

Die Gedanken sind frei
- das Internet auch!
Keine Verpflichtung zur
Errichtung von DNS- oder
IP-Sperren

Rechtswidrige Inhalte in
RSS-Feeds = Haftungsfrage?

Rechtliche Aspekte
sozialer Netzwerke:
Teil 2: Facebook und
Datenschutz –
Gefällt mir (nicht)



Die Gedanken sind frei – das Internet auch!

Keine Verpflichtung zur Errichtung von DNS- oder IP-Sperren

Von Dipl.-Jur. Julian Fischer

Erneut musste die Frage nach einer möglichen zivilrechtlichen Verantwortlichkeit des Access-Providers im Hinblick auf die Sperrung von IP-Adressen beantwortet werden. Abermals – nunmehr vom Landgericht Köln – wurde sie verneint. Das Gericht macht deutlich, dass eine entsprechende Errichtungsverpflichtung zu Filter- und Sperrmaßnahmen einer ausdrücklichen gesetzlichen Ermächtigung bedarf. Insoweit wäre also der Gesetzgeber aufgefordert, tätig zu werden. Allerdings ist fraglich, ob sich dieser der Aufgabe annehmen wird, denn ohnehin wird die Zumutbarkeit für den Access-Providers zur Aufrechterhaltung einer wirksamen Infrastruktur von DNS- oder IP-Sperren durch das Gericht verneint.

Wenn „geistiges Eigentum“ im Internet systematisch verletzt wird und sich Websites mit den bereitstellenden Inhalten immer größerer Beliebtheit erfreuen, wird der Ruf nach Unterbindung und Zugangsbeschränkung der betreffenden IP-Adressen laut. Dabei ist es erfahrungsgemäß besonders schwierig, die tatsächlichen Rechtsverletzter ausfindig zu machen bzw. den Host-Service-Provider zur Sperrung eines bestimmten Dienstes zu veranlassen. So zeigte sich etwa bei der Schließung des Streamingportals „kino.to“ Mitte des Jahres, wie aufwendig und langwierig Ermittlungen in diesem Bereich sein können. Interessanter für die verletzten Rechteinhaber wäre es daher, bereits den Zugangsvermittler (Access-Provider) zur Verantwortung ziehen zu können, sodass dieser verpflichtet würde, den Zugang zu derartigen Internetangeboten zu sperren. Dadurch wären die entsprechenden IP-Adressen gar nicht oder aber erst über Umwege erreichbar, wodurch der Domainname letztlich an Attraktivität einbüßen würde. Der kürzliche Versuch seitens einer Reihe von Tonträgerherstellern, eine derartige Sperrverfügung gegen ein den Zugang zum Internet vermittelndes Telekommunikationsunternehmen zu erwirken, wurde vom LG Köln (Urteil vom 31.08.2011, Az.: 28 O 362/10) allerdings abgewiesen. Wieder einmal, so müsste es heißen, denn nahezu alle Gerichte erteilten in der Vergangenheit einem derartigen Klägerbegehren eine Absage. Der Grund hierfür erscheint auf den ersten Blick recht trivial: Es fehlt an einer ausreichenden Gesetzesgrundlage. Weder deutsches noch europäisches Recht können den durch die Errichtung einer Sperrmaßnahme zwangsläufig einhergehenden Eingriff in das Fernmeldegeheimnis aus Art. 10 GG rechtfertigen.

I. Sperrungsmaßnahmen als unzulässige Verpflichtung des Access-Providers

Eine Haftung des Access-Providers als Täter oder Teilnehmer in Bezug auf die vorgenommene Rechtsverletzung scheidet aus. Derjenige, der Nutzerinformationen lediglich weiterleitet oder die Zugangsvermittlung zu einem Kommunikationsnetz herstellt, hat bereits rein

faktisch keinen Zugriff auf die betroffenen Webseiten mit dem inkriminierenden Inhalt. Zu überlegen wäre daher eine Haftung als mittelbarer Störer zu konstruieren. Dies könnte im Urheberrecht unter Anwendung von § 97 I Urheberrechtsgesetz (UrhG) i. V. m. § 1004 Bürgerliches Gesetzbuch (BGB) erfolgen.

1. Verursachungsbeitrag und Prüfungspflicht

Nach der Rechtsfigur der mittelbaren Störerhaftung kann neben einer eigenverantwortlich handelnden Person auch derjenige auf Unterlassung in Anspruch genommen werden, der in irgendeiner Weise – ohne Täter oder Teilnehmer zu sein – willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt. Zwar ist fraglich, ob in der von einem Internetzugangsanbieter bereitgestellten (rein technischen) Dienstleistung aufgrund ihrer sozial erwünschten Funktionsweise überhaupt ein adäquat kausales Handeln im haftungsrechtlichen Sinne gesehen werden kann. Allerdings muss sich die Frage des Verursachungsbeitrags danach beurteilen lassen, ob das beanstandete Verhalten im Allgemeinen geeignet ist, einen Erfolg der fraglichen Art herbeizuführen. Hierzu stellte das LG Köln richtigerweise fest, dass gerade beim Aufruf von Internetseiten, bei denen eine Vielzahl der Nutzer ohne eine entsprechende Lizenz urheberrechtlich geschützte Werke herunterlädt, in der Zugangsvermittlung ein solcher rechtlich relevanter Verursachungsbeitrag für die Rechtsverletzung zu sehen ist. Zu beachten ist jedoch, dass eine Haftungsmöglichkeit des nur mittelbar Mitwirkenden nicht dazu führen darf, dass dieser aus Praktikabilitätsgründen vorschnell in Anspruch genommen wird. Es bestünde die Gefahr, dass der eigentliche Täter außen vor bliebe, was mit den unterschiedlichen Beiträgen in Bezug auf die Rechtsverletzung nicht in Einklang gebracht werden könnte. Mit anderen Worten darf die „Störerhaftung“ nicht über Gebühr auf Dritte erstreckt werden, die lediglich neutrale Berührungspunkte zur Rechtsverletzung aufweisen. Deshalb fordert die Rechtsprechung bei einer Haftung des Störers für Handlungen Dritter eine Verletzung ihm obliegender Prüfungspflichten. Entscheidende Frage ist daher, ob

