Dispute Settlement 争议解决, 2024, 10(2), 929-935
Published Online February 2024 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2024.102126

Hans汉斯

论数据犯罪的限缩和分流
——从数据安全法益的角度切入

余嘉琪，董星宏

上海政法学院，刑事司法学院，上海

收稿日期：2024年1月7日；录用日期：2024年2月2日；发布日期：2024年2月21日

摘　要

针对司法实践中数据犯罪逐步沦为新“口袋罪”的乱象，通过对标前置法《数据安全法》中数据安全的定义，明确刑法数据犯罪所保护的法益内涵，确认数据安全法益的独立地位。并将数据剥离为表里层分别讨论，挖掘数据承载的实质法益。通过法益对犯罪构成的规制机能，厘清狭义数据犯罪同传统犯罪数据化之间的界限，将以数据为行为对象，实际上侵犯其他法益的行为分流于财产类、信息类等传统犯罪的规制当中，从而实现对数据犯罪入罪的限缩及分流，避免数据犯罪落入口袋罪的窠臼。

关键词

法益，数据犯罪，数据安全，分流规制

On the Limitation and Diversion of Data Crime
—From the Angle of Legal Interest of Data Security

Jiaqi Yu, Xinghong Dong

School of Criminal Justice, Shanghai University of Political Science and Law, Shanghai

Received: Jan. 7th, 2024; accepted: Feb. 2nd, 2024; published: Feb. 21st, 2024

Abstract

In view of the chaos of data crime gradually becoming a new “pocket crime” in judicial practice, through the definition of data security in the pre-standard law “Data Security Law”, the connotation of legal interest protected by data crime in criminal law is clarified, and the independent status of legal interest of data security is confirmed. And the data is separated into the surface and

文章引用: 余嘉琪, 董星宏. 论数据犯罪的限缩和分流[J]. 争议解决, 2024, 10(2): 929-935.
DOI: 10.12677/ds.2024.102126

inside layers to discuss separately, mining the real legal interests of data bearing. Through the regulatory function of legal interests on crime composition, the boundary between narrow data crime and traditional crime datafication is clarified, and the behavior that is ostensibly targeted at data but actually infringes on other legal interests is diverted into the regulation of traditional crimes such as property and information, so as to achieve the limitation and diversion regulation of data crime and avoid data crime falling into the pattern of pocket crime.

Keywords

Legal Interest, Data Crime, Data Security, Diversion Regulation

1. 引言

随着信息网络技术飞速发展，数据已经涉及人们生活的方方面面，我们在网络空间中进行交易、交流、阅览等活动均会在元宇宙中留下某种形式的痕迹，这些痕迹就是电子数据。电子数据频繁地记录着人们的一举一动，仅凭数据的汇总和分析就可以描摹出一个人的大致形象、一个组织的日常工作，大数据本身便具有极高的价值，占有数据者极可能先占高额经济利益，数据窃取、泄露、买卖等引发的刑事犯罪屡见不鲜，数据犯罪率显著飙升。数据安全问题愈发受到重视，已被纳入国家总体安全战略体系当中考量；2021 年 6 月 10 日人大常委会审议通过《数据安全法》，出台专项法律规范数据处理行为、保障数据安全；数据安全可以也应当成为独立的法益由刑法加以二次保障。

在大数据时代中，人们的财产、隐私、信息都逐渐倾向于电子化的存在形式，针对财产权、人格权等传统法益的犯罪行为模式发生翻天覆地的变化，窃取游戏装备、窃取账户密码等新型犯罪行为常发常见。传统犯罪与数据犯罪的行为模式产生交集，侵害范围存在交叉，其定性在司法实践中众说纷纭且各自为政。统观我国刑法分则规定的犯罪体系，只有非法获取计算机信息系统罪、非法控制计算机信息系统罪是规制数据犯罪的主要罪名；而司法实践常将侵犯承载财产利益和个人可识别信息的数据的犯罪不加区分、笼统置地于这两个罪名的规制中，忽略了数据安全作为独立法益的地位，导致数据犯罪有沦为新“口袋罪”的风险。

因此，笔者主张将数据犯罪对标《数据安全法》中数据安全的定义，重视数据安全法益的独立地位；并根据数据所承载的信息内容对数据进行分类分级，探寻作为载体的数据背后所深藏的实质法益，厘清狭义数据犯罪同传统犯罪数据化之间的界限，将表面上针对数据实施、实际上侵犯其他法益的行为分流于财产类、信息类等传统犯罪的规制当中，从而实现对数据犯罪的限缩和分流，避免数据犯罪落入口袋罪的窠臼。

