《学术界》(月刊)
总第301期,2023.6
ACADEMICS
No.6 Jun. 2023

数据犯罪“双轨+分级”治理机制的系统化构建〔*〕

房慧颖
(华东政法大学　刑事法学院,上海　200042)

〔摘　要〕在大数据时代,数据违法犯罪的主体逐渐从自然人转向企业。企业的运营过程伴随着数据的产生、利用、传输、存储、交易,这在多节点、多层次、大范围上造成对数据安全的威胁。现行数据犯罪刑法治理模式面临难以兼顾科技发展与社会治理需求的“顾此失彼”难题与难以准确把握刑法介入数据犯罪治理恰当时机的“进退两难”困境。应跳出刑法的闭塞体系,以求建立数据犯罪治理的新范式。为解决数据犯罪刑法治理模式面临的“顾此失彼”难题,应构建数据犯罪双轨治理机制,通过企业数据刑事合规计划的开展,促进企业内控机制与国家监管规则之间的功能化互动,同时构建配套刑事激励机制,实现国家单向度的“数据治理”到国家与企业双轨制的“数据共治”的转向。为突破数据犯罪刑法治理模式面临的“进退两难”困境,应构筑数据犯罪分级治理机制,充分发挥企业数据刑事合规计划与前置性法律法规对数据犯罪认定的“拦截”作用,只有在企业数据刑事合规计划失灵、前置性法律法规规制无效的前提下,刑法才能介入对数据犯罪的规制。同时,应以适度预防理念为指导设立数据犯罪的入罪标准,准确把握刑法介入数据犯罪治理的恰当时机。

〔关键词〕数据犯罪;刑事合规;前置法;分级治理
DOI:10.3969/j.issn.1002-1698.2023.06.015

一、问题的提出

我国已出现以数字经济为引领的新经济形态,近年来,我国的数据规模以几何级数爆发和增长,为经济和社会的发展带来了巨大效益,注入了新动能。2022年政府工作报告中提出加强数字中国建设整体布局。实体经济与数字经济的融合,极大地推动了数字产业化和产业数字化,这在促进经济高质量发展的同时,对国家治理模式的调整也提出了新要求。而在此之前,2021年国务院发布的“十四五”数字经济发展规划也明确提出,要进一步建立与完善和数字经济发展相适应的法律法规体系。

数据资源是数字经济的关键要素,实现数字经济的有规制发展,首先要规范数据的采集、存储、流转、利用行为。以往的数据侵权或数据犯罪大多是由单一自然人实施的行为,而在大数据时代,以互联网企业为首的网络服务提供者在数

作者简介:房慧颖,法学博士、博士后,华东政法大学刑事法学院特聘副研究员,从事预防性刑法、经济刑法、刑法解释研究。
〔*〕本文系上海市哲学社会科学规划课题“预防性刑事立法及其限度研究”(2022EFX003)的阶段性成果。

据业务运营过程中,理所当然地成为数据处理与利用的重要主体。与此同时,企业已成为数据侵权或数据犯罪的主要阵地,也即数据违法犯罪的主体逐渐从自然人转向企业。企业的运营过程伴随着数据的产生、利用、传输、存储、交易,这在多节点、多层次、大范围上造成对数据安全的威胁。当前,数据的采集、存储、流转、利用等环节仍存在巨大安全风险,例如,医疗、生物识别等特殊敏感的高价值数据泄露风险加剧;数据的非法获取行为会侵犯公民的隐私,进而威胁公民的人身、财产安全;数据的非法跨境流转会给国家安全带来隐患。[1]发挥刑法的社会保护机能,构建保护数据资源的刑事法治规则体系,是增强大数据时代数字经济风险防控能力的重要路径,也是实现国家治理能力现代化的时代课题。

对于上述侵犯数据安全的行为,如果刑法介入规制的时间过晚,则无法有效应对数据安全风险倍增的局面,从而无法实现有效的社会治理;但是如果刑法介入规制的时间过早,则有违刑法谦抑性,出现重刑主义、猛药治疴的负面效应,甚至可能会阻碍数字科技的发展。显然,采用单一刑法手段规制数据犯罪的单向度国家监管模式存在很大局限性,容易陷入进退两难的"僵死"局面,且规制效果难彰。

因此,既要充分发挥刑法治理数据犯罪的功效以实现保护社会的机能,又要避免因刑法过度介入社会治理而对经济发展和科技进步形成阻碍,这就需要我们探索以保护数据安全、促进数据利用为核心的数据犯罪治理新机制。[2]具体而言,如何应对单一刑法手段规制数据犯罪的局限性,实现企业内控机制与国家监管规则之间的功能化互动,[3]为数据犯罪治理提供充足的外部制度补给与支撑,以及如何准确把握刑法介入数据犯罪治理的时机,在实现对数据犯罪治理"到位"的同时避免刑法过度介入社会治理的"越位"现象,[4]是立法者、司法者和研究者共同面临的不可回避的重要议题,也是本文着重探讨和力图解决的问题。

二、数据犯罪刑法治理模式顾此失彼之难题、进退两难之困境

为了有效应对社会风险和满足公众的安全期待,数据犯罪刑法治理模式呈现出预防性趋势。但是,现行数据犯罪刑法治理模式面临难以兼顾科技发展与社会治理需求的"顾此失彼"难题与难以把握刑法介入数据犯罪治理恰当时机的"进退两难"困境。

(一)数据犯罪刑法治理模式呈现的趋势

数据犯罪刑法治理模式呈现出预备行为实行化、共犯行为正犯化、公民刑法义务增加等预防性趋势。有效应对社会风险和满足公众的安全期待,是数据犯罪刑法治理模式呈现出预防性趋势的动因。

1. 数据犯罪刑法治理模式呈现出预防性趋势

《数据安全法》第3条规定,数据是指任何以电子或者其他方式对信息的记录。数据与信息二者系内容与载体的关系,数据是信息的载体,信息是数据表达的内容,二者并非泾渭分明。[5]1997年刑法颁布之初,我国的信息化建设处于起步阶段,刑法中只规定了非法侵入计算机信息系统罪;随着我国信息技术的高速发展,信息化向智能化转型迭代,立法者通过刑法修正案的方式,增加了非法获取计算机信息系统数据、非法控制计算机信息系统罪,提供侵入、非法控制计算机信息系统程序、工具罪,拒不履行信息网络安全管理义务罪等有关侵犯计算机信息系统和网络安全的罪名。除此之外,为了打击大数据时代中的新型犯罪,《刑法修正案(九)》针对恐怖主义数字化的趋势,增设了相关的恐怖犯罪;针对编造有重要影响的虚假信息的情况,增设了编造、故意传播虚假信息罪;针对侵犯公民个人信息的行为,修改完善了侵犯公民个人信息罪。《刑法修正案(十一)》针对侵犯商业秘密行为的新情形,修改完善了侵犯商业秘密罪;在新增的危险作业罪条文中明确规定对篡改、隐瞒、销毁有关生产安全数据的行为进行处罚。无论立法

