·法学研究·

DOI:10.20004/j.cnki.ujn.2024.03.014

数据安全的法律保护立场与刑法回应

李怀胜

(中国政法大学 刑事司法学院,北京 100088)

[摘　要]数字时代"数据安全"概念的确立是多元价值维度参与的结果。数据安全和数据效率共同服务于数据发展的整体目标。前置法中数据安全的动态性、局限性和相对性等特征决定了数据安全法益刑法保护的谦抑性。数据安全的前置法律立场是我国刑事司法治理思路的基本遵循。然而我国刑事司法实践未能完全契合国家数据发展的整体导向,在一些新型数据不正当竞争案件中存在选择性执法、入罪说理薄弱、罪名选择困惑等问题。刑事司法对数据不正当竞争行为的过度介入推高了企业的合规成本,可能损害产业的竞争活力,在规范层面也存在可检讨之处。刑事司法应当回归数据安全法律保护的本源,坚持以包容审慎为导向的数据犯罪刑事政策,并在法秩序一体化立场的指导下,处置好数据犯罪违法性的依附性与独立性的关系,给予数据安全犯罪有效的出罪空间。

[关键词]数据安全;数据犯罪;数据犯罪治理;包容审慎;法秩序一体化

[中图分类号]D924.3　　[文献标识码]A　　[文章编号]1671-3842(2024)03-0150-14

在全球范围内,运用数据推动经济社会发展、完善经济社会治理已成为大势所趋。2015年我国颁布的《促进大数据发展行动纲要》统筹规划了新一代的数据基础战略,全面推进数据发展、数据效率提升以及切实保障数据安全。2021年9月1日起施行的《中华人民共和国数据安全法》(以下简称"《数据安全法》")第二章专章讨论"数据安全与发展",将数据安全与发展作为数据开发利用和技术研究的根本坚持。为维护数据安全,保障数据产业发展,我国刑事司法实践不断探索数据安全刑法保护的强度和力度,创造了各类数据安全犯罪"第一案"。然而,这类数据犯罪中的"标杆性"案件收获的并不完全是掌声①。需要追问的是,针对各类新型数据不正当竞争和数据违法行为,刑事司法究竟是该以能动司法的理念主动发挥刑法的社会治理功能,还是坚持司法谦抑,赋予数字经济自我修复的空间和时间?本文探讨了前置法中数据安全的内涵以及多元价值维度,进而分析了我国数据安全犯罪司法实践中的若干困境,并提出数据安全法律保护立场对刑事司法的约束路径。刑事司法不是封闭的规则系统,数据安全犯罪的治理策略和成效评估,应当以前置法中数据安全的基本理念和价值维度为评判尺度,数据安全犯罪治理既要保证数据安全的基本底线,又要防止因司法的过度裁判而扼杀数据产业的创新活力。

一、数据安全的内涵及其多元化价值

在新型产业结构下,海量数据为促进数字经济的发展和推动国家创新水平的提升锻造了崭新契机和强力引擎,但在数据生命周期实现价值输出的过程中也面临着各类风险。在充分认识到数

[基金项目]国家社会科学基金一般项目"人工智能时代算法安全的刑法保障研究"(项目编号:22BFX048)。

[作者简介]李怀胜,中国政法大学刑事司法学院副教授,法学博士,邮箱:lihuaisheng2002@163.com。

①冀洋:《网络黑产犯罪"源头治理"政策的司法误区》,《政法论坛》,2020年第6期。

据所带来机遇与风险并存的基础上，数据安全问题逐渐受到重视，数据安全概念在我国法律体系中逐步得以确立，并不断丰富和拓展出新的内涵和多元化价值维度。

（一）“数据安全”法律概念的确立

数据作为新时代的支配性生产资料，已成为国内外各大经济体可持续发展、国家和社会进步的重要支撑，而数据安全是保障数字经济发展、数字产业腾飞的基础和重要支柱。

1. “数据安全”规范的确立

从时间轴来看，“数据安全”的概念随着网络技术的迭代和场域的扩大在我国规范性文件中逐步确立。在互联网发展初期，我国仅初步意识到计算机系统安全的重要性，此时的计算机系统安全并无专有的“数据安全”概念。1994年发布的《计算机信息系统安全保护条例》第3条规定：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”随着中国信息化进程的加速，数据安全逐渐成为专有性概念，并被部分规范性文件、法律法规所独立表述和确定。例如，原劳动和社会保障部2006年公布的《关于进一步加强劳动保障数据安全管理的通知》在标题中突出了“数据安全”这一概念，要求保障全国劳动保障信息系统建设安全，重视数据安全管理工作；2015年施行的《国家安全法》第25条明确提出，要“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”。但此时信息和数据概念在法律表述中存在两者互相指代的混用现象，包括信息与数据互相包含、信息与数据并用的情形。前者如2005年施行的《电子签名法》第2条第2款，后者如工业和信息化部2010年出台的《通信网络安全防护管理办法》第2条第3款。信息与数据的混用代表着两者在词义和内涵上较为相似，附随的是“数据安全”与“信息安全”的互用。但随着经济数字化、政府数字化改革的驱动，信息与数据的区别愈来愈大。根据国际化标准组织（ISO）的界定，区别于信息是“在特定语境下对特定客体的具有特定含义的知识，例如事实、事件、事物、过程、思想、概念等”[①]，数据是“一种便于交流、解读和处理的，并可重复展现的信息表现形式”[②]。数据和信息因为具有介质的高度依存性而造成混用，但数据在表现性质、依存关系和运行规律上与信息均有所区分[③]。在网络场域内，以二进制代码为主的数据借助特定介质即可通过服从于网络场域内的数字技术运行规律进行跨地理、跨组织和网络域的流动和传递。在数据跨境流动极为频繁的新时期，数据安全问题愈发凸显，具有了区分于信息安全进行独立表述的紧迫性和必要性。2021年施行的《个人信息保护法》仅对违反该法的信息处理活动引起的“信息安全”威胁予以规范，并无包含数据安全的相关表述。与之相对应，《数据安全法》对数据安全的独立地位进行了明确和强化，为数据安全的统筹落地描绘了基础、系统和全面的框架。

2. 数据安全特性的演化

在数字化时代，随着数据作为经济增长引擎在我国国民经济生产要素中的深度嵌入，其有着从静态存储、调配向动态流动、利用的认知转变，以及朝着秩序价值与效用价值并重的价值取向演化的趋势。在认知上，我国对数据安全的认识和理解逐渐从静态安全走向动态安全，并体现在数据犯罪法益的动态化、数据流动和跨境传输的管理两个方面。

（1）对数据犯罪法益模式的认识。在新网络安全形势下，数据泄露事件层出不穷，数据安全的保障场域逐渐从可控的物理边界转为难以防范的技术边界。数据的特性，即流动性、重复利用性和

①Information（2121271），ISO/IEC 2382：2015（en）Information technology Vocabulary，https://www.iso.org/obp/ui/fr/#iso：std：iso-iec：2382：ed-1：v1：en，2020.06.25.

