

数字经济时代我国数据犯罪刑法规制的挑战与应对

刘银山

北京市公安局西城分局, 北京

收稿日期: 2024年7月15日; 录用日期: 2024年7月26日; 发布日期: 2024年8月30日

摘要

数字经济时代下, 我国数据犯罪呈现新的发展趋势, 具有企业性、大批量以及公开性等特点。数据利用安全法益关乎我国经济市场的稳定性, 只有加强数据安全规则制定, 顺应大数据反垄断的公共政策需求, 才能变消极防御为积极管控。为此, 本文从数据刑事保护法益的界定和数据犯罪构成要件两个方面出发, 详细分析了数字经济时代我国数据犯罪刑法规制所面临的挑战, 并从明晰数据犯罪法益保护内涵、细化数据分类模式、重释犯罪行为要件以及建立结果量化标准四个方面提出应对路径, 以期提升数据利用安全, 推动社会长远稳定发展。

关键词

数字经济, 数据犯罪, 刑法规制

Challenges and Responses to the Criminal Law Regulation of Data Crimes in China in the Digital Economy Era

Yinshan Liu

Xicheng Branch of Beijing Municipal Public Security Bureau, Beijing

Received: Jul. 15th, 2024; accepted: Jul. 26th, 2024; published: Aug. 30th, 2024

Abstract

In the era of digital economy, data crimes in China have shown new development trends, characterized by enterprise, large-scale, and openness. The legal interests of data utilization security are related to the stability of China's economic market. Only by strengthening the formulation of data

security rules and complying with the public policy needs of big data anti-monopoly can we transform passive defense into active control. Therefore, this article analyzes in detail the challenges faced by China's criminal law regulation of data crimes in the digital economy era from two aspects: the definition of legal interests in data criminal protection and the constituent elements of data crimes. It proposes a response path from four aspects: clarifying the connotation of legal interests protection of data crimes, refining the data classification mode, reinterpreting the elements of criminal behavior, and establishing quantitative standards for results, in order to enhance data utilization security and promote long-term social stability and development.

Keywords

Digital Economy, Data Crime, Criminal Law Regulation

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

随着数字经济的深入发展,有关数据泄漏、数据垄断、数据盗窃、数据滥用等在内的数据犯罪日甚,逐渐成为影响现代市场经济稳定发展的重要因素。作为现代犯罪刑法规制的新议题,数据犯罪多表现为集体性、公开性、整体化等特征,是数据安全维护面临的重要难点与挑战。2021年,我国正式颁布了《数据安全法》,对数据犯罪刑法规制有了新的防护要求。为此,数字经济时代,探讨我国数据犯罪刑法规制的挑战与应对措施具有重大现实意义。

2. 数字经济时代下数据犯罪内涵

我国立法并未对数据犯罪做出明确定义,从学界来看,对数据犯罪可以从狭义和广义方面来理解,狭义认为,数据犯罪是将数据作为犯罪对象的犯罪,即通过非法获取、篡改、增删等行为侵害数据。广义的数据犯罪,在狭义的基础上,增设了以数据为手段工具的犯罪行为,认为数据犯罪应当涵盖将数据作为犯罪工具、犯罪载体等行为。随着数字经济的快速发展,有关加密货币犯罪、AI技术犯罪以及数据存储系统攻击等数据犯罪呈现新样态,冲击着传统数据犯罪理论范围。基于此,数字经济时代下的数据犯罪概念应当是可延展性、流动性的,即以一切计算机技术和网络信息为手段,通过非法侵入、传输、破坏、篡改等违法行为,侵害个人隐私、商业利益和国家安全的行为。总的来说,数字经济时代下数据犯罪具有三个方面特征:其一,行为方式的多样性。从行为方式角度来看,数据犯罪可以分为非法取得型数据犯罪、流量造假型数据犯罪、手段工具型数据犯罪、破坏编纂型数据犯罪等,这些分类都是基于数据犯罪行为方式特点作出的划分。随着社会生活复杂程度的加深,有关数据犯罪行为还将呈现新的种类,比如,以“撞库”或“拖库”行为非法获取游戏账号、模拟用户规避平台监管、虚拟钱包窃取、虚拟图像诈骗以及篡改系统数据等犯罪行为的出现,对刑法规制提出了新的挑战;其二,保护法益的多重性。数据犯罪侵害法益既包括个人信息,也包括虚拟财产法益、国家安全、经济命脉、环境利益等各种法益类型,这些法益还与盗窃、诈骗、侵吞等传统犯罪联系在一起,呈现出保护法益的多重性特点。比如,在刑事司法实践,数据犯罪可以涉及的罪名包括但不限于破坏计算机信息系统罪、侵犯公民个人信息罪、侵犯商业秘密罪以及非法经营罪等等;其三,犯罪后果的不可预估性。与传统犯罪不同,数字经济时代数据流通及交易的高效性,使得数据犯罪在只对法益造成微量损害的前提下,还能依托信息技术的高渗透性,给社会造成指数级的伤害,从而导致难以预估的后果。同时,数据犯罪的网络外部性,致使数据

