Claudius Matthies, 2505729

Proseminar: Ethische Aspekte der Informationsverarbeitung

Vortrag:

Gesetze für den Cyberspace

GLIEDERUNG

1. Definition – Cyberspace

- Kunstwort
- Wörtlich: kybernetischer Raum (Kybernetik: Wissenschaft von Struktur komplexer Systeme, vor allem Kommunikation und Steuerung einer Rückkopplung)
- Umgangssprachlich: Internet oder auch WWW
    - aber: eher Infrastrukturen des Cyberspace
- virtualisierter Raumeindruck ohne topografische Position

2. Beschränkungen – reale Welt vs. Cyberspace

- reale Welt:
  - Gesetz
  - Soziale Normen
  - Markt
  - Natur (natürliche Beschränkungen) / „Architektur“
- Cyberspace:
  - Gesetz:
    - Copyrights
    - Ehrenverletzung (Beleidigung)
    - sexuelle Bedrohung / Belästigung
  - Normen:
    - Spezifische Regeln
    - Communities (Strafen androhen)
  - Markt:
    - Interzugangskosten
  - „Architektur“ = Code:
    - Hacker weniger davon betroffen
    - keine uniforme Architektur (Bedingungen variieren): z.B. Passwort vs. unidentifizierter Zugang
    - festgelegt durch den Codeschreiber

3. Gesetze – notwendig für den Cyberspace? – ein Fallbeispiel

- 1995: kontroverse Studie zur Pornografie im Internet (*Georgetown University Law Review*)
- *Time* und *Newsweak*: Coverstories zur Verfügbarkeit
- Senatoren und Kongressabgeordnete wurden mit Forderungen zur Regulierung bombardiert

Woher kam diese Wut angesichts der Tatsache, dass zu dem Zeitpunkt mehr Pornografie außerhalb des Internets verfügbar war?

- **Gesetz:** Verkauf von Pornografie nur für Volljährige, Erotik-Shops weit entfernt von „Kinder-Zonen“
- **Normen:** kein Pornografieverkauf an Kinder (recht effektiv)
- **Markt:** Pornografie zu teuer für Kinder
- **Natur:** Kinder können nicht verstecken Kinder zu sein → Zugang zur Pornografie verweigert
- aber: zu diesem Zeitpunkt sehr wenig Kinder mit Internetzugangsmöglichkeiten

- im Cyberspace wesentlicher Unterschied: Anonymität, also Verschweigen des „Kindseins“ möglich → Auskunft über Alter ist nicht gegeben, was aber für Händler notwenig wäre (architekturbedingt)

→ Communictations Decency Act (95/96) – Gesetzesänderungsvorschlag
    - beschränkte die Redefreiheit und wurde als verfassungswidrig eingestuft
- Entscheidung hing mit Annahmen über die Architektur des Internets zusammen, das zeigt:
    - Ausgangspunkt ist die Annahme einer festen Architektur
    - aber: Cyberspace
        - hat keine Natur
        - hat keine garantierte Unveränderlichkeit
        - hat keine Garantie für Freiheit
        - schafft keine garantierte Entkräftung von Regierungen, die Kontrolle wollen

Fazit: Internet ohne feste Architektur → es lassen sich keine allgemeingültigen Aussagen machen → Schwierigkeiten zur gesetzlichen Regelung, aber notwendig?!

4. Cyberspace – ein Rechtsraum? / Cyberlaw

- große Schwierigkeiten zur Bestimmung anwendbarer Rechtsordnung bei internetbezogenen Sachverhalten
- keine internationalen Abkommen
- bisher z.T. Festhalten am internationales Privatrecht → Parallelen zu staatsfreien Gebieten?
  Privatrecht: *Rechtgebiet, das Beziehungen von rechtlich gleichgestellten Rechtssubjekten untereinander regelt; aufgeteilt in Zivilrecht und sonstiges Privatrecht; Rechtgestaltung ohne staatlichen Einfluss*
- Forderungen Cyberspace als eigenständigen Rechtsraum zu behandeln
- Gesellschaft des Cyberspace ohne Staatseinflüsse organisierbar?
- Internet = staatsfreier Raum?
  - Der Nutzer verlässt seinen Staat nicht!
  - Staaten können sogar Vorschriften bezüglich exterritorialer Handlugen mit Auswirkungen auf den Staat selbst erlassen
  - würde bedeuten, dass Staat auf Rechtsdurchsetzungsbefugnisse verzichten müsste
    → undenkbar
  - Wer hätte dann die Befugnisse?
  - Sind Staaten in der Lage Regelungen durchzusetzen?
  - deterritoriales Element erschwert Rechtsdurchsetzung

