Technische Möglichkeiten der Datenerhebung und zivilrechtliche Folgen bei Verstoß gegen die datenschutzrechtlichen Informationspflichten

# Inaugural-Dissertation

zur Erlangung des akademischen Grades eines Doktors der Rechte durch die Rechtswissenschaftliche Fakultät der Westfälischen Wilhelms-Universität zu Münster

vorgelegt von Bonk, Barbara
aus München
2009

| | |
|---|---|
| Erster Berichterstatter: | Prof. Dr. Andreas Thier |
| Zweiter Berichterstatter: | Prof. Dr. Thomas Hoeren |
| Dekan: | Prof. Dr. Hans-Michael Wolffgang |
| Tag der mündlichen Prüfung: | 08.06.2010 |

*Meiner Familie*

# Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2009 von der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster als Dissertation angenommen. Rechtsentwicklung und Literatur sind bis Ende Mai 2009 berücksichtigt ebenso wie der Abruf der in der Arbeit zitierten Webseiten.

Soweit sich in den verwendeten Abbildungen kein Quellennachweis befindet, wurden die Graphiken unter Zuhilfenahme der „Open Clipart Library“ (`http://www.openclipart.org/`) selbst erstellt.

Bedanken möchte ich mich bei Herrn Prof. Dr. Andreas Thier für die Betreuung der Arbeit. Herrn Prof. Dr. Thomas Hoeren danke ich für die Übernahme und rasche Anfertigung des Zweitgutachtens.

Mein herzlicher Dank geht außerdem an das „Max-Planck-Institut für Geistiges Eigentum, Wettbewerbs- und Steuerrecht“ und hier besonders an Herrn Prof. Dr. Dres. h.c. Joseph Straus, der mir stets den nötigen wissenschaftlichen und zeitlichen Freiraum gelassen hat, um diese Arbeit anzufertigen. Ferner an die Mitarbeiter der Bibliothek unter der Leitung von Herrn Peter Weber, deren Kompetenz und Freundlichkeit sicher ihres gleichen sucht.

Der größte Dank geht zum einen an meine Eltern, die durch ihre großzügige Unterstützung meiner Ausbildung diese Promotion erst ermöglicht haben. Zum anderen an meinen Ehemann Daniel, der mich in diesem Lebensabschnitt stets voller Liebe und Geduld unterstützt hat. Meiner Familie widme ich dieses Werk.

# Inhaltsverzeichnis

# A. Einleitung

Das Internet hat sich in den letzten zehn Jahren als Alltagsmedium etabliert. Während 1997 nur 4,1 Millionen Internet-Nutzer in Deutschland zu verzeichnen waren, sind es heute bereits 43,5 Millionen[1]. Durch das rasante Wachstum der Zahl der Internetnutzer bieten auch eine steigende Anzahl von Unternehmen ihre Waren, Dienstleistungen und Informationen im Internet an, so dass der Online-Handel nach Prognose des Deutschen Einzelhandels im Jahr 2009 in Deutschland einen Umsatz in Höhe von 21,9 Milliarden Euro erzielen wird[2].

Die Vorteile der Verbraucher bei der E-Commerce-Nutzung sind vielfältig: Sie können ihre Einkäufe bequem von zu Hause aus erledigen, sind nicht an Ladenöffnungszeiten gebunden und können, wenn sie sich für ein Produkt entschieden haben, den Preis zwischen verschiedenen Anbietern vergleichen, um sich daraufhin für den günstigsten Anbieter zu entscheiden.

Der Unternehmer wiederum ist nicht länger an bestimmte Standorte gebunden und muss weniger Lagerkapazitäten bereithalten, erzielt also zum einen durch die Nutzung des Internets eine Kosternersparnis und ist zum anderen in der Führung seines Unternehmens zeitlich und örtlich flexibler.

Gleichzeitig erhält er aber durch die elektronische Vertragsabwicklung neue Möglichkeiten der Information und der Bewerbung des Kunden. Das Medium Internet ermöglicht es dem Unternehmer, dank seiner technischen Abläufe, jeden virtuellen Schritt des Verbrauchers zu beobachten. Vom ersten Besuch des Online-Shops, über das Stöbern durch das Angebot, bis hin zur Auswahl und

[1] ADR/ZDF-Onlinestudie 2009, zu finden unter `www.ARD-ZDF-Onlinestudie.de`.

[2] Ältester Vergleichswert ist hier von 1999; 1,25 Milliarden Euro, siehe `http://www.ebusiness-handel.de`.

Bestellung der Ware, kann der Unternehmer nicht nur detailliert die Nutzung des Kunden verfolgen, sondern diese auch dauerhaft speichern.

Das Medium Internet birgt daher nicht nur neue Herausforderungen für Unternehmer, sondern auch für die Gewährleistung des Datenschutzes ihrer Kunden. Das Internet mit seinen unendlichen Möglichkeiten eröffnet nicht nur einen unendlichen Zugriff des Staats auf die Daten seiner Bürger, sondern öffnet auch der Privatwirtschaft unendliche Zugriffsmöglichkeiten auf die Daten der Kunden oder Privatleute insgesamt[3]. Ein effektiver Datenschutz des Kundens kann aber nur durch ein hohes Maß an Transparenz erreicht werden. Eine transparente Datenerhebung und damit eine tatsächliche informationelle Selbstbestimmung des Kundens kann nur erreicht werden, wenn der Kunde über die Erhebungs- und Verarbeitungszusammenhänge umfassend informiert wird. Diese umfassende Information wiederum gewinnt ihre besondere Bedeutung bei der elektronischen Datenverarbeitung, da von dieser durch die gezielte Nutzung der Technik von Seiten des Unternehmers ein ungleich größeres Gefährdungspotenzial ausgeht, als im Offline-Bereich: Anders als bei Rechtsgeschäften unter Anwesenden in der „realen Welt“ hat hier meist nur der Anbieter den Überblick über die einzelnen Verarbeitungsvorgänge. Der Kunde hingegen hat ohne ausreichende Information durch den Anbieter keinerlei Möglichkeiten festzustellen, welche seiner Daten zu welchem Zeitpunkt und zu welchem Zweck verarbeitet werden.

Nach dem Prinzip *ubi jus, ibi remedium*[4] ist eine umfassende Information durch den Anbieter aber nur dann gewährleistet, wenn dem Kunden bei Verstößen gegen die Informationspflichten ausreichende Rechtsansprüche gegen den Anbieter zur Verfügung stehen. Ziel der vorliegenden Arbeit ist es daher, die zivilrechtlichen Rechtsfolgen bei Verstoß gegen die datenschutzrechtlichen Informationspflichten zu prüfen. Während sowohl das Bundesdatenschutzgesetz

[3] Zu den Anfängen der EDV siehe bereits *Bull*, Verwaltung durch Maschinen - Rechtsprobleme der Technisierung der Verwaltung.
[4] Dort wo es Recht gibt, gibt es auch ein Rechtsmittel.

als auch die bereichsspezifischen Regelungen (namentlich das Telemediengesetz und das Telekommunikationsgesetz) Straf- und Bußgeldvorschriften enthalten (§§ 43, 44 BDSG, § 16 TMG, §§ 148, 149 TKG), findet sich in den datenschutzrechtlichen Normen nur wenig zu den zivilrechtlichen Folgen (hier v.a. Schadensersatz nach § 7 BDSG und Berichtigung, Löschung und Sperrung nach § 35 BDSG). Es gilt also festzustellen, ob sich über diese Ansprüche hinaus auch welche aus den allgemeinen zivilrechtlichen Normen und welche Konkurrenzen sich hier zwischen den allgemeinen Ansprüchen und den besonderen Regelungen ergeben.

Da ein Bewusstsein des Gefährdungspotenzials des Internets für personenbezogene Daten und dessen rechtliche Bewertung die Kenntnis der teilweise komplexen, technischen Vorgänge voraussetzt, wird zunächst auf die verschiedenen technischen Möglichkeiten der Datenerhebung[5] grundlegend und allgemein verständlich eingegangen. Nach einer kurzen Zusammenfassung der historischen Entwicklung des allgemeinen Datenschutzrechts und des Multimediadatenschutzrechtes[6] und einen Überblick über die Phasen der Datenverarbeitung sowie der verschiedenen Datentypen[7] werden sodann die verschiedenen datenschutzrechtlichen Informationspflichten und deren Inhalt aufgezeigt.

Die praktische Relevanz der Thematik wird am Beispiel des bekannten Online-Händlers Amazon veranschaulicht[8], indem illustriert wird, an welchen Stellen der Nutzung datenschutzrechtliche Belange berührt werden, welche Informationspflichten sich daraus ergeben und von welchen Möglichkeiten Amazon Gebrauch macht, um diese zu erfüllen. Anhand der Datenschutzerklärung von Amazon werden Privacy Policies erörtert und geprüft, ob die Datenschutzerklärung von Amazon die entstehenden Informationspflichten im vollen Um-

[5] Kapitel B. auf Seite 5.
[6] Kapitel C. auf Seite 49.
[7] Kapitel D. auf Seite 73.
[8] Kapitel F. auf Seite 117.

fang erfüllt. Auch die mögliche Parallelität zwischen Privacy-Policies und der Einbeziehung allgemeiner Geschäftsbedingungen wird geschildert.

Abschließend werden die rechtlichen Folgen bei Verstößen gegen die Informationspflichten erläutert[9], wobei zunächst die Rechtsfolgen nach dem BDSG und dann die Folgen nach dem allgemeinen Zivilrecht beleuchtet werden. Hierbei liegen die Schwerpunkte insbesondere auf vertraglichen Ansprüchen wie den Rechtsfolgen bei Verletzung der vertraglichen Nebenpflichten (*culpa in contrahendo* (vorvertragliches Verschulden) und positive Vertragsverletzung), einer möglichen Anfechtung des Vertrages sowie dem erweiterten Widerrufsrecht bei Verstoß gegen Informationspflichten bei Fernabsatzverträgen und im elektronischen Rechtsverkehr. Darüber hinaus werden eventuelle delikts- und bereicherungsrechtliche, aber auch wettbewerbsrechtliche Folgen aufgezeigt.

Insbesondere bei der Prüfung eines eventuellen Anspruchs auf Geldersatz bei immateriellen Schäden, welcher bei der Verletzung des Rechts auf informationelle Selbstbestimmung besonders relevant ist, ist festzustellen, dass der momentane Rechtsschutz des Kunden nicht ausreicht und ein dringender Änderungsbedarf bei der datenschutzrechtlichen Gesetzgebung besteht. Denn nur, wenn die Überprüfung der verschiedenen Ansprüche ergibt, dass ein ausreichender Rechtsschutz des Kunden in Bezug auf die Erfüllung der datenschutzrechtlichen Informationspflichten durch den Anbieter gegeben ist, ist zu erwarten, dass auch die weitere Entwicklung des Internets nicht zu 42,7 Millionen gläsernen Kunden führt. Allein ein effektiver Datenschutz kann dafür sorgen, dass das Alltagsmedium Internet nicht zu einem alltäglichen und unkontrollierten Öffentlichwerden der Daten jedes Einzelnen führt.

[9] Kapitel G. auf Seite 155.

# B. Technische Möglichkeiten der Datenerhebung

## I. Kommunikation im Internet

Um das Verständnis der im Rahmen dieser Arbeit aufgeführten technischen Möglichkeiten der Datenerhebung[1] näher zu bringen, soll an dieser Stelle zunächst die Kommunikation im Internet mittels der dort benutzten TCP/IP-Verbindungen skizziert werden. Dazu gilt es zunächst zu erkennen, dass diese Kommunikation sich von den traditionellen Kommunikationsmedien wie z. B. der Festnetztelefonie schon allein dadurch unterscheidet, dass die Kommunikation nicht linear aufgebaut ist. Die Kommunikation im Internet geht vielmehr stets in mehreren Schichten vonstatten, welche im Folgenden einzeln geschildert werden.

Bei TCP/IP entsprechen die Spezifikationen dieser Schichten dem TCP/IP-Referenzmodell, das auf den Vorschlägen basiert, die bei der Fortentwicklung des ARPANETs gemacht wurden[2].

[1] Diese gelten gleichermaßen für die Tatbestände der Verarbeitung und Nutzung, zur vorliegend benutzten Terminologie s. Kapitel D. auf Seite 73.

[2] Demzufolge wird im Rahmen dieser Arbeit lediglich auf das TCP/IP-Referenzmodell und nicht auf das von der International Standards Organisation (ISO) entwickelte ISO/OSI-Referenzmodell eingegangen, das heutzutage häufig in Lehrbüchern (so z.B. in *Krüger/Reschke*, Lehr- und Übungsbuch Telematik. Netze, Dienste, Protokolle, S. 20ff.) zu finden ist und das die Aufgaben und Probleme der Netzwerkkommunikation etwas detaillierter unterteilt. Für einen Vergleich zwischen den beiden Modellen siehe *Meinel/Sack*, WWW, S. 7.

## 1. Das TCP/IP-Referenzmodell

Das TCP/IP-Referenzmodell besteht aus vier Schichten.

Die unterste Schicht ist dabei die *Netzwerkschicht*[3]. Sie stellt den direkten Kontakt zur Netzzugangshardware her und legt die Art und Weise fest, in der die IP-Pakete über das Netzwerk übertragen werden. Ihre Protokolle sind im TCP/IP-Referenzmodell nicht definiert, gebräuchlich sind aber LAN[4]-Protokolle wie Ethernet und WLAN (Wireless LAN) oder PPP (Point to Point Protocol) für Modemverbindungen.

Darüber befindet sich die *Internetschicht*. In dieser Schicht erhält der Computer seine „Hausnummer", die IP-Adresse[5]. Die Internetschicht ist zum einen dafür verantwortlich, dass der einzelne Computer im Netz eindeutig auffindbar ist, also eine weltweit eindeutige „Hausnummer" erhält, zum anderen übernimmt sie die Aufgabe des Routings[6] und bestimmt daher, auf welchem Weg die Daten von Hausnummer A zu Hausnummer B gelangen. Im Internet wird diese Aufgabe heutzutage vom IP-Protokoll erledigt, dessen Bestandteil das ICMP (Internet Control Message Protocol) ist[7]. Das ICMP dient dabei jedoch lediglich diagnostischen Zwecken, weshalb es an dieser Stelle nicht näher erläutert werden soll[8].

Über der Internetschicht befindet sich die *Transportschicht*, die sich meistens der Protokolle TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) bedient. Da das IP keinen Mechanismus zur Gewähr von Datensicherheit oder Datenflusssteuerung besitzt[9], kann nicht sichergestellt werden,

[3] Unter dieser Schicht befindet sich die Hardware. Da die Hardware aber streng genommen keine Protokollschicht darstellt, sondern lediglich die Voraussetzung für die Kommunikation schafft, wird diese in der Literatur zu TCP/IP häufig vernachlässigt.
[4] Local Area Network.
[5] Zum IP-Protokoll siehe ausführlich: RFC 791 (Internet Protocol), zur IP-Adresse siehe unter: Abschnitt B.I.2. auf Seite 8.
[6] Siehe ebenda unter Abschnitt B.I.2. auf Seite 8.
[7] RFC 1122 (Requirements for Internet Hosts - Communication Layers).
[8] Das ICMP ist in RFC 792 (Internet Control Message Protocol) definiert.
[9] *Lienemann*, TCP/IP-Grundlagen: Protokolle und Routing, 73ff.

dass Überlastungssituationen vermieden werden oder dass die Daten fehlerfrei und in der richtigen Reihenfolge vom Ausgangs- um Zielrechner gelangen. Dies ist vielmehr die Aufgabe der nächst höheren Schicht, also der Transportschicht. TCP stellt dabei ein zuverlässiges, verbindungsorientiertes Protokoll[10], UDP ein unzuverlässiges, verbindungsloses Protokoll dar[11]. Nun könnten selbstverständlich Zweifel darüber aufkommen, warum es Anwendungen geben sollte, die auf einem unzuverlässigen Protokoll basieren. Die Antwort liegt darin, dass UDP sich nur der Mindestmechanismen eines Protokolls bedient und daher wesentlich schneller ist als TCP. Handelt es sich um eine Kommunikationsart, bei der es nicht wichtig ist, dass 100% der Daten auf der Gegenseite ankommen, es aber zu einem hohen Anfall an Daten kommt, die möglichst rasch transportiert werden sollen, wie z.B. bei Bild- oder Voicekommunikation, ist UDP der Vorzug zu geben. Ein weiteres Protokoll, das sich auf der Ebene der Transportschicht befindet und an dieser Stelle erwähnt werden soll, weil es eine sichere Verbindung ermöglicht, ist SSL (Secure Sockets Layer)[12].

Oberste Schicht des TCP/IP-Referenzmodells und gleichzeitig auch diejenige Schicht, auf deren Ebene sich ein Großteil der Diskussion um die Erhebung von personenbezogenen Daten[13] abspielt, ist die *Anwendungsschicht*.

Wie der Name bereits suggeriert, findet in der Anwendungsschicht die Zusammenarbeit zwischen den Anwendungsprogrammen und dem Netzwerk statt. So lässt sich jedes Anwendungsprotokoll auch einem bestimmten Dienste- bzw. Programmtypus zuordnen. Die Protokolle SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol Version 3) und IMAP (Internet Message Access Protocol) werden beispielsweise von Mailclients wie Thun-

[10] RFC 793 (Transmission Control Protocol).
[11] RFC 768 (User Datagram Protocol).
[12] SSL wird in Verbindung mit dem sich auf der Anwendungsschicht befindlichen HTTP beispielsweise von Web-Stores benutzt, wenn sensible Daten wie die Kreditkartennummern übertragen werden.
[13] Zur Definition des Begriffs des Personenbezug siehe noch unter Abschnitt D.I.3. auf Seite 78.

derbird, Eudora, Pegasus oder Outlook benutzt, Internet Browser bedienen sich des HTTP (Hypertext Transfer Protocol), das Übermitteln von Dateien findet wiederum u.a. durch das FTP (File Transfer Protocol) statt. Weitere Protokolle der Anwendungsschicht sind Telnet, SSH (Secure Shell), DNS (Domain Name System) und PGP (Pretty Good Privacy) (Abbildung 2.1).

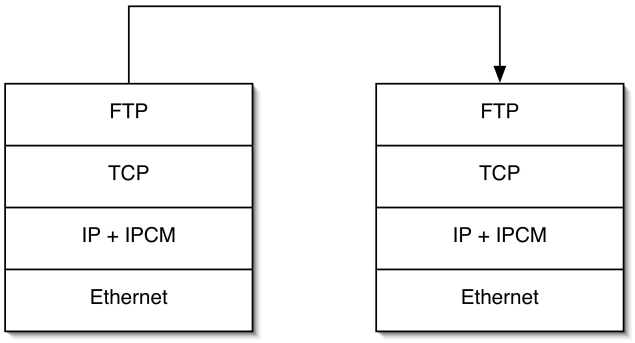


Abbildung 2.1: Beispiel einer TCP/IP-Kommunikation zwischen zwei Computern

## 2. Funktionsweise von IP-Adressen

Bei der Untersuchung der technischen Funktionsweise des Internets ist es unmöglich, nicht früher oder später dem Namen Jon Postel[14] zu begegnen. Jon Postel hat bereits in seiner Jugend mit der Entwicklung des TCP/IP-Protokolls begonnen, mehr als 204 RFCs verfasst und schließlich, zunächst als alleiniges Mitglied, IANA, die Internet Assigned Numbers Authority, gegründet. IANA, die heute eine Unterabteilung von ICANN (Internet Corporation for Assigned Names and Numbers) darstellt, unterliegt die Vergabe von Top Level Domains (TLDs) und IP-Adressen. Zur Erfüllung der Aufgabe der Vergabe der IP-Adressen verteilt die IANA große Kontingente an momentan vier RIRs (Regional Internet Registries)[15], welche diese wiederum an Internet-Provider

[14] Eine Biographie von Jon Postel findet sich unter dem Link http://www.postel.org/postel.html. Die Seite wurde anläßlich seines Todes ins Leben gerufen und wird durch die University Of Southern California betreut.

[15] Für Europa ist der zuständige RIR das RIPE (Réseaux IP Européens), http://ripe.net/.

vergeben, von denen aus sie dann letztendlich zu den Firmen oder Endverbrauchern gelangen.[16].

Was wird aber genau unter einer IP-Adresse verstanden? Am gebräuchlichsten ist heutzutage noch das der Adressierung zugrunde liegende IP-Protokoll in der Version 4 (IPv4). Es benutzt 32-bit Adressen und ist demzufolge auf 4.294.967.296 (also $2^{32}$) limitiert. In der „dotted decimal notation“ werden jeweils vier Bytes als vier durch Punkte getrennte Dezimalzahlen geschrieben, z.B. 66.102.9.104[17]. Jeder Rechner, der sich in einem TCP/IP-Netzwerk befindet, erhält eine IP-Adresse, die ihn eindeutig identifizierbar macht. Sendet A beispielsweise eine Suchanfrage an Google, muss Google bekannt sein, auf welchem Rechner die Seite mit den Ergebnissen angezeigt werden soll. Es findet in diesem Falle eine Kommunikation zwischen As Rechner mit der IP-Adresse 193.174.132.5 und dem vom Google mit der IP-Adresse 66.102.9.104 statt. Natürlich findet diese nicht auf direktem Wege statt, sondern über viele einzelne Computer, die das Datenpaket immer weiterleiten. Auch sie benötigen die Information, dass das Paket von 193.174.132.5 kommt und bei 66.102.9.104 landen soll. Die ordnungsgemäße Weiterleitung der Pakete vom Absenderrechner zum Empfangsrechner über mehrere Zwischenstationen wird *„Routing“* genannt. Da von dieser beschränkten Anzahl an Adressen viele für lokale Netzwerke oder andere spezielle Zwecke reserviert sind, war es bereits sehr früh offensichtlich, dass über kurz oder lang eine Knappheit an IP-Adressen herrschen wird[18]. Es sind daher verschiedene Lösungsmöglichkeiten entstanden, die entweder mit dem Ansatz zusammenhängen, dass nicht jeder Rechner, der sich mit dem Internet verbindet, die ganze Zeit online ist und deswegen nicht rund um die Uhr eine IP-Adresse benötigt oder dass es nicht notwendig ist, dass die

[16] Diese verwalten hingegen nicht die TLDs, welche an andere Organisationen delegiert wurden: Für die ccTLD „.de“ ist das beispielsweise DENIC (http://denic.de/).

[17] 66.102.9.104 entspricht derzeit der IP-Adresse der beliebten Suchengine http://www.google.com und würde in der binären Schreibweise folgendermaßen aussehen: 010000010 01100110 00001001 01101000.

[18] Für eine genaue Auflistung s. RFC 3330 (Special-Use IPv4 Adresses).

Kommunikation von einem abgrenzbaren Netzwerkbereich - wie dem CIP-Pool einer Universität oder einem Firmennetzwerk - ins Internet direkt von jedem Rechner ausgeführt können werden muss, sondern auch von einem zwischengeschalteten Server vonstatten gehen kann. Das Ergebnis des ersten Ansatzes waren die dynamischen IP-Adressen, das Ergebnis des zweiten hingegen die Network Adress Translation (NAT).

### a) dynamische IP-Adressen

Dynamische IP-Adressen werden meist von Internetprovidern vergeben. Wählt sich der Nutzer mit einem Modem beim Provider ein, prüft dieser, welche IP-Adresse seines Kontingents gerade nicht belegt ist und weist sie dem anfragenden Computer zu. Wird nach dem Surfen die Verbindung unterbrochen indem der Nutzer die Verbindung unterbricht, ist die IP-Adresse wieder frei und kann dem nächsten sich einwählenden Nutzer zugewiesen werden. Auf diese Art und Weise ändert sich die IP-Adresse, die der Einzelne erhält, jedes Mal wenn er sich einwählt. Den Gegensatz einer dynamischen IP-Adresse stellt die statische IP-Adresse dar. Statische IP-Adressen werden von Internetprovidern an Nutzer meist nur dann vergeben, wenn diese eine Standleitung, also eine permanente Verbindung ins Internet, haben.

Innerhalb eines Firmen- oder Heimnetzwerkes werden dynamische IP-Adressen mittels DHCP[19] vergeben. Vereinfacht gesagt fragt hier ein Client, der sich mit dem Netzwerk verbinden will beim DHCP-Server nach, ob ihm eine IP-Adresse zugewiesen werden kann. Dieser sieht nach, welche IP-Adressen ge-

[19] S. RFCs 2131 und 3315 (Dynamic Host Configuration Protocol, Version 4 and 6).

rade frei sind und bindet daraufhin eine dieser Adressen an die MAC-Adresse[20] des Clients[21].

### b) Network Adress Translation (NAT)

Der Network Adress Translation bedienen sich hingegen eher Firmen- oder Heimnetzwerke. Dabei übersetzt (englisch „to translate“) die NAT so genannte private in öffentliche IP-Adressen.

Nachdem mit dem Wachstum des Internets auch die Kommunikation mittels TCP/IP immer gängiger wurde und somit auch eine zunehmende Anzahl an Firmen sich untereinander nicht verbundener TCP/IP-Netzwerke bedienten, musste ein Weg gefunden werden, der nicht schon zur Erschöpfung von öffentlichen IP-Adressen durch die Vergabe an diese Firmen führte.

Bei der Vergabe der IP-Adressen hat sich die IANA daher bestimmte Bereiche vorbehalten, die sie nicht vergibt, weil sie ausschließlich für private Netzwerke gedacht sind. Folge daraus ist, dass diese Adressen dann auch nicht als öffentlich zugänglich im Internet zu finden sind.

In Firmen- oder Heimnetzwerken wiederum können sie frei vergeben werden, wobei die Gefahr einer Fehladressierung von Datenpaketen durch die Mehrfachvergabe privater IP-Adressen innerhalb mehrerer isolierter Netzwerke gerade nicht besteht (Abbildung 2.2 auf der nächsten Seite).

Die Kommunikation findet immer nur innerhalb der Netzwerke statt und gelangt nicht nach außen. Beispiel eines ausschließlich zu privaten Zwecken genutzten IP-Bereiches sind die IP-Adressen 192.168.0. - 255[22].

[20] Die Abkürzung MAC steht dabei für Medium Access Control. Die MAC-Adresse ist als Hardware-Adresse fest mit dem Netzwerkgerät verknüpft und ermöglicht somit eine eindeutige Zuordnung zu den sich jeweils im LAN befindenden Geräten, wie z.B. Computer, Router oder Netzwerkdrucker (für eine detaillierte Beschreibung s. *Meinel/Sack*, WWW, S. 262 f.).

[21] Zur Möglichkeit, auch statische IP-Adressen in einem Netzwerk mit DHCP zu vergeben, siehe RFC 2131.

[22] Siehe dazu ausführlich RFC 1918 (Address Allocation for Private Internets).

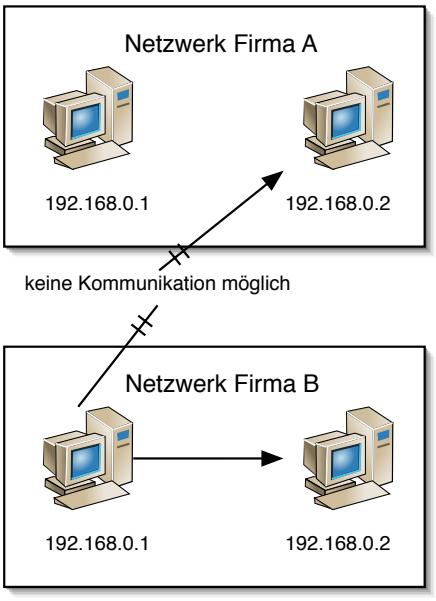


Abbildung 2.2: Keine Gefahr bei Mehrfachvergabe von privaten IP-Adressen in isolierten Netzwerken

Wird NAT zur Einsparung öffentlicher IP-Adressen genutzt, stellt sich der Aufbau des Netzwerkes meist in folgender Art und Weise dar: Sämtliche Rechner im lokalen Netzwerk erhalten eine private IP-Adresse und sind mit einem Router verbunden. Der Router, der mit zwei Netzwerkkarten ausgestattet ist (eine für die Kommunikation mit dem Internet und eine für die Kommunikation im lokalen Netzwerk), hat die Aufgabe zu kontrollieren, ob die Anfragen, die von den jeweiligen Rechnern kommen, für das lokale Netzwerk oder für das Internet bestimmt sind. Sind sie für das lokale Netzwerk bestimmt, leitet er sie an die private IP-Adresse des Zielrechners weiter, die Kommunikation findet dann ausschließlich zwischen privaten IP-Adressen statt.

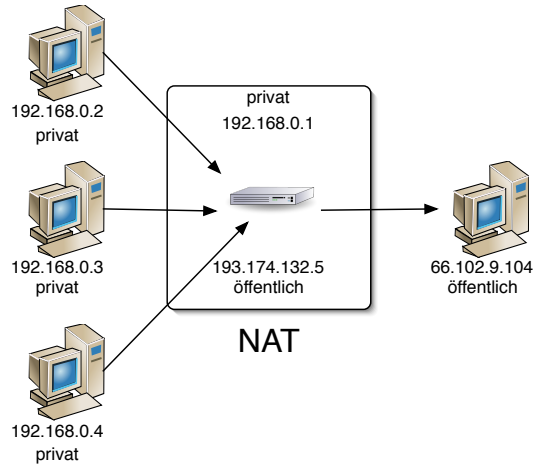


Abbildung 2.3: Umwandlung von privaten in öffentliche IP-Adressen mittels NAT

Sind sie hingegen für das Internet bestimmt, kommt NAT ins Spiel. Da der Router mit zwei Netzwerkkarten ausgestattet ist, hat er selbst auch zwei IP-Adressen: eine für das private und eine für das öffentliche Netzwerk. Bei der NAT wandelt der Router die private IP-Adresse in seine eigene öffentliche Adresse um und merkt sich gleichzeitig, welcher Rechner die Anfrage geschickt hat. Kommt die Antwort auf diese Anfrage von einem Rechner im Internet an den Router zurück, leitet er sie dann an den ursprünglichen Rechner im lokalen Netzwerk mittels privater IP-Adresse zurück (Abbildung 2.3). Auf diese Art kann ein gesamtes Firmennetzwerk mit nur einer öffentlichen IP-Adresse auskommen[23].

[23] Ein weiterer Vorteil von NAT ist, dass die einzelnen Clients nicht direkt, sondern über den Umweg des Routers in Erscheinung treten. Da sie keine öffentliche IP-Adresse haben,

## II. Non-Reaktive Maßnahmen zur Datenerhebung

Wie im rechtsdogmatischen Teil dieser Arbeit noch näher zu erläutern sein wird, spiegelt das Datenschutzrecht den verfassungsrechtlich verankerten Recht des Einzelnen auf informationelle Selbstbestimmung wieder[24]. Die informationelle Selbstbestimmung gewährleistet jedem Individuum die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen[25]. Im Idealfall werden daher die Daten beim Individuum selbst erhoben, da auf diese Weise, bei ausreichender Unterrichtung und Aufklärung, noch am ehesten sichergestellt wird, dass die Erhebung aufgrund einer Bestimmung stattfindet, die er bewusst getroffen hat. Werden die Daten jedoch nicht bei ihm erhoben, bedeutet Selbstbestimmung, ungewollte Erhebung, Verarbeitung und Nutzung personenbezogener Daten verhindern zu können[26]. Der sog. „Selbstdatenschutz" ist somit Kern des Datenschutzrechts und hängt wesentlich davon ab, ob die Datenerhebung in Kenntnis des Betroffenen geschieht oder diese vor ihm geheim gehalten wird beziehungsweise unfreiwillig vonstatten geht. Genauer gesagt wird schon dann von einer mangelnden Selbstschutzmöglichkeit auszugehen sein, wenn das Kriterium der Heimlichkeit und das der Unfreiwilligkeit kumulativ auftreten[27]. Da die Gefahr der Heimlichkeit und Unfreiwilligkeit größtenteils von non-reaktiven Maßnahmen der Datenerhebung ausgeht, werden sie in diesem Teil der Arbeit vorab und getrennt von den reaktiven Maßnahmen behandelt.

---

können sie auch nicht direkt von Computern im Internet „gesehen" werden, was zum einen im Sinne des Satzes „security by obscurity" Schutz vor verschiedenen Angriffen bietet, zum anderen für die Frage, ob in diesen Fällen die IP-Adresse ein personenbezogenes Datum darstellt, relevant ist (siehe dazu unter Abschnitt D.IV.1. auf Seite 81).

[24] *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 1.

[25] BVerfGE 65, 1.

[26] Grundlegend *Roßnagel* in: *Roßnagel*, Handbuch Datenschutzrecht, 3.4 Rdnr. 1; siehe aber zu den Grenzen des Rechts auf informationelle Selbstbestimmung umfassend *Bull*, NJW 2006, 1617–1624.

[27] So *Buxel*, Die sieben Kernprobleme des Online-Profiling aus Nutzerperspektive, 579–583.

## 1. Webserver

Ein Großteil der Nutzer benutzt das Internet fast ausschließlich zum Surfen. Demzufolge verwundert es nicht, dass die Mehrzahl der technischen Möglichkeiten der Datenerhebung im Zusammenhang mit Webservern steht. Im Folgenden werden daher die technischen Zusammenhänge, die hinsichtlich des Datenschutzes beim Internetsurfen relevant sind, dargestellt.

### a) Das Referer-Field, Auswertung des Clickstreams

Verwendet der Nutzer zum Surfen im Internet einen Browser (z.B. Firefox, Safari, Netscape Navigator, Opera, Internet Explorer), kommuniziert dessen Client auf der Anwendungsschicht[28] über HTTP (Hypertext Transfer Protocol)[29] mit dem Webserver.

Das HTTP trägt dabei ausschließlich dafür Sorge, dass vom heimischen Computer aus eine Anfrage an den Server, auf dem sich die gewünschte Internetseite befindet, geschickt wird, mit der Bitte, diese Seite auf den heimischen Computer zu laden. Der Name des Protokolls ergibt sich aus dem Umstand, dass die Internetseiten als Hypertext[30] häufig in der Sprache HTML (*Hypertext* Markup Language) übertragen (engl.: to *transfer*) werden. Über die bloße Anfrage, die Seite zu übertragen, werden dem Server jedoch noch weitere Informationen übermittelt, die von datenrechtlicher Relevanz sein können. Besonders bedeutsam ist hierbei das sog. Referer-Field. Aus einem lang zurückliegenden orthographischen Versehen immer noch mit einem R geschrieben[31], ist das Referer-Field eines der Request-Header Fields und somit eines der Felder, die einem Web-Server, wenn er eine HTTP-Anfrage erhält, Zusatzinformationen

[28] Siehe zur Anwendungsschicht unter Abschnitt B.I.1. auf Seite 6.
[29] RFC 2616 (Hypertext Transfer Protocol - HTTP/1.1), S. 10ff.
[30] Definition Hypertext: Ein Hyperdokument ist eine Ansammlung von Informationseinheiten, so genannten Knoten, die wie ein Netz miteinander verknüpft sind. (*Rosenbaum, Oliver*, Online Lexikon).
[31] RFC 2616, 14.36.

über den Absender liefert. Der Referrer (engl.: to refer: sich beziehen) enthält im Falle, dass ein Benutzer durch einen Link auf die neue Seite gelangt ist, die Adresse der Seite, die der Benutzer zuvor besucht hat. Diese Information wird wiederum häufig in den Logfiles der Server gespeichert. Die Vorteile liegen dabei klar auf der Hand: Zum einen ist es auf diese Weise möglich, private Homepageanbieter in ein Partnerprogramm zu integrieren. Der Homepageanbieter setzt dafür einen Link von seiner Seite auf einen Webshop; gelangt nun ein Homepagebesucher über diesen Link auf den Webshop und kauft dort daraufhin ein, wird dem Homepageanbieter ein bestimmter Betrag überwiesen. Eine weitere Möglichkeit, die häufig genutzt wird, ist anhand des Referrers zu kontrollieren, welche Begriffe einer Suchmaschinenanfrage zum eigenen Shop geführt haben: Der Referrer der meisten Suchmaschinen beinhaltet nicht nur, dass der Kunde beispielsweise über Google auf den Shop gelangt ist, sondern auch, dass er den Link über die Suche von „billige“, „Bücher“, „online“, „bestellen“ gefunden hat. Schon anhand dieser beiden Beispiele wird offensichtlich, dass der Referrer kommerziellen Anbietern eine ideale Möglichkeit bietet, ihre Marketingstrategien im Internet gezielter einzusetzen. Für den Bereich des Datenschutzes ergibt sich aber ein weiterer Punkt: Ist ein Internetnutzer bereits Kunde des jeweiligen Webshops oder wird er nach Anklicken des Links, der im Referrer angegeben ist, Neukunde, lässt sich durch den Referrer herausfinden und in der Kundendatenbank abspeichern, auf welche Art der Werbung dieser Kunde am ehesten anspricht. Diese Information wiederum lässt sich im eigenen Webshop ideal dazu nutzen, um den Kunden durch ein derartig erstelltes Profil gezielt zu bewerben. Da zur Erstellung dieses Profils der „Weg“ gespeichert wird, entlang dessen sich der Kunde mit der Maus von Link zu Link klickt, hat sich für die daraus entstandenen Daten der Begriff „Clickstream“ eingebürgert[32].

[32] Zur juristischen Einordnung von Nutzungsprofilen, s. Abschnitt D.VI.1.a) auf Seite 88.

### b) Logfile Formate

Zusätzlich zu den Daten des Referrers können in den Logfiles der Web-Server auch noch weitere Daten gespeichert werden.

Der Administrator eines Web-Servers hat hier die Möglichkeit, jeglichen Inhalt der Anfragen, die an ihn geschickt werden, im Logfile aufzunehmen. Es wird aber zumindest davon auszugehen sein, dass er die im Common Logfile Format (CLF) enthaltenen Daten bei einem HTTP-Request speichert.

Das CLF-Format sieht wie folgt aus:
*remotehost rfc931 authuser [date] "request" status bytes*
„Remotehost“ ist dabei der Hostname, von dem die Anfrage ausgeht, im Normalfall der Hostname des jeweiligen Access-Providers oder dessen IP-Adresse. „rfc931“ ist der Remote-Logname des Users. Wenn sich dieser mit Kennung und Passwort autorisiert hat, wird die Kennung in „authuser“ abgelegt, mit der Möglichkeit, auch das Datum der Autorisierung mitzuloggen („date“). „Request“ wiederum enthält die eigentliche Anfrage, „status“ enthält die Angabe darüber, ob das Objekt, das angefordert wurde, erfolgreich übermittelt wurde (genau genommen den sog. HTTP-Status-Code[33]) und „bytes“ die Anzahl der übertragenen Bytes[34].

Bei CLF handelt es sich aber lediglich um einen gängigen Minimalstandard[35]. Das W3C-Konsortium hat daher schon im Jahre 1996 ein erweitertes File Format vorgeschlagen (ELFF)[36], das neben den Parametern des CLF beispielsweise auch oben genannten Referrer enthält, sowie Daten über den verwendeten Browser.

[33] RFC 2616, 10.
[34] *Engler/Kurzidim*, Geheimakte Logfile, 124–147.
[35] *Grimm* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, 70.
[36] W3C Working Draft WD-logfile-960323, `http://www.w3.org/pub/WWW/TR/WD-logfile.html`.

Daneben gibt es noch viele andere Formate wie z. B. das NCSA Common Format oder das Format des Microsoft IIS (Internet Information Server), die aber im Wesentlichen die gleichen Informationen speichern[37].

### c) HTTP-Cookies

In Rahmen der Diskussion um die Möglichkeiten der Datenerhebung im Internet ist das weitaus am stärksten vertretene Thema in der Literatur das der Cookies[38]. Schon vor diesem Hintergrund ist es unverzichtbar, im Rahmen dieser Arbeit die genaue technische Funktionsweise von Cookies detailliert darzulegen, um eine fundierte rechtliche Analyse zu ermöglichen.

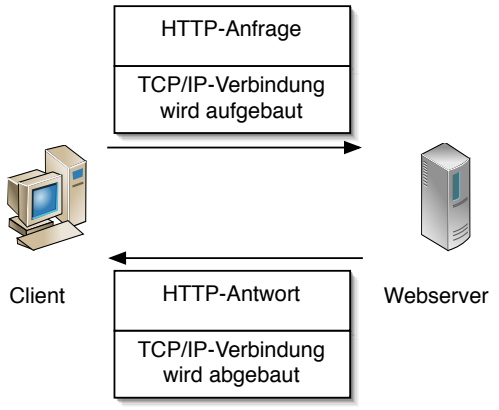


Abbildung 2.4: zustandslose Kommunikation des HTTP

Die Notwendigkeit für Cookies ergibt sich aus der Tatsache, dass das HTTP ein zustandsloses Protokoll ist. Wie bereits dargelegt[39], führt eine HTTP-Anfrage von Seiten eines Clients hauptsächlich dazu, dass die jeweilige Webseite von dem anfragenden Browser angezeigt wird. Ist die Seite erst lokal geladen, endet die Verbindung zum Server bereits. Klickt der Nutzer anschließend innerhalb der Seite auf einen Link, der zu einer weiteren Seite führt, die sich auf dem

[37] Dokumentation zu beiden Formaten finden sich in der IIS Documentation des TechNets von Microsoft, welches unter http://technet.microsoft.com/default.aspx zu erreichen ist.

[38] Als erster Überblick soll hier *Eichler*, Cookies - verbotene Früchte?, 76–81 genannt werden; weiterhin *Meyer*, Cookies & Co. - Datenschutz und Wettbewerbsrecht, 1028–1035; *Schaar*, Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, 275–277 und *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG Rdnr. 166ff.; technisch unsauber hingegen *Ihde*, Cookies - Datenschutz als Rahmenbedingung der Internetökonomie, 413–423.

[39] Vgl. Abschnitt B.II.1.a) auf Seite 15.

selben Server befindet, erfährt der Server anhand des HTTP allein nicht, dass es sich hierbei nach wie vor um denselben Nutzer handelt, der aus bestimmten Gründen länger auf dem Server verweilt. Es wird vielmehr jedes Mal eine neue und völlig isolierte Verbindung aufgebaut (Abbildung 2.4 auf der vorherigen Seite).

Der Vorteil einer zustandslosen Kommunikation ist, dass der Server keine Daten über bestehende Verbindungen zu speichern braucht und jede Anfrage in einem Schritt bearbeitet werden kann.

Der Nachteil besteht jedoch dann, wenn ein Nutzer gerade über mehrere Schritte respektive Webseiten Informationen an den Server übermitteln will, wie es beispielsweise bei einem virtuellen Warenkorb in einem Webshop der Fall ist.

Diesem Nachteil wird durch die Verwendung von Cookies begegnet. Ursprünglicher Entwickler von Cookies war die Firma Netscape, inzwischen wurden „Cookies“ mithin als Internetstandard festgesetzt[40]. Technisch gesehen funktionieren sie folgendermaßen: Wie bei jeder HTTP-Verbindung schickt der Client an den Server eine Anfrage. Der Server schickt jedoch nicht nur die Informationen der Webseite zurück, sondern im Header der HTTP-Antwort auch ein Set-Cookie-Feld. Daraufhin wird die Verbindung, welche ja zustandslos ist, wie gewohnt abgebaut. Darüber hinaus befindet sich nun aber ein Cookie auf dem Client, welches dort auch gespeichert wurde.

Bei der nächsten Anfrage, die im Rahmen einer neuen Verbindung stattfindet, sendet der Client neben der bloßen Anfrage auch das Cookie an den Server. Dieser verarbeitet es vor einer erneuten Antwort, z.B. mittels der CGI-Schnittstelle[41], weiter (Abbildung 2.5 auf der nächsten Seite[42]).

Auf diese Art und Weise ist es beispielsweise möglich, dass Erika Mustermann in einem Webshop ein Buch bestellt, indem sie es zunächst in den Wa-

[40] RFC 2965 (HTTP State Management Mechanism).
[41] *Meinel/Sack*, WWW, S. 780ff.
[42] *Meinel/Sack*, WWW, S. 780ff.

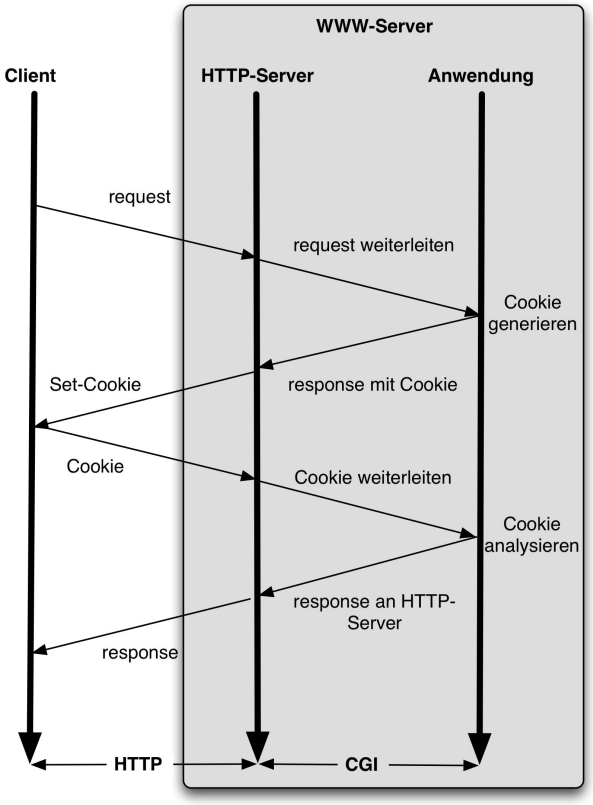


Abbildung 2.5: HTTP-Cookie-Mechanismus, Quelle: Meinel/Sack, WWW, S. 780

renkorb legt. Klickt sie den Warenkorb nun an, öffnet sich eine neue Seite, die dank des Cookies das Buch enthält. Sie kann nunmehr mit dem Buch zur virtuellen Kasse schreiten, bei der im Cookie die Zahlungsweise und der Versandweg gespeichert werden.

Da es wenig Sinn macht, dass die im Rahmen der Transaktion entstandenen Cookies über deren Zeitraum hinaus auf dem Rechner verweilen, kann in einem der Cookie-Parameter festgelegt werden, wie lange es auf der Festplatte des

Rechners gespeichert werden soll. Die einzelnen Parameter[43] von Cookies sehen folgendermaßen aus:

| Parameter | Bedeutung |
|---|---|
| Name | der Name des Cookies |
| Value | der Wert des Cookies |
| Comment | der Verwendungszweck des Cookies (optional) |
| Discard | gibt an, dass das Cookie nach Schließen des Browsers gelöscht werden soll |
| Domain | die Domain für die das Cookie gültig ist |
| Max-age | die „Lebensspanne“ eines Cookies; ist das *max-age* verstrichen, soll der Client das Cookie löschen (optional) |
| Path | der Serverpfad (+ dessen Unterverzeichnisse) für den das Cookie angelegt wird (optional) |
| Port | gibt die Ports an, an die das Cookie zurückgesendet werden darf |
| Secure | Ist dieser Parameter gesetzt, wird der Client dazu angewiesen, eine gesicherte Verbindung aufzubauen (optional) |
| Version | die Version des Cookie-Protokolls |

Wie aus dieser Aufstellung ersichtlich wird, ist (bis auf die Version) nur das Name-Value-Paar zwingend. Im Prinzip können diese beiden Parameter u.a. jeden beliebigen Wert aus der HTTP-Kommunikation wie auch diejenigen Werte enthalten, die der Nutzer während der Transaktion an den Browser übergibt.

[43] RFC 2965.

### aa) Beispiel der Funktionsweise von Cookies

Nachfolgend soll folgendes Beispiel eines normalen Online-Kaufs dazu dienen, die Funktionsweise noch zu veranschaulichen[44]:

1. Erika Mustermann meldet sich bei einem Shop als Benutzerin „emustermann“ an:
   Client -> Server
   *POST /login HTTP/1.1*
   *[Loginformulardaten]*[45]
2. Der Shop erkennt sie als Kundin und gibt ihre Identität zurück indem er ein Cookie mit Name „Kunde“ und Value „emustermann“ erzeugt:
   Server-> Client
   *HTTP/1.1 200 OK*
   *Set-Cookie2: Kunde=“emustermann“; Version=“1“*
3. Erika Mustermann bestellt das Buch „Datenschutz im Internet“ und legt es in den Warenkorb:
   Client->Server
   *POST /warenwahl HTTP/1.1*
   *Cookie: $Version=“1“; Kunde=“emustermann“*
   *[Warenkorbformulardaten]*
4. Im Warenkorb befindet sich nun das Buch, das ebenfalls im Cookie gespeichert wird:
   Server->Client
   *HTTP/1.1 200 OK*
   *Set-Cookie2: Ware=“DS_IM_INET“; Version=“1“*
5. Erika Mustermann wählt die Warensendung per UPS:
   Client->Server

[44] Es handelt sich hierbei um eine Vereinfachung des Beispiels, das im RFC 2965, S. 15 ff. zu finden ist.
[45] Zur Funktionsweise von Formularen, siehe unter Abschnitt B.III.1. auf Seite 40.

*POST /versandart HTTP/1.1*
*Cookie: $Version="1"; Kunde="emustermann"; Ware="DS_IM_INET"*
*[Versandartformulardaten]*

6. Der Shop legt im Cookie die Versandart ab:
   Server->Client
   *HTTP/1.1 200 OK*
   *Set-Cookie2: Versandart="UPS"; Version="1"*
7. Erika Mustermann sieht sich ihre Bestellung noch einmal an und klickt auf *Bestellung senden*:
   Client->Server
   *POST /bestellungok HTTP/1.1*
   Cookie: $Version="1"; Kunde="emustermann"; Ware="DS_IM_INET"; Versandart="UPS"
   [Bestellformulardaten]
8. Die Transaktion ist abgeschlossen, Erika Mustermann hat ein Buch im Internet bestellt.
   Server->Client
   *HTTP/1.1 200 OK*

Dieses Beispiel veranschaulicht, warum sich ein Großteil der Diskussionen im Datenschutz um das Name-Value-Paar dreht[46]. Es verdeutlicht aber darüber hinaus, dass Cookies auf sinnvolle Art genutzt aus dem heutigen E-Commerce kaum wegzudenken sind. Wie bei allen anderen Möglichkeiten, Daten im Internet zu erheben, gilt es daher vor allem im Bereich der Cookies zu erkennen, dass diese an und für sich nicht das Datenschutzrisiko darstellen. Dieses ergibt sich vielmehr erst aus dem Zusammenspiel zwischen User auf der einen und dem Betreiber der Server auf der anderen Seite: So könnte bei Punkt 8 des Beispieles bei einer datenschutzgerechten Verarbeitung das Cookie an und

[46] So zum Beispiel bei *Ihde*, Cookies - Datenschutz als Rahmenbedingung der Internetökonomie, S. 414 und *Meyer*, Cookies & Co. - Datenschutz und Wettbewerbsrecht, S. 1028.

für sich gelöscht werden. Es könnte aber ebenso dazu missbraucht werden, ein Nutzungsprofil von Frau Mustermann anzulegen, um ihr Konsumverhalten zu protokollieren.

Ein weiterer Punkt, der im Zusammenhang mit Cookies und Datenschutz Probleme aufwirft, ist das Anlegen anbieterübergreifender Cookies mittels Ad-Server, das im folgenden dargestellt werden soll:

### bb) anbieterübergreifende Cookies

Anbieterübergreifende Cookies werden meist von Werbefirmen wie z.B. Doubleclick abgelegt[47]. Besucht der Nutzer das erste Mal die Seite eines Werbekundens von Doubleclick, wird mittels eines Cookies getestet, ob der Browser des Besuchers Cookies akzeptiert. Falls dem so ist, wird ein Cookie mit einer Unique-ID, also einer Nummer, die ausschließlich diesem Nutzer und dem Browser auf dem Computer zuzuordnen ist, abgelegt. Surft der Nutzer zukünftig erneut auf Seiten des selben oder anderer Werbekunden, wird er durch das Cookie vom Ad-Server von Doubleclick erkannt. Doubleclick nutzt das Cookie daraufhin, um zum einen dafür zu sorgen, dass der Nutzer im Rahmen der Werbebanner, die sich auf den Seiten der Werbekunden befinden, immer neue Anzeigen zu Gesicht bekommt. Zum anderen ermöglicht das Cookie, dem Nutzer im Laufe der Zeit anhand der besuchten Seiten speziell auf ihn zugeschnittene Werbung zu senden.

Surft demzufolge Erika Mustermann auf der Seite des Werbekundens X und war sie zuvor auf mehreren Seiten für Schönheitsprodukte, deren Betreiber ebenfalls Werbekunden sind, wird sie im Werbebanner höchstwahrscheinlich Angebote für Kosmetika finden. Surft hingegen ihr Ehemann, Erich Mustermann, auf der gleichen Seite des Werbekundens X und benutzt das Ehepaar nicht dieselbe Kennung auf dem heimatlichen Computer, wird er wahrscheinlich Angebote für das neueste Automodell im Werbebanner finden.

[47] `Http://www.doubleclick.net`.

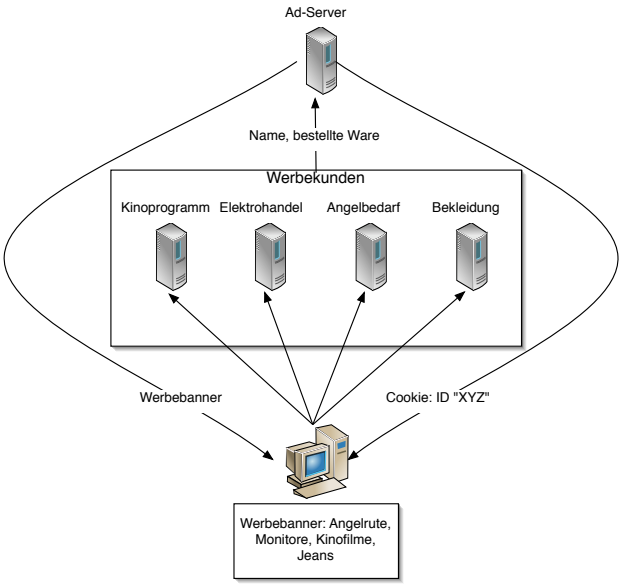


Abbildung 2.6: Cross-Reference-Verfahren und anbieterübergreifendes Cookie

Das technische Prinzip, das hinter anbieterübergreifenden Cookies steckt, entsteht einerseits dadurch, dass alle Werbekunden sich eines gemeinsamen Cookies bedienen und andererseits die Werbebanner allesamt über einen zentralen (Ad-)Server geladen werden.

Das Cookie wird dabei beim jeweiligen Request des Werbebanners generiert, da nur auf diese Weise die Möglichkeit besteht, dass es unabhängig vom jeweiligen Werbekunden die Domain der Werbefirma besitzt.[48]

Datenschutzrechtliche Probleme im Zusammenhang mit anbieterübergreifenden Cookies entstehen vor allem dann, wenn der Nutzer bei einem der Werbekunden etwas bestellt, der Werbekunde der Werbefirma die Daten des Nutzers daraufhin weitergibt und diese somit eine Verbindung zwischen dem

[48] Das liegt daran, dass der Server, der das Cookie generiert, immer ein Mitglied der Domain sein muss, die er im Cookie setzen will, www.werbekunde.com kann demnach kein Cookie für die Domain www.werbefirma.com setzen.

Nutzer und der Unique ID herstellen kann (sog. Cross-Reference-Verfahren[49]) (Abbildung 2.6 auf der vorherigen Seite).

Eng verwandt mit der technischen Funktionsweise von anbieterübergreifenden Cookies und üblicherweise ebenfalls im Zusammenhang mit einem Ad-Server treten die im Folgenden geschilderten Web-Bugs (aus dem Englischen „bug“ = „Wanze“) auf.

### d) Web-Bugs

Web-Bugs machen sich die Tatsache zu nutze, dass Browser und HTML-fähige E-Mail-Clients im Normalfall Bilder einer Web-Seite automatisch laden.

Das Tag <img> ist im Dokumentenformat HTML für Graphikreferenzen zuständig[50]. Um also dem Browser mitzuteilen, er soll beim Anzeigen einer Webseite an genau dieser Stelle die Graphik positionieren, die unter foo.jpg auf dem Webserver gespeichert ist, wird in den Quellcode der Webseite: <img src="verzeichnis/foo.jpg" alt="Foobild">[51] eingefügt. Der Browser sucht daraufhin beim Aufruf der Seite auf dem Server die Datei foo.jpg, überträgt sie auf den heimischen Computer und zeigt sie dort an.

Anstatt einer „normalen“ Graphikdatei könnte der <img>-Tag jedoch den Browser auch dazu veranlassen eine Datei zu laden, die nur 1x1 Pixel groß und somit für den Nutzer gar nicht sichtbar ist[52]: Dies ist die Vorgehensweise von Web-Bugs.

Bei der Verwendung von Web-Bugs baut der Browser also bei Abruf einer Webseite zeitgleich eine Verbindung zu dem Server auf, bei dem die Graphikdatei gespeichert ist. Der Nutzer bemerkt diesen Vorgang nicht. Im Vergleich

[49] Siehe dazu auch: *Hillenbrand-Beck/Greß*, Datengewinnung im Internet, 389–394.

[50] Die genaue Funktionsweise des <img>-Tags findet sich in der Online-HTML-Referenz `http://de.selhtml.org`.

[51] Wobei das Attribut „alt“ dazu dient, einen Alternativtext für den Fall, dass die Graphik nicht angezeigt wird, anzugeben und hier lediglich der Vollständigkeit halber aufgeführt ist.

[52] Üblicherweise übergibt das Attribut „alt“ in solchen Fällen einen leeren String.

zu Cookies bergen Web-Bugs darüber hinaus den großen Vorteil, dass sie so gut wie nie deaktiviert werden, weil der Nutzer im Alltag ein großes Interesse daran hat, dass ihm beim Internetsurfen die Graphiken der Webseiten automatisch angezeigt werden.

Web-Bugs werden zum einen von Werbefirmen, zum anderen aber auch von den Betreibern selbst verwendet. Neben der Firma Doubleclick, die bereits bei den anbieterübergreifenden Cookies Erwähnung fand, wurden Web-Bugs ebenso von Barnes and Nobles, eToys, Cooking.com, Microsoft und Infobeat verwendet[53].

Beim Aufbau der HTTP-Verbindung zum Abruf der Graphikdatei können dabei an den Server dieselben Informationen übermittelt werden wie bei jedem anderen HTTP-Request auch[54].

Interessant wird ein Web-Bug jedoch vor allem in Verbindung mit einem Cookie oder als Inhalt einer E-Mail: Da über HTTP auch der Inhalt des Cookies[55] abgerufen werden kann, stellt ein Web-Bug die ideale Ergänzung für die Fälle dar, in der dieser Inhalt Rückschlüsse auf die Person des Nutzers zulässt. Ein Web-Bug in einer E-Mail bringt überdies den Vorteil, dass abgerufen werden kann, ob und wann eine Werbe-E-Mail gelesen wurde. In einem Cookie kann ferner die E-Mail-Adresse des jeweiligen Nutzers abgelegt werden. Der Kombination aus den verschiedenen technischen Vorgehensweisen sind also keinerlei Grenzen gesetzt.

Die Verwendung von Web-Bugs für Dienste zur Überwachung von E-Mails wie „Did they read it?“[56] war daher bereits Kritikpunkt der Artikel 29-Arbeitsgruppe der EU-Datenschutzbeauftragten[57]. „Did they read it?“ ermöglicht es deren Nutzern, mittels Anhängen des Zusatzes *.didtheyreadit.com* an

[53] *Rötzer*, TP 1999.
[54] Siehe dazu oben unter Abschnitt B.II.1. auf Seite 15.
[55] Siehe dazu unter Abschnitt B.II.1.c) auf Seite 18.
[56] `www.didtheyreadit.com`.
[57] Siehe „Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services“ 00451/06/EN WP 118, S. 9.

die Empfänger-Adresse, die E-Mail durch das vorherige Senden an ihren Server mit einem Web-Bug zu versehen, bevor er sie an den eigentlichen Bestimmungsort weitervermittelt[58]. Wird die E-Mail geöffnet und ist das automatische Anzeigen von Bildern im Client nicht deaktiviert, erhält der Nutzer und ursprüngliche Absender von „Did they read it?“ eine Lesebenachrichtung, ebenso wie auf Wunsch Auskunft darüber, wie lang die E-Mail gelesen wurde, wie häufig sie geöffnet und an wen sie geforwardet wurde. Ferner werden dem Nutzer detaillierte Informationen wie die Empfänger-IP, das Betriebssystem, die Betriebssystem-Sprache, der verwendete Client, der Internet-Service-Provider und der Ort, an dem sich der Provider befindet, mitgeteilt.

### 2. Proxy-Cache-Server

Proxy-Cache-Server sind streng genommen kein Mittel zur Datenerhebung, sondern dienen heutzutage sogar häufig als Hilfmittel von Anonymisierungsdiensten[59]. Da sie sich aber durchaus auch dazu missbrauchen lassen, Daten versteckt zu erheben und Nutzerprofile zu erstellen, seien sie an dieser Stelle trotzdem erwähnt und ihre technische Funktionsweise erläutert.

Proxy-Server gab es schon zu Anfangszeiten des Internets, als Breitbandverbindungen selten waren und ein Großteil der Firmen und privaten Nutzer noch über Modems auf das Internet zugriff. Die Hauptfunktion der Proxy-Cache-Server war damals wie heute einen Zwischenspeicher zwischen verschiedenen Nutzern und dem WWW herzustellen:

Angenommen Nutzer A stellt über einen Proxy-Server die Verbindung zur Seite `http://www.foo.de` her. Der Proxy-Server würde in diesem Fall nachprüfen, ob diese Seite kürzlich bereits abgerufen wurde und sie sich somit bereits in seinem Speicher (Cache) befindet. Ist dies der Fall, wird dem Nutzer A einfach die gespeicherte Seite aus dem Cache übertragen und keine neue

[58] Der Zusatz an der Empfänger-Adresse wird dabei gleichzeitig wieder entfernt, damit eine Benutzung des Dienstes unbemerkt vonstatten geht.

[59] So zum Beispiel beim Anonymisierungsdienst JAP (`http://anon.inf.tu-dresden.de/`).

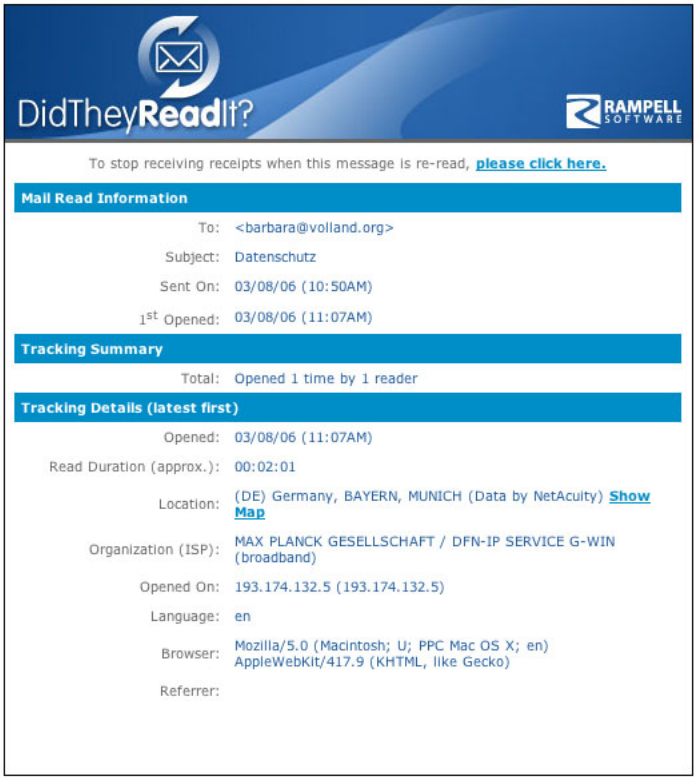


Abbildung 2.7: Durch „DidTheyReadyIt?“ übermittelte Informationen, Quelle: Screenshot eigener E-Mail

Verbindung zum Webserver mit der Adresse `http://www.foo.de` aufgebaut. Nur wenn dies nicht der Fall ist, wird die Verbindung aufgebaut und die Seite zum einem an den Nutzer A weitergeleitet, zum anderen im Cache abgelegt, damit sie zu einem späteren Zeitpunkt für den Nutzer B zur Verfügung steht, ohne dass dieser abwarten muss, dass die Seite vom Webserver geladen wird (Abbildung 2.8 auf der nächsten Seite)[60]. Der entscheidende Vorteil

[60] Da die Verbindung zwischen Nutzer und Proxy-Cache-Server nur wenige Schritte durchläuft, kann sie um einiges schneller sein als der direkte Zugriff auf den Webserver (Der Geschwindigkeitsvorteil bedeutete insbesondere vor der flächendeckenden Einführung von Breitbandanschlüssen für den einzelnen Nutzer eine Zeit - und damit eine Kostenersparnis).

für die Internet-Provider liegt in der Ersparnis von Traffic, da durch die Verwendung von Proxy-Cache-Servern die beliebtesten Webseiten nicht jedes Mal erneut beim Webserver angefordert werden müssen. Einer der Nachteile ist jedoch, dass dabei zwangsläufig alle Seiten auf dem Server zwischengespeichert werden[61]. Da der Betreiber des Proxy-Cache-Servers meist auch der Access-Provider ist, hat dieser überdies Kenntnis darüber, welcher seiner Kunden zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse zugewiesen bekommen hat. Von der IP-Adresse ausgehend werden wiederum die HTTP-Anfragen an den Proxy-Cache-Server weitergeleitet. Der Access-Provider hätte somit die Möglichkeit, von seinem gesamten Kundenstamm detaillierte Profile über das jeweilige „Surfverhalten“ zu erstellen.

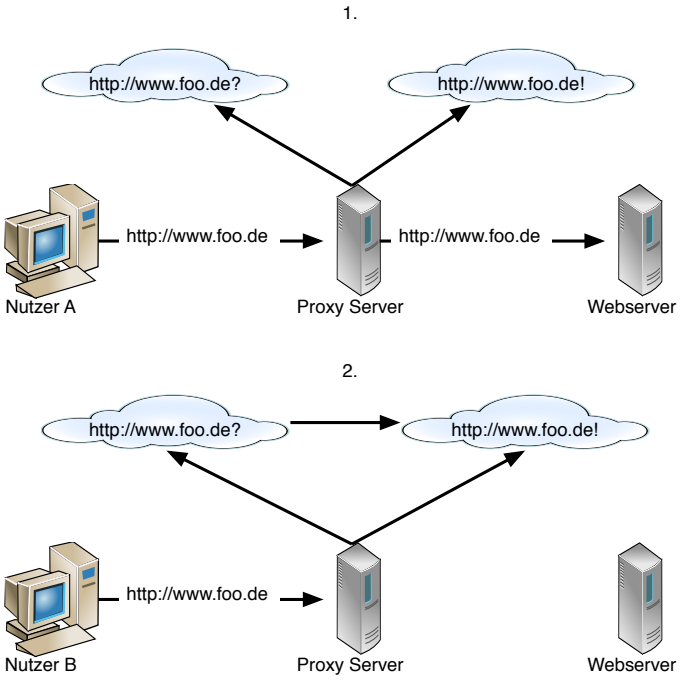


Abbildung 2.8: Proxy-Server als Zwischenspeicher

[61] Für eine Auflistung der Vor- und Nachteile von Proxy-Cache-Servern siehe *Schwiderski-Grosche*, Proxy-Cache-Server, 586–590.

## 3. Digital Rights Management

Um sich vor der freien Kopierbarkeit und der daraus resultierenden unkontrollierbaren Verbreitung insbesondere in Peer-To-Peer-Netzwerken wie z.B. Gnutella[62] oder Bittorrent[63] zu schützen, versehen heutzutage Händler digitaler Inhalte, so vor allem Musik-Händler, welche anbieten, dass der Nutzer sich Musikalben und -stücke direkt vom Online-Shop auf den Computer downloaden kann, diese mit besonderen technischen Mitteln, welche vor unbefugtem Zugang schützen und der Durchsetzung von Einschränkungen der eingeräumten Nutzerrechte dienen[64]. Nachdem die Mittel hauptsächlich dazu dienen, „digitale Rechte“ zu verwalten, werden sie gemäß der englischen Übersetzung ihrer Funktion Digital Right Management (kurz DRM) Systeme genannt. Ihrer Funktion zufolge verwundert es nicht, dass das Gros der rechtlichen Fragen, die im Zusammenhang mit der Verwendung von DRM entstehen, auf dem Gebiet des Urheber- und Wettbewerbsrechts diskutiert wird[65]. Da DRM jedoch auch gerade auf den Bereich des Datenschutzes erhebliche Auswirkungen hat, soll dessen technische Funktionsweise im Folgenden auch in diesem Kontext dargestellt werden.

[62] `Http://www.netzwelt.de/filesharing/gnutella.html/`.

[63] `Http://www.bittorrent.com/`.

[64] Vgl. *Arlt*, Digital Rights Management-Systeme - Begriff, Funktion und rechtliche Rahmenbedingungen nach den jüngsten Änderungen des UrhG - insbesondere zum Verhältnis der §§ 95a ff. UrhG zum Zugangskontrolldiensteschutzgesetz (ZKDSG), 548–554; *Arlt*, Marktabschottend wirkender Einsatz von DRM-Technik - Eine Untersuchung aus wettbewerbsrechtlichem Blickwinkel, 1003–1011.

