www.jusletter.ch

Urs Egli

Update IT-Recht

IT-Recht ist eine Querschnittsmaterie. Es ist die Rechtsprechung und Gesetzgebung aus zahlreichen Rechtsgebieten zu verfolgen. Der Beitrag gibt einen Überblick über aktuelle Entwicklungen.

Beitragsarten: Beiträge
Rechtsgebiete: Informatikrecht; Informatik und Recht

Zitiervorschlag: Urs Egli, Update IT-Recht, in: Jusletter 25. August 2014

Inhaltsübersicht

I. Vertragsrecht

1. Artikel 404 OR: Unsicherheitsfaktor bei der Kündigung von Dauerschuldverhältnissen

[Rz 1] Die Parteien hatten einen Vertrag über die Verwaltung eines Liegenschaftsportfolios abgeschlossen. Der Vertragswert belief sich auf über CHF 1 Mio. pro Jahr.[1] Die Auftraggeberin hatte diese Aufgaben bisher selber wahrgenommen. Im Hinblick auf den Vertrag übernahm die Liegenschaftsverwaltung das bisherige Personal der Auftraggeberin. Der Vertrag hatte eine feste Laufzeit von 5 Jahren und verlängerte sich anschliessend um jeweils 1 Jahr bei einer Kündigungsfrist von 12 Monaten. Für den Fall einer vorzeitigen Kündigung aus wichtigem Grund musste die kündigende Partei eine Entschädigung von CHF 200'000 zahlen.

[Rz 2] Bereits nach 2 Jahren kündigte die Auftraggeberin den Vertrag vorzeitig mit einer Frist von nur 2 Monaten. Das Bundesgericht erachtete die Kündigung unter Berufung auf Art. 404 Abs. 1 des Obligationenrechts (OR) als zulässig und die Entschädigung von CHF 200'000 wurde der

[1] Urteil des Bundesgerichts 4A_284/2013vom 13. Februar 2014.

Auftragnehmerin aberkannt.

[Rz 3] In mehreren früheren Urteilen hatte das Bundesgericht ähnlich entschieden, trotz Kritik aus der Praxis. Spielt bei einem Vertrag das Vertrauensverhältnis eine Rolle, gelangt der auftragsrechtliche Art. 404 Abs. 1 OR zwingend zur Anwendung und dagegen gerichtete Konventionalstrafen sind nichtig. Es gibt jedoch Ausnahmen für vom Bundesgericht als «Dauerschuldverhältnisse» bezeichnete Verträge. So wurde die Anwendung von Art. 404 Abs. 1 OR auf einen Franchisevertrag verneint.

[Rz 4] Die Rechtsprechung des Bundesgerichts ist interpretationsbedürftig. Es kann deshalb nicht ausgeschlossen werden, dass Art. 404 Abs. 1 OR auch auf Outsourcing- und ASP-Verträge angewendet wird. Nimmt man wie das Bundesgericht das Vertrauensverhältnis zum Massstab, könnten insbesondere Verträge über Cloud-Services gefährdet sein. Bei der Vertragsredaktion ist diesem Risiko mit einer ausführlichen Formulierung der Kündigungsbestimmungen zu begegnen. Insbesondere müssen sich allfällige Termination Fees mit effektiv ungedeckten Kosten rechtfertigen lassen.

2. AGB im Internet

[Rz 5] Ein österreichisches Unternehmen bestellte für ein Zentrallager bei einem deutschen Unternehmen Regalanlagen.[2] Die AGB des deutschen Unternehmens enthielten eine Gerichtsstandsklausel. Gemäss dieser war das Handelsgericht Zürich zuständig.

[Rz 6] Die AGB waren dem Vertrag nicht beigelegt. Dieser enthielt jedoch den Hinweis, dass die AGB per Fax angefordert oder von der Internetseite herunter geladen werden können.

[Rz 7] Das deutsche Unternehmen reichte beim Handelsgericht Zürich eine Klage über EUR 670'000 ein. Während sich das Handelsgericht als zuständig erachtete, hiess das Bundesgericht die Unzuständigkeitseinrede gut. Es beurteilte die Gerichtsstandsvereinbarung nach Art. 23 Ziff. 1 des Lugano-Übereinkommens (LugÜ). Konkret ging es um die Frage, ob dem Vertragspartner die AGB tatsächlich vorliegen müssen oder ob es ausreicht, dass sich der Vertragspartner die AGB unschwer und prompt verschaffen kann. Dabei setzte sich das Bundesgericht ausführlich mit der Rechtsprechung des EuGH auseinander. Es gelangte zum Schluss, dass der AGB-Verwender seinem Vertragspartner zumindest eine zumutbare Möglichkeit der Kenntnisnahme verschaffen muss. Die Zugänglichmachung über Fax erfüllt diese Voraussetzungen nicht, wohl aber die Bereitstellung über Internet. Dies gelte insbesondere dann, wenn die Parteien über E-Mail miteinander verkehrten, denn dann bestehe ein vernachlässigbarer Unterschied zwischen dem Öffnen eines angefügten Dokuments und dem Anklicken eines Links.

3. EULA und MSA – widersprüchliche Gerichtsstandsklauseln

[Rz 8] Ein schweizerisches Luftfahrtunternehmen hatte bei einem deutschen Softwarelieferanten ein ERP-System bestellt.[3] Die Parteien haben für die Lizenz mit einem EULA (Enduser License Agreement) und für die Implementation mit einem MSA (Master Service Agreement) samt State-

[2] Urteil des Bundesgerichts 4A_86/2013vom 1. Juli 2013, publiziert in BGE 139 III 345.

