



中共上海市委网络安全和信息化
委员会办公室



2026
CHINA CYBERSECURITY WEEK

国家网络安全宣传周 上海地区活动

// 网络安全宣传手册



CONTENTS

目录



1	习近平总书记关于网络安全的重要论述	01
2	网信工作“十个坚持”重要原则	02
3	网络安全相关法律法规	03
4	案例解析	05
5	AI时代新视点	21



习近平总书记关于网络安全的重要论述

2025年11月28日，
习近平在中共中央政治局第二十三次集体学习时强调：

源清则流清，要坚持以正面声音、主流价值、时代新风塑造网络空间，使互联网成为思想引领、道德培育、文化传承的重要阵地。

2023年11月8日，
习近平向2023年世界互联网大会乌镇峰会开幕式发表视频致辞：

互联网日益成为推动发展的新动能、维护安全的新疆域、文明互鉴的新平台，构建网络空间命运共同体既是回答时代课题的必然选择，也是国际社会的共同呼声。我们要深化交流、务实合作，共同推动构建网络空间命运共同体迈向新阶段。

2018年4月20日，
习近平在全国网络安全和信息化工作会议上的讲话：

网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点，让人民群众在信息化发展中有更多获得感、幸福感、安全感。

2016年4月19日，
习近平在网络安全和信息化工作座谈会上的讲话：

网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

网信工作“十个坚持”重要原则



坚持党管互联网

坚持网信为民

坚持走中国特色治网之道

坚持统筹发展和安全

坚持正能量是总要求、管得住是硬道理、用得好是真本事

坚持筑牢国家网络安全屏障

坚持发挥信息化驱动引领作用

坚持依法管网、依法办网、依法上网

坚持推动构建网络空间命运共同体

坚持建设忠诚干净担当的网信工作队伍

党的十八大以来，我国网络安全和信息化事业取得重大成就，党对网信工作的领导全面加强，网络空间主流思想舆论巩固壮大，网络综合治理体系基本建成，网络安全保障体系和能力持续提升，网信领域科技自立自强步伐加快，信息化驱动引领作用有效发挥，网络空间法治化程度不断提高，网络空间国际话语权和影响力明显增强，网络强国建设迈出新步伐。



网络安全相关法律法规

国家网络安全相关法律法规

《中华人民共和国网络安全法》：网络空间基础性法律，确立网络安全等级保护、关键信息基础设施保护等核心制度。

《中华人民共和国数据安全法》：规范数据处理活动的法律，建立数据分类分级等制度，保障数据安全，促进数据依法有序流动。

《中华人民共和国个人信息保护法》：保护个人信息权益的法律，规范个人信息处理活动，落实核心规则，守护个人隐私。

《中华人民共和国密码法》：规范密码应用和管理，促进密码事业发展，保障网络与信息安全，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。

《中华人民共和国反电信网络诈骗法》：打击电信网络诈骗的法律，构建多部门联动治理体系，保护公民财产安全和合法权益。

《关键信息基础设施安全保护条例》：保障关键信息基础设施安全的行政法规，明确运营者安全责任，提升重点行业和领域的网络安全防护能力。

《网络数据安全管理条例》：规范网络数据处理活动的行政法规，细化数据分类分级、风险评估等制度，防范网络数据安全风险。

《商用密码管理条例》：规范商用密码应用与管理的行政法规，健全商用密码产业发展制度，保障网络与信息安全，维护国家安全和社会公共利益。



网络安全相关法律法规

国家网络安全相关法律法规

《未成年人网络保护条例》：保护未成年人网络空间权益的行政法规，规定防沉迷、个人信息保护等制度，营造有利于未成年人健康成长的网络环境。

《关键信息基础设施商用密码使用管理规定》：规范关键信息基础设施商用密码使用的部门规章，健全商用密码应用管理机制，保护关键信息基础设施安全。

《网络安全审查办法》：开展网络安全审查的部门规章，评估关键信息基础设施采购活动的安全风险，保障供应链安全，维护国家安全。

《生成式人工智能服务管理暂行办法》：规范生成式人工智能服务的部门规章，明确服务提供者的安全义务，防范内容风险，促进人工智能健康发展。

上海地方性法规

《上海市数据条例》：规范和促进数据流通交易、保障数据安全的地方性法规，建立数据权益保护、数据流通等制度，赋能城市数字化转型。

《上海市促进人工智能产业发展条例》：立法立足于促进法的基本定位，注重创新性和引领性，充分发挥有效市场和有为政府的作用，采取各种激励措施推动人工智能产业高质量发展。这也是上海继《上海市数据条例》后的第二部数字经济领域地方法规。



案例解析



案例一

2025年，媒体调查发现，某AI陪伴APP存在突出的未成年人保护漏洞。该平台AI智能体内容生成环节存在不良低俗等违规内容，危害未成年人身心健康。属地网信部门依法约谈运营企业，责令立即整改，健全AI生成合成内容审核机制，加强涉未成年人不良内容的整治清理，维护清朗网络空间。