者通过刑法修正案新增罪名抑或对原条文进行修改完善、扩大处罚范围,都体现出刑法以扩张的姿态介入到社会生活中,以提前干预与预防的手段实现保护社会的机能。具体表现如下:

其一,预备行为实行化。《刑法修正案(七)》增设非法获取计算机信息系统数据、非法控制计算机信息系统罪。应当看到,非法获取计算机信息系统数据和非法控制计算机信息系统的行为,尚未实现危险的现实化,也即尚未出现侵害法益的实际后果,而是作为行为人实施其他犯罪行为的预备行为。立法者通过刑法修正案的方式将原本作为其他犯罪预备行为的行为规定在刑法分则条文中,赋予其实行行为的形式和意义,是刑法预防性趋势的典型表现。《刑法修正案(九)》增设的非法利用信息网络罪,也是赋予预备行为以实行行为的形式和意义,使之独立成罪。预备行为与法益侵害结果之间存在密切联系,立法者通过预备行为实行化的立法逻辑,也即通过在行为过程的前阶段阻断预备行为,实现对法益的间接性、前置性保护,达到阻止危害结果发生的目的,有效实现对法益侵害结果的预防。与之类似,《刑法修正案(十一)》增设危险作业罪,通过制裁篡改、隐瞒、销毁相关生产安全数据的行为,保护生产安全数据的真实性、完整性、可用性,来达到排除重大生产安全隐患,防范重大事故发生的目的。

其二,共犯行为正犯化。《刑法修正案(九)》增设帮助信息网络犯罪活动罪,赋予原本属于共犯范畴的帮助行为以正犯的形式和意义。对于帮助信息网络犯罪活动罪,有学者提出,应将其理解为量刑规则。[6]对于此观点,学界存在较大争议。但无论是将帮助信息网络犯罪活动罪条文理解为独立犯罪,还是理解为量刑规则,都可以在一定程度上摆脱帮助行为的定罪量刑对被帮助行为定罪量刑的依赖,弥补传统共犯理论在应对不断异化的数据犯罪共犯时的不足。[7]

其三,公民刑法义务的增加。《刑法修正案(九)》增设拒不履行信息网络安全管理义务罪,利用刑法的强制性,强化网络服务提供者的信息网络安全管理义务,来达到维护信息网络安全的目的。信息网络安全管理义务本属于行政义务的范畴,《刑法修正案(九)》通过增设新罪名,将原本属于公民行政义务的内容上升到刑法义务。赋予网络服务提供者在面对海量数据信息时对相关数据信息进行审查、甄别的行政义务,本身就可能对网络运营造成妨碍,[8]而将这种行政义务上升为刑法义务,更是立法者在网络运营效率和数据信息安全之间作出的侧重维护数据信息安全的抉择。显然,拒不履行信息网络安全管理义务罪是纯正不作为犯,其可罚性根据在于,当法益面临巨大危险时,处于保证人地位的行为人如不及时消除危险,将会造成难以挽回的重大损失。[9]“义务应当在何处止步是社会哲学所面临的一项最艰巨的课题”。[10]尽管立法者对网络服务提供者的入罪条件作出了相应限制,但不可否认,该罪的设立仍是对信息网络服务者刑法作为义务的增加。这超越了传统刑法事后回应型的体系定位,而是预防性刑法的典型表现。

2. 数据犯罪刑法治理模式呈现出预防性趋势的动因

在探寻数据犯罪刑法治理模式呈现预防性趋势的动因时,必须从宏观的视角出发,综合考量国家治理模式、刑事法治的发展阶段、犯罪治理的现实需求等诸种因素。“社会不是以法律为基础的。那是法学家们的幻想。相反地,法律应该以社会为基础。”[11]刑法应当敏感感知社会生活的变化,认清在不同时代承担的不同使命。如何妥当地实现对数据安全的保护,是刑法在大数据时代面临的重要课题。

应对社会风险是数据犯罪刑法治理模式呈现出预防性趋势的动因之一。在大数据时代,数据资源是数字经济发展的关键要素,对数据资源的侵害会在根本上危害数字经济的发展。在数据犯罪链条化、产业化的大背景下,侵犯数据法益的犯罪不仅是对数据本身的破坏,而且可能成为其他上游犯罪、伴随犯罪的预备行为或者帮助

行为。例如,侵犯公民个人信息的行为不仅是对公民隐私信息等的侵犯,而且可能会对公民的人身权、财产权造成威胁甚至实际的侵害。与侵犯传统法益的犯罪相比,侵犯数据法益犯罪的危害性往往会在网络时代、大数据时代的放射效应影响之下,呈现倍增性、规模化、扩散化特征,从而倒逼传统刑法治理犯罪的格局作出转型。数据包容国家利益、公共利益、个人利益等多元价值,而除了极少数条文(如《刑法》第 285 条第 2 款)之外,刑法并未专门对数据进行保护,更遑论对数据法益的全流程保护。然而,民法与行政法承认数据安全法益作为新型法益的法律地位,这使得刑法对数据法益进行独立保护的必要性凸显。同时,在大数据技术引发科技变革、数字经济重塑社会经济形态的背景下,刑事法治重塑对数据法益的保护也在所难免。为此,传统刑法作出了相应调整,以预防性的姿态应对社会风险,保护数据法益。

满足公众的安全期待是数据犯罪刑法治理模式呈现出预防性趋势的动因之二。在大数据时代,新型犯罪的规模化、扩散化效应以及对新型犯罪的不可预测性,使得公众的安全焦虑史无前例地增强。卢梭提出的社会契约论表明,国家权力形成的前提是公民让渡出自由,而公民让渡自由的目的是获得更多、更稳定的自由。“这里所讲的自由,本质上应该是安全”。[12]因此,公众对于安全的诉求和渴望,会在一定程度上体现在国家权力的表现形式之一——刑事政策乃至刑事立法中。数据安全事故发生后可能造成的规模化、扩散化危害后果强烈销蚀着公众的安全感,也冲击着社会的平稳与秩序。同时,传媒技术的发达,使得公众感知风险的途径增多,也容易让公众在主观上加剧对风险的担忧。公民个人没有足够的力量直接抗衡侵犯其权利的组织体的力量,从而迫切希望国家采取强有力的手段控制和预防社会风险,[13]而国家有义务以国家的强制力量实现对公民自由与权利的保护。作为社会治理工具,采用预防性姿态防范社会风险、维护社会治理、保护社会安全便成为刑法的不二选择。

