3. Kapitel. Schutz des Rechtsverletzten

Die Frage, wann eine Menschenfleischsuche rechtswidrig ist und wann die Teilnehmer, einschließlich des Informationsberichters, des Informationssammlers, des Veranlassers, des Kommentators, des ICP und des ISP, haften müssen, wurde bereits diskutiert. Jetzt wird die Frage, wie der Rechtsverletzte vor den Rechtsverletzungen geschützt werden kann, bzw. was für Ansprüche er gegen die Verletzer hat, behandelt. Darüber hinaus wird auch die Frage beantwortet, wie man rechtswidrige Menschenfleischsuche und die dadurch entstehenden Rechtsverletzungen von der Quelle an vermeiden kann und wie die Zielperson vorbeugend vor den Rechtsverletzungen geschützt werden kann.

§ 11 Maßnahmen zum Schutz des Rechtsverletzten gegen den rechtsverletzenden Internetnutzer

I Rechtsansprüche gegen den rechtsverletzenden Internetnutzer

1. Nach deutschem Recht

a) Beseitigung- und Unterlassungsanspruch

Ist eine Rechtsverletzung des Persönlichkeitsrechts begründet, hat der Rechtsverletzte gemäß § 1004 Abs. 1 Satz 1 BGB den Anspruch auf Entfernung der rechtsverletzenden Inhalte und gemäß § 1004 Abs. 1 Satz 2 BGB den Anspruch auf Unterlassung einer Rechtsverletzung ähnlicher Art in der Zukunft.

b) Schmerzensgeldanspruch

Die Verletzung des Persönlichkeitsrechts kann auch durch eine Geldentschädigung wiedergutgemacht werden. Nach der Rechtsprechung des BGH handelt es sich bei einer Geldentschädigung aufgrund einer Verletzung des Persönlichkeitsrechts „im eigentlichen Sinne nicht um ein Schmerzensgeld nach § 847 BGB a.F. (jetzt: § 253 Abs. 2 BGB n.F.)", „sondern um einen Rechtsbehelf, der auf den Schutzauftrag aus Art. 1 und Art. 2 Abs. 1 GG zurückgeht".[637] Darunter wird vor allem die Genugtuung des Opfers berücksichtigt.[638]

Ferner liegt hier auch ein Präventionsgedanken vor.[639] Das heißt, der Schmerzensgeldanspruch wird erst zugelassen, wenn die Gefahr besteht, dass ohne einen solchen Anspruch die Verletzungen der Persönlichkeit „ohne Sanktionen mit der Folge blieben, dass der Rechtschutz der Persönlichkeit verkümmern würde".[640]

Deswegen wird ein Schmerzensgeldanspruch nicht in jedem Fall zugebilligt.[641] Dazu müssen zwei Voraussetzungen erfüllt werden: zum einen muss es

637 BGH, NJW 2005, 58, 59.
638 BGH, NJW 2005, 58, 59; BGH, NJW 1996, 984; BVerfG, NJW 2000, 2187f.; siehe auch Schiemann in Staudinger, BGB § 253, Rn. 28ff. und 53ff.
639 BGH, NJW 2005, 58, 59.
640 BGH, NJW 2005, 58, 59; BGH, NJW 1996, 984.
641 Vgl. BGH, NJW 2005, 58, 59.

sich um einen schwerwiegenden Eingriff des Persönlichkeitsrechts handeln; und zum anderen muss die Beeinträchtigung nicht in anderer Weise befriedigend ausgeglichen werden können.[642]

Um einen schwerwiegenden Eingriff zu beurteilen, müssen nach der Rechtsprechung des BVerfG einige Elemente berücksichtigt werden. Dazu zählen das Ausmaß der Verbreitung der verletzenden Aussagen, die Nachhaltigkeit der Fortdauer der Entschädigung, der Anlass und Beweggrund des Verletzers, sowie der Grad seines Verschuldens.[643]

c) Schadensersatzanspruch

Außer Schmerzensgeld kann der Verletzte gemäß § 823 Abs. 1 BGB Schadensersatz des wegen Persönlichkeitsrechtsverletzung entstehenden materiellen Schadens einschließlich Rechtsverfolgungskosten verlangen.[644]

d) Antrag auf einstweilige Verfügung

Jedoch sind Schadensersatz-, Schmerzensgeld-, Beseitigungs- und Unterlassungsansprüche nachträgliche Maßnahmen, die erst nach der Rechtsverletzung durch ein Gerichtsverfahren verwirklicht werden können. Wegen der Besonderheit der Persönlichkeitsrechtsverletzung im Internet[645] ist ein vorbeugender Rechtsschutz effizienter, weil eine rechtzeitige Beendigung des laufenden Delikts während der Menschenfleischsuche die schnelle weitere Verbreitung der rechtsverletzenden Inhalte bzw. die Vertiefung der Rechtsverletzung vermeiden kann, während ein verletztes Persönlichkeitsrecht schlecht wiedergutgemacht werden kann. Beispielsweise kann eine offengelegte Intimsphäre nicht mehr wieder verdeckt werden.

§ 935 ZPO hat durch die Regelung der einstweiligen Verfügung die Möglichkeit eines vorbeugenden Rechtsschutzes geschaffen.[646] Nach dieser Vorschrift kann der Rechtsverletzte einen Antrag auf Erlass einer einstweiligen Verfügung stellen,[647] um die Verletzung seines Persönlichkeitsrechts rechtzeitig zu verhindern.[648] Zu den erlaubten Verfügungsansprüchen gehören die Ansprüche auf Handlung und Unterlassung, die für die Rechtsverletzung im Fall der

642 BVerfG, NJW 2004, 591, 592.
643 BVerfG, NJW 2004, 591, 592.
644 Nink in Spindler/Schuster, BGB § 823, Rn. 48.
645 Siehe oben unter § 2 II.
646 Mayer in Vorwerk/Wolf, ZPO § 935, Rn. 8.
647 Kemper in Saenger, ZPO § 935, Rn. 11.
648 Kemper in Saenger, ZPO § 935, Rn. 11, 13; Mayer in Vorwerk/Wolf, ZPO § 935, Rn. 9.

Menschenfleischsuche zum Schutz des Rechtsverletzens ausreichend sind.[649] Zu dem zulässigen Verfügungsgrund gehört der Schutz des Persönlichkeitsrechts.[650] Ein Antrag wäre begründet, wenn der Verletzte die Verfügungsansprüche und den Verfügungsgrund schlüssig behauptet und glaubhaft macht.[651]

2. Nach chinesischem Recht

a) Allgemeine Regelungen über die Ansprüche

Ist eine Rechtsverletzung des Persönlichkeitsrechts während Menschenfleischsuche nach chinesischem Recht begründet, hat der Rechtsverletzte gemäß § 3 i.V.m. § 15 Abs. 1 Delikthaftungsgesetz Ansprüche auf Entfernung der rechtsverletzenden Inhalte, Unterlassung weiterer Rechtsverletzung gleicher Art, Schadensersatz, Beseitigung der Wirkung, offizielle Entschuldigung und im Fall von Ehrverletzung auf Wiedergutmachung der Ehre. Diese Maßnahmen können gemäß § 15 Abs. 2 einzeln oder kombiniert verwendet werden.

b) Schmerzensgeldanspruch

Gemäß § 22 Delikthaftungsgesetz und § 1 Abs. 1 i.V.m. § 8 „Erklärung einiger Fragen über die Haftung für den immateriellen Schaden wegen zivilrechtlicher Rechtsverletzung" hat der Verletzte Anspruch auf Schmerzensgeld, wenn die Persönlichkeitsrechtsverletzung zu einem schwerwiegenden immateriellen Schaden führt. Die Beurteilung des schwerwiegenden immateriellen Schadens kann nur in jedem einzelnen Fall vom Gericht entschieden werden.[652]

Über die Höhe des Schmerzensgeldes müssen gemäß § 10 der oben genannten Erklärung die Schuld der Verletzer, die Konstellation des Vorgangs der Verletzung, das Ergebnis der Rechtsverletzung, das Profitieren des Verletzers durch

---

649 Mayer in Vorwerk/Wolf, ZPO § 935, Rn. 9.

650 Mayer in Vorwerk/Wolf, ZPO § 935, Rn. 9.

651 Kemper in Saenger, ZPO § 935, Rn. 10.

652 Vgl. Zhongshan Mitteleres Volksgericht, Urt. v. 25.11.2005 - (2005) zhong zhong fa min yi zhong zi di 1003 hao; Kaifeng Mitteleres Volksgericht, Urt. v. 19.12.2011 - (2011) bian min zhong zi di 1165 hao; Xi´an Mitteleres Volksgericht, Urt. v. 30.11.2012 - (2012) xi min er zhong zi di 02249 hao; Pukou Unteres Volksgericht, Urt. v. 12.12.2012 - (2012) pu min chu zi di 2125 hao; Shapingba Unteres Volksgericht, Urt. v. 17.9.2009 - (2009) sha fa min chu zi di 1800 hao; Nanjing Mittleres Volksgericht, Urt. v. 18.4.2013 - (2013) ning min zhong zi di 779 hao; Shanghai Zweite Mittleres Volksgericht, Urt. v. 5.5.2011 - (2010) hu er zhong min yi (min) zhong zi di 1593 hao.

die Verletzung, die wirtschaftliche Fähigkeit des Verletzers zur Haftung und das Lebensniveau der Region des zuständigen Gerichts berücksichtigt werden.

c) Antrag auf einstweilige Verfügung

Einstweiliger Rechtsschutz ist in China ursprünglich zum Schutz des geistigen Eigentums entwickelt worden,[653] und nach §§ 100 f. des neuen Zivilprozessgesetzes nur für vermögensrechtliche Ansprüche anwendbar. Jedoch hat ein unteres Volksgericht in der Provinz Jiangxi im März 2013 das erste Mal die einstweilige Verfügung offiziell auf den Fall über Persönlichkeitsrechtsverletzung analogisiert angewendet.[654]

Über die analoge Anwendung der einstweiligen Verfügung auf den Fall des Persönlichkeitsrechtsschutzes gibt es in der Literatur eine andere Meinung. Nach dieser Meinung ist eine Analogie im Persönlichkeitsrecht nicht möglich, weil die Rechtsverletzung des Vermögensrechts einfach bejaht oder verneint werden kann, während die Beurteilung der Rechtsverletzung des Persönlichkeitsrechts erst nach komplizierter Interessenabwägung möglich ist.[655]

Meiner Meinung nach sollte die analoge Anwendung möglich sein. Obwohl die Beurteilung der Persönlichkeitsrechtsverletzung in jedem einzelnen Fall durch Interessenabwägung erfolgt, ist sie nicht unbedingt schwieriger als die der Verletzung des Vermögensrechts. Dies ist besonders der Fall, wenn eine Verletzung des Persönlichkeitsrechts offensichtlich ist.

Die Bejahung der einstweiligen Verfügung ist möglich, wenn der Verletzte den Verfügungsgrund so glaubhaft begründet, dass eine Persönlichkeitsrechtsverletzung für jede Person offensichtlich ist. Für einen solchen Fall ist eine Interessenabwägung zwar notwendig, aber die Beurteilung ist nicht schwieriger als die von der Verletzung des Vermögensrechts.

Übrigens hat das untere Volksgericht in der Provinz Jiangxi den Prozess der einstweiligen Verfügung über das Vermögensrecht komplett übernommen.[656]

---

653 Zhu Wei, Legal Evening News, 10.05.2013, http://www.zxxk.com/article/245604.html (besucht am 04.04.2015).

654 Duchang Unteres Volksgericht, Beschl. v. 22.3.2013 - (2013) du wang chu zi di 2 hao; vgl. Guo Hongpeng/Huang Hui, Legal Daily, 25.03.2013, http://www.legaldaily.com.cn/index_article/content/2013-03/25/content_4308890.htm?node=5954 (besucht am 04.04.2015).

655 Zhu Wei, Legal Evening News, 10.05.2013, http://www.zxxk.com/article/245604.html (besucht am 04.04.2015).

656 Guo Hongpeng/Huang Hui, Legal Daily, 25.03.2013, http://www.legaldaily.com.cn/index_article/content/2013-03/25/content_4308890.htm?node=5954 (besucht am 04.04.2015).

Das heißt, der Antragsteller muss gemäß § 101 Zivilprozessgesetz eine Sicherheit leisten, um die Wahrheit seines Antrags zu garantieren. Dadurch wird das Recht des Äußernden ausreichend geschützt.

Der Verletzte muss die Rechtsverletzung des Persönlichkeitsrecht selbst beweisen und das Risiko tragen, wenn er den Antrag falsch gestellt hat. Eine einstweilige Verfügung für den Fall der Persönlichkeitsrechtsverletzung schadet keinem und ist zum Schutz des Verletzten vor Vertiefung der Rechtsverletzung erforderlich. Sie ist zu bejahen.

II. Identifizierung des rechtsverletzenden Internetnutzers im Gerichtsprozess

Um die oben genannten Ansprüche zu verwirklichen, muss der Verletzte Klage oder Antrag bei dem Gericht stellen. Dafür muss der Internetnutzer ersten einmal identifiziert werden.

1. In Deutschland

Gemäß § 50 ff. i.V.m. §§ 253 Abs. 2 Nr. 1, 130 Nr. 1 ZPO muss die Bezeichnung des Beklagten oder des Antragsgegners – im Fall vom Antrag auf Erlass einer einstweiligen Verfügung – eindeutig sein.[657] Eine eindeutige Bezeichnung des Beklagten oder Antragsgegners soll mindestens den Klarnamen, Beruf und Anschrift beinhalten.[658] Wie der Kläger oder Antragsteller diese Informationen hinter einem pseudonymen Internetnamen herausfinden kann, muss nach unterschiedlichen Fallgruppen diskutiert werden.

a) Für den Fall der Verletzung des Rechts am eigenen Bild

Der Rechtsinhaber des Bildes hat gemäß § 101 UrhG im Fall der offensichtlichen Rechtsverletzung einen Auskunftsanspruch gegen den Verletzer. Nach der herrschenden Meinung müssen die rechtsverletzenden Tätigkeiten nicht unbedingt im gewerblichen Ausmaß begangen worden sein.[659] Nach der aktuellsten Rechtsprechung muss das Urheberrecht oder ein anderes nach dem

657 Hüßtege in Thomas/Putzo, § 50 Vorbem. Rn. 4; Lindacher, Münchener Kommentar zur ZPO, Vorbemerkung zu §§ 50 ff., Rn. 12f.

658 Hüßtege in Thomas/Putzo, § 50 Vorbem. Rn. 4; Lindacher, Münchener Kommentar zur ZPO, Vorbemerkung zu §§ 50 ff., Rn. 12f.

659 Spindler in Spindler/Schuster, UrhG § 101, Rn. 1; Czychowski in Fromm/Nordemann, UrhG § 101, Rn. 2, 11.

Urheberrechtsgesetz geschütztes Recht auch nicht unbedingt in gewerblichem Ausmaß verletzt worden sein.[660] Das heißt, ein Auskunftsanspruch gegen den Verletzer kann auch während der Menschenfleischsuche gegen den rechtsverletzenden Internetnutzer geltend gemacht werden.

Um einen rechtsverletzenden Internetnutzer im Fall von Verletzung des Rechts am eigenen Bild zu identifizieren, gibt es in der Praxis zwei Möglichkeiten.

aa) Identifizierung durch Anmeldedaten

Es ist oft der Fall, dass man sich mit Namen, Anschriften oder mindestens Pseudonym und Email-adresse anmelden muss, bevor man auf der Webseite Beiträge eintragen darf. In diesem Fall ist das Pseudonym häufig direkt mit den rechtsverletzenden Beiträgen verbunden. Würde es auf dieser Webseite pflichtig sein, sich mit realen Namen und realer Anschrift anzumelden, könnte der Verletzte direkt einen Anspruch auf die Auskunft der Anmeldedaten dem Provider verlangen. Die Pflicht der Auskunft bezieht sich nach der aktuellsten Entscheidung nicht nur auf Hostprovider, sondern auch auf Webseitenbetreiber.[661]

Geht es um Anmeldedaten muss § 12 Abs. 2 TMG angewendet werden. Aufgrund dieses Paragraphen ist der Hostprovider oder Webseitenbetreiber nicht zur Herausgabe der zur Bereitstellung des Telemediums erhobenen Anmeldedaten befugt, mit der Ausnahme, dass soweit eine Rechtsvorschrift dies erlaubt oder der Nutzer - was hier nicht in Rede steht - eingewilligt hat.[662] Eine Ausnahme findet man jedoch in § 14 Abs. 2 TMG, aufgrund dessen der zuständigen Stellen auf Anordnung der Dienstanbieter im Einzelfall Auskunft über Bestandsdaten erteilen darf, soweit dies für Zwecke zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.[663] Die Anmeldedaten wie der Name und die Anschrift des Verletzers sind gemäß § 14 Abs. 1 TMG und § 3 Nr. 30 TKG zweifellos Bestandsdaten.[664]

Wegen der Verletzung des Rechts am eigenen Bild darf der Rechtinhaber Auskunft auf die Anmeldedaten des Verletzers vom Provider verlangen.

660 BGH, NJOZ 2013, 773.
661 OLG Dresden, ZUM-RD 2012, 536, 538.
662 BGH, K&R 2014, 589, Rz. 9ff.
663 BGH, K&R 2014, 589, Rz. 9ff.
664 BGH, NJOZ 2013, 773, 777.

bb) Identifizierung durch IP-Adresse

Es ist auch oft der Fall, dass man ohne Anmeldung Beiträge eintragen kann. Noch häufiger ist es, dass man nicht pflichtig ist, mit realen Namen oder realer Anschrift anzumelden. In diesen Fällen ist es unmöglich, den Verletzer durch Anmeldedaten unmittelbar zu identifizieren. Aber eine Identifizierung des Verletzers unter Verwendung der dynamischen IP-Adresse, die er bei der Eintragung der rechtsverletzenden Beiträge vergibt hatte, ist immer noch möglich.

Für diesen Fall ist die oben genannte Gesetzanwendung aber fraglich, weil gemäß § 14 Abs. 2 TMG nur Bestandsdaten des Nutzers an einem Dritten ermittelt werden darf, aber es fraglich ist, ob dynamische IP-Adresse zur Bestandsdaten oder eher zur Verkehrsdaten im Sinne von § 3 Nr. 30 TKG gehört. Verkehrsdaten sind nach der Begriffsbestimmung des § 3 Nr. 30 TKG Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Im Gegensatz handelt es sich bei Bestandsdaten nach der Legaldefinition des § 3 Nr. 3 TKG um Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.

Die Frage, ob dynamische IP-Adresse zur Bestandsdaten oder Verkehrsdaten gehört, ist schon immer umstritten und unklar gewesen. Die Aufsichtsbehörden für den Datenschutz vertrat eine vermittelnde Ansicht und sah in der IP-Adresse sowohl ein Bestands- als auch Verkehrsdatum.[665] Der BGH hatte in der „Sommer unseres Lebens"-Entscheidung[666] die Auffassung vertreten, IP-Adressen seien Bestandsdaten,[667] weil sie zum einen nur Auskunft über den Namen des Anschlussinhabers geben würden, und sie zum anderen keine Angaben beinhalten, worüber und wie lange kommuniziert wurde.[668] In der Literatur herrscht die Meinung, dass sich dynamische IP-Adresse offensichtlich um personenbezogenes Verkehrsdatum handelt, denn sie Anknüpfungspunkt für die Darstellung ist, welche Informationen mittels eines Rechners bzw. über den Anschluss abgerufen wurden.[669]

Der Beschluss vom BGH am 19. 4. 2012 hat jedoch die Diskussion zu Ende gebracht, und die Schlussfolgerung getroffen, dass sich die IP-Adresse um

665 Karg, MMR-Aktuell 2011, 315811.
666 BGH, MMR 2010, 565.
667 Karg, MMR-Aktuell 2011, 315811.
668 BGH, MMR 2010, 565.
669 Karg, MMR-Aktuell 2011, 315811.

