HUMBOLDT FORUM RECHT
- Die juristische Internet-Zeitschrift an der Humboldt-Universität zu Berlin -

HFR 10/2012 ISSN 1862-7617 Aufsatz

Dr. Tobias Reinbacher, Berlin*

Zur Strafbarkeit des Streamings und der Umgehung von Geo-IP-Sperren durch private Nutzer

Die Bereitstellung digitaler Inhalte im Internet ist durch oftmals regional abweichende Lizenzbedingungen reglementiert, deren Durchsetzung durch technische Maßnahmen wie insbesondere den sogenannten "Geo-IP-Sperren" praktisch gesichert werden soll. Die prinzipiell globale Abrufbarkeit der Inhalte kann dabei anhand der jedem Internetteilnehmer zugewiesenen IP-Adresse länderspezifisch begrenzt werden. Durch Umleitung des Datenstroms über bestimmte Dienste sind die Inhalte jedoch auch Nutzern außerhalb lizensierter IP-Bereiche möglich.

Im Folgenden versucht Reinbacher eine strafrechtliche Einordnung des populären Streamings von Inhalten unter Umgehung derartiger Zugangskontrollmechanismen. Dabei trennt der Autor den Vorgang in zwei eigenständige Handlungen, erläutert die relevanten technischen Hintergründe separat und untersucht diese auf ihre strafrechtliche Relevanz. Insbesondere diskutiert er die Auslegung der urheberrechtlichen Schrankenbestimmungen, widerspricht hierbei der umstrittenen Einschätzung des AG Leipzig im Fall "kino.to" und bezweifelt die praktische technische Wirksamkeit der Sperren. Im Ergebnis hält Reinbacher keine der Handlungen für strafbar.

A. Einleitung

1 Wer sich im Internet auf die Suche nach Filmen, TV-Serien oder Musikvideos begibt, um diese zu streamen, also online anzuschauen oder anzuhören, und dabei mit dem Satz „Dieses Video ist in Deutschland nicht verfügbar, da es möglicherweise Musik enthält, für die die erforderlichen Musikrechte von der GEMA nicht eingeräumt wurden" oder einem ähnlichen Hinweis für TV-Produkte abgespeist wird, ist auf eine so genannte „Geo-IP-Sperre" gestoßen. Diese wird durch eine spezielle Software errichtet, welche die Betreiber der jeweiligen Seiten im Internet einsetzen, um die Nutzung der Angebote auf bestimmte Länder zu beschränken bzw. bestimmte Länder auszusperren.[1]

2 Jeder Anschluss bekommt bei der Einwahl ins Internet eine IP-Adresse zugewiesen, die als seine persönliche Kennung fungiert, in der Regel – d.h. außer bei Standleitungen – dynamisch vergeben und daher nach jeder Nutzung wieder frei wird.[2] Die für Geo-IP-Sperren eingesetzte Software erkennt nun mit recht hoher Wahrscheinlichkeit, aus welchem Land der jeweilige Anschluss stammt, über den der entsprechende Server

* Der Verfasser ist Wissenschaftlicher Mitarbeiter am Lehrstuhl von Prof. Dr. Bernd Heinrich für Strafrecht, Strafprozessrecht und Urheberrecht an der Humboldt-Universität zu Berlin. Er dankt Herrn Prof. Dr. Bernd Heinrich und Herrn Dipl.-Inf. Gerrit Oldenburg herzlich für ihre hilfreichen Anmerkungen.

[1] Vgl. dazu *Mitsdörffer/Gutfleisch*, „Geo-Sperren" – wenn Videoportale ausländische Nutzer aussperren. Eine urheberrechtliche Betrachtung, MMR 2009, 731; vgl. ferner zu Geo-IP-Sperren beim so genannten Cloud Computing *Nägele/Jacobs*, Rechtsfragen des Cloud Computing, ZUM 2010, 281, 285.

[2] Ausführlich zu den IP-Adressen *Reinbacher*, Die Strafbarkeit der Vervielfältigung urheberrechtlich geschützter Werke zum privaten Gebrauch nach dem Urheberrechtsgesetz, Berlin 2007, S. 316 f.; *ders.*, Drahtlos – straflos?, in: Bosch/Bung/Klippel (Hrsg.), Geistiges Eigentum und Strafrecht, Tübingen 2011, S. 83, 90 f.

angewählt wird – und kann ihm den Zugang verwehren. Diese Methode der Zuordnung einer IP-Adresse an einen bestimmten Ort wird auch als „Geolocation" bezeichnet[3] und dadurch ermöglicht, dass die Vergabe von IP-Adressen nach einem hierarchischen System anhand von regionalen Räumen gegliedert ist.[4] So erhalten die jeweiligen Provider regelmäßig Blöcke von IP-Adressen, die sie an die Anschlüsse ihrer Kunden weitergeben. Welche IP-Adress-Blöcke etwa deutschen Providern zustehen, ist durchaus bekannt, was somit für eine Sperre fruchtbar gemacht werden kann.

3 Der Einsatz von Geolocation-Software ist dabei nicht nur für das Urheberrecht relevant, sondern kann etwa auch deutschen Nutzern den Zugang zu verbotenen Seiten mit verfassungsfeindlichen Inhalten verschließen.[5] *Hoeren*[6] nennt dies treffend einen Ansatz zur Reterritorialisierung des Internets. Gerade für die Vermarktung von lizenzabhängigen urheberrechtlich geschützten Werken bzw. Leistungsschutzrechten ist dieses Vorgehen jedoch höchst interessant. So haben Lizenznehmer oftmals nur für ein bestimmtes Territorium die entsprechenden Rechte erworben und möchten bzw. müssen die kommerzielle Auswertung daher auf diesen Bereich beschränken. Nicht wenige Fernsehsender stellen ihren Content bestimmten Nutzern – nicht selten sogar unentgeltlich – zur Verfügung. In den USA etwa ist das Portal *Hulu.com* ein beliebter Anbieter von TV-Serien verschiedener Sender, die sich zusammengeschlossen haben, um ein möglichst weit gefächertes Repertoire anbieten zu können. Deutschen Nutzern bleibt der Zugang zu diesem Portal jedoch verschlossen, da es per Geo-IP-Sperre auf das Territorium der Vereinigten Staaten beschränkt ist. Wer es mit einer IP-Adresse anwählt, die einem deutschen Provider zugeordnet werden kann, erhält die Auskunft: *„Sorry, currently our video library can only be watched from within the United States*".[7] Da viele Filme in Deutschland erst viel später in den Kinos anlaufen als in den USA, dort aber bereits online vermarktet werden, etwa durch ganz legale Streaming- oder Download-Angebote, ergibt es aus wirtschaftlichen Gesichtspunkten durchaus Sinn, dass die Rechteinhaber es den deutschen Nutzern verwehren möchten, sich den Film schon vor dem Filmstart zu besorgen. Ähnlich ist es beim britischen Fernsehsender BBC. Dieser bietet für Nutzer in Großbritannien viele Streaming-Angebote hinsichtlich seiner Nachrichten aus aller Welt an. Außerhalb des Vereinigten Königreiches sind diese allerdings nicht verfügbar. Teilweise haben Rechteinhaber ganz erfolgreich die territoriale Sperrung ihrer Werke gegenüber Internetplattformen wie *YouTube* durchsetzen können.[8]

S. 180 - HFR 11/2012 S. 2 -

4 Tatsächlich ist diese territoriale Beschränkung jedoch leicht zu umgehen. Denn der Nutzer ist nur dann ausgesperrt, wenn er eine IP-Adresse verwendet, die aus dem zugelassenen Länderpool herausfällt. Schafft man es aber, den eigenen Aufenthaltsort zu verschleiern, so ist die Geo-IP-Sperre nutzlos. Da dies auch tatsächlich gelingt, wie noch ausgeführt wird, ist es Nutzern möglich, Werke zu streamen, also Musikwerke anzuhören oder Filme anzuschauen, die ihnen eigentlich per Geo-IP-Sperre vorenthalten werden sollten. Doch wird dadurch überhaupt das Urheberrecht verletzt? Denn das Anschauen oder Anhören von Werken zählt nicht zu den Verwertungsrechten, welche den Urhebern durch das UrhG vorbehalten sind. Andererseits werden beim Streamen von Werken Datenpakete im Arbeitsspeicher abgelegt, sodass es sich um eine Kopie des Werkes und daher um eine urheberrechtlich relevante Vervielfältigung

[3] *Hoeren*, Zoning und Geolocation – Technische Ansätze zu einer Reterritorialisierung des Internet, MMR 2007, 3.
[4] *Hoeren* (o. Fn. 3), MMR 2007, 3, 4; *Mitsdörffer/Gutfleisch* (o. Fn. 1), MMR 2009, 731.
[5] Vgl. etwa *Mankowski*, Die Düsseldorfer Sperrungsverfügung – alles andere als rheinischer Karneval, MMR 2002, 277, und *Stadler*, Sperrungsverfügung gegen Access-Provider, MMR 2002, 343, zur Sperrungsverfügung der Bezirksregierung Düsseldorf bzgl. bestimmter Websites aus den USA mit rechtsradikalen Inhalten.
[6] *Hoeren* (o. Fn. 3), MMR 2007, 3.
[7] Vgl. www.hulu.com; zuletzt abgerufen am 1.7.2012.
[8] Gerade kürzlich konnte die GEMA vor dem LG Hamburg einen Rechtsstreit gegen *YouTube* für sich entscheiden, sodass es der Musikplattform untersagt wurde, Musiktitel des GEMA-Repertoires auf dem Gebiet der Bundesrepublik Deutschland zugänglich zu machen; vgl. LG Hamburg, MMR 2012, 404.

handeln könnte.

