



2025两会热议“网安提案” 为数字化发展保驾护航

目录

01

网络安全
-数字化发展的基石

02

人工智能安全
-前沿技术的保障需求

03

大模型安全
-筑牢人工智能的
安全根基

04

数据安全
-数字经济的核心
保障

05

网络谣言和
网络暴力治理
-营造清朗网络空间

06

结语
-共筑网络安全防线



01、 网络安全 -数字化发展的基石

两会网络安全提案的背景

- 当前，全球数字化转型进入加速期，人工智能、大数据、云计算等新兴技术的广泛应用推动了各行业的变革。然而，技术的快速发展也带来了新的安全风险，网络安全形势日益复杂严峻。



- 如人工智能技术在提升生产效率的同时，也可能被恶意利用，以“AI 换脸”技术为例，其被用于诈骗，给个人和社会带来巨大危害。因此，网络安全问题成为数字化转型过程中亟待解决的关键问题。

两会网络安全提案的背景

- 近年来，网络安全事件频发，从勒索软件攻击到数据泄露，从网络暴力到虚假信息传播，网络安全威胁无处不在。这些事件不仅影响了个人和企业的正常生活和运营，也对社会稳定和国家安全构成了严重威胁。

网络安全事件 频发

- 据《2024年全球网络安全报告》统计，2024年全球网络攻击事件数量同比增长30%，其中针对关键基础设施的攻击占比超过40%。这些数据表明，网络安全形势不容乐观，亟需采取有效措施加以应对。

两会网络安全提案的背景



社会各界的广泛关注

- 网络安全问题的复杂性和严重性引起了社会各界的广泛关注。政府部门、企业、学术界和普通民众都对网络安全问题高度关注，希望通过加强网络安全防护，保障数字化发展的安全稳定。

- 在2025年全国两会上，网络安全成为热点议题，众多代表和委员提出了多项提案，反映了社会各界对网络安全问题的高度关注和迫切需求。



02、人工智能安全 -前沿技术的保障需求

人工智能安全提案概览

1、全国政协委员、奇安信科技集团董事长齐向东：推广“AI+安全”创新成果落地，走好提升安全能力的必经之路。随着人工智能应用的进一步铺开，要鼓励更多产业用上、用好“AI+安全”创新成果，提高千行百业的网络安全防护效能。促进产学研用深度融合，推动科研成果从实验室走向市场，并以更加主动的姿态嵌入区域化、全球化的产业链条，占据关键节点位置，推动人工智能产业迈向更高发展水平。

2、全国政协委员、360集团创始人周鸿祎：支持安全技术创新与成果转化。建议相关部门及时出台配套政策措施，鼓励具备“安全+人工智能”完整解决方案的链主企业，针对人工智能应用所涉及的基座模型、知识库、智能体等安全问题，以模制模，基于安全大模型技术开展研发工作，加速推动技术成果转化，将安全要素深度嵌入人工智能应用全流程。

人工智能安全提案概览

3、全国政协委员、安天集团创始人肖新光：面对快速发展、日新月异的AI与智能设备发展情况，需由相关主管部门、行业协会和消费者协会推动手机厂商、互联网（含大模型）平台厂商、移动应用厂商和消费者协商。在用户个人信息采集、安全权限设定、无障碍功能使用、API标准接口授权机制等领域推进理解，更好地促进各方权责利的平衡，共同推进AI应用的行业合规，避免出现消费者权益和隐私安全受损。

4、全国人大代表、小米集团创始人、董事长兼CEO雷军：针对“AI换脸拟声”等问题，探索推出人工智能单行法，提高立法位阶及其效力，在分级分类的基础上进行务实治理，明确“AI换脸拟声”应用边界红线，完善侵权证据规则，加大对利用人工智能技术实施犯罪行为的刑事处罚力度。

人工智能安全提案概览

5、全国人大代表、TCL创始人、董事长李东生：一是加快人工智能深度合成内容标识管理规章制度的出台；二是明确对人工智能深度合成服务商未履行标识义务的惩罚制度，完善对深度合成内容服务提供商未按要求进行标识的行为界定、分类细则，以及相应的处罚标准；三是加强深度合成内容标识技术标准和发布的管理，出台深度合成内容标识的技术标准，保证标识的有效性；对相关内容平台出台要求，用户在发布深度合成的视频、音频等内容时，有义务对其进行标识；四是加强国际合作，形成人工智能生成合成内容的有效监管。

6、全国政协委员、清华大学教授李景虹：中国作为人工智能综合实力较强的国家，应该制定人工智能促进法，凝聚共识，形成合力，推动人工智能向造福于民的方向发展。同时，将该项立法提升至战略高度，立足于发展，结合最小化的包容性审慎监管规则，为社会各界提供最大程度的确定性和明确的预期。他认为立法应聚焦促进有效应用、普惠服务、技术创新、人才培养（包括尖端人才和复合型人才）、就业保障（包括扩大职业教育和全民通识教育）、国际合作等六个方面。

人工智能安全提案概览

7、全国政协委员、中华全国律师协会监事长吕红兵：应明确规定将社会主义核心价值观贯穿生成式人工智能全生态，并由其统领。行政法规应对生成式人工智能的技术开发者、服务提供者、使用者、监管者以及社会公众，分门别类明确各自权利和义务、职能与责任。他建议，应明确统一的监管者，对网信、发展改革、教育、科技、工信、公安、广电等部门的相关职责合并同类项，组建统一的监管部门，提高监管的专业性与权威性。

8、全国政协委员、金杜律师事务所高级合伙人张毅：立法应当坚持以人民为中心，保障人的主体地位和权益，遵循“以人为本、智能向善、造福人类”的原则。同时，人工智能的发展应以促进产业健康发展和经济社会深度融合为目标，推动人工智能健康可持续发展。对于相关部门已经出台的政策法规和各地试点经验，立法时应予以吸纳，将成熟的政策和机制上升为法律条文。建议将数据可信流通、算法备案、安全审查等有效条款纳入法律框架中。算法服务商应承担披露义务，确保用户对算法服务的选择权，并引入技术及合规专家参与监管。立法还应明确算力作为人工智能产业支柱的发展原则和目标，制定鼓励政策，覆盖芯片设计、开发、制造与流通等全环节。

人工智能安全提案概览

9、全国政协委员、四川大学华西医院教授甘华：首先是完善AI生成内容监管法律法规体系；其次，加强技术监管与防范，研发更加先进的人工智能算法，提高其对信息的识别和判断能力；第三是建立健全监管机制。设立专门的监管机构，负责对AI产品和服务进行审查和监督，确保其符合法律法规和道德规范。



03、大模型安全

- 筑牢人工智能的安全根基

大模型安全的挑战与应对

1、全国政协委员、奇安信科技集团董事长齐向东：一是建立适配大模型的纵深防御体系，筑牢人工智能的安全根基。做好“内防内鬼，外防攻击”，对数据安全、终端安全、API安全等方面给予全方位安全保障；二是制定大模型安全强制合规要求，夯实人工智能安全发展的制度保障。同时，做好大模型运行安全监测和内容风控，定期开展安全评估测试，完善应急响应机制，一旦发现异常行为或潜在的安全事件，第一时间进行处置，将安全威胁消除在萌芽状态。

