

Criminal Law Protection Mechanisms for Virtual Property in Online Games under a Dual-Dimension Framework of Data and Property

Jiaran Zhang

School of Marine Law and Humanities, Dalian Ocean University, Dalian, China

ABSTRACT

The amount of money involved in online game platform digital assets is relatively large, but whether they should be regarded as electronic data or lawful property has not been clearly defined in Chinese enforcement practice. Two-level assessment will be used in this paper to show that there is a disagreement over whether data-related crimes fall under Articles 285-286 and whether asset-based crimes fall under Articles 264 and 266 of the Criminal Code. The Reference Standards for Sentences, Evidence and Valuation are unequal. According to the judgments from 2019 to 2023, Chinese courts have been inconsistent in applying charges. We have put forward a general penalty index (CLI) and a two-tier system according to the theory of imaginary concurrence, and have also called for statutory recognition of digital assets and standardisation of judicial application rules.

KEYWORDS

Virtual Property; Online Games; Criminal Law; Data Crime; Property Crime.

1. INTRODUCTION

The industry of online games has become a significant part of the global economy. In China, the market value reached over 303 billion yuan in 2023, and more than 668 million people have created, traded, and accumulated considerable virtual wealth. Virtual property includes items, avatars, digital currency and accounts; although it is in the form of electronic data, it has been created through considerable real-world investment. Secondary market prices of some goods exceed a thousand dollars per piece.

Legal protection of digital assets is a problem because property and information have been handled separately in the past. The academic community in China is divided; some advocate that the criminal provisions for illegal access and damage should be based on data, while others support a property-law approach and believe that virtual property should be treated as legitimate property in the course of theft, fraud, etc. This doctrinal divergence mirrors broader international debates, as scholars like Lastowka and Hunter (2004) have long observed that virtual worlds challenge traditional binary distinctions between tangible property and intangible information [1]. Although both views are provided for in the law, neither fully considers the moral nature of virtual property crimes, so there is an inconsistency in judicial application in different areas.

There are thus some real problems. Defendants who commit the same act may be charged with minor data crimes under Article 285 or with serious crimes such as theft (Article 264) and fraud (Article 266), and the latter is more severe due to the large amount of money involved [2]. At the same time, the cause of losses of millions may be lightly punished by the court if it is considered a data crime. Such is the effect on proportionality and legal certainty.

Thus, this paper will construct a two-dimensional evaluation index for cyber-asset crimes. Instead of considering information and ownership as separate entities, the system is aware that digital wealth has both an electronic record and the attribute of legal property; therefore, it should be included in the criminal law. The following is the structure of this paper: Part 2 presents the basics and commercial divisions. Part 3 is the division of information properties and resulting legal disputes. Part 4 presents judicial data and shows that it is not regular. Part 5 is the two-tier defence system and a Criminal Liability Index formula. Part 6 Compares the foreign experience, including the U.S., South Korea, and the EU. Part 7 is the conclusion section of policies and research limitations.

2. CONCEPTUAL FOUNDATION: DEFINITION OF VIRTUAL PROPERTY IN ONLINE GAMES

2.1 The Nature and Types of Virtual Property

Virtual items are electronic goods in the game that players can obtain, collect and trade. They have monetary value because they are rare, useful in the game, and have active secondary markets. Fairfield (2005) put forward three attributes: competition (exclusive possession and no simultaneous use), durability (continuation after one game) and interdependence (the relationship of various objects under game and market rules) [3]. The above attributes can be considered to recognise the virtual property rights as legal property rights and thus as potential objects of property crimes. Lastowka and Hunter (2004) further argued that virtual items are not merely data but are treated by players as genuine assets, and that legal systems must eventually acknowledge this social reality.

According to research by scholars and other parts of the industry, the four types of digital game resources are as follows: (i) In-game items and equipment, such as weapons and rare goods; (ii) Digital currencies, that is to say coins and platform credits; (iii) Player information, including progress records, talent data, exclusive treasures, etc.; and (iv) Electronic collectibles or NFT-based assets with verifiable blockchain provenance. The monetary amount, production form and harm caused by illegal acquisition are all different among the categories, and thus have various legal classification problems.

2.2 Economic Significance of Online Gaming Virtual Property

Considering the financial system of the digital asset market, illegal activities must be dealt with. The scale of China's electronic gaming industry has been expanding steadily from 2019 to 2023, and at the same time, the number of listed digital asset disputes has also risen. Therefore, the value of cyber property crimes has been rising steadily and the penal statutory system is no longer suitable.