[3] Urteil des Bundesgerichts 4A_149/2013vom 31. Juli 2013.

ment of Work zwei separate Verträge abgeschlossen. Im MSA wurde Zürich als Gerichtsstand vereinbart. Im EULA war die Gerichtsstandsvereinbarung widersprüchlich. Während in einem «Supplement to EULA» Zürich als Gerichtsstand vereinbart wurde, beliessen die Parteien im EULA die ursprüngliche Gerichtsstandsvereinbarung, die auf Frankfurt lautete.

[Rz 9] Zwar sprach die vorprozessuale Korrespondenz für ein redaktionelles Versehen, allerdings nicht mit genügender Klarheit. Das Bundesgericht ging deshalb für das EULA nicht von einer gültigen Gerichtsstandsvereinbarung aus.

[Rz 10] Ein Gerichtsstand am Erfüllungsort gemäss Art. 5 Abs. 1 lit. a LugÜ lag nicht vor, da im EULA kein Erfüllungsort vereinbart war. Somit war auf die allgemeine Regel für Lizenzverträge zurückzugreifen, wonach sich bei einem gewöhnlichen Lizenzvertrag der Erfüllungsort am Sitz des Schuldners befindet. Art. 5 Abs. 1 lit. b LugÜ (Erfüllungsort für den Verkauf beweglicher Sachen am Lieferort) gelangte nicht zur Anwendung. Dafür ist bei Software erforderlich, dass sie in materialisierter Form übertragen wird, was die Klägerin im erstinstanzlichen Verfahren nicht vorgebracht hatte.

II. Datenschutz

1. Spyware beim Zivilschutz Tessin

[Rz 11] Das Bundesgericht hat einen Leitentscheid zur elektronischen Überwachung am Arbeitsplatz gefällt.[4] Der Chefinstruktor des Zivilschutzes eines Gemeindeverbundes im Kanton Tessin wurde wegen eines starken elektronischen Verkehrs am Arbeitsplatz heimlich elektronisch überwacht. Zu diesem Zweck wurde für einen Zeitraum von 3 Monaten eine Überwachungssoftware installiert. Dabei wurde festgestellt, dass der Arbeitnehmer während 71% seiner Computerzeit ausserdienstlichen Tätigkeiten nachgegangen war (Lektüre von Zeitungen, Konsultation von sozialen Netzwerken, Konsumation von Fernsehprogrammen, von Filmen – zum Teil pornografischen Inhalts – und von Spielen, Erledigung von E-Banking, Reisebuchungen, persönliche Mitteilungen, Versand von Dokumenten für private und politische Aktivitäten). Dies entsprach 23% der gesamten Arbeitszeit des Arbeitnehmers. In der Folge wurde der Arbeitnehmer fristlos entlassen.

[Rz 12] Das Bundesgericht setzte sich mit Art. 26 der Verordnung 3 zum Arbeitsgesetz (ArGV 3) auseinander. Diese Bestimmung verbietet Überwachungssysteme nicht generell, sondern nur dann, wenn ausschliesslich das Verhalten des Arbeitnehmers überwacht werden soll.

[Rz 13] Im vorliegenden Fall beurteilte das Bundesgericht den Einsatz der Spyware als unzulässige Verhaltensüberwachung, die zur Erreichung des beabsichtigten Zwecks (nämlich der Durchsetzung der arbeitsvertraglichen Pflichten) nicht erforderlich war. Der Arbeitgeber muss in erster Linie präventive Instrumente einsetzen (z.B. Sperren bestimmter Internetseiten) und darf erst bei Nichtbefolgung zu anderen Mitteln greifen.

[Rz 14] Die mit der Spyware beschafften Beweismittel wurden deshalb vom Gericht als unverwertbar beurteilt und die fristlose Entlassung wurde nicht geschützt.

---

4 Urteil des Bundesgerichts 8C_448/2012vom 17. Januar 2013, publiziert in BGE 139 II 7ff.

2. Steuerpranger

[Rz 15] Die Gemeinde Egerkingen gab an einer Gemeindeversammlung die Steuerschuldner bekannt, welche sich systematisch während mindestens vier aufeinanderfolgenden Jahren der Steuerpflicht entzogen hatten. Die Gemeinde berief sich dabei auf das öffentliche Interesse. Nach Auffassung der Gemeinde «unterhöhlten die betroffenen Schuldner mit ihrem Verhalten in stossender, dem Gerechtigkeitsgedanken zuwiderlaufender Weise das gesamte Gemeinwesen.» Das Verwaltungsgericht des Kantons Solothurn beurteilte die Publikation als rechtswidrig und bezog klar Stellung gegen solche Pranger.[5] Gemäss den anwendbaren § 15 und 21 des Informations- und Datenschutzgesetzes des Kantons Solothurn (InfoDG-SO) dürfen Personendaten nur bekanntgegeben werden, wenn die Publikation in einem Gesetz oder einer Verordnung vorgesehen ist oder wenn die Publikation zur Erfüllung einer auf einem Gesetz beruhenden Aufgabe zwingend erforderlich ist. Beides war nicht der Fall. Sich allein auf das öffentliche Interesse zu berufen, ersetzt die gesetzliche Grundlage nicht. Der gesetzlich vorgesehene Weg zur Eintreibung von Steuerschulden ist das Zwangsvollstreckungsverfahren. Zudem sei die Tauglichkeit solcher Mittel, so das Gericht weiter, mitnichten erwiesen. Die Publikation der Steuerschulden war deshalb zum Vollzug der Steuergesetze auch nicht erforderlich.

3. E-Mail Fälschung als Urkundenfälschung

[Rz 16] In einem Betrugsfall hat der Täter im Rahmen seiner Täuschungshandlungen an ihn gerichtete E-Mails von Drittpersonen abgeändert und zu Beweiszwecken an die Geschädigten weitergeleitet. Das Bundesgericht hält fest, dass E-Mails Urkunden im Sinne von Art. 110 Abs. 4 des Strafgesetzbuches (StGB) sind und dass die Fälschung von E-Mails als Urkundenfälschung zu qualifizieren ist.[6] Dies gilt unabhängig davon, ob eine E-Mail in ausgedruckter Form oder als Computer-Urkunde vorliegt. Auch nicht erforderlich ist, dass eine E-Mail digital signiert ist.

