刑事合规视域下企业数据全生命周期安全管理研究

李金珂

北京师范大学 法学院暨刑事法律科学研究院,北京 100875

摘要:企业数据安全管理是指对数据处理活动负安全主体责任的企业采取的对各类数据实行分级防护,确保数据持续处于有效保护和合法利用的状态的数据全生命周期管理活动。当前,数据已成为数字经济时代最为活跃的新型生产要素,处于全球化与数字化时代的我国企业面临数据采集风险、数据存储风险与数据利用风险等多重风险。应采取合理措施应对企业数据安全风险问题:首先,应建立企业数据全生命周期安全管理流程,完善数据采集管理、数据储存管理与数据利用管理制度;其次,应构建企业数据全生命周期安全管理刑事合规制度,包括以法秩序统一性原理指导企业数据安全刑事合规管理,以"事前预防"型合规嵌入企业数据安全刑事合规管理等。

关键词:刑事合规;数据安全风险;法秩序统一性原理;企业数据安全管理

中图分类号:F425;D925 **文献标识码**:A DOI:10.12186/2024.03.010

文章编号:2096 - 9864(2024)03 - 0088 - 07

企业数据安全管理是国家实施大数据战略,推进数据基础设施建设中的重要一环,是发展新质生产力的重要支撑[1],关乎国家安全、社会稳定与经济发展,通过企业刑事合规建设保护企业数据安全既有必要性也有紧迫性。在 2020 年国务院首次公布的关于要素市场化配置的文件《关于构建更加完善的要素市场化配置体制机制的意见》中,数据被列为继土地、劳动力、资本、技术之后的"第五大生产要素"[2]。2021 年《"十四五"大数据产业发展规划》指出,"十三五"时期,我国大数据企业规模年均复合增长率超过 30%,逾 1 万亿元,到 2025 年,大数据企业测算规模突破 3 万亿元,年均复合增长率保持在 25% 左右[3]。面对如此庞大的大数据市场,众多大数据行业企业如雨后春笋般拔地而起,疯狂进行"数据开荒"和"数据夺取"。但是任何领域的可持续发展,都离不开法律制度的规范和制约。企业在数据管理过程中稍有不慎即有可能走入刑事犯罪的歧途,一旦触及刑事犯罪,相关责任人、主要负责人甚至实际控制人都会陷入刑事犯罪风险,这对于企业来说无疑是致命性打击。而企业通过刑事合规制度建设可以完善企业内部自我管理,以事前预防规避企业刑事风险。鉴于此,本文拟通过厘清刑事合规与企业数据安全管理的基本概念、关系,分析刑事合规视域下企业数据安全管

收稿日期:2024 - 05 - 08

基金项目:北京市社会科学基金重点项目(23FXA005)

作者简介:李金珂(1999—),女,河南省信阳市人,北京师范大学博士研究生,主要研究方向:刑法学、刑事诉讼法学。

理的风险,探讨刑事合规视域下企业数据安全管理的应对策略,以期能为企业数据安全管理保驾护航,为新质生产力的高质量发展提质增效,不断形成推动经济社会发展的新动能。

一、刑事合规与企业数据安全管理之理论厘清

在数字化与智能化时代背景下,刑事合规视域下企业数据全生命周期安全管理是当今企业管理的重要方面之一。企业刑事合规涉及确保企业在其数据业务活动中遵守相关的法律法规,防止企业或其员工因违法行为而面临刑事责任。而数据全生命周期安全管理可保护企业数据资产不受威胁,确保数据的机密性、完整性与可用性。这两者虽然在实践中密切相关,但在理论基础上各有侧重。为此,有必要通过深入理解和系统分析相关基本概念,厘清二者之间的关系。

