Proceedings of the International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7064/15/20230534

The Social Harms and Criminal Liability of Selling Cheating Software for Online Games: A Legal Perspective

Wen Wang[1,a,*]

[1]*Huazhou No. 3 Middle School, Building A1401, Block 15, Ju Zhou No.1, Huazhou City, Guangdong Province, China*
a. 3077522896@qq.com
**corresponding author*

Abstract: With the advancement of science and technology, various forms of cybercrimes related to the internet have emerged. The sale and distribution of cheating software for online games are among these cybercrimes. However, when the criminal law was developed, the internet was not as advanced as it is today, leading to ambiguity in defining and prosecuting cybercrimes. This paper comprehensively analyzes the sale and distribution of cheating software for online games from the perspectives of its social harms and legal implications, taking into account national laws, regulations, and judicial interpretations.

Keywords: cybercrime, cheating software, sale, criminal liability

1. Introduction

In today's highly developed era of the internet, it has become an integral part of people's daily lives. Online gaming and online shopping have become popular ways for people to pass their leisure time. With a large user base, these activities have given rise to various unconventional criminal acts, such as intrusions into and modifications of others' online information or the creation and sale of cheating software for games. These emerging forms of criminal behavior pose new challenges for the application of criminal laws under the Chinese legal system. Furthermore, the use of cheating software in online games has a significant impact on the gaming experience of other users, disrupting the normal online environment. In severe cases, it can even jeopardize the personal privacy and property of other users, thereby undermining the order of the online community. Based on these premises, this paper examines the application of criminal liability to the sale and distribution of cheating software for online games from a legal perspective, offering new theoretical insights for judicial decision-making.

2. Overview of the Sale of Cheating Software for Online Games

2.1. Definition and Characteristics

"Cheating software" refers to programs or software created by third parties without the consent of the copyright owner, which maliciously modify game data to benefit players. "Cheating software for online games" refers to a type of program that maliciously alters the running data of a game. Its characteristics typically include: (1) malicious modification of program running data without the

DOI: 10.54254/2753-7064/15/20230534

consent of the game copyright owner, (2) the ability to save players time or money to achieve certain actions, and (3) widespread availability. The emergence of cheating software for online games has led to imbalances within these games, greatly undermining the fairness of online gaming and the order of the online market.

2.2. Market Size and Development Trends

According to estimates by Tencent's Guardian Program Security Team, the actual sales volume of cheating software for online games in China has exceeded 2 billion yuan annually [1]. This has a substantial impact on many popular domestic games, such as PlayerUnknown's Battlegrounds and Arknights. In games with fewer players, instances of cheating software for online games are much less frequent. Hence, the creators and sellers of cheating software tend to target games with larger player bases, and currently, cheating software is prevalent in a wide range of games, indicating an intent to infiltrate most games.

2.3. Analysis of Relevant Cases and Events

Basic Case Details and Judgment Outcomes:

Between January 2021 and February 2022, the defendants, Mr. Li and Mr. Chen, agreed that Mr. Li would develop cheating software (referred to as "cheats" hereafter) for the online game "Crossfire" ("逆战" in Chinese). These cheats included features like "wallhack" and "aimbot." Mr. Li sold the cheats, along with access passwords, to Mr. Chen, acting as an agent, for 200 yuan. Mr. Chen then resold the cheats at a higher price through platforms such as WeChat to his own agents, who further distributed the software. These cheats could technically enable features like "wallhack" and "automatic aiming."

The court determined that the actions of the two defendants violated Article 285 of the Criminal Law [2].

In the aforementioned case, Mr. Li developed cheating software for the game "Crossfire," which enabled features like "wallhack" and "automatic aiming" by illegally intruding into and modifying the game's running data. This was done to improve their in-game performance and ranking. The court convicted both Mr. Li and Mr. Chen of providing tools and programs to illegally access and control computer information systems. Mr. Li provided the tools and programs designed for illegal access and control, while Mr. Chen facilitated the sales and distribution channels, with both individuals infringing upon the computer information systems' programs. Their subjective intent was for profit, and the objective aspect involved the creation and sale of game cheats.