2、全国政协委员、360集团创始人周鸿祎：建议借鉴“避风港原则”成功经验，对大模型以及相关的产品和服务实施柔性监管，适度包容大模型的“幻觉”，对于“幻觉”导致的一般性失误，避免直接关停下架，给予企业自我纠正的机会，促进企业大胆创新、放手竞争。

大模型安全的挑战与应对

- ✓ - 大模型的训练和运行依赖大量数据，数据安全和隐私保护是大模型安全的核心问题。提案中提到，需建立适配大模型的纵深防御体系，对数据安全、终端安全、API安全等方面给予全方位保障。
- ✓ - 如大模型在训练过程中可能接触到敏感数据，如果没有有效的安全措施，可能导致数据泄露，给用户带来巨大损失。因此，加强数据安全是大模型安全的关键任务。



大模型安全的挑战与应对



- 随着大模型的广泛应用，制定强制合规要求和完善的应急响应机制是确保其安全运行的重要保障。提案建议定期开展安全评估测试，完善应急响应机制，确保在发现异常行为或潜在安全事件时能够及时处置。

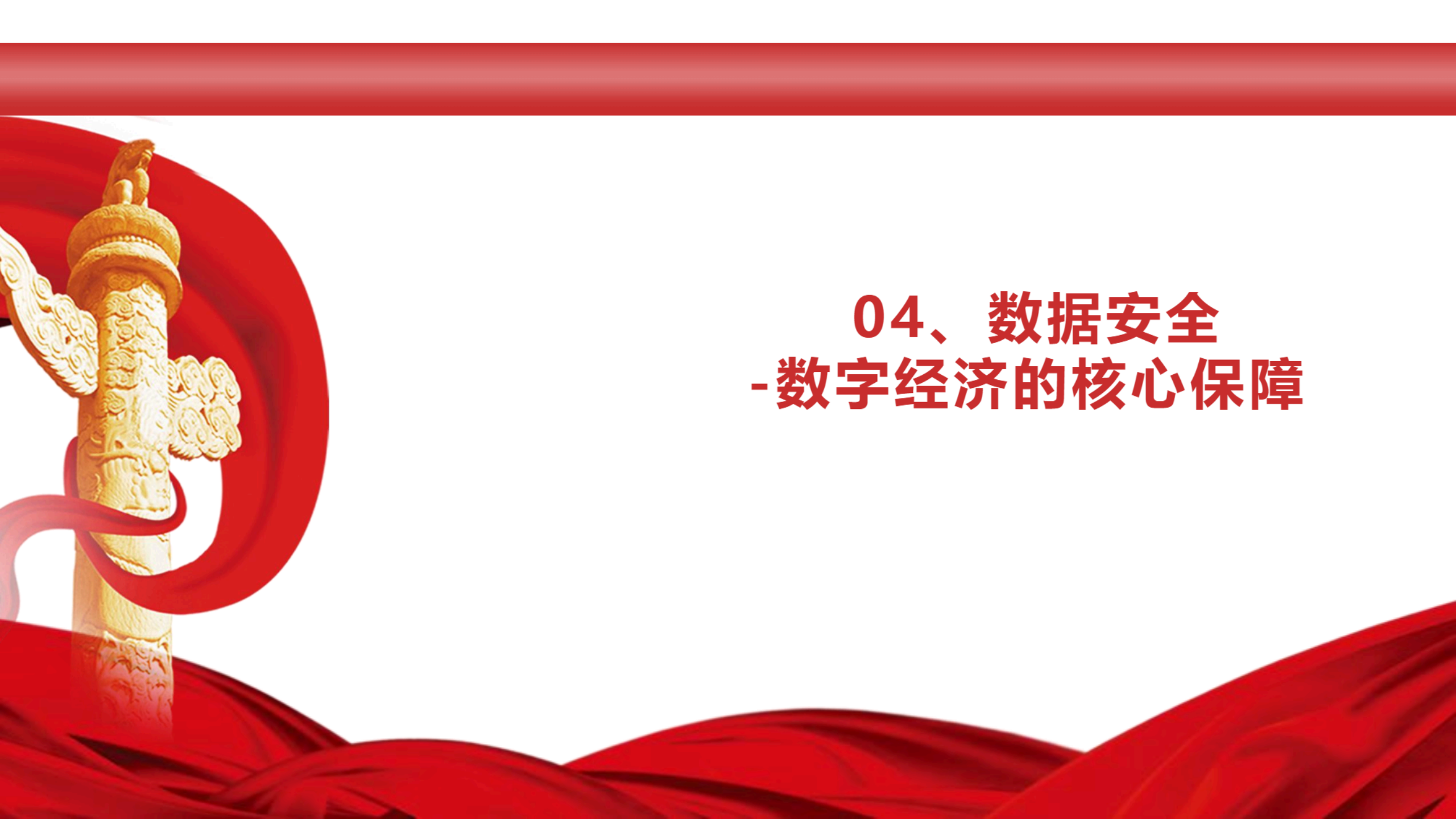
- 如大模型在运行过程中被检测到存在安全漏洞，及时的应急响应措施能够有效防止漏洞被利用，避免更大的安全风险。

大模型安全的挑战与应对

大模型安全

- 在保障大模型安全的同时，还需鼓励企业创新和竞争。提案建议借鉴“避风港原则”，实施柔性监管，给予企业自我纠正的机会，促进大模型技术的健康发展。

- 如对于大模型的“幻觉”问题，通过柔性监管可以在保障安全的前提下，鼓励企业不断优化模型，提升其性能和可靠性。



04、数据安全

- 数字经济的核心保障

数据安全提案概览

1、全国政协委员、中国工程院院士邓中翰：一是构建全国统一的数据市场，统筹国家数据基础设施，推动跨层级、跨领域数据可信流通；建立健全国家公共数据资源体系，支持公共数据与行业数据融合开发，在国家安全、经济民生等关键领域实现数据“有标识、受监管、被保护、可交易、能使用”；二是强化技术与标准支撑，加大数据加密、数字水印等关键技术攻关，推进视音频编解码（SVAC）、智能感知等领域自主标准制定，以标准优势带动产业优势，筑牢数据主权安全防线。

2、全国人大代表、长虹控股集团董事长柳江：AI技术的广泛应用仍面临可信数据空间技术标准不统一、数据要素市场机制不健全等问题，建议加快可信数据空间建设，推动数字经济与实体经济的深度融合。

数据安全提案概览

3、全国人大代表、科大讯飞董事长刘庆峰:构建安全可信数据标签体系,提升内容可靠性,建立安全可信、动态更新的信源和数据知识库,对不同类型数据的可信度和危害程度建立标签体系,降低人工智能幻觉出现概率,提升生成内容可靠性;研发AIGC幻觉治理技术和平台,定期清理幻觉数据,研究幻觉自动分析的技术和软件平台,开展幻觉自动分析、AIGC深度鉴伪、虚假信息检测、有害内容识别以及互联网传播溯源,由中央网信办、国家数据局等部门定期清理幻觉数据,为公众提供AIGC幻觉信息检测工具与服务。

