THOMAS HOEREN*

What's up? Trends im Internetrecht

Gernot Schulze ist einer meiner „Heroes" in der Welt des Internetrechts. In seiner ruhigen, bedächtigen Weise hat er die verschiedenen Kontroversen rund um die Digitalisierung im Urheberrecht vorbildhaft durchdacht und gemeistert.[1] Es freut mich, ihn zum runden Geburtstag durch einige Überlegungen über das Internetrecht zu ehren.

Das Internet verändert sich derzeit grundlegend. Ältere werden noch die Worte von John Perry Barlow im Ohr haben, der in seiner Unabhängigkeitserklärung für das Cyberspace[2] schon 1996 visionär formuliert hatte:

„Regierungen der Industriellen Welt, ihr müden Riesen aus Fleisch und Stahl, ich komme aus dem Cyberspace, dem neuen Zuhause des Geistes. Als Vertreter der Zukunft bitte ich euch aus der Vergangenheit, uns in Ruhe zu lassen. Ihr seid nicht willkommen unter uns. Ihr habt keine Souveränität, wo wir uns versammeln."

Von diesem Pathos ist heute kaum etwas geblieben. Nicht ohne Grund dümpeln die früher hochgefeierten Piraten bei Wahlen am Existenzminimum.[3] Die Zeiten, in denen Zehntausende gegen Beschränkungen des Internets demonstrierten,[4] sind lange vorbei.

I. Facebook-Bashing und der Tugendfuror

Das Netz galt Jahrzehnte als im Kern nicht regelbar und war damit Quelle der Meinungsfreiheit auch und gerade in Regimen wie in China oder Russland.[5] Heute kann jeder Politiker und jeder Journalist Facebook lesen und sich über extreme Postings von links und rechts aufregen.[6] Bedingt durch den derzeitigen

---

* Prof. Dr. iur., Professor an der Westfälischen Wilhelms-Universität Münster.

[1] Als kleines Beispiel *Schulze* ZUM 2000, 432.

[2] *Barlow,* A Declaration of the Independence of Cyberspace v. 8.2.1996, abrufbar unter: Electronic Frontier Foundation, https://www.eff.org/de/cyberspace-independence, zuletzt abgerufen am 22.3.2017.

[3] S. zum Thema den Schwerpunkt der TAZ v. 10./11.9.2016, abrufbar unter: https://taz.de/Ausgabe-vom-10/11-Sept-2016/!162844/, zuletzt abgerufen am 21.4.2017.

[4] Selbst in Münster waren mehr als 1000 Demonstranten gegen ACTA, s. dazu http://www.wn.de/Muenster/2012/02/Weltweiter-Protest-gegen-Acta-auch-in-Muenster-Tausende-demonstrierten-auf-dem-Ludgeriplatz, zuletzt abgerufen am 21.4.2017.

[5] *Arifon,* Hermès – La Revue 2012, 160ff.

[6] Bevor ich selbst Gegenstand heftiger Hass-Attacken werde, sei darauf verwiesen, dass es natürlich bei Facebook & Co. Fälle gibt, die eindeutig einer strafrechtlichen Verfolgung etwa wegen

„Tugendfuror"[7], in dem „man" weiß, was „man" im Netz sagen darf, erschallt der Ruf nach Meinungskontrolle insbesondere bei den sozialen Netzwerken. Die Tageszeitungen reagieren darauf und schließen ihre Kommentarrubriken. Die Politik macht die derzeitige Welle des Facebook-Bashings mit, in dem sie kurz vor dem Bundestagswahlkampf Schnellgesetze wie das Netzwerkdurchsetzungsgesetz[8] unter das Volk bringt.[9] Anmerkungen, dass im Netz zum Beispiel eine Sperrung von Zugängen technisch gar nicht möglich ist, entgegnet die Rechtsprechung nur mit dem ironischen Hinweis darauf, das gehe sie nichts an und müsse im Einzelfall anhand der Zumutbarkeit geprüft werden.[10]

