

数据合规刑事减免责功能的理解与适用

刘艳红* 龚文博**

内容提要: 随着数据日益成为重要犯罪对象,数据安全类犯罪逐渐转向企业行为,而罚金刑的威慑效果和预防效果较为有限,难以应对泛在的数据安全风险。我国引入具有预防与惩治双重面向的数据合规激励机制,在惩治企业违规数据处理行为的同时预防数据安全风险。涉案企业合规整改过程中,修复数据安全类犯罪保护的个人信息法益并重构数据安全管理体系,替代性遭受处罚措施。多种制裁方式的灵活并用和预防性的数据合规体系是能够真正实现制裁效果和预防效果的实质制裁机制,涉案企业因而获得减免责的刑事激励及改过自新的机会。数据合规整改以包含认罪悔罪的整改承诺为前提,以开展针对性整改活动和规范数据处理流程为内容,以制定全方位监测措施为保障,以数据处理全流程的整改防控为核心,形成“风险预防—风险识别—违规应对”一体化的数据保护合规体系。数据合规体系贯穿刑事诉讼全流程,在侦查阶段、审查起诉阶段通过合规不起诉制度,在审判量刑阶段通过宽缓量刑或合规缓刑实现刑事减免责功能。

关键词: 数据合规 合规减免责 实质制裁论 全流程合规 法院参与

一、引言:数据安全风险的泛在化及合规激励的犯罪治理方式

2023年2月27日,中共中央、国务院印发的《数字中国建设整体布局规划》强调,数字中国的建设需夯实数字基础设施和数据资源体系“两大基础”,两大基础体系的建立健全以保障国家数据安全为前提,数据安全已经上升至国家安全的战略高度。由于企业逐渐成为数据安全问题的主要阵地、数据违法犯罪已经由个人行为转向企业行为,^[1] 为了切实保障数据安全,不少学者提出数据安全法益观,并将其纳入刑法的保护范围,旨在发挥刑罚的威慑功能抑制企业违规处理数据行为的发生。^[2] 但传统刑事制裁针对企业犯罪仅设立单一的罚金刑,不仅容易使企业造成“交钱了事”的刻板印象,而且其犯罪预防

* 中国政法大学刑事司法学院教授、博士生导师。本文是2021年度国家社科基金重大项目“数字经济的刑事安全风险防范体系建构研究”(项目编号:21&ZD209)的阶段性研究成果。

** 中国政法大学刑事司法学院博士生。

[1] 参见于冲:《动态数据与动态安全:大数据时代个人信息的刑法保护进路》,中国法制出版社2021年版,第200页。

[2] 参见杨志琼:《我国数据犯罪的司法困境与出路:以数据安全法益为中心》,载《环球法律评论》2019年第6期;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》,载《法学论坛》2020年第2期。

效果有限,难以应对泛在的数据安全风险,需引入能够有效预防数据安全风险、防范数据安全类犯罪的新型治理方式。

首先,企业处理数据过程中的刑事安全风险泛在,数据安全类犯罪案发率居高不下。一方面,企业处理数据过程中会面临用户、员工、第三方合作商等多方主体和数据被非法收集、非法存储、非法提供等多种样态的刑事安全风险;另一方面,结合当前刑事法律体系的相关规定,企业数据处理过程中,用户、员工、第三方合作商的违规行为,可能使企业构成非法获取计算机信息系统数据罪、破坏计算机信息系统罪等数据类犯罪,也可能构成侵犯著作权罪、侵犯商业秘密罪等知识产权犯罪,还可能构成财产类犯罪和侵犯公民个人信息罪。正如最高人民检察院最新公布的数据显示,数据信息日益成为重要犯罪对象、威胁数据信息安全类犯罪常见多发,^[3] 数据安全风险广泛存在于数据处理全流程,为了保障数据安全,需对企业数据违法犯罪活动加以规制。但若过度强调数据安全的刑法保护,会与“统筹推进数据产权、流通交易、收益分配、安全治理”^[4] 和数字经济的高质量发展需求相违背,应在保障企业动态处理数据过程中数据安全的同时兼顾数据要素的开发利用。

其次,数据合规激励机制可以有效防范数据安全风险、避免数据违法犯罪活动。由于先前以刑罚为主的单一制裁措施无法防范企业数据处理过程中泛在的数据安全风险且会造成民营企业面临“一管就死”的现实困境,^[5] 在有关部门的部署与推进下,经过长达四年的试点工作,我国逐渐形成合规激励的新型犯罪治理方式,民营企业在合规制度的驱动下搭建民行刑协同共治的数字经济安全风险防范体系,^[6] 通过构建“风险预防—风险识别—违规应对”一体化的数据合规体系,有效防范数据安全风险,避免风险的现实化。如《中兴通讯隐私保护白皮书》中明确,其构建合规体系的首要目标在于“满足法规要求,充分防控风险”,中兴公司通过将合规要求嵌入业务流程,预防潜在数据安全风险,避免监管处罚和司法诉讼,有效应对和处置数据安全事件,系统性控制数据安全风险。