4.1 Rechtsdurchsetzung im Internet

- grundlegende unterschiedliche Netzwerke:
  - Internet: frei, unkontrolliert, anonym
  - Intranet: nicht anonym, Zugang kann kontrolliert werden, Gebrauch kann beobachtet / festgehalten werden
  - gleiche grundlegende Protokolle
  - Intranet mit weiteren Protokollen, die über anderen stehen und Kontrolle erleichtern
  - → Widerspiegelung zweier Philosophien über Zugang: Freiheit – Kontrolle
  - Wahl einer der beiden Architekturen ist politisch (vor allem wenn Staaten wählen)
  - entspricht in der Bedeutung einer Verfassung

4.1.1 Totalitäre Staaten

- Kontrollbestreben bezüglich Zugänglichkeiten von (speziellen) Inhalten = Zensur
- vor allem islamische Staaten, da sie politische, soziale und religiöse Strukturen bedroht sehen
- Rechtsdurchsetzungen mit Filter-Technologie schwer möglich
    - mangelnde Aktualität
    - ausländische Server und Satellitentelefon
    - Programme / Sites zum Seitenaufruf trotz Blocken (mit Wechsel der Internetadresse und entsprechender Mailmitteilung)
    - → Kontrolle unmöglich?
    - Kontrolle über psychologischen Faktor (Bewusstsein einer staatlichen Überwachung schaffen durch harte Eingriffe und breite Berichterstattung)

- Beispiele:
    - Afghanistan: Taliban verboten vom Juli 2001 bis zum Sturz (Ende 2001) generell die Nutzung des Internets (Schutz vor „Dingen, die falsch, obszön, unmoralisch und gegen den Islam sind“)
    - mindestens 20 weitere Staaten versuchen Zugriff aus „schädliche“ Seiten zu verhindern
    - Iran: Nutzung des Internets erst ab Volljährigkeit
    - Kuba: Internetzugang nur für Universitäten und einigen Organisationen
    - Saudi-Arabien: zentraler Server zur Unterbindung des Aufrufs von pornografischen Seiten (Blocken von IP-Adressen) → theoretisch Rückverfolgung beim Aufrufversuch möglich!
    - Razzien von Internetcafés in China zur psychologischen Manipulation (Juli 2001: 2494 Internetcafés geschlossen, ca. 78.000 überprüft und 9000 Auflagen erteilt wegen „Sicherheitsmängel“)
    - China: Verbot von Seiten mit Gewaltdarstellung, Pornografie, Glücksspiel, Sekten
    - Gerüchte über Proxy-Server der chinesischen Regierung um Nutzerdaten zu sammeln

4.1.2 Demokratische Staaten

- Cyberspace auch hier keine Immunität gegen staatliche Eingriffe
- Architektur des Internets kann verändert werden! – zu einem regulierbaren Design
- Strukturen wurden Erfordernissen angepasst: z.B. SSL-Protokoll zur sicheren Datenübertragung (Kreditkartennummern etc.)
- gleichermaßen können rechtliche und technische Rahmenbedingungen (Architektur) verändert werden zur Regulierbarkeit, also Anonymität einschränken
- Möglichkeit: Computer-Zertifikate (nicht als zwingend erforderlich, sondern für spezielle Seiten, z.B. jugendgefährdenden Seiten)
- Gesetze, die die drei anderen Einflussfaktoren regulieren, damit diese anders regulieren

→ Regulierbarkeit durch Regierung regulierbar (besonders über Architektur)

- Rahmenbedingungen zur Nutzung des Internets für Durchsetzungsmöglichkeiten nationaler Gesetze verändern

4.1.3 Beispiel USA

- drohte den Gebrauch von Verschlüsselung zu verbieten
- stoppte den Export der Verschlüsselung konsistent
- versuchte Markt mit Standard-Verschlüsselung zu „überschwemmen“

→ Hintertür für Regierung

- November 97, Gesetzesvorschlag des FBI: jegliche Verschlüsselung solle Hintertür offen lassen bzw. Schlüsselwiederherstellung für Regierung ermöglichen
- größter Markt für Internetprodukte – Produkterfolg nur bei Erfolg in USA

→ USA-Standards = Standards für die Welt (trotzdem Standards lokaler Regierungen, die Regulierung nicht ausschließen)

- Kontrolle durch (nichtdemokratische?) Regierung möglich

→ USA = „Schwarzmarkthändler der Kontrolle“?