dem Access-Provider eine derartige Pflicht zur Überprüfung der Inhalte der vom Vertragspartner aufgerufenen und von dritter Seite angebotenen IP-Adressen obliegt. Im Allgemeinen richtet sich die Reichweite der Prüf- oder Verhaltenspflicht nach den jeweiligen Umständen des Einzelfalls unter Berücksichtigung der Funktion und Aufgabenstellung des Störers und der Eigenverantwortlichkeit desjenigen, der die rechtswidrige Beeinträchtigung unmittelbar vorgenommen hat. Diese wertende Betrachtung lässt viel Raum für Argumentation, weshalb nicht ausgeschlossen werden kann, dass ein Access-Provider der Störerhaftung unterliegen kann; immer vorausgesetzt, dass ihm Kenntnis von der Rechtsverletzung vermittelt worden ist. Zur Beurteilung des Bestehens der gegenständlichen Prüfungspflicht stellte sich das LG Köln die Frage, worauf die Bejahung einer solchen hinauslaufen würde. So hätte der Access-Provider letztlich Vorsorge dafür zu treffen, dass es (möglichst) zu keinen gleichartigen Rechtsverletzungen kommt. Im Ergebnis wäre das Telekommunikationsunternehmen ab dem Zeitpunkt der Kenntniserlangung zu entsprechenden Vorsorgemaßnahmen verpflichtet, die auch die Errichtung von DNS- oder IP-Sperren umfassen würden.

2. Fehlen einer ausreichenden Gesetzesgrundlage

Unterstellt, derartige Maßnahmen zur Filterung des Datenverkehrs sind technisch so ausgestaltbar, dass die betroffenen Inhalte isoliert gesperrt werden können, ergibt sich die Frage nach deren rechtlicher Zulässigkeit. Filter- und Sperrungsmaßnahmen setzen voraus, dass der Access-Provider die Datenkommunikation kontrolliert, wozu er sich Kenntnisse von Umständen der Telekommunikation einschließlich ihres Inhalts verschaffen müsste. Ein derartiges Vorgehen greift nach Ansicht des LG Köln in das Fernmeldegeheimnis aus Art. 10 I GG ein, das jegliche Arten und Formen der Telekommunikation erfasst und auch vor Filter- und Sperrmaßnahmen schützt. Ein solcher Eingriff durch den Internetzugangsanbieter bedürfte zu seiner Rechtfertigung einer entsprechenden gesetzlichen Grundlage. Genau daran fehlt es an dieser Stelle: Weder die allgemeine Störerhaftung (§ 97 UrhG, § 1004 BGB) noch die Hinzuziehung europäischer Richtlinien können eine hinreichend bestimmte Grundlage sein, um dem grundrechtlichen Schutz des Fernmeldegeheimnisses zu genügen. Zwar bestimmt Art. 8 Abs. 3 der Richtlinie 2001/29/EG (Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft), dass gerichtliche Anordnungen gegen „Vermittler“, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandten Schutzrechts genutzt wurden, grundsätzlich möglich sind. Allerdings bedarf diese Regelung aufgrund ihrer Eigenart als Richtlinienvorschrift der weiteren Konkretisierung durch den nationalen Gesetzgeber. Sollte eine solche überhaupt gewollt sein, müsste sie Anlass, Zweck und Umfang des Eingriffs präzise und bereichsspe-

zifisch regeln. Dem Access-Provider müsste ein eindeutiger Rahmen vorgegeben werden, auf Grund dessen er entscheiden kann, wann die Voraussetzungen einer Zugangerschwerung vorliegen.

II. Unzumutbarkeit und Untauglichkeit der Errichtung von Filter- und Sperrungsmaßnahmen

Daneben bezog das LG Köln Stellung zu der Frage, ob die Errichtung von Filter- und Sperrungsmaßnahmen dem Access-Provider überhaupt zumutbar ist. Die Etablierung einer entsprechenden Vorsorgepflicht hätte zur Folge, dass der Zugangsvermittler eine Vielzahl von technischen Sicherungsvorkehrungen in Form von Datenfiltern einrichten müsste, die wiederum immer neuen Gegebenheiten sowie neuen Verletzungsformen angepasst werden müssten. Dem Gericht erscheint eine solche weitgehende Haftung des Internetzugangsanbieters, der lediglich die technische Infrastruktur für den Internetzugang zur Verfügung stellt, nicht gerechtfertigt. Maßgeblich ist hierbei, ob die begehrten Sperren überhaupt ein taugliches Mittel zur Verhinderung weiterer Rechtsverletzungen darstellen. Dabei gilt, je leichter eine Erschwerungsmaßnahme umgangen werden kann, desto weniger wird vom Internetanbieter die Errichtung einer solchen Sperre verlangt werden können. Zudem ist zu beachten, dass die Sperrung sämtlicher Inhalte einer Internetseite nicht in Betracht kommt, sofern dadurch auch der Zugang zu zulässigen Angeboten unmöglich gemacht wird. Das LG Köln hebt hierbei hervor, dass bereits die Änderung eines Zeichens der URL-Webseite dazu führt, dass das gleiche rechtswidrige Angebot unter der gleichen Internetdomain, wenn auch mit einer anderen URL, abrufbar bleibt. Vor diesem Hintergrund erscheint dem Gericht eine Verpflichtung des Internetanbieters zu einer effektiven technischen Infrastruktur mit entsprechendem Personal, die Grenze des Zumutbaren zu verlassen.

Diesen Ausführungen hätte es – nach Feststellung der fehlenden Ermächtigungsgrundlage – gar nicht mehr bedurft. Sie können insoweit als Hinweis des Gerichts verstanden werden, dass dieses ablehnend gegenüber einer Verpflichtung des Access-Providers zur Errichtung von DNS- oder IP-Sperren eingestellt ist.

III. Ausblick

Die zivilrechtliche Inanspruchnahme eines Access-Providers auf Sperrung einer Internetseite ist derzeit, mangels gesetzlicher Ermächtigungsgrundlage, nicht durchsetzbar. Es bleibt abzuwarten, ob der deutsche Gesetzgeber hier tätig wird, da dieser Netzsperrungen zur Durchsetzung zivilrechtlicher Ansprüche – beispielsweise bei Verletzungen von Persönlichkeits-, Namens- oder Markenrechten sowie urheberrechtlichen Rechtspositionen - durchaus kritisch sieht. Dies verdeutlichte auch

das gescheiterte Zugangerschwerungsgesetz, bei dem es sich um eine spezifische Regelung der Bekämpfung von Kinderpornographie handelte und welches bereits eine Geltendmachung derartiger Ansprüche explizit ausschloss (§ 7 II ZugErschwG).

