网络民营企业数据合规的风险防范与体系建设

——以Z公司非法获取计算机信息系统数据案为视角

谢登科

（吉林大学 理论法学研究中心，吉林 长春 130012）

摘　要：数据合规作为信息网络社会中企业合规的具体类型之一，它通过促进信息网络公司依法依规处理信息数据，实现企业利益与国家安全、个人信息保护的有效平衡，有利于实现个人信息保护和数据安全领域的“国家监管”向“合规治理”模式转变。信息网络公司作为数字经济时代和网络社会的“看门人”，数据合规是其履行信息网络安全管理义务的必要途径。从数据的完整生命周期来看，数据合规风险主要包括数据收集中的合规风险、数据提供中的合规风险、数据跨境中的合规风险等不同类型。企业需要根据《数据安全法》《个人信息保护法》等法律法规来制定相应的合规政策，在数据分类分级基础上确立不同类型数据的处理流程和内部规则，建立贯穿数据收集、存储、处理、提供、销毁等完整生命周期的数据合规体系，在公司治理结构中设置以数据安全负责人/个人信息保护负责人为核心的数据合规组织机构。

关键词：数据合规；网络民营企业；数据分类分级；数据生命周期

作者简介：谢登科，吉林大学理论法学研究中心教授、博士生导师，吉林省人民检察院吉林大学企业合规研究中心研究员，主要从事刑事诉讼法学、证据法学研究。

基金项目：吉林省人民检察院2023年检察理论研究课题“涉案企业合规立法建议研究”、吉林省教育厅2023年度社会科学研究重大项目“吉林省在线诉讼规则适用实证研究”（项目编号：JJKH20231101SK）的阶段性成果。

中图分类号：D925　　**文献标识码：**A　　**文章编号：**1001-4403(2024)01-0064-12

DOI：10.19563/j.cnki.sdzs.2024.01.007

数据已经成为数字经济时代的生产要素之一，对数据的合法合规使用能够创造社会价值和经济效益，这既表现为数据处理或交易所直接产生的经济利益，也包括数据与其他生产要素相结合所产生的价值增量。[①]为了促进数字经济发展和数据安全保护，我国制定了《数据安全法》《网络安全法》《个人信息保护法》等基础性法律，对数据处理行为进行调整和规范。企业作为数据处理者，对数据的掌控能力和处理能力要远超过其他主体，[②]特别是信息网络公司、数据公司等企业，他们在数据处理中创造了社会财富和企业利润，也很容易因数据违规而面临行政处罚、刑事追诉等合规风险。最高人民检察院2022年7月

①张平文、邱泽奇：《数据要素五论：信息、权属、价值、安全、交易》，北京大学出版社2022年版，第19页。

②李怀胜：《数据安全合规实务》，中国法制出版社2023年版，第4页。

公布的涉案企业合规典型案例(第三批)中的Z公司非法获取计算机信息系统数据案,[①]就是典型的涉案企业数据合规案例。Z公司通过爬虫程序获取E公司用户店铺信息等大量数据,因涉嫌非法获取计算机信息系统数据罪,而被公安机关立案侦查。在该案审查起诉阶段,检察机关对Z公司适用涉案企业合规,Z公司制定了有效的数据合规专项计划并进行整改,从数据获取来源、数据分类分级、数据安全管理等方面完善数据管理制度,设置了数据安全官和数据合规委员会对数据合规展开常态化管理,顺利通过第三方组织考察评估,检察机关经听证后依法对Z公司及相关人员做出不起诉决定。该案对于促进互联网企业健全数据合规经营体系、助力构建健康的网络生态环境具有积极意义,也是探讨数据合规问题的经典案例。因此,本文拟以该案例为视角对信息网络公司的数据合规风险防范和体系建设进行探讨。

一、网络民营企业数据合规的特点和功能

数据合规作为网络社会中企业合规的具体类型之一,除了具有与其他类型企业合规共同的特点和功能之外,比如促进企业依法合规经营和可持续发展,有利于实现国家治理体系和治理能力的现代化,有利于保护社会公共利益,[②]还具有自身的特点和功能。

(一)网络民营企业数据合规的主要特点

首先,数据合规目的是预防数据处理中的合规风险。企业在数据合规体系建设中通常会将已制定的相关法律法规中的法定义务转化为自己内部的管理制度,在利用数据创造社会价值和经济效益时兼顾保障数据安全、数据权利,由此实现以数据合规为连接点的"企业-政府"共治模式。[③]在Z公司非法获取计算机信息系统数据案中,Z公司开展的涉案企业数据合规,既是事后数据合规,即企业在刑事违法案件发生后进行的数据合规建设,也是刑事激励型数据合规,即涉案企业通过数据合规建设来换取司法机关对其犯罪行为的宽大处理,该案是将不起诉作为对Z公司开展数据合规整改后的宽大处理结果。有学者将"数据刑事合规"称为刑事驱动型合规、回应型合规、外压型合规。[④]但是,从信息网络公司角度来看,获得不起诉、定罪免除、减轻刑罚等从宽处理的刑事激励,[⑤]仅是涉案企业开展数据合规建设的短期目标,其长远目标是预防以后数据处理业务中可能会出现的合规风险。从司法机关角度来看,开展涉案企业合规,并非简单地实现对涉案企业的从宽处理,而是为了让企业形成依法依规经营的文化,预防企业以后再次出现数据违法犯罪。如果涉案企业单纯为了追求从宽处理而开展数据合规,可能会被司法机关认定为动机不纯而拒绝对其适用数据刑事合规,刑事激励仅是促进涉案企业开展数据合规的外部手段,最终目的是通过企业数据合规体系建设来防止发生数据违法犯罪。

其次,数据合规需要以数据类型化为基准。企业合规的灵魂是针对合规风险点建立专项合规计划,而不是大而全的综合性合规计划。[⑥]专项合规计划体现了企业合规的类型化、精细化、专业化特点,该特点在数据合规领域体现得更加淋漓尽致。数据合规要求以数据分类分级为基础,针对不同数据处理行为中可能出现的合规风险点,采取不同应对措施和处理方案。有学者将数据安全合规界定为"等保合规"模式,[⑦]要求将数据安全合规建立在数据安全等级保护基础之上,这种"等保合规"就体现了数据分类分

