《网络安全法》解读

网络技术与信息中心 宣

2017年9月12日-9月19日

四川中医药高等专科学校
SICHUAN COLLEGE OF TRADITIONAL CHINESE MEDICINE

深入贯彻落实
《中华人民共和国网络安全法》

共建网络安全 共享网络文明

In pursuit of the dream in the sky, even if broken wings,
the heart also want to learn to fly.if the dream is big enough,
the facts don’ t count.

《网络安全法》制定出台过程

- 《网络安全法》从草案发布到正式出台，共经历了三次审议，两次公开征求意见和修改。

《网络安全法》出台背景

落实国家总体安全观的重要举措

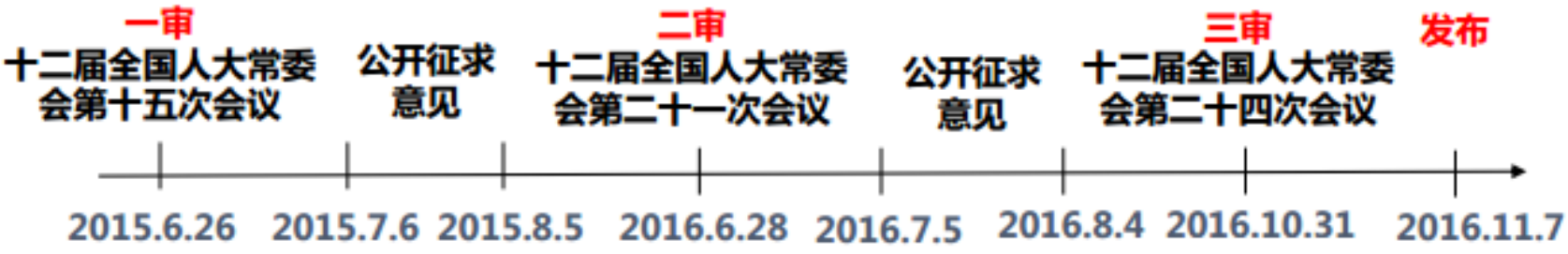
十八大以来，习总书记对加强国家网络安全工作做出了重要部署，对加强网络安全法制建设提出了明确要求

维护网络安全的客观需要

我国迫切需要建立和完善网络安全的法律制度，提高全社会的网络安全意识和网络安全的保护水平

维护人民群众切身利益的迫切需要

网络侵权行为严重损害了公民、法人和其他组织的合法权益，广大人民群众迫切地呼吁加强网络空间法制建设、净化网络环境



《 网络安全法》 正式发布


中国人大网
www.npc.gov.cn
网络安全法立法
（2015年6月—）
专题首页 | 最新动态 | 常委会一审 | 常委会二审 | 图片报道 | 文件资料 | 相关报道 | 其他专题
十二届全国人大常委会第二十四次会议第一次全体会议会场
· 张海阳作关于网络安全法草案审议结果的报告
· 十二届全国人大常委会第二十四次会议在京举行
· 网络安全法草案最新修改 拟强化关键信息基...
· 张德江主持召开十二届全国人大常委会第七 ...
· 十二届全国人大常委会第二十一次会议分组 ...
· 全国人大常委会分组审议网络安全法草案
· 进一步强化网络运营者社会责任
· 网络安全法草案拟加大对危害网络安全行为 ...
· 网络安全法草案拟进一步强化国家维护网络 ...
· 网络安全法草案拟加强对关键信息基础设施 ...
· 网络安全法草案拟增加多项促进网络安全的 ...
更多>>
常委会三审
网络安全立法
更多>>
（十二届全国人大常委会第二十四次会议·2016年10月）