Zugleich ist schwer vorstellbar, wie eine praktikable und rechtskonforme gesetzliche Regelung für Sperrverfügungen überhaupt aussehen könnte. So erteilt die Rechtsprechung auch der Frage der Zumutbarkeit einer Verpflichtung des Access-Providers zur Unterhaltung einer effektiven Sperrinfrastruktur eine Absage. Zudem führt der zwangsläufig einhergehende Zugriff auf Verkehrsdaten dazu, dass die Sperrverfügung dem Richtervorbehalt (§ 101 IX UrhG) unterfiele, weshalb eine entsprechende Ermächtigungsgrundlage sowohl die Verwendung der Daten, als auch den Rechtsschutz der betroffenen Internetnutzer zu regeln hätte. Gleiches gilt für die Notwendigkeit einer Kostenregelung (§ 101 II 3 UrhG), wie auch für die Sicherstellung effektiven Schutzes vor der Sperrung zulässiger Inhalte.

Trotz Fehlens einer gesetzlichen Regelung sowie der Fragwürdigkeit einer Neuregelung in der Zukunft, darf das Thema der Sperrverpflichtungen nicht ad acta gelegt werden. So erklären etwa englische Gerichte derartige Sperr- oder Verfügungsanordnungen für zulässig, obwohl im Zuge zunehmender europäischer Harmonisierung die wesentlichen Fragen einheitlich geregelt sein sollten. Sollte der deutsche Gesetzgeber weiterhin untätig bleiben, so ist eine Klärung der Rechtsfrage auf europäischer Ebene recht wahrscheinlich.

Rechtswidrige Inhalte in RSS-Feeds = Haftungsfalle?

Dipl. Jur. Eva-Maria Herring

Mit den Entscheidungen des Landgerichts Berlin (Urteil vom 27.04.2010 – 27 O 190/10 und Beschluss vom 15.02.2011 – 15 O 103/11) zur Haftung von RSS-Feeds sind zwei Entscheidungen ergangen, die Webseitenbetreiber aufhorchen lassen sollten. Immer öfter verwenden Webseitenbetreiber fremde RSS-Feeds, um das eigene Content-Angebot aufzuwerten. Mit der Einbindung fremder Inhalte über einen RSS-Feed in die eigene Onlinepräsenz setzen sich die Webseitenbetreiber jedoch einem enormen Haftungsrisiko aus. Denn nach Ansicht des LG Berlin macht sich ein Webseitenbetreiber die Inhalte durch die Einbindung auf die eigene Webseite zu eigen und haftet dementsprechend für sämtliche Rechtsverletzungen.

I. Einleitung

Ob Nachrichtenseiten, Börsenticker oder Blogs – nahezu jede Webseite mit täglich wechselnden Inhalten bietet inzwischen einen RSS-Dienst an, um die Leser immer auf dem neuesten Stand zu halten. Der Siegeszug von RSS-Feeds ist vor allem der Tatsache geschuldet, dass das zugrundeliegende Prinzip einfach und praktikabel ist. Das RSS-Format ist eine XML-Datei, in der Inhalte von Webseiten strukturiert ohne zusätzlichen Ballast wie Design- und Layout-Elemente veröffentlicht werden. Abonniert der Nutzer einen RSS-Channel, wird mithilfe eines Aggregatorprogramms oder eines Feedreaders in einstellbaren Intervallen automatisch geprüft, ob Artikel geändert wurden. Dem Nutzer wird nicht der gesamte Nachrichteninhalte angezeigt, sondern nur eine Liste der aktuellen Schlagzeilen mit knapper Kurzbeschreibung. Jede Schlagzeile ist mit einem Link versehen, der zum Volltext der entsprechenden Meldung führt. Ein RSS-Feed erfüllt die Benachrichtigungsfunktion auf nahezu ideale Weise: Der Nutzer kann sämtliche Änderungen einer Webseite schnell und effektiv verfolgen und verschafft sich dadurch stets einen aktuellen Überblick über den Stand der von ihm ausgewählten Quellen. Gleichzeitig spart er enorm viel Zeit ein, da er mithilfe der Kurzbeschreibung entscheiden kann, ob die Nachricht einen Besuch der ursprünglichen Webseite überhaupt wert ist. Aufgrund dieser Charakteristika sind RSS-Feeds gerade für Webseitenbetreiber interessant: Auch wenn diese selbst keinen eigenen RSS-Feed betreiben, können sie nämlich auf ihrer Webseite den RSS-Feed eines Dritten einbinden, um dadurch das eigene Content-Angebot interessanter zu gestalten.

II. Haftung als Störer für eingebundene RSS-Feeds

Während der erste der beiden vom LG Berlin zu entscheidenden Fälle eine Persönlichkeitsrechtsverletzung betraf, ging es im zweiten Fall um die Einbindung einer Fotografie, für die der Urheber dem Webseitenbetreiber kein Nutzungsrecht eingeräumt hatte. Unabhängig von der speziellen Rechtsverletzung dreht es sich aber im Kern um dieselbe Rechtsfrage: Haftet der Betreiber einer Webseite für Rechtsverletzungen in einem eingebundenen RSS-Feed eines Dritten.

In beiden Fällen nahm das Gericht eine Haftung als Störer an, da sich der Webseitenbetreiber den Inhalt des RSS-Feed zu eigen gemacht habe. Zur Begründung wurde ein Vergleich zu Forenbetreibern gezogen: Während jene nur die technische Plattform zur Verfügung stellen, auf der fremde Mitteilungen verbreitet werden, trete der Webseitenbetreiber, der fremde Inhalte aus einem RSS-Feed in seine eigene Webseite einbindet, als „Herr des Angebots“ auf. Er mache sich die beanstandete Nachricht zu eigen und füge sie bewusst seinem Angebot hinzu, sodass er von der Einstellung des Beitrags nicht erst mit der Abmahnung erfahre und sich somit auch nicht auf die fehlende Pflicht, vorbeugend Beiträge auf etwaige Rechtsverletzungen hin zu überprüfen, berufen könne.

Unerheblich sei, ob ein durchschnittlicher Nutzer der Internetseite habe erkennen können, dass die Mitteilung nicht vom Webseitenbetreiber selbst stamme, da sie jedenfalls von ihm im Internet verbreitet wurde. Die Verbreitung eines urheber- oder persönlichkeitsrechtsverletzenden Inhalts sei als eigenständige Rechtsverletzung zu werten, die einen Unterlassungsanspruch nach sich ziehen kann.

