·法学探索

数字经济时代企业数据合规及其构建

孙 跃

摘要:数字经济时代,企业数据合规不仅是一种具有创新性的企业数据治理模式,而且还是加强个人信息保护与规范数字经济发展的重要手段和方式。企业数据合规的主要功能在于应对数据处理中的多维法律风险。构建企业数据合规体系,需要树立合法合规、告知同意、正当目的、最小必要等数据处理活动的基本原则;明确企业在数据收集、数据存储、数据使用、数据流转等环节的流程及其内容;设立数据合规专门机构并建立健全数据合规日常管理机制与风险应对机制。

关键词:数字经济;企业合规;数据合规;个人信息保护;多元共治

中图分类号:D922.16;F279.23 **文献标识码**:A **文章编号**:1003-8477(2022)08-0119-10

DOI:10.13660/j.cnki.42-1112/c.015927

近年来,持续高速发展的数字经济已经成为我国经济增长和社会进步的重要驱动力之一。数据是数字经济的基本生产要素和载体,企业则是市场经济的主体及主要组织形式。因此,企业数据在数字经济中具有十分重要的地位。在域外,自2018年欧盟实施《通用数据保护条例》(简称GDPR)以来,西方发达国家围绕企业数据治理展开的执法活动日益频繁。在国内,随着《网络安全法》《数据安全法》《个人信息保护法》以及配套法律规范的相继实施,依法依规治理企业数据处理活动已成为政府和企业必须面对的现实课题。

随着合规制度被引入我国企业治理体系,通过合规建设来降低数据处理违规风险对企业经营造成的损失,具有较强的理论研究与实践应用价值。虽然当前有不少学者对企业合规问题进行了研究,[①]但普遍存在两方面不足:其一,现有研究大多侧重于从整体角度研究企业合规问题,针对企业数据合规的专门性研究成果还不够丰富;其二,围绕企业数据治理展开的研究更多侧重于行政监管与执法视角,对数据合规这一以企业自治为主的创新机制关注度有限。基于上述研究背景与问题意识,本文将在明确企业数据合规基本定位的基础之上,从应对多维法律风险的角度阐述企业数据合规的主要功能,并重点探讨企业数据合规体系的构建路径,为企业数据合规建设及数据治理政务活动提供参考和指引。[②]

一、企业数据合规的基本定位及作用

企业数据合规建设虽然以企业为中心和主体,但其重要意义并不局限于企业自身的经营管理,还涉及个人权益与公共利益。从企业的角度来看,数

作者简介:孙跃(1990—),男,法学博士,山东工商学院法学院讲师(山东烟台,264005)。

基金项目:国家社会科学基金青年项目"法律方法在类案检索中的运用及其改进研究"(22CFX049)。

①相关文献可参见陈瑞华:《企业合规基本理论》,法律出版社2021年版,第1—6页;武长海:《数据法学》,法律出版社2022年版,第1—15页。

②本文所称的"数据"主要指"个人信息数据"。根据我国《数据安全法》第3条与《个人信息保护法》第4条的规定,数据是指"任何以电子或者其他方式对信息的记录",个人信息是指"以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息"。

据合规是一种具有创新性的企业数据治理模式。从个人权益角度来看，企业数据合规是一种加强个人信息保护的有效手段。从公共利益角度来看，企业数据合规建设有助于规范数字经济的发展。

（一）作为企业数据治理创新模式的数据合规

从企业经营管理的角度来看，数据合规本质上是一种针对企业数据处理活动的自我治理机制。首先，企业数据合规是一种数据处理法律风险控制机制。根据法律风险来源，数据违规风险可以被分为两类。第一类为数据违规的原生性风险，主要是指因数据违规直接引发的风险，如企业在收集与处理数据过程中对个人信息权益或相关公共利益的侵害引发的不利法律后果等。第二类为数据违规的派生性或次生性风险，主要是指因数据违规间接引发的扩散性风险。在数字化的大趋势下，企业数据与财务、人力资源、法律事务、营销、技术研发等各个业务部门之间均可能发生交叉关系，由此加剧了数据违规风险的流动性与扩散性。通过建立数据合规机制，有助于降低数据违规的派生性风险在企业各个业务部门之间的流动与扩散，从而使企业治理与合规体系更加完整。

其次，数据合规也是一种数据违规事后处理的创新机制，旨在降低数据违规活动造成的损失成本。数据违规可能会带来大规模侵权、不正当竞争或滥用市场支配地位、刑事犯罪等法律风险，使包括企业在内的多方主体遭受巨大损失。尽管建立数据合规体系并不能绝对避免数据违规事故的发生，但通过与执法或司法活动的积极配合，可借助合规整改等方式减免相应的法律责任。

最后，企业数据合规亦是一种可用于改善企业数据治理形象的创新机制。企业数据合规主要依靠企业的自我治理与约束，本质上是一种“自律机制”。企业数据合规不仅可以提升企业处理数据的合法性，而且还可以增强企业的商业道德与科技伦理意识，有助于激励企业承担与之相匹配的社会责任，引导企业塑造良好的商业信誉与公共形象。