[65] Weiterführend dazu siehe *Arlt*, Digital Rights Management-Systeme - Begriff, Funktion und rechtliche Rahmenbedingungen nach den jüngsten Änderungen des UrhG - insbesondere zum Verhältnis der §§ 95a ff. UrhG zum Zugangskontrolldiensteschutzgesetz (ZKDSG), 548–554; *Arlt*, Marktabschottend wirkender Einsatz von DRM-Technik - Eine Untersuchung aus wettbewerbsrechtlichem Blickwinkel, 1003–1011; *Peukert*, Digital Rights Management und Urheberrecht, 689–713 zugleich eine Besprechung des zu dieser Thematik grundlegenden Werkes von *Bechtold*, Vom Urheber zum Informationsrecht; *Pleister/Ruttig*, Neues Urheberrecht - neuer Kopierschutz - Anwendungsbereich und Durchsetzbarkeit des § 95a UrhG, 763–767.

Grundsätzlich kann ein DRM auf dreierlei Weise alternativ oder kumulativ betrieben werden: durch Verschlüsselung, durch Kopierkontrollsysteme oder durch Passwörter[66].

Die Verschlüsselungsmethode, der sich meist beim Kauf digitaler Musik im Internet bedient wird, ist die Verschlüsselung mittels Digital Container[67]. Dabei erhält der Nutzer nicht die bloße Datei, welche aus dem von ihm gewünschten Inhalt besteht, sondern eine Datei, die sich aus zwei Teilen zusammensetzt: einem verschlüsselten Teil, welcher ähnlich einer Schachtel den eigentlichen Inhalt ummantelt, und dem Inhalt selbst. Die „Schachtel" enthält die Informationen, welcher Nutzer zum „Öffnen der Schachtel" berechtigt ist, welchem Nutzer es also beispielsweise erlaubt ist, das gekaufte Musikstück auf seinem Computer oder dem MP3-Spieler abzuspielen. Als Mittel zur Überprüfung des verschlüsselten Dateiteils kann dabei zum einen eine speziell zu diesem Zwecke

[66] Vgl. *Bechtold*, Vom Urheber zum Informationsrecht, S. 23.

[67] Dieser Methode, wenn auch anhand verschiedener Verschlüsselungsmethoden, bedienen sich der international erfolgreichste Internet-Musikshop „iTMS" (iTunes Music Store) von Apple und das Shopsystem „Musicload", welches nach eigenen Aussagen Marktführer in Deutschland ist, vgl. *Grimm* et al., Privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management (Studie im Auftrag des Bundesministeriums für Bildung und Forschung), S. 27.

[68] Anhand der technischen Funktionsweise offenbaren sich auch die zwei Hauptkritikpunkte, welche diese mit sich bringt: Zum einen muss der Schlüssel zur „Schachtel" zwangsläufig in der Software integriert sein. Daraus ergibt sich die stete Gefahr, dass der Schlüssel, der sich dadurch auf dem Computer des Nutzers befindet, geknackt wird. Durch das Internet ist es jedoch die Regel, dass ein einmal geknackter Mechanismus so rasch allgemein offen verfügbar sein wird, dass er als solcher nicht weiter wirksam verwendbar ist (so z.B. mit dem Content Scrambling System - kurz CSS - geschehen, mit dem Inhalte von DVDs verschlüsselt werden). Dieses Phänomen wird in Fachkreisen BORA genannt („Brake Once, Run Anywhere, vgl. *Spielkamp*, Das Radikale Maximum, 70–77) und führt dazu, dass sich aus einem in die Clientsoftware integrierten Schlüssel unweigerlich ein Wettlauf zwischen den Contentanbietern und den Nutzern ergibt. Wird das Abspielen hingegen einzig und allein auf festgeschriebenen Endgeräten erlaubt, schränkt das die Nutzer in ihren Rechten zu weit ein, da dieser die von ihm gekaufte Musik nicht nur über einen bestimmten MP3-Player, sondern beispielsweise auch über die heimische Stereoanlage hören will (zur Inkompatibilität als Hemmnis für den Marktzugang und Folge falscher DRM-Strategien s. auch *Bizer/ Grimm/ Will*, Privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management, 69–73).

installierte Abspielsoftware, wie Microsofts Media Player oder Apples iTunes dienen, zum anderen auch verschiedene Endgeräte, wie ein Premiere-Decoder oder der iPod[68].

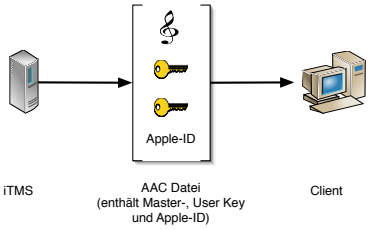


Abbildung 2.9: Download einer Musikdatei vom iTMS

Die zweite Kategorie von DRM-Systemen dient der Kontrolle über die zulässige Anzahl von Kopien und der technischen Erkennung von illegalen Kopien[69] und ist im Zusammenspiel mit der ersten diejenige, mittels derer Datenerhebungen möglich sind: Zusätzlich zur Verschlüsselung, die nur von einer bestimmten Software oder auf bestimmten Endgeräten entschlüsselt werden kann, werden der Datei noch sog. „Metadaten“ hinzugefügt. Diese Metadaten enthalten im einfachsten Falle lediglich die Daten, die den konkreten Inhalt betreffen wie z.B. das Genre, den Titel, das Jahr und das Album auf dem sich das Musikstück befindet[70]. Um eine Kontrolle über die zulässige Anzahl von Kopien zu erreichen, können sie darüber hinaus aber auch Informationen darüber beinhalten, wie oft ein bestimmtes Werk kopiert werden darf, ob Kopien von der Kopie hergestellt werden dürfen, wie lang ein Werk genutzt werden darf, in welchen Ländern es genutzt oder ob es verändert werden darf[71]. Überdies können Daten über den Nutzer als Metadaten abgelegt werden, z.B. um den Ursprung einer trotz des Schutzes in Umlauf gebrachten Datei zurückverfolgen

[69] Vgl. *Grimm* et al., Privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management (Studie im Auftrag des Bundesministeriums für Bildung und Forschung), S. 18.

[70] So z.B. bei iTMS und Musicload, *Grimm/Puchta*, Datenspuren bei der Nutzung von Digital Rights Management-Systemen (DRM), 74–79.

[71] Dies sind Beispiele, welche Nutzungsbeschränkungen sich über die Sprache MPEG REL (Moving Picture Experts Group Rights Expression Language) von ContentGuard, einer Firma deren Inhaber Microsoft, Time Warner Inc. und Thomson sind, implementieren lassen, vgl. `http://www.contentguard.com`.

zu können. Bei iTMS ist das die Apple-ID, die aus der bei Apple angegebenen E-Mail-Adresse des Nutzers besteht[72].

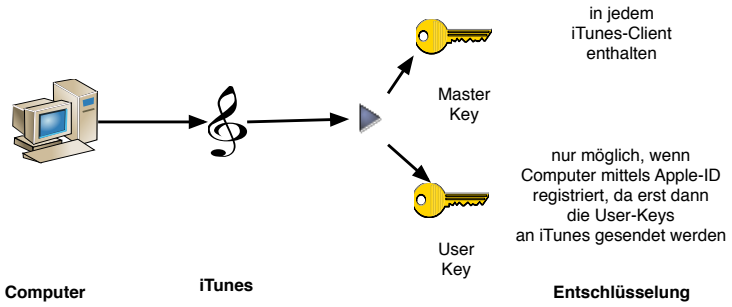


Abbildung 2.10: Entschlüsselung einer AAC-Datei mittels iTunes und registriertem Computer

Die dritte Art und Weise, wie die Nutzungsrechte kontrolliert werden können, ist die Kontrolle durch Passwörter. Sie fällt streng genommen nicht unter das klassische Digital Rights Management, da die Zugangskontrolle mittels Passwörtern allgegenwärtig und nicht auf bestimmte Dienste beschränkt ist. Sie soll jedoch trotzdem in diesem Zusammenhang nicht unerwähnt bleiben, weil sich heutzutage Online-Musikshops häufig aller drei Kategorien kumulativ bedienen, um eine Einschränkung und Kontrolle der Nutzungsrechte zu erreichen. Als Beispiel sei hier abermals der iTMS genannt: Da die Nutzung der downgeloadeten Musik jeweils nur auf fünf Rechnern gleichzeitig erlaubt ist, muss der Nutzer jeden Computer, den er zum Abspielen der Musik mittels iTunes oder zum Übertragen der Musik auf den iPod verwenden möchte, zuvor registrieren. Es ist daher ohne weiteres möglich, die vom iTMS geladene Musik auf eine mobile Festplatte oder CD-Rom zu kopieren und von dort aus auf einen zweiten Rechner zu kopieren. Soll sie jedoch von einem neuen Rechner aus abgespielt werden, öffnet sich ein Fenster, das den Nutzer dazu auffordert, die Apple-ID und das dazugehörige Passwort einzugeben.

[72] *Grimm/Puchta*, Datenspuren bei der Nutzung von Digital Rights Management-Systemen (DRM), 74–79.

## 4. Aktive Inhalte

Im Laufe des Fortschritts der Internettechnik waren die Fähigkeiten, die die Auszeichnungssprache HTML zur graphischen Darstellung von Seiten in einem Browser auswies, für viele Anbieter nicht mehr ausreichend. Demzufolge wurden von verschiedenen Firmen Programmiersprachen entwickelt, mittels derer Programme erschaffen werden können, die heutzutage unter den Begriff „aktive Inhalte“ fallen[73]. Die gängisten Programmiersprachen sind dabei ActiveX von Microsoft[74], VBScript[75], JavaScript[76] und Java[77].

Aktive Inhalte funktionieren nach folgendem Prinzip: Der Programmcode wird zunächst auf einem Webserver gespeichert. Ferner wird auf der Webseite, bei deren Darstellung die aktiven Inhalte ausgeführt werden sollen, die Aufforderung hinzugefügt, der Browser solle sich den aktiven Inhalt zunächst downloaden und ihn anschließend auf dem lokalen Rechner ausführen. Ruft der Nutzer daraufhin in seinem Browser die Webseite auf, wird demnach ein Programm auf seine Festplatte geladen und anschließend gestartet. Je nach Browsereinstellung und Programmiersprache erhält er darüber eine kurze Mitteilung oder einen Dialog, in dem er bestätigen muss, dass er mit dem Kopieren und Starten des Programmes auf seiner Festplatte einverstanden ist. Das Programm kann aber auch ohne Kenntnis des Nutzers ausgeführt werden, weil er

[73] Zur clientseitigen WWW-Programmierung siehe ausführlich in *Meinel/Sack*, WWW, S. 1032 ff.

[74] `Http://msdn.microsoft.com/en-us/library/aa268985.aspx`.

[75] Ebenfalls von Microsoft und u.a. bereits Inhalt des Windows Betriebssystems; VBScript wird sowohl clientseitig als auch serverseitig benutzt, `http://msdn.microsoft.com/en-us/library/t0aew7h6.aspx`.

[76] JavaScript war der ursprüngliche Name der Firma Netscape. Die von Microsoft angepasste Sprache nannte sich JScript. Inzwischen wurde die Sprache als ECMAScript von der ECMA (European Computer Manufacturers Association) standardisiert, s. ECMA 262 bzw. ISO/IEC 16262 (zu finden auf der Webseite der ISO, `Http://www.iso.org`).

[77] Von Ingenieuren bei Sun Microsystems entwickelt ist Java als einzige der aufgezählten Sprachen eine echte Programmiersprache und keine Skriptsprache.

dies entweder im Browser freigegeben hat oder auf böswillige Art und Weise eine Sicherheitslücke genutzt wurde.

Ebenso zahlreich wie die Möglichkeiten, für die aktive Inhalte eingesetzt werden können, sind auch die Möglichkeiten, mittels ihrer Daten beim Nutzer zu erheben. Zu einem Zeitpunkt, als ActiveX sich noch in einem frühen Entwicklungsstadium befand, gelang es dem Chaos Computer Club beispielsweise, mittels eines ActiveX Controls die Finanzmanagement-Software Quicken derart zu manipulieren, dass eine beliebige Summe auf ein Konto überwiesen wurde, sobald der ahnungslose Nutzer im Internet auf einen Link geklickt hat[78]. Sicherlich wird in diesem Fall die Tatsache, dass der Name und die Bankverbindung des Nutzers mitübermittelt werden, das geringere Problem sein, aber schon an diesem Beispiel lässt sich erkennen, dass aktive Browserinhalte datenschutzrechtlich betrachtet ein großes Risiko darstellen. Eine hinsichtlich ActiveX weiterhin häufig genutzte Methode, beim Nutzer heimlich Daten zu erheben, ist die Installation von beim Internet Explorer so genannten *browser helper objects* (BHOs)[79]. Für einen Angreifer im Internet stellen BHOs die einfachste Methode dar, auf Computern von Dritten Spyware auszuführen.

### 5. Spyware

Unter Spyware wird „jedes Programm verstanden, welches die Schritte eines Computernutzers verfolgt oder ausspioniert“[80]. ActiveX stellt in Verbindung mit BHOs aus dem Grund die einfachste Methode dar, Spyware zu installieren, weil zum einen das Sicherheitskonzept von ActiveX größtenteils auf die Fähigkeit des Nutzers vertraut[81], selbst zu beurteilen, welche Programme er

[78] *Donnerhacke/Peter*, Vorsicht, Falle!, 90.
[79] Siehe dazu und zu aktiven Inhalten sehr detailliert *Skoudis/Zeltser*, Malware, Chapter 4; zu BHOs siehe auch sogleich.
[80] *Bennett, John, Jr.*, The Digital Umbrella, S. 33.
[81] ActiveX läuft im Gegensatz zu Java oder JavaScript nicht in einer sog. Sandbox, welches die Programme in einem vom restlichen Betriebssystem ablaufenden Bereich isoliert und damit zumindest dann ein höheres Maß an Sicherheit garantiert, wenn der Nutzer dem

auf seinen Rechner installiert haben will. Zum anderen erfreut sich der Browser „Internet Explorer“ der größten Verbreitung. Somit ist es möglich, eine große Publikumsanzahl mit einer Spyware zu „versorgen“, die automatisch jedes Mal dann startet, wenn der Internet Explorer geöffnet wird[82]. Die Installation geschieht dabei entweder durch das Umgehen des Sicherheitskonzepts von Windows oder dadurch, dass davon ausgegangen wird, dass das Warnfenster, das sich öffnet, wenn das BHO installiert werden soll, ignoriert wird und das Applet installiert wird, weil der Nutzer befürchtet, einen aktiven Inhalt sonst nicht betrachten zu können. Wie bereits erwähnt, stellt BHO die Abkürzung für *browser helper objects* dar. Nicht immer sind diese „Plug-Ins“ des Internet Explorers bedenklich. So ist die Google Toolbar beispielsweise lediglich eine Erweiterung des Internet Explorers dahingehend, dass unter der Adressleiste eine weitere Leiste integriert wird, aus der heraus direkt in Google gesucht werden kann, ohne zuvor die Seite benutzen zu müssen[83].

Abbildung 2.11: Google-Toolbar, Quelle: http://toolbar.google.com

Gefährlich sind jedoch BHOs wie bestimmte Varianten des derzeit weit verbreiteten Gator oder ZQuest, die nicht nur die Homepage des Browsers umstellen, Werbe-Pop-Ups aufspringen lassen und sämtliche Suchanfragen über eigens zu diesem Zweck bestimmte Suchengines umleiten[84]. Diese verändern häufig auch die Sicherheitseinstellungen des Internet Explorers derart, dass das System anfälliger wird (z.B. für Trojaner[85]) oder sämtliche Eingaben mitgeloggt werden, die im Internet Explorer getätigt werden, um auf diese Weise das

Programm nicht willentlich oder durch Unachtsamkeit explizit mehr Rechte einräumt; zur Sandbox und zum JavaScript Sicherheitsmodell siehe *Powell, Thomas A. and Schneider, Fritz*, JavaScript 2.0, S. 679, zur Sandbox und dem Java Applet Sicherheitsmodell siehe außerdem *Skoudis/Zeltser*, Malware, S. 158 ff.

[82] *Skoudis/Zeltser*, Malware, S. 149.

[83] `Http://toolbar.google.com/intl/de/index_ie.php`.

[84] So genanntes Browser Hijacking.

[85] Siehe dazu unter Abschnitt B.II.6. auf der nächsten Seite

Surfverhalten, Kennwörter, Kreditkartennummern und sonstige private Daten auszuspionieren.

Darüber hinaus werden bei diesen BHOs meistens Mechanismen eingebaut, welche die Entdeckung durch ein Spyware Removal Tool[86] und die daraus resultierende Entfernung des BHOs verhindern sollen, so dass die einzige Lösung, um sich des BHOs zu entledigen dann ist, die Festplatte des Computers zu formatieren und das Betriebssystem neu zu installieren.

### 6. Trojaner

Ein Trojaner „ist ein Programm, das einen nützlichen oder guten Zweck zu haben scheint, um damit seine in Wirklichkeit bösartige Funktionalität zu tarnen“[87]. Gerade in Zeiten in der Tauschbörsen sich wachsender Beliebtheit erfreuen und viele Nutzer dort Dateien von zweifelhafter Herkunft herunterladen, um sie auf dem eigenen Computer zu installieren, ist das Gefährdungspotential von Trojanern stark gewachsen. Der Trojaner kann sich beispielsweise als nützliches Freeware-Kalender-Programm tarnen, dessen Funktionalität als solche zwar gegeben ist, der aber zusätzlich auch den Fernzugriff auf den Computer freigibt. Eine andere Vorgehensweise besteht darin, den Trojaner als Programm anzupreisen, der die zeitlimitierte Beschränkung eines Tests von kommerziellen Anwendungen aufheben soll. Derzeit im Umlauf ist auch das Programm Spyware Protection 2009, das sich als Spyware Removal Tool geriert[88], dabei angibt, auf dem Computer in Wahrheit nicht vorhanden gewesene Spyware entfernt zu haben und im Hintergrund Trojaner ausführt[89]. Wird der Trojaner auf dem befallenen Computer gestartet, ist über den Fernzugriff demjenigen, der auf den Computer zugreift, jede Möglichkeit eröffnet, die dem Administrator des Computers auch zur Verfügung steht: Mittels des weit verbreiteten Tro-

[86] Z. B. Ad-aware oder SpyBot - Search & Destroy.
[87] *Skoudis/Zeltser*, Malware, S. 251.
[88] Diese Art von Programme nennen sich „rogue software“ engl.: rogue: der Schurke).
[89] `Http://de.pcthreat.com/parasitebyid-7670de.html`.

janers SubSeven ist es zum Beispiel möglich, Dateien und Ordner zu löschen, ändern und zu kopieren, Instant-Messenger-Zugangsdaten zu stehlen oder den Computer dazu zu zwingen, Texte mit einer Computerstimme vorzulesen[90].

## 7. Spambots

Spambots sind kleine Programme, die von einer bestimmten Seite aus startend diese systematisch nach E-Mails und Links durchsuchen. Die gefundenen E-Mails werden in eine Spamadressdatenbank eingetragen, bei den gefundenen Links sucht das Programm weiter, um auf diese Weise ähnlich einer Lawine[91] an eine immer größer werdende Anzahl von E-Mail-Adressen zu gelangen. Spambots werden heutzutage in einem so hohen Ausmaß benutzt, dass sich jeder, der über einen „<a href="mailto:...>-Tag“ die E-Mail-Adresse auf seiner Homepage verlinkt, sicher sein kann, dass er über kurz oder lang eine hohe Anzahl an Spam-E-Mails erhalten wird[92]. Viele Programme beinhalten auch Zusatzfunktionen, mittels derer es möglich ist, aus Internetseiten, die ein Impressum enhalten, ganze Adresssätze mit Namen, Telefonnummer, Faxnummer und E-Mail-Adresse zu generieren[93].

[90] *Wang, Wallace*, Steal this Computerbook, S. 118.

[91] Da auch der Vergleich mit einer Spinne nahe liegt, die im (weltweiten) Netz entlang krabbelt, zählen diese Programme zu den sog. „Webcrawlern".

[92] Nähere Informationen über Spambots und welche Lösungen es gibt, um zu verhindern, dass durch Spambots die eigene Liste in Spamverteiler aufgenommen wird, finden sich unter der (englischsprachigen) Internetseite: `http://www.turnstep.com/Spambot/`. Ein Beispiel für ein Programm, welches zumindest als Spambot zu missbrauchen wäre, ist unter `http://www.1-bulk-email-software.net/spider-web.html` zu sehen.

[93] So z.B. der „Super Email Spider “ `http://www.futureality.com/`.

# III. Reaktive Maßnahmen zur Datenerhebung

## 1. Formulare

Um den Kontakt mit dem Betreiber einer Internet-Seite aufzunehmen, bietet dieser heutzutage statt der Angabe seiner E-Mail-Adresse häufig ein auszufüllendes Formular an. Für die Betreiber großer Firmen bieten Formulare den Vorteil, dass in Ihnen abgefragt werden kann, welche Art der Kontaktaufnahme der Benutzer verfolgt (z.B. Supportanfrage, Anfordern von Informationen, Abrechnungsfragen) und sie daraufhin gleich automatisch an die richtigen Ansprechpartner weitergeleitet werden. Im Übrigen wird durch die mangelnde öffentliche Preisgabe der eigenen E-Mail-Adresse durch den Betreiber auch der Erhalt von Spam verhindert, welchem sie anderenfalls durch die Verwendung von Spambots unweigerlich anheim fallen würde.

Technisch gesehen ermöglicht es HTML, ein Formular mit verschiedenen Eingabefeldern zu erstellen, bei denen der Ersteller zwischen Texteingabefeldern, Auswahllisten, Radio-Buttons und Checkboxen wählen kann. Ferner gibt es jedoch ein Eingabefeld, welches in der HTML-Sprache den Namen „hidden“ trägt[94]. Dieses ermöglich vor allem in Kombination mit JavaScript, vom Nutzer ungesehen Daten an den Web-Server zu übertragen. Auf diese Weise ist es beispielsweise realisierbar, den Namen des Browsers, die Browserversion, die Einstellung bzgl. der Cookies, die Browser-Sprache und das Betriebssystem, auf dem der Browser läuft, mit zu übertragen[95]. In diesem Umfang stellt die sonst reaktive Maßnahme des Ausfüllens und Absendens von Formularen eine non-reaktive Maßnahme dar.

Werden die Daten vom Nutzer über den Button „Senden“ an den WWW-Server übertragen, wird gleichzeitig mitgesendet, wie der WWW-Server mit den Daten weiterverfahren soll. Über die CGI-Schnittstelle (Common Gateway

[94] Engl. für „versteckt“.

[95] Zur genauen technischen Umsetzung s. das Kapitel über Formulare von SELFHTML (`http://de.selfhtml.org/`).

Interface) kann der Betreiber die Daten mit einer beliebigen Applikation (die meist in Perl[96] oder PHP[97] geschrieben sein wird) weiterverarbeiten.

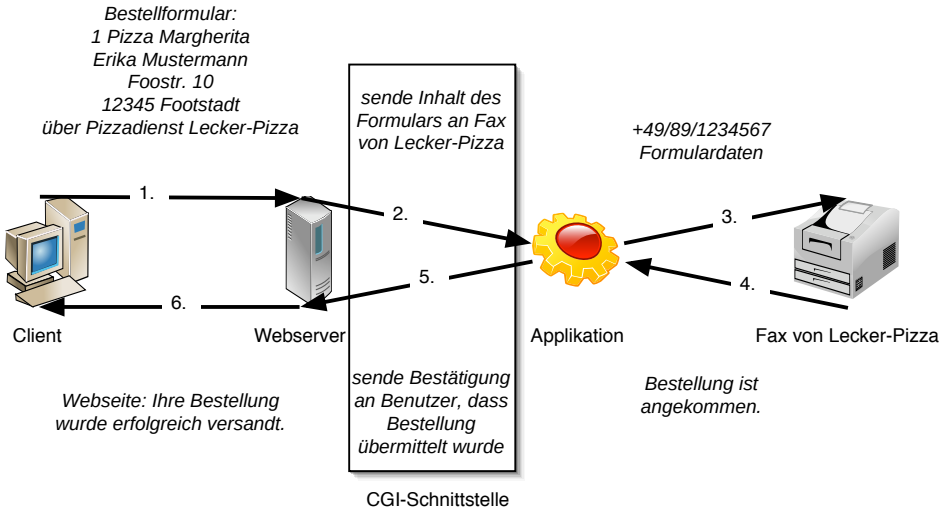


Abbildung 2.12: Funktionsweise der CGI-Schnittstelle anhand einer Bringdienst-Bestellung

Mittels CGI ist es daher beispielsweise möglich, sich bei einem Bringdienst-Portal einen Lieferservice auszusuchen, dort ein Bestellformular abzusenden und dieses über den WWW-Server an ein Programm weiterzuleiten, dass die Bestellung an das Fax des Bringdienstes übermittelt (Abbildung 2.12). Bei dieser Gelegenheit können die Kundendaten auch in die Datenbank des Bringdienstes eingefügt und dauerhaft hinterlegt werden.

Datenschutzrechtlich von besonderer Relevanz, weil sie in Unkenntnis vom Nutzer zu einer Erhebung führen können, sind im Zusammenhang mit Online-Formularen neben dem „hidden“ -Feld somit auch die CGI-Umgebungsvariablen des Webservers. Die sog. Umgebungsvariablen sind Zeichenketten, die der Webserver an das CGI-Skript automatisch weiterleitet,

[96] `Http://www.perl.org`.
[97] `Http://www.php.net`.

**CGI test script.**

Get the source for this script.

SSI Documentation

---

Results of the UNIX date command
Thu Feb 16 07:25:47 EST 2006

---

DOCUMENT_ROOT = /www/doc
GATEWAY_INTERFACE = CGI/1.1
HTTP_ACCEPT = */*
HTTP_ACCEPT_ENCODING = gzip, deflate
HTTP_ACCEPT_LANGUAGE = en
HTTP_CONNECTION = keep-alive
HTTP_COOKIE = __utmz=233409094.616783871.1140001640.1140001640.1140001640.1;
__utma=233409094.1140001640.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)
HTTP_HOST = www.itc.virginia.edu
HTTP_REFERER = http://www.itc.virginia.edu/desktop/web/cool_tools.html
HTTP_USER_AGENT = Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/417.9 (KHTML, like Gecko) Safari/417.8
PATH = /usr/bin:/usr/ucb:/bin:/usr/sbin:/sbin:/usr/local/bin
QUERY_STRING =
REMOTE_ADDR = 193.174.132.5
REMOTE_PORT = 37481
REQUEST_METHOD = GET
REQUEST_URI = /desktop/web/test.cgi
SCRIPT_FILENAME = /www/doc/desktop/web/test.cgi
SCRIPT_NAME = /desktop/web/test.cgi
SCRIPT_URI = http://www.itc.virginia.edu/desktop/web/test.cgi
SCRIPT_URL = /desktop/web/test.cgi
SERVER_ADDR = 128.143.22.53
SERVER_ADMIN = jbb@virginia.edu
SERVER_NAME = www.itc.virginia.edu
SERVER_PORT = 80
SERVER_PROTOCOL = HTTP/1.1
SERVER_SIGNATURE =
*Apache/1.3.27 Server at www.itc.virginia.edu Port 80*

SERVER_SOFTWARE = Apache/1.3.27 (Unix) mod_fastcgi/2.4.2 mod_ssl/2.8.12 OpenSSL/0.9.7a PHP/4.2.3 mod_pubcookie/3.2.0
TZ = EST5EDT
UNIQUE_ID = Q-RvS4CPFjUAA7CaYkQ
The results of the UNIX id command
uid=402(webuser) gid=100(usr) groups=101(users),951(kr2rgrp),428(attscgi),536(jlkgrp),786(emp-cvgi),768(bme-web),929(cfp-web),1024(rangephp),1028(resphp),1026(hstryphp),394(wwwdtc),522(dave_grp),1049(mgh3egrp),794(ppools),830(range),792(ortweb)

Abbildung 2.13: Ergebnis eines CGI-Requests, der mit dem eigenen Computer mittels des Beispielsskripts der University of Virginia erzeugt wurde

um diesen Informationen zur Umgebung, in welcher der Nutzer arbeitet, zu liefern. In dieser Eigenschaft dienen sie dazu, mit Hilfe des CGI-Skripts dynamische Webseiten zu generieren, die auf die Umgebung des Nutzers abgestimmt sind. Inhalt der Umgebungsvariablen können der DNS-Name bzw. die IP-Adresse des Nutzers, der Nutzername, der Name des Browsers, die Browserversion und das verwendete Betriebssystem des Nutzers und die Referer-Seite sein (Abbildung 2.13, welche die Ergebnisse eines zu Testzwecken eingerichteten Beispiel-Skripts der University of Virginia zeigt; zu finden unter: `http://www.itc.virginia.edu/desktop/web/webtests/test.cgi`).

Die datenschutzrechtlichen Belange des Nutzers können hier insbesondere dann empfindlich berührt sein, wenn er durch das Ausfüllen von Formularen

online an anonymen Umfragen oder Online-Experimenten teilnimmt und durch die Erhebung der IP-Adresse seine Identität rekonstruierbar wird.

### 2. Registrierung

Um Internet-Angebote nutzen zu können, ist meist eine einmalige „kostenlose“ Registrierung nötig. Nur nachdem der Nutzer sich registriert hat, erhält er vom Anbieter die Zugangsdaten und kann mit diesen das Angebot nutzen. Da ohne Verwendung der Zugangsdaten eine Nutzung des Angebots in der Regel nicht möglich ist, weiss der Anbieter, je nachdem wie viele Daten er dem Nutzer bei der Registrierung abverlangt hat, genau, wer wann sein Angebot nutzt. Nachdem heutzutage viele Anbieter eine Mischkalkulation aus werbefinanzierten und kostenpflichtigen Angeboten betreiben[98], unterscheidet sich häufig die Menge an Daten, die bei der Registrierung angeben werden muss, je nachdem, ob der Kunde sich für die kostenlose oder zu bezahlende Version des Zugangs entscheidet. Welche Daten für die erfolgreiche Durchführung einer Registrierung vom Nutzer angegeben werden müssen, kann der Anbieter über das Verwenden von sog. Pflichtfeldern in den Registrierungs-Formularen dabei frei bestimmen: Er braucht dazu lediglich das Formular dahingehend zu konfigurieren, dass die Registrierung erst dann abgeschlossen werden kann, wenn das entsprechende Formularfeld tatsächlich ausgefüllt wurde.

Als Beispiel kann hier der E-Mail-Anbieter GMX dienen, der mit dem Produkt GMX FreeMail einen werbefinanzierten und mit GMX ProMail oder TopMail werbefreie, aber kostenpflichtige Zugänge anbietet. Für die Anmeldung zu jedem Accounttypus muss zumindest der Vor- und Nachname, die Postadres-

[98] So z.B. die beiden großen deutschen E-Mail-Anbieter „Web.de“ und „GMX.de“ mit dem werbefinanzierten Angebot „WEB.DE FreeMail“ und dem kostenpflichtigen Angebot „WEB.DE Club“ (`http://www.web.de`) bzw. mit dem werbefinanzierten Angebot „GMX FreeMail“ und den kostenpflichtigen Angeboten „GMX ProMail“ und „GMX TopMail“ (`http://www.gmx.de`).

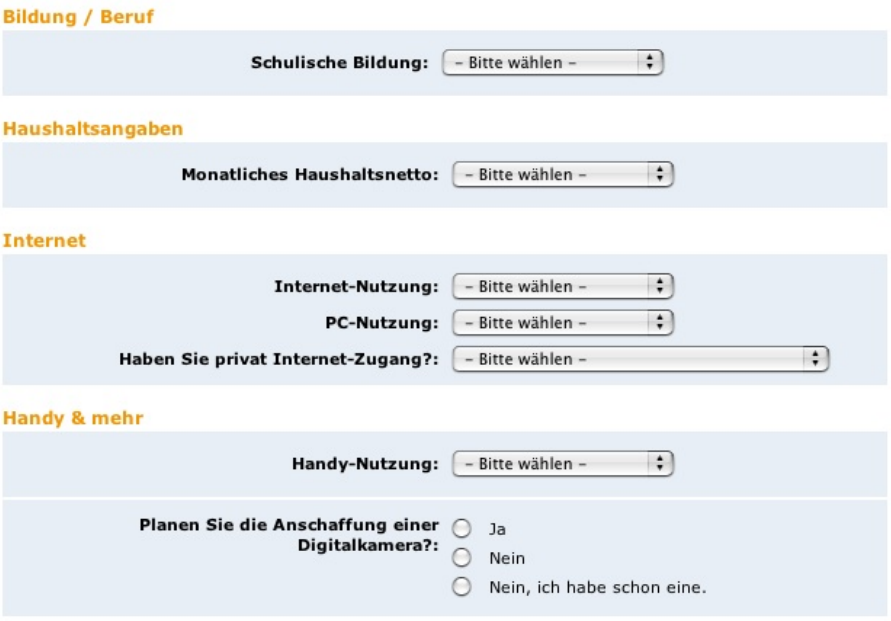


Abbildung 2.14: Freiwillige Daten, die bei der Registrierung bei GMX FreeMail abgefragt werden, Quelle: Screenshot von http://www.gmx.de

se sowie das Geburtsdatum angegeben werden, welches GMX nach eigenen Angaben benötigt, weil einige ihrer Angebote altersabhängig sind.

Die Daten, die anschließend von GMX abgefragt werden, sind dahingegen davon abhängig, für welche Art von Produkt sich der Kunde entschieden hat: Beim freien Produkt sind die Angabe einer Festnetznummer erforderlich und es erscheinen während des Anmeldevorgangs zwei weitere Fenster, die zumindest die Angabepflicht weiterer Daten suggerieren (wenn sie auch nicht notwendig sind, um die Anmeldung abzuschließen). Beim kostenpflichtigen Zugang hingegen ist lediglich die Angabe einer Bankverbindung notwendig (Abbildung 2.14).

Technisch gesehen birgt eine Registrierung bei einem Internetangebot keine Besonderheiten gegenüber den unter Abschnitt B.III.1. auf Seite 40 erwähnten

Formularen. Über ein CGI-Skript werden die während des Anmeldevorgangs angegebenen Informationen in eine Datenbank übermittelt und dort gespeichert. Zusätzlich werden über ein weiteres Programm die Logindaten generiert, im Fall von GMX eine neue E-Mail-Adresse erstellt und eine Benachrichtigung über die Einzelheiten des Zugangs an den Browser des Nutzers übermittelt.

### 3. Phishing

Die im folgenden dargestellten „Möglichkeiten" des Phishing und des Spoofing fallen streng genommen weder in die Kategorie der reaktiven noch der non-reaktiven Maßnahmen. Sie sind insofern reaktiv, als dass der Nutzer weiss, dass er seine Daten preisgibt, jedoch insofern non-reaktiv als dass der eigentliche Empfänger der Daten ihm bewusst verschleiert bleibt.

Nach der Erklärung der Anti-Phishing Working Group[99] ergibt sich der Begriff „Phishing" daraus, dass bei selbigen „E-Mails als Köder dafür ausgeworfen werden, um Passwörter und Finanzdaten aus dem See der Internet-User zu fischen", wobei die Buchstabenkombination „Ph" in Hackerkreisen einen üblichen Ersatz für den Buchstaben „F" darstellt.

Beim Phishing werden an eine Vielzahl von Nutzern Spam-E-Mails gesendet, die einer Kunden-E-Mail einer Bank, eines Bezahldienstes wie PayPal oder des Online-Auktionshauses Ebay täuschend ähnlich sehen. Der Versender spekuliert dabei darauf, ohne dies zuvor kontrolliert zu haben, dass sich unter dem großen Pool der Empfänger mit hoher Wahrscheinlichkeit auch tatsächlich Kunden der Banken oder des Bezahldienstes befinden. Auf diese Weise werden Phishingattacken, deren Opfer zunächst nur Kunden von amerikanischen Banken waren[100], seit Anfang 2004[101] bereits auf Kunden vieler, vor allem grosser,

[99] `Http://www.antiphishing.org`.
[100] *Gercke*, Die Strafbarkeit von Phishing und Identitätsdiebstahl, 606–612.
[101] *Fox*, Phishing, 365.

deutschen Banken wie der Citibank, der Deutschen Bank, der Postbank und der Volksbanken[102] ausgelegt.

Meist wird den Kunden in der E-Mail mitgeteilt, ihr Passwort sei ausgelaufen und es sei notwendig, die persönlichen Daten neu anzugeben. Am Ende der E-Mail befindet sich ein Link, der vermeintlich auf die Seite der Bank führt. Öffnet der Kunde den Link in seinem Browser, so gelangt er auf eine Seite, die von der optischen Gestaltung mit derjenigen der anvisierten Bank identisch ist. Auch die Formularseite, innerhalb derer der Kunde seine Daten eingibt, um sie daraufhin an den Angreifer zu übermitteln, ist meist derartig professionell gestaltet, dass der Kunde zu keinem Zeitpunkt den Verdacht schöpft, er könnte sich auf der Seite eines anderen Anbieters als seiner Bank befinden.

Während zu früheren Zeiten dabei darauf vertraut wurde, dass der Kunde, welcher gegenüber Phishing-Angriffe üblicherweise arglos war, dabei nicht genau darauf achten würde, ob er sich auf der Seite von `http://www.deutsche-bank.de` oder auf einer leicht gefälschten Seite vom Angreifer `http://deutsche-bank.angreifer.de` befindet, hat die Informationspolitik und die daraus resultierende steigende Achtsamkeit der Anwender dazu geführt, dass Phishing-Angriffe häufig mit einer Seite kombiniert werden, die sich des Visual-Spoofings bedient, um den Kunden über die eigentliche Identität des Betreibers hinwegzutäuschen[103].

Aktuelle Browser-Versionen sollen den Nutzer durch integrierte Schutzmechanismen davor bewahren, unbedarft Finanzdaten an Dritte weiterzugeben: So beinhaltet der Browser Firefox ab Version 2.0 die Erweiterung „Safe Browsing“[104] von Google, welcher zum einen die URL mit einer schwarzen Liste abgleicht und zum anderen die Möglichkeit bietet, besuchte Seiten von einen eigens zu diesem Zwecke eingerichteten Server prüfen zu lassen[105]. Im Gegen-

[102] *Knupfer*, Phishing for Money, 641–642.
[103] Zum Visual Spoofing siehe sogleich.
[104] Von Mozilla in „Phishing Protection“ umbenannt.
[105] `Http://www.firefox-browser.de/wiki/Phishing-Schutz`.

zug bietet der „Phishing Filter“ der im Internet Explorer ab Version 7 integriert ist, einen Abgleich mit einer Whitelist an, was dazu führt, dass der Benutzer stets dann eine Warnung erhält, wenn er auf einen Server zugreifen will, der sich nicht in dieser Liste befindet[106].

### 4. Visual-Spoofing

Visual-Spoofing ist das Abändern einer Webseite auf die Art und Weise, dass ihr Inhalt nicht nur den eigentlichen Inhalt der Seite, sondern auch Teile des Webbrowsers darstellt. Mittels einer visual gespooften Seite ist es daher möglich, den Benutzer zum einem durch eine Graphik, die den oberen Teil des Browsers samt Adressleiste darstellt, darüber hinwegzutäuschen, dass er sich auf dem Server eines Angreifers befindet, zum anderen durch eine Graphik, die den unteren Teil des Browsers darstellt, dem Benutzer durch Einblenden des Schlosses[107] in den Glauben zu versetzen, er hätte eine sichere Verbindung geöffnet. Damit das Visual Spoofing funktioniert, muss die gespoofte Seite auf den Browser ausgelegt sein, mit dem der Nutzer surft. Im Browser darf darüber hinaus nicht die Funktion deaktiviert sein, die es mittels JavaScript erlaubt, ein neues Browserfenster ohne Kopf und Fussleiste zu öffnen, welche sonst beispielsweise durch das Einfügen eines leeren Links, der die entsprechende JavaScript-Funktion ausführt, geöffnet werden kann:

```
<a href="" OnClick="javascript:window.open('http://www.
    gespoofte-seite.de','Fenster-Name','status='no',
    toolbar='no',menubar='no')">Bitte hier klicken</a>
```

[106] Siehe dazu den Blogeintrag des Lead Program Manager für die Sicherheit des Internet Explorer, Rob Franco, unter `https://blogs.msdn.com/ie/archive/2005/08/31/458663.aspx`.

[107] Das eingeblendete Bild eines Schlosses im Browserfenster, wie es in der Fussleiste von Abbildung 2.15 auf der nächsten Seite zu sehen ist, bedeutet, dass der Nutzer über eine gesicherte Verbindung mit dem Server kommuniziert.

Abbildung 2.15 zeigt ein im Internet erzeugtes Beispiel, aus dem erkennbar wird, wie täuschend echt eine mittels Visual-Spoofing erzeugte Seite aussehen kann. Es ist nicht auszuschließen, dass technisch versierte Angreifer in Zukunft unter Verwendung einer Kombination mehrerer der hier dargestellten Möglichkeiten beispielsweise zunächst eine Phishing-E-Mail senden und ihre Webserver zusätzlich so konfigurieren, dass vor Anzeige der Webseite zunächst der Browsertyp des Opfers ermittelt wird. Daraus ergäbe sich die Möglichkeit eine auf speziell auf das Opfer ausgelegte visual gespoofte Seite zu erzeugen. Der sicherste Schutz besteht daher darin, den eigenen Browser mit einem derart individuellen Aussehen zu konfigurieren, dass eine Spoofing-Attacke sofort ins Auge fallen würde[108].

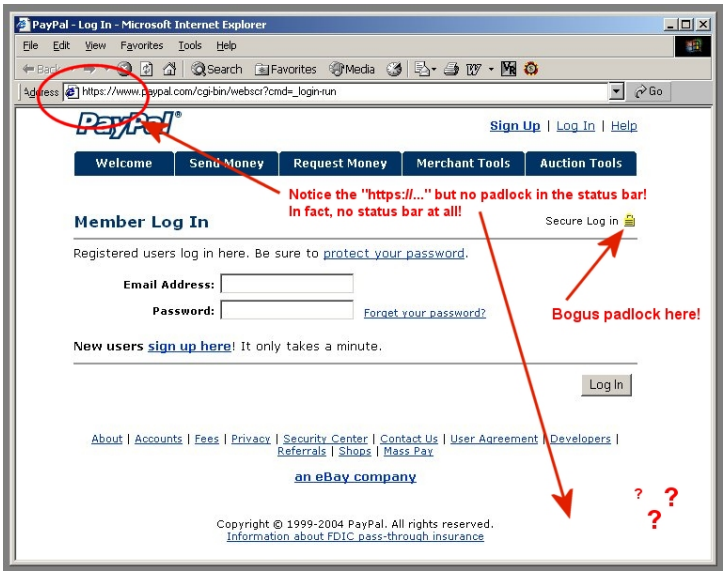


Abbildung 2.15: gespoofte PayPal-Seite, Quelle: http://www.paypalsucks.com

[108] So auch *Adelsbach/Gajek/Schwenk*, Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures, 204–217.

# C. Rechtlicher Rahmen für Datenerhebung

Wer sich mit Fragen des Datenrechts befasst, findet sich einer Vielzahl an Normen gegenübergestellt, welche im Laufe der letzten Jahre einem stetigen Wandel unterlagen. Eine an dieser Stelle folgende, bewusst kurz gehaltene Zusammenfassung der Entwicklung des Datenschutzrechts soll einen Überblick über die Entstehung des Datenschutzrechts auf internationaler sowie nationaler Ebene verschaffen. Auf nationaler Ebene ist dabei zur Klärung von Fragen im Bereich des Internets sowohl auf das Bundesdatenschutzgesetz (BDSG) als auch auf verschiedene spezialgesetzliche Regelungen einzugehen.

## I. BDSG

### 1. Entwicklungstendenzen bis zur Verkündung des BDSG

Auf nationaler Ebene beginnt die Geschichte von Datenschutzgesetzen erst im Jahre 1970 mit Erlass des Hessischen Datenschutzgesetzes. Bei dessen Erlass sowie dem Erlass weiterer Länderregelungen in den darauf folgenden Jahren ging es weniger um eine Reaktion auf Missbrauchshandlungen in der Praxis, als vielmehr um rein prospektive Befürchtungen angesichts der damals voranschreitenden technologischen Entwicklung[1].

Auf Bundesebene führte der Entschließungsantrag einer Gruppe von Abgeordneten am 27.3.1969 zur Bildung einer interparlamentarischen Arbeitsgemeinschaft. Diese legte am 02.12.1971 den ersten Entwurf eines Bundesdaten-

[1] *Abel* in: *Roßnagel*, Handbuch Datenschutzrecht, 2.7 Rdnr. 1.

schutzgesetzes vor[2], welcher aber aufgrund der vorgezogenen Bundestagswahlen 1972 der Diskontinuität zum Opfer fiel.

Neben dem Entwurf der Arbeitsgemeinschaft wurde vom Bundesminister des Inneren ein Referentenentwurf und von Podlech ein Alternativentwurf[3] vorgestellt, wobei letztendlich die eher pragmatisch angelegte Konzeption des Regierungsentwurfs übernommen wurde, dessen erste Lesung im Bundestag am 29.11.1973 stattfand[4].

Nach zwei weiteren Lesungen und Berücksichtigung der Einwände des Bundesrates, welcher unter anderem den Nachrang des BDSG gegenüber dem Landesrecht durchsetzen konnte, wurde die erste Fassung des Gesetzes am 27.1.1977 verkündet, dessen wesentliche Teile 1978 in Kraft getreten sind[5].

## 2. Das Volkszählungsurteil

Noch bevor die über Jahre geführte Diskussion über eine Novellierung des Datenschutzrechts in eine Gesetzesreform münden konnte, erging am 15.12.1983 das Volkszählungsurteil des Bundesverfassungsgerichts[6], in dem erstmals das Recht auf informationelle Selbstbestimmung als Grundrecht mit Verfassungsrang anerkannt wurde. Danach setzt die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus[7].

[2] BT-Drs. VI/2885.
[3] *Podlech*, Prinzipien des Datenschutzes in der öffentlichen Verwaltung, 3–13.
[4] BT-Drs. 7/1027, *Abel* in: *Roßnagel*, Handbuch Datenschutzrecht, 2.7 Rdnr. 15 f.
[5] BGBl. I 1977, S. 201 ff. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung; *Abel* in: *Roßnagel*, Handbuch Datenschutzrecht, 2.7 Rdnr. 17.
[6] BVerfGE 65, 1.
[7] BVerfGE 65, 1 [45]; zu den Reaktionen auf das Volkszählungsurteil in der Literatur siehe z.B. *Busch*, Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts, 385–389; *Hase*, Das Recht auf „informationelle Selbstbestimmung “, 39–47; *Mückenberger*, Datenschutz als Verfassungsgebot, 1–24; *Hufen*, Das Volkszählungsurteil des Bundesverfassungsgerichs und das Grundrecht auf informationelle Selbstbestimmung - eine juristische Antwort auf „1984“?, 1072–1078.

Die verfassungsrechtliche Grundlage des Rechts auf informationelle Selbstbestimmung leitete das Bundesverfassungsgericht im Volkszählungsurteil in „erster Linie“ aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG her. Auch aus späteren Urteilen ist ersichtlich, dass das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung einerseits als Konkretisierung des allgemeinen Persönlichkeitsrechts ansieht[8]. Andererseits darf jedoch nicht übersehen werden, dass das Recht auf Datenschutz auch in andere grundrechtlich geschützte Bereiche hineinfließt. Als solche seien die Meinungs- (Art. 5 Abs. 1 GG), die Versammlungs- (Art. 8 Abs. 1 GG) und Vereinigungsfreiheit (Art. 9 Abs. 1 GG), die Unverletzlichkeit der Wohnung (Art. 13 GG) und, für den Bereich der Telekommunikation besonders relevant, das Brief-, Post und Fernmeldegeheimnis (Art. 10 Abs. 1 GG) genannt[9].

Nach den Vorgaben des Volkszählungsurteils erfolgte die erste BDSG-Novelle, welche am 20.12.1990 als Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und der Datenschutzes verkündet wurde.[10]

Für den Problemkreis der Online-Geschäfte wichtige Änderungen der Novelle waren u. a. die neue Zielbestimmung des Datenschutzes in § 1 I BDSG, die Einbeziehung der Begriffe „Erheben“ (§ 3 IV BDSG), „Nutzen“ (§ 3 VI BDSG) und „Anonymisieren“ (§ 3 VII BDSG), die neue Definition des Datengeheimnisses (§ 5 BDSG), die verstärkte Zweckbindung (§ 14 I BDSG) und die Erweiterung der Straf- und Bußgeldvorschriften[11].

[8] BVerfG NJW 1988, 2031; BVerfG NJW 1991, 2411.

[9] *Simitis* in: *BDSG*, Simitis, § 1 BDSG, Rdnr. 34; für eine Aufzählung der „unterschiedlichen Facetten grundrechtlichen Schutzes“ siehe eingehend *Albers*, Informationelle Selbstbestimmung, S. 357 ff.

[10] BGBl. I 1990, 2954.

[11] Für eine vollständige Auflistung der geänderten Regelungen s. *Büllesbach*, Das neue Bundesdatenschutzgesetz, S. 2593.

## II. Europäisches Recht

### 1. Die EG/EU-Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Mit Inkrafttreten der EG/EU-Richtlinie 95/46/EG vom 24.10.1995[12] hatte der Gesetzgeber drei Jahre Zeit, das nationale Datenschutzrecht den Vorgaben dieser Norm anzupassen.

Da mit der Richtlinie keine eigene Konzeption des Datenschutzes realisiert wurde, diese vielmehr in ihren überwiegenden Teilen von einer Zusammenschau wesentlicher Grundgedanken bereits bestehender mitgliedsstaatlicher Regelungen geprägt war und Deutschland zum damaligen Zeitpunkt ohnehin hohe Datenschutzstandards besaß[13], waren durch die Richtlinie keine schwerwiegende Änderungen vonnöten. Umso verwunderlicher erschien es wohl, dass die Umsetzungsfrist wesentlich überschritten wurde, bis am 23.5.2001 die dritte und damit (bis auf einige unwesentliche Änderungen) aktuell geltende Fassung des BDSG in Kraft trat[14] .

Wichtigste Neuregelungen bei der zweiten Novelle waren die Erweiterung des Geltungsbereiches, eine erweiterte Transparenz gegenüber dem Betroffenen, erweiterte Verarbeitungsbeschränkungen und erweiterte Datenschutzkontrolle[15].

[12] ABl. 1995, L 281, S. 31 ff., im Folgenden: EG-Datenschutzrichtlinie.
[13] *Bachmeier*, EG-Datenschutzrichtlinie - Rechtliche Konsequenzen für die Datenschutzpraxis, S. 49.
[14] BGBl I. 2001, S. 904 ff. Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze.
[15] Zu den Änderungen im Einzelnen: *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 35 f. sowie *Tinnefeld*, Die Novellierung des BDSG im Zeichen des Gemeinschaftsrechts, 3078–3083.

## 2. Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

Nachdem zunächst am 15.12.1997 der Datenschutzrichtlinie die Telekommunikations-Datenschutzrichtlinie folgte[16], wurde diese von der Richtlinie 2002/58/EG (EK-DSRL[17] vom 12.7.2002) aufgehoben und ersetzt, da sie (so zu finden in (4) der Gründe) „an die Entwicklung der Märkte und Technologien für elektronische Kommunikationsdienste angepasst werden“ musste. Die Umsetzungsfrist für die EK-DSRL ist am 31.10.2003 abgelaufen, eine Umsetzung hat jedoch nur im Bereich der Telekommunikation stattgefunden. Eine Änderung für das Recht der Teledienste wird hier vor allem noch dem § 13 Abs. 1 S. 2 Telemediengesetz (TMG) widerfahren müssen, dessen Unterrichtungspflicht nur für die Fälle gilt, in denen „eine spätere Identifizierung des Nutzers [ermöglicht] und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten [vorbereitet wird].“ Artikel 5 Abs. 3 der Richtlinie sieht hingegen „klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung vor“, mit der einzigen Ausnahme, dass der „alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder [...] um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen“[18]. In der Neufassung des TKG[19] waren u.a. die Anpassung des Begriffes „Verbindungsdaten“ durch den Begriff der „Verkehrsdaten“ vorzunehmen[20]

[16] Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation; ABl.1998, L 24, S. 1ff.
[17] ABl. 2002, L 201, S. 37 ff.
[18] So dazu und zu den Neuerungen der Richtlinien im Allgemeinen: *Ohlenburg*, Die neue EU-Datenschutzrichtlinie 2002/58/EG - Auswirkungen und Neuerungen für elektronische Kommunikation, 82–86 und *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 195.
[19] BGBl I 2004, 1190.
[20] BR-Drs. 755/03, S. 124.

sowie die Neueinführung der Regelung zu den sogenannten „Standortdaten“[21] aufzunehmen.

### 3. Die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten

Am 14.03.2006 haben das Europäische Parlament und der Rat der Europäischen Union die Richtlinie über die Vorratsdatenspeicherung[22] erlassen. Die Umsetzungsfrist der Richtlinie endete am 15.09.2007, die Anwendung der Richtlinie auf die Speicherung von Kommunikationsdaten betreffend dem Internetzugang, der Internet-Telefonie und der Internet-E-Mail wurde jedoch von Deutschland mittels einer Erklärung im Sinne des Art. 15 Abs. 3 der Richtlinie bis zum 15.03.2009 aufgeschoben.

Nach Art. 3 Abs. 1 der Richtlinie müssen die Mitgliedsstaaten dafür Sorge tragen, dass in Zukunft u.a. die im Internet zugewiesenen Benutzerkennungen (Zugangs-Account, E-Mail-Account, Voice-Over-IP-Rufnummer), der Name, die Anschrift und die IP-Adresse des Nutzers, die Benutzerkennung des Empfängers, das Datum und die Uhrzeit der An- und Abmeldung beim Dienst, der in Anspruch genommene Dienst und die Rufnummer des anrufenden Anschlusses (bei Wählverbindung) bzw. der digitale Teilnehmeranschluss (bei DSL) für einen Zeitraum von mindestens sechs Monaten (Art. 6) auf Vorrat gespeichert werden. Zweck der Speicherung ist nach Art. 1 Abs. 1 der Richtlinie die Ermittlung, Feststellung und Verfolgung schwerer Straftaten.

Die Richtlinie hat vor allem bei Datenschützern, aber auch bei zahlreichen Verbänden, insbesondere auch bei juristischen Verbänden, Presseverbänden und Verbraucherverbänden[23] zu mehreren schweren Kritikpunkten geführt.

[21] A.a.O., S. 125.

[22] Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher Kommunikationsdienste oder öffentlicher Kommunikation erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. 2006, L 105, S. 54 ff.

[23] Siehe dazu die im Internet abzurufende „Gemeinsame Erklärung zum Gesetzesentwurf über die Vorratsdatenspeicherung“, die von 27 Verbänden, u.a. dem „Chaos Computer

Auf praktischer Ebene wird zum einen die Gefährdung der uneingeschränkten Kontaktaufnahme mit Beratungsstellen, Ärzten, Psychologen oder Seelsorgern genannt. Außerdem ist bei einer Registrierung aller Telekommunikationsdaten der Quellenschutz von Journalisten gefährdet[24]. So werden die gespeicherten Daten zwar rein zum Zwecke der Verfolgung schwerer Straftaten zur Verfügung gestellt, doch steht zu befürchten, dass sich Verbraucher allein aufgrund der Tatsache, dass ihre Kommunikation nicht mehr anonym verläuft, in der Kontaktaufnahme gehemmt fühlen.

Zum anderen wird die Frage der Kostenerstattung der Vorratsdatenspeicherung bei den Telekommunikationsunternehmen und Internetprovidern angeführt. Weder die Richtlinie noch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“[25] sehen eine Kompensation der Kosten vor. Laut Aussage des Bundesrats im Gesetzesentwurf wird der Mehraufwand, der zwischen einigen Tausend und mehreren Hunderttausend Euro betragen wird, von den Unternehmen in die Preisgestaltung einzukalkulieren und somit letztendlich vom Verbraucher zu tragen sein[26].

Auf rechtsdogmatischer Ebene wird hinsichtlich des nationalen Verfassungsrechts auf die Argumente der Bundesregierung zurückgegriffen, die bereits im Jahre 2002 dazu führten, eine Speicherpflicht für Telekommunikationsdaten einzuführen: Diese erfordere eine genaue Abwägung zwischen dem Fernmeldegeheimnis, *dem Grundrecht auf informationelle Selbstbestimmung*, dem Zweckbindungsgebot des Datenschutzes, der Grundsätze der Datenvermeidung und

Club“, der „Gesellschaft für Datenschutz und Datensicherung“, der „Deutschen Liga für Menschenrechte“ und dem „Verband Deutscher Zeitschriftenverleger“ unterzeichnet wurde, `http://erklaerung.vorratsdatenspeicherung.de`.

[24] Dieser, wie auch sämtliche weitere Kritikpunkte finden sich ausführlich erläutert auf der Webpage des Arbeitskreises Vorratsdatenspeicherung unter `http://www.vorratsdatenspeicherung.de`; *Sattler*, Bürger unter Generalverdacht, Nr. 51–52, 19.12.2005.

[25] BGBl. I 2007, S. 3198

[26] BR-Drs. 275/07, 7.

-sparsamkeit sowie der Verhältnismäßigkeit und der Grundrechte und schutzwürdigen Interessen der Diensteanbieter einerseits und Interessen der Sicherheitsbehörden andererseits[27]. Da es sich bei der Vorratsdatenspeicherung um eine heimliche Maßnahme handelt, von der fast jeder Mensch unmittelbar betroffen ist und es sich bei den gespeicherten Daten um solche handelt, die sich nicht im Herrschaftsbereich des jeweils Betroffenen befinden, ist eine hohe Eingriffsintensität gegeben[28]. Ferner erfolgt der Eingriff ohne konkrete Verdachtsmomente und stellt somit jeden Nutzer von Telekommunikationsmitteln unter Generalverdacht. Auf der anderen Seite sind laut Bundesverfassungsgericht schwerwiegende Eingriffen in das Fernmeldegeheimnis nur dann verhältnismäßig, wenn die Gegenbelange entsprechend gewichtig sind. Bei Strafverfolgungen ist das Gewicht des Interesses insbesondere von der Schwere und Bedeutung der aufzuklärenden Straftat abhängig und von dem hinreichenden Verdacht, dass Straftaten geplant oder begangen werden[29].

Die Richtlinie selbst definiert als Zweck der Vorratsdatenspeicherung lediglich die Ermittlung, Feststellung und Verfolgung von schweren Straftaten (Art. 1 Abs. 1 der RL) und überlässt die Entscheidung darüber, um welche Straftaten es sich dabei handelt, den Gesetzgebern. Ein hinreichender Verdacht für die Speicherung wird darüber hinaus nicht benötigt, da jeder Teilnehmer von der Speicherung betroffen ist. Laut Art. 4 der RL haben die Mitgliedstaaten lediglich Maßnahmen zu erlassen, die sicherstellen, dass die Vorratsdaten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden.

Auch bezüglich der Frage, ob die Richtlinie nicht gegen europäisches Vertragsrecht verstößt, bestanden Bedenken. So hatte am 6.7.2006 Irland gegen den Rat der Europäischen Union und das Europäische Parlament Klage vor

[27] *Leutheusser-Schnarrenberger*, ZRP 2007, 9–13.
[28] *Leutheusser-Schnarrenberger*, ZRP 2007, 9–13.
[29] BVerfGE 100, 313 [392].

dem EuGH erhoben[30], mit dem Antrag, die Richtlinie für nichtig zu erklären. Irland berief sich dabei darauf, dass die Wahl von Art. 95 EGV (Binnenmarktkompetenz) als Rechtsgrundlage für die Richtlinie nicht geeignet sei, da Zweck der Richtlinie nicht die Behebung von Mängeln des Binnenmarkts, sondern die Bekämpfung schwerer Verbrechen sei[31].

Aufgrund der geschilderten Kritikpunkte wurde dem Ausgang der Klage vor dem EuGH mit grosser Spannung entgegen gesehen und blieb zu hoffen, dass diese erfolgreich sein würde. Ein positiver Ausgang der Klage hätte insbesondere die Möglichkeit eröffnet, über sinnvolle Alternativen zur Vorratsdatenspeicherung nachzudenken[32]. Am 10.2.2009 hat der EuGH jedoch entschieden, dass die Richtlinie zu Recht aufgrund Art. 95 EGV erlassen wurde[33].

Die nationale Umsetzung erfolgte durch das soeben bereits genannte „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“[34]. Gegen einzelne Änderungen, die durch dieses Gesetz erfolgt sind, wurde Verfassungsbeschwerde eingelegt. Aufgrund der Beschwerde ist am 11.3.2008 eine einstweiligen Anordnung ergangen, die dazu führt, dass u.a. § 113b S. 1 Nr. 1

[30] Rechtssache C 301/06, ABl. 2009, C 82, S. 2f.

[31] Weitere, ausführliche Erläuterungen zur Diskussion finden sich bei *Westphal*, EuZW 2006, 555–560; *Leutheusser-Schnarrenberger*, ZRP 2007, 9–13; *Gola/Klug*, NJW 2007, 2599–2602; *Graulich*, NVwZ 2008, 485–492; *Brinkel/Lammers*, ZUM 2008, 11–22; .

[32] So z.B. das von der Artikel-29-Datenschutzgruppe vorgeschlagene „quick freeze“-Verfahren, bei dem sich die Strafverfolgungsbehörden in begründeten Fällen an die Unternehmen wenden und die Speicherung bestimmter Daten verlangen. Die Behörden haben dann mehrere Wochen Zeit zum Sammeln von Beweismitteln, um eine richterliche Anordnung zu erwirken; s. 1868/05/DE WP 113 „Stellungnahme 4/2005 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“; zum „quick freeze“-Verfahren s. auch *Westphal*, EuZW 2006, 555–560 *Gola/Klug*, NJW 2007, 2599–2602; *Graulich*, NVwZ 2008, 485–492; *Brinkel/Lammers*, ZUM 2008, 11–22; .

[33] MMR 2009, 244.

[34] Zu den Folgen der Umsetzung für die Privatwirtschaft siehe umfassend *Hoeren*, JZ 2008, 668–672.

TKG bis zur endgültigen Entscheidung nur eingeschränkt angewendet werden kann[35].

## III. Telekommunikation und Internetdatenschutzrecht (bereichsspezifische Regelungen)

Die durch den Fortschritt der Computertechnologie und des Internets neu geschaffenen technischen Möglichkeiten zur Datenerhebung führten zur Notwendigkeit, dem auch in speziellen Gesetzesregelungen Rechnung zu tragen.

Parallel zur Entwicklung des BDSG sind die für den Datenschutz relevanten §§ 85 ff. (und insbesondere § 89) TKG daher erstmalig am 01.08.1996 in Kraft getreten[36]. In Folge der Umsetzung der Richtlinien 2002/19/EG, 2002/20/EG, 2002/21/EG, 2002/22/EG[37], 2002/58/EG[38] wurde das TKG umfassend novelliert und ist in seiner nunmehr geltenden Form am 26.06.2004 in Kraft getreten[39]. Umfangreiche Änderungen im Datenschutzrecht fanden sich einerseits durch die Umsetzung der EK-DSRL in Teil 7 Abschnitt 2 und 3 TKG. So war § 89 TKG a.F. und die parallel geltende TDSV weggefallen und wurde das Datenschutzrecht in den §§ 91 – 107 TKG geregelt[40]. Weitere Änderungen ergaben sich durch die Umsetzung der Richtlinie über die Vorratsdatenspeicherung[41].

[35] BVerfG, 1 BvR 256/08, welche zuletzt am 22.4.2009 um weitere sechs Monate verlängert wurde.
[36] BGBl I 1996, 1120.
[37] Alle vier ABl. 2002, L 108, S. 7 ff.
[38] Siehe Abschnitt C.II.2. auf Seite 53.
[39] BGBl. I 2004, 1190.
[40] Zu den einzelnen Neuerungen siehe *Anna Ohlenburg*, MMR 2004, S. 431 und unter Abschnitt C.II.2. auf Seite 53.
[41] Siehe dazu das bereits genannte Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, welche u.a. die Einführung der §§ 113a und 113b zur Folge hatte. Zu den Folgen für die Praxis siehe *Redeker*, ITRB 2009, 112–113.

## 1. Das Telemediengesetz

Für den Bereich der Internetdaten traten zunächst der Mediendienste-Staatsvertrag (MDStV[42]) und das TDDSG[43] (im Rahmen des IuKDG[44]) am 1.8.1997 in Kraft. Sowohl der MDStV als auch das TDDSG wurden inzwischen jedoch durch das am 1.3.2007 inkraftgetretene Telemediengesetz (TMG[45].) ersetzt. Ziel des Gesetzes war dabei grundsätzlich nicht eine inhaltliche Änderung, sondern die Regelung bestimmter rechtlicher Anforderungen für Telemedien[46]. Für den Bereich des Datenschutzes wurde weitgehend an den Regelungen des TDDSG und des MDStV beibehalten. Das TMG beseitigt aber die Abgrenzungsschwierigkeiten[47] zwischen Telediensten, die früher unter das TDDSG und der Mediendienste, die unter den MDStV fielen[48]. Dennoch hat der Gesetzgeber die Chance für eine grundsätzliche Reform des Internet-Datenschutzes vertan[49]. Eine Präzisierung fand lediglich hinsichtlich der Verwendung von Daten statt. Hier schreibt § 12 Abs. 2 TMG nunmehr vor, dass eine Verwendung für andere Zwecke nur dann zulässig ist, soweit das TMG oder eine andere Rechtsvorschrift, *die sich ausdrücklich auf Telemedien bezieht*[50], es erlaubt oder der Nutzer eingewilligt hat. Neu im TMG ist auch, dass der Diens-

[42] BayGVBl 1997, S. 226.
[43] BGBl I 1997, 1870.
[44] Informations- und Kommunikationsdienste-Gesetz.
[45] BGBl I 2007, 179.
[46] BT-Drs. 16/3078, 11.
[47] Siehe dazu *Roßnagel*, Neues Recht für Multimediadienste, Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag, 1–8; *Gounalakis*, Der Mediendienste-Staatsvertrag der Länder, 2993–3000; *Gounalakis/Rhode*, Elektronische Kommunikationsangebote zwischen Telediensten, Mediendiensten und Rundfunk,Äö, 487–492; *Brunner* in: *Manssen, Gerrit*, Telekommunikations- und Multimediarecht, E § 3 Rdnr. 10; *Kröger/Moos*, Mediendienst oder Teledienst?, 675–680; *Spindler* in: *Roßnagel*, Recht der Multimedia-Dienste, § 2 TDG, Rdnr. 79.
[48] Eine Abgrenzung dahingehend, ob ein Telemediendienst ein journalistisch-redaktionelles Angebot beinhaltet, ist aber nach wie vor für die Frage relevant, ob über die Regelungen des TMG hinaus noch die §§ 54ff. TMG anwendbar sind, siehe dazu unter C.III.3.
[49] *Hoeren*, Das Telemediengesetz, 801–806.
[50] Dieser Zusatz fehlte im § 3 Abs. 2 TDDSG.

teanbieter im Einzelfall Auskunft nicht wie bisher nur zum Zwecke der Strafverfolgung, sondern auch dann erteilen darf, wenn es zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist. Diese Änderung dient der Sicherstellung des Anspruchs nach Art. 8 der EU-Enforcement-Richtlinie[51], welcher ein Auskunftsrecht in Verfahren wegen Verletzung eines Rechts des geistigen Eigentums vorsieht. Festzuhalten gilt hier jedoch, dass ein Auskunftsrecht in der Richtlinie von einer Anordnung des zuständigen Gerichts abhängt. Der Gesetzgeber hat es jedoch versäumt, klar zu definieren, wer die von § 14 Abs. 2 TMG erfassten zuständigen Stellen sind. In der Literatur wird daher befürchtet, dass § 14 Abs. 2 TMG dazu führen wird, dass Host-Provider, Auktionshäuser, Forenbetreiber usw. in Zukunft Daten für private und öffentliche Zwecke sammeln und somit Nutzer auf Rechtsbrüche ausspionieren[52]. Zu beachten wäre hier aber, dass nach dem Erforderlichkeitsgrundsatz ein Recht zur Speicherung der Bestandsdaten nur so lange besteht, wie es für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich ist (§ 14 Abs. 1 TMG). § 14 Abs. 2 TMG würde daher häufig ins Leere laufen, da die entsprechenden Daten zum Zeitpunkt der Anordnung schon gelöscht werden. Es ist allerdings zu vermuten, dass diese zeitliche Grenze den wenigsten Diensteanbietern bekannt sein dürfte, so dass im Ergebnis die Regelung des § 14 Abs. 2 TMG wegen der Ungenauigkeit hinsichtlich der zuständigen Stellen als missglückt bezeichnet werden kann. Leider hat der Gesetzgeber auch die Änderung der Urheber-, Patent- und Markengesetze infolge der EU-Enforcement-Richtlinie[53] nicht zum Anlass genommen, eine Nachbesserung der Vorschrift vorzunehmen[54].

[51] Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums, ABl. L 195, S. 16).

[52] *Hoeren*, Das Telemediengesetz, 801–806.

[53] Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, BGBl I 2008, 1191.

[54] Zur Auskunft der Diensteanbieter nach § 14 Abs. 2 TMG siehe auch *Moos*, K&R 2008, 137–145.

## 2. Abgrenzung Telekommunikation von Telemediendiensten

Ein weiteres Ziel des TMG war die Klärung des Verhältnisses der Datenschutzvorschriften des TMG zu denjenigen des TKG[55]. Da sowohl das TKG als auch das TMG datenschutzrechtliche Vorschriften enthalten, die bei der Nutzung des Internets allesamt berührt sein können, müssen deren Regelungsbereiche, um eine rechtliche Würdigung bei etwaigen Verstößen durchführen zu können, klar abgegrenzt werden. Auch schließt das TMG in seinem Geltungsbereich die Telekommunikationsdienste ausdrücklich aus, vgl. § 1 TMG.

