环球律师事务所
GLOBAL LAW OFFICE

2016 年 11 月 11 日

环球法律专递
Global Legal Updates

《中华人民共和国网络安全法》之关键信息基础设施重点保护制度要点解读

作者：刘斯佳

单位：环球律师事务所

2016 年 11 月 7 日，全国人民代表大会常务委员会表决通过了《中华人民共和国网络安全法》（下称“**《网络安全法》**”）。现如今，不仅是互联网企业，很多传统行业的企业也会通过网络开展相关业务活动或提供服务。因此，《网络安全法》的颁布，引起了社会各界的广泛关注。

《网络安全法》就保护网络安全这一主旨，主要通过以下三个制度对网络服务提供者【1】的相关义务和责任作出了规范：（1）网络安全等级保护制度；（2）用户信息保护制度；和（3）关键信息基础设施重点保护制度（下称“**关键设施制度**”）。其中，关键设施制度最为受关注，主要原因在于这个概念系首次出现在我国的法律法规中，并对网络服务提供者设定了较高的法定义务和限制。

因此，本文拟就《网络安全法》下的关键设施制度的关键内容作出解读，以期帮助可能受此影响的企业，特别是通过网络提供服务的企业更好地了解《网络安全法》的相关规定，并就关键问题可能存在的解决方案进行初步探讨。但因为关键设施制度与其他两个制度存在交叉关系，故本文以下将先就三个制度分别做简要的概述，再对关键设施制度作重点解读。

一、网络安全等级保护制度

环球律师事务所
GLOBAL LAW OFFICE

虽然网络安全等级保护制度是第一次出现在我国的法律法规中，但类似的概念并非首次提出。早在 1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》（下称“**《信保条例》**”【2】）中，就明确规定计算机信息系统（根据定义，计算机信息系统包含网络【3】）实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。2007 年，公安部等 4 部委联合制定了《信息安全等级保护管理办法》（下称“**《信息保护办法》**”），就信息安全等级保护制度（包括信息安全产品的使用）作出了具体的规范。【4】

虽然在《网络安全法》中没有明确指出《网络安全法》下的网络安全等级保护制度是否就是《信保条例》和《信息保护办法》下的信息安全等级保护制度或直接参照《信保条例》和《信息保护办法》的规定实施，但鉴于《网络安全法》的相关配套规定尚未出台，且《网络安全法》本身在此问题上也不具有很大的操作性，就目前情况而言，若网络服务提供者在经营活动中按照《网络安全法》的字面规定，以及按照现行的《信保条例》和《信息保护办法》及相关法律法规和技术要求等规范的规定来履行其网络安全等级保护义务的，我们认为是比较合规的。进一步说，在《网络安全法》的相关配套规定出来以及相关主管部门对《网络安全法》作出具体解释之前，《网络安全法》对于网络服务提供者在网络安全等级保护制度下所增加的法定义务并不是很多。

我们建议，相关网络服务提供者应依照现行的法律法规和部门规章对自身业务的合规性进行严格核查，并随时关注相关主管部门对《网络安全法》的解读，以及后续出台的配套规定，以及现行的法律法规和部门规章可能因此所进行的修订。

二、用户信息保护制度

类似于网络安全等级保护制度，用户信息保护制度也并非首次出现在我国的法律法规中。在《网络安全法》颁布之前，已经有多部法律法规或部门规章从不同层级及针对不同业务模式，对用户个人信息的保护作出了相应的规定。具体的规定包括但不限于《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《中华人民共和国消费者权益保护法》【5】、《电信和互联网用户个人信息保护规定》和《规范互联网信息服务市场秩序若干规定》。

综合前述各项法律法规的规定，网络服务提供者在通过网络提供服务的过程中收集、使用用户个人信息的，应当遵循合法、正当、必要的原则，明示收集、使用

环球律师事务所
GLOBAL LAW OFFICE

信息的目的、方式和范围，并经用户同意；且不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的。用户个人信息是指互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等的信息。

因此，类似于网络安全等级保护制度，就目前情况而言，《网络安全法》对于网络服务提供者在用户信息保护制度下所增加的法定义务并不是很多。如果网络服务提供者在经营活动中能够按照《网络安全法》的字面规定，以及现行的与用户个人信息保护相关的法律法规和部门规章的要求来履行其个人信息保护义务的，我们认为是比较合规的。但是，相关企业仍需随时关注相关主管部门对《网络安全法》的解读，以及后续出台的配套规定。

