数据安全行刑衔接的立法梳理与规范优化

王逍静[1] 代光胜[2]
(1.中共中央党校(国家行政学院)政治和法律教研部,北京 100091;
2.北京市顺义区人民法院 牛栏山人民法庭,北京 101300)

[摘 要] 数据违法与数据犯罪的界限模糊是导致数据安全行刑衔接不畅的主要原因,这一现象与数据立法采取“刑法先行”模式有关。但梳理立法发现,部分数据安全规范呈现出“行政引导刑事”的立法模式,且均采用行政前置性立法技术。为解决数据安全行刑衔接的失范问题,需从两个维度进行优化。在立法技术维度,应优先采用行政法先行立法模式,并有条件地选择适用前置不法性立法或前置程序性立法技术。在法律规范维度,罪质层面需以数据行为双重违法性为核心;罪量层面应明确犯罪对象数量、再次违法等认定标准;罪责层面则需结合罚款与罚金的功能差异正确处理二者关系。

[关键词] 行刑衔接;数据安全;立法技术;法律规范
[中图分类号] D922.1 [文献标识码] A [文章编号] 1008-7699(2026)02-0030-12

措辞变化表明行刑衔接制度在顶层设计层面已从单一维度的“正向衔接”转变为闭环结构的“正向衔接+反向衔接”①。行刑衔接的主要对象是行政犯,其核心特征是同时违反行政法与刑法,需承担行政与刑事双重法律责任。这一特征是行刑衔接问题的关键所在。从实体维度看,行刑正向衔接基本立场为限制绝对的“出行入罪”,立法上强调审慎将行政违法行为升格为刑事犯罪;行刑反向衔接基本立场则系畅通“出罪入行”渠道,将不具有实质可罚性的轻微不法行为排除在犯罪圈之外。② 从程序维度看,行刑衔接主要涉及行刑证据衔接、案件移送、行政违法行为监督等。相较而言,实体维度的行刑衔接机制研究更具基础性,有观点直接提出行政法和刑法衔接的问题主要体现在法律条文的设置上。③ 近年来高速增长的网络犯罪、个人信息犯罪等涉数据新型犯罪类型大多为行政犯,④这为数据安全行刑衔接机制研究提供了重要的现实基础与规范依据。结合行政犯的特征可知,认定一行为是否构成数据犯罪,首先须结合前置行政法规范判断其是否属于行政违法,故数据安全行刑衔接完善的首要任务是从法律层面对行刑衔接法律规定进行规范化。⑤ 目前,我国在数据管理领域的快速发展与数据犯罪治理非专门化之间出现不平衡,导致数据安全相关刑

[收稿日期] 2025-03-25
[作者简介] 王逍静(1997—),女,河南开封人,中共中央党校(国家行政学院)博士研究生;代光胜(1996—),男,安徽阜阳人,北京市顺义区人民法院法官助理。

① 刘艳红:《完善行政处罚和刑事处罚双向衔接制度》,《民主与法制》2025年第5期,第1页。
② 刘双阳:《行政处罚与刑事处罚双向衔接机制之构建》,《法商研究》2025年第2期,第153-170页。
③ 程凡卿:《行政刑法立法研究》,法律出版社2014年版,第3页。
④ 例如,《刑法》规定的拒不履行信息网络安全管理义务罪要求网络服务提供者拒不履行相关的信息网络安全管理义务,犯罪相关案件的判决需参考《网络安全法》《数据安全法》等法律法规。而《网络安全法》等法律法规虽然规定了对涉嫌相关犯罪需要追究刑事责任,但其本身并不规定犯罪与刑罚,对于相关犯罪的定罪与量刑就需要适用《刑法》及其相关司法解释。
⑤ 张旭、陈凯琳:《数据犯罪刑法应对的三个维度》,《法学杂志》2024年第2期,第111-123页。

事法律很难与前置行政法规范顺畅衔接，进而引发数据犯罪司法认定标准不统一的难题。[①] 当前理论与实践多聚焦于程序维度的行刑衔接问题，或是对某类具体犯罪的机制探讨，缺乏将数据安全案件作为一个整体继而从实体规范维度展开的研究，容易引发数据安全行刑衔接研究个案碎片化、体系性不足等问题。本文将视线集中在数据安全行刑衔接的实体维度，从立法与司法两个角度梳理其立法模式与立法技术，并从罪质、罪量、罪责三个方面提出实体规范的优化方案。

一、问题的提出

我国法律尚未对“数据犯罪”作出明确定义，学界对此存在广义说与狭义说之分。广义说认为，数据犯罪是指将数据作为犯罪手段和目标的犯罪；狭义说则主张，数据犯罪必须将“数据”作为犯罪目标。本文采用狭义说的观点。行刑衔接基础理论表明，数据犯罪及相应行政违法行为在侵害性层面存在“质”与“量”双重差异。[②] “质”是指罪质要素，即违法行为属于行政违法或刑事犯罪行为；“量”是指罪量要素，即危害程度是否达到一定标准，二者共同决定某一行为是否构成犯罪。数据违法与数据犯罪行为的理论界分模糊，导致实践中通常面临以下问题。

