

Research on the Criminal Law Regulation Path for Infringement of Virtual Property - Based on the Non Monetary Nature of Virtual Property

Yifei Zhu

ZUEL-SUR School of Law and Economics, Zhongnan University of Economics and Law, Wuhan, Hubei, China

*Correspondence Author

Abstract: *The term 'property' in China's criminal law includes tangible, intangible, and property interests. Virtual property, as a subjective new type of property with dual attributes of property and debt, is neither tangible nor intangible, nor property interests. Therefore, it does not belong to the term 'property' in criminal law and cannot be protected through property crimes. Under current legal norms, the infringement of virtual property should be mainly regulated from the perspective of data crimes. This is a regulatory approach based on traditional criminal law theory for infringement of virtual property, which can better maintain the stability of the current criminal law system; At the same time, it should also be recognized that this type of protection is limited, so we should start to include virtual property in the category of "property" through specialized legislation.*

Keywords: Virtual property, Property, Electromagnetic data, Data crime.

1. Introduction of the Problem

With the development of the network society, the protection of virtual property has become an unavoidable issue in the field of criminal law. However, the current criminal law norms have not yet clearly defined the specific regulatory methods for the theft of virtual property, resulting in a lack of consensus in the judicial practice regarding the handling of this behavior. Looking at the judicial precedents on the identification of theft of virtual property in recent years, there are two main approaches to conviction. One is to treat it as a traditional theft crime. This approach is straightforward, which is to directly regard virtual property as "property" in criminal law and protect it. The other approach to conviction appeared after the promulgation of the Criminal Law Amendment (VII), which added data-related crimes such as the crime of illegally obtaining computer information system data. Subsequently, the Research Office of the Supreme People's Court issued the "Research Opinions on How to Characterize the Illegal Sale of Others' Game Coins Using Computers for Profit" (hereinafter referred to as the "Opinions"). In the "Opinions", the Supreme People's Court believes that the act of illegally selling other people's game coins using computers should currently be convicted and punished as the crime of illegally obtaining computer information system data. Subsequently [1], judicial organs in various regions tend to identify the theft of virtual property as a data crime.

In the field of criminal law, there are currently three main viewpoints regarding the regulation of acts that infringe on virtual property: First, virtual property should be considered property under criminal law, and therefore the illegal acquisition of virtual property should be regulated by property crimes; Second, virtual property does not belong to property under criminal law, and it can only be regulated by data crimes [2]; Third, the nature of virtual property is unclear, but it is undeniable that virtual property establishes legal relationships with external parties through electromagnetic data, so it should be regulated from the perspective of data

crimes, which can also avoid the controversy over the nature of virtual property [3].

As can be seen, the core issue in the theoretical and practical handling of acts infringing upon virtual property lies in whether virtual property falls under the category of "property" in criminal law. If it does, then the regulation of acts infringing upon virtual property should naturally revolve around property crimes. If it does not fall under the category of property, then regulatory paths should be sought from other perspectives. Therefore, this paper will first clarify this core issue before proceeding to research regulatory pathways.

2. Virtual Property does not Fall under the Category of "property" in Criminal Law.

From the current research on virtual property in the field of criminal law theory, most scholars believe that virtual property should be classified as "property". For example, Professor Zhang Mingkai believes that: "Interpreting virtual property as property under criminal law will not infringe on the possibility of national prediction and will not violate the principle of legality in criminal law." [4] Professor Chen Xingliang also gave virtual property the evaluation of "property" from the perspective of the integration of criminal and civil law - "Virtual property is property that has property value and exists in cyberspace in the form of electromagnetic data." [5] From the perspective of the two scholars, they are actually based on the premise that "virtual property has economic value" and believe that virtual property has the characteristics of "property", and carry out specific construction accordingly. This view is quite convincing at first glance, but in fact, if further legal norms are applied, it will face many theoretical obstacles: such as the problem of possession of virtual property and the problem of determining the amount. In this regard, we can only further reconstruct the relevant norms based on hermeneutics, which will have a great impact on traditional criminal law.

A minority view, such as that of Professor Liu Mingxiang,

argues that although virtual property is property under criminal law, the core legal interest it represents is not property rights in property crimes, but rather the right to data security. Therefore, it does not belong to “property” under criminal law [6]. From this perspective, it emphasizes the damage caused to the legal interest of data security by the act of infringing on virtual property, while not denying the property attributes of virtual property. In fact, there are problems with this view: First, the argument that virtual property does not belong to “property” under criminal law by pointing out that the core legal interest infringed by the act of infringing on virtual property is the right to data security lacks persuasiveness; Second, while acknowledging the property attributes of virtual property, it does not explain why virtual property, which clearly possesses property attributes, does not belong to “property” under criminal law, thus exhibiting certain oversights in its argumentation.

