1980, S. 2321; *Lackner/Kühl*, § 206 StGB, Rn. 10; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 20; *Träger* in Leipziger Kommentar, § 206 StGB, Rn. 30
[958] RGSt 28, S. 100 f.; RGSt 52, S. 248 f.; RGSt 72, 197; BGH, NJW 1963, S. 1631; OLG Celle, NJW 1957, S. 1290; OLG Hamm, NJW 1980, S. 2321; OLG Köln, NJW 1987, S. 2596; KG, JZ 1977, S. 427; *Hoyer* in Systematischer Kommentar, § 206 StGB, Rn. 30; *Lackner/Kühl*, § 206 StGB, Rn. 10; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 20
[959] ebenso: *Heidrich/Tschoepe*, MMR 2004, S. 78
[960] *Schmidl*, DuD 2005, S. 270
[961] *Palm/Roy*, NJW 1996, S. 1793; *Dies*., NJW 1997, S. 1904
[962] *Palm/Roy*, NJW 1996, S. 1793; *Zerres* in Scheurle/Mayen, § 85 TKG, Rn. 11; aA.: BGH, NJW 1997, S. 1935; LG Hanau, NJW 1999, S. 3647

Hinsichtlich der Eingriffsbefugnisse nach den §§ 100 a, b StPO, die die Überwachung und Aufzeichnung der Telekommunikation betreffen, hat der Bundesgerichtshof entschieden, dass diese auch bei einem Zugriff auf Nachrichten anzuwenden sind, die in einer Mailbox gespeichert sind.[963] Dies begründet das Gericht damit, dass der Vorgang der Übermittlung noch nicht abgeschlossen ist, wenn Nachrichten in eine Mailbox eingestellt werden, da der technische Bereich der Fernmeldeanlage dabei nicht verlassen wird.[964] Nach der genannten Rechtsprechung gehören somit Nachrichten, die in einer Mailbox gespeichert sind, noch zum Fernmeldeverkehr, weshalb auch von einem Eingriff in den Übermittlungsvorgang und somit von einem Unterdrücken auszugehen sein könnte. Unlängst erging ein Urteil des Bundesverfassungsgerichts zur Frage der Reichweite des Schutzes des Art. 10 Abs. 1 GG.[965] Das Gericht entschied, dass der Schutz des verfassungsrechtlich geschützten Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG in dem Moment endet, in dem die Nachricht sich im Herrschaftsbereich des Empfängers befindet und der Übertragungsvorgang beendet ist.[966] Der Schutz der Fernmeldegeheimnisses reicht also bis zu dem Augenblick, in dem die Nachricht bei dem Empfänger angekommen ist, da sie ab diesem Zeitpunkt nicht mehr dem Zugriff Dritter ausgesetzt ist.[967] Bereits abgerufene Nachrichten kann der Empfänger bei sich speichern, so dass sie sich in seinem Herrschaftsbereich befinden.[968] Somit ist nach der Rechtsprechung auf die Beendigung der Zugriffsmöglichkeit der Transportperson und nicht wie nach der soeben genannten Auffassung einzig darauf abzustellen, ob sich die Nachricht in Bewegung befindet. Wenn die Email vor dem Abruf auf dem Server des Empfängers gespeichert wird, ist noch nicht in den alleinigen Herrschaftsbereich des Empfängers gelangt. In diesem Fall ist somit noch immer der Vorgang der Telekommunikation betroffen,[969] in den durch Löschen der Nachricht eingegriffen werden kann.
Daneben ist zu berücksichtigen, dass der Empfänger auch durch ein Löschen der Nachricht nach deren Eingang und Speicherung in der Mailbox beeinträchtigt wird. Denn für ihn ist in der Regel nicht entscheidend, ob die Möglichkeit der Kenntnisnahme bestand, sondern, ob er letztlich Kenntnis genommen hat und selbst entscheiden konnte, wie er mit der Email weiter verfahren möchte. Auch dieser Umstand spricht für eine Qualifikation des Vorgangs des Löschens aus der Mailbox als Unterdrücken in Sinne des § 206 Abs. 2 Nr. 2 StGB. Die Übermittlung ist somit ein einheitlicher Vorgang, der erst dann endet, wenn der Abruf durch den Empfänger erfolgt ist. Insofern liegt ein Eingriff in den Vorgang des Empfangens vor, wenn die Nachricht vor dem Abruf aus der Mailbox des Empfängers gelöscht wird. Erst nach diesem Zeitpunkt ist bei einem Löschen nicht mehr der Telekommunikationsvorgang betroffen. Ein nach dem Abruf erfolgtes Löschen von auf dem Server vorgehaltenen Kopien kann nicht mehr als Eingriff in den Vorgang des Empfangens angesehen werden und stellt folglich kein Unterdrücken der Nachricht dar.[970]

Im Fall des Markierens wird die Nachricht zwar als spamverdächtigt gekennzeichnet, sie erreicht jedoch den Empfänger. Insofern ist in diesem Fall nicht von einem Unterdrücken auszugehen.

---

[963] BGH, NJW 1997, S. 1934 ff., 1935; LG Hanau, NJW 1999, S. 3647
[964] BGH, NJW 1997, S. 1934 ff., 1935; LG Hanau, NJW 1999, S. 3647
[965] BVerfG, NJW 2006, S. 976 ff.
[966] BVerfG, NJW 2006, S. 976 ff.
[967] BVerfG, NJW 2006, S. 976 ff., 978; vgl. auch: BVerwGE 79, S. 110 ff., 115 (Eingreifen des Fernmeldegeheimnisses hinsichtlich in einem Postfach auf dem Postamt befindlicher Sendungen); *Bär*, MMR 2005, S. 524; *Bizer* in Alternativkommentar, Art. 10 GG, Rn. 67; *R. Günther*, NStZ 2005, S. 489; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 24; *Hermes* in Dreier, Art. 10 GG, Rn. 42; *Lührs*, wistra 1995, S. 20; *Welp*, NStZ 1994, S. 295; vgl. auch: Gliederungsziffer
[968] vgl.: 2. Kap. Teil 2 A. I. 2. a)
[969] vgl.: 2. Kap. Teil 2 A. I. 2. c) bb)
[970] vgl.: 2. Kap. Teil 2 A. I. 2. a)

Teilweise werden die eingehenden Emails, die als spamverdächtigt erkannt werden, umgeleitet. Fraglich ist, ob dieses Umleiten als Unterdrücken im Sinne des § 206 Abs. 2 Nr. 2 StGB zu qualifizieren ist.
Werden positiv gescannte Nachrichten in einen Quarantäneordner umgeleitet, auf den der Empfänger Zugriff hat, so wird nicht bewirkt, dass die Nachricht ihr Ziel nicht oder nur verstümmelt oder unvollständig erreicht. Insofern tangiert das bloße Umleiten der Nachricht nicht den Zweck der Norm, das Vertrauen der Bevölkerung in die Telekommunikation zu schützen. Denn da die Email beim Empfänger ankommt, steht die Zuverlässigkeit der Telekommunikation bei einem Umleiten der Email in einen Spam-Ordner nicht in Frage. Demnach ist davon auszugehen, dass ein Umleiten in einen speziellen Spam-Ordner, auf den der Empfänger Zugriff hat, den Tatbestand des Unterdrückens im Sinne des § 206 Abs. 2 Nr. 2 StGB nicht erfüllt. Etwas anderes gilt nach den soeben dargestellten Grundsätzen dann, wenn die Nachricht ausnahmsweise in einen Ordner umgeleitet wird, auf den der Empfänger keinen Zugriff hat. In diesem Fall wird auf den Vorgang des Nachrichtenempfangs eingewirkt, so dass von einem Unterdrücken auszugehen ist.

(5) Unbefugt

Weitere Voraussetzung des § 206 Abs. 2 Nr. 2 StGB ist, dass derjenige, der die Filtersoftware einsetzt, unbefugt handelt.
Der Täter handelt unbefugt, wenn nicht die Einwilligung der betroffenen Rechtsträger vorliegt. Die Einwilligung lässt dabei bereits die Tatbestandsmäßigkeit des Handelns entfallen.[971] Hier ist fraglich, ob es als ausreichend anzusehen ist, wenn der Empfänger seine Einwilligung erteilt oder ob sich alle am Fernmeldevorgang Beteiligten, also auch der Absender mit den Maßnahmen einverstanden erklären müssen, damit der Tatbestand des § 206 Abs. 2 Nr. 2 StGB entfällt.

Für ein Erfordernis der Einwilligung beider Kommunikationspartner spricht dabei auf den ersten Blick die Rechtsprechung des Bundesverfassungsgerichts.
Das Gericht entschied in Bezug auf Art. 10 Abs. 1 GG, dass ein Eingriff in die Vertraulichkeit der Kommunikation zu seiner Rechtfertigung der Einwilligung beider Kommunikationspartner bedarf.[972] Ebenso wie im Bereich des Art. 10 Abs. 1 GG sind auch hier zwei Personen betroffen, zwischen denen der Kommunikationsvorgang stattfindet. Demnach ist es an sich naheliegend, die vom Bundesverfassungsgericht entwickelten Grundsätze auf die Einwilligung im strafrechtlichen Bereich zu übertragen.[973] Des Weiteren lässt sich aus dem Umstand ein Argument für das Erfordernis der Einwilligung beider Kommunikationspartner ableiten, dass § 206 StGB nicht nur den Schutz der Allgemeinheit bezweckt, sondern auch den der einzelnen an einem Kommunikationsvorgang beteiligten

[971] OLG Karlsruhe, MMR 2005, S. 180; *Altenhain* in Münchener Kommentar, § 206 StGB, Rn. 41; *Heidrich/Tschoepe*, MMR 2004, S. 78; *Jung* in Kindhäuser/Neumann/Paeffgen, § 206 StGB, Rn. 18; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 11; a.A.: *Tröndle/Fischer*, § 206 StGB, Rn. 9
[972] BVerfGE 85, S. 399
[973] für das Erfordernis der Einwilligung beider Kommunikationsteilnehmer: OLG Karlsruhe, MMR 2005, S. 180; *Cornelius/Tschoepe*, K & R 2005, S. 270; *Hoyer* in Systematischer Kommentar, § 206 StGB, Rn. 39; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 12; *Schmidl*, DuD 2005, S. 270; *Tröndle/Fischer*, § 206 StGB, Rn. 9; für das Erfordernis der Einwilligung beider Kommunikationsteilnehmer speziell im Hinblick auf das Fernmeldegeheimnis: OLG Saarbrücken, NStZ 1991, S. 386; OVG Bremen, CR 1994, S. 703; *Amelung/Pauli*, MDR 1980, S. 801 ff.; *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 339 f.; *Gusy*, JuS 1986, S. 95; *Lisken*, NJW 1994, S. 2070; *Sternberg-Lieben*, Jura 1995, S. 300 f.; gegen das Erfordernis der Einwilligung beider Kommunikationsteilnehmer: *Heidrich*, MMR 2005, S. 182; *Ders./Tschoepe*, MMR 2004, S. 78

Personen.[974] Aufgrund dieser Argumentation wurde das Erfordernis der Einwilligung beider Kommunikationsteilnehmer von der Rechtsprechung bejaht.[975]
Die Anwendung der von der Rechtsprechung entwickelten Grundsätze ist im vorliegenden Fall allerdings fragwürdig. Denn hier wird eine das Verfassungsrecht betreffende Rechtsprechung unbesehen auf das Strafrecht übertragen.[976] Das Strafrecht verfügt jedoch über eine eigene Einwilligungsdogmatik.[977] Danach kann die Einwilligung nur durch den Inhaber des jeweils durch die Tat verletzten Rechtsguts erklärt werden.[978] Für die Beantwortung der Frage nach der Person bzw. den Personen, die hier ihre Einwilligung zu erklären haben, ist demnach auf die von § 206 Abs. 2 Nr. 2 StGB umfassten Schutzgüter abzustellen. Dabei verfolgen einige der im Tatbestand des § 206 StGB enthaltenen Alternativen ähnliche Intentionen, wie Art. 10 GG, allerdings decken sich die Vorschriften nicht völlig.[979]
Art. 10 GG will den Gefahren für die Vertraulichkeit der Mitteilung begegnen, indem der Kommunikationsinhalt und die näheren Informationen über den Kommunikationsvorgang vor Kenntnisnahme, Aufzeichnung und Verwertung durch staatliche Stellen geschützt werden.[980] Hingegen erfasst die Vorschrift nicht das ebenfalls durch die Einschaltung eines Nachrichtenübermittlers entstehende Übermittlungsrisiko.[981] Deshalb wird der Schutzbereich des Art. 10 GG nicht durch das Unterdrücken einer Nachricht berührt.
§ 206 Abs. 2 Nr. 2 StGB schützt dagegen einerseits Individualinteressen, nämlich das Interesse des Betroffenen an dem ordnungsgemäßen Umgang mit der Sendung, andererseits das Allgemeininteresse, das in dem öffentlichen Vertrauen in die Sicherheit und Zuverlässigkeit des Post- und Telekommunikationsverkehrs besteht.[982] Das durch § 206 Abs. 2 Nr. 2 StGB geschützte Individualinteresse stellt aus Empfängersicht sicher, dass der Übermittler an ihn gerichtete Sendungen zustellt und nicht eigenmächtig unterdrückt.[983] Grundsätzlich wird auch der Absender davon ausgehen dürfen, dass seine Sendung an den Empfänger zugestellt wird.[984] Hierbei ist allerdings zu beachten, dass es dem Empfänger freisteht, darüber zu entscheiden, ob er von einer Sendung Kenntnis nehmen oder sie unbesehen zurückschicken oder vernichten möchte. In diesem Kontext wird relevant, dass dem Empfänger das Recht zukommt, von unerwünschter Werbung verschont zu bleiben.[985]

---

[974] *Altenhain* in Münchener Kommentar, § 206 StGB, Rn. 3 ff.; *Cornelius/Tschoepe*, K & R 2005, S. 270; *Hoyer* in Systematischer Kommentar, § 206 StGB, Rn. 3; *Lackner/Kühl*, § 206 StGB, Rn. 1; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 2; *Träger* in Leipziger Kommentar, § 206 StGB, Rn. 4; *Tröndle/Fischer*, § 206 StGB, Rn. 1
[975] OLG Karlsruhe MMR 2005, S. 180
[976] *Kitz*, CR 2005, S. 452
[977] vgl. etwa: BGHSt 4, S. 90; BGHSt 17, S. 360; *Amelung/Eymann*, JuS 2001, S. 937 ff.; *Bichlmeier*, JZ 1980, S. 53 ff.; *Göbel*, a.a.O., S. 1 ff.; *Ostendorf*, JuS 1982, S. 433; *Rönnau* in Leipziger Kommentar, vor § 32 StGB, Rn. 146 ff.; *H. Schild*, Jura 1982, S. 525; *Schlehofer* in Münchener Kommentar, vor §§ 32 StGB, Rn. 112 ff.
[978] *Haft*, Strafrecht, Allgemeiner Teil, S. 75; *Paul*, a.a.O., S. 81 ff.; *Rönnau* in Leipziger Kommentar, vor § 32 StGB, Rn. 176; *Schlehofer* in Münchener Kommentar, vor §§ 32 StGB, Rn. 113; *Tröndle/Fischer*, vor § 32 StGB, Rn. 3 b
[979] BT-Drs. 13/8453, S. 12; *Graf* in Münchener Kommentar, vor § 201 StGB, Rn. 2; *Hoyer* in Systematischer Kommentar, vor § 201 StGB, Rn. 3, § 206 StGB, Rn. 4; *Kindhäuser*, Lehr- und Praxiskommentar, § 206 StGB, Rn. 1; *Kitz*, CR 2005, S. 452; *Lackner/Kühl*, § 206 StGB, Rn. 1; *Löwer* in Maunz/Dürig, Art. 10 GG Rn. 15; *Träger* in Leipziger Kommentar, § 206 StGB, Rn. 4
[980] BVerfGE 85, S. 398; BVerfGE 100, S. 366; BVerfGE 106, S. 36; BVerfGE 110, S. 53; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 51 ff.; *Jarass* in Jarass/Pieroth, Art. 10 GG, Rn. 1; *Löwer* in von Münch/Kunig, Art. 10 GG, Rn. 2, 11 ff.
[981] vgl.: 2. Kap. Teil 2 A. I. 2. c) aa)
[982] vgl.: 2. Kap. Teil 2 A. III. 3. b) aa) (2) und (4)
[983] *Kargl* in Kindhäuser/Neumann/Paeffgen, § 206 StGB, Rn. 3; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 2; *Tröndle/Fischer*, § 206 StGB, Rn. 13
[984] *Kitz*, CR 2005, S. 453
[985] vgl.: 2. Kap. Teil 1

Demnach kann der Empfänger einen Brief ungeöffnet an den Übermittler zurückgeben oder diesen anweisen, den Brief vor den Augen des Absender zu zerreißen oder die Annahme bestimmter Sendungen -hierunter fallen Emails ebenso wie Briefe- bereits im Voraus verweigern, mit der Folge, dass der Übermittler sie ihm gar nicht erst zustellt.[986] In diesem Fall verwirklicht der Übermittler im Auftrag des Empfängers dessen Rechte.[987] Es ist also zu beachten, dass das Versenden unverlangter Werbe-Emails eine Verwirklichung des Straftatbestands des § 303 a Abs. 1 StGB darstellt, wenn der Empfänger in kurzer Zeit so viele Werbe-Emails erhält, dass er die erwünschten Emails von den Werbenachrichten nicht mehr unterscheiden kann.[988] Daneben ist von einer unlauteren Wettbewerbshandlung auszugehen, wenn Email-Direktwerbung verschickt wird, ohne dass die Einwilligung des Adressaten oder die in § 7 Abs. 3 UWG genannte Ausnahmekonstellation vorliegt, vgl. §§ 7 Abs. 1, Abs. 2 Nr. 3 UWG.[989] Auch nach dem allgemeinen Zivilrecht ist Email-Werbung unzulässig. Ihr steht § 823 Abs. 1, 2 BGB in Verbindung mit § 249 Abs. 1 BGB bzw. § 1004 Abs. 1 BGB entgegen.[990] Zum einen verletzt der Versender den Empfänger der Email-Werbung durch das Zusenden der Nachricht in seinem allgemeinen Persönlichkeitsrecht.[991] Zum anderen kann der Straftatbestand des § 303 a Abs. 1 StGB verwirklicht sein, der als Schutzgesetz im Sinne des § 823 Abs. 2 BGB zu qualifizieren ist.[992] Gerechtfertigt werden kann die Zusendung der Werbe-Email, wenn zuvor die Einwilligung des Empfängers eingeholt wird.[993]

Auf Ebene des Verfassungsrechts lässt sich das Recht, von unerwünschter Email-Werbung frei zu bleiben aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG herleiten.[994] Da jedoch lediglich natürliche Personen Grundrechtsträger des allgemeinen Persönlichkeitsrechts sind, ist der Grundrechtsschutz juristischer Personen und gleichgestellter Personenvereinigungen auf Art. 2 Abs. 1 GG zu stützen.[995] Das Recht auf Abwehr unerwünschter Kommunikation ist auch auf internationaler Ebene geschützt und zwar durch das Gemeinschaftsgrundrecht auf Privatleben, Art. 8 Abs. 1 EMRK sowie Art. 17 IPbürgPR.[996]

Diese Rechte verwirklicht der Übermittler, wenn er auf Anweisung des Adressaten die Zustellung der Email unterlässt. Deshalb ist davon auszugehen, dass von § 206 Abs. 2 Nr. 2 StGB geschützte Individualinteressen des Absenders nicht betroffen sind, wenn der Übermittler dem Empfänger eine Sendung auf dessen eigenen Wunsch hin nicht zustellt und gegebenenfalls vernichtet.[997]

Demnach kann bei Vorliegen der Einwilligung des Empfängers in das Unterdrücken der Nachricht nur noch das durch die Vorschrift ebenfalls geschützte Allgemeininteresse in Form des öffentlichen Vertrauens in die Sicherheit und Zuverlässigkeit des Post- und Telekommunikationsverkehrs das Eingreifen der Vorschrift gebieten. Nach der strafrechtlichen Einwilligungsdogmatik kann der Einzelne auf ein Universalrechtsgut der Allgemeinheit auch dann nicht verzichten, wenn ein Tatbestand zugleich

---

[986] vgl.: 2. Kap. Teil 1
[987] *Kitz*, CR 2005, S. 453
[988] vgl.: 2. Kap. Teil 1 A. I.
[989] vgl.: 2. Kap. Teil 1 A. II.
[990] vgl.: 2. Kap. Teil 1 A. III.
[991] vgl.: 2. Kap. Teil 1 A. III. 1. a) aa)
[992] vgl.: 2. Kap. Teil 1 A. I.; 2. Kap. Teil 1 A. III. 2. b)
[993] vgl.: 2. Kap. Teil 1 A. I. 3; 2. Kap. Teil 1 A. II; 2. Kap. Teil 1 A. III. 1. c)
[994] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[995] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[996] vgl.: 2. Kap. Teil 1 B. II. 2.
[997] Kitz, CR 2005, S. 453; im Ergebnis auch: *Heidrich*, MMR 2005, S. 182; *Hoeren*, NJW 2004, S. 3515; a.A.: OLG Karlsruhe, MMR 2005, S. 180 f.; *Schmidl*, MMR 2005, S. 345 f.

Individualrechtsgüter schützt.[998] Allerdings wird das Allgemeingut nicht tangiert, soweit der Empfänger sein Einverständnis mit den genannten Maßnahmen erklärt hat. Denn an der grundsätzlichen Funktionsfähigkeit des Telekommunikationsverkehrs dürften keine Zweifel aufkommen, so lange der Übermittler nicht eigenmächtig Sendungen unterdrückt, sondern lediglich im Auftrag des Empfängers handelt.[999] Somit liegt hier eine andere Interessenslage vor, als im vom Bundesverfassungsgericht entschiedenen Fall.[1000] Der Rechtsprechung dahingehend, dass nur die Einwilligung beider Kommunikationspartner den Eingriff rechtfertigen kann, muss demnach nicht gefolgt werden.

Darüber hinaus würde die Annahme der Erforderlichkeit der Einwilligung auch des Absenders der Nachricht dazu führen, dass die Mehrzahl der gegen die Versender von Spammails gerichteten Maßnahmen nur mit dessen Einverständnis möglich wäre. Da dieser jedoch an der Zustellung interessiert ist, wird er seine Einwilligung grundsätzlich nicht erklären. Daneben wäre es für denjenigen, der den Filter einsetzt nicht realisierbar, jeden einzelnen Spam-Versender aufzufinden und um seine Einwilligung zu bitten. Das Erfordernis der Einwilligung auch des Absenders würde demnach dazu führen, dass dieser den Empfänger dazu zwingen könnte, unerwünschte Nachrichten entgegenzunehmen.[1001] Dem Empfänger muss es jedoch, wie eben erwähnt, gerade freigestellt sein, selbst zu entscheiden, welche Nachrichten er erhalten möchte und welche nicht. Um die Versender von Spammails nicht zu begünstigen, während die Empfänger letztlich machtlos gestellt sind, muss es für die Straffreiheit daher ausreichen, wenn der Empfänger seine Einwilligung erklärt hat.[1002]

Anders entschied allerdings das OLG Karlsruhe in dem oben genannten Urteil.[1003] Allerdings existiert noch keine gefestigte Rechtsprechung zu dieser Frage. Insofern muss abgewartet werden, ob an dem Erfordernis der Einwilligung beider Kommunikationspartner festgehalten wird. Folgt man der hier vertretenen Auffassung, die lediglich die Einwilligung des Empfängers für erforderlich hält, so ist zu beachten, dass die Einwilligung nicht nur in Bezug auf Spammails, sondern auf sämtliche spamverdächtige Emails eingeholt wird, da nur so auch die Strafbarkeit für das Löschen von false positives ausgeräumt werden kann.[1004]

bb) Subjektiver Tatbestand

Der subjektive Tatbestand ist erfüllt, wenn der Täter zumindest bedingt vorsätzlich handelt.[1005]
Dies ist hier grundsätzlich der Fall, da die Maßnahmen mit dem Ziel vorgenommen werden, die spamverdächtigen Nachrichten abzuwehren. Der Täter wird -angesichts der noch bestehenden Defizite bei der Filterung-[1006] auch damit rechnen, dass nicht nur Spammails, sondern bisweilen fälschlicherweise auch legitime Nachrichten gelöscht werden.

---

[998] BGHSt 6, S. 234; BGHSt 23, S. 264; BGH, NStZ 2004, S. 205; *Cramer/Heine/Lenckner* in Schönke/Schröder, Vorbem. §§ 32 ff. StGB, Rn. 36; *Duttge*, Jura 2006, S. 16; *Haft*, Strafrecht, Allgemeiner Teil, S. 74; *Paul*, a.a.O.; *Rönnau*, Jura 2002, S. 666 f.; *Ders*. in Leizipger Kommentar, vor § 32 StGB, Rn. 76
[999] *Kitz*, CR 2005, S. 453; *Koecher*, DuD 2005, S. 164
[1000] vgl.: BVerfGE 85, S. 399
[1001] ebenso: *Koecher*, DuD 2005, S. 164; ähnlich: *Heidrich*, MMR 2005, S. 182
[1002] ebenso: *Heidrich/Tschoepe*, MMR 2004, S. 76; *Heidrich*, MMR 2005, S. 182; *Kitz*, CR 2005, 453; tendenziell: Hoeren, NJW 2004, S. 3515; a.A.: OLG Karlsruhe, MMR 2005, S. 180; *Schmidl*, MMR 2005, S. 346
[1003] OLG Karlsruhe MMR 2005, S. 180
[1004] vgl. zu false positives.: 2. Kap. Teil 1 A. I.
[1005] BGHSt 7, S. 363; BGHSt 21, S. 283; BGHSt 36, S. 9; BGH, NStZ 1984, S. 19; BGH, NStZ 1988, S. 175; BGH, NStZ 1998, S. 616
[1006] vgl.: 1. Kap. Teil 2; vgl. auch: *Dietrich/Pohlmann*, DuD 2005, S. 550; *Hoeren*, NJW 2004, S. 3515; *Spindler/Ernst*, CR 2004, S. 438

cc) Rechtswidrigkeit

Fraglich ist, ob die tatbestandsmäßigen Handlungen rechtswidrig sind. Die Rechtswidrigkeit würde entfallen, wenn sich derjenige, der den Filter einsetzt, auf einen Rechtfertigungsgrund berufen könnte. In Betracht kommen § 109 TKG (1) oder § 34 StGB (2).

(1) § 109 TKG

Der Filtereinsatz könnte einerseits durch § 109 Abs. 1 TKG gerechtfertigt sein. Danach hat jeder Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen. Der Einsatz der Filtersoftware dient allerdings nicht diesen Zwecken, sondern soll einerseits die Kunden des Providers vor unerwünschter elektronischer Post, andererseits das System des Providers vor Überlastung schützen. Demnach greift § 109 Abs. 1 TKG hier nicht ein.

Möglicherweise ist der Einsatz der Filtersoftware jedoch durch § 109 Abs. 2 S. 1 TKG gerechtfertigt. Danach haben Betreiber von Telekommunikationsanlagen für die Öffentlichkeit bei den zu diesen Zwecken betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Verpflichtet sind nach dem Wortlaut nur Betreiber von Telekommunikationsanlagen für die Öffentlichkeit. Demnach findet § 109 Abs. 2 TKG, anders als § 109 Abs. 1 TKG, der auf sämtliche Diensteanbieter Bezug nimmt, nicht auf die unternehmensinterne Kommunikation Anwendung.[1007] Auch das Internet ist ein Telekommunikationsnetz im vorgenannten Sinne.[1008]

Die Verpflichtung zu Schutzmaßnahmen ist auf angemessene technische Vorkehrungen oder sonstige Maßnahmen beschränkt. Durch diese Formulierung, die auf das nach Rechtsstaatsgrundsätzen ohnehin zu beachtende Übermaßverbot Bezug nimmt, verdeutlicht der Gesetzgeber, dass § 109 Abs. 2 S. 1 TKG restriktiv auszulegen ist.[1009] Fraglich ist, ob der Filtereinsatz angemessen im Sinne des § 109 Abs. 2 S. 1 TKG ist. Die Angemessenheit technischer Vorkehrungen und sonstiger Schutzmaßnahmen ist dabei nach § 109 Abs. 2 S. 4 TKG dann gegeben, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und der zu schützenden Einrichtungen für die Allgemeinheit steht.
Der technische und wirtschaftliche Aufwand für die Email-Filterung ist relativ gering, da es ausreichend ist, Software zu installieren, die sodann eingehende Emails auf ihre Eigenschaft als Spam untersucht und gegebenfalls löscht, blockiert, umleitet oder markiert.[1010] Als Rechtspositionen, die mit dem technischen und wirtschaftlichen Aufwand ins Verhältnis zu setzen sind, kommen einerseits die Rechte der Kunden des Providers in Betracht, andererseits dessen eigenen Rechte. Das Interesse der Kunden ist darauf gerichtet, von unerwünschter Email-Werbung frei zu bleiben. Der Provider versucht, durch den Filtereinsatz die

[1007] BT-Drs. 15/2316, S. 91 f.; *Bock* in Beck´scher TKG-Kommentar, 109 TKG, Rn. 30; *Schütz*, Kommunikationsrecht, Rn. 815; *Zerres* in Scheurle/Mayen, § 87 TKG, Rn. 13
[1008] BT-Drs. 15/2316, S. 58; *Bock* in Beck´scher TKG-Kommentar§ 109 TKG, Rn. 34
[1009] *Ehmer* in Beck´scher TKG-Kommentar., 2. Aufl., § 87 TKG , Rn. 19; *Kemmler*, ArchPT 1996, S. 321 ff., 329; *Schmidt/Königshofen/Zwach*, § 87 TKG, Rn. 11
[1010] vgl.: 1. Kap. Teil 2

Funktionstüchtigkeit seines Servers zu erhalten. Das Recht der Kunden, keine unerwünschte Email-Direktwerbung zu erhalten, wird durch das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG erfasst.[1011] Da dieses allerdings nur natürlichen Personen zukommt, können sich inländische juristische Personen lediglich auf das subsidiäre Recht auf allgemeine Handlungsfreiheit berufen, Art. 2 Abs. 1 GG.[1012] Das Recht auf Privatleben, das auch den Schutz vor unerwünschter Korrespondenz beinhaltet, ist auch auf gemeinschafts-, konventions- und internationaler Ebene geschützt, vgl. das nicht kodifizierte Gemeinschaftsgrundrecht auf Privatleben, Art. 8 Abs. 1 EMRK sowie Art. 17 IPbürgPR.[1013] Auch im Bereich des einfachen deutschen Rechts ist der Schutz vor unerwünschter Email-Werbung gewährleistet.[1014] Daneben hat der Provider das Recht, sein Eigentum vor dem Mißbrauch durch Dritte zu schützen.[1015]
Dem geringen technischen und wirtschaftlichen Aufwand des Filtereinsatzes stehen folglich auf verfassungsrechtlicher aber auch internationaler Ebene sowie einfachgesetzlich geschützte Rechte der Adressaten unerwünschter Email-Werbung sowie eigene Rechte des Providers entgegen. Angesichts der Tatsache, dass Email zu einem der meistgenutzten Kommunikationsmittel gehört, kommt dem Schutz der Telekommunikationsanlage eine hohe Bedeutung zu. Folglich steht der zu erbringende Aufwand, nämlich der Einsatz der Filtersoftware in einem angemessenen Verhältnis zu den zu schützenden Rechten und Einrichtungen. Der Filtereinsatz stellt demnach eine angemessene technische Vorkehrung im Sinne des § 109 Abs. 2 S. 1 TKG dar.

Diese müsste dem Schutz gegen Störungen dienen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen. Es stellt sich also die Frage, ob es sich bei den durch Spammails ausgelösten Folgen um erhebliche Beeinträchtigungen im Sinne des § 109 Abs. 2 S. 1 TKG handelt.
Wird eine Vielzahl von Nachrichten zugestellt, so kann dies einerseits zu überquellenden Mailboxen führen, mit der Folge, dass erwünschte Kommunikation nicht mehr zugestellt werden kann.[1016] Andererseits resultiert das Aufkommen an Werbe-Emails in einer Belastung des Netzwerks, das die Geschwindigkeit des Datenstroms und damit die Funktionsfähigkeit des Internets als Ganzes beeinträchtigt.[1017] Dabei steigt der Anteil von Spammails am gesamten Email-Aufkommen stetig an, so dass zu erwarten ist, dass die Auswirkungen auf das Kommunikationsmedium sich noch verstärken.[1018] Aufgrund dieser Konsequenzen von Spammails könnte von einer erheblichen Beeinträchtigung auszugehen sein.
Allerdings zeigt das in § 109 Abs. 2 S. 1 TKG aufgenommene Merkmal der Erheblichkeit, dass nicht jede mögliche Beeinträchtigung des Telekommunikationsnetzes zum Erfordernis von Schutzmaßnahmen des Providers führen soll. Demnach können lediglich geringfügige Beeinträchtigungen Schutzmaßnahmen nicht rechtfertigen.[1019] Eine § 109 Abs. 2 S. 1 TKG entsprechende Verpflichtung enthält Art. 4 Abs. 1 S. 1 EK-DSRL. Auch Art. 4 Abs. 1 S. 1 EK-DSRL spricht die Verpflichtung von Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste aus, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten.

[1011] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[1012] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[1013] vgl.: 2. Kap. Teil 1 B. II. 2. a) und b)
[1014] vgl.: 2. Kap. Teil 1
[1015] *Härting/Eckart*, CR 2004, S. 120; *Hoeren*, NJW 2004, S. 3514
[1016] vgl.: 1. Kap. Teil 1 B. II. 4.
[1017] vgl.: 1. Kap. Teil 1 B. II. 4.
[1018] vgl.: 1. Kap. Teil 1 B. II. 4.
[1019] *Bock* in Beck´scher TKG-Kommentar, § 109 TKG, Rn. 33 f.; *BSI*, Antispam-Strategien, 6.5.5.; *eco*, Whitepaper, S. 21

Eine erhebliche Beeinträchtigung, die Schutzmaßnahmen des Providers und somit den Filtereinsatz rechtfertigt, wird bei der Zustellung von virenbehafteten Emails stets angenommen, da diese nicht lediglich den Rechner des Empfängers, sondern darüber hinaus das gesamte System des Providers beschädigen können.[1020] Des Weiteren wird bei Angriffen auf die IT-Infrastruktur des Providers oder Unternehmens etwa durch Mailbombing[1021] davon ausgegangen, dass eindeutig als Spam erkannte Nachrichten nach § 109 Abs. 2 S. 1 TKG vor Zustellung ohne Zustimmung des Betroffenen ausgefiltert oder die Zustellung verzögert werden darf.[1022] Dies ergibt sich aus einer Abwägung der im Raum stehenden Interessen. Dürfte der Provider im Fall einer Spamattacke eindeutig als Spam zu identifizierende Nachrichten nicht löschen oder blockieren, so wäre er letztlich nicht in der Lage, sein Eigentum vor Beeinträchtigungen zu schützen. Darüber hinaus sind die Kunden des Providers im Fall eines Zusammenbruchs des Servers für die Dauer der Funktionsunfähigkeit nicht mehr in der Lage, Emails zu senden oder zu empfangen. Würde es also den Providern verboten, den drohenden Zusammenbruch des Servers zu verhindern, so würden seine Rechte sowie diejenigen der Kunden und der Absender legitimer Emails, die sodann nicht mehr zugestellt werden können, einseitig zu Gunsten der Versender von Spammails zurückgedrängt. Demnach sollte der Provider im Notfall, also etwa im Fall eines Mailbombings, die geeigneten Maßnahmen zum Erhalt der Funktionsfähigkeit des Servers treffen dürfen. Im soeben genannten Fall ist somit davon auszugehen, dass Spammails gelöscht oder blockiert werden dürfen.[1023] Auf legitime Emails kann sich diese Befugnis des Providers jedoch nicht beziehen, da der Angriff von diesen nicht ausgeht und insofern eine Beeinträchtigung der Rechte der Absender solcher Nachrichten nicht gerechtfertigt erscheint. Werden also false positives gelöscht oder blockiert,[1024] so ist dies nicht gerechtfertigt. Zusammenfassend lässt sich somit festhalten, dass ein Löschen von Spammails zulässig ist, wenn davon auszugehen ist, dass der Email-Server ansonsten unter einer Spamattacke zusammenbricht.[1025]

Wird ein Server nicht gezielt attackiert, so ist Wahrscheinlichkeit eines Zusammenbruchs allerdings mittlerweile angesichts der technischen Entwicklung gering.[1026] Folglich kann unter normalen Umständen nicht von einer drohenden Funktionsunfähigkeit des Servers ausgegangen werden. Fraglich ist, ob in diesen Fällen Schutzmaßnahmen gerechtfertigt sind. Dies könnte man mit dem Argument bejahen, Spammails würden eine indirekte Bedrohung der Sicherheit der Dienste darstellen.[1027] Zwar gefährdet diese Art von Nachrichten für sich genommen nicht die Sicherheit der von dem Provider erbrachten Dienste.[1028] Es wird jedoch argumentiert, es würde sich eine indirekte Bedrohung durch den Einfluss versandter Spammails auf die Funktionsweise des Netzwerks und des Email-Dienstes ergeben.[1029]
Die Frage der Erforderlichkeit der Schutzmaßnahme lässt sich beantworten, wenn man die zu schützenden Interessen sowie die Wahrscheinlichkeit und die Intensität der zu erwartenden Beeinträchtigung betrachtet. Schutzgegenstand sind, wie eben erwähnt, die Rechte des Providers und seiner Kunden sowie die Funktionsfähigkeit der Anlage. Im Rahmen der Frage nach der Zulässigkeit unverlangter Werbe-Emails wurde eine Interessensabwägung zwischen

[1020] vgl.: 1. Kap. Teil 1 B. II. 5.
[1021] vgl. zum Begriff: 1. Kap. Teil 1 B. II. 4.
[1022] *BSI*, Antispam-Strategien, 6.5.5.; *Koecher*, DuD 2005, S. 165; einschränkend: *Rittweger/Schmidl*, MMR 2006, Heft 6, XI
[1023] *BSI*, Antispam-Strategien, 6.5.5.; *Koecher*, DuD 2005, S. 165
[1024] zum Begriff der false positives: 1. Kap. Teil 2 A. I.
[1025] *BSI*, Antispam-Strategien, 6.5.5.; *Koecher*, DuD 2005, S. 165
[1026] vgl.: 1. Kap. Teil 1 B. 4.
[1027] so: *Art. 29 Datenschutzgruppe*, WP 118, S. 7
[1028] *Art. 29 Datenschutzgruppe*, WP 118, S. 7
[1029] *Art. 29 Datenschutzgruppe*, WP 118, S. 7

der Kommunikations- und Berufsfreiheit der Werbetreibenden auf der einen Seite und den auf verfassungs- und gemeinschaftsrechtlicher sowie internationaler Ebene geschützten Grundrechten derjenigen Personenkreise durchgeführt, die solche Informationen nicht erhalten möchten.[1030] Im Ergebnis wurde festgestellt, dass weder den Rechten der Versender kommerzieller Emails, noch denjenigen der Adressaten, an die unverlangte Email-Werbung gesandt wird, der absolute Vorrang einzuräumen ist.[1031] Danach treten weder die Rechte der einen, noch der anderen Seite absolut zurück.[1032] Insofern kann es auch nicht zugelassen werden, dass Provider von sich aus die Zustellung bestimmter Emails an den Adressaten durch Löschen oder Blockieren verhindern. Wird Filtersoftware eingesetzt, die anhand bestimmter Kriterien Emails noch vor Einstellen in die Mailbox oder vor Abruf durch den Empfänger löscht bzw. deren Zugang blockiert, so würden hier einseitig die Rechte der Versender von Spammails und derjenigen Empfänger zurückgedrängt, die am Erhalt von Werbepost interessiert sind. Es würde durch das Tätigwerden des Providers den Rechten der Empfänger unerwünschter Email-Werbung und des Providers zur Geltung verholfen, während die Absender solcher Nachrichten in ihrem Recht faktisch beschränkt würden. Zusätzlich ist zu berücksichtigen, dass angesichts der stets vorhandenen Quote von false positives immer auch ein gewisser Prozentsatz legitimer Nachrichten von den Maßnahmen betroffen wäre. Das Löschen oder Blockieren solcher Nachrichten würde ebenfalls einen nicht zu rechtfertigenden Eingriff in die Rechte von Absender und Empfänger darstellen.[1033]
Da das Zusammenbrechen des Servers angesichts der technischen Entwicklung kaum mehr zu erwarten ist,[1034] erscheint eine Beeinträchtigung der Funktion des Servers nicht mehr als sehr wahrscheinlich. Demnach muss angesichts der in Kapitel 2 Teil 1 gefundenen Ergebnisse davon ausgegangen werden, dass das Löschen bzw. Blockieren der Nachrichten nicht erforderlich im Sinne des § 109 Abs. 2 TKG ist. Als unerhebliche Beeinträchtigungen sind somit eine durch das Volumen eingehender Spammails oder eine langsamere Funktion des Servers bewirkte Verzögerung der Nachrichten anzusehen.[1035] Auch das Überlaufen einzelner Email-Accounts kann noch nicht als erhebliche Beeinträchtigung des gesamten Netzes angesehen werden, da hier lediglich einzelne Empfänger betroffen sind, nicht jedoch die Anlage im Ganzen oder zumindest Teile des Telekommunikationsnetzes.[1036]

Somit kann sich die Zulässigkeit der fraglichen Maßnahmen nicht aus § 109 Abs. 2 S. 1 TKG ergeben.

(2) § 34 StGB

Fraglich ist, ob sich das Löschen und Blockieren positiv gescannter Emails durch § 34 StGB rechtfertigen lässt.

Voraussetzung ist, dass allgemeine Rechtfertigungsgründe wie § 34 StGB auf die vorliegende Fallkonstellation überhaupt anwendbar sind. Dies könnte deshalb zu verneinen sein, weil § 88 Abs. 3 S. 3 TKG als Rechtfertigungsgründe für Eingriffe in das Post- und Fernmeldegeheimnis nur solche Erlaubnissätze zulässt, die sich ausdrücklich auf Telekommunikationsvorgänge beziehen.

[1030] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[1031] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[1032] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[1033] vgl.: 2. Kap. Teil 1 B. I. 1. a) und b)
[1034] vgl.: Fn. 1041
[1035] im Ergebnis: *BSI*, Antispam-Strategien, 6.5.5.; vgl. auch: *Bock* in Beck´scher TKG-Kommentar, § 109 TKG, Rn. 33; *eco*, Whitepaper, S. 21
[1036] im Ergebnis: *BSI*, Antispam-Strategien, 6.5.5.; vgl. auch: *Bock* in Beck´scher TKG-Kommentar, § 109 TKG, Rn. 33; *eco*, Whitepaper, S. 21

Allerdings nimmt § 88 Abs. 3 S. 3 TKG auf die Verwendung von Kenntnissen Bezug und ist in Zusammenhang mit Abs. 1 zu sehen, was bedeutet, dass die Beschränkung des § 88 Abs. 3 S. 3 TKG dann nicht eingreift, wenn Sachverhalte betroffen sind, die außerhalb des Rahmens des § 88 Abs. 1 TKG liegen.[1037] Ein Zusammenhang des strafrechtlich relevanten Verhaltens mit Abs. 1 der Norm ist hier allerdings nicht gegeben, denn es steht kein Eingriff in das Fernmeldegeheimnis, sondern lediglich die Realisierung des Übermittlungsrisikos im Raum, das gerade nicht durch das Fernmeldegeheimnis erfasst wird.[1038] Da hier nicht die Verschaffung und Verwendung von Kenntnissen und Inhalten betroffen ist, ist folglich ein Rückgriff auf allgemeine Rechtfertigungsgründe möglich.[1039] Die Anwendbarkeit des § 34 StGB ist somit nicht durch § 88 Abs. 3 S. 3 TKG ausgeschlossen.

Fraglich ist jedoch, ob die Voraussetzungen des § 34 StGB vorliegen. Die Vorschrift lässt die Rechtswidrigkeit von Handlungen entfallen, die erfolgen, um eine nicht anders abwendbare Gefahr für ein notstandsfähiges Rechtsgut abzuwehren, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt.
Es stellt sich die Frage, ob sich der Provider oder das jeweilige Unternehmen darauf berufen kann, durch die Filtermaßnahmen eine gegenwärtige Gefahr für ein notstandsfähiges Rechtsgut abzuwehren. Ein solches Rechtsgut ist das Eigentum des Providers am Server. Daneben kommen die Rechte der Kunden als notstandsfähige Rechtsgüter in Betracht.
Jedoch kann § 34 StGB die Maßnahme nur dann rechtfertigen, wenn diese Interessen dasjenige von Empfänger und Absender an der Zustellung der elektronischen Nachricht überwiegen würde. Auch hier kann wie eben im Bereich des § 109 Abs. 2 TKG auf das in Kapitel 2 Teil 1 gefundene Abwägungsergebnis verwiesen werden.[1040] Daraus ergibt sich, dass das Interesse des Providers oder Unternehmens an der Abwehr unerwünschter Emails dasjenige von Empfänger und Absender an der Nachricht nicht überwiegt. Dagegen spricht auch, dass der Funktionsfähigkeit des Fernmeldeverkehrs nach deutschem Recht ein hoher Rang zukommt.[1041] Insofern müssten bedeutende Rechtsgüter gefährdet sein, um das Aussortieren von Nachrichten zu rechtfertigen.[1042] Eine derartige Gefährdung bedeutender Rechtsgüter ist hier jedoch zu verneinen. Insbesondere besteht die früher häufig zitierte Gefahr des „Überlaufens“ des Email-Accounts inzwischen angesichts des Zuwachses an Download- und Speicherkapazitäten in der Regel nicht mehr.[1043] Ein Eintritt eines Schadens am Server ist, wie bereits dargestellt, nicht zu erwarten.[1044]
Im Ergebnis überwiegen die Interessen, die durch den Softwareeinsatz geschützt werden sollen, nicht diejenigen, die hierdurch beeinträchtigt werden. Hinzu kommt, dass die Tatsache, dass eine Email positiv gescannt wird, nicht grundsätzlich bedeutet, dass es sich um eine Spammail handelt.[1045] Auch deshalb kann kein berechtigtes Interesse des Providers oder Unternehmens anerkannt werden, sämtliche unter Spamverdacht stehende Nachrichten zu löschen. Eine Rechtfertigung nach § 34 StGB scheidet somit aus.[1046]

[1037] OLG Karlsruhe, MMR 2005, S. 181; *Altenhain* in Münchener Kommentar, § 206 StGB, Rn. 68; *Lackner/Kühl*, § 206 StGB, Rn. 15; *Lenckner* in Schönke/Schröder, § 206 StGB, Rn. 14; a.A.: *Träger* in Leipziger Kommentar, § 206 StGB, Rn. 54; *Tröndle/Fischer*, § 206 StGB, Rn. 9
[1038] vgl.: 2. Kap. Teil 2 A. I. 2. c) aa)
[1039] OLG Karlsruhe, MMR 2005, S. 180 f.; *Cornelius/Tschoepe*, K & R 2005, S. 271
[1040] vgl.: 2. Kap. Teil 2 A. II. 3. b) cc) (1) und 2. Kap. Teil 1 B. I. 2. b) aa)
[1041] BVerfG, NJW 2003, S. 1789; BGH, NJW 2003, S. 1882; *Heidrich/Tschoepe*, MMR 2004, S. 79; *Jarass* in Jarass/Pieroth, Art. 10 GG, Rn. 1
[1042] BVerfG, NJW 2003, S. 1789; BGH, NJW 2003, S. 1882; *Heidrich/Tschoepe*, MMR 2004, S. 79; *Jarass* in Jarass/Pieroth, Art. 10 GG, Rn. 1
[1043] *BSI*, Antispam-Strategien, 6.3.1.
[1044] 2. Kap. Teil 2 A. II. 3. b) cc) (1)
[1045] vgl. zur stets vorhandenen Quote an false positives: 1. Kap. Teil 2 A. I.
[1046] ebenso: *Heidrich/Tschoepe*, MMR 2004, S. 79; *Lehnhardt*, DuD 2003, S. 488

dd) Zwischenergebnis

Der Tatbestand des § 206 Abs. 2 Nr. 2 StGB ist erfüllt, wenn ein Provider oder ein Unternehmen, das über ein eigenes Netzwerk verfügt, zentrale Filtermaßnahmen veranlasst, die die Löschung eingehender Emails vor dem Abruf durch den Empfänger, deren Blockade oder das Umleiten dergestalt bewirken, dass der Empfänger nicht auf die Nachricht zugreifen kann. Die Tatbestandsmäßigkeit des Verhaltens entfällt nur im Fall einer Einwilligung des Empfängers, die sich auf sämtliche positiv gescannten Nachrichten beziehen muss, um auch das Löschen von false positives zu rechtfertigen. Die Voraussetzungen der Rechtfertigungsgründe der §§ 109 TKG, 34 StGB liegen nicht vor.

4. § 303 a StGB

Derjenige, der den Filtereinsatz veranlasst, könnte neben § 206 Abs. 2 Nr. 2 StGB den Tatbestand des § 303 a Abs. 1 StGB verwirklichen. Die Vorschrift sanktioniert das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten im Sinne des § 202 a Abs. 2 StGB.

Im Gegensatz zu § 206 Abs. 2 in Verbindung mit Abs. 1 StGB beschränkt § 303 a StGB den Täterkreis nicht. Daher ist § 303 a StGB uneingeschränkt auf Unternehmen anwendbar, und zwar selbst dann, wenn die diese ihren Angestellten die private Email-Nutzung verbieten.[1047]

a) Objektiver Tatbestand

Voraussetzung des objektiven Tatbestands des § 303 a Abs. 1 StGB ist, dass es sich bei den gefilterten Emails um Daten im Sinne des § 202 a Abs. 2 StGB handelt, die nach der h.M. fremd zu sein haben (aa).[1048] Des Weiteren muss in den jeweiligen Maßnahmen eine Tathandlung im Sinne des § 303 a Abs. 1 StGB zu sehen sein (bb).

aa) Daten im Sinne des § 202 a Abs. 2 StGB und Fremdheit der Daten als ungeschriebenes Tatbestandsmerkmal

Es wurde bereits dargestellt, dass es sich sowohl bei eingehenden, als auch bei in der Mailbox gespeicherten Emails um Daten im Sinne des § 202 a Abs. 2 StGB handelt.[1049] Auch die Fremdheit der Daten ist nach den genannten Grundsätzen zu bejahen, da die Verfügungsberechtigung bis zum Einstellen der Nachricht in der Mailbox des Adressaten dem Absender und ab diesem Zeitpunkt dem Empfänger zusteht.[1050]

[1047] *Heidrich/Tschoepe*, MMR 2004, S. 77; *Jüngel/Schwan/Neumann*, MMR 2005, S. 820 ff.; im Ergebnis: *Kitz*, CR 2005, S. 453 f.; *Schmidl*, MMR 2005, S. 435
[1048] BayObLG, JR 1994, S. 476 mit Anmerkung *Hilgendorf*, JR 1994, S. 478 ff.; *Kitz*, CR 2005, S. 454; *Koecher*, DuD 2004, S. 274; *Lenckner/Winkelbauer*, CR 1986, S. 829; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 3; *Tröndle/Fischer*, § 303 a StGB, Rn. 4
[1049] vgl.: 2. Kap. Teil 1 A. I. 1. a)
[1050] vgl.: 2. Kap. Teil 1 A. I. 1. b)

bb) Tathandlung im Sinne des § 303 a Abs. 1 StGB

Fraglich ist, ob derjenige, der den Spamfilter einsetzt, eine der in § 303 a Abs. 1 StGB genannten Tathandlungsmodalitäten verwirklicht.
§ 303 a Abs. 1 StGB sanktioniert das Löschen, das Unterdrücken, das Unbrauchbarmachen und Verändern der Daten.

Das Überprüfen von Inhalt und Headerinformationen stellt bereits nach dem ausdrücklichen Wortlaut des § 303 a Abs. 1 StGB keine tatbestandsmäßige Handlung dar, da es sich keiner der genannten Handlungsmodalitäten zuordnen lässt. Fraglich ist jedoch, ob das durch die Filtersoftware bewirkte Blockieren, Löschen, Umleiten oder Markieren als Tathandlung im Sinne des § 303 a Abs. 1 StGB zu qualifizieren ist.

In dem Blockieren von Nachrichten könnte ein Unterdrücken von Daten liegen.
Unterdrücken von Daten bedeutet, dass sie dem Zugriff des Berechtigten auf Dauer oder zeitweilig entzogen werden und er sie deshalb nicht verwenden kann.[1051]
Durch das Blockieren wird zwar verhindert, dass der Empfänger auf die Email Zugriff nehmen kann. Allerdings kommt es im Hinblick auf die Zugriffsbefugnis nicht auf die Person des Empfängers, sondern auf die des Absenders an, da diesem, wie oben gezeigt, bis zum Einstellen der Email in die Mailbox des Empfängers die Verfügungsberechtigung über die Daten zukommt.[1052] Dem Absender wird die Verfügungsberechtigung jedoch nicht entzogen, da er noch über die gespeicherte Fassung der Email verfügt.[1053] Im Übrigen hätte er auf die übersandte Kopie der Email auch dann keinen Zugriff mehr, wenn sie zugestellt würde. Vielmehr entlässt er diese mit Absenden aus seinem Einflussbereich und zwar unabhängig davon, ob die Email letztendlich zugestellt wird oder nicht.
Insofern liegt in dem Blockieren eingehender Emails kein Unterdrücken im Sinne des § 303 a Abs. 1 StGB.

Das Löschen von Emails könnte unter den entsprechenden Begriff des Tatbestands des § 303 a StGB fallen.
Unter dem Löschen von Daten wird die Aufhebung ihrer Verkörperung, das bedeutet das unwiderbringliche Unkenntlichmachen der konkreten Speicherung verstanden.[1054] Es entspricht dem Zerstören einer Sache im Sinne des § 303 StGB und setzt insofern voraus, dass eine Rekonstruktion der Daten aufgrund der Aufhebung der physischen Verkörperung unmöglich ist.[1055]
Werden bereits in der Mailbox des Empfängers oder einen Quarantäne-Ordner eingegangene Emails gelöscht, so wird die Verkörperung der Daten aufgehoben. Sie werden unwiderbringlich vernichtet. Das Löschen ist in diesem Fall daher tatbestandsmäßig.[1056] Da auf die konkrete Speicherung abzustellen ist, schließt die Tatsache, dass die Original-Email beim Absender verbleibt, die Tatbestandsmäßigkeit nicht aus. Das Löschen noch nicht in die Mailbox eingestellter Emails verwirklicht den Tatbestand aus den im Bereich des Blockierens der Nachricht genannten Gründe nicht.

[1051] vgl.: 2. Kap. Teil 1 A. I. 1. c)
[1052] vgl.: 2. Kap. Teil 1 A. I. 1. b)
[1053] vgl.: 2. Kap. Teil 1 A. I. 1. c); *Ernst*, Hacker, Cracker & Computerviren, Rn. 272; *Hilgendorf*, JuS 1997, S. 325
[1054] BT-Drs. 10/5058, S. 34; *Gravenreuth*, NStZ 1989, S. 206; *Lenckner/Winkelbauer*, CR 1986, S. 829; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tröndle/Fischer*, § 303 a StGB, Rn. 9
[1055] BT-Drs. 10/5058, S. 34; *Gravenreuth*, NStZ 1989, S. 206; *Lenckner/Winkelbauer*, CR 1986, S. 829; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tröndle/Fischer*, § 303 a StGB, Rn. 9
[1056] *Heidrich/Tschoepe*, MMR 2004, S. 79; *Koecher*, DuD 2004, S. 274; *Lejeune*, MMR 2005, S. 291; *Spindler/Ernst*, CR 2004, S. 439; im Ergebnis: *Schmidl*, MMR 2005, S. 345

In dem Markieren von Nachrichten als potentielle Spammails durch Erweiterung der Subjektszeile oder Hinzufügen einer Zeile an den Header der Nachricht könnte ein Verändern von Daten liegen.
Verändern von Daten ist jede Form inhaltlichen Umgestaltens gespeicherter Daten, § 3 Abs. 5 Nr. 2 BDSG.[1057] Erforderlich ist, dass die betroffenen Daten durch das Verändern einen anderen Informationsgehalt erhalten und dadurch der ursprüngliche Verwendungszweck beeinträchtigt wird.[1058] Auch hier ist auf die konkrete Datenspeicherung abzustellen.[1059] Das blosse Hinzufügen von Daten auf leerem Speicherplatz ist kein Verändern, sofern hierdurch nicht der Bedeutungsgehalt der bereits gespeicherten Daten verändert wird.[1060] Das Markieren der Email als spamverdächtig erfolgt, wie oben dargestellt, in der Regel dadurch, dass der Email im automatisierten Verfahren eine Spam-Wahrscheinlichkeit zugeordnet und diese Bewertung an den Email-Header angefügt wird.[1061] Fraglich ist, ob in diesem Hinzufügen der Spam-Wahrscheinlichkeit ein Verändern der Daten gesehen werden kann. Dagegen spricht, dass in den Fällen, in denen der Email lediglich eine Subjektzeile im Header zugefügt wird im Gegensatz zu einer Veränderung oder Ergänzung der vom Absender ausgefüllten Subjektzeile- weder der Inhalt der Email, noch die Subjektzeile selbst einen anderen Informationsgehalt erhält. Im Übrigen erreicht die Email ohnehin den Empfänger nicht in der Form, in der der Absender sie versandt hat, da ihr stets zumindest ein Transport-Header beigefügt wird.[1062] Den Informationsgehalt der Email ändert das Hinzufügen derartiger Header demnach nicht.[1063] Folglich werden die Daten nicht im Sinne des § 303 a StGB verändert, wenn dem Header eine Zeile zugefügt wird, die auf den Spamverdacht verweist.
Anders sind die Fälle zu beurteilen, in denen eine Änderung an der durch den Absender ausgefüllten Subjektzeile vorgenommen wird. Denn wird die Subjektzeile geändert bzw. ergänzt, so erhält sie hierdurch einen anderen Bedeutungsgehalt.[1064] Während die Subjektzeile nämlich zuvor nicht die Information enthalten hat, es handle sich um eine Spammail, kommt ihr dieser Informationsgehalt nach Anfügen des entsprechenden Vermerks zu.
Somit ist davon auszugehen, dass in einer Veränderung der Subjektzeile ein Verändern von Daten im Sinne des § 303 a StGB liegt, nicht jedoch im Einfügen einer Spam-Wahrscheinlichkeit ohne Zusatz zur Subjektzeile.

Es stellt sich die Frage, ob in dem Umleiten der Email eine der in § 303 a Abs. 1 StGB sanktionierten Tathandlungen zu sehen ist. Zumindest in den Fällen, in denen durch das Umleiten der Emails bewirkt wird, dass diese den Empfänger nicht erreichen, könnte darin ein Unterdrücken von Daten gesehen werden.
Unterdrücken von Daten bedeutet dabei, dass diese dem Zugriff des Berechtigten auf Dauer oder zeitweilig entzogen werden und er sie deshalb nicht mehr verwenden kann.[1065] Das Unterdrücken kann durch Entziehen oder Vorenthalten des Datenträgers erfolgen, aber auch

[1057] *Buggisch*, NStZ 2002, S. 180; *Ernst*, NJW 2003, S. 3238; *Möhrenschlager*, wistra 1986, S. 141; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tröndle/Fischer*, § 303 a StGB, Rn. 12
[1058] *Buggisch*, NStZ 2002, S. 180; *Ernst*, NJW 2003, S. 3238; *Möhrenschlager*, wistra 1986, S. 141; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tröndle/Fischer*, § 303 a StGB, Rn. 12
[1059] *Ernst*, NJW 2003, S. 3238; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tolksdorf* in Leizipger Kommentar, § 303 a StGB, Rn. 31; *Tröndle/Fischer*, § 303 a StGB, Rn. 12
[1060] *Ernst*, NJW 2003, S. 3238; *Hilgendorf*, JuS 1996, S. 891; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tröndle/Fischer*, § 303 a StGB, Rn. 12; *Welp*, IuR 1988, 435
[1061] vgl.: 1. Kap. Teil 2 B.
[1062] *Hoeren*, NJW 2004, S. 3515; *Ders.*, Recht der Access Provider, Rn. 165
[1063] *Hoeren*, NJW 2004, S. 3515; *Ders.*, Recht der Access Provider, Rn. 165
[1064] *Hoeren*, NJW 2004, S. 3515; *Ders*., Recht der Access Provider, Rn. 165
[1065] vgl.: 2. Kap. Teil 1 A. I. 1. c)

dadurch, dass mittels einer Sperre der Verfügungsberechtigte vom Zugang zu den Daten ausgeschlossen wird.[1066]
Zwar wird -zumindest durch ein Umleiten in Ordner, auf die der Empfänger keinen Zugriff hat- verhindert, dass dieser die Email erhält. Allerdings kommt es im Hinblick auf die Zugriffsbefugnis nicht auf die Person des Empfängers, sondern auf die des Absenders an, da diesem, wie oben gezeigt, die Verfügungsbefugnis über die Daten bis zum Einstellen in die Mailbox des Empfängers zusteht.[1067] Jedoch wird dem Absender die Verfügungsbefugnis nicht entzogen, da er noch über die gespeicherte Fassung der Email verfügt.[1068] Im Übrigen hätte er auf die Kopie der Email auch dann keinen Zugriff mehr, wenn sie zugestellt würde. Vielmehr entlässt er diese mit dem Absenden aus seinem Einflussbereich und zwar unabhängig davon, ob sie letztendlich zugestellt wird oder nicht.
Insofern liegt in dem Umleiten eingehender Emails selbst dann kein Unterdrücken im Sinne des § 303 a Abs. 1 StGB, wenn hierdurch bewirkt wird, dass der Empfänger die Email nicht erhält.

b) Subjektiver Tatbestand

Zumindest bedingter Vorsatz wird hier in der Regel vorliegen, da der Verantwortliche bei Einsatz eines entsprechendes Programms damit rechnen muss, dass die Email nach dem Einstellen in einen Quarantäne-Ordner -gegebenenfalls nach Ablauf eines gewissen Zeitrahmens- gelöscht oder die Subjektzeile durch Anfügen der Spam-Wahrscheinlichkeit verändert wird. Angesichts der bestehenden Fehlerquote beim Einsatz von Spam-Filtern[1069] muss der Verantwortliche auch davon ausgehen, dass legitime Email den genannten Maßnahmen unterzogen werden.

c) Rechtswidrigkeit

Gerechtfertigt werden kann der Einsatz entsprechender Filter durch die Einwilligung des Berechtigten.[1070] Dies ist, wie bereits gezeigt, vor dem Zeitpunkt des Absendens und während des Übermittlungsvorgangs der Absender und ab dem Einstellen der Email in die Mailbox des Empfängers dieser.[1071]
Insofern wird die Rechtswidrigkeit des Löschens von Emails nach dem Einstellen in der Mailbox des Empfängers durch dessen Einwilligung ausgeschlossen. Da die Veränderung der Subjektzeile grundsätzlich vor dem Einstellen in die Mailbox erfolgt, ist die Einwilligung des Absenders erforderlich. Diese wird grundsätzlich nicht vorliegen, da er gerade ein Interesse an der Zustellung der Email sowie daran hat, dass diese nicht als Spam markiert wird. Im Fall des Erfordernisses der Einwilligung des Empfängers sollte -wie im Rahmen des § 206 Abs. 2 Nr. 2 StGB- die Einwilligung im Hinblick auf sämtliche positiv gescannten Nachrichten eingeholt werden, damit auch das Löschen von false positives gerechtfertigt werden kann. Eine Rechtfertigung nach § 109 TKG, § 34 StGB scheidet aus den im Rahmen des § 206 Abs. 2 Nr. 2 StGB genannten Gründen aus.

[1066] LG Ulm, CR 1989, S. 825 f.; *Schulze-Heimig*, a.a.O., S. 178; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 4; *Tröndle/Fischer*, § 303 a StGB, Rn. 10; *Wuermeling*, CR 1994, S. 592
[1067] vgl.: 2. Kap. Teil 1 A. I. 1. b) und c)
[1068] vgl.: 2. Kap. Teil 1 A. I. 1. c); *Ernst*, Hacker, Cracker & Computerviren, Rn. 272; *Hilgendorf*, JuS 1997, S. 325
[1069] vgl.: 1. Kap. Teil 2 A. I.
[1070] *Frommel*, Jus 1987, S. 667 f.; *Kitz*, CR 2005, S. 454; *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 6; *Tolksdorf* in Leipziger Kommentar, § 303 a StGB, Rn. 21; *Zaczyk* in Kindhäuser/Neumann/Paeffgen, § 303 a StGB, Rn. 11
[1071] vgl.: 2. Kap. Teil 1 A. I. 1. b)

d) Zwischenergebnis

Das Löschen von Emails nach Einstellen in die Mailbox des Empfängers verwirklicht den Tatbestand des § 303 a StGB. Markiert die Spamfiltersoftware lediglich die Nachricht und weist ihr eine bestimmte Spamwahrscheinlichkeit zu, so wird hierdurch nur dann der Tatbestand des § 303 a StGB erfüllt, wenn damit ein Verändern der vom Absender ausgefüllten Subjektzeile verbunden ist. Das Umleiten und Blockieren von Nachrichten verwirklicht den Tatbestand nicht. Erklärt der Empfänger seine Einwilligung, so kann das Löschen aus der Mailbox gerechtfertigt werden. Das Markieren der Nachricht ist allerdings nur dann rechtmäßig, wenn der Absender eingewilligt hat, was allerdings grundsätzlich nicht der Fall sein wird.

