数据犯罪治理困境与对策研究

于改之* 王嘉慧**

[关键词] 数据犯罪 刑法治理 数据法益 刑事合规 数字检察

[摘 要] 大数据时代下，数据犯罪治理存在犯罪圈划定有一定偏差、罪名界限模糊、出罪机制不足的现实困境，其原因在于现有治理路径未妥当应对风险社会现实挑战、未深度契合数据要素转型需求、未有效贯彻数据治理刑事政策。为健全数据治理体系，应强化数据犯罪精准治理、完善刑法数据分类分级保护制度，拓宽除罪化路径、优化数据合规机制，数字赋能数据犯罪防治、高质效管控数据风险。

[中图分类号] DF83 [文献标识码] A
[文章编号] 1004-4043(2023)16-0016-05

信息技术日新月异，数字化、网络化、智能化深度融入社会生活各领域、全过程，发展机遇与安全风险并存。完善数据治理体系，防范数据安全风险，是推进数字经济健康有序发展的必然要求。习近平总书记强调，要健全法律法规和政策制度，完善体制机制，提高我国数字经济治理体系和治理能力现代化水平。[①]为更好实现刑法规范供给，应立足司法实践中数据犯罪治理困境，剖析困境形成的深层次原因，探讨当下数据犯罪的防治对策。

一、数据犯罪的治理困境

（一）犯罪圈划定存在一定偏差

一方面，现有数据犯罪治理路径对具备严重社会危害性的数据滥用行为规制不足。现代社会中，大数据的价值逐渐从基本用途扩展到“二次利用”，[②]数据犯罪也向链条化、产业化趋势发展。2022年工业和信息化部发布的《工业和信息化领域数据安全管理办法（试行）》将“数据全生命周期”定义为数据收集、存储、使用、加工、传输等数据处理活动，[③]与之相对应的数据安全风险包括数据泄露、数据篡改、数据滥用、违规传输、非法访问、流量异常等数据安全风险。[④]然而，现行刑法相关罪名体系呈现“重控制轻利用”的特征，即重视对非法获取、泄露、篡改数据等行为的规制，而对滥用数据的行为打击力度不足。以“某公司泄露信息事件”为例，该公司过度收集乘客人脸识别信息1.07亿条，且在未尽到明确告知义务的情况下分析乘客出行意图信息539.76亿条，违法时间长达7年，[⑤]具有严重的社会危害性，但该公司非法使用数据的行为并未受到刑法规制，这一事件最后仅以行政处罚落幕。

*上海交通大学凯原法学院教授；
**作者单位：华东政法大学。

①习近平：《不断做强做优做大我国数字经济》，载《求是》2022年第2期。
②参见[英]维克托·迈尔-舍恩伯格、肯尼思·库克耶著：《大数据时代：生活工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社2013年版，第197页。
③参见《工业和信息化领域数据安全管理办法（试行）》第3条、第13条。
④参见《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》第2条。
⑤参见《国家网信办：滴滴存在严重影响国家安全的数据处理活动》，载人民网http://finance.people.com.cn/n1/2022/0721/c1004-32482059.html。

另一方面，为了回应数据犯罪治理的现实需求，实践中出现扩张适用非法获取计算机信息系统数据罪、破坏计算机信息系统罪的情形。其一，非法获取计算机信息系统数据罪的犯罪对象被不断扩大。即便“计算机信息系统数据”在司法解释中被限定为“身份认证信息”，[6]适用中仍然不加区分地将虚拟财产、商业秘密、个人信息、知识产权等其他数据形式纳入其中，难以区分罪与非罪的界限。基于司法适用惯性，司法人员也倾向于忽略数据承载信息的法律属性，通过更为简单的技术判断直接将行为对象认定为“数据”，从而扩张适用非法获取计算机信息系统数据罪。[7]其二，破坏计算机信息系统罪的打击范围持续扩张。司法人员对多个行为之间的手段与目的关联在规范适用中的重要意义重视不够，对作为手段行为侵入计算机信息系统的行为，即便目的行为另有所指，最终也常直接以破坏计算机信息系统罪定性。