2. 数据法益保护的属性与内涵之检视

我国数据犯罪的司法实践乱象频发，归根结底是因为立法未明确刑事法律中数据的内涵与外延，司法中未准确把握狭义数据犯罪所保护法益的内涵和外延，常将侵犯公民财产、个人信息相关数据的行为也笼统归置于保护数据安全法益的犯罪之下，造成数据犯罪开口广阔，而相对缺失了对公民财产权、隐私权等个人权益保护的畸形现象[1]。要厘清狭义数据犯罪与传统犯罪数据化之间的区别，必须明确数据

的概念和本质，明确我国刑法中数据犯罪所保护的法益，重视数据安全法益的独立地位，利用法益对犯罪的规制机能实现数据犯罪的限缩和分流。

2.1. 数据法益的属性为集体法益

在犯罪的本质究竟为何的问题上，A. Feuerbach (费尔巴哈)提出了权利侵害说，认为犯罪是侵害他人权利的行为，国家也具有人格享有权利，对国家的犯罪也是对权利的侵害，这是法益侵害说的前身。但权利侵害说本身存在明显弊病，使用权利的观念并不能很好地说明实定法规定的犯罪，例如对宗教、伦理实施的犯罪，就没有侵害具体的权利。因而法益侵害说逐渐替代了权利侵害说，成为了主流。法益侵害说是由 J.M.F. Birnbaum (比恩鲍姆)提出的，他认为犯罪侵害的作为权利的对象、由国家所保护的财(gut)或使其遭受危险，这个立场被李斯特与宾丁继承与发展。宾丁认为，规范的任务与国家的目的是一致的，就是保障和平、健康的生活的诸条件，这种人、物、状态等健全的共同生活的诸条件，就是保护客体，即法益[2]。而李斯特认为，“由法律所保护的利益，我们称之为法益。法益就是合法的利益。所有的法益，无论是个人的利益，还是集体的利益，都是生活利益，这些利益的存在并非法制的产物，而是社会本身的产物。但是，法律的保护将生活利益上升为法益”[3]。可见在李斯特看来，法益是前实定的概念，他赋予法益概念以刑事政策的机能，强调法益对立法权的指导和限制作用。总而言之，法益说回答了犯罪的本质问题，只有侵害法益的行为才可能构成犯罪，法益是一切犯罪成立的基础，是犯罪构成要件的基础，是解释其他犯罪构成部分的基础，更是了解并解释立法者意图的基础[4]。目前，学界普遍认为罪名所保护的法益具有立法批判功能和解释适用功能。从我国数据犯罪的司法窘境来看，实务界并未正确理解数据犯罪的法益内涵和外延，因其惰性而对数据的载体功能和客体功能不加区分，将所有以数据为媒介的行为都囊括到数据犯罪中来，使数据法益的构成要件解释机能未能正常发挥，进一步导致其犯罪界分功能的严重缺位。

法益对刑事立法和刑事司法都起到规制作用，只有对法益进行清晰厘定、才能准确界定犯罪行为的性质，从而正确地定罪量刑。我国刑法学界一般认为，法益是建立刑法分则体系的基本依据：从我国刑法分则的体例来看，我国刑法是按照同类客体对犯罪进行分类的，归于一章规定的犯罪，其侵害的法益必然具有共同特征。我国刑法第二条明确了刑法的任务是保护法益，我国刑法分则的每一个罪名背后都有其保护的特定法益，同一个条文也可能许保护了多个法益，这些法益又分为主要客体和次要客体，为分则条文着重保护的客体是主要客体，决定了该罪名的所处的章节位置。总而言之，法益对犯罪的构成具有规制功能，法益是区分具体犯罪类型的基本标准，法益对类罪的划分和个罪的归罪都有规制作用，对犯罪行为的定性必然要考虑其侵犯的法益：同样是盗窃行为，盗窃钱包和盗伐林木所构成的罪名不同，其本质区别在于侵害的法益不同。同理，狭义数据犯罪同传统犯罪数据化的区别，其本质在于行为所侵犯的主要法益不同。我国用于规制狭义数据犯罪的罪名在刑法分则中隶属扰乱公共秩序罪的章节，可见数据安全是有别于财产法益、人格法益等个人法益而独立存在的一种公法益，代表着大数据的公共管理秩序。而数据作为信息存在的形式和载体，必然同时具有数据、财产、人格、商业秘密等双重或多重属性，可能同时承载双重或多重法益。要将以数据为对象的犯罪行为正确定罪量刑，就必须对其承载的信息内容性质进行辨别和讨论，挖掘数据背后隐藏的法益，甄别行为到底是侵犯了动态的数据安全法益，还是侵犯了数据背后静态的传统法益，从而实现数据犯罪与传统犯罪数据化之间的分流。

