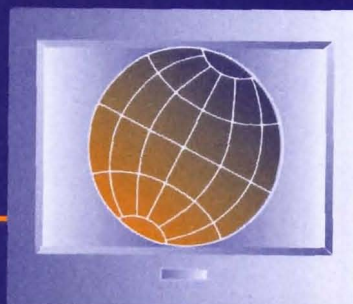


Kommunikation & Recht



Betriebs-Berater für

● Medien ● Telekommunikation ● Multimedia

9
K&R

Editorial: Lernen zu vergessen – Anmerkungen zum digitalen Verfallsdatum und zum digitalen Radiergummi
Dr. Thomas de Maizière

533 Aktuelle Entwicklungen im Fernabsatzrecht 2009/2010
Dr. Felix Buchmann

541 Selektiver Vertrieb und Internet
Dr. Jens Schulze zur Wiesche

545 Werbung für Telefentarife und notwendige Angaben – „Sondernewsletter“ · *Dr. Alexander Molle*

547 Wie sag ich's nur? Neues zur Formulierung von Unterlassungsanträgen · *Christian Franz*

551 Reaktionsmöglichkeiten des Arbeitgebers bei kritischen Äußerungen von Arbeitnehmern im Internet
Christian Willert

555 Das neue Leistungsschutzrecht für Presseverlage – eine Einführung · *Hendrik Wieduwilt*

562 Lobbyismus vs. Datenschutz: Zugang zu Dokumenten der Gemeinschaftsorgane · *Prof. Dr. Rainer Erd*

565 Länderreport Schweiz · *Dr. Ursula Widmer*

577 BGH: Hinsendekosten müssen bei Widerruf erstattet werden mit Kommentar von *Dr. Caroline Cichon*

13. Jahrgang **September 2010** Seiten 533–616

Verlag Recht und Wirtschaft · Frankfurt am Main

geregelt war. Nun muss aber auf dem fraglichen Treffen am 11. 10. 1996, also zwischen dem Beschluss der Kommission, an das Vereinigte Königreich eine Stellungnahme zu richten (26. 6. 1996) und der Ankündigung des Ministeriums für Handel und Industrie des Vereinigten Königreichs, die GBP so zu ändern, dass auch Flaschenbier nach England eingeführt werden darf (15. 3. 1997), etwas diskutiert worden sein, dass für Bavarian Lager von allergrößter Bedeutung war. Für das klagende Unternehmen waren die Informationen darüber wichtig, wer an dem Treffen teilgenommen hat, weil es selbst davon ausgeschlossen war.

Die Tatsache, dass Bavarian Lager trotz des Erfolgs das eigentlich nicht mehr erforderliche Datenschutzverfahren mit zäher Emsigkeit betrieben hat, lässt vermuten, dass auf der Sitzung am 11. 10. 1996, auf der neben Mitgliedern der Kommission auch Vertreter des englischen Ministeriums für Handel und Industrie sowie des Verbands der Bierbrauer des Gemeinsamen Marktes teilnahmen, Entscheidungen gefällt worden sind, mit denen Bavarian Lager nicht einverstanden war und die sie erhoffte, nach Kenntnis sämtlicher Teilnehmer des Treffens beeinflussen zu können. Da Bavarian Lager die Namen von fünf Teilnehmern und die Stellungnahme der Kommission nicht mitgeteilt wurde, war die Möglichkeit einer Konsultation aller Mitglieder der Kommission aufgrund der Kenntnis der Stellungnahme ausgeschlossen. Als die sich anschließende Klage von Bavarian Lager gegen die Kommission auf

Zugang zu diesen Informationen vom Gericht abgelehnt wurde (14. 10. 1999), war Bavarian Lager der Weg zu den gewünschten Informationen verschlossen. Man erfährt in dem Urteil des EuGH nicht, warum Bavarian Lager vier Jahre später (5. 12. 2003) die Kommission erneut um Zugang zu den bislang abgelehnten Dokumenten ersucht. Auf jeden Fall hat das erstinstanzliche Gericht Bavarian Lager Recht gegeben und die Entscheidung der Kommission für nichtig erklärt (8. 11. 2007).

III. Fazit

So wird der Leser der Entscheidung des EuGH mit der Erkenntnis konfrontiert, dass der erfreuliche Schutz personenbezogener Daten mit der wenig erfreulichen Unterstützung eines undurchsichtigen Lobbyismus erkaufte worden ist. In einer politischen Konstellation, in der Korruption und Undurchsichtigkeit politischer Entscheidungsprozesse ein herausragendes politisches Thema sind, ist die Entscheidung des EuGH unbefriedigend. Sie leistet einem Phänomen Vorschub, das aufklärungsorientierte Politiker beseitigen möchten: dem unkontrollierten Lobbyismus. Darüber hinaus kann der Leser der Entscheidung nur mutmaßen, warum ein Unternehmen wie Bavarian Lager, das scheinbar erfolgreich eine Entscheidung der Europäischen Kommission erreicht hat, ein datenschutzrechtliches Verfahren anstrengt, das es verliert und dessen nicht unbeachtliche Kosten es nun zu tragen hat.

