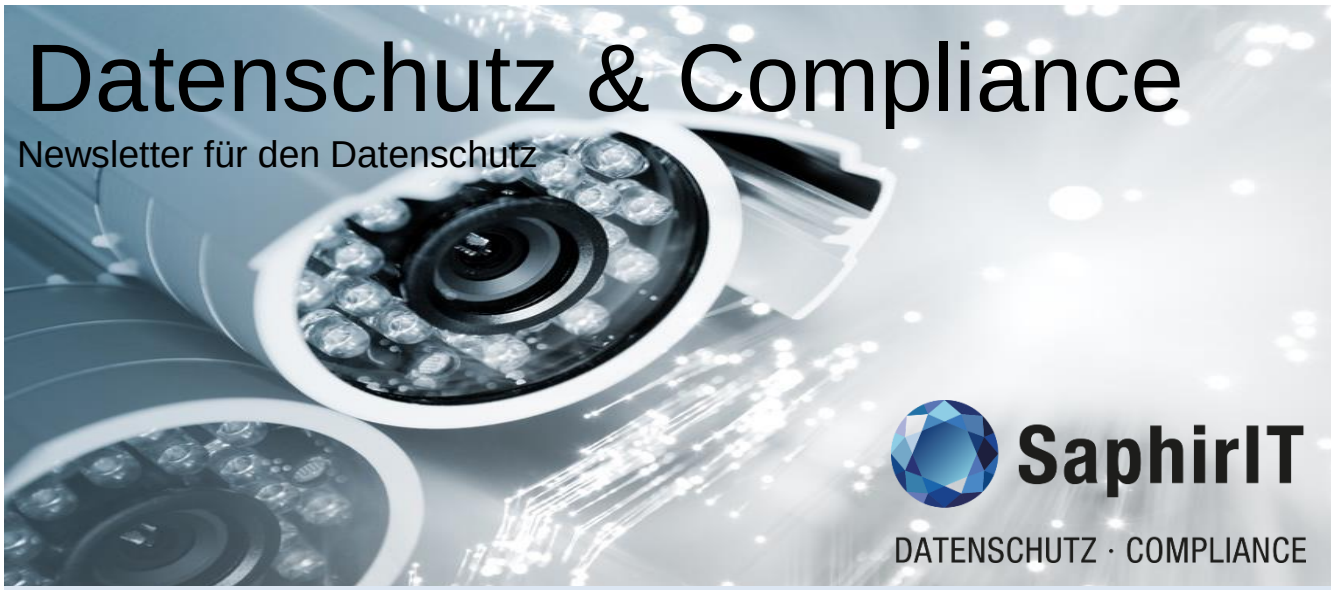

Ausgabe Juni 2017 | Seite 12-16

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren aktuellen Newsletter Juni 2017.

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Zwischen Transparenz und Datenschutz

- Verweise auf gelöschte Links müssen durch Google unterlassen werden -

Lumendatabase: Vielen womöglich noch komplett unbekannt. Es handelt sich dabei um ein Projekt, welches sich für Transparenz im Internet einsetzt und gelöschte Inhalte dokumentiert. Betrieben wird das Projekt von der *Berkman Klein Centre for Internet & Society at Harvard University*.

Nach eigenen Angaben soll das Projekt nicht nur die Löschung von Daten im Internet dokumentieren, sondern auch vermerken, wer wann die Löschung veranlasst hat und warum.

Wird dann beispielsweise Google, auf richterliche Anordnung dazu aufgefordert, eine Änderung/Löschung am Suchindex vorzunehmen, wird dieser Vorgang in der „Lumen“-Datenbank vermerkt.

In einem solchen von der Lumendatabase verlinkten Eintrag findet sich dann ein nicht aktiver Link zu einer archivierten Suche, welche die gelöschten Suchergebnisse weiter enthält.

Auch über die Suche der Datenbank lassen sich dann gelöschte Links noch rekonstruieren.

Transparenz für alle, im Grundsatz sicherlich ein lobenswertes Ziel. Dies gilt, gerade, wenn man an die heutige Zeit denkt, in der mit allen rechtlichen Möglichkeiten versucht wird bestimmte Berichte oder Informationen zu verhindern oder auch zu verändern.

Fraglich bleibt jedoch inwiefern dabei möglicherweise länderspezifisch datenschutzrechtlich gegen bestimmte Vorschriften verstoßen wird.