（二）罪名界限模糊

在数据安全法中，数据的定义为“以电子或者其他方式对信息的记录”，根据其所承载内容或利益的不同，数据可以是个人信息、商业秘密、国家情报等。现实中数据范围过于宽泛，加重了司法实践中区分数据类型、辨别数据法律属性的难度，以至于部分案件认定时未能明确罪名界限。最为典型的是对侵犯公民个人信息及网络虚拟财产案件的定性，甚至存在同一裁判前后矛盾、不同判决标准不一的情形。如，一起多人利用钓鱼网站盗取信息案，[8]法院在说理部分认为某社交软件的登录账号和密码既属于公民个人信息又是计算机信息系统数据，但在判决中却将同样实施利用钓鱼网站盗取账号和密码的两名行为人，分别认定为侵犯公民个人信息罪与非法获取计算机信息系统数据罪，而裁判理由则语焉不详。正是由于法院未准确识别数据与个人信息的区别及关系，才导致在罪名适用上产生了难以解释的混同。又如，有法院强调虚拟财产的数据形态，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。[9]经笔者统计，近五年，50份涉及非法获取虚拟财产的判决中，有18例根据刑法第285条、第286条定性，其余32例将相关行为认定为盗窃罪、诈骗罪、抢劫罪等财产犯罪。[10]

由此可见，实践中对于数据的法律属性认定尚未达成一致意见。为实现数据犯罪的精准界分与行为要件的合理阐释，理论界与实务界大多认可数据法益独立保护的必要性，意欲将数据法益作为分析工具以解决上述实践困境，但对于如何建立数据法益机能的具体实现路径，则在理论供给上仍显不足。

（三）出罪机制不足

从刑法教义学角度来看，涉数据罪名体系中尚未构建以行为实质违法性判断为核心的出罪机制。如针对已公开数据的抓取行为，实务中以绕开技术屏障具有惩罚必要性为由将其认定为非法获取计算机信息系统数据，却忽略了行为本身并未侵犯数据保密性。根据法秩序统一性原理，前置法上合法的行为不具有刑事违法性，[11]为促进数据治理法律体系的融会贯通，需要进一步探索刑法中正当行为的出罪路径，如合理使用原则等。

近年来，在全国范围内推行的涉案企业合规改革就是一种拓宽除罪化路径的综合尝试，在织密数据犯罪法网的同时也为企业改善治理结构留存出路。虽然数据刑事合规为企业数据犯罪治理开辟了新通道，但在合规制度设计与落实上仍存在不少挑战：一是涉案企业合规出罪的制度范式混杂，存在事前合规与事后合规的定位问题、实体出罪与程序出罪的路径争议。二是行刑衔接不畅，没有充分贯彻有效合规整改的理念。三是数据市场多头监管，配合机制不完善，难以有效发挥合力作用。

---

⑥参见2011年最高法、最高检《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》第1条。

⑦参见杨志琼：《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》，载《法学评论》2018年第6期。

⑧参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。

⑨参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。

⑩在“北大法宝”以关键词“虚拟财产”进行全文搜索，筛选“刑事案由”，审结日期为“2018年1月1日至2023年4月30日”，共检索到76篇文书，经排除无关文书、同案一审判决，共筛选出50篇具有研究价值的文书。

⑪参见于改之：《法域冲突的排除：立场、规则与适用》，载《中国法学》2018年第4期。

二、数据犯罪治理的困境成因

（一）未妥当应对风险社会现实挑战

毋庸置疑，“风险社会是科学、媒介和信息的社会”，[12]社会分化与社会冲突伴随风险而形成，市场机会也悄然而至。就数据而言，即便数据安全问题面临巨大挑战，也无法阻挡以数字科技为核心驱动力的生产力升级发展。在风险社会理论所揭示的现实语境下，“法律结构随着社会复杂性的进化而变迁”，[13]我国刑法体系也呈现积极性立法、预防性保护、前置化介入的特征，这大体上可以解释数据犯罪的刑法规制现状。

