《网络安全法》重磅修订：责任收紧、罚则升级与企业合规新纪元

作者：潘永建 | 朱晓阳 | 邓梓珊 | 李佳琪

引言

2025 年 10 月 28 日，《网络安全法》完成自 2017 年施行以来的首次重大修订，并将于 2026 年 1 月 1 日起施行。本次修订虽以“小切口”方式聚焦法律责任制度，但其变革深刻，对企业的合规实践提出了更高要求。以下是对本次修订要点的梳理与评析。

一. 修订概览与总体思路

本次修订主要遵循以下思路：一是坚持问题导向，重点强化网络安全法律责任，加大对违法行为的处罚力度；二是坚持体系化衔接，与《数据安全法》《个人信息保护法》《行政处罚法》等相关法律有机衔接；三是分类施策，科学设置网络运行安全、网络信息安全等不同类型违法行为的法律责任。

我们在 2017 年《网络安全法》条文基础上以修订模式具体体现了本次修订内容，请见后附(如需 PDF 版本请于公众号后台留言“网安法修订”获取，或直接与我们联系)，以下表格为修订内容总结：

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

修改领域	主要修改内容	法律影响
网络运行安全	区分一般与严重后果，大幅提高罚款额度，最高可达一千万元；新增对销售或提供不合规网络产品及服务的罚则。	确立了更为严格的网络安全保护义务标准，处罚威慑力显著增强。
网络信息安全	对未依法处置违法信息的行为，增设并提高了罚款额度，情节特别严重的可处二百万元以上一千万元以下罚款。	进一步压实了网络运营者在内容生态治理中的主体责任。
人工智能治理	新增纲领性条款，强调国家支持人工智能等关键技术研发与基础设施建设，同时完善人工智能伦理规范，加强风险监测评估和安全监管。	为人工智能的健康发展提供了初步的法律框架，标志着监管从局部转向系统。
重视 APP 监管	响应时代变化，将违反实名制、发布漏洞/病毒/网络攻击/侵入、发布/传输违法违规内容的处罚措施由“关停网站”拓展至“关停 APP”。	响应科技发展趋势与 APP 监管实践，从法律层面重申 APP 同样属于重点监管对象。
法律责任衔接	将侵害个人信息权益、违法向境外提供重要数据等行为的法律责任，指引适用《个人信息保护法》《数据安全法》 等规定。	构建了更加协同、有机的网络与数据监管法律体系，避免了重复立法。
处罚/制裁制度完善	引入行政处罚法的从轻、减轻或不予处罚情形；明确对境外危害我国网络安全的活动可采取冻结财产等必要制裁措施。	体现了过罚相当的原则；防范境外攻击范围不再限于关键信息基础设施，扩张了法律必要的域外威慑力。

除上述表格总结内容外，以下几点同样值得特别关注:

- **处罚力度空前，合规成本激增**：修订后《网络安全法》的罚款金额全面提升，不仅**提高罚款下限，上限也大幅提升至千万元级别**。这意味着网络安全合规不再仅是技术或管理问题，而已成为直接影响企业存续的核心法律风险。企业必须将合规投入视为保护自身价值的必要成本。
- **引入"双罚制"，问责到人**：多项罚则明确规定，在对单位处以罚款的同时，可以对**直接负责的主管人员和其他直接责任人员**处以罚款。这促使**企业高管乃至对应负责员工**均必须将网络安全合规提升至战略高度，视为个人的履职红线。
- **强化合规激励，构建动态体系**：修订案并非仅着重于严惩，同样也引入了《行政处罚法》中的**从轻、减轻及不予处罚**的条款。这实际上鼓励企业建立健全能够有效运行、并及时自我发现和纠正问题的内部合规体系。在监管调查中，一套完善且持续运行的合规机制将成为企业的有力抗辩或减免责任的依据之一。

二. 企业合规行动建议

当前，网络安全与数据合规领域的执法态势正呈现出前所未有的刚性。一方面，**处罚力度显著升级**，从迪奥案因数据出境违规、安全措施缺失等问题被行政处罚[1]，到虚构“女黑客”营销案中企业因虚假宣传被重罚 20 万元[2]，均强调我国监管部门对违法行为“零容忍”的立场。另一方面，**执法维度不断扩展**，既覆盖数据出境、个人信息告知同意等“对外”合规义务，也关注到了个人信息保护影响评估等内部合规管理行为，形成多维度监管闭环。因此面对明年起生效的新《网络安全法》，我们建议企业立即着手:

1. **开展合规差距审计:** 对照修订后《网络安全法》要求，全面梳理并评估企业在网络安全、数据保护及违法信息处置等方面的现行制度与操作流程；按照《个人信息保护合规审计管理办法》等法律规定定期完成个人信息保护合规审计，及时排查合规风险、查漏补缺。
2. **更新内部制度与协议:** 修订企业内部的网络安全管理制度、个人信息保护政策、数据分类分级指南等合规管理制度，并审视与供应商和合作伙伴的相关协议是否存在关键遗漏。
3. **加强组织保障与培训:** 确保法务、合规、技术与业务部门之间的顺畅沟通，建立特定事项能够直达决策层的汇报机制，并对全体员工进行定期合规培训和考核。
4. **建立并留存合规证据:** 建立企业网络安全、数据保护、个人信息合规记录制度或标准流程，注重要求员工在日常运营中及时生成和保存能够证明自身已履行网络安全保护义务的记录、日志和文件等书面存证，做到全程留痕，以备合规审计、监管调查等不时之需。

总而言之，本次修订标志着中国网络安全与数据合规监管进入了 "**严监管、高罚则、强衔接**" 的新阶段。对企业而言，被动应付监管要求的时代已经终结，主动将合规内化为企业文化和核心竞争力，才是新阶段下行稳致远的必然选择。

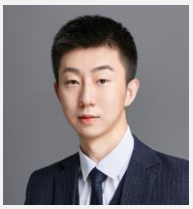
希望以上简评对您有所帮助。如果您在具体的合规落地方面有更细致的问题，欢迎与我们继续深入探讨。

[1] 国家网络安全通报中心：公安网安部门依法查处迪奥(上海)公司未依法履行个人信息保护义务案，发布于 2025 年 9 月 9 日，原文链接: https://mp.weixin.qq.com/s/0NZ852z1Jo7w4HkYiGJgVg?scene=1&click_id=203

[2] 公安部：整治网络虚假摆拍 维护企业合法权益，发布于 2025 年 10 月 27 日，原文链接: https://mp.weixin.qq.com/s/J-N7q4q3B4GobhvznTvwDQ

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com

邓梓珊
+86 21 6043 3793
susan.deng@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