（二）作为加强个人信息保护手段的数据合规

随着互联网时代的来临与数字科技的发展，数据已逐渐成为个人信息的主要载体。《民法典》虽然并未直接采用“个人信息权（利）”的表述方式，但在第111条明确了“自然人的个人信息受法律保护”，相当于确立了个人信息作为一种新兴权益的法律地位。根据《个人信息保护法》第54条的规定，个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。可见，通过建立合规机制保护个人信息及数据权益已成为企业必须履行的法定义务。

从企业与个人的相互关系来看，相对于个人，企业经营管理活动会有更大概率引发个人信息侵权行为。作为市场经济主导者的企业天然就拥有更多机会获取其他主体的个人信息，包括用户、员工以及来自第三方企业甚至政府机关的个人信息。例如，互联网平台企业拥有强大的科技和资本实力，能够更加快捷高效地收集与处理海量个人信息，一旦违规处理数据，将对个人信息保护产生巨大威胁。又如，关键信息基础设施运营者（CIIO）掌握的个人信息和数据关系到国计民生的重要领域，其对数据处理的合规性与国民数据安全之间具有密切联系。①因此，企业需要建立数据合规机制来履行保护个人信息和数据安全的法定义务。

从国家与个人的相互关系来看，个人信息权利束是国家履行积极保护义务和通过制度性保障对个人进行赋权的结果，是个人制衡信息处理者的工具和国家对数据处理者的规制策略。[1](p115)个人信息在概念上虽凸显“个人”，但其并非纯粹的私法权利，个人对其信息并不享有绝对支配权。质言之，个人信息只有在公共领域才能发挥其身份识别功能以及基于此产生的财产性利益。不仅如此，在经济全球化与经济数字化的叠加效应下，跨境数据流动不仅关乎国际贸易，而且也与国家数据安全甚至数据主权息息相关。数据合规建设的水平不仅关乎我国企业参与国际数字经济贸易活动，而且还会影响我国数字经济在全球范围内的战略布局。

①根据《关键信息基础设施安全保护条例》第2条，“关键信息基础设施”是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

（三）作为数字经济发展规范方式的数据合规

数字经济的发展是一个“去中心化”与“再中心化”相互交织的过程：在“去中心化”过程中，需要增强社会的信任，以互动性、参与性的制度构建回应这一趋势；在“再中心化”过程中，则需要防范平台的无序扩张、野蛮生长所带来的垄断、不正当竞争、隐私泄露等一系列风险。[2](p30)《网络安全法》第17条规定，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务是国家推进网络安全社会化服务体系建设的重要路径之一。《数据安全法》第18条规定，国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。鉴于此，数字经济发展的规范化需要引入“多元共治”理念，依靠由政府、企业、个人等“社会治理共同体”间的“共建共治共享”实现。[3](p116)

在企业层面，数据合规建设旨在引导企业从数字经济治理的对象转向数字经济治理的主体之一，进而提升企业参与数字经济治理的主动性与积极性，增强其在数据治理活动中的参与感与获得感。对于政府而言，企业数据合规建设可以降低行政监管与执法的成本，提高数据治理政务活动的效率与效果。就“企业—政府”的双向互动关系而言，企业数据合规建设可以促进形成“内外联动”与“自治+他治”的“数据多元共治”新格局，进一步凝聚企业与政府在规范数字经济发展方面的合力，最终形成更加持久稳固的数字经济秩序。

二、企业数据合规法律风险应对功能的多维展开

企业数据合规具有创新企业治理、加强个人信息保护、规范数字经济发展等诸多作用，而这些均建立在企业数据合规具有的数据处理活动风险应对功能之上。结合企业经营与管理的实际情况，企业数据合规的功能可从不同法律部门与领域的视角展开。

（一）基于民商经济法维度的分析

《民法典》在第四篇第六章中明确了个人信息及隐私保护的规则，奠定了个人信息保护的私法基础。根据《个人信息保护法》第69条和最高人民法院《关于人脸识别技术处理个人信息的司法解释》第6条的要旨，若企业平时不能采取有效措施存储证据以证明其在数据处理过程中不存在过错或不当行为，在日后纠纷中将可能承担败诉风险。由于数据往往以具体产品或服务为载体，互联网平台企业需要在提供服务时与用户订立合同。数据纠纷类案件不仅可能涉及民事法律关系，还可能与经济法中的滥用市场支配地位、不正当竞争以及消费者权益保护等问题相关联，数据处理违规引发的风险还会从传统侵权法领域扩展到合同法、经济法等领域。例如，在全国首例涉直播数据权益不正当竞争案中，法院就判定数据获取违规行为同时侵害了主播个人信息权利、消费者权益以及基于正当竞争市场经济秩序的公共利益。[4]法院认定企业通过App与用户签订了《服务协议》《隐私政策》，通过收集用户数据实施基于特定算法的价格歧视（即“大数据杀熟”）行为存在虚假宣传、价格欺诈和欺骗行为，判令企业应当承担《消费者权益保护法》第55条规定的“退一赔三”惩罚性赔偿责任。①

