01 网络安全政策法规

我国网络安全政策法规体系基本形成，已基本构建起网络安全政策法规体系的“四梁八柱”

制定出台相关战略规划。

颁布《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规。

出台《云计算服务安全评估办法》《汽车数据安全管理若干规定（试行）》《生成式人工智能服务管理暂行办法》《互联网政务应用安全管理规定》等政策文件。

建立关键信息基础设施安全保护、云计算服务安全评估、数据出境安全管理、网络安全服务认证等一系列重要制度。

法律

《中华人民共和国网络安全法》

2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过，自2017年6月1日起施行。

是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是让互联网在法治轨道上健康运行的重要保障。

《中华人民共和国数据安全法》

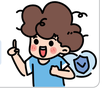
2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过，自2021年9月1日起施行。

是我国数据领域的基础性法律，也是国家安全领域的一部重要法律。

《中华人民共和国个人信息保护法》

2021年8月20日，第十三届全国人大常委会第三十次会议通过，自2021年11月1日起施行。

是为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用而制定的法律。



行政法规

《关键信息基础设施安全保护条例》 2021年9月1日起施行

是我国首部专门针对关键信息基础设施安全保护工作的行政法规，也是《网络安全法》的重要配套法规。

《云计算服务安全评估办法》 2019年9月1日起施行

为提高党政机关、关键信息基础设施运维采购使用云计算服务的安全可控水平而制定。《办法》明确了云计算服务安全评估目的、对象、申请方式、重点评估内容和主要环节等内容。

《汽车数据安全管理若干规定（试行）》 2021年10月1日起施行

为防范化解汽车数据安全风险、保障汽车数据依法合理有效利用制定此规定。《规定》明确了汽车数据处理者开展汽车数据处理活动的一般要求，倡导汽车数据处理者在开展汽车数据处理活动中坚持“车内处理”、“默认不收集”、“精度范围适用”、“脱敏处理”等原则，减少对汽车数据的无序收集和违规滥用。

《生成式人工智能服务管理暂行办法》 2023年8月15日起施行

是我国首个针对生成式人工智能服务的规范性政策，用于促进生成式人工智能健康发展和规范应用，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

《互联网政务应用安全管理规定》 2024年7月1日起施行

旨在提高互联网政务应用安全防护水平，保障和促进互联网政务应用安全稳定运行。《规定》要求，建设运行互联网政务应用应当依照有关法律、行政法规的规定以及国家标准的强制性要求，落实网络安全与互联网政务应用“同步规划、同步建设、同步使用”原则，采取技术措施和其他必要措施，防范内容篡改、攻击致瘫、数据窃取等风险，保障互联网政务应用安全稳定运行和数据安全。

02 关键信息基础设施网络安全保护

什么是关键信息基础设施

是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。**

怎样认定关键信息基础设施

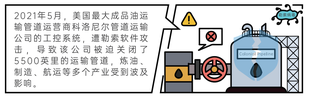
重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门，保护工作部门结合本行业、本领域实际，**制定关键信息基础设施认定规则。**

制定认定规则主要考虑因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的**重要程度**；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的**危害程度**；

（三）对其他行业和领域的**关联性影响**。



2021年5月，美国最大成品油运输管道运营商科洛尼尔管道运输公司的工控系统，遭勒索软件攻击，导致该公司被迫关闭了5500英里的运输管道，炼油、制造、航运等多个产业受到波及影响。

近年来，我国有关电信运营商、航空公司等单位内网和信息系统先后多次出现越权登录、数据外传等异常网络行为，疑似遭受网络攻击。

关键信息基础设施安全保护举措

2021年8月17日，国务院公布《**关键信息基础设施安全保护条例**》，自2021年9月1日起施行。

是落实《**网络安全法**》要求、构建国家关键信息基础设施安全保护体系的顶层设计和重要举措，更是保障国家安全、社会稳定和经济发展的现实需求。

2022年11月7日，我国《**关键信息基础设施安全保护要求**》国家标准（GB/T 39204-2022）发布，2023年5月1日，正式实施。是我国第一项关键信息基础设施安全保护的国家标准，对于我国关键信息基础设施安全保护有着重要的指导意义。

明责任 强举措 护安全

坚持综合协调

坚持分工负责

坚持依法保护

各部门职责

国家网信部门：统筹协调；

国务院公安部门：指导监督安全保护工作；

国务院电信主管部门和其他有关部门：依照相关规定，在各自职责范围内负责关键安全保护和监督管理工作；

省级人民政府有关部门：依据各自职责对关键基础设施安全保护和监督管理。

运营者责任义务

- 落实网络安全保护制度和责任制；
- 与关键信息基础设施同步规划、同步建设、同步使用安全保护措施；
- 建立健全网络安全保护制度；
- 设置专门安全管理机构；
- 开展安全监测和风险评估；
- 报告网络安全事件或网络安全威胁；
- 规范网络产品和服务采购活动。

