In Kooperation mit:
bitkom e.V.
davit im DAV
eco e.V.
game e.V.
VAUNET

MMR MultiMedia und Recht

Zeitschrift für Informations-, Telekommunikations- und Medienrecht

Herausgeber: Dr. Astrid Auer-Reinsdorff · Prof. Dr. Oliver Castendyk · Prof. Dr. Nikolaus Forgó · Prof. Dr. Sibylle Gierschmann · Prof. Dr. Christian-Henner Hentsch · Prof. Dr. Reto M. Hilty Prof. Dr. Thomas Hoeren · Prof. Dr. Bernd Holznagel · Wolfgang Kopf · Prof. Dr. Marc Liesching · Prof. Dr. Peter Raue · Prof. Dr. Alexander Roßnagel · Prof. Dr. Joachim Scherer Dr. Raimund Schütz · Prof. Dr. Ulrich Sieber · Prof. Dr. Louisa Specht-Riemenschneider · Dr. Axel Spies · Prof. Dr. Gerald Spindler

ROLF SCHWARTMANN / CHRISTIAN-HENNER HENTSCH
KONSTANTIN EWALD (Hrsg.)

Neue Wege der Rechtsdurchsetzung für Games

Editorial	**1**	KONSTANTIN EWALD **Neue Wege der Rechtsdurchsetzung für Games**
Rechtsdurchsetzung	**3**	CHRISTIAN-HENNER HENTSCH **Piraterie in der Games-Branche**
Illegale Internetangebote	**7**	JULIAN WAIBLINGER / STANISLAUS JAWORSKI **Games-Piraterie – Website-Sperren als Mittel der Rechtsdurchsetzung**
Erschöpfungsgrundsatz	**12**	THOMAS MERK / ADRIAN SCHNEIDER **Keyselling: Rechtliche Grenzen beim Handel mit Lizenzschlüsseln für Computerspiele**
Gewerbsmäßige Urheberrechtsverletzung	**16**	FELIX HILGERT / MARTIN SESTER **Strafrechtliche Verantwortlichkeit für den Betrieb von Piraterie-Servern**
Abwehransprüche	**20**	CHRISTIAN RAUDA **Cheatbots in Computerspielen**

game
Verband der deutschen Games-Branche

www.mmr.de

Osborne Clarke

Kölner Forschungsstelle für Medienrecht
Technology Arts Sciences TH Köln

MMR-Beilage
8/2019

Seiten 1–24
22. Jahrgang · 14. August 2019
Verlag C.H.BECK München

1830201908

In Kooperation mit:
bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
davit im DAV - Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein
eco - Verband der Internetwirtschaft e.V.
game - Verband der deutschen Games-Branche e.V.
VAUNET - Verband Privater Medien

MMR MultiMedia und Recht

Zeitschrift für Informations-, Telekommunikations- und Medienrecht

8/2019 Beilage

HERAUSGEBER

RAin **Dr. Astrid Auer-Reinsdorff**, FA IT-Recht, Berlin/Lissabon/Vorsitzende des Geschäftsführenden Ausschusses der Arbeitsgemeinschaft IT-Recht im DAV (davit) – RA **Prof. Dr. Oliver Castendyk**, MSc. (LSE), Direktor Allianz Deutscher Produzenten – Film & Fernsehen e.V., Berlin – **Prof. Dr. Nikolaus Forgó**, Professor für Technologie- und Immaterialgüterrecht und Vorstand des Instituts für Innovation und Digitalisierung im Recht, Universität Wien – RAin **Prof. Dr. Sibylle Gierschmann**, LL.M. (Duke University), FA Urheber- und Medienrecht, Hamburg – **RA Prof. Dr. Christian-Henner Hentsch**, M.A., LL.M., Leiter Recht und Regulierung beim game – Verband der deutschen Games-Branche e.V., Berlin/Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln – **Prof. Dr. Reto M. Hilty**, Direktor am Max-Planck-Institut für Innovation und Wettbewerb, München/Ordinarius an der Universität Zürich – **Prof. Dr. Thomas Hoeren**, Direktor der Zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Bernd Holznagel**, Direktor der Öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Wolfgang Kopf**, LL.M., Leiter Zentralbereich Politik und Regulierung, Deutsche Telekom AG, Bonn – **Prof. Dr. Marc Liesching**, Professor für Medienrecht und Medientheorie, HTWK Leipzig/München – RA **Prof. Dr. Peter Raue**, Raue LLP, Berlin – **Prof. Dr. Alexander Roßnagel**, Universität Kassel/Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) – RA **Prof. Dr. Joachim Scherer**, LL.M., Baker & McKenzie, Frankfurt a.M. – RA **Dr. Raimund Schütz**, Loschelder Rechtsanwälte, Köln – **Prof. Dr. Ulrich Sieber**, Direktor und Leiter der strafrechtlichen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Freiburg/Honorarprofessor und Leiter des Rechtsinformatikzentrums an der Ludwig-Maximilians-Universität, München – **Prof. Dr. Louisa Specht**, Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht, Rheinische Friedrich-Wilhelms-Universität Bonn – RA **Dr. Axel Spies**, Morgan, Lewis & Bockius LLP, Washington DC – **Prof. Dr. Gerald Spindler**, Universität Göttingen

WISSENSCHAFTLICHER BEIRAT

Daniela Beaujean, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Medien (VAUNET), Berlin – **Dietrich Beese**, Hamburg – **Prof. Dr. Herbert Burkert**, Forschungsstelle für Informationsrecht, Universität St. Gallen – RAin **Susanne Dehmel**, Mitglied der Geschäftsleitung BITKOM e.V., Berlin – **Jürgen Doetz**, Koordinator der Deutschen Content Allianz, Berlin – **Dr. Andrea Huber**, LL.M. (USA), Geschäftsführerin, ANGA Verband Deutscher Kabelnetzbetreiber e.V., Berlin – **Dr. Christine Kahlen**, Leiterin Öffentlichkeitsarbeit, Bundesministerium für Wirtschaft und Technologie, Berlin – **Dr. Christopher Kuner**, J.D., LL.M., Senior of Counsel, Wilson Sonsini Goodrich & Rosati, LLP, Brüssel – **Prof. Dr. Wernhard Möschel**, Vorsitzender des Wissenschaftlichen Beirats beim BMWi/Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Universität Tübingen – **Robert Queck**, Maître de Conférences, Centre de Recherches Informatique et Droit (CRID), Universität Namur, Belgien – **Prof. Dr. Eike Ullmann**, Vors. Richter des I. Zivilsenats am BGH a.D., Karlsruhe

REDAKTION

Anke Zimmer-Helfrich, Chefredakteurin – RAin **Ruth Schrödl**, Redakteurin – **Eva Wanderer**, Redaktionsassistentin
Wilhelmstr. 9, 80801 München

EDITORIAL

Neue Wege der Rechtsdurchsetzung für Games

Lesedauer: 8 Minuten

Am 20.8.2019 ist es wieder soweit: Die *gamescom*, das weltweit größte Event für Computer- und Videospiele, wird zum 11. Mal stattfinden und einmal mehr über die neuesten Trends der Computer- und Videospieleindustrie informieren. Die Innovationskraft und das wirtschaftliche Wachstum der Branche sind weiterhin atemberaubend.

Der Markt der Computerspiele wird nach Erwartung führender Analysten im Jahr 2019 auf etwa US-$ 150 Mrd. wachsen. Ein besonderer Umsatztreiber ist hierbei das Branchensegment der mobilen Games, also jener Spiele, die wir auf unseren Smartphones und Tablets spielen. Waren es am Anfang noch die sog. casual games wie „Candy Crush", die den Markt bestimmten, so ist spätestens seit dem beeindruckenden Erfolg von Spielen wie „Fortnite" oder „PlayerUnknown's Battlegrounds" klar, dass wir auch auf mobilen Geräten inhaltlich und technisch anspruchsvollere Spiele spielen werden.

Auf der technischen Seite zeichnet sich ab, dass nach dem großen Erfolg von Spielen wie Pokemon Go weitere Augmented Reality (AR)-Titel auf den Markt kommen werden und sich diese Technologie immer weiter durchsetzen wird. Gleiches gilt für den Bereich von Virtual-Reality (VR)-Anwendungen. Zur Darstellung virtueller Welten benötigt der Spieler VR-Headsets. Verbreiteten sich diese neuen VR-Konsolen zunächst langsamer als erwartet, so wurden mit der Veröffentlichung neuer VR-Modelle inzwischen die Voraussetzungen dafür geschaffen, dass diese neuen Spielekonsolen Einzug in die Wohnzimmer halten. Nebenbei: VR-Anwendungen entwickeln sich auch zu einem Segment, in dem Spieleentwickler und klassische Industrie, etwa im Bereich Automobilindustrie, Anlagenbau, Logistik oder im Gesundheitswesen, zunehmend mehr zusammenarbeiten.

Konstantin Ewald

Der Markt wird immer mehr von neuen Vertriebsformen geprägt. Eine wachsende Anzahl von Online-Distributionsplattformen führt dazu, dass Spieleanbietern neue digitale Vertriebswege offenstehen. Der Verbraucher freut sich über mehr Wettbewerb. Wirklich neu ist, dass Games nun zunehmend als Online-Stream konsumiert werden können. Die Spielebranche vollzieht also nach, was die Filmbranche mit Netflix & Co vorgemacht hat.

Für den deutschen Markt von besonderer Bedeutung ist der Start des Games-Fonds, der die Entwicklung von Computer- und Videospielen erstmalig bundesweit fördern wird. Im Bundeshaushalt 2019 sind hierfür € 50 Mio. allokiert worden, für dessen Umsetzung das *Bundesministerium für Verkehr und Digitale*

Infrastruktur verantwortlich ist. Durch eine erste vorgezogene Maßnahme können seit Juni 2019 Anträge für eine De-minimis-Beihilfe bis € 200.000,– pro Unternehmen in drei Jahren gestellt werden (FAQ zur De-minimis-Beihilfe, abrufbar unter: https://www.game.de/faq-deminimis-foerderung/).

Für gameslaw-Interessierte ist es wichtig, bei diesen neuen technischen wie wirtschaftlichen Trends am Ball zu bleiben. So lassen sich z.B. Fragen, ob AR- oder VR-Anwendungen ihre Umgebung urheberrechtlich zulässig erfassen und auswerten dürfen und welche Daten hierbei erhoben und verarbeitet werden dürfen, nur dann rechtlich diskutieren, wenn man die zu Grunde liegende Technologie verstanden hat. Gleiches gilt für die bereits begonnene Diskussion, in welchem Umfang der deutsche Jugendmedienschutz, der sich immer noch sehr an einer physischen Distribution von Games orientiert, reformiert werden muss.

Die MMR hat sich vorgenommen, wissenschaftliche Plattform für Beiträge zum Spielerecht zu sein und Beiträge zur Diskussion dieser neuen Rechtsfragen zu publizieren. So erschien im August 2018 die erste MMR-Beilage mit dem Themenschwerpunkt zu eSport. Der Themenschwerpunkt der diesjährigen Beilage lautet: „Neue Wege der Rechtsdurchsetzung für Games".

Christian-Henner Hentsch wird zunächst die Geschäftsmodelle der Spielebranche erläutern und einen Überblick über neue Piraterie-Herausforderungen geben. *Julian Waiblinger* und *Stanislaus Jaworski* befassen sich dann umfassend mit Seitensperren in der Games-Branche. Ein für die Rechtsverfolgung hoch relevantes Thema haben sich *Thomas Merk* und *Adrian Schneider* vorgenommen. Sie bewerten die rechtliche Zulässigkeit des Keyselling, also den isolierten Verkauf von Produktschlüsseln (Keys) für Computerspiele. Hieran schließt sich der Beitrag von *Martin Sester* und *Felix Hilgert* an, der Piraten-Server aus strafrechtlicher Sicht beleuchtet. *Christian Rauda* analysiert zum Abschluss die Zulässigkeit von Cheatbots in Computerspielen.

All diese Themen werden auch Gegenstand der wissenschaftlichen Diskussion des auch in diesem Jahr stattfindenden Summits der *Video Game Bar Association (vgba)* sein – dem führenden Event für Spielerechtler in Europa. Der *vgba*-Summit (www.vgbaeurosummit.org) findet am 19.8.2019 erstmals als Bestandteil der Entwicklermesse *devcom* im unmittelbaren Vorfeld der *gamescom* ebenfalls auf dem Messegelände in Köln statt.

Wir hoffen, den Lesern der MMR mit den Beiträgen der vorliegenden Beilage weitere wertvolle Einblicke in die Rechtsfragen der Spielebranche zu liefern. Wir danken dem Verlag C.H.BECK und ganz besonders Frau Anke Zimmer-Helfrich, Chefredakteurin der MMR, für die konstruktive Zusammenarbeit.

Köln, im August 2019

Konstantin Ewald
ist Rechtsanwalt bei Osborne Clarke und Betreiber des Blogs zu Rechtsfragen der Spieleindustrie www.spielerecht.de.

CHRISTIAN-HENNER HENTSCH

Piraterie in der Games-Branche

Ein Überblick über Geschäftsmodelle und Herausforderungen

Rechtsdurchsetzung

Neue Geschäftsmodelle und Vertriebswege der Games-Branche verändern auch die Herausforderungen und die Ansatzmöglichkeiten in der Pirateriebekämpfung. Beim klassischen Verkauf von Computerspielen auf Datenträgern oder als Download greift in den meisten Fällen wegen der Account-Bindung der technische Kopierschutz. Dafür sorgt das sich in einer rechtlichen Grauzone befindliche Keyselling von gebrauchten Spielen für Verwerfungen in der Preisgestaltung – mit Vor- und Nachteilen. Zudem gibt es bei Free-to-Play-Games und Abonnements Probleme mit illegalem Handel, Bots und Piraten-Servern. Vor allem für Konsolen bleiben strukturell rechtswidrige Plattformen ein Pirateriepoblem, weil dort Spiele und Umgehungssoftware zum Download angeboten werden. Besonderes Augenmerk gilt hier den Seitensperrverfahren, die auch für Games-Unternehmen interessant sein können. Für die meisten Ansätze ist mittlerweile das Zivilrecht das Mittel der Wahl. Das Strafrecht ist mit Blick auf Piraten-Server erfolgversprechend, verliert in der Tendenz für die Games-Branche allerdings zunehmend seine Bedeutung für die Verfolgung von Urheberrechtsverletzungen.

Lesedauer: 19 Minuten

I. Einleitung

Der *game – Verband der deutschen Games-Branche e.V.* – hat in seiner jüngsten Mitgliederversammlung beschlossen, seine Mitgliedschaft in der *Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU)* zum Ende des Jahres 2019 zu kündigen. Diese Entscheidung steht am Ende eines über ein Jahr dauernden Evaluierungsprozesses, der schon vor dem Austritt der Hollywood-Studios im Sommer 2018 begonnen wurde. Nach wiederholten Diskussionen in der Mitgliedschaft und intensiven Gesprächen und Verhandlungen mit der *GVU* wird die Games-Branche nun neue Wege gehen – und ist natürlich offen für neue Partnerschaften und Projekte. Denn die Beendigung der *GVU*-Mitgliedschaft bedeutet nicht, dass Piraterie in der Games-Branche keine Rolle mehr spielt. Sie ist vielmehr Ausdruck der gewandelten Geschäftsmodelle und neuer Ansätze zur Pirateriebekämpfung.

Als die *GVU* 1985 gegründet wurde, ging es vor allem um die strafrechtliche Verfolgung der massenhaften Anfertigung von illegalen Kopien auf physischen Datenträgern wie der aufkommenden VHS-Videokassette. Treiber eines Beitritts der Games-Branche zur *GVU* waren insbesondere Konsolenhersteller wie *Sony* und *Nintendo*, die gegen die massenhaften Raubkopien und gegen manipulierte Konsolen, auf denen diese Raubkopien genutzt werden konnten, vorgehen wollten. Für diese Herausforderungen war der erfolgversprechendste Ansatz damals das Strafrecht, weil damit Beschlagnahmen physischer Raubkopien möglich waren und die organisierte Raubkopier-Szene abgeschreckt werden konnte.

Inzwischen haben sich die Vertriebswege für Computerspiele deutlich ausdifferenziert und vor allem auch digitalisiert. Dadurch haben sich die Geschäftsmodelle der Games-Branche erheblich verändert. Damit verbunden sind neue Herausforderungen der Branche bei der Pirateriebekämpfung. Diese Veränderungen, deren Einfluss auf Pirateriemodelle und die möglichen Schutzmaßnahmen und Ansätze zur Rechtsverfolgung, soll dieser Beitrag im Folgenden aufzeigen.

Es wird dabei auf die Geschäftsmodelle abgestellt und jeweils ein Überblick über die Herausforderungen und die möglichen Ansätze zur Rechtsdurchsetzung im Zivil- oder Strafrecht aufgezeigt. Die Details der juristischen Rahmenbedingungen, konkrete Verfahren und die einschlägige Rechtsprechung dazu werden in den Beiträgen dieser Beilage von *Merk/Schneider* zu Keyselling, von *Waiblinger/Jaworski* zu Seitensperren, von *Hilgert/Sester* zu Piraten-Servern und von *Rauda* zu Bots dargestellt. I.E. sollen dieser Beitrag im Allgemeinen und auch die folgenden Beiträge im Konkreten deutlich machen, welche Rolle das Strafrecht und das Zivilrecht heute bei der Rechtsdurchsetzung im Gaming spielen.

II. Box Products und digitale Downloads

Die Computerspieleindustrie ist eine stark wachsende Medienbranche mit vielfältigen und innovativen Geschäftsmodellen. Im Jahr 2018 ist der Umsatz in Deutschland um 9% auf mehr als € 4,4 Mrd. gestiegen.[1] Etwa ein Viertel des Umsatzes – € 1,081 Mrd. – wird mit dem Verkauf von Spielen mit einem physischen Trägermedium und/oder einem Key in einer Box (Box Product) oder dem digitalen Download eines Spiels erwirtschaftet. Dabei handelt es sich sowohl um sog. AAA-Produktionen (Triple A), die teilweise mehrere 100 Mio. Euro Entwicklungskosten erfordern, als auch um Indie-Spiele, die teilweise von Studierenden und Hochschulabsolventen auf den Markt gebracht werden.

Die wichtigsten Vertriebswege sind neben dem Einzelhandel digitale Vertriebsplattformen für PC wie Steam und Epic Games Store, die Shops der Konsolen von *Microsoft*, *Nintendo* und *Sony*, firmeneigene Stores wie Uplay von *Ubisoft* oder Origin von *EA* und natürlich der Google Play Store sowie der App Store von Apple. Die Preise bewegen sich zwischen wenigen Cent in den App Stores und rd. € 60,– für sogenannte Vollpreisspiele. Oft werden solche Spiele noch querfinanziert durch Premium-Modelle mit bestimmten Vorzügen, kostenpflichtige DLCs (herunterladbare Inhalte), Online-Pässe zum Spielen im Mehrspielermodus oder andere Formen wiederkehrender Zahlungen. Diese letztgenannten Einnahmequellen bleiben in diesem ersten Abschnitt außer Acht und werden als In-Game-Käufe gesondert betrachtet.

1. Technischer Kopierschutz

Seit jeher schützen sich die Hersteller von Computerspielen mit technischen Kopierschutzmaßnahmen gegen unberechtigte Kopien ihrer Werke. Im Vergleich zu den ersten Schutzprogrammen sind die heutigen Verschlüsselungstechnologien inzwischen so ausgeklügelt, dass die Entschlüsselung – das „Cracken" – nur noch von Profis vorgenommen werden kann und daher die Kompromittierung eines Spiels immer länger dauert, wodurch zumindest die für die Refinanzierung so wichtige erste

1 Vgl. Umsatzzahlen des Branchenverbandes *game*, abrufbar unter: https://www.game.de/marktdaten/.

Auswertungsphase abgedeckt wird. Hinzu kommen Anwendungsschutzmethoden wie Passwortabfragen, Seriennummern, Dongles und hardwarebasierte Lizenzen und Regionalcodes sowohl für Datenträger als auch durch Aktivierungscodes für Downloads.

Dies führt dazu, dass die illegale Nutzung von Computerspielen erheblich zurückgegangen ist. Dazu tragen auch die nutzerfreundlichen Angebote in geschlossenen Systemen – sei es Konsole oder Smartphone – bei. Legal erworbene Inhalte sind mittlerweile auf allen Geräten nutzbar und einfach zu administrieren, während gecrackte Spiele mit einem gewissen IT-Sachverstand erst mühsam erstellt oder illegal erworben werden müssen und viele Einschränkungen das Spielerlebnis schmälern. Insofern ist der technische Urheberrechtsschutz immer erfolgversprechender und noch dazu weltweit einsetzbar. Hier hat sich also der Schwerpunkt von der strafrechtlichen Rechtsverfolgung gegen Brenner- und Cracker-Kollektive verschoben hin zu einem offensiven Kopierschutz und nutzerfreundlichen Angeboten.

2. Notice-and-Take-Down

Illegale, gecrackte Angebote und Umgehungssoftware auf strukturell rechtswidrigen Plattformen gibt es allerdings auch weiterhin. Daher haben die meisten großen Publisher auch jeweils einen eigenen Dienstleister für Notice-and-Take-Down-Maßnahmen (NTD) engagiert. Wegen des internationalen Vertriebs wird dies in der Regel nicht national durchgeführt, sondern zentral an einen Anbieter vergeben. Synergien wie bei den Filmstudios mit ihrer *Initiative Alliance for Creativity and Entertainment (ACE)*[2] sind hier nur schwer zu erreichen, weil abhängig von den Vertriebsplattformen, dem technischen Kopierschutz und der Distributionsreichweite unterschiedliche Anforderungen erfüllt werden müssen. Trotzdem gibt es nach dem Vorbild des britischen Verbands *UKIE* auch in Deutschland Bestrebungen Rahmenverträge mit NTD-Anbietern abzuschließen. Strafrechtliche Ermittlungen gegen Betreiber von strukturell rechtswidrigen Websites wie kinox.to sind aus Sicht der Branche wünschenswert, aber auch langwierig und aufwändig. Insofern sind schnelle Take-Down-Maßnahmen, wo sie funktionieren, vorzuziehen.

3. Seitensperren

Gerade weil NTD-Maßnahmen in Deutschland und anderen europäischen Ländern reibungslos laufen, finden sich strukturell rechtswidrige Plattformen und die dahinter liegenden illegalen Angebote inzwischen fast nur noch im Ausland und die Verantwortlichen können meist nicht ermittelt werden. Dies führt dazu, dass sowohl zivilrechtliche als auch strafrechtliche Anknüpfungspunkte für diese Rechtsverletzungen fehlen. Daher verfolgt die Games-Branche die laufenden Seitensperrverfahren mit großem Interesse.[3]

Die Entscheidung des *BGH* zum Computerspiel „Dead Island 2"[4] hat deutlich gemacht, dass Seitensperren grundsätzlich auch für Games relevant sein können. Insbesondere in Kombination mit technischen Kopierschutzmaßnahmen kann eine konsequente Seitensperre die erste Auswertungsphase nachhaltig schützen. Damit sind Seitensperren eine gute Ergänzung zum bisher genutzten zivilrechtlichen Instrumentarium. Um die Voraussetzungen für die Anordnung einer Sperre zu erfüllen, muss nachgewiesen werden, dass es sich um eine strukturell rechtswidrige Seite handelt und dass die Betreiber und deren Dienstleister (z.B. Host-Provider) erfolglos angegangen wurden. Hierfür braucht es dringend eine Institution wie die *GVU* oder einen vergleichbaren Dienstleister, der die entsprechenden Daten vorliegen hat und die erforderlichen Ermittlungen vornehmen kann.