From the perspectives of the two schools of thought mentioned above, a consensus is reached that virtual property possesses the attributes of property. In this regard, the author does not disagree. As Professor Zhao Bingzhi stated, virtual property possesses an “indelible property nature” [7], and the author also tends to believe that virtual property possesses the legal nature of property. However, the concept of “property” in property crimes under Chinese criminal law cannot encompass virtual property, a new type of property. In other words, virtual property does not belong to any type of “property” under Chinese criminal law.

The prevailing view is that “property” in China’s criminal law is a broad concept that includes tangible things, intangible things, and property interests: “As for property crimes, in general, property includes all tangible things, intangible things, and property interests that have value and manageability” [8]. The concept of tangible things is relatively simple. Tangible things are also called physical property. As property in the narrowest sense, they usually refer to “things that can be seen and touched and have a certain form [9]. Intangible things, in contrast to tangible things, refer to intangible things that do not have a specific shape but have a certain economic value and manageability. It is widely believed in academia that intangible things are items that do not have an objective tangible entity, such as electricity, gas, and natural gas [10]. It needs to be made particularly clear that both tangible and intangible objects belong to objective matter existing in nature. The only difference is whether they have a legally recognized substance. Therefore, they both belong to objectively existing property. However, the property interests mentioned below are different. They do not belong to objective matter in nature. Therefore, they should belong to conceptual property. Regarding the concept of property interests, China’s criminal law does not give a clear definition. The mainstream theory generally advocates defining property interests by drawing on the concept of Japanese criminal law theory - “Property interests generally refer to property interests other than property in the narrow sense (ordinary) property, including the increase of positive property and the decrease of negative property” [8].

Therefore, if virtual property is to be considered “property” under criminal law, then an applicable framework for virtual property must be found within the scope of “property.” This

leads us to the problem: virtual property is difficult to classify as any type of property; it is neither tangible nor intangible, nor is it a property interest. The issue of tangible property is relatively simple: virtual property lacks a fixed entity and therefore does not belong to tangible property; treating virtual property as tangible property is illogical. The issues of intangible property and property interests require further discussion.

2.1 Virtual Property does not Belong to Intangible Property.

Currently, scholars who hold a positive view on “virtual property belongs to property” mainly construct their arguments between intangible things and property interests, with intangible things occupying the majority. For example, in Professor Chen Xingliang’s view, virtual property is divided into three different types: account -type, item-type, and currency-type. Account-type and item-type virtual property should belong to the category of intangible things [4]. Professors Zhang Mingkai and Zhao Bingzhi did not explicitly state this, but they compared it to electricity and telecommunications information in their relevant articles. Therefore, it can be considered that virtual property belongs to intangible things in their perspective. The author believes that the logic of the above view is actually based on the perspective of electromagnetic data. The specific logical chain is “electromagnetic data belongs to intangible things - virtual property is electromagnetic data - virtual property belongs to intangible things”. The author believes that the fallacy lies in the incorrect confusion between virtual property and electromagnetic data. In fact, virtual property and electromagnetic data are not the same thing. The reasons for this view are as follows:

First, virtual property is subjective and belongs to subjective things, not objective matter, while electromagnetic data is objective matter. From the concept of electromagnetic data: the concept originates from German and Japanese criminal law. Article 7, Paragraph 2 of the Japanese Penal Code stipulates that electromagnetic records refer to records made electronically, magnetically, or otherwise in ways that cannot be perceived by human senses, for the purpose of processing information by electronic computers. Article 202-1, Paragraph 2 of the German Penal Code stipulates that the data mentioned in the preceding paragraph refers only to data stored or transmitted by electronic, magnetic, or other methods that cannot be directly extracted. Based on the above expressions [11], we can see that electromagnetic data is a type of electromagnetic signal made using electronic or magnetic methods, its function being to be recognized by electronic computers. After the electromagnetic data is recognized by the computer, the computer transmits information to humans through visual, auditory, and other sensory means. This information, after being re-recognized by the brain, forms the virtual property we perceive. Therefore, virtual property is a product of our subjective consciousness, unlike electromagnetic data, which is an objective matter.

Second, virtual property is property, while electromagnetic data, due to its infinite replicability, conflicts with the essence of property. Therefore, electromagnetic data can only be data, and no type of electromagnetic data can be evaluated as

property. Theories regarding the essence of property include the labor theory of value, the will to own property, and utilitarianism. However, regardless of the interpretation of the essence of property, it always revolves around the characteristics of value, scarcity, and manageability [12]. Electromagnetic data, theoretically, can be infinitely replicated as long as it exists in a storage medium, and therefore lacks value and scarcity. Thus, if virtual property and electromagnetic data are not distinguished independently, it fundamentally denies the value and scarcity characteristics of virtual property as property. Taking a game company as an example, as the operator of a game, it has the highest authority to modify game data. If electromagnetic data is considered virtual property, then this means that the game company possesses potentially unlimited virtual property (as long as they replicate the data). This conclusion is obviously absurd, because under this logic, every game company's assets would be unlimited.

