

非法获取网络虚拟财产的刑法定性分析

石诗雨

贵州财经大学法学院 贵州贵阳 550000

摘要: 随着互联网技术的普及和发展,衍生出以网络虚拟财产为窃取对象的新型犯罪。非法获取网络虚拟财产在司法实践中存在“同案不同判”的现象,主要处以盗窃罪等财产类犯罪和非法获取计算机信息系统数据罪等信息数据类犯罪。基于法律的滞后性,相关罪名在处理类似案件时均有不同程度的困境。基于大数据时代下数据安全的重要性,应当以非法获取计算机信息系统数据罪进行规制。

关键词: 虚拟财产;盗窃罪;非法获取计算机信息系统数据罪;破坏计算机信息系统罪

1. 提出问题

近年来,随着互联网技术的普及,网络游戏迅速发展,成为互联网应用的重要分支。据《2022年1-6月中国游戏产业报告》显示,2022年上半年中国游戏市场收入达1477.89亿元,用户规模约6.66亿,已成为一个庞大的市场。

然而,互联网技术的发展也为新型犯罪提供了空间。游戏玩家常因误操作、运营商保护不力或技术缺陷等原因,导致账号及虚拟物品被非法获取,财产权益受损。

目前在司法领域中,对非法获取网络虚拟财产的行为,主要以两类罪名进行规制,即盗窃罪等财产类犯罪和非法获取计算机信息系统数据罪等信息数据类犯罪。如王某鑫、王某国利用外挂软件修改游戏充值的参数,获取大量游戏内虚拟货币,被判处盗窃罪;而肖某利用之前管理维护公司计算机时获取的CD-KEY指令,获取大量游戏内虚拟货币,则被判处非法获取计算机信息系统数据罪。

“同案不同判”现象的出现,源于理论与实务界对虚拟财产刑法定性的分歧。本文拟从相关罪名及司法解释出发,探讨网络虚拟财产的刑法保护路径,以实现实质正义,并符合罪刑法定与罪责刑相适应的原则。

2. 相关罪名的立法规定及司法适用困局

2.1 盗窃罪的立法规定及其司法适用困局

2.1.1 盗窃罪的立法规定

根据《中华人民共和国刑法》(后文称“《刑法》”)的规定,盗窃罪是指行为人以非法占有为目的,秘密窃取公私财物,将他人占有的财物转移为自己或者第三者(包括单位)占有的行为。从盗窃罪的构成要件来看,客观方面要求

行为人具有秘密窃取数额较大的公私财物或者多次秘密窃取公私财物的行为。所谓秘密窃取,是指行为人采取自认为不为财物的所有者、保管者或者经手者发觉的方法,暗中将财物取走的行为;主观方面要求行为人以非法占有他人财物为目的,也即行为人明确地意识到其盗窃行为的对象是他人所有或占有的财物;侵犯的客体是公私财物的所有权。

同时,考虑到司法实践的需要,最高人民法院与最高人民检察院联合发布相关司法解释,对办理盗窃刑事案件适用法律的若干问题进行了详细的规定。

2.1.2 盗窃罪的司法适用困局

随着时代的发展和变化,盗窃罪所指向的对象也逐渐多样化。根据罪刑法定原则,盗窃罪的对象应根据《刑法》第92条的规定进行认定。值得注意的是,司法实践对于规定中社会公认的财物认定上,并无太多争议。但就其中的兜底性条款“其他财产”如何认定,已然成为司法实践中的难点之一。有的观点认为,基于罪刑法定原则,应当以立法或者司法解释的形式进行规定,如盗窃电信资费、电力、天然气等相关犯罪,均已出台相关司法解释予以规定。^[1]但有的观点认为,基于保护法益的角度,应当对“其他财产”进行扩大解释,只要具备效用性、价值性、稀缺性、可支配性四种特征的,就可以被认定为刑法上的“财物”。^[2]由此得出,因为网络虚拟财产被游戏用户所支配并可以在现实中进行交易,所以其具备效用性、价值性、稀缺性、可支配性四种特征,进而可以被评价为刑法上的“财物”。

2.2 非法获取计算机信息系统数据罪的立法规定及其司法适用困局

2.2.1 非法获取计算机信息系统数据罪的立法规定

本罪规定于2009年2月28日颁布实施的《刑法修正案(七)》,制定本罪的目的在于惩治网络犯罪。根据《刑法》的规定,非法获取计算机信息系统数据罪是指违反国家规定,侵入或者采用其他手段,非法获取国家事务、国防建设、尖端科学技术领域以外的计算机信息系统中存储、处理或者传输的数据的行为。从构成要件来看,客观方面要求行为人非法获取的是国家事务、国防建设、尖端科学技术领域以外的计算机信息系统中的数据;主观方面则要求行为人明知是侵入计算机信息系统或以其他技术手段获取数据的行为,仍故意为之;侵犯的客体则是计算机信息系统的安全。

