

Informatikrecht

Notizen

Nachfolgende Notizen wurden im Zusammenhang mit dem Informatikrecht (INFR) Unterricht an der Hochschule Luzern erstellt. Sie enthalten Informationen, Aussagen und Interpretationen von Dozenten (allen voran Frau lic. iur. Ursula Sury) und Studenten. Die Richtigkeit der Informationen ist keineswegs garantiert.

OUTSOURCING / OFFSHORING

Risiken bei Offshoring SW Entwicklung

- Kulturelle Differenzen
- Kommunikationsprobleme
- Anwendbares Recht, Korruption
- Investitionsschutz: Knowhow, Urheberrechtsschutz, Source Code Ablage
- Datenschutz, Persönlichkeitsschutz

Risiken bei Offshoring SW Betrieb

- Kulturelle Differenzen
- Sicherheit, Datenschutz
- Knowhow-Verlust
- Ausbildungsstand
- Infrastrukturprobleme
- Politische Instabilität
- Zeitverschiebung

Jeder Outsourced-Service unterliegt im Lauf der Zeit Änderungen. Outsourcing Partner können ändern. Es ist auch möglich, dass ein Service wieder insourced wird. Das Risikomanagement ist bis zum Schluss zu berücksichtigen, also inkl. Ausserbetriebnahme des Services.

ALLGEMEINE GESCHÄFTSBEDINGUNGEN

- Konkretisierung, Präzisierung und Explizierung des OR (OR ist dispositives Recht und kann daher von den Parteien ausgelegt werden.)
- Branchenabhängige Ergänzungen
- Standardisierung von Verträgen (sich wiederholende, allgemeingültige Elemente kommen in AGB)
- Risikoverschiebung, Verschleierung
- Verhandlungsvorteil für denjenigen mit dem ersten Vorschlag
- Globalakzept / Vollakzept:
 - o Ein Vollakzept besagt, dass ein Kunde die AGB's vollumfänglich gelesen und verstanden hat. Oberhalb der Unterschrift (also vor Vertragsabschluss) muss deshalb zwingend ein Satz ala „Hiermit bestätige ich, die AGB vollständig, selbständig gelesen und verstanden zu haben“.
 - o Ein Globalakzept liegt normalerweise dann vor, wenn der Kunde die AGB nicht gelesen und/oder nicht verstanden hat. In diesem Fall gewährt der Staat Rechtsschutz mit Hilfe der Unklarheits- und Ungewöhnlichkeitsregel.
- Unklarheitsregel + Ungewöhnlichkeitsregel: Bleiben Unklarheiten, weil die betreffende AGB-Bestimmung nach ihrem Sinngehalt mehrdeutig oder widersprüchlich ist, gilt die für den Kunden günstigste Auslegung. Leider ist das aber ein Witz, da der Kunde oft genötigt wird, eine Bestätigung abzugeben, dass er die AGB vollumfänglich verstanden und akzeptiert hat.

DATENSCHUTZ

- Daten dürfen dann bearbeitet werden, wenn
 - o 1) das Gesetz dies vorsieht (Legalitätsprinzip) oder
 - o 2) wenn eine explizite Zustimmung der betroffenen Person erfolgt (Privatautonomie).
- Grund für Datenschutz: Informelle Selbstbestimmung jeder Person. Ziel: Jede Person hat das Recht, selbst zu bestimmen, wer welche Daten über sie bearbeiten darf.
- DSGVO Art. 4 Abs. 1 und 2: Personendaten dürfen nur rechtmässig, d. h. auf legale Weise, bearbeitet werden. Die Bearbeitung der Daten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