5 Ob dieses Vorgehen strafbar ist, wird in diesem Aufsatz untersucht. Dabei sind, wie bereits in der Überschrift dieses Beitrages zum Ausdruck kommen soll, zwei Vorgänge zu unterscheiden, deren mögliche Strafbarkeit hier auch getrennt behandelt wird: Das Nutzen der Angebote im Wege des Streamings (dazu unter B.) und das Umgehen des IP-Filters, um dieses zu ermöglichen (dazu unter C.). Der rechtlichen Bewertung des Vorganges werden dabei jeweils kurze technische Hinweise vorangestellt, welche notwendig sind, um eine juristische Einordnung überhaupt vornehmen zu können. Dabei werden die Erörterungen sich auf private Nutzer beschränken, also auf solche Personen, die entsprechende Angebote ausschließlich zum privaten Gebrauch wahrnehmen, sowie andererseits auf Vorgänge des Streamings, die nicht mit einem dauerhaften Download des Werkes verbunden sind.

6 ## B. Das Streaming der Inhalte

I. Technische Hinweise zum Streaming

Unter Streaming ist die kontinuierliche Übertragung (Strömen = Streaming) von Daten vom Streaming-Server auf Streaming-Clients zu verstehen.[9] Es lassen sich Live-Streaming und On-Demand-Streaming unterscheiden.[10] Bei ersterem bestimmt der Anbieter Zeitpunkt und Dauer des Streams, während bei Letzterem der Nutzer selbst („on demand") darüber entscheidet, wann er den Stream starten möchte. Bei den hier interessierenden Formaten handelt es sich regelmäßig um On-Demand-Streams, bei welchen Radio- oder TV-Sender entsprechende Angebote für Interessierte zum Abruf zur Verfügung halten. Die Dateien werden im Stream jeweils in Datenpaketen übermittelt. Im Unterschied zum vollständigen Download der Dateien können die Werke aber in der jeweils übermittelten Sequenz bereits während des Streamings angesehen oder angehört werden. Dabei werden jedoch notwendigerweise in einem Puffer des Computers, im so genannten „Buffer", in der Regel im Arbeitsspeicher (RAM), Datenpakete abgelegt, um eine bessere Abspielbarkeit zu gewährleisten.[11]

7 ### II. Strafrechtliche Bewertung

Die Strafverfahren gegen die Betreiber des illegalen Streaming-Portals Kino.to haben – insbesondere wegen der hohen Haftstrafen – für großes Aufsehen und breite Medienresonanz gesorgt. Die rechtliche Beurteilung des unautorisierten Anbietens auf einer solchen Plattform ist weniger problematisch, streiten mag man im Falle Kino.to über das Strafmaß.[12] Unklarheit herrscht jedoch hinsichtlich des Verhaltens der privaten Nutzer, die Film- oder Musikwerke im Wege des Streamings anschauen. Wie bei den Anbietern kommt auch für die Nutzer eine nach dem Urheberrecht unerlaubte Verwertung der Werke und daher zunächst insbesondere eine Strafbarkeit nach § 106 UrhG in Betracht. Nach dieser Vorschrift macht sich strafbar, wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk vervielfältigt, verbreitet oder öffentlich wiedergibt. Das AG Leipzig[13] bemerkte hierzu in der ersten Instanz, auch die Nutzer machten sich durch das Streaming der Filme strafbar, da sie eine Vervielfältigung im Sinne dieser Vorschrift vornähmen und nicht durch einen gesetzlich zugelassenen Fall im Sinne der §§ 44a ff. UrhG privilegiert seien. Diese Einschätzung trifft jedoch nicht zu, was im Folgenden belegt werden soll.

---

[9] Vgl. zum Streaming auch *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (Hrsg.), UrhR, Kommentar, 4. Aufl. (im Erscheinen), § 106 Rn. 14; *Reinbacher* (o. Fn. 2), S. 126; *Schardt*, Musikverwertung im Internet und deren vertragliche Gestaltung, ZUM 2000, 849; *Stieper*, Rezeptiver Werkgenuss als rechtmäßige Nutzung. Urheberrechtliche Bewertung des Streaming vor dem Hintergrund des EuGH-Urteils in Sachen FAPL/Murphy, MMR 2012, 12.

[10] *Stieper* (o. Fn. 9), MMR 2012, 12.

[11] *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (o. Fn. 9), § 106 Rn. 14; *Reinbacher* (o. Fn. 2), S. 126.

[12] Zuletzt verurteilte das LG Leipzig den Gründer von Kino.to zu viereinhalb Jahren Haft; vgl. LG Leipzig, Urteil vom 14.06.2012, Az.: 11 KLs 390 Js 191/11.

[13] AG Leipzig, Urteil vom 21.12.2011, Az.: 200 Ls 390 Js 184/11, Rz. 46.

8 ***1. Strafanwendungsrecht***

Zunächst einige kurze Anmerkungen zur Anwendbarkeit des deutschen Strafrechts bei Internet-Sachverhalten. Diese bestimmt sich grundsätzlich nach den §§ 3 ff. StGB. Im Urheberrecht sind jedoch die Spezialvorschriften der §§ 120 ff. UrhG zu beachten.[14] Diese beschränken den Schutzbereich des deutschen Urheberrechts bei Auslandsbezügen.[15] Streng genommen liegt außerhalb der hier geregelten Fälle gar kein (durch das deutsche UrhG) „geschütztes Werk" vor, sodass es schon am Tatobjekt des § 106 Abs. 1 UrhG fehlt. Problematisch kann die Rechtslage daher dann sein, wenn Filme oder Songs von ausländischen Webseiten, wie etwa *Hulu.com*, gestreamt werden. Ausländische Urheber sind gemäß § 121 Abs. 1 UrhG durch das deutsche Urheberrecht – inklusive der Strafvorschriften – nämlich nur dann geschützt, wenn das Werk (auch) in Deutschland 30 Tage nach der Veröffentlichung erschienen ist. Dies dürfte bei vielen Filmen jedoch der Fall sein. Andernfalls sind ausländische Werke nur nach der Maßgabe der entsprechenden Staatsverträge geschützt, § 121 Abs. 4 UrhG.

9 Sind diese Voraussetzungen erfüllt, handelt es sich also insbesondere um Musik- oder Filmwerke, die auch im Inland erschienen sind, so begeht derjenige, der sich physisch in Deutschland aufhält und an seinem eigenen PC tätig wird, um die Werke zu streamen, die Tat im Sinne von § 3 StGB im Inland, da er gemäß § 9 Abs. 1 StGB die Tathandlung im Inland vollzieht. Auf den Standort des Servers kommt es hierbei nicht an.

10 ***2. Streaming als Vervielfältigung iSd. §§ 16, 106 UrhG***

Der Begriff der Vervielfältigung in § 106 UrhG entspricht dem zivilrechtlichen in § 16 UrhG.[16] Unter einer Vervielfältigung ist demgemäß jede körperliche Festlegung des Werkes zu verstehen, die geeignet ist, das Werk den menschlichen Sinnen in irgendeiner Weise unmittelbar oder mittelbar wahrnehmbar zu machen.[17] Daher muss es sich bei der vervielfältigten Datei mit dem Musikstück oder Film also immerhin um ein urheberrechtlich geschütztes Werk handeln. Eine Teilvervielfältigung fällt nur dann unter den Vervielfältigungsbegriff, wenn der kopierte Teil für sich genommen bereits ein Werk darstellt.[18] Dies kann beim Streaming aber gerade dann problematisch sein, wenn nur sehr kurze Sequenzen gespeichert werden, die für sich genommen noch nicht die Werkschwelle erreichen. In diesem Fall scheidet schon die Tathandlung des Vervielfältigens aus. Gerade bei Filmdateien dürfte dieses Erfordernis jedoch regelmäßig erfüllt sein, wobei dies von der Größe und Menge der im Buffer abgelegten Datenpakete abhängig sein kann.