明确我国计算机信息系统类犯罪的保护法益是数据安全，肯定数据安全法益的独立地位，其实是从法益角度对我国数据犯罪的入口进行限缩。我国典型的狭义数据犯罪，非法获取计算机系统信息罪，一般性地保护了计算机内的数据不受他人非法查看、下载、复制，侵入计算机系统获取了数据而未有进一步行为，则扰乱了数据的管理秩序，侵犯数据安全法益，仅构成数据犯罪。行为人侵犯数据表层外壳时

刑法即介入制止，以免行为人进一步对数据的里层进行侵犯，使公民的财产、人格等法益受损害，可以视为对公民法益的一种前置保护。而当行为人入侵数据的保护层后对其数据进行进一步的利用，如泄露、出售、非法利用数据，则在侵犯数据安全法益之后，又进一步侵犯了数据的里层法益，可能触及其他传统犯罪的射程，因此可将以数据为侵害对象的犯罪行为分流于传统犯罪的规制范围中。至于数据犯罪同传统犯罪数字化的异化之间究竟是竞合还是牵连，则要遵循罪数形态规则，结合具体案情分析。

2.2. 数据法益的双层次内涵检视

从技术层面来看，“数据具有工具性，它作为生成和传输信息的数字编码技术，体现为以二进制为基础的比特或比特币流”[5]，而这只是数据的形式体现。《数据安全法》第三条第一款将数据定义为任何以电子或者其他方式对信息的记录，这是数据的法规范定义。可见，在大数据时代，网络空间中的所有信息都以二进制代码的数据为载体，数据实质上是对信息的电子化记录形式，数据与信息是外壳与内核的关系。从规范层面来看，我们可以将数据剥离为表里两层讨论：表层是作为载体存在的二进制代码本身，里层是数据所承载的信息内容。

2.2.1. “数据”本体具有独立的刑法保护价值

表层作为信息载体的二进制代码本身就是一种资源，掌握数据库相当于掌握了财富密码，甚至可以在瞬息万变的时代中掌握博弈的先机。大数据资源本身就极具价值，如何有效保障数据安全成为大数据时代的重要课题；数据安全完全具备独立法益的地位，值得立法的专门保护。新出台的《数据安全法》第三条第三款将数据安全定义为“通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全的能力”；第四条对维护数据安全提出要求，要求建立健全数据安全治理体系，提高数据安全保障能力。由此可见，《数据安全法》实质上将数据安全定义为一个动态的过程，认为数据安全即围绕数据全生命周期进行规制和保护的一系列动态保障措施。当行为人通过“撞库”、“爬虫”违法抓取等手段攻击数据库的防火墙，破坏数据的外在保护措施、入侵数据库时，就已经侵犯了数据安全法益。

刑法是各部门法的保障法，应当与前置法相衔接；而《数据安全法》作为大数据管理的基本法律规范，对作为第二道防线的刑法具有塑造作用。在前置法的视野下，数据安全是一种独立存在的法益[6]。根据法秩序统一的原理，刑法所规制的数据犯罪，其保护法益应当同《数据安全法》对接。刑法第二百八十五条规定，非法获取计算机信息系统数据、非法控制计算机信息系统罪，是指违反国家规定，侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，情节严重的行为。上述两个罪名规定的行为模式，其实就是对保护数据的外在“防火墙”进行入侵，获取了作为数据表层的二进制代码，在行为人还未进一步深入侵犯数据的里层内容时即由刑法介入制止，可见《数据安全法》同刑法中规制数据犯罪的规定是可以完成自洽的。“法律的生命在于解释”，因此解释应该以解释法律文本内在的意义为目标，挖掘并阐明条文客观上蕴含的意义，使法律尽量摆脱其滞后性的桎梏，符合现实生活中规制行为的需要[7]。采取客观解释进路时，将非法获取计算机信息系统数据、非法控制计算机信息系统罪的保护法益扩大理解为保障数据生命全周期的数据安全并无语义障碍，将行为类型扩充至入侵、破坏数据的防护措施，未超出刑法条文的应有之义，将计算机信息系统扩充解释为包含移动智能终端、APP 应用软件、蓝牙等设备等新型数据载体，仍符合国民的“前理解”范围[8]。

