Universität St.Gallen

Informationsrecht

Internetrecht

Prof. Dr. iur. Daniel Hürlimann, Ass.-Prof. für Informationsrecht

16. März 2017

Überblick Internetrecht

- Privatrecht
  - Haftung von Online-Plattformen inkl. Suchmaschinen
  - E-Commerce-Recht inkl. Lauterkeitsrecht
- Öffentliches Recht
  - Internet Governance
  - Grundrechte im Internet
- Strafrecht
  - Cybercrime (Cybercrime-Konvention, Melani etc.)
  - Überwachung des Internetverkehrs
  - Kabelüberwachung

Haftung von Online-Plattformen

- EU: E-Commerce-Richtlinie
- CH: keine spezifische Regelung, rechtsgebietsabhängig
- Persönlichkeitsrecht: jede Mitwirkung genügt
- verschiedene Auffassungen in der Lehre bezüglich Dritthaftung im IGR

  → Cyrill P. Rigamonti, Providerhaftung – auf dem Weg zum Urheberverwaltungsrecht?, in: sic! 2016, S. 117-133
- spezifische Haftungsregelungen im Patentgesetz und Designgesetz
- Kartellrecht: Online-Plattformen können marktbeherrschende Stellung gemäss Art. 7 KG erreichen
- Lauterkeitsrecht: Verwertung fremder Leistung (Art. 5 UWG)

Fall: Immobilien-Suchmaschine

- BGE 131 III 384
- Übernahme der auf einer fremden Internet-Plattform erscheinenden Immobilien-Inserate

E. 4.5.: “Von einer unmittelbaren Übernahme im Sinne von Art. 5 lit. c UWG kann nur ausgegangen werden, wenn der für die Reproduktion und Verwertung der reproduzierten Arbeitsergebnisse erforderliche Aufwand im Verhältnis zum objektiv nötigen Aufwand für die erstmalige Herstellung der Daten unangemessen gering ist. Die Klägerinnen haben ihren (objektiv) für die Herstellung ihrer Inserate erforderlichen Aufwand nicht substanziiert. Zudem beschränkt sich der Aufwand der Beklagten für die eigene gewerbliche Verwertung dieser Inserate nicht auf deren Übernahme durch gängige technische Reproduktionsverfahren. Die Vorinstanz hat daher zutreffend die Tatbestandsvoraussetzungen von Art. 5 lit. c UWG als unerfüllt erachtet.”

Fall: Immobilien-Suchmaschine

- BGE 131 III 384

  E. 5.3: “Das Internet enthält eine Vielzahl von Daten. Sind diese als solche nicht immaterialgüterrechtlich geschützt, sondern frei zugänglich, so erscheint es grundsätzlich sinnvoll, dass sich der Wettbewerb unter den Plattform-Betreibern über die an bestimmten Bedürfnissen des Publikums orientierte Vollständigkeit, Verlässlichkeit und Erschliessung dieser Daten abspielt.”

  E 5.4: “Die systematische Suche der Beklagten nach veröffentlichten, in ihr Angebot passenden Immobilien-Inseraten, deren Übernahme in die eigene Website sowie deren Anzeige nach den Strukturmerkmalen der eigenen Immobilien-Plattform ist als solche nicht unlauter. Da vorliegend keine besonderen Umstände festgestellt sind, die dieses Vorgehen als unlauter erscheinen lassen, hat die Vorinstanz einen Verstoss im Sinne von Art. 2 UWG bundesrechtskonform verneint.”

Haftung von Suchmaschinen

- Haftung für eigenes Verhalten
  - Crawling
  - Indexing
  - Ranking
  - Caching
  - Thumbnails
  - Snippets
  - Suchvorschläge
- Haftung für verlinkte Inhalte
  - keine Vorabprüfung
  - Notice-and-Takedown
- Haftung für Werbung (Keyword Advertising)

EuGH zur Haftung von WLAN-Anbietern

- Schlussanträge des Generalanwalts vom 16. März 2016: Verpflichtung zu Passwortschutz würde unternehmerische Freiheit zu stark einschränken

- Urteil des EuGH vom 15. September 2016: Verpflichtung zu Passwortschutz durch Gericht oder Behörde zulässig

