



europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law
vienna | brussels | london | leipzig | prague | budapest

www.e-center.eu

partner: das | deloitte | erste bank | hutchison | mbo-media | microsoft | mobilkom austria | orange | raiffeisen
informatik | siemens | six card solutions | telekom austria | tele.ring | t-mobile | wolf theiss
leitung: ao. univ.-prof. dr. wolfgang zankl

Sehr geehrte Leserinnen und Leser der e-center law survey!

Das e-center freut sich, Ihnen wieder eine Auswahl aktueller Themen aus dem Bereich E-Commerce und IT-Recht übermitteln zu können, und wünscht eine informative Lektüre der neuen Artikel.

Falls Sie keine weiteren Zusendungen von uns erhalten wollen, teilen Sie uns dies bitte unter folgender Adresse mit: office@e-center.eu

Mit freundlichen Grüßen,
Ihr
e-center law survey-team

- 1) **News@e-center**
- 2) **Oberster Gerichtshof stärkt Medienfreiheit**
- 3) **Datenschutzrat hofft auf EU-Lösung**
- 4) **Frau für Filesharing ihrer Familie verurteilt**
- 5) **US-Gesetzesentwurf zu globaler Netzfreiheit wiederbelebt**
- 6) **Vorratsdaten: Raubkopierer statt Terroristen als Ziel**
- 7) **EuGH: Gewinnspielrechtliches Kopplungsverbot in Deutschland europarechtswidrig**
- 8) **Europol in der dritten Generation**
- 9) **Gezielte Angriffe auf Unternehmen gehen weiter**
- 10) **Neuerungen: Bei Angaben zu Mehrwertdienstenummern (Deutschland)**
- 11) **Kriminalpolizei: Köperscanner garantieren keine Sicherheit**
- 12) **Das neue Rechnungslegungsänderungsgesetz - was sich ab 2010 ändert!**

News@e-center

Veranstaltungen:

- 28.01.2010, 18.00 Uhr: Security 2010, Urania, Generalthema "Internetsperren aus der Sicht des Mobilfunks"

Oberster Gerichtshof stärkt Meinungsfreiheit

Der Oberste Gerichtshof von Kanada stärkte in einer aktuellen Entscheidung die Pressefreiheit. In Zukunft wird es für kanadische Journalisten möglich sein, sich in Verleumdungsprozessen auf "verantwortungsvolle Kommunikation im öffentlichen Interesse" zu berufen.

Für das Urteil des Supreme Court of Canada galt es für die Richter zwischen freier Meinungsäußerung, Pressefreiheit, dem Schutz der Ehre, dem Persönlichkeitsschutz und dem öffentlichen Interesse an Informationen abzuwägen. Es muss möglich sein, öffentliche und politische Debatten zu führen. *Der öffentliche Austausch von Informationen ist lebensnotwendig für eine moderne kanadische Gesellschaft*, so die Richter. Die Verteidigungsmöglichkeiten der Journalisten wurden ausgearbeitet. So muss dargelegt werden, dass die Nachricht von öffentlichem Interesse war und dass sich der Journalist verantwortungsvoll bei der Beschaffung der Informationen verhalten hat. Wenn dies der Fall ist, darf berichtet werden - auch wenn sich später Tatsachen als falsch erweisen.

Debatte über ein Bauprojekt

Der Fall drehte sich um einen Geschäftsmann, der auf seinem weitläufigen Grundstück einen Golfplatz errichtet hatte und diesen nun vergrößern wollte. Die Anrainer äußerten allerdings Kritik an dem Bauvorhaben, da der Golfplatz deren Lebensqualität und die Umwelt negativ beeinflussen würde. Nachdem Protestbriefe an die zuständige Umweltbehörde geschickt worden waren, wurde ein öffentliches Treffen abgehalten, um die Bedenken der Anrainer zu zerstreuen. Ein Journalist der Zeitung Toronto Star griff daraufhin das Thema auf und veröffentlichte schließlich am 23. Juni 2001 einen Artikel darüber. In dem Text wurden die politischen Kontakte des Geschäftsmannes aufgezeigt und die Meinungen der Anrainer wiedergegeben. Es wurde die Vermutung geäußert, dass der Geschäftsmann seinen politischen Einfluss dazu benutzte, um die Genehmigung für das Bauprojekt zu erhalten. Der Journalist hatte sich um eine Stellungnahme des Geschäftsmannes bemüht, dieser lehnte ein Interview allerdings ab.

Nach Veröffentlichung klagte der Geschäftsmann, da der Artikel einseitig sei und seinen guten Ruf gefährde. Dem Gericht stellte sich nun die Frage, ob eine Verteidigungsmöglichkeit aufbauend auf *verantwortungsvoller Kommunikation im Interesse der Öffentlichkeit* möglich gemacht werden soll. Für die Entscheidung wurde das Recht in Großbritannien, Australien, Neuseeland und Südafrika zitiert und damit aufgezeigt, dass eine Reihe von Ländern in den letzten Jahren das Persönlichkeitsrecht modifiziert haben.

Kommunikation im öffentlichen Interesse

Die kanadischen Richter kamen zu dem Schluss, dass die Kommunikation im öffentlichen Interesse besser geschützt werden müsse. Dazu wurden die Kriterien ausgearbeitet nach denen journalistische Arbeiten beurteilt werden sollen. Um festzustellen, ob es sich um eine Veröffentlichung im öffentlichen Interesse handelt, muss die gesamte Publikation bewertet werden, nicht die einzelne Aussage alleine. Das Thema muss die öffentliche Aufmerksamkeit auf sich ziehen, die Bevölkerung betreffen oder eine öffentliche Kontroverse beinhalten. Nicht notwendig ist, dass es sich dabei um politische Angelegenheiten handelt oder eine Person des öffentlichen Interesses betroffen ist. Ob eine Anschuldigung in verantwortungsvoller Art und Weise geschah, ist unter anderem abhängig von der Anschuldigung selbst, von der Dringlichkeit, von der Glaubwürdigkeit der Quelle und der Präsentation. So ist etwa zu beurteilen, ob beide Seiten zu Wort gekommen sind und der Kontext wiedergegeben wird, in dem die Aussagen gefallen sind.

Nach diesen Überlegungen hoben die Richter die vorinstanzliche Verurteilung des Journalisten und der Zeitung auf und ordneten ein neues Verfahren an. In dem Bericht des Toronto Stars wurde dieses Urteil als *historischer Sieg für alle Kanadier* und als *wichtigste Entscheidung in einem Ehrenbeleidigungsprozess* bezeichnet.
30.12.2009 journal.juridicum.at

Supreme Court of Canada, Urteil vom 22.12.2009
Grant v. Torstar Corp., 2009 SCC 61

Links zu dem Artikel

<http://www.scc-csc.gc.ca/>

<http://scc.lexum.umontreal.ca/en/2009/2009scc61/2009scc61.html>

<http://www.mnr.gov.on.ca/en/index.html>

<http://www.thestar.com/>

<http://www.thestar.com/news/canada/article/742242--top-court-expands-freedoms-for-media>

Datenschutzrat hofft auf EU-Lösung

Der Datenschutzrat (DSR) will die geplante Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung in Österreich vorerst nicht bewerten, weil ein zwischen den Ministerien abgestimmtes Gesamtpaket fehlt. DSR-Vorsitzender Johann Maier (SPÖ) hofft jedoch, dass die umstrittene Richtlinie auf europäischer Ebene zu Fall gebracht wird.

Am Freitag endete die Begutachtungsfrist zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung (Data-Retention). Schon davor zeichnete sich ab, dass der vom Ludwig-Boltzmann-Institut für Menschenrechte (BIM) erarbeitete Gesetzesentwurf zur Novelle des Telekommunikationsgesetzes (TKG) keine Mehrheit im Ministerrat finden wird.

Aus dem Innenministerium und aus dem Justizressort kamen Forderungen, die über den Entwurf hinausgehen. Der Datenschutzrat im Bundeskanzleramt werde daher vorerst kein detailliertes Gutachten abgeben, sagte Maier am Freitag bei einer Pressekonferenz in Wien.

Erst wenn die Wünsche der Ministerien in einem mit dem bei der Vorratsdatenspeicherung federführenden Infrastrukturministerium in einem interministeriell abgestimmten Gesamtpaket vorliegen, werde der Datenschutzrat eine Bewertung vornehmen, so Maier.