II. Die Haftung der Intermediäre

Immer mehr erweist es sich als Fluch, dass man im Internet bei der Durchsetzung von Immaterialgüterrechten Probleme vor allem bei der Durchsetzung und Vollstreckung von Unterlassungsansprüchen hat. Insbesondere wenn sich der Schuldner in eine Vollstreckungsoase[11] flüchtet, ist die stark an Staatsgrenzen orientierte Rechtsordnung der ubiquitären Macht des Internets hilflos ausgeliefert. In der Not frisst der Teufel Fliegen und macht die Intermediäre für solche Vollstreckungsprobleme verantwortlich. Denn Zahlungsdienste, Hosts oder Linksetzer sind einfacher greifbar und wirtschaftlich oft potenter. Gerade im Zusammenhang mit immaterialgüterrechtlichen Auskunftsansprüchen steht die Frage der Auskunftspflicht von Kreditinstituten im Interesse der Rechtsinhaber („Follow the money"). Der EuGH[12] hat jetzt entschieden, dass einer solchen Pflicht das Bankgeheimnis nicht entgegensteht. Der nationale Gesetzgeber dürfe nicht vorsehen, dass ein Bankinstitut unbegrenzt und bedingungslos eine Auskunft über Namen und Anschrift eines markenrechtsverletzenden Kontoinhabers unter Berufung auf das Bankgeheimnis verweigert.[13] Ähnlich werden die Access Provider in Anspruch genommen, auch wenn eine Sperrung des Internets schon aus technischen Gründen kaum möglich ist. Der BGH[14] verlangt, dass Access Provider ihre Systeme so einrichten müssen, dass sie Filter und Sperren

---

Volksverhetzung (§ 130 StGB) bedürfen. Nur sind solche Straftatbestände nicht einfach zu konturieren; nicht alles, was an Facebook-Hostings verärgert, ist automatisch strafbar.

[7] Der Begriff stammt von Altbundespräsident *Joachim Gauck*.

[8] Referentenentwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), abrufbar unter: https://netzpolitik.org/wp-upload/2017/03/1703014_NetzwerkDurchsetzungsG.pdf, zuletzt abgerufen am 21.4.2017. Dazu kritisch *Härting*, CR Online, abrufbar unter: http://www.cr-online.de/blog/2017/03/14/kurzer-prozess-fuer-die-meinungsfreiheit-entwurf-eines-netzwerkdurchsetzungsgesetzes/, zuletzt abgerufen am 13.4.2017.

[9] Dazu auch *Galetzka/Krätschmer* MMR 2016, 518.

[10] Vgl. BGH MMR 2016, 188 (Ls. 3); kritische Betrachtung der Einführung von Internetsperren in *Heidrich/Heymann* MMR 2016, 379ff.

[11] Dazu *Hoeren* MMR 2016, 518.

[12] EuGH C-580/13, ECLI:EU:C:2015:485 = GRUR 2015, 894 mAnm *Kamlah – Coty Germany*.

[13] BGH GRUR 2016, 497 – *Davidoff Hot Water II*.

[14] BGH MMR 2016, 188; MMR 2016, 616.

vorsehen. Der BGH hat zwar einige Vorbedingungen für eine solche Filterpflicht aufgestellt, diese aber nicht vollständig abgelehnt. Er verlangt vom Rechteinhaber, dass er zunächst gegen den unmittelbaren Verletzer und gegen den Host Provider vorgeht. Erst dann soll der Access Provider haften. Das Gericht begründet damit eine Subsidiarität der Störerhaftung im Sinne der französischen Kaskadenhaftung.[15]