- Folge: Unterlassungsanspruch gegenüber Betreibern von WLANs ohne Passwortschutz; Betreiber von passwortgeschützten WLANs haften nicht

Haftung von WLAN-Anbietern in der Schweiz

- Urteil des Bundesgerichts 5A_792/2011 vom 14. Januar 2013 (Tribune de Genève)
- unklar, ob weitreichender Unterlassungsanspruch nur für Persönlichkeitsverletzungen gilt
- Haftungsfreistellung für Provider im URG-Vorentwurf für Fernmeldedienstanbieter und "Anbieter von abgeleiteten Kommunikationsdiensten"
- Qualifikation von WLAN-Betreibern als Fernmeldedienstanbieter im Einzelfall zu bestimmen (insbesondere Art. 2 FDV)

E-Commerce-Recht

- Art. 3 UWG: Unlautere Werbe- und Verkaufsmethoden und anderes widerrechtliches Verhalten

[1] Unlauter handelt insbesondere, wer: [...]

o. Massenwerbung ohne direkten Zusammenhang mit einem angeforderten Inhalt fernmeldetechnisch sendet oder solche Sendungen veranlasst und es dabei unterlässt, vorher die Einwilligung der Kunden einzuholen, den korrekten Absender anzugeben oder auf eine problemlose und kostenlose Ablehnungsmöglichkeit hinzuweisen; wer beim Verkauf von Waren, Werken oder Leistungen Kontaktinformationen von Kunden erhält und dabei auf die Ablehnungsmöglichkeit hinweist, handelt nicht unlauter, wenn er diesen Kunden ohne deren Einwilligung Massenwerbung für eigene ähnliche Waren, Werke oder Leistungen sendet;

E-Commerce-Recht

- Art. 3 UWG: Unlautere Werbe- und Verkaufsmethoden und anderes widerrechtliches Verhalten

[1] Unlauter handelt insbesondere, wer: […]
s. Waren, Werke oder Leistungen im elektronischen Geschäftsverkehr anbietet und es dabei unterlässt:

1. klare und vollständige Angaben über seine Identität und seine Kontaktadresse einschliesslich derjenigen der elektronischen Post zu machen,
2. auf die einzelnen technischen Schritte, die zu einem Vertragsabschluss führen, hinzuweisen,
3. angemessene technische Mittel zur Verfügung zu stellen, mit denen Eingabefehler vor Abgabe der Bestellung erkannt und korrigiert werden können,
4. die Bestellung des Kunden unverzüglich auf elektronischem Wege zu bestätigen;

Internet Governance

- Entwicklung und Anwendung durch Regierungen, den Privatsektor und die Zivilgesellschaft, in ihren jeweiligen Rollen, von gemeinsamen Prinzipien, Normen, Regeln, Vorgehensweisen zur Entscheidungsfindung und Programmen, die die Weiterentwicklung und die Nutzung des Internets beeinflussen.“ (Bericht der Arbeitsgruppe zur Internet Governance, Juli 2005)

- Regelungen und Mechanismen für Internet Governance sind die Themen einer teilweise hitzigen internationalen Debatte zwischen vielen unterschiedlichen Interessenvertretern des Internets. Bis heute gibt es keine einheitliche Auffassung darüber, wie Internet Governance in Zukunft international gehandhabt werden soll. Während die USA Vertreter des Status Quo sind, fordern viele Länder, unter anderem die EU, aber auch viele Entwicklungsländer, weitergehende Mitsprache- und Mitbestimmungsmöglichkeiten.

  Quelle: de.wikipedia.org/wiki/Internet_Governance

Grundrechte im Internet

- Bundesverfassungsgericht (D): Computergrundrecht
- in CH bisher nicht anerkannt, aber
- Beispiel Staatstrojaner, betrifft
  - persönliche Freiheit (Art. 10 Abs. 2 BV)
  - Privatleben (Art. 13 Abs. 1 BV)
  - Grundrecht auf Wohnung (Art. 13 Abs. 1 BV)
  - Vertraulichkeit der Kommunikation (Art. 13 Abs. 1 BV)
  - Datenschutz (Art. 13 Abs. 2 BV)
- gesetzliche Grundlage für Staatstrojaner im revidierten BÜPF

Digitale Intimsphäre

- Privatrecht: Dreiteilung des gesamten Lebensbereichs eines Menschen in den Geheim-, Privat- und Gemeinbereich
- Übertragbar auf grundrechtlichen Schutz der Privatsphäre?
- Falls ja: Geheimbereich als Kernbereich?
- Konsequenzen für Zulässigkeit von Staatstrojanern?