So muss vor allem bei umfassenden Internetprodukten, in denen es zu einer Vermengung von Telekommunikationsdiensten und Telemediendienste kommt, jedes Dienstmerkmal dem jeweiligen Gesetz zugeordnet werden. Anderer Ansicht ist hier Waldenberger[56], welcher vertritt, dass die Aufspaltung des Gesamtspektrums eines Internet-Angebots in seine einzelnen Merkmale zu in der Praxis untragbaren Konsequenzen führen würde. Laut Waldenberger müsse eine Einordnung des gesamten Internetproduktes daher in das Gesetz stattfinden, in dem der Schwerpunkt der angebotenen Dienste anzusiedeln ist. Hierzu ist zu bemerken, dass die Aufspaltung in der Praxis zwar tatsächlich zu nicht unerheblichen Problemen führt, eine konsequente Anwendung des TKG und des TMG jedoch für eine „wertende Gesamtschau“ eines aus mehreren Dienstmerkmalen bestehenden Internetangebots wenig Spielraum lässt.

In der Literatur wird die funktionelle Aufteilung der einzelnen Merkmale wie im Folgenden darzustellen ist, daher zutreffend als nur begrenzt möglich bezeichnet[57]. Soweit es um die Trennung der Telekommunikation von Telemediendiensten geht, empfiehlt sich zur plastischen Veranschaulichung der Frage,

[55] BT-Drs. 16/3078, 12.

[56] *Waldenberger*, MMR 1998, 124–129; wobei dieser sich nur auf Medien- und Teledienste, nicht aber auch auf Telekommunikationsdienste bezieht, was im Ergebnis jedoch nichts ändert, siehe auch die Kritik von *Wittern/Schuster* in: *Büchner*, Beck'scher TKG-Kommentar, § 3 TKG, Rdnr. 49.

[57] *Kröger/Gimmy*, Handbuch zum Internet-Recht, S. 510.

welcher Bereich durch das jeweilige Dienstmerkmal betroffen ist, wohl am ehesten eine Abgrenzung der Bereiche Telekommunikation und Telemediendienst in zwei verschiedene Stufen:

Die Telekommunikation nach dem TKG stellt dabei die unterste und somit grundlegende Stufe dar. Das TKG selbst definiert in § 3 Nr. 22 „Telekommunikation" als technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen und in Nr. 24 „Telekommunikationsdienste" als in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen.

So ist das Bestehen der Telekommunikation stets Voraussetzung für die Erbringung von Telemediendiensten, die auf der zweiten, darüber liegenden Stufe angeboten werden.

Auf das Internet bezogen werden reine Telekommunikationsdienstleistungen von Network-Providern zur Verfügung gestellt, welche lediglich das Leistungsnetz zur Verfügung stellen, also weder Inhalte präsentieren, noch den Netzzugang ermöglichen[58]. Wie schwierig die Abgrenzung sich in der Praxis erweist, zeigt jedoch schon die kontroverse Diskussion[59] um die Einordnung der Access-Provider. Diese ermöglichen mittels Zurverfügungsstellung mehrerer Server, zu denen eine physikalische Verbindung aufgebaut wird, u.a. die Vergabe einer IP-Adresse, das Routing und den DNS-Service, welche der Nutzer für den Zugang

[58] *Brunner* in: *Manssen, Gerrit*, Telekommunikations- und Multimediarecht, R § 3 Rdnr. 7.

[59] In der Literatur wird daher häufig ohne weiteres Eingehen auf die technischen Vorgänge der Access-Provider unter das frühere TDG (jetzt TMG) subsumiert, so z.B. *Brunner* in: *Manssen, Gerrit*, Telekommunikations- und Multimediarecht, R § 3 Rdnr. 7, wobei insoweit unschlüssig erscheint, dass Brunner die Betreiber von Router-Rechnern wiederum ausnehmen will. Hier scheint die technische Funktionsweise des Wortes „Router" verkannt zu werden. Router verbinden einzelne Netze zu einem Internet (vgl. *Meinel/Sack*, WWW, S. 479) und sind somit Teil des Access-Providings, welche das Bestehen einer IP-Adresse voraussetzen; *Mairgünther, Markus*, Die Regulierung von Inhalten in den Diensten des Internet, S. 25 und *Waldenberger* in: *Roßnagel*, Recht der Multimedia-Dienste, § 3 TDG, Rdnr. 25; kritisch dagegen *Wittern/Schuster* in: *Büchner*, Beck'scher TKG-Kommentar, § 3 TKG, Rdnr. 49.

in das Internet benötigt. Technisch betrachtet fällt alles, was zur rein physikalischen Verbindung zählt, unter die Definition des § 3 Nr. 22 TKG und ist daher als Telekommunikation einzuordnen.

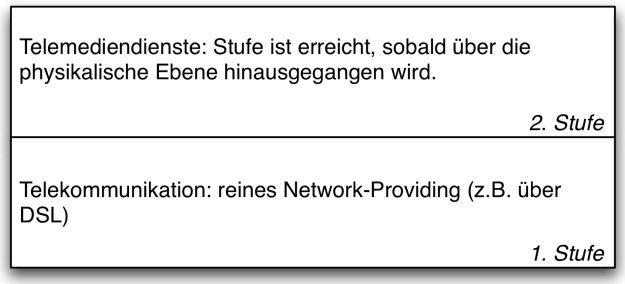


Abbildung 3.1: Unterscheidung zwischen Telekommunikation und Telemediendiensten

Der Gesetzgeber hat dieses Problem zwar bei der Begründung zum Telemediengesetz erkannt, als Lösung aber eine „Kombination“ aus Telekommunikationsdienst und Telemediendienst eingeführt. Danach sind Telekommunikationsdienste, die *überwiegend* in der Übertragung von Signalen über Telekommunikationsnetze bestehen sowohl Telekommunikationsdienste als auch Telemediendienste. Unter diese Mischform soll auch das Access-Providing fallen[60]. Die Folge dieser Einordnung sei dann, dass für Access-Provider die Vorschriften des TMG hinsichtlich des Herkunftslandsprinzips, der Zugangsfreiheit und der Haftungsprivilegierung gelte, die Vorschriften zum Datenschutz sich hingegen überwiegend aus dem TKG ergeben (§ 11 Abs. 3 TMG).

Durch diese Lösung hat der Gesetzgeber die Diskussion um die Einordnung der Access-Provider beendet, eine saubere funktionelle Trennung ist ihm aber freilich nicht gelungen. Die praktischen Schwierigkeiten für die Diensteanbieter bestehen fort. Sie sehen sich nach wie vor zwei verschiedenen Gesetzen gegenübergestellt und müssen von Fall zu Fall entscheiden, welches Gesetz gerade anwendbar ist.

[60] BT-Drs. 16/3078, S. 13;, wo auch die E-Mail-Dienste genannt werden.

Probleme in der Abgrenzung bestehen auch weiterhin, sobald die physikalische Ebene verlassen wird und die Vergabe der IP-Adresse beginnt. Gemäß § 2 S. 1 Nr. 1 TMG ist Diensteanbieter nicht nur derjenige, der Telemedien zur Nutzung bereithält, sondern auch derjenige, der den Zugang zur Nutzung vermittelt. Die Vergabe einer IP-Adresse wäre somit als Vermittlung zur weiteren Internetnutzung bereits ein Telemediendienst. Die Bundesregierung ist im Rahmen ihres Berichtes „über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des IuKDG“ auf das Problem insofern eingegangen, als sie die Vergabe von IP-Adressen nicht als Dienstleistung zur reinen Datenübertragung, sondern als „ein spezifisches Diensteangebot des Providers zur Nutzung von Informations- und Kommunikationsangeboten im Internet und anderen Netzen“ qualifiziert hat[61]. Wird dieser Aussage gefolgt, ist die Vergabe der IP-Adresse als Teledienst einzuordnen (Abbildung 3.1 auf der vorherigen Seite), obwohl das in Hinblick auf den rein computertechnischen Vorgang nicht einleuchtend ist:

Die IP-Adresse ist aus technischer Sicht nichts anderes als eine Telefonnummer oder eine Postadresse[62]. Warum die Zugangsvermittlung ausgerechnet an der Stelle beginnen soll und damit der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen verlassen werden soll, an dem eigentlich immer noch die Voraussetzungen für eben diesen Vorgang geschaffen werden (ohne IP-Adresse ist keine Kommunikation im Internet möglich), ist dogmatisch bisher nicht sauber dargelegt worden.

Eine deutlich bessere Lösung wäre es gewesen, die funktionelle Zuordnung auch hier durchgreifen zu lassen und die IP-Adresse folglich noch in den Bereich der Kommunikation einzuordnen. Die Inhalte, die von IP-Adresse zu IP-Adresse übermittelt werden, sind hingegen Telemediendienste[63].

[61] BT-Drs. 14/1191, S. 7f.
[62] Zur technischen Funktionsweise der IP-Adresse siehe unter Abschnitt B.I.2. auf Seite 8.
[63] So auch *Schmitz* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, Kapitel 16.4, Rdnr. 41.

Sind die rein technischen Voraussetzungen für den Zugang jedoch geschaffen und wird das Internet dann beispielsweise zum Surfen genutzt, begibt sich der Nutzer ohne Zweifel auf die Ebene der Telemediendienste.

Trotzdem bleibt in konkreten Einzelfällen eine Einteilung der anfallenden Daten auf die verschiedenen Dienste meist schwierig, wenn eine beinahe Verschmelzung zwischen Telekommunikation und Telemediendiensten stattfindet[64], wie z.B. das Instant-Messaging und der IRC (Internet Relay Chat). Allerdings wird in diesen Fällen aufgrund der komplexeren Anforderung an die Dienstleistung der Schwerpunkt häufig bei den Telemediendiensten liegen[65].

Bei E-Mail-Diensten ist demzufolge der reine Vorgang des Versendens eine Telekommunikationsdienstleistung, während das Zwischenspeichern oder das automatische Überprüfen einer E-Mail auf Viren von Seiten des Providers einen Telemediendienst darstellt[66].

Für die Voice-over-IP-Telefonie hat der Gesetzgeber klargestellt, dass es sich dabei um einen Telekommunikationsdienst handelt[67].

### 3. Telemediendienste mit journalistisch-redaktionellen Angeboten

Obwohl das TMG die Abgrenzungskriterien zwischen Tele- und Mediendiensten beseitigt, weil es nunmehr sowohl die früheren Tele- als auch die Mediendienste regelt, bleibt auch nach Inkraftreten des TMG die Frage zu beantworten, ob ein Telemediendienst ein journalistisch-redaktionelles Angebot enthält.

Dieses frühere Hauptunterscheidungskriterium zwischen Tele- und Mediendiensten ist nämlich entscheidend dafür, ob über die Vorschriften des TMG hinaus auch die §§ 54 ff. RStV zu beachten sind. Für den Datenschutz ist dabei § 57 RStV relevant, der den Datenschutz bei journalistisch-redaktionellen

[64] *Kröger/Gimmy*, Handbuch zum Internet-Recht, S. 510.
[65] *Roßnagel* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, S. 133.
[66] Zur Abgrenzung siehe auch *Oster* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, 4.B Rdnr. 18.
[67] BT-Drs. 16/3078, S. 13.

Zwecken regelt. Unter redaktioneller Gestaltung wird das Sammeln und Aufbereiten von verschiedenen Informationen oder Meinungen (mittels inhaltlicher, sprachlicher, graphischen oder akustischen Bearbeitung[68]) mit Blick auf den potentiellen Empfänger, wobei diesem nach der redaktionellen Gestaltung ein einheitliches Produkt übermittelt wird[69], verstanden. Ist die Grenze einer individuellen Meinungsäußerung überschritten, dient ein Telemediendienst zur Meinungsbildung für die Allgemeinheit.

Für diesen Fall beinhalten die §§ 54 ff. RStV über den Datenschutz[70] hinaus auch besondere Regelungen zu den allgemeinen Informationspflichten (§ 55 RStV), der Gegendarstellung (§ 56 RStV), der Werbung und dem Sponsoring (§ 58 RStV) sowie der Aufsicht durch Kontrollbehörden (§ 59 RStV)[71].

### 4. BDSG und Internetdatenschutzrecht

Das TMG hat zwar die Abgrenzungsprobleme zwischen Medien- und Telediensten behoben und einen Versuch der klareren Abgrenzung zwischen Telekommunikations- und Telemediendiensten unternommen, diejenige zwischen TMG und BDSG bleibt aber weiterhin unklar[72]. Die Dienstleister sehen sich weiterhin zwei unterschiedlichen Regelwerken gegenübergestellt, ohne eindeutige Kriterien vorliegen zu haben, welches Gesetz zu welchem Zeitpunkt anwendbar ist. Das führt zumindest für die Diensteanbieter zu einer Rechtsunsicherheit, die durch die Schaffung abstrakter Abgrenzungskriterien ausgeräumt werden könnte.

[68] *Gounalakis/Rhode*, Elektronische Kommunikationsangebote zwischen Telediensten, Mediendiensten und Rundfunk,Äö, 487–492.
[69] *Spindler* in: *Roßnagel*, Recht der Multimedia-Dienste, § 2 TDG Rdnr. 31.
[70] Zum Auskunftsanspruch nach § 57 Abs. 2 RStV siehe noch unter E.III.3.
[71] Zu Telemediendiensten mit meinungsbildender Funktion siehe auch *Schmitz*, Übersicht über die Neuregelung des TMG und des RStV, 135–138 und *Spindler*, Das neue Telemediengesetz - Konvergenz in sachten Schritten, 239–245.
[72] *Hoeren*, Das Telemediengesetz, 801–806.

Bei der Klärung des Verhältnisses zwischen BDSG und Internetdatenschutzrecht, müssen zunächst zwei verschiedene Fallkonstellationen berücksichtigt werden:

Zum einen enthält das BDSG über den Internetdatenschutz hinausgehende Regelungen, die bei der Beurteilung der datenschutzrechtlichen Zusammenhänge von Telemediendiensten stets subsidiär zu berücksichtigen sind, § 12 Abs. 4 TMG. Daher ist das BDSG vor allem hinsichtlich der Begriffsbestimmungen, für bestimmte Betroffenenrechte oder Vorschriften über die Datenschutzkontrolle anzuwenden[73].

Zum anderen bleibt das BDSG in den Fällen anwendbar, in denen zwar eine Erhebung oder Verarbeitung von Daten im Internet stattfindet, diese aber außerhalb des Regelungsgehalts des TMG liegt. Das TMG gilt gemäß § 12 Abs. 1 TMG nur für personenbezogene Daten zur *Bereitstellung von Telemedien*. Der Wortlaut impliziert dabei die Notwendigkeit des Vorliegens eines Anbieter-Nutzer-Verhältnisses. Davon nicht gedeckt sind daher diejenigen Daten, bei denen der Internetdienst lediglich das Übertragungsmedium ist, um Dienstleistungen für den Vertragspartner oder Kunden in elektronischer Form erbringen zu können[74]. Dies wird im TMG in § 11 Abs. 1 Nr. 2 TMG noch präzisiert, wonach das TMG nicht für die Bereitstellung solcher Dienste gilt, die ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

Die Anwendbarkeit des TMG ist also stets dann nicht mehr gegeben, wenn das Anbieter-Nutzer-Verhältnis endet und das Kunde-Dienstleistungsverhältnis beginnt. Es genügt gerade nicht, dass z.B. ein Kauf-, Miet- oder Werkvertrag online abgeschlossen wird, der auf dieselbe Weise auch ohne die Zuhilfenahme des Internets hätte entstehen müssen. Der Grund für die Beschränkung liegt darin, dass der Bedarf in den Genuss des erweiterten Schutzes der bereichsspezifischen Regelungen zu gelangen, in den Fällen nicht bestehen soll, in denen

[73] *Scholz*, Datenschutz beim Internet-Einkauf, S. 116.
[74] *Schulz* in: *Roßnagel*, Recht der Multimedia-Dienste, § 1 TDDSG, Rdnr. 43.

von den Verträgen kein höheres persönlichkeitsrechtliches Gefährungspotenzial ausgeht[75].

Die Unterscheidung zwischen Nutzungsdaten[76] auf der einen Seite und Inhaltsdaten auf der anderen Seite führt jedoch gerade im Bereich des Online-Handels zu nicht unerheblichen Schwierigkeiten, da die Daten, die zunächst für die reine Nutzung des Teledienstes erhoben wurden, häufig für den darauf folgenden Kaufvertrag weitergenutzt werden. Die Übergänge zwischen Nutzung und Inhalt der Nutzung sind dabei meist fließend. Auch die Risiken bleiben auf der Inhaltsebene dieselben. Die Möglichkeiten, die Daten durch das Medium Internet zu erheben, werden nicht etwa dadurch eingeschränkt, dass das Verhältnis zwischen Nutzer und Anbieter von der Teledienstebene auf das Verhältnis Kunde-Anbieter der Vertragsebene übergegangen ist. Wird der Vertrag online abgeschlossen, besteht vielmehr auch weiterhin die Möglichkeit, Daten des Kunden versteckt mitzuloggen oder Cookies abzulegen und damit eine Koppelung von Daten herzustellen, wie sie gerade nicht möglich gewesen wäre, wenn der Vertrag offline abgeschlossen worden wäre[77].

Die Telemedienebene ist nicht die einzige Ebene, auf der die technischen Vorgänge stattfinden[78], die zu einem höheren Gefährdungspotential führen. Es ist vielmehr darauf abzustellen, wem die Erhebung, Verarbeitung oder Nutzung dient[79]. So können datenschutzrechtliche Vorgänge, die elektronisch ausgeführt

[75] So z.B. *Scholz*, Datenschutz beim Internet-Einkauf, S. 160.

[76] Zu den Nutzungsdaten siehe noch unter D.VI.1.

[77] A.A. *Scholz*, Datenschutz beim Internet-Einkauf, S. 160, welcher in den Verträgen, die über das Internet abgeschlossen werden, kein größeres Gefährdungspotenzial sieht, da die Gefährdungslage sich „aus den unabhängig vom eigentlichen Vertragsschluss bestehenden Möglichkeiten zur Datengewinnung und -auswertung“ ergibt. Diese Ansicht verkennt aber, dass der Kunde sich in diese Gefährdungslage aber gerade nur deshalb begibt, weil er den Vertrag über das Internet abschließt, die Möglichkeiten also zwar unabhängig vom Vertragschluss bestehen, durch selbigen aber gerade geschaffen werden.

[78] So jedoch *Selk*, Datenschutz und Internet, S. 23.

[79] *Schulz* in: *Roßnagel*, Recht der Multimedia-Dienste, § 1 TDDSG, Rdnr. 43, wobei dieser heranziehen will, ob die spezifischen Risiken der Online-Kommunikation von Bedeutung sind, was im Hinblick auf vorangegangene Ausführungen als widersprüchlich erscheint, da es durchaus sein kann, dass sich ein Anbieter im Bereich der Inhalte missbräuchlich

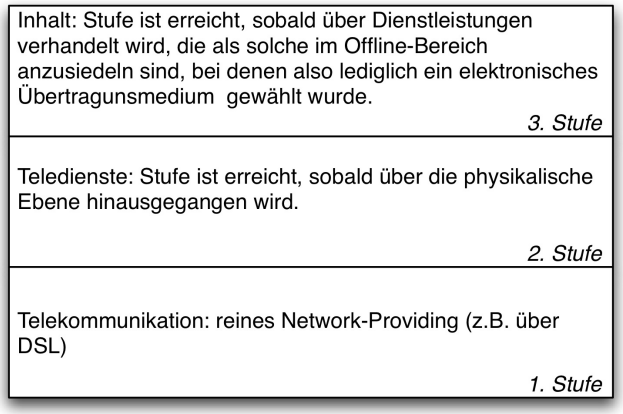


Abbildung 3.2: Unterscheidung zwischen Telekommunikation, Telediensten und Inhalt.

werden, zum einem dem Nutzer dienen und somit dem TMG zuzuordnen sein. Zum anderen können sich Inhaltsdaten im E-Commerce aber auch in der Hülle des elektronischen Übertragungsmediums befinden und als solche selbst elektronisch sein. Sind aber Inhaltsdaten selbst elektronisch, realisiert sich in ihnen gerade das Gefährdungspotenzial, vor dem die bereichsspezifischen Regelungen zum Datenschutz den Betroffenen bewahren wollen.

Gleichwohl bleibt es bei der Anwendbarkeit des BDSG, sobald die Ebene der Nutzungsdaten verlassen und die der Inhaltsdaten betreten wird, da der Gesetzeswortlaut eindeutig ist. Spätestens bei der Einführung des TMG war dem Gesetzgeber die Problematik bekannt[80]. Es wäre daher an ihm gewesen, Wertungswidersprüche zu verhindern[81].

des elektronischen Mediums bedient, was wohl kaum der Durchführung eines Telemediendienstes gelten kann.

[80] Ausführungen zu den verschiedenen Ansichten zur Auslegungsproblematik vor Einführung des TMG finden sich z.B. bei *Schmitz* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, Kapitel 16.4, Rdnr. 140 ff.

[81] Kritik am Festhalten an der Beschränkung auf das Anbieter-Nutzer-Verhältnis findet sich unter *Jandt*, Das neue TMG - Nachbesserungsbedarf für den Datenschutz im Mehrpersonenverhältnis, 652–657.

Es ergibt sich hinsichtlich des Dreiergespanns Telekommunikation, Telemedienste und Inhalt im Ergebnis eine dreistufige Abgrenzung (Abbildung 3.2 auf der vorherigen Seite).

## IV. Geplante Gesetzesänderungen

Sowohl zum BDSG als auch zum TMG befinden sich derzeit Änderungsentwürfe im Gesetzgebungsverfahren. Beim BDSG handelt es sich zum einen um den „Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes“[82] und zum anderen um den „Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“[83]. Im Rahmen dieser Arbeit relevante Änderungen ergeben sich hierbei einerseits durch das zukünftige Erfordernis der Einwilligung in die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung (§ 28 Abs. 3 iVm 3a BDSG-E). Hier sieht das BDSG bisher nur das Widerspruchsrecht nach § 28 Abs. 4 S. 1 BDSG vor[84]. Andererseits soll nunmehr auch ins BDSG ein allgemeines Koppelungsverbot eingeführt werden (§ 28 Abs. 3b BDSG-E). Änderungen im TMG würden sich aus dem „Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen“[85] und dem „Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes “[86] ergeben. Da letztgenannte Entwürfe zwar grundsätzlich datenschutzrechtliche Relevanz besitzen, aber kei-

[82] BT-Drs. 16/13219.

[83] BT-Drs. 16/12011; siehe auch die Kritik am Entwurf von *Hoeren*, bank und markt 2008, 32–34 sowie *Weichert*, DuD 2009, 7–18, welcher anmerkt, dass neben den geplanten Reformen auch eine Überarbeitung der Regelungen zur Verarbeitung personenbezogener Daten im Internet überfällig ist. Zu den geplanten Änderungen und insbesondere kritisch zur Abschaffung des Listenprivilegs siehe weiterführend auch *Breinlinger*, RDV 2008, 223–227; *Bierekoven*, ITRB 2009, 39–41; *Hoeren*, RDV 2009, 89–95; *Eckhardt*, CR 2009, 337–344; *Moos*, K&R 2009, 154–161; *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 368–375.

[84] Siehe dazu unter Abschnitt E.II.1.e) auf Seite 100.

[85] BT-Drs. 16/12850.

[86] BT-Drs. 16/11967, s. dazu *Köcher*, MMR 2009, V.

ne direkten Berührungspunkte zur Thema der vorliegenden Arbeit aufweisen, seien sie an dieser Stelle nur der Vollständigkeit halber genannt. Eine relevante Änderung würde hingegen die Umsetzung des „Telemedienänderungsgesetzes“ [87] mit sich führen, welches bei der Informationspflicht nach § 13 Abs. 1 TMG in Zukunft auch die Pflicht zur Information über die Länge der Speicherung der Daten vorsieht.

[87] BT-Drs. 16/11173.

# D. Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Internet

Obwohl im Verlauf dieser Arbeit oftmals zur sprachlichen Vereinfachung nur von der Erhebung personenbezogener Daten die Rede ist, sei an dieser Stelle betont, dass das Datenschutzrecht zwischen den Phasen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterscheidet. Die zur Erhebung stattfindenden Ausführungen hinsichtlich der Informationspflichten und der Zulässigkeit im nicht-öffentlichen Bereich, auf den sich diese Arbeit beschränkt, gelten jedoch gleicherweise für die Tatbestände der Verarbeitung und der Nutzung. Besonderheiten ergeben sich lediglich bei der Verarbeitung bezüglich der Frage, ob sie für eigene Zwecke, zum Zwecke der Übermittlung oder zum Zwecke der Übermittlung in anonymisierter Form stattfindet (§§ 28 ff. BDSG)[1]. Um die verschiedenen Phasen des Umgangs mit personenbezogenen Daten im Verlauf der weiteren Abhandlung dem Anwendungsbereich des BDSG oder der bereichsspezifischen Regelungen rechtlich zuordnen zu können, sei dessen ungeachtet kurz auf den begrifflichen Unterschied zwischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten eingegangen:

## I. Phasen der Datenverarbeitung

### 1. Erhebung

Ob die Erhebung einen Teil der Verarbeitung oder eine Vorstufe derselbigen darstellt, wurde vom deutschen Gesetzgeber anders umgesetzt, als von der

[1] Vgl. *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 1 BDSG, Rdnr. 15.

EG-Datenschutzrichtlinie vorgegeben. Während nach Art. 2 Buchst. b der EG-Datenschutzrichtlinie das Erheben von Daten in die Definition der Verarbeitung eingereiht wird, zählt zur Erhebung nach § 3 Abs. 3 BDSG die Beschaffung der Daten, während die Verarbeitung der Daten erst mit der Speicherung beginnt (Abs. 4). Im Ergebnis entsteht hier zwar ein Widerspruch, der bei er Umsetzung der Richtlinie hätte Berücksichtigung finden müssen, letztlich ergeben sich jedoch insofern keine Probleme, weil die Erhebung durch die Novellierung des BDSG 2001 der Verarbeitung im Schutze gleich gestellt wurde, so dass im Schutz der personenbezogenen Daten dadurch keine Lücken entstehen[2].

Erhebung im Sinne des § 3 Abs. 3 BDSG ist also nach deutschem Recht das finale zielgerichtete Beschaffen von Daten als „Vorstadium“ für das Speichern, wobei die Phase des Erhebens sich auf den Dateneingang in den Herrschaftsbereich der verantwortlichen Stelle bezieht[3]. Aus dem ersten Teil der Definition ergibt sich, dass eine rein zufällige Kenntnisnahme zur Annahme einer Erhebung nicht ausreichend ist. Der zweite Teil der Definition hat einen vergleichbaren Regelungsgehalt wie der Zugang von Willenserklärungen gegenüber Abwesenden gemäß § 130 I Satz 1 BGB[4]. Danach ist für eine Datenerhebung eine tatsächliche Kenntnisnahme auch hier nicht nötig, sie ist bereits gegeben, wenn der Kunde eines Online-Shops die Registrierung seines Accounts mit vollständigem Namen und Adresse fertig ausgefüllt und an den Server des Verkäufers gesendet hat.

Das Genügen dieser abstrakten Kenntnisnahmemöglichkeit ist vergleichbar mit dem Zugang von Willenserklärungen per E-Mail: Handelt es sich beim Empfänger der E-Mail um einen geschäftlichen Internet-Nutzer, der seine E-

[2] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 3 BDSG, Rdnr. 60.
[3] *Schaffland/Wiltfang*, BDSG, § 3 BDSG, Rdnr. 105
[4] Eine unter Abwesenden abgegebene Willenserklärung zugegangen, sobald sie derart in den Machtbereich des Empfängers gelangt, dass bei Annahme gewöhnlicher Verhältnisses damit zu rechnen ist, er *könne* davon Kenntnis erlangen; vgl. *Einsele* in: *Rebmann/-Säcker/Rixecker*, MüKo, § 130, Rdnr. 18ff.; *Heinrichs* in: *Palandt*, BGB, § 130, Rdnr. 5.

Mailadresse im Geschäftsverkehr bekannt gibt, stellt sein elektronischer Briefkasten eine mit einem Hausbriefkasten vergleichbare Empfangsvorrichtung dar. Den geschäftlichen Internet-Nutzer trifft dann eine Nachforschungsobliegenheit, welche zum Zugang der E-Mail spätestens am Tag nach Eintreffen der Nachricht führt[5].

### 2. Verarbeitung

Als Verarbeitung werden fünf verschiedene Vorgänge bezeichnet: Das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten. Die für das Internet relevantesten Vorgänge sind dabei das Speichern und das Übermitteln.

#### a) Speichern

Speichern ist nach der Legaldefinition des § 3 Abs. 4 Nr. 1 BDSG das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Ein Datenträger kann dabei jedes Medium sein, das geeignet ist, Daten aufzunehmen[6], im Internet üblicherweise die Festplatte eines Servers. Der Zweck der weiteren Verarbeitung oder Nutzung wird im Internet in aller Regel erfüllt sein. Der Gesetzgeber wollte mit der Angabe dieses Tatbestandsmerkmals lediglich klarstellen, dass die Daten zumindest für eine gewisse Dauer aufbewahrt werden müssen und nicht lediglich aufgenommen, verarbeitet und dann wieder gelöscht werden[7].

[5] Zum Zugang von Willenserklärungen im Internet siehe *Ultsch*, Zugangsprobleme bei elektronischen Willenserklärungen - Dargestellt am Beispiel der Electronic Mail, 3007–3009.

[6] *Schaffland/Wiltfang*, BDSG, § 3 BDSG, Rdnr. 24.

[7] BT-Drs. 7/1027, S. 23; nach *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 299, wäre dies zum Beispiel bei Gelegenheitskunden, bei denen keine Stammdaten angelegt werden, die Daten vielmehr nur auftragsbezogen erfasst und danach sofort wieder gelöscht werden, nicht der Fall. Bei Online-Shops ist es jedoch gebräuchlich, dass der Nutzer die Kundendaten bei der ersten Bestellung übermittelt und diese auf Dauer mit dem Account verknüpft bleiben. In den wenigstens Fällen werden sie gleich nach Ausführung der Bestellung gelöscht werden.

Im Bezug auf die Speicherung von Daten im Internet ist noch erwähnenswert, dass in den Fällen, in denen ein Content Provider sich der Dienste eines Host Service Providers bedient, um beispielsweise seine Kundendatenbank auf dessen Server abzulegen, zwei Akteure beteiligt sind: Während der Content Provider die Speicherung veranlasst, wird sie durch den Host Service Provider technisch vollzogen, wodurch ein Fall der Auftragdatenverarbeitung im Sinne des § 11 BDSG gegeben ist[8].

### b) Übermittlung

Von der Auftragdatenverarbeitung zu unterscheiden ist das Übermitteln von Daten. Eine Übermittlung liegt nach der Legaldefinition nämlich nur dann vor, wenn personenbezogene Daten entweder durch Weitergabe oder durch Einsichtnahme oder Abruf einem Dritten bekanntgegeben werden. Da im Rahmen von § 3 Abs. 8 S. 3 BDSG bestimmt ist, dass Auftragnehmer im Inland und EWR-Ausland keine Dritte sind, stellt die Weitergabe von Daten im Falle einer Auftragdatenverhältnisses keine Übermittlung dar. Einen Sonderfall, mit der Folge, dass ausnahmsweise doch eine Übermittlung vorliegt, ist nur gegeben, wenn der Auftragnehmer nicht im EU-Binnenmarkt tätig ist[9]. Dies ist zum Beispiel denkbar, wenn ein Unternehmen seine Daten auf einem Backup-Server sichert, der einem Unternehmen angehört, das sich ausserhalb der Grenzen des EU-Binnenmarkts befindet. Liegt eine Übermittlung aus dem Grund nicht vor, dass eine Bekanntgabe an einen Dritten nicht erfolgt ist, da sich die Weitergabe etwa lediglich innerhalb der verantwortlichen Stelle ereignet hat, ist gleichwohl stets an den Tatbestand der Nutzung zu denken[10].

[8] *Schaar*, Datenschutz im Internet, S. 69.
[9] So auch *Schaffland/Wiltfang*, BDSG, § 3 BDSG, Rdnr. 88, während diese aus dem Gesetz folgende logische Konsequenz in *Schaar*, Datenschutz im Internet, S. 70 und *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 3 BDSG, Rdnr. 98, keinerlei Erwähnung findet.
[10] Siehe dazu sogleich.

Der Vorgang der Übermittlung kann nach dem Gesetzeswortlaut auf aktive Weise im Rahmen einer Weitergabe stattfinden, wobei die Form der Bekanntgabe nicht relevant ist[11]. Daraus ergibt sich auf das Internet bezogen, dass es unerheblich ist, ob eine Übermittlung durch das Versenden einer Datei, welche personenbezogene Daten enthält - beispielsweise durch das Uploaden mittels FTP oder eines Instant Messaging Systems - geschieht oder durch das Verschicken personenbezogener Inhalte innerhalb einer E-Mail-Nachricht bzw. eines Attachements[12].

Ablehnend hat sich der EuGH hingegen zu einer Übermittlung in bloß passiver Weise in den Fällen geäußert, in denen die Daten lediglich zur Einsicht oder zum Abruf bereitgehalten werden wie es insbesondere bei der Veröffentlichung von Webseiten im Internet gegeben ist. Insofern hatte das BVerfG zunächst festgehalten, dass eine öffentliche Bekanntmachung, die eine Form der Veröffentlichung darstellt, eine Datenübermittlung „auf Vorrat“ verkörpert, durch die der Betroffene besonders gefährdet ist, da weder „vorhersehbar noch bestimmbar“ ist, „wer von diesen Daten Kenntnis erlangen wird und wie diese Daten verwendet werden können“[13]. Der EuGH hat diese Ansicht in der Lindqvist-Entscheidung jedoch klar verneint[14].

### 3. Nutzung

Findet keine Verarbeitung der Daten statt, so könnte dessen ungeachtet immer noch der Tatbestand der Nutzung erfüllt sein: Nach § 3 Abs. 5 BDSG ist Nutzen jede Verwendung von Daten, so weit es sich nicht um Verarbeitung handelt. Der Gesetzgeber wollte mit diesem umfangreichen Auffangtatbestand[15] den Schutzbereich des BDSG ausdrücklich auch für die Fälle des Gebrauchs

[11] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 3 BDSG, Rdnr. 91.
[12] Vgl. *Wohlgemuth, Hans H.*, Datenschutzrecht, S. 39.
[13] BVerfG, NVwZ 1990, 1162; so auch noch *Schaar*, Datenschutz im Internet, S. 71.
[14] Rechtssache C 101/01, ABl. 2004, C 7, S. 3f.
[15] Vgl. auch OLG Köln, MMR 2001, S. 386.

von Daten ausdehnen, welche sich nicht im Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten manifestieren[16]. Entscheidend für das Vorliegen einer Nutzung ist, dass die Verwendung sich auch auf den Personenbezug erstreckt. Dies ist für die Fälle zu verneinen, in denen eine Auswertung eines Weblogs lediglich statistischen Zwecken dient[17], um z.B. festzustellen, aus welchen Ländern, anteilig betrachtet, Zugriffe erfolgen. Bei der Auswertung einer Kundendatenbank, durch die im Wege des „Data-Minings“[18] Erkenntnisse über das Kaufverhalten der Nutzer eines Online-Shops erhalten werden, ist die Verwendung des Informationsgehalts personenbezogener Daten und somit eine Nutzung hingegen gegeben.

## II. Personenbezogene Daten

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist nur dann eröffnet, wenn es sich bei den fraglichen Daten um solche mit Personenbezug handelt. Personenbezogene Daten sind ihrer Legaldefinition des § 3 Abs. 1 BDSG nach „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“[19]. Da das TKG und das TMG keine eigene Definition kennen, ist auch bei diesen Normen die Definition des BDSG anzuwenden[20].

[16] BT-Drs. 11/4306, S. 40f.

[17] *Schaar*, Datenschutz im Internet, S. 73.

[18] Vgl. *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 3 BDSG, Rdnr. 125.

[19] Auf europäischer Ebene siehe aber auch die Stellungnahmen der Art.-29-Datenschutzgruppe „4/2007 zum Begriff der personenbezogenen Daten und zu Datenschutzfragen im Zusammenhang mit Suchmaschinen“ vom 20. Juni 2007 (01248/07/DE WP 136) sowie „1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation)“ vom 10. Februar 2009 (00350/09/DE WP 159).

[20] Vgl. § 12 Abs. 4 TMG; im TKG findet sich hingegen keine diesbezügliche Regelung, doch ist auch hier der Grundsatz der Subsidiarität anzuwenden.

Soll nun, ausgehend von der Definition des BDSG und der in dieser festgelegten Voraussetzungen, ein Vergleich zwischen Online- und Offline-Kommunikation gezogen werden, so ergibt sich, dass der entscheidende Unterschied zwischen den beiden Kommunikationsarten in der Bestimmbarkeit der von der Erhebung betroffenen Person liegt. Bestimmbar ist eine Person mithin immer dann, wenn sie durch die Daten nicht eindeutig identifiziert, jedoch durch entsprechendes Zusatzwissen festgestellt werden kann[21].

Während somit die ausgetauschten „Einzelangaben über persönliche oder sachliche Verhältnisse“ unabhängig von der gewählten Kommunikationsart nahezu gleich bleiben, weiss der Betroffene wenn er sich ausschließlich der Offline-Kommunikation bedient, in aller Regel, wann die bei ihm erhobenen Daten bestimmbar auf ihn zurückzuführen sind. Etwas anderes ergibt sich hingegen, wenn er im Internet kommuniziert und die Daten nicht willentlich durch ihn herausgegeben, sondern durch ein automatisiertes Verfahren erhoben werden.[22]

Umgekehrt kann nicht jeder Eintrag einer Logdatei oder jeder Inhalt eines Cookies im Nachhinein mit einer Person in Verbindung gebracht werden. Personenbezogene Daten fallen hier nur dann an, wenn z.B. eine Logdatei oder der Inhalt eines Cookies durch entsprechendes Zusatzwissen Rückschlüsse ermöglicht, die die Person des Nutzers eindeutig identifizieren. Das ist nur dann der Fall, wenn sich der Benutzer auf einer Webseite zur Nutzung der Dienste zuvor mit seinem Namen und seiner Wohnanschrift registrieren musste, ihm daraufhin ein Loginname zugeteilt wurde, welcher bei jeder darauf folgenden Anmeldung des Nutzers auf der Webseite in der Logdatei gespeichert wird. Hier existiert für den Benutzer ein Datensatz, welcher sowohl den Loginnamen als auch den Namen und die Wohnanschrift des Nutzers enthält. Für den Anbieter

[21] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 280.

[22] So auch *Roßnagel* in: *Roßnagel*, Handbuch Datenschutzrecht, 7.9 Rdnr. 3 ff; das Problem hat auch der Gesetzgeber gesehen, weshalb er im Rahmen des IuKDG die Ausweitung des Datenschutzes in Richtung der Gewährleistung einer anonymen und pseudonymen Nutzung und damit weg von der personenbezogenen Nutzung vollzogen hat, siehe BT/Drs. 14/1191, S. 13.

des Dienstes ist ein Rückschluss immer möglich[23], selbst wenn es sich bei dem Loginnamen um einen frei wählbaren Fantasienamen handelt. Differenzierter zu betrachten sind die Möglichkeiten der Zuordnung hingegen bei E-Mail- und IP-Adressen[24].

## III. Personenbezug im Zusammenhang mit E-Mail-Adressen

Eine E-Mail-Adresse wird dem Internetnutzer heutzutage als Arbeitnehmer vom Arbeitgeber, als Kunde eines Internet Service Providers (ISP)[25] oder eines E-Mail-Providers zugewiesen. Ein Inhaber einer Domain nebst E-Mail-Server kann sie sich darüber hinaus auch selbst einrichten. Abhängig davon, welche der Möglichkeiten in Anspruch genommen wird, ist die Wahl dessen, was der Nutzer als sog. *local-part* einer E-Mail-Adresse erhalten möchte, mehr oder weniger gross. Eine E-Mail-Adresse ist stets auf folgende Art und Weise aufgebaut: *local-part@domain*[26]. Wird die E-Mail-Adresse durch den Arbeitgeber zugeteilt, lautet diese demnach meist *vorname.nachname@firmenname.de*. Anders verhält es sich dagegen bei ISPs und Mail-Providern, bei denen zwischen

[23] Diese Vorgehensweise wird häufig bei kommerziellen Chat- oder Online-Dating-Systemen verwendet, da auf diese Weise der Nutzer gegenüber den anderen Nutzern die Möglichkeit hat, seine wahre Identität hinter dem Loginnamen zu verbergen. Die Loginnamen werden von den Nutzern solcher Systeme daher auch häufig Pseudonyme oder Pseudos genannt, was sogar mit der datenschutzrechtlichen Einordnung insofern übereinstimmt, als von Pseudonymisierung im Datenschutz dann die Rede ist, wenn die Daten durch eine Zuordnungsvorschrift derart verändert werden, dass die Einzelangaben ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden kann (*Gola/Schomerus*, BDSG, § 3 Rdnr. 45 ff.; zu Pseudonymen siehe sogleich unter Abschnitt D.VI.1.b) auf Seite 89). Es darf dabei jedoch nicht übersehen werden, dass die Betreiber der Systeme jederzeit die Möglichkeit haben, den Personenbezug wieder herzustellen.

[24] Zum Personenbezug von Daten im Internet s. auch *Härting*, CR 2008, 742–748.

[25] Zur Unterscheidung zwischen Access Provider und Service Provider s. *Marcus Hofer*, datenschutz@internet, S. 27 f.

[26] Zu den vorgegebenen Standards des Aufbaus einer E-Mail-Adresse siehe RFC 2822 (Internet Message Format).

den noch nicht vergebenen *local-parts* die freie Auswahl besteht. Hier könnte die Emailadresse auch *fantasiename@foo.de* lauten. Daraus ergibt sich, dass die E-Mail-Adresse nicht per se ein personenbezogenes Datum ist, sondern nur, wenn der Inhaber durch die E-Mail-Adresse identifizierbar ist[27]. Entspricht die E-Mail-Adresse dem Vor- und Nachnamen, ist immer von einem personenbezogenen Datum auszugehen, besteht sie hingegen aus einem Fantasienamen, dann ist das nur der Fall, wenn sie beispielsweise über ein öffentlich zugängliches Verzeichnis[28] mit dem Namen des Inhabers in Verbindung gebracht werden kann. Anders verhält es sich beim Provider der E-Mail-Adressen: Da dieser dem Nutzer eine E-Mail in aller Regel nur dann vermittelt, wenn dieser ihm seinen Namen und seine Postanschrift übermittelt, stellt die E-Mail-Adresse für den Provider in diesen Fällen immer ein personenbezogenes Datum dar.

## IV. Personenbezug im Zusammenhang mit IP-Adressen

Bei der Frage, ob es sich bei IP-Adressen um personenbezogene Daten handelt, ist zunächst zwischen statischen und dynamischen IP-Adressen zu unterscheiden[29]:

### 1. Statische IP-Adresse

Eine statische IP-Adresse ist einem Rechner fest zugewiesen, so dass bei jeder TCP/IP-Kommunikation, die von diesem Rechner ausgeht, grundsätzlich eindeutig identifizierbar ist, dass die Kommunikation von ihm ausging. Ausnah-

[27] So auch *Schmitz* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, 16.4, Rdnr. 56; undifferenziert immer von einem personenbezogenen Datum gehen hingegen *Engels/Eimterbäumer*, Sammeln und Nutzen von E-Mail-Adressen zu Werbezwecken, 196–200 und *Ihde*, Cookies - Datenschutz als Rahmenbedingung der Internetökonomie, 413–423 aus.

[28] Wie z.B. `http://people.yahoo.com/`.

[29] Zur Beschreibung des technischen Unterschiedes zwischen dynamischer und statischer IP-Adresse siehe oben unter Abschnitt B.I.2. auf Seite 8.

men bildet hier die oben beschriebene Zuweisung einer statischen IP-Adresse mittels NAT[30] oder die Verwendung eines Proxy-Cache-Servers[31]. In ersterem Fall ist anhand der IP-Adresse zwar innerhalb des Firmennetzes erkennbar, von welchem Rechner die Kommunikation stattfand, nach aussen hin kommuniziert der Rechner aber immer nur mit der IP-Adresse des Routers, so dass vom Internet aus allenfalls erkennbar ist, innerhalb welcher Firma die Kommunikation stattfand. Im zweiten Fall ist die statische IP-Adresse nur für den Betreiber des Proxy-Cache-Servers sichtbar, darüber hinaus wird die IP-Adresse des Proxy-Cache-Servers weiter ins Internet vermittelt.

Weiterhin ist zu beachten, dass die statische IP-Adresse zwar stets einem Rechner zugewiesen ist, dieser Rechner aber durchaus von verschiedenen Personen in Betrieb genommen werden kann, so dass in diesen Fällen zwar ein Bezug auf einen Personkreis, nicht aber auf eine Person mittels der IP-Adresse hergestellt werden kann. Da aber spätestens durch Art. 2 Buchst. a der EG-Datenschutzrichtlinie als personenbezogene Daten auch solche einbezogen werden müssen, welche eine auch nur indirekte Identifikation einer Person mittels einer Kennummer ermöglichen, sind statische IP-Adressen zumindest immer dann als personenbezogene Daten einzuordnen[32], wenn der Betreiber die Verknüpfung zwischen Nutzer und Rechner herstellen kann, weil er entweder weiss, dass nur eine Person den Rechner nutzt oder welche Person des Personenkreises zu einem bestimmten Zeitpunkt den Rechner nutzt[33].

[30] Siehe unter Abschnitt B.I.2.b) auf Seite 11.

[31] Siehe unter Abschnitt B.II.2. auf Seite 28.

[32] So auch *Helfrich* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, 16.1 Rdnr. 31; *Jasmin Merati-Kashani*, Der Datenschutz im E-Commerce, S. 166 f.

[33] Diese Differenzierung trifft auch *Bestmann*, Und wer muss zahlen?, 496–502, wohingegen von oben genannten Autoren der Personenbezug stets angenommen wird. Das ist dogmatisch jedoch nicht vertretbar, da in den Fällen, wo ein Bezug nur zu einer Personengruppe hergestellt werden kann, gerade keine Einzelangabe im Sinne des § 3 I BDSG vorliegt, vgl. *Gola/Schomerus*, BDSG, § 3 Rdnr. 3. Eine Identifizierung einer Person innerhalb der Gruppe könnte etwa durch das zusätzliche Mitloggen des Loginnamens innerhalb eines Netzwerkes von Seiten des Administrators stattfinden.

## 2. Dynamische IP-Adresse

Im Gegensatz zu den statischen IP-Adressen ändert sich die dynamische IP-Adresse jedes Mal, wenn eine neue Verbindung mit dem Access-Provider oder dem firmeninternen DHCP-Server stattfindet[34]. Ein Personenbezug zu einer dynamischen IP-Adresse kann daher nur vom Access-Provider bzw. Netzwerkadministrator oder in den Fällen, in denen der Nutzer, beispielsweise aufgrund eines Bestellvorgangs, entsprechende Zusatzangaben macht, hergestellt werden[35]. Zu erwähnen ist jedoch an dieser Stelle, dass der Betreiber eines Internetdienstes sich beim Speichern der IP-Adressen seiner Nutzer nie sicher sein kann, dass diese sein Angebot nur unter Verwendung dynamischer IP-Adressen in Anspruch nehmen. Besteht aber die Möglichkeit, dass nur einer von ihnen mittels einer IP-Adresse kommuniziert, die es beispielsweise durch die Verwendung von *whois* ermöglicht, ihn eindeutig zu identifizieren, ist das Risiko eines Verstoßes gegen das Datenschutzrecht immer gegeben[36].

## 3. IP-Adressen und die *whois*-Abfrage

Das whois-Prokoll entstand ursprünglich aus dem Gedanken, ein Verzeichnis mit Informationen über registrierte Domainnamen herstellen zu wollen[37]. Heutzutage besteht die Möglichkeit, über die IP-Adresse eine *whois*-Abfrage zu starten. Daraus ergeben sich über die bloße Angabe, welche IP-Adress-Bereich welchem Domainnamen zugewiesen ist, weitaus umfangreichere Informationen.

[34] Zur technischen Funktionsweise siehe unter Abschnitt B.I.2.a) auf Seite 10.

[35] So auch *Meyer*, Cookies & Co. - Datenschutz und Wettbewerbsrecht, 1028–1035; gegen dynamische IP-Adressen als personenbezogene Daten siehe auch AG München, K&R 2008, 767.

[36] a.A. *Meyerdierks*, MMR 2009, 8–13, der generell einen Personenbezug von IP-Adressen in Serverlogs ablehnt; die Frage, ob dynamische IP-Adressen personenbezogen sind, ist nach wie vor strittig. Weiterführend siehe dazu u.a.: *Engels/Jürgens/Kleinschmidt*, K&R 2008, 65 – 77; *Pahlen-Brandt*, K&R 2008, 288–290; *Härting*, ITRB 2009, 35–39; *Backu*, ITRB 2009, 88–91; *Voigt*, MMR 2009, 377–382.

[37] Siehe RFC 3912 (WHOIS Protocol Specification).

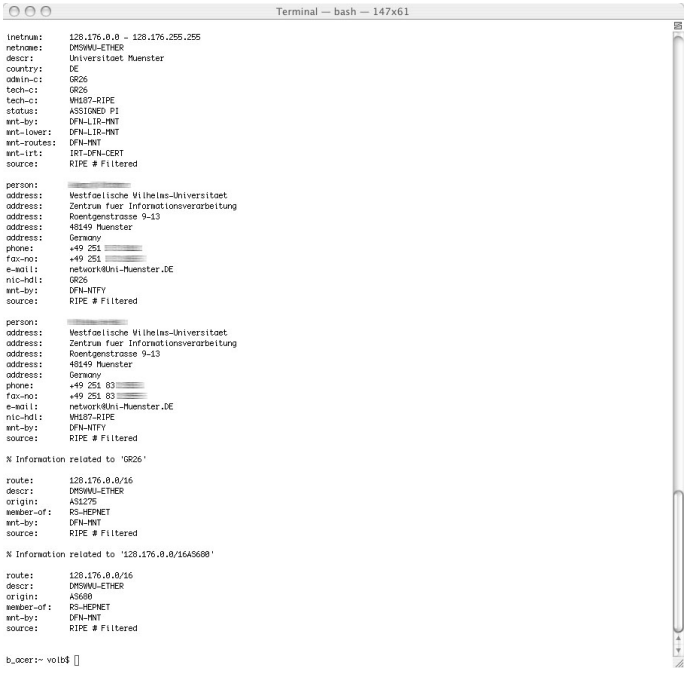


Abbildung 4.1: Ergebnis einer whois-Abfrage

Wird in die Konsole eines Computers der Befehl *whois 213.165.64.215* eingegeben, liefert das Ergebnis nicht nur, dass diese IP-Adresse der Westfälischen Wilhelms-Universität zugewiesen ist, sondern auch deren Adresse sowie die Namen des technischen und administrativen Ansprechpartners (Abbildung 4.1). Bei einer Privatperson entsprechen diese Angaben häufig dessen Namen sowie dessen Privatadresse. Abgesehen von der Tatsache, dass *whois*-Datenbanken als solche datenschutzrechtlich durchaus diskutabel[38] sind, stellen sie ein gutes Beispiel dafür da, wie schnell der Personenbezug bei einer Vielzahl von IP-Adressen hergestellt werden kann und warum ein Mitloggen derselbigen nie ohne Einwilligung des Nutzers stattfinden sollte.

[38] Siehe dazu *Roessler*, WHOIS: Datenschutz im DNS?, 666–671.

# V. Personenbezug im Zusammenhang mit Cookies

Wie bereits dargestellt[39], entsteht allein durch die Verwendung von Cookies nicht schon per se ein datenschutzrechtliches Risiko. Deswegen wird folgerichtig vertreten, dass die Frage nach der datenschutzrechtlichen Zulässigkeit von Cookies als solche bereits im Ansatz neben der Sache liegt[40]. Es ist zwar richtig, dass durch die technischen Möglichkeiten, die Cookies eröffnen, also im Gegensatz zum zustandslosen HTTP-Protokoll eine andauernde, bidirektionale Verknüpfung zwischen Server und Client herzustellen, Datenschutzverstöße begünstigt werden. Dagegen ist ein Cookie nicht schon aus dem Grund als personenbezogen einzustufen, weil bei dessen Übertragung auch die IP-Adresse übersandt wird[41]. Diese ist vielmehr Voraussetzung jeder Internet-Kommunikation, da ohne die IP-Adresse ein Server nicht wüsste, wohin er die angeforderten Datenpäckchen schicken soll. Datenschutzrechtlich relevant wird die Übersendung im Zusammenhang mit Cookies erst dann, wenn die IP-Adresse in einer Logdatei zusammen mit dem personenbezogenen Inhalt eines Cookies abgespeichert und auf diese Weise die Bestimmbarkeit des Nutzers hergestellt wird oder die Speicherung der IP-Adresse im Cookie die Identifikation des Nutzers ermöglicht. Richtig muss die Fragestellung daher lauten, ob der Inhalt eines Cookies

[39] Siehe unter Abschnitt B.II.1.c) auf Seite 18.

[40] *Jens Fröhle*, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 102.

[41] So jedoch anscheinend *Jasmin Merati-Kashani*, Der Datenschutz im E-Commerce, S. 170; nicht zu überzeugen vermag ihre Kritik dahingehend, dass bei der Reduzierung der Frage, ob ein Cookie als solches personenbezogen ist auf dessen Dateninhalt, die eigentlichen Fähigkeiten des Cookies außer acht gelassen werden. Es muss im Gegenteil gerade zwischen den Möglichkeiten, die datenschutzrechtlich betrachtet durch die Verwendung von Cookies erst eröffnet werden und der sich daraus ergebenden Frage, ob diese im konkreten Fall auch tatsächlich dazu genutzt wurden, personenbezogene Inhalte im Cookie zu erheben, getrennt werden. Nur weil der Inhalt des Cookies personenbezogen ist, bedeutet das bei weitem nicht, dass das Cookie an sich, welches nichts anderes darstellt als eine Textdatei, ebenfalls personenbezogen ist, ebenso wenig wie jedes Jagdgewehr eine Tatwaffe ist, nur weil es auch dazu benutzen werden kann, Straftaten zu begehen.

ein personenbezogenes Datum darstellt. Diese beantwortet sich aber ebenso wie in allen anderen Fällen allein aus der Definition des § 3 BDSG[42].

Ist der Inhalt des Cookies personenbezogen, stellt das Setzen des Cookies ein Speichern durch den Betreiber beim Nutzer dar. Daran ändert die Tatsache, dass das Cookie auf der Festplatte des Nutzers abgelegt ist, der Betreiber also nur eine Möglichkeit hat, den Inhalt abzufragen, wenn zwischen dem Computer des Nutzers und seinem Server eine Verbindung besteht, nichts. Der Nutzer hat zwar die Möglichkeit, das Setzen von Cookies im Browser zu deaktivieren, ist das Cookie jedoch gesetzt, hat er davon offensichtlich keinen Gebrauch gemacht. Ebenso wenig daran ändert die Verfügungsgewalt des Nutzers dahingehend, ein bereits gesetztes Cookie im Nachhinein zu löschen, da das Speichern in den Fällen zwar für die Zukunft, nicht aber für die Vergangenheit rückgängig gemacht werden kann[43]. Ferner ist zu beachten, dass es sich bei Cookies um ein automatisiertes Verfahren zur Datenerhebung handelt, weshalb der Nutzer zu Beginn nach § 13 Abs. 1 Satz 2 TMG zu unterrichten ist[44]. Diese Unterrichtungspflicht besteht auch dann, wenn der Personenbezug zwar nicht von Anfang an, aber zu einem späteren Zeitpunkt hergestellt werden kann. Ein solcher Fall kann etwa dann vorliegen, wenn ein Nutzer einen Online-Store zunächst besucht, um sich verschiedene Waren anzusehen und sich anschließend anmeldet, um eine der Waren zu bestellen. Der Betreiber hat daraufhin die

[42] Das Fehlen des Personenbezuges führt dazu, dass das Datenschutzrecht nicht einschlägig ist. Es kann sich für den Nutzer aber dennoch ein verschuldensunabhängiger Beseitigungs- und Unterlassungsanspruch aus § 862 Abs. 1 BGB ergeben, vgl. *Hoeren*, DuD 1998, 455–456.

[43] Der Ansicht, dass das Setzen eine Vorbereitung zur eigentlichen Erhebung ist, wird hier nicht gefolgt (so z.B. *Engel-Flechsig/Maennel/Tettenborn*, Das neue Informations- und Kommunikationsdienste-Gesetz, S. 2981–2990.). Das Setzen ist vielmehr einer dezentralen Speicherung auf der Rechner eines Dritten (also dem Nutzer) gleichzustellen, die ihrerseits eine Vorstufe zur Verarbeitung, dem späteren Abruf und somit eine Erhebung im Sinne des § 3 Abs. 2 BDSG darstellt, vgl. *Gola/Schomerus*, BDSG, § 3, Rdnr. 24. Der Ort der Speicherung ist wiederum dann unerheblich, wenn die verantwortliche Stelle über die Daten verfügen und sie ohne Schwierigkeiten wiedergewinnen kann (*Roßnagel* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, S. 170).

[44] Siehe dazu unter Abschnitt E.II.2.b) auf Seite 104.

Möglichkeit, das zunächst ohne Personenbezug gesetzte Cookie, welches eine Liste der bisher angesehenen Waren beinhaltet, mit den persönlichen Daten, die bei der Bestellung übermittelt werden, zusammenzuführen[45]. Nachdem der Nutzer über die Erhebung unterrichtet worden ist, ist das Setzen eines Cookies mit Personenbezug nur zulässig, wenn der Nutzer darin eingewilligt hat, § 12 Abs. 1 TMG. Die Einwilligung muss auch dann eingeholt werden, wenn die zunächst nicht direkt personenbezogenen Daten personalisiert werden sollen[46]. Daraus folgt, dass Unterrichtung und Einwilligung zeitlich auseinanderfallen können. Sicherlich nicht ausreichend für eine Einwilligung ist es, wenn der Browser des Nutzers so konfiguriert ist, dass er Cookies immer akzeptiert. Zum einem sind die meisten Browser standardmäßig so konfiguriert, zum anderen liegt in diesem Fall gerade keine informierte Einwilligung vor, welche sich immer nur auf den Einzelfall beziehen kann[47].

Einer Einwilligung bedarf es jedoch dann nicht, wenn es sich bei den erhobenen, verwendeten oder genutzten Daten um einen Datentypus handelt, für den im TMG oder dem TKG ein eigener Erlaubnistatbestand besteht. Um einen besseren Überblick zu gewinnen, unter welchen Voraussetzungen eine Einwilligung entbehrlich ist, soll nun im Folgenden eine Auflistung der verschiedenen Datentypen und der damit zusammenhängenden Erlaubnistatbestände erfolgen.

## VI. Datentypen

Die bei der Nutzung des Internet entstehenden personenbezogenen Daten teilen sich in Nutzungs-, Bestands-, Verkehrs- oder Inhaltsdaten auf.

[45] Siehe dazu schon oben unter Abschnitt B.II.1.c)aa) auf Seite 22 und bei *Eichler*, Cookies - verbotene Früchte?, 76–81.

[46] *Schaar*, Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, 275–277.

[47] *Banzhaf* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, S. 274.

## 1. Nutzungsdaten

Nutzungsdaten sind nach der Legaldefinition der § 15 Abs. 1 S. 1 TMG Daten, „die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen“. Satz 2 enthält eine katalogartige Aufzählung der Regelbeispiele. Nach dieser Definition sind Nutzungsdaten im Internet regelmäßig die IP-Adresse, die Informationen zur Anwendungsschicht (also, ob beispielsweise eine Kommunikation mittels ssh oder telnet gewünscht wird), technische Angaben wie der Browsertyp oder die gewünschte Sprache sowie der Inhalt personenbezogener Cookies[48].

Zu beachten ist an dieser Stelle, dass die Verarbeitung von Nutzungsdaten wesentlich strengeren Anforderungen unterliegt als die des BDSG. Nutzungsdaten dürfen nur dann erhoben, verarbeitet und genutzt werden, wenn dies für die Inanspruchnahme unmittelbar *erforderlich* ist. Das bedeutet zum einem, dass keine über die Erforderlichkeit hinausgehenden Daten erhoben, verarbeitet und genutzt werden dürfen, zum anderen aber auch, dass die erhobenen Daten für keine anderen Zwecke verwendet werden dürfen. Insofern stellt der § 15 Abs. 1 TMG eine spezialgesetzliche Regelung zu § 28 BDSG dar, welcher z. B. auch die Verwendung von Daten für Zwecke der Markt- und Meinungsforschung erlaubt.

### a) Nutzungsprofile

Die Erstellung von Nutzungsprofilen für Zwecke der Werbung, der Marktforschung und der bedarfsgerechten Nutzung ist hingegen im Rahmen des § 15 Abs. 3 TMG erlaubt, wenn sie unter der Verwendung von Pseudonymen geschieht. Voraussetzung dafür ist jedoch, wie sich aus der gesetzlichen Einord-

[48] Siehe dazu auch: *Zscherpe*, Datenschutzrechtliche Website-Kontrollen durch die Aufsichtsbehörde, XVII–XVIII; *Dix/Schaar* in: *Roßnagel*, Recht der Multimedia-Dienste, § 6 TDDSG Rdnr. 86; *Schaar*, Datenschutz im Internet, Rdnr. 426.

nung ergibt, dass diese sich ausschließlich aus Nutzungsdaten zusammensetzen. Ferner müssen die Nutzungsdaten ihrerseits rechtmäßig erhoben worden sein[49].

### b) Verwendung von Pseudonymen

Eine Erstellung von Nutzungsprofilen muss unter Verwendung von Pseudonymen geschehen. Das TMG selbst definiert den Begriff des Pseudonymisierens nicht, so dass auf die allgemeine Definition des § 3 Abs. 6a BDSG zurückzugreifen ist, wonach Pseudonymisieren „das Ersetzen des Namens und anderer Identifikationsmerkmale zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren ist“. Im Rahmen der Pseudonymisierung werden die Daten daher durch eine Zuordnungsvorschrift derart verändert, dass die Einzelangaben ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können[50]. In diesem Zusammenhang besteht Uneinigkeit[51] darüber, ob die bloße Möglichkeit, durch die Zuordnungsvorschrift einen Personenbezug herstellen zu können bereits genügt, Pseudonyme als personenbezogene Daten einzuordnen, was zur Folge hätte, dass die datenschutzrechtlichen Regelungen im vollen Umfang auch auf diese anwendbar sind.

Für eine Personenbezogenheit von Pseudonymen spricht einer Ansicht nach, dass das TMG, welches dem Schutz personenbezogener Daten dient, auch Vorschriften über den Umgang mit Pseudonymen enthält. Daraus solle resultieren, dass der Gesetzgeber der Auffassung ist, dass Daten, die unter Pseud-

[49] So auch *Schaar*, Persönlichkeitsprofile im Internet, 383–388 und *Jens Fröhle*, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 182 f. mit detaillierten Ausführungen, warum die zulässige Primärverarbeitung ungeschriebene Voraussetzung ist. Zur datenschutzrechtlichen Einordnung von Nutzungsprofilen siehe weiterführend außerdem: *Bauer*, MMR 2008, 435–438; *Schleipfer*, RDV 2008, 143–150.

[50] *Gola/Schomerus*, BDSG, § 3 BDSG, Rdnr. 46.

[51] Siehe *Bizer* in: *BDSG*, Simitis, § 3 BDSG, Rdnr. 217; a.A. *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität - Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, 721–731, m.w.N.

onym gespeichert sind, einen Personenbezug aufweisen[52]. Außerdem spreche der Gesetzgeber in der Begründung zum TDDSG auch nur vom pseudonymen Handeln als quasi-anonymes Handeln, bei dem über eine Referenzliste beim Diensteanbieter die Identität des Nutzers zusammengeführt werden können[53]. Der Gesetzgeber sähe also dadurch einen Personenbezug bei unter Pseudonym gespeicherten Daten zumindest als möglich an[54]. Überdies soll schon allein die drohende Gefahr einer nachträglichen Identifizierung ausreichen, um einen Personenbezug anzunehmen, da nur auf diese Weise ein ausreichender Schutz auch für die Fälle gewährleistet sei, in denen demjenigen, der die Zuordnungsregel kennt, die Daten in die Hände fallen[55]. Wird dieser Ansicht gefolgt, ist § 15 Abs. 3 S. 1 TMG eine Erlaubnisnorm, welche das Erstellen von Nutzungsprofilen auch ohne Einwilligung des Nutzers zulässt.

Die Gegenansicht sieht in den § 15 Abs. 3 TMG statt einer Erlaubnisnorm eine Vorsorgeregelung, welche den bei pseudonymen Profildaten bestehenden besonderen Aufdeckungsrisiken und Persönlichkeitsgefährdungen vorbeugen soll. Sie stelle demnach nicht etwa eine Ausnahme des grundsätzlichen Verbots der Verarbeitung personenbezogenen Daten dar, sondern beschränke vielmehr gerade die sonst immer erlaubte Verarbeitung nicht personenbezogenen Daten[56].

Beide Ansichten übersehen jedoch, dass sich die Frage, ob ein Pseudonym personenbezogen ist, nicht pauschal beantworten lässt, weil der Begriff des Personenbezugs nach seiner Definition in § 3 Abs. 1 BDSG relativ ist. Das bedeutet, dass bei ein und dem selben Datum durch die eine Person, die über entsprechendes Zusatzwissen verfügt, ein Personenbezug hergestellt werden kann,

[52] *Schaar*, Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, 275–277.
[53] BT-Drs. 13/7385 S. 23.
[54] *Gundermann*, E-Commerce trotz oder durch Datenschutz?, 225–235.
[55] *Jasmin Merati-Kashani*, Der Datenschutz im E-Commerce, S. 95.
[56] So etwa *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 109 sowie *Roßnagel* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, S. 222.

durch eine andere Person hingegen nicht[57]. Die Frage, ob ein Pseudonym personenbezogen ist, ist aber immer am Einzelfall zu bewerten und hängt vom Wissen des Erhebenden ab. Auf die selbe Weise sind auch die Fälle zu lösen, in denen der Personenbezug erst im Nachhinein hergestellt werden kann, weil einem Datenverwender die Zuordnungsvorschrift durch Missbrauch oder Zufall in die Hände fallen, da sich die rechtliche Beurteilung dieser Fälle nicht von anderen datenschutzrechtlich relevanten Vorgängen unterscheidet: Sobald ein Personenbezug bei Daten auch nur im Nachhinein hergestellt werden soll, muss vor Erhebung, Verarbeitung oder Nutzung entweder die Einwilligung des Betroffenen eingeholt werden oder ein gesetzlicher Erlaubnistatbestand vorliegen. Es besteht daher kein Bedarf, einen Personenbezug schon in Hinblick darauf anzunehmen, dass dieser erst in Zukunft hergestellt werden könnte. Eine Notwendigkeit, den Einzelnen zu schützen, sieht das BDSG vielmehr erst dann, wenn ein Personenbezug auch tatsächlich hergestellt werden kann, da nur in diesem Fall eine Beeinträchtigung seines Persönlichkeitsrechts denkbar ist (vgl. § 1 Abs. 1 BDSG).

Wurden die pseudonymen Daten zufällig aufgedeckt, wird dem Datenverwender eine angemessene Frist eingeräumt werden müssen, um den rechtswidrigen Zustand zu beseitigen und sich, wenn kein gesetzlicher Erlaubnistatbestand vorliegen sollte, um eine Einwilligung des Betroffenen zu bemühen. Dessen informationelle Selbstbestimmung ist dann zwar insofern eingeschränkt, dass die personenbezogenen Daten als solche bereits vorliegen, es könnte jedoch gleichwohl in seinem Interesse liegen, in die Nutzung der Daten einzuwilligen, falls diese im Vergleich zur Löschung der Daten das „kleinere Übel darstellt“[58].

[57] Siehe hierzu auch schon die Ausführungen unter Abschnitt D.I.3. auf Seite 78 sowie *Gola/Schomerus*, BDSG, § 3 Rdnr. 9 und *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität - Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, 721–731.

[58] *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität - Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, 721–731.

## 2. Bestandsdaten

Sind die Nutzungsdaten, welche für die Inanspruchnahme des Dienstes notwendig sind, vorhanden, kann damit begonnen werden, diesen zu nutzen. Handelt es sich um einen kommerziellen Dienst, dessen Nutzung ein Vertragsverhältnis voraussetzt, sind die Daten, die „für die Begründung, inhaltliche Ausgestaltung oder Änderung“ dieses Verhältnisses erhoben, verarbeitet oder genutzt werden, sog. Bestandsdaten, § 14 TMG. Mögliche Bestandsdaten sind der Name, die Anschrift, die Rufnummer bzw. IP-Adresse, die Login-Kennung, das Geburtsdatum, die Zahlungsart, die Kreditkartennummer und die Bankverbindung[59]. Ebenso wie bei den Nutzungsdaten ist auch bei Bestandsdaten das eng auszulegende Kriterium der Erforderlichkeit heranzuziehen. Bestellt beispielsweise ein Kunde eine Ware per Lastschriftverfahren, so ändert dies nichts am Charakter der Kreditkartennummer als Bestandsdatum. Eine Erhebung derselbigen wäre aber dennoch unzulässig, da sie für das konkrete Vertragsverhältnis nicht erforderlich ist[60]. Erforderlich ist eine Erhebung, Verarbeitung oder Nutzung also nur dann, wenn sie für das jeweilige Vertragsverhältnis *unerläßlich* ist[61]. Unerläßlich ist eine Datenerhebung auch in den Fällen nicht, in denen bei einem Webshop der Kunde sich noch in dem Stadium befindet, in dem er sich das Angebot bloß ansieht. Bestandsdaten dürfen erst dann erhoben werden, wenn der Kunde durch den Bestellvorgang eine vertragliche Beziehung mit dem Anbieter eingeht. Über diese vertragliche Beziehung hinausgehend bedeutet dies ferner, dass die Bestandsdaten weder weiterverarbeitet noch für andere Zwecke genutzt werden dürfen[62].

