DOI:10.19685/j.cnki.cn11-2922/n.2023.02.005

论我国企业数据合规体系的构建及其法律障碍

胡 玲[1],马忠法[2]

(1.安徽财经大学 法学院,安徽 蚌埠 233000;2.复旦大学 法学院,上海 200082)

摘 要:企业数据合规体系构建是数据安全治理的重要组成部分,数据合规性法律法规促使商业组织改进自身数据安全标准和实践。企业数据合规体系构建应坚持"数据安全"为首要原则,协调数据合规制度和公司管理及内控制度之间的冲突,并建立数据合规场景治理机制。我国企业数据合规体系构建中存在三个层面的法律障碍:立法层面,数据合规法律规范零散且存在相互冲突;执法层面,数据合规监督机构职责交叉、重叠;司法层面,数据合规类案件面临证据收集难、法律适用难及损失认定难。对此,也可从三个层面消除上述障碍:协调现有数据合规法律制度的冲突并出台数据合规条例;协调执法机构职责和梳理数据合规执法重点;完善证据保全制度,加强数据合规案例类型化研究以及完善损失认定。

关键词:企业数据合规;数据安全;场景治理;数据监管;数字证据

中图分类号:D 913 **文献标志码**:A **文章编号**:2096-9783(2023)02-0042-10

数据热潮正在席卷整个行业,数据生态系统的价值体现在收集和分析大量原始数据并将其转化为有用的信息。"数智化社会所展开的是一种超大规模、超复杂的经济社会关系全新形态。"[1]随着用于长期存储大量交易数据且颇具成本效益的技术和解决方案的涌现,越来越多的公司都在不断延长数据保存的时间。与此同时,监管机构和社会公众日益将目光转移到企业如何处理数据。在"后斯诺登"时代,数据隐私领域受到极大关注。用户的个人和交易数据是企业获取数据的主要来源,而绝大多数用户并不知晓企业基于各种目的保留个人数据的量。实践中,企业在实现数据保护时,通常可以从两个层面开展,即现有法律制度(成文规则)和隐私共识(隐含规则)。这意味着,一方面,现有法律制度构成企业数据合规要求的基础,如个人数据收集同意要求、目的声明等。另一方面,数据处理者和数据所有者之间往往会达成隐私共识(隐含规则)。随着我国数据强监管时代的开启,企业数据合规体系的构建面临着极大的法律挑战,无论是立法、执法还是司法层面。而研究数据合规体系中的法律障碍并提出相关移除建议对我国数字经济的健康可持续发展有着重要意义。

一、企业数据合规体系构建的理论基础

企业数据合规体系构建绝非单向度的,需在数据安全治理的视野下展开。准确识别企业数据合规的概念和特征,并梳理我国企业数据合规体系的内涵是研究相关法律问题的基础。

(一)数据合规概念和特征

1.数据合规概念

数据合规通常是指确保数据(尤其是敏感数据)免受丢失、被盗、损坏和滥用的正式标准和实践,这意味着要求相关机构和组织必须遵守关于如何收集、管理和存储数据的相关规定。各行各业的企业都应遵守数据合规标准,以确保客户个人身份信息(PII)和财务信息的安全,尤其需要防止敏感数据被窃取或滥用。当前,不同国家或地区的数据合规法律法规差异较大,但通常都会关注以下三个方面:其一,需要保护的是什么类型的数据;其二,需要实施哪些流程来保护该数据;其三,如果一个组织不遵守相关要求和程序,将面临何种处罚。实践中,企业进行数据合规可以遵循以下几个步骤:识别已有数据、尊重相关主体

基金项目:国家社科基金重大项目"构建人类命运共同体国际法治创新研究"(18ZDA153);国家社科基金重点项目"'人类命运共同体'国际法理论与实践研究"(18AFX025)

作者简介:胡 玲(1985—),女,江苏常州人,法学博士,讲师,研究方向:国际经济法,国际贸易的知识产权法;
马忠法(1966—),男,安徽滁州人,法学博士,教授,博士生导师,研究方向:国际法,国际经济法。

的权利、进行数据资产登记、绘制数据流（即如何收集、创建、存储以及分享数据）、确定处理数据流的合法依据、识别不合规的数据活动和建立高级别数据责任和报告机构[2]。

2.我国企业数据合规特征

获取、存储、使用和共享数据中每一个阶段都可能引发各种数据质量问题。高质量的数据是商业组织最宝贵的资产之一，有效利用高质量的数据对企业可持续发展至关重要，不准确或过时的数据则可能会导致错误的商业决策。我国企业数据合规将数据质量和安全作为治理的重心，这也是我国企业数据合规的重要特征。高质量的数据能直接转化为更优的商业智能，而企业确保能适用安全工具和遵循安全程序，则将减轻其相关合规责任。可以说，我国企业数据合规的目标就是确保商业组织对数据开展利用的同时，保障数据质量和安全。