Cybercrime

- Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
- basiert auf Verwaltungsvereinbarung zwischen Bund und Kantonen
- Zuständigkeit

  “In ihrer Eigenschaft als nationale Koordinationsstelle hat KOBIK die Aufgabe, die von unterschiedlichen Polizeikräften geführten Ermittlungen optimal zu koordinieren und die ihr zugestellten Verdachtsmeldungen möglichst schnell den zuständigen kantonalen Strafverfolgungsbehörden zukommen zu lassen.”
  www.cybercrime.admin.ch/kobik/de/home/ueberuns/zustaendigkeit_.html

Cybercrime-Konvention

- Übereinkommen zur Bekämpfung von Computer- und Internetkriminalität
- für die Schweiz seit dem 1. Januar 2012 in Kraft
- zwei kleinere Gesetzesanpassungen:
  - Vorverlagerung der Strafbarkeit beim Straftatbestand des unbefugten Eindringens in eine Datenverarbeitungsanlage (Art. 143bis StGB): Bereits das Zugänglichmachen und das Inverkehrbringen von Passwörtern, Programmen und anderen Daten unter Strafe, wenn der Betreffende weiss oder annehmen muss, dass diese für das illegale Eindringen in ein geschütztes Computersystem verwendet werden sollen
  - Rechtshilfegesetz: Verkehrsdaten können schon vor Abschluss des Rechtshilfeverfahrens zu Ermittlungszwecken an die ersuchende Behörde übermittelt werden (Art. 18b IRSG).

Überwachung des Internetverkehrs

- Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
  - 1. Abschnitt: Geltungsbereich und Organisation
  - 2. Abschnitt: Überwachung ausserhalb von Strafverfahren
  - 3. Abschnitt: Überwachung des Postverkehrs
  - 4. Abschnitt: Überwachung des Fernmeldeverkehrs
  - 5. Abschnitt: Gebühren und Entschädigungen
  - 6. Abschnitt: Schlussbestimmungen
- Art. 1 Abs. 2 BÜPF: "Es gilt für alle staatlichen, konzessionierten oder meldepflichtigen Anbieterinnen von Post- und Fernmeldedienstleistungen sowie für **Internet-Anbieterinnen**."
- aus grundrechtlicher Sicht problematisch: Vorratsdatenspeicherung und Staatstrojaner

29. Oktober 2015, 07:42 Uhr Vorratsdatenspeicherung

Dieses Thema interessiert Sie nicht - sollte es aber

Wer nicht will, dass ein Text gelesen wird, muss nur das lange V-Wort darüber schreiben. Warum das Desinteresse an der Vorratsdatenspeicherung falsch ist.

tinyurl.com/v-wort

Art. 15 Abs. 3 BÜPF:

"Die Anbieterinnen sind verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die **Verkehrs- und Rechnungsdaten** während sechs Monaten aufzubewahren."

Vorratsdatenspeicherung

- was sind Verkehrs- und Rechnungsdaten?
- Art. 16 VÜPF: Überwachungstypen (Echtzeit und rückwirkend)

“Folgende Überwachungstypen können angeordnet werden: […]

d. die Lieferung folgender Daten, sofern es zum Aufbau einer Kommunikation gekommen ist (rückwirkende Überwachung): […]

3. bei Mobil**telefonie**: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,”

Art. 16[16] Überwachungstypen (Echtzeit und rückwirkend)