2.2.2 非法获取计算机信息系统数据罪的司法适用困局

虽然有的观点认为,我国《刑法》增设本罪的目的,正是为了解决在处理以网络虚拟财产为盗窃对象的犯罪中存在的争议问题。^[3]但在实践中,仍然存在适用的难题。有的观点认为,盗窃账号密码后登录并转移网络虚拟财产的行为不应以本罪论处,因为“非法侵入”要求行为人需以技术手段进入计算机信息系统,且“获取数据”仅限于对数据进行复制,转移网络虚拟财产属于改变数据的形态,应以破坏计算机信息系统罪论处;即使以技术手段进入计算机信息系统,转移网络虚拟财产的行为构成牵连犯,也应适用刑罚较重的破坏计算机信息系统罪。^[4]反对该观点的则称,“非法侵入以及利用其他技术手段获取计算机信息数据”的非法性体现在获取了不应当属于行为人自身的数据。也有学者从数据分层这一特殊现象出发,认为应该在此基础上,分析具体的侵害网络虚拟财产的行为在物理层、符号层、信息内容层三个不同维度上进行分析,才能作出更好的判断。^[5]

2.3 破坏计算机信息系统罪的立法规定及其司法适用困局

2.3.1 破坏计算机信息系统罪的立法规定

破坏计算机信息系统罪被规定在《刑法》的第286条,其目的是全方位地保护计算机信息系统及其中数据的安全。从犯罪构成上看,客观方面表现为破坏计算机信息系统和信息系统中存储、处理、传输的数据和应用程序,后果严重的行为。其中前两款均要求行为人违反《网络安全法》等前置法的规定。客体即是计算机信息系统的安全。主观方面要求

行为人明知自己的行为会破坏计算机信息系统的安全运行而希望或是放任这种结果的发生。

同样,考虑到司法实践的需要,“两高”出台了《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(后文称“《解释》”),对条文中“后果严重”和“后果特别严重”的情形、认定计算机病毒等破坏性程序的标准、“计算机信息系统”的文义内涵等多个方面进行了说明和规定。

2.3.2 破坏计算机信息系统罪的司法适用困局

虽然“两高”出台了《解释》,但破坏计算机信息系统罪的适用仍然存在模糊不清的问题。如《刑法》第286条中的第1、3款均规定了行为人的行为需导致计算机信息系统不能正常运行,但第2款中却没有类似的规定。因此,对于实践中如何处理第2款的规定,学者就分为两种观点。一部分学者认为应当采取体系解释,既然第1、3款已经规定需导致计算机信息系统不能正常运行,则第2款应当含有同样的意思表述。^[6]另一部分学者则认为应当采取罪刑法定原则,既然第2款并未有相应的规定,则该行为不要求导致计算机信息系统不能正常运行,且基于第2款的构成要件,应当增设破坏计算机数据罪。^[3]

2.4 小结

至此,笔者对非法获取网络虚拟财产可能涉及罪名的立法规定以及司法适用困局进行了梳理,对该行为的定罪有了进一步的认识。大多数学者持有的观点是该行为应当认定为盗窃罪,认为该行为是行为人通过计算机技术,在游戏用户未察觉的情形下,获取了在刑法上可以被定义为“财物”的网络虚拟财产,符合盗窃罪客观方面中非法性和隐秘性的特征。少部分学者认为应该从网络虚拟财产的本质,即以代码为载体的计算机信息系统中的数据出发,处以相应的信息类犯罪。

3. 相关罪名的法理分析

3.1 不构成盗窃罪

盗窃罪的成立需行为人窃取他人占有的财物,而游戏用户对网络虚拟财产仅享有使用权,所有权归游戏公司所有。因此,非法获取行为并未侵犯用户的“占有”,且虚拟财产始终处于游戏公司控制下。^[7]因此,在客观方面不成立盗窃罪。

其次,盗窃罪的行为对象是公私财物,因此,网络虚拟财产能否被评价为刑法意义上的财物是评价该行为的关键。

张明楷教授认为,作为财产犯罪对象的财物,必须具有三个特征,即管理可能性、转移可能性、价值性。^[8]基于网络游戏公司对网络虚拟财产的所有权,应当认定具有管理性。而基于网络游戏公司对网络虚拟财产的定价以及玩家之间相互交易的价格,应当认定具有价值型。但就转移可能性而言,如上文所述,非法获取行为无法使其脱离网络游戏公司的控制,因而不能满足。由此可得,网络虚拟财产不应该认定为刑法上的财物。

最后,即便将网络虚拟财产视为刑法上的财物,鉴于《刑法修正案(七)》已设立非法获取计算机信息系统数据罪,应视其为盗窃罪的特殊规定,按法条竞合规则适用特殊法条。^[9]