"Nicht mit europäischen Grundrechten vereinbar"

Maier machte aber klar, dass die EU-Richtlinie nach Meinung des Datenschutzrates nicht mit den europäischen Grundrechten vereinbar sei. Die Richtlinie, die die verdachtsunabhängige verpflichtende Speicherung von Verbindungsdaten für mindestens sechs Monate vorsieht, verstoße gegen Datenschutzbestimmungen und gegen das Telekommunikationsgeheimnis.

Infrastrukturministerin Doris Bures (SPÖ) hatte die Novelle, mit der das TKG überarbeitet werden soll, von einer Expertengruppe unter Federführung des Boltzmann-Instituts für Menschenrechte ausarbeiten lassen. Der Vorschlag beinhaltet eine Mindestumsetzung der Richtlinie, also eine maximal sechsmonatige Speicherdauer der Daten, Verwendung nur für die Aufklärung von schweren

Straftaten und nur mit richterlicher Anordnung.

Die Richtlinie für die Vorratsdatenspeicherung, die unter dem Eindruck der Terroranschläge in New York und Spanien beschlossen wurde, sieht die Speicherung von Verbindungsdaten vor, im Wesentlichen wer mit wem wann wie lange von wo aus kommuniziert hat, nicht aber die Inhalte.

Forderungen von Justiz- und Innenministerium

Das Justizministerium dränge etwa darauf, dass auch bei Urheberrechtsverletzungen auf die gespeicherten Daten zugegriffen werden kann, so Maier. Der Datenschutzrat hält die Datenherausgabe zur Verfolgung zivilrechtlicher Ansprüche für problematisch. "Das entspricht nicht dem Zweck der Richtlinie", kritisierte Maier.

Konkret regte das Justizministerium in seiner Stellungnahme an, im Urheberrechtsgesetz (§87, Abs. 3) geregelte Auskunftspflichten gegenüber Rechteinhabern abzusichern. Um die Auskunftsansprüche erfüllen zu können, sollen die Daten Rechteinhabern "zumindest drei Monate" verpflichtend zur Verfügung stehen.

Auch das Innenministerium wolle einen Zugriff bei weniger schweren Straftaten, weswegen der Datenschutzrat eine restriktive Definition verlangt. Das Innenministerium behaupte, dass die Umsetzung der Richtlinie in ihrer derzeitigen Form die Arbeit der Polizei erschweren würde und niederschwellige Kriminalität nicht verfolgt werden können, sagte Maier. "Diese Argumentation ist in vielen Punkten nicht richtig." Auch sei vom Innenressort der Wunsch nach einer Speicherung für ein ganzes Jahr anstelle von sechs Monaten gekommen.

Begleitmaßnahmen erforderlich

Sollte es zu einer Umsetzung der EU-Richtlinie kommen, seien Begleitmaßnahmen bei Sicherheitsbehörden und Justiz erforderlich, "mit denen sichergestellt werde, dass der verhältnismäßige Einsatz gewährleistet ist", so Maier: "Das Rechtsbewusstsein muss gestärkt werden."

Maier forderte auch Ausnahmeregelungen für Journalisten, Ärzte und Seelsorger, deren Arbeitsgrundlage durch die Vorratsdatenspeicherung in Verbindung mit bereits bestehenden Überwachungsmöglichkeiten gefährdet sei.

Hoffen auf Umdenken in Europa

Der Datenschutzrat rät auch, die Entwicklung der Vorratsdatenspeicherung auf europäischer Ebene abzuwarten, und hofft auf ein Umdenken. Gegen 19 Staaten - darunter Österreich - würde derzeit ein Vertragsverletzungsverfahren wegen Nicht- oder mangelhafter Umsetzung laufen. Eben erst hatten auch die rumänischen Verfassungsrichter die Vorratsdatenspeicherung in ihrem Land aufgehoben.

Mit Spannung wird eine Entscheidung des deutschen Bundesverfassungsgerichts in Karlsruhe erwartet, die auch die deutsche Umsetzung kippen könnte. Maier brachte auch den Vertrag von Lissabon zur Sprache, der die Grundrechte stärken und es ermöglichen, die Richtlinie vor den Europäischen Gerichtshof zu bringen.

Mit der neuen EU-Kommission könnte eine grundsätzliche Änderung der Haltung zur Vorratsdatenspeicherung eintreten, sagte Maier unter Verweis auf die Stellungnahmen der designierten EU-Justizkommissarin Viviane Reding bei ihrer Anhörung vor dem EU-Parlament am Dienstag. Reding habe deutlich die Priorität der Privatsphäre und des Datenschutzes zum Ausdruck gebracht und das EU-Parlament aufgefordert, sich keine Regeln aufzwingen zu lassen, die gegen die Grundrechte verstoßen.

15.01.2010 futurezone.orf.at

Links zu dem Artikel

http://www.bka.gv.at/site/cob_37802/6343/default.aspx

http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117_12/imfname_177357.pdf

http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117_34/fname_177491.pdf

http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml

<http://futurezone.orf.at/stories/1636210/>

<http://futurezone.orf.at/stories/1636361/>

<http://futurezone.orf.at/stories/1633990/>

Frau für Filesharing ihrer Familie verurteilt

Anschlussinhaberin muss 2.380 Euro Abmahnkosten zahlen - 964 Songs zum Tausch angeboten

In Deutschland ist eine Frau zur Zahlung von 2.380 Euro Abmahnkosten verklagt worden, da über den auf ihren Namen laufenden Internetanschluss Musik zum Filesharing angeboten worden sei. Wer genau die rund 964 MP3-Dateien ins Web hochgeladen hat, sei zwar nicht bekannt, dennoch sei die Frau dafür verantwortlich, berichtet Golem.

Kontrollpflicht vernachlässigt

Neben der Frau hätten auch ihr Mann und die beiden Söhne Zugang zum Internet gehabt. Die Frau habe den Upload bestritten, wollte dem Gericht aber auch nicht sagen, wer die Songs im Jahr 2005 zum Tausch bereit gestellt habe. Das Gericht habe deshalb entschieden, dass die Anschlussinhaberin verantwortlich sei, da sie keine Maßnahmen eingesetzt habe, damit ihre Kinder keine Tauschbörsen nutzen können. Da sie die Aktivitäten über den Internetanschluss nicht überwacht habe, sei sie nicht ihrer elterlichen Kontrollpflicht nachgekommen.

Keine Berufung

Klage eingereicht hatten die Musikkonzerne EMI, Sony, Universal und Warner. Neben den Abmahnkosten in Höhe von 2.380 Euro müsse die Frau auch noch die Verfahrenskosten tragen, deren Höhe noch nicht festgesetzt sei. Da die Frau eine Unterlassungserklärung unterzeichnet habe, sei eine Berufung nicht möglich.

08.01.2010 www.derstandard.at

Links zu dem Artikel

<http://www.golem.de/1001/72284.html>

<http://www.emigroup.com/Default.htm>

<http://www.sony.at/section/home>

<http://www.it-recht-kanzlei.de/index.php?id=%2Fview&cid=4279>

US-Gesetzesentwurf zu globaler Netzfreiheit wiederbelebt

Nach dem angedrohten Rückzug von Google aus China hat der US-Abgeordnete Chris Smith die rasche Verabschiedung eines von ihm ins Repräsentantenhaus eingebrachten Gesetzesentwurfs gegen Internetzensur gefordert. Der sogenannte Global Online Freedom Act sei nötig, da ohne diesen US-Firmen "unausweichlich der

Zensur und der Überwachung repressiver Regierungen stärker nachkommen müssten". Googles chinesische Wende habe gezeigt, dass die Situation zu ernst sei, um das Gesetz durch einige "Hobbyisten" aufhalten zu lassen.

Das Gesetz würde es US-Unternehmen unter anderem verbieten, mit Regierungen zu kooperieren, die ihren Bürgern den freien Zugang zum Internet verweigern. Provider, die im Ausland oder in den USA behilflich sind, Internetangebote der US-Regierung oder von ihr geförderte Seiten zu blockieren, sollen mit Geldstrafen von bis zu zwei Millionen US-Dollar belangt werden können. Zudem soll es US-Firmen untersagt werden, ausländische Behörden mit personenbezogenen Informationen zu versorgen, die Rückschlüsse auf die Identität eines Internetnutzers ermöglichen. Nur im Rahmen rechtmäßiger Strafverfolgungsbegehren oder bei der drohenden Verletzung "nationaler Interessen der USA" sollen Ausnahmen gelten.