[Rz 17] Die Erkennbarkeit des Ausstellers ergibt sich, wenn nicht schon aus der Absenderadresse, so jedenfalls aus dem Inhalt der E-Mail. Diese wird dem Empfänger auf seinen E-Mail-Account zugestellt und dort gespeichert, wobei auf diesen E-Mail-Account nur mittels Passwort zugegriffen werden kann. Hieraus folgen Beständigkeit und Beweisfunktion der Erklärung. Beweiseignung und Beweisbestimmung ergeben sich aus dem Umstand, dass E-Mails im regulären Geschäftsverkehr weit verbreitet sind. Ob eine E-Mail digital signiert ist oder nicht, spielt dabei keine Rolle, denn die digitale Signatur hat gemäss Bundesgericht zwar Auswirkungen auf die Beweiskraft, nicht aber auf die Beweiseignung; und nur die Beweiseignung ist Tatbestandsmerkmal des Urkundenbegriffs.

4. Verkauf von Steuerdaten

[Rz 18] Das Bundesstrafgericht verurteilte einen externen IT-Mitarbeiter einer Bank wegen qualifiziertem wirtschaftlichen Nachrichtendienst (Art. 273 StGB) und Geldwäscherei (Art. 305bis StGB) sowie wegen der Verletzung des Geschäftsgeheimnisses (Art. 162 StGB) und des Bankge-

5 Urteil VWBES.2013.215des Verwaltungsgerichts des Kantons Solothurn vom 9. Dezember 2013.

6 Urteil des Bundesgerichts 6B_130/2012vom 22. Oktober 2012, publiziert in BGE 138 IV 209.

heimnisses (Art. 47 des Bankengesetzes [BankG]) zu 36 Monaten Gefängnis und zur Ablieferung von EUR 880'000 an die Staatskasse.[7] Der Mitarbeiter hatte interne Bankdaten kopiert und diese auf einem Datenträger für EUR 1.1 Mio. an deutsche Steuerbehörden verkauft. Vermittlerdienste leistete ein pensionierter deutscher Steuerfahnder, welcher dafür vom Verurteilten mit EUR 220'000 entschädigt wurde. Die Bankdaten betrafen 2'700 Datensätze von vermögenden ausländischen Bankkunden (Kontonummern, Name und Wohnort, Betrag, Währung, Eröffnungsdatum). Der Mitarbeiter hatte gezielt nach den Daten gesucht und sie sich an seinen privaten E-Mail-Account geschickt.

5. Anhang 3 (Umgang mit elektronischen Kundendaten) zum FINMA Rundschreiben 2008/21 «Operationelle Risiken Banken»

[Rz 19] Die eidgenössische Finanzmarktaufsicht FINMA reguliert die Informatik von Finanzdienstleistern mit zwei Rundschreiben.[8] Grundsatz 5 des Rundschreibens «Operationelle Risiken Banken» verpflichtet die Banken zum Unterhalt einer angemessenen Technologieinfrastruktur. Insbesondere ist die Sicherheit, die Integrität und die Verfügbarkeit der Daten und Systeme zu gewährleisten. Gestützt darauf hat die FINMA einen Anhang 3 zum Umgang mit elektronischen Kundendaten erlassen. Kundendaten werden als CID (Client Identifying Data) bezeichnet. Es handelt sich dabei um Daten, welche den Kunden direkt (Name, Kontoauszug, Unterschrift etc.) oder indirekt (Adresse, Telefonnummer, Geburtsdatum, Titel, Familienstand) identifizieren. Anhang 3 tritt auf den 1. Januar 2015 in Kraft und schreibt Folgendes vor:

- Governance: Systematische Überwachung der Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten, Einrichtung einer unabhängigen Kontrolle und Überwachung durch den Verwaltungsrat;
- Kategorisierung und Klassifizierung der Kundendaten nach Vertraulichkeitsstufen; Zuordnung von CID zu Data Owners;
- Need to Know-Grundsatz und Zugriffsberechtigungen;
- Inventarisierung der Applikationen, die CID verarbeiten;
- Anonymisierung, Pseudonymisierung oder Verschlüsselung von CID beim Datenexport;
- angemessene Sicherheitsstandards; Beurteilung auf allen Stufen (Endgeräte, Netzwerk, Speicher);
- Auswahl, Schulung und Überwachung der Mitarbeiter mit CID-Zugriff; Identifikation der privilegierten Nutzer (IT-Mitarbeiter, Massen-CID Bearbeitung, Kontrollverantwortung);
- 4-Augen- und Logprinzip;
- besondere Sorgfalt bei Datenmigrationen;
- Due Diligence des Outsourcing Providers im Hinblick auf seine Fähigkeit zur Verarbeitung von CID;
- Aufrechterhaltung einer «Retained Organisation» der Bank, welche die Einhaltung der CID-Richtlinien überwacht.