Zu den neu ins Visier genommenen Intermediären zählt auch der WLAN-Betreiber. Für solche sieht der EuGH[16] vor, dass dem geschäftlich tätigen Anschlussinhaber eines kostenlosen WLAN-Netzes die Pflicht zur Sicherung des WLAN durch ein Passwort auferlegt werden kann, um so Urheberrechtsverletzungen vorzubeugen.[17] Dies bringe die grundrechtlich geschützten Interessen beider Parteien in Einklang.[18] Hiermit stimmt auch der Wortlaut des § 8 TMG n.F. überein, der mit Wirkung zum 27. Juli 2016 durch das 2. Gesetz zur Änderung des Telemediengesetzes[19] geändert wurde und einen 3. Absatz erhielt. In diesem wird die Anwendbarkeit der Grundsätze des § 8 Abs. 1, Abs. 2 TMG auch auf Diensteanbieter nach § 8 Abs. 1 TMG, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen, ausgeweitet. Das Gesetz soll allerdings insoweit noch einmal geändert werden, um in § 7 Abs. 4 TMG eine Pflicht von WLAN-Betreibern zur Sperrung im Rahmen der Zumutbarkeit und Verhältnismäßigkeit vorzusehen.[20]

Neuestes Opfer der Intermediär-Hatz ist der gute alte Internetlink. In seinem Beschluss[21] vom 18. November 2016 hat das Landgericht Hamburg als erstes deutsches Gericht nach der EuGH-Entscheidung[22] vom 8. August 2016 entschieden, dass in das Recht der öffentlichen Zugänglichmachung aus § 19a UrhG durch eine Verlinkung eingegriffen werden kann. Demnach haftet der Betreiber einer gewerblich betriebenen Website grundsätzlich auch ohne Kenntnis für urheberrechtsverletzende Inhalte, auf die er verlinkt. In einer solchen Verlinkung sei eine eigenständige öffentliche Wiedergabe zu sehen, durch die der Zugriff für ein neues Publikum eröffnet sei. Haften solle der Verlinkende, wenn „die Linksetzung schuldhaft in dem Sinne erfolgt, dass der Linksetzer um die Rechtswidrigkeit der verlinkten Zugänglichmachung wusste oder hätte wissen müssen." Sofern jemand mit Gewinnerzielungsabsicht handele und einen fremden Inhalt verlinke, gilt ein strengerer Verschuldensmaßstab: Ihm sei zuzumuten, „sich durch Nachforschungen zu vergewissern, ob der verlinkte Inhalt rechtmäßig zugänglich gemacht wurde."

Eine Grenze findet die Hatz nach den Intermediären aber doch noch. So hat der BGH im Afterlife-Fall das Begehren der Abmahnkanzlei Walldorf Frommer in die

---

[15] Dazu kritisch *Heidrich/Heymann* MMR 2016, 370ff.

[16] EuGH C-484/14, ECLI:EU:C:2016:689 = BeckRS 2016, 82227 – *Mc Fadden*.

[17] EuGH C-484/14, ECLI:EU:C:2016:689 = BeckRS 2016, 82227 Rn. 99f. – *Mc Fadden*.

[18] EuGH C-484/14, ECLI:EU:C:2016:689 = BeckRS 2016, 82227 Rn. 90 – *Mc Fadden*.

[19] Zweites Gesetz zur Änderung des Telemediengesetzes v. 21.7.2016, BGBl. 2016 I 1766; berechtigte Kritik üben *Conraths/Peintinger* GRUR-Prax 2016, 297.

[20] Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes TMG-Änderungsgesetz v. 23.2.2017 – Referentenentwurf des BMWi, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/E/entwurf-drittes-gesetz-zur-aenderung-des-telemediengesetzes.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 23.3.2017.

[21] LG Hamburg AfP 2017, 78.

[22] EuGH C-160/15, ECLI:EU:C:2016:644 = GRUR 2016, 1152 – *GS Media*.