(二)数据犯罪刑法治理模式面临的困境

1. 顾此失彼:科技发展与社会治理难以兼顾

数据内容具有多样性,包括国家数据、公共数据、商业数据、个人数据等,这决定了数据安全不仅关乎数据本身,而且可能直接关乎国家安全、公共安全、企业安全与公民个人的人身财产安全。正如笔者在前文所述,在大数据时代,国家的任务与角色已发生根本性转变,国家有义务处理社会、经济、政治等各领域的潜在危机和风险,保障公民生活的安全、稳定、有序。[14]同时,在灾害频发的社会中,公众也对国家这一职能的发挥寄予厚望。因此,国家采取一定治理策略以保障社会安全的做法,具有深厚的政治基础与民主根基。为了实现保护社会的机能,刑法从风险源头对数据安全所面临的风险进行防控,也即实现对数据犯罪的事前规制。落后于时代发展现状的刑法体系,可能会牵制甚至阻挠社会发展与时代进步;超前于时代发展现状的刑法体系,可能会被束之高阁甚至对社会发展起掣肘作用。面临大数据时代的侵犯数据安全的新型犯罪,刑法如果坐视不理,可能无法实现有效的社会治理;如果在危害尚未实际发生时,仅因危险的存在就对相关行为人予以刑罚处罚,则可能会引发社会安全保障和技术研发自由之间的矛盾冲突,从而阻碍乃至扼杀数字科技的发展。

2. 进退两难:刑法介入数据犯罪治理的时机难以把握

刑法作为最严厉的法律,只应处罚具有严重社会危害性的行为。因此,刑法需寻找介入规制数据犯罪的恰当时机。[15]刑法过晚介入对数据犯罪的规制,会因监管与规制的空白而导致大数据技术与数字经济的无序发展和风险现实化;刑法过早介入对数据犯罪的规制,则可能会模糊刑法干预社会的应然界限,[16]甚至可能会扼杀大数据技术的创新与更迭,阻碍数字经济的发展。具体而言,当前数据犯罪呈现链条化、产业化特

征,数据犯罪不仅危害数据安全本身,而且通常情况下还可作为其他上游犯罪、伴随犯罪的预备行为或者帮助行为,为其他犯罪提供助力。而且,侵犯数据法益的犯罪往往会在网络时代、大数据时代的放射效应影响下,危害性呈现倍增性、扩散化效应。因此,数据安全事故所引发的附随性后果通常具有规模化特征,危害性极大。为了对大数据时代侵犯数据安全的犯罪行为进行有效应对,刑法逐渐从事后惩治型向事前预防型转向。德国和日本的刑法频繁修改,已明确展现出预防性趋势,[17]我国的刑事立法在今后一段时间也会坚持预防性方向。“随着风险社会特征的日渐明显,刑法逐渐蜕变成一项规制性的管理实务。在此背景下,作为风险控制机制中的组成部分,刑法一改为报应和谴责而惩罚的特性,转变为为了控制风险而威慑。”[18]预防性的刑事立法在实现有效社会治理、保护社会安全的同时,也意味着法益批判机能受到挑战、入罪门槛降低。把握不好刑法介入社会治理的限度,也即不能准确确定刑法介入规制数据犯罪的恰当时机,不仅可能会阻碍大数据技术和数字经济的发展,甚至可能会遏制社会活力、激化社会矛盾。因此,在数据犯罪刑法治理方面,刑法面临着进退两难的境地。

概言之,刑法具有最后手段性和不可避免的滞后性,单纯依靠刑法手段规制数据犯罪力所不逮。而采用预防型规制模式治理数据犯罪,则可能扭曲甚至扼杀数字科技的发展,引发社会安全保障和技术研发自由之间的矛盾冲突。[19]可见,单一刑法手段无法同时有效实现维护社会治理与促进科技发展的双重需求,在探讨数据犯罪治理机制构建的问题时,我们应跳出刑法的闭塞体系,以求建立数据犯罪治理的新范式。

为解决数据犯罪刑法治理模式面临的难以兼顾科技发展与社会治理需求的“顾此失彼”难题,应实现企业内控机制与国家监管规则之间的功能化互动,为数据犯罪治理提供充足的外部制度补给与支撑,构建内外共治的数据犯罪“双轨”治理格局。为突破数据犯罪刑法治理模式面临的难以准确把握刑法介入规制数据犯罪的恰当时机的“进退两难”困境,也即为了同时实现对数据犯罪的治理“到位”和避免刑法“越位”,应构筑数据犯罪分级治理机制,充分发挥企业数据刑事合规计划与前置性法律法规对数据犯罪认定的“拦截”作用,只有在企业数据刑事合规计划失灵、前置性法律法规规制无效的前提下,刑法才能介入对数据犯罪的规制。

三、内外共治:数据犯罪双轨治理机制的构建

以刑事制裁为主要方式的单向度国家监管模式存在显而易见的局限性,其规制效果难以彰显,亟需其他治理手段提供功能补给。企业数据刑事合规计划通过促进企业制度化、内控化地开展数据安全的保障工作,也即通过企业的事前主动介入,为企业和国家共同治理数据犯罪提供了平台。因此,企业数据刑事合规计划的启动,使得原本以国家为主导的单向度“数据治理”转向国家和企业共同主导的双轨制“数据共治”。

(一)数据犯罪双轨治理机制的显著优势

1.有利于实现对数据安全的协同化、双重性保护

在以刑事制裁为主要方式的国家单向度数据治理体系中,企业与国家处于对立地位;企业数据刑事合规计划的实施,使得国家和企业从对抗性的对立地位转向国家和企业共治的“契约”治理模式,[20]从而实现对数据安全的协同化、双重性保护。

从企业数据刑事合规计划的制定依据来看,企业制定数据刑事合规计划,需在法律和责任伦理的指引下,根据数据安全义务的履行要求,积极承担社会责任,参与到“数据共治”机制中来。企业制定数据刑事合规计划的参照包括前置性法律法规的规定和相关行业规范,也即将法律法规的规定和相关行业规范内化为本企业的行为规范。企业通过制定和实施数据刑事合规计划,将自身应尽的数据安全保障义务予以明确化、情

境化、具体化、个性化。同时,因刑法处于保障法地位,法律具有底线性特征,前置性法律法规所确定的企业数据安全保障义务不低于(通常高于)刑法所规定的企业数据安全保障义务;而相关行业规范所确定的企业数据安全保障义务不低于(通常高于)前置性法律法规所规定的企业数据安全保障义务。因此,以法律法规为依据、以相关行业规范为参照的企业数据刑事合规计划所确定的企业数据安全保障义务的实现方法,更有利于促进企业数据安全保障义务的履行,从而和国家监管方共同实现对数据安全的保护。