[59] *Dix* in: *Roßnagel*, Recht der Multimedia-Dienste, § 5 TDDSG, Rdnr. 29.
[60] Vgl. *Dix/Schaar* in: *Roßnagel*, Recht der Multimedia-Dienste, § 19 MDStV Rdnr. 59.
[61] BT-Drs. 13/7385 S. 24.
[62] *Dix* in: *Roßnagel*, Recht der Multimedia-Dienste, § 5 TSSDG, Rdnr. 42.

### 3. Verkehrsdaten

Welche Verkehrsdaten der Diensteanbieter erheben und verwenden darf, ist in § 96 Abs. 1 TKG geregelt. Danach sind unter Verkehrsdaten u.a. die Nummer oder die Kennung, der Beginn und das Ende der Verbindung, der in Anspruch genommene Telekommunikationsdienst sowie sonstige zur Entgeltabrechnung notwendige Daten zu verstehen. Auf das Internet übertragen können das abhängig von der Art der Kommunikation der Name und die Adresse des Nutzers, die E-Mail-Adresse des Nutzers und des Empfängers, Anfang und Ende der Verbindung und, besonders bei volumenbasierter Internetnutzung auch die Menge der übertragenen Daten sein[63].

### 4. Inhaltsdaten

Bei durch die Nutzung der Dienste entstehenden und weiterverarbeiteten Daten handelt es sich um sog. Inhaltsdaten. Sie werden häufig auch Offline-Daten genannt, da ihre Entstehung unabhängig von der Nutzung von Internet-Diensten ist[64]. Sie werden nach herrschender, nicht unumstrittener Meinung dem BDSG zugeordnet und wurden bereits unter Abschnitt C.III.4. auf Seite 66 umfassend dargestellt.

[63] Siehe auch *Weißnicht*, Die Nutzung des Internet am Arbeitsplatz, 449.

[64] So z.B. die essentialia negotii eines Kaufvertrages, zu deren Kenntnis ein Buchhändler unabhängig davon gelangen muss, ob er sein Geschäft on- oder offline betreibt.

# E. Informationspflichten im Datenschutzrecht

## I. Terminologie und Zwecksetzungen

Sowohl der Gesetzgeber als auch die Literatur benutzen die Begriffe „Unterrichtungspflicht“ und „Hinweispflicht“ offensichtlich als Synonyme. So ist der Betroffene nach § 4 Abs. 3 BDSG zu „unterrichten“, im Rahmen des § 4a Abs. 1 S. 2 BDSG ist er hingegen auf den vorhergesehenen Zweck und auf die Folgen der Verweigerung der Einwilligung „hinzuweisen“. In der Kommentarliteratur wird die Pflicht nach § 4 Abs. 3 BDSG wiederum teilweise als Hinweispflicht bezeichnet[1]. Eine Unterscheidung nach dem Wortsinn der beiden Verben „unterrichten“ und „hinweisen“ hätte nahegelegt, dass die Pflicht einer Unterrichtung weiterreicht als die eines Hinweises. Dies hat sich aber im rechtlichen Ergebnis nicht widergespiegelt. Um nicht durch eine uneinheitliche Terminologie für Verwirrung zu sorgen, wird im Folgenden daher von den Unterrichtungspflichten gesprochen, welche u.a. zusammen mit Auskunfts- und Aufklärungspflichten als Untergruppe der Informationspflichten[2] anzusiedeln sind.

Ziel und Zweck der Informationspflichten im Datenschutzrecht ist es, der Herstellung einer transparenten Datenverarbeitung zu dienen. In ihrer Rechtsnatur sind jedoch Unterrichtungs-, Aufklärungs- und Benachrichtigungspflichten von Auskunftsansprüchen zu trennen: Erstere haben wie auch im allgemeinen Zivilrecht das Ziel, den Betroffnen über erkennbar entscheidungserhebliche

[1] *Gola/Schomerus*, BDSG, § 4 Rdnr. 36.

[2] So auch *Stephan Breidenbach*, Die Voraussetzungen von Informationspflichten beim Vertragsabschluß, S. 4.

Umstände zu informieren, die ihm ansonsten verborgen blieben[3]. Sie stellen als solche eine strukturelle Anforderung an eine transparente Datenverarbeitung dar[4].

Bei den Auskunftsansprüchen handelt es sich hingegen um individuelle Rechte des Betroffenen, welche im Gegensatz zu den Unterrichtungs-, Aufklärungs- und Benachrichtigungspflichten als solche auch klagbar sind[5]. Sie werden daher im Folgenden getrennt aufgeführt.

## II. Unterrichtungs-, Benachrichtigungs- und Aufklärungspflichten

### 1. BDSG

Die Informationspflichten des BDSG finden sich in den §§ 4 Abs. 3, 4a Abs. 1 S. 2, 28 Abs. 4 S. 2 und 33 Abs. 1 BDSG[6].

#### a) Unterrichtungspflicht gem. § 4 Abs. 3 S. 1 BDSG

§ 4 Abs. 1 BDSG stellt klar, dass jede Datenerhebung, -verarbeitung und -nutzung ein Verbot mit Erlaubnisvorbehalt darstellt. Diese ist demnach nur zulässig, wenn eine Rechtsvorschrift oder das BDSG es gestattet oder der Betroffene eingewilligt hat. § 4 Abs. 1 BDSG enthält den Grundsatz der Direkterhebung[7], welcher besagt, dass „personenbezogene Daten beim Betroffenen zu erheben sind“ . Ohne dessen Mitwirkung dürfen sie nur in den Ausnahmefällen von § 4 Abs. 2 S. 2 BDSG erhoben werden. Ausschließlich im Falle einer Direkterhebung sind die §§ 4 Abs. 3 und 4a BDSG anwendbar. Deren Aufgabe ist es,

[3] *Roth* in: *Rebmann/Säcker/Rixecker*, MüKo, § 241, Rdnr. 114.
[4] *Roßnagel* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, S. 189.
[5] *Roth* in: *Rebmann/Säcker/Rixecker*, MüKo, § 241, Rdnr. 114.
[6] Siehe aber zu den weitreichenden geplanten Gesetzesänderungen unter Abschnitt C.IV. auf Seite 70.
[7] *Gola/Schomerus*, BDSG, § 4 Rdnr. 19.

für eine erweiterte Transparenz zu sorgen[8], indem der Betroffene, falls er darüber nicht schon auf andere Weise Kenntnis erlangt hat, über die Identität der verantwortlichen Stelle, dem Zweck der Erhebung und für die Fälle, dass „der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung“ rechnen muss – die Kategorien von Empfängern unterrichtet wird.

### b) Unterrichtungspflicht gem. § 4 Abs. 3 S. 2 BDSG

Nach § 4 Abs. 3 S. 2 BDSG ist der Betroffene in den Fällen, in denen seine personenbezogenen Daten aufgrund einer Rechtsvorschrift erhoben werden, die zur Auskunft verpflichtet auf diese Pflicht oder in den Fällen, in denen die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen (z.B. Subventionen) ist, auf die Freiwilligkeit seiner Angaben hinzuweisen. Die Unterrichtungspflicht gem. § 4 Abs. 3 S.2 BDSG wendet sich in erster Linie an öffentliche Stellen[9], da sie im Zivilrecht aufgrund der Vertragsautonomie eine geringe Rolle spielt[10]. Trotzdem hat der Gesetzgeber bei der Novellierung des BDSG 2001 diese Pflicht in Umsetzung des Art. 10 Buchst. c der EG-Datenschutzrichtlinie auch für den nicht-öffentlichen Bereich aufgenommen[11]. Die Frage, ob ein Vertragsabschluss von der Auskunft über personenbezogenen Daten abhängig gemacht werden kann, kann im Zivilrecht jedoch hinsichtlich des § 242 BGB eine Rolle spielen[12].

### c) Aufklärungspflicht gem. § 4 Abs. 3 S. 3 BDSG

Eine dem Wortlaut des § 4a Abs. 1 S. 1 2. HS BDSG entsprechende Aufklärungspflicht findet sich in § 4 Abs. 3 S. 3 BDSG. So ist der Betroffene, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen über die

[8] *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 50f.
[9] *Schaffland/Wiltfang*, BDSG, § 4 BDSG Rdnr. 15.
[10] *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 50.
[11] Vgl. auch BT-Drs. 14/4329 S. 34.
[12] *Gola/Schomerus*, BDSG, § 4 Rdnr. 41; siehe dazu unter Abschnitt G.I.3. auf Seite 159.

Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären. Eine nähere Ausführung, unter welchen Umständen der Gesetzgeber eine derartige Aufklärung für notwendig erachtet, fehlt. Es wird aber davon auszugehen sein, dass ein solcher Einzelfall immer dann gegeben ist, wenn eine ausreichende Transparenz beim Betroffenen nicht schon durch den Hinweis nach Satz 2 geschaffen wurde, sondern offensichtlich ist, dass er eine willentliche und freiwillige Entscheidung nur dann treffen kann, wenn er auch auf die Folgen der Verweigerung hingewiesen wird[13].

### d) Unterrichtungspflicht gem. § 4a Abs. 1 S. 2 BDSG

§ 4a Abs. 1 BDSG beinhaltet die Voraussetzungen der Einwilligung. Da in den Fällen, in denen eine vorherige Einwilligung des Betroffenen eingeholt wird, eine Rechtsvorschrift die Erhebung üblicherweise gerade nicht ausdrücklich gestattet, ist es umso wichtiger, dass dieser aufgrund seiner Einsichtsfähigkeit die Tragweite seiner Entscheidung voraussehen kann[14] . Aus diesem Grunde schreibt § 4a Abs. 1 S. 2 BDSG die so genannte „informierte Einwilligung“ vor: In den Fällen, in denen Daten aufgrund der Einwilligung des Betroffenen erhoben werden, ist dieser bereits vor der Einwilligung „auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung [ . . . ] hinzuweisen“. Bei einer grammatikalischen Auslegung der Vorschrift würde sich ergeben, dass der Umfang der Hinweispflicht sich lediglich auf den Zweck der Datenerhebung beschränkt. Teilweise wird vertreten, dass die bloße Nennung des Zweckes als solche daher nur als ein durch den Gesetzgeber benanntes Beispiel gesehen werden kann[15]. Dies widerspricht jedoch der Entstehungsgeschichte des heutigen § 4a Abs. 1 BDSG. Die Hinweispflicht und damit die Voraussetzung der „informierten Einwilligung“ fand sich erstmals in § 4 Abs. 2 S. 1 BDSG 1990,

[13] So im Ergebnis auch *Gola/Schomerus*, BDSG, § 4, Rdnr. 45.
[14] *Gola/Schomerus*, BDSG, § 4a Rdnr. 10.
[15] *Scholz*, Datenschutz beim Internet-Einkauf, S. 298.

welcher damals eingeführt wurde, um die Rechte des Betroffenen zu stärken[16] und wurde mit der Novellierung des BDSG 2001 an die Terminologie der EG-Datenschutzrichtlinie angepasst[17]. In der Richtlinie findet sich zugleich die Begründung dafür, warum der Umfang der Hinweispflicht sich wenigstens auf die in § 4 Abs. 3 BDSG genannten Punkte ausdehnen muss: Art. 2 Buchst. h der Richtlinie, welcher zur Änderung der § 4a Abs. 1 S. 1, 2 BDSG geführt hat, setzt voraus, dass die betroffene Person die Einwilligung in „Kenntnis der Sachlage“ abgibt. Von dieser Kenntnis kann jedoch im Falle, dass lediglich ein Hinweis auf den Zweck der Erhebung erfolgt ist, gerade nicht ausgegangen werden. Wiederum nennt § 4a Abs. 1 S. 1 BDSG nunmehr seinerseits als Voraussetzung der wirksamen Einwilligung die freie Entscheidung des Betroffenen. Würde daher der Umfang des Satzes 2 isoliert und als ausreichend betrachtet werden, läge darin bereits ein Verstoß gegen Satz 1 der Vorschrift. Zu beachten ist an dieser Stelle ebenso, dass die Reichweite der Einwilligung ihrem Sinn nach nicht weiter gehen kann als die der ihr vorangegangenen Unterrichtung, da nur insofern Einsichtsfähigkeit vorliegt und sich die Erlaubnis nicht über die Einsichtsfähigkeit hinaus erstrecken kann. Es liegt somit auch im Interesse der erhebenden Stelle, den Betroffenen möglichst umfassend zu informieren. Die Informationspflicht bezieht sich somit auf die gesamte beabsichtigte Verwendung und muss auch genaue Angaben über die jeweils gewünschten Daten enthalten[18].

Unklar in Bezug auf den Inhalt der Informationspflicht ist ferner die zweite Alternative des § 4a Abs. 1 S. 2 BDSG, nach welcher der Betroffene, soweit nicht wegen besonderer Umstände des Einzelfalles ohnehin nötig, auf sein Verlangen hin auf die Folgen der Verweigerung hinzuweisen ist. Bei alleini-

[16] BT-Drs. 11/4306, S. 41.

[17] BT-Drs. 14/4329, S. 34; die missverständliche Formulierung „Wird die Einwilligung bei dem Betroffenen eingeholt“ gab der Gesetzgeber bei der Novellierung des BDSG 2001 wieder auf, vgl. *Holznagel/Sonntag* in: *Roßnagel*, Handbuch Datenschutzrecht, 4.8 Rdnr. 8.

[18] *Simitis* in: *BDSG*, Simitis, § 4a Rdnr. 72.

ger Betrachtung des Wortlautes erstreckt sich die Informationspflicht nur in Ausnahmefällen auch auf die Folgen der Verweigerung der Einwilligung. Der Betroffene muss in allen anderen Fällen daher von sich aus aktiv werden, wenn er über die Folgen informiert werden möchte. Die Vorschrift erscheint jedoch, unter Berücksichtigung des Sinns und Zwecks der Informationspflicht nach § 4a Abs. 1 S. 2 BDSG, nicht konsequent: Aus der ersten Alternative des § 4 Abs. 1 S. 2 BDSG ergibt sich die Pflicht, den Betroffenen derart ausführlich zu informieren, dass er sein Selbstbestimmungsrecht in Kenntnis darüber ausübt, was die Folgen der Erteilung seiner Einwilligung in Bezug auf seine personenbezogenen Daten sind. Die zweite Alternative soll ihn dahingegen in Kenntnis darüber setzen, welche Folgen die Verweigerung seiner Einwilligung wären. Die beiden Alternativen ergänzen sich somit zu einem umfassenden Informationsrecht, welches den Betroffenen erst in die Lage versetzt, die Abwägung hinsichtlich der Vor- und Nachteile der Preisgabe seiner Daten unter Berücksichtigung sämtlicher Gesichtspunkte vorzunehmen.

Bei verfassungskonformer Auslegung (unter Berücksichtigung des Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) des § 4 Abs. 1 S. 2 BDSG wird entgegen der Entstehungsgeschichte, aus der sich das Ziel ergibt, die Informationspflicht zugunsten der verantwortlichen Stellen zu „entformalisieren“[19], selten ein aktives Tätigwerden des Betroffenen von Nöten sein, um die Informationspflicht auszulösen. Im Regelfall erstreckt sich die Informationspflicht vielmehr auch auf die Folgen der Verweigerung.

### e) Unterrichtungspflicht gem. § 28 Abs. 4 S. 2 BDSG

§ 28 Abs. 4 S. 1 BDSG enthält ein Widerspruchsrecht des Betroffenen gegenüber der verantwortlichen Stelle im Falle der Nutzung oder Übermittlung seiner personenbezogenen Daten für Zwecke der Werbung oder Markt- und Meinungsforschung. Um zu gewährleisten, dass der Betroffene nach Satz 2 von

[19] *Simitis* in: *BDSG*, Simitis, § 4a BDSG, Rdnr. 74 f.

seinem Widerspruchsrecht auch Kenntnis erlangt, ist der Betroffene darüber sowie über die verantwortliche Stelle zu unterrichten. Die Vorschrift nennt als letzten möglichen Zeitpunkt denjenigen, in dem der Betroffene erstmalig zum Zwecke der Werbung oder Markt- und Meinungsforschung angesprochen wird.

Dabei ist strittig, ob die Werbeaktion selbst und die Unterrichtung zeitlich zusammenfallen dürfen: Teilweise wird, wohl im Hinblick auf den Wortlaut[20] bzw. dem Argument der Praktikabilität und des Kostenaufwands[21] vertreten, dass eine Unterrichtung gleichzeitig mit der Werbemaßnahme genügt. Auf der anderen Seite ist das Argument überzeugend, dass das Widerspruchsrecht, über das informiert werden soll, sich gerade gegen die Nutzung oder Übermittlung der Daten zu Werbezwecken richtet und somit leer laufen würde, wenn die Unterrichtung nicht bereits vor der erstmaligen Nutzung bzw. Übermittlung erfolgt[22].

Der Betroffene ist vom Ansprechenden zu unterrichten. Dies ergibt sich inzident aus dem Wortlaut des § 28 Abs. 4 S. 2 2. HS BDSG, nachdem der Ansprechende (neben seiner Pflicht aus dem ersten Halbsatz) für die Fälle, in denen er Daten nutzt, die bei einer dem Betroffenen nicht bekannten Stelle gespeichert sind, *auch* sicherzustellen hat, dass der Dritte über die Herkunft dieser Daten Kenntnis erhält. Unter „Ansprechender“ im Sinne des § 28 Abs. 4 S. 2 BDSG ist in den Fällen, in denen eine Übermittlung stattfand, der Übermittlungsempfänger zu verstehen[23]. In den Fällen, in denen keine Über-

[20] *Gola/Schomerus*, BDSG, § 28 BDSG, Rdnr. 62.

[21] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 28 BDSG, Rdnr. 332.

[22] *Simitis* in: *BDSG*, Simitis, § 28 BDSG, Rdnr. 283.

[23] A.A. ist hier, entgegen dem Wortlaut, wonach Ansprechender derjenige ist, der den Betroffenen *zum Zweck der Werbung anspricht*, *Simitis* in: *BDSG*, Simitis, § 28 BDSG, Rdnr. 274, demzufolge sowohl die übermittelnde Stelle als auch der Übermittlungsempfänger Ansprechende sein können. *Simitis* will in den Fällen, in denen eine Übermittlung stattfand, dem Übermittelten die Unterrichtungspflicht auferlegen, da dieser die Gründe für das Abweichen vom ursprünglichen Zweck und den potenziellen Empfängerkeis besser kennt als der Übermittlungsempfänger. Diese Ansicht übersieht jedoch abgesehen vom Wortlaut, dass der Empfänger hingegen den „neuen Zweck“ also denjenigen, für den die Daten genutzt werden sollen, besser kennt als die übermittelnde Stelle und der Betroffene aufgrund

mittlung statt fand und der Betroffene die verantwortliche Stelle daher bereits gekannt hat, weil die Daten durch sie selbst gespeichert wurden, kann hingegen eine Unterrichtung über ihre Identität unterbleiben[24].

Offen lässt das Gesetz die Frage, ob die Unterrichtung bei jeder weiteren Ansprache erneut erfolgen muss. Dies ist schon aus Gründen der Praktikabilität, also der Beweissicherung darüber, dass die Information des Betroffenen stattgefunden hat, zu bejahen, da es gerade für die werbetreibende Wirtschaft oftmals schwer zu überschauen ist, ob der Betroffene von ihr bereits angeschrieben, geschweige denn bereits unterrichtet wurde[25].

### f) Benachrichtigungspflicht gem. § 33 Abs. 1 BDSG

§ 33 Abs. 1 BDSG hat die Fälle im Auge, in denen die Daten *ohne Kenntnis* des Betroffenen entweder für eigene Zwecke (Satz 1) oder zum Zwecke der Übermittlung (Satz 2) gespeichert werden. Da eine Erhebung ohne Kenntnis des Betroffenen eine Ausnahme des Grundsatzes der Direkterhebung darstellt, darf der Betroffene zumindest hinsichtlich seiner Kenntnis über das, was mit seinen personenbezogenen Daten „passiert“ nicht schlechter gestellt werden, als wenn sie direkt bei ihm erhoben worden wären. § 33 Abs. 1 BDSG legt somit eine Benachrichtungspflicht *nach* der Speicherung der Daten fest, die sich zwar im Zeitpunkt von der vorverlagerten Informationspflicht des § 4 Abs. 3 BDSG unterscheidet, im Umfang aber gleich ist[26]. Ausnahmen von der Benachrichtigungspflicht sind in Abs. 2 geregelt.

dieses Zweckes seine Entscheidung darüber besser treffen kann, ob er der Nutzung oder der Übermittlung widerspricht.

[24] *BDSG*, Simitis, § 28 BDSG Rdnr. 62.

[25] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 28 BSDG, Rdnr. 333.

[26] *Gola/Schomerus*, BDSG, § 33 BDSG Rdnr. 7f.

## 2. TMG

### a) Unterrichtungspflicht bei Erhebung, Verarbeitung und Nutzung personenbezogener Daten, § 13 Abs. 1 Satz 1 TMG

Die allgemeine Unterrichtungspflicht nach dem TMG, die spätestens zu Beginn des Nutzungsvorgangs erfüllt werden muss, findet sich in § 13 Abs. 1 TMG. Nach Satz 1 hat der Diensteanbieter den Nutzer über Art[27], Umfang und Zweck der Erhebung sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG[28] zu unterrichten. Die Unterrichtungspflicht ist ihrem Inhalt nach daher weiter gefasst als die des BDSG, nach der zwar über den Zweck und die Kategorien von Empfängern, nicht aber auch über Art und Umfang der Erhebung zu unterrichten ist[29]. Darüber hinaus ergibt sich auch hier die Pflicht zur Unterrichtung über die Identität aus der gesetzlich vorgeschriebenen Anbieterkennzeichnung gemäß § 5 Nr. 1 TMG, welche aus datenschutzrechtlicher Sicht insofern von großer Relevanz ist, als dass sie die Durchsetzung des Auskunftsanspruches erleichtert[30].

Satz 2 enthält die Unterrichtungspflicht für automatisierte Verfahren, welche der Gefahr Rechnung trägt, dass für Daten, die zunächst ohne Personenbezug registriert werden, ein solcher im Nachhinein hergestellt wird[31]. Der Inhalt der Unterrichtung muss nach Satz 3 für den Nutzer jederzeit abrufbar sein.

Besonderheiten gegenüber dem BDSG ergeben sich überdies hinsichtlich der Möglichkeit zur elektronischen Einwilligung, § 13 Abs. 2, Abs. 3 Satz 1 TMG. Gerade im Internet ist hier das Augenmerk auf § 13 Abs. 2 Nr. 1 TMG zu legen: Eine vorformulierte Einwilligung, welche sich innerhalb eines Formulars befindet und standardmäßig bereits mit einem zustimmenden Haken versehen ist, erfüllt nicht die Voraussetzung, dass die elektronische Einwilligung

[27] Zu den verschiedenen Arten von Daten siehe Abschnitt D.VI. auf Seite 87.
[28] Abl. EG Nr. L 281, 31.
[29] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 Rdnr. 97.
[30] *Bizer*/ *Trosch*, Die Anbieterkennzeichnung im Internet, 621–627.
[31] Siehe dazu sogleich und unter *Schaar*, Datenschutz im Internet, Rdnr. 327.

nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann. Andererseits war es Ziel des Gesetzgebers, mit Einführung der elektronischen Einwilligung in das damalige TDDSG dieser durch ein praxisnahes Verständnis zu einer breiten Anwendung im elektronischen Geschäftsverkehr zu verhelfen[32]. Eine eindeutige und bewusste Handlung des Nutzers ist daher jedenfalls dann anzunehmen, wenn dieser einen optisch abgetrennten Einwilligungstext selbst durch einen Haken bestätigt[33] oder eine wiederholte Übermittlung dadurch erfolgt, dass vor der erneuten Absendung der Informationen ausdrücklich auf die datenschutzrechtliche Einwilligung hingewiesen wird[34].

### b) Unterrichtungspflicht bei automatisierten Verfahren, § 13 Abs. 1 Satz 2 TMG

Eine Unterrichtungspflicht auch für automatisierte Verfahren bestand bereits in der Fassung des IuKDG, in dessen Begründung klargestellt wurde, dass *„sich die Unterrichtungspflicht auf automatisierte Verfahren bezieht, die eine Erhebung, Verarbeitung oder Nutzung ermöglichen (z. B. durch Speichern einzelner Nutzungsdaten auf der Festplatte des vom Nutzer benutzten PC), bei denen der Personenbezug aber erst zu einem späteren Zeitpunkt hergestellt werden kann“*[35]. Seit der Novellierung des TDDSG 2001 und nunmehr auch in § 13 Abs. 1 Satz 2 TMG muss die Unterrichtung zwecks der besseren Praktikabilität nicht mehr bereits vor Beginn, sondern erst zu Beginn des Verfahrens stattfinden[36]. Beispiele für automatisierte Verfahren im Sinne des § 13 Abs. 1 Satz 2 TMG sind Cookies, Web-Bugs, aktive Skripte (wie Java-Script und Ac-

[32] BT-Drs. 14/6098, S. 28.
[33] *Enzmann/Scholz*, Technisch-organisatorische Gestaltungsmöglichkeiten, 73–88.
[34] So wohl auch *Zscherpe*, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, 723–727.
[35] BT-Drs. 13/7385, S. 22.
[36] BT-Drs. 14/6098, S. 28.

tiveX) und Spyware[37]. Der Inhalt der Unterrichtungspflicht gleicht dabei der des Satzes 1.

### c) Unterrichtungspflicht über Widerruf der Einwilligung, § 13 Abs. 3 TMG

Als Besonderheit gegenüber § 4a Abs. 1 BDSG erweist sich die Unterrichtungspflicht über das Widerrufsrecht, das den Nutzern von Telemediendiensten zusteht: Nach Abgabe der Einwilligung in die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten hat der Nutzer gegenüber dem Diensteanbieter das Recht, diese mit Wirkung für die Zukunft zu widerrufen[38]. Über dieses Recht ist er vor Abgabe der Einwilligung zu unterrichten, wobei die Unterrichtung nach Satz 2 in Verbindung mit Absatz 1 Satz 3 jederzeit abrufbar sein muss. Zu beachten ist, dass diese Pflicht *neben* der Unterrichtungspflicht aus § 4a Abs. 1 Satz 2 BDSG besteht.

### d) Sonstige Unterrichtungspflichten

Die sonstigen Unterrichtungspflichten ergeben sich aus den datenschutzrechtlichen Besonderheiten, die im Rahmen der Nutzung von Telemediendiensten auftreten, namentlich aus der Möglichkeit zur pseudonymen und anonymen Nutzung. Nach § 13 Abs. 6 TMG hat der Anbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist[39]. Der Nutzer

[37] Siehe zur detaillierten Aufzählung auch *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 165 ff.

[38] Das Recht, die Einwilligung ex nunc zu widerrufen, ist auch im allgemeinen Datenschutzrecht anerkannt, vgl. *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 4a Rdnr. 23, die Besonderheit ergibt sich im Telemediendatenschutzrecht lediglich aus der diesbezüglichen Unterrichtungspflicht.

[39] An eine Möglichkeit der pseudonymen Bezahlung mittels Diensten wie Click&Buy (`http://clickandbuy.com`) wird immer dann zu denken sein, wenn der Nutzer ein rein digitales Produkt, wie z.B. die Softwareversion eines Wörterbuches, mittels Download erwerben will.

ist darüber zu informieren (Satz 2). Die Art und Weise, wie die Unterrichtung zu erfolgen hat, ist dabei gesetzlich nicht festgehalten. Da die anonyme bzw. pseudonyme Nutzung aber lediglich eine Alternative zur personenbezogenen Nutzungsmöglichkeit des Dienstes darstellt, über die der Nutzer durch Satz 2 informiert werden soll, wird eine allgemeine Möglichkeit der Nutzung, unabhängig der Ausprägung der Ausgestaltung, genügen[40].

Möchte der Diensteanbieter pseudonyme Nutzungsprofile erstellen, muss dies dem Nutzer gemäß § 15 Abs. 3 Satz 2 TMG im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG mitgeteilt werden. Darüber hinaus ist er über seine Möglichkeit, dem zu widersprechen, zu unterrichten[41].

### e) Verhältnis zum BDSG

Das Verhältnis zum BDSG bestimmt sich, wie schon unter Abschnitt C.III.4. auf Seite 66 erläutert, nach § 12 Abs. 4 TMG. Für die Informationspflichten ergibt sich daher, dass die speziellere und weitreichendere Pflicht nach § 13 Abs. 1 TMG dem § 4 Abs. 3 BDSG vorausgeht, während die Pflichten nach §§ 4a Abs. 1, 33 Abs. 1 BDSG, welche sich in vergleichbarer Form nicht im TMG finden, daneben bestehen bleiben[42]. An dieser Stelle ist jedoch ebenfalls zu erwähnen, dass es vor allem im Bereich des Internetrechts in der Praxis besonders wichtig sein wird, den Betroffenen auch außerhalb des Anwendungsbereichs der bereichsspezifischen Regelungen bereits im Vorfeld über den Zweck hinaus ebenso über die Art und den Umfang der Erhebung hinzuweisen, da nur dann gewährleistet werden kann, dass die Wirksamkeitsvoraussetzung des §4a Abs. 1 Satz 1 BDSG gewahrt ist[43].

[40] *Gola/Müthlein*, TDG/TDDSG, § 4 TDDSG, Rdnr. 2.6.
[41] Zu Nutzungsprofilen siehe Abschnitt D.VI.1.a) auf Seite 88.
[42] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 Rdnr. 91ff.
[43] *Helfrich* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, 16.1, Rdnr. 50.

## III. Auskunftsansprüche

Die Auskunftsansprüche im Datenschutzrecht werden zurecht auch als tragende Säule des Rechts auf informationelle Selbstbestimmung bezeichnet[44], da sie Grundvoraussetzung für die Ausübung der Folgerechte auf Berichtigung, Löschung, Sperrung, Widerspruch und Schadensersatz sind[45]. Somit sind sie grundlegend für den Grundsatz der Transparenz und können deshalb durch Rechtsgeschäft weder ausgeschlossen noch beschränkt werden, § 6 Abs. 1 BDSG[46].

### 1. Auskunftsanspruch nach § 34 BDSG

Nach § 34 Abs. 1 Satz 1 BDSG hat der Betroffene das Recht, über die zu seiner Person gespeicherten Daten, die Empfänger derselbigen und den Zweck der Speicherung Auskunft zu verlangen. Abs. 2 erweitert den Auskunftsanspruch auch auf Daten in Akten, wenn es sich bei der speichernden Stelle um eine Auskunftei handelt[47]. Eine bestimmte Form, mittels derer der Anspruch geltend gemacht werden muss, sieht § 34 BDSG nicht vor, es herrscht also Formfreiheit[48], wohingegen für die Auskunft selbst gem. Abs. 3 regelmäßig die Schriftform gilt. Der Empfänger soll jedoch die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnen, um pauschale Auskunftsersuchen zu vermeiden.

§ 34 Abs. 1 S. 3 und Abs. 2 S. 2 schränken das Auskunftsrecht dahingehend ein, dass über Herkunft und Empfänger der Daten dann keine Auskunft

[44] *Gounalakis*, Der Mediendienste-Staatsvertrag der Länder, 2993–3000.
[45] *Engel-Flechsig* in: *Engel-Flechsig/Maennel/Tettenborn*, Beck'scher IuKDG-Kommentar, § 16 MDStV, Rdnr. 1, der das Auskunftsrecht daher als *magna charta* des Datenschutzrechts bezeichnet.
[46] Dieser gilt auch für die bereichsspezifischen Auskunftsansprüche, vgl. § 1 Abs. 3 TDDSG bzw. § 6 Abs. 2 MDStV sowie *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 6 Rdnr. 44.
[47] *Schaffland/Wiltfang*, BDSG, § 34 BDSG, Rdnr. 6.
[48] *Schaffland/Wiltfang*, BDSG, § 34 BDSG, Rdnr. 2.

verlangt werden kann, wenn das Interesse an der Wahrung des Geschäftsgeheimnisses desjenigen, der Daten geschäftsmäßig zur Übermittlung speichert, überwiegt. Diese Änderung des BDSG, die mit der Novellierung des BDSG 2001 aufgenommen wurde, stellt eine Anpassung an Artikel 13 Buchst. g der EG-Datenschutzrichtlinie dar[49]. In der Praxis wird ein Interesse an der Wahrung des Geschäftsgeheimnisses jedoch nur selten das persönlichkeitsrechtliche Informationsinteresse überwiegen. Das faktische Zutreffen von Auskünften einer Auskunftei reicht für ein allgemeines Überwiegen des Interesses an der Wahrung des Geschäftsgeheimnisses beispielsweise noch nicht aus. Es muss vielmehr in jedem Einzelfall begründet werden und ist nur in Ausnahmefällen vorstellbar, da nur auf diese Weise eine ausreichende Transparenz gesichert werden kann[50].

### 2. Auskunftsanspruch nach § 13 Abs. 7 TMG

Der Auskunftsanspruch nach § 13 Abs. 7 TMG gibt dem Nutzer gegen den Diensteanbieter einen Anspruch, von ihm unentgeltlich und unverzüglich Auskunft über die zu seiner Person gespeicherten Daten sowie die Daten, die in § 13 Abs. 7 TMG nicht genannt sind, jedoch Inhalt des Auskunftsrechts nach § 34 BDSG sind, zu erhalten. Soweit diese Angaben ebenfalls gespeichert wurden, erstreckt sich das Auskunftsrecht daher auch auf den Zweck der Verarbeitung, die Herkunft und die Empfänger[51].

[49] BT-Drs. 14/4329, S. 45.

[50] So zutreffend der Hessische Landtag in der Vorlage der Landesregierung betreffend den Fünfzehnten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drs. 15/4659, S. 40; vgl. auch *Gola/Schomerus*, BDSG, § 34, Rdnr. 11a.

[51] *Roßnagel* in: *Roßnagel*, Handbuch Datenschutzrecht, 7.9 Rdnr. 101, jedoch ohne dahingehende Erklärung; die Erklärung dafür liegt indes darin begründet, dass das informationelle Selbstbestimmungsrecht eines Nutzers nicht nur hinsichtlich der zu seiner Person gespeicherten Daten, sondern auch im Umfang von § 34 BDSG den besonderen Risiken von Internetdiensten ausgesetzt ist.

Er bildet eine Spezialregelung zum allgemeinen Auskunftsanspruch nach § 34 BDSG für die Auskunftserteilung bei Telemediendiensten und geht diesem insofern voraus, bezieht sich dabei jedoch einzig und allein auf das Anbieter-Nutzer-Verhältnis im Rahmen des Telemediendienstes und der dabei gespeicherten Daten[52]. Nicht umfasst sind daher die Daten, die zwar über einen Telemediendienst erhoben wurden, für die jedoch die Bestimmungen des BDSG gelten[53]. Die Anwendbarkeit des § 34 BDSG bleibt in diesem Umfang bestehen und kann insoweit daneben geltend gemacht werden.

Da § 34 BDSG eine Ergänzungsregelung[54] zu § 13 Abs. 7 TMG darstellt, dessen Regelungsgehalt weiter reicht als § 13 Abs. 7 TMG, bleibt dieser auch insoweit bestehen, als in § 13 Abs. 7 TMG keine Regelung getroffen wurde[55]. Dies gilt insbesondere für den Ausschluss der Auskunftspflicht nach § 34 IV BDSG.

Nach der 2. Alternative von Satz 1 muss dem Nutzer auch über sein Pseudonym Auskunft erteilt werden. Die Erweiterung des Auskunftsanspruchs auch auf Pseudonyme hat in der Literatur zu Unstimmigkeiten geführt: während einerseits vertreten wird, dass zur Verhinderung der Aufdeckung die Inanspruchnahme des Rechts ebenfalls unter Pseudonym zu erfolgen hat[56], sieht eine andere Ansicht unter der Erfüllung der Auskunftsverpflichtung eine Reduzierung des Verbots der nachträglichen Zusammenführung ad minimum, weil diese erfordert, dass die in einem Nutzungsprofil unter dem Pseudonym erfassten Daten mit dessen Träger wieder zusammengeführt wird, woraus resultieren würde dass § 13 Abs. 7 TMG als untaugliche Eingriffsregelung verfassungswidrig ist[57].

[52] *Schaar* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 450.
[53] *Schaar* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 467; zu der Unterscheidung zwischen BDSG und Telemediendatenschutzrecht siehe oben unter Abschnitt C.III.4. auf Seite 66.
[54] *Schaar* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 467.
[55] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 34, Rdnr. 12.
[56] *Scholz*, Datenschutzrechtliche Anforderungen, 41–72.
[57] *Schmitz* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, 16.4 Rdnr. 170.

Diese Ansicht ist abzulehnen. Ihr ist zwar insofern zuzustimmen, dass im Auskunftsverlangen allein noch keine ausreichende Einwilligung zur nachträglichen Aufdeckung des Pseudonyms von Seiten des Diensteanbieter zu sehen ist. Wohl ist aber eine solche Einwilligung dann denkbar, wenn der Nutzer vor der Auskunftserteilung vom Diensteanbieter über die Notwendigkeit der Aufdeckung zur Erfüllung des Anspruchs ausreichend unterrichtet wurde. Überdies übersieht die kritisierte Ansicht die Fälle, in denen dem Nutzer mittels einem Zugangsschutz durch ein Passwort die ausschließliche Möglichkeit der Einsichtnahme in seinen pseudonymen Datensatz gegeben wird, ohne dass dieser auch vom Diensteanbieter eingesehen werden kann. Wird zudem § 13 Abs. 7 TMG als ein über den allgemeinen Anspruch des § 34 BDSG hinausgehender Schutz betrachtet, durch den der Nutzer bei Telemediendiensten auch einen Auskunftsanspruch bezüglich der pseudonym gespeicherten Daten erhält, so erscheint es wenig plausibel, warum dieser als solcher isoliert von seiner fallbezogenen Ausgestaltung verfassungswidrig sein sollte.

Aufgrund der Besonderheit, dass die Erstellung von Nutzungsprofilen im Rahmen des § 15 Abs. 3 TMG unter der Verwendung von Pseudonymen erlaubt ist, ist ein Auskunftsanspruch, der sich auch auf die unter Pseudonym gespeicherten Daten erstreckt, wie ihn § 13 Abs. 7 TMG vorsieht, vielmehr dringend angezeigt. Er ist jedoch so zu verwirklichen, dass eine Aufdeckung des Pseudonyms wenn möglich unterbleibt. In den Fällen, in denen sich eine solche nicht verhindern lässt, ist der Nutzer über die Aufdeckung und deren Folgen ausreichend zu unterrichten, so dass es ihm möglich ist, informiert in die Aufdeckung einzuwilligen.

Nach Satz 2 kann der Diensteanbieter auf Verlangen des Nutzers die Auskunft auch elektronisch erteilen.

### 3. Auskunftsanspruch nach § 57 Abs. 2 RStV

Besonderheiten gegenüber § 13 Abs. 7 TMG ergeben sich aus § 57 Abs. 2 RStV. Bei § 57 Abs. 2 RStV handelt es sich um eine lex specialis zu § 13 Abs. 7 TMG, die im Wesentlichen wortgleich mit § 41 Abs. 3 BDSG ist, welcher für Rundfunkanstalten des Bundesrechts gilt[58].

Nach § 57 Abs. 2 RStV besteht ein Auskunftsrecht des Betroffenen dann, wenn über Angebote personenbezogene Daten ausschließlich zu journalistisch-redaktionellen Zwecken verarbeitet werden und er dadurch in seinen schutzwürdigen Interessen beeinträchtigt wird. Anknüpfungspunkt für den Auskunftsanspruch ist daher der Zweck der Datenverarbeitung. Ein journalistisch-redaktioneller Zweck liegt dann vor, wenn die Zielrichtung der Verarbeitung in der Veröffentlichung für einen unbestimmten Personenkreis besteht[59]. Dazu muss zum einen eine redaktionelle Aufbereitung im Hinblick auf erwartete Benutzerbedürfnisse stattfinden, im Rahmen welcher der bloße Materialcharakter der ursprünglich gespeicherten Daten verloren geht[60], zum anderen muss eine Veröffentlichungsabsicht bestehen, welche sich auf die Massenkommunikation richtet[61].

Damit dem Betroffenen ein Auskunftsanspruch zusteht, muss er durch die Verarbeitung in seinen schutzwürdigen Interessen beeinträchtigt sein. Welche Interessen damit genau gemeint sind, ist gesetzlich nicht geregelt, die Regelung geht dabei jedoch über § 41 Abs. 3 BDSG hinaus, welcher eine Beeinträchtigung des Persönlichkeitsrechts voraussetzt. Daraus ergibt sich, dass zumindest dann eine Beeinträchtigung im Sinne des § 57 Abs. 2 RStV gegeben ist, wenn der

[58] *Beucher/Leyendecker/Rosenberg*, Mediengesetze, § 16 MDStV aF, Rdnr. 9.
[59] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 41 BDSG, Rdnr. 23.
[60] *Meilinger*, Datenschutz im Bereich von Information und Dokumentation, S. 162.
[61] Vgl. *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 41 Rdnr. 26, was jedoch im Zusammenhang mit Mediendiensten, die im offenen Internet angeboten werden, regelmäßig gegeben ist.

Betroffene auch in seinem Persönlichkeitsrecht beeinträchtigt ist[62]. Im Übrigen sind aufgrund des Sinnes und Zwecks des Auskunftsrechts, dem Betroffenen eine transparente Datenverarbeitung zu garantieren und evtl. Folgeansprüche geltend machen zu können, keine zu hohen Anforderungen an die Beeinträchtigung eines schutzwürdigen Interesses zu stellen[63].

Wurden die Daten zu einem ausschließlich journalistisch-redaktionellen Zweck verarbeitet und wird der Betroffene dadurch in seinen schutzwürdigen Interessen beeinträchtigt, so hat er einen Anspruch auf Auskunft über die zugrunde liegenden, zu seiner Person gespeicherten Daten. Die Auskunft kann jedoch verweigert werden, wenn eine Gefährdung der Ausforschung des Informationsbestandes des Anbieters oder des Informantenschutzes vorliegt.

§ 57 Abs. 2 RStV räumt daher denjenigen Anbietern, die nicht schon durch andere Rechtsvorschriften (vor allem § 41 BDSG) dem Medienprivileg unterliegen, insoweit ein Vorrecht ein, dass er anstelle der weitergehenden Auskunftsansprüche nach § 34 BDSG anzuwenden ist. Er begründet dadurch zwar kein eigenes Medienprivileg, weil im Gegensatz zu § 41 BDSG das Datenschutzrecht im Übrigen anwendbar bleibt, wird jedoch als Sonderregelung zumindest als eine Art „kleines Medienprivileg“ bezeichnet[64].

[62] Im Ergebnis so auch OLG Hamm, NJW 1996, 131, nach dem davon auszugehen ist, „dass grundsätzlich durch die Speicherung und Übermittlung von Daten, die unter dem Schutz des allgemeinen Persönlichkeitsrechts stehen, schutzwürdige Belange des Betroffenen beeinträchtigt werden“.

[63] *Beucher/Leyendecker/Rosenberg*, Mediengesetze, § 16 MDStV aF, Rdnr. 11.

[64] *Roßnagel*, Recht der Multimedia-Dienste, § 20 MDStV, Rdnr. 37; dies verkennt *Lazarakos, Grigirios G.*, Das datenschutzrechtliche Medienprivileg, S. 194, welcher behauptet, dass sich § 16 Abs. 3 MDStV aF mit § 41 Abs. 3 BDSG deckt und offensichtlich keine Unterscheidung zwischen den § 20 Abs. 1 und 3 MDStV (jetzt § 13 Abs. 7 TMG und § 57 Abs. 2 RStV) vornimmt, weil er als anspruchsbegründendes Tatbestandsmerkmal für Abs. 1 eine Datenverarbeitung zu journalistisch-redaktionellen Zwecken voraussetzt. Zu den widerstreitenden Interessen zwischen Medien und Datenschutz siehe weiterführend *Eberle*, MMR 2008, 508–513; zur Anwendung des Medienprivilegs auf Bewertungsportale im Internet siehe *Greve/Schärdel*, MMR 2008, 644–650.

## 4. Auskunftsansprüche ausserhalb des BDSG und des Telemediendatenschutzes

Auskunftsansprüche ausserhalb des BDSG und der bereichsspezifischen Regelungen können sich vor allem nach den allgemeinen, zivilrechtlichen Grundsätzen ergeben. So kennt das BGB zwar keine zentrale Norm für die Auskunftspflicht, sie kann sich aber durch bestehende besondere rechtliche Beziehungen ergeben[65]. Diese sind regelmäßig bei Verträgen und gesetzlichen Schuldverhältnissen gegeben, die gesteigerte Verhaltenspflichten oder besondere Schutzpflichten zum Gegenstand haben und insbesondere bei unerlaubter Handlung[66]. Dogmatisch wurde der Anspruch zunächst entweder durch Analogie respektive weiter Auslegung einzelner gesetzlicher Vorschriften oder in Form einer aus § 242 BGB entwickelten Generalklausel hergeleitet[67], bei Verträgen auch im Wege der ergänzenden Vertragsauslegung[68]. Inzwischen wird angenommen, dass eine Herleitung nicht mehr notwendig ist, weil die Regelungsinhalte nunmehr zu Gewohnheitsrecht geworden sind[69], § 242 wird jedoch weiterhin formal zitiert.

Strittig war in der Vergangenheit hinsichtlich des gewohnheitsrechtlich anerkannten Auskunftsrechts im Bezug auf § 34 BDSG vor allem, inwiefern er neben dem Auskunftsrecht nach § 34 BDSG überhaupt noch Anwendung findet. Nach Ansicht des BGH regelt § 34 BDSG abschließend, welche Auskünfte der Betroffene bei geschäftsmäßiger Datenverarbeitung nicht-öffentlicher Stel-

[65] Zur zivilrechtlichen Einordnung von Auskunftsansprüchen siehe umfassend: *Lorenz*, JuS 1995, 569–575; *Heinrichs* in: *Palandt*, BGB, § 261, Rdnr. 3 m.w.N.; *Stadler* in: *Jauernig*, BGB, § 259, § 260 und § 261, Rdnr. 3 m.w.N.; BGH, NJW 1981, 1733.

[66] BGH, NJW 1978, 1002; zur Auskunftspflicht aus § 823 Abs. BGB beispielsweise bei Verletzung des § 12 BGB siehe auch *Bayreuther* in: *Rebmann/Säcker/Rixecker*, MüKo, § 12 BGB, Rdnr. 249.

[67] *Stürner, Rolf*, Die Aufklärungspflicht der Parteien des Zivilprozesses, S. 293.

[68] *Stürner, Rolf*, Die Aufklärungspflicht der Parteien des Zivilprozesses, S. 297.

[69] *Heinrichs* in: *Palandt*, BGB, § 261, Rdnr. 8; *Krüger* in: *Rebmann/Säcker/Rixecker*, MüKo, § 260, Rdnr. 12; *Köhler*, Der Schadensersatz-, Bereicherungs- und Auskunftsanspruch im Wettbewerbsrecht, 1477–1482, BGH, NJW 1995, 386.

len für fremde Zwecke beanspruchen kann[70]. In der Literatur wurde diese Ansicht kritisiert, da sie sich nicht, wie vom BGH behauptet, aus der Entstehungsgeschichte ergäbe[71]. Hauptauslöser dieses Meinungsstreits war jedoch wohl, dass der § 34aF BDSG den Betroffenen nicht ausreichend geschützt hat[72] und daher versucht wurde, über den Umweg der §§ 823, 242 BGB, einen Anspruch auch über die Empfänger der Daten herzuleiten. Erst nach der Novellierung des BDSG 1990 konnte der Betroffene zumindest Auskunft über die Herkunft der Daten und der Empfänger für die Fälle verlangen, in denen die Daten automatisch verarbeitet wurden, um dann nach der Umsetzung der EG-Datenschutzrichtlinie eine Erweiterung des Auskunftsrechts regelmäßig auch über Herkunft und Empfänger zu erfahren, selbst wenn er keine begründete Zweifel an der Richtigkeit der Daten hatte.

Danach ist dem BGH nach über zwanzig Jahren und einer zweimaligen Verbesserung des Auskunftsrechts für den Betroffenen beizupflichten: Da der Gesetzgeber in § 34 BDSG den genauen Umfang des Auskunftsrechts festgelegt hat, hat er diesen zum Schutz des Einzelnen für ausreichend angesehen und bleibt so für ein umfangreicheres Auskunftsrecht nach gewohnheitsrechtlich anerkannten Grundsätzen kein Raum mehr[73]. Anders verhält es sich nur, wenn sich aus den konkreten Rechtsbeziehungen der Parteien ergibt, dass der Berechtigte in entschuldbarer Weise über Art und Umfang seines Rechts im Ungewissen ist und der Verpflichtete in der Lage ist, die Auskunft ohne größere Beschwernisse zu erteilen. So ist ein Anspruch auf Benennung des Datenempfängers beispielsweise dann denkbar, wenn der Betroffene wegen der Übermitt-

[70] BGH, NJW 1984, 1886.

[71] So *Simon/ Taeger*, Umfang des Auskunftsanspruchs gegen Handelsauskunfteien - BGH, NJW 1981, 1738, 96–101, wonach in § 34 II aF BGB lediglich die Betonung gelegen habe, dass jede Übermittlung grundsätzlich unter das Gebot falle, den Empfänger auf Anfrage zu nennen, nicht aber ein Ausschluss weiterer Auskunftsansprüche.

[72] So noch *Simitis*, Datenschutz: Von der legislativen Entscheidung zur richterlichen Interpretation, 1697–1701 zur damaligen Gesetzeslage.

[73] *Canaris*, Die Feststellung von Lücken im Gesetz, S. 29 f.

lung etwa von ehrenrührigen Daten Schadensersatzansprüche nach § 823 Abs. 1 und 2 BGB geltend machen will[74].

[74] BGH NJW 1984, 1886; *Gola/Schomerus*, BDSG, § 34 BDSG, Rdnr. 3.

# F. Praktische Relevanz der Informationspflichten bei Internetnutzung

Um die hohe praktische Relevanz der unter Kapitel B. dargestellten technischen Möglichkeiten für das Datenschutzrecht besser zu veranschaulichen, soll am Beispiel des Onlinehändlers Amazons[1] illustriert werden, an welchen Stellen der technischen Nutzung eines gängigen E-Commerce-Dienstes datenschutzrechtliche Belange berührt werden, welche Informationspflichten sich daraus ergeben und von welchen Möglichkeiten Gebrauch gemacht wird, um diese zu erfüllen.

## I. Datenfluss bei Internet-Rechtsgeschäften am Beispiel von Amazon

Begibt sich ein Nutzer zum ersten Mal auf die Seite des Onlinehändlers Amazon[2], werden auf der Festplatte dessen Computers zwei Cookies abgelegt (Abbildung 6.1 auf der nächsten Seite.).

Beim ersten Besuch begrüßen die Seiten von Amazon den Nutzer noch als Neukunden und in den Cookies sind keinerlei personenbezogenen Daten gespeichert. Loggt er sich jedoch zu einem späteren Zeitpunkt mit seinem bereits vorhandenen Account ein, werden weitere Cookies abgelegt und die Seiten wer-

[1] Basierend auf der erstmalig 2005 online verfügbaren Auskunft von Amazon ggü. einem Kunden, welche unter `http://www.daten-speicherung.de` verfügbar ist und der Datenschutzerklärung von Amazon (Stand 11.2.2009).

[2] `Http://www.amazon.de`.

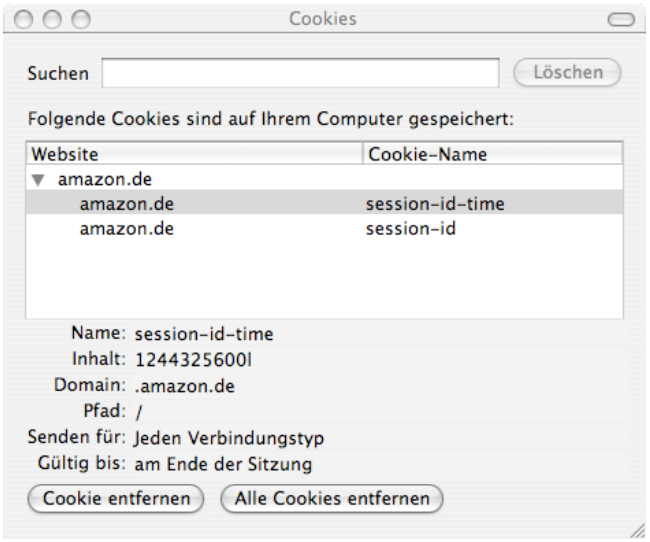


Abbildung 6.1: Cookies, die beim ersten Besuch von Amazon abgelegt werden

den von diesem Moment an individuell auf den Kunden abgestimmt dargestellt (Abbildung 6.2 auf der nächsten Seite).

Die angepassten Seiten werden auch dann angezeigt, wenn der Browser zwischendurch geschlossen und zu einem späteren Zeitpunkt erneut geöffnet wird. Ab dem Moment des Einloggens kann Amazon daher mittels der Cookies und der Daten, die er bei der Erstregistrierung für den Erhalt eines Accounts angeben muss (also den Namen und die E-Mail-Adresse), einen Personenbezug herstellen, um damit z.B. zu kontrollieren, wann der Kunde das Angebot zum letzten Mal besucht hat und ihm die in der Zwischenzeit eingetroffenen Neuerscheinungen einzublenden[3]. Ferner speichert Amazon im Weblog von Anfang an die IP-Adresse und die Informationen über den Computer wie den Browserytp, dessen Version und das Betriebssystem mit.

[3] Diese Funktion macht sich Amazon auch zunutze, s. die Datenschutzerklärung unter `http://www.amazon.de/exec/obidos/tg/browse/-/3312401/ref=cs_nav_bn_3_2/303-4640725-1478619`.


Abbildung 6.2: persönliche Begrüßung nach dem Einloggen bei Amazon

Ist der Kunde eingeloggt, wird er nun, wenn er nicht bereits ein Produkt zum Kauf ausgewählt hat, zunächst im Angebot von Amazon stöbern. Er kann dabei zum Beispiel entweder auf die verschiedenen Produktkategorien klicken oder sich der Amazon-eigenen Suchmaschine bedienen. Während der Kunde sich die verschiedenen Produkte ansieht, loggt Amazon den Clickstream mit[4]. Aus dem Clickstream generiert Amazon eine persönliche Seite des Kunden, welche z.B. kürzlich angesehenen Artikel sowie die mit der Suchanfrage verwandten Kategorien enthält.

Ist er unentschlossen, welches Produkt er kaufen soll, kann er sich zunächst die Rezensionen anderer Kunden anschauen und diese als mehr oder weniger hilfreich bewerten. Sowohl die verfassten Rezensionen als auch die Bewertungen der Rezensionen eines jeden Kunden speichert Amazon.

Hat sich der Kunde beispielsweise für ein Buch entschieden und legt es in den Warenkorb, wird der Inhalt des Warenkorbs gespeichert[5] und ergänzt, bis sich der Kunde zur Kasse begibt. Um die Bestellung abzuschließen, werden beim Kunden der Empfängername, Adresse, Telefonnummer, Versandart und die Zahlungsart (bei Versand auf Rechnung auch dessen Geburtsdatum) abgefragt. Diese bleiben auch dann im Kundenkonto gespeichert, falls der Kunde seine Meinung ändert und die Bestellung abbricht. Will der Kunde das Buch nicht für sich bestellen, sondern für einen Freund, werden auch die Adressdaten des Freundes im Kundenkonto gespeichert und verbleiben dies auch dann, wenn

[4] Zur technischen Funktionsweise des Clickstreams siehe Abschnitt B.II.1.a) auf Seite 15, zur datenschutzrechtlichen Einordnung siehe auch *Ott*, K&R 2009, 308–313.

[5] Zur technischen Funktionsweise des Warenkorbs, welcher u.a. durch Cookies bedient wird, s. unter Abschnitt B.II.1.c) auf Seite 18; zur datenschutzrechtlichen Einordnung s. unter Abschnitt D.V. auf Seite 85.

die Adresse im Nachhinein aus der Liste der möglichen Empfängeradressen gelöscht wird.

Nach Abschluss der Bestellung wird der gesamte mit dem Kunden geführte E-Mail-Verkehr (inkl. Empfangs- und Lesebestätigungen) ebenso gespeichert wie eine eventuelle Stornierung der Bestellung oder die Warenrückgabe. Hat der Kunde nicht bei Amazon selbst eingekauft, sondern über einen Drittanbieter, wird der Kunde nach einiger Zeit aufgefordert, diesen zu bewerten[6]. Die abgegebene Bewertung wird ebenfalls im Kundenkonto gespeichert.

Entscheidet sich der Kunde, selbst Ware über Amazon zu verkaufen, werden auch hier sämtliche Transaktionen gespeichert: gelistete und verkaufte Ware, Käufer der Ware, Zeitpunkt des Kaufs, Kaufpreis, Versandpreis, Bezahlstatus und auch hier die jeweiligen Bewertungen. Für die Erstregistrierung zum Amazon Marketplace muss der Verkäufer darüber hinaus seine in Deutschland gültige Kreditkarte, seine deutsche Bankverbindung, seine Rechnungsadresse und seine Telefonnummer angeben, unter der er vor Abschluss der Registrierung von Amazon angerufen wird.

Sämtliche Daten verbleiben auf unbestimmte Zeit bei Amazon Deutschland und werden darüber hinaus an Amazon in den USA, England, Frankreich, Japan, Österreich und Kalifornien weitergeleitet[7].

### 1. Rechtliche Einordnung der einzelnen Dienstmerkmale

Anhand des soeben dargestellten Besuchs eines Kunden in einem Online-Handel sollen im Folgenden die einzelnen Dienstmerkmale aufgeschlüsselt werden, um im Anschluss die daraus resultierenden Informationspflichten erörtern zu können[8].

[6] Zur datenschutzrechtlichen Einordnung von Bewertungsportalen siehe *Ballhausen/Roggenkamp*, K&R 2008, 403–410; *Greve/Schärdel*, MMR 2008, 644–650.

[7] Siehe auch dazu die Datenschutzerklärung von Amazon.

[8] Wie bereits unter Abschnitt C.III.2. auf Seite 61 dargestellt, muss bei umfangreichen Internetprodukten, wie hier eines vorliegt, jedes Dienstmerkmal dem jeweiligem Gesetz einzeln

Da seit Einführung des TMG nunmehr alle elektronischen Informations- und Kommunikationsdienste, die nicht Telekommunikationsdienste oder Rundfunk sind, Telemedien sind (§ 1 Abs. 1 TMG), handelt es sich beim Verkaufsangebot von Amazon um Telemedien. Es handelt sich dabei um ein „Angebot von Waren in elektronisch abrufbaren Datenbanken mit interaktiven Zugriff und unmittelbarer Bestellmöglichkeit“, welches schon im Beispielskatalog des § 2 Abs. 2 TDG aufgelistet war.

Ebenso nunmehr eindeutig als Telemedien einzuordnen sind die Rezensionen, die Warenkorbfunktion und die Bestellmöglichkeit[9].

Beim Übersenden der Daten zur Bezahlung ist hingegen grundsätzlich zu unterscheiden: Werden, wie bei Amazon, verschiedene Möglichkeiten zur Bezahlung angeboten, ist von einem eigenen Telemediendienst auszugehen[10]. Anders verhält es sich jedoch, wenn die Bezahlung sich auf das Ausfüllen eines vorgegebenen Formulars auf einen bestimmten Zahlungsweg beschränkt oder, wie bei einigen Online-Händlern der Fall, lediglich die Zahlung per Nachnahme vorgesehen ist. In diesen Fällen ist eine interaktive Einwirkungsmöglichkeit mittels des Nutzers im Wege der Individualkommunikation nicht gegeben und die Bezahlung ist daher dann dem Telemediendienst des Warenangebots mit Bestellmöglichkeit zuzurechnen[11].

Nach der Abgabe der Bestellung erhält der Nutzer von Amazon eine Bestätigungs-E-Mail. Diese dient zur Einhaltung der Pflicht gemäß § 312e Abs. 1 S. 1 Nr. 3 BGB und ist ein eigener Telemediendiest. Einen weiteren Telemediendienst, den Amazon den Kunden bietet, um sich über deren Produkte

zugeordnet werden; vgl. dazu auch BT-Drs. 13/7385, S. 53 sowie *Scholz*, Datenschutz beim Internet-Einkauf, S. 154 ff.

[9] Abgrenzungsschwierigkeiten gab es hingegen nach der alten Rechtslage, unter der stets eine Einordnung entweder als Teledienst, mit der Folge der Anwendbarkeit des TDG und des TDDSG oder als Mediendienst, mit der Folge der Anwendbarkeit des MDStV vorgenommen werden musste.

[10] So auch *Holznagel/Hoeren*, Rechtliche Rahmenbedingungen des elektronischen Zahlungsverkehrs, Rdnr. 420.

[11] Vgl. *Scholz*, Datenschutz beim Internet-Einkauf, S. 173.

zu informieren, ist die regelmäßige Übersendung von Newslettern zu einer bestimmten Thematik (Abbildung 6.3).

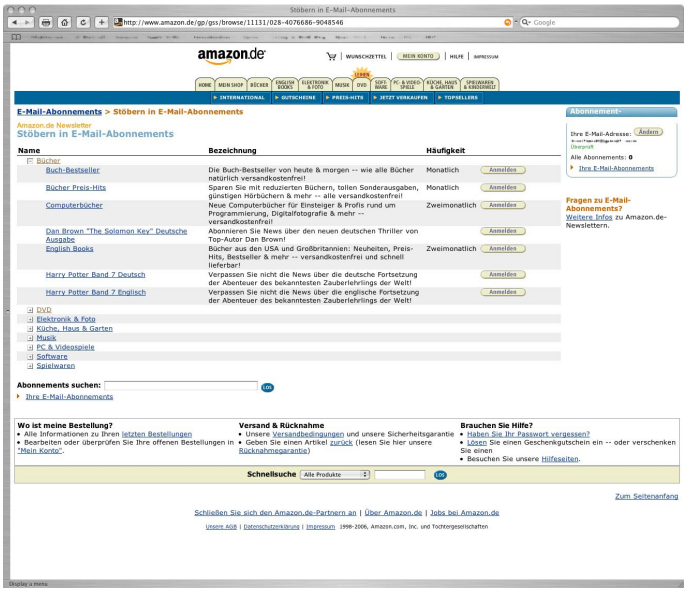


Abbildung 6.3: Newsletterstruktur bei Amazon

Zu betonen ist jedoch, dass die genannten Dienste streng vom Inhalt abzugrenzen sind, der durch sie ausgetauscht wird: So ist der Dienst, mittels dem die Produkte bestellt werden, zwar ein Telemediendienst. Die Daten, die zur Erfüllung des Kaufvertrages erhoben werden, sind dagegen Inhaltsdaten und nach dem BDSG zu bewerten. Gleiches gilt für den Telemediendienst zur Bezahlung: Die Daten, die in das Web-Formular eingetragen werden und aus denen Amazon die Zahlungsmodalitäten ersehen kann, beim Lastschriftverfahren z.B. Kontoinhaber, Kontonummer, BLZ und Bank, sind nach dem BDSG zu beurteilen[12].

[12] Vgl. *Spindler/Wiebe*, Internet-Auktionen, S. 266; *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 2 TDDSG, Rdnr. 61; *Schaar*, Datenschutz im Internet, Rdnr. 465; *Engel-Flechsig* in: *Engel-Flechsig/Maennel/Tettenborn*, Beck'scher IuKDG-Kommentar, Einf. TDDSG, Rdnr. 32.

In den Fällen, in denen der Amazon Marketplace genutzt wird, ist die Verkaufsplattform ein Telemediendienst, bei welcher der Nutzer im Falle eines erfolgreichen Verkaufs Gebühren an Amazon abführen muss. Hierzu schließt der Kunde, der über den Marketplace seine Ware verkauft, mit Amazon einen Maklervertrag mit dienstvertraglicher Komponente[13]. Ebenso handelt es sich beim sog. „Amazon Payments" System um einen Telemediendienst: Entsteht über den Amazon Marketplace ein Kaufvertrag, belastet Amazon die Kreditkarte oder das Konto des Käufers und schreibt sie dem Amazon-Payments-Konto des Verkäufers gut. Dieser kann daraufhin eine Überweisung des Betrages auf sein Bankkonto veranlassen[14]. An den Verkäufer werden daher lediglich die Adress-, nicht aber die Bankdaten des Käufers übermittelt. Da sie dem Verkäufer zum Zwecke der Kaufvertragsabwicklung mitgeteilt werden, fallen sie wiederum in den Anwendungsbereich des BDSG[15].

Etwas anderes ergibt sich jedoch bei den Bewertungen, die sich Kunden und Verkäufer gegenseitig nach der Abwicklung des Vertrages geben können und deren Sinn es ist, den zukünftigen Käufern/Verkäufern einen Anhaltspunkt für die Zuverlässigkeit des jeweiligen Käufers/Verkäufers anzubieten. Es handelt sich hier zwar um Daten, welche die Vertragsabwicklung betreffen und daher größtenteils aus einem „Offline-Verhalten" resultieren. Die Bewertungsplattform selbst stellt jedoch einen Telemediendienst dar, vergleichbar mit den Rezensionen, mittels derer die Qualität von (Offline-)Gegenständen bewertet werden kann. Der Bezug zu dem sich nach BDSG zu beurteilenden Rechtsgeschäft ist hier nur mittelbar und kann an diesem Ergebnis nichts ändern[16].

[13] Vgl. *Meyer/ Mönig*, Die vertragstypologische Einordnung von Online-Auktionen, S. 98 ff.; *Spindler/ Wiebe*, Internet-Auktionen, S. 54 ff.; *Huppertz* in: *Bräutigam/Leupold*, Online-Handel, B IV Rdnr. 31 ff.

[14] Die rechtliche Einordnung entspricht bei dieser Zahlungsmethode derjenigen des eCashs, für die es verschiedene Erklärungsansätze gibt. Da jedoch sämtliche Ansätze nichts an der Eigenschaft des Amazon Payments als Telemediendienst ändern, sei an dieser Stelle zur Vertiefung lediglich auf *Werner, Stefan*, Geldverkehr im Internet, S. 155 ff., verwiesen.

[15] Vgl. auch *Spindler/ Wiebe*, Internet-Auktionen, S. 266.

[16] A.A., jedoch ohne weitergehende Begründung *Spindler/ Wiebe*, Internet-Auktionen, S. 267.

## 2. Erhebung, Verarbeitung und Nutzung von personenbezogene Daten im Rahmen der verschiedenen Dienste

Im Rahmen der Erstregistrierung werden der Name und die E-Mail-Adresse erhoben und gespeichert. Dabei stellt der Name des Kundens ein personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG dar, mittels dessen die E-Mail-Adresse personenbeziehbar wird und damit ebenfalls datenschutzrechtlich geschützt ist[17]. Gleiches gilt ab diesem Zeitpunkt auch für bereits auf der Festplatte abgelegte Cookies, welche nach Angaben von Amazon dem Zwecke der Präsentation der seit dem letzten Zeitpunkt eingetroffenen Neuerscheinungen dienen und für diejenigen Cookies, die zum automatischen Einloggen des Kunden bei einem späteren Besuch mit dem selben Computer führen[18]. Die Notwendigkeit des direkten Zusammenhangs mit dem Nutzeraccount und der daraus resultierende Personenbezug ergeben sich hier bereits aus dem Zweck der Speicherung des jeweiligen Cookies.

Von diesem Zeitpunkt an wird ferner bei jedem Surfvorgang, der im eingeloggten Zustand stattfindet, im Clickstream[19] die genaue Spur verfolgt, die der Kunde zum Auffinden eines Produkts oder beim einfachen Stöbern des Shops hinterlässt. Der Personenbezug wird in diesem Fall dadurch hergestellt, dass in jedem Eintrag die Kundennummer vermerkt wird, die dem Nutzer bei der Erstregistrierung automatisch zugewiesen wurde. Im Weblog werden IP-Adressen, Betriebssystem sowie Browsername und -version gespeichert. Da im Rahmen der bisher genannten Daten die Ebene der Telemedien zu keinem Zeitpunkt verlassen wurde, bestimmt sich die Zulässigkeit der Erhebung, Verarbeitung und Nutzung ausschließlich nach dem TMG.

Weiterhin werden im Verlauf der Bestellung in der Datenbank die Empfängeradresse (insoweit auch die Adresse eines eventuell durch den Kunden Be-

[17] Zum Personenbezug von E-Mails siehe unter Abschnitt D.III. auf Seite 80.
[18] Siehe dazu schon unter Abschnitt F.I. auf Seite 117.
[19] Vgl. Abschnitt B.II.1.a) auf Seite 15.

schenkten), Telefonnummer, Versandart, Zahlungsart und evtl. Geburtsdatum des Kunden angelegt. Diese personenbezogenen Daten bestimmten sich nach dem BDSG, wobei zu beachten sein wird, dass der bei der Erstregistrierung angegebene Name des Kundens zunächst bei einem Telemediendienst erhoben und gespeichert wurde, bei der Bestellung hingegen eine Weiterverarbeitung stattfindet, die in den Anwendungsbereich des BDSG fällt.

