

数据犯罪司法认定的迷局及破解

成家颖

(湘潭大学 法学院, 湖南 湘潭 411105)

摘要:我国数据犯罪的司法认定存在罪名“口袋化”的迷局,原因在于司法实践中“数据”概念覆盖了“信息”概念、数据法益与信息法益纠缠不清。数据与信息是交叉关系。应将数据定义为:计算机信息系统内储存、处理、传输的二进制代码,和以其他形式记录的科学实验、检验、统计、计算等所获得的和用于科学研究、技术设计、查证、决策等的数值信息。数据包括“信息类数据”和“功能性数据”。信息类数据的法益应为其所记录的信息所涉法益,功能性数据的法益则是其本身的保密性、完整性和可用性。数据犯罪不应限于非法获取计算机信息系统数据罪和破坏计算机信息系统罪,而是包括所有以数据为对象的犯罪。对数据犯罪应采用类型化处理方式。信息类数据犯罪的罪名认定应以行为所侵犯的信息所涉法益为依据;功能性数据犯罪的罪名认定应以行为所侵犯的功能性数据的具体功能为依据。

关键词:数据犯罪;数据法益;信息类数据;功能性数据

中图分类号:D924

文献标识码:A

文章编号:1008-7699(2025)06-0062-10

1997 年《中华人民共和国刑法》(以下简称《刑法》)将破坏数据的行为纳入破坏计算机信息系统罪中,可见我国刑法很早就注意到了对计算机数据安全的保护。2009 年《中华人民共和国刑法修正案(七)》增设“非法获取计算机信息系统数据罪”,进一步保障计算机数据不被非法获取。在大数据时代,数据已成为个人重要的生产生活要素、国家重要的战略资源。2021 年,《中华人民共和国数据安全法》(以下简称《数据安全法》)出台,旨在加强对数据安全的专门保护,足见数据安全性的重要性。在北大法宝网搜索截至 2024 年 10 月 1 日被判处非法获取计算机信息系统数据罪的刑事判决书,可得到一审、简易程序和速裁程序的判决书 808 份,可见该罪名是一个适用较多的罪名。然而,刑法上数据的概念、数据法益与数据犯罪的认定问题至今仍然模糊、混乱,这导致了数据犯罪司法认定中的迷局,亟待破解。

一、数据犯罪司法认定之迷局

刑法学界一般认为,数据犯罪指我国《刑法》第 285 条第 2 款非法获取计算机信息系统数据罪和第 286 条破坏计算机信息系统罪的第 2 款。^[1]一直以来,我国法律对“数据”的内涵与外延缺乏明确界定。在《数据安全法》出台前,法学理论界通说认为,数据是指在计算机信息系统内存储、处理、传输的表现为 0 和 1 数字组合的二进制代码。^[2-5]然而,这种解释导致实践中司法机关往往只关注数据的形式而忽略其内容,^[6]将一切存在于计算机或手机等电子设备中的内容均认定为数据,^[7]上述两罪名逐渐“口袋化”。

其一,非法获取计算机信息系统数据罪的司法适用“口袋化”严重。因为现实中涉及信息网络的犯罪案件通常离不开计算机数据。此外,又因为该罪名较财产犯罪、个人信息犯罪、知识产权犯罪,罪名认定更容易,所以司法机关在处理盗窃虚拟财产、倒卖电子个人信息、剽窃电子知识产权等案件的过程中,往往就直接适用该罪名,导致对犯罪行为的社会危害性评价不足。^[8]例如,在武某盗窃案中,被告人武某侵

收稿日期:2025-06-17

基金项目:湖南省教育厅科学研究重点项目(23A0119)

作者简介:成家颖(1996-),男,湖南长沙人,湘潭大学法学院博士研究生。

入他人电脑并登录其在某比特币投资平台上的账户,随后篡改账户内的收款地址,盗走被害人账户中的比特币 70.96 个,价值人民币 20 万余元,最终法院判决被告人武某的行为构成盗窃罪,判处有期徒刑 6 年,并处罚金 8 万元。^①而在黎某非法获取计算机信息系统数据案中,被告人黎某“黑入”某比特币交易网站,盗取该网站内比特币 1478.22 个,价值人民币约 754 万元,最终法院判决被告人黎某的行为构成非法获取计算机信息系统数据罪,判处其有期徒刑 4 年,并处罚金 50 万元。^②比较上述两个案件可见,同样是盗窃比特币的案件,盗窃比特币价值少得多的行为反而被判处更高的刑罚,这显然有违罪刑相适应原则。此外,还有法院将同一案件中同样实施利用钓鱼网站盗取账号、密码的两名行为人,分别认定为非法获取计算机信息系统数据罪与侵犯公民个人信息罪,但并没有在判决书中说明二者的区别。^③还有法院以虚拟财产的数据形态为由,将检察机关指控的诈骗罪变更为非法获取计算机信息系统数据罪。^④