②Data（2121272），ISO/IEC 2382：2015（en）Information technology Vocabulary，https://www.iso.org/obp/ui/fr/#iso：std：iso-iec：2382：ed-1：v1：en，2024.04.15.

③梅夏英：《信息和数据概念区分的法律意义》，《比较法研究》，2020年第6期。

广域性决定了数据在生命周期的流动过程中承载着个人、组织、社会以及国家的多方利益,指向的法益侵犯更加动态化。《数据安全法》的制定和完善,有效整合了分散在《计算机信息系统安全保护条例》《电子签名法》等各个规范性文件中的数据安全规范,并对我国面临的数据的收集、存储、处理和传输等贯穿数据生命周期环节的安全威胁做出相应规定,从而实现数据的有序流转和动态保护。前置法《数据安全法》的实施,也为刑法层面规制数据犯罪问题提供了依据。《刑法》第285条规定的非法获取型犯罪和第286条第2款规定的破坏型犯罪,对于数据收集、传输、存储、以及使用等全生命周期环节的部分社会危害性较大的犯罪风险予以规制,以维护动态的数据处理安全。

(2)对动态数据的流动管理。随着信息技术的发展,数据的流动和跨境传输日益频繁,涉及国家间、企业间以及个人间的数据交换,跨境、跨领域的共享流动导致的安全风险逐渐扩大。我国十分重视数据流动和跨境传输的安全管理工作。《数据安全法》在宏观指导和微观管理层面上均作出规范,前者要求建立健全统一的数据分类制度、数据安全审查制度和出口管制制度以应对数据跨境、跨域传输的风险,尤其是建立实时监测和响应机制。通过数据安全事件的通报和处置机制及时发现和应对数据安全事件,有效防范和减少数据安全风险。后者要求在传输过程中的数据安全保障不仅仅局限于数据的静态存储和处理,还需要考虑数据在传输过程中包括加密传输、访问控制等具体安全问题,以综合保障数据的动态安全。

在价值取向上,数据安全承载的价值呈现多元化。数据保护的价值性不再局限于数据本身,部分政务数据、遗传数据等高敏感数据及数据集合的损害会严重破坏社会秩序和个人权益。数据的安全保障表征数据的秩序价值和效用价值,两者的耦合关系使跨系统的数据效益得以产生。从结构性视角出发,数据有着流动导向的网络化数据秩序,即数据通过网络连接,满足用户的数据需求或公共秩序供给。在一个相对稳定的数据秩序中,社会主体通过再生产和价值输出,服务更广义的价值体系[①]。对于拥有秩序价值的数据,保护其安全性有利于发挥其在经济社会中的重要作用。《数据安全法》规定,为保障数据"依法有序",有必要采取措施保护数据安全,以促进以数据要素为中心的数字经济发展。2022年12月,中共中央、国务院《关于构建数据基础制度更好发挥数据要素作用的意见》(以下简称"《数据二十条》")明确了若干制度性配套措施,对数据产权、数据流通与交易、数据收益分配以及数据要素治理四个领域建立数据基础制度,以维护数据的市场发展规律和数据的安全保护、有效利用、合规流通等整体秩序[②]。数据的效用价值指的是数据被有效利用所产生的价值,包括数据用于决策、分析、创新等方面的价值。数据本身拥有一定的价值,但如果数据没有被有效利用,即没有被转化为对组织或社会有益的信息或行动,那么不存在有实际效用价值的数据,就没有保护的必要性。概言之,数据安全既关注数据的秩序价值,也关注数据的效用价值。对于具有秩序价值且被有效利用的数据,我国通过制定政策、加强关键信息基础设施建设和利用技术等手段保护其安全;而对于没有效用的数据,则无需投入过多资源,仅需要重视对有实际价值的数据的安全给予保护和管理。

(二)数据发展、数据效率与数据安全的体用之辨

为有效发挥我国海量的数据规模和丰富的数据应用场景优势,充分激活数据要素潜能,有必要在数据管理和应用中,根据其内在逻辑,对数据发展、数据效率和数据安全三者进行有重点的概念厘清和梯层配置,以更好地理解和应对数据管理的风险挑战,实现数据管理流程的立体化、系统化。

1. 数据发展、数据效率与数据安全的概念厘清及功能区分

在数字经济中,数据的有效流转带来个人效益和社会效益的提升,从而能够最大限度发挥数

①胡凌:《两种数据秩序及其法律回应》,《社会科学》,2023年第4期。

②中共中央 国务院:《关于构建数据基础制度更好发挥数据要素作用的意见》,https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm,2024.04.03.

据的价值属性。在数据的管理和应用过程中，数据发展、数据效率以及数据安全是三个关键方面，有着服务于自身数据和市场运行等深层次的功能。

（1）数据发展。根据2015年国务院印发的《促进大数据发展行动纲要》整体内容的相关阐述，数据发展指的是数据自身的增长、积累和演变过程，包括数据量的增加、数据类型的丰富和应用场景的扩展，并通过这一生产要素的网络化共享、集约化整合、协作性开发和高效化利用，以支撑政府企业、经济产业以及民生的服务能力和产业发展的过程[①]。高质量的数据发展不仅能够持续性降低信息不对称，打破“信息孤岛”而促进主体间的共享互用，释放价值红利，更使得社会和组织体突破时间和空间的限制促进数据处理者之间的技术共享、创新研发，提升经济高质量发展，进而促进国家治理体系和治理能力的现代化。

（2）数据效率。根据《数据二十条》相关内容的表述[②]，数据效率指的是数据在其全生命周期内的获取、处理、分析和应用等环节的效率，目标是提高数据的利用率和价值创造能力，使数据能够更快地被转化为对各主体以及产业业务有益的信息和洞察。

（3）数据安全。对于数据安全，根据《数据安全法》第3条规定：“数据安全，是指通过采取必要措施，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状态的能力，”这里的“有效保护”和“合法利用”为的是保护数据免受未经授权访问、篡改、泄露或破坏的风险，防范他人通过数据处理活动危害国家安全、公共秩序和他人的民事权益。

概言之，数据发展强调的是持续性的数据价值创造、实现和利用，数据效率旨在促进数据资源的充分开发和利用，提升产业业务发展和个人决策的处理效率。数据安全则是为了保护数据的秩序价值和效用价值，防止数据受到损害或滥用，强调数据保护和风险管理，从而维护个人权益、市场运行以及国家安全等利益。

2. 数据发展、数据效率与数据安全的梯层配置

数据发展在促进数据产业创新和经济社会进步的同时，反映了技术发展下的效率提升、以及安全与发展的体用之辩。“体”是根本，“用”从属于体，这里的“体”与“用”，指的是数据管理与应用的本体目的即“数据发展”，以及发展中的重要外在表象即“数据效率”和必要保证即“数据安全”。

（1）数据发展是数据安全法律保护的根本目标。数据安全与数据发展之间具有十分紧密的内在联系。通过制定和完善数据安全法律，可以规范数据的收集、存储、使用和流通等行为，还可以防范数据安全领域的算法黑箱等内生性风险和数据泄露等外部性风险，从而为数据的规范性发展提供坚实的法律框架和规范保障。《网络安全法》《数据安全法》《个人信息保护法》的相继施行，构建起数据安全领域的“三驾马车”和安全防护网。其中《数据安全法》第13条明确规定：“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”。这里强调了数据发展的重要性，并将其作为该法的核心目标。数据发展事实上已成为数据安全法律保护的重要出发点和落脚点。此外，数据发展是一个动态演进的过程。随着技术的不断进步、数据价值的动态变化以及应用场景的不断拓展，数据安全面临的风险与挑战会不断变化，数据安全法律规范性文件的出台应与数据的风险应对与时俱进，应不断适应新的数据发展需求和挑战，以确保数据在发展过程中始终得到充分的保护。

（2）数据安全与效率是数据发展的有机组成部分。数据发展离不开数据安全的保障作用和数据效率。数据安全确保了数据处理过程的“三性”（即数据的机密性、完整性、可用性），是数据有效

---

①国务院：《关于印发促进大数据发展行动纲要的通知》，https://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm，2024.04.03.