Schranken gewiesen. Jene wollte dem Anschlussinhaber eine umfassende Dokumentationspflicht bezüglich der Internetnutzung seines Ehegatten oder eine regelmäßige Pflicht zur Untersuchung des Computers seines Ehegatten auferlegen. Gegenüber Erwachsenen mag die sekundäre Darlegungslast gebieten, den Namen desjenigen zu benennen, der für eine Urheberrechtsverletzung in Betracht kommt.[23] Nicht notwendig ist es aber, dass der Anschlussinhaber den PC zum Beispiel seiner Ehefrau durchsucht oder Abwesenheitslisten führt.[24]

III. M2M und Big Data

Ohnehin nimmt die Bedeutung des Internets ab. Ersetzt wird das Internet durch einen allgemeinen Schub der Digitalisierung, der Machine-to-Machine-Kommunikation (M2M) und des Internet of things (IoT). Diese Instrumente machen es viel leichter, den Konsumenten zu kontrollieren und dessen Nutzungsverhalten auszuwerten. Nicht ohne Grund entsteht parallel der Ruf nach Big Data, der geschickten Analyse großer Datenmengen. Big Data macht scheinbar anonyme Daten personenbeziehbar und unterläuft klassische Prinzipien des Datenschutzrechts wie das der Zweckbindung und der Datensparsamkeit. Deshalb wurde praktischerweise in der EU-DSGVO Big Data weitgehend freigestellt. Zwar umfasst Art. 4 Nr. 4 DSGVO auch das Profiling als Verarbeitungsvorgang. Auch verweisen Art. 5 lit. b und e der VO auf die Gebote der Datensparsamkeit und Zweckbindung. Allerdings sollen diese Grundsätze gerade nicht im Rahmen der wissenschaftlichen Forschung gelten (und solche Forschung findet nicht nur an den Universitäten statt). Damit sind weite Bereiche der Big-Data-Szene von zentralen Datenschutzgrundsätzen ausgenommen. Im Übrigen verbleibt noch Hilfe über das Pseudonymisieren, das zukünftig als Risikominimierungsmaßnahme eingestuft wird, die sowohl im Rahmen des Privacy-by-Design (Art. 25 VO) als auch als technische (Sicherheits-) Maßnahme (Art. 32 VO) verwendet werden kann. Das klassische Datenschutzrecht erweist sich als in Teilen inadäquat und ineffizient im Umgang mit Big Data. Traditionelle Denkfiguren wie der Personenbezug von Daten erweisen sich im Zeitalter der ubiquitären Verknüpfbarkeit von Daten als ebenso obsolet wie das Instrument der Zweckbindung oder der Einwilligung des Betroffenen. Hier bedarf es der zusätzlichen Einbeziehung weiterer Regulierungsansätze etwa aus dem Verbraucherschutz- und Kartellrecht, zum Beispiel des Blickes auf das Diskriminierungsverbot, der Betrachtung von Fragen der Datenqualität und -richtigkeit oder der Berücksichtigung von technischen Maßnahmen zur Transparenz von Algorithmen und Verfahren der Datenanalyse.[25]

Gleichzeitig wird die Digitalisierung ein Thema des TK-Rechts, ein Rechtsgebiet, das noch vor Jahren als tot galt. Während zwar das Rundfunkrecht gestorben

---

[23] BGH Urt. v. 30.3.2017 – I ZR 19/16.

[24] BGH WRP 2017, 448 – *Afterlife*.

[25] Verwiesen sei hier auf die zahlreichen Forschungsberichte des Großforschungsprojektes ABIDA, abrufbar unter: http://www.abida.de/, zuletzt abgerufen am 23.3.2017.

ist,[26] erfreut sich das TK-Recht einer Renaissance. M2M lässt sich durchaus als Telekommunikationsdienst (§ 3 Nr. 24 TKG) qualifizieren. Diese Dienste unterliegen dann der Meldepflicht (§ 6 TKG) und der Aufsicht durch die Bundesnetzagentur. Diese neue Situation kann sich aber schnell zu desaströsen Problemen für bestimmte Wirtschaftszweige entwickeln, etwa wenn man sich mit einem „connected car" durch Europa bewegt und damit den Aufsichtsregimen verschiedener EU-Staaten untersteht.[27]

