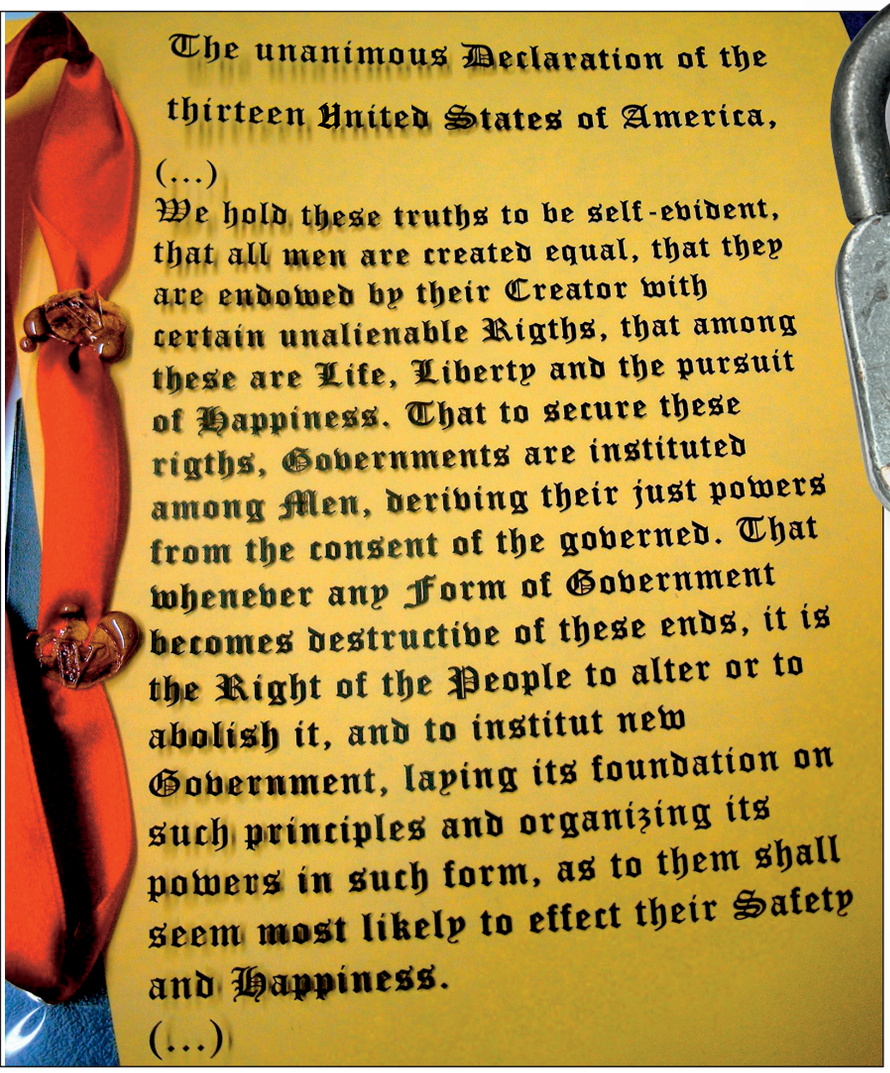
(IT-)Sicherheit durch Cyberlaw?

Prof. Dr. Viola Schmid



1776 empfahl die amerikanische Unabhängigkeitserklärung den Bürgern eine Regierung, die ihnen „Safety“ und „Liberty“ gewähre und „Pursuit of Happiness“ unterstütze.[1] Sicherheit („Safety“) und Freiheit („Liberty“) sind jahrhundertealte Konstanten der Staatlichkeit, die sich bis in den jüngsten europäischen Verfassungsentwurf des „Konvents für die Zukunft Europas“ vom 18. Juli 2003 fortsetzen, der in Art. 41 bestimmt:

„The Union shall constitute an area of freedom, security and justice“.[2]

Der Beitrag von IT-Systemen zur Erbauung dieses „sicheren Raums“ wird von den Verfassungsgebern vorausgesetzt, wenn sie fortfahren:

„Die Union bildet einen Raum der Freiheit, der Sicherheit und des Rechts ... durch operative Zusammenarbeit der zuständigen Behörden der Mitgliedstaaten einschließlich der Polizei, des Zolls und anderer auf die Prävention und die Aufdeckung von Straftaten spezialisierter Behörden.“

Sicherheit als Prävention und Sanktion von Verbrechen setzt Wissen voraus. Die (Europäische) Union will ihr Wissen durch IT-Systeme vermehren beziehungsweise unter den Mitgliedsländern verteilen. Denkbar sind zwei Strategien: zum einen der Aufbau von europäischen Behörden und Daten-„organisations“systemen[3] (etwa Europol[4]) und zum

[1] …it is the Right of the People…to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness.

