Jahrbuch des Umwelt- und Technikrechts 2003

Redaktion:
Professor Dr. Meinhard Schröder

ERICH SCHMIDT VERLAG

Inhalt

I. Abhandlungen

II. Bericht

Cyberlaw – eine neue Disziplin im Recht?

Viola Schmid

Übersicht

b) Cyberspace
c) Cybergovernance
(1) Gubernative, Adminstrative, Judikative, Legislative
(2) Technizität
2. Cross-Border-Sachverhalte und -Personen
a) Begriff
b) Methodische Herausforderung
3. Zukunftsoptionen: Konservatismus- und Erneuerungsthese
4. Zukunftsoptionen: Kommerzialisierung des Cyberspace

I. Cyberlaw: eine Vorbemerkung zur Methode und Vorgehensweise

Dieser Beitrag versucht ein (neues) „Rechtsgebiet" bekannter zu machen. Der Umfang und die Thematik des Beitrags bedingen eine Einschränkung des Anspruchs auf Vollständigkeit und verlangen eine Modifizierung der Präsentation, der Recherche und der Zitierweise. Methodisch steht nicht die Lösung von Problemen, sondern die Darstellung der Herausforderungen an das Cyberlaw im Mittelpunkt.

II. „Cyberlaw" oder „Cyber Law" in einer orthographischen Betrachtung

Bei der Rechtschreibung stellt sich die Frage nach der Trennung beider Begriffe oder der Vereinigung in einem zusammengesetzten Substantiv: „Cyber Law"[1] und/oder „Cyberlaw"[2] werden verwandt. Für die Trennung beider Begriffe spricht, dass „Cyber" und „Law" durchaus in einem antagonistischen Verhältnis stehen können und die Ausdifferenzierung dieses Verhältnisses nicht auf der Definitionsebene vorweggenommen werden sollte.

1 So das angelsächsische „Cyber Law Centre", http://www.cyberlawcentre.org.uk/mapindex.html (28.02.2003).

2 *A. Schwerdtfeger*, Cyberlaw, 1999; Berkman Center an der Harvard Law School, http://cyber.law.harvard.edu/ilaw (28.02.2003).

Für die Vereinigung in einem zusammengesetzten Substantiv spricht, dass potentielle „Regelungsobjekte" des Cyberlaw wie etwa Cyberspace[3], Cyberworld[4], Cyberwar[5] und Cyberpublic überwiegend[6] in zusammengesetzten Substantiven verwandt werden.

Des Weiteren stellt sich die Frage, warum ein Anglizismus gewählt wird: Warum soll dieses „Rechtsgebiet" (quod erit demonstrandum) nicht „Cyberrecht", sondern „Cyberlaw" heißen? Die letztere Benennung kann man mit der Entstehungsgeschichte des Internet, der Hardware (etwa Computer), der Software (etwa Betriebs- und Anwendungssysteme) und des Cyberlaw begründen. Dass Computer und Software von privaten US-amerikanischen Unternehmen und Staatsangehörigen (statt vieler IBM und Bill Gates) entwickelt wurden, ist banales Alltagswissen. Auch die Entstehung des Internet ist das Ergebnis eines amerikanischen, wenn auch eines staatlichen Projekts. In den Zeiten des „kalten Krieges" sollten nach der Vorstellung des Verteidigungsministeriums Datentransfers selbst im Falle eines Nuklearschlages möglich und möglichst sicher sein.[7] Die am 7. Januar 1958 gegründete Advanced Research Projects Agency (ARPA)[8] schuf in der Folge das erste „Internet". Dieses sogenannte ARPAnet verband 1971 nur 23 „Militärcomputer".[9] Später wurde das ARPAnet an ein weiteres Verbindungsnetz angeschlossen, nämlich das von der National Science Foundation (NSF) geförderte, sogenannte NSFnet. In Europa wurde zunächst in Dänemark, Schweden, den Niederlanden und in Großbritannien das so genannte EUnet (European Unix Network) etabliert. In der Bundesrepublik erfolgte 1986 die Aufspannung des EUnet an der Universität Dortmund[10] und 1989 der Anschluss an das amerikanische NSFnet.[11] Über 30 Jahre später haben nach Ermittlung

3 *B. Großfeld/J. Hoeltzenbein*, Global Powers: International Aspects of Cyberspace Patents, K&R 2003, 1.

4 *T. L. Kunii*, Cyberworlds, 1998.

5 Etwa: The Great Cyberwar of 2002, http://www.wired.com/wired/archive/6.02/cyberwar.html?topic=hacking_warez &topic_set=newtechnology (28.02.2003).

6 *V. Boehme-Neßler*, CyberLaw Lehrbuch zum Internetrecht, 2001: „CyberLaw"; *M. Kloepfer*, Informationsrecht, 2002: „Cyber-War" (§ 1 Rn. 43).

7 *H.-J. Teuteberg*, Strukturmerkmale multimedialer Revolutionierung von Wirtschaft, Gesellschaft und Kultur an der Wende zum 21. Jahrhundert, in: H.-J. Teuteberg und C. Neutsch (Hrsg.), Vom Flügeltelegraphen zum Internet: Geschichte der modernen Telekommunikation, 1998, S. 317.

8 *L. Determann*, Kommunikationsfreiheit im Internet, 1999, S. 40 ff.

9 *T. Hoeren*, Grundzüge des Internetrechts, 2002, S. 9.

10 Einen Überblick über die Entwicklung in Deutschland gibt, http://www.uunet.de/ 2/s1.asp (28.02.2003).

11 Einen Überblick über die Entwicklung gibt, http://www.uunet.de/2/s1.asp (28.02.2003).

der Nielsen/Netrating[12] – einer auf die Ermittlung von (Online-) Werbemärkten spezialisierten und eingeführten Agentur – 2003 weltweit 580 Millionen Personen Zugang zum Internet. Das bedeutet nicht, dass diese 580 Millionen Menschen selbst einen Computer haben, sondern vielmehr dass sie Zugang zum Netz haben. Darüber hinaus sollen in Deutschland 35,6 Millionen Menschen (also fast die Hälfte der Bevölkerung) über einen eigenen Home PC (Personal Computer) verfügen und damit an das Netz angeschlossen sein. Diese Computer sollen es 63 % der deutschen Bevölkerung (79% der US-amerikanischen Bevölkerung) ermöglichen, im Netz zu surfen und zu handeln. Im E-Commerce (Electronic Commerce) soll Deutschland weltweit einen Spitzenplatz einnehmen.[13]

Neben der Entstehungsgeschichte des Cyberspace spricht auch die Entwicklung des Cyberlaw für die Anglizierung. Das Cyberlaw wurde und wird, wie das frühere Common Law, in weiten Teilen durch die Rechtsprechung und weniger durch den normativ agierenden Verfassungs- und Gesetzgeber geschaffen.[14] Das Cyberlaw muss sich seine rechtlichen (normativen) Strukturen erst noch erarbeiten – vorläufig bleibt es bei einem eher tentativen und topischen Vorgehen der Rechtsprechung (siehe zum fragmentarischen Charakter unter III. 2. b) (3) wie der beteiligten Verkehrskreise (siehe zur Forderung nach regulierter Selbstregulierung IV. 3.). Festzuhalten ist, dass die Wiege des „Cyberspace" und des „Cyberlaw" in den Vereinigten Staaten stand und steht. Die (aktuellen) Rechts- und Technikentwicklungen, die dort stattfinden, sind von elementarem Interesse für das „deutsche" Cyberlaw. Die Forderung *Peter Häberles*[15], den Auslegungskanon von *Friedrich Carl von Savigny* um die Rechtsvergleichung zu erweitern, ist für das Cyberlaw demzufolge Selbstverständlichkeit.

[12] Nielsen/Netratings Press Releases v. 20.02.2003, Global Internet Population Grows An Average of Four Percent Year-Over-Year, http://www.nielsen-netratings.com/pr/pr_030220.pdf (28.02.2003).

[13] FAZ v. 24.02.2003, S. 18, „Deutschland führt Weltrangliste im E-Commerce an" berichtet über eine Untersuchung des Weltwirtschaftsforums.

[14] Dafür gibt es territoriale Gründe („Globalität des Internets") und strukturelle Gründe (siehe die Diskussion um die Freiheit vor dem Recht im Internet unter IV. 3.

[15] Von einer „fünften" Auslegungsmethode spricht *P. Häberle*, in: „Der Verfassungsstaat als Glied einer Europäischen Gemeinschaft", VVDStRL 50 (1990), S. 157.

III. Cyberlaw in einer disziplinären Betrachtung

Hier soll keine in die Vergangenheit blickende Betrachtung zur Sinnhaftig- oder Sinnlosigkeit von disziplinärem Denken in der Rechtswissenschaft erfolgen, sondern pragmatisch gefragt werden,

- welche Kriterien die Annahme rechtfertigen, dass eine Disziplin sich in statu nascendi befindet oder entstanden ist und
- welche Charakteristika es rechtfertigen, das Cyberlaw als eigene Disziplin zu qualifizieren.

Im Rahmen dieses Beitrags wird der Begriff „Disziplin" gegenüber den Bezeichnungen „Rechtsgebiet" und „Wissenschaftszweig" bevorzugt, weil Cyberlaw eine transdisziplinäre Methodik verlangt, die mit den abgegrenzten Vorstellungen über ein „Gebiet" oder einen „Zweig" schlechter vereinbar ist.[16]

1. Wie entsteht eine Disziplin?

Michael Stolleis nennt den Diskurs derjenigen, „die an einem wissenschaftlichen, im engeren Sinne universitären Diskurs teilnehmen und ihm die Richtung geben" als Entstehungsgrund eines neuen Wissenschaftszweigs.[17] Die Staatsrechtslehrertagung hat sich bisher nur einmal mit dem Informationsrecht – aber nur am Rande mit dem Internet oder dem Cyberspace – befasst.[18] Eher könnte ein Anzeichen für eine Richtungsvorgabe beim deutschen Juristentag erkannt werden, der eine viel Interesse findende Abteilung „Medienrecht" eingerichtet hat.[19] Der Diskurs über Cyberlaw findet nicht nur an den rechtswissenschaftlichen Fakultäten[20], sondern auch an Fach-

[16] Hier wird der Begriff „Disziplin" auch deshalb bevorzugt, weil es sich nicht nur um einen Wissenschaftszweig handelt, sondern auch um ein Tätigkeitsgebiet für Juristen (Rechtsanwälte, Synidici). Andere verwenden den Begriff „Rechtsgebiet" wie *Kloepfer* (Fn. 6), § 1 Rn. 80 „Konstituierung des Informationsrechts als Rechtsgebiet".

[17] *M. Stolleis*, Wie entsteht ein Wissenschaftszweig? Wirtschaftsrecht und Wirtschaftsverwaltungsrecht nach dem Ersten Weltkrieg, in: H. Bauer/D. Czybulka/W. Kahl/A. Voßkuhle, Umwelt, Wirtschaft und Recht: Wissenschaftliches Symposium aus Anlass des 65. Geburtstages von Reiner Schmidt, 2002, S. 12.

[18] *F. Schoch/H.-H. Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998).

[19] http://www.djt.de/content/aktuell/programm.phtml?F=1 (28.02.2003).