其二,破坏计算机信息系统罪的司法适用也存在“口袋化”趋势。^[9]主要体现为司法机关将删除、修改、增加不影响计算机信息系统运行的数据的行为认定为《刑法》第 286 条第 2 款规定的行为。例如,最高人民检察院第 34 号指导案例李骏杰等破坏计算机信息系统案中,被告人李骏杰从他人处非法购买在某购物网站发表中、差评的买家个人信息 300 余条,利用这些信息盗取买家账号、密码,登录账号并删改这些买家已发布的中、差评,从店铺处获取报酬,最终被检察院认定为破坏计算机信息系统罪。又如马某梅、谢某琴等破坏计算机信息系统案中,被告人马某梅、谢某琴伙同他人,采取偷配钥匙、遮挡监控摄像头等手段,组织替考人员在夜间非考试时间进入泰州市安全生产考试考核中心,登录江苏省三项岗位人员考试考核系统代替他人考试,获取报酬。法院认为,被告人的行为属于非法增加学员考试通过的成绩数据,判决被告人的行为构成破坏计算机信息系统罪。^⑤

司法实践中“数据”概念覆盖了以计算机代码形式存在的“信息”,导致刑法中“数据法益”与“信息法益”两个概念纠缠不清,进而导致数据犯罪与信息犯罪的司法认定混乱,这已成为我国数据犯罪治理的迷局。要破解这一迷局,首先需厘清法律上“数据”的概念,唯有在明确了数据的概念及其与信息的关系的前提下,方能准确地识别数据所蕴含的法益,进而为数据犯罪的准确认定奠定基础。

二、“数据”概念之厘清

要解决数据犯罪的认定问题,首先需厘清何谓“数据”,但当前我国法律上的“数据”概念并没有厘清,“数据法益”更是无根之木。数据的概念以及数据与信息之间的关系,法学理论界主要存在以下四种观点:一是互为表里说,即认为数据是信息的载体,信息是数据的内容;^[4-5]二是区分说,即认为数据是物理上的“文件”,信息是存在于人脑中的“知识”,二者代表了不同的权利类型;^[10]三是信息外延大于数据说,即认为数据是计算机代码形式的信息,信息包括数据和其他形式的信息;^[3]四是数据外延大于信息说,即认为数据包括承载信息的数据和不承载任何信息内容的数据。^[11]笔者认为,上述观点有的只关注数据的信息载体属性,有的只关注数据的计算机代码属性,均存在局限性。数据与信息应为交叉关系,数据可划分为“信息类数据”和“功能性数据”。

(一)数据与信息交叉关系

数据与信息长期以来难以区分的根本原因在于二者本来就无法完全界分。“数据”本就是一个多义词,它既是信息的一种载体,同时也是信息的一种类型:一方面,很长一段时间内法学界通常采取的是计算机科学对“数据”的定义,即将计算机信息系统内所有的二进制代码统称为“数据”,这些代码有的用于

① 参见浙江省台州市中级人民法院(2016)浙 10 刑终 1043 号刑事判决书。

② 参见辽宁省阜新市中级人民法院(2020)辽 09 刑终 23 号刑事判决书。

③ 参见广西壮族自治区河池市(地区)中级人民法院(2021)桂 12 刑终 199 号刑事裁定书。

④ 参见浙江省温州市中级人民法院(2019)浙 03 刑终 1117 号刑事裁定书。

⑤ 参见江苏省泰州市高港区人民法院(2023)苏 1203 刑初 169 号刑事判决书。

记录信息,但有的并不记录信息,如有的代码只是用于创建管理和运行计算机程序;另一方面,在我国社会一般人的认识中,表现为“有意义的数值”的信息也被称为“数据”。《现代汉语词典》中数据的定义为“科学实验、检验、统计等所获得的和用于科学研究、技术设计、查证、决策等的数值”,而不论其是以电子形式还是纸质等形式进行记录。例如,被记录在纸上的身高、体重、年龄等个人信息的统计表,虽然不是二进制代码,但在日常生活中也通常被称为“统计数据”或“个人数据”。在大数据时代,部分非数值的信息也逐渐被称为“数据”,如公民的姓名、性别、血型甚至指纹、行动轨迹、人脸识别等信息通常也被认为属于“个人数据”。^[12]

事实上,“数据”一词最早来源于对测量和计算所得结果的记录,^[13]远比计算机信息系统的发明更早。由此可见,要改变人们这种根深蒂固的认识是几乎不可能的。虽然法律上的概念并非一定要以社会一般人的认识为准,但立法者、司法工作者、法学学者不可能也不应该脱离社会一般人的理解,在立法、法律文书和学术写作中,他们也总是不可避免地、无意识地将某些信息称为“数据”。例如我国2024年新修订的《中华人民共和国统计法》第40条中有“编造虚假统计数据”“统计数据严重失实”这样的表述,显然是将统计所得到的“统计信息”称为了“统计数据”。又如,在脉脉非法抓取使用微博用户信息案的判决书中,法官交替使用“用户数据”“用户信息”“数据信息”指代同一对象。^①再如,有学者在理论研究中将姓名、电话号码、血型、指纹、行动轨迹等个人信息纳入“个人数据”中进行研究。^[12]当前其他许多国家的立法和法学理论中,也经常有“数据”与“信息”混用的现象。^[3]如2018年5月欧盟《一般数据保护条例》(GDPR)中将“个人数据”定义为“任何已识别或可识别的自然人相关的信息”,即将数据(data)定义为信息(information)。