- DSG Art. 4 Abs. 5: Personendaten dürfen erst nach Einwilligung der betroffenen Person bearbeitet werden. Besonders schützenswerte Personendaten oder Persönlichkeitsprofile unterliegen einer ausdrücklichen Zustimmung der betroffenen Person.
- DSG Art. 5: Wer Personendaten bearbeitet, hat sicherzustellen, dass diese korrekt sind: Konsistenz, Verwechslungen, Eingabevalidierung
- Informationen müssen geschützt werden (technisch)
- DSG Art. 3 lit. a: Als Personendaten und somit Daten gemäss Datenschutzgesetz gelten alle Angaben, die sich auf eine natürliche oder juristische Person beziehen. Anonymisierte Daten sind gemäss Definition des Datenschutzgesetzes keine Personendaten mehr.
- DSG Art. 3 lit. c: Mit dem Begriff „besonders schützenswerte Personendaten“ sind Aussagen über die religiösen, politischen, gesundheitlichen, etc. Belange gemeint.
- DSG Art. 3 lit. e: Mit Bearbeiten ist jeder Umgang mit Personendaten gemeint. Auch das blosses Aufbewahren oder etwa das Löschen von Daten ist damit gemeint.
- StGB Art. 179novies: Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft, wird mit Gefängnis oder Busse bestraft. Dieser Tatbestand kann nur unter folgenden Voraussetzungen erfüllt sein:
 - o Die Daten dürfen nicht „frei zugänglich“ sein. (StGB Art.179novies)
 - o Die Daten müssen „durch angemessene technische und organisatorische Massnahmen (...) geschützt werden“. (DSG Art. 7 und VDSG)
- Softwareentwicklungen, welche Personendaten bearbeiten, müssen die gesetzlichen Anforderungen des DSG sowie der VDSG berücksichtigen.
- Zielkonflikt: Betriebswirtschaftlichkeit versus Sicherheit

DATENARCHIVIERUNG

- Fallbeispiel:
 - o Fixtermin bedeutet, dieser Termin muss zwingend eingehalten werden. Nicht als „fix“ markierte Termine müssen „abgemahnt“ werden (Stichwort Mängelrüge).
 - o Konkludenter Vertragsabschluss => durch Handel vereinbarter Vertrag; formlos und non-verbal.
 - o Über Projektprotokolle können Terminverschiebungen festgelegt werden. Das ist eine gültige Vertragsanpassung.
- OR Art. 957 Abs 1: Firmen, welche im Handelsregister eingetragen werden müssen, sind verpflichtet, Bücher ordnungsgemäss zu führen und aufzubewahren (...), um die Vermögenslage des Geschäftes und die mit dem Geschäftsbetriebe zusammenhängenden Schuld- und Forderungsverhältnisse sowie die Ergebnisse der einzelnen Geschäftsjahre festzustellen.
- Die elektronische Archivierung ist mit der heutigen Gesetzgebung erlaubt (OR Art. 957ff; GeBüV).
- Beim Archivieren geht es u.a. um die Beweiskraftsicherung: Man muss immer das beweisen können, was man zum eigenen Vorteil in einem Prozess verwenden könnte.
- Das Gesetz meint mit „archivieren“ das Ablegen von Dokumenten in Staatsarchiven. Das Archivieren von Geschäftsdokumenten wird „aufbewahren“ genannt.
- OR Art. 962 Abs. 2: Die Aufbewahrungsfrist beginnt mit dem Ende des Geschäftsjahres, in welchem die Geschäfte getätigt wurden. Aber Achtung: Laufende Verträge werden nicht archiviert, bis ihr Geschäftsgang beendet wurde (Mietverträge, Leasingverträge, Wartungsverträge, usw..)
- Aufbewahrungsform: Bilanz und Erfolgsrechnung sind stets schriftlich und mit Originalunterschrift (keine Fotokopie!) aufzubewahren. Alle anderen Dokumente (Geschäftsbücher, Buchungsbelege, Korrespondenz) kann schriftlich oder elektronisch archiviert werden.
- Zur Korrespondenz gehört u.U. auch der Email Verkehr, sofern darin buchungsrelevante Informationen enthalten sind. (Das Archivieren aller Emails darf nur dann erfolgen, wenn die Mitarbeiter eine Weisung unterzeichnet haben, dass sie den Dienst nicht privat nutzen. Ansonsten müssen sie über die Archivierung informiert werden bzw. die Möglichkeit haben, private Mails von der Archivierung auszuschliessen).
- Die Geschäftsbücherverordnung (GeBüV) legt fest, wie elektronische Dokumente archiviert werden müssen, damit Sie dieselbe Beweiskraft haben, wie Papierdokumente.
- „Nicht löschen“ bedeutet nicht „archiviert“!
- Wann müssen zusätzliche Dokumente archiviert werden?
 - o Wenn auf den Dokumenten entscheidende Mehrinformationen vorhanden sind.
- Wann müssen Dokumente länger als nach Art. 957 ff. OR archiviert werden?
 - o MwSt Immobilienbelege: 20-25 Jahre
 - o Immobilienbelege für Grunstückgewinnsteuer: Während Eigentumsdauer
 - o Verlustscheine: 20 Jahre

