

In cooperation
with: **bitkom e.V.**
davit in the
DAV eco e.V.
game e.V.
VAUNET

MMR

MultiMedia and Law

Journal for information, telecommunications and media law

Publisher: 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 Holznapel - Wolfgang Kopf - Prof. Dr. Reto M. Hilty 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 (Ed.)

New ways of law enforcement for games

- | | | |
|-----------------------------------|----|--|
| editorial | 1 | KONSTANTIN EWALD
New ways of law enforcement for games |
| law enforcement | 3 | CHRISTIAN-HENNER HENTSCH
Piracy in the games industry |
| illegal internet offers | 7 | JULIAN WAIBLINGER / STANISLAUS JAWORSKI
Games Piracy - Website blocking as a means of law enforcement |
| principle of exhaustion | 12 | THOMAS MERK / ADRIAN SCHNEIDER
Key selling: Legal limits to the trade with license keys for computer games |
| commercial copyright infringement | 16 | FELIX HILGERT / MARTIN SESTER
Criminal liability for the operation of piracy servers |
| defensive claims | 20 | CHRISTIAN RAUDA
Cheatbots in computer games |

game
Verband der deutschen
Games-Branche

www.mmr.de



Kölnener Forschungsstelle
für Medienrecht
Technology
Arts Sciences
TH Köln

MMR Supplement
8/2019

Pages 1-24
22nd Volume - August 14, 2019
Verlag C.H.BECK Munich



1830201908

In cooperation with:

bitkom - Federal Association for Information Technology, Telecommunications and New Media e.V.

davit in the DAV - Working Group IT Law in the German Bar Association

eco - Association of the Internet Industry e.V.

game - Association of the German Games Industry e.V.

VAUNET - Association of Private Media

MMR

MultiMedia and Law

Journal for information, telecommunications and media law

8/2019 Supplement

PUBLISHERS

Dr. Astrid Auer-Reinsdorff, FA IT-Recht, Berlin/Lisbon/Chairwoman of the Executive Committee of the DAV Working Group on IT Law (davit) - **Prof. Dr. Oliver Castendyk**, MSc. (LSE), Director Allianz Deutscher Produzenten - Film & Fernsehen e.V., Berlin - **Prof. Dr. Nikolaus Forgó**, Professor for Technology and Intellectual Property Law and Director of the Institute for Innovation and Digitisation in Law, University of Vienna - **Prof. Dr. Sibylle Gierschmann**, LL.M. (Duke University), FA Urheber- und Medienrecht, Hamburg - **Prof. Dr. Christian-Henner Hentsch**, M.A., LL.M., Head of Law and Regulation at game - Verband der deutschen Games-Branche e.V. (German Games Industry Association), /Professor for Copyright and Media Law at the Cologne Research Centre for Media Law at the TH Köln - **Prof. Dr. Reto M. Hilty**, Director at the Max Planck Institute for Innovation and Competition, Munich/Ordinarius at the University of Zurich - **Prof. Dr. Dr. Hilty**, Director at the Max Planck Institute for Innovation and Competition, Munich/Ordinary at the University of Zurich - **Prof. Dr. Thomas Hoeren**, Director of the Civil Law Department of the Institute for Information, Telecommunications and Media Law, University of Münster - **Prof. Dr. Bernd Holznapel**, Director of the Public Law Department of the Institute for Information, Telecommunications and Media Law, University of Münster - **Wolfgang Kopf**, LL.M., Head of Politics and Regulation, Deutsche Telekom AG, Bonn - **Prof. Dr. Marc Liesching**, Professor for Media Law and Media Theory, HTWK Leipzig/Munich - **Prof. Dr. Peter Raue**, Raue LLP, Berlin - **Prof. Dr. Alexander Roßnagel**, University of Kassel/Head of the Project Group Constitutional Technology Design (provet) - **Prof. Dr. Joachim Scherer**, LL.M., Baker & McKenzie, Frankfurt a.M. - **Dr. Raimund Schütz**, Loschelder Rechtsanwälte, Cologne - **Prof. Dr. Ulrich Sieber**, Director and Head of the Criminal Law Department of the Max Planck Institute for Foreign and International Criminal Law, Freiburg / Honorary Professor and Head of the Legal Information Centre at the Ludwig Maximilian University, Munich - **Prof. Dr. Louisa Specht**, Holder of the Chair of Civil Law, Information and Data Law, Rheinische Friedrich-Wilhelms-Universität Bonn - **Dr. Axel Spies**, Morgan, Lewis & Bockius LLP, Washington DC - **Prof. Dr. Gerald Spindler**, University of Göttingen

SCIENTIFIC ADVISORY BOARD

Daniela Beaujean, Member of the Executive Board, Legal Affairs and Regulation, Association of Private Media (VAUNET), Berlin - **Dietrich Beese**, Hamburg - **Prof. Dr. Herbert Burkert**, Research Centre for Information Law, University of St. Gallen - **Susanne Dehmel**, Member of the Executive Board, BITKOM e.V., Berlin - **Jürgen Doetz**, Coordinator of the German Content Alliance, Berlin - **Dr. Andrea Huber**, LL.M. (USA), Managing Director, ANGA Association of German Cable Operators, Berlin - **Dr. Christine Kahlen**, Head of Public Relations, Federal Ministry of Economics and Technology, Berlin - **Dr. Christopher Kuner**, J.D., LL.M., Senior of Counsel, Wilson Sonsini Goodrich & Rosati, LLP, Brussels - **Prof. Dr. Wernhard Möschel**, Chairman of the Scientific Advisory Board of the BMWi/ Chair of Civil Law, Commercial and Economic Law, University of Tübingen - **Robert Queck**, Maître de Conférences, Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium - **Prof. Dr. Eike Ullmann**, Judge of the First Civil Senate of the Federal Court of Justice (retd.), Karlsruhe

EDITING

Anke Zimmer-Helfrich, Chief Editor –

Ruth Schrödl, Editor –

Eva Wanderer, Editorial Assistant

Wilhelmstr. 9, 80801 Munich, Germany

EDITORIAL New ways of law enforcement for games

Reading time: 8 minutes

It's time again: *gamescom*, the world's largest event for computer and video games, will take place for the 11th time, starting August 20, 2019, and once again inform about the latest trends in the computer and video games industry. The innovative strength and economic growth of the industry are still breathtaking.

The market for computer games is expected by leading analysts to grow to around US\$ 150 bn in 2019. A particular revenue driver here is the mobile games segment, i.e. the games that we play on our smart phones and tablets. While in the beginning it was the so-called casual games like "Candy Crush" that dominated the market. Since the impressive success of games like "Fortnite" or "PlayerUnknown's Battlegrounds", though, it has become clear that we will also play games on mobile devices which are more advance in terms of content and technical requirements.

On the technical side, it is becoming apparent that after the great success of games such as Pokemon Go, further Augmented Reality (AR) titles will be launched and this technology will continue to assert itself. The same applies to virtual reality (VR) applications. The player needs VR-Headsets to experience virtual worlds. While these new VR consoles spread more slowly than expected, the release of new VR models has set up the conditions for these new game consoles to find their way into our living rooms. And by the way: VR applications are also creating a segment in which game developers and classic industries, such as the automotive industry, plant construction, logistics or healthcare, are increasingly working together.

The market is increasingly characterized by new forms of distribution. A growing number of online distribution platforms is opening up new digital distribution channels for game providers. The consumer is happy about more competition as well. What is new is that games can now increasingly be consumed via online stream. The games industry is finally following what the film industry has done with Netflix & Co.

The introduction of the Games Fund, which will promote the development of computer and video games nationwide for the first time, is of particular importance for the German market. The amount of € 50 m has been allocated for this purpose in the federal budget for 2019, and the *Federal Ministry of Transport and Digital*



Konstantin Ewald

Infrastructure is responsible. As a result of a first early measure, applications for de minimis aid of up to € 200,000 per company in three years can be submitted since June 2019 (FAQ on de minimis aid, available at: <https://www.game.de/faq-deminimis-foerderung/>).

For those interested in games law, it is important to stay up to date with these new technical and economic trends. Questions resulting from this are for example whether AR or VR applications are permitted under copyright law to record and evaluate their environment, and which data may be collected and processed. These can only be legally discussed if the underlying technology has been understood. The same applies to the discussion already underway regarding a possible reformation of German youth media protection, which is still very much oriented towards the physical form of games distribution.

MMR is determined to be a scientific platform for gaming law articles and to publish articles with the intent to start discussions of these new legal issues. In August 2018, for example, the first MMR supplement focusing on eSport was published. The main topic of this year's supplement is: "New ways of law enforcement for games".

Christian-Henner Hentsch will commence with an explanation of the business models of the games industry and give an overview of new challenges. *Julian Waiblinger* and *Stanislaus Jaworski* will then deal comprehensively with blocking of websites in the games industry. *Thomas Merk* and *Adrian Schneider* have chosen a highly relevant topic for prosecution.

They assess the legal admissibility of selling keys, i.e. the isolated sale of product keys for computer games. This is followed by the contribution by *Martin Sester* and *Felix Hilgert*, which illuminates pirate servers from a criminal law perspective. *Christian Rauda* analyzes the admissibility of cheatbots in computer games.

All these topics will also be the subject of the scientific discussion at the *Video Game Bar Association's (vgba)* – the leading event for gaming lawyers in Europe - which will also take place this year. The *vgba summit* (www.vgbaeurosummit.org) will take place on August, 19 2019 for the first time as part of the developer fair *devcom* also on the exhibition grounds in Cologne immediately prior to *gamescom*.

We hope that the articles in this supplement will provide MMR readers with further valuable insights into the legal issues of the games industry. We thank the publishing house C.H.BECK and especially Mrs. Anke Zimmer-Helfrich, chief editor of MMR, for the constructive cooperation.

Cologne, August 2019



Konstantin Ewald

is a lawyer at Osborne Clarke and operator of the blog www.spielerecht.de on legal issues of the gaming industry.

CHRISTIAN-HENNER HENTSCH

Piracy in the games industry

An overview of business models and challenges

law enforcement

New business models and distribution channels in the games industry are also changing the challenges and opportunities in the fight against piracy. The classic sale model of computer games on data carriers or as downloads usually involves a technical copy protection because it is bound to an account. Selling keys for used games, which is a legal grey area, entails distortions in pricing - with advantages and disadvantages. In addition, free-to-play games and subscriptions face problems of illegal trading, bots and pirate servers. Especially for consoles,

structurally illegal platforms remain a major piracy problem because anyone can download games and software to bypass security programs there. Procedures blocking access to websites are of particular interest in this respect for games companies. For most approaches, civil law has become the means of choice. Criminal law on the other hand is promising with regard to pirate servers, but is increasingly losing its importance for the games industry in the prosecution of copyright infringements.

Reading time: 19 minutes

I. Introductory Remarks

Game - Verband der deutschen Games-Branche e.V. - decided at its latest general meeting to terminate its membership in the *Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU)* by the end of 2019. This decision comes at the end of a year-long evaluation process that began even prior to the Hollywood studios leaving in summer of 2018. After repeated membership discussions and intensive discussions and negotiations with *GVU*, the games industry will now break new ground - and is of course open to new partnerships and projects. The termination of the *GVU membership* does not mean, however, that piracy no longer affects the games industry. It rather is an expression of the changed business models and new approaches to combating piracy.

When the *GVU* was founded in 1985, its main purpose was to prosecute the mass production of illegal copies on physical media such as the VHS video cassette. The main drivers for the games industry to join *GVU* were console manufacturers such as *Sony* and *Nintendo*, who wanted to take action against mass pirated copies and manipulated consoles on which these pirated copies could be used. For these challenges, the most promising approach at that time was criminal law, because it made seizures of physical pirated copies possible and deterred the organized pirated copying scene.

The distribution channels for computer games have meanwhile become much more diverse and, more importantly, more digital. The business models of the games industry have changed considerably as a result. This is associated with new challenges for the industry in the fight against piracy. These changes, their influence on piracy models and the possible protective measures and approaches to prosecution, will be highlighted in the following article.

It focuses on the business models and provides an overview of the challenges and possible approaches to law enforcement in civil and criminal law. The details of the legal framework, concrete procedures and the relevant case law will be discussed in detail in this supplement's articles by

Merk/Schneider on selling keys, by *Waiblinger/Jaworski* on blocking websites, by *Hilgert/Sester* on piracy servers and by *Rauda* on bots. This article in general, and the following articles in particular, will I.E. highlight what role criminal law and civil law play today in law enforcement for gaming.

II. Box Products and Digital Downloads

The computer games industry is a rapidly growing media industry with diverse and innovative business models. In 2018, sales in Germany rose by 9% to more than €4.4 billion.¹ About a quarter of the turnover - €1.081 billion - is generated by the sale of games with a physical carrier medium and/or a key in a box (box product) or the digital download of a game. These include so-called AAA productions (triple A), some of which require several 100 million euros in development costs, as well as indie games, some of which are marketed by students and university graduates.

In addition to retail, the most important distribution channels are digital distribution platforms for PC, such as Steam and the Epic Games Store, the stores on *Microsoft's*, *Nintendo's* and *Sony's* consoles, company-owned stores such as Uplay by *Ubisoft* or Origin by *EA*, and of course the Google Play Store and Apple's App Store. The prices range between a few cents in the App Stores and around €60,- for so-called full price games. Such games are often cross-financed by premium models with certain advantages, paid DLCs (downloadable content), online passes for playing in multiplayer mode or other forms of recurring payments. These latter sources of income are disregarded in this first section and are considered separately as in-game purchases.

1. Technical copy protection

Manufacturers of computer games have always used technical copy protection measures to protect themselves against unauthorized copies of their works. In comparison to the first protection programs, today's encryption technologies have become so advanced that decryption - "Cracking" - can only be done by professionals and it takes proportionally more time for a game to become compromised. As a result, the first evaluation phase, which is essential for refinancing the game, is covered.

¹ Cf. turnover figures of *game*, available at: <https://www.game.de/marktdaten/>.

In addition, there are security applications such as password queries, serial numbers, dongles and hardware-based licenses and regional codes for data carriers as well as activation codes for downloads.

This has led to a significant reduction in the illegal use of computer games. The user-friendly offers in closed systems - on consoles or smartphones - also contribute to this effect. Legally acquired content can now be used on all devices and is easy to apply, while cracked games have to be laboriously created or illegally acquired with a certain IT expertise, and many restrictions reduce the gaming experience. In light of this, technical copyright protection has become more promising and can additionally be applied globally. The focus in this field has shifted from criminal prosecution against burners and cracker collectives to offensive copy protection and user-friendly offers.

2. Notice and take down

However, illegal cracked offers and bypass software continue to exist on structurally illegal platforms. That is why most major publishers have always hired their own service providers for Notice-and-Take-Down (NTD) measures. Due to their global distribution, this is generally not carried out on a national basis but is given to a single central provider. Synergies such as those of the film studios with their *Alliance for Creativity and Entertainment (ACE)*² initiative are difficult to achieve because different requirements must be met depending on the distribution platform, the technical copy protection and the distribution range. Nevertheless, following the example of the British association *UKIE*, there are also efforts in Germany to conclude framework agreements with NTD providers. Criminal investigations against operators of structurally illegal websites such as *kinox.to* are desirable from the point of view of the industry but are also lengthy and costly. In this respect, quick take-down measures are preferable if successfully applicable.