[20] Etwa Institut für Informations-, Telekommunikations- und Medienrecht (ITM) der Universität Münster mit einer zivilrechtlichen und öffentlich-rechtlichen Abteilung, Institut für

hochschulen[21] und Technischen Universitäten statt. Auch die weiteren Kriterien, die *Michael Stolleis* für das Entstehen eines Wissenschaftszweiges nennt, sind erfüllt. Es gibt Vorlesungen zum Informations- und Datenschutzrecht, es gibt Prüfungen, es existiert eine Lehrbuchkultur[22] und es existieren Zeitschriften[23]. Darüber hinaus fördern Ministerien Projekte etwa zur „Internetökonomie" (Forschungsförderung) und fragen Gutachten zu Cyberlawsachverhalten in der Rechtswissenschaft nach (etwa zur Novelle des Urheberrechtsgesetzes [24] oder die Machbarkeitsstudie für biometrische Merkmale, die zur Authentifizierung und Identifizierung der Autoren elektronischer Dokumente benutzt werden könnten[25]).

2. Warum entsteht eine Disziplin?

Michael Stolleis nennt zwei Gründe für das Entstehen neuer Wissenschaftszweige: zum einen den Einfluss realer Gegebenheiten auf das Recht[26] (in Abwandlung einer berühmten Formel: die Wissen verlangende Kraft des Faktischen) und zum anderen einen Wandel in der juristischen Methode. Beide Argumente treffen für das Cyberlaw zu.

a) Veränderungen der (Rechts-)Tatsachen

Das Internet ist ein Publikationsmedium, das wegen seiner Reichweite (580 Millionen), Individualität (siehe zur Intimisierung des Internets unter IV. 2. a)) und relativen Kostengünstigkeit (Flatrate, die eine ständige Verbindung ermöglicht) einen weiteren Raum für die Verwirklichung von Freiheit schafft. Die Kommunikation via E-Mail und der Zugriff auf wie die Zurverfügungstellung von Daten in einem Intranet – etwa über eine Software wie

Rechtsinformatik der Universität Saarbrücken, Institut für das Recht der Informations- und Kommunikationstechnik der Humboldt Universität Berlin; weitere Beispiele bei *Hoeren* (Fn. 9), S.7 und *Kloepfer* (Fn. 6), § 1 Rn 81.

21 Etwa das Synergieprojekt an der Fachhochschule Bielefeld, http://www.uni-protokolle.de/nachrichten/id/3798/ (28.02.2003).

22 Übersicht bei *Kloepfer* (Fn. 6), § 1 Rn. 83f.

23 Computer & Recht (CR); Kommunikation & Recht (K&R); MultiMedia und Recht (MMR); Telekommunikations- & MedienRecht (TKMR).

24 http://www.heise.de/newsticker/data/jk-17.01.03-000/ (28.02.2003), wo die faktische Entwertung des Rechts auf Privatkopie aus verfassungsrechtlichen Gründen (Art. 5 Abs. 1 S. 1 2. Alt. GG) kritisiert wird.

25 http://www.heise.de/newsticker/data/pmz-16.12.02-000/ (28.02.2003).

26 *Stolleis* (Fn. 17), S.7 zu den Themen der „Freirechtler"; S. 3 zu technischer und sozialer Innovation.

R3 von SAP[27] – verändern die (Arbeits-)Welt. E-Mail macht den Postkasten, die Postboten und die Postfahrzeuge entbehrlich. Die Kommunikation mit Attachments (Fotos, Filmen und Texten) ist nicht mehr zeitversetzt, sondern für die Kommunikatoren und Rezipienten, die online sind, fast in Echtzeit organisier-[28] und realisierbar. Die „Organisation"[29] von Daten in einem Intranet stellt bisherige (Informations-)Hierarchien auf den Prüfstand, wie ein Praxisbeispiel verdeutlicht. So ist etwa der R3-systemimplementierende Informatiker bei einem Krankenhaus mit der Frage konfrontiert, ob beide Chefärzte durch das Programm in die Lage versetzt werden sollen, Einsicht in den Operationsplan des jeweils anderen Kollegen zu erhalten. Diese „Öffentlichkeit" entspräche einer effizienten und patientenwohlorientierten zukünftigen Praxis – nicht aber der Praxis, die bisher praktiziert wurde. Mit diesem Beispiel wird deutlich, dass Experten-, Eliten-, und Nischenwissen nicht mehr ohne weiteres (mit Hilfe der (Chef-)Sekretärin) in Aktenschränken weggeschlossen werden kann. Wenn solche (Nicht-)Informationsstrategien weiter verfolgt werden sollen, gerät der reservatsinteressierte Chefarzt zumindest gegenüber dem (externen) Informatiker[30] in eine Argumentationsposition und -situation. Die Implementierung einer solchen Software verpflichtet also zur Offenlegung von (Informations-) hierarchien und -strategien und bietet die Chance der Reflexion, Transparenz und Korrektur. Und für das (Beamten-)Recht stellt sich die Frage, mit welchen Sanktionen auf subversive Informationsstrategien[31] von „Arbeitnehmern im weitesten und untechnischen Sinne" zu reagieren ist (Abmahnung, Disziplinarrecht, ...).

27 Systeme Anwendungen Programmierung.

28 Etwa wenn das E-Mail-Programm eingehende Mails während anderer Anwendungen bekannt gibt.

29 „Organisation" wird hier als Oberbegriff für die im Datenschutzrecht geltenden Definitionen des Erhebens, des Verarbeitens und des Nutzens (§ 3 Abs. 3- 5 BDSG) verwandt.

30 Hier zeigt sich auch die Bedeutung der juristischen Ausbildung dieser „Technikwissenschaftler", deren Handlungssicherheit erhöht werden soll. Andernfalls drohen diese sach- und personenwohlfremden Informationsstrategien zu einer Verschlechterung des SAP-Systems zu führen.

31 Diese Nichtinformationsstrategien sind – weil die Technik mehr Informationsangebote erlauben würde – evident und nachweisbar. Siehe aber zum Folgeproblem, nämlich der Dokumentenflut FAZ v. 18.02.2003, S. 18 „Unternehmen versinken in der Dokumentenflut".

b) *Veränderung der Methodenlehre*

Das verhältnismäßig junge[32] Cyberlaw kann sich auch auf den zweiten Entstehungsgrund, nämlich die Notwendigkeit von Differenzierungen der juristischen Methode, berufen. Hier lassen sich fünf Aspekte unterscheiden.

(1) Solo- und Multidisziplinarität

Dass „junge" Disziplinen solo- und/oder multidisziplinär sind, ist wegen der fehlenden Breite der Rechtsprechung,[33] der (vielleicht) fehlenden Tiefe der Durchdringung der Probleme in der Literatur (aufgrund anfangs weniger und in diesem „Rechtsgebiet" weniger erfahrener Diskursteilnehmer)[34] und wegen der anfänglich fehlenden Breite des „Rechtsgebiets" erklärbar. Mit Solodisziplinarität wird hier der Befund beschrieben, dass sich unterschiedliche Disziplinen parallel für die Herausforderungen eines „Rechtsgebiets" interessieren und dann wegen der Komplexität und Vernetzung der Sachverhalte auch mit Fragestellungen befassen, die in einer überkommenen Betrachtung zu anderen Disziplinen gehören.[35] Ein Beispiel ist das Gemeinschaftsrecht, das in seinen Anfängen solo- und multisdisziplinär war und sich erst im Laufe der Zeit und mit der Schaffung des Sekundärrechts etwa in europäisches Agrar-, „Verfassungs-"[36], Arbeits-, Umwelt- und Zivilrecht ausdifferenziert hat. Das Cyberlaw ist – und das ist in dieser Kombination ungewöhnlich – bereits jetzt eine Querschnittsmaterie aus „Zivil-"[37], Straf- und Öffentlichem Recht. Diese Solo- und Multidisziplinarität zeigt sich auch in *Michael Kloepfers* Lehrbuch zum „Informationsrecht", das neben den traditionellen medienrechtlichen Themen[38] Kapitel, die mit „Informationszivilrecht" und mit „Informationsstraf- und -ordnungswidrigkeitenrecht"[39] überschrieben sind, enthält. Personal lässt sich die Multidisziplinarität des Rechtsgebiets anhand der Entwicklung etwa des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster verdeutlichen, das eine zivilrechtliche und eine öffentlichrechtliche Abteilung kennt.[40]

Für einige Themenbereiche des Cyberlaw scheint es einen Wettbewerb der Rechtsdisziplinen um die „beste Lösung" zu geben. Ein Beispiel ist die Convention on Cybercrime (CCC) [41] – ein völkerrechtliches Übereinkommen des Europarats – die den Mitgliedstaaten zivil-, straf- und öffentlichrechtliche Umsetzungsmodalitäten offen lässt.[42] Inhaltlich befasst sich die CCC mit drei zentralen Aspekten des Cyberspace: Zum einen der „Organisation" von Daten zum Zweck der (inter-)nationalen Strafverfolgung (Art. 20f. CCC); zum zweiten dem Schutz der „Organisation" und des „Transfers" von Daten vor Angriffen (Art. 2ff. CCC) und zum dritten der Prävention und Sanktion der Kinderpornographie im Internet (Art. 9 CCC).

Mit diesem Beispiel soll nicht angedeutet oder untersucht werden, dass und ob die drei Disziplinen bisher gleichen Anteil an den rechtlichen Regelungsoptionen des Cyberspace hätten. Eine solche Evaluation wäre zum einen wenig weiterführend und methodisch zu komplex für diesen Beitrag. Cum grano salis lässt sich festhalten, dass weniger die ex-ante Regulierungsoptionen des öffentlichen Rechts,[43] das sehr schnell auf territoriale Grenzen (und Umgehungslösungen) treffen würde[44], genutzt werden, son-

---

32 Bereits die Anfänge dieses Rechtsgebiets zu terminieren, fällt schwer. Für den deutschen Raum kann vor 1986 nicht von relevanten (Rechts-)Tatsachen ausgegangen werden.

33 Heute würde eine Arbeit über die allgmeinen Rechtsgrundsätze quantitativ einen anderen Umfang einnehmen als *H. Lecheler*, Der Europäische Gerichtshof und die allgemeinen Rechtsgrundsätze, 1971, S. 56 ff.

34 Hier sollen keine Qualitätskriterien angelegt werden. Die Chance auf eine breite und tiefe Diskussion der Chancen und Herausforderungen einer Technik wächst jedenfalls zumindest statistisch mit der Anzahl der Diskursteilnehmer.

35 Ein späteres Beispiel ist die TCPA-Problematik, bei der urheberrechtliche Fragen des Digital Rights Managments mit den in der Verfassung gewährleisteten Eigentums- und Datenschutzrechten des Surfers in untrennbarem Zusammenhang stehen.

36 Siehe nunmehr die Beratungen des europäischen Verfassungskonvents.

37 „Zivilrecht" soll hier sehr weit verstanden werden und auch das Urheber- und Patentrecht umfassen.

38 *Kloepfer* (Fn. 6) § 8 Datenschutzrecht, § 10 Informationszugangsrecht, § 11 Telekommunikationsrecht, § 12 Postrecht, § 13 Recht der elektronischen Informations- und Kommunikationsdienste, § 14 Rundfunkrecht, § 15 Presserecht.

39 *Kloepfer* (Fn. 6) §7 Informationsstraf- und ordnungswidrigkeitenrecht.

40 http://www.uni-muenster.de/Jura.itm/ie.html (28.02.2003).

41 Überblick: *D. Kugelmann*, Völkerrechtlich Mindeststandards für die Strafverfolgung im Cyberspace, TMR 2002, 14ff.; Diese Konvention des Europarats (42 Konventionsstaaten) verspricht Bedeutung zu erlangen, weil auch die USA, die einen anderen kulturellen Umgang mit „free speech" pflegen, die Konvention ratifiziert haben.

42 Art. 12 Absatz 3 CCC: Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

43 Hypothetisch: ein öffentlichrechtliches Anzeigeverfahren für die Eröffnung einer Homepage mit Bekanntgabe des Verantwortlichen.