由于企业数据处理违规引发的个人信息侵权风险可能会从个人利益层面扩张到公共利益层面，根据《个人信息保护法》第70条以及《民事诉讼法》第55条的规定，企业数据的违规处理还会产生被提起公益诉讼的风险。在最高人民检察院2021年4月发布的“检察机关个人信息保护公益诉讼典型案例”中，有一起案例涉及某网络科技企业侵害公民个人信息，最终该企业被当地检察机关提起民事公益诉讼并责令限期整改。[5]

综上，基于民商经济法的维度，加强企业数据合规建设主要具有以下功能：（1）降低因侵害个人信息及数据权益引发的民事诉讼概率；（2）防止因侵害个人信息及数据权益引发的个体诉讼向群体诉讼甚至公益诉讼转化；（3）通过替代性的纠纷解决方案控制因侵害个人信息及数据权益引发的诉讼烈度，降低数据处理活动引发的民事争议解决成本；（4）对于难以避免的民事诉讼风险，企业可通过数据合规建设来强化日常管理与证据固定，在一定程度上避免其在诉讼中处于明显不利地位。

（二）基于行政法维度的分析

自2017年《网络安全法》实施以来，各级执法机

①参见（2020）浙0603民初9440号民事判决书。

关越发重视对企业数据合规的行政监管，企业因未落实网络安全等级保护制度及网络安全保护义务、未履行个人信息保护义务、未落实真实身份信息认证、未履行网络信息内容审核义务、网络产品和服务不符合法定要求等方面的事由遭受行政处罚的案例日益增多。[6]实践中，银行、证券、保险等金融行业是企业数据合规风险的高发领域。自2018年中国银保监会发布《银行业金融机构数据治理指引》后，不少企业因监管标准化数据（EAST）系统数据质量及报送存在违法违规行为而受罚。[7]根据《个人信息保护法》第66条的规定，个人信息违法行为的行政处罚责任被进一步加重，主要体现在“罚金幅度提高”和“行业禁入”两个方面。不仅如此，数据违规行为还会影响企业上市与投融资业务的开展。随着网信、工信、市场监管、公安等部门以及地方政府陆续制定关于数据合规的各种规范与标准，数据行政监管规范体系将日益健全，行政监管和处罚力度将呈现加大趋势。在此背景下，企业建立数据合规可主动配合数据行政监管，通过“内外结合”的方式满足合规经营需求。

除配合日常行政监管外，企业数据合规还具有促进行政执法和解的激励功能。所谓行政执法和解，即行政机关在执法活动中与行政相对人进行协商并达成和解协议的方式，在行政相对人满足限定条件的前提下减免行政处罚。[8](p83-98)行政执法和解具有较强的协商性与民主性，有助于将行政监管理念从处罚转变为预防，通过督促企业整改等方式降低行政执法成本、提高行政执法效率、激励企业合规经营。尽管我国尚未建立一般性行政执法和解制度，但中国证监会早在2015年就发布了《行政和解试点实施办法》，尝试在金融监管与执法领域探索构建行政和解制度。可以预见的是，随着行政执法和解制度的日益成熟，其迟早会进入数据治理系统并与数据合规机制建立耦合关系。可见，企业通过建立数据合规并将其作为一种行政执法和解的激励工具，具有降低因行政处罚等制裁措施造成的经营损失以及预防数据监管与处罚风险的重要功能。

（三）基于刑事法维度的分析

《刑法》中与企业数据合规相关的罪名可以被分为两类。一类是与个人信息保护直接相关的罪名，主要包括《刑法》第253条之一规定的“侵犯公民个人信息罪”以及第286条之一规定的“拒不履行信息网络安全管理义务罪”。另一类则是与个人信息保护存在间接关联的罪名。①以侵犯公民个人信息罪为例，该罪名增设于2009年实施的《刑法修正案（七）》。2015年实施的《刑法修正案（九）》将该罪的主体范围进行了扩张，并提高了最高法定刑幅度，折射出立法机关对个人信息保护重视程度不断提高的总体趋势。在司法领域，最高人民法院、最高人民检察院近年来也陆续在涉及数据及个人信息保护等领域发布了刑事司法解释及指导性案例，体现出司法机关对打击治理相关领域犯罪活动的重视。

《刑法》中关于个人信息保护的罪名有相当一部分属于单位犯罪。从程序法与实体法互动角度来看，即便企业最后被追究的罪名不成立，刑事诉讼程序的严苛性与复杂性也会严重影响企业的经营及公众形象。根据实践经验，企业合规可以在争取不起诉或暂缓起诉、寻求无罪抗辩、减轻刑事处罚等方面产生积极作用。[9](p3-24)综上，将数据合规作为专项计划融入企业刑事合规体系之中，不仅具有预防数据犯罪活动的重要功能，同时还具有减免此类犯罪刑事法律责任的刑事诉讼激励功能。