保护关键信息基础设施 筑牢网络安全屏障

03 数据安全

是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

数据是什么

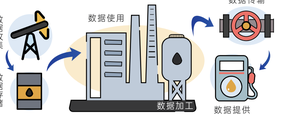
个人购物产生的交易记录

快递物流信息

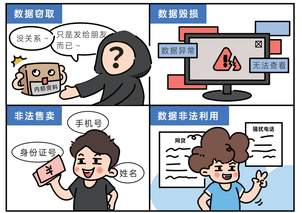
大型互联网平台处理的海量数据信息

网约车共享单车的地图轨迹

数据处理



突出问题



危害数据安全的典型案例

2020年1月，某航空公司数据被境外间谍情报机关网络攻击窃取。

2021年3月，李某等人私自在某重要军事基地周边架设气象观测设备，采集并向境外传送敏感气象数据。

2021年5月，某境外咨询调查公司秘密搜集窃取航运数据。

怎样加强数据安全保护

数据处理者：

备份、加密、访问控制、应急处置、风险评估。

重要数据的处理者：

明确数据安全负责人，成立数据安全管理机构；制定数据安全培训计划，组织开展全员数据安全教育培训；优先采购安全可信的网络产品和服务、定期开展数据安全评估。

互联网平台运营者：

建立与数据相关的平台规则、隐私政策和算法策略披露制度，及时披露制定程序、裁决程序、保障平台规则、隐私政策、算法公平公正。

《促进和规范数据跨境流动规定》

主要内容

明确重要数据出境安全评估申报标准。

明确免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件。

设立自由贸易试验区负面清单制度。

调整应当申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件。

延长数据出境安全评估结果有效期，增加数据处理者可以申请延长评估结果有效期的规定。

强化数据安全治理，推动持续健康发展

04 个人信息保护

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

泄露途径

防范建议

① 要优先选择尊重个人信息保护的产品、服务。

② 要仔细审核 App 请求授权的权限内容，并谨慎授权。

③ 要对重要信息进行加密保护。

④ 要差异化设置社交平台好友的信息访问权限。

⑤ 不要随意连接免费 Wi-Fi 热点。

⑥ 不访问陌生网站并留下个人信息。

⑦ 不要在网上随意发布个人照片或其他涉及个人隐私的影像。

⑧ 尊重他人隐私，不随意披露他人隐私信息。

个人信息保护好，畅游网络无烦恼

组织编制：2024年国家网络安全宣传周指挥部办公室

国家网络安全宣传周
China Cybersecurity Week

国家网络安全宣传周官方网站

国家网络安全宣传周官方微信账号

国家网络安全宣传周网络安全云竞答

05 网络安全教育技术产业融合发展

网络空间的竞争，归根结底是人才竞争。建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。

——习近平在网络安全和信息化工作座谈会上的讲话（2016.4.19）

一流网络安全学院建设示范项目

为贯彻落实习近平总书记关于加强一流网络安全学院建设和坚持网络安全教育技术产业融合发展的重要指示精神，经高校申报、专家评审等环节，2024年1月，中央网信办、教育部评选产生新一期一流网络安全学院建设示范项目高校。

建立健全网络安全创新人才培养的课程、教材、实训环境体系，**鼓励和支持**教师学生参与开源生态建设，创新网络安全教育技术产业**融合发展模式**，深入开展网络安全学院学生创新资助计划。

创新网络安全人才评价机制，不将发表学术论文作为学生毕业、教师晋升的必要条件。

教师学生参与重要课题、重大工程建设、企业和科研单位技术研发过程中的优秀成果，视同高水平学术论文。

给大家分享个好消息

2017 年以来，中央网信办、教育部组织实施一流网络安全学院建设示范项目，网络安全人才培养规模大幅增长，人才培养模式不断创新，极大促进了网络安全人才培养工作。

国家网络安全人才与创新基地

武汉

2016年，中央网信办正式批复支持武汉市建设国家网络安全人才与创新基地；2020年，武汉大学、华中科技大学网络安全学院正式入驻办学；2023年，“国家关键信息基础设施安全保护培训基地”授牌落户。

福州

2023 年 9 月，中央网信办批复创建国家网络安全人才与创新（福州）基地。

国家网络安全教育技术产业融合发展试验区

目的				
目的	**探索**网络安全教育技术产业融合发展的新机制新模式。	**形成**一系列鼓励和支持融合发展的制度和政策。	**培育**一批支撑融合发展的创新载体。	**推动**在全国范围内形成网络安全人才培养、技术创新、产业发展的良好生态。

首批试验区

安徽省 合肥高新技术产业开发区	**北京市** 海淀区	**陕西省** 西安市雁塔区	**湖南省** 长沙高新技术产业开发区	**山东省** 济南高新技术产业开发区