- Wann sollen Dokumente zusätzlich in Papierform aufbewahrt werden?
 - o Originalunterzeichnete Kaufverträge können im Falle einer Betreibung (mit Rechtsvorschlag) die sofortige Rechtsöffnung herbeiführen.
 - o Eingescannte und nach Geschäftsbüchervorschriften archivierte Dokumente können keine sofortige Rechtsöffnung herbeiführen. Tipp zur Risikominderung: Verträge erst vernichten, wenn Kunde bezahlt hat.
- ZertES stellt elektronische und handschriftliche Unterschrift gleich.
- Zertifikate: Elektronische Signatur, fortgeschrittene elektronische Signatur, qualifizierte Signatur. Letztere ist gleichgestellt mit einer handschriftlichen Signatur.

URHEBERRECHT

- Was ist urheberrechtlich geschützt? Warum? (URG 1, 2)
 - o URG Art. 2 Werkbegriff, Lit. a) Werke sind, unabhängig von ihrem Wert oder Zweck, geistige Schöpfungen der Literatur und Kunst, die individuellen Charakter haben.
 - o Abs. 3) Als Werke gelten auch Computerprogramme. Die Dokumentation gehört zur Software.
- Wer ist Urheber? Warum? (URG 6, 7, 17)
 - o URG Art. 6: Urheber oder Urheberin ist die natürliche Person, die das Werk geschaffen hat.
 - o URG Art. 7: Haben sie nichts anderes vereinbart, so können sie das Werk nur mit Zustimmung aller verwenden.
 - Das bedeutet, dass jeder der sich (mit noch so kleinem Beitrag) beteiligt hat, hat gleichwertiges Mitbestimmungsrecht.
 - o URG Art. 17: Rechte an Programmen: Wird in einem Arbeitsverhältnis bei Ausübung dienstlicher Tätigkeiten sowie in Erfüllung vertraglicher Pflichten ein Computerprogramm geschaffen, so ist der Arbeitgeber oder die Arbeitgeberin allein zur Ausübung der ausschliesslichen Verwendungsbefugnisse berechtigt.
 - Die Unternehmung besitzt die Lizenzrechte an der Software. Das Urheberrecht liegt aber weiterhin bei den natürlichen Personen, welche am Werk mitgearbeitet haben.
 - Davon ausgeschlossen sind also Freelancer, da diese kein Arbeitsverhältnis haben!
 - Ausnahmen werden oft in Arbeitsverträgen geregelt.
- Als Auftragnehmer ist es von Vorteil, wenn die Rechte an der Software mir gehören. Aber Achtung: Wer den Source Code besitzt, besitzt nicht automatisch die Urheberrechte!
- Der Urheber hat alle Rechte an seinem Werk (Veräusserung, Präsentation, Lizenzierung, usw.). Ohne ausdrückliche Zustimmung des Urhebers darf das Werk von keiner anderen Person verwendet werden.
- URG Art 19, Abs 1 besagt, dass die Verwendung von urheberrechtlich geschützten Werken für
 - o Eigengebrauch
 - o Ausbildungszwecke, Klassenunterricht
 - o Information- und Dokumentationszwecke
 erlaubt sei. Laut Abs. 4 ist Computersoftware davon explizit ausgenommen.
- URG Art 20 Abs 3: Wer Leerkassetten und andere zur Aufnahme von Werken geeignete Ton- und Tonbildträger herstellt oder importiert, schuldet dem Urheber oder der Urheberin für die Werkverwendungen nach Artikel 19 eine Vergütung.
- URG Art 21: Wer das Recht hat, ein Computerprogramm zu gebrauchen, darf sich die erforderlichen Informationen über Schnittstellen mittels Entschlüsselung des Codes (Reverse Engineering) beschaffen. Die gewonnenen Informationen dürfen auch zur Entwicklung von Um-Systemen, zur Wartung oder zu Interoperabilitätszwecken genutzt werden.
- URG Art 24: Werke dürfen zu Sicherungszwecken archiviert werden. Aufbewahrung an einem für andere Leute nicht zugänglichen Ort. Kein kommerzieller Hintergedanke. Dasselbe gilt auch für Computersoftware.
- URG Art 39a Abs 4: Das Umgehungsverbot kann gegenüber denjenigen Personen nicht geltend gemacht werden, welche die Umgehung ausschliesslich zum Zweck einer gesetzlich erlaubten Verwendung vornehmen. (*Oftmals kann dieses Recht nicht wahrgenommen werden, da Kopierschutzmechanismen das Anfertigen von Sicherheitskopien verhindern*).
- URG Art 68: Wer es vorsätzlich unterlässt, in den gesetzlich vorgesehenen Fällen (Art. 25 und 28) die benützte Quelle und, falls er in ihr genannt ist, den Urheber anzugeben, wird auf Antrag der in ihren Rechten verletzten Person mit Busse bestraft.
- Fallbeispiel: Mehrere Firmen arbeiten zusammen mit Fachhochschulen und ETH an einer gemeinsamen Steuerungssoftware für Kraftwerke. Gesponsert wird das Projekt von der Kommission für Technologie und Innovation (KTI). Die entstehende Software soll unter der GNU/GPL Lizenz