《网络安全法》三审主要修改内容

- **第一次审议（2015年6月26日）**
  - 明确网络空间主权原则；对关键基础设施安全实行重点保护；加强网络安全监测预警和应急制度建设
- **第二次审议（2016年6月28日）**
  - 明确重要数据境内存储，建立数据跨境安全评估制度
  - 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
- **第三次审议（2016年10月31日）**
  - 进一步界定关键信息基础设施范围
  - 增加惩治攻击破坏我国关键信息基础设施的境外组织和个人的规定
  - 增加惩治网络诈骗等新型网络违法犯罪活动的规定
  - 加强网络安全人才培养、保护未成年人上网安全

《网络安全法》特色与亮点

主要特点

全面性

- 确定了各相关主体在网络安全保护中的义务和责任
- 确定了网络信息安全各方面的基本制度

针对性

- 从我国的国情出发，坚持问题导向，总结实践经验，借鉴了其他国家的一些做法，重在管用和解决实际问题。

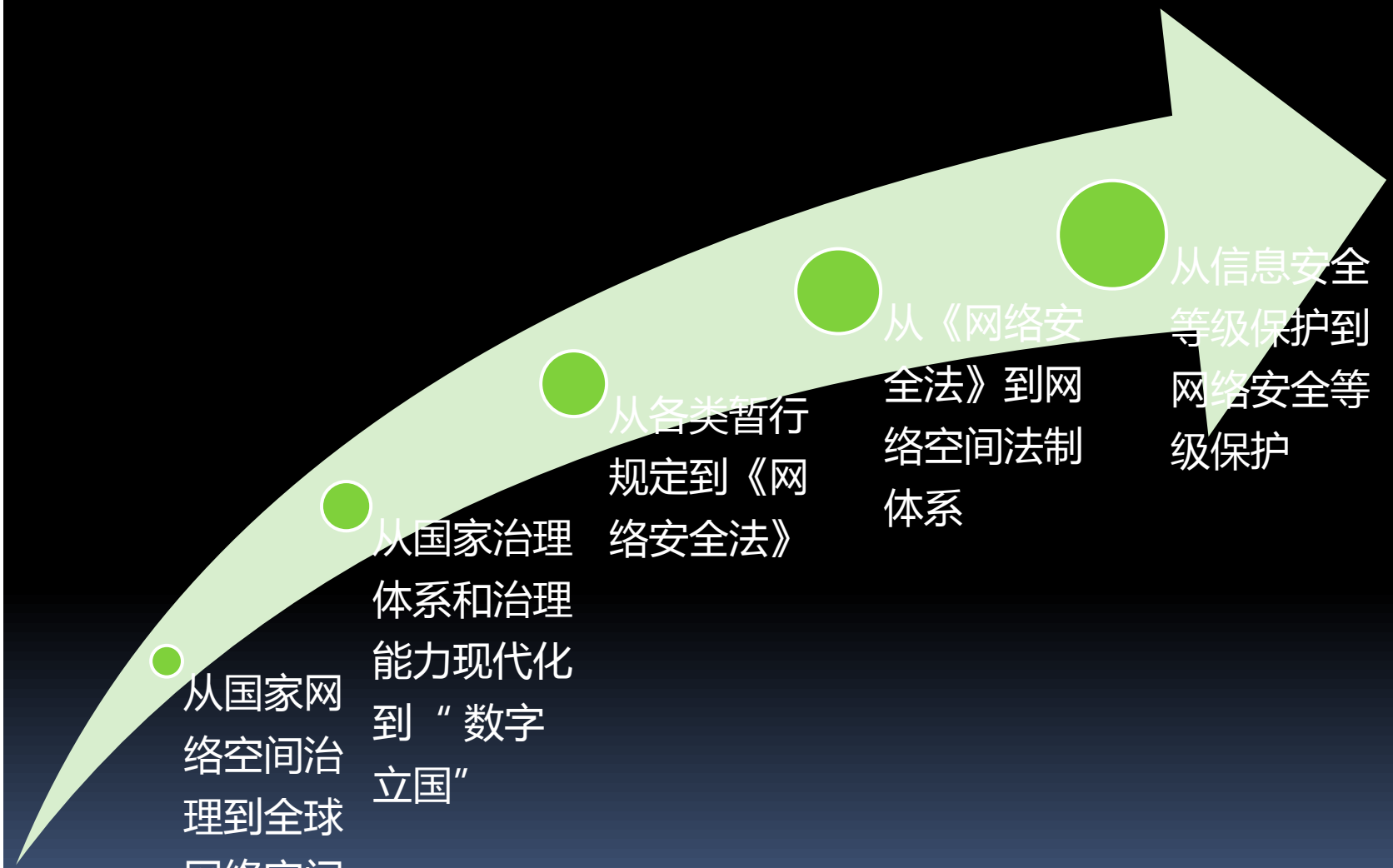
协调性

- 注重保护网络主体的合法权益，保障网络信息依法、有序、自由地流动，促进网络技术创新
- 最终实现以安全促发展，以发展来促安全

《网络安全法》突出亮点

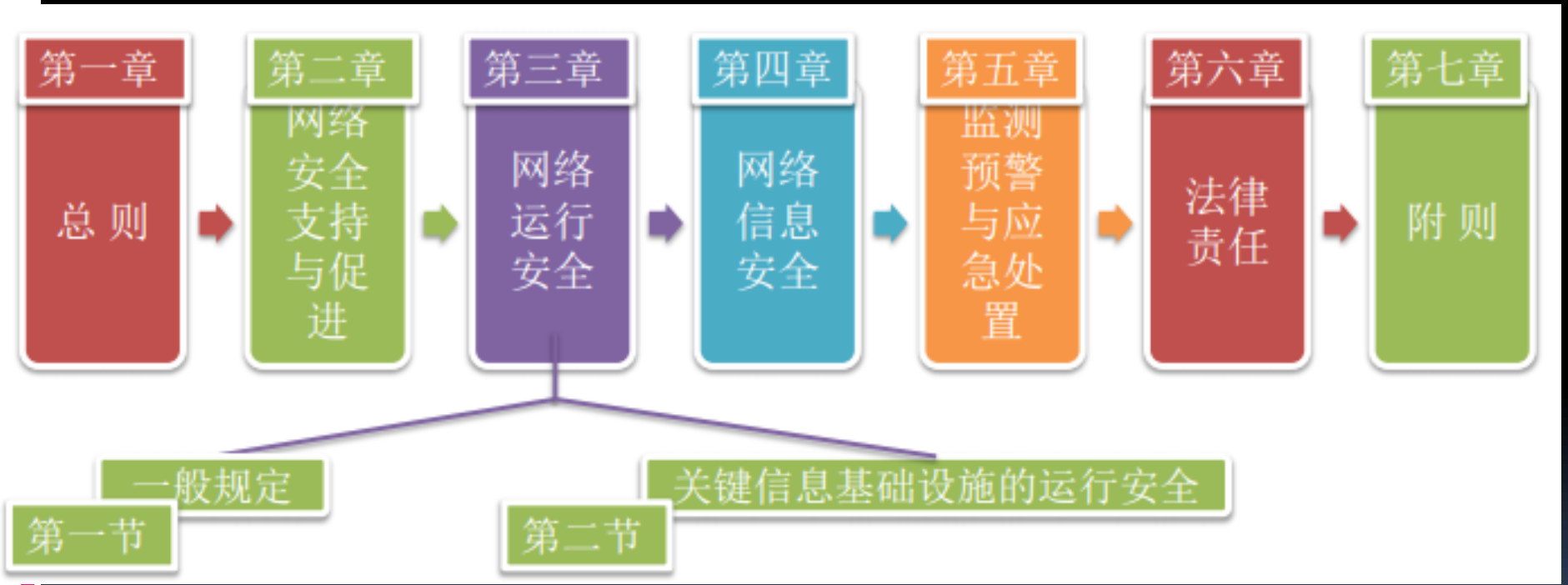
明确网络空间主权的原则	进一步完善个人信息保护规则
明确网络产品和服务提供者的安全义务	建立关键信息基础设施安全保护制度
明确了网络运营者的安全义务	确立重要数据跨境传输的规则