①详见最高人民检察院涉案企业合规典型案例(第三批)之案例一。

②最高人民检察院涉案企业合规研究指导组:《涉案企业合规办案手册》,中国检察出版社2022年版,第19-22页。

③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,第98页。

④刘品新:《论数据刑事合规》,《法学家》2023年第2期,第91-92页。

⑤李本灿:《刑事合规的制度史考察:以美国法为切入点》,《上海政法学院学报(法治论丛)》2021年第6期,第41-45页。

⑥陈瑞华:《企业合规基本理论》,法律出版社2021年版,第151-152页。

⑦杨力:《论数据安全的等保合规范式转型》,《法学》2022年第6期,第20-30页。

级的基本理念。数据类型多样,法律对不同类型数据处理的要求和标准也不尽相同。对数据进行分类分级,是企业在数据收集、存储、加工、提供等处理行为中遵法守规的基本前提。在Z公司非法获取计算机信息系统数据案中,司法机关专门分析了涉案数据的属性,由爬虫程序收集的E公司订单信息等数据体量较大、类型复杂,其中既有企业信息数据,也有个人信息数据;既有内容信息数据,也有附属信息数据;既有一般个人信息数据,也有敏感个人信息数据。由于这些数据属性复杂、种类繁多,抓取这些数据需要遵循不同规则,在确定遵守或适用何种规则之前,首先需理清数据所属类型,这就必然要求数据分类分级。

再次,数据合规具有"法律-技术"双重性。数据是现代信息网络技术的产物,数据处理行为通常具有较强的科学性、技术性特征,这就要求信息网络企业的数据处理行为应符合技术标准。数据承载了国家安全、公民隐私权、财产权、个人信息权等法益,这就要求企业的数据处理行为应符合法律法规。因此,企业数据合规就呈现出"技术合规"和"法律合规"的双重属性。有学者将数据合规分为"技术意义上的数据合规"和"法律意义上的数据合规",主张早期人们主要是从数据安全角度,采取各种科学技术措施或方法来保障数据安全,此时开展的主要是技术意义上的数据合规,但现在已经将数据安全技术措施纳入法律规范的要求之中,实现了从"技术型合规"向"法律型合规"的转化。[①]也有学者主张建立数据"技术与法律一体化"治理方案,建立以"技术标准"和"法律规范"双要素的等保合规方案。[②]还有学者主张数据合规应借助于"制度力量与技术力量"的共同配合,实现法律与技术在数据治理中的有效联手。[③]上述观点虽就技术与法律在数据合规中的地位、功能等内容有争议,但都关注到数据合规的双重性,即既要重视数据处理中的技术合规,也需重视数据处理中的法律合规。在Z公司非法获取计算机信息系统数据案中,Z公司既从法律层面开展了数据合规建设,比如与E公司签订数据交互协议,保障数据来源具有合法性,也从技术层面开展了数据合规建设,比如对非法获取的涉案数据进行无害化、脱敏化处理,提升安全威胁识别和响应处置能力。"技术合规"和"法律合规"并非截然对立而是相辅相成的关系,它们共同构成数据合规的一体两翼。

(二)网络民营企业数据合规的价值功能

第一,数据合规可以通过促进信息网络公司依法依规处理信息数据,实现企业利益与国家安全、个人信息保护的有效平衡。网络公司、数据公司是通过出售、开发、利用数据来创造社会价值和经济效益的重要主体,不同类型的网络企业和数据企业利用信息数据创造价值的方式也不尽相同。有些企业是直接从数据出售或交易中来获取利益,有些企业是通过对数据分析、处理来创造价值,还有些企业是以创新性思想为基础,将数据与技术等生产要素予以结合从而通过创新商业模式来获取经济效益。[④]数据合规要求企业依法依规处理信息数据,不能为了追逐高额利润而忽视数据处理中的国家安全、信息权益保护风险。虽然从短期来看,数据合规体系建设可能会增加企业的管理、营运成本,也可能会导致企业丧失部分交易机会和经营利益,但是从长远来看,数据合规既有利于实现企业利益与国家安全、个人信息保护的有效平衡,也有助于实现信息网络公司的长期化、持续性发展。比如在Z公司非法获取计算机信息系统数据案中,Z公司在建立数据合规体系后,公司业务仍然稳步发展,分支机构逐步扩大,企业员工人数和营收数额也都有大幅增加。

第二,数据合规有利于实现个人信息保护和数据安全从"国家监管"向"合规治理"模式转变。在对企业违法犯罪治理中,传统上主要是采取国家行政监管和刑事追诉方式进行治理,具有例行性、事后化的

①刘品新:《论数据刑事合规》,《法学家》2023年第2期,第92页。

②杨力:《论数据安全的等保合规范式转型》,《法学》2022年第6期,第29页。

③姜涛、郭欣怡:《数据安全治理的刑事合规建设方案》,《江苏行政学院学报》2023年第3期,第133页。

④张平文、邱泽奇:《数据要素五论:信息、权属、价值、安全、交易》,北京大学出版社2022年版,第138-140页。

特点。监管方式的例行性就意味着可能存在监管盲区。企业经营活动通常具有持续性、常态化的特点，仅由国家采取例行性的外部监管，就会因监管盲区而无法消除企业违规风险。而监管方式的事后性，仅能在企业违法犯罪已完成的情况下发挥作用，可能无法实现对既定损害的有效修复和救济，也无法实现对企业违法犯罪的前置化、常态化预防治理。[①]对于违法犯罪，“国家监管”治理模式存在低效能问题，[②]在数据违法犯罪治理中体现得更为明显，这就需要引入“数据合规”治理模式。企业合规是通过优化治理结构、健全规章制度来防范解决合规风险的企业内部控制机制。[③]信息网络企业既是数字经济的直接参与者，也是信息技术创新的重要践行者，他们在信息数据处理和数据技术创新中，能够比较容易地发现其中蕴含的安全风险和漏洞，他们有技术和能力促进数据安全和数据权益保护。与行政监管机关、司法机关相比，信息网络公司直接从事数据处理行为，更加清楚数据处理中的合规风险和技术缺陷，其制定的内部政策和预防措施通常更具针对性，数据合规是企业规避数据合规风险、实现数据业务可持续发展的重要途径。