→ USA hat besondere Macht, die Architektur zu beeinflussen

4.2 Staatsfreie Gebiete als Grundlage für Cyberlaw?

- Internet zwar nicht staatsfrei, aber Rechtsdurchsetzung aufgrund der Globalität des Mediums schwierig
- besonders bei Ländern mit vielen virtuellen Ausweichmöglichkeiten zum Konsum des Mediums
- trotz keiner Staatsfreiheit, könnten staatsfreie Gebiete als Vorbild dienen (besonders für kollisionsrechtliche Fragen)
- staatsfreie Gebiete: Weltraum, Hohe See, Tiefseeboden, Antarktis
- gekennzeichnet durch Fehlen eines Ordnungsrahmens, der gegensätzlicher Interessen von Staaten ausgleicht und Nutzung dieser koordiniert
- keine Staatszuordnung, stehen allen Staaten zur Nutzung offen

→ keine Herrschaft von einzelnen Staaten

- Einschränkungen durch gleichberechtigte nationale Rechtssysteme in Konkurrenz

4.2.1 Beispiel Antarktis

- 1959: Antarktisvertrag, besonders beeinflusst durch wissenschaftliche Forschungstätigkeiten

→ Naturreservat
→ Zurückstellung territorialer Ansprüche (aufgrund Entdecker ihrer Nationalität)
  - viele Stationen erhalten territoriale Ansprüche weiter

→ Ausrichtung auf Demilitarisierung, Umweltschutz, wissenschaftliche Forschung
→ kein Regelungsrahmen für wirtschaftliche Nutzung
→ Erreichung der Vertragsziele über Inspektionen durch (nationale) Beobachter (sind nur ihrer nationalen Gerichtsbarkeit unterworfen)
→ keine Aussagen über Behandlung anderer Personen
→ durch nachfolgende Abkommen wieder Anknüpfung an Nationalität, z.B. Flaggenprinzip

- **Übertragbarkeit auf das Internet?**
  - gleicht einem staatsfreien Raum in seinen Eigenschaften in vielen Punkten
  - **Antarktisvertrag**
    - ohne umfassende Regelung international privatrechtlicher Probleme
    - keine Behandlung von Touristen (→ Haftungs- und Strafrecht)
    - praktisch keine Anknüpfung an Handlungs- oder Erfolgsort (z.B. bei Unfällen), denn keine territoriale Zuordnung (aber Staaten vollzogen vor Vertragsabschluss entsprechend ihren Ansprüchen Rechtssprechung → Probleme bei von zwei Staaten beanspruchtem Gebiet)
  - im Cyberspace oft mehrere Erfolgsorte vorhanden oder möglich
  - territoriale Anknüpfungspunkte müssen eingeschränkt werden, da sonst Rechtsordnungen aller Länder berücksichtigt werden müssten
  - besser: völkerrechtliche Verträge möglichst ohne strenge Erfolgsortanknüpfung
  - nationale Anknüpfungspunkte im Allgemeinen unbrauchbar für das Internet
  - urheber- und wettbewerbsrechtliche Probleme für Antarktis nicht relevant

  → Regelung staatsfreier Gebiete keine Grundlage für Cyberlaw

4.3 Netiquette und „Provider-Law“

4.3.1 Netiquette

- unverbindliche Verhaltensmaßstäbe, die sich zur Benutzung des Internets herausgebildet haben = Normen
- oft nur technische Hinweise
- keine einheitliche Fassung
- z.T. keine Beantwortung wichtiger, praxisrelevanter Fragen
- keine Rechtsverbindlichkeit (auch keine Gewohnheitsrecht oder Handelsbrauch)
- keine zwangsweise Durchsetzung

→ Fazit: ungeeignet

4.3.2 „Provider-Law“

- Providerverträge als Ansatzpunkt für Lösungsmodelle:
- „Provider-Law“: ausführlich geregeltes System von Vorschriften, dem sich Kunden unterwerfen müssen
- Verweisung von Streitigkeiten an Schiedsgerichte
- Durchsetzung möglich durch Internetzugangssperre
- darf nationale Rechtsordnung nicht aufheben, sondern muss sich daran messen lassen (besonders Regelungen über AGB)
- kann nur für Personen gelten, die den Provider-Vertrag unterzeichnet haben → Verträge zu Lasten Dritter sind unzulässig!