4、全国政协委员、新大陆科技集团CEO王晶:通过完善数字身份认证体系、构建广泛的应用接入与数据服务能力、构建可市场化运营的第三方服务模式等措施,构建起数据安全的新防线,推动数字公民建设,为构建网络强国、数字中国贡献力量。

数据安全的挑战与应对

数据市场与基础设施建设



- 构建全国统一的数据市场和统筹国家数据基础设施是数据安全的重要基础。通过推动跨层级、跨领域数据可信流通，可以实现数据资源的最大化利用，同时确保数据的安全和合规使用。
- 建立统一的数据市场可以促进公共数据与行业数据的融合开发，提高数据的利用效率，为数字经济的发展提供有力支撑。



数据加密与标准制定

- 数据加密和自主标准制定是数据安全的关键技术支撑。通过加大数据加密、数字水印等关键技术攻关，可以有效保护数据的隐私和完整性。
- 国密技术的持续发展以及相关标准的制定和应用，可以推动相关产业的发展，筑牢数据主权安全防线。

数据安全的挑战与应对

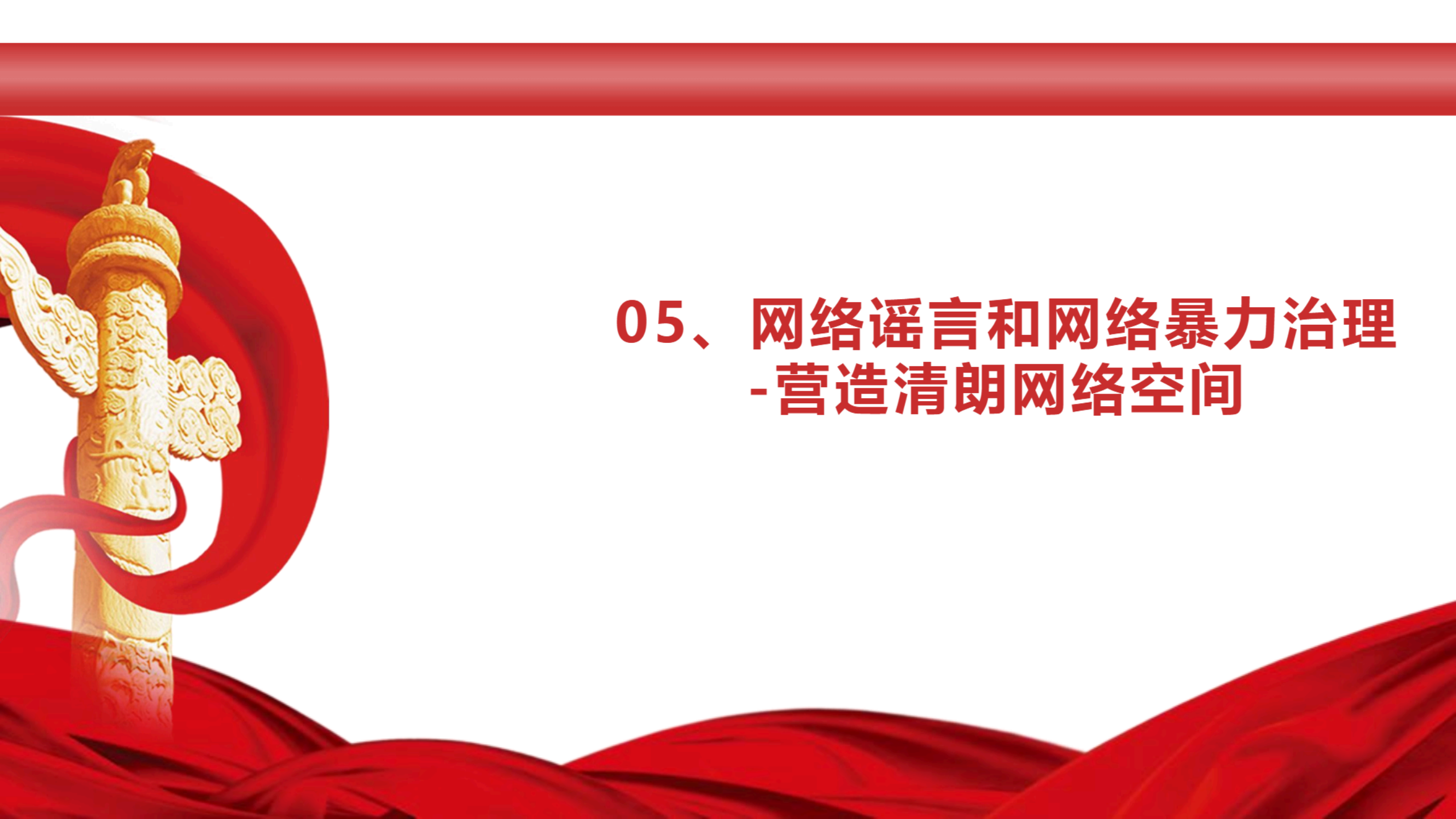
数据治理与身份认证

01

- 数据治理和身份认证是数据安全的重要保障。通过构建安全可信数据标签体系和数字身份认证体系，可以有效提升数据的可靠性和安全性。

02

- 研发AIGC幻觉治理技术和平台，可以定期清理幻觉数据，降低人工智能幻觉出现的概率，提升生成内容的可靠性。



05、网络谣言和网络暴力治理 -营造清朗网络空间

网络谣言和网络暴力治理提案概览

1、全国人大代表、格力电器董事长董明珠：一是尽快全面修订《中华人民共和国网络安全法》；二是国家网信办尽快出台《网络谣言、网络暴力信息互联网平台治理规定》；三是在拟出台的新《治安管理处罚法》中新增对网络谣言、网络暴力信息的分类界定与处罚条款；四是两高尽快出台统一的专门针对网络谣言、网络暴力信息犯罪行为的司法解释；建议最高人民法院出台专门针对网络谣言、网络暴力信息民事侵权的司法解释。

2、全国政协委员、中华全国律师协会监事长吕红兵：呼吁加快制定反网络暴力法，充分借鉴反电信网诈立法实践，制定统一的反网络暴力法，推进网暴治理模式从碎片化到体系化、提高网暴治理整体效能。

网络谣言和网络暴力治理的挑战与应对



法律法规的完善

- 网络谣言和网络暴力的治理需要完善的法律法规支持。提案建议全面修订《中华人民共和国网络安全法》，并出台专门的治理规定和司法解释，明确网络谣言和网络暴力的定义、分类及处罚标准。
- 通过明确网络暴力的定义和分类，可以为执法部门提供明确的依据，有效打击网络暴力行为。