In the view of this study, Mr. Li's actions also constituted the offense of damaging computer information systems. To determine whether Mr. Li's actions constituted this offense, it is necessary to establish whether the game "Crossfire" falls under the definition of a computer information system according to China's "Regulations on the Security Protection of Computer Information Systems" [3]. According to Article 2 of these regulations: "A human-machine system composed of computers and their related and supporting devices and facilities (including networks) that collect, process, store, transmit, retrieve, and otherwise handle information in accordance with specific application objectives and rules." It is evident that online games fall within the scope of computer information systems as defined by Chinese law.

In the aforementioned case, Mr. Li's cheating software for the game "Crossfire" involved the criminal act of deleting, modifying, and adding functionalities to the computer system, which satisfies the elements of the offense of damaging computer information systems.

Considering other relevant provisions of the Criminal Law, it can be concluded that Mr. Chen also violated Article 287-2 of the Criminal Law by assisting in activities related to information network

DOI: 10.54254/2753-7064/15/20230534

crimes [4]. In this case, Mr. Chen, despite knowing that Mr. Li's creation of cheating software for "Crossfire" was illegal, continued to supply this software to Mr. Wei and Mr. Zhang, his agents, for resale, and facilitated the payment settlement process for Mr. Li. Therefore, it can be determined that Mr. Chen violated the offense of assisting in activities related to information network crimes.

3. Social Harms and Impacts

Issues of Game Balance and Fairness: In recent years, online games have experienced rapid development and have become an integral part of daily life for a wide range of users, making them a mainstream form of entertainment. When discussing game balance and fairness, it is essential to address the disruption caused by cheating software to these aspects of gaming. Currently, most game designs focus on "non-absolute balance," characterized by fast iterations, strong player experiences, and a high sense of participation. In such designs, all players can achieve a sense of satisfaction that is roughly equal when investing their time, energy, and money into the game, provided there are no major errors in the game data platform. Game fairness implies that under equal efforts, there should not be significant disparities within the game environment. However, it is evident that the introduction of cheating software disrupts game balance and fairness. Malicious actors profit from the creation and sale of cheating software, while buyers, equipped with "cheats," obtain a gaming experience that exceeds the norm by enhancing certain virtual values. This undoubtedly undermines the game's balance and fairness.

4. Legal Framework and Criminal Liability

Overview of Relevant Laws and Regulations:

(1) The sale of cheating software for online games is closely related to laws such as the "Cybersecurity Law" and the "Criminal Law." Several specific legal provisions are frequently applied, including Article 287-2 of the Criminal Law, which defines the offense of assisting in activities related to information network crimes. This article recognizes the act of "selling" cheating software for games as providing pathways for advertising and payment settlement. However, it does not classify this as aiding and abetting the primary offense; instead, it establishes sentencing guidelines [5]. It should be noted that if a behavior aligns with this provision but also fully meets the conditions for establishing joint principal offenders, it should be directly regarded as the primary offender of the relevant cybercrime [5].

(2) The sale of cheating software for online games is also applicable to Article 285-2 of the Criminal Law, which stipulates the offense of providing tools and programs to illegally access and control computer information systems. The act of "selling" can be construed as "knowingly providing tools and programs for someone else's illegal actions of invading and illegally controlling computer information systems."

(3) This behavior also falls under the "other circumstances" category specified in Article 225 of the Criminal Law [6]. To determine the criminal liability of selling cheating software for online games, several factors need to be considered: a. Clarify whether "cheating" programs belong to the "other circumstances" category defined in Article 225 of the Criminal Law. b. Determine whether the act of selling cheating software for games constitutes illegal business operations. c. Assess whether the act of selling cheating software for games meets the criteria for criminal liability as outlined in this article.

According to Article 24 of the "Regulations on the Protection of Computer Software" issued by the State Council, cheating software for games can be classified as illegal publications [7]. Engaging in illegal publishing activities related to such software has already been deemed a criminal offense, as indicated by Article 19 of the "Internet Information Service Management Measures," which elevates China's efforts against illegal publishing activities to the criminal level [8].

DOI: 10.54254/2753-7064/15/20230534

(4) Finally, the sale of cheating software for online games also constitutes an offense under Article 218 of the Criminal Law [9]. The scenarios recognized under this offense are those specified in Article 217, Section 6 of the Criminal Law [10].

