

Rechtliche Aspekte im eCommerce 2

Eine kurze Einführung in ein buntes Themengebiet

Wolfgang Auer

14. Juni 2006

Gliederung

Providerhaftung

- Übersicht
- Rechte und Pflichten der Provider
- Vorratsdatenspeicherung

Strafrecht

- Übersicht
- Neue Tatbestände im Detail
- Datendelikte
- Inhaltsdelikte

Kennzeichnungs- und Domainrecht

- Grundsätzliches zu Kennzeichen und Marken
- Domains im Kennzeichenrecht

Providerhaftung – Inhaltsverantwortung

Verantwortung für fremde Inhalte?

Haftungsausschluss im ECG für

- ▶ Access Provider (§13)
- ▶ Suchmaschinenbetreiber (§14)
- ▶ Caching Provider (§15)
- ▶ Host Provider (§16)
- ▶ Links (§17)

Umfang des Haftungsausschlusses (§19)

- ▶ Gilt (natürlich) auch für Anbieter unentgeltlicher Dienste
- ▶ Kein Haftungsausschluss für «Content Provider»

Access Provider und Suchmaschinenprovider

Haftungsausschluss für Access Provider

- ▶ Wer als Diensteanbieter von einem **Nutzer eingegebene Informationen** in einem **Kommunikationsnetz übermittelt** oder zu einem solchen den **Zugang vermittelt**, ist für die Informationen **nicht verantwortlich**, wenn er
 - ▶ sie nicht selbst veranlasst
 - ▶ den Empfänger der Informationen nicht auswählt
 - ▶ die Informationen weder auswählt noch verändert
- ▶ Dies gilt auch bei erforderlicher, automatischer kurzzeitiger Zwischenspeicherung
- ▶ Analoges gilt für Suchmaschinenbetreiber

Host Provider, Caching Provider und Linksetzer

Haftungsausschluss für Host Provider

- ▶ Wer als Diensteanbieter von einem Nutzer eingegebene Informationen **speichert**, ist für die Informationen **nicht verantwortlich**, wenn er
 - ▶ von einer rechtswidrigen Information oder Tätigkeit keine tatsächliche Kenntnis hat bzw.
 - ▶ falls er doch Kenntnis erlangt hat, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren
- ▶ Rechtswidrigkeit für **Laien** offensichtlich
- ▶ Analoges bei Caching (mit Aktualisierungspflicht)
- ▶ Analoges bei Linksetzung (außer bei «Verinnerlichung»)

Diensteanbieterpflichten

Diensteanbieterpflichten

- ▶ Keine Verpflichtung zu Überwachung oder Forschung nach rechtswidrigen Tätigkeiten
- ▶ Bei Verdacht auf strafbare Taten bei Access und Host Providern: Informationsoffenlegung an Gericht
- ▶ Bei Bedarf einer Verwaltungsbehörde: Offenlegung von Namen und Adresse der Vertragspartner durch Host Provider
- ▶ Bei begründetem und qualifiziertem Bedarf eines Dritten analog

Vorratsdatenspeicherung

Brandaktuell: Vorratsdatenspeicherung – RL 2006/24/EG

- ▶ Pflicht (statt Verbot) der Vorratsspeicherung
- ▶ Speicherungen ansonsten nicht gebrauchter Daten auf Verdacht
- ▶ Umfassende Datenkategorien
 - ▶ Rufnummern, Benutzerkennungen, Adressdaten
 - ▶ IMSI, IMEI, Standortkennung
 - ▶ Wo sinnvoll möglich: Quelle und Ziel
- ▶ Speicherzeitraum zwischen sechs Monaten und zwei Jahren
- ▶ Terrorklausel
- ▶ Richtlinienumsetzung bis 17. September 2007

Grundprobleme des Strafrechts

Strenge Anforderungen des Strafrechts

- ▶ *nulla poena sine lege* (§1 StGB)
- ▶ Analogieverbot
- ▶ Bestimmtheitsgebot
- ▶ Vorsatzerfordernis

Überkommene Begriffe

- ▶ Körperlichkeit der Sachen
- ▶ Wertträgereigenschaft

Neue Qualität

- Enorme technische Möglichkeiten
- Datenmassen
- Internationales Handeln – Territorialitätsprinzip

Arbeitsteilung

- Vorbereitung
- Beitrag
- Besitz

Störung der Funktionsfähigkeit eines Computersystems: §126a StGB

Tatbestandsmerkmale

- Wer einen **anderen** dadurch **schädigt**, dass er
- **automatisationsunterstützt** verarbeitete, übermittelte oder überlassene **Daten**,
- über die er **nicht** oder **nicht allein verfügen darf**,
- **verändert, löscht** oder sonst **unbrauchbar macht** oder **unterdrückt**, ...