5. § 44 Abs. 1 BDSG

Schließlich könnte durch den Filtereinsatz der Tatbestand des § 44 Abs. 1 BDSG verwirklicht werden.
Die Vorschrift sanktioniert denjenigen, der eine in § 43 Abs. 2 S BDSG bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Von der durch den Filtereinsatz bedingten Überprüfung des Inhalts und der Headerinformationen sind jedoch, wie bereits ausgeführt, keine personenbezogenen Daten betroffen. Deshalb greift § 44 Abs. 1 BDSG nicht ein. Auch in Bezug auf das Blockieren, Umleiten, Markieren und vor der Einstellung in der Mailbox des Empfängers erfolgenden Löschen der Nachricht sind, wie oben dargestellt, keine personenbezogenen Daten betroffen, so dass keine der in § 43 Abs. 2 S. 2 BDSG genannten Handlungen begangen wird. Werden Emails gelöscht, die bereits in die Mailbox oder einen Quarantäne-Ordner des Empfängers eingespeichert wurden, so liegt ein nach § 35 Abs. 2 S. 1 BDSG zulässiger Vorgang vor, der ebenfalls keiner der in § 43 Abs. 2 BDSG genannten Alternativen unterfällt.

Im Übrigen wird es in der Regel an der Tatbegehung gegen Entgelt oder mit Schädigungsabsicht im Sinne des § 44 Abs. 1 BDSG fehlen.
Somit kommt eine Strafbarkeit nach § 44 Abs. 1 BDSG nicht in Betracht.

6. Zwischenergebnis

Provider und diejenigen Entscheidungsträger in Unternehmen, die Filtersoftware einsetzen, machen sich nach § 206 Abs. 2 Nr. 2 StGB strafbar, wenn hierdurch bewirkt wird, dass eingehende Emails vor dem Abruf durch den Empfänger gelöscht, blockiert oder derart umgeleitet werden, dass der Empfänger nicht auf die Nachricht zugreifen kann. Die Tatbestandsmäßigkeit des Verhaltens entfällt, wenn der Empfänger seine Einwilligung erklärt hat. Nach in der Rechtsprechung vertretener Auffassung ist darüber hinaus die Einwilligung des Absenders erforderlich.
Der Tatbestand des § 303 a StGB ist verwirklicht, wenn Emails nach Einstellen in die Mailbox gelöscht oder durch Verändern der vom Absender ausgefüllten Subjektzeile als spamverdächtig gekennzeichnet werden. Die Rechtswidrigkeit des Löschens entfällt, wenn der Empfänger seine Einwilligung erklärt hat. Das Markieren der Nachricht kann hingegen nur gerechtfertigt werden, wenn der Absender eingewilligt hat, was allerdings grundsätzlich nicht der Fall sein wird.

In den Fällen, in denen sowohl § 206 Abs. 2 Nr. 2 StGB, als auch § 303 a StGB eingreifen, ist wegen der unterschiedlichen Rechtsgüter, die die Strafnormen schützen, davon auszugehen, dass die Vorschriften in Idealkonkurrenz stehen.[1072]

III. Deliktsrecht

Dem Filtereinsatz könnten deliktsrechtliche Vorschriften, insbesondere die §§ 823 Abs. 1, 1004 Abs. 1 BGB bzw. §§ 823 Abs. 2, 1004 Abs. 1 BGB entgegenstehen.
§ 1004 Abs. 1 schützt seinem Wortlaut nach zwar nur das Eigentum, findet jedoch nach einhelliger Auffassung daneben auf sämtliche absoluten Rechte sowie alle durch §§ 823 Abs. 2, 824, 825 und 826 BGB geschützten Rechtsgüter entsprechend Anwendung.[1073] Der Unterlassungsanspruch richtet sich dabei sowohl gegen die Person, die die Filtersoftware einsetzt,[1074] als auch gegen denjenigen, der Dritte hierzu beauftragt.[1075] Dasselbe gilt für einen etwaigen Schadensersatzanspruch. Anspruchsgegner ist hier derjenige, der die Rechtsgutsverletzung im Sinne des § 823 Abs. 1 BGB kausal verursacht bzw. das Schutzgesetz nach § 823 Abs. 2 BGB verletzt hat.

1. §§ 823 Abs. 1, 1004 Abs. 1 BGB

Fraglich ist, ob die Vorschriften der §§ 823 Abs. 1, 1004 Abs. 1 BGB dem Filtereinsatz entgegenstehen. Grundvoraussetzung ist die Verletzung eines durch § 823 Abs. 1 BGB geschützten Rechtsguts. Hier könnte das Recht am eigenen Datum (a), das Eigentum (b), das allgemeine Persönlichkeitsrecht der von dem Filtereinsatz betroffenen Personen (c) sowie das Recht der Anschlussinhaber am eingerichteten und ausgeübten Gewerbebetrieb (d) tangiert sein.

a) Recht am eigenen Datum

In der Überprüfung des Inhalts und der Headerinformationen der eingehenden Emails könnte eine Verletzung des Rechts am eigenen Datum liegen.
Fraglich ist, ob ein solches Recht im Rahmen des § 823 Abs. 1 BGB anzuerkennen ist. Dies wird teilweise bejaht.[1076] Zur Begründung wird angeführt, die technologische Entwicklung bewirke, dass der entscheidende wirtschaftliche Wert nicht mehr lediglich dem Anlagevermögen wie Maschinen oder sonstigen industriellen Gütern zukomme, sondern auch Informationen und Daten.[1077] Gegen die Existenz eines solchen Rechts spricht jedoch einerseits, dass dieses durch die Rechtsprechung nicht hinreichend konkretisiert ist. Im Übrigen würde die Anerkennung eines solchen Rechts neben dem allgemeinen Persönlichkeitsrecht und dem Recht auf den eingerichteten und ausgeübten Gewerbebetrieb

---

[1072] *Heidrich/Tschoepe*, MMR 2004, S. 79; *Lenckner* in Schönke/Schröder, 206 StGB, Rn. 39; *Spindler/Ernst*, CR 2004, S. 439; *Tröndle/Fischer*, § 303 a StGB, Rn. 16
[1073] RGZ 60, S. 9; RGZ 61, S. 369; RGZ 116, S. 153; BGH, NJW 1951, S. 843; BGH, NJW 1999, S. 2141; BGH, NJW 2001, S. 157; std. Rspr.; *Bassenge* in Palandt, § 1004 BGB, Rn. 3; *Fritzsche* in Bamberger/Roth, § 1004 BGB, Rn. 2; *Gursky* in Staudinger, § 1004, Rn. 15 f.
[1074] vgl. zum unmittelbaren Störer i.S.d. § 1004 BGB: BGH, NJW 1983, S. 751; *Bassenge* in Palandt, § 1004 BGB, Rn. 16; *Medicus* in Münchener Kommentar, § 1004 BGB, Rn. 53
[1075] vgl. zum mittelbaren Störer i.S.d. § 1004 BGB: BGH, NJW 2000, S. 2902; *Bassenge* in Palandt, § 1004 BGB, Rn. 17; *Medicus* in Münchener Kommentar, § 1004 BGB, Rn. 53
[1076] *Meier/Wehlau*, NJW 1998, S. 1588
[1077] *Meier/Wehlau*, NJW 1998, S. 1588

ein weiteres Recht begründen, das tatbestandlich nur schwer zu fassen ist und eines Korrektivs bedarf, um nicht zu umfassend ausgestaltet zu sein.[1078]

Somit ist nicht davon auszugehen, dass das Recht am eigenen Datum als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anzuerkennen ist.[1079] Insofern erübrigt sich die Beantwortung der Frage, ob dieses Recht schon durch die durch ein Computerprogramm durchgeführte Kontrolle tangiert würde.

b) Eigentum

In dem Löschen, Blockieren, Markieren oder Umleiten positiv gescannter Nachrichten könnte eine Eigentumsverletzung im Sinne des § 823 Abs. 1 BGB liegen.

Voraussetzung des Eigentumsschutzes ist nach Maßgabe der §§ 903 S. 1 BGB, 90 BGB, dass es sich bei dem beeinträchtigten Gut um eine Sache, also um einen körperlichen Gegenstand handelt. Die notwendige Verkörperung des Gegenstandes liegt dabei vor, wenn dieser im Raum abgrenzbar ist und zwar entweder durch eigene körperliche Begrenzung, durch Fassung in einem Behältnis oder durch sonstige künstliche Mittel, wie Grenzsteine oder Einzeichnung in Karten oder Liegenschaftskataster.[1080] Keine Sachen sind hingegen Computerdaten, es sei denn sie sind auf Datenträgern wie Disketten oder Festplatten gespeichert.[1081] Dies ist hier zwar der Fall, wenn die Daten bereits auf der Festplatte des Servers abgelegt wurden. Aus dem Anwendungsbereich fallen insofern auf den ersten Blick lediglich diejenigen Emails heraus, die bereits vor der Speicherung auf einem Speichermedium gelöscht, blockiert, umgeleitet oder markiert werden.
Allerdings wird eine Eigentumsverletzung des betroffenen Kunden bzw. Arbeitnehmers auch bei der Löschung bereits eingegangener Daten ausscheiden. Denn grundsätzlich werden eingehende Emails, wie oben ausgeführt, auf dem Server des Email-Service-Providers gespeichert, so dass das Eigentum des Kunden bereits aus diesem Grund nicht betroffen sein kann. Ebenso kommt dem Arbeitnehmer am Server seines Arbeitgebers kein Eigentum zu, da die Arbeitsmittel grundsätzlich vom Arbeitgeber zur Verfügung gestellt werden.
Eine Eigentumsverletzung scheidet hier somit aus.

c) Allgemeines Persönlichkeitsrecht

Der Einsatz des Filters könnte das allgemeine Persönlichkeitsrecht der Kommunikationspartner verletzen.
Das allgemeine Persönlichkeitsrecht ist als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anerkannt.[1082] Es umfasst auch die informationelle Selbstbestimmung, das bedeutet die

[1078] *Hager* in Staudinger, § 823 BGB, Rn. C 173; ähnlich: *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 96
[1079] *Hager* in Staudinger, § 823 BGB, Rn. C 173; *Spindler* in Bamberger/Roth, § 823 BGB, Rn. 93; *Wagner* in Münchener Kommentar, § 823 BGB, Rn. 96
[1080] RGZ 87, S. 45; BGH, MDR 1977, S. 1002; BayObLG, NJW 1980, S. 132; BayObLG, NJW 1995, S. 974; *Heinrichs* in Palandt, § 90 BGB, Rn. 1; *Holch* in Münchener Kommentar, § 90 BGB, Rn. 8; *Jauernig* in Ders., Vorbem. § 90 BGB, II. 2. a) bb); *Lober/Weber*, MMR 2005, 655
[1081] BGHZ 102, S. 144; BGH, NJW 1990, S. 321; OLG Karlsruhe, NJW 1996, S. 201; LG Konstanz, NJW 1996, S. 2662; *Bartsch*, CR 2000, S. 723; *Heinrichs* in Palandt, § 90 BGB, Rn. 1; *Holch* in Münchener Kommentar, § 90 BGB, Rn. 27; *König*, NJW 1993, S. 3123; *Marly,* BB 1991, S. 432 ff.; *Meier/Wehlau*, NJW 1998, S. 1588; *Wagner* in Münchener Komm., § 823 BGB, Rn. 96
[1082] vgl.: 2. Kap. Teil 1 A. III. 1. a) aa)

Befugnis des Einzelnen, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[1083]

Jedoch ist hier ebenso wie im Bereich des Datenschutzrechts zu berücksichtigen, dass die genannten Daten, insbesondere die Email- und IP-Adresse des Absenders, zwar durch das Filterprogramm überprüft, allerdings zu diesem Zweck nicht dauerhaft gespeichert oder für den Provider oder seine Mitarbeiter lesbar abgelegt werden.[1084] Es finden damit lediglich Zwischenspeichervorgänge statt, wie sie bei der Datenübermittlung ständig durchgeführt werden.[1085] Eine dauerhafte Fixierung der Daten auf einem Speichermedium erfolgt hingegen nicht.[1086] Somit steht derjenige, dessen Daten von der Filtermaßnahme betroffen sind, hinsichtlich der Vertraulichkeit der ihn betreffenden Informationen nicht anders, als dies ohne den Filtereinsatz der Fall sein würde.[1087] Denn die in der Email enthaltenen Informationen werden während des Filtereinsatzes nicht durch eine natürliche Person wahrgenommen und mit dem Betroffenen in Verbindung gebracht. Dies kann auch nicht später nachgeholt werden, da die Daten nicht infolge des Filtereinsatzes dauerhaft gespeichert bleiben.[1088] Da demnach weder während der Überprüfung, noch zu einem späteren Zeitpunkt die Daten der betroffenen Person zugeordnet werden bzw. werden können, ist eine Persönlichkeitsrelevanz der fraglichen Maßnahmen abzulehnen. Das Gleiche muss im Hinblick auf die inhaltliche Überprüfung der Email gelten, da es auch in diesem Zusammenhang, wie dargestellt, weder zu einer inhaltlichen Wahrnehmung der Email durch eine Person, noch zu einer Speicherung der Nachricht kommt, so dass der Inhalt auch nicht später kommunikationsfremden Dritten zur Kenntnis gelangen kann.[1089] Demnach wird das allgemeine Persönlichkeitsrecht durch die Filtermaßnahmen nicht tangiert. Folglich ergeben sich -unabhängig von der Frage nach der Subsidiarität des Schutzes durch das allgemeine Persönlichkeitsrecht gegenüber dem Schutz nach dem BDSG-[1090] keine Ansprüche aus dem allgemeinen Persönlichkeitsrecht.

Hier könnte jedoch das Persönlichkeitsrecht der Absender legitimer Emails betroffen sein, wenn diese irrtümlich als Spam gekennzeichnet oder abgelegt werden, da dann der Anschein erweckt wird, dass es sich bei dem fraglichen Absender um einen Versender von Werbe-Emails handelt. Auch die Ehre ist Bestandteil des allgemeinen Persönlichkeitsrechts.[1091] Eine Verletzung des allgemeinen Persönlichkeitsrechts in der genannten Ausprägung läge demnach dann vor, wenn mit dem Einsortieren der Email in einen speziellen Spamordner oder in der entsprechenden Markierung der Nachricht eine unwahre Tatsachenbehauptung in Bezug auf die Person des Absenders zu sehen wäre, die sich abträglich auf das Bild des Betroffenen in

---

[1083] BVerfGE 65, S. 41 ff. unter Bezugnahme auf BVerfGE 54, S. 155, BVerfGE 27, S. 6, BVerfGE 27, S. 350 f., BVerfGE 32, S. 379, BVerfGE 35, S. 220, BVerfGE 44, S. 372 f., BVerfGE 56, S. 41 ff. und BVerfGE 63, S. 142 f.; BVerfG, NJW 2006, S. 980; BVerwG, NJW 2004, S. 1192; BGH, NJW 1991, S. 2651; BGH, NJW 2004, S. 766 f.; BGH, NJW 2005, S. 498; OLG Stuttgart, NJW-RR 2003, S. 1410; OLG Hamburg, AfP 2006, S. 257 f.; LG Köln, MMR 2006, S. 758 f.; KG Berlin, NJW-RR 2005, S. 1710; *Bamberger* in Bamberger/Roth, § 12 BGB, Rn. 160; *Bull*, NJW 1979, S. 1180

[1084] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[1085] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[1086] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[1087] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[1088] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[1089] vgl.: 2. Kap. Teil 2 A. I. 2. c) bb)

[1090] vgl. dazu: BGH, NJW 1981, S. 1740; BGH, NJW 1984, S. 436; BGH, NJW 1984, S. 1886; *Bamberger* in Ders./Roth, § 12 BGB, Rn. 161; *Hager* in Staudinger, § 823 BGB, Rn. C 173; *Rixecker* in Münchener Kommentar, Anhang zu § 12 BGB, Rn. 6

[1091] BGHZ 31, S. 311; BGHZ 39, S. 127 f.; BGH, NJW 1996, S. 1131 ff.; OLG Frankfurt a.M., NJW 1990, S. 2002; OLG Frankfurt a.M., NJW-RR 1993, S. 852; OLG Frankfurt a.M., NJW-RR 1996, S. 1051; OLG Celle, NStZ 1998, S. 88 f.; LG Berlin, NJW-RR 1998, S. 316 f.; AG Düsseldorf, NJW-RR 1998, S. 1482; *Bamberger* in Ders./Roth, § 12 BGB, Rn. 139; *Hager* in Staudinger, § 823 BGB, Rn. C 63

der Öffentlichkeit auswirken könnte.[1092] Fraglich ist bereits, ob mit dem Einsortieren der Email in einen speziellen Spam-Ordner oder mit der entsprechenden Markierung der Nachricht eine unwahre Tatsachenbehauptung in Bezug auf die Person des Absenders verbunden ist. Dem steht entgegen, dass -wie oben dargelegt- die Markierung stets nur eine Anmerkung im Hinblick auf die Spamwahrscheinlichkeit darstellt.[1093] Eine Aussage dahingehend, der Versender der Nachricht sei ein Spammer, wird daher mit der Markierung nicht getroffen. Auch mit dem Einstellen der Email in eine Quarantäne-Ordner ist eine derartige Aussage nicht verbunden, insbesondere da als allgemein bekannt vorausgesetzt werden kann, dass Spam-Filter nicht fehlerfrei funktionieren. Insofern liegt weder in dem Markieren, noch in dem Umleiten eine Äußerung dahingehend, es handle sich bei dem Versender um einen Spammer. Eine Persönlichkeitskeitsverletzung scheidet insofern aus. Werden die Nachrichten gelöscht oder blockiert, so wird es nicht nur an einer definitiven Aussage dahingehend, dass der Versender ein Spammer ist, fehlen, sondern darüber hinaus an einer Äußerung. Voraussetzung einer Ehrverletzung ist jedoch notwendigerweise die Äußerung einem Dritten gegenüber.[1094]
Insofern wird das allgemeine Persönlichkeitsrecht durch die Email-Filterung nicht tangiert.

d) Recht am eingerichteten und ausgeübten Gewerbebetrieb

Schließlich kommt eine Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb in Betracht.

Dieses als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anerkannte Recht schützt vor betriebsbezogenen Eingriffen.[1095] Unter einem betriebsbezogenen Eingriff ist eine unmittelbare Beeinträchtigung des Gewerbebetriebs zu verstehen.[1096] Der Eingriff muss sich spezifisch gegen den betrieblichen Organismus oder die unternehmerische Entscheidungsfreiheit richten, nicht nur gegen vom Betrieb ohne weiteres ablösbare Rechte oder Rechtsgüter.[1097]

Eine bloße Überprüfung der von einem bestimmten Betrieb versandten oder empfangenen Emails tangiert weder den betrieblichen Organismus, noch die unternehmerische Entscheidungsfreiheit. Denn weder wird durch die Überprüfung in die betriebliche Organisation eingegriffen, noch kommt es anderweitig zu einer Beeinträchtigung des betrieblichen Ablaufs. Insofern wird das Recht auf den eingerichteten und ausgeübten Gewerbebetrieb nicht bereits dadurch tangiert, dass eine Überprüfung des Inhalts und der Headerinformationen eingehender Emails durch die Filtersoftware vorgenommen wird.

Allerdings könnte das Löschen, Blockieren, Markieren und Umleiten von Emails einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb von Absender und Empfänger darstellen. Ein betriebsbezogener Eingriff durch Spamfiltermaßnahmen wird teilweise mit dem Argument bejaht, in dem Sperren der Kommunikation über eine Email-Adresse läge eine

---

[1092] BVerfG, NJW 1999, S. 1323; BVerfG, NJW 2004, S. 590 f.; *Hager* in Staudinger, § 823 BGB, Rn. C 64; *Sprau* in Palandt, § 823 BGB, Rn. 110
[1093] vgl.: 1. Kap. Teil 2 B.
[1094] BGH, NJW 1996, S. 1131 ff.; OLG Frankfurt a.M., NJW 1990, S. 2002; OLG Frankfurt a.M., NJW-RR 1993, S. 852; OLG Frankfurt a.M., NJW-RR 1996, S. 1051; OLG Celle, NStZ 1998, S. 88 f.; LG Berlin, NJW-RR 1998, S. 316 f.; AG Düsseldorf, NJW-RR 1998, S. 1482; *Bamberger* in Ders./Roth, § 12 BGB, Rn. 139; *Hager* in Staudinger, § 823 BGB, Rn. C 84
[1095] vgl.: 2. Kap. Teil 1 A. III. 1. a) bb)
[1096] vgl.: 2. Kap. Teil 1 A. III. 1. a) bb)
[1097] vgl.: 2. Kap. Teil 1 A. III. 1. a) bb)

Betriebsblockade.[1098] In Kapitel 2 Teil 1 wurde jedoch bereits ausgeführt, dass in der Beeinträchtigung von Produktions- oder Kommunikationsmitteln kein betriebsbezogener Eingriff zu sehen ist.[1099] Demnach ist auch der Einsatz von Spamfiltersoftware nicht als Eingriff in das Recht auf den eingerichteten und ausgeübten Gewerbebetrieb zu qualifizieren.

e) Zwischenergebnis

Weder durch das Überprüfen von Inhalt und Headerinformationen eingehender Emails, noch durch das Löschen, Blockieren, Markieren und Umleiten von Nachrichten wird ein Rechtsgut im Sinne des § 823 Abs. 1 BGB tangiert.

2. §§ 823 Abs. 2, 1004 Abs. 1 BGB

Möglicherweise stehen die §§ 823 Abs. 2, 1004 Abs. 1 BGB der uneingeschränkten Zulässigkeit der Maßnahmen entgegen.
Grundvoraussetzung wäre die Verletzung eines Schutzgesetzes im Sinne des § 823 Abs. 2 BGB. Als Schutzgesetz gemäß § 823 Abs. 2 BGB wird jede Rechtsnorm im Sinne des Art. 2 EGBGB verstanden.[1100] Diese muss zumindest auch dem Individualschutz dienen.[1101] Des Weiteren ist Voraussetzung, dass der Interessensbereich des Einzelnen nicht nur durch staatliche Maßnahmen -etwa das Tätigwerden einer Behörde- geschützt werden soll, sondern dass dem Einzelnen unmittelbar selbst die Rechtsmacht in die Hand gegeben wird, mit Mitteln des Privatrechts gegen den Störer vorzugehen.[1102] Als Schutzgesetze kommen hier internationale oder gemeinschaftsrechtliche Vorschriften oder Vorgaben des einfachen Gesetzesrechts in Betracht. Oben wurde allerdings bereits dargestellt, dass der deliktische Schutz nach § 823 Abs. 2 BGB im Grundsatz entbehrlich ist, wenn dieselben Belange des Geschädigten bereits anderweitig abgesichert sind.[1103] Etwas anderes gilt, wie oben dargelegt nur im Rahmen strafbewehrter Normen.[1104]
Im Bereich der Frage nach der Zulässigkeit des Überprüfung von Inhalt und Headerinformationen stehen allerdings lediglich die Vorschriften § 202 Abs. 1 StGB, § 202 a Abs. 1 StGB, § 206 Abs. 2 Nr. 1 StGB, § 303 a Abs. 1 StGB oder § 44 Abs. 1 BDSG im Raum, deren Tatbestandsmerkmale -wie oben bereits dargestellt wurde- jedoch nicht erfüllt sind.[1105] Insofern stehen auch die §§ 823 Abs. 2, 1004 Abs. 1 BGB den fraglichen Maßnahmen nicht entgegen.
Im Hinblick auf das weitere Vorgehen hinsichtlich positiv gescannter Nachrichten greifen jedoch hier die §§ 206 Abs. 2 Nr. 2 StGB, 303 a Abs. 1 StGB ein.[1106] Fraglich ist, ob diese Vorschriften Schutzgesetze im Sinne des § 823 Abs. 2 BGB sind. Dies wäre der Fall, wenn die betreffenden Normen zumindest auch den Schutz bestimmter Rechtsgüter oder Interessen des Einzelnen bezwecken würden.[1107] § 206 Abs. 2 Nr. 2 StGB schützt, wie bereits erwähnt, zwar einerseits das Allgemeininteresse in Form des öffentlichen Vertrauens in die Sicherheit und Zuverlässigkeit des Post- und Telekommunikationsverkehrs, andererseits jedoch auch Individualinteressen, nämlich das Interesse des Betroffenen am ordnungsgemäßen Umgang

[1098] *Spindler/Ernst*, CR 2004, S. 444
[1099] vgl.: 2. Kap. Teil 1 A. III. 1. a) bb)
[1100] vgl.: 2. Kap. Teil 1 A. III. 2.
[1101] vgl.: 2. Kap. Teil 1 A. III. 2.
[1102] vgl.: 2. Kap. Teil 1 A. III. 2.
[1103] vgl.: 2. Kap. Teil 1 A. III. 2. a)
[1104] vgl.: 2. Kap. Teil 1 A. III. 2. b)
[1105] vgl.: 2. Kap. Teil 2 A. II.
[1106] vgl.: 2. Kap. Teil 2 A. II.
[1107] vgl.: 2. Kap. Teil 1 A. III. 2.

mit der Sendung.[1108] Somit ist § 206 Abs. 2 Nr. 2 StGB als Schutzgesetz im Sinne des § 823 Abs. 2 BGB anzusehen. Es wurde oben bereits dargelegt, dass § 303 a StGB ein Schutzgesetz im Sinne des § 823 Abs. 2 StGB darstellt.[1109]

3. Zwischenergebnis

Dem Überprüfen von Inhalt und Headerdaten stehen deliktsrechtliche Vorgaben nicht entgegen. Dagegen sind die durch den Filtereinsatz bedingten Maßnahmen in Bezug auf positiv gescannte Nachrichten nicht uneingeschränkt zulässig. So bestehen Ansprüche auf Unterlassung und gegebenenfalls Schadensersatz aus §§ 823 Abs. 2, 1004 Abs. 1 BGB in Verbindung mit 206 Abs. 2 Nr. 2 StGB gegen denjenigen, der den Filter eingesetzt oder einen Dritten hierzu beauftragt hat, wenn dies zur Folge hat, dass eingehende Emails vor Abruf durch den Empfänger gelöscht, blockiert oder so umgeleitet werden, dass dieser darauf nicht Zugriff nehmen kann. Ansprüche ergeben sich auch, wenn elektronische Nachrichten nach dem Einstellen in die Mailbox des Empfängers gelöscht oder wenn die Nachricht durch Abändern der Subjektzeile als spamwahrscheinlich markiert wird, §§ 823 Abs. 2, 1004 Abs. 1 in Verbindung mit § 303 a Abs. 1 StGB.

IV. Ergebnis

Im deutschen Recht ist das Überprüfen von Inhalt und Headerinformationen durch Filtersoftware zulässig, da keine natürliche Person von den entsprechenden Daten Kenntnis erlangen kann. Hingegen ist es unzulässig, den Zugang elektronischer Post zu verhindern, Emails aus der Mailbox des Empfängers zu löschen und die vom Absender ausgefüllte Subjektzeile abzuändern.

B. Völker-, Gemeinschafts- und Verfassungsrecht

Im Folgenden soll überprüft werden, ob die einfachgesetzliche Rechtslage mit verfassungs-, gemeinschafts- sowie völkerrechtlichen Vorschriften im Einklang steht. Ist dies nicht der Fall, so kann daraus -abhängig davon, gegen welche Norm verstoßen wird- die Ungültigkeit des Gesetzes, eine Verpflichtung des Gesetzgebers zur Aufhebung der Norm, der Anwendungsvorrang der verletzten Vorschrift, oder aber die unmittelbare Anwendbarkeit bzw. eine Verpflichtung zu einer Umsetzung oder richtlinienkonformen Auslegung des nationalen Rechts folgen. Resultiert der Verstoß aus einem Unterlassen, so könnte der Gesetzgeber zu einem Tätigwerden verpflichtet sein, falls den maßgeblichen Vorschriften des internationalen-, gemeinschafts- und Verfassungsrechts eine Schutzpflichtdimension zukommt.

I. Verfassungsrecht

Fraglich ist, ob der Gesetzgeber aufgrund verfasssungsrechtlicher Vorgaben verpflichtet ist, Vorschriften zu erlassen, welche das Überprüfen von Inhalts- und Headerinformationen verbieten und das weitere Vorgehen in Bezug auf positiv gescannte Nachrichten anderweitig regeln. Eine Handlungsverpflichtung des Gesetzgebers würde sich ergeben, wenn durch das gesetzgeberische Unterlassen ein Grundrecht beeinträchtigt würde und diesem eine

[1108] vgl.: 2. Kap. Teil 2 A. II. 3. b) aa) (2) und (4)
[1109] vgl.: 2. Kap. Teil 1 A. III. 2. b)

Schutzpflichtdimension zukäme,[1110] die den Gesetzgeber zu einem konkreten Tätigwerden verpflichtet.

Grundvoraussetzung ist allerdings, dass die Grundrechte des deutschen Grundgesetzes hier überhaupt Anwendung finden. Oben wurde bereits dargestellt, dass nationales Recht, das in Umsetzung sekundären Gemeinschaftsrechts erlassen wird, nicht am Maßstab deutscher Grundrechte überprüft wird, soweit die Normsetzung zwingend dem Gemeinschaftsrecht folgt.[1111] Der Bereich des Datenschutzes wäre demnach der Überprüfung anhand deutscher Grundrechte entzogen, soweit die Umsetzung völlig durch die DSRL oder die EK-DSRL determiniert war. Danach greifen die mitgliedstaatlichen Grundrechte hier nur insoweit ein, als das zu überprüfende nationale Gesetz nicht durch sekundäres Gemeinschaftsrecht determiniert wurde.[1112] Dies ist der Fall, soweit Vorschriften des Datenschutzes unabhängig von Sekundärrecht erlassen wurden, was im Bereich der Verarbeitung personenbezogener Daten von juristischen Personen der Fall ist. Darüber hinaus finden die nationalen Grundrechte auf die hier einschlägigen Vorschriften außerhalb des Datenschutzrechts Anwendung, da diese nicht aufgrund sekundären Gemeinschaftsrechts erlassen wurden. Nach den genannten Grundsätzen ist auch das gesetzgeberische Unterlassen dem Maßstab der deutschen Grundrechte zu unterwerfen.
Soweit die Grundrechte des deutschen Grundgesetzes danach Prüfungsmaßstab sind, wird nachfolgend dargestellt, ob die einfachgesetzliche Rechtslage zu diesen in Widerspruch steht. Dabei wird zwischen dem Überprüfen von Inhalt und Headerinformationen eingehender Emails (1.) und dem Blockieren, Löschen, Umleiten sowie Markieren positiv gescannter Nachrichten (2.) unterschieden.

1. Überprüfen von Inhalt und Headerinformationen

Es könnte eine gesetzgeberische Verpflichtung zu einer anderweitigen Regelung der Frage nach der Zulässigkeit des Überprüfens von Inhalt und Headerinformationen beim Einsatz von Spamfiltersoftware bestehen. Voraussetzung ist, dass der Geltungsbereich eines Grundrechts betroffen ist. Es könnte das Fernmeldegeheimnis (a), die Meinungsäußerungsfreiheit (b) oder aber das informationelle Selbstbestimmungsrecht (c) einschlägig sein.

a) Fernmeldegeheimnis, Art. 10 Abs. 1 GG

Das Grundrecht des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG könnte dadurch beeinträchtigt sein, dass der deutsche Gesetzgeber keine Regelung erlassen hat, die den Einsatz von Spamfiltersoftware untersagt mit der Folge, dass Private diese rechtmäßigerweise einsetzen können. Da gemäß Art. 1 Abs. 3 GG lediglich staatliche Behörden Grundrechtsadressaten sind, hier jedoch Private handeln, kann Art. 10 Abs. 1 GG in der vorliegenden Konstellation nur in Gestalt einer gesetzgeberischen Schutzpflicht eingreifen.

[1110] vgl. dazu: BVerfGE 39, S. 41; BVerfGE 46, S. 164; BVerfGE 49, S. 140 ff.; BVerfGE 53, S. S. 57; BVerfGE 56, S. S. 73; BVerfGE 75, S. 66; BVerfGE 77, S. 214 f.; BVerfGE 77, S. 402 f.; BVerfGE 79, S. 201 f.; BVerfGE 81, S. 254 ff.; BVerfGE 81, S. 339; BVerfGE 84, S. 147; BVerfGE 85, S. 212; BVerfGE 87, S. 386; BVerfGE 88, S. 251 ff.; BVerfGE 89, S. 286 f.; BVerfGE 91, S. 339; BVerfGE 92, S. 46; BVerfGE 97, S. 148 f.; BVerfGE 102, S. 18; BVerfGE 102, S. 393; *E.Klein*, NJW 1989, S. 1633 ff.; *H. Klein*, DVBl. 1994, S. 489 ff.; *Oeter*, AöR 119 (1994), S. 529 ff., 535 ff., 549 ff.; *Pietrzak*, JuS 1994, S. 748 ff.; *Sachs* in Ders., vor Art. 1 GG, Rn. 35; *Starck* in von Mangoldt/Klein/Starck, Art. 1 Abs. 3 GG, Rn. 193
[1111] vgl.: 2. Kap. Teil 1 B. I.
[1112] vgl.: 2. Kap. Teil 1 B. I.

Art. 10 GG kommt eine Schutzpflichtdimension zu.[1113] Insbesondere hat der Gesetzgeber danach die Anbieter von Telekommunikationsdiensten zu verpflichten, das Fernmeldegeheimnis bei ihrer Geschäftstätigkeit zu wahren.[1114]

Es stellt sich allerdings die Vorfrage, ob der Filtereinsatz Art. 10 Abs. 1 GG oder dem ebenfalls die Privatsphäre schützenden Recht auf informationelle Selbstbestimmung unterfällt, das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitet wird. Ist der Schutzbereich beider Gewährleistungen eröffnet, so geht Art. 10 Abs. 1 GG kraft Spezialität vor.[1115]
Allerdings ist die Reichweite des Fernmeldegeheimnisses zeitlich durch den Abschluss des Kommunikationsvorgangs begrenzt, sofern die betroffene Nachricht bzw. die Informationen über die betreffenden Kommunikationsumstände sich im Herrschaftsbereich des Empfängers befinden.[1116] Inhalte und Verbindungsdaten, die nach Abschluss des Kommunikationsvorgangs im Herrschaftsbereich des Teilnehmers gespeichert sind, unterliegen dem Fernmeldegeheimnis nicht mehr.[1117] Das Gleiche gilt aus den oben genannten Gründen für Inhalte und Verbindungsdaten, die nach Abschluss des Kommunikationsvorgangs auf dem Server des Providers bzw. Unternehmens gespeichert bleiben.[1118] Der Kommunikationsvorgang ist dabei erst abgeschlossen, wenn der Empfänger die Nachricht vom Empfängerserver abgerufen hat.[1119] Eingehende Emails unterfallen daher dem Fernmeldegeheimnis so lange, bis sie vom Empfänger abgerufen werden, da der Kommunikationsvorgang in diesem Fall noch nicht abgeschlossen und die Kommunikationsinhalte und -umstände sich noch nicht im alleinigen Herrschaftsbereich des Empfängers befinden.[1120] Da das Überprüfen von Inhalts- und Headerinformationen vor Abruf durch den Empfänger stattfindet, ist grundsätzlich der Anwendungsbereich des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG betroffen, nicht derjenige des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG.

Es stellt sich die Frage, ob die durch den Filtereinsatz bedingte Überprüfung von Inhalt und Headerdaten eingehender Emails den Schutzbereich des Art. 10 Abs. 1 GG berührt. Unter das Fernmeldegeheimnis fällt auch die Kommunikation per Email.[1121] Allerdings wurde oben bereits dargestellt,[1122] dass hier das Fernmeldegeheimnis nicht beeinträchtigt ist, weil Vorgänge, die nicht in einer Kenntnisnahme oder einem Niederlegen der betreffenden Informationen mit der Folge der Möglichkeit der späteren Kenntnisnahme, Verwendung oder Weitergabe resultieren, nicht die Vertraulichkeit der räumlich distanzierten Kommunikation berühren, was auch durch die bereits zitierte Rechtsprechung bestätigt wird.

[1113] BVerfGE 106, S. 28, Ls. 2; *Gramlich*, CR 1996, S. 110; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 61; *Hermes* in Dreier, Art. 10 GG, Rn. 83 ff.; *Jarass* in Ders./Pieroth, Art. 10 GG, Rn. 14; *Löwer* in von Münch/Kunig, Art. 10, Rn. 14; *Müller-Dehn*, DÖV 1996, S. 868 f.
[1114] BVerfGE 106, S. 37; *Gusy* in von Mangoldt/Klein/Starck, Art. 10 GG, Rn. 63; *Hermes* in Dreier, Art. 10 GG, Rn. 83; *Jarass* in Ders./Pieroth, Art. 10 GG, Rn. 14; *Krüger* in Sachs, Art. 10 GG, Rn. 21 f.; *Löwer* in von Münch/Kunig, Art. 10 GG, Rn. 14
[1115] BVerfGE 67, S. 171; BVerfGE 100, S. 358; BVerfG, NJW 2003, S. 1788; *Dreier* in Ders., Art. 2 Abs. 1 GG, Rn. 94; *Löwer* in Kunig, Art. 10 GG, Rn. 22; *Schulz*, Die Verwaltung 1999, S. 137 ff., 139
[1116] BVerfG, NJW 2006, S. 976 ff., 978; anders noch: BVerfG, CR 2005, S. 799 ff.
[1117] BVerfG, NJW 2006, S. 979; a.A.: Störing, CR 2006, S. 392 f., 393, der vorschlägt Verbindungsdaten, denen seiner Auffassung nach ein „nachträgliches Element“ immanent ist, dem Schutzbereich des Fernmeldegeheimnisses zuzuordnen.
[1118] vgl.: 2. Kap. Teil 2 A. I. 2. a)
[1119] vgl.: 2. Kap. Teil 2 A. I. 2. a)
[1120] vgl.: 2. Kap. Teil 2 A. I. 2. a)
[1121] vgl.: 2. Kap. Teil 2 A. II. 3. b) aa) (2)
[1122] vgl.: 2. Kap. Teil 2 A. I. 2. c)

Im Übrigen ist zu beachten, dass eine Schutzpflicht den Gesetzgeber nicht zu einem bestimmten Tätigwerden verpflichten kann, da ihm in diesem Bereich ein weiter Einschätzungs-, Wertungs- und Gestaltungsbereich zukommt.[1123] Er darf zwar nicht darüber entscheiden, ob er einer bestehenden Schutzpflicht nachkommt, jedoch liegt es in seinem Ermessen, wie er diese erfüllt.[1124] Aufgrund dieser Tatsache ist nach der Rechtsprechung des Bundesverfassungsgerichts davon auszugehen, dass der Staat seiner Schutzpflicht genügt hat, wenn er nicht gänzlich untätig geblieben ist und nicht offensichtlich völlig ungeeignete und unzulängliche Maßnahmen ergriffen hat.[1125]

Der Gesetzgeber hat das Fernmeldegeheimnis durch § 88 TKG gegenüber Eingriffen privater Übermittler geschützt.[1126] Bei der Kommunikation anfallende Daten, denen ein Personenbezug zukommt, sind daneben durch das bereichsspezifische, ergänzend durch das allgemeine Datenschutzrecht und das Datenschutzstrafrecht erfasst. Insofern wurde der Gesetzgeber tätig und unterstellte sowohl den Inhalt der Kommunikation, als auch die hierbei anfallenden Daten einem einfachgesetzlichen Schutz. Die Tatsache, dass im vorliegenden Fall die genannten Vorschriften nicht eingreifen, ist darauf zurückzuführen, dass ein Eindringen in die Geheimnissphäre durch die fraglichen Maßnahmen nicht bewirkt wird und der Betroffene damit auch nicht in seinen Rechten beeinträchtigt ist. Da der Gesetzgeber seinen Schutzpflichten somit nachgekommen ist, besteht auch deshalb keine Handlungspflicht.

b) Meinungsfreiheit, Art. 5 Abs. 1 GG

Fraglich ist, ob das Grundrecht der Meinungsfreiheit gemäß Art. 5 Abs. 1 GG den Gesetzgeber dazu verpflichtet, die Filtermaßnahmen zu untersagen. So wird im Fall eines staatlichen Eingreifens in die Telekommunikation durch heimliches Abhören oder heimliches Festhalten von Äußerungen durch Tonbandaufnahmen ein Eingriff in das Grundrecht angenommen, mit der Begründung, dass hierdurch die Integrität der Äußerung, ihre Unbefangenheit, Exklusivität bzw. Vertraulichkeit angetastet wird.[1127]

Allerdings wurde bereits dargestellt, dass die Geheimnissphäre der Kommunikationspartner durch den Einsatz der Filtersoftware nicht tangiert ist, da eine Wahrnehmung des Inhalts sowie der Verbindungsdaten der Email praktisch ausgeschlossen ist.[1128] Wenn allerdings die Kommunikationspartner wie hier davon ausgehen können, dass ein Dritter den Gesprächsinhalt weder zum Zeitpunkt der Überprüfung, noch später wahrnehmen kann, bleibt die Integrität der Äußerung, ihre Unbefangenheit, Exklusivität und Vertraulichkeit unberührt. Da die Geheimnissphäre der Kommunikationspartner nicht beeinträchtigt wird, wird auch das

---

[1123] BVerfGE 46, S. 164 f.; BVerfGE 49, S. 126 ff.; BVerfGE 53, S. 57 ff.; BVerfGE 56, S. 78; BVerfGE 77, S. 214 f.; BVerGE 79, S. 202; BVerfGE 88, S. 262; std. Rspr.; *Brüning/Helios*, Jura 2001, S. 162; *Dirnberger*, DVBl. 1992, S. 879 ff.; *Erichsen*, Jura 1997, S. 85 ff.; *Kunig* in von Münch/Kunig, Art 2 GG, Rn. 54 ff.; *v. Münch* in Ders./Kunig, Vorbemerkung zu Art. 1-19, Rn. 22; *Sachs* in Ders., vor Art. 1 GG, Rn. 37; *Starck* in v. Mangoldt/Klein/Starck, Art. 1 Abs. 3 GG, Rn. 196

[1124] BVerfGE 46, S. 164 f.; BVerfGE 49, S. 126 ff.; BVerfGE 53, S. 57 ff.; BVerfGE 56, S. 78; BVerfGE 77, S. 214 f.; BVerGE 79, S. 202; BVerfGE 88, S. 262; std. Rspr.; *Brüning/Helios*, Jura 2001, S. 162; *Dirnberger*, DVBl. 1992, S. 879 ff.; *Erichsen*, Jura 1997, S. 85 ff.; *Kunig* in von Münch/Kunig, Art 2 GG, Rn. 54 ff.; *v. Münch* in Ders./Kunig, Vorbemerkung zu Art. 1-19, Rn. 22; *Sachs* in Ders., vor Art. 1 GG, Rn. 37; *Starck* in v. Mangoldt/Klein/Starck, Art. 1 Abs. 3 GG, Rn. 196

[1125] BVerfGE 56, S. 81; BVerfGE 77, S. 215; BVerfGE 77, S. 405; BVerfGE 79, S. 202; BVerfGE 85, S. 212

[1126] vgl.: 2. Kap. Teil 2 A. I. 2.

[1127] *Herzog* in Maunz/Dürig, Art. 5 GG, Rn. 79; *Hoffmann-Riem* in Denninger, Alternativkommentar, Art. 5 GG, Rn. 31; *Jarass* in Ders./Pieroth, Art. 5 GG, Rn. 9; *Schmidt-Jortzig* in Isensee/Kirchhof, Band VI, § 141, Rn. 26; *Wendt* in v. Münch/Kunig, Art. 5 GG, Rn. 18; vgl. auch: Eberle, DÖV 1977, S. 306 ff., 308 ff.

[1128] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b); 2. Kap. Teil 2 A. I. 2. c) bb)

Grundrecht der Meinungsfreiheit nicht durch den Filtereinsatz berührt. Ein etwaiges gesetzgeberisches Untätigbleiben stellt danach keine Verletzung seiner Schutzpflicht dar.

c) Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG

Nach den oben genannten Abgrenzungskriterien greift das Recht auf informationelle Selbstbestimmung nicht ein, soweit eingehende Emails von der Filtermaßnahme betroffen sind.[1129] Erst bereits abgerufene Inhalte bzw. beim Empfänger gespeicherte Verbindungsdaten unterfallen dem Schutzbereich des informationellen Selbstbestimmungsrechts. Dieses wird hier somit von Art. 10 Abs. 1 GG verdrängt.[1130]

d) Allgemeine Handlungsfreiheit, Art. 2 Abs. 1 GG

Gegenüber Art. 2 Abs. 1 GG spezielle Grundrechtsgewährleistungen sind hier, wie eben dargestellt wurde, nicht einschlägig. Es könnte jedoch Art. 2 Abs. 1 GG beeinträchtigt sein. Art. 2 Abs. 1 GG umfasst die allgemeine Handlungsfreiheit.[1131] Das Überprüfen von Inhalt und Headerinformationen eingehender Emails hindert die Kommunikationspartner jedoch nicht daran, wie gewünscht zu handeln. Wie bereits gezeigt wurde,[1132] nehmen weder während des Filtereinsatzes kommunikationsfremde Dritte vom Inhalt der Email oder den Headerdaten Kenntnis, noch ist eine Kenntnisnahme zu einem späteren Zeitpunkt möglich. Auch der Vorgang der Nachrichtenübertragung wird durch das blosse Überprüfen der entsprechenden Informationen nicht beeinträchtigt. Daher werden die Kommunikationspartner durch den Vorgang des Überprüfens eingehender Nachrichten nicht an einem Tätigwerden gehindert. Eine gesetzgeberische Verpflichtung dazu, die allgemeine Handlungsfreiheit der Betroffenen zu schützen, indem er die Filtervorgänge untersagt, besteht danach nicht.

2. Blockieren, Löschen, Umleiten sowie Markieren positiv gescannter Nachrichten

Fraglich ist, ob sich aus verfassungsrechtlichen Vorgaben eine Handlungspflicht des Gesetzgebers zu einer anderweitigen Regelung der Frage der Zulässigkeit des Blockierens, Löschens, Umleitens sowie Markierens positiv gescannter Nachrichten ergibt. Dabei könnten hier das Fernmeldegeheimnis, Art. 10 Abs. 1 GG (a), das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG (b) oder Grundrechte betroffen sein, die nicht spezifisch die Privatsphäre, sondern andere Rechtsgüter schützen (c).

a) Fernmeldegeheimnis, Art. 10 GG

Die gesetzgeberische Pflicht zum Schutz vor dem Unterdrücken, Löschen oder anderen Handlungen, die den Zugang der Nachricht verhindern könnte aus Art. 10 Abs. 1 GG folgen, soweit die Vorschrift gemäß der oben entwickelten Abgrenzungskriterien eingreift. Dies ist dann der Fall, wenn Emails bzw. Daten betroffen sind, die noch nicht nach Abschluss des Kommunikationsvorgangs im Herrschaftsbereich des Empfängers befindlich sind.[1133]

[1129] vgl.: 2. Kap. Teil 2 A. I. 2. a); 2. Kap. Teil 2 A. I. 2. c) bb)
[1130] vgl.: 2. Kap. Teil 2 A. I. 2. a); 2. Kap. Teil 2 A. I. 2. c) bb)
[1131] BVerfGE 6, 32 ff., 36 - Elfes; BVerfGE 20, 150 ff., 154 - Veranstaltung von Sammlungen; BVerfGE 54, S. 143 ff., 146 - Taubenfütterung; BVerfGE 55, S. 159 ff., 165 - Falknerjagdschein; BVerfGE 59, S. 275 ff., 278 - Schutzhelm; BVerfGE 63, S. 88 ff., 108 - Versorgungsausgleich; BVerfGE 80, S. 137 ff., 152 - Reiten im Walde; BVerfGE 90, S. 145 ff., 171 - Unerlaubter Umgang mit Cannabisprodukten
[1132] vgl.: 1. Kap. Teil 2 A. II.
[1133] vgl.: 2. Kap. Teil 2 A. I. 2. a); 2. Kap. Teil 2 A. I. 2. c) bb)

Zu beachten ist allerdings, dass Art. 10 Abs. 1 GG zwar vor illegitimer Kommunikationsteilhabe schützt, nicht jedoch vor dem Übermittlungsrisiko.[1134] Genau dieses realisiert sich allerdings, wenn durch den Einsatz der Filtersoftware in den Übermittlungsvorgang eingegriffen wird mit der Folge, dass die Nachricht dem Empfänger nicht zugeht. Danach ist hier ein gerade nicht von Art. 10 Abs. 1 GG erfasstes Risiko betroffen. Insofern folgt hier keine gesetzgeberische Schutzpflicht aus Art. 10 Abs. 1 GG dahingehend, dass Vorschriften erlassen werden müssten, die dem Unterdrücken, Löschen oder anderen Handlungen, die den Zugang der Nachrichten verhindern, zu verbieten.

b) Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG

Fraglich ist, ob das Recht auf informationelle Selbstbestimmung, das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitet wird, den Gesetzgeber dazu verpflichtet, dem durch den Filtereinsatz bewirkten Unterdrücken, Löschen oder anderen Handlungen, die den Zugang von Emails verhindern können, durch den Erlaß gesetzlicher Maßnahmen entgegenzuwirken.
Die Anwendbarkeit des Rechts auf informationelle Selbstbestimmung ist nach Maßgabe der genannten Abgrenzungskriterien auf solche Emails begrenzt, die bereits durch den Empfänger vom Server abgerufen wurden.[1135]

Das Recht auf informationelle Selbstbestimmung ist eine Ausformung des allgemeinen Persönlichkeitsrechts, das von der Literatur und Rechtsprechung entwickelt wurde.[1136] Es umfasst die Befugnis des Einzelnen, selbst zu entscheiden, wann und wem er zu welchem Zeitpunkt personenbezogene Daten offenbaren möchte.[1137] Dies ergibt sich daraus, dass derjenige, der nicht mit Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen weiß, in seiner Freiheit wesentlich gehemmt sein kann, aus eigener Selbstbestimmung zu planen und zu entscheiden.[1138]
Den Staat trifft hinsichtlich des Grundrechts eine Schutzpflicht.[1139] Das Grundrecht steht natürlichen Personen zu, auch wenn sie Ausländern sind.[1140] Aufgrund der Mitprägung des

---

[1134] vgl.: 2. Kap. Teil 2 A. I. 2. c) aa)
[1135] vgl.: 2. Kap. Teil 2 A. I. 2. a)
[1136] grundlegend: BVerfGE 65, S. 1 ff., 41 ff.; *Podlech* in Perels, S. 50 ff., 55; *W. Schmidt*, JZ 1974, S. 241 ff.; vgl. auch: BVerfGE 78, S. 84; BVerfGE 84, S. 194; BGH, NJW 1991, S. 1533; BVerfG, NJW 2005, S, 1917 ff.; BVerfG, NJW 2006, S. 976 ff.; BVerfG, NJW 2006, S. 1939 ff.; *Di Fabio* in Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 176; *Duttge*, Der Staat 36 (1997), S. 281 ff.; *Hoffmann-Riem*, AöR 123 (1998), S. 513 ff.; *Jarass* in Jarass/Pieroth, Art. 2 GG, Rn. 44; *Krause*, JuS 1984, S. 268 ff.; *Kunig*, Jura 1993, S. 595 ff.; *Ders.* in v. Münch/Kunig, Art. 2 GG, Rn. 38; *H. Schneider*, DÖV 1984, S. 161 ff.; *Simitis*, NJW 1984, S. 398 ff.; *Starck* in von Mangoldt/Klein/Starck, Art. 2 Abs. 1 GG, Rn. 114
[1137] grundlegend: BVerfGE 65, S. 1 ff., 41 ff.; *Podlech* in Perels, S. 50 ff., 55; *W. Schmidt*, JZ 1974, S. 241 ff.; vgl. auch: BVerfGE 78, S. 84; BVerfGE 84, S. 194; BGH, NJW 1991, S. 1533; BVerfG, NJW 2005, S, 1917 ff.; BVerfG, NJW 2006, S. 976 ff.; BVerfG, NJW 2006, S. 1939 ff.; *Di Fabio* in Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 176; *Duttge*, Der Staat 36 (1997), S. 281 ff.; *Hoffmann-Riem*, AöR 123 (1998), S. 513 ff.; *Jarass* in Ders./Pieroth, Art. 2 GG, Rn. 44; *Krause*, JuS 1984, S. 268 ff.; *Kunig*, Jura 1993, S. 595 ff.; *Ders.* in v. Münch/Kunig, Art. 2 GG, Rn. 38; *H. Schneider*, DÖV 1984, S. 161 ff.; *Simitis*, NJW 1984, S. 398 ff.; *Starck* in von Mangoldt/Klein/Starck, Art. 2 Abs. 1 GG, Rn. 114
[1138] BVerfGE 65, S. 43
[1139] BVerfGE 34, S. 281 f.; BVerfGE 79, S. 63; BVerfGE 83, S. 140; *Jarass* in Ders./Pieroth, Art. 2 GG, Rn. 13; *Kunig* in von Münch/Kunig, Art. 2 GG, Rn. 40; *Murswiek* in Sachs, Art. 2 GG, Rn. 27; *Schulz*, Die Verwaltung 1999, S. 143; *Starck* in von Mangoldt/Klein/Starck, Art. 2 Abs. 1 GG, Rn. 173
[1140] BVerfGE 35, S. 399; BVerfGE 78, S. 196 f.; BVerfGE 104, S. 346; *Jarass* in Ders./Pieroth, Art. 2 GG, Rn. 9; *Kunig* in von Münch/Kunig, Art. 2 GG, Rn. 39; *Leibholz/Rinck*, Art. 2 GG, Rn. 4; *Starck* in von Mangoldt/Klein/Starck, Art. 2 Abs. 1 GG, Rn. 42

Grundrechts durch Art. 1 Abs. 1 GG ist eine Anwendung auf juristische Personen und gleichgestellte Personenmehrheiten abzulehnen, da diesen keine Würde im Sinne des Art. 1 Abs. 1 GG zukommt.[1141] Diese sind daher auf die subsidiäre Handlungsfreiheit verwiesen.[1142]

Fraglich ist allerdings, ob das Recht auf informationelle Selbstbestimmung beeinträchtigt ist. Dabei gewinnt der Umstand Bedeutung, dass die Daten nicht erhoben, gespeichert, verwendet oder weitergegeben, sondern gelöscht werden. Eine Gefahr für das Recht auf informationelle Selbstbestimmung ist demnach nicht gegeben, da der Betroffene so trotz des Ausfiltervorgangs noch darüber Bescheid weiss, wer was über ihn erfährt.
Im Übrigen gelten die Ausführungen zum Fernmeldegeheimnis dahingehend, dass der Gesetzgeber tätig wurde und folglich seiner Schutzpflicht nachgekommen ist.[1143]
Im Ergebnis wird danach durch die geltende Rechtslage nicht das Recht auf informationelle Selbstbestimmung beeinträchtigt.

c) Nicht die Privatsphäre schützende Grundrechte

Eben wurde dargestellt, dass die Privatsphäre schützende Grundrechte nicht eingreifen. Allerdings können solche Grundrechte betroffen sein, die nicht spezifisch die Privatheit der Kommunikation schützen. So kann sich eine gesetzgeberische Verpflichtung, dem Löschen und Unterdrücken von Emails durch den Einsatz von Filtersoftware entgegenzuwirken, aus dem Grundrecht auf Informationsfreiheit derjenigen Empfänger ergeben, die Werbung erhalten möchten, Art. 5 Abs. 1 GG bzw. aus Art. 2 Abs. 1 GG. Es wurde bereits dargestellt, dass sich Personen, die Werbe-Emails erhalten möchten, auf diese Grundrechte berufen können.[1144] Seitens der Versender von Email-Werbung greifen, wie oben dargestellt, Art. 5 Abs. 1 GG sowie, falls ihre berufliche Tätigkeit betroffen ist, Art. 12 Abs. 1 GG ein.[1145]
Im Rahmen der Frage nach einer Schutzpflichtverletzung dieser Grundrechte ist allerdings zu beachten, dass im Übermittlungsvorgang befindliche Emails bereits davor geschützt sind, durch den Übermittler blockiert, gelöscht oder dergestalt umgeleitet zu werden, dass der Adressat sie nicht erhält. Das Blockieren, Löschen vor dem Abruf durch den Empfänger und Umleiten mit der Folge, dass der Adressat auf die Email nicht zugreifen kann, ist dabei, wie oben dargestellt, durch § 206 Abs. 2 Nr. 2 StGB strafrechtlich sanktioniert, das Löschen nach Einstellen in der Mailbox des Empfängers zusätzlich durch § 303 a Abs. 1 StGB.[1146] Insofern besteht ein gesetzlicher Schutz der Absender von Email-Werbung und solcher Empfänger, die die Nachrichten erhalten möchten.

Eine darüber hinausgehende gesetzgeberische Schutzpflicht dahingehend, die Zustellung sämtlicher -auch unerwünschter- Emails zu gewährleisten, kann deshalb nicht bestehen, weil so die Rechte derjenigen Adressaten, die an einem Erhalt solcher Nachrichten nicht interessiert sind, einseitig zurückgedrängt würden. Nicht an Werbung interessierte Adressaten werden durch das Zusenden unerwünschter Email-Werbung in ihrem allgemeinen Persönlichkeitsrecht bzw. Art. 2 Abs. 1 GG betroffen.[1147] Oben wurde bereits dargestellt, dass die sich gegenüberstehenden Rechtsgüter in einen verhältnismäßigen Ausgleich zu bringen

[1141] *Kunig* in von Münch/Kunig, Art. 2 GG, Rn. 39; das BVerfG zieht Art. 14 GG heran: vgl. BVerfGE 67, S. 142 f.; BVerfGE 77, S. 47; BVerfG, NJW 1991, S. 2132; für eine beschränkte Anwendung des Grundrechts auf juristische Personen in den Fällen, in denen der deren sozialer Geltungsanspruch als Arbeitgeber oder Wirtschaftsunternehmen betroffen ist: BGHZ 81, S. 78; BVerwGE 82, S. 78
[1142] vgl.: 2. Kap. Teil 2 B. I. 1. b)
[1143] vgl.: 2. Kap. Teil 2 B. I. 1. a)
[1144] vgl.: 2. Kap. Teil 1 B. I. 1. b)
[1145] vgl.: 2. Kap. Teil 1 B. I. 1. a)
[1146] vgl.: 2. Kap. Teil 2 A. II. 3. und 4.
[1147] vgl: 2. Kap. Teil 1 B. I. 2 b) aa)

sind.[1148] Ein solcher liegt darin, dass der Provider bzw. das Unternehmen, in dem der Adressat tätig ist, berechtigt ist, Nachrichten auszufiltern, soweit der Empfänger seine Einwilligung erklärt hat. Hierdurch wird das Recht des Adressaten, von unerwünschter Email-Werbung frei zu bleiben, realisiert. Bestünde hingegen eine Zustellungsverpflichtung auch bei Einwilligung des Empfängers mit dem Ausfiltern der Nachrichten, so wäre dieser faktisch seines Rechtes, von unerwünschter Korrespondenz frei zu bleiben, das sich einfachgesetzlich in der Opt-In-Lösung widerspiegelt, beraubt.

Aus verfassungsrechtlicher Sicht besteht daher keine Veranlassung zu einer von der gegenwärtigen Rechtslage abweichenden einfachgesetzlichen Regelung, welche die Zustellung sämtlicher Nachrichten gewährleistet, selbst wenn der Adressat mit einem Ausfiltern einverstanden ist.

3. Zwischenergebnis

Aus dem deutschen Verfassungsrecht ergibt sich keine Verpflichtung des Gesetzgebers zum Erlass von der geltenden Rechtslage abweichender Vorschriften.

II. Völker- und Gemeinschaftsrecht

Fraglich ist, ob die in Deutschland bestehende Rechtslage mit Gemeinschafts- (1.) und Völkerrecht (2.) in Einklang steht.

1. Gemeinschaftsrecht

Die Vorschriften des einfachen deutschen Gesetzesrechts könnten gegen Gemeinschaftsrecht verstoßen. Die Folgen eines solchen Verstoßes wurden bereits dargestellt.[1149] Im Folgenden wird das deutsche Recht am Maßstab des europäischen Sekundär- (a) und Primärrechts (b) überprüft.

a) Sekundärrecht

Fraglich ist, ob die einfachgesetzlichen Vorschriften gegen europäisches Sekundärrecht verstoßen. Dieses könnte der gesetzlichen Zulässigkeit der Überprüfung von Inhalts- und Headerdaten durch Filtersoftware entgegenstehen. Darüber hinaus könnte sich eine Verpflichtung des deutschen Gesetzgebers ergeben, die Versender von Emails davor zu schützen, dass ihre Emails aufgrund des Einsatzes von Spamfiltersoftware den Adressaten nicht erreichen.

Hier gewinnen die DSRL sowie die EK-DSRL Bedeutung. Allerdings stellt sich hinsichtlich noch nicht dauerhaft gespeicherter Emails bereits die Frage nach der Anwendbarkeit der Richtlinien. Sowohl Art. 3 Abs. 1 DSRL, als auch Art. 3 Abs. 1 EK-DSRL setzen für eine Eröffnung ihres Anwendungsbereichs voraus, dass personenbezogene Daten verarbeitet werden. Unter personenbezogenen Daten versteht die DSRL alle Informationen über eine bestimmte oder eine bestimmbare Person, Art. 2 lit. a) Hs. 1 DSRL. Bestimmt ist hierbei eine ausdrücklich genannte Person,[1150] während als bestimmbar eine Person angesehen wird, die

[1148] vgl: 2. Kap. Teil 1 B. I. 2 b) aa)
[1149] vgl.: 2. Kap. Teil 1 B. II. 1.
[1150] *Brühann* in Grabitz/Hilf, A 30, Art. 2, Rn. 8; *Dammann* in Simitis, § 3 BDSG, Rn. 21; *Gola/Schomerus*, § 3 BDSG, Rn. 9; *S. Meyer*, WRP 2002, S. 1029 f.; *Tinnefeld* in Roßnagel, 4.1., Rn. 20; *Tinnefeld/Ehmann/Gerling*, S. 279 f.

direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen oder kulturellen Identität sind, Art. 2 lit. a) Hs. 2 DSRL. Da die Definition im Wesentlichen der des BDSG entspricht,[1151] kann hier auf die oben gefundenen Ergebnisse verwiesen werden.[1152] Danach fehlt es bereits am Personenbezug der Daten. Die Richtlinien finden somit bereits keine Anwendung. Sie können daher den deutschen Gesetzgeber auch nicht zu einem Tätigwerden verpflichten dergestalt, dass die Überprüfung von Inhalt und Headerinformationen eingehender Nachrichten im Rahmen von Spamfiltermaßnahmen zu verbieten ist.
Gleiches gilt für die Blockade, das Löschen, Umleiten und Markieren eingehender Nachrichten vor deren endgültiger Speicherung, da hier, wie bereits dargestellt, ebenfalls keine personenbezogenen Daten betroffen sind.[1153] Da mit dem Filtereinsatz auch keine Kenntnisnahme der Inhalte von Emails einhergeht, greift auch die Vorschrift des Art. 5 EK-DSRL, welche die Vertraulichkeit der Kommunikation schützt, hier nicht ein und steht folglich dem Filtereinsatz nicht entgegen.

Etwas anderes könnte sich hinsichtlich der Frage nach der Zulässigkeit des Löschens bereits auf dem Server oder in der Mailbox des Empfängers gespeicherter Emails ergeben, da der Personenbezug der darin enthaltenen Daten, wie oben bereits dargestellt wurde, zu bejahen ist.[1154] Da im deutschen Recht das Löschen der personenbezogenen Daten nach § 35 Abs. 2 S. 1 BDSG zulässig ist, stellt sich hier die Frage, ob die Rechtslage den sekundärrechtlichen Vorgaben entspricht. Dies wäre einerseits dann der Fall, wenn auch nach Maßgabe des Sekundärrechts das Löschen der Nachrichten zulässig wäre, andererseits könnte eine richtlinienkonforme Rechtslage auch durch einfachgesetzliche Vorschriften außerhalb des BDSG herbeigeführt werden.