从法律制定的角度来看，虽已限制数据获取，以非法获取计算机信息系统数据罪控制前端行为，实现风险预防的目的，但难以应对更严重的数据泄露风险。据《2022年数据泄露成本报告》记载，全球数据泄露成本在过去两年间上涨近13%，83%的受访组织遭遇过不止一次的数据泄露事件，而单次事件所造成的平均损失高达435万美元，其中近50%的数据泄露成本是在事后一年多才产生的，企业长期受到威胁勒索。[14]足以见得，数据泄露会带来无法估量的“后遗症”，若无法从源头上控制数据泄露风险，次生犯罪风险会不断增加，这是着眼于事前防范的保护模式所无力解决的。不过，在数据传输与信息传播的多环节、长链条中常常无法确认数据泄露源头，难以对相关行为进行追责。数据泄露具有风险的高发性与不确定性，为减轻证明负担，处罚源头的数据获取行为也实属无奈之举。从法律解释的角度来看，数据犯罪刑法规制通过拓展法益范围、扩张构成要件，将公共利益与犯罪形态纳入考量范畴。司法者似乎也意识到了“现代风险显现的时间滞后性、突发性和超常规性”，[15]摇摆在安全与发展之间，在打击犯罪的同时忽略了罪刑法定这一重要原则。

（二）未深度契合数据要素转型需求

通说认为，数据权可分为数据主权、数据人格权以及数据财产权，[16]数据人格权强调隐私权及个人信息自主决定权的维护，[17]数据财产权则着眼于社会经济利益而进行绝对权的配置。受私法上赋权观念的影响，数据犯罪的刑法规制依托于维护计算机信息系统安全，更多针对数据合法占有的侵权行为进行处罚。这种基于传统权利理论的规制模式虽然依照实体逻辑可以实现数据控制的安全保障目的，但仍未能在数据利用与处理过程中有效甄别利益类型，从而揭示侵害多重法益行为的不法本质。究其根源，在于数据需要通过分析、处理、聚合、配置方能发掘出其独立价值。事实上，自“数据要素”概念被首次提出，[18]正视数据的公共产品属性便是数据资源市场化的题中应有之义，防范和化解技术风险成为促进数据流通利用与信息开放交流的基础前提。同时，由于数据与信息在网络空间内可以随时互相转换、传播时瞬息千里，强化数据控制安全的“静态”保护模式易引发利益识别困难、刑法评价错位的后果，未深度契合数据要素的转型需求。

（三）未有效贯彻数据治理刑事政策

“刑事政策是国家的政治意志与诉求在刑事领域的体现”，[19]从政治需要、社会需求中来，到刑法立法、司法适用中去，为刑法体系的构建提供目标性的指引。[20]党的十八大以来，发挥数据要素作用和

⑫[德]乌尔里希·贝克著：《风险社会：新的现代性之路》，张文杰、何博闻译，译林出版社2018年版，第43页。

⑬[德]尼克拉斯·卢曼著：《法社会学》，宾凯、赵春燕译，上海人民出版社2013年版，第185页。

⑭《Cost of a Data Breach Report 2023》，载https://www.ibm.com/reports/data-breach。

⑮薛晓源、刘国良：《全球风险世界：现在与未来——德国著名社会学家、风险社会理论创始人乌尔里希·贝克教授访谈录》，载《马克思主义与现实》2005年第1期。

⑯参见齐爱民、盘佳：《数据权、数据主权的确立与大数据保护的基本原则》，载《苏州大学学报（哲学社会科学版）》2015年第1期。数据主权与本文议题无关，不再赘述。

⑰参见王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，载《现代法学》2013年第4期。

⑱2020年3月30日，中共中央、国务院《关于构建更加完善的要素市场化配置体制机制的意见》“六、加快培育数据要素市场”要求“推进政府数据开放共享”“提升社会数据资源价值”“加强数据资源整合和安全保护”。

⑲劳东燕：《刑事政策与刑法体系关系之考察》，载《比较法研究》2012年第2期。

⑳参见聂慧苹：《刑事政策的刑法转化与限制——以我国刑事政策研究现状为视角》，载《中国刑事法杂志》2014年第4期。

完善数据基础制度受到高度重视，以信息化、数字化驱动中国式现代化的中国方案行稳致远：2021年施行的数据安全法确立了数据安全和发展并重的产业政策，[21]2023年2月发布的中共中央、国务院《数字中国建设整体布局规划》强调“统筹发展和安全”，由此，指引我国数据犯罪治理的刑事政策必须兼顾安全与发展的价值目标。不过，刑法在规制数据犯罪时往往会面临上述价值冲突问题：数据推进资源快捷流动的同时会带来全周期安全风险，而严格监管则可能阻碍创新发展。根据2022年12月发布的中共中央、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》，可以辨明安全与发展的关系：以数字社会建设推动国家现代化发展是大政方针的长远考量，而构建全方位的数据安全法治保障体系则是其前提条件。

