理论前沿

我国数据犯罪的司法困境与出路：以数据安全法益为中心

杨志琼

内容提要：通过对我国数据犯罪的判决梳理可发现，当前数据法益定位不清，引发了数据犯罪的解释难题和界分难题。究其原因，立法独立性上的“先天不足”和后天技术识别障碍叠加，导致数据犯罪保护法益及其规范体系被传统计算机犯罪体系所遮蔽，难以消弭数据犯罪中技术评价与规范评价的分歧，无法应对不断更新的数字化犯罪技术。大数据时代，由数据保密性、完整性、可用性需求组成的数据安全法益（CIA）应成为我国数据犯罪的独立保护法益，以确保从数据自身内容、使用价值和侵害风险等角度对数据犯罪进行独立规范评价。未来数据犯罪的司法适用应跳脱出传统计算机犯罪体系，以数据安全法益的解释功能重释数据犯罪的构成要件，推动数据犯罪规范体系与技术规则的深度融合；以数据安全法益的界分功能明确数据犯罪与其他计算机犯罪、传统犯罪的区别，合理确定数据犯罪的适用边界。

关键词：数据犯罪　数据安全　解释功能　界分功能

杨志琼，东南大学法学院讲师。

近年来，国内首起“流量劫持案”、〔1〕首起“制售微信外挂软件案”、〔2〕首起“干扰环保监测系统案”、〔3〕首起“获取微信公众号案”、〔4〕首起“撞库打码案”、〔5〕首起“利用‘爬虫’技术抓取数据案”〔6〕等相继发生，数字化犯罪技术引发的数据安全风险触目惊心，技术识别难题也令司法人员无所适从，一直以来栖身于计算机犯罪之中的数据犯罪开始引

〔1〕 参见上海市浦东区人民法院（2015）浦刑初第1460号刑事判决书。
〔2〕 参见广东省广州市海珠区人民法院（2016）粤0105刑初1040－1号刑事判决书。
〔3〕 参见陕西省西安市中级人民法院（2016）陕01刑初第233号刑事判决书。
〔4〕 参见广东省广州市珠海区人民法院（2017）粤0105刑初第39号刑事判决书。
〔5〕 参见浙江省杭州市余杭区人民法院（2017）浙0110刑初664号刑事判决书。
〔6〕 参见北京市海淀区人民法院（2017）京0108刑初2384号刑事判决书。

起学界关注。但已有研究主要采用规范分析方法,从立法论角度对数据犯罪提出体系化建构,〔7〕缺乏对我国数据犯罪实践面相的整体把握和对典型判例的具体梳理,难以消弭新型数据犯罪中技术评价与规范评价的分歧并妥当地指导司法实践。2019 年 5 月 28 日,国家互联网信息办公室就数据搜集、处理、使用、监管等安全问题发布了《数据安全管理办法(征求意见稿)》,再次将数据安全防范上升至国家战略高度。如何在大数据时代基于我国数据犯罪的实践现状,明确我国数据犯罪的法益侵害实质,并推动数据犯罪规范体系与技术规则的深度融合以应对不断更新的数字化犯罪技术,是当前我国数据犯罪亟需解决的难题。

一 我国数据犯罪的司法困境及其成因

本文所称的数据犯罪,是指以数据为对象的非法获取、删除、修改、增加等行为,主要包括我国《刑法》第 285 条第 2 款非法获取计算机信息系统数据罪(以下简称获取型数据犯罪)和第 286 条破坏计算机信息系统罪第 2 款删除、修改、增加数据之规定(以下简称破坏型数据犯罪)。本文对中国裁判文书网上所收集的数据犯罪判决书进行了系统梳理,以期全面、深刻地把握当前我国数据犯罪的真实面貌。在中国裁判文书网上以“非法获取计算机信息系统数据罪”“破坏计算机信息系统数据罪”为关键词,案件类型选择“刑事案件”,获得非法获取计算机信息系统数据罪的有效判决样本 475 份,获取破坏计算机信息系统罪中关于数据犯罪的有效判决样本 226 份。其中,获得非法获取计算机信息系统数据罪的判决样本共 795 份,包括 539 份刑事判决书和 256 份刑事裁定书。其中刑事裁定书主要是关于该罪减刑、假释等情况,不在本文的研究范围之内。在剩余的 539 份刑事判决书中,排除与该罪无关的判决书 64 份,共获得有效判决书 475 份。获得破坏计算机信息系统罪判决样本 1036 份,包括 733 份刑事判决书和 288 份刑事裁定书、3 份调解书、12 份决定书。其中刑事裁定书、调解书、决定书主要是关于该罪的减刑、假释、管辖权、驳回再审请求等情况,不在本文研究范围之内。在剩余的 733 份刑事判决书中,排除有关《刑法》第 286 条第 1 款与第 3 款的判决书 507 份,获得破坏型数据犯罪的有效判决书共 226 份。通过对上述判决书的整理可发现当前我国数据犯罪在司法适用中存在诸多问题。

(一)当前我国数据犯罪的司法困境

1. 数据犯罪中“数据”的范围日益“口袋化”

我国《刑法》将数据犯罪中的“数据”限定为“计算机信息系统中存储、处理或者传输的数据”。但从所收集的判决书来看,数据犯罪中的“数据”事实上包括了所有能以代码形式储存于计算机信息系统中的权利客体,具体有以下几类。(1)以电子数据方式记录

〔7〕 参见于志刚、李源粒:《大数据时代数据犯罪的制裁思路》,《中国社会科学》2014 年第 10 期,第 116 – 118 页;于志刚、李源粒:《大数据时代数据犯罪的类型化与制裁思路》,《政治与法律》2016 年第 9 期,第 25 – 27 页;孙道萃:《网络刑法知识转型与立法回应》,《现代法学》2017 年第 1 期,第 127 – 128 页;王倩云:《人工智能背景下数据安全犯罪的刑法规制思路》,《法学论坛》2019 年第 2 期,第 35 – 36 页。

的公民个人信息,如考生信息、学籍管理信息、人才信息、评标专家信息、违法犯罪记录、驾驶证信息、户口信息等;(2)身份认证信息,如淘宝购物账号密码、网络游戏账号密码、微信账号密码、wifi 账号密码、苹果手机 APP 账号密码等。(3)网络虚拟财产,如网络游戏装备、网络游戏道具等物品类虚拟财产和 Q 币、金币等货币类虚拟财产;(4)网络知识产权,如游戏源代码、网络课堂教学视频资料、公司的设计图纸等网络著作权、商业秘密等;(5)财产性利益,即以数据形式储存于电脑系统之中又具有经济价值的网络积分、手机靓号、电信资费套餐、会员卡资金等;(6)普通数据产品,如医院用药统方数据、客户订单数据、考试成绩、考试志愿、环保监测数据、生产经营数据等。这种广义的"数据"范畴使数据犯罪呈现出不同种类和不同程度的法益侵害,涉及个人信息权、财产权、知识产权等权利,数据犯罪保护法益的内涵和外延极其模糊。

2. 数据犯罪的构成要件解释缺乏独立标准

我国数据犯罪在体系上隶属于《刑法》第 285 条和第 286 条所规定的计算机犯罪范畴,保护法益也受制于"计算机信息系统安全",导致数据犯罪构成要件解释始终受制于计算机犯罪。第一,对"数据"的判断依附于"计算机信息系统"的判断。多数判决书对"数据"的认定停留于"计算机信息系统中储存、处理、传输的数据",而未能详细阐述"数据"的实质内容。而对移动智能终端、APP 应用软件、蓝牙等设备中储存、处理、传输的新型"数据"的判断,则又被置换为对"计算机信息系统"的判断而掏空了"数据"的实体判断。如在全国首例非法获取微信公众号案件中,被告人林某等制作了钓鱼链接并登陆至微信公众平台,以被侵权为由向其它微信公众号进行投诉,在投诉描述中植入钓鱼链接,诱骗微信公众号运营者点击登录并查看投诉内容,从而在后台窃取他人微信公众号的账号及密码等共计 715 组。[8] 实务界花费了大量精力来讨论微信是否"计算机信息系统"以证成微信公众号账号密码是"计算机信息系统中储存、处理、传输的数据"。[9] 第二,对数据的侵害行为与对计算机信息系统的侵害行为难以区分。数字化犯罪技术快速更新增加了数据犯罪的技术认定难度,尤其是对计算机信息系统的非法侵入、非法控制或破坏必须通过对数据的删除、修改、增加来完成,引发了数据犯罪与其他计算机犯罪罪名选择、行为定性等适用争议。如在全国首起"流量劫持案"、首起"制售微信外挂软件案"、首起"撞库打码案"中,都产生了上述行为的实质是"对数据的侵害"还是"对计算机信息系统功能的侵害"的争议。第三,对数据犯罪后果的判断受制于计算机信息系统功能是否受损害。对删除、修改、增加数据而未影响计算机信息系统功能的行为应否构成数据犯罪,实务中存在诸多争议,不少判例将影响计算机信息系统功能作为入罪标准。[10]

3. 数据犯罪普遍存在定性争议而边界模糊

"数据"表征权利客体的多样化使得获取、删除、修改、增加数据行为在形式上符合多

〔8〕 参见广东省广州市珠海区人民法院(2017)粤 0105 刑初第 39 号刑事判决书。

〔9〕 参见最高人民检察院法律政策研究室组织编写:《网络犯罪指导性案例实务指引》,中国检察出版社 2018 年版,第 206 - 209 页。

〔10〕 参见安徽省芜湖市中级人民法院(2015)芜中刑终字第 00304 号刑事判决书;辽宁省盘锦市大洼县人民法院(2017)辽 1104 刑初 123 号刑事判决书。