三、关键信息基础设施重点保护制度

如前所述，《网络安全法》下的关键设施制度是一个比较新的内容，也是最受关注的一个方面。

根据《网络安全法》第 31 条和 37 条的规定，关键设施制度与网络安全等级保护制度和用户信息保护制度存在一定的交叉关系，即关键信息基础设施（下称“**关键设施**”）中的网络，除适用一般的网络安全等级保护制度之外，国家对其实施重点保护；同时，关键设施在中国境内运营中收集和产生的个人信息（还包括重要数据），除应按照用户信息保护制度进行保护之外，还应当确保该等内容在境内存储，如果需要向境外提供的，应符合另行制定的法规的相应规定。

之所以关键设施制度备受关注，除了这个概念是首次出现在我国的法律法规中以及对网络服务提供者设定了较高的法定义务和限制外，还在于《网络安全法》中规定关键设施制度下主要内容的法律条款只有两条，且明确指出相关的配套规定将由国务院和相关主管部门另行制定。因此，很多企业都对自己是否会落入《网络安全法》下的关键设施制度的适用范围感到疑惑甚至不安。为此，笔者下文将从文义解读和现行的法律法规及规范性文件的规定这两方面，试图就关键设施可能涵盖的范围进行探讨。

(一) 文义解读

《网络安全法》第 31 条对于关键设施的范围作了如下规定：国家对公共通信和信息服务、能源、交通、水利、金融、公共服

环球律师事务所
GLOBAL LAW OFFICE

务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键设施，在网络安全等级保护制度的基础上，实行重点保护。关键设施的具体范围和安全保护办法由国务院制定。

《网络安全法》以举例方式列明了8个适用关键设施制度的行业和领域，并以设定一般原则的方式作了一个类似兜底条款的规定。此外，《网络安全法》第31条还将关键设施的具体范围和安全保护办法授权由国务院制定。

先不考虑国务院另行制定的关于关键设施的具体范围这一因素，仅从《网络安全法》第31条的文本内容来看，似乎只要网络运营者所处行业和领域是列举的8个行业和领域之一的，将会自动被适用关键设施制度。但是，实践中如何认定相关网络服务提供者所处的行业和领域可能是一个比较困难的问题。就以《网络安全法》第31条中的信息服务举例来说，各个行业的企业（如医疗机构、制造业企业或电子商务企业）都有可能在主营业务以外从事信息服务业务。那么，在该等情形下，即网络服务提供者本身所处的行业不是信息服务行业，但其开展的部分业务为信息服务，那么该等网络服务提供者是否应自动被适用关键设施制度，目前并不很确定。

另一方面，《网络安全法》草案的一次审议稿、二次审议稿和《网络安全法》对于关键设施的具体范围的描述也是三易其稿。相比《网络安全法》，一次审议稿分5大类对关键设施的范围进行了描述，并作了相关列举：（1）基础信息网络（如公共通信和广播电视传输等）；（2）重要行业和公共服务领域（如能源、交通和医疗卫生等）；（3）军事网络；（4）政务网络（设区的市级以上国家机关）；和（5）用户数量众多的网络。而二次审议稿和《网络安全法》相比，只是少了8个列举的行业和领域，其仅以一般原则的方式对关键设施的范围作了规定。《网络安全法》订制过程中对关键设施的范围规定，从分5大类并举例，到只有一般认定原则，再到列举8个行业和领域并设置一般认定原则，似乎表明立法者对明确需被适用关键设施制度的行业范围的认定，从较大确定，到很不确定，到最后相对确定。特别是，《网络安全法》所列明的行业和领域相比二次审议稿中列举的内容，减少了医疗卫生这个行业，这是否意味着立法者最终并不想将关键设施制度适用范围扩展到医疗卫生这一行业中？我们认为也不排除这种可能

环球律师事务所
GLOBAL LAW OFFICE

性，【6】虽然立法者的本意也可能是认为医疗卫生行业应当被包含在公共服务这个大行业中。

综上，仅从《网络安全法》的文义解读方面，我们很难就关键设施制度所适用的范围作出一个较精确的预判。但是，除了需要等待国务院以及其他相关主管部门作出配套规定来明确相关问题以外，我们也可以通过现行的法律法规以及部门规范性文件中已有的规定，试图对此作出更深的解读。

