

《网络安全法》修订中的内容调整与思路转变

王立梅

3月28日，国家互联网信息办公室（以下简称“网信办”）发布《中华人民共和国网络安全法（再次征求意见稿）》（以下简称“征求意见稿”），向社会公开征求意见。此次修订是继2022年首次征求意见后的重要调整，旨在强化网络安全法律责任体系、适应新技术发展需求，并实现与《数据安全法》《个人信息保护法》《产品质量法》《行政处罚法》等法律的有机衔接。以下将从核心内容调整、立法思路变化及立法建议三方面展开分析。

修正草案的核心内容调整

2025年修正草案在法律责任、关键信息基础设施（CII）保护、法律衔接机制、豁免规则等方面进行了全面深化，具体表现为以下五大方面：

1. 法律责任全面强化，处罚力度显著提高。

首先，针对严重危害网络安全的行为，“征求意见稿”提高了处罚力度，比如第五十九条规定，若关键信息基础设施运营者因安全漏洞导致“主要功能丧失”，罚款可达200万至1000万元，并可能吊销营业执照。

其次，新增禁止性条款。第六十一条明确禁止销售或提供未经安全认证的网络设备，违者除没收违法所得外，还需承担最高三倍违法所得的罚款，明确了服务提供者责任，填补了对服务提供者的处罚漏洞。

最后，增设责任主体。除了明确区分一般基础设施运营者与关键基础设施运营者的法律责任之外，“征求意见稿”还新增电子信息发送服务提供者、应用软件下载服务提供者的安全管理义务，并规定了处罚方式。

2. 明确关键基础设施运营者责任，细化违法情形分类。

一是明确关键信息基础设施运营者安全审查义务。第六十七条规定：关键信息基础设施的运营者违反本法第三十五条规定，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，由有关主管部门责令限期改正、消除对国家安全的的影响，并处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。关键基础设施运营者使用未经安全审查的网络产品或服务，处罚措施从“责令停止使用”调整为“限期改正+消除国家安全影响”，并处采购金额1-10倍罚款，直接责任人员最高可罚10万元。

二是细化违法情形分类。首次明确“局部功能丧失”与“主要功能丧失”的后果分级，细化了“情节特别严重”的具体情形，规定了造成关键信息基础设施丧失局部功能和主要功能两种主要情形，并分别给直接负责的主管人员及其他直接责任人员设定相应的处罚。

3. 引入豁免机制，实行政处罚裁量基准化。

“征求意见稿”明确了从轻、减轻或免罚情形。新增豁免机制，规定了若企业主动消除危害后果、违法行为轻微

- 当前“征求意见稿”虽规定了造成关键信息基础设施丧失局部功能和主要功能这两种主要情形，但对于上述这两种情形仍缺乏具体认定指标（如瘫痪时长、影响用户范围），仍有待相关的法律法规对此做出具体的认定。
- “征求意见稿”引入了豁免机制，但豁免条款中关于“危害后果轻微”“及时改正”等表述仍较为模糊，后续应出台相关法律法规或司法解释进一步细化“危害后果轻微”“及时改正”的边界与范围。
- 由于合规成本往往较高，中小企业难以承担。建议主管部门应发布针对不同规模企业的合规指引，并通过专项资金或培训计划支持中小微企业建立基础合规体系，避免“一刀切”执法。

且及时改正，或初次违法且后果轻微，可依法免于或减轻处罚。实现与《行政处罚法》第三十三条衔接，体现“过罚相当”原则。例如，数据泄露后及时补救并报告的企业可能免于处罚。新增第七十二条，网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。

此外，“征求意见稿”还要求制定裁量基准。新增第七十二条第二款，首次明确有关主管部门依据职责制定相应的行政处罚裁量基准，规范行使行政处罚裁量权，提高执法活动科学性，同时激励企业建立内部合规体系。

4. 细化分级分类监管，科学设置不同违法类型的法律责任。

“征求意见稿”实施分类监管模式。不同于对同类违法行为进行系统性整合，明确区分出一般的网络运营者和关键基础设施运营者的违法行为与责任，这一举措是“征求意见稿”对现行《网络安全法》的回应。

在处罚方面，“征求意见稿”严格遵循过罚相当原则，对违法情形进行了更为细致、具体的分级：（1）一般违法行为；（2）加重情节：拒不改正或危害网络安全等后果；（3）严重情形：造成大量数据泄露或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以及（4）特别严重情形：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。