44 *J. A. Graham*, Der virtuelle Raum – sein völkerrechtlicher Status, Abs. 20, http://www.jurpc.de/aufsatz/19990035.htm (28.02.2003), zu so genannten „Mirror-Sites" die, wenn der deutsche Staat im „deutschen Internet" Inhalte untersagen würde, in anderen Teilen der Welt entstünden.

dern auf die ex-post Sanktionierung durch das Strafrecht[45] und das (zivile) Haftungsrecht[46] rekurriert wird.

Inhaltlich ist die Nähe der drei traditionellen Disziplinen im Cyberlaw durch das hohe staatliche Sanktionsinteresse erklärbar. Wenn eine Rechtsordnung sich für eine bestimmte Handhabung der Meinungsfreiheit entscheidet, dann will sie mit allen Einwirkungsmöglichkeiten der drei Disziplinen verhindern, dass diese Entscheidung durch die Technik des Cyberspace (das Internet) in Frage gestellt wird. In Erinnerung gerufen sei, dass das Internet mit seinem großen Kreis von teilweise gleich(englisch)sprachigen Mitwirkenden (580 Millionen) die erste reelle Chance für die Bildung einer globalen „öffentlichen Meinung" darstellt. Diese Chance ist sicher eine Herausforderung für die Politik (einzelner Staaten) wie sich etwa bei der Sperrung der Suchmaschine „Google" in China[47] und der gegenwärtigen Sperrung irakischer Server zeigt. Dass selbst die deutsche öffentliche Gewalt ihre Vorstellung von öffentlicher Meinung im Ausland durchsetzen will, zeigte sich bei der Strafverfolgung der sogenannten „qualifizierten Ausschwitzlüge" (§ 130 Abs. 3 StGB), die in Australien auf einer Homepage aufgestellt wurde. Der BGH nahm an, dass das friedliche Miteinander wie die öffentliche Ordnung in Deutschland bereits dadurch gefährdet seien, dass einige Kriminalbeamte in deutschen Amtsstuben diese englischsprachige Homepage lasen (ein Zugriff deutscher „Privatpersonen" musste nicht nachgewiesen werden).[48] Bereits diese wenigen Beispiele belegen, dass es sich um Kernfragen der öffentlichen, privaten und staatlichen Meinung handelt, die jeweils ihren Beitrag zur öffentlichen Meinungsbildung leisten sollen. Dass diese öffentliche Meinung prozesshaft entsteht und zur Effektivierung der Wahlentscheidung wie der Kontrolle der drei „Gewalten" beitragen soll, kann vorausgesetzt werden. Es ist deswegen nicht fernliegend, dass die „Nationalstaaten" – wie auch die Bundesrepublik in dem genannten Fall – (un-) gewöhnlich schnell zu einer starken Sanktion, nämlich dem Strafrecht, tendieren. Dagegen könnte man einwenden, dass die „qualifizierte Auschwitzlüge" auch in anderen „Medien" strafbar ist (§ 11 Abs. 3 StGB) und es sich deswegen nicht um ein Charakteristikum des Cyberspace und –law handelt. Charakteristisch ist aber, dass ein Nationalstaat Kommunikationsangebote, die in einem anderen Staat nicht strafbar sind und dort rechtlich zulässig angeboten werden[49], sanktionieren will.

[45] Etwa: § 202a StGB Ausspähen von Daten, § 203 StGB Verletzung von Privatgeheimnissen; § 263a Computerbetrug, §§ 269, 270 Täuschung im Rechtsverkehr bei Datenverarbeitung, § 303a Datenveränderung, § 303b Computersabotage.

[46] Etwa: Markenrechtsverletzungen durch Onlineauktion, LG München I, Urt. v. 01.03.2002, MMR 2003, 120ff.; Haftung für Links: *A. Müglich*, Auswirkung des EGG auf die haftungsrechtliche Behandlung von Hyperlinks, CR 2002, 583ff.; zu Sperrungsverfügung gegen Provider im einstweiligen Verfahren wegen nationalsozialistischer Inhalte: http://www.hei se.de/newsticker/data/anw-11.02.03-003/ (28.02.2003) „Neuer Gerichtsentscheid bestätigt Website-Sperrungen".

[47] ftd.de v. 03.09.2002, China sperrt Google aus, http://www.ftdlatestnews.de/pw/in/1030954733557.html?nv=rs (28.02.2002).

[48] BGHSt, 46, 212; der, trotz der Tatsache, dass es sich bei § 130 StGB um ein abstraktes Gefährdungsdelikt handelt, auf § 9 Abs. 1 Alt. 3 StGB abstellt, der einen Taterfolg voraussetzt. Kritisch: *K. Bremer*, Radikal-Politische Inhalte im Internet – ist ein Umdenken erforderlich?, MMR 2002, 147, 152, der die Konstruktion des BGH in Frage stellt und nur deutsche Täter auf ausländischen Servern verantwortlich machen will.

[49] Sowohl die Tatsache, dass gegen australisches Recht nicht verstoßen wurde als auch der fehlende Nachweis eines nicht professionell interessierten Rezipienten (Privatleute) hinderten den BGH nicht an einer Verurteilung.

(2) Transdisziplinarität

Über den bereits praktizierten, multidisziplinären Ansatz hinaus, stellt sich die Frage nach den Vorteilen und/oder der Notwendigkeit eines transdisziplinären Ansatzes. Paradigmatisch könnte das Signaturrecht und der Signaturmarkt sein. Was elektronische Signaturen sind und warum sie für E-Commerce und E-Government große Bedeutung haben, soll im Folgenden vorausgesetzt werden.[50] Interessant am Signaturrecht und –markt ist, dass hier das Recht den Markt schafft. Das ist ungewöhnlich, weil vom Atomrecht über das Gen- bis zum Klonierungsrecht bisher das Recht auf technische Entwicklungen reagieren sollte – nicht aber mit der Chance oder Pflicht konfrontiert war, proaktiv tätig zu werden. Diese Chance und diese Pflicht zu proaktiver Tätigkeit ist für den Signaturmarkt prägend, weil der Bund bis 2005 30 % der Verwaltungstätigkeit online abwickeln will (E-Government)[51] und das Gemeinschaftsrecht eine Implementierung elektronischer Dokumente (E-Documents) in den Rechts- und Geschäftsverkehr verlangt.[52] Unbestritten unter „Insidern" ist: das (Gemeinschafts-)Recht verlangt mehr als der Markt und die Technik gegenwärtig anbieten. So bedarf es der „economies of scale", damit möglichst viele Bürger eine elektro-

[50] *A. Roßnagel*, Die elektronische Signatur in der öffentlichen Verwaltung, S. 13ff. in *ders.* (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung, 2002, S. 13 ff; *ders.*, NJW 2003, 469ff.; *V. Schmid*, § 86a VwGO in: H. Sodan/J. Ziekow, Nomos Kommentar zur Verwaltungsgerichtsordnung, 2003, Rn 3.

[51] http://www.bund.de/BundOnline2005-.6164.htm (28.02.2002).

[52] Art. 5 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen ABl. Nr. L 13 v. 19.01.2000 S. 12ff.

nische Unterschrift erwerben können, die elektronische Dokumente authentifiziert. Circa € 60 für ein Gerät, das den Bürger im elektronischen Geschäfts- und Rechtsverkehr im rechtlichen Sinne „handlungsfähig" macht, sind für viele zu viel.[53] Darüber hinaus stellt sich die Frage der Qualität der Signaturen, die gewährleisten sollen, dass das elektronische Dokument wirklich von dem Autor stammt, der es unterzeichnet haben will (Authentizität und Identität[54]). Hier werden bereits integrierte Applikationen von Signaturen und Biometrik (etwa Fingerabdrücke, Iriskennung) untersucht[55], deren Vor- und Nachteile zu evaluieren oder prognostizieren sind. Wenn Juristen nicht nur Lösungen verhindern, sondern zu Lösungen beitragen wollen, verlangt dies eine Änderung der Methode. In Bereichen, die wie das Cyberlaw von Technizität und Faktizität geprägt werden, wird ein transdisziplinärer Ansatz vorgeschlagen:

[53] Idealiter wäre natürlich auch noch eine wirtschaftswissenschaftliche Ergänzung. Signaturen als Marktfaktor in einer mikro- und makroökonomischen Betrachtung. *A. Roßnagel*, Eine konzertierte Aktion für die elektronische Signatur, MMR 2003, 1f, der sinngemäß die „economies of scale" für den Signaturmarkt fordert. Zum Stand: CHIP März 2003, 204 ff: E-Government: Stadt, Land, Verdruss.

[54] Es ist in der juristischen Literatur noch nicht so deutlich geworden, dass Signaturen keine Garantie für die Sicherheit der Kommunikation sind. Die Geheimhaltung vertraulicher Informationen wird erst durch die Verschlüsselung – die zur Signatur hinzutritt – gewährleistet (*W. Schindler*, Sichere digitale Kommunikation – Motivation, Anforderungen, mathematisch-technische Realisierung und rechtliche Aspekte, K&R 2002, 481, 483).

[55] Konferenzen wie http://www.biosig.org/biosig2003/biosig%202003--cfp--v1.1.pdf (01.03.2003), die Themen wie integrierte Kartenapplikationen mit Biometrik und elektronischen Signaturen bei Smartcards und Tokens untersuchen, http://www.cast-forum.de/events/2002/biometrie (01.03.2003).

Rechtswissenschaft	Technische Praxis	Wirtschaftliche Praxis	Technikwissenschaft
Welches Signaturrecht gibt es im Völker-, Europa- und deutschen Recht?	Welche Techniken gibt es?	Welche Anbieterstrategien gibt es und wie können sie sich am Markt durchsetzen?	Welche Optimierungspotentiale werden für ein bestimmtes Produkt in der Wissenschaft untersucht?
Synthese Welche Chancen der Optimierung und welche Risiken bestehen?[56]			

(3) Fragmentalität im Cyberlaw

Das Cyberlaw ist bisher ein fragmentarisches Recht. Dieser Befund wird mit dem Blick in die Verfassung deutlich. Mit der Bio- und der Nanotechnologie hat das Cyberlaw gemein, dass es weder in den Grundrechten noch im Kompetenzteil des Grundgesetzes[57] grammatisch verankert ist – anders als etwa der Tierschutz (Art. 20a GG) oder der Schutz vor Zwangsarbeit (Art. 12 Abs. 2 GG). Bloße Technik „verdient" vielleicht aufgrund ihrer transitorischen und akzessorischen „Natur" nicht die Aufnahme in die Verfassung. Was aber, wenn diese Technik so transitorisch sie sein mag, nicht akzessorisch ist (also nicht nur Inhalte übermittelt, sondern die Verwirklichung von grundrechtlicher Freiheit effektiv beeinflusst; dazu siehe unter IV. 3.) und aufgrund ihrer Technizität und Faktizität die Entscheidungen der Verfassung in anderen Lebensbereichen konterkariert? Ein bekanntes Beispiel ist die Frage nach der Bedeutung eines Umwelt-, Tier und Menschenschutzes (Art. 20a GG), wenn die Frage der atomaren Zwischen- und Endlagerung und des weiteren Betriebs von Kernkraftwerken vom Verfassungsgeber (jenseits des Kompetenzartikels Art. 74 Abs. 1 Nr. 11 a GG)

[56] Nach hier vertretener Ansicht bergen etwa biometrische Elemente, die zur Kostensenkung und Sophistizierung der Signatur in Frage kommen könnten, ganz andere datensicherheits- und datenschutzrechtliche Risiken und Chancen.