从企业数据刑事合规计划的运行原理来看,企业数据刑事合规计划的实施,是国家介入企业运作的有效工具与有力手段,也是国家犯罪治理制度与企业内控机制之间形成良好互动的必由之路。从企业数据刑事合规计划的内在运行机制而言,其属于一种企业根据刑事法律规定而自主开展的预防数据犯罪的特殊方式,本质上属于一种社会自治手段。从企业数据刑事合规计划的外在运行机制而言,其与刑法的社会治理相结合,形成协商共治模式,本质上属于犯罪治理的体系化,在国家强制力和企业能动性之间形成"1 + 1 > 2"的整体效果,[21]从而达到对数据安全的协同化、双重性保护。

2. 有利于实现对数据犯罪的有效预防

近年来,国内外频繁发生大规模的侵犯数据安全的事件,其中大多数根源于企业内部的安全漏洞。[22]随着大数据技术的快速发展,技术和伦理之间的矛盾冲突也频繁显现,如大数据"杀熟"、非法使用个人数据等。与数据犯罪的急剧增长相比,国家刑罚权的启动则明显缓慢和滞后。尽管数据犯罪刑法治理模式呈现出预防性趋势,但仍无法改变刑法事后惩治的主旋律。单纯依靠以刑事制裁为主的国家单向度监管模式治理数据犯罪显得捉襟见肘。且以国家单向度监管为主的数据犯罪治理模式将企业置于单纯接受刑法强制治理的被动地位,忽略了企业自身所具有的主观能动性。

根据《数据安全法》第 8 条的规定,企业在开展数据处理活动时,应履行数据安全保护义务,承担社会责任。因此,企业应将伦理责任观念贯穿于生产经营管理过程中,在促进企业良好发展的同时,履行好数据安全保护义务。[23]也即企业具备一定的社会属性,其是社会治理共同体的一员,[24]需要秉持技术向善的伦理旨趣,而不能任由数据进行超越法律底线和伦理道德的"赋能"。[25]企业数据刑事合规计划成为企业承担上述社会责任的重要途径,对于防范数据安全风险具有重要的"治本"功效。[26]企业数据刑事合规计划的实施,促使企业主动介入对数据犯罪行为的事前预防,从而防患于未然,实现对数据犯罪的积极一般预防,提升对数据犯罪的积极防控。[27]同时,如果企业的行为涉嫌危害数据安全的刑事犯罪,涉案企业的数据刑事合规计划的制定和实施,可能成为影响定罪量刑的因素,这是对企业数据犯罪特殊预防的体现。[28]

在数字经济社会中,企业构建数据刑事合规计划,从而和国家一道形成数据犯罪的共治格局,是预防和减少数据犯罪的重要手段,有利于为大数据时代数字经济的发展提供有效的安全屏障。可见,企业的数据刑事合规计划是数据犯罪事前预防制度架构中的重要组成部分,具有提示潜在刑事风险、提供刑事风险规避方法、提出刑事风险处理策略的重要作用,与刑法的预防犯罪机能遥相呼应,[29]成为预防数据犯罪的重要途径,有利于实现对数据犯罪的有效预防。

3. 有利于实现科技发展与社会治理之间的平衡

在大数据时代,企业成为数据处理和利用的主要主体,加之数据安全保障法律法规相对滞后于技术的发展水平,复杂的数据处理、利用活动加剧数据安全风险的同时,也导致法律法规对企业数据安全责任认定相对严苛,表现为法律法规赋予企业较多的数据安全保障义务,间接导致企业关涉数据安全的法律风险急剧上升。有学者提出,可以通过企业数据刑事合规计划的实施,

“放过涉案的企业,留下犯罪的自然人”。[30]这对于降低企业的涉数据刑事风险、促使企业持续进行技术创新,具有一定的积极作用。但是,对于中小企业而言,直接负责的主管人员和直接责任人员往往和企业的生存直接关联,追究直接负责的主管人员和直接责任人员的刑事责任,实际就等同于切断了企业生存的命脉。换言之,追究涉案企业的刑事责任,等同于阻断企业进一步发展的道路,企业为科技创新所作的贡献也将戛然而止。

企业数据刑事合规计划的引入,为企业提供了自我“体检”与主动自律的根据与机会。企业在设计、制定、实施、调整数据刑事合规计划的过程中,可以根据自身实际经营情况,将数据安全保障义务融入到生产经营活动中,将刑法和其他法律法规赋予企业的数据犯罪预防义务内化为企业的个性化内控机制。企业的内部自律机制和以国家强制力为主要表现形式的外部监管机制融合在一起,有利于推动企业识别数据犯罪刑事风险、制定预防数据犯罪刑事风险的计划、完善规避数据犯罪刑事风险的措施,从而达到有效预防数据犯罪的目的。企业数据刑事合规计划的制定和实施,不仅为国家治理数据犯罪提供了助力,而且是企业防范国家非理性干预企业管理的重要手段,成为企业抵御刑事风险、减少犯罪损失的重要屏障。企业的生存和发展,关乎企业活力和创新力的维系。因此,数据犯罪双轨治理机制的构建,使得以刑事制裁为主的国家单向度的“数据治理”转向国家与企业双轨制的“数据共治”,有利于降低企业刑事风险,增强企业创新动力,实现科技发展与社会治理之间的平衡。

(二)数据犯罪双轨治理机制的实现路径

构建数据犯罪双轨治理机制,需在企业治理中引入数据刑事合规计划,为企业提供主动自律的根据,促使企业将刑事治理的规则、政策和理念内化为企业的内控机制;同时,国家需构建和企业数据刑事合规计划配套的刑事激励机制,将企业的数据刑事合规计划作为出罪或减免刑罚的事由,从而增强企业制定和实施数据刑事合规计划的积极性,巩固和完善国家和企业双轨制的数据共治格局。

1. 构建企业数据刑事合规机制

企业通过制定数据刑事合规计划,把刑法及其他法律法规所赋予的法律义务内化为企业及企业组成人员的内部规则和行为规范。[31]企业在日常经营管理活动过程中,通过建立内部的风险防控机制,防范企业的数据安全风险,此为企业数据刑事合规计划中的事前自主合规机制;企业在触及涉数据安全的刑事风险之后,通过制定或调整数据刑事合规计划进行补救和整改,以防止数据犯罪的再次发生,此为企业数据刑事合规计划中的事后强制合规机制。[32]企业数据刑事合规计划的制定和实施具有充足的法律法规和政策依据。《网络安全法》《数据安全法》《个人信息保护法》等赋予企业开展数据刑事合规计划的义务,可以作为企业制定、实施数据刑事合规计划的重要指南;国务院国有资产监督管理委员会发布的《中央企业合规管理指引(试行)》、国家发展和改革委员会等发布的《企业境外经营合规管理指引》、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)》等一系列行业规范性指导文件,可以作为企业数据刑事合规计划的指引。同时,最高人民检察院制定的《关于开展企业合规改革试点工作方案》,以及最高人民检察院会同多部门联合制定的《关于建立涉案企业合规第三方监督评估机制的指导意见(试行)》,[33]也为企业数据刑事合规计划的开展提供了重要参考。