2021年出台的《数据安全法》第3条规定:“本法所称数据,是指任何以电子或者其他方式对信息的记录。”这无疑是考虑到了在社会一般人的认识中,数据既是信息的一种载体,也是信息的一种类型,写在纸上的某些信息也被称为“数据”。^[14]《数据安全法》出台后,互为表里说已成为刑法学界多数说,该说将数据定义为信息的载体。^[15-17]然而,一方面该规定在内容上过于扩大了数据概念的范围,可能将某些通常不被人们称为“数据”的信息也定义为数据,如将写在宣纸上的书法作品《兰亭序》归为“数据”,显然是不合适的。另一方面,该规定在形式上又过于限缩了数据概念的范围,将数据与信息完全绑定起来,忽视了当前在社会一般人的认识中,计算机内那些不记录信息的其他计算机代码也被称为“数据”。例如,计算机中的应用程序虽然不是对信息的记录,但《刑法》第286条第2款明确将应用程序作为保护对象。由此可见,《数据安全法》将数据作为信息的下位概念,^[18]也没有准确认识到数据与信息概念的交叉关系,具有一定的局限性。

由此可见,数据与信息有交叉关系。数据包括计算机信息系统内存储、处理、传输的二进制代码,和以其他方式记录的、通常被人们称为“数据”的信息。“通常被人们称为数据的信息”既是数据的一种,又是信息的一种。除此之外,数据还包括所有的计算机代码,信息则还包括其他不被人们称为“数据”的信息。但由于“通常被人们称为数据的信息”具有较强的主观性、模糊性和变化性,因此本文采用《现代汉语词典》对数据的定义,更具有客观性、明确性和稳定性。综上所述,应将法律上的数据定义为:计算机信息系统内储存、处理、传输的二进制代码,和以其他方式记录的科学实验、检验、统计、计算等所获得的和用于科学研究、技术设计、查证、决策等的数值信息。

(二)数据分为信息类数据与功能性数据

基于以上定义,根据是否以记录信息为目的,将法律上的数据分为“信息类数据”和“功能性数据”。这一分类可作为数据法益识别及数据犯罪认定的底层逻辑,亦是破解当前数据犯罪迷局的可行路径。所谓“信息类数据”,是指以记录信息为目的的计算机代码,以及以其他方式记录的实验、检验、统计、计算等

① 参见北京知识产权法院(2016)京73民终588号民事判决书。

获得的和用于科学研究、技术设计、查证、决策等的数值类信息。所谓“功能性数据”，是指不以记录信息为目的的，在计算机信息系统内存储、处理、传输的，具有编写和运行程序、连接互联网、控制计算机系统、作为交易凭证等各种功能的二进制代码。以视频和视频播放器的区别为例：视频以记录信息为目的，故其属于信息类数据；但视频播放器只是用来播放视频的应用程序，若没有视频，则视频播放器内不存在任何信息，因此视频播放器属于功能性数据。

长期以来，实务中司法机关从未注意信息类数据与功能性数据的差异，这是导致数据犯罪罪名认定混乱的重要原因。在过去的刑事司法实践中，通常将非法获取计算机信息系统数据罪和破坏计算机信息系统罪的第二款称为“数据犯罪”。笔者通过分析北大法宝网搜索到的最终被判处非法获取计算机信息系统数据罪的808份刑事判决书和最终被判定为破坏计算机信息系统罪第二款行为的刑事判决书，系统考察了司法实践中行为人所非法获取、增加、修改、删除的“数据”类型，并依据本文提出的标准进行归类。

其中，个人手机号码、身份认证信息等数据属于个人信息，购物订单、快递信息等数据属于经营信息，车牌选号信息、违章信息等数据属于政府管理信息，视频资源数据属于视频内容信息，工程图纸、设备研发文件等属于商业秘密信息，教材等数据属于作品信息，考试成绩数据属于考生考试成绩凭证信息，购物评价、网络帖子等数据属于网络用户发布的留言信息，以上数据应被归入信息类数据。

除此之外，游戏币、装备等虚拟财产是具有赋予网络用户某些特定权限（如购买服务、增强游戏角色能力）功能的代码，比特币等电子货币是具有交易凭证功能的代码，^①网络域名是具有在网站浏览器中跳转到相应网页功能的代码，应用程序源代码是具有创建和运行应用程序功能的代码，网络服务数据是具有将计算机连接到互联网功能的代码，服务器数据是具有向其他计算机信息系统提供服务功能的代码，以上数据应被归入功能性数据。

