NEWSLETTER
LIFANG & PARTNERS 立方观评

No.48
2017.07

长按或扫描二维码
关注“立方律师事务所”
更多精彩内容

中国网络安全法律框架

【引言】

从“棱镜门”事件的曝光到勒索病毒“WannaCry”的全球肆虐，信息技术日新月异的发展带来了全球频发的网络安全问题。正如国际电信联盟 7 月 5 日发布的《2017 年全球网络安全指数》报告所述，“网络的互联性越高，意味着任何东西和所有东西都可能遭入侵，而从国家的重要基础设施到基本人权的一切，都可能被危及”。

虽然，中国作为网络大国还不是网络强国，在网络安全方面还面临着严峻挑战。但是，伴随着《中华人民共和国网络安全法》的颁布实施及其配套法规规章的相继制定发布，中国的网络安全立法和网络安全保障制度构建都在迅速推进，相信不久的将来，中国的互联网将更加安全、开放、便利并充满活力。

立方律师事务所在 TMT 领域有着卓越的业绩表现，并一直关注网络安全立法的发展动态。我们将通过本专题，对《网络安全法》颁布以来的一系列重要法规规章进行概述梳理，供大家参考。

【立法进程】

十八大以来，我国网络空间法制化开始全面推进。2016 年 11 月 7 日，全国人大常委会发布的《中华人民共和国网络安全法》，并于今年 6 月 1 日起生效。作为网络安全方面的上位法，《网络安全法》在两个大方面、四个小方面有重点的、分层次的对于网络中的核心问题进行了规范。两个大方面主要是信息和数据安全以及负责承载上述信息数据的设施安全。其中，信息和数据安全指网络中的个人信息和重要数据的保护、出境问题；承载设施的安全指网络关键设备、网络安全专用产品以及关键信息基础设施的保障。因此，在《网络安全法》的大框架下，相关主管部门相继出台了针对上述两个大方面的规范性文件，逐步建立起网络安全法的体系。

在信息与数据安全方面，2017 年 4 月 11 日国家互联网信息办公室发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》，该征求意见稿主要针对网络运营者将在中国境内运营过程中收集和产生的个人信息和重要数据向境外提供的情况。具体而言，征求意见稿定义了个人信息和重要数据，确定了安全评估的主体，列举了安全评估的内容以及不得出境的禁止性规定。值得一提的是，其明确规定了网络运营者应当报请行业主管或监管部门组织安全评估的具体情况，如数据量超过 1000GB 的，上述规定对企业进行安全评估和项目可行性评估具有重大的指导作用。

2017 年 5 月 27 日，国家信息安全标准化技术委员会发布了《关于开展国家标准 <信息安全技术数据出境安全评估指南（草案）>征求意见工作的通知》规定了评估流程和评估要点。其中评估流程为自评估启动、指定数据出境计划、评估数据出境计划的合法正当和风险可控、评估要点及方法、形成评估报告及检查修正。评估要点区分了个人信息和重要数据，二者应就信息或数据的类型和敏感程度、数量、范围、技术处理情况方面结合自身特点进行评估。

在设施安全方面，2017 年 2 月 4 日，国家互联网信息办公室发布了《关于<网络产品和服务安全审查办法（征求意见稿）>公开征求意见的通知》，主要用于提高网络产品和服务安全可控水平，防范供应链安全风险。

2017 年 6 月 1 日，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定发布了《网络关键设备和网络安全专用产品目录（第一批）》，要求列入目录的设备和产品，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，同时，检测结果需要认证上报。

2017 年 7 月 11 日，国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》，使关键信息基础设施的保护制度更加完善且更具可操作性。

附图：立法时间轴


2016年11月7日通过的《网络安全法》已于2017年6月1日起正式施行
《网络安全法》
国家互联网信息办公室2017年5月2日发布，自2017年6月1日正式实施
《网络产品和服务安全审查办法（试行）》
2017年6月1日，国家互联网信息办公室、工业和信息化部、公安部、中国国家认证认可监督管理委员会公告2017年第1号
《网络关键设备和网络安全专用产品目录（第一批）》
《国家网络安全检查操作指南》
中央网络安全和信息化领导小组办公室和国家安全协调局2016年6月发布
《个人信息和重要数据出境安全评估办法（征求意见稿）》
2017年4月11日，国家互联网信息办公室关于《个人信息和重要数据出境安全评估办法（征求意见稿）》公开征求意见的通知
《信息安全技术 数据出境安全评估指南（草案）》征求意见稿
2017年5月27日，全国信息安全标准化技术委员会关于开展国家标准《信息安全技术 数据出境安全评估指南（草案）》征求意见工作的通知
《关键信息基础设施安全保护条例（征求意见稿）》
2017年7月11日，国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知