在制定企业数据刑事合规计划时,应将刑法赋予企业的数据安全保障义务予以具体化,明确企业在生产经营时所应具体承担的作为义务,并明确设定义务履行的方法和手段,以真正实现刑法赋予企业的作为义务内化为企业的内部管理制度与运行方式。具体而言,企业应分阶段设定数据刑事合规计划的实际内容。在数据的获取阶段,在数据刑事合规计划中,企业应明确规定

获取数据的途径,明晰获取数据过程中的刑法风险,并制定具有明确性、针对性的风险识别、评估及防控措施。在数据的存储、利用阶段,在数据刑事合规计划中,企业应明确规定相关责任人的具体义务,提升企业对违规或违法处理、利用数据行为的预防、识别、反应功能,着重建立内部调查机制与吹哨人机制,从源头上防控数据非法泄露风险和数据滥用风险。[34]在实施企业数据刑事合规计划时,应确保企业的刑事合规计划落到实处而非流于形式。[35]企业数据刑事合规计划的实施是企业履行数据安全保障义务的核心,比数据刑事合规计划的制定更为重要和关键。在企业数据刑事合规计划的实施过程中,应明确划分企业管理人员的数据刑事合规责任,从企业的管理层面确保刑事合规计划对企业的管理和运营产生实际作用,保证数据刑事合规计划真正在企业的运行过程中得以贯彻和实施。另外,对于因高昂成本或因合规能力有限而缺乏合规动力的中小企业,应引入数据刑事合规支持机制,通过外部的专业支持,帮助企业制定数据刑事合规计划,并在运行过程中予以专业指导、进行风险提示,以提高企业的刑事合规能力。

2. 构建与企业数据刑事合规机制相配套的刑事激励机制

构建与企业数据刑事合规机制相配套的刑事激励机制,核心在于明确企业数据刑事合规计划在何种条件、何种程度上可以作为企业出罪或者刑罚减免的事由。笔者认为,企业制定并执行了数据刑事合规计划,但企业内部人员为了企业利益、以企业名义实施了犯罪行为,此时数据刑事合规计划可以将企业和企业内部人员的刑事责任予以切割,作为涉案企业的出罪事由。在刑罚减免方面,无论企业在涉案之前制定并实施了数据刑事合规计划,还是在涉案之后知错就改,制定了数据刑事合规计划,都可以从侧面体现出涉案企业对遵守法规范的意愿与对规则的认同和遵守,也就意味着对企业预防必要性的降低,[36]此为对制定并实施数据刑事合规计划的企业减免刑罚的正当性根据。

由于公安机关对于犯罪情节轻微的案件没有免予刑事处罚的权力,因此,负责侦查环节的公安机关很难成为与企业数据刑事合规机制相配套的刑事激励机制的主导。构建与企业数据刑事合规机制相配套的刑事激励机制,应从审查起诉、审判等环节入手,探索有效路径。在审查起诉环节中,检察院可对企业作出相对不起诉的决定,通过检察建议的方式监督企业制定并实施数据刑事合规计划。另外,尽管当下的附条件不起诉制度只适用于未成年人犯罪案件,但是可通过对法律的适当修改,使得附条件不起诉制度的适用范围涵盖企业刑事合规领域。对于在涉案前已经制定了数据刑事合规计划的企业,适用相对不起诉;对于涉案前尚未制定数据刑事合规计划的企业,通过附条件不起诉制度,监督其及时制定数据刑事合规计划。在审判环节,同样存在开展企业数据刑事合规计划的空间。法院应告知并促使涉案企业开展刑事合规计划,企业如果在开庭之前制定刑事合规计划,可以作为减免刑罚的依据。[37]同时,在现有的刑法框架之下,应当赋予数据刑事合规计划以明确的量刑价值,法院在认定涉数据犯罪企业的刑事责任时,可以将企业建立并实施了数据刑事合规计划作为减轻甚至免除刑罚处罚的事由。当然,目前的企业数据刑事合规计划的制定和实施只能作为酌定量刑情节,立法者可以考虑在未来时机成熟时,将其作为法定量刑情节。因此,与企业数据刑事合规机制相配套的刑事激励机制,有利于引导、督促企业建立并实施数据刑事合规计划,从而巩固与完善数据犯罪共治局面。

四、三道防线:数据犯罪分级治理机制的构建

数据犯罪分级治理机制的具体内涵为,只有在企业数据刑事合规计划失灵、前置性法律法规规制无效的前提下,刑法才能介入对数据犯罪行为的规制。换言之,企业刑事合规计划是预防数据犯罪的“第一道防线”,前置性法律法规是预

防数据犯罪的“第二道防线”,刑法则是规制数据犯罪的“最后一道防线”。

(一)数据犯罪分级治理机制的显著优势

1.有利于为数据犯罪的认定提供细致、具体的标准

数据刑事合规计划为刑法赋予企业的数据安全保障义务的明确化、具体化提供了现实的可操作标准。不同企业可以根据自己的实际经营情况和业务范围,建立个性化的、有针对性的数据刑事合规计划。这不仅能够避免国家公权力过多介入企业内部具体业务的情况,而且更有利于企业发挥自身能动性,充分实现对数据犯罪的内部防控和源头防控。一方面,企业数据刑事合规计划能够将包括刑法在内的法律法规所确定的企业数据安全保障义务内化为企业的内部管理机制和具体运营规范。法律法规所确定的违法类型,是企业行为的“禁区”,企业的所有具体活动,都应该避开可能触犯刑事风险的“禁区”,这有助于明确企业的行为边界与责任承担前提。另一方面,将抽象的法律规则予以具体化所形成的企业数据刑事合规计划,可以作为判定企业未履行数据安全保障义务的明确标准,避免了法律因抽象性而产生的认定结果具有不确定性的弊端。