最后,数据合规激励机制具有刑事减免责功能,可以避免因涉案企业遭受刑事制裁措施和刑罚的附随后果,阻碍数据进一步地开发利用并波及无辜第三方。企业合规作为一种刑事激励机制被引入我国司法实践中,合规刑事减免责功能是我国当前合规试点工作的重心所在,涉案企业可以通过构建合规体系换取检察机关的不起诉决定或人民法院的宽缓量刑,企业的合规整改效果成为影响企业刑事责任的因素之一。如在最高人民检察院公布的第三批企业合规典型案例中,上海Z公司违规获取E平台店铺信息、订单信息等数据后,与3家大型互联网企业达成数据合作,完成数据合规建设的整改措施,将合规内化为企业内部长效机制,被检察机关不起诉处理。^[7] 企业通过构建数据合规体系形成有效防范数

[3] 参见孙凤娟:《最高检召开新闻发布会并发布典型案例 为良好网络生态提供有力法治保障》,载《检察日报》2024年2月24日,第1版。

[4] 参见《习近平主持召开中央全面深化改革委员会第二十六次会议强调 加快构建数据基础制度 加强和改进行政区划工作》,载《人民日报》2022年6月23日,第1版。

[5] 参见刘艳红:《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》,载《社会科学辑刊》2024年第1期。

[6] 参见刘艳红:《合规驱动:民行刑协同共治数字经济安全风险防范体系构建》,载《江苏社会科学》2024年第1期。

[7] 参见张昊:《能动履职提升企业合规改革工作质效》,载《法治日报》2022年8月11日,第3版。

据安全风险机制,可以达到预防再犯罪的效果,^[8]也表征其特殊预防必要性的降低,实现合规减免责功能。一旦企业遭受刑罚处罚,则可能对企业的用户、员工、第三方合作商等无辜第三者造成不利影响,合规激励则可以避免这种刑罚“水波效应”。^[9]

综上所述,合规激励机制可以有效防范企业数据处理过程中泛在的数据安全风险,且具有刑事减免责功能,可以避免企业因遭受刑事制裁被宣告“死刑”和波及无辜第三者,有助于统筹推进数据的开发利用和安全治理。但作为一种新型治理方式,数据合规刑事减免责功能的理论依据及适用方式尚不明确,本文将围绕数据合规刑事减免责功能的合法性依据、可行性前提及实践性规则展开探讨。

二、数据合规刑事减免责功能的理论依据:实质制裁论

在面临数据安全风险或涉及数据安全类犯罪时,涉案企业通过业务改造、处理责任人等合规整改活动,以契合涉案企业合规改革的“严管”机制定位,同时涉案企业积极补救挽损、修复受损法益并构建预防性的数据安全合规体系,应落实“厚爱”的刑事治理理念,注重刑法的谦抑性,发挥合规的刑事减免责功能,使合规激励机制成为刑罚制裁功能的有效替代和有效犯罪预防功能的必要补充。^[10]简言之,涉案企业构建的数据合规体系作为能够真正实现制裁效果和预防效果的实质制裁机制,具有刑事减免责功能。

(一)“严管”与“厚爱”相结合的刑事治理理念

数据合规激励机制践行“严管厚爱”的治理理念,兼顾预防与惩治的双重面向,减免涉案企业的刑事责任并替代性落实相应处罚措施,贯彻实质制裁论。2022年3月8日,最高人民检察院工作报告强调:“依法可不捕、不诉的,责成涉案企业作出合规承诺、切实整改;与国务院国资委、全国工商联等8部门共建第三方监督评估机制,司法、执法、行业监管联手,以严管体现厚爱。”^[11]涉案企业的数据合规体系包含针对犯罪行为的应急处置、整改措施与预防违法、犯罪行为的数据合规计划,鉴于其积极补救挽损、修复受损法益、再犯可能性的降低而获得减免刑事责任的激励效果,在惩治违规数据处理行为的同时预防数据安全风险,促进涉案企业合规经营。

一方面,涉案企业及时开展合规整改活动、制定有效预防犯罪的数据合规计划,是基于实质制裁论减免其刑事责任的“厚爱”基础。其一,企业涉嫌数据安全类犯罪后及时应急处置、补救挽损并开展合规整改活动的行为,是减轻预防刑的量刑情节。合规整改作为涉案企业的事后纠错机制,在侵犯数据安全类犯罪已经成立的情形下,无法通过犯罪论体系而影响其责任(刑)的认定,但其立即停止违规行为并作出合规承诺,及时采取查漏补缺的补救措施,凸显其悔罪意图使其预防必要性减小。其二,数据合规的犯罪预防面

[8] 参见陈瑞华:《企业合规不起诉改革的八大争议问题》,载《中国法律评论》2021年第4期。

[9] 参见陈瑞华:《企业合规改革与刑事诉讼立法》,载《政法论坛》2024年第1期。

[10] 参见刘艳红:《涉案企业合规建设的有效性标准研究》,载《东方法学》2022年第4期。

[11] 参见《最高人民法院工作报告——2022年3月8日在第十三届全国人民代表大会第五次会议上》,载最高人民法院网, https://www.spp.gov.cn/spp/gzbg/202203/t20220315_549267.shtml, 2024年3月5日访问。