Verkehrsdatum handelt.[670] Eine dynamische IP-Adresse ist nach der Meinung des BGH keinem bestimmten Nutzer dauerhaft zugeordnet, sondern wird unterschiedlichen Nutzern jeweils nur für eine Sitzung (dynamisch) zugeteilt.[671] Eine Verknüpfung der dynamischen IP-Adresse mit dem Nutzer, dem sie zu einem bestimmten Zeitpunkt zugewiesen war, ist daher nur unter Verwendung der jeweils hierzu gespeicherten Verkehrsdaten wie des Datums und der Uhrzeit der Verbindung möglich.[672]

Als Ergebnis des Falles, wenn der Verletzer nur durch Verwendung dynamischer IP-Adresse identifiziert werden kann, muss der Verletzte gemäß § 101 Abs. 9 S. 1 UrhG eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten beantragen.

b) Für den Fall der Verletzung des Persönlichkeitsrechts allgemein

Weiter wird diskutiert, ob die Situation der Verletzung des Rechts am eigenen Bild auch auf die Situation der Verletzung des allgemeinen Persönlichkeitsrechts angewendet wird.

Wie oben bereits erwähnt, dürfen für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwendet werden, soweit eine Rechtsvorschrift dies erlaubt oder der Nutzer - was hier nicht in Rede steht - eingewilligt hat (§ 12 Abs. 2 TMG). Die Ermächtigung besteht im Fall der Verletzung des Rechts am eigenen Bild im Rahmen der Durchsetzung der Rechte am geistigen Eigentum in § 14 Abs. 2 TMG. Eine gleiche Regelung zum Schutz der allgemeinen Persönlichkeitsrechte findet man innerhalb TMG jedoch nicht.[673]

Ein Auskunftsanspruch könnte aber aus Treu und Glauben im Sinne von § 242 BGB ausgeleitet werden. Liegt auf der Webseite eine Persönlichkeitsrechtsverletzung vor, muss der Webseitenbetreiber unabhängig von seiner Schuld als Störer haften.[674] Daraus entstehen die Ansprüche der Verletzten auf Unterlassung und Löschung persönlichkeitsverletzender Einträge. Wegen dieser Ansprüche entsteht zwischen dem Verletzten und dem Betreiber oder dem Provider ein gesetzliches Schuldverhältnis.[675] Nach der ständigen Meinung des BGH besteht ein Auskunftsanspruch

670 BGH, NJOZ 2013, 773, 777.
671 BGH, NJOZ 2013, 773, 777.
672 BGH, NJOZ 2013, 773, 777; vgl. OLG Hamburg, NJOZ 2010, 1222 = ZUM 2010, 893, 898.
673 BGH, K&R 2014, 589.
674 OLG Dresden, ZUM-RD 2012, 536, 538.
675 OLG Dresden, ZUM-RD 2012, 536, 538.

des Berechtigten gegen den Verpflichteten in jedem Rechtsverhältnis, „in dem der Berechtigte in entschuldbarer Weise über Bestehen und Umfang seines Rechtes im Ungewissen und der Verpflichtete unschwer zur Auskunftserteilung in der Lage ist".[676] Dazu gehört auch das Schuldverhältnis in unserem Fall.

Diese Meinung wurde vom BGH in seiner aktuellsten Entscheidung am 1. 7. 2014 bejaht.[677] Nach seiner Meinung hat der Provider im Fall der Persönlichkeitsrechtsverletzung eine „Auskunftspflicht".[678] Jedoch hat er die Anspruchsmöglichkeit des Verletzten abgelehnt, weil der Provider doch „nicht zur Herausgabe der zur Bereitstellung des Telemediums erhobenen Anmeldedaten befugt ist".[679]

Der BGH geht davon aus, dass eine Erlaubnis zur Auskunft der Nutzerdaten durch Rechtsvorschrift außerhalb des Telemediengesetzes lediglich dann in Betracht kommt, wenn sich eine solche Vorschrift ausdrücklich auf Telemedien bezieht.[680] Dies scheidet dann den aus Treu und Glauben (§ 242 BGB) hergeleiteten allgemeinen Auskunftsanspruch aus, weil sich § 242 BGB nicht ausdrücklich auf Telemedien bezieht.

Der BGH hat weiterhin die Möglichkeit eine analoge Anwendung von § 14 Abs. 2 TMG, § 15 Abs. 5 Satz 4 TMG zur Durchsetzung der Rechte am geistigen Eigentum ebenfalls ausgeschieden, da es seiner Meinung nach an einer planwidrigen Regelungslücke fehlt.[681] Die Vorschriften dienen ausschließlich dem Schutz des geistigen Eigentums, um Innovation und kreatives Schaffen zu fördern, den Arbeitsmarkt zu entwickeln und die Wettbewerbsfähigkeit zu verbessern; Persönlichkeitsrechte werden hier nicht bezogen.[682]

Die Absage der analogen Anwendung wurde in der Literatur kritisiert.[683] Der BGH geht selbst auch davon aus, dass seine Meinung wenig überzeugend ist.[684]

Meiner Meinung nach soll eine analoge Anwendung von § 14 Abs. 2 TMG, § 15 Abs. 5 Satz 4 TMG zur Durchsetzung der Rechte am geistigen Eigentum zulässig sein. Wie oben schon diskutiert, hat der BGH einen Auskunftsanspruch wegen Verletzung des Rechts am eigenen Bild zugesagt. Bei der Begründung

676 BGH, BGHZ 10, 385; BGHZ 126, 109, 113; BGHZ 149, 165, 175; OLG Dresden, ZUM-RD 2012, 536, 538.
677 BGH, K&R 2014, 589.
678 BGH, K&R 2014, 589, Rn. 6.
679 BGH, K&R 2014, 589, Rn. 9.
680 Nach dem Gesetzeswortlaut von § 12 Abs. 2 TMG.
681 BGH, K&R 2014, 589, Rn. 13ff.
682 BGH, K&R 2014, 589, Rn. 15.
683 Klein, GRUR-Prax 2014, 539.
684 BGH, K&R 2014, 589, Rn. 17.

wurde allgemein anerkannt, dass die rechtsverletzenden Tätigkeiten nicht unbedingt im gewerblichen Ausmaß begangen worden sein,[685] und das geschütztes Recht auch nicht unbedingt in gewerblichem Ausmaß verletzt worden sein müssen.[686] Das bedeutet, dass der Schutzgegenstand nicht nur der wirtschaftliche Teil des Rechts am eigenen Bild als Urheberrecht ist, sondern auch lediglich der persönlichkeitsrechtliche Teil des Rechts am eigenen Bild als Persönlichkeitsrecht sein kann. Dies hat offensichtlich die Tür zur analogen Anwendung auf den Fall der allgemeinen Persönlichkeitsrechtsverletzung geöffnet.

Der BGH hat am Ende seiner Entscheidung am 1. 7. 2014 zugegeben, dass die Beschränkung der Ermächtigung zur Auskunftserteilung auf Inhaber von Rechten am geistigen Eigentum wenig nachvollziehbar und eine Ausweitung auf Persönlichkeitsrechtsverletzungen wünschenswert sein mag.[687] Aber eine solche Regelung müsste seiner Meinung nach der Gesetzgeber treffen.[688]

Durch die Entscheidung des BGH wird ein allgemeiner Auskunftsanspruch gegen den Provider wegen Persönlichkeitsrechtsverletzung in Deutschland abgesagt. Außer dem Fall der Verletzung des Rechts am eigenen Bild kann ein Auskunftsanspruch nur noch verlangt werden, wenn sich das Persönlichkeitsrechtsverletzen, zum Beispiel in Form von Beleidigung oder Verleumdung, zu Straftat wandelt, und der Auskunftsanspruch dann zum Zweck der Strafverfolgung dient.[689]

c) Zwischenergebnis

In Deutschland hat der Verletzte Auskunftsanspruch gegen den ISP auf die Nutzerdaten des unmittelbaren Verletzers im Fall von Verletzung des Rechts am eigenen Bild oder in den Fällen von schwerwiegenden Persönlichkeitseingriffen, Beleidigungen oder Verleumdungen wie zum Beispiel, zu Zwecken der Strafverfolgung.[690] Ein allgemeiner Auskunftsanspruch wegen Verletzung allgemeiner Persönlichkeitsrechte wird vom BGH ausdrücklich abgelehnt.

Jedoch hat der BGH durch seine Entscheidung die Diskussion über den allgemeinen Auskunftsanspruch nicht beendet. Auf einer Seite sind die Begründungen

685 Spindler in Spindler/Schuster, UrhG § 101, Rn. 1; Czychowski in Fromm/Nordemann, UrhG § 101, Rn. 2, 11.
686 BGH, NJOZ 2013, 773.
687 BGH, K&R 2014, 589, Rn. 17.
688 BGH, K&R 2014, 589, Rn. 17.
689 § 14 Abs. 2 TMG.
690 Klein, GRUR-Prax 2014, 539, 541.

zur Ablehnung des Auskunftsanspruch nicht überzeugend genug. In der Literatur gibt es schon kräftige Gegenmeinungen. Auf der anderen Seite hat der BGH in der Entscheidung auch selbst hingewiesen, dass eine Anerkennung des Auskunftsanspruchs nachvollziehbar und wünschenswert ist, nur nicht er sondern der Gesetzgeber dafür zuständig ist.

Es ist verständlich, dass sich der BGH nicht traut, einen allgemeinen Auskunftsanspruch anzuerkennen, weil dahinten doch die Sorge auf Beschränkung der Meinungsäußerungsfreiheit im Sinne von anonymen Äußerungen steht.[691] Die weitere Entwicklung über dieses Thema ist in Deutschland zu erwarten.

Zurzeit ist es in Deutschland für den Verletzten ggf. einfacher und praktischer, direkt auf den ISP einzuwirken, ein Beseitigungs- und Unterlassungsanspruch im Rahme der Störerhaftung geltend zu machen.[692] Dies hilft jedoch nicht, die Verletzungen der Persönlichkeitsrechte von der Quelle an zu vermeiden.

2. In China

Um einen Zivilprozess in China durchzuführen, muss der Kläger gemäß § 119 Abs. 1 Nr. 2 Zivilprozessgesetz einen klaren Beklagten haben, gegen den er klagt. Ein klarer Beklagter bedeutet gemäß § 121 Abs. 1 Nr. 2 Zivilprozessgesetz, dass der Name, das Geschlecht, die Anschrift und der Beruf des Beklagten vorhanden sein müssen. Dies gilt gemäß § 100 f. Zivilprozessgesetz auch für den Prozess auf Erlass einer einstweiligen Verfügung.

Bei dem Fall der Persönlichkeitsrechtsverletzung während der Menschenfleischsuche ist es am häufigsten, dass die wahren persönlichen Daten des Verletzers unbekannt sind. Nach chinesischem Recht besteht zwischen dem Verletzten und dem Provider entweder eine vertragliche oder eine gesetzliche Verbindung, aus der der Verletzte einen Auskunftsanspruch auf die persönlichen Daten des Internetnutzers verlangen kann. Um einen rechtsverletzenden Internetnutzer zu identifizieren muss der Verletzte vor dem Gericht klagen, weil nur das Gericht von Amts wegen die Identifizierung des Beklagten erwirken kann. Dies schafft eine Zwickmühle für den Verletzten.

Um dieses Problem zu lösen, haben die Gerichte in der Provinz Jiangxi eine neue Methode geschaffen. Gemäß § 9 „Leitlinie einiger Fragen über die Gesetzesanwendung für die Beurteilung der Fälle über Rechtsverletzung im Internet von dem Oberen Volksgericht in der Provinz Jiangxi (Probe-Version)“ kann die IP-Adresse oder das Pseudonym des Beklagten vorläufig verwendet werden, um ein Vorverfahren

691 LG München, BeckRS 2013, 12855, in Anlehnung an BGH MMR 2009, 608, 612.
692 Uffeln/Günther, http://www.kanzlei-uffeln.de/ku/ (besucht am 04.04.2015), S. 6.

vor dem offiziellen Gerichtsprozess einzuleiten. Während dieses Vorverfahrens kann der Kläger gemäß § 64 Abs. 2 Zivilprozessgesetzes beim Gericht beantragen, von Amts wegen die Registrierungsinformation oder IP-Adresse des Beklagten von dem ISP zu fordern. Gleichzeitig kann der Kläger bei der Behörde für die Sicherheitskontrolle im Internet beantragen, den Beklagten durch die IP-Adresse oder Registrierungsinformation zu identifizieren. Erst nachdem der Beklagte als eine bestimmte Person festgestellt wurde, beginnt der offizielle Gerichtsprozess. Sonst wird die Klage abgewiesen. Diese Methode ist zwar noch nicht vom höheren Gericht offiziell anerkannt, aber ihr begegnet jedoch auch keine Gegenmeinung.

3. Ein kurzer Vergleich zwischen Deutschland und China

Bei der Identifizierung des Verletzers haben Deutschland und China zwei unterschiedliche Wege genommen.

Um eine Klage oder eine einstweilige Verfügung gegen den Internetnutzer durchzuführen, muss sich der Verletzte in Deutschland erst an den ISP wenden, um gegen ihn einen Auskunftsanspruch zu verlangen. Hier soll der ISP nach seinen Kenntnissen entscheiden, ob eine offensichtliche Persönlichkeitsrechtsverletzung vorliegt. Wenn der ISP eine andere Meinung als der Verletzte hat, und deswegen eine Auskunftserteilung verneint, muss der Verletzte erst gegen den ISP klagen, um seinen Auskunftsanspruch zu verwirklichen, bevor er endlich eine Klage gegen den unmittelbaren Verletzer erheben kann.

Dieses Verfahren ist für den Verletzten viel unpraktischer als direkt einen Beseitigungs- oder Unterlassungsanspruch gegen den ISP zu stellen. Übrigens muss der ISP ein hohes Risiko für seine Entscheidung tragen, ob eine offensichtliche Persönlichkeitsrechtsverletzung vorliegt. Wird eine Verletzung von ihm irrtümlich bejaht, und die Kundendaten dem „Verletzten" mitgeteilt, muss er wegen Pflichtverletzung i.S.v. § 13 Abs. 6 TMG haften. Verneint er eine offensichtliche Persönlichkeitsrechtsverletzung muss er an einem Gerichtverfahren auf Auskunftsanspruch gegen ihn teilnehmen. Durch dieses Verfahren werden die hohen Belastungen dem ISP gegeben. Der unmittelbare Verletzer, der die Verletzung verursacht, ist dagegen vom Verletzten schlecht erreichbar. Dem Verfahren dient es nicht, die Verletzungen von der Quelle an zu vermeiden.

Durch das Vorverfahren, in dem der unmittelbare Verletzer von Amts wegen ermittelt wird, ist in China eine Klage direkt gegen den unbekannten rechtsverletzenden Internetnutzer möglich. Der ISP ist dadurch von der Beurteilung der Persönlichkeitsrechtsverletzung befreit, und braucht sich nicht um die falsche Erteilung der Kundendaten sorgen, weil die Erteilung immer

auf Verlangen des Gerichts durchgeführt wird. Das Gericht ist in diesem Fall der einzige, der die Persönlichkeitsrechtsverletzung beurteilt und der wegen seiner Fachkenntnisse die Richtigkeit der Beurteilung garantieren kann. Das Verfahren in China bzw. in der Provinz Jiangxi ermöglicht dem Verletzten einen besseren Weg, um den Rechtsanspruch direkt gegen den unmittelbaren Verletzer zu verlangen.

III. Real-Name-System

Real-Name-System bedeutet, dass die Internetnutzer mit ihren realen Namen und ID-Nummer oder Passnummer registriert sein müssen, bevor sie Beiträge im Internet veröffentlichen. Die Wahrheit der beim Registrieren eingegebenen Information wird durch Zusammenarbeit zwischen dem ISP und der Behörde der öffentlichen Sicherheit überprüft. Bei der Meinungsäußerung auf der Webseite darf der Internetnutzer ein Pseudonym benutzen. Aber nach Real-Name-System steht hinter jeden pseudonymen Namen immer eine richtige Person, die für ihr online Verhalten verantwortlich sein soll.

Durch Real-Name-System wird das Problem der unbekannten Verletzer im Internet gelöst. Der Verletzte kann gegen den Beklagten direkt mit dem pseudonymen Namen vor Gericht klagen, weil die richtige Person hinter dem pseudonymen Namen durch Real-Name-System sofort herausgefunden werden kann.

Jedoch besteht für Real-Name-System auch die Gefahr, dass die Internetnutzer aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen ihre Meinungen nicht mehr äußern, was zur Selbstzensur führt.

Real-Name-System ist ein heißes Thema in China. Deswegen wird die folgende Diskussion über Real-Name-System mit China anfangen.

1. Real-Name-System in China

a) Die Entwicklung des Real-Name-System in China

Am 21. Nov. 2001 hat das chinesische Bildungsministerium die „Regelung zur Verwaltung des Diensts des elektronischen schwarzen Brettes (BBS-Service) des Hochschulnetzwerkes" erlassen. Aufgrund § 9 dieser Regelung sollen Hochschulen beim Anbieten eines elektronischen schwarzen Brettes das Real-Name-System benutzen. Das ist die früheste Regelung über Real-Name-System in China.

Im Jahr 2002 hat ein Journalistischer Professor Xiguang Li eine Rede gehalten, dass niemand in China anonym im Internet Einträge veröffentlichen soll. Diese Rede hat intensive Diskussionen über das Real-Name-System herbeigeführt.

Viele Regelungen über Real-Name-System wurden damals entworfen und sind in Kraft getreten.[693]

Im Jahr 2004 begann die Webseite „Chinavalue.net", Real-Name-System auf der Webseite durchzusetzen. Das war die erste kommerzielle Webseite in China, die das Real-Name-System verwendet hat.

Im selben Jahr hatte das Bildungsministerium den „Vorschlag über die Verstärkung der Verwaltung des internen Hochschulnetzwerkes" erlassen, um das Real-Name-System im internen Hochschulnetzwerk einen Schritt weiter einzusetzen. Die Meinungsäußerung im internen Hochschulnetzwerk stand unter strenger Untersuchung und starken Beschränkungen.[694]

Am 1. 5. 2009 hatte das ständige Komitee des Volkskongresses der Stadt Hangzhou die „Administrative Verordnung zum Schutz der Informationssicherheit im Internet von der Stadt Hangzhou" erlassen. Gemäß dieser Verordnung mussten sich die Internetnutzer bei Meinungsäußerungen im Internet mit gültigen ID-Nummern registrieren. Das war die erste offizielle regionale Vorschrift in China, die das Real-Name-System festgelegt hatte. Aber weil die Verordnung nach der Erlassung zu stark kritisiert wurde, wurde sie nie wirklich durchgesetzt.[695]

Die am 16.12.2011 erlassene „Regelungen zur Verwaltung der Entwicklung des Mikrobloggings" hat auch verlangt, dass sich die Nutzer von Mikroblogging mit realen Namen registrieren sollen.

Am 26.3.2013 hat das General Büro des Staatsrats in der „Mittelung über die Verteilung der Aufgaben, um den Plan für institutionelle Reform und Transformation der Funktion des Staatsrates durchzusetzen" festgestellt, dass es die Aufgabe der Regierung im Jahr 2014 ist, das Real-Name-Registrieren-System zu verbreiten und durchzusetzen. Diese Aufgabe wird von dem Ministerium für Industrie und Informationstechnologie, National Büro für Internetinformation, Ministerium für öffentliche Sicherheit aufgenommen, und muss bis Ende Juni 2014 erledigt werden.[696]

Bis zu dieser Mitteilung wird die Durchsetzung des Real-Name-System in China fast festgestellt. Jedoch ist es immer notwendig, die Verhältnismäßigkeit des Real-Name-System zu überprüfen.

---

693 Lu Wei, Lanzhou Academic Journal 2012, No. 9, 161.

694 Wikipedia, http://en.wikipedia.org/wiki/SMTH_BBS (besucht am 04.04.2015).

695 http://it.people.com.cn/GB/42891/42894/11777005.html (besucht am 04.04.2015).