Weitere Daten, die in der Datenbank gespeichert werden, sind der gesamte E-Mail-Verkehr, die Stornierung einer Bestellung oder eine Warenrückgabe nebst jeweiligem Grund, eine zu einer Bestellung eines Drittanbieters abgegebene Bewertung, jede Bewertung, die der Nutzer selbst als Verkäufer bei Nutzung des Amazon-Marketplaces seitens Dritter erhält und der Inhalt abgegebener Rezensionen. Bei der Einordnung dieser Daten kann im Wesentlichen auf das bereits Ausgeführte verwiesen werden: Der E-Mail-Verkehr, wenn es sich um Bestellbestätigungen, Versandbestätigungen oder Reklamationen handelt, ist nach dem BDSG zu beurteilen. Gleiches gilt für die Transaktionsdaten des Amazon-Marketplace. Hier wird Amazon zum einen als Übermittler der Daten zwischen Verkäufer und Käufer tätig[20], zum anderen werden vor allem die Daten über den jeweiligen Vertragsgegenstand von Amazon zu eigenen Zwecken der Werbung weiterverarbeitet.

Die Bewertungen, die nach Abwicklung des Vertrages über den Amazon Marketplace von den Parteien abgegeben werden, bestimmen sich wiederum nach dem TMG[21].

[20] Vgl. hierzu auch die Einordnung von *Andexer/Lehmann*, Datenschutzrechtliche Aspekte bei Online-Auktionen, 185–236.

[21] Zur Einordnung der Bewertungsplattform als Telemediendienst siehe Abschnitt F.I.1. auf Seite 120.

## 3. Aus der Erhebung, Speicherung und Nutzung der Daten entstehende Informationspflichten

Vor diesem Hintergrund ist nach den aus der einzelnen Diensten resultierenden Informationspflichten zu fragen.

### a) Informationspflichten, die bei der Verwendung von Cookies entstehen

Hinsichtlich der seitens Amazon abgelegten Cookies ist dahingehend zu unterscheiden, ob deren Inhalt einen (späteren) Personenbezug ermöglicht oder nicht. In dem Umfang, in dem sie eine spätere Identifizierung des Nutzers ermöglichen, entsteht die Unterrichtungspflicht des § 13 Abs. 1 S. 2 TMG. Die Unterrichtungspflicht hat zu Beginn des automatischen Verfahrens zu erfolgen. Der Zeitpunkt muss dabei so gewählt sein, dass der Nutzer Maßnahmen ergreifen kann, um eine spätere Identifizierung zu verhindern[22]. Eine Möglichkeit, der Unterrichtungspflicht gerecht zu werden, wäre hier, vor dem Ablegen des ersten Cookies mit personenbeziehbarem Inhalt, mittels eines gesonderten Browserfensters[23], darüber zu unterrichten, dass in einem nächsten Schritt ein Cookie auf der Festplatte des Nutzers abgelegt wird. Ferner müsste der Nutzer Kenntnis darüber erlangen, welche Art von Daten im Cookie gespeichert werden (hier z.B. Customer-ID als Nutzungsdatum), in welchem Umfang (hier vor allem Vorhaltezeit des Cookies) und zu welchem Zweck sie gespeichert werden (Ermöglichen der späteren Identifikation des Kundens zum Zwecke des automatischen Einloggens/Anzeigen der Neuvorstellungen). Darüber hinaus müsste der Nutzer, um § 13 Abs. 6 S. 2 TMG gerecht zu werden, darauf hingewiesen werden, dass er auf das Ablegen der Cookies auch verzichten kann.

[22] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 192.
[23] So der Vorschlag der Artikel 29-Arbeitsgruppe der EU-Datenschutzbeauftragten im WP 37, 47.

Durch das spätere Empfangen der Cookies durch Amazon wird der Personenbezug zu einem künftigen Zeitpunkt tatsächlich hergestellt und die Daten dann erstmalig erhoben werden. Es erscheint also überdies geboten, bereits an dieser Stelle auch darüber zu informieren, dass jede spätere Erhebung der Einwilligung bedarf, welchen Zweck die Erhebung verfolgt (§ 4a Abs. 1 S. 2 BDSG; wobei dieser mit dem Zweck des Ablegens identisch ist) und dass die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann (§ 13 Abs. 3 TMG). Diese Vorgehensweise empfiehlt sich vor allem aus dem Grund, weil sich der Gesetzgeber mit der Wahl der Voraussetzung der *Einwilligung* eindeutig auf die Notwendigkeit einer der Datenverarbeitung vorausgehenden Handlung des Rechtsinhabers festgelegt hat. Die Möglichkeit einer nachträglichen Zustimmung zur Heilung einer wegen Fehlens der Einwilligung zunächst unzulässigen Datenverarbeitung ist dabei ausgeschlossen[24].

Gewiss stellt sich schon jetzt die Frage der Praktikabilität der faktischen Umsetzung der Informationspflichten. Die datenschutzrechtliche Verwendung eines Cookies ist grundsätzlich dreigegliedert: So liegt beim Ablegen, sofern das Cookies bereits personenbeziehbaren Inhalt enthält, ein Speichern vor[25], das Senden des Cookies vom Browser des Nutzers stellt eine Nutzung dar[26] und durch das Empfangen der Daten findet letztendlich die Erhebung statt. Probleme ergeben sich daraus insofern, dass die Unterrichtung nach § 13 Abs. 1 S. 2 TMG nicht nur bei der ersten Initiierung des automatischen Verfahrens stattzufinden hat, sondern jedes Mal, wenn das automatische Verfahren

[24] *Schaffland/Wiltfang*, BDSG, § 4a BDSG, Rdnr. 2f., mit dem Hinweis, dass eine nachträgliche Genehmigung jedoch Folgen auf die Möglichkeit der Geltendmachung zivilrechtlicher Ansprüche haben kann.

[25] Dass das Speichern hier auf der Festplatte des Nutzers „ausgelagert" wird, ändert nichts, da der Tatbestand des Speicherns nicht vorschreibt, wo sich der Datenträger zu befinden hat und die spätere Möglichkeit der Kenntnisnahme der speichernden Stelle unter normalen Umständen möglich bleibt, s. dazu bereits unter Abschnitt D.V. auf Seite 85.

[26] Nicht hingegen liegt eine Übermittlung vor, da es für eine Übermittlung an einem Dritten fehlt. Nach § 4 Abs. 8 S. 2 BDSG ist die verantwortliche Stelle, also die Stelle, an die das Cookie gesendet wird, gerade nicht Dritter. Dies scheint *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 204, zu übersehen.

beginnt, eine in Hinblick auf eine spätere Identifizierung oder eine Erhebung, Verarbeitung oder Nutzung relevante Funktion auszulösen[27]. Während § 4 Abs. 3 BDSG eine Ausnahme von der Unterrichtungspflicht für die Fälle vorsieht, in denen der Betroffene von der Erhebung der Daten bereits auf andere Weise Kenntnis erlangt hat, sieht das TMG eine solche nicht vor. Im Hinblick auf eine praktikable Lösung muss hier jedoch die Unterrichtungspflicht zumindest dann erfüllt sein, wenn der Nutzer beim ersten Besuch umfassend unterrichtet und ihm dann die Wahl gelassen wird, ob er in Zukunft vor jedem Verfahren erneut das Öffnen eines Browserfensters mit der Unterrichtung wünscht oder ob es ihm genügt, diese jederzeit einsehen zu können, wie es durch § 13 Abs 1 S. 3, Abs. 3 S. 2 TMG ohnehin vorgeschrieben ist. Dies ist jedenfalls dann anzunehmen, wenn der Nutzer die anfangs getroffene Wahl in seinen Benutzereinstellungen jederzeit ändern kann.

Dafür spricht auch die Gesetzesbegründung zum EGG, in welcher der Gesetzgeber hinsichtlich der Unterrichtungspflicht des § 4 Abs. 1 S. 1 TDDSG (jetzt § 13 Abs. 1 S. 1 TMG) klargestellt hat, dass es einer Wiederholung der Unterrichtung bei jeder erneuten Nutzung aufgrund der sich aus § 4 Abs. 1 S. 3 TDDSG ergebenden Pflicht zur jederzeitigen Abrufbarkeit der Unterrichtung gerade nicht bedarf. Zwar stellt ein automatisiertes Verfahren eine ungleich größere Bedrohung der informationellen Selbstbestimmung als die Nutzungsvorgänge gemäß § 13 Abs. 1 S. 1 TMG dar und bezieht sich die Aussage des Gesetzgebers daher explizit nur auf diese. Die Bedrohung kann jedoch insofern auf ein angemessenes Maß geschmälert werden, als dass sich die Unterrichtung im Zusammenhang mit den Cookies auch darauf erstrecken muss, wann durch deren Verwendung in Einzelnen, auch mit Blick auf zukünftige Nutzungsvorgänge, eine spätere Identifizierung des Nutzers ermöglicht bzw. eine Erhebung, Verarbeitung oder Nutzung personenbezogenen Daten vorbereitet wird.

[27] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 193.

### b) Informationspflichten bei der Nutzung des Amazon Marketplaces und Amazon Payments

Bei der Nutzung des Amazon Marketplaces und Amazon Payments kommen zwischen Amazon und dem Nutzer Verträge zustande[28]. Bei den Daten, die Amazon erhebt, verarbeitet oder nutzt, um die Begründung, inhaltliche Ausgestaltung oder Änderung dieser Verträge zu ermöglichen, handelt es sich daher um Bestandsdaten, im Sinne des § 14 TMG, die Amazon auch ohne Einwilligung erheben darf. Zu beachten ist hier aber besonders das Kriterium der Erforderlichkeit. Erforderlich ist hinsichtlich des Dienstes Amazon Marketplace auf Seiten des Verkäufers eine Kontaktmöglichkeit, unter der er zur Benachrichtigung über einen erfolgreichen Verkauf erreichbar ist und an welche Name und Lieferadresse des Käufers weitergeleitet werden können. Ferner benötigt Amazon vom Verkäufer beim jeweiligen Einstellen der Ware deren Beschreibung sowie den für die Ware geforderten Preis. Für die Übermittlung an den Verkäufer benötigt Amazon den Namen des Käufers, die Bezeichnung der bestellten Ware und seine Lieferadresse. Soweit Amazon den geforderten Preis dazu verwendet, die aus dem Verkauf für den Verkäufer an Amazon zu zahlende Vergütung zu errechnen, handelt es sich nicht um Bestandsdaten, sondern um Daten, welche zum Zwecke der Abrechnung erforderlich sind[29] (sog. Abrechnungsdaten gem. § 15 Abs. 6 TMG), bei denen es sich um eine Unterkategorie der Nutzungsdaten handelt.

Für den Dienst Amazon Payments erforderlich sind beim Verkäufer die Erhebung und Verarbeitung seiner Bankverbindung, auf die Amazon das Geld auf Anforderung überweisen soll, beim Käufer hingegen, da eine anonyme bzw. pseudonyme Zahlung nicht angeboten wird, je nach Zahlungsart die Daten seiner Bankverbindung oder der Kreditkarte.

[28] Siehe Abschnitt F.I.1. auf Seite 120.
[29] Vgl. *Andexer/Lehmann*, Datenschutzrechtliche Aspekte bei Online-Auktionen, S. 210.

Hinsichtlich dieser Daten entsteht zu Beginn des Nutzungsvorgangs die Unterrichtungspflicht aus § 13 Abs. 1 S. 1 TMG, da das Erheben von Bestands- und Nutzungsdaten zwar von der Notwendigkeit des Vorliegens einer Einwilligung des Nutzers, nicht aber von der allgemeinen Unterrichtungspflicht befreit. Weitergehende Informationspflichten bei der Nutzung vom Amazon Marketplace und Amazon Payments entstehen mithin bezüglich der Daten, deren Erhebung nicht erforderlich ist und der zwar rechtmäßig ohne Einwilligung erhobenen und verarbeiteten Daten, wenn diese über den Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung bzw. dem der Abrechnung hinaus gespeichert werden. Amazon speichert vom Verkäufer über den Namen, die E-Mail-Adresse, die Login-Daten und die Bankverbindung hinaus, auch seine Adresse, seine Telefonnummer und die Daten seiner Kreditkarte (u. a. um im Falle des Missbrauchs die Identität des Verkäufers zu kennen). Ferner bleiben auch nach dem erfolgreichen Abschluss des Kaufvertrages sowie Überweisung des Geldes an den Verkäufer sämtliche Transaktionsdaten gespeichert und werden zu weiteren Zwecken (z.B. Werbung) weiterverarbeitet. All diese Verarbeitungsvorgänge setzen eine Einwilligung der Nutzer voraus, woraus sich die Informationspflichten der § 4a Abs. 1 S. 2 BDSG und des § 13 Abs. 3 TMG ergeben.

### c) Informationspflichten bei der Erstregistrierung und Nutzung der Telemediendienste

Die bei der weiteren Nutzung der verschiedenen Teledienste anfallenden Daten lassen sich zusammenfassen, da sie keine Besonderheiten bergen. Hinsichtlich Ihrer entstehen wiederum für die Einwilligung, soweit diese nicht entbehrlich ist, weil die Daten aufgrund des TMG oder einer anderen Rechtsvorschrift erhoben wurden, die Informationspflichten des § 4a Abs. 1 S. 2 BDSG und des § 13 Abs. 3 TMG und für die eigentliche Erhebung, Verarbeitung oder Nutzung die des § 13 Abs. 1 S. 2 TMG. Zu denken ist hier in erster Linie

an § 15 TMG. § 14 TMG scheidet hingegen aus, da abgesehen von Amazon Marketplace und Amazon Payments die einzigen Verträge, die mit Amazon geschlossen werden, die Kaufverträge im Rahmen der Bestellung sind, welche sich nach dem BDSG richten. Als Nutzungsdatum kommt wiederum lediglich die IP-Adresse und der Inhalt der HTTP-Anfrage zumindest in dem Umfang, in der er für die Kommunikation zwischen dem Server von Amazon und dem Client des Nutzers vonnöten ist, in Frage. Das bedeutet im Umkehrschluss, dass jede über die für die Inanspruchnahme der Teledienste absolut notwendige Speicherung hinausgehende Verarbeitung, also die Speicherung des Betriebssystems, der Browser-Art und dessen Sprache wie auch die des Clickstreams, nicht von § 15 TMG erfasst sind. So sind zwar alle eben genannten Daten grundsätzlich den Nutzungsdaten zuzurechnen, es scheitert aber am von § 15 TMG vorausgesetzten Kriterium der Erforderlichkeit. Nach eigener Aussage speichert Amazon die Daten unter anderem, um daraus Profile zu erstellen, die es ermöglichen sollen, dem Kunden Waren und Dienstleistungen zu empfehlen, ihn daher zu bewerben. Für die Erstellung von Nutzungsprofilen zum Zwecke der Werbung hat sich der Gesetzgeber bewusst im Bereich der Teledienste für den im Vergleich zu § 28 Abs. 3 Nr. 3 BDSG restriktiveren § 15 Abs. 3 TMG entschieden[30]. Dessen Voraussetzungen sind jedoch im Rahmen der Nutzungsprofile, welche durch Amazon erstellt werden, nicht erfüllt, da die Erstellung nicht unter Verwendung von Pseudonymen vonstatten geht, sondern ein direkter Personenbezug möglich ist. Aufgrund der Tatsache, dass dadurch ein wesentlich größerer Eingriff in das Recht auf informelle Selbstbestimmung entsteht als vom Gesetzgeber eigentlich vorgesehenen, ist bei der Formulierung der Informationspflichten ein verstärktes Augenmerk darauf zu richten, dass der Nutzer im Gegenzug besonders umfassend unterrichtet wird.

Gleiches gilt für den bei der Erstregistrierung anzugebenden Vor- und Nachnamen des Nutzers sowie, soweit ein Personenbezug hergestellt werden kann,

[30] Siehe dazu bereits unter Abschnitt D.VI.1.a) auf Seite 88.

die E-Mail-Adresse, solange diese noch nicht in Zusammenhang mit einer Warenbestellung angegeben werden.

### d) Informationspflichten bei Abschluss und Abwicklung des Kaufvertrages

Anders verhält es sich jedoch, bei den Daten, die im Zusammenhang mit der Bestellung erhoben, verarbeitet und genutzt werden. Für sie ist das TMG nicht anwendbar, so dass sich die Zulässigkeit nach § 28 BDSG bestimmt. Dieser erlaubt die Erhebung als Mittel für die Erfüllung eigener Geschäftszwecke, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient (Abs. 1 Nr. 1). Hierzu zählt der Name des Betroffenen, die Lieferadresse, die Bank-/Kreditkartendaten, der Zeitpunkt des Bestellung, die Versandart, die bestellte Ware und deren Preis[31]. Da Amazon die Pflicht zur unverzüglichen Bestätigung des Zugangs der Bestellung auf elektronischem Wege trifft (§ 315e Abs. Nr. 3 BGB), gehört dazu ebenfalls die E-Mail-Adresse des Kundens. Nicht darunter fallen hingegen das Geburtsdatum des Kundens (welches erhoben wird, falls der Kunde auf Rechnung bestellt) und dessen Telefonnummer. Die zulässige Länge der Speicherung der Daten bestimmt sich wiederum nach der Erreichung des Zwecks. Bei den mit Amazon abgeschlossenen Kaufverträgen, denen die Erhebung und Verarbeitung der Kundendaten zunächst dient, ist eine Speicherung zumindest während des Fristenlaufs eventueller Gewährleistungsansprüche gegeben[32].

Da Amazon die Daten über die Abwicklung des Vertrages hinaus auch für Werbezwecke weiterverarbeitet, ist die Zulässigkeit diesbezüglich nach § 28 Abs. 1 Nr. 2 BDSG zu prüfen. Danach ist die weitere Verarbeitung dann zulässig, soweit es zur Wahrung berechtigter Interessen Amazons erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse

[31] Vgl. *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 551.
[32] *Breinlinger* in: *Roßnagel*, Handbuch Datenschutzrecht, 7.6 Rdnr. 42.

des Betroffenen an dem Ausschluss der Verarbeitung überwiegt. Berechtigtes Interesse setzt dabei kein rechtliches Interesse voraus, ein wirtschaftliches Interesse, wie es bei der Werbung[33] der Fall ist, genügt[34]. Der Schwerpunkt der Prüfung der Zulässigkeit liegt hier bei der Interessenabwägung, namentlich inwiefern schutzwürdige Interessen der Kunden nicht dem der Verarbeitung der Daten zu Werbezwecken überwiegen. Problemlos möglich ist es unter diesem Gesichtspunkt, anhand der bestellten Waren den Kunden in bestimmte Kategorien-Listen einzutragen (z.B. Krimis, Thriller, historische Romane) und diese bei späteren Besuchen verstärkt auf der Begrüßungsseite des Kundens einzubauen oder ihm dahingehende Empfehlungen einzublenden[35]. Zulässig, weil den Kunden nicht in seinem Recht auf informationelle Selbstbestimmung beeinträchtigend, ist ferner, beim Kauf mehrerer Titel aus einer Kategorie diese unter Verwendung anonymisierter Listen weiterzuverarbeiten, um auf diese Weise anderen Kunden, die den Kauf eines der Titel erwägen, auch den der weiteren in diesem Zusammenhang erworbenen Waren vorzuschlagen.

Unzulässig wäre eine weitere Verarbeitung jedoch dann, wenn die Waren aus verschiedenen Kategorien auf eine Weise zusammengeführt würden, die zu einer Analyse der Persönlichkeit der Kunden mit dem Ziel eines „gläsernen Konsumenten“ anstrebt[36]. Für jede über die Grenzen der Abwägung nach § 28 Abs. 1 Nr. 2 BDSG hinausgehende Verarbeitung zu Werbezwecken ist daher erneut die Einwilligung des Betroffenen von Nöten. Die Einholung der Einwilligung des Kundens wird bei groß angelegten Online-Shops wie Amazon aus diesem Grund generell anzuraten sein, weil die Datenmenge, die im Laufe häufig über Jahre andauernde Geschäftsbeziehungen anfällt, überdies meist mit den im Rahmen der Nutzung der Teledienste entstandenen Daten kombiniert

[33] *Wolber*, Zulässigkeit der Werbung mit Adressen aus Online-Bestellungen, 16–18.
[34] BGH NJW 1984, 1886.
[35] Vgl. ein ähnliches Beispiel in *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 128.
[36] *Scholz* in: *Roßnagel*, Handbuch Datenschutzrecht, 9.2 Rdnr. 100; *Tinnefeld/Ehmann/-Gerling*, Einführung in das Datenschutzrecht, S. 560.

wird. Bei letzteren ist eine Verarbeitung ohnehin nur mit Einwilligung zulässig, die Kombination wird indes die Grenzen der Interessenabwägung schnell sprengen. Dies ist vor allem immer dann der Fall, wenn sich Unternehmen der Customer Relationship Methoden des Data Warehousing und Data Minings bedienen, mittels derer große Datenmengen zunächst gespeichert und anschließend gezielt analysiert werden, falls in diesen wie üblich auch personenbezogene Daten verarbeitet werden sollen[37]. Darüber hinaus ist der Betroffene in jedem Fall auch nach § 28 Abs. 4 S. 2 über sein Widerspruchsrecht zu unterrichten.

### e) Informationspflichten bei Übermittlung von personenbezogenen Daten an Dritte

Amazon gibt nach eigenen Angaben personenbezogene Daten an verbundene Unternehmen, Partnerunternehmen, Dienstleister, Unternehmen, die auf Minimierung von Kreditkartenbetrug spezialisiert sind und im Falle der Übertragung von Geschäftsteilen weiter.

Hierbei ist zunächst anzumerken, dass es für die datenschutzrechtliche Beurteilung keinen Unterschied macht, ob Amazon die Daten an verbundene Unternehmen, Partnerunternehmen oder im Falle der Übertragung von Geschäftsteilen (bei Kauf oder Verkauf von Unternehmensteilen) übermittelt werden, da für Konzerne zwar handels- und wirtschaftsrechtliche Sonderbestimmungen existieren, beim Datenschutz jedoch die allgemeinen Bestimmungen gelten, aus denen sich ergibt, dass ein Konzern keine einzelne nicht-öffentliche Stelle ist, sondern aus vielen nicht-öffentlichen Stellen besteht[38]. Dementsprechend sind sämtliche Stellen untereinander Dritte im Sinne des § 3 Abs. 8 S. 2 BDSG[39] und ist die Übermittlung nur in den Grenzen des § 28 BDSG bzw. mit Ein-

[37] Weiterführend zum Datenschutz im Zusammenhang mit Data Warehousing und Data Mining: *Scholz* in: *Roßnagel*, Handbuch Datenschutzrecht, 9.2; *Hahn*, Data Warehousing und Data Mining in der Praxis, 605–608; *Hoeren* in: *Kilian/Heussen*, Computerrechts-Handbuch, Rdnr. 18-19.

[38] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 2 BDSG, Rdnr. 52 ff.

[39] Vgl. *Büllesbach* in: *Bräutigam/Leupold*, Online-Handel, A III Rdnr. 70.

willigung des Betroffenen zulässig. Soweit Amazon sich Tochterunternehmen zur Erfüllung der Kaufverträge bedient, ergibt sich die Zulässigkeit aus § 28 Abs. 1 Nr. 1 BDSG. Anders verhält es sich jedoch mit den Daten des Kundens, wie die Login-Daten, Kreditkartendaten, Adressdaten, die Amazon.de an Amazon.com, Amazon.co.uk, Amazon.fr, Amazon.at und Amazon.ca übermittelt. Diese Übermittlung dient weder der Zweckbestimmung eines Vertragsverhältnisses, noch ist sie für die Wahrung berechtigter Interessen von Amazon.de (§ 28 Abs. 1 Nr. 2 BDSG) erforderlich. Sie dient vielmehr dem Zweck, dass der Kunde bei den Unternehmen anderer Länder Bestellungen vornehmen kann, ohne seine Daten erneut angeben zu müssen. Eine im Zusammenhang von mehrfachen Vertragsbedingungen eventuell zukünftig erforderliche Datenerhebung fällt aber mithin nicht unter § 28 Abs. 1 Nr. 1 BDSG, sondern stellt eine Zweckänderung dar, welche nur unter erneuter Prüfung und Bejahung einer in § 28 genannten Zulässigkeitsalternativen gestattet ist. Dies käme allenfalls zu einem eventuell späteren Zeitpunkt in Betracht, wenn es tatsächlich zu einer Bestellung in einem anderen Land kommt und nicht etwa bereits dann, wenn die Übermittlung stattfindet[40]. Die Übermittlung der Daten bedarf daher der Einwilligung und ist nur unter der Voraussetzung der ausreichenden Unterrichtung gemäß §§ 4 Abs. 3 S. 1, 4a Abs. 1 S. 2 BDSG zulässig.

Bezüglich der Übermittlung der personenbezogenen Daten an Unternehmen, die auf Minimierung von Kreditkartenbetrug spezialisiert sind, ist ein berechtigtes Interesse im Sinne des § 28 Abs. 1 Nr. 2 BDSG vonseiten Amazons hingegen bei Bezahlung mit Kreditkarte und in dem Umfang, wie sie zur Erreichung der Minimierung des Betruges notwendig ist, gegeben. Dieses Interesse ergibt sich schon allein aus dem Grund, dass Vertragsunternehmen gegenüber Acquirern im Falle eines Kreditkartenmissbrauchs durch unbekannte Dritte das Risiko zumindest anteilig tragen[41]. Das schutzwürdige Interesse des Betroffe-

[40] *Gola/Schomerus*, BDSG, § 28 BDSG, Rdnr. 17.

[41] Eine anteilige Abwälzung des Missbrauchsrisikos auf das Vertragsunternehmen ist auch rechtmäßig, BGH, NJW 2002, 2234.

nen ist insofern auch nicht unbillig belastet, als dass ihm die Wahl der Zahlungsmethode freigestellt wird und er eine Übermittlung der Daten verhindern kann, wenn er sich beispielsweise für die Zahlung mittels Lastschriftverfahren entscheidet.

Die Übermittlung der Daten an Dienstleister ist gem. § 28 Abs. 1 Nr. 1 BDSG in dem Umfang zulässig, in denen sich die Dienstleistung unmittelbar aus den vertraglichen Pflichten Amazons ergibt. So ergibt sich die Notwendigkeit der Übermittlung der Adressdaten des Betroffenen an den Paketdienst zwangsläufig aus dem Kaufvertrag, der in Form eines Versandhandels abgeschlossen wird[42].

## II. Informationspflichten im Zusammenhang mit dem Einsatz von Privacy-Policies

Gerade auf den Homepages größerer Online-Händler wie Amazon wird zur Einhaltung der datenschutzrechtlichen Bestimmungen gegenüber den Kunden fast ausschließlich auf die Privacy-Policies bzw. Datenschutzerklärung Bezug genommen, welche häufig am Ende der Startseite über einen Link einsehbar sind. Aufgabe der Privacy-Policies ist dabei zum einen die Erfüllung der Informationspflichten, zum anderen die Einholung der Einwilligung für die Fälle, in denen die Datenverarbeitung nicht aufgrund eines Erlaubnistatbestandes erfolgt[43]. Im Folgenden soll daher auf die Voraussetzungen ihrer wirksamen Einbeziehung und der notwendigen Form sowie den Inhalt eingegangen werden.

Da kollisionsrechtliche Fragen im Rahmen dieser Arbeit zu weit führen würden, wird in der weiteren Schilderung stets davon ausgegangen, dass der Inter-

[42] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 28 BDSG, Rdnr. 189.
[43] *Von Lewinski*, Privacy Policies: Unterrichtungen und Einwilligung im Internet, 395–400.

netanbieter in Deutschland niedergelassen ist, womit deutsches Recht anwendbar ist[44].

### 1. Wirksame Einbeziehung

Bei der Frage nach der wirksamen Einbeziehung einer Privacy-Policy drängt sich fast zwangsläufig der Gedanke nach der juristischen Einordnung der Privacy-Policies als allgemeine Geschäftsbedingungen auf. Hierzu sei bemerkt, dass eine absolute Deckungsgleichheit zwischen AGBs und Privacy-Policies aus dem Grund nicht gegeben ist, weil die Informationspflichten des Datenschutzes abseits jeglicher vertraglicher Beziehungen und somit auch im Rahmen reiner Gefälligkeitsverhältnisse wie das unentgeltliche Anbieten von Informationen[45] entstehen können.

Auch ist es strittig, ob die datenschutzrechtliche Einwilligung eine Willenserklärung darstellt. So wird einerseits behauptet, sie beziehe sich auf eine tatsächliche Handlung, den Eingriff in das Persönlichkeitsrecht und habe somit keinen rechtsgeschäftlichen Charakter[46]. Einer anderen Ansicht nach handelt es sich zumindest um eine geschäftsähnliche Handlung[47], da es sich bei ihr um eine Erklärung handelt, die sich auf eine tatsächliche Handlung, die Datenverarbeitung, bezieht und auf die grundsätzlich die Vorschriften über Willenserkärungen anzuwenden sind. Eine Entscheidung des Meinungsstreits kann hier

[44] Im Übrigen wären hier §§ 1 Abs. 5 BDSG, 3 TMG bzw. Art. 40 EGBGB anwendbar; Zur Vertiefung der Thematik siehe *Dammann* in: *BDSG*, Simitis, § 1 BDSG, Rdnr. 197 ff., *Spindler/Schuster*, Recht der elektronischen Medien, § 3 TMG, Rdnr. 1 ff., *Gounalakis/Rhode*, Persönlichkeitsschutz im Internet, Teil 2, *Jotzo*, MMR 2009, 232–237.

[45] Zur Frage des Rechtsbindungswillens und der rechtlichen Einordnung unentgeltlicher Internetangebote vgl. *Schmitz*, Vertragliche Haftung bei unentgeltlichem Informationserwerb via Internet, 396–399.

[46] *Scholz*, Datenschutz beim Internet-Einkauf, S. 281; *Gola/Schomerus*, BDSG, § 4a BDSG, Rdnr. 10.

[47] *Holznagel/Sonntag* in: *Roßnagel*, Handbuch Datenschutzrecht, 4.8, Rdnr. 20f.; OLG Celle NJW 1980, 1287; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht; *Schmitz/Eckhardt*, AGB - Einwilligung in Werbung, 533–539; *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 4a BDSG, Rdnr. 8ff.; *BDSG*, Simitis, § 4a BDSG, Rdnr. 20ff. m.w.N.

jedoch offen bleiben[48], da bei der Frage nach der wirksamen Einbeziehung von Datenschutzerklärungen zumindest ein ähnlicher Maßstab wie bei den Allgemeinen Geschäftsbeziehungen heranzuziehen ist, dienen doch sowohl § 305 Abs. 2 BGB als auch die Informationspflichten im Datenschutzrecht der Transparenz und tragen der Tatsache Rechnung, dass einer der Beteiligten gegenüber den anderen einen Wissensvorsprung hat.

Einen weiteren Anhaltspunkt liefert das bereichsspezifische Internetrecht selbst durch § 5 TMG. Auch wenn diese Vorschrift nicht direkt auf die Informationspflichten des Datenschutzes anwendbar ist, da sie die Anbieterkennzeichnung betrifft[49], lässt sich aus ihr zumindest herleiten, welche Mindestanforderung der Gesetzgeber an die Form der Wahrnehmung allgemeiner Informationspflichten auf dem Gebiet des Internetrechts stellt.

Zusammenfassend ist daher festzustellen, dass die Einbeziehung der Datenschutzerklärung immer dann wirksam ist, wenn dem Nutzer in leicht erkennbarer und unmittelbar erreichbarer Weise zum Zeitpunkt des Entstehens der Informationspflicht Gelegenheit zur Kenntnisnahme gegeben wird. Wann diesen Voraussetzungen Genüge getan wird, ist jedoch strittig.

Einigkeit[50] besteht insofern, dass die Erklärung nicht bereits in ihrem vollen Textumfang auf der Startseite erfolgen muss, sondern ein direkter Link, der mit den Worten Datenschutzerklärung bzw. Privacy Policies optisch deutlich kenntlich gemacht wird, genügt. Insofern ist aber anzumerken, dass sich die Notwendigkeit durchaus zumindest dann ergeben könnte, wenn schon durch das Aufrufen der Startseite personenbezogene Daten erhoben werden. Ist dies nicht der Fall, ist schon allein aus Praktikabilitätsgründen dieser Ansicht zuzustim-

[48] Er spielt freilich dann eine Rolle, wenn über eine eventuelle Wirksamkeit der Einwilligung in den Fällen der Minderjährigkeit des Betroffenen entschieden werden soll, vgl. *Holznagel/Sonntag* in: *Roßnagel*, Handbuch Datenschutzrecht, 4.8, Rdnr. 20.

[49] A.A. *Zscherpe*, Datenschutz im Internet - Grundsätze und Gestaltungsmöglichkeiten für Datenschutzerklärungen, 264–269 und *Von Lewinski*, Privacy Policies: Unterrichtungen und Einwilligung im Internet, 395–400, die § 6 TDG (jetzt in § 5 TMG geregelt) direkt auf die Datenschutzerklärung anwenden.

[50] *Von Lewinski*, Privacy Policies: Unterrichtungen und Einwilligung im Internet, 395–400.

men, da eine seitenlange Erklärung noch vor Anzeige der Startseite sowohl den Betreiber in seiner Möglichkeit, sein Angebot optisch ansprechend zu gestalten, einschränken würde, als auch den Nutzer behindern würde, der nicht auf allen Internetseiten kommerzieller Anbieter, die personenbezogene Daten über das Internet verarbeiten, erst einen langen Informationstext durchlesen möchte, bevor er an die für ihn interessanten Informationen gelangt. Darüber hinaus ist der Nutzer durch einen Link nicht unbillig benachteiligt, da es heutzutage im Internet bereits Usus geworden ist, auf weiterführende Informationen wie die AGBs, das Impressum und Möglichkeiten der Kontaktaufnahme in Form von Links hinzuweisen, die sich auf der Startseite befinden[51]. Es erscheint sogar wahrscheinlicher, dass ein Nutzer, der dem Link zur Datenschutzerklärung gefolgt ist, diese auch zur Kenntnis nimmt, als ein Nutzer, der die Datenschutzerklärung erst wegklicken muss, um auf das eigentliche Angebot zu gelangen. Uneinigkeit besteht aber hinsichtlich der genauen Platzierung des Links. Einerseits wird vertreten, dass der Verweis auf die Datenschutzerklärung stets im oberen Bereich der Seite angebracht werden muss, so dass ein Scrollen bis zu dem Link nicht nötig ist[52]. Diese Bedingung erscheint insofern fraglich, als dass die Länge der Seite, ab der ein Nutzer das Scrollen anfängt, von der möglichen Auflösung seines Bildschirms abhängt, die der Betreiber nicht kennt. Einzig praktikable Lösung unter dieser Annahme wäre es, dem Betreiber die Pflicht aufzuerlegen, den Link auf die Datenschutzerklärung gleich zu Beginn der Seite anzubringen.

Einer anderer Ansicht nach genügt es, die Datenschutzerklärung im sog. „Footer“, also dem Ende der Seiten zu platzieren, weil es inzwischen üblich

[51] So auch *Von Lewinski*, Privacy Policies: Unterrichtungen und Einwilligung im Internet, 395–400.
[52] *Schaar*, Datenschutz im Internet, S. 331.

geworden ist, dass rechtliche Hinweise am Ende der Bildschirmseite stehen, so dass der Nutzer damit rechnet[53].

Da die erste Ansicht zu strikt und wenig praktizierbar ist, die zweite dagegen die Informationspflicht als aktive Pflicht verkennt, dem Nutzer auch ohne die Notwendigkeit einer seinerseitigen Suche unmittelbare Kenntnis über den Inhalt der Unterrichtung zu verschaffen[54], ist eine Lösung vorzuziehen, die sowohl dem Praktikabilitätsaspekt als auch dem Transparenzgedanken Rechnung trägt: Ein Hinweis auf die Datenschutzerklärung im Footer mit direktem Link ist jedenfalls dann ausreichend, wenn er lediglich der Wahrung der Pflicht der jederzeitigen Abrufbarkeit (§ 13 Abs. 1 S. 3 TMG) dient. Hier ist davon auszugehen, dass der Nutzer, der bereits unterrichtet wurde, aufgrund der Üblichkeit der Platzierung derlei Informationen an dieser Stelle, gezielt dort nach dem Link zur Datenschutzerklärung sucht[55]. Anders verhält es sich hinsichtlich der erstmaligen Informationspflichten. Anders als bei der Pflicht zur jederzeitigen Abrufbarkeit, geht diesen keine anderweitige Unterrichtung vor und ist aus diesem Grund ein wesentlich höheres Maß an Transparenz notwendig. Ferner hat der Gesetzgeber bei den Informationspflichten nach den §§ 4, 33 BDSG und den §§ 13, 15 TMG bewusst die Zeitpunkte, in denen die Unterrichtungspflichten entstehen, derart vorgegeben, dass dem Nutzer/Betroffenen ausreichend Gelegenheit gegeben wird über sein Recht der informationellen Selbstbestimmung frei und umfassend zu verfügen. Danach hat die Unterrichtung zu Beginn des Nutzungsvorgangs (§ 13 Abs. 1 S. 1 TMG) bzw. des automatischen Verfahrens (§ 13 Abs. 1 S. 2 TMG) oder vor Abgabe der Einwilligung (§ 13 Abs. 3

[53] *Von Lewinski*, Privacy Policies: Unterrichtungen und Einwilligung im Internet, 395–400; *Zscherpe*, Datenschutz im Internet - Grundsätze und Gestaltungsmöglichkeiten für Datenschutzerklärungen, 264–269.

[54] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 152; *Enzmann/ Scholz*, Technisch-organisatorische Gestaltungsmöglichkeiten, 73–88.

[55] A.A. *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 212, der davon ausgeht, dass der Nutzer auch über eine andere als die Hauptseite ins Angebot einsteigen kann und daher zur Wahrung der Pflicht der jederzeitigen Abrufbarkeit zumindest einen Link in einem Frame vonnöten hält.

TMG) zu erfolgen. Wichtig ist es in diesem Zusammenhang also, zwischen verschiedenen Diensten, die der Betreiber anbietet, zu unterscheiden, da sich der Nutzungsvorgang stets auf den konkreten Dienst bezieht[56]. Bietet ein Online-Handel beispielsweise das Stöbern durch sein Angebot auf eine Weise ein, die ohne die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zurechtkommt und wird ein Personenbezug erst zum Zeitpunkt des Einloggens zum Zwecke der Bestellung hergestellt, wäre der frühestmögliche Zeitpunkt, an dem der nicht zu übersehende Link auf die Datenschutzerklärung zu erfolgen hat, das Login-Fenster. Im Umkehrschluss bedeutet dies aber, dass durch die gängige Praxis, Daten auch dann zu erheben, wenn eine Bestellung während des Bestellvorgangs abgebrochen wird, den Hinweis auf die Datenschutzerklärung aber erst im Fenster zu positionieren, das dem Abschluss der Bestellung unmittelbar voran geht, als verspätet einzuordnen ist.

Es bleibt zuletzt erneut zu betonen, dass das Datenschutzrecht dem Betreiber eines Online-Angebotes die Pflicht auferlegt, eine Trennung in die verschiedenen Dienste dahingehend vorzunehmen, dass es ihm möglich ist, für jeden einzelnen Dienst zu Beginn des Nutzungsvorgangs (bzw. bei einer Kombination verschiedener Dienste zu Beginn des Nutzungsvorgangs des ersten Dienstes) einen Hinweis auf die Datenschutzerklärung zu erteilen. Dabei hat er besonders darauf zu achten, dass er alle virtuellen Wege, durch die ein Nutzer zu den einzelnen Diensten gelangen kann, auch tatsächlich abdeckt.

## 2. Form und Inhalt der Datenschutzerklärung

Die Informationspflichten müssen in der Datenschutzerklärung verständlich, umfassend und hinreichend auffällig dargestellt werden[57]. Eine Aufnahme in die AGBs des Anbieters ist zwar möglich, der Aufbau der AGBs muss dann aber so gewählt sein, dass der datenschutzrechtliche Teil als solcher deutlich

[56] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 120.
[57] *Schaar*, Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, 275–277.

erkennbar ist und nicht zwischen den anderen Klauseln untergeht[58]. Hinsichtlich der Einwilligung muss vor allem zwischen der Hinweispflicht des § 4a Abs. 1 S. 2 BDSG und der besonderen Hervorhebung der Einwilligungserklärung im Sinne des § 4a Abs. 1 S. 4 BDSG unterschieden werden. Während die Hinweispflicht im Rahmen der sonstigen datenschutzrechtlichen Klauseln erfüllt werden kann, wird an die Einwilligungserklärung vom Gesetzgeber ein deutlich höherer Maßstab angesetzt. So genügt ein bloßer Hinweis in den AGBs, wenn auch in Fettdruck, für die Hervorhebung der Einwilligungserklärung nicht[59]. Sie muss vielmehr vom restlichen Text drucktechnisch abgesetzt werden, um zu vermeiden, dass der Nutzer, der bereits seitenlange AGBs heruntergescrollt hat, sich der Tragweite seiner Erklärung nicht bewusst ist[60]. Auf zivilrechtlicher Ebene ist diesbezüglich auch auf die Klauselverbote zu achten. Neben dem allgemeinen Verbot überraschender Klauseln gemäß § 305c BGB[61], sind hier insbesondere § 308 Nr. 5 BGB, der eine Erklärungsfiktion verbietet und § 309 Nr. 12 BGB, wonach es nicht möglich ist, die Beweislast hinsichtlich des Vorliegens einer wirksamen Erklärung dem Betroffenen aufzuerlegen, relevant[62].

Im Bezug auf eine umfassende Unterrichtung liegt der Mangel vieler Datenschutzerklärungen in der Offenbarung des Zwecks. Die Zweckbestimmung erfordert eine für den Betroffenen nachvollziehbare Information, die sich nicht in pauschale Aussagen erschöpfen darf[63]. Sie ergibt sich unmittelbar aus dem Grundsatz der Zweckbindung, welcher einer der tragenden Prinzipien des Datenschutzrechts ist und der gerade im Zuge der automatischen Datenverarbeitung an besonderer Bedeutung gewonnen hat, weil anhand der durch sie angefertigten Datensammlungen ein teilweise oder weitgehend vollständiges

[58] Vgl. auch *Zscherpe*, Datenschutz im Internet - Grundsätze und Gestaltungsmöglichkeiten für Datenschutzerklärungen, 264–269.
[59] *Gola/Schomerus*, BDSG, § 4a BDSG, Rdnr. 14.
[60] *Gola/Schomerus*, BDSG, § 4a BDSG, Rdnr. 14; *Zscherpe*, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, 723–727.
[61] Vgl. *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 322.
[62] *Zscherpe*, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, 723–727.
[63] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 4 BDSG, Rdnr. 43.

Persönlichkeitsbild zusammengefügt werden kann, ohne dass dies vom Betroffenen noch kontrolliert werden könnte[64]. Individuelle Selbstbestimmung muss aber dem Einzelnen die Möglichkeit geben, frei zu entscheiden, wer was wann und bei welcher Gelegenheit über ihn weiss[65]. Dazu gehört auch die Kenntnis darüber, in welchem Zusammenhang dieses Wissen genau verwertet wird.

Zu pauschal sind in diesem Sinne die Angabe von Zwecken wie „zur Darstellung einer personalisierten Startseite und weiterer Dienste", „zur Verbesserung der Plattform" oder „zum Bereitstellen wichtiger Informationen des verwendeten Dienstes"[66]. Auch ist in den Fällen, in denen eine Erhebung, Verarbeitung oder Nutzung aufgrund einer Zulässigkeitsnorm stattfindet, der Hinweis auf die ermächtigende Vorschrift nicht ausreichend, wenn nicht der Erhebungszweck unmissverständlich aus ihr hervorgeht[67]. Hinzuweisen ist im Hinblick auf den Online-Handel insbesondere auf § 28 Abs. 1 S. 1 BDSG, im Rahmen dessen sich bereits aus § 28 Abs. 1 S. 2 BDSG ergibt, dass eine konkrete Festlegung der Zwecke bei der Erhebung stattzufinden hat. Da sich diese regelmäßig ohnehin nur anhand einer schriftlichen Dokumentation realisieren lässt, kann die Dokumentation die Grundlage für die Hinweispflicht bilden[68].

Ebenso großen Wert wie auf die umfassende Unterrichtung hinsichtlich des Zweckes muss bei Internetdiensten auch auf die Unterrichtung hinsichtlich der Art der Daten sowie der Herstellung des Bezuges zwischen Art der erhobenen Daten und deren Zweck gelegt werden. Der Gesetzgeber hat schon beim Gesetzesentwurf zum IuKDG zu erkennen gegeben, dass sich aus den Risiken im Internet eine weitreichendere Unterrichtungspflicht ergibt, so dass die Pflicht aus § 13 Abs. 1 S. 1 TMG insbesondere im Hinblick auf die Art der

[64] So das Bundesverfassungsgericht schon beim „Volkszählungsurteil" BVerfGE 66, 1 [43].
[65] BVerfGE 65, 1 [44].
[66] Diese Beispiele stammen aus Datenschutzerklärungen verschiedener Unternehmen. Für weitere Beispiele siehe auch: *Holznagel/Sonntag* in: *Roßnagel*, Handbuch Datenschutzrecht, 4.8 Rdnr. 53.
[67] *Roßnagel*, Handbuch Datenschutzrecht, § 4 BDSG, Rdnr. 31.
[68] *Roßnagel*, Handbuch Datenschutzrecht, § 28 BDSG, Rdnr. 48, *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 28 BDSG, Rdnr. 260.

Daten umfangreicher ist als die des § 4 Abs. 3 S. 1 BDSG[69]. Auch gem. § 13 Abs. 1 S. 1 TMG sind daher pauschale Klauseln, die den Nutzer lediglich darüber informieren, dass personenbezogene Daten über ihn verarbeitet weren, zu vermeiden. Vielmehr besteht die Unterrichtungspflicht nicht nur darin, die verarbeiteten Datenarten en détail aufzuzählen, sondern den Nutzer auch darüber zu informieren, welche Datenart genau welchem Zweck zugeführt wird. So müsste bei Web-Formularen dem Nutzer bei jedem Eingabefeld mitgeteilt werden, wozu dieses Feld konkret benötigt wird[70], da es für den Nutzer beispielsweise einen Unterschied bedeutet, ob er seine E-Mail-Adresse dazu angibt, im Falle von Rückfragen zur Vertragsabwicklung kontaktiert werden zu können oder ob die E-Mail-Adresse darüber hinaus dazu verwendet wird, Statistiken darüber zu erheben, welchen E-Mail-Provider die Kunden des Internetdienstes bevorzugen, um bei diesen gezielt Werbung schalten zu können[71]. Eine getrennte Aufzählung der verarbeiteten Datenarten und deren Zwecke in der Datenschutzerklärung ist dem Nutzer daher nur zumutbar, wenn sich der Zweck der Verarbeitung anhand der Datenarten unmittelbar erschließt, der Nutzer also den Zusammenhang, der gerade bei Angeboten, die aus einer Vielzahl von Telemediendiensten bestehen, häufig schwer zu überblicken ist, nicht erst durch persönliche Überlegungen selbst herzustellen versuchen muss[72].

## III. Rechtmäßigkeit der Datenschutzerklärung von Amazon

Um die in diesem Kapitel ausgeführten Überlegungen abzurunden und mit der tatsächlichen Praxis zu vergleichen, bietet sich abschließend die Überprüfung

[69] Siehe dazu bereits unter Abschnitt E.II.2.a) auf Seite 103 und BT-Drs. 13/7385, S. 22.
[70] *Schleipfer*, Datenschutzgerechte Gestaltung von Web-Eingabeformularen, 56–61.
[71] Zur formularmäßigen Einwilligung in die Speicherung und Nutzung von personenbezogenen Daten für die Zusendung von Werbung im Rahmen eines Kundenbindungs- und Rabattsystems siehe umfassend auch BGHZ 177, 253.
[72] Zur Gestaltung von Datenschutzhinweisen siehe auch *Niclas*, ITRB 2008, 280–283.

der Datenschutzerklärung von Amazon auf ihre Konformität mit den datenschutzrechtlichen Informationspflichten an. Diese soll in zwei Schritten erfolgen. Zunächst folgt eine Schritt-für-Schritt-Analyse des Textes selbst, um eine bessere Transparenz zu gewährleisten und eventuelle Verarbeitungszwecke, die unter Abschnitt F.I. auf Seite 117 nicht hervorgetreten sind, die Amazon nach eigenen Angaben erzielen will, ebenso zu bewerten.

Im Anschluss wird überprüft, ob die unter Abschnitt F.I.3. auf Seite 126 beschriebenen Informationspflichten auch tatsächlich eingehalten wurden.

### 1. Schrittweise Überprüfung des Erklärungstextes

Im ersten Absatz des Textes informiert Amazon über die „Verantwortliche Stelle“ und wird somit der Pflicht aus § 4 Abs. 3 S. 1 Nr. 1 BDSG gerecht. Der Hinweis auf das Programm „Safe Harbour“ ist als (freiwillige) Information darüber zu verstehen, dass bei der Übermittlung der personenbezogenen Daten ins Ausland gem. § 4b Abs. 2 BDSG ein angemessenes Datenschutzniveau gewährleistet ist[73].

Im nächsten Absatz (Welche persönlichen Informationen unserer Kunden erheben und nutzen wir?), klärt Amazon zunächst über einige Verarbeitungszwecke auf. Genannt werden die „Abwicklung von Bestellungen, die Lieferung von Waren und das Erbringen von Dienstleistungen sowie die Abwicklung der Zahlung“, zusätzlich bei Rechnungskauf die erforderlichen Prüfungen. Sowohl erstere als auch letztere fallen unter § 28 Abs. 1 Nr. 1 BDSG, soweit unter „erforderliche Prüfungen“ die Überprüfung der Bonitätsdaten[74] gemeint ist, was Amazon leider nicht deutlich darlegt. Sie bedürfen daher keiner Einwilligung, müssen aber im Rahmen von § 4 Abs. 3 S. 1 Nr. 2 BDSG und § 13 Abs. 1 S. 1 TMG dem Betroffenen mitgeteilt werden. Die Unterhaltung der Kundenkonten fällt, zumindest für den Zeitraum der Gewährleistungfrist ebenso unter §

[73] Zu den „Safe Harbour Grundsätzen“ siehe *Simitis* in: *BDSG*, Simitis, § 4b, Rdnr. 70ff.
[74] *Gola/Schomerus*, BDSG, § 28, Rdnr. 27.

28 Abs. 1 Nr. 1 BDSG, bedarf danach aber der Einwilligung[75]. Gleiches gilt für die Auftragsverarbeitung von Dritten, um die Durchführung technischer, logistischer oder anderer Dienstleistungen zu ermöglichen. An dieser Stelle ist aber darauf hinzuweisen, dass § 28 Abs. 1 Nr. 1 BDSG nur dann denkbar ist, wenn es tatsächlich zu einer Bestellung durch den Betroffenen kommt, nicht aber schon bei den Daten, die bereits erhoben werden, während der Betroffene nur das Angebot durchstöbert.

Die Nutzung zum Zwecke des Marketings, der Verbesserung der Plattform und der Verhinderung des Missbrauchs fällt unter § 28 Abs. 1 Nr. 2 BDSG[76], soweit es sich bei den Daten um Inhaltsdaten handelt, die nach dem BDSG erhoben wurden. Für Daten, die unter das TMG fallen, bedarf es der Einwilligung[77], da hier § 28 BDSG nicht anwendbar ist.

Der nächste Absatz, der unter „Wir sammeln folgende Informationen“ zu finden ist, weist auf den Ursprung der jeweils genutzten Daten hin. Hier versucht Amazon seiner Unterrichtungspflicht nach § 13 Abs. 1 TMG gerecht zu werden, den Nutzer über Art und Umfang der verwendeten Daten zu informieren. Dabei wird nach Daten, die der Nutzer selbst preisgibt, welchen, die automatisch erhoben werden, welchen, die aus der E-Mail-Kommunikation[78] entstehen und welchen, die Amazon aus anderen Quellen erhält, unterteilt. Zu den ersten beiden Kategorien nennt Amazon an einer weiteren Stelle noch Beispiele, welche Daten genau erhoben werden.

Diese finden sich unter dem Absatz „Informationen, die Sie uns geben“ und „Automatische Informationen“. Unter die „Informationen, die Sie uns geben“ fallen neben dem Namen, die Versandadressen, die Zahlungsdaten auch diejenigen Daten, die der Nutzer freiwillig dem System übergibt, wenn er an einem

[75] Siehe dazu bereits unter Abschnitt F.I.3.d) auf Seite 132.
[76] Siehe dazu bereits unter Abschnitt F.I.3.d) auf Seite 132.
[77] Siehe Abschnitt F.I.3.c) auf Seite 130.
[78] Amazon unterlässt es an dieser Stelle, auf die technischen Details einzugehen, wie es die Bestätigung darüber erhält, welche E-Mails der Nutzer öffnet. Es darf aber davon ausgegangen werden, dass hierzu Web-Bugs verwendet werden.

Gewinnspiel teilnimmt, einen Fragebogen ausfüllt oder einen Wunschzettel anlegt. Darüber hinaus speichert Amazon allerdings auch die Telefonnummer des Kunden, ohne welche die Bestellung angeblich nicht abwickelt werden kann. An dieser Stelle wäre wünschenswert gewesen zu erfahren, warum dies der Fall sein soll, wo durch die E-Mailadresse und die Postadresse bereits ausreichend Kommunikationsmöglichkeiten eröffnet sind und es bei einer rein online durchgeführten Bestellabwicklung des Telefons gerade nicht bedarf. Die Pflicht zur Angabe der Telefonnummer scheint hier folglich unnötig, weshalb eine Erklärung des genauen Verwendungszwecks aus Gründen der Transparenz notwendig gewesen wäre.

Bei den „Automatischen Informationen“ werden neben den Bestands- und Nutzungsdaten auch die Cookies und der Clickstream erwähnt. Besonderes Augenmerk gilt hier der Bestellhistorie, die Amazon zu Zwecken der Werbung in nicht persönlich identifizierbarer Form weiterverwendet und die als solche unter § 15 Abs. 3 fällt. Eine Erfüllung der Hinweispflicht gem. § 15 Abs. 3 S. 2 TMG lässt die Datenschutzerklärung vermissen. Die Cookies werden laut der Datenschutzerklärung genutzt, um Missbrauch vorzubeugen und *für andere Zwecke*. Welche Zwecke konkret gemeint sind, wird nicht weiter erklärt. Darüber hinaus informiert Amazon darüber, dass diejenigen Telefonnummern des Nutzers gespeichert werden, die er benutzt, um die 0800-Nummern des Unternehmens anzurufen. Auch hier erfolgt keine Erklärung darüber, zu welchem Zwecke die Speicherung erfolgt. Sowohl bei der Unterrichtung über die Zweckbestimmung der Cookies als auch hinsichtlich der Speicherung der Telefonnummer liegt also ein klarer Verstoß gegen § 13 Abs. 1 S. 1 TMG vor.

Bei den „Informationen aus anderen Quellen“ gibt Amazon zunächst an, dass ein Datenabgleich mit den Paketdienstleistern erfolgt, um die Aktualität der Bestellerdaten zu gewährleisten. Dies fällt ohne weiteres unter die zulässige Verarbeitung nach § 28 Abs. 1 Nr. 1 BDSG. Eine Erklärung bleibt Amazon jedoch wiederum dahingehend schuldig, zu welchem Zwecke es Informationen,

die es über das Tochternunternehmen Alexa Internet hinsichtlich der Suchworte und Suchergebnisse erhält, verwendet. Bei Alexa, vom Landesdatenschutzbeauftragten in Bremen[79] als Spyware bezeichnet, handelt es sich um eine Suchengine, die von Amazon 1999 aufgekauft wurde[80] und die Amazon auf der eigenen Seite zur Produktsuche verwendet.

Zusammenfassend bleibt festzustellen, dass zum einen an vielen Stellen keine Information hinsichtlich der Verwendungszwecke erfolgt und dass Amazon bei allen drei Kategorien nach eigener Aussage lediglich Beispiele nennt, welche Daten verarbeitet werden. Für eine vollumfängliche Erklärung, die eine informierte Einwilligung voraussetzt, genügen Beispiele aber gerade nicht. Auch ist darin ein Verstoß gegen § 13 Abs. 1 S. 1 TMG zu sehen, der eine Unterrichtung über den gesamten Umfang der Verarbeitung vorsieht und somit eine Erklärung darüber, welche Angaben im Einzelnen verarbeitet werden und für welche konkreten Zwecke[81].

Im Absatz „Gibt Amazon.de die erhaltenen Informationen weiter?“ weist Amazon auf weitere Empfänger der Daten hin. Zu unterscheiden gilt es hier, ob es sich beim Empfänger um Dritte handelt oder um Dienstleister, die für Amazon im Wege der Auftragsdatenverarbeitung die Vertragsabwicklung übernehmen. Während letztere unter § 28 Abs. 1 Nr. 1 BDSG fallen, muss der Betroffene in die Übermittlung der Daten an Dritte einwilligen. Als Dritter sind bei der Auflistung Amazons die Verbundenen Unternehmen, die Partnerunternehmen und die Übermittlung im Falle der Übertragung von Geschäftsteilen zu sehen. Darüber hinaus gibt Amazon an, dass es zuweilen seine Angebote im Auftrag anderer Unternehmen versendet. Hierbei handelt es sich allerdings nicht um eine datenschutzrechtliche Übermittlung, sondern um die Verwertung der Kundendaten zum Zwecke der Promotion. Da diese nicht zur Erfüllung ei-

[79] `Http://www.datenschutz-bremen.de/sv_internet/spyware.php`.
[80] `Http://www.newstatesman.com/200510170018`.
[81] *Scholz*, Datenschutz beim Internet-Einkauf, S. 317.

gener Belange[82] dient, fällt sie anders als die Werbung, die Amazon für seine eigenen Produkte versendet, nicht unter § 28 Abs. 1 Nr. 2 BDSG. Der Betroffene muss in die Nutzung daher einwilligen. Da Amazon darauf hinweist, wie der Betroffene einstellen kann, dass er derartige Angebote nicht mehr erhält, ist die Unterrichtungspflicht gem. § 28 Abs. 4 S. 2 BDSG gewahrt. Ein Verstoß gegen § 4 Abs. 3 BDSG bzw. § 13 Abs. 1 TMG liegt hingegen in der Übermittlung der Daten, um die Rechte Dritter zu schützen. Eine rein zivilrechtlich bedingte Weitergabe von Daten zur Rechtsdurchsetzung sehen über § 28 Abs. 3 S. 1 Nr. 1 BDSG hinaus weder das BDSG noch das TMG vor. Der Betroffene müsste daher in die Übermittlung einwilligen. Für eine Einwilligung ist der Zweck jedoch durch Amazon zu allgemein gehalten. Es wird weder dargestellt, wer genau die Dritten sind, deren Rechte geschützt werden sollen, noch um welche Rechte es sich handelt.

Zuletzt erklärt Amazon, in allen anderen Fällen den Betroffenen darüber zu informieren, wenn eine Übermittlung erfolgt und ihm die Möglichkeit gibt eine Einwilligung zu erteilen. Diese Aussage ist in zweierlei Hinsicht unglücklich formuliert: Zum einen suggeriert sie dem Betroffenen, in allen übrigen beschriebenen Fällen sei eine Übermittlung auch ohne seine Einwilligung rechtens, zum anderen hat Amazon in allen anderen Fällen dem Betroffenen nicht nur die Möglichkeit zu geben, eine Einwilligung zu erteilen, die Einwilligung ist vielmehr Voraussetzung für eine rechtmäßige Übermittlung. Auch lässt die Datenschutzerklärung nicht erkennen, zu welchen Zwecken Amazon die Daten an Verbundene und Partnerunternehmen übermittelt.

Im Absatz „Welche Wahlmöglichkeiten habe ich“, weist Amazon daraufhin, dass der Betroffene auch die Möglichkeit hat, keine Daten weiterzugeben, wenn er darauf verzichtet, Waren zu kaufen oder Dienste wie den Wunschzettel oder die Kundenrezension zu nutzen. Diese Erklärung kann als Erfüllung der Informationspflicht gemäß § 13 Abs. 6 S. 2 TMG gesehen werden, wonach der Nutzer

[82] *Simitis* in: *BDSG*, Simitis, § 28, Rdnr. 140.

über die Möglichkeit der anonymen oder pseudonymen Nutzung zu informieren ist. Ferner weist Amazon darauf hin, dass der Betroffene bestimmte Daten aktualisieren oder hinzufügen kann. Hierbei ist auffällig, dass sich Amazon ausdrücklich vorbehält, eine Kopie der ursprünglichen Daten aufzuheben. Amazon nennt hierbei jedoch keinen Zweck. Handelt es sich nicht um Daten, die aufgrund einer Erlaubnisnorm, beispielsweise innerhalb der Speicherfrist des § 15 Abs. 7 TMG aufbewahrt werden dürfen, müsste der Betroffene ausdrücklich in die Speicherung der Ursprungsdaten einwilligen. Unabhängig davon, ist er jedenfalls über den Zweck der Speicherung zu informieren.

Die sonstigen Abschnitte der Datenschutzerklärung dienen nicht der datenschutzrechtlichen Information und werden daher an dieser Stelle nicht näher erläutert.

## 2. Erfüllung der aus der Erhebung, Speicherung und Nutzung der Daten entstandenen Informationspflichten

Hinsichtlich der Cookies ist die Erfüllung der Informationspflichten nur unzureichend. Zwar informiert Amazon darüber, dass der Nutzer auf das Ablegen der Cookies auch verzichten kann (§ 13 Abs. 6 S. 2 TMG), eine umfassende Unterrichtung über die Zwecke bleibt jedoch aus. Es erfolgen an verschiedenen Stellen der Datenschutzerklärung lediglich Beispiele, wie die Nutzung des Einkaufswagens, der Checkout oder die Verhinderung von Missbrauch. Darüber hinaus weist Amazon lediglich darauf hin, Cookies auch für „andere Zwecke“ und für „andere Funktionen“ zu nutzen. Auch der Zeitpunkt der Erklärung ist zu spät gewählt: Klickt der Benutzer nicht von sich aus auf den Link zu Datenschutzerklärung, der sich am Ende der Startseite befindet, erfährt er von ihrem Vorhandensein erst vor Absenden der Bestellung, also zu einem Zeitpunkt zu dem bereits Cookies abgelegt und ausgelesen wurden. Eine Information darüber, dass jede spätere Erhebung erneut der Einwilligung bedarf sowie darüber,

dass die Einwilligung mit Wirkung für die Zukunft widerrufen werden kann (§ 13 Abs. 3 TMG) wird ebenso vermisst.

Bezüglich der Nutzung von Amazon Marketplace nimmt Amazon in den „Teilnahmebedingungen Amazon Services Europe S.a.r.l.“[83] zum einen Bezug auf die Datenschutzerklärung. Zum anderen befindet sich unter IV. noch eine eigene Datenschutzklausel. In dieser wird zunächst der Verkäufer darüber informiert, dass die von ihm angegebenen persönlichen Informationen auf der Webseite einsehbar sind. Darüber hinaus räumt Amazon sich und seinen verbundenen Unternehmen das Recht ein, die personenbezogenen Daten zur Kommunikation mit den Teilnehmern zum Zwecke der Werbung zu nutzen. Eine Unterrichtung gemäß § 28 Abs. 4 S. 2 BDSG unterbleibt auch hier. Die Einwilligungserklärung findet sich innerhalb der Teilnahmebedingungen als letzter Satz im Fettdruck. Für die Pflicht zur besonderen Hervorhebung gem. § 4a Abs. 1 S. 4 BDSG ist der Fettdruck jedoch nicht ausreichend[84]. Bezüglich der Weitergabe der Daten des Käufers an den Verkäufer findet sich in der Datenschutzerklärung lediglich der Hinweis, dass eine Weitergabe an die Verkäufer des Marketplace erfolgt, nicht jedoch in welchem Umfang und zu welchem Zweck. Die übrigen Zwecke, zu denen Amazon selbst die Daten nutzt, finden sich an verschiedenen Stellen in der Erklärung. Nähere Informationen zu den datenschutzrechtlichen Vorgängen, die Amazon Payments betreffen, insbesondere, warum der Verkäufer sowohl seine Kreditkartendaten als auch seine Bankkontodaten preisgeben muss, unterbleiben.

Bei den Daten, die der Nutzer bei der Erstregistrierung angibt, finden sich die verschiedenen Zwecke, für die Amazon seinen Vor- und Nachnamen sowie die E-Mailadresse nutzt, ebenso an verschiedenen Stellen der Datenschutzerklärung. Es unterbleibt die Erklärung, dass jede angegebene Adresse, selbst

[83] `Http://www.amazon.de/gp/help/customer/display.html?ie=UTF8&nodeId=3367031&pop-up=1`.

[84] *Gola/Schomerus*, BDSG, § 4a BDSG, Rndr. 14.

in den Fällen, in denen die Bestellung unterbrochen oder die Adresse gelöscht wird, weiterhin gespeichert bleibt.

Im Hinblick auf die Daten, die bei Abschluss und Abwicklung des Kaufvertrages anfallen, kann auf die Ausführungen verwiesen werden, die soeben bei der schrittweisen Überprüfung getroffen wurden. Gleiches gilt für die Übermittlung der Daten an Dritte.

### 3. Wirksame Einwilligung des Betroffenen bzw. Einbeziehung der Datenschutzerklärung

Ein Hinweis auf die Datenschutzerklärung findet sich primär an vier Stellen: Als Link im Footer des gesamten Angebots, auf der Bestätigungsseite, die dem Abschluss jeder Bestellung vorausgeht und auf der Webseite, die der Angabe der Verkäuferdaten im Amazon Marketplace vorausgeht sowie als Hinweis auf die Allgemeinen Geschäftsbedingungen, die ihrerseits auf die Datenschutzerklärung verweisen.

Der Footer ist dabei lediglich dazu geeignet, die Pflicht der jederzeitigen Abrufbarkeit gem. § 13 Abs. 1 S. 3 zu erfüllen[85]. Hinsichtlich der anderen Stellen gilt folgendes: Soweit lediglich diejenigen Daten verarbeitet werden, die im Rahmen der Verkaufsabwicklung bzw. der Registrierung bei Amazon Marketplace oder der Nutzung eines Telemediendienstes (wie z.B. der Abgabe einer Rezension) anfallen, ist der Zeitpunkt des erstmaligen Hinweises ausreichend. Nicht jedoch gilt dies für diejenigen Daten, die entweder automatisch erhoben werden oder auch bei Abbruch der Bestellung oder die bereits bei der Erstregistrierung entstehen. Hier müsste eine Information bereits vor der Entscheidung über die Preisgabe (§ 4 Abs. 3 S. 1 BDSG), zu Beginn der Nutzung (§ 13 Abs. 1 S. 1 TMG) oder zu Beginn des automatischen Verfahrens erfolgen (§ 13 Abs. 3 S. 2 TMG).

[85] Vgl. hierzu bereits Abschnitt F.II. auf Seite 136.

Bezüglich der Einwilligungserklärung gilt zu bemerken, dass eine schriftlich zu erteilende, besonders hervorgehobene Einwilligungserklärung, wie sie von § 4a Abs. 1 S.3 BDSG vorausgesetzt, weder in den Hinweisen auf die Datenschutzerklärung zu sehen ist, noch in der Datenschutzerklärung selbst zu finden ist.

Zusammenfassend ist festzustellen, dass von den einzeln hervorgehobenen Kritikpunkten abgesehen, an der Datenschutzerklärung von Amazon auffällig ist, dass sie zu unstrukturiert erscheint, als dass sie dazu geeignet wäre, einen juristischen Laien umfassend über seine Rechte zu informieren. Hierzu wäre es zunächst notwendig gewesen, diejenigen Zwecke, die von einer Erlaubnisnorm abgedeckt werden, von denjenigen zu trennen, die einer Einwilligung bedürfen[86]. Überdies hätte eine genaue Auflistung, genau welche Daten für welchen Zweck verwendet werden, erfolgen müssen. Die Datenschutzerklärung beschränkt sich indes darauf, an vielen verschiedenen Stellen Beispiele zu nennen, ohne auf die Gesamtheit der Verwendungszwecke einzugehen. Auch eine Information darüber, wie lange die einzelnen Daten gespeichert werden, unterbleibt. Damit die Datenschutzerklärung von Amazon tatsächlich datenschutzkonform wird, besteht an einer Vielzahl von Stellen noch Nachbesserungsbedarf.

[86] So im Ergebnis auch *Taeger*, K&R 2003, 220–227.

# G. Zivilrechtliche Folgen bei Verstoß gegen die Informationspflichten

Ob überhaupt und gegebenenfalls welche privatrechtlichen Rechtsfolgen sich aus einem Verstoß gegen die Informationspflichten ergeben, ist gesetzlich nicht geregelt und muss daher am Inhalt der jeweiligen Informationspflicht gemessen werden.

In den datenschutzrechtlichen Vorschriften selbst finden sich größtenteils nur sanktionsrechtliche Rechtsfolgen bei Verstößen (z. B. in §§ 43, 44 BDSG, § 16 TMG und §§ 148, 149 TKG)[1]. Eine ausdrückliche Regelung der zivilrechtlichen Folgen findet sich lediglich in den § 7 und 35 BDSG[2]. Nach dem Prinzip *ubi jus, ibi remedium*[3] ist eine umfassende Information durch den Anbieter aber nur dann gewährleistet, wenn dem Betroffenen bei Verstößen gegen die Informationspflichten ausreichende Rechtsansprüche gegen den Anbieter zur Verfügung stehen[4].

Im Folgenden wird daher zunächst auf die unterschiedlichen Folgen eines Verstoßes gegen die einzelnen Informationspflichten eingegangen. Anschließend muss geklärt werden, welche zivilrechtlichen Rechte dem Betroffenen daraus zum einen aus den datenschutzrechtlichen Vorschriften, zum anderen aber auch unter Anwendung des allgemeinen Zivilrechts erwachsen. Abschließend ist zu klären, ob die Rechtsfolgen als ausreichendes Mittel dazu dienen können, um

[1] Zum Vollzugsdefizit des Datenschutzstrafrechts siehe *Weichert*, NStZ 1999, 490–493.
[2] § 8 und 20 BDSG regeln die Rechte des Betroffenen bei Erhebung durch öffentliche Stellen, auf die hier nicht weiter eingegangen wird.
[3] Dort wo es Recht gibt, gibt es auch ein Rechtsmittel.
[4] Zum Vollzugsdefizit am Beispiel der Auskunfteien und des Credit Scoring siehe *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 128 f.

die Wirksamkeit datenschutzrechtlicher Informationspflichten auch tatsächlich zu garantieren.