5. Challenges and Issues in Criminal Liability

5.1. Challenges in Conviction and Sentencing

In terms of judicial application, there are four applicable charges for the sale of cheating software for online games. These charges include aiding in activities related to information network crimes, providing tools and programs to illegally access and control computer information systems, illegal business operations, and selling infringing copies. Notably, the offense of aiding in activities related to information network crimes was added after the promulgation of the "Criminal Law Amendment (XI)" [11]. Consequently, there were no judicial cases involving this charge before 2020. Similarly, before the promulgation of the "Criminal Law Amendment (VII)," the offense of providing tools and programs to illegally access and control computer information systems was not a part of judicial practice. It can be observed that as the state introduces and improves relevant legal provisions, the conviction of computer and internet-related crimes becomes clearer. Currently, most academic discussions on the conviction and sentencing of individuals involved in selling cheating software for online games focus on these four charges. Challenges in conviction and sentencing still persist and are characterized by the following issues:

(1) Further clarification of the concept of "copying" is needed. To determine whether the sale of cheating software for online games aligns with the definition of selling infringing copies as stipulated in Articles 217 and 218 of the Criminal Law, a precise definition of the act of creation and sale must be established.

(2) Regarding the recent application of Article 287-2 of the Criminal Law, there is a challenge in setting sentencing standards. This article recognizes aiding behaviors as primary offenses and imposes sentencing based on relevant primary offenses or the "sentencing standards for aiding offenses" specified in the article. Judicial practice needs to clarify whether a criminal act indeed meets the conditions for joint principal offenders, which remains one of the current challenges.

(3) In terms of judicial application, the conviction of the sale of cheating software for online games should be based on the actual circumstances and facts of each case, aligning with the principles of justice.

5.2. Technological Means and Challenges in Evidence Collection

To establish that the creation and sale of cheating software for online games constitute criminal acts, it is necessary to understand what "cheating software" entails and conduct investigations to gather evidence. Currently, both judicial practice and academic research are constrained by technological limitations, which hinder timely detection and evidence collection. This has allowed unlawful actors to evade punishment. In light of these challenges, judicial authorities and experts in relevant fields should employ more advanced technologies to achieve timely evidence collection. Scholars should also contribute to further defining "cheating software."

6. Conclusion

6.1. Summary of Research Findings

In summary, the judicial application regarding the sale of cheating software for online games remains complex. This study finds that such behavior can be more suitably categorized within the scope of

DOI: 10.54254/2753-7064/15/20230534

Article 287-2 of the Criminal Law. In terms of judicial application, technical professionals should focus on technological innovations related to "cheating" behaviors and collaborate with relevant gaming companies to disrupt the circulation of the cheating software industry. Experts and scholars in relevant fields should stay updated with legal developments and provide reasonable interpretations of the charges based on the evolving national context.

6.2. Prospects for Future Research and Practice

In the rapidly evolving era of technology, with continuous technological advancements, there will inevitably be emerging forms of computer-based criminal activities. It is believed that future experts and scholars will be able to promptly identify, address, and resolve these issues through research and practical solutions.

References

[1] *Author(s). (2020, November 24). Exploring multidimensional approaches to combat governance [News article]. Legal Daily, 10.*
[2] *Qingdao Haitai Xinguang Technology Co., Ltd. (2022, June 7). Notification regarding the reduction of shares by shareholders holding more than 5% of the total shares exceeding 1% [Notice]. Securities Daily, D21.*
[3] *See Article 2 of the Regulations on the Security Protection of Computer Information Systems.*
[4] *See Article 287-2 of the Criminal Law.*
[5] *Zhang, M. (2016). On the crime of aiding online criminal activities. Political and Legal Studies, (2), 5.*
[6] *See Article 225 of the Criminal Law.*
[7] *See Article 24 of the Regulations on the Protection of Computer Software.*
[8] *See Article 19 of the Administrative Measures for Internet Information Services.*
[9] *See Article 218 of the Criminal Law.*
[10] *See Article 217 of the Criminal Law.*
[11] *See Amendment XI to the Criminal Law.*