【重要规章文件解读】

《个人信息和重要数据出境安全评估办法（征求意见稿）》解读

2017 年 4 月 11 日，国家互联网信息办公室发布了关于《个人信息和重要数据出境安全评估办法（征求意见稿）》公开征求意见的通知，以期进一步明确在中国境内收集和产生的个人信息和重要数据的出境问题。下文将结合现有法律法规，以该专项征求意见稿为主线，解读我国关于个人信息与重要数据跨境传输的新规定。

一、现有涉及信息或数据跨境传输问题的法律法规

在《个人信息和重要数据出境安全评估办法（征求意见稿）》（简称“征求意见稿”）发布前，涉及信息或数据的跨境传输问题的法律法规主要包括《中华人民共和国网络安全法》（简称《网络安全法》）、《中华人民共和国反恐怖主义法》（简称《反恐怖主义法》）、《人口健康信息管理办法（试行）》、《人类遗传资源管理条例（科技部送审稿）》（尚未生效）、《人类遗传资源管理暂行办法》，但上述文件多为对信息或数据跨境传输的概括性规定，鲜少详细解答企业在信息跨境传输中应当如何判断信息能否出境这一问题。

《网络安全法》

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

《反恐怖主义法》

第十九条第二款 对互联网上跨境传输的含有恐怖主义、极端主义内容的信息，电信主管部门应当采取技术措施，阻断传播。

《人口健康信息管理办法（试行）》

第十条第二款 不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。

《人类遗传资源管理条例（科技部送审稿）》

第十五条第二款 将我国境内采集的人类遗传信息资源提交给境外机构或者以任何形式开放使用前，应当先向国务院科学技术行政部门指定的机构提交。

《人类遗传资源管理暂行办法》

第十七条 我国境内的人类遗传资源信息，包括重要遗传家系和特定地区遗传资源及其数据、资料、样本等，我国研究开发机构享有专属持有权，未经许可，不得向其他单位转让。获得上述信息的外方合作单位和个人未经许可不得公开、发表、申请专利或以其他形式向他人披露。

通过上述涉及不同领域或行业的法律规定可以看出，我国对于特定领域的重要信息或数据、涉及国家安全的信息或数据以及特殊的敏感数据等倾向于境内存储，如因特殊原因需要传输出境的，需要有关部门进行审核。但是，以上规定仅为一般性规定，境内外企业无从得知企业自身在信息或数据跨境传输中负有何种义务，同时相应的监管部门又承担了怎样的职责。因此，突破行业之间的隔阂，制定一项适用于所有网络经营者的信息或数据跨境传输的管理办法十分必要。

二、《个人信息和重要数据出境安全评估办法（征求意见稿）》的适用

《个人信息和重要数据出境安全评估办法（征求意见稿）》作为《国家安全法》、《网络安全法》中关于个人信息和数据管理规定的细化操作办法，明确企业应当对待出境的信息或数据进行安全评估，对于跨境贸易中的网络运营者的信息传输行为具有指导作用。

1 适用范围

征求意见稿用于规范网络运营者向位于境外的机构、组织、个人提供在中华人民共和国境内运营中收集和产生的个人信息和重要数据的行为。

其中，网络运营者指网络的所有者、管理者和网络服务提供者；个人信息指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等；重要数据则是指与国家安全、经济发展，以及社会公共利益密切相关的数据。重要数据的具体范围在征求意见稿中并未做出详细规定，仅表明可参照国家有关标准和重要数据识别指南。从事跨境交易的国内外企业可密切关注各行业及相关部门出具的有关重要数据的标准或指南。