11 Ein weiteres Problem des Streamings liegt aber darin, dass die Daten im so genannten Buffer einerseits nur kurzzeitig gespeichert und danach wieder gelöscht werden[19] und dass andererseits diese Zwischenspeicherung technisch bedingt und nicht vom Nutzer selbst bewusst veranlasst ist. Ob eine solche vorübergehende, technisch bedingte Speicherung überhaupt unter den Begriff der Vervielfältigung im Sinne der §§ 16, 106 UrhG fällt, war bis zur Einführung des § 44a UrhG sehr umstritten.[20] Denn der Schwerpunkt der Handlung liegt hier nicht auf dem technisch bedingten

[14] Dazu *Hildebrandt*, Die Strafvorschriften des Urheberrechts, Berlin 2001, S. 316 ff.; *Reinbacher* (o. Fn. 2), S. 314 ff.; Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Auflage, Berlin 2012, Rn. 688 ff.
[15] *Hildebrandt* (o. Fn. 14), S. 139 f.; *Kaiser*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, U 180, Loseblattsammlung, Stand: 188. Ergänzungslieferung, München 2012, § 106 UrhG Rn. 38.
[16] *Dreier*, in: Dreier/Schulze (Hrsg.), UrhG, Kommentar, 3. Aufl., München 2008, § 106 Rn. 5; *Haß*, in: Schricker/Loewenheim (Hrsg.), Urheberrecht, Kommentar, 4. Aufl., München 2010, § 106 Rn. 5; *Heinrich*, in: Joecks/Miebach/Schmitz (Hrsg.), Münchener Kommentar zum StGB (MüKo), Band 6/1, Nebenstrafrecht II, München 2010, § 106 UrhG Rn. 46; *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (o. Fn. 9), § 106 Rn. 12; *Kaiser*, in: Erbs/Kohlhaas (o. Fn. 15), § 106 Rn. 12; *Reinbacher* (o. Fn. 2), S. 82.
[17] Vgl. statt Vieler *Kaiser*, in: Erbs/Kohlhaas (o. Fn. 15), § 106 Rn. 12; *Reinbacher* (o. Fn. 2), S. 82.
[18] *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (o. Fn. 9), § 106 Rn. 12; *Reinbacher* (o. Fn. 2), S. 91.
[19] *Reinbacher* (o. Fn. 2), S. 126.
[20] Zu diesem nun überholten Streit *Reinbacher* (o. Fn. 2), S. 99 ff.

Speichervorgang, sondern vielmehr auf der rein rezeptiven Nutzung des Werkes. Nicht die Vervielfältigung, sondern das Ansehen des Filmes oder das Anhören der Musik stehen im Vordergrund und bilden die eigentliche Nutzung des Werkes. Dieser rezeptive Werkgenuss ist jedoch nicht von einem der urheberrechtlichen Verwertungsrechte erfasst, sondern grundsätzlich urheberrechtsfrei.[21] Soll es also rechtlich einen Unterschied machen, ob eine CD im CD-Player oder „im Internet angehört", also gestreamt wird, nur weil bei letzterem Vorgang zufälligerweise eine temporäre Kopie erstellt wird? Denn der Vorgang der Speicherung läuft nun einmal automatisch ab.

12 Dadurch, dass § 44a UrhG Fälle solcher vorübergehenden und technisch bedingten Speicherungen erfasst, belegt er im Umkehrschluss implizit, dass es sich auch bei kurzzeitigen Speicherungen grundsätzlich um Vervielfältigungen handelt, wenngleich um solche, die unter den Voraussetzungen des § 44a UrhG urheberrechtlich nicht relevant sind.

S. 182

13 ***3. Gesetzlich zugelassener Fall***

a) Privilegierte Nutzung nach § 44a UrhG

Ob das Streaming indessen die Voraussetzungen der Privilegierung des § 44a UrhG erfüllt, ist streitig.[22] In Betracht kommt insbesondere § 44a Nr. 2 UrhG, wonach vorübergehende Vervielfältigungshandlungen, die flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen und deren alleiniger Zweck es ist, eine rechtmäßige Nutzung des Werks zu ermöglichen und die keine eigenständige wirtschaftliche Bedeutung haben, zulässig sind. Durch diese Regelung wird der soeben angeführten Tatsache Rechnung getragen, dass das Ansehen und Anhören von Werken grundsätzlich urheberrechtsfrei ist und nur durch die technischen Bedingungen der Internet-Übertragung zu einer verwertungsrechtlich relevanten Nutzung werden könnte. Gerade aus diesem Grund sind die Voraussetzungen des § 44a Nr. 2 UrhG beim Streaming aber auch erfüllt:

14 Die Vervielfältigung im Buffer ist vorübergehend, flüchtig und technisch bedingt. Zudem ist es ihr alleiniger Zweck, eine rechtmäßige Nutzung, nämlich den rezeptiven Werkgenuss durch Ansehen oder Anhören des Werkes, zu ermöglichen.[23] Anderer Auffassung war freilich das AG Leipzig im Verfahren Kino.to.[24] Ohne Zustimmung der Rechteinhaber sei eine rechtmäßige Nutzung der Werke nicht möglich. Das Gericht interpretiert das Merkmal der rechtmäßigen Nutzung daher offenbar so, dass eine Nutzung gegen oder ohne den Willen der Rechteinhaber stets ausgeschlossen ist. Dadurch wird aber verkannt, dass eine Einwilligung der Berechtigten hier gar nicht erforderlich ist, da beim rein rezeptiven Anschauen oder Anhören des Werkes, wie dargestellt, gerade keine zustimmungspflichtige und von den Rechten der Urheber erfasste Verwertung stattfindet.

15 Schließlich hat der Vorgang der kurzzeitigen Speicherung hier auch keine eigenständige, über diesen kurzzeitigen Werkgenuss hinausgehende Bedeutung, da die Daten automatisch wieder gelöscht werden.[25] Das AG Leipzig teilte auch diese Einschätzung nicht. Der Vorgang sei wirtschaftlich bedeutsam, da der Nutzer „mittels

[21] BGH, GRUR 1991, 449, 453; *Schulze*, Wann beginnt eine urheberrechtlich relevante Nutzung?, ZUM 2000, 126, 129 f.
[22] Vgl. dazu *Fangerow/Schulz*, Die Nutzung von Werken auf www.kino.to. Eine urheberrechtliche Analyse des Film-Streamings im Internet, GRUR 2010, 677; *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (o. Fn. 9), § 106 Rn. 14; *Koch*, Der Content bleibt im Netz – gesicherte Werkverwertung durch Streaming-Verfahren, GRUR 2010, 574; *Stieper* (o. Fn. 9), MMR 2012, 12.
[23] So auch *Fangerow/Schulz* (o. Fn. 22), GRUR 2010, 677, 681; *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (o. Fn. 9), § 106 Rn. 14; *Stieper* (o. Fn. 9), MMR 2012, 12, 16.
[24] AG Leipzig, Urteil vom 21.12.2011, Az.: 200 Ls 390 Js 184/11, Rz. 46.
[25] So auch *Fangerow/Schulz* (o. Fn. 22), GRUR 2010, 677, 680 f.; *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (o. Fn. 9), § 106 Rn. 14; *Stieper* (o. Fn. 9), MMR 2012, 12, 16.

dieser gespeicherten Daten sich den wirtschaftlichen Wert der Nutzung"[26] verschaffe. Dem ist jedoch entgegen zu halten, dass der Speichervorgang nach dem Wortlaut der Ausnahmevorschrift eine „eigenständige" wirtschaftliche Bedeutung haben muss. Dies kann nur so verstanden werden, dass diese Bedeutung vom automatischen Speichervorgang zu abstrahieren ist und daher eine eigene, über den Zweck, zu welchem die vorübergehende Speicherung erfolgt, hinausgehende Nutzung ermöglichen muss.[27] Diese Auslegung hat der EuGH in einer ähnlichen Konstellation ebenfalls zu Grunde gelegt, indem er feststellte, dass für Art. 5 Abs. 1 der Richtlinie 2001/29/EG, welcher der Schrankenbestimmung zu Grunde liegt, ebenfalls ein über die betreffende Nutzung hinausgehender Vorteil erforderlich ist.[28] Dieser unionsrechtlichen Auslegung ist auch im deutschen Recht Geltung zu verleihen. Der deutsche Gesetzgeber hat die Vorschrift seinerzeit zur Umsetzung der Richtlinie 2001/29/EG eingeführt und explizit die Puffer-Speicherung im Cache als Beispiel für eine privilegierte Nutzung genannt.[29] Dies sollte dann selbstverständlich auch für die ähnlich gelagerten RAM-Speicherungen im Buffer gelten.

16 Daher ist das Streaming eine nach § 44a Nr. 2 UrhG privilegierte Nutzung. Faktisch ist damit eine urheberrechtlich relevante Vervielfältigung ausgeschlossen. Gesetzestechnisch ist § 44a UrhG jedoch als „gesetzlich zugelassener Fall" im Sinne des § 106 Abs. 1 UrhG konzipiert. Ein solcher schließt den objektiven Tatbestand des § 106 UrhG aus, da dieser als negativ formuliertes Tatbestandsmerkmal das Nicht-Vorliegen eines gesetzlich zugelassenen Falles voraussetzt.[30]

S. 183

17 ***b) Privilegierte Nutzung nach § 53 Abs. 1 UrhG***

Zudem greift in Fällen der Nutzung durch Privatpersonen bei ansonsten rechtmäßig angebotenen Werken die Schranke des § 53 Abs. 1 S. 1 UrhG. Auch sie stellt einen gesetzlich zugelassenen Fall dar und schließt den Tatbestand des § 106 UrhG aus.[31] Da nach der hier vertretenen Auffassung schon die Privilegierung des § 44a Nr. 2 UrhG greift, dürfen die Ausführungen hierzu kurz bleiben.