696 http://www.gov.cn/zwgk/2013-03/28/content_2364821.htm (besucht am 04.04.2015).

b) Die Verhältnismäßigkeit des Real-Name-System

aa) Der legitime Zweck des Real-Name-System

Außer dem oben genannten Zweck, dass der unmittelbare Verletzer durch Real-Name-System leichter identifiziert werden kann, und der Verletzte dadurch besser geschützt werden kann, lag der ursprüngliche Zweck des Real-Name-System auch oder mehr in der Kontrolle der Internetgewalt. Dazu gehören die im Internet umfangreich verbreiteten Handlungen wie Internet-Mobbing, Beschmutzung, Betrug, Verbrechen und anderes rechtswidriges Verhalten.[697]

Dieses Chaos kann nicht durch Selbstregulierung der Internetnutzer gelöst werden. Das Einsetzen der öffentlichen Macht ist nötig, um die Internetwelt wieder in Ordnung zu bringen.[698] Zu diesen Zwecken ist Real-Name-System als die passende Maßnahme ausgewählt worden, weil sich die Internetnutzer durch die Abschreckungsfunktion des Real-Name-System im Internet vernünftiger und vorsichtiger verhalten würden.

Das Real-Name-System dient zum legitimen Zweck.

bb) Die Geeignetheit des Real-Name-System

Hier wird diskutiert, ob das Real-Name-System geeignet ist, das Chaos im Internet wieder in Ordnung zu bringen.

Die Förderung wird hauptsächlich durch die Abschreckungsfunktion des Real-Name-System verwirklicht. Nicht zu negieren ist es, dass die Anonymität und Pseudonymität im Internet die Internetnutzer ermutigen, sich so zu verhalten wie sie es sich im realen Leben nicht trauen würden. Durch Real-Name-System wird jeder Internetnutzer mit seinem Verhalten im Internet eng verbunden. Besonders bei der Ausübung rechtswidrigen Verhaltens zwingt das Real-Name-System die Internetnutzer zu überlegen, dass sie wegen des rechtswidrigen Verhaltens genau wie im normalen Leben bestraft würden. Diese Abschreckungsfunktion würde schon eine Verminderung der rechtswidrigen Handlungen im Internet fördern.

Das Real-Name-System könnte von einem anderen Aspekt auch dem legitimen Zweck dienen, Klagen gegen den unmittelbaren rechtsverletzenden Internetnutzer zu erleichtern. Der Verletzer würde leichter identifiziert, was zur Folge hätte, dass der Verletzer für seine rechtswidrige Handlung im Internet haften müsste. Dies hilft auch die Rechtsverletzung von der Quelle an zu vermindern.

---

697 Yang Fuzhong, Studies in Law and Business 2012, No. 5, 32.

698 Gao Wenmiao, Lanzhou Academic Journal 2012, No. 3, 167, 168.

Jedoch ist es fraglich, ob die Abschreckungsfunktion wirklich funktioniert. Das Real-Name-System braucht technische Unterstützung. Ein Programm muss entwickelt werden, um das Real-Name-System zu verwirklichen. Ein Programm kann leider niemals so perfekt bzw. lückenlos sein, damit es von keinem eingehackt werden kann. Andererseits würden die meisten Internetnutzer es bevorzugen, anonym zu bleiben. Darum würde es großen Bedarf geben, das Real-Name-System zu umgehen. Für diesen Bedarf würde es auch genug Hacker geben, ein Programm für die Umgehung des Real-Name-System zu programmieren.

Übrigens würde ein verständiger Internetnutzer, der schon weiß, dass sein Verhalten rechtswidrig sein würde, auf keinen Fall dieses Verhalten unter seinem eigenen realen Namen begehen.[699] Ein Umweg würde von ihm gefunden werden. Im Gegenteil wäre es der normale Internetnutzer, der Abschreckung für seine sehr wahrscheinlich rechtsmäße Meinungsäußerung bekommt.

Das Real-Name-System würde seine erwartete Funktion nicht erreichen.[700]

cc) Die Erforderlichkeit des Real-Name-System

Hier soll diskutiert werden, ob ein milderer Weg zur Verfügung steht, Internetgewalt zu kontrollieren.

Die Abschreckungsfunktion des Real-Name-System funktioniert eigentlich dadurch, dass die Internetnutzer Angst haben sollen, leicht identifiziert zu werden, wenn sie rechtswidrige Handlungen begehen. Aber ohne Real-Name-System ist es schon möglich, durch pseudonymen Name und IP-Adresse den Verletzer zu identifizieren.[701] Das ist auch die üblichste Methode weltweit, um Verletzer oder Verbrecher im Internet zu identifizieren.

Der Unterschied zwischen IP-Identifizierung und Real-Name-System-Identifizierung ist nur, dass Real-Name-System-Identifizierung schneller sein könnte. Jedoch ist es möglich, durch andere Wege den Prozess zur Identifizierung des Verletzers zu beschleunigen. Die Gerichte in der Provinz Jiangxi haben durch ihre Praxis die Möglichkeiten erwiesen.[702]

Übrigens kann der Beklagte im offline Leben auch nicht immer sofort identifiziert werden. Es ist unmöglich, dass jeder Verletzte jeden Verletzer kennt. Eine

699 Xu Zhenzeng, Hebei Law Science 2012, No. 9, 166, 170.

700 Vgl. Yang Fuzhong, Studies in Law and Business 2012, No. 5, 32, 37-38.

701 Xu Zhenzeng, Hebei Law Science 2012, No. 9, 166, 171; Han, Ning, Legal Science Monthly 2012, No. 4, 3, 8.

702 Siehe oben unter § 11 II 2.

Reihe von Untersuchungen ist im offline Leben auch nötig, um den beklagten Verletzer zu identifizieren. Darum wäre es eine Überforderung für die Internetwelt, den Verletzer sofort finden zu müssen.

Außerdem steht schon z.B. das Notice-and-Take-Down-Verfahren zur Verfügung, damit der Verletzte eine Rechtsverletzung rechtzeitig abbrechen kann.

Um die Nicht-Erforderlichkeit des Real-Name-System zu erklären, hat ein Jurist ein Metapher erfunden: weil es Internetgewalt gäbe, müsse Real-Name-System durchgeführt werden; nach dieser Theorie, müsse jeder schon seinen Namen, ID-Nummer auf die Stirn schreiben, weil es im offline Leben auch Gewalt geben könnte.[703]

Nach alledem ist ein Real-Name-System nicht erforderlich.

dd) Die Angemessenheit des Real-Name-System

Hier wird geprüft, ob die Nachteile des Real-Name-Systems völlig außer Verhältnis gegenüber den Vorteilen stehen.

(1) Bewertung über die Abschreckungsfunktion des Real-Name-Systems

Das Real-Name-System könnte im Internet eine Situation schaffen, in der die Meinungsäußerung viel stärker als im offline Leben beschränkt wird, weil alle im Internet eingetragenen Inhalte gespeichert und zur Abrufung bereitgestellt werden. Wenn das Real-Name-System durchgeführt würde, könnte jedes Wort, das ein Internetnutzer im Internet eingetragen hat, unter seinem Namen aufgenommen werden und in der Zunft als Beweis gegen ihn verwendet werden. Im offline Leben wird auf keinen Fall jedes Gespräch aufgenommen.

Es ist vorstellbar, dass der Internetnutzer bei der Meinungsäußerung sehr vorsichtig sein wird und viel überlegen muss, um einen Fehler zu vermeiden, der in der Zukunft zu einer Haftung für ihn führen könnte. Die Abschreckungsfunktion erstreckt sich nicht nur auf die Äußerung der rechtswidrigen Inhalte, sondern auch auf die der rechtmäßigen Inhalte.

Besonders zu erwähnen ist es, dass die Abschreckungsfunktion des Real-Name-Systems auch dazu führen könnte, dass die Denunziation der Korruptionen durch das Internet nicht mehr oder seltener funktioniert, was in der letzter Zeit eine wichtige bzw. hauptsächliche Methode zur Ausübung des Aufsichtsrechts chinesischer Bürger über die Beamten ist. Das Aufsichtsrecht von den Bürgern über die Beamten ist gemäß § 41 chinesisches Verfassungsgesetz

703 Zhou Yongkun, Jinan Journal (Philosophy and Social Sciences) 2013, No. 2, 1, 5.

ein Grundrecht der chinesischen Bürger. Die Daten zeigen, dass 80% der Korruption in China unmittelbar durch anonyme Denunziation der Bürger aufgedeckt wurden.[704] Es herrscht die Meinung von einem Beamtem aus der Höchsten Staatsanwaltschaft, dass tatsächlich 100% der Korruption in China durch unmittelbare und mittelbare anonyme Denunziation der Bürger aufgedeckt sind.[705] In der letzten Zeit ist die Häufigkeit der anonymen Online-Denunziation um das 8 fache gestiegen.[706]

Wenn das Real-Name-System durchgesetzt werden würde, würden anonyme Denunziationen schlecht möglich sein, weil der Denunziant Angst haben würde, dass er nach der Denunziation von demjenigen Beamten gerächt wird, bevor er aufgrund der Korruption seine Macht verliert. Das wäre offensichtlich eine Beschränkung des Aufsichtsrechts des Volkes.[707]

(2) Real-Name-System erhöht das Risiko vom Durchsickern der persönlichen Informationen

Die Hauptgefahr vom „Leak" der Informationen kommt nicht von normalen Internetnutzern sondern aus den Hackerkreisen. Am Ende des Jahres 2011 gab es ein Ereignis des Durchsickerns der registrierten Daten beim CSDN (Chinese Software Developer Network). CSDN wurde Opfer eines Hackerangriffs; eine Datenbank mit den Informationen von 6 Millionen bei CSDN registrierten Internetnutzern, einschließlich ihrer Nutzernamen, Passwörter, registrierten Email-adressen, wurden im Internet offengelegt.[708] Jedoch ist das nur ein kleines Beispiel. Fast alle bekannten großen Webseiten in China wurden bereits Opfer von Hackerangriffen. Es ist deswegen nicht unvorstellbar, dass die Datenbank des Real-Name-System mit allen realen Informationen der Internetnutzer das Ziel von Hackern sein würde, weil diese Informationen ein hohes wirtschaftliches Interesse herbeiführen können. Die Durchsetzung vom Real-Name-System hat ohne Zweifel die persönlichen Informationen der Internetnutzer an das

704 Jiang Zengpei, Dong fang wang, http://www.jxnews.com.cn/jxcomment/system/2008/01/02/002647086.shtml (besucht am 04.04.2015).

705 Song Wei/Tan Jing/Guo Peng, Zheng yi wang, 02.07.2008, http://news.xinhuanet.com/legal/2008-07/02/content_8473380.htm (besucht am 04.04.2015).

706 Zhou Yongkun, Jinan Journal (Philosophy and Social Sciences) 2013, No. 2, 1, 4; siehe auch http://www.cctvxwpd.com/detail.asp?id=6516 (besucht am 04.04.2015).

707 Yang Fuzhong, Studies in Law and Business 2012, No. 5, 32, 33.

708 Qi Aimin, Chinese Social Sciences Today, 02.04.2012, S. A07; siehe auch http://en.wikipedia.org/wiki/CSDN (besucht am 04.04.2015).

Messer des Hackers geliefert.[709] Es ist auch nicht zu vernachlässigen, dass manche Unternehmen aufgrund ihrer wirtschaftlichen Interessen auch am Sammeln und Verkaufen persönlicher Daten interessiert sind, was ebenfalls die Sicherheit der Datenbank gefährdet.[710]

Übrigens ist die Datenbank des Real-Name-System in Bezug auf Undichtigkeiten und Durchsickern der Informationen völlig anders zu betrachten als die Datenbank mit registrierten Informationen der Internetnutzer von einer Webseite. Wenn z.B. die Datenbank von einem Sozialnetzwerk undicht ist, kann man durch einfaches Ändern des Benutzernamens, des Passwortes und der Emailadresse den weiteren Schaden vermeiden. Aber wenn die Datenbank des Real-Name-Systems einmal offengelegt ist, können die persönlichen Daten nicht mehr zurückgezogen werden. Und es ist fast unmöglich, den realen Namen und die ID-Nummer aller Personen zu ändern. Durch die Änderung würden auch riesige Kosten für die Personen und den Staat entstehen. Also ein „Leak" in der Datenbank des Real-Name-System wäre eine pure Katastrophe.

(3) Real-Name-System ermöglicht den Missbrauch der persönlichen Daten durch den Staat

Wie oben bereits gesagt wurde, muss die Datenbank für Real-Name-System stabil genug sein, um vor einem Eingriff durch Hacker geschützt zu sein. Die Datenmenge unter Berücksichtigung der Gesamtbevölkerung Chinas muss übrigens auch dazugerechnet werden. Für die Entwicklung eines solchen Systems kann der normale ISP offensichtlich nicht leisten.[711] Die Aufgabe muss vom Staat übernommen werden.[712] Tatsächlich hat die chinesische Regierung auch aktiv diese Aufgabe übernommen.[713] Das führt dazu, dass der Staat die Informationen, wann wer was im Internet eingetragen hat, sammeln kann. Es ist anzumerken, dass China bisher noch kein Datenschutzgesetz hat. Unter diesem Umstand besteht die hohe Gefahr, dass der Staat die Informationen missbraucht, weil es keine Regelungen gibt, wie der Staat die gesammelten Informationen verwenden soll. Der Missbrauch besteht besonders darin, dass der Staat mittels Real-Name-System das online Verhalten des Volkes überwacht.[714]

709 Vgl. Han, Ning, Legal Science Monthly 2012, No. 4, 3, 7, 9.
710 Zhou Yongkun, Jinan Journal (Philosophy and Social Sciences) 2013, No. 2, 1, 4.
711 Lu Wei, Lanzhou Academic Journal 2012, No. 9, 161, 164.
712 Wang Gang, The Time Weekly, 09.01.2012.
713 http://www.gov.cn/zwgk/2013-03/28/content_2364821.htm (besucht am 04.04.2015).
714 Zhou Yongkun, Jinan Journal (Philosophy and Social Sciences) 2013, No. 2, 1, 3.

(4) Real-Name-System ist schädlich für die Erziehung des demokratischen Gedankens und die soziale Sicherheit

Anonymität ist eine grundsätzliche Voraussetzung für die Entwicklung der Demokratie.[715] Der Politiker hat naturgemäß die Angst, aufgrund seiner politischen Meinung gerächt zu werden. Anonymität kann diese Angst des Politikers am besten vermindern.[716] Das ist auch der wesentliche Grund, warum eine Abstimmung immer anonym ist.[717] Das gilt auch für die Demokratie im Internet. Wegen der mangelnden Möglichkeiten zur Teilnahme an der Politik oder anderer staatlichen Angelegenheiten hat das Internet ein Feld geschaffen, um dort den demokratischen Gedanken zu erziehen und um manchmal sogar unmittelbar an der Politik teilzunehmen.[718] Der Hauptgrund liegt darin, dass die Internetnutzer wegen der Anonymität im Internet ihre Meinungen relativ frei äußern können. Die Durchsetzung des Real-Name-System hat den Weg der demokratischen Entwicklung im Internet gesperrt.

Die anonyme öffentliche Diskussion ermöglicht den Menschen auch, ihre Unzufriedenheit mit der Regierung auszudrücken. Das dadurch entstandene „Ventil" wird vom Volk genutzt, um schlechte Laune abzulassen, was wiederum mehr Sicherheit in die Gesellschaft bringt. Das Blockieren oder die Beschränkung der anonymen öffentlichen Diskussion könnte langsam zu einem Vulkanausbruch ähnlichen Bewegung führen, um eine freie Meinungsäußerung von der Regierung zu erlangen.[719]

(5) Das Vorbild von Südkorea ist als ein Fehler erwiesen

Anonymität im Internet ist das übliche Prinzip auf der Welt. Die meisten Länder haben das Prinzip akzeptiert. Südkorea ist eine Ausnahme, die China immer als Vorbild genommen hat. Aber auch die Praxis in Südkorea hat schon bewiesen, dass das Real-Name-System nicht funktioniert.[720] Am 23.08.2012 hat das Verfassungsgericht in Südkorea entschieden, dass das Real-Name-System ver-

715 Xu Zhenzeng, Hebei Law Science 2012, No. 9, 166, 167.
716 Xu Zhenzeng, Hebei Law Science 2012, No. 9, 166, 167.
717 Xu Zhenzeng, Hebei Law Science 2012, No. 9, 166, 168; Wang Zhigang, Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition) 2006, No. 6, 46, 47f.
718 Xu Zhenzeng, Hebei Law Science 2012, No. 9, 166, 171.
719 Vgl. Yang Fuzhong, Studies in Law and Business 2012, No. 5, 32; Xu Zhenzeng, Hebei Law Science 2012, No. 9, 166, 169; Han, Ning, Legal Science Monthly 2012, No. 4, 3, 9; Zhou Yongkun, Jinan Journal (Philosophy and Social Sciences) 2013, No. 2, 1, 4.
720 Zhou Yongkun, Jinan Journal (Philosophy and Social Sciences) 2013, No. 2, 1, 2.

fassungswidrig ist. Aufgrund dieser Entscheidung wird das Real-Name-System in 5 Jahren in Südkorea abgeschafft.[721] Der erfolglose Versuch Südkoreas sollte für China eine Warnung sein.[722]

ee) Zwischenergebnis

Internetgewalt ist nach allem nur ein kleiner Teil der Internetwelt, die auch durch mildere Wege als Real-Name-System vermindert werden kann. Nur um die Internetgewalt ein bisschen schneller und einfacher zu lösen, aber deswegen eine ganze Reihe von Nachteile hingenommen werden müssen, besonders dass die Meinungsfreiheit des ganzen Volks beschränkt werden muss, ist die Durchführung eines nicht unbedingt funktionierten Real-Name-System nicht verhältnismäßig.[723]

2. Real-Name-System in Deutschland

Anonymität und Pseudonymität im Internet ist in Deutschland gesetzlich anerkannt und garantiert. Gemäß § 13 Abs. 6 TMG hat der Dienstanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Aber im Gegensatz zur überwiegende intensiven Kritik gegen Real-Name-System in China, gibt es in der deutschen Literatur die Tendenz, die Anonymität im Internet einigermaßen zu beschränken.

a) Kein Grundrecht auf Anonymität

Über die Grundlage der Anonymität gibt es in der Literatur unterschiedliche Meinungen. Zum einen existiert die Meinung, dass es bei der Meinungsäußerung das Grundrecht auf Anonymität gibt, das seine Grundlage in Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 sowie Art. 5 Abs. 1, 10 und 13 GG findet.[724] Zum anderen existiert eine Meinung, die für ein eigenständiges Grundrecht auf Anonymität keinen Bedarf sieht, weil das Recht auf informationelle Selbstbestimmung zum Schutz der Internetnutzer vor Ausspähung ausreicht.[725] Allerdings stimmt die Meinung für ein Grundrecht auf Anonymität zu, dass das Grundrecht auf Anonymität mit dem Recht auf informationelle Selbstbestimmung korrespondiert,

721 Wikipedia, http://en.wikipedia.org/wiki/Real-name_system (besucht am 04.04.2015).
722 Zhou Yongkun, Jinan Journal (Philosophy and Social Sciences) 2013, No. 2, 1, 7.
723 Han, Ning, Legal Science Monthly 2012, No. 4, 3, 9; Lu Wei, Lanzhou Academic Journal 2012, No. 9, 161, 163.
724 Heckmann, NJW 2012, 2631, 2632.
725 Spindler, GRUR 2013, 996, 1001.

wonach jeder Internetnutzer selbst entscheiden können soll, wer erfährt, welche Handlungen von ihm stammen.[726]

Meiner Meinung nach ist ein Grundrecht auf Anonymität in Deutschland nicht begründet. § 13 Abs. 6 TMG hat dem ISP die Möglichkeit gegeben, die Anonymität oder die Pseudonymität für seinen Dienst auszuwählen. Wenn sich der ISP für die Pseudonymität entscheidet, hat der Nutzer keinen Anspruch auf anonymisierte Benutzung des Dienstes, wenn er eigenständig den Dienst des ISP in Anspruch nimmt. Gemäß § 13 Abs. 6 TMG ist es durchaus möglich und rechtmäßig, dass jeder ISP in Deutschland statt der Anonymität die Pseudonymität für seinen Dienst durchführt, obwohl in der Praxis die Gefahr bestehen könnte, dass er deswegen seine Kunden verliert. Wenn es bei dem Grundrecht auf Anonymität auf die freie Entscheidung des ISP ankommt, ist nicht nachvollziehbar, dass es noch ein Grundrecht ist.

b) Die Einschränkung der Anonymität im Internet

Nach der aktuellsten Entwicklung in der Literatur ist es schon allgemein anerkannt, dass die Anonymität im Internet eingeschränkt werden soll.[727] Über den Grad der Einschränkung gibt es jedoch unterschiedliche Meinungen.