第一，行政不法与刑事不法的界限混淆。行政犯的双重违法性特征导致行政不法与刑事犯罪在行为类型上存在天然重合，[③]加之数据领域的行政法律规范不断更新，数据犯罪刑事立法存在滞后性，二者边界模糊导致衔接不畅。[④] 实际操作中体现为认定数据犯罪时容易混淆行政违法与刑事犯罪行为，进而对该行为是否属于数据犯罪作出相反的判断。例如，我国首例“爬虫”案中，被告人利用技术方法爬取某公司公布的录像资料，法院将该行为定性为非法获取计算机信息系统数据罪。[⑤] 然而，当数据承载的内容已被披露后，数据的秘密性等关键要素已发生改变，若仍将携带着信息的载体（数据）作为非法获取的客体，存在过度适用刑法之嫌。另外，最高检第 36 号指导性案例卫某案[⑥]中，司法机关将非法获取计算机信息系统数据罪中的“侵入”要件扩大解释为采用特定技术手段、未取得授权或超过权限获取数据的行为，这实际上是将本属于行政违法的行为纳入刑事犯罪范畴，扩大了数据违法行为的入罪边界。[⑦]

第二，情节严重性判断标准不统一。数据犯罪入罪标准的多样性与数据违法行为的交叉性，共同导致数据犯罪在司法实践中情节严重性认定难。最高人民法院、最高人民检察院联合发布的《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《计算机解释》）明确指出，违法所得数额 10 000 元以上即构成非法获取计算机信息系统数据罪。但在实践中，此类行为常被认定为不正当竞争或行政违法行为。例如，杭州铁路运输法院审理的一起案例中，[⑧]某公司非法抓取用户上传至某平台的数据并用于商业经营。法院最终认定该行为构成不正当竞争，判决被告立即停止数据抓取行为，消除影响，并赔偿该平台经济损失 60 万元。

---

① 秦长森：《数字经济时代我国数据安全刑法保护的不足与完善》，《中国矿业大学学报（社会科学版）》2025 年第 2 期，第 121-139 页。

② 韩千、李正源：《组织未成年人进行违反治安管理活动罪“组织”行为类型化探析》，《中国刑警学院学报》2023 年第 2 期，第 68-77 页。

③ 孙国祥：《行政犯违法性判断的从属性和独立性研究》，《法学家》2017 年第 1 期，第 48-62 页。

④ 梅传强、徐智鹏：《论数据违法的行刑界分》，《重庆理工大学学报（社会科学）》2024 年第 7 期，第 135-145 页。

⑤ 参见北京市海滨区人民法院（2017）京 0108 刑初 2384 号刑事判决书。

⑥ 参见最高人民检察院指导性案例第 36 号：卫梦龙、龚旭、薛东东非法获取计算机信息系统数据案。

⑦ 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》，《华东政法大学学报》2024 年第 2 期，第 94-106 页。

⑧ 参见杭州铁路运输法院（2021）浙 8601 民初 309 号民事判决书。

第三,行政处罚与刑事处罚适用边界模糊。就法律规范而言,刑法与行政法在保护法益、责任形态及构成要件上均有明确界分。司法实践中基于促进数据发展等考量,常出现行刑责任适用混同现象。例如,滴滴公司巨额罚款案中,有观点认为根据《中华人民共和国刑法》(以下简称《刑法》)及相关司法解释,滴滴公司非法过度采集用户照片、面部特征等数据已涉嫌构成侵犯公民个人信息罪。厘清并解决该案引发的"以罚代刑"争议,还需结合《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)进一步明确行刑责任边界。

二、数据安全行刑衔接法律规范立法进程梳理与模式剖析

行刑衔接源于法律明文规定,对其制度剖析要回归法律规范本身。① 完善数据安全领域的行刑衔接法律规范,要解决的是如何通过立法技术实现新情况下的数据违法与犯罪的内容衔接。当前我国法律尚未对数据犯罪作出明确界定,亦未设立独立的数据安全犯罪罪名。学界通说认为,由于计算机犯罪与个人信息犯罪在侵害对象、行为方式等方面与数据安全紧密相关,故可纳入数据安全犯罪范畴。实践中,与数据直接相关的犯罪类型包括计算机犯罪、个人信息犯罪、国家秘密犯罪、商业秘密类犯罪及其他犯罪等五大类。② 最高人民检察院《行政检察工作白皮书(2024)》显示,帮信罪已位列反向衔接案件数量第六位。基于规范衔接性与实践典型性双重考量,本文选取计算机犯罪、个人信息犯罪与信息网络犯罪作为数据安全行刑衔接的核心研究对象。

(一)计算机犯罪——行政引导刑事的改进立法模式

我国刑法学界依据网络技术的发展程度、犯罪行为的特点等因素,将网络犯罪分为三个阶段。③ 第一阶段为互联网发展初期,数据主要依托网络存储和传输,此时数据安全保护主要聚焦于网络系统中的数据安全。《计算机信息系统安全保护条例》(以下简称《计算机保护条例》)于 1994 年颁布,将计算机及相关配套设施资料列为系统的重要组成部分,并规定由公安部负责监管,涉嫌违法者将被追究法律责任。由于当时计算机尚未普及,故 1979 年《刑法》未对数据犯罪作出专门规定。然而随着计算机的推广应用,针对计算机的违法行为日益增多。为此,公安部提交《危害计算机信息系统安全罪方案(草案)》,建议设立破坏计算机信息系统罪。④ 该建议被 1997 年《刑法》采纳,与《计算机保护条例》相衔接。