Nach Ansicht des Gericht lagen in beiden Fällen auch keine Umstände vor, die eine Rechtsverletzung ausschließen: Insbesondere reiche eine pauschale Haftungsausschlussklausel im Impressum nicht aus, um sich ernsthaft von den Inhalten im RSS-Feed zu distanzieren. Ebenso lasse die fehlende Kenntnis von der konkreten Rechtsverletzung die Haftung nicht entfallen, da es im Rahmen der Störerhaftung weder darauf ankomme, ob der Webseitenbetreiber die Tatbestandsmäßigkeit und Rechtswidrigkeit begründenden Umstände gekannt habe noch ob ihn Verschulden in Form von Vorsatz oder Fahrlässigkeit treffe. Störer sei nämlich jeder, der in irgendeiner Weise willentlich und adäquat kausal an der Herbeiführung der rechtswidrigen Beeinträchtigung mitgewirkt habe. Während die Rechtsverletzung bei der persönlichkeitsrechtsverletzenden Mitteilung in der Verbreitung der Information auf der eigenen Webseite liege, greife der Webseitenbetreiber bei der Veröffentlichung eines urheberrechtlich geschützten Bildes in das dem Urheber ausschließlich zugewiesene Recht der öffentlichen Zu-

gänglichmachung ein. Zudem habe er als Betreiber der Webseite selbst Einfluss auf die Beiträge nehmen können, sodass es ihm möglich gewesen wäre, die rechtswidrige Handlung zu verhindern.

Schließlich werde die Haftung auch nicht dadurch beschränkt, dass Diensteanbieter im Falle der Durchleitung und Speicherung fremder Informationen für Rechtsverletzungen nur eingeschränkt haften (vgl. §§ 8 bis 10 TMG). Erstens greifen die Privilegierungen nicht für Unterlassungsansprüche ein und zweitens handele es sich nicht um fremde Informationen, sondern um zu eigen gemachte Inhalte des Webseitenbetreibers. Er müsse daher für den Content des RSS-Feeds in gleicher Weise wie für eigene Inhalte einstehen und hafte daher auch für etwaige Rechtsverletzungen, die durch den Feed verursacht würden.

III. Unterschied zum Forenbetreiber?

Bemerkenswert ist an den Entscheidungen des LG Berlin vor allem die Abgrenzung zwischen der Einbindung eines RSS-Feeds auf der einen und dem Betrieb eines Online-Forums auf der anderen Seite: Während sich ein Webseitenbetreiber, der fremde RSS-Feeds in seine Onlinepräsenz einbindet, nach Meinung des Gerichts die Inhalte des RSS-Feeds zu eigen macht, kann nach allgemein anerkannter Auffassung ein Zu-eigen-machen von fremden Informationen in einem Forum nicht ohne weiteres angenommen werden. Forenbetreiber stellen ihren Nutzern lediglich eine Plattform zur Verfügung, auf der sich diese zu verschiedenen Themen äußern können. Sie stellen also lediglich die technischen Mittel bereit, um Dritten einen freien Meinungs austausch zu ermöglichen. Zwar leistet auch der Forenbetreiber durch die bloße Eröffnung eines Forums einen willentlichen und ursächlichen Beitrag zur Rechtsverletzung. Allerdings ist es ihm wirtschaftlich und technisch nicht zumutbar, jeden einzelnen Beitrag auf potentielle Rechtsverletzungen hin zu überprüfen, sodass eine Haftung als Störer in der Regel daran scheitert. Erst ab dem Zeitpunkt, ab dem der Betreiber eines Meinungsforums positive Kenntnis von einem unschwer zu erkennenden Rechtsverstoß hat, ist eine Störerhaftung grundsätzlich möglich.

Auf den ersten Blick erscheint es verwunderlich, dass die Rechtslage bei der Einbindung von RSS-Feeds anders zu beurteilen sein soll. Vor allem ist die Ansicht des Gerichts kritisch zu hinterfragen, dass sich der Webseitenbetreiber die Inhalte des RSS-Feeds zu eigen machen soll. Aus der bloßen Einbindung des RSS-Feed in den eigenen Content kann nämlich nicht automatisch der Schluss gezogen werden, dass sich der Webseitenbetreiber mit den Inhalten identifiziert. Hierfür spricht zunächst, dass in aller Regel offensichtlich ist, dass die Inhalte nicht vom Webseitenbetreiber selbst stammen. Zudem scheint fragwürdig, ob ähnliche Kriterien, wie die, die nach Ansicht des BGH in der „Chefkoch-Entscheidung“ (Urteil vom 12. November 2009 – I ZR 166/07) für ein Zu-eigen-machen sprachen, auch im vorliegenden Fall gegeben sind: So

wurde in dem vom BGH zu entscheidenden Fall jedes Foto mit dem eigenen Emblem von chefkoch.de (der Kochmütze) versehen, der ursprüngliche Verfasser wurde an keiner Stelle hervorgehoben und chefkoch.de hat sich sämtliche Rechte bezüglich der Vervielfältigung und Weitergabe der Fotos an Dritte einräumen lassen. Zwar sind diese Aspekte nicht zwingend verallgemeinerungsfähig; die ausführliche Auseinandersetzung des BGH mit dieser Frage lässt aber die Schlussfolgerung zu, dass ein Zu-eigen-machen von fremden Inhalten nicht ohne konkrete Anhaltspunkte angenommen werden kann. Außer der bewussten Einbindung des RSS-Feeds auf der eigenen Seite bestehen in den zu betrachtenden Fällen keine besonderen Anhaltspunkte, die für ein Zu-eigen-machen der Inhalte sprechen.