5. 强化部门法之间的体系化与有机衔接。

“征求意见稿”转致适用其他法律法规的规定，既避免了重复立法、提升效率，又保持了法律体系内部逻辑的统一。例如，删除现行《网络安全法》中关于关键信息基础设施运营者的数据出境罚则，转而直接适用《数据安全法》。“征求意见稿”明确以下三种违法行为将转致适用其他法律法规的规定进行处罚：（1）发布或传输法律法规禁止发布或者传输的信息内容的；（2）侵害个人信息主体合法权利的；（3）关键信息基础设施运营者违法在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

此外，“征求意见稿”还合并了同类责任条款，将原分散的条款合并，简化责任体系，提升执法效率。例如，将第六十四条第一款、第六十六条、第七

十条合并为第七十一条，修改为：有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：（一）发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的；（二）违反本法第二十二第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的；（三）违反本法第三十七条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

立法思路的三大转变

“征求意见稿”体现了立法思路的三大转变：

首先是从“粗放式分类”转变为“精细化分类”。修正草案首次明确“局部功能丧失”与“主要功能丧失”的后果分级，细化了“征求意见稿”中“情节特别严重”的具体情形，规定了造成大量数据泄露、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这两种主要情形。在处罚方面，基于严格遵循过罚相当原则，对违法情形进行了更为细致、具体的分级：一般违法行为；加重情节；严重情形；特别严重情形。

第二大变化是从“碎片化治理”转变为“体系化衔接”。2025年“征求意见稿”更加注重与《数据安全法》《个人信息保护法》《行政处罚法》《产品质量法》等相关法律之间的有机协调。例如，个人信息保护责任直接转致适用《个人信息保护法》。此外，鉴于《数据安全法》对现行《网络安全法》第六十六条涉及重要数据违法行为的处罚作出了新的专门规定，明确转致适用的规定。同时，新增的豁免规则与《行政处罚法》第三十三条衔接，体现“过罚相当”原则。新增第六十一条规定了网络关键设备和网络安全专用产品的销售或者提供责任，填补了现行《网络安全法》对产品提供者的处罚漏洞，与《产品质量法》形成了衔接。

第三重转变体现为从“事后处罚”到“预防性合规监管”。一方面，2025年“征求意见稿”统筹考虑《网络安全法》和《行政处罚法》的适用关系，专门新增一条衔接规定，明确网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依法从轻、减轻或者不予处罚；另一方面，明确有关

主管部门依据职责制定相应的行政处罚裁量基准。通过豁免机制和裁量基准鼓励企业主动建立合规体系。根据具体案件中相关主体的过错程度来认定法律责任，防止处罚不当，为企业的创新、发展提供足够的激励与容错机制；也可以将执法资源聚焦于解决系统化、结构化的问题，提高网络安全领域执法工作的精细化与精准化。

完善修正草案的几点建议

相比于2022年“征求意见稿”，2025年“征求意见稿”在制度设计上已有显著进步，但仍存在以下配套法规中需要完善的空间：

首先，应明确“功能丧失”的认定标准。当前“征求意见稿”提出了“局部功能丧失”“主要功能丧失”等概念，进一步细化了此前“征求意见稿”中“情节特别严重”的具体情形，规定了造成关键信息基础设施丧失局部功能和主要功能这两种主要情形，但对于上述这两种情形仍缺乏具体认定指标（如瘫痪时长、影响用户范围），仍有待相关的法律法规对此做出具体的认定。可以尝试引入第三方专业机构参与认定，避免执法过程中因标准模糊导致的裁量权滥用，完善“局部功能丧失”与“主要功能丧失”的区分与认定标准。

其次，需细化豁免机制的适用条件。“征求意见稿”引入了豁免机制，规定了企业主动消除危害后果、违法行为轻微且及时改正，或初次违法且后果轻微，可依法免于或减轻处罚。但豁免条款中关于“危害后果轻微”“及时改正”等表述仍较为模糊，可能出现实践中执法不一的情形。后续应出台相关法律法规或司法解释进一步细化“危害后果轻微”“及时改正”的边界与范围。

再次，要加强中小企业合规支持。豁免机制虽为中小企业提供容错空间，但不同于大企业，由于合规成本往往较高，中小企业难以承担。建议主管部门应发布针对不同规模企业的合规指引，并通过专项资金或培训计划支持中小微企业建立基础合规体系，避免“一刀切”执法。

最后，应明确电子信息发送服务与应用下载服务提供者的责任边界。针对新增责任主体（如电子信息发送服务提供者、应用软件下载服务提供者），“征求意见稿”只设置处罚规定，但对于第六十九条第二款中“安全管理义务”并未作出明确规定。建议在配套法规中明确其安全管理义务的具体范围，明确明确电子信息发送服务与应用下载服务提供者的责任边界。

（作者系中国政法大学数据法治研究院教授、博导、电子证据研究中心主任，中国法学会网络与信息法学研究会副会长）



扫描左侧二维码关注