数据合规风险衍生与网络安全治理

闫 东
北京盈科（沈阳）律师事务所，辽宁 沈阳 110000

摘要：数据安全合规是网络安全的重要内容之一。当前《数据安全法》等法律对各企事业单位的网络安全与数据治理问题提出了新要求，本文从法规疏解视阈梳理网络安全与数据合规的立法态势，从网络安全视角剖析数据安全、数据合规、风险处理问题，从法律规制视域研讨数据合规与安全治理的安全性、隐私权、责任制。

关键词：数据合规；数据治理；网络安全；法律规制

由于个人信息被滥用行为屡禁不止，引发数据安全“立法热”[1]，《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》）等多项法律的颁布实施，为我国网络信息安全奠定了强而有力的基础，为企业明确指出数据合规的方向。在网络安全的大背景之下，数据合规成为一个重要的时代课题[2]，数据合规对于进一步提高数据安全，维护国家网络空间主权意义重大。

一、法规梳理下的数据合规与网络安全

网络安全审查制度与数据安全审查制度是《网络安全法》《数据安全法》确立的两项重要国家安全审查制度。2021年6月10日全国人民代表大会常务委员会出台了《数据安全法》，于9月1日起正式施行，此法作为我国数据安全领域的专门法律，其目的是为保障国家、企业及个人的数据安全，为个人信息数据保护提供可靠的法律依据。《数据安全法》共七章五十五条，围绕数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放等提出系列要求，在完善数据安全保护的同时，也为企业未来数据合规指明了道路。

《数据安全法》将数据定义为，任何以电子或者其他方式对信息的记录，这进一步扩大了数据保护的范围。《数据安全法》最大的特色就是将数据安全与数据开发利用提升至同等重要的高度。其设立专章，明确提出“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”，并从技术研发、标准体系建设、检测评估认证、数据交易管理、教育培训、人才培养等多方面，体现数据开发利用和数据安全治理并行的思想内涵。该法虽然称为《数据安全法》，但却不只关注于安全，而是将安全与发展同步考虑。《数据安全法》另一大重要变化就是首次提出“国家核心数据”概念，明确关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，并增加了相应处罚措施，规定违反国家核心数据管理制度，危害国家主权安全的可处200万至1000万的罚款。2017年《网络安全法》首次提出了重要数据的概念，而《数据安全法》在“重要数据”之外又新增了“国家核心数据”概念，更加彰显了贯彻对数据实行分类分级保护的思想，对未来出台数据分类分级统一标准或细则提供了更加精细化的设计思路。

2017年6月1日，《网络安全法》正式施行，其作为我国第一部全面规范网络空间安全管理方面问题的基础性法律为中国网络安全保护奠定了基础。《网络安全法》从2013年下半年就被列入立法日程，2016年底即被颁布，速度之快充分说明党的十八大期间出台这部法律的重要性和紧迫性。《网络安全法》共七章七十九条，内容十分丰富，具有六大亮点。第一，明确了网络空间主权原则。该法在第一条就明确规定要维护我国的网络空间主权，网络空间主权最初是规定在《中华人民共和国国家安全法》中，在《网络安全法》中又进一步明确。网络空间主权是一国国家主权在网络空间的自然延伸和表现。[3] 第二，明确了网络产品和服务提供者的安全义务。网络产品、服务应当符合相关国家标准的强制性要求。第三，明确

了网络运营者的安全义务。网络经营者要遵守法律、遵守社会公德、遵守商业道德、负有诚实信用义务等。第四，进一步完善了个人信息保护制度。网络运营者收集、使用个人信息，必须符合合法、正当、必要的要求，不得违反法律、行政法规使用个人信息。第五，建立关键信息基础设施安全保护制度。关键信息基础建设是指那些一经破坏，就会丧失功能泄露数据，严重危害到国家安全及公共利益的设施。第六，确立了关键信息基础设施重要数据跨境传输规则。“《网络安全法》具有整体性、协调性、稳定性和可操作性等特征，是我国应对国际网络安全挑战、维护网络空间主权、保障公民网络空间的合法权益不受侵害、保障国家安全的利器，为全球互联网的治理贡献了中国智慧。”[4]《网络安全法》正式施行已经超过四年，《数据安全法》也已生效并展现出执行力，我们正亲历并见证我国网络安全、数据安全这座大厦从最初的夯实地基，到如今搭建起房梁支柱，相应地配套法律法规和规范性文件也逐步颁布，将一步步落实国家总体安全观下的网络空间治理的智慧。