IV. Big Data und Data property

Ungeklärt ist auch die Frage, wem das „Eigentum" an Daten zusteht.[28] Diese Frage ist in jüngster Vergangenheit missverstanden worden. So wurde ein eigenes Leistungsschutzrecht für Daten diskutiert.[29] Dabei geht es um die Frage, wie de lege lata ein Verfügungsrecht an Daten begründet werden kann.[30] Die Idee eines Dateneigentums wurde in der Literatur zu § 303a StGB schon kurze Zeit nach der Entstehung der Vorschrift diskutiert[31] und zugunsten desjenigen gelöst, der im Wege eines Skripturaktes die Daten aufgezeichnet hat. Im Sinne einer einheitlichen Rechtsordnung ist derjenige, der eine Datenverfügungsbefugnis nach § 303a StGB unter den oben ausgeführten Bedingungen erlangt hat, auch nach dem Zivilrecht als Berechtigter an den Daten anzusehen. Dabei gilt es zu beachten, dass Daten zwar keine Sachen im Sinne von § 90 BGB sind, aber Gegenstand eines Kaufvertrages sein können. Nach herrschender Meinung fallen unter den Begriff der sonstigen Gegenstände im Sinn von § 453 BGB einzelne unkörperliche Vermögenswerte, wie zum Beispiel Knowhow, Erwerbs- oder Gewinnchancen sowie Informationen.[32] Auf Daten als „sonstige Gegenstände" findet nach dieser Vorschrift daher Kaufrecht entsprechende Anwendung, weswegen dem schuldrechtlichen Verpflichtungsakt auch eine dingliche Zuordnung entsprechen sollte. Anzuwenden sind hier Skripturakttheorie und Verarbeitungsrechtsprechung im Sinne von § 950

---

[26] Sieht man einmal ab von *Piet Smiet,* s. dazu http://www.faz.net/aktuell/feuilleton/medien/die-youtuber-vom-let-s-play-kollektiv-piet-smiet-sollen-eine-rundfunklizenz-beantragen-14939592.html, zuletzt abgerufen am 21.4.2017.

[27] *Grünwald/Nüßing* MMR 2015, 378ff.; *Scherer/Heinickel* ENLR 2014, 141ff.; *Herrmann* RAW 2017, 19ff.

[28] *Hoeren* MMR 2013, 486; *Dorner* CR 2014, 617; *Zech* GRUR 2015, 1151; *Zech,* Information as a tradable commodity, in De Franceschi, European Contract Law and the Digital Single Market, 2016, 51; *Wiebe* GRUR-Int 2016, 877; *Kerber* GRUR-Int 2016, 989; *Faust* NJW Beil. 2/2016, 29.

[29] *Ensthaler* NJW 2016, 3473 (3476); s. auch Commission Staff Working Document on the free flow of data and emerging issues of the European economy v. 10.1.2017, abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy, zuletzt abgerufen am 23.3.2017.

[30] MüKoBGB/*Wagner,* 7. Aufl. 2017, BGB § 823 Rn. 296. Gerade im Datenschutzrecht finden sich Anknüpfungspunkte im Hinblick auf eine Datenherrschaft, die auf ein umfassendes Datenschutzrecht hinauslaufen, dazu *Buchner,* Informationelle Selbstbestimmung im Privatrecht, 2006; *Kilian,* Strukturwandel der Privatheit, in Garstka/Coy, Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten – Wilhelm Steinmüller zum Gedächtnis, 2014, 195–224.

[31] *Welp* IuR 1988, 448; vgl. va dort die alte Kommentierung, Fn. 46.

[32] Staudinger/*Beckmann,* 2004, BGB § 453 Rn. 20; *Spindler/Klöhn* VersR 2003, 410.