（二）企业数据合规体系构建是数据安全治理的重要组成部分

对数据安全治理的理解可以分别从广义（整体）和狭义（组织内部）展开。从广义上看，数据安全治理包含国家相关机构、社会组织（行业组织、企业等），以及个人共同参与和实施数据安全治理一系列活动的有机集合体。从狭义上看，数据安全治理主要是指在一个机构或组织的内部整体数据安全战略指引下，为确保数据安全和有效利用数据，多部门联动协作完成一系列方案和活动的集合体。技术的快速迭代使得数据安全等规则面临重大挑战[3]。随着技术受到前所未有的重视，商业组织几乎每天都在产生、共享和存储大量数据，数据安全也成为全球热议话题之一。目前，行业的数据安全治理尚处于早期阶段，企业整体数据安全治理能力参差不齐。数据合规性法律法规迫使商业组织不断改进和完善其数据安全标准和实践，以防发生违规行为以及造成客户敏感数据被暴露、被盗或损坏。数据合规法律法规规定了如何收集、使用、存储和管理数据的要求，而这些数据合规性要求与数据治理和数据安全保护休戚相关。建立企业数据合规体系是数据安全治理的重要组成部分，这将为企业带来至少两方面好处，即更好地赢得客户信任和节约成本。总之，构建企业数据合规体系应在数据安全治理视野下展开。

（三）我国企业数据合规体系构建的内涵

对企业而言，不论是出于遵守法律法规还是对声誉的考量，首先应了解清楚需要保护的数据类型有哪些，以及保护的目的是什么，这是开展数据合规的前提。我国企业数据合规体系的构建离不开以下几个方面：首先，坚持“数据安全”为基本原则。对企业而言，数据安全涵盖了组织用来保护数据的工具和流程，以防止未经授权的人访问相关信息。其中，保护敏感数据是首要任务，如客户信息、财务数据或知识产权等企业核心数据的安全和隐私。其次，充分协调数据合规制度与其他公司管理和内控制度的冲突和矛盾。随着公众对数据隐私的呼声越来越高以及政府对数据隐私和安全的干预，企业纷纷开启数据合规治理，无论是出台隐私声明和政策还是其他制度，都需要检视企业现存的内部管理和控制制度，以使其形成内在有机统一体。最后，建立和落实数据合规场景治理机制。企业利用数据方式和场景多样，应根据具体业务条线的规划和开展，准确识别需要进行数据合规治理的场景，实现精准高效应对。尤其在个人数据处理上，企业应在现行法律基础上不断调整自身内部管理制度，做到合规收集和使用个人数据[4]。

（四）企业数据合规体系构建的迫切性

数字时代，数据已成为企业最关键的组成部分之一。过去这些年，大规模的数据安全漏洞不断占据头条新闻[5]。数据泄漏通常是指有意或者无意地将机密信息暴露给未经授权的各方，数据泄漏通常会对企业构成严重的声誉和财务威胁。随着数据量呈指数级增长，数据泄漏比以往任何时候都更加频繁，且会造成无可估量的后果。可以说，预防数据丢失已成为企业最紧迫的安全问题之一。引发企业数据泄漏原因多样，但通常包括以下几个方面：公司内部人员有意或无意泄漏数据；承载数据的设备被盗取或丢失，如包含敏感信息的未加密笔记本电脑或硬盘丢失或被盗；遭遇黑客攻击。总之，数据泄漏会对商业组织的声誉和财产造成毁灭性影响，不少商业组织一直是数据泄漏的受害者。而企业不断完善自身数据合规体系则在一定程度上能缓解因数据泄露带来的损害。

综上，随着数据在企业实践中的用途边界不断拓展，如何识别各种利用场景的数据合规风险成为企业

数据合规治理的重点及难点。企业要保障业务的连续性应建立整体数据安全防护,尤其应采取“真正动态和无缝的举措”来为商业开展提供安全保障[6]。厘清数据合规相关概念、特征和企业数据合规体系的内涵,并梳理企业数据合规的迫切性对其相关法律障碍分析及移除建议的提出有着重要理论意义。