②国务院：《关于印发促进大数据发展行动纲要的通知》，https://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm，2024.04.03.

利用和价值创造的前提。数据效率则代表着数据处理和应用的时效性,是数据发挥价值的关键。对于数据安全与数据发展的关系,数据安全是保障数据发展的前提和基础。在数据管理和应用的过程中,首先,要确保数据的安全性。没有市场要素规则、立法保障等数据安全保护机制,数据处理活动可能会存在数据损坏、泄露或滥用等巨大风险,进而影响到数据的处理效果和价值输出。值得注意的是,数据领域没有绝对的安全,数据海量递增、重复利用等特性决定了数据处理活动的动态性和复杂性,只有在实时性的数据发展过程中解决安全问题,才能维护数据的秩序价值和效用价值。换言之,保护数据安全的目的最终是为了保护数据发展中的数据价值与衍生利益,如果没有实实在在的利益,就没有实施数据安全保护的必要。其次,技术进步带来的数据效率提升体现了数据生产理念和技术方法的变革。数据处理者通过数据流促进数据周期各个环节的高效贯通、优化数据处理和分析流程、提升数据分析技术和工具的使用效能、促进数据价值的深度挖掘和高效发挥,通过数据要素潜能的激活实现数据发展。与此同时,数据效率的提升也有助于加强数据安全,因为高效的数据处理和应用活动可以减少数据在传输、存储和使用过程中所致风险的暴露时间,从而降低被攻击、被滥用的可能性风险。

从数据安全的确立立场以及数据安全、数据效率与数据犯罪的辩证关系可以看出,数据安全具有动态性,随着时代的发展,其内涵不断发展变化。数据安全具有附属性,它从属于数据发展的整体目标;数据安全具有相对性,它有具体存在的语境。总之,不宜对数据安全秉持过于刚性的立场,为了一时的、表层的安全而忽视了数据发展的长远利益,最终也会让安全荡然无存。

二、数据安全犯罪的刑法应对之偏差

回顾前置法中数据安全概念的确立历程与价值导向,数据安全是皮囊,数据发展是内核,数据安全法律体系的确立最终是为数字经济和数字发展服务的。当前数据安全与国家利益、产业秩序等出现了更为密切的绑定,安全不再是事物自发自为的有序状态,而是带有国家主动建构和有意引导的价值,这更强化了刑法保护的必要性,数据安全犯罪概念应运而生[①]。它的提出既是学术界回应现实罪情发展的理论自觉,又是司法实践的实时映射。数据安全犯罪作为法定犯具有国家行政监管的需求,因此数据安全犯罪的刑事司法立场、思路与策略,应当自觉对标数据安全的上位法律。上位法律确立的数据安全的价值维度是数据安全犯罪的参照尺、坐标系。令人遗憾的是,我国司法实践在数据安全犯罪上的若干应对策略未能完全契合数据安全产业发展的客观需求,从而与数据安全法律保护的诉求存在龃龉之处。在网络互联互通的背景下,司法裁判的对象或许是地域性的,其影响却一定是全国性的。

(一)数据安全犯罪的刑法应对之偏差

近年来的网络法治建设,无论是在立法领域还是司法层面,“安全”都占有浓墨重彩的一面。立法领域的数据安全犯罪体系和司法层面的数据安全犯罪治理实效,保障了网络发展的行稳致远,同时也划定了网络安全的基本底线。但网络时代安全问题的复杂性在于,网络的快速变动性与立法的恒常稳定性存在突出矛盾,因为往往不待立法者对某类网络无序或者违法行为展开有效回应,这类行为可能就已很快销声匿迹或者异化为其他违法行为了。例如,立法者曾经慎重考虑过将“人肉搜索”入罪化[②],不曾想理论上的入罪合理性讨论尚未完全展开,“人肉搜索”的声浪很快就衰

①“数据安全犯罪”的类型范围,理论上存在不同认识,但学者们一般将数据安全犯罪和数据犯罪等同视之。参见喻海松:《数据犯罪刑法规制模式的现状评析与未来展望》,《法学杂志》,2023年第5期。

②郑赫南:《“人肉搜索”缘何没入罪》,《检察日报》,2009年3月1日第3版;李怀胜:《刑事立法的国家立场》,北京:中国政法大学出版社,2015年版,第7页。

落了。在基础规则和底层规范缺失的背景下，司法的果断亮剑，有助于快速确立网络社会的规则意识，并为后续立法积累先决性的司法经验。这也是网络法治领域不乏各类网络司法“第一案”的重要原因。

1. 司法能动还是刑法谦抑：规范失灵下的选择执法

在从传统经济向数字经济转化的过程中，新型的产业形态不断出现。新兴产业发展必然带来新型产业风险，新型产业风险产生新型治理难题。客观上讲，成熟于农业社会完善于工业社会的传统刑法理论在信息化时代下面临着整体性滞后，这包括对新型互联网犯罪的理论解释力度不足，一次应对失措往往造成极其不良的社会后果。就如案发于2013年的快播案件，一度让“技术无罪论”成为部分网络黑灰产业链从业者的挡箭牌，同时也引发了理论界关于平台责任、电子取证等话题的诸多讨论[①]。