---

7 Urteil des Bundesstrafgerichts SK.2013.26vom 22. August 2013.

8 FINMA-Rundschreiben 2008/7 «Outsourcing Banken» und FINMA-Rundschreiben 2008/21 «Operationelle Risiken Banken».

III. Urheberrecht

1. Bildungssoftware

[Rz 20] Das Obergericht des Kantons Zürich äusserte sich im Entscheid «Bildungssoftware» zum urheber- und lauterkeitsrechtlichen Schutz von Software.[9] Die Klägerin entwickelte und vertrieb eine Software für die Aufzeichnung und Verbreitung von Lehrveranstaltungen. Die Beklagten waren als Softwareentwickler bei der Klägerin angestellt. Unmittelbar nach der Kündigung ihrer Arbeitsverhältnisse gründeten sie ein eigenes Unternehmen und brachten eine eigene Software mit praktisch identischer Funktionalität auf den Markt. Ein gerichtliches Gutachten ergab, dass einzelne Komponenten kopiert und anschliessend bearbeitet wurden. Abgesehen von den kopierten Komponenten beurteilte der Gutachter die Software der Beklagten jedoch als Neuentwicklung.

[Rz 21] Auch in der Schweiz gilt die in der deutschen Lehre entwickelte «kleine Münze» als unterste Grenze der Schutzwürdigkeit. Urheberrechtlicher Schutz von Software stellt die Regel dar, fehlende Individualität die Ausnahme, weshalb beim urheberrechtlichen Schutz von Software von der erforderlichen Individualität ausgegangen werden kann, ohne dass dies durch ein Gutachten nachzuweisen ist.

[Rz 22] Wer behauptet, eine Software sei nicht schutzfähig, weil sie Komponenten enthalte, die banal oder maschinell produziert worden seien oder die aus frei zugänglichen Drittquellen stammten, muss dies substantiieren und beweisen.

[Rz 23] Die Vermutung der Schutzfähigkeit gilt auch für Progammsequenzen, die für sich allein genommen schutzfähig sind (sog. Elementschutz). Auch wenn die Beeinträchtigung der Urheberrechte gering ist, muss der Inhaber nicht hinnehmen, dass Programmteile kopiert, bearbeitet oder vertrieben werden. Das Obergericht hat die Entscheidung «Bliss» nicht als einschlägig betrachtet, weil dort nicht auf den Elementschutz eingegangen worden war. In Bliss wurde eine Urheberrechtsverletzung noch abgelehnt, weil die Software zu 95% eine Neuentwicklung war.[10]

[Rz 24] Ob eine Urheberrechtsverletzung vorliegt, entscheidet sich aufgrund eines Vergleichs des geschützten Programms mit dem zu beurteilenden Programm. Dabei ist auf den Quell- oder Sourcecode abzustellen. Indizien, die auf ein Kopieren schliessen lassen, sind:

- die Übereinstimmung von Programmcode in einem Umfang, der nicht mehr durch Zufall oder freies Nachschaffen erklärt werden kann (in casu Übereinstimmung von 46–98% des Programmcodes der betroffenen Module);
- Übernahme von Eigentümlichkeiten;
- identische Reihenfolge von Funktionen;
- identische Kommentare.

[Rz 25] Ob eine freie Benutzung oder eine Bearbeitung bzw. ein Werk zweiter Hand vorliegt, entscheidet sich ebenfalls anhand einer Codeanalyse. Bei der Abgrenzung zwischen freier Benutzung und Bearbeitung ist zu beachten, dass als Ausgleich zu den geringen Anforderungen an die Individualität von Computerprogrammen der Spielraum für erlaubte Nachschöpfungen relativ gross ist. Die Verfolgung des gleichen Zweckes, ein ähnlicher Programmierstil und eine ähnliche

---

[9] Urteil des Obergerichts des Kantons Zürich LK100006-0/Uvom 24. Januar 2013; kommentiert durch Reto M. Hilty in sic! 2013 697 ff.

[10] Urteil des Einzelrichters am Obergericht des Kantons Aargau vom 31. Juli 1990, publiziert in SMI 1991 97 ff.

Funktionalität sind sowohl urheberrechtlich als auch lauterkeitsrechtlich unbedenklich.

[Rz 26] Die einem Computerprogramm zugrunde liegenden Grundsätze und Ideen, insbesondere die Algorithmen und die Programmlogik, fallen nicht in den Schutzbereich des Urheberrechts.

[Rz 27] Für einen maschinell durch die Entwicklungsumgebung generierten Code besteht kein urheberrechtlicher Schutz.

[Rz 28] Für in sich geschlossene Teile von Computerprogrammen kann lauterkeitsrechtlicher Schutz bestehen, selbst wenn sie dem urheberrechtlichen Werkbegriff nicht genügen. Doch setzt ein Arbeitsergebnis im Sinne von Art. 5 des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) eine gewisse geistige oder materielle Anstrengung voraus.

[Rz 29] Die Erstellung von Software während des Arbeitsverhältnisses, ohne dafür Werbung und Marketing zu machen, ist keine arbeitsvertraglich verpönte Konkurrenzierungshandlung.

[Rz 30] Die Klägerin hatte den Beklagten auch vorgeworfen, den Sourcecode als Werkzeugkasten und als Entwicklungsvorlage benutzt zu haben. Mit diesem Vorwurf der Vorlagenausbeutung drang sie nicht durch, weil er nicht ausreichend substantiiert worden war.

2. Private Strafverfolgung von illegalen Downloads

[Rz 31] Die Schweizer Landesgruppe der International Federation of the Phonographic Industry (IFPI Schweiz), der Branchenverband der Musiklabels, erstattete Strafanzeige wegen Verletzung des URG. Die Strafanzeige richtete sich gegen Nutzer bestimmter IP-Adressen. Über diese IP-Adressen waren insgesamt 1482 Musiktitel zum Download über das Internet zugänglich gemacht worden. Die Staatsanwaltschaft des Kantons Zürich trat auf die Strafanzeige nicht ein, weil sich die Strafanzeige auf IP-Adressen stützte, die in Verletzung des Datenschutzgesetzes beschafft worden waren. Die Staatsanwaltschaft berief sich dabei auf die Logistep-Praxis des Bundesgerichts.[11]