[57] Art. 73 Nr. 7 GG; Art. 87 f GG spiegeln die Qualität der Fragestellungen in der Realität nicht wider.

nicht diskutiert wird.[58] Es stellt sich nicht nur angesichts eines „besonderen Mordes", bei dem sich Opfer und Täter über das Internet kennen gelernt zu haben scheinen[59], die Frage, ob die Existenz des Internet vom Verfassungsgeber nicht wenigstens diskursiv zur Kenntnis genommen werden sollte. Die Rechtsprechung des BVerfG etwa im Mikrozensus-Urteil aus dem Jahre 1967 kann sowohl für das Informationsinteresse (Personal Aktiv dazu siehe unter III. 3. c)) als auch für den Datenschutz (Personal Passiv Datenschutz dazu siehe unter III. 3. c)) nur als veraltet qualifiziert werden,[60] weil sie den gegenwärtigen (technischen) Optionen, Chancen und Risiken nicht Rechnung trägt. Um ein weiteres Beispiel zu nennen: Der Mensch kann in einer Kombination von Verkehrs-(etwa von Handy- und Internetdaten) und Überwachungsdaten (Video-Überwachung im öffentlichen[61] und privaten Raum[62]) immer weitgehender in seiner persönlichen Lebensführung überwacht werden. Und es gibt in weiten Bereichen keinen technischen Schutz, den der Bürger ex ante gegen diese technisch möglichen Erfassungen seiner Persönlichkeit und seiner persönlichen Lebensführung einsetzen kann.[63] Der Bürger ist auf Information, das Recht und auf Kontrollorgane bzw. E-Law Enforcement (siehe unter IV. 3.) angewiesen, um sein im Volkszählungsurteil skizziertes Recht auf informationelle Selbstbestimmung[64] effektiv verwirklichen zu können. Diese faktische Verkehrung der Argumentations- und Beweislast – und die Frage nach der technischen Entwertung des

[58] Zur umstrittenen Wirkung von Absprachen zwischen Regierung und betroffener Industrie vergleiche: BVerfG, 2 BvG 2/00 v. 19.02.2002 „Atomkonsens".

[59] *F. Patalong*, Die hässliche Fratze des World Wide Web, Spiegel-Online v. 12.12.2002, http://www.spiegel.de/netzwelt/tech nologie/0,1518,226774,00.html (28.02.2003).

[60] BVerfGE 27, 1, 6: „Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist". Kritisch: *A. Roßnagel/A. Pfitzmann/H. Garstka*, Modernisierung des Datenschutzrechts, 2001; *W. Kilian*, Informationelle Selbstbestimmung und Marktprozesse, CR 2002, 923; *P. Schmitz*, Datenschutz in der Informationsgesellschaft – gelten die Grundrechte, das Volkszählungsurteil und die Datenschutzgesetze noch?, MMR, 2003, 69.

[61] VG Karlsruhe, Urt. v. 10.10.2001, NVwZ 2002, 117ff.; *R. Maske*, Die Videoüberwachung von öffentlichen Plätzen, NVwZ 2001, 1248ff.

[62] ArbG Frankfurt am Main, Urt.v. 26.9.2000, RDV 2001, 190 „Schmerzensgeld aufgrund unzulässiger Videobeobachtung".

[63] Wenn man nicht vermummt oder in der Burka gekleidet in der realen Welt sich bewegen und arbeiten will.

[64] BVerfGE 65, 1, 41f.: „Es umfaßt ..die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden".

Rechts auf informationelle Selbstbestimmung – ist auch der Hintergrund der seit langem geführten Kryptographiedebatte, in der das Recht des Einzelnen seine „Informationen" (mit einer bestimmten Qualität) zu verschlüsseln mit dem Recht des oder der Staaten konkordiert werden muss, eine solche Technik nicht überwinden zu müssen, wenn ein Rechtfertigungsrechtsgut (etwa Kampf gegen den Terrorismus) den Eingriff in die Intimsphäre (technikwissenschaftlich als „Vertraulichkeit" definiert) rechtfertigt. Nicht überraschend gibt der Erfinder des Verschlüsselungsprogramms Pretty Good Privacy (PGP) zu bedenken, dass man nach gegenwärtiger Rechtslage zwar Informationen verschlüsseln könne, nicht aber sein eigenes Gesicht.[65] Gerade nach dem 11.09.2001 bestünde nicht nur in den USA die Gefahr, von Videokameras aufgezeichnet und von Computern identifiziert zu werden. Die technischen Optionen haben sich also verändert und mit Ihnen die Chancen sowohl auf die Begehung von (Cyber)Crime als auch auf eine effektive Verbrechensbekämpfung.[66] Die Chancen für Freizügigkeit, Anonymität und Intimität haben sich ob dieser technischen Optionen strukturell verschlechtert. Nicht nur nach hier vertretener Ansicht bedarf es einer Neuevaluation des Rechts auf Datenschutz und Datensicherheit – auch Datenschutzbeauftragte von 8 Bundesländern fordern eine grammatische Verankerung des Datenschutzes in der Verfassung.[67] Sinn dieser Verankerung ist die Förderung des Diskurses in der Gesellschaft, in der Politik und den beteiligten Disziplinen (etwa Informatik, Rechtswissenschaften, Sozial- und Geisteswissenschaften), der mit der Hoffnung verbunden ist, dass eine andere und – um ein bekanntes Wort zu verwenden – nachhaltigere Evaluierung der Chancen und Risiken des Cyberspace stattfinden kann.

[65] http://www.heise.de/newsticker/data/jk-30.01.03-011/ (28.02.2003).

[66] FAZ v. 11.09.2002, S. 13 „Korruptionsregister bleibt umstritten"; FAZ v. 22.08.2002, S. 3 „EU will Zugriff auf Computerdaten"; *R. Allitsch*, Data Retention on the Internet, Cri 2002, 61f zu Vorhaltung von Verkehrsdaten (Traffic Data) für Sanktion und Prävention; http://www.heise.de/newsticker/data/pmz-16.12.02-000/ (28.02.2003) „Machbarkeitsstudien zu biometrischen Daten im Personalausweis" berichtet von einem Pilotprojekt am deutsch-tschechischen Grenzübergang Waidhaus, in dem Live-Aufnahmen von Durchreisenden mit ihren Passbildern verglichen werden. Siehe zu den Möglichkeiten, biometrische Merkmale in Personalausweise zu integrieren: Art. 8 Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz). Ohne dass hier die bewegte Diskussion um die Videoüberwachung an öffentlichen Plätzen und am Arbeitsplatz aufgegriffen werden soll. Siehe hierzu etwa *A. Schmitt Glaeser*, Videoüberwachung öffentlicher Räume – zur Möglichkeit administrativer panoptischer Machtausübung, BayVBl. 2002, 584ff.

[67] FAZ v. 22.08.2002, S. 4.

(4) Recherchestrategien und zu ändernde Zitier-, Archivierungs-, Verifizierungs- und Publikationsetiketten

Das Cyberlaw verlangt nach neuen Recherchestrategien. So finden sich Hinweise auf und die Literatur und die Rechtsprechung im Internet selbst. Ein Beispiel ist etwa die Seite http://www.findlaw.com/01topics/10cyberspace/, die zu Gerichtsurteilen und Homepages amerikanischer Regierungsbehörden führt. Die Zitierstrategie für den Cyberspace muss sich ändern, weil die zitierten Quellen (die Sites) nicht permanent sind. Für diesen Beitrag wird deshalb das Datum der Abfrage zu der Adresse hinzugefügt. Idealiter sollten die Seiten, die zitiert werden, vom Autor archiviert – also auf einem Datenträger oder wenigstens auf Papier gespeichert werden. Wissen aus dem Internet sollte darüber hinaus mit herkömmlichen Recherchestrategien verifiziert werden. Dafür gibt es zwei Gründe – zum einen die Kommerzialisierung des Internet (dazu siehe unter IV. 4.) und zum anderen die Intimisierung des Internet.[68] Aus technischer Sicht ist anzufügen, dass Internet-Veröffentlichungen (zum Cyberlaw) die Chance bieten, dass mit Links unmittelbar auf die Internetquelle, die zitiert wird, zugegriffen werden kann.[69] Eine jüngere (Fort-)Entwicklung ist die Schaffung einer neuen Textkultur durch „Blogging"[70], also der Schaffung von Tagebüchern, die zum Teil nur aus Links bestehen. Dass die Publikationsetikette sich ändern könnte, ist bereits (Hochschul-)Politikum. So gibt es etwa die Forderung nach der Publikationspflicht für Professoren im Internet,[71] die in diesem Beitrag wegen des anderen thematischen Schwerpunktes nicht weiter untersucht werden soll. Hingewiesen sei nur darauf, dass etwa Gesetze immer

[68] Die für „Massenmedien" herkömmliche Kontrolle der Redakteure entfällt.

[69] Insbesondere die neue Fassung des Programms Adobe Acrobat (5.0) ermöglicht mit wenig Aufwand diese Form der Präsentation.

[70] Es handelt sich um (Tagebuch-)texte, die miteinander verlinkt sind und/oder zum Teil nur Links enthalten (zu den Feinheiten wie permalinks, trackbacks, etc.: http://www.tzw.biz/www/home/print.php?p_id=2030 (28.02.2003). Der Begriff „Blogging" ist eine Mischung aus „Web" und „Log" (FAZ v. 24.02.2003, S. 18 „Die Weblog-Szene wird erwachsen").

[71] http://heise.de/newsticker/data/jk-10.11.02-003/ (28.02.2003) „Publikationspflicht für Professoren im Netz gefordert". http://www.heise.de/ct/02/18/084/ (28.02.2003) „E-Publish oder Perish", zu der Initiative einer weltweiten Digital Mathematical Library"; http://heise.de/newsticker/data/jk-28.04.02-004/ (28.02.2003) „E-Publishing-Revolte in der Wissenschaft". Auch die Hochschulrektorenkonferenz soll eine solche Publikationspflicht erwägen: In Promotionsordnungen findet sich auch die Möglichkeit, elektronische Versionen, die ins Netz gestellt werden können, abzuliefern und dadurch die Anzahl der Belegexemplare zu vermindern (etwa Promotionsordnung der Juristischen Fakultät der Bayerischen Julius-Maximilians-Universität Würzburg, § 19 Abs. 1 Nr. 4 und Abs. 2).

noch nicht kostenfrei im Internet erhältlich sind[72] – und die Kenntnis der Gesetze ist doch immer die erste Voraussetzung ihrer Befolgung.

(5) Dynamik: Der Anfang ist der Beginn des Endes und das Ende ist der Beginn des Anfangs

Cyberlaw ist ein junges „Rechtsgebiet" und gewährtigt wie jedes Rechtsgebiet sein Ende. Mit den Worten von *Michael Stolleis*: „Zuletzt ist das Fach „etabliert", man kann es begehen und möblieren wie ein neu gebautes Haus, das allerdings eines Tages auch zum Abbruch freigegeben werden kann, wenn sich die juristische Weltsicht geändert hat."[73] Abgesehen von diesem Anfang-Ende-Szenario gilt für die „Lebenszeit" des Cyberlaw: Technische Änderungen werden zu Änderungen des Rechts führen – oder zumindest zu Diskussionen „de lege ferenda". Ein Beispiel, über das diskutiert werden sollte, ist der Umgang mit Verkehrsdaten, die in Zukunft bei der Benutzung sogenannter Smart Little Objects (Internetuhren und Internethandys)[74] „organisiert"[75] werden. Die ubiquitäre und allzeit mögliche Vernetzung des Menschen mit dem Internet (etwa wenn in einer Kirche Informationen über den Erbauer, in einem Museum Informationen über einen Maler abgefragt werden) ermöglicht die Erstellung sogenannter Nutzerprofile, die den, die oder einzelne Menschen durchsichtig machen könnten. Es besteht eine große (Rechts-)Unsicherheit welche Reise- und Aufenthaltsdaten von Menschen im Cyberspace von wem, unter welchen Voraussetzungen und wie lange „organisiert" werden dürfen.[76] Und es stellt sich die weitere in der Zu-

[72] Das Bundesgesetzblatt unter www.makrolog.de umfasst nur den Zugang zu den letzten 3 Jahren; aktualisierte Fassungen eines Gesetzes, die als Arbeitsgrundlage für sämtliche beteiligten Verkehrskreise (außer bekannten Druckereien und Verlagen) nützlich sein könnten, sind in authentischer Form auch im Cyberspace rar.