4. Keyselling

Eine bislang noch recht Games-spezifische Herausforderung ist das Keyselling, also der Weiterverkauf „gebrauchter Spiele". In der Regel werden inzwischen auch Box Products wie beim digitalen Download mit einem Aktivierungs-Key verkauft, oftmals sogar ganz ohne Datenträger. Für bloße Software greift der Erschöpfungsgrundsatz des §§ 17 Abs. 2 bzw. 69c Nr. 3 UrhG: Ein Computerprogramm, das innerhalb des EWR im Wege des Verkaufs in den Verkehr gebracht wurde, darf im EWR auch frei weiterverkauft werden – vorausgesetzt der Rechteinhaber konnte eine angemessene Vergütung erzielen und der Verkäufer vernichtet seine eigene Kopie.[5] Das gilt nach Ansicht des *BGH* auch, wenn Key und Installations-DVD aufgespalten werden.[6]

Doch Computerspiele sind keine reine Software im Sinne der o.g. Rechtsprechung, sondern eine Mischform aus verschiedenen technischen und vor allem auch künstlerischen Elementen. Die Rechtsprechung spricht von sog. „hybriden Werken"[7], auf die die Rechtsprechung zu reiner Software (wie etwa Business-Software) nicht anwendbar ist. Die Ausnahme für „Gebrauchtsoftware" ist daher bislang nicht auf Computerspiele übertragbar. Hier ist natürlich das dem *EuGH* vorliegende Verfahren in Sachen „Tom Kabinet" (Rs. C-263/18) interessant, inwieweit der Erschöpfungsgrundsatz analog auch auf eBooks bzw. urheberrechtlich geschützte Werke anwendbar ist. Die Games-Branche, die Buchwirtschaft und andere Content-Industrien haben hier gleichlaufende Interessen und stehen vor gemeinsamen Herausforderungen.

In der Praxis haben sich im Games-Bereich aber schon heute Keyselling-Plattformen wie G2A, Gamesrocket und Kinguin etabliert, auf denen millionenfach Computerspiele gehandelt werden. Neben der vorgeschriebenen Umsatzsteuerabführung, jugendschutzrechtlichen Bestimmungen und möglicher irreführender Werbung stellt sich hier zunehmend auch das Problem der Geldwäsche und des Betrugs, wenn Keys mit gestohlenen Kreditkartendaten gekauft und dort weiterverkauft werden.

Schon deshalb scheidet der Erschöpfungsgrundsatz in diesen Fällen regelmäßig aus: Wurde der Rechteinhaber im Wege des Betrugs um die Möglichkeit gebracht, eine angemessene Vergütung für den verkauften Key zu erzielen, sind die Voraussetzungen für den Eintritt der Erschöpfung nicht erfüllt. Die Beweislast dafür, dass die Voraussetzungen der Erschöpfung erfüllt sind, liegt zudem beim Keyseller.[8] Sie müssen nachweisen, dass der verkaufte Key innerhalb des EWR auf den Markt gebracht wurde und vollständig bezahlt wurde. Einen lückenlosen Herkunftsnachweis sucht man bei unautorisierten Keyselling-Plattformen in der Praxis jedoch fast ausnahmslos vergeblich.

Unter diesem Druck haben aber auch die Keyseller ihre Geschäftsmodelle angepasst und „Whitewashing" betrieben. Soweit sie die rechtlichen Voraussetzungen einhalten und Geldwäsche und Betrug auf ihren Plattformen unterbinden, stellen sie sich für einige Publisher und deren Marketing-Abteilungen zunehmend als Partner dar. So können über diesen Vertriebsweg gerade am Anfang oder Ende einer Auswertungsphase auf einen Schlag größere Stückzahlen abgesetzt werden. Zudem wird dadurch neben quasi-monopolistischen Vertriebsplattfor-

2 Abrufbar unter: https://www.alliance4creativity.com.
3 Hierzu ausf. *Waiblinger/Jaworski*, MMR-Beil. 8/2019, 7 – in diesem Heft.
4 *BGH* MMR 2018, 811; ausf. dazu *Nordemann*, GRUR 2018, 1016: Die Haftung allgemeiner Zugangsprovider auf Website-Sperren. Der aktuelle Stand nach *BGH* „Dead Island".
5 *EuGH* MMR 2012, 586.
6 *BGH* MMR 2015, 735.
7 *EuGH* MMR 2014, 401.
8 *BGH* MMR 2014, 232 m. Anm. *Heydn* – UsedSoft II.

men eine Alternative etabliert. Hier bleibt also abzuwarten, ob das ursprünglich eher rechtsverletzende Geschäftsmodell des Keyselling sich vielleicht zu einem legalen und von der Branche unterstützen Vertriebsweg entwickeln wird.

5. Zwischenfazit

Ein näherer Blick auf Box Products und digitale Downloads zeigt, dass die Games-Branche bei technischen Kopierschutzmaßnahmen, NTD und Seitensperren und z.T. auch beim Keyselling vor ähnlichen Herausforderungen wie andere Content-Industrien steht und vergleichbare Ansätze verfolgt.

Auf Grund des Mediums ist der Vertrieb jedoch schon deutlich digitaler und lässt sich wegen der Account-Bindung und anderer Maßnahmen teilweise besser schützen. Bei allen Ansätzen spielt allerdings das Strafrecht nur noch eine untergeordnete Rolle. Im Vordergrund der Rechtsdurchsetzung stehen zivilrechtliche Ansprüche gegen Content- und Host-Provider und zukünftig vielleicht auch gegen Service-Provider.

III. In-Game-Käufe

Eine noch recht Games-spezifische Refinanzierungsquelle stellen die sog. In-Game-Käufe dar. 2018 wurden damit € 1,949 Mrd. umgesetzt, was fast einem doppelten Umsatz im Vergleich zum Verkauf von Spielen entspricht. Dieser Bereich wächst seit Jahren rasant, allein im vergangenen Jahr um 28%.[9]

In-Game-Käufe sind vor allem bei sog. Free-to-Play-Spielen (F2P)[10] verbreitet. Hierbei wird das Spiel kostenlos zur Verfügung gestellt, ausschließlich für Zusatzinhalte können Kosten entstehen. Dies betrifft vor allem die zahlreichen mobilen Spiele, die ausschließlich digital angeboten werden. In-Game-Käufe werden aber zunehmend auch in Vollpreistiteln integriert, um zusätzliche Einnahmequelle zu erschließen und damit die immens steigenden Produktionskosten für AAA-Titel zu refinanzieren.[11]

Ein besonders interessanter Aspekt, gerade bei eSport-Titeln, ist die Verlängerung der Auswertungsphase, weil hier auch nach dem Verkauf des Spiels Einnahmen erzielt werden. Im Angebot sind in der Regel sowohl rein dekorative Zusatzinhalte (sog. „Skins", etwa Rüstungen oder auffällige Kleidung) als auch funktionelle Zusatzinhalte, die spielerische Vorteile gewähren (insbesondere Waffen oder auch Charaktere).[12]

Eine besondere Form der In-Game-Käufe sind sog. Lootboxen in denen gegen Geld zufällig ausgewählte Inhalte gekauft werden können – wie in einem Überraschungsei.[13] Dieser Bereich der In-Game-Käufe, der inzwischen die umsatzstärkste Säule der Refinanzierung von Games ausmacht, ist für Piraterie relativ wenig anfällig. Wegen der Account-Bindung und den hinterlegten Bezahldaten ist ein Crack im Spiel nahezu unmöglich. Stattdessen gibt es neue Wege, In-Game-Käufe illegal zu Geld zu machen, zu umgehen oder gar zu kapern.

1. Handel mit In-Game-Währung oder virtuellen Gütern

Naheliegend ist natürlich der Handel mit virtuellen Gütern im Spiel und auf Plattformen außerhalb des Spiels. Dabei handelt es sich zwar nicht um Piraterie im engeren Sinne, aber dem Anbieter entgehen dadurch zumindest mittelbar Einnahmen, weil die virtuellen Güter nicht mehr gegen Geld gekauft werden. Daher ist der Handel mit In-Game-Währung oder virtuellen Inhalten in den meisten AGB auch grundsätzlich untersagt. Dies hat das *OLG Hamburg*[14] für den Betrieb einer Plattform für den Handel mit Spielwährung bestätigt, soweit der Handel mit virtuellen Gütern in den AGB ausdrücklich ausgeschlossen ist.[15]

Dieses Vorgehen ist nicht nur aus Finanzierungsinteressen wichtig, sondern auch um der Gefahr des sog. Skin-Gambling oder Skin-Betting zu begegnen, bei dem gekaufte virtuelle Güter als Wetteinsatz in Onlinekasinos hinterlegt werden. Auf dem Schwarzmarkt für virtuelle Güter werden z.B. Drachenmuster-Skins für Scharfschützengewehre im Taktik-Shooter CS:GO für € 1.000,– gehandelt.[16] Damit entwickeln sich virtuelle Güter zunehmend zu einer milliardenschweren Kryptowährung. Ganz abgesehen von den glücksspielrechtlichen und auch sonstigen rechtlichen Problemen, gehen die Publisher auch aus eigenem Interesse vehement gegen solche Plattformen vor.[17] In all diesen Fällen kann der Spieleanbieter zwar nicht aus Strafrecht vorgehen, wohl aber aus Vertragsrecht, Wettbewerbsrecht und auch Markenrecht.

2. Bots

Eine weitere Herausforderung für In-Game-Käufe sind Bots. Mit solchen Computerprogrammen, die selbstständig Aktionen durchführen, können virtuelles Gold oder sonstige virtuelle Güter gesammelt („farmen" oder „looten") werden. Weil diese Güter getauscht oder im Spiel gegen In-Game-Währung verkauft werden können, wird dadurch der Kaufanreiz des Spielers gesenkt und damit auch die Refinanzierungsmöglichkeiten des Spieleanbieters eingeschränkt. Auch hier gibt es über das Vertragsrecht, das Urheberrecht, das Markenrecht und das UWG zahlreiche Möglichkeiten, zivilrechtlich gegen unerlaubte Bots und auch den Vertrieb solcher Bots vorzugehen.[18]

3. Piraten-Server

Eine Möglichkeit In-Game-Währung zu kapern, sind sog. Piraten-Server (auch P-Server), die den Server eines frei verfügbaren Spiels kopieren, auf einem eignen Server anbieten und damit Einnahmen generieren, die sonst auf dem Original-Server entstehen würden. Hierbei handelt es sich um eine Urheberrechtsverletzung, gegen die sowohl zivilrechtlich als auch strafrechtlich vorgegangen werden kann.

Ein Musterverfahren vor dem A*G Heidelberg* haben der Karlsruher Publisher *Gameforge* und die *GVU* ins Rollen gebracht. Von 2014 bis 2016 hatte ein Jugendlicher zwei Piraten-Server für das Online-Rollenspiel „Metin2" betrieben, auf denen zeitweise mehre hunderttausend Spieler angemeldet waren. Durch den Verkauf virtueller Gegenstände und Fähigkeiten wurden durch den Täter und seine Helfer sechsstellige Gewinne erzielt.[19] Bei Piraten-Servern stehen zivil- und strafrechtliche Rechtswege offen, wegen der im Strafrecht vorgesehenen Abschöpfungsmöglichkeiten ist das Strafverfahren hier vorzuziehen.

4. Zwischenfazit

Im Bereich der In-Game-Käufe hat die Games-Branche weitgehend neue Geschäftsmodelle erschlossen und betritt rechtlich häufig Neuland. Auf Grund der Gestaltung des Geschäftsmo-

9 Vgl. hierzu https://www.game.de/9-prozent-im-plus-deutscher-games-markt-waechst-2018-deutlich/.
10 Zum Begriff: *Mankowski*, in: Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG, 3. Aufl. 2016, Bd. 1, Zweiter Teil, S 12 Kap. M Rdnr. 293a.
11 Das Produktionsbudget für AAA-Produktionen ist gerade bei Open-World-Spielen immens gestiegen und beträgt inzwischen oft mehrere 100 Mio. Euro. Um den Preis für ein Vollpreisspiel konstant bei ca. € 60,– zu halten, ist eine Querfinanzierung durch Spieler, die mehr ausgeben können/wollen, angestrebt worden.
12 Hierzu auch *Fischer*, CR 2014, 588.
13 Zur Lootbox-Debatte *Nickel/Feuerhake/Schelinski*, MMR 2018, 586.
14 *OLG Hamburg* MMR 2013, 453.
15 Näher hierzu https://spielerecht.de/olg-hamburg-verbot-eines-goldseller-forums-volltext/.
16 Vgl. http://www.taz.de/Glueckksspiel-im-Internet/!5325377/.
17 Vgl. hierzu https://spielerecht.de/virtuelle-waehrungen-social-gaming-und-esports-im-fokus-der-gluecksspielregulierung/.
18 Hierzu *Rauda*, MMR-Beil. 8/2019, 20 – in diesem Heft.
19 Näheres zu dem Fall *Hilgert/Sester*, MMR-Beil. 8/2019, 16 – in diesem Heft.

dells geht es vielfach nicht mehr um technischen Kopierschutz, sondern um vertragliche Bestimmungen, dies vor allem vor dem Trend hin zu „Games as a service". Es werden also nicht mehr Inhalte verkauft, sondern vielmehr die Teilhabe am Spielspaß. Entsprechend ist das Urheberrecht nur noch bedingt für die Rechtsdurchsetzung geeignet, stattdessen wird vielmehr das Vertrags- und Wettbewerbsrecht geltend gemacht.

Entsprechend läuft häufig auch das Strafrecht leer und daher verlagert sich die Rechtsdurchsetzung in der Games-Branche zunehmend in den zivilrechtlichen Bereich. Gerade vor dem Hintergrund stagnierender Umsätze mit dem Verkauf von Spielen und rasant steigenden Einnahmen aus In-Game-Käufen, wird sich diese Tendenz noch verstärken.

IV. Gebühren für Onlinedienste

Als eine neue Säule bei der Refinanzierung von Computerspielen entwickeln sich gerade die Gebühren für Onlinedienste. Im Jahr 2018 haben sie sich nahezu verdoppelt auf jetzt € 353 Mio.[20] Zu solchen kostenpflichtigen Onlinediensten auf Spielekonsolen gehören Services wie Nintendo Switch Online, PlayStation Plus und Xbox Live Gold. Zum Leistungsumfang dieser Dienste gehört etwa die Möglichkeit, online mit- und gegeneinander zu spielen sowie Speicherstände in der Cloud zu sichern. Teil des Angebots sind häufig auch der kostenfreie Zugang zu wechselnden Computer- und Videospielen sowie Rabatte für den Kauf von Games und Erweiterungen in den Online-Stores der unterschiedlichen Plattformen.

Bei anderen Onlinediensten wie Origin Access oder dem Xbox Game Pass können Spieler für einen festen Betrag pro Monat auf einen großen Katalog an Games zugreifen, die sie dann auf ihre Spielekonsole und den PC installieren können. Andere Angebote wie PlayStation Now von *Sony* setzen dagegen auf Cloud-Gaming: Hierbei ist kein leistungsstarker Spiele-PC oder eine aktuelle Spielekonsole notwendig. Die eigentlichen Berechnungen des Spiels finden im Rechenzentrum statt. Dadurch können selbst Blockbuster-Titel mit aufwändiger Grafik auf leistungsschwachen Endgeräten gespielt werden. Notwendig ist allerdings eine schnelle und latenzarme Internetverbindung. Mit „Stadia" kündigte zuletzt auch *Google* einen solchen Cloud-Gaming-Dienst an.

Gerade mit Blick auf die aktuelle Entwicklung beim Cloud-Gaming ist von einem weiteren Wachstum der Onlinedienste in den kommenden Jahren auszugehen.

1. Cloud-Gaming

Cloud-Gaming ist eine konsequente Weiterentwicklung des Gedankens „Games as a service", weil der Spieler keine urheberrechtliche Lizenz mehr benötigt, sondern lediglich für den Zugang zum Spiel bezahlt. Damit kommt der Nutzer mit dem Urheberrecht quasi nicht mehr in Berührung und folglich sind Urheberrechtsverletzungen nahezu ausgeschlossen. Insoweit wird es wohl auch keine strafrechtlichen Ermittlungen wegen Urheberrechtsverletzungen geben.

2. Verkauf von Nutzer-Accounts

Bei allen Onlinediensten kommt jedenfalls auch der Verkauf von Accounts in Betracht, der jetzt schon z.B. bei Browser-Games oder auch bei der Spielevertriebs-Plattform Steam stattfindet. Dabei ist nach ständiger Rechtsprechung[21] ein Verkaufsverbot von Accounts bei entsprechenden AGB zulässig.[22] Das *Kammergericht* stellt hier ausdrücklich darauf ab, dass es nicht auf die urheberrechtliche Befugnis zur Weiterübertragung des Spiels ankommt, weil es bei der Anlage und Nutzung eines Accounts an einem Kauf fehle. Es kommt bei einem Steam-Nutzer-Account vielmehr auf die dort angebotenen Services an wie Achievements, die dort angezeigt werden. In der Praxis hat diese Rechtsprechung bislang nur den Account-Inhaber getroffen. Offen ist, ob auch Plattformen, die den Verkauf von Accounts organisieren, von den Games-Anbietern belangt werden können und ob hier der zivilrechtliche oder vielleicht sogar eher der strafrechtliche Weg erfolgversprechender wäre.

V. Ergebnis

Letztendlich kann festgehalten werden, dass beim Verkauf von Computerspielen die klassische Pirateriebekämpfung mit technischem Kopierschutz, Take-Down-Notices, Seitensperren und urheberrechtlichen Verfahren gegen Keyseller auch weiterhin eine wichtige Rolle spielt. Insbesondere die Seitensperren könnten sich als wirksames neues Instrument im Kampf gegen strukturell rechtswidrige Plattformen herausstellen.

Insgesamt lässt sich für die Pirateriebekämpfung feststellen, dass das Strafrecht meist nicht mehr das Mittel der Wahl ist. Außerdem nimmt die Refinanzierung über Verkäufe an Bedeutung ab, weil sich die Umsätze der Branche auf neue Säulen wie In-Game-Käufe und Onlinedienste verlagern, die mittlerweile zusammen mehr als zwei Drittel des Gesamtumsatzes mit Computer- und Videospielen ausmachen. Hier spielen das Urheberrecht und insbesondere das Strafrecht nur noch eine untergeordnete Rolle. Viel wichtiger werden das UWG und die AGB für vertragliche Ansprüche. Die Games-Branche und ihre neuen Geschäftsmodelle entfernen sich damit mehr und mehr von der klassischen Pirateriebekämpfung und müssen vielfach neue Wege in der Rechtsdurchsetzung gehen.

RA Prof. Dr. Christian-Henner Hentsch, M.A., LL.M.,
ist Leiter Recht und Regulierung beim game – Verband der deutschen Games-Branche e.V. und Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln sowie Mitherausgeber der MMR.

20 Abrufbar unter: https://www.game.de/umsatz-mit-online-diensten-fuer-gamer-hat-sich-innerhalb-eines-jahres-nahezu-verdoppelt/.
21 *KG* MMR 2016, 340; ähnl. *BGH* MMR 2010, 771 m. Anm. *Heydn* – Half-Life 2.
22 So auch *Rauda*, Recht der Computerspiele, 2013, Rdnr. 797; näher dazu auch https://spielerecht.de/kg-berlin-erneut-unuebertragbare-nutzeraccounts-bei-steam-sind-zulaessig/.

JULIAN WAIBLINGER / STANISLAUS JAWORSKI

Games-Piraterie – Website-Sperren als Mittel der Rechtsdurchsetzung

Effiziente Sperrmaßnahmen und Dringlichkeitsvermutung

Illegale Internetangebote

Piraterie im Internet stellt auch für die Games-Branche eine große Herausforderung dar. So existiert eine Vielzahl strukturell rechtswidriger Internetangebote, die illegal Computerspiele öffentlich zugänglich machen. Bei der Rechtsverfolgung sind Rechteinhaber in der Regel damit konfrontiert, dass die Betreiber solcher Piraterie-Websites nicht identifizierbar sind. Auch ein Vorgehen gegen die Dienstleister der Seiten ist in der Regel aussichtslos, da diese zumeist im Ausland sitzen und ohnehin von den Betreibern häufig ausgetauscht werden. Rechteinhabern bietet jedoch das Urheberrecht die Möglichkeit, gegen allgemeine Internetzugangsprovider auf Sperrung der strukturell rechtswidrigen Piraterie-Websites vorzugehen. Mit Blick auf die existierende Rechtsprechung untersucht der vorliegende Beitrag, auf welcher rechtlichen Grundlage Sperransprüche gegen allgemeine Internetzugangsprovider möglich sind und welche besonderen Herausforderungen zur erfolgreichen Geltendmachung solcher Ansprüche nach deutschem Urheberrecht bestehen. Lesedauer: 25 Minuten

I. Einleitung

Piraterie im Internet betrifft nicht nur die Film-, Musik- oder Verlagsbranche, sondern auch die Spieleindustrie. Das Angebot von Websites, die gezielt urheberrechtsverletzend Spiele öffentlich zugänglich machen, ist kaum überschaubar. Im Games-Bereich spielen dabei nach wie vor BitTorrent-Seiten eine große Rolle, bei denen Nutzer illegal Dateien austauschen.[1] Diese strukturell rechtswidrigen Seiten werden anonym betrieben. Die Host-Provider der Seiten liegen häufig im nicht-EU-Ausland; sie können bei Bedarf auch beliebig gewechselt werden (sog. Hosting-Nomadismus). Ein Vorgehen gegen die Betreiber der Seiten oder deren Host-Provider ist daher in der Regel aussichtslos.

Als letztes Mittel der Rechtsdurchsetzung verbleibt Rechteinhabern daher nur noch, allgemeine Internetzugangsprovider auf Sperrung der illegalen Seiten in Anspruch zu nehmen. Als mögliche Sperrmaßnahmen kommen insbesondere DNS-Sperren sowie IP-Sperren in Betracht. Während in Deutschland bereits einige wenige Entscheidungen zu Website-Sperren von Rechteinhabern im Film-, Musik- und Verlagsbereich ergangen sind, existiert bislang noch keine Entscheidung über die Sperrung eines rechtswidrigen Games-Portals. Doch auch für Rechteinhaber der Spielebranche bietet das geltende Urheberrecht die Möglichkeit der Website-Sperre gegen allgemeine Zugangsprovider, wie nachfolgend aufgezeigt wird.

II. Entwicklung der Rechtsprechung zu Website-Sperren

1. Art. 8 Abs. 3 Info-RL und EuGH: UPC Telekabel

Während Website-Sperren in anderen EU-Mitgliedstaaten schon seit Jahren zum Tagesgeschäft gehören – so etwa in Dänemark, Großbritannien, Irland oder Portugal –,[2] geraten Sperrverfahren gegen allgemeine Zugangsprovider erst in jüngerer Vergangenheit verstärkt in den Fokus der deutschen Rechtsprechung; dies, obwohl die Leitentscheidung des *EuGH* i.S. „UPC Telekabel"[3] bereits im Jahre 2014 den Grundstein für Website-Sperren gegen allgemeine Zugangsprovider gelegt hatte.