BGB.[33] Eigentum an den Daten bekommt der, der die Daten technisch aufgezeichnet hat oder diesen Skripturakt verantwortet hat.[34] Diese Frage ist keine akademische. Denn von ihr hängt ab, ob bei der Insolvenz eines Cloud-Anbieters (besonders im Auftragsverhältnis) Daten wieder ausgesondert werden können[35] oder wie sich ein Pfandrecht an Daten begründen lässt.[36]

V. Blockchain und der Sieg des Algorithmus

Und die Freaks? Sie träumen von einer digitalen Welt ohne staatliche Aufsicht, selbstreguliert mittels Algorithmen. Das Phänomen ist nicht neu. Schon beim Einsatz von Scoring durch Schufa & Co. tauchte die Besonderheit auf, dass die dem Scoring zugrunde liegenden Algorithmen als Betriebsgeheimnisse nicht eingesehen werden können und sich damit einer Kontrolle entziehen.[37] Diese Schwäche wird bei Blockchain-Verfahren dadurch behoben, dass an die Stelle staatlicher Aufsicht die Schwarmintelligenz, die Kontrolle durch Internettransparenz aller, tritt. Blockchains sind dezentrale Datenbanken, die unter anderem als technische Basis für sogenannte Kryptowährungen (zum Beispiel Bitcoin) fungieren, jedoch auch in anderen Bereichen verwendet werden können, in denen Informationen sicher aber zugleich transparent gespeichert und transferiert werden müssen. Letzteres wird gewährleistet, indem alle Transaktionen von Daten chronologisch archiviert und in Datenblöcken kettenartig aneinandergereiht werden. Die Informationen werden verifiziert und nahezu unveränderbar öffentlich (aber pseudonymisiert) gespeichert. Durch ein System des wechselseitigen Informationsabgleichs mit dem vorangegangenen Block und der Prüfsumme der gesamten Kette wird ein zuverlässiger Schutz vor Manipulationen ermöglicht. Nicht mehr erforderlich ist dabei ein Intermediär (zum Beispiel eine Bank). Die Datenbank liegt vielmehr dezentral in einem Netzwerk vieler Computer, sodass jeder Teilnehmer die gleichen Zugriffsrechte hat. Vorteil des Verfahrens ist die Minimierung des Datenaustausches. Es müssen nur noch Informationen ausgetauscht werden, die wirklich erforderlich sind. Ermöglicht werden zudem automatisierte Vertragsschlüsse oder -abwicklungen (sogenannte „Smart Contracts"), die nur noch an den Eintritt bestimmter Bedingungen, wie zum Beispiel den Zahlungseingang, geknüpft sind. Potentielle Gefahren bestehen jedoch im Hinblick auf Datenschutz,[38] Geldwäsche[39] oder das Dark-

[33] Dazu ausführlicher *Hoeren,* Big Data und Recht, 2014.

[34] *Boehm* ZEuP 2016, 358 (383); *Hieke* InTeR 2017, 10 (13); vgl. zu dieser Frage auch *Zech* GRUR 2015, 1151 (1151ff.).

[35] *Jülicher* ZIP 2015, 2063 (2065); *Jülicher* K&R 2015, 448 (450); zur Diskussion in der Schweiz: Parlamentarische Anfrage v. 16.9.2014 und Antwort des Bundesrates v. 12.11.2014, abrufbar unter: http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20141064, zuletzt abgerufen am 21.4.2017; s. auch zur Reform des Handelsgesetzbuches in Luxemburg Art. 567 Abs. 2 Code de Commerce.

[36] Court of Appeal, 2014, EWCA Civ 281.

[37] BGH CR 2014, 364.

[38] Dazu *Guggenberger* ZD 2017, 49ff.

[39] Dazu *Oberschelp,* Geldwäsche und Bitcoin, abrufbar unter: http://www.internet-law.de/2016/02/geldwaesche-und-bitcoin.html, zuletzt abgerufen am 21.4.2017.

net[40]. Im juristischen Bereich sind vielfältige positive Anwendungen denkbar, etwa im Bereich EGovernment, zum Beispiel bei öffentlichen Katastern vom Grundbuchamt bis hin zur Steuerverwaltung. Auch das Stromnetz könnte sich über Blockchain dezentral selbst verwalten. Inzwischen denken auch viele Kreditinstitute und Versicherungen über den Einsatz solcher Instrumente nach.[41]

[40] *Rennard,* Darknet Mythes et réalités, 2016.
[41] Dazu *Prinz/Schulte,* Fraunhofer-Positionspapier Blockchain, 2017.