## I. Verstöße gegen Informationspflichten des BDSG

### 1. Verstoß gegen § 4 Abs. 3 S. 1 BDSG

Ob ein Verstoß gegen die Unterrichtungspflicht des § 4 Abs. 3 S. 1 BDSG notwendigerweise die Unzulässigkeit der Datenerhebung zur Folge hat, ist strittig. Auf der einen Seite[5] wird vertreten, dass sich die Zulässigkeit der Daten grundsätzlich ausschließlich nach § 4 Abs. 1 BDSG (im nicht-öffentlichen Rechtsverkehr häufig in Verbindung mit § 28 BDSG) richtet. Ist diese Vorschrift gewahrt, sind zwei Fallkonstellationen denkbar: Entweder der Betroffene hat in die Erhebung eingewilligt und wurde daher wegen § 4a Abs. 1 S. 2 BDSG ohnehin im vollen Umfang des § 4 Abs. 3 BDSG unterrichtet[6] oder die Erhebung fand aufgrund einer Rechtsvorschrift statt. Ist letzteres der Fall, sorgt die in der Rechtsbestimmung vorgegebene und von ihr beschränkte Zweckbestimmung für einen ausreichenden Schutz des Betroffenen[7]. Dieser Ansicht nach, wird jedoch immer dann, wenn die Unterrichtungspflicht gem. § 4 Abs. 3 S. 1 BDSG unterlassen wurde, zumindest von einer nachträglichen Pflicht der Benachrichtigung, wie sie in § 33 Abs. 1 BDSG vorgesehen ist, auszugehen sein, um den Betroffenen nicht in der Ausübung seines Auskunfts- bzw. Widerspruchsrechts zu behindern. Es drängt sich bei diesem Ergebnis allerdings die Frage auf, ob immer dann, wenn eine Erhebung aufgrund einer Rechtsvorschrift erfolgt, der verantwortlichen Stelle nicht die Möglichkeit an die Hand gegeben wird, auf eine Unterrichtung generell zu verzichten und unabhängig davon, ob die Erhe-

[5] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 4 Rdnr. 17; *Gola/Schomerus*, BDSG, 46.

[6] Zum Umfang der Unterrichtungspflicht des § 4a Abs. 1 S. 2 BDSG vgl. oben unter Abschnitt E.II.1.d) auf Seite 98.

[7] So im Ergebnis auch noch *Gola/Schomerus*, BDSG in der Vorauflage, dort unter § 4 Rdnr. 46.

bung in Kenntnis oder Unkenntnis des Betroffenen stattfindet, stets auf eine nur nachträgliche Benachrichtigung zurückzugreifen.

Da ferner davon auszugehen ist, dass die letzte Änderung des § 4 Abs. 3 BDSG darin bestand, den Voraussetzungen des Art. 10 der EG-Datenschutzrichtlinie gerecht zu werden[8], welcher eine Gewährleistung einer Verarbeitung nach Treu und Glauben zum Zwecke hat[9], ist daher der Ansicht[10] Vorzug zu geben, nach der eine rechtmäßige Datenerhebung grundsätzlich auch die umfassende und ordnungsgemäße Information der betroffenen Person voraussetzt. Zu weitreichend wäre allerdings hierbei die Annahme, dass jede Erhebung, bei der der Betroffene nicht zuvor die in § 4 Abs. 3 S. 1 BDSG vorgeschriebenen Informationen erhält, per se unzulässig ist[11]. Richtig erscheint es vielmehr, gerade in Hinblick auf Art. 10 der EG-Datenschutzrichtlinie, die Frage der Zulässigkeit am Grundsatz von Treu und Glauben zu messen. Dies ergibt sich bereits aus dem Sinn und Zweck der Informationspflicht, mithin der Wahrung eines effektiven Rechtsschutzes[12] und der Ermöglichung einer selbstbestimmten Entscheidung über die Preisgabe der Daten zur eigenen Person[13]. Eine Zulässigkeit ist daher zumindest in den Fällen anzunehmen, in welchen dem Betroffene ohnehin keine Wahlmöglichkeit hinsichtlich der Preisgabe zustanden und ein effektiver Rechtsschutz dahingehend gewahrt wird, dass die Informationen frühzeitig und baldmöglichst nachgereicht werden. Ist hingegen davon auszugehen, dass der Betroffene im Falle einer ordnungsgemäßen Unterrichtung an einer Preisgabe seiner Daten weder mitgewirkt, noch diese ausdrücklich geduldet hätte oder hat sich die Möglichkeit zur Geltendmachung seines Auskunfts- und Widerspruchsrechts durch ihr Fehlen verzögert, führt

[8] BT-Drs. 14/4329, S. 34.
[9] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Art. 10 Rdnr. 1.
[10] *Sokol* in: *BDSG*, Simitis, § 4 BDSG, Rdnr. 57.
[11] So jedoch offenbar *Simitis* in: *BDSG*, Simitis, § 28 BDSG, Rdnr. 65, wobei nicht klargestellt wird, ob ein „Vorenthalten" von Informationen nicht nur dann angenommen wird, wenn die verantwortliche Stelle die Unterrichtung wissentlich und wollentlich unterlässt.
[12] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 10 Rdnr. 2.
[13] *Gola/Schomerus*, BDSG, § 4 Rdnr. 29; *Sokol* in: *BDSG*, Simitis, § 4 Rdnr. 39.

dies zur Unzulässigkeit der Erhebung mit den sich daraus ergebenden Rechtsfolgen.

### 2. Verstoß gegen § 4 Abs. 3 S. 2 BDSG

Bei Verstößen gegen die Unterrichtungspflicht des § 4 Abs. 3 S. 2 BDSG gilt es zu unterscheiden. Diese Vorschrift regelt einen Sonderfall der Erhebung durch Mitwirkung des Betroffenen, die sich einerseits durch die Auskunftspflicht aufgrund einer gesetzlichen Vorschrift, andererseits als Voraussetzung für die Gewährung von Rechtsvorteilen ergeben kann. Bezieht sich die Unterrichtungspflicht lediglich auf das Hinweisen des Vorhandenseins einer gesetzlichen Auskunftspflicht (Alternative 1) und hat der Betroffene ohnehin keine Wahlmöglichkeit hinsichtlich der Preisgabe seiner persönlichen Daten, führt ein Verstoß aus den selben Erwägungen, wie sie gerade zu Satz 1 stattgefunden haben, nicht zur Unzulässigkeit der Erhebung[14]. Von der Unterrichtungspflicht des § 4 Abs. 3 S. 2 1. Alt. BDSG sind im Übrigen aufgrund des Grundsatzes der Privatautonomie vorwiegend öffentliche Stellen betroffen.

Anders verhält es sich aber, wenn auf die Freiwilligkeit der Angaben als Voraussetzung für die Gewährung von Rechtsvorteilen hingewiesen werden muss (Alternative 2). Sinn und Zweck der Unterrichtungspflicht ist hier, dass der Betroffene selbstbestimmt abwägen soll, ob ihm die Gewährung eines rechtlichen Vorteils die Preisgabe der eigenen Daten wert ist. Wurde er über die Möglichkeit des Verzichts auf den rechtlichen Vorteil zum Zwecke des Schutzes der Daten nicht unterrichtet, könnte der Betroffene irrigerweise davon ausgehen, dass er zur Preisgabe der Daten auf jeden Fall verpflichtet ist, also das freiwillige Element und damit die Selbstbestimmung übersehen. Die daraus resultierende Gefährdung seines Grundrechts muss demnach im Falle eines Verstoßes stets eine Unzulässigkeit der Erhebung zu Folge haben.

[14] *Gola/Schomerus*, BDSG, 46 und *Schaffland/Wiltfang*, BDSG, § 4 Rdnr. 17; a.A., allerdings ohne Begründung, *Sokol* in: *BDSG*, Simitis, § 4 Rdnr. 59.

### 3. Verstoß gegen § 4a Abs. 1 S. 2 BDSG

Genau wie bei § 4 Abs. 3 S.2, 2. Alternative BDSG ist die Informationspflicht des § 4a Abs. 1 S. 2 BDSG Vorraussetzung für die Ausübung des Selbstbestimmungrechts. Der Betroffene erfährt durch § 4a Abs. 1 S. 2 BDSG dabei zum einen, dass es einzig von seinem freien Willen abhängt, ob eine Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten stattfindet, zum anderen wird er umfassend nicht nur über den vorgesehenen Zweck unterrichtet, wie von § 4a Abs. 1 S. 2 BDSG festgelegt, sondern auch über die Identität der verantwortlichen Stelle, die gewünschten Daten, evtl. Kategorien von Empfängern und evtl. Folgen der Verweigerung[15].

Nach § 4 Abs. 1 BDSG ist die Einwilligung des Betroffenen für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung Voraussetzung. Die Interessenlage liegt hier anders als bei der Erhebung, Verarbeitung und Nutzung aufgrund einer Rechtsvorschrift: Während der Gesetzgeber im Falle des Vorliegens der Vorraussetzungen eines Erlaubnistatbestandes die Interessenabwägung bereits zu Gunsten der verantwortlichen Stelle vorgenommen hat, hat eine solche immer dann, wenn eine Einwilligung des Betroffenen eingeholt werden muss, gerade nicht stattgefunden. Sie erfolgt vielmehr erst durch das Ausüben des informationellen Selbstbestimmungsrechts von Seiten des Betroffenen. Das Vorliegen einer Einwilligung begründet somit gerade die Zulässigkeit. Wird dem Betroffenen daher durch einen Verstoß gegen die Informationspflicht des § 4a Abs. 1 S. 2 BDSG die vollumfängliche Einsichtsfähigkeit und mit ihr die Möglichkeit einer hinreichend bestimmten Einwilligung genommen, muss dies stets die Unzulässigkeit der Erhebung, Verarbeitung und Nutzung zur Folge haben.

In diesem Zusammenhang sei überdies das im Gegensatz zum Telemediengesetz (dort § 12 Abs. 3 TMG) (noch[16]) nicht ausdrücklich normierte, aber doch

[15] Vgl. hierzu Abschnitt E.II.1.d) auf Seite 98.
[16] Zur dahingehend geplanten Gesetzesänderung siehe unter Abschnitt C.IV. auf Seite 70.

bestehende, generalisierte Koppelungsverbot hingewiesen. Der Vertragsschluss darf auch nach den allgemeinen Vorschriften nicht davon abhängig gemacht werden, dass der Betroffene den Vertragszweck nicht deckende Daten mitteilt. Dies ergibt sich aus der Voraussetzung der freien Entscheidung des § 4a Abs. 1 S. 1 BDSG. Daraus folgt, dass unabhängig davon, ob die Koppelung im Zusammenhang mit einer Arbeitsbeziehung, einem Versicherungsverhältnis einer Kontoeröffnung oder einem Krankenhausaufenthalt steht, diese stets unzulässig ist[17]. Ein Verstoß gegen das Koppelungsverbot führt zur Unwirksamkeit der Datenerhebung. Darüber hinaus ist ein derartiges „Abpressen“ von Daten als unzulässige Rechtsausübung im Sinne des § 242 BGB zu werten[18].

### 4. Verstoß gegen § 28 Abs. 4 S. 2 BDSG

Um der Erleichterung der Möglichkeit, personenbezogene Daten zum Zwecke der Werbung zu erheben, verarbeiten oder zu nutzen, wie sie in § 28 Abs. 1 Nr. 1, und 3, Abs. 3 Nr. 3 BDSG eröffnet wird, Rechnung zu tragen, wird dem Betroffenen in § 28 Abs. 4 S. 1 BDSG ein Widerspruchsrecht eingeräumt[19]. Über dieses Widerspruchsrecht ist der Betroffene gem. § 28 Abs. 4 S. 2 BDSG zu unterrichten[20].

Der Widerspruch selbst führt zu einem Verwendungsverbot, der gemäß § 28 Abs. 4 S. 1 BDSG eine Nutzung oder Übermittlung der Daten für Werbezwecke unzulässig macht[21]. Vor Geltendmachung des Widerspruchs bestimmt sich die Zulässigkeit dagegen weiterhin nach § 4 Abs. 1 BDSG, in Fällen der Erhebung, Verarbeitung und Nutzung zu Werbezwecken meist in Verbindung mit den soeben genannten § 28 Abs. 1 Nr. 1, und 3, Abs. 3 Nr. 3 BDSG.

[17] *Simitis* in: *BDSG*, Simitis, § 4a BDSG, Rdnr. 63.
[18] *Gola/Schomerus*, BDSG, § 4 Rdnr. 41.
[19] Vgl. *Gola/Schomerus*, BDSG, § 28 BDSG, Rdnr. 54; siehe aber zu den weitreichenden, geplanten Änderungen des § 28 Abs. 4 BDSG bereits unter Abschnitt C.IV. auf Seite 70.
[20] Siehe dazu ausführlich unter E.II.1.e).
[21] Vgl. *Simitis* in: *BDSG*, Simitis, § 28 BDSG, Rdnr. 303.

Das Fehlen der Unterrichtung führt hingegen nicht zur Unzulässigkeit, da durch das Fehlen allein noch nicht davon ausgegangen werden kann, dass der Betroffene im Falle der Kenntnis von seinem Widerspruchsrecht auch tatsächlich gebraucht gemacht hätte.

Sie stellt jedoch eine Ordnungswidrigkeit gemäß § 43 Abs. 1 Nr. 3 BDSG dar. Darüber hinaus kann der Betroffene einen Anspruch auf Schadensersatz haben, wenn ihm durch die Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten ein Schaden entstanden ist, welcher vermieden hätte werden können, wenn er durch rechtzeitige Kenntniserlangung seines Widerspruchsrechts von selbigen Gebrauch hätte machen können, § 7 BDSG[22].

### 5. Verstoß gegen § 33 Abs. 1 BDSG

§ 33 Abs. 1 BDSG dient der Transparenz der Datenverarbeitung, indem dem Betroffenen ermöglicht wird, seine Rechte auf Auskunft, Berichtigung, Sperrung und Löschung geltend zu machen[23]. Da § 33 Abs. 1 BDSG immer nur dann einschlägig ist, wenn erstmals personenbezogene Daten ohne Kenntnis des Betroffenen gespeichert werden, ist davon auszugehen, dass der Betroffene ohne die Benachrichtigung durch die verantwortliche Stelle gar nicht wüsste, dass eine eventuelle Ausübung seiner Rechte überhaupt nötig ist[24].

Die Frage der Zulässigkeit bestimmt sich hingegen weiterhin nach § 4 Abs. 1 BDSG, so dass ein Verstoß gegen die Benachrichtigungpflicht zwar zivil- und strafrechtliche Folgen[25] mit sich ziehen kann, nicht aber zur Unzulässigkeit der Speicherung führt.

[22] Dazu sogleich mehr unter Abschnitt G.III.5. auf Seite 176.
[23] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 33 BDSG, Rdnr. 9.
[24] *Dix* in: *BDSG*, Simitis, § 33, Rdnr. 1.
[25] Ein Verstoß gegen die Benachrichtigungspflicht ist zumindest ordnungswidrig, § 43 Abs. 1 Nr. 8 BDSG.

## II. Verstöße gegen Informationspflichten des Telemediengesetzes

Wie gerade im Rahmen des BDSG dargelegt, ergibt sich aus einem Verstoß gegen eine der Informationspflichten des TMG nicht zwangsläufig auch die Unzulässigkeit der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten. Die Zulässigkeit bestimmt sich vielmehr nach der zentralen Erlaubnisnorm des § 12 Abs. 1 TMG, wonach personenbezogene Daten nur dann erhoben und verwendet werden dürfen, wenn das TMG oder eine andere Rechtsvorschrift es erlauben oder der Nutzer eingewilligt hat. Der Erlaubnistatbestand für Bestandsdaten ist in § 14 Abs. 1 TMG normiert, der für Nutzungsdaten in § 15 Abs. 1 TMG und der für Abrechnungsdaten in § 15 Abs. 2 und 4 bis 7 TMG, wobei für die Missbrauchsbekämpfung noch die gesonderte Erlaubnis zur Verwendung von Nutzungs- und Abrechnungsdaten gem. § 15 Abs. 8 TMG gilt[26].

### 1. Verstoß gegen § 13 Abs. 1 S. 1 und 2 TMG

§ 13 Abs. 1 S. 1 TMG regeln die allgemeine Unterrichtungspflicht, die sich im BDSG unter § 4 Abs. 3 S. 1 findet. Dementsprechend gelten für sie die gleichen Erwägungen: Grundsätzlich führt ein Verstoß nicht zur Unzulässigkeit. Etwas anderes kann sich jedoch dann ergeben, wenn der Nutzer im Falle einer ordnungsgemäßen Unterrichtung an einer Preisgabe seiner Daten weder mitgewirkt, noch diese ausdrücklich geduldet hätte oder sich die Möglichkeit zur Geltendmachung seines Auskunfts- und Widerspruchsrechts durch ihr Fehlen verzögert hat.

Gleiches gilt auch für § 13 Abs. 1 S. 2 TMG, die sich zwar im Anknüpfungspunkt, Beginn des automatisierten Verfahrens, nicht aber im Inhalt von Satz 1 unterscheidet.

[26] Vgl. *Roßnagel* in: *Roßnagel*, Handbuch Datenschutzrecht, 7.9 Rdnr. 68.

## 2. Verstoß gegen § 13 Abs. 3 S. 1 TMG

Die Widerrufsmöglichkeit der Einwilligung mit ex nunc Wirkung für die Zukunft ist keine Besonderheit des Internetdatenschutzes, sondern besteht, wenn auch nicht ausdrücklich normiert, ebenso im allgemeinen Datenschutzrecht[27]. Die Besonderheit im Internetdatenschutzrecht liegt jedoch darin, dass über das Widerrufsrecht vor Abgabe der Einwilligung unterrichtet werden muss. Das Widerrufsrecht soll dabei dem Nutzer zum einen eine nachträgliche Kontrolle der zunächst gebilligten Verwendung seiner Daten ermöglichen, zum anderen schützt es ihn vor einer übereilt getroffenen Entscheidung[28].

Der Hinweis auf das Widerrufsrecht soll den Nutzer in die Lage versetzen, von der Möglichkeit des Widerrufes Kenntnis zu erlangen, um ihn eventuell ausüben zu können. Er ist als solcher daher Teil der informierten Einwilligung[29], ohne den der Nutzer sich über die Tragweite seiner Entscheidung mitunter nicht bewusst sein könnte. Um den Nutzer auch nach Abgabe der Einwilligung daran zu erinnern, dass er jederzeit die Wahl zwischen der Alternative hat, Dienste aufgrund seines Widerrufs eventuell nur noch unpersonalisiert nutzen zu können und derjenigen, dass Daten über ihn verarbeitet werden, muss der Diensteanbieter gemäß § 13 Abs. 3 S. 1 iVm Abs. 1 S. 3 TMG dafür Sorge tragen, dass der Inhalt der Unterrichtung jederzeit abrufbar ist. Der Gesetzgeber gibt damit zu erkennen, dass er im Bereich des Internetdatenschutzes, in dem eine elektronische Einwilligung nach § 13 Abs. 2 TMG möglich ist, die eine geringere Warnfunktion besitzt als die sonst übliche Schriftform[30], besonders grossen Wert darauf legt, dass der Nutzer nicht dem Irrtum unterliegt, er müsse an einer vorschnell abgegebenen Einwilligung festhalten.

[27] *Schaar*, Datenschutzrechtliche Einwilligung im Internet, 644–648; *Simitis* in: *BDSG*, Simitis, § 4a BDSG, Rdnr. 94; *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 4a BDSG, Rdnr. 24.
[28] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 288.
[29] *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 299.
[30] Vgl. *Bizer* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 217.

Die Hinweispflicht ist somit als Ergänzung der auch im Internetdatenschutzrecht gemäß § 12 Abs. 4 TMG anzuwendenden Hinweispflicht des § 4a Abs. 1 S. 2 BDSG zu sehen, aus deren Verstoß sich die Unzulässigkeit der Erhebung, Verarbeitung oder Nutzung ergibt.

### 3. Verstoß gegen § 13 Abs. 6 S. 2 TMG

Als eine Ausprägung des Gebotes der Datensparsamkeit verpflichtet § 13 Abs. 6 S. 1 TMG den Diensteanbieter immer, wenn es technisch zumutbar und möglich ist, sein Angebot in pseudonymer bzw. anonymer Form zu ermöglichen. Über diese Form der Nutzung ist der Nutzer gemäß S. 2 zu unterrichten. Um zu klären, in welchen Fällen die Unterrichtungspflicht entsteht, gilt es zunächst zu untersuchen, für welche Datentypen § 13 Abs. 6 TMG überhaupt anwendbar ist.

Teilweise wird vertreten[31], dass § 13 Abs. 6 TMG nur auf Nutzungsdaten anwendbar ist, so dass der Diensteanbieter nur die pseudonyme bzw. anonyme Inanspruchnahme zu ermöglichen hat, nicht aber auch den in ihrem Rahmen stattfindenden Vertragsabschluss. Diese Ansicht wird mit der Legaldefinition des § 15 Abs. 1 S. 1 TMG begründet, wonach Nutzungsdaten all diejenigen sind, die dazu erforderlich sind, eine Inanspruchnahme zu ermöglichen. Dagegen entstehen Bestandsdaten bei der Begründung, inhaltlichen Ausgestaltung oder Änderung von Vertragsverhältnissen (§ 14 Abs. 1 S. 1 TMG) und fallen somit nicht unter § 15 Abs. 6 TMG.

Diese Auslegung überzeugt nicht. Der Gesetzgeber definiert zwar in § 15 Abs. 1 S. 1 TMG Nutzungsdaten als solche, durch die eine Inanspruchnahme von Telediensten ermöglicht wird. Daraus ergibt sich aber nicht auch der Schluss, dass einzig und allein Nutzungsdaten für die Ermöglichung der Inanspruchnahme maßgeblich sind. Bestandsdaten können von der Inanspruchnahme vielmehr

[31] Dieser Ansicht folgt *Schmitz* in: *Hoeren/Sieber*, Handbuch Multimedia Recht, 16.4, Rdnr. 99.

nicht isoliert betrachtet werden. Es handelt sich bei beiden Datentypen um Nutzerdaten, die sich lediglich in ihrem Zweck unterscheiden. Bei kommerziellen Angeboten kann ein Datum folglich sowohl unter § 15 Abs. 1 S. 2 Nr. 1 TMG als auch unter § 14 Abs. 1 TMG fallen, wenn es mehrere Zwecke erfüllt. Dies wäre beispielsweise beim Namen des Nutzers eines Online-Spieles gegeben, da er zum einen zur Identifikation des Nutzers des Teledienstes dient, zum anderen aber auch zur Festlegung der Vertragspartei führt.

Die Ansicht übersieht daher, dass das Eingehen und Durchführen von Vertragsverhältnissen im Rahmen kommerzieller Online-Dienste mit der Nutzung einhergehen. Das Vertragsverhältnis ist häufig untrennbarer Bestandteil der Inanspruchnahme. Hätte der Gesetzgeber die Bestandsdaten von der Anwendung des § 15 Abs. 6 TMG ausschließen wollen, würde die Vorschrift gerade für diesen datenschutzrechtlich besonders relevanten Bereich ins Leere laufen: Wird erneut auf das Beispiel eines kostenpflichtigen Online-Spieles zurückgegriffen, so würde es zur reinen Erhebung von Nutzungsdaten nur solange kommen, so lange der Nutzer sich über die technischen Details und die Spielregeln informiert. Will er am Spiel aktiv teilnehmen, muss er zunächst einen Vertrag mit dem Diensteanbieter abschließen, in dem er zumindest seinen Namen, die Kreditkartendaten und den Abonnementszeitraum hinterlässt. In der Nutzung des Spieles besteht aber gerade der Kern der Inanspruchnahme des Dienstes. Eine vollumfängliche Inanspruchnahme gemäß § 15 Abs. 6 TMG setzt somit bei richtiger Auslegung des Tatbestandsmerkmals der Ermöglichung nicht nur die rein technische Ermöglichung, wie sie § 15 Abs. 1 S. 1 TMG im Auge hat voraus, sondern vielmehr auch die rechtliche.

Da bei Herstellung der rechtlichen Ermöglichung durch Abschließen eines Vertrages Bestandsdaten entstehen, wenn nicht eine anonyme bzw. pseudonyme Alternativmöglichkeit angeboten wird, fallen diese ohne weiteres unter § 13 Abs. 6 TMG, weil eine Inanspruchsnahme eines Teledienstes unter Entstehung von Bestandsdaten insgesamt als nicht anonym bzw. pseudonym einzuordnen

ist. Der Sinn und Zweck von § 13 Abs. 6 TMG, Daten zu vermeiden[32], könnte unter Ausschluss seiner Anwendbarkeit auch auf Bestandsdaten gar nicht erreicht werden.

Eine pseudonyme Nutzungsmöglichkeit wäre hier im Verkauf sog. PrePaid-Game-Cards zu sehen, die ähnlich wie die Karten im Mobilfunkbereich mit einer bestimmten Nutzungszeit „beladen“ sind und die in jedem Fachhandel anonym gegen eine bestimmte Summe Bargeld gekauft werden kann.

Kommerzielle Dienste wie das Online-Spiel dieses Beispiels stellen gleichzeitig den Hauptanwendungsbereich des § 13 Abs. 6 TMG dar, da bei nichtkommerziellen Angeboten in aller Regel keine Identifikation des Nutzers notwendig ist. Geht es nämlich nur darum, dem Nutzer ein persönlich gestaltetes Angebot anzubieten, ist es ausreichend, diesen unter einem anonymen Benutzernamen zu speichern. Der Gesetzgeber hat in § 13 Abs. 6 TMG ferner ausdrücklich auch die Ermöglichung der anonymen oder pseudonymen Bezahlung vorgesehen, welche klassischerweise nur in Erfüllung einer vertraglichen Leistungspflicht und somit unter Entstehung von Bestandsdaten stattfinden wird.

Somit ergibt sich bei teleologischer Auslegung des § 13 Abs. 6 TMG, dass dieser auch auf Bestandsdaten anzuwenden ist[33].

Ob ein Verstoß gegen die Unterrichtungspflicht des § 13 Abs. 6 S. 2 TMG jedoch auch die Unzulässigkeit der Erhebung zur Folge hat, hängt davon ab, wie die Angebotspflicht des Diensteanbieters rechtlich einzuordnen ist. Es wäre denkbar, dass es sich dabei um eine weitere Voraussetzung der Erlaubnistatbestände für Bestands- und Nutzungsdaten handelt. In diesem Fall wäre eine Erhebung nach den §§ 14, 15 TMG nur unter dem Vorbehalt zulässig, dass die anonyme oder pseudonyme Inanspruchnahme von Telediensten und ihre Bezahlung entweder technisch nicht möglich oder nicht zumutbar war[34].

[32] *Schulz* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 422; *Dix* in: *Roßnagel*, Handbuch Datenschutzrecht, Kapitel 3.5 Rdnr. 19 ff.; *Bizer* in: *BDSG*, Simitis, § 3a Rdrn. 73f.

[33] So im Ergebnis auch *Scholz*, Datenschutz beim Internet-Einkauf, S. 207.

[34] Vgl. *Gundermann*, E-Commerce trotz oder durch Datenschutz?, 225–235.

Folgerichtig müßte dann auch ein Verstoß gegen die Unterrichtungspflicht zur Unzulässigkeit der Erhebung führen: Sowohl bei einem Verstoß gegen die Pflicht der Zurverfügungstellung der Möglichkeit als auch bei Verstoß gegen die Pflicht der Unterrichtung über das Bestehen der Möglichkeit einer anonymen bzw. pseudonymen Inanspruchnahme oder Bezahlung, ist nicht auszuschließen, dass es bei ordnungsgemäßer Erfüllung der jeweiligen Pflicht erst gar nicht zur Entstehung von personenbezogenen Daten gekommen wäre.

Aus dem Wortlaut der Vorschriften ergeben sich jedoch wenig Anhaltspunkte, dass der Gesetzgeber die Datenverarbeitungsbefugnisse der §§ 14, 15 TMG nur unter den Voraussetzungen des § 13 Abs. 6 S. 1 TMG gewähren wollte. Hätte der Gesetzgeber einen dahingehenden Willen gehabt, wäre es ihm ohne weiteres möglich gewesen diesen, wie in der datenschutzrechtlichen Gesetzgebung der Länder teilweise geschehen[35], eindeutig zu formulieren[36].

Eine dahingehende Auslegung würde ferner zu einer gewissen Rechtsunsicherheit führen: Maßgeblich dafür, ob die Pflicht aus § 13 Abs. 6 S. 1 TMG erfüllt ist, ist fast ausschließlich die Frage, ob die Schaffung der Möglichkeit für den Diensteanbieter zumutbar ist. Die Voraussetzung der technischen Umsetzbarkeit wird hingegen selten eine Rolle spielen, da nur wenig Fälle denkbar sind, in denen die Technik eine anonyme bzw. pseudonyme Nutzung verhindert: Bereits für eine anonyme Inanspruchnahme reicht allein ein passives Tun des Diensteanbieters aus. Erstellt dieser keine Logdateien, legt er auf dem Rechner des Nutzers keine Cookies mit personenbezogenen Inhalt ab und stellt er dem Benutzer auch keine Formulare zur Verfügung, mittels derer der Nutzer personenbezogene Inhalte übermittelt, kann es noch nicht einmal zu einer versehentlichen Erhebung von personenbezogenen Daten kommen. Bezüglich der anonymen Bezahlungsweise kann sich der Anbieter hingegen Bezahlsystemen wie Click&Buy bedienen, bei denen zwar der Anbieter des Bezahlsystems den Namen und die Konto- oder Kreditkartendaten des Nutzers erfährt, die Über-

[35] Vgl. z.B. § 28 Abs. 2 DSG NRW.
[36] *Gundermann*, E-Commerce trotz oder durch Datenschutz?, 225–235.

mittlung des Geldes zwischen dem Diensteanbieter und dem Nutzer hingegen anonym verläuft[37].

Der Begriff der Zumutbarkeit ist relativ, da er die unterschiedliche subjektive Leistungsfähigkeit von Unternehmen berücksichtigt[38]. So kann beispielsweise das Angebot der anonymen Bezahlung, welches für ein größeres Unternehmen ohne Weiteres zumutbar ist, für ein anderes einen unverhältnismäßig hohen Zeit- und Kostenaufwand[39] bedeuten und damit unzumutbar sein. Es muss dabei für jeden Einzelfall geprüft werden, ob die Verhältnismäßigkeit zwischen den grundrechtlich geschützten Interessen des Diensteanbieters und dem Recht auf informationelle Selbstbestimmung des Nutzers gegeben ist[40]. Ob eine bestimmte Maßnahme zur Pseudonymisierung bzw. Anonymisierung für den jeweiligen Diensteanbieter im Einzelnen zumutbar gewesen wäre, ist dabei vom Diensteanbieter zu beweisen[41]. Für den Nutzer hingegen, der allein aufgrund des Online-Angebots meist keinerlei Einsicht in die Größe und Struktur des Unternehmens des Diensteanbieters erhält, ist das Kriterium der Zumutbarkeit nicht greifbar. Die Frage, ob eine zulässige Datenverarbeitung vorlag, darf daher nicht von diesem schwer handhabbaren Begriff abhängen[42].

[37] Zur technischen Funktionsweise von Click&Buy: *Grimm* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, S. 37f; zur technischen Funktionsweise und den Rechtsrahmen von elektronischen Zahlungssystemen: *Hoenike/Szodruch*, Rechtsrahmen innovativer Zahlungssysteme für Multimediadienste, 519–526.

[38] BT-Drs. 13/7385, S. 23; *Engel-Flechsig/Maennel/Tettenborn*, Das neue Informations- und Kommunikationsdienste-Gesetz, S. 2981–2990; *Schulz* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 443.

[39] *Engel-Flechsig* in: *Engel-Flechsig/Maennel/Tettenborn*, Beck'scher IuKDG-Kommentar, § 4 TDDSG, Rdnr. 12.

[40] *Schulz* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 443; aA hingegen *Roßnagel* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, S. 198, welcher entgegen der Begründung des Gesetzgebers, der in BT-Drs. 13/7385, S. 23 selbst subjektive Kriterien aufführt, auch auf den objektiven Bewertungsmaßstab der branchenbezogenen durchschnittlichen Zumutbarkeit abstellt.

[41] *Schulz* in: *Roßnagel*, Recht der Multimedia-Dienste, § 4 TDDSG, Rdnr. 445.

[42] *Roßnagel* in: *Roßnagel*, Handbuch Datenschutzrecht, 7.9, Rdnr. 115.

Im Ergebnis führt also weder ein Verstoß gegen § 13 Abs. 6 S. 1 TMG, noch die auf seinen Inhalt verweisende Informationspflicht des Satzes 2 zu einer Unzulässigkeit der daraus resultierenden Datenerhebung.

### 4. Verstoß gegen § 15 Abs. 3 S. 2 TMG

Zunächst ergibt sich aus § 15 Abs. 3 S. 2 TMG, dass der Nutzer auch dann nach § 13 Abs. 1 TMG zu unterrichten ist, wenn der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste pseudonyme Nutzungsprofile erstellt. Diese Regelung stellt insofern eine Besonderheit dar, als dass die Unterrichtungspflicht nach § 13 Abs. 1 TMG grundsätzlich nur bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten entsteht, pseudonyme Daten hingegen nur einen relativen Personenbezug[43] aufweisen.

Über die allgemeine Unterrichtungspflicht hinaus, hat der Diensteanbieter den Nutzer auch über sein Widerspruchsrecht nach § 15 Abs. 3 S. 1 TMG zu unterrichten. Hinsichtlich der Frage der Zulässigkeit der Verwendung von Pseudonymen bei der Erstellung von Nutzungsprofilen ergeben sich die selben Erwägungen, die schon bei § 28 Abs. 4 S. 2[44] BDSG: Die fehlende Unterrichtungspflicht führt für sich gesehen noch nicht zur Unzulässigkeit der Erstellung. Die Frage, ob der Benutzer bei ausreichender Unterrichtung einer Nutzung seiner Daten widersprochen hätte, spielt hingegen bei der Frage evtl. Schadensersatzansprüche eine Rolle. Ferner ist zu beachten, dass es bei der Erstellung von Nutzungsprofilen, die über die in § 15 Abs. 3 S. 1 TMG genannten Zwecke hinausgehen, der Einwilligung des Nutzers bedarf.

[43] Zum Personenbezug von pseudonymen Daten siehe bereits ausführlich unter Abschnitt D.VI.1.b) auf Seite 89.
[44] Siehe unter Abschnitt G.I.4. auf Seite 160.

## III. Rechte des Betroffenen aus dem BDSG

Die soeben und bereits unter Abschnitt E. auf Seite 95 dargestellten Informationspflichten sollen den Betroffenen/den Nutzer, gekoppelt mit seinen Auskunftsansprüchen[45] in die Lage versetzen, Kenntnis darüber zu erlangen, ob die über ihn erhobenen Daten richtig sind und ob die Erhebung, Verarbeitung oder Nutzung auf zulässige Art und Weise vonstatten gegangen ist. Dementsprechend finden sich im BGSG selbst auch Eingriffsrechte, welche an die Unzulässigkeit bzw. Unrichtigkeit der Speicherung anknüpfen, wobei sich die Unzulässigkeit, wie gerade festgestellt, schon aus dem Verstoß gegen die Informationspflichten ergeben kann. Die Eingriffsrechte des Betroffenen sind in § 35 BDSG geregelt.

Darüber hinaus kann der Betroffene, wenn er durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung einen Schaden erlitten hat, nach § 7 BDSG verlangen, diesen ersetzt zu bekommen.

### 1. Berichtigung

Gemäß § 35 Abs. 1 S. 1 BDSG sind personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Unrichtig sind personenbezogene Daten zum einen, wenn sie falsch sind (z.B. Schreibfehler, falsches Geburtsjahr, falsche Anschrift), zum anderen, wenn sie unvollständig sind und dadurch einen falschen Eindruck vermitteln[46]. Der Begriff „Unrichtig“ hat dieselbe Bedeutung wie „der Wahrheit zuwider“ (§ 824 BGB)[47]. Es können immer nur Tatsachen unrichtig sein, keine Werturteile. So können Werturteile zwar auch personenbezogene Daten sein, sie entziehen sich aber der Überprüfung ihrer Richtigkeit. Es gelten

[45] Ebenfalls unter Abschnitt E. auf Seite 95 erläutert.
[46] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 35, Rdnr. 26; *Gola/Schomerus*, BDSG, § 20, Rdnr. 3.
[47] *Mallmann* in: *BDSG*, Simitis, § 20 BDSG, Rdnr. 11.

hier die selben Erwägungen wie bei allgemeinen zivilrechtlichen Beseitigungsanspruch des § 1004 Abs. 1 S. 1 BGB[48].

Die Unrichtigkeit der personenbezogenen Daten hat dabei keinen Unwertgehalt[49]. Es gibt weder eine Pflicht der verantwortlichen Stelle, nur richtige Daten zu verarbeiten, noch führt jede Unrichtigkeit zu einer Beeinträchtigung des Persönlichkeitsrechts[50]. Auch ist es unerheblich, ob die unrichtige Speicherung versehentlich oder absichtlich erfolgte[51].

Das Recht auf Berichtigung ist dabei nicht lediglich ein Anspruch. Es besteht vielmehr auch ohne Antrag des Betroffenen eine Pflicht der verantwortlichen Stelle auf Korrektur der Unrichtigkeit, sobald diese Kenntnis davon erlangt[52]. Dabei ist jedoch davon auszugehen, dass die verantwortliche Stelle von der Unrichtigkeit spätestens dann Kenntnis nimmt, wenn der Betroffene einen Berichtigungsantrag stellt.

Eine Ausnahme von der Berichtigungpflicht ergibt sich aus § 35 Abs. 6 BDSG, wenn die verantwortliche Stelle die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung speichert, die Daten aus allgemein zugänglichen Quellen gespeichert wurden und sie zu Dokumentationszwecken gespeichert wurden. Es handelt sich hierbei beispielsweise um Stellen, die Presseauswertungen, also Ereignisse, die von jedermann zur Kenntnis genommen werden können, geschäftsmäßig zur Verfügung stellen[53]. Im Internet läßt sich ein solcher Dienst unter `http://news.google.de` finden, wo zu jeder Schlagzeile eine Linksammlung von Seiten angezeigt wird, die zu dieser Nachricht

[48] *Mallmann* in: *BDSG*, Simitis, § 20 BDSG, Rdnr. 17; BGH, NJW 1989, 2942; *Sprau* in: *Palandt*, BGB, Einf v § 823, Rdnr. 28 m. w. N.; *Rixecker* in: *Rebmann/Säcker/Rixecker*, MüKo, APKR, Rdnr. 146.

[49] *Gola/Schomerus*, BDSG, § 20 BDSG, Rdnr. 2.

[50] So ist z.B. eine Speicherung eines Kundennamens als „Stephan Maier“ unrichtig, falls dieser „Stefan Meier“ heisst. Trotzdem wird in diesem Falle nur schwer davon auszugehen sein, dass er sich durch die falsche Schreibweise in seinem Persönlichkeitsrecht verletzt fühlt.

[51] *Schaffland/Wiltfang*, BDSG, § 25 BDSG, Rdnr. 5.

[52] *Wedde* in: *Roßnagel*, Handbuch Datenschutzrecht, Kapitel 4.4, Rdnr. 559.

[53] *Gola/Schomerus*, BDSG, § 35 BDSG, Rdnr. 7.

ebenfalls einen Artikel veröffentlicht haben. Eine Berichtigung würde in diesen Fällen eine eigenständige Ausarbeitung der Quelle erfordern, was dem Dokumentationszweck zuwiderlaufen würde. Der Gesetzgeber hat dem Betroffenen daher statt des Rechtes auf Berichtigung ein Recht auf Gegendarstellung eingeräumt (§ 35 Abs. 6 S. 2 BDSG). Nimmt der Betroffene dieses Recht wahr, so dürfen seine Daten nicht mehr ohne die Gegendarstellung übermittelt werden (Satz 3).

### 2. Löschung

Nach der Legaldefinition des § 3 Abs. 4 Nr. 5 BDSG ist Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten. Dem Grundsatz der Datenvermeidung folgend, steht es der verantwortlichen Stelle nach § 35 Abs. 2 S. 1 BDSG grundsätzlich frei, Daten zu löschen, falls dem nicht eine Aufbewahrungsfrist entgegensteht (Abs. 3 Nr. 1) oder schutzwürdige Interessen des Betroffenen durch die Löschung überwiegen (Abs. 3 Nr. 2).

Wie schon beim Anspruch auf Berichtigung ist auch der Anspruch des Betroffenen auf Löschung der Daten jedoch mit einer Pflicht zur Löschung von Seiten der verantwortlichen Stelle unverzüglich ab dem Zeitpunkt der Kenntnisnahme gekoppelt, wenn die Voraussetzungen des § 35 Abs. 2 S.2 BDSG gegeben sind[54]. Dieser sieht eine Pflicht zur Löschung in vier verschiedenen Fällen vor. Nach § 35 Abs. 2 S. 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen, wenn die Speicherung der Daten unzulässig ist. An dieser Stelle wird auf die Ausführungen das vorhergehenden Abschnittes verwiesen: Führt der Verstoß gegen eine Informationspflicht unmittelbar zur Unzulässigkeit der Speicherung, so ergibt sich daraus im selben Zuge auch der Anspruch auf und die Pflicht zur Löschung der daraus entstandenen Daten.

Nach Nr. 2 besteht eine Löschungspflicht bei den dort aufgeführten besonders sensitiven Daten (z.B. Daten über rassische oder ethnische Herkunft, Da-

[54] *Dix* in: *BDSG*, Simitis, § 35, Rdnr. 23.

ten über Gesundheit oder das Sexualleben), wenn die Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann. Die Vorschrift bildet eine Sonderregelung zu § 35 Abs. 4 BDSG, wonach die Daten zu sperren sind, falls der Betroffene die Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit beweisen lässt[55]. Anders als bei § 35 Abs. 4 kann wegen der besonderen Sensitivität der Daten eine Unklarheit über ihre Richtigkeit nicht genügen.

Die Nr. 3 und 4 des § 35 Abs. 2 S. 2 BDSG stellen die jeweiligen Parallelnormen zu den Erlaubnistatbeständen der §§ 28 und 29 BDSG dar. Gemäß Nr. 3 sind personenbezogene Daten bei Erfüllung des Zwecks der Speicherung zu löschen, wenn die Daten für eigene Zwecke verarbeitet wurden. Die Prüfung, ob ein späterer Wegfall der Erforderlichkeit der Speicherung vorliegt, hat sich an § 28 BDSG zu orientieren[56]. § 35 Abs. 2 S. 2 Nr. 3 BDSG ist dabei eine konsequente Fortführung des bereits in § 28 BDSG umgesetzten Prinzips der Erforderlichkeit: Während § 28 BDSG die Zwecke, für die eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig ist, restriktiv festsetzt, sorgt § 35 Abs. 2 S. 2 Nr. 3 dafür, dass die Daten nicht über ihre Erfüllung hinaus gespeichert werden.

Den selben Sinn und Zweck verfolgt auch § 35 Abs. 2 S. 2 Nr. 4 BDSG, welcher jedoch den Sonderfall der geschäftsmäßigen Verarbeitung zum Zwecke der Übermittlung Rechnung trägt. Die Zulässigkeit der Erhebung, Speicherung und Veränderung personenbezogener Daten zu diesem Zweck ist in § 29 BDSG geregelt. Die Überprüfung der weitergehenden Erforderlichkeit der Speicherung hat in diesem Fall jeweils am Ende des vierten Kalenderjahres vom Zeitpunkt ihrer erstmaligen Speicherung aus beginnend stattzufinden.

Neben oder schon vor dem Anspruch auf Löschung kann der Betroffene einen Anspruch auf Anonymisierung der Daten als „Minus“ zur Löschung geltend

[55] Siehe dazu sogleich.
[56] *Schaffland/Wiltfang*, BDSG, § 35, Rdnr. 35.

machen[57]. Ein solcher Anspruch ist im Wortlaut des § 35 Abs. 2 BDSG nicht vorgesehen, er ergibt sich jedoch aus dem Sinn und Zweck der Norm, den zunächst bestehenden Personenbezug nachträglich aufzuheben[58].

### 3. Sperrung

Wie gerade erwähnt, tritt nach § 35 Abs. 3 BDSG an die Stelle der Löschung die Sperrung der Daten, wenn der Löschung Aufbewahrungsfristen entgegenstehen (Nr. 1) oder durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden (Nr. 2). „Sperren“ ist nach der Legaldefinition des § 3 Abs. 4 Nr. 4 BDSG das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

Daten sind ferner zu sperren statt zu löschen, falls eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist (Nr. 3). Diese Vorschrift soll betriebswirtschaftlich unsinnige Forderungen ausschließen und ist daher restriktiv auszulegen[59]. Mit dem heutigen Stand der Technik, durch den wiederbeschreibbare Medien wie CDs und DVDs oder auch Massenspeicher (Festplatten) kostengünstig geworden sind, ist zumindest auf der Ebene der elektronischen Datenverarbeitung ein unverhältnismäßig großer Aufwand nur ausnahmsweise anzunehmen.

Neben den in § 35 Abs. 3 BDSG geregelten Fällen sieht Abs. 4 die Sperrung bei sog. Non-Liquet-Situationen vor. Der Betroffene muss dafür die Richtigkeit der personenbezogenen Daten gegenüber der speichernden Stelle bestritten haben und die Richtigkeit darf durch die verantwortliche Stelle nicht bewiesen werden können. Den Betroffenen trifft dabei zwar die Beweislast für das Bestreiten der Richtigkeit, er muss das Vorliegen der Unrichtigkeit jedoch nicht durch die Angabe richtiger Daten nachweisen. Anderenfalls hätte die verant-

[57] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 178.
[58] *Dix* in: *BDSG*, Simitis, § 35, Rdnr. 43.
[59] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 35, Rdnr. 107; *Wedde* in: *Roßnagel*, Handbuch Datenschutzrecht, Kapitel 4.4, Rdnr. 74.

wortliche Stelle die Möglichkeit, durch das bewusste Speichern falscher Daten den Betroffenen auszuforschen, um die Offenbarung richtiger Daten zu erreichen[60].

Die Sperrung der Daten hat ein relatives Nutzungsverbot zur Folge, dessen Ausnahmen in § 35 Abs. 8 BDSG geregelt sind[61]. Die Zweckbindung wird danach dahingehend verschärft, dass gesperrte Daten ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden dürfen, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist (§ 35 Abs. 8 Nr. 1 BDSG). Unerlässlich ist die Übermittlung oder Nutzung des Daten nur dann, wenn der Zweck ohne die „Entsperrung" der Daten nicht erreicht werden kann[62]. Zusätzlich hätte die Übermittlung oder die Nutzung zu den genannten Zwecken zulässig sein müssen, wenn sie nicht gesperrt worden wären (Nr. 2).

### 4. Widerspruch

§ 35 Abs. 5 regelt das Widerspruchsrecht gegen die Erhebung, Verarbeitung oder Nutzung für die Fälle, in denen das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation dem Interesse der verantwortlichen Stelle überwiegt. Der Gesetzgeber hat mit dieser Vorschrift Art. 14 Buchst. a der EG-Datenschutzrichtlinie umgesetzt. Gemäß Satz 2 ist das Widerspruchsrecht ausgeschlossen, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet. Um das Widerspruchsrecht auszuschließen, muss die Rechtsvorschrift dazu tatsächlich verpflichten, es genügt nicht, dass die Norm die Erlaubnis zur Erhebung, Verarbeitung oder Nutzung

[60] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 35, Rdnr. 112; *Gola/Schomerus*, BDSG, § 35, Rdnr. 18.
[61] *Dix* in: *BDSG*, Simitis, § 35, Rdnr. 45; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 597.
[62] *Gola/Schomerus*, BDSG, § 35, Rdnr. 21.

erteilt. Es handelt sich also um Normen, die Privatunternehmen konkret vorschreiben, personenbezogene Daten an staatliche Stellen zu übermitteln oder zumindest bereitzuhalten[63]. In den Fällen, in denen die Erhebung, Verarbeitung oder Nutzung hingegen beispielsweise aufgrund von § 28 BDSG erfolgte, bleibt der Widerspruch möglich.

### 5. Schadensersatz

Die in § 35 BDSG geregelten Korrekturrechte stellen zwar für den Betroffenen ein geeignetes Mittel dar, seine schutzwürdigen Interessen für die Zukunft gegenüber der verantwortlichen Stelle zu sichern, sie vermögen aber nicht die Unrechtslage zu beheben, die dadurch entstanden ist, wenn diese in der Vergangenheit durch eine unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung verletzt wurden.

Daher hat der Gesetzgeber mit § 7 BDSG erstmalig und in Umsetzung des Art. 23 der EG-Datenschutzrichtlinie eine eigenständige Verschuldenshaftung im BDSG für den nicht-öffentlichen Bereich geschaffen[64].

Die Voraussetzung der unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung als *haftungsbegründender* Datenverstoß wurde dabei von § 8 BDSG a.F. wortgleich übernommen und erscheint auf den ersten Blick dogmatisch unsauber. Die Begriffe „unzulässig“ und „unrichtig“ überschneiden sich, weil eine unrichtige Datenverarbeitung regelmäßig auch unzulässig ist[65]. Der Gesetzgeber wollte jedoch damit einen möglichst umfassenden Schutz bezwecken, welcher keine Zweifel an der Reichweite zulässt[66]. Er knüpft überdies an

[63] *Gola/Schomerus*, BDSG, § 35, Rdnr. 29.

[64] BT-Drs. 14/4329, S. 38; Im BDSG 1990 war hingegen für die Erhebung, Verarbeitung oder Nutzung durch nicht-öffentliche Stellen lediglich eine Beweislastumkehr für das Verschulden in § 8 BDSG vorgesehen; a.A. hier aber *Hoeren*, Internet- und Kommunikationsrecht, Rdnr. 655, der in § 7 BDSG auch weiterhin nur eine Norm lediglich zur Beweiserleichterung sieht

[65] *Gola/Schomerus*, BDSG, § 7 BDSG, Rdnr. 4.

[66] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 7 BDSG, Rdnr. 6; *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 18.

die Korrekturrechte an, welche ebenfalls eine Trennung zwischen Unrichtigkeit (§ 35 Abs. 1 BDSG) und Unzulässigkeit (§ 35 Abs. 2 Nr. 1 BDSG) vollziehen.

Wie aus § 7 S. 2 BDSG ersichtlich, setzt die Schadensersatzpflicht ein Verschulden der verantwortlichen Stelle voraus. Die Definition des Verschuldens als die Nichtbeachtung der nach den Umständen des Falles gebotene Sorgfalt weicht dabei von § 276 Abs. 2 BGB ab, wonach fahrlässig handelt, wer die *im Verkehr* erforderliche Sorgfalt außer Acht läßt[67]. Nach § 7 S. 2 BDSG hat die verantwortliche Stelle zu beweisen, dass ein Verschulden ihrerseits nicht vorgelegen hat (Exkulpation). Insofern findet eine Beweislastumkehr zu Lasten der verantwortlichen Stelle statt. Das Gesetz hat hier dem Umstand Rechnung getragen, dass dem Betroffenen der Einblick in die Datenverarbeitungsvorgänge der verantwortlichen Stelle in aller Regel fehlt, ihm somit ein Beweis des Verschuldens meist nicht möglich wäre.

Verwunderlich erscheint jedoch in diesem Zusammenhang, dass der Gesetzgeber nicht an dem Wortlaut des § 8 BDSG a.F. festgehalten hat, wonach die verantwortliche Stelle auch zu beweisen hatte, dass der Schaden keine Folge des von ihr zu vertretenden Umstandes war. Nach § 8 BDSG a.F. wurde die Beweislast somit auch auf den Ursachenzusammenhang zwischen der unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten und dem den Betroffenen entstandenen Schaden ausgeweitet (sog. *haftungsausfüllende* Kausalität[68]). Bei wortgetreuer Auslegung des § 7 S. 2 BDSG wäre die Beweislastumkehr hingegen lediglich auf das Verschulden beschränkt. Es spricht jedoch einiges dafür, dass es sich dabei um ein Versehen des Gesetzgebers handelt: Zum einen wollte der Gesetzgeber mit Satz 2 den Artikel 23 Abs. 2 der EG-Datenschutzrichtlinie umsetzen[69], welcher vorsieht, dass der für die „Verarbeitung Verantwortliche“ von seiner Haftung befreit

[67] *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 121.

[68] Siehe dazu ausführlich *Oetker* in: *Rebmann/Säcker/Rixecker*, MüKo, § 249 BGB, Rdnr. 99 ff.; *Sprau* in: *Palandt*, BGB, Einf v § 823, Rdnr. 2a; *Rönnau/Faust/Fehling*, Durchblick: Kausalität und objektive Zurechnung, 113–118.

[69] BT-Drs. 14/4329, S. 38.

werden kann, „wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann“ . Die Formulierung der Richtlinie bezieht sich daher sowohl auf das Verschulden als auch auf die haftungsausfüllende Kausalität. Zum anderen würde eine Beschränkung des Satzes 2 auf das Verschulden den Sinn und Zweck der Norm widersprechen, den Betroffenen davon zu befreien, Umstände beweisen zu müssen, die ihm ohne den Einblick in die Organisation der verantwortlichen Stelle verwehrt bleiben. So ist es dem Betroffenen dahingehend noch schwerer möglich, den exakten Verlauf der Schädigung zu beschreiben, als lediglich das Verschulden darzulegen[70].

Neben der Exkulpationsmöglichkeit des § 7 S. 2 BDSG steht der verantwortlichen Stelle im Übrigen eine mit § 831 Abs. 1 S. 2 BGB vergleichbare Entlastung nicht zu, da dieser einzig und allein dann greift, wenn das Verhalten der verantwortlichen Stelle zwar den gesetzlichen Anforderungen entsprach, ein Schaden aber trotzdem nicht verhindert werden konnte. Ein solcher Fall ist aber allenfalls dann denkbar, wenn ein mißbräuchlicher Eingriff eines Außenstehenden vorgenommen wurde. Fehler oder Nachlässigkeiten des Personals innerhalb der verantwortlichen Stelle liegen hingegen ausserhalb seines Anwendungsbereiches[71].

Mangels spezialgesetzlicher Regelungen bestimmen sich Art, Inhalt und Umfang des Schadensersatzes nach den §§ 249 ff. BGB. Danach ist dem Geschädigten grundsätzlich gemäß § 249 Abs. 1 BGB der hypothetisch schadensfreie

[70] Ebenso *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 23; *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 7 BDSG, Rdnr. 17; *Gola/Schomerus*, BDSG, § 7 BDSG, Rdnr. 11; a.A. *Schaffland/Wiltfang*, BDSG, § 7 BDSG, Rdnr. 2; zum Problem der Beweislastverteilung bei Datenschutzverstößen siehe auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 181 f.

[71] *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 25; *Gola/Schomerus*, BDSG, § 7 BDSG, Rdnr. 10, will eine darüber hinausgehende Exkulpation aber zumindest dann zulassen, wenn die unzulässige Datenverarbeitung auf rein persönliche Motive des Arbeitnehmers resultierte.

Zustand wiederherzustellen (Grundsatz der Totalreparation)[72]. Wie aus § 251 Abs. 1 BGB ersichtlich, geht die in § 249 Abs. 1 BGB vorgesehen Naturalrestitution der Kompensation vor. Ausser in den nachgeordneten Fällen der Kompensation ist im Rahmen der Restitution ein Anspruch auf Geldersatz nur dann gegeben, wenn entweder ein Personen- oder Sachschaden vorliegt (§ 249 Abs. 2 S. 1 BGB) oder bei immateriellen Schäden, wenn die Voraussetzungen des § 253 BGB gegeben sind[73].

Es stellt sich daher zunächst die Frage nach den durch Verstoß gegen datenschutzrechtliche Vorschriften überhaupt in Betracht kommenden Vermögensschäden und der Möglichkeit einer daraus resultierenden Naturalrestitution. Die Beantwortung dieser Frage führt dabei direkt zum Hauptproblem des Schadensersatzes bei Verstößen gegen das Datenschutzrecht. Schon aus dem Schutzzweck, dem Schutz des Rechtes auf informationelle Selbstbestimmung, wird ersichtlich, dass der Betroffene im Falle eines Verstoßes nur in Ausnahmefällen einen Vermögensschaden erleiden wird. Ein solcher Fall ist beispielsweise denkbar, falls der Betroffenen aufgrund des Öffentlichwerdens diskreditierender Informationen seine Arbeitsstelle verliert, er nicht eingestellt wird oder ihm kein Kredit gewährt wird[74]. Ferner kann ein materieller Schaden auch dann entstehen, wenn dem Betroffenen die Geltendmachung von Ansprüchen infolge der Löschung wichtiger Daten unmöglich gestaltet wurde oder der Betroffenen Aufwendungen für die Schadensabwendung (z.B. Rechtsverfolgung, richtigstellende Anzeigenaktionen) getätigt hat[75].

[72] *Schiemann* in: *Staudinger*, Kommentar zum BGB, § 249 BGB, Rdnr. 1; *Heinrichs* in: *Palandt*, BGB, Vorb v § 249 BGB, Rdnr. 5; *Schlechtriem, Peter*, Schuldrecht AT, Rdnr. 298.

[73] Zu Systematik des deutschen Schadensrecht siehe ausführlich in *Brox/Walker*, Schuldrecht AT, § 31.

[74] *Born*, Schadensersatz bei Datenschutzverstößen, S. 67; *Prinz/Peters*, Medienrecht, Rdnr. 716.

[75] In der Kommentarliteratur zum Datenschutzrecht findet sich zu Vermögensschäden meist nur die Aussage, dass sie zu ersetzen sind, nicht aber, worin sie bestehen können. Beispiele finden sich lediglich in *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 31 und in der Kommentarliteratur zum allgemeinen Persönlichkeitsrecht, hierzu vgl. insbesondere

Eine steigende Relevanz ergibt sich jedoch bezüglich der Schadensersatzpflicht bei der Verletzung vermögenswerter Interessen des allgemeinen Persönlichkeitsrechts. Da der elektronische Rechtsverkehr dem Unternehmer neue und vereinfachte Möglichkeiten einräumt, die Adressen seiner Kunden zu Werbezwecken entweder selbst einzusetzen oder an Adresshändler zu verkaufen, nimmt auch der Wert der Adressdaten des einzelnen Verbrauchers, vor allem wenn diese mit Informationen über sein Konsumverhalten gekoppelt sind, zu[76]. So geht aus der „Dialogmarketing Studie Deutschland 2009" der Deutschen Post AG[77] hervor, dass 19% des Werbemitteleinsatzes von insgesamt 12 Milliarden € im Jahre 2008 in die Finanzierung von adressierten Werbesendungen investiert wurde. Aus einem steigenden Wert der Adressdaten des Verbrauchers folgt indes die Notwendigkeit, im Falle einer Schädigung dieser dann vermögenswerten Interessen gegen das schädigende Unternehmen aufgrund schadensersatzrechtlicher Ansprüche vorgehen zu können. Die hier zugrunde liegende Frage nach der Ausgestaltung von Schadensersatzansprüchen bei der Verletzung vermögenswerter Bestandteile des Persönlichkeitsrechts war schon mehrfach Gegenstand der Rechtsprechung des BGH im Rahmen des § 823 BGB und wird daher an der entsprechenden Stelle[78] noch ausführlich zu erörtern sein.

*Rixecker* in: *Rebmann/Säcker/Rixecker*, MüKo, APKR, Rdnr. 218 ff., wo sich nicht nur Beispiele, sondern auch Ausführungen hinsichtlich des Umfangs des Ersatzes von Aufwendungen finden.

[76] In diesen Fällen gilt auch nicht das Listenprivileg des § 28 Abs. 3 Nr. 3 BDSG, welcher ausser der Zugehörigkeit zu einer Personengruppe ausschließlich die Übermittlung oder Nutzung der Berufs-, Branchen- oder Geschäftsbezeichnung, den Namen, den Titel, den akademischen Grad sowie Anschrift und Geburtsjahr vorsieht. Zur datenschutzrechtlichen Einordnung von Adresshändlern siehe im Übrigen *Weichert*, WRP 1996, 522–534; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 153 f.

[77] Abzurufen auf der Homepage der Deutschen Post Dialogmarketing unter `http://www.dialogmarketing-shop.de/`.

[78] Unter G.IV.3.c).

Eine Verletzung des Datenschutzrechts, die zu Personen- oder Sachschäden führt, mit der Folge der Anwendbarkeit des § 249 Abs. 2 BGB scheint hingegen kaum vorstellbar. Meist führt ein Verstoß lediglich zu immateriellen Schäden.

Diese werden nach wohl h.M. jedoch nicht von § 7 BDSG ersetzt[79]. Nach anderer Ansicht zwinge Art. 23 EG-Datenschutzrichtlinie, in dessen Lichte § 7 BDSG ausgelegt werden muss, auch zur Ersetzung immaterieller Schäden[80]. Für die herrschende Meinung spricht indes die klare Aussage des Gesetzgebers, die sich zum einen argumentum e contrario aus § 8 Abs. 2 BDSG ergibt: Während bei diesem in der Novellierung des BDSG 2001 die Ersatzfähigkeit von immateriellen Schäden, wie sie sich schon in § 7 Abs. 2 BDSG a.F. fand, bestehen blieb, hat der Gesetzgeber sie im neugeregelten § 7 BDSG bewusst ausgelassen. Dies ergibt sich auch aus § 253 Abs. 1 BGB, welcher den Ersatz immaterieller Schäden nur für die gesetzlich geregelten Fälle zulässt.

### 6. Konkurrenzen

Schon allein aus der Tatsache heraus, dass ein Anspruch auf Geldersatz aufgrund immaterieller Schäden durch § 7 BDSG nicht gewährt wird, stellt sich die Frage der Anwendbarkeit günstigerer schadensrechtlicher Vorschriften neben § 7 BDSG.

Dieser ist auch ohne besondere gesetzliche Bestimmungen gegeben. Eine besondere gesetzliche Regelung, die sich zum Verhältnis des § 7 BDSG zu anderen Normen äußert, existiert zwar nicht, der Gesetzgeber hätte eine solche aber auch nur dann treffen müssen, wenn er die Anwendbarkeit anderer Normen neben § 7 BDSG hätte ausschließen sollen[81]. Es bleibt daher beim haftungsrechtlichen Grundsatz, dass der Geschädigte bei Vorhandensein von mehr als einer Haftungsnorm wählen kann, aus welcher er vorgeht (Grundsatz der Unabhän-

[79] So *Gola/Schomerus*, BDSG, § 7 BDSG, Rdnr. 12; *Schneider, Jochen*, Handbuch des EDV-Rechts, Rdnr. 367; *Schaffland/Wiltfang*, BDSG, § 7 Rdnr. 9.
[80] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 7 BDSG, Rdnr. 12.
[81] *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 53.

gigkeit)[82]. Dem Betroffenen bleibt also der Weg, vertragliche oder deliktische Ansprüche gegen die verantwortliche Stelle geltend zu machen, die nicht den Einschränkungen des § 7 BDSG unterliegen (keine Haftung für immaterielle Schäden, Exkulpationsmöglichkeit) offen.

Anders verhält es sich jedoch beim Anspruch auf Löschung bzw. Sperrung gemäß § 35 BDSG. Hier stellt das BDSG eine abschließende Spezialregelung dar, die für eine Anwendung allgemeiner Rechtsgrundsätze keinen Raum lässt[83]. Anwendbar bleibt dennoch der Löschungsanspruch gem. § 824 BGB, da dieser eine besondere Ausprägung des Persönlichkeitsrechts, die Kreditgefährdung regelt[84]. Desweiteren kann ein vorbeugender Unterlassungsanspruch aus § 1004 BGB analog gegen künftige rechtswidrige Datenspeicherungen bestehen, da vorbeugende Ansprüche auf ein künftiges Verhalten vom Regelungsgehalt des § 35 BDSG nicht umfasst werden, Verletzungen des allgemeinen Persönlichkeitsrechts aber grundsätzlich auch negatorischen Schutz nach den allgemeinen Vorschriften geniessen[85].

Mangels spezieller Regelungen sind die §§ 7, 35 BDSG auch im Bereich der Tele- und Mediendienste anzuwenden[86].

## IV. Rechte des Betroffenen aus zivilrechtlichen Normen

Wie besonders beim Schadensersatz ersichtlich wird, bietet das BDSG allein noch keinen ausreichenden Schutz des Betroffenen bei Verstößen gegen sein Recht auf informationelle Selbstbestimmung. So stellt § 7 BDSG lediglich einen Mindestanspruch dar, welcher ausschließlich den Ersatz von Vermögensschä-

[82] BGH NJW 1998, 1008; *Teichmann* in: *Jauernig*, BGB, Vorbem. Rdnr. 3; *Sprau* in: *Palandt*, BGB, Einf v § 823, Rdnr. 4; *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 53.
[83] BGH NJW 1986, 2505; *Dix* in: *BDSG*, Simitis, § 35, Rdnr. 69; *Gola/Schomerus*, BDSG, § 35, Rdnr. 25.
[84] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 35 BDSG, Rdnr. 81.
[85] BGH NJW 1986, 436; *Gola/Schomerus*, BDSG, § 35, Rdnr. 26.
[86] *Engel-Flechsig* in: *Engel-Flechsig/Maennel/Tettenborn*, Beck'scher IuKDG-Kommentar, § 7 TDDSG, Rdnr. 1 ff.

den regelt[87]. Es stellt sich also die Frage, inwiefern der Betroffene Möglichkeiten hat, unter der Berücksichtigung allgemeiner zivilrechtlicher Ansprüche umfassenderen Schutz zu geniessen. Zu beleuchten ist diese vor allem auch vor dem Hintergrund, dass die Vielzahl der durch das BDSG und der bereichsspezifischen Regelungen vorgegebenen Informationspflichten nur einen geringen Nutzen haben, wenn bei einem Verstoß gegen dieselbigen der Betroffene schutzlos gestellt bleibt. Umgekehrt wird auf Seiten der verantwortlichen Stellen nur dann ein ausreichender Anreiz zur Einhaltung der Informationspflichten geschaffen, wenn sie bei einem Verstoß befürchten müssen, zivilrechtlich belangt zu werden.

### 1. Vertragliche Ansprüche

Aufgrund der neuen Möglichkeiten, die das digitale Zeitalter bei der automatisierten Verarbeitung von personenbezogenen Daten geschaffen hat, spielen diese gerade im Verhältnis zwischen Unternehmen und deren Kunden eine immer bedeutendere Rolle. Mit dem Zweck schon im Vorfeld die Bonität des Kunden festzustellen, bestimmte Vertragsrisiken ausschließen zu können oder auch nur die gezieltere Bewerbung einzelner Kundenstämme zu erreichen, hat dabei vor allem der wirtschaftliche Aspekt personenbezogener Daten deutlich zugenommen[88]. Auf der anderen Seite ist es, wie bereits aus den vorangegangenen Ausführungen hinsichtlich der technischen Methoden der Datenerhebung ersichtlich wird, für den Kunden nahezu unmöglich, den Überblick zu bewahren, welche Daten zu welchen Zwecken ein Unternehmen über ihn gespeichert hat. Es soll daher zunächst untersucht werden, ob dem Kunden als (potenziellen) Vertragspartner des datenverarbeitenden Unternehmens nicht bereits aufgrund

[87] Zu dieser Problematik siehe bereits unter Abschnitt G.III.5. auf Seite 176 und unter Abschnitt G.III.6. auf Seite 181; *Simitis* in: *BDSG*, Simitis, § 7 BDSG.

[88] *Weichert*, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, 1463–1469.

seiner vertraglichen Ansprüche ein ausreichender Schutz bei Verstößen gegen das Datenschutzrecht gewährt wird.

### a) Vorvertragliches Verschulden

Obwohl das vorvertragliche Schuldverhältnis bereits vor Abschluss des Vertrages entsteht, muss es an dieser Stelle Erwähnung finden. Dies ergibt sich zum einen aus der systematischen Stellung im Gesetz, in dem sich der § 311 BGB im Abschnitt 3 befindet, welcher die Schuldverhältnisse aus Verträgen regelt. Zum anderen erschließt es sich aus dem Sinn der *culpa in contrahendo*, welche verhindern will, dass eine Haftung bei einer Schutzpflichtverletzung sachwidrig vom späteren Vertragsschluss abhängig gemacht wird, wenn der Geschädigte bereits vor dem Vertragsabschluss seine Rechtsgüter Gefahren aussetzt, die aus der Sphäre der anderen Partei entstammen[89].

Nach dem seit der Schuldrechtsreform 2002[90] nunmehr im § 311 Abs. 2 BGB gesetzlich geregelten Institut der *culpa in contrahendo* besteht ein Schuldverhältnis bereits dann, wenn es zur Aufnahme von Vertragsverhandlungen kommt (Nr. 1), eine Vertragsanbahnung vorliegt (Nr. 2) oder ähnliche geschäftliche Kontakte bestehen (Nr. 3). Aus diesem Schuldverhältnis kann die Pflicht resultieren, auf die Rechte, Rechtsgüter und Interessen des jeweils anderen Teils Rücksicht zu nehmen (§ 241 Abs. 2 BGB). § 241 Abs. 2 BGB, der ebenfalls mit der Schuldrechtsreform Einzug in das Bürgerliche Gesetzbuch fand, normiert die Schutzpflichten: Während die Leistungspflichten darauf abzielen, am *status quo* einer Rechtsposition etwas zu verändern, zielen die Schutzpflichten darauf ab, diesen zu bewahren[91].