Der *EuGH* hatte Sperransprüche gegen Zugangsprovider, die nur neutral und passiv Zugang zum Internet gewähren, auf der Grundlage von Art. 8 Abs. 3 Info-RL[4] bejaht. Sperransprüche kommen danach in Abwägung der Grundrechte aller Beteiligten in Betracht, wenn Internetnutzern nicht unnötig die Möglichkeit vorenthalten wird, in rechtmäßiger Weise Zugang zu den verfügbaren Informationen zu erlangen; Sperren müssen ferner bewirken, dass unerlaubte Zugriffe auf die geschützten Werke verhindert oder zumindest erschwert werden und dass die Internetnutzer, die die Dienste des Adressaten der Anordnungen in Anspruch nehmen, zuverlässig davon abgehalten werden, auf die ihnen unter Verletzung des Rechts des geistigen Eigentums zugänglich gemachten Schutzgegenstände zuzugreifen.[5]

2. BGH: Störerhaftung des Access-Providers

Unter Verweis auf die europarechtlichen Vorgaben bestätigte auch der *BGH* im Nachgang in der Entscheidung „Störerhaftung des Access-Providers"[6], dass Zugangsprovider auf Website-Sperren in Anspruch genommen werden können. Art. 8 Abs. 3 Info-RL wurde durch den *BGH* also im Wege der Störerhaftung ins deutsche Recht umgesetzt. Auch wenn die konkrete Entscheidung auf den letzten Metern nicht zu Gunsten der Rechteinhaber ausfiel, war damit der Weg für Website-Sperrverfahren auch in Deutschland geebnet.

Allgemeine Zugangsprovider sollen nach der Entscheidung allerdings nur subsidiär haften. Rechteinhaber müssen danach zunächst erfolglos zumutbare Anstrengungen unternommen haben, gegen diejenigen Beteiligten vorzugehen, die die Rechtsverletzung selbst begangen oder zur Rechtsverletzung durch die Erbringung von Dienstleistungen beigetragen haben.[7] Der *BGH* nennt hier ausdrücklich die Betreiber der betreffenden Internet-

1 S. etwa die „Counterfeit and Piracy Watch List" der *EU-Kommission* v. 7.12.2018 mit anschaulichen Beispielen, abrufbar unter: http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf.

2 S. hierzu *J. B. Nordemann*, GRUR 2018, 1016 m.w.Nw. aus der europäischen Rspr.

3 *EuGH* MMR 2014, 397 m. Anm. *Roth* – UPC Telekabel/Constantin Film u.a. – kino.to.

4 RL 2001/29/EG des Europäischen Parlaments und des Rates v. 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (im Folgenden: „Info-RL"). Für andere Rechte des geistigen Eigentums können Sperransprüche auf Art. 11 Satz 3 RL 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums (im Folgenden: „Enforcement-RL") gestützt werden.

5 *EuGH* MMR 2014, 397 Rdnr. 42 ff. m. Anm. *Roth* – UPC Telekabel/Constantin Film u.a. – kino.to.

6 *BGH* MMR 2016, 180 m. Anm. *Finger* – Störerhaftung des Access-Providers.

7 *BGH* MMR 2016, 180 Rdnr. 83 ff. m. Anm. *Finger* – Störerhaftung des Access-Providers.

seite sowie deren Host-Provider; diese seien wesentlich näher an der Rechtsgutsverletzung als derjenige, der nur allgemein Zugang zum Internet vermittelt. Die Geltendmachung von Ansprüchen gegen Zugangsvermittler komme unter dem Gesichtspunkt der Verhältnismäßigkeit nur in Betracht, wenn der Inanspruchnahme des Betreibers der Webseite jede Erfolgsaussicht fehle und deshalb anderenfalls eine Rechtsschutzlücke entstünde.

Wie weit Rechteinhaber konkret gehen müssen, um diesem „Subsidiaritätserfordernis" genüge zu tun, lässt sich der Entscheidung nicht zweifelsfrei entnehmen. Im Hinblick auf das Vorgehen zur Ermittlung der Identität der Betreiber der betreffenden Website kommt nach dem *BGH* insbesondere die Einschaltung der staatlichen Ermittlungsbehörden im Wege der Strafanzeige oder alternativ die Vornahme privater Ermittlungen etwa durch einen Detektiv oder einen Dienstleister in Betracht.[8] Dabei wird man die Anforderungen an Rechteinhaber sicherlich nicht überspannen dürfen (zu den Anforderungen nach § 7 Abs. 4 TMG analog s.u.). Zivilrechtliche Vollstreckungsversuche im Ausland verbieten sich im Regelfall.[9]

3. TMG-Novelle 2017 und die Münchener Entscheidungen zu „Kinox.to"

Obwohl mit der TMG-Novelle 2017[10] vielfach die „Abschaffung der Störerhaftung" proklamiert wurde, erwirkte ein deutscher Filmrechteinhaber Anfang 2018 die erste Sperrverfügung gegen einen deutschen Internetzugangsprovider – auf Basis der Störerhaftung. So verurteilte das *LG München I* den Internetzugangsprovider *Vodafone* zur Sperrung der Website „Kinox.to", die urheberrechtswidrig tausende Spielfilme und TV-Serien öffentlich zugänglich macht.[11] Das *OLG München* bestätigte diese Entscheidung.[12]

Nach dem durch die TMG-Novelle 2017 eingeführten § 8 Abs. 1 Satz 2 TMG sind Ansprüche gegen alle Zugangsprovider ausgeschlossen; der Wortlaut der Vorschrift umfasst dabei nicht nur WLAN-Betreiber, sondern auch allgemeine Zugangsprovider. Mit § 7 Abs. 4 TMG wurde jedoch auch ein neuer Sperranspruch eingeführt, der sich nach seinem ausdrücklichen Wortlaut jedoch nur auf WLAN-Anbieter bezieht. Sperransprüche gegen allgemeine Zugangsprovider schienen angesichts dieser Gesetzeslage nicht mehr zu existieren. Das *LG München I* und das *OLG München* erkannten jedoch, dass ein Ausschluss von Sperransprüchen gegen allgemeine Zugangsprovider nicht mit dem Unionsrecht vereinbar ist. Unter ausführlicher Analyse der Gesetzgebungsmaterialen der TMG-Novelle 2017 kam das *OLG München* zu dem Ergebnis, dass § 8 Abs. 1 Satz 2 TMG teleologisch dahingehend zu reduzieren sei, dass sich die Bestimmung nur auf Zugangsprovider bezieht, die WLAN-Anbieter sind.[13] Ansprüche gegen allgemeine Zugangsprovider waren nach dieser Lesart nicht durch die TMG-Novelle 2017 ausgeschlossen. Sperransprüche konnten daher weiterhin auf Grundlage der Störerhaftung zuerkannt werden.

4. BGH: Dead Island – Sperransprüche nach § 7 Abs. 4 TMG analog

Mit der Entscheidung „Dead Island"[14] scheint der *BGH* auch für allgemeine Zugangsprovider die Abkehr von der Störerhaftung vollzogen zu haben. Der Fall betraf das Computerspiel „Dead Island", das über eine Internettauschbörse illegal zum Herunterladen angeboten wurde. Die Inhaberin der ausschließlichen Nutzungsrechte an „Dead Island" nahm den Betreiber mehrerer öffentlich zugänglicher WLAN-Hotspots sowie eines drahtgebundenen Zugangs zum Tor-Netzwerk (Tor-Exit-Nodes) in Anspruch.

Der *BGH* entschied, dass der Sperranspruch des neuen § 7 Abs. 4 TMG nicht nur gegen WLAN-Betreiber, sondern auch gegen Anbieter drahtgebundener Internetzugänge geltend gemacht werden kann. Der Ausschluss von Ansprüchen gem. § 8 Abs. 1 Satz 2 TMG gelte nicht nur zu Gunsten von WLAN-Betreibern, sondern für alle Zugangsprovider.[15] Da sich dies jedoch nicht mit den Vorgaben für Sperransprüche des Unionsrechts (Art. 8 Abs. 3 Info-RL und Art. 11 Satz 3 Enforcement-RL) vereinbaren lässt, sei der neue Sperranspruch nach § 7 Abs. 4 TMG richtlinienkonform so fortzubilden, dass er auch im Hinblick auf Zugangsvermittler, die den Zugang zum Internet nicht mittels WLAN, sondern auf andere Weise bereitstellen, Anwendung findet.[16]

Ansprüche gegen allgemeine Zugangsprovider auf Website-Sperren können daher seit *BGH* i.S. „Dead Island" auf § 7 Abs. 4 TMG analog gestützt werden. Eine aktuelle Entscheidung des *LG München I* bestätigt die Anwendung von § 7 Abs. 4 TMG analog als Anspruchsgrundlage (hierzu sogleich).[17] Die frühere Lösung der *Münchener Gerichte* über eine einschränkende Auslegung von § 8 Abs. 1 Satz 2 TMG wird damit in der Praxis wahrscheinlich keine Rolle mehr spielen, obwohl sie gegenüber der analogen Anwendung des § 7 Abs. 4 TMG vorzugswürdig war.[18] Im Folgenden soll skizziert werden, unter welchen Voraussetzungen nach § 7 Abs. 4 TMG analog Sperransprüche gegen allgemeine Zugangsprovider bestehen.

5. Aktuelle Entscheidung des LG München I zu „Goldesel.to"

In der o.g. aktuellen Entscheidung des *LG München I* hat das *LG* den Zugangsprovider *Deutsche Telekom* auf zur Sperrung des illegalen Portals „Goldesel.to" verurteilt, über das insbesondere Musiktitel illegal zugänglich gemacht werden. Es handelt sich bei diesem von der Musikindustrie geführten Verfahren um die erste instanzgerichtliche Entscheidung, die Sperransprüche gegen einen allgemeinen Zugangsprovider auf Grundlage von § 7 Abs. 4 TMG analog zuerkennt.[19]

III. Anspruchsvoraussetzungen des § 7 Abs. 4 TMG analog

1. Probleme bei der Inanspruchnahme eines Internetzugangsproviders von seinen Nutzern

§ 7 Abs. 4 Satz 1 TMG analog setzt zunächst voraus, dass ein Telemediendienst, also etwa ein Internetzugangsprovider, von einem Nutzer in Anspruch genommen wird, um das Recht am geistigen Eigentum eines anderen zu verletzen. Ein Internetzugangsprovider wird von seinen Nutzern in Anspruch genommen, wenn diese Piraterie-Websites aufsuchen, um dort urheberrechtlich geschützte Computerspiele herunterzuladen und damit unerlaubt zu vervielfältigen (§ 16 UrhG). Auf die Schranke der Privatkopie (§ 53 Abs. 1 UrhG) können sich die Nutzer von Piraterie-Websites nicht berufen.[20]

Zu kritisieren an diesem Tatbestandsmerkmal ist, dass es den Anwendungsbereich von Sperransprüchen nach seinem Wortlaut

8 *BGH* MMR 2016, 180 Rdnr. 87 m. Anm. *Finger* – Störerhaftung des Access-Providers.
9 *Leistner/Grisse*, GRUR 2015, 105, 107 f.; *J. B. Nordemann*, in: Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 97 Rdnr. 171a.
10 3. TMGÄndG v. 28.9.2017 (im Folgenden: „TMG-Novelle 2017").
11 *LG München I* MMR 2018, 322 m. Anm. *Sesing/Baumann*.
12 *OLG München* MMR 2018, 832 – Störerhaftung des Access-Providers bei Urheberrechtsverletzungen – Kinox.to.
13 *OLG München* MMR 2018, 832, Rdnr. 41 – Störerhaftung des Access-Providers bei Urheberrechtsverletzungen – Kinox.to.
14 *BGH* MMR 2018, 811 – Dead Island; s. hierzu *J. B. Nordemann*, GRUR 2018, 1016 sowie *Spindler*, GRUR 2018, 1012.
15 *BGH* MMR 2018, 811 Rdnr. 45 – Dead Island.
16 *BGH* MMR 2018, 811 Rdnr. 46 ff. – Dead Island.
17 *LG München I* MMR 2019, 535 m. Anm. *Müller*; zuvor bereits in diese Richtung gehend *LG München I*, U. v. 21.9.2018 – 21 O 11606/18; *OLG* München MMR 2019, 317 m. Anm. *Rehart* – mit mehreren Verweisen auf § 7 Abs. 4 TMG.
18 *J. B. Nordemann*, GRUR 2018, 1016, 1018.
19 *LG München I* MMR 2019, 535 m. Anm. *Müller*.
20 Vgl. *EuGH* MMR 2014, 679 Rdnr. 41 – ACI Adam/Stichting de Thuiskopie.

auf die Verletzung von Rechten des geistigen Eigentums begrenzt. Im Computerspielbereich ist dies wenig problematisch, da Computerspiele urheberrechtlich geschützt sind und daher deren illegaler Download eine Verletzung von Rechten am geistigen Eigentum darstellt. Grundsätzlich ist aber für eine erweiternde Auslegung von § 7 Abs. 4 Satz 1 TMG zu plädieren, da es ansonsten zu unerträglichen Wertungswidersprüchen kommt.[21] Denn nach dem bloßen Wortlaut der Norm hätten etwa Opfer von Gewalt- und Sexualverbrechen keinen Anspruch auf Sperrung von Websites, auf denen Videos der jeweiligen Straftaten abgerufen werden können.

2. Subsidiarität („keine andere Möglichkeit")

Wie bereits erwähnt, hatte der *BGH* in der Entscheidung „Störerhaftung des Access-Providers" ein Subsidiaritätskriterium für die Haftung allgemeiner Zugangsprovider aufgestellt.[22] Die TMG-Novelle 2017 hat dies übernommen: Gem. § 7 Abs. 4 Satz 1 TMG analog setzen Sperransprüche gegen Internetzugangsprovider voraus, dass dem Rechteinhaber keine andere Möglichkeit zusteht, der Rechtsverletzung abzuhelfen. Dieses Tatbestandsmerkmal muss mit Blick auf die Gesetzeshistorie sowie unionsrechtliche und verfassungsrechtliche Vorgaben gelesen werden.

Der Gesetzgeber hat deutlich zum Ausdruck gebracht, dass „keine andere Möglichkeit" wie das (vom *BGH* so nicht genannte) Subsidiaritätsmerkmal der Störerhaftung zu verstehen ist: „Der Rechteinhaber muss zunächst zumutbare Anstrengungen unternommen haben, gegen diejenigen Beteiligten vorzugehen, die – wie der Betreiber der Internetseite – die Rechtsverletzung selbst begangen haben oder – wie der Host-Provider – zur Rechtsverletzung durch die Erbringung von Dienstleistungen beigetragen haben. Nur wenn die Inanspruchnahme dieser Beteiligten scheitert oder ihr jede Erfolgsaussicht fehlt und deshalb andernfalls eine Rechtsschutzlücke entstünde, ist die Inanspruchnahme des Zugangsvermittlers zumutbar. Bei der Ermittlung der vorrangig in Anspruch zu nehmenden Beteiligten hat der Rechteinhaber in zumutbarem Umfang Nachforschungen anzustellen."[23]

Diese Begründung orientiert sich weitgehend wörtlich an den entsprechenden Ausführungen des *BGH* i.S. Störerhaftung des Access-Providers.[24] Es kommt damit auf „zumutbare Anstrengungen" an. Folglich ist das Tatbestandsmerkmal der „keine andere Möglichkeit" im Lichte der Verhältnismäßigkeit auszulegen. Hiervon ist der *BGH* in Bezug auf Sperransprüche nach der Störerhaftung bereits ausgegangen.[25]

Es wäre auch mit der Zielsetzung der RL 2001/29/EG (Urh-RL), insbesondere der effektiven Rechtsdurchsetzung und des Schutzes von Urheberrechten, nicht vereinbar, von Rechteinhabern zu fordern, dass diese zunächst jede noch so aussichtslose (kostspielige) Maßnahme zur Abstellung der Rechtsverletzung durchführen, bevor sie Sperransprüche gegen Internetzugangsprovider geltend machen können. Zudem lässt Erwägungsgrund 59 Info-RL erkennen, dass an die Haftungsvoraussetzungen von Internetzugangsvermittlern keine zu strengen Anforderungen gestellt werden dürfen, da „diese Vermittler selbst am besten in der Lage [sind], diesen Verstößen ein Ende zu setzen".

Schließlich ist fraglich, ob das Tatbestandsmerkmal „keine andere Möglichkeit, der Rechtsverletzung abzuhelfen" überhaupt mit Art. 8 Abs. 3 Info-RL vereinbar ist. Denn hierdurch wird in der Sache ein Subsidiaritätserfordernis aufgestellt, welche Sperransprüche verhindern kann. Damit wird gerade nicht nur eine Modalität (i.S.v. Erwägungsgrund 59 Info-RL) geregelt, sondern eine materielle Voraussetzung der Sperranordnung, die Sperranordnungen im Weg stehen kann.[26] Ob und in welcher Form ein Subsidiaritätserfordernis („keine andere Möglichkeit") in § 7 Abs. 4 Satz 1 TMG vorgesehen werden darf, sollte letztlich durch eine Vorlage gem. Art. 267 AEUV geklärt werden, weil andere Mitgliedstaaten eine andere Praxis zur Subsidiarität haben und teilweise ganz auf ein solches Erfordernis verzichten.[27]

Sofern man davon ausgeht, dass das Tatbestandsmerkmal „keine andere Möglichkeit" auch bei richtlinienkonformer Auslegung Bestand hat, ist es jedenfalls derart auszulegen, dass Rechteinhabern nur zumutbare Maßnahmen zur Unterbindung der Rechtsverletzung abverlangt werden.[28] I.E. bleiben daher die Grundsätze der *BGH*-Rechtsprechung zur Subsidiarität der Internetzugangsvermittlerhaftung[29] bestehen[30]. Die Zumutbarkeit der Inanspruchnahme von Betreibern und ihren Dienstleistern muss aus der Sicht eines objektiven Betrachters im Rahmen einer lebensnahen Einzelfallbetrachtung erfolgen, die allerdings typisieren kann.[31]

In der Regel sichern sich die Betreiber von Piraterie-Websites professionell gegen ihre Identifizierung und eine Abschaltung ihrer Dienste ab. Selbstverständlich halten sie kein Impressum vor, hinterlassen bei technischen Dienstleistern, wie etwa Host-Providern, keine korrekten Kontaktdaten, und kontrahieren vorzugsweise mit technischen Dienstleistern in Staaten, in denen nicht mit einer effektiven Durchsetzung von Urheberrechten gerechnet werden kann und die auch keinerlei Auskünfte erteilen. So finden sich etwa besonders viele Host-Provider von Piraterie-Websites in der Ukraine, in Moldawien und in Russland. Teilweise lassen die Betreiber solcher Websites die Nutzung ihrer Websites in den Staaten, in denen die Seiten gehostet werden, sperren, um sicherzugehen, dass sie nicht nach lokalem Urheberrecht in Anspruch genommen werden können. Schließlich werden regelmäßig Anonymisierungsdienste, wie etwa Cloudflare und Ddos-Guard, genutzt, die es z.T. schon unmöglich machen, die Host-Provider der jeweiligen Piraterie-Websites überhaupt zu identifizieren. Bei derart agierenden Kriminellen, die sich professionell gegen eine Identifizierung absichern, besteht von Vornhinein keine aussichtsreiche Möglichkeit, die Verletzung von Rechten abzustellen. Das Verlangen irgendwelcher Subsidiaritätsmaßnahmen ist in solchen Fällen unzumutbar. Jedenfalls sollte von Rechteinhabern nicht verlangt werden, dass sie gegen im Ausland sitzende Dienstleister vorgehen, die leicht austauschbar sind und zudem in der Vergangenheit häufiger gewechselt haben, wie dies bei Host-Providern von Piraterie-Websites in der Regel der Fall ist (Hosting-Nomadismus). Ein Vorgehen ist hier ohne Erfolgsaussicht und damit selbst bei strenger Auslegung des Subsidiaritätserfordernisses in § 7 Abs. 4 Satz 1 TMG analog nicht erforderlich.

Dies hat jüngst das *LG München I* in seiner Entscheidung zur Sperrung der Seite „Goldesel.to" bestätigt.[32]

Im Rahmen der Zumutbarkeit von Subsidiaritätsmaßnahmen ist noch zu berücksichtigen, dass diese in der Regel sinnlosen Be-

21 *Ohly*, JZ 2019, 251, 253; *Grisse*, GRUR 2017, 1073, 1079; dies andeutend auch *Spindler*, GRUR 2018, 1012, 1016.
22 *BGH* MMR 2016, 180 Rdnr. 83 ff. m. Anm. *Finger* – Störerhaftung des Access-Providers – wenngleich der *BGH* sich ausdrücklich weigert, den Begriff der Subsidiarität zu verwenden.
23 RegE, BT-Drs. 18/12202, S. 12.
24 *BGH* MMR 2016, 180 Rdnr. 82, 83 m. Anm. *Finger* – Störerhaftung des Access-Providers.
25 *BGH* MMR 2016, 180 Rdnr. 83 m. Anm. *Finger* – Störerhaftung des Access-Providers.
26 *J. B. Nordemann*, GRUR 2018, 1016, 1018.
27 Vgl. die Nw. bei *J. B. Nordemann*, GRUR 2018, 1016, 1018.
28 *Ohly*, JZ 2019, 251, 254.
29 *BGH* MMR 2016, 180 Rdnr. 83 m. Anm. *Finger* – Störerhaftung des Access-Providers; *BGH* MMR 2016, 188 Rdnr. 73 – Goldesel.to.
30 *Conrads/Peitinger*, GRUR-Prax 2017, 206, 207; *Sesing/Baumann*, MMR 2017, 583, 587; *J. B. Nordemann*, GRUR 2018, 1016, 1018; *ders*. (o. Fußn. 9), § 97 Rdnr. 171a, 172a.
31 *Leistner/Grisse*, GRUR 2015, 105, 107; *J. B. Nordemann* (o. Fußn. 9), § 97 Rdnr. 171a.
32 *LG München I* MMR 2019, 535 m. Anm. *Müller*.

mühungen der Rechteinhaber mit erheblichen Kosten verbunden sind. Es müssen technische Dienstleister/Ermittler und Rechtsanwälte beauftragt werden, um im ersten Schritt die Dienstleister der Betreiber der Piraterie-Seiten zu ermitteln und in einem zweiten Schritt per Notifizierungen und Abmahnungen gegen diese vorzugehen. Hierdurch könnte der Anspruch aus § 7 Abs. 4 TMG analog zu einem Recht verkommen, welches nur besonders wirtschaftsstarken Unternehmen zur Verfügung steht. Für Rechteinhaber von Werken, die nicht herausragend erfolgreich sind, wird sich ein Verfahren auf Grundlage von § 7 Abs. 4 TMG analog wirtschaftlich auf Grund der hohen Kosten, welche das Subsidiaritätserfordernis verursacht, nicht lohnen. Dies dürfte mit Art. 8 Abs. 3 Info-RL nicht vereinbar sein. Jedenfalls spricht das dafür, die Anforderungen an die Subsidiarität zu begrenzen.

Im Hinblick auf Websites mit illegalem Geschäftsmodell lassen sich insoweit sogar grundsätzlich „tatsächliche Vermutungen" begründen. Zum einen liegt es nach der Lebenserfahrung absolut nahe, dass die Betreiber solcher Websites regelmäßig Vorkehrungen getroffen haben, sich durch verschiedene Schutzmaßnahmen gegen eine Identifizierung abzusichern. Zum anderen ist es auch absolut lebensnah, dass ein Vorgehen gegen die Host-Provider solcher Websites regelmäßig sinnlos ist, weil sie von den Betreibern ausgewechselt werden, sobald sie von Rechteinhabern angegriffen werden.[33] Das Instrument der tatsächlichen Vermutung ist in der deutschen Rechtsprechung anerkannt[34] und müsste nun nur im Sinne der beiden vorgenannten Vermutungen umgesetzt werden; selbstverständlich einschließlich der für tatsächliche Vermutungen geltenden Regel, wonach sie dann nicht zur Anwendung kommen, wenn sie im Einzelfall durch besondere Umstände erschüttert sind.