Im US-Außenministerium soll zudem ein Office of Global Internet Freedom eingerichtet werden, das als eine Art Sammelstelle für Klagen über Internetzensur fungiert. Das Weiße Haus wird gemäß dem Entwurf verpflichtet, sich für internationale Abkommen einzusetzen, die den freien Zugang zum Internet und eine ungehinderte Nutzung von Webseiten der US-Regierung garantieren. Ein ähnliches Vorhaben gibt es seit 2008 auch auf EU-Ebene.

Der 2007 erstmals in der Abgeordnetenkammer behandelte und auch von Demokraten unterstützte US-Entwurf ist bislang noch nicht weit gekommen im Gesetzgebungsverfahren. Nach mehreren Anhörungen und Konsultationen dazu sei es nun an der Zeit, es im Plenum des Repräsentantenhauses zu behandeln, meinte Smith Ende vergangener Woche. Er verwies zugleich auf die Unterstützung des Vorhabens durch zahlreiche zivilgesellschaftliche Organisationen wie Reporter ohne Grenzen. "Bitte lassen Sie amerikanische Internetfirmen nicht böse werden, indem Sie ihnen die Mittel zum Kampf gegen chinesische Restriktionen verweigern", appellierte eine Sprecherin der sich für die Pressefreiheit stark machenden Vereinigung unter Anspielung auf Googles Firmenmotto "Don't be evil" an die Politik. Im Hintergrund tobt derweil eine rhetorische Schlacht zwischen China und den USA rund um Zensur sowie Meinungs- und Wirtschaftsfreiheit. So bezeichnet der in Japan sitzende Forscher Philip Cunningham den Anspruch des Suchmaschinenprimus im regierungsnahen Blatt "China Daily" als "scheinheilig". Google sammle unzählige Daten über seine Nutzer und könne so ausgefeilte personenbezogene Profile erstellen, mokiert sich der Medienprofessor über den von seinen Gründern erschaffenen "Frankenstein". In weiteren Artikeln der Zeitung wird darauf verwiesen, dass der Internetkonzern im Reich der Mitte wirtschaftlich keinen Fuß gefasst habe und daher den theoretisch großen Markt mit dem Knall des Stopps der Zensur des eigenen Angebots gemäß den chinesischen Regierungsvorgaben mehr oder weniger freiwillig aufgeben wolle.

Im Gegenzug wirft das US-Diplomatenmagazin "Foreign Policy" Peking vor, mit dem aufgezogenen großen virtuellen Schutzwall rund um das chinesische Intranet einen "Protektionismus mit der Firewall" zu betreiben. Google sei genauso wie Yahoo und andere große internationale Internetfirmen durch die Auflagen der chinesischen Regierung "systematisch aus dem Markt getrieben worden". So würden Angebote wie Facebook, Flickr, Bloggerdienste oder YouTube in China immer wieder blockiert, während die einheimische Konkurrenz "mit ausländischer Technologie und ohne ausländische Wettbewerber" wachsen könne. Die von Google beklagten gezielten Trojanerangriffe auf Mail-Konten von Bürgerrechtlern seien eventuell noch der letzte "Druckknopf" Pekings gewesen, um auch den Branchenvorreiter in China auszuschalten. Im Sinne dieser Sichtweise gibt es in den USA seit geraumer Zeit Stimmen, die in der chinesischen Firewall eine Handelsbeschränkung und einen Verstoß gegen Abkommen der Welthandelsorganisation (WTO) sehen. Google und die chinesische Regierung sollen derweil Gespräche aufgenommen haben über das Vorhaben des Internetkonzerns, seine Suchergebnisse künftig nicht mehr zu filtern. 18.01.2010 www.heise.de

Links zu dem Artikel

<http://www.heise.de/newsticker/meldung/Google-pokert-mit-Rueckzugsdrohung-aus-China-903819.html>

<http://chrissmith.house.gov/News/DocumentSingle.aspx?DocumentID=166817>

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f%3Ah2271ih.txt.pdf

<http://www.heise.de/newsticker/meldung/EU-Abgeordnete-wollen-weltweit-gegen-Internet-Zensur-eintreten-192698.html>

http://www.chinadaily.com.cn/china/2010-01/18/content_9334543.htm

http://www.foreignpolicy.com/articles/2010/01/14/chinas_foreign_internet_purge

<http://www.reuters.com/article/idUSTRE5A520220091106>

Vorratsdaten: Raubkopierer statt Terroristen als Ziel

Die ursprünglich zur Terrorabwehr vorgesehene Datenspeicherung soll auch zur Ermittlung von Kleinstkriminellen dienen. Auch für Zivilprozesse sollen die Daten ausgewertet werden dürfen.

Wien. Das Gesetz, das die Speicherung aller Internet-, Festnetz- und Mobilfunkdaten regeln soll, ist noch gar nicht auf Schiene, da werden bereits weitere Begehrlichkeiten publik. Ursprünglich sollte die Speicherung sogenannter Vorratsdaten ausschließlich der Verfolgung von Terroristen und der Aufklärung schwerster Straftaten dienen. Wie „Die Presse“ erfuhr, fordert das Justizministerium (mit Rückendeckung aus dem Innenministerium) nun, die entsprechenden Daten auch für Zivilprozesse und die Verfolgung von Kleinstkriminalität auswerten zu dürfen. Zwei ranghohe Beamte aus den beiden Ressorts hatten die Wünsche am Donnerstag in einer vertraulichen Sitzung dem Datenschutzrat des Bundeskanzleramts vorgetragen. Christian Pilnacek, Leiter der Abteilung für Strafprozessordnung im Justizministerium, bestätigte der „Presse“ diese Information.

WLAN als Terrorwerkzeug

Der Plan birgt einiges an grundrechtlichem Sprengstoff. Weil die EU nach den Anschlägen vom 11. September 2001 mehr Handhabe zur Ausforschung von Terroristen und Schwerstkriminellen haben wollte, verpflichtete sie in einer Richtlinie alle Mitglieder dazu, künftig genau zu protokollieren (und über einen längeren Zeitraum zu speichern), wer wann mit wem von wo aus und wie lange kommuniziert hat. Und zwar im Internet (Word Wide Web, E-Mail etc.), Fest- und Mobilnetz. Anstatt zur Terrorabwehr wollen die österreichischen Behörden diese Daten nun auch zur Ermittlung von Internetschwindlern, Raubkopierern und Kleinstkriminellen einsetzen. Die Ministeriumsbeamten sollen in der Sitzung sogar den Wunsch geäußert haben, die Daten zur Ausforschung von Personen einzusetzen, die Dritte über Internetforenbeiträge beleidigt haben.

Damit wird die Gruppe der potenziell Verdächtigen allein aus technischen Gründen auf weite Teile der Bevölkerung ausgedehnt. Zehntausende Bürger in ganz Österreich sind derzeit nicht in der Lage, ihre privaten und meist mit WLAN-Funktion ausgestatteten Internetzugänge vor unbefugten Zugriffen zu sichern.

In praktisch jeder größeren Wohnanlage finden sich offene Zugänge, über die man von der Straße aus mit einem Laptop ins Internet gelangt. Während sich technisch Interessierte einen (vergleichsweise harmlosen) Spaß daraus machen, über fremde Internetzugänge große Datenmengen zu verschicken oder zu empfangen, dienen sie echten Kriminellen als wertvolles Werkzeug. Verfolgen Polizei und Staatsanwalt etwa

abgefangene E-Mails eines Terroristen zurück, der diese über einen offenen WLAN-Zugang eines Unschuldigen verschickt hat, führt die Spur zu einem Anschlussinhaber, dessen größter Fehler es war, das Kapitel „Sicherheit“ in der Bedienungsanleitung nicht gelesen (oder verstanden) zu haben. Für Laien ist eine solche Fremdnutzung des Zugangs praktisch nicht zu bemerken. Wird so jeder Bürger zum Verdächtigen? Pilnacek versucht zu beruhigen: „Im Strafrecht muss der Ankläger immer noch die Schuld eines anderen nachweisen, und nicht umgekehrt.“ Die Begutachtungsfrist zum entsprechenden Gesetz, das im Auftrag des Verkehrsministeriums vom Ludwig-Boltzmann-Institut für Menschenrechte ausgearbeitet wurde, ging am Freitag zu Ende. Der Entwurf sieht vor, dass die Daten nach sechs Monaten gelöscht werden müssen, nur nach richterlichem Beschluss herausgegeben werden dürfen und auch dann nur zur Verfolgung von Straftaten, die mit wenigstens drei Jahren Haft bedroht sind. Während sich Justiz- und Innenressort eine Herabsetzung der Strafgrenze auf ein Jahr, einzelne Beamte der beiden Ministerien gar vollen Zugriff und eine Beurteilung von Fall zu Fall wünschen, forderte der Datenschutzrat am Freitag alle Beteiligten auf, ihre Wünsche aufeinander abzustimmen. ORF-Redakteursrat und der Österreichische Journalistenclub befürchteten, dass das Gesetz die Basis zur Ausforschung unbequemer Informanten sei und damit die Pressefreiheit gefährde. Ähnliche Befürchtungen äußerten Rechtsanwälte und Seelsorger.
16.01.2010 Printausgabe der Tageszeitung „[Die Presse](#)“

Links zu dem Artikel

[http://diepresse.com/home/meinung/kommentare/533203/index.do?direct=533166
& vl_backlink=/home/panorama/oesterreich/533166/index.do&selChannel](http://diepresse.com/home/meinung/kommentare/533203/index.do?direct=533166&vl_backlink=/home/panorama/oesterreich/533166/index.do&selChannel)

EuGH: Gewinnspielrechtliches Kopplungsverbot in Deutschland europarechtswidrig

Der EuGH hat eine der wichtigsten gewinnspielrechtlichen Entscheidungen in den letzten Jahren getroffen: Das deutsche, nationale Kopplungsverbot im Gewinnspielrecht (§ 4 Nr. 6 UWG) verstößt gegen EU-Recht.