犯罪责任主体认定困难，一定程度影响犯罪后果的责任分配。

3. 数字经济时代我国数据犯罪刑法规制的挑战

3.1. 数据刑事保护法益的界定

由于数据概念本身的可扩展性和多重解释性，传统数据安全法益难以精准描述数据安全需求，对数据保护法益的界定成为当前数据犯罪刑法规制的首要挑战之一。比如，从计算机科学来看，数据代指计算机系统中以数字或字母等为客观形式的介质统称；在国际信息技术术语中，数据更侧重于信息表达，强调数据为适用于沟通的形式化方法；从欧盟的定义来看，数据偏向“个人数据”解释，代指可以是被自然人身份的信息本身；而当前，我国在《数据安全法》中将数据定义为网络活动中产生的一系列电子纪录。基于此，有关数据安全犯罪的相关罪名众多，包括但不限于非法获取计算机信息系统数据罪、破坏计算机系统罪、非法利用信息网络罪、侵犯公民个人信息罪、侵犯商业秘密罪、非法获取国家秘密罪等，其现代立法保护法益杂糅不清。同时，对数据的法律安全保护更多是从静态、监管以及个人信息保护层面出发^[1]，强化民事以及行政法意义的安全防护，从而忽略刑事安全防护功能。但数据本身是一种沟通与交互表达，在现实生活中具有无形流动的特点，数据刑事保护法益更多偏向于个人信息保护功能，对数据之间大规模交互与流动中产生的利益冲突缺乏规定，无法满足现代公益性数据保护需求。随着信息技术的深入发展，数据的利益主体将会愈加多元，利益规模将会不断扩张，有关企业、金融机构以及社会团体等多主体数据犯罪行为还将持续深化，在诈骗罪、敲诈勒索罪等犯罪领域出现扩散化特征。传统数据刑事保护法益如果不能突破私域限制，就无法针对这些问题做出有效回应，也就无法满足公共数据共享与利用趋势下，经济社会对刑法数据安全保护的期待与要求。

3.2. 数据犯罪构成要件判断

构成要件判断是数据犯罪构成要件的另一重点难题。具体来说，数据犯罪构成要件主要存在客体法益界定范围狭窄、法益保护模式单一、构成要件缺乏独立标准等问题。从客体法益界定范围狭窄来看，当前，数据犯罪法益保护对象仍然侧重个人信息保护，对其他关联信息或者特定信息保护只是通过传统刑法所规定的罪名体系，即对信息犯罪予以扩张、外延方式实现，没有实现数据法益独立性的保护。同时，在数字经济时代，数据隐私保护与可公开获取企业数据的反垄断保护交叉重叠、关系复杂，在立法、司法以及学界尚存争议，给数据犯罪对象要件判断带来一定难度；从法益保护模式单一来看，随着数字经济商业模式的多样化发展，有关数据窃取、数据破坏、数据污染、数据丢失以及垃圾邮件等犯罪行为层出不穷，不仅包括了侵害数据载体的传统犯罪，还包括了以数据为侵害对象的新型犯罪。基于此，有关数据犯罪刑法规制应当根据数据在经济社会中的重要程度，建立分级分类保护制度，在遵守罪刑均衡的基本刑法原则的基础上，推行个性化的法益保护方案。但是，我国刑事立法并未对数据安全采取分级分类保护模式，导致数据保护的不合理、不公平现象的发生。比如，从《刑法》第 285 条规定来看，对于国家重要领域的核心数据保护力度远不如其他领域；从构成要件缺乏独立标准来看，在审判实践中，对有关数据的侵害行为往往与计算机信息系统犯罪过度关联、边界模糊，导致数据犯罪构成标准长期受制于计算机犯罪，没有明确且统一的专属性规范。同时，数据犯罪构成要件的独立标准欠缺，导致数据权利保护链条不全，致使有关数据违法公开、违规销毁、擅自提供等犯罪行为游离于我国刑法打击范围之外。