个罪名,检察机关、辩护人和法院基于不同司法立场在选择罪名时争议较大。以破坏计算机信息系统罪为例,有学者于 2018 年对所收集的 100 份破坏计算机信息系统罪判决书进行梳理,发现检察机关、辩护人和法院最终认定罪名之间出现过争议的案件有 56 个,比例约 56%。[11] 这主要表现在两个方面。第一,数据犯罪与传统犯罪的适用争议。即数据犯罪和《刑法》第 287 条利用计算机实施的传统犯罪之间的争议,主要包括:其一,数据犯罪与财产犯罪的争议。如盗窃网络虚拟财产、修改付款软件中的价格数据、修改电信资费套餐等,都是通过获取、修改数据来侵犯财产权,引发了数据犯罪与财产犯罪的法律适用争议。其二,数据犯罪与侵犯公民个人信息罪的适用争议。如非法获取考生信息、学籍管理信息、车辆登记信息等,以及删除消除违法犯罪记录、修改驾驶证记分信息、修改购房个人户口信息等,都是通过干扰数据来侵犯公民个人信息权,因而引发了数据犯罪相关罪名与侵犯公民个人信息罪的适用争议。其三,数据犯罪与侵犯知识产权犯罪的适用争议,如非法获取游戏源代码、商业秘密等,以及修改游戏源代码,究竟是认定为侵犯知识产权的专属罪名还是按照其犯罪手段认定为数据犯罪,[12] 也存在争议。第二,数据犯罪与《刑法》第 285 条、第 286 条规定的其他计算机犯罪之间适用争议。主要包括:一是数据犯罪与非法控制计算机罪适用争议。如在“流量劫持案”中,由于对“破坏”“控制”的规范评价不同,引发了破坏型数据犯罪与非法控制计算机信息系统罪的争议。[13] 二是数据犯罪与提供侵入、非法控制计算机信息系统程序、工具罪的争议。如在撞库打码案中,由于立法对数据犯罪帮助行为正犯化规定的不明晰,引发了获取型数据犯罪与提供侵入、非法控制计算机信息系统程序、工具罪之间的适用争议。[14]

(二)造成司法困境之成因:数据犯罪保护法益定位不清与功能缺位

数据犯罪的司法适用有赖于数据犯罪保护法益立法批判功能和解释适用功能的正常发挥。但从前述数据犯罪“内外交困”的司法窘境来看,数据犯罪保护法益的上述功能并未正常发挥,其原因在于以下几点。

1. 数据犯罪保护法益定位不清

随着数字化技术的迅猛发展,越来越多的权利客体都卸下物质载体这一“枷锁”,以数据的形式储存、传输和利用。受此影响,“数据”所表征的法益种类具有不同功能。第一,数据具有表征传统法益的媒介、工具功能。从各国数据犯罪的发展历史来看,数据犯罪首先侵害的是以数据形式表征的传统法益,如以电子数据方式记录的“可识别性”个人数据表征了个人信息权;以数据形式显示的财产性利益表征了财产权;以数据形式记载的“创造性”智力成果体现了知识产权等。第二,数据本身具有表征数据安全需求的对象功能。随着数字化技术的发展,数据利用渗透至生活的每一个角落,针对数

〔11〕 参见周立波:《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》,《法治研究》2018 年第 4 期,第 68 页。

〔12〕 “侵犯知识产权的专属罪名”主要是指我国刑法分则设立的四种特殊的知识产权罪名:著作权特殊罪名、商标权特殊罪名、专利权特殊罪名和商业秘密特殊罪名。参见于志强:《我国网络知识产权犯罪制裁体系检视与未来建构》,《中国法学》2014 年第 3 期,第 157 页。

〔13〕 参见孙道萃:《“流量劫持”的刑法规制及完善》,《中国检察官》2016 年第 4 期,第 77 页。

〔14〕 参见杨赞:《撞库打码牟利行为如何定性》,《人民检察》2018 年第 4 期,第 42 页。

据的窃取、篡改、破坏、扩散等行为日益增多,因而产生了针对数据自身安全的独立保护需求,特别是与数据的保密性、完整性和可用性相关的新利益。[15] 这迫使各国刑法保护防线前移,在计算机犯罪之外规定特别的数据犯罪。因此,可将数据犯罪分为两种:一种是以数据为媒介、工具侵犯传统法益的犯罪,其与传统犯罪的区别在于通过对数据载体的侵害来完成,是传统犯罪的数字化异化;另一种是以数据为对象侵害数据安全新生法益的犯罪,是随着数字化技术发展而产生的应对全新法益保护需求的犯罪类型。[16] "数据"的"口袋化"现象恰恰源于当前我国司法实务并未区分数据的对象功能和媒介、工具功能,而是将所有以数据为载体的法益侵害行为都涵盖进来,导致"数据"无所不包,其内涵和外延极不清晰。

2. 数据犯罪保护法益的解释功能缺位

数据犯罪保护法益具有指导数据犯罪构成要件解释适用的机能,但当前我国以计算机犯罪为中心的立法逻辑及司法解释导致该功能严重缺位。这主要源于以下两方面原因。一方面,数据犯罪保护法益存在立法独立性上的"先天不足"。我国计算机犯罪在立法之初就采取了设备、计算、数据三位一体的模式,即以计算能力为主要视角、兼有物理设备隐形视角、不彻底数据视角的混合模式,数据犯罪及其保护法益的独立地位并不显见。[17] 虽然删除、修改、增加数据的行为在立法之初就被规定在第 286 条第 2 款中,但无论在罪名设置还是在保护法益的解释上都受制于破坏计算机信息系统罪;非法获取计算机信息系统数据罪在《刑法修正案(七)》中始被增设,却又与非法控制计算机信息系统罪捆绑立法而未能真正独立。正是这种立法上的"先天不足"导致我国数据犯罪的解释适用长期受计算机犯罪的"裹挟"而难以获得独立判断。另一方面,相关司法解释未能增加数据犯罪保护法益的解释功效。数据犯罪的技术性极强且代际升级较快,但当前司法解释仍以计算机犯罪为中心,通过扩大"计算机信息系统安全"法益的涵摄范围,而非提出独立的数据犯罪保护法益来解决对数据犯罪的规制。如 2011 年 8 月 1 日最高人民法院、最高人民检察院联合颁发的《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》(以下简称《计算机安全解释》)通过扩大"计算机信息系统"来包容移动智能终端、APP 应用软件、蓝牙等新型数据载体,以扩大数据犯罪的处罚范围。而对于数据犯罪中"数据""获取""删除""修改""增加"等规范性构成要件要素,相关司法解释却始终未能结合独立的数据犯罪保护法益来加以说明。

3. 数据犯罪保护法益的界分功能缺位

数据犯罪保护法益具有区分数据犯罪与其他犯罪的界分功能,却在司法适用中严重缺位,导致数据犯罪普遍存在定性争议。究其原因,除前述立法独立性欠缺之外,还

〔15〕 参见[德]乌尔里希·齐白著:《全球风险社会与信息社会中的刑法》,周遵友、江溯等译,中国法制出版社 2012 年版,第 308 页。

〔16〕 参见杨志琼:《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》,《法学评论》2018 年第 6 期,第 167 页。

〔17〕 参见李源粒:《破坏计算机信息系统罪"网络化"转型中的规范结构透视》,《法学论坛》2019 年第 2 期,第 44 页。

由于立法和司法中规定和解释的诸多不足。第一,在立法层面表现为立法漏洞倒逼数据犯罪保护法益的多元化。由于刑法对以数据为载体的其他权利客体在保护种类或者保护行为上存在立法漏洞,导致数据犯罪沦为其他犯罪网络异化的“兜底条款”,倒逼数据犯罪保护法益内涵的多元化。如现有知识产权犯罪罪名体系不够完善,当侵害知识产权的目的行为没有具体罪名进行规制时,只能依据作为手段行为的数据犯罪来进行制裁,使数据犯罪保护法益涵盖了知识产权。[18] 此外,侵犯公民个人信息罪对侵害“个人信息”的行为方式只包括了非法获取、出售和提供,大量非法修改、删除个人重要信息的行为虽然也涉及对个人信息的实质化变动,却无法用侵犯公民个人信息罪处理,最后只能认定为破坏型数据犯罪,使数据犯罪保护法益涵盖了个人信息权。第二,在司法层面表现为司法惰性回避了数据犯罪保护法益的实质判断。数据犯罪的适用需要对“数据”进行技术属性判断和法律属性判断。技术属性判断只需认定是否存在“计算机信息系统中存储、处理、传输的数据”即可,而法律属性判断则需要仔细分析“数据”所表征的传统法益与新生法益。实务中司法人员基于司法惰性更青睐数据的技术属性判断而回避其法律属性判断。以网络虚拟财产为例,涉及对网络虚拟财产的法律属性判断(财产属性或数据属性的论证)和价值评估难题(虚拟财产犯罪数额的确定),实务中多数判例直接回避其法律属性判定难题,径行将盗窃虚拟财产的行为认定为非法获取计算机信息系统数据罪。[19]