（四）基于国际法维度的分析

企业数据合规具有引导企业数据处理活动符合域外及国际数据规范的功能。在经济全球化与经济数字化两大趋势的叠加背景下，各国对个人信息保护及跨境数据合规的重视程度越来越高。这意味着企业在参与国际数字经济贸易活动中，因违反国际组织或外国相关法律法规而引发的数据处理风险不断上升。欧盟GDPR第六章规定，各国应当设立独立的政府监管机构来监督数据合规问题。2021年，欧盟依据GDPR进行的罚款总额为11亿欧元，约为2020年罚款总额的7倍。[10]近年来，我国已有多家企业因数据合规问题遭到不同方式与程度的制裁；亦有部分国家通过提高数据合规准入门槛，在实质上设立了“数据贸易壁垒”。跨国企业的合规建设已无法回避国际法律维度下的数据

①这些罪名主要分布在《刑法》第177条、219条、285条、286条、287条、308等条款中。

跨境合规问题。

不同国家或国际组织对数据合规设置的具体标准碎片化现象比较严重，容易引发规范间的冲突，具体体现在“价值”与“规则”两方面。一方面，不同国家、地区对数据合规价值取向的侧重有所不同。例如，相对于欧盟GDPR，美国2018年颁布的《加利福尼亚消费者隐私法》（简称CCPA）更加重视产业利益，强调通过合理地削弱个人对数据信息的绝对控制权来为数据所有者与控制者留有探索创新性数据交易商业模式的空间。[11](p85-94)另一方面，不同国家、地区关于同一数据合规事项的规定不尽相同。例如，我国2022年制定的《数据出境安全评估办法》就面临与GDPR、美国与欧盟的《隐私盾协议》（U.S.-EU Privacy Shield）、OECD规则体系的衔接问题。[12](p61-72)为了应对上述挑战，数据合规的功能需要从衔接本国数据规范与国际多元数据规范的维度展开。

三、企业数据合规体系的构建路径

企业数据合规体系主要包括基本原则、流程及其内容、专门机构与运行机制三部分。数据合规基本原则为企业数据合规奠定价值取向与总体目标，是数据合规体系的“灵魂”；数据合规流程及内容确定了企业数据合规体系建设的框架和具体事项，是数据合规的“骨骼”与“血肉”；数据合规专门机构与运行机制涉及企业数据合规的具体实施主体及作业模式，是数据合规体系的“神经系统”。

（一）树立企业数据合规的基本原则

通过综合分析我国数据领域的主要立法以及域外代表性法律规范（特别是欧盟GDPR）中的一般性条款与法律原则规定，可以提炼出数据合规应遵循的四项基本原则：合法合规、告知同意、正当目的、最小必要。合法合规原则是数据合规建设的首要原则与最低限度；告知同意原则是数据合规风险控制的主要准则；正当目的原则是在实质层面对合法合规原则的补充与调整；最小必要原则是在企业数据权益与个人信息权益之间进行权衡所应遵循的原则。

1.合法合规原则

关于个人信息保护与数据处理的立法，无论是我国还是欧盟GDPR，都将合法性（合法合规）原则确立为企业数据合规应当满足的首要原则与最低标准。合法合规原则可以从狭义和广义两个角度理解。狭义上的合法合规原则要求企业处理数据活动必须遵守法律、行政法规的基本规定，特别是与个人信息保护及数据处理直接相关的法律规定。广义上的合法合规原则要求企业数据合规除符合相关法律、行政法规外，还必须符合与这些法律、行政法规相关的辅助性或解释性规范。[13](p222)由于法律、行政法规的内容相对抽象和概括，在适用与执行过程中还需要进一步的细化与解释。实践中，行政机关或司法机关往往会制定一系列规范以作为监管执法活动或司法裁判活动的依据，这些规范虽然并非我国2015年《立法法》中规定的法律或行政法规，但在内容上具有更强的可操作性，因而也应当被作为企业合规建设遵守的规范依据。

行政执法机关制定的数据规范主要包括：（1）国务院各部门制定的规章，如工信部制定的《电信和互联网用户个人信息保护规定》、国家互联网信息办公室制定的《儿童个人信息网络保护规定》、国家互联网信息办公室和工业和信息化部等部门联合制定《App违法违规收集使用个人信息行为认定方法》等；（2）地方性法规，如《深圳经济特区数据条例》《上海市数据条例》等；（3）地方规范性文件，如广州市国资委制定的《广州市国资委监管企业数据安全合规管理指南（试行2021年版）》等；（4）国家标准或团体规定，如全国信息安全标准化技术委员会制定的《信息安全技术—个人信息去标识化指南》（GB/T 37964—2019）、《个人信息安全影响评估指南》（GB/T 39335—2020）等。