laufen.

Bei den Diskussionen um die Lizenz- und Patentrechte kommt es zum Rechtsstreit: Einige Firmen wollen ihre Geschäftsgeheimnisse –verständlicherweise – nicht preisgeben. Die GNU/GPL würde nur die Offenlegung des Quellcodes verlangen. Oft ist es aber so, dass mit Hilfe des Quellcodes Rückschlüsse auf Geschäftsprozesse gemacht werden können. Das ist sehr heikel für die betroffenen Firmen.

Da die General Public License vorschreibt, dass das Werk als Ganzes unter GPL stehen muss, können Teile davon nicht ausgeschlossen werden – es sei denn, die Teile würden unabhängig voneinander laufen.

- Definitionen: Freeware: Kostenloses Nutzen. Shareware: Zeitlich und vom Umfang her beschränkte Nutzung; oft kostenpflichtig. Open Source: Quellfreie Software, muss oft selber kompiliert werden, da von irgendeinem Freak in der dunklen Kammer gestrickt...

PRODUKTHAFTUNG

- Fallbeispiel: Ein Spital bezieht von OS AG eine Software. Diese Software läuft auf Linux, welches unter GNU/GPL lizenziert ist. Darunter läuft auch eine Oracle Datenbank Instanz. Wer haftet für Fehler im Zusammenhang mit der erstellten Software?
 - Grundsätzlich haftet die OS AG für alles, was im Zusammenhang mit der Software steht. Auch wenn Fehler im Betriebssystem/DBMS auftreten.
 - Nach abgeschlossener Entwicklung kann der Betrieb bei einem externen Hoster eingerichtet werden, dann haftet dieser für Störungen.
 - Haftungsausschluss mit Klauseln in der AGB können helfen, die Haftung bestimmter Systembestandteile zu minimieren.
 - Falls das Projekt abgeschlossen, vom Auftraggeber akzeptiert und in den Betrieb übergegangen ist, so muss im Fehlerfall eine Expertise erstellt werden, welche die schuldige Partei (Hoster oder Entwickler) ausfindig macht.

