Prof. Dr. Viola Schmid, LL.M. (Harv.)

TUD Fachgebiet Öffentliches Recht /cyberlaw@jus.tu-darmstadt.de

CAST Workshop: Recht und IT-Sicherheit

22.04.2004

Grundlagen des Sicherheitsrechts für IT-Systeme (SITS)

A. IT-Sicherheit im Völker-, Europa- und deutschen Recht

B. Datenschutz via/contra Datensicherheit via/contra IT-Sicherheit?

C. (Verkehrssicherungs-)Pflichten bei Privaten zum Schutz vor Dialern

[Bundesgerichtshof Entscheidung vom 4.3.2004 Az. III ZR 96/03]

A. IT-Sicherheit im Völker-, Europa- und deutschen Recht

Rechtsordnungshierarchie

Rechtsnormenhierarchie

- Völkerrecht: - Convention on Cybercrime ; Two OECD Guidelines
  - [OECD Guidelines for Security…: 9 Prinzipien →
    Prinzip Nr. 8: „Security management" (soft law)]

A. IT-Sicherheit im Völker-, Europa- und deutschen Recht

Rechtsordnungshierarchie

Rechtsnormenhierarchie

- Völkerrecht: - Convention on Cybercrime ; Two OECD Guidelines
  - [OECD Guidelines for Security…: 9 Prinzipien → Prinzip Nr. 8: „Security management" (soft law)]
- Europarecht: - Verordnung: European Network and Information Security Agency (www.enisa.eu.int)
  - Datenschutzrichtlinie für elektronische Kommunikation (Art. 4 Datensicherheit und Art. 13 Schutz vor Spams)

A. IT-Sicherheit im Völker-, Europa- und deutschen Recht

Rechtsordnungshierarchie

Rechtsnormenhierarchie

- Völkerrecht: - Convention on Cybercrime ; Two OECD Guidelines
  - [OECD Guidelines for Security…: 9 Prinzipien → Prinzip Nr. 8: „Security management" (soft law)]
- Europarecht: - Verordnung: European Network and Information Security Agency (www.enisa.eu.int)
  - Datenschutzrichtlinie für elektronische Kommunikation (Art. 4 Datensicherheit und Art. 10 Schutz vor Spams)
- Deutsches Recht: - § 9 Bundesdatenschutzgesetz (BDSG)
  - § 10 Hessisches Datenschutzgesetz (HDSG)
  - § 87 Abs. 2 Telekommunikationsgesetz (TKG)

Rechtsnormenhierarchie

Rechtsordnungshierarchie

Völkerrecht: Charakteristika

- keine Unmittelbarkeit: muss grundsätzlich durch deutschen Gesetzgeber transformiert werden
- abgeschwächte Bindung (soft law?) gerade OECD Guidelines
- grundsätzlich für private Kläger nicht einklagbar (Ausnahme: Europäische Menschenrechtskonvention, …)

Rechtsnormenhierarchie

Rechtsordnungshierarchie

Europarecht

- europäische Verordnung: unmittelbare Geltung in Europa: ENISA
- europäische Richtlinie: grundsätzlich Transformation

  (Art. 13 und Art. 4 der Datenschutzrichtlinie) ➔Schutz vor Spams ➔ § 7 des Entwurfs des Gesetz gegen den unlauteren Wettbewerb in der Fassung 24.3.2004 – Rechtsausschuss des Bundestags

  (FAZ v.6.4.2004: Vertragsverletzungsverfahren)

- Einklagbarkeit vor deutschen Gerichten und Europäischem Gerichtshof

CyLaw

IT-Sicherheit im Völker-, Europa- und deutschen Recht

Rechtsordnungshierarchie

Rechtsnormenhierarchie

Bundesrecht	Landesrecht
Grundgesetz Bundesgesetz Rechtsverordnung Satzung	Landesverfassung Landesgesetz Rechtsverordnung Satzung

Beachte:

- Verwaltungsvorschriften = Innenrecht {Schwellach: Bremer Landesrichtlinie?}
- Technische Normen (Common Criteria 2.1, ISO/IEC 17799)
  → Selbstregulierung

CyLaw

Grundrecht auf Datensicherheit ? Theoretisches Szenario

Daten- und IT-Sicherheit

◆Normenhierarchie:➔ Verfassungsrecht➔einklagbar➔

Grundrecht auf Datensicherheit? Ausgangspunkt: Datensicherheit (DaSi) im Wortlaut der Verfassung nicht existent; aber:

kein Datenschutz (DaSchu) ohne Datensicherheit (DaSi); und

Datenschutz als Grundrecht

(„informationelle Selbstbestimmung” in Artikel 2 Absatz 1 und Artikel 1 Absatz 1 Grundgesetz)

geschützt → Datensicherheit **mit**geschützt

CyLaw

Grundrecht auf Datensicherheit ? Theoretisches Szenario

Relation „via"