司法机关制定或通过个案裁判形成的数据规范主要包括：（1）司法解释，如最高人民法院制定的《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》《关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》等；（2）判例，特别是最高人民法院或最高人民检察院发布的指导性案例、典型案例等。[14](p103)例如，最高人民法院指导案例145至147号、最高人民检察院发布的检察机关个人信息保护公益诉讼典型案例等权威性司法案例，均涉及个人信息保护与数据合规问题。

2.告知同意原则

我国《民法典》第1035条第一款第(一)项、《数据安全法》第18条和第19条、《个人信息保护法》第13条第一款第(一)项、《网络安全法》第22条第三款共同确立了个人信息数据处理的“告知同意原则”;欧盟GDPR在第7条和第8条对数据处理的同意原则进行了专门规定。告知同意本质上是一种建立在企业与个人之间的数据处理合意(契约)行为,其内涵可以从程序前置性、告知方式、特殊情形下的单独同意以及例外情形等四个方面展开。

首先,通过特定的方式告知并取得个人同意应当作为所有个人信息数据处理活动的前置程序。为了避免没有履行告知与同意义务的风险,应根据我国《个人信息保护法》第17条规定,采取“处理前告知同意”而非“事后追认”的方式。其次,告知应当采用明确易理解的方式。根据《个人信息保护法》第14条的规定,基于个人同意处理个人信息的,该同意应当由个人在充分知情的前提下自愿且明确地作出。以网站或App中的“隐私政策”为例,不能期待用户以全文阅读的方式了解所有的隐私条款,因而企业在设定用户的义务或者扩大经营者被授权的范围时,应当采取更加显著的方式进行重点提示和解释说明。再次,要对法定应当采取单独同意方式处理个人信息数据进行专门的合规审查。根据《个人信息保护法》,当存在“向第三方提供其处理的个人信息”“公开其处理的个人信息”“对外提供个人图像、个人身份特征信息”“处理敏感个人信息”“向境外提供个人信息”等情形时,需要以单独方式征求个人同意。最后,需要明确告知同意原则的例外情形。实践中常见的除外情形有两类:其一为“法律、行政法规另有规定的事项”,通常是紧急情况下出于维护重大公共利益的需求。此种情形下需要遵循比例原则,衡量并判断个人信息权益与公共利益孰轻孰重,同时应根据《个人信息保护法》第18条第二款的规定,在紧急情况消失后及时告知个人。其二为“特殊群体的告知同意规则”。例如,根据《个人信息保护法》第31条,个人信息处理者处理不满14周岁未成年人的个人信息应当取得其父母或者其他监护人的同意。

3.正当目的原则

我国《民法典》第1035条第一款、《个人信息保护法》第5条、《数据安全法》第17条第一款、《网络安全法》第41条第一款共同确立了个人信息数据处理的正当性(正当目的)原则;欧盟GDPR第5条和第6条中均有关于数据处理目的限制的规定。如果说合法合规原则是对数据合规进行判断的形式标准,那么正当目的则是对数据合规进行实质性判断的重要标准之一。

首先,基于正当性原则的合规性审查,要重点考察企业对个人信息数据进行处理时是否具有明确的正当性依据。根据《民法典》第1036条以及《个人信息保护法》第13条的规定,个人信息处理的正当性依据主要包括:(1)为了履行约定义务;(2)为了履行法定义务;(3)为了应对突发公共卫生事件或者紧急情况下保护自然人的生命健康和财产安全;(4)为了公共利益并合理处理;(5)在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息。因此,在个人信息数据处理缺乏以上法定事由作为正当性基础时,就应当认定处理行为违规。其次,根据《个人信息保护法》第21条的规定,在个人信息处理者委托处理个人信息的情况下,还需要审查受托人是否在约定的目的范围内处理个人信息数据。最后,根据《个人信息保护法》第26条的规定,企业收集的个人图像、身份识别信息只能用于维护公共安全的目的,不得用于其他(如商业营利)目的。

4.最小必要原则

我国《民法典》第1035条第一款、《个人信息保护法》第5条、《数据安全法》第17条第一款、《网络安全法》第41条第一款共同确立了数据处理活动的最小必要原则;欧盟GDPR则在第5条1(c)中规定了最小必要原则。

首先,企业在处理个人信息数据时,需要将数据处理限定在实现其服务功能的最小信息范围内。为了满足这一要求,应当从“定性”和“定量”两个维度对企业数据合规进行审查。定性审查的重点在于考察企业处理个人信息是否与其提供的服务密切相关,在非必要的情况下不得收集个人信息。[15](p72)定量审查需要考察企业处理数据的规模体量与其提供服务基本需求之间的比例是否得当,不应以提供必要服务为由进行个人信息数据的超量处理。其次,企业在对最小必要原则进行抗辩

时，要遵循《个人信息保护法》第16条的规定。除非处理个人信息属于企业提供产品或者服务所必需，否则企业不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务。最后，要对最小必要原则进行动态合规性审查。根据《个人信息保护法》第19条的规定，个人信息数据存储期限应当为实现处理目的所必要的最短时间。此外，还要根据《个人信息保护法》第47条的规定，审查个人信息数据存储的必要性基础是否丧失，当存在以下两种情形时，应当主动删除或配合个人行使删除权（被遗忘权）：（1）处理目的已实现、无法实现或者为实现处理目的不再必要；（2）企业停止提供产品或者服务或存储期限已届满。