向,表征其再犯可能性的降低,成为减轻预防刑的正当化依据。涉案企业结合具体数据处理的业务内容和业务流程,通过完善内部人员和机构配置、制定合规评估与安全审计文件、加设监督检查体系等方式,构建能够长期、有效预防数据安全风险的专项合规计划,并通过岗前培训、定期教育培训等途径推动合规计划的落实与合规文化的形成,体现了企业预防再犯罪的决心,表征了社会危险性及其再犯可能性的降低,进而成为减免刑事责任的事由。其三,对涉案企业减免刑事责任或合规不起诉,是“厚爱”理念的实现途径。数据合规通过设立具有刑法问责性预期的预防规则,使涉案企业的一般预防必要性与其再犯可能性即特殊预防必要性降低,影响企业的预防刑认定,在立法尚未认可的情形下,结合“严管厚爱”的治理理念及相应的刑事政策,给予涉案企业刑事激励,促进企业的合规经营和数字经济的稳步发展。

另一方面,涉案企业基于风险识别机制查找经营漏洞和潜在的数据安全风险,并针对性开展整顿提升的合规整改活动是“严管”的主要替代措施之一,^[12]涉案企业合规整改的过程中大量的人力、物力投入体现了实质制裁的理念。合规整改作为多部门协同合作、第三方评估机构积极参与的一种纠错机制,涉案企业需积极评估、及时发现、立即停止数据处理违规行为,并针对性地纠正违法事实和开展整改活动,处理违规责任人并完善人员配置。涉案企业虽获得减免责任的刑事激励,但在整改过程中需投入多方人力物力的支持,且需面临行政处罚等非刑罚处罚措施,企业遭受实质性制裁。即使无须遭受较大数额的行政处罚,在风险识别、监测、应对,以及后续制定预防性合规计划的过程中,涉案企业均需大量的资金及人员投入,以保障合规计划的完善与落实。长期的、自发的、系列的合规举措体现了涉案企业事后补救挽损的积极态度,也反映了对所有违规数据处理行为均加以惩治的“严管”理念。结合企业的社会责任与经济使命,应注重刑法的谦抑性,企业依据前置数据法规进行民事赔偿并接受行政处罚足以规制其违规行为时,减免其刑事责任,给予企业一个改过自新的机会,在“向后看”(惩治)的同时注重“向前看”(预防),落实宽严相济的实质制裁理念。

(二) 基于法益修复理论的宽缓刑事政策

数据合规以预防数据安全类风险、防范数据安全类犯罪为最终目的,兼具实质制裁的目的,与恢复性司法将刑罚的视角从消极的控制与惩罚转向积极预防相契合。涉案企业通过弥补与修复受损的数据法益,缓和社会矛盾,获得减免责任的刑事激励及改过自新的机会。

首先,数据合规以法益修复为前提,基于恢复性司法理念与宽缓的刑事政策,修复被侵害法益而获得刑事激励。不同于刑事制裁的惩戒性,恢复权利性制裁旨在消除非法行为造成的损害,注重既遂之后行为人主导的危险消除与法益恢复的良善行为,恢复被侵害的合法权利,保证已有义务的履行,是“法益可恢复性犯罪”出罪化、轻刑化刑法评价的论证渊源。^[13]也就是说,数据安全类犯罪既遂后,若涉案企业立即停止违规行为并消除不良影响,能够恢复被侵害的社会秩序与个人权益,则基于恢复性司法理念,对其轻刑化

[12] 参见李玉华:《企业合规本土化中的“双不起诉”》,载《法制与社会发展》2022年第1期。

[13] 参见庄绪龙:《“法益可恢复性犯罪”概念之提倡》,载《中外法学》2017年第4期。

的实质制裁是正当、可行的。企业犯罪成立后,合规整改即意味着立即停止违规行为并采取补救挽损措施,避免损害的进一步扩大,处罚相关责任人并向检察院或法院作出合规整改承诺。若涉案企业能够修复违规数据处理行为侵害的法益,则基于恢复性司法理念与“少捕慎诉”的宽缓刑事政策,合规整改可以成为诉讼和量刑中获得宽大处理的重要因素。

其次,数据安全类犯罪侵害的数据安全管理秩序与被害人个人权益均可修复。其一,若涉案企业侵犯数据安全犯罪保护的数据安全管理秩序的,修复受损法益时不同于直接采取国家强制性措施惩治相关责任人,涉案企业在数据安全相关主管部门的介入下,通过采取补救挽损、赔偿损失等方式正向维护数据安全管理秩序的不可亵渎性,重构该社会秩序。其二,若涉案企业侵犯海量数据承载的个人信息自决权、知识产权、财产权等个人权益,合规整改虽然无法采取返还原物、恢复原状等重置性措施将法益恢复至原始状态,但并不涉及被害人的人身权益,涉案企业可以通过立即停止违规行为、加置安全保障措施、赔礼道歉、经济补偿等多举措修复被侵害的个人法益、弥补被害人损失。其三,对于被侵害的各类法益,修复的侧重点有所不同。对于社会秩序,企业通过积极履行合规义务维护数据安全管理制度,侧重于积极的法益重构;而对于个人法益,则通过赔偿、恢复声誉等弥补损失、缓和被害人情绪,侧重于消极的补救挽损。