[2] Zukünftiges Recht: Art. 41 und Art. 3 Abs. 2 des Entwurfs eines Vertrags für eine Verfassung für Europa (Europäischer Verfassungsentwurf). Geltendes Recht: Art. 29 des Vertrags über die Europäische Union (EU).

[3] „Organisation“ wird hier als Oberbegriff für die Erhebung, Verarbeitung und Nutzung im Sinne von § 3 Abs. 3-5 BDSG verwandt.

[4] Art. 30 Abs. 1 b) EU: Das gemeinsame Vorgehen im Bereich der polizeilichen Zusammenarbeit schließt ein: …das Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen, einschließlich Informationen der Strafverfolgungsbehörden zu Meldungen über verdächtige finanzielle Transaktionen, insbesondere unter Einschaltung von Europol, wobei die entsprechenden Vorschriften über den Schutz personenbezogener Daten zu beachten sind;…

IT-Security via Cyberlaw?

As a young discipline in the Law, Cyberlaw is a work-in-progress whose content is being defined and whose options are being explored as technology changes. What is „Cyberlaw," and what are its potential contributions to IT-security, in particular, and to public security and private safety, in general? This article takes a legal and philosophical approach to the discussion of security and liberty - with reference to actual developments in European legislatures and the German and European Data Protection Laws. Examples include injunctions ordering Internet providers to block web sites containing hate speech, access of the US-Administration to personal data of flight passengers in Europe, and storage of dynamic uniform resource locators by providers. Such examples characterize in part the internationality, the technical reference, the perspectives and the limits of this new discipline in the Law. The conclusion reached herein is that, in spite of technical, economic and legal challenges, IT-Security and Cyberlaw are necessary prerequisites to maintaining freedom, security and justice in Europe.

anderen die Förderung der Interoperabilität von mitgliedstaatlichen Behörden und Datenorganisationssystemen untereinander. Allein die Komplexität und Quantität dieser sicherheitsrechtlichen Zusammenarbeit verlangt nach IT-Sicherheit. De facto sind Prozesse der Datenorganisation nicht mehr auf einen Mitgliedstaat oder die (Europäische) Union beschränkbar – Datenorganisationen via Cyberspace sind international, wie etwa der Zugriff amerikanischer Zoll- und Grenzschutzbehörden[5] auf die Fluggastdaten von (europäischen) Fluggesellschaften zeigt. Diese Internationalität der IT-Systeme verlangt, dass sie, wenn sie sicherheitspolitisch eingesetzt werden, selbst sicher (und selbstsicher) sind. Andernfalls würde IT-Sicherheit zu einem zusätzlichen Risiko für die Sicherheit. Auch diese Gefahr lässt sich anhand des europäisch-amerikanischen Konflikts über die „Organisation" von Fluggastdaten belegen. Wie auch immer man diesen transatlantischen Zugriff datenschutzrechtlich bewerten mag – sicherheitsrechtlich ist evident, dass es Kriminellen nicht ermöglicht werden soll, die Angriffsziele sophistiziert zu ermitteln, indem sie die potentiellen Opfer zwischen den Fluggästen konkreter Routen informiert auswählen. Diese Gefahr ist nicht zu gering einzuschätzen, wenn man den Inhalt der Daten[6] in Betracht zieht. Zusammengefasst: Sicherheit durch IT-Systeme; aber keine Sicherheit ohne IT-Sicherheit.