第二阶段,数据安全的独立保护逐渐受到重视。2000 年全国人大常委会《关于维护互联网安全的决定》规定,对非法侵入计算机系统构成犯罪的行为,依法追究刑事责任。该规定与 1997 年《刑法》第二百八十五条、第二百八十六条规定的计算机犯罪实现衔接。鉴于司法实践中计算机犯罪种类和数量的持续增长,⑤公安机关指出,当前存在大量以非法获取数据为主要目标的计算机犯罪行为。⑥ 故《中华人民共和国刑法修正案(七)》(以下简称《刑法修正案(七)》)在此基础上进行补充。2011 年 1 月,《计算机保护条例》仅进行文字上的改动;同年 6 月,最高人民法院、最高人民检察院联合发布的《计算机解释》对"情节严重""后果严重"等内容进行详细界定,极大填补了计算机

① 方颉琳:《数字检察赋能行刑衔接:前提、可行性及路径》,《山东科技大学学报(社会科学版)》2025 年第 1 期,第 32-39 页。

② 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,第 50-61 页。

③ 刘艳红:《Web3.0 时代网络犯罪的代际特征及刑法应对》,《环球法律评论》2020 年第 5 期,第 100-116 页。

④ 高铭暄、赵秉志:《新中国刑法立法文献资料总览(第二版)》,中国人民公安大学出版社 2015 年版,第 1274 页。

⑤ 参见《"两高"出台司法解释保障计算机信息系统安全促进互联网健康发展》,https://www.court.gov.cn/zixun/xiangqing/7495.html,2025 年 4 月 20 日访问。

⑥ 黄太云:《〈刑法修正案(七)〉解读》,《人民检察》2009 年第 6 期,第 5-21 页。

犯罪中行刑衔接的空白。自此,数据安全相关犯罪在我国法律体系中的规制更加完善,数据安全领域的犯罪行为得到更明确的界定和规范。

第三阶段,计算机犯罪的形态和特征趋于稳定。海量的数据聚合使得人们的行为轨迹可通过算法精确识别,公民个人信息权利保护逐渐受到刑事立法重视。在计算机犯罪方面,《中华人民共和国刑法修正案(九)》(以下简称《刑法修正案(九)》)中只增加了单位犯罪类型,其他未作出实质性改变。《网络安全法》于2017年施行,在第三章"网络运行安全"规定了互联网经营者应承担的安全保障责任。直至2021年《数据安全法》问世,我国才在法律层面明确数据的概念。该法亦将"盗窃""侵犯"数据等行为纳入违法范畴,实现了与《刑法》第二百八十五条第二款"非法获取"的衔接。

总体而言,我国计算机犯罪立法过程体现出"行政引导刑事"的立法特点,关键节点上由行政部门提出刑事立法建议,前置法规范采用"违反国家规定"的方式。从其制定历程看,1997年《刑法》对数据的保护以维护计算机信息系统安全为目的,将数据认定为计算机信息系统的重要组成部分。随着针对数据违法行为的增多,立法增设了专门的数据保护条款。

(二)个人信息犯罪——刑法先行的新立法模式

个人信息犯罪的行刑衔接立法经历了由扩张到固定的过程。第一阶段,受当时社会信息化程度较低以及科技发展水平有限等因素的制约,1997年《刑法》没有设立以个人信息为犯罪对象的罪名,对相关行为通过侮辱、诽谤等间接罪名进行规制。《刑法修正案(七)》将出售、非法提供、非法获取公民个人信息行为纳入犯罪,旨在通过对侵犯公民个人信息行为施加刑事处罚来保护公民信息。该罪虽采用"违反国家规定"的空白罪状表述,但设置了较为严格的适用条件。此后,我国一直没有针对"违反国家规定"进行特别立法,有关个人信息保护的规定分散在各部门法中。

第二阶段,《刑法修正案(九)》将前述几种具体违法行为统一纳入侵犯公民个人信息罪,将犯罪主体由特殊主体扩展为一般主体,提高法定最高刑,增设一档量刑区间,均体现出刑法对个人数据保护力度的加大。然而,刑法仅设定了个人信息犯罪的构成要件及量刑标准,却未对"出售、非法获取个人数据"及其他"非法处理个人数据"等关键概念作出具体规定,导致司法实践中对该罪的认定存在较大争议,进而难以准确打击相关犯罪行为。至此,我国尚无针对个人信息保护的专门行政法规范,可谓"刑法先行、前置法不足"。同时,该罪因缺乏前置性规定的指引,在司法适用中面临行为认定标准不统一、证据收集与认定困难等困境。可以说,《刑法修正案(九)》扩大犯罪行为类型进一步加大了个人信息领域行政法与刑法的制度性矛盾。①

第三阶段,《网络安全法》与《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)的出台完善了个人信息保护制度。《网络安全法》首次在法律层面系统规定个人信息保护制度,2017年最高人民法院、最高人民检察院出台《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》(以下简称《个人信息解释》),对个人信息犯罪中的"情节严重"和"情节特别严重"作出界定,明确不同情节下的量刑标准,解决了部分司法实践中定罪量刑标准不统一等难题。2021年《个人信息保护法》颁布实施,对个人信息保护作出系统性规定,其中包括个人信息处理规则、个人在信息处理中的权利、个人信息处理者的责任与义务等。至此,我国法律为个人信息保护提供了全面、细致的法律依据,强化个人信息的保护力度,此前"刑事先行、前置法落后"的局面才得以扭转。

① 胡江:《侵犯公民个人信息罪中"违反国家有关规定"的限缩解释——兼对侵犯个人信息刑事案件法律适用司法解释第2条之质疑》,《政治与法律》2017年第11期,第34-42页。