18 aa) § 53 Abs. 1 S. 1 UrhG erlaubt einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch auf beliebigen Trägern, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen, soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird. Der private Gebrauch bestimmt sich in Abgrenzung einerseits zur Öffentlichkeit und andererseits zu den Erwerbszwecken.[32] Wer also einzelne[33]

[26] AG Leipzig, Urteil vom 21.12.2011, Az.: 200 Ls 390 Js 184/11, Rz. 46.
[27] *Stieper* (o. Fn. 9), MMR 2012, 12, 16; in diesem Sinne wohl auch *Wiebe*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., München 2011, § 44a Rn. 4.
[28] EuGH, MMR 2011, 817, 824 – *Football Association Premier League Ltd.* (Rs. C-403/08) und *Murphy* (Rs. 429/08), Rz. 175 m. Anm. *Stieper* (o. Fn. 9).
[29] BT-Drs. 15/38, S. 18.
[30] *Dreier*, in: Dreier/Schulze (o. Fn. 16), § 106 Rn. 6; *Gercke*, Tauschbörsen und Urheberstrafrecht, ZUM 2007, 791, 792; *Haß*, in: Schicker/Loewenheim (o. Fn. 16), § 106 Rn. 23; *Heinrich* in: Wandtke (Hrsg.), Medienrecht, Band 5, 2. Aufl., Berlin 2011, Kap. 5 Rn. 318; *ders.*, in: MüKo (o. Fn. 16), § 106 Rn. 78; *Hildebrandt* (o. Fn. 9), S. 124; *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger (o. Fn. 9), § 106 Rn. 21; *Kaiser*, in: Erbs/Kohlhaas (o. Fn. 15), § 106 Rn. 21; *Reinbacher* (o. Fn. 2), S. 175; *ders*., Strafbarkeit der Privatkopie von offensichtlich rechtswidrig hergestellten oder öffentlich zugänglich gemachten Vorlagen, GRUR 2008, 394.
[31] Ausführlich dazu *Reinbacher* (o. Fn. 2), passim; *ders.* (o. Fn. 30), GRUR 2008, 394.
[32] Ausführlich zum Merkmal des privaten Gebrauchs *Reinbacher* (o. Fn. 2), S. 179 ff.
[33] Gemeint sind damit „einige wenige"; vgl. *Lüft*, in: Wandtke/Bullinger (Hrsg.), UrhR, Kommentar, 3. Aufl., München 2009, § 53 Rn. 12; *Schack*, Urheber- und Urhebervertragsrecht, 5. Aufl., Tübingen 2010, Rn. 496. BGH, GRUR 1978, 474, 476, hat dieses Merkmal bei einer Anzahl von sieben Exemplaren als noch erfüllt angesehen. Diese Zahl ist in der Literatur in der Folge häufig als Höchstgrenze interpretiert worden. Sie war jedoch dem Klageantrag geschuldet und ist daher keineswegs als absolute Zahl zu verstehen. Vielmehr muss der private Gebrauch sich nach den persönlichen Verhältnissen bestimmen; vgl. *Reinbacher* (o. Fn. 2), S. 193. Ohnehin erscheint die Zahl angesichts der verschiedenen Medien wie PCs, MP3-Playern, Telefonen etc. häufig nicht angemessen. Beim erstmaligen Streaming eines Filmes besteht diesbezüglich ohnehin kein Problem.

Vervielfältigungen herstellt, um sie für sich oder seinen engen Freundes- oder Familienkreis zu nutzen, und dabei keinerlei Erwerbszwecke verfolgt, erfüllt die Voraussetzungen des Tatbestandsausschlusses.

19 bb) § 53 Abs. 1 S. 1 UrhG enthält jedoch einen Rückausschluss bei offensichtlich rechtswidrig hergestellten oder öffentlich zugänglich gemachten Vorlagen. Originalfilme und Musikstücke sind rechtmäßig hergestellt. Werden sie jedoch auf einen Server geladen, damit sie dort angeboten werden können, so kann diese Herstellung rechtswidrig sein, wenn sie durch nicht-autorisierte Personen vorgenommen wird. Davon zu unterscheiden ist die andere Alternative, das öffentliche Zugänglichmachen. Dieses beurteilt sich, unabhängig von der Herstellung der angebotenen Datei, danach, ob der Betreffende berechtigt war, das Werk in der Öffentlichkeit anzubieten. Es ist jedoch in beiden Fällen zu prüfen, ob diese Rechtswidrigkeit offensichtlich ist. Dies ist der Fall, wenn eine rechtmäßige Herstellung oder Zugänglichmachung für den entsprechenden Verkehrskreis vernünftigerweise ausgeschlossen werden kann.[34] Ob diese Voraussetzungen bei Portalen wie Kino.to erfüllt sind, kann hier dahinstehen.[35] Denn in den hier interessierenden Fällen des Anbietens von Werken auf mit Geo-IP-Sperren versehenen Plattformen lässt sich der Rückausschluss in verschiedener Hinsicht ablehnen. Zum einen handelt es sich bei Portalen wie *Hulu.com* – zumindest im Hinblick auf das nicht durch Geo-IP-Sperre ausgeschlossene Land – um rechtmäßige Anbieter, denn entsprechende Rechte wurden ja erworben. Zum anderen lässt sich daran zweifeln, ob die jeweiligen Anbieter das Werk überhaupt in Deutschland rechtswidrig öffentlich zugänglich machen,[36] da sie durch den Filter deutsche Nutzer ja gerade ausschließen wollen. Aber selbst bei Plattformen, die über gar keine entsprechenden Rechte verfügen, ist das Merkmal nur dann erfüllt, wenn diese Tatsache auch offensichtlich ist.

20 ***4. Vorsatz***

Schließlich ist – nochmals hilfsweise – darauf hinzuweisen, dass die Nutzer Vorsatz hinsichtlich der Erfüllung des objektiven Tatbestandes des § 106 Abs. 1 UrhG aufweisen müssen. Dies folgt aus § 15 StGB, der über § 1 EGStGB auch im Nebenstrafrecht Anwendung findet. Konkret bedeutet dies, dass die Nutzer nicht nur wissen und wollen müssten, dass sie beim Streaming überhaupt eine Vervielfältigung erstellen, sondern auch, dass diese nicht von einer Schranke gedeckt ist, also etwa die Ausschlusskriterien der §§ 44a, 53 UrhG greifen. Auch dies erscheint in den hier interessierenden Konstellationen höchst zweifelhaft.

21 ***5. Eingriff in Verwandte Schutzrechte***

Die soeben gefundenen Ergebnisse gelten in gleicher Weise für eine Strafbarkeit nach § 108 UrhG, der verwandte Schutzrechte, etwa der Tonträgerhersteller, unter strafrechtlichen Schutz stellt. Denn auch hiernach ist die Verwertung nur strafbar,

[34] *Reinbacher* (o. Fn. 2), S. 224; *ders.* (o. Fn. 30), GRUR 2008, 394, 399; ähnl. *Dreier*, in: Dreier/Schulze (o. Fn. 16), § 53 Rn. 12: Wenn keine ernsthaften Zweifel an der Rechtswidrigkeit bestehen; *Freiwald*, Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, Baden-Baden 2003, S. 150: keine vernünftigen Zweifel an der Rechtswidrigkeit; *Loewenheim*, in: Schricker/Loewenheim (o. Fn. 16), § 53 Rn. 23: wenn die Rechtswidrigkeit ohne Schwierigkeiten erkennbar ist; *Lüft*, in: Wandtke/Bullinger (o. Fn. 32), § 53 Rn. 15: nur in eindeutigen Fällen; *Pichlmaier*, Abschied von der Privatkopie? Von der Zukunft einer Institution, CR 2003, 910, 912: wenn die Rechtswidrigkeit zweifelsfrei feststellbar ist.

[35] Der Vorgang des Herstellens der Dateien entzieht sich jedoch auch hier der Kenntnis der Nutzer, sodass kaum von einer offensichtlich rechtswidrigen Herstellung gesprochen werden kann. Anders mag es aber mit dem Merkmal der offensichtlich rechtswidrig öffentlich zugänglich gemachten Vorlage stehen, sofern und soweit für die Nutzer klar zu Tage tritt, dass Filme o.ä. auf der Plattform von anderen als den berechtigten Personen angeboten werden. Vgl. zu diesem Merkmal *Reinbacher* (o. Fn. 30), GRUR 2008, 394, 400.

[36] So auch *Mitsdörffer/Gutfleisch* (o. Fn. 1), MMR 2009, 731, 734, die jedoch lediglich die zivilrechtliche Lage prüfen und daher eine Analogie befürworten, wenn der Nutzer die Geo-IP-Sperre selbstständig umgeht und (sich) das Werk erst dadurch zugänglich macht. Dieser Ansicht ist hier jedoch aus zwei Gründen nicht zu folgen. Einerseits macht der Nutzer das Werk dann ja nicht „öffentlich" zugänglich, sondern nur sich selbst, sodass die Voraussetzungen einer Analogie gar nicht gegeben sind. Andererseits scheidet im Strafrecht eine den Täter belastende Analogie im Hinblick auf Art. 103 Abs. 2 GG und § 1 StGB ohnehin aus.

wenn kein gesetzlich zugelassener Fall vorliegt.

