

前言

在中华民族伟大复兴战略全局、世界百年未有之大变局与信息革命时代潮流发生历史性交汇的当下，《中华人民共和国数据安全法》（下称“《**数据安全法**》”）与《中华人民共和国个人信息保护法》（下称“《**个人信息保护法**》”）的先后落地施行与《中华人民共和国网络安全法》（下称“《**网络安全法**》”）共同构建了中国网络空间治理的顶层设计，引领着我国网络法治建设迈上新台阶，并在“总体国家安全观”指引下日臻完善。在持续推进网络法治的科学立法，监管工具日渐转型优化的同时，国家网信部门有序加强对地方网信部门工作指导以及对有关主管部门的统筹协调，持续加大网络安全与数据合规等领域的网络执法力度，彰显了中国网络法治工作合力，为网络法治建设注入了坚实的发展基础的同时，也为全球互联网发展治理贡献了中国智慧和方案。

回望2023年的网络安全与数据合规实践，我们全面拥抱和步入网络安全与数据合规2.0时代，网络安全与数据合规不断激活、产生数据价值，带动了新一轮以生成式人工智能服务为代表的人工智能技术发展，而以数据驱动为基础的智能产业又回归网络安全与数据合规的逻辑起点。在数字化尚未完全落地，智能化提前进场的复杂经济和社会变革阶段，为充分把握个体合法权益、企业数据价值利用以及国家数字经济有序发展之间的平衡之道，我们需要系统性地认识与理解中国网络空间治理的动态与趋势，心怀互联互通的远大宏景，秉持“合规创造价值”的理念，从而在中国网络法治体系的护航下从容应对数字社会的新变局，主动把握信息技术发展的新机遇。

正所谓“秉纲而目自张，执本而末自从”，本文旨在回顾2023年网络安全与数据合规领域重大进展与变化趋势，展望2024年网络安全与数据合规建设蓝图，以期共同开创数字经济发展新局面。

一、2023年网络安全与数据合规回顾

1. 网络法治全面铺开——网络领域立法日趋体系化，法律实施成为关键

2023年3月，国务院新闻办公室首次发布网络法治建设领域政府白皮书——《新时代的中国网络法治建设》，白皮书充分肯定了依法治网是全面依法治国和网络强国建设重要内容，回顾中国网络法治建设的历史性成就并总结我国网络法治建设经验，也为进一步做好网络法治工作指明了方向，对于企业把握我国网络法治建设态势，解构网络法治的系统性提出了重要的指引。

在科学立法方面，白皮书明确了我国基本形成以传统立法为基础，以网络内容建设与管理、网络全和信息化等网络专门立法为主干的网络法律体系，网络权益保障（主要涉及个人信息权益、未成年人网络保护等）、数字经济法治规则（主要涉及网络交易监管、数据竞争、算法规制等互联网经济新业态监管）、网络安全法律制度（主要涉及网络安全、关键信息基础设施安全、数据安全等）以及网络生态治理规范（主要涉及互联网信息服务、内容治理等）共同构成了中国网络空间法制基础，而未来网络立法的系统性、整体性、协同性、时效性也将不断增强，以期维护数字市场秩序，规范数字经济新业态新模式，并切实回应网络安全风险，提升我国网络法治治理能力。**对此，我们建议企业密切关注以上四大维度的国家法律规范、行业立法以及标准文件的出台动态，灵活调整与及时完善企业内部网络安全与数据合规管理机制，并加强与主管部门的标准共建、立法调研、研讨解读等工作。**

在严格执法方面，白皮书肯定了严格执法是依法治网的关键环节的同时，也强调了**网络执法的五大重点领域**：保障个人信息权益、保护网络知识产权、规范网络市场秩序、维护国家网络安全以及营造清朗网络空间。**以上领域始终是我国网络执法的重点，未来也将是我国网络法治常态化监管的主要方向。**

在公正司法方面，白皮书彰显了坚决打击网络违法犯罪活动的决心，提出了构建更为完善的网络司法规则，而强化公民网络民事权益司法保护与加大网络犯罪惩治力度也将相应成为网络空间司法保障的重点。

可见，我国已从整体性视角考虑和构建网络法治体系，推进常态化网络执法活动，加强网络空间司法保障，而企业网络安全与数据合规管理工作也因此相应需要构建全面性、整体性认识框架。对于企业经营而言，企业网络安全与数据合规工作不能仅满足于偶然性、应对性合规模式，而应该有效融入网络法律体系，按照网络安全、数据安全、个人信息保护的法律结构，调整完善企业治理结构，统筹企业合规设计，节约企业合规成本，创造企业合规价值。