2 主管及监管部门

征求意见稿将负责安全评估的部门分为两个层次：总体上，由国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估；涉及具体行业，则由行业主管或监管部门负责本行业数据出境安全评估工作，并定期组织开展本行业数据出境安全检查。

根据现有经验，各行业的主管或监管部门可能出具相应的规章制度用以规范行业内的信

息管理。例如，国家卫生计生委针对印发了《人口健康信息管理办法（试行）》，其中涉及人口健康信息在境外存储问题；交通运输部门印发了关于《民航网络信息安全管理规定（暂行）（征求意见稿）》，包含了个人信息和重要数据应在境内存储的规定；农业部印发了《关于加快推进“互联网+农业政务服务”工作方案》的通知；中国银监会办公厅对各银监局、机关部门下发了《关于加快推进“互联网+政务服务”工作的实施意见》，上述文件中均涉及对重要数据的规范内容，其发文单位及文件中所涉部门将来可能作为具体行业的监管部门负责对个人信息和重要数据进行安全评估。

3 评估方式及标准

根据征求意见稿的规定，安全评估分为网络运营者自行组织安全评估及行业主管或监管部门组织安全评估两种。一般情况下，企业可自行对出境数据进行安全评估，并对评估结果负责。但如果出境数据存在以下情况之一的，网络运营者则应报请行业主管或监管部门组织安全评估：

（一）含有或累计含有 50 万人以上的个人信息；

（二）数据量超过 1000GB；

（三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；

（四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；

（五）关键信息基础设施运营者向境外提供个人信息和重要数据；

（六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

行业主管或监管部门不明确的，由国家网信部门组织评估。

由行业主管或监管部门组织安全评估的数据可能涉及敏感信息或较为重要的信息。上述条款包含了五项具体规定和一项兜底条款，因此行业主管或监管部门可能基于该兜底条款对行业内的出境信息或数据的安全评估享有一定的“自由裁量权”。

五项具体规定中，前三项均提供了具体的判断数据或例证，判断起来较为容易。第四项和第五项所涉及的关键信息基础设施是近年来新出现的热点问题。就目前立法情况而言《网络安全法》、《国家网络空间安全战略》（国家互联网信息办公室于 2016 年 12 月 27 日发布）中均提及关键信息基础设施，但并未给出详细的定义和例证。目前，关于关键信息基础设施最为详细的规定是国家互联网信息办公室 7 月 11 日公布的《关键信息基础设施安全保护条例（征求意见稿）》（详见后文）。

4 评估内容

评估主要涉及以下内容：

（一）数据出境的必要性；

（二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；

（三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；

（四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

（五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

（六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；

（七）其他需要评估的重要事项。

其中，有关数据出境的必要性、个人信息的情况、个人信息主体是否同意出境、数据被毁损等风险方面，网络经营者可根据跨境交易、合作项目等的具体内容作出判断。但就信息或数据的敏感程度、对于国家安全或社会公共利益的潜在风险，主管或监管部门的评估结果对于信息或数据能否出境具有决定作用。

5 评估结果

通过安全评估，一部分数据可能并不具备出境的条件。征集意见稿第十一条为禁止性规定，即存在以下情况之一的，数据不得出境：

（一）个人信息出境未经个人信息主体同意，或可能侵害个人利益；

（二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；

（三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

总体而言，《个人信息和重要数据出境安全评估办法（征求意见稿）》的发布为《网络安全法》等法律法规的实施提供了细化的规定，使网络经营者在从事相关数据跨境业务时明确了具体的操作方法，是我国逐步完善信息管理整体制度中的重要一环。

----文/李纯 立方知识产权诉讼部律师

《数据出境安全评估指南(草案 》解读

2017 年 6 月 1 日正式实施的《网络安全法》首次规定了数据出境的安全评估制度。以此为立法基础，国家网信办于 2017 年 4 月 11 日制定并公布了《个人信息和重要数据出境安全评估办法（征求意见稿 》，构建了个人信息和重要数据出境安全评估的基本框架，规定了自行评估和监管机构评估两种评估方式以及安全评估的内容。2017 年 5 月 27 日，全国信息安全标准化技术委员会发布了《关于开展国家标准《信息安全技术数据出境安全评估指南（草案 》》征求意见工作的通知》，《信息安全技术数据出境安全评估指南》（简称“评估指南”）又进一步明确了数据出境安全评估流程、评估要点、评估方法等内容。