二、网络安全视角下的数据合规与数据安全

（一）网络安全治理的关键：数据安全。数字经济时代，数据安全必须成为当下各个公司网络安全的红线与底线问题，尤其是置身数字业务的公司，在共享和传输大量个人数据的在线环境中，应越来越重视数据信息的安全。以数据泄露为例，其通常涉及各种类型的个人数据，例如财务账户信息、驾驶执照号码、生物识别标识和身份证信息。如果公司未能充分尽职履行数据安全的义务，黑客可以轻而易举地访问公司的计算机网络，窃取数千人的敏感个人数据而导致黑客从中掌握了公司与用户的数据钥匙：身份证件信息、生物识别标识和公司财务信息。因此，无论是公司内部安全机制漏洞，还是由于第三方供应商、勒索软件攻击导致的数据泄露，犯罪分子都有无穷无尽的机会窃取企业与个人数据的敏感信息。

（二）网络安全治理的核心：数据合规。数据合规是数据保护合规的简写，是遵循各种法规和标准以维护受监管数据（例如个人身份信息、医疗信息）或敏感数据（例如客户名单）的完整性和可用性的过程。数据合规性的关键在于跟踪正在存储的数据类型和数量，以及在其生命周期中管理存储的数据，数据合规是确保企业对敏感数据进行管理的过程实现对适用法律、法规和标准的遵守。数据合规包括企业使用其个人数据以及授权消费者在个人信息应修改时与企业沟通等规则，同时按照规律赋予用户个人访问、纠正或请求删除数据的权利。

（三）网络安全治理的监管：风险处理。当网络安全问题涉及公司与用户的数据风险时，风险很容易被处理、量化并考虑到公司业务决策中，因为人们对未来做出的任何决定都必须考虑到一定程度的不确定性与数据风险的负外部性。一方面，内部风险源于企业内部。当下公司不断共享数据以进行协作并推动业务向前发展，无论在办公环境还是远程工作，只需点击几下鼠标即可轻松共享文件，在此过程中网络安全的内部风险纯粹是偶然的，因为数据泄露涉及安全信息的无意发布。另一方面，外部风险包括来自网络犯罪分子的攻击。以身份信息盗用后的处理为例，身份盗用的问题在于，个人数据不能像银行卡号那样轻易地被“取消”，身份证号码不能更改，指纹或眼部扫描、健康信息和基因数据等生物特征数据无法变更，而且犯罪分子可能会在获取受害者的个人数据后的数月或数年后使用，此时的风险更是隐藏于事后的风险。

三、法律规制视域下的数据合规与安全治理

当下，针对数据合规与安全治理问题，域外的立法与法规围绕数据安全和网络安全对不同的行业而展开规制。以数据安全为例，以下是一些域外著名的数据保护法规与规则（见表 1）。

因此，国内根据我国最新的《网络安全法》《数据安全法》等法律规定的内容，国外根据全球网络数据安全规范性法律文件立法的经验，当下企业的数据合规与网络安全治理应注重以下几点：

（一）数据合规与安全治理：安全性。当下企业用户数据已成为企业在线业务中最敏感的部分。许多公司将有关客户或员工的敏感个人信息保存在其文件或网络中，由于企业在互联网上留下了大量的数字足迹，因此企业保护和谨防用户个人数据泄露变得至关重要，尤其是需确保受监管和敏感数据免遭未经授权的使用。企业针对数据合规中的未经授权的访问情况，对管理有权访问数据的人员，必须确保相关人员了解网络安全与数据合规，明确他 / 她在保护敏感数据方面的责任。因此数据安全性问题可能会导致无法挽回的声誉损害，因此公司需要制定完善的安全计划确保数据安全并安全处置数据，切实履行保护敏感数据的法律义务。