Es herrscht die Meinung, dass eine allumfassende anlasslose Identifizierung der Nutzer im Internet zu vermeiden ist.[728] Dennoch soll der ISP für besonders gefahrgeneigte Dienste verpflichtet sein, die Identität ihrer Nutzer zu verifizieren, ausreichend auch in pseudonymer Form,[729] um den Auskunftsanspruch im Fall der Rechtsverletzung zu garantieren.[730]

Er herrscht auch die Meinung, dass alle Internetnutzer, die aktiv Informationen im Netz veröffentlichen, dies in pseudonymer Form (oder unter Klarnamen) tun müssen.[731] Anonymisiert sind dagegen nur die Nutzer, die das Internet passiv als Informationsquelle nutzen.

---

726 Heckmann, NJW 2012, 2631, 2632.

727 Spindler, GRUR 2013, 996; Herwig, ZD 2012, 558; Dix, Zitat aus: Begleitheft zum Deutschen Juristentag 2012, Thesen der Gutachter & Regerenten, S. 70 ff, abrufbar unter: http://www.djt.de/fileadmin/downloads/69/120809_djt_69_thesen_web.pdf. (besucht am 04.04.2015).

728 Spindler, GRUR 2013, 996, 1001.

729 Spindler, GRUR 2013, 996, 1001.

730 Spindler, NJW-Beil. 2012, 98, 99.

731 Dix, Zitat aus: Begleitheft zum Deutschen Juristentag 2012, Thesen der Gutachter & Regerenten, S. 70 ff, abrufbar unter: http://www.djt.de/fileadmin/downloads/69/120809_djt_69_thesen_web.pdf. (besucht am 04.04.2015).

Es herrscht weiterhin die Meinung, dass der ISP selbst entscheiden soll, ob er die Anonymität oder Pseudonymität für seinen Dienst wählt. Wenn der ISP seinen Dienst für die Nutzer aktiv anonymisiert, kann er theoretisch den Auskunftsanspruch des Verletzten im Fall der Rechtsverletzung nicht mehr erfüllen.[732] In diesem Fall muss er die anonymisierten Inhalte stärker kontrollieren und für die rechtswidrigen Inhalte als ICP haften.[733] Wenn der ISP dagegen Pseudonymität von seinen Nutzern verlangt und ggf. den Verletzten über die Identität der rechtsverletzenden Nutzer informieren kann, haftet er im Fall der Rechtsverletzung nur als Störer.[734]

Am Fall der Menschenfleischsuche kann man deutlich sehen, dass nicht nur das Verhalten des Nutzers, der aktiv Informationen veröffentlicht, sondern auch das des Nutzers, der das Internet als Informationsquelle passiv verwendet, Rechtsverletzungen begründen kann. Durch diesen Standard die Anonymität und Pseudonymität zu unterscheiden ist meiner Meinung nach unpraktisch.

Die anderen zwei Meinungen können meiner Meinung nach kombiniert betrachtet werden. Für den besonders gefahrgeneigten Dienst, in dem Rechtsverletzungen häufig auftauchen, ist es für den ISP vernünftiger, von den Nutzern zu verlangen, sich unter einem Pseudonym zu registrieren, bevor sie im Internet aktiv werden. Das Problem liegt nur darin, ob dies vom ISP frei entschieden werden kann[735] oder als eine Pflicht durchgeführt wird[736]. Um diese Frage zu beantworten, soll Perspektive des ISP und des möglichen Verletzten betrachtet werden.

Wenn sich der ISP statt für Pseudonymität für Anonymität entscheidet, muss er mehr Pflichten bezüglich der Überwachung der Inhalte auf seiner Webseite haben, um die möglichen Verletzungen zu vermeiden, für die er als unmittelbarer Verletzer (ICP) haften müsste, obwohl er dafür mehr Nutzer bekommen könnte, weil die vernünftigen Nutzer es bevorzugen, anonym zu bleiben. Die Kosten für die allgemeine Überwachung und das Risiko, für die Rechtsverletzung seiner Nutzer unmittelbar zu haften, können schwerwiegender sein. Jedoch darf sich der ISP nach seiner freiwilligen Abwägung auch für die Anonymität entscheiden, weil kein überwiegend zu schützendes Interesse anzunehmen ist. Der Schutz der Verletzten führt auch nicht zu einem Verbot des anonymisierten Dienstes, weil der Verletzte in diesem Fall direkt Ansprüche

732 Herwig, ZD 2012, 558, 560.
733 Herwig, ZD 2012, 558, 562.
734 Herwig, ZD 2012, 558, 560.
735 Herwig, ZD 2012, 558, 562.
736 Spindler, GRUR 2013, 996, 1001.

gegen den ISP bzw. den ICP geltend machen kann, was für den Verletzten einfacher und praktischer ist.

Nach meiner Meinung soll der ISP nicht gezwungen werden, Pseudonymität für seinen Dienst durchzuführen. Aber die Möglichkeit, im Fall der Rechtsverletzung einen Rechtsanspruch direkt gegen den Provider zu verlangen, soll garantiert werden. Wenn anonymisierte Einträge auf seiner Webseite zur Rechtsverletzung führen, soll der ISP wegen Zueigenmachen verantwortlich sein.[737] Müsste er ständig deswegen haften, würde er schon automatisch die Pseudonymität seines Diensts bevorzugen.

3. Ein Vergleich zwischen Deutschland und China

Obwohl in Deutschland auch versucht wird, die Anonymität zu beschränken und in manchen Fällen die Identität der Internetnutzer zu verifizieren, ist es immer noch anders als das Real-Name-System in China.

Der Unterschied liegt erstens darin, dass die Beschränkungen der Anonymität in Deutschland durch die ISP durchgeführt werden oder werden sollen, während die Durchführung des Real-Name-System in China die Aufgabe der Regierung ist.

Der Unterschied liegt weiterhin darin, dass die Beschränkung der Anonymität in Deutschland rechtsverletzungs-orientiert ist. Nach den Vorschlägen der Juristen ist die Beschränkung nur für besonders gefahrgeneigte Dienste oder aktive Veröffentlichung der Informationen höchst notwendig, wodurch Rechtsverletzungen leicht entstehen. In China wird das Real-Name-System allgemein und umfassend durchgeführt.

Der letzte Unterschied liegt darin, dass es in Deutschland entwickelte und ausführliche Datenschutzgesetze gibt, durch die man den Missbrauch der Daten der Internetnutzer durch den Staat vermeiden kann, während es in China nur eine Informationsschutz-Entscheidung gibt, die 12 schwache Paragraphen beinbehaltet. Bei der Durchführung des Real-Name-System unter diesem Umstand besteht eine hohe Gefahr des Datenmissbrauchs durch den Staat.

Jedoch ist es auch in China zu empfehlen, Pseudonymität für die aktive Teilnahme an der Menschenfleischsuche durchzuführen, um im Fall von Rechtsverletzung die Identifizierung des unmittelbaren Verletzers zu ermöglichen.

737 Siehe oben unter § 9 I 1.

§ 12 Rechtsansprüche gegen den ISP als Störer

I. Nach deutschem Recht

1. Die Reihenfolge der Ansprüche gegen den Internetnutzer als unmittelbarer Verletzer und den ISP als Störer

Im Jahr 2006 hat das OLG Düsseldorf in seiner Rechtsprechung die Anonymität der rechtswidrigen Einträge als Kriterium für das Bestehen eines Unterlassungsanspruchs gegen den ISP entschieden.[738] Das bedeutet, der Kläger muss die Reihenfolge seines Anspruchs gegen den unmittelbaren Verletzer und den ISP vor Gericht einhalten. Eine direkte Klage gegen den ISP ist erst möglich, wenn der unmittelbare Verletzer wegen Anonymität unbekannt ist. Das OLG Düsseldorf hat einmal einen gegen den ISP gestellten Unterlassungsanspruch abgelehnt, weil der Autor der rechtswidrigen Inhalte dem Verletzten bekannt war, und der Verletzte somit gegen den Autor vorrangig vorgehen könne.[739] Umgekehrt hat das Gericht einen Unterlassungsanspruch bejaht, weil der Verletzer anonym war, und der Provider dessen Identität nicht preisgab.[740]

Diese Entscheidungen haben von der Literatur viele Kritiken bekommen. Der BGH hat durch sein Urteil vom 27.03.2007 eine völlig andere Meinung dargelegt. Aufgrund dieser Rechtsprechung gibt es zwischen dem Provider und dem Äußernden in einem Meinungsforum keinen Anspruchsvorrang.[741] Gegen wen der Betroffenen seinen Anspruch geltend machen soll, „liegt allein im Ermessen des Betroffenen, wie er effizient seine Rechte verfolgt".[742] Die zivilrechtliche Verantwortlichkeit des Providers für die auf seiner Webseite eingestellten Beiträge entfällt nicht deshalb, weil dem Verletzten die Identität des Äußernden bekannt ist.[743]

Auch diese Rechtsprechung wurde nicht problemlos akzeptiert. Es herrscht die Meinung, dass das Fehlen des Subsidiaritätsgrundsatzes zwischen den Ansprüchen gegen den Provider und den unmittelbaren Verletzter zur Folge hat, dass der Weg von einer direkten Auseinandersetzung zwischen den Konfliktparteien (der

738 OLG Düsseldorf, CR 2007, 588.
739 OLG Düsseldorf, CR 2007, 588.
740 OLG Düsseldorf, CR 2007, 588.
741 BGH, CR 2007, 586, 589.
742 BGH, CR 2007, 586, 589.
743 BGH, CR 2007, 586, 587.

Verletzte und der Äußernde) gesperrt worden ist.[744] Diese Sperrung dient erstens nicht dazu die Rechtsverletzung von der Quelle an zu vermindern; sie führt zweitens dazu, dass sich der ISP als ein „Ersatz"-Richter verhalten muss, wozu er nicht unbedingt in der Lage ist.[745] Der zweite Aspekt wird im Folgenden diskutiert.

2. Die Störerhaftung des ISP

Oben unter § 10 I 2 sind die Voraussetzungen einer Störerhaftung ausgeführt worden. Sind die Voraussetzungen erfüllt, muss der ISP als Störer haften. Wegen einer Persönlichkeitsrechtsverletzung kommen die Beseitigungs- und Unterlassungsansprüche in Frage, die ihre Grundlage in § 1004 BGB finden.[746]

a) Die Beseitigungs- und Unterlassungsansprüche fallen nicht unter die Haftungsprivilegierung des § 10 Satz 1 TMG

Vor einer ausführlichen Diskussion über Beseitigungs- und Unterlassungsansprüche muss erst die Frage beantwortet werden, ob die Beseitigungs- und Unterlassungsansprüche unter die Haftungsprivilegierung des § 10 Satz 1 TMG fallen. Wäre die Frage zu bejahen, bräuchte der ISP für den Fall der Unschuld, also Unkenntnis der rechtswidrigen Handlung oder der rechtswidrigen Information, überhaupt nicht haften. Das heißt, auch die Beseitigungs- und Unterlassungsansprüche gegen ihn wären in diesem Fall erfolglos.

Aber der BGH hat durch seine Entscheidung „Internetversteigerung I" diese Möglichkeit verneint. Seiner Meinung nach erfasst die Haftungsprivilegierung des Art. 14 Abs. 1 RL 2000/31/EG (korrespondiert mit § 10 Satz 1 TMG, damals umgesetzt durch § 11 Satz 1 TDG 2001), nicht die Beseitigungs- und Unterlassungsansprüche.[747] Der Grundgedanke liegt im Satz 2 des § 11 TDG n. F., dass die „Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen… auch im Falle der Nichtverantwortlichkeit des Dienstanbieters nach den §§ 9 bis 11 unberührt bleiben".[748]

Meiner Meinung nach kann man im § 10 TMG selbst die Antwort finden. Ab dem Zeitpunkt, wenn ein Beseitigungs- oder Unterlassungsanspruch gegen den ISP erhoben wird, erhält der ISP die Kenntnisnahme über die rechtswidrige Handlung oder Information. Es begründet tatsächlich die Kenntnisnahme i.S.v.

744 Spindler, CR 2012, 176, 178.
745 Spindler, CR 2012, 176, 178.
746 Spindler/Anton in Spindler/Schuster, § 1004 BGB, Rn. 2.
747 Rössel, CR 2011, 589, 590; vgl. auch BGH, CR 2008, 579; BGH, MMR 2007, 507.
748 BGH, GRUR 2004, 860, 863.

§ 10 Satz 1 Nr. 2 TMG, nach der der ISP die rechtswidrige Handlung oder Information unverzüglich beseitigen muss. Eine Unkenntnis bzw. Unschuld des ISP könnte höchstens bis zum Zeitpunkt existieren, bevor ein Beseitigungs- oder Unterlassungsanspruch gegen ihn gestellt wird. Danach hat er keinen Grund mehr, einen Beseitigungs- oder Unterlassungsanspruch abzuwehren. Eine Privilegierung beider Ansprüche ist demnach sinnlos.

§ 1004 BGB gewährt dem Verletzten einen verschuldensunabhängigen Beseitigungs- und Unterlassungsansprüche gegen den ISP.[749]

b) Beseitigungsanspruch

Wie bereits ausgeführt worden ist, ist ein ISP nicht verpflichtet, die von seinen Nutzern auf die Webseite gestellten Beiträge vor der Veröffentlichung auf eventuelle Rechtsverletzungen hin zu überprüfen.[750] Aber sobald er Kenntnis von der Rechtsverletzung erlangt, entsteht die Verantwortlichkeit.[751] Die Verantwortlichkeit zeigt sich im Fall vom Beseitigungsanspruch als eine Pflicht, die in Frage gestellten Einträge zu löschen oder zu sperren, um die Rechtsverletzung zu beseitigen. Anders als ein Unterlassungsanspruch richtet sich der Beseitigungsanspruch auf die Beendigung der gegenwärtigen Störung.[752]

Der Beseitigungsanspruch bedeutet nach der Rechtsprechung des BGH aber nicht, dass der ISP auf jedes Verlangen des Betroffenen aktiv werden muss, die der Rechtsverletzung verdächtigten Einträge zu löschen.[753] Sonst würde die Meinungsfreiheit der Äußernden überhaupt nicht geschützt. Durch ein Urteil im Jahr 2011 hat der BGH festgestellt, dass ein Tätigwerden des Providers erst veranlasst wird, wenn die Behauptung des Betroffenen so konkret gefasst ist, dass der Rechtsverstoß „unschwer - das heiß ohne eigehende rechtliche und tatsächliche Überprüfung- bejaht werden kann".[754] Dieses vom BGH entwickelte Prinzip korrespondiert mit § 10 Satz 1 Nr. 2 TMG, in dem das auf EU-Ebene gerade heftig diskutierte „Notice-and-Take-Down"-Verfahren vorliegt.[755]

---

749 Spindler/Anton in Spindler/Schuster, § 1004 BGB, Rn. 1.
750 BGH, K&R 2012, 110, 113.
751 BGH, K&R 2012, 110, 113.
752 Spindler/Anton in Spindler/Schuster, § 1004 BGB, Rn. 13; BGHZ 28, 110, 113 = NJW 1958, 1580, 1581; Bassenge in Palandt, § 1004 BGB Rn. 28; Fritzsche in Bamberger/Roth, § 1004 BGB Rn. 56.
753 BGH, K&R 2012, 110, 113.
754 BGH, K&R 2012, 110, 113.
755 Hoeren, MMR 2012, 124, 127.

Das „Notice-and-Take-Down"-Verfahren stammt aus den USA. Aufgrund Section 512 (c) des US-amerikanischen Digital Millenium Copyright Act 1998 (DMCA) muss der Provider den beanstandeten Inhalt nach Eingang einer Beschwerde des Betroffenen sofort sperren.[756] Im Anschluss muss er dem verdächtigen Verletzer nach Section 512 (g) DMCA Gelegenheit zur Stellungnahme geben.[757] Erhebt der Betroffene auf diese Stellungnahme hin innerhalb einer Frist von zehn Tagen Klage, bleibt der beanstandete Inhalt gesperrt.[758] Sieht der Betroffene von einer Klage ab, wird die Sperrung wieder aufgehoben.[759]

Aber statt dem „Notice-and-Take-Down"-Verfahren hat der BGH in diesem Urteil ein sogenanntes „Notice-and-Action"-Verfahren (oder „Quasi-Notice-and-Take-Down"-Verfahren[760]) entwickelt,[761] das von der Europäischen Kommission in ihrer Mitteilung zum elektronischen Geschäftsverkehr und zu anderen Online-Diensten von Januar 2012 anerkannt wurde.[762] Der Unterschied zwischen diesen zwei Verfahren liegt darin, dass das „Notice-and-Action"-Verfahren nicht zu einer sofortigen Sperrung der beanstandeten Inhalte, sondern lediglich zu einer Untersuchung des beanstandeten Sachverhalts führt.[763] Dieses „Notice-and-Action"-Verfahren wird in der Literatur auch als Kommunikationsprozess bezeichnet.[764]

aa) Der Vorgang des Kommunikationsprozesses

Falls dem Provider unklar ist, ob die Beanstandung des Betroffenen annahmebedürftig ist, ist eine Ermittlung und Bewertung des gesamten Sachverhalts unter Berücksichtigung einer etwaigen Stellungnahme des Äußernden erforderlich.[765] Der Ermittlungs- bzw. Bewertungsprozess läuft wie folgt[766]:

---

756 Rühl, LMK 2012, 338417.
757 Rühl, LMK 2012, 338417.
758 Rühl, LMK 2012, 338417.
759 Rühl, LMK 2012, 338417.
760 Spindler, CR 2012, 176, 178.
761 Rühl, LMK 2012, 338417.
762 Rühl, LMK 2012, 338417.
763 Rühl, LMK 2012, 338417.
764 Feldmann, K&R 2012, 113, 115.
765 BGH, K&R 2012, 110, 113.
766 BGH, K&R 2012, 110, 113.

(a) Zunächst ist die Beanstandung des Betroffenen an den verdächtigen Verletzer zur Stellungnahme weiterzuleiten.
(b) Bleibt eine Stellungnahme innerhalb einer nach den Umständen angemessenen Frist aus, ist von der Berechtigung der Beanstandung auszugehen und der beanstandete Eintrag zu löschen.
(c) Stellt der verdächtige Verletzer die Berechtigung der Beanstandung substantiiert in Abrede und ergeben sich deshalb berechtigte Zweifel, ist der Provider grundsätzlich gehalten, dem Betroffenen dies mitzuteilen und ggf. Nachweise zu verlangen, aus denen sich die behauptete Rechtverletzung ergibt.
(d) Bleibt eine Stellungnahme des Betroffenen aus oder legt er ggf. erforderliche Nachweise nicht vor, ist eine weitere Prüfung nicht veranlasst.
(e) Ergibt sich aus der Stellungnahme des Betroffenen oder den vorgelegten Belegen auch unter Berücksichtigung einer etwaigen Äußerung des verdächtigen Verletzer eine rechtswidrige Verletzung des Persönlichkeitsrechts, ist der beanstandete Eintrag zu löschen.