3. Site blocks

It is precisely because NTD measures in Germany and other European countries run smoothly that structurally illegal platforms and the underlying illegal services are now found almost exclusively abroad, and it is usually not possible to identify those responsible. This leads to the fact that both civil law and criminal law connection points for these violations of rights are missing. Therefore, the games industry follows the current side blocking procedures with great interest.³

The *BGH's* decision on the computer game "Dead Island 2"⁴ made it clear that side blocks can also be relevant for games. Especially in combination with technical copy protection measures, a consistent site block can protect the first evaluation phase in the long term. This makes blocking websites a good supplement to the civil law instruments used to date. In order to meet the requirements for the imposition of a block, it must be proven that the site is structurally illegal and that the operators and their service providers (e.g. host providers) were unsuccessfully approached. This urgently requires an institution such as *GVU* or a comparable service provider who has the relevant data and can carry out the necessary investigations.

4. Key selling

A challenge still quite specific to games is key selling, i.e. the resale of "used games". Usually, box products are now also sold with an activation key, often even without a data carrier, as in the case of digital downloads. The creation principle of Sections 17 (2) and 69c no. 3 UrhG applies to mere software: A computer program placed on the market within the European Economic Area (EEA) by way of sale may also be freely resold within the EEA provided that the right holder has obtained an equitable remuneration and the seller destroys his own copy.⁵ In the opinion of the *BGH*, this also applies if the key and installation DVD are split.⁶

Computer games are not pure software in the sense of the above-mentioned jurisprudence but rather a mix of different technical and, above all, artistic elements. Case law speaks of so-called "hybrid works"⁷ to which the case law on pure software (such as business software) does not apply. The exception for "used software" has therefore not yet been transferable to computer games. The *ECJ* case of "Tom Kabinet" (Case C-263/18) is interesting in this regard as to the extent the principle of exhaustion also applies analogously to eBooks or works protected by copyright. The games industry, the book industry and other content industries have concurrent interests here and face common challenges.

In practice, however, key-selling platforms such as G2A, Gamesrocket and Kinguin on which millions of computer games are traded are already established in the games sector. In addition to the mandatory sales tax payment, provisions for the protection of minors and possible misleading advertising, the problems of money laundering and fraud, e.g. when keys are purchased with stolen credit card data and resold on these platforms, are also becoming increasingly important.

For this reason alone, the principle of exhaustion does usually not apply in these cases: If the right holder has been fraudulently deprived of the possibility of obtaining an appropriate remuneration for the key sold, the conditions for exhaustion are not met. The burden of proving that the conditions for exhaustion are met lies with the key-seller.⁸ He must prove that the key sold was placed on the market within the EEA and paid for in full. In practice, however, there is almost no comprehensive proof of origin for unauthorized key-selling platforms.

Under this pressure, key sellers have now also adapted their business models and engaged in "whitewashing". If they comply with the legal requirements and prevent money laundering and fraud on their platforms, they increasingly present themselves as partners for some publishers and their marketing departments. This sales channel allows for larger quantities to be sold at a stroke, especially at the beginning or end of an evaluation phase. In addition, this establishes an alternative to nearly monopolistic distribution platforms. It

² Available at: <https://www.alliance4creativity.com>.

³ To this end, exec. *Waiblinger/Jaworski*, MMR-Beil. 8/2019, 7 - in this issue.

⁴ *BGH* MMR 2018, 811; see *Nordemann*, GRUR 2018, 1016: Liability of general access providers for website blocks. The current status according to *BGH* "Dead Island".

⁵ *ECJ* MMR 2012, 586.

⁶ *BGH* MMR 2015, 735.

⁷ *ECJ* MMR 2014, 401.

⁸ *BGH* MMR 2014, 232 comments by *Heydn* - UsedSoft II.

therefore remains to be seen whether the originally rather infringing business model of key-selling will perhaps develop into a legal sales channel supported by the industry.

5. Interim conclusion

A closer look at box products and digital downloads shows that the games industry faces similar challenges as other content industries in terms of technical copy protection measures, NTD and site blocking and, in some cases, key selling, and pursues comparable approaches.

Due to the medium, however, the distribution is already much more digital and can be better protected due to the account being connected and other measures. Nevertheless, criminal law only plays a subordinate role in all approaches. Civil law claims against content, host providers and, in future, also against service providers are paramount for law enforcement here.

III. In-game Purchases

A still quite games-specific source of refinancing are so-called in-game purchases. In 2018, €1.949 billion was generated, which corresponds to almost double the sales volume of games. This sector has been growing rapidly for years, by 28% last year alone.⁹

In-game purchases are particularly common in free-to-play (F2P)¹⁰ games. The game is made available free of charge; costs may arise exclusively for additional content. This particularly applies to the numerous mobile games which are offered exclusively in digital form. In-game purchases are also increasingly being integrated into full-price games in order to tap into additional sources of income and thus refinance the rapidly rising production costs for AAA-titles.¹¹

A particularly interesting aspect, especially with eSports titles, is the extension of the evaluation phase. Revenues are also generated here after the game has already been bought. The offers include both purely decorative additional content (so-called "Skins" such as armor or eye-catching clothing), as well as additional functional content that provides in-game advantages (especially weapons or characters).¹²

A special form of in-game purchases are so-called lootboxes in which randomly selected content can be bought for money - just like in a KINDER Surprise.¹³ This area of in-game purchases, which meanwhile accounts for the largest share of sales in refinancing games, is relatively unaffected by piracy. Because of connection to an account and the deposited payment data, a crack in the game is almost impossible. Instead there are new ways to illegally make money out of in-game purchases, to bypass or even hijack them.

⁹ Cf. <https://www.game.de/9-prozent-im-plus-deutscher-games-markt-wachstum-2018-deutlich/>.

¹⁰ About the term: *Mankowski*, in: Fezer/Büscher/Obergfell, unfair competition law: UWG, 3rd ed. 2016, vol. 1, second part, page 12, chapter M, para 293a.

¹¹ The production budget for AAA productions has increased immensely, especially for open world games, and now often amounts to several 100 million euros. In order to keep the price for a full price game constant at approx. € 60,-, a cross-financing by players who can/would like to spend more has been strived for.

¹² See also *Fischer*, CR 2014, 588.

¹³ To the Lootbox Debate *Nickel/Firehake/Schelinski*, MMR 2018, 586.

¹⁴ *OLG Hamburg* MMR 2013, 453.

¹⁵ For more information, see <https://spielrecht.de/olg-hamburg-verbot-eines-goldseller-forums-fulltext/>.

¹⁶ See <http://www.taz.de/Gluecksspiel-im-Internet/!5325377/>.

¹⁷ Cf. <https://spielrecht.de/virtuelle-waehrungen-social-gaming-und-esports-im-fokus-der-gluecksspielregulierung/>.

¹⁸ On this *Rauda*, MMR-Beil. 8/2019, 20 - in this issue.

¹⁹ More about the case *Hilgert/Sester*, MMR-Beil. 8/2019, 16 - in this issue.

1. Trade in in-game-currency or virtual goods

Trade with virtual goods in the game and on platforms outside the game is obvious. Although this is not piracy in a strict sense, it does at least indirectly deprive the provider of income because the virtual goods are no longer bought for money. Therefore, trading in in-game-currency or virtual content is usually prohibited in most terms and conditions. This has been confirmed by the *OLG Hamburg*¹⁴ for the operation of a platform trading in-game-currency, insofar as trading in virtual goods is expressly excluded in the T&C.¹⁵

This procedure is not only important for reasons of financing interest, but also to counter the danger of so-called skin gambling or skin betting, in which purchased virtual goods are deposited as leverage in online casinos. Dragon pattern skins for sniper rifles in the tactical shooter CS:GO e.g. are traded on the black market for virtual goods for €1.000,-.¹⁶ Virtual goods are thus increasingly developing into a billion-dollar crypto currency. Problems with gambling law and other legal problems aside, publishers also take strong action against such platforms out of their own interest.¹⁷ In all these cases the gaming company cannot rely on criminal law, but instead on contract law, competition law and also trademark law.

2. Bots

Bots are another challenge with in-game purchases. With such computer programs, which carry out actions independently, virtual gold or other virtual goods can be collected ("farmed" or "looted") automatically. Because these goods can be exchanged or sold in the game for in-game-currency, the player's incentive to spend money as well as the refinancing possibilities for the game's company are reduced. There are numerous possibilities to take civil action against the unauthorized use and distribution of such bots through contract law, copyright law, trademark law and the German law against unfair competition.¹⁸

3. Pirate servers

One possibility to tap into in-game currency are so-called pirate servers (or P-servers), which clone the server of a freely available game, offer it on their own server and thus generate revenues that would otherwise be generated on the original server. This is a copyright infringement that can be prosecuted under both civil and criminal law.

Karlsruher publisher *Gameforge* and the *GVU* initiated proceedings before the *AG Heidelberg*. From 2014 to 2016, an adolescent operated two pirate servers for the online role-playing game "Metin2", on which at times several hundred thousand players were registered. The perpetrator and his helpers made six-figure profits by selling virtual objects and skills.¹⁹ Pirate servers can be prosecuted by means of civil and criminal law; criminal law proceedings are to be preferred, however, because of the potential levies the criminal law provides.

4. Interim conclusion

The games industry has opened a wide range of new business models and is frequently breaking new legal ground in the area of in-game purchases. Due to the structure of the business model, it often is no longer a question of technical copy protection, but of contractual provisions - especially in view of the trend towards "games as a service". Thus, it is no longer content that is sold, but rather the participation in the fun of gaming.

Accordingly, copyright law is only conditionally suitable for law enforcement; instead, one should claim under contract and competition law.

As a consequence, criminal law often runs empty and therefore law enforcement in the games industry is increasingly shifting to civil law. Especially against the background of stagnating revenues from the sale of games and rapidly increasing revenues from in-game purchases, this trend will intensify.

IV. Fees for Online Services

The fees for online services are currently developing as a new pillar in refinancing of computer games. In 2018, revenues from them have almost doubled to €353 million.²⁰ Such paid online services on gaming consoles include services such as Nintendo Switch Online, PlayStation Plus and Xbox Live Gold. The scope of these services includes the ability to play online with and against each other and to save your progress in the cloud. The offer often also includes free access to changing computer and video games as well as discounts for the purchase of games and extensions in the online stores of the various platforms.

Other online services such as Origin Access or Xbox Game Pass allow players to access a large catalog of games for a fixed monthly fee, which they can then install on their gaming consoles and/or PC. Other offerings such as PlayStation Now from Sony, on the other hand, rely on cloud gaming: no powerful gaming PC neither the latest gaming console is required. The actual calculations of the game take place in the providers data center. This means that even blockbuster titles with elaborate graphics can be played on low-power devices. What is required, however, is a fast and low latency internet connection. Google only recently announced such a cloud gaming service called "Stadia".

In view of the current developments in cloud computing, further growth in online services can be expected in the coming years.

1. Cloud gaming

Cloud gaming is the consistent next step towards the idea of "games as a service", because the player no longer needs a copyright license, but only pays for access to the game. This means that the user no longer is in contact with copyright law and, as a result, copyright infringements are virtually excluded. In this respect, there probably will be no more investigations for criminal violations of copyright.

2. Sale of user accounts

With all online services, selling accounts has to be considered. This already takes place with browser games or the game sales platform Steam, for example. According to the established case law²¹, it is permissible to prohibit the sale of accounts in the corresponding general terms and conditions.²² In the present case, the *Kammergericht* expressly states that it is not a question of the right to retransmit the game under copyright law because the creation and use of an account does not involve a purchase. With a Steam user account, it rather depends on the services offered there, such as achievements, which are displayed there. This case law has so far only affected the holder of the license. It remains to be seen whether platforms that organize the sale of accounts can also be prosecuted by gaming companies and whether the civil law or perhaps even the criminal law approach would be more promising.

V. Conclusion

Ultimately, it can be stated that in the sale of computer games, the classic fight against piracy with technical copy protection, take-down notices, site blocking and copyright proceedings against key sellers continues to play an important role. Side blockings in particular could prove to be an effective new instrument in the fight against structurally illegal platforms.

It can be said for the fight against piracy that criminal law is usually no longer the means of choice. In addition, refinancing via sales is losing importance as the industry's revenues are shifting to new fields such as in-game purchases and online services, which now account for more than two-thirds of total revenues from computer and video games. Copyright law and especially criminal law play only a subordinate role here. The German law against unfair competition and the General Terms and Conditions are becoming much more important for contractual claims. The games industry and its new business models are consequently moving more and more away from the classic fight against piracy and are often forced to take new paths in law enforcement.



Prof. Dr. Christian-Henner Hentsch, M.A., LL.M., is Head of Law and Regulation at game - Verband der deutschen Games-Branche e.V. and Professor for Copyright and Media Law at the Cologne Research Centre for Media Law of the TH Köln as well as co-editor of the MMR.

²⁰ Available at: <https://www.game.de/umsatz-mit-online-diensten-fuer-gamer-hat-sich-innerhalb-eines-jahres-nahezu-verdoppelt>

²¹ KG MMR 2016, 340; *similar* BGH MMR 2010, 771 comments by Heydn - Half-Life 2.

²² See also Rauda, *Recht der Computerspiele*, 2013, para. 797; for more details visit <https://spielerecht.de/kg-berlin-erneut-unuebertragbare-nutzeraccounts-bei-steam-sind-zulaessig/>.

Games Piracy - Website Blocking as a Means of Law Enforcement

Efficient blocking measures and presumption of urgency

Illegal Internet Offerings

Internet piracy is also for the games industry a major challenge. There are many structurally illegal Internet offers that make computer games illegally accessible to the public. In prosecution, rights holders are usually confronted with the fact that it is impossible to identify the operators of such piracy websites. Any action against the service providers of these sites is usually hopeless too, since they are mostly located abroad and frequently exchanged between operators. Copyright law, however, provides copyright

holders the opportunity to take action against general internet access providers by block structurally illegal piracy websites. In view of the existing case law, this article examines the legal basis on which blocking decisions against general internet access providers are possible and the particular challenges that exist for the successful assertion of such claims under German copyright law.

Reading time: 25 minutes

I. Introductory Remarks

Internet piracy affects not only the film, music and publishing industries, but also the games industry. The range of websites that deliberately make games available to the public in a way that violates copyright law is hardly manageable. BitTorrent pages, where users illegally exchange files, continue to play an important role for games.¹ These structurally illegal sites are operated anonymously. The host providers of the sites are often located in non-EU countries; they can also be changed as required (so-called hosting nomadism). An action against the operators of the sites or their host providers is therefore usually hopeless.

As a last resort of law enforcement, the only remaining rights holders are therefore to make use of general internet access providers to block the illegal web pages. Possible blocking measures include DNS and IP blocking. While a few judgements have already been passed in Germany on website blocking by rights holders in the film, music and publishing sectors, there is no judgement on the blocking of an illegal games portal. However, the copyright law also offers the possibility of website blocking against general access providers for rights holders in the games industry, as shown below.

II. Case Law Development on Website Blocking

1. Art. 8 (3) of Information Directive and ECJ: UPC Telekabel

While website blocking has been part of day-to-day business in other EU member states for years - for example in Denmark, Great Britain, Ireland or Portugal -,² blocking proceedings against general access providers have only recently come to the fore in German jurisdiction; this is despite the fact that the ECJ's landmark decision in the "UPC Telekabel"³ case had already laid the foundation for website blocking against general access providers in 2014.

The ECJ had affirmed blocking claims against access providers that only grant neutral and passive access to the internet on the basis of Art. 8 (3) of the Info Directive.⁴ In the light of the fundamental rights of all parties concerned, blocking claims can be considered if internet users are not unnecessarily deprived of the possibility of lawfully gaining access to the information available; blocking must also prevent or at least make unauthorized access to protected works more difficult and reliably prevent internet users using the services of the addressee of the order from accessing the subject-matter of protection made available to them in violation of intellectual property rights.⁵

2. BGH: Liability of the access provider for interference

Referring to the requirements of European law, the *Bundesgerichtshof (BGH) - Federal Court of Justice of Germany* - subsequently confirmed in its decision "Liability of the Access Provider for Interference"⁶ that access providers can be held accountable for website blocking. Art. 8 (3) of the Info Directive was thus transposed into German law by the BGH by way of "Störerhaftung" – Liability for interference. Even though the decision in question was ultimately not in favor of the rights holders, the way was paved for website blocking proceedings in Germany as well.