S. 184

22 **C. Das Umgehen der Geo-IP-Sperre**

I. Technische Hinweise zu Umgehungsmöglichkeiten

Das Umgehen der Geo-IP-Sperre ist nicht sonderlich schwierig. Denn dazu muss lediglich die eigene Herkunft verschleiert werden. Es stehen inzwischen verschiedene Methoden zur Verfügung. Die einfachste Möglichkeit besteht darin, die betreffenden Seiten über einen so genannten Proxy-Server anzuwählen.[37] Der Proxy-Server ist ein Computer auf einem fremden Server, der durch die Anwahl zwischengeschaltet wird, sodass jede Website im Internet über diesen Server aufgerufen wird und nicht vom Nutzer direkt. Insoweit fungiert der Proxy-Server lediglich als Mittler. Wird dieser Umweg beschritten, so erkennt die Geolocation-Software einzig die IP-Adresse des Proxy-Servers und damit dessen Standort, nicht aber IP-Adresse und Herkunft des konkreten Nutzers. Denn der IP-Adressen-Filter kann nicht feststellen, ob es sich um eine direkte Verbindung handelt oder ob ein anderer Computer dazwischen geschaltet ist. Werden nun etwa Proxy-Server in den USA verwendet, so lässt sich dadurch ohne weiteres suggerieren, dass ein US-amerikanischer Nutzer die Streaming-Anfrage sendet. Freie Proxy-Server sind im Internet in größerer Zahl verfügbar. Dort finden sich Listen freier Proxys, häufig nach Ländern geordnet, aus denen man einen auswählen und dessen IP-Adresse im eigenen Browser eingeben kann, sodass standardmäßig alle Internetseiten über diesen Proxy angewählt werden. Es existieren auch so genannte Anonymisierungsprogramme, wie etwa für den Browser Firefox das Add-on *anonymox*[38], welche diesen Vorgang ermöglichen bzw. eine Liste von Proxys zur Verfügung stellen.

23 Ähnlich funktioniert auch das Programm *Hotspot Shield*[39], welches grundsätzlich jede Anfrage an das Internet zunächst über einen US-Server umleitet. Bei diesen Programmen ist das Umgehen der Geo-IP-Sperre sicher nicht der Hauptzweck, sondern ein (vielleicht auch gewünschter) Nebeneffekt.

24 Eine weitere Möglichkeit ist die Teilnahme an dem Anonymisierungsnetzwerk „Tor" („*The Onion Routing*")[40]. Dieses bedient sich eines Tunnel- oder Zwiebelsystems, indem es Anfragen zunächst über drei Tor-Server laufen lässt. Da jeder Server immer nur den jeweiligen Partner kennt, der ihm die Anfrage stellt, sowie denjenigen Server, an den die Anfrage weitergeleitet wird, soll sich die Spur des Anfragenden verlieren. Er kann damit auf eine Seite im Internet zugreifen, ohne dass dabei nachvollzogen werden kann, woher die Anfrage tatsächlich stammte, da sie zunächst per Zufallsprinzip umgeleitet wurde. Das Tor-Projekt wird von vielen mit den unterschiedlichsten Intentionen genutzt, da es eine anonyme Kommunikation ermöglichen soll, ohne dass diese ohne weiteres „abgehört" werden kann. Im Fall der Geo-IP-Sperren verhindert Tor jedoch auch, dass der ursprüngliche Nutzer lokalisiert werden kann. Es funktioniert also ähnlich wie die zuvor beschriebenen Ansätze und macht sich wiederum den Umweg über einen anderen Rechner, in diesem Fall sogar mehrere Server, zu Nutze.

25 Schließlich lässt sich auch Speicherplatz auf externen Rechnern erwerben und ein eigenes virtuelles privates Netzwerk (VPN) erstellen, das verschlüsselt werden kann und mittels dessen alle Verbindungen über den externen Server laufen.

26 All diesen Lösungen ist gemeinsam, dass Rechner oder Rechnernetze im Datenverkehr zwischengeschaltet werden, sodass nicht die IP-Adresse des ursprünglichen Anschlusses, sondern die des Mittlers gesendet wird. Befindet sich dieser im

[37] Hierzu *Hoeren* (o. Fn. 3), MMR 2007, 3, 6.
[38] www.anonymox.net; zuletzt abgerufen am 3.8.2012.
[39] www.hotspotshield.com; zuletzt abgerufen am 3.8.2012.
[40] www.torproject.org; zuletzt abgerufen am 3.8.2012.

zugelassenen Land, so ist die Geo-IP-Sperre wirkungslos.

S. 185

27 **II. Rechtliche Bewertung**

Das Nutzen von Proxy-Servern und insbesondere von Anonymisierungsdiensten selbst ist legal. Hierzu kann bereits auf den allgemeinen Freiheitsgedanken verwiesen werden, nach dem alles, was nicht explizit durch ein Gesetz verboten ist, rechtlich erlaubt ist. Denn ein die Offenlegung der eigenen Identität im Netz gebietendes bzw. die Anonymisierung verbietendes Gesetz gibt es nicht. Darüber hinaus wird ein solches Vorgehen zum Schutz der eigenen Privatsphäre und Daten von Datenschützern sogar empfohlen. In diesem Zusammenhang interessant ist die Frage, ob nicht ohnehin ein Recht auf anonyme Internetnutzung besteht. Ein entsprechendes (selbstständiges) Grundrecht auf Anonymität – auch in Datennetzen – wird von manchen aus Art. 1 Abs. 2 GG in Verbindung mit Art. 2 Abs. 1 GG bzw. aus den Art. 5, 10 und 13 GG hergeleitet.[41] Letztlich kann es aber insbesondere als Ausfluss des Rechts auf informationelle Selbstbestimmung bzw. des Allgemeinen Persönlichkeitsrechts verstanden werden.[42] Eine Einschränkung wäre daher auch gar nicht ohne weiteres möglich, sondern nur zum Schutz anderer Grundrechte im Rahmen des Erforderlichen und Angemessenen. Dabei kann zwischen verschiedenen Stufen der Anonymität unterschieden werden, etwa dem Verwenden von Pseudonymen auf der einen und dem Verbergen der IP-Adresse auf der anderen Seite. Der 69. Deutsche Juristentag sprach sich in seinem Beschluss 6 b) der Abteilung IT- und Kommunikationsrecht zwar jüngst gegen ein „Recht auf anonyme Internetnutzung" aus. Bei aktiver Nutzung des Internets mit eigenen Beiträgen dürfe der Nutzer nicht anonym bleiben, sondern müsse im Rahmen einer Verwendung von Pseudonymen zumindest identifizierbar sein. Hier stand insbesondere die Frage im Raum, welche Ermittlungsmöglichkeiten den Strafverfolgungsbehörden bei Straftaten zur Verfügung stehen sollen.

28 Es sollte jedoch außer Frage stehen, dass der Kommunikationsvorgang sowie die informationelle Selbstbestimmung grundrechtlich auch im Internet geschützt sind. Es ist nicht ersichtlich, warum der offline anerkannte Schutz von Daten und Kommunikation hier nicht gelten sollte. Das Internet ist eben nicht nur kein rechtsfreier Raum, es ist auch kein grundrechtsfreier Raum. Daher geht es auch bei der Frage der Ermittlungsbefugnisse um Schranken der einschlägigen Grundrechte. Schranken müssen jedoch gesetzlich festgelegt und verhältnismäßig sein. Das BVerfG entschied etwa kürzlich, dass die Zuordnung von dynamischen IP-Adressen über § 113 Abs. 1 S. 2 TKG das Telekommunikationsgeheimnis nach Art. 10 GG betrifft und hielt die Vorschrift für unverhältnismäßig und daher für unvereinbar mit dem Grundgesetz.[43]

29 Für die Zwecke dieses Beitrages bleibt jedenfalls festzuhalten, dass ein gesetzliches Verbot der Verwendung von Anonymisierungssoftware derzeit nicht besteht. Das Unabhängige Landeszentrum für Datenschutz des Landes Schleswig-Holstein hat in Kooperation mit verschiedenen Universitäten und gefördert durch das Bundesministerium für Wirtschaft und Technologie sogar selbst den Anonymisierungsdienst JAP im Rahmen des Projektes „AN.ON – Anonymität im Internet" entwickelt. Beruhend auf einem Mix-Netz von vielen angeschlossenen

[41] *Heckmann*, Persönlichkeitsschutz im Internet. Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz, NJW 2012, 2631, 2632; vgl. insbesondere auch *Bäumler*, Das Recht auf Anonymität, in: Bäumler/v. Mutius (Hrsg.), Anonymität im Internet, Braunschweig/Wiesbaden 2003, S. 5; *v. Mutius*, Anonymität als Element des allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: Bäumler/v. Mutius (ebd.), S. 12 ff.

[42] *Bäumler*, in: Bäumler/v. Mutius (o. Fn. 41), S. 5; *Heckmann* (o. Fn. 41), NJW 2012, 2631, 2632: informationelle Selbstbestimmung; *v. Mutius*, in: Bäumler/v. Mutius (o Fn. 41), S. 12 ff.: Allgemeines Persönlichkeitsrecht; vgl. auch *Denninger*, Anonymität – Erscheinungsformen und verfassungsrechtliche Fundierung, in: Bäumler/v. Mutius (o Fn. 41), S. 41 ff.