[Rz 32] Das Obergericht hob die Einstellungsverfügung auf, weil sie den Grundsatz «im Zweifel für die Anklageerhebung» verletzte.[12] Es hielt zunächst fest, dass auf die Datenerhebung durch Private im Hinblick auf eine Strafanzeige das Datenschutzgesetz und nicht die Strafprozessordnung zur Anwendung gelangt. Davon zu unterscheiden ist die Frage der Verwertbarkeit solcher Daten im Strafverfahren. Diesbezüglich ist Art. 141 der Strafprozessordnung (StPO) einschlägig. Diese Bestimmung richtet sich nur an die Strafverfolgungsbehörden und die Frage der Verwertbarkeit von Beweismitteln, die durch Private unrechtmässig beschafft wurden, ist durch den Gesetzgeber offen gelassen worden. Gemäss Praxis ist eine Verwertung solcher Beweise dann zulässig, wenn sie auch von den Strafverfolgungsbehörden hätten erlangt werden können und kumulativ eine Interessenabwägung für die Verwertung spricht. Im vorliegenden Fall hatte die Staatsanwaltschaft beide Fragen nicht genügend abgeklärt.

11 BGE 136 II 508.

12 Beschluss der III. Strafkammer des Obergerichts des Kantons Zürich UE130087vom 3. Februar 2014, ZR 113/2014, S. 34.

3. AGUR 12

[Rz 33] Das Eidgenössische Justiz- und Polizeidepartement hatte im August 2012 Kulturschaffende, Produzenten, Konsumenten, Wirtschaftsverbände und Verwaltungseinheiten eingeladen, in einer Arbeitsgruppe zur kollektiven Verwertung von Urheberrechten und verwandten Schutzrechten (AGUR 12) mitzuwirken. Die AGUR 12 hatte die Aufgabe, das Urheberrecht an die Bedingungen der digitalen Wirtschaft anzupassen. Am 28. November 2013 hat die AGUR 12 den Schlussbericht abgeliefert.[13] Dabei machte die AGUR 12 die folgenden Empfehlungen, die über die reinen Urheberrechtsthemen hinaus auch für das IT-Recht relevant sind:

- Der Download aus illegaler Quelle soll, wie nach herrschender Lehrmeinung im geltenden Recht vorgesehen, weiterhin zulässig bleiben.
- Take Down: Hosting Provider sollen auf Anzeige der Rechteinhaber oder einer zuständigen Behörde unerlaubt hochgeladene Inhalte entfernen müssen.
- Stay Down: Hosting Provider, deren Geschäftsmodell offensichtlich auf Rechtsverletzungen durch Nutzer angelegt ist, sollen zusätzlich im Rahmen des Zumutbaren das erneute Hochladen verhindern müssen.
- Access Provider sollen auf behördliche Anweisung hin in schwerwiegenden Fällen den Zugang zu Webportalen mit offensichtlich illegalen Quellen über IP- und DNS-Blocking sperren müssen.
- Rechteinhaber sollen für die Ermittlung von Urheberrechtsverletzungen Internetverbindungsdaten bearbeiten dürfen, soweit sie sich an die Vorgaben des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten halten.
- Access Provider sollen auf Veranlassung der Rechteinhaber dem Inhaber eines Internetanschlusses, über welchen P2P-Netzwerke genutzt werden, einen einmaligen Warnhinweis zustellen müssen.
- Es soll den Rechteinhabern auch zum Zweck zivilrechtlicher Verfolgung möglich sein, vom Access Provider die Bekanntgabe der Identität des Anschlussinhabers zu verlangen. Bisher ist das nur im Rahmen von Strafverfahren möglich.
- Es soll analog zur Rechtslage in der EU eine Haftungsbeschränkung für Provider eingeführt werden.

4. Canal plus – eine Nachlese aus zivilrechtlicher Sicht

[Rz 34] 2012 hat das schweizerische Bundesgericht entschieden, dass der Betrieb eines Kartenfreigabesystems nicht unter den Straftatbestand von Art. 67 Abs. 1 lit. i und Art. 69 Abs. 1 lit. e des Urheberrechtsgesetzes (URG) fällt und auch nicht gegen das UWG verstösst.[14] Die Begründung war, dass der Betreiber die ausgestrahlten Sendungen nicht im Sinne von Art. 10 Abs. 2 lit. f URG wahrnehmbar macht.

[Rz 35] Trotzdem hat das anschliessend mit der Sache befasste jurassische Gericht die Zivilforderungen der Sender gestützt auf Art. 423 OR (Geschäftsführung ohne Auftrag) und Art. 41 OR

[13] Schlussbericht der AGUR 12.

[14] BGE 139 IV 1.

(unerlaubte Handlung) gutgeheissen.[15] Die Tatbestandsvoraussetzungen der Geschäftsanmassung waren erfüllt. Die unerlaubte Handlung bestand in einer Verletzung des Art. 150bis StGB (Herstellung und Inverkehrbringen von Materialen zur unbefugten Entschlüsselung von codierten Angeboten) und im Gegensatz zur strafrechtlichen war die zivilrechtliche Verjährung noch nicht eingetreten.