(Aus der Pressemitteilung des EuGH v. 14.01.2010:)

"Die europäische Richtlinie über unlautere Geschäftspraktiken¹ hat den Zweck, zu einem reibungslosen Funktionieren des Binnenmarkts und zum Erreichen eines hohen Verbraucherschutzniveaus beizutragen. Sie stellt ein generelles Verbot von unlauteren Geschäftspraktiken auf, die geeignet sind, das wirtschaftliche Verhalten des Verbrauchers zu beeinflussen. Sie stellt zudem Regeln über irreführende und aggressive Geschäftspraktiken auf. Anhang I enthält eine Liste jener Geschäftspraktiken, die unter allen Umständen unlauter sind.

Das deutsche Einzelhandelsunternehmen Plus ermunterte im Rahmen seiner Bonusaktion „Ihre Millionenchance“ dazu, bei Plus einzukaufen, um Punkte zu sammeln. Die Ansammlung von 20 Punkten ermöglichte es, kostenlos an bestimmten Ziehungen des Deutschen Lottoblocks (eines nationalen Verbands von 16 Lotteriegesellschaften) teilzunehmen. Die deutsche Zentrale zur Bekämpfung unlauteren Wettbewerbs e. V. sah diese Praxis als unlauter im Sinne des deutschen Gesetzes gegen den unlauteren Wettbewerb (UWG) an, nach dem Preisausschreiben und Gewinnspiele mit einer Kaufverpflichtung generell verboten sind.

Auf Antrag der Zentrale wurde Plus in erster und in zweiter Instanz verurteilt, diese Praxis zu unterlassen. Der Bundesgerichtshof, der in letzter Instanz über diesen Rechtsstreit zu entscheiden hat, möchte vom Gerichtshof wissen, ob die Richtlinie einem Verbot wie dem im UWG aufgestellten entgegensteht.

In seinem heutigen Urteil stellt der Gerichtshof fest, dass die Richtlinie einer nationalen Regelung wie der im UWG vorgesehenen entgegensteht, nach der Geschäftspraktiken, bei denen die Teilnahme von Verbrauchern an einem Preisausschreiben oder Gewinnspiel vom Erwerb einer Ware oder von der Inanspruchnahme einer Dienstleistung abhängig gemacht wird, ohne Berücksichtigung der besonderen Umstände des Einzelfalls grundsätzlich unzulässig sind.

Einleitend legt der Gerichtshof dar, dass Werbekampagnen, mit denen die kostenlose Teilnahme des Verbrauchers an einer Lotterie davon abhängig gemacht wird, dass in bestimmtem Umfang Waren oder Dienstleistungen erworben bzw. in Anspruch genommen werden, sich eindeutig in den Rahmen der Geschäftsstrategie eines Gewerbetreibenden einfügen und unmittelbar mit der Absatzförderung und dem Verkauf zusammenhängen. Sie stellen folglich Geschäftspraktiken im Sinne der Richtlinie dar und fallen damit in deren Geltungsbereich.

Sodann weist er darauf hin, dass die Regeln über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern mit der Richtlinie auf Gemeinschaftsebene vollständig harmonisiert werden. Daher dürfen die Mitgliedstaaten, wie dies in der Richtlinie ausdrücklich vorgesehen ist, keine strengeren als die in der Richtlinie festgelegten Maßnahmen erlassen, und zwar auch nicht, um ein höheres Verbraucherschutzniveau zu erreichen.

In Bezug auf die in der vorliegenden Rechtssache fragliche Praxis stellt der Gerichtshof fest, dass sie nicht von Anhang I der Richtlinie erfasst wird, der die Praktiken, die allein ohne eine Einzelfallprüfung verboten werden dürfen, abschließend aufzählt. Daher kann diese Praxis nicht verboten werden, ohne dass anhand des tatsächlichen Kontexts des Einzelfalls bestimmt wird, ob sie im Licht der in der Richtlinie aufgestellten Kriterien „unlauter“ ist. Zu diesen Kriterien gehört insbesondere die Frage, ob die Praxis in Bezug auf das jeweilige Produkt das wirtschaftliche Verhalten des Durchschnittsverbrauchers wesentlich beeinflusst oder dazu geeignet ist, es wesentlich zu beeinflussen.“

15.01.2010 www.dr-bahr.com

EuGH, Urteil vom 14.01.2010
C-304/08

Links zu dem Artikel

http://www.gesetze-im-internet.de/uwg_2004/_4.html

Europol in der dritten Generation

Ab 1. Januar wird die Polizeibehörde zur EU-Agentur. Ihre Kompetenzen erweitern sich erneut erheblich

Mit Beginn des Jahres 2010 wird die "Polizeibehörde" Europol zur "Polizeiagentur" und, wie das "Europäische Amt für Betrugsbekämpfung" (OLAF) oder die "Europäische Polizeiakademie" (CEPOL), fortan durch den Gesamthaushalt der Europäischen Union finanziert. Das Europol-Übereinkommen wurde im April durch einen Ratsbeschluss ersetzt. Europol will laut Selbstauskunft ein "weltweit herausragendes Zentrum der Weltklasse" sein und mitmischen bei der Bekämpfung "sämtlicher Formen von schwerer internationaler Kriminalität und Terrorismus". 2011 bezieht Europol ein neues Hauptquartier im Stadtteil Statenviertel in Den Haag.

Die Schaffung von Europol wurde 1992 im Vertrag von Maastricht als "Europäisches Polizeiamt" mit Sitz in Den Haag festgeschrieben. Vorausgegangen war ein Vorschlag Deutschlands im Europäischen Rat aus dem Jahr 1991, eine "Europäische

Kriminalpolizeiliche Zentralstelle" zu errichten, um grenzüberschreitende Kooperationen zu vereinfachen. Als Priorität galten damals die Koordination und der Informationsaustausch unter europäischen Polizeien. Bis zur Ausgestaltung und Annahme eines Europol-Übereinkommens 1999 widmete sich Europol ab 1994 in der European Drug Unit (EDU) der Rauschgiftkriminalität und Geldwäsche.

Bis zum Lissabon-Vertrag galt Europol als zwischenstaatliche Einrichtung der sogenannten "Dritten Säule" zur polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS), in der die EU keine eigenen Beschlüsse fassen konnte. Das EU-Parlament musste lediglich über Veränderungen unterrichtet werden, eine Kontrolle verblieb höchstens indirekt in den Parlamenten der Mitgliedsstaaten.