Wegen der Erfindungen dieses außergerichtlichen schlichtungsähnlichen Prozesses wurde das Urteil spontan als „legendär" bezeichnet.[767] Der Pressesenat des BGH hat mit diesem Prozess ein neues Haftungsmodell für die Internetwelt entwickelt.[768] Aufgrund der Entscheidung sind nicht nur Verhaltenspflichten für den Provider, sondern auch die für den Betroffenen und den Äußernden beim Streitfall eingerichtet.[769]

Der Provider soll den Kommunikationsprozess zwischen den Betroffenen und den Äußernden durchführen. Darauf sollen der Betroffene und der Äußernde demgemäß reagieren. Der Betroffene muss nicht nur die Tatsache der Veröffentlichung eines rechtswidrige Drittinhaltes dem Provider mitteilen, sondern auch begründen, aus welchen Gründen die Information rechtswidrig ist.[770] Dem entsprechend muss sich der Äußernde für seine Äußerung verteidigen. Für den Streitfall muss er sein berechtigtes Interesse begründen. Zum Schluss soll der Provider entweder dem Äußernden oder dem Betroffenen den Vorzug geben.[771] Der Provider ist „nicht lediglich Moderator und Vermittler dieses Kommunikationsprozesses", „sondern eine Art Schiedsrichter in einer Auseinandersetzung".[772]

767 Feldmann, K&R 2012, 113, 114.
768 Hoeren, MMR 2012, 124, 127.
769 Feldmann, K&R 2012, 113, 114.
770 Feldmann, K&R 2012, 113, 114.
771 Feldmann, K&R 2012, 113, 115.
772 Feldmann, K&R 2012, 113, 115.

Dieser Kommunikationsprozess ist die aktuellste Methode, um den Beseitigungsanspruch im Fall einer Persönlichkeitsrechtsverletzung während der Menschenfleischsuche durchzuführen. Seiner Anwendung stehen jedoch viele Kritiken gegenüber.

bb) Die Kommentare über den Kommunikationsprozess

(1) Die Gefahr der extra entstehenden Pflichten und Kosten des ISP

Um die Aufgabe des ISP im Kommunikationsprozess zu beschreiben, hat der BGH einige unbestimmbare Ausdrücke verwendet, wie z.B. „substantiierte" Gegenäußerung, „berechtigte Zweifel"[773]. Solche Ausdrücke sind relativ subjektiv und umfangreich, die von jedem unterschiedlich beurteilt werden könnten.[774] Um den Kommunikationsprozess durchzuführen ist eine Prüfung der zu beanstandenden Inhalte vom ISP unvermeidlich.[775] Wegen der Unbestimmbarkeit des Beurteilungsstandards ist es in der Praxis für den ISP häufig schwer einzuschätzen[776], ob eine Rechtsverletzung vorliegt. Hierdurch würden den Provider komplexe Prüfungspflichten treffen.[777]

Die Prüfungspflicht während des Kommunikationsprozesses kann nicht durch Computerprogramme automatisiert werden. Um die komplexe Anforderung des BGH zu erfüllen, muss der ISP während des Betriebs der Webseite passende beschwerdebezügliche Verfahren entwickeln.[778] „Dazu gehört möglicherweise die Entwicklung spezieller Formulare, die Einrichtung von Beschwerdestellen und die Einstellung neuer Mitarbeiter".[779] Dies bedeutet für den Provider eine deutliche Mehrbelastung und eine enorme Kostensteigerung.[780]

Jedoch hat der BGH in der Entscheidung „Jugendgefährdende Medien bei eBay" ausdrücklich klargestellt, dass „keine Anforderungen auferlegt werden (dürfen), die (ein) von der Rechtsordnung gebilligtes Geschäftsmodell gefährden oder (die) Tätigkeit unverhältnismäßig erschweren".[781]

773 BGH, K&R 2012, 110, 113.
774 Vgl. Hoeren, MMR 2012, 124, 127.
775 Rühl, LMK 2012, 338417.
776 Spindler, CR 2012, 176, 178.
777 Hoeren, MMR 2012, 124, 127.
778 Rühl, LMK 2012, 338417.
779 Rühl, LMK 2012, 338417.
780 Rühl, LMK 2012, 338417.
781 BGH, K&R 2007, 517 ff.

Ob die Pflicht des ISP im Kommunikationsprozess sein Geschäftsmodell gefährdet oder seine Tätigkeit unverhältnismäßig erschwert, hängt mindestens davon ab, wie oft die Rechtsverletzungen passieren und wie oft die Betroffenen diese beanstanden. Weil der Kommunikationsprozess in der Praxis noch nicht umfangreich durchgesetzt ist, kann man diese Frage nicht überzeugend beantworten. Klar ist aber, dass die Anzahl der von den Internetnutzern begangenen Verletzungen hier ein entscheidendes Element ist. Um den Kommunikationsprozess vernünftig durchzusetzen, und gleichzeitig das Geschäftsmodell des ISP nicht zu gefährden oder seine Tätigkeit nicht unverhältnismäßig zu erschweren, ist ein Mechanismus zu überlegen, der die Rechtsverletzungen von der Quelle an vermindert.

(2) Die Gefahr einer haftungsrechtlichen Zwickmühle für den ISP

Der BGH hat bei der Erfindung des Kommunikationsprozesses die Situation vernachlässigt, in der sich eine Persönlichkeitsrechtsverletzung weder zweifelsfrei feststellen noch zweifelsfrei ausschließen lässt[782]. Bei dem Tätigwerden soll es nach den Umständen klar sein, dass ein Rechtsverstoß unschwer bejaht werden kann. Aber nach den gegenseitigen Stellungnahmen des Äußernden und des Betroffenen könnten die Umstände so geändert werden, dass ein Rechtverstoß nicht mehr unschwer bejaht werden kann.

Für diesen Fall erfasst die herrschende Meinung, dass der BGH den Provider von seiner eigentlich neutralen Rolle zu einer haftungsrechtlichen Zwickmühle - Haftung wegen Persönlichkeitsrechtsverletzung einerseits, Haftung wegen Vertragsverletzung andererseits - geführt hat.[783] Das heißt, für den Fall, in dem der ISP nicht leicht entscheiden kann, muss der ISP das Risiko der Fehleinschätzung selbst tragen[784]; entweder begründet er zugunsten des Betroffenen die Rechtsverletzung und verletzt die vertragliche Pflicht zu seinem Kunden oder er verletzt als Störer das Persönlichkeitsrecht des Betroffenen.

Meiner Meinung nach würde die Zwickmühlenwirkung aus folgenden Gründen überhaupt nicht eintreten:

1. In der Rechtsprechung über den Kommunikationsprozess hat der BGH nicht ausdrücklich festgelegt, dass eine eindeutige Entscheidung zugunsten einer Partei getroffen werden muss. Es wurde zwar geschrieben, dass die Durchführung des Kommunikationsprozesses eine Pflicht der Provider ist; aber diese

782 Rühl, LMK 2012, 338417.
783 Rühl, LMK 2012, 338417.
784 Feldmann, K&R 2012, 113, 115.

Pflicht bezieht sich nicht spezifisch oder nicht allein auf den Kommunikationsprozess, sondern auch auf das Tätigwerden des Providers überhaupt. Die Pflicht entsteht, wenn der Provider tätig sein muss; dies setzt voraus, dass der Hinweis des Betroffenen über eine Rechtsverletzung so konkret gefasst ist, dass der Rechtsverstoß auf der Grundlage der Behauptungen des Betroffenen unschwer - das heiß ohne eingehende rechtliche und tatsächliche Überprüfung- bejaht werden kann.[785] Wenn der Provider nach dem Tätigwerden Schwierigkeit mit einer Entscheidung des Rechtsverstoßes hat, bedeutet es dann, dass die Voraussetzung für das Tätigwerden des Providers nicht mehr besteht. Wäre dieses Ergebnis vorauszusehen, sollte der Kommunikationsprozess überhaupt nicht stattfinden. In diesem Fall braucht der Provider meiner Meinung nach nicht unbedingt eine Entscheidung treffen, sondern dem Betroffenen Bescheid geben, sich an ein Gericht zu wenden, um sein Recht zu verteidigen.

2. Auch wenn der Provider eindeutig entscheiden muss, soll er nicht für die falsche Entscheidung das Risiko tragen. Die Durchführung des Kommunikationsprozesses ist eine Pflicht, die der BGH dem Provider erteilt hat. Aber der Provider ist kein professioneller Richter oder Schiedsrichter; von ihm kann nur die zivilrechtliche verkehrsübliche Sorgfalt erwartet werden.[786] Das bedeutet, dass seine Entscheidung von der Entscheidung des Gerichts abweichen darf. Selbst wenn die falsche Entscheidung von ihm getroffen wird, sollte er nicht deswegen haften, solange er die verkehrsübliche Sorgfalt beachtet und bei der Beurteilung keinen offensichtlichen Fehler gemacht hat.

(3) Die Gefahr der Beschränkung der Meinungsfreiheit

Die Rechtsprechung hat dem ISP eine Rolle eines Richters gegeben. Dem entsprechend erwartet der BGH von dem ISP, idealerweise nach verkehrsüblichem Standard seine Rolle durchzuführen. Aber der ISP ist nichts anders als ein „Homo oeconomicus", der eigeninteressiert und rational handelt bzw. seinen eigenen Nutzen maximiert.[787]

Nach der Rechtsprechung verlangt das Anschalten des Kommunikationsprozesses die positive Kenntnis der Rechtverletzung. Wenn der Betroffene durch das Beanstanden die Rechtsverletzung gegen ihn nicht deutlich begründen kann, braucht der ISP den Kommunikationsprozess nicht anschalten.

785 BGH, K&R 2012, 110, 113.
786 Spindler, CR 2012, 176, 178.
787 Franz, http://potsdamer-koepfe.de/u/makrooekonomie/docs/studoc/stud7.pdf. (besucht am 04.04.2015), S. 4.

Unter dieser Konstellation verletzt der ISP auch keine Prüfungspflicht.[788] Aber wie es zu beurteilen ist, ob der Betroffenen die Rechtsverletzung hinreichend begründet hat, ist ungewiss.[789] Um jeden möglichen Fehler zu beseitigen bzw. eine Haftung von der Seite der Betroffenen zu vermeiden, wird ein umsichtiger Provider aus Sicherheitserwägungen jedes Mal den Kommunikationsprozess anschalten, „selbst wenn die Beanstandung des Betroffenen jedweder fundierten Grundlage entbehrt".[790] Dadurch könnten übrigens die Kosten des ISP bei der Beurteilung des Tätigwerdens eingespart werden, weil er nur am Schluss des Kommunikationsprozesses einmalig beurteilen müsse. Dies erhöht entsprechend die Kosten, um Meinungsfreiheit auszuüben, weil der Äußernde auch für seine rechtmäßige Äußerung jeder Zeit bereit sein muss, sich gegen die unvernünftige Beanstandung des Betroffenen zu verteidigen, weil die Äußerung gelöscht werden könnte, wenn er nicht rechtzeitig seine Stellungnahme abgibt.

Das Verhalten des Providers als „Homo oeconomicus" könnte auch bei der Schlussphase passieren. Wie bereits erwähnt wurde, ist der Kommunikationsprozess für den ISP aufwendig. Um die Kosten der Prüfung zu sparen und eine Haftung als Störer zu vermeiden, könnte ein vorsichtiger und vernünftiger Provider ohne Prüfung gegenseitiger Stellungnahmen direkt die bezüglichen Einträge löschen, auch wenn die Gegendarstellung des Äußernden vielleicht haltbar ist und die Entfernung damit eine Verletzung des Vertrags mit dem Nutzer sein könnte.[791] Ein derartiges Ergebnis wäre sicherlich eine Katastrophe für die Ausübung der Meinungsfreiheit.[792]

Die Beschränkung der Meinungsfreiheit könnte übrigens noch darin liegen, dass der BGH überfordert, dass die beanstandeten Einträge endgültig gelöscht werden sollen, wenn der Äußernde sie nicht erfolgreich als rechtmäßig nachweisen kann. Es herrscht die Meinung, dass eine Sperrung der Einträge, wie es in § 10 Satz 1 Nr. 2 TMG und auch im „Notice-ande-Take-Down"-Verfahren in den USA geregelt wurde,[793] schon genügt, um eine weitere Persönlichkeitsrechtsverletzung zu verhindern.[794]

---

788 Feldmann, K&R 2012, 113, 115.
789 Feldmann, K&R 2012, 113, 115.
790 Feldmann, K&R 2012, 113, 115.
791 Feldmann, K&R 2012, 113, 115.
792 Feldmann, K&R 2012, 113, 115.
793 Rühl, LMK 2012, 338417.
794 Spindler, CR 2012, 176, 178.

(4) Die Gefahr des ungenügenden Schutzes im Fall offensichtlicher Rechtsverletzung und der besonders schweren Persönlichkeitsverletzung

Durch diese Rechtsprechung hat der BGH zwei Begriffe aus § 10 Satz 1 Nr. 2 TMG einen Schritt weiter ausgelegt:

Der Erste Begriff ist die „Kenntnis". Für den Provider reicht eine bloße Kenntnis durch die Beanstandung des Betroffenen nach der Rechtsprechung nicht mehr, um die Prüfungspflicht des Providers auszulösen.[795] Dafür muss er eine positive Kenntnis an der Rechtsverletzung eines Dritten haben[796]. Positive Kenntnis bedeutet, dem Provider müssen nicht nur die Tatsachen sondern auch die Umstände bekannt sein, die die Rechtswidrigkeit der Informationen begründen.[797]

Der Zweite Begriff ist „unverzüglich". Wegen der Änderung der Bedeutung der Kenntnis ist der Begriff „unverzüglich" dementsprechend auch geändert, weil der Provider den Kommunikationsprozess durchführen muss, um eine positive Kenntnis zu erlangen. Deswegen ist es für den Provider nicht mehr notwendig, den beanstandeten Inhalt nach der Ermittlung des Betroffenen sofort zu entfernen, sondern nur unverzüglich seinen Nutzer zur Stellungnahme aufzufordern bzw. den Kommunikationsprozess anzuschalten.[798]

Diese Änderungen führen direkt dazu, dass der Verletzte auch im Fall der offensichtlichen Rechtsverletzung keinen Anspruch mehr auf sofortige Entfernung der bezüglichen Einträge hat, weil genau die Offensichtlichkeit einer Rechtsverletzung Voraussetzung für das Anschalten des Kommunikationsprozesses ist.[799]

Die Rechtsprechung hat auch keine Sonderregel für den Fall der besonders schweren Persönlichkeitsverletzung geschaffen, die dringend Rechtsschutz benötigt.[800] In diesem Fall könnte die hohe Vermehrungsgeschwindigkeit der Information im Internet dem Betroffenen eine enorme Prangerwirkung bringen, während eine vorläufige Sperrung der Einträge des Äußernden ihm nicht so viel Schaden bringen würde. Übrigens werden die Einträge schnell wieder veröffentlicht, solange der Äußernde seine Stellungnahme durch Belegen rechtzeitig nachweisen kann. Abzuwägen ist in diesem Fall auf einer Seite die Bedrohung

795 OLG Hamburg, K&R 2006, 470 ff.
796 Feldmann, K&R 2012, 113, 114.
797 Feldmann, K&R 2012, 113, 114.
798 Feldmann, K&R 2012, 113, 114.
799 Hoeren, MMR 2012, 124, 127.
800 Vgl. Hoeren, MMR 2012, 124, 127.

einer schweren Persönlichkeitsverletzung mit keiner Möglichkeit der Wiedergutmachung und auf der anderen Seite eine vorläufige Beschränkung der Meinungsfreiheit mit leichtem Schaden. Meiner Meinung nach ist der Betroffene schutzwürdiger. Die bezüglichen Einträge sollen in diesem Fall nach der Beanstandung des Betroffenen sofort vorläufig gesperrt werden.[801]

Als eine Unterstützung meiner Meinung hatte das KG Köln in einer Entscheidung über ein Hotelbewertungsportal im Internet für die Seite der Bewertenden entschieden, dass der Portalbetreiber im Fall einer Beschwerde den bewerteten Touristikunternehmen die Möglichkeit geben soll, die beanstandete Äußerung solange nicht online zu stellen, bis deren Berechtigung geklärt ist.[802] Zum Schutz der Ehre eines Touristikunternehmens ist eine vorläufige Beschränkung der Meinungsfreiheit sogar möglich, ganz zu schweigen vom Schutz des hochwertigeren Persönlichkeitsrechts.

Ein Anschalten des Kommunikationsprozesses ohne Differenzierung der Situation ist also bedenklich.[803]

(5) Der Kommunikationsprozess erfordert den Verzicht der Anonymität

Der Kommunikationsprozess korrespondiert mit der Tendenz, auf die Anonymität für die aktive Teilnahme an der Aktivität im Internet zu verzichten und stattdessen die Pseudonymität durchzuführen.[804] Um die Durchsetzung des Prozesses zu ermöglichen, müssen erstens die Einträge dem zuständigen Internetnutzer zugeordnet und zweitens die Internetnutzer erreicht werden können.[805] Dies setzt meiner Meinung nach voraus, dass die Internetnutzer mindestens mit dem Pseudonym registriert sein müssen, bevor sie Einträge auf der Webseite veröffentlichen.[806]

(6) Zusammenfassung über den Kommunikationsprozess

Obwohl der Kommunikationsprozess viele Kritiken bekommen hat, ist er zurzeit die beste Methode, um die Persönlichkeitsrechte des Betroffenen vor weiteren Rechtsverletzungen im Internet rechtzeitig zu schützen. Der ISP ist wegen

801 Vgl. Rühl, LMK 2012, 338417.
802 KG Berlin, K&R 2011, 671, 672.
803 Vgl. Rühl, LMK 2012, 338417.
804 Siehe oben unter § 11 III 2.
805 Vgl. Rühl, LMK 2012, 338417; Feldmann, K&R 2012, 113, 115.
806 Vgl. Rühl, LMK 2012, 338417; Hoeren, MMR 2012, 124, 127.

seiner Fähigkeit unfreiwillig an die Stelle wie ein Richter gestellt worden. Von ihm kann man jedoch nur die vernünftige Entscheidung wie von einer durchschnittlichen verständigen Person erwarten, wenn er zwingend eine Entscheidung treffen muss.

Die Rechtsprechung des BGH soll trotzdem so ausgelegt werden, dass der ISP nur im Fall offensichtlicher Rechtsverletzung eine Entscheidung treffen muss. Dies wäre der Fall, wenn der ISP den Rechtsverstoß auf der Grundlage der Behauptungen des Betroffenen unschwer - das heißt ohne eingehende rechtliche und tatsächliche Überprüfung- bejaht werden kann. Wenn sich diese Situation nach der gegenseitigen Stellungnahme des Äußernden geändert hat, das heißt, wenn der Rechtsverstoß nicht mehr eindeutig ist, muss der ISP nicht mehr eine eindeutige Entscheidung zugunsten einer Partei machen, sondern nur den Parteien mitteilen, sich wegen der Schwierigkeit des Falles an das Gericht zu wenden. Wenn der ISP in diesem Fall trotzdem eine Entscheidung getroffen hat, muss er nicht für seine falsche Entscheidung haften, solange er die Sorgfaltspflicht wie eine durchschnittliche verständige Person nicht verletzt hat.

Dies würde nicht dazu führen, dass der ISP eine Entscheidung auch für den Fall der offensichtlichen Rechtsverletzung verweigert, weil er in diesem Fall wegen der Verletzung der Beseitigungspflicht haften muss, wenn das Gericht die Rechtsverletzung nachher als offensichtlich beurteilen würde.

Wenn es in einem komplexen Fall um schwerwiegende Persönlichkeitsrechtsverletzung geht, soll der ISP trotz der Komplexität des Falles eine Entscheidung zugunsten des Betroffenen treffen. Dies wäre z.B. der Fall, wenn durch die Einträge des Äußernden die Intimsphäre einer normalen Person offengelegt wird.

c) Unterlassungsanspruch

Wie bereits erwähnt wurde, ist ein Beseitigungsanspruch auf die Beendigung der gegenwärtigen Störung gerichtet[807]. Im Gegenteil ist der Unterlassungsanspruch auf die Abwehr erneuter Verletzungen in der Zukunft gerichtet.[808] Ist eine gleichartige Verletzung in der Zukunft zu erwarten, reicht ein „Take-Down" allein nicht aus, um den Provider von weiteren Verpflichtungen gegenüber dem Rechtsinhaber freizustellen.[809] Der Provider hat vielmehr aktiv einer wiederholten bzw.

807 Spindler/Anton in Spindler/Schuster, § 1004 BGB, Rn. 13; BGHZ 28, 110, 113 = NJW 1958, 1580, 1581; Bassenge in Palandt, § 1004 BGB Rn. 28; Fritzsche in Bamberger/Roth, § 1004 BGB Rn. 56.