[89] *Brox/Walker*, Schuldrecht AT, § 5, Rdnr. 2; *Emmerich* in: *Rebmann/Säcker/Rixecker*, MüKo, § 311 BGB, Rdnr. 51; *Medicus*, Bürgerliches Recht, Rdnr. 199

[90] BGBl. I 2001, S. 3138 ff., Gesetz zur Modernisierung des Schuldrechts.

[91] Vergleiche auch die Definition des Gesetzgebers in der Begründung des Regierungsentwurf zur Schuldrechtsreform, BT-Drs. 14/6040, S. 125; *Roth* in: *Rebmann/Säcker/Rixecker*, MüKo, § 241BGB, Rdnr. 39; *Ackermann/Ivanov*, Zwischen „OPT-IN“, „OPT-OUT“ und „NO-OPT“, § 241BGB, Rdnr. 9.

Nicht beabsichtigt hat der Gesetzgeber mit der Aufnahme der *culpa in contrahendo* in das Bürgerliche Gesetzbuch hingegen eine Änderung ihrer bisherigen Fallgruppen. Er wollte lediglich eines der zentralen Rechtsinstitute kodifizieren[92]. Die Anwendbarkeit der c.i.c. beschränkt sich daher auf die bisher in der Rechtsprechung anerkannten Fallgruppen, also der Verletzung von Schutzpflichten hinsichtlich des Integritätsinteresses (Verletzung allg. Schutzpflichten), Verletzung vertragsbezogener Loyalitätspflichten und die Fälle der Haftung Dritter, die nunmehr in § 311 Abs. 3 BGB geregelt sind[93].

Für die hier zu untersuchenden Fälle des Verstoßes gegen die datenschutzrechtlichen Informationspflichten ist unter diesen Fallgruppen zunächst die der Verletzung des Integritätsinteresses von Bedeutung. Schon vom Reichsgericht wurde durch die berühmte Linoleumrollen-Entscheidung[94], später auch vom BGH unter anderem durch die Entscheidungen „Bananenschale“[95] und „Gemüseblatt“[96] anerkannt, dass die körperliche Integrität eines (potenziellen) Vertragspartners in den Schutz der c.i.c. fällt.

Der Schutz der c.i.c. kann sich aber keinesfalls nur auf die körperliche Integrität beschränken, sondern muss sich vielmehr auch auf die personenrechtliche Integrität erstrecken: Die Verletzung des Integritätsinteresses wurde mithin aus dem Grund in die c.i.c. mit einbezogen, um den Schwächen des Deliktsrechts, wie z.B. die Exkulpationsmöglichkeit nach § 831 Abs. 1 S. 2 BGB statt der Haftung des Erfüllungsgehilfen nach § 278 BGB entgegenzuwirken und diese durch eine vorvertragliche, schuldrechtliche Haftung zu überwinden[97]. Diese

[92] BT-Drs. 14/6040, 162f.; *Keilmann*, Vorsicht! - Zum Gehalt des §311 II, III BGB, 500–504; *Emmerich* in: *Rebmann/Säcker/Rixecker*, MüKo, § 311 BGB, Rdnr. 52.

[93] Zu den verschiedenen Fallgruppen siehe: *Keilmann*, Vorsicht! - Zum Gehalt des §311 II, III BGB, 500–504, *Gastroph*, Dogmatik und Entwicklung der culpa in contrahendo, 803–809; *Medicus*, Schuldrecht AT, Rdnr. 103 ff.

[94] RGZ 78, 239.

[95] BGH NJW 1962, 31.

[96] BGH NJW 1976, 712.

[97] *Emmerich* in: *Rebmann/Säcker/Rixecker*, MüKo, § 311 BGB, Rdnr. 51; *Medicus*, Schuldrecht AT, Rdnr. 104; *Gastroph*, Dogmatik und Entwicklung der culpa in contrahendo, 803–809.

Schwächen wirken sich jedoch nicht nur bei Verletzungen des Körpers, sondern ebenso bei Verletzungen der anderen in § 823 Abs. 1 BGB aufgeführten Rechtsgüter sowie der sonstigen Rechte aus. Unter die sonstigen Rechte des § 823 Abs. 1 BGB fällt u.a. das allgemeine Persönlichkeitsrecht und als eine seiner besonderen Ausprägungen das Recht auf informationelle Selbstbestimmung[98]. Für eine Anwendbarkeit der c.i.c. auch auf andere Rechtsgüter als Leben, Körper und Gesundheit spricht auch der durch die Schuldrechtsreform neugefasste § 241 Abs. 2 BGB, dessen Rücksichtsnahmepflicht nicht auf bestimmte Rechtsgüter beschränkt ist, so dass generell auf sämtliche „Rechte, Rechtsgüter und Interessen“ Rücksicht genommen werden muss[99].

Es kann im Ergebnis daher keinen Unterschied machen, ob ein potenzieller Käufer in einem Ladengeschäft im Vertrauen darauf, der Fussboden sei durch den Verkäufer sauber gehalten, auf einem Gemüseblatt ausgleitet und sich dabei ein Bein verletzt oder er in einem Online-Shop im Vertrauen darauf, der Zweck der Verarbeitung seiner Daten diene lediglich der ordnungsgemäßen Abwicklung seines Vertrages, diese in seinem Kundenprofil preisgibt und durch eine zweckfremde Weiterverarbeitung in seiner Persönlichkeit verletzt wird.

Festzuhalten bleibt jedoch, dass ein Verstoß gegen die datenschutzrechtlichen Informationspflichten im soeben genannten Fall nicht allein ursächlich für die Verletzung des allgemeinen Persönlichkeitsrechtes ist. Die Verletzungshandlung liegt vielmehr in der Verarbeitung der vom potenziellen Vertragspartner erlangten Daten. Entscheidend für das Vorliegen einer Haftung aus c.i.c. aufgrund eines Verstoßes gegen die Informationspflicht ist daher nicht nur, ob diese für die Preisgabe der Daten durch die (potenziellen) Vertragspartei kausal war, sondern auch, ob die Preisgabe für die Verwertungshandlung kausal

[98] BGHZ 50, 133; zur Entwicklung des Anspruchs auf Schadensersatz bei Verstößen gegen das allgemeine Persönlichkeitsrecht siehe unter Abschnitt G.IV.3. auf Seite 203.

[99] So auch *Canaris*, Die Reform des Leistungsstörungsrechts, 499–524, nach dem § 241 Abs. 2 BGB sogar eindeutig klarstellen will, dass nicht etwa nur Rechte und Rechtsgüter im Sinne von § 821 Abs. 1 BGB und auch nicht nur Vermögensinteressen, sondern eben Interessen aller Art gemeint sind.

war, die zur Verletzung des allgemeinen Persönlichkeitsrecht geführt hat. Die Preisgabe der Daten muss wiederum im Rahmen eines vorvertraglichen Vertrauensverhältnisses erfolgt sein. Das wäre beispielsweise dann der Fall, wenn der Kunde die Daten für eine Bestellung eines Buches in sein Profil eingibt und im Anschluss erst festzustellen ist, dass das gewünschte Buch vergriffen ist. Es genügt dann bereits, dass der Kunde sich mit seinen Daten registriert und daraufhin nur das Warenangebot betrachtet hat. Denn für eine Haftung nach § 311 Abs. 2 BGB ist bereits ausreichend, dass irgendein Zusammenhang mit einem eventuellen Vertragsschluss besteht[100].

Rechtsfolge der c.i.c. ist ein Schadensersatzanspruch nach § 280 Abs. 1 BGB, dessen Art und Umfang sich aus den §§ 249 ff. BGB ergibt. Im Unterschied zu § 7 S. 2 BDSG ist bei der Haftung nach den Regeln der c.i.c. eine Exkulpationsmöglichkeit nur im eingeschränkten Rahmen des § 280 Abs. 1 S. 2 BGB möglich, wenn der Schuldner beweisen kann, dass er die Pflichtverletzung nicht zu vertreten hat (§ 278 BGB). Eine Exkulpationsmöglichkeit, wie sie in § 831 Abs. 1 S. 2 BGB vorgesehen ist, bleibt ihm verwehrt. Setzt der Schuldner einen Erfüllungsgehilfen ein, so bestimmt sich die Haftung für sein Verschulden nach § 278 BGB.

Wie bereits beim Schadensersatz nach § 7 BDSG sind daher dem Gläubiger zunächst eventuell erlittene Vermögensschäden im Wege des § 249 Abs. 1 BGB zu ersetzen. Über den bloßen Ersatz von Vermögensschäden ist bei der Verletzung vorvertraglicher Pflichten darüber hinaus aber auch der Vertrauensschaden zu ersetzen[101]. Der Gläubiger ist also so zu stellen, wie er stehen würde, wenn das schädigende Ereignis nicht eingetreten wäre[102].

In diesem Zusammenhang stellt sich die Frage, wie beispielsweise zu verfahren ist, wenn der Geschädigte bei einer Verletzung seines Rechts auf in-

[100] *Canaris*, Die Reform des Leistungsstörungsrechts, 499–524.
[101] BGH NJW 2001, 2875; *Emmerich* in: *Rebmann/Säcker/Rixecker*, MüKo, § 311 BGB, Rdnr. 234; *Heinrichs* in: *Palandt*, BGB, § 311 BGB, Rdnr. 55.
[102] *Oetker* in: *Rebmann/Säcker/Rixecker*, MüKo, § 249 BGB, Rdnr. 122; *Heinrichs* in: *Palandt*, BGB, Vorb v § 249, Rdnr. 17.

formationelle Selbstbestimmung beweisen kann, dass er den Kaufvertrag dann nicht abgeschlossen hätte, wenn der Verkäufer ihn unter Einhaltung der datenschutzrechtlichen Informationspflichten über diejenigen Zwecke ausreichend in Kenntnis gesetzt hätte, die über § 28 Abs. 1 S. 1 Nr. 1 BDSG hinausgehen. Denkbar wäre hier, das Zustandekommen des Vertrags als schädigendes Ereignis einzuordnen, mit der Folge, dass dieser im Wege der Naturalrestitution rückgängig zu machen wäre. Eine schadensersatzrechtliche Rückabwicklung des Vertrages, ist für die Fälle in denen der Geschädigte ohne die Informationspflichtverletzung jedenfalls zu den vereinbarten Konditionen nicht geschlossen hätte, sowohl von der Rechtsprechung[103] als auch von der herrschenden Literatur (wenn auch unter verschiedenen Herleitungen)[104] anerkannt.

Es wird jedoch vorausgesetzt, dass es sich bei der verletzten Informationspflicht um eine *vertragsbezogene* handelt. Dies ist nur dann der Fall, wenn die Pflicht dazu dient, die informationelle Entscheidungsgrundlage des Gläubigers für den Vertragsschluss zu verbessern[105]. Zu unterscheiden ist hier zwischen reinen Schutzpflichten auf Information, welche ausschließlich dem Erhaltungsinteresse dienen und denjenigen Informationspflichten, die (nicht notwendigerweise ausschließlich wohl aber auch) dem Leistungsinteresse dienen[106]. So kommt es zwar bei einem Verstoß im Rahmen von Vertragsverhältnissen in beiden Fällen zu einer Haftung aus culpa in contrahendo, aber nur die letzteren sind als vertragliche (Neben-)Leistungen zu qualifizieren mit der Folge, dass der zustanden gekommene Vertrag als Schaden überhaupt in Betracht kommt.

[103] BGH NJW 1964, 1196; BGH NJW 1981, 1035; BGH NJW 1998, 302.

[104] Zur Rückabwicklung siehe ausführlich: *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, S. 69ff.; 387ff.; *Mertens*, Die Rechtsfolgen einer Haftung aus culpa in contrahendo beim zustande gekommenen Vertrag nach neuem Recht, 67–73; *Rieble*, Die Kodifikation der culpa in contrahendo, 137–157; *Grigoleit*, Vorvertragliche Informationshaftung, S. 137ff.; *Stoll*, Schädigung durch Vertragsschluss, 361–373; a.A. jedoch *Lieb*, Vertragsaufhebung oder Geldersatz? Überlegungen über die Rechtsfolgen von culpa in contrahendo, 251 ff.

[105] *Rehm*, Aufklärungspflichten im Vertragsrecht, S. 3.

[106] *von Mohrenfels*, Abgeleitete Informationsleistungspflichten im deutschen Zivilrecht, S. 23.

Bei den datenschutzrechtlichen Informationspflichten handelt es sich um solche, die ausschließlich das Rechtsgut der informationellen Selbstbestimmung und somit das Integritätsinteresse schützen wollen. Eine Verletzung des Integritätsinteresses im Rahmen vorvertraglicher Verhandlungen berührt den Vertragsinhalt sowie die mit ihm verbundenen berechtigten Erwartungen nicht. Die im Rahmen des Vertragsverhältnisses erhobenen personenbezogenen Daten finden zwar in aller Regel ihren Zweck zunächst allein in der ordnungsgemäßen Vertragsabwicklung. Soweit diese berührt ist, ist die Datenerhebung jedoch auch rechtmäßig und liegt eine schädigende Handlung gerade nicht vor. Der Schaden tritt vielmehr außerhalb des Vertrages, namentlich in der zweckfremden und unzulässigen Weiterverarbeitung ein. Es ist daher zwar gerechtfertigt, die durch die Verletzung entstandenen Schäden des Integritätsinteresses nach den Regeln der culpa in contrahendo zu ersetzen, nicht aber kann allein die Verletzung datenschutzrechtlicher Informationspflichten auch zu einer Rückabwicklung des Vertrages führen.

Eine weitere Frage, die sich beim Verstoß gegen datenschutzrechtliche Informationspflichten in Verbindung mit den Rechtsfolgen der culpa in contrahendo aufdrängt, ist, ob neben den Vermögensschäden auch eventuell entstandene Nichtvermögensschäden zu ersetzen sind. Dafür spricht erneut, dass die c.i.c den Schwächen des Deliktsrechts entgegenwirken soll. Nur wenn ein Schadensersatz im selben Umfang wie bei den deliktischen Ansprüchen gewährt wird, kann dieser Zweck erfüllt werden. Im Deliktsrecht ist ein Geldersatz auch immaterieller Schäden bei Verstößen gegen das allgemeine Persönlichkeitsrecht vom BGH und dem Bundesverfassungsgericht anerkannt[107].

Gegen einen Anspruch auf Geldersatz auch im Rahmen eines (vor-) vertraglichen Verhältnisses spricht jedoch § 253 BGB. Dieser sieht in seinem ersten Absatz einen Ersatz von Schäden, die nicht Vermögensschäden sind, nur in

[107] Zur Entwicklung der Rechtsprechung zum Anspruch auf Geldersatz bei Verletzung des allgemeinen Persönlichkeitsrecht siehe noch ausführlich unter Abschnitt G.IV.3. auf Seite 203.

den durch das Gesetz bestimmten Fällen vor. Die Vorschrift unterliegt dabei einem absolutem Analogieverbot[108]. Dennoch drängt sich die Frage auf, ob der Anspruch auf Geldersatz nicht auch hier, wie im Deliktsrecht, direkt aus dem Wertesystem des Art. 1 und Art. 2 Abs. 1 GG herzuleiten ist. Inwiefern auch ausserhalb des Regelungsbereichs des § 253 BGB Raum für den Ersatz immaterieller Schäden bei der c.i.c. bleibt, wurde in der Literatur bisher so gut wie nicht diskutiert. Einzig in einem Aufsatz von *Diedrich*[109], der sich noch auf die Rechtslage vor dem zweiten Schadensersatzänderungsgesetz bezieht, äußert dieser Kritik dahingehend, dass § 253 BGB einen Wertungswiderspruch innerhalb des BGB zwischen Deliktsrecht und Vertragsrecht darstellt, der letztlich den Schädiger begünstigt. So berechtigt diese Kritik auch bei der heutigen Fassung des § 253 BGB erscheint, so wenig darf jedoch übersehen werden, dass eben dieser Widerspruch durch das zweite Schadensersatzänderungsgesetz und mithin der Ersatz des § 847 BGB a.F. durch § 253 Abs. 2 BGB aufgehoben werden sollte. Abweichend von der vor dem zweiten Schadensersatzänderungsgesetz geltenden Rechtslage wird eine Entschädigung nunmehr stets dann zugebilligt, wenn eines der in Absatz zwei genannten Rechtsgüter verletzt wurde. Ob die zum Schadensersatz verpflichtende Anspruchsgrundlage delikts- oder vertragsrechtlicher Natur ist, ist dabei unerheblich[110].

Hinsichtlich des Geldersatzes von Nichtvermögensschäden hat der Gesetzgeber eine dahingehende Aufhebung des Widerspruchs hingegen bewusst unterlassen. In der Gesetzesbegründung der Bundesregierung zum zweiten Schadensersatzänderungsgesetz wird klargestellt, dass eine Aufnahme des allgemeinen Persönlichkeitsrechts in den neuen § 253 Abs. 2 BGB (ehemals § 847 BGB)

[108] *Schiemann* in: *Staudinger*, Kommentar zum BGB, § 253 BGB, Rdnr. 1; *Oetker* in: *Rebmann/Säcker/Rixecker*, MüKo, § 253, Rdnr. 27.

[109] *Diedrich*, MDR 1994, 525– 529; interessanterweise wird hier auch auf den Geldersatz bei Verletzung des allgemeinen Persönlichkeitsrechts, damals noch gestützt auf § 847 alg., als einzige Ausnahme von § 253 hingewiesen. Der Gedanke, inwiefern diese Ausnahme auch Auswirkungen auf Ansprüche bei der cic hat, wird allerdings nicht weitergeführt.

[110] *Oetker* in: *Rebmann/Säcker/Rixecker*, MüKo, § 253 BGB, Rdnr. 2, *Schiemann* in: *Staudinger*, Kommentar zum BGB, § 253 BGB, Rdnr. 3.

nicht geboten sei, da es sich beim Anspruch auf Geldentschädigung wegen Verletzung des allgemeinen Persönlichkeitsrechts um ein eigenes Recht handle, welches sich direkt aus dem Schutzauftrag aus den Art. 1 und 2 Abs. 1 GG ergäbe und sich vom Schmerzensgeld unterscheide[111].

Obwohl durch die Entscheidung des Gesetzgebers, keine in der Zivilrechtsordnung verankerte Regelung des Geldersatzes als Folge einer Persönlichkeitsrechtsverletzung im Rahmen des zweiten Schadensersatzänderungsgesetz einzuführen, sondern es bei der Herleitung direkt aus der Grundrechtsordnung zu belassen, weiterhin methodische Bedenken hervorruft[112], lässt sie keinen Raum für eine dahingehende analoge Anwendung des § 253 Abs. 2 BGB. Ein Geldersatz für Nichtvermögensschäden bei Verletzungen des Persönlichkeitsrecht aus vertraglichen Anspruchsgrundlagen ist daher ausgeschlossen.

### b) Anfechtung

Das Recht zur Anfechtung einer Willenserklärung durch den Betroffenen spielt im Zusammenhang mit der datenschutzrechtlichen Einwilligung eine Rolle. Unabhängig von der bereits erwähnten[113] Diskussion hinsichtlich der Frage, ob es sich bei der datenschutzrechtlichen Einwilligung um eine Willenserklärung oder eine geschäftsähnliche Handlung handelt, besteht Einigkeit darüber, dass eine infolge von Irrtum oder Täuschung abgegebene Einwilligung anfechtbar ist[114].

[111] BT-Drs. 14/7752, S. 24 f.; zum zweiten Schadensersatzrechtsänderungsgesetz siehe ausführlich: *Wagner*, Das Zweite Schadensersatzrechtsänderungsgesetz, 2049–2064; kritisch zur fehlenden gesetzlichen Regelung des Geldersatzes durch das zweite Schadensersatzrechtsänderungsgesetz äußert sich *Schiemann* in: *Staudinger*, Kommentar zum BGB, § 253, Rdnr. 57ff.

[112] Siehe dazu ausführlich *Schiemann* in: *Staudinger*, Kommentar zum BGB, § 253, Rdnr. 52ff. m.w.N.

[113] Abschnitt F.II.1. auf Seite 137.

[114] *Simitis* in: *BDSG*, Simitis, § 4a, Rdnr. 25; *Holznagel/Sonntag* in: *Roßnagel*, Handbuch Datenschutzrecht, 4.8, Rdnr. 23; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, Rdnr. 324.

Zu beachten sind jedoch auch hier die bereits hinsichtlich der vorvertraglichen Pflichtverletzung getroffenen Erwägungen: Führt eine unzureichende Information gem. § 4a Abs. 1 S. 2 BDSG (und im Internetdatenschutzrecht darüber hinaus gem. § 13 Abs. 3 S. 1 TMG) des Betroffenen zu einer Täuschung oder einem Irrtum beim Betroffenen, welche ihn zur Anfechtung der Einwilligung berechtigt, so führt dies einzig und allein zu einer rückwirkenden Aufhebung der Einwilligung[115] (§ 142 Abs. 1 BGB). Nicht betroffen sind hiervon hingegen die vertraglichen Willenserklärungen, mit der Folge, dass der Vertrag als solcher wirksam abgeschlossen ist. Soweit die Datenerhebung und -verarbeitung der Zweckbestimmung des Vertragsverhältnisses dient, ist ohnehin § 28 Abs. 1 S. 1 Nr. 1 BDSG zu beachten, mit der Folge, dass diese auch ohne Einwilligung rechtmäßig ist.

Aus den durch die Anfechtung ex tunc nichtig gewordene Einwilligungserklärung resultiert, dass all diejenigen Verarbeitungen, die eine Einwilligung voraussetzen, von Anfang an unzulässig gewesen sind. Der Betroffenen hat insoweit einen Anspruch auf Löschung dieser Daten[116].

### c) Nichtigkeit gemäß §§ 134, 138 BGB

Wie bereits die Regeln über die Anfechtbarkeit, ist auch die Nichtigkeit wegen Gesetzesverstoßes (§ 134 BGB) und über die Folgen eines sittenwidrigen Rechtsgeschäftes auch auf die datenschutzrechtliche Einwilligung anwendbar.

Grundsätzlich hat sich der Gesetzgeber jedoch durch die Schaffung der datenschutzrechtlichen Einwilligung für den Vorrang der Privatautonomie im Datenschutzrecht entschieden, so dass § 134 BGB bei einer gegen die Vorgaben des BDSG verstoßenden Erhebung oder Verarbeitung nicht anwendbar ist[117] .

[115] *Simitis* in: *BDSG*, Simitis, § 4a, Rdnr. 25; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, Rdnr. 324.
[116] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, Rdnr. 324.
[117] BGH BB 2007, 793 m.w.N.

Seine Grenzen findet die Privatautonomie allerdings dann, wenn die datenschutzrechtliche Einwilligung zu einer sittenwidrigen rechtswidrigen Selbstbeschränkung oder zu einer menschenunwürdigen Erniedrigung führen würde[118]. Auch hier knüpft sich die Anwendbarkeit des § 138 BGB allerdings nicht an die Verletzung von datenschutzrechtlichen Informationspflichten, sondern an die Einwilligung als solche.

### d) Erweitertes Widerrufsrecht im Rahmen der §§ 312 ff. BGB

Die besonderen Vertriebsformen der §§ 312-312f BGB wurden in das BGB durch die Schuldrechtsreform 2002 eingefügt. Dabei wurden teils bereits bestehende Vorschriften in das BGB übernommen, im Hinblick auf den für den Internetversandhandel relevanten § 312e BGB wurde das BGB aber auch um eine neue Vorschrift ergänzt. § 312 BGB und der damit zusammenhängende § 3 BGB-InfoV setzen Art. 10 und 11 der sog. E-Commerce-Richtlinie um[119].

Die zentrale Frage, die sich durch den Zusammenhang der besonderen Vertriebsformen und der datenschutzrechtlichen Informationspflichten ergibt, ist, ob ein Verstoß gegen datenschutzrechtliche Informationspflichten für den Verbraucher zu einem erweiterten Widerrufsrecht gemäß § 355 Abs. 1 BGB führt.

#### aa) Fernabsatzverträge

Bei der Bestellung von Waren über das Internet durch einen Verbraucher, handelt es sich um einen in den §§ 312b ff. BGB geregelten Fernabsatzvertrag. Der Gesetzgeber nennt in § 312b Abs. 2 BGB bei der beispielshaften Aufzählung von Fernkommunikationsmitteln ausdrücklich Tele- und Mediendienste.

[118] *Weichert* in: *Kilian/Heussen*, Computerrechts-Handbuch, 132, Rdnr. 46.
[119] Richtlinie 2001/31/EG, ABl. 2000, L 178, S. 1 ff.; *Staudinger*, Kommentar zum BGB, § 312e, Rdnr. 3; *Grigoleit*, NJW 2002, 1151–1152.

Hier ist eventuell im Hinblick auf das TMG eine Anpassung des Gesetzeswortlautes zu erwarten, wonach es sich um Telemedien handelt[120].

Zu den Unterrichtungspflichten des Unternehmers bei Fernabsatzverträgen[121] gehört nach § 312c Abs. 1 S. 2 BGB unter anderem auch die Mitteilung der Vertragsbestimmungen einschließlich der Allgemeinen Geschäftsbedingungen. Unter Vertragsbestimmungen sind dabei nicht sämtliche Informationen, die den Vertrag bestimmen, zu verstehen, sondern nur der eigentliche Vertragstext[122].

Hier gilt es sauber zu unterscheiden: Vertragsbestimmungen sind, unabhängig davon, ob als Bestandteil von Allgemeinen Geschäftsbedingungen oder einer isolierten Datenschutzerklärung, in der Regel diejenigen Informationspflichten, die einen vertraglichen Bezug aufweisen. Es handelt sich hierbei üblicherweise um die Informationspflichten nach §§ 4 Abs. 3 S. 1, 4a Abs. 1 S. 2 BDSG sowie §§ 13 Abs. 1 S. 1 und 2, Abs. 3 und Abs. 6 S. 2 TMG. Anders verhält es sich hingegen in den Fällen, in denen der Unternehmer über die Grenzen der Einwilligung des Verbrauchers und § 28 BGSG hinaus plant, die Daten zu anderen Zwecken weiterzuverarbeiten: Nur aus der Tatsache allein, dass im Falle einer erfolgten Information diese im Rahmen der Datenschutzerklärung auch Bestandteil des Vertrages geworden wäre, lässt sich noch nicht schließen, dass sich aus ihrem Fehlen ein Verstoß gegen § 312c Abs. 2 S. 1 BGB ergibt. Vertragsbestimmungen werden die datenschutzrechtlichen Informationspflichten also lediglich dann, wenn sie auch in den Vertragstext aufgenommen wurden.

Sind die datenschutzrechtlichen Informationspflichten jedoch Vertragsbestimmungen, so sind sie dem Verbraucher spätestens bis zur vollständigen

[120] Zu den geplanten Gesetzesänderungen im Fernabsatzrecht siehe den „Entwurf eines Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht“ (BT-Drs. 16/11643); *Bierekoven*, CR 2008, 785–791.

[121] Diese wurden zuletzt durch die Änderungen des Fernabsatzänderungsgesetzes (BGBl. I 2004, S. 3102 ff.) neugefasst; *Grüneberg* in: *Palandt*, BGB, § 312c, Rdnr. 1.

[122] *Staudinger*, Kommentar zum BGB, § 312c BGB, Rdnr. 75; BT-Drs. 15/2946, S. 21.

Erfüllung des Vertrages, bei Waren spätestens bis zur Lieferung mitzuteilen (§ 312c Abs. 2 S. 1 Nr. 2 BGB). Die Unterrichtung hat dabei gem. § 312c Abs. 2 BGB in Textform zu erfolgen (§ 126b BGB). Die Textform nach § 126b BGB ist nach einhelliger Meinung dann gewahrt, wenn die Mitteilung per E-Mail erfolgt[123]. Uneinigkeit besteht aber dahingehend, ob für einen Zugang der Informationspflichten auf einer Webseite die bloße Möglichkeit des Downloads schon ausreicht[124] oder ob es tatsächlich zum Download kommen muss[125]. Dafür, dass die Möglichkeit des Downloads allein genügt, spricht die Überlegung, dass eine Kontrolle des Unternehmers, ob der Verbraucher die Webseite tatsächlich heruntergeladen oder ausgedruckt hat, in der Praxis einen hohen Aufwand bedeutet, welcher dazu geeignet ist, den elektronischen Geschäftsverkehr in größerem Maße durch formale Informationsanforderungen zu belasten, als dies zum Schutz des Verbrauchers unbedingt notwendig ist[126]. Der Wortlaut des § 126b BGB setzt überdies nur die Eignung zur dauerhaften Wiedergabe voraus. Diese ist bei der erstmaligen Anzeige im Browser noch nicht gegeben. So vertritt zwar eine Ansicht, dass in dem Moment, in dem der Verbraucher eine Webseite auf seinem Client anzeigt, diese sich im Cache seines Computers befindet und damit dauerhaft wiedergegeben werden könne. Dass die Seite, wenn der Verbraucher sie nicht auf einem Datenträger abspeichert, nur vorübergehend im Cache zugänglich bleibt, sei dagegen keine Frage der Eignung zur dauerhaften Wiedergabe, sondern des dauerhaften Konservierens[127].

Eine solche rein technische Betrachtungsweise würde jedoch den Schutzzweck des § 126b BGB verkennen. Die Funktion der Textform besteht mithin im Gegensatz zur bloß mündlich zugegangenen Erklärung darin, durch ein Medium

[123] *Einsele* in: *Rebmann/Säcker/Rixecker*, MüKo, § 126b, Rdnr. 9; *Heinrichs* in: *Palandt*, BGB, § 126b, Rdnr. 3.
[124] *Einsele* in: *Rebmann/Säcker/Rixecker*, MüKo, § 126b, Rdnr. 9.
[125] *Heinrichs* in: *Palandt*, BGB, § 126b, Rdnr. 3; LG Kleve NJW-RR 2003, 196.
[126] In diese Richtung argumentiert OLG München, NJW 2001, 2265.
[127] *Janal*, Die Errichtung und der Zugang einer Erklärung in Textform gem. §126b BGB, 368–373.

zu informieren, durch das die Erklärung dauerhaft wiedergegeben werden kann. Sie soll dabei die Zwecke der Information und der Dokumentation erfüllen[128]. Diese Funktion droht unterlaufen zu werden, wenn der technisch wenig versierte Nutzer beim Anzeigen der Informationen diese nicht sofort ausdruckt, weil er darauf vertraut, sie seien zu einem späteren Zeitpunkt noch verfügbar. Eine eventuelle Speicherung auf dem Nutzeraccount des Servers des Unternehmers bleibt dabei flüchtig, weil dieser die Webpage jederzeit ändern kann[129].

Letztlich vermag auch das Argument der Praktikabilität nicht zu überzeugen, da der Unternehmer die Informationen zusätzlich bei der Lieferung der bestellten Ware in Papierform beilegen kann[130]. Findet eine solche nicht statt, bleibt im Ergebnis festzuhalten, dass der Unternehmer seinen Pflichten nicht nachkommt, wenn durch den Verbraucher weder eine Speicherung, noch ein Ausdruck der sich auf der Webseite befindenden Information erfolgt.

Kommt der Unternehmer seinen Pflichten nach § 312c Abs. 2 BGB nicht nach, beginnt die Widerrufsfrist des dem Verbraucher nach § 355 BGB zustehenden Widerrufsrechts erst dann zu laufen, wenn der Unternehmer die Erfüllung der Pflichten zu einem späteren Zeitpunkt wahrnimmt (§ 312d Abs. 2 BGB). Zu beachten sind hier jedoch die Ausschlusstatbestände des § 312d Abs. 4 BGB. Für das Internet relevant können insbesondere die Nr. 1 sein, also die Lieferung von Waren, die nach Kundenspezifikation angefertigt werden (z.B. ein nach den Wünschen des Verbrauchers im Internet selbst konfigurierter Aufdruck eines T-Shirts), nach Nr. 2 die Lieferung von Software, falls die gelieferten Datenträger vom Verbraucher entsiegelt worden sind und nach Nr. 3 die Lieferung von Zeitungen, Zeitschriften und Illustrierten (z.B. online abgeschlossenes Printabonnement, wobei gemäß § 312d Abs. 5 BGB trotzdem

[128] *Einsele* in: *Rebmann/Säcker/Rixecker*, MüKo, § 126b BGB, Rdnr. 1.
[129] *Hoeren*, Informationspflichten im Internet - im Lichte des neuen UWG, 2461–2470; *Horn*, Verbraucherschutz bei Internetgeschäften, 209–214; BT-Drs. 14/2658, 40.
[130] *Hoeren*, Informationspflichten im Internet - im Lichte des neuen UWG, 2461–2470.

§ 505 BGB anwendbar bleibt[131]). Anzumerken gilt es an dieser Stelle auch, dass § 312d Abs. 4 Nr. 5 BGB lediglich Versteigerungen im Sinne des § 156 BGB meint, eine Versteigerung über die Onlineplattform Ebay daher nicht vom Anwendungsbereich umfasst wird[132].

### bb) Pflichten im elektronischen Geschäftsverkehr

Bedient sich ein Unternehmer zum Zwecke des Abschlusses des Vertrages über die Lieferung von Waren oder über die Erbringung von Dienstleistungen eines Telemediums, so handelt es sich um einen Vertrag im elektronischen Rechtsverkehr und ist § 312e BGB anwendbar. Im Gegensatz zu den Vorschriften des § 312b ff. BGB ist § 312e BGB nicht nur auf Verträge zwischen Unternehmern und Verbrauchern anwendbar, sondern können beide Vertragsparteien auch Unternehmer sein. Grund dafür, dass die Schutzregelungen des § 312e BGB auch anwendbar sind, wenn sich beide Vertragsparteien auf Augenhöhe befinden, sind die technischen Unwägbarkeiten, die sich bei der Nutzung von Telemedien ergeben können. So soll in erster Linie verhindert werden, dass der Diensteanbieter die elektronischen Medien dazu nutzt, um den Nutzer über Einzelheiten des Vertrages im Unklaren zu lassen[133]. Handelt es sich aber um ein Rechtsgeschäft zwischen Unternehmern, können diese hinsichtlich des § 312e Abs. 1 S. 1 Nr. 1 bis 3 und S. 2 eine anderweitige Vereinbarung treffen (§ 312e Abs. 2 S. 2 BGB).

Zu den vom Unternehmer im elektronischen Geschäftsverkehr zählenden und im Zusammenhang mit datenschutzrechtlicher Information relevanten Pflichten zählen die des § 312e Abs. 1 Nr. 2 und 4 BGB. Nach § 312e Abs. 1 Nr. 2 BGB hat der Unternehmer dem Kunden die in § 3 der BGB-Informationspflichten-

[131] Dies wird sich mit der geplanten Gesetzesänderung zur Umsetzung der Verbraucherkreditrichtlinie jedoch ändern, BT-Drs. 16/11643, 69.
[132] BGH ZUM 2005, 66; *Grüneberg* in: *Palandt*, BGB, § 312d BGB, Rdnr. 13 m.w.N.
[133] *Thüsing* in: *Staudinger*, Kommentar zum BGB, § 312e BGB, Rdnr. 1; *Wendehorst* in: *Rebmann/Säcker/Rixecker*, MüKo, § 312e BGB, Rdnr. 1.

Verordnung (BGB-InfoV) festgehaltenen Pflichten mitzuteilen. Nach § 3 Nr. 5 BGB-InfoV beinhaltet dies die Information über sämtliche einschlägigen Verhaltenskodizes, denen sich der Unternehmer unterwirft, sowie die Möglichkeit eines dahingehenden elektronischen Zugangs.

Verhaltenskodizes sind bestimmte Verhaltensregelwerke, denen sich ein Unternehmer, zumeist zu Werbezwecken, unabhängig vom Vertragsschluss mit dem einzelnen Kunden freiwillig unterwirft, um damit im Wettbewerb eine besondere Unternehmens- und/oder Produktqualität dokumentieren zu können[134]. Im Datenschutzrecht findet sich die Regelung über Verhaltenskodizes in § 38a BDSG wieder, nach dem u.a. Berufsverbände Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten können. Als Beispiel eines für den Bereich des Internets relevanter Verhaltenskodex, der unter anderem dem Schutz personenbezogenen Daten dient, kann hier der „Ehrenkodex eMail-Marketing“ des Deutschen Direktmarketing Verbandes e.V. (DDV) dienen[135]. Obwohl an der Pflicht der Unterrichtung über Verhaltenskodizes teilweise kritisiert wird, dass der Verbraucher sich in der Praxis kaum mit den jeweiligen Verhaltenskodizes auseinander setzen wird und die Selbstverpflichtung des Unternehmers als solche keine Rechtswirkung in der Rechtsbeziehung zwischen Unternehmer und Kunden entfaltet, da diese bereits aus der Unterwerfung unter das entsprechende Regelwerk erfolge[136], so besteht ihr sinnvoller Zweck doch darin, die Durchsetzbarkeit der Regeln für das konkrete Vertragsverhältnis si-

[134] BT-Drs. 14/6040, 171.

[135] Im Internet zu finden unter: `http://www.ddv.de/downloads/Service/Ehrenkodex_eMail-Marketing.pdf`.

[136] So *Janal*, Sanktionen und Rechtsbehelfe bei der Verletzung verbraucherschützender Informations- und Dokumentationspflichten im elektronischen Geschäftsverkehr, S. 113, welche die Einführung der Informationspflicht daher u.a. kritisiert und daher die Meinung vertritt, sie sei bestenfalls überflüssig und sei im ungünstigsten Fall dazu geeignet, den Verbraucher durch eine vermeintliche Qualitätssicherung zum Vertragsabschluss zu verleiten.

cherzustellen[137]. Dies hat wiederum zur Folge, dass sich zwar der Unternehmer eventuell durchaus zu Werbezwecken und aus Wettbewerbsgründen den Kodizes unterwirft, ein praktischer Nutzen für die Kunden aber trotzdem erkennbar ist: Würde beispielsweise eine vermehrte Unterwerfung grosser Unternehmen unter die Kodizes des DDV tatsächlich in Zukunft dazu führen, dass der Kunde gezielt nur mit solchen Unternehmen in Rechtsbeziehungen tritt, wäre dies dazu geeignet, auf andere Unternehmen einen Druck auszuüben, welcher der Anhebung datenschutzrechtlicher Standards gerade im Bereich E-Commerce unzweifelhaft dienlich wäre.

Die Erfüllung der Informationspflicht erfolgt über die Möglichkeit eines elektronischen Zugangs zum Verhaltenskodex[138]. Hierbei bietet es sich an, dem Kunden im Rahmen der sonstigen Unterrichtung gem. § 312e Abs. 1 BGB mittels eines Hyperlinks direkt auf das Regelwerk zu verweisen. Hat sich der Unternehmer für einen bestimmten Bereich einem Verhaltenskodex nicht unterworfen, ist er nicht verpflichtet, den Kunden auch darüber zu informieren[139].

Nach § 312e Abs. 1 S.1 Nr. 4 BGB hat der Unternehmer die Möglichkeit zu verschaffen, die Vertragsbestimmungen einschließlich der Allgemeinen Geschäftsbedingungen bei Vertragsschluss abzurufen und in wiedergabefähiger Form zu speichern. Zu der Frage, inwiefern es sich bei den datenschutzrechtlichen Informationspflichten um Vertragsbestimmungen handelt, gelten die gleichen Ausführungen wie bei den Pflichten des Unternehmers bei Fernabsatzverträgen (Abschnitt G.IV.1.d)aa) auf Seite 193). Ein Unterschied besteht hier

[137] *Grigoleit*, NJW 2002, 1151–1152.

[138] Dass auch die Erfüllung der Pflichten nach § 312e Abs. 1 BGB auf elektronischem Wege erfüllt werden müssen und nicht etwa ein Faxabruf genügt, ergibt sich aus dem Kontext mit § 312e BGB, welcher die Pflichten im elektronischen Geschäftsverkehr regelt; *Thüsing* in: *Staudinger*, Kommentar zum BGB, § 312e, Rdnr. 58; *Wendehorst* in: *Rebmann/Säcker/Rixecker*, MüKo, § 312e, Rdnr. 105.

[139] *Aigner/Hofmann*, Fernabsatzrecht im Internet, S. 243; *Janal*, Sanktionen und Rechtsbehelfe bei der Verletzung verbraucherschützender Informations- und Dokumentationspflichten im elektronischen Geschäftsverkehr, S. 114; *Martinek* in: *Staudinger*, Kommentar zum BGB, Art. 242 EGBGB, Rdnr. 8.

jedoch in der Form und im Zeitpunkt der Mitteilung. Ferner kann die Pflicht nach § 312e Abs. 1 S. 1 Nr. 4 BGB auch nicht unter Unternehmern abbedungen werden. Im Gegensatz zur unter § 312c Abs. 2 BGB statuierten Textform hat die Mitteilung der Vertragsbestimmungen im elektronischen Geschäftsverkehr auf elektronischem Wege zu erfolgen. Hierzu eignet sich zum einen die Übermittlung per E-Mail, zum anderen kann diese aber auch auf einer Webseite erfolgen. Eine tatsächliche Speicherung durch den Kunden muss anders als bei § 312c Abs. 2 BGB nicht stattfinden, es muss ihm vielmehr nur die Möglichkeit eingeräumt werden. In diesem Zusammenhang hat der Unternehmer auch darüber zu informieren, wie und wann der Kunde die Vertragsbestimmungen abrufen und in wiedergabefähiger Form speichern kann. Diese Pflicht ergibt sich aus § 312e Abs. 1 Nr. 2 in Verbindung mit § 3 Nr. 2 BGB-InfoV[140] und ist daher unter Unternehmern abdingbar.

Die Mitteilung hat bei Vertragsschluss zu erfolgen. Darunter ist der Zeitrahmen unmittelbar nach dem Vertragsschluss gemeint, welcher mit Zugang der zweiten korrespondierenden Willenserklärung beginnt und nach vollständiger Leistungserbringung endet[141]. Ein früherer Zeitpunkt ist nicht anzunehmen, da der vollständige, dem Kunden mitzuteilende Inhalt des Vertrages erst durch den Vertragsschluss selbst festgelegt wird[142].

Nach § 312e Abs. 3 S. 2 BGB beginnt die Widerrufsfrist des Rechts, welches dem Kunden nach § 355 BGB zusteht, nicht vor Erfüllung der in § 312e Abs. 1 S. 1 BGB genannten Pflichten. So berechtigt die Sanktion bei der Pflicht nach § 312e Abs. 1 S. 1 Nr. 4 BGB erscheinen mag, auf umso größere Kritik stößt sie bei denjenigen Pflichten, die für die Ausübung des Widerrufsrechts nicht von Bedeutung sind. So erscheint es unbillig, dem Unternehmer eine Ausdehnung der Widerrufsfrist auf sechs Monate (§ 355 Abs. 3 S. 1 BGB) auch dann aufzu-

[140] *Thüsing* in: *Staudinger*, Kommentar zum BGB, § 312e, Rdnr. 58; *Wendehorst* in: *Rebmann/Säcker/Rixecker*, MüKo, § 312e, Rdnr. 80f.
[141] *Wendehorst* in: *Rebmann/Säcker/Rixecker*, MüKo, § 312e, Rdnr. 108.
[142] *Grigoleit*, NJW 2002, 1151–1152.

bürden, wenn er eine nur unerhebliche Pflichtverletzung begangen hat, die den Kunden in seiner Ausübung des Widerrufsrechts nicht gehindert hat[143]. Eine solche nur unerhebliche Pflichtverletzung liegt auch dann vor, wenn der Kunde nicht über die Bindung des Unternehmers an Verhaltenskodizes informiert wurde[144]. Da der Verhaltenskodex lediglich dazu dienen soll, den Kunden durch die in ihm enthaltenen Regelungen davon zu überzeugen, dass der Unternehmer bestimmten Qualitätsstandards genügt, haben sie für das Widerrufsrecht überhaupt keine Bedeutung. Ein Nachteil entsteht durch die Pflichtverletzung dem Kunden nur insofern, dass er einen eventuellen Verstoß des Unternehmers gegen den Verhaltenskodex nicht geltend machen kann. Da aus diesen Gründen Einigkeit darüber besteht, dass die Rechtsfolge des § 312e Abs. 3 S. 2 BGB nur dann eintritt, wenn sie im Verhältnis zur Pflichtverletzung steht, ergibt sich aus der fehlenden Information über die Unterwerfung unter Verhaltenskodizes kein verzögerter Beginn der Widerrufsfrist. Eine dahingehende Einschränkung wird in der Literatur entweder durch eine teleologische Reduktion[145] oder mittels verfassungskonformer Auslegung vorgenommen[146].

### cc) Verhältnis zwischen §§ 312b, c, d BGB und § 312e BGB sowie Zusammenfassung des erweiterten Widerrufsrechts

Da eine Verwendung von Telemedien zum Zwecke des Abschlusses eines Vertrages über die Lieferung von Waren oder über die Erbringung von Dienstleistungen eines Tele- oder Mediendienstes in der Regel auch zur ausschließlichen Verwendung von Fernkommunikationsmitteln führt, sind in den Fällen, in denen der Kunde ein Verbraucher ist, sowohl die Pflichten gem. § 312c Abs. 1, 2

[143] *Wendehorst* in: *Rebmann/Säcker/Rixecker*, MüKo, § 312e, Rdnr. 112.
[144] *Janal*, Sanktionen und Rechtsbehelfe bei der Verletzung verbraucherschützender Informations- und Dokumentationspflichten im elektronischen Geschäftsverkehr, S. 114; *Grüneberg* in: *Palandt*, BGB, § 312e, Rdnr. 11.
[145] So *Grigoleit*, NJW 2002, 1151–1152.
[146] So *Wendehorst* in: *Rebmann/Säcker/Rixecker*, MüKo, § 312e, Rdnr. 112.

BGB als auch diejenigen des § 312e Abs. 1 BGB zu erfüllen. Eine Ausnahme ergibt sich nur dann, wenn eine Ausnahme nach § 312c Abs. 3 BGB vorliegt oder die Parteien auch persönlichen Kontakt hatten[147]. Handelt es sich hingegen bei beiden Parteien um Unternehmer, ist lediglich § 312e BGB zu beachten.

Für die datenschutzrechtlichen Informationspflichten gilt es in beiden Fällen zu ermitteln, ob es sich bei ihnen um Vertragsbestimmungen handelt. Ist dies zu bejahen und handelt es sich sowohl um einen Fernabsatzvertrag als auch um einen Vertrag im elektronischen Rechtsverkehr, so sind die Informationspflichten nach der Norm zu erfüllen, die dem Verbraucher den weitergehenden Schutz einräumt. Im konkreten Fall müsste der Unternehmer den Verbraucher also unter Einhaltung der Textform informieren. Findet ein Pflichtverstoß durch den Unternehmer statt, beginnt die Widerrufsfrist erst dann zu laufen, wenn der Unternehmer die Information nachholt (§§ 312d Abs. 2, 312e Abs. 3 S. 2 BGB), erlischt aber spätestens sechs Monate nach Vertragsschluss (§ 355 Abs. 3 S. 1 BGB).

### 2. Besitzstörungsanspruch

Nur im mittelbaren Zusammenhang mit den Verstoß gegen datenschutzrechtliche Informationspflichten stehend, aber trotzdem nicht unerwähnt bleiben soll der Beseitigungsanspruch gegen den Störer, welcher unaufgefordert Cookies auf den Rechnern seiner Kunden ablegt. Das unaufgeforderte Ablegen von Cookies stellt, unbeschadet der datenschutzrechtlichen Bewertung, auch eine Handlung in verbotener Eigenmacht im Sinne von § 858 Abs. 1 BGB dar, mit der Folge, dass dem Nutzer ein verschuldensunabhängiger Beseitigungs- und Unterlassungsanspruch aus § 862 Abs. 1 BGB entsteht[148].

[147] *Grigoleit*, NJW 2002, 1151–1152.
[148] *Hoeren*, DuD 1998, 455–456.

### 3. Deliktische Ansprüche

#### a) Geldersatz bei Verstößen gegen das allgemeine Persönlichkeitsrecht

Begonnen mit der berühmten Schacht-Leserbrief-Entscheidung[149], in welcher der BGH erstmalig das allgemeine Persönlichkeitsrecht als Grundrecht angesehen hat, über den Herrenreiter-Fall, in welchem erstmals ein Anspruch auf Geldersatz bei Verletzung des allgemeinen Persönlichkeitsrechts[150] (zunächst analog § 847 BGB a.F.) bejaht wurde, greift der BGH seit dem Fall „Ginsengwurzel“[151] bei der rechtlichen Einordnung des Anspruchs auf Geldentschädigung direkt auf das Wertesystem der Art. 1 und Art. 2 Abs. 1 GG zurück.

In jüngeren Entscheidungen[152] hat der BGH die Verknüpfung des allgemeinen Persönlichkeitsrechts mit den Art. 1 und 2 Abs. 1 GG mehrfach bestätigt, wobei er seit der Caroline-von-Monaco-Entscheidung regelmäßig betont, dass der Anspruch auf Geldersatz bei Verletzung des allgemeinen Persönlichkeitsrechts sich vom Anspruch auf Schmerzensgeld unterscheide, da beim Anspruch auf Geldentschädigung die Genugtuung des Opfers und die Prävention vor weiteren Verletzungen im Vordergrund stehe[153]. Der BGH hat damit der Gefahr Rechnung getragen, dass ein blosses Durchsetzen von Abmahnungen und Unterlassungsverfügungen den Verletzer nicht beeindrucken, ein ausreichender Schutz des allgemeinen Persönlichkeitsrechts ohne Entschädigungszahlungen mit Präventivfunktion daher nicht gegeben wäre[154]. Diese Rechtsprechung

[149] BGH NJW 1954, 1404.
[150] BGH NJW 1958, 827.
[151] BGH NJW 1961, 2059.
[152] BGH NJW 1995, 861 (Caroline von Monaco I); BGH NJW 1996, 984 (Caroline von Monaco II); BGH NJW 1997, 1148 (Chefarzt); zur geschichtlichen Entwicklung der Anerkennung des allgemeinen Persönlichkeitsrechts durch den BGH siehe ausführlich *Kastl, Karin*, Das allgemeine Persönlichkeitsrecht, S. 201 ff.
[153] BGH NJW 1995, 861, dort insb. S. 864.
[154] *Prinz*, Geldentschädigung bei Persönlichkeitsrechtsverletzungen durch Medien, 953–958.

wurde vom Bundesverfassungsgericht in mehreren jüngeren Entscheidungen bestätigt[155].

Der Anspruch auf Geldersatz bei Verletzung immaterieller Schäden des allgemeinen Persönlichkeitsrechts unterliegt jedoch strengen Voraussetzungen: Die Geltendmachung der Schäden ist zum einen subsidiär. Sie ist also nur dann möglich, wenn der Eingriff von der Art ist, dass Gegendarstellung, Widerruf, Unterlassung, materieller Schadensersatz für die Gewährleistung der Persönlichkeit unzureichend sind[156]. Zum anderen muss eine schwerwiegende Persönlichkeitsverletzung vorliegen[157].

### b) Geldersatz bei Verletzung immaterieller Schäden des allgemeinen Persönlichkeitsrechts

Gerade eine schwerwiegende Verletzung des Rechts auf informationelle Selbstbestimmung wird aber häufig entweder nicht vorliegen oder schwer zu beweisen sein. Die Voraussetzung des Vorliegens eines schweren Eingriffs auch im Datenschutzrecht wird daher von *Simitis* kritisiert[158]. Laut *Simitis* kann dann, wenn immaterielle Schäden eine so zentrale Rolle spielen wie bei den Folgen des Verstoßes gegen das Datenschutzrecht, eine Begrenzung der Ersatzpflicht nur verfehlt sein. Der Vorteil, die möglichen Belastung der verarbeitenden Stelle zu reduzieren, könne nicht dazu führen, dass der Ausgleichspflicht und damit dem Schutz des Betroffenen weitgehend die Wirkung genommen werde[159]. Seiner Ansicht nach dürfe die Schwere des Eingriffs sich zwar auf die Höhe des

[155] BVerfG NJW 2000, 2187; BVerfG NJW 2004, 2371; BVerfG NJW 2006, 595.
[156] *Steffen*, Schmerzensgeld bei Persönlichkeitsverletzung durch Medien - Ein Plädoyer gegen formelhafte Berechnungsmethoden bei der Geldentschädigung, 10–14; BGH NJW 1961, 2059 (Ginsengwurzel); *Rixecker* in: *Rebmann/Säcker/Rixecker*, MüKo, APKR, Rdnr. 232; *Sprau* in: *Palandt*, BGB, § 823 BGB, Rdnr. 124.
[157] BGH NJW 1979, 1041 (Exdirektor); BGH NJW 1995, 1617 (Nacktfoto); *Sprau* in: *Palandt*, BGB, § 823 BGB, Rdnr. 124.
[158] *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 34.
[159] *Simitis* in: *BDSG*, Simitis, § 8 BDSG, Rdnr. 18.

Anspruchs auswirken, dürfe aber keine Konsequenz für die Anerkennung des Anspruchs haben[160].

So berechtigt die Kritik in der Sache auch erscheinen mag, so wenig hält sie der gefestigten Rechtsprechung des Bundesverfassungsgerichts Stand. Diese bestätigt die Rechtsprechung des BGH, wonach ein schwerer Eingriff deswegen gefordert werden muss, damit nicht unbedeutende Beeinträchtigungen in unangemessener Weise ausgenutzt würden, um daran zu verdienen[161]. Es betont daher, dass die Voraussetzung eines schwerwiegenden Eingriffs verfassungsrechtlich nicht zu beanstanden ist[162].

Im Ergebnis ist festzustellen, dass ein Anspruch auf Geldersatz bei Datenschutzverstößen, die zu immateriellen Schäden führen, zwar denkbar ist, in der Praxis aber abgesehen von den wenigen Fällen, in denen ein schwerwiegender Schaden vorliegt (so beispielsweise bei medizinischen Daten oder sonstigen Daten, die einem besonderen Amtsgeheimnis oder der Verschwiegenheitspflicht unterliegen[163]), nie zugesprochen werden wird. Im Interesse einer durchsetzbaren zivilrechtlichen Sanktion, die der verarbeitenden Stelle einen Anreiz für die Einhaltung der datenschutzrechtlichen Vorschriften, insbesondere im elektronischen Bereich, schafft, wäre die Einführung einer solchen Norm durch den Gesetzgeber jedoch dringend geboten[164].

[160] *Simitis* in: *BDSG*, Simitis, § 7 BDSG, Rdnr. 34.
[161] BVerfG NJW 1973, 1221 (Soraya).
[162] BVerfG NJW 1973, 1221; dem Beschluss des BVerfG geht ein Urteil des Brandenburgischen OLG voraus, wonach kein schwerwiegender Eingriff in das APKR vorliegt, wenn ein niedergelassener Arzt auf die Übersendung eines Kurantrags eines Patienten durch dessen öffentlich-rechtlichen Dienstherrn hin, dem Dienstherren Auskunft über seinen Gesundheitszustand erteilt, ohne sich bei dem Patienten darüber erkundigt zu haben, ob dieser einverstanden ist. In der Entscheidung wird zwar auf Vorschriften des Datenschutzes nicht eingegangen, eine mit den Erwägungen von Simitis vergleichbare Interessenlage ist aber dennoch gegeben.
[163] *Schneider, Jochen*, Handbuch des EDV-Rechts, Rdnr. 375.
[164] *Schneider*, EG-Richtlinie zum Datenschutz, 35–39.

### c) Schadensersatz bei Verletzung vermögenswerter Interessen

Eine wirkungsvolle Rechtsdurchsetzung, die dem Betroffenen zumindest einen Schadensersatz bei der Verletzung vermögenswerter Interessen des allgemeinen Persönlichkeitsrechts zubilligt, könnte sich aber aus der BGH-Rechtsprechung, die sich aus den Fällen „Marlene Dietrich[165]“ und „Der blaue Engel[166]“ entwickelt hat, ergeben.

In den beiden Entscheidungen, die sich mit dem postmortalen Persönlichkeitsrecht befassen, hat der BGH festgestellt, dass „das durch § 823 I BGB geschützte allgemeine Persönlichkeitsrecht und seine besonderen Erscheinungsformen wie das Recht am eigenen Bild dem Schutz nicht nur ideeller, sondern auch kommerzieller Interessen an der Persönlichkeit dienen und diese vermögenswerten Bestandteile des Persönlichkeitsrechts vererblich sind“. Zwar hatte der BGH bereits in der Entscheidung „Mephisto[167]“ ausgesprochen, dass das Persönlichkeitsrecht - abgesehen von seinen vermögenswerten Bestandteilen - unübertragbar und unvererblich ist und wurde in der Entscheidung „Paul Dahlke[168]“ das Recht am eigenen Bild als ein vermögenswertes Ausschließlichkeitsrecht bezeichnet.

Der Fall „Marlene Dietrich“ stellt aber zum ersten Mal klar, dass die vermögenswerten Teile des allgemeinen Persönlichkeitsrecht zum einen veräußerbar und vererbbar sind und dass zum anderen bei einer Verletzung über die bloßen Abwehransprüche hinaus auch eine Schadensersatzplicht besteht[169].

[165] BGH, NJW 2000, 2195.
[166] BGH, NJW 2000, 2201.
[167] BGH, NJW 1968, 1773.
[168] BGH, NJW 1956, 1554.
[169] Zur Entwicklung der Rechtsprechung zur Anerkennung der vermögenswerten Bestandteile des Persönlichkeitsrechts siehe *Götting*, Die Vererblichkeit der vermögenswerten Bestandteile des Persönlichkeitsrechts - ein Meilenstein in der Rechtsprechung des BGH, 585–587 sowie ausführlich *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 4 ff.

Das allgemeine Persönlichkeitsrecht bildet insofern als einheitliches Rahmenrecht eine Art Dach über die unterschiedlichen Persönlichkeitsmerkmale[170]. Dabei unterliegt der Geldersatz bei einer Verletzung der ideellen Interessen des Persönlichkeitsrechts den oben genannten strengen Voraussetzungen der Subsidiarität und des Vorliegens eines schweren Eingriffes. Anders ist es bei den vermögenswirksamen Bestandteilen des allgemeinen Persönlichkeitsrechts. Diese gewähren die „wirtschaftliche Selbstbestimmung“ des Betroffenen und schützen daher die kommerziellen Interessen. Liegt eine Verletzung der vermögenswirksamen Bestandteile vor, haftet der Verletzer ebenso wie bei der Verletzung anderer vermögenswerter Ausschließlichkeitsrechte für den eingetretenen Schaden[171]. Das bedeutet, dass keine strengeren Voraussetzungen gelten dürfen, als bei der Beeinträchtigung sonstiger vermögenswerter Rechte im Sinne des § 823 Abs. 1 BGB[172]. Auf einen schwer wiegenden Eingriff kann auch deswegen verzichtet werden, weil die Entschädigungsfrage in diesen Fällen gerade nicht den Restriktionen des § 253 BGB unterliegt[173].

Für die Berechnung des Schadens steht dem Geschädigten die Wahlmöglichkeit nach den Grundsätzen der dreifachen Schadensberechnung[174] zu. Diese Art der Schadensberechnung ist vor allem bei der Verletzung von Immaterialgüter-

[170] Dabei ist strikt vom amerikanisch dualistischen System des „right of privacy“ and „right of publicity“ zu unterscheiden; vgl. dazu die ausführliche Kritik von *Götting* am dualistischen System von *Fikentscher* (*Fikentscher*, Wirtschaftsrecht, Band 2, S. 132) und am von *Beuthien* (*Beuthien/Schmölz*, Persönlichkeitsschutz durch Persönlichkeitsgüterrechte) postulierten Persönlichkeitsgüterrecht, *Götting*, Die Vererblichkeit der vermögenswerten Bestandteile des Persönlichkeitsrechts - ein Meilenstein in der Rechtsprechung des BGH, 585–587.

[171] BGH, NJW 2000, 2195 (Marlene Dietrich).

[172] *Tobias*, Vererblichkeit vermögenswerter Bestandteile des Persönlichkeitsrechts - Die neueste Rechtsprechung des BGH zum postmortalen Persönlichkeitsrecht, 31–34.

[173] *Wagner*, Prominente und Normalbürger im Recht der Persönlichkeitsverletzungen, 1305–1310.

[174] Zur dreifachen Schadensberechnung einschließlich der Vor- und Nachteile der einzelnen Berechnungsarten siehe ausführlich *Kraßer*, Schadensersatz für Verletzungen von gewerblichen Schutzrechten und Urheberrechten nach deutschem Recht, 259–272.

rechten gewohnheitsrechtlich anerkannt[175]. Der BGH hat aber bereits bei der Entscheidung „Paul Dahlke[176]“ festgestellt, dass diese auch bei der Verletzung des allgemeinen Persönlichkeitsrechts angewendet werden kann.

Bei der dreifachen Schadensberechnung handelt es sich dabei nicht um unterschiedliche Ansprüche, sondern um drei unterschiedliche Arten der Schadensliquidation[177]. Der Anspruch selbst bestimmt sich nach § 7 BDSG oder § 823 Abs. 1 BGB oder § 823 Abs. 2 BGB i.V. mit §§ 4, 28 oder 29 BDSG[178]. Der Verletzte kann bei der Schadensberechnung zum einen den Ersatz des konkreten Schadens einschließlich des entgangenen Gewinns verlangen. Diese Berechnung bestimmt sich nach den Regeln der § 249 ff. BGB. Zum anderen kann der Geschädigte sich für eine angemessene Lizenzgebühr entscheiden, welche dem Bereicherungsausgleich entspricht. Zuletzt kann der Verletzte die Herausgabe des Verletzergewinns verlangen, welcher wiederum dem Herausgabeanspruch bei der angemaßten Eigengeschäftsführung (§§ 687 Abs. 2 Satz 1, §§ 681 Satz 2, § 667 BGB) entspricht[179].

Die dreifache Schadensberechnung bei Verletzung vermögenswerter Interessen wurde bisher hauptsächlich unter dem Aspekt der Verletzung des Rechts am eigenen Bildes (§§ 22, 23 KUG) oder der Benutzung eines fremden Namens diskutiert. Häufig findet eine Verletzung in diesen Fällen einerseits durch die Medienberichterstattung, andererseits durch die Nutzung des Bildes[180] oder des Namens[181] zu Werbezwecken statt.

Trotzdem ist die Rechtsprechung ihrem Grunde nach auch auf die sonstigen Ausprägungen des allgemeinen Persönlichkeitsrechts auszuweiten. So zeigt die wirtschaftliche Entwicklung, dass das allgemeine Persönlichkeitsrecht in

[175] *Ehmann* in: *Erman*, BGB, Anh § 12 BGB, Rdnr. 374.
[176] NJW 1956, 1554.
[177] *Lettl*, Allgemeines Persönlichkeitsrecht und Medienberichterstattung, 1045–1086.
[178] Zum BDSG als Schutzgesetz siehe *Sprau* in: *Palandt*, BGB, § 823 BGB, Rdnr. 62 m.w.N.
[179] *Lettl*, Allgemeines Persönlichkeitsrecht und Medienberichterstattung, 1045–1086.
[180] Z.B. BGH NJW 1992, 2084 (Talkmaster); BGH NJW 1956, 1554 (Paul Dahlke); BGH NJW-RR 1987, 231 (Nena).
[181] BGH NJW 1962, 12 (Caterina Valente); NJW 1981, 2402 (Carrera).

der Gegenwart in einer Vielzahl von Elementen einer Verwertung im Rechtsverkehr unterworfen ist[182]. Im Bezug auf die mißbräuchliche Veröffentlichung personenbezogener Daten hatte sich der BGH bislang nur mit der Presseveröffentlichung einer Wegbeschreibung zu einer Finca einer Prominenten zu befassen[183]. Vorliegend hatte der BGH eine Verletzung des Rechts auf informationelle Selbstbestimmung, ohne jedoch auf datenschutzrechtliche Vorschriften einzugehen, durch die Veröffentlichung der Wegbeschreibung in einem Artikel einer Fernsehzeitschrift erkannt.

Auch wenn die Verletzung vermögenswerter Interessen des allgemeinen Persönlichkeitsrechts durch den Verstoß gegen datenschutzrechtliche Informationspflichten bisher in der Rechtsprechung keine Rolle gespielt hat und in der Literatur erst wenig diskutiert wurde[184], ist davon auszugehen, dass der Grundsatz der dreifachen Schadensberechnung auch in diesen Fällen anzuwenden ist. Dieses Ergebnis ergibt sich auch zwangsläufig aus der zunehmenden Kommerzialisierung des Datenschutzes[185].

Im Gegensatz zu den Fällen der Verletzung des Persönlichkeitsrechts in der Medienberichtserstattung und in der Werbung ergibt sich jedoch auch hier wieder die Frage der Höhe des Schadens. Ein Grossteil der Verletzungshandlungen dürfte hier in der fehlenden Information über die Übermittlung der Daten zum Zwecke der Werbung durch das Direktmarketing oder an Adresshändler liegen. Hierbei werden die Adressdaten des Verbrauchers mit verschiedenen Konsumgewohnheiten gekoppelt, in Datenbanken zusammengeführt und an Werbekunden weitervermittelt, um diesen eine gezieltere Bewerbung des Einzelnen zu ermöglichen.

[182] *Ullmann*, Caroline v., Marlene D., Eheleute M. - ein fast geschlossener Kreis, 1049–1054.
[183] BGH NJW 2004, 762.
[184] Zum vermögensrechtlichen Charakter des informationellen Selbstbestimmungrechts siehe beispielsweise *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 208 ff; *Kilian*, CR 2002, 921–929.
[185] Siehe dazu *Weichert*, Datenschutz im Wettbewerbs- und Verbraucherrecht, 377–383.

Das Problem für den Verletzten ergibt sich dabei daraus, dass zwar der Adresshandel in seiner Gesamtheit durch die Vielzahl der gehandelten Adressen für die Unternehmen sehr lukrativ ist, eine einzelne Adresse jedoch nur wenige Cent kostet[186]. Damit sind für den Geschädigten weder die Lizenzanalogie, noch die Herausgabe eines Verletzererlöses von Interesse.

Der Grund, warum also schadensersatzrechtliche Ansprüche auch im Falle des Adresshandels, welcher für den Unternehmer ein sehr lohnendes Geschäft darstellt, bisher nicht geltend gemacht wurden, ist der fehlende Anreiz für den Einzelnen. Auf der anderen Seite wäre es erforderlich, gerade für die Adresshändler, für die Verstöße gegen das Datenschutzrecht ein sehr lohnendes Geschäft darstellen können, eine juristische Sanktionsmöglichkeit zu haben, um „einen gewissen Druck“ zur Einhaltung des Datenschutzrechts ausüben zu können[187]. Dies ergibt sich vor allem aus der Tatsache, dass es unbefriedigend erscheint, dass auf der einen Seite ein Unternehmer steht, der bei einer Vielzahl an Verbrauchern einen in der Summe hohen Schaden verursacht, dieser aber eine Rechtsverfolgung nicht befürchten muss, weil sich die Rechtsverfolgung für den auf der anderen Seite stehenden Einzelnen nicht rechnet.

Genau diese Konstellation wurde bei dem mit der UWG-Novelle 2004 eingeführten § 10 UWG berücksichtigt[188]. § 10 UWG sieht für diejenigen Fälle, in denen ein Wettbewerber vorsätzlich unlautere Wettbewerbshandlungen betreibt und hierdurch zu Lasten einer Vielzahl von Abnehmern einen Gewinn erzielt (sog. „Streuschäden“), eine Gewinnabschöpfung in Form der Herausgabe des Gewinns an den Bundeshaushalt vor. Es wäre also, dem Normzweck der Vorschrift folgend, sinnvoll, wenn sich § 10 UWG auch auf die Fälle anwenden ließe, in denen Streuschäden bei Verbrauchern eintreten, deren Geschäftspartner unbefugt mit ihren persönlichen Daten handeln. Ob in dieser Vorgehensweise

[186] Siehe dazu *Dambeck*, Die Adress-Schnüffler, Nr. 34–35, 21.08.2006.
[187] So bereits *Hoeren/Lütkemeier*, Unlauterer Wettbewerb durch Datenschutzverstöße, 107–123.
[188] BGBl I 2004, 1414.

se jedoch ein Wettbewerbsverstoß liegt, ist bei der Frage nach den Rechtsfolgen aufgrund wettbewerbsrechtlicher Normen noch näher zu erläutern[189].

### 4. Bereicherungsrechtliche Ansprüche

Der Bereicherungsanspruch steht in Anspruchskonkurrenz zum Deliktsanspruch auf Ersatz des immateriellen Schadens und kann daher neben diesem geltend gemacht werden[190].

Nach der Entscheidung „Herrenreiter“ des BGH ist aber der bereicherungsrechtliche Ausgleich (und damit auch der deliktsrechtliche Ausgleich im Wege der Lizenzanalogie) dann zu versagen, wenn eine Bereitschaft des Verletzers zum Abschluss des (fiktiven) Vertrages nicht bestand. Der BGH argumentierte dabei, dass eine Fiktion auch des Willens zum Vertragsabschluss dem Verletzten ein Verhalten unterstellen würde, das er als erneute Persönlichkeitsminderung empfinden würde[191]. Der BGH sah also einen offenen Widerspruch darin, dass der Verletzte gegen die Verletzung seines allgemeinen Persönlichkeitsrechts einerseits vorgeht, andererseits aber Schadensersatz oder einen bereicherungsrechtlichen Anspruch in einer Art und Weise geltend macht, welche die von ihm rechtlich verfolgte Verletzungshandlung gerade fingiert.

In der Entscheidung „Fußballtorwart“ ist der BGH von dieser Ansicht abgewichen. Als einzig allein entscheidende Tatsache sah der BGH an, dass der in Anspruch genommene tatsächlich geldwerte Vorteile gezogen hat und dass dies

[189] Siehe dazu sogleich unter Abschnitt G.V. auf Seite 215; beachte jedoch, dass auch der „Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“ eine Gewinnabschöpfung als Verschärfung des Bußgeldrahmens vorsieht, BT-Drs. 16/12011, 36.