综上可见,我国数据犯罪规制的实践难题源于立法独立性上的“先天不足”和后天数字化技术识别障碍,而其深层原因则在于数据犯罪保护法益定位不清,导致对数据犯罪的解释适用未能跳脱于“计算机信息系统安全”法益,数据犯罪规范体系最终为传统计算机犯罪体系所遮蔽。大数据时代数字化技术日新月异,数据犯罪的司法适用应挣脱计算机犯罪体系走向独立化道路,以积极回应司法实践需求。因此,下文将论述数据犯罪的独立保护法益内涵,并依其法益侵害实质来重释数据犯罪的规范体系。

二 数据犯罪的教义学基点:数据安全法益之提倡

对数据犯罪的深层次界定,“与其说体现为技术层面,不如说体现在其与现实世界受保护法益的联系上”。[20] 而当前我国数据犯罪的保护法益仍受制于传统计算机信息系统安全法益,既与数字化犯罪技术的实质不相吻合,也难以满足数据保护的社会利用需求,亟需调整。

(一)“计算机信息系统安全”法益的理解难题

我国数据犯罪栖身于《刑法》第 285 条和第 286 条的计算机犯罪之中,但传统观念认

〔18〕 参见于志强:《我国网络知识产权犯罪制裁体系检视与未来建构》,《中国法学》2014 年第 3 期,第 158 页。

〔19〕 参见浙江省临海市人民法院(2015)台临刑初字第 1155 号刑事判决书;广东省珠海市斗门区人民法院(2015)珠斗法刑初字第 119 号刑事判决书;山东省日照经济开发区人民法院(2016)鲁 1191 刑初 24 号刑事判决书。

〔20〕 于志刚、李源粒:《大数据时代数据犯罪的制裁思路》,《中国社会科学》2014 年第 10 期,第 105 页。

为《刑法》第285条和第286条是以计算机信息系统安全为保护法益,[21]因而不少学者依据体系解释将计算机信息系统安全视为数据犯罪的保护法益。[22] 1997年刑法规定计算机犯罪时的主流计算机信息技术以PC系统为主要载体,而随着新型移动终端(如智能手机、平板电脑、传感器和RFID等)的逐渐普及,"计算机信息系统"面临新的认定难题。此后,《计算机安全解释》不得不将"计算机信息系统""计算机系统"扩大解释为"具备自动处理数据功能的系统,包括计算机、网络设备、通信设备、自动化控制设备等",以回应实践需求。但无论是传统PC终端保护还是移动智能终端保护,都旨在保护计算机信息系统对数据的存储、处理、传输能力,以及计算机信息系统的运行过程安全。显然,保护"计算机信息系统安全"的目的在于保障计算机信息系统的处理数据功能能够安全运行,以使计算机信息系统能够正常地、符合操作人预期地完成数据处理需求。[23]

但是,从体系解释出发将"计算机信息系统安全"视为数据犯罪的保护法益并不合适,易导致数据犯罪沦为计算机犯罪的"附属品"而难以获得独立判断,并在技术评价与规范评价上产生分歧。

1."计算机信息系统安全"法益并不符合数据犯罪的技术实质和保护需求

因为"计算机信息系统安全"法益着重考虑特定计算机信息系统的应用主体和应用目标,其本质是动态地对数据的运算、传输、储存的过程,而"数据"则是静态地被计算机信息系统处理的对象,体现的是数据本身的安全需求。从计算机犯罪历史来看,在技术发展的早期,作为数据载体的计算机信息系统是主要的攻击对象,而在大数据时代,作为计算机信息系统"内容物"的数据则具备了更重要的价值,成为主要攻击对象。[24] 随着数字化技术的发展,数据与"计算机信息系统"这一载体的关系逐渐松弛,破坏计算机信息系统安全的行为并不必然同时侵害数据安全,反之亦然。因此,试图通过保护"计算机信息系统安全"来保护数据本身安全无异于"隔靴搔痒",甚至导致动态的计算机信息系统功能安全与静态的数据安全呈混淆状态而无法突出法益保护重点。

2."计算机信息系统安全"法益难以合理解释数据犯罪的构成要件并限定处罚范围

如果将计算机信息系统安全直接纳入数据犯罪的构成要件之中,会出现很多无法解决的问题。首先,这种观点将"数据"界定的着力点依附于"计算机信息系统",难以说明"数据"的实质内容。"数据"依附于"计算机信息系统"而得以存储、传输和处理,而前述对"计算机信息系统"的判断是以"具有数据处理功能"为关键,[25]这将导致"数据"与"计算机信息系统"成为相互解释、相互论证的对象、工具,在方法论上陷入循环论证而无法

〔21〕 参见高明暄著:《中华人民共和国刑法的孕育诞生和发展完善》,北京大学出版社2012年版,第513页;于志刚、于冲著:《网络犯罪的裁判经验与学理思辨》,中国法制出版社2013年版,第66页;孙道萃:《网络刑法知识转型与回应》,《现代法学》2017年第1期,第125页。

〔22〕 参见王作富主编:《刑法分则实务研究(中)》(第五版),中国方正出版社2013年版,第1075页;周道鸾、张军主编:《刑法罪名精释(下)》(第四版),人民法院出版社2013年版,第713-714页;俞小海:《破坏计算机信息系统罪之司法实践分析与规范含义重构》,《交大法学》2015年第3期,第150页。

〔23〕 参见王倩云:《人工智能背景下数据安全犯罪的刑法规制思路》,《法学论坛》2019年第2期,第33页。

〔24〕 参见王倩云:《人工智能背景下数据安全犯罪的刑法规制思路》,《法学论坛》2019年第2期,第31-33页。

〔25〕 参见王倩云:《人工智能背景下数据安全犯罪的刑法规制思路》,《法学论坛》2019年第2期,第31页。

最终说明“数据”的实质内涵。其次,这种解释方式将破坏计算机信息系统功能的行为与侵害数据安全的行为相混淆,导致数据犯罪与其他计算机犯罪难以区分。以流量劫持类案件为例,实务中存在破坏型数据犯罪与非法控制计算机信息系统罪的争议。如在全国首起“流量劫持案”中,被告人付宣豪、黄子超等人在 2013 年底至 2014 年 10 月间,租赁多台服务器,使用恶意代码修改互联网用户路由器的 DNS 设置,使用户登录“2345. com”等导航网站时跳转至其设置的“5w. com”导航网站,再将获取的互联网用户流量出售给“5w. com”导航网站,违法所得合计人民币 70 余万元。法院认为被告人通过修改路由器、浏览器设置等技术手段,强制网络用户访问指定网站的“DNS 劫持”,实质是对计算机信息系统中存储的数据进行修改、增加,应依据第 286 条第 2 款构成破坏计算机信息系统罪。而在全国第二例“流量劫持案”中,被告人施硕等共同利用职务便利,控制重庆某公司的互联网域名解析系统,致使用户在访问被劫持的网站时被强行跳转到另外的页面,或者致使在用户访问网站时,自动加入推广商的代码,实施 DNS 域名劫持或流量劫持。法院认为施硕等人违反国家规定,对计算机信息系统实施非法控制,应构成非法控制计算机信息系统罪。〔26〕 就构成要件而言,破坏型数据犯罪与非法控制计算机信息系统罪之间的界限比较清晰:前者强调对数据的删除、修改、增加侵害了数据内容本身的安全,但不要求造成计算机信息系统不能正常运行;后者强调通过技术手段使他人计算机信息系统处于自己掌控之下,侵害了他人计算机信息系统的正常运行。但以“计算机信息系统安全”为法益指导破坏型数据犯罪适用时,必然强调对数据的删除、修改、增加还必须同时影响计算机信息系统功能的正常运行,导致对数据的“破坏”与对计算机信息系统功能的“干扰”“控制”等行为概念发生混淆,难以区分破坏型数据犯罪与非法控制计算机信息系统罪。最后,如果将计算机信息系统功能作为入罪标准,将难以合理限定数据犯罪的处罚范围。以破坏型数据犯罪为例,由于《刑法》第 286 条破坏计算机信息系统罪中第 1 款、第 3 款的罪状表述要求“造成计算机信息系统不能正常运行”或“影响计算机信息系统正常运行”,而对于第 2 款删除、修改、增加数据行为则未有类似规定,引发了实务中对于该款应否具备“使计算机信息系统不能正常运行”的激烈争论。〔27〕 虽然《计算机安全解释》对该罪的危害后果采取了区分判定的司法逻辑:对侵害数据安全的情节需求与侵害计算机信息系统安全的情节需求应相互独立,前者不要求对计算机信息系统造成损害,只要满足其罪量要素即可。〔28〕 但学界多数观点仍对“计算机信息系统安全”法益进行体系解释,认为删除、修改、增加数据行为必须导致“计算机信息系统不能正常运行”或者至少与计算机信

〔26〕 参见上海市浦东区人民法院(2015)浦刑初第 1460 号刑事判决书;重庆市渝北区人民法院(2015)渝北法刑初字第 00666 号刑事判决书。

〔27〕 参见邢永杰:《破坏计算机信息系统罪疑难问题解析》,《社会科学家》2010 年第 7 期,第 83 页;俞小海:《破坏计算机信息系统罪之司法实践分析与规范含义重构》,《交大法学》2015 年第 3 期,第 73 页;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》,《法治研究》2018 年第 4 期,第 149 - 150 页。

〔28〕 参见喻海松:《〈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〉的理解与适用》,《人民司法》2011 年第 19 期,第 27 页。