According to the judgement, general access providers should only be liable in a subsidiary way. Rights holders must then have made reasonable efforts to take action against those parties who committed the infringement themselves or who contributed to the infringement by providing services.⁷ BGH expressly mentions the operators of the website

¹ See for example the EU Commission's "Counterfeit and Piracy Watch List" of 7 December 2018 with illustrative examples, available at: http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf.

² See also J. B. Nordemann, GRUR 2018, 1016 m.w.Nw. from the European Rspr.

³ ECJ MMR 2014, 397 comments by Roth - UPC Telekabel/Constantin Film et al. - kino.to.

⁴ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (hereinafter referred to as "the Directive"). For other intellectual property rights, blocking claims can be based on Art. 11 clause 3 of Directive 2004/48/EC on the enforcement of intellectual property rights (hereinafter "Enforcement Directive").

⁵ ECJ MMR 2014, 397 para 42 ff. comments by Roth - UPC Telekabel/Constantin Film and others - kino.to.

⁶ BGH MMR 2016, 180 comments by Finger - Liability of the access provider for interference.

⁷ BGH MMR 2016, 180 para 83 ff. comments by Finger - Liability of the access provider for interference.

concerned and its host provider. They are much closer to the infringement than those who only provide general access to the internet. The assertion of claims against access intermediaries can only be considered from the point of view of proportionality if claims against the operator of the website lack any prospect of success and would therefore otherwise create a legal protection gap.

How far rights holders have to go in concrete terms in order to comply with the requirements for subsidiarity is not clear from the decision. Regarding the procedure for determining the identity of the operators of the website in question, the *BGH* considers in particular the involvement of the Federal investigating authorities by way of criminal charges or, alternatively, conducting private investigations through a detective or a provider of such services.⁸ It will certainly not be possible to overstretch the requirements for rights holders (analogous to the requirements under Section 7 (4) TMG, see below). Generally, enforcement attempts under civil law abroad are to be avoided.⁹

3. TMG amendment 2017 and the Munich judgements on "Kinox.to"

Although an "abolition of "Störerhaftung" was often pronounced in connection to the TMG Amendment 2017¹⁰, a German film rights holder achieved the first blocking order against a German internet access provider by the beginning of 2018 - on the basis of Störerhaftung. *LG München I* (*Munich Regional Court*), for instance, sentenced the internet access provider *Vodafone* to block the "Kinox.to" website, which unlawfully makes thousands of feature films and TV series publicly available.¹¹ The *OLG München*, the *Munich Higher Regional Court*, confirmed that decision.¹²

Under Section 8 (1) clause 2 TMG, introduced by the 2017 amendment to the TMG, claims against all access providers are excluded; the wording of the provision covers not only wifi providers but also general access providers. However, Section 7 (4) of the TMG also introduced a new blocking claim which, according to its express wording, only targets wifi providers. In view of this situation, blocking claims against general access providers no longer seemed to exist. However, the *LG München I* and the *OLG München* recognized that an exclusion of blocking claims against general access providers is not compatible with Union law. After a detailed analysis of the regulatory material of the TMG Amendment 2017, the *OLG München* came to the conclusion that Sec. 8 (1) clause 2 TMG should be reduced teleologically to the effect that the provision only refers to access providers that are also wifi providers.¹³ Claims against general access providers were not excluded by the TMG amendment 2017 according to this reading.

4. BGH: Dead Island - blocking claims according to Sec.7 (4) TMG analogous

With the "Dead Island"¹⁴ decision, *Bundesgerichtshof* seems to have also abandoned interference liability for general access providers. The case concerned the computer game "Dead Island", which was illegally offered for download via online filesharing. The owner of the exclusive usage rights to Dead Island made claims against the operator of several publicly accessible wifi hotspots as well as a wireless access to the gate network (gate exit nodes).

The *BGH* ruled that the right to block under the new Sec.7 (4) TMG claims can not only be made against wifi providers but also access providers to wireless internet connections. Excluding claims in accordance with Sec. 8 (1) clause 2 TMG

Does not only benefit wifi providers but all access providers.¹⁵ However, as this is not compatible with the requirements for blocking claims under Union law (Article 8 (3) of the Information Society Directive and Sec. 11, third clause, of the Enforcement Directive), the new blocking claim under Article 7 (4) of the German Telemedia Act (TMG) is to be further developed in accordance with the Directive in such a way that it also applies to access intermediaries who provide access to the internet not via wifi but by other means.¹⁶

Claims on website blocks against general access providers can therefore be based analogously to the *BGH* "Dead Island" judgement on Sec. 7 (4) TMG. A current decision of the *LG München I* confirms the application of Sec.7 (4) TMG analogously as a basis for claims (more on this hereinafter).⁷ The previous solution of the *Munich courts* concerning a restrictive interpretation of Sec.8 (1) clause 2 TMG will therefore probably no longer play a role in practice, although it was preferable to the analogous application of Sec.7 (4) TMG.¹⁸ The following section outlines the requirements for blocking claims against general access providers under Sec.7 (4) TMG analogously.

5. Current judgement of the LG München I in "Goldesel.to" case

In the above-mentioned current decision of the *LG München I*, the *court* condemned the access provider *Deutsche Telekom* to block the illegal portal "Goldesel.to", through which especially music titles are made illegally accessible. The proceedings conducted by the music industry mark the first court judgement to grant blocking claims against a general access provider on the basis of Section 7 (4) of the German Telemedia Act (TMG).¹⁹

III. Eligibility Requirements of Sec.7 (4) TMG analogous

1. Problems with claims against an internet access provider by its users

Sec.7 (4) clause 1 TMG requires, by analogy, that a media service, such as an internet access provider, is used by a user in order to infringe the intellectual property rights of another user. The services of an internet access provider are used by its users when they visit piracy websites in order to download computer games protected by copyright and to reproduce them without permission (Section 16 UrhG(German Copyright Law)). Users of piracy websites may not invoke the private copying exception (Section 53 (1) UrhG).²⁰

The criticism of this element of the offence is that, according to its wording, it limits the scope of application of blocking

⁸ *BGH* MMR 2016, 180 para 87 comments by *Finger* - Liability of the Access-Provider for interference.

⁹ *Leistner/Grisse*, GRUR 2015, 105, 107 f.; *J. B. Nordemann*, in: *Fromm/Nordemann*, Copyright, 12th ed. 2018, Sec. 97, para 171a.

¹⁰ 3. TMGÄndG of 28.9.2017 (hereinafter referred to as "TMG Amendment 2017").

¹¹ *LG München I* MMR 2018, 322 comments by *Sesing/Baumann*.

¹² *OLG München* MMR 2018, 832 - Access provider's liability for breaches of copyright - Kinox.to.

¹³ *OLG München* MMR 2018, 832, para. 41 - Access provider's liability for breaches of copyright - Kinox.to.

¹⁴ *BGH* MMR 2018, 811 - Dead Island; see *J. B. Nordemann*, GRUR 2018, 1016 and *Spindler*, GRUR 2018, 1012.

¹⁵ *BGH* MMR 2018, 811 paragraph 45 - Dead Island.

¹⁶ *BGH* MMR 2018, 811 paragraph 46 et seq. - Dead Island.

¹⁷ *LG München I* MMR 2019, 535 comments by *Müller*; previously similarly decided *LG München I*, U. v. 21.9.2018 - 21 O 11606/18; *OLG München* MMR 2019, 317 comments by *Rehart* - with several references to Sec. 7 Abs. 4 TMG.

¹⁸ *J. B. Nordemann*, GRUR 2018, 1016, 1018.

¹⁹ *LG München I* MMR 2019, 535 comments by *Müller*.

²⁰ See *ECJ* MMR 2014, 679 para 41 - ACI Adam/Stichting de ThuisKopie.

claims to infringement of intellectual property rights. In the area of computer games, this is not a problem, since computer games are protected by copyright and therefore illegal downloading constitutes a violation of intellectual property rights. In principle, however, a plea should be made for a more detailed interpretation of Section 7 (4) clause 1 of the German Telemedia Act (TMG), as otherwise intolerable valuation contradictions would arise.²¹ According to the mere wording of the provision, victims of violent and sexual crimes, for example, are not entitled to the blocking of websites on which videos of the respective crimes can be accessed.

2. Subsidiarity ("no other option")

As already mentioned, the *BGH* had established a subsidiarity criterion for the liability of general access providers in the decision "Interference liability of the access provider".²² The TMG amendment 2017 has adopted this: Pursuant to Sec. 7 (4) clause 1 TMG, blocking claims against internet access providers require that the right holder has no other option to remedy the infringement. This fact must be read in view of the history of the law as well as the legal and constitutional requirements of the Union.

The legislator has clearly stated that "no other option" such as the subsidiarity feature of "Störerhaftung" (Breach of Duty of Care) (not mentioned by the *BGH*) is to be understood: "The right holder must first have made reasonable efforts to take action against those participants who - like the operator of the internet site - have committed the infringement themselves or - like the host provider - have contributed to the breach of law through the provision of services. The use of the access intermediary is only reasonable if the use of these participants fails or if it lacks any prospect of success and would therefore otherwise create a legal protection gap. When determining the parties to be given priority, the rights holder shall carry out investigations to a tolerable extent."²³

This justification is largely based literally on the corresponding statements of the *BGH* in the case of the access provider's "Störerhaftung" (Breach of Duty of Care).²⁴ It thus depends on "reasonable efforts". Consequently, the 'no other option' criterion must be interpreted in consideration of proportionality. The *BGH* has already assumed this with regard to blocking claims under Störerhaftung.²⁵

It would also be incompatible with the objectives of Directive 2001/29/EC (Copyright Directive), in particular the effective enforcement and protection of copyrights, to require rights holders to initially take any costly measure, however

improbable the prospect of success, to prevent a breach of law in order to effectively assert any blocking claims against an internet access provider. Moreover, recital 59 of the Directive indicates that the liability requirements of Internet access intermediaries must not be too strict, since 'these intermediaries themselves are best suited to put an end to these infringements'.

Finally, it is questionable whether the criterion of "no other option to remedy the infringement" is compatible with Article 8 (3) of the Directive at all. This is because it imposes a subsidiarity requirement in the matter, which can prevent blocking claims. This not only regulates a modality (as defined in Recital 59 of the Directive), but also a material prerequisite for the blocking order, which can stand in the way of blocking orders.²⁶ Whether and in what form a subsidiarity requirement ("no other option") may be provided for in Sec.7 (4) clause 1 TMG, should ultimately be clarified by a draft according to Sec. 267 TFEU, because other member states have a different practice on subsidiarity and partially completely dispense with such a requirement.²⁷

If one assumes that the constituent element "no other option" is also relevant in the case of interpretation in conformity with the Directive, it must in any case be interpreted in such a way that rights holders are only required to take reasonable measures to prevent rights infringements.²⁸ I.E., the principles of the *BGH* case law on the subsidiarity of internet access liability²⁹ therefore remain in force³⁰. The reasonableness of using an operator and its service providers must take place from the point of view of an objective observer within the framework of a true-to-life individual case consideration, which can, however, be typified.³¹

Generally, the operators of piracy websites professionally protect themselves against their identification and the deactivation of their services. Of course, they do not post any imprint, leave no correct contact data with technical service providers, such as host providers, and contract with technical service providers in states in which an effective enforcement of copyrights cannot be expected from and which do not provide any information. For example, there are particularly many host providers of piracy websites in Ukraine, Moldova and Russia. To some extent, the operators of such websites block the use of their websites in the states in which the pages are hosted in order to ensure that they cannot be used in accordance with local copyright law. After all, anonymization services such as Cloudflare and Ddos-Guard are regularly used, some of which already make it impossible to transfer the host providers of the respective piracy websites. With criminals acting like that, professionally protecting themselves from any identification, there is no initially promising possibility of eliminating the infringement of rights. The request for any subsidiarity measures is unreasonable in such cases. In any case, rights holders should not be required to take action against foreign-based service providers who are easily interchangeable and who have changed frequently in the past, as is usually the case with host providers of piracy websites (hosting nomadism). A precedent is not necessary here without any prospect of success and thus even with a strict interpretation of the subsidiarity requirement in Section 7 (4) clause 1 of the German Telemedia Act (TMG).

This was recently confirmed by the *LG München I* in its decision to block the site "Goldesel.to".³²

Within the framework of the reasonableness of subsidiarity measures, it must still be taken into account that these usually pointless measures of rights holders often entail

²¹ *Ohly*, JZ 2019, 251, 253; *Grisse*, GRUR 2017, 1073, 1079; this implies also *Spindler*, GRUR 2018, 1012, 1016.

²² *BGH* MMR 2016, 180 para 83 ff. comments by *Finger* - Liability of the access provider for interference - although *BGH* expressly refuses to use the concept of subsidiarity.

²³ RegE, BT-Drs. 18/12202, p. 12.

²⁴ *BGH* MMR 2016, 180 para 82, 83 comments by *Finger* - Liability of the access provider for interference

²⁵ *BGH* MMR 2016, 180 para 83 comments by *Finger* Liability of the access provider for interference

²⁶ *J. B. Nordemann*, GRUR 2018, 1016, 1018.

²⁷ See also *Nw.* in *J. B. Nordemann*, GRUR 2018, 1016, 1018.

²⁸ *Ohly*, JZ 2019, 251, 254.

²⁹ *BGH* MMR 2016, 180 para 83 comments by *Finger* - Liability of the access provider for interference; *BGH* MMR 2016, 188 para 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.* (footnote 9 above), Sec. 97, para 171a, 172a.

³¹ *Leistner/Grisse*, GRUR 2015, 105, 107; *J. B. Nordemann* (footnote 9 above), Sec. 97 Para 171a.

³² *LG München I* MMR 2019, 535 comments by *Müller*.

considerable costs. Technical service providers/investigators and lawyers must be commissioned to identify the service providers of the operators of the piracy sites in a first step and to take action against them in a second step by means of notifications and warnings. As a result, the claim under Section 7 (4) of the German Telemedia Act could degenerate analogously to a right which is only applicable for particularly economically strong companies. For rights holders of works that are not successful, a procedure based on Sec. 7 (4) TMG is not economically viable analogously due to the high costs caused by the subsidiarity requirement. This should not be compatible with Sec. 8 (3) of the Directive. In any case, this suggests that the requirements for subsidiarity should be limited.

With regard to websites with an illegal business model, "actual assumptions" can even be justified in principle. On the one hand, life experience suggests that the operators of such websites have regularly taken precautions to protect themselves against identification by means of various protective measures. It is also realistic that action against the host providers of such websites is usually pointless because they are replaced by the operators as soon as they are attacked by rights holders.³³ The instrument of actual presumption is recognized in German case-law³⁴ and would now only have to be implemented in the sense of the two aforementioned presumptions; of course, including the rule applicable to actual presumptions, according to which they do not apply if they are shaken by special circumstances in the individual case.

