《网络安全法》解读

《中华人民共和国网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定。由全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行。

一、相关概念

为了统一术语，《网络安全法》给出了相关概念。

**（一）网络**

网络是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收集、存储、传输、交换、处理的系统。

**（二）网络安全**

网络安全是指通过采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

从这个概念来讲，网络安全包括传统的网络安全、数据安全，是范围更大的网络安全，更加侧网络运行安全、信息安全。

**（三）网络运营者**

网络运营者是指网络的所有者、管理者和网络服务提供者。

网络运营者是网络安全法中非常重要的概念，是关键义务主体或者核心义务主体。如几大电信运营商、BAT等企业以及国家机关中的网络执法部门都属于网络运营者的范畴。同时，关键信息基础设施也是一种网络运营者。

《网络安全法》去掉了草案中关于“包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等”的规定，可能考虑到在互联网飞速发展的现今，对于“网络运营者”这一概念只规定内涵而对其外延采用开发的描述方式，似乎是一种更聪明也是更合乎时宜的做法，需要注意的是，是否被认定为“网路运营者”主要取决于企业是否成为了网络信息系统的所有者和管理者，以及企业的业务是否提供了各类网络服务，特别是互联网信息服务。

**（四）网络数据**

网络数据是指通过网络收集、存储、传输、处理和产生的各种电子数据。

**（五）个人信息**

个人信息是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、身份证号码、个人生物识别信息、住址、电话号码等。

从定义中可以看出，网络安全法中个人信息多则重自然人的信息，对虚拟人的信息如用户、密码、IP、MAC、上网时间、Cookies等信息还没有明确定义。个人信息不同于个人数据、个人隐私，自然人的健康、犯罪、私人等活动信息，网络安全法中并没有提到。

**（六）关键信息基础设施**

国家需要对公共通信和信息服务、能源、交通、水利、金融、公共服务、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、公共利益的关键信息基础设施进行保护。

《网络空间安全战略》中进一步明确，公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统（如阿里巴巴、腾讯、百度）等14个大行业领域属于国家关键信息基础设施。

《关键信息基础设施安全保护条例（征求意见稿）》中对关键信息基础设施范围进行了更具体的界定。下列单位运行、管理的网络设施和信息系统，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、公共利益等，应当纳入关键信息基础设施保护范围：

1.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、共用事业等行业领域的单位；

2.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；

3.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；

4.广播电台、电视台、通讯社等新闻单位；

5.其他重点单位。

二、法律框架

《网络安全法》全文共七章七十九条，包括总则、网络安全支持与促进、网络运行安全、网络信息安全、检测预警与应急处置、法律责任以及附件。从主体对象角度，可将各条款分为10大类。