The "Wang Yihui et al. embezzlement case" in judicial practice embodies the above-mentioned erroneous view: In 2004, the defendant Wang Yihui, taking advantage of his position at Shanda Games, copied virtual property such as weapons and equipment from the company's "Legend of Mir" game, and then sold it to players through various channels, illegally profiting more than 1.22 million yuan. The court of first instance held that Wang Yihui was guilty of embezzlement, on the grounds that the weapons and equipment copied by Wang Yihui were virtual property, and the ownership of these virtual property belonged to Shanda Games. Therefore, Wang Yihui's illegal appropriation of Shanda Games' virtual property by taking advantage of his position constituted embezzlement [13]. According to the logic of this judgment, the 1.22 million yuan illegally obtained by Wang Yihui was in fact the valuation of the copied weapons and equipment owned by Shanda. Based on Shanda's unlimited ability to copy the above weapons and equipment, we would eventually arrive at the absurd conclusion that "Shanda has unlimited assets because it has unlimited weapons and equipment that can be valued."

Therefore, the court's reasoning in the Wang Yihui case was clearly flawed. We need to clarify that virtual property exists subjectively in the mind of the internet user. It is presented to the user on electromagnetic data and engages in legal relationships through this data (similar to the relationship between sound waves and air; sound waves propagate through air and are perceived by humans, but sound waves cannot be perceived without air, yet this doesn't mean sound waves are air). Only when users invest time or money and fulfill the conditions for acquiring virtual property through the operation of the game program will it be carried on electromagnetic data and enter the user's control. In the aforementioned case, the weapons and game equipment illegally copied by Wang Yihui and others were merely a set of data, possessing neither intrinsic value nor scarcity. Only when players paid Wang Yihui money and obtained the data of the aforementioned weapons and equipment did their subjectively valuable and scarce virtual property form on the data of the weapons and equipment.

Therefore, virtual property and electromagnetic data are not the same thing. Electromagnetic data is an intangible thing,

but this does not mean that virtual property is an intangible thing. On the contrary, virtual property is a subjective property, which is fundamentally different from the objective reality of intangible things.

2.2 Virtual Property does not Fall under the Category of Property Interests.

To explain why virtual property does not belong to property interests, we need to start from the rights attributes of property interests. The prevailing view is that the rights attributes of property interests should belong to creditor's rights: "From the perspective of the unity of legal order, all the rights that constitute property interests can be found in the corresponding positions in civil law... Criminal law only needs to take things and debts as objects of protection, and correspond the two to property and property interests respectively, so as to reasonably realize the distinction between property and property interests [14]. The author agrees with the above view. In fact, property interests should be identified as creditor's rights in both theory and practice. According to practical view, the specific identification of property interests in practice can be summarized as "all property interests other than property, in addition to positive interests such as obtaining creditor's rights or security rights, and making others provide labor or services, also include negative interests such as debt relief and deferred payment" [15].

It is worth noting that some argue that the definition of property interests should be broadly interpreted, not limited to claims, but encompassing all legal interests with objective economic value. I disagree with this view. Property interests, as an independent form of "property" in property crimes, inherently possess a strong expansive meaning due to the word "interest." Therefore, a strict, restrictive interpretation is necessary to avoid the misinterpretation in practice of all economically valuable property not explicitly defined in criminal law as property interests. This would essentially transform property interests into a catch-all category, unduly expanding the scope of criminal law and violating the principles of restraint and legality in criminal law. Therefore, virtual property should be strictly defined as a claim.

From the perspective of the property rights of virtual property, this author believes that virtual property belongs to a new type of property that combines the characteristics of both real property and contractual property. Currently, there are three main theories regarding the property rights of virtual property: the real property theory, the contractual property theory, and the theory of new types of property rights. Traditional real property rights and contractual rights cannot directly encompass the property rights attributes of virtual property.