最后,数据合规因重构被侵害的数据安全管理秩序、弥补被害人损失而具备减免刑事责任功能,落实实质制裁理念。基于以法益恢复为基础的犯罪合作理论,企业犯罪后与行政机关合作或采取其他方式恢复被侵害的法益,则可以免责。^[14]而当前实践试点过程中的数据合规恰属于涉案企业在检察机关或人民法院的主导下,多机关共同参与的整改机制,通过建立符合数据法规的合规体系,证实涉案企业对数据安全管理制度尊重与维护,重构数据安全管理秩序。同时,对于被害人的损失,即使涉案企业遭受罚金刑、责任人入狱,对于被害人也无济于事;而合规整改注重消除不法后果,弥补被害人损失、修复被侵害的个人法益,积极重构各类法益,并使涉案企业得到实质制裁。涉案企业开展数据合规整改活动会产生积极的社会效应、行业效果,使数据处理者的预防必要性降低,而“责任的内容,不应当和科处刑罚的实质意义即犯罪的一般预防和特殊预防分开考虑”^[15],应注重刑罚的预防目的对责任的影响,数据处理器因合规整改而获得轻刑化处理。

(三) 替代刑罚功能的多元刑事制裁方法

数据安全类犯罪涉及行业规范、数据法规、知识产权法规、刑法法规等多层次、多维度的问题,单靠刑事法律的“孤军作战”,难以取得良好的社会治理效果。检察机关、人民法院开展企业合规改革以推动源头治理为着力点,会同有关部门综合运用经济、行政、刑事等手段促进企业依法合规经营发展,对于完善制度机制、形成治理合力具有积极意义。^[16]刑罚作为国家强制力为保障的惩戒性措施过于严厉且单一,在行业处罚、民事赔

[14] 参见姜涛:《法定犯中行政前置性要件的法理基础与制度构造》,载《行政法学研究》2022年第1期。

[15] [日]大谷实:《刑法讲义总论》,黎宏译,中国人民大学出版社2008年版,第287页。

[16] 参见徐日丹:《真严管真厚爱,做好服务企业“后半篇文章”》,载《检察日报》2022年6月4日,第1版。

偿、行政处罚等前置性制裁足以规制违规行为，使涉案企业得到有效制裁时，应注重刑法的谦抑性，多种制裁方式的灵活并用是贯彻实质制裁论的具体体现。

一方面，实质制裁论以有效制裁为具体内涵，要求数据合规整改注重多元制裁方法并举。网络大数据的蓬勃发展使以数据为对象的犯罪呈现多样化的局面，而我国当前针对单位犯罪仅存在罚金刑，且罚金刑容易使企业造成“交钱了事”的刻板印象，不利于保障刑法规范的行为规制能力，而企业合规整改过程中的多元化制裁方式有利于针对性惩治违规行为。首先，数据合规整改作为犯罪行为成立后，涉案企业的自主应对机制，企业内部需采取针对责任人的惩戒、补救措施；其次，数据合规整改涉及行业规范与前置数据法规，在企业违规处理数据侵害数据安全秩序或知识产权等个人权益时，履行数据安全保护责任的部门可依情形作出责令改正、警告、责令暂停或终止提供服务、罚款等多重处罚，且涉案企业需承担损害赔偿等侵权责任；最后，数据合规整改的过程中，涉案企业修复被侵害法益、完善数据合规体系需要大量的资金投入，将本应科处的罚金刑变相运用至数据安全秩序维护，是一种带有民事制裁性质的辅助性措施。

另一方面，数据合规整改的严厉性并不亚于刑事制裁，确保涉案企业得到相适应的实质制裁。各种制裁的严厉程度对企业而言与对自然人而言有所差异，有学者以企业为对象提出“强制手段金字塔”，相较于罚金，暂扣许可证件、吊销许可证件对于企业是更为严厉的限制从业资格的法律后果，而责令停产停业、责令关闭则相当于对企业宣告“死刑”。^[17]且根据最高人民法院公布的企业治理模式的司法探索流程图，在涉案企业合规整改的过程中，检察机关认为需要行政追责的，可以通过检察建议的方式，建议行政机关作出行政处罚，^[18]即依据前置数据法规，数据处理者的违规行为情节严重时，行政监管部门可以作出暂扣许可证件、吊销许可证件、责令停产停业等行政处罚。此时，于企业而言，合规整改比刑事制裁更为严厉。

三、数据合规刑事减免责功能的必要前提：全流程合规

依据实质制裁论，涉案企业开展数据合规整改活动并经验收合格足以真正实现制裁和预防效果，可以获得减免刑事责任的激励效果，但有效合规整改的内部构成要素即减免责的事实依据仍需进一步探究。由于数据合规整改以包含认罪悔罪的整改承诺为前提，以开展针对性整改活动、制定或完善预防性合规计划和规范数据处理流程为内容，以制定全方位监测措施为保障，故其减免责功能以有效整改、长效预防和全面监测的数据保护体系为必要前提，即合规减免责功能以数据处理全流程有效的整改防控为核心。