A. Was ist (IT-)Sicherheit?

Auffallend ist in beiden Rechtstexten der unterschiedliche Sprachgebrauch – die ältere amerikanische Unabhängigkeitserklärung strebt nach „Safety", der jüngere europäische Verfassungsentwurf nach „Security". Beiden Begriffen entspricht im Deutschen „Sicherheit". Für die Sicherheit in der Informationstechnologie (IT-Sicherheit) differenziert Claudia Eckert[7] zwischen „Safety" als Funktions- und „Security" als Informationssicherheit. Jenseits dieser grundsätzlichen Differenzierung gilt: „Begriffsauffassungen zum Thema Sicherheit in der Informationstechnologie gibt es viele."[8] Diese Diversität erschließt sich auch für die „Sicherheit" im Rechtssystem: So definieren Gesetze[9] und ISO-Standards[10] für den jeweiligen territorialen, personalen und objektiven Geltungsbereich (IT-)Sicherheit unterschiedlich. Die informationstechnische Differenzierung zwischen „Safety" und „Security" lässt sich im Grundsatz auch für das Recht belegen. So verwendet der Vorschlag zur Gründung einer „Europäischen Agentur für Netz- und Informationssicherheit" vom 11.2.2003 in der englischen Übersetzung konsequent „Security" („European Network and Information Security Agency").[11] Diese Agentur soll die oben zitierte, von der Europäischen Verfassung vorausgesetzte Interoperabilität von

[5] Geregelt im Aviation and Transportation Security Act vom 19.11.2001, zu finden unter http://www.house.gov/transportation/aviation/3150issues.html (10.11.2003). Den amerikanischen Behörden müssen nicht nur Daten übermittelt, es muss ihnen darüber hinaus der Zugriff auf die Fluggastdatenbank gewährt werden.

[6] So enthält etwa der PNR (Passenger Name Record) Fluggastdatensatz Informationen über Buchungsinformationen (Daten, Kreditkarteninformationen, etc.), Reisestrecke und Angaben zu Religion und Ethnie (Wahl des Menüs).

[7] Claudia Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 2. Aufl., 2003, S. 4, unter Funktionssicherheit (Safety) wird das Funktionieren eines Systems unter normalen Betriebsbedingungen verstanden; unter Informationssicherheit seine Resistenz gegenüber Angriffen.

[8] Martin Raepple, Sicherheitskonzepte für das Internet, 2. Aufl., 2001, S.3.

[9] § 2 Abs. 2 des Gesetzes über die Errichtung des Bundesamts für Sicherheit in der Informationstechnik („Sicherheit in der Informationstechnik…bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen…") verzichtet in grammatischer Auslegung auf die Authentifizierung, die etwa in dem Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Gründung der Europäischen Agentur für Netz- und Informationssicherheit enthalten ist („…Netz- und Informationssicherheit bieten…eine zuverlässige Authentifizierung, d.h. die Bestätigung einer behaupteten Identität von…Nutzern…").

[10] Vgl. Karl L. Lincke/Jesús Sanchez Echeverría, Die neue ISO/IEC 17799 – Sicherheitsverwaltung von Informationen, ecolex 2003, 382-385.

[11] Vorschlag des Europäischen Parlaments und des Rates zur Gründung der Europäischen Agentur für Netz- und Informationssicherheit KOM(2003)63 endgültig vom 11.2.2003.

unterschiedlichen IT-Sicherheitsprodukten wie die Sicherheit der Netze fördern (siehe oben zu Art. 41 des Europäischen Verfassungsentwurfs). Aus rechtswissenschaftlicher Sicht ist festzuhalten, dass eine Definition der IT-Sicherheit normspezifisch ermittelt werden muss.[12] Regelmäßig setzt IT-Sicherheit im Kontext von Sicherheitspolitik „Safety“ und „Security“ voraus: Sicherheitsrelevante Daten müssen nicht nur effektiv und effizient organisiert werden, sondern – wie beim Fluggastdatensachverhalt dargestellt – gegenüber Angriffen wehrfähig („resistent“) sein. Darüber hinaus gilt: Sicherheit und (IT-)Sicherheit gilt es zu optimieren– und nicht „nur“ zu definieren. Bevor nunmehr der Beitrag des Cyberlaw zur (IT-) Sicherheit dargestellt werden kann, bedarf es einer weiteren Begriffsbestimmung.