（二）明确企业数据合规的流程及其内容

数据处理是由多个环节组成的活动。根据数据处理活动的不同环节，企业数据处理活动主要包括数据收集、数据存储、数据使用、数据流转等流程。明确这些流程中的合规事项及其审查标准，是企业数据合规体系构建的主要内容。

1.数据收集合规

根据来源的不同，数据收集可以被分为直接收集和间接收集。直接收集即企业采用一定的技术手段直接获取个人信息数据。根据《信息安全技术个人信息安全规范》《App违法违规认定方法》《App违法违规收集使用个人信息自评估指南》的相关规定，企业在收集用户个人信息时要坚持合法与诚信原则，不得使用欺诈、诱骗、误导或以合法形式掩盖非法目的等方式；也不得隐瞒产品或服务的个人信息收集功能。因此，数据收集合规审查应当围绕企业是否将收集活动的目的、方式、可能的后果等如实告知用户进行。间接收集即企业从第三方（通常是数据交易相对人）处获取个人信息等数据。针对第三方提供的个人信息，企业有必要将数据合规审查嵌入与目标企业交易的尽职调查流程中，防止数据收集违规引发的法律风险在具有交易关系的企业之间传递。

同时，企业还要对个人信息数据收集的技术手段进行合规审查，例如实践中被广泛使用“网络爬虫”。网络爬虫是一种由机器模仿人的行为抓取数据的工具，爬虫的活动一般表面显现为正常用户的操作。[16](p245)当企业运营爬虫工具收集数据时，如果没有履行对个人的告知同意义务或违反被爬取网站的Robots协议（反爬虫协议），则有可能会面临承担民事侵权责任甚至刑事责任的后果。因此，企业需要对爬虫技术的运用进行合规监控，在直接爬取个人信息数据时要履行告知同意义务；在爬取其他网站数据时，要遵循网站的Robots协议，不得运用技术手段绕开或破坏被爬取网站的反爬取系统。

2.数据存储合规

企业数据存储的合规事项包括三个主要内容。首先，企业要加强个人信息数据存储的安全保障机制。“对外”层面，非因法定或约定事由，企业不得随意公开个人信息数据，并应当采取必要技术手段对个人信息数据进行加密保护。“对内”层面，企业需要建立完整的数据访问权限与监管机制，防止数据被无权或越权访问，并能够通过数据访问记录追踪数据访问情况，确定数据安全的责任主体。

其次，企业要对存储的个人信息数据进行分类与分级管理。企业应当运用类型化思维，综合现行法律法规、国家标准（如《信息系统安全等级保护定级指南》）以及地方政府数据分类分级指南的规定，对各类数据分类分级管理，以确保数据存储的安全性。[17](p29)在此基础上，企业还应当着重加强对生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹、未成年人等个人敏感信息的保护，防止个人敏感信息被泄露、非法提供或滥用。

最后，根据《个人信息保护法》第51条规定，企业还需要对个人信息进行去标识处理。企业需要建立“确定目标—识别标识—处理标识—验证审批”的个人信息去标识化流程机制，运用统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术以及数据合成技术等手段进行个人信息数据的去标识化。

3.数据使用合规

狭义上的数据使用合规主要面向企业自身使用数据的行为。企业在使用数据时往往需要借助特定的算法实现，因而除应当贯彻企业数据合规的基本原则外，企业还需要重视对算法合规的审查。根据《个人信息保护法》第24条以及网信办、工信部、公安部、市场监管总局制定的《互联网信息服务算法推荐管理规定》，对算法合规的审查主要从“算法透明”“算法公正”“算法弱势群体保护”等角度展

开。[18](p138-159)算法透明要求企业应当以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图和主要运行机制等，避免“算法黑箱”损害个人信息权益。算法公正要求企业应当向用户提供不针对其个人特征的选项或者向用户提供便捷的关闭算法推荐服务的选项，不得运用算法技术手段进行“算法歧视”（如“大数据杀熟”）。算法弱势群体保护要求企业应对未成年人、老年人、劳动者、消费者等特定情境下的算法弱势群体给予合理的差别待遇，以保护这些群体的数据权益。

广义上的数据使用合规除包括企业自身使用数据的行为合规外，还应当包括对企业配合用户行使个人信息权能的情况进行审查与规范。在我国现行立法框架下，个人信息权利束主要包括查询权、更正权、删除权（被遗忘权）、复制权、转移权（可携权）等。由于个人信息及其数据产生与流通均具有公共性，因而相关权利束的行使无法建立在个人对其信息的绝对控制之上，而是需要包括企业在内的多方主体的配合。[19](p194-206)基于上述原理，企业不仅负有消极不作为方式避免侵害个人信息数据权益的义务，而且负有以积极作为方式配合用户在合法合理的限度内行使其个人信息权利以满足用户数据权益的义务。