（一）采取针对性消除数据安全漏洞的整改措施

在制定或完善预防性的数据合规计划之前，企业整改承诺的落实需主动开展内部合规自查活动，查明犯罪原因并形成合规“自查报告”，进而精准且有针对性地消除犯罪原因。不同于风险防范的不确定性，涉案企业针对具体违规行为，需结合内部情况，靶向消

[17] 参见刘鹏、王力：《回应性监管理论及其本土适用性分析》，载《中国人民大学学报》2016年第1期。

[18] 参见蒋安杰：《企业合规：企业治理模式的司法探索》，载《法治日报》2021年3月17日，第9版。

融犯罪诱因,采取补救措施修复受损法益并预防犯罪行为的再次发生。针对性的整改行为是合规整改的启动程序、激发减免责功能的基本条件。

一方面,涉案企业需主动开展全面的合规自查活动,识别并分析犯罪诱因。在发现数据安全类犯罪行为后,涉案企业应迅速开展自查自纠活动,以查明犯罪原因为导向,探究企业管理制度或治理结构等方面的合规管控漏洞,将客观原因分析和主观原因分析相结合,剖析违规行为的具体诱因,以真正体现企业对自身犯罪行为的认识;^[19]同时,涉案企业还需开展全面性合规自查活动,识别潜在的合规隐患及未发现的其他犯罪行为,查明内部管理漏洞和治理缺陷,并针对性改进内部合规管理体系进而形成合规文化,落实合规整改预防犯罪的目的。如最高人民检察院公布的第三批企业合规典型案例中,K公司员工泄露内幕信息产生犯罪行为后,在第三方组织的引导下,K公司深入挖掘犯罪成因的同时,以合规风险自查清单形式逐员、逐部门排查合规风险点,并制定多个层面的信息保密专项合规计划,而被第三方机构认定整改效果良好。^[20]在企业违规处理数据构成犯罪时,首先,涉案企业要结合具体法益侵害类型从数据处理流程入手,查明犯罪原因与具体责任人;其次,企业的自查自纠活动不应局限于某一业务流程,而要全方位查明内部数据安全漏洞,避免未发现的数据安全风险现实化、损害扩大化。

另一方面,涉案企业对犯罪诱因作出针对性补救措施,预防再次发生同类型犯罪。针对性整改行为是减免刑事责任的基础。涉案企业通过内部自查活动,查明犯罪原因并加以分析后,应针对性弥补组织管理漏洞并完善内部安全体系等内控机制,对不同类型的数据安全类犯罪采取相应的补救挽损措施,防范再次发生同类违规行为。对于员工违规处理数据的行为或此类风险,涉案企业因未落实对员工的监督管理义务而触及犯罪,故在处置责任人、消除风险点的基础上,应明确员工处理权限,加强数据处理审批程序,合理配置监督管理人员,建立内部管控机制。对于第三方合作商违规处理数据的行为或此类风险,涉案企业因未落实对数据的安全保护义务而触及犯罪,应通过签订使用协议等方式提醒、明确第三方的处理权限,并强化内部数据安全技术保障措施,完善数据安全管理体系。对于企业违规处理数据的行为或此类风险,涉案企业因治理结构失灵、缺乏内部制约而触及犯罪,应及时解散相关决策机构、调离责任人,引入合规监管机构、明确合规监管权限,规范内部决策机制。在采取类型化补救措施的基础上,涉案企业应结合内部具体情况,生成定制化方案,在针对性消除安全隐患的同时,注重重点领域、薄弱环节和重要岗位的风险防范。

(二) 制定有效预防数据安全风险的合规计划

在作出针对性整改措施后,涉案企业应制定或完善数据保护合规计划,形成以预防数据安全风险为宗旨,以全流程合规处理数据为主线,以落实对员工的监督管理义务、对数据的安全保护义务为内容,以充分设计、有效监测、可实际执行为关键考量因素的数据保

[19] 参见 [德] Marc Engelhart:《德国经济刑法的发展与现状》,陈尔彦译,载刘艳红主编:《东南法学》第11辑,东南大学出版社2017年版,第146页。

[20] 参见孙凤娟:《深化典型案例示范指引 推进涉案企业合规改革》,载《检察日报》2022年8月11日,第2版。

护合规计划。涉案企业制定有效预防数据安全风险的合规计划，是降低其预防必要性、发挥刑事减免责功能的必备条件。

在针对性整改、消除违规行为之余，涉案企业建立预防数据安全风险的合规体系，以形成数据处理全流程合规的企业文化为追求。其一，数据保护合规计划应包含与第三方签订的风控协议，约定第三方主体的数据处理权限，履行对数据的安全保护义务，规避第三方主体带来的外部数据安全风险。其二，数据保护合规计划需规范企业内部的数据处理流程，通过员工手册和岗位培训等途径明确员工处理数据的程序与权限，尽到对员工的监督管理义务，遏制员工超越授权导致的违规数据处理行为，阻断企业的组织体责任。其三，数据保护合规计划促进形成数据合规文化，制定数据合规政策，培养员工合规处理数据的行为意识与行为习惯，并改善内部治理结构，完善合规监管人、内部监督举报等机制，形成真正有效的数据保护合规计划。