肯定数据安全法益的独立地位，运用数据安全法益的规范解释机能，可以使实践中许多数据犯罪的疑难案件得以妥善处置。例如，在陈某等破坏计算机信息系统罪一案中((2020)浙 10 刑终 334 号)，对于陈某与他人共谋通过非法手段侵入计算机系统，修改系统内储存的考生成绩使相关考生通过考试，但并

未造成计算机信息系统不能正常运行的行为，产生了是否构成破坏计算机信息系统罪的争议[9]。若按照传统刑法解释对于计算机信息系统类犯罪的理解，行为未破坏、扰乱计算机信息系统的运行，则不能纳入该类罪的管制；但在陈某一案中，其采用技术手段侵入计算机系统并修改内部储存的数据信息、获取非法利益的行为，虽未破坏计算机系统的正常运行，但已然扰乱了数据管理秩序、使行为人获取不当竞争利益，具有明显的社会危害性，应当纳入刑法的规制范畴。若肯定数据安全法益的存在，不拘泥于数据犯罪必须破坏计算机信息系统的正常运行，则可肯定陈某采用技术手段破坏系统存储数据的外在保障措施从而获取并修改数据的行为，已然侵害数据生命周期位于存储阶段的安全，可防止司法实践中不恰当限缩数据犯罪的处罚范围的乱象，妥善处理该类行为的刑法规制问题。

2.2.2. “数据”载体背后的权益侵害

随着数字化技术的迅猛发展，越来越多权利客体都卸下了物质载体这一“枷锁”，以数据的形式储存、传输和利用[10]。越来越多权利客体披上了数据的外壳，形成了了狭义数据犯罪同传统犯罪的数字化异化之间的模糊地带。许多犯罪行为通过侵害数据载体而侵犯数据表征的传统法益，在这类犯罪案件当中，数据仅仅起到中间媒介的作用，而非犯罪行为的最终损害客体，例如以“撞库”形式窃取考生信息以侵害受害人的个人信息权益，以盗窃网络虚拟财产来侵犯被害人的财产权益等。数据的载体作用也体现在我国的立法体系当中：《数据安全法》第二十一条规定了数据的分类分级制度，对数据进行分类就意味着对数据的讨论不能仅停留在表层，而必须深入到数据的里层分析其属性，根据数据所承载的信息内容不同对其进行分类。2021 年通过的《上海市数据条例》第十二条规定，“本市依法保护自然人对其个人信息享有的人格权益。本市依法保护自然人、法人和非法人组织在使用、加工等数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益。”可见数据权益不仅包含数据安全本身，还可能包含财产权益、人格权益等传统法益，至于数据到底承载了哪些法益，则由数据的里层信息决定。

根据数据所承载的信息内容不同，可以大致将数据分为财产利益类数据、个人信息类数据与其他数据三类，前两类数据背后分别隐藏着公民的财产法益和人格法益[11]。而传统财产类犯罪和个人信息类犯罪的网络化、数据化，正是与狭义数据犯罪产生模糊交界的“重灾区”，针对前两类数据的犯罪行为可能为财产犯罪、侵犯个人信息犯罪所涵盖，究竟以何罪对个案进行规制，需要结合具体案件的事实、对犯罪行为所侵犯的法益进行小心甄别。

3. 狭义数据犯罪与传统犯罪数据化之间的界分

通过检索我国关于数据犯罪的司法判决来看，网络虚拟财产和不具有财产属性的网络账号及其密码是非法获取计算机信息系统数据罪中的主要数据类型[11]。此外还包括户口信息、生物识别信息、社保信息等个人信息数据。可见涉及财产性数据、个人信息类数据的犯罪行为最容易产生定性争议。接下来，笔者将根据数据类别不同，厘清狭义数据犯罪同财产犯罪和个人信息犯罪数据化之间的界限，将以数据为侵害对象而进一步侵犯他人财产权、个人信息权益的犯罪行为分流于传统犯罪的规制当中。

