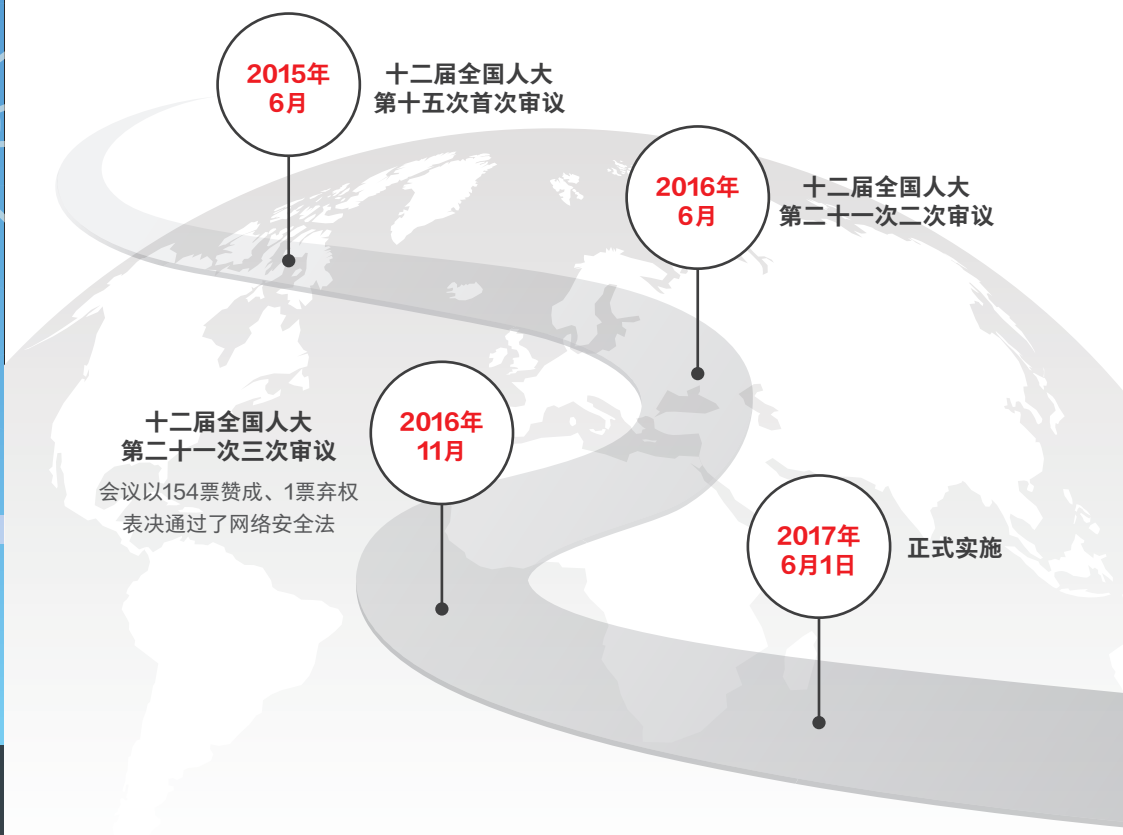
《网络安全法》解读

《网络安全法》的出台



我国网络领域的基础性法律，

明确加强对个人信息保护，打击网络诈骗。

网络安全的关键控制节点

1. 网络安全等级保护
2. 关键信息基础设施安全保护
3. 网络安全监测预警和信息通报
4. 用户信息保护
5. 网络信息安全投诉举报等制度
6. 网络关键设备和网络安全专用产品认证
7. 关键信息基础设施运营者网络产品和服务采购的安全审查
8. 关键信息基础设施运营者信息/数据境内存储
9. 关键信息基础设施运营者信息/数据境外提供安全评估
10. 关键信息基础设施运营者年度风险检测评估
11. 网络可信身份管理
12. 建设运营网络或服务的网络安全保障
13. 网络安全事件应急预案/处置
14. 漏洞等网络安全信息发布
15. 网络信息内容管理
16. 网络安全人员背景审查和从业禁止
17. 网络安全教育和培训
18. 数据留存和协助执法等制度

《网络安全法》概要

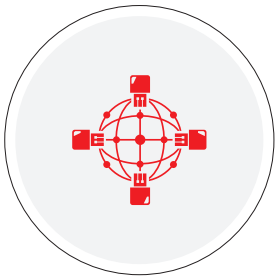
7 章 79 条

- 第一章 总则（十四条）
- 第二章 网络安全支持与促进（六条）
- 第三章 网络运行安全（十九条）
- 第四章 网络信息安全（十一条）
- 第五章 监测预警与应急处置（八条）
- 第六章 法律责任（十七条）
- 第七章 附则（四条）