二、我国企业数据合规体系构建的行业实践和域外借鉴

(一)企业数据合规体系构建的行业实践

1.企业数据合规适用场景

数据正通过各种方式影响着商业组织的业务开展,诸如改善决策制定、改进业务流程和实施、创造收入来源和模式等。在数据为商业组织带来价值的同时,数据隐私和安全问题也日益凸显。可以说,数据在什么场景下为企业带来效益,这样的商业场景就离不开数据的合规治理。商业实践中,我国企业对数据的处理主要涉及数据的收集、分析、存储和跨境流动。首先,收集数据可以使得企业存储和分析现有和潜在客户的重要信息,并为未来的营销建立更好的客户数据库,从而为企业节约成本。企业收集和拥有的数据越多,作出正确决策和创新商业模式的可能性就越大,质量高的数据甚至将成为企业决策时的直接依据。其次,光有数据是不够的,对企业来说,如何利用已搜集的数据作出正确且富有远见的商业决策才是核心。再次,随着企业数据量呈指数级增长,数据存储成为企业利用数据以成就业绩的重要组成部分,有效管理数据是确保组织高效使用存储资源并依照法律法规和公司政策安全存储数据的关键。最后,随着企业将业务触角伸向全球,企业数据跨境流动能让用户实时传输信息并进行在线互动、更好地追踪全球供应链、共享研究成果并进行技术创新,等等。数据跨境流动已成为国际数字贸易的核心议题,更高水平和更严标准是其发展的必然趋势[7]。在我国现有的数据相关法律法规下,企业收集、分析、存储和开展数据跨境业务需要遵循《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》)、《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》)等相关法律的规定,构建和完善自身数据合规体系是企业持续健康开展数字业务的重要保障。

2.企业数据合规制度

早期的企业合规治理主要是企业自我管理和自我监督的治理方式[8]。随着数据保护相关法律的完善,企业为了应对数据合规要求,纷纷颁布或更新隐私政策和内部合规指引。概括来看,这样的隐私政策或内部指引的内容通常会包括以下几个方面:第一,收集限制,一般会规定仅收集特定目的所需的最少数据量,同时仅保留所需的最少时间。但是随着“匿名化”神话被打破,大量用户数据被推断出来,简单删除客户数据的主要索引远远不够。第二,目的规范,要求明确和专门说明收集数据的目的。但是实践中,往往数据收集的原始用途过于局限,无法涵盖大数据提供的创新用途。商业组织出于商业利益的考量,往往会突破原始收集目的,实践中确实也产生了诸多创新用途。第三,使用限制,这主要是规制数据使用方未经数据所有人同意与第三方共享或以其他方式改变数据用途。第四,安全保障,处理个人数据的组织需要提供必要的保障和机制,以确保个人信息不会落入危险境地。随着商业组织将更多数据放入低成本存储(如云存储)解决方案中,审查这些外部存储系统的数据访问控制则变得至关重要。第五,个人主体参与,强调个人在管理自身数据中的作用和地位,比如用户个人有权删除、更正其数据,但是实践中,存在很多难以擦除或纠正的数据。第六,问责制,要求进行数据收集和存储的组织对自身数据使用行为负责。不容忽视的是,不论数据保护立法多完善,最终都需要落实到企业的数据合规实践中,而隐私政策则是重中之重[9]。

3.企业数据合规实践

随着数据法律法规的出台,各行各业都应根据《数据安全法》《个人信息保护法》《网络安全审查办法》等法律法规和标准加强自身数据安全和隐私保护能力建设。事实上,在数据收集、融合、再利用、流转、推送等各个环节都存在合规问题。数据合规凸显着时代意义。首先,应重点梳理和识别自身数据资产中是否存在重要数据,其一旦泄露可能直接影响国家安全、经济安全、社会稳定以及公共健康和安全,应时刻关注所在地区主管部门对重要数据目录的编制进展。其次,一旦涉及数据跨境则需及时检视是否需要本地存储数据以及进行数据跨境评估,以确保数据出境安全。再次,一些企业的网络平台和信息系统如果一旦

被识别为关键信息基础设施，则需要落实更严格的数据合规义务。最后，企业在采购相关网络产品和服务时还应严格落实数据安全审查制度。总之，各行各业的企业都应围绕自身的义务特点来构建数据合规体系。

（二）企业数据合规体系构建的域外法律借鉴

纵观全球，数据安全威胁的数量和复杂程度与日俱增，监管也日趋严格。企业保持对国家标准以及越来越多全球标准的遵守需要花费大量的时间和资源。

1.国际法层面

技术在不断更新迭代，全球范围内的数据隐私法也正在不断涌现以适应这一现状。目前，数据隐私法的一个共同特点是将个人隐私置于中心位置，尝试构建更符合道德的数据处理流程。联合国、世界贸易组织（WTO）、经合组织（OECD）、全面与进步跨太平洋伙伴关系协定（CPTPP）等都积极回应了全球数字经济迅猛发展下的个人数据/隐私问题。如今，已有100多个国家/地区参与了某种形式的数据保护国际隐私法，以确保为公民信息提供更为严格的保护和控制。整体而言，数据保护的国际隐私法通常遵循以下几项隐私原则：通知、选择和同意、访问和参与、完整性和安全性、执行和实施。可以看出，国际数据保护规则侧重于保护个人数据/信息免受内外部威胁，通过降低欺诈、妥协和腐败等风险来保护个人数据。面对全球范围内兴起的个人数据保护，企业的担忧随之而来，在大数据时代，数据往往是在商业使用中才发现新的用途，难以一一提前规划好用途和目的后，告知用户并获得授权。为应对全球多样化、碎片化的法律法规，各国应更加紧密地相互协调，从而为国家、公民和组织提供更坚实的监管基础。