[43] BVerfG NJW 2012, 1419, 1421, 1429 f.

Computern an verschiedenen Standorten soll eine weitgehende Anonymität beim Surfen im Internet gewährleistet werden.[44] Damit soll auch der in § 13 Abs. 6 TMG grundsätzlich normierten Verpflichtung von Diensteanbietern zur Ermöglichung der anonymen Nutzung der Telemedien im Rahmen des technisch Möglichen und Zumutbaren Rechnung getragen werden. Auch § 13 Abs. 6 TMG wird als Ausfluss des Grundrechts auf informationelle Selbstbestimmung angesehen.[45] Der Gesetzgeber hat hierzu seinerzeit ausgeführt, dass das Recht auf informationelle Selbstbestimmung in globalen Netzwerken wirksam nur durch größtmögliche Anonymität der Nutzer gewährleistet werden könne.[46] Dennoch lässt sich trotz der grundsätzlichen Zulässigkeit der Anonymisierung wegen des Umgehens der Geo-IP-Sperre in verschiedener Hinsicht an eine Strafbarkeit denken. Hinsichtlich der Fragen des Strafanwendungsrechts sei auf obige Ausführungen unter B. II. 1. verwiesen, wobei bei den Tatbeständen des StGB die Restriktionen des UrhG nicht greifen. Nach allgemeinen Grundsätzen ist ein Täter damit jedenfalls dann nach deutschem Recht strafbar, wenn er die Tathandlung im Inland vollzieht, also die Tathandlung etwa zu Hause an seinem Computer in Deutschland vornimmt, §§ 3, 9 StGB.

S. 186

30 ***1. Strafbarkeit nach § 108b Abs. 1 UrhG***

Zunächst kommt § 108b Abs. 1 UrhG in Betracht. Die Vorschrift stellt einen Verstoß gegen § 95a Abs. 1 UrhG unter Strafe, sanktioniert also das Umgehen einer vom Rechteinhaber zulässigerweise angebrachten wirksamen technischen Schutzmaßnahme.[47] Hiernach wird bestraft, wer in der Absicht, sich oder einem Dritten den Zugang zu einem nach dem UrhG geschützten Werk oder dessen Nutzung zu ermöglichen, eine wirksame technische Maßnahme ohne Zustimmung des Rechtsinhabers umgeht.

31 ***a) Objektive Tatbestandsvoraussetzungen***

Da § 108b Abs. 1 UrhG aber nur Maßnahmen im Sinne des § 95a UrhG strafrechtlich absichert, ist dessen Ratio zu berücksichtigen. § 95a Abs. 1 UrhG spricht zwar, ebenso wie der insoweit formulierungsgleiche § 108b Abs. 1 UrhG, vom Zugang zu Werken, jedoch geht es, anders als etwa im Rahmen des Gesetzes über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG), nicht alleine um den Zugang. Vielmehr muss die technische Maßnahme dem Zweck dienen, eine urheberrechtlich relevante Nutzung des Werkes zu verhindern.[48] Zugangskontrollmechanismen fallen daher nur dann unter die Vorschriften, wenn sie Handlungen verhindern sollen, welche die Ausschließlichkeitsrechte der Urheber berühren.[49] So sind etwa die Regionalcodes auf DVDs gerade nicht von den §§ 95a, 108b UrhG erfasst.[50] Sie sollen nämlich nicht etwa die Vervielfältigung als den Urhebern gemäß § 16 UrhG vorbehaltene Verwertungshandlung verhindern, sondern das Ansehen des Filmes außerhalb der jeweiligen Region. Bei Geo-IP-Sperren gilt jedoch nichts anderes.[51] Denn auch diese sind nicht darauf gerichtet, Kopien zu verhindern, sondern sollen das Anhören und Ansehen von Musik und Filmen im Wege des Streamings der Werke auf eine bestimmte Personengruppe beschränken. Schon aus diesem Grund sind sie nicht als technische Schutzmaßnahmen im Sinne des

[44] Zum technischen Konzept von AN.ON siehe die Broschüre Sicherheit im Internet durch Anonymität; abrufbar im Internet unter https://www.datenschutzzentrum.de/projekte/anon/; zuletzt abgerufen am 3.9.2012; vgl. dazu auch *Federrath*, Das AN.ON-System – Starke Anonymität und Unbeobachtbarkeit im Internet, in: Bäumler/v. Mutius (o. Fn. 41), S. 172 ff.; *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., München 2011, § 13 TMG Rn. 12.
[45] *Spindler/Nink*, in: Spindler/Schuster (o. Fn. 44), § 13 TMG Rn. 10.
[46] BT-Drs. 13/7385, S. 71.
[47] *Heinrich*, in: MüKo (o. Fn. 16), § 108b Rn. 1.
[48] *Wandtke/Ohst*, in: Wandtke/Bullinger (o. Fn. 33), § 95a Rn. 7.
[49] *Wandtke/Ohst*, in: Wandtke/Bullinger (o. Fn. 33), § 95a Rn. 15.
[50] *Wandtke/Ohst*, in: Wandtke/Bullinger (o. Fn. 33), § 95a Rn. 35.
[51] Auf den Einzelfall abstellend *Mitsdörffer/Gutfleisch* (o. Fn. 1), MMR 2009, 731, 735.

§ 108b Abs. 1 UrhG einzustufen.

32 Ferner ist sehr zweifelhaft, ob diese Sperre überhaupt „wirksam" ist, wie es § 95a Abs. 1 UrhG fordert. Denn, wie unter C. I. gezeigt, ist das Überwinden dieser Technologie höchst einfach. Eine Eingabe der Begriffe „Geo IP Sperre umgehen" ergab alleine bei der Suchmaschine *Google* 11.100 Treffer. Zudem erfordert es keine technischen Kenntnisse, sondern etwa einzig die Installation einer Anonymisierungssoftware. Bei Einsatz eines solchen Programms erfolgt die Umgehung der Geo-IP-Sperre sogar automatisch ohne weiteres Zutun des Betreffenden. Wer sich also aus Gründen des Schutzes seiner Privatsphäre einer Anonymisierungssoftware bedient, überwindet diese Blockade unter Umständen sogar, ohne dies zu merken – was zwar erst für die Ebene des subjektiven Tatbestandes relevant, jedoch auch aussagekräftig ist im Hinblick auf die „Wirksamkeit" der Sperre. Nach noch weiter gehender Auffassung wird schließlich durch den Einsatz von Proxys noch nicht einmal das Schutzziel der Maßnahme umgangen, da dieses nur darauf gerichtet sei, die IP-Adresse des Anfragenden zu ermitteln, was weiterhin möglich sei, da die IP-Adresse des Proxys erkannt werde.[52] Selbst wenn man dem im Hinblick auf die Interessen der Rechteinhaber nicht folgt, scheidet aus den zuvor angeführten Gründen aber jedenfalls die Annahme einer wirksamen technischen Schutzmaßnahme im Sinne des § 108b Abs. 1 UrhG aus – und damit auch der objektive Tatbestand.

S. 187

33 ***b) Ausschluss der Strafbarkeit für den privaten Gebrauch***

Im Übrigen ist hinsichtlich des privaten Gebrauchs jegliche Strafbarkeit ausgeschlossen, denn in § 108b Abs. 1 UrhG heißt es: „[…] wenn die Tat nicht ausschließlich zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht." Im Gegensatz zu § 53 Abs. 1 UrhG findet sich hier auch keinerlei weitere Einschränkung. Wer also zum privaten Gebrauch handelt, ist stets straflos.

34 **2. Strafbarkeit nach § 202a StGB**

Des Weiteren ist an § 202a StGB zu denken, der nach der Reform des Jahres 2007[53] das Sich-Verschaffen des bloßen Zugangs zu Daten und damit grundsätzlich auch das so genannte Hacking erfasst.

35 ***a) Objektive Tatbestandsvoraussetzungen***

Hiernach wird bestraft, „wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft". Bei den gespeicherten Musik- oder Filmdateien handelt es sich um Daten im Sinne des § 202a Abs. 2 StGB, nämlich um solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind, denn es sind technische Geräte zu ihrer Wahrnehmung erforderlich. Problematischer sind aber die beiden weiteren Einschränkungen: Die Daten dürfen einerseits nicht für den Täter bestimmt sein und müssen andererseits gegen den unberechtigten Zugang besonders gesichert sein. Beide Kriterien sind hier höchst zweifelhaft.