政产融学研用一体，共同建设网络强国

06 电信网络诈骗

是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。

刷单返利类诈骗

小额任务佣金小“赚”，大额投入没法提现

虚假网络投资理财类诈骗

“旁门左道”迷双眼，试水投资有风险

冒充领导、熟人类诈骗

诈骗技术新升级，涉及资金要警惕

防范建议

保护个人信息：不在社交平台随意发布身份证、家庭住址、车票等涉及个人信息的影像资料。不将自拍照等个人照片发给陌生人。

不透露密码：为银行卡、网上银行、手机银行设置复杂程度较高的密码，不向任何人透露或转发短信验证码或其它形式动态密码。

官方渠道办业务：办理银行信用卡及额度提升等业务，一定要通过银行官方平台等可靠渠道进行申请。在网购平台办理退款、退货要通过官方App渠道。

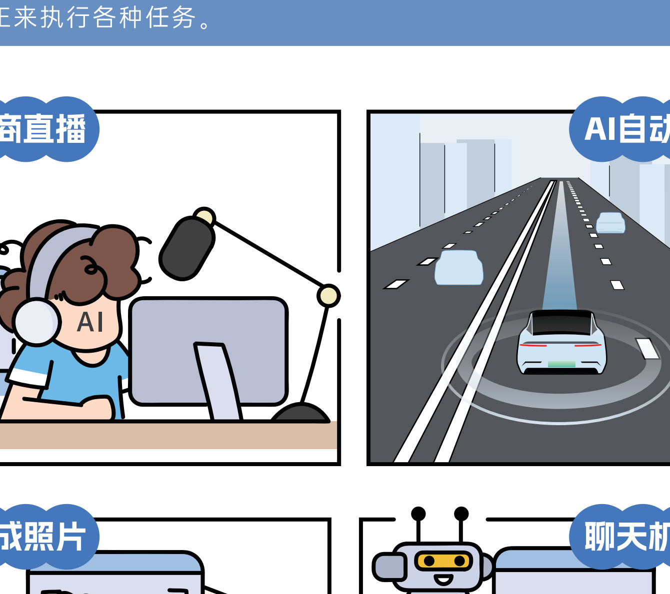
加强对电话、短信或社交媒体信息真实性甄别：尤其在接到涉及钱款的电话、语音或视频时，要通过挂断当前通话，主动拨打联系人或官方客服电话等方式确认。也可以让视频中的人做一些复杂动作，比如张大嘴巴、扮鬼脸、用手在人脸前来回摆动等，以观察人脸是否出现形变。

下载和使用手机应用程序：在手机官方应用商店下载App，避免从非官方渠道下载。网购退款等操作一定要通过官方App进行，电商物流客服人员说要给你私下汇款的很可能是诈骗。

花言巧语投入一文不值，卷款跑路骗走白银真金

07 人工智能安全

人工智能（AI）是一种模拟人类智能的技术，它通过学习、推理和自我修正来执行各种任务。



生成式人工智能技术

是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。主要是利用机器学习模型，通过对大量数据的学习来理解并创建新内容。

生成式人工智能带来的网络安全风险

利用人工智能技术进行诈骗：诈骗分子通过AI换脸、拟声手段，佯装亲属或好友拨打视频电话，博取信任后，谎称急需资金周转等实施诈骗。

利用人工智能技术编造谣言：违法行为人往往为了博取流量获得收益，利用AI软件输入关键词生成谣言文章并对外发布，引发大量网络关注，造成不良社会影响。

AI换脸直播带货：有直播间利用AI换脸技术“以假乱真”实现“明星”代言，来增加流量，提高销量。

人工智能治理

2023年10月18日，中国政府发布《全球人工智能治理倡议》，围绕人工智能发展、安全、治理三方面系统阐述了人工智能治理中国方案。倡议：

——发展人工智能应坚持**“以人为本”理念**；

——发展人工智能应坚持**“智能向善”的宗旨**；

——发展人工智能应坚持**相互尊重、平等互利的原则**；

——坚持**公平性和非歧视性原则**；

——坚持**广泛参与、协商一致、循序渐进**的原则。

《生成式人工智能服务管理暂行办法》自2023年8月15日起施行。该办法突显了**中国特色的人工智能治理之道，为世界人工智能治理贡献中国智慧**。

鼓励生成式人工智能**创新应用**；

强化风险治理，突出**分类分级监管**；

强调**个人信息保护、知识产权保护**；

明确生成式人工智能服务提供者的**内容安全主体责任**。

坚持以人为本，智能向善

国家网络安全宣传周
China Cybersecurity Week

网络安全为人民 网络安全靠人民

网络安全知识宣传手册

2024年国家网络安全宣传周