3. Zumutbarkeit und Verhältnismäßigkeit der Sperrung

Der Anspruch nach § 7 Abs. 4 TMG analog setzt nach dessen Satz 2 voraus, dass die Sperrung zumutbar und verhältnismäßig ist.

a) Ausreichende Effizienz von DNS- und IP-Sperren

Gegen die Verhältnismäßigkeit und Zumutbarkeit von Website-Sperren wird regelmäßig vorgebracht, dass die gegebenen technischen Mittel, insbesondere DNS-Sperren und IP-Sperren nicht ausreichend effizient seien, um die Verpflichtung der Internetzugangsprovider zur Vornahme von Sperrmaßnahmen zu rechtfertigen. Dies überzeugt nicht, da es nach der Rechtsprechung des *BGH* schon ausreichend ist, dass unerlaubte Zugriffe auf die geschützten Werke „zumindest erschwert werden".[35] Es genügt etwa bei DNS-Sperren, dass die Internetnutzer, etwa nach illegal herunterladbaren Spielen Suchende, durch diese bei fehlender Abrufbarkeit der angesteuerten Domain in ihrem Unrechtsbewusstsein gestärkt werden und dadurch ihrer Bereitschaft, die Sperren zu umgehen, entgegengewirkt wird.[36]

b) Kosten von Sperrmaßnahmen

Die am häufigsten angewendeten und zugleich begehrtesten Sperrmaßnahmen, DNS-Sperren und IP-Sperren, sind nicht mit unverhältnismäßig hohen Kosten verbunden. Die Umsetzung wird bei Internetzugangsprovidern automatisiert möglich sein und verursacht Kosten im drei- bis vierstelligen Eurobereich.[37] Selbst behauptete Sperrkosten von € 150.000,– wurden vom *LG München I* als verhältnismäßig angesehen.[38] Zudem sind Internetzugangsprovider mit einer Infrastruktur, die DNS-Sperren erschwere, nicht schutzwürdig, da Internetzugangsprovider spätestens seit dem *BGH*-Urteil i.S. „Störerhaftung des Accessproviders" v. 26.11.2015 damit rechnen mussten, zur Einrichtung von DNS- und IP-Sperren verpflichtet zu werden.[39]

Nach der Rechtsprechung des *BGH* sollte eine Unverhältnismäßigkeit der Kosten ohnehin die Ausnahme bleiben. Er betont, dass der *EuGH* den Wesensgehalt des Rechts auf unternehmerische Freiheit durch eine Sperranordnung nicht tangiert sieht, wenn dem Diensteanbieter die Verpflichtung auferlegt wird, seine Ressourcen für eventuell kostenträchtige Maßnahmen einzusetzen, die beträchtliche Auswirkungen auf die Ausgestaltung seiner Tätigkeit haben oder schwierige und komplexe technische Lösungen erfordern.[40]

c) Berücksichtigung von Art. 5 Abs. 1 GG

Art. 5 Abs. 1 GG steht einer Sperrung von illegalen Websites nicht entgegen.[41] Das Recht auf Informationsfreiheit wird nicht schrankenlos gewährt und findet jedenfalls seine Grenzen, wenn das Aufrufen der Information klar Urheberrechte verletzt. In diesem Zusammenhang ist auch zu berücksichtigen, dass nicht-illegale Inhalte auf Piraterie-Websites, sofern es sie dort geben sollte, in geringerem Umfang schutzwürdig sind und der Sperrung einer Website nicht entgegenstehen, wenn es sich um eine eindeutig und gezielt auf die Verletzung von Urheberrechten ausgerichtete Website handelt. Der Aspekt des Overblocking ist daher nicht unter rein quantitativen Gesichtspunkten, sondern vielmehr vordergründig unter qualitativen Gesichtspunkten zu betrachten. Ansonsten hätten es die Betreiber von Piraterie-Websites durch die wahllose Einfügung von gemeinfreiem Content oder Schaffung von Nutzerforen auf ihren Websites in der Hand, Website-Sperren rechtlich unmöglich zu machen.

IV. Dringlichkeitsbeurteilung im Eilverfahren

Auch wenn es sich bei dem Sperranspruch gem. § 7 Abs. 4 TMG analog nicht mehr um einen Unterlassungsanspruch, sondern einen auf positive Leistung gerichteten Sperranspruch handelt, können Zugangsprovider nach wie vor im Rahmen des einstweiligen Verfügungsverfahrens in Anspruch genommen werden.[42]

Neue Herausforderungen für den einstweiligen Rechtsschutz in Sperrverfahren lauern jedoch an anderer Stelle: in den bereits erwähnten jüngsten Entscheidungen des *LG München I* und *OLG München*[43] verneinten die Gerichte das Bestehen des Verfügungsgrunds der Dringlichkeit, da die Rechteinhaber – hier: führende Wissenschaftsverlage – bereits länger als einen Monat von den strukturellen urheberrechtsverletzenden Seiten, deren Sperrung sie begehrten, Kenntnis hatten. Zwar hatten die Klägerinnen innerhalb eines Monats nach Kenntnis der konkreten Rechtsverletzung, d.h. der illegalen öffentlichen Zugänglichmachung (§ 19a UrhG) urheberrechtlich geschützter wissenschaftlicher Publikationen auf zwei notorisch bekannten Piraterie-Seiten, Antrag auf Erlass der einstweiligen Verfügung gestellt. Damit hatten sie also grundsätzlich innerhalb der von den *Münchener Gerichten* etablierten Dringlichkeitsfrist von einem Monat

33 So zum „Hosting-Nomadismus" i.R.d. Störerhaftung bereits *OLG München* MMR 2018, 832 Rdnr. 55 – Störerhaftung des Access-Providers bei Urheberrechtsverletzungen – Kinox.to.

34 Zur Rechtsnatur von tatsächlichen Vermutungen s. *BGH* NJW 2010, 363.

35 *BGH* MMR 2016, 180 Rdnr. 47 m. Anm. *Finger* – Störerhaftung des Access-Providers unter Verweis auf *EuGH* MMR 2014, 397 Rdnr. 62 f. m. Anm. *Roth* – UPC Telekabel/Constantin Film u.a. – kino.to.

36 *BGH* MMR 2016, 180 Rdnr. 48 m. Anm. *Finger* – Störerhaftung des Access-Providers; *LG München I* MMR 2019, 535 m. Anm. *Müller*.

37 *Landesgericht ZRS Wien*, U. v. 12.10.2017 – 47 R 281/17x.

38 *LG München I* MMR 2018, 322 m. Anm. *Sesing/Baumann*.

39 *LG München I* MMR 2018, 322 m. Anm. *Sesing/Baumann*.

40 *BGH* MMR 2016, 180 Rdnr. 38 m. Anm. *Finger* – Störerhaftung des Access-Providers unter Verweis auf *EuGH* MMR 2014, 397 Rdnr. 49 ff. m. Anm. *Roth* – UPC Telekabel/Constantin Film u.a. – kino.to.

41 *BGH* MMR 2016, 180 Rdnr. 53 ff. m. Anm. *Finger* – Störerhaftung des Access-Providers.

42 S. hierzu *J. B. Nordemann*, GRUR 2018, 1016, 1019.

43 *LG München I*, U. v. 21.9.2018 – 21 O 11606/18; *OLG* München MMR 2019, 317 m. Anm. *Rehart*.

gehandelt.[44] Allerdings hatten die Klägerinnen bereits länger als einen Monat Kenntnis von der Tatsache, dass auf den streitgegenständlichen Internetseiten ihre Rechte an anderen Werken verletzt wurden.

Das *OLG München* bestätigte die Entscheidung der Vorinstanz, wonach bei Sperransprüchen gegen Zugangsprovider die Dringlichkeit – anders als nach ständiger Rechtsprechung im Urheberrecht üblich – nicht werksbezogen, sondern seitenbezogen auszulegen sei.[45] Das *Gericht* begründet dies mit der Wirkung der begehrten Sperrmaßnahme: die begehrte Website-Sperre sei nicht auf ein bestimmtes Schutzrecht ausgerichtet, sondern darauf, dass den Internetnutzern der Zugang zu den Portalen insgesamt nicht mehr vermittelt wird und sie somit auf sämtliche Inhalte der Portale nicht mehr zugreifen können. Da sich also die begehrte Sperrmaßnahme nicht schutzrechtsbezogen auswirke, sei auch hinsichtlich der Frage der Dringlichkeit eine auf eine einzelne schutzrechtsbezogene Betrachtungsweise nicht angezeigt.[46] Nimmt ein Rechteinhaber einen Zugangsprovider auf Sperrung eines bestimmten Portals in Anspruch, weil über dieses Portal laufend Urheberrechtsverletzungen begangen werden, dann stellen die Verletzungen der Rechte an den verschiedenen Werken im Hinblick auf die begehrte Maßnahme der Sperrung nach Auffassung des *OLG München* zu den Portalen kerngleiche Verletzungen dar. Dies hat zur Folge, dass wenn der Antragsteller trotz Kenntnis der Möglichkeit, eine Sperrung zu bewirken, eine einzelne Verfügung nicht binnen eines Monats beantragt, zeigt, dass ihm die Angelegenheit nicht dringlich sei.[47] Nach Auffassung des *Gerichts* müssen Rechteinhaber, die Kenntnis von einer Rechtsverletzung und der betreffenden Website haben, dann gegen den Zugangsprovider vorgehen, wenn sie zudem davon Kenntnis haben, dass ein Vorgehen gegen den Betreiber der Website und dessen Host-Provider aussichtslos ist und sich auf dem Portal hauptsächlich rechtswidrige Inhalte befinden.[48]

Die Abkehr von der werksbezogenen Auslegung der Dringlichkeit überzeugt aus mehreren Gründen nicht. Zunächst gibt – anders als vom *OLG München* festgestellt – die Entscheidung des *BGH* zu „Dead Island" dieses Ergebnis nicht vor. Die vom *Gericht* in Bezug genommene Passage aus der Entscheidung[49] bezog sich auf die materiell-rechtliche Frage der Entstehung von Verhaltenspflichten im Rahmen der Störerhaftung, nicht hingegen auf eine prozessrechtliche Erwägung zur Auslegung der Dringlichkeit. Ferner ist zu berücksichtigen, dass auch der Wortlaut von § 7 Abs. 4 TMG eine werksbezogene Auslegung fordert, da er auf die Verletzung und die Verhinderung der Verletzung einzelner bestimmter Rechte abstellt. Der Umstand, dass bestimmte Sperrmaßnahmen, wie etwa die DNS-Sperre oder die IP-Sperre, aus technischen Gründen nicht auf ein einzelnes Werk bezogen sein können, sondern in der Regel eine gesamte Website erfassen, kann nicht dazu führen, dass zu Lasten der Rechteinhaber davon ausgegangen wird, dass § 7 Abs. 4 TMG kein werksbezogener Anspruch ist. Mit anderen Worten: eine technisch bedingte unbeabsichtigte Nebenfolge einer Sperrmaßnahme vermag nicht den rechtlichen Charakter einer werksbezogenen Norm zu ändern. Schließlich sprechen auch verfassungsrechtliche Argumente gegen die nicht-werksbezogene, d.h. seitenbezogene, Auslegung der Dringlichkeit. Sowohl Art. 14 GG als auch Art. 17 Abs. 2 GRCh verbürgen das Urheberrecht verfassungsrechtlich und gewähren ein verfassungsmäßiges Recht auf einen wirksamen Rechtsbehelf.[50] Das führt vor allem dann zu einer verfassungskonformen Auslegung, wenn ansonsten absolute Schutzlücken zu Lasten der Rechteinhaber entstehen. Der Rechteinhaber darf nicht faktisch schutzlos gestellt sein.

Bei konsequenter Anwendung der Auffassung des *OLG München* entstehen aber solche absoluten Schutzlücken. Wenn ein Rechteinhaber eine bestimmte Internetplattform kennt, die ihrem Wesen nach „gleichartige" Rechtsverletzungen ständig produziert, müsste gegen eine solche Website sofort innerhalb der Dringlichkeitsfrist nach Kenntnis und Abschluss der „Subsidiaritätsarbeit", d.h. dem erfolglosen Vorgehen gegen Betreiber oder Host-Provider, vorgegangen werden. Andernfalls ist kein einstweiliger Rechtsschutz mehr möglich und zwar auch nicht für neue Verletzungen, obwohl es sich dabei um einen eigenen Streitgegenstand und einen eigenen Kern handelt. Der Rechteinhaber kann dann nur noch im Hauptsacheverfahren vorgehen, was einen erheblichen Zeitverlust bedeutet. Während dieses Zeitraums ständig weiter produzierte Rechtsverletzungen müssten nach der nicht-werksbezogenen Auslegung des Dringlichkeitsgrunds vom Rechteinhaber toleriert werden. Vor diesem Hintergrund scheint es sachgerecht, auch bei Sperransprüchen gegen Zugangsprovider mit der bisherigen ständigen Rechtsprechung im Urheberrecht[51] die werksbezogene Auslegung des Verfügungsgrunds der Dringlichkeit beizubehalten.

V. Fazit

Content-Piraterie ist ein branchenübergreifendes Phänomen und macht auch vor Computerspielen nicht halt. Den Rechteinhabern stehen in der Regel aus tatsächlichen Gründen keine Möglichkeiten zu gegen die Betreiber von Piraterie-Websites vorzugehen, da es sich hier um professionelle Kriminelle handelt, die die technischen Möglichkeiten des Internets nutzen, um einer Identifizierung und Inanspruchnahme zu entgehen. Entsprechend wählen die Betreiber der Piraterie-Websites Dienstleister, wie etwa Host-Provider, aus, die ohnehin austauschbar sind und zumeist im Ausland sitzen.

Den Rechteinhabern bleibt hier keine andere Möglichkeit als gegen Internetzugangsprovider auf Sperrung der jeweiligen Piraterie-Websites vorzugehen. Seit der *BGH*-Entscheidung „Dead Island" kann dies auf Grundlage von § 7 Abs. 4 TMG analog erfolgen. § 7 Abs. 4 TMG analog ist dabei unionsrechtskonform derart auszulegen, dass entweder schon auf ein Subsidiaritätserfordernis („keine andere Möglichkeit, der Rechtsverletzung abzuhelfen") zu verzichten ist oder jedenfalls Rechteinhabern nur zumutbare Maßnahmen zur Unterbindung der Rechtsverletzung abverlangt werden. Dies sollte auf Grund der Werkbezogenheit des § 7 Abs. 4 TMG entgegen der neuerlichen Auffassung des *OLG München* auch gegen länger bekannte Piraterie-Websites im Eilverfahren möglich sein, sofern dort neue Computerspiele öffentlich zugänglich gemacht werden.

Dr. Julian Waiblinger
ist Rechtsanwalt und Fachanwalt für Urheber- und Medienrecht in Berlin.

Dr. Stanislaus Jaworski
ist Rechtsanwalt in Berlin.

44 Zur Dringlichkeitsfrist von einem Monat: *OLG* München MMR 2017, 114 – *Kein Vollgas*; *OLG* München GRUR-RR 2008, 310, 312.
45 *OLG* München MMR 2019, 317 m. Anm. *Rehart*.
46 *OLG* München MMR 2019, 317 m. Anm. *Rehart* unter Verweis auf *BGH* MMR 2018, 811 – Dead Island.
47 *OLG* München MMR 2019, 317 m. Anm. *Rehart*.
48 *OLG* München MMR 2019, 317 m. Anm. *Rehart*.
49 *BGH* MMR 2018, 811 – Dead Island.
50 *EuGH* GRUR 2017, 316, Rdnr. 25 – New Wave; *EuGH* MMR 2011, 596 Rdnr. 131 m. Anm. *Hoeren* – L'Oréal SA; *BGH* MMR 2011, 391 Rdnr. 20 – Any DVD.
51 S. etwa *OLG Köln* ZUM-RD 1998, 110; *OLG Hamburg* ZUM 2009, 575, 577 f.; *LG Hamburg* ZUM 2009, 582, 587 – Zattoo; *J. B. Nordemann* (o. Fußn. 9), § 97 UrhG Rdnr. 205.

THOMAS MERK / ADRIAN SCHNEIDER

Keyselling: Rechtliche Grenzen beim Handel mit Lizenzschlüsseln für Computerspiele

Anmerkungen aus praktischer und rechtlicher Sicht

Erschöpfungsgrundsatz

Der Verkauf von Lizenzschlüsseln für Computerspiele – das sog. Keyselling – ist nach wie vor ein lukrativer Markt. Neben legalen Vertriebsplattformen findet im Netz jedoch auch ein florierender Handel mit hochrabattierten Lizenzschlüsseln aus teilweise fragwürdigen Quellen statt. Literatur und Rechtsprechung haben sich dementsprechend in den vergangenen Jahren mehrfach mit den rechtlichen Grenzen des Keyselling befasst. Der nachfolgende Beitrag fasst die rechtliche Behandlung aus praktischer Sicht zusammen. Lesedauer: 22 Minuten

I. Was ist Keyselling?

Lizenzschlüssel (Keys) sind heutzutage das Kernstück des Vertriebs von PC-Spielen. Wer im Geschäft eine DVD mit einem Computerspiel erwirbt, erhält mit der DVD einen Schlüssel – ein kurzer Code aus Zahlen und Buchstaben, mit dem das Spiel aktiviert und regelmäßig auch bei Online-Vertriebsplattformen, wie z.B. Steam, Origin oder Uplay registriert werden muss.

Dabei hat der Key bei Weitem nicht nur die Funktion eines Kopierschutzes. Mit seiner Hilfe können Erwerber das Spiel auch jederzeit erneut von den jeweiligen Online-Vertriebsplattformen herunterladen, z.B. wenn der Datenträger beschädigt wird oder verloren geht. Dem Key kommt damit die Funktion eines Schlüssels im wörtlichen Sinne zu:[1] Er ermöglicht den eigentlichen Zugang zum Spiel – der Datenträger dient im Grunde nur noch dazu, lange Downloadzeiten zu vermeiden, ist für das Spielen des erworbenen Computerspiels jedoch nicht erforderlich. Bedeutsamer ist daher der Key, mit dem das Spiel registriert und heruntergeladen werden kann.

Dieser wird dementsprechend immer häufiger gleich ganz ohne dazugehörigen Datenträger verkauft – das sog. Keyselling. Erfolgt der Verkauf durch die Rechteinhaber oder ihre Vertriebspartner, ist das rechtlich unproblematisch.

Die rechtliche Diskussion beginnt, wo Keyseller Keys ohne oder sogar gegen den Willen der Rechteinhaber veräußern. Dabei erwerben Keyseller Keys aus verschiedensten Quellen zu einem möglichst günstigen Preis. Beispielsweise werden massenweise DVDs in Ländern mit niedriger Kaufkraft und entsprechend niedrigen Verbraucherpreisen erworben. Die in den DVD-Hüllen enthaltenen Keys werden sodann abfotografiert und digital weiterverkauft – zuzüglich der Marge des Keysellers, aber regelmäßig immer noch unter dem regulären Handelspreis in den Ländern mit hoher Kaufkraft. Bisweilen werden auch die Keys allein gänzlich digital bei günstigen Gelegenheiten erworben. So bietet z.B. die Onlineplattform „Humblebundle"[2] in Zusammenarbeit mit Spielepublishern bei besonderen Aktionen Keys zu einem selbst festzulegenden Preis an, der deutlich unter dem üblichen Verkaufspreis liegt und deren Erlös teilweise gemeinnützigen Projekten zu Gute kommt. Keyseller erwerben die Keys hier gleich in größeren Mengen besonders günstig und veräußern sie mit Gewinn weiter.

II. Rechtliche Bewertung

1. Urheberrecht

Wer ein Computerspiel erwirbt, erwirbt auch Nutzungsrechte. Da der Umfang der Nutzungsrechte beim Kauf selten konkret definiert wird, ergibt sich die Reichweite der eingeräumten Nutzungsrechte nach § 31 Abs. 5 UrhG aus dem zu Grunde liegenden Vertragszweck. Bei Spielen, die für Endverbraucher bestimmt sind, besteht der Vertragszweck darin, dem Spieler eine dauerhafte Nutzung des Spiels – also das Installieren und Spielen des Spiels – zu ermöglichen. Die eingeräumten Rechte werden daher das Recht zur Vervielfältigung auf dem vom Erwerber betriebenen Endgerät, also die Installation, sowie das Ablaufenlassen des Computerspiels, also das Spielen, umfassen. Ein Recht zur Verbreitung des Spiels ist vom Vertragszweck eines Verbraucherverkaufs jedoch regelmäßig gerade nicht umfasst. Insoweit schützt § 31 Abs. 5 UrhG auch die Rechteinhaber, indem eine restriktive Auslegung der konkludent eingeräumten Nutzungsrechte vorgeschrieben wird.

Für das (körperliche) Recht zur Verbreitung – also z.B. den Verkauf von Datenträgern – sieht das Urheberrecht allerdings ausdrücklich eine Ausnahme vor. Nach §§ 17 Abs. 2, 69c Nr. 3 Satz 2 UrhG kann der Rechteinhaber die Verbreitung eines Werks nicht untersagen, wenn es im Wege der Veräußerung innerhalb des Europäischen Wirtschaftsraums (EWR) in den Verkehr gelangt ist (sog. Erschöpfungsgrundsatz). Die Regelung schützt die Warenverkehrsfreiheit: Sachen sollen ohne urheberrechtliche Beschränkung im EWR frei gehandelt werden dürfen.

Dies kann auch Keys für Computerspiele betreffen, wenn sie in körperlicher Form vertrieben werden: Wird ein Key gemeinsam mit einem Datenträger (erstmalig) innerhalb des EWR im Wege des Verkaufs in den Verkehr gebracht, erschöpft sich insoweit das Verbreitungsrecht. Der Weiterverkauf des Datenträgers einschließlich des Key darf innerhalb des EWR vom Rechteinhaber nicht untersagt werden – auch dann, wenn er dem Ersterwerber kein Recht zur Verbreitung eingeräumt hat.

Die eigentliche Diskussion um Keyselling entfacht sich an der Frage, ob und inwieweit auch der unkörperliche Vertrieb von Keys Gegenstand des Erschöpfungsgrundsatzes ist.

a) Grundsätze der UsedSoft-Entscheidung

Den Ausgangspunkt der Diskussion um Keyselling bildet die UsedSoft-Entscheidung des *EuGH*.[3] Danach können Rechteinhaber auch die Verbreitung einer unkörperlich in den Verkehr gebrachten Kopie eines Computerprogramms i.S.v. § 69a Abs. 1 UrhG unter den folgenden Voraussetzungen nicht untersagen:[4]

1 So auch *OLG München* MMR 2017, 838.
2 S. https://www.humblebundle.com.
3 *EuGH* MMR 2012, 586 m. Anm. *Heydn* – UsedSoft.
4 *EuGH* MMR 2012, 586, 587 ff. m. Anm. *Heydn* – UsedSoft.

- Das Computerprogramm wurde mit dem Willen des Rechteinhabers innerhalb des EWR in den Verkehr gebracht.
- Das Computerprogramm wurde im Wege des Kaufs in den Verkehr gebracht, d.h. der Ersterwerber hat dauerhafte und nicht bloß vorübergehende Nutzungsrechte erhalten.
- Der Veräußerer weist nach, dass er über keine weitere Kopie des Computerprogramms verfügt und eventuelle Vervielfältigungen gelöscht hat.
- Der Rechteinhaber hatte die Möglichkeit, eine angemessene Vergütung für die Programmkopie zu erhalten.