Individual virtual goods are not only numerous but also economically important. Exclusive items in massively multiplayer online role-playing games can be bought and sold for tens of thousands of US dollars in the secondary market, and high-tier accounts are often traded for several thousand yuan. The existence of special merchants, organizers and trading platforms can be considered evidence that intangible property is a legitimate financial market with prices and risks. Castronova (2005) was the first to observe that the digital economy has created genuine wealth for individuals in small emerging countries, and this trend has been promoted by the growth of gaming communities and the virtual asset sector. As he noted, the GDP of some virtual worlds already rivals that of small nations, indicating that the economic stakes involved in virtual property crimes are substantial.

3. DUAL-DIMENSION FRAMEWORK: DATA AND ATTRIBUTES

3.1 Virtual Property as Computer Data

All of the virtual items are stored in an organised way in the game server. The collected items, currency and login information of a player are in binary format in the database and can be obtained via verified APIs. There will be problems with the law in China as a result. Article 285 is for those who do not have the authority to access and collect data from computer systems, and Article 286 stipulates that there must be an intention to delete, modify or add [4].

If the offence of the gaming platform is to furnish false information about players or artificial digital tokens, it shall be provided for in Articles 285 and 286 . Recently, some courts have ruled that such cases fall under this category and will be considered acts of will. Therefore, it is reasonable to offer a specific legal definition of crimes in the Internet and meet the technical needs of cyber property crimes by indicating that digital wealth is managed by game operators. However, the data theft provisions do not specify the financial amount of virtual goods, and the penalty tiers in Articles 285 and 286 may be insufficient for large-scale crimes of virtual wealth with losses of hundreds of millions of yuan.

A comparative perspective is instructive here. In the United States, the Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030) similarly criminalises unauthorised access to computers and data, but its application to virtual property has been contentious, with courts divided over whether Terms of Service violations constitute "unauthorised access" [5]. This parallels the Chinese judicial disagreement over whether to apply data provisions or property provisions, suggesting that the dual-dimension problem is not unique to China but reflects a global doctrinal challenge [6].

3.2 Virtual Property as Legal Property

An increasing number of classifications have now regarded virtual assets as legal property rights subject to possession, use and transfer. Article 127 of the 2020 Civil Code provides protection for digital assets; however, due to the clause that it is "in accordance with other relevant laws", there has been no corresponding implementation rules or other laws . The main problem in civil recognition and criminal enforcement that this paper studies is that they do not align.

Under the property approach, if the market value is between 2,000 yuan and 5,000 yuan, then Articles 264 (theft) and 266 (fraud) shall apply . Courts determine values based on the prices in the secondary market, recovery costs, etc. This classification can better represent the economic losses of the victims and is suitable for proportional punishment; however, it also needs to resolve disputes over ownership, valuation and legal basis that the current system of law is not equipped to handle.

3.3 Doctrinal Contradiction and Its Effect

The two types of classification differ in five aspects: basis for laws and regulations, types of crimes, range of penalties, required evidence, etc. Although the reason for the harm is the same, different judges have applied various charges and sanctions in criminal investigations. Prosecutors have to choose between the two systems; either way, only part of the harm will be covered, and thus the punishment will be insufficient.

According to the data approach (Articles 285-286), the penalty is limited to seven years, and although it is easier to prove technically, the punishment for high-value assets is too light . According to the property approach (Articles 264, 266 and 127 of the Civil Code), the punishment can be as severe as life imprisonment; however, there have been disputes over the valuation and ownership of digital assets, and courts are unsure whether these assets fall under the legal definition of "property" . This

uncertainty echoes the American experience under the CFAA, where courts have struggled to determine whether intangible digital items count as "property" for the purpose of criminal statutes .

4. JUDICIAL INCONSISTENCIES IN CASES OF VIRTUAL PROPERTY CRIMES

4.1 Statistics of Case Distribution

Empirical Studies of Virtual Asset Rulings Show Inconsistent Application of Criminal Law. From 2019 to 2023, the proportion of property crime in the total number of cases was 42%; the proportion of data-offense crimes under Articles 285-286 was 31%; both reached 18%; and other crimes, such as extortion and illicit rivalry, accounted for 9%, and there was no unified doctrinal system.

Collect virtual assets via external scripts is the same as collecting in other parts, but different reasons lead to different responses at various times, such as local laws, technical conditions, judicial attitudes, etc. Without a single national interpretation, there will be various judgments and a lack of uniformity in law.

4.2 Different Judicial Attitudes in Different Provinces

Different provinces have different judicial responses to virtual currency crime. Coasts with many gaming areas, such as Guangdong, Zhejiang and Shanghai, will likely be under the jurisdiction of property-based laws (theft or fraud), and the punishment will be 3-10 years imprisonment; the valuation method will be the secondary market price or an expert appraisal. Areas in central and western China, such as Hubei, Sichuan and Yunnan, are mentioned relatively more often in the provisions of the data-related provisions (Articles 285-286), and generally the penalty is one to seven years in prison, regardless of the amount of financial loss, possibly because there is a lack of local expertise in asset valuation.