在新兴业态监管中，刑事司法的困境主要在于：当面临新兴业态的重大安全风险时，选择司法能动还是刑法谦抑，缺乏清晰可操作的标准。既然是新兴业态，必然缺乏足够的底层法律规范，存在较大的监管空白，由此司法机关掌握着巨大的自由裁量权。司法机关的判决对类似案件的处理往往将造成巨大影响。以近年来受到广泛关注的网络爬虫案为例。网络爬虫可以批量化处理和搜集信息，是网络浏览器和搜索引擎必备的工具。网络爬虫本来是中性的技术工具，但是在特定情况下可能构成侵权或者违法。在由中立技术应用向民事侵权转变的标准性案件即“酷米客案”中，法院查明，自2015年到2016年，武汉元光公司为提高本公司开发的实时公交到站信息软件“车来了”APP的准确性，指使本公司员工运用爬虫技术盗取竞争对手“酷米客”APP的数据并运用到本公司软件中。法院经审理后认为，“元光公司利用网络爬虫技术大量获取并无偿使用‘酷米客’APP实时公交信息数据的行为，是一种不劳而获的行为，破坏他人的市场竞争优势，具有主观过错，违反了诚实信用原则，扰乱了竞争秩序，构成不正当竞争”[②]。据笔者了解，最初司法机关一度希望以刑事犯罪处理本案。而在所谓的网络爬虫第一案中，法院认定，上海晟品网络科技有限公司的主管人员破解北京字节跳动科技有限公司的网络防护措施，爬取该公司服务器中储存的视频，给北京字节跳动公司造成了2万元人民币的损失。法院认为，被告“使用了伪造Device_id绕过服务器的身份校验，伪造UA及IP绕过服务器的访问频率限制等规避或突破计算机系统保护措施的手段获取数据，构成非法获取计算机信息系统罪”[③]。但问题在于，只要是不法的数据爬取，一定妨碍了原服务器的访问权限，从而侵犯了对方的数据保密性，这既可能是侵权行为，也可能是犯罪行为，但法院的判决书并没有清晰说明网络爬虫的罪与非罪的界限。因此，网络爬虫入罪第一案尽管受到理论界和实务界的极大关注，却没有形成示范性的裁判规则。在此后各地法院的处理中，多数法院继续按照反不正当竞争案件处理。在选择以刑事案件处理的案件中，有的地方法院仍按照侵犯公民个人信息罪处罚[④]。究竟按照刑事案件还是民事案件处理，起决定作用的往往是对各种案外因素的考量。

2. 严格解释还是扩张适用：新型案件中的入罪之惑

对于具有明显的或者严重危害性的案件，入罪化的共识很容易达成，但是在罪刑法定原则的约束下，司法机关依然要履行全部的说理和论证义务。究竟是选择严格解释下的无罪处理还是扩张解释下的入罪化，依然是对司法智慧的巨大考验。例如，在“人脸数据刑事第一案”中，“原判认定，2018年7月份开始，被告人张某、余某飞等人以牟利为目的，利用已非法获取的公民个人信息，通过使用软件将相关公民头像照片制作成公民3D头像，从而通过支付宝人脸识别认证，并使用上

①谢登科：《论电子数据与刑事诉讼变革：以“快播案”为视角》，《东方法学》，2018年第5期。

②参见广东省深圳市中级人民法院（2017）粤03民初822号民事判决书。

③参见北京市海淀区人民法院（2017）京0108刑初2384号刑事判决书。

④参见杭州市西湖区人民法院（2020）浙0106刑初437号刑事判决书。

述公民个人信息注册支付宝账户。张某、余某飞等人通过这种方式来获取支付宝提供的邀请注册新支付宝用户的相应红包奖励(包括邀请新人红包、通用消费红包、花呗红包等)。”法院判处张某等人构成侵犯公民个人信息罪[①]。在笔者看来,法院的判决结果明显属于类推,超越了侵犯公民个人信息罪的应有界限。依照《数据安全法》第3条的规定,“数据处理,包括数据的收集、存储、使用、加工、传输、提供、公开等”,可见,数据的全生命周期至少包括这7个阶段,但依照《刑法》“第253条之一”的规定,侵犯公民个人信息罪的行为方式包括出售、提供、窃取及非法获取四种,实质是两种行为方式,即不法提供和不法获取。另外,《个人信息保护法》第13条规定了个人信息合法处理的7种情形,其中第一种情形为“征得个人同意”。在本案中,张某等人获得的他人头像信息均是通过网络渠道公开检索和自行下载的。对于此类任何人均可以通过公开渠道收集和检索到的个人信息,应推定为个人已许可他人在不违背公序良俗和不侵犯第三方利益的情况下进行收集、存储和传输,否则将造成公共信息资源的萎缩。甚至电影明星、政客等公众人物还特意发布个人视频、图像资源,以供社会公众传播和欣赏。诚然,依照《个人信息保护法》第29条,“处理敏感个人信息应当取得个人的单独同意”,但是侵犯公民个人信息罪仅处罚个人信息的不法流转,它既不处罚个人信息的不法收集,也不处罚个人信息后续的不法利用。因此,法院的判决不当扩大了本罪的适用范围。

此外,在其他一些网络不正当竞争行为如流量劫持、流量造假、刷机中,有的地方司法机关按照民事侵权不正当竞争行为处理,有的地方司法机关按照犯罪处理。即使同一地区的不同司法机关,案件定性也可能存在差异。

(二)数据安全犯罪的刑事司法应对偏差之因

诚然,司法裁判不是简单的对症下药。司法裁判活动是将抽象的、一般性的法律规则变成具体的、个案的裁判规则的过程,期间是政策、经济、文化、心理等诸多因素共同作用的结果。法律适用不是机械照搬法律条文,而是通过在现实和规范之间的来回关照、进行反复法律推理,由此获得最妥当的结论。法律的含义确实“应稳定在一定的区域内,否则,法律将失去作为行为尺度的作用”[②]。在刑事司法中,对法律确定性有更高的价值追求,但法律内外的多重因素导致了司法适用结果的偏差。

1. 技术规则与法律规范之间的错位

在网络时代,社会结构的升级以技术驱动为推进力量,因此,新兴技术及其产生的风险贯穿社会治理的全过程[③]。快速迭代的网络底层技术以及变动不居的网络犯罪类型是网络犯罪的鲜明特色。在网络的不同发展阶段,网络犯罪都有其各自特色。在网络1.0时期,网络犯罪体现为对大型计算机信息系统的侵害;在网络2.0时期,网络犯罪体现在以网络为犯罪工具;而在人工智能时代,网络犯罪体现在线上线下的双层融合和弥散化。刑事立法和刑事司法要有效应对网络犯罪,首先要把握网络犯罪的脉搏,挖掘犯罪与技术的互动规律,明晰犯罪的技术特征。“实现网络犯罪刑事对策现代化的必经之路是深度融合法律规范与技术规则,真正做到技术为法律所用”[④]。当前在网络犯罪尤其是数据安全犯罪领域,技术规则与法律规范之间的错位,很容易导致网络犯罪罪名选择的随意性。北京市某司法机关办理的“星援APP案”中,被告人蔡某苗制作并出售星援APP,粉丝利用星援APP可以不限次数地对心仪的明星打榜,点赞。星援APP突破微博的加密算法,对微博设定的数据搜集功能造成干扰,破坏了微博的转发机制。法院经审理后认为,被告人蔡某苗构成提供侵入计算机信息系统程序罪,判处有期徒刑5年,并处罚金人民币10万元,同时追缴其所有违法所

