

2 Fälle und Entscheidungen

Im folgenden Teil werden die im weiteren Verlauf der Arbeit analysierten Sachverhalte realer Gerichtsentscheidungen und hypothetischer Fälle dargestellt.¹

2.1 Fall: Georgier

Der georgische Staatsangehöriger G., der seinen Wohnsitz in Deutschland hat, platzierte auf seinen Skype-Avatar² nach dem bewaffneten Konflikt zwischen Russland und Georgien im August, 2008 folgende Aussage: „Russia is a devil State“. Strafrechtliche Zuständigkeit.

2.2 Fall: Herr Pornikov

Der russische Staatsangehöriger Herr Pornikov, der sich auf dem Territorium des Staates A befand, speicherte jedermann zugängliche Websites (nach russischem Recht strafbaren) kinderpornographischen Inhalts auf einem Server des Staates A. Außerdem verbreitete er entsprechende Inhalte mittels E-Mail. Nach dem Recht des Staates A. sind das Zugänglichmachen und die Verbreitung der kinderpornographischen Materialien (z.B. wegen höherer Altersgrenzen) rechtswidrig, allerdings nicht strafbar.³ P. wurde aufgrund der Rechtswidrigkeit seines

¹ Für die Lösungen der Fälle siehe Kapitel 6 Falllösung, S. 179 ff.

² Avatar – Hauptbild von Nutzern der VoIP-Dienste (z.B. Skype), soziale Netzwerken (z.B. Facebook, StudiVZ) usw. mit möglichen kurzen Privatinformationen, Nachrichten, Slogans usw. Die Informationen und das Bild sind normalerweise allen Internetnutzern zugänglich, es sei denn, der Nutzer es anderes einstellt: [http://de.wikipedia.org/wiki/Avatar_\(Internet\)](http://de.wikipedia.org/wiki/Avatar_(Internet)).

³ Im Bezug auf die Kinderpornographie gibt es viele Fragen, die entscheidend sind bei der Qualifizierung dieser Tat, die allerdings unterschiedlich je nach der Rechtsordnung einzustufen sind. Beispielsweise wird die Frage der Altersgrenze der Kinder, die tatbestandsmäßig sind, auf verschiedene Weise entschieden. Ein anderer umstrittener Punkt kann die (Nicht)Kriminalisierung der sogenannten „virtual child pornography“ sein. Darunter versteht man ein digitalisiertes Bild, ein Computerbild oder computererzeugtes Bild, bei dem nicht möglich zu unterscheiden ist, ob Kinder tatsächlich in die sexuellen Handlungen involviert waren oder nicht. Zum Beispiel blieb „virtual child pornography“ in den USA nach der Entscheidung des Supreme Court (*Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 2002) bis 2003 legal. Mit dem Verabschieden des Protect Act (April 2003) wurde das ursprüngliche Verbot wieder eingeführt. In Russland gibt es kein Tatbe-

Handelns zur Verantwortung gezogen und zu einer Geldbuße verurteilt. Grundlage zur Legitimierung russischer Strafgewalt?

2.3 Fall: Herr Lust

Der deutsche Staatsangehöriger Herr Lust, der sich auf dem Territorium des Staates A befand, speicherte jedermann zugängliche Websites (nach deutschem Recht strafbaren) kinderpornographischen Inhalts auf einem Server des Staates A. Außerdem verbreitete er entsprechende Inhalte mittels E-Mail. Nach dem Recht des Staates A. sind das Zugänglichmachen und die Verbreitung der kinderpornographischen Materialien rechtswidrig, allerdings nicht strafbar. L. wurde aufgrund der Rechtswidrigkeit seines Handelns zur Verantwortung gezogen und zu einer Geldbuße verurteilt. Grundlage zur Legitimierung deutscher Strafgewalt?⁴

2.4 Fall: Berliner Unternehmen

Der Zentralrechner des Unternehmens D in Berlin wurde über das Internet von einem russischen Hacker von einem sich in Moskau befindlichen Rechner angegriffen.