[73] *Stolleis*, Fn. 17, S. 10.

[74] Es ist in der juristischen Literatur noch nicht so verbreitet, dass Signaturen keine Garantie für die Sicherheit der Kommunikation sind. Die Geheimhaltung vertraulicher Informationen wird erst durch die Verschlüsselung – die zur Signatur hinzutritt – gewährleistet (*W. Schindler*, Sichere digitale Kommunikation – Motivation, Anforderungen, mathematisch-technische Realisierung und rechtliche Aspekte, K&R 2002, 481, 483).

[75] „Organisation" wird hier als Oberbegriff für die im Datenschutzrecht geltenden Definitionen des Erhebens, des Verarbeitens und des Nutzens (§ 3 Abs. 3-5 BDSG) verwandt.

[76] Aus der Praxis zu einer grundsätzlichen Frage (wie in Zukunft auch Straftäter im Cyberspace erkannt und verfolgt werden können) *H. Bleich/J. Heidrich*, Ach wie gut, dass niemand weiß..., c't 19/2002, S. 124, 126; insbesondere dazu, wer mitliest: *P. Brauch*, Von wegen Incognito, c't 19/2002, S. 129. Strittig ist die Frage, ob bei Flatrates (die zu einer zeitlich unbegrenzten Nutzung des Internet berechtigen) gespeichert werden darf, welche „Reisen im Cyberspace" unternommen werden. Für den Diensteanbieter sollte das irrelevant sein, weil es sich um eine „Flatrate" handelt. Dennoch hat das Regierungspräsidium

kunft zu beantwortende Frage, ob das Recht es hinnimmt, dass vorläufig elitäres Wissen und Engagement Einzelne in die Lage versetzt, maskiert zu „reisen" und zu „leben" (siehe oben unter III. 2. b) (2) zur Kryptographiediskussion).[77]

3. „Cyberlaw": eine vergleichende Betrachtung mit anderen Bezeichnungen dieses „Rechtsgebiets"

Wenn man in der juristischen Lehrbuch-, Kommentar- und Zeitschriftenliteratur nach Bezeichnungen für die Themen und Elemente dieses „Rechtsgebiets" sucht, wird man nur im Ausnahmefall mit „Cyberlaw"[78] fündig. Verwandt werden „Informationsrecht" (*M. Kloepfer*); „Internetrecht" (*T. Hoeren*); „Computerrecht" (*J. Marly*[79]; Zeitschriften CR[80] und CRi[81]), „Datenschutzrecht" (*S. Simitis*[82], Zeitschrift DUD[83]), „Telekommunikationsrecht"

Darmstadt als zuständige Datenschutzaufsichtsbehörde für T-Online entschieden, dass solche Daten gespeichert werden dürfen http://www.heise.de/ct/aktuell/data/hob-14.01.03-000/ (28.02.2003) und *J. Heidrich/A. Neue*, Internet-Privat, c't 3/2003, S. 78. (Anders: „Hamburgs Datenschutzbeauftragter gegen die IP-Adressen-Speicherung bei Flatrates" http://www.heise.de/newsticker/data/hod-28.01.03-000/ (28.02.2003) und „Datenschützer gegen pauschale Speicherung von Internet-Nutzerdaten" http://www.heise.de/newsticker/data/jk-25.10.02-011/ (28.02.2003) und Vorratsdatenspeicherung in der Europäischen Union" http://www.heise.de/newsticker/data/anm-27.11.02-000/ (28.02.2003). Allgemein: *I. Geis*, Das neue Datenschutzrecht für Teledienste, CR 2002, S. 667; *H. Rasmussen*, Datenschutz im Internet (Gesetzgeberische Maßnahmen zur Verhinderung der Erstellung ungewollter Nutzerprofile im Web...) CR 2002, 36. *A. Ohlenburg*, Die neue EU-Datenschutzrichtlinie 2002/58/EG, MMR 2003, 82, 83 die grundsätzlich eine zügige Löschung der Verkehrsdaten verlangt (Art. 6 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ABl. Nr. L 201 vom 31.07.2002, S. 37ff., in Art. 15 werden Ausnahmen im Interesse der öffentlichen Sicherheit zugelassen). Anschließend stellt sich die Frage, inwieweit das „Personal Passiv Datenschutz" einwilligen muss und welche Anforderungen an diese Einwilligung zu stellen sind: Zur (elektronischen) Einwilligung und allgemein *S. Simitis*, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., 2003, § 4a (Rn. 38f.).

77 Aus der Praxis: *S. Köpsell/A. Kassel*, Maskenball (Tools zum anonymen Surfen), c't 19/2002, S.132 134 zu den Schwierigkeiten und Chancen von Steganos (mit dieser Technik soll man Cookies, Browser-Cache, History- und Papierkorb-Funktionen überschreiben können).

78 *Boehme-Neßler* (Fn. 6); *A. Schwerdtfeger* (Fn. 2).

79 *J. Marly*, Einführung zum Computerrecht, in: Beck-Texte im dtv, Bd. 5562, Computerrecht, 4. Aufl. 2000.

80 Computer und Recht, Verlag Otto Schmidt.

81 Computer und Recht International, Verlag Otto Schmidt.

82 *Simitis* (Fn. 76).

(*B. Holznagel*[84]) und „Medienrecht"(Zeitschrift MMR[85]). Diese Begriffe können den innovativen Charakter des Cyberspace[86] und die Komplexität und Konnexität der dort zu wahrenden Interessen aus unterschiedlichen Gründen nicht widerspiegeln. Deutlich wird bei dieser Begriffssammlung und bei der Lektüre der Inhalte, dass es eine Zweiteilung dieses „Rechtsgebiets" gibt, die hier als „spezielles" und „allgemeines Technikrecht" kategorisiert werden soll.

a) „Spezielles Technikrecht"

Hierzu gehören die Rechtsfragen, die mehr oder weniger unmittelbar mit einer spezifischen Technik verbunden sind – wie etwa das Telekommunikationsrecht[87]. Weitere Beispiele der Zukunft könnten das Signaturrecht, das Kryptographierecht und das Recht der biometrischen Daten sein. Dass hier weitere Gliederungen vorstellbar und Abgrenzungsunschärfen bisweilen unvermeidbar sind, darf als bekannt vorausgesetzt werden.[88] Deutlich wird, dass der hier vertretene Ansatz sachverhalts- und problemorientiert ist (rechtsrealistisch) und nicht das Kompetenzrecht (etwa die Abgrenzungsschwierigkeiten des bundesrechtlichen Gesetzes über die Nutzung von Telediensten (TDG) zum länderrechtlichen Mediendienstestaatsvertrag) oder die lege lata in den Mittelpunkt stellt. Für das Cyberlaw wird diese Ebene mit der Abkürzung „E-" (Electronic) überschrieben. Also etwa E-Elections[89]; E-Documents (§ 86a VwGO) und E-Commerce[90].

83 Datenschutz und Datensicherheit, Verlag Vieweg.

84 *B. Holznagel/C. Enaux/C. Nienhaus*, Grundzüge des Telekommunikationsrechts, 2001.

85 MultiMedia und Recht, Verlag C.H. Beck.

86 *Kloepfer* (Fn 6): „Cyberpublic" (§ 1 Rn. 97) und „Cyberspace" (§ 1 Rn. 42); Cybersquatting (§ 1 Rn. 47) und Cyber-War" (§ 1 Rn. 43).

87 Telekommunikationsgesetz (TKG); Teledienstegesetz (TDG); einführend: *Holznagel* (Fn. 84).

88 Etwa das „Recht der elektronischen Dokumente", das Signaturen, Verschlüsselungen, biometrische Daten, Datensicherheitsrecht (Schutz vor und Sanktion von Angriffen durch Viren, Würmer und Trojaner etwa durch die telekommunikationsrechtliche Speicherung von Verkehrsdaten; siehe oben in Fn. 66) und Datenschutzrecht enthält.

89 *M. Will*, Wahlen und Abstimmungen via Internet und die Grundsätze der allgemeinen und gleichen Wahl, CR 2003, 126.

90 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 08.06.2000 über bestimmte rechtliche Aspekte des Dienstes der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. Nr. L 178 v. 17.07.2000, S. 1ff.

b) „Allgemeines Technikrecht"

Auf dieser Ebene sind die grundsätzlichen und „alten" Fragen zu untersuchen. Also etwa die Themen der informationellen Grundversorgung (Art. 16 EG; „Digital Divide"[91]), der öffentlichen Aufgaben[92], der virtuellen Persönlichkeit (siehe dazu unter IV. 2. a)) und des Selbstbewußtseins der realen Absenz im Cyberspace (der negativen Rezipientenfreiheit). Konstruktiv soll die Trennung beider Ebenen dazu beitragen, dass Synergie- und Hierarchiechancen offen gelegt und vielleicht genutzt werden.

c) „Cyberlaw"

Die Begriffswahl „Cyberlaw" ist nach hier vertretener Meinung notwendig, um deutlich zu machen, dass es um die Verteilung von Lebenschancen in einem neuen „Raum" geht (Cyberspace[93]). Die Technik hat diesen „Raum" geschaffen und das Recht sollte die Kompetenz erwerben und ausüben, um seiner Steuerungsfunktion zu genügen (etwa durch „regulierte Selbstregulierung", siehe unter IV. 3.). Es geht um Kybernetik (Cybernetics)[94] durch Technik- und Geisteswissenschaften angesichts der Fragestellungen und Herausforderungen des Internets und der Internetökonomie – und damit nicht nur seit griechischen Zeiten um die Kompetenz der (Nicht-)Steuerung (kybernetiké; Cybernetics). Für Cyberlaw spricht weiter, dass in der anglo-amerikanischen Literatur die „Regelungsobjekte" des Cyberlaw mit Cyberspace, Cyperpublic, Cyborg, ... bezeichnet werden. Cyberlaw ist demzufolge der Oberbegriff für die eingangs geschilderten Medien-, Telekommunikations-, Computer-, Internet-, Informations-, Datensicherheits- und Datenschutzrechte, die sich mit den Themen des Cyberspace befassen. Diese Begriffe tragen der Komplexität und Konnexität des Cyberspace nicht Rechnung, wie auch ein Schema, das als „Suchmaschinenstrategie" für Interessen und Recht (insbesondere Normen bei Informations- und Cybersachverhalten) entwickelt wurde, verdeutlicht:

---

[91] *Klopefer* (Fn. 6) § 1 Rn. 17 ff; § 4 Rn. 27.

[92] *I. E. Vassilaki*, Das Prinzip Vertrauen für Informationsdienste, CR 2002, 742, 746 formuliert eine Aufforderung, die informationelle „Grundversorgung" (die auch die Datensicherheit beinhaltet) zu sichern und so den elektronischen Geschäftsverkehr zu begleiten.

[93] Zur Verwendung der Domain „cyberspace.de" OLG Dresden, Urt. v. 20.10.1998, CR 1999, 589, wenn damit eine Absatzbehinderung verbunden ist. Zur Errichtung eines „Cybernariums" Darmstädter Echo v. 26.02.2003, S.9.

[94] Zum Begriff siehe Principia Cybernetica Web (http://pespmc1.vub.ac.be/ASC/cybernetics.html (28.02.2003), die den Begriff auf den Mathematiker Norbert Wiener zurückführen. Zur Entstehung des Begriffs „Cyberspace": *Kloepfer* (Fn. 6), § 1 Fn. 98.