ARBEITSVERTRÄGE IN DER INFORMATIK

- Arten von Arbeitsverträgen: Einzelarbeitsvertrag (EVA), Gesamtarbeitsvertrag (GAV), Auftrag (OR Art. 394-406), Werkvertrag (OR Art. 363-379), Maklervertrag.
- Mit dem Werkvertrag verpflichtet sich der Unternehmer zur Herstellung eines Werkes, der Besteller zur Leistung einer Vergütung (OR 363). Aus heutiger Sicht muss das herzustellende Werk nicht stofflich fassbar sein, auch geistige Leistungen (Erstellung von Gutachten oder von Konstruktionsplänen, Vermessungsarbeit eines Geometers, so BGE 109 II 37) können Inhalt eines Werkvertrages bilden.
- Wartungsverträge sind sog. Dauerschuldverhältnisse und stellen einen Werkvertrag dar. Folgende Punkte sind beim Abschluss eines Werkvertrags zu beachten:
 - o Leistung: Welche Arbeiten sind gedeckt? Wie schnell wird reagiert? Eskalationsprozess? Wie wird die Sicherheit und der Datenschutz gewährleistet?
 - o Wem gehören die Urheberrechte, sofern solche im Rahmen des Vertrags entstanden sind?
 - o Kosten: Statisch oder dynamisch? Teuerung oder andere Faktoren mit einbezogen?
- Befristete Arbeitsverhältnisse:
Arbeitet ein Arbeitnehmer nach Ablauf eines befristeten Arbeitsverhältnisses beim Arbeitgeber weiter, so läuft der neue, formlose Arbeitsvertrag unbefristet weiter bis dieser von der einen Partei gekündigt wird. Dabei gelten aber die Regeln des unbefristeten Arbeitsvertrags. (OR Art 334, Abs 1 und 2)
- Maklervertrag: Vermittelt die Gelegenheit für Vertragsabschlüsse. Beispiel: Stellenvermittlung, Lizenzvermittlung, Outsourcing Vermittlung.

STRAFRECHT / CYBER CRIME

- Cyber Crime (oder Computer-Kriminalität) befasst sich mit Delikten, welche mit Hilfe neuer Informationstechnologie ermöglicht werden.
- Folgende Tatbestände können im Zusammenhang mit Cyber Crime auftreten:
Hacking, Eindringen in Systeme, Datendiebstahl, Industriespionage, Datenmanipulation, verbotene Pornographie, verbotene Gewaltdarstellung, Verstoss gegen Antirassismuskonvention, Spam, Cyber-Mobbing, Cyberstalking, Filesharing, und vieles mehr...
- Die allgemeinen Voraussetzungen der Strafbarkeit setzt folgende Bedingungen voraus:
 - o Tatbestandsmässigkeit bedeutet, dass eine Handlung bzw. Unterlassung ausdrücklich per Gesetz verboten ist.
 - o Rechtswidrigkeit ist bereits gegeben, sofern die Tat „tatbestandsmässig“ ist und sofern es keine Rechtfertigungsgründe (z.B. Notwehr) gibt.

- Schuldhaftigkeit bedeutet, dass ein (urteilsfähiger) Täter das Unrecht der Tat hätte voraussehen müssen. Durch die Rechtswidrigkeit des Verhaltens wird die Schuld indiziert.
 - Schuldfähigkeit: Kinder unter 10 Jahren sind nicht schuldfähig. Ihre Eltern haften kausal für alle Straftaten.
 - Formen der Schuld: Vorsätzlich (StGB Art 12 Abs 2) oder fahrlässig (StGB Art 12 Abs 3).
(Alkohol, Drogen, Medikamente, Krankheiten können die Urteilsfähigkeit und damit die Straffähigkeit stark mindern).
- Es gilt das Legalitätsprinzip (StGB Art. 1 und BV Art 5 Abs 1): Keine Strafe ohne Gesetz.
- Folgendes Strafrecht kann zum Einsatz kommen:
 - Medienstrafrecht gemäss StGB Art. 27 und Art. 322bis.
 - StGB Art. 135, Brutaloartikel
 - StGB Art. 197 Ziff. 3, harte Pornografie
 - StGB Art. 261bis Abs. 4 Rassendiskriminierung
- Fallbeispiel „Epileptiker“: Ein Epileptiker fällt während eines Anfalls in eine Schaufensterscheibe. Es entsteht Sachschaden. Ist er dafür strafrechtlich verfolgbar?
 - StGB Art. 144, Abs. 1: Wer eine Sache, an der ein fremdes Eigentums-, Gebrauchs- oder Nutzniessungsrecht besteht, beschädigt, zerstört oder unbrauchbar macht, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
 - Im Moment des Anfalls ist der Epileptiker nicht zurechnungs- und handlungsfähig. Er ist deswegen strafrechtlich nicht verfolgbar.
 - Es gibt für den Epileptiker keine Pflicht die Medikamente zu nehmen. Würde es das geben und der Epileptiker hätte den Anfall wegen Unterlassens der Einnahme der Medikamente erlitten, so wäre er tatsächlich strafbar.
- Fallbeispiel „SMS Dienst“: Ein Typ erstellt ein System für den Autonummer Lookup via SMS. Dabei verwendet er Daten, welche über ein gestohlenes Passwort von einem Strassenverkehrsamt abgezogen wurden.
Welche Computerdelikte sind vorgefallen:
 - Argument für Verletzung des Datenschutzes: Es werden Personeninformationen gespeichert ohne dafür eine Einwilligung der betroffenen Personen einzuholen.
 - Unbefugtes Eindringen in ein Datenverarbeitungssystem: Art. 143bis: *Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*
 - Art 143 (Offizialdelikt) verlangt ein „besonders gesicherter“ Zugang. Fragt sich, ob ein schwaches Passwort den ganzen Artikel nichtig macht? Wohl kaum. Sobald ein Passwort vorhanden ist, ist das System geschützt.
 - Art 143bis (Antragsdelikt) würde nur zum Zuge kommen, wenn er „nur“ gehackt hätte, also keine Bereicherungsabsicht bestanden hätte.
 - Datenbeschädigung, Art. 144bis, Abs. 1: *Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*
 - Der Täter hat keine Spuren an den Daten hinterlassen.
 - Betrügerischer Missbrauch einer Datenverarbeitungsanlage: Art. 147.
 - Keine Vermögensverschiebung und kein betrügerischer Missbrauch feststellbar (Abs.1). (Bei Betrug muss ein bestimmtes Mindestmass an Lug und Trug vorliegen. Beispielsweise Falschaussagen bei der Beschaffung von Kennwörtern)
 - Erschleichen einer Leistung, Art. 150.
 - Ist nicht der Fall, da die Autonummern in beschränkter Zahl kostenlos abgefragt werden können.
 - Unbefugtes Beschaffen von Personendaten: Art. 179novies 1: *Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*