3. Reasonability and proportionality of blocking

According to clause 2 of Section 7 (4) of the German Telemedia Act (TMG), the claim pursuant to Section 7 (4) requires that the blocking is reasonable and proportionate.

a) Sufficient efficiency of DNS and IP blocking

It is regularly argued against the proportionality and reasonableness of website blocks that the given technical means, in particular DNS blocking and IP blocking, are not sufficiently efficient to justify the obligation of internet access providers to take blocking measures. This is not convincing because, according to the case-law of the *BGH*, it is sufficient that unauthorized access to the protected works is "at least aggravated".³⁵ It is sufficient, for example in the case of DNS blocks, that internet users, such as those searching for illegally downloadable games, are strengthened in their sense of illegality by these if the domain being accessed cannot be retrieved, thereby counteracting their willingness to circumvent the blocks.³⁶

b) Costs of blocking measures

The most commonly used and coveted blocking measures, DNS blocking and IP blocking, are not disproportionately expensive. The implementation will be possible automatically with internet access providers and will generate costs in the three- to four-digit euro range.³⁷ Self claimed blocking costs of €150,000.00 were regarded by the *LG München I* as proportionate.³⁸ In addition, internet access providers with an infrastructure that aggravates DNS blocking are not worthy of protection, as internet access providers had to expect to be obliged to set up DNS and IP blocks at the least since the *BGH* ruling in the case "Störerhaftung des Accessproviders" dated November, 26 2015.³⁹

According to the case-law of the *BGH*, disproportionate costs should remain the exception anyway. It emphasises that the *ECJ* does not see the substance of the right to entrepreneurial freedom affected by a blocking order when an obligation is imposed on the service provider to use resources for potentially costly measures which have a significant impact on the organization of his activity or which require difficult and complex technical solutions.⁴⁰

c) Consideration of Sec.5 (1) GG

Sec. 5 (1) GG (German Constitution) does not preclude the blocking of illegal websites.⁴¹ The right to freedom of information is not granted unrestrictedly and in any event finds its limits if the access to information clearly infringes copyrights. In this context, it should also be taken into account that to a lesser extent, non-genuine content on piracy websites, insofar as it is to be found there, is worthy of protection and does not prevent the blocking of a website if it is a website that is clearly and specifically aimed at the infringement of copyrights. The aspect of overblocking should therefore not be considered from a purely quantitative point of view, but rather from a more superficial qualitative point of view. Otherwise, by indiscriminately inserting public domain content or creating user forums on their websites, the operators of piracy websites would have the power to make website blocking legally impossible.

IV. Urgency assessment by urgent procedure

Even if the blocking claim pursuant to Section 7 (4) of the German Telemedia Act (TMG) is no longer a cease-and-desist claim, but rather a blocking claim aimed at positive performance, access providers can still be held accountable within the framework of the interim injunction proceedings.⁴²

However, new challenges for provisional legal protection in revocation proceedings lurk elsewhere: in the recent decisions of the *LG München I* and *OLG München*⁴³ the courts denied the existence of the reason for the injunction of urgency as the rights holders - here: leading scientific publishers - had already known for more than a month of the structural copyright infringing pages which they sought to block. It is true that the plaintiffs had filed for an injunction within one month of becoming aware of the concrete violation of the law, i.e. the illegal public access (Section 19a UrhG) to copyright-protected scientific publications on two well-known piracy pages. Thus, they had acted within the urgency period of one month established by the Munich courts.⁴⁴

³³ As on "hosting nomadism" i.R.d. Störerhaftung already *OLG München* MMR 2018, 832 Para 55 - Störerhaftung des Access-Providers bei Urheberrechtsverletzungen - Kinox.to.

³⁴ For the legal nature of actual presumptions, see *BGH* NYY 2010, 363.

³⁵ *BGH* MMR 2016, 180 para 47 comments by *Finger* - Liability of the access provider for interference with reference to *ECJ* MMR 2014, 397, para. 62 f. comments by *Roth* - UPC cable/Constantin Film and others - kino.to.

³⁶ *BGH* MMR 2016, 180 para 48 comments by *Finger* - Liability of the access providers for interference; *LG München I* MMR 2019, 535 comments by *Müller*.

³⁷ *Landesgericht ZRS Vienna*, U. v. 12.10.2017 - 47 R 281/17x.

³⁸ *LG München I* MMR 2018, 322 comments by *Sesing/Baumann*.

³⁹ *LG München I* MMR 2018, 322 comments by *Sesing/Baumann*.

⁴⁰ *BGH* MMR 2016, 180 para 38 comments by *Finger* - Liability of the Access Provider for interference with reference to *ECJ* MMR 2014, 397, paragraph 49 et seq. comments by *Roth* - UPC Telekabel/Constantin Film et al. - kino.to.

⁴¹ *BGH* MMR 2016, 180 para 53 ff. comments by *Finger* - Liability of the Access-Providers.

⁴² See *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. *Rehart*.

⁴⁴ On the urgency period of one month: *OLG München* MMR 2017, 114 - *Kein Vollgas*; *OLG München* GRUR-RR 2008, 310, 312.

However, the plaintiffs had been aware for more than one month of the fact that their rights to other works had been infringed on the disputed websites.

The *OLG München* confirmed the decision of the previous instance, according to which, in the case of blocking claims against access providers, the urgency - in contrast to the customary case law in copyright law - is not to be interpreted in relation to a work but rather in relation to a page.⁴⁵ The *court* bases its reasoning on the effect of the requested blocking measure: the requested website block is not aimed at a specific intellectual property right, but is based on the fact that internet users are no longer provided access to the portals as a whole and are therefore no longer able to access all the contents of the portals. Since the requested blocking measure does not have any property rights related effects, a view on single property rights with regard to the question of urgency was not appropriate either.⁴⁶ If a rights holder makes claims against an access provider to block a particular portal because copyright infringements are constantly committed via that portal, then, in the opinion of the *OLG München*, the infringements of the rights to the various works in respect of the requested measure of blocking the portals constitute essentially identical infringements. Consequently, if the applicant, although aware of the possibility of blocking, does not request an individual decision within one month, it shows that the matter is not urgent.⁴⁷ In the view of the *Court*, rights holders who are aware of an infringement and of the website concerned must take action against the access provider if they are also aware that action against the operator of the website and its host provider is futile and that the portal mainly contains unlawful content.⁴⁸

The departure from the work-related interpretation of urgency is not convincing for several reasons. First - contrary to what was established by the *OLG München* - the decision of the *BGH* regarding "Dead Island" does not present this result. The passage from the decision referred to by the court⁴⁹ referred to the material-law question of the emergence of behavioral obligations in the context of "Störerhaftung", but not to a procedural-law consideration of the interpretation of urgency. It must also be taken into account that the wording of Section 7 (4) of the German Telemedia Act (TMG) also requires a work-related interpretation, since it is based on the infringement and prevention of the infringement of individual specific rights. The fact that certain blocking measures, such as DNS blocking or IP blocking, cannot, for technical reasons, be related to a single work, but generally cover an entire website, cannot lead to the assumption, to the detriment of the rights holders, that Section 7 (4) TMG is not a work-based claim. In other words: a technically induced unintended secondary consequence of a blocking measure cannot change the legal character of a work-related standard. Finally, constitutional arguments also argue against the non-work-related - but page related - interpretation,

⁴⁵ *OLG München* MMR 2019, 317 comments by *Rehart*.

⁴⁶ *OLG München* MMR 2019, 317 comments by *Rehart* with reference to *BGH* MMR 2018, 811 - Dead Island.

⁴⁷ *OLG München* MMR 2019, 317 comments by *Rehart*.

⁴⁸ *OLG München* MMR 2019, 317 comments by *Rehart*.

⁴⁹ *BGH* MMR 2018, 811 - Dead Island.

⁵⁰ *ECJ* GRUR 2017, 316, para 25 - New Wave; *ECJ* MMR 2011, 596, paragraph 131 comments by Hoeren - L'Ore' al SA; *BGH* MMR 2011, 391 para 20 - Any DVD.

⁵¹ See e.g. *OLG Köln* ZUM-RD 1998, 110; *OLG Hamburg* ZUM 2009, 575, 577 et seq; *LG Hamburg* ZUM 2009, 582, 587 - Zattoo; *J. B. Nordemann* (footnote 9 above), Sec. 97n UrhG Para 205

of the urgency. Both Section 14 GG and Sec. 17 (2) of the Charter of fundamental rights of the European Union guarantee copyright under constitutional law and grant a constitutional right to an effective remedy.⁵⁰ This leads above all to an interpretation in conformity with the constitution if otherwise absolute gaps in protection arise to the detriment of the rights holders. The right holder must not be de facto defenseless.

If the opinion of the *OLG München* is consistently applied, however, such absolute gaps in protection arise. If a rights holder knows a certain internet platform which by its nature constantly produces similar infringements, claims against such a website would have to be immediately asserted within the urgency period after knowledge and conclusion of the "subsidiarity work", i.e. the unsuccessful action against the operator or host provider. Otherwise, interim relief is no longer possible, not even for new infringements, although this is a separate subject-matter with its own substance. The holder of the rights can then only prevail in the main proceedings, which means a considerable loss of time. Any infringement of rights that continues to be produced during this period would have to be tolerated by the right holder according to the non-work interpretation of the urgency principle. Against this background, it seems appropriate to maintain the work-related interpretation of the principle of urgency also in the case of blocking claims against access providers with the previous permanent jurisprudence in copyright.⁵¹

V. Conclusion

Content piracy is a cross-industry phenomenon and does not stop at computer games. For real reasons, the rights holders generally have no possibility of taking action against the operators of piracy websites, as these are professional criminals who use the technical possibilities of the internet to avoid identification and claims. Accordingly, the operators of the piracy websites select service providers, such as host providers, who are exchangeable anyway and are mostly based abroad.

The rights holders have no other option than to proceed to the blocking of the respective piracy websites with an internet access provider. Since the *BGH's* "Dead Island" judgement, this can analogously be based on Section 7 (4) TMG. Sec. 7 (4) TMG is to be interpreted analogously in accordance with Union law in such a way that either a subsidiarity requirement ("no other option to remedy the infringement") is to be waived or, in any case, rights holders are only required to take reasonable measures to prevent the transfer of rights. Contrary to the new interpretation of the *OLG München*, this should also be possible on the basis of the work reference of Sec. 7 (4). TMG against longer known piracy websites in urgent proceedings if new computer games are made publicly accessible there.



Dr. Julian Waiblinger

is a lawyer and specialized in copyright and media law in Berlin.



Dr. Stanislaus Jaworski

is a lawyer in Berlin.

Key selling: Legal limits to the trade with license keys for computer games

Comments from a practical and legal point of view

principle of exhaustion

The sale of license keys for computer games - key selling - is still a lucrative market. In addition to legal distribution platforms, however, there is also a flourishing trade in highly discounted license keys from partly questionable sources on the internet. Accordingly, literature and case law have

discussed the legal limits of key selling several times in the past years. The following article summarizes the legal treatment from a practical point of view.

Reading time: 22 minutes

I. What is Key Selling?

Nowadays, license keys are the core of the distribution of PC games. Anyone who buys a DVD with a computer game in a store receives a key with the DVD - a short code consisting of numbers and letters which activates the game and which usually has to be registered on online sales platforms such as e.g. Steam, Origin or Uplay.

The key has by far not only the function of copyright protection. Purchasers can also download the game again from the respective online sales platforms at any time using the key, e.g. if the data carrier is damaged or lost. The key thus has the function of a key in the literal sense:¹ It allows the actual access to the game - the data carrier basically only serves to avoid long downloading times. It is not necessary for playing the acquired computer game, however. The key with which the game can be registered and downloaded is therefore more important.

Accordingly, more keys are being sold and ever more frequently without the corresponding data carrier - the so-called key selling. If the sale is carried out by the rights owners or their distribution partners, this is legally unproblematic.

The legal discussion begins when key sellers sell keys without or even against the will of the right holders. Key sellers acquire keys from various sources at the lowest possible price. For example, DVDs are purchased in large quantities in countries with low purchasing power and proportionately low consumer prices. The keys contained in the DVD cases are then photographed and resold digitally - with an extra charge for the margin of the key seller, but usually still below the regular retail price in countries with high purchasing power. Sometimes only the completely digital keys are acquired on favorable occasions. The online platform "Humblebundle"², for example, offers keys in cooperation with game publishers for special campaigns at a self-determined price, which is significantly below the usual selling price, the earnings of which partly benefit charity projects. Key sellers acquire the keys immediately in larger quantities at particularly favorable prices then and resell them with profit.

II. Legal Evaluation

1. Copyright

Anyone who acquires a computer game also acquires rights of use. As the scope of the rights of use at the time of purchase is rarely concretely defined, the scope of rights of

use granted under Section 31.5 *UrhG* is determined by the purpose of the contract. In the case of games that are intended for end users, the purpose of the contract is to enable the player to use the game on a permanent basis, i.e. to install and play the game. The rights granted will therefore include the right to reproduce on the device used by the purchaser, i.e. the installation, as well as the running of the computer game, i.e. the playing. However, the contractual purpose of a consumer sale does not normally include a right to distribute the game. In this respect, Section 31.5 *UrhG* also protects the right holders by prescribing a restrictive interpretation of the implied rights of use.

However, for the (physical) right of distribution - e.g. the sale of data carriers - copyright law expressly provides for an exception. According to Sections 17 (2), 69c No. 3 clause 2 *UrhG*, the right holder may not prohibit the dissemination of a work if it has been put on the market by way of sale within the European Economic Area (EEA) (so-called principle of exhaustion). The regulation protects the free movement of goods: goods should be allowed to trade freely within the EEA without any copyright restrictions.

This may also affect keys for computer games if they are distributed in physical form: If a key is placed on the market (for the first time) within the EEA together with a data carrier by way of sale, the distribution right is exhausted in this respect. The resale of the data carrier - including the key - may not be prohibited within the EEA by the rights holder - even if he has not granted the first purchaser the right to distribute it.

The actual discussion about key selling arises from the question of whether and to what extent the immaterial distribution of keys is also subject to the principle of exhaustion.

a) Principles of the *UsedSoft* judgement

The starting point of the discussion about key selling is the *ECJ*'s *UsedSoft* decision.³ Accordingly, right holders may not prohibit the distribution of a non-physical copy of a computer program within the meaning of Section 69a (1) *UrhG* under following conditions:⁴

¹ See also *OLG München* MMR 2017, 838.

² See <https://www.humblebundle.com>

³ *ECJ* MMR 2012, 586 m. *Heydn* - *UsedSoft*.

⁴ *ECJ* MMR 2012, 586, 587 ff. m. *Heydn* - *UsedSoft*.

c The computer program was placed on the market within the EEA with the consent of the rights holder.

c The computer program was placed on the market by way of purchase, i.e. the first purchaser was granted permanent and not merely temporary rights of use.

c The Seller proves that he has no further copy of the computer program and has deleted any duplications.

c The right holder had the opportunity to receive an appropriate remuneration for the copy of the program.