通过以上立法进程可知,个人信息犯罪立法呈现出明显的“刑法先行”特点。在具体表述上,经过对相关前置性法律规范的几次修改,最终采取“违反国家有关规定”的方式来界定个人信息犯罪中的一般违法情形。《刑法修正案(七)》与《刑法修正案(九)》之间,有关公民个人信息保护的前置法规范极为匮乏,形成“刑法先行、行政法滞后”的立法格局。然而,伴随着《网络安全法》和《个人信息保护法》的相继颁布,有关个人信息的行政法律规范逐渐完备,“先行介入”的刑法规制模式得以改变,个人信息犯罪重新回归最后保障手段的功能定位。

(三)信息网络犯罪——刑法先行的新立法模式

信息网络犯罪的行刑衔接立法进程相对较短。随着互联网从“信息媒介”逐渐向日常生活渗透,通过信息网络进行的传统犯罪,如网络诈骗、网络盗窃等,在犯罪数量、涉及范围和危害程度等方面逐渐成为当今社会的主要犯罪形态。《刑法修正案(九)》增设了三种新型的网络犯罪,其中,由于缺乏对网络安全管理义务具体内容、判定标准等的明确界定,导致司法实践中对拒不履行网络安全管理义务罪的认定困难,该罪名适用率偏低。《网络安全法》出台,将此项义务明确,并增设不履行该义务应承担的行政责任,实现了行政法与刑法的衔接。但学界和实务界中对本罪“拒不改正”“严重后果”的理解仍存争议。2019年10月,最高人民法院、最高人民检察院颁布司法解释对犯罪构成的罪量因素作出细化,①在一定程度上顺畅了此类案件的行刑衔接。

由此可见,信息网络犯罪立法也体现出“刑法先行”的特征,并采用“违反国家规定”的空白罪状立法技术。但因违反“国家规定”涉及的法律规定多、范围大、认定标准尚未体系化,且随着信息技术的快速发展,如人工智能、区块链等新技术的出现,违反国家规定的行为会随着技术变迁发生动态性变化,单纯采取“空白罪状”的立法方式难以取得预期成效。

(四)立法规范与特征总结

就立法规范而言,我国数据相关立法在罪名的增设、处罚范围的扩大等方面均体现出明显的扩张性趋势。1997年《刑法》代表着我国刑事法律趋于成熟,第二百八十六条增设“破坏计算机信息系统罪”,是我国法律首次纳入“数据”这一概念。② 后经四次修改,刑法逐步将信息网络犯罪、个人信息犯罪等与网络相关的犯罪纳入其中。总体而言,自1997年《刑法》出台以来,立法针对数据犯罪共增加了四条、六项规定(新增四项罪名)。

就立法技术而言,数据立法整体呈现出“刑法先行”的特征。其中,个人信息犯罪和信息网络犯罪均先于行政法规范而直接进入刑法规制范畴,实现“从无到有”的改变。当前阶段,数据行政立法呈现出活性化趋势,③表现为数据行政法规、规章等不断出台,对数据收集、使用、存储等环节的监管日益细化,而刑事立法对数据保护则存在滞后与错位。例如,部分新型数据犯罪行为未能及时纳入刑法规制范围等。行政法体系尚未完备时,刑法先行介入往往会引发数据犯罪认定和治理分歧,进而出现行刑衔接问题。

三、数据安全行刑衔接法律规范的立法技术取舍

如前所述,行政引导刑事的立法技术在部分数据犯罪中均有体现。在具体规范上,上述三类犯

① 《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第1条、第2条分别释明第286条之一中网络服务提供者、监管部门责令采取改正措施、经监管部门责令采取改正措施而拒不改正的认定方式,第3至第6条为入罪标准,明确“致使违法信息大量传播”“造成严重后果”“情节严重”“有其他严重情节”的具体内涵。

② 此次修订还增加了第285条“非法侵入计算机信息系统罪”,该罪条文中未出现数据的概念。

③ 秦长森:《数字经济时代我国数据安全刑法保护的不足与完善》,《中国矿业大学学报(社会科学版)》2025年第2期,第121-139页。

罪均采用了行政前置性立法，其中又包括不法性立法与程序性立法两种方式。在对立法技术进行取舍时需考虑到数据安全案件的特殊性。就实体维度而言：一方面，当前社会背景决定数据安全案件治理需在个人权利与公共安全中实现平衡；另一方面，数据相关行政立法与刑事立法不平衡，导致违法行为方式与信息分级标准存在差异。此外，数据安全案件呈现出对技术网络、电子数据的高度依赖，而数据隐蔽性强、影响范围广、数据壁垒与数据孤岛等天然属性也决定了立法技术应不断调整。下文结合数据安全行刑衔接的特点，对当前立法技术进行分析与选择。

（一）刑法先行立法模式的不足

近几年，人工智能、大数据、区块链等新兴产业的法律规制呈现出“刑法先行”的趋势，但受制于缺乏相应的监管措施，其规制效能无法充分发挥。

第一，前置性立法缺失致使犯罪标准模糊，影响罪名认定。刑法设定拒不履行网络安全管理义务罪时设立了特别的行政前置程序，即拒不履行网络安全管理义务且“经监管部门责令采取改正措施而拒不改正”的。此时配套的《网络安全法》尚未出台，司法实践中本罪的入罪标准偏高，相较其他两种信息网络犯罪，本罪司法适用率也较低。因此，立法者强化互联网安全管理的立法目标在司法实务中未得到很好落实。