1. 刑事合规

企业刑事合规是企业合规的重要内容。企业在治理中面临的合规风险主要分为两大类:一是企业因违法违规行为而受到监管部门行政处罚的风险;二是企业因犯罪受到起诉而被定罪量刑的风险。企业刑事合规的重要目的之一是防范企业的刑事风险的发生,从而减少企业损失。但是,当前学界无论是在理论层面还是在实践层面对于企业刑事合规的界定尚未形成统一的概念。陈瑞华[4]认为,企业刑事合规是指企业为有效防范、识别、应对可能发生的刑事风险所建立的一整套公司治理体系。李本灿[5]认为,刑事合规是旨在推动企业自我管理的刑事法制度工具。孙国祥[6]认为,刑事合规是指为规避企业的刑事责任,企业内部通过实施一系列符合国家规定的措施,推动企业识别、评估和预防自身的刑事风险的一种管理活动。张远煌[7]认为,刑事合规作为企业预防、发现犯罪的内控机制,是指为消除、抑制企业内生性犯罪而采取的一系列合规计划以及相应的活动。由此可见,实践中各个学者关于刑事合规的概念尚未形成一致意见。

刑事合规是一个较为复杂的问题,既要从犯罪预防的高度来认识刑事合规,通过刑事合规为我国的犯罪预防政策找到途径、建构制度,又要把刑事合规和国家治理体系与治理能力结合起来。有鉴于此,本文认为刑事合规是指企业为预防犯罪的发生所采取的各种内控机制与管理活动。

2. 企业数据安全管理

在数字经济快速发展的时代,数据安全事关国家安全与发展。我国《数据安全法》第三条第三款规定:“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。”因此,企业数据安全管理是指对数据处理活动负安全主体责任的企业采取的对各类数据实行分级防护,确保数据持续处于有效保护和合法利用的状态的数据全生命周期管理活动。

3. 企业数据安全刑事合规管理

企业数据安全刑事合规管理是企业刑事合规管理的重要方面。当前,数据已成为数字经济时代最为活跃的新型生产要素,处于全球化与数字化时代的我国企业,不仅应注重经营风险,而且应关注由数据管理违规而产生的刑事风险,因此企业数据安全刑事合规管理势在必行。企业数据安全刑事合规作为企业避免因刑事制裁而产生负外部效应的新兴治理机制,对于防控数据合规风险具有重要价值[8]。因此,本文认为企业数据安全刑事合规管理是指负有数据安全管理义务的企业采取全方位措施维护数据安全,减少刑事风险的数据全生命周期治

理活动。

4. 企业数据安全法益保护

企业数据安全法益是指刑法所保护的为犯罪行为所侵犯的企业数据权益。在当前社会由信息时代向数字与智能化时代转型的过程中,刑法对数据权益的保障应由系统安全转向数据安全[9]。维护企业数据安全是保护企业关键信息、防止数据泄露、滥用或丢失的重要手段,因此,通过刑法保护企业数据安全既有必要性也有紧迫性。刑法应当在《网络安全法》《数据安全法》等前置法的基础上,构建刑法对企业数据安全法益的保障体系。而刑事合规与企业数据安全管理之间有着密切的联系,这两者共同构成了企业防范数据安全风险的重要基础[10]。因而此种刑法保障体系应当是建立于企业刑事合规管理条件下的数据安全保障体系,既应包含数据管理安全,也应包含数据利用安全。

二、刑事合规视域下企业数据全生命周期安全管理之风险分析

企业在数据全生命周期管理过程中面临多重风险。企业数据在其被创建至销毁的生命周期中,可能经由提取、导入、导出、迁移、验证、编辑、更新、清洗、转型、转换、整合、隔离、汇总、引用、评审、报告、分析、挖掘、备份、恢复、归档和检索,最终被删除。基于大数据环境下数据在企业业务中的流转情况,数据全生命周期可划分为六个阶段,分别为数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁。但是特定的数据所经历的生命周期由实际的业务场景决定,并非所有的数据都会完整地经历这六个阶段[11]。因此我们按照数据的全生命周期,又将企业数据分为上、中、下游三个层次,把六个生命周期的阶段归纳为数据获取、数据存储、数据利用三个环节,分别对应于企业数据安全刑事合规管理息息相关的三种风险,即数据采集风险、数据存储风险和数据利用风险。