第三，信息网络公司作为数字经济时代的“看门人”，数据合规是其履行信息网络安全管理义务的必要途径。信息网络公司作为数字经济时代和网络社会的“看门人”，承担了对信息网络安全监管的社会责任和法律责任。企业通过建立各种专项合规计划，维持特定业务领域的企业道德，承担特定领域的社会责任。[④]数据与土地、资本、人力等传统生产资源不同，其具有多样性、共享性、系统性等特征，由此就决定了企业在数据处理业务中需要承担更多的社会责任。数据资产的虚拟性、复制性特征，决定了数据共享是同样数据被多个主体所拥有，他们可以拥有完全一样的数量容量、形式和内容，[⑤]在共享主体和次数上，可以被无限主体所拥有，即无限等量共享，这就很容易导致数据被滥用、违规使用。因此，信息网络公司在数据处理中需要承担更高的社会责任。我国《数据安全法》第 8 条在法律层面规定了数据处理者应当承担社会责任。社会责任作为数据处理者法定义务之外的“软法义务”，它要求数据处理者在履行法律规定的强制性义务、数据安全保护义务基础上，还应当基于自身业务和社会可持续发展，在数据处理中履行商业伦理、科技伦理等为社会公共利益服务的责任。[⑥]数据合规是企业在数据业务中自律治理的重要手段和方式，它可以将企业文化、商业伦理等融入企业日常数据业务和管理体系之中，让企业在处理数据中创造商业利润的同时，承担起净化网络空间、保护数据权益、维护数据安全等社会责任。比如我国网络暴力治理中，国家互联网信息办公室颁布的《网络暴力信息治理规定》，就确定了网络服务提供者对信息内容管理承担主体责任。[⑦]企业需要通过数据合规体系建设，将其法律义务和社会责任贯彻于数据业务和网络服务中。

二、网络民营企业数据合规的风险类型

企业合规在本质上是以合规风险防控为导向的企业内部管理系统。[⑧]合规风险是企业在经营过程中因存在违法违规行为而可能遭受的监管部门行政处罚和司法机关刑事追诉风险，它主要包括监管处罚风险、刑事责任风险和国际制裁风险。[⑨]数据合规主要是预防因数据违法违规处理所产生的监管处罚和刑

①程雷、曲育铮：《涉案企业合规改革现状及批判性反思》，《上海政法学院学报（法治论丛）》2023 年第 5 期，第 36 页。
②李本灿：《刑事合规的基础理论》，北京大学出版社 2022 年版，第 13-16 页。
③最高人民检察院涉案企业合规研究指导组：《涉案企业合规办案手册》，中国检察出版社 2022 年版，第 9 页。
④⑨陈瑞华：《企业合规基本理论》，法律出版社 2021 年版，第 115、22-23 页。
⑤张平文、邱泽奇：《数据要素五论：信息、权属、价值、安全、交易》，北京大学出版社 2022 年版，第 19 页。
⑥龙卫球：《中华人民共和国数据安全法释义》，中国法制出版社 2021 年版，第 25 页。
⑦谢登科：《网络暴力犯罪的公私协同治理模式》，《法律科学》2023 年第 5 期，第 99-100 页。
⑧最高人民检察院涉案企业合规研究指导组：《涉案企业合规办案手册》，中国检察出版社 2022 年版，第 19 页。

事责任风险。在探讨建立数据合规体系之前,需要明确数据合规风险的常见类型,才能够确立数据合规体系建设的重点内容。因此,下文将从数据的完整生命周期角度来分析数据处理中常见的合规风险。

(一)数据收集中的合规风险

数据收集,是从他人处获取或者取得数据的行为。对于信息网络公司而言,数据获取是其后续开发、利用、交易数据的前提和起点,他们掌握的信息数据越多,通常意味着其进行技术创新和创造财富的能力越强。按照占有主体的不同,可以将数据分为个人数据、企业数据、政务数据,此三类数据之间可能会存在交叉,比如企业数据、政务数据中可能包含着个人信息数据。在Z公司非法获取计算机信息系统数据案中,Z公司获取的主要是企业数据,但该数据中也包含了E平台店铺用户的个人信息。在获取数据时,需要区分数据的不同类型,比如公开数据与非公开数据、一般个人信息数据和敏感个人信息数据等。不同类型的数据,法律法规对其保护的方法和程度并不完全相同,对数据获取行为的规制措施也不尽相同,由此决定了其合规风险类型也不完全相同。以公开个人信息数据为例,对于依法公开的个人信息数据,任何人都可以查询、获取,信息网络公司自然也可以收集获取,且对公开个人信息数据的获取通常无需取得个人“知情-同意”,但后期应当在合理范围内对其予以处理和使用,若不在合理范围内使用,则可能会产生合规风险。[①]对于非公开个人信息的获取,通常需要取得信息权人“知情-同意”,除非存在法定例外情形;在获取个人信息数据之后,对于信息数据的使用和处理,应当限定于信息权人同意或授权的范围;若对于非公开个人信息的获取,没有取得个人“知情-同意”,或者经同意后对信息数据的处理超出了同意或授权范围,则可能会产生合规风险。由于数据具有聚合性特征,某组数据或某数据包中可能含有若干不同类型的数据,对于此类数据的收集、获取,就需要组合适用不同规则。在Z公司非法获取计算机信息系统数据案中,Z公司获取的E平台店铺用户信息数据,就可能既有公开个人信息数据,也有非公开个人信息数据。网络平台开设店铺的目的,主要是为了进行相应商品交易,此时需要公开店铺摊主的部分个人信息,以便让潜在交易方知悉、获取此部分信息。对于此部分信息的自动抓取或者获取,即使没有取得平台同意或者店铺摊主同意,通常也并不违规。但是,在平台店铺用户信息中,也有部分非公开个人信息,比如店铺的交易信息、资金流水等信息,这些信息数据不仅是非公开个人信息,而且还因涉及个人财产信息(支付记录)而属于敏感个人信息,对于此类个人信息的获取,可能不宜通过爬虫技术来自动抓取,因为敏感个人信息的收集需要取得个人“单独同意”。Z公司在利用爬虫技术来抓取E平台店铺用户信息数据时,可能仅注意到平台店铺中的公开个人信息数据,而忽视了其中蕴含的非公开个人信息数据甚至敏感信息数据,由此导致被刑事追诉的合规风险。