→ wieder nationale Rechtsordnung für alle, die den Vertrag nicht unterzeichnet haben, aber Zugang nutzen

- weitere Probleme bei Streitigkeiten zwischen Personen unterschiedlicher Provider, vor allem auch international
- einheitliches „Provider-Law“ unrealistisch, aufgrund von unterschiedlichen Wertvorstellungen
- Gefahr der Beeinflussung nach wirtschaftlichen Interessen
- gesperrte Seite kann über anderen Server wieder verfügbar gemacht werden, wenn dort Rechtsverletzungen anders definiert sind

- wirtschaftliches Interesse der Provider an vielen Kunden → „Provider-Law“ wirkt dem entgegen
- finanzkräftige Kunden als Manipulatoren des Rechts nach ihren Vorstellungen

→ neben demokratische Legitimation auch Finanzkraft als „Formgeber“

- Übertragung politischer Entscheidungen an private Institutionen fragwürdig

→ Fazit: ungeeignet

- aber: rechtswidrige Inhalte sperren wird z.T. schon von Providern verlangt
- 2002: EU-Parlament stimmte gegen Sperrung einzelner Seiten (illegale, schädliche Inhalte), da nicht effektiv und Fragmentierung des Internet-Zugangs bzw. Verhinderung des Zugangs zu erlaubten Seiten

→ Setzen auf Selbstregulierung der Medienbranche und Provider (Kooperation zwischen Internet-Industrie, Regierungen und nationalen Behörden vorhanden)

→ Verantwortung für Jugendliche bei gesetzlichen Betreuern

→ erfordert Medienkompetenz und „Aufgeklärtsein“ der Eltern → viele Dienstleistungen / Websites und Initiativen dazu

5. Zusammenfassung / Fazit

- Cyberspace ohne Natur, keine garantierte Unveränderlichkeit, keine Garantie für Freiheit, keine garantierte Entkräftung von Regierungen, die Kontrolle wollen
- Harmonisierung durch völkerrechtliche Abkommen nicht in Sicht
- Rechtsmaterie lässt sich schwer vereinheitlichen
- berührt viele Rechtsgebiete
- sehr unterschiedliche Interessen einzelner Staaten
- alle weiteren Ansätze scheinen erfolglos / ungeeignet zu sein

5.1 Gefahren:

- Veränderung des Internets von Freiheit zur Kontrolle (auch ohne Regierung, aber sie beschleunigt Vorgang)
- Beispiel Führerschein (und andere Pässe): hat und braucht fast jeder → trotzdem Anonymität (auf der Straße), da umfassende Kontrollmöglichkeiten zu teuer
- Internet: Datensammlung sehr kostengünstig, unsichtbar, stetig → ob zum guten oder schlechtem Nutzen ist nicht entscheidend, sondern Wirksamkeit eines so nie erreichten Systems von Kontrolle
- deshalb:
    - Veränderung verstehen, wahrnehmen
    - politischer Konsequenzen bewusstmachen
    - negative Wertung? → Handeln
    - Sollten rechtsstaatliche Werte die Möglichkeiten der Regulierbarkeit begrenzen, die solche Architekturen gestatten?
    - kritische Einstellung gegenüber Macht von Souveränen?
    - Übersetzen, was hervorstechend und wichtig ist in Bezug auf heutige Freiheit und verfassungsgemäße Demokratie in Architektur des Internets
    - „Checks & Balances“ (Überprüfen und Ausgeglichenheit) in Regulation des Codes / der Architektur sichern

Quellen:

www.lessig.org/content/articles/works/laws_cyberspace.pdf (30.06.06)

http://de.wikipedia.org/wiki/Cyberspace (03.07.06)

http://de.wikipedia.org/wiki/Kybernetik (03.07.06)

http://www.linksandlaw.de/ipr-internationales-privatrecht.htm

http://www.newsfactor.com/perl/story/12017.html (03.07.06)

http://www.heise.de/newsticker/meldung/19503 (03.07.06)

http://www.linksandlaw.de/ipr-internationales-privatrecht.htm (04.07.06)

http://de.wikipedia.org/wiki/Privatrecht (04.07.06)

http://www.heise.de/newsticker/meldung/26463 (05.07.06)