息系统具有关联性,[29]不恰当地增加了数据犯罪的成立条件而限缩了处罚范围。

(二)数据安全法益(CIA)之提倡

1975 年学者 Saltzer 和 Schroeder 在总结当时未经授权泄露、修改、使用数据等法律风险时提出了"数据安全"概念。[30] "数据安全"旨在保护数据利用的三个面向(CIA triad),即"数据安全"三要素,包括数据的保密性(confidentiality)、完整性(integrity)和可用性(availability)。侵犯上述法益的行为被称为 CIA 犯罪,主要针对当时网络黑客的犯罪行为。[31] 数据的"保密性"是指确保数据免受未授权人探知、获悉或使用。对"保密性"的侵害意味着对数据的非法访问、读取、获取,导致其陷入随时被扩散、公布的风险之中。通常的侵害方式包括数据包嗅听、密码破解、回收站搜寻、键盘测录、网络钓鱼等。数据"完整性"是指确保数据不被修改或损害。对"完整性"的侵害意味着对数据进行删除、修改或者增加等破坏行为,导致其记载的信息内容无法被完整地读取和使用,进而侵害了数据的真实性、可靠性。通常的侵害方式包括:萨拉米攻击、[32]数据欺骗攻击、会话劫持等。数据"可用性"是指确保权利人能及时、有效地获取、使用数据。对"可用性"的侵害将导致授权用户无法访问数据或系统,如通过使网络堵塞而阻止合法用户进入等。典型的是分布式拒绝服务(Distributed Denial of Service,DDos)攻击曾使全球众多网站瘫痪。[33] 此后,一连串以保护数据安全为主轴的立法趋势也在 20 世纪 80 年代末逐渐扩散到世界各国。一种是以美国为典型的集中式立法,以数据安全的社会信赖感为规范基础建构数据犯罪的各项规定,如美国联邦《电脑诈欺与滥用法》(*Computer Fraud and Abuse Act*,CFAA)规定了侵入、取得、删除、变更电脑数据等行为属于违法犯罪行为;另一种是以德国为典型的分布式立法,将数据犯罪分别置于欺诈罪章、妨害秘密罪章、伪造文书罪章与毁损罪章之中。[34] 我国《网络安全法》第 10 条也明确规定保护"网络数据的完整性、保密性和可用性"。

大数据时代"数据"的量级、结构等已经复杂化、多样化,数据犯罪的保护法益已非纯粹依附于"计算机信息系统安全"的技术性范畴,其自身包含了信息社会某些最重要的利

〔29〕 参见俞小海:《破坏计算机信息系统罪之司法实践分析与规范含义重构》,《交大法学》2015 年第 3 期,第 150 页;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》,《法治研究》2018 年第 4 期,第 75 页。

〔30〕 See Yulia Cherdantseva, Jeremy Hilton, *A Reference Model of Information Assurance & Security*, IEEE proceedings of ARES 2013, SecOnt workshop. 2 (2 - 6 September, 2013, Regensburg, Germany).

〔31〕 参见[德]乌尔里希·齐白著:《全球风险社会与信息社会中的刑法》,周遵友、江溯等译,中国法制出版社 2012 年版,第 308 页。

〔32〕 萨拉米技术(salami technique)是通过计算机程序控制自动进行的一种数据窃取行为,多采用不易觉察的手段,不断偷取、由少积多的方式进行,以达到某种犯罪目的。https://baike.so.com/doc/4984774 - 5208170.html,最近访问时间[2019 - 11 - 12]。

〔33〕 See Sagar Ajay Rahalkar, *Certified Ethical Hacker (CEH) Foundation Guide*, at 85 - 86 (Apress Media, LLC, 2016).

〔34〕 参见许恒达:《资讯安全的社会信赖与刑法第 359 条的保护法益——评士林地方法院 99 年度诉字第 122 号判决》,《月旦法学杂志》2011 年第 11 期,第 243 页;林山田著:《刑法各罪论》(上册),北京大学出版社 2012 年版,第 392 页。

益和价值观,[35]即公众对数据储存状态及其内容的信赖感。因为对于公众利用电脑或网络所产生的值得信赖的数据状态,法律应确保其不被侵犯、修改,以保护数据利益主体对数据的“排他性使用权限”、数据的“排他性复制、用益与处分权限”以及数据的“正确性”,[36]从而维护数据在社会往来中的安全性和可信赖性。[37] 因此,“数据安全”应作为独立保护价值来合理评价,从“技术性”回归“本体性”。在比较法上,无论欧洲理事会的《网络犯罪公约》(*Convention on Cybercrime*)还是欧盟理事会《关于攻击信息系统的理事会框架决议》(*EU Council Framework Decision* 2005/222/*JHA on attacks against information systems*),都将数据安全与计算机信息系统安全分别予以保护,规定不同的罪名和构成要件。对前者的保护,主要考虑数据的机密性、完整性和可用性;而对后者的保护,主要是维护计算机信息系统运营安全,即计算机信息系统功能的保密性、完整性和有用性。[38]

相较于计算机信息系统安全法益而言,数据安全法益是基于数据自身内容、使用价值和侵害风险所进行的独立规范评价,能更合理地解释数据犯罪的构成要件。首先,它以数据安全的不同保护需求来界定“数据”本身。大数据时代,数据的异构性、规模性、实时性、复杂性等特点决定了对数据安全法益侵害的分析必须在不同层次进行,因而数据本身的内容、数据结构、数据周期、数据源等表征不同数据安全风险的要素,应成为我国数据犯罪中“数据”界定的主要依据,这关系到立法确认的数据权利的性质和保护范围。其次,它依据数据安全的不同侵害侧面来解释数据犯罪的行为要件。数据犯罪方式是数据安全风险在不同侧面的类型化表达,如获取型数据犯罪侵害了数据的保密性需求,破坏型数据犯罪侵害了数据的完整性、可用性需求。但“数据客体本身的可无限复制性、使用的无消耗性、数据主体对数据的无控制性、数据控制主体应用数据行为的隐蔽性等特点”,[39]增加了其行为要件的判断难度。实务中对数据犯罪行为要件的认定不能仅采取形式判断,应深入考察其法益侵害实质,对于删除、修改、增加数据但未侵犯数据安全法益或者侵害程度甚微的行为,不宜认定为数据犯罪,否则对计算机信息系统实施的任何操作都可能被评价为对数据的删除、修改、增加,进而被认定为破坏型数据犯罪,最终导致数据犯罪的“口袋化”而使其他计算机犯罪没有存在的余地。最后,它以数据安全法益侵害程度来评价数据犯罪的行为后果。数据安全法益受侵害的严重程度决定了“情节严重”“后果严重”等入罪标准的解释适用。当前司法实务普遍采用的“违法所得”“经济损失”等数额标准均弱化了行为后果与数据安全法益的关联性,而更能体现数据安全法益侵害程度的数据性质、数据种类等情节标准却被忽略。未来数据犯罪的入罪标准应从以“数额标准”为重心转向“数额标准”与“情节标准”并重的格局,以合理评价数据犯罪的法益侵害程度。

当前我国数据犯罪的立法规定与司法解释均未能围绕数据安全法益来解释数据犯罪

〔35〕 参见[德]乌尔里希·齐白著:《全球风险社会与信息社会中的刑法》,周遵友、江溯等译,中国法制出版社 2012 年版,第 303 页。

〔36〕 参见许恒达:《资讯安全的社会信赖与刑法第 359 条的保护法益——评士林地方法院 99 年度诉字第 122 号判决》,《月旦法学杂志》2011 年第 11 期,第 242 页。

〔37〕 参见徐育安:《资讯风险与刑事立法》,《台北大学法学论刊》2013 年第 91 期,第 141 页。

〔38〕 参见皮勇:《论欧洲刑事一体化背景下的德国网络犯罪立法》,《中外法学》2011 年第 5 期,第 1040 – 1046 页。

〔39〕 李爱君、苏桂梅著:《国际数据保护规则要览》,法律出版社 2018 年版,第 4 页。

的构成要件,导致数据安全法益的立法批判功能和解释适用功能均未能正常发挥。因此,未来数据犯罪的解释适用应着重将数据安全法益纳入数据犯罪的构成要件之中,为数据犯罪的司法适用提供新的解决思路和依据。

三 以数据安全法益重释数据犯罪的构成要件

如前所述,数据安全法益既是检验数据犯罪立法科学性的基本准则,也是解释数据犯罪构成要件的实质判断标准。数据犯罪的刑法规制应依据数据安全法益来实现数据犯罪规范体系与技术规则的深度融合,以应对不断更新的数字化犯罪技术。

(一)对象:体现不同数据安全需求的数据类型

数据本身的具体内容、类型划分等决定了数据犯罪的成立和责任的轻重,应成为数据犯罪的研究起点。早先,学界将"数据"理解为从外部输入计算机信息系统内部的图片、文字、影音资料、专有的程序或者软件等,也包括网页浏览痕迹、下载记录、关键词搜索记录等电脑操作行为产生的网络行为数据。[40] 随着移动计算的快速发展,当前"数据"更受关注的是数据的存在体系——结构化和非结构化,和数据的价值链——数据生成、数据获取、数据存储和数据分析。[41] 这意味着大数据时代对数据犯罪中"数据"的规范判断应逐步弱化与"计算机信息系统"等储存设备、载体、媒介的关联性,而更多地关注数据类型、结构、组织、粒度、生命周期及由此形成不同层级法益侵害风险和保护需求。从司法实践来看,我国数据犯罪中的"数据"主要包括以下几种。