企业应结合风险点与自身需求，定制数据保护合规计划，并持续改进、动态落实合规计划，方能有效预防数据安全风险。不同类型、不同级别企业的数据安全风险指数及防范需求有所差异，涉案企业应结合其用户规模和业务种类，细化其合规计划内容，使定制的数据保护合规计划扎根于企业内部，形成有效预防、现实可操作的合规计划，并塑造特有的企业文化。为了避免企业机械地响应有效性审查评估的要素制定“纸面化”的合规计划，但不足以执行落地和预防企业风险，改革决策者可选择在消除企业的管理漏洞和治理缺陷后，建立针对性、可行性合规管理体系的模式，发挥合规整改长远的犯罪预防效力。^[21]但“合规风险是动态的，会随着环境、业务等因素动态变化”，合规计划的针对性要求“对监测到的风险以及已经实现的风险作出反应”。^[22]即使是验收合格的数据保护合规计划在执行的过程中也会出现新的安全风险、漏洞，企业制定的合规计划要想全面落实预防犯罪的功能，就不能一成不变，而需持续更新、应对风险。

（三）形成全方位监测数据安全风险的识别机制

涉案企业针对性开展整改活动和形成有效合规计划实现减免责和预防犯罪的目的，以能够及时发现数据安全风险为前提，以企业具有监测分析数据安全风险的敏锐识别机制为技术保障。由于合规风险来源的不确定性和类型的多样性，风险识别机制需实时地、全方位地监测企业数据处理活动，避免内外部数据安全风险的现实化。

一方面，风险识别机制是有效合规整改的重要组成部分。合规整改体系由风险预防机制、风险识别机制和违规行为应对机制组成。其中，风险预防机制和违规行为应对机制与降低预防必要性直接关联，是减免企业刑事责任的首要条件和必要条件；风险识别机制是实时监测数据处理活动、筛查内外部数据安全风险，并在发现风险后及时作出安全预警提示，便于迅速开展应急处置活动、控制风险的间接保障性机制，以提高风险预防的有效性和违法应对的准确性。具体而言，在企业犯罪成立后，风险识别机制可及时筛查、识别、确定风险源，针对性开展整改活动，从源头消除不法要素、避免损害后果的进一步扩大。

[21] 参见陈瑞华：《企业有效合规整改的基本思路》，载《政法论坛》2022年第1期。

[22] 李勇：《涉罪企业合规有效性标准研究——以A公司串通投标案为例》，载《政法论坛》2022年第1期。

在企业合规考察验收合格后,由于风险的多变性与频发性,风险识别机制仍需监测内部数据处理活动,规避数据安全风险,确保预防性合规计划的有效执行。在合规整改完成后,风险识别机制可并入数据安全保护体系保障企业合规开展数据处理活动。换言之,风险识别机制贯穿企业数据处理全流程,是有效预防犯罪的有力工具。

另一方面,风险识别机制全面监测企业数据处理活动、有效预防数据安全风险,降低企业的预防必要性,是减免企业刑事责任的重要条件。首先,风险识别机制以专业监测设施为技术基础。由于信息网络算法复杂化和风险隐蔽化的特征,企业数据处理过程中存在难以发现的潜在安全风险,无法满足合规自治的需求,而对智能技术最有效的治理就在于“以技术反制技术”,即通过“反制技术”作为企业自治的具体形式,引入专业性和技术性的风险识别机制,通过监测技术、检测技术和数据分析等“反制技术”,实时监测企业的数据处理活动及其算法技术的更新,尽早识别、追踪内外部的风险和异常。^[23]其次,风险识别机制以全面监测风险为主要内容。由于数据安全风险无时不在、无处不在而又隐秘、难以察觉,存在泛在化趋势,^[24]对于数据安全风险无法实现精准监测、定向预防,故笔者认为,在实时监测的同时也应做到全方位监测,智能化识别内外部数据安全风险后便于后续纠正、消除,通过“打早打小”,全面确保企业的合规经营。最后,风险识别机制以及时安全预警为重要措施。企业智能化识别数据安全风险后,应迅速记录、作出安全预警提示并按要求报告,发挥安全保护措施与违规应对机制的应急处置效用,评估风险并针对性地补救、消除,避免同类风险的再次发生,形成“风险预防—风险识别—违规应对”一体化的数据保护合规体系。

四、数据合规刑事减免责功能的诉讼全流程贯彻与适用

数据合规整改因针对性的应急处置和有效的预防性合规计划减轻了企业的预防必要性,在宽严相济的刑事政策下,减免其刑事责任是正当且可行的。但当前司法实践试点过程中,合规整改多限于检察机关通过不起诉制度在审查起诉阶段直接免除涉案企业的刑事责任,而相对忽视合规整改在侦查、审判量刑等阶段减免责功能的适用。对此,笔者认为,应积极重构数据合规的司法适用规则,明确其在不同诉讼阶段对认定数据处理者刑事责任的具体影响。

(一) 侦查阶段的数据合规减免责

先前合规改革试点案例多为审查起诉阶段的合规整改,这与检察机关主导改革试点工作密切相关。为了进一步扩大刑事合规的司法适用,学界围绕合规中检察职能延伸的主题,试图将研究视角从审查起诉阶段向前延伸到侦查阶段、向后扩展到审判执行阶段,探究刑事诉讼全流程中的检察职能,进而明晰合规整改在不同诉讼阶段的司法适用。^[25]