1.	***Personal-aktiv*** *Informationsrecht*	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen interessiert ist
2a)	***Personal-passiv*** *Datenschutz*	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an der Reservierung und Sicherung von Informationen interessiert ist.
2b)	***Personal-passiv*** *Informationskosten*	Hierunter fallen die Kosten für die Erhebung, Speicherung, Aufbereitung und Übermittlung von Informationen. Ein Beispiel, das die Rechtsprechung bereits beschäftigt hat, ist § 90 TKG.[95]
3.	***Objekt***	Auf Informationen welchen Inhalts soll zugegriffen werden?
4.	***Kausal/Zweck***	Zu welchem Zweck soll auf diese Informationen zugegriffen werden (etwa: Kampf gegen den Terrorismus; Wahrung der Urheberrechte)?
5a)	***Qualität der Information(-stechnik)*** *Personal-passiv* *Datenschutz*	Hierunter sind die unterschiedlichen Formen der „Organisation" von Daten zu verstehen. Beispielhaft wie in § 3 Abs. 3 – 5 BDSG (Erheben, Verarbeiten, Nutzen) aufgezählt.
5b)	***Qualität der Information(-stechnik)*** *Personal-aktiv* *Informationsrecht*	Hierzu zählen etwa Suchmaschinen (Google), die mit Algorithmen die im Cyberspace verfügbaren Informationen leichter zugänglich machen.
6.	***Verfahren***	Welches Verfahren verlangt das Recht für die Organisation und den Umgang mit diesen Daten? (Etwa: die Einwilligung des Betroffenen, § 4a BDSG; die Einschaltung eines Gremiums, §§ 14, 15 Artikel 10-Gesetz – G 10)

---

[95] OVG Münster Beschl. v. 17.05.2002, TKMR 2002, 400. Zur Pflicht zur Führung von Kundendateien in sicherheitsbehördlichem Interesse bei Prepaid-Produkten.

7.	***Rechtfertigung/ Verhältnismäßigkeit***	Hier findet die aus dem deutschen Verfassungsrecht bekannte Verhältnismäßigkeitsprüfung statt, die das Interesse von Personal Aktiv (Rechtfertigungsrechtsgut) mit dem Interesse des Personal Passiv Datenschutz (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Interesse des Personal Passiv Informationskosten (Art. 12, 14, 2 Abs. 1 GG) (als Eingriffsrechtsgütern) abwägt.

Der Begriff „Informationsrecht" reicht demzufolge nicht aus, weil sich in ihm das Datenschutzrecht (Personal Passiv Datenschutz) und damit die Bi- und Mulitpolarität von Kommunikation nicht wiederfindet. Der Begriff „Internetrecht" reicht nicht aus, weil mit diesem Begriff nicht zum Ausdruck kommt, dass es grundlegende und bekannte Fragestellungen sind (siehe sogleich unter IV.), die im Cyberlaw neu zu diskutieren sind. Auch die Begriffe „Telekommunikationsrecht" und „Medienrecht" spiegeln in ihrer Technizität nur das Transportmedium Internet wieder.[96] Das „Computerrecht"[97] ist ein Teil des Cyberlaw, den man in einer Parallelbetrachtung als sein Baurecht bezeichnen könnte. So wie die reale Welt Bauplanungs- und Bauordnungsrecht kennt, damit die Welt so schön und sicher wie möglich bebaut wird – so liefert das Computerrecht einen Beitrag dazu, wie die „Häuser" im virtuellen Raum gebaut werden. Eine aktuelle Frage ist etwa, ob die Hard- und Software eines Computers so angeboten werden darf, dass Urheberrechtsverletzungen durch den Nutzer dokumentiert oder verhindert werden oder der Computer selbst bei der Befassung mit bestimmten Texten (via Textverarbeitung oder E-Mail-Versand) Mitteilungen an den Verfassungsschutz sendet.[98] Der Begriff „Datenschutzrecht" reicht nicht aus, weil – wie beim Begriff „Informationsrecht" – die Fokussierung auf Rechte und

[96] Hinzukommt, dass die Unterscheidung von Telekommunikations- und Medienrecht zwar im Kompetenzrecht der deutschen Verfassung angelegt ist, in der Zukunft durch die „Konvergenzentwicklung" auf europäischer Ebene an Bedeutung verlieren wird. *M. Rosenthal*, Neue Antworten auf Fragen der Konvergenz, TMR 2002, 181, 184 mit der Befürchtung der weiteren Vergemeinschaftung der Rundfunkregulierung.

[97] *Marly* (Fn. 79).

[98] Zur Implementation von Trusted Platform Modulen (TMP) in den Computer, die von einer Allianz führender Hard- und Softwarehersteller der Trusted Computing Platform Alliance (TCPA) erwogen wird: *M. Plura*, Schlossgespenst, c't 2002/26, S. 54; *ders.*, Entmündigung des PC-Besitzers, c't 2002/26, S.58; Der PC mit den zwei Gesichtern, c't 2002/24, S. 186; *ders.*, Der versiegelte PC, c't 2002/22, S. 204.

Interessen von „Personal Passiv Datenschutz" nicht die Informationsansprüche von „Personal-aktiv Informationsrecht" wiedergibt. Auch aus einem anderen Grund reicht die datenschutzrechtliche Perspektive nicht mehr aus: angesichts von Angriffen auf das Internet (Home Pages, die verändert werden[99]; E-Mail-Adressen, die mit Spams funktionsunfähig gemacht werden; Intranets und Wireless Local Area Networks (WLANS), die abgehört werden[100]) wird das Datensicherheitsrecht in Zukunft an Bedeutung gewinnen. Anders als beim Datenschutzrecht, dem mit dem Schutz personenbezogener Daten seit dem Volkszählungsurteil ein inhaltsbetonter Ansatz zugrunde liegt,[101] befasst sich das Datensicherheitsrecht mit der Qualität der Informationstechnik: Wie kann der Cyberspace technisch organisiert und strukturiert werden, damit die elektronische Kommunikation einer der Beförderung eines realen Briefes ähnliche Sicherheitsqualität erhält.[102] Dass dieser technikorientierte Detailbereich des Datenschutzrechtes durchaus in Konflikt mit den Informationsinteressen (Personal-aktiv Informationsrecht) kommen kann, dokumentieren zwei Beispiele aus der Praxis: So wollte ein mittelständisches Unternehmen sich vor der Zusendung mit „Sexmails" beziehungsweise dem Aufklicken der Werbeanzeigen von einschlägigen Diensten (Pop Up Advertisements) durch eine sogenannte Firewall schützen. Dieses Filterinstrument ließ dann auch keinen E-Mail-Verkehr, der das Wort „screw" beinhaltete, mehr zu. Die Patentabteilung dieses Unternehmens konnte mit externen Anwälten nicht mehr per E-Mail kommunizieren, weil „schrauben" ein Tätigkeitsbereich des Unternehmens war. Ähnliche Probleme mit einer Firewall hatte das englische Parlament, das eine Verschärfung des Sexualstrafrechts erwog – und diese Novelle aber nicht über E-Mail vorbereiten konnte, weil die Inhalte nicht zugestellt wurden.[103]

[99] Etwa der Angriff auf die Website der Bundeswehr in Strausberg http://www.heise.de/newsticker/data/tol-20.01.03-000/ (28.02.2003); FAZ v. 10.02.2003, S. 15 „Hacker finden immer mehr Schwachstellen in den Schutzmauern der Firmennetze" mit einer Aufstellung der Herkunft und der Ziele der Attacken auf Firmennetze; Technisch: *P. Lippert*, Neue sicherheitsbezogene IT-Dienstleistungen, CR 2002, 458. Die EU plant eine Agentur für Internetsicherheit zu gründen, FAZ v. 10.02.2003, S. 11.

[100] Zur Anzeigepflicht: *J. Röhrborn, P. Katko* , Rechtliche Anforderungen an Wireless LAN, CR 2002, 884.

[101] BVerfGE 65, 1ff.

[102] Selbstverständlich gibt es hier auch Veruntreuungen durch Beschäftigte der Transportunternehmen; diese halten sich statistisch aber wohl in einem anderen Rahmen als die Angriffe auf das Netz.

[103] Http://www.heise.de/newsticker/data/wst-09.02.03-003/ (28.02.2003) „Spam-Filter verärgert britische Abgeordnete".

d) „E-Law" (Electronic Law) als spezielles Technikrecht

Das E-Law als spezielles Technikrecht des Cyberspace läßt sich hinsichtlich seiner Konturen wie seiner Erforschung weiter unterteilen. So gibt es zum einen E-Law-Bereiche, die in einer juristischen Betrachtung[104] weniger komplex sind und zum anderen E-Law-Bereiche, die Komplexität nahelegen. So ist der Bedeutungsgehalt von „E-Documents" (elektronischen Dokumente")[105] offensichtlich einfacher zu bestimmen als zu entscheiden, wie E-Government (E-Governance[106]) und E-Democracy zu verwirklichen sind.[107] Es handelt sich um die Virtualisierung bekannter und höchst komplexer Fragestellungen, für die die weitere Perspektive – des Cyberlaw und des Cyberspace – vorgeschlagen wird.

IV. IV. Cyberspace und „reales Leben" – Cyberlaw und überkommene rechtliche Strukturen

1. Parallelität von Cyberspace und „realem Leben" und von Cyberlaw und überkommenen rechtlichen Strukturen

Hier soll eine Parallelitätsthese aufgestellt werden: (Rechts-)tatsächlich stellen danach das „Leben im Cyberspace" und das „Leben im realem Raum" vergleichbare Anforderungen und Fragen an das Recht. Das ist auch die Erklärung für den hier skizzierten Befund, dass kein „Rechtsgebiet" er-

[104] In einer technischen Betrachtung kann die Verwendung von E-Documents sehr hohe Anforderungen an die Organisation und Sicherheit des Workflow bei Gerichten stellen. Das ist der Grund, weshalb bisher nur Pilotprojekte zu existieren scheinen (etwa Verwaltungsgericht Sigmaringen http://www.justiz.baden-wuerttemberg.de/vg/VGSIG/Serv Abschlussbericht .DOC (28.02.2003) und Verordnung über den elektronischen Geschäftsverkehr beim BGH v. 26.11.2001 (BGBl I, 2001, S. 3225)).

[105] „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr" vom 13.07.2001 (BGBl I, 2001, S. 1542, 1545), das zur Einführung elektronischer Dokumente mit §§ 126ff. BGB, § 130a ZPO, § 81 Abs. 2 GBO, § 46b ArbGG, § 108a SGG und § 77a FGO geführt hat.

[106] „Governance" hat auch einen methodischen Charakter: method or system of government or management (Webster's Encyclopedic Unabridged Dictionary of the English Language, 1996.

[107] Statt „E" wird bisweilen „Digital" verwandt.

sichtlich ist, das im Cyberspace nicht als Cyberlaw vorstellbar wäre[108] – auch wenn es aufgrund der Globalität des Cyberspace, der Jugend des Cyberlaw und vielleicht einer anderen Gestaltungsvision (siehe dazu unter IV. 3.) (noch nicht) erlassen ist. Diese These der theoretischen Parallelität kann hier nicht in allen Einzelheiten aufgefächert werden; sie soll nur anhand einiger Aspekte plausibel gemacht werden. Die Grobgliederung gibt die traditionelle Drei-Elemente-Lehre[109] vor, die Staatsvolk, Staatsgebiet und Staatsgewalt verlangt.

a) Cyberpublic

Es gibt Internet Societys, die sich als solche begreifen und in Newsgroups, Chatrooms und per E-Mail interagieren. Eine Society hat sich bereits selbst einen Code of Conduct gegeben.[110] Akteure der Cyberpublic sind natürliche und juristische Personen, die im Cyberspace Namen und Adressen haben.