(二) 现有规定及可能的解决方案

前面提到了关键设施制度是一个比较新的内容，系首次出现在我国的法律法规。但是，一次审议稿在 2015 年 7 月便向社会公开征求意见。虽然那个时候《网络安全法》尚处于审议阶段，但关键设施制度已被明确提出。在《网络安全法》于 2016 年 11 月最终被表决通过前，关键设施制度这一概念就已被相关主管部门运用到相关的规范性文件中。

在相关主管部门颁布的《网络安全检查操作指南》【7】（下称“**《安全指南》**”）中，其明确提及了“关键信息基础设施”。根据《安全指南》的相关内容，颁布《安全指南》的目的在于指导相关政府主管部门的关键设施网络安全检查工作。在《安全指南》的“确定关键信息基础设施步骤”这一章节里，其提供了一个表格，以供关政府主管部门在确定关键设施时作参考。

表格就关键设施的认定，列举了 14 大行业：（1）能源；（2）金融；（3）交通；（4）水利；（5）医疗卫生；（6）环境保护；（7）工业制造（原材料、装备、消费品、电子制造）；（8）市政；（9）电信与互联网；（10）广播电视；（11）教育；（12）新闻网站；（13）商业平台；（14）政府部门。其中，能源又细分为电力、石油石化和煤炭；交通又细分为铁路、民航、公路和水运。除此之外，该表格又进一步对不同的行业列举了“关键业务”，如电力包括：电力生产（含火电、水电、核电等）、电力传输和电力配送；公路包括：公路交通管控和智能交通系统（一卡通、ETC 收费等）；医疗卫生包括：医院等卫生机构运行、疾病控制和急救中心运行；电信与互联网包括：语音、数据、互联网基础网络及枢纽、域名解析服务和国家顶级域注册管理和数据中心/云服务。此外其他的关键业务就不在此一一列举了。

从中我们可以看到，就某一特定行业而言，并非所有的业务都会被视为与关键设

环球律师事务所
GLOBAL LAW OFFICE

施制度直接相关。以医疗卫生行业为例，该表格列举了三个关键业务，即医院等卫生机构运行、疾病控制和急救中心运行。也就是说，一个医疗机构除此以外的其他业务（如医患沟通交流平台）可能不会被视为关键业务，进而可能无需适用关键设施制度。进一步地说，按照此表格的内容，特别是“关键业务”这一用语，似乎意味着就某一网络服务提供者而言，即使其因为其本身的行业原因被适用关键设施制度，也并不意味着其所有网络【8】（包括其中的个人信息和重要数据）都适用关键设施制度。这一推论也可以从现行的法律法规中找到一定的支撑。

根据《通信网络安全防护管理办法》（下称“**《网络防护办法》**”）第7条的规定，“通信网络运行单位应当对本单位已正式投入运行的通信网络进行单元划分，并按照各通信网络单元遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度，由低到高分别划分为一级、二级、三级、四级、五级。电信管理机构应当组织专家对通信网络单元的分级情况进行评审。通信网络运行单位应当根据实际情况适时调整通信网络单元的划分和级别，并按照前款规定进行评审。”【9】《网络防护办法》第8条和第9条还规定通信网络运行单位应当在通信网络定级评审通过后向电信管理机构备案，备案时应当提交的信息主要包括：通信网络单元的名称、级别和主要功能；通信网络单元责任单位的名称和联系方式；通信网络单元主要负责人的姓名和联系方式；通信网络单元的拓扑架构、网络边界、主要软硬件及型号和关键设施位置。《网络防护办法》第11条和第12条进一步规定，三级及三级以上通信网络单元应当每年进行一次符合性评测和安全风险评估；二级通信网络单元应当每两年进行一次符合性评测和安全风险评估。