1. 数据采集风险

企业在数据管理过程中可能因违规而面临数据采集风险。企业数据安全刑事合规管理中的数据采集风险是指企业为了自身发展通过自行收集、委托第三方收集以及通过大数据交易市场获得数据[12]时可能面临的刑事风险。无论是专门从事大数据获取业务的企业,还是企业内部数据支撑部门,获取数据的手段和所得数据的性质,均对收集数据行为的合法性认定至关重要,最为典型的例证就是侵犯公民个人信息的行为。因此,“侵犯公民个人信息罪”是数据采集环节刑事风险最高的罪名之一。《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》第四条规定,“违反国家有关规定……在履行职责、提供服务过程中收集公民个人信息的”构成侵犯公民个人信息罪,因此不仅企业有可能因违反《个人信息保护法》等规定违法收集公民个人信息而触犯刑法[13],企业员工也可能因履职过程中的违法行为牵涉到企业的利益,导致企业无法正常经营。

2. 数据存储风险

企业在数据管理过程中可能因违规而面临数据存储风险。企业数据安全刑事合规管理中的数据存储风险是指企业在非动态数据以任何数字格式进行物理存储的阶段[14]可能面临的刑事风险。例如,在生成式人工智能发展过程中,新型人工智能企业在数据存储过程中面临的数据泄露风险。以 ChatGPT 为例,OpenAI 官方在 2023 年 3 月 24 日发布声明称,有 1.2% 的 ChatGPT Plus 的用户数据存在泄露风险,其中包含姓名、聊天记录片段、电子邮箱和付款地址等信息[15]。面对未来生成式人工智能发展的不确定性问题,企业在数据管理过程中的数据

存储风险也会呈上升趋势。

3. 数据利用风险

企业在数据管理过程中可能因违规而面临数据利用风险。企业数据安全刑事合规管理中的数据利用风险是指企业在数据被经过处理、分析后投入到终端用户,服务于生产和经营过程中可能面临的刑事风险。例如,2019 年,具有六家上市公司股东的“考拉征信”被江苏省淮安市公安局立案调查,相关负责人被依法拘留配合调查。在该案中,考拉征信公司非法缓存征信系统公民个人身份信息并予以出售,已经涉嫌侵犯公民个人信息罪,同时下游公司购买、再出售的行为同样涉嫌相关犯罪[16]。

三、刑事合规视域下企业数据全生命周期安全管理之对策

企业数据安全刑事合规管理作为应对因刑事制裁而产生重大外部负面效应的新型风险防范机制,对于企业防控数据管理过程中的安全风险具有重要价值。数据企业因管理大量数据,无论是在何种数据阶段、流程,都可能面临数据安全风险,一种是外部因素,遭遇网络攻击、网络爬虫等;一种是内部因素,员工故意或者过失导致数据泄露等。数据企业应当建立有效的应对措施,防止发生刑事法律风险,保障企业数据全生命周期的管理安全。

1. 建立企业数据全生命周期安全管理流程

企业数据全生命周期安全管理是指在企业数据自创建至销毁的生命周期中,企业采取全方位措施对数据采集、传输、存储、处理、交换、销毁的全过程进行保障和优化的管理活动。企业数据全生命周期式安全管理流程主要包括以下三个方面。