If the above conditions are met cumulatively, the distribution right of the right holder is exhausted. The acquirer of the software thus becomes the entitled party within the meaning of Section 69d (1) of the German Copyright Act (UrhG), which enables him to legally reproduce the software by downloading it from the internet for the intended use of the computer program. The transfer of a copy already in the seller's possession is therefore unnecessary.⁵

The exhaustion of the distribution right is thus decoupled from any substrate.⁶ The object of distribution is rather a "virtual copy" of the computer program.⁷ Whether a tangible or intangible copy has been put into circulation is irrelevant to the exhaustion of the right of distribution. While the Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society (InfoSoc Directive) clarifies in recital 29 that exhaustion is linked to the 'material medium' of the work and therefore plays no role in online services, the Directive 2009/ 24/EC on the legal protection of computer programs (Computer Program Directive) lacks such a restriction. This restriction is not only non-binding. It is an expression of an interpretation to which the signatory states of the WIPO Copyright Treaty (WTC) have agreed in a declaration on the principle of exhaustion enshrined in the WTC.⁸ Consequently, the German legislator has also implemented exhaustion in the (physical) distribution law in Section 17 (2) UrhG for works that are subject to the InfoSoc Directive.

c Transferability to computer games

The fundamental question therefore arises as to whether the *ECJ's* observations in the *UsedSoft* ruling apply to computer games. According to common belief, computer games are copyrightable as cinematographic works.⁹ Computer games are complex artistic forms of moving images. It does not stand in the way of the protection of computer games as film works

that the player interactively participates in the film works and can influence the action and course of events.¹⁰ At the same time, computer games are also controlled by computer programs. They are therefore "hybrid works".¹¹

In the opinion of both the *BGH*¹² and the *ECJ*¹³, the scope of protection of a hybrid work may not be reduced because it is capable of being protected under several aspects of copyright law. Otherwise, the creator of a particularly complex work which can be protected under several aspects would be placed in a worse position than the author of a less complex work which can only be protected under one single aspect.

However, it would contradict this idea if the *ECJ's* *UsedSoft* ruling were to be applied to computer games in an undifferentiated manner: If computer games were only works according to the InfoSoc Directive, an exhaustion of the distribution right would not be considered in the case of a purely immaterial distribution.¹⁴ The rights holder of a work under the InfoSoc Directive is in a better position than the rights holder of a computer program.

The fact that computer programs are protected according to both the InfoSoc Directive and the Computer Program Directive - the right recognizes them as eligible for protection in several respects - must not result in the right holder being placed in a worse position by the extended protection. If one were to apply the principles of the *UsedSoft* decision to computer games as well, it would be exactly this effect that would occur: The mere fact that computer games as hybrid works are subject to additional protection by the Directive on computer programs would mean that exhaustion of the distribution right could also occur in the case of intangible distribution. The extended protectability recognized by the legislator as a work that falls under several protection categories would thus lead to a de facto shortening of the protection.

In this respect, there are already considerable doubts as to whether the principles of the *UsedSoft* judgment can be applied to computer games.¹⁵

c No exhaustion with non-activated keys

Another special feature is the purely digitally distributed keys - i.e. keys that are not sold together with a physical data carrier, but completely digital. In this case, the transfer of keys does not serve to pass on an already existing duplication piece, but rather to produce it for the first time. In comparison to the case of "used software", which also formed the basis of the *ECJ's* *UsedSoft* ruling, there is another significant difference. The *OLG Frankfurt/M.* and the *OLG München* also assumed that the rules on exhaustion and thus also the principles of the *UsedSoft* decision were not applicable in the case of the resale of digitally acquired, non-activated keys.¹⁶

c No splitting of license keys and data carriers

Even in the case of such keys which are distributed together with a physical data carrier, there is a significant peculiarity compared to the *UsedSoft* case law. According to the *LG Berlin*, exhaustion can only occur from the outset in the product which has been put on the market within the EEA with the consent of the entitled party.¹⁷ The splitting of licenses - such as the separate distribution of license keys from a data carrier originally placed on the market - is therefore out of the question from the outset.

⁵ *ECJ* MMR 2012, 586, 590 comments by *Heydn* - *UsedSoft*.

⁶ *Hilgert*, CR 2014, 354, 357.

⁷ *Speakers*, CR 2014, 73, 75.

⁸ *Krüger/Biehler/Apel*, MMR 2013, 760, 764.

⁹ *Bullinger*, in: *Wandtke/Bullinger*, Copyright Law, 4th ed. 2014, Sec. 2, para 129; *Rentscher*, IT-Recht, 6th ed. 2017, Chapter A, para 118; *Kaboth/Spies*, in: *BeckOK Copyright*, status: 15.4.2019, Sec. 69a, para 8; *Picot*, in: *Auer-Reinsdorff/Conrad*, Hdb. IT and Data Protection Law, 2nd ed. 2016, Sec. 29, no. 4.

¹⁰ *Schricker/Loewenheim*, Copyright, 4th ed. 2017, Sec. 2 para no. 217 m.w.Nw.

¹¹ *Kreutzer*, CR 2007, 1, 2.

¹² *BGH* MMR 2013, 671 comments by *Roth* - Video game consoles, para 24.

¹³ *ECJ* MMR 2014, 401 comments by *Oehler*, paragraph 23.

¹⁴ *Apel*, ZUM 2015, 640 m.w.Nw.; *OLG Hamm* GRUR 2014, 853, 859 f. - General terms and conditions for audio books with regard to the distribution of audio books.

¹⁵ So also *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.; with respect to transferability to audio books *OLG Hamm* GRUR 2014, 853, 859 f.; with respect to transferability to other types of works generally also *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.

For computer programs, however, the *BGH* has judged this differently: Accordingly, it is not a question of whether a license key for software is obtained by handing over the data carrier or by simply disclosing the license key that is important for exhaustion to occur.¹⁸

b) Failure to meet the criteria for exhaustion under the UsedSoft decision

Even if, contrary to the above-mentioned doubts, the principles of the UsedSoft decision were also to be applied to computer games, the conditions laid down by the *ECJ* for exhaustion to occur are generally not fulfilled in practice. It must be taken into account that key sellers who invoke the occurrence of exhaustion as a copyright exception are generally burdened with evidence of the existence of the constituent elements of the offence.¹⁹

c Placing on the market within the EEA

Already the place of putting something on the market regularly poses a considerable obstacle. On the one hand, for factual reasons: Keys placed on the market outside the EEA are often particularly cheap and therefore economically very attractive for key sellers. It is therefore not uncommon for keys that have been put on the Russian market, for example, to be sold. In this case, exhaustion does not occur for factual reasons because the keys have not been put on the market within the EEA and therefore the conditions for exhaustion are not actually fulfilled.

On the other hand, in practice it is difficult, if not impossible, to document the origin of a key in a court of law. Keys are regularly procured and distributed on a division of labor basis – key sellers can purchase them in large quantities on specialized online marketplaces, often anonymously for the buyers and sellers involved. A clean documentation of origin is guaranteed in the rarest cases, so that in practice the proof of the placing on the market of the keys within the EEA is often not successful.

c Full payment for the initial purchase

In order for exhaustion to occur, the right holder must also be able to obtain remuneration corresponding to the economic value of the copy of the work belonging to him.²⁰ In the opinion of the *BGH*, it is not absolutely essential that the right holder actually received adequate remuneration - he must only have been given the opportunity to do so.²¹ If a right holder decides, for example, to grant licenses at a very favorable price or even to make his computer program or parts thereof available free of charge, this does not prevent exhaustion from occurring.²² However, the possibility of receiving equitable remuneration must be granted to the right holder.

In practice, it is not uncommon for keys to be misused for money laundering purposes and acquired with stolen credit cards for resale.²³ In that case, it is doubtful whether a fraudulently acquired key was even deliberately put into circulation by the right holder. In any event, the right holder was deprived by the complainant of the possibility of compensating his investment in the creation of the computer program with an appropriate remuneration if the purchase price was not paid on the basis of a payment guarantee from the credit institution.

Proof that a sold key was actually paid for by the original purchaser is therefore of utter importance in key selling.

In view of the above-mentioned gaps in documentation in practice, a key seller is not in a position to demonstrate whether a key was actually paid for by its first purchaser - whom the ultimate seller of the keys often does not even know by name to end users.

2. Unfair competition law

Violations of unfair competition law by key sellers are also regularly considered. This is mainly because the unfair competition law imposes extensive information obligations on key sellers, whose non-compliance could result in a violation.

*OLG Hamburg*²⁴ decided regarding the sale of keys for computer programs that the key seller has to inform the buyer whether and to whom the respective key has been issued by the right holder and whether an exhaustion of the corresponding distribution right has occurred. Information should also be provided on the nature of the license granted and whether the copy of the programme was destroyed by the first purchaser or intermediate purchaser. These information obligations are in part strongly based on the criteria established by the *ECJ* in the UsedSoft ruling. If the UsedSoft decision is also applied to computer games, the criteria established by the *ECJ* must not only be fulfilled and proven by the key seller - the customer must also be informed about this. In practice this is usually not to be observed.

In addition, it represents an essential characteristic of the product in the sense of Sec. 5 (1) (1) of unfair competition law if the acquirer is not entitled to download or use a computer program in relation to the right holder.²⁵ Thus, if the purchaser does not actually receive access authorization when purchasing a key, the key seller not only acts contrary to copyright law, but also unfairly.

3. Criminal law

In addition to copyright and unfair competition law, key selling has also recently been given an increasingly criminal dimension. As key sellers generally act commercially, the unauthorized sale of keys is punishable under Secs. 106 (1), 108a (1) UrhG if no exhaustion has occurred. In addition, there is regularly a commercial fraud at the expense of the customers in accordance with Sec. 263 (3) (1) StGB, because they are deceived about being granted usage rights for a copyrighted work against payment of a fee, to which the key seller is not entitled.

The *AG Gießen* sentenced the online seller of license keys for various *Microsoft programs* to 18 months imprisonment on probation on this very basis.²⁶ Recently, the *BGH* also confirmed a conviction of two key sellers who had apparently sold software keys originating from China on the Internet.²⁷

¹⁸ *BGH MMR* 2015, 735 - Green IT.

¹⁹ *BGH MMR* 2014, 232, 238 comments by *Heydn* - UsedSoft II.

²⁰ *ECJ MMR* 2012, 586, 589 comments by *Heydn* - UsedSoft, para 72.

²¹ *BGH MMR* 2014, 232, 238 comments by *Heydn* - UsedSoft II.

²² *BGH MMR* 2015, 530 - UsedSoft III.

²³ Cf. for example the reports on credit card fraud in connection with key selling, available at: <https://kotaku.com/g2a-scammer-explains-how-he-pro-fited-off-stolen-indie-g-1784540664> and <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 Casting MMR* 2016, 696 m. *Rosemann* = *GRUR-Prax* 2016, 415 comments by *Hansen*.

²⁷ *BGH MMR* 2019, 444.

4. Liability of key selling marketplaces

In recent years, a trend has emerged in the area of key selling. While keys were originally sold directly to customers by large key selling shops, many providers have now developed their business models into marketplace opportunities: Instead of selling keys directly to end customers, they now offer an intermediary platform between anonymous sellers of keys and customers. The operators of the key selling marketplaces are increasingly arguing that they themselves are not responsible for the permissibility of the keys distributed via their marketplaces, that they only act as host providers within the meaning of Section 10 of the German Telemedia Act (TMG) and that they are therefore only obliged to act once they become aware of the illegality.

However, only telemedia providers who merely store external information benefit from Section 10 TMG.²⁸ Whether the keys offered on the key selling marketplaces really are foreign information can hardly be judged from the outside: The sellers usually appear anonymously, an imprint or even only contact opportunities to the sellers are usually not available. In the case of some key selling marketplaces, it is also not at all apparent on the individual product pages that a sale is being made by third parties and not by the provider himself - at most during the course of the purchase process, a reference to a pseudonym of a alleged seller appears in an inconspicuous place.

Legally it has to be considered that a liability for the storage of external information according to Section 10 TMG can also be considered if the telemedia provider has adopted this information as his own.²⁹ Information that has been made proprietary is treated as proprietary information and is present when third-party information is integrated into one's own offer in such a way that the objective recipient of the explanation gets the impression that it is information provided by the provider itself.³⁰

For the addressed visitors of the telemedia service it must therefore be recognizable that not the website operator sells the keys, but any of the sellers. It doesn't matter whether are – hidden - indications that it is external information. Rather, the content must be presented in an overall view in such a way that, for an objective observer, a serious and sufficient distancing from the third-party content takes place.³¹

Such dissociation will be missing if the distribution of keys represents the very purpose of such marketplaces, if the operator does not take measures to limit the typical risks associated with such distribution - e.g. by obligatory and detailed documentation of the keys' origin – in addition to protecting sellers of potentially infringing keys from prosecution by granting them anonymity.

It is true that the granting of a pseudonymous use of a telemedia service does not in itself constitute the appropriation of third-party content.³² However, service providers which store information provided by users must apply the due diligence which they reasonably expect and which is laid down in national law in order to detect and prevent certain types of illegal activity.³³ However, the legal system does not provide for anonymity in commercial transactions. For example, Sec. 5 (1) TMG requires the identity of telemedia providers to be disclosed. This also applies to sellers on online marketplaces.³⁴ The essentialia negotii also provide for agreement between the parties as a minimum condition for an effective contract. This will not be fulfilled if it is not recognizable to the buyer of a key from whom he acquires it and whether his alleged seller even exists. The lack of recognizability of the trader rather leads to the fact that the marketplace operator comes to the fore from the customer's point of view instead of distancing himself from the foreign content.³⁵ The disclosure of the identity of the seller within the framework of the legal requirements will also be possible with the operators of key selling marketplaces.

III. Law Enforcement in Practice

In practice, enforcement against unauthorized key selling poses a challenge. Many providers have countered the above-mentioned legal considerations against unauthorized key selling by relocating their headquarters to outside Europe. This makes law enforcement laborious, but by no means impossible.

Because in many cases the providers may have relocated their headquarters. The actual business operations, however, still take place regularly to a large extent within the EU. Assets are also generally available in the EU, e.g. trademarks, domains or clearing accounts with banks and payment service providers. This enables the enforcement of assets within the European legal order.

The initial delivery of civil procedural documents, such as the statement of claim, to non-European countries must be effected ex officio in accordance with Section 183 (2) clause 1 of the ZPO (Code of Civil Procedure) on the basis of the respective complete agreements. In particular, if experience has shown that foreign service in the country concerned is difficult pursuant to Sec. 183 ZPO, the court may, however, order pursuant to Sec. 184 (1) clause 1 ZPO that the party located abroad designate within a reasonable period of time (generally two to six weeks from service)³⁶ a domestic service agent to whom any future order is to be sent.³⁷ If this does not happen, the court may effect subsequent service by simple mail pursuant to Sec. 184 (1) clause 2 ZPO.

If the judicial proceedings are concluded successfully, the question arises as to the possibility and prerequisites of enforcement. Enforcement in non-European countries is often governed by intergovernmental agreements which contain a wide variety of regulations.³⁸ However, since the key sellers' business operations are often conducted to a large extent within the EU and corresponding assets such as trademarks, domains or clearing accounts are therefore held by banks and payment service providers in this area, enforcement within the European legal system has high prospects of success. A seat outside the EU thus offers only limited protection against domestic judicial action.

²⁸ Hoffmann, in: Spindler/Schuster, Law of Electronic Media, 3rd edition 2015, TMG Sec. 10 para 16.

²⁹ BGH MMR 2017, 526 comments by Becker - klinikbewertungen.de; Paal, in: BeckOK InfoMedienR, status: 1.2.2019, Sec. 7 para 31 m.w.Nw.

³⁰ Paal (footnote 29 above), Sec. 7 para 31.

³¹ BGH MMR 2010, 556, 557 - marions-kochbuch.de.

³² Hoffmann (footnote 28 above), Sec. 7 para 22.

³³ BGH MMR 2013, 185, 186 comments by Hoeren - Alone in the Dark.

³⁴ Cf. OLG Hamburg MMR 2010, 29; OLG Düsseldorf MMR 2013, 649.

³⁵ LG Köln ZUM 2001, 716, 718.

³⁶ Cf. OLG Hamm NJW-RR 2012, 62, 64, under-period of two weeks for service in Turkey; BGH NJW 2013, 387, 390 comments by Schäfer, four weeks for delivery to China.

³⁷ Roth, in: Stein/Jonas, ZPO, 23rd ed. 2016, Sec. 184, para 5.