36 Zum einen fragt sich, ob durch Geo-IP-Sperren „gesicherte" Dateien tatsächlich nicht für den Täter bestimmt sind. Für den Täter nicht bestimmt sind die Daten nur dann, wenn sie ihm nach dem Willen des Berechtigten im Zeitpunkt der Tathandlung nicht zur Verfügung stehen sollen.[54] Der Täter selbst soll aber mittels der Geo-IP-Sperre

[52] *Mitsdörffer/Gutfleisch* (o. Fn. 1), MMR 2009, 731, 735.
[53] 41. StÄG v. 7. 8. 2007, BGBl. I S. 1786.
[54] *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Leipziger Kommentar (LK) zum StGB, Band 6, 12. Aufl., Berlin 2010, § 202a Rn. 21; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar (NK) zum StGB, 3. Aufl., München 2010, § 202a Rn. 7; *Lenckner/Eisele*, in: Schönke/Schröder (Hrsg.), StGB, Kommentar, 28. Aufl., München 2010, § 202a Rn. 6.

persönlich gar nicht von der Nutzung ausgeschlossen werden. Denn würde er die Seite aus einem anderen Land anwählen, das im zugelassenen Bereich liegt, so dürfte er sie ohne weiteres nutzen. Mit anderen Worten soll nicht der Zugriff dieses Täters generell verhindert werden, sondern nur dann, wenn er sich (nicht) in einem bestimmten Land aufhält. Dies kann man allerdings unter der Prämisse anders sehen, dass es auf den konkreten Tatzeitpunkt und die konkrete Sachlage ankommt, sodass es unerheblich ist, ob demselben Täter der Zugang unter anderen Umständen durchaus gewährt worden wäre.[55] Es ist dabei zudem der Wille desjenigen ausschlaggebend, der die Daten abspeichert.[56] Dieser kann die Bestimmung auch unter eine Bedingung stellen und z.B. den Zugang zu Datenbanken von der Zahlung eines Entgelts abhängig machen. Hier dürften die Berechtigten wegen der territorialen Lizenzierung ihr Einverständnis an die Bedingung knüpfen, dass sich der betreffende Nutzer im Lizenzbereich aufhält. Der IP-Adressen-Filter fungiert dann als Schutz dieser Begrenzung des Zugriffs auf die Daten.

S. 188

37 Zum anderen verlangt das Gesetz aber eine „besondere Zugangssicherung". Zwar handelt es sich bei den Geo-IP-Sperren, wie gesehen, nicht um einen bloßen Kopierschutz, welcher im Rahmen des § 202a StGB alleine nicht ausreichen würde,[57] sondern es geht auch und gerade um den Zugang zu den Daten. Eine „besondere Zugangssicherung" ist jedoch nur anzunehmen bei Vorrichtungen, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren.[58] Jedenfalls daran lässt sich in verschiedenerlei Hinsicht zweifeln. Eine besondere Zugangssicherung lässt sich nämlich nicht annehmen, wenn die Aufhebung des Schutzes ohne weiteres möglich ist.[59] Denn gerade aus der Überwindung dieser besonderen Sicherung schöpft sich die erhöhte kriminelle Energie des Täters, die eine Strafbarkeit begründen soll.[60] Auch der Gesetzgeber maß diesem Merkmal eine „besondere Bedeutung für die Eingrenzung des Tatbestandes" zu.[61] Daher sind besondere Anforderungen zu stellen, sodass ein nicht unerheblicher zeitlicher und technischer Aufwand zur Umgehung der Sicherung erforderlich ist.[62] Die Zwischenschaltung eines Proxys ist hingegen äußerst einfach. Ein kurzer Blick auf freie Proxy-Listen in einer Suchmaschine genügt. Der Einsatz eines Proxy-Servers erfordert gerade keinen erheblichen zeitlichen oder technischen Aufwand. Genau betrachtet, ist die Geo-IP-Sperre also gar keine Sicherung, da sie bereits dann nicht greift, wenn man sich – u.U. standardmäßig – einer Anonymisierungstechnik bedient. Zudem verträgt sich das Vorgehen zur Anonymisierung des eigenen Surf-Vorganges nicht mit dem Bild des Hackers, der erst einmal tüfteln muss, um sich Zugang zu geheimen Daten zu verschaffen. Von einem „Überwinden" der Zugangssperre in einer Weise, die kriminelle Energie offenbart, kann daher nicht die Rede sein – schon gar nicht, wenn man bedenkt, dass – auch im Hinblick auf das Recht auf informationelle Selbstbestimmung sowie § 13 Abs. 6 TMG als dessen Konkretisierung – eine Anonymisierung im Internet grundsätzlich erlaubt ist. Will man solchen – auch verfassungsmäßigen – Vorgaben Rechnung tragen, sollte man dies nicht durch eine Strafbarkeit nach § 202a StGB „ausbremsen", sondern das Gesetz diesen entsprechend auslegen.

---

[55] In diese Richtung *Hilgendorf*, in: LK (o. Fn. 54), § 202a Rn. 21.
[56] *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl., München 2012, § 202a Rn. 7a; *Hilgendorf*, in: LK (o. Fn. 54), § 202a Rn. 26; *Kargl*, in: NK (o. Fn. 54), § 202a Rn. 7; *Lenckner/Eisele*, in: Schönke/Schröder (o. Fn. 54), § 202a Rn. 6.
[57] *Fischer* (o. Fn. 56), § 202a Rn. 8a; *Lenckner/Eisele*, in: Schönke/Schröder (o. Fn. 54), § 202a Rn. 7; vgl. aber auch *Hilgendorf*, in: LK (o. Fn. 54), § 202a Rn. 30, der davon ausgeht, dass Kopiersperren i.d.R. auch der Zugangssicherung dienen.
[58] BT-Drs. 16/3656, S. 10; *Lenckner/Eisele*, in: Schönke/Schröder (o. Fn. 54), § 202a Rn. 7; dazu ausführlich *Hilgendorf*, in: LK (o. Fn. 54), § 202a Rn. 29 ff.; Hilgendorf/Valerius (Fn. 14), Rn. 550.
[59] BT-Drs. 16/3656, S. 10; *Lenckner/Eisele*, in: Schönke/Schröder (o. Fn. 54), § 202a Rn. 7.
[60] BT-Drs. 16/3656, S. 10; *Fischer* (o. Fn. 56), § 202a Rn. 8; *Hilgendorf*, in: LK (o. Fn. 54), § 202a Rn. 3.
[61] BT-Drs. 16/3656, S. 10.
[62] BT-Drs. 16/3656, S. 10; *Hilgendorf*, in: LK (o. Fn. 54), § 202a Rn. 32; *Lenckner/Eisele*, in: Schönke/Schröder (o. Fn. 54), § 202a Rn. 7.

38 ***b) Subjektiver Tatbestand***

Schon objektiv ist das Verhalten also nicht tatbestandsmäßig, da jedenfalls keine besondere Zugangssicherung überwunden wird. Es soll aber dennoch kurz darauf hingewiesen werden, dass Täter darüber hinaus wiederum auch vorsätzlich handeln müssen, § 15 StGB. Wer jedoch standardmäßig ein Anonymisierungsprogramm verwendet, bemerkt im Zweifelsfall nicht einmal, wenn er eine Geo-IP-Sperre umgeht. Will man daher nicht – generell oder zumindest im Einzelfall – ein Für-Möglich-Halten unterstellen, was zu weitgehend erscheint, so fehlt es bereits am Wissenselement des Vorsatzes, sodass selbst ein dolus eventualis ausscheidet.

S. 189

39 ***3. Strafbarkeit gemäß § 263a StGB***

Zuletzt ließe sich auch eine Strafbarkeit nach § 263a StGB wegen einer „Täuschung" des Anbieters der Streaming-Dateien durch das Verwenden eines Proxys oder VPN oder ähnliche Vorgehensweisen erwägen. Hierzu müsste der Täter in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigen, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst. In Betracht kommt hier zunächst das Verwenden unrichtiger oder unvollständiger Daten (2. Variante). In diesem Fall wäre die IP-Adresse des Proxys oder des Netzwerkes etc. das entsprechende Datum. Es ist dann unrichtig, wenn der dadurch bezeichnete Sachverhalt in Wahrheit nicht oder anders gegeben ist, die Information also mit der Wirklichkeit nicht übereinstimmt.[63] Schon hier lässt sich einwenden, dass die mit der IP-Adresse des Proxys mitgeteilte Information letztlich zutreffend ist. Denn die IP-Adresse wird nicht verfälscht, es wird dem Server des Anbieters die korrekte IP-Adresse des Proxys zugeleitet. Ist es aber grundsätzlich zulässig, einen Proxy dazwischenzuschalten, was, wie gesehen, aus unterschiedlichen Gründen erfolgen kann, so werden keine falschen Daten übermittelt. Es stünde den Anbietern durchaus frei, ihre Software so zu programmieren, dass nicht nur die IP-Adressen bestimmter Länderkontingente ausgeschlossen werden, sondern auch die frei erhältlichen Proxys, zumal die entsprechenden Listen auch den Rechteinhabern verfügbar sind. Unterlassen sie dies, so tragen sie das Risiko, dass der Proxy, der die Anfrage sendet, nur als Mittler fungiert.

40 Man könnte ferner an das unbefugte Verwenden von Daten (3. Variante) denken. Legt man dieses Merkmal mit der h.M. „betrugsspezifisch" aus, so liegt ein unbefugtes Verwenden dann vor, wenn es gegenüber einer natürlichen Person eine Täuschung darstellen würde.[64] Wiederum wird hier zwar keine falsche Information übermittelt, jedoch ließe sich behaupten, dass die Situation damit vergleichbar sei, dass eine andere (natürliche) Person vorgeschickt wird, welche durch den Berechtigten einen Vorteil gewährt bekommt, der dann einem Dritten zufließt, der eigentlich nicht in den Genuss dieses Vorteils hätte kommen sollen. Es fragt sich jedoch, ob bei der Verwendung des Proxys und der Übermittlung seiner IP-Adresse konkludent täuschungsgleich erklärt wird, dass sich nicht ein Dritter derselben bedient. Insgesamt erscheint es auch problematisch, die durchaus zulässige Verwendung von Anonymisierungssoftware als „unbefugt" einzustufen. Das Risiko, ob die Daten nur dem Proxy oder über diesen auch Dritten zugänglich gemacht werden, liegt beim Systembetreiber.