B. Was ist Cyberlaw?

Cyberlaw, wie es an der TUD gelehrt und erforscht wird, ist ein multi- und transdisziplinäres Rechts„gebiet“, das für die Voraussetzungen für E-Government (Electronic Government), E-Commerce (Electronic Commerce) im Besonderen und für E-Liberty (Electronic Liberty) im Allgemeinen sorgt.[13] Der Cyberspace als von der Technik geschaffener Raum wird sowohl von Privaten als auch von Staaten genutzt: Private wollen Handel treiben (E-Commerce), im Cyberspace reisen (surfen) und sich etwa mit Homepages und so genannten Weblogs („elektronischen Tagebucheinträgen“) freiheitlich verwirklichen (E-Liberty). Staaten und die (Europäische) Union wollen die drei Gewalten – Legislative, Exekutive und Judikative – „elektronisieren“ (E-Democracy, E-Government und E-Justice). Sowohl die Ausübung privater Freiheit (E-Liberty) als auch hoheitlicher Gewalt (E-Government) verlangen nach (Vertrauen in die) Funktionalität der IT-Systeme, Identifizierung und Authentifizierung von Cyberakteuren. IT-Sicherheitsrecht ist ein Teilbereich des Cyberlaw, der sich mit der Sicherheit der Infrastrukturen des Cyberspace, der informationellen Grundversorgung als Voraussetzung für die Freiheit der Cyberakteure und dem Schutz vor rechtswidrigen Inhalten befasst. Grundsätzlich stellt sich die Frage, wie viel (IT-) Sicherheit das Recht im Allgemeinen und das Cyberlaw im Besonderen verlangen kann oder muss. Dieser Frage soll zunächst anhand der traditionellen Trias von Freiheit, Sicherheit und Recht und ihrer funktionalen Korrelation („durch“) nachgegangen werden.[14] Bereits an dieser Stelle ist darauf hinzuweisen, dass die herausfordernde Konstellation „(IT-)Sicherheit durch (IT-)Freiheit“ ist.

C. Freiheit durch Sicherheit durch Recht – und vice versa?

	Freiheit	Sicherheit	Recht
Freiheit		Sicherheit durch Freiheit	Recht durch Freiheit
Sicherheit	Freiheit durch Sicherheit		Recht durch Sicherheit
Recht	Freiheit durch Recht	Sicherheit durch Recht	

	Freiheit	Sicherheit	Recht
Freiheit		Sicherheit contra/via Freiheit	EU-Verfassung
Sicherheit	Untersuchung des Gepäcks von Fluggästen		Untersuchung des Gepäcks von Fluggästen
Recht	Datenschutz	Art. 41 EU-Verfassung	

Ein Beispiel dafür, dass **„Freiheit durch Sicherheit“** gefördert werden kann, ist die Untersuchung des Gepäcks von Fluggästen. Ohne diese Untersuchungen würden insbesondere nach den Ereignissen des 11. Septembers 2001 weniger Menschen von ihrer Reisefreiheit (im deutschen Recht: Art. 11 Grundgesetz) Gebrauch machen. Ein Beispiel für **„Freiheit durch Recht“** ist die Entwicklung „neuer“ Grundrechte durch das Bundesverfassungsgericht, das bereits 1983 das Recht auf informationelle Selbstbestimmung „entwickelte“ und eine staatliche Volkszählung als ver-

[12] Nach dem Urteil des LG Hamburg v. 31.10.2002 (MMR 2003, 340) ist es irreführend (§ 3 des Gesetzes gegen den unlauteren Wettbewerb), wenn ein Provider damit wirbt, dass der Netzzugang „sicher“ sei.

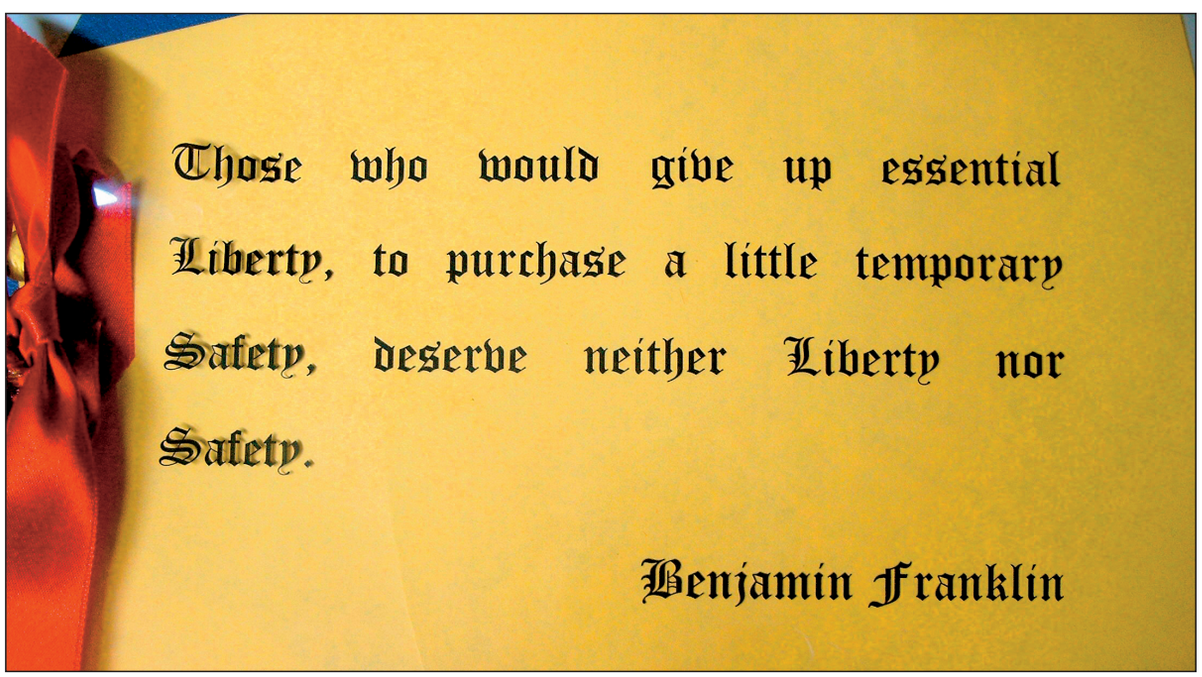
[13] Eingehender dieselbe, Cyberlaw eine neue Disziplin im Recht, in: Hendler/Marburger/Reinhardt/Schröder Trierer Jahrbuch zum Umwelt- und Technikrecht 2003 (UTR 71), S. 449-480.