平台责任与治理机制

- 互联网平台在治理网络谣言和网络暴力中承担重要责任。提案建议平台应加强对网络信息的审核和管理，建立健全治理机制，及时发现和处理网络谣言和网络暴力信息。
- 社交平台可通过引入人工智能技术，对网络暴力信息进行实时监测和处理，有效减少了网络暴力事件的发生。

网络谣言和网络暴力治理的挑战与应对



网络谣言和网络暴力的治理需要全社会的共同参与。通过加强宣传教育，提高公众的法律意识和网络素养，可以有效减少网络谣言和网络暴力的发生。

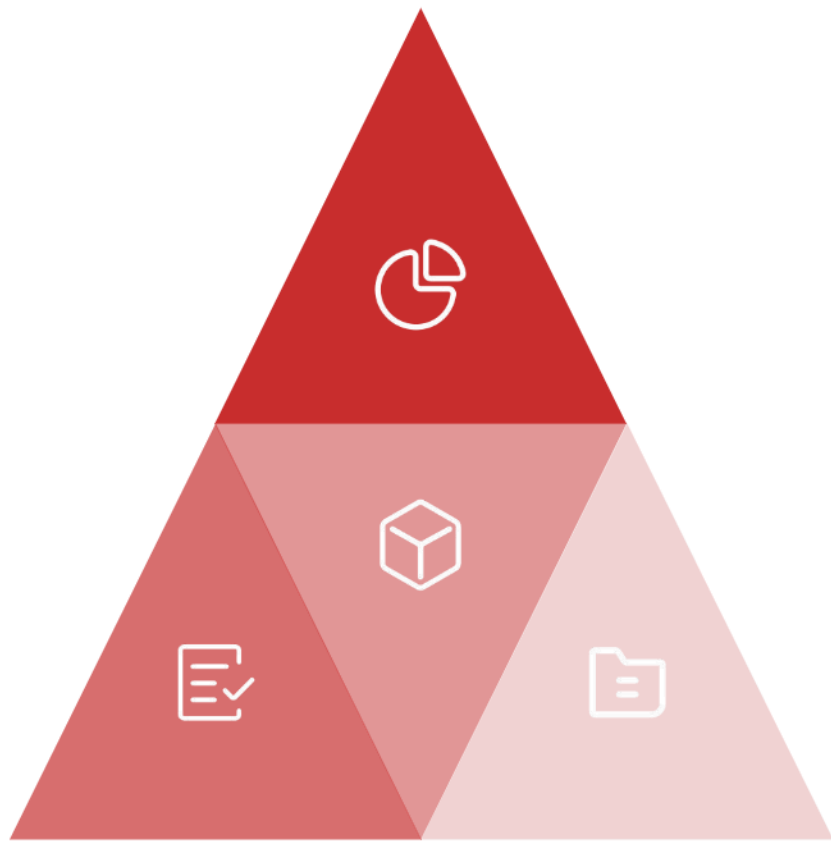
可通过开展网络素养教育活动，引导公众理性表达，抵制网络谣言和网络暴力，营造清朗的网络空间。



06、结语

-共筑网络安全防线

网络安全的重要性与紧迫性



网络安全的全局影响

- 网络安全不仅是技术问题，更是社会稳定、经济发展和个人权益的重要保障。随着数字化进程的加速，网络安全的重要性日益凸显，成为全社会共同关注的焦点。
- 从关键信息基础设施的安全防护到个人隐私的保护，网络安全贯穿于社会的各个层面，影响着每一个人的生活和工作。

网络安全的未来展望

- 面对日益复杂的网络安全形势，需要不断加强技术创新，完善法律法规，提升公众意识，共同构建网络安全防线。
- 通过加强国际合作，分享网络安全经验和最佳实践，可以更好地应对全球性的网络安全挑战，推动数字化的健康发展。

共同行动与责任担当

政府与企业的责任

- 政府部门应加强网络安全监管，制定和完善相关法律法规，推动网络安全技术创新和产业发展。企业应积极履行社会责任，加强网络安全防护能力，保护用户数据和隐私。
- 政府通过出台相关政策，鼓励企业加大网络安全投入，推动网络安全产业的发展。企业则通过加强技术研发和管理，提升自身的网络安全防护水平。

公众的参与和责任

- 公众应提高网络安全意识，增强自我保护能力，积极参与网络安全治理。
- 通过开展网络安全宣传活动，引导公众正确使用网络，保护个人信息，抵制网络谣言和网络暴力，营造清朗的网络空间。



共同行动与责任担当

- 网络安全是全球性问题，需要国际社会的共同努力。通过加强国际合作，分享网络安全经验和最佳实践，可以更好地应对全球性的网络安全挑战，推动数字化的健康发展。



- 各国可以通过建立网络安全合作机制，共同打击跨国网络犯罪，保护全球网络空间的安全和稳定。

The background features a scenic view of the Great Wall of China winding across mountains at sunset. The sky is a mix of blue, orange, and red. A large, flowing red ribbon is draped across the top right and bottom of the image. Two bright starburst effects are visible: one on the left near the wall and one on the right near the text.

谢谢

Thank you

《网络数据安全管理条例》 解读



CONTENTS

目录

01 条例出台的背景与目标

02 重要条款解读与分析

03 条例执行与分工

04 条例颁布的积极意义

05 挑战与展望

06 名词解释

01

条例出台的背景与目标



条例出台背景

数字化时代数据的重要性

在数字化时代，数据已成为重要的生产要素，推动经济和社会发展。从电商购物到智能交通，数据贯穿各个领域，成为创新的关键资源。

数据泄露、滥用等事件频发，严重威胁个人隐私与国家安全。近年来，多起数据泄露事件导致大量用户信息被非法利用。



国家立法加强数据安全监管

国家通过立法加强数据安全监管，保障个人、企业与国家利益。《网络数据安全管理条例》为数据安全提供了明确的法律依据。

法律依据：《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等。

实施时间：2025年1月1日。

条例适用范围与核心目标

适用范围

在境内开展网络数据处理活动及其安全监督管理。

在境外处理中华人民共和国境内自然人个人信息的活动，符合《中华人民共和国个人信息保护法》第三条第二款规定情形的。

在境外开展网络数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

核心目标

规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，明确法律责任和处罚措施，维护国家安全和公共利益。

02

重要条款解读与分析



个人信息保护的有关规定 (第三章 第二十一条、第二十二条)

➤ **第二十一条：**网络数据处理者在处理个人信息前，通过制定个人信息处理规则的方式依法向个人告知的，个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、清晰易懂。

第二十二条：网络数据处理者基于个人同意处理个人信息的，应当遵守下列规定：

- （一）收集个人信息为提供产品或者服务所必需，不得超范围收集个人信息，不得通过误导、欺诈、胁迫等方式取得个人同意；
 - （二）处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的，应当取得个人的单独同意；
 - （三）处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意；
 - （四）不得超出个人同意的个人信息处理目的、方式、种类、保存期限处理个人信息；
 - （五）不得在个人明确表示不同意处理其个人信息后，频繁征求同意；
 - （六）个人信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。
- 法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