3.2 不构成破坏计算机信息系统罪

高铭暄教授在书中对本罪的介绍是:“此罪旨在加强对计算机信息系统的管理和保护,保障计算机信息系统功能的正常发挥,维护计算机信息系统的安全运行。”本罪的立法目的在于维护计算机信息系统的正常运行。尽管第2款未明确列举,但应通过体系解释认为其包含“导致系统无法正常运行”的情形。非法获取网络虚拟财产的行为虽涉及数据修改,但未对网络游戏的正常运行造成实质性影响,也未引发系统崩溃或损坏。因此,该行为不符合本罪的客观要件,不宜以本罪定罪量刑。

3.3 构成非法获取计算机信息系统数据罪

3.3.1 符合非法获取计算机信息系统数据罪的客体

网络虚拟财产本质上是计算机信息系统中的数据,其财产性仅为外在表现。这些数据以代码形式存储于游戏公司服务器中,用户需通过账号密码登录才能使用。无论是通过窃取账号密码还是突破服务器防火墙获取数据,行为人均侵犯了游戏系统的内部安全。由于网络游戏依托互联网运行,系统安全受损必然影响整个互联网空间,符合本罪作为扰乱公共秩序罪的立法背景。

此外,非法获取网络虚拟财产常伴随获取用户账号密码的行为。在计算机犯罪中,“撞库”是一种利用已泄露账号密码批量登录其他网站以牟利的手段。由此可见,该行为侵害了计算机信息系统安全及公共秩序,符合本罪的客体要件。

3.3.2 符合非法获取计算机信息系统数据罪的客观方面

本罪客观方面在司法适用中存在争议,尤其是对“侵入”和“采用其他技术手段”是否需具备技术性争论激烈。

然而,笔者认为盗窃账号密码后登录游戏转移虚拟财产的行为应纳入本罪范畴。根据司法解释,“身份认证信息”包括账号、口令、密码等用于确认用户权限的数据,明确将其纳入本罪保护范围。因此,无论是通过软件、病毒等技术手段,还是通过账号密码登录非法获取网络虚拟财产,均符合本罪的客观要件。

对于“获取”的理解,有学者认为仅限于复制或转移数据,但这一观点过于表面且与计算机技术不符。从文义解释看,“获取”可理解为暂时取得对数据的控制。^[10]因此,非法获取网络虚拟财产虽未脱离游戏公司服务器,但行为人通过账号密码或其他技术手段暂时控制了虚拟财产(如将其转移至自己的游戏账号),将其解释为“获取”是合理的。

3.3.3 符合非法获取计算机信息系统数据罪的主体和主观方面

《刑法》中,对该罪犯罪主体的规定较为明确,即包括自然人和单位。对此,在司法实践中甚少争议,因此笔者在此不再赘述。而在主观方面,即使行为人主观上是以网络虚拟财产的财产性外表作为行为对象,但不妨碍行为人基于常识认识到网络虚拟财产的数据本质。因此符合行为人明知是侵入计算机信息系统或以其他技术手段获取数据的行为,仍故意为之的要求。

4. 结语

随着互联网技术不断深入生活中的方方面面,计算机信息系统中的数据已经脱离了传统的观念,即维持计算机信息系统正常运行的介质,而披上了财产性的外观。仅仅考虑将非法获取网络虚拟财产的行为定义为盗窃罪,保护私人财产利益,既不符合立法者的目的,也不符合时代背景。当下正处于大数据时代,数据的财产性利益只是其中的一部分,真正重要的是数据背后的各种信息。因此,希望通过笔者的浅显之见,可以对司法实践如何保护数据安全提供帮助。

参考文献:

- [1] 徐彰. 盗窃网络虚拟财产不构成盗窃罪的刑民思考[J]. 法学论坛, 2016, 31(02): 152-160.
- [2] 于志刚. 《虚拟空间中的刑法理论》[M]. 中国方正出版社, 2003年版
- [3] 喻海松. 《网络犯罪二十讲》[M]. 法律出版社, 2018年版
- [4] 欧阳本祺. 论虚拟财产的刑法保护[J]. 政治与法

律,2019,(09):39-54.

[5] 朱宣焯. 数据分层与侵犯网络虚拟财产犯罪研究 [J]. 法学杂志,2020,41(06):121-130.

[6] 王华伟. 破坏计算机信息系统罪的教义学反思与重构 [J]. 东南大学学报(哲学社会科学版),2021,23(06):93-104+147.

[7] 张凯. 虚拟财产刑事保护新论——以规范视角和主体性理论的展开 [J]. 刑法论丛,2016,45(01):306-330.

[8] 张明楷. 非法获取虚拟财产的行为性质 [J]. 中国检察官,2015,(11):78.

[9] 梁根林. 虚拟财产的刑法保护——以首例盗卖QQ号案的刑法适用为视角 [J]. 人民检察,2014,(01):6-13.

[10] 李遐桢, 侯春平. 论非法获取计算机信息系统数据罪的认定——以法解释学为视角 [J]. 河北法学,2014,32(05):65-71.