808 Spindler/Anton in Spindler/Schuster, § 1004 BGB, Rn. 14.

809 Rössel, CR 2011, 593.

weiteren Rechtsverletzung entgegenzuwirken.[810] Das ist das sogenannte „Notice-and-Stay-Down"- oder „ Notice-and-Keep-Off"-Verfahren.[811] Dieses Prinzip hat der BGH in der Entscheidung „Internetversteigerung I" im Jahr 2004 für Markenrechtverletzungen entwickelt.[812] Durch die „Blogspot"-Entscheidung von 2011 hat der BGH weiterhin festgestellt, dass es auch auf Persönlichkeitsverletzungen im Internetforum anwendbar ist.[813]

Der Gedanke des Unterlassungsanspruchs findet seine Grundlage auch auf europäischer Ebene. Der EuGH leitet aus dem Zweck der RL 2004/48/EG, effektiven Rechtsschutz zu bieten, sowie deren Erwägungsgrund 25 ab, dass aus deren Art. 11 Satz 3 die Verpflichtung der Mitgliedstaaten folgt, gerichtliche Anordnungen gegenüber Mittelspersonen nicht nur zur Beseitigung einer Rechtsverletzung, sondern auch zu deren künftiger Verhinderung vorzusehen.[814]

Im Folgenden werden die Voraussetzungen eines Unterlassungsanspruchs diskutiert.

aa) Die Voraussetzungen eines Unterlassungsanspruchs gegen den ISP im Fall der Persönlichkeitsverletzung

(1) Wiederholungsgefahr und Erstbegehungsgefahr

Ein Störer kann nach der Rechtsprechung nicht nur aufgrund von Wiederholungsgefahr sondern auch wegen Erstbegehungsgefahr[815] auf Unterlassung in Anspruch genommen werden.

Der Hintergedanke liegt darin, dass der Betroffene bei einer drohenden Gefährdung nicht erst abzuwarten braucht, bis der erste Eingriff in ein Rechtsgut erfolgt ist.[816] Um einen solchen Unterlassungsanspruch geltend zu machen, muss eine Erstbegehrungsgefahr begründet werden.[817] Dies wäre der Fall, wenn es noch nicht zu einer Verletzung des geschützten Rechts gekommen ist, eine Verletzung in der Zukunft aber auf Grund der Umstände zu befürchten ist.[818]

Die Begründung des Unterlassungsanspruchs wegen Erstbegehungsgefahr hat viele Kritiken erhalten, weil es zu einer allgemeinen Überwachungspflicht

---

810 BGH, GRUR 2004, 860, 862; vgl. auch BGH, K&R 2012, 110, 113.
811 Rössel, CR 2011, 593.
812 BGH, GRUR 2004, 860, 862; vgl. auch BGH, K&R 2012, 110, 113.
813 BGH, K&R 2012, 110, 113.
814 Rössel, CR 2011, 589, 590; EuGH, CR 2011, 597.
815 BGH, MMR 2007, 507 ff.
816 Vgl. OLG Hamburg, MMR 2006, 744, 746; s. a. BGH, MMR 2007, 507, 510.
817 BGH, MMR 2007, 507.
818 BGH, MMR 2007, 507.

des Providers führen könnte, die mit Art. 15 der E-Commerce-Richtlinie nicht zu vereinbaren wäre.[819]

Für den Unterlassungsanspruch nach einer bereits erfolgten Rechtsverletzung kann der Provider aufgrund der Kerntheorie[820] auf „klare" und „gleichgelagerte" Rechtsverletzungen aufpassen, die noch als spezifische Überwachungspflicht eingeordnet werden kann.[821] Für den Fall, das eine Rechtsverletzung nur droht und nicht einmal wirklich passiert, existiert weder ein Inhalt auf dem Server des Providers, noch kann der Provider von dem Inhalt vor seiner Speicherung Kenntnis erhalten.[822] Um die erste Begehung zu vermeiden, muss der Provider jeden einzelnen neu eingestellten Beitrag vor der Freischaltung prüfen.[823] Dies könnte zu einer allgemeinen Überwachungspflicht des Providers führen.

Zu berücksichtigen ist es jedoch, dass die Anerkennung der Erstbegehungsgefahr als Voraussetzung des Unterlassungsanspruchs von dem BGH in einem Spezialfall festgestellt ist. Unter jenen Konstellationen war es möglich, eine bestimmte Rechtsverletzung zu identifizieren oder zu erwarten. Die Voraussetzung für das Vorliegen einer Erstbegehungsgefahr soll deswegen eng gefasst werden.[824] Die Einwirkung zu einer allgemeinen Überwachungspflicht des Providers ist auf jeden Fall zu vermeiden.

(2) Qualifiziertes Notice

Ob es nötig ist, eine Rechtsverletzung dem ISP zu beweisen, oder ob es reicht, den ISP auf die vermutliche Rechtsverletzung einfach hinzuweisen, um „Notice-and-Stay-Down"- oder „ Notice-and-Keep-Off"-Verfahren anzuschalten, hatten das OLG Düsseldorf als Vorinstanz und der BGH in der „Stiftparfüm"-Entscheidung unterschiedliche Meinungen gehabt.[825]

Nach der Meinung vom OLG Düsseldorf reicht die bloße Mitteilung über die Rechtsverletzung nicht, um eine zukünftige Prüfungspflicht des Plattformbetreibers auszulösen.[826] Vielmehr sei es hierfür erforderlich, Belege für diese Behauptung beizubringen.[827]

819 Vgl. Roggenkamp, jurisPR-ITR 11/2007 Anm. 2.
820 Siehe unten.
821 Roggenkamp, jurisPR-ITR 11/2007 Anm. 2.
822 Vgl. Spindler, MMR 2007, 511, 512.
823 Roggenkamp, jurisPR-ITR 11/2007 Anm. 2.
824 Vgl. Jürgens, K&R 2007, 392, 393.
825 BGH, K&R 2011, 727, 729; GRUR 2011, 1038.
826 Volkmann, K&R 2012, 381, 382.
827 Volkmann, K&R 2012, 381, 382.

Der BGH hat die Meinung des OLG Düsseldorf korrigiert und meinte, dass ein Beleg der im Hinweis mitgeteilten Umstände nur dann erforderlich sei, wenn schutzwürdige Interessen des Plattformbetreibers dies rechtfertigten.[828] Dies könne z. B. der Fall sein, wenn es berechtigte Zweifel am Bestehen des Schutzrechts gibt und die begründete Verletzung vom Provider aufwendige eigene Recherchen verlangen würde.[829]

(3) Zumutbarkeit

Um eine zukünftig gleichartige Rechtverletzung zu verhindern, ist vom Störer nur eine zumutbare Kontrolle erforderlich.[830] Es wäre eine Überforderung und würde deswegen zu einer allgemeinen Überwachung führen, wenn der Provider „jeden in einem automatisierten Verfahren von Benutzer unmittelbar ins Internet gestellten Inhalt darauf überprüfen" muss, um zu sichern, dass keine Schutzrechte Dritter verletzt werden.[831]

Die Standards zur Beurteilung der Zumutbarkeit haben der BGH und der EuGH aus ihren Markenrechtsverletzungs-Entscheidungen entwickelt. Nach der Rechtsprechung des BGH können sie aber auch auf den Fall der Persönlichkeitsrechtsverletzung angewendet werden.[832]

Die Zumutbarkeit soll in jedem einzelnen Fall unter einzelnen Umständen bestimmt werden. Das Hauptprinzip, dass die unternehmerische Freiheit des ISP nicht einschränkt werden soll, soll aber unberührt bleiben.[833] Übrigens wurden in der Praxis noch andere Prinzipien für die Beurteilung der Zumutbarkeit entwickelt:

(a) Dass der Provider zusätzliches Personal für die Kontrolle einsetzen müsste, ist kein hinreichender Grund einer unzumutbaren Maßnahme.[834] Das Einsetzen des zusätzlichen Personals ist erst unzumutbar, wenn durch den dadurch entstehenden Überprüfungsaufwand das Geschäftsmodell in Frage gestellt würde.[835]

---

828 Volkmann, K&R 2012, 381 382; vgl. BGH, K&R 2011, 727, 729 = GRUR 2011, 1038.
829 Volkmann, K&R 2012, 381 382.
830 BGH, GRUR 2004, 860, 863; Rössel, CR 2011, 589, 594.
831 BGH, GRUR 2004, 860, 863f.
832 BGH, K&R 2012, 110, 113 = GRURInt 2012, 259.
833 EuGH, K&R 2012, 35ff.
834 Spindler/Anton in Spindler/Schuster, § 1004 BGB, Rn. 9; OLG Köln, ZUM 2007, 927, 930.
835 Spindler/Anton in Spindler/Schuster, § 1004 BGB, Rn. 9; BGHZ 173, 188, 202, Rn. 39 = CR 2007, 728, 732 = MMR 2007, 634, 637; BGH, NJW 2010, 2061, Rn. 24.

(b) Ist zum Überprüfen der behaupteten Rechtsverletzungen eine uneingeschränkte manuelle Kontrolle der Inhalte erforderlich, ist es dem Provider nicht mehr zumutbar.[836] Dies wäre nach der Rechtsprechung des BGH der Fall, wenn die zukünftig zu vermeidende Rechtsverletzung keine Merkmale aufweist, die sich zur Eingabe in ein automatisiertes Suchsystem eignen.[837]

(c) Die Zumutbarkeit bzw. die Intensität der Prüfungspflicht kommt auch auf das Geschäftsmodell an. Dafür müssen einige Frage beantwortet werden: Erstens, ob das Geschäftsmodell auf der Nutzung der Rechtswidrigkeit eingestellter Inhalte beruht[838]; zweitens, ob und in welcher Weise der Provider direkt oder indirekt an den rechtswidrigen Inhalten mitverdient[839]; drittens, inwiefern eine rechtswidrige Nutzung der Webseite allgemein bekannt ist[840]. Je mehr es sich bei dem Provider um rechtswidrige Inhalte handelt, desto intensiver ist seine Prüfungspflicht der fremden Informationen auf seiner Webseite.

bb) Kerntheorie

Wenn ein Unterlassungsanspruch gegen den ISP begründet ist, ist die Kerntheorie anwendbar.

Auf Grund dieser Theorie verpflichtet sich der ISP nicht nur zur Verhinderung weiterer Verletzungen durch denselben Verletzer, sondern auch die durch andere Internetnutzer begangenen Verletzungen über dieselbe bzw. im Kern gleichen Inhalte.[841]

cc) Selbstaufspürung der Rechtsverletzung durch den Betroffenen

Die Verurteilung des ISP zur Unterlassungspflicht ist nicht selbstverständlich, weil unter der Situation, wenn weder der Provider noch der Betroffene für die Verletzung schuldig ist, immer die Frage steht, wer von den Beiden unter Effizienzgesichtspunkten derjenige ist, der die Rechtsverletzungen am besten überwachen und verfolgen kann.[842] Wenn die Überwachung- und Verfolgungspflicht vom ISP an den Betroffenen übertragen werden kann, soll sich der Betroffene

836 Volkmann, K&R 2012, 381 383; vgl. BGH, K&R 2011, 117 ff.
837 BGH, K&R 2007, 387 ff. = MMR 2007, 507, 511.
838 Wilmer, NJW 2008, 1845, 1847.
839 Vgl. OLG Düsseldorf, MMR 2006,618; siehe auch Wilmer, NJW 2008, 1845, 1847.
840 Wilmer, NJW 2008, 1845, 1847.
841 Vgl. Rössel, CR 2011, 596; BGH, CR 2007, 728.
842 Spindler, MMR 2007, 507, 514.

mit dem gleichen Aufwand mehr um sich kümmern.[843] Dieser Gedanke ist von der Rechtsprechung nachgewiesen.

Der BGH hat in der Kinderhochstühle-Entscheidung festgestellt, dass, wenn der ISP (eBay in diesem Fall) ein passendes Programm (VeRI-Programm von eBay) anbietet, mit dem der Betroffenen eine Rechtsverletzung selbst aufspüren kann, die Prüfungspflicht seitens des ISP entfällt.[844]

Der BGH hat mit diesem Urteil der Praxis einen wichtigen Hinweis gegeben, wie „ausufernde Unterlassungspflichten in Zukunft zwar nicht uneingeschränkt aber doch auf bestimmten Ebenen vermieden werden können"[845]. *„Es ist damit für Provider empfehlenswert, Nutzern* (der Betroffene bzw. der Verletzte) *die Möglichkeit zu geben, auf einfachem Weg Verletzungen ihrer Schutzrechte auf der Plattform aufzufinden, die der Provider sodann nach entsprechender Monierung löscht.*"[846]

Aufgrund dieser Entscheidung ist es ein Abwägungselement der Zumutbarkeit geworden, ob der Provider dem Betroffenen die Möglichkeit einer Selbstkontrolle anbietet.[847] Hätte der Betroffene diese Möglichkeit, wäre die Kontrolle derselben Inhalte für den Provider weniger zumutbar.

Das „Notice-and-Stay-Down"-Verfahren i.S.v. dieser Entscheidung ist nämlich eine Kombination mit einem System, mit dem der Betroffenen auf einfachem Weg die gleichartigen Rechtsverletzungen selbst aufspüren kann, und mehreren „Notice-and-Take-Down"-Verfahren, mit dem der Verletzte vom ISP verlangen kann, ohne Einsetzen des Kommunikationsprozesses die aufgespürten Rechtsverletzungen zu stoppen. Mit dem Anbieten eines Selbstkontroll-Systems hat der ISP die Möglichkeit, die Pflicht zur Entdeckung zukünftiger derartiger Rechtsverletzungen auf den Betroffenen zu übertragen und dadurch die wegen Unterlassungsansprüchen entstehenden Prüfungskosten im großen Umfang einzusparen.

d) Schadensersatz- und Schmerzensgeldansprüche gegen den ISP wegen Pflichtverletzung

Eine Störerhaftung eröffnet gegen den Provider einen Beseitigungs- oder Unterlassungsanspruch, niemals unmittelbar einen Schadensersatzanspruch.[848]

---

843 Vgl. Spindler, MMR 2007, 507, 514.
844 BGH, K&R 2011, 117, 120 f.
845 Volkmann, K&R 2012, 381 383.
846 Volkmann, K&R 2012, 381 383.
847 Volkmann, K&R 2012, 381 383.
848 Vgl. BGH, GRUR 2004, 860, 864; BGH, GRUR 2002, 618, 619.

Dennoch besteht ab der dem Provider bekannt gewordenen Rechtsverletzung eine Beseitigungspflicht, eine auf die zukünftigen gleichartigen Verletzungen gerichtete Untersuchungspflicht und ggf. eine damit verbundene Beseitigungspflicht des ISP.[849] Bei Nichterfüllung dieser Pflichten kann der Betroffene wegen Pflichtverletzung gemäß § 280 I BGB Schadensersatz von dem Provider verlangen,[850] wenn es zu einer Rechtsverletzung des Betroffenen kommt, die hätte vermieden bzw. hätte geringer gehalten werden können, wenn der Provider die Pflichten erfüllt hätte.[851]

Zu bemerken ist es, dass ein Schadensersatzanspruch gemäß § 10 Satz 1 Nr. 1 TMG auch begründet wäre, wenn der Provider die rechtswidrige Handlung oder die Information wegen der Offensichtlichkeit kennen sollte.

Dieser Schadensersatzanspruch gegen den Provider stammt nicht aus seiner Verantwortung für fremde Informationen als Störer, sondern aus der Verletzung seiner Handlungspflichten, die aus der Störerhaftung einen Schritt weiter entwickelt worden sind.[852]

Im Fall der Verletzung dieser Handlungspflicht kann auch ein Schmerzensgeldanspruch gegen den ISP bestehen, wenn dieser Anspruch gegen den unmittelbaren rechtsverletzenden Internetnutzer begründet ist. Der ISP muss für wegen seiner Pflichtverletzung entstehenden oder erweiterten Schaden haften.

II. Nach chinesischem Recht

1. Die Reihenfolge der Ansprüche gegen den unmittelbaren rechtsverletzenden Internetnutzer und den ISP

Gemäß § 36 Delikthaftungsgesetz haftet der ISP gesamtschuldnerisch mit dem rechtsverletzenden Internetnutzer. Deswegen gibt es für die Ansprüche gegen die beiden keine Reihenfolge. Ungünstig für den Betroffenen wäre es aber, wenn er zwingend den ISP und den Internetnutzer gleichzeitig anklagen muss.

Wie vorher bereits diskutiert wurde, liegt der Grund der gesamtschuldnerischer Haftung des ISP nach der herrschenden Meinung an seiner Mittäterschaft mit dem unmittelbaren rechtsverletzenden Internetnutzer. Gemäß § 5 „Erklärung einiger Fragen über die Gesetzesanwendung für die Beurteilung der Fälle

849 Ensthaler/Heinemann, GRUR 2012, 433, 440.
850 Ensthaler/Heinemann, GRUR 2012, 433, 440; Vgl. Westermann in Erman, BGB § 280, Rn. 6.
851 Ensthaler/Heinemann, GRUR 2012, 433, 439.
852 Ensthaler/Heinemann, GRUR 2012, 433, 439.

über den aufgrund von personenbezogenen (körperliche und geistliche) Rechtsverletzungen entstehenden Schadenersatzanspruch“[853] soll das Gericht in diesem Fall von Amts wegen die anderen Täter als Mitbeklagte hinzufügen, wenn der Rechtsinhaber nur gegen einen Teil der Täter wegen Rechtsverletzung klagt. Nach § 53 chinesischen Zivilprozessgesetzes ist diese Klage eine notwendige gemeinsame Klage.[854] Für eine notwendige gemeinsame Klage müssen alle Beklagten an der Gerichtshandlung teilnehmen. Sonst wäre die Gerichtshandlung prozesswidrig.

Im Fall der Menschenfleischsuche müssen dann der ISP und der unmittelbarere rechtsverletzende Internetnutzer bei der Gerichtshandlung da sein. Hier entstünde wegen der Anonymität und der Pseudonymität wiederum die Frage der Identifizierung des beklagten Internetnutzers im Gerichtsprozess, die, wie oben gesagt wurde, immer noch eine ungelöste Frage ist.[855] Falls der Kläger auf die Ansprüche gegen den schwierig identifizierbaren Internetnutzer verzichtete, verzichtete er gemäß § 5 „Erklärung einiger Fragen über die Gesetzesanwendung für die Beurteilung der Fälle über den aufgrund von personenbezogenen (körperliche und geistliche) Rechtsverletzungen entstehenden Schadenersatzanspruch“[856] gleichzeitig auf den Teil vom Schadenersatz, für den der Internetnutzer haften sollte. Für diesen Teil haftete der ISP auch nicht mehr.

Die Regelungen würden den Betroffenen beim Schutz seines Rechts vor dem Gericht offensichtlich in Schwierigkeit bringen, wenn sie so wie oben eng ausgelegt würden. Um einen besseren Schutz des Betroffenen zu schaffen, haben die Gerichte in der Praxis einen abweichenden Weg genommen. Wenn der Betroffene gegen den ISP und den unmittelbaren Verletzer als Beklagte klagt, wird der Prozess vom Gericht als eine normale gemeinsame Klage behandelt. Wenn der Betroffene nur gegen den ISP klagt, wird das Gericht den unmittelbaren Verletzer nicht als weiteren Beklagten hinzufügen. Die Ansprüche gegen den unmittelbaren Verletzer werden auch nicht als verzichtet behandelt.[857]

Eine abweichende Auslegung der gesetzlichen Regelungen in der Entscheidungspraxis ist in diesem Fall durchaus möglich, weil das Verhältnis zwischen dem ISP und dem unmittelbaren Verletzer mit dem typischen Verhältnis zwischen den Mittätern nicht völlig identisch ist. Wie bereits erwähnt, wird dem ISP die gesamtschuldnerische Haftung unter Berücksichtigung der öffentlichen

853 Vom chinesischen Obersten Volksgerichtshof.
854 Yao Hong, S. 74.
855 Siehe oben unter § 11 II 2.
856 Vom chinesischen Obersten Volksgerichtshof.
857 Chen Jinchuan, Journal of Law Application 2011, No. 6, 52, 56.