有观点认为，有几类数据兼具信息性与功能性，但只要抓住这些数据的本质属性，就会发现这些数据都能被归入其中一类。例如，有的游戏装备除具有赋予玩家特权的功能外，其在游戏中呈现出的外观、动画也属于信息。但事实上，“游戏装备数据”与“游戏装备的外观、动画数据”本质上是两类数据，前者为游戏运营商中的程序工程师通过编程设定的触发游戏中某种权限的指令，而后者则是由游戏运营商中的美术设计师通过绘画、3D建模等方法创作出的美术、动画作品，前者是功能性数据，后者是信息类数据，二者相结合才能带给玩家完整的游戏体验，但二者不应混为一谈。又如，非同质化代币（NFT）数据不仅可以记录信息，而且可以借助区块链和智能合约赋予自己一个不可复制、不可篡改的身份认证信息，即赋予该数据唯一性，以实现对数字艺术品、商品等资产的确权与交易。但是，我们并不能说，非同质化代币数据具有赋予自身唯一性的功能，而是因为其在记录信息的同时通过区块链和智能合约记录了自己的所有权信息，该所有权信息赋予了非同质化代币数据唯一性。因此，非同质化代币本质上是一种信息类数据。

三、数据法益之识别

明确了数据的概念及其与信息的关系，也就决定了数据法益的识别方法。法益是区分罪与非罪、此罪与彼罪的关键要素，因此准确识别“数据法益”对于数据犯罪的认定有着重要意义。当数据概念覆盖信息概念时，数据法益就会覆盖信息法益，导致司法实践中出现对信息法益评价不充分的问题。当前刑法学界多数学者认为，数据是信息的载体，载体具有脱离其记录的信息之外的独立的法益，即数据的保密性、完整性、可用性，并且与信息所涉法益构成“双层法益”。^{[15-17][19]}与之相反，也有少数学者反对数据具有值得刑法独立保护的法益，认为数据的保密性、完整性和可用性只是技术概念，不能直接拿来当作法益，数据的价值在于信息，数据犯罪的法益应以数据所表征的信息为中心来判断。^[20]笔者认为，上述观点均

^① 本文所称“虚拟财产”是指由网络平台自行发行和管理，虽需用法定货币购买但仅限于购买发行方服务，不可直接提现为法定货币的财产，如Q币、游戏币、游戏装备等，不包括比特币等可以与法定货币相互转化的去中心化“电子货币”。

未注意到数据与信息的交叉关系,忽视了信息类数据和功能性数据的差异,因此均存在局限性。信息类数据的法益应为所记录的信息所涉法益,功能性数据的法益则是其本身的保密性、完整性和可用性。

(一)信息类数据之法益

“法益必须与利益相关联,利益是能够满足人们需要的东西。”^[21]可见,法益的本质是人的现实利益,刑法保护虚拟数据权利的根本目的是保护公民的现实利益,但信息类数据只是信息的载体,在不转化为信息的情况下并不会直接与某种现实利益相关联,原因如下。

其一,信息类数据的保密性完全为信息的保密性而存在,数据技术具有保密性不能证明数据具有保密性。信息的保密性与利益息息相关,如公民个人信息的泄露会使得公民的隐私权受到侵犯,又如企业商业秘密的泄露会使得企业的预期经济利益即财产权受到侵犯。但当信息类数据所记录的信息不值得保密或无法转化为信息时,例如信息类数据所记录的是公开的信息,或行为人获取信息类数据后由于技术原因而不可能获取其中的信息,那么即使未经授权者非法获取到这些信息类数据,也不可能侵犯任何利益。在晟品公司非法获取计算机信息系统数据案^①中,被告晟品公司采用技术手段破解字节跳动公司的防抓取措施,使用网络爬虫抓取字节跳动公司已公开的视频数据。法院认为,信息公开并不代表数据公开,被害单位允许用户通过观看视频获取视频信息,但并未允许用户通过下载视频获取这些视频的数据,这些视频数据包含着被侵权单位的技术,具有独立价值。最终,法院判处被告的行为构成非法获取计算机信息系统数据罪。^[22]该判决引起了刑法学界很大的争议,许多学者认为爬取公开数据不应构成犯罪。^[23-24]笔者认为,法院对本案中视频数据独立价值的论证并不具有说服力。针对信息类数据作为信息载体本身的技术价值的问题,应当承认数据技术确实具有独立价值,在数据加密、存储等方面具有独创性的技术本身是一种知识产权,具有保密性,但这并不能推理得出任何包含数据技术的数据都具有保密性,因为技术与技术的产物是两码事。比如独创的冰箱制冷技术是一种知识产权,具有保密性,但我们显然不能说包含该技术的冰箱具有保密性。回到本案中,即使行为人通过爬取的代码剽窃被害单位的数据技术并利用该技术获利,也只是侵犯了数据技术的保密性,而不能说侵犯了数据的保密性。归根到底,本案中法官并没有准确认定被害单位的何种利益遭受了侵害。显然,被害单位不可能仅仅因为拥有这些二进制代码感到欢欣鼓舞。^[25]本案中被害单位所受到的利益损失在于,原本只能通过被害单位开发的应用程序观看的视频,可以脱离该应用程序观看,这可能导致用户流失,进而影响广告收入等财产利益。也即,本案中视频数据的价值仅仅在于用来播放视频以吸引网络用户。可见,本案中的信息类数据只有转化为信息才可能为数据权利人带来利益。