Folgende Überwachungstypen können angeordnet werden:

a. die Übertragung des Fernmeldeverkehrs (Echtzeit-Überwachung der Nutzinformationen);

b. bei Mobiltelefonie: die Bestimmung und die simultane oder periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist (Echtzeit-Überwachung);

c. die Bereitstellung und die simultane oder periodische Übertragung folgender Angaben, selbst wenn es nicht zum Aufbau einer Kommunikation kommt, (Echtzeit-Überwachung):
   1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und ankommenden Kommunikationsvorgänge),
   2. die tatsächliche bekannte Zielrufnummer und die zwischengeschalteten verfügbaren Rufnummern, falls der Anruf um- oder weitergeleitet wurde,
   3. die erzeugten Signale, einschliesslich der Zeichengabe für den Bereitschaftszustand, die Parameter der Fernmeldeanlagen (z.B. IMSI-Nummer, IMEI-Nummer) und die erzeugten Signale für die Aktivierung der Konferenzschaltung oder der Anrufumleitung,
   4. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,
   5. das Datum und die Uhrzeit;

d. die Lieferung folgender Daten, sofern es zum Aufbau einer Kommunikation gekommen ist (rückwirkende Überwachung):
   1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldedienstanbieterin bekannt sind),
   2. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die IMSI-Nummer und die IMEI-Nummer),
   3. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,
   4. das Datum, die Zeit und die Dauer der Verbindung;

e. der Antennensuchlauf: rückwirkende Eruierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge während eines bestimmten Zeitraumes, sofern es zum Aufbau einer Kommunikation gekommen ist.

Urteil des EuGH zur Vorratsdatenspeicherung

- EU: Richtlinie über die Vorratsspeicherung von Daten
- EuGH: Vorratsdatenspeicherung verletzt die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, weil
  - erstreckt sich auf sämtliche Personen und elektronischen Kommunikationsmittel
  - Zugang zu den Daten ist zu wenig genau geregelt
  - Speicherdauer von mindestens sechs Monaten unabhängig vom etwaigen Nutzen der Daten
  - keine Massnahmen zum Schutz vor unberechtigtem Zugang und unberechtigter Nutzung
  - keine Speicherung der Daten im Unionsgebiet
- VDS gemäss EU-Richtlinie schränkt die Grundrechte unverhältnismässig ein
- Richtlinie ungültig

Weitere Urteile zur Vorratsdatenspeicherung

- 2009: Rumänien
- 2010: Deutschland
- 2011: Tschechien
- 2014: Österreich
- 2015: Niederlande, Bulgarien

Sämtliche Verfassungsgerichte, welche eine zur Schweiz vergleichbare Regelung zu prüfen hatten, haben die Vorratsdatenspeicherung als unrechtmässigen Eingriff in die Grundrechte eingestuft und sie aufgehoben.

Vorratsdatenspeicherung in der Schweiz

- 6 Monate Aufbewahrungsdauer
- Bundesrat wollte auf 12 Monate verdoppeln
- Urteil des EuGH betrifft die Schweiz nur indirekt
- Verdoppelung wurde vom Parlament gestrichen
- Hauptproblem besteht aber immer noch: flächendeckende Aufzeichnung von Bewegungsprofilen (vgl. Visualisierung zur Vorratsdatenspeicherung)
- Revidiertes BÜPF am 18. März 2016 verabschiedet, noch nicht in Kraft
- Urteil des Bundesverwaltungsgerichts vom 9. November 2016

Urteil des BVGer zur Vorratsdatenspeicherung

- Urteil des Bundesverwaltungsgerichts A-4941/2014 vom 9. November 2016
- Vorratsdatenspeicherung gemäss BÜPF zulässig
  - Vorratsdatenspeicherung dient der Strafverfolgung
  - daher überwiegendes öffentliches Interesse
  - Datenschutzrecht schützt vor missbräuchlicher Verwendung der Daten
  - Eignung der VDS gestützt auf Einzelfälle bejaht
- Medienmitteilung des Bundesverwaltungsgerichts: tinyurl.com/bvger-vds
- Beschwerde beim Bundesgericht hängig
- je nach Fortgang: Weiterzug an EGMR

Kabelaufklärung

- Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG)
- Vom Parlament am 25. September 2015 beschlossen (BBl 2015 7211)
- 7. Abschnitt: Kabelaufklärung
- Art. 39 Abs. 1 NDG:

  "Der NDB kann den durchführenden Dienst damit beauftragen, zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland (Art. 6 Abs. 1 Bst. b) sowie zur Wahrung weiterer wichtiger Landesinteressen nach Artikel 3 grenzüberschreitende Signale aus leitungsgebundenen Netzen zu erfassen." → alles klar?