[63] *Fischer* (o. Fn. 56), § 263a Rn. 7; *Tiedemann/Valerius*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Leipziger Kommentar (LK) zum StGB, Band 9/1, 12. Aufl., Berlin 2012, § 263a Rn. 33.

[64] BGHSt 38, 120, 121 f.; *Cramer/Perron*, in: Schönke/Schröder (o. Fn. 54), § 263a Rn. 9; *Fischer* (o. Fn. 56), § 263a Rn. 11; *Heinrich*, in: Arzt/Weber/Heinrich/Hilgendorf, Strafrecht Besonderer Teil, 2. Aufl., Bielefeld 2009, § 21 Rn. 32.

41 Ferner müsste mittels Vermögensverfügung aber auch unmittelbar ein Vermögensschaden beim Anbieter entstehen.[65] Die Beeinflussung des Ergebnisses eines Datenverarbeitungsvorganges nach § 263a Abs. 1 StGB ersetzt Irrtum und Vermögensverfügung im Sinne des § 263 Abs. 1 StGB.[66] Dabei sprechen wiederum verschiedene Erwägungen gegen eine Strafbarkeit. Sämtliche hier angesprochenen Portale bieten nämlich den Content kostenfrei an. Selbst wenn also die Nutzungsmöglichkeit per Stream als Vorteil des Nutzers anzusehen ist, der aufgrund der Mitteilung der IP-Adresse des Proxys demselben und damit auch der diesen verwendenden konkreten Person gewährt wird, so entgeht dem Rechteinhaber, der seine Werke anbietet, dadurch keine seitens des Abrufenden geschuldete Gegenleistung. Es ist ja nicht so, dass die Dateien nur den Personen innerhalb des inkludierten geografischen Bereiches kostenfrei angeboten würden, während alle anderen dafür zahlen müssten. Darauf abzustellen, dass Nutzer sich ansonsten die entsprechenden Werke käuflich erwerben müssten, geht fehl, denn eine solche Möglichkeit besteht nur potenziell und ist nicht Gegenstand des konkreten Austauschverhältnisses.

42 Als letztes wäre noch zu erwägen, ob sich etwas anderes für solche Websites ergibt, auf welchen die Rechteinhaber die Dateien nicht selbst anbieten. Bei Portalen wie *YouTube*, bei welchen Rechteinhaber und Anbieter nicht identisch sind, ist jedoch wiederum problematisch, dass den Anbietern selbst ohnehin keinerlei Schaden entsteht, da sie weder Urheber oder Leistungsschutzberechtigte sind noch ein Entgelt für das Abrufen der Dateien verlangen. Sie verständigen sich regelmäßig mit den Rechteinhabern gegen Zahlung von Pauschalbeträgen auf eine bestimmte territoriale Nutzung, d.h. sie entrichten ein bestimmtes Entgelt für den Erwerb des Nutzungsrechts des Anbietens der Werke. Wenn überhaupt, so kann in diesem Fall daher nur von einem Dreieckscomputerbetrug[67] gesprochen werden, bei welchem die Rechteinhaber als Geschädigte in Betracht kämen. Hier erscheint es aber einerseits schon äußerst zweifelhaft, ob der Getäuschte, also der Anbieter, im Sinne der h.M. in einem „Näheverhältnis" zum eigentlichen Rechteinhaber steht, sodass eine entsprechende Nähe zwischen Verfügendem und Geschädigtem hergestellt wäre.[68] Denn bei Personen, die Dateien auf *YouTube* einstellen, handelt es sich regelmäßig um private Anbieter, die, wie auch das Unternehmen selbst, andere, sogar gegenläufige Interessen verfolgen als Urheber und Leistungsschutz- oder Nutzungsberechtigte. Die privaten Anbieter selbst wollen die Werke allen zugänglich machen und auch *YouTube*, welches als Systembetreiber diesen Vorgang ermöglicht und dessen Geo-IP-Sperre umgangen wird, hat ein Interesse an möglichst weitgehenden Angeboten. Vertraglich berechtigt zur Verfügung im Sinne des Anbietens und der Ermöglichung des Streaming etwa in Deutschland sind die Beteiligten nicht, und im „Lager" der Rechteinhaber, wie es insbesondere die Rechtsprechung fordert,[69] dürften sie auch sonst nicht stehen.[70] Daher scheidet auch hier schon der objektive Tatbestand aus.

43 Im Übrigen kann aber der Schaden der Rechteinhaber bei Abruf in anderen Ländern nur entweder im Entgehen des pauschalierten Entgelts für das Anbieten der Werke oder der entgangenen Einnahme aus einem – rein hypothetischen – Verkauf des Werkes an die Endnutzer liegen, sodass jeweils wiederum nur mittelbare Schäden entstehen. Das Streaming selbst ist kostenfrei und auch, wie dargestellt, nicht urheberrechtswidrig. Der Vorteil, den der Täter hier in Bereicherungsabsicht erlangen wollen muss, wäre daher jedenfalls nicht stoffgleich mit den soeben angeführten

[65] Der Vermögensschaden entspricht hier § 263 StGB; vgl. *Cramer/Perron*, in: Schönke/Schröder (o. Fn. 54), § 263a Rn. 24.; Hilgendorf/Valerius (Fn. 14), Rn. 523.
[66] *Tiedemann/Valerius*, in: LK (o. Fn. 63), § 263a Rn. 65.
[67] Zur Anwendung der Grundsätze des Dreiecksbetruges auf den Computerbetrug Tiedemann/Valerius, in: LK (o. Fn. 63), § 263a Rn. 71.
[68] Ausführlich zu den Voraussetzungen des Dreiecksbetruges *Hefendehl*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum StGB (MüKo), Band 4, München 2006, § 263 Rn. 282 ff.; *Tiedemann*, in: LK (o. Fn. 62), § 263 Rn. 112 ff.
[69] Vgl. BGHSt 18, 221, 223.
[70] Zur Lagertheorie *Hefendehl*, in: MüKo (o. Fn. 68), § 263 Rn. 285.

eventuellen Schäden, sodass es immerhin am subjektiven Tatbestand fehlt. Denn mittelbare Schäden und Folgeschäden sind gerade nicht stoffgleich mit dem erlangten Vorteil.[71]

44 **D. Gesamtergebnis**

Das Streaming von Werken ist straflos. Sofern das deutsche UrhG anwendbar ist, kommt zwar eine Strafbarkeit gemäß § 106 Abs. 1 UrhG (bzw. § 108 UrhG) in Betracht. Der objektive Tatbestand scheidet jedoch aus, weil das negativ formulierte Tatbestandsmerkmal des Nichtvorliegens eines gesetzlich zugelassenen Falles nicht erfüllt ist. Denn es greift § 44a Nr. 2 UrhG, der Vervielfältigungen privilegiert, die flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen und deren alleiniger Zweck es ist, eine rechtmäßige Nutzung des Werks zu ermöglichen und die keine eigenständige wirtschaftliche Bedeutung haben. Der rezeptive Werkgenuss ist urheberrechtsfrei und daher rechtmäßige Nutzung. Ferner hat der Vorgang der temporären und technisch bedingten Zwischenspeicherung im Buffer keine über diese Nutzung hinausgehende eigenständige Bedeutung, sodass die Voraussetzungen der Privilegierungsvorschrift erfüllt sind.

45 Auch das Umgehen einer Geo-IP-Sperre ist strafrechtlich nicht relevant. Denn es handelt sich nicht um eine technische Schutzmaßnahme im Sinne des § 108b UrhG. Auch Strafvorschriften des StGB scheiden aus. § 202a StGB setzt die Überwindung einer besonderen Schutzvorrichtung voraus, welche bei einem Geo-IP-Filter ebenfalls nicht angenommen werden kann, da dieser sich bei Einsatz eines Proxys gar nicht als wirksam darstellt. § 263a StGB scheitert ganz allgemein daran, dass den Anbietern kein Schaden entsteht, da sie ihre Leistungen ohnehin kostenlos für alle Nutzer zur Verfügung stellen, die sich in einem bestimmen geografischen Bereich aufhalten. Ein Schaden entsteht allenfalls mittelbar, was von § 263a StGB nicht erfasst ist. Das hier gefundene Ergebnis erscheint auch rechtspolitisch zu unterstützen, denn die Anonymisierung im Internet ist – auch im Hinblick auf das Recht auf informationelle Selbstbestimmung und die Telekommunikationsfreiheit – per se kein strafwürdiges Unrecht.

Zitierempfehlung: Tobias Reinbacher, HFR 2012, S. 179 ff.

[71] *Fischer* (o. Fn. 56), § 263 Rn. 187; *Tiedemann*, in: LK (o. Fn. 63), § 263 Rn. 257.