2.美国和欧盟

（1）美国。在数据合规层面影响力比较大的有加州消费者隐私法（CCPA）和加州隐私权法案（CPRA）。加州消费者隐私法（CCPA）要求告知数据主体何时以及如何使用他们的个人数据，且消费者有权在其个人信息应修改时与企业沟通更正或删除[①]。加州隐私权法案（CPRA）或称CCPA-plus于2023年1月生效，其目的是对延展CCPA中对消费者个人数据的保护，其赋予消费者要求组织更正档案中虚假信息的权利，它还将建立加州隐私保护署（CPPA），并重新定义“违规”等关键词[②]。

（2）欧盟。《通用数据保护条例》（GDPR）的出台旨在改变各行业对个人数据的处理方式，让消费者重掌数据收集和使用的最终话语权。GDPR对企业的合规要求主要体现在以下几个方面：只要向欧盟数据主体提供商品或服务，或监控欧盟数据主体的行为，都将受到GDPR的规制；要求适用于几乎所有类型的个人数据，比如IP地址、电子邮件地址和物理设备信息等；GDPR要求尊重用户在个人数据和数据隐私方面拥有的八项基本权利，即访问权、知情权、迁移权、被遗忘权、反对权、限制处理权、被告知权以及修改权；不遵守GDPR将面临重罚；企业需要聘请数据保护官（DPO）来管理GDPR的要求，一般需要负责监督公司的数据保护策略、监控数据存储和数据传输、对员工进行合规性教育和培训等。DPO是组织内的重要职位，可确保组织实现更高的数据保护合规性[10]。

在数据合规法律体系方面，欧盟对数据隐私采取自上而下的方法，对个人数据进行了几乎全方位和全流程的保护，而美国则更多采用自下而上的方法。要想解决行业、国家和全球数据合规问题，应树立总体合规战略，其中涉及法律、人力资源、IT等之间的协调，同时还需要自上而下实施持续的安全和隐私策略。国际法层面和欧盟及美国的数据合规相关立法给我国完善数据合规法律法规以及构建企业数据合规体系提供了很好的域外借鉴视角和经验。

三、我国企业数据合规体系构建的法律障碍

数据相关法律法规是企业数据合规体系建立的法律基础和实施指引。实践中，企业通过数据分享、交换和共享等途径不断创新和挖掘数据的价值，直接或间接为企业创造经济效益。对企业而言，对自身数据合规体系建设的投入需要平衡数据资源开发和合规经营之间的关系。随着网络安全和数据法律法规体系的完善和执法力度的上升，相关司法判例和行政

① California Consumer Protection Act.

② California Privacy Rights and Enforcement Act.

处罚案例开始涌现,数据合规得到越来越多企业的重视。我国企业数据合规体系构建中存在三个层面的法律障碍:立法层面,数据合规法律规范零散且存在相互冲突;执法层面,数据合规监督机构职责交叉、重叠;司法层面,数据合规类案件面临证据收集难、法律适用难及损失认定难。

(一)企业数据合规体系构建的相关法律规定及其不足

我国直接规制数据安全和隐私的两部基础法律已于2021年生效,这对中国企业以及业务涉及中国的跨国公司产生重大影响。《数据安全法》和《个人信息保护法》对此前《网络安全法》中的数据本地化、数据跨境和数据保护等提出了具体要求。就企业数据合规的实施指导而言,当前的法律法规尚存在以下几个方面的不足。

1.数据合规相关法律制度分散

(1)《数据安全法》。整体上,该法为我国数据利用和数据安全搭建了基本的法律框架。规定了数据安全基本制度,明确了促进和支持数据安全与发展的各项措施,并规定了相关主体的数据安全保护义务。该法根据数据对我国国家安全的潜在影响对在国内收集和存储的数据进行分类,并根据数据的分类级别对其存储和传输进行规范。该法也是市场主体(主要为企业)落实合规义务的基本指引。其要求在我国开展业务的公司建立和完善其数据安全体系,在发现数据安全缺陷时及时采取补救措施,并及时通知用户和监管机构。处理"重要数据"的数据公司需指定负责数据安全的人员或团队,并定期向有关监管机构提交风险评估。此外,对相关违法行为,也规定了罚款等处罚措施。