第二，前置性立法缺失导致法律适用选择困境。① 以个人信息犯罪为例，个人信息的概念表明其无需具备私密性，故即使信息已经公开仍应属于个人信息范畴。但法律规定，依法取得已经公开的个人信息不构成违法处理个人信息，且后续出售、非法提供个人信息是否构成违法也缺乏行政前置性法律规范，这导致司法实践中出现个案处理差异。直至《个人信息保护法》第十三条明确六项个人信息处理规则，规定在合理范围内处理已经公开的个人信息无需取得个人同意，该问题才得以缓解。综上，前置性规范缺失引发的法律选择适用难题，需通过完善前置性规范予以解决。

（二）行政法先行立法模式的优先适用

“立法技术的本质是，将要制定的法律与其来源的逻辑推理关系问题，故法律推理构成立法技术的基础思维方式。”②法律推理既适用于司法推理，又适用于立法推理。数据安全领域行刑衔接立法技术的选择，既要契合数据安全违法犯罪特征，又不能违背刑罚作为我国法律制裁体系中最后、最严厉制裁手段的功能定位。而行政法先行的立法模式无论是在规制数据安全违法行为，还是维护立法体系性与协调性方面，均具有理论优势，在数据安全领域行刑衔接法律规范体系中宜优先适用。

一方面，数据犯罪作为典型的行政犯，构成犯罪需以行政法中明确的违法性评价为前提。有关数据的行政法规范实质上属于数据治理标准，它详细规定了数据收集、存储、使用、共享等各环节的规范要求，明确规定了数据安全主管部门需承担的监管责任与义务，为数据安全保障提供了具体指引。相较而言，刑法对此规定较为笼统。刑法在规定具体犯罪时，通常采取“行政违法＋构成要件＋加重要件”的三阶层立法方式。“行政违法”仅是对违反相关法律规定的概括性描述，内容较为抽象。“构成要件”则是通过明晰违法行为的具体方式，实现对刑事犯罪的界定。与行政法中关于数据侵权复杂、细化的规定相比，目前我国刑法对违法行为方式的规定较为简明、笼统，在打击犯罪方面相对局限。虽然“加重要件”并非成立数据犯罪的必要条件，但此类规定混淆了数据行政违法行

① 时延安：《数据安全的刑法保护路径及方案》，《江海学刊》2022年第2期，第142-150页。

② 马怀德：《法典化时代行政法总则的规范功能与构建》，《政法论丛》2025年第3期，第47-60页。

为与数据犯罪的边界。故“行政违法+构成要件+加重要件”的立法模式在甄别数据犯罪与数据侵权的作用上并非周延且精确,采用行政法先行的立法技术一定程度上可以突破其局限性。后续制定刑事法律时需注意与前置行政法的衔接,避免将行政违法行为纳入刑事犯罪,这也是当前阶段制定相关刑事司法解释的关键所在。

另一方面,行政法先行的立法模式有助于增强行政法规的法律效力与权威。1997年《刑法》体现出明显的重刑主义倾向,这也是当时的社会环境所致。重罚既体现为犯罪起点较低、刑罚规定较严,强调惩罚的功能和有错即罚的刑罚观念。然而,随着社会经济的不断变革,市场规制手段由单一走向多元、由公权力主导走向公私合作共治,加之新兴领域的不断涌现,行政犯种类日益增多,法律规制手段的复杂化与专业化也日益提高。行政犯刑事责任的确立已无法脱离行政不法的先行判断。

(三)行政前置性立法技术的选择适用

如前所述,为顺应数字化社会发展的需要,我国数据犯罪立法宜优先采用行政前置性立法模式。“行政”主要体现在对数据行为作出的正当性判断,以及通过动态行政监管程序作出的合法性评估;“前置”则表现为对数据安全行为的行政评估位于刑事责任评估之前。行政前置性立法包含不法性立法和程序性立法,二者在具体方式与功能上存在差异。

不法性立法是一种静态的评价,行为违背行政法规就属于“行政不法”。非法获取计算机信息系统罪中的“违反国家法律法规”是典型的不法性前置立法。① 类似的规定还有“违反相关法律法规”“违反……法规”“违反……管理规定”等。以不法性前置立法的方式设定的空白罪状,进行犯罪事前判定时仅需满足违反了静态的行政规范,此外没有其他任何限制。不法性立法的判断较为简单,一定程度上扩大了刑事不法的行为范畴。

程序性立法不仅是对行政行为的认定与评估,还包括对行政监管程序的评价。程序性前置规范规定了违法主体负有主动纠正违法行为的义务,并通过对违法主体进行事前处置从而达到限缩犯罪圈的效果。② 拒不履行信息网络安全管理义务罪是采用该立法技术的典型罪名,该罪在以存在行政不法行为作为构成要件的基础上,增设了行政程序性规定,即无论是认定犯罪还是作出裁判,都需要针对违法行为作出更为实质的判断。有学者进一步提出,本罪的构成要件中采取了实体性和程序性上的双重前置结构。③ 具体而言,成立本罪需经过双重判断:第一阶段,在实体维度,行为人必须实施了未依法履行法律规定的网络安全管理义务行为,即不作为或履职不当,此系成立本罪的基本边界;第二阶段,在程序维度,行为人必须经过监管机构责令改正的程序,仍未改正才成立犯罪,将监管机构责令改正的程序前置,进一步加大了本罪犯罪构成对行政法规范的依赖。行政程序前置性立法技术反映出某一具体领域内违法行为行刑共治的特点。因网络安全领域的行政规范不断更新,加之数据管理需较强的专业性,直接将是否已履行监管职责的审查义务交由网络服务提供者过于苛责。在以实体性不法作为入罪标准的基础上,通过程序不法可以实现对犯罪圈的调适。故与静态的不法性立法相比,动态的程序性立法更加灵活,可以较好地适应网络数据发展规律。