[14] Die Paarungen „Freiheit durch Freiheit“, „Sicherheit durch Sicherheit“ und „Recht durch Recht“ sind ausgeblendet, weil sie keine weiteren Erkenntnisse versprechen.

fassungswidrig untersagte.[15] **„Sicherheit contra Freiheit“** war und ist die Herausforderung der Vergangenheit, der Gegenwart und der Zukunft. Bereits vor der zitierten Unabhängigkeitserklärung wird Benjamin Franklin für das Verhältnis von Sicherheit zu Freiheit 1755 folgende Warnung zugeschrieben:[16]

Es gäbe demnach einen Kernbereich von Freiheit („Essential Liberty“), der nie für (zeitweilige) Sicherheit („Temporary Safety“) aufgegeben werden solle. Dass des einen Sicherheit des anderen Unfreiheit sein kann, wird bei unterschiedlichen Bewertungen der Sicherheitslage deutlich. Vielgründlichen, teuren und langwierigen Prüfung von Gepäck und Personen absehen wollen, weil ein Angriff nur mit geringer statistischer Wahrscheinlichkeit erfolgen wird. Es bedarf hier der Entscheidung des Gemeinwesens, der res publica, wie die Preisgabe von Freiheit für die Erreichung von Sicherheit zu bewerten ist, damit als Ergebnis dieses Abwägungsprozesses die Chance auf die größtmögliche Ausübung von Freiheit („Pursuit of Happiness“) steht. Wegweisend bereits im Motto Benjamin Franklins ist die Andeutung der Notwendigkeit einer transdisziplinären Betrachtung, die technische und ökonomische Aspekte von (IT-)Sicherheit einbezieht. Er betont nämlich, dass (IT-)Sicherheit „eingekauft“ werden müsse („Purchase“) – und die Kosten von (IT-)Sicherheit sind auch in der heutigen Praxis ein kritischer Faktor. Umgekehrt bieten in der Zeit nach Franklin gerade sichere IT-Systeme Kosten- und Effizienzchancen für die Erhöhung von Sicherheit.

Moderner als die traditionelle Korrelation **„Sicherheit contra Freiheit“** ist die Idee von **„Sicherheit via Freiheit“.** Hier könnten aus der jüngeren Staatsrechtslehre viele Quellen zur modernen Bürgergesellschaft und zur Motivation der Bürger für den Staat (Vorstellungen über „Communitarian Society“ in den USA und Deutschland) beigetragen werden. Im Cyberspace ist diese moderne Korrelation von großer Bedeutung, weil der durch die Technik geschaffene Raum weder vom Staat noch von der (Europäischen) Union „beherrscht“ wird und deshalb - das wird im nächsten Abschnitt darzutun sein – das Engagement der Cyberpersonalities eine elementare Voraussetzung für IT-Sicherheit ist.



leicht wären einige Menschen[17] interessiert, schneller und flexibler zu reisen – zumal die Luftfahrttechnik genau dies seit Jahrhunderten unter Einsatz von Wissen und Menschenleben erstrebt und ermöglicht hat. Diese Reisenden würden von einer sehr

Ein Beispiel für **„Sicherheit durch Recht“** ist der eingangs

[15] BVerfGE 65, 1 ff.