一、适用范围

《评估指南》适用于网络运营者开展的个人信息和重要数据出境安全评估工作，也适用于行业主管或监管部门对网络运营者开展个人信息和重要数据出境安全评估进行的指导、监督等工作。网信部门、行业主管或监管部门依职权开展的个人信息和重要数据出境安全评估，也可参考该标准。

二、"重要数据"

《评估指南》中对于“重要数据”的概念进行了明确，重要数据是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成严重后果的数据。

《评估指南》列举了石油天然气、煤炭、石化、电力等 27 个行业（领域）以及其他相关行业（领域），指出各行业（领域）主管部门结合实际，明确本行业（领域）重要数据定义、范围或判定依据，并根据行业（领域）发展变化，及时更新或替换指南中相关内容。

三、评估流程

《评估指南》从自评估启动、制定数据出境计划、评估数据出境计划的合法正当和风险可控、评估要点及方法、评估报告、检查修正六个方面对流程进行了规范。

1、自评估启动

网络运营者应在如下情况启动自评估：

a）产品或服务涉及向境外机构、组织或个人提供数据的；

b）已完成数据出境安全评估的产品或业务所涉及的数据出境，在目的、范围、类型、数量等方面发生较大变化、数据接收方变更或发生重大安全事件的。

2、制定数据出境计划

网络运营者应首先制定数据出境计划，计划的内容包括但不限于：

a) 数据出境目的、范围、类型、规模；

b) 涉及的信息系统；

c) 中转国家和地区（如存在）；

d) 数据接收方及其所在的国家或地区的基本情况；

e) 安全控制措施等。

3、评估数据出境计划的合法正当和风险可控

数据出境安全评估首先评估数据出境计划的合法性和正当性 ;数据出境活动不具有合法性和正当性，不得出境。在此基础上再评估数据出境计划是否风险可控，有效避免数据出境及再转移后被泄露、损毁、篡改、滥用等风险。

4、评估要点及方法

《评估指南》对评估要点和评估方法单独作了详细介绍，内容见下文。

5、评估报告

网络运营者在完成对数据出境计划的评估后，应形成评估报告，评估报告应至少保存 5 年。

6、检查修正

如数据出境计划不满足合法正当要求，或经评估后不满足风险可控的要求，网络运营者可修正数据出境计划，或采用相关措施降低数据出境风险，并重新开展自评估。

四、评估要点

评估要点包括合法正当和风险可控两方面。

1、合法正当

数据出境计划应同时满足合法性和正当性的要求：

a) 合法性包括：

1） 不属于法律法规明令禁止的；

2） 符合我国政府与其他国家、地区签署的关于数据出境条约、协议的；

3） 个人信息主体已授权同意的，危及公民生命财产安全的紧急情况除外；

4） 不属于国家网信部门、公安部门、安全部门等有关部门依法认定不能出境的。

b) 正当性包括：

1） 网络运营者在合法的经营范围内从事正常业务活动所必需的；

2） 履行合同义务所必需的；

3） 履行我国法律义务要求的；

4） 司法协助需要的；

5） 其他维护网络空间主权和国家安全、社会公共利益、保护公民合法利益需要的。

2、风险可控

评估数据出境计划的风险可控，应综合考虑出境数据的属性和数据出境发生安全事件的可能性。其中个人信息属性评估要点包括个人信息的类型、敏感程度、数量、范围和技术处理情况。重要数据的属性，包括数量、范围、类型和技术处理情况等。指南在个人信息和重要数据出境范围上，提出了“最小化原则”，包含：（1）出境与功能直接关联；（2）最低频率；（3）最低数量。

数据出境发生安全事件的可能性主要评估：（1）发送方数据出境的技术和管理能力（包括内部的安全管理制度、应急预案等）；（2）数据接收方的安全保护能力、采取的措施（包括主体审查、人员能力等）；（3）数据接收方所在国家或区域的政治法律环境（包括立法状况、司法机制等）。