其二,信息类数据的完整性和可用性归根到底是为了保障数据权利人使用完整信息的权利。因为破坏本来就已损坏的信息类数据,或破坏某信息类数据的副本,对数据权利人不可能造成任何利益损失,显然不构成犯罪。在前述李骏杰等破坏计算机信息系统案中,检察院认为,侵入评价系统删改购物评价,其实质是对计算机信息系统内存储的数据进行非法删除、修改操作的行为,导致网站商品评价功能无法正常运转,侵害了购物网站所属公司的信息系统安全和消费者的知情权。笔者认为,本案中的检察院也没有准确定位遭到侵犯的利益究竟为何。本案中购物网站受到的损害在于,行为人删改差评的行为,将导致未购买该商品的用户看不到差评,以为该商品口碑很好,结果买到劣质商品,由此对购物网站的商品评价机制产生不信任,最终导致购物网站的用户减少,影响购物网站的财产利益。假如行为人删除的全是空白的购物评价,则没有任何利益遭到损害。可见,购物评价数据的核心价值就在于买家对特定商品的评价信息可供买家参考。

由此可见,信息类数据的保密性、完整性、可用性只是行为与法益之间的一个中间概念。司法实践中,行为人针对信息类数据的非法获取或破坏行为,通常是为达到非法获取或破坏信息目的而实施的手

① 参见北京市海淀区人民法院(2017)京0108刑初2384号刑事判决书。

段行为。^[26]因此,信息类数据的法益应为所记录的信息所涉法益,如经济利益、个人信息、知识产权等。

(二)功能性数据之法益

功能性数据不记录信息,它的价值在于其自身功能的发挥给人们带来的现实利益。非法获取数据权利人不愿意共享的功能性数据的行为会侵害权利人通过该数据的功能获取价值的独享性;破坏功能性数据的行为则会直接阻碍数据所有人通过该数据的功能获取价值。因此,功能性数据的法益是其本身的保密性、完整性和可用性。下面借助典型案例来具体阐释功能性数据与功能性数据法益之间的关系。

以晟品公司非法获取计算机信息系统数据案为例。如前所述,视频是信息类数据,视频播放器是功能性数据。故本案中被害单位所拥有的视频数据是信息类数据,而被害单位服务器中用于运行视频播放器的计算机代码则属于功能性数据,具有法律保护的价值。假设有行为人侵入被害单位的服务器,复制其中用于运行视频播放器的代码并用于自己开发应用程序,则属于侵犯功能性数据本身的保密性。

再以前述李骏杰等破坏计算机信息系统案为例,其中购物评价属于网络用户发布留言信息的记录,是信息类数据,而购物网站服务器中用于商品评价的计算机代码则属于功能性数据,其本身的可用性和完整性具有值得法律保护的价值。假设有行为人侵入购物网站的服务器,删除其中运行商品评价功能的程序,使得购物网站的所有用户都无法查看也无法发布购物评价,则属于直接破坏功能性数据本身的可用性和完整性。

综上所述,信息类数据本身不与任何有价值的利益相关联,值得保护的仅为其所记录的信息所涉法益,而功能性数据的法益为其本身的保密性、可用性和完整性,但功能性数据又不记录任何信息,不存在“第二层法益”。这显示出,信息类数据和功能性数据都只包含单层法益,当前受到广泛欢迎的“数据—信息双层法益”理论存在漏洞。

四、数据犯罪司法认定之类型化处理

对法益的识别方法,决定了对侵犯法益行为的认定方法。若忽视信息法益,就会导致“一刀切”“口袋罪”的问题。而基于双层法益理论,许多学者认为,应当在将数据犯罪认定为非法获取计算机信息系统数据罪或破坏计算机信息系统罪的同时,认定其构成与侵犯公民个人信息罪、侵犯商业秘密罪等信息犯罪的想象竞合。^{[15][19]}还有学者认为,数据犯罪是信息犯罪的兜底罪名。^{[16][26]}另有学者认为,数据犯罪是信息犯罪的前置化。^[27]笔者认为,双层法益理论没有注意到信息类数据的法益完全依赖于所记录的信息,并且忽视了不记录信息的功能性数据,缺乏类型化思维,因此存在较大的局限性。应将数据犯罪区分为信息类数据犯罪和功能性数据犯罪,并进行类型化处理,方能使司法实践中的疑难问题得到妥当解决。

(一)数据犯罪之类型化认定规则

如前所述,大数据时代明确界分“数据”与“信息”概念已无必要,但刑法理论与实务界仍执着于区分数据与信息、数据法益与信息法益、数据犯罪与信息犯罪,根源在于仍将数据犯罪局限于非法获取计算机信息系统数据罪和破坏计算机信息系统罪两个罪名,进而认为“数据法益”仅指该两个罪名的保护法益。

首先,将数据犯罪局限于前述两罪名,正是导致司法实践中前述两罪名“口袋化”的直接原因。例如,盗窃他人电子版设计图纸、设备研发文件等商业秘密的行为,在司法实践中通常被认定为非法获取计算机信息系统数据罪,但该罪名显然无法准确评价该类行为的法益侵害性,因为该类行为应构成侵犯商业秘密罪。