Politik auferlegt, weil dadurch das Recht des Verletzten im Internet am besten geschützt werden kann. Die zivilprozessrechtlichen Regelungen in China sind aufgrund der schnellen Entwicklung des Internets nicht mehr aktuell, und müssen geändert werden.[858]

2. Der Beseitigungsanspruch gegen den ISP

Der Beseitigungsanspruch gegen den ISP in China findet seine Grundlage in § 36 Abs. 2 Delikthaftungsgesetz, gemäß dem der Verletzte das Recht hat, den ISP zu informieren und nötige Maßnahmen vom ISP zu verlangen, um den rechtswidrigen Inhalt zu löschen, zu sperren oder das Verlinken zu dem Inhalt abzubrechen, wenn ein Internetnutzer mit Benutzung des Internets eine Rechtsverletzung begangen hat. Der vom § 36 Abs. 2 Delikthaftungsgesetz geregelte Beseitigungsanspruch ist eigentlich eine Übernahme des „Notic-and-Take-Down"-Verfahrens von den USA.[859]

a) Über Notice

Ein qualifiziertes Notice ist eine Voraussetzung des Beseitigungsanspruchs. Um das „Notice-and-Take-Down"-Verfahren erfolgreich durchzuführen, soll der ISP gemäß § 9 Abs. 1 Nr. 5 „Regelung einiger Fragen über die Gesetzanwendung auf die Beurteilung der Fälle über den zivilrechtlichen Rechtsstreit wegen Verletzung des informationellen Verbreitungsrechts im Internet" ein funktioniertes Programm entwickeln, um damit Notice zu bekommen und auf die Notice schnell zu reagieren. Ob so ein Programm existiert, ist ein Standard zu beurteilen, ob der ISP während „Notice-and-Take-Down"-Verfahren Schuld hat.

Gemäß § 13 der oben genannten Regelung kann das Notice in Form von Brief, Fax oder E-Mail sein. Nach dem Erlangen des Notice soll der ISP rechtzeitig passende Maßnahmen vornehmen. Um zu beurteilen, ob die von dem ISP vorgenommenen Maßnahmen rechtzeitig sind, soll das Gericht mit Berücksichtigung der Form und der Ausführlichkeit des Notice, der Schwierigkeit der vorzunehmenden Maßnahmen, der Art des von dem ISP angebotenen Dienstes, der Art der vom Internetnutzer begangenen Rechtsverletzung, der Anzahl der rechtsverletzenden Inhalte usw. zusammen entscheiden.[860]

858 Chen Jinchuan, Journal of Law Application 2011, No. 6, 52, 56.

859 Xie Xuekai, Oriental Law 2013, No. 2, 149, 154f.

860 § 14 „Regelung einiger Fragen über die Gesetzanwendung auf die Beurteilung der Fälle über den zivilrechtlichen Rechtsstreit wegen Verletzung des informationellen Verbreitungsrechts im Internet" vom chinesischen Obersten Volksgerichtshof.

b) Über „Anti-Notice"

Das Delikthaftungsgesetz hat jedoch das „Notice-and-Take-Down"-Verfahren von den USA nicht komplett übernommen, weil die Regelung von § 36 Delikthaftungsgesetz nur zugunsten des Betroffenen ist. Ein „Anti-Notice"-Verfahren zugunsten des Äußernden, der die vermutlich rechtsverletzenden Inhalte veröffentlicht hat, ist vom Delikthaftungsgesetz vernachlässigt.

Ein „Anti-Notice"-Verfahren ist aber in der „Verordnung zum Schutz des informationellen Verbreitungsrechts im Internet" - eine Verordnung über Urheberrecht - geregelt. Aufgrund § 16 dieser Verordnung kann der verdächtige Verletzer schriftlich beim ISP beantragen, die gelöschten oder gesperrten Werke oder Links widerherzustellen, wenn er nach dem Erhalt der Beanstandung des Rechtsinhabers daran glaubt, dass die von ihm angebotenen Werke keine Rechtsverletzung begründen. Der Antrag des verdächtigten Verletzers soll nach § 16 Abs. 2 der Verordnung durch grobes Beweismaterial unterstützt werden. Der ISP soll nach § 17 der Verordnung das bezügliche Werk sofort wiederherstellen, nachdem er den schriftlichen Antrag bekommen hat. Gleichzeitig soll der ISP den Antrag an den Rechtsinhaber weiterleiten. Eine weitere Beanstandung an dem gleichen Werk von dem gleichen Rechtsinhaber wird nicht mehr berücksichtigt.

Jedoch beschränkt sich diese Verordnung nur auf Urheberrechtsverletzungen, während § 36 i.V.m. § 2 Delikthaftungsgesetz für jede Art von Rechtsverletzungen gilt. Deswegen entsteht die Frage, ob es möglich ist, für das im Bereich des Urheberrechts geregelte „Anti-Notice"-Verfahren eine analoge Anwendung auf dem Schutz des Persönlichkeitsrechts zu finden.[861] Auf diese Frage gibt es in der Literatur hauptsächlich Gegenmeinungen.

Der Grund für die Gegenmeinungen liegt hauptsächlich darin, dass es für die Beurteilung von Persönlichkeitsrechtsverletzungen und Urheberrechtsverletzungen unterschiedliche Kriterien gebe.[862] Das Beweisen[863] und das Identifizieren[864] der Urheberrechtsverletzung seien relativ einfach, weil die Dimension des Urheberrechts relativ klar sei. Im Gegensatz dazu sei die Dimension der Persönlichkeitsrechte relativ undeutlich. Auch die Gerichte müssen unter

861 Cai Chang, Studies in Law and Business 2013, No. 2, 113, 115.

862 Yuan Xueshi, Political Science and Law 2008, No. 4, 19, 22; Lu Chunya, Journal of Henan University of Economics and Law 2012, No. 5, 58, 60; Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 90.

863 Cai Chang, Studies in Law and Business 2013, No. 2, 113, 116.

864 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 90.

Berücksichtigung der Konstellation in jedem einzelnen Fall eine Interessenabwägung durchführen, um eine Entscheidung der Rechtsverletzung zu treffen.[865] Dafür sei der ISP nicht unbedingt in der Lage.[866]

Diese Gegenmeinung ist nicht überzeugend, weil der ISP beim Notice im Fall der Persönlichkeitsrechtsverletzung bereits überprüfen muss, ob der Inhalt überzeugend ist. Wäre er für „Anti-Notice" nicht in der Lage, sollte der Gesetzgeber ihm auch diese Überprüfungspflicht bei Notice nicht geben. Übrigens kommt es für die Beurteilung einer Verletzung auf die Ausführlichkeit des Notice an. Auch für die Persönlichkeitsrechtsverletzung könnte es einen einfach zu beurteilenden Fall geben. Übrigens wird vom ISP bei der Beurteilung auch nur eine allgemeine Sorgfaltspflicht erwartet, der Betroffene und der Äußernde sollen mehr für die Wahrheit ihrer Stellungnahmen verantwortlich sein.[867]

Es herrscht jedoch die Meinung, dass das Dilemma der Analogisierung völlig vernachlässig werden kann. Nach dieser Meinung ist eine oben genannte Analogisierung gar unnötig, weil ein „Anti-Notice"-Verfahren für jede Rechtsverletzung im Sinne von § 36 i.V.m. § 2 Delikthaftungsgesetz ein impliziertes „Muss" ist.[868] Ohne das „Anti-Notice"-Verfahren würde das Recht des Rechtinhabers sehr leicht missbraucht, weil die der Rechtsverletzung verdächtigten Inhalte nur auf Verlangen des Rechtsinhabers ohne inhaltliche Prüfung gesperrt oder gelöscht würden.[869] Die Stimme der Gegenseite würde in diesem Fall gar nicht angehört werden. Ihre Rechte und Freiheiten würden völlig vernachlässigt, zu denen insbesondere die Meinungsfreiheit gehört. Ohne „Anti-Notice"-Verfahren bestände die Gefahr der Verfassungswidrigkeit des Delikthaftungsgesetzes, weil die Meinungsfreiheit durch das Delikthaftungsgesetz unter alle anderen Rechte gesetzt würde, was offensichtlich gegen § 51 chinesisches Verfassungsgesetzes widrig wäre, aufgrund dessen das Ausüben der Rechte und Freiheiten von einem Bürger die Rechte und Freiheiten der anderen nicht verletzen darf.

Es ist in der Literatur allgemein anerkannt, dass das Fehlen des „Anti-Notice"-Verfahrens im Delikthaftungsgesetz ein Fehler des Gesetzgebers ist. Diese Lücke soll entweder durch die Rechtsprechung oder durch die Novellierung des Gesetzes erfüllt werden.

---

865 Zhou Hua, Journal of China Three Gorges University (Humanities & Social Sciences) 2012, No. 5, 87, 89.

866 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 84, 90.

867 Xie Xuekai, Oriental Law 2013, No. 2, 149, 154f.

868 Yang Lixin/Li Jialun, Science of Law 2012, No. 2, 157, 157.

869 Yang Lixin/Li Jialun, Science of Law 2012, No. 2, 157, 158.

c) *Die Kommentare über das chinesische „Notice-and-Take-Down"-Verfahren*

Gleich wie die Kritiken gegen den Kommunikationsprozess gibt es in der chinesischen Literatur auch zahlreiche Kritiken gegen das „Notice-and-Take-Down"-Verfahren. Viele Kritiken sind mit denselben Gründen wie in Deutschland argumentiert. Im Folgenden werden nur die Argumente mit chinesischen Besonderheiten diskutiert.

aa) Die Gefahr einer haftungsrechtlichen Zwickmühle für den ISP

Es ist nicht zu verneinen, dass es manchmal Fälle von Rechtsverletzungen gibt, die schwierig zu beurteilen sind. Wenn der ISP zwingend eine Entscheidung treffen muss, könnte er entweder die rechtsverletzenden Fälle als nicht rechtsverletzend fehlerhaft entscheiden und wegen Pflichtverletzung gesamtschuldnerisch haften,[870] oder die nicht rechtsverletzenden Fälle als rechtsverletzend fehlerhaft entscheiden und wegen vertraglicher Pflichtverletzung haften. Für die schwierig zu entscheidenden Fälle könnte der ISP in eine haftungsrechtliche Zwickmühle geraten.

Die Zwickmühle ist sogar in der Entscheidungspraxis in China tatsächlich passiert. Im Jahr 2011 hat Frau Fang Jing beim Betreiber der Mikroblogging-Webseite „Sina Weibo" beanstandet, dass Frau Yu auf ihrem Blog rechtsverletzende Inhalte über sie geschrieben hat. „Sina Weibo" hat deswegen den Account von Frau Yu gesperrt. Nach der Beurteilung des Gerichts hat die Äußerung von Frau Yu auf ihrem Blog die Grenze der Meinungsfreiheit nicht überschritten. „Sina Weibo" musste wegen vertraglicher Pflichtverletzung die wegen des Gerichtsprozesses entstehenden Kosten für Frau Yu übernehmen. „Sina Weibo" hat während des Prozesses behauptet, dass sein Dienst kostenlos ist, und er deswegen ohne Grund den Dienst jeder Zeit beenden kann. Nach der Entscheidung kann „Sina Weibo" nicht damit argumentieren, dass sein Dienst kostenlosen ist, weil er wegen Werbung auf der Webseite, orientierte Werbung per E-Mail zu den Nutzern usw. tatsächlich von den Nutzern profitiert. Ein Dienstvertrag kommt zwischen „Sina Weibo" und den Nutzern zustande.

Angeblich hat diese Entscheidung den ISP zu einer relativ strengen Pflicht verurteilt. Aber der Grund dieser Entscheidung liegt meiner Meinung nach eher darin, dass ein „Anti-Notice"-Verfahren für die Persönlichkeitsrechtsverletzung im chinesischen Gesetz fehlt. „Sina Weibo" hat nach der Beanstandung von Frau

870 Zhou Hua, Journal of China Three Gorges University (Humanities & Social Sciences) 2012, No. 5, 87, 90.

Fang Jing schnell reagiert, hat aber das Verlangen von Frau Yu auf Wiederherstellung ihres Accounts vernachlässigt, weil eine Pflicht zur Wiederherstellung nicht im Gesetz vorgeschrieben ist.

Das Fehlen des „Anti-Notice"-Verfahrens bzw. der aus diesem Verfahren entstehenden Pflicht des ISP könnte leicht dazu führen, dass der ISP die Beanstandung des Betroffenen ohne Prüfung zu 100% akzeptieren könnte, um eine gesamtschuldnerische Haftung zu vermeiden.[871] Das wäre offensichtlich eine starke Beschränkung der Meinungsfreiheit.[872]

bb) Die Unfähigkeit des ISP bei der Beurteilung komplexer Persönlichkeitsrechtsverletzung

Nicht nur in China sondern auch in Deutschland ist es eine entscheidende Frage, was der ISP zum Schluss des „Notice-and-Take-Down"-Verfahrens oder des Kommunikationsprozesses machen soll, wenn die Konstellation so kompliziert ist, dass der ISP die Persönlichkeitsrechtsverletzung nicht beurteilen kann.

Bei dieser Diskussion im deutschen Teil habe ich vorgeschlagen, dass der ISP in diesem Fall nicht zwingend eine Entscheidung zugunsten einer Partei treffen muss, sondern den Parteien mitteilen soll, sich direkt an das Gericht zu wenden. Auch nachdem der ISP eine Entscheidung gegeben hat, soll er nicht für seinen Fehler haften, solange er die allgemeine Sorgfaltspflicht bei der Überprüfung nicht verletzt hat.[873] Ob es sich um einen schwierigen Fall handelt, soll nach der Konstellation betrachtet werden, ob ein Rechtsverstoß so offensichtlich ist, dass auch eine durchschnittliche verständige Person die Rechtsverletzung unter Berücksichtigung der Situation unschwer bejahen kann. Die Offenlegung der Intimsphäre einer normalen Person z.B. soll zur offensichtlichen Rechtsverletzung gehören. Dieser Vorschlag wird nicht dazu führen, dass der ISP jede Entscheidungsfindung ablehnt, denn ist eine Rechtsverletzung nach der Entscheidung des Gerichts offensichtlich, muss der ISP wegen Pflichtverletzung haften.

---

871 Civil Law Department of Legislative Affairs Commission of NPC Standing Committee, S. 588, 611, 620f.; vgl. Zhou Hua, Journal of China Three Gorges University (Humanities & Social Sciences) 2012, No. 5, 87, 89; Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 84.

872 Vgl. Xie Hongfei, Procuratorial View 2010, No. 3, 26; Zhou, Bo/Yang, Kangrui, Chinese Journal of Law 2012, No. 1, 108, 114; Cai Chang, Studies in Law and Business 2013, No. 2, 113, 114f.; Yang Lixin/Li Jialun, Science of Law 2012, No. 2, 157, 158.

873 Yang Lixin/Li Jialun, Science of Law 2012, No. 2, 157, 162; Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 84.

cc) Die Möglichkeit, von der Quelle an die Rechtsverletzungen zu vermindern

Der ISP ist prinzipiell Mittäter mit dem unmittelbaren rechtsverletzenden Internetnutzer. Jedoch ist der ISP als Verletzer im Vergleich mit dem rechtsverletzenden Internetnutzer einfacher zu finden. Gleichzeitig hat er auch die größere Fähigkeit, die Schäden des Verletzten zu ersetzen. Der vernünftige Verletzte würde sich lieber direkt an den ISP wenden, um Schadensersatz zu verlangen, als den Internetnutzer als unmittelbaren Verletzer zu suchen. Obwohl es gesetzlich geregelt ist, dass der ISP von dem unmittelbaren Verletzer den von ihm haftenden Teil verlangen kann, ist es in der Praxis aber schwierig zu verwirklichen.[874] Das alles gibt dem Internetnutzer die Chance, eine Haftung wegen seiner rechtswidrigen Handlung zu vermeiden. Seine Kosten für rechtswidrige Handlungen sind im großen Maße vermindert.[875]

Das „Notice-and-Take-Down"-Verfahren hat tatsächlich die Kosten des Internetnutzers wegen seiner rechtswidrigen Handlung durch die gewerblichen Kosten des ISP zur Kontrolle rechtswidriger Inhalte auf seiner Webseite ersetzt.[876] Nach der Theorie der ökonomischen Analyse des Rechts soll derjenige haften, der mit geringsten Kosten das rechtsverletzende Ergebnis vermeiden kann.[877] Für die Internetnutzer liegen die Transaktionskosten auf einem direkten Zivilprozess gegen ihn, um eine von ihm begangene Rechtsverletzung zu beurteilen. Im Gegensatz liegen die Transaktionskosten beim ISP im Fall von „Notice-and-Take-Down"-Verfahren auf der Bereitstellung Fachleute, um „Notice" über Rechtsverletzungen zu bearbeiten, die möglichen Rechtsverletzungen zu beurteilen, und gegebenenfalls den rechtswidrigen Inhalt zu löschen. Dazu kommt noch der mögliche Zivilprozess gegen den ISP wegen Pflichtverletzung und gegebenenfalls eine Klage gegen den Internetnutzer als der tatsächliche Verletzer, um den vom ISP zuerst bezahlten Schadensersatz zu übernehmen. Offensichtlich werden durch das „Notice-and-Take-Down"-Verfahren zu viele Umwege gebaut. Ökonomisch betrachtet soll in diesem Fall der Internetnutzer direkt der Träger der Haftung sein.[878]

---

874 Zhou Hua, Journal of China Three Gorges University (Humanities & Social Sciences) 2012, No. 5, 87, 89.

875 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 89.

876 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 85

877 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 85

878 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 85

§ 36 des Delikthaftungsgesetzes hat durch das „Notice-and-Take-Down"-Verfahren die Last dem ISP gegeben. Als Ergebnis würde der Internetnutzer eine rechtswidrige Handlung wegen ihrer geringen Kosten leicht begehen, während der ISP eine schwere Pflicht zur Kontrolle der rechtswidrigen Inhalte und ein hohes Risiko für die falsche Beurteilung tragen muss.

Das „Notice-and-Take-Down"-Verfahren ist wegen der Besonderheit im Internet für den schnellen Schutz des Persönlichkeitsrechts des Betroffenen vor vertiefter Rechtsverletzung effizient, aber nicht geeignet, die Rechtsverletzungen von der Quelle an zu vermeiden oder eine gesunde Kultur im Internet aufzubauen.[879]

3. Der Unterlassungsanspruch gegen den ISP

Ein direkter Ausdruck über einen Unterlassungsanspruch besteht in § 9 Abs. 1 Nr. 6 „Regelung einiger Fragen über die Gesetzesanwendung auf die Beurteilung der Fälle über den zivilrechtlichen Rechtsstreit wegen Verletzung des informationellen Verbreitungsrechts im Internet", wonach der Verletzte nach der ersten Rechtsverletzung das Recht hat, vom ISP zu verlangen, passende Maßnahmen vorzunehmen, um die wiederholte Rechtsverletzung durch den gleichen Nutzer zu vermeiden oder rechtzeitig zu stoppen. Sonst wird die Kenntnisnahme des ISP über die Rechtverletzung gesetzlich vermutet. Die Schuld des ISP wird deswegen begründet; er muss dann gemäß § 8 Abs. 1 Satz 2 dieser Regelung als Gehilfe haften.

Aber als Grundlage des Unterlassungsanspruchs ist diese als Rechtsprechung erlassene Regelung nicht in der Lage. Meiner Meinung nach korrespondiert § 9 Abs. 1 Nr. 6 i.V.m. § 8 Abs. 1 Satz 2 der oben genannten Regelung mit § 36 Abs. 3 Delikthaftungsgesetz, das als Grundlage des Unterlassungsanspruchs gegen den ISP angesehen werden kann. Gemäß § 36 Abs. 3 Delikthaftungsgesetz soll der ISP mit demjenigen Internetnutzer gesamtschuldnerisch für den gesamten Schaden haften, wenn der ISP wusste, dass der Internetnutzer unter Benutzung seines Internetdienstes die zivilrechtlichen Rechte oder Interessen des anderen verletzt und keine nötigen Maßnahmen vorgenommen hat. Diese Paragraphen können kombiniert verwendet werden. Nach der ersten Rechtsverletzung soll die Kenntnisnahme des ISP über die wiederholte Rechtsverletzung durch den gleichen Nutzer vermutet werden. Der ISP soll nötige Maßnahmen vornehmen; sonst muss er als Gehilfe gesamtschuldnerisch haften, weil hier ein bewusstes Nicht-Verhalten besteht, damit eine Garantenstellung begründet werden kann.