①参见浙江省衢州市中级人民法院(2019)浙08刑终333号刑事裁定书。

②周永坤:《错案追究制与法治国家建设——一个法社会学的思考》,《法学》,1997年第9期。

③刘艳红:《网络时代社会治理迭代升级与犯罪控制协同化的刑事政策》,《社会科学辑刊》,2024年第1期。

④喻海松:《网络犯罪二十讲》第2版,北京:法律出版社,2022年版,第20页。

得[①]。但是，本案最初是以涉嫌犯破坏计算机信息系统罪被逮捕的，那么如何在规范层面区分“控制”和“破坏”，两者的技术原理有何不同?在数据安全犯罪中，功能破坏、系统控制和数据失真经常被混为一谈，控制和破坏存在极大的解释空间。只要是损害系统权限的不法行为，都可以被解释进控制型数据安全犯罪和破坏型数据安全犯罪中，这直接导致司法观点的来回摇摆。在某流量劫持案中，被告人施某等人利用职务便利，实施DNS域名劫持，控制某公司的互联网域名系统，导致用户在访问该公司页面时被强行跳转到其他页面。法院认为，施某等人违反国家规定，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[②]。但2018年12月25日最高人民法院发布的第20批指导性案例·指导案例102号·付某豪、黄某超破坏计算机信息系统案中，法院的裁判要旨又认为：“通过修改路由器、浏览器设置、锁定主页或者弹出新窗口等技术手段，强制网络用户访问指定网站的‘DNS劫持’行为，属于破坏计算机信息系统，后果严重的，构成破坏计算机信息系统罪”[③]。可见，最高人民法院和地方法院的观点产生了直接冲突。因而有学者干脆认为，破坏计算机信息系统中的干扰行为与非法控制行为重合，没有单独立法的必要性[④]。也有学者仍然囿于现行立法的框架，坚持通过包括的一罪或想象竞合来处理，将两者当作包容或交叉关系来审查[⑤]。类似的争议，几乎遍布数据安全犯罪的各类案件之中。

2. 逐利性执法支配的非政策性冲动

所谓逐利性执法，是指执法者为了利益违反法律法规和公正原则而执法，执法目的不是为了维护社会秩序和法律尊严，而是为了追逐利益。逐利性执法不同程度地存在于许多地方的行政执法领域，尤其在经济下行时期更加明显。网络犯罪案件的逐利性执法，主要体现在司法机关跨地域查办案件，这种现象与网络犯罪管辖权的急剧扩张有密切关系。司法机关有惩治犯罪的责任和义务，传统空间的犯罪治理责任具有特定性和专门化，即以地域管辖和级别管辖为基础的刑事管辖权制度承担了限定责任范围和明确责任对象的双重功能，但是网络犯罪的跨地域性和时空延展性给传统的管辖权制度造成了直接的冲击[⑥]。一个普通的网络诈骗犯罪，其被害人所在地、犯罪人所在地、服务器所在地可能分属不同区域。2021年施行的《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第2条第2款规定，“针对或者主要利用计算机网络实施的犯罪，犯罪地包括用于实施犯罪行为的网络服务使用的服务器所在地，网络服务提供者所在地，被侵害的信息网络系统及其管理者所在地，犯罪过程中被告人、被害人使用的信息网络系统所在地，以及被害人被侵害时所在地和被害人财产遭受损失地等”，前述司法解释通过扩张传统的地域管辖权来解决网络犯罪的管辖权冲突。而2021年最高人民法院、最高人民检察院、公安部联合发布的《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见(二)》，更是对电信网络诈骗犯罪创设了俗称“沾边管辖”的制度，其本意是解决电信网络诈骗犯罪的并案处罚难题，节约司法资源，但被个别司法机关滥用，竟成为逐利性执法的方便之门。

逐利执法的危害是多方面的。它偏离了刑事司法的固有目的，容易造成冤假错案；容易诱发网络从业者用刑事手段解决民事纠纷；容易污染司法环境，影响司法公正，损害法律权威。

---

①参见北京市丰台区人民法院(2019)京0106刑初1813号刑事判决书。

②参见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。

③《最高人民法院关于发布第20批指导性案例的通知》，http://gongbao.court.gov.cn/Details/fd33e76142bf3ada6cabe0b81dc6d9.html，2024.04.03.

④皮勇：《我国网络犯罪刑法立法研究——兼论我国刑法修正案(七)中的网络犯罪立法》，《河北法学》，2009年第6期。

⑤张明楷：《刑法学》(第6版下册)，北京：法律出版社，2021年版，第1376页。

⑥于志刚：《关于网络空间中刑事管辖权的思考》，《中国法学》，2003年第6期。

3. “刑先民后”下的不良司法惯性

从法律的位阶性原理和责任梯次配置原理出发,刑法理应在其他部门法的规则建构基本到位的情况下,再针对危害后果严重的行为设定相应的罪刑情节,这是刑法作为“最后法”和“保障法”的应有之义。但网络法治领域事实上已走上了一条“刑先民后”的立法探索路径,即在民商事等法律规则长期缺位的情况下,刑法率先建立犯罪体系,利用刑罚的严厉性和对特定行为的专门规制来实现规范意识的传导。例如,1997年《刑法》就规定了侵犯计算机信息系统罪和破坏计算机信息系统罪,而直到2017年6月1日《网络安全法》才生效实施。再比如,2009年《刑法修正案(七)》就规定了侵犯公民个人信息类的犯罪,并在2015年《刑法修正案(九)》将其修改为侵犯公民个人信息罪,而直到2021年11月1日,《个人信息保护法》才生效实施,此时距离《刑法修正案(七)》已过去12年之久。“刑先民后”的立法取向并非一无是处,通过刑罚的“敲山震虎”或可形成暂时的威慑效应,但其弊端也是明显的,即对某些新型的数据安全案件,司法者可能因忽略审查底层法律规则的导向,导致案件判决的社会效果偏离了法律效果。

(三)数据安全犯罪的刑事司法应对偏差之害

德国刑法学家李斯特的名言——“最好的社会政策就是最好的刑事政策”,揭示了犯罪规律与社会治理之间的复杂性,故而被学术界奉为圭臬。犯罪是复杂社会机制作用下的特定产物,其发生和发展受制于复杂的社会变量,对任何单一变量的依赖都无法完成有效的犯罪治理,反映在刑法中就是要避免所谓的“刑罚依赖症”。这种现象也存在于数据安全犯罪,进而导致刑事司法的应对偏差。数据安全犯罪的刑事司法应对的偏差可能产生诸多不良后果。

1. 间接推高企业的数据合规成本

所谓数据合规,是指企业在现有的数据法律、行政法规、国家标准的框架下,建立相应的业务流程配套,以符合法律规定。数据合规有利于推动企业建立科学、规范的数据治理体系,有益于提高企业应对数据内源性风险和外源性风险的能力,最终促进了企业的整体商业价值和市场竞争力的提高。企业的数据合规体系的构成受制于内外多方面因素,除了企业自主性的数据合规意识之外,主要受制于外部的数据安全合规风险。对企业科以责任,应当考虑企业合规的可行性、可信性以及合规成本与收益的均衡性。例如,《反电信网络诈骗法》赋予了平台企业多种义务要求,如用户身份核验制度、风险评估制度等。某些企业为了避免业务风险,不断推高合规标准,导致原本能正常使用的银行卡、电信卡被冻结,而解冻流程又异常繁复。再比如《个人信息保护法》的出台极大提升了我国互联网企业的个人信息保护水平。但是在实际的业务流程中,企业对个人信息的掌握程度与企业应对网络黑灰产的业务能力直接相关。没有有效的用户数据,就无法建立有用的企业风控模型。