《网络安全法》的五个升级



《网络安全法》主要结构

- 共7章79条。



《网络安全法》基本概念

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进行收集、存储、传输、交换、处理的系统。

网络安全

是指通过采取必要措施，防范对网络的攻击、侵入、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。

网络运行安全

\+

网络信息安全

→ 网络安全

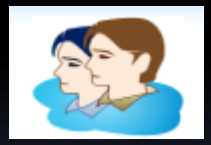
《网络安全法》基本概念

关键信息基础设施

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。关键信息基础设施的具体范围和安全保护办法由国务院制定

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



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

总则：明确网络空间主权原则

- 作为我国网络安全治理的基本法，《网络安全法》在总则部分确立了网络主权原则，明确了网络安全管理体制和分工，及域外的适用效力。

确立网络空间主权原则

◆第1条“立法目的”中明确规定要维护我国网络空间主权。

明确网络安全管理体制及职责分工

国家网信部门	国务院电信主管部门、公安部门和其他有关机关	县级以上地方人民政府有关部门
统筹协调	依法在职责范围内负责	依规定确定

明确特定情况下的域外适用效力

对来源于境外的网络安全风险和威胁	对来源于境外的违法信息	对境外危害我国关键信息基础设施的活动
监测、防御、处置	采取措施阻断传播	追究法律责任

网络安全等级保护制度

- 明确要求落实网络安全等级保护制度

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：（一）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；（二）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；（三）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；（日志留存）；（四）采取数据分类、重要数据备份和加密等措施；（数据安全）；（五）法律、行政法规规定的其他义务。

网络运行安全要求：明确网络运营者的安全义务

- **内部安全管理**：制定内部安全管理制度和操作规程，确定网络安全负责人
- **安全技术措施**：采取防范网络安全行为的技术措施；采取监测、记录网络运行状态、网络安全事件的技术措施，留存相关的网络日志不少于六个月
- **数据安全管理**：采取数据分类、重要数据备份和加密等措施，防止网络数据泄露或者被窃取、篡改
- **网络身份管理**：办理网络接入、域名注册服务，或固定电话、移动电话等入网手续，或为用户提供信息发布、即时通讯等服务，应要求用户提供真实身份信息。
- **应急预案机制**：制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。
- **安全协助义务**：为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助

网络运行安全要求：
明确网络产品、服务提供者的安全义务

- **强制标准义务**：网络产品、服务应当符合相关国家标准的强制性要求，不得设置恶意程序；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
- **告知补救义务**：网络产品、服务提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，及时告知用户，向有关主管部门报告。
- **安全维护义务**：网络产品、服务提供者应为产品、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；
- **个人信息保护**：网络产品、服务具有收集用户信息功能的，网络产品、服务提供者应向用户明示并取得同意；涉及用户个人信息的，还应遵守相关法律、行政法规中有关个人信息保护的规定。

网络运行安全制度：明确一般性安全保护义务

- **安全信息发布**：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。
- **禁止危害行为**：任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等。
- **信息使用规则**：网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

关键信息基础设施保护

1、关键信息基础设施内涵

- 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务重要行业和领域的关键信息基础设施
- 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

2、关键信息基础设施外延

- 关键信息基础设施的具体范围由国务院制定
- 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

3、关键信息基础设施管理机制

- 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门具体负责实施本行业、本领域的关键信息基础设施保护工作
- 国家网信部门统筹协调有关部门对关键信息基础设施采取安全保护措施