Firstly, some scholars argue that virtual property rights constitute real rights because internet users have the right to directly control virtual property, and under the perspective of the dichotomy of property and obligations, it should be incorporated into real rights [16]. This view is untenable. The author believes that interpreting virtual property as a thing inevitably means breaking through the traditional theory of real rights: traditional theory holds that the object of real rights is limited to things in a narrow sense, namely specific tangible things. Virtual property lacks a physical form and is

difficult to interpret as a traditional object of real rights; at the same time, interpreting virtual property as a thing also requires breaking through the traditional theory of “dominance” of things. The dominance of real rights is manifested in the right holder’s control over the object, which is independent and requires no intervention or assistance from others [17]. However, in the context of virtual property, the right holder’s control over virtual property depends on the continuous service provision of the network operator, which differs significantly from the traditional theory of dominance. Therefore, under the existing theory of real rights, virtual property should not be classified as an object of real rights, and virtual property rights are not real rights.

Secondly, some scholars believe that virtual property rights constitute a claim: “Virtual property is the service provided by network service operators to users, and virtual property rights are the claim between users and network service operators based on legal acts such as contracts [18].” The author also disagrees with this view. The aforementioned view identifies virtual property as a contractual claim between network service operators and users, which in fact only reveals the cause of the creation of virtual property [19]. Furthermore, regarding virtual property as a user’s request for continuous services from network service operators ignores the user’s actual right to control virtual property and identifies it as a “claim of debt,” essentially confusing the object attributes and ownership of virtual property [20]. Therefore, it is also inappropriate to consider virtual property as an object of a claim. The new property rights theory, which combines the attributes of property and obligations, can better summarize virtual property rights: On the one hand, virtual property is generated and depends on the continuous supply of network services by network service operators. Based on this, network users have the right to claim “obligation” from the operator to continue to provide network services according to the network contract. On the other hand, virtual property has the functions of use, income and disposal, and also has a certain property rights characteristics.

Therefore, virtual property is a new type of property that combines the characteristics of both property and debt, and does not fall under the category of debt-related property interests in criminal law. In light of the preceding text, virtual property is neither tangible nor intangible property, nor does it constitute a property interest; therefore, it does not fall under the category of “property” in Chinese criminal law. Under current Chinese criminal law, it is difficult to regulate acts that infringe upon virtual property through property crimes.

3. Application and Regulation of Crimes Regulating Infringement of Virtual Property

As previously stated, virtual property does not fall under the category of “property” in Chinese criminal law. However, it resides on electromagnetic data and uses this data as a medium for establishing legal relationships. Therefore, any infringement of virtual property inevitably involves the acquisition, modification, or deletion of electromagnetic data. Thus, data crime is currently the best approach under Chinese criminal law to regulate infringements of virtual property. It is important to emphasize two points: First, the core legal interest protected by data crime is the right to data security;

therefore, its object of protection is the electromagnetic data itself. Thus, we primarily need to regulate infringements of virtual property from the perspective of data crime, specifically through Article 285-2 of the Criminal Law, which pertains to the crime of illegally obtaining computer system data. Second, as emphasized above, electromagnetic data and virtual property are not the same thing. Therefore, regulating infringements of virtual property through data crime is essentially a secondary form of regulation, providing supplementary protection to virtual property on top of data security. Therefore, in reality, direct protection of virtual property under current Chinese criminal law is virtually nonexistent, and separate legislation to protect virtual property should be considered.

3.1 Regulatory Perspective on the Crime of Illegally Obtaining Computer System Data

Infringement of virtual property inevitably involves computer data. Data crime is currently the best option for regulating acts that infringe on virtual property. In China’s criminal law, data crime specifically refers to the crime of illegally obtaining computer system data, which provides protection for computer data.

Regarding the crime of illegally obtaining computer system data, Article 285-2 of the Criminal Law stipulates: “Whoever violates state regulations by intruding into a computer information system other than those specified in the preceding paragraph or by using other technical means to obtain data stored, processed, or transmitted in such a computer information system... shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention...” From this provision, we first need to extract several basic points: First, the object of this crime is the right to security of computer electromagnetic data; second, the behavioral structure of this crime is complex, requiring intrusion into a computer information system before obtaining the data within it; third, the distinction between this crime and the “crime of illegally intruding into a computer information system” stipulated in Article 285-1 lies in the fact that this crime involves intruding into computers in fields other than state affairs, national defense construction, and cutting-edge science and technology.