Fraglich ist also, ob das Löschen der Emails nach Maßgabe des Sekundärrechts zulässig ist. Art. 7 Hs. 1 DSRL sieht vor, dass die Verarbeitung personenbezogener Daten nur erfolgen darf, wenn ein in Art. 7 genannter Erlaubnistatbestand eingreift. Gemäß Art. 2 lit. b) DSRL stellt auch das Löschen von Daten eine Verarbeitung dar. Es stellt sich demnach die Frage, ob ein Erlaubnistatbestand eingreift.
Hier könnten hier die Voraussetzungen des Art. 7 lit. b) Alt. 1 DSRL vorliegen. Die Vorschrift sieht vor, dass die Verarbeitung personenbezogener Daten zulässig ist, wenn die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist, dessen Vertragspartei die betroffene Person ist. Betroffene Person ist allerdings nicht nur der Empfänger, der einen Vertrag mit dem Provider oder Unternehmen hat, der bzw. das die Emails ausfiltert, sondern auch der Absender hinsichtlich ihn betreffender Daten und Dritte in Bezug auf im Text enthaltener Informationen. Diese Personen werden grundsätzlich in keinem Vertragsverhältnis zu demjenigen stehen, der den Filtereinsatz veranlasst. Insofern greift Art. 7 lit. b) Alt. 1 DSRL nicht ein.[1155] Darüber hinaus könnte die Vorschrift eine Löschung von false positives keinesfalls rechtfertigen, da das Löschen gerade nicht der Erfüllung des Vertrages dient, dessen Ziel grundsätzlich das Zustellen der eingehenden Emails und Vorhalten auf dem Server bis zum Abruf ist.
Die Zulässigkeit des Verarbeitungsvorgangs könnte sich jedoch aus Art. 7 lit. f) DSRL ergeben. Der Erlaubnistatbestand greift ein, wenn die Verarbeitung zur Verwirklichung des berechtigten Interesses erforderlich ist, das von dem für die Verarbeitung Verantwortlichen

[1151] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a) (aa)
[1152] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)
[1153] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)
[1154] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a)
[1155] a.A.: *Art. 29 Datenschutzgruppe*, WP 118, S. 8

wahrgenommen wird, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Art. 1 Abs. 1 geschützt sind, überwiegen. Allerdings wurde im Rahmen des § 109 TKG dargelegt, dass von einer Erforderlichkeit des Löschens unerwünschter Emails angesichts der im Raum stehenden gegeneinander abzuwägenden Interessen nicht auszugehen ist.[1156] Gleiches hat hier zu gelten, da auch Art. 7 lit. f) DSRL auf die Erforderlichkeit des Verarbeitungsvorgangs abstellt.
Die Zulässigkeit des Einsatzes der Filtersoftware könnte sich jedoch aus Art. 4 Abs. 1 S. 1 Hs. 1 EK-DSRL ergeben. Die Vorschrift sieht vor, dass Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die Sicherheit ihrer Dienste zu gewährleisten. Im Fall von Viren greift Art. 4 Abs. 1 S. 1 Hs. 1 EK-DSRL unproblematisch ein, da durch Zustellung von virenbehafteten Emails nicht nur der Rechner des Empfängers, sondern daneben auch das gesamte System des Providers beschädigt werden kann.[1157] Fraglich ist, ob das Gleiche für Spammails gilt. Teilweise wird angenommen, Spammails würden zu einer Bedrohung der Sicherheit der Dienste des Email-Service-Providers führen, mit der Folge, dass der Einsatz der Filtersoftware nach Art. 4 Abs. 1 S. 1 Hs. 1 EK-DSRL gerechtfertigt wäre.[1158] Allerdings wurde oben bereits dargelegt, dass allein das Zusenden von unerwünschten Emails keine Gefahr für die Sicherheit der Dienste des Providers darstellt.[1159] Dies wäre nur dann der Fall, wenn Anhaltspunkte bestehen würden, dass der Server deshalb zusammenbricht, so etwa im Fall eines Mailbombing.[1160] Art. 4 Abs. 1 S. 1 Hs. 1 EK-DSRL vermag somit das Löschen der Daten nicht zu rechtfertigen.
Folglich ist das Löschen bereits auf dem Server eingegangener Emails nach Maßgabe des Sekundärrechts nicht zulässig.

Fraglich ist, ob deshalb die deutsche Rechtslage in Widerspruch zu Vorgaben im Gemeinschaftsrecht steht. Hier ist zu beachten, dass im deutschen Recht Vorschriften vorhanden sind, die dem Löschen eingehender Emails vor und nach Abruf durch den Empfänger entgegenstehen, vgl. §§ 206 Abs. 2 Nr. 2, 303 a StGB. Die hier fragliche Fallkonstellation ist demnach durch strafrechtliche Vorschriften erfasst. Insofern ist zwar keine Regelung im allgemeinen Datenschutzrecht, dafür jedoch in einer strafrechtlichen Norm getroffen worden. Im Übrigen ist das Löschen von Daten auch nach allgemeinem Datenschutzrecht nicht ohne Einschränkung möglich. So können Daten beispielsweise nicht gelöscht werden, wenn ein Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt würden, § 35 Abs. 2 S. 1 in Verbindung mit Abs. 3 Nr. 2 BSDG.
Demnach besteht keine Verpflichtung des deutschen Gesetzgebers, eine von der geltenden Rechtslage abweichende Regelung im Hinblick auf das Löschen in Emails enthaltener Daten zu treffen, da dies einerseits strafrechtlich sanktioniert und andererseits ausweislich der Vorschrift des § 35 Abs. 2 S. 1 in Verbindung mit Abs. 3 Nr. 1, 2 BDSG nicht ohne Weiteres möglich ist.

[1156] vgl.: 2. Kap. Teil 2 A. II. 3. b) cc) (1)
[1157] *Art. 29 Datenschutzgruppe*, WP 118, S. 5
[1158] *Art. 29 Datenschutzgruppe*, WP 118, S. 7
[1159] vgl.: 2. Kap. Teil 2 A. II. 3. b) cc) (1)
[1160] vgl.: 2. Kap. Teil 2 A. II. 3. b) cc) (1)

b) Primärrecht

Fraglich ist, ob die Vorschriften des einfachen deutschen Rechts im Einklang mit europäischem Primärrecht stehen. Ein Verstoß würde, wie oben dargestellt,[1161] zu einem Anwendungsvorrang der entsprechenden gemeinschaftsrechtlichen Vorschrift bzw. zu einer Verpflichtung zum Tätigwerden des Gesetzgebers führen.

In diesem Zusammenhang ist auch die Frage der Rechtmäßigkeit des Sekundärrechts zu überprüfen, auf dessen Grundlage das einschlägige nationale Recht erlassen wurde,[1162] da primärrechtswidriges Sekundärrecht im Rahmen einer Nichtigkeitsklage für nichtig erklärt werden kann, Art. 230, 231 EGV; dies hätte wiederum zur Folge, dass auch der nationale Umsetzungsakt förmlich außer Kraft zu setzen und soweit erforderlich durch neue rechtmäßige Maßnahmen zu ersetzen wäre.[1163]

aa) Europäische Grundfreiheiten

Fraglich ist, ob durch die genannten Vorschriften des deutschen einfachen Rechts in die Waren- oder Dienstleistungsfreiheit nach Art. 28 ff., 49 ff. EGV eingegriffen bzw. eine gesetzgeberische Schutzpflicht verletzt wird. Eine Verletzung der genannten Grundfreiheiten könnte sich dabei einerseits aus der Tatsache ergeben, dass nach Maßgabe des einfachen deutschen Rechts die durch den Filtereinsatz bewirkte Überprüfung von Inhalts- und Headerinformationen zulässig ist. Daneben könnte sich aus der Waren- oder Dienstleistungsfreiheit eine Verpflichtung des deutschen Gesetzgebers ergeben, Versender von Werbe-Emails vor Maßnahmen Privater zu schützen, die dazu führen, dass die Nachrichten den Empfänger nicht erreichen.

Allerdings ist nicht davon auszugehen, dass die blosse Überprüfung der Headerinformationen oder des Inhalts einer Email, selbst wenn es sich hierbei um Werbung mit Binnenmarktrelevanz handelt, die genannten Grundfreiheiten beschränkt. Denn diese Maßnahme für sich genommen bewirkt nicht, dass der innergemeinschaftliche Verkehr mit Waren oder Dienstleistungen in irgendeiner Art und Weise beeinträchtigt wird. Daher erfordern die Europäischen Grundfreiheiten hinsichtlich der Zulässigkeit der Überprüfung von Inhalt und Header einer Email keine andere Regelung.

Daneben stellt sich jedoch die Frage, ob der deutsche Gesetzgeber nach Maßgabe der Warenverkehrsfreiheit nach Art. 28 ff. EG oder der Dienstleistungsfreiheit nach den Art. 49 ff. EG verpflichtet ist, die Versender von Werbe-Emails vor Maßnahmen Privater zu schützen, die diese Emails ausfiltern. Allerdings stellen selbst mitgliedstaatliche Werbebeschränkungen für Waren keine Maßnahmen gleicher Wirkung wie Ausfuhrbeschränkungen dar, wie oben bereits dargelegt wurde.[1164] Gleiches hat im Bereich faktischer Beeinträchtigungen grundfreiheitsrelevanter Bereiche durch Private zu gelten. Im Übrigen fallen Werbebeschränkungen nach den oben dargestellten Grundsätzen, bereits unter die Keck-Formel,[1165] soweit die Beschränkungen vom Einfuhrmitgliedstaat ausgehen, weshalb der Schutzbereich der Grundfreiheiten bereits nicht eröffnet ist. Filtern in Deutschland ansässige Provider somit eingehende Emails, so greift bereits die Keck-Formel,

---

[1161] vgl.: 2. Kap. Teil 1 B. II. 1.
[1162] vgl.: 2. Kap. Teil 1 B. II. 1. b)
[1163] *Borchardt* in Lenz, Art. 233 EGV, Rn. 6; *Cremer* in Calliess/Ruffert, Art. 233 EGV, Rn. 5; *Gaitanides* in v. d. Groeben/Schwarze, Art. 231 EGV, Rn. 5, Art. 233 EGV, Rn. 12
[1164] vgl.: 2. Kap. Teil 1 B. II. 1. b) aa) (1)
[1165] vgl.: 2. Kap. Teil 1 B. II. 1. b) aa) (2)

so dass auch hier der Schutzbereich der Grundfreiheiten bereits nicht eröffnet ist. Darüber hinaus wären selbst durch den Staat ausgesprochene Werbebeschränkungen nach Maßgabe der Cassis-Rechtsprechung dem Schutzbereich der Waren- und Dienstleistungsfreiheit entzogen.[1166] Für faktische Beschränkungen und einer möglichen daraus resultierenden Schutzpflicht des mitgliedstaatlichen Gesetzgebers kann nichts anderes gelten, da die Auswirkungen insofern ähnlich sind.
Daneben kann es keine Verpflichtung des nationalen Gesetzgebers geben, ein nach gemeinschaftsrechtlichen Maßstäben, nämlich Art. 13 Abs. 1 EK-DSRL unzulässiges Verhalten, nämlich Direktwerbung mittels Email ohne vorherige Einwilligung des Empfängers gegen Maßnahmen Privater zu schützen. Hier gewinnen also die bereits dargestellten Grundsätze zur Frage der Zulässigkeit von Email-Werbung Bedeutung.[1167]

Insofern ergibt sich aus den europäischen Grundfreiheiten keine Verpflichtung des deutschen Gesetzgebers zu einer von der geltenden Rechtslage abweichenden Regelung.

bb) Europäische Grundrechte

Fraglich ist, ob die genannten Vorschriften des einfachen deutschen Rechts mit den Gemeinschaftsgrundrechten in Einklang stehen. Es ist danach zu prüfen, ob dem deutschen Gesetzgeber aufgrund der Gemeinschaftsgrundrechte eine Verpflichtung zukommt, die Frage nach der Zulässigkeit der Überprüfung der Inhalts- und Headerinformationen eingehender Emails durch die Spamfiltersoftware anders zu regeln. Ebenso stellt sich die Frage, ob aus den Grundrechten auf Gemeinschaftsebene eine Verpflichtung des deutschen Gesetzgebers resultiert, Versender von Werbe-Emails vor Maßnahmen Privater zu schützen, die bewirken, dass diese Nachrichten dem Adressaten nicht zugehen und falls ja, ob dieser Pflicht bereits nachgekommen wurde.

Die Tatsache, dass das Überprüfen von Inhalts- und Headerinformationen nach dem deutschen einfachen Recht zulässig ist, könnte das die Gemeinschaftsgrundrechte auf Privatleben und Korrespondenz beeinträchtigen.
Auch auf gemeinschaftsrechtlicher Ebene ist das Recht auf Privatleben geschützt, wobei dieses im Wesentlichen dem in Art. 8 Abs. 1 EMRK kodifizierten Recht entspricht.[1168] Das Gleiche gilt im Bereich des Rechts auf Korrespondenz, da EuGH und EuG auf Art. 8 Abs. 1 EMRK Bezug nehmen.[1169] Eine Verpflichtung zum Tätigwerden könnten die Rechte auf Privatleben oder Korrespondenz begründen, wenn ihnen eine Schutzpflichtdimension zukäme.

Dabei ist einerseits fraglich, ob die Rechte auf Privatleben und Korrespondenz durch das Überprüfen des Inhalts und der Headerinformationen eingehender Emails im Rahmen der Spamfilterung berührt werden. Zwar ist eine Tendenz des EGMR erkennbar, das Recht auf Privatleben sehr weit auszulegen, um die freie Entfaltung der Persönlichkeit des Grundrechtsträgers zu gewährleisten,[1170] was aufgrund der Bezugnahme des EuGH auf das Konventionsrecht und die dazu ergangene Rechtsprechung des EGMR entsprechend für das Gemeinschaftsgrundrecht angenommen werden kann. So sind nach der Rechtsprechung des

[1166] vgl.: 2. Kap. Teil 1 B. II. 1. b) aa) (3)
[1167] vgl.: 2. Kap. Teil 1
[1168] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)
[1169] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (1) (a)
[1170] EGMR, NJW 1993, S. 718 ff. - Niemitz/Deutschland; *Frowein* in Ders./Peukert, Art. 8 EMRK, Rn. 3; Grabenwarter, § 22, Rn. 6; *Meyer-Ladewig*, Art. 8 EMRK, Rn. 3; *Uerpmann* in Ehlers, § 3, Rn. 3 ff.

EGMR das Recht auf ein selbstbestimmtes Leben,[1171] berufliche Tätigkeiten und das Hinaustreten in die Öffentlichkeit,[1172] auf den Schutz persönlicher Daten,[1173] vor dem Abhören und Aufzeichnen privater und geschäftlicher Telefongespräche[1174] und sonstiger Gespräche[1175] vom Schutzbereich des Rechts auf Privatleben erfasst. Des Weiteren stellt jegliche Registrierung und Weitergabe von Informationen einen Eingriff in das Recht auf Privatleben dar und zwar auch dann, wenn es sich um Informationen handelt, die der Betroffene selbst zu einem anderen Zeitpunkt veröffentlicht hat.[1176] Allerdings ist auch hier zu berücksichtigen, dass es bei der Filterung weder zu einer Kenntnisnahme der überprüften Daten und Inhalte durch eine Person, noch zu einer Speicherung der Emails kommt, so dass eine Beeinträchtigung des Rechts auf Privatsphäre aus den im Bereich des Datenschutz- und allgemeinen Persönlichkeitsrechts genannten Gründen ausscheidet.[1177]

Eine Verpflichtung des deutschen Gesetzgebers zum Schutz vor der Überprüfung von Inhalt- und Headerinformationen durch Private könnte sich jedoch aus dem Grundrecht auf Korrespondenz ergeben. Dieses richtet sich gegen das Anhalten und Verzögern von Briefen, das Öffnen, das Lesen und Kopieren, das Löschen bestimmter Stellen, Genehmigungsvorbehalte sowie Beschränkungen der Zahl oder Länge von Briefen.[1178] Aus den verschiedenen Urteilen zum Recht auf Korrespondenz lässt sich folgern, dass stets diejenigen Vorgänge in den Schutzbereich des Konventionsrechts eingreifen, die entweder eine inhaltliche Kontrolle des Briefverkehrs mit sich bringen, das Recht auf Versendung von Briefpost beschränken oder bewirken, dass der Betroffene nicht vollständig, verspätet oder überhaupt nicht vom Inhalt der Nachricht Kenntnis nehmen kann. Allerdings liegt hier kein derartiger Fall vor, der etwa einem Lesen oder Kopieren des Briefs vergleichbar ist, da der Inhalt und die Steuerungsdaten der Nachricht weder von einer Person gelesen, noch für den späteren Gebrauch gespeichert werden.[1179]
Die Rechte auf Korrespondenz und Privatleben werden daher durch das Überprüfen von Inhalt und Headerinformationen durch die Filtersoftware nicht berührt.

Fraglich ist jedoch, ob sich eine Verpflichtung des deutschen Gesetzgebers ergibt, das Löschen, Blockieren, Umleiten und Markieren von Nachrichten im Rahmen von Spamfiltermaßnahmen zu untersagen.
Eine derartige Verpflichtung könnte das Recht auf Korrespondenz begründen, wenn ihm eine Schutzpflichtdimension zukäme. Das Anhalten und Verzögern von Briefen und das Löschen bestimmter Stellen fallen grundsätzlich in den Schutzbereich der Korrespondenz.[1180] Hierbei ist davon auszugehen, dass der Schutzbereich die individuelle Kommunikation nach Maßgabe

[1171] EGMR, EuGRZ 2002, S. 234 - Pretty
[1172] EGMR, NJW 1993, S. 718 ff. - Niemitz/Deutschland, EGMR, Nr. 44647/98 - Peck gegen Vereinigtes Königreich
[1173] EGMR, Nr. 10/1985/96/144 - Leander gegen Schweden; EGMR, Nr. 27798/95 - Amann gegen Schweiz; EGMR, Nr. 28341/95 - Rotaru gegen Rumänien; EGMR, Nr. 44647/98 - Peck gegen Vereinigtes Königreich
[1174] EGMR, EuGRZ 1979, S. 278 ff Klass/Bundesrepublik Deutschland; EGMR, Nr. 13/1997/797/1000 - Kopp gegen Schweiz; EGMR, Nr. 27798/95 - Amann gegen Schweiz
[1175] EGMR, Nr. 44787/98- P.G. und J.H. gegen Vereinigtes Königreich
[1176] EGMR, Nr. 10/1985/96/144 - Leander gegen Schweden; EGMR, Nr. 28341/95 - Rotaru gegen Rumänien
[1177] ähnlich: *Art. 29 Datenschutzgruppe*, WP 118, S. 3, die in ihrem Arbeitspapier im Hinblick auf Art. 8 EMRK anmerkt, eine Überwachung und damit ein Eingriff in die Privatsphäre liege nur dann vor, wenn ein Dritter Zugang zum Inhalt oder den Verbindungsdaten erhält.
[1178] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)
[1179] ähnlich: *Art. 29 Datenschutzgruppe*, WP 118, S. 6, die in ihrem Arbeitspapier im Hinblick auf Art. 8 EMRK anmerkt, eine Überwachung und damit ein Eingriff in die Privatsphäre liege nur dann vor, wenn ein Dritter Zugang zum Inhalt oder den Verbindungsdaten erhält.
[1180] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)

der jeweils bestehenden faktischen und technischen Möglichkeiten umfasst.[1181] Demnach ist die Übermittlung mittels elektronischer Post vom Gemeinschaftsgrundrecht wie vom Konventionsrecht[1182] ebenso erfasst, wie das Telefonieren. Dies bedeutet, dass derjenige, der eingehende elektronische Nachrichten löscht, blockiert oder so umleitet, dass der Adressat die Email nicht mehr erhält im konventionsrechtlich relevanten Bereich handelt. Das blosse Markieren der Nachrichten fällt bereits deshalb nicht in den Schutzbereich des Konventionsrechts auf Korrespondenz, weil ausweislich der oben genannten Rechtsprechung hiervon nur solche Maßnahmen erfasst sind, die bewirken, dass die versandten Nachrichten verzögert oder gar nicht zugestellt werden.
Im Hinblick auf die übrigen Maßnahmen stellt sich das Problem, dass diese grundsätzlich durch Privatpersonen vorgenommen werden, nicht durch die Konventionsstaaten. Allerdings ist auch im Bereich der Gemeinschaftsgrundrechte -unabhängig von der Frage, ob sich diese hier überhaupt an die Mitgliedstaaten richten-[1183] davon auszugehen, dass, selbst wenn eine Schutzpflichtdimension zu bejahen sein sollte,[1184] stets nur eine Verpflichtung des jeweiligen Grundrechtsadressaten zur Ergreifung effektiver Maßnahmen, nicht aber zur Vornahme bestimmter Handlungen in Betracht kommt.[1185] Somit können auch die Gemeinschaftsgrundrechte den deutschen Gesetzgeber nicht zu einem bestimmten Tätigwerden verpflichten. Aus der der Europäischen Verfassung, die den Text der GRC ohne inhaltliche Änderungen übernommen hat, ergibt sich nichts anderes, da dem bisher noch nicht in Kraft getretenen Europäischen Verfassungsvertrag keine rechtliche Bindungswirkung zukommt. Hier wurde der Gesetzgeber bereits tätig, indem er bestimmte Maßnahmen in Bezug auf Emails unter Strafe stellte. Insbesondere greifen die Straftatbestände der §§ 303 a Abs. 1, 206 Abs. 2 Nr. 2 StGB. Da der Gesetzgeber somit tätig wurde, hat er seine Schutzpflicht erfüllt. Eine durch die Konvention begründete Verpflichtung zu einer anderen Lösung kann aufgrund des dem Gesetzgeber zustehenden Spielraums nicht bestehen.

Demnach folgt auch aus den Europäischen Grundrechten keine gesetzgeberische Verpflichtung, von der geltenden Rechtslage abweichende Vorschriften zu schaffen.

2. Völkerrecht

Es stellt sich die Frage, ob die Regelungen, die nach Maßgabe des einfachen deutschen Rechts hinsichtlich der Frage der Zulässigkeit des Einsatzes von Spamfiltersoftware gelten, im Einklang mit den Vorgaben des Völkerrechts stehen. Wäre dies nicht der Fall, so könnte sich eine Verpflichtung des deutschen Gesetzgebers ergeben, die Kommunikationspartner vor dem Überprüfen von Inhalts und Headerinformationen ihrer Emails sowie die genannten weiteren Vorgehensweisen in Bezug auf positiv gescannte Nachrichten zu schützen.

Im Hinblick auf die Frage, inwieweit Vorgaben der EMRK den deutschen Gesetzgeber zu einer abweichenden Regelung der Frage nach der Zulässigkeit der Überprüfung von Inhalt- und Headerinformationen eingehender Emails verpflichten, kann auf die Ausführungen zu den Gemeinschaftsgrundrechten verwiesen werden, da diese mit den Konventionsrechten im

[1181] *Kugelmann*, EuGRZ 2003, S. 21
[1182] EGMR, Nr. 8691/79 - Malone/Vereinigtes Königreich; EGMR, Nr. 88/1997/872/1084 - Lambert/Frankreich; *Kugelmann*, EuGRZ 2003, S. 16 ff., 22
[1183] vgl. dazu bereits: 2. Kap. Teil 1 B. II. 1. b) bb)
[1184] dafür: *Borowsky* in Meyer, Art. 51 GRC, Rn. 22; *Suerbaum*, EuR 2003, S. 390 ff.; *Thym*, NJW 2006, S. 3252; dagegen: *Nicolaysen*, EuR 2003, S. 723; differenzierend: *Kingreen* in Calliess/Ruffert, Art. 51 GRC, Rn. 25; vgl. zu Schutzpflichten im Bereich der Grundfreiheiten: EuGH, Slg. 1996, I-2143 - P./S. und Cornwall Council-Transsexuelle; EuGH, NJW 1998, S. 1931 ff. - Kommission/Frankreich
[1185] EuGH, NJW 1998, S. 1931 ff.- Kommission/Frankreich; *Ehlers* in Ders., § 14, Rn. 24; *Kühling*, NJW 1999, S. 403

Wesentlichen deckungsgleich sind.[1186] Danach werden die Rechte auf Korrespondenz und Privatleben durch das Überprüfen von Inhalt und Headerinformationen durch die Filtersoftware nicht berührt.

Fraglich ist, ob die EMRK den deutschen Gesetzgeber dazu verpflichtet, Versender von Werbe-Emails vor Maßnahmen Privater zu schützen, die diese Emails ausfiltern. Zwar kommt sowohl dem Konventionsrecht auf Privatleben, als auch dem Recht auf Korrespondenz eine Schutzpflichtdimension zu.[1187] Allerdings besteht in diesem Bereich nach der Rechtsprechung des EGMR ein Beurteilungsspielraum der Konventionsstaaten, welcher Ausfluss des Grundsatzes der Subsidiarität des EMRK-Grundrechtsschutzes gegenüber dem nationalen Grundrechtsschutz ist.[1188] Insofern gibt die EMRK den Konventionsstaaten keine bestimmte Regelung vor.
Hier wurde der Gesetzgeber bereits tätig, indem er bestimmte Maßnahmen in Bezug auf Emails unter Strafe stellte. Insbesondere greifen hier die Straftatbestände der §§ 303 a Abs. 1, 206 Abs. 2 Nr. 2 StGB. Da der Gesetzgeber somit tätig wurde, hat er seine Schutzpflicht erfüllt. Eine durch die Konvention begründete Verpflichtung zu einer anderen Lösung kann aufgrund des dem Gesetzgeber zustehenden Spielraums nicht bestehen.

Im Hinblick auf die Frage nach der Zulässigkeit der Überprüfung des Inhalts sowie der Headerinformationen eingehender Emails könnten internationale Abkommen eingreifen.
Allerdings finden hier mangels Personenbezugs der betroffenen Daten weder das Abkommen über den Datenschutz des Europarats,[1189] noch die Leitlinien der OECD für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten[1190] oder die Richtlinien der Generalversammlung zur Verarbeitung personenbezogener Daten in automatisierten Dateien[1191] Anwendung. Die beiden letztgenannten internationalen Regelungen entfalten darüber hinaus auch keine völkerrechtlich bindende Wirkung.[1192] Hinsichtlich der Frage nach der Zulässigkeit des Löschens bereits eingegangener Emails kann auf die Ausführungen zur Datenschutzrichtlinie verwiesen werden.[1193]

III. Ergebnis

Was die Zulässigkeit der Filtermaßnahmen betrifft stehen die genannten einfachgesetzlichen Vorschriften sowie das einschlägige Sekundärrecht mit den jeweils höherrangigen Vorgaben des Verfassungs-, Gemeinschafts- und Völkerrechts im Einklang.

[1186] vgl. zum Grundrecht auf Meinungsfreiheit und Korrespondenz: 2. Kap. Teil 1 B. II. 1. b) bb) (1) (a); vgl. zum Recht auf Privatleben: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)
[1187] vgl.: 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa)
[1188] EGMR, EuGRZ, S. 317 - Johnston u.a./Irland; EGMR, Serie A, Nr. 172, S. 18 - Powell u. Rayner/Vereinigtes Königreich; EGMR, NJW 1995, S. 2154 - Keegan/Irland; *Bernsdorff* in Meyer, Art. 7 GRC, Rn. 16; *Meyer-Ladewig*, Art. 8 EMRK, Rn. 2
[1189] ABl. C 364 vom 18.12.2000, 1.
[1190] OECD-Dokument C (80) 58 (Final)
[1191] „Guidelines Concerning Computerized Data Files", Resolution 44/132-14.12.1990- UN Doc. E/CN.4/Sub. 2/1988/22
[1192] *Burkert* in Roßnagel, 2.3., Rn. 30; *Schaar*, Datenschutz im Internet, Rn. 79; *Simitis* in Ders., § 1 BDSG, Rn. 144, 149
[1193] vgl.: 2. Kap. Teil 2 B. II. 1. a)

C. Ergebnis

Die durch den Einsatz der Filtersoftware bewirkte Überprüfung von Inhalt und Headerinformationen ist nach Maßgabe des deutschen Rechts zulässig. Unzulässig sind Vorgänge, welche die Zustellung der Email verhindern, das Löschen von Nachrichten nach Einstellen in der Mailbox durch den Provider oder das Unternehmen, das den Email-Zugang zur Verfügung stellt sowie das Abändern der vom Absender ausgefüllten Subjektzeile. Die geltende Rechtslage steht im Einklang mit den maßgeblichen höherrangigen Vorschriften.

3. Kapitel: Rechtslage in den USA

Nachfolgend wird die Rechtslage in den USA dargestellt.
Gegenstand der Arbeit ist die Frage nach der rechtlichen Zulässigkeit der verschiedenen Maßnahmen, die zur automatisierten Identifizierung und Abwehr von Werbe-Emails vorgenommen werden. Der Einsatz von Filtersoftware stellt die Reaktion auf das Versenden unverlangter kommerzieller Emails dar. Die Widerrechtlichkeit der abgewehrten Nachrichten könnte folglich mögliche Abwehrmaßnahmen rechtfertigen. Deshalb wird nachfolgend zunächst darauf eingegangen, ob bzw. unter welchen Voraussetzungen der Versand solcher Emails nach Maßgabe des US-amerikanischen Rechts als zulässig anzusehen ist (Teil 1). Anschließend wird dargestellt, wie technische Maßnahmen zur Identifizierung und Vermeidung unerbetener Werbe- Emails rechtlich zu beurteilen sind (Teil 2).

Teil 1: Zulässigkeit unerbetener elektronischen Nachrichten

Die rechtliche Zulässigkeit unverlangter elektronischer Werbepost wird zunächst an den Vorgaben des einfachen Rechts gemessen (A.), im Anschluss werden die einschlägigen Vorschriften darauf überprüft, ob sie im Einklang mit völker- und verfassungsrechtlichen Vorgaben stehen (B.).

A. Einfaches Recht

Das US-amerikanische Recht wird unterteilt in Bundesrecht (I.) und das Recht der einzelnen Bundesstaaten (II.).

I. Bundesrecht

Dem uneingeschränkten Versand unverlangter elektronischer Werbe-Emails könnte auf Bundesebene der so genannte CAN-SPAM Act entgegenstehen, der in 15 U.S.C. §§ 7701 ff. und 18 U.S.C. § 1037 niedergelegt ist.

In den Anwendungsbereich des CAN-SPAM Act fallen allerdings nicht sämtliche Werbe-Emails, sondern lediglich solche, die als kommerzielle Email[1194] im Sinne der Definition des 15 U.S.C. § 7702 (2) (A) zu qualifizieren sind.[1195]
Unter einer kommerziellen Email versteht das Gesetz jede elektronische Nachricht, deren primärer Zweck die kommerzielle Werbung oder die Förderung eines kommerziellen Produktes oder einer Dienstleistung ist, 15 U.S.C. § 7702 (2) (A), wobei auch die Werbung für eine kommerzielle Web-Seite erfasst sein soll. Vom Begriff der kommerziellen Email ausgenommen sind dagegen solche Nachrichten, die Transaktionen bzw. Beziehungen betreffen, 15 U.S.C. § 7702 (2) (B). Hierunter werden Emails gefasst, deren primärer Zweck darin besteht, eine kommerzielle Transaktion, die der Empfänger zuvor mit dem Versender vereinbart hat, zu fördern, zu vervollständigen oder zu bestätigen, 15 U.S.C. § 7702 (17) (A) (i), bzw. Garantie-, Produktrückrufs- oder Sicherheitsinformationen in Bezug auf ein kommerzielles Produkt zu übermitteln, das der Empfänger gekauft hat oder nutzt, 15 U.S.C. § 7702 (17) (A) (ii). Schließlich betreffen solche Nachrichten Transaktionen oder Beziehungen, deren primärer Zweck es ist, über Änderungen bestimmter Bedingungen oder des Status des Empfängers zu unterrichten oder einen Kontoauszug oder eine andere Abrechnung in Bezug

[1194] „commercial electronic message“
[1195] *Fritzemeyer*, K & R 2005, S. 50; *Manishin/Joyce*, The Computer & Internet Lawyer 2004, Nr. 9, S. 2; auf das Vorliegen einer kommerziellen elektronischen Nachricht nehmen Bezug: 18 U.S.C. § 1037 (a) (1), 15 U.S.C. § 7704 (a) (1) - (3), (4) (A) und 15 U.S.C. § 7705 (a)

auf ein Abonnement, eine Mitgliedschaft, ein Konto, ein Darlehen oder eine vergleichbare Geschäftsbeziehung, insbesondere einen noch nicht abgewickelten Kauf- oder Dienstvertrag, zu übermitteln, 15 U.S.C. § 7702 (17) (A) (iii). Auch den Empfänger betreffende Informationen im Hinblick auf ein Arbeitsverhältnis oder Rentenansprüche betreffen lediglich Beziehungen und Transaktionen, 15 U.S.C. § 7702 (17) (A) (iv). Schließlich sind Emails, deren primärer Zweck darin besteht, die Lieferung von Waren oder die Erbringung von Dienstleistungen zu ermöglichen, auf die der Empfänger einen vertraglichen Anspruch hat, als Transaktions- oder Beziehungsnachricht anzusehen, 15 U.S.C. § 7702 (17) (A) (v). Eine elektronische Nachricht wird danach nicht bereits deshalb zu einer kommerziellen Email im Sinne des CAN- SPAM Act, weil sie auf kommerzielle Rechtsträger Bezug nimmt oder einen Link zu deren Web-Seite enthält, sofern sich nicht aus dem Inhalt oder den Umständen ergibt, dass ihr primärer Zweck darin besteht, ein kommerzielles Produkt oder eine Dienstleistung zu vermarkten, 15 U.S.C. § 7702 (2) (D).

Die positiven und negativen Abgrenzungsmerkmale, die für die Frage nach dem Vorliegen einer kommerziellen elektronischen Nachricht heranzuziehen sind, stellen grundsätzlich darauf ab, worin der primäre Zweck der Nachricht besteht. Die Federal Trade Commission (FTC) hat diesen Begriff definiert. Es ergeben sich unterschiedliche Ergebnisse, je nachdem, welche Inhalte die fragliche Email enthält. Beinhaltet eine Email ausschließlich kommerzielle Werbung oder Informationen, die den Verkauf eines Produktes oder die Inanspruchnahme einer Dienstleistung fördern sollen, so dient sie primär einem kommerziellen Zweck.[1196] Enthält eine Email hingegen sowohl kommerzielle, als auch Transaktionen oder Beziehungen betreffende Inhalte, so ist ihr primärer Zweck nur dann kommerzieller Art, wenn entweder der Empfänger bereits anhand der Subjektzeile berechtigterweise davon ausgehen kann, dass die Nachricht kommerziellen Inhalts ist, wobei die Angabe unrichtiger, missverständlicher Subjektzeilen nach 15 U.S.C. § 7704 (a) (2) verboten ist, oder der nicht-kommerzielle Inhalt nicht gänzlich oder hauptsächlich am Anfang des Nachrichtentextes erscheint.[1197] Das gleiche Abgrenzungkriterium findet auch Anwendung, wenn eine Email sowohl kommerzielle, als auch solche Inhalte enthält, die weder kommerziell, noch transaktions- oder beziehungsbezogen sind.[1198] Enthält eine Email ausschließlich Transaktionen oder Beziehungen betreffende Inhalte so ist ihr primärer Zweck nicht kommerziell.[1199]

Die eben genannten durch die FTC entwickelten Kriterien haben zur Folge, dass der primäre Zweck einer Email bereits dann als kommerziell anzusehen ist, wenn sich dies aus der Subjektzeile ergibt.[1200] Lässt nicht bereits die Subjektzeile auf einen kommerziellen Inhalt schließen, so ist auf den Inhalt der Nachricht abzustellen. Enthält die Email kommerzielle und nicht-kommerzielle Inhalte, so ist entscheidend, ob der nicht-kommerzielle Inhalt am Beginn der Nachricht erscheint. Ist dies der Fall, so wird der primäre Zweck der Nachricht als nicht-kommerziell angesehen. Gehen dem kommerziellen Bestandteil der Nachricht jedoch keine substanziellen nicht-kommerziellen Inhalte voraus, so ist vom kommerziellen Charakter der Email auszugehen, wobei bislang keine Definition des Terminus „substanziell“ existiert.[1201]

Festzuhalten bleibt, dass den Vorschriften des CAN-SPAM Act sogar offensichtlich werbende Emails entzogen werden können, indem dem werbenden Inhalt nicht-kommerzielle

---

[1196] Titel 16 Kapitel 1 des Code of Federal Regulations, Abschnitt 316.3 (a) (1); vgl. auch: *Lewczak*, The Computer & Internet Lawyer 2005, Nr. 5, S. 11

[1197] Titel 16 Kapitel 1 des Code of Federal Regulations, Abschnitt 316.3 (a) (2) (i), (ii); *Lewczak*, The Computer & Internet Lawyer 2005, Nr. 5, S. 11

[1198] Titel 16 Kapitel 1 des Code of Federal Regulations, Abschnitt 316.3 (a) (3) (i), (ii); *Lewczak*, The Computer & Internet Lawyer 2005, Nr. 5, S. 11

[1199] Titel 16 Kapitel 1 des Code of Federal Regulations, Abschnitt 316.3 (b); *Lewczak*, The Computer & Internet Lawyer 2005, Nr. 5, S. 11

[1200] *Lewczak*, The Computer & Internet Lawyer 2005, Nr. 5, S. 11

[1201] *Lewczak*, The Computer & Internet Lawyer 2005, Nr. 5, S. 11

Informationen vorangestellt werden, die jedoch substanziell sein müssen.[1202] Generell vom Anwendungsbereich des CAN-SPAM Act ausgenommen sind Emails, deren primärer Zweck nicht kommerziell ist, so etwa Nachrichten politischer oder religiöser Natur.[1203]

Ist eine kommerzielle Email nach den Vorgaben des CAN-SPAM Act unzulässig, so zieht dies unterschiedliche Folgen nach sich. Teilweise können bestimmte Personen oder Rechtsträger auf zivilrechtlichem Weg gegen denjenigen vorgehen, der gegen den CAN-SPAM Act verstoßen hat. So können die Justizminster der Bundesstaaten sowie einige andere staatliche Amtsträger im Namen der Bürger des betroffenen Staates Klage erheben, wenn sie der Auffassung sind, dass deren Interessen bedroht sind oder durch die Verletzungshandlung negativ beeinflusst werden, 15 U.S.C. § 7706 (f) (1). Die Klage kann sich dabei einerseits auf ein Verbot weiterer Verletzungshandlungen richten, 15 U.S.C. § 7706 (f) (1) (A), andererseits auf Schadensersatz,[1204] 15 U.S.C. § 7706 (f) (B). Neben den genannten staatlichen Amtsträgern sind auch Internet-Service-Provider dazu ermächtigt, Klage einzureichen, 15 U.S.C. § 7706 (g) (1). Auch sie sind berechtigt, das Verbot weiterer Verletzungen oder aber Schadensersatz in der Höhe des tatsächlichen Verlustes oder des nach 15 U.S.C. § 7706 (g) (3) berechneten Betrages zu verlangen.[1205] Als klageberechtigte Internet-Service-Provider sind auch Arbeitgeber anzusehen, die ihren Arbeitnehmern einen Internet-Zugang anbieten.[1206] Im Übrigen besteht eine Befugnis der FTC, Unterlassungsverfügungen zu erlassen und zivilrechtliche Sanktionen zu verhängen.[1207] Aus der abschließenden Aufzählung der klageberechtigten Personenkreise in den Vorschriften des CAN-SPAM Act ergibt sich, dass das Gesetz keine Möglichkeit für Privatpersonen vorsieht, mittels Klage auf dem Zivilrechtsweg gegen Versender kommerzieller Emails vorzugehen.[1208]
Bestimmte Verstöße gegen den CAN-SPAM Act sind strafrechtlich sanktioniert. Dabei kann der Täter mit einer Gefängnisstrafe von bis zu fünf Jahren belegt werden, wobei sich die Höhe der Strafe nach der Art und der Schwere des Verstoßes richtet, 18 U.S.C. § 1037 (b) (1), (2), (3). Zusätzlich kann das Gericht die Einziehung des durch die Tat erlangten Gewinns sowie der technischen Einrichtungen, der Software und weiteren Ausrüstung anordnen, die der Täter

---

[1202] *Kennedy/Lyon*, The Computer & Internet Lawyer, Nr. 2, S. 7
[1203] *Fritzemeyer*, K & R 2005, S. 57; *Geary/Dave*, Computers & Law, März 2005, S. 19
[1204] Dabei ist entweder der wirklich entstandene Schaden oder aber eine nach 15 U.S.C. § 7706 (f) (3) zu berechnende Pauschale zu ersetzen, 15 U.S.C. § 7706 (f) (1) (B). Maßgebend ist der jeweils höhere Betrag. Der nach U.S.C. § 7706 (f) (3) zu ersetzende Schadensersatz errechnet sich, indem die Zahl der Verletzungen, also der versandten Emails, mit einem Betrag von bis zu US- $ 250,00 multipliziert wird, 15 U.S.C. § 7706 (f) (3) (A). Der Betrag darf $ 2.000.000 nicht überschreiten. Unter bestimmten Umständen wird der Betrag erhöht oder reduziert, vgl. 15 U.S.C. § 7706 (f) (3) (C).
[1205] Der Geldbetrag mit dem eine einzelne Verletzung geahndet wird, beträgt dabei jedoch lediglich $ 25,00, vgl. 15 U.S.C. § 7706 (g) (3) (ii). Auch hier können erschwerende oder mildernde Umstände zu einer Erhöhung oder Reduktion des Schadensersatzes führen.
Im März 2004 erhoben vier der größten Internet-Service-Provider der USA, America Online Inc., Earthlink Inc., Microsoft Inc. und Yahoo! Klage in ihren jeweiligen Sitzsstaaten gegen Spammer auf der Basis des CAN-SPAM Act, vgl.: *BNA* 2004, S. 1024; *Funk/Zeifang/Johnson/Spessard*, CRi 2004, S. 142; *Geary/Dave*, Computers & Law, März 2005, S. 20
[1206] *BNA* 2004, S. 467; *Funk/Zeifang/Johnson/Spessard*, CRi 2004, S. 142
[1207] Ein Verstoß gegen den CAN- SPAM Act wird als unlautere oder irreführende Handlung eingestuft, 15 U.S.C. § 7706 (a), die in den Zuständigkeitsbereich der FTC fällt. In Übereinstimmung mit seiner Durchsetzungsbefugnis darf die FTC ermitteln, Geldstrafen auferlegen, Verfügungen im Vergleichsweg erlassen oder Verstöße dem Justizministerium melden, 15 U.S.C. § 7706 (a) in Verbindung mit 15 U.S.C. 57 a (a) (1) (B); vgl.: *Funk/Zeifang/Johnson/Spessard*, CRi 2004, S. 142; *Kennedy/Lyon*, The Computer & Internet Lawyer 2005, Nr. 2, S. 5 ; die FTC erhob gegen verschiedene Unternehmen Klage wegen illegaler Spam-Versendung, vgl.: Federal Trade Commission v. Phoenix Avatar LLC, N.D. Ill., No. 04C 2897; Federal Trade Commission v. Global Web Promotions Pty Ltd., N.D. Ill., No. 04C 3022, beide abrufbar unter: http://www.ftc.gov (letzter Abruf: 29.04.2007); *BNA* 2004, S. 433; *Funk/Zeifang/Johnson/Spessard*, CRi 2004, S. 142
[1208] *Manishin/Joyce*, The Computer & Internet Lawyer, Nr. 9, S. 2; *Zhang*, 20 Berkeley Tech. L. J. (2005), S. 318

für die Tat benutzt hat oder die für die Begehung solcher Taten bestimmt ist, 18 U.S.C. § 1037 (b), (c).

Nach Maßgabe des CAN-SPAM Act ist der Versand kommerzieller Emails nach erfolgtem Widerspruch (1.) unzulässig. Darüber verstoßen bestimmte weitere Verhaltensweisen im Zusammenhang mit dem Versenden einer Mehrzahl von kommerziellen Emails gegen den CAN-SPAM Act (2.).[1209]

1. Unzulässigkeit kommerzieller Emails nach erfolgtem Widerspruch

Der Versand einer kommerziellen Email ist dann unzulässig, wenn der Empfänger nach dem in 15 U.S.C. § 7704 (a) (3) (A) beschriebenen Mechanismus erklärt hat, keine solchen Emails erhalten zu wollen. Nach erklärtem Widerspruch darf demnach nicht mehr veranlasst werden, dass der Empfänger weiterhin kommerzielle Emails erhält, 15 U.S.C. § 7704 (a) (4) (A). Im US-amerikanischen Recht gilt somit das Opt-Out-Prinzip.[1210] Dies bedeutet, dass kommerzielle Emails grundsätzlich als zulässig angesehen werden, auch wenn der Empfänger nicht zuvor in deren Zusendung eingewilligt hat.[1211] Die Unzulässigkeit kommerzieller Emails ergibt sich nur, wenn der Empfänger nach dem in 15 U.S.C. § 7704 (a) (3) (A) beschriebenen Mechanismus erklärt, keine kommerziellen Emails mehr erhalten zu wollen. In diesem Fall ist es jedem, der Kenntnis vom Widerspruch des Empfängers hat oder dem Kenntnis billigerweise unterstellt werden kann, verboten, weitere kommerzielle Emails an den Betroffenen zu veranlassen, 15 U.S.C. § 7704 (a) (4) (A).[1212]
Veranlassen der Zustellung von Emails bedeutet nach 15 U.S.C. § 7702 (9), dass die Nachricht von dem fraglichen Versender stammt oder übertragen wird oder dass das Versenden oder die Übertragung der Nachricht durch eine andere Person herbeigeführt wird, die dafür eine Zahlung oder anderweitige Gegenleistung erhält.[1213] Ausgenommen sind lediglich so genannte Routine-Übermittlungen.[1214] Unter diesen Begriff fallen die Übermittlung, das Routing,[1215] die Weitergabe oder das Speichern einer Email durch automatisierte Vorgänge, für die eine andere Person den Empfänger oder die Empfängeradresse vorgegeben hat.

Das Veranlassen der Übermittlung der kommerziellen Email ist erst dann rechtswidrig, wenn seit der Erklärung des Empfängers zehn Werktage vergangen sind, 15 U.S.C. § 7704 (a) (4) (A) (i), (ii). Diese Zeitspanne kann durch die FTC geändert werden, 15 U.S.C. § 7704 (c) (1). Trotz eines erklärten Widerspruchs gilt das Verbot der Zustellung dann nicht, wenn der Empfänger danach seine Einwilligung erklärt hat, 15 U.S.C. § 7704 (a) (4) (B). Konsequenz

---

[1209] Darüber hinaus erklärt der CAN- SPAM Act bestimmte Umgangsformen mit Email- Adressen für unzulässig, 15 U.S.C. § 7704 (a) (4) (A) (iii, iv) und verbietet weitere Tätigkeiten, beispielsweise falsche Headerinformationen, Abschnitt 5 (a) (1), und Betreffangaben, Abschnitt 5 (a) (2). Folge der Verletzung der genannten Vorschriften ist die Möglichkeit einer zivilrechtlichen Klage nach Abschnitt 7 (f) (1). Schließlich sind bestimmte Handlungen strafrechtlich sanktioniert, so etwa das Verschleiern des Absenders, Abschnitt 4 (a) (2), die Fälschung von Headerinformationen in einer Mehrzahl von Emails, Abschnitt 4 (a) (3). Strafbar macht sich auch derjenige, der sich unter Verwendung falscher Informationen fünf oder mehr Email- oder User - Accounts oder zwei oder mehr Domainnamen besorgt und über diese Adressen oder Domains Emails verschickt, Abschnitt 4 (a) (5). Die vorgenannten Verbote betreffen jedoch nicht die Zulässigkeit des Versendens von kommerziellen Emails an sich, weshalb nicht näher darauf eingegangen werden soll.
[1210] *Kennedy/Lyon*, The Computer & Internet Lawyer 2005, Nr. 2, S. 1; *Manishin/Joyce*, The Computer & Internet Lawyer 2004, Nr. 9, S. 1
[1211] *Kennedy/Lyon*, The Computer & Internet Lawyer 2005, Nr. 2, S. 1
[1212] *Geary/Dave*, Computers & Law, März 2005, S. 20; *Wendlandt*, MMR 2004, S. 367
[1213] Der CAN- SPAM Act verwendet den Terminus "initiate".
[1214] Der CAN- SPAM Act verwendet den Terminus "routine conveyance".
[1215] zum Begriff: 1. Kap. Teil 1 A. I. 3.

eines Verstoßes gegen die soeben genannten Vorgaben des CAN-SPAM Act ist die Möglichkeit der Erhebung einer Klage auf dem Zivilrechtsweg durch die oben genannten klageberechtigten Rechtsträger,[1216] 15 U.S.C. § 7706 (f) (1).

Die Möglichkeit des Empfängers, den Widerspruch zu erklären, wird dadurch sichergestellt, dass es nach Maßgabe des CAN-SPAM Act einerseits verboten ist, die Zusendung einer kommerziellen Email zu veranlassen, wenn diese nicht klar und deutlich auf die Widerspruchsmöglichkeit nach (3) hinweist, 15 U.S.C. § 7704 (a) (5) (A) (ii). Des Weiteren dürfen kommerzielle Emails nicht versandt werden, wenn diese keine funktionierende Rückantwortadresse oder einen anderen internetbasierten Mechanismus besitzen, der klar und deutlich sichtbar ist und den der Empfänger dazu benutzen kann, den Widerspruch im Hinblick auf weitere kommerzielle Emails zu erklären, 15 U.S.C. § 7704 (a) (3) (A). Folge einer Verletzung der vorgenannten Vorschriften ist die Möglichkeit einer zivilrechtlichen Klage nach 15 U.S.C. § 7706 (f) (1).

2. Unzulässigkeit bestimmter Verhaltensweisen bei Versand einer Mehrzahl kommerzieller Emails

Des Weiteren sind bestimmte Verhaltensweisen unzulässig, sofern sie im Zusammenhang mit dem Versenden einer Mehrzahl kommerzieller Emails stehen, vgl. 18 U.S.C. § 1037 (a) (1)-(5).[1217] Ein Verstoß gegen die Vorschrift des 18 U.S.C. § 1037 (a) (1)-(5) ist strafrechtlich sanktioniert.[1218] Allerdings ist Anknüpfungspunkt der Norm nicht die Tatsache, dass kommerzielle Emails versandt werden, sondern dass hierbei betrügerische oder täuschende Verhaltensweisen an den Tag gelegt werden. Die Frage, ob das Versenden kommerzieller Emails per se als zulässig anzusehen ist, wird von der Vorschrift also nicht geregelt, weshalb hier keine weiteren Ausführungen gemacht werden.

II. Einzelstaatliches Recht

Es stellt sich die Frage, ob sich aus einzelstaatlichem Recht etwas anderes ergeben kann, als dies nach Maßgabe des CAN-SPAM Act der Fall ist.[1219] Der CAN-SPAM Act verfolgt das Ziel der einheitlichen Rechtsanwendung im gesamten Gebiet der USA, weshalb er nach Maßgabe des 15 U.S.C. § 7707 (b) (1) jeden ausdrücklich den Gebrauch elektronischer Post zur Versendung kommerzieller Nachrichten betreffenden Rechtsakt eines Bundesstaats oder einer bundesstaatlichen Behörde verdrängt.[1220] Der Vorrang gilt allerdings nicht, soweit das bundesstaatliche Gesetz falsche oder irreführende Angaben in einer kommerziellen Email reguliert, vgl. 15 U.S.C. § 7707 (b) (1) oder sich nicht spezifisch auf elektronische Nachrichten bezieht, so etwa Gesetze über Computerstraftaten und Betrug sowie das Vertrags- und Deliktsrecht, vgl. 15 U.S.C. § 7707 (b) (2) (A), (B).[1221]

[1216] vgl.: 3. Kap. Teil 1 A. I.

[1217] Eine Mehrzahl von Nachrichten im vorgenannten Sinne ist gegeben, wenn mehr als 100 Emails im Zeitraum von 24 Stunden, mehr als 1.000 Emails in einem Zeitraum von 30 Tagen oder mehr als 10.000 Emails in einem Zeitraum von einem Jahr versandt werden, 18 U.S.C. § 1037 (d) (3).

[1218] zum Strafmaß und der möglichen Einziehung bestimmter Gegenstände: 3. Kap. Teil 1 A. I.

[1219] vgl. etwa auf bundesstaatlicher Ebene: California Business and Professions Code, § 17529; Nevada Revised Statutes, §§ 41.705-41.735; Revised Code of Washington, §§ 19.190.10 - 19.190.070, alle abrufbar unter: http://www.spamlaws.com (letzter Abruf: 29.04.2007)

[1220] *BNA* 2005, S. 735; *Fritzemeyer*, K & R 2005, S. 55; *Hopper*, 59 SMU L.Rev., S. 389; *Manishin/Joyce*, The Computer & Internet Lawyer 2004, Nr. 9, S. 1; *Zhang*, 2005 Berkeley Tech. L. J., S. 320

[1221] *BNA* 2005, S. 735; *Fritzemeyer*, K & R 2005, S. 55; *Hopper*, 59 SMU Law Review, S. 389

Nicht verdrängt sind nach 15 U.S.C. § 7707 (b) (2) (A) deliktsrechtlichen Vorschriften. Hier könnte in den Fällen, in denen massenhaft Emails an Kunden eines Providers übersandt werden, die deliktische Handlung des „trespass to chattels", das bedeutet Besitzstörung an beweglichen Sachen, verwirklicht sein. Voraussetzung des Delikts ist das vorsätzliche Entziehen der Sache oder der Nutzung der Sache, die im Besitz eines anderen steht, vgl. Restatement 2d of Torts § 217.[1222] Allerdings haftet derjenige, der die Handlung begangen hat nur dann, wenn er dem anderen den Besitz entzieht, wenn die Sache hinsichtlich ihres Zustandes, der Qualität oder des Wertes beeinträchtigt wird, dem Besitzer für eine nicht unbeträchtliche Zeit die Sache entzogen oder der Besitzer oder eine andere Person, an deren Schutz der Besitzer ein Interesse hat, körperlich verletzt wird, Restatement 2d of Torts § 218.[1223] Des Weiteren setzt das Delikt einen physischen Kontakt voraus, 2d Torts § 221.[1224] Die Frage, ob das Zusenden einer Email einen derartigen Kontakt darstellt, ist umstritten.[1225] Dafür wird die Rechtsprechung im Bereich des Hacking angeführt, die davon ausgeht, dass das Versenden von elektronischen Signalen den physischen Kontakt ersetzen kann, wenn der Gegenstand hierdurch beeinträchtigt wird.[1226] Eine Beeinträchtigung sei in der langsameren Funktion des Servers aufgrund der massenweise versandten Emails zu sehen.[1227] Das Vorliegen einer physischen Berührung ist dabei allerdings fraglich, denn das Eingehen von Emails auf einem dafür vorgesehenen Server bewirkt eine solche grundsätzlich nicht.[1228] Es ist auch fernliegend in dem Empfang einer Email eine Beeinträchtigung des Servers zu sehen, wenn der Inhalt unerwünscht ist.[1229] Ansonsten wäre auch ein Radio- oder Fernsehgerät beeinträchtigt, wenn dort unerwünschte Programme gesendet werden.[1230] Bereits deshalb scheidet das Delikt „trespass to chattels" aus. Darüber hinaus wird es schwierig sein, einen

---

[1222] Restatement 2d of Torts § 217 lautet*:„A trespass to a chattel may be committed by intentionally*
(a) dispossessing another of the chattel, or
(b) using or intermeddling with a chattel in the possession of another."; vgl. auch: Koepnick v. Sears Roebuck & Company, 158 Ariz. 322, 762 P.2d, S. 609, Court of Appeals of Arizona, Division 1, Department D, (1988)

[1223] Restatement 2d of Torts § 218 lautet: *„One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if*
(a) he dispossesses the other of the chattel, or
(b) the chattel is impaired as to its condition, quality or value, or
(c) the possessor is deprived of the use of the chattel for a substantial time, or
(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest."; vgl. auch: Koepnick v. Sears Roebuck & Company, 158 Ariz. 322, 762 P.2d, S. 609, Court of Appeals of Arizona, Division 1, Department D, (1988)

[1224] Restatement 2d Torts § 221 lautet: *„A dispossession may be committed by intentionally*
(a) taking a chattel from the possession of another without the other´s consent, or
(b) obtaining possession of a chattel from another by fraud or duress, or
(c) barring the possessor´s access to a chattel, or
(d) destroying a chattel while it is in another´s possession, or
(e) taking the chattel into the custody of the law."

[1225] dafür: CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp., S. 1021, United States District Court, S.D. Ohio, (1997); dagegen: Intel Corporation v. Hamidi, 30 Cal.4th, S. 1359, Supreme Court of California, (2003); Quilter, 17 Berkeley Tech. L. J., 421; *Burk*, 4 J. Small & Emerging Bus. L., S. 27 ff.

[1226] State of Indiana v. McGraw, 480 N.E.2d, S. 554, Supreme Court of Indiana, (1985); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp., S. 1021, United States District Court, S. D. Ohio, (1997) unter Bezugnahme auf Thrifty-Tel., Inc v. Bezenek, 46 Cal.App.4th, S. 1567, Court of Appeal, Fourth District, Division 3, California, (1996)

[1227] America Online, Inc. v. IMS et al., 24 F.Supp.2d, S. 550, United States District Court, E.D. Virginia, (1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp., S. 1021,United States District Court, S. D. Ohio, (1997)

[1228] Intel Corporation v. Hamidi, 30 Cal.4th, S. 1359, Supreme Court of California, (2003); *Burk*, 4 J. Small & Emerging Bus. L., S. 27 ff.; *Quilter*, 17 Berkeley Tech. L. J., S. 421 ff.

[1229] Intel Corporation v. Hamidi, 30 Cal.4th, S. 1359, Supreme Court of California, (2003); *Burk*, 4 J. Small & Emerging Bus. L., 36 f.

[1230] Intel Corporation v. Hamidi, 30 Cal.4th, S. 1359, Supreme Court of California, (2003); *Burk*, 4 J. Small & Emerging Bus. L., 37

konkreten Schaden nachzuweisen, denn die Verzögerung durch die übersandten Nachrichten wird in der Regel nicht meßbar sein. Demnach ist davon auszugehen, dass der Tatbestand des trespass to chattels hier nicht gegeben ist.[1231]

III. Ergebnis

Das Versenden kommerzieller Emails ist nach US-amerikanischem Recht grundsätzlich zulässig. Es dürfen an einen bestimmten Empfänger erst dann keine solchen Nachrichten mehr versandt werden, wenn dieser seinen Widerspruch erklärt hat und die durch den Gesetzgeber eingeräumte Frist abgelaufen ist. Unzulässig sind daneben solche kommerziellen Nachrichten, die keine hinreichende Widerspruchsbelehrung oder funktionierende Rückantwortadresse enthalten. Nachrichten, die nicht unter den Begriff der kommerziellen Email im Sinne des CAN-SPAM Act fallen, sind bereits seinem Anwendungsbereich entzogen und brauchen die Vorgaben des Gesetzes folglich auch nicht zu erfüllen.

B. Verfassungs- und Völkerrecht

Fraglich ist, ob die genannten Vorschriften des einfachen US-amerikanischen Rechts verfassungs- (I.) und völkerrechtlichen Vorgaben (II.) genügen. Wäre dies nicht der Fall, so würde sich möglicherweise die Unwirksamkeit der einfachrechtlichen Vorschriften oder ein Verpflichtung des Gesetzgebers zum Tätigwerden ergeben.

I. Verfassungsrecht

Der CAN-SPAM Act könnte aufgrund eines Verstoßes gegen die US-Verfassung ungültig sein.[1232] Dies wäre der Fall, wenn das Gesetz in rechtswidriger Weise in das im ersten Verfassungszusatz festgeschriebene Recht auf freie Meinungsäußerung eingreifen würde.[1233] Die Frage wurde bisher nicht gerichtlich entschieden. Der CAN-SPAM Act wurde lediglich insofern auf seine Verfassungsmäßigkeit überprüft, als er die Versender von kommerziellen Emails dazu verpflichtet, bestimmte Informationen zu erteilen, wie dies in 18 U.S.C. § 7704 (a) (1)-(4) der Fall ist;[1234] hierin wurde keine Verletzung des Grundrechts gesehen.[1235] Die Frage, ob die Opt-Out-Lösung verfassungswidrig ist, wird damit allerdings nicht beantwortet.

Das Grundrecht auf Meinungsfreiheit beinhaltet die kommerzielle Rede,[1236] wenngleich die Schutzintensität in diesem Bereich geringer ist, als bei nicht-kommerziellen

---

[1231] Intel Corporation v. Hamidi, 30 Cal.4th, 1359, Supreme Court of California, (2003); *Burk*, 4 J. Small & Emerging Bus. L., S. 27 ff.; *Quilter*, 17 Berkeley Tech. L. J., S. 421 ff.; aA.: CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp., S. 1021,United States District Court, S. D. Ohio, (1997); America Online, Inc. v. IMS et al., 24 F.Supp.2d, S. 550, United States District Court, E.D. Virginia, (1998)

[1232] zur Ungültigkeit von Rechtsvorschriften bei einem Verfassungsverstoß: R.A.V. v. City of St. Paul, Minnesota, 505 U.S., S. 377, 112 S. Ct., S. 2538, Supreme Court of the United States, (1992); vgl. auch: Ashcroft v. American Civil Liberties Union, 542 U.S., S. 656, 124 S. Ct., S. 2783, Supreme Court of the United States, (2004)

[1233] der erste Verfassungszusatz lautet: *„Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or of the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."*

[1234] vgl. zum Gesetzestext: Anhang I

[1235] Federal Trade Commission v. Phoenix Avatar, LLC d/b/a Avatar Nutrition, Not Reported in F.Supp.2d, 2004 WL 1746698, United States District Court for the Northern District of Illinois, Eastern Division, (2004)

[1236] Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 48 L Ed. 2d, S. 358 ff., Supreme Court of the United States, (1976); Friedman v. Rogers, 440 U.S., S. 1, 99 S. Ct., S. 887, Supreme Court of the United States, (1979); Central Hudson Gas & Electric Corporation v. Public Service Commission of

Meinungsäußerungen.[1237] Kommerzielle Rede liegt vor, wenn die Äußerung auf eine kommerzielle Transaktion ausgerichtet ist.[1238] Der verfassungsrechtliche Schutz der kommerziellen Rede entfällt allerdings im Hinblick auf unrichtige Informationen sowie Werbung für unrechtmäßige Aktivitäten.[1239] Email-Werbung fällt somit als kommerzielle Rede in den Schutzbereich der Meinungsäußerungsfreiheit, sofern sie nicht unwahr ist oder unerlaubte Tätigkeiten betrifft.