In ihrer Geschichtsschreibung sieht Europol 1999 als das Jahr, in dem die Behörde in ihrer heutigen Form entstand. Standen zuvor strategische Aktivitäten im Vordergrund, erhielt die Behörde mit "Aufklärung" und Entsendung von "Spezialisten" zunehmend operative Kompetenzen. Das Aufgabengebiet wandelte sich von der Bekämpfung und Prävention des Drogenhandels hin zu neuen Formen grenzüberschreitender Straftaten, darunter die Fälschung der neuen Euro-Währung und Kreditkarten, Geldwäsche, Wirtschaftskriminalität und Korruption, Umweltkriminalität, Schutzgelderpressung, KFZ-Kriminalität oder Produktpiraterie, aber auch Kriminalitätsforschung und grenzüberschreitende Aus- und Fortbildung. Nach dem "Tampere Programm", dem Mehrjahresprogramm der EU aus dem Jahre 1999, kam die Einbindung in die "European Police Chiefs Task Force" (EPCT) zur Erleichterung grenzüberschreitender Polizei-Missionen hinzu. 2001 wurden die Abteilungen "Ermittlungsunterstützung", "Analyse und Aufklärung" und "Organisiertes Verbrechen" zur "Abteilung für ernsthafte Straftaten" zusammengefasst; im Jubiläumsheft zum zehnjährigen Bestehen verstanden als "Informationsaustausch, Analyse und Sachverstand unter einem Dach". Nach 9/11 geriet der "Kampf gegen Terrorismus" und seiner Finanzierung zum neuen zentralen Arbeitsbereich der Behörde, kurz darauf ergänzt durch eine "Counter Terrorism Task Force". 2002 wurde der Aufgabenbereich auf den "Kampf gegen illegale Migration" und "Menschenhandel" ausgeweitet. Seit 2002 beteiligt sich Europol an länderübergreifenden "gemeinsamen Ermittlungsgruppen" (JIT). Die Anbindung an die Verfolgungsbehörden der EU-Mitgliedsstaaten erfolgt durch die nationalen "Europol National Units" (ENU) und ein undurchsichtiges Netzwerk von "Europol-Liaison Officers" (ELO).

Mit dem Haager Programm von 2004 rückte Europol ins "Zentrum der EU-weiten Kooperation zur Strafverfolgung". Kurz zuvor hatte Europol ein Kooperationsabkommen mit der "Europäischen Einheit für justizielle Zusammenarbeit" (Eurojust) unterzeichnet. Die 2002 eingerichtete europäische Justizbehörde, ebenfalls mit Sitz in Den Haag, ist das justizielle Pendant Europols und koordiniert grenzüberschreitende Strafverfahren, fördert den Informationsaustausch zwischen nationalen Justiz- und Polizeibehörden und widmet sich ebenfalls der Terrorismusbekämpfung, dem illegalen Handel mit Waffen und Drogen, der Kinderpornografie und der Geldwäsche. Mit Beschluss des Europäischen Rates vom 16. Dezember 2008 erweitert sich auch der Kompetenzbereich von Eurojust ab 2010 beträchtlich:

- Auf der Grundlage einer Bewertung der von Eurojust gesammelten Erfahrung ist es geboten, Eurojusts operative Effizienz unter Berücksichtigung dieser Erfahrung weiter zu verbessern. Es ist an der Zeit dafür Sorge zu tragen, dass Eurojust operativer wird und dass der Status der nationalen Mitglieder angenähert wird. (Europäischer Rat)

Gemäß dem Lissabon-Vertrag ist Eurojust befugt, grenzüberschreitende Ermittlungen und Strafverfolgungen einzuleiten. In den Mitgliedstaaten sollten nationale Eurojust-Koordinierungssysteme zur Fallbearbeitung eingerichtet werden, um die bereits existierenden nationalen Eurojust-Anlaufstellen miteinander zu verzahnen (Anlaufstellen für Terrorismusfragen, das Europäische Justizielle Netz, gemeinsame Ermittlungsteams, Kontaktstellen gegen Kriegsverbrechen, Vermögensabschöpfung

und Korruption). Eurojust kann personenbezogene Daten verarbeiten, darunter neben rechtskräftig Verurteilten auch Daten von Verdächtigen oder Kontaktpersonen inklusive Telefonnummern, E-Mailadressen, Fahrzeugregisterdaten, DNA-Profile, Lichtbilder, Fingerabdrücke, Verbindungs- und Standortdaten "sowie alle damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder Benutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes erforderlich sind".

"The keyword here is information"

Zur grenzüberschreitenden Kooperation schließt Europol Abkommen mit "Drittstaaten" außerhalb der EU und supranationalen Organisationen, darunter Estland, Lettland, Marokko, Rußland, Türkei, Kanada und Interpol. Europol unterstützt etwa Kolumbien in der Kontrolle der FARC und anderer Guerillas. Seit 2001 kooperiert die Behörde mit den USA, zunächst in einer "strategischen und technischen Kooperation", seit 2002 auch auf "operativer Ebene" und einem Austausch personenbezogener Daten. Ähnliche Abkommen werden regelmäßig erneuert und erweitert.

Auch in der Errichtungsanordnung zur Einrichtung der EU-Grenzpolizei Frontex wird die Zusammenarbeit mit Europol festgeschrieben. Das Papier regelt den Austausch "operativer, strategischer oder technischer Informationen" einschließlich personenbezogener Daten und Verschlussachen, im März 2008 wurde ein weiteres "strategisches Kooperationsabkommen" geschlossen. Frontex hilft Europol bei der Erstellung von Risikoanalysen zur "Bedrohungslage im Bereich der organisierten Kriminalität". Im Juni 2008 hatte der Rat Frontex angewiesen, im Rahmen des Europäischen Grenzschutzsystems enger mit Europol zusammenzuarbeiten und etwa zu prüfen, welcher "Zusatznutzen" mit der Integration Europols in das web-gestützte "Netz zur Koordinierung und zum Austausch von Informationen über illegale Einwanderung" (ICONet) verbunden sein könnte.

Automatisierte Informationssammlungen

Zentraler Bestandteil von Europol sind die umfangreichen Datenbanken, deren Einrichtung im Europol-Übereinkommen festgelegt ist. Dieses "automatisierte System" besteht aus drei Säulen:

1. "Informationssystem": Angaben zu Personen, Straftaten und Verweisen auf ak werden Verdächtige oder Verurteilte, gefüttert wird die Datei per "Data Upload".
2. "Analysedateien": Fallbezogene Dateien mit Daten von Zeugen, Opfern, Kontaktpersonen, darunter etwa "DOLPHIN" "(Non-Islamist extremist terror "Antiterrorliste" der EU.
3. "Indexsystem" zur Verschlagwortung aller Einträge.

Seit 2005 haben alle Mitgliedsstaaten Zugriff auf das Informationssystem, wobei der automatisierte Upload erst von wenigen Ländern umgesetzt wird. Etliche EU-weite Abkommen erweitern die Möglichkeiten der Behörde, hinzu kommen "ergänzende" Datensammlungen mit "zahlreichen weiteren Informationsprodukten und -dienstleistungen", darunter etwa ATLAS ("Verbesserung der Zusammenarbeit zwischen Anti-Terror-Teams) oder OASIS ("Übergreifendes Analysesystem zur Aufklärung und Unterstützung"). Mit der 2007 installierten Plattform "Check the Web" sollen Internetseiten auf Zusammenhänge mit Terroranschlägen durchsucht werden. Der Zugriff auf "Check the Web" ist angeblich auf fünf "Experten" pro Mitgliedsstaat beschränkt. Erst kürzlich hatte Europol eine "Europe Bomb Database" ausgeschrieben.

Zwar gibt es grundsätzlich ein individuelles Auskunftsrecht über gespeicherte Daten, das allerdings durch "Rechte und Freiheiten Dritter" eingeschränkt wird. "Unmittelbar betroffene Mitgliedstaaten" können Einspruch gegen eine Auskunft einlegen, Betroffenen wird dann kein Hinweis über einen Eintrag mitgeteilt. 2008 hat es

lediglich 135 Auskunftsersuchen gegeben. Nationale Kontrollinstanzen dürfen immerhin Datenübermittlungen und -abrufe ihrer Behörden prüfen. Europol selbst bezeichnet sich als "Information Broker" und sieht sich dem Grundsatz eines "proaktiven Handelns" verpflichtet. Seit 2006 gibt die Behörde die jährlichen "Trend-Reports" zu organisierter Kriminalität Organised Crime Threat Assessment (OCTA) heraus, ein Jahr später folgte das Pendant Terrorism Situation and Trend Report (TE-SAT). TE-SAT wird zwar seit 9/11 unter Mithilfe von Europol publiziert, ging allerdings erst nach einem Ratsbeschluss 2006 in die Herausgeberschaft der Behörde über. Beobachtet werden "Islamisten", "Separatisten", "Linksgerichtete", "Rechtsgerichtete" und "Einzelfälle", zu denen auch Aktionen von Tierrechtsgruppen gerechnet werden.

Auch die halbjährlich erneuerte "Antiterrorliste" der EU wird unter Mithilfe von Europol erstellt. Laut britischem Telegraph rückt mit der Finanzkrise ein "Mittelmeer-Dreieck" linker Gruppen aus Griechenland, Italien, Spanien und Portugal ins Fadenkreuz von Europol.