4、关键信息基础设施建设要求

- 确保具有支持业务稳定、持续运行的性能
- 安全技术措施同步规划、同步建设、同步使用

关键信息基础设施保护

5、关键信息基础设施运营者安全保护义务

- **人员安全管理**：设置专门安全管理机构和安全管理负责人；对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、培训和考核。
- **数据境内留存**：在我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。确需向境外提供的，需经国家安全评估；对重要系统和数据库进行容灾备份。
- **应急预案机制**：制定网络安全事件应急预案，并定期进行演练。
- **安全采购措施**：采购网络产品和服务可能影响国家安全的，应当通过国家安全审查。应与网络产品和服务提供者签订安全保密协议。
- **风险评估机制**：自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关部门。

关键信息基础设施保护

个人信息和重要数据出境安全评估办法

2017年04月10日国家互联网信息办公室发布关于《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。明确了：

- 个人信息和重要数据出境的范围
  - 有50万人以上的个人信息
  - 数据量超过1000GB
  - 7大重要领域数据等
- 数据出境评估原则
- 评估7个方面主要内容

网络安全审查制度

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

2017年05月02日中央网信办正式发布《网络产品和服务安全审查办法（试行）》。其中就审查的目的、需要审查的网络产品和服务的范围、网络安全审查的管理部门（网络安全审查委员会）、审查的机构（国家统一认定网络安全审查第三方机构）和对党政机关和重点行业的审查工作提出要求。并于2017年6月1日同《网络安全法》一同实施。