4.数据流转合规

数据流转合规主要针对企业向第三方转让个人信息数据的行为。根据《个人信息保护法》第23条的规定，企业向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。同时，接收企业应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息，变更原先的处理目的、处理方式应当依照本法规定重新取得个人同意。考虑到SDK（软件开发包）可能产生的数据合规隐患，企业在涉及运用SDK进行第三方接入管理的数据处理行为时，还应当建立专门的第三方接入管理机制，明确企业与第三方的权责划分。企业还需要对第三方接入进行实时监管与审计，在出现安全隐患时应当及时停止第三方接入。

由于数据跨境流动涉及国家数据安全甚至数据主权问题，企业应严格依照《个人信息保护法》《数据出境安全评估办法》中关于个人信息及数据跨境提供的规则进行评估，并结合数据接收方所在国家或地区的规定以及双方订立的合同进行合规审查。对于金融、生物医疗等领域的个人信息出境规则，应当依据国务院《人类遗传资源管理条例》、中国人民银行《个人金融信息保护技术规范》（JR/T 0171—2020）以及国家卫健委《国家健康医疗大数据标准、安全和服务管理办法（试行）》规定的标准，审查数据能否跨境流转以及流转的具体程序。

（三）健全企业数据合规专门机构与运行机制

企业数据合规部门是企业数据合规建设与运行的主导者。就工作模式而言，企业数据合规可以分为数据合规的日常管理机制与违规风险应对机制，前者致力于预防数据合规风险，后者则以应对已经发生的数据违规风险为目标。基于数据合规部门及相关工作机制的运行，企业数据合规体系得以实现从静态到动态运转，形成一个鲜活的数据治理有机体。

1.设立数据合规专门机构

企业数据合规管理部门是数据合规体系运行的主导者。从企业数据合规部门与其他企业部门的关系来看，数据合规管理部门的设立模式主要有三种。第一种模式是将数据合规内置于企业的法律事务部门（即“法务部”）。在这一模式下，数据合规部门作为综合性合规部门的组成部分之一内置于法务部。第二种模式是合规部门独立于法务部，但数据合规部门并不独立于综合性的合规部门。第三种模式则是将数据合规部门独立于法务部和综合性合规部门。

第一种模式的优点在于可以精简企业的管理部门，降低管理成本，且有助于促进合规事务与法律事务的一体化处理，这一模式适合传统中小企业。对于以数字经济为主要业务领域的企业（如互联网企业、高新制造业或服务业企业等），其数据合规事项较为庞杂，专业性较强，因而不宜采用此种模式。同时，从治理逻辑层面看，数据合规并不完全属于法律事务的下位概念。由于数据合规不仅局限于企业交易过程，还包括事前评估与事后督导，超出了传统法务的工作范围。因此，对于数据合规事务需求量较大且具备一定人财物条件的企

业，应当优先采用第二或第三种模式，将企业数据合规部门与传统意义上的法务部门进行分离。①至于数据合规专门机构的负责人，则可以借鉴德国1977年《联邦数据保护法》的规定，任命至少一名“数据保护官（DPO）”，赋予其独立履行企业数据合规监管职权的地位。[20](p127)

2.数据合规日常管理机制

数据合规日常管理机制的主要功能在于通过系统性管理工程降低数据违规风险，持续性改进企业数据合规治理体系。数据合规日常管理工作包括以下方面：其一，确定企业数据合规管理团队。考虑到企业数据合规管理具有很强的综合性，因而应当为此组建具有法律、科技、财务等多元知识结构背景的人才队伍，以确保数据合规日常管理的专业性。其二，参与制定或修改企业数据合规文件（如数据合规管理规定、数据合规员工手册、数据合规指引等），为数据合规公司治理制度提供明确而完备的规范依据，监督这些规范文件的执行情况。[21](p97)其三，对数据合规事务进行全方位督导，及时发现、记录、审查、评估、通报数据违规的潜在风险并提出具体建议与方案；对其他部门执行数据合规事项的情况进行考核与评价。其四，组织数据合规培训，增强企业数据合规意识与治理能力。其五，与企业其他职能部门、政府机关、第三方机构进行对接，通过协作共同推动企业数据合规体系的建设与完善，形成企业数据合规的“多元共治”格局。

3.数据违规风险的应对机制

健全的数据合规日常管理机制虽然可以有效防控数据违规风险，但并不能完全消除企业违规数据风险。因此，对于已经发生的数据违规风险，还需要建立特定的应对机制。[22](p19)根据法律关系与法律责任的性质，企业数据违规风险主要包括民事法律风险、行政法律风险以及刑事法律风险。