解读：

第二十一条，明确通过制定个人信息处理规则履行告知义务的内容、形式等要求。

第二十二条，明确基于个人同意处理个人信息应当遵守的基本要求。

个人信息保护的有关规定 (第三章 第二十三条、第二十六条、第二十八条)

- **第二十三条：**个人请求查阅、复制、更正、补充、删除、限制处理其个人信息，或者个人注销账号、撤回同意的，网络数据处理者应当及时受理，并提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件限制个人的合理请求。
- **第二十六条：**中华人民共和国境外网络数据处理者处理境内自然人个人信息，依照《中华人民共和国个人信息保护法》第五十三条规定在境内设立专门机构或者指定代表的，应当将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市级网信部门；网信部门应当及时通报同级有关主管部门。

- **第二十八条：**网络数据处理者处理1000万人以上个人信息的，还应当遵守本条例第三十条。

解读：

第二十三条，明确行使个人信息查阅、复制、更正、补充、删除等权利的要求，细化个人信息转移的具体条件。

第二十六条，明确按照《中华人民共和国个人信息保护法》第五十三条规定在境内设立专门机构或者指定代表的要求。

第二十八条，明确网络数据处理者处理1000万人以上个人信息还应当履行的义务。

保障重要数据安全的有关规定
(第四章 第二十九条、第三十条)

➤ **第二十九条：**国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的网络数据进行重点保护。网络数据处理者应当按照国家有关规定识别、申报重要数据。对确认为重要数据的，相关地区、部门应当及时向网络数据处理者告知或者公开发布。网络数据处理者应当履行网络数据安全保护责任。

➤ **第三十条：**重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任：

- （一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；
- （二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；
- （三）受理并处理网络数据安全投诉、举报。

解读：

第二十九条，明确制定重要数据目录的要求，规定网络数据处理者识别、申报重要数据义务。

第三十条，规定网络数据安全负责人和网络数据安全管理机构责任。

条款解读

保障重要数据安全的有关规定 (第四章 第三十一条、第三十三条)

➤ **第三十一条：**重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，但是属于履行法定职责或者法定义务的除外。

风险评估应当重点评估下列内容：

- （一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；
- （二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；
- （三）网络数据接收方的诚信、守法等情况；
- （四）与网络数据接收方订立或者拟订立的相关合同中关于网络安全的要求能否有效约束网络数据接收方履行网络安全保护义务；
- （五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；
- （六）有关主管部门规定的其他评估内容。

➤ **第三十三条：**重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。

解读：

第三十一条，要求提供、委托处理、共同处理重要数据前进行风险评估，并明确重点评估内容。

第三十三条，要求重要数据的处理者每年度对其网络数据处理活动开展风险评估，并明确风险评估报告内容。

数据跨境流动机制的有关规定 (第五章 第三十四条、第三十五条)

➤ **第三十四条：**国家网信部门统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。

➤ **第三十五条：**符合下列条件之一的，网络数据处理者可以向境外提供个人信息：

- （一）通过国家网信部门组织的数据出境安全评估；
- （二）按照国家网信部门的规定经专业机构进行个人信息保护认证；
- （三）符合国家网信部门制定的关于个人信息出境标准合同的规定；
- （四）为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；
- （五）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息；
- （六）为履行法定职责或者法定义务，确需向境外提供个人信息；
- （七）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息；
- （八）法律、行政法规或者国家网信部门规定的其他条件。

解读：

第三十四条，明确国家网信部门统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。

第三十五条，明确符合法规中规定的八项条件之一的，网络数据处理者可以向境外提供个人信息。

条款解读

数据跨境流动机制的有关规定 (第五章 第三十七条-三十九条)

- **第三十七条：**网络数据处理者在中华人民共和国境内运营中收集和产生的重要数据确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。网络数据处理者按照国家有关规定识别、申报重要数据，但未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。
- **第三十八条：**通过数据出境安全评估后，网络数据处理者向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。

- **第三十九条：**国家采取措施，防范、处置网络数据跨境安全风险和威胁。任何个人、组织不得提供专门用于破坏、避开技术措施的程序、工具等；明知他人从事破坏、避开技术措施等活动的，不得为其提供技术支持或者帮助。

解读：

第三十七条、三十八条，明确网络数据处理者通过数据出境安全评估后向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。

第三十九条，规定了国家采取措施，防范、处置网络数据跨境安全风险和威胁。

网络平台服务提供者的有关规定
(第六章 第四十条、第四十二条)

➤ **第四十条：**网络平台服务提供者应当通过平台规则或者合同等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全保护。

预装应用程序的智能终端等设备生产者，适用前款规定。

第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。

国家鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端等设备生产者投保。

➤ **第四十二条：**网络平台服务提供者通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。预装应用程序的智能终端等设备生产者，适用前款规定。

解读：

第四十条，规定了网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者的网络数据安全保护义务，并要求提供应用程序分发服务的网络平台服务提供者建立应用程序核验规则并开展网络数据安全相关核验。

第四十二条，针对当前个性化推荐服务关闭难、收集个人信息类型多、个人精准画像数据滥用等问题，明确网络平台服务提供者应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。

条款解读

网络平台服务提供者的有关规定 (第六章 第四十三条、第四十六条)

➤ **第四十三条：**国家推进网络身份认证公共服务建设，按照政府引导、用户自愿原则进行推广应用。鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份信息。

➤ **第四十六条：**大型网络平台服务提供者不得利用网络数据、算法以及平台规则等从事下列活动：

- (一) 通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据；
- (二) 无正当理由限制用户访问、使用其在平台上产生的网络数据；
- (三) 对用户实施不合理的差别待遇，损害用户合法权益；
- (四) 法律、行政法规禁止的其他活动。

解读：

第四十三条，明确国家推进网络身份认证公共服务建设，按照政府引导、用户自愿原则进行推广应用。鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份信息。

第四十六条，明确大型网络平台服务提供者不得利用网络数据、算法、平台规则等从事的相关活动。

条款解读

责任分工的有关规定 (第七章 第四十七条-第四十九条)

- **第四十七条：**国家网信部门负责统筹协调网络数据安全和相关监督管理工作。公安机关、国家安全机关依照有关法律、行政法规和本条例的规定，在各自职责范围内承担网络数据安全监督管理职责，依法防范和打击危害网络数据安全的违法犯罪活动。国家数据管理部门在具体承担数据管理工作中履行相应的网络数据安全职责。各地区、各部门对本地区、本部门工作中收集和产生的网络数据及网络数据安全负责。
- **第四十八条：**各有关主管部门承担本行业、本领域网络数据安全监督管理职责，应当明确本行业、本领域网络数据安全保护工作机构，统筹制定并组织实施本行业、本领域网络数据安全事件应急预案，定期组织开展本行业、本领域网络数据安全风险评估，对网络数据处理者履行网络数据安全保护义务情况进行监督检查，指导督促网络数据处理者及时对存在的风险隐患进行整改。