其一,数据采集管理。数据采集活动是企业数据的源泉,完善的数据采集管理是企业数据安全管理的重要方面。在数据采集过程中,企业获取数据的手段及其所得数据的性质,对收集数据行为的合法性认定至关重要,因此企业在收集、使用信息过程中,应当遵循合法、正当、必要的原则,公开收集、使用信息的规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。首先,在采集数据前,企业应了解并遵循相关法律法规的规定。一方面,在开始数据采集之前,企业必须熟悉并遵守所有适用的数据保护法律,如欧盟的《通用数据保护条例》、我国的《个人信息保护法》《数据安全法》等;另一方面,在采集个人数据前,应获得数据主体权利人的明确同意,同时确保此种同意具有自愿性、明确性和可撤回性。其次,在数据采集过程中,企业应坚持透明度、目的限定和必要性原则。一方面,数据采集者应当向数据主体清晰地解释数据采集的目的、使用方式和存储期限等,并使用易于理解的语言编写隐私政策和同意书,同时,应确保数据的采集和使用仅限于事先明确的、合法的目的[17],不得滥用或用于非预期的目的。另一方面,在数据采集过程中,数据采集者应做到只采集完成预定目的所必需的最少量数据,避免“过度采集”个人数据;只有当员工或第三方因工作需要而必须接触数据时,才应该授予其访问权限,并实行严格的访问控制和监督制度;在不影响使用目的的情况下,尽可能对数据进行去标识化处理,以减少对个人隐私的影响。再次,在完成数据采集后,企业应进行内部或外部审计,检查数据采集活动是否符合法律法规与公司的政策规定。基于审计过程中发现的问题,企业应调整和改进数据采集管理策略和流程,确保其随着法律法规和技术的发展而不断更新。

其二,数据存储管理。数据存储活动的目的是保障数据的完整性与安全性,同时提高数

据的使用效率和便利性,完善的数据存储管理是企业数据安全管理的重要支撑,可为企业数据的有效利用提供安全基础。为此,企业数据存储管理部门应制定分级分类存储管理制度[18]。首先,制定数据分类政策。在企业信息管理部门、法律顾问、业务单位等相关方参与下,根据数据的敏感性、法律要求、业务价值和风险等级,制定明确的分类标准,以确保数据存储管理的安全性与适用性。其次,建立数据分类制度。依据数据重要性的不同对数据进行识别和评估,确定数据的来源、类型、存储位置、使用方式和相关的合规要求,根据制定的标准对数据应用采取适当的分类标签,包括公开级、内部级、秘密级、机密级等[19]。再次,完善数据安全存储措施。对重要程度不同的数据采取不同的管理措施,采用不同的加密与归档存储方式;对存储介质性质不同的数据采用不同的安全保障措施,保障介质安全性。同时,需要确保所有数据按分类进行定期备份,并制定有效的数据恢复计划以应对数据丢失或被破坏的状况。最后,健全数据存储审核与审计机制。针对不同级别的数据制定不同的安全审核与审计制度,定期审核数据分类和存储制度的执行情况,确保其始终符合法律法规要求与业务需求,对存储介质、存储内容的管理情况进行定期检查,并定期报告审计结果。

其三,数据利用管理。数据利用活动是发掘数据价值的重要过程,完善的数据利用管理是企业数据安全管理的重要保障。企业数据利用安全机制的建设应注意以下三个方面:一是建立安全监控和日志记录制度。应组建数据安全专业团队,保障数据不轻易被网络攻击、网络爬虫等行为获取,对网络和系统进行实时监控,及时发现并响应安全威胁。同时,应详细记录和分析安全事件的日志,以便于事后审计和追踪问题源头。二是强化员工培训,提升员工安全意识。企业应加强对内部人员接触数据的全流程追踪,防止人为违规利用数据事件发生。企业应定期开展员工数据安全和隐私保护的培训,持续提升员工对数据安全重要性的认识,确保他们能够及时识别响应数据安全的威胁。三是设立应急数据救援部门,在违规利用数据事件发生后及时发现问题并填补管理漏洞,企业应急数据救援部门通常包括数据恢复管理员、系统管理员、网络安全管理员和技术支持人员。同时应当明确团队成员的职责,确保其职责覆盖到应急响应、数据恢复、系统修复和安全分析等关键领域。