(1) Namen und Adressen natürlicher und juristischer Personen

Hier ist zwischen dem Namen, den eine Person im realen und/oder virtuellen Leben (Domain[111]) führt und der Adresse, mit der sie im Internet von den Rechnern und Netzwerken identifiziert wird (Internet Protocol (IP) und Transmission Control Protocol (TCP)) zu unterscheiden. Die Tatsache, dass die virtuellen Namen – die Domains – von einer privaten juristischen Person (DENIC eG)[112] vergeben werden, wird hier nur referiert und noch nicht kritisiert. In einer Parallelbetrachtung zum Namensrecht ist überraschend, dass der Staat nur bei den Namen natürlicher Personen (Standesamt) und den Firmen (Handelsregister) eine ex-ante-Kontrolle vornimmt; die Namensgebung im Internet aber einer juristischen Person des Privatrechts

[108] Um nur einige Beispiele zu nennen: Gewerberecht könnte etwa die Zulassung von Anbietern sein (§ 11 TKG); Umweltrecht könnte sich mit dem Schutz vor Spamming und Kettenmails befassen; Seucherecht könnte vor Viren, Würmern und Trojanern schützen; Telekommunikationsrecht könnte funktionsadäquat zum Straßenrecht interpretiert werden.

[109] Hierzu etwa: *K. Hailbronner* in: W. Graf Vitzthum (Hrsg.), Völkerrecht, 2001, S. 191f.

[110] http://www.isoc.org/members/codeconduct.shtml (28.02.2003), der in einer traditionellen rechtlichen Betrachtung marginal zu sein scheint, aber dennoch den Regelungsbedarf vorskizziert.

[111] Inzwischen gibt es nicht nur die Top-level-Domain „.de", sondern es soll auch eine „EU-Domäne"zur Verfügung gestellt werden *C. König/A. Neumann*, Die neue Top-Level-Domain „.eu" als Beitrag zum Auf- und Ausbau transeuropäischer Netze?, EuZW 2002, 485f.; EuZW 2002, 322 „.eu"-Domänenname".

[112] http://www.denic.de/doc/DENIC/statuten.html (28.02.2003) „Statut der Genossenschaft".

(Genossenschaft) und der Rechtsprechung im Wege der ex-post-Kontrolle überlässt.[113]

(2) Externes und internes Familienrecht

Die Mitglieder der Cyberpublic sind zum Teil jung und diese Tatsache hat bereits zu einer Beschäftigung der Rechtsprechung mit Fragen der Strafmündigkeit[114] wie der Geschäftsfähigkeit[115] im Cyberspace geführt, die hier als „externes Familienrecht" bezeichnet werden. Eine weitere in Deutschland bisher im Gegensatz zu den USA und Dänemark weniger problematisierte Frage ist der Schutz der personenbezogenen Daten von Kindern vor Schulen, Werbeagenturen, Providern und Eltern, wenn letzere ihre Kinder auf ihren Homepages präsentieren oder ihre Einwilligung zur „Organisation" der Daten der Kinder geben.[116] Auch die Fragen, ob, wie (geschützt durch Filterprogramme) und wie lange sich Kinder im Cyberspace aufhalten dürfen, beschäftigen die mit der Personensorge (§ 1631 BGB) betrauten Eltern (internes Familienrecht).[117]

(3) „Staatenlose"

Auch im Cyberspace gibt es Menschen, die keinen oder schwerer Zugang zu den Bürger"chancen" der Cyberpublic haben. In einer globalen Betrachtung führen technische und wirtschaftliche Gründe zu einer unterschiedlichen Cyberspaceaffinität der Süd- und Nordhalbkugel der Erde. Darüber hinaus bringt nicht jeder Bürger die Eintrittsgelder für den Cyberspace auf (Computer, Flatrate, Drucker...) – ein Sachverhalt, der als digitale Spaltung

113 Der Schwerpunkt liegt hier im Wettbewerbsrecht bei §§ 1 und 3 UWG; etwa OLG Hamburg, Urt. v. 02.05.2002, K&R 2002, 610 zur irreführenden Domain-Adresse –"rechtsanwalt.com".

114 http://www.heise.de/newsticker/data/anw-07.01.03-001/ (28.02.2003) „Freispruch für DVD-Hacker" durch ein norwegisches Gericht: Ein 16 jähriger Norweger hatte sich an der Entwicklung und Verbreitung eines Programms beteiligt, das den Kopierschutz auf DVDs ineffektiv machte.

115 http://www.heise.de/newsticker/data/hob-28.01.03-000/ (28.02.2003) zu einer Entscheidung des Kammergerichts Berlin: „Einwahl von betrügerischem Dialer muss nicht bezahlt werden", wenn ein 16-Jähriger ohne Wissen der Mutter agiert.

116 Mit der Folge, dass die Chancen einer selbstbewußten Entwicklung der (Nicht-)Cyberpersönlichkeit der „Kinder" durch diese Kindheitsveröffentlichungen verringert werden (*S. Nouwt*, Kid's Privacy on the Internet (Collecting Children's Personal Data on the Internet and the Protection of Privacy, MMR 2002, 703f. mit Beispielen).

117 FAZ v. 03.03.2002, S.18 „Eltern setzen Kindern Internet-Regeln".

der Gesellschaft („Digital Divide") bezeichnet wird und die aus dem Medienrecht bekannte Frage nach der „Grundversorgung" stellt.[118]

b) Cyberspace

Der Cyberspace ist sicher nicht vom Territorialitätsprinzip als Ausdruck und Begrenzung der (national)staatlichen Souveränität geprägt.[119] Dafür gibt es mehrere Gründe: zum einen muss das Recht erst (Nicht-)Steuerungskompetenz erwerben; zum anderen hat der Cyberspace noch Elemente einer technisch gewährleisteten und vorrechtlichen Freiheit (siehe unter IV. 3.) und zum dritten ist der Cyberspace technisch definiert und determiniert. So stellt sich – anders als in der „realen Welt" – stets die technische Option für eine Lösung, weil die Technik, die den Raum groß macht, ihn auch verkleinern kann. Ein Beispiel ist die Unterbindung nationalsozialistischer Inhalte auf den Homepages, die ein Server anbietet.[120] Hier stellt sich die Frage, inwieweit es dem „Personal-passiv Informationskosten" (im Sinne der Skizze unter III. 3. c)) zumutbar ist, entsprechende Filtermechanismen zu entwickeln, zu pflegen und einzusetzen, damit diese Homepages nicht veröffentlicht werden können. Und: Da später andere Unternehmen wieder „workaround tools" (Umgehungsstrategien) entwickeln werden, dann die Frage der zu fordernden Qualität dieser Filterinstrumente, die vom Recht ex-post (Rechtsprechung) oder ex-ante (Normgeber) beurteilt werden muss.

c) Cybergovernance

(1) Gubernative, Adminstrative, Judikative, Legislative

Die Terminologie Staats"gewalt" der Drei-Elemente-Lehre trägt der innerstaatlichen Diskussion nicht mehr Rechnung. Wie auch immer man Privatisierungsbemühungen oder die Erfolgsgeschichte des Begriffs „regulierte

118 *Kloepfer* (Fn. 6), § 1 Rn. 17, § 4 Rn. 27ff. Unter anderem auf privater und UN-Ebene gibt es Initiativen: http://www.heise.de/newsticker/data/em-14.07.01-003/ (28.02.2003) „Digital-Divide-Initiative: Schweiz übernimmt Vorsitz" mit dem Hinweis auf ein Global Knowledge Partnership Portal; http://www.bmz.de/themen/imfokus/ppp/ppp59.html (28.02.2003) „Entwicklungspartnerschaften mit der Wirtschaft (Public Private Partnership)"; *K. Windthorst*, Von der Informationsvorsorge des Staates zur staatlichen Gewährleistung eines informationellen Universaldienstes, CR 2002, 121 ff.

119 *Graham* (Fn. 44); *Determann* (Fn. 8).

120 Siehe Fn. 46.

Selbstregulierung“[121] in der deutschen Rechtswissenschaft bewerten mag: Festzuhalten ist, dass es gegenwärtig näher liegt, Staatlichkeit nicht am Gewaltmonopol – sondern an der Fähigkeit zur Initiierung und Kontrolle gesellschaftlicher Prozesse zu erkennen. Es erscheint deswegen unmodern und nicht sachgerecht, für den Cyberspace die Existenz von „Cybergewalt“ zu fordern. Der Cyberspace ist indes weder staatlich noch staatsähnlich organisiert, weshalb sich die überkommene Gewaltenteilungsperspektive nur in einer Grobgliederung zugrunde legen läßt. Die Legislative wird vom Landesgesetzgeber (Mediendienstestaatsvertrag), vom Bundesgesetzgeber (Teledienstegesetz) und vom europäischen „Gesetzgeber“ wahrgenommen (E-Commerce-Richtlinie). Die Judikative (nicht nur der drei Disziplinen in der Bundesrepublik) wird mit Cyberlawsachverhalten befaßt.[122] Die Administrative erfolgt zum einen durch die ICANN[123], zum anderen durch die DENIC eG – die beides Ausprägungen sogenannter „regulierter Selbstregulierung“ sein könnten. [124]

Von zentraler Bedeutung für den Kontakt des Bürgers mit dem Cyberspace (Administrative), sind privatrechtlich organisierte Suchmaschinen, wie etwa „Google“, die – soweit kein Vorwissen besteht – den Kontakt der Cyberpublic untereinander vermitteln. „Google“ fungiert damit als Rankinginstrument der Informations“eliten“ – ein Element des Cyberspace, über dessen Korrelat in der „realen Welt“ man länger nachdenken müßte. Die Gubernative des Cyberspace ist unbesetzt. Eine Regierung, die etwa Leitentscheidungen (Art. 65 GG) fällen oder über Kompetenzen in der „auswärtigen Gewalt“[125] verfügt, hat der Cyberspace nicht. Der Cyberspace selbst ist deswegen unqualifiziert, um auf Herausforderungen von Cross-Border-Sachverhalten (siehe unter IV. 2.) zu reagieren. Für die Zukunft deutet sich

[121] *A. Voßkuhle*, „Regulierte Selbstregulierung“ – Zur Karriere eines Schlüsselbegriffs, in: Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Die Verwaltung, 2001, Beiheft 4, 197, 200; *ders.*, Beteiligung Privater an öffentlichen Aufgaben und staatliche Verantwortung, S. 310ff. zum „Gewährleistungsverwaltungsrecht“, in: VVDStRL 62 (2003), 266.

[122] Strafgerichte: LG München I, Urt. v. 17.11.1999, MMR 2000, 171ff. „CompuServe-Urteil“: Strafbarkeit eines Access-Providers; Verwaltungsgerichte: Fn. 46 Sperrungsverfügung gegen Provider; Zivilgerichte: Fn. 113 irreführende Domain „rechtsanwalt.com“.

[123] Hierzu etwa: *Boehme-Neßler* (Fn. 78), S. 8, 92ff.; *Hoeren* (Fn. 9), S. 27ff.; http://www.icann.org .

[124] *Vassilaki* (Fn. 92), S. 747; für das us-amerikanische Recht für die ICANN mit der Terminologie „private ordering“ belegt: *S. L. Schwarcz*, Private Ordering, Northwestern University Law Review 97 (2002), 319, 344ff.