2. 可能扼杀新兴产业的创新活力

生命体无时无刻不在裂变与增生,由此才形成了生物的多样性,自然界如此,人类社会也一样。此起彼伏涌现的网络新型产业,不但给经济发展提供了动力之源,也是社会变革的重要推动力量。但既然是新生事物,必然和既有的法律体系产生冲突,也必然和既存的利益格局发生摩擦。对于新生事物一味追求安全,可能会扼杀新的产业生长点。对于网络新型产业的监管,我国整体还是持有宽容态度的,亦形成了产业发展与有效监管的良好互动格局,推动了产业发展和社会进步。例如,共享单车占用了公共路权,网约车也曾诱发了一些违法犯罪现象,但监管者的包容态度最终收获了正向的社会价值[①]。当然更应值得警醒的是一些争议性案件带来的行业负面价值。如在“摩蝎数据爬取案”中,杭州魔蝎数据科技有限公司(以下简称“魔蝎公司”)为国内众多网络金融客户提

①马长山:《智慧社会建设中的“众创”式制度变革——基于“网约车”合法化进程的法理学分析》,《中国社会科学》,2019年第4期。

供精准评分模型、授信评分等信用工具，其业务流程是用户提供网络账号和密码，授权摩蝎公司进入其个人账户，再通过账号中的各类数据判断用户的征信情况并提供给相关公司。但摩蝎公司将其获取的用户个人账号和密码予以留存，法院判决其构成侵犯公民个人信息罪[①]。但是很显然，存储行为不等于获取行为，摩蝎公司属于合法获取+非法留存，但法院却将后续的非法留存直接判定为“非法获取”[②]。司法机关固然想通过对网络风控行业的治理来刹一刹网络小贷的势头，但这也动摇了大数据行业和网络信用行业赖以维系的业务逻辑。对于公开个人信息的使用问题，司法实践的态度摇摆不定，有的法院依照侵犯公民个人信息罪处理[③]，有的法院依照无罪处罚[④]。其实只要对各种工商登记查询平台稍加留意，这些行业的业务模式都是建立在对信息（不限于个人信息）公开使用的基础之上。司法实践的不确定态度时刻给相关行业的发展带来了隐忧。

三、数据安全法律保护立场对刑事司法的约束

我国数据安全犯罪刑事裁判的结果和走向偏离数据安全法律保护的上位立场有其根本原因，即在数据安全犯罪领域未能建立导向性的刑事政策，前置法与刑法裁判之间未能形成有效的规范连接，前置法的价值观念无法有效传递给刑事司法。这导致司法实践自说自话，死板的适用法律导致机械的裁判后果。数据安全犯罪的刑事司法实践回归数据安全法律保护的基本立场，应当以明确的刑事政策作为指导，并在具体的解释路径上妥善处理与上位法的关系。

（一）以包容审慎为导向的数据犯罪刑事政策

理论界关于政策与司法裁判的关系存在正反两方面的观点，否定性的观点认为，“要想在我国真正厉行法治就必须使公共政策逐步淡出诉讼领域，特别是在已有明确法律规定的情况下”[⑤]。而主流观点则认为，“在弥补形式主义司法的局限和推动实质正义的实现中，司法政策具有独特优势”。[⑥]“只有允许刑事政策的价值选择进入刑法体系中去，才是正确之道”[⑦]。因为，刑事政策的功能是在“相对抗的个体利益或社会整体利益与个体需求之间产生冲突时，应该如何进行社会纠纷的处理”[⑧]。刑事政策的价值性在于弥补文本裁判的不足。在数据犯罪治理乃至整个网络犯罪领域，应以包容审慎原则作为调控性的司法政策。

1. 为什么是“包容审慎原则”

国家“发改委”于2017年印发的《关于促进分享经济发展的指导性意见》通知明确要求：“坚持包容审慎的监管原则，探索建立政府、平台企业、行业协会以及资源提供者和消费者共同参与的分享经济多方协同治理机制。”这是“包容审慎监管”首次在规范性文件中提出[⑨]，之后其开始反复出现在各类文件和法律中。2020年5月，中共中央、国务院发布的《关于新时代加快完善社会主义市场经济体制的意见》提出：要求“健全对新业态的包容审慎监管制度”。2021年1月，《法治中国建设规

①参见杭州市西湖区人民法院（2020）浙0106刑初437号刑事判决书。

②刘宪权，石雄：《网络数据犯罪刑法规制体系的构建》，《法治研究》，2021年第6期。

③参见徐州市铜山区人民法院（2018）苏0312刑初字第85号刑事判决书。

④参见重庆市渝中区人民法院（2017）渝0103刑初字第1563号刑事判决书。

⑤袁明圣：《公共政策在司法裁判中的定位与适用》，《法律科学》，2005年第1期。

⑥李红勃：《通过政策的司法治理》，《中国法学》，2020年第3期。

⑦[德]克劳斯·罗克辛著，蔡桂生译：《刑事政策与刑法体系》（第2版），北京：中国人民大学出版社，2011年版，第21页。

⑧国务院：《关于印发促进大数据发展行动纲要的通知》，https://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm，2024.04.03.

⑨王永强：《包容审慎监管视角下平台经济竞争失序的法治应对》，《法学评论》，2024年第2期。

划(2020-2025)》要求探索“包容审慎监管等新型监管方式”。《优化营商环境条例》第55条提出,要对“新技术、新产业、新模态、新模式”实现包容审慎监管。该原则早期针对的主要是共享经济,之后扩展到所有的新经济形态。包容审慎原则作为新经济领域的监管价值在于,它明确了政府与市场的关系,“其要求政府以包容之心对待新经济,给予其必要的发展时间与试错空间,并根据公共风险的大小进行适时适度干预,从而有效破解传统监管所面临的困局”①。在科技驱动下的新经济形态可能存在不成熟、不稳定甚至灰色地带②,如过早介入可能会扼杀新经济的积极因素,使其丧失自我净化和迭代更新的功能。这种观念已基本被各地的监管实践所接受。例如,《吉林省优化营商环境条例实施细则》第31条规定:“对新技术、新产业、新业态、新模式的‘四新经济’实体,只要不碰触安全环境底线,科学设置观察期、给予过渡期、实行保护期,通过包容审慎监管执法方式,引导规范和督促其依法经营。”包容审慎原则何以能够成为刑法规制数据安全犯罪的刑事政策,笔者认为有以下两个理由:第一,数据安全犯罪作为典型的法定犯,其犯罪治理策略自然是受制于顶层法律规范确立的价值导向,不能背离国家对数据安全犯罪所对应产业的政策取向。数据安全犯罪是以数据作为侵害对象的犯罪,对数据犯罪的打击要与国家对数据产业发展的政策目标合拍。而包容审慎作为国家当前对包括数据产业在内的新兴业态监管的一般原则,自然对数据安全犯罪的刑事治理具有制约性。第二,包容审慎原则内涵的发展与安全的辩证关系符合刑法治理数据犯罪的内在气质。包容审慎原则中所谓的包容,是指要客观理性看到新兴业态发展中所暴露出来的安全风险,不能因为新兴业态的某些安全问题受到了舆论的格外关注和放大就惊慌失措,而是要给予新兴业态足够的时间去解决自身的安全风险,不要急于实施法律尤其是刑法的外部规制。包容审慎原则中所谓的审慎,则是对新兴业态的社会价值和存在必要性予以充分评估,既不要因为是新兴业态而过度宽容,也不要因为某业态自诩为“新”就放弃监管、放任自流。而要客观审慎对待该种业态的社会价值、经济价值以及其对传统业态的补强作用,只有该种业态产生了社会积极效果或者有此可能性时,才值得对其安全风险予以适度宽容。