Länderreport Schweiz

RAin Dr. Ursula Widmer, Bern*

I. Beschwerde für Open Source Software in der Bundesverwaltung ohne Erfolg

Das Bundesamt für Bauten und Logistik (BBL) vergab im Februar 2009 ohne öffentliche Ausschreibung einen Auftrag über 42 Mio. CHF an Microsoft. Gegenstand war die Verlängerung von Lizenzen sowie von Wartungs- und Supportleistungen für Microsoft-Produkte über eine Dauer von 3 Jahren. Gegen diese Vergabe führten 18 Anbieter von Open Source Software (OSS) beim schweizerischen BVerwG Beschwerde. Dieses hat am 6. 7. 2010 in öffentlicher Sitzung entschieden, dass die Beschwerde nicht zulässig sei, und ist demzufolge darauf nicht eingetreten.

Die Bundesverwaltung setzt seit Anfang der 90er Jahre Microsoft-Produkte ein. Diese sind Bestandteil des für die Bundesverwaltung definierten Standardarbeitsplatzes. Auf dieser Basis wurden über die Zeit mit Microsoft immer wieder Verträge zur Lizenzierung sowie für Wartung und Support von Microsoft-Produkten abgeschlossen. Die Auftragsvergabe an Microsoft erfolgte jeweils ohne Ausschreibung im so genannten freihändigen Verfahren. Es fand auch keine Publikation der Vergabe im Schweizerischen Handelsamtsblatt (SHAB) statt. Erst der Zuschlag für den Auftrag vom Februar 2009 ist im SHAB publiziert worden, was Anlass für die Beschwerde der OSS-Anbieter war.

Die Beschwerdeführer beantragten, den Zuschlag an Microsoft aufzuheben und das BBL als zuständige Vergabestelle des Bundes zu verpflichten, ein rechtskonformes Vergabeverfahren mit einer Ausschreibung durchzuführen.

Diesen Anträgen ist das Gericht nicht gefolgt. Das Gericht hat seinen Entscheid in der mündlichen Beratung damit begründet, dass die beschwerdeführenden OSS-Anbieter nicht in der Lage wären, ein mit Microsoft vergleichbares Alternativangebot zu machen. Da die Bundesinformatik auf einer Microsoft-Umgebung beruhe, könnten die OSS-Anbieter den zu vergebenden Auftrag, der die Verlängerung der Nutzung von Microsoft-Produkten und der damit im Zusammenhang stehenden Dienstleistungen zum Gegenstand habe, gar nicht erfüllen. Damit seien sie aber durch die Vergabe des Auftrags an Microsoft in ihren Interessen nicht betroffen und daher nicht legitimiert, Beschwerde zu führen.

Es wird interessant sein, die schriftliche Begründung des Entscheids zu analysieren. Insbesondere stellt sich die Frage, ob das Gericht auf mögliche Schranken hinweist, die verhindern, dass ein von der Bundesverwaltung einmal getroffener Produktentscheid durch die laufende Verlängerung bestehender Verträge zementiert wird, und alternative Anbieter keinerlei Chance mehr haben, berücksichtigt

* Mehr über die Autorin erfahren Sie auf S. XII.

zu werden. Ebenso darf man gespannt sein, ob die unterlegenen OSS-Anbieter den Entscheid an das Bundesgericht weiterziehen werden. Dies dürfte davon abhängen, wie überzeugend dem Gericht die Begründung für sein Urteil gelingt.

II. Bundesrat beantragt Ratifizierung der Cybercrime-Konvention

Der Bundesrat hat im Juni die Botschaft zur Ratifizierung der Europarats-Konvention über Cyberkriminalität an das Parlament weitergeleitet. Die Schweiz hatte die Konvention zusammen mit den meisten anderen Europarats-Staaten sowie den USA, Kanada, Japan und Südafrika im November 2001 unterzeichnet. Die beantragte Ratifizierung der Konvention ist zeitlich koordiniert mit der neuen schweizerischen Strafprozessordnung, welche per 1.1.2011 in Kraft treten und die einzelnen Strafprozessgesetze der Kantone ablösen wird.

Die Konvention sieht die Harmonisierung des materiellen Strafrechts bezüglich Computerdelikten (Computerbetrug, Datendiebstahl, Datenbeschädigung, Fälschung von Daten, Eindringen in fremde Datenverarbeitungssysteme) sowie betreffend Kinderpornographie und Urheberrechtsverletzungen im Internet vor. Die Konvention enthält ferner Regeln über die Beweiserhebung und -sicherung bei elektronischen Daten, mit dem Ziel, dass die Daten für den weiteren Ablauf des Verfahrens gesichert und nicht verfälscht oder vernichtet werden können. Schließlich betrifft die Konvention die grenzüberschreitende Zusammenarbeit zwischen den Behörden der Vertragsstaaten.