Diese Vorgehensweise scheint insbesondere deshalb fragwürdig, weil das Gericht den Rechteinhabern auch ohne diesen Kunstgriff einen Unterlassungsanspruch hätte zuerkennen können. Unabhängig von einem Zu-eigen-machen der Inhalte, welches bei konsequenter Anwendung der bisherigen Rechtsprechung ohnehin eine täterschaftliche Haftung hätte auslösen müssen, sind nämlich zumindest die Voraussetzungen einer Störerhaftung gegeben: Durch die Einbindung des RSS-Feeds hat der Webseitenbetreiber einen willentlichen Beitrag gesetzt, der ursächlich für die Rechtsverletzung ist. Denn mit der Einbindung auf seiner Webseite verbreitet er die Inhalte bzw. macht sie öffentlich zugänglich. Hinsichtlich des Umfangs der Prüfungspflichten stellt sich zwar die Frage, wie es dem Betreiber der Webseite möglich sein soll, sämtliche Schlagzeilen mit Kurzbeschreibungen auf mögliche Rechtsverletzungen hin zu überprüfen. Dies gilt vor allem dann, wenn man bedenkt, dass in der Regel mehrmals täglich eine automatische Aktualisierung der Inhalte erfolgt. Das Gericht rechtfertigt eine proaktive Prüfungspflicht aber letztlich vor allem damit, dass der Webseitenbetreiber – im Gegensatz zu einem Forenbetreiber – die Veröffentlichung des über den RSS-Feed bezogenen Beitrags auf seiner eigenen Internetseite selbst veranlasst hat. Er mache sich also gezielt Informationen einer bestimmten Quelle zu Nutzen; der Forenbetreiber stelle dagegen lediglich die technischen Mittel für einen freien Meinungs austausch einem ihm (üblicherweise) unbekanntem Dritten zur Verfügung. Deswegen könne von ihm mehr verlangt werden als von einem Forenbetreiber. Diese Sichtweise kann durchaus überzeugen und rechtfertigt letztlich auch die Differenzierung zwischen dem Betrieb eines Internetforums und der Einbindung eines fremden RSS-Feeds auf einer Webseite.

IV. Fazit

Die Entscheidung, Webseitenbetreiber eine vorherige Prüfungspflicht aufzubürden, führt dazu, dass der Nutzen von RSS-Feeds – sämtliche Informationen einer bestimmten Quelle in Echtzeit weiterleiten zu lassen – zunichte gemacht wird. Zumal der Webseitenbetreiber sich nicht darauf berufen kann, der RSS-Feed stamme von einer renommierten Quelle. Da es Webseitenbetreibern jedoch

wohl kaum möglich sein dürfte, sämtliche fremde Inhalte in RSS-Feeds vor Veröffentlichung auf der eigenen Seite auf rechtsverletzende Inhalte hin zu überprüfen, läuft es letztendlich darauf hinaus, dass auf die Einbindung fremder RSS-Feeds gänzlich verzichtet werden sollte. Vom Ergebnis her scheint dies auch angemessen: Der Sinn und Zweck von RSS-Feeds besteht darin, Nutzer schnell und effektiv über Änderungen von Webseiten, insbesondere von Nachrichtenseiten, wo sich die Schlagzeilen fast stündlich ändern, zu informieren. Nicht beabsichtigt ist dagegen, dass Webseitenbetreiber die RSS-Feeds Dritter dazu benutzen, das eigene Content-Angebot aufzuwerten, um dadurch mehr Clicks auf der eigenen Seite zu erzeugen. RSS-Feeds sind auch nicht dazu da, fremden Webseiten kostenlose Inhalte zu liefern. Hochschulen sollten vor dem Hintergrund dieser Entscheidungen in jedem Fall davon Abstand nehmen, auf der hochschuleigenen Webseite RSS-Feeds von Dritten einzubinden. Das AG Hamburg hatte sogar in einem ähnlichen Fall eine täterschaftliche Haftung angenommen und neben dem Unterlassungsanspruch auch einen Schadensersatzanspruch zugiebilligt, so dass das Haftungsrisiko bisher nicht abzuschätzen ist.

Rechtliche Aspekte sozialer Netzwerke

Teil 2: Facebook und Datenschutz – Gefällt mir (nicht)

von Ass. iur. Johannes Franck

Seit einiger Zeit werden Vor- und Nachteile der sozialen Netzwerke in Deutschland kontrovers diskutiert. Im Mittelpunkt dieser Diskussion steht das hierzulande populärste soziale Netzwerk Facebook. Seit einer im August 2011 verkündeten Entscheidung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) besteht nun bei einigen Hochschulen konkreter Handlungsbedarf.

I. Einleitung

Viele Unternehmen, aber zunehmend auch öffentliche Stellen, nutzen soziale Netzwerke. Der privaten Wirtschaft dienen derartige Plattformen zu Marketingzwecken, aber auch Behörden setzen immer mehr auf Öffentlichkeitsarbeit und politische Kommunikation via Facebook. Dies soll zum einen dazu führen, dass sich die Bürgerbeteiligung an demokratischen Entscheidungsprozessen verbessert, zum anderen sollen Einblicke in die Arbeit von Behörden mehr Transparenz bieten und dadurch Verständnis bei Bürgern hervorrufen.

Zu diesem Zweck betreiben viele Unternehmen, Behörden und auch Hochschulen sogenannte Fanpages. Viele Betreiber verbinden außerdem ihre Webseiten über Social Plugins mit Facebook. So ist der Like Button samt hochgestrecktem Daumen zum Markenzeichen von Facebook avanciert.

In der juristischen Debatte stehen neben urheber- und arbeitsrechtlichen Fragestellungen (s. dazu DFN-Infobriefe 5/2011 und 7/2011) insbesondere datenschutzrechtliche Probleme im Fokus. Facebook hat im Laufe der letzten Monate verschiedene technische Innovationen in sein Netzwerk implementiert, die seither unentwegt Schlagzeilen machen. Datenschutzrechtlich relevant sind insbesondere die Dienste „Social Plugins“ und „Fanpages“ sowie das Statistik-Tool „Facebook Insights“.

II. Technischer Hintergrund

1. Social Plugins

Über ein sogenanntes Social Plugin kann jeder Webseitenbetreiber eine bestimmte Anwendung in sein eigenes Internetportal integrieren. Die bekanntesten Facebook-Plugins sind der Activity Feed, der Like Button, die Like Box und die Facebook Comment Box. Mithilfe des Like Buttons kann ein Nutzer gegenüber seinen Facebook-Kontakten bekunden, dass ihm eine bestimmte Webseite oder ein darauf veröffentlichter Text, ein Bild oder ähnliches gefällt.

Technisch funktioniert dies folgendermaßen: Durch die Integration des Like Buttons auf einer Webseite wird ein JavaScript von einem Facebook-Server in den Quellcode der eigenen Webseite eingebunden. Vom Browser des Seitenbesuchers (sog. Client bzw. Nutzer) wird

dieses JavaScript dann ebenfalls abgerufen und ausgeführt. Sofern man gleichzeitig bei Facebook eingeloggt ist, werden beim Laden des Scripts diverse Informationen an Server der Facebook Inc. in den USA übermittelt, darunter die Adresse der besuchten Webseite, Datum und Uhrzeit des Besuchs, der verwendete Browser und das Betriebssystem sowie die IP-Adresse des Nutzers. Gleichzeitig wird bei jedem Aufruf der Webseite ein Facebook-Cookie namens „datr“ gesetzt, welcher zwei Jahre gespeichert bleibt. Die Übermittlung dieser Daten geschieht unabhängig davon, ob man den Like Button tatsächlich betätigt.