6大亮点

- 明确了网络空间主权的原则
- 明确了网络产品和服务提供者的安全义务
- 明确了网络运营者的安全义务
- 进一步完善了个人信息保护规则
- 建立了关键信息基础设施安全保护制度
- 确立了关键信息基础设施重要数据跨境传输的规则

《网络安全法》的基本原则



网络空间主权原则

第1条 立法目的：明确规定要维护我国网络空间主权。

第2条 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。

网络安全与信息化发展并重原则

第3条 国家坚持网络安全与信息化发展并重，做到“双轮驱动、两翼齐飞”。

共同治理原则

第6条 采取措施鼓励全社会共同参与，政府部门、网络建设者、网络运营者、网络服务提供者、网络行业相关组织、高等院校、职业学校、社会公众等都应根据各自的角色参与网络安全治理工作。

《网络安全法》解读

《网络安全法》与等级保护

第二十一条

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

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。

《网络安全法》与网络产品和服务提供者

第二十二条

- 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、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。
- 网络产品、服务的提供者应当为其产品、服务持续提供安全维护；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；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

2017年3月7日

关于Apache　Struts2存在S2-045远程代码执行漏洞的安全公告

2017年5月12日

新型“蠕虫”式勒索软件 “WannaCry”全面爆发

2017年6月1日

开始实施网络产品和服务安全审查办法（试行）

《网络安全法》与网络运营者

第9条

网络运营者开展经营和服务活动必须接受社会监督

第14条

任何个人和组织有权对危害网络安全的行为进行举报

第43条

发现个人信息被冒用有权要求网络运营者删除

第49条

网络运营者应当建立举报制度、公布举报方式、及时受理举报

《网络安全法》与网络诈骗

精准诈骗

- 不法分子
- XX高考网上报名信息系统
- 植入木马病毒
- 大量考生报名信息糟泄露
- 学生被骗学费近万元

01	02	03	04
焦点1	焦点2	焦点3	焦点4
第40条、第41条	第42条、第44条、第46条	第42条	第64条
如何规范个人信息收集行为? 保护用户权益并确立边界。	如何斩断信息买卖利益链? 未经同意提供、出售个人信息违法。	个人信息泄露如何补救? 运营者要告知并报告。	如何对网络诈骗溯源追责? 重罚甚至吊销执照。

《网络安全法》与个人信息保护

个人信息安全面临严峻挑战

- 信息泄漏事件频频发生
- 个人信息过度收集屡禁不止
- 个人信息非法买卖日益猖獗
- 个人信息滥用助长恶意违法行为

《网络安全法》重点解决个人信息保护的痛点问题

1、规范了相关网络安全监管部门的责权范围

中央网信办、国务院电信主管部门、公安部门等

2、明确了个人信息保护相关主体的法律责任

建立健全用户信息保护制度、对收集信息的安全保密原则、公民信息境内存放原则、泄露报告制度等

3、提高了个人对隐私信息的管控程度

通过引入了删除权和更正制度，进一步提高了个人对隐私信息的管控程度

4、增强了针对侵犯个人信息权益行为的威慑

罚款、停业整顿、关闭网站、撤销相关业务许可或吊销营业执照的处罚

傅莹 | 十二届全国人大新闻发言人

今年将开展网络安全法执法检查重点关注个人信息保护

中央网信办

正制定个人信息收集规范标准

《网络安全法》与关键信息基础设施

419网络安全和信息化工作座谈会

“树立正确的网络安全观，加快构建关键信息基础设施安全保障体系”

“全天候全方位感知网络安全生态，增强网络安全防御能力和威慑能力”

2016年7月8日

《全国范围关键信息基础设施网络安全检查工作启动》“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改”（检查时间至12月底。）

基本制度

关键信息基础设施安全保护制度确立为国家网络空间基本制度保护办法由国务院制定

设施范畴

网络安全法规定了原则性范围：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和领域

责任追责

从国家、行业、运营者三个层面，分别规定了国家职能部门、行业主管部门及运营企业等各相关方的责任与义务，同时对境外的个人或者组织破坏关键信息基础设施提供法律依据

制度框架

关键信息基础设施运营者采购网络产品、服务的安全审查制度；加强国家的网络安全监测预警和应急制度建设，提高网络安全保障能力；尽快出台《国家关键信息基础设施安全保护条例》