2. 包容审慎原则之于刑法的运用

把包容审慎原则引入刑法,其目的是为了调控刑法规范的机械性,即在形式理性之外为刑法规范注入价值理性的灵魂,使刑法更能符合国家设定的价值目标。“实在法只是提供了一种文本规范,只有保持刑法体系的开放性,即纳入刑事政策层面的评价,才能将文本规范转换为裁判规范,完成裁判之大前提的构建”③。当然,将刑事政策引入刑法,绝不是为了“以策破法”“以策控法”“有策无法”,而是让合法律性论证与合政策性论证相得益彰④。笔者认为,包容审慎原则之于刑法的具体运用需要注意以下两点。

(1)根据底层监管法律判断是新兴业态还是负面业态。新兴业态之“新”体现在符合国家新的产业发展方向、符合新质生产力发展需求、能够产生新的产业生长点,而并非只要是以前不存在的业态就一定是“新”。对于国家明确判定不支持乃至禁止的所谓业态,刑事司法在审查时则可以报之以严格审查的态度。当然,随着时间的推移,国家对某些业态的监管态度可能会发生转变,刑事司法自然也要因时而动。以数字货币为例,数字货币又称虚拟货币、加密货币,是不由货币当局发行的、运用区块链技术发行和交易的数字货币。我国的行政规范性文件有意区分了比特币、以太坊、泰达币等数字货币与英雄币等代币、通证(Token)之间的关系,但是在技术形态上,这类数字货币的技术特性是完全一致的,因此,我国的规范性文件对此作出区分的意义并不大。我国对比特币

①王俊豪等:《中国特色政府监管理论体系与应用研究》,北京:中国社会科学出版社,2022年版,第400页。

②周汉华:《网络法治的强度、灰度与维度》,《法制与社会发展》,2019年第6期。

③张心向:《死刑案件裁判中非刑法规范因素考量》,《中外法学》,2012年第5期。

④崔志伟:《刑法合政策解释的学理表达与规范化路径》,《中外法学》,2023年第5期。

的法律属性以及监管态度存在一个由模糊到明晰，由宽松到严格的转变。早在2013年12月5日中央人民银行等五部委发布的《关于防范比特币风险的通知》提出，比特币“不具有法偿性与强制性等货币属性，并不是真正意义的货币”，但同时也认为“从性质上看，比特币应当是一种特定的虚拟商品”。而随着以比特币为代表的虚拟货币非法融资、集资诈骗活动日渐猖獗，2017年9月4日中央人民银行等七部委发布的《关于防范代币发行融资风险的公告》明确提出：“代币发行融资是指融资主体通过代币的违规发售、流通，向投资者筹集比特币、以太币等所谓‘虚拟货币’，本质上是一种未经批准非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动。”该规定虽然不能直接作为非法经营罪、非法吸收公众存款罪的非法性审查依据，但前置法的态度转变将会直接影响刑事法律对类似案件的判断结论。

（2）对于没有严重危害性的网络灰色产业，应当审查刑事处罚的必要性。网络黑灰产业，是网络黑色产业链和灰色产业链的统称。虽然人们常并称“网络黑灰产业”，但黑色产业和灰色产业还是有所区别的。网络黑产是指法律所明文禁止的产业，例如，通过远程侵入计算机系统或植入木马病毒，批量窃取他人数据信息的行为。而网络灰产是打法律擦边球的产业。这类行为在查处或定性上存在模糊地带，但客观上又具备一定的危害性。严厉打击网络黑产在我国刑法和刑事政策层面都不存在障碍，对于网络灰产则要根据其危害性、行为的违法性等做综合评估。以“乌云网事件”为例，乌云网曾经是国内著名的“白帽子黑客”社区，大量技术能力高超的网络技术人员和程序员在此论坛上交流技术心得。该论坛致力于发现和发布网络安全漏洞并提交各网站，企业用户也可以主动提交自己的平台漏洞。之所以称为“白帽子”，是因为这些技术人员并不以抓取漏洞为不法收入来源，而是将认可感、荣誉感作为追求，故将自己和真正的黑客相区别。该论坛的部分技术人员曾发布国内多家知名互联网企业的高危安全漏洞，引起较大社会反响，但相关公司出于商誉考虑，矢口否认。之后一家公司认为该论坛技术人员侵入其计算机信息系统而向司法机关报案，乌云网最终遭至关闭。该事件在某种程度上标志着国内黑客的网络田园精神和理想情怀的终结。“乌云网事件”引发的思考是，对于善意挖掘漏洞的行为如何建立法律上的免责机制，以建立“白帽子”们与网络厂商有效的技术互动与激励机制[①]。可惜的是相关问题仅停留在学术讨论。目前在网络黑灰产业中，网站漏洞早就成了炙手可热的资源，常常被用于实施网络敲诈勒索和网络攻击等违法犯罪活动，主动向网站告知而不收取回报的行为无异于“活雷锋”。乌云网事件甚至直接促成了《网络安全法》第26条的出台，即“开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。”但应遵守何种国家规定，目前只有入罪规则没有滤罪条款。

（二）兼顾数据犯罪违法性的依附性与独立性

除了在刑事政策上调控数据安全犯罪的惩处范围，使其不过于偏离我国数据安全保护的法律立场之外，刑法规范承担着更重的说理义务。在犯罪判断的阶层理论中，构成要件符合性具有违法性推定机能。为符合罪刑法定的形式理性的侧面，不宜对构成要件附加过多价值判断的功能，否则可能会使犯罪的构成要件判定丧失定型化和规范化的风险。故笔者认为，应当在违法性层面结合法定犯的违法性特征建立数据犯罪的出罪机制。也就是说，通过法秩序一体化的原理实现数据安全犯罪对数据安全法律保护的一般立场的回归。

1. 数据犯罪的违法性判定：缓和的违法一元论

法律规范的功能之一就是以明确的行为规范指引公民的行为。为实现此要求，就需要各部门法相互协调，统一立场，没有冲突和矛盾，这就是法秩序一体化产生的原因。“法秩序统一是指整个国家法律体系内部的协调一致。也就是说，一行为在某个部门法中被规定为违法，则不可能在另外