五、评估方法

《个人信息和重要数据出境安全风险评估方法》（附录 B）按照相关数据信息的数量、范围、类型等因素，分别将个人信息出境对个人权益产生的影响、重要数据出境对国家安全、社会公共利益产生的影响、安全事件的可能性、安全风险综合评估划分为高、中、低等影响。

综合来说，《信息安全技术数据出境安全评估指南（草案）》的发布是在《网络安全法》正式生效背景下对其中一些规定提供了细化的指南，将为网络经营者从事相关数据出境业务明确具体的操作方法，对保护国家安全、社会公共利益、个人隐私安全具有重要意义。目前《评估办法》和《评估指南》都在征求意见阶段，还未正式出台，我们会持续关注的同时，建议相关企业尤其是网络经营者应当对自身情况进行初步判定，提前准备企业内部的相关规章制度，加强信息数据的风险防控。

----文/立方网络安全法研究小组

《关键信息基础设施安全保护条例（征求意见稿）》解读

2017 年 6 月 1 日起实施的《网络安全法》将“关键信息基础设施（CII）”纳入了法律保护的范畴，并进行了一些系列的立法探索。7 月 11 日，国家互联网信息办公室公布备受瞩目的《关键信息基础设施安全保护条例（征求意见稿）》，揭开了中国关键信息基础设施安全保护立法进程的新篇章。

一、CII 相关的立法背景及进程

关键信息基础设施在国内立法中属于一个新概念，自 2016 年以来开始频繁出现在法律、法规以及政策性文件中，提出此概念旨在通过建设关键信息基础设施保护制度提高国家的网络安全和自主保障能力。

目前，我国发布的与 CII 相关的法律法规及文件列举如下（按发文时间先后排序）：

- 《中华人民共和国国家安全法》（下称《国家安全法》），主席令第二十九号，2015 年 7 月 1 日发布并生效；
- 《中华人民共和国经济和社会发展第十三个五年规划纲要》（下称《十三五规划纲要》），全国人民代表大会于 2016 年 3 月 16 日发文，同日生效；
- 《国家网络安全检查操作指南》（下称《操作指南》），中央网络安全和信息化领导小组办公室、网络安全协调局于 2016 年 6 月联合发文；
- 《中华人民共和国网络安全法》（下称《网络安全法》），主席令第五十三号，2016 年 11 月 7 日发布，2017 年 6 月 1 日生效；
- 《国务院关于印发“十三五”国家信息化规划的通知》（下称《“十三五”国家信息化规划的通知》），国务院于 2016 年 12 月 15 日发文，同日生效；
- 《国家网络空间安全战略》，国家互联网信息办公司于 2016 年 12 月 27 日发文，同日生效；
- 《关键信息基础设施安全保护条例（征求意见稿）》（下称《保护条例》），国家互联网办公室于 2017 年 7 月 1 日发文。

CII 的概念被正式提出后，从事互联网业务、大数据、云计算等涉及数据传输和网络安全领域的企业开始密切关注立法动态，尤其是立法中可能涉及的如下三方面的问题：第一，相关服务及产品是否可能被认定为关键信息基础设施；第二，如被认定为关键信息基础设施，相关服务及产品的具体监管主体和监管方式有哪些；第三，如违反有关关键信息基础设施的法律规定，企业可能承担怎样的法律责任。在 2017 年 7 月 1 日发布《保护条例》之前，上

述问题尚处于模糊地带，企业在评估其业务是否存在被监管的法律风险时也表现出无所适从。《保护条例》的发布恰逢其时，对于上述问题做出了较为清晰的规定，促进了关键信息基础设施保护制度的建立。

二、CII 相关的核心问题

1. CII 的认定

相关业务是否涉及关键信息基础设施应当依据法律法规中关于关键信息基础设施的定义及范围进行判断。《保护条例》出台前，不同法律文件中对于 CII 的定义存在一定差别，也引发了实务操作中的争议。《保护条例》提供了更为具体、易识别的定义，对 CII 的范围进行了规定。根据该条例第十八条的规定，关键信息基础设施指网络设施和信息系统，具体涉及的单位包括：