A crucial aspect requiring in-depth discussion is the behavioral structure: this crime is a complex offense, so how should “illegally obtaining” in the crime’s name be interpreted? Theoretically, there are two main approaches: one is that “illegally obtaining” refers solely to “illegally intruding” and acquiring data. This approach focuses on the intrusion itself, arguing that the act of intrusion inherently carries the connotation of “illegality.” As long as it involves intruding into another person’s computer system, the illegality requirement of this crime is met, and the acquisition itself does not need further discussion. The second approach argues that the act of intrusion alone is insufficient to demonstrate the illegality of this crime; the act of acquiring data must also be illegal for “illegally obtaining” to be accurately defined. The author leans towards the second approach, where the act of intrusion alone is insufficient to demonstrate the illegality of this crime. It is worth noting that this has not been discussed in depth in judicial practice. Taking the case of “Wei Menglong,

Gong Xu, and Xue Dongdong's crime of illegally obtaining computer system data" as an example, this case was released as a guiding case by the Supreme People's Procuratorate. The Supreme People's Procuratorate stated in the key points: "Using an account and password to log in to a computer information system beyond the scope of authorization constitutes an act of intruding into a computer information system; downloading the data stored in a computer information system after intruding into it can be identified as illegally obtaining computer information system data [21]". From this guiding opinion, the Supreme People's Procuratorate actually tends to believe that as long as one illegally intrudes into another's system, obtaining system data based on this constitutes this crime, without needing to discuss whether the acquisition behavior is legal. This line of thinking is actually problematic: if the perpetrator illegally intrudes into the victim's computer system with the intention of obtaining data that the victim has already made public and that is available to users at will, according to the Supreme People's Procuratorate's approach, the perpetrator has obtained the data because of the illegal intrusion, so it is directly identified as the crime of illegally obtaining computer system data; but in fact, in this case, the perpetrator did not infringe on the victim's legal interest in data security, because this data itself is fully public and available to users at will. Therefore, the author believes that the objective behavioral structure of the crime of illegally obtaining computer system data should be based on the second line of reasoning mentioned above. On the one hand, the perpetrator enters another person's computer system for illegal reasons, and on the other hand, the perpetrator obtains another person's computer data for illegal reasons due to the aforementioned intrusion.

Having clarified the understanding of the behavioral structure, let's further define the specific acts of infringing on virtual property. In practice, acts of infringing on virtual property commonly manifest as "account theft," "Trojan viruses," and "phishing websites." Theoretically, it can be manifested as stealing virtual property, such as using account-stealing software to access someone else's online game account and transfer the virtual property within, or it can be manifested as defrauding virtual property, such as obtaining virtual property from the victim through deception. The author believes that not all acts of infringing on virtual property can be classified as the crime of illegally obtaining computer system data. Taking the case of "Meng Chenlin and Liu Zhu's crime of illegally obtaining computer information system data (hereinafter referred to as the Meng Chenlin case)" as an example, in this case, the defendants Meng Chenlin and Liu Zhu created the "btceth escrow transaction group" WeChat group, recruiting members under the pretext of providing transaction guarantees for Ethereum virtual currency (hereinafter referred to as Ether). In December 2017, the victim, Zhu, posted a message in a group chat about selling Ethereum. Liu Zhu and Meng Chenlin conspired to buy 50 Ethereum from Zhu at a price of 5,000 yuan each. After Zhu transferred the Ethereum to the designated account, Liu and Meng failed to deliver the agreed price to Zhu and kicked Zhu out of the group chat. Both the first and second instance courts held that Liu and Meng constituted the crime of illegally obtaining computer system data in this case [22]. This view has a problem: In this case, although the perpetrators Liu and

Meng infringed on Zhu's virtual property, they did so by deceiving Zhu into disposing of his virtual property on his own. They did not intrude into anyone else's computer system, nor did they obtain computer system data based on intrusion. Therefore, Liu and Meng's act of infringing on virtual property in this case does not actually meet the objective behavioral structure of the crime of illegally obtaining computer system data.

Therefore, when determining whether an act of infringing on virtual property constitutes the crime of illegally obtaining computer system data, the objective behavioral structure of "illegally intruding into a computer system - illegally obtaining system data" should be strictly followed. If the perpetrator does not intrude into another person's computer system to obtain virtual property data, or if the perpetrator enters the computer system for a legitimate reason (such as the victim lending their account to the perpetrator) and obtains virtual property data, it is not appropriate to determine it as the crime of illegally obtaining computer system data.

3.2 Regulatory Perspective on Crimes of Infringing on Citizens' Personal Information

From a practical perspective, virtual property mainly includes game account levels, virtual currency, virtual equipment, virtual plants and animals, virtual ID accounts, and game character attributes, etc. [23]. According to general theory, these virtual properties are generally divided into two categories: account-type virtual property and item-type virtual property [5]. It should be affirmed that some account-type virtual property has a strong personal information character, so acts that infringe on this part of account-type virtual property may also involve the crime of infringing on citizens' personal information.