Sind die vorgenannten Voraussetzungen kumulativ erfüllt, erschöpft sich das Verbreitungsrecht des Rechteinhabers. Der Erwerber der Software wird damit zum Berechtigten i.S.d. § 69d Abs. 1 UrhG, was es ihm ermöglicht, eine rechtmäßige Vervielfältigung durch den Download der Software aus dem Internet zur bestimmungsgemäßen Nutzung des Computerprogramms herzustellen. Die Übertragung einer beim Verkäufer bereits vorhandenen Kopie ist damit entbehrlich.[5]

Die Erschöpfung des Verbreitungsrechts wird also von einem etwaigen Substrat entkoppelt.[6] Gegenstand der Verbreitung ist vielmehr ein „virtuelles Exemplar" des Computerprogramms.[7] Ob ein materielles oder immaterielles Vervielfältigungsstück in den Verkehr gebracht wurde, spielt für die Erschöpfung des Verbreitungsrechts keine Rolle. Denn während die RL 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (InfoSoc-RL) in Erwägungsgrund 29 klarstellt, dass die Erschöpfung an den „materiellen Träger" des Werks geknüpft ist und daher bei Onlinediensten keine Rolle spielt, fehlt in der RL 2009/24/EG über den Rechtsschutz von Computerprogrammen (Computerprogramm-RL) eine solche Einschränkung. Diese Einschränkung hat auch nicht nur unverbindlichen Charakter. Sie ist vielmehr Ausdruck einer Auslegung, auf die sich die Unterzeichnerstaaten des WIPO Copyright Treaty (WTC) in einer Erklärung zu dem im WTC verankerten Erschöpfungsgrundsatz geeinigt haben.[8] Konsequenterweise hat der deutsche Gesetzgeber die Erschöpfung bei Werken, die der InfoSoc-RL unterfallen, auch im (körperlichen) Verbreitungsrecht in § 17 Abs. 2 UrhG umgesetzt.

Übertragbarkeit auf Computerspiele

Grundlegend stellt sich daher die Frage, ob die Ausführungen des *EuGH* in der UsedSoft-Entscheidung auf Computerspiele Anwendung finden. Computerspiele sind nach ganz h.M. jedenfalls als Filmwerke urheberrechtlich schutzfähig.[9] Bei Computerspielen handelt es sich um komplexe künstlerische Gestaltungen von Bewegtbildern. Dass der Spieler interaktiv an diesen Filmwerken teilnehmen und Handlung und Ablauf mit beeinflussen kann, steht einem Schutz von Computerspielen als Filmwerke nicht entgegen.[10] Gleichzeitig werden Computerspiele aber auch von Computerprogrammen gesteuert. Es sind daher „hybride Werke".[11]

Sowohl nach Ansicht des *BGH*[12] als auch des *EuGH*[13] darf der Schutzbereich eines hybriden Werks nicht deshalb verkleinert werden, weil dieses gleich unter mehreren urheberrechtlichen Gesichtspunkten schutzfähig ist. Andernfalls würde der Urheber eines besonders komplexen Werks, das unter mehreren Aspekten schutzfähig ist, schlechter gestellt als der Urheber eines weniger komplexen und nur unter einem Einzelaspekt schutzfähigen Werks.

Diesem Gedanken widerspräche es jedoch, würde man die UsedSoft-Entscheidung des *EuGH* undifferenziert auf Computerspiele anwenden: Würde es sich bei Computerspielen allein um Werke nach der InfoSoc-RL handeln, käme eine Erschöpfung des Verbreitungsrechts bei einem rein unkörperlichen Vertrieb nicht in Betracht.[14] Der Rechteinhaber eines Werks nach der InfoSoc-RL ist insoweit besser gestellt, als der Rechteinhaber eines Computerprogramms.

Der Umstand, dass Computerprogramme sowohl nach der InfoSoc-RL als auch nach der Computerprogramm-RL geschützt sind – das Recht sie also gleich in mehrfacher Hinsicht als schutzfähig anerkennt – darf dementsprechend nicht dazu führen, dass der Rechteinhaber durch den erweiterten Schutz schlechter gestellt wird. Würde man die Grundsätze der UsedSoft-Entscheidung auch auf Computerspiele anwenden, träte aber genau dieser Effekt ein: Allein der Umstand, dass Computerspiele als hybride Werke einem zusätzlichen Schutz der Computerprogramm-RL unterfallen, würde dazu führen, dass eine Erschöpfung des Verbreitungsrechts auch beim unkörperlichen Vertrieb eintreten kann. Die vom Gesetzgeber anerkannte erweiterte Schutzfähigkeit als Werk, das mehreren Schutzkategorien unterfällt, würde also zu einer faktischen Verkürzung des Schutzes führen.

Insofern bestehen bereits erhebliche Zweifel daran, dass die Grundsätze des UsedSoft-Urteils auf Computerspiele übertragbar sind.[15]

Keine Erschöpfung bei nicht aktivierten Keys

Eine weitere Besonderheit besteht bei rein digital vertriebenen Keys – also solche, die nicht zusammen mit einem physischen Datenträger, sondern gänzlich digital verkauft werden. Denn in diesem Fall dient die Übertragung von Keys nicht der unkörperlichen Weitergabe eines bereits existierenden Vervielfältigungsstücks, sondern vielmehr dessen erstmaliger Herstellung. Insofern besteht im Vergleich zum Fall der „Gebrauchtsoftware", der auch der UsedSoft-Entscheidung des *EuGH* zu Grunde lag, ein weiterer wesentlicher Unterschied. So nahmen auch das *OLG Frankfurt/M.* sowie das *OLG München* an, dass die Regelungen zur Erschöpfung und damit auch die Grundsätze der UsedSoft-Entscheidung im Falle des Weiterverkaufs digital erworbener, nicht aktivierter Keys schon gar nicht anwendbar sind.[16]

Keine Aufspaltung von Lizenzschlüssel und Datenträger

Auch bei solchen Keys, die gemeinsam mit einem physischen Datenträger vertrieben werden, besteht eine wesentliche Besonderheit im Vergleich zur UsedSoft-Rechtsprechung. Nach Ansicht des *LG Berlin* könne Erschöpfung von vornherein nur an dem Produkt eintreten, das mit Zustimmung des Berechtigten innerhalb des EWR in den Verkehr gelangt ist.[17] Das Aufspalten von Lizenzen – also etwa der getrennte Vertrieb von Lizenzschlüsseln von einem ursprünglich in den Verkehr gebrachten Datenträger – komme daher von vorneherein nicht in Betracht.

---

5 *EuGH* MMR 2012, 586, 590 m. Anm. *Heydn* – UsedSoft.
6 *Hilgert*, CR 2014, 354, 357.
7 *Redeker*, CR 2014, 73, 75.
8 *Krüger/Biehler/Apel*, MMR 2013, 760, 764.
9 *Bullinger*, in: Wandtke/Bullinger, Urheberrecht, 4. Aufl. 2014, § 2 Rdnr. 129; *Redeker*, IT-Recht, 6. Aufl. 2017, Kap. A Rdnr. 118; *Kaboth/Spies*, in: BeckOK Urheberrecht, Stand: 15.4.2019, § 69a Rdnr. 8; *Picot*, in: Auer-Reinsdorff/Conrad, Hdb. IT- und Datenschutzrecht, 2. Aufl. 2016, § 29 Rdnr. 4.
10 *Schricker/Loewenheim*, Urheberrecht, 4. Aufl. 2017, § 2 Rdnr. 217 m.w.Nw.
11 *Kreutzer*, CR 2007, 1, 2.
12 *BGH* MMR 2013, 671 m. Anm. *Roth* – Videospiel-Konsolen, Rdnr. 24.
13 *EuGH* MMR 2014, 401 m. Anm. *Oehler*, Rdnr. 23.
14 *Apel*, ZUM 2015, 640 m.w.Nw.*; OLG Hamm* GRUR 2014, 853, 859 f. – Hörbuch-AGB in Bezug auf den Vertrieb von Hörbüchern.
15 So auch *LG Berlin* MMR 2014, 838; *Krüger/Biehler/Apel*, MMR 2013, 760; *Wolff*, ITRB 2014, 155; *Hilgert*, CR 2014, 354, 356; *Lober/Klein/Groothuis*, Interactive Entertainment Law Review 2018, p. 44, 48 f.; in Bezug auf die Übertragbarkeit auf Hörbücher *OLG Hamm* GRUR 2014, 853, 859 f.; in Bezug auf die Übertragbarkeit auf andere Werkarten generell auch *Apel*, ZUM 2015, 640 m.w.Nw.
16 *OLG Frankfurt/M.* MMR 2016, 819; *OLG München* MMR 2017, 838, 840.
17 *LG Berlin* MMR 2014, 838.

Für Computerprogramme hat dies allerdings der *BGH* anders beurteilt: Demnach komme es für den Eintritt der Erschöpfung nicht darauf an, ob ein Lizenzschlüssel für eine Software durch Übergabe des Datenträgers oder durch bloße Bekanntgabe des Lizenzschlüssels erfolge.[18]

b) Keine Erfüllung der Tatbestandsmerkmale für Eintritt der Erschöpfung nach der UsedSoft-Entscheidung

Selbst wenn man entgegen der o.g. Zweifel die Grundsätze der UsedSoft-Entscheidung auch auf Computerspiele übertragen wollte, werden die vom *EuGH* aufgestellten Voraussetzungen für den Eintritt der Erschöpfung in der Praxis regelmäßig nicht erfüllt. Dabei ist insbesondere zu berücksichtigen, dass Keyseller, die sich auf den Eintritt der Erschöpfung als urheberrechtliche Ausnahme berufen, in aller Regel für das Vorliegen der Tatbestandsmerkmale beweisbelastet sind.[19]

■ Inverkehrbringen innerhalb des EWR

Bereits der Ort des Inverkehrbringens stellt in der Praxis regelmäßig eine erhebliche Hürde dar. Einerseits aus tatsächlichen Gründen: Keys, die außerhalb des EWR in den Verkehr gebracht wurden, sind häufig besonders günstig und daher wirtschaftlich für Keyseller sehr attraktiv. Nicht selten werden daher Keys veräußert, die z.B. auf dem russischen Markt in den Verkehr gebracht wurden. In diesem Fall tritt die Erschöpfung bereits aus tatsächlichen Gründen nicht ein, weil die Keys nicht innerhalb des EWR in den Verkehr gebracht wurden und daher die Voraussetzungen für den Eintritt der Erschöpfung tatsächlich nicht erfüllt sind.

Andererseits ist es in der Praxis nur schwer bzw. gar nicht zu bewerkstelligen, die Herkunft eines Keys gerichtsfest zu dokumentieren. Regelmäßig erfolgen Beschaffung und Vertrieb von Keys arbeitsteilig – Keyseller können diese in großen Mengen auf spezialisierten Onlinemarktplätzen, oft für die beteiligten Käufer und Verkäufer anonym, erwerben. Eine saubere Herkunftsdokumentation ist hierbei in den seltensten Fällen gewährleistet, sodass praktisch der Beweis für das Inverkehrbringen der Keys innerhalb des EWR oftmals nicht gelingt.

■ Vollständige Bezahlung des Ersterwerbs

Voraussetzung für den Eintritt der Erschöpfung ist zudem, dass es dem Rechteinhaber ermöglicht wurde, eine dem wirtschaftlichen Wert der Kopie des ihm gehörenden Werks entsprechende Vergütung zu erzielen.[20] Zwar kommt es nach Ansicht des *BGH* nicht zwingend darauf an, dass der Rechteinhaber auch tatsächlich eine angemessene Vergütung erhalten hat – er muss lediglich die Möglichkeit hierfür erhalten haben.[21] Entscheidet sich ein Rechteinhaber z.B. dazu, Lizenzen zu einem sehr günstigen Preis zu vergeben oder gar sein Computerprogramm oder Teile hiervon kostenlos zur Verfügung zu stellen, steht dies dem Eintritt der Erschöpfung nicht entgegen.[22] Die Möglichkeit, eine angemessene Vergütung zu erhalten, muss dem Rechteinhaber jedoch gewährt werden.

In der Praxis ist es keine Seltenheit, dass Keys auch für Geldwäschezwecke missbraucht und mit gestohlenen Kreditkarten zum Zweck des Weiterverkaufs erworben werden.[23] In diesem Fall lässt sich schon daran zweifeln, ob ein betrügerisch erworbener Key überhaupt willentlich vom Rechteinhaber in den Verkehr gebracht wurde. Jedenfalls wurde der Rechteinhaber durch den Betrug der Möglichkeit beraubt, seine Investition in die Erstellung des Computerprogramms durch eine angemessene Vergütung zu kompensieren, wenn der Kaufpreis nicht etwa auf Grund einer Zahlungsgarantie des Kreditinstituts beglichen wird.

Der Nachweis darüber, dass ein veräußerter Key tatsächlich auch vom Ersterwerber bezahlt wurde, ist daher im Fall des Keyselling von besonderer Bedeutung. Angesichts der bereits o.g. Dokumentationslücken in der Praxis, lässt sich für Keyseller aber regelmäßig eher nicht nachweisen, ob ein Key von seinem Ersterwerber – den der letztendliche Veräußerer der Keys an Endverbraucher häufig noch nicht einmal namentlich kennt – tatsächlich bezahlt wurde.

2. Lauterkeitsrecht

Auch Verstöße gegen das Lauterkeitsrecht durch Keyseller kommen regelmäßig in Betracht. Dies vor allem deswegen, weil das Lauterkeitsrecht Keysellern umfangreiche Informationspflichten auferlegt, bei deren Nichteinhaltung ein Verstoß droht.

Das *OLG Hamburg*[24] hatte etwa hinsichtlich des Verkaufs von Keys für Computerprogramme entschieden, dass der Keyseller dem Käufer mitzuteilen hat, ob und an wen der jeweilige Key vom Rechteinhaber ausgegeben worden und ob eine Erschöpfung des entsprechenden Verbreitungsrechts eingetreten ist. Auch sei über die Art der eingeräumten Lizenz zu informieren sowie ob die Programmkopie vom Erst- oder Zwischenerwerber vernichtet wurde. Diese Informationspflichten sind teilweise stark an die vom *EuGH* in der UsedSoft-Entscheidung aufgestellten Kriterien angelehnt. Wendet man die UsedSoft-Entscheidung also auch auf Computerspiele an, müssen die vom *EuGH* aufgestellten Kriterien nicht nur tatsächlich erfüllt und vom Keyseller bewiesen werden – der Kunde muss hierüber auch informiert werden. In der Praxis ist dies in aller Regel nicht zu beobachten.

Darüber hinaus stellt es ein wesentliches Merkmal der Ware i.S.d. § 5 Abs. 1 Nr. 1 UWG dar, wenn der Erwerber im Verhältnis zum Rechteinhaber nicht berechtigt wird, ein Computerprogramm herunterzuladen oder zu nutzen.[25] Erhält der Erwerber beim Kauf eines Key also tatsächlich keine Zugangsberechtigung, handelt der Keyseller nicht nur urheberrechtswidrig, sondern auch unlauter.

3. Strafrecht

Neben einer urheber- und lauterkeitsrechtlichen hat Keyselling in jüngster Zeit auch zunehmend eine strafrechtliche Dimension erhalten. Da Keyseller in aller Regel gewerbsmäßig handeln, ist der unautorisierte Verkauf von Keys nach §§ 106 Abs. 1, 108a Abs. 1 UrhG strafbar, wenn keine Erschöpfung eingetreten ist. Darüber hinaus liegt regelmäßig ein gewerbsmäßiger Betrug zu Lasten der Kunden gem. § 263 Abs. 1, 3 Nr. 1 StGB vor, da diese darüber getäuscht werden, gegen Zahlung des Entgelts ein urheberrechtliches Nutzungsrecht zu erhalten, der Keyseller hierüber aber nicht zu verfügen berechtigt ist.

So verurteilte das *AG Gießen* den Onlineverkäufer von Lizenzschlüsseln für diverse *Microsoft*-Programme auf eben dieser Grundlage zu einer 18-monatigen Freiheitsstrafe auf Bewährung.[26] Zuletzt hat auch der *BGH* eine Verurteilung zweier Keyseller bestätigt, die offenbar aus China stammende Softwarekeys im Internet verkauft hatten.[27]

---

18 *BGH* MMR 2015, 735 – Green-IT.
19 *BGH* MMR 2014, 232, 238 m. Anm. *Heydn* – UsesSoft II.
20 *EuGH* MMR 2012, 586, 589 m. Anm. *Heydn* – UsedSoft, Rdnr. 72.
21 *BGH* MMR 2014, 232, 238 m. Anm. *Heydn* – UsedSoft II.
22 *BGH* MMR 2015, 530 – UsedSoft III.
23 Vgl. beispielhaft die Berichte zu Kreditkartenbetrug im Zusammenhang mit Keyselling, abrufbar unter: https://kotaku.com/g2a-scammer-explains-how-he-profited-off-stolen-indie-g-1784540664 sowie https://www.eurogamer.net/articles/2015-01-28-deactivated-ubisoft-game-keys-bought-from-eas-origin-using-stolen-credit-cards.
24 *OLG Hamburg* MMR 2017, 344.
25 *OLG Frankfurt/M.* MMR 2017, 263.
26 *AG Gießen* MMR 2016, 696 m. Anm. *Rosemann* = GRUR-Prax 2016, 415 m. Anm. *Hansen*.
27 *BGH* MMR 2019, 444.

4. Haftung von Keyselling-Marktplätzen

In den vergangenen Jahren hat sich im Bereich des Keyselling ein Trend abgezeichnet. Während Keys ursprünglich direkt von großen Keyselling-Shops an Kunden vertrieben wurden, haben viele Anbieter mittlerweile ihr Geschäftsmodell zu Marktplatzmodellen weiterentwickelt: Anstatt Keys direkt an Endkunden zu vertreiben, bieten sie nunmehr eine Vermittlungsplattform zwischen anonymen Verkäufern von Keys und Kunden. Dementsprechend argumentieren die Betreiber der Keyselling-Marktplätze zunehmend, selbst für die Zulässigkeit der über ihre Marktplätze vertriebenen Keys nicht verantwortlich zu sein, sondern lediglich als Host-Provider i.S.v. § 10 TMG zu agieren und demnach erst ab Kenntnis der Rechtswidrigkeit zum Handeln verpflichtet zu sein.

Von § 10 TMG profitieren jedoch nur solche Anbieter von Telemedien, die lediglich fremde Informationen speichern.[28] Ob es sich bei den auf den Keyselling-Marktplätzen angebotenen Keys tatsächlich um fremde Informationen handelt, lässt sich von außen kaum beurteilen: Die Verkäufer treten in aller Regel anonym auf, ein Impressum oder auch nur Kontaktmöglichkeiten zu den Verkäufern sind in aller Regel nicht vorhanden. Bei einigen Keyselling-Marktplätzen ist auf den einzelnen Produktseiten zudem überhaupt nicht zu erkennen, dass ein Verkauf durch Dritte und nicht den Anbieter selbst erfolgt – allenfalls im Laufe des weiteren Kaufprozesses erscheint an unauffälliger Stelle ein Verweis auf ein Pseudonym eines angeblichen Verkäufers.

Rechtlich ist hier zu berücksichtigen, dass eine Haftung für die Speicherung von fremden Informationen nach § 10 TMG auch dann in Betracht kommt, wenn sich der Telemedienanbieter diese Informationen zu Eigen gemacht hat.[29] Zu-eigen-gemachte Informationen werden wie eigene Informationen behandelt und liegen vor, wenn fremde Information derart in das eigene Angebot integriert werden, dass für den objektiven Erklärungsempfänger der Eindruck entsteht, es handle sich um Informationen des Anbieters selbst.[30]

Für die angesprochenen Besucher des Telemediendienstes muss es danach also erkennbar sein, dass nicht der Website-Betreiber die Keys verkauft, sondern etwaige Verkäufer. Dabei kommt es nicht darauf an, ob an irgendeiner – ggf. sogar nur versteckten – Stelle ein Hinweis darauf erfolgt, dass es sich um fremde Informationen handelt. Vielmehr muss sich der Inhalt im Wege einer Gesamtbetrachtung so darstellen, dass für einen objektiven Betrachter eine ernsthafte und genügende Distanzierung von den Drittinhalten erfolgt.[31]

An einer solchen Distanzierung wird es dann fehlen, wenn der Vertrieb von Keys gerade der Zweck solcher Marktplätze darstellt, der Betreiber keine Maßnahmen ergreift, um die typischen Risiken bei einem solchen Vertrieb einzuschränken – z.B. durch verpflichtende und detaillierte Dokumentation der Herkunft der Keys – und obendrein den Verkäufern von potenziell rechtsverletzenden Keys durch Gewährung von Anonymität Schutz vor Verfolgung gewährt.

Zwar stellt die Gewährung einer pseudonymen Nutzung eines Telemediendienstes nicht per se ein Zu-Eigen-Machen von Drittinhalten dar.[32] Allerdings müssen Diensteanbieter, die von Nutzern bereitgestellte Informationen speichern, die nach vernünftigem Ermessen von ihnen zu erwartende und in innerstaatlichen Rechtsvorschriften niedergelegte Sorgfaltspflicht anwenden, um bestimmte Arten rechtswidriger Tätigkeiten aufzudecken und zu verhindern.[33] Eine Anonymität im gewerblichen Geschäftsverkehr sieht die Rechtsordnung jedoch gerade nicht vor. So schreibt § 5 Abs. 1 TMG eine Offenlegung der Identität von Anbietern von Telemedien vor. Dies gilt auch für Verkäufer auf Onlinemarktplätzen.[34] Auch die essentialia negotii sehen als eine Mindestvoraussetzung für einen wirksamen Vertrag eine Einigung über die Parteien vor. Dies wird nicht erfüllt sein, wenn für den Käufer eines Keys nicht erkennbar ist, von wem er diesen erwirbt und ob sein angeblicher Verkäufer überhaupt existiert. Die fehlende Erkennbarkeit des Händlers führt vielmehr dazu, dass der Marktplatzbetreiber aus Sicht der Kunden in den Vordergrund tritt, anstatt sich von den fremden Inhalten zu distanzieren.[35] Die Offenlegung der Identität des Verkäufers im Rahmen der gesetzlichen Anforderungen wird somit auch von den Betreibern von Keyselling-Marktplätzen verlangt werden können.

III. Rechtsdurchsetzung in der Praxis

In der Praxis stellt die Rechtsdurchsetzung gegen unzulässiges Keyselling eine Herausforderung dar. Den o.g. rechtlichen Bedenken gegen das unautorisierte Keyselling sind viele Anbieter dadurch begegnet, dass sie ihren Sitz ins außereuropäische Ausland verlagert haben. Das macht die Rechtsdurchsetzung mühsam, aber keineswegs unmöglich.

Denn in vielen Fällen mögen die Anbieter zwar ihren Sitz verlegt haben. Der tatsächliche Geschäftsbetrieb erfolgt regelmäßig jedoch noch zu großen Teilen innerhalb der EU. Auch Vermögenswerte sind in der Regel in der EU vorhanden, z.B. Marken, Domains oder Verrechnungskonten bei Banken und Zahlungsdienstleistern. Dies ermöglicht die Vollstreckung in Vermögenswerte innerhalb der europäischen Rechtsordnung.

Die initiale Zustellung zivilprozessualer Dokumente, wie etwa der Klageschrift ins außereuropäische Ausland hat vorrangig nach § 183 Abs. 2 Satz 1 ZPO auf Grundlage der jeweiligen völkerrechtlichen Abkommen von Amts wegen zu erfolgen. Insbesondere wenn die Auslandszustellung nach § 183 ZPO in das jeweilige Land erfahrungsgemäß schwierig ist, kann das Gericht jedoch nach § 184 Abs. 1 Satz 1 ZPO anordnen, dass die im Ausland gelegene Partei innerhalb angemessener Frist (in der Regel zwei bis sechs Wochen ab Zustellung)[36] einen Zustellungsbevollmächtigten im Inland benennt, an den die künftige Zustellung erfolgen kann.[37] Geschieht dies nicht, kann das Gericht spätere Zustellungen nach § 184 Abs. 1 Satz 2 ZPO durch einfache Post bewirken.