(2)《个人信息保护法》。《个人信息保护法》是我国第一部规范个人信息保护的综合性法律,以欧盟GDPR为蓝本。"个人信息"被定义为涵盖"以电子或任何其他格式存储的与已识别或可识别自然人相关的任何信息",只要该信息"与已识别或可识别的自然人有关",不包括不可逆转的匿名个人信息。具体要求以下几个方面:第一,同意要求。原则上,在收集或处理某人的个人信息之前,数据处理者必须获得数据主体的自愿、明确和知情同意。此外,收集或处理"敏感个人信息"(包括数据主体的生物特征、宗教信仰、健康、财务、地理位置和未成年人信息)必须告知数据收集的特定目的和必要性,并遵循《个人信息保护法》中的要求落实数据保护措施。第二,数据本地化和数据删除要求。如果数据处理者正在处理的个人信息量达到一定阈值,则可能触发数据本地化要求,并且数据处理者还应任命一名信息保护官来监督妥善处理和保护。而当收集目的已完成、保留期限届满、用户撤回同意时,数据处理者应履行删除义务。第三,向第三方和海外传输个人信息的限制。数据处理者在将个人信息传输给境内外第三方之前,必须先征得数据主体的知情同意,并确保数据接收者对数据的使用和数据处理方式在数据主体同意范围内。对于跨境传输,数据处理者必须确保数据的外国接收者具有不低于《个人信息保护法》规定的数据保护要求。使用算法和类似的自动决策功能来分析数据主体个人信息的公司必须遵守《个人信息保护法》中规定的"透明度"和"公平"原则,禁止基于数据主体的个人特征进行歧视性定价和营销活动。整体上,对企业而言,《个人信息保护法》要求处理个人数据的公司定期进行自我审核,以评估其信息安全风险并实施相应的政策和保障措施。

(3)其他法律规定。除了《数据安全法》和《个人信息保护法》外,在涉及个人数据合规层面,《中华人民共和国民法典》(以下简称《民法典》)也有着重要意义。实践中,还有很多实施指南,对企业数据合规体系构建提供了重要指引。这些指南包括公安部2019年发布的《互联网个人信息安全保护指南》、信标委2020年7月发布的《网络安全标准实践指南——移动互联网应用程序(APP)收集使用个人信息自评估指南》和9月发布的《网络安全标准实践指南——移动互联网应用程序(APP)个人信息保护常见文集及处置指南》,这些都是经常被实务中提及和参考的一些文件。

整体而言,我国企业数据合规涉及的法律众多,规则分散。其中,《数据安全法》和《个人信息保护法》是我国企业构建数据合规体系最主要的法律依据。但是,企业在落实数据合规常常会面临困境,需要根据不同的法律规定和要求实施合规政策,这无疑增添了企业的数据合规不确定性和负担,在一定程度上也不利于企业对数据的创造性利用,也难以真正实现监管机构的数据合规监管目标,最终难以实现保护个人

数据隐私和数据安全的目的。

2.相关法律制度用词模糊

《数据安全法》和《个人数据保护法》对企业落实数据合规规定了诸多细致要求，但是很多法律用词模糊。如随着对数据的监管深入，需要关注公司是否符合“主要互联网服务平台”的资格、是否拥有“大量”用户以及从事“复杂的商业活动”而适用越来越严格的规则，但是很多术语目前在《个人信息保护法》中尚未有明确定义。

3.尚未出台专门的数据合规法律或法规

中国数据治理是全球数据治理的重要组成部分，数据（尤其是个人数据）创造价值的同时也对个体、群体和国家带来了重要威胁，如数据泄漏等。随着企业数据合规进入强监管阶段，私营部门是数字经济的主要创新主体，为实现数字经济的健康持续发展，应夯实数据合规的法律基础，国家层面应出台数据合规行政法规，为企业构建数据合规体系提供明确落地指引。

（二）企业数据合规体系构建中监管困境

近年来，从中央到地方都从不同视角展开对网络安全、数据以及个人信息保护方面的执法活动，积极查处并要求相关机构和企业进行合规整改，以完善网络安全与数据合规体系。当前，涉及数据合规的执法机构职权交叉、边界不清，对网络安全、数据安全和个人信息保护形成了多头监管的局面。目前监管机构主要有公安部门、网信部门、电信部门、工商部门和行业监管部门。整体而言，涉及数据的监管职责纵横交错，企业进行数据合规需要应对不同的监管机构，一方面会不利于企业构建科学高效的数据合规体系，另一方面也会给企业利用数据创新业务模式造成障碍。

（三）企业数据合规体系构建中司法难题

企业数据合规体系的构建离不开司法保护。一旦发生数据合规事件，如何取证和认证成了棘手的问题。个人数据是企业构建合规体系重要的保护对象，也是行政执法的重点，但是在具体法律适用和损失认定上也面临着不小挑战。