随着数字科技在经济发展中的地位逐渐攀升,数据资源在数字经济中的基础性地位日益显现,以及数据犯罪呈现链条化、产业化特征,立法机关对数据安全的保护高度重视,近年来陆续颁布了《数据安全法》《网络安全法》《个人信息保护法》等法律;同时,有关部门也制定了保护数据安全的一系列国家标准和行业规范,既是对相关法律的落实、补充与细化,也为企业数据刑事合规计划提供了法律依据、政策依据和明确标准。有学者提出,法律法规及行业规范等对企业设定了过多的数据安全保障义务,从而导致企业的义务过度增加,这是立法过度重视数据安全而忽略了对企业的合法权益保护的体现。[38]笔者认为上述观点值得商榷。特定身份的主体对危险源的管控,或者是特定身份的主体对特定法益的保护义务,使得行为人取得相应作为义务。[39]企业由于自身的经营范围或业务种类,处于对相关数据的存储或者管控状态;基于企业对数据的存储或者管控状态,我们可以认定企业具有保护数据安全的保证人地位。换言之,企业如果基于其自身的生产经营状况而产生对数据的管控状态,则企业自然具有了保证人地位,这一地位决定了企业存在相应的数据安全保障义务;反之,假如企业客观上未处于对数据的管控状态中,则我们不可能认定企业具有数据安全保证人地位,也就不可能赋予企业数据安全保障义务。法律法规并非毫无依据地过度增加企业义务,而是基于企业对数据的实际控制状态判断其是否具有保证人地位,进而决定是否赋予其数据安全保障义务,这一做法并未过度增加企业义务。

2.有利于合理限制刑法的适用范围

对于企业数据刑事合规计划可以阻却违法或是可以阻却责任,学界存在争议。有学者提出,企业数据刑事合规计划可以成为违法阻却事由;[40]也有学者则提出,企业数据刑事合规计划只能阻却企业本身的责任,即当企业涉嫌数据犯罪时,可以已经制定和实施数据刑事合规计划为由,主张企业本身不具有故意或者过失,进而主张对企业减免刑罚甚至主张企业不构成犯罪,但无法主张免除企业内部实施犯罪的自然人的刑事责任。[41]笔者赞同后一种观点。

一方面,从理论层面而言,我国刑法中将自然人犯罪和单位犯罪并列,也即自然人和单位是并列犯罪主体。企业数据刑事合规计划实质上是将法律赋予企业的数据安全保障义务内化为企业的内部规程也即企业运转过程中的“合规义务”。[42]根据新过失论,企业对企业内部员工具有监督义务,这种监督义务可以作为监督过失犯罪中的注意义务。[43]如果企业未制定或实施数据刑事合规计划,则企业对企业员工为了企业利益、以企业名义实施的数据犯罪,至少应当承担监督过失责任。而企业数据刑事合规计划的引

入,可以在事实评价上排除涉案企业的罪过认定,将企业与企业内部人员的刑事责任予以切割,这也是构建与企业数据刑事合规机制相配套的刑事激励机制的理论依据所在。如果企业制定并实施了数据刑事合规计划,且所涉数据犯罪情节显著轻微、社会危害性程度较小,可根据《刑法》第13条"但书规定",以无罪论处。[44]可见,企业数据刑事合规计划不仅可以作为量刑时的酌定从轻处罚情节,而且可以通过切割企业与企业内部人员的刑事责任而阻却企业的责任。

另一方面,从实践层面而言,司法实践中出现了因涉案企业制定并实施了有效的数据刑事合规计划而被判处无罪的案例。"杨某等侵犯公民个人信息案"中,因雀巢公司明确规定禁止其员工非法收集消费者的个人信息,且对员工进行了相关培训并要求员工签署承诺函,最终法院判决雀巢公司无罪。[45]这被称为"企业刑事合规抗辩第一案",雀巢公司因实施了数据刑事合规计划而将自身责任和内部员工责任切割,阻却了企业自身的责任。因此,企业的数据刑事合规计划有利于合理限制刑法的适用范围,避免殃及无辜,避免对经济发展和科技进步形成阻碍。

3.有利于准确把握刑法介入数据犯罪治理的时机

刑法在确定其介入规制数据犯罪行为的时机时,应注意平衡好社会治理和科技发展双重目的。包括大数据技术等在内的科学技术的发展,是全社会全人类的福祉。在技术发展的早期,必然需要一定的试错成本,刑法不能盲目介入对数据犯罪行为的规制,而需要严格的介入前提。刑法介入规制数据犯罪的前提,应当是经过了企业数据刑事合规计划与前置性法律法规的双重过滤。[46]数据犯罪的分级治理机制,将企业数据刑事合规计划作为过滤数据犯罪的"第一道屏障",将前置性法律法规作为过滤数据犯罪的"第二道屏障",将刑法作为规制数据犯罪的"最后一道屏障"。详言之,对于轻微的不当获取数据或者滥用数据的行为而言,企业数据刑事合规计划能够及时纠偏,防止其进一步恶化为数据违法行为或者数据犯罪行为;对于触犯法律底线但尚未达到犯罪标准的非法获取数据或者滥用数据的行为而言,前置性法律法规及时对其进行处理,可阻拦其进一步恶化为数据犯罪行为;对于严重的数据犯罪行为而言,才可考虑适用刑法规定对其进行刑罚处罚。这一有层次、有尺度、轻重得当、缓急分明的治理机制,有利于准确把握刑法介入数据犯罪治理的时机,防止刑法过早介入而造成对科技发展的阻碍,而企业数据刑事合规计划和前置性法律法规对违法违规获取数据或滥用数据的行为具有一定的治理和矫治作用,也防止了刑法过晚介入而无法实现有效社会治理的弊端,有利于同时实现维护社会治理和保护技术创新的双重目的。

(二)数据犯罪分级治理机制的实现路径

构建数据犯罪分级治理机制,需充分发挥企业数据刑事合规计划与前置性法律法规对数据犯罪认定的"拦截"与"过滤"作用。同时,应以适度预防理念为指导设立数据犯罪的入罪标准,准确把握刑法介入数据犯罪治理的恰当时机。

1.发挥前置性法律法规承上启下的衔接作用

与其他制裁手段相比,刑罚是最为严厉的手段,因此我们必须固守刑法的谦抑性。一方面,如果运用前置性法律法规能够对某一个危害数据安全的行为进行有效惩处,则该行为无需被纳入刑法规制范围。换言之,只有穷尽包括前置性法律法规等所有措施与手段依然无法有效惩处某一个危害数据安全的行为时,该行为才能被纳入刑法规制范围。[47]另一方面,数据犯罪是典型的法定犯,其具有双重违法性特征,即同时具有刑事违法性和行政违法性。所以,"当某种行为尚未被行政、经济法明确规定为违法之前,说明在行政经济法规看来,该行为的违法类型尚不足以确定。若将该类行为认定为犯罪,不仅缺乏前提性法律法规的支撑,也会动摇刑法属于保障法这一刑法的基础理念,是不妥当的"。[48]对于数据犯罪的规制,应首先发挥前置性法律法规以及