[16] Das sehr populäre Zitat kursiert in Abwandlungen in der Literatur und Civil Rights Bewegungen und ist auch im Pedestal der Statute of Liberty eingelassen: „Those who would give up essential liberty to obtain a little safety deserve neither liberty nor safety.“

[17] Nach der ökonomischen Analyse des Rechts gibt es Personen, die „risk neutral“, die „risk aware“ und die „risk averse“ sind. Simplifiziert: Es gibt also Personen, die „uninteressiert“ sind, Personen, die Risiken und Chancen einschätzen wollen (bevor sie sich entscheiden zu reisen) und Personen, die nahezu jedes Risiko (ohne die Chancen bewerten zu wollen) ablehnen. Die statistische Verteilung dieser Präferenzen wie die Kosten der Sicherheitstechnik bereiten dann eine Entscheidung vor, in welche Techniken investiert und gegen welche schädigenden Ereignisse versichert werden solle. Zu IT-Risiken und ihrer Versicherbarkeit: Frank Romeike, Cyber Risks, http://www.risknet.de/Risk_Management/Themen/Cyber_Risk/cyber_risk.html (10.11.2003).

zitierte Art. 41 des Europäischen Verfassungsentwurfs, der auch die unionsweite Anerkennung und Vollstreckung mitglied-staatlicher Gerichtsentscheidungen fordert.[18]

„Recht durch Freiheit“ exemplifiziert auch der am 18. Juli 2003 beendete Konvent zur Zukunft Europas, bei dem Mitglieder von 28 Staaten eine europäische Verfassung entwarfen, der sich die Staaten freiwillig und freiheitlich unterwerfen sollen.

„Recht durch Sicherheit“ wird wiederum am Beispiel der Überprüfung von Fluggästen deutlich. Wie wollen die Staaten ihren verfassungsrechtlichen Schutzpflichten für Leib und Leben der Menschen genügen – wenn nicht durch Schaffung und Unterhaltung von Prozessen, Anlagen und durch die Auswahl von Personen, die eine Erhöhung von Sicherheit „versprechen“? Welche Änderungen ergeben sich, wenn man diese traditionelle Trias im Cyberspace diskutiert?

D. IT-Freiheit durch IT-Sicherheit durch Cyberlaw – und vice versa?

	IT-Freiheit	IT-Sicherheit	Cyberlaw
IT-Freiheit		Security aware Cyberpersonality	RFC
IT-Sicherheit	Funktionssicherheit und Resistenz (Safety+Security)		Vorratsdaten-speicherung
Cyberlaw	Sozialhilfe für PC?	§ 9 BDSG	

„IT-Freiheit durch IT-Sicherheit“ konturiert den Rahmen sowohl für „Safety“ als auch „Security“. Die Existenz der IT-Systeme wie ihre Resistenz gegenüber Angriffen (Viren, Würmer, Trojaner …) sind Voraussetzung für den Zugang zum Cyberspace und die Ausübung von IT-Freiheit.

Die Frage nach **„IT-Freiheit durch Cyberlaw“** stellte sich für das Oberverwaltungsgericht Lüneburg. Wenn ein PC zum „notwendigen Lebensunterhalt“ gehört, dann muss er von der Sozialhilfe finanziert werden.[19] Im Ergebnis hat das Gericht den Anspruch einer Gymnasiastin nach akribischer Beweisaufnahme und Einzelfallprüfung verneint. So deutet sich aber bereits an, dass sich deutsche Gerichte mit der Sicherung der IT-Grundversorgungsansprüche nicht finanzkräftiger Bürger (Digital Divide?) in Zukunft befassen müssen.

„IT-Sicherheit via IT-Freiheit“ überschreibt das Risiko und die Chance der Ausübung von Freiheit im Cyberspace. Unbestritten ist der Cyberspace ein technischer, und kein staatlicher Raum. So können Staaten das Internet filtern und/oder die Abschaltung von Servern anordnen – sie können aber derzeit weder die Existenz des Cyberspace garantieren noch ihn aufteilen noch die Existenz von Sicherheit selbst gewährleisten. Konzepte des Selbstdatenschutzes (etwa der Kryptographie) werden deshalb von der Bundesregierung gefördert und ihre Verbreitung im Wege der Öffentlichkeitsarbeit propagiert.[20] Ähnlich dem traditionellen Ideal des informierten Verbrauchers („Informed Consumer“) – der in einem von Angebot und Nachfrage bestimmten Wettbewerbsmarkt möglichst marktoptimale Allokationsentscheidungen treffen soll – verlangt IT-Sicherheit die „Security aware Cyberpersonality“ (SaCyp).

