网络安全法解读

目 录

CONTENTS

01

法律要点

一、概述

目标

- 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、法人和其他组织合法权益，促进经济社会信息化健康发展

范围

- 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

总览

- 法律条文：共7章，79条
- 2016年11月7日发布
- 2017年6月1日起施行

一、概述

➢ 法律体系

《网络安全法》构成我国网络空间安全管理的基本法律，与《国家安全法》、《反恐怖主义法》、《刑法》、《保密法》、《治安管理处罚法》、《关于加强网络信息保护的决定》、《关于维护互联网安全的决定》、《计算机信息系统安全保护条例》、《互联网信息服务管理办法》等现行法律法规共同构成中国关于网络安全管理的法律系统。

➢ 配套法规

国务院及相关的部门会制定和颁布一系列的配套法律法规，比如网络安全等级保护制度、关键信息基础设施的认定和保护办法、数据跨境传输的安全评估办法、网络产品和服务的国家安全审查制度等，数量上可能会达十余部。

一、概述

➢ 法律适用与管辖

在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

➢ 域外管辖

《网络安全法》采取了有限的域外管辖原则，依照法七十五条，境外的主体实施入侵或攻击境内关键信息基础设施的活动，造成严重后果的，依法追究法律责任，且中国执法机关可实施财产冻结等制裁措施，这是为应对日益严重的全球网络安全威胁的需要。

二、总则

➢ 目标

◆ 保障网络安全，维护网络空间主权和国家安全、公共利益，保护合法权益....

➢ 国家职责

◆ 网络安全与信息化发展并重

◆ 制定、完善网络安全战略

◆ 监测、防御、初置网络安全风险及威胁

◆ 倡导诚实守信、健康文明的网络行为

◆ 积极推进国际交流与合作

◆ 国家网信部门负责统筹协调，国务院电信主管部门、公安部门等各司其职

二、总则

➢ 网络运营者职责

- ◆ 遵守法律、行政法规，履行网络安全保护义务
- ◆ 接受政府和社会的监督，承担社会责任。
- ◆ 保障网络安全、稳定运行，维护网络数据的完整性、保密性和可用性。

➢ 行业组织职责

- ◆ 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

三、网络运行安全

➢ 网络安全等级保护制度

第二十一条规定，国家实行网络安全等级保护制度。安全保护义务包括：

1）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

2）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

3）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

4）采取数据分类、重要数据备份和加密等措施；

5）法律、行政法规规定的其他义务。

➢ 解读

信息系统安全等级保护制度已实施多年，网络安全等级保护制度应当会与目前的信息系统安全等级保护制度相衔接和融合，而不会成为两个并行的制度体系。

三、网络运行安全

➢ 网络产品和服务

- ◆ 符合相关国家标准的强制性要求
- ◆ 不得设置恶意程序
- ◆ 发现存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
- ◆ 持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。
- ◆ 用户信息和个人信息合规

➢ 网络关键设备和网络安全专用产品

- ◆ 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。
- ◆ 国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

三、网络运行安全

➢ 网络实名制

◆ 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

◆ 国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

三、网络运行安全

➢ 关键信息基础设施范围

“国家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…实行重点保护”。国务院另行制定关键信息基础设施的具体范围和安全保护办法。

➢ 法律义务

关键信息基础设施运营者将会承担相应的网络安全保护法定义务：

1）建设要求：业务运行稳定可靠，安全技术措施同步规划、同步建设、同步使用；

2）安全保护：专门安全管理机构和安全管理负责人；安全教育、培训、考核；

容灾备份；应急预案、定期演练

3）安全审查：采购网络产品和服务，应当通过国家安全审查

4）保密要求：签订安全保密协议，明确安全和保密义务与责任

5）境内存储：个人信息和重要数据应当在境内存储

➢ 法律义务

6）检测评估：每年至少进行一次检测评估，报送检测评估情况和改进措施。

7）统筹协调：国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

四、网络信息安全—数据保护

- **数据保护范围**：个人信息保护、用户信息保护和商业秘密保护。
- **用户信息**： 引入了“用户信息”的概念，可以理解为在用户使用产品或服务过程中收集的信息构成用户信息，包括IP地址、用户名和密码、上网时间、Cookie信息等。
- **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。
- **商业秘密**：是指不为公众所知悉、能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。

四、网络信息安全—数据保护

➢ 用户信息保护要点

- ◆ 收集：网络产品、服务具有收集用户信息功能的，其提供者应当向用户**明示并取得同意**；
- ◆ 保护：网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