1. 未经技术加工的数据集合体(非结构化数据)

这种由单个数据组成的集合体,包含了"海量"特性但又缺乏"技术分析、加工"的无数个有价值数据、低价值数据和无价值数据。[42] 典型的是《计算机安全解释》在获取型数据犯罪中规定的"身份认证信息",如支付宝账号密码、证券交易账号密码、期货交易账号密码、wifi 账号密码、网络游戏账号秘密等。从内容来看,身份认证信息具有高度私密性,与个人法益安全紧密相关,用户不会将其内容告知数据收集者,更不会将其使用权授权或让渡给数据收集者。实务中由海量"身份认证信息"所组成的数据集合体大多是收集者非法获取且未经编排而随意堆积的初始数据,收集者无意了解数据的具体内容,更无意对其加工整理,其目的仅在于非法获取后用来实施犯罪或转卖他人。因此,未经技术加工的数据集合体尚不能称为数据产品,数据收集者不可能获得法律意义上的支配权,但此种数据集合体能表征海量用户对自身初始数据的安全诉求,对其非法获取的行为仍侵犯了用户对数据的保密性需求。

2. 经技术加工的数据产品(结构化数据)

这类数据是指数据经营者依特定逻辑对网络数据进行收集、整理、分析等增值处理而

〔40〕 于志刚主编:《网络犯罪公约的修正思路》,中国法制出版社 2016 年版,第 55 页。

〔41〕 参见李学龙、龚海刚:《大数据系统综述》,《中国科学:信息科学》2015 年第 1 期,第 7 - 8 页。

〔42〕 参见李爱君:《数据权利属性与法律特征》,《东方法学》2018 年第 3 期,第 66 页。

生成的系统化、有价值的数据。从内容来看,这些数据产品由用户个人初始数据集合而成,如通过网络交易的点击日记,加工、计算、聚合成交易数据;通过用户的浏览点击日志,加工、计算、聚合成偏好数据。[43] 从来源来看,这些数据产品主要产生于商业性利用环境之中。一是用户利用个人数据获得经济利益或者某种社会评价、服务等时主动提供的,如公民在进行求职、购物、贷款、保险等活动时都必须主动、如实披露个人资料;二是专门数据经营者通过用户协议对个人信息进行收集、处理。如大数据公司或数据交易平台对数据信息的收集、加工、处理形成特定类别的数据库,对外提供查询、租赁、销售等服务。数据经营者正是通过对数据的收集、利用、交易等形成了动态的数据使用、利益关系,应当受到法律的保护。[44] 例如在"实时公交查询软件'酷米客'诉'车来了'盗取后台数据案"中,元光公司为了提高其开发的智能公交 APP"车来了"的市场用户量及信息查询的准确度,由其法定代表人邵某授意公司技术人员利用网络爬虫技术大量获取竞争对手谷米公司同类公交软件 APP"酷米客"中的实时公交信息数据,然后无偿使用于"车来了"APP,并对外提供给公众进行查询。法院认为邵某等人利用非法手段侵入被害单位服务器并获取实时数据,构成非法获取计算机信息系统数据罪。[45] 该案也是近年来大数据不正当竞争纠纷的典型案例,虽然公交车作为公共交通工具,其实时运行路线、运行时间等信息是客观事实,但当此类信息经过人工收集、分析、编辑、整合并配合 GPS 精确定位后已成为公交信息查询软件的后台数据,具有了实用性并能够为权利人带来经济利益,权利人对该数据享有占有、使用、收益及处分权益。[46] 显然,数据经营者通过对数据的收集、加工、利用、交易等而获得了数据资产的经营权和资产权,并形成了保密性、完整性和有用性需求,应受到刑法保护。

(二)行为:侵犯不同数据安全侧面的获取、删除、修改、增加行为

对于数据犯罪中"获取""破坏"等规范性构成要件要素,立法和司法解释一直未有正面阐述,因而给司法适用留下巨大的解释空间。尤其是对获取、删除、修改、增加数据而未侵害数据安全法益的行为定性,在技术层面与规范层面存在较大分歧,亟需依据数据安全法益进行实质解释以合理出罪。

1. 侵犯数据保密性的"获取"行为

对数据这种虚拟物品的"获取"并不意味着如有体物般的转移占有,因为数据具有非排他性和非消耗性特点,只有是否知悉、分享、控制问题,而不存在占有与转移的问题。[47] "非法获取"是指非法改变了数据主体所设定的数据不被知悉的状态,进而非法取得了本应保密的数据,侵犯了数据的保密性需求。[48] 在行为类型上包括:(1)未经授权访问、取

〔43〕 参见杨立新、陈小江:《衍生数据是数据专有权的客体》,《中国社会科学报》2016 年 7 月 13 日第 005 版。

〔44〕 参见张新宝:《从隐私到个人信息:利益再衡量的理论与制度安排》,《中国法学》2015 年第 3 期,第 46 页;龙卫球:《数据新型财产权构建及其体系研究》,《政法论坛》2017 年第 4 期,第 74 页。

〔45〕 参见广东省深圳市南山区人民法院(2017)粤 0305 刑初 153 号刑事判决书。

〔46〕 参见广东省深圳市南山区人民法院(2017)粤 03 民初 822 号民事判决书。

〔47〕 参见欧阳本祺:《论网络时代刑法解释的限度》,《中国法学》2017 年第 3 期,第 169 页。

〔48〕 参见于志刚、李源粒:《大数据时代数据犯罪的类型化与制裁思路》,《政治与法律》2016 年第 9 期,第 24 页。

得他人数据,主要针对外部网络黑客的行为。“未经授权”的方式包括明示与暗示:明示的“未经授权”包括与员工签订保密协议、[49]网页上明确标注禁止爬虫的警告、[50]合同使用条款中的特殊说明;[51]暗示的“未经授权”主要是指密码认证,强调用户需要通过密码来获取访问权限,如果规避技术访问障碍、绕开认证,就属于“未经授权”。[52] (2)被授权者超越授权访问、取得数据,主要针对内部网络黑客的行为。如被授权者超越代理权限、违反合同规定的义务而访问、获取数据。[53]

显然,对“获取”的界定必须围绕数据保密性需求来展开以限定数据的处罚范围,通常要求权利人主观上对数据具有保密的意思,客观上对数据采取一定的安全控制措施,[54]因而对于未侵犯数据保密性的“获取”行为,不应评价为数据犯罪。在全国首起“爬虫”获取数据案中,被告人张某等采用技术手段破解被害单位的防抓取措施,使用软件绕过服务器的身份校验和访问频率限制,并抓取被害单位服务器中存储的视频数据,造成被害单位损失技术服务费2万元。后法院认定被告人违反国家规定,采用了规避或突破被害单位反“爬虫”安防措施的技术手段,属于“未经授权”获取非公开信息,构成非法获取计算机信息系统数据罪。[55] 对于利用“爬虫”软件绕过技术障碍获取非公开数据的行为,因为侵犯了数据的保密性需求,可以认定为非法获取计算机信息系统数据罪。但对于利用“爬虫”软件获取已公开数据的行为,由于不存在侵害权利人的保密意思和安全控制措施等所表征的保密性法益,在我国当前数字经济背景下,亦认定为不正当竞争行为而非数据犯罪,如2017年“新浪微博诉脉脉不正当竞争案”。[56] 美国司法实务的最新观点也认为,公开数据缺少相应的保护措施,如同商店对其橱窗里对外展示的物品或广告不能禁止他人观看一样,不存在保密性需求,不属于“受保护的计算机数据”。[57]

2. 侵犯数据完整性、可用性的“删除、修改、增加”行为

《刑法》第286条破坏计算机信息系统罪的立法目的是为数据、应用程序提供类似于物质物体所享有的免受故意侵害的保护。[58] 如刑法中破坏交通工具罪、破坏交通设施罪、破坏生产经营罪等破坏型犯罪,尽管“破坏”的手段、方法多样,但本质上都要求影响物品的正常使用或事物的正常运行。[59] 删除、修改、增加数据妨害了权利人对数据的正常使用权利,侵害了数据在事实上的利用可能性,因而侵害了数据的完整性、可用性。其中,“删除”“增加”主要是在数量上对数据的减少或增加,即将数据在数据载体中移除或

〔49〕 See EFCultural Travel BV v. ZeferCorp., 318 F. 3d 58, 62 (1st Cir. 2003).

〔50〕 See SouthwestAirlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 – 440 (N. D. Tex. Mar. 19, 2004).

〔51〕 See College Source, Inc. v. Academy One, Inc., 597 Fed. Appx. 116, 130 (3d Cir. 2015).

〔52〕 See CraigslistInc. v. 3 Taps Inc., 942 F. Supp. 2d 962 (N. D. Cal. 2013).

〔53〕 See Samantha Jensen, Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fall, *Hamline Law Review* 10 (2013).

〔54〕 参见皮勇:《论欧洲刑事一体化背景下的德国网络犯罪立法》,《中外法学》2011年第5期,第1051页。

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

〔56〕 “新浪微博诉脉脉大数据引发不正当竞争第一案”,http://news.sina.com.cn/sf/news/ajjj/2017 – 02 – 08/doc – ifyafenm3035943.shtml,最近访问时间[2019 – 11 – 10]。

〔57〕 See hiQLabs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N. D. Cal. 2017).