IV. Internet

1. Tribune de Genève

[Rz 36] Ein Genfer Politiker griff einen ehemaligen Direktor der Genfer Kantonalbank auf einem Blog der Tribune de Genève an. Er bezichtigte ihn der Bilanzfälschung und wies ihm die Verantwortung für mehrere Unternehmenskonkurse zu. Die Zeitung wurde gerichtlich angewiesen, den Beitrag von der Webseite zu entfernen.[16]

[Rz 37] Für diese Persönlichkeitsverletzung war nicht nur der Verfasser, sondern auch die Tribune de Genève verantwortlich. Anders als in der EU gibt es in der Schweiz kein gesetzliches Haftungsprivileg für Blog-Hoster und Internet-Service-Provider. Massgebend sind einzig die allgemeinen Regeln zum Persönlichkeitsrecht (Art. 28 ff. des Zivilgesetzbuches [ZGB]). Passivlegitimiert sind alle Personen, welche eine Verletzung verursachen, dulden oder begünstigen. Auch die blosse Mitwirkung führt zu einer Verletzung, selbst wenn der Handelnde sich dessen nicht bewusst ist. Der Einwand der Zeitung, dass eine Kontrolle bei Blogs anders als bei Leserbriefen gar nicht möglich sei, war unbeachtlich, denn für einen Beseitigungs- oder Unterlassungsanspruch wird kein Verschulden vorausgesetzt. Das Verschulden ist einzig bei Schadenersatz- und Genugtuungsansprüchen relevant.

[Rz 38] Dem Urteil wird einige Bedeutung zugemessen. Dies gilt nicht nur für den Bereich der Online-Medien. Es ist nicht mehr auszuschliessen, dass bei Anwendung dieser Rechtsprechung auch ein klassischer Hosting-Provider für Inhalte auf gehosteten Webseiten in Anspruch genommen werden kann.

2. Öffentlichkeit von Facebook

[Rz 39] Ein Schüler drohte auf seinem Facebook-Profil: «Ich vernichte euch alle – Pow!! Pow!! Pow!!» Das Obergericht des Kantons Zürich bestätigte die erstinstanzliche Verurteilung wegen versuchter Schreckung der Bevölkerung gemäss Art. 258 StGB.[17] Der Tatbestand setzt voraus, dass die Androhung der Gefahr öffentlich ist. Der Angeklagte argumentierte, die Äusserungen auf seinem Facebook-Profil seien privat. Das Obergericht beurteilte das anders. Privat sind Äusserungen im Familien- oder Freundeskreis oder in einem anderen, durch persönliche Beziehungen oder besonderes Vertrauen geprägten Umfeld. Das war bei diesem Facebook-Account mit 290 Facebook-Freunden nicht mehr der Fall.

---

15 Jugement de la Cour pénale du Canton Jura du 27 juin 2013, bestätigt in Urteil des Bundesgerichts 6B_819/2013vom 27. März 2014.

16 Urteil des Bundesgerichts 5A_792/2011vom 14. Januar 2013.

17 Urteil des Obergerichts des Kantons Zürich SB130371-0vom 25. November 2013.

3. Domain Namen Register

[Rz 40] Der Bundesrat hat den Entwurf der neuen Verordnung über die Internet-Domains in die Vernehmlassung gegeben. Er sieht eine Trennung der Funktionen der Registerbetreiberin (Registry) und der Vermarktung der Domain-Namen durch Registrare vor.

4. Eine neue GTLD für die Schweiz

[Rz 41] Für die neue Generic Top Level Domain (GTLD) «.swiss» übernimmt das Bundesamt für Kommunikation (BAKOM) die Funktion der Registerbetreiberin. Unternehmen, die eine solche Domain beantragen, müssen einen Sitz in der Schweiz oder einen besonderen Bezug zur Schweiz haben.

[Rz 42] Ursprünglich war beabsichtigt, die Registrierung von Domainnamen unter der GTLD «.swiss» ab Herbst 2014 zuzulassen. Dies wird nicht möglich sein, weil die Behörden zuerst die erforderlichen Voraussetzungen zur administrativen Abwicklung schaffen müssen.

[Rz 43] Das Verfahren wird in der neuen Verordnung über Internet Domains geregelt. Bei der Zuteilung erfolgt eine Prüfung, ob eine ausreichende Verbindung zur Schweiz besteht und ob die beantragte Bezeichnung einen objektiven Bezug zwischen dem Gesuchsteller und der vorgesehenen Nutzung aufweist. Mit diesem Prüfungsverfahren wird Neuland betreten. Erstmals wird bei der Registrierung von Domains analog zum Firmen- und Markenrecht präventiv eine inhaltliche Berechtigung geprüft.

5. Passivlegitimation der Registerbetreiberin

[Rz 44] Zwei Parteien stritten sich über die Berechtigung an einem Domainnamen. Die Klägerin hatte den Domainnamen ursprünglich selber reserviert, jedoch nicht direkt bei der Registerbetreiberin, sondern bei einem Registrar. Der Klägerin sind die Zugangsdaten zur Verwaltung des Domainnamens auf nicht näher geklärte Weise abhanden gekommen und der Registrar stellte ihr keine neuen Zugangsdaten zu. Die Klägerin richtete ihr Massnahmebegehren nicht nur gegen ihre direkte Prozessgegnerin, sondern auch gegen die Registerbetreiberin. Sie wollte ihr verbieten lassen, Zugangsdaten zu den umstrittenen Domainnamen an ihre Gegnerin herauszugeben.

[Rz 45] Das Gericht hat die Passivlegitimation der Registerbetreiberin verneint und das Massnahmebegehren abgewiesen.[18] Das von der Klägerin gewählte Vorgehen war nicht zielführend. Besser wäre es gewesen, nur ihre direkte Prozessgegnerin ins Recht zu fassen. In diesem Verfahren kann auch eine gerichtliche Anordnung gegenüber der Registerbetreiberin beantragt werden.

6. Verzicht auf ein Social Media-Gesetz

[Rz 46] Die Schweiz verzichtet darauf, Social Media in einem Spezialgesetz zu regeln. Nach einem Bericht des Bundesrates genügen die allgemeinen Regeln des Daten- und Persönlichkeitsschutzes. Hingegen wurde das Eidgenössische Justiz- und Polizeidepartement beauftragt, gesetz-

[18] Urteil des Handelsgerichts des Kantons Zürich HE130146-Ovom 25. Juni 2013.

geberischen Handlungsbedarf in Bezug auf die zivilrechtliche Verantwortlichkeit von Internet-Dienstleistern abzuklären. Zudem wird geprüft, welche Regeln des Fernmelderechts auch für Social Media-Plattformen gelten sollen.