（二）数据合规与安全治理：隐私权。公司在处理或传输个人敏感数据之前需获得“肯定的明确同意”，发布透明的隐私政策，实施“合理的数

据安全实践”，同时公司需向消费者披露隐私政策，详细说明他们的数据收集、处理和传输活动，并将这些活动的任何重大变化通知消费者并允许用户访问、更正、删除和移植用户个人的数据。以敏感信息的合规为例，如果信息揭示了一个用户想要向他人隐瞒的令人尴尬或损害名誉的事情，则该信息可能是敏感的，针对此，应考虑为用户提供访问、更正、删除和可移植性的权利。

（三）数据合规与安全治理：责任制。网络安全中数据的收集、存储、处理、获取、维护都需要约束性规则和问责制度。网络数据安全责任制度在于事后规制身份盗用和数据泄露的网络安全影响。网络数据安全责任制度的目的在于督促网络平台企业遵守正在进行的、预定的粉碎和数据销毁程序性的规则，从而避免数据泄露的风险和网络安全隐患。网络数据安全责任制度需要自我或共同监管机制来监管隐私和数据保护，为保护个人数据的权利建立强有力的具体保障措施。一方面，为公司员工制定与实体营业场所外记录和个人信息的收集、存储、访问和运输相关的可靠安全政策，针对违反信息安全计划的行为制定和实施纪律处分规则。另一方面，与服务提供商或服务组织合作并对其进行监督，要求他们遵守企业客户的个人信息安全措施。

四、结语

当今世界已经进入数据时代，随着数据价值不断升高，数据安全风险也不断升高。数据权属之争，归根结底还是利益之争。[5]《数据安全法》等法律的相继生效，我国迎来了全面的数据安全与个人信息保护的新周期，这也彰示着我国从规范监管层面顺应时代信息的系统设计，但我们还需要关注每一处细节的合规风险管控，实时关注着来自技术发展与监管所带来的新要求，在企业数据驱动的经营理念中树立起合规价值的认知。

表1 域外著名的数据保护法规与规则

	规范性文件	数据安全与合规的要求
美国	《健康保险流通与责任法案》（HIPAA）	《健康保险流通与责任法案》为企业和提供者必须如何处理患者的个人健康信息以确保其保密和安全设定了数据安全标准。HIPAA定义的所有“涵盖实体”都必须保HIPAA合规性。从本质上讲，任何从事医疗保健业务的组织都必须遵守HIPPA数据安全和合规标准。
	《萨班斯-奥克斯利法案》（SOX）	2002年萨班斯-奥克斯利法案是在安然丑闻发生后不久颁布的，以防止类似的欺诈事件发生。虽然SOX主要处理财务报告，但它仍然是一个重要的合规性考虑因素，IT组织仍然需要了解并确保财务报告的准确性和及时性。美国的每家上市公司都必须符合SOX。
欧盟	《通用数据保护条例》（GDPR）	《通用数据保护条例》保护其用户的数据以及了解数据提供者收集的有关他们的信息的权利。它还为报告违规行为以及如何存储和保护数据制定了严格的规则。任何与欧盟客户的业务都受GDPR约束，而GDPR在惩罚方面是较为严厉的规定之一。它允许根据违规的严重程度采取分层方法，最高罚款为全球年营业额的4%或2000万欧元。
加拿大	《支付卡行业数据安全标准》（PCI-DSS）	《支付卡行业数据安全标准》（PCI-DSS）由独立监管机构支付卡行业安全标准委员会制定。与其他法规不同，它不是由政府实体强加的；这是一组由PCI-SSC执行的合同承诺。任何接受、存储或传输持卡人数据的企业都受PCI-DSS约束，需要采取适当的保护措施，以确保他们正确处理和存储该数据。

参考文献

[1] 唐林垚. 数据合规科技的风险规制及法理构建[J]. 东方法学，2022(1)：1-15.
[2] 颜新华. 网络安全视阈下的数据合规：基本理论、问题审视与中国方案[C] // 上海市法学会.《上海法学研究》集刊（2021年第1卷总第49卷）——上海市法学会国家安全法治研究小组文集. 上海：上海市法学会，2021.
[3] 若英. 什么是网络主权？[J]. 红旗文稿，2014(13)：39.
[4] 王春晖.《网络安全法》六大法律制度解析[J]. 南京邮电大学学报（自然科学版），2017，37(1)：1-13.
[5] 陈兵，胡珍. 数字经济下统筹数据安全与发展的法治路径[J]. 长白学刊，2021(5)：2，84-93.