其次,数据犯罪应包括所有以数据为对象的犯罪行为。如前所述,数据并非仅指记录信息的计算机代码,还包括不记录信息的功能性数据,以及以纸质文件等其他方式记录的某些信息。例如,同样一份记录着50条以上个人财产信息的数据,行为人可以使用U盘或网络窃取,也可以将其打印或抄写在纸上偷走。这两种行为最终侵犯的法益都是公民个人信息的保密性,在法益侵害性即犯罪本质上没有区别,故二者均为数据犯罪,但非法获取纸质的个人信息数据不可能构成计算机犯罪罪名,只可能构成侵犯公民

个人信息罪,这说明数据犯罪也包括侵犯公民个人信息罪等其他罪名。

最后,应将数据犯罪分为信息类数据犯罪和功能性数据犯罪进行类型化认定。其一,对信息类数据犯罪应根据行为所侵犯的信息所涉法益决定构成何罪名,因为信息类数据的法益完全依赖于其所记录的信息。此外,因为非法获取计算机信息系统数据罪和破坏计算机信息系统罪是侵害数据本身的法益犯罪,而信息类数据的法益不在数据本身,侵犯信息类数据的行为只是为达成侵犯信息目的的手段,所以信息类数据犯罪不能被认定为上述两罪名。其二,《刑法》第285条第2款和第286条第2款中的“数据”,应仅指功能性数据,因为功能性数据的法益才涉及保密性、可用性和完整性。值得注意的是,功能性数据犯罪并非一律认定为上述两罪名,对功能性数据犯罪应根据所侵犯的功能性数据的具体功能决定构成何罪名。例如,比特币等电子货币是一种特殊的代码,其功能是作为一种交易凭证,其本质属性是财产,因此侵犯电子货币的保密性、可用性和完整性的行为,本质上是窃取公私财物,应定为盗窃罪。^[28]

(二)数据犯罪类型化认定规则之实践展开

将数据犯罪区分为信息类数据犯罪和功能性数据犯罪进行类型化认定,可以更好地解决司法实践中的数据犯罪疑难案件中的刑法适用难题。本文以修改、增加、删除信息类数据和盗窃虚拟财产案件为例进行分析。

1. 增加、修改、删除信息类数据案件

该类案件是破坏计算机信息系统罪“口袋化”的典型案件,原因在于司法实践中将改变计算机信息系统内任何内容的行为都认定为第286条第2款中的破坏计算机信息系统数据行为。若采用本文所提倡的类型化认定规则,首先认定案件中出现数据的类型,其次根据数据类型认定数据法益,最后就能清晰地认定该类案件中的行为所构成的罪名。

以李骏杰等破坏计算机信息系统案为例。首先,购物评价属于信息类数据,应根据数据所记录信息所涉法益来认定犯罪,但购物评价信息并不涉及刑法上的法益,因此不应将行为人删除购物评价的行为作为犯罪处理。其次,行为人从他人处购买的买家个人信息数据属于信息类数据,所记录的个人信息可能涉及个人信息法益,行为人的行为可能构成侵犯公民个人信息罪,但由于这些个人信息的性质和数量未达到2017年最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第5条所规定的入罪标准,因此本案中行为人的行为不构成侵犯公民个人信息罪。最后,由于本案中不存在对功能性数据的侵犯,所以案涉行为不构成破坏计算机信息系统罪。综上,案涉行为不构成犯罪。

再以前述马某梅、谢某琴等破坏计算机信息系统案为例。其中,本案行为人所非法增加的“学员考试成绩数据”属于信息类数据,所记录的考试成绩信息可能涉及考试公平法益,行为人的行为可能构成代替考试罪,但是本案中的考试“江苏省应急管理厅委托泰州市应急管理局所组织的特种行业考试”不属于《刑法》第284条规定的“法律规定的国家考试”,因此行为人的行为不构成代替考试罪。此外,由于本案中不存在对功能性数据的侵犯,案涉行为不构成破坏计算机信息系统罪。综上所述,案涉行为不构成犯罪。

2. 盗窃虚拟财产案件

盗窃虚拟财产行为如何定罪,一直是刑法学界的疑难问题,实践中司法机关的观点不一,学界对司法判决也提出了许多质疑。原因在于虚拟财产同时具有实质上的财产属性和形式上的计算机代码属性,但这导致虚拟财产的法益是应由其财产属性决定还是由其计算机代码属性决定这一问题陷入两难境地。2014年最高人民法院研究室认为,该行为宜以非法获取计算机信息系统数据罪定罪处罚,主要原因有:其一,虚拟财产的本质是电磁记录,不能进行交易;其二,虚拟财产的价值依赖于运营商的控制,难以鉴

定。^①但近年来包括陈兴良、张明楷教授在内的多数刑法学者都认为,该行为应认定为财产犯罪,主要原因有:其一,虚拟财产具有排他的支配性,不能因载体否定其财产性;^[29]其二,非法获取虚拟财产数额巨大的,可能造成被害人特别巨大的财产损失,而认定为非法获取计算机信息系统数据罪将导致罪责刑不相适应。^[30]