Virtual property related to accounts mainly refers to network service accounts, which are accounts set up by network service providers to distinguish service recipients in network services. These accounts are held by users after they register and agree to their network service contracts, or acquired through transfer [24]. Examples include various online game accounts and QQ accounts. Currently, most network service accounts generally require users to provide their real name, date of birth, ID number, mobile phone number, and other personal information during the registration process. Therefore, if a user's account is illegally obtained by others, their personal information rights are often infringed. Thus, the crime of infringing on citizens' personal information should be included in the regulatory framework for infringing on virtual property related to accounts.

the specific legal provisions of Article 253-1 of China's Criminal Law regarding the crime of infringing on citizens' personal information, the objective behavioral structure of this crime manifests in two ways: first, selling or providing citizens' personal information to others; second, illegally obtaining citizens' personal information by means of theft or other illegal methods. It is worth noting the understanding of "illegally obtaining". The author believes that the illegal acquisition of citizens' personal information here should be equivalent to the aforementioned "theft", including but not limited to illegal acts explicitly stipulated by law such as fraud,

inducement, coercion, robbery, and intimidation. Obtaining personal information by illegally intruding into other people's computer systems is of course also within the scope of "illegally obtaining". Therefore, if the perpetrator infringes on citizens' virtual property such as account, it may also constitute the crime of infringing on citizens' personal information. Regarding the specific standards for identification [25], the author believes that:

First, it should be clarified what constitutes "personal information" as an object of this crime. In practice, not all account-type virtual assets contain personal information; furthermore, not all accounts containing personal information have that information readily accessible. For example, while some accounts may require users to provide names, ID numbers, and other personal information during registration, this is merely for record-keeping purposes, and the personal information is not readily available for viewing. Therefore, it should be clear that only account-type virtual assets that explicitly contain various types of personal information and whose personal information can be viewed during the user's use of online services can be considered as objects of this crime.

Second, it is necessary to clarify the determination of the objective acts in the crime of infringing on citizens' personal information. As mentioned earlier, the acts of infringing on citizens' personal information mainly include the sale, provision, and illegal acquisition of citizens' personal information. From the perspective of virtual property such as accounts, this should be identified as the illegal provision or sale of online accounts containing personal information, and the illegal acquisition of online accounts containing personal information. For example, the act of obtaining another person's online account containing personal information through Trojan virus software, phishing websites, etc., should simultaneously meet the objective act elements of the crime of illegally obtaining computer system data and the crime of infringing on citizens' personal information. On the other hand, the act of purchasing another person's online account containing personal information and then reselling it separately meets the objective act elements of the crime of infringing on citizens' personal information. The difficulty here lies in whether the act of buying accounts containing personal information should be evaluated as the crime of infringing on citizens' personal information. The author holds a negative view on this. As mentioned earlier, the illegal acquisition of citizens' information is equivalent to the act of "stealing," while the illegality of the act of "buying" is significantly weaker than that of illegal acts such as "stealing." "Judicial precedents also support this view: In the case of "Zhong Chaochao infringing on citizens' personal information," Zhong Chaochao purchased a large number of QQ accounts and passwords from his superior for illegal profit, and then sold them to his subordinate Zhao Jun. Zhao Jun then used the account passwords to log in to the online games under the account name to illegally obtain virtual property such as game equipment and game currency. In the court's judgment, Zhao Jun's behavior was only identified as the crime of illegally obtaining computer system data, and his act of buying online accounts was not identified as the crime of infringing on citizens' personal information [26].

In addition, some scholars believe that there is no room for the application of the crime of infringing on citizens' personal information for the infringement of virtual property. The reason is that the object of this crime, the online account, does not have the property attribute, so it does not belong to virtual property, but is merely personal information [27]. I disagree with this view and believe that online accounts should be affirmed as virtual property: At present, most online accounts can be sold and transferred. Taking various game accounts as an example, if you search for the keyword "game account" on various online shopping platforms, various finished game accounts will appear on the product page. It can be determined that the relevant market transaction system of online accounts is the same as other virtual property, and is no different from ordinary commodities. Therefore, it is illogical to deny its virtual property nature.

In conclusion, the regulation of acts that infringe upon virtual property such as accounts can also be approached from the perspective of the crime of infringing upon citizens' personal information.

3.3 Direction of Legal Amendment - Including Virtual Property in the Scope of "Property"

Currently, the mainstream view in academic circles tends to protect acts that infringe upon virtual property from the perspective of property crimes, and explores its rationale from an interpretative perspective. In fact, as mentioned earlier, virtual property is a new type of property, so protecting it from the perspective of property crimes is the most scientific and reasonable approach, and can more comprehensively protect the legal interests behind it. However, under the current criminal law norms, the interpretative approach commonly used in academic circles—interpreting virtual property as "property" and modifying the relevant elements of its constitution—is ineffective and would significantly impact traditional criminal law theory. While adhering to the current regulatory model focused on data crimes, I believe we should consider incorporating virtual property into the category of "property" in criminal law through specific legislation, making it a special legal fiction. The feasibility of this approach lies in:

First, this approach will not undermine the stability of criminal law. By enacting special legislation to classify virtual property as "property" in criminal law, it will not shake the original traditional property theory, nor will it require special modifications to the relevant elements of the crime, such as the issue of possession of virtual property. It can better regulate acts that infringe on virtual property based on the traditional criminal law itself.