企业数据刑事合规计划的作用。只有在企业刑事合规计划失灵、前置性法律法规规制无效的前提下,刑法才能介入对数据犯罪行为的规制。前置性法律法规具有承上启下的衔接作用,当企业数据刑事合规计划失灵时,应考虑采用前置性法律法规对不当获取或者滥用数据的行为进行规制;当不当获取或者滥用数据行为的社会危害性极为严重时,应考虑运用最为严厉的刑罚手段予以制裁。只有充分发挥前置性法律法规承上启下的衔接作用,才能建立完善的数据犯罪分级治理机制,以准确把握实现有效社会治理与保护科技创新的刑法规制“尺度”。

同时,为更好地发挥前置性法律法规承上启下的作用,应加强科技监管手段在行政监管手段中的运用比重,提高行政监管力度,通过有效的行政规制手段降低刑事风险现实化的可能性。例如,行政监管机构可以和企业建立数据共享机制,实现监管者和被监管者之间数据的互联互通,从而使被动获取数据的传统监管模式转变为主动收集数据的科技驱动型监管模式。这有利于行政监管机构直接、实时、准确地获取企业的数据运营和处理动向,并通过建模分析,及时发现异常情况,作出预警并介入规制,在危害结果尚未实际发生之前将危机化解于无形之中。行政监管机构事前、实时、动态的监督也可以为事后治理提供详尽、有力的证据依据和参考。

2. 正确处理数据违法与数据犯罪之间的关系

作为法定犯,数据犯罪的罪状中包含前置性法律法规的规定,也即数据犯罪的构成要件是开放的犯罪构成要件,前置性法律法规对于数据犯罪的认定具有关键的定型性作用,也即前置性法律法规事实上具有填充犯罪构成要件的作用。因此有权力解释前置性法律法规的行政机关在客观上存在对刑法规范进行扩大解释的可能,也有司法机关为追求刑事违法性认定和行政违法性认定的统一,而随意扩大前置认定规范依据范围,这些都是需要加以克服的。[49] 应当看到,对于数据犯罪的认定而言,违反前置性法律法规是构成相关数据犯罪的必要不充分条件。也即行为人的行为构成相关数据犯罪,则其必然违反了前置性法律法规的规定;但反之,行为人的行为违反了前置性法律法规的规定,并不必然构成相关数据犯罪。认定某一行为是否构成数据犯罪时,不应直接以行政违法性判断替代刑事违法性判断,而应从行为侵害法益的实质解释角度,充分发挥法益的限缩功能,以免将数据违法行为误认为数据犯罪而不当扩大刑法的处罚范围。

对于违反数据安全保护制度与数据安全保护义务的数据违法行为,在何种情况下应被认定为数据犯罪,应设置一定的理论标尺和判断标准,以便进行统一的整体性、实质性判断。具体而言,确定数据违法行为犯罪化的实质认定标准时,应考虑以下因素:其一,在确定数据违法与数据犯罪的界限时,应以数据犯罪治理的特别需求为前提,以正当性、合法性、必要性、有效性作为主要判断内容,贯彻宽严相济的刑事政策立场。其二,数据犯罪作为新型犯罪,其认定标准应与传统犯罪的认定标准有所区别。认定数据违法行为是否构成数据犯罪时,应结合数据处理活动的特征、规律、应用方式等,围绕数据违法行为是否对数据的有效保护和合法利用状态或者持续安全状态造成了实质性破坏这一核心内容进行判断。其三,数据犯罪作为典型的法定犯,其认定标准应遵循法定犯的认定规律。认定数据违法行为是否构成数据犯罪时,可以采取法律拟制或者司法推定,并允许反证的存在。[50] 只有充分考虑上述因素,才能正确处理数据违法和数据犯罪的关系,合理限定数据犯罪刑法规制范围。

3. 以适度预防理念为指导设立数据违法行为犯罪化的标准

适度预防理念,从方法论意义上而言,在于为具有一般预防必要性的行为提供犯罪化标准。根据适度预防理念,不能仅因具有法益侵害性就认定行为符合犯罪化标准。只有当行为是法益侵害既遂结果发生的必经环节或者对既遂结果的发生具有不可或缺的作用时,具有一般预防必

要性的行为才可被犯罪化。具体到数据违法行为犯罪化标准的设置方面,需要满足以下两个条件:其一,穷尽前置性法律法规的防控手段。数据犯罪作为法定犯,应当具有“二次违法性”,也即当且仅当某一行为违反相关前置性法律法规的规定,其严重性程度超出前置性法律法规的规制范畴时,才进入刑法的评价视野。在数据犯罪领域存在的某一行为先进入刑法评价视野而后才被行政性法律法规规定为违法行为的现象,实属异常。例如,2009 年的《刑法修正案(七)》增设出售、非法提供公民个人信息罪和非法获取公民个人信息罪,2015 年《刑法修正案(九)》予以修正,设立侵犯公民个人信息罪,也即刑法早在 2009 年就将侵犯公民个人信息的行为予以犯罪化,但是直到 2017 年《民法总则》(已废止)才把公民个人信息作为独立人格权予以保护,2021 年才有专门保护公民个人信息的《个人信息保护法》。对于侵犯公民个人信息的行为,在民法、行政法等前置性法律法规尚未出台明确规制措施时,刑法先行入罪,实质上违背了行政犯“二次违法性”特征,也不符合刑法作为“社会最后一道防线”的保障法地位。其二,遵循比例原则。对于可能危害国家安全、为恐怖活动等严重危及公共安全的犯罪行为提供助力或者可能造成无法进行事后补救的损失的数据犯罪,可以奉行“打早打小”原则,以积极刑法观为指导,将具有一般预防必要性的行为予以犯罪化。而对于其他类型的数据违法行为,应着重突出前置性法律法规的治理作用,严守刑法的保障法地位。[51] 如此,方能准确把握刑法介入社会治理的限度。

五、结　语

采用单一刑法手段规制数据犯罪的单向度国家监管模式存在很大局限性,对于数据犯罪的治理,不应局限在刑法的闭塞体系中,而应实现企业内控机制与国家监管规则之间的功能化互动,为数据犯罪治理提供充足的外部制度补给与支撑,构建内外共治的数据犯罪“双轨”治理格局。同时,为了同时实现对数据犯罪的治理“到位”和避免刑法“越位”,应准确把握刑法介入数据犯罪治理的时机,构筑防范数据犯罪的“三道防线”:发挥企业自身能动性,通过企业数据刑事合规计划推进对数据犯罪的预防,构筑“第一道防线”;利用前置性法律法规限制数据犯罪相关罪名的适用范围,构筑“第二道防线”;将刑法作为保护数据安全、惩治数据犯罪的“最后一道防线”,由此形成数据犯罪的分级治理格局。