Wenn man während des Browsens auf einer mit einem Social Plugin versehenen Webseite nicht gleichzeitig bei Facebook eingeloggt ist, werden die Daten durch den zuvor gesetzten Cookie später beim Wiedereinloggen an Facebook übertragen und können sodann dem jeweiligen Nutzer zugeordnet werden.

Facebook kann auf diese Weise beobachten, welche Webseiten seine Nutzer besuchen, sofern dort der Like Button eingebunden ist. Im Gegensatz zu andern Statistik-Servern (wie z. B. Google Analytics), von denen grundsätzlich nur „allgemeine Informationen“ gesammelt werden, kann Facebook mithilfe der hinterlegten Nutzerinformationen die erhobenen Daten einer realen Person zuordnen. Das bedeutet, dass Facebook eine umfassende und personalisierte Profilbildung vornehmen kann.

Der Webseitenbetreiber hat bei dem gesamten Vorgang keine Eingriffs- und Kontrollmöglichkeiten.

2. Fanpages

Fanpages hingegen sind Webseiten, die direkt in ein soziales Netzwerk eingebunden sind. Sie werden von Unternehmen, Organisationen oder öffentlichen Stellen eingerichtet, um über ihre Produkte, Dienstleistungen oder sonstige Anliegen zu informieren. Die Inhalte der Fanpages werden ausschließlich von den Anbietern verwaltet, Facebook stellt lediglich die Infrastruktur zur Verfügung. Selbst wenn die Seiten meist durch jedermann aufrufbar sind, stehen der Großteil ihrer Funktionen und Informationen nur registrierten Facebook-Nutzern zur Verfügung. Der Nutzer kann „Fan“ einer solchen Seite werden und wird sodann regelmäßig über Neuigkeiten des Anbieters

informiert. Daneben ist für die befreundeten Facebook-Kontakte sichtbar, dass der Nutzer sich für den Anbieter der Fanpage interessiert.

3. Reichweitenanalyse

Eine Reichweitenanalyse ist die qualifizierte Rückmeldung an den Betreiber hinsichtlich der Nutzung eines Internetangebots. Der Dienst Facebook Insights stellt den Betreibern von Fanpages und Webseiten mit Social Plugins detaillierte Statistiken über Nutzerverhalten, Demografie etc. kostenlos zur Verfügung. Hieraus wird ersichtlich, wie viele Personen welche Aktionen auf der Seite getätigt haben. Ergänzt werden diese Angaben durch demografische Daten wie Alter, Geschlecht und Herkunft der Nutzer. Ferner werden dabei IP-Adressen der Seitenbesucher übermittelt. Diese Datensätze hat Facebook zuvor durch die oben beschriebene Zuordnung der Besucher zu den einzelnen Facebook-Nutzerprofilen gewonnen.

III. Stellungnahme des ULD vom 19. August 2011

Mit Pressemitteilung vom 19. August 2011 hat das ULD alle Webseitenbetreiber in Schleswig-Holstein dazu aufgefordert, bis zum 30. September 2011 ihre Fanpages bei Facebook sowie alle Social Plugins von Ihren Webseiten zu deaktivieren oder zu entfernen.

Nach Auffassung des ULD verstoßen die Dienste Like Button und Fanpages gegen das deutsche und europäische Datenschutzrecht. Denn sowohl die mit deren Nutzung verbundene Weitergabe von Daten an die Facebook Inc. in den USA als auch die Reichweitenanalyse seien rechtswidrig.

Stellen, die der Aufforderung nicht Folge leisten, müssen mit Bußgeldern von bis zu 50.000 Euro rechnen. In der Zwischenzeit sind erste Abmahnungen durch das ULD ausgesprochen worden, darunter gegenüber der Staatskanzlei des Ministerpräsidenten von Schleswig-Holstein. Sowohl öffentliche Stellen als auch Unternehmen haben mittlerweile Konsequenzen gezogen und ihre Social Plugins entfernt oder sich gar komplett aus Facebook zurückgezogen.

IV. Stand der rechtlichen Diskussion

Das Kammergericht hat mit Beschluss vom 29.04.2011 (Az. 5 W 88/11) entschieden, dass die Verwendung des Facebook Like Buttons auf der Internetseite eines Onlinehändlers wettbewerbsrechtlich unbedenklich ist. Zu den datenschutzrechtlichen Fragen hat sich das Gericht dabei allerdings nicht geäußert.

1. Datenschutzrechtliche Verantwortlichkeit

Einigkeit herrscht darüber, dass Facebook für eigene Datenschutzverstöße als Diensteanbieter im Sinne des Te-

lemediengesetzes (TMG) bzw. verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes (BDSG) bzw. des jeweiligen Landesdatenschutzgesetzes (LDSG) datenschutzrechtlich verantwortlich ist.

Da sich die Aufforderung des ULD allerdings nicht gegen Facebook, sondern gegen die Seitenbetreiber richtet, ist fraglich, ob auch diese Verantwortlichem im Sinne des BDSG bzw. TMG sind.

Die Aggregation der Daten erfolgt nur durch Facebook. Die Vorschriften des TMG treffen den Betreiber der Fanpage also nur dann, wenn er selbst Diensteanbieter im Sinne des TMG ist. Diese Frage ist höchst umstritten.

Einige sind der Auffassung, dass zumindest bei den Fanpages ausschließlich Facebook Diensteanbieter sei. Dafür spricht, dass die Fanpage derart fest in das soziale Netzwerk eingebunden ist, dass der Betreiber der Fanpage nach außen nicht mehr zwangsläufig als Diensteanbieter wahrgenommen wird.

Nach der Legaldefinition des § 2 Abs. 1 TMG kann allerdings auch derjenige Diensteanbieter sein, der den Zugang zur Nutzung von Telemedien vermittelt. Der ULD argumentiert, dass der Webseitenbetreiber dem Nutzer die Nutzung des sozialen Netzwerks dadurch vermittelt, dass er das JavaScript auf seiner Fanpage einbindet bzw. die Fanseite bei Facebook präsentiert. Der Seitenbetreiber sei daher Diensteanbieter und damit verantwortlich i. S. d. TMG. Nach dieser Auffassung initiieren die in Frage stehenden Fanpagebetreiber sowie Betreiber externer Webseiten mit eingebundenen Social Plugins die Datenweitergaben an Facebook und seien daher jeweils selbst Diensteanbieter und damit Verantwortliche im Sinne des TMG für die hierbei vorgenommene Verarbeitung personenbezogener Daten.