Beschränkungen der Meinungsfreiheit in Gestalt der kommerziellen Rede sind zulässig, wenn hieran ein wesentliches staatliches Interesse besteht (1.),[1240] wenn die Regelung das Interesse fördert (2.)[1241] und sie nicht weitergehender ist, als dies die Zweckerreichung erfordert (3.).[1242]

1. Wesentliches staatliches Interesse

Zunächst stellt sich hier die Frage, ob ein wesentliches staatliches Interesse daran besteht, die Zulässigkeit des Versands kommerzieller Emails zu beschränken.[1243] Dabei verfolgt die Beschränkung der Email-Direktwerbung zwei Ziele und zwar einerseits den Schutz der

---

New York, 65 L. Ed. 2d, S. 348 f., Supreme Court of the United States, (1980); Florida Bar v. Went for It, Inc., 515 U.S., S. 618, 115, S. Ct., S. 2371, Supreme Court of the United States, (1995)

[1237] Ohralik v. Ohio State Bar Association, 436 U.S., S. 447, 98 S. Ct., S. 1912, Supreme Court of the United States, (1978); Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, 65 L. Ed. 2d, 348 f., Supreme Court of the United States (1980); In re Doser v. United States Trustee, 412 F.3d, S. 1056, United States Court of Appeals, Ninth Circuit, (2005)

[1238] Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc. 425 U.S., S. 762, 96 S. Ct., S. 1826, Supreme Court of the United States, (1976); U.S. West, Inc. v. F. C. C., 182 F.3d, S. 1232 f., United States Court of Appeals, Tenth Circuit, (1999)

[1239] Friedman v. Rogers, 440 U.S., S. 1, 99 S. Ct., S. 887, Supreme Court of the United States, (1979); Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, 65 L. Ed. 2d, S. 341 ff., Supreme Court of the United States (1980); im Bereich der nicht-kommerziellen Rede: Pittsburgh Press v. Pittsburgh Commission on Human Relations et al., 413 U.S., S. 376, 93 S. Ct., S. 2553, Supreme Court of the United States, (1973); Gertz v. Robert Welch, Inc. 418 U.S., S. 323, 94 S. Ct., S. 2997, Supreme Court of the United States, (1974); Ohralik v. Ohio State Bar Association, 436 U.S., S. 447, 98 S. Ct., S. 1925, Supreme Court of the United States, (1978)

[1240] „(substantial) governmental interest", vgl.: Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, 65 L. Ed. 2d, S. 348 f., Supreme Court of the United States (1980); vgl. auch: Edenfield v. Fane, 507 U.S., S. 761, 113 S. Ct., S. 1799, Supreme Court of the United States, (1993); U.S. Florida Bar v. Went for It, Inc., 515 U.S., S. 618, 115 S. Ct., S. 2382, U.S. Supreme Court, (1995); Florida State v. Bradford, 787 So. 2d, S. 821, Supreme Court of Florida, (2000);
Video Gaming Consultants, Inc. v. South Carolina Department of Revenue, 342 S.C., 34, 535 S.E. 2d, 642, Supreme Court of South Carolina, (2000)

[1241] Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, 65 L. Ed. 2d, S. 341 ff., U. S. Supreme Court (1980)

[1242] die Beschränkung muss „narrowly tailored/drawn" sein bzw. muss ein „fit between the restriction and the government interest" bestehen, vgl.: Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, 65 L. Ed. 2d, S. 341, Supreme Court of the United States, (1980); vgl. auch: Frisby v. Schultz, 487 U.S., S. 474, 108 S. Ct., S. 2495, Supreme Court of the United States, (1988); Valley Broadcasting v. U.S., 107 F.3d, S. 1328, United States Court of Appeals, Ninth Circuit, (1997); Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004); Fraternal Order of Police v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005)

[1243] Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, 65 L. Ed. 2d, S. 348, U. S. Supreme Court (1980); vgl. auch: Edenfield v. Fane, 507 U.S., S. 761, 113 S. Ct., S. 1799, Supreme Court of the United States, (1993); U.S. Florida Bar v. Went for It, Inc., 515 U.S., S. 618, 115 S. Ct., S. 2382, Supreme Court of the United States, (1995); Florida State v. Bradford, 787 So. 2d, S. 821, Supreme Court of Florida, (2000); Video Gaming Consultants, Inc. v. South Carolina Department of Revenue, 342 S.C., S. 34, 535 S.E. 2d, S. 642, Supreme Court of South Carolina, (2000)

Privatsphäre der Adressaten, andererseits das Verhindern betrügerischer sowie ehrverletzender Werbung.[1244]

Die Privatsphäre soll nach der Rechtsprechung ein Abwehrrecht gegen unerwünschte Meinungsäußerungen Dritter geben.[1245] In den USA werden der Privatsphäre verschiedene Gewährleistungsgehalte zugewiesen.[1246] Einerseits kommt ihr der Aspekt der informationellen Selbstbestimmung zu, das bedeutet, das Recht dem Mißbrauch und der Verbreitung von Informationen zu widersprechen.[1247] Andererseits folgt aus dem Schutz der Privatsphäre das Recht des Betroffenen, in Ruhe gelassen zu werden[1248] und unerwünschte Kommunikation nicht wahrzunehmen.[1249] Dieses Recht besteht innerhalb der Wohnung sowie außerhalb in Situationen, in denen der Betroffenen der unerwünschten Situation nicht entkommen kann.[1250] Es erfasst auch Meinungsäußerungen vor der Wohnung mit Zielrichtung auf die Bewohner.[1251] Das Recht auf Privatsphäre kann Beschränkungen der kommerziellen Rede rechtfertigen.[1252]

[1244] Senate Report No. 108-102, 2004 U.S.C.C.A.N., S. 2348; vgl. auch für das Telefonmarketing: Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004)

[1245] Rowan v. United States Post Office Department, 397 U.S., S. 728, 90 S. Ct., S. 1484, Supreme Court of the United States, (1970); Frisby v. Schultz, 487 U.S., S. 474, 108 S. Ct., S. 2495, Supreme Court of the United States, (1988); U.S. West, Inc. v. F.C.C., 182 F.3d, S. 1234, United States Court of Appeals, Tenth Circuit, (1999)

[1246] U.S. West, Inc. v. F.C.C., 182 F.3d, S. 1234, United States Court of Appeals, Tenth Circuit, (1999); *Rosenbaum*, 38 Jurimetrics J. (1998), S. 566

[1247] U.S. West, Inc. v. F.C.C., 182 F.3d, S. 1234, United States Court of Appeals, Tenth Circuit, (1999); *Rosenbaum*, 38 Jurimetrics J. (1998), 566

[1248] Ohralik v. Ohio State Bar Association, 436 U.S., S. 447, 98 S. Ct., S. 1925, Supreme Court of the United States, (1978); Frisby v. Schultz, 487 U.S., S. 474, 108 S. Ct., S. 2495, Supreme Court of the United States, (1988); Edenfield v. Fane, 507 U.S., S. 761, 113 S. Ct., S. 1792, Supreme Court of the United States (1993); Van Bergen v. State of Minnesota, 59 F. 3d, S. 1541, United States Court of Appeals, Eighth Circuit, (1995); Fraternal Order of Police, North Dakota State Lodge, Veterans of Foreign Wars v. Stenehjem, 431 F. 3d 591, United States Court of Appeals, Eigth Circuit, (2005); White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, 366, United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006); U.S. West, Inc. v. F.C.C., 182 F.3d, S. 1234, United States Court of Appeals, Tenth Circuit, (1999); *Rosenbaum*, 38 Jurimetrics J. (1998), S. 566

[1249] Rowan v. U.S. Post Office Department, 397 U.S., S. 728, 90 S. Ct., S. 1484, Supreme Court of the United States, (1970); Cohen v. California, 403 U.S., S. 15, 91 S. Ct., S. 1780, Supreme Court of the United States, (1971); Ward v. Rock against Racism, 491 U.S., S. 781, 109 S. Ct., S. 2746, Supreme Court of the United States, (1989); Hill v. Colorado, 530 U.S., S. 703, 120 S. Ct., S. 2480, Supreme Court of the United States, (2000); Van Bergen v. State of Minnesota, 59 F. 3d, S. 1541, United States Court of Appeals, Eighth Circuit, (1995); U.S. West, Inc. v. F.C.C., 182 F.3d, S. 1234, United States Court of Appeals, Tenth Circuit, (1999); *Rosenbaum*, 38 Jurimetrics J. (1998), S. 566

[1250] Rowan v. U.S. Post Office Department, 397 U.S., S. 728, 90 S. Ct., S. 1484, Supreme Court of the United States,(1970); Cohen v. California, 403 U.S., S. 15, 91 S. Ct., S. 1780, Supreme Court of the United States, (1971); Ward v. Rock against Racism, 491 U.S., S. 781, 109 S. Ct., S. 2746, Supreme Court of the United States, (1989); Hill v. Colorado, 530 U.S., S. 703, 120 S. Ct., S. 2480, Supreme Court of the United States, (2000); Van Bergen v. State of Minnesota, 59 F. 3d, S. 1541, United States Court of Appeals, Eighth Circuit, (1995)

[1251] Frisby v. Schultz, 487 U.S., S. 474, 108 S. Ct., S. 2495, Supreme Court of the United States, (1988)

[1252] Ohralik v. Ohio State Bar Association, 436 U.S., S. 447, 98 S. Ct., S. 1925, Supreme Court of the United States, (1978); Frisby v. Schultz, 487 U.S., S. 474, 108 S. Ct., S. 2495, Supreme Court of the United States, (1988); Edenfield v. Fane, 507 U.S., S. 761, 113 S. Ct., S. 1792, Supreme Court of the United States (1993); Van Bergen v. State of Minnesota, 59 F. 3d, S. 1541, United States Court of Appeals, Eighth Circuit, (1995); Fraternal Order of Police v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005); vgl. auch: White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, S. 366, United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006)

Fraglich ist, ob das Recht auf Privatsphäre durch das Zusenden unverlangter Email-Werbung beeinträchtigt wird. Zahlenmäßig überhand nehmende Werbeanrufe, die in einer wiederkehrenden Belästigung des Angerufenen resultierten, sah die Rechtsprechung als Beeinträchtigung der Privatsphäre an.[1253] Zwar kommt der Email-Werbung, wie im Bereich des deutschen Rechts erläutert,[1254] insofern kein genauso störender Effekt zu, wie der Telefonwerbung, da der Betroffenen selbst entscheiden kann, wann er die Email liest und er nicht mit der direkten Ansprache konfrontiert ist. Allerdings stellen auch kommerzielle Emails aufgrund ihrer steigenden Anzahl eine Belastung für den Empfänger dar, die nicht nur in der Verlagerung der Kosten besteht, sondern auch in dem Zwang die Email -sofern sie nicht gekennzeichnet ist- erst einmal zu öffnen und Zeit für das Aussortieren und Löschen aufzuwenden.[1255] Insofern ist von einer Beeinträchtigung des Rechts auf Privatsphäre durch das Zusenden kommerzieller Emails auszugehen.
Fraglich ist, ob etwas anderes deshalb gilt, da Emails auch wenn sie an einen privaten Account verschickt wurden, nicht notwendigerweise von der eigenen Wohnung aus abgerufen werden müssen. Insofern könnte ein Eingriff in die Privatsphäre zu verneinen sein. Allerdings ist der Schutz der Privatsphäre innerhalb der eigenen vier Wände lediglich stärker ausgeprägt; er existiert jedoch -wie dargestellt wurde- auch dort, wo der Kommunikationsempfänger nicht die Möglichkeit hat, der Kommunikation auszuweichen.[1256] Gerade dies ist der Fall, wenn dem Adressaten unerwünschte kommerzielle Emails zugesandt werden, da diese in aller Regel geöffnet werden müssen, um sicherstellen zu können, dass keine legitime Post betroffen ist. Etwas anderes gilt möglicherweise dann, wenn kommerzielle Emails eindeutig als solche gekennzeichnet werden. Allerdings muss auch in diesem Fall der Betroffenen Zeit zum Abrufen und Löschen der Emails aufwenden, so dass der Belästigungseffekt insofern nicht entfällt.[1257] Demnach kann als rechtfertigendes Interesse für die durch den CAN-SPAM Act bewirkte Beschränkung des Rechts auf kommerzielle Rede darauf abgestellt werden, dass dieser das Recht der Adressaten kommerzieller Emails auf Privatsphäre zu schützen sucht.[1258] Daneben kann sich der Gesetzgeber darauf berufen, dass ein wesentliches staatliches Interesse daran besteht, betrügerische Verkaufspraktiken zu unterbinden[1259] sowie vor dem Abwälzen der Kosten auf den Empfänger zu schützen.[1260]

[1253] Fraternal Order of Police v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005); National Federation of the Blind v. Federal Trade Commission, 420 F.3d, S. 331, United States Court of Appeals, Fourth Circuit, (2005); zu automatisierten Telefonanrufen zum Zweck der politischen Werbung: Van Bergen v. State of Minnesota, 59 F.3d, S. 1541, United States Court of Appeal, Eighth Circuit, (1995)
[1254] vgl.: 2. Kap. Teil 1 A. III. 1. a) aa)
[1255] vgl.: 2. Kap. Teil 1 A. III. 1. a) aa)
[1256] Rowan v. U.S. Post Office Department, 397 U.S., S. 728, 90 S. Ct., S. 1484, Supreme Court of the United States, (1970); Cohen v. California, 403 U.S., S. 15, 91 S. Ct., S. 1780, Supreme Court of the United States, (1971); Ward v. Rock against Racism, 491 U.S., S. 781, 109 S. Ct., S. 2746, Supreme Court of the United States, (1989); Hill v. Colorado, 530 U.S., S. 703, 120 S. Ct., S. 2480, Supreme Court of the United States, (2000); Van Bergen v. State of Minnesota, 59 F. 3d, S. 1541, United States Court of Appeals, Eighth Circuit, (1995)
[1257] vgl. zum Zeit- und Kostenaufwand: 2. Kap. Teil 1 A. III. 1. a) aa) sowie 1. Kap. Teil 1 B. II. 4.
[1258] Senate Report No. 108-102, 2004 U.S.C.C.A.N., S. 2348; a.A.: U.S. West, Inc. v. Federal Communications Commission, 182 F.3d, S. 1224, United States Court of Appeals, Tenth Circuit, (1999)
[1259] Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 48 L Ed. 2d, S. 358 ff., Supreme Court of the United States, (1976); Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, 65 L. Ed. 2d, S. 348 f., U. S. Supreme Court (1980); Edenfield v. Fane, 507 U.S., S. 761, 113 S. Ct., S. 1792, Supreme Court of the United States, (1992); In re R.M.J., 455 U.S., S. 191, Supreme Court of the United States, (1982); Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004)
[1260] Kaufman v. ACS Systems, Inc., 110 Cal.App. 4th, S. 886, 2 Cal. Rptr.3d, S. 296, Court of Appeal, Second District, Division 1, California, (2003)

2. Förderung des staatlichen Interesses durch die Beschränkung der kommerziellen Rede

Fraglich ist, ob die Beschränkung der kommerziellen Rede durch den CAN-SPAM Act das staatliche Interesse fördert.
Der CAN-SPAM Act verbietet bestimmte Vorgehensweisen bei der Email-Direktwerbung, wie das Versenden nach erklärtem Widerspruch, das Fälschen bestimmter Informationen sowie bestimmte betrügerische Verhaltensweisen.[1261] Somit wird das Gesetz zumindest rechtstreue Unternehmen davon abhalten, weiterhin in unzulässiger Art und Weise zu werben sowie Informationen zu fälschen oder betrügerische Verhaltensweisen an den Tag zu legen; insofern ist davon auszugehen, dass der CAN-SPAM Act die verfolgten staatlichen Ziele fördert.[1262] Dem steht auch nicht entgegen, dass sich durch den CAN-SPAM Act das Spam-Volumen nicht merklich verringerte, weil eine Vielzahl von Spam auch aus dem Ausland kommen.[1263] So entschied das US-Supreme Court, dass einem Verbot der Radiowerbung für Lotteriespiele eines US-Bundesstaates nicht deshalb die Eignung für die Zweckerreichung abgesprochen werden kann, weil die Bewohner dennoch Werbung aus einem anderen Bundesstaat empfangen.[1264] Auf internationaler Ebene kann nichts anderes gelten. Dies wäre auch wenig sinnvoll, da dem Gesetzgeber so stets die Hände gebunden wären, wenn auf nationaler Ebene ein nur geringer Erfolg zu erwarten ist, weil ein Problem, wie Spam, mittlerweile internationale Ausmaße angenommen hat. Folglich ist davon auszugehen, dass der CAN-SPAM Act die Ziele des Schutzes der Privatsphäre und vor bestimmten betrügerischen Verhaltensweisen fördert.[1265]

3. Zweck-Mittel-Relation

Schließlich stellt sich die Frage nach der Angemessenheit der Zweck-Mittel-Relation. Staatliche Einschränkungen müssen, anders als im Bereich der nicht-kommerziellen Rede, nicht das am wenigsten eingreifende Mittel zum Erreichen des verfolgten Zwecks sein.[1266] Erforderlich ist lediglich ein angemessenes Verhältnis zwischen dem vom Staat mit der Beschränkung verfolgten Ziel und dem eingesetzen Mittel.[1267] Die Einschränkung der

---

[1261] vgl.: 3. Kap. Teil 1 A. I. 2.
[1262] ähnlich für den Bereich der Telefonwerbung: Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004)
[1263] *Alongi,* 46 Ariz. L. Rev., S. 288; *Zhang*, 20 Berk. Tech. L. J., S. 324; *Fritzemeyer,* K & R 2005, S. 58
[1264] Federal Communications Commission v. Edge Broadcasting Company, 509 U.S., S. 418, Supreme Court of the United States, (1993)
[1265] ähnlich für den Bereich der Telefonwerbung Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004); a.A.: U.S. West, Inc. v. Federal Communications Commission, 182 F.3d, S. 1224 ff., United States Court of Appeals, Tenth Circuit, (1999)
[1266] Board of Trustees of State University of New York v. Todd Fox et al., 492 U.S., 469, S. Ct., 3028, Supreme Court of the United States, (1989); Greater New Orleans Broadcasting Association v. United States et al., 527 U.S., S. 173, 119 S. Ct., S. 1923, Supreme Court of the United States, (1999); Hill v. Colorado et al., 530 U.S., S. 703, 120 S. Ct., S. 2480, Supreme Court of the United States, (2000); Desdick v. Department of Professional Regulation, 171 Ill.2d, S. 510, Supreme Court of Illinois, (1996); Hamilton Amusement Center v. Verniero, 156 N.J., S. 254, 716 A.2d, S. 1137, Supreme Court of New Jersey, (1998); Kitsap County v. Mattress Outlet/Kevin Gould, 153 Wash.2d, 506, 104 P.3d, S. 1280, Supreme Court of Washington, (2005); Fraternal Order of Police, North Dakota State Lodge, Veterans of Foreign Wars v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005)
[1267] Board of Trustees of State University of New York v. Todd Fox et al., 492 U.S., S. 469, Supreme Court of the United States, (1989); City of Cincinnati v. Discovery Network, Inc., 507 U.S., S. 410, 113 S.Ct., S. 1505, Supreme Court of the United States, (1993); Minnesota League of Credit Unions v. Minnesota Deparment of Commerce, 486 N.W.2d, S. 399, Supreme Court of Minnesota, (1992); Desdick v. Department of Professional Regulation, 171 Ill.2d, S. 510, Supreme Court of Illinois, (1996); Gerawan Farming, Inc. v. Kawamura, 33 Cal.

Meinungsfreiheit muss in einem angemessenen Verhältnis zum geschützten Interesse stehen.[1268] Um festzustellen, ob eine Beschränkung weitgehender ist, als notwendig, ist darauf abzustellen, ob zahlreiche und ersichtlich die kommerzielle Rede weniger belastende Alternativen bestehen.[1269]

Hier ist daher das Recht betroffener Empfänger auf Privatsphäre zum Eingriff in das Recht auf kommerzielle Rede ins Verhältnis zu setzen.
Gegen einen zu weitreichenden Eingriff spricht, dass lediglich gegenüber solchen Empfängern kommerzielle Emails unzulässig sind, die das Opt-Out erklärt haben, sowie Nachrichten verboten sind, die betrügerisch sind oder falsche Informationen enthalten.[1270] Folglich wird die kommerzielle Rede nicht sehr weitgehend eingeschränkt, vielmehr sind kommerzielle Emails gegenüber denjenigen Empfängern nach Maßgabe des CAN-SPAM Act weiterhin zulässig, die von der Möglichkeit des Opt-Out keinen Gebrauch gemacht haben.[1271] Der CAN-SPAM Act verbietet nicht per se die kommerzielle Rede, sondern bewirkt die Unzulässigkeit erst dann, wenn der Adressat geäußert hat, kommerzielle Emails nicht mehr erhalten zu wollen.[1272] Die Opt-Out-Lösung greift danach weniger tiefgehend in das Recht auf kommerzielle Rede ein, als dies im Fall der Opt-In-Lösung oder gar eines gänzlichen Verbots der Email-Werbung der Fall wäre. Demnach erscheint die Beschränkung der kommerziellen Rede in diesem Bereich nicht unverhältnismäßig weit.[1273] Ein im Vergleich

---

4th, S. 14, Supreme Court of California, (2004); Kitsap County v. Mattress Outlet/Kevin Gould, 153 Wash.2d, S. 506, 104 P.3d, S. 1280, Supreme Court of Washington, (2005); die Gerichte verwenden mehrheitlich den Begriff „fit" um die geringeren Anforderungen an die Verhältnismäßigkeit zu bezeichnen, die im Bereich der kommerziellen Rede gelten: Board of Trustees of State University of New York v. Todd Fox et al., 492 U.S., S. 469, Supreme Court of the United States, (1989); City of Cincinnati v. Discovery Network, Inc., 507 U.S., S. 410, 113 S.Ct., S. 1505, Supreme Court of the United States, (1993); Minnesota League of Credit Unions v. Minnesota Deparment of Commerce, 486 N.W.2d, S. 399, Supreme Court of Minnesota, (1992); Desdick v. Department of Professional Regulation, 171 Ill.2d, S. 510, Supreme Court of Illinois, (1996); Gerawan Farming, Inc. v. Kawamura, 33 Cal. 4th, S. 14, Supreme Court of California, (2004)

[1268] Greater New Orleans Broadcasting Association v. United States et al., 527 U.S., S. 173, 119 S. Ct., S. 1923, Supreme Court of the United States, (1999); Desdick v. Department of Professional Regulation, 171 Ill.2d, S. 510, Supreme Court of Illinois, (1996); Gerawan Farming, Inc. v. Kawamura, 33 Cal. 4th, S. 14, Supreme Court of California, (2004); Kitsap County v. Mattress Outlet/Kevin Gould, 153 Wash.2d, S. 506, 104 P.3d, S. 1280, Supreme Court of Washington, (2005)

[1269] City of Cincinnati v. Discovery Network, Inc., 507 U.S., S. 410, 113 S. Ct., S. 1505, Supreme Court of the United States, (1993); Florida Bar v. Went for It, Inc., 515 U.S., S. 618, 115 S. Ct., S. 2371, Supreme Court of the United States, (1995); State of Florida v. Charles Bradford, 787 So.2d, S. 811, Supreme Court of Florida, (2001); Fraternal Order of Police, North Dakota State Lodge, Veterans of Foreign Wars v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005); Kitsap County v. Mattress Outlet/Kevin Gould, 153 Wash.2d, S. 506, 104 P.3d, S. 1280, Supreme Court of Washington, (2005)

[1270] Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004); Fraternal Order of Police, North Dakota State Lodge, Veterans of Foreign Wars v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005); gegen ein Recht, Dritten seine Meinung bzw. Äußerungen aufdrängen zu dürfen: Rowan v. United States Post Office Department et al., 397 U.S., S. 728, 90 S. Ct., S. 1484, Supreme Court of the United States (1970); Frisby v. Schultz, 487 U.S., S. 474, 108 S. Ct., S. 2495, United States Supreme Court, (1988); Dan Leroy Hall v. Commonwealth of Virginia, 188 Va., S. 72, Supreme Court of Appeals of Virginia, (1948) die Berufung wurde zurückgewiesen, Dan Leroy Hall v. Commonwealth of Virginia, 335 U.S., S. 875, Supreme Court of the United States, (1948); vgl. auch: White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, S. 366, United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006)

[1271] ähnlich für das Telefonmarketing: Fraternal Order of Police, North Dakota State Lodge, Veterans of Foreign Wars v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005)

[1272] ähnlich für das Telefonmarketing: Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004)

[1273] ähnlich für das Telefonmarketing: Fraternal Order of Police, North Dakota State Lodge, Veterans of Foreign Wars v. Stenehjem, 431 F. 3d, S. 591, United States Court of Appeals, Eigth Circuit, (2005); vgl. auch: Frisby v. Schultz, 487 U.S., S. 474, 108 S. Ct., S. 2495, United States Supreme Court, (1988)

zur Opt-Out-Lösung milderes Mittel kann auch nicht darin gesehen werden, es dem Adressaten zu überlassen, sich selbst durch Einsatz technischer Mittel gegen die Zustellung kommerzieller Emails zu wehren. Denn in diesem Fall würden einerseits einseitig die Kosten auf den Empfänger verlagert, andererseits ist ein Schutz mittels Einsatz technischer Mittel auch deshalb nicht zu gewährleisten, weil bisher keine fehlerfrei funktionierenden Filter existieren.[1274]

Anders entschied das US-Supreme Court allerdings im Hinblick auf Vorschriften, die das Einstellen jugendgefährdender Inhalte in das Internet betrafen, vgl. 47 U.S.C. § 231 sowie die Vorgängervorschrift 47 U.S.C. § 223.[1275] Hier sollten privat veranlasste Filtermaßnahmen ein im Vergleich zum Verbot der Verbreitung jugendgefährdender Inhalte milderes Mittel darstellen, weshalb eine Rechtfertigung der Beschränkung verneint wurde.[1276] Der Grund für die Entscheidungen des Supreme Court lag allerdings darin, dass der Staat nicht dargelegt und bewiesen hatte, dass Filter, die jugendgefährdende Materialien ausfiltern sollen, weniger effektiv sind, als ein Verbot, solche Materialien in das Internet einzustellen.[1277] Ein solcher Beweis kann allerdings im Bereich Spam angesichts der stets vorhandenen Quote von false positives und false negatives erbracht werden.[1278] Darüber hinaus ist die durch die Opt-Out-Lösung bewirkte Beschränkung der Meinungsäußerung wesentlich weniger weitgehend, als das vollständige Verbot des Einstellens bestimmter Inhalte in das Internet in den Fällen Ashcroft und Reno.[1279] Im Ergebnis ist deshalb davon auszugehen, dass in dem Verweis der Betroffenen darauf, technische Filter einzusetzen, kein milderes Mittel zu sehen ist.

Schließlich ist auch der Grad der Belästigung zu berücksichtigen, der mittlerweile durch Email-Werbung verursacht wird.[1280] Hinzu kommt, dass der kommerziellen Rede ausweislich der oben genannten Rechtsprechung eine geringere Schutzintensität zukommt, als der nicht-kommerziellen Rede.[1281] Insofern muss es dem Gesetzgeber möglich sein, eine Regelung zu treffen, die dieses Recht beschränkt, um die Privatsphäre der Empfänger kommerzieller Emails zu schützen.

Von der Angemessenheit der Beschränkung ist nach Auswertung der bisher ergangenen Rechtsprechung somit auszugehen.[1282] Ein Verstoß gegen die Verfassung liegt nach der hier vertretenen Auffassung folglich nicht vor.

[1274] ähnlich für das Telefonmarketing: Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F. 3d, S. 1228, United States Court of Appeals, Tenth Circuit, (2004); zur stets vorhandenen Anzahl von false positives: 1. Kap. Teil 2 A. I.

[1275] Reno v. American Civil Liberties Union et al., 521 U.S., S. 844, 117 S. Ct., S. 2329, Supreme Court of the United States, (1997); Ashcroft v. American Civil Liberties Union, 542 U.S., S. 656, 124 S. Ct., S. 2783, Supreme Court of the United States, (2004)

[1276] Reno v. American Civil Liberties Union et al., 521 U.S., S. 844, 117 S. Ct., S. 2329, Supreme Court of the United States, (1997); Ashcroft v. American Civil Liberties Union, 542 U.S., S. 656, 124 S. Ct., S. 2783, Supreme Court of the United States, (2004)

[1277] Ashcroft v. American Civil Liberties Union, 542 U.S., S. 656, 124 S. Ct., S. 2783, Supreme Court of the United States, (2004); Reno v. American Civil Liberties Union et al., 521 U.S., S. 844, 117 S. Ct., S. 2329, Supreme Court of the United States, (1997)

[1278] vgl.: 1. Kap. Teil 2 A. I.

[1279] Reno v. American Civil Liberties Union et al., 521 U.S., S. 844, 117 S. Ct., S. 2329, Supreme Court of the United States, (1997); Ashcroft v. American Civil Liberties Union, 542 U.S., S. 656, 124 S. Ct., S. 2783, Supreme Court of the United States, (2004)

[1280] vgl.: 1. Kap. Teil 1 B. II. 4.

[1281] vgl.: 3. Kap. Teil 1 B. I.

[1282] im Bereich der Telefaxwerbung: Kaufman v. ACS Systems, Inc., 110 Cal.App. 4th, S. 886, 2 Cal. Rptr.3d, S. 296, Court of Appeal, Second District, Division 1, California, (2003); Missouri ex. rel. Nixon v. American Blast Fax, Inc., 323 F.3d, S. 649, United States Court of Appeals, Eighth Circuit, (2003) zur Telefax-Werbung; Rudgayzer & Gratt v. Enine, Inc. 4 Misc.3d, S. 779 N.Y.S.2d, S. 882, Supreme Court, Appellate Term, New York.2nd and 11th Judicial Districts, (2004); a.A.: U.S. West, Inc. v. Federal Communications Commission, 182 F.3d, S.1224, United States Court of Appeals, Tenth Circuit, (1999)

II. Völkerrecht

Fraglich ist, ob völkerrechtliche Vorgaben den US-amerikanischen Gesetzgeber verpflichten, eine von der geltenden Rechtslage abweichende Regelung zu treffen, so beispielsweise die Opt-In-Lösung gesetzlich zu verankern.
Zwar wurde die Problematik, die mit dem wachsenden Volumen unverlangter Email-Werbung einhergeht auf internationaler Ebene mittlerweile erkannt, was auch zu Aktivitäten geführt hat.[1283] Bindende internationale Dokumente, die speziell Spam betreffen, gibt es jedoch bisher nicht.

Oben wurde bereits dargelegt, dass auch im IPbürgPR ein Recht auf Privatleben enthalten ist, vgl. Art. 17 IPbürgPR, sowie ein Recht auf freie Meinungsäußerung, vgl. Art. 19 IPbürgPR.[1284] Diese sind gegeneinander abzuwägen. Hier ist zu berücksichtigen, dass die Beschränkung der Werbemöglichkeit, also der Meinungsäußerung durch die Opt-Out-Lösung nicht besonders schwerwiegend ist. Denn kommerzielle Emails sind, sofern sie keine unzulässigen Inhalte enthalten, grundsätzlich rechtmäßig, solange der Empfänger ihrem Erhalt nicht widersprochen hat oder bestimmte mißbräuchlichen Praktiken angewandt werden.[1285] Andererseits wird diese Form der Werbung auch nicht uneingeschränkt zugelassen, was zu einem einseitigen Zurücktreten der Rechte derjenigen Adressaten führen würde, die Email-Werbung nicht empfangen möchten. Diese sind dadurch geschützt, dass ihnen Email-Werbung nicht mehr zugestellt werden darf, wenn sie von der Möglichkeit des Opt-Out Gebrauch gemacht haben. Folglich ist davon auszugehen, dass das Opt-Out-Prinzip dazu führt, dass die kollidierenden Grundrechte in einen angemessenen Ausgleich gebracht werden, dergestalt, dass keines zugunsten des jeweils anderen völlig zurückgedrängt wird. Folglich ist nicht von einer Verpflichtung des US-amerikanischen Gesetzgebers auszugehen, eine andere Regelung, etwa ein Opt-In-Prinzip im nationalen Recht zu installieren oder aber kommerzielle Emails grundsätzlich zuzulassen.

Hinzu kommt, dass die USA das IPbürgPR zwar ratifiziert, jedoch dabei einen Vorbehalt dergestalt angebracht haben, sich nicht durch den IPbürgPR zur Beschränkung der durch ihre Verfassung, Gesetze und Rechtspraxis gewährleisteten Kommunikationsfreiheit zu verpflichten.[1286] Des Weiteren brachten sie einen Vorbehalt dergestalt an, die Ratifizierung des Pakts vermöge innerstaatlich derartige Beschränkungen -so etwa durch den Gesetzgeber oder die Gerichte- nicht zu rechtfertigen.[1287] Danach ist völkerrechtlich wie staatsrechtlich

---

[1283] So veröffentlichte die OECD ein Task Force on Spam background paper, DSTI/CP/ICCP/SPAM/2005/10/FINAL, das den Mitgliedstaaten bei der Entwicklung der Spam- Gesetzgebung helfen soll und veranstaltete die UNO einen Gipfel zur Informationsgesellschaft, dessen zweiter Teil im November 2005 in Tunesien stattfand; die OECD hat mittlerweile einen Antispam-Toolkit entwickelt, an dem sich Gesetzgeber sowie die Industrie orientieren sollen; der Anti-Spam-Toolkit ist abrufbar unter http://www.oecd-antispam.org/ (letzter Abruf: 29.04.2007). Des Weiteren hat sich die Initiative London Action Plan (LAP), der mittlerweile Regierungsorganisationen sowie Wirtschaftsakteure aus 27 Staaten angehören den Kampf gegen Spam zum Ziel gesetzt; vgl. hierzu: http://www.londonactionplan.com/ (letzter Abruf: 29.04.2007).

[1284] vgl.: 2. Kap. Teil 1 B. II. 2. b)

[1285] vgl.: 3. Kap. Teil 1 A. I.

[1286] *Determann*, Kommunikationsfreiheit im Interenet, S. 248; zum Status der Ratifizierungen: http://www.ohchr.org/english/law/ccpr-ratify.htm (letzter Abruf: 29.04.2007)

[1287] Der Vorbehalt lautet: „*The Constitution of the United States and Art. 19 of the International Covenant on Civil and Political Rights contains provisions for the protection of individual rights, including the right of free speech, and nothing in this Covenant shall be deemed to require or to authorize legislation or other action by the United States which would restrict the right of free speech protected by the Constitution, law, and practice of the United States.*“, vgl. *Defeis*, 29 SJIL, S. 84; *Determann*, Kommunikationsfreiheit im Internet, S. 248

eine entsprechende Verpflichtung der USA ausgeschlossen.[1288] Insofern besteht keine Verpflichtung des US-amerikanischen Gesetzgebers, aufgrund internationaler Vorschriften von der geltenden Regelung abzuweichen.

III. Ergebnis

Die Rechtslage in den USA verstößt nicht gegen die US-amerikanische Verfassung oder gegen Völkerrecht. Ersteres ist allerdings noch nicht abschließend richterlich geklärt worden.

C. Ergebnis

Das Versenden kommerzieller Emails ist nach US-amerikanischem Recht grundsätzlich zulässig, wenn der Empfänger nicht den Widerspruch erklärt hat. Es gilt folglich das Opt-Out-Prinzip. Die Vorschriften des einfachen US-amerikanischen Rechts verstoßen weder gegen die Verfassung, noch gegen anderweitige höherrangige Vorschriften.

Teil 2: Zulässigkeit technischer Maßnahmen zur Identifizierung und Vermeidung unerbetener elektronischer Werbenachrichten

Gegenstand dieser Arbeit ist die Frage nach der rechtlichen Zulässigkeit der verschiedenen Maßnahmen, die der Filtereinsatz zum Zweck der automatisierten Identifizierung und Abwehr unverlangter elektronischer Werbenachrichten mit sich bringt. Die Filtersoftware bewirkt, wie bereits dargestellt, dass Inhalt und Headerinformationen eingehender Emails durch das Programm überprüft werden.[1289] Positiv gescannte Nachrichten werden entweder gelöscht, blockiert, als verdächtig markiert oder in Quarantäne-Ordnern abgelegt.[1290] Der Einsatz von Filtersoftware stellt die Reaktion auf das Versenden unverlangter kommerzieller Emails dar. Da die Widerrechtlichkeit der abgewehrten Nachrichten demnach mögliche Abwehrmaßnahmen rechtfertigen kann, wurde in Kapitel 3 Teil 1 darauf eingegangen, ob bzw. unter welchen Voraussetzungen der Versand solcher Emails als zulässig anzusehen ist. Nachdem diese Frage beantwortet wurde, kann nun auf das Hauptproblem der Arbeit eingegangen werden. Nachfolgend wird daher dargestellt, wie die Überprüfung von Inhalt und Headerinformationen eingehender Emails durch die zur Filterung eingesetzte Software rechtlich zu beurteilen und ob es rechtlich zulässig ist, Emails im Rahmen von Spam-Filtermaßnahmen zu blockieren, zu löschen, durch Hinzufügen einer zusätzlichen Headerzeile oder Veränderung der Subjektzeile zu markieren oder in Quarantäne-Ordner umzuleiten.
Dabei wird zunächst auf den Maßstab des einfachen Rechts eingegangen (A.), im Anschluss daran wird überprüft, ob die maßgeblichen Vorschriften im Einklang mit völker- und verfassungsrechtlichen Vorgaben stehen (B.).

[1288] Art. 19, 20 Wiener Übereinkommen über das Recht der Verträge, BGBl. II 1990, 1415 ff.; *Defeis*, 29 STJIL, S. 84; vgl. auch: *Determann*, Kommunikationsfreiheit im Internet, S. 254 f.
[1289] vgl.: 1. Kap. Teil 2 A.
[1290] vgl.: 1. Kap. Teil 2 B.

A. Einfaches Recht

Im Bereich des US-amerikanischen Rechts sind, wie bereits erwähnt, verschiedene Rechtsquellen zu unterscheiden und zwar Bundes- (I.) und einzelstaatliches Recht (II.).

I. Bundesrecht

Der Zulässigkeit des Filtereinsatzes könnten der Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 ff., §§ 2701 ff. (1.),[1291] weitere Vorschriften zum Schutz der Privatsphäre (2.) sowie der CAN-SPAM Act (3.) entgegenstehen.

1. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 ff., §§ 2701 ff.

Fraglich ist, ob der Filtereinsatz nach Maßgabe des Electronic Communications Privacy Act unzulässig ist. Das Gesetz unterteilt sich in zwei Abschnitte und zwar in den Wiretap Act, 18 U.S.C. §§ 2510 ff. (a) und den Stored Communications Act, 18 U.S.C. §§ 2701 ff. (b).

a) Wiretap Act, 18 U.S.C. §§ 2510 ff.

Nachfolgend soll dargestellt werden, ob die in 18 U.S.C. §§ 2510 ff. niedergelegten Vorschriften des so genannten Wiretap Act der Überprüfung des Inhalts und der Headerinformationen eingehender Emails sowie den verschiedenen Vorgehensweisen in Bezug auf als Spam identifizierte Emails durch Anti-Spam-Filtersoftware entgegenstehen.
Ein Verstoß gegen die Vorschriften des Wiretap Act, insbesondere gegen das in 18 U.S.C. § 2511 (1) (a) enthaltene Verbot der Überwachung elektronischer Kommunikation führt nach 18 U.S.C. § 2511 (4) zu einer Geld- oder Gefängnisstrafe von nicht unter fünf Jahren oder einer Kombination von beidem. Daneben kann der Betroffene auf dem Zivilrechtsweg Klage gegen die Person oder den Rechtsträger einreichen, der die Verletzungshandlung begangen hat, 18 U.S.C. § 2520 (a), und so einen etwaigen Schadensersatzanspruch durchzusetzen, 18 U.S.C. § 2520 (b) (2).[1292]

18 U.S.C. § 2511 (1) (a) schreibt den Grundsatz fest, dass sich Personen, die vorsätzlich einen elektronischen Kommunikationsvorgang überwachen, dies versuchen oder einen Dritten hierzu veranlassen, strafbar machen. Im Folgenden ist die Frage zu beantworten, ob derjenige, der eingehende Emails durch Filtersoftware auf in ihrem Inhalt und ihren Headerinformationen enthaltene werbetypische Merkmale überprüfen oder elektronische Nachrichten blockieren, löschen, markieren oder umleiten lässt, elektronische Kommunikation überwacht und damit ausweislich 18 U.S.C. § 2511 (1) (a) rechtswidrig handelt.
Dabei ist die Maßnahme nach 18 U.S.C. § 2511 (1) (a) dann rechtswidrig, wenn die betroffenen Emails als elektronische Kommunikation im Sinne des Gesetzes zu qualifizieren sind (aa), in den Filtervorgängen ein Überwachen zu sehen ist (bb) und keine im Gesetz genannte Ausnahme eingreift (cc).

[1291] vgl.: Anhänge II und III

[1292] Die Höhe des Schadensersatzanspruches ergibt sich hierbei entweder aus dem tatsächlich eingetretenen Schaden zuzüglich eines etwaigen Gewinns, den der Überwachende aufgrund der Verletzung erlangt hat, 18 U.S.C. § 2520 (b) (2) (A) oder nach der in 18 U.S.C. § 2520 (b) (2) (B) genannten Pauschale. Diese beträgt $ 100 pro Tag oder insgesamt $ 10.000, wobei der jeweils höhere Wert in Ansatz zu bringen ist. Auch im Verhältnis der Vorschriften 18 U.S.C. § 2520 (b) (A) und (B) ist der höhere Betrag maßgebend für den Schadensersatzanspruch, vgl. 18 U.S.C. § 2520 (b) (2).

aa) Elektronische Kommunikation, 18 U.S.C. § 2511 (1) (a) i.V.m. § 2510 (12)

Fraglich ist, ob es sich bei den von den Filtermaßnahmen betroffenen Emails um elektronische Kommunikation handelt.
18 U.S.C. § 2510 (12) enthält eine Legaldefinition dieses Begriffs. Danach ist unter elektronischer Kommunikation die Übermittlung von Zeichen, Signalen, Schrift, Bild, Ton, Daten oder anderen Informationen zu verstehen, die in ihrer Gesamtheit oder Teilen über Leitungen, Radio, elektromagnetische, photoelektronische oder photooptische Systeme übertragen werden, wobei die Übermittlung den zwischenstaatlichen oder internationalen Handel betreffen muss. Diese weite Definition wird durch vier Ausnahmetatbestände wieder eingeschränkt. Demnach sind bestimmte Kommunikationsformen, so insbesondere telegraphische, mündliche oder über einen nur Töne übertragenden Pager getätigte Äußerungen nicht als elektronische Kommunikation anzusehen, ebenso wie bestimmte finanzielle Informationen, 18 U.S.C. § 2510 (12) (a) (A)-(D).

Emails fallen unter 18 U.S.C. § 2510 (12), da hier Zeichen in Form von Daten über elektromagnetische Systeme übertragen werden. Die Passage, dass elektronische Kommunikation nur vorliegt, wenn die versandten Nachrichten den innerstaatlichen oder internationalen Handel betreffen, bewirkt keine Einschränkung, da ausweislich der Rechtsprechung schon häufig elektronische Kommunikation unter den Anwendungsbereich gefasst wurde, die nicht kommerzieller, sondern privater Natur war.[1293]

bb) Überwachen, 18 U.S.C. § 2511 (1) (a) i.V.m. § 2510 (4)

Unzulässig sind die aus dem Einsatz der Software resultierenden Maßnahmen jedoch nur, wenn sie sich als Überwachen im Sinne des 18 U.S.C. § 2510 (1) (a) i.V.m. § 2510 (4) qualifizieren lassen. Dies setzt einerseits voraus, dass die fraglichen Vorgänge zeitgleich mit der Übermittlung der Nachricht stattfinden (1).[1294] Andererseits ist erforderlich, dass die durch den Filtereinsatz bewirkten Maßnahmen der Legaldefinition des 18 U.S.C. § 2510 (4) unterfallen (2).

(1) Überwachen zeitgleich mit der Übermittlung

Wie bereits dargestellt wurde, werden im Fall des Black- oder Whitelisting die Headerinformationen eingehender Emails gescannt.[1295] Die Verbindung wird unterbrochen, sobald ersichtlich ist, dass die eingehende Nachricht von einem auf der schwarzen oder nicht auf der weißen Liste befindlichen Absender stammt.[1296] Insofern setzt die Filtermethode des Black- oder Whitelisting bereits zu einem Zeitpunkt an, zu dem die Email noch nicht vollständig auf dem Empfänger-Server eingetroffen ist. Demnach finden Maßnahmen beim Filtern durch Black- oder Whitelisting stets während der Übermittlung der Nachricht statt.

[1293] United States v. Reyes, 922 F. Supp., S. 836 f., United States District Court S.D. New York, (1996); Bohach v. City of Reno, 932 F. Supp., S. 1232 ff., United States District Court of Nevada, (1996)
[1294] United States v. Turk, 526 F. 2d, S. 658, United States Court of Appeals, Fifth Circuit, (1976); Steve Jackson Games v. U.S. Secret Service, 36 F. 3d, S. 460, United States Court of Appeals, Fifth Circuit, (1994); Konop v. Hawaiian Airlines, Inc., 302 F. 3d, S. 878 f., United States Court of Appeals, Ninth Circuit, (2002); United States v. Steiger, 318 F. 3d, S. 1048 f., United States Court of Appeals, Eleventh Circuit, (2003); Fraser v. Nationwide Life Insurance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003); aA.: United States v. Smith, F. 3d, S. 1059, United States Court of Appeals, Ninth Circuit, (1998)
[1295] vgl.: 1. Kap. Teil 2 A. I.
[1296] vgl.: 1. Kap. Teil 2 A. I.

Fraglich ist, ob sich für diejenigen Filterverfahren eine andere Beurteilung ergibt, bei denen es zu einer inhaltlichen Überprüfung eingehender Emails kommt. Hier werden die Maßnahmen zu einem Zeitpunkt vorgenommen, in dem bereits sämtliche Datenpakete den Empfänger-Mailserver erreicht haben und wieder zusammengesetzt wurden.[1297] Normalerweise wird sodann durch einen so genannten „mail delivery agent" entschieden, welcher Nutzer die Nachricht erhalten soll und diese sodann in die entsprechende Empfänger-Mailbox eingestellt.[1298] Zuvor finden jedoch die Filtermaßnahmen statt. Fraglich ist, ob die Durchführung dieser Maßnahmen, die zwar nach Eingang und Zusammensetzen sämtlicher Datenpakete, aber vor einem endgültigen Speichern auf dem Server oder in der Mailbox des Empfängers vorgenommen werden, zeitgleich mit der Übermittlung stattfinden.

Nach einer Auffassung fallen nur solche Emails in den Anwendungsbereich des Wiretap Act, die sich gerade auf dem virtuellen Weg zwischen zwei Rechnern befinden.[1299] Ausgangspunkt ist der in der Rechtsprechung vielfach ausgesprochene Grundsatz, dass elektronisch gespeicherte Kommunikation nicht im Sinne des 18 U.S.C. § 2511 (1) (a) überwacht werden kann.[1300] Da ausweislich der Definition des 18 U.S.C. § 2510 (17) (A) auch lediglich temporär zwischengespeicherte Kommunikation als elektronisch gespeichert anzusehen ist, könnten daher Maßnahmen, die während des momentanen Ruhens im Zwischenspeicher vorgenommen werden, vom Anwendungsbereich des 18 U.S.C. §§ 2510 ff. ausgeschlossen sein. Folgt man dieser Meinung, so ergibt sich, dass eine Email auf ihrem Weg vom Absender zum Empfänger verschiedene Stadien durchläuft und der Vorschrift des 18 U.S.C. § 2511 (1) (a) nur dann unterfällt, wenn sie gerade nicht zwischengespeichert ist.
Die Auffassung wird damit begründet, die in 18 U.S.C. § 2510 (12) enthaltene Definition der elektronischen Kommunikation sei im Zusammenhang mit derjenigen der telegraphischen Kommunikation in 18 U.S.C. § 2510 (1) zu sehen.[1301] Hierbei ist zu beachten, dass die in 18 U.S.C. § 2510 (1) enthaltene Legaldefinition der telegraphischen Kommunikation lange Zeit eine Passage enthielt, die explizit elektronisch gespeicherte Kommunikation mit einschloss. 18 U.S.C. § 2510 (12) enthält hingegen hinsichtlich der elektronischen Kommunikation keine derartige Textpassage. Aus dieser Tatsache folgerte man, dass der Gesetzgeber beabsichtigt habe, elektronisch zwischengespeicherte Emails vom Anwendungsbereich des Wiretap Act auszuschließen.[1302] Zur Begründung dieser Auffassung wurde auf die so genannte Russello-Rechtsprechung verwiesen, ausweislich derer in Fällen, in denen der Kongress in einem Teil eines Gesetzes eine explizite Regelung trifft, dies jedoch in einem anderen Teil unterlässt, davon auszugehen ist, dass diese Auslassung beabsichtigt war.[1303] Mittlerweile wurde allerdings die Passage, die elektronisch gespeicherte Kommunikation unter den Begriff der

[1297] vgl.: 1. Kap. Teil 2 A. II. und III.
[1298] United States v. Councilman, 418 F.3d, S. 69, United States Court of Appeals, First Circuit, (2005)
[1299] so die Argumentation des Angeklagten in: United States v. Councilman, 418 F.3d, S. 67 ff., United States Court of Appeals, First Circuit, (2005)
[1300] United States v. Turk, 526 F. 2d, S. 658 f., United States Court of Appeals, Fifth District, (1976); Steve Jackson Games v. United States Secret Service, F. 3d, S. 461 f., United States Court of Appeals, Fifth Circuit, (1994); United States v. Reyes, 922 F. Supp., S. 836, United States District Court S.D. New York, (1996); United States v. Steiger, 318 F.3d, S. 1049, United States Court of Appeals, Eleventh Circuit, (2003)
[1301] Steve Jackson Games v. United States Secret Service, F. 3d, S. 461 f., United States Court of Appeals, Fifth Circuit, (1994); Fraser v. Nationwide Life Insturance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003); so die Argumentation des Angeklagten Councilman in United States v. Councilman, 418 F.3d, 67 ff., United States Court of Appeals, First Circuit, (2005)
[1302] so die Argumentation des Angeklagten Councilman in: United States v. Councilman, 418 F.3d, 67 ff., United States Court of Appeals, First Circuit, (2005)
[1303] Russello v. United States, 464 U.S., S. 23, United States Supreme Court, (1983); United States v. Councilman, 418 F.3d, S. 73, United States Court of Appeals, First Circuit, (2005)

telegraphischen Kommunikation nach 18 U.S.C. § 2510 (1) fasste, durch den USA PATRIOT ACT[1304] gestrichen.

Einige Aspekte sprechen dafür, kurzzeitig in den Zwischenspeicher geladene Emails in den Anwendungsbereich des Wiretap Act einzubeziehen. Hier lässt sich einerseits die weit formulierte Legaldefinition der elektronischen Kommunikation in 18 U.S.C. § 2510 (12) anführen. Unter diesen Begriff lassen sich grundsätzlich auch im Zwischenspeicher befindliche Nachrichten fassen.[1305] Auch ist die oben dargestellte, auf die Unterschiede der Definitionen der telegraphischen und elektronischen Kommunikation abstellende Argumentation nicht zwingend. Denn zwar ist es richtig, dass die US-amerikanische Rechtsprechung im Rahmen der Gesetzesauslegung bisweilen auf die oben erwähnte Russello-Vermutung zurückgreift. Allerdings kann diese widerlegt werden, wenn nachgewiesen wird, dass der Gesetzgeber mit der Auslassung kein bestimmtes Ziel verfolgte.[1306] Dabei spricht Einiges gegen eine Absicht des Gesetzgebers, im Zwischenspeicher befindliche Emails dadurch vom Anwendungsbereich des Wiretap Act auszuschließen, dass diese nicht explizit durch Aufnahme einer entsprechenden Passage in die Definition der elektronischen Kommunikation miteinbezogen wurden. Insbesondere ergeben sich Zweifel an einer derartigen Schlussfolgerung, wenn man die Regelungstechnik der beiden Definitionen vergleicht. Es zeigt sich, dass die Definition der telegraphischen Kommunikation aus einer Aufzählung von Einzelfällen besteht, die demnach nur vollständig sein kann, wenn sie alle denkbaren Fälle nennt, die hiervon erfasst sein sollen.[1307] Im Gegensatz dazu wird der Begriff der elektronischen Kommunikation in 18 U.S.C. § 2510 (12) sehr weit gefasst und lediglich durch explizit normierte Ausnahmebestimmungen wieder eingeschränkt.[1308] Demnach erfasst die Definition grundsätzlich alle genannten Übermittlungsformen, die nicht unter eine der aufgezählten Ausnahmebestimmungen fallen. Daher kann aus der fehlenden Aufnahme einer Passage, in der die gespeicherte Kommunikation explizit in den Anwendungsbereich einbezogen wird, nicht gefolgert werden, dass diese deshalb nicht als elektronische Kommunikation zu qualifizieren ist.[1309] Vielmehr spricht die gewählte gesetzliche Regelungstechnik dafür, dass die Aufzählung der Ausnahmebestimmungen in der Legaldefinition der elektronischen Kommunikation abschließend ist.[1310] Danach ist die Russello-Vermutung hier widerlegt.[1311] Somit sprechen gute Gründe dafür, im Zwischenspeicher befindliche Nachrichten in den Anwendungsbereich miteinzubeziehen.
Auch die der Gesetzgebung vorausgehende Entwicklung spricht für eine Einbeziehung zwischengespeicherter Emails in den Anwendungsbereich des Wiretap Act. Denn der Gesetzgeber verfolgte das Ziel, den Schutz der Privatsphäre zu stärken und fasste die Definition des Begriffs der elektronischen Kommunikation deshalb bewusst weit.[1312] Daneben war es nicht Ziel der Einbeziehung der gespeicherten Kommunikation in die Legaldefinition des 18 U.S.C. § 2510 (1), diese aus dem Anwendungsbereich des 18 U.S.C. §

[1304] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Publ. L. No. 107-56
[1305] United States v. Councilman, 418 F.3d, S. 73 f., United States Court of Appeals, First Circuit, (2005)
[1306] United States v. Councilman, 418 F.3d, S. 73 f., United States Court of Appeals, First Circuit, (2005)
[1307] United States v. Councilman, 418 F.3d, S. 75, United States Court of Appeals, First Circuit, (2005)
[1308] United States v. Councilman, 418 F.3d, S. 75, United States Court of Appeals, First Circuit, (2005)
[1309] TRW v. Andrews, 543 U.S., S. 28, 122 S. Ct., S. 441, Supreme Court of the United States, (2001); United States v. Councilman, 418 F.3d, S. 75 f., United States Court of Appeals, First Circuit, (2005)
[1310] TRW v. Andrews, 543 U.S., S. 28, 122 S. Ct., S. 441, Supreme Court of the United States, (2001); United States v. Councilman, 418 F.3d, S. 75 f., United States Court of Appeals, First Circuit, (2005)
[1311] TRW v. Andrews, 543 U.S., S. 28, 122 S. Ct., S. 441, Supreme Court of the United States, (2001); United States v. Councilman, 418 F.3d, 75 f., United States Court of Appeals, First Circuit, (2005)
[1312] United States v. Councilman, 418 F.3d, S. 76 f., United States Court of Appeals, First Circuit, (2005)

2510 (12) auszunehmen. Vielmehr erfolgte die Aufnahme der Passage einzig und allein zu dem Zweck, auch Voice-Mail-Nachrichten in den Anwendungsbereich des Wiretap Act einzubeziehen.[1313]
Für eine Einbeziehung im Zwischenspeicher befindlicher Emails in den Anwendungsbereich des Wiretap Act spricht daneben, dass das Wortlautargument, das sich früher aus dem Vergleich der Definitionen der telegraphischen und der elektronischen Kommunikation ergab, nicht mehr angeführt werden kann, da diese Passage durch den USA PATRIOT ACT gestrichen wurde.
Auch die Tatsache, dass zwischengespeicherte elektronische Nachrichten möglicherweise auch dem Stored Communications Act unterfallen, spricht nicht gegen deren Einbeziehung in den Wiretap Act. Denn es ist möglich, dass im Hinblick auf ein- und denselben Sachverhalt verschiedene Vorschriften eingreifen. In Bezug auf den Wiretap Act und den Stored Communications Act ist anerkannt, dass diese sich teilweise überschneiden.[1314]

Demnach sprechen die besseren Argumente für eine Einbeziehung der im Zwischenspeicher befindlichen elektronischen Nachrichten in den Anwendungsbereich des Wiretap Act. Hierdurch werden auch Schwierigkeiten vermieden, die andernfalls daraus resultieren würden, dass jeweils im Einzelfall festgestellt werden müsste, ob eine Email, die sich auf dem Weg vom Absender zum Empfänger befand, zum Zeitpunkt einer bestimmten Maßnahme gerade zwischengespeichert war oder nicht.
Insofern ist davon auszugehen, dass Emails auf ihrem gesamten Weg vom Absender zum Empfänger bis zu dem Zeitpunkt vom Schutz des Wiretap Act umfasst sind, in dem die Nachricht auf dem Empfänger-Server oder in der Mailbox abgespeichert wird.[1315] Denn erst zu diesem Zeitpunkt endet der Vorgang der Übermittlung auf den die Definition der elektronischen Kommunikation in 18 U.S.C. § 2510 (12) abstellt. Findet die Überwachung während des vorgenannten Zeitrahmens statt, so geschieht sie demnach zeitgleich mit der Übermittlung.

(2) Voraussetzungen der Legaldefinition des 18 U.S.C. § 2510 (4)

Unter dem Begriff des Überwachens ist nach der gesetzlichen Legaldefinition des 18 U.S.C. § 2510 (4) das Beschaffen der Inhalte einer telegraphischen, elektronischen oder mündlichen Kommunikation zu verstehen, die mittels elektronischer, mechanischer oder anderer Mittel durchgeführt wird. Es stellt sich hier demnach die Frage, ob davon gesprochen werden kann, dass sich eine Person Inhalte der Kommunikation verschafft, wenn sie Filtersoftware verwendet, die den Inhalt und die Headerinformationen eingehender Email-Nachrichten elektronisch überprüft oder das Blockieren, Löschen, Markieren und Umleiten elektronischer Nachrichten bewirkt.

Hierbei umfasst der Begriff der Inhalte Informationen, die den Inhalt, Wortlaut oder die Bedeutung der Kommunikation betreffen, 18 U.S.C. § 2510 (8). Demnach handelt es sich zwar bei den im eigentlichen Text der Email und entsprechenden im Betreff enthaltenen Informationen um Inhalte, da diese Bestandteile der Nachricht den Wortlaut und die Bedeutung der Information enthalten. Die bloße Überprüfung der Steuerungsdaten fällt

[1313] United States v. Councilman, 418 F.3d, S. 76 f., United States Court of Appeals, First Circuit, (2005)
[1314] United States v. Davis, 978 F. 2d, S. 420, United States Court of Appeals, Eighth Circuit (1992); United States v. Herring, 993 F. 2d, S. 788, Fn. 4, United States Court of Appeals, Eleventh Circuit (1993)
[1315] Steve Jackson Games v. United States Secret Service, 36 F. 3d, S. 461 f., United States Court of Appeals, Fifth Circuit, (1994); United States v. Reyes, 922 F. Supp., S. 836 f., United States District Court S.D. New York, (1996); United States v. Councilman, 418 F.3d, S. 77 f., United States Court of Appeals, First Circuit, (2005)

allerdings nicht unter die Vorschrift, da diese keine Informationen in Bezug auf Inhalt, Wortlaut oder Bedeutung der Kommunikation sind.

Schließlich nennt das Gesetz in 18 U.S.C. § 2510 (4) ein weiteres Merkmal, das vorliegen muss, damit von einer Überwachung der elektronischen Kommunikation ausgegangen werden kann und zwar das Beschaffen der Inhalte. Fraglich ist, ob derjenige, der die entsprechende Filtersoftware einsetzt, sich hierdurch Inhalte der fraglichen Nachrichten beschafft.
Oben wurde ausgeführt, dass durch die entsprechenden Programme eingehende Emails, die auf werbebezogene Textbausteine untersucht werden sollen, virtuell geöffnet werden.[1316] Letztlich bedeutet dies, dass das Programm „Kenntnis“ vom Inhalt der Nachricht nimmt.[1317] Hierzu werden die Nachrichten momentan in den Zwischenspeicher geladen, aber zu diesem Zweck nicht dauerhaft gespeichert oder für den Provider oder seine Mitarbeiter lesbar abgelegt.[1318] Eine dauerhafte Fixierung der Daten auf einem Speichermedium erfolgt hingegen nicht.[1319] Somit steht derjenige, dessen Daten von der Filtermaßnahme betroffen sind, hinsichtlich der Vertraulichkeit der ihn betreffenden Informationen nicht anders, als dies ohne den Filtereinsatz der Fall sein würde. Denn die in der Email enthaltenen Informationen werden während des Filtereinsatzes nicht durch eine natürliche Person wahrgenommen und mit dem Betroffenen in Verbindung gebracht. Dies kann auch nicht später nachgeholt werden, da die Daten nicht infolge des Filtereinsatzes dauerhaft gespeichert bleiben. Dies bedeutet, dass im Rahmen der durchgeführten Maßnahmen keine natürliche Person von den Informationen Kenntnis nimmt und diese auch nicht später zum Zweck der Kenntnisnahme zur Verfügung stehen. Daher kann nicht davon gesprochen werden, dass derjenige, der die Filtersoftware einsetzt, sich die überprüften Inhalte beschafft.

Wer als Spam identifizierte Emails blockiert, löscht, markiert oder umleitet, zielt erst gar nicht darauf ab, sich deren Inhalt zu beschaffen. Vielmehr ist Zweck des Filtereinsatzes, unerwünschte Nachrichten zu entfernen bzw. erst gar nicht auf dem Server zu speichern. Auf eine inhaltliche Wahrnehmung oder ein Ablegen bzw. Speichern der Nachrichten zu diesem Zweck sind sie hingegen nicht gerichtet. Aus diesem Grund verstößt auch das Blockieren, Löschen, Markieren oder Umleiten von Nachrichten nicht gegen die Vorschriften des Wiretap Act, 18 U.S.C. §§ 2510 ff.

(3) Zwischenergebnis

Im Ergebnis stellt weder das Überprüfen des Inhalts und der Headerdaten eingehender Emails, noch das Löschen, Umleiten, Markieren oder Blockieren positiv gescannter Emails ein Überwachen elektronischer Kommunikation im Sinne des 18 U.S.C. § 2510 (4) dar.

cc) Ausnahmen, 18 U.S.C. § 2511 (2) (a) (i) und § 2511 (2) (c) und (d)

Soweit von einem Überwachen elektronischer Kommunikation im Sinne des 18 U.S.C. § 2510 (4) auszugehen wäre, würde 18 U.S.C. § 2511 (2) (a) (i) Bedeutung gewinnen. Bei Vorliegen der Voraussetzung der Vorschrift kann ein Provider elektronische Kommunikation überwachen, ohne rechtswidrig zu handeln. Die Vorschrift sieht vor, dass keine rechtswidrige Handlung vorliegt, wenn Angestellte oder Beauftragte eines Providers, dessen Einrichtungen zum Zweck der elektronischen Kommunikation genutzt werden, diese überwachen, sofern die

[1316] vgl.: 1. Kap. Teil 2 A. II. und III.
[1317] vgl.: 1. Kap. Teil 2 A. II. und III.
[1318] vgl.: 1. Kap. Teil 2 A. II.
[1319] vgl.: 1. Kap. Teil 2 A. II.

Maßnahme der Erbringung der Dienstleistung oder dem Schutz der Rechte des Providers oder seines Eigentums dient, 18 U.S.C. § 2511 (2) (a) (i).

Demnach wäre die Untersuchung eingehender Emails durch den Provider einerseits dann zulässig, wenn die entsprechende Maßnahme der Erbringung der Dienstleistung dienen würde. Wie oben bereits dargestellt, hat das Volumen der versandten unerwünschten Werbe-Emails mittlerweile solche Ausmaße angenommen, dass die Server der Provider diese teilweise nicht mehr zeitnah verarbeiten können.[1320] Die unerwünschten Werbe-Emails haben zur Folge, dass Speicherplatz blockiert wird und die Rechnerleistung des Servers des Providers nachlässt.[1321] Somit steigt auch der Zeitaufwand der Kunden für die Datenübernahme vom Server des Providers auf das eigene System und für das Aussortieren der unverlangten Werbe-Emails.[1322] Folglich dient das Überwachen eingehender Emails der Erbringung der Dienstleistung.

Andererseits wäre der Einsatz der Filtersoftware auch dann zulässig, wenn die Maßnahme dem Schutz von Rechten oder des Eigentums des Providers dienen würde. Hiervon wird beispielsweise dann ausgegangen, wenn durch die entsprechende Maßnahme der Missbrauch des Systems des Providers aufgedeckt und verhindert werden soll.[1323] Auch rein finanzielle Interessen rechtfertigen das Tätigwerden des Providers.[1324]
Durch das Volumen eingehender Werbe-Emails entstehen auf Seiten des Providers, wie oben bereits dargestellt,[1325] Kosten. Diese fallen beispielsweise für den Einsatz eigener Mittel an, so etwa durch das Erfordernis der Bereitstellung von zusätzlichem Speicherplatz, höherer Rechnerleistung oder des Einstellens weiterer Arbeitskräfte. Demnach tangieren kommerzielle Emails den Provider in seinen finanziellen Interessen. Insofern ist davon auszugehen, dass er eingehende elektronische Nachrichten auf werbebezogene Merkmale untersuchen darf. Die vorgenommenen Maßnahmen kann er auch nicht auf unerwünschte Nachrichten beschränken, da er vor der Filterung gerade keine Kenntnis davon haben kann, ob es sich bei einer einzelnen Email um Spam oder eine legitime Nachricht handelt.
Des Weiteren darf der Provider einen Missbrauch seines Systems ausweislich der oben zitierten Rechtsprechung durch Überwachungsmaßnahmen verhindern. Somit ist der Filtereinsatz auch aus diesem Grund als zulässig anzusehen. Demnach greift hier die Ausnahme zugunsten der Provider ein. Auch Arbeitgeber, die ihren Angestellten die Möglichkeit zum Versenden und Empfang von Emails über das Firmennetzwerk zur Verfügung stellen, sind als Provider im vorgenannten Sinne zu qualifizieren.[1326] Somit sind beide Personengruppen dazu berechtigt, Filtersoftware einzusetzen und eingehende Emails auf ihre Eigenschaft als Spam zu überprüfen.[1327] Dies bedeutet, dass -selbst wenn die inhaltliche Überprüfung als Überwachung im Sinne des 18 U.S.C. § 2511 (1) (a) zu qualifizieren wäre- hier die Ausnahmekonstellation des 18 U.S.C. § 2511 (2) (a) (i) dazu führen würde, dass die vorgenommene Handlung nicht als rechtswidrig anzusehen ist.