[23] 参见刘蓓:《智能社会中技术治理与法律治理关系论纲》,载《上海师范大学学报》2022年第2期。

[24] 参见刘双阳:《风险泛在语境下间接危险犯的扩张逻辑与教义限缩——以信息散布型网络犯罪为视角》,载《河南财经政法大学学报》2020年第6期。

[25] 参见董坤:《检察机关在侦查阶段推进企业合规的路径探索》,载《苏州大学学报》2022年第4期。

检察机关提前介入侦查阶段的数据合规整改活动具有合法性、可实践性。其一，根据最高人民检察院等九部委联合制定的《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）》，合规材料既可以作为检察机关审查起诉的依据，也可以作为检察机关决定是否批准逮捕的重要参考。批准逮捕是侦查阶段检察机关审查监督公安机关工作的重要方式，故检察机关可借助批准逮捕的权力提前介入侦查阶段涉案企业的数据合规整改活动。其二，检察机关提前介入侦查阶段的合规活动是有迹可循的。在Z公司非法获取计算机信息系统数据案中，公安机关提请检察机关审查批准逮捕时，检察机关不批准逮捕且综合运用引导取证、审查逮捕、强制性措施适用等法定职权，提前介入侦查，与公安机关密切配合并引导其收集合规信息与材料，推动侦查阶段数据合规整改活动的顺利开展。^[26]在类似数据安全类犯罪案件中，检察机关提前介入侦查活动，引导构建数据合规体系是可行的。其三，检察机关提前介入侦查阶段的合规整改活动以审查批准逮捕为原则，以主动介入为例外。在公安机关提请批准逮捕时，检察机关审查相关材料、确定责任人员的逮捕必要性与涉案企业整改可行性，可以此为契机介入、引导公安机关考察企业合规情况，适当延长合规考察期，确保有效整改。同时，为避免检察机关的过度介入、干扰公安机关独立行使侦查权，若公安机关未邀请且尚未提请审查批捕，则仅在涉案企业未及时开展整改活动且有提前整改必要性时，检察机关可以主动和公安机关商议提前介入侦查阶段，引导合规整改活动的开展。

侦查阶段数据合规整改的刑事激励功能仍需通过检察机关审查起诉阶段的不起诉决定体现。一方面，公安机关无权通过撤销案件，免除涉案企业的刑事责任。公安机关侦查终结的案件，公安机关或移送检察机关审查起诉，或撤销案件处理。根据《公安机关办理刑事案件程序规定》的规定，若无其他法定免责事由，公安机关仅可依据“情节显著轻微、危害不大，不认为是犯罪”撤销案件。而数据合规整改以成立“情节严重”的数据安全类犯罪为前提，即使涉案企业合规整改验收合格，公安机关亦无权通过撤销案件免除其责任，只能移送检察机关审查起诉。另一方面，检察机关可以作出不起诉决定，免除涉案企业的刑事责任。在公安机关移送审查起诉后，检察机关参照公安机关移送的材料，启动或延续侦查阶段的整改活动并明确合规考察期，组织涉案企业作出针对性整改并制定或完善有效的预防性数据保护合规计划。对考察期满并验收合格的企业，检察机关可基于认罪认罚从宽、恢复性司法理念和预防必要性的降低，拓宽适用附条件不起诉制度，作出不起诉决定，免除企业的刑事责任。^[27]

（二）审判量刑阶段的数据合规减免责

在侦查阶段和审查起诉阶段，涉案企业完成合规整改并经验收合格的，检察机关应当通过不起诉决定免除涉案企业的刑事责任。而在侦查阶段、审查起诉阶段未开展整改活动或虽启动整改活动但碍于合规考察期的有限性，审查起诉时未完成整改的企业，可以在审判量刑阶段继续开展合规整改活动，以换取减免刑事责任的激励效果，即涉案企业合规整

[26] 参见孙凤娟：《深化典型案例示范指引 推进涉案企业合规改革》，载《检察日报》2022年8月11日，第1版。

[27] 参见刘磊：《认罪认罚从宽制度的模式选择》，载《苏州大学学报（法学版）》2023年第2期。

改活动从侦查阶段到审判量刑阶段的全诉讼过程均具有启动可能性。对于审判量刑阶段涉案企业合规整改的刑事激励效果,虽有学者主张可以通过检察机关撤回起诉或法院宣判企业缓刑两种模式实现^[28],但涉案企业难以满足检察机关撤销案件所要求的“有重大立功或案件涉及国家重大利益”,且检察机关撤回起诉的模式在我国不具有普及性,故应着重构建企业缓刑模式。即不同于检察机关审查起诉阶段可以直接通过合规不起诉免除违规企业的刑事责任,法院审判量刑阶段合规整改的刑事激励效果主要围绕从轻量刑和适用企业缓刑展开制度设计,^[29]将合规整改的内容作为法院从轻量刑或适用企业缓刑的依据。