- a) *Der Hacker verschaffte sich Zugang zu Informationen des Unternehmens (allerdings nicht zu den Betriebs- oder Geschäftsgeheimnissen von D). Dabei wurden keine Informationen geändert und die Website des Unternehmens auch nicht beschädigt. Für das Unternehmen entstanden daher kein Schaden und keine Beeinträchtigung seines Computernetzwerks.⁵*
- b) *Durch den Eingriff wurden Informationen auf der Website (mit TLD „com“) vom Hacker erheblich verändert, allerdings keine solchen, die zu den Betriebs- oder Geschäftsgeheimnissen des Unternehmens D gehören.*

stand, der „virtual child pornography“ kriminalisieren würde. Siehe auch dazu: *Brenner/Koops*, *Approaches to Cybercrime Jurisdiction*, 2004, S. 3 ff.

⁴ Siehe dazu: *Hörmle*, in: Münchener Kommentar, § 184 StGB, Rn. 107 ff.

⁵ Nach Angaben der Antivirus-Unternehmen wird oft von „Forschern der Computerfauna“ in die gesicherten Systeme eingedrängt oder neue Viren entwickelt um bloß ihre „Kräfte zu messen“. Interessant, dass einige fertig geschriebene Viren und Hacking-Algorithmen ohne weiteres Nutzen den Antivirus-Unternehmen von Hackern selbst geschickt wurden, damit sie nicht weiter für schädlichen Zwecken verbreitet werden konnten: *Kaspersky*, *Kompýuternoe zlovredstvo*, 2009, S. 15 ff.

- c) *Durch den Eingriff wurden solche Informationen auf dem Server des Unternehmens vom Hacker erheblich verändert, die zu dessen Geschäftsgeheimnissen gehören.*

2.5 Fall: Moskauer Unternehmen

Der Zentralrechner des russischen Unternehmens R in Moskau wurde mittels Internet von einem Hacker deutscher Staatsangehörigkeit, welcher sich in Berlin aufhielt, angegriffen.

- a) *Der deutsche Hacker verschaffte sich dabei Zugang zu den internen Daten des Unternehmens des R. Dabei wurden Informationen nicht verändert, kopiert oder anderweitig beschädigt. Für das Unternehmen entstanden daher kein Schaden und keine Beeinträchtigung seines Computernetzwerks.*
- b) *Durch den Eingriff wurden Informationen auf der Website des Unternehmens vom Hacker erheblich verändert, allerdings keine solchen, die zu den Betriebs- oder Geschäftsgeheimnissen gehören.*

2.6 Fall: Computervirus „Loveletter“

Ein Philippinischer Staatsangehöriger (P) entwickelte das Virus „Loveletter“ und verbreitete es von den Philippinen aus im Internet. Weltweit waren mehrere Computer (von Privatpersonen und Unternehmen) betroffen, unter anderem auch in Russland, Deutschland und in den USA.

- a) *P schickte virenverseuchte E-Mails weltweit an unbekannte Internet-Nutzer.*
- b) *P platzierte das Virus in ein Softwareprogramm, das frei zugänglich und zum kostenlosen Herunterladen auf einer Website mit amerikanischer TLD⁶ angeboten wurde. Das Herunterladen des Programms führte zur Virenverseuchung des Computers.⁷*

⁶ Top-Level-Domain, z.B. „at“ für Österreich, „ru“ für Russland, „de“ für Deutschland; thematisch: „edu“, „net“, „com“.

⁷ Love Bug infects computers worldwide: <http://www.highbeam.com/doc/1P1-26415167.html>; Goodman/ Brenner, Criminal Conduct in Cyberspace, 2002.

2.7 Fall: Kasache (Entscheidung des Bezirksgerichts, Russland)⁸

Ein Kasache, der sich als Russe ausgab und sich in Kasachstan aufhielt, stellte in einen Internetblog der Website eines russischen Servers mit Blick auf armenische Volkszugehörige herabsetzende Äußerungen ein.

2.8 Fall: Konzentrationslager

Der australische Staatsangehörige A stellte Informationen auf einem australischen Server ins Internet, in denen er unter dem Vorwand wissenschaftlicher Forschung darlegte, dass die Konzentrationslager in Russland gar nicht existierten und Behauptungen über diesbezügliche Opfer eine Erfindung sind.