[1320] vgl.: 1. Kap. Teil 1 B. 4.
[1321] vgl.: 1. Kap. Teil 1 B. 4.
[1322] vgl.: 1. Kap. Teil 1 B. 4.
[1323] für die Überwachung durch einen Telefonanbieter: United States v. DeLeeuw, 368 F. Supp., S. 427 f., United States District Court, Eastern District of Wisconsin, (1974); United States v. Freeman, 373 F.Supp., S. 50 ff., United States District Court, S.D. Indiana, Indianapolis Division, (1974)
[1324] für den vergleichbaren Fall der Einsichtnahme in Telefonunterlagen: Schmidt v. Ameritech, 115 F.3d, S. 501 ff., United States Court of Appeals, Seventh Circuit, (1997)
[1325] vgl.: 1. Kap. Teil 1 B. II. 4.
[1326] United States v. McLaren, 957, F.Supp., S. 215 ff., United States District Court, M.D. Florida, (1997); *Greenberg*, 44 Am. U. L. Rev. (1994), S. 236; *Hymowitz/Bendana*, S. 17; *Kierkegaard*, Computer Law & Security Report 2005, S. 233
[1327] *Greenberg*, 44 Am. U. L. Rev. (1994), S. 236; *Hymowitz/Bendana*, S. 17; *Kierkegaard*, Computer Law & Security Report 2005, S. 233

Im Übrigen ist der Einsatz dann nicht rechtswidrig, wenn eine der Parteien des Kommunikationsvorgangs ihre Einwilligung damit erklärt hat, 18 U.S.C. § 2511 (2) (c) und (d).

dd) Zwischenergebnis

Der Einsatz von Filtersoftware, die Inhalt und Headerinformationen eingehender Emails auf bestimmte Merkmale durchsucht, verstößt nicht gegen die Vorgaben des Wiretap Act. Gleiches gilt für das Blockieren, Löschen, Markieren und Umleiten positiv gescannter Emails.

b) Stored Communications Act, § 18 U.S.C. §§ 2701 ff.

Die Unzulässigkeit der fraglichen Maßnahmen ergibt sich möglicherweise aus den in 18 U.S.C. §§ 2701 ff. niedergelegten Vorschriften des Stored Communications Act.
Ein Verstoß gegen die genannten Vorschriften, insbesondere gegen 18 U.S.C. § 2701 (a) ist strafrechtlich sanktioniert und kann -je nach Schwere des Falles- zu einer Geldstrafe oder einer Freiheitsstrafe von bis zu fünf, im Wiederholungsfall zehn Jahren führen, wobei Geld- und Freiheitsstrafe auch kombiniert werden können, 18 U.S.C. § 2701 (b). Des Weiteren sind diejenigen Personen und Rechtsträger, die von dem Verstoß betroffen sind, so der Provider des elektronischen Kommunikationsdienstes, der Teilnehmer oder andere betroffene Personen berechtigt, auf dem Zivilrechtsweg Klage gegen denjenigen zu erheben, der den Verstoß begangen hat, 18 U.S.C. § 2707 (a). Hierdurch besteht für den Geschädigten insbesondere die Möglichkeit Schadensersatz zu erhalten, 18 U.S.C. § 2707 (b) (2).[1328]

18 U.S.C. § 2701 (a) schützt davor, dass sich ein kommunikationsfremder Dritter vorsätzlich und ohne Berechtigung Zugang zu einer Vorrichtung verschafft, mittels derer ein elektronischer Kommunikationsdienst erbracht wird, 18 U.S.C. § 2701 (a) (1), oder die eigene Handlungsbefugnis überschreitet, um sich den Zugang zu verschaffen, 18 U.S.C. § 2701 (a) (2). Erhält die Person auf diese Weise Zugang zu einer elektronischen Kommunikation oder ändert bzw. verhindert er den autorisierten Zugang zu dieser, während sie in einem System elektronisch gespeichert ist, so handelt er rechtswidrig, 18 U.S.C. § 2701 (a).

Der Einsatz der Software wäre demnach rechtswidrig, wenn es sich bei den betroffenen Emails um elektronisch gespeicherte Kommunikation handeln würde (aa), wenn sich derjenige, der die Software einsetzt, hierdurch ohne Berechtigung Zugang zu einer Vorrichtung verschafft, mittels derer ein elektronischer Kommunikationsdienst erbracht wird und er dabei autorisierten Zugang zu der Kommunikation erhält oder diesen ändert bzw. verhindert, während sie in einem System elektronisch gespeichert ist (bb). Allerdings fehlt es trotz Vorliegens der genannten Voraussetzungen an einer rechtswidrigen Handlung, wenn eine gesetzliche Ausnahmevorschrift eingreift (cc).

aa) Elektronisch gespeicherte Kommunikation

Elektronisch gespeichert ist Kommunikation einerseits im Fall der temporären Zwischenspeicherung, die in Zusammenhang mit ihrer elektronischen Übermittlung steht, 18 U.S.C. § 2711 (1) in Verbindung mit 18 U.S.C. § 2510 (17) (A). Das Gleiche gilt, wenn die Aufbewahrung der Nachricht durch den Dienstleister eines elektronischen

[1328] Der Schadensersatz richtet sich nach dem real erlittenen Schaden zuzüglich eines etwaigen Gewinns, den der Schädiger infolge der Verletzung erhält, beträgt jedoch mindestens $ 1.000; wenn die Verletzung vorsätzlich ist, kommt daneben ein Strafschadensersatz in Betracht, 18 U.S.C. § 2701 (c).

Kommunikationsdienstes zum Zweck der Back-Up-Sicherung erfolgt, 18 U.S.C. § 2711 (1) in Verbindung mit § 2510 (17) (B). Ein Zwischenspeichern im Sinne des 18 U.S.C. § 2510 (17) (A) liegt etwa dann vor, wenn Emails auf dem Server des Internet-Service-Providers gespeichert sind, bevor sie ausgeliefert werden.[1329] Nach der Auslieferung liegt allerdings keine Zwischenspeicherung mehr vor, da von diesem Begriff ausweislich der gesetzlichen Definition lediglich temporär gespeicherte Nachrichten erfasst sind.[1330] Jedoch handelt es sich bei weiterhin auf dem Server des Providers befindlichen Nachrichten dennoch um elektronisch gespeicherte Kommunikation.[1331] Denn ab dem Zeitpunkt der Auslieferung der Email an den Empfänger erfüllt die auf dem Server des Providers gespeicherte Nachricht die Vorgaben des 18 U.S.C. § 2510 (17) (B).[1332] Das Speichern der Nachricht dient dem Zweck, eine Kopie für den Fall bereitzuhalten, dass der Nutzer diese nochmals vom Server des Providers herunterladen möchte. Sie dient demnach als Back-Up und fällt deshalb unter die Definition des 18 U.S.C. § 2510 (17) (B).[1333]

Daraus folgt, dass in den Fällen, in denen die Nachricht noch nicht temporär gespeichert ist, während die darin enthaltenen Daten überprüft werden, der Vorgang bereits aufgrund dieser Tatsache nicht unter die Vorschrift des 18 U.S.C. § 2701 (a) fällt. Eine derartige Konstellation wird insbesondere dann vorliegen, wenn durch die entsprechende Software lediglich die Headerinformationen abgeglichen werden, so etwa die Email-, IP- oder Domain-Adresse des Absenders, da dies, wie dargestellt, gerade erfolgt, bevor die Nachricht vollständig beim Server des Empfängers eingeht.[1334] Aus dem Anwendungsbereich der Vorschrift fallen demnach solche Nachrichten, die bereits aufgrund der Email-, IP- oder Domain- Adresse ihres Absenders zurückgewiesen werden. Denn in diesem Fall kommt es gar nicht zu einer vollständigen Zustellung sämtlicher Datenpakete, da die Verbindung zuvor unterbrochen wird.[1335] Folglich betreffen etwaige Maßnahmen nicht eine im Zustand der momentanen Zwischenspeicherung befindliche Email. Hingegen wird in den Fällen, in denen die Nachricht virtuell geöffnet wird, um ihren Inhalt zu untersuchen, davon auszugehen sein, dass sie zu diesem Zeitpunkt zumindest temporär zwischengespeichert wird, da andernfalls ein Öffnen nicht möglich wäre.[1336] Da das zeitweilige Zwischenspeichern nach 18 U.S.C. § 2711 (1) in Verbindung mit 18 U.S.C. § 2510 (17) (A) als elektronisches Speichern im Sinne des 18 U.S.C. § 2701 (a) gilt, scheitert die Anwendbarkeit der Vorschrift im Fall des virtuellen Öffnens nicht bereits daran, dass die Nachricht nicht elektronisch gespeichert ist.

[1329] Steve Jackson Games v. United States Secret Service, 36 F. 3d, S. 461 f., United States Court of Appeals, Fifth Circuit, (1994); In re Doubleclick, Inc. Privacy Litig., 154 F. Supp. 2d, S. 511 f., United States District Court, S.D.N.Y., (2001); Theofel v. Farey- Jones, 341 F.3d, S. 984 f., United States Court of Appeals for the Ninth Circuit, (2003); zweifelnd: Fraser v. Nationwide Life Insturance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003)

[1330] In re Doubleclick, Inc. Privacy Litig., 154 F. Supp. 2d, S. 511 f., United States District Court, S.D.N.Y., (2001); Fraser v. Nationwide Life Insturance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003); Theofel v. Farey- Jones, 341 F.3d, S. 985, United States Court of Appeals for the Ninth Circuit, (2003)

[1331] Theofel v. Farey- Jones, 341 F.3d, S. 984, United States Court of Appeals for the Ninth Circuit, (2003); zweifelnd: Fraser v. Nationwide Life Insturance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003)

[1332] Theofel v. Farey- Jones, 341 F.3d, S. 984, United States Court of Appeals for the Ninth Circuit, (2003); zweifelnd: Fraser v. Nationwide Life Insturance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003)

[1333] Theofel v. Farey- Jones, 341 F.3d, S. 984, United States Court of Appeals for the Ninth Circuit, (2003); zweifelnd: Fraser v. Nationwide Life Insturance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003)

[1334] vgl.: 1. Kap. Teil 2 A. I. und IV.

[1335] vgl.: 1. Kap. Teil 2 A. I.

[1336] vgl.: 1. Kap. Teil 2 A. II. und III.

bb) Zugangverschaffen zu der Vorrichtung und der Kommunikation bzw. Verhindern des Zugangs zu der Kommunikation

Fraglich ist, ob davon auszugehen ist, dass derjenige, der die entsprechende Software einsetzt, sich ohne Berechtigung Zugang zu einer Vorrichtung verschafft, mittels derer ein elektronischer Kommunikationsdienst erbracht wird und hierdurch autorisierten Zugang zu der Kommunikation erhält oder diese ändert bzw. verhindert. Die durch den Filtereinsatz bewirkte Überprüfung von Inhalt und Headerinformationen eingehender Emails kann bereits vom Wortlaut her nicht als Ändern oder Verhindern der Kommunikation angesehen werden. Auch in dem Markieren oder Umleiten der Nachricht in einen Ordner, auf den der Empfänger Zugriff hat, ist kein Ändern oder Verhindern des Zugangs zu der Kommunikation zu sehen, da der autorisierte Nutzer trotz dieser Maßnahmen auf die gespeicherte Kommunikation zugreifen kann.

Im Hinblick auf das Blockieren und Löschen eingehender Emails durch die Filtersoftware stellt sich die Frage, ob sich derjenige, der die entsprechende Software einsetzt, ohne Berechtigung Zugang zu der Vorrichtung verschafft und so autorisierten Zugang zu der Kommunikation erhält. Es wird bereits an der ersten Voraussetzung fehlen. Denn derjenige, der die Filtermaßnahmen vornimmt bzw. anordnet, besitzt grundsätzlich berechtigten Zugang zu der eigenen Vorrichtung. Insofern kann nicht davon gesprochen werden, dass sich die Person oder der Rechtsträger ohne Berechtigung Zugang verschafft. Im Übrigen erhält er auch keinen Zugang zu der Kommunikation. Denn -wie oben bereits erläutert-[1337] wird die Nachricht während des Filtervorgangs zwar momentan in den Zwischenspeicher geladen, aber zu diesem Zweck nicht dauerhaft gespeichert oder für den Provider oder seine Mitarbeiter lesbar abgelegt. Eine dauerhafte Fixierung der Daten auf einem Speichermedium erfolgt hingegen nicht.[1338] Somit steht derjenige, dessen Daten von der Filtermaßnahme betroffen sind, hinsichtlich der Vertraulichkeit der ihn betreffenden Informationen nicht anders, als dies ohne den Filtereinsatz der Fall sein würde.[1339] Denn die in der Email enthaltenen Informationen werden während des Filtereinsatzes nicht durch eine natürliche Person wahrgenommen und mit dem Betroffenen in Verbindung gebracht.[1340] Dies kann auch nicht später nachgeholt werden, da die Daten nicht infolge des Filtereinsatzes dauerhaft gespeichert bleiben.[1341] Insofern ist der Inhalt der Kommunikation, den 18 U.S.C. § 2701 (a) schützt, hier nicht gefährdet. Es kann daher nicht davon gesprochen werden, dass sich derjenige, der die Software einsetzt, Zugang zu der Kommunikation beschafft.

18 U.S.C. § 2701 (a) greift demnach bereits deshalb nicht ein, weil derjenige, der den Filter einsetzt, nicht unberechtigt handelt und auch nicht davon gesprochen werden kann, dass er Zugang zu der Kommunikation erhält. Demnach stehen die Vorgaben des Stored Communications Act dem Filtereinsatz nicht entgegen.

cc) Ausnahmen, 18 U.S.C. § 2701 (c) (1) und § 2701 (c) (2)

Wäre ein Rechtsverstoß zu bejahen, so könnte hier einer der in 18 U.S.C. § 2701 (c) normierten Ausnahmetatbestände eingreifen. Eine Ausnahme vom Verbot des 18 U.S.C. § 2701 (a) (1) liegt nach 18 U.S.C. § 2701 (c) vor, wenn derjenige, der die in (a) genannten Handlungen vornimmt, durch die Person oder den Rechtsträger dazu autorisiert wurde, der die

[1337] vgl.: 1. Kap. Teil 2 A. II.
[1338] vgl.: 1. Kap. Teil 2 A. II.
[1339] vgl.: 1. Kap. Teil 2 A. II.
[1340] vgl.: 1. Kap. Teil 2 A. II.
[1341] vgl.: 1. Kap. Teil 2 A. II.

elektronische Kommunikation als Leistung anbietet, 18 U.S.C. § 2701 (c) (1) oder wenn der Nutzer ihn in Bezug auf eine Kommunikation autorisiert hat, die für ihn bestimmt ist, 18 U.S.C. § 2701 (c) (2).

Aus der Ausnahme nach 18 U.S.C. § 2701 (c) (1) resultiert eine nahezu vollständige Immunität des Diensteanbieters, der auf Nachrichten zugreift, die in seinem System gespeichert sind.[1342] Als Provider in diesem Sinn ist auch der Arbeitgeber anzusehen, der seinen Angestellten die Möglichkeit gibt, über das Firmennetz elektronisch zu kommunizieren.[1343]

Im Übrigen kann sich der Provider oder Arbeitgeber durch den intendierten Empfänger der Kommunikation dazu autorisieren lassen, die eingehenden Emails durch ein Filterprogramm auf werbetypische Merkmale zu untersuchen, indem er eine entsprechende Bestimmung in den Vertrag aufnimmt, 18 U.S.C. § 2701 (c) (2).

dd) Zwischenergebnis

Der Filtereinsatz ist nicht nach Maßgabe der 18 U.S.C. §§ 2701 ff. unzulässig.

c) Zwischenergebnis

Weder aus den Vorschriften des Wiretap Act, 18 U.S.C. §§ 2510 ff., noch aus denjenigen des Stored Communications Act, 18 U.S.C. §§ 2701 ff. ergibt sich die Unzulässigkeit des Einsatzes der Filtersoftware.

2. Weitere Vorschriften zum Schutz der Privatsphäre

Fraglich ist, ob dem Schutz der Privatsphäre dienende Vorschriften dem Filtereinsatz entgegenstehen. In den USA finden sich in diesem Bereich verschiedene sektorale Ansätze.[1344]

Dem Schutz der Privatsphäre dient etwa der Fair Credit Reporting Act, 15 U.S.C. §§ 1681 ff. Das Gesetz verpflichtet so genannte „consumer reporting agencies", ein Verfahren anzuwenden, das die größtmögliche Sicherheit der erstellten „consumer reports" sicherstellt, vgl. 15 U.S.C. § 1681. Voraussetzung der Anwendbarkeit des Gesetzes wäre hier damit, dass es sich bei denjenigen Personen, welche die Filtersoftware einsetzen um „consumer reporting agencies" handelt, vgl. 15 U.S.C. § 1681 b. Hierunter fällt jede Person, die sich regelmäßig damit beschäftigt, Informationen über Verbraucher zu sammeln, mit dem Ziel, so genannte „comsumer reports" für dritte Personen zusammenzustellen, 15 U.S.C. § 1681 a (f).[1345]

[1342] Bohach v. City of Reno, 932 F. Supp., S. 1235, United States District Court of Nevada, (1996); Fraser v. Nationwide Life Insturance Co., 352 F. 3d, S. 113 f., United States Court of Appeals, Third Circuit, (2003); United States v. Councilman, 418 F.3d, S. 81 f., United States Court of Appeals, First Circuit, (2005); *Fishman*, 72 Geo. Wash. L. Rev., S. 1529

[1343] Bohach v. City of Reno, 932 F. Supp., S. 1236, United States District Court of Nevada, (1996)

[1344] *Cody*, 48 Cath. U.L. Rev. (1999), S. 1199 ff.; *Fromholz*, 15 Berkeley Tech. L. J., S. 461 ff., 472; *Gubitz*, 39 New Eng. L. Rev., S. 431 ff., 446; *Peeters*, MMR 2005, S. 417; *Reidenberg*, 44 Fed. Comm. L. J., S. 195 ff., S. 209; *Solove/Hoofnagle*, 2006 U. Ill. L. Rev., S. 357 ff., 357

[1345] Porter v. Perkins Children´s Services, 355 F. Supp., S. 174 ff., United States District Court, S. D. New York, (1973); Todd v. Associated Credit Bureau Services, Inc., 451 F. Supp., S. 447 ff., United States District Court, E.C. Pennsylvania (1977), der Antrag auf writ of certiorari wurde zurückgewiesen, 439 U.S., S. 1068, 99 S. Ct., S. 834, Supreme Court of the United States, (1979); Alexander v. Moore & Associates, Inc., 553 F.Supp., S. 948 ff., United States District Court, D. Hawai'i, (1982); *Seep*, 101 A.L.R. Fed., S. 751 ff.; *Solove/Hoofnagle*, 2006 U. Ill. L. Rev., S. 357 ff., 364

Diesem Zweck dient der Filtereinsatz ersichtlich nicht. Insofern findet der FCRA keine Anwendung.

Fraglich ist, ob der Privacy Act[1346] Anwendung findet. Allerdings betrifft das Gesetz lediglich den Umgang mit persönlichen Informationen durch Behörden der Bundesverwaltung, 5 U.S.C. §§ 552 a (b), (a) (1), 552 (f) (1). Deshalb findet der Privacy Act hier keine Anwendung.

Weitere bereichsspezifische Vorschriften greifen jeweils deshalb nicht ein, weil die vorliegende Situation nicht in den geregelten Sektor fällt. So findet der Gramm-Leach-Bliley Act nur auf Finanzinstitutionen Anwendung, vgl. 15 U.S.C. § 6801 (a). Der Drivers' Privacy Protection Act, 18 U.S.C. § 2721 ff. betrifft lediglich die Weitergabe bestimmter Daten durch das Department of Motor Vehicles, 18 U.S.C. § 2721 (a). Schließlich verbietet der Video Privacy Protection Act die Bekanntgabe persönlicher Informationen, insbesondere Titel einer ausgeliehenen oder gekauften Videokassette, 18 U.S.C. § 2710 (b).

Im Ergebnis greift hier damit keine die Privatsphäre schützende Vorschrift ein.

3. CAN-SPAM Act

Auch der CAN-SPAM Act zwingt Provider nicht dazu, sämtliche danach zulässigen Nachrichten zuzustellen. Der Gesetzgeber wollte mit den Vorgaben des CAN-SPAM Act nicht die Rechtmäßigkeit der Bemühungen von Providern regeln, Emails zu filtern oder zu blockieren, die über ihr System geleitet werden.[1347] Deswegen wurde in 15 U.S.C. § 7707 (c) eine Regelung dahingehend aufgenommen, dass der CAN-SPAM Act keinen Einfluss auf die Rechtmäßigkeit oder Unrechtmäßigkeit von Grundsätzen haben, die der Provider hinsichtlich der Übermittlung, dem Routing,[1348] Weiterleiten, Befördern oder Speichern einer bestimmten Art von Nachrichten annimmt, implementiert oder durchsetzt. Die Tatsache, dass eine Email nach Maßgabe des CAN-SPAM Act zulässig oder aber unzulässig ist, soll demnach keinen Einfluss darauf entfalten, ob der Provider oder ein Unternehmen, das über ein eigenes Netzwerk verfügt, diese blockieren, löschen oder umleiten darf. Demnach werden die genannten Personen bzw. Rechtsträger durch den CAN-SPAM Act nicht daran gehindert, eigene Grundsätze darüber aufzustellen, welche Arten von Emails sie annehmen und an ihre Kunden bzw. Angestellten weiterleiten und welche sie zurückweisen oder löschen.[1349]

4. Ergebnis

Im Ergebnis lässt sich festhalten, dass der Einsatz von Filtersoftware mit der Folge einer Überprüfung des Headers und Inhalts eingehender Emails auf werbetypische Merkmale nach dem einfachen US-amerikanischen Bundesrecht rechtlich zulässig ist. Auch das Blockieren, Löschen, Markieren und Umleiten elektronischer Nachrichten ist nach Maßgabe des einfachen Rechts grundsätzlich rechtmäßig.

[1346] vgl.: Anhang IV
[1347] S. REP. 108-102, 2004 U.S.C.C.A.N., S. 2348 ff., 2366
[1348] zum Begriff: 1. Kap. Teil 1 B. II. 4.
[1349] vgl. 15 U.S.C. § 7707 (c); vgl. auch: White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F.3d, S. 366 ff., United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil eingereichte Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., 1039, Supreme Court of the United States, (2006)

II. Einzelstaatliches Recht

Fraglich ist, ob sich aus einzelstaatlichem Recht eine andere Beurteilung ergibt.

1. Gesetzliche Vorschriften zum Schutz der Privatsphäre

Auch die Bundesstaaten haben Vorschriften zum Schutz gegen das Überwachen der Email-Kommunikation erlassen.[1350] Allerdings sind die Regelungen nicht einheitlich. Sie unterscheiden sich insbesondere im Hinblick auf die Frage, ob es ausreichend ist, wenn lediglich eine Kommunikationspartei den Überwachungsmaßnahmen zustimmt[1351] oder ob beide bzw. alle Beteiligten[1352] einwilligen müssen. Dabei ist ausweislich der Rechtsprechung davon auszugehen, dass die Staaten zwar Gesetze erlassen dürfen, die dem Bundesgesetz ähnlich sind oder auch strengere Vorschriften, allerdings nicht weniger strenge Regelungen.[1353] Demnach besteht also mindestens der bereits beschriebene Standard, den das Bundesrecht festlegt. Dieser soll nachfolgend anhand verfassungsrechtlicher und völkerrechtlicher Vorschriften überprüft und zum Vergleichsmaßstab gemacht werden, da ein Eingehen auf die verschiedenen Gesetze sämtlicher Bundesstaaten den Rahmen dieser Arbeit sprengen würde und allein aufgrund der Darstellung eines einzelnen bundesstaatlichen Rechtssystems kein Rückschluss auf die Rechtslage in den anderen Staaten möglich ist.

2. Deliktsrecht

Der Filtereinsatz könnte die Voraussetzung eines durch das Common Law herausgebildeten deliktischen Tatbestands erfüllen.

a) „tort of intrusion of seclusion“

Durch die fraglichen Maßnahmen könnte eine als „tort of intrusion of seclusion“ bezeichnete unerlaubte Handlung begangen werden. Der Tatbestand dieses Delikts setzt dabei voraus, dass in die räumliche oder sonstige Privatsphäre eines anderen in grob anstößiger Weise eingedrungen wird.[1354]
Zu überprüfen ist, ob in der fraglichen Maßnahme ein vorsätzliches Eindringen in die Zurückgezogenheit der betroffenen Person zu sehen (aa) und die zu beurteilende Handlung

---

[1350] vgl. etwa: California Penal Code, § 632.5; General Laws of Massachusetts, Chapter 272, § 99; Minnesota Statutes, § 626 A.02; Montana Code Annotated, § 45-8-213; Code of Virginia, § 19.2-62, alle abrufbar unter: http://www.ncsl.org/programs/lis/cip/surveillance.htm (letzter Abruf: 29.04.2007)
[1351] Minnesota Statutes, § 626 A.02; Code of Virginia, § 19.2-62, alle abrufbar unter: http://www.ncsl.org/programs/lis/cip/surveillance.htm (letzter Abruf: 29.04.2007)
[1352] California Penal Code, § 632.5; General Laws of Massachusetts, Chapter 272, § 99; Montana Code Annotated, § 45-8-213, alle abrufbar unter: http://www.ncsl.org/programs/lis/cip/surveillance.htm (letzter Abruf: 29.04.2007)
[1353] State of Florida v. McGillicuddy, 342 So.2d, S. 567, District Court of Appeals of Florida, Second District, (1977); State of Florida v. Rivers, 660 So.2d, S. 1361, Supreme Court of Florida, (1995); State of Florida v. Otte, 887 So.2d, S. 1186, Supreme Court of Florida, (2004)
[1354] Bourke v. Nissan Motor Corp., No. B068705, Court of Appeal of the State of California, Second Appellate District, Division Five, (1993); Smyth v. Pillsbury Co., C.A. No. 95-5712, United States District Court, Eastern District of Pennsylvania, (1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999); Fischer v. Mt. Olive Lutheran Church, No. 01-C-0158-C, United States District Court, Western District of Wisconsin, (2002); Muick v. Glenayre Electronics, No. 00-3299, United States Court of Appeals, Seventh Circuit, (2002); *Kierkegaard*, Computer Law & Security Report 2005, S. 226 ff., 234; *Zekoll/Felming* in Clark/Ansay, Introduction to the Law of the United States, S. 205

aus dem Blickwinkel eines objektiven Beobachters als höchst offensiv zu qualifizieren ist (bb).[1355]

aa) Vorsätzliches Eindringen in die Zurückgezogenheit

Es ist bereits fraglich, ob in der Überprüfung der Email-Korrespondenz ein Eindringen in das Alleinsein bzw. die Zurückgezogenheit der betroffenen Person liegen kann. Grundvoraussetzung ist, dass derjenige, dessen Privatsphäre betroffen ist, berechtigterweise davon ausgehen kann, dass ihm eine solche zukommt.[1356]

Hierbei legt die Rechtsprechung strenge Maßstäbe an.
So wurde entschieden, dass einem Arbeitnehmer, der freiwillig per Email über das betriebliche Netz seines Arbeitgebers kommuniziert keine berechtigte Erwartung auf Privatsphäre gegenüber dem Arbeitgeber zusteht.[1357] Hat der Arbeitgeber sogar angekündigt, die dienstliche Email-Kommunikation zu kontrollieren, so besteht erst Recht keine berechtigte Erwartung der Privatheit.[1358] Diese fehlt im Verhältnis von Arbeitgeber und Arbeitnehmer auch dann, wenn Email-Kommunikation betroffen ist, die sich in einem privaten, passwortgeschützten Ordner des Arbeitnehmers im vom Arbeitgeber zur Verfügung gestellten Netz befindet.[1359] Die genannten Grundsätze werden von der Rechtsprechung damit begründet, dass Emails stets über das Firmennetzwerk übertragen werden und insofern immer an irgendeinem Punkt während der Übertragung dem Zugriff Dritter ausgesetzt sind.[1360] Unter diesen Umständen sei trotz der Tatsache, dass der Betroffene die Emails nach dem Lesen in persönlichen, passwortgeschützten Ordnern speichere, nicht von einer berechtigten Erwartung dahingehend auszugehen, dass der Arbeitgeber nicht Einblick in die Emails nehmen.[1361] Auch außerhalb von Arbeitsverhältnissen wird davon ausgegangen, dass bei der Email-Kommunikation eine geringere Erwartung hinsichtlich der Privatheit der Kommunikation besteht, als etwa bei Gesprächen unter Anwesenden oder der Telefonkommunikation, weil Emails gespeichert und deshalb abgerufen werden können und die nie völlig auszuschließende Möglichkeit besteht, dass etwa ein Angestellter des Providers sich Zugang zu der

---

[1355] so einerseits das Restatement (2nd) of Torts, Abschnitt 652B: *„One who intentionally intrudes physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."* vgl.: Bourke v. Nissan Motor Corp., No. B068705, Court of Appeal of the State of California, Second Appellate District, Division Five, (1993); Smyth v. Pillsbury Co., C.A. No. 95-5712, United States District Court, Eastern District of Pennsylvania, (1996); Muick v. Glenayre Electronics, No. 00-3299, United States Court of Appeals, Seventh Circuit, (2002); Fischer v. Mt. Olive Lutheran Church, No. 01-C-0158-C, United States District Court, Western District of Wisconsin, (2002); *Kierkegaard*, Computer Law & Security Report 2005, S. 226 ff., 234

[1356] Die Gerichte verwenden die Begriffe "legitimate expectation of privacy" oder "reasonable expectation of privacy", vgl.: Bourke v. Nissan Motor Corp., No. B068705, Court of Appeal of the State of California, Second Appellate District, Division Five, (1993); Smyth v. Pillsbury Co., C.A. No. 95-5712, United States District Court, Eastern District of Pennsylvania, (1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999); Garrity v. John Hancock Mutual Life Insurance Co., C.A. No. 00-12143-RWZ, United States District Court, District of Massachusetts, (2002); Muick v. Glenayre Electronics, No. 00-3299, United States Court of Appeals for the Seventh Circuit, (2002); hinsichtlich des Schutzes der Privatsphäre gegen Tätigkeiten staatlicher Behörden durch den Vierten Verfassungszusatz: Katz v. United States, 389 U.S., S. 347 ff., 88 S.Ct., S. 507 ff., United States Supreme Court, (1967)

[1357] Smyth v. Pillsbury Co., C.A. No. 95-5712, United States District Court, Eastern District of Pennsylvania, (1996)

[1358] Muick v. Glenayre Electronics, No. 00-3299, United States Court of Appeals for the Seventh Circuit, (2002)

[1359] McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999)

[1360] McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999)

[1361] McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999)

Kommunikation verschafft.[1362] Die Erwartung hinsichtlich der Privatsphäre ist selbst dann eingeschränkt, wenn das Unternehmen die Vertraulichkeit der Kommunikation vertraglich zugesichert hat.[1363] Denn auch wenn der Provider eine entgegenstehende Geschäftspolitik verfolgt, besteht dennoch die Gefahr, dass entweder der Empfänger die Email weiterverbreitet oder aber ein Angestellter der Providers trotz gegenteiliger Anweisung die Email liest.[1364]

Im Bereich der Email-Kommunikation wird eine berechtigte Erwartung der Privatheit lediglich dahingehend angenommen, dass staatliche Behörden, insbesondere die Polizei nicht ohne berechtigten Anlaß oder Durchsuchungsbefehl Einblick in die Kommunikation nehmen.[1365] Gegenüber Privaten besteht diese Erwartung hingegen nicht.[1366] Weder gegenüber dem Email-Provider, noch gegenüber dem Arbeitgeber ergibt sich damit eine berechtigte Erwartung der Privatheit der Email-Korrespondenz.

Zusammenfassend lässt sich somit festhalten, dass weder die Überprüfung des Inhaltes, noch die der Headerinformationen ein Eindringen in das Alleinsein bzw. die Zurückgezogenheit der betroffenen Person darstellt und damit keine unerlaubte Handlung der „tort of intrusion" gegeben ist.

bb) Beurteilung des Eindringens durch einen objektiven Beobachter als höchst offensiv

Soweit die sonstigen Voraussetzungen der unerlaubten Handlung vorliegen würden, wäre dennoch zweifelhaft, ob ein objektiver Beobachter das Eindringen in die Privatsphäre durch ein rein automatisiertes Überwachen der Email-Korrespondenz mittels elektronischer Filter als höchst offensiv empfinden würde. Letztlich gilt hier nichts anderes, als im deutschen Recht. Es wurde dargestellt, dass die bloße automatisierte Überwachung nicht zu der Gefahr führt, dass die betroffenen Personen identifiziert werden können.[1367] Insofern würde ein objektiver Beobachter die Kontrolle des Inhalts und der Headerinformationen durch den elektronischen Email-Filter nicht als höchst offensiv ansehen.[1368] Dies wurde auch durch die Rechtsprechung bestätigt, die feststellte, dass die inhaltliche Email-Überwachung keine Maßnahme darstellt, die eine normale Person als höchst offensiv empfinden würde.[1369]

[1362] U.S. v. Maxwell, 45 M.J., S. 417, U.S. Court of Appeals for the Armed Forces, (1996) in Bezug auf den Vierten Verfassungszusatz; *Ko*, 22 J. Marshall J. Computer & Info. L., S. 495

[1363] U.S. v. Maxwell, 45 M.J., S. 417, U.S. Court of Appeals for the Armed Forces, (1996) in Bezug auf den Vierten Verfassungszusatz; Ko, 22 J. Marshall J. Computer & Info. L., S. 495

[1364] Smyth v. Pillsbury Co., C.A. No. 95-5712, United States District Court, Eastern District of Pennsylvania, (1996); Muick v. Glenayre Electronics, No. 00-3299, United States Court of Appeals for the Seventh Circuit, (2002); McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999); U.S. v. Maxwell, 45 M.J., S. 417 f., U.S. Court of Appeals for the Armed Forces, (1996) in Bezug auf den Vierten Verfassungszusatz

[1365] U.S. v. Maxwell, 45 M.J., S. 418, U.S. Court of Appeals for the Armed Forces, (1996) in Bezug auf den Vierten Verfassungszusatz; ebenso hinsichtlich der Telefonkommunikation: United States v. Sullivan, 42 M.J., S. 364, United States Court of Appeals for the Armed Forces, (1995)

[1366] U.S. v. Maxwell, 45 M.J., S. 418, U.S. Court of Appeals for the Armed Forces, (1996) in Bezug auf den Vierten Verfassungszusatz; ebenso hinsichtlich der Telefonkommunikation: United States v. Sullivan, 42 M.J., S. 364, United States Court of Appeals for the Armed Forces, (1995)

[1367] vgl.: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (b)

[1368] ebenso: *Solove*, 53 Stan. L. Rev., S. 1432 f.; nicht als höchst offensiv angesehen wurden beispielsweise angesehen: Zusammenstellung und Weitergabe von Versicherungsdaten, vgl. Tureen v. Equifax, Inc., 571 F.2d, S. 411, United States Court of Appeals, Eighth Circuit, (1978); der Erhalt einer nicht im Telefonbuch aufgeführten Telefonnummer, vgl. Seaphus v. Lilly, 691 F. Supp., S. 132, United States District Court, N.D. Illinois, Eastern Division, (1988)

[1369] Smyth v. Pillsbury Co., C.A. No. 95-5712, United States District Court, Eastern District of Pennsylvania, (1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999)

Insbesondere gilt das nach Auffassung der Gerichte dann, wenn ein berechtigtes Interesse desjenigen an der Überwachung besteht, der diese vornimmt.[1370]

cc) Zwischenergebnis

Derjenige, der Filtersoftware einsetzt, begeht nicht die unerlaubte Handlung der „tort of intrusion" und zwar einerseits deshalb, weil in aller Regel keine berechtigte Erwartung der Privatsphäre besteht, andererseits ist der Eingriff auch so minimal, dass er nicht als höchst offensiv anzusehen ist.

b) Beeinträchtigung vertraglicher Beziehungen Dritter

Denkbar ist, dass durch das Löschen, Blockieren, Umleiten oder Markieren positiv gescannter Emails die deliktische Handlung der Beeinträchtigung der vertraglichen Beziehungen Dritter[1371] verwirklicht wird.[1372] Dies könnte der Fall sein, wenn aufgrund der Filtermaßnahmen Geschäftsemails nicht zugestellt oder wegen einer entsprechenden Markierung als Spam oder einem Einstellen in den Quarantäne- Ordner vom Empfänger nicht gelesen, sondern sofort gelöscht werden. Voraussetzung des Delikts ist (1) die Existenz eines wirksamen Vertrages oder einer zu erwartenden zukünftigen Geschäftsbeziehung zwischen dem Betroffenen und einem Dritten, (2) Kenntnis des Anspruchsgegners von der Existenz dieser Beziehung bzw. des Vertrages, (3) eine vorsätzliche Handlung, die darauf ausgerichtet ist, die Vertrags- oder Geschäftsbeziehung zu zerrütten, (4) der Eintritt der Zerrüttung der

[1370] Smyth v. Pillsbury Co., C.A. No. 95-5712, United States District Court, Eastern District of Pennsylvania, (1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, Court of Appeals of Texas, Dallas, (1999)

[1371] Das Delikt wird als „tortious interference with contract" oder „tortious interference with contractual relations" bezeichnet; teilweise wird auch angenommen, dass es ein einheitliches "tort of interference" gibt, das zwei Tatbestände umfasst und zwar (1) "interference with contract" und (2) "interference with prospective business relations", vgl. *Varadarajan*, The Yale Law Journal, S. 736; das vom American Law Institute herausgegebene und von den Gerichten anerkannte und als Leitlinie verwendete Restatement (2d) of Torts § 766 A lautet: *„One who intentionally and improperly interferes with the performance of a contract (except a contract to marry) between another and a third person, by preventing the other from performing the contract or causing his performance to be more expensive or burdensome, is subject to liability to the other for the pecuniary loss resulting to him."*; Restatement (2d) of Torts, § 766 B lautet: *„One who intentionally and improperly interferes with another´s prospective contractual relation (except a contract to marry) is subject to liability to the other for the pecuniary harm resulting form loss of the benefits of the relation, whether the interference consists of (a) inducing or otherwise causing a third person not to enter into or continue the prospective relation or (b) preventing the other from acquiring or continuing the prospective relation."* Rspr. zum Delikt der tortious inteference: Leo Spear Contruction Company v. Fidelity & Casualty Company of New York, 446 F.2d, S. 439 ff., United States Court of Appeals, Second Circuit, (1971); Thompson v. Allstate Insurance Company, 476 F.2d, S. 746 ff., United States Court of Appeals, Fifth Circuit (1973); Kademos v. Equitable Life Assurance Society of the United States, 513 F.2d, S. 1073 ff., United States Court of Appeals, Third Cicuit, (1975); Morton Buildings of Nebraska v. Morton Buildings, Inc., 531 F.2d, S. 910 ff., United States Court of Appeals, Eighth Circuit, (1976)

[1372] Beispielsweise verklagte White Buffalo, ein Online- Dating- Service, der für seine Dienste mittels Email werben wollte, die Universität von Texas, die diese Nachrichten blockierte und stützte sich hierbei unter anderem darauf, dass hierin das Delikt „tortious interference with contract" zu sehen sei, vgl. White Buffalo Ventures v. University of Texas at Austin, 420 F.3d, S. 366 ff. , United States Court of Appeals, Fifth Circuit, (2004), das Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006); Exactis, ein Versender von erwünschten Marketing-Emails verklagte den damaligen Betreiber der RBL, das Mail Abuse Prevention System unter anderem mit der Argumentation, MAPS würde durch die Drohung, Exactis auf die RBL-Liste aufzunehmen, vorsätzlich in die mit Kunden bestehenden Vertragsbeziehungen eingreifen, vgl. Exactix.com, Inc. v. Mail Abuse Prevention System, LLC, No. 1:00cv2250, United States District Court for the District of Colorado, (2000)

Vertrags- oder Geschäftsbeziehung und (5) ein Schaden des Betroffenen, der unmittelbar durch die Handlung des Anspruchsgegners verursacht wird.[1373]

Die erste Voraussetzung, nämlich die Existenz eines wirksamen Vertrages oder einer zu erwartenden zukünftigen Geschäftsbeziehung zwischen dem Betroffenen und einem Dritten wird grundsätzlich vorliegen. Dies ist einerseits dann der Fall, wenn Werbung im Rahmen eines Verhältnisses versandt wird, das bereits auf eine zukünftige Geschäftsbeziehung hoffen lässt. Andererseits ist denkbar, dass das Versenden der Emails in Erfüllung eines bestehenden Vertragsverhältnisses erfolgt. Insbesondere Informationsdienste und Email-Marketinganbieter handeln auf Grundlage vertraglicher Beziehungen, wenn sie Emails an Dritte versenden.[1374]

Auch wird dem Email-Service-Provider, der Emails von kommerziellen Versendern blockiert, löscht, umleitet oder markiert, bewusst sein, dass unter Umständen derartige Verträge oder zu erwartende Geschäftsbeziehungen existieren, so dass auch die zweite Voraussetzung grundsätzlich vorliegt.

Daneben ist allerdings erforderlich, dass die vorsätzliche Handlung darauf gerichtet ist, die Vertrags- oder Geschäftsbeziehung zu zerrütten.
Am Vorliegen dieser Voraussetzung könnten hier Zweifel bestehen. Denn das Verhalten des Email-Service-Providers bzw. des jeweiligen Unternehmens, das den Spam- Filter einsetzt, hat nicht zum Ziel, Vertrags- oder Geschäftsbeziehungen zu beeinträchtigen. Vielmehr ist es darauf gerichtet, eigene Kunden und Ressourcen zu schützen und bewirkt nur als etwaige Nebenfolge die Zerrüttung fremder Vertrags- und Geschäftsbeziehungen. Vorsatz setzt voraus, dass der Handelnde eine bestimmte Konsequenz entweder bezweckt oder doch als Konsequenz seines Tuns voraussieht.[1375] Dem Provider wird allerdings durchaus bewusst sein, dass die Möglichkeit besteht, dass er durch sein Verhalten, fremde Geschäfts- und Vertragsbeziehungen beeinträchtigt. Ihm wird somit bewusst sein, dass er möglicherweise in fremde Geschäftsbeziehungen eingreift.[1376] Bei Einsatz des Filters werden die Email-Service-Provider und Unternehmen in der Regel davon ausgehen, dass hiervon fremde Vertragsbeziehungen betroffen sind. Somit liegt eine vorsätzliche Zerrüttung vor.

Allerdings muss die fragliche Handlung unberechtigt sein.
Restatement 2d of torts § 767 nennt Faktoren, die helfen sollen, festzustellen, ob die Handlung unberechtigt ist oder nicht. Danach sind bei der Frage danach, ob derjenige, der vorsätzlich in eine fremde Vertragsbeziehung eingreift, unberechtigt handelt, (a) die Verhaltensweise des Handelnden, (b) das Motiv des Handelnden, (c) das Interesse desjenigen,

---

[1373] Greenberg v. Hollywood Turf Club, 86 Cal. Rptr., S. 885 ff., Court of Appeal, Second District, Division 5, California, (1970); O´Fallon Development Co. v. City of O´Fallon, 43 Ill.App.3d, S.348 ff., Appellate Court of Illionois, Fifth District, (1976); Edwards v. Anaconda Company, 565 P.2d, S. 190 ff., Court of Appeals of Arizona, Division 2, (1977); American Private Line Services v. Eastern Microwave, 980 F. 2d, S. 36, United States Court of Appeals, First Circuit (1992); Exactis v. Mail Abuse Prevention System, No. 1:00cv2250, United States District Court for the District of Colorado, (2000); Media3 Technologies v. Mail Abuse Prevention System, 00-CV-12524-MEL, United States District Court, District of Massachusetts, (2001)

[1374] Exactix.com v. Mail Abuse Prevention System, No. 1:00cv2250, United States District Court for the District of Colorado, (2000)

[1375] vgl.: Restatement (2d) of Torts § 8 A: *„The word „intent" is used throughout the Restatement of this Subject to denote that the actor desires to cause consequences of his act, or that he believes that the consequences are substantially certain to result from it."*

[1376] In der Sache Exactis v. Mail Abuse Prevention System sah das Gericht das vorsätzliche Verhalten mit dem Ziel der Zerrüttung fremder Geschäftsbeziehungen als gegeben an, da eine Angestellte von MAPS geäußert hatte, die Vertragsbeziehungen zwischen Exactis und seinen Kunden sei seine Sache, vgl. Exactix.com v. Mail Abuse Prevention System, No. 1:00cv2250, United States District Court for the District of Colorado, (2000).

der vom Handelnden beeinträchtigt wird, (d) die Interessen, die der Handelnde zu fördern versucht, (e) das öffentliche Interesse daran, die Freiheit des Handelnden oder aber die vertraglichen Interessen des anderen zu schützen (f), die Nähe oder Entfernung des Verhaltens des Handelnden zum Eingriff und (g) die Beziehungen zwischen den Parteien zu berücksichtigen.[1377]

Das Motiv des Einsatzes von Spam-Filtern besteht darin, eigene Ressourcen, wie Speicherkapazitäten und Arbeitskraft zu schützen und daneben den Kunden die Belästigung durch unerwünschte Werbe- Emails zu ersparen. Zwar mag derjenige, der durch den Einsatz des Filters beeinträchtigt wird, ein Interesse an der Fortsetzung seiner Tätigkeit haben. Allerdings ist die Tatsache zu beachten, dass -wie bereits oben erwähnt-[1378] die Versendung von Spammails ein extrem kostengünstiges Werbemittel für den Versender darstellt, jedoch auf Seiten der Empfänger und deren Provider Kosten anfallen, so etwa für Ressourcen, wie Speicherplatz, Arbeitskraft und Verbindungskosten. Daneben resultieren die Nachrichten in einer Netzbelastung, was entsprechende Nachteile für die legitimen Nutzer mit sich bringt und mittlerweile zu einem Vertrauensverlust hinsichtlich des Kommunikationsmediums Email geführt hat.[1379]
Im Hinblick auf die Frage, ob hier das öffentliche Interesse an der Handlungsfreiheit oder aber das am Erhalt der vertraglichen Beziehung im Vordergrund steht, ist zwar zu berücksichtigen, dass es nach Erlass des CAN-SPAM Act -wie oben ausgeführt- grundsätzlich zulässig ist, Werbe-Emails zu versenden, falls nicht der Empfänger seinen Widerspruch erklärt hat. Um es jedoch den betroffenen Providern und Unternehmern zu ermöglichen, sich vor der Vielzahl an eingehenden Spammails zu schützen, liegt es im öffentlichen Interesse, die Freiheit des Einzelnen in diesem Bereich nicht dahingehend einzuschränken, dass dies rechtlich nicht mehr möglich ist. Die vertraglichen Beziehungen der Versender von Spammails müssen gegenüber diesem Interesse auch deshalb zurückstehen, weil keine besondere Nähe desjenigen, der die Emails ausfiltert, zum Eingriff in die Vertragsbeziehung besteht, denn letztlich verfolgt er mit dem Einsatz der Filter eigene Ziele. Auch ist kein Grund für Provider oder private Unternehmen ersichtlich, kostenlos ihre Kapazitäten zur Verfügung zu stellen, um den Versendern von Spammails das Betreiben ihrer Geschäfte zu ermöglichen. Hierbei ist auch zu berücksichtigen, dass, wie oben ausgeführt wurde, der CAN-SPAM Act die Frage der Zulässigkeit von Filtermaßnahmen durch Provider nicht regulieren wollte.[1380]

Sind durch die Maßnahme ausnahmsweise legitime Emails betroffen, so stellt sich die Frage, ob ein durch den Filtereinsatz bedingtes Blockieren oder Löschen solcher Nachrichten als Beeinträchtigung vertraglicher oder zu erwartender geschäftlicher Beziehungen Dritter angesehen werden kann. Hierfür wird es allerdings nicht ausreichen, dass dem Betroffenen eine von mehreren Kommunikationsmöglichkeiten genommen wird.
Im Übrigen darf -angesichts der Tatsache, dass mittlerweile Kenntnis davon besteht, dass sämtliche Provider Filtersoftware einsetzen- erwartet werden, dass Kommunikationspartner, die auf die Zustellung einer bestimmten Email angewiesen sind, geeignete Sicherheitsvorkehrungen treffen, die gewährleisten, dass die fragliche Nachricht auch zugeht.

[1377] Restatement (2d) of Torts § 767 lautet: *„In determining whether an actor´s conduct in intentionally interfering with a contract or a prospective contractual relationship of another is improper or not, consideration is given to the following factors: (a) the nature of the actor´s conduct, (b) the actor´s motive, (c) the interests of the other with which the actor´s conduct interferes, (d) the interests sought to be advanced by the actor, (e) the social interests in protecting the freedom of action of the actor and the contractual interests of the other, (f) the proximity or remoteness of the actor´s conduct to the interference and (g) the relations between the parties.“*
[1378] vgl.: 1. Kap. Teil 1 B. II. 4.
[1379] *Spindler/Ernst*, CR 2004, S. 437; 15 U.S.C. § 7701 (a) (4)
[1380] vgl.: 3. Kap. Teil 2 A. I. 3.

Einerseits besteht hier die Möglichkeit, sich durch den Adressaten auf eine weiße Liste setzen zu lassen, andererseits kann eine Funktion im eigenen Email-Programm aktiviert werden, die den Zugang der Nachricht bestätigt.
Trifft ein Dritter keinerlei derartiger Vorkehrungen und kommt es deshalb aufgrund der unterbliebenen Zustellung einer Nachricht nicht zum Vertragsschluss bzw. dem Zustandekommen der Geschäftsbeziehung, so ist dennoch nicht davon auszugehen, dass der deliktische Tatbestand verwirklicht wird. Denn hier geht das Motiv des Handelnden nicht dahin, Vertragsbeziehungen Dritter zu beeinträchtigen. Im Übrigen dürfte es an einer Nähe des Verhaltens des Handelnden zum Eingriff in das Vertragsverhältnis fehlen, da erst das fahrlässige Verhalten des Geschädigten selbst die Zerrüttung der Vertrags- oder Geschäftsbeziehung letztendlich herbeiführt. Demnach ist die Handlung nicht unberechtigt.

Setzt ein Unternehmen, das über ein eigenes Netzwerk verfügt, Filtersoftware ein, so betrifft das hierdurch bewirkte Löschen oder Blockieren eingehender Emails grundsätzlich nicht vertragliche Beziehungen oder zu erwartende Geschäftsbeziehungen Dritter. Denn das Email-System soll durch die Angestellten beruflich genutzt werden, so dass Nachrichten, die möglicherweise durch den Spam-Filter aussortiert werden, in aller Regel die vertraglichen Beziehungen des den Filter nutzenden Unternehmens selbst betreffen.
Sind dennoch ausnahmsweise vertragliche Beziehungen oder zu erwartende geschäftliche Beziehungen Dritter durch die Filtermaßnahme tangiert, so handelt das Unternehmen dennoch nicht unberechtigt. Denn es ist zu berücksichtigen, dass durch die Filtermaßnahme das eigene System geschützt werden soll. Insofern ist nicht ersichtlich, wieso eine Verpflichtung bestehen soll, das firmeneigene Netzwerk Dritten zur Verfügung zu stellen, um Verträge mit Angestellten zu fördern. Der Filtereinsatz durch Unternehmen ist demnach nicht unberechtigt.

Somit kann derjenige, der den Einsatz der Filtersoftware veranlasst, selbst dann nicht auf Ersatz des dadurch entstandenen Schadens in Anspruch genommen werden, wenn aufgrund dieser Maßnahmen Verträge gekündigt werden oder aufgrund fehlender Informationen nicht zu Stande kommen.

c) „defamation“

Aus dem Blickwinkel desjenigen, der durch eine Markierung oder durch ein Einstellen durch ihn versandter Emails in einen Quarantäne-Ordner letztlich als Spammer bezeichnet wird, geht hiermit eine Herabwürdigung einher. Demnach könnte das fälschliche Markieren oder Einstellen von Nachrichten in einen solchen Ordner als „defamation“ im Sinne des US-amerikanischen Common Law zu qualifizieren sein. Hierunter wird die Verbreitung einer unrichtigen Meinung verstanden, die den Betroffenen schädigt.[1381] So sieht die Rechtsprechung die Aufnahme eines Unternehmens auf eine schwarze Liste als „defamation“

[1381] vgl. Restatement (2d) of Torts § 558: *“To create liability for defamation there must be: (a) a false and defamatory statement concerning another; (b) an unprivileged publication to a third party; (c) fault amounting at least to negligence on the part of the publisher; and (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication.”*; vgl. zur Rechtsprechung und der Bezugnahme auf § 558: Jimenez-Nieves v. United States, 682 F.2d., S. 6, United States Court of Appeals, First Circuit, (1982); St. John v. Town of Elletsville, 46 F. Supp. 2d, S. 848, United States District Court, S.D. Indiana, (1999); Chalal v. Northwest Med. Center, Inc., 147 F.Supp.2d, S. 1180, United States District Court, N.D. Alabama, (2000); Brown v. O´Bannon, 84 F.Supp. 2d, S. 1181, United States District Court, D. Colorado (2000); Flowers v. Carville, 292 F.Supp.2d, S. 1232, United States District Court, D. Nevada, (2003); Graziani v. Epic Data Corporation, 305 F.Supp. 2d, S. 1197 f., United States District Court, D. Colorado, (2004)

an, da damit die Aussage einhergehe, es handle sich bei dem betreffenden Unternehmen um einen Spammer.[1382]

Ähnliches könnte auch für das fälschliche Einsortieren einer Email in einen speziellen Quarantäne-Ordner oder für das Markieren der Nachricht als Spam gelten. Allerdings ist hiermit noch keine unwahre Tatsachenbehauptung in Bezug auf die Person des Absenders verbunden.
Es ist allgemein bekannt, dass Spamfilter nicht fehlerfrei funktionieren und die Möglichkeit besteht, dass legitime Emails von den Programmen fälschlicherweise als Spam eingeordnet werden. Wie dargestellt wurde,[1383] erteilen Email-Service-Provider auch stets entsprechende Hinweise. Insofern liegt weder in dem Markieren, noch in dem Umleiten der Nachricht in einen speziellen Quarantäne-Ordner eine Äußerung dahingehend, es handle sich bei dem Versender um einen Spammer.
Werden Nachrichten gelöscht oder blockiert, so wird es nicht nur an einer definitiven Aussage fehlen, sondern darüber hinaus auch an einer Entäußerung der Behauptung.

Der Tatbestand der „defamation" ist somit nicht verwirklicht.

d) Ergebnis

Der Filtereinsatz bedingt nicht die Verwirklichung eines deliktischen Tatbestands.

B. Verfassungs- und Völkerrecht

Es stellt sich die Frage, ob das US-amerikanische Verfassungsrecht oder völkerrechtliche Vorschriften einen Einfluss auf die Rechtslage ausüben, dergestalt, dass dem Gesetzgeber eine Verpflichtung zukommt, von der geltenden Rechtslage abweichende Vorschriften zu erlassen.

I. Verfassungsrecht

Eine solche Verpflichtung des US-amerikanischen Gesetzgebers könnte aus der Verfassung resultieren. Voraussetzung wäre, dass ein in durch die Verfassung geschütztes Grundrecht ein Tätigwerden erfordert.

Hinsichtlich des Scannens der Emails durch die Filtersoftware könnte hier das Recht auf Privatsphäre ein Tätigwerden des Gesetzgebers zum Schutz dieses Rechts verlangen mit dem Ziel Privatpersonen den Einsatz von Spamfiltern zu verbieten, die zu einer Überprüfung des Inhalts und der Headerinformationen eingehender Emails führen. Eine verfassungsrechtliche Bestimmung, die die Privatsphäre schützt, existiert im US-amerikanischem Recht grundsätzlich nicht. Allerdings statuierte das US-Supreme Court, dass das Recht auf Privatsphäre als Naturrecht in der Verfassung verankert sei.[1384] Das Recht, das sich gegen die Überwachung durch staatliche Behörden richtet, wird im vierten Verfassungszusatz

[1382] Exactis v. Mail Abuse Prevention System, No. 1:00cv2250, United States District Court for the District of Colorado (2000); Media3 Technologies v. Mail Abuse Prevention System, 00-CV-12524- MEL, United States Court for the District of Massachusetts, (2001)
[1383] vgl.: 2. Kap. Teil 2 A. I. 1. b) bb)
[1384] Griswold v. Connecticut, 381 U.S., S. 497 ff., Supreme Court of the United States, (1965); Roe v. Wade, 410 U.S., S. 113 ff., 93 S.Ct., S. 705 ff., Supreme Court of the United States; Katz v. United States, 389 U.S., 347 ff., 88 S. Ct., 507 ff., Supreme Court of the United States, (1967)

verankert.[1385] Vom vierten Verfassungszusatz ist dabei entgegen seines Wortlauts, der auf eine Durchsuchung abstellt, auch das Abhören bzw. Mitlesen von Kommunikation ohne physisches Eindringen in den Privatbereich des Betroffenen erfasst,[1386] da die Vorschrift generell die Privatsphäre vor dem Eindringen durch staatliche Behörden schützen soll.[1387] Der vierte Verfassungszusatz richtet sich jedoch nur gegen Aktivitäten staatlicher Behörden, nicht gegen die Handlungen Privater.[1388] Dem US-amerikanischen Gesetzgeber obliegen anders, als dies im deutschen Recht der Fall ist, keine Schutz- oder Leistungspflichten.[1389] Grundrechte sind nach der Rechtsprechung des Supreme Court rein negatorische Abwehrrechte.[1390] Nach US-amerikanischem Recht stellt die staatliche Duldung oder Hinnahme von privaten Akten noch nicht eine so genannte „state action", also eine staatliche Handlung dar, die notwendige Voraussetzung des Eingreifens von Grundrechtsgarantien ist.[1391] Demnach findet eine Gleichstellung staatlichen Unterlassens mit staatlichem Tätigwerden nicht statt.[1392] Folglich existieren keine unmittelbaren Verpflichtungen des US-amerikanischen Gesetzgebers, die ihn zu einer von der geltenden Rechtslage abweichenden Regelung im Hinblick auf die Überprüfung des Inhalts und der Headerinformationen durch Einsatz der Filtersoftware zwingen könnten. Hinzu kommt, dass gegenüber Providern keine berechtigte Erwartung der Privatheit besteht.[1393]

Etwas anderes könnte jedoch im Hinblick auf die Frage gelten, ob die Blockade, das Löschen, Umleiten oder Markieren eingehender Nachrichten zulässig ist. Das Grundrecht auf freie Meinungsäußerung könnte eine andere gesetzliche Regelung dieser Frage gebieten.[1394] Wie eben erwähnt stellen jedoch die Grundrechte im US-amerikanischen Recht rein negatorische Abwehrrechte dar. Eine bloße Duldung oder Hinnahme von privaten Akten ist demnach kein

---

[1385] Olmstead v. United States, 277 U.S., S. 438 ff., 48 S.Ct., S. 564 ff., Supreme Court of the United States, (1928); Goldman v. United States, 316 U.S., S. 129 ff., 62 S.Ct., S. 993 ff., Supreme Court of the United States, (1942); On Lee v. United States, 343 U.S., S. 747 ff., 72 S. Ct., S. 967 ff., Supreme Court of the United States, (1952); Silverman v. United States, 365 U.S., S. 505 ff., 81 S. Ct., S. 679 ff., Supreme Court of the United States, (1961); Wong Sun v. United States, 371 U.S., S. 471 ff., 83 S.Ct., S. 407 ff., Supreme Court of the United States, (1963); der vierte Verfassungszusatz lautet: *„The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

[1386] Wong Sun v. United States, 371 U.S., S. 471 ff., 83 S. Ct., S. 407 ff., Supreme Court of the United States, (1963); Berger v. State of N.Y., 388 U.S., S. 51, 87 S. Ct., S. 1880, Supreme Court of the United States, (1967); Alderman v. United States, 394 U.S., S. 176, 89 S. Ct., S. 968, Supreme Court of the United States, (1969); anders noch: Olmstead v. United States, 277 U.S., S. 438 ff., 48 S.Ct., S. 564 ff., Supreme Court of the United States, (1928); Goldman v. United States, 316 U.S., S. 129 ff., 62 S.Ct., S. 993 ff., Supreme Court of the United States, (1942); On Lee v. United States, 343 U.S., S. 747 ff., 72 S. Ct., S. 967 ff., Supreme Court of the United States, (1952)

[1387] Camara v. Municipal Court of City and County of San Francisco, 387 U.S., S. 523 ff., 87 S. Ct., S. 1717 ff., Supreme Court of the United States, (1967)

[1388] United States v. Goldstein, 532 F.2d, S. 1311, United States Court of Appeals, Ninth Circuit, (1976)

[1389] Columbia Boadcasting System, Inc v. Democratic National Committee, 94, S. Ct., S. 2080, Supreme Court of the United States, (1973); vgl. auch: Arkansas Educational Television Commission v. Forbes, 523 U.S. S. 666, 118 S. Ct., S. 1633, Supreme Court of the United States, (1998)

[1390] Columbia Boadcasting System, Inc v. Democratic National Committee, 412 U.S., S. 94, S. Ct., S. 2080, Supreme Court of the United States, (1973); Arkansas Educational Television Commission v. Forbes, 523 U.S., S. 666, 118 S. Ct., S. 1633, Supreme Court of the United States, (1998); *Determann*, Kommunikationsfreiheit im Internet, S. 299

[1391] Chicago Area Military Project v. City of Chicago, 508 F.2d, S. 921, United States Court of Appeals, Seventh Circuit, (1975); *Brugger,* Einführung in das öffentliche Recht der USA, § 8, IV.; vgl. auch den Wortlaut des ersten Verfassungszusatzes: "Congress shall make no law…"

[1392] *Brugger*, Einführung in das öffentliche Recht der USA, § 8, IV.; vgl. auch den Wortlaut des ersten Verfassungszusatzes: "Congress shall make no law…"

[1393] vgl.: 3. Kap. Teil 2 A. II. 2. a) aa)

[1394] zum Schutzbereich bereits: 3. Kap. Teil 1 B. I.