Rechtsfolge

... ist mit Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Datenspionage

Dogmatische Einordnung

- Datenschutz vergleichbar Briefgeheimnis? (§118 StGB)
- Analogieverbot!
- Widerrechtlicher Zugriff auf ein **Computersystem** (§118a StGB)

Computersystem nach §74 Abs 1 Z 7

Sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen.

Datenspionage

Verletzung des Telekommunikationsgeheimnisses (§119 StGB)

- Strafbar ist die Benützung einer Vorrichtung
- im Rahmen der Telekommunikation oder eines Computersystems
- um sich oder einem Dritten Kenntnis einer Nachricht zu verschaffen (also mit Spionageabsicht zu handeln)
- die nicht für den Abfangenden bestimmt war
- Ermächtigungsdelikt

Datenbeschädigung (§126a StGB)

- Analogietatbestand zur Sachbeschädigung
- Problem: Körperlichkeit der Sache
- 0 bis 6 Verurteilungen pro Jahr seit 1995

Betrügerischer Datenverarbeitungsmissbrauch (§148a StGB)

- Analogietatbestand zum Betrug
- Problem: Ziel des Betrugs
- 3 bis 15 Verurteilungen pro Jahr seit 1995

Missbrauch von Computerprog. oder Zugangsdaten. Oder: «Komplexe» Gesetzgebung – §126c StGB

(1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung
2. oder ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. [...]

Datenspionage

Widerrechtlicher Zugriff auf ein Computersystem (§118a StGB)

- Strafbar ist, wer eine spezifische Sicherheitsvorkehrung verletzt
- in einem **Computersystem**
- über das er nicht oder nicht alleine verfügen darf
- mit der Absicht, sich von Daten unbefugt Kenntnis zu verschaffen und
- sich einen Vermögensvorteil oder einem anderen einen Nachteil zuzuwenden
- indem er die Daten selbst benützt, einem anderen zugänglich macht oder veröffentlicht

Datenspionage

Missbräuchliches Abfangen von Daten (§119a StGB)

- Auffangtatbestand für §119 bei **jeder** Abhörvorrichtung
- Umfasst auch elektromagnetische Abstrahlung
- Vorsatz auf Vermögensvorteil oder Nachteilszufügung

Datenverwendung in Gewinn- oder Schädigungsabsicht (§51 DSGVO)

- Verletzung schutzwürdigen Geheimhaltungsinteresses an personenbezogenen Daten
- Durch Eigennutzung oder Veröffentlichung bzw. Weitergabe
- Betrifft widerrechtlich oder berufsbedingt erlangte Daten
- Vorsatz auf Vermögensvorteil oder Nachteilszufügung

Inhaltsdelikte

Pornographie allgemein (§1 Pornographiegesezt)

- ▶ Unzüchtige Schriften, Abbildungen, Laufbilder oder andere unzüchtige Gegenstände, also auch «Unbildliches»
- ▶ Nur bei Gewinnabsicht

Pornographische Darstellungen Minderjähriger (§207a StGB)

- ▶ Umfasst sind «**wirklichkeitsnahe Abbildungen**»
- ▶ Schon das «**Vermitteln des Eindrucks**» genügt
- ▶ Strafbar sind das Herstellen, Anbieten, Überlassen, Vorführen, Zugänglichmachen und zur Verbreitung Einführen, Befördern und Ausführen
- ▶ Ausgenommen ist nur die qualifizierte Einwilligung

Schutzfähige Unterscheidung

Merkmale der Schutzfähigkeit von Kennzeichen

- ▶ «Etwas Besonderes, Individuelles»
- ▶ Glaube der Verkehrsteilnehmer an Unterscheidungsfähigkeit

Schutzzweck der Kennzeichenrechte

- ▶ Unterscheidbarmachung – Individualisierung
- ▶ Schutz vor Beeinträchtigung:
 - ▶ Verwechslung («Zuordnungsverwirrung»)
 - ▶ Rufausbeutung
- ▶ Schutzverstärkung bei «bekannter Marke»

Namensschutz – Kollisionsfall

Namensschutz – auch außerhalb des geschäftlichen Verkehrs

- ▶ Bezeichnung natürlicher und juristischer Personen
- ▶ Griffige Namensteile, verkehrsbliche Kurzbezeichnungen
- ▶ Weiter Schutzbereich, bis hin zu ideellen Beziehungen

Prioritätsprinzip des Schutzes

- ▶ *Prior tempore, potior iure*:
Wer zuerst kommt, mahlt zuerst
- ▶ Registrierung bzw. Gebrauchsaufnahme