³⁸ Haag, in: Geigel, Haftpflichtprozess, 27th edition 2015, 43rd chapter, para 27.

Also the increased criminal law measures show that right holders are not unprotected against unauthorized key selling.

The formally registered office of the provider plays no role in criminal law investigations.

The decisive factor is rather where the actual business operations take place - if only because the investigations are not directed against the company, but against the persons involved. In this respect, a mere transfer of the registered office from criminal investigations offers only limited protection in practice.

IV. Conclusion

As highly technical and at the same time creative works, computer games are subject to numerous peculiarities in the copyright network of the various intellectual property rights, which represent a further complication for the already very complex legal issues surrounding the digital distribution of keys.

There are serious doubts as to whether the general principles developed for the distribution of computer programs can be easily applied to hybrid works such as computer games. In any event, practice has shown that the high hurdles that the case-law imposes on the resale of soft-

ware licenses are hardly practicable for buyers of keys.

At the same time, both the key selling market and the distribution of computer games are constantly on the move. Some publishers, for example, are now doing away with keys altogether and activate their products directly through the users' accounts on their respective online sales platforms.³⁹

That key sellers will become account sellers in future is not to be feared - *BGH* already closed this door in 2010 with its *Half-Life 2* decision.⁴⁰



Thomas Merk

is head of the legal department of Koch Media Group. Koch Media, headquartered in Planegg near Munich, is an international producer and marketer of PC and console games as well as films.



Adrian Schneider

is an attorney with Osborne Clarke in Cologne and advises, among others, companies of the games industry in IT law matters.

³⁹ Cf. <https://www.heise.de/newsticker/meldung/Ubisoft-schiebt-Key-Resellern-einen-Riegel-vor--4412269.html>.

⁴⁰ *BGH* MMR 2010, 771 comments by *Heydn* - *Half-Life 2*.

FELIX HILGERT / MARTIN SESTER

Criminal Liability for the Operation of Piracy Servers

Criminality, prosecution and claims for damages

Commercial copyright infringement

The operation of unlicensed pirate servers for online games violates copyright and trademark laws and causes considerable financial damage to legitimate game providers. Operators of such servers practically always commit considerable criminal offences according to the copyright law and in some cases also according to the trademark law. In addition to imprisonment or fines, there are other consequences, such as the skimming off of profits and the introduction of new

I. Introduction

Piracy servers, also known as pirate servers, are servers that allow an online game to be played without a license from the actual owner of the rights and regardless of the latter's infrastructure. They are available especially for a range of MMORPGs (Massively Multiplayer Online Role-Playing Games). The operator of such a server must use illegally copied versions of the software of the official server or, in rare cases, emulate its functionality. Some of the piracy servers also modify the integrity of the games, offering additional features (mods) or even older versions of a game. The operators earn money by selling in-game currency and in-game items.

The operators of piracy servers follow the same principle of monetization as the legitimate operators of the games. It is obvious that the operation of such servers infringes copyright

the perpetrator's IT equipment in the room. Right-holders can take part in criminal proceedings as joint plaintiffs and thus also work towards an effective deterrence of counterfeiters. This applies in particular to foreign perpetrators as long as their activities have an impact on the German market.

Reading time: 16 minutes

of the exclusive supplier, which is legitimate and regularly exclusive within a certain territory and causes him damage, for example through the loss of revenue or generally through the commercial exploitation of the legal position to which this supplier is entitled. The piracy server operator is spared any license fees which the provider has to pay to his licensor(s) in comparison to a bona fide provider. If the provider has developed the game himself, the piracy server operator saves the development costs. Marketing costs of the provider are hardly incurred by the piracy server operator. On the contrary, he benefits from the provider's efforts to introduce the game to the market and make it known. The honest provider regularly has considerable expenses for data protection and data security measures. Such things will hardly play a role for the piracy server operator. After all, the honest operator pays taxes - both sales tax and income tax. Ultimately, the absence of expenses and levies in regard to

the market position that the provider has created for the respective game, led to the piracy server operator acting much more profitable than the official provider.

Such damages can be claimed by injured companies via Sec. 97 (2) UrhG. In the assessment of the damage - at the option of the claim holder - the actual damage suffered, the profit made by the infringer through the infringement of the right or a hypothetical license fee are decisive. The same shall apply mutatis mutandis to a claim for damages due to the infringement of trademark rights pursuant to Sec. 14 (6) MarkenG.

Just as important to companies as financial redress is often the rapid shutdown of piracy servers and an effective deterrent to potential counterfeiters. Criminal law can help here. This article uses the example of a precedent¹ to illustrate the consequences of criminal law for the operator of a piracy server and examines the question of how providers of online games can effectively use criminal law to enforce their claims.

II. The AG Heidelberg "Cyperia" Case

The fact that the operation of a piracy server can also have consequences under criminal law was recently demonstrated by the case of the servers "Cyperia" and "Hardcore Reloaded" for the online game "Metin 2", which were operated from 2014 to 2016 and on which several hundred players registered for the game were active. With the sale of virtual currency, the operator had been able to achieve six-digit profits. In addition to various PCs, notebooks and storage media, money exceeding €100,000 was confiscated during the search.

In April 2018, the *AG Heidelberg* sentenced the operator for commercial copyright infringement to a fine of 90 daily rates of 20.00 Euro each. The operator was able to avert a more severe penalty by working intensively with *GVU (Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V.)* and the authorities.

However, this cooperation also had a positive effect for the injured company, as it led to references to the operator of another "Metin 2" server in Berlin, who was arrested in connection with a search in March 2018. He, too, is said to have made six-figure profits from the piracy server he runs.²

III. Criminality and Prosecution of an Operation of Piracy Servers

The operation of a piracy server involves various criminal offences under the Copyright Act and the Trademark Act. For the operation of a piracy server, it is regularly not only necessary to copy the software of the game server and install it on one's own server. The client software must also be copied, modified and made publicly available, for example by making it available on the operator's own website. In most cases, it will not be possible to access any

servers other than the official game servers of the provider using the original client software. Finally, the operator of the piracy server will also have to use the name of the game, which as a rule is protected by trademark law. This happens rather rarely directly in the name of the respective piracy server, but more frequently by used metatags or keywords, in order to appear in search engine hits or so-called top lists. In some constellations, criminal applications by the rights holder are necessary.

1. Criminality according to German Copyright Law

a) Punishable copyright infringement

In the above-mentioned manner (Sec. 16 UrhG) the server operator therefore duplicates several objects of protection of copyright, processes (Sec. 23 UrhG) them partially and makes them publicly accessible (Sec. 19a UrhG). Offering the edited client also represents a copyright infringement in accordance with Sec. 69c No. 1 UrhG. For the unlawful reproduction, distribution or public communication of an object of protection under copyright law, copyright law provides for a custodial sentence of up to three years or a fine in Section 106 (1) UrhG.

b) Circumvention of technical protective measures

Computer games are not just computer programs in the sense of Secs. 69a ff UrhG. Rather, they consist of a large number of protected objects solely on the basis of their graphic and aural components, so that the general copyright rules based on the InfoSoc Directive also apply to them.³ This is relevant in practice because the special legal protection of technical protection measures under Section 95a UrhG, which does not apply to pure software (Section 69a (5) UrhG), applies nevertheless to computer games.

As a prerequisite for the modification of the client software, such technical protection measures are usually also bypassed. In this respect, a custodial sentence of up to one year or a fine can be considered pursuant to Sec. 108b (1) UrhG.

c) Commercial operation

In both cases, the penalty is even higher if the offender is acting commercially. In the case of Sec. 106 (1) UrhG, the penalty then amounts to imprisonment for up to five years or a fine, Sec. 108a (1) UrhG. Regarding the circumvention of technical protective measures, the penalty is increased to imprisonment for up to three years or a fine, Section 108b (3) UrhG.

This is a commercial practice for anyone who wants to obtain a source of income of some magnitude from repeated offenses that is not only temporary. For this purpose, the judges have already considered a profit of approx. €1,000 to be sufficient.⁴ The continued operation of an illegal server shall also be deemed a repeated commission of an offence.⁵ The qualification should therefore generally be available when operating a piracy server.⁶

2. Criminal liability under the Trademark Act

The operation of a piracy server can also lead to criminal liability in terms of trademark law, for example if the protected name or logo of the game is used. Thus, Sec. 143 (1) No. 1 MarkenG provides for a custodial sentence of up to three years or a fine if a sign is used unlawfully in the course

¹ *AG Heidelberg* MMR 2019, 547.

² Cf. <https://www.golem.de/news/gameforge-erstes-urteil-gegen-betreiber-illegaler-spieleserver-1804-133970.html>.

³ *ECJ* MMR 2014, 401 comments by *Oehler*.

⁴ *AG Mainz* NJW 1989, 2637.

⁵ *Sternberg-Lieben*, in: BeckOK UrhR, as at: 15.4.2019, Sec. 108a para 2.

⁶ Cf. *AG Heidelberg* MMR 2019, 547; *LG Leipzig* ZUM 2013, 338 - kino.to.

of business contrary to Sec. 14 (2) clause 1 no. 1 or 2.

If the offender acts commercially, Sec. 143 (2) MarkenG also provides for a higher penalty here (imprisonment of three months up to five years).

3. Penalty requirement

The simple punishable copyright infringement according to Sec. 106 UrhG, the unauthorized interference in technical protective measures according to Sec. 108b UrhG as well as the simple punishable trademark infringement according to Sec. 143 (1) MarkenG are relative offences, Sec. 109 UrhG, Sec. 143 Abs. 3 MarkenG. Providers must therefore in principle file a criminal complaint in order to initiate criminal prosecution. The authors themselves and the owners of exclusive rights of use are entitled to this, but not the owners of simple rights of use.⁷ Only in the case of special public interest can the public prosecutor's office initiate an investigation procedure without a criminal complaint.

If the offender acts commercially, both the copyright infringement according to Secs. 106, 108a UrhG and the trademark infringement according to Sec. 143 (2) MarkenG are official offences. The unauthorized interference with technical protective measures, however, remains an offence even in the case of commercial conduct, as is evident from the clear wording of Sec. 109 UrhG.

4. Private lawsuit

Finally, Secs. 106, 108b UrhG, Sec. 143 (1) MarkenG are private actions under Sec. 374 (1) No. 8 StPO. The Public Prosecutor's Office will only prosecute this if there is a public interest and will otherwise refer the right holder to the patent action, Sec. 376 StPO. In the case of Sec. 108b UrhG this applies, unlike in the case of the other offences, even in the case of commercial conduct by the perpetrator.

A public interest is already given if the infringement of the right is not only minor, taking into account the damage (potential) and the offender's intention of enrichment. Insignificance may be present when individual pirated copies are passed on, but not when protected works are made available online.⁸ In the relevant constellations here, there will therefore always be a public interest.

IV. Further Consequences of the Act

In addition to the above-mentioned penalties, the perpetrator also faces other unpleasant consequences, in particular the confiscation of proceeds from crime and IT equipment. Alternatively, right holders may themselves claim damages in criminal proceedings.

1. Confiscation of proceeds from crime

According to Sec. 73 StGB, the court may order the confiscation of the person obtained through or for the unlawful act, of the uses drawn from the obtained goods or of the corresponding surrogate. In this way, both the profit of the operator of a piracy server and any fees paid for the commission of the crime can be skimmed off. Confiscation is mandatory unless an exclusion rule applies.

Exclusion regulations can be found in Sec. 73e StGB. Paragraph 1 excludes confiscation, for example, to the extent that the injured party's right to restitution or compensation for the value of the property obtained has lapsed as a result of the act. The extent of the confiscation thus depends on the fulfilment of civil claims by the injured party. If the claims are not asserted by the injured party,

there is an opportunity for the state to siphon off the wealth of the perpetrator.

Section 73e (2) of the Criminal Code provides for a provision reminiscent of the provisions of Sections 818 (3) and 819 (1) of the German Civil Code: if the value of the acquired asset is no longer present in the assets of the person concerned at the time of the order, confiscation is to be excluded. However, this shall apply only if the person concerned cannot be accused of knowing or recklessly ignorant of the circumstances which would have permitted the order of confiscation at the time when the enrichment ceases to exist.

2. Confiscation of property

Not only the uses and surrogates obtained from the act can be confiscated, but also objects of the operator which refer to the started offence according to Secs. 106, 108a, 108b UrhG, Sec. 143 MarkenG, Sec. 110 clause 1 UrhG or Sec. 143 (5) clause 1 MarkenG in conjunction with Sec. 143 (5) clause 1 UrhG. Secs. 74 et seq. StGB.

Beyond Sec. 74 StGB, not only the objects which were created by the offence ("producta sceleris") or which were used to commit or prepare the offence ("instrumenta sceleris") can be confiscated, but also the objects which are necessary objects of the offence itself: the pirated goods.⁹

However, the principle of proportionality to be found in Sec. 74b StGB must be observed in the confiscation. The consequence of this is that objects which have been used to commit the offence, but which at the same time are also and predominantly used for lawful purposes, such as computers, cannot regularly be confiscated.¹⁰ Something else may apply, however, if the perpetrator acted commercially,¹¹ which will at least be the case if the operator of a piracy server offers paid services to users. In these cases, the entire IT equipment used by the perpetrator can also be confiscated.

In addition to the intentional commission of the offence (Sec. 74 (1) StGB), the precondition for confiscation is that the objects belong to or are due to the offender or participant of the offence at the time of the decision, Sec. 74 (3) clause 1 StGB. The latter, however, is exceptionally dispensable if the person to whom the object belongs or is entitled at the time of the decision has at least recklessly contributed to the fact that the object is or has been used as a means of committing an offence, or has acquired the object in a reprehensible manner with knowledge of the circumstances which would have permitted confiscation, Sec. 110 clause 2 UrhG or Section 143 (5) clause 2 MarkenG in connection with Sec. 74a StGB.

If the confiscation of such an object is not possible because the perpetrator or participant has sold, used or otherwise frustrated the confiscation, the court may also order the confiscation of a corresponding amount of money, Sec. 74c (1) StGB.

⁷ Ernst, in: GJW Wirtschafts- und Steuerstrafrecht, 2nd edition 2017, UrhG Sec. 106 para 92.

⁸ Ernst (footnote 7 above), para 95.

⁹ Heinrich, in: MüKoStGB, 2nd edition 2015, UrhG Sec. 110, para 1.

¹⁰ Sternberg-Lieben (footnote 5 above), Sec. 110 Para 6; Heinrich (footnote 9 above), Sec. 110 para 5; Hildebrandt/Reinbacher, in: Wandtke/Bullinger, UrhR, 4th ed. 2014, Sec. 110 para 1.

¹¹ Sternberg-Lieben (footnote 5 above), section 110 para 6; Hildebrandt/Reinbacher (footnote 10 above).

3. Adhesion processes

If criminal proceedings are brought against the operator of the pirate server, the rights holder may not only participate as a joint plaintiff (Sec. 395 Paragraph 1 No. 6 StPO), but may also apply for the conduct of an adhesion procedure, Secs. 403 et seq. StPO.

Adhesion proceedings are a criminal procedural appendix procedure which enables the assertion of property rights claims of the injured party against the offender already in criminal proceedings, and in particular - in a cost-saving manner for companies with their own legal department - without the need for a lawyer, even if the asserted sum exceeds the value of the jurisdictional dispute of the local court.¹²

Any adhesion proceedings have priority over confiscation, Sec. 110 clause 3 UrhG or Sec. 143 (5) clause 3 MarkenG. If, in such proceedings, a claim under Sec. 98 UrhG for the destruction, recall or transfer of the reproductions or the devices for the production of these reproductions is upheld, confiscation is to be carried out in accordance with Sec. 110 (1) UrhG or Sec. 143 (5) (1) MarkenG.