Deutschland will noch mehr Datenausch

Das Personal der Behörde hat sich in zehn Jahren auf 634 vervierfacht. Mit dem Deutschen Jürgen Storbeck als erstem amtierenden Direktor 1999 und seinem Nachfolger Max-Peter Ratzel, vorher BKA-Abteilungspräsident, konnte Deutschland bis zum Antritt des britischen Rob Wainwright 2009 sein Gewicht in der Organisation ausbauen. Ratzel hatte im Oktober 2007 die neue Strategy for Europol vorgestellt, das "letzte Puzzle-Teil" der neuen Zukunft Europols. Durch die Ausweitung analytischer Kapazitäten sollte die Behörde zum Pionier des "Wandels, Identifizierung und Antwort auf neue Bedrohungen und der Entwicklung neuer Technik" werden: "As a consequence, the volume of data to be analysed will increase and the scope of information exchange will widen." Zum zehnjährigen Bestehen bekräftigte der Parlamentarische Staatssekretär beim Bundesinnenminister, Peter Altmaier, die bisherige Arbeit und die Bedeutung von Europol:

- Unter maßgeblicher politischer, personeller und finanzieller Mithilfe der Bundesrepublik Deutschland hat sich Europol in den vergangenen zehn Jahren zu einem wichtigen Baustein in der europäischen Sicherheitsarchitektur entwickelt. (Peter Altmaier)

Unter deutscher EU-Ratspräsidentschaft 2007 waren bereits drei Änderungsprotokolle des Europol-Durchführungsabkommens unter anderem zum vereinfachten Datenausch verabschiedet und von Innenminister Schäuble feierlich überreicht worden. Schäuble hatte sich auch für die Einrichtung der "Check the Web"-Plattform bei Europol stark gemacht. Beim Treffen der Innenminister der so genannten G6-Staaten im Seebad Heiligendamm 2006 warb Schäuble dafür, Europol stärker als Eckpfeiler im Kampf gegen "illegale Einwanderung" zu nutzen. Deutschland gilt als größter Beitragszahler für Europol und hatte bis zur bevorstehenden Umwandlung in eine Agentur nach eigenen Angaben 20 % des sich auf ca. 65 Mio. Euro belaufenden Haushaltes finanziert. Dafür haben deutsche Verfolgungsbehörden enormen Gebrauch von der Behörde gemacht: Nachdem neben dem Bundeskriminalamt auch die Landeskriminalämter an das Europol-Informationssystem angeschlossen waren, "nutzt Deutschland das System in der Fläche" und verbucht die "meisten Zulieferungen und Abfragen". Nicht durchsetzen konnte sich das deutsche Bundesinnenministerium mit dem vom Bundesrat gebilligten Vorschlag, die Errichtung einer "Datei über international agierende Gewalttäter" im Europol-Informationssystem anzusiedeln. Mit der Änderung des deutschen Europol-Gesetzes (EuropolGuaÄndG), das vom Bundesrat angenommen und von der Regierung verabschiedet wurde, erhalten die Bundespolizei und der Zollfahndungsdienst Zugriff auf das Europol-Informationssystem.

Ambitionierte Pläne für Europol im "Stockholmer Programm"

"Europäische Stellen wie Europol, Eurojust, die Agentur für Grundrechte und Frontex

haben in ihrem jeweiligen Tätigkeitsbereich volle Funktionsfähigkeit erreicht", freut sich der Europäische Rat im jüngst verabschiedeten "Stockholmer Programm", dem neuen Mehrjahresprogramm für die Ausgestaltung der inneren Sicherheit in der EU. Dennoch definiert das "Stockholmer Programm" weitere ambitionierte Ziele zur Einbindung Europols in die nächsten fünf Jahre der EU-Innenpolitik, darunter auch in Missionen der "Gemeinsamen Europäischen Sicherheits- und Verteidigungspolitik" (ESVP), gleichfalls ein Herzenswunsch des Hohen Vertreters für die Gemeinsame Außen- und Sicherheitspolitik, Javier Solana.

Neben der fortschreitenden Koordinierung mit der Grenzschutzagentur Frontex, der Lissabonner Drogenbeobachtungsstelle, dem künftigen Europäischen Unterstützungsbüro für Asylfragen und der Agentur für Grundrechte soll Europol als europäisches Ressourcenzentrum für Cyberkriminalität fungieren. Zur Analyse der "Terrorgefahr auf europäischer Ebene" soll Europol mit dem Geheimdienstzentrum SitCen in Brüssel eine neue "Methodik" entwickeln. Der Europäische Rat empfiehlt, "Kontakte zwischen ranghohen Beamten der Mitgliedstaaten" zu fördern, darunter "die obersten Polizeichefs oder Staatsanwälte, die Leiter von Aus- und Fortbildungsinstituten, die Leiter der Gefängnisverwaltungen oder die Generaldirektoren der Zollbehörden". Europol soll für diese vage als "Netze" bezeichneten Strukturen ein "Angelpunkt des Informationsaustauschs" werden. Zur Stärkung der "externen Dimension" europäischer Innenpolitik, der im "Stockholmer Programm" ein eigenes Kapitel gewidmet ist, soll sich die Prioritätensetzung von Europol und Eurojust "an den außenpolitischen Prioritäten" der EU orientieren. Neben "engeren Beziehungen zu den Nachbarregionen und -ländern der Union" fordert der Rat die zunehmende Einbindung Europols in EU-Polizeimissionen und, falls gesetzliche oder administrative Schranken etwa zu Einsätzen von verdeckten Ermittlern bestehen, "geeignete Vorschläge zur Beseitigung solcher Hindernisse vorzulegen". Als Pilotprojekte gelten gemeinsame operative Einsätze und grenzüberschreitende Risikobewertungen wie die Einrichtung von Gemeinsamen Polizei- und Zollzentren oder Kooperationen im Rahmen von Gipfelprotesten und Sportereignissen. Europol und Eurojust sollen zudem in den im Lissabon-Vertrag definierten "Ständigen Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit "

[<http://register.consilium.europa.eu/pdf/de/09/st16/st16075-re01.de09.pdf>] als Beobachter teilnehmen.

Neue "Work Packages"

Nach wie vor ist unklar, wie der im Lissabon-Vertrag niedergelegte Grundsatz der "Offenheit" durch Europol umgesetzt werden soll, wie also die Behörde durch das Parlament kontrolliert wird oder ob das Parlament bei internationalen Abkommen mitentscheiden darf. "Soll diese Zustimmung als Voraussetzung für die Abkommen gesehen werden?", fragt der Vorsitzende des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE), Juan Fernando López Aguilar. Mit dem Lissabon-Vertrag wird die Arbeit von Europol – zumindest in Theorie - der Kontrolle des Parlaments unterworfen. Während die Verabschiedung des SWIFT-Abkommens einen Tag vor Inkrafttreten des Lissabon-Vertrags gegen ein ablehnendes Votums des Parlaments in der Öffentlichkeit für Furore sorgte, hatten die europäischen Innenminister weitgehend unbeachtet auch neue "Work Packages" für Europol beschlossen. Auch hier hatte das Parlament zuvor die neuen Pläne kritisiert und sich gegen ihre Verabschiedung gestellt:

- Das Europäische Parlament [...] lehnt den Text des Rates ab; vertritt die Auffassung, dass [...] so lange keine Änderungen der Maßnahmen zur Umsetzung des Europol-Beschlusses ergriffen werden sollten, bis diese Maßnahmen in dem durch den Vertrag von Lissabon geschaffenen neuen Rechtsrahmen angenommen werden können; fordert den Rat auf, seinen Vorschlag zurückzuziehen. (EU-Parlament)

Die vom Parlament beanstandeten und dennoch durchgewunkenen

Durchführungsbestimmungen betreffen die "Beziehungen von Europol zu anderen Stellen einschließlich des Austauschs von personenbezogenen Daten und Verschlusssachen", "Vertraulichkeitsregeln für Europol-Informationen" und Regelungen zu den "von Europol geführten Arbeitsdateien zu Analysezwecken". Europol darf neben Daten zu Verurteilten und Verdächtigen auch Informationen zu "Kontakt- und Begleitpersonen" sedimentieren, darunter "Vermutete Beteiligung", "bei Ermittlungen zusammengetragenes Material wie Videos und Fotos", "Lebensweise (etwa über seine Verhältnisse leben) und Gewohnheiten", "Einsatz von Doppelagenten", "Drogenmissbrauch", "Kommunikationsmittel wie Telefon (Festverbindung/Mobiltelefon), Fax, Funkrufdienst, elektronische Post, Postadressen, Internetanschluss/-anschlüsse", "Stimmprofil, Blutgruppe" oder "Gebiss":

- Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben einer Person dürfen nur übermittelt werden, wenn dies unbedingt notwendig ist.