Ein Beispiel für **„IT-Sicherheit contra IT-Freiheit“** zeigt sich personalisiert auf der betrieblichen und behördlichen Ebene im Nebeneinander von Datenschutz- und IT-Sicherheitsbeauftragten. IT-Sicherheitsbeauftragte sollen die Anforderungen des Cyberlaw an die IT-Sicherheit in der Praxis kompetent, kontinuierlich und vorsorgend durchsetzen. Die **„IT-Sicherheit durch Cyberlaw“** versucht § 9 Bundesdatenschutzgesetz mit seinen anlagen- und prozessorientierten Anforderungen zu erhöhen, die nach der bevorstehenden Novellierung des Telekommunikationsgesetzes bei allen für die Öffentlichkeit angebotenen Telekommunikationsdiensten von einem IT-Sicherheitsbeauftragten organisiert und kontrolliert werden sollen.[21] Dass die Interessen der Arbeitgeber an einer Sicherung ihres IT-Systems (insbesondere der Security) durchaus im Widerspruch zum Interesse der „internet-mündigen“ Arbeitnehmer (als SaCyp) an einer auch privaten Nutzung des IT-Arbeitsplatzes stehen können, ist evident.[22]

Ein Beispiel für **„Cyberlaw durch IT-Freiheit“** sind die Requests for Comments, die den Cyberspace technisch mitgestalten und als in der jüngeren Staatsrechtslehre diskutierte „regulierte Selbstregulierung“ zu qualifzieren sein könnten. Die Selbstregulierung

[18] Die Union bildet einen Raum der Freiheit, der Sicherheit und des Rechts … insbesondere auf der Grundlage der gegenseitigen Anerkennung der gerichtlichen und außergerichtlichen Entscheidungen; …“.
[19] § 12 Bundessozialhilfegesetz; OVG Lüneburg, Urt.v.11.6.2003 Az. 4 LB 279/02.
[20] Siehe etwa die Initiative des Bundesministeriums für Wirtschaft und Technologie „GnuPP“.
[21] Bisher § 87 Abs. 2 Telekommunikationsgesetz für lizenzpflichtige Betreiber. Nach neuem Recht voraussichtlich § 107 Abs. 3 Telekommunikationsgesetz (Kabinettsbeschluss vom 15.10.2003).
[22] DSB 3/2003, S.10 zu einem Praktikerseminar „Rechtsfallen für IT-Sicherheitsbeauftragte.

gleicht das Spannungsfeld zwischen dem Steuerungsdefizit des Rechts und dem faktischen Bedürfnis nach (technischer) Normgebung aus.

Ein gerade aus Darmstädter Sicht relevantes Beispiel für **„Cyberlaw durch IT-Sicherheit“** ist die Organisation von Verbindungsdaten zur Protokollierung von Reisen im Cyberspace (Reisefreiheit im Cyberspace). Ein Dienstanbieter hatte dynamische IP-Adressen auch bei Flatrate-Kunden über die Verbindungszeit hinaus gespeichert. Die zuständige Datenschutzbehörde[23] beanstandete unter Berufung auf die Sicherheitsziele des § 9 BDSG diese Organisation von Daten nicht, weil die Prävention und Sanktion von „Angriffen“ eine Protokollierung der „IT-Reisen“ verlange. Das Cyberlaw verlange für seine Durchsetzung (etwa bei der Verfolgung von Urheberrechtsverletzungen oder der Reise zu strafrechtlich zu beanstandenden IT-Angeboten) nach Protokollierung. Das „IT-Szenario“ stellt sich so als Parallele zur „Realworld“ dar, in der Menschen über die Ausübung und Qualität ihrer Reisefreiheit selbst entscheiden wollen. Der Vollständigkeit halber ist darauf hinzuweisen, dass andere Datenschutzbehörden diese Logbuchhaltung für übermäßig und rechtswidrig erachteten.[24] Die Frage der Organisation und Verfügungsmacht über Verbindungsdaten beschäftigt in den USA bereits die Gerichte: Dort sehen sich die Provider Auskunftsansprüchen[25] der Musikindustrie ausgesetzt, die mit der Behauptung von Urheberrechtsverletzungen die Protokolle einsehen wollen.