上述两种观点都有其道理,但问题在于,法官和学者没有注意到盗窃虚拟财产案件在司法实践中表现出的两种本质不同的行为类型。一种是针对网络运营商的盗窃行为,在实践中体现为侵入运营商的服务器更改用户的虚拟财产数额的行为;另一种是针对网络用户的盗窃行为,在实践中体现为先盗取用户账户,然后将虚拟财产转移到其他账户,或直接修改密码后将账户交易给他人的行为。上述两种观点分别只分析了其中一种行为类型。

面对该类案件复杂的行为类型,只要采取本文所提倡的类型化认定规则,就能很清晰地认定该类案件中的行为所构成的罪名。如前所述,虚拟财产是用于赋予用户使用某些特定功能(如购买服务、增强游戏角色能力)权限的代码,应属于功能性数据。因此,应根据所侵犯的功能性数据的具体功能决定行为构成何罪名。而虚拟财产的具体功能恰恰是因人而异的。

首先,对于运营商而言,虚拟财产的功能是通过调控虚拟财产的价值,并根据用户的使用或消费情况,调整用户所持有的虚拟财产的数额,以维持稳定的网络服务环境,并借此吸引更多用户和消费。然而,如果有用户侵入运营商的服务器,随意修改虚拟财产余额,则会导致越来越多的人不得愿再通过消费而是通过非法手段获取网络服务,破坏网络服务环境的稳定性,最终引起用户流失,影响运营商的经济利益。正因如此,运营商通常都会对服务器采取严格的加密和安全防护措施。

其次,对于用户而言,虚拟财产的功能是购买服务和交易,目前我国虚拟财产的交易市场已经具有相当大的规模,大部分虚拟财产已经形成相对稳定的市场价格。^[30]在孟动等盗窃案中,法院认为,用户以支付真实货币的方式购买虚拟财产后,就能得到发行公司提供的等值服务,这体现着发行公司提供服务的劳动价值。因此,虚拟财产也代表着购买者在现实生活中实际享有的财产,应当受刑法保护。^②

最后,“法益的价值是与法益的主体密切关联的”^[30],虚拟财产对于运营商和用户而言功能不同,这决定了二者对于虚拟财产的法益也不同,因此窃取不同主体虚拟财产的行为所构成的罪名也不同。对于运营商而言,最重要的是防止他人非法获取虚拟财产,此时需要保护的法益是虚拟财产的保密性,侵入运营商的服务器更改用户的虚拟财产数额,情节严重的,应认定为非法获取计算机信息系统数据罪;同时,虚拟财产并不具有消耗性,运营商可通过服务器随时、随意生成无数虚拟财产,或更改虚拟财产的价值以及任何用户虚拟财产余额,即使行为人通过侵入服务器的手段非法获取数额特别巨大的虚拟财产,运营商也并不会受到直接财产损失,因此对于运营商而言虚拟财产不具有财产属性,侵入运营商的服务器更改用户虚拟财产数额的行为,并不会使运营商的财产法益受到损害,不宜认定为盗窃罪。而对于网络用户而言,虚拟财产的功能是消费和交易,具有财产属性,虚拟财产的损失与现实财产的损失没有区别,因此虚拟财产的法益是财产法益,盗取用户账户后,在游戏中将虚拟财产转移给其他账户,或直接修改密码后将账户交易给他人的,符合《刑法》第264条规定,应认定为盗窃罪。

五、结语

针对数据犯罪的认定,过往司法实践中存在的只要涉及数据就“一刀切”式地以非法获取计算机信息系统数据罪和破坏计算机信息系统罪来定性的现象,会导致对数据的内容和价值评价不充分,应当予以摒弃。但当前理论界所推崇的“双层法益理论”,本质上是为了回避数据与信息的法益区分这一疑难问

① 参见2014年4月22日《最高人民法院研究室关于利用计算机窃取他人游戏币非法销售获利如何定性问题的研究意见》。

② 参见上海市黄浦区人民法院(2006)黄刑初字第186号刑事判决书。

题,直接以想象竞合或数罪并罚来处理,但论者既无法证明信息类数据除了其记录的信息外还有什么独立的价值,也无法解释不记录任何信息的功能性数据除了其本身的保密性、完整性、可用性之外还存在何种“第二层法益”,可以说该理论是存在漏洞的。当前,只有区分信息类数据和功能性数据的类型化方法论,才能实现对实践中的数据犯罪案件的较为合理的认定。这种方法论首先要对实践中多种多样的数据类型进行准确认定,其次还要对信息类数据记录的信息所涉法益和功能性数据的功能对应着何种法益进行分析,为司法人员带来了更大的工作量。但数据技术以及现实中的数据犯罪案件本来就是复杂、困难的,因此期望通过“一刀切”或“规避”的方法来解决复杂、困难的问题是不可取的。

参考文献:

- [1] 刘宪权. 元宇宙空间中数据的分类分级与刑法保护[J]. 比较法研究, 2023(4): 51-64.
- [2] 于志刚, 李源粒. 大数据时代数据犯罪的制裁思路[J]. 中国社会科学, 2014(10): 100-120.
- [3] 梅夏英. 数据的法律属性及其民法定位[J]. 中国社会科学, 2016(9): 164-183+209.
- [4] 程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122+207-208.
- [5] 王倩云. 人工智能背景下数据安全犯罪的刑法规制思路[J]. 法学论坛, 2019(2): 27-36.
- [6] 赖早兴. 论刑法中的数据: 概念、文本与实践[J]. 政治与法律, 2024(6): 64-82.
- [7] 郭旨龙. 非法获取计算机信息系统数据罪的规范结构与罪名功能——基于案例与比较法的反思[J]. 政治与法律, 2021(1): 64-76+63.
- [8] 杨志琼. 非法获取计算机信息系统数据罪“口袋化”的实证分析及其处理路径[J]. 法学评论, 2018(6): 163-174.
- [9] 周立波. 破坏计算机信息系统罪司法实践分析与刑法规范调适——基于100个司法判例的实证考察[J]. 法治研究, 2018(4): 67-76.
- [10] 纪海龙. 数据的私法定位与保护[J]. 法学研究, 2018(6): 72-91.
- [11] 李爱君. 数据权利属性与法律特征[J]. 东方法学, 2018(3): 64-74.
- [12] 李凤梅. 个人数据权利刑法保护的立场选择及实现路径[J]. 法商研究, 2021(6): 46-60.
- [13] 祝振媛, 李广建. “数据—信息—知识”整体视角下的知识融合初探——数据融合、信息融合、知识融合的关联与比较[J]. 情报理论与实践, 2017(2): 12-18.
- [14] 张平. 中华人民共和国数据安全法理解适用与案例解读[M]. 北京: 中国法制出版社, 2021: 9.
- [15] 陆一敏. 数据安全新型法益的建构——基于数据与信息的双向关系[J]. 苏州大学学报(哲学社会科学版), 2023(4): 77-87.
- [16] 欧阳本祺. 论数据犯罪的双层法益[J]. 当代法学, 2023(6): 64-74.
- [17] 李怀胜. 数据安全的法益变迁与刑法规制[J]. 江西社会科学, 2023(7): 33-44.
- [18] 龙卫球. 中华人民共和国数据安全法释义[M]. 北京: 中国法制出版社, 2021: 7.
- [19] 庄劲. 开放的中国数据刑法体系之建构——基于本体法益与功能法益的区分[J]. 中国刑事法杂志, 2023(2): 37-53.
- [20] 赵春玉. 大数据时代数据犯罪的法益保护: 技术悖论、功能回归与体系建构[J]. 法律科学(西北政法大学学报), 2023(1): 95-107.
- [21] 张明楷. 刑法学(第六版)[M]. 北京: 法律出版社, 2021: 77.
- [22] 游涛, 计莉卉. 使用网络爬虫获取数据行为的刑事责任认定——以“晟品公司”非法获取计算机信息系统数据罪为视角[J]. 法律适用, 2019(10): 3-10.
- [23] 孙禹. 强行爬取公开数据构成犯罪吗[J]. 国家检察官学院学报, 2021(6): 121-139.
- [24] 石经海, 苏桑妮. 爬取公开数据行为的刑法规制误区与匡正——从全国首例“爬虫”入刑案切入[J]. 北京理工大学学报(社会科学版), 2021(4): 154-164+172.
- [25] 黎森予. “数据犯罪”概念的否定与化归[J]. 南大法学, 2024(4): 30-47.
- [26] 姚瑶. 非法获取计算机信息系统数据罪的限缩适用——兼论数据犯罪的法益侵害[J]. 华东政法大学学报, 2024(2): 94-106.
- [27] 姚万勤. 信息视角下数据犯罪的前置化定位及其立法边界[J]. 政治与法律, 2024(5): 49-62.

- [28] 赖早兴. 加密资产刑事案件: 样态、种类、问题及解决——基于 551 份刑事判决的分析[J]. 经贸法律评论, 2022(4): 72-95.
- [29] 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.
- [30] 张明楷. 非法获取虚拟财产的行为性质[J]. 法学, 2015(3): 12-25.

The Puzzle of Judicial Determination of Data Crime and Its Solution

CHENG Jiaying

(Law School, Xiangtan University, Xiangtan, Hunan 411105, China)

Abstract: There exists a puzzle of “pocketization” of the crime name in the judicial determination of data crime in our country. The reason lies in the generalization of the concept of “data” in judicial practice and the confusion between data interests and information interests. Data and information are in an overlapping relationship. “Data” should be defined as numerical information, which are stored, processed and transmitted in binary codes within computer information systems, and obtained through scientific experiments, tests, statistics, calculations, etc. which are recorded in other forms, and used for scientific research, technical design, verification, decision-making, etc. Data includes “informational data” and “functional data”. The legal interests of informational data should be the legal interests involved in the recorded information, while the legal interests of functional data lie in its own confidentiality, integrity and availability. Data crime should not be limited to the crime of illegally obtaining data in computer information systems and the crime of destroying computer information systems, but should include all crimes with data as the object. A typological approach should be adopted for data crime. For informational data crime, the crime should be determined based on the legal interests involved in the information that the behavior infringes upon. For functional data crime, the crime should be determined based on the specific function of the functional data that the behavior infringes upon.

Key words: data crime; legal interests of data; informational data; functional data

(责任编辑: 董兴佩)