Neben dem klaren Gesetzeswortlaut des § 2 TMG spricht dafür auch Art. 2 d) der EU-Datenschutzrichtlinie (RiLi 95/46/EG). Danach ist derjenige verantwortlich, der über die Zwecke und Mittel der Datenverarbeitung entscheidet. Es kommt mithin nicht darauf an, ob jemand tatsächlich personenbezogene Daten erhebt und verarbeitet, sondern nur, ob er die Verfügungsmacht über die Daten besitzt. Da das Erheben und Speichern dieser Daten erst durch die vom Seitenbetreiber vorgenommene Einbindung des Social Plugins bzw. die Erstellung der Fanpage ermöglicht wird, lässt sich dessen datenschutzrechtliche Verantwortlichkeit bejahen.

Der Anbieter ist demnach wie ein „normaler“ Webseitenbetreiber zu behandeln, der seine Webseite von der Plattform Facebook hosten lässt. Als Adressat möglicher Maßnahmen kommt demnach neben Facebook auch der Fanpage-Betreiber in Betracht. Auf Grund der praktischen Probleme im Zusammenhang mit einem Vorgehen gegen das US-amerikanische Unternehmen, erscheint dies sogar wahrscheinlich.

2. Datenschutzverstöße

Das ULD und weitere Datenschutzexperten werfen Facebook zahlreiche Datenschutzverstöße vor. Hauptkritikpunkt ist derzeit die beschriebene Reichweitenanalyse.

Sowohl auf den Fanpages als auch beim Einbinden von Social Plugins findet durch den Dienst Facebook Insights die oben erläuterte Reichweitenanalyse statt. Dabei werden personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG erhoben. Eine Verarbeitung von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG nur dann zulässig, wenn dies ausdrücklich gesetzlich erlaubt ist oder der Betroffene in die Datenverarbeitung eingewilligt hat.

§ 4a BDSG setzt voraus, dass die Einwilligung auf der freien Entscheidung des Betroffenen beruht. Der Betroffene muss außerdem über den vorgesehenen Zweck der Datenverarbeitung aufgeklärt werden. Dies bedeutet, dass der Betroffene darüber zu informieren ist, auf welche personenbezogenen Daten sich die Einwilligung bezieht und was mit diesen Daten geschehen soll. Eine pauschale Erklärung durch den Betroffenen, dass er mit jeder weiteren Verarbeitung seiner Daten einverstanden sei, genügt hierfür nicht.

Im Zuge der Registrierung bei Facebook muss jeder Nutzer bestätigen, dass er die nach § 13 TMG gesetzlich vorgesehene Datenschutzerklärung akzeptiert. Diese Datenschutzerklärung ist äußerst kompliziert und zudem nur in englischer Sprache verfügbar. Allein deswegen ist bereits zweifelhaft, ob sie überhaupt mit deutschem AGB-Recht (§§ 305 ff. BGB) vereinbar ist.

Nach Ansicht von Facebook erteilt der Nutzer durch seine Bestätigung gleichzeitig eine Einwilligung zur Datenerhebung für sämtliche Facebook-Dienste.

Dass dieses Vorgehen den Anforderungen an eine Einwilligung im Sinne des § 4a BDSG genügt, darf bezweifelt werden. Denn zum einen fehlt es schon an einer eindeutigen Willensbekundung des Nutzers. Zum anderen mangelt es an der erforderlichen Transparenz hinsichtlich Art, Umfang und Dauer der Datenverarbeitung sowie des Zwecks der Datenverwendung. Schließlich erfährt der Nutzer auch nicht, wohin die erhobenen Daten übermittelt werden.

Dieser Ansicht folgend müsste mangels Einwilligung also ein gesetzlicher Erlaubnistatbestand vorliegen.

§ 15 Abs. 1 TMG erlaubt das Erheben und Verwenden von sogenannten Nutzungsdaten: Dies sind neben Merkmalen zur Identifikation des Nutzers auch Informationen über Beginn und Ende sowie den Umfang der Nutzung des Mediums. Allerdings dürfen diese Daten nur erhoben werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Die Erhebung der oben genannten Daten geht jedoch ersichtlich über das zur Inanspruchnahme des Dienstes oder zur Abrechnung erforderliche Maß hinaus, sodass § 15 Abs. 1 TMG die Datenverarbeitung nicht rechtferti-

gen kann.

Eine Datenverarbeitung zur Erstellung von Reichweitenanalysen ist grundsätzlich zulässig. § 15 Abs. 3 S. 1 TMG sieht vor, dass der Anbieter eines Telemediendienstes bestimmte Daten für Zwecke der Werbung, Marktforschung oder Optimierung des Dienstes erheben und verwenden darf, sofern der Nutzer dem nicht widerspricht. Nach § 15 Abs. 3 S. 2 TMG muss der Anbieter den Nutzer allerdings im Rahmen der Datenschutzerklärung auf sein Widerspruchsrecht hinweisen.

Da die Fanpagebetreiber sowie Webseitenbetreiber mit Social Plugins – wie oben erläutert – datenschutzrechtlich verantwortlich sind, sind diese neben Facebook selbst verpflichtet, gegenüber ihren Nutzern auf diese Widerspruchsmöglichkeit hinzuweisen. Für die Seitenbetreiber ist es allerdings derzeit technisch überhaupt nicht möglich, eine solche Widerspruchserteilung in ihr Angebot einzubinden. Daher liegt zwangsläufig ein Verstoß gegen § 15 Abs. 3 TMG durch die Seitenbetreiber vor.

Darüber hinaus regelt § 15 Abs. 3 S. 3 TMG, dass die gebildeten Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen. Gerade dies geschieht jedoch bei Facebook Insights. Denn das Nutzungsprofil, das zunächst unter Pseudonym erstellt wurde, wird bei der Reichweitenanalyse mit den Kontoinformationen des jeweiligen Nutzers verknüpft. Im Nutzerkonto sind Name, Geschlecht, Alter sowie gegebenenfalls Bilder und andere Informationen des Nutzers hinterlegt. Die Facebook-Nutzungsbedingungen verbieten, dass sich Nutzer unter einem Pseudonym oder einem falschen Namen anmelden. Sofern der Nutzer diese Nutzungsbedingungen einhält, ist daher für Facebook ohne weiteres möglich, die Identität des Nutzers herauszufinden. Es liegt mithin ein Verstoß gegen das Trennungsgebot nach § 15 Abs. 3 TMG vor.