数据违规的民事法律风险主要体现为数据违规引发的侵权责任和违约责任。考虑到民商事纠纷解决机制相对多元化，企业应当及时采取停止侵害、继续履约或积极赔偿等方式化解矛盾，防止数据违规产生高昂的诉讼成本或对企业声誉造成严重负面影响。数据违规的行政法律风险主要体现为企业因违规处理个人信息数据遭受行政处罚。为了应对此类风险，企业数据合规部门应当在第一时间告知企业管理层及其他部门配合行政监管执法部门的调查并及时进行合规整改，确保在最短时间内消除企业数据违规事由。数据违规的刑事法律风险主要指企业因违反刑法而涉嫌犯罪。鉴于刑罚的严厉性，企业在面临此类风险时应当格外审慎，需要及时采用认罪认罚、补救挽损、查出责任人、评估整改等手段，争取程序层面的合规不起诉或实体层面的刑事责任减免。②

结语

尽管近年来数字经济的发展为我国带来了“数字红利”，但企业处理数据的行为在促进数字经济发展与提高人民生活水平福利的同时，也对个人信息保护与数字经济治理提出了诸多新挑战。正是在这一时代背景下，作为一种数据治理创新模式的企业数据合规应运而生。企业数据合规机制本质上是一种基于多元共治理念的数据治理模式。在规范依据方面，其涉及民商经济法、行政法、刑事法、国际法等多元法律规范体系；在治理主体方面，其涉及立法机关、行政（监管与执法）机关、司法机关、企业自身以及第三方机构等多元主体；在治理机制方面，企业数据合规同时涉及数据的日常治理与涉案风险应对（整改）。正因如此，对企业数据合规的研究以及实践应用转化，需要整合多重维度的智识。

沿着上述思路，本文从基本定位、多维功能以及构建路径的角度，对数字经济时代背景下的企业数据合规基本问题进行了探讨。可以预见，随着国家、企业以及个人对数据合规建设的日益重视，企业数据合规体系也会越发完备。在企业数据合规体系的保驾护航下，数字经济发展产生的“数字红利”也将进一步惠及更多市场主体，这对于数字科

①例如，上海市杨浦区检察院联合市信息服务业行业协会、市数据合规与安全产业发展专家工作组、区工商业联合会制定发布的《企业数据合规指引》就不建议将企业合规部门设置在法务部门之下。

②此类做法在实践中已有成功案例，参见《以企业合规护航数字经济创新发展——上海首例数据合规案件办案侧记》，载《检察日报》2022年5月30日，第01版。

技时代个人信息权益的保护、数字经济的健康持续发展以及通过科技赋能促进共同富裕的实现，都将产生更加显著而深远的积极效用。

参考文献：

[1]王锡锌.国家保护视野中的个人信息权利束[J].中国社会科学，2021，(11).

[2]王伟，任豪.数字中国建设的法治保障[J].法律适用，2021，(12).

[3]张吉豫.构建多元共治的算法治理体系[J].法律科学，2022，(1).

[4]余建华，庞楚楚.杭州余杭法院宣判首例涉直播数据权益不正当竞争案[N].人民法院报，2022-01-27(03).

[5]检察机关个人信息保护公益诉讼典型案例[EB/OL].https://www.spp.gov.cn/spp/xwfbh/wsfbt/202104/t20210422_516357.shtml?ivk_sa=1024320u#1，2022-03-01.

[6]吴丹君，周天一.网络安全法执法案例汇总与合规建议[EB/OL].https://www.sohu.com/a/251013656_658347，2022-03-01.

[7]8家银行遭重罚合计罚款1770万元[EB/OL].https://www.sohu.com/a/394583759_565332，2022-03-01.

[8]方世荣，白云锋.行政执法和解的模式及其运用[J].法学研究，2019，(5).

[9]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).

[10]亚马逊、脸书"贡献"10亿欧元 欧洲2021数据保护罚款创纪录[EB/OL].https://ishare.ifeng.com/c/s/v002RNs2wj8YU-_MOH0yu253ar0wu1DLaor0mFtvb-djnshjI，2022-03-01.

[11]相丽玲，贾昆.中外个人数据保护标准研究进展与未来趋势分析[J].情报杂志，2020，(2).

[12]洪延青.数据跨境流动的规则碎片化及中国应对[J].行政法学研究，2022，(4).

[13]孙光宁.社会主义核心价值观的法源地位及其作用提升[J].中国法学，2022，(2).

[14]孙跃.指导性案例与抽象司法解释的互动及其完善[J].法学家，2020，(2).

[15]武腾.最小必要原则在平台处理个人信息实践中的适用[J].法学研究，2021，(6).

[16]Riley K .Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases，Fordham Intellectual Property[J].Media & Entertainment Law Journal，2019，(29).

[17]杨力.论数据安全的等保合规范式转型[J].法学，2022，(6).

[18]丁晓东.论算法的法律规制[J].中国社会科学，2020，(12).

[19]丁晓东.个人信息私法保护的困境与出路[J].法学研究，2018，(6).

[20]武长海.国际数据法学[M].北京：法律出版社，2021.

[21]毛逸潇.数据保护合规体系研究[J].国家检察官学院学报，2022，(2).

[22]陈瑞华.有效合规管理的两种模式[J].法制与社会发展，2022，(1).

责任编辑　王　京