数据获取的方式很多,既包括对信息数据的主动收集,即基于权利人的主动提供而获得其信息数据,也包括对信息数据的被动收集,即向权利人索要或者抓取等方式而取得相关信息数据;既包括对信息数据的人工收集,也包括对信息数据的自动收集,比如通过cookie技术自动记录浏览网页的相关信息;既可以是直接收集,即直接从信息数据权主体处获得相应数据,也可以是间接收集,即从信息数据权主体之外的第三方主体处获取相关信息数据。在数据收集中,信息网络公司可能会面临以下合规风险:①数据获取行为欠缺合法性依据。数据获取行为,在本质上属于数据处理行为,其应当具有合法性依据。对于个人信息获取,通常需要基于个人“知情-同意”,除非存在法定例外情形。若欠缺合法性依据,对于信息数据的收集,则会产生合规风险。在Z公司非法获取计算机信息系统数据案中,Z公司面临刑事追诉合规风险的主要原因,就是其收集信息数据欠缺合法性依据。②超范围、过度收集个人信息数据。虽然数据是信息网络社会的生产要素,但对其获取、占有并不是越多越好。有观点甚至认为:最小化数据是降低风

①谢登科:《公开个人信息处理中的企业合规》,《甘肃社会科学》2023年第5期,第135-143页。

险的最佳方法。[①]上述观点主要是从防范数据泄露所引发的合规风险进行阐述。从个人信息保护角度来看,对信息数据的收集应当遵循“最小范围原则”,该原则意味着信息处理者在收集个人信息数据时,需要平衡数据开发利用与个人信息权益保护,在数据处理中将对个人的影响降至最小范围,将个人信息数据收集限定于实现数据处理目的的最小范围,而不得过度收集个人信息。[②]2022 年 7 月,国家网信办对滴滴处以 80 多亿元罚款,其中的重要原因就是对乘客个人的人脸信息、学历信息、评价信息等数据过度收集。[③]从实践来看,对信息数据的超范围、过度收集,是最为常见的数据合规风险点。③获取的数据本身不具有合法来源。在实践中,获取公民个人信息数据的来源和渠道较为广泛,有些信息数据甚至经过数次转手或者直接购买自网络空间。[④]若获取的信息数据来源本身不具有合法性,通常会阻碍其后续环节获取信息数据的合法性。比如在 S 科技股份公司涉嫌非法侵害公民个人信息案中,S 公司获取的个人信息数据因欠缺合法来源,而导致其面临刑事追诉的合规风险。S 公司获取的数据,最初系 L 公司基于其客户“知情-同意”而合法获取,但其代理商内部员工私自窃取上述个人信息数据予以出售,后经 J 公司交易至 S 公司。[⑤]此案中,由于 L 公司代理商内部员工获取数据方式不具有合法性,由此导致其后续环节的数据交易都受到“污染”而不合规。④不同数据获取方式中的合规风险。数据获取中的合规性,不仅取决于数据类型,也取决于数据获取方式。如前所述,数据收集可以区分为“主动收集”与“被动收集”、“人工收集”与“自动收集”、“直接收集”与“间接收集”等不同类型。这些不同类型的数据收集方式,对于数据合规的具体要求,既存在共性,比如都要求数据收集具有合法性依据,也存在差异,比如不同数据处理方式取得合法性的标准和要求也不尽相同。以个人信息数据的“直接获取”和“间接获取”为例,前者通常需要收集者取得个人信息主体的“知情-同意”,后者由于不是直接从个人信息权人处取得信息数据,而是从第三方处取得相关信息数据,此时需要由信息提供者根据《个人信息保护法》第 23 条之规定取得信息权人单独同意,而不是数据获取方来取得信息权人同意。在数据获取中,若不区分数据获取方式,并采取有针对性的合规计划和方案,也很容易产生数据合规风险。

(二)数据提供中的合规风险

数据提供,是数据权人或者数据处理者将其占有的信息数据提供给其他组织或者个人的行为。数据提供是共享信息数据的重要方式,也是数据再利用的重要前提,它有利于防止数据垄断,有利于推动信息网络技术和数据经济发展。[⑥]数据提供,既包括有偿提供,比如数据交易,也包括无偿提供,比如在特定范围内的数据公开;既包括数据主动提供,比如数据互换,也包括数据被动提供,比如数据泄露。在实践中,信息网络公司可以通过有偿数据提供行为来获得利润,也可以通过无偿数据提供来获得效益,比如利用特定数据公开吸引流量。但是,数据可能承载个人信息、国家安全、公共利益等法益,数据提供需合法合规开展,否则也会产生数据合规风险。比如在美国 ChoicePoint 公司数据泄露案中,犯罪分子通过盗窃的身份信息办理了虚假营业执照,然后向 ChoicePoint 公司提交申请,并顺利通过该公司的背景审查,获取了进入该公司数据库的权限,由此导致美国 14.5 万人个人信息数据档案被盗,该公司不仅面临市值大幅降低的经济损失,还面临大量行政监管调查和消费者集体诉讼、派生集体诉讼等共计 40.1 万件民事赔偿诉讼案件。[⑦]我国现有涉案企业数据合规案件,大多数集中于数据非法获取领域,存在对数据提供中合规风险重视不够的问题。实际上,“数据获取”和“数据提供”是紧密联系的,在同一数据交易行为或者数据