Anknüpfungspunkt für das Eingreifen einer Grundrechtsgarantie. Eine Verpflichtung zum Tätigwerden kann sich für den US-amerikanischen Gesetzgeber demnach nur dann ergeben, wenn die Person oder das Unternehmen, das den Filter einsetzt, eine staatliche Behörde ist, der Email-Server als öffentliches Forum anzusehen ist oder zwar eine private Handlung vorliegt, diese aber dem Staat als so genannten „state action" zuzurechnen ist.[1395]
Die Personen bzw. Rechtsträger, die die fraglichen Maßnahmen vornehmen, sind grundsätzlich weder staatliche Behörden, noch lassen sich ihre Email-Server als öffentliche Foren ansehen, innerhalb derer dem Einzelnen das verfassungsrechtlich garantierte Recht auf freie Meinungsäußerung zukommt.[1396] Denn die Tatsache, dass das Internet als Kommunikationsforum zu Verfügung steht, macht es noch nicht zu einer öffentlichen Einrichtung.[1397] Eine Widmung als öffentliches Forum erhält damit weder ein durch einen Email-Provider zur Verfügung gestellter Dienst, noch ein Firmennetz, das die Angestellten benutzen dürfen.[1398]
Ein Schutz nach Maßgabe des ersten Verfassungszusatzes kommt demnach nur dann in Betracht, wenn die entsprechende Maßnahme als staatliche Handlung zu qualifizieren ist.[1399] Eine solche liegt vor, wenn eine ausreichende Verbindung zwischen dem Staat und der beanstandeten Handlung des privaten Rechtsträgers vorliegt, die es rechtfertigt, die Maßnahme dem Staat zuzurechnen.[1400] Zur Beantwortung dieser Frage werden drei verschiedene Kriterien herangezogen.[1401] Einerseits wird die Frage gestellt, ob der private Rechtsträger Befugnisse wahrgenommen hat, die herkömmlicherweise als alleiniges Vorrecht des Staates angesehen werden.[1402] Andererseits ist zu fragen, ob der private Rechtsträger mit der Hilfe oder in Verabredung mit staatlichen Handlungsträgern tätig wurde.[1403] Schließlich

---

[1395] Adickes v. S.H. Kress & Company, 398 U.S., S. 170, 90 S. Ct., S. 1615, Supreme Court of the United States, (1970); Moose Lodge No. 107 v. Irvis, 407 U.S., S. 173, 92 S. Ct., S. 1971, Supreme Court of the United States, (1972); Jackson v. Metropolitan Edison Company, 95 S.Ct., S. 456, Supreme Court of the United States, (1974); Flagg Brothers, Inc. v. Brooks, 436 U.S., S. 164 f., 98 S. Ct., S. 1737 f., Supreme Court of the United States, (1978); Blum v. Yaretsky, 457 U.S., S. 1004 f., 102 S.Ct., S. 2786 f., Supreme Court of the United States, (1982); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 440, United States District Court, Eastern District of Pennsylvania (1996); Noah v. AOL Time Warner, Inc. and America Online, 261 F. Supp. 2d, S. 545 f., United States District Court, E.D. Virginia, (2003)
[1396] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 440 ff., United States District Court, Eastern District of Pennsylvania (1996); United States v. American Library Association, 539 U.S., S. 195, 123 S. Ct., S. 2298 f., Supreme Court of the United States, (2003)
[1397] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 440 ff., United States District Court, Eastern District of Pennsylvania (1996); für das Telefonnetz: Van Bergen v. State of Minnesota, 59 F. 3d, S. 1552, United States Court of Appeals, Eighth Circuit, (1995)
[1398] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 440 ff., United States District Court, Eastern District of Pennsylvania (1996); für das Telefonnetz: United States v. American Library Association, 539 U.S., S. 195, 123 S. Ct., S. 2298 f., Supreme Court of the United States, (2003)
[1399] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996); Noah v. AOL Time Warner, Inc. and America Online, 261 F. Supp. 2d, S. 545 f., United States District Court, E.D. Virginia, (2003)
[1400] Blum v. Yaretsky, 457 U.S., S. 1004, Supreme Court of the United States, (1983); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1401] Mark v. Borough of Hatboro, 51 F. 3d, S. 1142, United States Court of Appeals, Third Circuit, (1995); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996) mehr Rspr.
[1402] so genannter "exclusive public function test", vgl.: Marsh v. State of Alabama, 326 U.S., S. 506, 66 S. Ct., S. 278 f., Supreme Court of the United States, (1946); Blum v. Yaretsky, 457 U.S., S. 1004, Supreme Court of the United States, (1983); Mark v. Borough of Hatboro, 51 F. 3d, S. 1142, United States Court of Appeals, Third Circuit, (1995); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1403] Mark v. Borough of Hatboro, 51 F. 3d, S. 1142, United States Court of Appeals, Third Circuit, (1995); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)

ist zu prüfen, ob der Staat sich im Hinblick auf den handelnden Rechtsträger in eine Position der wechselseitigen Abhängigkeit begeben hat, mit der Folge dass er als Mitverursacher der beanstandeten Maßnahme angesehen werden muss.[1404] Die Frage danach, ob Befugnisse wahrgenommen wurden, die herkömmlicherweise als Vorrecht des Staates angesehen werden, ist schon deshalb zu verneinen, weil es weder als Vorrecht, geschweige denn als alleiniges Vorrecht des Staates anzusehen ist, die Nutzung des Internet zu regeln.[1405] Denn die wesentlichen Bestandteile des Internet befinden sich in privater Hand und werden auch von privaten Rechtsträgern verwaltet.[1406] Email-Service-Provider sind lediglich private Anbieter, die es ihren Kunden ermöglichen, durch ihr Email-System Informationen mit anderen Internet-Nutzern auszutauschen.[1407] Erst Recht gilt dies für Arbeitgeber, da diese die Nutzung des Firmennetzes lediglich geschlossenen Benutzergruppen anbieten. Der Staat hat hingegen kein Interesse daran, den Austausch von Informationen über das Internet zu regulieren und wird auch nicht dergestalt tätig.[1408]
Email-Provider und Arbeitgeber üben auch keine kommunalen oder sonstigen öffentlichen Aufgaben aus. Denn zwar ist ihr Netz an das Internet angeschlossen, jedoch bedeutet dies nicht, dass der Provider oder Arbeitgeber deswegen eine öffentliche oder kommunale Aufgabe übernimmt.[1409] Ein öffentliches Forum kann nur durch eine entsprechende positive Handlung geschaffen werden, während die bloße Herrschaft ein solches nicht automatisch entstehen lässt.[1410] Gegen die Qualifikation des Internet als öffentliches Forum spricht auch die Existenz alternativer Kommunikationswege. So können Unternehmen ihre Werbung auch auf anderem Weg verbreiten und stehen immer noch die Empfänger anderer Email-Service-Provider zur Verfügung, die Emails des fraglichen Versenders bisher nicht blockieren.[1411]
Die Fragen danach, ob der betroffene private Rechtsträger mit Hilfe oder in Verabredung mit staatlichen Handlungsträgern tätig wurde oder ob sich der Staat im Hinblick auf den handelnden Rechtsträger in eine Position der wechselseitigen Abhängigkeit begeben hat, überschneiden sich teilweise. Es ist festzuhalten, dass die Email-Service-Provider sowie

---

[1404] Mark v. Borough of Hatboro, 51 F. 3d, S. 1142 f., United States Court of Appeals, Third Circuit, (1995); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1405] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1406] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 441 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1407] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 441 ff., United States District Court, Eastern District of Pennsylvania (1996); Noah v. AOL Time Warner, Inc. and America Online, 261 F. Supp. 2d, S. 545 f., United States District Court, E.D. Virginia, (2003)
[1408] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 441 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1409] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1410] Hague v. Committee for Industrial Organizations et al., 307 U.S., S. 496 ff., 59 S.Ct., S. 954 ff., Supreme Court of the United States (1939); United States v. American Library Association, 539 U.S., 195, 123 S. Ct., 2298 f., Supreme Court of the United States, (2003); Cyber Promotions , Inc. v. America Online, Inc., 948 F. Supp., S. 446, United States District Court, Eastern District of Pennsylvania, (1996); vgl. zum öffentlichen Forum: Commonwealth of Pennsylvania v. Tate, 495 Pa., S. 173, Supreme Court of Pennsylvania, (1981)
[1411] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 441 ff., United States District Court, Eastern District of Pennsylvania (1996); zur Rechtfertigung bei Vorhandenseins anderer Kommunikationswege: Heffron v. International Society for Krishna Consciousness, Inc. et al., 452 U.S., S. 647, 101 S. Ct., S. 2563, Supreme Court of the United States, (1981); United States v. Grace, 461 U.S., S. 177, 103 S. Ct., S. 1707, Supreme Court of the United States, (1983); Perry Education Association v. Perry Local Educators Association, 460 U.S., S. 45, 103 S. Ct., S. 955, Supreme Court of the United States, (1983); Clark v. Community for Creative Non-Violence, 468 U.S., S. 293, 104 S. Ct., S. 3069, Supreme Court of the United States, (1984); Members of City Council of City of Los Angeles v. Taxpayers for Vincent et al., 466 U.S., S. 812, 104 S. Ct., S. 2133, Supreme Court of the United States, (1984); Clark v. Community for Creative Non-Violence, 468 U.S., S. 293, 104 S. Ct., S. 3069, Supreme Court of the United States, (1984)

andere private Unternehmen die Entscheidung, Werbe- Emails zu blockieren oder zu löschen ohne staatliche Beteiligung treffen.[1412] Eine derartige Zusammenarbeit staatlicher und privater Handlungsträger ist auch nicht dann anzunehmen, wenn der Private sein Recht mittels einer zivilrechtlichen Klage durchsetzt.[1413] Danach ist ein Email-Service-Provider kein staatlicher Handlungsträger und nimmt auch keine staatlichen Handlungen vor.[1414] Somit sind solche Rechtsträger, die Emails an Kunden des fraglichen Providers senden wollen, nicht berechtigt, sich auf den ersten Verfassungszusatz zu berufen.[1415] Demnach kann der Provider Nachrichten blockieren, wenn er dies möchte.[1416] Dieselbe Argumentation gilt für Unternehmen, die die Filtermaßnahmen selbst anordnen.

Aus der US-Verfassung lässt sich demnach keine Verpflichtung des Gesetzgebers ableiten, von der geltenden Rechtslage abweichende Regelungen zu treffen.

II. Völkerrecht

Es existieren bisher keine internationalen Dokumente mit Bindungswirkung, die in einer Verpflichtung des US-amerikanischen Gesetzgebers dahingehend resultieren könnten, von der geltenden Rechtslage abweichende Vorschriften zu erlassen.[1417]

III. Ergebnis

Das einfache US-amerikanische Recht entspricht völker- und verfassungsrechtlichen Vorgaben.

C. Ergebnis

Nach US-amerikanischem Recht ist es zulässig, Filtersoftware einzusetzen, die den Inhalt und die Headerinformationen eingehender Emails überprüft und positiv gescannte Nachrichten entweder löscht, blockiert, markiert oder in spezielle Quarantäne-Ordner einstellt.

[1412] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1413] Cobb v. Georgia Power Co., 757 F. 2d, S. 1251, United States Court of Appeals, Eleventh Circuit, (1985); Tunstall v. Office of Judicial Support of the Court of Common Pleas of Delaware County, 820 F. 2d, S. 634, United States Court of Appeals, Third Circuit, (1987)
[1414] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996); Noah v. AOL Time Warner, Inc. and America Online, 261 F. Supp. 2d, S. 545 f., United States District Court, E.D. Virginia, (2003)
[1415] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996)
[1416] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp., S. 436 ff., United States District Court, Eastern District of Pennsylvania (1996); vgl. auch: United States v. American Library Association, 539 U.S., S. 194 ff., 123 S. Ct., S. 2297 ff., Supreme Court of the United States, (2003); *Nunziato*, 20 Berkeley Tech. L. J., S. 1118; a.A.: *Goldstone*, 46 Hastings L. J., S. 335 ff.
[1417] vgl.: 2. Kap. Teil 2 B. II. 2.

4. Kapitel: Exkurs: Zulässigkeit der Virenfilterung

Bisher wurde dargestellt, inwieweit der Einsatz von Filtersoftware zum Zweck der Spamfilterung zulässig ist. Nachfolgend soll kurz auf die Rechtslage im Bereich der Virenfilterung eingegangen werden.
Viren werden, wie oben dargestellt,[1418] zum Ausspähen von Informationen verwendet und zeichnen sich durch ihre schädigende Wirkung aus. Sie können Daten oder Dateien löschen oder schlimmstenfalls die gesamte Festplatte neu formatieren.[1419] Mögliche Folgen sind die Funktionsunfähigkeit des Rechners des Email-Empfängers sowie des Serverbetreibers.[1420]
Es stellt sich die Frage, ob Filtersoftware, die virenbehaftete Emails anhand bestimmter Merkmale erkennt und abwehrt, rechtmäßigerweise eingesetzt werden darf. Nachfolgend soll zunächst auf die Rechtslage nach Maßgabe des deutschen (Teil 1) und anschließend des US-amerikanischen Rechts (Teil 2) eingegangen werden.

Teil 1: Zulässigkeit der Virenfilterung nach Maßgabe des deutschen Rechts

Zunächst stellt sich die Frage nach der Zulässigkeit des Durchsuchens eingehender Nachrichten auf virentypische Merkmale. Hier kann auf die oben gefundenen Ergebnisse verwiesen werden,[1421] da es in rechtlicher Hinsicht keinen Unterschied macht, ob Emails automatisch auf spam- oder virenspezifische Merkmale untersucht werden. Das Scannen eingehender Emails ist danach rechtmäßig.

Fraglich ist, ob das Löschen oder Umleiten positiv gescannter Emails zulässig ist. Die Verwirklichung der Tatbestände der §§ 206 Abs. 2 Nr. 2, 303 a Abs. 1 StGB könnte hier nach § 109 TKG oder § 34 StGB gerechtfertigt sein.

Nach § 109 Abs. 1 TKG hat jeder Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen. Sofern also der Filtereinsatz dazu dient, den Zugriff Unberechtigter auf personenbezogene Daten zu verhindern oder das Fernmeldegeheimnis zu schützen, lässt er sich nach § 109 Abs. 1 TKG rechtfertigen.
Daneben könnte § 109 Abs. 2 S. 1 TKG eingreifen. Danach haben Betreiber von Telekommunikationsanlagen für die Öffentlichkeit bei den zu diesen Zwecken betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Eine Störung, die zu erheblichen Beeinträchtigungen führt, setzt voraus, dass wichtige Funktionen in den Telekommunikationsanlagen nicht mehr oder nur noch fehlerhaft funktionieren, so dass mindestens in Teilen des Telekommunikationsnetzes die Telekommunikation nur noch eingeschränkt möglich ist.[1422] Viren können diese Auswirkungen haben.[1423] In der Vergangenheit haben sie sogar den Zusammensturz ganzer Server herbeigeführt.[1424] Sie bergen insofern die Gefahr, dass eine Störung der Telekommunikationsanlage mit der Folge

[1418] vgl.: 1. Kap. Teil 1 B. II. 5.
[1419] vgl.: 1. Kap. Teil 1 B. II. 5.
[1420] vgl.: 1. Kap. Teil 1 B. II. 5.
[1421] vgl.: 2. Kap. Teil 2
[1422] *Bock* in Beck´scher TKG-Kommentar, § 109 TKG, Rn. 33; weitere Definition: *Zerres* in Scheurle/Mayen, § 87 TKG, Rn. 13
[1423] zu den Auswirkungen von Viren und Würmern: 1. Kap. Teil 1 B. II. 5.
[1424] zu den Auswirkungen von Viren und Würmern: 1. Kap. Teil 1 B. II. 5.

erheblicher Beeinträchtigungen hervorgerufen wird. Daneben könnten sie auch als äußere Angriffe zu qualifizieren sein. Hierunter sind gezielte systemwidrige Einwirkungen auf die Funktionsfähigkeit der Systeme zu verstehen, die auf ein vorsätzliches menschliches Handeln zurückzuführen sind.[1425] Sofern die Funktionsfähigkeit der Systeme das Ziel des Angriffs ist, liegt also auch die Voraussetzung eines äußeren Angriffs vor. Die Angemessenheit des Filtereinsatzes ist aus den bereits genannten Gründen zu bejahen.[1426] Folglich lässt sich das Löschen von virenverseuchten Emails samt Anhang sowie die Blockade und das Umleiten solcher Emails nach § 109 TKG rechtfertigen.[1427] Allerdings bezieht sich diese Befugnis des Providers nicht auf legitime Emails, da die Störung bzw. der Angriff von diesen nicht ausgeht und insofern eine Beeinträchtigung der Rechte der Absender solcher Nachrichten nicht gerechtfertigt ist.[1428] Das Löschen von false positives ist danach weiterhin strafbar.[1429]

Neben § 109 TKG könnte auch § 34 StGB das Löschen und Blockieren virenbehafteter Emails rechtfertigen. Dies wäre der Fall, wenn sich der Provider oder das jeweilige Unternehmen darauf berufen könnte, durch die Filtermaßnahmen eine gegenwärtige Gefahr für ein notstandsfähiges Rechtsgut abzuwehren. Virenbehaftete Emails stellen aufgrund der genannten Auswirkungen eine Gefahr für das Eigentum des Providers bzw. Unternehmens und des Email-Empfängers sowie für das allgemeine Persönlichkeitsrecht derjenigen Personen dar, deren Daten durch den Virus ausgespäht werden sollen.[1430] Voraussetzung des § 34 StGB ist, dass diese Interessen diejenigen der Absender an der Zustellung der elektronischen Nachricht überwiegen. Hier ist von Bedeutung, dass im Fall der Zustellung verseuchter Emails irreversible Schäden an den betroffenen Rechnern oder am System des Serverbetreibers sowie die Weitergabe ausgespähter Daten drohen. Hingegen ist einzige Konsequenz des Ausfilterns einer virenbehafteten Email, dass diese nicht bei dem Adressaten eintrifft. Insofern ist davon auszugehen, dass die Interessen von Serverbetreiber und Empfänger der virenbehafteten Email diejenigen des Absenders an der Zustellung selbst dann überwiegen, wenn dieser von der Virenverseuchung keine Kenntnis hatte. Vorsätzlichen Versendern virenverseuchter Emails kann von vorneherein keine berechtigte Zustellungserwartung zukommen. Insofern überwiegen die Interessen der Träger der durch den Virus gefährdeten Rechtsgüter diejenigen des Absenders der betroffenen Nachricht. Demnach sind Abwehrmaßnahmen wie das Löschen, Blockieren oder Umleiten virenverseuchter Emails durch § 34 StGB gerechtfertigt. Etwas anderes gilt allerdings für false positives. Filtermaßnahmen in Bezug auf diese Emails können nicht gerechtfertigt werden, da von diesen Emails keine Gefahr für notstandsfähige Rechtsgüter ausgeht. Eine Rechtfertigung nach § 34 StGB ergibt sich demnach lediglich für virenbehaftete Emails.

Etwas anderes ergibt sich auch nicht aus verfassungs-, gemeinschafts- sowie völkerrechtlichen Vorgaben. Die grundrechtliche Situation ist hier eine andere, als dies im Bereich der Spamfilterung der Fall ist. Bei der vorsätzlichen Versendung von Viren besteht keine grundrechtliche Rechtsposition, die gegenüber dem Recht des Empfängers und des Providers bzw. Unternehmens abzuwägen wäre. Bei der fahrlässigen Versendung virenbehafteter Emails sind zwar die oben genannten grundrechtlich geschützten Rechtspositionen des Absenders zu berücksichtigen, angesichts der Gefahren die von Viren insbesondere für das Eigentum von Empfänger und Serverbetreiber ausgehen, hat dieses

[1425] *Bock* in Beck´scher TKG-Kommentar, § 109 TKG, Rn. 35; *Zerres* in Scheurle/Mayen, § 87 TKG, Rn. 14
[1426] vgl.: 2. Kap. Teil 2 A. II. 3. b) cc) (1)
[1427] im Ergebnis ebenso: OLG Karlsruhe, MMR 2005, S. 181; *Heidrich/Tschoepe*, MMR 2004, S. 78; *Schmidl*, MMR 2005, S. 344; vgl. auch: *Art. 29 Datenschutzgruppe*, WP 118, S. 6 f.; kritisch: *Hoeren*, NJW 2004, S. 3516
[1428] vgl.: 2. Kap. Teil 2 A. II. 3. b) cc) (1)
[1429] vgl.: 2. Kap. Teil 2 A. II. 3. b) cc) (1)
[1430] *Koch*, NJW 2004, S. 801 ff.; *Libertus*, MMR 2005, S. 508 ff.; vgl. zu den Auswirkungen von Viren: 1. Kap. Teil 1 B. II. 5.

allerdings gegenüber dem Schutz der gefährdeten Rechtsgüter zurückzutreten. Eine Schutzpflichtverletzung scheidet darüber hinaus deshalb aus, weil im deutschen Recht bereits Schutzvorschriften bestehen, die im Übermittlungsvorgang befindliche Emails davor schützen, durch den Übermittler blockiert, gelöscht oder umgeleitet zu werden mit der Folge, dass der Adressat sie nicht erhält. Diese Vorschriften greifen hier nur deshalb nicht ein, weil Schutzmaßnahmen gegen Eigentums- und anderweitige Rechtsgutsverletzungen durch gesetzliche Vorschriften, hier §§ 109 TKG, 34 StGB, zugelassen sind.
Das Ergebnis steht auch im Einklang mit sekundärrechtlichen Vorgaben. So sieht Art. 4 Abs. 1 S. 1 Hs. 1 EK-DSRL vor, dass Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die Sicherheit ihrer Dienste zu gewährleisten. Da das Zustellen von virenbehafteten Emails die Gefahr der Schädigung nicht nur des Rechners des Empfängers, sondern daneben auch des gesamten Systems des Providers verursacht, legitimiert Art. 4 Abs. 1 S. 1 Hs. 1 EK-DSRL den Filtereinsatz als technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit des Dienstes.[1431] Art. 7 lit. b) DSRL greift hingegen aus den oben genannten Gründen nicht ein.[1432] Allerdings könnte ein Fall des Art. 7 lit. f) DSRL vorliegen. Die Voraussetzungen des Erlaubnistatbestandes liegen vor, wenn die Verarbeitung zur Verwirklichung des berechtigten Interesses erforderlich ist, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Art. 1 Abs. 1 geschützt sind, überwiegen. Soeben wurde im Rahmen der §§ 109 TKG, 34 StGB dargestellt, dass hier berechtigte Interessen der Kunden betroffen sind, die diejenigen der betroffenen Person überwiegen. Diese Interessen nimmt der Provider bzw. das jeweiligen Unternehmen wahr, wenn es virenbehaftete Emails löscht, um die Funktionalität des Servers, das Eigentum der Kunden bzw. deren Datenbestände vor Kenntnisnahme zu schützen. Grundfreiheiten und grundrechtliche Positionen des Versenders stehen hier nicht entgegen, da diese nicht dahin gehen können, vorsätzlich oder fahrlässig fremdes Eigentum zu schädigen oder die Daten Dritter auszuspähen. Folglich greift der Erlaubnistatbestand des Art. 7 lit. f) DSRL hier ein, wobei auch hier aus den soeben genannten Gründen die Löschung von false positives nicht rechtmäßig ist.

Teil 2: Zulässigkeit der Virenfilterung nach Maßgabe des US-amerikanischen Rechts

Fraglich ist, wie sich die Rechtslage im Bereich des US-amerikanischen Rechts darstellt.

Hier können sich Unterschiede allenfalls hinsichtlich der Frage des Ausfilterns von Emails ergeben. Denn wie bereits dargestellt ist das Scannen von Emails auf werbetypische Merkmale zulässig. Hinsichtlich des Durchsuchens eingehender Nachrichten auf virentypische Merkmale kann nichts anderes gelten, denn rechtlich macht es keinen Unterschied, wonach das Programm in der Email sucht.

Wie oben bereits dargestellt wurde besteht im US-amerikanischen Recht zwar eine Vorschrift, die Zugriffe auf fremde Kommunikation und das Verhindern des Zugangs durch den Berechtigten zu verhindern sucht, nämlich der Stored Communications Act. Allerdings ist einerseits das Zugreifen des Serverbetreibers auf die eigene Anlage, also den eigenen Server nicht unberechtigt. Andererseits besteht eine Ausnahmevorschrift zugunsten der Provider, die diese weitgehend vom Anwendungsbereich der Vorschrift ausnimmt, vgl. 18 U.S.C. § 2701 (c) (1). Oben wurde bereits gezeigt, dass die soeben genannten Vorschriften in Einklang mit verfassungsrechtlichen Vorgaben stehen, da hier nicht staatliche Rechtsträger, sondern Private

[1431] *Art. 29 Datenschutzgruppe*, WP 118, S. 7
[1432] vgl.: 2. Kap. Teil 2 B. II. 1. a)

handeln. Darüber hinaus ist hier bereits nicht das Grundrecht der Meinungsäußerungsfreiheit betroffen, da dieses nicht die Berechtigung beinhalten kann, der Meinungsäußerung schädigende Anhänge beizufügen.
Das Ausfiltern von Viren ist nach US-amerikanischem Recht somit unproblematisch zulässig.

5. Kapitel: Vergleich der Rechtslage nach deutschem und US-amerikanischem Recht

Im Folgenden soll die in den beiden Rechtsordnungen geltende Rechtslage gegenübergestellt werden. Dabei wird zwischen Vorschriften zum Schutz vor unerwünschter Kommunikation (Teil 1), zum Schutz der Privatsphäre der Kommunikationspartner (Teil 2) und zum Schutz der Sicherheit und Zuverlässigkeit der Kommunikation mittels Email (Teil 3) unterschieden.

Teil 1: Schutz vor unerwünschter elektronischer Kommunikation

Zunächst soll auf die Unterschiede und Gemeinsamkeiten der Regelungen in den beiden Rechtsordnungen eingegangen werden (A.) und im Anschluss auf die dafür verantwortlichen Gründe (B.). Dann werden die Lösungen und hierdurch erzielten Folgen wertend gegenübergestellt und die sich daraus ergebenden rechtspolitischen Forderungen aufgezeigt (C.).

A. Unterschiede und Gemeinsamkeiten

Die Rechtslage hinsichtlich der Zulässigkeit unverlangter Email-Werbung in den beiden Staaten unterscheidet sich in mehreren Punkten. Einerseits gilt in Deutschland nach Maßgabe des UWG und der §§ 823, 1004 Abs. 1 BGB das lediglich bei bestimmten bereits bestehenden Geschäftskontakten abgeschwächte Opt-In-Prinzip,[1433] in den USA hingegen die Opt-Out-Lösung.[1434] Darüber hinaus erfassen im deutschen Recht die deliktsrechtlichen Vorschriften auch nicht-kommerzielle Emails, während den einschlägigen Vorgaben in den USA lediglich solche Nachrichten unterfallen, deren primärer Zweck kommerzieller Natur ist.[1435] Ein Unterschied besteht auch darin, dass in den USA nur bestimmten Rechtsträgern eine Klagemöglichkeit zukommt, während nach deutschem Recht auch Privatpersonen gegen die Spammer vorgehen können. In den seltenen Fällen, in denen das Volumen eingehender Emails zur Folge hat, dass der Adressat die in seiner Mailbox legitime nicht mehr von unerwünschten Emails unterscheiden kann, ist das Versenden unerwünschter Emails auch im deutschen Recht auch strafrechtlich sanktioniert.

B. Gründe für die Unterschiede bzw. Gemeinsamkeiten

Begründen lassen sich die Unterschiede, wenn man sich die abweichende Bewertung der im Raum stehenden Rechtspositionen in den beiden Rechtsordnungen vor Augen führt, wobei insbesondere die verfassungsrechtlichen Rahmenbedingungen in den beiden Staaten zu berücksichtigen sind.

Aus deutscher Sicht besteht ein Recht, von unerwünschter Email-Werbung frei zu bleiben, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK.[1436] Diesem Recht stehen die Meinungs- und Berufsfreiheit der Werbetreibenden, Art. 5 Abs. 1 GG, Art. 12 Abs. 1 GG, Art. 10 Abs. 1 EMRK, sowie die Informationsfreiheit der an Werbung interessierten Marktteilnehmer, Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK, gegenüber.[1437] Der Privatsphäre des Betroffenen wird dabei insofern der Vorrang eingeräumt, als der Werbende verpflichtet wird, vor Zusendung der Werbung die Einwilligung des Adressaten einzuholen. Die Opt-In-Lösung wird auf Gemeinschaftsebene damit begründet, dass Email-Direktwerbung leicht und

[1433] vgl.: 2. Kap. Teil 1
[1434] vgl.: 3. Kap. Teil 1
[1435] vgl.: 3. Kap. Teil 1. A. I.
[1436] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa); 2. Kap. Teil 1 B. II. 1. b) bb) (2) (b) (aa); 2. Kap. Teil 1 B. II. 2. a)
[1437] vgl.: 2. Kap. Teil 1 B. I. 1. a); 2. Kap. Teil 1 B. II. 1. b) bb) (1) (a); 2. Kap. Teil 1 B. II. 2. a)

preiswert zu versenden ist, eine Belastung und bzw. oder einen Kostenaufwand für den Empfänger darstellt und Schwierigkeiten für die elektronischen Kommunikationsnetze verursachen kann, Nr. 40 EK-DSRL. Auch im deutschen Recht wird zur Begründung einer Persönlichkeitsrechtsverletzung durch Werbung auf deren Belästigungseffekt abgestellt.[1438] Die Entscheidung für das Opt-In-Prinzip basiert demnach darauf, dass die Interessen der Empfänger an der Privatsphäre höher bewertet werden, als diejenigen der Werbetreibenden, ohne vorheriges Einholen der Einwilligung der Adressaten Email-Werbung zu versenden. Zudem soll vermieden werden, dass die Versender kommerzieller Emails ihre Werbekosten auf die Email-Empfänger abwälzen. Die Opt-Out-Lösung ist deshalb kein milderes Mittel, da sie nicht gleich effektiv ist.[1439] Da die Privatsphäre der Empfänger auch durch nicht-kommerzielle unerwünschte Emails beeinträchtigt wird, können sich auch Adressaten solcher Nachrichten dagegen mittels Schadensersatz- und Unterlassungsansprüchen zur Wehr setzen.[1440] Denn für den Empfänger, der sich nicht mit unerwünschten Inhalten auseinandersetzen möchte, macht es keinen Unterschied, ob ihm der Abschluss eines Vertrages angetragen wird oder ob es sich um politische oder religiöse Nachrichten handelt.[1441] Die strafrechtliche Sanktionierung der Beeinträchtigung der Gebrauchsfähigkeit von Daten beruht letztlich darauf, dass Daten im deutschen Recht einen der Sachbeschädigung äquivalenten Schutz erhalten sollten.[1442]

Die zurückhaltende Haltung in den USA basiert hingegen auf der großen Bedeutung, die dem im ersten Verfassungszusatz enthaltenen Recht auf Meinungsfreiheit dort zukommt. Das Grundrecht dient dazu, staatliche Beschränkungen aus dem Bereich der öffentlichen Diskussion fernzuhalten.[1443] Der Erhalt der Vielfalt des unbeschränkten Austauschs von Ideen ist dabei nach US-amerikanischer Auffassung essentiell für die politische und soziale Entwicklung der Bürger und damit des Staates.[1444] Insofern wird das Grundrecht der Meinungsfreiheit als Grundstein für alle anderen Grundrechte angesehen.[1445] Deshalb werden dem Grundrecht eine vorrangige Stellung innerhalb der Verfassung[1446] und ein weiter Schutzbereich zugewiesen.[1447] Auch die kommerzielle Rede ist von dem Grundrecht erfasst, wenngleich der Schutzumfang im Vergleich zur nicht-kommerziellen Rede geringer ist.[1448]

[1438] vgl.: 2. Kap. Teil 1 A. III. 1. a) aa)
[1439] vgl.: 2. Kap. Teil 1 B. I. 2. b) aa)
[1440] vgl.: 2. Kap. Teil 1 A. III.
[1441] vgl.: 2. Kap. Teil 1 A. III.
[1442] vgl.: 2. Kap. Teil 1 A. I. 1. b)
[1443] Roth v. United States, 354 U.S., S. 476 ff., 77 S. Ct., S. 1304 ff., Supreme Court of the United States, (1957); New York Times v. Sullivan, 376 U.S., S. 254 ff., 85 S. Ct., S. 710 ff., Supreme Court of the United States, (1964); Texas v. Johnson, 491 U.S., S. 397 ff., 109 S. Ct., S. 2533 ff., Supreme Court of the United States, (1989); Simon & Schuster, Inc. v. Members of the New York State Crime Board et al., 502 U.S., S. 105, 112 S. Ct., S. 501, Supreme Court of the United States, (1991); Thomas v. Board of Education, Granville Central School District, 607 F.2d, S. 1043 ff., (1979) der Antrag auf writ of certiorari wurde zurückgewiesen, 100 S. Ct., S. 1034, 444 U.S., S. 1081
[1444] Roth v. United States, 354 U.S., S. 476 ff., 77 S. Ct., S. 1304 ff., Supreme Court of the United States, (1957); New York Times v. Sullivan, 376 U.S., S. 254 ff., 85 S. Ct., S. 710 ff., Supreme Court of the United States, (1964); Texas v. Johnson, 491 U.S., S. 397 ff., 109 S. Ct., S. 2533 ff., Supreme Court of the United States, (1989)
[1445] Nelson v. McClatchy Newspapers, Inc. 131 Wash.2d, S. 523, 936 P.32d, S. 1123, Supreme Court of Washington, (1997)
[1446] Follett v. Town of McCormick, S.C., 321 U.S., S. 573, 64 S. Ct., S. 717, Supreme Court of the United States, (1944); Greenberg v. CBS, Inc., 69 A.D.2d, S. 693, 419 N.Y.S.2d, S. 988, Supreme Court, Appellate Division, Second Department, New York, (1979); Watts v. Civil Service Board for Columbia, 606 S.W.2d, S. 274, Supreme Court of Tennessee, (1980); The People of the State of Colorado v. Smith, 862 P.2d, S. 939, Supreme Court of Colorado, (1993)
[1447] vgl.: 3. Kap. Teil 1 B. I.
[1448] vgl.: 3. Kap. Teil 1 B. I.

Zwar besteht keine Verpflichtung des Gesetzgebers, zum Schutz vor Grundrechtsbeeinträchtigungen Privater tätig zu werden, allerdings hat er es zu unterlassen, die Meinungsäußerungsfreiheit zu weitgehend einzuschränken.[1449] Deshalb hatte der Gesetzgeber zurückhaltend vorzugehen, worauf sich die Opt-Out-Lösung im US-amerikanischen Recht zurückführen lässt.
Der Opt-Out-Lösung hätte der US-amerikanische Gesetzgeber auch politische Werbung unterwerfen können, denn auch die politische Meinungsäußerung lässt sich einschränken.[1450] Allerdings bestehen in Bezug auf die Regulierung politischer Äußerungen doch größere Bedenken, als im Fall kommerzieller Werbung.[1451] Als problematisch wird im Bereich der politischen Werbung angesehen, wenn Regelungen getroffen werden, die die Adressaten der Möglichkeit berauben, von politischen Meinungen Kenntnis zu nehmen, sich also letztlich auf den politischen Meinungsbildungsprozess auswirken würde.[1452] Dies erklärt die Zurückhaltung des US-amerikanischen Gesetzgebers und damit die Beschränkung der Regulierung des Email-Versands auf kommerzielle Emails.[1453]

C. Wertung der Lösungen und erzielten Folgen und rechtspolitische Forderungen

Die Opt-In- und die Opt-Out-Lösung resultieren in unterschiedlichen Anforderungen an den Empfänger potentieller Spammails. Während im ersten Fall der Empfänger bereits dann geschützt wird, wenn er passiv bleibt, ist ein Tätigwerden des Empfängers im Rahmen der Opt-Out-Lösung erforderlich, falls keine weitere Email-Werbung erwünscht ist. Zugunsten der Opt-In-Lösung lässt sich anführen, dass Adressaten an dem Erhalt von Werbe-Emails angesichts des dargestellten Belästigungseffekts[1454] und der auf sie durch die Absender vorgenommene Kostenverlagerung in aller Regel nicht interessiert sein werden.[1455] Von einer ablehnenden Haltung ist folglich auch ohne erklärten Widerspruch grundsätzlich auszugehen.[1456] Das US-amerikanische Opt-Out-System hat demnach zur Folge, dass viele Empfänger erlaubterweise Werbung erhalten, obwohl sie diese nicht erhalten möchten, wenn sie nicht der Übersendung widersprochen haben.[1457]

Aus US-amerikanischer Sicht lässt sich dem entgegenhalten, dass es auch Empfänger gibt, die am Erhalt der kommerziellen Emails interessiert sind, insbesondere dann, wenn die Werbung auf die Bedürfnisse des Empfängers abgestimmt ist.[1458] Daneben berücksichtigt nur die US-amerikanische Regelung die Interessen der Werbewirtschaft an einem schnellen, billigen und einfachen Weg der Werbung. Rechtspolitisch bedenklich ist allerdings, dass der CAN-SPAM Act das Versenden kommerzieller Emails nicht verbietet, sondern vielmehr grundsätzlich erlaubt. Auch besteht das Problem, dass Vorschriften zur Regulierung der Email-Werbung

[1449] vgl.: 3. Kap. Teil 2 B. I.
[1450] Rowan v. United States Post Office, 397 U.S., S. 728 ff., 90 S. Ct., S. 1484 ff., Supreme Court of the United States, (1970); Ward v. Rock against Racism, 491 U.S., S. 800, 109 S. Ct., S. 2758, Supreme Court of the United States, (1989); Van Bergen v. State of Minnesota, 59 F. 3d, S. 1541 ff., United States Court of Appeals, Eighth Circuit, (1995); *Grossman*, 19 Berkeley Tech. L. J., S. 1533 ff.
[1451] *Grossman*, 19 Berkeley Tech. L. J., S. 1571; *Sweet*, 2003 Duke L. & Tech. Rev. 0001
[1452] *Grossman*, 19 Berkeley Tech. L. J., S. 1571
[1453] So führte der Kongressabgeordnete Gary Miller aus, dass die Hauptursache, dass politischer Spam nicht gesetzlich geregelt werde der ist, dass sichergestellt werden soll, dass der CAN-SPAM Act nicht für rechtswidrig erklärt wird, vgl. *Grossman*, 19 Berkeley Tech. L. J., Fn. 82
[1454] vgl.: 1. Kap. Teil 1 B. 4.
[1455] *Alongi*, 46 Ariz. L. Rev., S. 280; *Grossman*, 19 Berkeley Tech. L. J., S. 1541 f.; *Wendlandt*, MMR 2004, S. 369; *Zhang*, 20 Berkeley Tech. L. J., S. 320
[1456] *Alongi*, 46 Ariz. L. Rev., S. 280; *Grossman*, 19 Berkeley Tech. L. J., S. 1541 f.; *Wendlandt*, MMR 2004, S. 369
[1457] *Wendlandt*, MMR 2004, S. 369; *Zhang*, 20 Berkeley Tech. L. J., S. 320
[1458] *Funk/Zeifang/Johnson/Spessard*, CRi 2004, S. 139; *Grossman*, 19 Berkeley Tech. L. J., S. 1573

lediglich auf rechtstreue Unternehmen einen Effekt haben werden. Zieht man in Betracht, dass viele Spammer gerade nicht rechtstreu sind, so zeigt sich, dass das Erfordernis eines Widerspruchs auch deshalb nicht wünschenswert ist, weil solche Unternehmen hierdurch verifizieren können, ob die Email-Adresse des Empfängers existent ist.[1459] Hinzu kommt, dass Privatpersonen ihre Ansprüche nicht selbst klageweise geltend machen können, was sie möglicherweise ebenfalls davon abhalten wird, das Opt-Out zu erklären. Aufgrund des Fehlens individueller Klagemöglichkeiten auf Seiten der Empfänger werden Verstöße gegen den CAN-SPAM Act auch häufig ungeahndet bleiben, da die klageberechtigten Personengruppen erst ab einer gewissen Belästigungsschwelle gegen einen bestimmten Spammer rechtlich vorgehen werden.
Da das US-amerikanische Opt-Out-Prinzip im Gegensatz zur deutschen Regelung nur solche Empfänger vor Email-Werbung schützt, die sich dagegen wehren, bürdet es dem Empfänger den Zeit- und Kostenaufwand auf, der mit der Erklärung des Widerspruchs verbunden ist. Hält man sich vor Augen, welches Ausmaß Email-Werbung mittlerweile angenommen hat, so wird erkennbar, dass es für einen Empfänger jedoch überhaupt nicht möglich sein wird, sämtlichen unerwünschten Werbe-Emails zu widersprechen. Damit wird der Empfänger in nicht zu rechtfertigender Weise gegenüber der Werbewirtschaft benachteiligt.

Die strafrechtliche Sanktion für das Unbrauchbarmachen von Daten im deutschen Recht wird kaum praktische Folgen nach sich ziehen, da ein Eingang einer solchen Vielzahl an Nachrichten in einem Mailaccount innerhalb so kurzer Zeit, dass die unerwünschten Emails nicht mehr aussortiert werden können, in aller Regel nicht erfolgen wird.

Daneben besteht zwischen den beiden Rechtsordnungen ein Unterschied hinsichtlich Art der erfassten Emails. Da auch massenweise versandte elektronische Post, die nicht der Definition der kommerziellen Email im Sinne des CAN-SPAM Act entspricht, die beschriebenen Folgen nach sich ziehen kann, ist es kritikwürdig, dass diese im US-amerikanischen Recht erst gar nicht in den Anwendungsbereich der Spam-Gesetzgebung fallen.

Rechtspolitisch wünschenswert ist eine Regelung, die nicht die Versender unverlangter Email-Werbung gegenüber den Empfängern dahingehend privilegiert, dass letzteren zu Gunsten der Direktmarketingunternehmen der Zeit- und Kostenaufwand für einen Widerspruch aufgebürdet wird. Insofern erscheint das deutsche Opt-In-Prinzip als vorzugswürdig, da nur so wenigstens rechtstreue Unternehmen daran gehindert werden können, unbeschränkt Emails zu versenden und nicht rechtstreue Unternehmen nicht aufgrund des zu erklärenden Widerspruchs die Email-Adressen, die sie verwendet haben, verifizieren können. Aus Sicht der Empfänger unerwünschter Email-Werbung sowie der Provider ist folglich das deutsche Opt-In-System gegenüber der US-amerikanischen Opt-Out-Lösung vorzuziehen. Da auch unerwünschten elektronischen Nachrichten, die der Definition der kommerziellen Email im Sinne des CAN-SPAM Act nicht unterfallen, die genannten negativen Auswirkungen zukommen können, sprechen die besseren Argumente gegen die Beschränkung des Begriffs auf lediglich solche Nachrichten.
Angesichts des verfassungsrechtlichen Umfelds in den USA ist jedoch davon auszugehen, dass das Opt-In-System dort nicht umgesetzt werden wird, da die Lösung der in der USA vorherrschenden Auffassung widerspricht, welche die freie -auch kommerzielle- Meinungsäußerung als eine Grundbedingung der sozialen und wirtschaftlichen Entwicklung begreift.[1460] Eine Übertragung der deutschen Lösung auf das US-amerikanische Recht kann demnach trotz der auf den ersten Blick bestehenden rechtspolitischen Vorteile nicht empfohlen werden.

[1459] *Alongi*, 46 Ariz. L. Rev., S. 288; *Zhang*, 20 Berkeley Tech. L. J., S. 320
[1460] vgl.: 5. Kap. Teil 1 B.

In beiden Rechtsordnungen stellt sich das Problem, dass die Versender von Spammails aufgrund der Praxis des Verschleierns der Absenderadresse oder des Missbrauchs fremder Server sowie aufgrund der Tatsache, dass solche Nachrichten international und häufig über im Ausland befindliche Server versandt werden, in der Regel nicht gefasst werden können. Insofern sind international bindende Regelungen bzw. eine internationale Zusammenarbeit im Bereich der Spambekämpfung unumgänglich.[1461] Allein durch nationale Vorgaben wird sich hingegen die Spamproblematik nicht in den Griff bekommen lassen. Da viele Unternehmen sich nicht an die gesetzlichen Vorschriften halten bzw. vom Ausland aus agieren, wird es daneben stets erforderlich sein, technische Mittel, wie Spamfilter, fortzuentwickeln und einzusetzen, um unerwünschte Email-Werbung abzuwehren.

Teil 2: Schutz der Privatsphäre der Kommunikationspartner

Nachfolgend wird die in den beiden Rechtsordnungen bestehende Rechtslage in Bezug auf den Schutz der Privatsphäre der Kommunikationspartner verglichen. Dabei sollen zunächst die Unterschiede und Gemeinsamkeiten der Regelungen in den beiden Rechtsordnungen (A.), sodann die dafür verantwortlichen Gründe (B.) dargestellt werden. Im Anschluss werden die Lösungen und hierdurch erzielten Folgen wertend gegenübergestellt und die sich daraus ergebenden rechtspolitischen Forderungen aufgezeigt (C.).

A. Unterschiede und Gemeinsamkeiten

Im deutschen Recht ist das Überprüfen von Inhalt und Headerinformationen durch Filtersoftware zulässig, da keine natürliche Person von den entsprechenden Daten Kenntnis erlangen kann.[1462] Aus diesem Grund ist der Personenbezug im datenschutzrechtlichen Sinne zu verneinen und liegt auch keine Verletzung des Telekommunikationsgeheimnisses und des allgemeinen Persönlichkeitsrechts vor.[1463]
Auch nach US-amerikanischem Recht ist der Einsatz der Filtersoftware zulässig. Die Vorgaben des Wiretap Act sind nicht einschlägig, da kein Verschaffen der Kommunikationsinhalte vorliegt. Die Filtermaßnahmen sind auch nicht nach Maßgabe des Stored Communications Act unzulässig, da kein unberechtigter Zugang zu der Anlage und der Kommunikation gegeben ist. Weitere datenschutzrechtliche Regelungen sind aufgrund des nur sektoralen Regelungsansatzes im Hinblick auf den Schutz persönlicher Informationen im Verhältnis zu Privaten nicht einschlägig. Das Überprüfen eingehender Emails auf werbetypische Merkmale stellt auch keine deliktische Handlung dar, da hinsichtlich versandter Emails keine berechtigte Erwartung der Privatheit besteht und der Filtereinsatz nicht als höchst offensiv anzusehen ist.

Ein Unterschied zwischen dem deutschen und dem US-amerikanischen Recht besteht darin, dass Provider nach dem deutschen Recht in sehr viel begrenzterem Umfang Schutzmaßnahmen vornehmen dürfen, als nach Maßgabe des US-amerikanischen Rechts. Nach deutschem Recht ist dies nur dann möglich, wenn erhebliche Beeinträchtigungen von Telekommunikationsnetzen zu erwarten sind, vgl. § 109 Abs. 2 S. 2 TKG oder wenn die

[1461] zu internationalen Anti-Spam-Initiativen: vgl. etwa: *London Action Plan*, einsehbar unter: http://londonactionplan.org (letzter Abruf: 29.04.2007); *OECD*, Anti-Spam Toolkit, einsehbar unter: http://www.oecd-antispam.org/ (letzter Abruf: 29.04.2007); *Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam*, einsehbar unter: http://www.acma.gov.au/acmainterwr/comsumer_info/spam/spam_mou.rtf (letzter Abruf: 29.04.2007)
[1462] vgl.: 2. Kap. Teil 2
[1463] vgl.: 2. Kap. Teil 2 A.

Interessen des Providers und seiner Kunden dasjenige von Empfänger und Absender an der Zustellung der elektronischen Nachricht überwiegen, § 34 StGB. Dagegen enhält 18 U.S.C. § 2511 (2) (a) (i) eine Ausnahme bereits für den Fall, dass die Maßnahme der Erbringung der Dienstleistung oder dem Schutz der Rechte des Providers oder seines Eigentums dient, wobei im Rahmen der zuletztgenannten Alternativen bereits rein finanzielle Interessen das Tätigwerden des Providers rechtfertigen. Das US-amerikanische Recht räumt demnach dem Provider weitergehendere Möglichkeiten zum Schutz seiner Rechte und denen seiner Kunden ein, als das deutsche.

B. Gründe für die Unterschiede bzw. Gemeinsamkeiten

Die Vorschriften in beiden Rechtsordnungen kommen zu dem gleichen Ergebnis, wenngleich dem Datenschutz bzw. dem Schutz der Privatsphäre im Sinne des Schutzes personenbezogener Informationen in den beiden Rechtsordnungen ein unterschiedlicher Stellenwert zukommt.[1464]
So wird in Deutschland, wie auch auf Ebene des europäischen Gemeinschaftsrechts das Ziel verfolgt, ein möglichst hohes Maß an Datenschutz zu erreichen.[1465] Dahinter steht die Auffassung, dass Datenschutz bzw. das Recht auf informationelle Selbstbestimmung Grundvoraussetzung der Ausübung anderer Grundrechte und somit eine elementare Funktionsbedingung eines freiheitlich demokratischen Gemeinwesens ist.[1466] Deshalb soll der Betroffene selbst entscheiden können, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[1467] Mit der informationellen Selbstbestimmung ist es danach nicht vereinbar, wenn der Bürger nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß.[1468]
Im US-amerikanischen Recht herrrscht jedoch eine andere Auffassung vor. Dort wird der freie Datenverkehr als Grundvoraussetzung für eine positive ökonomische und soziale Entwicklung angesehen, da es nur bei genauer Kenntnis eines Sachverhalts möglich ist, informierte Entscheidungen zu treffen.[1469] Demnach besteht die Befürchtung, dass ein starker Datenschutz[1470] es erschwert, für die wirtschaftliche und soziale Entwicklung relevante Daten zu erhalten.[1471] Dies bedeutet allerdings nicht, dass in den USA die Privatsphäre keinerlei Schutz erfährt. Allerdings beschränkt sich der Schutz auf bestimmte Aspekte der

[1464] vgl. zu den aus der Diskrepanz der Auffassung in den USA und der EU resultierenden Schwierigkeiten, insbesondere im Hinblick auf den Datentransfer aus der EU in die USA: *Gilbert*, 865 PLI/Pat, S. 545 ff.; *Pearce/Platten*, 22 Fordham Int´l L. J., S. 2024 ff.; zur Safe Harbor Lösung, die den Datentransfer in die USA ermöglicht: http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_de_htm (letzter Abruf: 29.04.2007)
[1465] vgl.: Art. 1 Abs. 1, Erwägungsgrund Nr. 10 DSRL; BVerfGE 65, S. 1 ff., 41 ff.; vgl. auch: 2. Kap. Teil 2 A. I. 1. a) aa) (2) (a)
[1466] BVerfGE 65, S. 1 ff., 41 ff.; vgl. auch: Hessisches Datenschutzgesetz von 1970, GVBl. I, 625; Rapport de la Commission Informatique et Libertés, (1975); *Gallwas*, § 1 BDSG, Rn. 8 ff.; *Simitis* in Ders., Einl., Rn. 30 f.
[1467] BVerfGE 65, S. 1 ff., 41 ff.; vgl. auch: BVerfGE 56, S. 37 ff., 41 ff.; BVerfGE 63, S. 131 ff., 142 f.
[1468] BVerfGE 65, S. 1 ff., 41 ff.
[1469] *Fromholz*, 15 Berkeley Tech. L. J., S. 465; *Gilbert*, 865 PLI/Pat, S. 553; Heise Online News vom 28.03.2001, abrufbar unter: http://www.heise.de/newsticker/meldung/16616 (letzter Abruf: 29.04.2007); *McCullagh*, Privacy Laws: Not Gonna Happen, abrufbar unter: http://www.wired.com/news/politics/1,42123-0.html (letzter Abruf: 29.04.2007); *Solove/Hoofnagle*, 2006 U. Ill. L. Rev., S. 384
[1470] in den USA wird häufig nicht der Begriff data protection verwendet wird, sondern der Datenschutz als Teil der Privatsphäre (privacy) angesehen; dieser wird auch die so genannte „information privacy“ zugeordnet, vgl. *Kang*, 50 Stan. L. Rev., S. 1193
[1471] *Fromholz*, 15 Berkeley Tech. L. J., S. 465; *Gilbert*, 865 PLI/Pat, 553; *McCullagh*, Privacy Laws: Not Gonna Happen, abrufbar unter: http://www.wired.com/news/politics/1,42123-0.html (letzter Abruf: 29.04.2007); *Solove/Hoofnagle*, 2006 U. Ill. L. Rev., S. 384

Privatsphäre.[1472] Darüber hinaus ist zu beachten, dass die Verfassung in den USA lediglich vor Beeinträchtigungen der Privatsphäre durch staatliche Behörden schützt, also keine Schutzpflicht des Gesetzgebers gegen private Beeinträchtigungen des Rechts bestehen, weswegen der Datenschutz in den USA im öffentlichen Sektor sehr viel strenger ist, als im privaten Bereich.[1473] Schließlich wird in den USA eher als in Deutschland darauf vertraut, dass die Betroffenen durch Instrumente der Selbstregulierung oder durch den Einsatz technischer Mittel einen angemessenen Ausgleich finden werden, so dass ein gesetzgeberisches Tätigwerden nicht immer als notwendig angesehen wird.[1474] Deshalb existieren in den USA in erster Linie Gesetze, die den Umgang mit personenbezogenen Daten durch staatliche Behörden regulieren sowie weitere sektorale Ansätze des Datenschutzes.[1475] Hinzu kommt, dass im Bereich der Kommunikation mittels Email nicht davon ausgegangen wird, dass der Betroffene eine berechtigte Erwartung der Privatsphäre dahingehend hat, dass Angestellte des Providers nicht auf die Email zugreifen, was jedoch Voraussetzung des Eingreifens des vierten Verfassungszusatzes ist, der die Privatsphäre schützt.[1476]

Trotz der unterschiedlichen Auffassung in Bezug auf den Datenschutz kommen hier beide Rechtsordnungen zu demselben Ergebnis. Diese Übereinstimmung beruht darauf, dass die Privatsphäre in Gestalt der informationellen Selbstbestimmung im vorliegenden Fall nicht beeinträchtigt wird, da eine Kenntnisnahme von Inhalten oder Daten aufgrund des Filtereinsatzes praktisch ausgeschlossen ist. Deshalb greift auch das im Verhältnis zum Recht der USA strengere und umfassendere deutsche Datenschutzrecht nicht ein, ebensowenig wie straf- und bürgerlich-rechtliche Vorschriften, die dem Schutz der Privatsphäre dienen.

Auch was den Schutz der Kommunikationsinhalte betrifft, kommen hier beide Rechtsordnungen zu dem gleichen Ergebnis. Der Grund hierfür ist darin zu sehen, dass es im deutschen Recht an einem Kenntnisverschaffen im Sinne der das Fernmeldegeheimnis schützenden Vorschriften fehlt. Ebenso fordert der Wiretap Act im US-amerikanischen Recht das Verschaffen der Kommunikationsinhalte. Die Vorschriften beider Staaten greifen folglich aus dem Grund nicht ein, weil durch den Filtereinsatz kein Dritter Kenntnis vom Inhalt der Kommunikation erlangt oder später erlangen kann. Es besteht demnach keine Gefahr für die Privatheit der räumlich distanzierten Kommunikation, weshalb diese hier auch keines Schutzes bedarf.

[1472] *Fromholz*, 15 Berkeley Tech. L. J., S. 465, 472; *Gilbert*, 865 PLI/Pat, S. 553; *Gubitz*, 39 New Eng. L. Rev., S. 446; *Peeters*, MMR 2005, S. 417; *Reidenberg*, 44 Fed. Comm. L. J., S. 209; *Schwartz/Reidenberg*, S. 6; *Solove/Hoofnagle*, 2006 U. Ill. L. Rev., S. 357, 384; vgl. auch: 3. Kap. Teil 2 A. I. 2.; grundlegend zur Privatsphäre: *Warren/Brandeis*, 4 Harv. L. Rev., S. 194 ff.

[1473] Griswold v. Connecticut, 381 U.S., S. 479, 85 S. Ct., S. 1678, Supreme Court of the United States, (1965); *Fromholz*, 15 Berkeley Tech. L. J., S. 470; *Gubitz*, 39 New Eng. L. Rev., S. 446; vgl. auch: 3. Kap. Teil 2 B. I.

[1474] *Art. 29 Datenschutzgruppe*, WP 15; *Cody*, Cath. U.L. Rev., S. 1183 ff.; *Fromholz*, 15 Berkeley Tech. L. J., S. 472; *Gilbert*, 865 PLI/Pat, S. 545 ff; *Pearce/Platten*, 22 Fordham Int´l L. J., S. 2035 f.; *Schneider* in Bäumler, S. 153;*Tröndle*, RDV 1999, S. 718 f.; zu Selbstregulierungsansätzen in den USA: Projekt *The Better Business Bueau Online* (BBBOnline), homepage: http://www.bbbonline.org (letzter Abruf: 29.04.2007); Projekt *TRUSTe*, homepage: http://www.truste.org (letzter Abruf: 29.04.2007); vgl. auch: *Jacob/Heil* in Bizer u.a., Freundesgabe Büllesbach, S. 220; *Roßnagel*, Regulierung und Selbstregulierug im Datenschutz; vgl. auch den Safe Harbor Ansatz, der auf selbstregulierende Elemente zurückgreift:
http://www.export.gov/safeharbor/doc_safeharbor_index.asp (letzter Abruf: 29.04.2007);
http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_en.htm (letzter Abruf: 29.04.2007)

[1475] vgl.: 3. Kap. Teil 2 A. I. 2; 3. Kap. Teil 2 B. I.

[1476] U.S. v. Maxwell, 45 M.J., S. 418, United States Court of Appeals for the Armed Forces, (1996); ebenso hinsichtlich der Telefonkommunikation: United States v. Sullivan, 42 M. J., S. 364, United States Court of Appeals for the Armed Forces, (1995)

Der Unterschied hinsichtlich der Reichweite der Befugnisse von Providern lässt sich damit begründen, dass -wie soeben dargestellt- in den USA anders, als im deutschen Recht, sehr auf Selbstregulierungsmaßnahmen oder den Einsatz technischer Mittel vertraut wird und diese bisweilen durchaus als Alternative zur gesetzgeberischen Tätigkeit angesehen werden. Damit muss es allerdings dem Betroffenen auch erlaubt sein, solche Mechanismen einzusetzen. So lässt sich die im Verhältnis zum deutschen Recht weitergehendere Ausnahmeregelung mit der größeren Eigenverantwortung begründen, die dem Einzelnen im US-amerikanischen Recht für den Schutz der eigenen Interessen zukommt.

C. Wertung der Lösungen und der hierdurch erzielten Folgen und rechtspolitische Forderungen

Es ist folgerichtig, die automatisierte Überprüfung von Header- und Inhaltsinformationen zuzulassen. Denn eine Kenntnisnahme durch Dritte ist nicht zu befürchten. Insofern besteht keine Gefahr für die Privatsphäre. Die Zulässigkeit des Filtereinsatzes ist auch wünschenswert, da die Provider nur so die Möglichkeit haben, ihre Kunden gegen unerwünschte sowie möglicherweise schadensverursachende elektronische Post zu schützen. Im Ergebnis wird die Privatsphäre der Kommunikationspartner durch Maßnahmen dann nicht tangiert, wenn die Kenntnisnahme von Kommunikationsinhalten und -daten durch Dritte ausgeschlossen ist.
Die Diskrepanz der Sichtweisen in den verschiedenen Staaten im Hinblick auf den Datenschutz würde sich auch nicht beseitigen lassen. Angesichts der bestehenden Rechtslage, insbesondere den gemeinschafts- und verfassungsrechtlichen Vorgaben wäre es unwahrscheinlich, dass einer der Staaten von seiner Vorstellung hinsichtlich des Schutzes der Privatsphäre bzw. des Datenschutzes abweicht und ein anderes System einführt. In Deutschland besteht hinsichtlich der Gestaltung des Datenschutzrechtes bereits deshalb kein großer Spielraum, weil die Gesetzgebung in weitem Umfang durch europäisches Sekundärrecht vorgegeben ist.[1477] Auch ist es angesichts der in den USA vorherrschenden Auffassung dahingehend, dass der freie Datenfluss für Zwecke der wirtschaftlichen Entwicklung erforderlich ist, unwahrscheinlich, dass die USA vom sektoralen Regelungsansatz zu einem umfassenden Datenschutzsystem übergehen wird,[1478] wenngleich teilweise die Forderung nach datenschutzrechtlichen Vorschriften zumindest als Ergänzung der Selbstregulierungsmaßnahmen laut wird.[1479] Als Nachteile der Selbstregulierung wird hierbei insbesondere die Schwierigkeit der Überwachung der Einhaltung der entsprechenden Standards sowie generell die fehlende Möglichkeit der Durchsetzung der vereinbarten Prinzipien angeführt.[1480] Vorteile von Selbstregulierungsmechanismen im Internet sind hingegen insbesondere darin zu sehen, dass sie international ausgestaltet werden können, also anders, als nationale Gesetze auch den im Bereich des Internet häufigen Fall erfassen können, dass Datenpakete mehrere Staaten passieren.[1481] Die Diskrepanz und die fehlende Bereitschaft insbesondere der USA, sich von einem anderen Verständnis des Datenschutzes bzw. Schutzes der Privatsphäre beeinflussen zu lassen, zeigte sich inbesondere im Rahmen der langandauernden Diskussion über den Datentransfer aus der EU in die USA. Hier greifen die Art. 25, 26 DSRL ein. Danach ist die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, aus der EU in ein Drittland nur zulässig, wenn das Drittland über ein angemessenes

[1477] vgl.: 2. Kap. Teil 2 B. II. 1. a); 2. Kap. Teil 2 A. I.
[1478] so auch: *Solove/Hoofnagle*, 2006 U. Ill. L. Rev., S. 357
[1479] ausführlich: *Cody*, Cath. U.L. Rev., S. 1223 ff.; *Heil*, DuD 2001, S. 129 f.
[1480] *Cody*, Cath. U.L. Rev., S. 1223 ff.; *Heil*, DuD 2001, S. 130
[1481] *Christiansen*, MMR 2000, S. 123; *Heil*, DuD 2001, S. 129

Dateschutzniveau verfügt. Da dies in Bezug auf die USA jedoch nicht anerkannt wurde,[1482] wurde schließlich nach längeren Verhandlungen zwischen der EG-Kommission und der US-Regierung eine Kompromisslösung gefunden. Dies führte zur Vereinbarung der so genannten Grundsätze des sicheren Haftens, die den Datenfluss in die USA für solche Unternehmen ermöglicht, die sich nach den Safe Harbor Prinzipien zertifizieren.[1483]

Teil 3: Schutz der Sicherheit und Zuverlässigkeit der Kommunikation mittels Email

Nachfolgend soll die Rechtslage in beiden Ländern hinsichtlich des Schutzes der Sicherheit und Zuverlässigkeit der Kommunikation mittels Email verglichen werden. Dabei werden zunächst die Unterschiede und Gemeinsamkeiten der Regelungen in den beiden Rechtsordnungen (A.), sodann die dafür verantwortlichen Gründe (B.) dargestellt. Im Anschluss werden die Lösungen und hierdurch erzielten Folgen wertend gegenübergestellt und die sich daraus ergebenden rechtspolitischen Forderungen aufgezeigt (C.).

A. Unterschiede und Gemeinsamkeiten

Hinsichtlich des Schutzes der Sicherheit und Zuverlässigkeit der Kommunikation mittels Email zeigen sich Unterschiede zwischen den Regelungen in den beiden Rechtsordnungen. Während es nach deutschem Recht unzulässig ist, unerwünschte Direktwerbung nach dem Eingang auf dem Empfängerserver zu löschen, sowie ihren Eingang zu blockieren, greift in den USA keine Vorschrift, die diese Vorgänge verbietet. In beiden Rechtsordnungen ist allerdings das Ausfiltern von virenbehafteten Emails zulässig.

B. Gründe für die Unterschiede bzw. Gemeinsamkeiten

Die Tatsache, dass es den Providern nach Maßgabe des US-amerikanischen Rechts möglich ist, unerwünschte Direktwerbung zu blockieren oder noch vor Zugang zu löschen, beruht auf mehreren Faktoren.

Im US-amerikanischen Recht besteht zwar grundsätzlich eine Vorschrift, die Zugriffe auf fremde Kommunikation und das Verhindern des Zugangs durch den Berechtigten zu unterbinden sucht, nämlich der Stored Communications Act. Allerdings ist einerseits das Zugreifen auf die eigene Anlage, also den eigenen Server, nicht unberechtigt, andererseits besteht eine Ausnahmevorschrift zugunsten der Provider, die diese weitgehend vom Anwendungsbereich der Norm ausnimmt.[1484] Hier zeigt sich, dass nicht etwa eine unbeabsichtigte Regelungslücke vorliegt, sondern der Gesetzgeber festschreiben wollte, dass Provider entsprechende Maßnahmen vornehmen dürfen. Die Tatsache, dass der US-amerikanische Gesetzgeber den Providern keine Vorschriften dahingehend machen wollte, dass sämtliche Emails zugestellt bzw. gespeichert werden müssen, zeigt sich auch, wenn man das Gesetzgebungsverfahren des CAN-SPAM Act betrachtet. In dessen Verlauf brachte der Senat explizit zum Ausdruck, dass der CAN-SPAM Act keine Regelung zu der Frage treffen sollte, ob Filter- oder Blockademaßnahmen durch Internet-Service-Provider zulässig sind.[1485] Dies führte zur Aufnahme des 15 U.S.C. § 7707 (c) in das Gesetz.[1486] Die Norm schreibt fest, dass der CAN-SPAM Act keine Aussage zur Frage trifft, ob Grundsätze, die Internet-Provider

[1482] zu den Staaten, denen mittlerweile ein angemessenes Datenschutznivau zugesprochen wurde: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de_htm (letzter Abruf: 29.04.2007)
[1483] vgl. dazu: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de_htm (letzter Abruf: 29.04.2007) sowie http://www.export.gov/safeharbor/sh_overview.html (letzter Abruf: 29.04.2007)
[1484] vgl.: 3. Kap. Teil 2 A. I. 1. b) bb) und cc)
[1485] S. REP. 108-102, 2004 U.S.C.C.A.N., S. 2348 ff., 2366
[1486] vgl. dazu: 3. Kap. Teil 2 A. I. 3.

in Bezug auf das Ablehnen der Übermittlung, des Routing, der Weiterleitung, der Behandlung oder des Speicherns einer bestimmten Arten von Emails annimmt, implementiert oder durchsetzt, rechtmäßig sind oder nicht. Es zeigt sich, dass der US-amerikanische Gesetzgeber keine Regelung treffen wollte, die Providern die Pflicht auferlegt, sämtliche eingehenden Nachrichten anzunehmen und zu speichern. Der Gesetzgeber ist auch nicht unter dem Blickwinkel der durch den ersten Verfassungszusatz geschützten Meinungsfreiheit verpflichtet, entsprechende Vorgehensweisen von Providern zu verhindern. Dies ergibt sich einerseits, wie bereits dargestellt,[1487] daraus, dass eine Verpflichtung des Gesetzgebers zum Tätigwerden in den USA nur dann besteht, wenn die Person oder das Unternehmen, das den Filter einsetzt, eine staatliche Behörde ist,[1488] der Email-Server als öffentliches Forum anzusehen ist oder zwar eine private Handlung vorliegt, diese aber dem Staat als so genannte „state action" zuzurechnen ist.[1489] Wie bereits dargestellt liegen diese Voraussetzungen nicht vor.[1490] Demnach besteht hier weder eine staatliche Verpflichtung zum Tätigwerden, noch eine Beeinträchtigung des Grundrechts durch die Untätigkeit.