Nimmt das gerichtliche Verfahren einen erfolgreichen Abschluss, stellt sich die Frage nach Möglichkeit und Voraussetzungen einer Vollstreckung. Eine Vollstreckung im außereuropäischen Ausland richtet sich oftmals nach zwischenstaatlichen Abkommen, die unterschiedlichste Regelungen enthalten.[38] Da der Geschäftsbetrieb der Keyseller jedoch nicht selten zu großen Teilen innerhalb der EU erfolgt und sich daher entsprechende Vermögenswerte wie Marken, Domains oder Verrechnungskonten bei Banken und Zahlungsdienstleistern in diesem Raum befinden, ist die Vollstreckung innerhalb der europäischen Rechts-

28 *Hoffmann*, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, TMG § 10 Rdnr. 16.
29 *BGH* MMR 2017, 526 m. Anm. *Becker* – klinikbewertungen.de; *Paal*, in: BeckOK InfoMedienR, Stand: 1.2.2019, § 7 Rdnr. 31 m.w.Nw.
30 *Paal* (o. Fußn. 29), § 7 Rdnr. 31.
31 *BGH* MMR 2010, 556, 557 – marions-kochbuch.de.
32 *Hoffmann* (o. Fußn. 28), § 7 Rdnr. 22.
33 *BGH* MMR 2013, 185, 186 m. Anm. *Hoeren* – Alone in the Dark.
34 Vgl. nur *OLG Hamburg* MMR 2010, 29; *OLG Düsseldorf* MMR 2013, 649.
35 *LG Köln* ZUM 2001, 716, 718.
36 Vgl. etwa *OLG Hamm* NJW-RR 2012, 62, 64, Unterfrist von zwei Wochen für eine Zustellung in die Türkei; *BGH* NJW 2013, 387, 390 m. Anm. *Schäfer*, vier Wochen für eine Zustellung nach China.
37 *Roth*, in: Stein/Jonas, ZPO, 23. Aufl. 2016, § 184 Rdnr. 5.
38 *Haag*, in: Geigel, Haftpflichtprozess, 27. Aufl. 2015, 43. Kap. Rdnr. 27.

ordnung durchaus praktikabel. Ein Sitz außerhalb der EU bietet somit nur begrenzten Schutz vor inländischen gerichtlichen Maßnahmen.

Auch die vermehrten strafrechtlichen Maßnahmen zeigen, dass Rechteinhaber unzulässigem Keyselling gegenüber nicht unbedingt schutzlos gestellt sind. Für die strafrechtlichen Ermittlungen spielt der formelle Unternehmenssitz der Anbieter ebenso keine Rolle. Maßgeblich ist vielmehr, wo der tatsächliche Geschäftsbetrieb erfolgt – schon weil sich die Ermittlungen nicht gegen das Unternehmen, sondern die handelnden Personen richten. Insofern bietet eine bloße Sitzverlegung vor strafrechtlichen Ermittlungen in der Praxis nur bedingten Schutz.

IV. Fazit

Als hochtechnische und zugleich kreative Werke ergeben sich für Computerspiele im urheberrechtlichen Geflecht der verschiedenen Schutzrechte zahlreiche Besonderheiten, die für die ohnehin bereits sehr komplexen Rechtsfragen rund um den digitalen Vertrieb von Keys eine weitere Komplikation bedeuten.

Dabei bestehen erhebliche Zweifel, ob sich die allgemeinen Grundsätze, die für den Vertrieb von Computerprogrammen entwickelt wurden, auch auf hybride Werke wie Computerspiele ohne weiteres übertragen lassen. Jedenfalls zeigt sich in der Praxis, dass die hohen Hürden, die die Rechtsprechung an den rechtmäßigen Zweitvertrieb von Softwarelizenzen stellt, für Verkäufer von Keys kaum praktikabel zu erfüllen sind.

Zugleich sind sowohl der Keyselling-Markt als auch der Vertrieb von Computerspielen ständig in Bewegung. So gehen einige Publisher mittlerweile dazu über, auf Keys ganz zu verzichten und die Produktaktivierung gleich durch die Accounts ihrer jeweiligen Online-Vertriebsplattformen vorzunehmen.[39] Dass aus Keysellern künftig Accountseller werden, ist hierbei nicht zu befürchten – diese Türe hat der *BGH* bereits 2010 mit seiner Half-Life 2-Entscheidung[40] geschlossen.

RA Thomas Merk
ist Leiter der Rechtsabteilung der Koch Media Gruppe. Koch Media mit Hauptsitz in Planegg bei München ist ein internationaler Produzent und Vermarkter von PC- und Konsolenspielen sowie Filmen.

Adrian Schneider
ist Rechtsanwalt bei Osborne Clarke in Köln und berät u.a. Unternehmen der Gamesbranche in IT-rechtlichen Fragestellungen.

39 Vgl. https://www.heise.de/newsticker/meldung/Ubisoft-schiebt-Key-Resellern-einen-Riegel-vor-4412269.html.
40 *BGH* MMR 2010, 771 m. Anm. *Heydn* – Half-Life 2.

FELIX HILGERT / MARTIN SESTER

Strafrechtliche Verantwortlichkeit für den Betrieb von Piraterie-Servern

Strafbarkeit, Verfolgung und Schadensersatzansprüche

Gewerbsmäßige Urheberrechtsverletzung

Der Betrieb von unlizenzierten Piraten-Servern für Onlinespiele verletzt Urheber- und Markenrechte und fügt den legitimen Spieleanbietern erhebliche finanzielle Schäden zu. Betreiber solcher Server begehen dabei praktisch immer erhebliche Straftaten nach dem Urheber- und in einigen Fällen auch nach dem Markengesetz. Neben Freiheits- oder Geldstrafen stehen weitere Folgen, wie die Abschöpfung von Gewinnen und die Einziehung von tatrelevanter IT-Ausrüstung des Täters im Raum. Rechteinhaber können sich als Nebenkläger an Strafverfahren beteiligen und so auch auf eine effektive Abschreckung von Nachahmern hinwirken. Dies gilt insbesondere auch bei ausländischen Tätern, solange sich ihre Aktivitäten auf den deutschen Markt auswirken. Lesedauer: 16 Minuten

I. Einführung

Unter Piraterie-Servern, auch bekannt als Piraten-Server, versteht man Server, die das Spielen eines Onlinespiels ohne Lizenz des eigentlichen Rechteinhabers und unabhängig von dessen Infrastruktur ermöglichen. Es gibt sie insbesondere für eine Reihe von MMORPGs (Massively Multiplayer Online Role-Playing Games). Der Betreiber eines solchen Servers muss hierzu auf rechtswidrig kopierte Versionen der Software des offiziellen Servers zurückgreifen oder, in selteneren Fällen, deren Funktionsweise emulieren. Einige der Piraterie-Server modifizieren den Inhalt der Spiele auch, bieten zusätzliche Funktionen (Mods) oder auch ältere Versionen eines Spiels an. Durch den Verkauf von In-Game-Währung und In-Game-Items verdienen die Betreiber Geld.

Die Betreiber von Piraterie-Servern folgen bei der Monetarisierung demselben Prinzip wie die rechtmäßigen Betreiber der Spiele. Es liegt auf der Hand, dass der Betrieb solcher Server Urheberrechte des legitimen und regelmäßig innerhalb eines bestimmten Territoriums exklusiven Anbieters verletzt und ihm Schäden verursacht, etwa durch den Einnahmeausfall oder allgemein durch die kommerzielle Ausbeutung der diesem Anbieter zukommenden rechtlichen Position. Der Piraterie-Server-Betreiber erspart sich im Vergleich zum redlichen Anbieter etwaige Lizenzgebühren, die der Anbieter an seine(n) Lizenzgeber zu entrichten hat. Sofern der Anbieter das Spiel selbst entwickelt hat, spart der Piraterie-Server-Betreiber die Entwicklungskosten. Marketingkosten des Anbieters fallen beim Piraterie-Server-Betreiber kaum an. Im Gegenteil profitiert er von den Aufwendungen des Anbieters zur Markteinführung und zum Bekanntmachen des Spiels. Der redliche Anbieter hat regelmäßig erhebliche Aufwendungen für Maßnahmen zum Datenschutz und zur Datensicherheit. Solcherlei wird beim Piraterie-Server-Betreiber kaum eine Rolle spielen. Schließlich führt der redliche Betreiber Steuern ab – sowohl Umsatz- als auch Ertragsteuer. Letztlich führt das Ausbleiben der Aufwendungen und Abgaben unter

Anlehnung an die Marktposition, die der Anbieter für das jeweilige Spiel geschaffen hat, nicht selten dazu, dass der Piraterie-Server-Betreiber viel profitabler agiert als der offizielle Anbieter.

Solche Schäden können verletzte Unternehmen über § 97 Abs. 2 UrhG ersetzt verlangen. Bei der Bemessung des Schadens ist – nach Wahl des Anspruchsinhabers – der tatsächlich entstandene Schaden, der Gewinn, den der Verletzer durch die Verletzung des Rechts erzielt hat, oder eine hypothetische Lizenzvergütung maßgeblich. Entsprechendes gilt für einen Schadensersatzanspruch wegen der Verletzung von Markenrechten nach § 14 Abs. 6 MarkenG.

Ebenso wichtig wie eine finanzielle Wiedergutmachung ist den Unternehmen aber oft die schnelle Abschaltung von Piraterie-Servern und eine effektive Abschreckung potenzieller Nachahmer. Hier kann das Strafrecht helfen. Dieser Beitrag beleuchtet am Beispiel eines Präzedenzfalls[1] die strafrechtlichen Konsequenzen für den Betreiber eines Piraterie-Servers und geht der Frage nach, wie Anbieter von Onlinespielen das Strafrecht auch zur Durchsetzung ihrer Ansprüche effektiv nutzen können.

II. Der Fall „Cyperia" des AG Heidelberg

Dass der Betrieb eines Piraterie-Servers auch strafrechtliche Konsequenzen haben kann, zeigte zuletzt der Fall der von 2014 bis 2016 betriebenen Server „Cyperia" und „Hardcore Reloaded" für das Onlinespiel „Metin 2", auf denen mehrere hunderttausend angemeldete Spieler aktiv waren. Mit dem Verkauf virtueller Währung hatte der Betreiber sechsstellige Gewinne erzielen können. So wurden bei der Durchsuchung neben diversen PCs, Notebooks und Speichermedien auch Geldbeträge über € 100.000,– beschlagnahmt.

Im April 2018 verurteilte das *AG Heidelberg* den Betreiber wegen gewerbsmäßiger Urheberrechtsverletzung zu einer Geldstrafe von 90 Tagessätzen i.H.v. jeweils € 20,–. Eine schärfere Strafe konnte der Betreiber abwenden, indem er intensiv mit der *GVU (Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V.)* und den Behörden zusammenarbeitete.

Diese Zusammenarbeit wirke sich aber auch für das verletzte Unternehmen positiv aus, denn sie führte zu Hinweisen auf den Betreiber eines weiteren „Metin 2"-Servers in Berlin, der im Anschluss an eine Durchsuchung im März 2018 in Untersuchungshaft genommen werden konnte. Auch er soll durch den von ihm betriebenen Piraterie-Server Gewinne in sechsstelliger Höhe erzielt haben.[2]

III. Strafbarkeit und Verfolgung des Betriebs von Piraterie-Servern

Bei dem Betrieb eines Piraterie-Servers stehen verschiedene Straftatbestände aus dem UrhG und dem MarkenG im Raum. Denn zum Betrieb eines Piraterie-Servers ist es regelmäßig nicht nur erforderlich, die Software des Game-Servers zu kopieren und auf einem eigenen Server zu installieren. Auch die Clientsoftware muss kopiert, modifiziert und öffentlich zugänglich gemacht werden, etwa durch das Verfügbarmachen auf der eigenen Webseite des Betreibers. Mit der Original-Clientsoftware wird nämlich zumeist eine Verbindung mit anderen als den offiziellen Spiele-Servern des Anbieters nicht möglich sein. Schließlich wird der Betreiber des Piraterie-Servers auch den im Regelfall markenrechtlich geschützten Namen des Spiels verwenden müssen. Dies geschieht eher selten direkt in der Bezeichnung des jeweiligen Piraterie-Servers, sondern häufiger durch verwendete Metatags oder Schlagworte, um in Suchmaschinentreffern oder sog. Toplisten zu erscheinen. In manchen Konstellationen sind Strafanträge des Rechteinhabers erforderlich.

1. Strafbarkeit nach dem UrhG

a) Strafbare Urheberrechtsverletzung

Auf die o.g. Art und Weise vervielfältigt (§ 16 UrhG) der Server-Betreiber daher gleich mehrere Schutzgegenstände des Urheberrechts, bearbeitet (§ 23 UrhG) sie teilweise und macht sie öffentlich zugänglich (§ 19a UrhG). Das Anbieten des bearbeiteten Clients stellt außerdem einen Urheberrechtsverstoß nach § 69c Nr. 1 UrhG dar.

Für die rechtswidrige Vervielfältigung, Verbreitung oder die öffentliche Wiedergabe eines Schutzgegenstands des Urheberrechts sieht das Urheberrecht in § 106 Abs. 1 UrhG eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vor.

b) Umgehung technischer Schutzmaßnahmen

Computerspiele sind nicht nur Computerprogramme i.S.d. §§ 69a ff. UrhG. Vielmehr bestehen sie allein auf Grund ihrer grafischen und klanglichen Bestandteile aus einer Vielzahl von Schutzgegenständen, sodass auch die auf der InfoSoc-Richtlinie beruhenden Regelungen des allgemeinen Urheberrechts auf sie Anwendung finden.[3] Dies ist praktisch relevant, weil dadurch der besondere rechtliche Schutz technischer Schutzmaßnahmen nach § 95a UrhG, der auf reine Software keine Anwendung findet (§ 69a Abs. 5 UrhG), für Computerspiele dennoch gilt.

Als Voraussetzung für die Modifikation der Clientsoftware werden in der Regel auch solchen technischen Schutzmaßnahmen umgangen. Insoweit kommt nach § 108b Abs. 1 UrhG eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe in Betracht.

c) Gewerbsmäßigkeit

Ein noch höherer Strafrahmen ergibt sich in beiden Fällen, wenn der Täter gewerbsmäßig handelt. Im Fall des § 106 Abs. 1 UrhG beträgt die Strafe dann Freiheitsstrafe sogar bis zu fünf Jahren oder Geldstrafe, § 108a Abs. 1 UrhG. In Bezug auf das Umgehen technischer Schutzmaßnahmen erhöht sich das Strafmaß auf Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, § 108b Abs. 3 UrhG.

Gewerbsmäßig handelt dabei, wer sich aus wiederholter Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang verschaffen will. Hierfür haben die Gerichte bereits einen Gewinn von ca. € 1.000,– als ausreichend angesehen.[4] Als wiederholte Tatbegehung gilt auch der fortlaufende Betrieb eines illegalen Servers.[5] Die Qualifikation dürfte daher beim Betrieb eines Piraterie-Servers in aller Regel vorliegen.[6]

2. Strafbarkeit nach dem MarkenG

Der Betrieb eines Piraterie-Servers kann auch in markenrechtlicher Hinsicht zur Strafbarkeit führen, etwa wenn der geschützte Name oder das geschützte Logo des Spiels verwendet werden. So sieht § 143 Abs. 1 Nr. 1 MarkenG eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vor, wenn im ge-

1 *AG Heidelberg* MMR 2019, 547.
2 Vgl. https://www.golem.de/news/gameforge-erstes-urteil-gegen-betreiber-illegaler-spieleserver-1804-133970.html.
3 *EuGH* MMR 2014, 401 m. Anm. *Oehler*.
4 *AG Mainz* NJW 1989, 2637.
5 *Sternberg-Lieben*, in: BeckOK UrhR, Stand: 15.4.2019, § 108a Rdnr. 2.
6 Vgl. dazu auch *AG Heidelberg* MMR 2019, 547; *LG Leipzig* ZUM 2013, 338 – kino.to.

schäftlichen Verkehr widerrechtlich entgegen § 14 Abs. 2 Satz 1 Nr. 1 oder 2 ein Zeichen benutzt wird.

Handelt der Täter gewerbsmäßig, sieht § 143 Abs. 2 MarkenG auch hier ein höheres Strafmaß vor (Freiheitsstrafe von drei Monaten bis zu fünf Jahren).

3. Strafantragserfordernis

Die einfache strafbare Urheberrechtsverletzung nach § 106 UrhG, der unerlaubte Eingriff in technische Schutzmaßnahmen nach § 108b UrhG sowie die einfache strafbare Markenverletzung nach § 143 Abs. 1 MarkenG sind relative Antragsdelikte, § 109 UrhG, § 143 Abs. 3 MarkenG. Anbieter müssen also grundsätzlich einen Strafantrag stellen, um eine Strafverfolgung auszulösen. Berechtigt hierzu sind Urheber selbst und die Inhaber ausschließlicher Nutzungsrechte, nicht aber Inhaber einfacher Nutzungsrechte.[7] Nur bei besonderem öffentlichen Interesse kann die Staatsanwaltschaft ohne Strafantrag ein Ermittlungsverfahren einleiten.

Handelt der Täter gewerbsmäßig, sind sowohl die Urheberrechtsverletzung nach §§ 106, 108a UrhG als auch die Markenverletzung nach § 143 Abs. 2 MarkenG Offizialdelikte. Der unerlaubte Eingriff in technische Schutzmaßnahmen bleibt jedoch auch bei gewerbsmäßigem Handeln Antragsdelikt, wie sich aus dem klaren Wortlaut von § 109 UrhG ergibt.

4. Privatklage

Schließlich sind die §§ 106, 108b UrhG, § 143 Abs. 1 MarkenG Privatklagedelikte nach § 374 Abs. 1 Nr. 8 StPO. Die Staatsanwaltschaft verfolgt diese nur bei Vorliegen eines öffentlichen Interesses und verweist den Rechteinhaber ansonsten auf den Privatklageweg, § 376 StPO. Bei § 108b UrhG gilt dies, anders als bei den übrigen Delikten, sogar bei gewerbsmäßigem Handeln des Täters.

Ein öffentliches Interesse ist schon dann gegeben, wenn die Rechtsverletzung unter Berücksichtigung von Schaden (Potenzial) und Bereicherungsabsicht des Täters nicht nur geringfügig ist. Geringfügigkeit kann bei der Weitergabe einzelner Raubkopien vorliegen, wohl aber nicht bei der Online-Verfügbarmachung geschützter Werke.[8] In den hier einschlägigen Konstellationen wird ein öffentliches Interesse daher stets vorliegen.

IV. Weitere Konsequenzen der Tat

Neben den o.g. Strafen drohen dem Täter auch noch weitere unangenehme Konsequenzen, insbesondere die Einziehung von Taterträgen und der IT-Ausrüstung. Alternativ können die Rechteinhaber im Strafverfahren selbst Schadensersatzansprüche geltend machen.

1. Einziehung von Taterträgen

Gem. § 73 StGB kann das Gericht die Einziehung des durch oder für die rechtswidrige Tat Erlangten, der aus dem Erlangten gezogene Nutzungen oder des entsprechenden Surrogats anordnen. Auf diese Weise können sowohl der Gewinn des Betreibers eines Piraterie-Servers, als auch ggf. für die Tatbegehung geleistete Entgelte abgeschöpft werden. Die Einziehung ist zwingend, sofern keine Ausschlussregelung greift.

Ausschlussregelungen finden sich in § 73e StGB. Nach Absatz 1 ist die Einziehung etwa ausgeschlossen, soweit der Anspruch, der dem Verletzten aus der Tat auf Rückgewähr des Erlangten oder auf Ersatz des Werts des Erlangten erwachsen ist, erloschen ist. Der Umfang der Einziehung ist damit abhängig von der Erfüllung zivilrechtlicher Ansprüche des Verletzten. Werden die Ansprüche nicht durch den Verletzten geltend gemacht, so besteht die Möglichkeit für den Staat, die Bereicherung des Täters abzuschöpfen.

Der § 73e Abs. 2 StGB sieht eine Regelung vor, die an die Regelung der §§ 818 Abs. 3, 819 Abs. 1 BGB erinnert: Soweit der Wert des erlangten zum Anordnungszeitpunkt nicht mehr im Vermögen des Betroffenen vorhanden ist, soll die Einziehung ausgeschlossen sein. Dies gilt jedoch nur, wenn dem Betroffenen kein Vorwurf der Kenntnis oder leichtfertigen Unkenntnis der Umstände, die die Anordnung der Einziehung zugelassen hätten, zum Zeitpunkt des Wegfalls der Bereicherung gemacht werden kann.

2. Einziehung von Gegenständen

Nicht nur das aus der Tat Erlangte, hieraus gezogene Nutzungen und entsprechende Surrogate können eingezogen werden, sondern auch Gegenstände des Betreibers, die sich auf die begangene Straftat nach den §§ 106, 108a, 108b UrhG, § 143 MarkenG beziehen, § 110 Satz 1 UrhG bzw. § 143 Abs. 5 Satz 1. MarkenG i.V.m. §§ 74 ff. StGB.

Über § 74 StGB hinausgehend können dabei nicht nur die Gegenstände eingezogen werden, die durch die Straftat hervorgebracht wurden („producta sceleris") oder zur Begehung oder Vorbereitung der Straftat gebraucht worden sind („instrumenta sceleris"), sondern auch die Gegenstände, die notwendiger Gegenstand der Tatbegehung selbst sind: die Pirateriewaren.[9]

Allerdings ist bei der Einziehung der in § 74b StGB wiederzufindende Grundsatz der Verhältnismäßigkeit zu wahren. Dies hat zur Konsequenz, dass Gegenstände, die zur Begehung der Tat genutzt wurden, gleichzeitig aber auch und überwiegend zu rechtmäßigen Zwecken verwendet werden, wie z.B. Computer, regelmäßig nicht eingezogen werden können.[10] Etwas anderes kann jedoch dann gelten, wenn der Täter gewerbsmäßig handelte,[11] was zumindest dann der Fall sein wird, wenn der Betreiber eines Piraterie-Server den Nutzern entgeltliche Leistungen anbietet. In diesen Fällen kann daher auch die gesamte genutzte IT-Ausstattung des Täters eingezogen werden.

Voraussetzung für eine Einziehung ist neben der vorsätzlichen Begehung der Tat (§ 74 Abs. 1 StGB), dass die Gegenstände zur Zeit der Entscheidung dem Täter oder Teilnehmer der Tat gehören oder zustehen, § 74 Abs. 3 Satz 1 StGB. Letzteres ist aber ausnahmsweise dann entbehrlich, wenn derjenige, dem der Gegenstand zur Zeit der Entscheidung gehört oder zusteht, mindestens leichtfertig dazu beigetragen hat, dass der Gegenstand als Tatmittel verwendet wird oder Tatobjekt gewesen ist, oder den Gegenstand in Kenntnis der Umstände, welche die Einziehung zugelassen hätten, in verwerflicher Weise erworben hat, § 110 Satz 2 UrhG bzw. § 143 Abs. 5 Satz 2 MarkenG i.V.m. § 74a StGB.

Sollte die Einziehung eines solchen Gegenstands nicht möglich sein, weil der Täter oder Teilnehmer diesen veräußert, verbraucht oder die Einziehung auf andere Weise vereitelt hat, so kann das Gericht auch die Einziehung eines entsprechenden Geldbetrags anordnen, § 74c Abs. 1 StGB.

---

7 *Ernst*, in: GJW Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2017, UrhG § 106 Rdnr. 92.
8 *Ernst* (o. Fußn. 7), Rdnr. 95.
9 *Heinrich*, in: MüKoStGB, 2. Aufl. 2015, UrhG § 110 Rdnr. 1.
10 *Sternberg-Lieben* (o. Fußn. 5), § 110 Rdnr. 6; *Heinrich* (o. Fußn. 9), § 110 Rdnr. 5; *Hildebrandt/Reinbacher*, in: Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 110 Rdnr. 1.
11 *Sternberg-Lieben* (o. Fußn. 5), § 110 Rdnr. 6; *Hildebrandt/Reinbacher* (o. Fußn. 10).