3.1. 财产利益类数据

承载财产利益类的数据，最典型的就是虚拟财产，虚拟财产兼具数据和财产利益双重属性。但司法实践中普遍将窃取虚拟财产的行为评价为非法获取计算机信息系统数据罪，甚至最高人民法院在《关于办理盗窃刑事案件适用法律若干问题的解释》中指出，虚拟财产的法律属性是计算机信息系统数据而不是公私财物。要疏通财产类数据的传统犯罪进路，就必须回答以下三个问题：虚拟财产无实体，能否评价为财产类犯罪中的公私财物？窃取虚拟财产是否符合盗窃罪转移占有的行为模式？通过对数据的操作

窃取虚拟财产，其与非法获取数据罪的关系是什么[12]？

第一，传统观点将盗窃罪的犯罪对象限定于实体物，已经跟不上现代社会的发展进程，线上支付、网购等早已成为人们生活的一部分，通过网络数据进行经济往来早已在日常生活中司空见惯，没有人会否认微信零钱、支付宝余额的财物属性，盗取微信零钱的行为毫无争议地构成盗窃罪，因为其代表了受害人的财产利益，有体性不应再是限制财物构成的条件。 我国民法典制定以前，《物权法》规定：“本法所称物，包括不动产和动产。法律规定权利作为物权客体的，依照其规定。”其中权利是物权的无形客体。民法典制定后，其总则第五章“财产权利”的第一百零七条明确指出：“法律对数据、网络虚拟财产的保护有规定的，依照其规定。”可见我国民法对于财物并没有恪守物必有体的立场，而包容了无体物，且首次以立法形式对虚拟财产作出宣誓性规定[13]。民法作为前置法，其对无体物的立场也深刻影响着我国刑法及其司法解释的方向。我国刑法司法解释明确规定：“盗窃的公私财物，包括电力、煤气、天然气等。”且我国刑法学界的通说认为，财产性利益属于财物，可以成为财产犯罪的客体[13]。

第二，在窃取网络游戏装备、虚拟货币等虚拟财产的场合，相关账号内以数据形式呈现的装备、余额，可以视为用户要求网络供应商兑现服务的权利凭证。行为人通过控制账号获得了对网络供应商的债权，从而实现了虚拟财产的转移，使受害人失去了可兑现财产利益的权利凭证。债权债务系民法中的财产性利益，可为虚拟财产的法律属性提供依据[14]。且该行为模式也符合盗窃罪“打破原占有、建立新占有”的行为构造。

第三，虚拟财产犯罪最典型的模式就是利用技术手段非法获取他人网络游戏账号及密码，并通过登录该账号实现虚拟财产转移。通过对该模型进行分析，发现其中其实存在两个行为：第一个行为是利用技术手段登录受害人账号，第二个行为是对账号内的虚拟财产进行转移。若坚持数据安全法益同财产法益独立的立场，真正具备财产利益属性的是账号内的虚拟财产，而账号只是权利人访问服务系统的门户凭证。窃取他人账号密码并登录其实是扰乱了网络空间的正常管理秩序，其背后象征的是位于公共秩序章节的数据安全法益。若只是窃取了他人的账号并倒卖，未侵占、转移账号内的虚拟财产，应当归于狭义数据犯罪规制；若窃取账号并盗窃、倒卖其中的虚拟财产，实际上是两个行为侵犯两个法益的数罪形态，可考虑按照牵连犯原则从一重而处，分流于财产犯罪规制。

3.2. 个人信息类数据

在网络信息技术发达的今天，个人信息常以电子数据的形式呈现和储存，但也不仅限于电子形式，保护个人信息的立法目的是避免公民的特定信息被非法获取、传播，保证公民的私生活不受干扰，与数据犯罪保护数据生命全周期的动态安全目的有着本质区别。在司法实践中，常出现数据属性界定不清，从而将侵犯可识别自然人信息的数据定性为数据犯罪或将不能联结特定个人的数据定性为侵犯个人信息罪得现象。