①⑦雪莉·大卫杜夫:《数据大泄露:隐私保护与数据安全依据》,马多贺、陈凯、周川译,机械工业出版社 2021 年版,第 55、82-121 页。
②龙卫球:《中华人民共和国数据安全法释义》,中国法制出版社 2021 年版,第 24-25 页。
③陆涵之:《滴滴被罚 80.26 亿元》,《第一财经日报》2022 年 7 月 22 日,第 A04 版。
④喻海松:《最高人民法院、最高人民检察院侵犯公民个人信息罪司法解释理解与适用》,中国法制出版社 2018 年版,第 5-6 页。
⑤何渊等:《大数据战争:人工智能时代不得不说的事》,北京大学出版社 2019 年版,第 5-8 页。
⑥程啸:《个人信息保护法理解与适用》,中国法制出版社 2021 年版,第 215 页。

流动中,必然存在数据获取方和数据提供方。比如在Z公司非法获取计算机信息系统数据案中,Z公司是数据获取方,而其作为数据获取对象或者来源的网站平台则是数据提供方,即E网站平台是数据提供方。当然,Z公司是采用非法技术手段即爬虫程序,利用了E网站平台漏洞,突破、绕开E网站设置的网络安全措施,获取了E网站平台存储的店铺信息等数据。在该案中,E网站平台是被动的数据提供方,Z公司采用技术手段侵入E网站平台获取信息数据,导致E网站平台中存储的用户数据泄露。E公司可能并没有因为其用户数据泄露而遭受监管调查、刑事追诉等合规风险,也没有用户因个人信息数据泄露而向其提出民事赔偿诉讼,但这并不意味着其数据存储、处理就是完全合法合规的。根据《数据安全法》第27条、第29条、第30条之要求,展开数据处理活动,应采取技术措施和其他必要措施来保障数据安全;发现数据安全缺陷、漏洞等风险时,应立即采取补救措施;发生数据安全事件时,应立即采取处置措施,按规定及时告知用户并向有关主管部门报告。Z公司能够成功利用技术手段绕开E网站的网络安全措施,本身可能就意味着E网站平台数据处理中的网络安全措施存在漏洞或问题。若确实因网络技术安全漏洞而导致其用户信息大量泄露,行政监管部门就有权依据《数据安全法》第45条之规定对其予以行政处罚。

数据提供中的合规风险,有些是基于数据处理者疏忽大意,比如前文ChoicePoint公司数据泄露案,主要原因是该公司对犯罪分子伪造的身份信息和背景信息没有尽到谨慎审核义务,从而导致其数据库中存储的海量个人信息泄露。有些是数据处理者的故意,比如为了追求非法利益而故意将相关数据信息提供给他人,此时若造成严重后果,则会涉嫌侵犯公民个人信息罪、帮助信息网络犯罪活动罪等犯罪。比如在S科技股份公司涉嫌非法侵害公民个人信息案中,S公司就将相关个人信息数据对外出售获利,经过多次交易后挂至QQ群中公开出售,从而被警方立案侦查。[①]数据提供中的合规风险,主要基于以下原因:①数据来源欠缺合法性。数据提供本质上是数据处理行为,作为其处理对象的数据应当具有合法来源,而不能是通过非法渠道或者非法方法获取的数据。若数据提供者向他人提供的信息数据不具有合法来源,比如通过盗窃、非法买卖等方式获取的信息数据,其向他人提供信息就属于非法提供个人信息数据。②数据提供行为欠缺合法性依据。数据提供行为,作为典型的数据处理行为之一,其应当具有合法性依据。以个人信息数据为例,信息网络公司将其掌握的个人信息数据提供给他人,主要是基于个人“知情-同意”或者强制许可而取得合法性依据。根据《个人信息保护法》第23条之规定,在提供个人信息数据时,应当取得个人的“单独同意”,这主要是考虑到提供个人信息对个人权益会产生重大影响,会导致处理个人信息主体的增多,提供过程中也存在各种不确定性因素,会导致个人信息泄露、增减、丢失等风险的加大,故个人信息数据提供需要取得个人“单独同意”。[②]③对数据接收方欠缺有效审查和监督,导致数据被接收方用于违法犯罪活动。数据作为网络时代的重要生产要素,既可用于创造社会财富,也可用于实施网络诈骗、网络传销、网络敲诈等违法犯罪活动。在数据提供中,信息网络公司需要审查交易相对方的身份、资质,通过合同对交易数据的目的、用途、方式等内容进行限定,并对接收方数据处理和合同履行情况进行监督。若在数据交易中,信息网络公司明知相对方或者其下游环节将相关数据用于网络违法犯罪,而仍然向相对方提供个人信息数据,则可能涉嫌帮助信息网络犯罪活动罪而产生合规风险。

(三)数据出境中的合规风险

信息技术的发展和商业模式的革新,引发数据从过去临时性、分散性跨境流动向现代常态性、大规模数据流动的巨大改变。[③]根据数据在境内外流动的方向,可以将数据跨境流动中的合规风险分为数据出

①何渊等:《大数据战争:人工智能时代不得不说的事》,北京大学出版社2019年版,第5-8页。

②程啸:《个人信息保护法理解与适用》,中国法制出版社2021年版,第220-221页。

③个人信息保护课题组:《个人信息保护国际比较研究》,中国金融出版社2017年版,第159页。

境合规风险和数据入境合规风险。我国现有关于数据跨境流动的法律法规对数据出境和数据入境均制定了相应规则,比如前者中对重要数据出境和个人信息数据出境的限制规则,后者中出于保护公共利益等社会需求而对色情、侵犯知识产权等信息数据限制入境。由于数据出境会导致数据主体对信息数据控制的弱化,在遭受侵害后因境外管辖、司法主权等问题而无法获得有效救济,现有法律法规对数据跨境流动规制的重点是数据出境。因此,本文亦主要探讨数据出境中的合规风险。