2. 网络安全——网络安全法律制度纵深发展，网络安全保障义务不容忽视

(1) 网络安全服务认证进入实施阶段

2023年3月，国家市场监管总局、国家网信办、工业和信息化部（下称“**工信部**”）、公安部联合发布《关于开展网络安全服务认证工作的实施意见》（下称“**《实施意见》**”），规定了网络安全服务认证机构的资质要求及其开展安全服务认证等安全服务的合规要求，新增工信部为网络安全服

务认证工作的监管部门之一，形成了由市场监管部门统筹，网信部门、工业和信息化部门、公安部门依据各自职责开展网络安全服务监督管理的统分协作的监管工作机制。而认证规则和认证标志由市场监管总局征求中央网信办、工业和信息化部、公安部意见后另行制定发布。据此，《实施意见》已从国家层面初步明确了开展网络安全服务认证工作的主要要求，与此前公安部第三研究所公布的“全国网络安全等级测评与检测评估机构目录，均为国家统一推行的网络安全服务认证工作提供了实践指引，以期提升网络安全服务机构能力水平和服务质量。

在法律合规走向纵深之际，技术合规相应要求也陆续落地，“技术合规+法律合规”双管齐下，对于企业构建更高水平的网络安全合规体系起到了重要的作用。正如《实践意见》所言“鼓励网络运营者等广泛采信网络安全服务认证结果”，网络安全认证、检测和风险评估等安全服务是企业开展网络运营活动过程中履行网络安全保障义务的重要自证合规材料之一，**在采购网络安全服务的过程中，建议作为网络运营者的企业采购通过网络安全服务认证的认证机构所提供的网络安全服务**，从而为企业内部网络安全管理机制提供可信的安全评估支持。

(2) 网络关键设备和网络安全专用产品目录更新

国家网信办等五部门于2023年4月联合发布的《关于调整网络安全专用产品安全管理有关事项的公告》的要求，提出了网络安全专用产品检测认证领域建立统一制度。为推动安全认证和安全检测结果互认，2023年7月，《计算机信息系统安全专用产品销售许可证》开始停发，信息安全产品强制性认证的相关公告及通知停止执行，而国家网信办、工信部、公安部、国家认证认可监督管理委员会则更新了《网络关键设备和网络安全专用产品目录》，并相应废止了《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017年第1号）中的网络关键设备和网络安全专用产品目录，其中未对网络关键设备进行调整，但对网络安全专用产品目录进行了全面更新。

根据《网络安全法》的相关要求，**列入签署目录的网络关键设备与网络安全专用产品在销售或提供前**应注意按照《GB 40050-2021 网络关键设备安全通用要求》《GB 42250-2022 信息安全技术 网络安全专用产品安全技术要求》等国家标准的强制性要求，由《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）》中列明的机构安全认证合格或者安全检测符合要求。与此同时，**对于采购网络产品和服务的关键信息基础设施运营者**也应当重视并关注《网络关键设备和网络安全专用产品目录》，以降低和管控适用网络产品和服务可能带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险，产品和服务安全性，供应渠道的有效性，以及相关产品和服务提供者遵守中国法律、行政法规、部门规章情况等国家安全风险因素。

(3) 网络安全事件报告制度流程即将确定

2023年12月8日，国家网信办向社会公开征求对《网络安全事件报告管理办法（征求意见稿）》（下称“**《管理办法》**”）的意见，从报告主体、监管部门、触发机制、报告时限、报告内容、法律责任和尽职免责等方面对网络安全事件的报告机制作出明确、具体的规定。（详见此前文章：[一笼烽火报平安——《网络安全事件报告管理办法（征求意见稿）》解读和实践挑战](#)）。

从触发机制而言，对于网络运营者来说，依法依规落实网络安全事件报告义务，需要准确理解网络安全事件的定义以及识别网络安全事件等级。《管理办法》确定了网络安全事件的定义，并通过《管理办法》附件2的《网络安全事件信息报告表》明确了网络安全事件的具体类型。同时，《管理办法》在其附件1《网络安全事件分级指南》（下称“**《分级指南》**”）主要从“网络和信息系
统是否处于正常运行的状态，以及安全事件造成系统或者业务的瘫痪程度或受影响范围”与“国家秘密信息、重要敏感信息、重要数据是否完整、保密、可用”两个维度明确了确定事件级别的判断标准与识别指引，同时也设置了用于参照衡量和判断的兜底情形。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/567043111146006040>