上述数据治理的刑事政策理念在实践中未被全面、有效地贯彻。一方面，基于谋发展、促经营的价值目标，结合宽严相济刑事政策，即便涉案企业合规改革正在形成互惠共赢的企业犯罪治理新模式，若企业无法很好理解政策背后的激励目的时，合规计划也很难即时有效地完全融入数据运营企业的行业生态，[22]从而引发前文所述涉案企业合规改革过程中的现实困境。另一方面，基于功能主义的考量，需要能动地通过目的论解释，将实质性的刑事政策价值理念贯穿于刑法规范的适用中以限制犯罪的成立；[23]然而，现实中未能充分发挥刑事政策价值理念在构建体系化的正当化事由中的积极作用。

三、数据犯罪的防治对策

（一）强化数据犯罪精准治理，完善刑法数据分类分级保护制度

为合理划定犯罪圈、精准界分涉数据相关罪名，可以通过明晰数据法益内涵，形成规范化的解释路径。维护数据安全蕴含了数据风险防控、公共属性确证、政策精神贯彻的内在要求，[24]可以认为，数据法益兼容个体法益与集体法益，[25]前者包括数据作为载体所反映的人格利益与财产利益，后者关涉社会秩序、公共利益和国家安全。我国刑事立法中尚未明确数据法益，就现有罪名来看，可将非法获取计算机信息系统数据罪作为保护数据法益的一般条款，以维护数据的私密性、完整性、可用性。为实现罪质界定与罪界区分，应当将身份认证信息作为犯罪对象以限缩该罪的打击范围，[26]排除具有可识别性的数据信息。对于造成严重法益侵害后果的数据滥用行为，可运用填补法律漏洞的方式进行适当的扩大解释。

详言之，根据法秩序统一性原理，首先判断前置法是否足以规制违法行为，以确定刑法作为最后保障在不违反比例原则的要求下介入的必要性；而后识别相关数据承载的利益类型及行为手段侵犯的法益属性；最后确定犯罪性质，选择应当适用的刑法规范。需要注意的是，应当厘清非法获取计算机信息系统数据罪与个人信息犯罪、财产犯罪、知识产权犯罪、国家安全犯罪等相关罪名的交叉关系，根据是否存在构成要件要素上的部分重叠，来认定普通法条与特别法条的竞合关系；在同一行为触犯两罪的场合，则根据法条竞合中“特别法优先”的原则定罪处罚。同时，不能将非法获取计算机信息系统数据罪异化为兜底罪名，当行为按照特别法条不构成犯罪时，不能兜底适用普通法条，否则便是逾越了特别法条的规范保护目的，不当扩大处罚范围。

实现数据犯罪的精准治理离不开对数据的精细化管理，因此，完善数据分类分级保护制度是数据安全刑法治理的重要环节。数据分类是指根据

㉑数据安全法第1条规定：“为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。”

㉒参见于改之、陈博文：《数据犯罪的教义形塑及其风险防控——刑事合规语境下的考察》，载《上海法学研究》集刊2021年第21卷。

㉓参见杜宇：《刑事政策与刑法的目的论解释》，载《法学论坛》2013年第6期。

㉔根据数据安全法第3条，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。

㉕参见王华伟：《数据刑法保护的比较考察与体系建构》，载《比较法研究》2021年第5期。

㉖参见2011年最高法、最高检《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》第1条。

数据的内容进行类型化区分，数据分级是指依照数据的重要程度、风险威胁、危害性质等标准进行等级划分。现有规范性文件以数据处理的行业领域为分类标准，并根据数据值得保护的程度将其通常分为“轻微损害—一般损害—严重损害”或“一般数据—重要数据—核心数据”三级。在化解数据犯罪的刑法治理难题时，可以考虑引入前置法已经确立的数据分级分类制度，依照数据分类标准识别法益以界定罪质，并根据数据分级标准指引刑事责任轻重的追究，形成数据安全保护的经纬线。