数据出境,是数据处理者将在境内收集或产生的数据提供给境外组织或个人。[①]数据出境在本质上是数据提供行为,其也可以分为不同类型,比如主动提供和被动提供。我国《数据安全法》《个人信息保护法》等法律法规对数据出境的范围、条件、流程等内容作了较为全面的规定。若违反这些法律法规,则会产生数据出境中的合规风险。具体来说,主要包括以下方面:①违反重要数据境内存储。《个人信息保护法》第 40 条要求关键信息基础设施运营者和特定个人信息处理者,在我国境内收集和产生的个人信息数据,须存储于我国境内。因为这些信息数据关涉国家安全和公共利益,若存储于境外或者未经法定程序出境,则可能会危害国家安全和公共利益。[②]对于关键信息基础设施运营者和处理个人信息达到法定数量的企业,若违反重要数据境内存储规则,则会产生数据合规风险。②欠缺合法性依据的数据跨境流动。个人信息数据承载了自然人的人格利益,企业处理个人信息数据应遵循“知情-同意”规则。个人信息数据的跨境流动,会对个人权益造成更大的消极影响,它会导致对个人信息数据的监管场域、法律适用、维权成本等方面巨大变化,自然人对其个人信息数据控制弱化、维权难度上升。《个人信息保护法》第 39 条从告知事项、同意方式等方面,对个人信息数据出境中的“知情-同意”创设了更为严格的标准。若企业在个人信息数据出境中,没有按标准取得个人“知情-同意”,则会产生欠缺合法性依据的合规风险。③未经过法定程序的跨境数据流动。企业在开展信息数据跨境流动业务时,不仅需要具有合法性依据,还应遵守法定程序。这些程序主要是依据《个人信息保护法》第 38 条之规定进行安全评估、个人信息保护认证、订立标准合同等。若在数据跨境流动中违反上述法定程序和条件,则可能会危害国家安全、[③]公共利益和个人信息保护,而产生数据跨境流动中的合规风险。

三、网络民营企业数据合规的体系建设

由于企业性质、业务类型、经营规模等差异,通常很难要求企业确立整齐划一的合规计划,这就需要企业根据自身业务、规模和合规风险等因素来制定合规计划。[④]对于信息网络公司而言,数据处理通常是其常态业务,这要求其建立专门的数据合规计划体系。数据合规计划与其他类型的合规计划相比,既存在共性,也存在自身独特之处。

首先,企业需要根据《数据安全法》《个人信息保护法》等法律法规制定相应的合规政策,为企业及其员工的数据处理业务提供行为准则。国家制定的法律法规是企业合规的基本前提和依据,企业需要将相关法律法规转化为其内部合规政策。比如在个人信息数据处理中需遵循《个人信息保护法》确立的基本原则,即合法原则、比例原则、公开原则。合法原则要求数据处理者对个人信息数据的处理应当遵守法律,这既包括数据处理行为具有合法性依据,也包括处理行为应当符合法定条件和程序。比例原则,是数据法领域衡量数据处理目的与处理方式之间利益关系合理性的基本原则,[⑤]它要求数据处理具有正当目的,数据处理手段或方式具有必要性,将对数据权利主体的利益损害或者干预降至最小。相较于合法性

①李怀胜:《数据安全合规实务》,中国法制出版社 2023 年版,第 190-191 页。
②龙卫球:《中华人民共和国个人信息保护法释义》,中国法制出版社 2021 年版,第 187 页。
③李怀胜:《数据全生命周期安全风险及其刑法回应路径》,《苏州大学学报(哲学社会科学版)》2023 年第 3 期,第 79 页。
④陈瑞华:《企业合规基本理论》,法律出版社 2021 年版,第 130 页。
⑤何渊:《数据法学》,北京大学出版社 2020 年版,第 16 页。

原则,比例原则对信息网络企业提出了更高的合规要求,但它很容易被企业忽视,因为它将数据处理中的合理性上升为法律规则。从实践来看,违反比例原则过度收集个人信息数据,是较为常见的数据合规风险点。这就需要信息网络公司在开展数据处理业务前,将比例原则转化为更具操作性、执行性的企业内部政策。比如在数据处理前,对数据处理目的的合理性、处理手段的必要性等内容进行评估,在此基础上确定数据收集或者处理的最小范围。数据处理应有明确、合理的目的,应与该目的具有直接联系,主要是为了促进或实现该目的;数据收集范围应限于对个人信息权益影响的最小数量。这些原则并不是截然分离或对立的,比如合法性原则要求个人信息处理通常需要取得个人"知情-同意",但知情范围并不限于数据处理,还包括数据处理目的。这就要求企业向个人告知数据处理的目的或用途,数据处理不得超出告知个人的目的范围。公开原则,也是个人信息数据保护的核心原则,它要求企业公开对个人信息的处理目的、规则、方式和范围。若企业以秘而不宣、暗箱操作的方式处理个人信息,既会损害个人信息主体的知情权,也会阻碍其救济权利的有效实现。基于公开原则,企业在数据处理中需要对个人履行告知义务。在发生数据泄露、丢失等事件时,也应及时告知相关主管部门和信息权人。

其次,企业需要在数据分类分级基础上确立不同类型数据的处理流程和内部规则。我国《数据安全法》等法律规定了数据分类分级制度。在数据合规中,企业需要根据自身性质和业务,对数据进行识别和分类,针对不同类型的数据采取与之相匹配的保护措施和处理流程。在Z公司非法获取计算机信息系统数据案中,Z公司制定并实施了《数据分类分级管理制度》。《数据安全法》第21条要求在国家、地区、行业层面建立数据分类分级保护制度,并将数据区分为一般数据、重要数据、核心数据三类,这主要是依据数据在经济社会中的重要程度以及数据泄露或者破坏所产生的危害程度为标准。从数据合规角度来看,企业需要将数据分类分级保护制度转化为企业内部安全管理措施和制度,通过履行不同数据处理中的相应义务来实现数据分类分级管理。[①]以重要数据为例,企业经营业务若涉及重要数据处理,除了需要遵循一般数据的处理规则之外,还需要设立数据安全负责人或机构,定期开展风险评估并报送主管部门。《个人信息保护法》将个人信息分为一般个人信息和敏感个人信息、公开个人信息和非公开个人信息,不同类型的个人信息,既遵循共通性的处理规则,也存在自身处理的独特性规则。以敏感个人信息为例,它具有很强的致损性,与个人的人格尊严、人身权、财产权等基本权利紧密联系,若泄露或非法使用,则很容易导致上述基本权利的侵害。《个人信息保护法》对敏感个人信息设置了更为严格的处理规则:在告知内容上,除了需要告知处理者名称、处理目的、处理方式等常规事项外,还需要告知敏感个人信息处理的必要性和对个人权益产生的影响等内容;在同意方式上,处理敏感个人信息,需要取得个人单独同意,有些甚至需要取得书面同意,比如《征信业管理条例》第14条第2款要求征信机构在收集个人收入等敏感个人信息时,就必须取得书面同意。企业在个人信息处理中,通过对敏感个人信息的识别和保护,可以提高对个人信息处理行为合法性的预期性,降低履行个人信息保护义务的合规成本和风险。[②]我国已经在国家、地区、行业等不同层面对数据制定了相应的分类分级标准,比如对网络数据,国家信息安全标准化技术委员会已经颁布《网络数据分类分级指引》,企业在进行数据合规建设时,就需要结合自身所在行业、地区以及企业性质、规模等因素,依据国家、地区、行业的数据分类分级要求,对其业务经营中遇到的各种数据予以归类和定级,并对各种类型、级别的数据依据法律法规制定相应的处理流程和规则。