Relation „contra"

Daten- und IT-Sicherheit

◆Normenhierarchie:➔ Verfassungsrecht➔einklagbar➔

Grundrecht auf Datensicherheit?: Ausgangspunkt: Datensicherheit (DaSi) im Wortlaut der Verfassung nicht existent; aber:

kein Datenschutz (DaSchu) ohne Datensicherheit (DaSi); und

Datenschutz als Grundrecht

(„informationelle Selbstbestimmung" in Artikel 2 Absatz 1 und Artikel 1 Absatz 1 Grundgesetz)

geschützt → Datensicherheit **mit**geschützt

◆Normenhierachie:➔Gesetzesrecht➔Schadensersatzpflichten nach §§ 7 und 8 Bundesdatenschutzgesetz und § 823 Abs. 1 Bürgerliches Gesetzbuch

Cy Law

Grundrecht auf IT-Sicherheit ? Visionäres Szenario

Relation „via"

Relation „contra"

Daten- und IT-Sicherheit

◆Normenhierarchie:➔Verfassungsrecht➔einklagbar➔
Grundrecht auf IT-Sicherheit? Nein, weil IT-Sicherheitsrecht (IT-Si) (objektives) Infrastrukturrecht ist.

◆Normenhierachie:➔Gesetzesrecht➔§ 87 Telekommunikationsgesetz (demnächst § 107 TKG) –
Voraussetzung für das Angebot von Telediensten.
IT-Sicherheit auch Voraussetzunung für die Zurverfügungstellung der Informationstechnologie für staatliche Sanktions- und Präventionsinteressen; für E-Government und E-Commerce im allgemeinen

Sicherheitsrecht für IT-Systeme (SITS) ”

Vorgeschlagenes Gliederungsschema

Akteure	OECD, ENISA, BSI, IT-Sicherheitsbeauftragter (Wehrmann; Donabauer)	Zertifizierungen; Gütesiegel (Maseberg); Datenschutzaudit
Prozesse	Informationssicherheitsmanagement Risiko- und Chancenanalyse (Krasemann, Beaupoil, Schwellach)	
Produkte	(Nouak)	

CyLaw

B. Datenschutz via Datensicherheit via IT-Sicherheit

Daten- und IT-Sicherheit

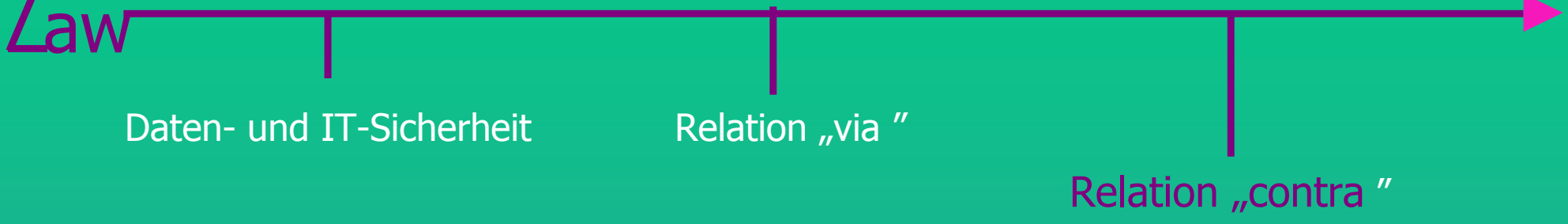
Relation „via "

Relation „contra "

	DaSchu	DaSi / IT-Si
DaSchu		Datenschutz setzt Schutz vor Vernichtung, Veränderung und unbefugter Einsichtnahme voraus
DaSi / IT-Si	Daten- und IT-Sicherheit wird von der Quantität der Daten bestimmt: ➢ Datensparsamkeit ➢ Zweckbindung/Einwilligung ➢ „Verbot" bei sensiblen Daten	

CyLaw

B. Datenschutz contra Datensicherheit contra IT-Sicherheit



	DaSchu	DaSi / IT-Si
DaSchu		- Daten der Angreifer werden geschützt - Anonymisierungsdienste contra Strafverfolgung
DaSi / IT-Si	- Protokollierung von Verbindungsdaten - IT-Sicherheitsbeauftragter contra Datenschutzbeauftragter	