2. 构建企业数据全生命周期安全管理刑事合规制度

其一,以法秩序统一性原理指导企业数据安全刑事合规管理。法秩序统一性原理是指在处理不同法律部门之间的关系时,为确保法律秩序的内部一致性和协调性应遵循的基本规则。法秩序统一性原理是处理法域间关系的基本原则[20],将法秩序统一性原理融入企业数据安全刑事合规管理,有助于促进企业刑事合规建设,完善企业数据安全管理制度。为此,本文认为有必要从以下两个方面做起。一方面,企业数据安全刑事合规管理应重视发挥企业管理、行业自治、行政监管、司法处罚的重要作用。企业数据安全合规建设是内在管理与外在监督的双层建设,需要内在企业管理、行业自治与外在行政监管、司法处罚的有机统一,在重视企业内部数据采集、存储、利用管理建设的同时,发挥外在市场监管部门、知识产权监管部门、国家安全部门的监督管理作用,完善企业数据管理规章制度,提高企业数据管理水平与管理效率。为应对潜在的企业数据安全管理事故风险,应建立完善的企业、行业与监管部门联动机制,更

好地保护企业数据安全。一方面,企业数据安全刑事合规管理应重视处理好前置法与刑事法律的关系,以前置法为管理手段,以刑法为保障措施,协调好二者的关系,更好地完善企业数据安全刑事合规管理。从行业规定、行政法规的角度来看,立法者应强化对于企业数据安全的保护,严厉打击危害企业数据安全的行为。从刑法益保护的角度来看,刑事立法者应完善刑法对数据安全法益的保护,完成从系统安全法益到数据安全法益的转变。从刑法对数据安全保护的种类上来看,刑事立法者不仅要关注事关国家利益的数据安全,也应当关注事关企业利益的数据安全。从犯罪人的主观表现来看,刑法不仅应惩治故意危害企业数据安全的行为,也应惩治过失严重危害企业数据安全的行为。

其二,以“事前预防”型合规嵌入企业数据安全刑事合规管理。与“事后惩治”型企业合规相比较,“事前预防”型企业合规能更好地完善企业数据安全刑事合规管理,降低企业数据安全刑事风险。企业数据安全管理制度建设是“事前预防”型企业合规管理体系建设的核心,企业数据安全管理制度实施则是合规管理体系运行的核心。通过事先制定和发布完整体系的制度,可以规范企业数据安全合规管理的各项行为,保障第一时间识别企业数据安全风险,并将安全风险扼杀于萌芽之中。在作出任何重大决策之前,应提请进行合规审查,非经审查不进行决策。企业应将数据安全合规审查、合规咨询、合规风险预警等制度建设与完善“事前预防”型企业数据安全刑事合规管理机制结合起来。一是数据安全合规审查。企业应定期进行数据安全合规审查,以确保其数据管理和保护措施符合当前的法律法规要求,这包括对数据的采集、存储、传输和利用过程进行详细检查,以及评估与第三方合作时的数据保护措施。二是数据安全合规咨询。企业可以聘请外部法律顾问或设立内部合规部门,为数据安全和刑事合规提供专业的咨询服务。这些专家可以帮助企业理解和适应不断变化的法律环境,同时提供针对特定业务场景的合规建议。三是数据安全合规风险预警。企业应建立一个全面的合规风险预警系统,及时识别和响应可能导致刑事责任的数据安全风险[21]。这可能包括定期的风险评估、监控关键数据操作和设立紧急响应计划来处理潜在的安全事件。