Second, this approach can truly provide criminal law protection for virtual property. Currently, protecting virtual property through data crimes and personal information crimes is a lateral protection based on the theories that "infringement of virtual property inevitably involves modification of electromagnetic data" and "some virtual property possesses personal information characteristics." It regulates acts that infringe on data security rights and personal information rights, not acts that infringe on property rights. It should be

clear that virtual property, as a type of virtual property with both property and debt attributes, inherently possesses property characteristics. Therefore, including virtual property under the category of “property” through legislation is a natural consequence of the inherent nature of virtual property itself.

Third, this approach better reflects the principle of proportionality between crime and punishment. The current model of regulating infringements on virtual property, primarily based on data crimes, is insufficient to comprehensively protect virtual property. For example, in the aforementioned “Meng Chenlin case,” if the perpetrator did not intrude into a computer system but instead used fraud to induce the victim to voluntarily dispose of virtual property, this cannot be regulated as a data crime. Furthermore, the Ethereum obtained through fraud in this case did not possess personal information characteristics, making it difficult to punish Meng Chenlin under current criminal law. In fact, this type of fraudulent infringement and the illegal acquisition of virtual property through direct computer intrusion are equivalent in their infringement on virtual property; both infringe upon virtual property and, from the perspective of the principle of proportionality between crime and punishment, should be punished. The essence of this issue lies in the legal interests protected by data crimes. Fraudulent infringements of virtual property do not infringe upon data security; only the virtual property rights are damaged. The protection of virtual property rights requires specific legislative avenues.

Fourth, judging from the current state of legislation both domestically and internationally, it is not uncommon for the legal status of a particular object to be confirmed through specific legislation. For example, Japanese criminal law has a similar approach: the standards for identifying “property” in Japanese criminal law are relatively strict, referring only to objectively existing tangible objects; intangible objects, property interests, etc., are not within the scope of “property”. However, Article 245 of the Japanese Criminal Code stipulates that “television is considered property in this chapter [28], that is, electricity, as an intangible object, is regarded as “property” in theft by the Japanese Criminal Code through special legal provisions; there is also a precedent for similar provisions in China’s Criminal Law, for example, Article 265 stipulates: “Whoever, for the purpose of profit, steals another person’s communication line, copies another person’s telecommunication number, or knowingly uses telecommunication equipment or facilities that have been stolen or copied, shall be convicted and punished in accordance with the provisions of Article 264 of this Law.” The legislative logic of this article is to directly clarify from a legislative perspective that the act of stealing telecommunication fees by stealing communication circuits and copying telecommunication numbers falls within the scope of property crimes. Although some scholars believe that the content of this article is not a legal fiction, but a notice [2], its function is to clarify the act of stealing another person’s long-distance account, which has been controversial in judicial practice for a long time [29]. But even if it is considered to be a notice, it cannot be denied that the Criminal Law has indeed established the form of criminal protection for telecommunication fees through special legislation. Given the current disputes over the ownership of virtual property, the

legislative community could take a similar approach and include virtual property separately in the category of “property” through special legislation. This would not only resolve the disputes in theory and practice but also demonstrate the restraint of criminal law.

4. Conclusion

Taking all the information into account, we should be clear that, given the non-property nature of virtual property, it is appropriate to regulate it from the perspective of data crime and personal information crime at present.

In fact, regulating the infringement of virtual property from a criminal law perspective is currently facing a dilemma: interpreting virtual property as real property faces challenges from traditional criminal law theory and requires further theoretical development; regulating it from the perspective of data crimes and personal information crimes is not perfect either, and its deterrent effect needs to be further strengthened. Therefore, from the perspective of legal sociology, incorporating online virtual property into separate criminal law provisions is the only way to achieve criminal protection of virtual property in both theory and practice.

Admittedly, legislation requires the right timing. For the structure of virtual property, a new type of property still in constant flux, we need to wait patiently for its development. I believe that with the continuous development of internet information technology, virtual property will inevitably be incorporated into legal regulations.