Nach Ansicht des Bundesrates sind die Anforderungen der Konvention im schweizerischen Recht, insbesondere auch in der neuen schweizerischen Strafprozessordnung, bereits weitestgehend erfüllt, jedoch unter der Voraussetzung, dass zu mehreren Bestimmungen der Konvention entsprechende Vorbehalte gemacht und Erklärungen abgegeben werden, wie dies die Konvention den Vertragsstaaten als Möglichkeit einräumt. Anpassungen des schweizerischen Rechts sind daher nur in zwei Fällen notwendig. Einmal ist der Tatbestand des unbefugten Eindringens in ein fremdes Datenverarbeitungssystem (Hacking) in dem Sinne zu erweitern, dass bereits das Inverkehrbringen oder das Zugänglichmachen von Passwörtern, Programmen oder anderen Daten, von denen der Täter weiss oder annehmen muss, dass sie zum Zweck des Hacking verwendet werden sollen, strafbar sind. Zum Zweiten ist das Gesetz über die Internationale Rechtshilfe um eine Bestimmung zu ergänzen, die den Behörden gestattet, Verkehrsdaten aus der Überwachung des Fernmeldeverkehrs bereits vor Abschluss des Rechtshilfeverfahrens an die ersuchenden ausländischen Behörden weiterzuleiten.

Ausgeschlossen von der beantragten Ratifikation ist das Zusatzprotokoll zur Cybercrime-Konvention gegen Rassismus und Fremdenfeindlichkeit. Über dessen Ratifizierung soll zu einem späteren Zeitpunkt in einem separaten Schritt entschieden werden.

III. Totalrevision der Fernmeldeüberwachung in Vorbereitung

Nachdem, wie hier berichtet (vgl. K&R-Newsletter Schweiz, K&R 2009, 631), eine erste Ausdehnung der

Fernmeldeüberwachung im Bereich des Internetverkehrs bereits auf Verordnungsstufe erfolgte, ist nun die Totalrevision des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) mit dem Hauptziel der konsequenten Erfassung des Internetverkehrs, insbesondere der Internettelefonie, eingeleitet worden. Es wurde bei den interessierten Kreisen eine Vernehmlassung zum Gesetzes-Vorentwurf durchgeführt. Nach Auswertung der Vernehmlassungsergebnisse wird die Ausarbeitung eines Gesetzesentwurfs erfolgen, der dann vom Bundesrat zur Beratung an das Parlament weitergeleitet wird.

Gemäß dem Vorentwurf regelt das Gesetz die Überwachung des Post- und Fernmeldeverkehrs im Zusammenhang mit Strafuntersuchungen, der internationalen Rechtshilfe in Strafsachen, der Suche nach vermissten Personen und neu auch bei der Fahndung nach Personen, die zu Freiheitsstrafen verurteilt oder gegen die freiheitsentziehende Maßnahmen angeordnet sind. Der persönliche Geltungsbereich soll erweitert werden und neu nicht nur Fernmeldediensteanbieter, wie Anbieter von Festnetz- und Mobiltelefonie und Internet Zugangsanbieter, sondern auch Hosting-Anbieter erfassen, mit dem Argument, dass auch Letztere zu bestimmten Zeitpunkten Kommunikationsdaten in ihrem Besitz haben.

Die Pflicht zur Aufbewahrung von Verkehrs- und Rechnungsdaten (Vorratsdatenhaltung) durch die Anbieter soll von bisher 6 Monaten auf neu 12 Monate ausgedehnt werden. Ferner sollen die Anbieter, die an den Überwachungen mitwirken müssen, für ihren Aufwand nicht mehr entschädigt werden. Dies erscheint fragwürdig. Die Tätigkeit der Fernmeldediensteanbieter im Zusammenhang mit Fernmeldeüberwachungen stellt eine echte Dienstleistung dar und ist mit Kosten verbunden. Das Argument, dass Fernmeldediensteanbieter aus der Nutzung des öffentlichen Fernmeldemonopols Nutzen ziehen würden und sich daher Gratisleistungen an den Staat rechtfertigen, ist nicht überzeugend. Damit ließe sich auch begründen, dass staatliche Stellen für ihre normale Nutzung von Fernmeldediensten (Telefon, Fax, E-Mail etc.) auch keine Kosten zu tragen hätten. Konsequenterweise hätten dann auch andere Wirtschaftsbereiche, die auf der Nutzung öffentlicher Monopole beruhen, z. B. das Transportgewerbe, ihre Leistungen an den Staat gratis zu erbringen.

Weitere Neuerungen betreffen die Präzisierung der Aufgaben des Dienstes für Besondere Aufgaben, der bei der Durchführung der Überwachung zwischen den Strafverfolgungsbehörden und den Fernmeldediensteanbietern eingeschaltet ist, sowie die Bearbeitung der aus den Überwachungen gewonnenen Daten durch den Dienst, z. B. bezüglich der Aufbewahrung der an den Dienst übermittelten Daten in dessen System.

Hinweise der Redaktion:

Siehe auch den Beitrag von *Schirnbacher/Bühlmann*, „Grenzüberschreitender E-Commerce zwischen Deutschland und der Schweiz am Beispiel der Preiswerbung im Internet“, in: K&R 2010, 220 ff. (Heft 4) sowie die weiteren Länderreports von *Widmer*, in: K&R 2009, 631 (Heft 10), K&R 2010, 29 (Heft 1) und K&R 2010, 316 (Heft 5).