7. Internet-Teilnehmeridentifikation

[Rz 47] In einer Strafuntersuchung wegen Kinderpornografie verlangte die ermittelnde Staatsanwaltschaft am 13. August 2012 die rückwirkende Teilnehmeridentifikation eines Internetanschlusses. Das Zwangsmassnahmengericht des Kantons Aargau wies das Gesuch ab mit der Begründung, die sechsmonatige Frist gemäss Art. 273 Abs. 3 StPO sei abgelaufen. Das war gemäss Bundesgericht nicht zulässig.[19]

[Rz 48] Art. 273 StPO regelt die Bekanntgabe der sog. Verbindungsranddaten an Strafverfolgungsbehörden. Abs. 3 besagt, dass die Bekanntgabe von Randdaten für die Dauer der Überwachung sowie bis zu 6 Monate rückwirkend verlangt werden kann. Gleichzeitig sind Fernmeldedienstanbieter gemäss Art. 12 Abs. 2 und Art. 15 Abs. 3 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) verpflichtet, Randdaten während mindestens 6 Monaten aufzubewahren.

[Rz 49] Wie aber verhält es sich, wenn Fernmeldedienstanbieter wie vorliegend Randdaten freiwillig für eine längere Frist aufbewahren? Dabei sind zwei Fälle zu unterscheiden.

[Rz 50] Wurde eine Straftat über das Internet begangen, gelangt Art. 14 Abs. 4 BÜPF als lex spezialis zur Anwendung. Diese Bestimmung sieht keine zeitliche Beschränkung vor. In allen anderen Fällen ist Art. 273 Abs. 3 StPO einschlägig. Diese Bestimmung ist so auszulegen, dass die Bekanntgabe für eine rückwirkende Dauer von bis zu 6 Monaten ohne weitere Begründung erlaubt ist. Für eine längere Dauer sind besondere Gründe erforderlich.

8. Büpf-Revision

[Rz 51] Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs befindet sich in Revision. Die Dauer der Vorratsdatenspeicherung soll von 6 auf 12 Monate erhöht werden und die Verwendung von Staatstrojanern soll ausdrücklich erlaubt sein. Die Revision wird von der ICT-Branche wegen der damit verbundenen Kosten kritisiert. Es ist nicht mit einem Inkrafttreten vor 2016 zu rechnen.

V. Vergaberecht

1. Produktebezogene Ausschreibungen

[Rz 52] Die AlpTransit Gotthard AG ist eine Tochtergesellschaft der SBB und ist für den Bau des Gotthard-Basistunnels verantwortlich. Sie schrieb die Entwicklung einer Projektmanagementsoftware für das Kosten- und Finanzcontrolling sowie den Landerwerb des Infrastruktur-Grossprojektes AlpTransit Gotthard aus. Ausgeschrieben war ein Basissystem, das im Projektverlauf auf die indi-

[19] Urteil des Bundesgerichts 1B_481/2012vom 22. Januar 2013, publiziert in BGE 139 IV 98ff.

viduellen Bedürfnisse angepasst werden sollte. Ein Kriterium war, dass das Gesamtsystem auf einer mit VMWare virtualisierten Microsoft-Plattform (inkl. der Datenbank Microsoft SQL-Server) betrieben werden sollte.

[Rz 53] AlpTransit untersteht dem öffentlichen Beschaffungsrecht der Schweizerischen Eidgenossenschaft. Der Auftrag wurde für CHF 3 Mio. vergeben. Ein im Ausschreibungsverfahren unterlegenes Konsortium hat den Zuschlag angefochten. Die Vergabestelle hatte das Konsortium schon frühzeitig ausgeschlossen, weil ihr Basissystem auf einer Oracle Datenbank basierte. Dieser Ausschluss war unzulässig.

[Rz 54] Das Gericht stellte aufgrund einer Analyse der Ausschreibungsbedingungen fest, dass erst das fertiggestellte Gesamtsystem die Anforderungen betreffend Interoperabilität mit der Microsoft-Technologie-Plattform erfüllen müsse. Dies gelte nicht schon für das Basissystem. Wird im Rahmen der Erteilung des Zuschlags nur ein bestimmtes Fabrikat zugelassen, obwohl dieses nicht als technische Spezifikation definiert worden ist, liegt ein Verstoss gegen das Transparenzprinzip vor. Um eine übermässige Beschränkung des Wettbewerbs zu verhindern, soll das gewünschte Produkt nicht unter Bezugnahme auf besondere Handelsmarken oder Handelsnamen oder einen bestimmten Ursprung umschrieben werden. Und weiter: Vergabebehörden dürfen technische Spezifikationen im Regelfall nicht derart eng umschreiben, dass nur ein ganz bestimmtes Produkt oder nur wenige Anbieter für die Zuschlagserteilung in Frage kommen.

2. Inländerbevorzugung nach NSA-Skandal

[Rz 55] Das Bundesamt für Bauten und Logistik (BBL) hat im Juni 2013 die Carrier Ethernet Dienste für die Bundesverwaltung ausgeschrieben. Der Zuschlag ging am 5. Februar 2014 an die Swisscom. Der Auftrag hat einen Wert von CHF 230 Mio. 7 Tage vorher hatte der Bundesrat mit Beschluss vom 29. Januar 2014 entschieden, dass aufgrund des NSA-Skandals kritische Informations- und Kommunikationstechnik-Leistungen für die Bundesverwaltung aus Gründen der Staatssicherheit künftig von ihr selbst oder von besonders qualifizierten Unternehmen erbracht werden sollen. Bei letzteren muss es sich um Unternehmen handeln, welche ausschliesslich unter Schweizer Recht agieren, welche sich zur Mehrheit in Schweizer Eigentum befinden und welche ihre Leistungen gesamtheitlich innerhalb der Schweizer Landesgrenzen erzeugen. Ein amerikanisch-englisches Unternehmen führte dagegen Beschwerde. In einem Zwischenentscheid hat das Bundesverwaltungsgericht dessen Beschwerdelegitimation einstweilen bejaht.[20] Diese war strittig, denn nach Ansicht der Verwaltung kam das Unternehmen aufgrund des besagten Bundesratsbeschlusses als Anbieterin gar nicht mehr in Frage. Der materielle Entscheid ist noch ausstehend.