Darüber hinausgehend könnte der Filtereinsatz -gesetzt den Fall, es würde ein staatlicher Rechtsträger tätig- unter Zugrundelegung des Central-Hudson-Tests zulässig sein. Wäre dies zu bejahen, so ergäbe sich im Wege des Erst-Recht-Schlusses, dass auch die entsprechenden Maßnahmen privater Provider nicht aus verfassungsrechtlichen Gründen zu verbieten sind, da Private keiner Grundrechtsbindung unterliegen und an sie damit keine strengeren Anforderungen gestellt werden, als an staatliche Rechtsträger.
Wesentliche Interessen im Sinne des Central-Hudson-Tests wären hier einerseits der Schutz der Rechte der Email-Nutzer vor unerwünschter Email-Direktwerbung, andererseits die Server-Effizienz.[1491] Es bestehen auch keine Zweifel daran, dass die Blockade unerwünschter Emails diese Interessen fördert,[1492] da hierdurch eine Entlastung des Servers bewirkt wird, der weniger Informationen zu verarbeiten hat und sich die Empfänger der Nachrichten nicht mit von ihnen unerwünschten Emails auseinandersetzen müssen. Daneben setzt der Central-Hudson-Test voraus, dass die Regelung nicht weitgehender als erforderlich ist.[1493] Soweit nur bestimmte Emails blockiert werden und die Blockade nicht spezifische Inhalte betrifft, ist in Bezug auf den Schutz der Interessen der Empfänger davon auszugehen, dass die Regelung nicht zu weitgehend ist. Gegen das Vorliegen eines zu weitgehenden Eingriffs spricht, dass es für Provider möglich sein muss, die Privatsphäre der Email-Nutzer vor Nachrichten zu schützen, die diese nicht erhalten möchten. Ein milderes Mittel, als der Einsatz von Filtersoftware ist nicht ersichtlich, insbesondere kann ein solches nicht darin gesehen werden, die Empfänger zum manuellen Aussortieren zu zwingen, weil dies wieder die unerwünschte Verlagerung von Kosten und Zeitaufwand auf den Empfänger zur Folge hätte. In Bezug auf die Server-Effizienz wurden allerdings Zweifel daran geäußert, ob der Einsatz eines Filters mit der Folge der Blockade bestimmter Emails nicht zu weitgehend ist, da eine zeit- oder volumenrestringierte Annahme dieser Emails möglicherweise als milderes Mittel anzusehen

---

[1487] vgl.: 3. Kap. Teil 2 B. I.
[1488] vgl. den ersten Verfassungszusatz der auszugsweise lautet: Congress shall make no law…"; zur Anwendbarkeit des ersten Verfassungszusatzes auch auf andere Zweige als die Legislative: Rust et al. v. Sullivan, 500 U.S., S. 173, 111 S. Ct., S. 1759, Supreme Court of the United States, (1991); U.S. West, Inc. v. F.C.C., 182 F.3d, S. 1232, United States Court of Appeals, Tenth Circuit, (1999)
[1489] vgl.: 3. Kap. Teil 2 B. I.
[1490] vgl.: 3. Kap. Teil 2 B. I.
[1491] White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, S. 366 ff., United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006)
[1492] White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, S. 366 ff., United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006)
[1493] vgl.: 3. Kap. Teil 1 B. I. 3.

sei.[1494] Hiergegen spricht allerdings, dass Emails aufgrund der Zeitverschiebung und der Möglichkeit der internationalen sowie automatisierten Versendung immer eingehen werden, nicht nur während der Arbeitszeit. Insofern werden auch außerhalb der Arbeitszeit eingehende kommerzielle Emails den Eingang legitimer Nachrichten beeinträchtigen. Darüber hinaus werden auch so Kosten vom Versender auf den Provider und die Empfänger übertragen. Es ist kein Grund dafür ersichtlich, den Kostenaufwand, den sich der Versender der entsprechenden Nachrichten erspart, dem Empfänger sowie seinem Provider aufzuerlegen. Anders, als in dem Fall, in dem ein Gesetz vollumfänglich die Unzulässigkeit einer bestimmten Art von Emails ausspricht, ist bei einem Provider, der zugleich staatlicher Rechsträger ist, kein Mittel ersichtlich, welches das verfolgte Interesse ebenso effizient realisiert, wie der Einsatz eines Email-Filterprogramms. Im Ergebnis ist davon auszugehen, dass die Email-Filterung durch einen Provider, der gleichzeitig eine staatliche Behörde ist, nicht gegen das Grundrecht der Meinungsäußerungsfreiheit verstößt.[1495] Danach können selbst Provider, die zugleich staatliche Rechtsträger und damit in vollem Umfang an den ersten Verfassungszusatz gebunden sind, unerwünschte Emails blockieren oder anderweitig ausfiltern und zwar auch dann, wenn diese nach Maßgabe des CAN-SPAM Acts legal sind.[1496] Anders, als staatliche Rechtsträger unterliegen jedoch private Provider und Unternehmen nicht den strengen Anforderungen des Grundrechts auf freie Meinungsäußerung.[1497] Wenn es jedoch selbst staatlichen Behörden zugestanden wird, zum Schutz der Interessen der Email-Nutzer selbst legale Emails nach vordefinierten Kriterien auszufiltern, so muss dies privaten Rechtsträgern, die an das Grundrecht der Meinungsfreiheit nicht gebunden sind, erst Recht möglich sein.
Aufgrund dieser Tatsache und der fehlenden gesetzgeberischen Schutzpflicht besteht im US-amerikanischen Recht kein Anlaß, gesetzliche Vorgaben zu treffen, die zur Zustellung sämtlicher eingehender Emails verpflichten. Hier besteht damit weder eine Verpflichtung, noch eine Veranlassung des Gesetzgebers, gesetzliche Vorschriften zu erlassen, die die Möglichkeit des Filtereinsatzes restringieren. Dies ist der Grund warum sich im US-amerikanischen Recht keine Regelung findet, wie dies etwa im deutschen Recht der Fall ist.
Dort unterliegt der Gesetzgeber der Verpflichtung, zum Schutz der Grundrechte auch gegen Beeinträchtigungen durch Private tätig zu werden.[1498] Es besteht ein gesetzlicher Schutz versandter und auf dem Empfänger-Server eingegangener Emails durch die §§ 206 Abs. 2 Nr. 2, 303 a Abs. 1 StGB. Die erstgenannte Vorschrift erfasst das Interesse des Betroffenen am Umgang mit Sendungen und das öffentliche Vertrauen in die Sicherheit und Zuverlässigkeit des Post- und Fernmeldeverkehrs, die zweitgenannte möchte der Beschädigung und Zerstörung nicht unmittelbar wahrnehmbar gespeicherter Daten entgegenwirken.[1499] Der Schutz elektronischer Nachrichten wird so umfassend gewährleistet. Die Tatsache, dass in Deutschland virenbehaftete Emails ausgefiltert werden dürfen, beruht darauf, dass hier das Interesse an der Zustellung hinter das Interesse am Schutz des Eigentums sowie anderer bedrohter Rechtsgüter zurückzutreten hat.[1500]

[1494] White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, S. 377, United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006)
[1495] White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, S. 366 ff., United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006)
[1496] White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F. 3d, S. 366 ff., United States Court of Appeals, Fifth Circuit, (2005), das gegen das Urteil gerichtete Rechtsmittel zum Supreme Court (petition for writ of certiorari) wurde zurückgewiesen, vgl. 126 S. Ct., S. 1039, Supreme Court of the United States, (2006); vgl. auch: 15 U.S.C. § 7707 (c)
[1497] vgl.: 3. Kap. Teil 2 B. I.
[1498] vgl.: 2. Kap. Teil 2 B. I. 2. c)
[1499] vgl.: 2. Kap. Teil 2 A. III. 2.; 2. Kap. Teil 1 A. I.
[1500] vgl.: 4. Kap. Teil 1

C. Wertung der Lösungen und der hierdurch erzielten Folgen und rechtspolitische Forderungen

Fraglich ist, wie sich die in den beiden Rechtsordnungen getroffenen Regelungen in ihren Auswirkungen unterscheiden, insbesondere, wie sie das Verhalten des Einzelnen in die eine oder andere Richtung zu beeinflussen vermögen und ob die tatsächlichen Folgen der Regelungen erwünscht sind.

Die übereinstimmende Zulässigkeit des Ausfilterns von Viren ist folgerichtig, da nur so der Provider bzw. das Unternehmen sein Eigentum bzw. das Eigentum der Email-Nutzer vor Schäden bewahren können.
Fraglich ist, wie die Rechtslage im Bereich der Spamfilterung zu beurteilen ist. Unproblematisch erscheint die Tatsache, dass im deutschen Recht der Subjektzeile kein Vermerk angefügt werden kann, denn die Filter können so eingestellt werden, dass sie die Spam-Wahrscheinlichkeit anders darstellen. Daneben ist allerdings Folge der im deutschen Recht geltenden Vorschriften, dass Unternehmen, die Telekommunikationsdienstleistungen erbringen, grundsätzlich nicht dazu berechtigt sind, die Kommunikation gänzlich zu unterbinden.[1501] Eine solche Berechtigung besteht selbst dann nicht, wenn der Adressat der betroffenen Nachricht vor der Maßnahme seine Einwilligung erklärt hat.[1502] Vielmehr ist es nach der bisher existenten Rechtsprechung erforderlich, dass auch der Absender eingewilligt hat, was grundsätzlich nicht der Fall sein wird. Filterprogramme, die den Zugang von Nachrichten unterbinden, die als Spam identifiziert wurden, können demnach nach Maßgabe des deutschen Rechts nicht eingesetzt werden. Dies bedeutet, dass der Zugang elektronischer Post in der Regel zu bewerkstelligen ist. Danach kann der Absender den Adressaten faktisch durch Verweigern der Einwilligung in das Ausfiltern der entsprechenden Email dazu zwingen, die elektronische Kommunikation entgegenzunehmen. Da jedoch ein Anspruch des Adressaten dahingehend besteht, von unerwünschter elektronischer Direktwerbung frei zu bleiben,[1503] steht dieses Ergebnis im Widerspruch zu den Rechten des Empfängers. Mit diesen geht einher, dass der Adressat die Annahme entsprechender Kommunikation verweigern oder aber bereits den Übermittler anweisen kann, diese nicht zuzustellen.[1504] Somit sollte es im Bereich des elektronischen Direktmarketing möglich sein, unerwünschte Emails zurückzuweisen, wenn der Adressat seine Einwilligung mit der Maßnahme erklärt hat. Dem steht auch nicht der Schutzzweck der betroffenen Norm entgegen.[1505] Denn letztlich können die Versender von Werbe-Emails nicht darauf vertrauen, dass sämtliche oder eine bestimmte Anzahl der von ihnen versandten Emails tatsächlich zugehen. Dies ist bereits deshalb unwahrscheinlich, da die Email-Adressen teilweise generiert werden, so dass beim Versenden der Werbe-Nachrichten grundsätzlich nicht feststeht, ob diese überhaupt eine existente Adresse erreichen. Ein Vertrauen der Allgemeinheit in die Zustellung von Spammails kann aus diesem Grund nicht angenommen werden.
Hingegen betrifft das Ausfiltern von legitimen Nachrichten das Vertrauen in die Störungsfreiheit der Kommunikation. Insofern erscheint es auf den ersten Blick gerechtfertigt, die Einwilligung des Absenders zu verlangen, die jedoch grundsätzlich nicht vorliegen wird. Zugunsten der deutschen Lösung spricht demnach, dass die fraglichen Maßnahmen nicht stets lediglich Spammails betreffen, sondern bisweilen auch legitime Emails, die positiv gescannt wurden. Fragwürdig ist jedoch, ob es allein der Schutz der legitimen Email-Korrespondenz bzw. des Vertrauens in diese es rechtfertigt, den Provider zur Zustellung sämtlicher -auch

[1501] vgl.: 2. Kap. Teil 2
[1502] vgl.: 2. Kap. Teil 2
[1503] vgl.: 2. Kap. Teil 1
[1504] vgl.: 2. Kap. Teil 1
[1505] vgl.: 2. Kap. Teil 2 A. III. 2.

spam-verdächtiger- Emails zu verpflichten und zwar selbst dann, wenn der Empfänger seine Einwilligung dahingehend erklärt hat, dass das Einstellen spamverdächtiger Emails in die Mailbox unterbleibt. Die Verpflichtung zur Zustellung sämtlicher -auch unerwünschter- Emails führt nicht nur zu einem erheblichen Aufwand an Speicherkapazitäten und Kosten auf Seiten der Provider, sondern auch dazu, dass die Adressaten gezwungen werden, die betreffenden Nachrichten entgegenzunehmen und somit ihrerseits Zeit und Ressourcen für das Aussortieren der fraglichen Emails aufzuwenden. Die Möglichkeit, Emails lediglich zu markieren oder in spezielle Ordner einzustellen, hat dabei gegenüber dem Abbrechen der Verbindung vor Eingehen bzw. dem Löschen der Email vor dem Einstellen in die Mailbox den Nachteil, dass dennoch Speicherkapazitäten sowie Rechnerleistung für die Verarbeitung aufgewendet werden müssen. Die hierfür entstehenden Kosten werden durch die Provider an ihre Kunden weiterbelastet.[1506]
Im Übrigen ist der Zweck der im Raum stehenden Norm des § 206 Abs. 2 Nr. 2 StGB zu berücksichtigen, das Vertrauen in die Sicherheit des Post- und Fernmeldeverkehrs zu schützen. Dabei geht mittlerweile von dem zunehmenden Volumen an Spammails ebenfalls eine Gefahr für das Vertrauen in die Sicherheit des Kommunikationsmediums Email aus.[1507]
Der Vertrauensverlust durch diese Entwicklung dürfte ebenso groß sein, wie derjenige, der eintritt, wenn aufgrund des Filtereinsatzes fälschlicherweise Emails vereinzelt nicht zugestellt werden. Insofern lässt sich aus dem US-amerikanischen Recht die Lehre ziehen, dass den Übermittlungsunternehmen im Bereich der elektronischen Kommunikation größere Befugnisse eingeräumt werden müssen. Diese dürfen allerdings -aufgrund der verfassungsrechtlich gewährleisteten Rechte auf informationelle Selbstbestimmung und des Fernmeldegeheimnisses- lediglich das Übermittlungsrisiko betreffen. Ein Recht der Einblicknahme in die eingehenden Emails durch Angestellte des Providers oder Unternehmens kann daher nicht gesetzlich festgeschrieben werden. Dies ist aber auch nicht notwendig, da die Filtersoftware nicht zu einer Kenntnisnahme durch diese Personen führt. Die Zustellung legitimer Emails lässt sich weitgehend durch Maßnahmen der Kommunikationspartner schützen. So kann der Empfänger den Absender auf eine weiße Liste setzen,[1508] während der Absender eine Funktion in seinem Email-Programm aktivieren kann, die ihm bei Zustellung der Nachricht eine Bestätigung zukommen lässt. Es zeigt sich also, dass die Teilnehmer einer legitimen Email-Kommunikation den Kommunikationsvorgang durch verhältnismäßig einfache Mittel gewährleisten können, während eine Verpflichtung zur Zustellung sämtlicher Emails, auch wenn der Empfänger diese nicht einmal erhalten möchte, für den Empfänger, dessen Provider und das gesamte Netzwerk nachteilhafte Folgen hat. Darüber hinaus läuft so das Recht des Adressaten darauf, unerwünschte Kommunikation vor ihrem Erhalt abzulehnen, leer.
Nach Maßgabe des US-amerikanischen Rechts können Filter, die bestimmte Emails von vorneherein ablehnen, hingegen rechtmäßigerweise eingesetzt werden. Hieraus folgt, dass die Absender legitimer Emails eigene Maßnahmen treffen müssen, um den Zugang der Nachricht sicherzustellen bzw. zu erfahren, ob dieser erfolgt ist. Dies ist allerdings einfach möglich, indem eine Funktion des Email-Programms aktiviert wird, die bewirkt, dass eine Zugangsbestätigung erfolgt bzw. der Adressat der Email um kurze Rückbestätigung gebeten wird. Seitens des Adressaten ist es zudem möglich, den Empfänger auf eine weiße Liste zu setzen. Ein Vorteil der US-amerikanischen Regelung ist darin zu sehen, dass der Filtereinsatz unbeschränkt und unabhängig davon erfolgen kann, ob auch die Absender der Nachrichten ihre Einwilligung erklärt haben. Auch ist es grundsätzlich irrelevant, wenn fälschlicherweise legitime Nachrichten von den Filterprogrammen erfasst werden. Deshalb verfügt der Provider nach Maßgabe des US-amerikanischen Rechts über einen weiteren Handlungsspielraum, der

[1506] *Alongi*, 46 Ariz. L. Rev., S. 277
[1507] *Spindler/Ernst*, CR 2004, S. 437; 15 U.S.C. § 7701 (a) (4)
[1508] vgl.: 1. Kap. Teil 2 A. I.

es ihm ermöglicht, das Netzwerk sowie die Kunden vor unerwünschten Nachrichten zu schützen. Der Absender unerwünschter Email-Direktwerbung kann so nicht de facto den Adressaten zwingen, die Email entgegenzunehmen. Demnach kann letztlich jede Art von Filter eingesetzt werden. Somit ist das US-amerikanische System insofern gegenüber dem deutschen vorzugswürdig, als es den Providern das Recht einräumt, Emails bereits im Vorfeld zu blockieren oder zu löschen. Generell ist zu fordern, dass im deutschen Recht ebenfalls eine Situation geschaffen wird, die es den Providern- zumindest in Bezug auf solche Absender oder eine Gruppe von Absendern, die der Adressat bezeichnet hat- ermöglicht, die Annahme von Emails zu verweigern.

Fraglich ist, wie diese Situation hergestellt werden kann.
Die Aufnahme einer weitgehenden Ausnahmeregelung zugunsten der Provider ähnlich der Vorschriften des Stored Communications oder des Wiretap Act kommt im deutschen Recht nicht in Betracht. Denn diese Ausnahmebestimmungen würden gerade dem eindeutigen Sinn und Zweck des § 206 Abs. 2 Nr. 2 StGB, vor dem Zugriff der Übermittlungsperson zu schützen, widersprechen.
Denkbar wäre, im Hinblick auf das Einwilligungserfordernis auch des Absenders dahingehend zu differenzieren, dass dieses nur besteht, wenn eine legitime Email vorliegt. Daneben bestünde die Möglichkeit, das Merkmal des Anvertrautseins nur dann zu bejahen, wenn eine legitime Email betroffen ist. Eine derartige Differenzierung innerhalb ein- und desselben Tatbestandes erscheint allerdings inkonsequent und deshalb rechtspolitisch wenig wünschenswert. Mit einer solchen Differenzierung wäre auch den Providern wenig geholfen, da für diese -angesichts der Tatsache, dass die Filterung automatisiert durch ein entsprechendes Computerprogramm erfolgt- nicht erkennbar wäre, ob sie eine Einwilligung benötigen bzw. ob ihnen die Nachricht anvertraut ist. Deshalb sollte eine einheitliche Lösung gefunden werden.
Das gewünschte Ergebnis lässt sich erzielen, indem im Rahmen des § 206 Abs. 2 Nr. 2 StGB nicht gefordert wird, dass auch der Absender in die Maßnahme einwilligt. Diese Rechtslage kann bereits dadurch geschaffen werden, dass die Rechtsprechung zur Frage des Einwilligungserfordernisses geändert wird. Möglich erscheint auch das Einfügen einer klarstellenden Passage in die Vorschrift durch den Gesetzgeber.
Daneben sollte auch kein Verstoß gegen § 303 a Abs. 1 StGB vorliegen, wenn bereits auf dem Empfänger-Server eingegangene, aber noch nicht in die Mailbox eingestellte Nachrichten gelöscht werden, sofern der Adressat in die Spamfilterung eingewilligt hat. Zu diesem Zweck kann eine klarstellende Passage in die Vorschrift eingefügt werden. Dies ist ohnehin aufgrund der oben dargestellten Auslegungsschwierigkeiten wünschenswert. Letztlich ist -wie gezeigt wurde- das Interesse des Absenders an der Verfügungsberechtigung hinsichtlich der in der versandten Email enthaltenen Daten gar nicht beeinträchtigt. Denn der Absender behält in aller Regel die Originalversion der Email, während er lediglich die Kopie aus seiner Verfügungsbefugnis entlässt und an den Adressaten schickt. Insofern ist ein strafrechtlicher Schutz im Hinblick auf die Übermittlung nicht erforderlich. Letztlich sollte es -angesichts der beschriebenen Nachteile von Spammails- den Providern möglich sein, die Zustellung von Nachrichten abzulehnen, die unter Spamverdacht stehen. Für die Kommunikationspartner ist es einfach möglich, die Zustellung zu gewährleisten. Die eingefügte Passage könnte beispielsweise Daten, bei denen es sich lediglich um eine Kopie handelt oder bei denen der Absender dadurch, dass er Daten versandt, aber keine eigene Kopie zurückbehalten hat, gezeigt hat, dass an der Unversehrtheit der Daten kein Interesse besteht, von der Strafbarkeit ausnehmen. In diesem Fall greift auch der Sinn und Zweck des § 303 a StGB nicht ein, der darin besteht, das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit

der in den gespeicherten Daten enthaltenen Informationen zu schützen.[1509] Denn wenn der Absender die Möglichkeit hat, sich Orginaldaten zurückzubehalten, ist sein Interesse am Erhalt der Kopie nicht schutzwürdig. Sind bereits in die Mailbox des Empfängers eingestellte Nachrichten von den entsprechenden Maßnahmen betroffen, so bestehen keine größeren Probleme, da der Provider einfach durch Einholen der Einwilligung des Empfängers bzw. durch das Festschreiben eines bestimmten Höchstspeichervolumens oder einer Speicherfrist einem strafrechtlichen Vorwurf entgehen kann. Es sollte ein expliziter Hinweis seitens des Providers erfolgen, dass möglicherweise auch legitime Nachrichten von der Maßnahme erfasst werden können. Dies wird bereits praktiziert.[1510]

[1509] vgl.: BT-Drs.10/5058, S. 34; ebenso: *Stree* in Schönke/Schröder, § 303 a StGB, Rn. 1; a.A.: *Haft*, NStZ 1987, S. 6 ff., 10

[1510] vgl. etwa: http://privacy2.msn.com-anti-spam.aspx?cp-documentid=85690&wa=wsignin1.0 (letzter Abruf: 29.04.2007); http://about.aol.com/aolnetwork/aolcom_terms (letzter Abruf: 29.04.2007)

Ergebnisse

I.

Email ist eines der weltweit meistgenutzten Kommunikationsmedien. Die Vorteile der elektronischen Post liegen vor allem in ihrer Geschwindigkeit und Kostengünstigkeit. Diese Vorteile werden allerdings durch das Aufkommen an Emails geschmälert, die zum Zwecke der Direktwerbung versandt werden. Virenbehaftete Emails können erhebliche Schäden am Rechner des Empfängers oder auf dem Server verursachen. Deshalb setzen Email-Service-Provider und Unternehmen, die ihren Angestellten ein Email-Netz zur Verfügung stellen, Email-Filtersoftware ein, um unerwünschte oder virenbehaftete Nachrichten bereits vor oder spätestens bei ihrem Eingang erkennen und abwehren zu können. Dabei gibt es inzwischen verschiedene Filterverfahren. Diesen ist gemeinsam, dass eingehende Emails auf bestimmte Merkmale in ihrem Text oder Header überprüft und anschließend anhand der gefundenen Kriterien als erwünscht oder unerwünscht qualifiziert werden. Als unerwünscht erkannte Emails werden sodann von dem Programm gelöscht, blockiert, als kommerzielle Email markiert oder aber in spezielle Quarantäne-Ordner im Email-Postfach des Empfängers umgeleitet. Die Zulässigkeit der verschiedenen Vorgänge, die aufgrund des Filtereinsatzes ablaufen nach Maßgabe des deutschen und US-amerikanischen Rechts, ist Gegenstand dieser Arbeit. Als Vorfrage war darauf einzugehen, wie die rechtliche Zulässigkeit von Email-Werbung in den beiden Rechtsordnungen zu beurteilen ist.

II.

1. Die Rechtslage hinsichtlich der Zulässigkeit unverlangter Email-Werbung in den beiden Staaten unterscheidet sich in zwei Punkten. Einerseits gilt in Deutschland der lediglich durch § 7 Abs. 3 UWG abgeschwächte Grundsatz, dass Email-Werbung nur mit vorheriger Einwilligung des Empfängers zulässig ist. In den USA findet hingegen das Opt-Out-Prinzip Anwendung. Darüber hinaus erfassen im deutschen Recht die deliktsrechtlichen Vorschriften auch nicht-kommerzielle Emails, während den einschlägigen Vorschriften in den USA lediglich solche Nachrichten unterfallen, deren primärer Zweck kommerzieller Natur ist.

2. Dabei basieren die verschiedenen Lösungen auf einer unterschiedlichen Sicht der im Raum stehenden Rechtspositionen, insbesondere auch aufgrund der jeweiligen verfassungsrechtlichen Rahmenbedingungen in den beiden Staaten. In Deutschland, wie in der gesamten EU, wird der Privatsphäre des von Email-Werbung Betroffenen der Vorrang vor den Interessen des Werbetreibenden an einem ohne vorherige Einwilligung des Adressaten erfolgenden Versand von Werbe-Emails und vor den Interessen etwaiger an der Werbung interessierter Empfänger eingeräumt. Die Regelung in den USA erklärt sich hingegen, wenn man sich die große Bedeutung vor Augen führt, die dort dem Grundrecht der Meinungsfreiheit zukommt. Dieses wird als essentielle Voraussetzung der politischen und sozialen Entwicklung der Bürger und damit als Grundlage aller anderen Grundrechte angesehen. Dabei erfasst die Meinungsfreiheit auch die kommerzielle Rede, wenngleich der Schutzumfang im Vergleich zur nicht-kommerziellen Rede geringer ist. Der Gesetzgeber darf die Meinungsfreiheit nicht zu weitgehend einschränken. Deshalb hatte der US-amerikanische Gesetzgeber vorsichtig vorzugehen und schrieb folglich lediglich eine Opt-Out-Lösung, keine Opt-In-Lösung fest.

3. Rechtspolitisch erscheint die in Deutschland gewählte Lösung gegenüber dem Opt-Out-Prinzip als vorzugswürdig. Allerdings ist angesichts der verfassungsrechtlichen Rahmenbedingungen in den USA davon auszugehen, dass das Opt-In-System dort nicht

umgesetzt werden wird, da die Lösung der in der USA vorherrschenden Auffassung widersprechen würde, die die freie -auch kommerzielle- Meinungsäußerung als eine Grundbedingung der sozialen und wirtschaftlichen Entwicklung begreift.
Generell stellt sich das Problem, dass sich die Spamproblematik allein durch nationale Vorgaben nicht in den Griff bekommen lassen wird. Folglich sind international bindende Regelungen, eine internationale Zusammenarbeit im Bereich der Spambekämpfung sowie der Einsatz technischer Mittel unumgänglich.

III.

1. Im deutschen Recht ist das Überprüfen von Inhalt und Headerinformationen durch die Filtersoftware zulässig, da keine natürliche Person von den entsprechenden Daten Kenntnis erlangen kann. Auch nach Maßgabe des US-amerikanischen Rechts ist der Einsatz der Filtersoftware rechtmäßig, da kein Verschaffen von Kommunikationsinhalten vorliegt und im Übrigen bei der Versendung von Emails keine berechtigte Erwartung der Privatheit besteht.

2. In beiden Rechtsordnungen ergibt sich das gleiche Ergebnis, wenngleich dem Datenschutz bzw. dem Schutz der Privatsphäre in den beiden Staaten nicht der gleiche Stellenwert zukommt. Während Deutschland wie auch die europäische Gemeinschaft auf ein möglichst hohes Datenschutzniveau abzielen, bestehen in den USA Vorbehalte gegen einen zu stark ausgeprägten Datenschutz. Trotz der unterschiedlichen Auffassungen kommen beide Rechtsordnungen zu demselben Ergebnis. Diese Übereinstimmung beruht darauf, dass die Privatsphäre in Gestalt der informationellen Selbstbestimmung hier nicht beeinträchtigt wird, da eine Kenntnisnahme von Inhalten oder Daten aufgrund des Filtereinsatzes praktisch ausgeschlossen ist.

3. Es ist folgerichtig, die automatisierte Überprüfung von Header- und Inhaltsinformationen zuzulassen, da eine Kenntnisnahme durch Dritte nicht zu befürchten ist. Eine Gefahr für die Privatsphäre besteht insofern nicht. Daneben ist die Zulässigkeit des Filtereinsatzes wünschenswert, da die Provider nur so die Möglichkeit haben, ihre Kunden gegen unverlangte elektronische Post zu schützen. Beide Rechtsordnungen kommen zu dem identischen Ergebnis. Angesichts der bestehenden Rechtslage, insbesondere auch der gemeinschafts- und verfassungsrechtlichen Vorgaben wäre es unwahrscheinlich, dass einer der Staaten von seiner Vorstellung hinsichtlich des Schutzes der Privatsphäre sowie des Datenschutzes abweicht und ein anderes System einführt.

IV.

1. Hinsichtlich des Schutzes der Sicherheit und Zuverlässigkeit der Kommunikation mittels Email zeigen sich Unterschiede zwischen den Regelungen in den beiden Rechtsordnungen. Während es nach deutschem Recht unzulässig ist, unerwünschte kommerzielle Nachrichten nach dem Eingang auf dem Empfängerserver zu löschen, sowie ihren Eingang zu blockieren, sind die Vorgänge in den USA rechtmäßig. Das Löschen von virenbehafteten Emails ist hingegen nach Maßgabe der in beiden Rechtsordnung geltenden Vorschriften zulässig.

2. Im US-amerikanischen Recht besteht grundsätzlich eine Vorschrift, die Zugriffe auf fremde Kommunikation und das Verhindern des Zugangs durch den Berechtigten verbietet, allerdings hat der Gesetzgeber hiervon bewußt Provider sowie den berechtigten Zugriff auf das eigene System ausgenommen. Die verfassungsrechtlichen Rahmenbedingungen erfordern auch kein Tätigwerden des Gesetzgebers. Dies folgt einerseits daraus, dass der Zugriff durch Private

erfolgt, jedoch die Grundrechte der US-Verfassung keine Schutzpflicht für den Gesetzgeber begründen. Der Email-Server ist auch kein öffentliches Forum, so dass auch nicht aus einer etwaigen öffentlichen Funktion das Eingreifen des Grundrechts hergeleitet werden kann. Im Übrigen wäre selbst das Ausfiltern von Emails durch einen Provider, der gleichzeitig staatlicher Rechtsträger ist, zulässig, obwohl dieser im Gegensatz zu Privaten an das Grundrecht der Meinungsfreiheit gebunden ist. Die Voraussetzungen des Central-Hudson-Tests liegen auch bei einem staatlichen Provider vor, da kein milderes Mittel ersichtlich ist, um den Schutz der Email-Nutzer und der Server-Effizienz zu gewährleisten. Wenn jedoch selbst Provider, die zugleich staatliche Rechtsträger und damit in vollem Umfang an den ersten Verfassungszusatz gebunden sind, unerwünschte Emails blockieren oder anderweitig ausfiltern können, und zwar auch dann, wenn diese nach Maßgabe des CAN-SPAM Act legal sind, so muss dies privaten Rechtsträgern, die das Grundrecht der Meinungsfreiheit nicht zu beachten haben, erst Recht möglich sein. Aufgrund dieser Tatsachen bestand im US-amerikanischen Recht kein Anlaß, gesetzliche Vorgaben zu treffen, die private Provider zur Zustellung sämtlicher eingehender Emails verpflichten.
Der deutsche Gesetzgeber unterliegt hingegen grundsätzlich der Verpflichtung die im Grundgesetz gewährleisteten Grundrechte auch gegen Beeinträchtigungen durch Private zu sichern. Hier wurde er sowohl zum Schutz von Allgemein- oder Individualinteressen tätig. Deshalb besteht im deutschen Recht ein strafrechtlicher Schutz versandter und auf dem Empfänger-Server eingegangener Emails durch die §§ 206 Abs. 2 Nr. 2, 303 a Abs. 1 StGB. Eine Rechtfertigung gemäß §§ 109 TKG, 34 StGB kommt erst dann in Betracht, wenn die geschützten Interessen diejenigen der Absender der betroffenen Nachrichten bei weitem überwiegen. Dies ist bei dem Versand der Spammails grundsätzlich nicht der Fall, solange nicht gezielt ein Server so attackiert wird, dass mit seinem Ausfall zu rechnen ist. Virenbehaftete Emails können hingegen gelöscht werden, da diese eine Gefahr für die IT-Infrastruktur und Rechtsgüter des Providers bzw. Unternehmers oder aber der Empfänger darstellen und keine berechtigte Zustellungserwartung besteht.

3. Nach Maßgabe des deutschen Rechts sind danach Unternehmen, die Telekommunikationsdienstleistungen erbringen, grundsätzlich nicht dazu berechtigt, zum Zweck des Schutzes vor unerwünschter Direktwerbung die Kommunikation gänzlich zu unterbinden. Eine solche Berechtigung besteht selbst dann nicht, wenn der Adressat der betroffenen Nachricht vor der Maßnahme seine Einwilligung erklärt hat. Vielmehr ist es erforderlich, dass auch der Absender eingewilligt hat, was grundsätzlich nicht der Fall sein wird. Wünschenswert ist allerdings, dass der Filtereinsatz zulässig ist, wenn der Adressat eingewilligt hat. Denn die Verpflichtung zur Zustellung sämtlicher auch unerwünschter Emails führt nicht nur zu einem erheblichen Speicheraufwand seitens des Providers, sondern auch dazu, dass die Adressaten gezwungen werden, die betreffende Nachricht entgegenzunehmen, obwohl sie grundsätzlich einen Anspruch darauf haben, von unerwünschter Werbung freizubleiben.
Nach Maßgabe des US-amerikanischen Rechts können Filter, die bestimmte Emails von vorneherein ablehnen hingegen rechtmäßigerweise eingesetzt werden. Hieraus folgt allerdings, dass die Absender legitimer Emails eigene Maßnahmen treffen müssen, um den Zugang der Nachricht sicherzustellen bzw. zu erfahren, ob dieser erfolgt ist. Dies ist einfach möglich, indem eine Funktion des Email-Programms aktiviert wird, die bewirkt, dass eine Zugangsbestätigung erfolgt. Seitens des Adressaten ist es zudem möglich, den Empfänger auf eine weiße Liste zu setzen. Der Vorteil der US-amerikanischen Regelung liegt insofern darin, dass der Filtereinsatz unbeschränkt und unabhängig davon erfolgen kann, ob auch die Absender der Nachrichten ihre Einwilligung erklärt haben. Auch ist es -zumindest in den Fällen, in denen der Provider auf den Einsatz des Spamfilters hingewiesen hat- irrelevant, wenn fälschlicherweise legitime Nachrichten von den Filterprogrammen erfasst werden.

Generell ist zu fordern, dass im deutschen Recht ebenfalls eine Situation geschaffen wird, die es den Providern- zumindest in Bezug auf solche Absender oder eine Gruppe von Absendern, die der Adressat bezeichnet hat- ermöglicht, die Annahme von Emails zu verweigern. Dieses Ergebnis lässt sich erzielen, wenn im Rahmen des § 206 Abs. 2 Nr. 2 StGB nicht gefordert wird, dass auch der Absender in das Löschen bzw. die Blockade einwilligt. Möglich erscheint auch das Einfügen einer klarstellenden Passage in die Vorschrift durch den Gesetzgeber. Daneben sollte auch kein Verstoß gegen § 303 a Abs. 1 StGB vorliegen, wenn bereits auf dem Empfänger-Server eingegangene, aber noch nicht in die Mailbox eingestellte Nachrichten gelöscht werden, sofern der Adressat in die Spamfilterung eingewilligt hat. Zu diesem Zweck kann eine klarstellende Passage in die Vorschrift eingefügt werden. Die eingefügte Passage könnte beispielsweise Daten, bei denen es sich lediglich um eine Kopie handelt oder bei denen der Absender dadurch, dass er Daten versandt, aber keine eigene Kopie zurückbehalten hat, gezeigt hat, dass an der Unversehrtheit der Daten kein Interesse besteht, von der Strafbarkeit ausnehmen. Die Zulässigkeit des Löschens von virenbehafteten Emails ist folgerichtig, da nur so ein effektiver Schutz gegenüber Schädigungen möglich ist.

Literaturverzeichnis

Ahrens, Hans-Jürgen, Das Herkunftslandprinzip in der E- Commerce-Richtlinie, CR 2000, S. 835 ff.

Alexy, Robert, Theorie der Grundrechte, Baden- Baden, 1984

Alongi, Elizabeth, Has the U.S. Canned Spam?, 46 Ariz. L. Rev., S. 263 ff. (2004)

Alt, Wilfried, Die Zusendung von Werbematerialien trotz Widerspruchs des Umworbenen, NJW 1986, S. 1597 ff.

Altenburg, Stephan/ v. Reinersdorff, Wolfgang/ Leister, Thomas, Telekommunikation am Arbeitsplatz, MMR 2005, S. 135 ff.

Dies., Betriebsverfassungsrechtliche Aspekte der Telekommunikation am Arbeitsplatz, MMR 2005, S. 222 ff.

Amelung, Knut/ Pauli, Gerhard, Einwilligung und Verfügungsbefugnis bei staatlichen Beeiträchtigungen des Fernmeldegeheimnisses iSd Art. 10 GG, MDR 1980, S. 801 ff.

Amelung, Knut/ Eymann, Frieder, Die Einwilligung des Verletzten im Strafrecht, JuS 2001, S. 937 ff.

Amelung, Knut, Sitzblockaden, Gewalt und Kraftentfaltung. Zur dritten Sitzblockade-Entscheidung des BVerfG, NJW 1995, S. 2584 ff.

Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, Ablehnung der Vorratsdatenspeicherung. Stellungnahme zur Anhörung der Europäischen Kommission. Public consultation on traffic data retention, DuD 2004, S. 603 ff.

Art. 29 Datenschutzgruppe, Stellungnahme 1/99 zum Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung vom 26.01.1999, WP 15, 5092/98/DE/endg. [Zitat: WP 15]

Dies., Arbeitsdokument. Privatssphäre im Internet -Ein intergrierter EU-Ansatz zum Online-Datenschutz, WP 37, 5063/2000/DE-ENDG., abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37de.pdf (letzter Abruf: 11.01.2007) [Zitat als: Art. 29 Datenschutzgruppe, WP 37]

Dies., Stellungnahme 9/2004 zum Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus [Vorschlag Frankreichs, Irlands, Schwedens und Großbritanniens, Ratsdokument 8958/04 v. 28.04.2004], abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_de.pdf (letzter Abruf: 30.01.2007) [Zitat: WP 99]

Dies., Stellungnahme 2/2006 der Artikel 29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_de.pdf (letzter Abruf: 30.01.2007) [Zitat: WP 118]

Auernhammer, Herbert, Die Europäische Datenschutz-Konvention und ihre Auswirkungen auf den grenzüberschreitenden Datenverkehr, DuD 1985, S. 7 ff.

Ders., Bundesdatenschutzgesetz Kommentar, 3. Aufl., Köln, 1993

Ayad, Patrick, E- Mail- Werbung- Rechtsgrundlagen und Regelungsbedarf, CR 2001, S. 535 ff.

Bär, Wolfgang, Der Zugriff auf Computerdaten im Strafverfahren, Köln, Berlin u.a., 1992

Ders., Strafrechtliche Kontrolle in Datennetzen, MMR 1998, S. 463 ff.

Ders., Anmerkung zu LG Hanau, MMR 2003, S. 175 f., MMR 2003, S. 176 f.

Ders., Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100 g, h StPO, MMR 2002, S. 358 ff.

Ders., Auslesen der SIM-Karte bei beschlagnahmten Mobiltelefon, MMR 2005, S. 523 ff.

Bäumler, Helmut (Hrsg.), E-Privacy. Datenschutz im Internet, Braunschweig u.a., 2000

Ders./ von Mutius Albert (Hrsg.), Anonymität im Internet. Grundlagen Methoden und Tools zur Realisierung eines Grundrechts, Braunschweig u.a., 2003

Baetge, Dietmar, Unverlangte E-Mail-Werbung zwischen Lauterkeits- und Deliktsrecht, NJW 2006, S. 1037 ff.

Bamberger, Heinz/ Roth, Herbert, Beck´scher Online-Kommentar. BGB, Stand: 01.11.2006, München, 2006 [Zitat: *Bearbeiter* in Bamberger/Roth]

Barton, Dirk, E- Mail – Kontrolle durch Arbeitgeber- Drohen unliebsame Überraschungen?, CR 2003, S. 839 ff.

Ders., Risiko- Management und IT- Sicherheit, K & R 2004, S. S. 305 ff.

Bartsch, Michael, Computerviren und Produkthaftung, CR 2000, S. 721 ff.

Baumbach, Adolf (Begr.)/ Köhler, Helmut/ Bornkamm, Joachim, Wettbewerbsrecht, Gesetz gegen den unlauteren Wettbewerb, Preisangabenverordnung, 25. Aufl., München, 2007

Bergmann, Lutz/ Möhrle, Roland/ Herb, Armin, Datenschutzrecht. Handkommentar. Bundesdatenschutzgesetz. Datenschutzgesetze der Länder und Kirchen. Bereichsspezifischer Datenschutz, 24. Ergänzungslieferung, Stuttgart. München u.a., 2000

Beutler, Bengt, Die Erklärung des Europäischen Parlaments über Grundrechte und Grundfreiheiten vom 12. April 1989, EuGRZ 1989, S. 185 ff.

Bichlmeier, Gerd, Die Wirksamkeit der Einwilligung in einen medizinisch nicht indizierten Eingriff, JZ 1980, S. 53 ff.

Bizer, Johann, Anmerkung zu BGH, NJW 1997, S. 1934 ff., DuD 1996, S. 627

Ders., Personenbezug bei Cookies, DuD 2003, S. 10

Bleckmann, Albert, Der Grundsatz der Völkerrechtsfreundlichkeit der deutschen Rechtsordnung, DÖV 1996, S. 137 ff.

Böhm, Steffen, Unerlaubte Telefonwerbung im geschäftlichen Bereich, MMR 1999, S. 643 ff.

Bone, Robert G., A New Look at Trade Secret Law: Doctrine in Search of Justification, 86 Cal. L. Rev., S. 241 ff.

Brockhaus (Hrsg.), Computer und Informationstechnologie- Hardware, Software, Multimedia, Internet, Telekommunikation, Mannheim, 2002

Bröhmer, Jürgen, Die Bosphorus-Entscheidung des Europäischen Gerichtshofs für Menschenrechte - Der Schutz der Grund- und Menschenrechte in der EU und das Verhältnis zur EMRK, EuZW 2006, S. 71 ff.

Brömmelmeyer, Christoph, E-Mail-Werbung nach der UWG-Reform, GRUR 2006, S. 285 ff.

Brugger, Winfried, Einführung in das öffentliche Recht der USA, 2. Aufl., München 2000

Büchner, Wolfgang/ Ehmer, Jörg/ Geppert,Martin, Kerkhoff, Bärbel/ Piepenbrock, Hermann-Josef/ Schütz, Raimund/ Schuster, Fabian (Hrsg.), Beck'scher TKG- Kommentar, 1. Aufl., München, 2000 [*Bearbeiter* in Beck´scher TKG-Kommentar, 1. Aufl.]

Bühler, Christoph, Ein Versuch Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, MDR 1987, S. 448 ff.

Buggisch, Walter, Dialer-Programme -Strafrechtliche Bewertung eines aktuellen Problems, NStZ 2002, S. 178 ff.

Bull, Hans Peter, Datenschutz als Informationsrecht und Gefahrenabwehr, NJW 1979, S. 1177 ff.

Bullinger, Martin, Wettbewerbsgerechtigkeit bei präventiver Wirtschaftsaufsicht, NJW 1978, S. 2173 ff.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Antispam- Strategien. Unerwünschte E- Mails erkennen und abwehren, abrufbar unter: www.bsi.bund.de [Zitat: *BSI*, Antispam-Strategien]

Dass., Das Ende der Anonymität?, Datenspuren in modernen Netzen, abrufbar unter: http://www.bsi.de/literat/anonym/wwwmail.htm, (letzter Abruf: 22.08.2006) [Zitat als: *BSI*, Das Ende der Anonymität?]

Dass., Vortäuschen eines falschen Absenders“, abrufbar unter: http://www.bsi.bund.de/gshb/deutsch/g/g05073.htm (letzter Abruf: 21.08.2006)

Dass., Computer-Viren. Definition und Wirkungsweise, abrufbar unter: http://www.bsi.de (letzter Abruf: 12.01.2007)

Burk, Dan L., The Trouble with Trespass, 4 J. Small & Emerging Bus. L., S. 27 ff. (2000)

Burkert, Herbert, Die Konvention des Europarates zum Datenschutz, CR 1988, S. 751 ff.

Busche, Jan/ Kraft Hartmut, Werbung per electronic mail: Eine neue Herausforderung für das Wettbewerbsrecht?, WRP 1998, S. 1142 ff.

Brüning, Christoph/ Helios, Markus, Die verfassungsprozessuale Durchsetzung grundrechtlicher Schutzpflichten am Beispiel des Internets, Jura 2001, S. 155 ff.

Brunnstein, Klaus, Fischer- Hübner, Simone, Globale Informationsgesellschaft, CR 1998, S. 125 ff.

Calliess, Christian, Zwischen staatlicher Souverätität und europäischer Effektivität: Zum Beurteilungsspielraum der Vertragsstaaten im Rahmen des Art. 10 EMRK- Zugleich eine Urteilsanmerkung zu den Entscheidungen des EGMR in den Fällen markt intern und Jacubowski, EuGRZ 1996, S. 293 ff.

Ders., Die Charta der Grundrechte der Europäischen Union- Fragen der Konzeption, Kompetenz und Verbindlichkeit, EuZW 2001, S. 261 ff.

Ders./ Ruffert, Matthias, Kommentar des Vertrages über die Europäische Union und des Vertrages zur Gründung der Europäischen Gemeinschaft- EUV/EGV, 3. Aufl., Neuwied u.a., 2007

Christiansen, Per, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, S. 123 ff.

Clark, David S., Ansay, Tuğrul, Introduction to the Law of the United States, 2. Aufl., London, 2002

Classen, Claus Dieter, Die Grundfreiheiten im Spannungsfeld von europäischer Marktfreiheit und mitgliedstaatlichen Gestaltungskompetenzen, EuR 2004, S. 416 ff.

Cody, Jonathan, Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation?, 48 Cath. U.L. Rev., S. 1183 ff. (1999)

Coppel, Jason/ O´Neill, Aidan, The European Court Of Justice: Taking Rights Seriously?, CML Rev. 1992, S. 669 ff.

Cornelius, Kai/ Tschoepe, Sven, Strafrechtliche Grenzen der zentralen E- Mail- Filterung und -Blockade, K & R 2005, S. 269 ff.

Crutchfield George, Barbara/ Lynch, Patricia/ Marsnik, Susan J., U.S. Multinational Employers: Navigating Through the „Safe Harbor" Principles to Comply with the EU Data Privacy Directive, 38 Am. Bus. L. J., S. 735 ff. (2001)

Däubler, Wolfgang, Nutzung des Internet durch Arbeitnehmer, K & R 2000, S. 323 ff.

Dammann, Ulrich/ Simitis, Spiros, EG- Datenschutzrichtlinie. Kommentar, Baden-Baden, 1997

Dannecker, Gerhard, Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, BB 1996, S. 1285 ff.

Dauses, Manfred, Die rechtliche Dimension des Binnenmarktes, EuZW 1990, S. 8 ff.

Ders. (Hrsg.), Handbuch des EU-Wirtschaftsrechts, Band 1, München, 2000

Defeis, Elizabeth, Freedom of Speech and International Norms: A Response to Hate Speech, 29 Stan. J. Int´l Law, S. 57 ff. (1992)

Degenhardt, Christoph, Das allgemeine Persönlichkeitsrecht, Art. 2 I i.V.m. Art. 1 I GG, JuS 1992, S. 361 ff.

Denninger, Erhard, Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle Selbstbestimmung, ZRP 1981, S. 231 ff.

Deselaers, Wolfgang, Die „Essential Facilities" - Doktrin im Lichte des Magill - Urteils des EuGH, EuZW 1995, S. 563 ff.

Determann, Lothar, Kommunikationsfreiheit im Internet, Baden-Baden, 1999

Diaz, Claudia/ Claessens, Joris/ Preneel, Bart, APES -Anonymity and Privacy in Electronic Services, DuD 2003, S. 143 ff.

Dietrich, Christian J./ Pohlmann, Norbert, IP- Blacklisting zur Spam- Abwehr, DuD 2005, S. 548 ff.

Dietrich, Ralf, Rechtliche Bewältigung von netzbasiertem Datenaustausch und Verteidigungsstrategien -20000 Verfahren gegen Filesharingnutzer, NJW 2006, S. 809 ff.

Dirnberger, Franz, Grundrechtliche Schutzpflichten und Gestaltungsspielraum, DVBl. 1992, S. 879 ff.

Dittrich, Klaus/ Schlörer, Jan, Anonymisierung von Forschungsdaten und Identifikation anonymer Datensätze, DuD 1987, S. 30 ff.

Dörr, Erwin/ Schmidt, Dietmar, Neues Bundesdatenschutzgesetz, Handkommentar - Die Arbeitshilfe für Wirtschaft und Verwaltung-, 1. Aufl., Köln, 1991, 3. Aufl., Köln, 1997

Dreier, Horst (Hrsg.), Grundgesetz Kommentar, Band 1 (Präambel, Art. 1 - 19), 2. Aufl., 2004, Band 2 (Artikel 20 - 82), 2. Aufl., Tübingen, 2006

Droop, Christian,, Sachrechte der Gliedstaaten der USA und ihre kollisionsrechtliche Bewältigung, JURA 1993, S. 293 ff.

Dürig, Günter, Der Grundrechtssatz von der Menschenwürde. Entwurf eines praktikablen Wertsystems der Grundrechte aus Art. 1 Abs. 1 in Verbindung mit Art. 19 Abs. 2 GG des Grundgesetzes, AöR 81 (1956), S. 117 ff.

Duttge, Gunnar, Recht auf Datenschutz? Ein Beitrag zur Interpretation der grundrechtlichen Schutzbereiche, Der Staat 36 (1997), S. 281 ff.

Ders., Strafrechtliche Rätsel -Zur Bedeutung der Rechtsgutslehre für Einwilligung und Gesetzeskonkurrenz, Jura 2006, 15 ff.

Eberle, Carl-Eugen, Datenschutz durch Meinungsfreiheit, DÖV 1977, S. 306 ff.

Eckert, Claudia, IT- Sicherheit, Konzepte-Verfahren-Protokolle, 4. Aufl., München, 2006

Eckhardt, Jens, Datenschutzrichtlinie für elektronische Kommunikation-Auswirkungen auf die Werbung mittels elektronischer Post, MMR 2003, S. 557 ff.

Ders., Wie weit reicht der Schutz des Fernmeldegeheimnisses (Art. 10 GG)? Zugleich Anmerkung zu BVerfG, Urt. v. 2.3.2006, 2 BVR 2099/04, DuD 2006, S. 365 ff.

Ehlers, Dirk, Die unerwünschte Zustellung von Werbematerial durch öffentliche Unternehmen, JZ 2001, S. 231 ff.

Ders. (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 2. Aufl., Berlin, 2005 [Zitat: *Bearbeiter* in Ehlers]

Ehmann, Eugen, Helfrich, Marcus, EG Datenschutzrichtlinie, Kurzkommentar, Köln, 1999

Eichelberger, Jan, Sasser, Blaster, Phatbot & Co. -alles halb so schlimm? - Ein Überblick über die strafrechtliche Bewertung von Computerschädlingen, MMR 2004, S. 594 ff.

Eichler, Alexander, Cookies- verbotene Früchte? - Eine datenschutzrechtliche und technik- orientierte Betrachtung, K & R 1999, S. 76 ff.

Electronic Commerce Forum, Verband der deutschen Internetwirtschaft e.V. (eco), Whitepaper. Vollversion. Anti-Spam Task Force - ASTF, abrufbar unter: http://www.eco.de, letzter Abruf: 14.11.2006

Ellger, Reinhard, Datenschutz und Europäischer Binnenmarkt (Teil 1), RDV 1991, S. 57 ff.

Ders., Datenschutz und Europäischer Binnenmarkt (Teil 2), RDV 1991, S. 121 ff.

Engel, Christoph, Eigentumsschutz für Unternehmen, AöR 118 (1993), S. 169 ff.

Engel-Flechsig, Stefan, Die datenschutzrechtlichen Vorschriften im neuen Informations- und Kommunikationsdienste-Gesetz, RDV 1997, S. 59 ff.

Engels, Stefan/ Eimterbäumer, Elke, Sammeln und Nutzen von e- Mail- Adressen zu Werbezwecken, K&R 1998, S. 196 ff.

Erichsen, Hans-Uwe, Grundrechtliche Schutzpflichten in der Rechtsprechung des Bundesverfassungsgerichts, Jura 1997, S. 85 ff.

Erman, Walter/ Westermann, Harm, Bürgerliches Gesetzbuch, Handkommentar, 11. Aufl., 2004

Ernst, Stefan (Hrsg.), Der Arbeitgeber, die E- Mail und das Internet, NZA 2002, 585 ff.

Ders., Vertragsgestaltung im Internet, München, 2003

Ders., Hacker und Computerviren im Strafrecht, NJW 2003, S. 3233 ff.

Ders., Hacker, Cracker & Computerviren. Recht und Praxis der Informationssicherheit, Köln, 2004

Ders./ Seichter, Dirk, Werben mittels E-Cards- Rechtliche Beurteilung als Spamming?, MMR 2006, S. 779 ff.

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über unerbetene Werbenachrichten (Spam), KOM/2004/0028

Faber, Heiko, Innere Geistesfreiheit und suggestive Beeinflussung, Berlin, 1968

Faßbender, Kurt, Der grundrechtliche Schutz der Werbefreiheit in Deutschland und Europa, GRUR Int. 2006, S. 965 ff.

Ders., Von Fachanwälten und selbsternannten Spezialisten - Ein Beitrag zu den zulässigen Grenzen werblicher Äußerungen von Rechtsanwälten, NJW 2006, S. 1463 ff.

Federal Trade Commission, National Do Not Email Registry, A Report To Congress, abrufbar unter: http://www.ftc.gov/reports/dneregistry/report.pdf (letzter Abruf: 11.01.2007)

Feger, Dieter, Grundrechtliche Aspekte des Rechts der Europäischen Gemeinschaften auf dem Gebiet der abhängigen Arbeit, RdA 1987, S. 13 ff.

Fenchel, Jörg, Negative Informationsfreiheit, Zugleich ein Beitrag zur negativen Grundrechtsfreiheit, Berlin, 1995

Fezer, Karl- Heinz (Hrsg.), Lauterkeitsrecht. Kommentar zum Gesetz gegen den unlauteren Wettbewerb, 1. Aufl., München, 2005

Fikentscher,Wolfgang/ Möllers,Thomas, Die (negative) Informationsfreiheit als Grenze von Werbung und Kunstdarbietung, NJW 1998, S. 1337 ff.

Fishman, Clifford, Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media, 72 Geo. Wash. L. Rev., 1503 ff. (2004)

Frank, Thomas, „You've got (Spam-) Mail"- Zur Strafbarkeit von Email-Werbung, CR 2004, S. 123 ff.

Frenz, Walter, Handbuch Europarecht, Band 1, Europäische Grundfreiheiten, Berlin u.a., 2004

Friauf, Karl Heinrich/ Höfling, Wolfram, Meinungsgrundrechte und Verfolgung von wirtschaftlichen Belangen, AfP 1985, S. 249 ff.

Fritzemeyer, Wolfgang, Der US- amerikanische CAN- SPAM Act- Darstellung und Analyse, auch im Vergleich mit der Spam – Gesetzgebung der Europäischen Union, K & R 2005, S. 49 ff.

Fröhle, Jens, Werb Advertising, Nutzerprofile und Teledienstedatenschutz, München, 2003

Fromholz, Julia M., The European Union Data Privacy Directive, 15 Berkeley Tech. L. J., S. 461 ff. (2000)

Frommel, Monika, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, JuS 1987, S. 667 f.

Frowein, Jochen/ Peukert, Wolfgang, Europäische Menschenrechtskonvention, EMRK Kommentar, 2. Aufl., Kehl u.a., 1996, [Zitat: *Bearbeiter* in Frowein/Peukert]

Füller, Jens Th., Grundlagen und inhaltliche Reichweite der Warenverkehrsfreiheit nach dem EG-Vertrag, Baden-Baden, 2000

Funk, Axel, Wettbewerbsrechtliche Grenzen von Werbung per E-Mail, CR 1998, S. 411 ff.

Ders./ Zeifang, Gregor, Johnson Douglas T., Spessard III, Robert W., Unsolicited Commercial Emails in the Jurisdictions of Germany and the USA- Some thoughts on the new anti-spam laws in consideration of the interests of the parties involved in email traffic, CRi 2004, S. 138 ff.

Ders., Verfassungsrechtliche Grundlagen des Datenschutzes, Der Staat 1979, S. 507 ff.

Gallwas, Hans- Ullrich, Faktische Beeinträchtigungen im Bereich der Grundrechte, Berlin, 1970

Ders./
Geiger, Hansjörg/
Schneider, Jochen/
Schwappach, Jürgen /
Schweinoch, Joachim, Datenschutzrecht - Kommentar und Vorschriftensammlung, Stuttgart, 1978 ff., Stand: Januar 1986 [Zitat: *Bearbeiter* in Gallwas]

Geary, John P.,
Dave, Dinesh S, The CAN- SPAM Act of 2003: An end to Unsolicited Email?, Computers & Law, März 2005, S. 19 ff.

Geiger, Rudolf, EUV/EGV, Vertrag über die Europäische Union und Vertrag zur Gründung der Europäischen Gemeinschaft, 4. Aufl., München, 2004

Geis, Ivo, Haftungsrisiken im Datenschutzrecht für Unternehmen, CR 1993, 269 ff.

Ders./
Geis, Esther, Das informationelle Selbstbestimmungsrecht als Pathosformel des Datenschutzrechts oder Schutz der Privatheit während und nach der elektronischen Kommunikation. Zugleich Anmerkung zum Urteil des Bundesverfassungsgerichts 2.3.2006 – 2 BvR 2099/04 (K & R 2006, 178 ff.), K & R 2006, S. 279 f.

Gellman, Robert M., Can Privacy be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules, 41 Vill. L. Rev., S. 129 ff. (1996)

Gentz, Manfred, Zur Verhältnismäßigkeit von Grundrechtseingriffen, NJW 1968, S. 1600 ff.

Geppert, Martin/
Piepenbrock Hermann-Josef/
Schütz, Raimund/
Schuster, Fabian, Beck´scher TKG-Kommentar,
2. Aufl., München 2000
[Zitat: *Bearbeiter* in Beck´scher TKG-Kommentar, 2. Aufl.]
3. Aufl., München, 2006
[Zitat: *Bearbeiter* in Beck´scher TKG-Kommentar]

Geppert, Martin/
Ruhle, Ernst-Olav/
Schuster, Fabian, Handbuch Recht und Praxis der Telekommunikation. EU, Deutschland, Österreich, Schweiz, Baden-Baden, 2. Aufl., 2002

Gerling, Rainer, Verschlüsselungsverfahren. Eine Kurzübersicht, DuD 1997, S. 197 ff.

Gersdorf, Hubertus, Funktionen der Gemeinschaftsgrundrechte im Lichte des Solange II-Beschlusses des Bundesverfassungsgerichts, AöR 119 (1994), S. 400 ff.

Gerstner, Stephan/ Goebel, Burkhart, Grundrechtsschutz in Europa, Jura 1993, S. 626 ff.

Gilbert, Francoise, How to Legally Transfer Personal Data from the European Union, 865 PLI/Pat, S. 545 ff.

Gilles, Peter, Recht und Praxis des Telemarketing – Werbung und Vertrieb unter Einsatz teletechnischer Kommunikationsmittel und ihre Schranken im Privat- und insbesondere Wettbewerbsrecht, NJW 1988, S. 2424 ff.

Glöckner, Jochen, „Cold Calling" und europäische Richtlinie zum Fernabsatz – ein trojanisches Pferd im deutschen Lauterkeitsrecht, GRUR Int. 2000, S. 29 ff.

Gloy, Wolfgang, Loschelder, Michael (Hrsg.), Handbuch des Wettbewerbsrechts, 3. Aufl., München, 2005

Gnirck, Karen/ Lichtenberg, Jan, Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen. Auskunftsersuchen zu IP-Adressen, DuD 2004, S. 598 ff.

Göbel, Alfred, Die Einwilligung im Strafrecht als Ausprägung des Selbstbestimmungsrechts, Frankfurt, 1991

Gößmann, Christine, Electronic Commerce- Die EU – Fernabsatzrichtlinie und ihre Auswirkungen auf den Handel über neue Medien, MMR 1998, S. 88 ff.

Götting, Horst-Peter, Vom Right of Privacy zum Right of Publicity- Die Anerkennung eines Immaterialgüterrechts an der eigenen Persönlichkeit im amerikanischen Recht, GRUR Int. 1995, S. 656 ff.

Götzfried, Eva, Das Recht, nicht zuhören zu müssen, NJW 1961, S. 1961 ff.

Gola, Peter, Neuer Tele- Datenschutz für Arbeitnehmer? – Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 1999, S. 322 ff.

Ders./
Müthlein, Thomas, Teledienstegesetz, Teledienstedatenschutzgesetz, Kommentierung für die Praxis, Frechen, 2000

Ders./
Schomerus, Rudolf, BDSG- Bundesdatenschutzgesetz Kommentar, zitiert: Gola/Schomerus, BDSG Kommentar, 8. Aufl., München, 2005

Ders./
Klug, Christoph, Die Entwicklung des Datenschutzrechts in den Jahren 2005/2006, NJW 2006, S. 2454 ff.

Goldstone, David J., The Public Forum Doctrine in the Age of the Information Superhighway (Where are the Public Forums on the Information Superhighway?), 46 Hastings L. J., S. 335 ff. (1995)

Golembiewski, Claudia, Anonymität im Recht der Multimediadienste, in Bäumler/v. Mutius (Hrsg.), Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, S. 107 ff. 1. Aufl., Braunschweig/Wiesbaden, 2003 [Zitat: *Golembiewski* in Bäumler/von Mutius]

Gounalakis, Georgios,
Mand, Elmar, Die neue EG- Datenschutzrichtlinie- Grundlagen einer Umsetzung in nationales Recht (I), CR 1997, S. 431 ff.

Dies., Die neue EG- Datenschutzrichtlinie- Grundlagen einer Umsetzung in nationales Recht (II), CR 1997, S. 497 ff.

Grabenwarter, Christoph, Die Charta der Grundrechte für die Europäische Union, DVBl. 2001, S. 1 ff.

Ders., Europäische Menschenrechtskonvention, Ein Studienbuch, München, 2003 [Zitat: Grabenwarter]

Ders., Auf dem Weg in die Grundrechtsgemeinschaft?, EuGRZ 2004, S. 563 ff.

Grabitz, Eberhard, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Bundesverfassungsgerichts, AöR 98 (1973), 568 ff.

Ders.
Hilf, Meinhard (Hrsg.), Das Recht der Europäischen Union, 29. Ergänzungslieferung, München, 2005

Graham, Paul, A Plan for Spam, abrufbar unter: http://www.paulgraham.com/spam.html (letzter Abruf: 29.04.2007)

Gramlich, Ludwig, Art. 110 GG nach der zweiten Postreform 1994, CR 1996, 102 ff.

Gravenreuth, Frhr. v., Computerviren, Hacker, Datenspione, Crasher und Cracker- Ein Überblick und rechtliche Einordnung, NStZ 1989, S. 201 ff.

Greenberg, Thomas R., E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev., S. 219 ff. (1994)

Groß, Thomas, Die Schutzwirkung des Brief-, Post- und Fernmeldegeheimnisses nach der Privatsierung der Post, JZ 1999, S. 326 ff.

Grossman, Seth, Keeping Unwanted Donkeys and Elephants out of your Inbox: The Case for Regulating Political Spam, 19 Berkeley Tech. L. J., S. 1533 ff., (2004)

Gubitz, Arnulf S., The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?, 39 New Eng. L. Rev., S. 431 ff. (2005)

Günther, Andreas,, Erwünschte Regelung unerwünschter Werbung?- Zur Auslegung von Art. 10 der Fernabsatzrichtlinie 97/7/EG, CR 1999, S. 172 ff.

Günther, Ralf, Zur strafprozessualen Erhebung von Kommunikationsdaten - Verpflichtung zur Sachverhaltsaufklärung oder verfassungsrechtlich unkalkulierbares Wagnis?, NStZ 2005, S. 485 ff.

Gummig, Christian, Rechtsfragen bei Werbung im Internet, ZUM 1996, S. 573 ff.

Gundermann, Lukas, E- Commerce trotz oder durch Datenschutz?, K & R 2000, S. 225 ff.

Gusy, Christoph, Das Grundrecht des Post- und Fernmeldegeheimnisses, JuS 1986, S. 89 ff.

Haager, Johannes, Grundrechte im Privatrecht, JZ 1994, S. 373 ff.

Häberle, Peter, Die Wesensgehaltsgarantie des Art. 19 Abs. 2 Grundgesetz, Karlsruhe, 1962

Härting, Niko, Die Gewährleistungspflichten von Internet-Dienstleistern, CR 2001, S. 37 ff.

Ders./ Eckart, Christian, Provider gegen Spammer- Können sich Provider mit rechtlichen Ansprüchen gegen die Mailflut wehren?, CR 2004, S. 119 ff.

Haft, Fritjof, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG)-Teil 2: Computerdelikte, NStZ 1987, S. 6 ff.