《个人信息保护法》第四条将个人信息定义为个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。可见区别个人信息类数据和其他数据的关键在于特定个人的可识别性，当通过获取某些数据能直接识别到特定自然人时，其行为可能已经侵犯到公民的个人信息权利。实践中常出现争议的是非法获取个人账号类信息到底归于数据犯罪还是侵犯公民个人信息罪。为了规范网络空间的治理、规范公民的网络言行，许多网站和 app 都已经要求用户账号进行实名认证，账号及其密码往往绑定了公民个人的身份证号、手机号等特定信息，从这个意义上说，账户类数据确实属于个人信息。但在对行为进行定性时，除考虑数据的类别以外，还需关注行为所实质侵害的法益，保护个人信息的罪名旨在保护公民的私生活安宁，而在实践中，行为人通过技术手段获取公民的账号及密码，通常是为了窃取公民账号内的财产，却并不关心账号背后的特定个人，更不会对特

定个人的私生活进行干扰。其行为威胁到了受害人的财产权益，威胁到了网络空间的数据管理和保护秩序，却并未打扰公民的私生活安宁，从法益规制的角度分析，该行为只构成数据犯罪和财产犯罪。但若行为人通过“撞库”等技术行为，海量获取网站用户的账户信息并进行非法提供、非法出售、非法利用，其前一行为破坏了数据位于储存周期的保障措施、对数据安全造成威胁，后一行为则进一步威胁到了公民的私生活安宁，因而构成数据犯罪和侵犯公民个人信息罪的牵连，可根据牵连犯的处置原则，将该类行为分流于个人信息犯罪的规制当中。

4. 结语

侵犯数据的行为繁杂多样不可一概而论，数据里层承载的信息也多种多样。要在司法实践中对以数据为侵犯对象的行为进行准确定性，就必须坚持数据安全法益的独立地位，并结合具体案情分析行为的样态，透过现象看本质，小心甄别行为所实质侵犯的法益。本文通过对数据表里层蕴藏法益的分析，将数据犯罪的保护法益定位于数据安全法益，试图运用法益对犯罪构成的规制机能，对狭义数据犯罪的入口进行限缩，以期实现数据犯罪与传统犯罪数据化之间的分流，避免数据犯罪落入“口袋罪”的窠臼，推动司法实践的研究与进步。

参考文献

[1] 苏青. 数据犯罪的规制困境及其对策完善——基于非法获取计算机信息系统数据罪的展开[J]. 法学, 2022(7): 72-83.

[2] 牛忠志. 德日“法益说”适应中国的“四维”改良[J]. 政治与法律, 2022(9): 112-129. https://doi.org/10.15984/j.cnki.1005-9512.2022.09.008

[3] [德]弗兰茨·冯·李斯特. 德国刑法教科书[M]. 徐久生, 译. 北京: 法律出版社, 2006.

[4] 魏东. 论作为犯罪客体的法益及其理论问题[J]. 政治与法律, 2003(4): 32-36.

[5] 阎二鹏. “数据安全法益”命题下虚拟财产犯罪的归责路径重构[J]. 政治与法律, 2022(12): 45-59. https://doi.org/10.15984/j.cnki.1005-9512.2022.12.004

[6] 王惠敏. 网络数据安全独立性之提倡及其刑法展开[J]. 法治研究, 2023(3): 117-131. https://doi.org/10.16224/j.cnki.cn33-1343/d.20230505.003

[7] 阮林赟. 双层社会背景下隔空猥亵的客观解释[J]. 青少年犯罪问题, 2020(6): 102-110.

[8] 杨志琼. 我国数据犯罪的司法困境与出路: 以数据安全法益为中心[J]. 环球法律评论, 2019, 41(6): 151-171.

[9] 童德华, 王一冰. 数据犯罪的保护法益新论——“数据内容的保密性和效用性”的证成与展开[J]. 大连理工大学学报(社会科学版), 2023, 44(3): 54-64.

[10] 劳东燕. 个人数据的刑法保护模式[J]. 比较法研究, 2020(5): 35-50.

[11] 韩婧颖. 数据犯罪的司法困境及治理进路[C]//北京师范大学刑事法律科学研究院. 《上海法学研究》集刊 2022年第 17 卷——长三角法治论坛文集. 2023: 8.

[12] 刘宪权. 元宇宙空间非法获取虚拟财产行为定性的刑法分析[J]. 东方法学, 2023(1): 49-61. https://doi.org/10.19404/j.cnki.dffx.20230111.005

[13] 陈兴良. 虚拟财产的刑法属性及其保护路径[J]. 中国法学, 2017(2): 146-172. https://doi.org/10.14111/j.cnki.zgfx.2017.02.008

[14] 陈罗兰. 虚拟财产的刑法意义[J]. 法学, 2021(11): 86-98.