《网络安全法》首次修订要点解读

作者：杨迅 | 李依然 | 郑学易

2025 年 10 月 28 日，《全国人民代表大会常务委员会关于修改<中华人民共和国网络安全法>的决定》由第十四届全国人民代表大会常务委员会第十八次会议通过，并自 2026 年 1 月 1 日起施行。这是《网络安全法》这部我国网络安全领域的基础性立法自 2017 年 6 月 1 日实施以来的首次修订，旨在回应网络安全形势的新要求、新挑战。

本文将简要介绍《网络安全法》本次修订的主要变化。

一. 对人工智能的健康发展做出前瞻性规定

人工智能作为战略性技术，正引领新一轮科技革命和产业变革。特别是随着近年来，语言大模型、多模态大模型、人工智能体、具身智能等技术领域的突破性创新，人工智能正深刻改变人类的生产生活方式。但亦应注意的是，人工智能技术的快速发展也为国家安全、网络安全、社会治理等带来了新的机遇和挑战。

为了回应人工智能治理和促进发展的需要，修订后的《网络安全法》新增第 20 条规定“国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。”该条从宏观层面，明确了国家对人工智能的战略定位和发展方向，推动人工智能治理从局部监管转向系统性规制。

本条增订一方面为人工智能高速发展下的网络安全治理提出总体原则，另一方面也标志着我国的网络安全治理从单纯的安全保护到发展中求安全的进步。可见，今后的网络安全法制建设和执法中会有越来越多的人工智能方面的考虑。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

二. 强化法律之间的衔接

自《网络安全法》颁布以来，我国不断夯实网络空间法制基础，相继出台《数据安全法》、《个人信息保护法》等法律法规，以规范数据处理活动，保障数据安全，促进数据开发利用，保护个人信息权益。相关立法在《网络安全法》的基础上，进一步细化了数据处理以及个人信息保护的具体要求(例如，数据跨境传输等)以及罚则。

为了加强《网络安全法》与其他法律法规的衔接，修订后的《网络安全法》第 42 条新增第 2 款，规定"网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定"。该条将侵害个人信息权益、违规跨境传输数据等违法违规行为的罚则转致相应的法律法规，以统一法律责任逻辑，增强法律体系的协调性和一致性。

三. 新增违法销售或者提供网络关键设备、网络安全专用产品的法律责任

修订前的《网络安全法》在第 23 条提出了网络关键设备安全认证和安全检测制度，规定"网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供"。但是，修订前的《网络安全法》未就该条设立相应的罚则条款。

在网络安全领域，网络关键设备和网络安全专用产品(例如，防火墙等)承担着重要职责，为保证网络运行的可靠性和安全性提供支撑。自《网络安全法》实施以来，我国网络关键设备和网络安全专用产品的安全认证和安全检测制度不断完善，特别是 2023 年网信办、公安部、工信部、认监委等部委相继发布《关于调整网络安全专用产品安全管理有关事项的公告》、《网络关键设备和网络安全专用产品目录》，进一步落实了我国网络关键设备以及网络安全专用产品认证检测制度。

此次《网络安全法》的修订填补了"违法销售或者提供网络关键设备、网络安全专用产品的行为"相关罚则条款的空缺，修订后第 63 条规定"违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。"

我们提示相关产品的销售和提供企业注意排查产品的认证和检测情况，特别是具有外资背景的网络安全设备厂商或网络安全设备进口商，应当落实认证和检测要求，确保落入目录范畴内的网络安全设备已经完成相应的安全认证检测后方可提供或销售。

四. 完善网络安全处罚机制

本次修订回应了网络安全技术的发展，对法律责任章节进行系统性完善，一方面扩张了违法行为的处罚方式、数额、完善分级处罚机制；另一方面引入了部分从轻、从减和不予处罚的情况，从而构建了更加科学精细的法律责任框架。

1. 细化未履行网络安全保护义务的处罚机制，具体包括:

   (1) 调整了处罚方式和数额。例如，根据修订后的《网络安全法》第 61 条规定，对于未依法履行网络运行安全保护义务的网络运营者，基础处罚由“给予警告”变为“给予警告，可处以一万元以上五万元以下罚款”，若仍拒不改正或导致网络安全事故等后果的罚款上下限均提高五倍。对于关键信息基础设施运营者，基础处罚由“给予警告”变为“给予警告，可处五万元以上十万元以下罚款”。这标志着修订后的《网络安全法》取消了“首次警告”的原则，主管部门可以对违法行为直接罚款。

   (2) 新增了针对严重后果以及特别严重后果的加重处罚条款。修订后的《网络安全法》第 61 条第 3 款新增了对于“造成大量数据泄露、关键信息基础设施丧失局部功能”、“关键信息基础设施丧失主要功能等特别严重危害网络安全后果”的处罚条款，对于企业最高罚款可至 1000 万元，对于相关责任人员最高罚款可至 100 万元。

   (3) 扩张对个人的处罚范围。修订后的《网络安全法》第 61 条将对个人处罚的对象由“直接负责的主管人员”扩张至“直接负责的主管人员和其他直接责任人员”。据此，除主管人员以外的安全、技术等人员亦面临罚款风险。

2. 新增特定违法行为的处罚方式。例如对未履行实名制义务(修订后第 64 条)，违法开展网络安全认证、监测、风险评估以及违法发布系统漏洞(修订后第 65 条)的网络运营者新增关停应用程序(即 App)的处罚，以适应移动互联网的发展。

3. 加大内容安全处罚力度。修订后的《网络安全法》第 69 条对于未处置违法信息的网络运营者施以更高的罚款上下限，并新增关停应用程序的处罚。

4. 调整关键信息基础设施相关罚则。修订后的《网络安全法》第 67 条对关键信息基础设施运营者使用未经安全审查或者安全审查未通过的网络产品或者服务的相关罚则进行了调整，新增“责令限期改正、消除对国家安全的影响”的规定。

5. 新增从轻、从减和不予处罚的情形。修订后的《网络安全法》新增第 73 条，规定“违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚”。

6. 扩张制裁境外实体的情形。修订后的《网络安全法》第 77 条将对境外主体实施制裁、追究法律责任的情形从境外主体“从事危害中国关键信息基础设施安全的活动”扩张至“从事危害中国网络安全的活动”，进一步扩张了对外实施制裁的适用情形，拓宽我国在网络安全领域的政策工具箱。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野