3. HP-Bildschirme

[Rz 56] Das Bundesamt für Bauten und Logistik (BBL) wollte insgesamt 40'000 Flachbildschirme in zwei Dimensionen (22 und 24 Zoll) beschaffen. Es schrieb dafür Rahmenverträge aus. Die von Hewlett Packard offerierten 22-Zoll-Bildschirme wiesen eine Bilddiagonale von 22.9921 Zoll (584

[20] Zwischenentscheid des Bundesverwaltungsgerichts B-998/2014vom 21. Mai 2014.

mm) auf. In den Ausschreibungsunterlagen wurde für die 22-Zoll-Bildschirme (wenn auch etwas missverständlich) ein Toleranzbereich von 535–575 mm angegeben.

[Rz 57] Gemäss Art. 12 Abs. 1 des Bundesgesetzes über das öffentliche Beschaffungswesen (BöB) bezeichnet die Auftraggeberin die technischen Spezifikationen. Ihre Nichterfüllung führt unabhängig vom Vergleich mit den anderen Angeboten zur Nichtberücksichtigung. Dem steht auch das Verbot des überspitzten Formalismus nicht entgegen. Das Bundesverwaltungsgericht hat deshalb die Nichtberücksichtigung der HP-Bildschirme als rechtmässig beurteilt.[21]

[Rz 58] Der Entscheid steht in einem gewissen Widerspruch zu einem früheren Entscheid des Bundesgerichts, in welchem es eine Vergabestelle schützte, die ein Kopiergerät in die Evaluation einbezogen hatte, das mehr als die vorgegebene Höchstleistung von 20 Kopien pro Minute erbrachte.[22]

4. AGB SIK

[Rz 59] Die Schweizerische Informatikkonferenz (SIK), ein Interessenverband von Informatikanwendern aus dem Bereich der öffentlichen Verwaltung, überarbeitet ihre AGB. Sie sollen nach einer Vernehmlassung 2014 in Kraft treten. Die Version 2004 der AGB SIK hat bei der Beschaffung von Informatikleistungen durch öffentliche Verwaltungen eine grosse Verbreitung erreicht. Die AGB SIK gelten auch aus Sicht der Anbieter als ausgewogen und geniessen eine hohe Akzeptanz.

[Rz 60] Die wesentlichste Neuerung betrifft den formellen Aufbau. Der Revisionsentwurf besteht nicht mehr aus fünf unabhängigen AGB für die einzelnen Leistungsarten. Stattdessen werden alle Leistungsarten in einem einzigen, einheitlich gestalteten Dokument geregelt.

[Rz 61] Der Revisionsentwurf ist auf werkvertragliche, auftragsrechtliche und kaufrechtliche Leistungen beschränkt. Der bedeutende und stark wachsende Bereich der Services (z.B. Outsourcing) bleibt unberücksichtigt.

[Rz 62] Inhaltlich bringt der Revisionsentwurf tendenziell eine Verschlechterung der Position der Anbieter:

- Es fehlt eine betragsmässige Beschränkung für die Haftung des Anbieters. Ausgeschlossen ist nur noch die Haftung für entgangenen Gewinn. Im Übrigen sollen die Anbieter unbeschränkt haften. Dies gilt beispielsweise auch für die Verursachung von Datenschäden.
- Der Revisionsentwurf verzichtet auf die Abnahmefiktion bei Aufnahme des Produktivbetriebs und schliesst die Anrechnung einer Konventionalstrafe an den Gesamtschaden aus.
- Die Gewährleistungsfrist wird entsprechend dem revidierten Kauf- und Werkvertragsrecht auf 2 Jahre verlängert.
- Bei Vertragsrücktritt durch den Kunden infolge Verzugs soll der Anbieter verpflichtet werden, den Quellcode herauszugeben.
- Bei der Zuteilung der Immaterialgüterrechte bleibt es dabei, dass diese bei Individualentwicklungen auf den Kunden übergehen sollen.
- Bezüglich Vertragshierarchie wird ausdrücklich gesagt, dass die Offerte dem Pflichtenheft

[21] Urteil des Bundesverwaltungsgerichts B-3526/2013vom 20. März 2014.

[22] Urteil des Bundesgerichts 2P.141/2002vom 7. Januar 2003.

vorgeht.
- Die kostenpflichtige Wartung setzt nicht mehr automatisch erst nach Ablauf der Garantiefrist ein.

[Rz 63] Der stark im OR und in der schweizerischen Vertragstradition verankerte Revisionsentwurf ist handlicher als die Vorgängerversion. Er wird von internationalen Anbietern deswegen aber möglicherweise weniger gut verstanden.

Dr. Urs Egli, Rechtsanwalt, ist Partner in einer Wirtschaftskanzlei in Zürich (www.epartners.ch) und hat sich auf Informatik- und Technologierecht spezialisiert. Der Beitrag basiert auf einem Referat des Autors anlässlich des Dreiländer-Treffens der deutschen Gesellschaft für Recht und Informatik (DGRI) vom 11./12. Juli 2014 in Linz.