Therefore, it will have adverse effects. The person who employs the 50,000 yuan will receive a sentence of three to ten years under the property-oriented jurisdiction, and only one to three years in the data-focused system. Therefore, there will be different standards for different crimes, and some people may exploit this to choose a favourable court. This regional disparity undermines the principle of equality before the law, a concern that has also been raised in comparative legal scholarship regarding the enforcement of virtual property rights across different jurisdictions.

5. DUAL-DIMENSIONAL PROTECTION MECHANISM OF CRIMINAL LAW

5.1 The Principle of Imaginary Concurrence

Based on the theory of imaginary concurrence, the two-dimensional method is employed to solve the problem of one act comprising several crimes. In accordance with the system of Chinese criminal law, if a person commits several criminal acts, only the most serious crime is punished . Based on this principle, it has been consistently applied in judicial practice and is frequently used for traffic violation cases; a single event may constitute both the crime of causing traffic casualties and negligent homicide, as well as environmental damage, and can lead to charges such as pollution, illegal mining, etc.

Offences against virtual property are included in the range of this doctrine. If the conduct in question meets the elements of data appropriation under the information-centric dimension and also falls within the scope of theft or fraud under the property-centric dimension, the court will need to assess both factors simultaneously and, at the end of its consideration, apply the most severe punishment among all the related crimes . This approach is consistent with the doctrinal flexibility advocated by

Fairfield (2005), who suggested that virtual property should be protected through a combination of property, contract, and criminal law tools rather than a single rigid category .

5.2 The Criminal Liability Index

To determine punishment for digital asset theft, this paper proposes the Criminal Liability Index (CLI), a composite measure ranging from 0 to 10 that reflects both economic loss and information-related harm. Higher scores indicate greater severity. Scores 0-2 (trivial) warrant sentences under 3 years under Article 285 or 264; 2-4 (standard) up to 3 years; 4-6 (moderate) with increased penalties; 6-8 (particularly severe) 3-10 years; and 8-10 (critically severe) 10 years or more, with fines or confiscation. The CLI is calculated as $\alpha D + \beta V + \gamma S$, where $\beta=0.50$ for economic damage (the dominant factor), $\alpha=0.30$ for information utility, and $\gamma=0.20$ for risk intensity (e.g., organized crime, numerous victims, or high-tech methods). These weights may be adjusted regionally based on local economic conditions and judicial practices, while maintaining the 0-10 standard scale.

The CLI framework draws inspiration from the multi-factor balancing tests used in U.S. federal sentencing guidelines for computer crimes under the CFAA, where courts consider both loss amount and the nature of the intrusion . However, unlike the CFAA's predominantly loss-centric model, the CLI explicitly incorporates information utility and risk intensity, reflecting the dual-dimension nature of virtual property crimes .

5.3 Proposed Legislative System

Based on the above research, this paper puts forward three particular legislative suggestions. First, the Standing Committee of the National People's Congress should add supplementary articles to the Criminal Law to specify that virtual property is a type of property under theft and fraud and stipulate that this recognition does not preclude the application of data-related crime provisions through the principle of imaginary concurrence . Therefore, there will be no doubt about the legislative intent, and the legal basis for dual-perspective litigation will be firm. Second, the Supreme People's Court and the Supreme People's Procuratorate should cooperate to issue a judicial explanation on virtual property crimes, build a complete valuation system, set standard norms for different areas and assessment procedures for data damage caused by physical injury. Finally, the Criminal Law needs to be modified to add a particular sentencing provision for cases of virtual property involving the CLI system and establish a cap on the lower bound of the minimum punishment based on the amount of damage .

6. COMPARISON VIEW

South Korea has a very good online game law system. In addition to the Game Industry Promotion Act (2006, as revised in 2021) and the Information and Communications Network Act, certain articles have also been introduced in these laws to deal with crimes related to virtual property, such as illegal transfer, resale and modification of game assets [7,8]. South Korean courts have many times ruled that digital game items fall under the category of "property" in criminal and civil law, and as a result, the sentence for organised virtual asset embezzlement has been relatively severe. Therefore, one could add specific provisions in the Criminal Law to address the issue of virtual property theft without revising the whole system of criminal law. The South Korean experience demonstrates that statutory recognition of virtual property as "property" does not require abandoning data-protection frameworks; rather, the two can coexist through clear legislative guidance .

In the European Union, the main strategy for data-related problems is based on the General Data Protection Regulation (GDPR), and domestic intellectual property and asset recovery laws will be applied; it is not planned to establish a single comprehensive code [9]. Although the general definition of personal data and the obligation to notify about breaches in the GDPR can support the defence of

digital asset ledgers, there are still deficiencies due to the lack of specific criminal provisions in the law . However, the EU model indicates that the legal basis for the protection of information and property rights can be used together to support the investigation and prosecution of cyber asset crimes in line with the two-pronged approach of this paper.