➢ 商业秘密保护要点

- ◆ 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

四、网络信息安全—数据保护

- **个人信息保护**：与以往法律法规相比，增加了删除权和更正权：
  - 应当遵守本法和**有关法律、行政法规**的规定。《**电信和互联网用户个人信息保护规定**》
  - 收集、使用个人信息：应当遵循**合法、正当、必要**的原则，公开收集、**使用规则**，明示收集、使用信息的目的、方式和范围，并经被收集者**同意**。
  - 不得泄露、篡改、毁损其收集的个人信息：1）采取技术措施和其他必要措施保护；2）若泄漏，立即采取补救措施，告知用户并向有关主管部门报告。
  - 未经被收集者同意，不得向他人提供个人信息。**但是，经过处理无法识别特定个人且不能复原的除外。--利好“大数据发展”**
  - 个人信息主体拥有**删除权**（保护使用不当）和**更正权**（有误）
  - 不得非法获取、窃取，不得非法出售、非法向他人提供
  - **管理部门**不得泄露履行职责中知悉的个人信息

四、网络信息安全—数据本地化

➢ 数据本地化

- ◆ 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，应当进行安全评估；法律、行政法规另有规定的，依照其规定。

➢ 其它规定

- ◆ 下列数据在其它法律里有本地化要求：国家秘密和国家安全数据、征信数据、个人金融信息、地图数据、网络出版服务所需的必要的技术设备、网约车相关数据和信息。

四、网络信息安全—网络行为

➢ 网络行为要求

◆ 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

五、监测预警与应急处理

➢ 国家及主管部门

- ◆ 建立网络安全监测预警和信息通报制度。按照规定**统一发布网络安全监测预警信息**
- ◆ 关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的**网络安全监测预警和信息通报制度**，并按照规定报送网络安全监测预警信息
- ◆ 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件**应急预案，并定期组织演练**
- ◆ 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害：**检测、评估、预警、补救措施**
- ◆ 发生网络安全事件，应当立即**启动网络安全事件应急预案**，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息

五、监测预警与应急处理

➢ 国家及有关部门

- ◆ 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行**约谈**。
- ◆ 因**网络安全事件，发生突发事件或者生产安全事故**的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。
- ◆ 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对**网络通信采取限制等临时措施**。

➢ 网络运营者

- ◆ 存在较大安全风险或发生安全事件：网络运营者应当按照要求**采取措施**，进行**整改，消除隐患**。

六、法律责任

➢ 行政处罚

- ◆ 责令改正、警告、罚款，
- ◆ 责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员等进行罚款等；
- ◆ 有关机关还可以把违法行为记录到信用档案。
- ◆ 对于“非法入侵”等，法律还建立了职业禁入的制度。

➢ 民事责任

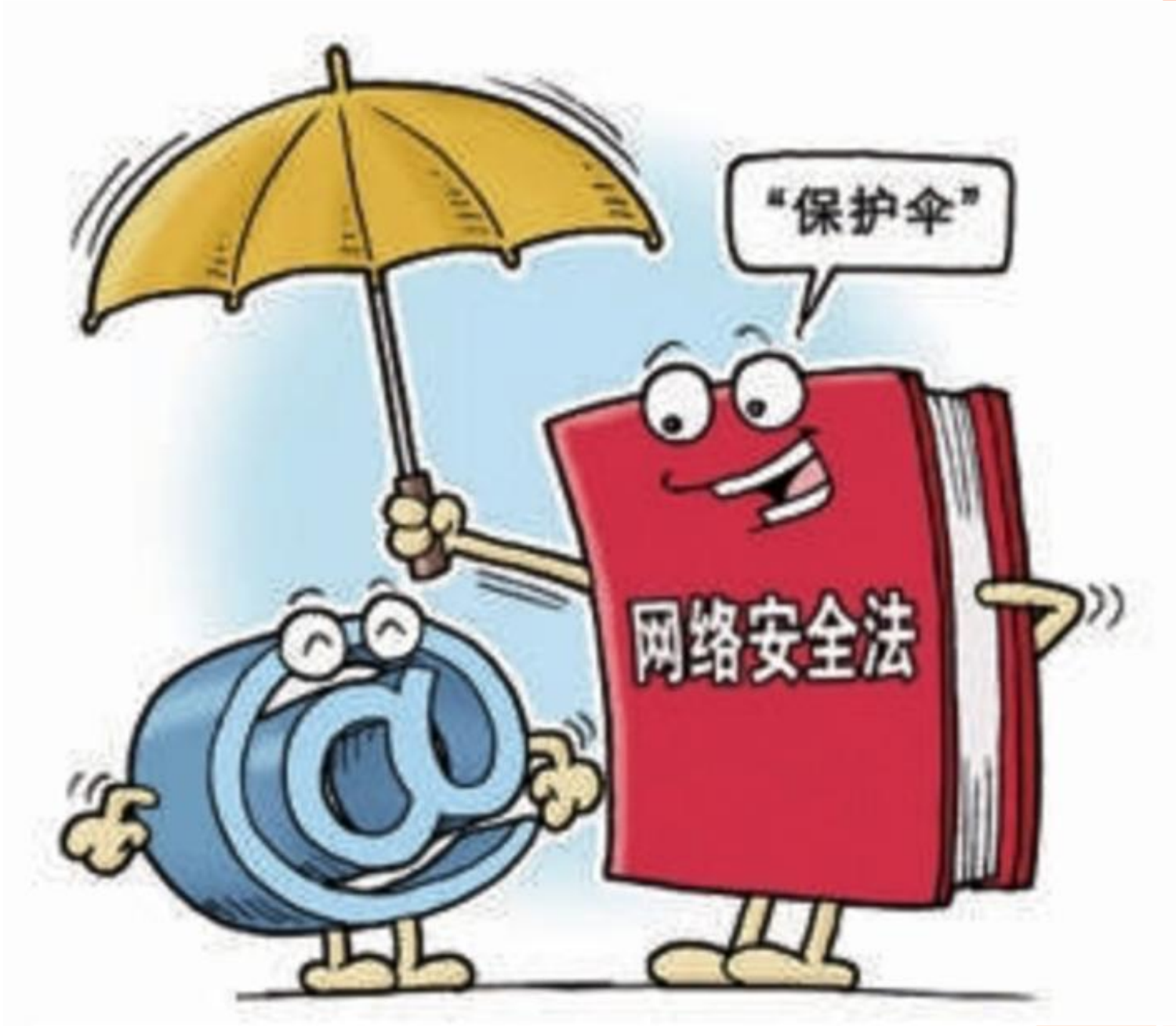
- ◆ 违法《网络安全法》的行为给他人造成损失的，网络运营者应当承担相应的民事责任。