4. 数字经济时代我国数据犯罪刑法规制路径

4.1. 明晰数据犯罪的法益保护内涵

要建立完整的数据保护法益体系，清晰定位刑事法律保护的法益类型。一方面，扩充数据法益内涵。

要摒弃传统以计算机系统固化数据概念的做法，以数据生存周期界定数据刑事保护范围，利用过程思维，对数据参与生产过程中的采集、传输、存储、处理、交换、消费等阶段中的数据资源获取成本和数据流转特性予以充分考量，以明确数据法益保护特征，全面把握数据利用动态环节需求，并由此确定数据刑事法律保护应对何种类型、范围的数据信息进行规范；另一方面，充分考虑数据独立价值。我国立法可以从刑法条文出发，在罪名设置上以数据的独立价值为核心，认定数据犯罪的独立立法方向，从而将其从以计算机系统罪名规制的桎梏中摆脱出来，以独立罪名对数据法益予以直接保护。比如，根据数据利用全过程中造成的侵害设立相对独立的具体罪名，在数据收集环节设立非法收集数据罪，在数据传输环节设立非法传输数据罪，在数据管理环节设立妨害数据管理罪等，从而避免现行《刑法》第285条第2款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在“计算机信息系统”和“数据”上的杂糅。

4.2. 建立细化的数据分级分类模式

数字经济时代下的数据类型不仅包括计算机信息系统内部存在的以图片、软件、浏览痕迹为主的数据信息，还包括数据从产生到管理的全生命周期进程中的各类数据。不同种类的数据所蕴含的法益性质、安全层级以及重要程度具有差异，为了进一步明确数据犯罪成立条件及责任分配，释析数据犯罪构成要件的前提必须是建立细化的数据分级分类模式。具体来说，可以从属性标准和危害结果两个方面建立分级分类模式。从属性标准来看，可以按照数据本体的内容、来源、行业、特征、效用等属性，将具有相同属性的数据划分在一起，并针对该种属性的数据采取针对性安全保护措施。比如，以行业维度为标准，将数据划分医疗、交通、商业、金融等不同领域的的数据；从危害结果来看，可以按照数据对经济社会的贡献程度或危害程度，将数据进行安全分级。比如，以国家安全、政府治理、公民个人信息、商业秘密为顺序，确定国家安全数据作为最高层级数据加以重点保护，对涉及到公民个人信息及企业数据应被划分第二层级加以相对宽松保护^[2]。此外，数据分级分类还要在确定具有足够全面性的基础上，确定好不同类型数据之间的平等关系。

4.3. 重释数据犯罪的行为类型要件

对于数据犯罪的正确认定，除了需要考法益保护内涵，还要考虑行为类型要件，解决数据行为认定困难与争议。首先，要完善数据犯罪行为技术判断。行为类型要件的认定难题常常源于判定技术水平不够。要积极通过网络爬虫、数据解密技术、深度伪造技术等数字技术，对数据收集、处理、修改等行为进行科学识别，以明确界定行为特征，识别数据犯罪危害；其次，延展数据犯罪行为。要适度扩张信息数据罪名的客观行为要件，以数据生命周期延展已有罪名行为范围。比如，在非法获取计算机信息系统罪中原有的“系统侵入”获取数据与“其他技术手段”获取数据的行为类型基础上，进一步明确非侵入系统方式获取数据行为，从非法获取系统数据的角度，归类违法行为特征；最后，明确数据犯罪行为类型概念。当前，我国《刑法》针对数据犯罪创设了很多新的罪名，这些新兴罪名的创设会因表述概括、语言偏差，造成罪名边界的模糊性，从而导致相关罪名适用的困难。为此，刑事立法要在严格遵循罪刑法定原则基础上，对其罪名保护法益、行为类型、刑罚种类予以确定性规定，并根据宏观布局、新旧法条安排及司法实践需求，细化罪名的客观构成要件。