Dem Urteil des OLG München liegt folgender Sachverhalt – welcher nicht auf den ersten Blick mit Lumendatabase in Berührung kam – zu Grunde:

Es existierten offenbar Äußerungen im Internet mit denen behauptet wurde, dass gegen ein betroffenes Unternehmen Ermittlungen wegen eines Betrugsverdachts eingeleitet worden sind. Tatsächlich, so stellte sich dann heraus, handelte es sich aber um Ermittlungen wegen eines Verdachts auf Kapitalanlagebetrug.

Das OLG München gelangte zu der Auffassung, dass sich ein Betrugsverdacht erheblich von einem Kapitalanlagebetrugsverdacht unterscheide und ordnete die bisherigen Äußerungen als falsche Tatsachenbehauptungen ein.

Google wurde daraufhin verpflichtet die entsprechend falschen Suchergebnisse zu löschen. Der Aufforderung kam Google nach. Problematisch wurde es dann jedoch, als Google gleichzeitig das Gericht darauf hinwies, dass bestimmte Suchergebnisse von Nutzern bei der Löschung nicht berücksichtigt werden könnten und verwies auf die Website der *lumendatabase.org*.

Die Löschung wurde dort offensichtlich dokumentiert und ferner ein Link bereitgehalten, welcher zu einer weiteren Website führte, auf der die rechtsverletzenden Inhalte einsehbar waren.

Beantwortet werden musste dann die Frage, ob es Google auch untersagt werden kann, im Zusammenhang mit den gelöschten Ergebnissen auf *lumendatabase.org* zu verlinken. Wie Google vortrug, handelte es sich jedoch nicht um eine direkte Verlinkung auf den gegenständlichen Inhalt selbst, sondern der Nutzer, der die Daten einsehen wollte, musste seinerseits noch weitersuchen.

Im Ergebnis war das OLG München dennoch der Auffassung, dass Google neben der konkreten Löschung der Daten auch diese Verlinkung zu *lumendatabase.org* zu unterlassen habe.

Dieser Fall schildert besonders deutlich wo die Kollisionen zwischen Persönlichkeitsrechten und der Meinungs- und Informationsfreiheit liegen. Auf der einen Seite das Projekt einer Amerikanischen Universität, die Transparenz schaffen will und auf der anderen Seite eine nach deutschem Recht bestehende Rechtsverletzung und dementsprechende Ansprüche eines betroffenen Unternehmens. Zusätzlich stellt sich durch die weltweite Aufrufbarkeit das Problem, dass verschiedene Rechtsordnungen, verschiedene Äußerungen zulassen und unterschiedlich sanktionieren.

Bezogen auf den Fall wird es jedoch immer auf den konkreten Einzelfall ankommen und letztlich eine Entscheidung der Gerichte sein, welche Äußerungen rechtmäßig sind, welche nicht und welche dieser Daten dann wo weiterverlinkt und zu finden sein dürfen (OLG München, Urt. v. 07.06.2017 – Az. 18 W 826/17).

Prüfpflichten des Inhabers eines Internetanschlusses

- Nutzer dürfen voreingestelltem Router Passwort vertrauen -

Mit Urteil vom 24.11.2016 hat der BGH eine Störerhaftung des Inhabers eines Internetanschlusses verneint, wenn das WLAN ausreichend verschlüsselt ist.

Das meist aus einer zufälligen 16-stelligen Ziffernfolge voreingestellte Passwort genüge dabei den Anforderungen an die sicherzustellende Passwortsicherheit. Sofern ferner davon ausgegangen werden kann, dass im Zeitpunkt der Bereitstellung des Anschlusses keine Sicherheitslücke vorlag, stünden einer Beibehaltung des Passworts keine Bedenken entgegen und stellten keinen Verstoß gegen die Prüfungspflicht des Anschlussbesitzers dar.

Der Sachverhalt stellte sich wie folgte dar: Über den Internetanschluss der Beklagten wurde ein Film Dritten im Internet zum Download angeboten. Die Beklagte erhielt daraufhin eine Abmahnung und sollte 750,- zahlen. Es stellte sich heraus, dass ein unbekannter Dritter sich in das WLAN der Beklagten gehackt hatte, den Film heruntergeladen und angeboten hatte. Es musste nun die Frage geklärt werden, inwieweit sie selbst für den entstandenen Schaden zu haften hatte.

Der genutzte Router wurde im Februar 2012 eingerichtet und nach den oben genannten Kriterien gesichert. Das Passwort hätte individuell geändert werden können. Diese Änderung wurde aber nicht vorgenommen.