发挥刑法的社会保护机能,构建保护数据资源的刑事法治规则体系,是增强大数据时代数字经济风险防控能力的重要路径,也是实现国家治理能力现代化的时代课题。笔者在文中所提出的数据犯罪“双轨 + 分级”治理机制并非盖棺之论,更重要的目的在于抛砖引玉,以求引发立法者、司法者与研究者更多的关注与思索,共同对数据犯罪刑法治理模式进行省思与厘革,探寻数据犯罪刑法规制的恰当路径,实现科技进步、经济发展与社会治理之间的平衡。

注释:

〔1〕〔7〕〔37〕〔51〕贾宇:《数字经济刑事法治保障研究》,《中国刑事法杂志》2022 年第 5 期。

〔2〕房慧颖:《数据犯罪刑法规制的具象考察与策略优化》,《宁夏社会科学》2023 年第 3 期。

〔3〕〔34〕敬力嘉:《个人信息保护合规的体系构建》,《法学研究》2022 年第 4 期。

〔4〕魏东:《功能主义刑法解释论“问题性思考”命题检讨》,《法学评论》2022 年第 2 期。

〔5〕于改之:《从控制到利用:刑法数据治理的模式转换》,《中国社会科学》2022 年第 7 期。

〔6〕张明楷:《论帮助信息网络犯罪活动罪》,《政治与法律》2016 年第 2 期。

〔8〕周光权:《转型时期刑法立法的思路与方法》,《中国社会科学》2016 年第 3 期。

〔9〕张明楷:《刑法学》(上),北京:法律出版社,2016 年,第 147 页。

〔10〕〔美〕富勒:《法律的道德性》,郑戈译,北京:商务印书馆,2005 年,第 15 页。

〔11〕《马克思恩格斯全集》第 6 卷,北京:人民出版社,1961 年,第 291 – 292 页。

〔12〕姜涛:《为风险刑法辩护》,《当代法学》2021 年第 2 期。

〔13〕高铭暄、孙道萃:《预防性刑法观及其教义学思考》,《中国法学》2018 年第 1 期。

〔14〕〔德〕汉斯·J. 沃尔夫等:《行政法》第三卷,高家伟译,北京:商务印书馆,2007 年,第 3 页。

〔15〕房慧颖:《新型操纵证券市场犯罪的规制困局与破解之策》,《华东政法大学学报》2022 年第 1 期。

〔16〕房慧颖:《人工智能犯罪刑事责任归属与认定的教义学展开》,《山东社会科学》2022 年第 4 期。

〔17〕程红:《德国刑事立法的最新动态及解读》,《国外社会科学》2019 年第 4 期。

〔18〕〔美〕理查德·A·波斯纳:《法理学问题》,苏力译,北京:法律出版社,2002 年,第 210 页。

〔19〕〔瑞士〕比扬·法塔赫 – 穆加达姆:《刑法中的创新责任:在严格责任、过失与容许风险之间》,唐志威译,《苏州大学学报(法学版)》2022 年第 3 期。

〔20〕孙国祥:《刑事合规的刑法教义学思考》,《东方法学》2020 年第 5 期。

〔21〕〔27〕于冲:《数据安全犯罪的迭代异化与刑法规制路径——以刑事合规计划的引入为视角》,《西北大学学报(哲学社会科学版)》2020 年第 5 期。

〔22〕王林、孙吉:《AI 安防企业被曝数据泄露 敲响人脸识别安全警钟》,《中国青年报》2019 年 2 月 26 日。

〔23〕刁生富、姚志颖:《大数据技术的价值负载与责任伦理建构——从大数据“杀熟”说起》,《山东科技大学学报(社会科学版)》2019 年第 5 期。

〔24〕潘斌:《风险社会与责任伦理》,《伦理学研究》2006 年第 3 期。

〔25〕闫宏秀:《数据赋能的伦理基质》,《社会科学》2022 年第 1 期。

〔26〕李玉华、冯泳琦:《数据合规的基本问题》,《青少年犯罪问题》2021 年第 3 期。

〔28〕李本灿:《刑事合规制度的法理根基》,《东方法学》2020 年第 5 期。

〔29〕石磊:《刑事合规:最优企业犯罪预防方法》,《检察日报》2019 年 1 月 26 日。

〔30〕〔36〕孙国祥:《企业合规改革实践的观察与思考》,《中国刑事法杂志》2021 年第 5 期。

〔31〕刘伟:《刑事合规的溯源、反思与构建》,《江海学刊》2021 年第 4 期。

〔32〕汪明亮:《作为犯罪治理方式的企业合规》,《政法论坛》2020 年第 3 期。

〔33〕〔49〕张勇:《数据安全刑事合规的滤罪模式》,《学术论坛》2022 年第 3 期。

〔35〕于冲:《网络平台刑事合规的基础、功能与路径》,《中国刑事法杂志》2019 年第 6 期。

〔38〕刘艳红:《无罪的快播与有罪的思维——“快播案”有罪论之反思与批判》,《政治与法律》2016 年第 12 期。

〔39〕许玉秀:《当代刑法思潮》,北京:中国民主法制出版社,2005 年,第 590 页。

〔40〕黎宏:《合规计划与企业刑事责任》,《法学杂志》2019 年第 9 期。

〔41〕姜涛:《数字安全与刑事合规建设》,《检察日报》2021 年 11 月 4 日。

〔42〕韩轶:《企业刑事合规的风险防控与建构路径》,《法学杂志》2019 年第 9 期。

〔43〕王志祥、融昊:《刑事合规中主体监管义务的教义学分析》,《法律适用》2021 年第 7 期。

〔44〕卢勤忠:《民营企业刑事合规的理论基础和实践展开》,《辽宁师范大学学报(社会科学版)》2021 年第 5 期。

〔45〕甘肃省兰州市中级人民法院(2017)甘 01 刑终 8 号刑事裁定书。

〔46〕房慧颖:《刑法谦抑性原则的价值定位与规范化构造——以刑民关系为切入点》,《学术月刊》2022 年第 7 期。

〔47〕陈兴良:《刑法哲学》,北京:中国政法大学出版社,2004 年,第 7 页。

〔48〕何荣功:《刑法“兜底条款”的适用与“抢帽子交易”的定性》,《法学》2011 年第 6 期。

〔50〕孙道萃:《数据犯罪刑事合规治理的边界》,《西南政法大学学报》2022 年第 6 期。

〔责任编辑:邹秋淑〕