1.数字证据带来的问题

数字证据可以被看成以二进制形式存储或传输的信息，可以在法庭上使用，通常被存储在计算机、手机和移动硬盘中。“电子数据鉴真已成为网络信息时代重要的证据问题。”[11]一旦发生企业数据违法违规事件，相关人员在处理数字证据时面临着不小挑战。首先，数据泄漏、篡改和网络攻击的风险。其次，数字设备往往没有足够的存储空间来保存各种数字证据。再次，提取或保存数字证据时，都不能排除人为因素，难免会产生各种错误。此外，证据在传输过程中面临的风险最大，也最容易遭到破坏、暴露或篡改。最后，数字证据容易因处理不当而在法庭上不被采信。总之，数字证据越来越成为各类案件的核心部分，相关人员和机构应采取适当的措施和解决方案来应对上述问题。

2.法律适用难和损失认定难

就个人信息保护而言，目前的法律主要有《民法典》和《个人信息保护法》。在具体案件中，存在法律适用难的问题。在《民法典》下，对个人信息的保护主要体现在人格权层面。《个人信息保护法》则是系统规制个人信息安全和利用的法律，尤其通过确立个人信息处理的一系列规则来维护个人信息权利。在个人信息受到侵害时，如何识别《民法典》和《个人信息保护法》所保护的法益存在难点，在一定程度上给法律适用带来不确定性和复杂性。此外，司法实务中，如何对侵害个人信息的损害事实进行认定是个棘手的问题。

从立法、执法和司法三个层面梳理和识别我国企业数据合规体系面临的法律障碍，能从整体上看待我国企业数据合规体系构建中的法律难题，并提出有效对策，也才能真正将企业数据合规体系构建纳入到我国数据安全治理中来。

四、我国企业数据合规体系构建中的法律障碍的消除

当前，我国企业数据合规体系构建分别面临着立法、执法和司法三个层面的法律障碍。对此，也可从三个层面消除上述障碍：协调现有数据合规法律制度的冲突并出台数据合规条例；协调执法机构职责和梳理数据合规执法重点；完善证据保全制度，加强数据合规案例类型化研究以及完善损失认定办法。

（一）企业数据合规体系构建中的立法完善

各地已纷纷开展数据合规实践，并出台了相关合

规指引,急需对数据合规相关法律制度进行梳理,为我国企业数据合规体系构建保驾护航。目前,与数据合规相关的法律主要有《数据安全法》《个人信息保护法》《民法典》,这些法律都有各自侧重保护的法益,加以梳理和明确能使适用时更清晰、更明确。此外,随着我国数字经济的蓬勃发展,数据安全不仅关系个人隐私安全,更关系到国家信息安全,而数据的创新使用和合规实践主要发生在企业,出台相关数据合规条例能在全国范围内协调各地企业数据合规治理的标准,为我国数字经济健康持续开展提供坚实的制度指引。

1.协调现有数据合规法律制度立法冲突

当前,数据合规相关立法和标准稳步出台,但在具体适用时难免存在冲突。其中,《数据安全法》应成为我国企业数据合规立法层面的顶层指引,尤其在涉及数据安全和重要数据等相关规制时,需在该法的规制下开展。企业在数据合规治理时应采取数据加密、访问控制等措施,建立健全全流程数据安全管理制度。在个人信息保护层面,应明确《民法典》和《个人信息保护法》的适用规则。其中,《民法典》侧重保护人格权益,《个人信息保护法》对个人信息的保护则更为全面和细致。在涉及个人信息私法规制层面,首先,应坚持《民法典》对个人信息保护的原则性规定,强调保护人的尊严。其次,在尊重和保护个人信息人格尊严的基础上,充分依据《个人信息保护法》的要求开展个人信息处理活动。此外,还应重视敏感信息和特殊主体的保护,一般而言,企业只有在具有特定目的以及具备充分必要的前提下,并依据法律规定履行相关手续,采取严格保护措施后,方能处理此类信息。这样明确了《民法典》和《个人信息保护法》各自保护和规制的侧重点,未来在法律适用上就不会发生困惑甚至混乱。

2.出台数据合规实施条例

目前,国家对企业数据合规的要求主要散见于《网络安全法》《数据安全法》《个人信息保护法》等法律法规和标准中,尚未出台专门的国家层面立法文件,这无法适应当前企业的数据合规实践,无法对企业数据合规体系的建立提供明确价值指引和要求,也会导致各地企业数据合规治理标准和水平不一,从而可能引发潜在的系统性数据安全问题。此外,数据泄露和个人隐私侵权案件的不断增多,执法和司法都面临不小的挑战。随着数据合规实践的不断丰富和变化,直接出台单行法律存在不小难度,但是国家层面出台数据合规实施条例有其必要性。该条例可以对目前法律规定模糊之处以及疏漏之处进行完善,尤其需要明确大中型企业进行数据合规治理时需重点关注重要数据的识别、数据跨境传输、内部合规体系构建,以及数据合规治理的相关组织架构等问题。此外,还应对各地出台的数据合规相关条例和指引进行整理协调,将各地企业尤其是中大型企业数据合规治理要求和水平尽快调整到同一水平线。总之,该条例应将协同治理、企业数据合规业务场景、技术标准以及全过程监督等合规要求纳入其中。