网络信息安全—个人信息保护

保护规范

原则：合法、正当、必要（第41条）

规则：吸收了国际通行规则

规则透明：公开规则、获得同意（第41条）

目的限制：不得超范围收集、违法和违约收集（第41条）

安全保密：不得泄露毁损、预防措施、补救措施（第40、42条）

删除改正：删除违法、违约信息、改正有误信息（第43条）

规范主体

网络运营者、任何个人和组织、负有网络安全监督管理职责的部门及其工作人员

网络运营者

安全保密、知情同意、目的限制、删除改正、

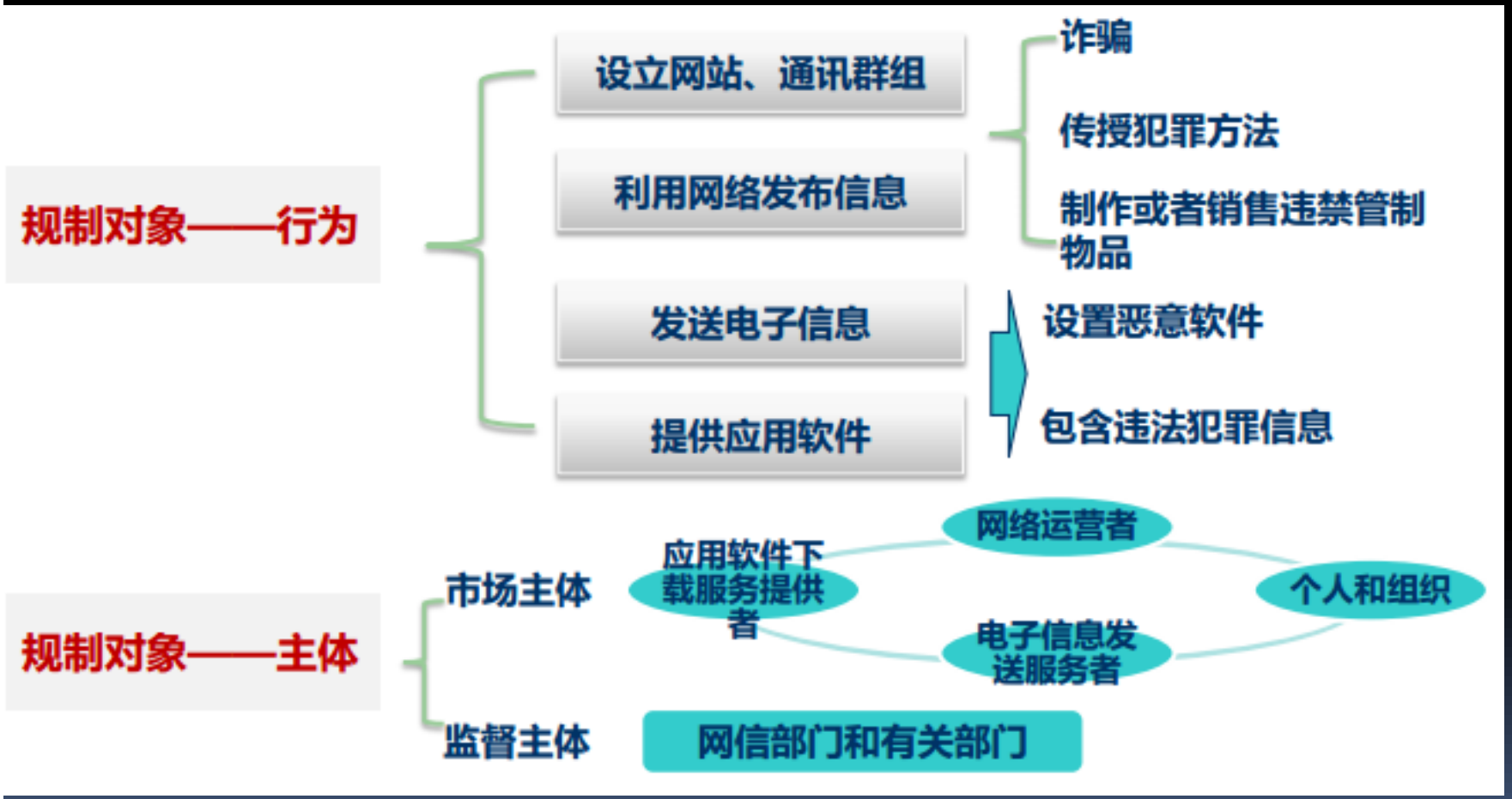
个人和组织

不得窃取、非法出售个人信息

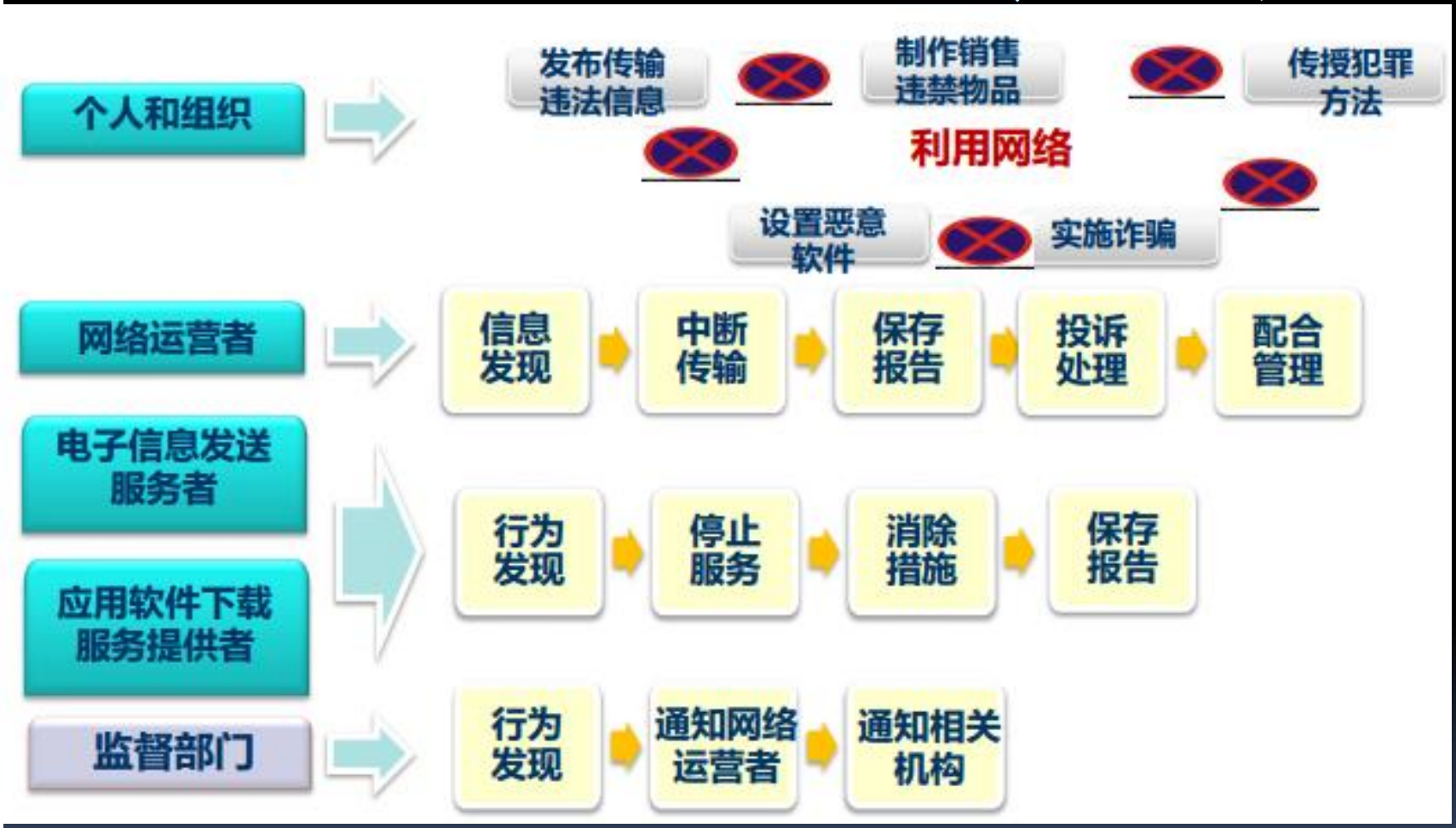
监督部门

保密、不得泄露出售

网络信息安全—违法犯罪信息管理



网络信息安全—违法犯罪信息管理



网络信息安全-

《互联网新闻信息服务管理规定》

2017年05月02日国家互联网信息办公室正式发布《互联网新闻信息服务管理规定》（国信办1号令），于6月1日同《网络安全法》一起实施。规范了：

- 互联网新闻信息服务的范围
- 互联网新闻信息服务的6项许可条件
- 互联网新闻信息服务提供者的责任义务
- 网信部门对互联网新闻信息服务的监督检查要求
- 相关法律责任

网络信息安全-

《互联网信息内容管理行政执法程序规定》

同日国家互联网信息办公室一并发布《互联网信息内容管理行政执法程序规定》（国信办1号令），于6月1日同《网络安全法》一起实施。规范了：

- 互联网信息内容管理部门行政执法依据
- 管辖范围
- 立案流程
- 调查取证过程
- 听证及约谈机制
- 处罚决定及执行办法等

监测预警与应急处置工作制度化、法制化

责任主体	具体制度
国家网信部门	• 统筹网络安全信息收集、分析和通报，统一发布网络安全监测预警信息；制定网络安全事件应急预案，定期组织演练。
负责关键基础设施安全保护工作部门	• 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，按照规定报送预警信息；制定本行业、本领域的网络安全事件应急预案，定期组织演练。
省级以上人民政府有关部门	• 网络安全事件发生的风险增大时，采取信息报送、网络安全风险信息评估、向社会预警等措施；按照规定程序及权限对网络运营者法定代表人进行约谈
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；按照省级以上人民政府要求进行整改，消除隐患

法律责任

- 对违反《网络安全法》的行为，第六章规定了民事责任、行政责任、刑事责任。