- **第四十九条：**国家网信部门统筹协调有关主管部门及时汇总、研判、共享、发布网络数据安全风险相关信息，加强网络数据安全信息共享、网络数据安全风险和威胁监测预警以及网络数据安全事件应急处置工作。

解读：

第四十七条，规定了国家网信部门、公安机关、国家安全机、国家数据管理部门依照有关法律、行政法规和本条例的规定，在各自职责范围内承担网络数据安全监督管理职责，以及各地区、各部门对本地区、本部门工作中收集和产生的网络数据及网络数据安全负责。

第四十八条，明确各有关主管部门承担本行业、本领域网络数据安全监督管理责任。

第四十九条，规定了国家网信部门协调相关机构，及时汇总、研判、共享和发布网络数据安全风险信息，加强信息共享、风险监测预警及应急处置工作。

条款解读

法律责任的有关规定 (第八章 第五十五条-第五十七条)

- **第五十五条：**违反本条例第十二条、第十六条至第二十条、第二十二条、第四十条第一款和第二款、第四十一条、第四十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处100万元以下罚款，并可以责令暂停相关业务、停业整顿、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和其他直接责任人员可以处1万元以上10万元以下罚款。
- **第五十六条：**违反本条例第十三条规定的，由网信、电信、公安、国家安全等主管部门依据各自职责责令改正，给予警告，可以并处10万元以上100万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处1万元以上10万元以下罚款；拒不改正或者情节严重的，处100万元以上1000万元以下罚款，并可以责令暂停相关业务、停业整顿、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和其他直接责任人员处10万元以上100万元以下罚款。

- **第五十七条：**违反本条例第二十九条第二款、第三十条第二款和第三款、第三十一条、第三十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，可以并处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处1万元以上10万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处50万元以上200万元以下罚款，并可以责令暂停相关业务、停业整顿、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和其他直接责任人员处5万元以上20万元以下罚款。

解读：

第五十五条至第五十七条针对违反不同条款的行为，设定了从责令改正、警告到罚款、暂停业务、停业整顿、吊销许可证或营业执照等一系列行政处罚措施。处罚力度与违法行为的严重程度相匹配。

例如，第五十六条针对违反第十三条的行为，最高罚款可达1000万元，并可吊销营业执照，反映了对关键领域数据安全的高度重视。第五十七条则聚焦数据泄露等严重后果，最高罚款200万元，体现了对危害后果的针对性惩治。此外，对直接负责的主管人员和其他直接责任人员也规定了个人罚款，增强了法律的震慑力。

03

条例执行与分工



国家层面工作项

制度优化与规范

《管理条例》在融合《网络安全法》《数据安全法》《个人信息保护法》等法律法规的基础上，进一步优化了国家层面针对网络数据安全制度的有关规定。具体包括鼓励创新应用、加强网络数据安全防护能力建设、开展网络数据安全宣传和人才培养等。

《管理条例》延续了《数据安全法》自上而下的重要数据目录制定方式，规定了国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强了对重要数据的保护。各地区、各部门应确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的网络数据进行重点保护。

01

个人信息量级规范

《管理条例》将个人信息类重要数据的认定数量门槛从100万提升为1000万，明确网络数据处理者处理1000万人以上个人信息的，还应当履行重要数据的处理者的安全保障义务。解决了当前对于个人信息量级的模糊之处，减轻了处理百万级别的非头部或超大型网络服务提供者的合规义务。

02

企业层面工作项

重要数据处理者义务

明确网络安全负责人，负责制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案。规定重要数据处理者应履行识别申报义务、风险评估义务，确保网络数据安全。

对于发生网络数据安全事件，企业应立即启动预案、按规定报告主管业务部门、通知相关权益受损方、对涉嫌犯罪活动依规定报案，并配合开展侦查、调查和处置工作。

01



02

一般网络数据处理者义务

《管理条例》定义“网络数据处理者”，是指在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。明确了网络数据处理者在网络数据安全、应急处理、通知与报告、人工智能训练数据合规、个人信息展示、告知、同意等方面的具体义务。

企业需建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用。

个人层面工作项

个人行为规范

《管理条例》第八条规定，任何个人不得利用网络数据从事非法活动。不得从事窃取或者以其他非法方式获取网络数据、非法出售或者非法向他人提供网络数据等非法网络数据处理活动。

禁止提供非法帮助

不得提供专门用于从事非法活动的程序、工具。不得为其提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助。

个人权利保护

《管理条例》在结合行业实践的基础上进一步细化了《个人信息保护法》关于告知同意、个人信息权利等有关规定。明确进行告知的具体内容及形式的要求，明确个人信息“可携带权”的具体落实。

04

条例颁布的积极意义



条例颁布的积极意义

法规支撑与规范框架

作为网络数据安全领域的首个行政法规级别的文件，《管理条例》为网络数据安全提供了法规层面的支撑，为网络数据安全行为的规范化、制度化提供了清晰的框架。



提升安全意识与产业发展

有助于提升整个社会的网络数据安全意识，促进网络数据安全产业的健康发展，推动网络数据安全技术的研发和应用，提高网络数据安全防护水平。



国际交流与合作

《管理条例》积极参与网络数据安全相关国际规则和标准的制定，促进国际交流与合作，提升我国在网络数据安全领域的国际影响力和话语权，为我国网络数据安全产业发展创造良好的国际环境。



05

挑战与展望



面临的挑战与展望

01

部门协调问题

部门之间存在“九龙治水”的问题，造成实践中各种管理权争夺或者推诿的问题，有待在实践中进一步得到解决。需要进一步明确各部门在网络数据安全监督管理中的职责分工，建立健全协同监管机制。



02

社会参与与共治

网络数据安全不仅是政府的责任，也需要全社会的共同参与。加强网络数据安全宣传教育，提高公众的网络数据安全意识 and 自我保护能力，形成政府、企业、社会组织和公众共同参与的网络安全共治格局。



03

技术与监管适应

随着网络技术的快速发展，新的网络数据安全问题不断涌现，对监管提出了更高的要求。监管部门需要不断更新监管技术和手段，提高监管的科学性和有效性，以适应网络安全形势的变化。



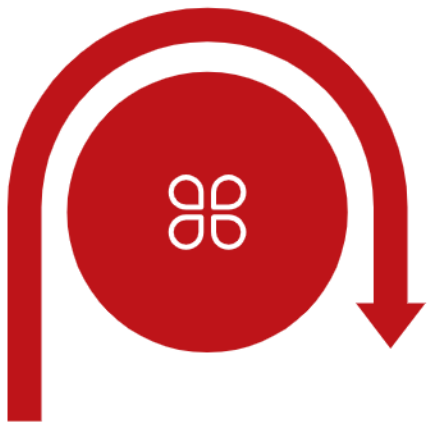
苏州大学

06

名词解释



名词解释



网络数据

通过网络处理和产生的各种电子数据。

单独同意

个人针对其个人信息进行特定处理而专门作出具体、明确的同意。

重要数据

特定领域、群体、区域或达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。



网络数据处理活动

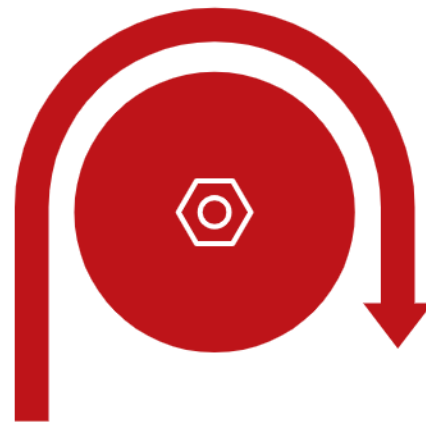
网络数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