四、结语

在刑事合规视域下,企业数据全生命周期安全管理是一项复杂而关键的任务,它不仅涉及技术层面的防护,而且包括法律和道德方面的考量。企业数据安全管理应覆盖数据的全生命周期,从数据的采集、存储到利用的每一个阶段。在每个阶段,企业都必须实施适当的安全措施,同时确保这些措施符合法律法规的要求,以预防和减少刑事法律风险。企业在制定和实施数据安全策略时,应将刑事合规纳入考虑之中,建立系统的数据风险管理机制,定期进行风险评估,以识别和评估与数据安全相关的刑事法律风险。通过对企业数据全生命周期安全管理的研究,我们可以看到,企业数据安全刑事合规不仅是法律责任的问题,也是企业保持竞争力和健康发展的关键。为此,企业应把握好发展与安全的关系,以实现企业健康可持续发展。

参考文献:

[1] 刘文祥.塑造与新质生产力相适应的新型生产关系[J].思想理论教育,2024(5):41-47.

[2] 关于构建更加完善的要素市场化配置体制机制的意见[EB/OL].(2020-04-09)[2024-

03 -01]. https://www.gov.cn/zhengce/2020 - 04/09/content_5500622.htm.

[3] 《"十四五"大数据产业发展规划》解读[EB/OL]. (2021 -12 -01)[2024 -03 -01]. https://www.gov.cn/zhengce/2021 - 12/01/content _ 5655197.htm? eqid = dcaf 72a40001cc600000000 464980bde.

[4] 陈瑞华. 企业合规的基本问题[J]. 中国法律评论,2020(1):178 -196.

[5] 李本灿. 刑事合规制度的分则体系[J]. 清华法学,2024,18(1):134 -153.

[6] 孙国祥. 刑事合规的理念、机能和中国的构建[J]. 中国刑事法杂志,2019,2(2):3 -24.

[7] 张远煌. 刑事合规视野下探索企业犯罪相对不起诉[J]. 人民检察,2020(19):39.

[8] 徐长江. 数据刑事合规的多元挑战与制度完善[J]. 数字法治评论,2022(3):102 -118.

[9] 李怀胜. 数据安全的法益变迁与刑法规制[J]. 江西社会科学,2023,43(7):33 -44.

[10] 杨猛,李嘉硕. 企业数据刑事合规的建构路径及其具体展开:以数据安全法益为切入[J]. 湘潭大学学报(哲学社会科学版),2024,48(2):88 -94.

[11] 郑斌. 企业数据安全能力框架:数据安全能力成熟度模型的构建及应用[J]. 信息安全与通信保密,2017(11):70 -78.

[12] 闫兆腾,朱红松. 智能网联汽车数据采集安全风险研究[J]. 保密科学技术,2021(10):41 -43.

[13] 卜天石. 网络爬虫技术侵犯公民个人信息的刑事规制[J]. 网络空间安全,2023,14(3):115 -120,126.

[14] 刘建忠. 数据存储、信息安全性及智能 IT 运维研究与对策[J]. 信息系统工程,2024(3):66 -69.

[15] March 20 ChatGPT outage:Here's what happened [EB/OL]. (2023 -03 -24)[2024 -03 -11]. https://openai.com/safety.

[16] 王倩. 深陷"考拉征信丑闻"拉卡拉"甩锅"何以抽身? [J]. 商学院,2019(12):73 -75.

[17] 孙红梅,贾瑞生. 大数据时代企业信息安全管理体系研究[J]. 科技管理研究,2016,36(19):210 -213.

[18] 侯利阳,贺斯迈. 如何对数据进行分级分类保护[J]. 检察风云,2020(19):14 -15.

[19] 金涛. 数据安全分级划分[J]. 信息安全研究,2021,7(10):969 -972.

[20] 喻浩东. 过失犯注意义务违反的交叉研究:兼论法秩序统一性原理[J]. 中国刑事法杂志,2023(3):50 -71.

[21] 薛兴华. 依法构建企业数据合规体系[J]. 通信企业管理,2023(11):47 -49.

[责任编辑:毛丽娜　王天笑]

引用格式:李金珂. 刑事合规视域下企业数据全生命周期安全管理研究[J]. 郑州轻工业大学学报(社会科学版),2024,25(3):88 -94.