再次,企业需建立贯穿数据收集、存储、处理、提供、销毁等完整生命周期的数据合规体系。从数据分类分级角度建立的数据合规体系,主要是以数据类型为基点的横向数据合规体系。不同类型的数据,都会面临数据收集、存储、处理、提供、销毁等各个阶段的数据生命周期,这就需要以数据完整生命周期为基

①龙卫球:《中华人民共和国数据安全法释义》,中国法制出版社2021年版,第71页。

②程啸:《个人信息保护法理解与适用》,中国法制出版社2021年版,第266页。

点建立纵向数据合规体系。需要注意的是,“横向合规”和“纵向合规”并不是两套独立的数据合规体系,在企业数据合规体系建设中,它们两者是紧密联系、彼此交融的关系,共同构成完整的数据合规体系。在数据生命周期的不同环节,对数据的处理,既要遵循共通性规则,比如需要有正当目的和合法性依据,也存在仅适用于不同环节的独特性规则。数据收集是其他处理活动的起点,传统数据收集主要采取“面对面”“一对一”等方式开展信息数据收集,此种方式比较有利于保障“知情-同意”规则得以有效实施,但存在效率较低、无法适用于海量数据获取等问题。大数据时代的数据收集或获取,主要通过 APP 注册信息弹框填写、数据自动抓取、系统自动记录等方式,[①]由此就形成了“机对人”“一对多”的信息数据收集方式,此种收集方式虽然比较高效、便捷,但存在“知情-同意”规则无法有效实施的问题,这需要在 APP、网站等通过告知弹窗、用户协议等方式,对个人信息收集的用途、类型、范围、方式等内容予以充分告知。对于非本人个人信息的获取,则需要数据提供方取得信息权人的授权。在数据存储环节,主要需考虑数据的存储地点、存储时间和存储安全。从存储地点来看,对于特定数据应当在我国境内存储。从存储期限来看,数据存储时间应遵循比例原则中的最小化要求,即对信息数据存储时间应仅限于实现该数据处理目的的最短时间。这一方面是通过尽可能减少存储时间将对个人信息权益的干预或影响降至最低,另一方面则将企业在数据存储中的泄露风险降至最低,从而将数据泄露所引发的合规风险降至最小。一般来说,数据越多、价值越高、存储时间越长,数据泄露的风险也会越大。数据存储时间,除了需要考虑数据处理目的或用途之外,还需要考虑相关法律法规对数据存储期限的特别规定,比如《网络安全法》第 21 条,就要求网络运营者对网络日志的存储时间不得少于 6 个月。在数据存储中,企业需要采取加密化、匿名化等信息技术方式来保障数据安全。数据提供是信息网络公司获得利润的重要途径之一,此种行为会让更多企业或个人参与开发、使用信息数据,从而让数据创造更多的社会价值,但也意味着数据处理主体范围的扩大,数据在提供环节及其后续处理环节存在泄露、破坏等风险,这可能会损害信息权利人的合法权益。[②]数据提供行为的合规性,不仅取决于提供人自身行为的合法性,也取决于数据接受方后续处理行为的合法性。若接收方将数据用于违法犯罪活动,则数据提供企业也会面临很高的合规风险,故需要在订立合同中对接收方数据处理的目的、方式、范围等予以限定,并对后续的数据处理活动进行持续性、动态性监督。数据跨境流动,在本质上也是一种特殊的数据提供行为,但由于其涉及国家安全、个人信息保护等因素,故《数据安全法》《个人信息保护法》对其合规性提出了更高的要求。对于跨境个人信息数据的提供,既需要取得个人同意,也需要遵循安全评估、个人信息保护认证、订立标准合同等法定程序和条件,企业可以根据自身类型、业务类型、个人信息类型等因素做出合理选择和制度设计。[③]在实践运行中,企业可以根据自身业务类型和合规风险点,对数据生命周期不同环节的合规建设有所侧重,对于高风险环节或阶段进行重点、专项治理和监控。比如在 Z 公司非法获取计算机信息系统数据案中,由于该案主要是在数据获取阶段产生的合规风险,Z 公司就重点开展了数据来源合规建设,比如采取了与 E 公司达成合规数据交互协议,对获取的涉案数据进行无害化处理等措施,从而在收集阶段实现数据来源的合法化。

最后,企业需要在公司治理结构中设置以数据安全负责人/个人信息保护负责人为核心的数据合规组织机构。企业合规管理部门是合规计划得以有效运行的组织保障,企业可以根据自身性质、规模、业务等因素,设置独立的企业合规部门,也可以由法律事务部门、风险防控部门等履行合规管理职责,并设置合规负责人。[④]在数据合规的组织结构设置中,由于数据合规具有较强的专业性,[⑤]原则上应当在企业治