综上,考虑到数据犯罪作为行政犯的规范特征,数据安全行刑衔接法律规范应当优先适用行政引导刑事的立法技术,当前行政法规范的逐渐完备也为采用该立法技术提供了现实基础。在前置

① 熊波:《行政犯的类型与违法性判断的区分》,《政治与法律》2020年第5期,第40-55页。

② 熊波:《网络服务提供者刑事责任“行政程序前置化”的消极性及其克服》,《政治与法律》2019年第5期,第50-65页。

③ 杜小丽:《社会治理视角下拒不履行信息网络安全管理义务罪再审视》,《中国法律评论》2024年第3期,第86-95页。

性立法技术的具体选择上，可根据不同领域的数据违法行为特点，有针对性地选择使用不法性立法或程序性立法。

四、行刑衔接在数据安全法律规范层面的优化

《中华人民共和国行政处罚法》（以下简称《行政处罚法》）第二十七条是行刑衔接的基本法律依据。该条第一款规定，应当移送司法机关的是“涉嫌犯罪”的案件，此规定构成了案件移送的实体标准。数据犯罪的行刑边界应结合罪质与罪量双重差异论予以确定。罪质要素要以数据行为的双重违法性判断为核心，明确前置法规范的适用范围并通过司法解释将前置行政法与刑法有效衔接，以准确认定数据犯罪。罪量要素则需以相关司法解释中的细化规定为核心，厘清几种罪量要素的认定准则。另外，在责任承担方面，关键在于协调行政罚款与刑事罚金的设定与执行，避免引发反向衔接中的行刑倒挂问题。

（一）行刑衔接在数据安全罪质层面的优化

1. 前置性规范法律适用范围的统一

部分个人信息类犯罪的刑法条文包含诸如“违反国家规定”“违反国家有关规定”的表述，这是判断不法行为是否属于行政违法的最直接依据，也是数据犯罪行政法与刑法的立法衔接点。根据刑法及相关司法解释规定，此处的“国家规定”不包括国务院部门规章和行业规章。[①] 然而，当前存在一些司法解释或规范性文件对个人信息犯罪的规定不一，主要问题在于是否将违反“部门规章”作为个人信息犯罪的前置性规范。此外，我国现行法律对相关条文规定得过于笼统，有的甚至援引了一些效力位阶较低的规范性文件。

本文认为，无论是违反“国家规定”还是违反“国家有关规定”，其范围都应当以刑法规定为准，即不包括部门规章及其他规范性文件。一方面，根据罪刑法定原则，其他法律规定与刑法不一致的，应以刑法规定为准。既然刑法及相关司法解释已就国家规定的范围作出规定，就应严格遵守。另一方面，“有关”是指需参照的法律应为与该罪名相关的、某一行政管理领域的法律规范，目的是避免前置规范过于宽泛和模糊，而非对前置性法律效力位阶的扩大。

2. 刑法解释的结合功能

从立法上看，认定数据犯罪双重违法性需结合行政法中的特定条款和犯罪构成要素，并通过刑法解释加以解决。行政法规通常设定多种违法行为表现形式，当刑法犯罪构成要件中的行为模式明显无法与行政法对应时，判定不法行为是否构成犯罪应遵守以下条件：一是行政法所确定的行为方式必须处于刑法所确定的行为模式的意义范围之内；二是损害相关利益。

例如，《个人信息保护法》明确规定任何组织和个人不得非法采集、使用、处理、传输他人的个人信息，故从事上述活动的任何组织或个人都可能违反行政管理秩序，存在行政违法风险。但上述行为方式无法直接与刑法规定的“提供”相对应。遵循上述步骤可以判断：一是非法收集、加工、传输实际上也属于一种信息传输形式，属于刑法规定的非法“提供”公民个人数据的文义射程，[②]也有观

① 《刑法》第96条：本法所称违反国家规定，是指违反全国人民代表大会及其常务委员会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。《最高人民法院关于准确理解和适用刑法中“国家规定”的有关问题的通知》（法发〔2011〕155号）第1条规定，根据刑法第九十六条的规定，刑法中的“国家规定”是指，全国人民代表大会及其常务委员会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。

② 另外，《个人信息保护法》第三条还规定“不得非法买卖、提供或者公开他人个人信息”，这里的“买”可认定为非法获取，“卖”为“出售”，而“公开”则可以认定为个人信息保护法司法解释“其他途径发布公民个人信息”，即非法“提供”公民个人信息。

点主张将“收集”解释为“窃取”“非法获取”,或者将其理解为刑法规定的以“其他”方式获取。[①] 二是非法收集、加工公民个人信息的行为本身也会对个人隐私造成侵害。故非法收集、加工、传输个人数据行为,满足一定条件的,应属于刑法调整范围,当前可先通过司法解释将上述行为与刑法罪名中现有行为方式进行衔接。