①徐小康，汪文涛：《漏洞战争：“白帽子”法律之争》，《方圆》，2016年第21期。

一个部门法中被规定为合法,否则必然造成各部门法之间的矛盾"[①]。如果法律为公民提供的行为规范是相互矛盾的,就会造成公民生活的无所适从[②]。因此,对同一行为在不同部门法是否能够得到统一的法律结论,是法秩序一体化的重要内容。罗克辛认为,"违法性领域,人们则要贯彻和履行整体法秩序的任务。按照这一原则,正当化事由可以产生于任何法律的领域,这样,刑法才和其他的法律领域相衔接,并形成统一的法秩序"[③]。尽管刑法学界均认可法秩序一体化的命题,但是在何种程度上实现一体化却争议颇大,大致有严格的违法一元论、缓和的一元论和违法的相对论等观点。

严格的违法一元论认为,刑法与民法等其他部门法的违法性判断要坚持违法判断的统一性,即民法上判断为违法的行为,在刑法上也判断其为违法;同样,在民法上判断为合法的行为,在刑法上也判断其为合法。严格的违法一元论以刑法的附属性为理论预设,要求刑法对民法的绝对一致。这种观点目前支持者寥寥。缓和的一元论和违法性相对论观点类似,都认为前置法合法的行为,刑法上一定作出罪化;前置法违法的行为,刑法上也未必一定入罪[④]。违法性判断的上述理论分歧,源自法秩序一体化是存在论基础上的一体化还是价值论基础上的一体化这一分歧。笔者原则上支持缓和的违法一元论,并且认为,刑法上的违法性判断兼具依附性和独立性。违法性判断的依附性体现在,其他部门法认定为合法的行为,刑法也要阻却犯罪的成立,即使行为具备构成要件符合性的,依然也要在违法性判断中将其排除,否则必然会造成公民法意识的混乱。而在入罪方面,刑事违法性判定对民法和行政法相对分离,具有独立性。自然犯的犯罪与违法的界限只具有量上的程度差异,盗窃200元财物是民事的侵权行为,也是行政的违法行为,但却不构成刑法的犯罪行为;行政犯的违法性需满足两次判断,即前置法的行政违法性和刑事法的刑事违法性,缺少任何一个违法性都无法构成犯罪。

2. 数据安全犯罪违法性依附性与独立性之运用

(1)刑事手段介入要慎重。数据安全犯罪的违法性审查,应当将民商事法律或者行政法律作前置审查,前置法对定性悬而未决或者存有争议的,刑法介入要慎重。以目前争议较大的切条视频为例,切条视频将他人完整的视听作品截取成几分钟的短视频,在此基础上还进行"集成""混剪"等深加工,例如,"五分钟看电影"等等。目前知识产权法学界对此争议很大。独创性元素越多,"短视频"离侵权和犯罪就越远,此时"短视频"是否构成合理使用,是否属于原创的新作品,就更有争议了。如果"短视频"有了明显的独创性,达到了二次创作的程度,就属于演绎作品。一方面演绎者对其新作品投入了独创性成分,对这部分享有著作权。但另一方面,演绎作品是以原作品为基础,对原作品具有依赖性,也很难将其按照侵犯著作权罪追究刑事责任,更重要的是,"短视频"和二次创作视频的界限并不明晰。切条视频目前是否属侵权作品,在民商法领域并没有形成统一意见。在基础民事法律关系悬而未决的情况下,应当慎用刑事手段,避免过早介入,尤其是要避免对个人的泄愤式的惩处进而达到所谓的刑罚威慑效果。刑事违法性的审查,应当在法秩序统一原理支配下,坚持民事审查在先的路径,对于民事侵权属性不明的,慎用刑事手段。

(2)保持刑事司法审查的独立性。仅有行政违法性而无刑事违法性的,不能作为犯罪处理。例如,在数字经济中,良好的商誉成为网络商家赖以生存的命脉和根本。为了打击以诋毁、商誉造假为业的网络黑公关,2013年最高人民法院、最高人民检察院颁布了《关于办理利用信息网络实施诽

①陈兴良:《民法对刑法的影响与刑法对民法的回应》,《法商研究》,2021年第2期。

②吴镝飞:《法秩序统一视域下的刑事违法性判断》,《法学评论》,2019年第3期。

③[德]克劳斯·罗克辛著,蔡桂生译:《刑事政策与刑法体系》(第2版),第22页。

④更详细的论证可参见张峰铭:《法秩序在何种意义上是统一的——对部门法交叉问题的前提性反思》,《东岳论丛》,2022年第4期。

谤等刑事案件适用法律若干问题的解释》,明确了网络背景下侮辱罪、诽谤罪、非法经营罪等罪的适用规则。该解释第7条规定:“违反国家规定,以营利为目的,通过信息网络有偿提供删除信息服务,或者明知是虚假信息,通过信息网络有偿提供发布信息等服务,扰乱市场秩序,具有下列情形之一的,属于非法经营行为‘情节严重’,依照刑法第225条第(4)项的规定,以非法经营罪定罪处罚……。”细究该条,如果说“以营利为目的+发布虚假信息”构成犯罪尚且可以理解的话,那么“以营利为目的+删除(虚假)信息”的危害性会是什么呢?如果说被甲公司雇佣要求删除涉及公司的虚假信息就构成非法经营罪的话,甲公司岂不是也要构成非法经营罪的共犯了[①]。删除信息的行为并没有对应的行政违法性[②]。实际上,所谓的网络黑公关不过是网络不正当竞争的副产品,黑公关充当的是网络打手的角色,其问题的根源在于网络空间尚未建立完善有序的竞争秩序,如果因为底层规则的不完善而“迁怒于”网络不正当竞争的末端链条,相当于又走上了“刑先民后”“杀一儆百”的老路。

四、结 语

数字技术的快速发展与广泛应用推动人类社会由知识经济向数字经济的转型,同时引发深刻而热烈的社会整体性变革。在此背景下,发挥刑法的保障和规制机能,促进数字经济的蓬勃发展是数字时代刑事司法的基本任务和当然使命。不可否认,当前数据安全犯罪的司法治理存在三重困境:一是法秩序一体化视野下民行刑边界模糊;二是数据法益立场差异下的归责路径困惑;三是数据安全犯罪体系内部界分混乱。如果说后两重困境折射出刑事司法内部的治理策略的选择差异,可通过加强刑法的教义学研究逐步化解,那么第一重困境对数字时代刑事司法的机能发挥就具有根本性的影响和制约。对此,仅仅在教义学层面作罪与非罪的区分是不够的,还必须发挥刑事政策对刑法规范的调控功能,自觉接受前置法中数据安全的价值引领和导向功能。刑事司法应当理性看待数字经济中安全与发展、秩序与风险的关系,防止对安全的过度治理而妨碍可能的创新因子,充分重视民商法和行政法对数字经济秩序的调控作用,不断明晰刑事司法对数据安全的治理边界。

[责任编辑:郑 毅]

①参见荆州市沙市区人民法院(2019)鄂1002刑初71号一审刑事判决书。

②李怀胜:《信息秩序法益视野下网络公关犯罪的完善路径》,《当代法学》,2022年第3期。