Ob ein Datenausch über sexuelle Orientierung oder politische Überzeugung "unbedingt notwendig" ist, kann etwa der Direktor von Europol entscheiden. Deutlich wird, dass Europol seit seiner Gründung keinesfalls nach dem Grundsatz der Datensparsamkeit oder Datenvermeidung operiert, sondern im Gegenteil alle personenbezogenen Informationen aus seinem nun erweiterten Zuständigkeitsbereich speichern und analysieren darf. "Unbedingt notwendig" ist demgegenüber eine ernsthafte europäische Bürgerrechtsbewegung, die der Datensammelwut und Verschränkung der Behörden unter dem Vorwand einer "Bekämpfung des Terrorismus" etwas entgegensetzt. Eine solche Bewegung ist allenfalls in wenigen Teilbereichen sichtbar und agiert meist ohne grenzüberschreitende Bezugnahme. Eine Auseinandersetzung mit der innenpolitischen Staatswerdung der EU und den damit einhergehenden nebulösen Kompetenzen von Europol, Eurojust oder Frontex wird damit den Parteien überlassen.

Immerhin fordert das Europäische Parlament eine Überarbeitung der Verordnung zur Informationsfreiheit, um Europol und Eurojust besser kontrollieren zu können und Einsicht in internationale Abkommen zu bekommen. Das Parlament kündigte letzte Woche an, dass es "keine legislativen Versuche der Kommission oder des Rates, den öffentlichen Zugang zu Dokumenten zu begrenzen oder das Informationsrecht der Bürger einzuschränken, hinnehmen" will.

29.12.2009 www.telepolis.de

Links zu dem Artikel

<http://www.europol.europa.eu/>

<http://www.cepol.europa.eu/>

http://ec.europa.eu/anti_fraud/index_de.html

[http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:EN:PDF)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:EN:PDF)

http://www.europol.europa.eu/index.asp?page=facts_de&language=de

http://de.wikipedia.org/wiki/Polizeiliche_und_justizielle_Zusammenarbeit_in_Strafsachen

<http://euro-police.noblogs.org/gallery/3874/st10505-re04.en09.pdf>

<http://www.euractiv.com/de/sicherheit/haager-programm-programm-2005-10-justiz-inneres/article-132148>

<http://www.eurojust.europa.eu/>

http://eurojust.europa.eu/official_documents/Eurojust_Decision/2009/NewEJDecision2009-DE.pdf

http://europa.eu/lisbon_treaty/index_de.htm

<http://colombiareports.com/colombia-news/news/5127-europol-and-colombia-to-fight-farc-together.html>

<http://register.consilium.europa.eu/pdf/en/09/st15/st15184.en09.pdf>
<http://www.frontex.europa.eu/>
<http://euro-police.noblogs.org/gallery/3874/st12954.de09.pdf>
<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/57&format=HTML&aged=1&language=DE&guiLanguage=en>
<http://www.statewatch.org/news/2009/nov/europol-awfs-third-parties.pdf>
<http://euobserver.com/9/24162>
http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_%28OCTA%29/OCTA2009.pdf
http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2009.pdf
http://www.telegraph.co.uk/finance/comment/ambroseevans_pritchard/6851932/Euro-Diktats-risk-terrorist-response-across-Southern-Europe.html
http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2009/10/europol_10.html
http://www.berlin.de/imperia/md/content/seninn/imk2007/beschluesse/imk_185_berecht_top03.pdf?start&ts=1260969051
<http://www.n-tv.de/politik/EU-vereinbart-Zusammenarbeit-article176143.html>
http://www.bundesrat.de/cln_050/SharedDocs/Drucksachen/2007/0501-600/589-1-07.templateId=raw,property=publicationFile.pdf/589-1-07.pdf
<http://www.gesetze-im-internet.de/bundesrecht/europolg/gesamt.pdf>
<http://register.consilium.europa.eu/pdf/de/09/st17/st17024.de09.pdf>
http://diepresse.com/home/politik/eu/519864/index.do?vl_backlink=/home/index.do
<http://www.heise.de/newsticker/meldung/SWIFT-Abkommen-zum-Transfer-von-Bankdaten-an-US-Behoerden-beschlossen-872553.html>
<http://register.consilium.europa.eu/pdf/de/09/st15/st15138.de09.pdf>
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2009-0068+0+DOC+XML+V0//DE>
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+P7-RC-2009-0191+0+DOC+XML+V0//DE>

Gezielte Angriffe auf Unternehmen gehen weiter

Die Lücke im Internet Explorer, die bei den Angriffen auf Google benutzt wurde, ist zwar derzeit in aller Munde, doch Ungemach droht auch weiterhin aus anderer Richtung: präparierte PDF-Dokumente. Adobe hat zwar letzte Woche ein Update für seinen kostenlosen Reader veröffentlicht, doch offenbar setzen Kriminelle und Spione weiterhin darauf, dass noch nicht alle Anwender und Firmen die Updates installiert haben.

F-Secure berichtet von einem Angriff auf ein US-Unternehmen, das beim US-Verteidigungsministerium unter Vertrag steht. Vermutlich taiwanische Angreifer hatten vergangene Woche ein täuschend echtes Dokument dorthin verschickt, das eine seit mehreren Wochen bekannte Lücke (doc.media.newPlayer) im Reader ausnutzte, um auf einem Windows-PC eine Backdoor zu installieren. Das Update von Adobe schließt genau diese Lücke.

Für die Lücke im Internet Explorer gibt es indes immer noch kein Update. Nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI) haben nun auch die französischen (CERTA) und australischen CERTs vor dem Einsatz von Microsofts Browser gewarnt und auf alternative Produkte verwiesen. Mittlerweile kursiert der Exploit zum Ausnutzen der Lücke öffentlich. Die Lücke beruht auf einem Fehler bei der Verarbeitung bestimmter JavaScript-Event-Objekte in der "Microsoft HTML Viewer"-Bibliothek mshtml.dll.

Erste deutsche Firmen haben bereits reagiert und untersagen ihren Mitarbeitern das Surfen mit dem Internet Explorer. Zwar hat Microsoft Workarounds veröffentlicht, wie das Anschalten der Datenausführungsverhinderung (DEP) und das Abschalten von Active Scripting, vermutlich dürfte die breite Masse der Anwender jedoch mit dem Nachvollziehen der Schritte Probleme haben – wenn sie denn überhaupt das eigentliche Problem wahrgenommen haben. Bislang gibt es jedoch keine Berichte, dass allgemein verfügbare Webseiten die Lücke ausnutzen.

Unterdessen untersucht Google, ob möglicherweise Mitarbeiter in der chinesischen Niederlassung bei den Angriffen eine Rolle gespielt haben. Dazu sollen nun die Netzwerke der chinesischen Niederlassung noch einmal analysiert werden, um eventuell Spuren des benutzten Backdoor-Trojaners zu finden. McAfee, die die ersten Analysen der Aurora-Attacken veröffentlicht hatten, nennen das Schädlingkonglomerat "Exploit-Comele" und "Roarur.dr" und stellen dafür Signaturen bereit. Andere Antivirenhersteller haben ebenfalls bereits Signaturen zum Erkennen des Exploits (unter anderen Namen) bereitgestellt.

19.01.2010 www.heise.de

Links zu dem Artikel

<http://www.f-secure.com/weblog/archives/00001859.html>

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-001/CERTA-2010-ALE-001.html>

http://news.yahoo.com/s/nm/20100118/wr_nm/us_google_china_attack

<http://www.avertlabs.com/research/blog/index.php/2010/01/14/more-details-on-operation-aurora/>

Neuerungen: Bei Angaben zu Mehrwertdienstenummern (Deutschland)

Zum 01.03.2010 tritt auf Grund des ersten Gesetzes zur Änderung des Telekommunikationsgesetzes und des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln das neue Telekommunikationsgesetz (TKG) in Kraft und beschert den Anbietern von Servicenummern einige Neuerungen. Nachdem bereits zum 01.09.2007 diesbezüglich das TKG geändert wurde, werden sich zum 01.03.2010 wiederum einige Neuerungen hinsichtlich der Informationspflichten beim Umgang mit Servicenummern ergeben. Die wichtigsten Neuerungen erläutert der folgende Artikel.