需要注意的是,《个人信息保护法》还规定了非法使用、删除个人信息等违法行为,根据语义不宜将其直接纳入刑法规定的“提供”或“非法获取”个人信息范畴。若直接将“存储、使用、加工和删除”等行为认定为犯罪,不仅涉嫌违反罪刑法定原则,也不利于对违法行为的精准治理。为保护公民个人信息,今后我国刑法可以考虑修改构成要件行为类型,同时要注重与《个人信息保护法》的内容保持一致,以促进相关法律的行刑衔接。

(二)行刑衔接在数据安全罪量层面的优化

对数据安全的罪量要素,刑法通常表述为“情节严重”“情节特别严重”“造成严重后果”“后果特别严重”,只有拒不履行信息网络安全管理义务罪采用了列举式的规定。数据犯罪相关司法解释都对相关罪量要素进行了明确与细化,主要是设定入罪数量标准、“受过刑事或行政处罚”,此外还包括违法所得数额,造成死亡、证据灭失等后果。本文仅讨论前两种情形。

1.限定犯罪对象数量的理解

在限定犯罪对象数量方面,部分数据犯罪采用兜底式规定,这需要准确理解其适用范围。如,个人信息犯罪中的“窃取或者以其他方法非法获取公民个人信息”,信息网络犯罪中的“有其他严重情节的”。但在具体的定罪量刑中缺少明确标准,容易造成量刑上的困难。

例如,除“出售、提供、非法获取”以外的其他类型个人信息犯罪,是否均需达到一定数额才能成立?解决该问题需厘清行政法中的“个人信息处理”与“非法获取、出售、提供”的法律关系。上文分析可知,“非法获取、出售、提供”是一种广义的概念,司法实践中不能仅限于文义解释,而应该在侵权行为的多样性和不可预见性的基础上进行理解。刑法规定“以其他方式非法获取”个人信息,也显示出立法者有意将更多的个人信息处理活动纳入刑法规制范围之中。但刑罚毕竟是最严厉的制裁手段,刑罚使用应具有谦抑性,故法律往往规定只有造成严重后果才能认定“情节严重”。因此,在将其他非法处理个人信息行为理解为刑法规制范畴的前提下,也需适用刑法及相关司法解释对“情节严重”规定的入罪条件。

2.“受过刑事或行政处罚入罪”的适用

“受过刑事或行政处罚入罪”是指将特定条件下受过刑事或行政处罚作为入罪的常设标准。数据犯罪中采用此种罪量要素的主要有信息网络犯罪和个人信息犯罪,二者将受过刑事或行政处罚直接作为认定“情节(或后果)严重”的情形之一,进而影响定罪。

一方面,此种罪量要素方式有助于预防数据领域犯罪风险。有学者指出,将“受过行政处罚”纳入刑法的量化要素实质上是以危险因子为基础,是立法者在面对风险社会时重新建构入罪标准的一种尝试。[②] 作为新兴领域,数据本身具有虚拟性,数据犯罪行为对技术依赖性高,智能化手段适用性强,这些因素使得数据作案的隐蔽性更强。另外,数据传播范围广,与人身权、财产权等密不可

① 童云峰:《个人信息保护法与侵犯公民个人信息罪的衔接机制》,《中外法学》2024年第2期,第366-385页。

② 赖早兴、罗素敏:《论“受过行政处罚”单独作为入罪定量因素的正当性及其限制》,《湖南社会科学》2024年第1期,第120-127页。

分，很容易发生涉众类案件，造成巨大损害。另外，此种立法方式增加了在受到刑事或行政处罚之后，对相同的危害行为进行重新处罚的可能性，更好地发挥了刑罚特殊预防作用，并可以提高人们对法律规范的认知。

另一方面，“受过刑事或行政处罚入罪”的适用程序应得到优化。我国采用行刑二元制裁体系，行政与司法信息各自独立，因尚未建立完备的行政执法与刑事司法信息共享平台，致使有关主体无法及时、精确核查行为人的先前违法行为，“受到刑事或者行政处罚”在司法实践中难以有效执行。此外，数据安全案件的事实认定高度依赖电子证据，其本身存在的数据孤岛现象及技术依赖性加大了行刑数据共享难度。例如，最高人民检察院公布的医保诈骗监督等典型案例表明，通过搭建大数据监督模型实现行刑交叉对比，才能更好地发现案件线索。① 为此，行刑二元制裁体系下，为实现数据安全案件行刑衔接，更应注重建设行刑数据共享平台，有效发挥刑事档案资料作用。

（三）行刑衔接在数据安全犯罪责任承担层面的优化

《行政处罚法》第八条第二款规定：“违法行为构成犯罪，应当依法追究刑事责任的，不得以行政处罚代替刑事处罚。”因此，对违反行政秩序且构成犯罪的行为须同时施加行政与刑事处罚。但二者合并适用并不意味着同类处罚在执行中不可相互折抵。行政责任和刑事责任在性质上有很大区别，但二者当中的财产罚存在一致性，数据安全责任承担模式中行刑衔接的难点就在于行政罚款与刑事罚金的适用问题。

1. 刑事罚金与行政罚款设定方式的协调

行政处罚与刑事处罚在功能定位上具有层次性。② 功能定位层次性是指行政处罚与刑事处罚均具有制裁性，但因违法行为社会危害程度不同使得制裁严厉程度有所差异。从制裁的严厉程度与终局效力看，刑事处罚的对象具有比行政处罚对象更大的社会危害性。从处罚内容看，刑事罚金的最低标准原则上不应低于对应行政罚款的最高限额。如果在立法上忽视了两者之间的层级关系，刑事罚金与行政罚款的设置标准不协调，加之一些罪名中对罚金的规定过于笼统，就容易导致针对同一行为的刑事罚金数额低于行政罚款，此即理论与实践界广泛关注的“行刑倒挂”现象。