〔58〕 于志刚主编:《网络犯罪公约的修正思路》,中国法制出版社2016年版,第61页。

〔59〕 参见杨赞:《开发外挂软件营利行为如何定性》,《人民检察》2017年第16期,第43页。

添加;“修改”则是指在内容上对数据进行改动导致数据完整性的消极改变。上述行为都要求达到使数据丧失正常功效,影响数据的正常使用或运行的程度。

对“删除、修改、增加”的解释认定应围绕数据完整性、可用性需求来展开,对未侵犯数据完整性、可用性的删除、修改、增加行为,不应评价为数据犯罪。但数字化犯罪技术的快速更新增加了“删除、修改、增加”的认定难度,导致其范围一再扩大而逐渐丧失构成要件的定型性,司法实务甚至将“破坏”数据行为扩大至增强数据功能或应用程序功能的无害行为。如在全国首例“制售微信外挂软件案”中,被告人张某、刘某未经授权、许可,制作了能对微信手机客户端安装文件进行修改的“数据精灵”“果然叼”“玩得溜”等计算机软件,并在网络上销售。该软件的功能经鉴定包括微信多开、一键转发朋友圈内容、朋友圈无限制提醒好友,但并不影响消费者微信功能的正常使用,相反,其使用依赖于微信的正常运行,也未对整个手机终端造成现实影响。〔60〕 从技术角度而言,微信外挂软件功能的实现依赖于微信软件启动后,加载下载的动态文件,对微信手机客户端界面进行修改,因而增加了微信服务平台传输的数据总量,貌似符合破坏型数据犯罪中“增加数据”这一行为要件。但从刑法角度而言,构成破坏型数据犯罪要求对数据的删除、修改、增加导致数据丧失正常功效或者影响数据正常运行。但本案中制售的微信外挂软件在功能和用途上并未影响微信数据、微信程序的正常运行,也不影响用户手机的正常使用,没有破坏微信功能反而增强了微信功能。〔61〕 因此,制售微信外挂行为不应被评价为刑法意义上的“破坏”行为,不构成破坏计算机信息系统罪。

(三)结果:体现数据安全法益侵害程度的数额与情节

从数据安全法益出发,非法获取、删除、修改、增加的数据数量、数据类型、数据性质等决定了数据犯罪责任的轻重,应成为主要入罪标准。而《计算机安全解释》除了在获取型数据犯罪中明确认可网络金融服务的身份认证信息的重要性并规定数量标准外,对其他类型数据本身的重要性及其法益侵害性均缺乏明确的规定,亟需补齐。

1. 数量标准的补齐

现有数据犯罪的入罪标准包括数额标准和物数标准,其中数额标准包括经济损失、违法所得;物数标准包括计算机台数、身份认证信息组数。但上述标准均弱化了“后果”、“情节”与数据安全法益的关联性,而更能体现数据犯罪法益侵害性的数据数量标准,却未被《计算机安全解释》详细提及。因为《计算机安全解释》仅在获取型数据犯罪中明确了身份认证信息的组数标准,对于身份认证信息之外的其他类型数据,则未明确规定数量标准。而在破坏型数据犯罪中,则彻底未规定数据数量标准,仅规定了数据赖以储存的计算机台数。〔62〕 当行为人侵害的数据并非储存于“计算机信息系统”中时,该台数标准便无

〔60〕 参见广东省广州市海珠区人民法院(2016)粤 0105 刑初 1040 - 1 号刑事判决书。

〔61〕 参见杨赞:《开发外挂软件营利行为如何定性》,《人民检察》2017 年第 16 期,第 43 - 44 页;聂立泽、胡洋:《全国首例开发微信外挂软件销售案的刑法定性问题研究》,《南都学坛(人文社会科学学报)》2018 年第 3 期,第 66 - 67 页。

〔62〕 《计算机安全解释》第 4 条规定:破坏计算机信息系统功能、数据或者应用程序,具有下列情形之一的,应当认定为《刑法》第 286 条第 1 款和第 2 款规定的“后果严重”:(二)对 20 台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的。

法适用,引发司法判断难题。如在“张某破坏计算机信息系统案”中,被告人张某于2014年12月20日及28日登陆法制晚报官方微博“法晚壹现场”,并对该官方微博进行删除(约3000条)。法院认为张某违反国家规定,非法删除计算机信息系统中的数据,后果严重,构成破坏计算机信息系统罪。〔63〕但从破坏计算机信息系统罪的入罪标准来看,本案并不符合《计算机安全解释》第4条第(二)(三)项中计算机台数、违法所得、经济损失等标准,只能适用第(五)项“造成其他严重后果的”这一兜底规定。〔64〕从现有案情来看,这里的“其他严重后果”应是指张某所删除的微博数据数量。但数据数量标准的缺乏,导致本案的司法适用仍缺乏明确指引。

2. 情节标准的补齐

数字化技术的广泛运用正在将传统犯罪定量评价机制中“数额为主,情节为辅”向“数额与情节并重”过渡,并进一步向“情节”为主的新型“双层社会”入罪标准转移。〔65〕数据犯罪的情节标准是指在行为人违法所得、被害人经济损失、被侵害的数据数量等数额条件之外,影响国家、社会或个人正常的工作秩序或生活秩序,或造成恶劣社会影响等情形。对情节标准的适用,应结合被侵害数据的重要性、危害性进行实质性、综合性评价。当前司法实务中典型案例包括以下三类。第一类是修改高考志愿,干扰考试录取秩序。〔66〕此类案件中,行为人非法侵入考试志愿系统,修改了某个或某些特定被害人的考试志愿,使其无法被正常录取,或者只能被行为人所篡改的学校录取。该行为虽然无法用数额标准来定罪量刑,但影响了被害人考试志愿的实现,干扰了正常的考试录取秩序,应属于破坏计算机信息系统罪中“造成其他后果严重的”情形。第二类是修改考试成绩,干扰正常教学秩序或影响考试的公平性、权威性。〔67〕此类案件中行为人往往以牟利为目的修改考试系统中的考生成绩,导致系统将不及格的考生成绩默认为合格,极大影响了考试的公平性和权威性,扰乱了社会公共秩序,应当属于破坏计算机信息系统罪中“造成其他后果严重的”情形。第三类是修改环保监测数据,影响环境监测评估的准确性。在国内首起“环保监测数据案”中,被告人李某等多次潜入某区环境空气自动监测站内,利用棉纱堵塞采样器的方法,干扰站内环境空气质量自动监测系统的数据采集功能,造成该站自动监测数据多次出现异常,严重影响了国家环境空气质量自动监测系统正常运行。〔68〕该案的“严重后果”无法用具体的数额标准来衡量,但从情节严重角度考

〔63〕 参见北京市丰台区人民法院(2015)丰刑初字第1964号刑事判决书。

〔64〕 《计算机安全解释》第4条规定:破坏计算机信息系统功能、数据或者应用程序,具有下列情形之一的,应当认定为《刑法》第286条第1款和第2款规定的“后果严重”:(一)造成10台以上计算机信息系统的主要软件或者硬件不能正常运行的;(二)对20台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的;(三)违法所得5000元以上或者造成经济损失10000元以上的;(四)造成为100台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为10000以上用户提供服务的计算机信息系统不能正常运行累计1小时以上的;(五)造成其他严重后果的。

〔65〕 参见于志刚、郭旨龙:《信息时代犯罪定量标准的体系化构建》,《法律科学》2014年第3期,第133页。

〔66〕 参见山西省高平市人民法院(2016)晋0581刑初字290号刑事判决书;山东省临沂市沂水县人民法院(2015)沂刑一初字第124号刑事判决书;江苏省徐州市睢宁县人民法院(2017)苏0324刑初408号刑事判决书。

〔67〕 参见广西省南宁市青秀区人民法院(2013)青刑初字第758号刑事判决书。

〔68〕 参见陕西省西安市中级人民法院(2016)陕01刑初第233号刑事判决书。

察,用棉纱等物品堵塞环境监测采样器,干扰采样,造成监测数据失真,由于该监测数据已被传输发送至中国环境监测总站并制成环境质量评估报告,因而影响了全国大气治理评估的真实性并损害政府公信力,属于“造成其他严重后果的”情形,应认定为破坏计算机信息系统罪。

四 基于数据安全法益的数据犯罪边界厘定

数据犯罪的定性争议源于其内部边界与外部边界模糊不清:在内部边界上与其他计算机犯罪相混淆,在外部边界上与传统犯罪相混淆。未来数据犯罪的司法适用应依据数据安全法益的界分功能和现有立法,厘清数据犯罪与其他计算机犯罪、传统犯罪之间的区别,以合理限定数据犯罪的处罚范围。

(一)内部边界:数据犯罪与其他计算机犯罪的区分

这主要涉及数据犯罪与《刑法》第 285 条、第 286 条规定的其他计算机犯罪之间的区分。由于立法对数据犯罪帮助行为正犯化规定的不明晰,以及技术层面对计算机信息系统安全的侵害与对数据安全的侵害具有同步性,引发了数据犯罪与其他计算机犯罪的区分难题。