其一,涉案企业在法院审判量刑过程中开展数据合规整改的行为可以成为减免责任事由。不同于审查起诉阶段,出于对民营经济的特殊保护及基于合规整改与附条件不起诉制度的契合性,检察机关可通过拓宽适用附条件不起诉制度对整改验收合格的企业作不起诉处理,在审判量刑阶段,法院可以因整改验收合格而减免企业的刑事责任。这是因为合规整改活动的开展以认罪悔罪为前提,最高人民法院与最高人民检察院均认可审判阶段的认罪认罚同样具有从宽处理的法律效果,^[30]以合规计划为核心的整改合规有合作性、协商性和激励制约共融性特质,^[31]与认罪认罚从宽制度的协商性司法理念有共通之处,故依据认罪认罚从宽制度,在审判量刑阶段的合规整改可以成为法院对企业从宽量刑的事由。与此同时,审判量刑过程中涉案企业制定预防性的数据保护合规计划同样会降低其预防必要性、影响其预防刑,法院可基于预防刑的降低而从宽处罚、减免企业的刑事责任。

其二,可以通过增加企业缓刑,激励企业有效执行合规计划。所谓企业缓刑即在企业制定预防性合规计划后,法院确定合规考验期并对企业判处缓刑,“将积极进行合规治理规定为宣告企业缓刑的条件”^[32],法院主要考察企业在缓刑期间的补救计划是否有效,^[33]在缓刑考察期内考察合规计划的有效性与落实情况。若被认定为无效的合规计划或涉案企业未切实履行合规计划,则可能被撤销缓刑、发挥刑罚的威慑力,若在缓刑考察期内有效落实合规计划则重新获得合规经营的机会。同时,在整改合规向后延伸至法院审判量刑阶段后,不仅应构建“行检协同式”的数据保护合规体系,而且应当注重法院与行政机关的衔接,企业缓刑恰可以成为法院与行政机关协同构建数据保护合规体系的桥梁。在缓刑考验期内,行政机关可以参与企业落实合规计划的过程,提前了解刑事合规情况而确保后续行政合规的顺利开展,有助于在全诉讼阶段构建数据保护合规体系。

五、结语

数据日益成为重要犯罪对象,数据安全类犯罪逐渐转向企业行为,而罚金刑的威慑效果和预防效果较为有限,难以应对泛在的数据安全风险。笔者认为,我国可引入具有预防与惩治双重面向的数据合规激励机制,在惩治企业违规数据处理行为的同时预防数据安全

[28] 参见杨帆:《企业刑事合规的程序应对》,载《法学杂志》2022年第1期。

[29] 参见李传轩:《绿色治理视角下企业环境刑事合规制度的构建》,载《法学》2022年第3期。

[30] 参见闫召华:《附条件认罪认罚的法理检讨与实践应对》,载《政治与法律》2022年第8期。

[31] 参见周佑勇:《契约行政理念下的企业合规协议制度构建》,载《法学论坛》2021年第3期。

[32] 周振杰:《企业合规的刑法立法问题研究》,载《中国刑事法杂志》2021年第5期。

[33] 参见马明亮:《作为犯罪治理方式的企业合规》,载《政法论坛》2020年第3期。

风险。涉案企业合规整改过程中，修复数据安全类犯罪保护的合法权益并重构数据安全管理体系，替代性遭受处罚措施。多种制裁方式的灵活并用和预防性的数据合规体系是能够真正实现制裁效果和预防效果的实质制裁机制，涉案企业因而获得减免责的刑事激励并避免刑罚的“水波效应”。数据合规整改以包含认罪悔罪的整改承诺为前提，以开展针对性整改活动和规范数据处理流程为内容，以制定全方位监测措施为保障，以数据处理全流程的整改防控为核心，形成“风险预防—风险识别—违规应对”一体化的数据保护合规体系，成为减免企业刑事责任的必要前提。数据合规减免责功能贯穿刑事诉讼全流程：在侦查阶段，检察机关通过审查批准逮捕权提前介入企业的合规整改活动，通过合规不起诉免除企业的刑事责任；在审判量刑阶段，数据合规整改的内容成为法院从轻量刑或适用企业缓刑的依据。同时，应注重法院与检察机关、行政机关的衔接，协同构建数据保护合规体系。

Abstract: Data has increasingly become an important criminal object, and data security crimes have gradually turned to corporate behavior. The deterrent effect and prevention effect of fines are limited, and it is difficult to cope with ubiquitous data security risks. China has introduced a data compliance incentive mechanism with dual aspects of prevention and punishment to prevent data security risks while punishing illegal data processing behaviors of enterprises. Repairing the personal legal interests of data security crime protection and reconstructing the data security management order in the compliance rectification of the enterprises involved, the flexible combination of various sanctions and the preventive data compliance system are the substantive sanctions mechanisms that can truly achieve the sanctions effect and prevention effect, thus the criminal incentives and opportunities for the enterprises involved to reduce their responsibilities and turn over a new leaf. Data compliance rectification takes the rectification commitment including confession and repentance as the premise, carries out targeted rectification activities and standardizes data processing processes as the content, formulates all-round monitoring measures as the guarantee, and forms an integrated data protection compliance system of “risk prevention, risk identification and violation response” with the rectification and prevention of the whole process of data processing as the core. The data compliance system realizes the criminal responsibility reduction function through compliance non-system in the investigation stage and compliance probation stage in the trial sentencing stage.

[责任编辑 郭 粹]