委托处理

网络数据处理者委托个人、组织按照约定的目的和方式开展的网络数据处理活动。

大型网络平台

注册用户5000万以上或者月活跃用户1000万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。



网络数据处理者

在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。

共同处理

两个以上的网络数据处理者共同决定网络数据的处理目的和处理方式的网络数据处理活动。

数据分类分级

数据分类分级是根据数据的属性特征、敏感程度和安全影响，将其划分为不同类别和级别的系统性管理方法，旨在平衡数据利用与安全防护。

谢谢大家



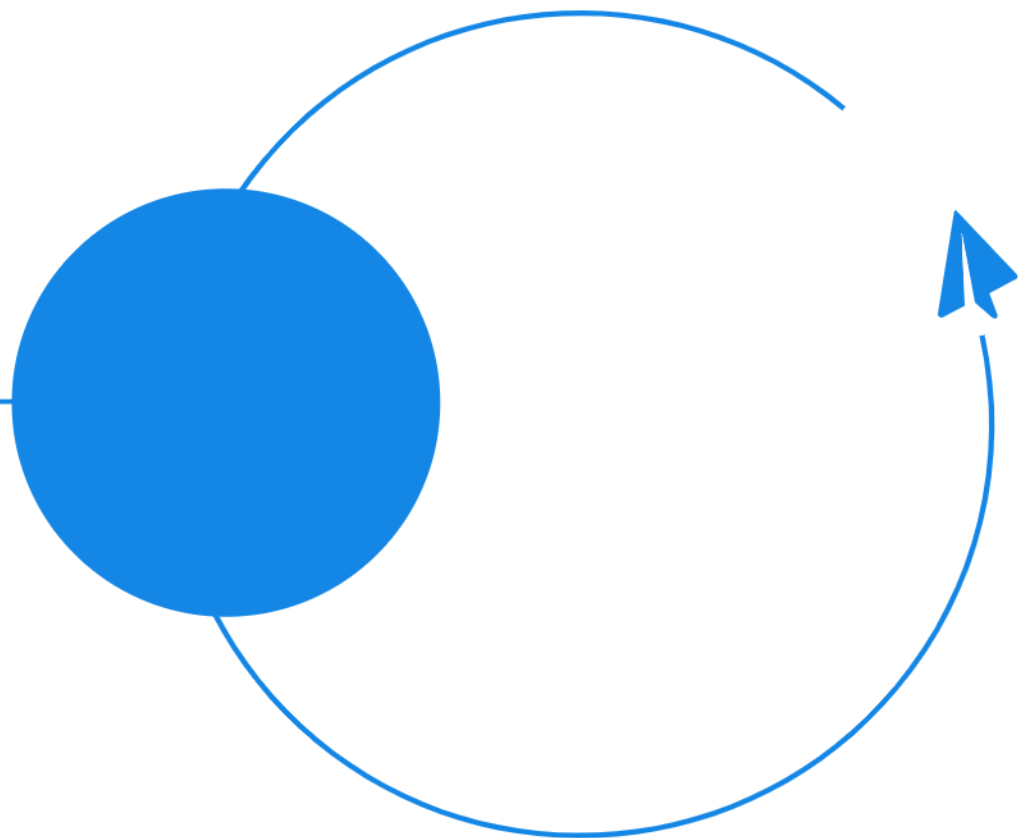
推进软件正版化 共建安全创新校园



目录

CATALOGUE

-
- 01. 什么是软件正版化
 - 02. 法律保护与侵权后果
 - 03. 为什么要使用正版软件
 - 04. 如何区分正版软件
 - 05. 推进软件正版化，我们在行动



PART 01

什么是软件正版化



软件正版化的定义



高校软件正版化

高校软件正版化，指的是在高校范围内，于教学、科研、行政办公等各类活动中，所使用的计算机软件均为通过合法授权途径获取的正版产品。这涵盖操作系统(如Windows、Mac OS)、办公软件(如Microsoft Office、WPS)、教学专用软件以及科研相关软件（如数据分析软件、仿真模拟软件）等。正版化强调的是软件使用的合法性、规范性，杜绝任何未经授权的复制、使用或传播盗版软件的行为。



正版软件

正版软件是指由合法的软件开发者或拥有者授权，并按照其规定的许可协议进行销售和分发的软件产品。这类软件产品提供完整的功能，包括但不限于全部功能模块、用户手册、更新支持以及客户服务等。

校园推进软件正版化工作，既是防范计算机病毒、保障信息安全的技术基础，也是规范计算机系统管理、提升信息化建设水平的重要途径，更是高校履行知识产权保护义务、营造良好创新生态环境的必然要求。

PART 02

法律保护与侵权后果



法律保护与侵权后果



知识产权保护的 legal 框架

我国《著作权法》明确规定，计算机软件属于著作权保护的对象，软件开发者对其开发的软件享有著作权。未经软件著作权人许可，复制、发行、传播其软件的行为构成侵权。



侵权行为的法律责任

对于侵权行为，侵权人需承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任。

情节严重的侵权行为，还可能构成侵犯著作权罪，依法追究刑事责任。



企业与个人的法律责任

企业使用盗版软件，不仅面临巨额赔偿，还可能影响企业声誉和市场竞争力。

个人使用盗版软件，同样构成侵权，需承担相应法律责任，且可能面临法律制裁。

法律保护与侵权后果



教育部规定

2024年11月25日，教育部、国家版权局共同发布了《关于做好教育系统软件正版化工作的通知》，明确将加强和完善教育系统软件正版化工作的长效机制，提升软件正版率，加强师生版权保护意识，营造尊重知识产权的良好环境。



师生的法律义务

师生在使用软件时，应自觉遵守法律法规，使用正版软件，避免因使用盗版软件而面临法律风险。师生有责任维护学校的良好形象，积极参与学校的软件正版化工作，共同营造良好的校园文化环境。

PART 03

为什么要使用正版软件



符合法律要求

严格遵守著作权法相关法规要求，切实维护软件著作权人的合法权益，保障其在软件开发、传播及商业化过程中的正当权利，为软件产业健康有序发展提供法治化保障。

通过合法使用正版软件，既能充分尊重创作者的智力成果，也有利于营造公平竞争的市场环境，从而激发行业创新活力，推动软件产业可持续发展。

若使用盗版软件，不仅直接违反著作权法中对软件作品的保护规定，严重损害权利人的经济利益与创作积极性，更与我国“实施创新驱动发展战略”“加快建设创新型国家”的核心方针背道而驰。同时，盗版行为将扰乱软件市场定价机制与供需平衡，导致“劣币驱逐良币”的恶性循环，最终破坏整个产业链的良性生态，阻碍产业升级与高质量发展进程。