1. 数据犯罪与提供侵入、非法控制计算机信息系统程序、工具罪的区分

数字化技术的复杂性、专业性使得为数据犯罪提供网络技术支持的帮助行为越来越重要,甚至成为整个数据犯罪链条中最重要的一环,在法益侵害性和独立性上已突破传统共犯从属性地位,因而网络帮助行为正犯化成为立法主要应对模式。[69] 如《刑法修正案(七)》将为非法侵入、非法控制计算机信息系统提供帮助的行为单独规定为提供侵入、非法控制计算机信息系统程序、工具罪。虽然从文义解释来看,该罪似乎并不包括为非法获取数据提供帮助的行为。但是从目的解释来看,该罪是《刑法》第 285 条第 1 款和第 2 款的工具犯,所提供的“程序、工具”既包括专门用于侵入、非法控制计算机信息系统的程序、工具,也包括通过侵入计算机信息系统而非法获取数据的专门性程序、工具。即主要强调程序、工具本身的获取数据和控制功能。[70] 据此,为非法获取数据提供帮助的行为应认定为提供侵入、非法控制计算机信息系统程序、工具罪。

但由于立法对数据犯罪帮助行为正犯化的规定不够明晰,以及提供侵入、非法控制计算机信息系统程序、工具罪罪状表述的不科学,引发了数据犯罪与提供侵入、非法控制计算机信息系统程序、工具罪的区别难题。以全国首起“撞库打码案”为例,[71] 2015 年 1

〔69〕 参见刘艳红:《网络帮助行为正犯化之批判》,《法商研究》2016 年第 3 期,第 20 页;于志刚:《网络空间中犯罪帮助行为的制裁体系与完善思路》,《中国法学》2016 年第 2 期,第 7 页;于冲:《网络犯罪帮助行为正犯化的规范解读与理论省思》,《中国刑事法杂志》2017 年第 1 期,第 80 页。

〔70〕 参见喻海松:《〈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〉的理解与适用》,《人民司法》2011 年第 19 期,第 28 页。

〔71〕 “撞库”又称“扫存”,是指非权利人通过收集互联网已泄露的各类帐户和密码生成对应的字典表,通过工具尝试批量登录其他网站,从而得到一系列可以登录的帐户密码的行为。

月,叶某编写了“小黄伞”扫号软件,并将识别图片验证码的工作(俗称“打码”)交给张某来完成。张某组织大量码工并建立打码平台完成工作,以此从被告人叶某处获取好处。2015 年 1 月到 9 月,谭某购买验证码充值卡并使用叶某编制的“小黄伞”软件,在张某帮助打码的情况下,成功刷取了 2.2 万余组淘宝账号并出售牟利,违法所得达 25 万余元。〔72〕 本案中谭某使用“小黄伞”软件和打码平台等技术手段,对淘宝网站实施撞库,获取的淘宝用户账密等属于《计算机安全解释》中的“身份认证信息”,其行为符合非法获取计算机信息系统数据罪的构成要件。但对叶某、张某的行为定性,存在非法获取计算机信息系统数据罪(共犯)和提供侵入、非法控制计算机信息系统程序、工具罪的争议。〔73〕 从技术层面而言,叶某编写的“小黄伞”软件主要具有三个功能。第一,具有获取计算机信息系统数据的功能。如“小黄伞”能进入淘宝数据系统自动抓取淘宝账号对应的昵称、注册时间、是否认证等信息。第二,具有避开或突破计算机信息系统安全保护措施的功能。如“小黄伞”能不断地更换 IP 地址,接入打码平台,并且突破验证码的防范。第三,“小黄伞”获取数据的功能是在未经授权的情况下完成的,从而区别于“中性程序、工具”而具有违法性。因而“小黄伞”软件符合《计算机安全解释》第 2 条第 1 项规定的“专门用于侵入计算机信息系统的程序”,即“具有避开或者突破计算机信息系统安全保护措施,未经授权或者超越授权获取计算机信息系统数据的功能”。从在犯罪中所起的作用来看,叶某编写“小黄伞”的行为和张某帮助打码的行为都是为谭某非法获取数据提供帮助的行为。在立法已将为非法获取数据提供帮助的行为正犯化后,对叶某和张某的行为应定性为提供侵入、非法控制计算机信息系统程序、工具罪,而非非法获取计算机信息系统数据罪(共犯)。

2. 数据犯罪与非法控制计算机信息系统罪的区分

由于对计算机信息系统的非法控制需要通过对数据或应用程序的删除、修改、增加来完成,导致非法控制计算机信息系统罪与破坏型数据犯罪之间的适用争议。以“汪某等非法控制计算机信息系统案”为例,2014 年 1 月至 8 月期间,被告人汪某等人采用远程连接方式,进入芜湖市公安局交警支队车管所服务器,用申请人满意的车牌号码替换十选一选号系统流水号 10 个车辆号牌中的 1 个,从而使得选号者选中替换后的车牌号码,以获取不正当报酬。一审法院认为汪某等人违反国家规定,对计算机信息系统中存储、处理、传输的数据进行删除、修改,构成破坏计算机信息系统罪。二审法院认为汪某等人违反国家规定,侵入芜湖市交警支队计算机信息系统,对该计算机信息系统实施非法控制,构成非法控制计算机信息系统罪。〔74〕 该案的定性争议在于被告人的行为修改了计算机信息系统中储存、处理、传输的数据还是控制了计算机信息系统,在法益评价上的争议则体现为对数据安全的侵害还是对计算机信息系统安全的侵害。

随着对数据处理功能的增强,计算机信息系统已经成为高速运转的动态数据处理

〔72〕 参见浙江省杭州市余杭区人民法院(2017)浙 0110 刑初 664 号刑事判决书。

〔73〕 参见杨赞:《撞库打码牟利行为如何定性》,《人民检察》2018 年第 4 期,第 42 页。

〔74〕 参见安徽省芜湖市中级人民法院(2015)芜中刑终字第 00304 号刑事判决书。

系统,任何对计算机信息系统实施的简单操作都会在后台体现为对数据的删除、修改、增加等,导致计算机信息系统及数据的动态特征与计算机信息系统及数据的“破坏”被等同起来。〔75〕 这使得侵害计算机信息系统安全的行为同时具有了侵害数据安全法益的风险,加之破坏型数据犯罪的法定刑较之于其他计算机犯罪的法定刑更重,因此无论按想象竞合犯还是牵连犯从一重处罚,最后适用破坏计算机信息系统罪都不存在太大问题。〔76〕 但在规范层面,虽然汪某等人的行为涉及对车辆号牌数据的修改,但对数据安全法益的侵害并未达到可罚程度,且修改数据只是控制计算机信息系统的必经步骤和手段,其最终目的仍是控制计算机信息系统,因而行为评价重点应是对计算机信息系统安全的侵害,认定为非法控制计算机信息系统罪更能体现该行为的法益侵害性。而不能径行依据修改数据行为将其认定为破坏型数据犯罪,否则会导致其他与计算机有关的犯罪没有存在的余地。

(二)外部边界:数据犯罪与传统犯罪的区分

这主要是指数据犯罪与《刑法》第 287 条利用计算机实施传统犯罪的区分。《刑法》第 287 条规定:“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照本法有关规定定罪处罚。”随着数字化技术的发展,司法实务已将“利用计算机”侵犯传统法益的犯罪置换为“利用数据”侵犯传统法益的犯罪。实务中行为人单纯获取、删除、修改、增加数据的情形较少,多数是通过对数据的侵害来实现非法取财、获取个人信息、商业秘密等其他目的,极易出现一个行为或多个行为同时触犯数个罪名的想象竞合犯、法条竞合、牵连犯、数罪并罚等情形。但是,表征个人信息权、〔77〕财产权、知识产权等传统法益的“数据”与表征数据安全法益的“数据”在法律属性和受侵害方式上有较大区别。前者通过对数据的非法获取、删除、修改、增加来侵害其他传统法益,而后者只是对数据安全本身的侵害足以构成犯罪。因此,可依据数据在法益侵害中的不同作用对其分而治之。仅对其本体加以侵害时,应适用数据犯罪;但对于其功能性作用加以侵害时,应依其表征的法益回归各自的犯罪类型进行处理。〔78〕

1. 以数据为对象侵犯数据安全的行为应构成数据犯罪

此种类型是指对数据的非法获取、删除、修改、增加行为是以侵犯数据安全法益为终极目的,而非实施其他犯罪的工具、手段的犯罪。比如,删除天涯论坛帖子、〔79〕删除京东差评或淘宝网差评〔80〕等行为都应认定为数据犯罪。如被告人李某在 2011 年 5 月至

〔75〕 参见林建辉、黄学鹏:《破坏计算机信息系统罪的电子数据适用研究》,《信息安全与技术》2014 年第 8 期,第 15 页。

〔76〕 参见于志刚:《口袋罪的时代变迁、当前乱象与消减思路》,《法学家》2013 年第 3 期,第 70 页。

〔77〕 个人信息权虽然是近年来民法和刑法探讨的一种新型权利,但在本文中,个人信息权仍属于传统个人法益范畴,原本为个人隐私权所涵括,只是近年来刑法学界开始采用民法学界通说,即个人信息权不仅包括了传统隐私权消极防御的一面,也包括积极利用的一面。但这只是对个人信息权内容的扩充,其本质仍然是传统个人法益。

〔78〕 参见柯耀程:《“电磁记录”规范变动之检讨》,《月旦法学教室》2008 年第 72 期,第 127 页。

〔79〕 参见海南省海口市龙华区人民法院(2015)龙刑初字第 296 号刑事判决书。

〔80〕 参见江苏省宿迁市宿豫区人民法院(2016)苏 1311 刑初 520 号刑事判决书;浙江省杭州市滨江区人民法院(2014)杭滨刑初字第 106 号刑事判决书。