[125] *O. Rojahn*, in: I. v. Münch/P. Kunig (Hrsg.), Grundgesetz-Kommentar, Band 2, 5. Aufl. 2001, Rn. 19ff. zu Art. 59.

mit dem Abschluss multilateraler völkerrechtlicher Verträge wie der Convention on Cybercrime (CCC) an, dass nationalstaatliche Regierungen konzertiert die Rahmenbedingungen für die Strafverfolgung im Cyberspace konturieren.

(2) Technizität

Mit den Filterinstrumenten (etwa Firewalls) ist bereits die große Bedeutung der Technik für die Effektivität und Effizienz von (Cyber-)Governance hervorgehoben worden (siehe unter IV. 1. c)). Auch pseudo-administrative Suchmaschinen wie „Google“ drohen technisch manipuliert zu werden. In Erinnerung gerufen sei: Wer Google – und hierzu sind Fundstellen überflüssig – aufruft, erwartet die beste Navigation, die im Cyberspace erreichbar ist. Die Kommerzialisierung des Internets droht diese Oligarchie im Sinne des Bildes von Aristoteles zu einer Ochlokratie zu verwandeln. Die Werbeindustrie sucht nach Mitteln, um das Ranking von Google zu beeinflussen (und so Einnahmen für das Angebot von Homepages mit hohen Ranks zu generieren). Google kann sich demgegenüber nur auf die Sophistikation der Technik (Algorithmen) und inzwischen und vorläufig auf die amerikanische Rechtsprechung berufen.[126]

2. Cross-Border-Sachverhalte und -Personen

a) Begriff

Virtuelles und reales Leben sind voneinander nicht mit einer „Berliner Mauer“, die mit Minen bewehrt ist, getrennt. Beide Lebensräume beeinflussen sich gegenseitig, wie sich anschaulich am Beispiel von Cyberpersonalities zeigen lässt. So trifft man in der realen Welt eine Person (Dr. Jekyll), die im virtuellen Leben eine weitere Haut (Mr. Hide) hat. So präsentieren sich etwa Studenten mit ihren Freunden, Reise- und Studienerfahrungen mit eigenen Homepages im Cyberspace. Sie gewähren so Einblicke in ihre Kreativität wie auch – in der realen Welt würde man es so bezeichnen – ihr

[126] http://www.heise.de/newsticker/data/jo-28.01.03-001/ (28.02.2003)“Google darf Suchmaschinenoptimierer ausbremensen“ berichtet von der gerichtlichen Behandlung des Versuchs des Suchmaschinenoptimierers „SearchKing“ die „Integrität“ des Rankingsystems zu beeinträchtigen. Google hatte als „Höchststrafe“ SearchKing aus dem System entfernt.

Familien- und Freundesalbum sowie in ihre Tagebücher.[127] Die Persönlichkeit dieser Cyberpersonalities teilt sich in eine reale und eine virtuelle Präsentation. Die gesellschaftlichen und rechtlichen Folgen, die diese Präsentationen haben, sind nicht eindeutig absehbar. Sollen solche Persönlichkeiten wie „Personen der Zeitgeschichte"[128] in Zukunft im Urheber-, Medien- und Zivilrecht weniger Anspruch auf Schutz der Intimsphäre haben? Jedenfalls wird, falls sich diese Intimisierung des Internets verbreiten sollte, auch die Nichtexistenz einer privaten Homepage Schlussfolgerungen auf die reale Persönlichkeit einer natürlichen Person ermutigen. Einen Schritt weiter werden in der Literatur bereits Akteure genannt, die als „Cyborgs" bezeichnet werden.[129] Es handelt sich um Organismen, die über „Maschinenbestandteile" verfügen (und dadurch ihre Funktions- oder Lebensweise ändern). So futuristisch wie das klingen mag, sind diese „Cyborgs" nicht. Es gibt zum einen Menschen, die mit künstlichen Organen leben und es gibt Tiere, deren Verhalten mit einoperierten Chips erfasst und in der Zukunft verändert werden soll.[130] Auch der Schutz von Kindern in einem bestimmten Alter mag in der Zukunft solchen Visionen Realität verleihen. Vorstellbar wäre ein Chip, der mit einem Satellitennavigationssystem verbunden ist, und die Kinder vor dem Beschreiten von Strassen oder Flüssen warnt.[131]

b) *Methodische Herausforderung*

Cross-Border-Sachverhalte verlangen eine multi- und transdisziplinäre Kompetenz des Lawmakers – sei er im Rahmen der Gesetzgebung, der Rechtsprechung oder der Verwaltung mit diesen Sachverhalten konfrontiert. Ein Beispiel ist die Diskussion um ein „Gesetz über die Einführung des elektronischen Rechtsverkehrs bei den Gerichten" (Elektronisches Rechtsverkehrsgesetz – ERVG), das vom Bundesjustizministerium entworfen wird. Zwei kommentierende Richter kommen zu dem Ergebnis, dass der aktuelle Entwurf keine Verbesserung für die Praxis verspricht: „Diese Vor-

[127] Beispiele: www.mkhahn.de oder www.powderstyle.de; *N. Döring*, Öffentliches Geheimnis (Online Tagebücher – ein paradoxer Trend im Internet), c't 2001, 88, 92, die diese Autoren als „gläsern, aber glücklich" beschreibt.

[128] Im Sinne von § 23 KUG.

[129] http://pespmc1.vub.ac.be/ASC/cyborg.html (28.02.2003).

[130] Bekannt sind etwa Programme mit Elefanten und Vögeln, deren Fortbewegungsrouten aufgezeichnet werden sollen.

[131] Für gefahrbringende Geräte existieren solche Schutzvorrichtungen schon, Der Spiegel, 32/2002, 150 „Computer verpetzt Fahrsünden, berichtet von einem Fahrtenschreiber für jugendliche Autofahrer, das signifikante Geschwindigkeitswechsel oder heftige Lenkmanöver registriert und Warntöne ausstößt.

schrift, ernst genommen, zwingt dazu, bei jedem Ausdruck eines elektronischen Textdokuments den Text am Bildschirm laut vorzulesen und eine zweite Person den Text vergleichen zu lassen."[132] Ein weiteres Beispiel ist der Versuch, Leistungen in der realen Welt nur unter Voraussetzungen anzubieten, die Vermarktungschancen in der virtuellen Welt versprechen (Koppelungsgeschäfte). So kam die Münchner Informationstechnologie-Fachmesse (IT-Fachmesse Systems) „auf die Idee, die Daten sämtlicher Besucher zu erfassen, um sie anschließend für gezielte (E-Mail, Anm. d. V.) Werbeaktionen zu nutzen. Ohne Preisgabe von Name, Anschrift, E-Mail-Adresse und Interessengebiet gab's keine Eintrittskarte (...) Immerhin bot die Prozedur ein Opt-Out-Kästchen, um der Nutzung der Daten zu widersprechen. Dies tat so mancher, doch vergeblich. Ende Dezember (2002, Anm. d. V.) erhielten alle registrierten Besucher die Ausgabe 1 des „Systemworld Businessesletter".[133] Ein drittes Beispiel für diese Herausforderungen ist die Organisation des Fahrkartenverkaufs durch die Bahn. Nicht nur, dass der Bahnfahrer sich beim Intraneteinkauf Bahnverwaltungswissen aneignen soll und so frühere Funktionen von Bahnbeamten übernimmt; vielmehr wird die Präsenz an den realen Fahrkartenschaltern eingeschränkt, was die Chance erhöht, dass nicht internetkundige Teile der Bevölkerung zu „Schwarzfahrern" (free rider) werden (müssen). Diese Entwicklung birgt die Gefahr eines „social divide".

Mit dieser Beschreibung aktueller Fragestellungen sind die Aufgaben für die Zukunft bereits angedeutet.

3. Zukunftsoptionen: Konservatismus- und Erneuerungsthese

Die grundsätzlichen Positionen, die schwarzen und weißen Teile von Yin und Yang, finden sich exemplarisch in einer Zeitung für Informatiker. Eine Position verlangt im Sinne einer hier so bezeichneten Konservatismusthese nach dem „Staat im Cyberspace". Kein Vertrauen in die Selbstregulierung („Trust in Cyberspace"), sondern Electronic Law Enforcement sei gefordert.[134] Hinter dieser Ansicht steckt das Postulat, dass der Cyberspace paral-

[132] *W.Viefhues/H.Hoffmann*, ERVG: Gesetz zur Verhinderung des elektronischen Rechtsverkehrs?, MMR 2003, 71,74.

[133] *H. Dambeck*, Systems-Besucher erhalten unerwünschte Post c't 3/2003, S.55.

[134] *H. Fiedler*, Der Staat im Cyberspace, Informatik-Spektrum 24 (2001) 5, S. 309-314 und *A. Rossnagel*, Freiheit im Cyberspace, Informatik-Spektrum 25 (2002) 1, S. 33-38: andernfalls läge ein „Selbstmord des Rechtsstaats" vor.

lel zur realen Welt rechtlich zu ordnen sei. Auch die Gegenthese – hier als Erneuerungsthese bezeichnet – wird vertreten. So sei ein Konzept der regulierten Selbstregulierung zu wählen, das gerade das Eliten- und Nischenwissen der Cyberpersönlichkeit achtet und honoriert: „Privacy Enhancing Technologies" mit den Möglichkeiten der Verschlüsselung und Steganographie, Signaturen, Anonymität und Pseudonymität erweisen sich somit als moderne Formen des Schutzes von Individual- und Allgemeininteressen".[135] Das Technikwissen und die finanziellen Möglichkeiten zu seiner Anwendung in der Praxis werden so zu Vorrausetzungen der effektiven Verwirklichung von Freiheit(srechten) wie Datenschutz (wie man „Privacy" in diesem Zusammenhang übersetzen müßte). Es ist vorhersehbar, dass diese Forderung zu einem Intellectual Divide im Cyberspace führen wird.[136] Beide Thesen sollen für diesen Beitrag in ihrer Kontroversität nur präsentiert werden; gemein ist beiden Thesen, dass die Freiheit im Cyberspace weitere technische und/oder rechtliche Schutzvorkehrungen verlangt.

4. Zukunftsoptionen: Kommerzialisierung des Cyberspace

Der Grund, wieso die Sicherung dieser Freiheit zu diskutieren sein wird, ist die Kommerzialisierung des Cyberspace. Die Technik hat im Sinne der Erneuerungsthese die reale Welt überholt. Diejenigen, die Rechte in dieser realen Welt haben, stehen nun vor der Aufgabe, diese Rechte im Cyberspace zu verteidigen. Ein Beispiel ist die Musikindustrie, die sich gegen Raubkopien wendet. So hat ein amerikanisches Gericht einen Provider verpflichtet, den Namen eines Nutzers bekannt zu geben, ohne dass vorher (gerichtlich) festgestellt wurde, dass eine Urheberrechtsverletzung vorlag.[137] Die „Organisation" von Daten erfolgt also nicht mehr nur zum Schutz des Allgemeinwohls – wie bei der Prävention und Sanktion von Straftaten – sondern wird zunehmend privatnützig. Diese Privatnützigkeit stellt dann die altbekannte Frage nach der Freiheit des Einen, die die Unfreiheit des anderen sein kann.

---

135 *Roßnagel* (Fn. 133), S. 33, 37.

136 Jeder der Inhalte über das Medium Internet transportiert oder transportieren läßt, wird sich Gedanken über die Sicherheit und Vertraulichkeit dieses Transportmittels machen müssen. Siehe auch die Inititiative des Bundesminsteriums für Wirtschaft und Technologie, GnuPP für Durchblicker (Hintergrund-KnowHow zum E-Mail-Verschlüsselungsssystem GnuPP.

137 http://www.heise.de/newsticker/data/anw-31.01.03-000/ (28.02.2003) Provider will sich mit allen Mitteln gegen die Musikindustrie wehren (zur Rechtssache Verizon).