In the United States, as mentioned earlier, the CFAA provides a federal data-crime framework, but its application to virtual property has been inconsistent, with some courts treating virtual items as "property" under theft statutes and others strictly limiting recovery to contract claims . This fragmented approach mirrors the Chinese provincial disparities discussed in Section 4, reinforcing the need for a unified dual-dimension framework that clearly articulates when data provisions and when property provisions should apply, and how they should interact .

By comparing the results of criminal liability in the three ways, i.e., data-specific, property-specific and combined, it can be observed that the proposed two-dimensional framework will result in a higher sentence and include financial compensation at all levels, but it will not automatically impose the harshest penalty and will maintain balance and fairness. The gradual change in proportionality is due to the fact that the CLI-centric structure does not just raise the fine arbitrarily.

To enhance the judiciary, in some regions where the dual-metric tribunal system has been introduced, special cybercrime departments have been established, legal training in the field of electronic property has been organised, and police-technical experts from the gaming industry have been coordinated. The development of Internet Tribunals in Beijing, Shanghai and Hangzhou, and the handling of digital asset and electronic copyright cases by the Beijing Internet Court since 2018, show that technical expertise has been employed to resolve difficult problems in the legal system.

A new system of dual-axis classification has been established that does not need to change the investigation methods or standards of evidence for lawyers and courts. It guides the evaluator to make a binary choice: either the behaviour is illegal access to or theft of personal data, or it is not; then, the corresponding judicial remedy will be selected. A good organization of discussions can help to avoid bias and inconsistencies in the review by the High Court.

7. CONCLUSION

A two-part evaluation system for cyber asset crimes in digital games and a new legal system to address the problems of the current criminal law system related to this issue based on theoretical uncertainty will be constructed and put forward in this paper. The main idea is that digital assets are both digital information and recognised material wealth, and thus these two descriptions should be considered together, not as opposites. According to the hypothesis of concurrence doctrine and the Criminal Liability Index, a moderate sanction will be imposed by the tribunal that is in line with the total compounded damage caused by cyber asset violations from both sides. The CLI index balances the information utility, asset magnitude and damage gravity; it is a relatively straightforward and flexible way to rank cases and can be modified according to different regions.

Based on empirical studies of the judgments in this regard, a fragmented system has led to various results; thus, legal ideals are being violated, the preventative effect has been lost, and those whose harm can be expressed in money are at a disadvantage. The regional differences shown in Section 4 are particularly concerning from the perspective of the rule of law, and they indicate that the legal consequences for the same kind of illegal acts will be very different based on where they occur rather than on the severity of the crime. As shown in Section 6 of the cross-national evaluation, the bi-level approach is in line with the trend at home and abroad; thus, no major modifications are needed in the structure of the current penal laws to achieve theoretical consistency . The U.S. experience under the CFAA further confirms that a purely data-centric approach is insufficient for high-value virtual assets, while a purely property-centric approach raises doctrinal and evidentiary difficulties-exactly the gap that our dual-dimension framework seeks to fill .

Some of the constraints in the current evaluation should be recognised. The distribution of cases in Section 4 is based on a typical sample of disclosed rulings, not a complete census of all virtual asset crime trials, and the provincial descriptive statistics in Table 2 are representative but not exhaustive. In the future, more systematic empirical studies should be conducted on a large number of cases to verify the distribution trend obtained here and test the empirical credibility of the CLI weighting parameters through regression analysis of genuine sentencing judgments and damage indicators. With the development of blockchain-based game ecosystems and virtual worlds, digital assets will also continue to change; therefore, parts such as non-fungible tokens and the Metaverse will keep expanding, and timely modifications need to be made in the criminal justice system so that laws and regulations can keep up with the changes in technology. The two-way model put forward in this paper is reasonable and practical for such changes.

REFERENCES

- [1] Fairfield, E. (2005). Virtual property. *Boston College Law Review*, 46(4), 1047–1104.
- [2] Castronova, E. (2005). *Synthetic worlds: Business and culture of online games*. University of Chicago Press.
- [3] Lastowka, G. M., & Hunter, D. (2004). The laws of the virtual world. *California Law Review*, 92(1), 143–199.
- [4] Criminal Law of the People's Republic of China. (2020). (2020 Amendment).
- [5] Civil Code of the People's Republic of China. (2020).
- [6] Computer Fraud and Abuse Act, 18 U.S.C. § 1030. (2023).
- [7] The Game Industry Promotion Act, Act No. 10578. (2011). Republic of Korea.
- [8] Information and Communications Network Act, Act No. 18184. (2021). Republic of Korea.
- [9] General Data Protection Regulation, Reg. (EU) 2016/679. (2016).