➢ 治安管理处罚/刑事责任

- ◆ 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

02

守法要点



守法要点

➢ 网络运营者法律合规要求

需要网络运营者建立企业的管理制度和操作规程，以满足法律合规性的要求，避免法律风险，主要包括如下：

1）与实施网络安全等级保护制度相关的义务和制度建设，包括制定内部安全管理制度和操作规程，确定网络安全负责人等（第二十一条）；

2）健全用户信息保护制度（第二十二条和第四十条）；

3）落实网络实名制（第二十四条）；

4）网络安全事件应急预案（第二十五条）；

5）关键信息基础设施的安全保护义务，包括：设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；定期对从业人员进行网络安全教育、技术培训和技能考核；对重要系统和数据库进行容灾备份；制定网络安全事件应急预案，并定期进行演练；法律、行政法规规定的其他义务（第三十四条）；

守法要点

➢ 网络运营者法律合规要求

6）采购关键信息基础设施产品和服务的保密制度（第三十六条）；

7）关键信息基础设施安全性的年度评估（第三十六条）；

8）个人信息的收集和利用规则及制度（第四十一条和第四十二条）；

9）个人信息泄露事件的报告制度（第四十二条）；

10）违法使用个人信息删除和错误个人信息更正制度（第四十三条）；

11）网络运营者对用户非法信息传播的监管（第四十七条）；

12）网络信息安全投诉、举报制度（第四十九条）。

守法要点

➢ 产品研发

- ◆ 符合相关国家标准的强制性要求。不得设置恶意程序；发现存在安全缺陷、漏洞等风险时，应当立即采取补救措施，及时告知用户并向有关主管部门报告。
- ◆ 持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。
- ◆ 网络关键设备和网络安全专用产品安全认证合格或者安全检测符合要求后，方可销售

➢ 个人

- ◆ 规范上网行为：
  - ◆ 诈骗、传授诈骗方法、制售违禁物品
  - ◆ 不得危害网络安全（入侵、窃取等）、国家安全；
  - ◆ 不得发布不良信息
  - ◆ 不得侵犯他人权益
- ◆ 不为上述违法行为提供便利

03

发展机遇

发展机遇

➢ 标准制定

◆ 国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定（网络安全管理以及网络产品、服务和运行安全）。

➢ 产品运营

◆ 国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

◆ 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

◆ 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训。

➢ 产业机会

◆ 扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，支持企业等参与国家网络安全技术创新项目。

发展机遇

➢ 产业机会

- 关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。
  - 并保证安全技术措施同步规划、同步建设、同步使用。
  - 采购网络产品和服务，应当通过国家安全审查。
  - 每年至少进行一次检测评估
  - 定期开展网络安全应急演练
- 为未成年人提供安全、健康的网络环境
- 推进网络基础设施建设和互联互通，鼓励网络技术创新和应用
- 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放。
- 防范计算机病毒和网络攻击、网络侵入的产品
- 数据分类、重要数据备份和加密
- 支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认

谢　谢