**（一）网络安全法的目的和范围**

第一条：网络安全法的目的

第二条：网络安全法的管辖权

**（二）国家角度**

第三条：网络安全法的原则、方针、现实路径。

第四条：解决顶层设计问题。

第五条：国家采取多种手段保护网络安全风险和威胁，解决行业力量不足问题。

第六条：构建网络安全的良好环境。

第七条：网络空调治理的国际合作态度。

第八条：赋予国际相关部门网络安全的监督职责。

第十二条：国家保护公民、法人和其他组织依法使用网络的权利，同时履行义务。

第十三条：未成年人保护。

第十四条：白虎举报人的合法权益。

第十五条：国家强化标准体系建设。

第十六条：国家加大投入，解决投入不足问题。

第十七条：建设网络安全社会化服务体系。

第十八条：鼓励和支持创新。

第十九条：网络安全宣传教育。

第二十条：促进网络安全人才培养。

**（三）网络用户角度**

第十一条：行业组织规范和自律。

第十二条：权利和义务。

第十四条：有权对网络安全违法行为进行举报。

第二十六条：开展安全认证、检测、风险评估，发布的网络安全信息应遵守国家规定。

第二十七条：违法网络安全的范围定义。

第二十九条：情报交换和风险评估。

第四十六条：严禁网络犯罪。

**（四）网络运营者角度**

第九条：遵纪守法、履行义务、接受监督、承担责任。

第二十一条：实现网络安全等级保护制度。

第二十四条：实名制要求、网络身份认证，贯彻落实真实身份的用户服务。

第二十五条：网络安全事件的应急处置和报告。

第二十八条：提供合法的侦查协助。

第四十条：建立用户信息保护制度。

第四十一条：强化个人信息保护，收集使用个人信息要合法、正当、必要。

第四十二条：个人信息保护责任，不得泄露、篡改、销毁。

第四十三条：要合理合法支持个人删除权和更正权。

第四十四条：不得窃取、非法获取、非法出售个人信息。

第四十七条：具有违法信息传播的阻断义务。

第四十九条：建立投诉、举报制度。

第五十六条：较大安全风险或者安全事件约谈。

**（五）关键信息基础设施的运营者角度**

第三十一条：定义，落实国家等级保护制度，突出保护重点。

第三十二条：工作规划、实施安全保护工作。

第三十三条：建设三同步原则。

第三十四条：关键信息基础设施运营者的义务。

第三十五条：网络产品和服务的采购，应通过国家安全审查。

第三十六条：采购网络产品和服务，应签订保密协议。

第三十七条：个人信息和重要数据应境内存储。

第三十八条：每年至少一次风险评估。

**（六）网络产品和服务提供者角度**

第十条：网络安全和数据安全的要求。

第十六条：加大投入、知识产权保护、支持国家网络安全技术创新项目。

第十七条：支持网络安全认证、检测和风险评估等安全服务。

第十八条：网络数据保护和利用、公共数据资源开发、网络安全管理方式的创新。

第二十一条：网络安全等级保护制度。

第二十二条：产品服务的强制性准入要求和义务。

第二十三条：网络关键设备和网络安全专业产品的强制性认证或检测。

第三十五条：网络产品和服务需要通过国家安全审查。

第三十六条：产品和服务的保密协议。

第三十七条：境外数据传输需要进行安全评估。

第三十八条：开展风险检测评估工作。

第四十八条：电子信息发送和应用软件下载的安全。

**（七）国家网信部门角度**

第八条：统筹协调网络安全工作和相关监督管理工作。

第十四条：具有对危害网络安全行为举报的处置权利。

第二十三条：主导安全专用产品目录、安全认证、安全检查工作。

第三十条：赋予获取维护网络安全的各种信息的权利。

第三十五条：主导国家安全审查。

第三十七条：主导数据境外传输的安全评估工作。

第三十九条：统筹协调关键信息基础设施的安全风险检查、安全应急演练、网络安全信息共享。

第五十条：违规违法信息的处置、阻断的权利。

第五十一条：统筹协调网络安全监测预警和信息通报工作。

第五十三条：协调简历网络安全风险评估、应急工作。

第七十三条：对第十三条的约束、权利约束。

**（八）有关部门角度**

第八条：赋予网络安全保护和监督管理职责和权利。

第十四条：保护举报人的合法权益。

第十五条：组织制定产品、服务和运行安全的国家标准、行业标准等。

第十九条：组织、指导、督促网络安全宣传教育。

第二十三条：制定、公布安全产品目录、开展安全认证和安全监测工作。

第三十条：赋予获取维护网络安全的各种信息的权利。

第三十五条：在网信络协同下开展国家安全审查。

第三十七条：在网信络协同下开展安全评估。

第三十九条：对网络运营者依法实施监督检查。

第四十九条：对网络运营者依法实施监督检查。

第五十条：违规违法信息的处置、阻断的权利。

第五十一条：建立网络安全监测预警与信息通报制度。

第五十三条：建立网络安全风险评估、应急工作机制。

第五十四条：开展网络安全风险监测和评估。

第五十六条：省级以上人民政府有关部门可以启动安全时间约谈。

第六十九条：违反有关部门要求，可以进行处罚。

第七十三条：对三十条的约束、权利约束。

**（九）公安部门角度**

第八条：赋予网络安全保护和监督管理权利。

第十四条：举报处置权利。

第二十八条：侦查协助制度。

第六十三条：第二十七条网络犯罪的处罚权利。

第六十四条：第四十四条个人信息违法的处罚权利。

第六十七条：第四十六条违法网站、通信群组、违法信息发布违法的处罚权利。

第六十九条：不提供侦查协助单位的处罚。

第七十四条：境外违法的制裁措施。

**（十）个人信息角度**

第二十二条：个人信息收集必须明示并取得用户同意，并遵守相关法律法规。

第三十七条：个人享有信息的数据主权。

第四十一条：个人信息的使用和收集必须合法、正当、必要。

第四十二条：不得泄露、篡改、销毁其收集的个人信息。

第四十三条：个人具有信息的删除权和更正权。

第四十四条：严禁个人信息的非法获取、非法出售和提供。

第四十五条：安全监管部门必须对个人信息进行保密。

第六十四条：违反个人信息的处罚。