Für die Klägerin war klar, dass die Beklagte als Störerin daher haften müsse.

Sowohl das Amtsgericht Hamburg, als auch das Landgericht Hamburg hatten den Anspruch der Klägerin auf Erstattung der Abmahnkosten abgewiesen.

Mit der von der Beklagten getätigten Verschlüsselung sei sie den Sicherungspflichten

ausreichend nachgekommen und sie sei ohne konkrete Anhaltspunkte auch nicht zu einer vorsorglichen Änderung des Passworts verpflichtet gewesen.

Es lasse sich auch nicht feststellen, dass der Router nicht mit einem vom Hersteller individuell für das Gerät vergebenen Schlüssel gesichert gewesen sei, wie es die Klägerin behauptete, was zu einer Pflicht der Änderung geführt hätte.

Auch wenn die Beklagte in diesem Fall die Abmahngebühren nicht zahlen musste, lag es nur daran, dass sie selbst nachweisen konnte, dass Dritte ihr WLAN unrechtmäßig genutzt hatten. Häufig ist ein solcher Nachweis in der Praxis jedoch nicht möglich. In einer solchen Konstellation wären die Betroffenen auch nach diesem Urteil weiterhin in der Haftung (BGH, Urt. v. 24.11.2016 – I ZR 220/15).

Keinen Zugriff für Eltern auf Facebook Account verstorbener Tochter

- Schutz des Fernmeldegeheimnisses steht Anspruch der Erben entgegen -

Das Berliner Kammergericht entschied vergangenen Monat in zweiter Instanz, dass die Mutter eines 2012 verstorbenen Mädchens keinen Zugriff auf das Facebook Konto ihrer Tochter und damit zu der Kommunikation mit Dritten bekommt. Das Kammergericht stellte sich damit gegen das Urteil des Berliner Landgerichts aus dem Jahre 2015.

Hintergrund war, dass die Mutter wissen wollte, ob es sich bei dem Unfall 2012, bei dem das Mädchen vor einer einfahrenden U-Bahn tödlich verletzt worden war möglicherweise um einen Suizid handelte. Dafür forderte sie von Facebook Zugang zu den Chat Nachrichten ihrer Tochter.

Obwohl die Eltern die Zugangsdaten der Verstorbenen besaßen, weigerte Facebook sich den Zugriff zu ermöglichen und verwies dabei auf den Datenschutz.

Eine Anmeldung war deshalb nicht möglich, weil das Konto von Facebook in den sogenannten Gedenkzustand versetzt wurde, in welchem ein Zugang zu dem Konto nicht mehr ohne weiteres möglich ist. Dieser Zustand wurde laut Facebook durch einen Nutzer veranlasst, den die Eltern der Verstorbenen nicht kennen.

Nach Ansicht des Kammergerichts stehe der Schutz des Fernmeldegeheimnisses dem Anspruch der Erben entgegen eine Einsicht in die Kommunikation der Tochter mit Dritten zu erhalten. Dies sei selbst anzunehmen, wenn man davon ausgehe, dass der Account in das Erbe falle und somit die Erbengemeinschaft Zugang zu den Inhalten des Accounts erhalten müsse.

Das Telekommunikationsgesetz sei ursprünglich für Telefonanrufe geschaffen worden, es erstrecke sich nach der Ansicht des Bundesverfassungsgerichts aber auch auf E-Mails, die auf einem Server gespeichert sind. Insbesondere durch das Grundrecht aus Art. 10 werde dies geschützt.

Es gebe auch keine andere gesetzliche Vorschrift, die eine Ausnahme des Fernmeldegeheimnisses rechtfertige. Insbesondere das Erbrecht nach dem BGB lasse nicht erkennen, dass der Gesetzgeber den Willen gehabt habe, das Fernmeldegeheimnis einzuschränken, führte das Kammergericht weiter aus.

Die Tatsache, dass die Mutter vortrug, die Tochter habe ihr ihre Zugangsdaten überlassen hätte nichts geändert, so der Senat. Selbst, wenn man davon ausgehen würde, dass diese Behauptung der Wahrheit entspreche, hätten alle Dritten, mit denen die Tochter kommuniziert hatte auf den Schutz des Fernmeldegeheimnisses verzichten müssen (KG Berlin, Urt. v. 31.05. 2017 – 21 U 9/16).

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de