保障信息安全



防范恶意程序

正版软件经过严格的安全检测，能够有效防止恶意软件和病毒的攻击，保护用户的数据安全和隐私。

盗版软件可能携带病毒、木马等恶意程序，容易导致用户电脑被攻击，个人隐私和重要数据泄露。

例如：盗版Photoshop安装包曾携带隐蔽的加密货币挖矿程序，导致电脑性能骤降、硬件寿命缩短。

另外部分盗版软件伪装成激活工具（如“KMS激活器”），实际为远程控制木马，可窃取用户隐私。



保障信息安全



确保持续安全更新

正版软件可通过官方渠道自动获取补丁，例如：

- 操作系统：微软每月发布“Patch Tuesday”修复高危漏洞。
- 专业软件：Adobe定期更新PDF阅读器的零日漏洞防护。

盗版软件因无法更新，长期暴露于已知漏洞中。2017年“WannaCry”病毒通过Windows漏洞传播，全球超20万台设备被加密勒索。

据赛门铁克报告，未打补丁的软件被攻击概率是已打补丁的3.5倍。



保障信息安全



保障数据隐私与完整性

盗版软件可能内置键盘记录器或屏幕监控程序，
例如：

- 键盘记录：盗版游戏修改器窃取Steam账号密码。
- 文件窃取：某设计公司使用盗版AutoCAD，图纸文件被自动上传至第三方服务器。

正版软件通过加密传输（如SSL）和本地数据保护机制降低风险。



维护系统稳定性

避免崩溃与兼容性问题。

盗版软件因破解不完整，常导致功能异常或系统冲突。

正版软件通过严格兼容性测试，适配主流硬件与操作系统。



享受优质服务



免费更新与技术支持

正版软件用户可享受软件开发商提供的免费更新服务，确保软件始终处于最新状态。如Microsoft Update可帮助用户更新Windows系统及其他Microsoft程序，提高系统性能和安全性。



售后服务保障

正版软件用户在使用过程中遇到问题，可获得软件开发商的专业技术支持和售后服务。盗版软件用户则无法享受这些服务，一旦出现问题，只能自行解决，增加了使用成本。



个性化服务与定制

正版软件开发商可根据用户需求提供个性化服务和定制开发，满足用户的特殊需求。这种定制服务可提高软件的适用性和用户体验，为企业和个人带来更大的价值。

PART 04

如何识别正版软件



如何识别正版软件

01

软件来源渠道

- 对于常见的软件，如操作系统、办公软件、浏览器等，应该从其官方网站下载。
- 对于一些开源软件，也要从其官方的开源代码托管平台（如GitHub、GitLab等）或者官方网站下载。
- 对于移动APP，要选择正规的软件商店下载。

02

产品密钥验证

正版软件通常会在安装或首次使用时要求输入产品密钥。这个密钥是独一无二的，只有正版软件才能提供。输入密钥后，软件会连接到官方服务器进行验证。如果是正版软件，验证过程会顺利通过，否则会提示密钥无效或盗版。

03

官方认证标志

- 包装标志：正版软件的包装盒上通常会有官方认证标志或防伪标签。这些标志是盗版软件无法复制的。
- 电子标志：在软件的关于页面或设置中，通常可以找到官方认证的数字标志或链接，点击后会跳转到官方认证页面。

如何识别正版软件

04

软件许可证协议

- 阅读协议：安装软件时，系统会弹出软件许可证协议。正版软件的协议内容详细、合法，并且与官方网站上的协议内容一致。
- 法律声明：正版软件的许可证协议中会包含法律声明，说明用户的权利和义务，盗版软件通常没有这些内容。

05

技术支持和更新服务

- 官方技术支持：正版软件用户可以享受官方提供的技术支持服务，包括在线客服、电话支持和邮件支持等。
- 自动更新：正版软件会定期推出更新，修复漏洞和添加新功能。通过自动更新功能，可以验证软件的正版性。

PART 05

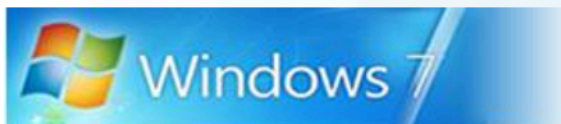
推进软件正版化，我们 在行动



学校目前有哪些正版软件



操作系统类软件：Windows系列操作系统



办公类软件：Office系列软件

Microsoft Office：2010、2013、2016、2019、2021

Microsoft Office for Mac：2011、2016、2019、2021



Microsoft
Office 2019 for MAC



杀毒软件：天融信杀毒软件



如何获取

在数据资源与信息化建设管理处网站上的“软件”栏目里即可下载上述软件：

<https://its.suda.edu.cn/wrzbrjfw/list.htm>



its.suda.edu.cn/wrzbrjfw/list.htm

苏州大学 SOOCHOW UNIVERSITY 数据资源与信息化建设管理处 Office of Data and Information Management

站内搜索/search 搜索 旧版回顾

开始 GET STARTED 服务 SERVICE 软件 SOFTWARE 信息安全 SECURITY 关于我们 ABOUT US

首页

软件 > 微软正版软件服务 > 软件下载

微软正版软件服务

软件下载

激活与帮助

工具与其他服务

杀毒软件

安装完成后须用激活工具激活

Windows 7

Microsoft Windows 7 Enterprise with sp1 [Windows 7 企业版]

这个版本的主要对象是企业用户以及其市场，通过大量授权给与与微软签订软件授权合约的公司；同时有一个大量授权的产品密钥，必须通过其激活。这个版本不会通过零售以及OEM贩卖。它提供的功能包含多国语言用户接口包、BitLocker设备加密以及UNIX应用程序的支持。

>> [64bit \[English\]](#)

>> [32bit \[English\]](#)

>> [64bit \[中文版\]](#)

>> [32bit \[中文版\]](#)

联系我们 GET HELP

服务热线: 65880000 (内线80000)

办公地点:

天赐庄校区: 东校区教育超市北

独墅湖校区: 独墅湖一期304号楼5楼

阳澄湖校区: 行政楼401房间

未来校区: 未来校区教学中心628办公室

办公时间:

周一至周五 (8:00—12:00, 13:30—17:00)

周末及节假日 (8:30—11:30, 14:00—17:00, 仅天赐庄校区)

Windows 10

如何安装激活

校园正版软件有不同的安装激活办法，在“软件” 页面中即可查看详细的安装和激活说明。

- Windows系统和Office软件：“微软正版软件服务” → “激活与帮助”，下载KMS激活工作，安装后需运行激活工具进行激活。
- 天融信杀毒软件：“软件” → “其他服务”。



谢谢大家！