- NDG in Volksabstimmung vom 25. September 2016 angenommen

Staatstrojaner

- Spionageprogramm, das gegen Computer und Smartphones eingesetzt werden kann
- Kauf eines Staatstrojaners beinhaltet auch Kauf geheimer Sicherheitslücken in Software
- Gesetzliche Grundlage?

  Art. 280 StPO: Zweck des Einsatzes

  Die Staatsanwaltschaft kann technische Überwachungsgeräte einsetzen, um:

  a. das nicht öffentlich gesprochene Wort abzuhören oder aufzuzeichnen;
  b. Vorgänge an nicht öffentlichen oder nicht allgemein zugänglichen Orten zu beobachten oder aufzuzeichnen;
  c. den Standort von Personen oder Sachen festzustellen.

Art. 280 lit. a StPO

tinyurl.com/govware

Thomas Hansjakob: «Man könnte am ehesten versucht sein, den Einsatz von GovWare unter Art. 280 lit. a StPO zu subsumieren. Eingesetzt werden aber eben keine technischen Geräte, sondern es wird in ein Datenverarbeitungssystem des Beschuldigten eingegriffen. Dessen Software wird so manipuliert, dass das dem Beschuldigten gehörende technische Gerät dazu verwendet werden kann, seine Gespräche zu überwachen. Das ist offensichtlich von der Eingriffstiefe her etwas anderes als der Einsatz von Geräten der Strafverfolgungsbehörden, und es betrifft eben einen Eingriff nach Art. 143bis StGB, für welchen Art. 280 lit. a StPO meines Erachtens keine gesetzliche Grundlage liefern kann.

Dies führt zum (zugegebenermassen für den Praktiker unbefriedigenden) Ergebnis, dass die Überwachung der Internet-Telefonie mittels GovWare zurzeit mangels klarer gesetzlicher Grundlage nicht zulässig ist.»

Art. 280 lit. a StPO

tinyurl.com/govware

Thomas Hansjakob: «Man könnte am ehesten versucht sein, den Einsatz von GovWare unter Art. 280 lit. a StPO zu subsumieren. Eingesetzt werden aber eben keine technischen Geräte, sondern es wird in ein Datenverarbeitungssystem des Beschuldigten eingegriffen. Dessen Software wird so manipuliert, dass das dem Beschuldigten gehörende technische Gerät dazu verwendet werden kann, seine Gespräche zu überwachen. Das ist offensichtlich von der Eingriffstiefe her etwas anderes als der Einsatz von Geräten der Strafverfolgungsbehörden, und es betrifft eben einen Eingriff nach Art. 143bis StGB, für welchen Art. 280 lit. a StPO meines Erachtens keine gesetzliche Grundlage liefern kann.

Dies führt zum (zugegebenermassen für den Praktiker unbefriedigenden) Ergebnis, dass die Überwachung der Internet-Telefonie mittels GovWare zurzeit mangels klarer gesetzlicher Grundlage nicht zulässig ist.»

Art. 280 lit. a StPO

tinyurl.com/govware

Thomas Hansjakob: «Ich halte denn auch den vorgesehenen Weg des Bundesrates, die gesetzliche Grundlage mit der Revision des BÜPF zu schaffen, für richtig – in der VÜPF wäre eine solche Regelung unzulässig gewesen, weil von der Eingriffsschwere her eine Grundlage in einem formellen Gesetz erforderlich ist. […]

Fazit: Der Einsatz von GovWare zur verdeckten Beweiserhebung ist nach der geltenden Rechtslage in der Schweiz zurzeit noch nicht möglich. Die Revision des BÜPF und die damit verbundene Ergänzung der StPO sollen diese Lücke schliessen, wobei (wohl vorwiegend aus politisch-taktischen Gründen) die GovWare auch in Zukunft in der Schweiz nur dazu verwendet werden soll, Internet-Telefonie und verschlüsselten Mailverkehr überwachen zu können.»