Neben der Rechtswidrigkeit der Reichweitenanalyse werden Facebook von Datenschützern zahlreiche weitere Datenschutzverstöße vorgeworfen. So wird moniert, dass ein Verstoß gegen Art. 5 Abs. 3 der E-Privacy-Richtlinie (RL 2002/58/EG) vorliege. Dort ist geregelt, dass beim Setzen von Cookies, die nicht zum Betrieb der Seite unbedingt erforderlich sind, eine vorherige Einwilligung eingeholt werden muss. Der Facebook-Nutzer wird über das Setzen des Cookies „datr“ bei den Social Plugins weder in Kenntnis gesetzt noch wird ihm ein Widerspruchsrecht eingeräumt, weswegen es hier an einer Einwilligung fehlt, zumal Cookies auch ohne eine Anmeldung bei Facebook gesetzt werden.

Darüber hinaus entspricht die derzeitige Gestaltung der Angebote nach Auffassung von Datenschützern weder den Anforderungen an die Datensicherheit nach § 13 Abs. 4 TMG noch denen eines ordnungsgemäßen Impressums nach § 5 Abs. 1 TMG bzw. § 55 Rundfunkstaatsvertrag.

3. Kritik am Vorgehen des ULD

Viele kritische Stimmen haben sich gegen das Vorgehen des ULD ausgesprochen. Zunächst wird bemängelt, dass dadurch vor allem kleine und mittelständische Unternehmen und Behörden „kriminalisiert“ werden. Adressat der Kritik solle stattdessen Facebook selbst sein. Darüber hinaus wird von Kritikern darauf hingewiesen, dass ein Großteil der Besucher auf Ihren Webseiten zumindest mittelbar über Facebook komme und daher bei einer Verbannung dieser Dienste mit immensen wirtschaftlichen Einbußen zu rechnen sei. Weiterhin wird bemängelt, dass Wettbewerbsverzerrungen entstünden, wenn einige Bundesländer einzeln vorgingen und daher nur bestimmte Unternehmen und Behörden betroffen seien. Außerdem wird argumentiert, dass hierdurch sowohl Unternehmen als auch Bürger bevormundet würden.

Schließlich bestehen erhebliche Zweifel an der Zuständigkeit des ULD für die Verhängung von Bußgeldern für Datenschutzverstöße nach § 16 TMG. Zuständige Behörde sei vielmehr das Landesinnenministerium. Zu diesem Ergebnis kommt auch ein kürzlich veröffentlichtes Gutachten des wissenschaftlichen Dienstes des Deutschen Bundestages.

V. Praktische Hinweise

Internetnutzer können die Datenübertragung durch den Like Button und Social Plugins auf Seiten außerhalb von Facebook deaktivieren. Dazu müssen sie allerdings in ihrem Browser Filter-Erweiterungen installieren, wie sie auch zur Blockade von Werbeanzeigen verwendet werden (z. B. „Facebook Blocker“ oder „Adblock Plus“). Heise Online hat die sogenannte „2-Click-Lösung“ vorgestellt, die sich zunehmender Beliebtheit erfreut. Hierbei wird der Like Button und die Datenübertragung an Facebook nicht bereits mit dem Aufrufen der Webseite, sondern erst nach einem Klick auf den Button aktiviert. Eine andere, wenn auch wenig praktikable Möglichkeit ist es, Facebook stets mit einem anderen Browser aufzurufen, als alle anderen Webseiten.

VI. Fazit

Es bleibt festzuhalten, dass die Entscheidungen des ULD gemäß § 3 LDSG SH nur für die Einrichtungen Rechtswirkung entfalten, die unter das schleswig-holsteinische Datenschutzrecht fallen. Die Datenschutzbeauftragten von Niedersachsen und Hamburg haben allerdings bereits kurze Zeit später angekündigt, dass sie die Rechtslage ähnlich bewerten. Insofern ist nicht auszuschließen, dass demnächst auch in anderen Ländern ähnliche Entscheidungen ergehen.

Das ULD beschränkt seine Stellungnahme auf den Branchenprimus Facebook. Ähnliche datenschutzrechtliche Probleme gelten aber auch für andere soziale Netzwerke wie XING und das noch im Aufbau befindliche Angebot

Google Plus. Auf Grund der aktuellen Debatte zeigte sich Facebook gegenüber den deutschen Behörden zuletzt gesprächsbereit. Was sich hier tun wird, bleibt abzuwarten.

Selbst wenn das ULD für die Verhängung der Bußgelder nicht zuständig sein sollte, lässt sich daraus nicht ableiten, dass Verstöße nicht von der stattdessen zuständigen Stelle verfolgt und geahndet werden.

Die Entscheidung des ULD ist auf teilweise heftige Kritik gestoßen und die Rechtslage ist mangels gerichtlicher Entscheidungen weiterhin unklar. Dass viele soziale Netzwerke in einer datenschutzrechtlichen Grauzone agieren, dürfte aber offensichtlich sein. Ob die Hochschulen ihre Fanpages und Like Buttons entfernen, bleibt ihnen überlassen und sollte sorgsam abgewogen werden. Denn wer in vorauseilendem Gehorsam Fanpages löscht, muss damit leben, dass dadurch sämtliche „Fans“ verloren gehen. Sollte Facebook einlenken und Änderungen derart vornehmen, dass die Dienste datenschutzkonform werden, müssten diese „Fans“ bei Reaktivierung der Fanpage mühsam zurückgewonnen werden.

Zumindest den Hochschulen in Schleswig-Holstein wird allerdings dringend geraten, den Forderungen des ULD Folge zu leisten.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.

DFN-Verein

Alexanderplatz 1, 10178 Berlin

E-Mail: DFN-Verein@dfn.de

Redaktion

Forschungsstelle Recht im DFN, ein Projekt des DFN-Vereins an der WESTFÄLISCHE WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung, unter Leitung von Prof. Dr. Thomas Hoeren

Leonardo-Campus 9

D-48149 Münster

E-Mail: recht@dfn.de

Nachdruck sowie Wiedergabe in elektronischer Form, auch auszugsweise, nur mit schriftlicher Genehmigung des DFN-Vereins und mit vollständiger Quellenangabe.