(二)企业数据合规体系构建中的执法完善

当前,我国数据合规面临多头监管的困境,协调数据合规执法机构职责冲突成为当务之急。否则,不仅企业应对数据合规监管的义务和成本在不断增加,也会不利于企业合规体系的构建和合规义务的落地。对此,执法部门应梳理企业数据合规的监管重点和企业清单,根据立法对执法部门的授权厘清各自涉及数据合规的监管重点,避免职权交叉。个人信息保护依然是当前数据合规执法的重心和核心。在数据合规监管职责划分上,应不断明确和强调各监管机构的主要监管目标和任务,在发生职权竞合时方能理性回归行政执法权的初衷。其中,网信办负责统筹和协调,实施检查调查以及约谈处罚等监管措施下,国务院部委工业和信息化部主要负责工业、电信领域的网络信息安全;国务院直属机构市场监督管理局则具体负责与消费者有关的个人信息安全;公安机关则主要负责数据合规涉及的刑事侦查;其他行业监管部门,如中国人民银行、中国银保监会等依据行业特性确定细则。总之,我国虽无需像欧盟GDPR那样建立统一的执法体系,但也要在实践中不断厘清相关执法机构的执法边界。

(三)企业数据合规体系构建中的司法完善

在数据和算法的双轮驱动下,企业不断创新发展其自身数据业务,以求新的盈利增长点。与此同时,数据侵权甚至网络犯罪也日渐增加。司法实务中,数据相关案件不断呈现,出现了包括数据权益的权属判

断、数据产品的法律属性及其保护、数据爬虫行为的认定、平台算法自动化决策和算法歧视等新型案件类型，给司法审判带来新的挑战。这需要从完善数字证据收集和保全制度、加强案例类型化研究和完善对损失的认定这两个层面展开。

1.完善数字证据收集和保全制度

数字证据正日益成为各种案件调查的重要部分，收集和保存数字证据带来诸多挑战，应积极应对。首先，数据和计算机系统相互依存，在网络环境下，一旦缺乏相应安全措施，数据极易被篡改或删除。应选择高安全性能的证据篡改检测系统，确保数字证据处于其原始状态，并以加密格式存储在具有内置安全协议的硬件设备中。其次，数据是信息的载体，信息是数据的内容呈现，存储在计算机系统中的数据往往来源多元且格式多样。因此，需采用一套完整的数字证据管理系统，该系统能自动提取各种来源的证据，支持多种格式，集合存储、保护和分析功能。再次，还应加强相关人员的技术和培训，否则任何人为的轻微错误都可能导致证据在法庭上难以被采信。此外，在管理数字证据时，还应遵循数据传输安全的相关认证和解决方案。最后，证据提交时应关注法院的技术设置和互联网连接，这样才能安全传输和呈现证据。如果相关证据无法直接显示，可以提前下载并出示。无论采取何种展示方式，必须确保在法庭上出示的证据是以原始形式保存的且未经任何形式的更改，这样才能确保证据的真实性。

2.加强案例类型化研究和完善对损失的认定

加强数据合规相关案例类型化研究不仅能更规范、精确解释相应法律规范，也能弥补法律漏洞，其在裁判依据模糊的案件中更是发挥着重要作用。目前，数据合规民事和刑事案件不断增多，法律规范在司法实践中的指导性还需完善，对数据合规案件进行类型化研究就显得尤为重要，从中发现案件事实的规律并抽象出背后的法理，这对于司法裁判无疑有着直接指导意义。数据相关案例是数字经济发展下的新兴产物，数据的无形性、易复制性、无边界性，以及其关涉个人隐私安全和国家数据安全，加上当前各类企业数据合规治理水平不一，加强对同类案件的研究和分析，能对相关审判实务和企业数据合规治理起到明确的指引作用。此外，在我国民事法律体系下，损害是认定侵权和确定损害赔偿责任的重要条件，这在《民法典》第一千一百六十五条和第一千一百六十六条都可以见到相关表述③。数字经济时代，数据（尤其是个人数据）蕴含着重要商业价值，但由于数据本身具有易复制性和无形性，其与传统的民事客体所遭受的侵害不一样，除了会造成他人财产损害或者精神损害之外，还会给权利人带来潜在危险和威胁。为应对数字时代瞬息万变的挑战，应适当延展数据引发的损害认定范围。

总之，数据相关法律法规是我国企业构建数据合规体系的重要依据，梳理相关法律规定，准确识别其中的法律障碍，并提出有效对策，是我国企业将数据合规落地的重要法律基础，对我国数据安全治理有着重要意义。我国企业数据合规治理的核心就是确保商业组织对数据进行创新使用的同时保障数据质量和安全。