综合上述内容我们可以看出，就某一网络服务提供者的网络而言，不仅其具体的业务单元可以进行单独的划分并分别管理，相关主管部门对此也是根据其级别适用不同的规定。因此，我们不排除在《网络安全法》以及配套规定下，某一适用关键设施制度行业的网络服务提供者，其部分网络也可以不适用关键设施制度。以医疗卫生领域为例，如果一个医疗机构有两个域名并分别通过不同的网络提供服务，一个域名下提供的是关键业务（如卫生机构运行、疾病控制或急救中心运行），另一个域名下提供的是非关键业务（如医患沟通交流平台），则非关键业务下涉及的域名及对应的网络和相关设施，可能不会因为该医疗机构本身被归入医疗卫生领域就一定被适用关键设施制度。

环球律师事务所
GLOBAL LAW OFFICE

《安全指南》中规定，除了通过关键业务对关键设施的范围进行判定外，还要综合其他因素进行判定，比如是否属于重点新闻网站、日均访问人次、发生网络安全事故可能造成的影响的范围和程度等。限于篇幅原因，本文就不在此一一具体阐述了。

四、总结

《网络安全法》是我国第一部就网络安全方面进行总体规范的法律。其不仅将之前分散在各个法律法规或部门规章中的相关或类似规则进行了整体规范，还将该等规则上升到了人大常委会所制定的法律的层面。这表明了我国政府维护我国网络安全的力度在不断增强。因此，即使《网络安全法》下的部分规则或原则已可在现行的法律法规或部门规章中找到相关或类似的规定，与此相关的网络服务提供者仍需要对《网络安全法》高度重视，因为相关主管部门可能会因《网络安全法》的颁布对现行的相关法律法规或部门规章作出更为严格的解释，或在实践操作中作出更加严格的管理。除此之外，我们还是建议相关的网络服务提供者应随时关注《网络安全法》及配套规定的出台以及相关主管部门的态度和实践操作。

《网络安全法》将于 2017 年 6 月 1 日起施行。在此期间内，各网络服务提供者可以就自身的业务合规性进行普查，并对相关业务进行相应的梳理。同时，网络服务提供者应及时地根据《网络安全法》后续的相关配套规定对自己的业务进行调整，以期在《网络安全法》实施后能够在完全合规的基础上，顺利地开展各项业务。

尾注

【1】根据《网络安全法》的规定，网络运营者作为《网络安全法》下的主要责任主体之一，承担相关的责任和义务。又根据《网络安全法》第 76 条的规定，网络运营者包括网络的所有者、管理者和网络服务提供者。但是，《网络安全法》并未对网络服务提供者作出进一步解释。虽然如此，结合《网络安全法》第 10 条的规定，即“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性”，以及我们的实践经验，我们认为网络服务提供者可以被进一步地理解为或至少应当包括通过网络提供服务的主体。

环球律师事务所
GLOBAL LAW OFFICE

【2】《信保条例》于 2011 年被修订，计算机信息系统安全等级保护制度继续沿用执行。

【3】《信保条例》第 2 条：本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

【4】相关的法律法规还包括：《互联网安全保护技术措施规定》和《计算机信息系统安全专用产品检测和销售许可证管理办法》等。

【5】《中华人民共和国消费者权益保护法》第 29 条：经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。 经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。 经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

【6】《网络安全法》相比二次审议稿，还删除了供电、供水、供气等行业，但我们认为该等行业可以被能源等其他更大范围的行业所包含。

【7】我们在中共洛南县委宣传部 2016 年 8 月发布的关于开展关键信息基础设施网络安全检查的通知的附件中找到了《安全指南》。同时鉴于我们在其他政府官网上找了中央网络安全和信息化领导小组办公室于 2015 年 7 月制定的《国家网络安全检查操作指南》，以及其他相关信息，我们认为《安全指南》可能也是由中央网络安全和信息化领导小组办公室制定的。

【8】《网络安全法》第 76 条将网络定义为：指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

【9】通信网络运行单位定义参见《网络防护办法》第 2 条：中华人民共和国境内的电信业务经营者和互联网域名服务提供者（以下统称“通信网络运行单位”）管理和运行的公用通信网和互联网（以下统称“通信网络”）的网络安全防护工作，适用本办法。

环球律师事务所
GLOBAL LAW OFFICE

刘斯佳为环球律师事务所上海办公室的律师，其执业领域主要涵盖医药和健康领域的投资、并购和合规，以及私募股权投资/风险投资和日常公司业务。

邮箱: sijialiu@glo.com.cn

微信号：globallawoffice