3. Adhäsionsverfahren

Kommt es zum Strafverfahren gegen den Betreiber des Piraterie-Servers, so kann sich der Rechteinhaber nicht nur als Nebenkläger beteiligen (§ 395 Abs. 1 Nr. 6 StPO), sondern zusätzlich die Durchführung eines Adhäsionsverfahrens beantragen, §§ 403 ff. StPO.

Das Adhäsionsverfahren ist ein strafprozessuales Anhangsverfahren, das die Geltendmachung von vermögensrechtlichen Ansprüchen des Verletzten gegen den Täter bereits im Strafverfahren ermöglicht, und zwar – insbesondere für Unternehmen mit eigener Rechtsabteilung kostensparend – auch dann ohne Anwaltszwang, wenn die geltend gemachte Summe den Zuständigkeitsstreitwert des Amtsgerichts übersteigt.[12]

Ein etwaiges Adhäsionsverfahren hat Vorrang vor der Einziehung, § 110 Satz 3 UrhG bzw. § 143 Abs. 5 Satz 3 MarkenG. Wird in einem solchen Verfahren ein Anspruch aus § 98 UrhG auf Vernichtung, Rückruf oder Überlassung der Vervielfältigungsstücke oder der Vorrichtungen zur Herstellung dieser Vervielfältigungsstücke stattgegeben, ist eine Einziehung nach § 110 Satz 1 UrhG bzw. § 143 Abs. 5 Satz 1 MarkenG ausgeschlossen.

V. Internationale Sachverhalte

In Konstellationen mit Auslandsberührung kann sich die (Vor-)Frage stellen, inwieweit deutsches Immaterialgüter- und Strafrecht anwendbar ist. Dem Territorialitätsprinzip zufolge werden deutsche Marken- und Urheberrechte jedoch nur in Deutschland geschützt. In reinen Auslandssachverhalten kann es daher schon gar nicht zu den erforderlichen Marken- und Urheberrechtsverletzungen kommen.

1. Verletzung deutschen Urheberrechts

Das Vervielfältigungsrecht nach § 16 UrhG wird nach allgemeiner Auffassung an dem Ort verletzt, an dem das Vervielfältigungsexemplar entsteht.[13] Das ist grundsätzlich der Standort des Piraterie-Servers. Allerdings kann die (technische) Herstellung der Vervielfältigung auch durch die Bedienung eines PCs in Deutschland veranlasst worden sein. Es stellt sich die Frage, ob in diesem Fall auch Deutschland als Verletzungsort anzusehen ist. Verneinte man dies, hätte die Verletzung des Vervielfältigungsrechts ggf. nur im Ausland stattgefunden, sodass ein Vorgehen auf Grundlage des deutschen Urheberrechts nicht möglich wäre. Diese Konsequenz ist jedoch nicht hinnehmbar.[14]

Schließlich richtet sich das Recht aus § 16 UrhG nicht nur gegen die Existenz von Vervielfältigungen, sondern gerade gegen deren Herstellung. Hierfür sind Initiierung und Steuerung aber wesentlich, weshalb auch der Ort, an dem diese Handlungen vorgenommen werden, als Verletzungsort angesehen werden sollte.

Problematischer ist der Verletzungsort bei der öffentlichen Zugänglichmachung über das Internet. Es wäre möglich, allein auf den Ort, an dem diese veranlasst wurde, oder den Standort der Server abzustellen.[15] Nach der Rechtsprechung des *EuGH* tritt eine Urheberrechtsverletzung bei Internetsachverhalten aber auch in jedem Land ein, in dem der Schutzgegenstand abrufbar ist.[16] Nur diese Ansicht trägt auch dem Umstand angemessen Rechnung, dass die Einstellung in das Internet den Abruf des Schutzgegenstands und damit die Beeinträchtigung der Schutzrechte in zahlreichen Ländern zur Folge hat, und verringert den Anreiz zur Flucht potenzieller Täter in Länder, die einen geringen Urheberrechtsschutz bieten.[17] Dementsprechend ist davon auszugehen, dass § 19a UrhG selbst dann verletzt sein kann, wenn der Betreiber eines Piraterie-Servers vom Ausland aus gehandelt und einen ausländischen Server verwendet hat, sofern der Schutzgegenstand auch aus Deutschland (bestimmungsgemäß) abrufbar ist.

2. Anwendbarkeit deutschen Strafrechts

Die Anwendbarkeit deutschen Strafrechts richtet sich in erster Linie nach den §§ 3, 9 StGB. Nach § 3 StGB gilt das deutsche Strafrecht für Taten, die im Inland begangen werden. § 9 StGB konkretisiert den Ort der Tat. Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat (Handlungsort) oder der zum Tatbestand gehörende Erfolg eingetreten ist (Erfolgsort). Da der Schutz des Urheberrechts auf das jeweilige Territorium begrenzt ist (Territorialitätsprinzip), kann der Erfolgsort, nur im Inland liegen. § 7 StGB, der die Anwendbarkeit deutschen Strafrechts bei Auslandsdelikten ermöglicht, ist damit ohne Relevanz.[18]

Hat der Täter in Deutschland gehandelt, ist es dementsprechend nicht entscheidend, ob der Piraterie-Server im Ausland steht. Probleme ergeben sich aber, wenn der Handlungsort nicht im Inland liegt. Denn das Abstellen auf einen Erfolgsort setzt grundsätzlich voraus, dass der verwirklichte Straftatbestand überhaupt den Eintritt eines Erfolgs verlangt. Während der Vervielfältigungstatbestand unzweifelhaft ein Erfolgsdelikt ist,[19] wird für den Tatbestand des öffentlichen Zugänglichmachens auch vertreten, dass nur ein Tätigkeitsdelikt vorliege, da es gerade nicht erforderlich sei, dass der zugänglich gemachte Schutzgegenstand auch tatsächlich die Öffentlichkeit erreicht.[20] Dem ist entgegen zu halten, dass die Abrufbarkeit von Werken bereits einen Verbreitungserfolg gem. § 106 UrhG darstellen kann.[21] Die Frage ist derzeit aber weitgehend offen.[22]

Felix Hilgert
ist Rechtsanwalt bei Osborne Clarke in Köln und berät schwerpunktmäßig Unternehmen der Spielebranche.

Dr. Martin Sester
ist Leiter Recht der Gameforge AG und Rechtsanwalt in Karlsruhe.

Wir danken unserer wissenschaftlichen Mitarbeiterin Frau Alina Betzemeier für die Unterstützung bei der Recherche zu diesem Beitrag.

12 *Ferber*, in: BeckOK StPO, Stand: 1.4.2019, § 403 Rdnr. 11.
13 *Ziegler*, Urheberrechtsverletzungen durch Social-Sharing, Tübingen 2016, S. 75.
14 *Ziegler* (o. Fußn. 13).
15 *Dreier*, in: Dreier/Schulze,UrhG, 6. Aufl. 2018, § 120 Vor Rdnr. 41; *Dieselhorst*, ZUM 1998, 293, 299 f.
16 *EuGH* MMR 2015, 187 – Hejduk/EnergieAgentur; *Sternberg-Lieben* (o. Fußn. 5), § 106 Rdnr. 18.
17 *Ziegler* (o. Fußn. 13), S. 76.
18 *BGH* GRUR 2004, 421, 422 f. = MMR 2004, 355 (Ls.); *Dreier* (o. Fußn. 15), § 106 Rdnr. 16.
19 *Sternberg-Lieben* (o. Fußn. 5), § 106 Rdnr. 23; *Hildebrandt/Reinbacher* (o. Fußn. 10), § 106 Rdnr. 12.
20 *Hildebrandt/Reinbacher* (o. Fußn. 10), § 106 Rdnr. 20; a.A. *Heghmanns*, MMR 2004, 14, 15.
21 *Sternberg-Lieben* (o. Fußn. 5), § 106 Rdnr. 18; vgl. auch *LG Hamburg* GRUR-RS 2016, 12262.
22 Zum Meinungsstand *Sternberg-Lieben* (o. Fußn. 5), § 106 Rdnr. 18 f.; *Hildebrandt/Reinbacher* (o. Fußn. 10), § 106 Rdnr. 46, jew. m.w.Nw.

CHRISTIAN RAUDA

Cheatbots in Computerspielen

Urheber-, wettbewerbs- und markenrechtliche Ansprüche gegen Schummelsoftware

Abwehransprüche

Anbieter von Online-Computerspielen haben mit Unternehmen zu kämpfen, die Cheatbot-Software anbieten.
Ein Cheatbot (oder Bot) ist eine Software, die automatisiert periodisch wiederkehrende Aufgaben im Spiel ausführt, ohne dabei auf die Bedienung durch einen Menschen angewiesen zu sein. Durch den Einsatz der Software kann ein Spieler im Spiel Handlungen ausführen, ohne physisch präsent zu sein. Er verschafft sich dadurch Vorteile und kommt schneller im Spiel voran als seine Konkurrenten. Die Herstellung von Cheatbots greift in das Vervielfältigungsrecht des Inhabers der Nutzungsrechte am Computerprogramm nach § 69c Nr. 1 UrhG sowie der übrigen betroffenen Werke nach § 16 Abs. 1 UrhG ein. Es greift keine Schranke ein, weil die Rechteeinräumung nicht die Vervielfältigung der Client-Software zu kommerziellen Zwecken, nämlich im Rahmen der Entwicklung der Cheatbot-Software erfasst (vgl. § 31 Abs. 5 UrhG). Wettbewerbsrechtlich sind Cheatbots eine gezielte Behinderung des Publishers der Spiele „unter dem Gesichtspunkt der unlauteren vertriebsbezogenen Behinderung durch einen empfindlichen Eingriff in das Spielsystem". Ansprüche aus Markenrecht bestehen, wenn der Cheatbot das Spiel, in dem er zum Einsatz kommt, im Namen trägt, etwa „World of Warcraft Bot". Lesedauer: 23 Minuten

I. Einleitung

Seit es Computerspiele gibt, suchen und finden Spieler Wege, im Spiel zu betrügen (sog. cheaten). Einige Spielehersteller haben in den Code ihrer Software bereits Funktionen eingebaut, die dem Spieler erlauben, bestimmte Spielmechaniken außer Kraft zu setzen.

1. Anfänge der Cheatfunktionen

Früher wurden solche Funktionen oft mit einer geheimen Tastenkombination ausgelöst. Wenn man also etwa bei „The Great Giana Sisters" auf dem C64 die Tastenkombination A+R+M+N drückte, konnte man ein Level überspringen (*Armin Gessert*, der Programmierer, hatte sich damit verewigt). Es bildeten sich in den 1980er Jahren Kollektive, die Cheats in Computerspiele integriert haben.

2. Onlinespiele

Ende der 1990er, Anfang der 2000er Jahre kamen Spiele auf, die man im Internet über den Browser spielen konnte. Die Spielewelten zeichneten sich dadurch aus, dass tausende, später Millionen Spieler gleichzeitig gegeneinander spielen konnten. Ein beliebtes Genre waren etwa Aufbau-Strategiespiele, bei denen man Ressourcen abbauen und dann eine Infrastruktur aufbauen musste (etwa Dörfer, Stützpunkte und militärische Macht). Es ist möglich, die gegnerische Infrastruktur anzugreifen und bei einem Sieg über den Gegner zu übernehmen. Um bei diesen Spielen erfolgreich zu sein, ist es erforderlich, bestimmte Tätigkeiten im Spiel immer wieder auszuführen (etwa der Abbau von Rohstoffen). Diese Handlungen können nur vom Spieler selbst ausgeführt werden, dieser muss also aktiv am Spiel teilnehmen. Wie wäre es aber, wenn man sich lästige, sich wiederholende Handlungen sparen könnte und diese Tätigkeiten an eine Software „delegieren" könnte? An dieser Stelle kommen Cheatbots (oder kurz: Bots) ins Spiel: Das Wort Bot findet seinen sprachlichen Ursprung in dem Wort Roboter und ist eine Kurzform hiervon. Ein Bot ist eine Software, die automatisiert periodisch wiederkehrende Aufgaben im Spiel ausführt, ohne dabei auf die Bedienung durch einen Menschen angewiesen zu sein.[1] Der häufigste Fall des automatisierten Einsatzes ist der Abbau von Rohstoffen im Spiel. Rohstoffe sind häufig der Schlüssel zum Spieleerfolg, weil sie gegen Gegenstände und Einheiten eingetauscht werden können. Wer also über viele Ressourcen verfügt, kommt schneller im Spiel voran als seine Konkurrenten. Die Nutzung eines Cheatbot rund um die Uhr entspricht also der Situation, dass ein Mensch das Spiel 24 Stunden spielt und durch eigene Handlungen etwa Rohstoffe abbaut.

3. Online-Rollenspiele

Am häufigsten werden Cheatbots in Zusammenhang mit Online-Rollenspielen wie „World of Warcraft" genutzt, an denen viele Spieler teilnehmen. Indem man einen Cheatbot verwendet, verschafft man sich gegenüber den anderen Spielern einen Vorteil. Dies führt dazu, dass der den Cheatbot nutzende Spieler im Vergleich zu den anderen Spielern im Vorteil ist. Ein solcher Vorteil lässt sich auch monetarisieren, denn es gibt Plattformen im Internet, auf denen sich weiterentwickelte Charaktere und andere Spielinhalte zu beachtlichen Preisen verkaufen lassen.[2]

Um an dem Spiel „World of Warcraft" teilzunehmen, muss der Spieler auf einem Datenträger oder online eine Client-Software erwerben, die er lokal auf seinem Rechner installiert. Wenn man die Software startet, verbindet sich diese über das Internet mit einem Server des Spieleanbieters, auf dem die virtuelle Spielwelt und die Spielercharaktere verwaltet und verarbeitet werden (Battle.net-Server). Eine Verbindung mit dem Battle.net-Server ist nur über einen Account möglich. Der Spieler muss sich also jedes Mal mit einem Benutzernamen und einem Passwort zur Teilnahme am Spiel über den Server anmelden.

Im Zuge des Registriervorgangs werden ihm die „Battle.net-Nutzungsbestimmungen", die „World of Warcraft-Endbenutzerlizenzvereinbarung" und die „World of Warcraft-Nutzungsbestimmungen" angezeigt, denen er zustimmen muss. Verweigert er seine Zustimmung, kann er die Registrierung nicht abschließen und folglich an dem Spiel auch nicht teilnehmen. Im Rahmen der zu akzeptierenden Bedingungen wird der Spieler verpflichtet, keine Cheatbots einzusetzen, also keine Spielhandlungen über externe Software automatisiert ausführen zu lassen.

Der Spieleanbieter steht allerdings vor praktischen Schwierigkeiten, wenn er einem Spieler die Nutzung einer Cheatbot-Software nachweisen möchte. Er kann auf den Client-Rechner des Spielers nicht zugreifen und muss sich damit begnügen, Zugriffsmuster darzulegen, die ein Indiz dafür liefern, dass ein Cheatbot eingesetzt wurde.[3] Spielentwickler setzen hierzu Soft-

1 *Rauda*, Recht der Computerspiele, 2013, Rdnr. 226.
2 *Röttgen/Juelicher*, DSRITB 2017, 227, 232.
3 *Röttgen/Juelicher*, DSRITB 2017, 227, 233.

ware ein, die Handlungen in ihren Spielen aufspüren, die voraussichtlich nicht von realen Spielern ausgeführt wurden, sondern von Cheatbots. Die Hersteller der Bots wiederum versuchen, die Entdeckung zu verhindern, indem sich der Cheatbot so weit wie möglich einem realen Spieler ähnlich verhält. Die Spieleheresteller sperren dann die Accounts dieser Spieler. Ein solches Vorgehen gleicht allerdings dem „Kampf gegen die Windmühlen". Viel effektiver ist es, den Anbieter des Cheatbot rechtlich zu attackieren und so das Problem an der Wurzel zu packen.

Die Spieleheresteller haben die Cheatbots auf Basis des Urheberrechts, des Gesetzes gegen den unlauteren Wettbewerb, des Markenrechts, des Vertragsrechts, des „virtuellen Hausrechts" und des Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb angegriffen.

II. Ansprüche aus Urheberrecht

1. Vervielfältigung

Die Spieleheresteller haben argumentiert, dass die Entwicklung eines Cheatbot das Urheberrecht am Spiel berührt. Die Software, die sich der Nutzer herunterladen muss, um das Spiel zu spielen, ist urheberrechtlich geschützt, und zwar sowohl nach § 69a Abs. 1 UrhG als auch nach § 2 Abs. 1 UrhG. Denn das Spiel enthält neben dem Code, also dem Computerprogramm, auch Grafiken, Musik, Filmsequenzen, Texte und Modelle,[4] die als audiovisuelle Bestandteile getrennt schutzfähig sind, nämlich entweder einzeln als Sprachwerke, Musikwerke, Werke der bildenden Kunst oder als kombiniertes Multimediawerk.[5] Eine Vervielfältigung greift in das Vervielfältigungsrecht des Inhabers der Nutzungsrechte am Computerprogramm nach § 69c Nr. 1 UrhG sowie der übrigen betroffenen Werke nach § 16 Abs. 1 UrhG ein. Zwar hat der *BGH* aufgeführt, dass die isolierte Anzeige des Spiels auf einem Bildschirm keinen Eingriff in das Recht des Spieleherstellers darstellt. Denn die Anzeige auf einem Bildschirm erfüllt nicht das Kriterium der für eine Vervielfältigung erforderlichen Körperlichkeit.[6] Die Software wird allerdings in den Arbeitsspeicher und Grafikspeicher des Rechners des Nutzers geladen[7] und damit körperlich dupliziert. Um einen Cheatbot zu testen, muss man die Client-Software, die der Spieleheresteller zur Verfügung stellt, vervielfältigen.

2. Schranken

Die Vervielfältigung der Client-Software durch einen „normalen Nutzer" ist zwar durch die Erlaubnis des Spieleherstellers gedeckt. Der Zweck der Rechteübertragung umfasst allerdings nur die Nutzung zum Zweck, das Spiel privat zu spielen. Nicht vom Zweck der Rechteeinräumung umfasst ist daher die Vervielfältigung der Client-Software zu kommerziellen Zwecken, nämlich im Rahmen der Entwicklung der Cheatbot-Software (vgl. § 31 Abs. 5 UrhG).[8] Konsequenterweise haben das *OLG München* und das *OLG Dresden* ihre jeweiligen Verbote zur Vervielfältigung der Client-Software auf die gewerbliche Vervielfältigung beschränkt.[9] Dies steht auch im Einklang der Schranke des § 53 Abs. 1 UrhG, wonach nur eine private Vervielfältigung privilegiert ist.[10] Der Hersteller des Cheatbot kann für sich zwar die Ausnahme des § 69d Abs. 3 UrhG in Anspruch nehmen, wonach eine Software (hier: die Client-Software) zur Programmbeobachtung und -analyse auch ohne Zustimmung des Rechteinhabers vervielfältigt werden darf.[11] Diese Vorschrift erlaubt allerdings nur die Vervielfältigung des Computerprogramms als solchem, nicht jedoch die Vervielfältigung von audiovisuellen Bestandteilen des Spiels. Weder das nationale deutsche Urheberrecht noch die Richtlinie 2001/29/EG enthalten eine Art. 5 Abs. 3 RL 2009/24/EG entsprechende Bestimmung, wonach die Vervielfältigung eines Werks oder sonstigen Schutzgegenstands, bei dem es sich nicht um ein Computerprogramm handelt, zu Analysezwecken erlaubt ist.[12] Wenn man die Client-Software aber ablaufen lässt, vervielfältigt man zwangsläufig auch grafische Inhalte des Spiels oder die Spielmusik.[13] Die unzulässige Vervielfältigung der Client-Software im Rahmen der Entwicklung des Cheatbot führt sogar dazu, dass nicht nur Unterlassungsansprüche, sondern auch Auskunfts- und Schadensersatzansprüche in Bezug auf den Vertrieb der Cheatbot-Software bestehen. Der *BGH* stellte einen Konnex zwischen der Vervielfältigung der Client-Software und der Auswertung der Cheatbot-Software her: Die mit dem Verkauf der Automatisierungssoftware erzielten Umsätze und Gewinne beruhten (auch) auf der Vervielfältigung der Client-Software.[14] Hinsichtlich der Herstellung, Nutzung und Verbreitung der Cheatbot-Software besteht allerdings mangels relevanter Verletzungshandlung kein urheberrechtlicher Unterlassungsanspruch.[15]

III. Ansprüche aus Wettbewerbsrecht

1. § 4 Nr. 4 UWG

Noch bevor die Publisher von Computerspielen gegen die Hersteller und Verbreiter von Cheatbot-Software auf Basis des Urheberrechts vorgingen, erfolgte der Angriff auf die Cheatbot-Software auf Grundlage des Wettbewerbsrechts, nämlich wegen gezielter Behinderung nach § 4 Nr. 4 UWG[16]. Der Anbieter der Cheatbot-Software lizenzierte diese kostenpflichtig an interessierte Nutzer.[17] Aus Sicht der Publisher lag ein Eingriff in den Leistungswettbewerb vor. Der Cheatbot wirkte mit der Spielsoftware auf eine Weise zusammen, die dazu führte, dass die Nutzer des Cheatbot Vorteile hatten gegenüber ihren Mitspielern, die keine Cheatbots nutzten. Die Cheatbots sind im Spiel „unterwegs" und sammeln etwa Gegenstände, ohne dass der Spieler seine Figur selbst steuern muss. Auf diese Weise werden die Figuren derjenigen Spieler „mächtiger", die Cheatbots einsetzen. Es kommt zu einem Wettbewerbsgefälle. Ehrliche Spieler, also Spieler, die sich an das in den Nutzungsbedingungen des Publishers verankerte Verbot des Einsatzes von Cheatbots hal-

4 BGH MMR 2017, 171 m. Anm. *Biehler/Apel* – World of Warcraft I.
5 *EuGH* MMR 2014, 401 m. Anm. *Oehler*, Rdnr. 23 – Nintendo/PC Box und 9Net; MMR 2013, 671 m. Anm. *Roth* Rdnr. 20 – Videospiel-Konsolen I; MMR 2015, 460 m. Anm. *Roth* Rdnr. 43 – Videospiel-Konsolen II.
6 *BGH* GRUR 1991, 449 – Betriebssystem; a.A. *Haberstumpf* in: Büscher/Dittmer/Schiwy, Gewerblicher Rechtsschutz, Urheberrecht, Medienrecht, 3. Aufl. 2014, § 15 UrhG Rdnr. 3 f. und § 69c UrhG Rdnr. 2 f. Der *BGH* führt in MMR 2017, 171 m. Anm. *Biehler/Apel* aus, warum sich nichts anderes aus der *EuGH*-Entscheidung „Football Association Premier League" ergibt: Dort sei die Körperlichkeit bejaht worden, weil die flüchtigen Fragmente des auf dem Bildschirm gezeigten Werks im Satellitendecoder vorübergehend körperlich festgelegt waren.
7 *Hentsch*, Die Urheberrechte der Publisher bei eSport, MMR-Beil. 8/2018, 3, 5.
8 *BGH* MMR 2017, 171 m. Anm. *Biehler/Apel* – World of Warcraft I.
9 *OLG München* BeckRS 2015, 119932: „Die Bekl. hat das Recht zur Vervielfältigung der Software zu gewerblichen Zwecken nicht mit dem Kauf der Client-Software erworben. Bei der Client-Software handelt es sich um Installationssoftware. Der Käufer soll durch die Installation und damit die dauerhafte Vervielfältigung der Software auf seinem PC die technischen Voraussetzungen für die Teilnahme an den Online-Spielen erhalten. Dieses Vervielfältigungsrecht besteht jedoch nicht zu gewerblichen Zwecken."; *OLG Dresden* MMR 2015, 402 m. Anm. *Struwe/Hansen*.
10 *OLG München* BeckRS 2015, 119932; *Röttgen/Juelicher*, DSRITB 2017, 227, 233, dort Fußnote 27.
11 *BGH* MMR 2017, 171 m. Anm. *Biehler/Apel* – World of Warcraft I; *Czychowski*, GRUR 2017, 362 meint, dass die Kl. einen Pyrrhus-Sieg errungen habe, denn der *BGH* sei grundsätzlich der Auffassung, dass die Entwicklung von Bots nach § 69d Abs. 3 UrhG zulässig sei. Dies sei eine „sehr weitgehende Auffassung". Das *OLG Dresden* hatte noch geurteilt, dass die Untersuchung der Funktionalität der Spielesoftware des Publishers von den Beobachtungs- und Untersuchungshandlungen nach § 69d Abs. 3 UrhG nicht erfasst werde, *OLG Dresden* MMR 2015, 407 m. Anm. *Struwe/Hansen*.
12 *BGH* MMR 2017, 171 m. Anm. *Biehler/Apel* – World of Warcraft I.
13 *BGH* MMR 2017, 171 m. Anm. *Biehler/Apel* – World of Warcraft I.
14 *BGH* MMR 2017, 171 m. Anm. *Biehler/Apel* – World of Warcraft I.
15 *OLG München* BeckRS 2015, 119932.
16 § 4 Nr. 10 UWG a.F. (gleichlautend).
17 Vgl. zu dem Lizenzmodell die Sachverhaltsdarstellung in *LG Hamburg* MMR 2013, 725.

ten, werden benachteiligt. Bei gleicher Spielzeit erreichen sie weniger. Es ergibt sich aber noch eine weitere Problematik: In vielen Onlinespielen gibt es Mechanismen, Spielfortschritt entweder durch Spielzeit oder alternativ durch den Erwerb kostenpflichtiger Spielvorteile (sog. Items) zu erzielen. Diejenigen Spieler, die einen Cheatbot einsetzen, können sich auf diese Weise oft den Kauf von Items sparen. Würden sämtliche Spieler Cheatbots einsetzen statt die Leistungen des Publishers zu erwerben, könnte der Publisher sein Spiel nicht mehr wirtschaftlich betreiben. Dem Publisher entgehen durch den Einsatz von Cheatbots jedenfalls solche Umsätze, die von Spielern getätigt worden wären, wenn diese keine Bots eingesetzt hätten. Der Umsatz des Schadens ist allerdings schwer zu schätzen, da in den meisten Free-to-Play-Onlinespielen nur 1-5% der Spieler Items erwerben.[18] Nicht jeder, der einen Cheatbot einsetzt, hätte also ansonsten Geld für die Leistungen ausgegeben, die er mit dem Cheatbot erlangt.