例如，《个人信息解释》中设置的罚金数额普遍低于违法所得的一至五倍，并在第五条第七项中将违法所得超过 5 000 元作为情节严重的认定标准。若非法处理个人信息违法所得 5 000 元构成犯罪，根据法律规定刑事罚金幅度一般在 0.5 万元以上 2.5 万元以下。《个人信息保护法》第六十六条规定，对非法处理个人信息且拒不改正的处以 100 万元以下罚款，相关负责人处以 1 万至 10 万元罚款。因此，违法所得在 0.5 万元至 1 万元的个人信息犯罪中，行政罚款幅度整体上高于刑事罚金，容易出现“行刑倒挂”情况。今后立法应进一步精确、细化个人信息犯罪的罚金刑幅度，并在适用标准上与行政法保持一致。

2. 刑事罚金与行政罚款的吸收与折抵

功能定位相似性是指行政罚款与刑事罚金在功能上具有相似性，在执行上可以折抵和吸收。行政罚款与刑事罚金均以财产给付义务为主要内容，它们采用了对利益最简单的衡量方法，通过迫使违法行为人付出超过损失限额的成本来调节行为，故在性质上二者并没有什么区别。③ 也就是说，尽管行政罚款与刑事罚金本质上是两个不同的概念，但是它们的内容和目标都是一样的，只要

① 参见最高人民检察院 2025 年 11 月 6 日贸易的《公诉讼大数据法律监督模型办案典型案例》。

② 应松年、冯健：《行政罚款制度的困境及其破解——以证券行政处罚为例》，《求索》2021 年第 1 期，第 141-150 页。

③ 徐科雷：《罚款与罚金在经济法责任体系中的辨析与整合》，《政治与法律》2015 年第 3 期，第 131-136 页。

求违法者缴纳一种费用便可实现对其经济上的惩罚。[①] 这一点在我国现行立法中也有所体现,如《行政处罚法》第三十五条第二款规定,行政机关已经给予当事人行政罚款的,该罚款可以折抵刑事处罚中的罚金。

行政罚款的运用应当把握两个方面。一是,对判处罚金后的行为不再给予行政罚款。尽管二者在本质上存在差异,但都具有剥夺行为人再犯经济能力的作用。如果先对违法者处以刑事罚金,继而作出行政罚款,容易出现被执行人的全部财产只够支付罚金无法支付罚款的局面。此类处罚执行难度大且会导致企业完全丧失继续经营能力,不利于数据产业发展。二是,作出刑事罚金前已经给予行政罚款的,相应金额应当折抵,但若拟作出的罚金数额高于已施加的罚款,超过的数额仍应执行。《行政处罚法》中关于折抵的规定仅是为了处理两者之间的"重合",并非否认行政罚款的效力。可以说,若先前作出的处罚决定是合法有效的,那么剩余罚金的执行也是应该的。

五、结语

数据安全行刑衔接运行不畅的核心症结在于数据违法与犯罪的界分模糊,这与当前数据领域"刑法先行"与"行政引导刑事"并存的立法模式密切相关。破解这一难题,应从立法技术与实体规范两个维度对数据安全行刑衔接立法进行优化。随着数据安全治理需求的不断提升,数据安全立法也将促使立法技术更加精细、法律规范更加完善。今后,为进一步完善数据安全领域的行政处罚与刑事处罚双向衔接机制,可针对立法技术的实施细节、法律规范的适用场景等展开研究,以期为数据安全提供更加坚实的法律制度保障。

① 周佑勇、刘艳红:《论行政处罚与刑罚处罚的适用衔接》,《法律科学(西北政法学院学报)》1997 年第 2 期,第 88-91 页

Legislative Review and Normative Optimization of the Connection Between Administrative and Criminal Law Enforcement in Data Security

WANG Xiaojing[1], DAI Guangsheng[2]

(1. *Department of Political and Legal Education, Party School of the CPC Central Committee (National Academy of Governance), Beijing* 100091, *China*;
2. *Niulanshan People's Court, People's Court of Shunyi District, Beijing* 101300, *China*)

Abstract: There is confusion between illegal and criminal acts in data crimes, which leads to the poor connection between administrative and criminal law enforcement in data security. This is related to the fact that the criminal law takes the lead in data legislation. However, a closer examination of the legislative process reveals that there is also a model where administrative law guides criminal legislation, and nearly all data crimes adopt the administrative pre-legislative technology. To address the disorder and poor connection between administrative and criminal law enforcement in data security, efforts should be made from two dimensions in the future. As to the dimension of legislative technology, the administrative law should be given priority, and the pre-illegality and pre-procedural legislative technologies should be selectively applied when conditions permit. As to the dimension of legal norms, several aspects warrant attention. Firstly, in defining the nature of the crime, the focus should be on the core of the dual illegal acts of data behavior. Secondly, in terms of quantity, it is crucial to clearly specify the number of criminal objects and the criteria for determining repeated violations. Lastly, in the aspect of responsibility, the interplay between fines and penalties should be properly handled in combination with their hierarchical and similar functions.

Key words: connection between administrative and criminal law enforcement; data security; legislative technology; legal norms

(责任编辑:董兴佩)