2012 年 12 月期间,冒用淘宝买家身份骗取淘宝账号密码重置后,非法登录淘宝评价系统从而删除、修改淘宝买家的中差评 347 个,从中获利 9 万余元。法院经审理认为,淘宝网站是一个具备自动处理数据功能的计算机信息系统,信用评价系统属于整个淘宝系统的一个子系统,用户评价以数据形式储存于买家评价系统之中,成为购物网站整体数据的重要部分。被告人李某对中差评数据的删除行为,系对计算机信息系统中存储的数据进行修改操作,侵害了计算机信息系统数据的安全,其行为符合破坏计算机信息系统罪的构成要件。〔81〕

2. 以数据为工具、媒介侵害传统法益的行为应认定为传统犯罪

以数据为载体的传统法益具有特定内涵和识别标识,从而区别于数据犯罪,应依照传统法益的不同性质认定为相应的传统犯罪。〔82〕

首先,侵犯"可识别性"个人数据的行为应构成侵犯公民个人信息罪。以电子方式记录的个人信息以数据为载体,使得"个人信息"与"数据"在真实的"个人数据"上重叠,如学籍管理系统中的真实用户名和密码。〔83〕但个人信息与普通数据的最大区别就在于其具有"可识别性",能识别特定的个人身份。因为只有那些能识别特定个人的信息,才具有侵犯隐私权与信息自决权的风险,应成为个人信息法的保护对象;而无法或者难以识别特定个人的信息,则应作普通数据予以保护。〔84〕据此,高考志愿、考试成绩等信息虽然与特定个人相联,但不具备"可识别性",应视为普通数据,对之加以侵害的行为应认定为数据犯罪。〔85〕而具有"可识别性"的个人电子数据则应属于"公民个人信息",对之加以侵害的行为应构成侵犯公民个人信息罪。

其次,侵犯具有"财产属性"数据的行为应构成财产犯罪。具有"财产属性"数据的显着特征是具有经济价值和权利可转移性。〔86〕因为"可以以金钱来出让或转变为金钱",具有交换价值和使用价值,应被视为"财产"。〔87〕据此,以数据为载体的网络虚拟财产(主要是货币类网络虚拟财产和装备类网络虚拟财产)和储存于计算机信息系统中的手机靓号、优质车辆号牌、电信资费套餐等,应视为网络财产性利益来加以保护。数字时代上述网络财产性利益的产生、利用、交易中所体现的利益形态和财产价值已不言而喻,财产制造者的财产权应受到法律保护。〔88〕实践中应警惕忽略数据的"财产属性"而径行依据数据载体将相关侵害行为认定为数据犯罪的做法。

---

〔81〕 参见浙江省杭州市滨江区人民法院(2014)杭滨刑初字第 106 号刑事判决书。

〔82〕 参见杨志琼:《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》,《法学评论》2018 年第 6 期,第 188 页。

〔83〕 参见江苏省南京市鼓楼区人民法院(2011)鼓刑初字第 123 号刑事判决书。

〔84〕 参见黄翰义:《自直接识别性及公共利益之观点论个人资料保护法之缺失》,《裁判时报》2015 年第 31 期,第 76 页。

〔85〕 参见辽宁省阜新市细河区人民法院(2015)阜细刑初字第 00001 号刑事判决书;山东省菏泽市曹县人民法院(2016)鲁 1721 刑初 515 号刑事判决书。

〔86〕 参见李爱君:《数据权利属性与法律特征》,《东方法学》2018 年第 3 期,第 68 页。

〔87〕 [德]卡尔·拉伦茨著:《德国民法通论(上)》,王晓晔等译,法律出版社 2003 年版,第 305 页。

〔88〕 参见季境:《互联网新型财产利益形态的法律建构——以流量确权规则的提出为视角》,《法律科学》2016 年第 3 期。

最后,侵犯具有“创造性”数据的行为应构成知识产权犯罪。数字化时代网络知识产权大多以电子数据的形式予以存储、利用,因而容易导致“数据”与“知识产权”混淆不清。但网络知识产权和普通电子数据存在显著区别,其创造性,既非现有产品的简单重复,也非对现有事物的客观描述和记录,而是必须在选择和编排上具有创新性和突破性。〔89〕 网络知识产权主要包括:其一,具有“独创性”的网络著作权客体。“独创性”是指受著作权法保护的客体必须是作者智力劳动创作出来的,而非抄袭他人作品,也非将公共领域的作品据为己有或对现有事实的重复描述。〔90〕 典型的是作者通过智力劳动创造出来的电子课程视频、网络游戏源代码等,对之加以侵害的行为应构成侵犯著作权罪。而那些不具有“独创性”的数据,如考试成绩数据库、考试志愿数据库、环保监测数据库等,通常以简单易识别的方式进行编排、储存,难言“独创性”,只能视为普通数据加以保护;其二,具有“秘密性”“价值性”的商业秘密。商业秘密是指不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息。商业秘密作为智力创造成果,其特有的信息性、保密性、未公开性、实用性决定了其应与著作权、商标权、专利权等一样作为知识产权加以特别保护,对之加以侵害的行为应构成侵犯商业秘密罪。

值得注意的是,数据表征的数据安全法益和传统法益之间是非此即彼关系,而非包容关系,这决定了数据犯罪与传统犯罪在法条关系上呈现出中立关系,而非竞合关系。对于一个侵犯数据的行为,因为作为犯罪对象的“数据”具有单一性,只能评价为一罪。其要么侵害了数据表征的数据安全法益而构成数据犯罪,要么侵犯了数据表征的传统法益而构成传统犯罪,而不可能同时对“数据”进行多次法益评价,认定为数据犯罪、传统犯罪等不同罪名进而适用法条竞合〔91〕或想象竞合犯〔92〕。

五 结 语

近年来,新型数据犯罪案件的接连发生昭示着我国数据犯罪研究时代的到来。尤其是民法总则对“数据”作出了宣示性规定之后,〔93〕刑法对数据犯罪的研究意义并非仅关照刑法法域之内,同时对其他部门法也具有关照、回应意义。而已被大陆法系国家多次探讨的数据犯罪,在我国却面临立法独立性上的先天不足和后天数字化技术识别的难题,其保护法益和规范体系被传统计算机犯罪体系所遮蔽,在应对新型数字化犯罪技术时一筹莫

〔89〕 这里的“创造性”是对不同类型知识产权客体的高度概括,因为不同知识产权客体的创造性要求并不完全相同。专利权要求发明具有“技术先进性”,著作权要求作品具有“独创性”,商标权要求商标具有“易于区别性”。参见吴汉东主编:《知识产权法学》(第六版),北京大学出版社 2014 年版,第 15 页。

〔90〕 参见吴伟光著:《网络环境下的知识产权法》,高等教育出版社 2011 年版,第 32 页。

〔91〕 参见任彦君:《网络中财产性利益的刑法保护模式探析》,《法商研究》2017 年第 5 期,第 120 页。

〔92〕 参见陈陶麟、潘安民、郭敏:《“撞库”类网络侵犯个人信息犯罪的刑法规制——以最高法、最高检〈个人信息司法解释〉为视角》,《“新时代刑事法治的理论前沿及司法适用”江苏省法学会刑法学研究会 2017 年年会论文集》,第 518 页。

〔93〕 《民法总则》第 127 条规定:“法律对数据、网络虚拟财产的保护有规定的,依照其规定。”

展。本文以数据安全法益为中心,将其纳入数据犯罪的构成要件之中。以数据安全的不同需求来界定“数据”类型;以数据安全的不同侵害侧面来界定数据犯罪的行为要件;以数据安全法益侵害程度来界定“数额”“情节”等入罪标准。最终,数据安全法益较之于传统“计算机信息系统安全”法益的卓越性,在于能通过实质解释促进数据犯罪规范体系与技术规则的深度融合,消弭数据犯罪中技术评价与刑法评价的分歧。在此基础上,本文进一步强调以数据安全法益的界分功能厘清数据犯罪的内部边界与外部边界。以数据犯罪帮助行为的正犯化规定厘清数据犯罪与其他计算机犯罪之间的界限;以数据的所表征不同法益厘清数据犯罪与传统犯罪界限,最终合理限定数据犯罪的适用范围。

[本文为作者主持的2018年度江苏省社会科学基金一般项目“网络空间治理的‘双维’刑事政策研究”(18FXB009)的研究成果。]

[**Abstract**] It can be found by sorting out the judgments of data crimes in China that, the legalization of data crimes protection in China is unclear, which has led to the problem of interpretation and boundary of data crimes. This stems from the “congenital deficiency” in the independence of data crimes’ legislation and the obstacles to the recognition of technology nowadays. As a result, the data crimes protection legal interests and normative system are obscured by the traditional computer crime system, and it is difficult to eliminate the differences between technical evaluation and normative evaluation in data crimes. The judicial application of future data crimes should be separated from the traditional computer crime system, and the data security (CIA) should be used to reproduce the constituent elements of data crimes, in order to promote the deep integration and evaluation of data crime norms and technical rules, and to clarify data crimes borders with other computer crimes and traditional crimes, to reasonably determine the scope of application of data crimes.

(责任编辑:贾　元)