①谢登科:《电子数据冻结:一种新兴的证据保全措施》,《东岳论丛》2023 年第 6 期,第 162-164 页。

②程啸:《个人信息保护法理解与适用》,中国法制出版社 2021 年版,第 220-221 页。

③谢登科:《个人信息跨境提供中的企业合规》,《法学论坛》2023 年第 1 期,第 93-94 页。

④最高人民检察院涉案企业合规研究指导组:《涉案企业合规办案手册》,中国检察出版社 2022 年版,第 23 页。

⑤陈瑞华:《企业合规不起诉改革的动向和挑战》,《上海政法学院学报(法治论丛)》2022 年第 6 期,第 32 页。

理结构中设置专门的数据合规机构或人员,将其纳入企业合规管理部门,由数据合规负责人主要处理企业数据合规的监督和管理。在企业数据合规机构中,数据安全负责人处于核心地位。在Z公司非法获取计算机信息系统数据案中,Z公司就在合规整改中设立了数据安全官,专门负责数据安全及个人信息保护工作。我国《数据安全法》中的数据安全负责人,比较类似于欧盟《通用数据条例》中数据保护官的角色和功能。数据安全负责人在企业数据合规中主要承担以下职责:①组织职责。全面统筹企业的数据安全和个人信息保护工作,对信息数据合规工作直接负责,制定数据安全和个人信息保护的决策建议和相关制度。②监督职责。监督企业及其员工按照法律法规、合规计划、政策制度开展数据处理活动。定期或不定期进行数据安全的评估检查、教育培训,对相关的数据违法违规投诉或举报线索进行调查、处理和反馈。③报告职责。发现数据安全事件或侵犯公民个人信息的事件,及时采取救济措施,及时告知用户,并向主管部门报告。④沟通职责。对企业内部存在的数据安全风险,及时采取有针对性的处理措施,及时向主管部门报告;对主管部门下达的数据安全政策和要求,及时向企业有关部门和人员传达。[①]总体来看,数据安全负责人的功能定位具有双重性,其既具有依附性,也具有独立性。从公司治理结构的内部视角来看,以数据安全负责人为核心的数据合规部门,是企业的内设机构或部门之一,数据安全负责人是企业员工,需要接受企业管理。从外部视角来看,数据安全负责人具有独立性,他在发现企业数据处理业务损害个人合法权益、危害社会秩序或国家安全时,有义务及时向行政监管机关进行报告,他是行政监管机关对数据安全监管在企业内部的必要延伸和补充,由此就决定了其在企业内部的地位具有相对独立性和中立性。正是基于此种独立性,数据安全负责人的某些履职行为,可能并不符合企业短期利益,但有利于企业持续性、合规性发展,因此,数据安全负责人不得因其正当履职行为而被数据处理企业解雇或者处罚。有学者将数据安全负责人称为数据处理者与数据监管机关之间的“纽带”,[②]此比喻形象地界定了数据安全负责人功能定位的双重性。这主要源于行政监管机关无法常驻企业内部,无法实现对企业数据业务合规性的常态化、持续化监管,而数据安全负责人通常就是企业内部员工,可以实现对企业数据业务合规性的自我监管,实现数据合规监管的常态化、持续化。有学者将数据保护官区分为“内部数据保护官”和“外部数据保护官”,前者是由数据处理企业内部员工担任,后者是由数据处理企业员工以外的其他人员担任。内部人员更加熟悉企业对数据处理的实践操作、流程和风险,也更容易了解到数据安全和个人信息保护中的问题、漏洞,但其独立性可能会存在不足。外部人员对行业标准更为精通,比内部人员可能更有经验、更加专业,但企业可能会基于商业秘密等因素而拒绝向外部人员提供相应信息数据,[③]由此就可能会导致外部人员对数据处理的主要流程、核心内容等了解不够,对企业数据处理合规性监管不足的问题。较为妥当的解决方法,是在数据合规机构中采取内部数据保护官和外部数据保护官相结合的组织或人员设置,并对他们各自的职责进行科学划分。我国《个人信息保护法》规定了个人信息保护负责人制度,其和数据安全负责人在功能上具有相似之处,都是企业在信息数据领域实现自我监管、补充行政监管职能的重要方式;只不过各自侧重点有所不同,前者侧重于对企业在个人信息数据处理中的监督和管理,后者侧重于企业数据业务中的数据安全问题。在数据合规机构设置中,企业可以根据自身规模、数据业务量等因素,[④]对个人信息保护负责人与数据安全负责人予以适当整合。若企业规模相对较小、数据业务量不大,则可以由一人兼任个人信息保护负责人与数据安全负责人;若企业规模较大、数据业务量较大,则可以在数据合规部门分设个人信息保护负责人与数据安全负责人。

[责任编辑:无 边]

①李怀胜:《数据安全合规实务》,中国法制出版社2023年版,第87-89页。

②龙卫球:《中华人民共和国数据安全法释义》,中国法制出版社2021年版,第88页。

③程啸:《个人信息保护法理解与适用》,中国法制出版社2021年版,第410页。

④邵聪:《涉案企业合规的评估标准研究》,《苏州大学学报(哲学社会科学版)》2022年第4期,第82-92页。

Risk Prevention and System Construction of Data Compliance in Cyber Private Enterprise: From the Perspective of Z Company's Illegal Acquisition of Computer Information System Data

XIE Deng-ke

(Research Centers of Theoretical Law, Jilin University, Changchun Jilin 130012, China)

Abstract: As a main type of corporate compliance in the information network society, data compliance promotes information network enterprises to abide by laws and regulations, and achieve balance between corporate interests and national security, personal information protection in the process of data. Data compliance is conducive to the transformation from government regulation to self-governance in the field of personal information protection and data security. Data compliance is a necessary way to meet the obligations of information network security management for the enterprises who are the gatekeepers of the digital economy and the network society. From the perspective of data lifecycle, compliance risks of data mainly include risks in data collection, provision, cross-border and other different process. Enterprises need to formulate data compliance in accordance with laws such as the Data Security Law and the Personal Information Protection Law. It's need to establish processing procedure and internal rules for different types of data, and make data compliance system covering data lifecycle. It's also need to set up data compliance organization around a core group of data security officer and personal information protection officer in the corporate governance structure.

Key words: data compliance; cyber private enterprises; data classification and grading; data lifecycle