Domains als Kennzeichen

Kennzeichenrechtliche Stellung der Domain

- ▶ Domains können in Markenrechte eingreifen
- ▶ Geschäftlicher Verkehr – white pages?
- ▶ Sonderfall Serienzeichen:
erhöhte Verkehrsgeltung, erhöhter Schutz

Verletzungsbereich bei Domains – «Ähnlichkeitsmaß»

- ▶ Wortbild (optische Ähnlichkeit)
- ▶ Wortklang (akustische Ähnlichkeit)
- ▶ Wortbedeutung (semantische Ähnlichkeit)

Inhaltsdelikte

Nationalsozialistische Inhalte (Verbotsgesetz)

- ▶ Internet als Medium problemlos
- ▶ Zugang an «viele Menschen» notwendig
- ▶ Freie Meinungsäußerung? EMRK!

Selbstmord«foren»

- ▶ Beitrag zum Selbstmord – spezifisch österreichisches Delikt

Aufforderung zur Begehung strafbarer Handlungen

- ▶ Zugänglichmachung an «breite Öffentlichkeit» notwendig
- ▶ Umfasst auch die qualifizierte Gutheißung schwerer Delikte
- ▶ Eigenes Delikt – ggf. aber auch Beitrag zu schweren Delikten!

Was ist geschützt und was nicht?

Schutzfähige Kennzeichen

- ▶ Name
- ▶ Firma, Geschäftsbezeichnung
- ▶ Marke, Ausstattung
- ▶ Werktitel (in der Praxis meist auch Marke)

Nicht schutzfähige Kennzeichen

- ▶ Gattungsbezeichnungen
- ▶ Geographische Angaben (als Marke!)
- ▶ Beschreibende Angaben:
Etwa Herkunft, Verwendungszweck etc. einer Ware
- ▶ (Prinzipiell) Farben

Verletzungen im Kennzeichnungs- und Markenrecht

Verletzungsarten

- ▶ Doppelidentität: **Absolute Identität** (in der Praxis selten)
- ▶ Verwechslungsgefahr: **Ähnliche Zeichen für ähnliches Produkt**
 - ▶ ...eng: Zuordnung zum selben Unternehmen
 - ▶ ...weit: Unterstellung wirtschaftlicher Verbundenheit

Verletzungsfolgen

- ▶ Unterlassung
- ▶ Beseitigung
- ▶ Angemessenes Entgelt
- ▶ Urteilsveröffentlichung
- ▶ Schadenersatz (bei Verschulden)

Gleichnamigkeitsproblematik

Namenskonflikte

- ▶ Gebrauch des eigenen Namens **immer zulässig**;
auch bei Eingriff in Markenrecht
- ▶ Domains weltweit **eindeutig**: hohes **Konfliktpotential**
- ▶ Deswegen: Vorrang der früheren Domainregistrierung
- ▶ In Deutschland nicht bei «überwältigender Verkehrsgeltung»
- ▶ Bei Gleichnamigkeit:
 - ▶ Rücksichtnahmegebot
 - ▶ «Fair Use»

Konfliktfälle

Beschreibender Zeichengebrauch

- Verwendung fremder Kennzeichen zulässig:
 - Hinweis auf Beschaffenheit oder Verwendungszweck
 - Notwendige Verwendung etwa bei Ersatzteilanbietern
- «Fair Use» bei der Domainbezeichnung:
Den anständigen Gepflogenheiten des Marktes entsprechend

Rechtliche Bedeutung von Disclaimern

- Beseitigung der «Zuordnungsverwirrung»
- Prominente Positionierung nötig
- Irrelevant bei
 - Rufausbeutung
 - Gravierender Interessendivergenz

Gefahren der Domainwahl

Nach Möglichkeit vermeiden:

- Fremde Marken
- Fremde Firmen
- Fremde Namen, v. a. bekannte
- Fremde schutzfähige Titel
- Geographische Bezeichnungen
- Bezeichnungen hoheitlicher Einrichtungen
- Latent irreführende Domains (Tippfehler!)

Domaingrabbing

Grundlagen

- Sperrrecht ist prinzipiell vorhanden
- Nicht aber zu sittenwidrigem Behinderungswettbewerb:
 - Bewusstes Aufbauen eines Hindernisses
 - Behinderung als eigentliche Leistung («Abkaufenlassen»)
- Domaingrabbing ist schon per se gewerblicher Gebrauch

Beweisproblematik – Glaubhaftmachung durch Indizienkette

- Domain hat nichts mit Inhaber zu tun
- Es gibt schon eine andere Domain des Inhabers
- Inhaber registriert viele Domains ohne vernünftigen Grund
- Keine Nutzung der Domain bzw. keine Anstrengung dazu