（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；

（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

（四）广播电台、电视台、通讯社等新闻单位；

（五）其他重点单位。

属于上述领域的单位可依据《操作指南》中确定关键信息基础设施的三个步骤对于相应的业务性质进行判断。需要指出的是，虽然某些单位包含在上述规定的范围内，但其从事的具体业务可能并不涉及关键信息基础设施。例如，医疗卫生行业虽然是国家的重点行业，但并非此行业的所有业务均被认为与关键信息基础设施相关。就医院运营而言，患者的电子病历系统、急救中心运行系统显然直接关系到患者是否能够及时、有效的接受相应治疗，属于医院运行的核心部分。但如果仅仅是为医院某特殊疾病提供的临床试验系统，其是否应当归于关键信息基础设施则需要具体识别。对于此类难以认定的网络设施或信息系统，《保护条例》规定“国家网信部门会同国务院电信主管部门、公安部门等制定关键信息基础设施识别指南”，用以识别各行业、领域的关键信息基础设施。

2. CII 的监管

2.1 监管主体

根据《保护条例》的相关规定，CII 的监管主体可分为两层，国家监管和行业监管。总体上，国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门在各自职责范围内负责相关网络安全保护和监督管理工作。行业内，国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。国家行业主管或监管部门设立或明确专门负责本行业、本领域关键信息基础设施安全保护工作的机构和人员，编制并组织实施本行业、本领域的网络安全规划等。

2.2 监管方式

国家行业主管或监管部门的监管方式可总结为日常监管和抽查检测。日常监管包括制定相关的制度文件、接受有关人员举报、报备等。此外，国家行业主管或监管部门会定期组织对本行业、本领域关键信息基础设施的安全风险以及运营者履行安全保护义务的情况进行抽查检测，可能采取如下几种措施：

（一）要求运营者相关人员就检测评估事项作出说明；

（二）查阅、调取、复制与安全保护有关的文档、记录；

（三）查看网络安全管理制度制订、落实情况以及网络安全技术措施规划、建设、运行情况；

（四）利用检测工具或委托网络安全服务机构进行技术检测；

（五）经运营者同意的其他必要方式。

3. 法律责任

关键信息基础设施的运营者、个人、有关部门及工作人员三类主体如违反《保护条例》的规定，则应承担相应的行政责任和刑事责任。具体而言，运营者违反网络安全保护义务、境外存储数据的禁止性规定及违规使用未经安全审查或未通过安全审查的网络产品或服务的，应当承担相应的行政责任，并且对直接负责的主管人员或其他责任人员处以相应的罚款。个人如从事危害关键信息基础设施的活动或行为，如攻击、侵入、干扰、破坏关键信息基础设施，则可能承担行政或刑事责任。有关部门或工作人员如存在滥用职权等违法行为的，对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

《关键信息基础设施安全保护条例（征求意见稿）》的颁布使我国关键信息基础设施保护制度更加完善，有关关键信息基础设施的立法正在向着规范清晰、可操作性强的方向发展。同时，《保护条例》中提及的关键信息基础设施识别指南、关键信息基础设施安全监测评估文件及各行业、各领域的网络安全时间应急预案等后续相关法律法规的出台同样值得期待。

----文/立方网络安全法研究小组

【结语】

纵观我国近期围绕网络安全问题的一系列立法活动，在加强网络监管的同时也对网络运营者的责任与义务提出了新的挑战。作为企业既要认真领会《网络安全法》等既有法律法规及规范性文件，对自己进行风险自测；又要密切关注它们实施后的后续动态，如相关配套措施的出台，避免因忽略或误读带来的合规风险。

立方律师事务所编写《立方观评》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

有关我所详细介绍请登录网站 http://www.lifanglaw.com，或请联系我们：

北京：北京市东四十条甲 22 号南新仓商务大厦 A1105 室（100007）

电话：+86 10 64096099

传真：+86 10 64096260

广州：广州市天河区珠江新城珠江东路 16 号高德置地广场 G 座 3806

电话：+86 20 85561566/85561660/38898535

传真：+86 20 38690070

武汉：湖北省武汉市武昌区中北路 171 号汉街总部国际 c 座 1002 室

电话：+86 27 87301677

传真：+86 27 86652877

首尔：首尔市钟路区新门内路 92 OFFICIA 大厦 1416 号

电话：+0082 02 69590780

传真：+0082 02 21799332

联系邮箱：**info@lifanglaw.com**