2. Wettbewerbsverhältnis

Zwischen dem Cheatbot-Hersteller und dem Publisher des Computerspiels, mit dem der Cheatbot interagiert, besteht ein Wettbewerbsverhältnis. Dieses ist weit zu verstehen.[19] Zwar besteht im vorliegenden Falle kein direkter Wettbewerb dergestalt, dass sich Kunden alternativ zwischen der Spielesoftware des Publishers und der Lizenzierung der Cheatbot-Software entscheiden. Die Cheatbot-Software stellt eher ein komplementäres Produkt dar, eine Art „Zubehör". Man muss allerdings beachten, dass der Einsatz der Cheatbot-Software einen erheblichen Einfluss auf den Absatz der Spielesoftware hat. In dem Fall, in dem sich eine Handlung ihrer Art nach notwendigerweise nachteilig für den Wettbewerb eines anderen Unternehmers auswirken kann, besteht zu diesem Unternehmer ein konkretes Wettbewerbsverhältnis und zwar – im Unterschied zum Substitutionswettbewerb – unabhängig davon, ob die jeweiligen Unternehmen auf demselben relevanten Markt tätig sind.[20] Spieler, die sich für das Spiel des Publishers interessieren, aber wissen, dass es auf Grund des Cheatbot Möglichkeiten gibt, sich illegal Vorteile im Spiel zu verschaffen, werden vom Erwerb der Software abgeschreckt.

3. Schädigung des Mitbewerbers

Eine gezielte Behinderung nach § 4 Nr. 4 UWG setzt voraus, dass die wettbewerblichen Entfaltungsmöglichkeiten eines Mitbewerbers nicht nur als Reflex der Anpreisung und des Vertriebs der eigenen Leistungen beeinträchtigt werden, sondern die Behinderung primär der Schädigung des Mitbewerbers dient. Eine gewisse Behinderung des Mitbewerbers ist auch dem Leistungswettbewerb immanent, denn dieser ist ja darauf gerichtet, dem Wettbewerber Marktanteile zu entziehen. Um die erlaubte von der unerlaubten Behinderung abzugrenzen, ist eine Gesamtwürdigung der Umstände des Einzelfalls erforderlich. Hierbei sind die sich gegenüberstehenden Interessen der beteiligten Mitbewerber, Verbraucher oder sonstigen Marktteilnehmer sowie der Allgemeinheit gegeneinander abzuwägen.[21] Im Falle der Cheatbots hat die Rechtsprechung eine gezielte Behinderung des Publishers der Spiele „unter dem Gesichtspunkt der unlauteren vertriebsbezogenen Behinderung durch einen empfindlichen Eingriff in das Spielsystem" angenommen.[22] Der Publisher sei als Entwickler des Spiels völlig frei, die Spielregeln des Spiels festzulegen. Die Hersteller von Cheatbots greifen „empfindlich in das Spielsystem von „World of Warcraft" ein, indem sie Mitspieler dazu verleiten und es ermöglichen, dass sie diese Bots verwenden, deren Anwendung gegen die Spielregeln verstoßen".[23] Das *LG Hamburg* hat angenommen, dass ein Spiel, bei dem ehrliche Spieler benachteiligt werden, erheblich an Attraktivität einbüßt, wenn sie wissen, dass ihre Mitspieler ihre Fertigkeiten „nicht ebenso teuer oder langwierig erwerben mussten".[24] Das *LG Hamburg* ließ auch nicht das Argument gelten, dass Spieler im Allgemeinen mit der Existenz von Bots vertraut seien und sich daran gewöhnt hätten, dass sich einige Figuren dynamischer entwickeln als andere.[25] Die Attraktivität des Spiels wird darüber hinaus dadurch gemindert, dass sich ein Spieler nicht sicher sein kann, ob die Figuren, die er im Spiel selbst antrifft, von echten Menschen gesteuert werden, oder ob es sich um von Cheatbots gesteuerte Charaktere handelt.[26] Gerade bei einem Spiel, das auf Interaktion der Mitspieler angelegt ist, leidet der Spielspaß natürlich, wenn in dem Spiel „Roboter" unterwegs sind, die man auf den ersten Blick nicht von Figuren unterscheiden kann, die von echten Menschen gesteuert werden.[27] Die Cheatbots haben daher eine erhebliche Auswirkung auf das Geschäftsmodell des Publishers: „Werden Kunden abgeschreckt, wird jedenfalls ein Teil von ihnen davon Abstand nehmen, das Spiel zu erwerben und diejenigen, die es bereits gekauft haben, werden jedenfalls z.T. vom weiteren Spiel absehen und/oder andere Kunden warnen, indem sie sich z.B. auf Internetforen kritisch, enttäuscht oder verärgert äußern und auf diese Weise wieder andere Kunden vom Erwerb des Spieles abhalten."[28]

4. Verleiten zum Vertragsbruch

Ob neben dem Aspekt der gezielten Behinderung auch ein unlauteres Verleiten zum Vertragsbruch vorlag, ließ die *12. Zivilkammer des LG Hamburg* im Jahr 2012 offen,[29] das *OLG Hamburg* verneinte dies.[30] Im Jahr 2009 hatte die *8. Zivilkammer des LG Hamburg* im Rahmen eines einstweiligen Verfügungsverfahrens ein Verleiten zum Vertragsbruch noch bejaht. Wer Funktionen anbiete, durch die sich der jeweilige Nutzer gegenüber seinen Mitspielern einen Wettbewerbsvorteil verschaffen kann, weil sie von dem Publisher für das Spiel nicht vorgesehen sind

18 Bei World of Warcraft handelt es sich allerdings nicht um einen Free-to-play-Titel, also ein Spiel, das man grds. kostenfrei spielen kann und bei dem man nur bei Bedarf Items dazukaufen kann. Bei World of Warcraft muss man ein Abonnement erwerben. Ferner existiert im Spiel ein Wirtschaftssystem, wonach man eine spieleigene Währung („Gold") in Ausrüstungsgegenstände etc. umtauschen kann.
19 *BGH* GRUR 2006, 1042 Rdnr. 16 – Kontaktanzeigen.
20 *BGH* GRUR 2006, 1042 Rdnr. 16 – Kontaktanzeigen
21 *BGH* MMR 2004, 662 m. Anm. *Funk/Zeitfang* – Werbeblocker
22 *LG Hamburg* MMR 2013, 725.
23 *LG Hamburg* MMR 2013, 725.
24 *LG Hamburg* MMR 2013, 725 mit Verweis auf *LG Hamburg* GRUR-RR 2011, 478 (Ls.) – Runes of Magic Trading.
25 *LG Hamburg* MMR 2013, 725.
26 S.a. der Beitrag von Æxitus der Mönch v. 6.5.2016, abrufbar unter: https://www.youtube.com/watch?v=IcTKEFh8GtQ.
27 *LG Hamburg* MMR 2013, 725: „Insb. ist davon auszugehen, dass es für relevante Teile des Publikums ein Reiz des Spiels ist, mit den anderen Charakteren in der Spielewelt kommunizieren zu können. Es ist zwischen den Parteien unstreitig geblieben, dass ein Bot auf eine Kommunikationsanfrage eines realen Spielers nicht reagieren kann. Bereits unter Berücksichtigung von Lebenswahrscheinlichkeiten werden daher reale Spieler, die „World of Warcraft" kauften, um auch mit anderen realen Spielern zu kommunizieren, verärgert sein, wenn sich unter den Spielercharakteren nicht als solche erkennbare Bots befinden, die auf ein Ansprechen nicht reagieren. Es ist daher insgesamt anzunehmen, dass der Einsatz von Bots für potenzielle Käufer ein Grund sein kann, von dem Kauf eines Spiels abzusehen, und für Spieler ein Grund sein kann, ihr Abonnement zu kündigen, wenn sie von dem Einsatz von Bots in dem Spiel Kenntnis nehmen."
28 *LG Hamburg* MMR 2019, 404.
29 *LG Hamburg* MMR 2013, 725.
30 *OLG Hamburg* MMR 2015, 313, 316 f.: „Der Begriff des „Verleitens zum Vertragsbruch" darf jedoch nicht derart weit ausgelegt werden, dass bereits jedwede auf den Vertrieb gerichtete Tätigkeit gegenüber den gebundenen Adressaten davon erfasst wird (vgl. *OLG Düsseldorf* NJW-RR 2003, 104 zur einfachen Lieferanfrage eines außerhalb eines Vertriebsbindungssystems stehenden gewerblichen Abnehmers bei einem gebundenen Vertragshändler). Die Entscheidung, den Bot zu verwenden, liegt hier nicht bei den Bekl., sondern letztlich beim jeweiligen Spieler. An die Allgemeinheit gerichtete Anzeigen reichen für das Tatbestandsmerkmal des Verleitens in aller Regel nicht aus (*BGH* MMR 2009, 108 – bundesligakarten.de). Da eine über das bloße Angebot der Buddy-Bot hinausgehende Einwirkung auf die Spieler nicht festgestellt werden kann, liegt mithin kein unlauteres Verleiten zum Vertragsbruch vor."

und folglich auch nicht angeboten werden, verleite zum Vertragsbruch. Denn nach den Vertragsbedingungen sei die Verwendung von „Zusatzprogrammen, Skripten oder sonstigen Hilfsmitteln" ausdrücklich untersagt.[31] Wenn für ein Spiel Funktionen angeboten würden, die vom Publisher nur als kostenpflichtige Premium-Funktionen angeboten werden, liege darin zudem eine Rufausbeutung im Sinne eines „Einschiebens in eine fremde Serie".[32] Diese Rechtsprechung ist überholt, nämlich einerseits durch das zitierte Urteil des *OLG Hamburg*[33] und andererseits durch den Umstand, dass der *BGH* die Rechtsfigur des „Einschiebens in eine fremde Serie" ausdrücklich aufgegeben hat.[34]

IV. Ansprüche aus Markenrecht

Publisher von Spielen haben sich auch eines markenrechtlichen Instrumentariums gegen Anbieter von Cheatbot-Software bedient. Die Anbieter bewerben ihren Cheatbot mit Verweis auf das Spiel, in dem der Cheatbot zum Einsatz kommt, also etwa „WOW Bot" sowie „World of Warcraft Bot" (auch in Metatags ihrer Webseite). Das *LG Hamburg* hielt eine solche Verwendung für kennzeichenmäßige Benutzung der Zeichen „WOW" bzw. „World of Warcraft" und für einen Herkunftshinweis.[35] Eine lediglich beschreibende Verwendung liege nicht vor, da keine beschreibenden Zusätze wie etwa „Bot für" benutzt würden.[36] Es bestehe Verwechslungsgefahr. Eine Benutzung sei nicht durch Art. 12 VO (EU) 2017/1001 (Unionsmarkenverordnung – UMV) gerechtfertigt, weil sie gegen die guten Sitten verstoße.[37] Es liege schließlich ein wettbewerbswidriges Handeln vor. Die Entscheidung des *LG Hamburg* wurde vom *OLG Hamburg*[38] und vom *BGH*[39] bestätigt.

V. Ansprüche aus Vertragsrecht

Das *OLG München* hatte einem Publisher von Spielen keinen Anspruch zugesprochen, auf Basis des Vertragsrechts gegen den Verbreiter von Cheatbots vorzugehen.[40] Begründet wurde dies damit, dass die Nutzungsbedingungen, die den Einsatz von Cheatbots untersagten, nicht vertraglich vereinbart worden seien. Es sei zwischen dem Erwerb des Nutzungsrechts an der Client-Software und der Nutzung der Onlinedienste des Publishers zu unterscheiden. Die Verbreiterin der Bots habe aber nur die Client-Software erworben und nicht auch die Geschäftsbedingungen der Nutzung der Onlinedienste des Publishers akzeptiert.[41] Der Publisher habe die Bedingungen gar nicht an Cheatbot-Betreiber gerichtet und diesen gar keinen Vertragsschluss angeboten.[42]

VI. Ansprüche aus virtuellem Hausrecht

Das *OLG München* hat dem Publisher eines Spiels einen Anspruch gegen die Herstellerin von Cheatbot-Software auf Unterlassung der Nutzung ihrer Onlinedienste aus virtuellem Hausrecht analog §§ 903, 1004 BGB zugesprochen.[43] Das virtuelle Hausrecht umfasst die Befugnis des Betreibers eines Forums im Internet, einem Nutzer den Zutritt zu dem virtuellen Raum, also der Seite, auf der das Forum betrieben wird, zu verweigern.[44] Dieses Hausrecht hat das *OLG München* auch auf Onlinespiele angewandt. Aus dem Eigentumsrecht kann der Publisher untersagen, dass Mitarbeiter des Cheatbot-Herstellers sich Zugang zu den Spielen verschaffen[45] (eine Duldungspflicht des Publishers nach § 1004 Abs. 2 BGB besteht nicht[46] und auch keine kartellrechtliche Duldungspflicht[47]). Ein solcher Anspruch ist indes wirtschaftlich nicht viel wert, da der Schaden ja nicht durch den Zugang der Hersteller des Cheatbot zu den Spielen entsteht, sondern dadurch, dass Spieler im Spiel den Cheatbot einsetzen und sich so Spielvorteile verschaffen. Das virtuelle Hausrecht geht nicht so weit, dass man aus ihm einen Unterlassungsanspruch hinsichtlich Herstellung, Nutzung und Verbreitung des Cheatbot ableiten kann.[48] Eine Verwertung der durch den unautorisierten Zugriff auf die Onlinedienste des Publishers erlangten Informationen kann nicht untersagt werden, da eine unter Verletzung des Eigentumsrechts erfolgte Informationserlangung und -verwertung keine Fruchtentziehung darstellt.[49]

VII. Ansprüche aus dem eingerichteten und ausgeübten Gewerbebetrieb

Aus § 823 Abs. 1 BGB unter dem Gesichtspunkt des eingerichteten und ausgeübten Gewerbebetriebs lässt sich der Vertrieb der Cheatbot-Software nicht untersagen. Das Anbieten der Software stellt keinen unmittelbaren, betriebsbezogenen Eingriff in den Gewerbebetrieb des Publishers dar.[50] Es liegt bei den Spielern, ob sie sich an die Spielregeln halten oder unter Verstoß gegen die Spielregeln Cheatbots einsetzen.[51] Die Spieler treten also zwischen den Publisher und den Anbieter der Cheatbots.

VIII. Ergebnis

Es wurde aufgezeigt, dass die Publisher von Spielen erfolgreich rechtliche Wege gefunden haben, um den Vertrieb und die Nutzung von Cheatbots einzudämmen. Es ging dabei nicht darum, den Nutzer der Cheatbots zu treffen, sondern das „Übel an der Wurzel" zu fassen und gegen den Anbieter vorzugehen. Unterlassungsansprüche gegen den Nutzer, der Cheatbots verwendet, ergeben sich regelmäßig wegen eines Verstoßes gegen die Nutzungsbedingungen. Ein solcher Verstoß rechtfertigt die Kündigung des Nutzungsvertrags zwischen Nutzer und Publisher. Markenrechtliche Ansprüche gegen Vertreiber von Cheatbots betreffen die Nutzung der Cheatbots im Zusammenhang mit dem Markennamen des Spiels. Solche Ansprüche können ggf. noch umgangen werden, indem die Cheatbots mit „Bot für XYZ" beschrieben und nicht unter „XYZ Cheatbot" angeboten werden. Die urheberrechtlichen Ansprüche richten sich gegen die Vervielfältigung der Client-Software, nicht dagegen der Cheatbot-Software. Am Wirksamsten sind jedoch die wettbewerbsrechtlichen Ansprüche, da sie sich gegen das Angebot der Cheatbot-Software selbst richten.

Dr. Christian Rauda
ist Fachanwalt für Informationstechnologierecht, Fachanwalt für Urheber- und Medienrecht und Fachanwalt für gewerblichen Rechtsschutz und Partner der Medienrechtskanzlei GRAEF Rechtsanwälte (Hamburg/Berlin) sowie Dozent an der Hamburg Media School, der Bucerius Law School und der HTW Berlin.

31 *LG Hamburg* MMR 2009, 772 (Ls.) = BeckRS 2009, 20232.
32 *LG Hamburg* MMR 2009, 772 (Ls.) = BeckRS 2009, 20232; krit. zum Einschieben in eine fremde Serie: *Rauda*, GRUR 2002, 38 ff.
33 *OLG Hamburg* MMR 2015, 313, 316 f.
34 *BGH* GRUR 2017, 79 – Segmentstruktur.
35 *LG Hamburg* MMR 2013, 725.
36 *LG Hamburg* MMR 2013, 725.
37 *LG Hamburg* MMR 2013, 725.
38 *OLG Hamburg* MMR 2015, 313, 319 f.
39 *BGH* GRUR-Prax 2017, 110 ff.; *Lambrecht*, GRUR-Prax 2017, 91, 92 weist auf Besonderheiten bei den Annexansprüchen hin.
40 *OLG München* BeckRS 2015, 119932.
41 *OLG München* BeckRS 2015, 119932.
42 *OLG München* BeckRS 2015, 119932.
43 *OLG München* BeckRS 2015, 119932.
44 *Maume*, MMR 2007, 620, 622; *OLG Hamm* MMR 2009, 269 – „Hausverbot" im Internet; *OLG Hamburg* MMR 2008, 58 – „Hausverbot" im Internet.
45 *OLG München* BeckRS 2015, 119932.
46 *OLG München* BeckRS 2015, 119932.
47 *OLG München* BeckRS 2015, 119932.
48 *OLG München* BeckRS 2015, 119932.
49 *OLG München* BeckRS 2015, 119932.
50 *OLG München* BeckRS 2015, 119932.
51 *OLG München* BeckRS 2015, 119932.

MMR MultiMedia und Recht

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (verantwortlich für den Textteil); RAin Ruth Schrödl, Redakteurin; Eva Wanderer, Redaktionsassistentin; Maren Otter, Volontärin, Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/381 89-427, Telefax: 089/38189-197, E-Mail: mmr@beck.de

Manuskripte: Manuskripte sind an die Redaktion zu senden. Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag C.H.BECK an seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Peer-Review-Verfahren: Jeder Beitrag wird vor Abdruck von der Schriftleitung und ferner von zwei Gutachtern in anonymisierter Form gelesen und bewertet.

Urheber- und Verlagsrechte: Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Das gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, denn diese sind geschützt, soweit sie vom Einsender oder von der Redaktion erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlags in irgendeiner Form vervielfältigt, verbreitet oder öffentlich wiedergegeben oder zugänglich gemacht, in Datenbanken aufgenommen, auf elektronischen Datenträgern gespeichert oder in sonstiger Weise elektronisch vervielfältigt, verbreitet oder verwertet werden.

Anzeigenabteilung: Verlag C.H.BECK, Anzeigenabteilung, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München.
Media-Beratung: Telefon 089/3 81 89-687, Telefax 089/3 81 89-589.
Disposition, Herstellung Anzeigen, technische Daten: Telefon (0 89) 3 81 89-603, Telefax 089/3 81 89-589, E-Mail anzeigen@beck.de.
Verantwortlich für den Anzeigenteil: Bertram Götz

Verlag: Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Tel.: 089/381 89-0, Telefax: 089/38 18 93 98, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX.

Erscheinungsweise: Monatlich.

Bezugspreise 2019: Jährlich € 429,– (inkl. MwSt.). Vorzugspreis für Mitglieder der davit € 335,– (inkl. MwSt.). Alle Abopreise inklusive Newsdienst MMR-Aktuell und MMRDIREKT. Einzelheft: € 41,50 (inkl. MwSt.); Versandkosten jeweils zuzüglich. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Abonnement und Bezugspreis beinhalten die Printausgabe sowie eine Lizenz für die Online-Ausgabe. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden. Jahrestitelei und -register sind nur noch mit dem jeweiligen Heft lieferbar.

Bestellungen über jede Buchhandlung und beim Verlag. Vertriebskooperation in der Schweiz: Helbing & Lichtenhahn Verlag AG (CH) & Co.KG, Elisabethenstraße 8, CH-4051 Basel, Tel.: +41 (0)61 228 90 70, Fax: +41 (0)61 228 90 71, E-Mail: zeitschriften@helbing.ch.

KundenServiceCenter: Tel.: 089/3 81 89-750, Fax: 089/3 81 89-358, E-Mail: kundenservice@beck.de

Abbestellungen müssen 6 Wochen vor Jahresschluss erfolgen.

Adressenänderungen: Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an. Hinweis gemäß § 4 Abs. 3 der Postdienst-Datenschutzverordnung: Bei Anschriftsänderungen des Beziehers kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen des Heftes beim Verlag widersprechen.

Satz: FotoSatz Pfeifer GmbH, 82152 Krailling.
Druck: Druckerei C.H.BECK, Bergerstraße 3–5, 86720 Nördlingen.
ISSN 1434-596X