Szenario

(nach Bundesgerichtshof Entscheidung vom 4.3.2004 Az. III ZR 96/03)

K ist Endanschlussteilnehmerin des Telekommunikationsunternehmens T. Das Unternehmen stellt über zwischengeschaltete Plattformbetreiber auch Verbindungen zu Mehrwertedienstanbietern her. Der Sohn S der K lädt beim Internetsurfen ein Programm (exe.-Datei) herunter, von dem er sich eine bessere Bildqualität verspricht. Als er feststellt, dass lediglich eine teure 0190-Verbindung zu Erotikseiten hergestellt wurde, löschte er das Programm. Das Programm hat jedoch die Einstellungen im DFÜ-Netzwerk so geändert, dass sämtliche Verbindungen in das Internet nicht mehr über die Standardeinwahl erfolgen, sondern über die 0190-Nummer. T stellt nach vier Monaten der K ca. 16.000,00 DM für diese Verbindungen in Rechnung.

(Verkehrssicherungs-)Pflichten bei Privaten (zum Schutz vor Dialern)

Bundesgerichtshof am 4.3.2004:

◆ Ein durchschnittlicher Endnutzer muss nicht damit rechnen, dass sich in harmlos erscheinenden Dateien illegale Dialer verstecken, die nicht durch bloßes Löschen unschädlich werden

◆ Ohne besonderen Anlass (Verdacht) müssen Nutzer nicht

- ihre Zugangsprogramme auf Dialer überprüfen.

- ihre Verbindungen ins Internet überwachen oder nur ausdrücklich freigeben

- Dialerschutzprogramme installieren

- vorsorglich sämtliche Mehrwertdienstrufnummern sperren lassen (insoweit keine Sorgfaltspflicht gegenüber dem TK-Anbieter) .

(Verkehrssicherungs-)Pflichten bei Privaten und Unternehmen?

Übertragbarkeit der Entscheidung des Bundesgerichtshof vom 4.3.2004 für das Szenario einer Weiterverbreitung von Viren und Würmern …..?

PRO

- Vergleichbarkeit der Anforderungen an Security aware Cyberpersonality (SaCyp), wenn auf dem Endgerät ein Dialer installiert oder dieses mit Viren infiziert wird.

(Verkehrssicherungs-)Pflichten bei Privaten und Unternehmen?

Übertragbarkeit der Entscheidung des Bundesgerichtshof vom 4.3.2004 für das Szenario einer Weiterverbreitung von Viren und Würmern …..?

PRO

- Vergleichbarkeit der Anforderungen an Security aware Cyberpersonality (SaCyp), wenn auf dem Endgerät ein Dialer installiert oder dieses mit Viren infiziert wird.
- Rechtsdogmatisch: Grundsätzlich keine Rechtspflicht, andere vor Schaden zu bewahren (Koch, NJW 2004, S. 801, 803). Verkehrssicherungspflicht setzt voraus:

(1) Beherrschung einer Gefahrenquelle und/oder

Hängt nach „Koch" von der Art der Weiterverbreitung (automatisch…) ab.

(2) Schaffung einer besonderen Gefahr

Hängt nach „Koch" davon ab, ob Empfang von infizierten E-Mails zum allgemeinen Lebensrisiko gehört.

- Offen in BGH-Entscheidung: Unterschiedliche Maßstäbe für Private und andere Koch: keine Pflicht zur Datensicherheit bei Privaten (§ 9 BDSG)

(Verkehrssicherungs-)Pflichten bei Privaten und Unternehmen?

Übertragbarkeit der Entscheidung des Bundesgerichtshof vom 4.3.2004 für das Szenario einer Weiterverbreitung von Viren und Würmern …..?

CONTRA

- ◆ Einzelfallentscheidung, die dem Familienrecht und den sozialen Verhältnissen in besonderem Maße Rechnung trägt und deshalb nicht verallgemeinerungsfähig ist.
- ◆ E-Mail und Internetsurfen haben unterschiedliche Gefahren- und Nutzenpotentiale
- E-Mails setzen Vertrauensbeziehung voraus; das Internetsurfen nicht
- Virenscanner könnten verbreiteter sein als Dialerschutzprogramme
- Bei der Sorgfaltspflichtverletzung könnte eine entscheidende Rolle spielen, ob Anhänge geöffnet wurden (vielfältigste Aufklärung in der Öffentlichkeit)

Grundlagen des Sicherheitsrechts für IT-Systeme (SITS)

?