1. Neudefinition „Service-Dienste“

Der Begriff "Service-Dienste" ist neu in § 3 Nr. 8a TKG definiert. Danach sind Service-Dienste "Dienste, insbesondere des Rufnummernbereichs (0)180, die bundesweit zu einem einheitlichen Entgelt zu erreichen sind;"

2. Angabe von Mobilfunkpreisen

§ 66a TKG wird dahingehend geändert, dass die Informationspflichten zur Höhe des Verbindungsentgeltes nunmehr auch die Mobilfunkpreise umfassen.

3. Angabe von Mobilfunkhöchstpreisen

In § 66d TKG ist ab dem 01.03.2010 bestimmt, dass Höchstpreise pro Minute oder pro Anruf für Verbindungen aus dem Mobilfunknetz zu nennen sind.

Die IT-Recht Kanzlei empfiehlt in diesem Zusammenhang in Zukunft folgende Formulierungen:

- Bei Minutenabrechnung: "X € (inkl. Mwst.) / Min. aus dem deutschen Festnetz; aus den Mobilfunknetzen höchstens X € pro Minute.
- Bei Verbindungsabrechnung: X € (inkl. Mwst.) / Verbindung aus dem deutschen Festnetz; aus den Mobilfunknetzen höchstens X € pro Anruf.

4. Weiterhin Abmahn- und Bußgeldgefahr

Die Nichtangabe der Mehrkosten für Anrufe aus den Mobilfunknetzen ist bereits jetzt ein Grund für eine Abmahnung. So hatte etwa bereits das Landgericht Hildesheim im Rahmen einer einstweiligen Verfügung einem Online-Shopanbieter untersagt, 0900er-Serviceummern im geschäftlichen Verkehr anzubieten, ohne auf die durch eine Nutzung eben dieser Rufnummer entstehenden Kosten im Einzelnen hinzuweisen (Beschluss vom 26.09.2006, Az. 11 O 17/06).

Zudem stellt die Nichtangabe auch eine Ordnungswidrigkeit nach § 149 TKG dar. Bei einem Verstoß kann die Geldbuße nach § 149 Abs. 2 bis zu 100.000 Euro betragen. 22.12.2009 www.it-recht-kanzlei.de

Links zu dem Artikel

http://www.gesetze-im-internet.de/tkg_2004/_3.html

http://www.gesetze-im-internet.de/tkg_2004/_66d.html

http://www.gesetze-im-internet.de/tkg_2004/_149.html

Kriminalpolizei: Köperscanner garantieren keine Sicherheit

Der Vorsitzende des Bundes Deutscher Kriminalbeamter (BDK), Klaus Jansen, relativiert den Nutzen von Körperscannern an Flughäfen. "Wir müssen sehen, dass wir hier nicht einer technischen Lösung aufsitzen, die eine trügerische Ruhe verbreitet", sagte Jansen am Samstag im Deutschlandfunk.

Die Scanner könnten einen gewissen Bereich abdecken, "aber wenn Selbstmordattentäter entschlossen sind, tatsächlich sich selber zu vernichten und andere mitzunehmen, dann wird der Sprengstoffgürtel möglicherweise nicht außerhalb des Körpers, sondern im Körper getragen", gab Jansen zu bedenken. Zudem sei fraglich, ob beim versuchten Flugzeugattentat von Detroit der in die Unterhose des Täters eingenähte Sprengsatz von einem Scanner erkannt worden wäre. Es sei der falsche Ansatz, sich nur auf die Technik zu verlassen, sagte Jansen. Maschinen und Computer könnten keinen Verdacht schöpfen. Den US-Behörden hätten alle notwendigen Informationen vorgelegen, um den Mann nicht auf die Passagierliste setzen zu lassen.

Die Sicherheitspanne müsse kritisch hinterfragt werden, dabei müssten die USA "professionell und ehrlich" aufzeigen, wie es zur Fehleinschätzung gekommen sei. Eine ähnliche Panne könne auch für Deutschland nicht ausgeschlossen werden, sagte Jansen. Hier müsse überprüft werden, ob die Anti-Terror-Datei handhabbar sei und das Terrorabwehrzentrum funktioniere: "Wir sollten erstmal sehen, ob das Vorhandene professionell belastbar ist."

02.01.2010 www.zeitong.de

Links zu dem Artikel

<http://www.kleinezeitung.at/nachrichten/politik/2259361/eu-staaten-zerstritten-ueber-koerperscanner.story>

Das neue Rechnungslegungsänderungsgesetz - was sich ab 2010 ändert!

Am 10.12.2009 hat der Nationalrat das neue Rechnungslegungsänderungsgesetz (RÄG) beschlossen. Mit einer Beschlussfassung im Bundesrat ist am 18.12.2009 zu rechnen, sodass das Gesetz noch rechtzeitig mit Beginn 2010 in Kraft treten kann. Mit dem RÄG wurde insbesondere die Bilanzierungspflicht von Unternehmen neu geregelt und die Einnahmen-Ausgaben-Rechnung auch bei höheren Umsätzen als zulässig erklärt. Auf den ersten Blick erscheint diese Neuregelung als Erleichterung für KMUs, doch steckt der Teufel wie so oft im Detail.

Nach bisheriger Rechtslage trat die Bilanzierungspflicht bei gewerblicher Einkünfteerzielung erst dann ein, wenn ein Umsatz von € 400.000 in zwei aufeinander folgenden Geschäftsjahren oder in einem Geschäftsjahr ein Umsatz von € 600.000 überschritten wurde. Diese Beträge werden ab 1.1.2010 auf € 700.000 bzw. € 1.000.000 angehoben. Für Unternehmer, die nach der bisherigen Regelung verpflichtet waren zu bilanzieren, ist ein etwaiger Wegfall dieser Verpflichtung zu prüfen.

Beispiel:

Ein Unternehmer erzielt im Geschäftsjahr 2009 Umsatzerlöse i.H.v. € 500.000, im vorangegangenen Geschäftsjahr betragen die Umsatzerlöse € 650.000. Da die Umsatzerlöse in den dem Geschäftsjahr 2010 vorangegangenen zwei Geschäftsjahren jeweils unter der neuen maßgeblichen Schwelle (€ 700.000) lagen, entfällt für das Geschäftsjahr 2010 die Rechnungslegungspflicht.

Doch was gilt für Unternehmer, die bisher ihren Gewinn mittels Pauschalierung ermittelt haben? Die geänderten Schwellenwerte haben direkten Einfluss auf die unterschiedlichen steuerlichen Pauschalierungsvorschriften.

Gute Nachrichten gibt es für Künstler, Drogisten, Lebensmittelhändler und Einnahmen-Ausgaben-Rechner, die ihren Gewinn mittels Pauschalierung ermittelt haben. In diesen Fällen wird die neue Grenze der Pauschalierung auf € 700.000 angehoben. Für andere Berufsgruppen wie zum Beispiel Gaststätten- und Beherbergungsbetriebe ändert sich durch die genannte Gesetzesänderung nichts. Deren Schwellenwert für die Anwendbarkeit der Pauschalierung bleibt mit € 255.000 gleich.

Neben den neuen Grenzwerten für die Bilanzierungspflicht wurden durch das Rechnungslegungsänderungsgesetz bestehende Bewertungswahlrechte gestrichen bzw. angepasst (z.B. Aufwendungen für Ingangsetzen und Erweitern eines Betriebes, Aktivierung eines Firmenwerts). Diese Wahlrechte wichen teilweise von den steuerlichen Bestimmungen ab und bedeuteten daher nicht nur einen Mehraufwand bei der Bilanzerstellung nach Unternehmensrecht und Steuerrecht, sondern erschwerten auch die Vergleichbarkeit der unternehmensrechtlichen Jahresabschlüsse.

LBG-Tipp:

Durch das Rechnungslegungsänderungsgesetz ist der Unternehmer zwar von der Aufstellung einer Bilanz bis zu den neuen Schwellenwerten befreit, doch sollte gerade in wirtschaftlich schlechten Zeiten überlegt werden, ob der geringe Mehraufwand für die freiwillige Bilanzierung nicht durch den zusätzlichen Informationsgehalt einer zeitnahen doppelten Buchführung und Bilanzierung (z.B. durch einen aktuellen Überblick über die Höhe und Außenstandsdauer von Forderungen) kompensiert wird. Der Vorteil des dadurch ermöglichten Forderungsmanagements wird im Allgemeinen die zusätzlichen Kosten der Bilanzierung bei weitem übersteigen. Darüber hinaus wird auch in Bankgesprächen die Vorlage von Bilanzen in der Regel einen leichteren Zugang zu Finanzierungen ermöglichen.

27.12.2009 www.lbg.at