技术防护措施引发的网页篡改、数据泄露事故时有发生，已对网络安全造成严重影响。

此次网络安全法修改虽未调整网络运营者的定义，但在义务主体层面，第六十一条第一款和第二款已经根据网络运营者的经营特征，通过区分一般网络运营者与关键信息基础设施（如公共通信、能源、交通、金融等领域的网络设施和信息系统）运营者的方式，提升了处置处罚精度。

同时，新修改的网络安全法尝试根据数据处理活动的风险等级以及违法行为造成后果的严重程度，构建起更具层次性的梯度处罚体系。以第六十九条为例，网络运营者对法律、行政法规禁止发布或者传输的信息未尽信息管理义务的，处罚标准在原来“一般违法”“拒不改正或者情节严重”两级的基础上，增加了“造成特别严重影响、特别严重后果的”情形，并设定了更高的处罚标准。此外，新修改的网络安全法还引入情节轻微情形下的豁免机制，首次明确应适用行政处罚法中“关于从轻、减轻或者不予处罚情形”的具体规定，就违反网络安全法的行为从轻、减轻或者不予处罚，以防止“小过重罚”。通过构建包容审慎、罚当其错的监管框架，网络安全法为主动消除或减轻危害后果、积极配合调查、认真整改的企业提供激励。

亮点4

加大监管力度实行“首违即罚”

加大监管力度，显著提高违法成本是此次网络安全法修改的亮点之一。其直指当前网络安全领域的核心风险，在提升罚款上限的同时，通过扩大规制范围提升网络安全法的威慑力。

提升罚款金额是最为直观的增加违法成本的方式。网络安全法第六十一条新增第三款，网络运营者及关键信息基础设施的运营者不履行特定网络安全保护义务，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成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，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。新修改的网络安全法不仅关注运营者自身责任，而且强调将责任传导到个人，大幅提升直接负责的主管人员和其他直接责任人员的经济责任。

同时，网络安全法确立了首违即罚制度。首违即罚制度的确立，突破了以往“责令改正”的前置程序，明确授权主管部门在首次发现违法行为时，就有权在责令改正、给予警告的同时，直接作出罚款决定。同时，通过差异化的罚款额度设置，将法律评价与行为风险等级挂钩，使关键信息设施运营者负有更高标准的网络安全保护义务。首违即罚制度的确立显著提高了违法行为的即时成本，网络安全保护不再是可被权衡、延后的“软约束”，而是一项具有明确、即时经济后果的“刚性法律要求”，从而将依法依规履行网络安全保护义务转化为必须计算的现实经营成本。

亮点5

对境外网络攻击将采取制裁措施

中国国家网络与信息安全信息通报中心去年发现了一批境外恶意网址和恶意IP，境外黑客组织利用这些网址和IP持续对我国和其他国家发起网络攻击，带来巨大安全风险。境外网络攻击不仅直接威胁国家安全，也危害公民个人权益。网络攻击突破安全屏障时，个人隐私便成为首当其冲的攻击目标，社交媒体、消费评价等社会活动及身份证号等敏感个人信息极易产生大规模泄露，引发隐私与财富的双重危机。

新修改的网络安全法第七十七条规定，境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。其中明确，网络安全法的适用范围由危害关键信息基础设施并造成严重后果，扩展为危害国家网络安全。通过取消受害对象以及损害后果严重性程度的双重限制，将所有来自境外的、危害国家网络安全的违法行为纳入网络安全法的管辖范围。换言之，只要境外主体实施了危害国家网络安全的活动，我国即可依法追究其相应责任，且不限于一般性法律责任，必要时，有关机关可针对性采取冻结财产或其他必要的制裁措施，在确保网络安全法前瞻性与灵活性的基础上，大幅提升对境外网络攻击的威慑力。

新修改的网络安全法第七十七条的直接规制对象虽是境外违法主体，但该条款社会效应的最终落点仍在于保护国内公众个人、企业和国家的切身利益，通过提供网络环境的“远端防护”，在网络疆域构建“法律防火墙”，从根本上保护数字资产、个人隐私以及社会运行安全。

编辑/李程（lcpupu@126.com）