V. International Issues

In constellations involving foreign countries, the (preliminary) question may arise as to the extent to which German intellectual property and criminal law is applicable. However, according to the territoriality principle, German trademarks and copyrights are only protected in Germany. In purely foreign cases, therefore, the necessary trademark and copyright infringements cannot occur at all.

1. Violation of German copyright law

The reproduction right according to Sec. 16 UrhG is generally considered to be infringed at the place where the reproduction copy is created.¹³ This is basically the location of the piracy server. However, the (technical) production of the duplication may also have been caused by the operation of a PC in Germany. The question arises whether, in this case, Germany should also be regarded as the place of infringement. If this were to be denied, the infringement of the reproduction right would, if necessary, have taken place only abroad, so that it would not be possible to proceed on the basis of German copyright law. However, this consequence is unacceptable.¹⁴

¹² Ferber, in: BeckOK StPO, as of: 1.4.2019, Sec. 403 para 11.

¹³ Ziegler, Copyright Infringements by Social-Sharing, Tübingen 2016, p. 75.

¹⁴ Ziegler (footnote 13 above).

¹⁵ Dreier, in: Dreier/Schulze, UrhG, 6th edition 2018, Sec. 120 para 41; Dieselhorst, ZUM 1998, 293, 299 f.

¹⁶ ECJ MMR 2015, 187 - Hejduk/EnergieAgentur; Sternberg-Lieben (footnote 5 above)

¹⁷ Ziegler (footnote 13 above), p. 76.

¹⁸ BGH GRUR 2004, 421, 422 f. = MMR 2004, 355 (Ls.); threesome (footnote 15 above) Sec. 106 para 16.

¹⁹ Sternberg-Lieben (footnote 5 above), Sec. 106 para 23; Hildebrandt/Reinbacher (footnote 10 above), Sec. 106 para 12.

²⁰ Hildebrandt/Reinbacher (footnote 10 above), Sec. 106 para 20; different view by Heghmanns, MMR 2004, 14, 15.

²¹ Sternberg-Lieben (footnote 5 above), Sec. 106, para 18; see also LG Hamburg GRUR-RS 2016, 12262.

²² On the state of opinion Sternberg-Lieben (footnote 5 above), Sec. 106 para 18 f.; Hildebrandt/Reinbacher (footnote 10 above), Sec. 106 para 46, each m.w.Nw.

Finally, the right under Sec. 16 UrhG is directed not only against the existence of reproductions, but precisely against their production. However, initiation and control are essential for this, which is why the place where these actions are carried out should also be regarded as the place of infringement.

More problematic is the place of infringement in the case of public access via the Internet. It would be possible to locate the servers solely at the location where the request was made or at the location of the servers.¹⁵ According to the case law of the *European Court of Justice*, however, copyright infringement in Internet cases also occurs in every country in which the object of protection can be retrieved.¹⁶ Only this view takes due account of the fact that the inclusion on the internet leads to the retrieval of the subject-matter and thus to the impairment of intellectual property rights in many countries, and reduces the incentive for potential perpetrators to flee to countries offering low levels of copyright protection.¹⁷ Accordingly, it must be assumed that Sec. 19a UrhG can be infringed even if the operator of a piracy server has acted from abroad and used a foreign server, provided that the object of protection can also be retrieved (as intended) from Germany.

2. Applicability of German Criminal Law

The applicability of German criminal law is primarily governed by Secs. 3, 9 StGB. According to Sec. 3 StGB, German criminal law applies to offences committed in Germany. Sec. 9 StGB specifies the place of the act. An offence has begun at every place where the offender acted (place of action) or the success belonging to the offence occurred (place of success). Since the protection of copyright is limited to the respective territory (territoriality principle), the place of success can only be domestic. Sec. 7 StGB, which makes the applicability of German criminal law to foreign offences possible, is therefore without relevance.¹⁸

If the perpetrator has acted in Germany, it is accordingly not decisive whether the piracy server is located abroad. However, problems arise when the place of action is not in the country. This is because the focus on a place of success basically presupposes that the actual criminal offence requires the occurrence of a success in the first place. While the fact of multiplication is undoubtedly an offence of success,¹⁹ the fact of making it publicly available will also imply that only an offence of activity exists, since it is not necessary that the object of protection made accessible actually reaches the public.²⁰ It is to be held against this that the retrievability of works can already constitute a distribution success pursuant to Sec. 106 UrhG.²¹ At present, however, the question is mostly unanswered.²²



Felix Hilgert

is a lawyer with Osborne Clarke in Cologne and focuses on advising companies in the gaming industry



Dr. Martin Sester

is head of law at Gameforge AG and attorney at law in Karlsruhe.

We would like to thank our research assistant Mrs. Alina Betzemeier for her support in researching this article.

Cheatbots in Computer Games

Copyright, competition and trademark claims against Cheat software

defensive claims

Providers of online computer games are struggling with companies that offer cheatbot software.

A cheatbot (or bot) is a software that automatically executes periodically recurring tasks in the game without being dependent on a human operator. By using the software, a player can perform actions in the game without being physically present. He gains advantages and gets ahead in the game faster than his competitors. The production of cheatbots is subject to the reproduction right of the owner of the rights of use of the computer program according to Sec. 69c No. 1 UrhG as well as of the other

works concerned pursuant to Section 16 (1) UrhG. It does not interfere with any restriction, because the granting of rights does not cover the duplication of the client software for commercial purposes, namely within the scope of the development of the cheatbot software (cf. Sec. 31 (5) UrhG). In terms of competition law, cheatbots are a targeted obstacle to the publisher of the games "from the point of view of unfair sales-related disability due to a sensitive intervention in the game system". Claims under trademark law exist if the cheat offered bears the game in which it is used in the name, such as "World of Warcraft Bot". **Reading time: 23 minutes**

I. Introductory remarks

Since there have been computer games, players have been looking for and finding ways to cheat in the game. Some game manufacturers have already built functions into the code of their software that allow the player to override certain game mechanics.

1. Beginnings of cheat functions

In the past, such functions were often triggered with a secret combination of keys. For example, if you pressed the key combination A+R+M+N on the C64 title "The Great Giana Sisters", you could skip a level (*Armin Gessert*, the programmer, had immortalized himself with it). In the 1980s, collectives were formed that integrated cheats into computer games.

2. Online games

At the end of the 1990s and beginning of the 2000s, games appeared that could be played on the internet via the browser. The game worlds were characterized by the fact that thousands, later millions of players could play against each other at the same time. A popular genre was build-up strategy games, in which you had to mine resources and then build an infrastructure (such as villages, bases and military power). It is possible to attack the opponent's infrastructure and take it over in the event of a victory over the opponent. In order to be successful in these games, it is necessary to carry out certain activities in the game again and again (such as the extraction of resources). These actions can only be performed by the player himself, so he must actively participate in the game. How would it be, however, if one could save oneself annoying, repetitive actions and delegate these activities to a software? At this point cheatbots (or bots for short) come into play: The word bot finds its linguistic origin in the word robot and is a short form of it. A bot is a software that automatically performs periodically recurring tasks in the game, without being dependent on human intervention.¹ The most common case of automated usage is the extraction of resources in the game. Raw materials are often the key to success because they can be exchanged for items and units. If you have a lot of resources, you'll progress faster in the game than your competitors. The use of a cheatbot around the clock is working like

the idea that a human being plays the game 24 hours a day and extracts raw materials through his own actions.

3. Online role-playing games

Cheatbots are most commonly used in connection with online role-playing games such as World of Warcraft, in which many players participate. By using a cheatbot, you gain an advantage over the other players. This means that the player using the cheatbot has an advantage over the other players. Such an advantage can also be monetized, because there are platforms on the internet on which advanced characters and other game content can be sold at considerable prices.²

In order to participate in the game "World of Warcraft", the player must purchase client software on a data carrier or online, which he installs locally on his computer. When the software is started, it connects via the Internet to a server of the game provider on which the virtual game world and the player characters are managed and processed (Battle.net server). A connection to the Battle.net server is only possible via an account. The player must therefore log in to the game via the server with a username and password each time he wants to participate in the game.

During the registration process, they will be shown the "Battle.net Terms of Use", the "World of Warcraft End User License Agreement", and the "World of Warcraft Terms of Use", which they must agree to. If he refuses his consent, he cannot complete the registration and therefore cannot participate in the game. Within the framework of the conditions to be accepted, the player is obligated not to use cheatbots, i.e. not to automatically execute games using external software.

However, the game provider faces practical difficulties if he wants to prove the use of a cheatbot software to a player. He cannot access the client computer of the player and must be content with presenting access patterns that provide an indication that a cheatbot has been used.³ Game developers use software detecting actions in their games that

¹ Rauda, Law of Computer Games, 2013, para 226.

² Röttgen/Juelicher, DSRITB 2017, 227, 232.

³ Röttgen/Juelicher, DSRITB 2017, 227, 233.

were probably not performed by real players, but by cheatbots. The manufacturers of the bots in turn try to prevent the discovery of the cheatbot by having it behave similar to a real player. The game producers then block the accounts of these players. However, such a precedent resembles the "fight against the windmills". It is much more effective to legally tackle the provider of the cheatbot and thus get to the root of the problem.

The game manufacturers attacked the cheatbots on the basis of copyright law, the law against unfair competition, trademark law, contract law, the "virtual house right" and the intervention in the established and operated business.

II. Copyright claims

1. Duplication

The game manufacturers have argued that the development of a cheatbot affects the copyright of the game. The software that the user has to download in order to play the game is protected by copyright, both according to Sec. 69a (1) UrhG as well as pursuant to Section 2 (1) UrhG. In addition to the code, i.e. the computer program, the game also contains graphics, music, film sequences, texts and models,⁴ which can be protected separately as audiovisual components, i.e. either individually as language works, musical works, works of fine art or as a combined multimedia work.⁵ A reproduction interferes with the right of reproduction of the holder of the rights of use to the computer program under Section 69c No. 1 UrhG and of the other works concerned under Section 16 (1) UrhG. It is true that the *BGH* has stated that the isolated display of the game on a screen does not constitute an encroachment on the rights of the game manufacturer. Because the display on a screen does not meet the criteria of physicality which constitutes a

reproduction.⁶ However, the software is loaded into the main memory and graphics memory of the user's computer⁷ and physically duplicated. In order to test a cheatbot, you have to duplicate the client software provided by the game manufacturer.

2. Barriers

The reproduction of the client software by a "normal user" is covered by the permission of the game manufacturer. The purpose of the transfer of rights, however, only includes the use for the purpose of playing the game privately. Therefore, the purpose of the granting of rights does not include the reproduction of the client software for commercial purposes, namely within the scope of the development of the cheatbot software (cf. Sec. 31 (5) UrhG).⁸ Consequently, the *OLG München* and the *OLG Dresden* have limited their respective prohibitions of reproduction of the client software to commercial reproduction.⁹ This is also in line with the exception of Sec. 53 (1) UrhG, which only grants privileges to private copying.¹⁰ The manufacturer of the cheatbot can claim the exception of Sec. 69d Abs. 3 UrhG, where a software (here: the client software) for program observation and analysis may be reproduced without the consent of the right holder.¹¹ However, that provision allows only the reproduction of the computer program as such, but not the reproduction of audiovisual elements of the game. Neither German copyright law nor Directive 2001/29/EC contain a provision corresponding to Article 5(3) of Directive 2009/24/EC which permits the reproduction for analysis purposes of a work or other subject-matter other than a computer program.¹² But if you run the client software, you inevitably multiply the graphical content of the game or the game music.¹³ The inadmissible reproduction of the client software within the scope of the development of the cheatbot even leads to the fact that there are not only injunctive relief claims, but also claims for information and damages with regard to the distribution of the cheatbot software. The *BGH* established a connection between the duplication of the client software and the evaluation of the cheatbot software: The revenues and profits generated by the sale of the automation software were (also) based on the duplication of the client software.¹⁴ With regard to the production, use and distribution of the cheatbot software, however, there is no right to an injunction under copyright law in the absence of a relevant infringing act.¹⁵

III. Claims under Competition Law

1. Sec. 4 (4) UWG

Even before the publishers of computer games took action against the manufacturers and distributors of cheatbot software on the basis of copyright law, the attack on the cheatbot software took place on the basis of competition law, i.e. targeted obstruction according to Sec. 4 No. 4 UWG.¹⁶ The provider of the cheatbot software licensed it to integrated users for a fee.¹⁷ From the publishers' point of view, there was an interference in the competition for performance. The cheatbot interacted with the game software in a way that resulted in the users of the cheatbot having advantages over their fellow players who did not use cheatbots. The cheatbots are in the game. The player can "travel" and collect items without having to control his character himself. In this way, the figures of those players who use cheatbots become more "powerful". There is a competitive divide. Honest players, i.e. players who adhere to the ban on the use of cheatbots enshrined in the publisher's

⁴ *BGH MMR* 2017, 171 comments by *Biehler/Apel* - World of Warcraft I.

⁵ *ECJ MMR* 2014, 401 comments by *Oehler*, para 23 - Nintendo/PC Box and 9Net; *MMR* 2013, 671 comments by *Roth* para 20 - Video game consoles I; *MMR* 2015, 460 comments by *Roth* para 43 - Video game consoles II.

⁶ *BGH GRUR* 1991, 449 - Operating system; different view by *aberstumpf* in: *Büscher/Dittmer/Schiwy, Intellectual Property, Copyright, Media Law*, 3rd ed. 2014, Sec.15 UrhG para 3 et seq. and Section 69c UrhG para 2 et seq. *BGH* explains in *MMR* 2017, 171 commented by *Biehler/Apel* why nothing else emerges from the *ECJ*'s "Football Association Premier League" decision: There, the physicality had been affirmed by the court because the fleeting fragments of the work shown on the screen were temporarily physically fixed in the satellite decoder.

⁷ *Hentsch*, The Copyright of Publishers at eSport, *MMR-Beil.* 8/2018, 3, 5.

⁸ *BGH MMR* 2017, 171 comments by *Biehler/Apel* - World of Warcraft I.

⁹ *OLG München BeckRS* 2015, 119932: "The defendant has not acquired the right to reproduce the software for commercial purposes with the purchase of the client software. The client software is installation software. By installing and thus permanently reproducing the software on his PC, the buyer shall obtain the technical prerequisites for participation in online games. However, this right of reproduction does not exist for commercial purposes"; *OLG Dresden MMR* 2015, 402 comments by *Struwe/Hansen*.

¹⁰ *OLG München BeckRS* 2015, 119932; *Röttgen/Juelicher, DSRITB* 2017, 227, 233, there footnote 27.

¹¹ *BGH MMR* 2017, 171 comments by *Biehler/Apel* - World of Warcraft I; *Czychowski, GRUR* 2017, 362, believes that the class has won a Pyrrhic victory, because the *BGH* is basically of the opinion that the development of bots is permissible under Section 69d (3) UrhG. This was a "very broad view". *OLG Dresden* had still ruled that the examination of the functionality of the publisher's game software was not covered by the observation and investigation acts pursuant to Section 69d (3) UrhG, *OLG Dresden MMR* 2015, 407 comments by *Struwe/Hansen*.

¹² *BGH MMR* 2017, 171 comments by *Biehler/Apel* - World of Warcraft I.

¹³ *BGH MMR* 2017, 171 comments by *Biehler/Apel* - World of Warcraft I.

¹⁴ *BGH MMR* 2017, 171 comments by *Biehler/Apel* - World of Warcraft I.

¹⁵ *OLG München BeckRS* 2015, 119932.

¹⁶ Formerly Sec. 4 No. 10 UWG (identical).