（二）拓宽除罪化路径，优化数据合规机制

数据的自由流通和有效利用要求研判数据犯罪边界。对此，应为正当的数据获取、利用行为提供出罪路径，积极探索利益平衡视野下的豁免事由。首先，在数据获取环节，可以通过用户有效的“知情同意”将合理的信息采集、使用行为予以正当化。在判断用户“知情同意”的有效性时，应当考虑企业是否明确了数据获取的方法与目的，以及在条款中有无明示数据利用的预备用途与伴随风险。其次，在数据使用环节，应当构筑个人信息合理使用作为数据犯罪的实质出罪路径。可以考虑区分三种合理使用的情形：维护国家利益与社会公共利益、保护主体合法权益以及合理处理已合法公开的个人信息。[27]再次，还应当探索其他的数据犯罪豁免事由，如作为法令行为的行政许可、授权范围内的技术中立等等，并将其规范化、体系化。

涉案企业合规改革是积极防控数据安全犯罪、促进市场主体健康发展、营造法治化营商环境的重大举措，应当从以下三个方面优化数据合规机制，以有效提升数据治理能力、实现数据价值。第一，明确涉案企业合规出罪的基本范式，即对于已实施犯罪行为的涉案企业，由检察机关综合考察其合规情况，在侦查起诉阶段作出不批捕、不起诉的决定，或者在起诉时提出减免刑罚的量刑建议，以司法处置的宽宥达到社会治理的效果。第二，推进数据刑事合规与行政合规的实体、程序衔接，司法机关与行政机关在处理案件时应遵循处罚手段配合原则和处罚结果互认原则，防止企业因被重复处罚而面临不公正的结果。[28]第三，促进相关职能部门在企业合规中的职责配合与规范制度衔接，可以考虑在刑事诉讼法中规定“涉案企业合规刑事案件诉讼程序”作为特别程序，以促进双轨执法、多部门移送的合规处理机制顺畅进行。[29]

（三）数字赋能数据犯罪防治，高质效管控数据风险

数字化转型的变革势不可挡，大数据也可以为我所用；以数字技术提升司法效率、以数字检察加强数据犯罪防治，能够更好地实现刑事诉讼保障数字经济转型升级的功能与价值。[30]刑事检察作为检察机关的基本职能集指控犯罪与诉讼监督于一身，应当以提升办案质效为本质要求，深度运用大数据全面打击数据安全犯罪：一方面，建立办案信息查询协作机制，推进执法司法信息共享平台建设，实现刑事检察数字化一体建构，维护司法公正；另一方面，深化“个案办理—类案监督—系统治理”的数字化办案模式，优化诉源治理、架构法律监督模型，实现数字监督、经济发展与社会治理的相融共进。[31]同时，应建立健全公益诉讼检察与刑事检察衔接协作机制，打破各业务条线之间的信息壁垒，实现对网络违法犯罪全链条打击、一体化治理。[32]此外，还应当建立健全法律监督数据风险防控机制，坚持技术创新与风险防控、技术赋能与制度规制统筹推进，完善司法数据风险评估、预警处置机制，确保包括法律监督在内的各类司法数据均在安全轨道上共享、交互与运用。[33]

[编辑：张　倩]

㉗参见程啸：《论我国民法典中的个人信息合理使用制度》，载《中外法学》2020年第4期。
㉘参见高景峰、刘艺、柳慧敏：《行刑双向衔接的内在逻辑与有效运用》，载《人民检察》2023年第3期。
㉙参见朱孝清：《论能动检察》，载《人民检察》2022年第13期。
㉚参见高景峰：《数字检察的价值目标与实践路径》，载《中国法律评论》2022年第6期。
㉛参见叶伟忠：《检察工作高质量发展示范窗口的能动创建》，载《人民检察》2022年第10期。
㉜参见《加强新时代检察机关网络法治工作 有力助推网络强国数字中国建设》，载《检察日报》2023年4月19日，第3版。
㉝参见高景峰：《数字检察的价值目标与实践路径》，载《中国法律评论》2022年第6期。