- Urkundenfälschung, Art. 251, Abs. 1: Wer in der Absicht, (...) einem andern einen unrechtmässigen Vorteil zu verschaffen (...).
→ Gemäss StGB Art. 110, Abs.5 zählt ein Login nicht als Urkunde.
- Verkehrszulassungsverordnung (VZV), Art. 126 „Auskünfte über Fahrzeugzulassungen“, Abs. 1, *Namen und Adresse von Inhabern eines Kontrollschildes können jedermann bekanntgegeben werden.*
- Inwiefern sind die Beteiligten (Freund bei Versicherungsfirma und Hacker in China) strafbar?
→ Hacker in China sind ebenfalls strafbar. Der Auftraggeber des Hacking Auftrags steht aber als Tatvermittler klar im Vordergrund.
→ Der Freund bei der Versicherung hat das Kennwort offenbar nicht absichtlich weitergegeben und ist deshalb unschuldig.
- Fazit: Einziger Tatbestand, welcher geltend gemacht werden kann, ist Art 143bis. Erst wenn die Staatsanwaltschaft die Voraussetzungen für strafbares Verhalten (Tatbestand + Rechtswidrigkeit + Schuldhaftigkeit) nachgewiesen kann, wird ein Strafprozess eröffnet.

FERNMELDEGESETZ

- FMG Art. 1 Zweck Abs. 1: Das Fernmeldegesetz bezweckt, dass der Bevölkerung und der Wirtschaft vielfältige, preiswerte, qualitativ hoch stehende sowie national und international konkurrenzfähige Fernmeldedienste angeboten werden.
- Providerhaftung: Der Internet Access Provider wird nur strafbar, wenn er vom rechtswidrigen Handeln seiner Kunden gewusst hat.
- In der Schweiz existiert kein Domainnamenrecht, d.h. es gibt von Gesetztes wegen keinen Anspruch auf einen bestimmten „.ch“ Domänennamen. Das Markenschutzgesetz (MSchG), das Bundesgesetz über unlauteren Wettbewerb (UWG) sowie die Artikel des Obligationenrechts betreffend des Firmenschutzes können missbräuchlich verwendeten Domänennamen jedoch Nachdruck verleihen.
- BÜPF und VÜPF überwachen den Post-/Fernmeldeverkehr: Bei dringendem Tatverdacht können Postsendungen und Verbindungsdaten können aufgezeichnet und ausgewertet werden.