¹⁷ For a description of the facts regarding the license model, see *LG Hamburg MMR* 2013, 725.

terms of use are at a disadvantage. With the same playing time they achieve less. However, there is another problem: In many online games there are mechanisms to achieve game progress neither through playing time nor alternatively through the acquisition of costly game advantages (so-called items). Those gamers who use a cheatbot can often save themselves the purchase of items in this way. If all players were to use cheat bots instead of purchasing the publisher's services, the publisher would no longer be able to operate his game economically. In any case, the use of cheatbots deprives the publisher of revenues that would have been generated by players if they had not used bots. However, it is difficult to estimate the damage revenue, as in most free-to-play online games only 1-5% of players buy items.¹⁸ Therefore, not everyone who uses a cheatbot would have spent any other money on the services he obtained with the cheatbot.

2. Competitive relationship

There is a competitive relationship between the cheatbot manufacturer and the publisher of the computer game with which the cheatbot interacts. This is understandable.¹⁹ It is true that in the present case there is no direct competition of customers alternatively choosing between the publisher's gaming software and the licensing of the cheatbot software. The cheatbot software is rather a complementary product, a kind of "accessory". However, it must be noted that the use of the cheatbot software has a significant influence on the sales of the game software. In the case where an act of its nature may necessarily have an adverse effect on the competition of another undertaking, a concrete competitive relationship exists with that undertaking, irrespective of whether the undertakings concerned are active on the same relevant market, as opposed to substitute competition.²⁰ Players, who are interested in the game of the publisher, but know that there are possibilities to get illegal advantages in the game because of the cheatbot, are deterred from purchasing the software.

3. Injury to the competitor

A targeted obstruction pursuant to Section 4 No. 4 UWG presupposes that the competitive development opportunities of a co-applicant are not only impaired as a reflex of the promotion and distribution of its own services, but that the obstruction primarily serves to damage the competitor. A certain obstruction of the competitor is also immanent to the performance competition, because it is aimed at withdrawing market shares from the competitor. In order to distinguish the permitted from the unauthorized disability, an overall assessment of the circumstances of the individual case is necessary. The conflicting interests of the participating competitors, consumers or other market participants as well as the general public must be weighed against each other.²¹ In the case of cheatbots, case law has assumed that the publisher of the games was deliberately obstructed "from the point of view of unfair sales-related obstructions by a sensitive intervention in the game system".²² As the developer of the game, the publisher is completely free to lay down the rules of the game. Cheatbot manufacturers "sensitively interfere with the World of Warcraft game system by tempting fellow players into using these bots and allowing them to use them in violation of the game rules".²³ The *LG Hamburg* has assumed that a game in which honest players are disadvantaged loses a lot of attractiveness if they know that their fellow players did not have to "acquire their skills just as expensively or protractively".²⁴

Nor did the *LG Hamburg* accept the argument that players are generally familiar with the existence of bots and have become accustomed to the fact that some figures develop more dynamically than others.²⁵ The attractiveness of the game is also diminished by the fact that a player cannot be sure whether the characters he encounters in the game are controlled by real people or whether they are characters controlled by cheatbots.²⁶ Especially in a game that is designed for the interaction of the other players, the fun of the game is reduced if there are "robots" in the game that at first glance cannot be distinguished from figures that are controlled by real people.²⁷ The cheatbots therefore have a significant impact on the publisher's business model: 'If customers are deterred, some of them will in any event refrain from purchasing the game and those who have already bought it will in some cases refrain from further playing and/or warn other customers by, for example, expressing themselves critically, disappointed or angrily on internet forums and in this way prevent other customers from purchasing the game'.²⁸

4. Incitement to breach of contract

In 2012, the 12th Civil Chamber of the *LG Hamburg* left open the question of whether, in addition to the aspect of targeted disability, there was also an unfair temptation to breach the contract,²⁹ the *OLG Hamburg* denied this.³⁰ In 2009, the 8th Civil Chamber of the *LG Hamburg* had still affirmed an incitement to breach the contract within the framework of an interim injunction procedure. Who offers functions by which the respective user can gain a competitive advantage over his fellow players because they are not intended by the publisher for the game and hence

¹⁸ However, World of Warcraft is not a free-to-play game, i.e. a game that is basically free to play and can only be bought as needed. World of Warcraft requires you to purchase a subscription. Furthermore, there is an economic system in the game, according to which you can exchange a gambling currency ("gold") for equipment etc.

¹⁹ BGH GRUR 2006, 1042 para 16 - Personal ads.

²⁰ BGH GRUR 2006, 1042 para 16 - Personal ads

²¹ BGH MMR 2004, 662 comments by *radio/time catch* - advertising blocker

²² *LG Hamburg* MMR 2013, 725.

²³ *LG Hamburg* MMR 2013, 725.

²⁴ *LG Hamburg* MMR 2013, 725 with reference to *LG Hamburg* GRUR-RR 2011, 478 (Ls.) - Runes of Magic Trading.

²⁵ *LG Hamburg* MMR 2013, 725.

²⁶ Also see the contribution of *Æxitus the monk* of 6.5.2016, available at: <https://www.youtube.com/watch?v=lcTKEFh8GtQ>.

²⁷ *LG Hamburg* MMR 2013, 725: "In particular, it can be assumed that it is an attraction of the game for relevant parts of the audience to be able to communicate with the other characters in the game world. It has remained undisputed between the parties that a bot cannot respond to a communication request of a real player. Even taking life probabilities into account, real players who bought "World of Warcraft" in order to communicate with other real players will be annoyed if there are no bots among the player characters that are recognizable as not responding to a response. It can therefore be generally assumed that the use of bots may be a reason for potential buyers to refrain from purchasing a game and a reason for players to cancel their subscription if they become aware of the use of bots in the game."

²⁸ *LG Hamburg* MMR 2019, 404.

²⁹ *LG Hamburg* MMR 2013, 725.

³⁰ *OLG Hamburg* MMR 2015, 313, 316 f.: "The term "temptation to breach a contract" may not, however, be interpreted so broadly that it already covers any activity directed towards distribution vis-à-vis the tied addressees (see *OLG Düsseldorf* NJW-RR 2003, 104 on the simple delivery request of a commercial buyer standing outside a distribution system to a tied authorized dealer). The decision to use the bot does not lie with the player, but with the player. Advertisements addressed to the general public are generally not sufficient for the element of misleading (*BGH* MMR 2009, 108 - bundesligakarten.de). Since an effect on the players beyond the mere offer of the Buddy-Bot cannot be determined, there is therefore no unfair inducement to breach the contract."

not offered, tempts you to commit a breach of contract. Under the terms of the contract, the use of 'additional programmes, scripts or other aids' is expressly prohibited.³¹ Furthermore, where a game is offered functions which are offered by the publisher only as premium functions subject to a cost obligation, this constitutes an exploitation of reputation in the sense of 'insertion in a foreign series'.³² That case-law is obsolete, namely, on the one hand, by the judgment of the *OLG Hamburg*³³ cited above and, on the other hand, by the fact that the *BGH* has not yet established the legal figure of the "Insertion into a foreign series."³⁴

IV. Claims under Trademark Law

Publishers of games have also used trademark law instruments against providers of cheatbot software. The providers advertise their cheatbot with reference to the game in which the cheatbot is used, i.e. about "WOW Bot" and "World of Warcraft Bot" (also in metatags of their website). The *LG Hamburg* considered such use to be distinctive use of the signs 'WOW' and "World of Warcraft" respectively and a trace of origin.³⁵ There is no descriptive use since no descriptive additions such as 'bot for' are used.³⁶ There is a likelihood of confusion. Use is not justified by Article 12 of Regulation (EU) 2017/1001 (Union Trade Mark Regulation) because it is contrary to accepted principles of morality.³⁷ Finally, there was anti-competitive conduct. The decision of the *LG Hamburg* was confirmed by the *OLG Hamburg*³⁸ and the *BGH*.³⁹

V. Claims from Contract Law

The *OLG München* had not confirmed a publisher of games any claim to take action against the distributor of cheatbots on the basis of contract law.⁴⁰ This was justified by the fact that the terms of use prohibiting the use of cheatbots had not been contractually agreed. A distinction must be made between the acquisition of the right to use the client software and the use of the publisher's online services. However, the bots' propagator only acquired the client software and did not accept the terms and conditions of the publisher's online services.⁴¹ The publisher did not address the conditions at all to cheat operators and did not offer them any conclusion of contract.⁴²

³¹ *LG Hamburg* MMR 2009, 772 (ls.) = BeckRS 2009, 20232.

³² *LG Hamburg* MMR 2009, 772 (Ls.) = BeckRS 2009, 20232; critical for insertion into a foreign series: *Rauda*, GRUR 2002, 38 ff.

³³ *OLG Hamburg* MMR 2015, 313, 316 f.

³⁴ *BGH* GRUR 2017, 79 - Segment structure.

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 points out special features of the annex claims.

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 - "House ban" on the Internet; *OLG Hamburg* MMR 2008, 58 - "House ban" on the 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.

VI. Claims from Virtual House Rules

The *OLG München* has confirmed the publisher of a game a claim against the manufacturer of cheatbot software for failure to allow the use of its online services on the basis of virtual domestic law analogous to Secs. 903, 1004 BGB (German Civil Code).⁴³ Virtual domestic law includes the authority of the operator of a forum on the internet to refuse a user access to the virtual room, i.e. the page on which the forum is operated.⁴⁴ The *OLG München* also applied this domestic right to online games. The Publisher may prohibit employees of the cheatbot host from gaining access to the games⁴⁵ (there is no obligation of the Publisher to tolerate according to Sec. 1004 (2) BGB⁴⁶ and also no obligation to tolerate according to antitrust law⁴⁷). However, such a claim is not worth much economically, since the damage is not caused by the access of the manufacturers of the cheatbot to the games, but by the fact that players in the game use the cheatbot and thus gain game advantages. The virtual house right does not go so far that one can derive from it a cease-and-desist claim regarding production, use and spreading of the cheatbot.⁴⁸ Utilization of the information obtained by unauthorized access to the publisher's online services cannot be prohibited, since obtaining and using information in breach of property rights does not constitute deprivation of fruit.⁴⁹

VII. Claims from the established and exercised Business Enterprise

From Sec. 823 (1) BGB from the point of view of the established and exercised business enterprise the distribution of the cheatbot software cannot be forbidden. Offering the software does not constitute any direct, operational intervention in the Publisher's business.⁵⁰ It is up to the players to decide whether they will play by the rules or using cheatbots in violation of the rules.⁵¹ The players thus act between the publishers and the providers of the cheatbots.

VIII. Conclusion

It has been shown that game publishers have successfully found legal ways to curb the distribution and use of cheatbots. The aim was not to meet the user of the cheatbots, but to get to the root of the problem and take action against the provider. Subscription claims against the user who uses cheatbots regularly arise due to a violation of the terms of use. Such a violation justifies the termination of the user contract between the user and the publisher. Trademark claims against distributors of cheat bots relate to the use of cheatbots in connection with the brand name of the game. Such claims can be circumvented by describing the cheatbots with "Bot for XYZ" and not offering them under "XYZ Cheatbot". The copyright claims are directed against the reproduction of the client software, not against the cheatbot software. Most effective, however, are the claims under competition law, as they are directed against the offer of the cheatbot software itself.



Dr. Christian Rauda

is a board-certified specialist lawyer for information technology law, board-certified specialist lawyer for copyright and media law and board-certified specialist lawyer for industrial property rights and partner of the media law firm GRAEF Rechtsanwälte (Hamburg/Berlin) as well as lecturer at the Hamburg Media School, Bucerius Law School and the HTW Berlin.

Editor: Anke Zimmer-Helfrich, Editor-in-Chief (responsible for the text section); Ruth Schrödl, Editor; Eva Wanderer, Editorial Assistant; Maren Otter, Volunteer, Wilhelmstr. 9, 80801 Munich, Postal address: Postfach 40 03 40, 80703 Munich, Telephone: +49 89/381 89-427, Fax: +49 89/38189-197, E-Mail: mmr@beck.de

Manuscripts: Manuscripts must be sent to the editors. The publisher is not liable for manuscripts that are submitted unsolicited. They can only be returned if return postage is enclosed. Acceptance for publication must be in writing. With the acceptance for publication the author transfers to the publishing house C.H.BECK for the legal duration of the copyright the exclusive, regionally and temporally unrestricted right to the duplication and distribution in physical form, the right to reproduction and making available, the right to inclusion in data bases, the right to the storage on electronic data media and the right to their distribution and duplication as well as the right to other utilization in electronic form to the publishing house C.H.BECK at its contribution. These include forms of use that are still unknown today. The author's mandatory secondary exploitation right laid down in Sec. 38 (4) UrhG after 12 months after publication remains unaffected by this.

Peer review process: Each contribution will be read and evaluated in anonymized form by the editors and two reviewers prior to publication.

Copyright and publishing rights: All articles published in this journal are protected by copyright. This also applies to the published court decisions and their guidelines, because these are protected insofar as they have been prepared or edited by the sender or by the editorial staff. The legal protection also applies to databases and similar facilities. No part of this journal may be reproduced, distributed or publicly reproduced or made accessible in any form, stored in databases, stored on electronic data carriers or otherwise electronically reproduced, distributed or used in any other way outside the narrow limits of copyright law without the written permission of the publisher.

Advertising Department: Verlag C.H.BECK, Advertising Department, Wilhelmstraße 9, 80801 Munich, Germany, Postal address: Postfach 40 03 40, 80703 Munich, Germany.

Media consulting: Telephone +49 89/3 81 89-687, Fax +49 89/3 81 89-589. Disposition, production of advertisements, technical data: Phone (+49 89) 3 81 89-603, Fax +49 89/3 81 89-589, E-mail: anzeigen@beck.de.
Responsible for the advertising section: Bertram Götz

Publisher: Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 Munich, Postal address: Postfach 40 03 40, 80703 Munich, Tel.: +49 89/381 89-0, Telefax: +49 89/38 18 93 98, Postbank Munich IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX.

Frequency of publication: Monthly.

Purchase prices 2019: Annually €429,- (incl. VAT). Special price for members of davit €335,- (incl. VAT). All subscription prices including news service MMR-Aktuell and MMRDIREKT. Single issue: €41,50 (incl. VAT); shipping costs extra. The invoice is issued at the beginning of a reference period. Subscription and subscription price include the print edition as well as a license for the online edition. The components of the subscription cannot be cancelled individually. Complaints about copies not received can only be made within 6 weeks of the publication date. The annual title pages and register are only available with the respective issue.

Orders through any bookshop or with the publisher. Sales Cooperation in Switzerland: Helbing & Lichtenhahn Verlag AG (CH) & CoKG, Elisabethenstraße 8, CH-4051 Basel, Tel.: +41 (0)61 228 90 70, Fax: +41 (0)61 228 90 71, e-mail: zeitschriften@helbing.ch.

Customer Service Center: Telephone: +49 89/3 81 89-750, Fax: +49 89/3 81 89-358, E-mail: kundenservice@beck.de

Cancellations must be made 6 weeks before the end of the year.

Address changes: Please let us know your changes of address in good time. Please state the title of the magazine and the new and the old address. Notice according to Sec. 4 (3) of the Postdienst-Datenschutz-Verordnung (Postal Privacy Provision): If the address of the subscriber changes, Deutsche Post AG can inform the publisher of the new address even if no forwarding request has been made. The subscriber may object to this within 14 days of the publication of the magazine at the publisher.

Set: FotoSatz Pfeifer GmbH, 82152 Krailling.

Printing: Print shop C.H.BECK, Bergerstraße 3-5, 86720 Nördlingen.
ISSN 1434-596X