References

- [1] Yu Haisong. Research Opinions of the Research Office of the Supreme People’s Court on How to Characterize the Illegal Sale of Others’ Game Currency for Profit Using Computers [J]. *Judicial Research and Guidance*, 2012(2): 128.
- [2] Liu Xianquan. Criminal Law Analysis on the Characterization of Illegal Acquisition of Virtual Property in Metaverse Space [J]. *Oriental Law*, 2012(2): 48-51.
- [3] Chen Yunliang, Zhou Xin. Choice of Criminal Law Protection Path for Virtual Property [J]. *Law Review*, 2009(2): 147.
- [4] Zhang Mingkai: “The Illegal Acquisition of Virtual Property.”
- [5] Chen Xingliang. The Criminal Law Attributes of Virtual Property and Its Protection Path [J]. *Chinese Jurisprudence*, 2017(2): 146-168.
- [6] Liu Mingxiang. A Study on the Characterization of Stealing Online Virtual Property [J]. *Jurisprudence*, 2016(1): 151-153.
- [7] Zhao Bingzhi, Yin Jianfeng. A Study on the Criminal Law Regulation of Infringement of Virtual Property [J]. *Legal Science*, 2008(4): 153.
- [8] Zhang Mingkai. *Criminal Law* [M]. Legal Publishing House, 2021. Page 750.
- [9] Chen Xingliang. *Detailed Explanation of Specific Criminal Law* [M]. People’s Court Press, 2016. Page 261.

- [10] Zhang Mingkai. Research on Fraud and Financial Fraud [M]. Tsinghua University Press, 2006. Page 14.
- [11] Xu Jiusheng (trans.). German Criminal Code [M]. Peking University Press, 2019. Page 148.
- [12] Jia Zhangfan. The Legal Nature of Online Virtual Property and Its Dispute Resolution Mechanism [J]. Shanghai Legal Studies, 2021(11): 123.
- [13] Wang Yihui et al. Copyright Infringement Case: (2007) Shanghai No. 1 Intermediate People's Court Criminal Final Judgment No. 285 [EB/OL]. (2007-06-14) [2026-04-19].
- [14] Li Hong, Chen Shaoqing. On property interests in property crimes[J]. Jiaotong University Law Journal, 2022(5):30.
- [15] [Japan] Nishida Noriyuki. Japanese Criminal Law Specific Theories[M]. Translated by Liu Mingxiang and Huang Zhaowu. Wuhan University Press, 2005. Page 173.
- [16] Lin Xuxia. On the nature of virtual property rights[J]. Chinese Jurisprudence, 2009(1):90.
- [17] Wang Lei. Adherence to the theory of online virtual property claims-and on the systematic status of virtual property in the Civil Code[J]. Hanjiang Forum, 2017(1):123.
- [18] Chen Su. Commentary on the General Principles of Civil Law[M]. Legal Publishing House, 2017. Page 886.
- [19] Xie Xiao. The property and debt interest attributes of online virtual property and the construction of its protection rules [J]. Nanjing Social Sciences, 2022(9): 90.
- [20] Wang Zhu. The dichotomy of virtual property and its legal rules under the perspective of the Property Law [J]. Journal of Fujian Normal University, 2008(5): 33.
- [21] Gazette of the Supreme People's Procuratorate, 2017, No. 6.
- [22] Second Instance Criminal Ruling on the Crime of Illegally Obtaining Computer Information System Data and Illegally Controlling Computer Information System by Meng Chenlin and Liu Zhu: (2019) Zhe03 Criminal Final No. 1117 [G]. Wenzhou: Intermediate People's Court of Wenzhou City, Zhejiang Province, 2019.
- [23] Yu Jing v. Sun Jiangtai Virtual Property Sales Contract Dispute Case: (2009) Erzhong Minzhong No. 18750 [G]. Beijing: China Renmin University Press, 2011.
- [24] Jiang Bo, Zhang Jinping. Difficulties in the Judicial Trial of Virtual Property Transaction Disputes - A Perspective from Online Game Equipment Transaction Disputes [J]. Network Law Review, 2011(2): 5-8.
- [25] Wang Zhaowu. Several Issues in the Identification of Crimes Infringing on Citizens' Personal Information [J]. Jurisprudence, 2009(12): 147.
- [26] (2019) Xiang 0405 Criminal First Instance No. 104 Criminal Judgment.
- [27] Zhang Yiran. The Conceptual Restriction of "Virtual Property" and the Reconstruction of Criminal Law Path Protection - A Reference to the Tripartite Rights System of Data [J]. Journal of Nanjing University of Science and Technology, 2021(2): 109.
- [28] "Meiji 40th Year Law No. 45, Criminal Code", https://elaws.e-gov.go.jp/document?lawid=140AC000000045_20220707_504AC0000000067&keyword=刑法
- [29] September 14, 1991, Supreme People's Court Research Office's "Reply Regarding the Issue of How to Characterize Cases of Misappropriation of Others' Long-Distance Telephone Accounts".