4.4. 建立数据犯罪的结果量化标准

在认定数据犯罪过程中，鉴于数据犯罪整体呈现动态性和片段性特点，数据价值评估容易出现不到位、不明确等问题，亟待构建数据结果量化标准，以客观衡量犯罪危害结果，确保数据价值评估的准确性。比如，对侵犯公民个人信息罪的有关案件中，如果犯罪人仅是购买等非法方式获取、收集公民个人信息，而非利用计算机信息系统实施数据犯罪，则可通过犯罪人获得的具体收益量刑裁判。同时，当数

据收益无法确定,无法以数额定性犯罪时,还可以通过数据本身在经济社会中的重要程度或者数据犯罪产生的危害结果,以具体情节为切入点进行综合判断。比如,针对高考志愿被篡改案件,一般来说,司法实践都是根据篡改数据行为产生的危害结果决定量刑程度,当篡改行为被及时发现而并未实施成功时,可以不做刑事处理,只给予相应的治安管理处罚。一旦篡改行为成功造成损害后果,则以破坏计算机信息系统罪定罪处罚。鉴于篡改他人高考志愿产生的危害结果是无法用损失数额来具体认定,我国立法应对该种数据犯罪行为设立单独罪名,承认该类数据犯罪行为对社会公共秩序的破坏,并根据具体后果和影响来准确量刑相关行为,确保罪责刑相适应原则。

4.5. 处理刑法与行政前置法的关系

刑法对数据犯罪的规制效果,不仅与刑法本身的规范质量与司法技术相关,还与刑法和行政法等其他法律共同组成的社会调控关系相关。为此,要处理好刑法与行政前置法的关系。一方面,贯彻法秩序统一性原理。作为其他部门法的基本保障,刑法对信息网络犯罪、数据犯罪的许多规定牵涉行政法内容,二者在相关领域规制目标一致,具有统一性关系,要始终确保二者的有效衔接。比如,要在整体法秩序基础上,以“可识别性”为标准,对侵犯公民个人信息罪中有关“个人信息”的认定标准和判断依据予以统一,即确保我国《刑法》相关概念始终与《个人信息保护法》《民法典》等相关规定界定一致,避免彼此之间出现冲突^[3]。同时,对于匿名化信息、已经合法公开的个人信息是否作为“公民个人信息”问题予以明确,前者因其无法识别性和不可逆性特征无法构成侵犯公民个人信息罪,后者原则上虽不能作为侵犯公民个人信息罪的对象,但还要结合不同法律解释,根据权利人公开数据原因、自主意愿、公开途径等因素进行综合判断。

5. 结束语

鉴于法律规定的滞后性,有关数字犯罪刑法规制总是落后于技术发展,为数字犯罪提供法外空间。特别是随着数字技术不断成熟,有关数字风险概率不减反增,更加难以察觉和防范。同时,我国数据规则尚不成熟,在数据流通、法益确定、要件内容以及裁判规则方面都面临重大挑战。未来,相关工作者要深入实践,在顺应数字经济发展趋势的基础上,不断完善我国数据犯罪的刑法规制。

参考文献

- [1] 杨志琼. 数字经济时代我国数据犯罪刑法规制的挑战与应对[J]. 中国法学, 2023(1): 124-141.
- [2] 袁彬, 薛力铭. 数据犯罪的双重法益及其保护路径[J]. 中州学刊, 2024(6): 70-78.
- [3] 热娜古·阿帕尔. 数字经济刑事合规风险的多维性分析及规制路径[J]. 中国海商法研究, 2024, 35(2): 77-90.