五、结语

随着全球数字经济不断向纵深发展，数据为商业组织提供了诸多用途，不断创新着企业的商业模式。追求利润和利润的不断增长往往是商业组织的主要目标甚至最终目的。但是，数据并非专属推动私营部门创新和增加收入的资源，能否有效治理数据直接关系个人隐私安全和国家信息安全。数据安全也是我们利用技术而产生的最重要问题之一[12]。数字经济时代企业在进行知识产权治理时也重视协调数字经济发展、社会公众隐私与数据使用商业利益之间关系[13]。在企业数据合规治理中应重视在个人信息保护、数据安全和商业效益等之间达成动态平衡。在处理各种数据隐私和保护框架所涵盖的数据时，企业必须确保遵守相关法律和监管要求。企业想要获得数据资产的持续变现必须在合规前提下开展。当前，良好的网络安全和数据合规能力已成为不少大型企业评定合作商的重要指标，也成为企业向社会和其客户展示实力的一大体现。其实，在大数据时代之前，数据保护和隐私问题就已经存在了，涉及数据处理的组织必须遵循相关规则。对于一家明智的企业，在确保

③《民法典》第一千一百六十五条和一千一百六十六条将“造成他人民事权益损害”作为侵权责任归责体系的构成要件。

数据合规时应做到以下几个方面:将合规落实到日常行为中;协同和整合数据保护模型和其他内部控制模型;为相关人员提供合规培训;为合规管理者提供准确的报告和信息[14]。企业的这些合规措施都离不开法律文件的指引。只有梳理我国数据合规体系面临的法律障碍并提出相关对策,才能为我国企业构建良好的数据合规体系提供坚实的法律基础,也才能为企业增强市场竞争力,并吸引更多的合作伙伴和客户。

参考文献:

[1] 齐延平. 数智化社会的法律调控[J]. 中国法学, 2022(1): 78.
[2] WITHERS P. Data compliance: achieving it all[J]. International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, 2019, 3(7): 19.
[3] MCGEVERAN W. The duty of data security[J]. Minnesota Law Review, 2019, 103(3): 1198.
[4] 张晶. 我国数据主权研究的系统性文献综述[J]. 情报杂志, 2022(4): 133.
[5] MORINGIELLO M J. Warranting data security[J]. Brooklyn Journal of Corporate, Financial & Commercial Law, 2010, 5(1): 63.
[6] 韩轶. 网络数据安全领域的企业刑事合规体系建构[J]. 江西社会科学, 2022(5): 141.
[7] 何波. 中国参与数据跨境流动国际规则的挑战与因应[J]. 行政法学研究, 2022(4): 99.
[8] 王诚, 魏雅雪. 企业合规治理: 平台经济反垄断行政执法新视角[J]. 东岳论丛, 2022(4): 184.
[9] 李延舜. 隐私政策在企业数据合规实践中的功能定位[J]. 江汉论坛, 2020(10): 136.
[10] GOSHADZE K. The Data Protection Officer (DPO) –ensuring greater data protection compliance[J]. Law and World, 2020, 14: 46.
[11] 谢登科. 电子数据的技术性鉴真[J]. 法学研究, 2022(2): 209.
[12] ALLEN J. Data security in mobile world[J]. GPSolo, 2010, 27(8): 4.
[13] 郑鲁英. 数据经济知识产权治理: 现状、困境及治理[J]. 贵州师范大学学报(社会科学版), 2022(6): 154.
[14] IMPERIALI R. The data protection compliance program [J]. Journal of International Commercial Law and Technology, 2012, 7(3): 288.

On the Construction and Legal Obstacles of China´s Enterprise Data Compliance System

Hu Ling, Ma Zhongfa

（**School of Law, Anhui University of Finance and Economics, Bengbu, Anhui 233000, China; Law School, Fudan University, Yangpu, Shanghai 200433, China**）

Abstract: The construction of enterprise data compliance system is an important part of data security governance. Data compliance laws and regulations prompt commercial organizations to improve their data security standards and practices. The construction of an enterprise data compliance system should adhere to the primary principle of "data security", coordinate the conflict between the data compliance system and the company′s management and internal control system, and establish a data compliance scenario governance mechanism. The legal obstacles in the construction of China′s enterprise data compliance system are put forward from three levels: Firstly, at the legislative level, the data compliance legal system is fragmented and conflicted. Secondly, at the law enforcement level, data compliance supervision agencies have overlapping responsibilities. Finally, at the judicial level, data compliance cases face difficulties in collecting evidence, applying laws, and identifying losses. It puts forward suggestions in three ways: coordinate the conflicts of existing data compliance legal systems, and issue implementation regulations related to data compliance; coordinate the conflict of responsibilities of law enforcement agencies and find out the focus of data compliance enforcement; improve the evidence preservation system, strengthen the typed research on data compliance cases, and improve the identification losses.

Keywords: enterprise data compliance; data security; scenario governance; data supervision; digital evidence