2.9 Fall: Australier (Entscheidung des deutschen BGH)⁹

Der australische Bürger A machte über das Internet Materialien durch das Versenden englischsprachiger E-Mails (auch an Adressaten in Deutschland) zugänglich, in denen unter dem Vorwand wissenschaftlicher Forschung die unter der Herrschaft des Nationalsozialismus begangene Ermordung der Juden bestritt und als Erfindung „jüdischer Kreise“ dargestellte. Außerdem speicherte er Websites gleichen Inhalts auf einem australischen Server, der Internetnutzern in Deutschland zugänglich war. Unter anderen wurden folgende Äußerungen eingespeist: "Wir erklären stolz, dass es bis heute keinen Beweis dafür gibt, dass Millionen von Menschen in Menschengaskammern umgebracht wurden." „Dies allein ist schon eine gute Nachricht, bedeutet es doch, dass ca. 3,2 Millionen Menschen nicht in Auschwitz gestorben sind - ein Grund zum Feiern." „Daher können alle Deutschen und Deutschstämmigen ohne den aufgezwungenen Schuldkomplex leben, mit dem sie eine böartige Denkweise ein halbes Jahrhundert lang versklavt hat."

⁸ Stadtbezirksgericht (StBezG) von Krasnodar, Bulletin N8, August 2008.

⁹ BGHSt 46, 212 („Ausschwitzlüge“-Urteil); dazu siehe: Götting, Kriminalistik 2007, S. 615 ff.

2.10 Fall: CompuServe (Entscheidung des Münchener Amtsgerichts)¹⁰

Die Firma CompuServe Information Services GmbH (Deutschland) war eine hundertprozentige Tochterfirma des weltweit tätigen Online-Service-Providers CompuServe (USA). CompuServe (Deutschland) hatte u.a. die Aufgabe, für Kunden von CompuServe (USA) in Deutschland Einwahlknoten bereitzustellen. Der jeweilige Kunde wählte sich bei dem für ihn nächstgelegenen Einwahlknoten in Deutschland ein. Er wurde dann von dort ohne weitere Plausibilitätsprüfung via Standleitung zwischen Tochter- und Muttergesellschaft mit dem in den USA befindlichen Rechenzentrum der Muttergesellschaft verbunden. Der Angeklagte war Geschäftsführer der Firma CompuServe Information Services GmbH (Deutschland). Das Gericht stellte fest, dass der Angeklagte, ein in Deutschland wohnhafter schweizer Staatsangehöriger, gemeinschaftlich mit der Firma CompuServe (USA) Kunden von CompuServe (USA) in Deutschland gewalt-, kinder- und tierpornographische Darstellungen zugänglich gemacht hatte. Die Darstellungen wurden auf dem Server von CompuServe (USA) zur Nutzung bereitgehalten. CompuServe Information Services GmbH hat die gegebenen Inhalte für deutsche Kunden zugänglich gemacht. Der Angeklagte wurde schuldig gesprochen. Keiner von den Mittätern von CompuServe (USA) wurde hingegen verurteilt.

2.11 Fall: People v. World Interactive Gaming Corp. (Entscheidung des New Yorker Gerichts)¹¹

Auf dem Territorium des Staates New York sind Glücksspiele verboten. Ein entsprechendes Online-Angebot wurde auf einem Server in Antigua gehostet und von einer Tochterfirma von „World Interactive Gaming Corporation“ (WIGC) mit einer nach dem dortigen Recht notwendigen Genehmigung betrieben. Ist es der WIGC erlaubt, auf dem Territorium des Staates New York verbotene Glücksspiele über das Internet anzubieten?

¹⁰ AG München NJW 1998, 2836 („CompuServe“-Urteil); siehe dazu: Hörnle, in: Münchener Kommentar, § 184g StGB, Rn. 1 ff., § 184 StGB, Rn. 107 ff.

¹¹ People v. World Interactive Gaming Corp., 714 N.Y.C. 2d 844 (N.Y. App. Div. 1999).

<http://www.springer.com/978-3-658-04398-8>

Internationales Strafrecht im Cyberspace
Strafrechtliche Analyse der Rechtslage in Deutschland,
Russland und den USA

Paramonova, S.

2013, XXX, 314 S. 9 Abb., 6 Abb. in Farbe., Softcover

ISBN: 978-3-658-04398-8