[190] *Canaris*, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, S. 98.

[191] BGH NJW 1958, 827; So auch *Steffen*, Schmerzensgeld bei Persönlichkeitsverletzung durch Medien - Ein Plädoyer gegen formelhafte Berechnungsmethoden bei der Geldentschädigung, 10–14.

nach der Verkehrsübung nicht hätte geschehen können, ohne dem Betroffenen dafür eine geldwerte Gegenleistung zu erbingen[192].

*Canaris* weist darauf hin, dass die Ansicht des BGH, wie er sie beim „Herrenreiter"-Fall noch vertreten hat, zumindest nicht auf bereicherungsrechtliche Fälle, sondern allenfalls auf das Schadensersatzrecht zutreffen kann[193]. Eine etwaige Vermögensminderung auf Seiten des Bereicherungsgläubigers ist mithin gerade nicht nötig, da es für das Bereicherungsrecht einzig darauf ankommt, dass der Bereicherungsschuldner gem. § 812 Abs. 1 S. 1 BGB etwas auf Kosten des Gläubigers erlangt hat. Es handelt sich deswegen gerade um Bereicherungsrecht und nicht etwa um Entreicherungsrecht[194]. *Canaris* bezeichnet insofern die Entscheidung „Herrenreiter" zutreffend als „Relikt einer längst überwundenen Sichtweise"[195].

Indes ist aber auch die Notwendigkeit einer Lizenzbereitschaft als Voraussetzung für den schadensersatzrechtlichen Anspruch abzulehnen[196]. Die Notwendigkeit einer Lizenzbereitschaft würde denjenigen Schädiger privilegieren, der gezielt davon ausgehen konnte, dass bei entsprechenden Verhandlungen der Eingriff vom Geschädigten nicht lizenziert worden wäre[197]. Auf der anderen Seite gingen dann gerade die Geschädigten leer aus, die einen Eingriff in ihr Persönlichkeitsrecht strikt ablehnen, während diejenigen Ersatz erhalten, die grundsätzlich dazu bereit gewesen wären, über die vermögenswerten Interessen ihres Persönlichkeitsrechts in Verhandlungen zu treten. Darüber hinaus würde der Anspruch gerade in den Fällen entfallen, in denen eine besonders schwe-

[192] BGH NJW 1979, 2205; Zur Rechtsprechung des BGH siehe auch *Prinz/Peters*, Medienrecht, Rdnr. 900 m.w.N.
[193] *Canaris*, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, S. 89.
[194] So auch *Götting*, Sanktionen bei Verletzung des postmortalen Persönlichkeitsrechts, 801–808 sowie *Götting*, Persönlichkeitsrechte als Vermögensrechte, S. 55.
[195] *Canaris*, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, S. 90.
[196] A.A. *Gounalakis*, AfP 1998, 10–25.
[197] *Wagner*, Prominente und Normalbürger im Recht der Persönlichkeitsverletzungen, 1305–1310.

re Form der Verletzung vorliegt, weil diese regelmäßig ohne Zustimmung des Verletzten stattfindet[198].

Es ist daher unerheblich, ob der Verletzte zum Abschluss des Vertrages bereit gewesen wäre oder er die Möglichkeit gehabt hätte, durch einen derartigen Vertrag auch tatsächlich einen Gewinn zu erzielen. Auf das Datenschutzrecht übertragen bedeutet dies, dass auch in denjenigen Fällen, in denen der Betroffene bei ordnungsgemäßer Information eine Einwilligung zur Nutzung seiner personenbezogenen Daten nicht zugestimmt hätte, ein bereicherungsrechtlicher Anspruch trotzdem gegeben sein kann.

Das erlangte „Etwas“ im Sinne des § 812 Abs. 1 S. 1 BGB ist im Falle einer datenschutzrechtlichen Verletzung die Nutzung des fremden Persönlichkeitsrecht, die beispielsweise in der rechtsgrundlosen Weitergabe von Adressdaten an einen Adresshändler bestehen kann[199]. Da die Herausgabe der Nutzung wegen „der Beschaffenheit des Erlangten nicht“ möglich ist, ist der Wert zu ersetzen (§ 818 Abs. 2 BGB). Dieser berechnet sich seiner Höhe nach wie der Schadensersatz im Wege der Lizenzanalogie, setzt aber im Gegensatz zu ihm kein Verschulden voraus[200]. Im Falle des Adresshandels wäre dies der Preis, den ein Adresshändler für die Adresse eines Betroffenen zu zahlen bereit gewesen wäre.

Eine Herausgabe des Gewinns ergibt sich hingegen nur nach §§ 819 Abs. 1, 818 Abs. 4 in Verbindung mit § 281 BGB, falls der Bereicherungsschuldner den Mangel des Rechtsgrunds kannte, also im konkreten Fall wusste, dass der Betroffene in eine Weitergabe seiner Adressdaten nicht eingewilligt hat[201]. Leider ergibt sich sowohl beim Anspruch auf Herausgabe nach § 818 Abs. 2 BGB wie auch bei Anspruch auf Gewinnherausgabe das bereits unter Ab-

[198] *Götting*, Sanktionen bei Verletzung des postmortalen Persönlichkeitsrechts, 801–808.
[199] Vgl. zum Inhalt des Anspruchs auch *Canaris*, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, 85–109.
[200] Vgl. *Bayreuther* in: *Rebmann/Säcker/Rixecker*, MüKo, § 12, Rdnr. 248.
[201] Dieser gilt auch für die Eingriffskondiktion, vgl. *Larenz/Canaris*, Schuldrecht BT mit w. N. auch für die Gegenansicht.

schnitt G.IV.3.c) Ausgeführte: Zwar entstand aus der rechtsgrundlosen Nutzung fremder Daten ein sehr lukrativer Geschäftszweig, da dieser jedoch aus der Nutzung einer Vielzahl verschiedener Daten entsteht, ist das Datum des Einzelnen mit solch einem geringen Wert zu beziffern, dass einer Rechtsdurchsetzung in der Praxis keinerlei Bedeutung zuzumessen ist.

### 5. Anspruch aus angemaßter Eigengeschäftsführung

Ein Anspruch auf Herausgabe des Verletzergewinns kann sich zuletzt noch aus §§ 687 Abs. 1 S. 1, 681 S. 2, 667 BGB ergeben. Nach herrschender Ansicht ist ein fremdes Geschäft auch dann gegeben, wenn der Betroffene in die Verwertung seines Persönlichkeitsrechts unter keinen Umständen zugestimmt hätte[202]. Einer anderen Ansicht nach ist hier ein fremdes Geschäft zu verneinen, weil in diesen Fällen kein fremdes Geschäft, sondern ein eigenes Geschäft des Verletzers vorliegt[203]. Der herrschenden Ansicht ist hier der Vorzug zu geben, da die Frage nach dem mutmaßlichen Willen des Geschäftsherren lediglich für die Entscheidung relevant ist, ob eine berechtigte oder eine unberechtigte Geschäftsführung ohne Auftrag vorliegt[204], nicht aber ob ein fremdes Geschäft vorliegt.

Rechtsfolge ist auch hier die Herausgabe des Verletzergewinns, §§ 687 Abs. 2 S. 1, 681 S. 2, 667 BGB. Eine Besonderheit ergibt sich hierbei nur insofern, dass dem Betroffenen gegen den Geschäftsführer ein Auskunftsanspruch nach §§ 687 Abs. 2 Satz 1, 681 Satz. 2, 666 BGB zusteht. Dieser richtet sich zwar danach, was nach Treu und Glauben auch im Hinblick auf die Art und Schwere der Rechtsverletzung geboten erscheint[205]. Wird jedoch erneut auf das Bei-

[202] *Götting*, Sanktionen bei Verletzung des postmortalen Persönlichkeitsrechts, 801–808; *Beuthien/Schmölz*, Persönlichkeitsschutz durch Persönlichkeitsgüterrechte, S. 52.
[203] So im Ergebnis *Seiler* in: *Rebmann/Säcker/Rixecker*, MüKo, § 687, Rdnr. 20; *Gounalakis*, AfP 1998, 10–25.
[204] *Götting*, Sanktionen bei Verletzung des postmortalen Persönlichkeitsrechts, 801–808; *Beuthien/Schmölz*, Persönlichkeitsschutz durch Persönlichkeitsgüterrechte, S. 52.
[205] Vgl. *Bayreuther* in: *Rebmann/Säcker/Rixecker*, MüKo, § 12 BGB, Rdnr. 249.

spiel des Adresshändlers zurückgegriffen, bleibt festzustellen, dass eine gezielte Frage nach dem Umfang des mit der unberechtigten Weitergabe der Adresse erwirtschafteten Gewinns und der damit verbundene Schriftverkehr zumindest dazu geeignet sein dürfte, für Unannehmlichkeiten zu sorgen. Ob diese jedoch dazu ausreichen, eine abschreckende Wirkung zu erzielen, ist zweifelhaft[206]. Eine wirksame Abschreckung für den Adresshändler ließe sich vielmehr nur dann erreichen, wenn er nicht nur den zu vernachlässigenden Gewinn des einzelnen herausgeben müsste, sondern den Gesamtgewinn der veräußerten Adressen. Ein derartiger Gewinnabschöpfungsanspruch wäre aber lediglich dann denkbar, wenn in den Fällen der Verletzung des allgemeinen Persönlichkeitsrechts auch wettbewerbsrechtliche Belange berührt wären, mit der Folge der Anwendbarkeit des § 10 UWG.

## V. Rechte des Betroffenen aus Verstößen gegen Wettbewerbsrecht

### 1. Datenschutz und unlauterer Wettbewerb

Zunächst gilt es zu klären, ob Datenschutzverstöße überhaupt dazu geeignet sind, gleichzeitig auch unlautere Wettbewerbsmaßnahmen darzustellen. Diese Frage war zumindest vor der umfassenden Reform des UWG 2004, welches nunmehr zum 1.1.2009 erneut novelliert wurde[207], stark umstritten[208]. Sie wurde insbesondere in den 1990er Jahren im Zusammenhang damit, ob die datenschutzwidrige Übernahme von Telefonbuchdaten auf CD-Rom auch

[206] Für eine abschreckende Wirkung des Auskunftsanspruchs aus angemaßter Eigengeschäftsführung in Verbindung mit Verletzungen des allgemeinen Persönlichkeitsrechts, s. *Lettl*, Allgemeines Persönlichkeitsrecht und Medienberichterstattung, 1045–1086.

[207] 1. UWGÄndG, BGBl. I 2008, 2949.

[208] Vgl. *Weichert*, Datenschutz im Wettbewerbs- und Verbraucherrecht, 377–383, m.w.N.

einen Wettbewerbsverstoß darstellt, von der Rechtsprechung unterschiedlich bewertet[209].

Nach altem Recht galt es dabei zwischen wertbezogenen und wertneutralen Normen zu unterscheiden. Während bei Verletzung gegen eine wertbezogene Norm stets auch ein Verstoß gegen § 1 UWG a.F. gegeben war, war Voraussetzung für einen Wettbewerbsverstoß durch wertneutrale Normen, dass der Handelnde unter Ausnutzung der Gesetzestreue seiner Mitbewerber sich bewusst und planmäßig über eine Norm hinweg setzte, um sich einen Wettbewerbsvorteil zu verschaffen[210]. Der Verletzer musste daher vorsätzlich einen „Vorsprung durch Rechtsbruch“ erhalten wollen[211].

Die Unterscheidung zwischen wertbezogenen und wertneutralen Normen wurde jedoch im Schrifttum kritisiert, da sie zu nicht lösbaren Abgrenzungsschwierigkeiten führe[212]. Bereits vor der Reform 2004 war dahingehend auch ein Wandel in der Rechtsprechung des BGH zu verzeichnen, indem er Ende der 1990er Jahre vom Dualismus zwischen wertbezogenen und wertneutralen Normen abrückte[213] und zuletzt für die Beurteilung, ob ein Wettbewerbsverhalten sittenwidrig sei, eine am Schutzzweck des § 1 UWG a.F. ausgerichtete Würdigung forderte[214]. Die vom BGH zuletzt entwickelte Rechtsprechung wurde mit der Reform nunmehr in § 4 Nr. 11 UWG niedergelegt. Demnach handelt unlauter insbesondere derjenige, *der einer gesetzlichen Vorschrift zuwiderhandelt,*

[209] Dafür vgl. LG Mannheim, NJW 1996, 1829, LG München I, CR 1998, 83; dagegen u.a. OLG Frankurt/Main, WRP 1996, 1175; S. dazu auch ausführlich *Hoeren/Lütkemeier*, Unlauterer Wettbewerb durch Datenschutzverstöße, 107–123 m.w.N.

[210] BGH GRUR 1963, 578 (Sammelbesteller), BGH GRUR 1988, 699 (qm-Preisangaben), BGH GRUR 2002, 636 (Sportwetten).

[211] Zum Vergleich zwischen neuer und alter Rechtslage siehe ausführlich *Ernst*, WRP 2004, 1133–1137.

[212] *Hoeren/Lütkemeier*, Unlauterer Wettbewerb durch Datenschutzverstöße, 107–123; zur früheren Rechtsprechung siehe umfassend *Piper* in: *Piper/Ohly*, UWG, Rdnr. 11/1.

[213] Zum Paradigmenwechsel in der Rechtsprechung des BGH siehe die drei zentralen Entscheidungen: BGH GRUR 1998, 407 (TIAPRIDAL); BGH GRUR 1999, 1128 (Hormonpräparate); BGH GRUR 2000, 237 (Giftnotruf-Box); hier stellt der BGH klar, dass ein Verstoß gegen wertbezogene Normen nicht per se als Verstoß gegen § 1 UWF a.F. zu werten ist.

[214] BGH GRUR 2000, 1076 (Abgasemissionen).

*die auch dazu bestimmt ist, im Interesse der Martktteilnehmer das Marktverhalten zu regeln.*

Vor diesem Hintergrund muss die im Rahmen der Entscheidungen bezüglich der Übernahme der Telefonbuchdaten auf CD-Rom vormals strittige Frage, ob es sich bei den datenschutzrechtlichen Normen um wertbezogene oder wertneutrale handelt, nunmehr in einem neuen Licht betrachtet werden. Es gilt zu beurteilen, welche der datenschutzrechtlichen Normen über den Schutz des Rechts auf informationelle Selbstbestimmung des Einzelnen hinaus, auch dem Schutz des Wettbewerbs dienen können, mithin also Wettbewerbsbezogenheit aufweisen. Während bei der alten Rechtslage die Gerichte überwiegend[215] darin übereinstimmten, dass die Normen des BDSG aus dem Grunde wertbezogen seien, weil ein Verstoß gegen das Recht auf informationelle Selbstbestimmung stets sittenwidrig ist, kann auf die Argumentation nunmehr nicht mehr zurückgegriffen werden[216].

Die Analyse, ob eine Norm marktbezogen ist, ergibt sich aus deren Normzweck. Dabei muss der Schutz der Marktbeteiligten nicht der alleinige oder hauptsächliche Zweck sein, sondern es genügt (bereits dem Wortlaut des § 4 Nr. 11 UWG nach), dass der Schutz vom Gesetz auch bezweckt ist. Das ist jedoch nur dann der Fall, wenn der Gesetzgeber den Sinn und Zweck der Norm auch auf diesen Schutz gerichtet hat und dieser nicht bloss reflexartig entsteht[217]. Genau im Hinblick auf diese Reflexartigkeit besteht hinsichtlich der wenigen Stimmen, die sich mit der Frage nach dem Zusammenhang zwischen Datenschutz- und Wettbewerbsrecht nach neuer Rechtslage auseinander gesetzt haben, Uneinigkeit[218].

[215] Vgl. LG Mannheim, NJW 1996, 1829, LG München I, CR 1998, 83; dagegen u.a. OLG Frankurt/Main, WRP 1996, 1175

[216] So zutreffend *Gärtner/Heil*, WRP 2005, 20–24.

[217] *Piper* in: *Piper/Ohly*, UWG, § 4 UWG, Rdnr. 11/17.

[218] Siehe dazu *Gärtner/Heil*, WRP 2005, 20–24; *Heil*, RDV 2004, 205–211; *Weichert*, Datenschutz im Wettbewerbs- und Verbraucherrecht, 377–383.

Einer Ansicht nach wird behauptet, die datenschutzrechtlichen Informationspflichten dienen allein der persönlichkeitsrechtlichen Integrität und wiesen somit keinen Wettbewerbsbezug auf[219]. Zum Widerspruchsrecht gem. § 28 Abs. 4 S. 1 und S. 2 BDSG wird angeführt, dass Werbung zwar grundsätzlich auf einen potenziellen Nachfrager von Waren abzielt, ein nur mittelbarer Zusammenhang mit dem Verhalten der Marktteilnehmer aber nicht genüge, um die Marktbezogenheit zu bejahen[220]. Das *Hanseatische Oberlandesgericht* geht sogar so weit, § 28 Abs. 4 S. 2 BDSG seine verbraucherschützende Funktion ganz abzusprechen[221].

In der Kommentarliteratur wird indes von der Marktbezogenheit des § 28 BDSG ausgegangen[222]. Dem OLG Stuttgart zufolge „wohnt dem Erwerb von Kundendaten, deren Weitergabe gegen § 28 Abs. 3 BDSG verstößt, jedenfalls dann ein Marktbezug inne, wenn der Empfänger, der um die rechtswidrige Weitergabe derselben weiß, diese Daten zu Werbezwecken oder in sonstiger Weise wettbewerbserheblich verwenden will und verwendet“[223]. Dieser Ansicht ist auch zu folgen. Der bestehende Zusammenhang zwischen Datenschutz und Wettbewerbsrecht findet bereits in den Erwägungsgründen zur EG-Datenschutzrichtlinie Erwähnung: In Erwägungsgrund (7) heißt es, dass das unterschiedliche Schutzniveau der Privatsphäre den Wettbewerb verfälschen kann.

Er wird durch die EK-DSRL noch stärker herausgestrichen: Auch wenn die Richtlinie Art. 1 Abs. 1 zufolge in erster Linie dem Schutz der Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation dient, so ergibt sich doch insbesondere aus Art. 13 der Richtlinie, welcher den Schutz vor unerbetenen Nachrichten regelt, dass der Datenschutz, vor allem durch

[219] *Heil*, RDV 2004, 205–211.
[220] *Gärtner/Heil*, WRP 2005, 20–24.
[221] OLG Hamburg, AfP 2004, 554.
[222] *Piper* in: *Piper/Ohly*, UWG, § 4, Rdnr. 37; *Köhler* in: *Hefermehl/Köhler/Bornkamm*, UWG, § 4 UWG, Rdnr. 11.42.
[223] OLG Stuttgart GRUR-RR 2007, 330.

Mittel der elektronischen Kommunikation, über den reinen Schutz des Rechts auf informationelle Bestimmung hinaus, längst schon an Bedeutung sowohl für den Verbraucherschutz, als auch für das Wettbewerbsrecht erlangt hat. So wurde folgerichtig Art. 13 national in § 7 Abs. 2 und 3 UWG umgesetzt und insoweit unterstrichen, dass Art. 13 in Bezug auf belästigende Werbung nicht nur den Aspekt des Datenschutzes, sondern auch den des Wettbewerbsrechts berücksichtigt[224].

Überdies ist der Studie des Unabhängigen Landeszentrum für Datenschutz Schleswig Holstein zur „Erhöhung des Datenschutzniveaus zugunsten der Verbraucher“ zu folgen[225]. Diese bezeichnet die Trennung der datenschutz- und verbraucherrechtlichen Informationspflichten als künstlich, da „außer der Perspektive der Daten verarbeitenden Stelle die Erhebung und Verarbeitung personenbezogener Kundendaten nur ein Baustein eines umfassenden Marketingkonzepts ist, mit dem der Verbraucher als Kunde geworben werden soll“[226]. Ferner sei „der eigentliche Sinn und Zweck der datenschutzrechtlichen Pflichten, den Betroffenen nicht nur einen Ausgleich für die von ihnen nach § 28 f. BDSG hinzunehmende Datenverarbeitung, sondern ihnen auch Entscheidungsfähigkeit in der Auswahl ihrer Kommunikationspartner zu verschaffen, denen sie ihre Daten zu überlassen bereit sind“[227].

Es wäre aber verfehlt, nach der Novellierung der UWG die Frage, ob ein Verstoß gegen die datenschutzrechtlichen Informationspflichten auch wettbewerbswidrig ist, allein an § 4 Nr.11 UWG festzumachen. Die neuen UWG-Regelungen enthalten darüber hinausgehende Verbraucherschutztatbestände, die teilweise auch an einen nach BDSG unzulässigen Datenumgang anknüpfen[228]. Nennenswert ist hier zum einen der bereits soeben erwähnte § 7 Abs. 2

[224] So im Ergebnis auch *Ohly* in: *Piper/Ohly*, UWG, § 7, Rdnr. 10 und *Eckhardt*, MMR 2003, 557–562.
[225] *Bizer, u.a.*, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher.
[226] *Bizer, u.a.*, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, S. 182.
[227] *Bizer, u.a.*, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, S. 183.
[228] *Gola/Reif*, RDV 2009, 104–112.

UWG. Liegt in den Fällen personalisierter Werbung ein Verstoß gegen § 7 Abs. 2 UWG vor, so ist auch immer von einem Datenschutzverstoß auszugehen[229].

In Bezug auf die Informationspflichten nach § 4 Abs. 3 BDSG und § 13 Abs. 1 TMG ist darüber hinaus die neue Regelung in § 5a Abs. 2 UWG zu beachten. Danach handelt unlauter, wer die Entscheidungsfähigkeit von Verbraucher dadurch beeinflusst, dass er eine wesentliche Information vorenthält. Der eigentliche Sinn und Zweck der datenschutzrechtlichen Informationspflichten ist nicht nur ein Ausgleich der vom Betroffenen hinzunehmenden Datenverarbeitung, sondern auch ihnen Entscheidungsfreiheit in der Auswahl ihrer Kommunikationspartner zu verschaffen[230]. Werden personenbezogene Daten also im Zusammenhang mit einer geschäftlichen Handlung erhoben, dienen die Informationspflichten nach § 4 Abs. 3 BDSG und § 13 Abs. 1 TMG mithin dazu, eine an ihnen ausgerichtete geschäftliche Entscheidung vornehmen zu können. So ergibt sich ein Verstoß gegen § 5a Abs. 2 UWG zumindest dann, wenn die verschwiegene Information dazu führt, den Betroffenen von einer geschäftlichen Entscheidung abzuhalten[231].

Ferner ist bei Verstoß gegen die datenschutzrechtlichen Informationspflichten auch an die Verwirklichung des § 4 Nr. 2 UWG zu denken. Danach verhält sich unlauter, wer „Wettbewerbshandlungen vornimmt, die geeignet sind, die geschäftliche Unerfahrenheit insbesondere von Kindern und Jugendlichen [...] auszunutzen“. Dabei ist zwar die Datenerhebung bei Kindern und Jugendlichen nicht an sich unlauter, sie wird es aber dann, wenn der wahre Grund der Datenerhebung, also z.B. die Verwertung der Daten zu Werbezwecken, verschwiegen

[229] *Gola/Reif*, RDV 2009, 104–112; umgekehrt wird dies zumindest in den Fällen anzunehmen sein, in denen der Betroffene sein Widerspruchsrecht nach § 28 Abs. 4 BDSG wahrgenommen hat, da spätestens dann erkennbar ist, dass er diese Werbung nicht wünscht.
[230] *Bizer*, Datenschutzrechtliche Informationspflichten, 454 ff..
[231] *Gola/Reif*, RDV 2009, 104–112.

wird und auch nicht ohne weiteres erkennbar ist[232]. In letzterem Fall ist auch § 4 Nr. 3 UWG verwirklicht.

## 2. Rechtsfolgen bei Verstößen gegen Wettbewerbsrecht

Die Rechtsfolgen bei Verstößen gegen das Wettbewerbsrecht finden sich in den §§ 8 ff. UWG. Sie bestehen zum einen im Anspruch auf Beseitigung und Unterlassung des § 8 UWG, zum anderen im Schadensersatzanspruch § 9 UWG. Beide Ansprüche laufen parallel zum Anspruch auf Beseitigung, Berichtigung oder Sperrung des § 35 BDSG auf der einen Seite und dem Anspruch auf Schadensersatz des § 7 BDSG auf der anderen Seite. Die datenschutzrechtlichen Regelungen sind insofern weder abschließend, noch schließen sie die Anwendung von Wettbewerbsrecht aus[233]. Daraus folgt, dass neben dem Betroffenen, vor allem auch Mitbewerbern, Ansprüche aus Beseitigung, Unterlassung und Schadensersatz zustehen können, wobei sich der Schadensersatz in diesem Fälle auf Vermögensschäden begrenzen wird. Der Vorteil ist, dass Mitbewerber, gerade im Internet, mitunter durch die Verwendung ähnlicher technischer Vorgänge eher einen Einblick haben könnten, wann und ob es zu Verstößen gegen das Datenschutzrecht kommt.

Besonders interessant für die Fälle von Datenschutzverstößen durch Adresshändler, in denen eine Rechtsdurchsetzung durch den Betroffenen, wie bereits geschildert[234], nicht zu erwarten ist, ist der mit der UWG-Novelle neu eingeführte § 10 UWG. § 10 UWG wurde geschaffen, um eine Rechtsschutzlücke innerhalb der zivilrechtlichen Sanktionen gegen Wettbewerbsverstöße zu schließen. Diese ergab sich immer dann, wenn eine Vielzahl von Abnehmern bei gleichzeitiger geringerer Schadenshöhe im Einzelnen geschädigt wurde[235].

[232] OLG Frankfurt, GRUR 2005, 785; *Köhler* in: *Hefermehl/Köhler/Bornkamm*, UWG, Rdnr. 2.24.
[233] *Gola/Schomerus*, BDSG, § 7 BDSG, Rdnr. 16 und § 35, Rdnr. 26.
[234] Siehe Abschnitt G.IV.3.c) auf Seite 206 und Abschnitt G.IV.4. auf Seite 211.
[235] *Köhler* in: *Hefermehl/Köhler/Bornkamm*, UWG, § 10 UWG, Rdnr. 3.

Das Problem bei den sog. Streuschäden war einerseits, dass eine Durchsetzung durch den Einzelnen selten erfolgte, weil der geringe Schaden den Aufwand der Rechtsdurchsetzung nicht aufwog oder er sich der Schädigung oftmals gar nicht bewusst war, dem Mitbewerber aber andererseits kein Schaden entstanden war. § 10 UWG dient nunmehr der zivilrechtlichen Prävention indem er verhindern soll, dass ein Unternehmer den durch Streuschäden erwirtschafteten Gewinn behalten darf[236].

Anspruchsberechtigte des Gewinnabschöpfungsanspruchs sind gem. § 8 Abs. 3 Nr. 2 bis 4 UWG die dort genannten Kammern und Verbände, nicht aber die Mitbewerber. Den Anspruchsberechtigten wird somit durch den Gewinnabschöpfungsanspruch ein zusätzliches Mittel an die Hand gegeben, da ihnen der Schadensersatzanspruch nach § 9 UWG gerade nicht zusteht[237].

Als Voraussetzungen nennt § 10 Abs. 1 UWG einen vorsätzlichen Wettbewerbsverstoß und eine Gewinnerzielung zu Lasten einer Vielzahl von Abnehmern. Beide Voraussetzungen führen in der Praxis zu nicht unerheblichen Beweisschwierigkeiten[238]. Sind diese Einschränkungen noch zu befürworten, weil sie gewährleisten, dass sich die Unternehmer weiterhin im Graubereich wettbewerbsrechtlicher Zulässigkeit bewegen können, ohne befürchten zu müssen, die damit erwirtschafteten Gewinne zu verlieren[239], so führt die Rechtsfolge der Herausgabe an den Bundeshaushalt dazu, dass den Klagebefugten zudem der finanzielle Anreiz für die Rechtsdurchsetzung fehlt[240]. Somit ist die Praxisrelevanz des § 10 UWG mit bisher 15 eingeleiteten Verfahren[241] gering. Es bleibt

[236] *Köhler* in: *Hefermehl/Köhler/Bornkamm*, UWG, § 10 UWG, Rdnr. 3.
[237] Dies führte unter anderem dazu, dass Schadensersatzansprüche im Gegensatz zu den Abwehransprüchen eine untergeordnete Rolle spielen, vgl. *Neuberger*, Der wettbewerbsrechtliche Gewinnabschöpfungsanspruch im europäischen Rechtsvergleich, S. 37.
[238] *Beuchler*, WRP 2006, 1288–1293.
[239] So *Neuberger*, Der wettbewerbsrechtliche Gewinnabschöpfungsanspruch im europäischen Rechtsvergleich, S. 136.
[240] Siehe hierzu deutlich: *vzbv*, Verbraucherschutz: Recht harmlos? - Verbandsklage auf dem Prüfstand (Redebeiträge); *Piper* in: *Piper/Ohly*, UWG, § 10 UWG, Rdnr. 4.
[241] *Beuchler*, WRP 2006, 1288–1293.

zu hoffen, dass der Gesetzgeber durch Nachbesserung der Norm das Prozesskostenrisiko auf Seiten der klagende Verbände absichert. Lediglich in diesem Fall würde § 10 UWG mehr als nur ein stumpfes Schwert gerade auch für die Fälle des Verstoßes gegen den Datenschutz bei Adresshändlern darstellen.

Im Ergebnis bleibt festzuhalten, dass in naher Zukunft Verstöße gegen den Datenschutz, die gleichzeitig auch Wettbewerbsverstöße darstellen, wohl nur im Rahmen von § 8 UWG eine Rolle spielen werden. Hierbei ist insbesondere der Unterlassungsanspruch für die Fälle denkbar, in denen Wiederholungsgefahr droht.

# H. Ergebnis und Ausblick

Eine Wahrung der datenschutzrechtlichen Informationspflichten ist im Rahmen der geltenden Rechtslage weder zu erwarten, noch ist sie in der heutigen Internetpraxis vorhanden. So wird am Beispiel Amazons augenscheinlich, was den datenschutzrechtlichen Alltag der Internetnutzer beherrscht: Große Unternehmen verarbeiten eine Vielzahl der Daten Ihrer Kunden zu verschiedensten Zwecken, ohne dass diese durch übersichtliche und umfassende Datenschutzerklärungen ihr Recht auf informationelle Selbstbestimmung derart ausüben können, wie es ursprünglich vom Bundesverfassungsgericht im „Volkszählungsurteil“ festgelegt war: als „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.

Zu diesem Ergebnis führt jedoch nicht das Fehlen umfassender Informationspflichten im BDSG und den bereichsspezifischen Regelungen. Bei Wahrung der darin enthaltenen Pflichten wäre eine umfassende Information des Betroffenen bzw. des Nutzers durchaus gewährleistet. Eine ex ante Regelung durch den Gesetzgeber, in der alle nur denkbaren Verwendungsweisen personenbezogener Informationen abgedeckt werden, wäre ohnehin nicht möglich und würde lediglich in eine „Verrechtlichungsfalle“ führen[1]. Es liegt vielmehr am Fehlen zivilrechtlich wirksamer Instrumente, die dem Betroffenen Werkzeuge zur Hand geben würden, im Falle einer Verletzung ihres Rechts auf informationelle Selbstbestimmung gegen den Verantwortlichen vorzugehen.

Das Datenschutzrecht selbst kennt neben dem Anspruch auf Berichtigung, Löschung und Sperrung (§ 35 BDSG) lediglich den Schadensersatzanspruch aus § 7 BDSG, welcher wiederum auf Vermögensschäden begrenzt ist. Bei

[1] *Bull*, RDV 1999, 148–153; *Bull*, RDV 2008, 47–55.

den Ansprüchen aus dem allgemeinen Zivilrecht ergibt sich eine Fragestellung, die mindestens so alt ist wie die Herrenreiter-Entscheidung des BGH: Findet eine indirekte Kommerzialisierung höchstpersönlicher Rechtsgüter durch die Gewährung von Geldersatz im Verletzungsfall statt und falls diese Frage bejaht wird, ist diese überhaupt vom deutschen Recht gewünscht?

Eine Beantwortung dieser Fragen dürfte spätestens seit der Marlene-Dietrich-Entscheidung möglich sein. Das Persönlichkeitsrecht enthält vermögenswerte Bestandteile. Immer dann also, wenn zu Lasten des Inhabers des Persönlichkeitsrechtes diese vermögenswerten Bestandteile genutzt wurden, müssen diesem dagegen auch zivilrechtliche Ansprüche zustehen. Die Kommerzialisierung der höchstpersönlichen Rechtsgüter findet insofern nicht durch die zivilrechtlichen Ansprüche, sondern vielmehr bereits durch die Verletzungshandlung statt.

Dass eine zunehmende Kommerzialisierung von personenbezogenen Daten gerade durch das Medium Internet stattfindet, zeigt wiederum bereits die Auflistung der technischen Möglichkeiten im ersten Teil dieser Arbeit. Doch so lukrativ die Verarbeitung von personenbezogenen Daten für die Unternehmen sein mögen, ergibt sich dadurch auf rechtlicher Ebene ein neuer Problemkreis: Selbst bei Bejahung der zivilrechtlichen Ansprüche ist der Schaden beim Einzelnen zu gering, als dass dieser eine Rechtsdurchsetzung anstreben würde.

Damit die bereits vorhandenen, umfassenden, datenschutzrechtlichen Informationspflichten in Zukunft im Internet nicht vollständig ausgehöhlt werden, ist eine Änderung der Gesetze dahingehend notwendig, dass dem Betroffenen im Falle von Verstößen ausreichende Rechtsansprüche zur Verfügung stehen, die er gegen die verantwortliche Stelle geltend machen kann. Die Schwierigkeit bei der Umsetzung dieser Rechtsansprüche wird darin liegen, eine Rechtsdurchsetzung für den Einzelnen trotz der Tatsache lohnend zu machen, dass er selbst nur einen geringen Schaden erlitten hat. Einen Anhaltspunkt für einen derar-

tigen Anspruch kann eventuell § 10 UWG bieten[2]. Insofern ist vor allem auf dessen Schwächen zu achten, damit von der Gesetzgebung nicht erneut ein „stumpfes Schwert“ geschaffen wird. Die geplante Änderung des § 43 Abs. 3 BDSG[3] vermag in diesem Zusammenhang gerade nicht zu überzeugen, da auch hier auf eine sanktionsrechtliche Lösung zurückgegriffen wurde, statt den Weg in eine zivilrechtliche Rechtsdurchsetzung zu eröffnen.

Einen eigenen Regelungsvorschlag möchte diese Arbeit hierzu bewusst nicht liefern. Wohl aber soll die vorangegangene strukturierte Darstellung sowohl der datenschutzrechtlichen Informationspflichten als auch der derzeitigen zivilrechtlichen Folgen den Weg zur weiteren wissenschaftlichen Auseinandersetzung ebnen[4].

[2] So im Ergebnis auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 316.
[3] BT-Drs. 16/12011.
[4] Siehe auch die in diesem Zusammenhang bereits erfolgten, begrüßenswerten Vorschläge in *Abel*, RDV 2009, 51–57.

# I. Abkürzungsverzeichnis

Soweit nicht sprachgebräuchliche Abkürzungen verwendet wurden wird verwiesen auf: Kirchner, Abkürzungsverzeichnis der Rechtssprache, Berlin 2008.

# J. Literaturverzeichnis


| | |
|---|---|
| *Abel, Ralf B.* | Mehr Datenschutz im Zivilrecht, RDV, 2009, 51–57. |
| *Ackermann, Frank/ Ivanov, Ivo* | Zwischen „OPT-IN“, „OPT-OUT“ und „NO-OPT“, DuD, 2005, 643–646. |
| *Adelsbach, Andre/ Gajek, Sebastian/ Schwenk, Jörg* | Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures, in: *Deng, Robert H. et al. (Hrsg.):* Information Security Practice and Experience: First International Conference, ISPEC 2005, Singapore, April 11-14, 2005, Berlin, Heidelberg, New York 2005, Lecture Notes in Computer Science, 204–217. |
| *Aigner, Dietmar/ Hofmann, Dietrich* | Fernabsatzrecht im Internet, München 2004. |
| *Albers, Marion* | Informationelle Selbstbestimmung, Baden-Baden 2005. |
| *Andexer, Frank/ Lehmann, Stefanie* | Datenschutzrechtliche Aspekte bei Online-Auktionen, in: *Hoeren, Thomas/Müglich, Andreas/Nielen, Michael (Hrsg.):* Online-Auktionen, Berlin 2002, Electronic Commerce und Recht, 185–236. |
| *Arlt, Christian* | Digital Rights Management-Systeme - Begriff, Funktion und rechtliche Rahmenbedingungen nach den jüngsten Änderungen des UrhG - insbesondere zum Verhältnis der §§ 95a ff. UrhG zum Zugangskontrolldiensteschutzgesetz (ZKDSG), GRUR, 2004, 548–554. |
| *Ders.* | Marktabschottend wirkender Einsatz von DRM-Technik - Eine Untersuchung aus wettbewerbsrechtlichem Blickwinkel, GRUR, 2005, 1003–1011. |
| *Bachmeier, Roland* | EG-Datenschutzrichtlinie - Rechtliche Konsequenzen für die Datenschutzpraxis, RDV, 1995, 49–57. |
| *Backu, Frieder* | Geolokalisation und Datenschutz, ITRB, 2009, 88–91. |
| *Ballhausen, Miriam/ Roggenkamp, Jan Dirk* | Personenbezogene Bewertungsplattformen, K&R, 2008, 403–410. |

| | |
|---|---|
| *Bauer, Stephan* | Personalisierte Werbung auf Social Community-Websites Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen, MMR, 2008, 435–438. |
| *Bechtold, Stefan* | Vom Urheber zum Informationsrecht - Implikationen des Digital Rights Management, München 2002. |
| *Bennett, John, Jr.* | The Digital Umbrella: Technology's Attack on Personal Privacy in America, Boca Raton, Florida 2004. |
| *Bergmann, Lutz/ Möhrle, Roland/ Herb, Armin (Hrsg.)* | Datenschutzrecht : Kommentar Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, bereichsspezifischer Datenschutz, München, Stuttgart Losebl.-Ausg., Stand: Januar 2009. |
| *Bestmann, Sylle* | Und wer muss zahlen? K & R, 2003, 496–502. |
| *Beucher, Klaus/ Leyendecker, Ludwig/ Rosenberg, Oliver von* | Mediengesetze (Rundfunk, Mediendienste, Teledienste), 2. Auflage. München 2005. |
| *Beuchler, Holger R.* | Das „Schreckgespenst" § 10 UWG: mehr Gespenst als Schrecken, WRP, 2006, 1288–1293. |
| *Beuthien, Volker/ Schmölz, Anton* | Persönlichkeitsschutz durch Persönlichkeitsgüterrechte, München 1999. |
| *Bierekoven, Christiane* | Die Neuregelung des Widerrufs- und Rückgaberechtes im Fernabsatz und E-Commerce, CR, 2008, 785–791. |
| *Ders.* | Internationaler Handel mit Kundendaten, ITRB, 2009, 39–41. |
| *Bizer, Johann* | Datenschutzrechtliche Informationspflichten, Dud, 2005, 454 ff.. |
| *Ders./ Grimm, Rüdiger/ Will, Andreas* | Privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management, DuD, 2006, 69–73. |
| *Bizer, Johann et al.* | Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2006 – Technischer Bericht. |
| *Ders./ Trosch, Daniel* | Die Anbieterkennzeichnung im Internet, Datenschutz und Datensicherheit, 1999, 621–627. |
| *Born, Christian* | Schadensersatz bei Datenschutzverstößen, Jur. Diss., Universität Münster, Münster 2001. |

| | |
|---|---|
| *Bräutigam, Peter/ Leupold, Andreas (Hrsg.)* | Online-Handel - Betriebswirtschaftliche und rechtliche Grundlagen, Einzelne Erscheinungsformen des E-Commerce, München 2003. |
| *Breidenbach, Stephan* | Die Voraussetzungen von Informationspflichten beim Vertragsabschluß, München 1989. |
| *Breinlinger, Astrid* | Abschaffung des Listenprivilegs - Zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, RDV, 2008, 223–227. |
| *Brinkel, Guido/ Lammers, Judith* | Innere Sicherheit auf Vorrat? ZUM, 2008, 11–22. |
| *Brox, Hans/ Walker, Wolf-Dietrich* | Allgemeines Schuldrecht, 33. Auflage. München 2009. |
| *Buchner, Benedikt* | Informationelle Selbstbestimmung im Privatrecht, München 2006. |
| *Bull, Hans Peter* | Verwaltung durch Maschinen - Rechtsprobleme der Technisierung der Verwaltung, Köln 1964. |
| *Ders.* | Aus aktuellem Anlaß - Bemerkungen über Stil und Technik der Datenschutzgesetzgebung, RDV, 1999, 148–153. |
| *Ders.* | Zweifelsfragen um die informationelle Selbstbestimmung - Datenschutz als Datenaskese? NJW, 2006, 1617–1624. |
| *Ders.* | Informationsrecht ohne Informationskultur? RDV, 2008, 47–55. |
| *Büllesbach, Alfred* | Das neue Bundesdatenschutzgesetz, NJW, 1991, 2593–2600. |
| *Busch, Jost-Dietrich* | Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts, DVBl, 1984, 385–389. |
| *Buxel, Holger* | Die sieben Kernprobleme des Online-Profiling aus Nutzerperspektive, DuD, 2001, 579–583. |
| *Canaris, Claus-Wilhelm* | Die Feststellung von Lücken im Gesetz, Berlin 1983. |
| *Ders.* | Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, in: *Ahrens, Hans-Jürgen et al. (Hrsg.):* Festschrift für Erwin Deutsch, Köln 1999, 85–109. |
| *Ders.* | Die Reform des Leistungsstörungsrechts, JZ, 2001, 499–524. |
| *Dambeck, Holger* | Die Adress-Schnüffler, Das Parlament, 2006, Nr. 34–35, 21.08.2006. |

| | |
|---|---|
| *Dammann, Ulrich/ Simitis, Spiros* | EG-Datenschutzrichtlinie, Baden-Baden 1997. |
| *Diedrich, Frank* | Schließt § 253 BGB den Ersatz immaterieller Personenschäden auch bei pVV und cic aus? MDR, 1994, 525– 529. |
| *Donnerhacke, Lutz/ Peter, Steffen* | Vorsicht, Falle! iX, 1997, 90. |
| *Eberle, Carl-Eugen* | Medien und Datenschutz – Antinomien und Antipathien, MMR, 2008, 508–513. |
| *Eckhardt, Jens* | Datenschutzrichtlinie für elektronische Kommunikation - Auswirkungen auf Werbung mittels elektronischer Post, MMR, 2003, 557–562. |
| *Ders.* | Datenschutz und Direktmarketing nach dem BDSG - Quo vadis, CR, 2009, 337–344. |
| *Ehmann, Eugen/ Helfrich, Marcus* | EG-Datenschutzrichtlinie, Köln 1999. |
| *Eichler, Alexander* | Cookies - verbotene Früchte? K&R, 1999, 76–81. |
| *Engel-Flechsig, Stefan/ Maennel, Frithjof A./ Tettenborn, Alexander* | Das neue Informations- und Kommunikationsdienste-Gesetz, NJW, 1997, S. 2981–2990. |
| *Dieselben* | Beck'scher IuKDG-Kommentar, München 2001. |
| *Engels, Stefan/ Eimterbäumer, Elke* | Sammeln und Nutzen von E-Mail-Adressen zu Werbezwecken, K&R, 1998, 196–200. |
| *Engels, Stefan/ Jürgens, Uwe/ Kleinschmidt, Katja* | Die Entwicklung des Telemedienrechts im Jahr 2007, K&R, 2008, 65 – 77. |
| *Engler, Tobias/ Kurzidim, Michael* | Geheimakte Logfile, c't, 2002, 124–147. |
| *Enzmann, Matthias/ Scholz, Philip* | Technisch-organisatorische Gestaltungsmöglichkeiten, in: *Roßnagel, Alexander (Hrsg.):* Datenschutz beim Online-Einkauf, Braunschweig, Wiesbaden 2002, 73–88. |
| *Erman, Walter* | Bürgerliches Gesetzbuch, Bd. 1, 12. Auflage. Köln 2008. |
| *Ernst, Stefan* | Abmahnungen auf Grund von Normen außerhalb des UWG, WRP, 2004, 1133–1137. |

| | |
|---|---|
| *Fikentscher, Wolfgang* | Wirtschaftsrecht, Band 2: Deutsches Wirtschaftsrecht, München 1983. |
| *Fox, Dirk* | Phishing, DuD, 2005, 365. |
| *Fröhle, Jens* | Web Advertising, Nutzerprofile und Teledienstedatenschutz, München 2003. |
| *Gärtner, Anette/ Heil, Ulf* | Kodifizierter Rechtsbruchtatbestand und Generalklausel - Zur Bedeutung des Marktbezugs im neuen UWG, WRP, 2005, 20–24. |
| *Gastroph, Bettina* | Dogmatik und Entwicklung der culpa in contrahendo, JA, 2000, 803–809. |
| *Geppert, Martin et al. (Hrsg.)* | Beck'scher TKG-Kommentar, 3. Auflage. München 2006. |
| *Gercke, Marco* | Die Strafbarkeit von Phishing und Identitätsdiebstahl, CR, 2005, 606–612. |
| *Gola, Peter/ Klug, Christoph* | Grundzüge des Datenschutzrechts, München 2003. |
| *Ders.* | Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung ", NJW, 2007, 2599–2602. |
| *Gola, Peter/ Müthlein, Thomas* | TDG/TDDSG - Kommentierung für die Praxis, Frechen 2000. |
| *Gola, Peter/ Reif, Yvette* | Datenschutzrelevante Aspekte des novellierten UWG, RDV, 2009, 104–112. |
| *Gola, Peter/ Schomerus, Rudolf* | Bundesdatenschutzgesetz, München 2007. |
| *Götting, Horst-Peter* | Persönlichkeitsrechte als Vermögensrechte, Tübingen 1995. |
| *Ders.* | Die Vererblichkeit der vermögenswerten Bestandteile des Persönlichkeitsrechts - ein Meilenstein in der Rechtsprechung des BGH, NJW, 2001, 585–587. |
| *Ders.* | Sanktionen bei Verletzung des postmortalen Persönlichkeitsrechts, GRUR, 2004, 801–808. |
| *Gounalakis, Georgios* | Der Mediendienste-Staatsvertrag der Länder, NJW, 1997, 2993–3000. |
| *Ders.* | Persönlichkeitsschutz und Geldersatz, AfP, 1998, 10–25. |
| *Ders./ Rhode, Lars* | Elektronische Kommunikationsangebote zwischen Telediensten, Mediendiensten und Rundfunk, CR, 2004, 487–492. |

| | |
|---|---|
| *Gounalakis, Georgios, Rhode Lars* | Persönlichkeitsschutz im Internet, München 2002. |
| *Graulich, Kurt* | Telekommunikationsgesetz und Vorratsdatenspeicherung, NVwZ, 2008, 485–492. |
| *Grentzenberg, Verena/ Schreibauer, Marcus/ Schuppert, Stefan* | Die Datenschutznovelle (Teil I), K&R, 2009, 368–375. |
| *Greve, Holger/ Schärdel, Florian* | Der digitale Pranger – Bewertungsportale im Internet, MMR, 2008, 644–650. |
| *Grigoleit, Hans Christoph* | Vorvertragliche Informationshaftung, München 1997. |
| *Ders.* | Besondere Vertriebsformen im BGB, NJW, 2002, 1151–1152. |
| *Grimm, Rüdiger et al.* | Privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management (Studie im Auftrag des Bundesministeriums für Bildung und Forschung), ⟨URL: `https://www.datenschutzzentrum.de/drm/`⟩. |
| *Ders./ Puchta, Stefan* | Datenspuren bei der Nutzung von Digital Rights Management-Systemen (DRM), DuD, 2006, 74–79. |
| *Gundermann, Lukas* | E-Commerce trotz oder durch Datenschutz? K & R, 2000, 225–235. |
| *Hahn, Oliver* | Data Warehousing und Data Mining in der Praxis, DuD, 2003, 605–608. |
| *Härting, Niko* | Datenschutz im Internet - Wo bleibt der Personenbezug? CR, 2008, 742–748. |
| *Ders.* | Schutz von IP-Adressen, ITRB, 2009, 35–39. |
| *Hase, Friedhelm* | Das Recht auf „informationelle Selbstbestimmung“, DuR, 1984, 39–47. |
| *Heil, Ulf* | Neues Wettbewerbsrecht - Wechselwirkungen zwischen UWG und Datenschutz, RDV, 2004, 205–211. |
| *Hillenbrand-Beck, Renate/ Greß, Sebastian* | Datengewinnung im Internet, DuD, 2001, 389–394. |
| *Hoenike, Mark/ Szodruch, Alexander* | Rechtsrahmen innovativer Zahlungssysteme für Multimediadienste, MMR, 2006, 519–526. |
| *Hoeren, Thomas* | Web-Cookies und das römische Recht, DuD, 1998, 455–456. |

| | |
|---|---|
| *Hoeren, Thomas* | Informationspflichten im Internet - im Lichte des neuen UWG, WM, 2004, 2461–2470. |
| *Ders.* | Das Telemediengesetz, NJW, 2007, 801–806. |
| *Ders.* | Entwurf des Bundesdatenschutzgesetzes: handwerklich misslungen, bank und markt, 2008, 32–34. |
| *Ders.* | Internet- und Kommunikationsrecht, Köln 2008. |
| *Ders.* | Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung - Konsequenzen für die Privatwirtschaft, JZ, 2008, 668–672. |
| *Ders.* | Die Vereinbarkeit der jüngsten BDSG-Novellierungspläne mit der Europäischen Datenschutzrichtlinie, RDV, 2009, 89–95. |
| *Ders./ Lütkemeier, Sven* | Unlauterer Wettbewerb durch Datenschutzverstöße, in: *Sokol, Bettina (Hrsg.):* Neue Instrumente im Datenschutz, Düsseldorf 1999, 107–123. |
| *Hoeren, Thomas/ Sieber, Ulrich (Hrsg.)* | Handbuch Multimedia Recht - Rechtsfragen des elektronischen Geschäftsverkehrs, München Losebl.-Ausg., Stand: Dezember 2008. |
| *Hofer, Marcus* | datenschutz@internet - Die Privatsphäre im Informationszeitalter, Wien 2002. |
| *Holznagel, Bernd/ Hoeren, Thomas* | Rechtliche Rahmenbedingungen des elektronischen Zahlungsverkehrs - Hemmnisse - Verletzungspotentiale - Haftung, Berlin 1999. |
| *Horn, Christian* | Verbraucherschutz bei Internetgeschäften, MMR, 2002, 209–214. |
| *Hufen, Friedhelm* | Das Volkszählungsurteil des Bundesverfassungsgerichs und das Grundrecht auf informationelle Selbstbestimmung - eine juristische Antwort auf „1984“? JZ, 1984, 1072–1078. |
| *Ihde, Rainer* | Cookies - Datenschutz als Rahmenbedingung der Internetökonomie, CR, 2000, 413–423. |
| *Janal, Ruth* | Sanktionen und Rechtsbehelfe bei der Verletzung verbraucherschützender Informations- und Dokumentationspflichten im elektronischen Geschäftsverkehr, Berlin 2003. |
| *Dies.* | Die Errichtung und der Zugang einer Erklärung in Textform gem. §126b BGB, MDR, 2006, 368–373. |

| | |
|---|---|
| *Jandt, Silke* | Das neue TMG - Nachbesserungsbedarf für den Datenschutz im Mehrpersonenverhältnis, MMR, 2006, 652–657. |
| *Jauernig, Othmar* | Bürgerliches Gesetzbuch, 12. Auflage. München 2007. |
| *Jotzo, Florian* | Gilt deutsches Datenschutzrecht auf für google, Facebook & Co. bei grenzüberschreitendem Datenverkehr? MMR, 2009, 232–237. |
| *Kastl, Karin* | Das allgemeine Persönlichkeitsrecht - Der Prozess seiner Anerkennung als „sonstiges Recht“im Sinne von §823 Abs. 1 BGB, Edelsbach 2004. |
| *Keilmann, Annette* | Vorsicht! - Zum Gehalt des §311 II, III BGB, JA, 2005, 500–504. |
| *Kilian, Wolfgang* | Informationelle Selbstbestimmung und Marktprozesse, CR, 2002, 921–929. |
| *Ders./ Heussen, Benno* | Computerrechts-Handbuch, München Losebl.-Ausg., Stand: Februar 2009. |
| *Knupfer, Jörg* | Phishing for Money, MMR, 2004, 641–642. |
| *Köcher, Jan* | Gesetzentwurf zum TMG - Erhebung von IP-Adressen zur Störungserkennung bald zulässig, MMR, 2009, V. |
| *Köhler, Helmut* | Der Schadensersatz-, Bereicherungs- und Auskunftsanspruch im Wettbewerbsrecht, NJW, 1992, 1477–1482. |
| *Ders./ Bornkamm, Joachim* | Gesetz gegen den unlauteren Wettbewerb, 27. Auflage. München 2009. |
| *Kraßer, Rudolf* | Schadensersatz für Verletzungen von gewerblichen Schutzrechten und Urheberrechten nach deutschem Recht, GRUR Int. 1980, 259–272. |
| *Kröger, Detlef / Gimmy, Marc (Hrsg.)* | Handbuch zum Internet-Recht - Electronic Commerce, Informations-, Kommunikations- und Mediendienste, 2. Auflage. Berlin, Heidelberg, New York 2002. |
| *Kröger, Detlef / Moos, Flemming* | Mediendienst oder Teledienst? AfP, 1997, 675–680. |
| *Krüger, Gerhard / Reschke, Dietrich* | Lehr- und Übungsbuch Telematik. Netze, Dienste, Protokolle, 3. Auflage. Leipzig 2004. |
| *Larenz, Karl / Canaris, Claus-Wilhelm* | Lehrbuch des Schuldrechts, Band II/2, Besonderer Teil, 13. Auflage. München 1994. |

| | |
|---|---|
| *Lazarakos, Grigirios G.* | Das datenschutzrechtliche Medienprivileg - Presseprivileg bei Multimediaanwendungen in Deutschland, Griechenland und Großbritannien unter dem Einfluß des Europarechts, Berlin 2003. |
| *Lettl, Tobias* | Allgemeines Persönlichkeitsrecht und Medienberichterstattung, WRP, 2005, 1045–1086. |
| *Leutheusser-Schnarrenberger, Sabine* | Vorratsdatenspeicherung - Ein vorprogrammierter Verfassungskonflikt, ZRP, 2007, 9–13. |
| *Lieb, Manfred* | Vertragsaufhebung oder Geldersatz? Überlegungen über die Rechtsfolgen von culpa in contrahendo, in: *Hirsch, Hans Joachim (Hrsg.):* Festschrift der Rechtswissenschaftlichen Fakultät zur 600-Jahr-Feier der Universität zu Köln, Köln u.a. 1988, 251 ff.. |
| *Lienemann, Gerhard* | TCP/IP-Grundlagen: Protokolle und Routing, 2. Auflage. Hannover 2000. |
| *Lorenz, Stephan* | Auskunftsansprüche im Bürgerlichen Recht, JuS, 1995, 569–575. |
| *Ders.* | Der Schutz vor dem unerwünschten Vertrag, München 1997. |
| *Mairgünther, Markus* | Die Regulierung von Inhalten in den Diensten des Internet, Berlin 2003. |
| *Manssen, Gerrit* | Telekommunikations- und Multimediarecht, Berlin Losebl.-Ausg., Stand: Februar 2008. |
| *Medicus, Dieter* | Bürgerliches Recht, 21. Auflage. Köln, Berlin, München 2007. |
| *Ders.* | Schuldrecht I - Allgemeiner Teil, 18. Auflage. München 2008. |
| *Meilinger, Franz* | Datenschutz im Bereich von Information und Dokumentation, Baden-Baden 1984. |
| *Meinel, Christoph/ Sack, Harald* | WWW - Kommunikation, Internetworking, Web-Technologien ; mit 106 Tabellen, Berlin 2004. |
| *Merati-Kashani, Jasmin* | Der Datenschutz im E-Commerce - Die rechtliche Bewertung der Erstellung von Nutzerprofilen durch Cookies, München 2005. |
| *Mertens, Bernd* | Die Rechtsfolgen einer Haftung aus culpa in contrahendo beim zustande gekommenen Vertrag nach neuem Recht, ZGS, 2004, 67–73. |

| | |
|---|---|
| *Meyer, Lena/ Mönig, Judith* | Die vertragstypologische Einordnung von Online-Auktionen, in: *Hoeren, Thomas/Müglich, Andreas/Nielen, Michael (Hrsg.):* Online-Auktionen, Berlin 2002, Electronic Commerce und Recht, 75–104. |
| *Meyer, Sebastian* | Cookies & Co. - Datenschutz und Wettbewerbsrecht, WRP, 2002, 1028–1035. |
| *Meyerdierks, Per* | Sind IP-Adressen personenbezogene Daten? MMR, 2009, 8–13. |
| *Mohrenfels, Peter Winkler von* | Abgeleitete Informationsleistungspflichten im deutschen Zivilrecht, Berlin 1986. |
| *Moos, Flemming* | Die Entwicklung des Datenschutzrechts im Jahr 2007, K&R, 2008, 137–145. |
| *Ders.* | Die Entwicklung des Datenschutzrechts im Jahr 2008, K&R, 2009, 154–161. |
| *Mückenberger, Ulrich* | Datenschutz als Verfassungsgebot, KJ, 1984, 1–24. |
| *Neuberger, Julius* | Der wettbewerbsrechtliche Gewinnabschöpfungsanspruch im europäischen Rechtsvergleich, Tübingen 2006. |
| *Niclas, Vilma* | Datenschutz als Werbevorteil - Gestaltung von Datenschutzhinweisen für Websites und Webshops, ITRB, 2008, 280–283. |
| *Ohlenburg, Anna* | Die neue EU-Datenschutzrichtlinie 2002/58/EG - Auswirkungen und Neuerungen für elektronische Kommunikation, MMR, 2003, 82–86. |
| *Ott, Stephan* | Datenschutzrechtliche Zulässigkeit von Webtracking? K&R, 2009, 308–313. |
| *Pahlen-Brandt, Ingrid* | Zur Personenbezogenheit von IP-Adressen, K&R, 2008, 288–290. |
| *Palandt, Otto* | Bürgerliches Gesetzbuch, 68. Auflage. München 2009. |
| *Peukert, Alexander* | Digital Rights Management und Urheberrecht, UFITA, 2002, 689–713. |
| *Piper, Henning/ Ohly, Ansgar* | Gesetz gegen den unlauteren Wettbewerb, 4. Auflage. München 2006. |
| *Pleister, Christian C. W./ Ruttig, Markus* | Neues Urheberrecht - neuer Kopierschutz - Anwendungsbereich und Durchsetzbarkeit des § 95a UrhG, MMR, 2003, 763–767. |

| | |
|---|---|
| *Podlech, Adalbert* | Prinzipien des Datenschutzes in der öffentlichen Verwaltung, in: *Kilian, Wolfgang/Lenk, Klaus/Steinmüller, Wilhelm (Hrsg.):* Datenschutz, Band 1, Frankfurt am Main 1973, 3–13. |
| *Powell, Thomas A./ Schneider, Fritz* | JavaScript 2.0: The Complete Reference, 2. Auflage. Sebastopol, California 2004. |
| *Prinz, Matthias* | Geldentschädigung bei Persönlichkeitsrechtsverletzungen durch Medien, NJW, 1996, 953–958. |
| *Ders./ Peters, Butz* | Medienrecht - Die zivilrechtlichen Ansprüche, München 1999. |
| *Redeker, Helmut* | Die Pflicht zur Vorratsdatenspeicherung, ITRB, 2009, 112–113. |
| *Rehm, Gebhard* | Aufklärungspflichten im Vertragsrecht, München 2003. |
| *Rieble, Volker* | Die Kodifikation der culpa in contrahendo, in: *Dauner-Lieb, Barbara/Konzen, Horst/Schmidt, Karsten (Hrsg.):* Das neue Schuldrecht in der Praxis, Köln 2003, 137–157. |
| *Roessler, Thomas* | WHOIS: Datenschutz im DNS? DuD, 2002, 666–671. |
| *Rönnau, Thomas/ Faust, Florian/ Fehling, Michael* | Durchblick: Kausalität und objektive Zurechnung, JuS, 2004, 113–118. |
| *Rosenbaum, Oliver* | Online Lexikon, Feldkirchen 1996. |
| *Roßnagel, Alexander* | Neues Recht für Multimediadienste, Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag, NVwZ, 1998, 1–8. |
| *Ders.* | Handbuch Datenschutzrecht, München 2003. |
| *Ders.* | Recht der Multimedia-Dienste, München Losebl.-Ausg., Stand: April 2005. |
| *Ders./ Banzhaf, Jürgen/ Grimm, Rüdiger* | Datenschutz im Electronic Commerce. Technik - Recht - Praxis, Heidelberg 2003. |
| *Roßnagel, Alexander/ Pfitzmann, Andreas/ Garstka, Hansjürgen* | Modernisierung des Datenschutzrechts, Berlin 2001, Gutachten im Auftrag des Bundesministerium des Inneren. |

| | |
|---|---|
| *Roßnagel, Alexander/ Scholz, Philip* | Datenschutz durch Anonymität und Pseudonymität - Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR, 2000, Nr. 12, 721–731. |
| *Rötzer, Florian* | Nach den Cookies die Web Bugs, TP 1999. |
| *Säcker, Franz Jürgen/ Rixecker, Roland (Hrsg.)* | Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 5, 4. Auflage. München 2004. |
| *Ders.* | Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 1. Halbband, 5. Auflage. München 2006. |
| *Ders.* | Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2, 5. Auflage. München 2007. |
| *Sattler, Karl-Otto* | Bürger unter Generalverdacht, Das Parlament, 2005, Nr. 51–52, 19.12.2005. |
| *Schaar, Peter* | Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, DuD, 2000, 275–277. |
| *Ders.* | Datenschutzrechtliche Einwilligung im Internet, MMR, 2001, 644–648. |
| *Ders.* | Persönlichkeitsprofile im Internet, DuD, 2001, 383–388. |
| *Ders.* | Datenschutz im Internet - Die Grundlagen, München 2002. |
| *Schaffland, Hans-Jürgen/ Wiltfang, Noeme* | Bundesdatenschutzgesetz, Berlin Losebl.-Ausg., Stnad: Februar 2009. |
| *Schlechtriem, Peter* | Schuldrecht Allgemeiner Teil, 6. Auflage. Tübingen 2005. |
| *Schleipfer, Stefan* | Datenschutzgerechte Gestaltung von Web-Eingabeformularen, RDV, 2005, 56–61. |
| *Ders.* | Nutzungsprofile unter Pseudonym - Die datenschutzrechtlichen Bestimmungen und ihre Anwendung im Internet, RDV, 2008, 143–150. |
| *Schmitz, Dirk* | Vertragliche Haftung bei unentgeltlichem Informationserwerb via Internet, MMR, 2000, 396–399. |
| *Schmitz, Peter* | Übersicht über die Neuregelung des TMG und des RStV, K&R, 2007, 135–138. |
| *Ders./ Eckhardt, Jens* | AGB - Einwilligung in Werbung, CR, 2006, 533–539. |
| *Schneider, Jochen* | EG-Richtlinie zum Datenschutz, CR, 1993, 35–39. |

| | |
|---|---|
| *Schneider, Jochen* | Handbuch des EDV-Rechts, 4. Auflage. Köln 2009. |
| *Scholz, Philip* | Datenschutzrechtliche Anforderungen, in: *Roßnagel, Alexander (Hrsg.):* Datenschutz beim Online-Einkauf, Baden-Baden 2002, 41–72. |
| *Ders.* | Datenschutz beim Internet-Einkauf, Baden-Baden 2003. |
| *Schwiderski-Grosche, Scarlet* | Proxy-Cache-Server, DuD, 1999, 586–590. |
| *Selk, Robert* | Datenschutz und Internet, Dissertation Universität Augsburg, Osnabrück 2003. |
| *Simitis, Spiros* | Datenschutz: Von der legislativen Entscheidung zur richterlichen Interpretation, NJW, 1981, 1697–1701. |
| *Ders.* | Bundesdatenschutzgesetz, 6. Auflage. Baden-Baden 2006. |
| *Simon, Jürgen/ Taeger, Jürgen* | Umfang des Auskunftsanspruchs gegen Handelsauskunfteien - BGH, NJW 1981, 1738, JuS, 1983, 96–101. |
| *Skoudis, Ed/ Zeltser, Lenny* | Malware: Fightung Malicious Code, Upper Saddle River, New Jersey 2004. |
| *Spielkamp, Matthias* | Das Radikale Maximum, brand eins, 2004, Nr. 9, 70–77. |
| *Spindler, Gerald* | Das neue Telemediengesetz - Konvergenz in sachten Schritten, CR, 2007, 239–245. |
| *Ders./ Schuster, Fabian* | Recht der elektronischen Medien, München 2008. |
| *Spindler, Gerald/ Wiebe, Andreas* | Internet-Auktionen, Köln 2005. |
| *Staudinger, Julius von* | Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Art. 219-245 EGBGB, 14. Auflage. Berlin 2003. |
| *Ders.* | Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, 2. Band, Recht der Schuldverhältnisse, §§ 249-254, 14. Auflage. Berlin 2005. |
| *Ders.* | Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, 2. Band, Recht der Schuldverhältnisse, §§ 311, 311a, 312, 312a-f, Neubearbeitung 2005, 15. Auflage. Berlin 2005. |

*Steffen, Erich* Schmerzensgeld bei Persönlichkeitsverletzung durch Medien - Ein Plädoyer gegen formelhafte Berechnungsmethoden bei der Geldentschädigung, NJW, 1997, 10–14.

*Stoll, Hans* Schädigung durch Vertragsschluss, in: Festschrift für Erwin Deutsch, Köln 1999, 361–373.

*Stürner, Rolf* Die Aufklärungspflicht der Parteien des Zivilprozesses, Tübingen 1976.

*Taeger, Jürgen* Kundenprofile im Internet, K&R, 2003, 220–227.

*Tinnefeld, Marie-Theres* Die Novellierung des BDSG im Zeichen des Gemeinschaftsrechts, NJW, 2001, 3078–3083.

*Dies./ Ehmann, Eugen/ Gerling, Rainer W.* Einführung in das Datenschutzrecht, 4. Auflage. München, Wien 2005.

*Tobias, Müller.* Vererblichkeit vermögenswerter Bestandteile des Persönlichkeitsrechts - Die neueste Rechtsprechung des BGH zum postmortalen Persönlichkeitsrecht, GRUR, 2003, 31–34.

*Ullmann, Eike* Caroline v., Marlene D., Eheleute M. - ein fast geschlossener Kreis, WRP, 2000, 1049–1054.

*Ultsch, Michael* Zugangsprobleme bei elektronischen Willenserklärungen - Dargestellt am Beispiel der Electronic Mail, NJW, 1997, 3007–3009.

*Voigt, Paul* Datenschutz bei Google, MMR, 2009, 377–382.

*Von Lewinski, Kai* Privacy Policies: Unterrichtungen und Einwilligung im Internet, DuD, 2002, 395–400.

*vzbv* Verbraucherschutz: Recht harmlos? - Verbandsklage auf dem Prüfstand (Redebeiträge), ⟨URL: `http://www.vzbv.de/go/dokumente/507/1/1/`⟩.

*Wagner, Gerhard* Prominente und Normalbürger im Recht der Persönlichkeitsverletzungen, VersR, 2000, 1305–1310.

*Ders.* Das Zweite Schadensersatzrechtsänderungsgesetz, NJW, 2002, 2049–2064.

*Waldenberger, Arthur* Teledienste, Mediendienste und die „Verantwortlichkeit“ ihrer Anbieter, MMR, 1998, 124–129.

*Wang, Wallace* Steal this Computer Book 4.0, 4. Auflage. Heidelberg 2006.

| | |
|---|---|
| *Weichert, Thilo* | Datenschutzrechtliche Probleme beim Adressenhandel, WRP, 1996, 522–534. |
| *Ders.* | Datenschutzstrafrecht - ein zahnloser Tiger? NStZ, 1999, 490–493. |
| *Ders.* | Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW, 2001, 1463–1469. |
| *Ders.* | Datenschutz im Wettbewerbs- und Verbraucherrecht, VuR, 2006, 377–383. |
| *Ders.* | BDSG-Novelle zum Schutz von Internet-Inhaltsdaten, DuD, 2009, 7–18. |
| *Weißnicht, Elmar* | Die Nutzung des Internet am Arbeitsplatz, MMR, 2003, 448–453. |
| *Werner, Stefan* | Geldverkehr im Internet, Heidelberg 2002. |
| *Westphal, Dietrich* | Die neue EG-Richtlinie zur Vorratsdatenspeicherung - Privatsphäre und Unternehmerfreiheit unter Sicherheitsdruck, EuZW, 2006, 555–560. |
| *Wohlgemuth, Hans H.* | Datenschutzrecht - Eine Einführung mit praktischen Fällen, Neuwied u.a. 2005. |
| *Wolber, Tanja* | Zulässigkeit der Werbung mit Adressen aus Online-Bestellungen, DSB, 2003, 16–18. |
| *Zscherpe, Kerstin* | Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR, 2004, 723–727. |
| *Dies.* | Datenschutzrechtliche Website-Kontrollen durch die Aufsichtsbehörde, MMR, 2004, XVII–XVIII. |
| *Dies.* | Datenschutz im Internet - Grundsätze und Gestaltungsmöglichkeiten für Datenschutzerklärungen, K & R, 2005, 264–269. |