879 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 85

Ein Unterlassungsanspruch im Fall von Persönlichkeitsrechtsverletzung ist in China relativ neu. Die „Regelung einiger Fragen über die Gesetzesanwendung auf die Beurteilung der Fälle über den zivilrechtlichen Rechtsstreit wegen Verletzung des informationellen Verbreitungsrechts im Internet", die direkt den Unterlassungsanspruch regelt, ist auch erst seit 1.1.2013 in Kraft getreten. Über dieses Thema fehlen in der Literatur und in der Praxis Diskussionen.

Aber eine Anlehnung an das deutsche Recht könnte in diesem Fall durchaus möglich sein, weil das am 1.10.2007 in Kraft getretene chinesische Sachenrechtgesetz die Struktur des Sachenrechts im deutschen BGB übergenommen hat, und § 35 des chinesischen Sachenrechtgesetzes eine direkte Übersetzung von § 1004 Abs. 1 BGB ist, wo die Grundlage des Unterlassungsanspruchs liegt.

4. Der Schadensersatzanspruch und der Schmerzensgeldanspruch gegen den ISP

Hätte der ISP die Beseitigungs- oder Unterlassungspflicht vorsätzlich oder fahrlässig verletzt, könnte der Betroffene Schadensersatz oder Schmerzensgeld von ihm verlangen.[880] Wegen der gesamtschuldnerischen Haftung gelten für die weiteren Voraussetzungen eines Schadensersatz- oder Schmerzensgeldanspruchs gegen den ISP die gleich Prinzipien wie gegen den unmittelbaren rechtsverletzenden Internetnutzer.[881]

Obwohl Deutschland und China bei der Beurteilung der Schadensersatz- und Schmerzensgeldansprüche ähnliche Regelungen haben, führt dies wegen der unterschiedliche Kriterien bei der Beurteilung der Verletzung der Beseitigungs- und Unterlassungspflicht zu unterschiedlichen Ergebnisse. In Deutschland beschränkt sich die Beseitigungs- und Unterlassungspflicht auf positive Kenntnis der Rechtsverletzung. Im Gegensatz dazu besteht die Handlungspflicht des ISP in China auch auf der Rechtsverletzung, die er aufgrund des Umstandes kennen soll.

Die gesetzliche Gestaltung in China könnte dazu führen, dass der ISP ein hohes Risiko für die von seinen Nutzern begangene Rechtsverletzung tragen muss.[882] Als unmittelbares Ergebnis dieser Wirkungen könnte der ISP in China die allgemeine Überwachungspflicht tatsächlich tragen müssen. Dies wäre offensichtlich mit der Tendenz der Entwicklung des Internets und auch der aktuellsten Rechtsprechung des Obersten Volksgerichtshofes nicht zu vereinbaren.[883]

---

880 Vgl. Liu Xiaochun, Internet Law Review 2011, No. 1, 3, 8, 15.

881 Siehe oben unter § 11 I 2 a) und b).

882 Mei Xiaying/Liu Ming, Science of Law 2013, No. 2, 82, 87.

883 Siehe oben unter § 10 II 1.

III. Eine Rechtsvergleichende Zusammenfassung

Die Providerhaftung bietet dem Verletzten Schutz aus drei Aspekten, nämlich die laufende Rechtsverletzung rechtzeitig zu stoppen, den entstehenden Schaden zu ersetzen und die zukünftige gleichartige Rechtsverletzung zu vermeiden.

1. Über Beseitigungsanspruch

Um die laufende Rechtsverletzung rechtzeitig zu stoppen ist durch den Beseitigungsanspruch verwirklicht. Dafür hat Deutschland „Notice-and-Action"-Verfahren bzw. Kommunikationsprozess und China „Notice-and-Take-Down"-Verfahren zur Verfügung gestellt. Die beiden Verfahren stammen aus dem „Notice-and-Take-Down"-Verfahren in den USA, das den ISP auf dem Kernpunkt des Anspruchsprozesses stellt. Funktional betrachtet dienen die beiden Verfahren dazu, die Rechte des Verletzten ohne Gerichtsverfahren effizient zu schützen.

Im Vergleich mit dem „Notice-and-Action"-Verfahren in Deutschland ist das Chinesische „Notice-and-Take-Down"-Verfahren zum Schutz des Verletzten effizienter, weil ein „Anti-Notice"-Verfahren vernachlässigt wird. Dies könnte aber zur Beschränkung der Meinungsfreiheit des Äußernden führen. Als Ausgleich kann der Äußernde jedenfalls Delikthaftung wegen falsches „Notice" gegen den „Notice-Geber (Melder)" verlangen.

Der Kommunikationsprozess erfordert nicht, dass der ISP nach der Beanstandung des Betroffenen den bezüglichen Inhalt sofort sperrt. Das bietet zwar einen guten Schutz der Meinungsfreiheit, aber im Fall der schwerwiegenden Persönlichkeitsrechtsverletzung wird der Betroffene nicht rechtzeitig genug geschützt. Der Kommunikationsprozess soll für diesen Sonderfall eine vorläufige Beschränkung der Meinungsfreiheit bejahen.

Von den beiden Verfahren sind Verbesserungen zu erwarten. Idealerweise wäre eine Kombination beider Verfahren, dass für den Sonderfall wie zum Beispiel im Fall der schwerwiegenden Persönlichkeitsrechtsverletzung ein einstweiliges schnelles „Take-Down" Vorrang hat, während für normale Situationen ein „Anti-Notice" berücksichtigt werden muss.

2. Über Schadensersatz- und Schmerzensgeldansprüche

Die Beurteilung der Schadensersatz- und Schmerzensgeldansprüche gegen den ISP als Störer setzt in Deutschland und China voraus, dass der ISP die Beseitigungs- oder Unterlassungspflicht verletzt hat. In den beiden Ländern ist es anerkannt, dass eine Handlungspflicht des ISP besteht, wenn er die Rechtsverletzung den Umständen nach kennen soll. Von dieser Hinsicht gibt es in den beiden Ländern kaum ein Unterschied.

Aber für die Beurteilung, wann der ISP eine Rechtsverletzung kennen soll, hat China strengere Regeln entwickelt. Dies könnte dazu führen, dass der ISP in China tatsächlich die allgemeine Überwachungspflicht trägt.

3. Über Unterlassungsanspruch

Um die zukünftige gleichartige Rechtsverletzung zu vermeiden wurden in Deutschland ausführliche Theorien über Unterlassungsanspruch entwickelt.

Anders als in Deutschland gibt es in China kein Konzept wie Unterlassungsanspruch gegen den Provider. Ein Unterlassungsanspruch gegen den Provider wird in China im Rahmen der Delikthaftung bzw. der Mittäterhaftung des Providers betrachtet. Wenn eine vom Internetnutzer begangene Rechtsverletzung eine wiederholte Rechtsverletzung ist, soll der Provider über die Rechtsverletzung wissen und sich ohne „Notice" des Verletzten aktiv verhalten, die Inhalte zu sperren oder entfernen, um eine gesamtschuldnerische Haftung mit dem unmittelbaren Verletzer zu vermeiden.

Durch diesen Weg kann in China das gleiche Ergebnis im Sinne vom Schutz der Verletzten erreicht werden. Aber weil die allgemein anerkannten Grundtheorien über Unterlassungsanspruch fehlen, ist es nicht zu vermeiden, willkürliche Entscheidungen bei der Beurteilung der Pflichte des Providers zu treffen.

Jedoch ist eine Anlehnung des chinesischen Rechts am deutschen Recht in diesem Fall möglich, weil das chinesische Sachenrechtgesetz die Struktur vom Sachenrecht im deutschen BGB übergenommen hat und § 35 chinesisches Sachenrechtgesetzes eine direkte Übersetzung von § 1004 Abs. 1 BGB ist, wo die Grundlage des Unterlassungsanspruchs geregelt ist.

Bezüglich des Unterlassungsanspruchs ist übrigens der Gedanke des BGH besonders zu empfehlen, dass der ISP ein Selbstkontroll-System dem Betroffenen zur Verfügung stellt, um dem Betroffenen die Aufgabe zu übergeben, die zukünftige gleichartige Rechtsverletzung aufzuspüren.

§ 13 Die anderen Maßnahmen zum Schutz des Rechtsverletzten während der Menschenfleischsuche

I. Ansprüche gegen den ICP und ISP als Täter oder Mittäter

Im Fall von unmittelbaren Rechtsverletzungen durch den ICP und ISP haften sie als Täter oder Mittäter.[884] Dementsprechend hat der Verletzte die Ansprüche gegen sie vergleichbar mit den gegen den unmittelbaren rechtsverletzenden Internetnutzer.[885] Wegen mangelnden Besonderheiten werden diese Ansprüche nicht mehr konkret diskutiert.

II. Selbstregulierung durch Internetnutzer

Die meisten Menschenfleischsuchen sind von den Internetnutzern unmittelbar eingeleitet und durchgeführt. Deswegen kann es eine wirksame Methode sein, durch die Selbstregulierung das Verhalten der Internetnutzer zu disziplinieren, um die Rechtsverletzungen von der Quelle an zu vermindern.

Am 1.1.2009 hat in China eine Internetgruppe, die „Nichtorganisatorische Alliance der Menschenfleischsuche" heißt, eine „Menschenfleischsuche-Konvention (Version 1.0 Beta)" in einem bekannten Internetforum „Douban" veröffentlicht, um an die Internetnutzer zu appellieren, ihr Verhalten während der Menschenfleischsuche selbst zu kontrollieren.[886]

Die Konvention gemäß ihrem Wortlaut zielt darauf, die moralischen Gedanken der Internetnutzer zu wecken, richtiges Verständnis über Menschenfleischsuche zu verbreiten, und die richtige Orientierung der Entwicklung der Menschenfleischsuche zu garantieren.

Die wichtigsten Inhalte bestehen in den folgenden Paragraphen der Konvention:

§ 2. Es wird vorgeschlagen, die Menschenfleischsuche im originalen Sinnen zu benutzen, um Kenntnis zu erlangen.

§ 3. Die Informationen im Bereich der Privatsphäre der Anderen sollen möglicherweise nicht durch Menschenfleischsuche gesucht werden.

---

884 Siehe oben unter § 9, § 10 I 1 und II 3.

885 Vgl. oben unter § 11 I.

886 http://www.douban.com/group/topic/5032183/ (besucht am 04.04.2015).

§ 4. Die Offenlegung der Privatsphäre der Anderen soll möglicherweise verhindert werden. Die Privatsphäre der Anderen soll nicht im öffentlichen Bereich einer Webseite offengelegt werden.

§ 5. Für den Fall der Korruption und den Fall von „Strafe den Bösen, Belohne den Guten" gelten §§ 3, 4 nicht.

§ 6. Während der Menschenfleischsuche sollen nur die richtigen und glaubwürdigen Informationen veröffentlicht werden. Der Anbieter der Informationen soll für ihre Wahrheit verantwortlich sein.

§ 7. Nicht an der böswilligen Menschenfleischsuche teilnehmen, und Möglicherweise den Betroffenen oder den ISP über die böswillige Menschenfleischsuche informieren.[887]

Diese Konvention hat gezeigt, dass einige Internetnutzer in China die negative Wirkung der Menschenfleischsuche bemerkt haben, und versuchen, die teilnehmenden Internetnutzer der Menschenfleischsuche zu disziplinieren. Jedoch sind nicht alle Inhalte der Konvention mit dem Gesetz zu vereinbaren.

Vom Gesetz zu begrüßen sind die Vorschläge in § 3 und § 4, auf die Privatsphäre der Anderen aufzupassen und die Privatsphäre betroffene Information nicht im öffentlichen Bereich offenzulegen. Durch den Vorschlag in § 6 wird vermieden, aufgrund von falschen Tatsachenbehauptungen eine Ehrverletzung zu begründen. Der Vorschlag von § 7 garantiert weiterhin den rechtsmäßigen Zweck einer Menschenfleischsuche. Problematisch ist die Regelung in § 5, die die Teilnehmer der Menschenfleischsuche berechtigt, im Fall der Entdeckung von Korruptionen oder im Fall von „Strafe den Bösen, Belohne den Guten" die Privatsphäre betroffene Information der Zielperson offenzulegen. § 5 der Konvention hat wiederum das Lynchjustiz-Merkmal der Menschenfleischsuche dargestellt. Die Fähigkeit der Internetnutzer, um „Böse" und „Gut" zu beurteilen, wird in § 5 der Konvention leider nicht ausreichend berücksichtigt.

Immerhin ist die Methode von Selbstregulierung im Vergleich mit den Maßnahmen durch die Regierung milder und von den Internetnutzern leichter zu akzeptieren. Es ist zu überlegen, durch die Selbstregulierung der Internetnutzer flankiert die gesunde Entwicklung der Menschenfleischsuche anzuleiten. Vorausgesetzt ist jedoch eine besser durchdachte Konvention.

III. Regulierung durch die ISP

Mit der Popularisierung der Menschenfleischsuche sind viele ISP motiviert, spezifische Bereiche auf ihren Webseiten für Menschenfleischsuche zur Verfügung

887 http://www.douban.com/group/topic/5032183/ (besucht am 04.04.2015).

zu stellen. Diese ISP sollen mehr Sorgfaltspflicht über den Inhalt der Menschenfleischsuche als die anderen ISP tragen, auf deren Webseiten die Menschenfleischsuche selten passiert. Für die ISP, die mit Absicht ihre Webseiten für Menschenfleischsuche bereitgestellt haben, ist es vorstellbar, dass sie die allgemeine Überwachungspflicht auf die Inhalte der Menschenfleischsuche haben.

In zwei Entscheidungen über Urheberrecht in China[888] haben die Gerichte aufgrund der hohen Gefahr der Urheberrechtsverletzung auf der Movie-Sharing-Webseite festgestellt, dass der ISP von solchen Webseiten eine allgemeine Überwachungspflicht bezüglich der Inhalte hat.[889] Die Urheberrechtsverletzungen auf der Movie-Sharing-Webseite haben normalerweise wirtschaftliches Interesse als Schutzobjekt, das durch Schadensersatz wiedergutgemacht werden kann, während der Menschenfleischsuche bezüglich hauptsächlich um Persönlichkeitsrechtsverletzungen geht, die starke Prangerwirkung dem Betroffenen bringen könnte, die durch Schadensersatz schlecht wiedergutgemacht werden kann. Übrigens hat Menschenfleischsuche eine hohe Gefahr von Persönlichkeitsrechtsverletzung.[890] In dieser Hinsicht braucht es für die Menschenfleischsuche-Webseite höhere oder mindestens ebenso hohe Überwachungspflichten wie für die Movie-Sharing-Webseite.

Diese Meinung wird in der Praxis tatsächlich von einigen ISP in China akzeptiert, die Menschenfleischsuche-Webseiten betreiben. Der Betreiber von „Mop", die Webseite aus der die Menschenfleischsuche in China stammt, hat auf der Webseite deutlich geschrieben, dass alle Inhalte, die zur Privatsphäre gehören, während der Menschenfleischsuche gelöscht oder gesperrt werden.[891] Der Betreiber kontrolliert tatsächlich alle Inhalte während der Menschenfleischsuche.[892] Der Betreiber von „Douban", der auch eine Menschenfleischsuche-Webseite zur Verfügung gestellt hat, hat auch Regelungen für Menschenfleischsuche auf seiner Webseite deutlich festgelegt: die Suche nach persönlicher Privatsphäre, einschließlich Name, Kontaktinformation, ID, privates Verhalten, sind verboten;

888 Haidian Unteres Volksgericht, Urt. v. 09.12.2008 - (2008) hai min chu zi di 14025 hao; Shanghai Erstes Mittleres Volksgericht, Urt. v. 23.06.2009 - (2009) hu yi zhong min wu (zhi) zhong zi di 20 hao.

889 Chen Jinchuan, Intellectual Property 2011, No. 2, 56, 60.

890 Vgl. Liu Wenjie, Peking University Law Journal 2012, No. 2, 395, 410.

891 Meng chi xue gao, http://dzh.mop.com/whbm/20080828/0/F53OSOI1b228c4z8.shtml (besucht am 04.04.2015).

892 Meng chi xue gao, http://dzh.mop.com/whbm/20080828/0/F53OSOI1b228c4z8.shtml (besucht am 04.04.2015); vgl. Wang Chengwei, Journal of Public Management 2011, No. 4, 21, 29.

wegen der Schwierigkeit, die Rechtmäßigkeit der Menschenfleischsuche zu beurteilen, darf die Suche nur Prominente als Zielpersonen haben.[893]

Es wird in der Literatur sogar vorgeschlagen, dass der Veranlasser vor der Einleitung einer Menschenfleischsuche erst einen Antrag an den ISP stellen muss, um die Notwendigkeit der Menschenfleischsuche zu beweisen und eine Erlaubnis für die Suche zu erhalten.[894]

Durch die Diskussion in dieser Arbeit soll erkennbar werden, dass die ISP in China eine hohe Pflicht und ein hohes Risiko für die auf ihren Webseiten passierten Rechtsverletzungen tragen müssen. Um die Haftung wegen einer Persönlichkeitsrechtsverletzung durch ihren Nutzer zu erleichtern, ist es für die ISP sinnvoller, Maßnahmen vorzunehmen, die Inhalte der Menschenfleischsuche zu kontrollieren.

Übrigens könnte eine qualifizierte Menschenfleischsuche zahlreiche Teilnehmer bekommen, von denen der ISP gut profitieren kann. Es wird deswegen auch nicht gefordert, dass er eine höhere Überwachungspflicht als ein anderer ISP tragen muss.

IV. Einleitung der Menschenfleischsuche von Journalisten oder zuständigen Behörden

Wie am Anfang der Arbeit schon erwähnt wurde, gibt es in Deutschland nicht selten Menschenfleischsuche ähnliche Ereignisse.[895] Der Unterschied zwischen diesen Ereignissen und Menschenfleischsuche liegt darin, dass sie häufig von den Journalisten oder zuständigen Behörden eingeleitet worden sind, und die Offenlegung der Informationen der Zielperson häufig offline durchgeführt wird. Durch diesen Weg können die rechtswidrigen Handlungen während der Suche im großen Maße vermieden werden.

Die Menschenfleischsuchen mit den Motivationen, um Korruptionen oder andere rechtswidrige Verhalten aufzudecken, zielen häufig darauf, die Zielperson zu bestrafen. Dieses Ziel kann ebenfalls erreicht werden, wenn die Internetnutzer die bezügliche Information der Zielperson den zuständigen Behörden offline mitteilen. Das wäre ein idealer Weg, um die Nachteile der Menschenfleischsuche zu vermeiden. Dies setzt jedoch voraus, dass genug Vertrauen vom Volk an die Regierung vorhanden ist,[896] und die zuständigen Behörden die vorkommenden

893 http://www.douban.com/group/72544/?type=essence (besucht am 04.04.2015).
894 Tian Feilong, Internet Law Review 2009, 80, 91.
895 Siehe oben unter § 1 VII 2 c).
896 Siehe oben unter § 1 V 3 b).

Fälle effizient lösen können. Die Erfüllung dieser Voraussetzungen ist in China zu erwarten.

Die Menschenfleischsuchen mit den Motivationen, um gegen unmoralisches Verhalten zu kämpfen oder um die Internetnutzer zu amüsieren, können idealerweise durch Berichterstattung von den Journalisten eingeleitet werden. Wegen ihrer professionellen Ethik werden die Persönlichkeitsrechte der Zielperson besser berücksichtigt.

Diese Wege sind jedoch nur zu empfehlen und können als Vorbilder der zukünftigen Menschenfleischsuchen berücksichtigt werden. Die durch Internetnutzer eingeleiteten rechtmäßigen Menschenfleischsuchen dürfen nicht zwingend durch diese Wege ersetzt werden.