Ders., Strafrecht, Allgemeiner Teil, 9. Aufl., 2004; Besonderer Teil, 7. Aufl., München, 1998

Hain, D. Karl- Eberhard, Der Gesetzgeber in der Klemme zwischen Übermaß – und Untermaßverbot?, DVBl. 1993, S. 982 ff.

*Hammerbacher, Hans***,** Zu den Voraussetzungen und Grenzen eines wirksamen Datenschutzes – Ein Beitrag zur Bestimmung und Anwendung wesentlicher Begriffsmerkmale im (Bundes) Datenschutz- und entsprechenden Strafrechten, DVBl. 1978, S. 421 ff.

Hanebeck, Alexander/ Neunhoeffer, Friederike, Anwendungsbereich und Reichweite des telekommunikationsrechtlichen Fernmeldegeheimnisses

- Rechtliche Schwierigkeiten bei der Anwendung des TKG, K & R 2006, S. 112 ff.

Hartmann, Christian, Verfassungswidrige und doch wirksame Rechtsnormen, DVBl. 1997, S. 1265 ff.

Hassemer, Ines/ Witzel, Michaela, Filterung und Kontrolle des Datenverkehrs. Ist die Filterung von E-Mails im Unternehmen rechtmäßig?, ITRB 2006, S, 139 ff.

Hay, Peter, US- amerikanisches Recht, Ein Studienbuch, 3. Auflage, München, 2005

Heidrich, Joerg/ Tschoepe, Sven, Rechtsprobleme der E- Mail- Filterung, MMR 2004, S. 75 ff.

Heidrich, Joerg, MMR 2005, 181 f., Anmerkung zu OLG Karlsruhe, MMR 2005, 178 ff.

Heil, Helmut, Europäische Herausforderung- Transatlantische Debatte- Zur Datenschutzdiskussion zwischen der EU und den USA, DuD 1999, S. 458 ff.

Ders., Safe Harbor: Ein Zwischenstandsbericht, DuD 2000, S. 444 f.

Ders., Datenschutz durch Selbstregulierung, DuD 2001, S. 129 ff.

Heil, Ulf, Neues Wettbewerbsrecht: Wechselwirkungen zwischen UWG und Datenschutz, RDV 2004, S. 205 ff.

Hellermann, Johannes, Die sogenannte negative Seite der Freiheitsrechte, Berlin, 1993

Henning, Peter, Taschenbuch Multimedia, 3. Aufl., München, 2003

Heußner, Hermann, Das informationelle Selbstbestimmungsrecht des Grundgesetzes als Schutz des Menschen vor totaler Erfassung, BB 1990, S. 1281 ff.

Hilgendorf, Eric, Anmerkung zu BayObLG, JR 1994, S. 476 ff., JR 1994, S. 478

Ders., Grundfälle zum Computerstrafrecht, JuS 1996, 890 ff.

Ders., Grundfälle zum Computerstrafrecht, JuS 1997, S. 323 ff.

Hirsch, Günter, Europäischer Gerichtshof und Bundesverfassungsgericht- Kooperation oder Konfrontation?, NJW 1996, S. 2457 ff.

Hirte, Heribert, Mitteilung und Publikation von Gerichtsentscheidungen- Zum Spannungsverhältnis von Persönlichkeitsschutz und Interessen der Öffentlichkeit, NJW 1988, S. 1698 ff.

Hoffmann- Riem, Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft- Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 1998, S. 513 ff.

Hoeren, Thomas, Cybermanners und Wettbewerbsrecht- Einige Überlegungen zum Lauterkeitsrecht im Internet, WRP 1997, S. 993 ff.

Ders., Recht der Access Provider, 1. Aufl., München, 2004

Ders., Privacy, Direktmarketing und das neue UWG, DuD 2004, S. 611 ff.

Ders., Virenscanning und Spamfilter- Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co., NJW 2004, S. 3513 ff.

Ders., Der Tod und das Internet- Rechtliche Fragen zur Verwendung von E- Mail- und WWW- Accounts nach dem Tode des Inhabers, NJW 2005, S. 2113 ff.

Ders., Auskunftspflichten der Internetprovider an Strafverfolgungs- und Sicherheitsbehörden -eine Einführung, wistra 2005, S. 1 ff.

Ders., Das Telemediengesetz, NJW 2007, S. 801 ff.

Ders./ Sieber, Ulrich, (Hrsg.), Handbuch Multimediarecht, Rechtsfragen des elektronischen Geschäftsverkehrs, 13. Ergänzungslieferung, München, 2006

Hösch, Ulrich, Meinungsfreiheit und Wettbewerbsrecht am Beispiel der „Schockwerbung“, WRP 2003, S´. 936 ff.

Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft - Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 123 (1998), S. 513 ff.

Holoubek, Michael, Der Grundrechtseingriff - Österreichische und konventionsrechtliche Aspekte, DVBl. 1997, S. 1031 ff.

Holznagel, Bernd/ Enaux, Christoph/ Nienhaus, Christian, Grundzüge des Telekommunikationsrechts. Rahmenbedingungen. Regulierungsfragen. Internationaler Vergleich, 2. Aufl., München, 2001 [Zitat: *Holznagel/Enaux/Nienhaus*, Grundzüge des Telekommunikationsrechts]

Holznagel, Bernd/ Enaux, Christoph/ Nienhaus, Christian, Telekommunikationsrecht. Rahmenbedigungen. Regulierungspraxis, 2. Aufl., München, 2006 [Zitat: *Holznagel/Enaux/Nienhaus*, Telekommunikationsrecht]

Hopper, Dan, Do You Want Spam with That? The CAN-SPAM Act, Preemption, and First Amendment Commercial Speech Jurisprudence Concerning State University Anti-Solicitation E-Mail Policy, 59 SMU L.Rev., S. 387 ff., (2006)

Hornung, Gerrit, Der Personenbezug biometrischer Daten. Zugleich eine Erwiderung auf Saeltzer, DuD 2004, S. 218 ff., DuD 2004, S. 429 ff.

Hufen, Friedhelm, Berufsfreiheit- Erinnerung an ein Grundrecht, NJW 1994, S. 2913 ff.

Huster, Stefan, Gleichheit und Verhältnismäßigkeit, JZ 1994, S. 541 ff.

Hymowitz, Steven, Bendana, David, Privacy Limitations for Electronic Surveillance and Genetic Testing in the Workplace, abrufbar unter: http://www.bna.com/bnabooks/ababna/99/annual07.pdf (letzter Abruf: 17.01.2007)

Ihde, Rainer, Cookies- Datenschutz als Rahmenbedingung der Internetökonomie, CR 2000, S. 413 ff.

Immega,Ulrich/ Mestmäcker, Ernst- Joachim (Hrsg.), GWB, Gesetz gegen Wettbewerbsbeschränkungen Kommentar, 3. Auflage, München, 2001

Internet Engineering Task Force (IETF), Request for Comments (RFC): 793, Transmission Control Protocol, abrufbar unter http://tools.ietf.org/html/rfc793 (letzter Abruf: 29.01.2007) [Zitat: *IETF*, RFC 821]

Dies., Request for Comments (RFC): 821, Simple Mail Transfer Protocol, abrufbar unter: http://www.ietf.org/rfc/rfc0821.txt, letzter Abruf: 21.08.2006 [Zitat als: *IETF,* RFC 821]

Dies., Request for Comments (RFC): 822, Standard for the Format of ARPA Internet Text Messages, abrufbar unter: http://www.ietf.org/rfc/rfc0822.txt, letzter Abruf: 21.08.2006 [Zitat als: *IETF,* RFC 822]

Dies., Request for Comments (RFC): 1034, Domain Names Concepts and Facilities, abrufbar unter: http://www.ietf.org/rfc/rfc1034.txt, letzter Abruf: 21.08.2006 [Zitat als: *IETF,* RFC 1034]

Dies., Request for Comments (RFC): 1035, Domain Names-Implementation and Specification, abrufbar unter: http://www.ietf.org/rfc/rfc1035.txt, letzter Abruf: 21.08.2006 [Zitat als: *IETF*, RFC 1035]

Dies., Request for Comments (RFC) 1288: The Finger User Information Protocol, 1991, abrufbar unter: http://www.ietf.org/rfc/rfc/1288.txt (letzter Abruf: 11.01.2007) [Zitat als: *IETF*, RFC 1288]

Dies., Request for Comments (RFC): 1752, The Recommendation for the IP Next Generation Protocol, abrufbar unter: http://www.ietf.org/rfc/rfc1752.txt, letzter Abruf: 21.08.2006 [Zitat als: *IETF*, RFC 1752]

Dies., Request for Comments (RFC): 2026, The Internet Standards Process-Revision 3, abrufbar unter: http://www.ietf.org/rfc/rfc2026.txt, letzter Abruf: 21.08.2006 [Zitat: *IETF*, RFC 2026]

Dies., Request for Comments (RFC): 2460, Internet Protocol, Version 6 (Ipv6) Specification, abrufbar unter: http://www.ietf.org/rfc/rfc2460.txt, (letzter Abruf: 21.08.2006) [Zitat: *IETF*, RFC 2460]

Dies., Request for Comments (RFC): 2822, Internet Message Format, abrufbar unter: http://www.ietf.org/rfc/rfc2822.txt, (letzter Abruf: 22.08.2006) [Zitat: *IETF*, RFC 2822]

Irlbeck, Thomas, Computer-Lexikon, Das Nachschlagewerk zum Thema EDV, 3. Aufl., München, 1998

Isensee, Josef,
Kirchhof, Paul, Handbuch des Staatsrechts der Bundesrepublik Deutschland, 1989,
Band I, Grundlagen von Staat und Verfassung
Band V, Allgemeine Grundrechtslehren
Band VI, Freiheitsrechte,
Band VII, Normativität und Schutz der Verfassung-Internationale Beziehungen
[Zitat: *Bearbeiter* in Isensee/Kirchhof]

Jacob, Joachim/ Heil, Helmut, Datenschutz im Spannungsfeld von staatlicher Kontrolle und Selbstregulierung in Bizer u.a., Umbruch von Regelungssystemen in der Informationsgesellschaft, Freundesgabe Büllesbach, 2002, 213 ff., abrufbar unter: http://www.alfred-buellesbach.de/PDF/20_Jacob_Heil.pdf (letzter Abruf: 11.01.2007)

Jahn, Matthias, Der strafprozessuale Zugriff auf Telekommunikationsverbindungsdaten - BVerfG, NJW 200, 976, JuS 2006, S. 491 ff.

Jankowski, Rayner, Kosten beim Empfänger unverlangter E- Mails- nur ein Scheinargument?, K & R 2000, S. 499 ff.

Jarass, D., Die freien Berufe zwischen Standesrecht und Kommunikationsfreiheit, NJW 1982, 1833 ff.

Ders., Konflikte zwischen Polizei und Presse bei Demonstrationen, JZ 1983, S. 280 ff.

Ders., Grundrechte als Wertentscheidungen bzw. objektivrechtliche Prinzipien in der Rechtsprechung des Bundesverfassungsgerichts, AöR 1985, S. 363 ff.

Ders., Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, S. 857 ff.

Ders., Konflikte zwischen EG-Recht und nationalem Recht vor den Gerichten der Mitgliedstaaten, DVBl. 1995, S. 954 ff.

Ders., Elemente einer Dogmatik der Grundfreiheiten II, EuR 2000, 705 ff.

Ders., EU-Grundrechte, Ein Studien- und Handbuch, München, 2005

Ders./ Pieroth, Bodo, Grundgesetz für die Bundesrepublik Detuschland Kommentar, 8. Aufl., München, 2006

Jauernig, Othmar (Hrsg.), Jauernig, Bürgerliches Gesetzbuch, Kommentar, 11. Aufl., München, 2004

Joecks, Wolfgang, Studienkommentar StGB, 6. Aufl., München, 2005

Ders./
Miebach, *Klaus*, Münchener Kommentar zum Strafgesetzbuch,, München, Band 1 (§§ 1 -51), 2003, Band 3 (§§ 185 - 262) 2003 [Zitat: *Bearbeiter* in Münchener Kommentar]

Jüngel, Marc/Schwan, Markus Alexander/Neumann, Nicolas, Das Abfangen von E- Mails nach § 303 a StGB, MMR 2005, S. 820 ff.

Kadelbach, Stefan, Der Status der Europäischen Menschenrechtskonvention im deutschen Recht – Anmerkungen zur neuesten Rechtsprechung des Bundesverfassungsgerichts, Jura 2005, S. 480 ff.

Kämmerer, Ludwig/ Eidenmüller, Alfred (Hrsg.), Post- und Fernmeldewesen, Loseblattkommentar, 26. Ergänzungslieferung, Heidelberg, 1981

Kang, Jerry, Information Privacy in Cyberspace Transactions, 50 Stanford Law Review, S. 1193 ff. (1998)

Kapersky, Eugene, Die moderne Anti-Virus-Industrie und ihre Problemfelder, abrufbar unter: http://www.securitymanager.de (letzter Abruf: 11.01.2007)

Karl, Wolfram (Hrsg.), Internationaler Kommentar zur Europäischen Menschenrechtskonvention, 7. Lieferung, Köln, 2004 [Zitat: *Bearbeiter* in Karl]

Kemmler, Anne, Telekommunikationsgesetz (TKG). Einführung und Stand der Umsetzung, Archiv PT 1996, S. 321 ff.

Kennedy, Charles H., Lyon, E. Christine, The CAN- SPAM Act of 2003: A New Regime for Email Advertising, The Computer & Internet Lawyer 2005, Nr. 2, S. 1 ff.

Kieper, Marcus, Datenschutz für Telearbeitnehmer, DuD 1998, S. 583 ff.

Kierkegaard, Sylvia, Privacy in electronic communication, Watch your e-mail: Your boss is snooping!, Computer Law & Security Report 2005, S. 226 ff.

Kimminich, Otto, Die Freiheit, nicht zu hören, Der Staat 3 (1964), S. 61 ff.

Ders., Einführung in das Völkerrecht, 6. Aufl., Stuttgart, 1997 [Zitat: *Kimminich*]

Kindhäuser, Urs, Strafgesetzbuch. Lehr- und Praxiskommentar, 2. Aufl., Baden- Baden, 2005

Ders./ Neumann, Ulfried/ Paeffgen, Hans-Ullrich, Nomos Kommentar, Strafgesetzbuch, Band 2, 2. Aufl., Baden-Baden, 2005 [Zitat: *Bearbeiter* in Kindhäuser/Neumann/Paeffgen]

Kingreen, Thorsten, , Die Gemeinschaftsgrundrechte, JuS 2000, S. 857 ff.

Ders./, Störmer Rainer, Die subjektiv-öffentlichen Rechte des primären Gemeinschaftsrechts, EuR 1998, S. 263 ff.

Kitz, Volker, Meine E- Mails les' sich nicht!, Zur Einwilligung in die Spamfilterung, CR 2005, S. 450 ff.

Klein, Eckart, Grundrechtliche Schutzpflichten des Staates, NJW 1989, S. 1633 ff.

Klein, Hans, Die grundrechtliche Schutzpflicht, DVBl. 1994, S. 489 ff.

Klußmann, Niels, Lexikon der Kommunikations- und Informationstechnik, 2. Aufl., Heidelberg, 2000

Kleine-Voßbeck, Bernd, Electronic Mail und Verfassungsrecht, Marburg, 2000

Klippel, Diethelm, Deliktsrechtliche Probleme des Datenschutzes, BB 1983, S. 407 ff.

Klug, Christoph, Beispiele richtlinienkonformer Auslegung des BDSG, RDV 2001, S. 266 ff.

Ko, Jim W., The Fourth Amendment and the Wiretap Act Fail to Protect Against Random ISP Monitoring of E-Mails for the Purpose of Assisting Law Enforcement, 22. J. Marshall J. Computer & Info. L., S. 493 ff. (2004)

Koch, Robert, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, S. 801 ff.

Ders., Versicherungsschutz bei Gestattung privater Online-Nutzung am Arbeitsplatz -(k)ein neues Risiko?, VersR 2006, 1433 ff.

Köbele, Bernd, Anspruch auf Mitteilung des Anschlussinhabers bei bekannter IP-Adresse, DuD 2004, S. 609 f.

Koecher, Jan K., Zentrale Spam- und Virenfilterung, DuD 2004, S. 272 ff.

Ders., Strafbarkeit der Ausfilterung von E- Mails Anmerkung zum Beschluss des OLG Karlsruhe vom 10.01.2005- 1 Ws 152/04, DuD 2005, S. 163 ff.

Koenig, Christian/ Röder, Ernst, Die EG – Datenschutzrichtlinie für Telekommunikation-Verpflichtungen auch für Internetdienstleister, CR 2000, S. 668 ff.

König, Michael, Software (Computersoftware) als Sache und deren Erwerb als Sachkauf, NJW 1993, S. 3121 ff.

Köhler, Helmut, UWG-Reform und Verbraucherschutz, GRUR 2003, S. 265 ff.

Ders., Das neue UWG, NJW 2004, S. 2121 ff.

Ders., Kartellverbot und Schadensersatz, GRUR 2004, S. 99 ff.

Ders./ Piper, Henning, Gesetz gegen den unlauteren Wettbewerb mit Preisangabenverordnung. Kommentar, 3. Auflage, München, 2002

Ders./ Lettl, Tobias, Das geltende europäische Lauterkeitsrecht, der Vorschlag für eine EG-Richtlinie über unlautere Geschäftspraktiken und die UWG-Reform, WRP 2003, S. 1019 ff.

Köhler, Markus/ Arndt, Wolfgang/ Fetzer, Thomas, Recht des Internet, 5. Aufl., Heidelberg, 2006

Köhntopp, Marit/ Köhntopp Kristian, Datenspuren im Internet, abrufbar unter: http://kris.koehntopp.de/artikel/datenspuren/CR_Datenspuren_im_Internet.pdf (letzter Abruf: 21.08.2006)

Königshofen, Thomas, Die Telekommunikations-Datenschutzverordnung - TDSV, DuD 2001, S. 85 ff.

Köpsell, Stefan/ Miosga, Tobias, Strafverfolgung trotz Anonymität, DuD 2005, S. 403 ff.

Krause, Peter, Das Recht auf informationelle Selbstbestimmung, JuS 1984, S. 268 ff.

Kremer, Carsten, Die Haftung Privater für Verstöße gegen Gemeinschaftsrecht, EuR 2003, S. 696 ff.

Kresse, Hermann, Wirtschaftswerbung und Art. 5 Grundgesetz (GG), WRP 1985, S. 536 ff.

Kröger, Detlef/ Gimmy, Marc, Handbuch zum Internetrecht. Electronic Commerce-Informations-, Kommunikations- und Mediendienste, Berlin, 2000 [Zitat: *Bearbeiter* in Kröger/Gimmy]

Kubicek, Herbert, Der Schutz des Fernmeldegeheimnisses auf dem Telekommunikationsmarkt, DuD 1995, S. 656 ff.

Kudlich, Hans, Der heimliche Zugriff auf Daten einer Mailbox -ein Fall der Überwachung des Fernmeldeverkehrs? -BGH, NJW 1997, S. 1934, JuS 1998, S. 209 ff.

Kühl, Kristian (Bearb.), Lackner/Kühl, Kommentar zum Strafgesetzbuch, 25. Aufl., München, 2004 [Zitat: *Lackner/Kühl*]

Kühling, Jürgen, Staatliche Handlungspflichten zur Sicherung der Grundfreiheiten, NJW 1999, 403 f.

Ders., Freiheitsverluste im Austausch gegen Sicherheitshoffnungen im künftigen Telekommunikationsgesetz? Verfassungsrechtliche Determinanten am Beispiel der Vorratsdatenspeicherung, K & R 2004, S. 105 ff.

Küper, Wilfried, Das BVerfG, das Analogieverbot und der Bedrohungstatbestand -BVerfG NJW 1995, S. 2776, JuS 1996, S. 783 ff.

Kugelmann, Dieter, Der Schutz privater Individualkommunikation nach der EMRK, EuGZR 2003, S. 16 ff.

Kunig, Philip, Der Grundsatz informationeller Selbstbestimmung, Jura 1993, S. 595 ff.

Krüger, Herbert, Der Wesensgehalt der Grundrechte i.S. des Art. 19 GG, DÖV 1955, S. 597 ff.

Lange, Knut Werner, Werbefinanzierte Kommunikationsdienstleistungen, WRP 2002, S. 786 ff.

Larson, Aaron, Defamation: Libel and Slander Law, abrufbar unter: http://www.expertlaw.com/library/personal_injury/defamation.html (letzter Abruf: 17.01.2007)

Lehman, Jeffrey/

Phelps, Shirelle (Hrsg.), West´s Encyclopedia of American Law, 2. Aufl., Detroit, 2005

Lehnhardt, Joachim, Löschung virenbehafteter Emails, Eine Radikalkur und ihre rechtlichen Folgen, DuD 2003, S. 487 ff.

Leibholz, Gerhard/ Rinck, Hans- Justus/ Hesselberger, Dieter (Begr.), Grundgesetz für die Bundesrepublik Deutschland. Kommentar. Rechtsprechung des Bundesverfassungsgerichts, 43. Ergänzungslieferung, Köln-Marienburg, 2005 [Zitat: *Leibholz/Rinck*]

Leible, Stefan/ Sosnitza, Olaf, Telefonwerbung und Fernabsatzrichtlinie, K&R 1998, S. 283 ff.

Leicht, Armin, Computerspionage -Die „besondere Sicherung gegen unberechtigten Zugang“ (§ 202 a StGB), IuR 1987, S. 45 ff.

Leistner, Matthias/ Pothmann, Julia, E- Mail- Direktmarketing im neuen europäischen Recht und in der UWG-Reform, WRP 2003, S. 815 ff.

Lenckner, Theodor/ Winkelbauer, Wolfgang, Computerkriminalität- Möglichkeiten und Grenzen des 2. WiKG (I), CR 1986, S. 483 ff.

Dies. Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG (III), CR 1986, S. 824 ff.

Lengning, Kurt, Post- und Fernmeldegeheimnis, 3. Aufl., 1967

Lenz, Carl Otto/ Borchardt, Klaus-Dieter, EU- und EG - Vertrag, Kommentar zu dem Vertrag über die Europäische Union und zu dem Vertrag zur Gründung der Europäischen Gemeinschaft, jeweils in der durch den Vertrag von Nizza geänderten Fassung, 3. Aufl., Köln, 2003 [Zitat: *Bearbeiter* in Lenz/Borchardt]

Lepperhoff, Niels/ Tinnefeld, Marie-Theres, Aussagewert von Verkehrsdaten – Aspekte der Sicherheitspolitik, des Datenschutzes und der Wirtschaft, RDV 2004, S. 7 ff.

Lerche, Peter, Werbung und Verfassung, Berlin, 1967

Ders., Aktuelle Grundfragen der Informationsfreiheit, Jura 1995, S. 561 ff.

Lettl, Tobias, Rechtsfragen des Direktmarketing per Telefon und e-mail, GRUR 2000, S. 977 ff.

Ders., Das neue UWG, München, 2004

Ders., Der Schutz der Verbraucher nach der UWG-Reform, GRUR 2004, S. 449 ff.

Leupold, Andreas/ Bräutigam, Peter/ Pfeiffer, Markus, Von der Werbung zur kommerziellen Kommunikation: Die Vermarktung von Waren und Dienstleistungen im Internet, WRP 2000, S. 575 ff.

Lewczak, Joseph, Complying with the Can- Spam Act: New FTC Regulations Provide Guidance on „Primary Purpose", The Computer & Internet Lawyer 2005, Nr. 5, S. 10 ff.

Libertus, Michael, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Weiterverbreitung von Computerviren, MMR 2005, S. 507 ff.

Lindemann, Achim/ Simon, Oliver, Betriebsvereinbarungen zur E-Mail-, Internet- und Intranet-Nutzung, BB 2001, S. 1950 ff.

Lipinski, Klaus (Hrsg.), Handlexikon der Informationstechnologie, 1. Aufl., Bonn, 2004

Lisken, Hans, Telefonmithören erlaubt?, NJW 1994, S. 2069 f.

Lober, Andreas/ Weber, Olaf, Money for Nothing? Der Handel mit virtuellen Gegenständen und Charakteren, MMR 2005, S. 653 ff.

Löwisch, Manfred, Briefkastenwerbung von Parteien, NJW 1990, S. 437 f.

Louis, Hans Walter, Grundzüge des Datenschutzrechts, Köln u.a., 1981

Lübbe-Wolff, Die Grundrechte als Eingriffsabwehrrechte, Baden-Baden, 1988

Lüder, Tilman E., Die Grenzen der Keck- Rechtsprechung, EuZW 1996, S. 615 ff.

Lührs, Wolfgang, Eingeschränkte Beschlagnahmemöglichkeit von „Mailbox-Systemen“ aufgrund des Fernmeldegeheimnisses?, wistra 1995, S. 19 f.

Manishin, Glenn B., Joyce, Stephanie A., Current Spam Law & Policy: An Overview and Update, The Computer & Internet Lawyer 2004, Nr. 9, S. 1 ff.

Marberth- Kubicki, Annette, Computer- und Internetstrafrecht, zitiert: Marberth-Kubicki, Computer- und Internetstrafrecht, München, 2005

Masing, Johannes, Vorrang des Europarechts bei umsetzungsgebundenen Rechtsakten, NJW 2006, S. 264 ff.

Marly, Jochen, Die Qualifizierung der Computerprogrammen als Sache nach § 90 BGB, BB 1991, S. 432 ff.

Maunz, Theodor/ Dürig, Günter/ Herzog, Roman/ Scholz, Rupert/ Herdegen, Matthias/ Klein, Hans (Hrsg.) Grundgesetz. Kommentar,
Band I: Art. 1- 5 GG
Band II: Art. 6 - 16 a GG
Band III: Art. 17-27 GG
Band IV: Art. 28 - 9 GG
47. Lieferung, München, 2006
[Zitat: *Bearbeiter* in Maunz/Dürig]

McCullagh, Declan, Privacy Laws: Not Gonna Happen, abrufbar unter: http://www.wired.com/news/politics/1,42123-0.html (letzter Abruf: 11.01.2007)

Medicus, Dieter, Entscheidungen des BGH als Marksteine für die Entwicklung des allgemeinen Zivilrechts, NJW 2000, S. 2921 ff.

Meesen, Karl Matthias, Das Grundrecht der Berufsfreiheit, JuS 1982, S. 397 ff.

Mehrings, Josef, Der Rechtsschutz computergeschützter Fachinformationen. Unter besonderer Berücksichtigung von Datenbanken, Baden-Baden, 1990

Meier, Klaus/ Wehlau, Andreas, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, S. 1585 ff.

Meister, Herbert, Das Schutzgut des Datenschutzrechts, DuD 1983, S. 163 ff.

Mengel, Anja, Kontrolle der Telekommunikation am Arbeitsplatz, BB 2004, S. 1445 ff.

Dies., Kontrolle der E- mail und Internetkommunikation am Arbeitsplatz, BB 2004, S. 2014 ff.

Menzel, Andreas, Kompetenzkonflikt zwischen Bund und Land in der Gesetzgebung, DVBl. 1997, S. 640 ff.

Meyer, Jürgen, Charta der Grundrechte der Europäischen Union, 2. Aufl., Baden-Baden, 2006 [Zitat: *Bearbeiter* in Meyer]

Meyer, Sebstian, Cookies & Co. - Datenschutz und Wettbewerbsrecht, WRP 2002, S. 1028 ff.

Meyer-Goßner, Lutz, Beck´sche Kurzkommentare. Strafprozessordnung. Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 49. Aufl., München, 2006

Meyer-Ladewig, Jens, Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Handkommentar, 1. Aufl., Baden-Baden, 2003 [Zitat: *Meyer-Ladewig*]

Ders./ Petzold, Herbert, Die Bindung deutscher Gerichte an Urteile des EGMR- Neues aus Straßburg und Karlsruhe, NJW 2005, S. 15 ff.

Miller, Gary, How to Can Spam, 2 Van. J. Ent. L. & Prac., 127 ff. (2000)

McDonagh, Maeve, Freedom of Information in Common Law Jurisdictions- The Experience and the Challenge, MMR 2000, S. 251 ff.

Möhrenschlager, Manfred, Das neue Computerstrafrecht, wistra 1986, S. 128 ff.

Möller, Hauke, Regulierung anonymer E-Mail, DuD 2000, S. 267 ff.

Ders., Gesetzliche Vorgaben für anonyme E-Mail, DuD 2000, S. 344 ff.

Montag, Frank, Gewerbliche Schutzrechte, wesentliche Einrichtungen und Normung im Spannungsfeld zu Art. 86 EGV, EuZW 1997, S. 71 ff.

Moos, Flemming, Dürfen Access-Provider IP-Nummern speichern? Analyse und Kritik der T-Online-Entscheidung der

hessischen Datenschutz-Aufsichtsbehörde, CR 2003, S. 386 ff.

Müller, Wolfgang, Duden. Bedeutungswörterbuch, 2. Aufl., Mannheim, 1985

Müller-Dehn, Christian, Das Postgeheimnis nach § 5 PostG und die Postreform, DÖV 1996, S. 863 ff.

Müller-Graff, Die Verdichtung des Binnenmarktrechts zwischen Handlungsfreiheit und Sozialgestaltung, EuR Beiheft 1/2001, S. 7 ff.

Muhl, Charles J., Workplace e- mail and Internet use: employees and employers beware, Monthly Labor Review, Februar 2003, S. 36 ff.

Nägele, Stefan/ Meyer, Lars, Internet und E-Mail am Arbeitsplatz: Rechtliche Rahmenbedingungen der Nutzung und Kontrolle sowie der Reaktion auf Missbrauch, K & R 2004, S. 312 ff.

Nicolaysen, Gert, Die gemeinschaftsrechtliche Begründung von Grundrechten, EuR 2003, S. 719 ff.

Ders./ Nowak, Carsten, Teilrückzug des BVerfG aus der Kontrolle der Rechtmäßigkeit gemeinschaflicher Rechtsakte: Neuere Entwicklungen und Perspektiven, NJW 2001, S. 1233 ff.

Niedermeier, Robert, Schröcker, Stefan, Ersatzfähigkeit immaterieller Schäden aufgrund rechtswidriger Datenverarbeitung, RDV 2002, S. 217 ff.

Notthoff, Martin, Grundrechte in der Europäischen Gemeinschaft, RIW 1995, S. 541 ff.

Nucleus Research, Spam: The Serial ROI Killer, abrufbar unter: http://www.nucleusresearch.com/research/e50.pdf (letzter Abruf: 25.01.2007)

Nunziato, Dawn N., The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L. J., S. 1115 ff. (2005)

Oeter, Stefan, „Drittwirkung" der Grundrechte und die Autonomie des Privatrechts, AöR 119 (1994), S. 529 ff.

Ohlenburg, Anna, Die neue EU-Datenschutzrichtlinie 2002/58/EG- Auswirkungen und Neuerungen für elektronische Kommunikation, MMR 2003, S. 82 ff.

Dies. Der neue Telekommunikationsdatenschutz - Eine Darstellung von Teil 7 Abschnitt 2 TKG, MMR 2004, S. 431 ff.

Ohly, Ansgar, Harmonisierung des Persönlichkeitsrechts durch den Europäischen Gerichtshof für Menschenrechte? - Rechtsvergleichende Anmerkungen zum Urteil in der Sache von Hannover/Deutschland, GRUR Int. 2004, S. 902 ff.

Oppermann, Thomas, Wirtschaftswerbung und Art. 5 GG, Festschrift für Gerhard Wacke, Köln, 1972, S. 393 ff.

Ordemann, Hans-Joachim/ Schomerus, Rudolf, Bundesdatenschutzgesetz. Kommentar, 1. Aufl., München, 1988

Ossenbühl, Fritz, Eine Fehlerlehre für untergesetzliche Normen, NJW 1986, S. 2805 ff.

Ostendorf, Heribert, Grundzüge der konkreten Gefährdungsdelikte, JuS 1982, S. 426 ff.

Otto, Harro, Die objektive Zurechnung eines Erfolges im Strafrecht, Jura 1992, S. 90 ff.

Ovey, Clare/ White, Robin, Jacobs and White, The European Convention On Human Rights, 3. Aufl., Oxford, 2002 [Zitat: *Ovey/White*, ECHR]

Paaß, Gerhard, Anonymität statistischer Einzelangaben, DuD 1985, S. 97 ff.

Pache, Eckhard, Die Europäische Menschenrechtskonvention und die deutsche Rechtsordnung, EuR 2004, S. 393 ff.

Palandt, Otto (Begr.), Bürgerliches Gesetzbuch Kommentar, 66. Auflage, München, 2007 [Zitat: *Bearbeiter* in Palandt]

Palm, Franz, Die Übermittlung personenbezogener Daten in das Ausland, CR 1998, S. 65 ff.

Ders./ Roy, Rudolf, Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, NJW 1996, S. 1791 ff.

Dies., Der BGH und der Zugriff auf Mailboxen, NJW 1997, S. 1904 ff.

Papier, Hans-Jürgen, Die Beeinträchtigungen der Eigentums- und Berufsfreiheit durch Steuern vom Einkommen und Vermögen, Der Staat 11 (1972), S. 483 ff.

Ders., Art. 12 GG- Freiheit des Berufs und Grundrecht der Arbeit, DVBl. 1984, S. 801 ff.

Paul, Carsten, Zusammengesetztes Delikt und Einwilligung, Berlin, 1997

Pearce, Graham/ Platten, Nicholas, Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective, 22 Fordham Int´l L. J., S. 2024 ff. (1999)

Peeters, Maarten, Identity Theft Scandals in the U.S.: Opportunity to Improve Data Protection, MMR 2005, S. 415 ff.

Peitsch, Dietmar, Grundrechtswesentlichkeit polizeilicher Informationssammlung und -verarbeitung, CR 1989, S. 721 ff.

Penski, Ulrich/ Elsner, Bernd Roland, Eigentumsgewährleistung und Berufsfreiheit als Gemeinschaftsgrundrechte in der Rechtsprechung des Europäischen Gerichtshofs, DÖV 2001, S. 265 ff.

Pernice, Ingolf, Gemeinschaftsverfassung und Grundrechtsschutz-Grundlagen, Bestand und Perspektiven, NJW 1990, S. 2409 ff.

Pfeiffer, Gerd, Strafprozeßordnung und Gerichtsverfassungsgesetz. Kommentar, 4. Aufl., München, 2002

Pieroth, Bodo, Der Wert der Auffangfunktion des Art. 2 Abs. 1 GG. Zu einem bundesverfassungsinternen Streit um die allgemeine Handlungsfreiheit, AöR 115 (1990), S. 33 ff.

Ders./ Schlink, Bernhard, Grundrechte - Staatsrecht II, 22. Aufl., Heidelberg, 2006

Pietrzak, Alexandra, Die Schutzpflicht im verfassungsrechtlichen Kontext - Überblick und neue Aspekte, JuS 1994, S. 748 ff.

Pietzcker, Jost, Zur Inzidentverwerfung untergesetzlicher Rechtsnormen durch die vollziehende Gewalt, AöR 101 (1976), S. 374 ff.

Piper, Henning/ Ohly, Ansgar, Gesetz gegen den unlauteren Wettbewerb, 4. Aufl., München, 2006

Podlech, Adalbert, Das Recht auf Privatheit, in Joachim Perels (Hrsg.), Grundrechte als Fundament der Demokratie, Frankfurt a.M., 1979, S. 50 ff.

Ders./ Pfeifer, Michael Die informatielle Selbstbestimmung im Spannungsverhältnis zu modernen Werbestrategien, RDV 1998, S. 139 ff.

Post- Ortmann, Karin, Der Arbeitgeber als Anbieter von Telekommunikations- und Telediensten, RDV 1999, S. 102 ff.

Postel, Jonathan, Request for Comments (RFC): 793, Transmission Control Protocol- DARPA Internet Program Protocol Specification, abrufbar unter: http://www.ibiblio.org/pub/docs/rfc/rfc793.txt (letzter Abruf: 21.08.2006)

Quilter, Laura, The Continuing Expansion of Cyberspace Trespass to Chattels, 17 Berkeley Tech. L. J., S. 421 ff. (2002)

Rebmann, Kurt/ Säcker, Franz Jürgen/ Rixecker, Roland (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, München, Band 1, 1. Halbband (§§ 1-240), 2006; Band 2 a (§§ 241-432), 4. Aufl., 2006, Band 5 (§§ 705-853.Partnerschaftsgesetz. Produkthaftungsgesetz), 4. Aufl., 2004, Band 6 (§§ 854-1296), 4. Aufl., 2004 [Zitat: *Bearbeiter* in Münchener Kommentar]

Reichelsdorfer, Jörg, „eMails“ zu Werbezwecken- ein Wettbewerbsverstoß?, GRUR 1997, S. 191 ff.

Reidenberg, Joel R., Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L. J., S. 195 ff. (1992)

Reimann, Mathias, Einführung in das US- amerikanische Privatrecht, 2. Auflage, München, 2004

Ders., Anmerkung zum Urteil LG Traunstein, CR 1998, S. 172 f.

Rengeling, Hans-Werner/ Szczekalla, Peter, Grundrechte in der Europäischen Union, Köln. München u.a., 2004 [Zitat: *Rengenling/Szczekalla*]

Ricker, Reinhardt, Rechte und Pflichten der Medien unter Berücksichtigung des Rechtsschutzes des einzelnen, NJW 1990, S. 2097 ff.

Riemann, Thomas, Künftige Regelungen des grenzüberschreitenden Datenverkehrs, CR 1997, S. 762 ff.

Rieß, Peter (Hrsg.), Löwe-Rosenberg. Die Strafprozeßordnung und das Gerichtsverfassungsgesetz. Großkommentar. 25. Aufl., Berlin, 2004 [Zitat: *Bearbeiter* in Löwe-Rosenberg]

Rittweger, Christoph/ Schmidl, Michael, E-Mail-Filterung -Stellungnahme der Art. 29-Gruppe, MMR 2006, S. XI f.

Rönnau, Thomas, Voraussetzungen und Grenzen der Einwilligung im Strafrecht, Jura 2002, S. 665 ff.

Roessler, Thomas, Vermeidung von Spuren im Netz, in Bäumler (Hrsg.), E-Privacy. Datenschutz im Internet, 2000, S. 205 ff.

Rötzer, Florian, Das Recht auf Anonymität, in in Bäumler (Hrsg.), E-Privacy. Datenschutz im Internet, 2000, S. 27 ff.

Rojas, Raúl (Hrsg.), Encyclopedia of Computers and Computer History, Chicago, 2001

Rosenbaum, Joseph I., Privacy on the Internet: Whose Information is it Anyway?, 38 Jurimetrics J., S. 565 ff., (1998)

Roßnagel, Alexander/ Scholz, Philip, Datenschutz durch Anonymität und Pseudonymität- Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, S. 721 ff.

Ders./ Pfitzmann, Andreas/ Garstka, Hansjürgen, Modernisierung des Datenschutzrechts, DuD 2001, S. 253 ff.

Ders. (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München, 2003 [Zitat: *Bearbeiter* in Roßnagel]

Ders., Regulierung und Selbstregulierug im Datenschutz, abrufbar unter http://www.emr-sb.de/news/JTG-Selbstreg-PDF (letzter Abruf: 19.12.2006);

Rother, Jaenine, Die Geschichte der Computerviren, abrufbar unter: http://www.securitymanager.de (letzter Abruf: 11.01.2007)

Rudolphi, Hans-Joachim/ Horn, Eckhard/ Günther, Hans-Ludwig/ Hoyer, Andreas, Systematischer Kommentar zum Strafgesetzbuch. Loseblattausgabe, Band 1, Allgemeiner Teil, 7. Aufl., 2000, Band 2 bis 4, Besonderer Teil, 6. Aufl., 2000 [Zitat: *Bearbeiter* in Systematischer Kommentar]

Rüpke, Giselher, Der verfassungsrechtliche Schutz der Privatheit, Zugleich ein Versuch pragmatischen Grundrechtsverständnisses, Baden-Baden, 1976

Ders., Perspektiven für ein europäisches Datenschutzrecht, Überlegungen zum Richtlinienvorschlag n.F. aus britischer und deutscher Sicht für die Datenverarbeitung im Bereich von Wirtschaft und Beruf- Eine Betrachtung aus deutscher Sicht, EuZW 1993, S. 149 ff.

Ruess, Peter/ Patzak, Andrea, Marktortprinzip und Nutzerortung –Gedanken zum Problemfeld Internationales Wettbewerbsrecht und Datenschutz im Internet, RDV 2003, S. 167 ff.

Ruffert, Matthias, Die Mitgliedstaaten der Europäischen Gemeinschaft als Verpflichtete der Gemeinschaftsgrundrechte, EuGRZ 1995, S. 518 ff.

Sachs, Michael (Hrsg.), Grundgesetz Kommentar, 3. Aufl., München, 2003

Sack, Rolf, Deliktsrechtlicher Verbraucherschutz gegen unlauteren Wettbewerb, NJW 1975, S. 1303 ff.

Säcker, Franz Jürgen, Das UWG zwischen den Mühlsteinen europäischer Harmonisierung und grundrechtsgebotener Liberalisierung, WRP 2004, S. 1199 ff.

Saeltzer, Gerhard, Sind diese Daten personenbezogen oder nicht? – Wie der Personenbezug von Daten, auch biometrischer, sich fundiert prüfen lässt..., DuD 2004, S. 218 ff.

Sankol, Barry, Die Qual der Wahl: § 113 TKG oder §§ 100 g, 100 h StPO?- Die Kontroverse über das Auskunftsverlangen von Ermittlungsbehörden gegen Access-Provider bei dynamischen IP-Adressen, MMR 2006, S. 361 ff.

Ders., Strafprozessuale Zwangsmaßnahmen und Telekommunikation -Der Regelungsgehalt der §§ 100 a ff. StPO, JuS 2006, S. 698 ff.

Ders., Ermittlungsbehördliche Zugriffe auf E-Mails im Serverbereich, MMR 2006, Heft 12, S. XXX ff.

Schaar, Peter, Datenschutzfreier Raum Internet?, CR 1996, S. 170 ff.

Ders., Was lange währt...Gesetzgebungsverfahren zum BDSG abgeschlossen, MMR 2001, Heft 6, S. 345 f.

Ders., Datenschutzrechtliche Einwilligung im Internet, MMR 2001, S. 644 ff.

Ders, Datenschutz im Internet- Die Grundlagen, München, 2002 [Zitat als: *Schaar*, Datenschutz im Internet]

Schaffland, Hans-Jürgen/ Wiltfang, Noeme, Bundesdatenschutzgesetz. Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Berlin, 2004

Scheffler, Uwe, Die Wortsinngrenze bei der Auslegung, Jura 1996, S. 505 ff.

Scherer, Joachim, Das Bronner- Urteil des EuGH und die Essential facilities - Doktrin im TK- Sektor, MMR 1999, S. 315 ff.

Scheurle, Klaus-Dieter/ Mayen, Thomas (Hrsg.), Telekommunikationsgesetz. Kommentar, 2. Aufl., München, 2007

Schild, Hans-Hermann, Die Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, EuZW 1999, S. 69 ff.

Schild, Wolfgang, Das strafrechtliche Problem der Sportverletzung (vorwiegend im Fußballkampfspiel), Jura 1982, S. 520 ff.

Schmid, Pirmin, Computerhacken und materielles Strafrecht -unter besonderer Berücksichtigung des § 202 a, 2001, abrufbar unter: http://deposit.db.de/cgin-bin/dokserv?idn=96239971x&dok_var=d1&dok_ext=pdf&filename=96239971x.pdf (letzter Abruf: 30.01.2007)

Schmidl, Michael, E- Mail- Filterung am Arbeitsplatz, MMR 2005, S. 343 ff.

Ders. Private E- Mail- Nutzung - Der Fluch der guten Tat, DuD 2005, S. 267 ff.

Schmidt, Joachim/ Königshofen, Thomas/ Zwach, Ulrich, Telekommunikationsrecht der Bundesrepublik Deutschland, 19. Aufl., Heidelberg, 2000

Schmidt, Walter, Die bedrohte Entscheidungsfreiheit, JZ 1974, S. 241 ff.

Schmidt- Bleibtreu, Bruno/ Klein, Franz (Begr.), Kommentar zum Grundgesetz, 10. Aufl., München, 2004

Schmitt Glaeser, Walter Das Grundrecht auf Informationsfreiheit, Jura 1987, S. 567 ff.

Ders., Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts, AöR 113 (1988), S. 52 ff.

Schmittmann, Jens, Anmerkung zum Urteil des LG Berlin, Beschluss v. 14. Mai 1998 - 16 O 301/98, CR 1998, S. 499 f.

Ders., Anmerkung zu dem Urteil BGH XI ZR 76/98, MMR 1999, S. 478 ff.

Ders., Rechtliche Aspekte der Short-Message-Service-Werbung, MMR 1998, 346 ff.

Ders., Anmerkung zu OLG Hamburg, MMR 2000, 611 ff., MMR 2000, S. 616

Schmitz, Thomas, Die EU- Grundrechtscharta aus grundrechtsdogmatischer und grundrechtstheoretischer Sicht, JZ 2001, S. 833 ff.

Ders., Die Grundrechtecharta als Teil der Verfassung der Europäischen Union, EuR 2004, S. 691 ff.

Schnapp, Friedrich, Die Verhältnismäßigkeit des Grundrechtseingriffs, JuS 1983, S. 850 ff.

Schneider, Hans, Verfassungsrechtliche Beurteilung des Volkszählungsgesetzes 1983, DÖV 1984, S. 161 ff.

Schneider, Michael, Selbstregulierung der Wirtschaft, in Bäumler (Hrsg.), E-Privacy. Datenschutz im Internet, Braunschweig u.a., 2000, S. 153 ff.

Schönke, Adolf, Schröder, Horst (Hrsg.), Strafgesetzbuch Kommentar, 27. Aufl., München, 2006

Scholz, Rupert, Wie lange bis „Solange III“?, NJW 1996, S. 941 ff.

Schrick, Alexandra, Direktmarketing mittels E- Mail und seine Entwicklung, MMR 2000, S. 399 ff.

Schricker, Gerhard, Schadensersatzansprüche der Abnehmer wegen täuschender Werbung?- Betrachtungen im Anschluss an die Prüfzeichen – Entscheidung des BGH vom 14. Mai 1974, GRUR 1975, S. 111 ff.

Ders. (Hrsg.), Recht der Werbung in Europa, Bonn, 1990

Ders., Zur wettbewerbsrechtlichen Beurteilung der Telefonwerbung im geschäftlichen Bereich, GRUR Int. 1998, S. 541 ff.

Schütz, Raimund, Kommunikationsecht. Regulierung von Telekommunikation und elektronischen Medien, München, 2005

Schulz, Wolfgang, Verfassungsrechtlicher „Datenschutzauftrag" in der Informationsgesellschaft- Schutzkonzepte zur Umsetzung informationeller Selbstbestimmung am Beispiel der Online- Kommunikation, Die Verwaltung 1999, S. 137 ff.

Schulze, Reiner/ Zuleeg, Manfred, Europarecht, Handbuch für die deutsche Rechtspraxis, Baden- Baden, 2006

Schulze-Heming, Ingeborg, Der strafrechtliche Schutz von Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Münster u.a., 1995

Schuppert, Gunnar Folke, Rigidität und Flexibilität von Verfassungsrecht. Überlegungen zur Steuerungsfunktion von Verfassungsrecht in normalen wie in „schwierigen Zeiten", AöR 120 (1995), S. 32 ff.

Schuster, Fabian, Die Grenzen polizeilicher Ermittlungen in Bäumler (Hrsg.), E-Privacy. Datenschutz im Internet, Braunschweig u.a., 2000, S. 77 ff. [Zitat als: Schuster in Bäumler]

Ders., Müller, Ulf Enwicklung des Internet- und Multimediarechts von Januar 1999 bis Juni 2000, MMR 2000/Beilage 20, S. 1 ff.

Dies., Entwicklung des Internet- und Multimediarechts von Juli 2000 bis März 2001, MMR 2001/Beilage 7, S. 1 ff.

Dies./ Drewes, Stefan Entwicklung des Internet- und Mulitmediarechts von April bis Dezember 2001, MMR 2002/Beilage 3, S. 1 ff.

Schwabe, Jürgen, Die Stufentheorie des Bundesverfassungsgerichts zur Berufsfreiheit, DÖV 1969, S. 734 ff.

Schwan, Eggert, Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, Verwaltungsarchiv 1975, S. 120 ff.

Schwarze, Jürgen (Hrsg.), EU – Kommentar, Baden- Baden, 2000

Ders., Der Verfassungsentwurf des Europäischen Konvents, Baden-Baden, 200

Schwartz, Paul M./ Reidenberg, Joel R. Data Privacy Law. A Study of United States Data Protection, Charlottesville u.a., 1996

Schwerdtner, Peter, Der zivilrechtliche Persönlichkeitsschutz, JuS 1978, S. 289 ff.

Seer, Roman, Die Unvereinbarkeitserklärung des BVerfG am Beispiel seiner Rechtsprechung zum Abgabenrecht, NJW 1996, S. 285 ff.

Seichter, Dirk, Die Umsetzung der Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, WRP 2006, S. 391 ff.

Seidel, Gerd, Handbuch der Grund- und Menschenrechte auf staatlicher, europäischer und universeller Ebene, Eine vergleichende Darstellung der Grund- und Menschenrechte des deutschen Grundgesetzes, der Europäischen Menschenrechtskonvention von 1950 und des Internationalen Pakts über bürgerliche und politische Rechte von 1966 sowie der Entscheidungspraxis des Bundesverfassungsgerichts und der zuständigen Vertragsorgane, Baden-Baden, 1996 [Zitat: *Seidel*, Handbuch]

Seifert, Fedor, Postmortaler Schutz des Persönlichkeitsrechts und Schadensersatz – Zugleich ein Streifzug durch die Geschichte des allgemeinen Persönlichkeitsrechts, NJW 1999, S. 1889 ff.

Seitz, Walter, Prinz und Prinzessin- Wandlungen des Deliktsrechts durch Zwangskommerzialisierung der Persönlichkeit, NJW 1996, S. 2848 ff.

Shah, Rajiv, History of the Finger Protocol, abrufbar unter: http://www.rajivshah.com/Case_Studies/Finger/Finger.htm, (letzter Abruf: 21.08.2006)

Simitis, Spiros, Datenschutz: Von der legislativen Entscheidung zur richterlichen Interpretation, NJW 1981, S. 1697 ff.

Ders., Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S. 398 ff.

Ders., Die EU-Datenschutzrichtlinie - Stillstand oder Anreiz?, NJW 1997, S. 281 ff.

Ders., Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 2000, S. 714 ff.

Ders./ Dammann, Ulrich/ Mallmann, Otto/ Reh, Hans-Joachim, Kommentar zum Bundesdatenschutzgesetz, 1. Aufl., Baden-Baden, 1978 3. Aufl., Baden-Baden, 1981 5. Aufl., Baden-Baden, 2003

Ders. (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 6. Aufl., Baden-Baden, 2006 [Zitat: *Bearbeiter* in Simitis]

Ders./ Dammann/Ulrich (Bearb), Dokumentation zum Bundesdatenschutzgesetz. Bund-Länder-Kirchen-Ausland und Internationales, 39 Lfrg., Baden-Baden, Nov. 2005 [Zitat: Simitis/Dammann, Dokumentation]

Skouris, Wassilios, Der Einfluß des Europäischen Gemeinschaftsrechts auf die Unterscheidung zwischen Privatrecht und Öffentlichem Recht - dargestellt für das öffentliche Auftragswesen und die Privatisierung -,EuR 1998, S. 111 ff.

Soergel, Hans Th. (Begr.), Siebert, Wolfgang (Hrsg.), Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Kommentar, 12. Aufl., Stuttgart, u.a., Band 1 (§§ 1-240 BGB; Haustürwiderrufsgesetz), 1988; Band 2 (§§ 241-432), 1990; Band 5 (§§ 823-853), 1999; Band 6 (§§ 854- 1296), 1990

Solove, Daniel Justin, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev., 1393 ff., (2001)

Ders./ Hoofnagle, Chris Jay, A Model Regime of Privacy Protection, 2006 U. Ill. L. Rev., S. 357 ff.

Spiegel, Gerald, Spuren im Netz. Welche Spuren der Internet-Nutzer hinterlässt und wie man sie vermeiden kann, DuD 2003, S. 265 ff.

Spiekermann, Sarah, Die Konsumenten der Anonymität, DuD 2003, S. 150 ff.

Spindler, Gerald, Haftungsklauseln in Provider- Verträgen, Probleme der Inhaltskontrolle, CR 1999, S. 626 ff.

Ders., Das Gesetz zum elektronischen Geschäftsverkehr- Verantwortlichkeit der Diensteanbieter und Herkunftslandsprinzip, NJW 2001, S. 921 ff.

Ders., *Schmittmann, Jens,* Unerwünschte E- Mail- Werbung- Zivil- und wettbewerbsrechtliche Zulässigkeit in Europa, MMR 2001/Beilage 8, S. 10 ff.

Ders./ *Ernst, Stefan,* Vertragsgestaltung für den Einsatz von E- Mail- Filtern, CR 2004, S. 437 ff.

Ders./ *Schmitz, Peter*/ *Geis, Ivo*, Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, Kommentar, 1. Aufl., München, 2004 [Zitat: *Bearbeiter* in Spindler/Schmitz/Geis]

Steffen, Erich, Schmerzensgeld bei Persönlichkeitsverletzung durch Medien - Ein Plädoyer gegen formelhafte Berechnungsmethoden bei der Geldentschädigung, NJW 1997, S. 10 ff.

Steindorff, Ernst (Hrsg.), Persönlichkeitsschutz im Zivilrecht, Juristische Studiengesellschaft, Karlsruhe, 1983

Sternberg-Lieben, Detlev, Die „Hörfalle“ -Eine Fall für die rechtsstaatliche Strafverfolgung?, Jura 1995, 299 ff.

Ders., Die objektiven Schranken der Einwilligung im Strafrecht, 1997

Störmer, Rainer, Gemeinschaftsrechtliche Diskriminierungsverbote versus nationale Grundrechte?, AöR 123 (1998), S. 541 ff.

Streinz, Rudolf (Hrsg.), EUV/EGV. Vertrag über die Europäische Union und Vertrag zur Gründung der Europäischen Gemeinschaft, 1. Aufl., München, 2003 [Zitat: *Bearbeiter* in Streinz]

Ders., Europarecht, 7. Aufl., Heidelberg, 2005

Strömer, Tobias, Online-Recht. Rechtsfragen im Internet, 4. Aufl., Heidelberg, 2006

Suerbaum, Joachim, Die Schutzpflichtdimension der Gemeinschaftsgrundrechte, EuR 2003, S. 390 ff.

Sweet, Mark, Political E-Mail: Protected Speech or unwelcome Spam?, 2003 Duke L. & Tech. Rev., S. 0001 ff.

Taeger, Jürgen, Datenschutzrechtliche Haftung – insbesondere bei unrichtiger Datenverarbeitung durch fehlerhafte Computerprogramme, RDV 1996, S. 77 ff.

Terwangne, Cécile de, Louveaux, Sophie, Data Protection and Online Networks, MMR 1998, S. 451 ff.

Thym, Daniel, Europäischer Grundrechtsschutz und Familienzusammenführung, NJW 2006, S. 3249 ff.

Tiedemann, Klaus, Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber, JZ 1986, S. 864 ff.

Tinnefeld, Marie-Theres, Ehmann/ Gerling, Eugen, Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 4. Aufl., München, 2005

Tröndle, Herbert, Fischer, Thomas, Strafgesetzbuch und Nebengesetze, 54. Aufl., München, 2007

Tröndle, Rüdiger, „Privacy Policies" und das Internet- Noch immer ein Streitpunkt zwischen den Vereinigten Staaten von Amerika und der Europäischen Union, CR 1999, S. 717 ff.

Trosch, Daniel, Unmittelbare Anwendbarkeit der EG-Datenschutz-Richtlinie, DuD 1998, S. 724

Trute,Hans-Heinrich, Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 1998, S. 822 ff.

Ueckert, Andre, Private Internet- und E-Mail-Nutzung am Arbeitsplatz, ITRB 2003, S. 158 ff.

v. Bogdandy, Armin (Hrsg.), Europäisches Verfassungsrecht, Theoretische und dogmatische Grundzüge, Berlin u.a., 2003 [Zitat: *Bearbeiter* in von Bogdandy]

v. d. Groeben, Hans/ Schwarze, Jürgen (Hrsg.), Kommentar zum Vertrag über die Europäische Union und zur Gründung der Europäischen Gemeinschaft, Band 1 (Art. 1- 53 EUV - Art. 1- Art. 80 EGV), Band 2 (Art. 81 - 97 EGV), Band 4 (Art. 198- 314 EGV), 6. Aufl., Baden-Baden, 2003

v. Hippel, Eike, Grenzen und Wesensgehalt der Grundrechte, Berlin, 1965

v. Jähnke, Burkhard/ Laufhütte Heinrich Wilhelm/ Odersky, Walter, Leipziger Kommentar zum Strafgesetzbuch,
Band 1: Einl., §§ 1 - 32 StGB, 11. Aufl., Berlin, 2003
Band 2: §§ 32 - 60 StGB, 11. Aufl., Berlin, 2003
Band 5: §§ 146 - 222 StGB, 11. Aufl., Berlin, 2005
Band 8: §§ 302 a - 335 a StGB, 11. Aufl., Berlin, 2005
[Zitat: *Bearbeiter* in Leipziger Kommentar]

v. Mangoldt, Hermann (Begr.)/ Klein, Friedrich/ Starck, Christian (Hrsg.) Bonner Grundgesetz. Kommentar, 4. Aufl., München, Band 1 (Präambel, Art. 1 - 19), 1999; Band 2 (Art. 20-78), 2000

v. Münch,Ingo(Begr.)/ Kunig, Philip (Hrsg.), Grundgesetz Kommentar, Band 1, Art. 1- 19 GG, Band 2, Art. 20-69 GG, 5. Aufl., München, 2000

v. Staudinger, J. Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen
Erstes Buch. Allgemeiner Teil: §§ 90 - 133 BGB, 1-54, 63 BeurkG, 13. Bearbeitung, Berlin, 2004
Zweites Buch: §§ 823 - 825 BGB, 13. Bearbeitung, Berlin 1999
Drittes Buch: §§ 985 - 1011 BGB, 13. Bearbeitung, Berlin 1999 [Zitat: *Bearbeiter* in Staudiger]

Varadarajan, Deepa, Tortious Interference and the Law of Contract, The Case for Specific Performance Revisited, The Yale Law Journal 2001, S. 735 ff.

Vehslage, Thorsten, Auswirkungen der Fernabsatzrichtlinie auf die Telefon- und E- Mail- Werbung, GRUR 1999, S. 656 ff.

Verdross, Alfred/ Simma, Bruno, Universelles Völkerrecht, Theorie und Praxis, 3. Aufl., Berlin, 1984

Vogelsang, Klaus, Verfassungsregelungen zum Datenschutz, CR 1995, S. 554 ff.

Volesky, Karl-Heinz, Hacking -Strafbarkeit und Strafwürdigkeit nach englischem Recht. Untersuchung der Vorschläge der britischen Law Comission zur Bekämpfung der Computerkriminalität, CR 1991, S. 553 ff.

Wacke, Gerhard, Werbeaussagen als Meinungsäußerungen, Festschrift für Friedrich Schack, Hamburg, 1966, S. 197 ff.

Warren, Samuel/ Brandeis, Louis, The Right of Privacy, in: 4 Harv. L. Rev., S. 194 ff., (1890)

Wassermann, Rudolf (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland
Band 1, Art. 1- 20 GG, 1. Aufl., Neuwied und Darmstadt, 1984 [Zitat: *Bearbeiter* in Alternativkommentar, 1. Aufl.]

Wassermann, Rudolf, Denninger,Erhard/ Hoffmann-Riem, Wolfgang/ Schneider, Hans-Peter/ Stein, Ekkehardt, (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Reihe Alternativkommentare, 3. Aufl., 2001 [Zitat: *Bearbeiter* in Alternativkommentar, 3. Aufl.]

Weber, Albrecht, Die Europäische Grundrechtscharta-auf dem Weg zu einer europäischen Verfassung, NJW 2000, S. 537 ff.

Weber, Juliane, Mit undurchsichtigen Methoden zum durchsichtigen Verbraucher? Eine wettbewerbsrechtliche Analyse neuer Marketingmethoden zur gezielten Verbraucherwerbung im Internet, DuD 2003, S. 625 ff.

Weiler, Frank, Spamming- Wandel des europäischen Rechtsrahmens, MMR 2003, S. 223 ff.

Weiler, J.H.H./ Lockhart, Nicolas J.S., „Taking Rights Seriously" Seriously: The European Court And Its Fundamental Rights Jurisprudence- Part I, CML Rev. 1995, S. 51 ff.

Dies., „Taking Rights Seriously“ Seriously: The European Court And Its Fundamental Rights Jurisprudence- Part II, CML Rev. 1995, S. 597 ff.

Welp, Jürgen, Strafprozessuale Funktionen der Post, ArchPT 1976, S. 763 ff.

Ders., Datenveränderung (§ 303 a StGB)- Teil 1, IuR 1988, S. 443 ff.

Ders., Wird in das Fernmeldegeheimnis eingegriffen, wenn ein Polizeibeamter im Einverständnis des Telefoninhabers ein Gespräch ohne Wissen des Gesprächspartners mithört?, NStZ 1994, S. 294 ff.

Wendlandt, Bettina, Europäische, deutsche und amerikanische Regelungen von E- Mail- Werbung- Überlegungen zum Nutzen des „CAN- SPAM Act“, MMR 2004, S. 365 ff.

Wente, Jürgen, Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte, NJW 1984, S. 1446 f.

Weise, Karl Theodor, Datenschutz für „Trivialdaten“, DuD 1989, S. 79 ff.

Weißnicht, Elmar, Die Nutzung des Internet am Arbeitsplatz, MMR 2003, S. 448 ff.

Weitnauer, Wolfgang (Hrsg.)/ Baumann, Diethelm (Bearb.), Beck´sches Formularbuch E-Commerce, München, 2003 [Zitat als: *Bearbeiter* in Weitnauer]

Westphal, Dietrich, Die neue EG-Richtlinie zur Vorratsdatenspeicherung – Privatsphäre und Unternehmerfreiheit unter Sicherheitsdruck, EuZW 2006, S. 555 ff.

Wiese, Markus, Unfreiwillige Spuren im Netz, in Bäumler (Hrsg.), E-Privacy. Datenschutz im Internet, Braunschweig u.a., 2000, S. 9 ff.

Wikipedia, Die freie Enzyklopädie, abrufbar unter: http://de.wikipedia.org (letzter Abruf: 16.01.2007)

Wind, Irene, Haftung bei der Verarbeitung personenbezogener Daten, RDV 1991, S. 16 ff.

Wittig, Peter, Zum Standort des Verhältnismäßigkeitsgrundsatzes im System des Grundgesetzes, DÖV 1968, S. 817 ff.

Wohlgemuth, Hans H., Auswirkungen der EU – Datenschutzrichtlinie auf den Arbeitnehmerdatenschutz, BB 1996, S. 690 ff.

Ders./
Gerloff, Jürgen, Datenschutzrecht. Eine Einführung mit praktischen Fällen, 3. Aufl., München u.a., 2005

Wollweber, Gottfried, Der Schutz des Grundrechts auf Wahrung des Briefgeheimnisses im Grundgesetz und in der Europäischen Menschenrechtskonvention, Köln, 1967

Wronka, Georg, Auswirkungen der EU - Datenschutzrichtlinie auf die Werbung - Eine praxisbezogene Zusammenfassung, RDV 1995, S. 197 ff.

Wuermeling, Ulrich, Einsatz von Programmsperren, Zivil- und strafrechtliche Aspekte, CR 1994, S. 585 ff.

Ders./
Felixberger, Stefan, Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, CR 1997, S. 230 ff.

Dies., Staatliche Überwachung der Telekommunikation, CR 1997, S. 555 ff.

Wunderlich, Nina, Das Grundrecht der Berufsfreiheit im Europäischen Gemeinschaftsrecht, Baden-Baden, 2000

Zhang, Lily, The Can-Spam Act: An Insufficient Response to the Growing Spam Problem, 20 Berkeley Technology Law Journal, S. 301 ff. (2005)

Zehentmeier, Ursula, Unaufgeforderte E- Mail-Werbung- Ein wettbewerbswidriger Boom im Internet?, BB 2000, S. 940 ff.

Ziem, Claudia, Spamming – Zulässigkeit nach § 1 UWG, Fernabsatzrichtlinie und E- Commerce-Richtlinienentwurf, MMR 2000, S. 129 ff.

Zitelmann, Ernst, Ausschluß der Widerrechtlichkeit, AcP 99 (1906), S. 1 ff.

Zscherpe, Kerstin A., Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, S. 723 ff.

Dies./
Splittgerber, Andreas, Anti- Spam- Gesetz: Inhalt und Auswirkungen der geplanten Regelungen, MMR 2005, S. V ff.

Zuleeg, Manfred, Zum Verhältnis nationaler und europäischer Grundrechte, EuGRZ 2000, S. 511 ff.