E. Beitrag des Cyberlaw zur (IT)-Sicherheit?

Die vorangehenden Abschnitte wollten das Arbeitsprogramm eines Cyberlaw, das sich mit „Security“ und „Safety“ befasst, konturieren. Die Virtualität, Technizität und Internationalität dieser Rechtsdisziplin sowie ihre rechtspolitischen und rechtsphilosophischen Herausforderungen verlangen den Diskurs mit den Technikwissenschaften und die Suche und das Ringen um die „Lösung“ – eine Lösung, die Sicherheit und Freiheit in ein angemessenes Verhältnis zueinander bringt. Vorläufig kann das Recht vor allem einen strukturierenden Beitrag für diesen Diskurs und den Weg zur Lösung zu finden.

Festzuhalten ist: Auch wenn gegenwärtig viele Lösungen erst erforscht und diskutiert werden müssen – die Entscheidung darüber, dass ein Raum der Freiheit, der Sicherheit und des Rechts geschaffen werden muss, ist bereits gefallen.

[23] Die zuständige Datenschutzbehörde ist das Regierungspräsidium Darmstadt.
[24] Das Unabhängige Landeszentrum für Datenschutz Schleswig Holstein ist der Ansicht: „Die dynamische IP-Nummer, die der Access-Provider einem Kunden zeitweilig zuweist, ist jedoch nicht zum Schutz der eigenen Datensicherheit des Anbieters erforderlich.“ Pressemitteilung vom 16.1.2003 unter http://www.datenschutzzentrum.de/material/themen/presse/ipspeich.htm (10.11.2003).
[25] Der Telekom-Konzern Verizon wurde von dem United States District Court for the District of Columbia verurteilt, Daten eines Nutzers an den Verband der Musikverleger RIAA herauszugeben. Der Nutzer wurde verdächtigt, illegale Raubkopien gemacht zu haben.

Informationen zum Fachgebiet Öffentliches Recht an der TU Darmstadt

Das Fachgebiet wurde zum 1.9.2002 besetzt und wird im Fachbereich Rechts- und Wirtschaftswissenschaften durch Frau Prof. Dr. jur. Viola Schmid, LL.M. (Harvard) in Forschung und Lehre vertreten.

In der Forschung konzentriert sich das Fachgebiet auf zwei Themenbereiche, nämlich zum einem auf das Umwelt- und Technikrecht und zum anderen auf die Etablierung eines in Deutschland neuen Forschungsgebiets, des Cyberlaw. Diese Kombination birgt den Vorteil, dass die aus dem Umwelt- und Technikrecht bekannte Chancen-, Risiko- und Technikfolgenabschätzung tentativ auf die (Nicht-)Steuerung eines von der Technik geschaffenen Raums – des Cyberspace – übertragen wird. In der Grundlagenforschung werden die geltenden wie die zu schaffenden rechtlichen Regelungen für Biometrie und Kryptographie untersucht bzw. entworfen. Neben den völker- und europarechtlichen Rahmenbedingungen für deutsches Cyberlaw versucht das Fachgebiet, amerikanisches Cyberlaw rechts- und technikvergleichend in die Forschung und Lehre zu integrieren und zu diskutieren.

„Öffentliches Recht“ an der TUD ist „veröffentlichtes Recht“. Die wesentlichen Lehrinhalte und Gesetzgebungsmaterialien sind in Online-Skripten zugänglich. Für die Erstsemester-Veranstaltung „Grundzüge des Öffentlichen Rechts“ stellt das Fachgebiet eine Lernplattform zur Verfügung, die im Laufe des Jahres 2004 durch ein internetgestütztes Recherchespiel ISJ (Interactive Studies of Jurisprudence) ergänzt werden soll.

Dieses Projekt wird von dual mode TUD unterstützt.

Kontakt
TU Darmstadt
Fachgebiet Öffentliches Recht
Prof. Dr. V. Schmid

Hochschulstr. 1
64289 Darmstadt
Tel.06151/16-6464 · Fax 06151/16-3984

E-Mail: cyberlaw@jus.tu-darmstadt.de
Für die USA: Berkman Center an der Harvard Law School,
http://cyber.law.harvard.edu/ilaw