面向校园群体

法律法规条例：

1.《中华人民共和国网络安全法》

第二十条 国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。

2.《未成年人网络保护条例》

第二十五条 任何组织和个人不得向未成年人发送、推送或者诱骗、强迫未成年人接触含有危害或者可能影响未成年人身心健康内容的网络信息。

“沪”航安全指南：

1.家长应主动了解掌握孩子使用的生成式AI产品的使用内容，若发现有不良内容，应及时制止孩子使用，并与孩子耐心沟通。

2.家长应教育孩子不要向AI透露姓名、家庭住址、银行卡号等个人敏感信息。

3.AI平台须严格履行内容审核责任，禁止生成、推送不良内容。



<https://mp.weixin.qq.com/s/X9cFX9Eaw0BLbMdxV9GbKg>



案例解析



案例二

在某高校反诈课堂上，某检察院检察官引用了一起真实办案案例：诈骗分子提前在网上搜集辅导员照片和线上会议视频素材，利用AI换脸技术和声音克隆技术，生成高度仿真的视频材料，并通过其他非法渠道定位到特定学生的联系信息。随后，诈骗分子用伪造的视频直接与目标学生建立联络，利用学生对辅导员身份的天然信任感设局，一个电话就骗走了1.2万元学费。



展示图片均由ai模组生成

面向校园群体

法律法规条例：

1.《中华人民共和国个人信息保护法》

第二十八条 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，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

2.《生成式人工智能服务管理暂行办法》

第四条 提供和使用生成式人工智能服务，应当遵守法律、行政法规，尊重社会公德和伦理道德，遵守以下规定：

（一）坚持社会主义核心价值观，不得生成煽动颠覆国家政权、推翻社会主义制度，危害国家安全和利益、损害国家形象，煽动分裂国家、破坏国家统一和社会稳定，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，暴力、淫秽色情，以及虚假有害信息等法律、行政法规禁止的内容；

（二）在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取有效措施防止产生民族、信仰、国别、地域、性别、年龄、职业、健康等歧视；

（三）尊重知识产权、商业道德，保守商业秘密，不得利用算法、数据、平台等优势，实施垄断和不正当竞争行为；

（四）尊重他人合法权益，不得危害他人身心健康，不得侵害他人肖像权、名誉权、荣誉权、隐私权和个人信息权益；

（五）基于服务类型特点，采取有效措施，提升生成式人工智能服务的透明度，提高生成内容的准确性和可靠性。

“沪”航安全指南：

1.接到转账请求，先挂断，再用自己的通讯录回拨确认，或问一句只有你们知道的“暗号”。

2.学校教师、辅导员在收集学生个人信息后，应当妥善保管防止泄露，不得在互联网上公开收集到的个人信息。

3.如已转账，需立刻联系银行冻结账户，同时保留转账记录。

<http://www.shzfz.net/article/4486/380df92100474d26bc6e133c8d5ac5b9>



案例解析



案例一

2025年，某知名品牌因违规向境外总部传输中国区用户个人信息被公安网安部门查处。经查，该公司存在三项违法事实：一是未通过数据出境安全评估、订立个人信息出境标准合同或通过个人信息保护认证，违规向其总部传输用户个人信息。二是向总部提供用户个人信息前，未向用户充分告知其个人信息境外接收方的处理方式，未取得用户“单独同意”。三是未对收集的个人信息采取加密、去标识化等安全技术措施。属地公安机关依据《中华人民共和国个人信息保护法》依法给予行政处罚，为跨国企业数据出境合规敲响了警钟。



面向企业群体



法律法规条例：

1. 《中华人民共和国个人信息保护法》

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

- (一) 依照本法第四十条的规定通过国家网信部门组织的安全评估；
- (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) 按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

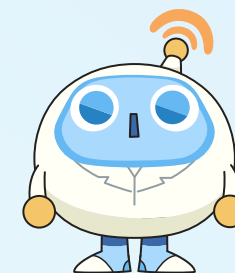
(四) 法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

“沪”航安全指南：

- 1. 企业向境外传输用户信息前，应完成数据出境安全评估或认证，并取得用户单独同意。
- 2. 企业应对出境个人信息采取加密、去标识化等安全措施，并定期开展合规自查。
- 3. 市民在注册或下单前，请仔细阅读隐私政策，是否存在“数据出境”条款，了解个人信息流向。



https://m.gmw.cn/2025-09/09/content_1304141463.htm



案例解析



案例二

某企业主营业务是为物流行业提供技术开发和运维服务。工作中发现，涉案企业开放数据库9200端口向公共网络传输大量业务数据，导致其包含部分敏感个人信息的数据疑似被境外可疑IP访问窃取。经查，企业未开展网络安全等级保护测评，涉事系统相关信息未采取加密、访问控制、端口安全策略等防护技术措施，存在未授权访问漏洞，存在数据泄露风险。网信部门依法责令企业限期改正，并予以警告、罚款处罚。



面向企业群体

法律法规条例：

1.《网络数据安全管理条例》

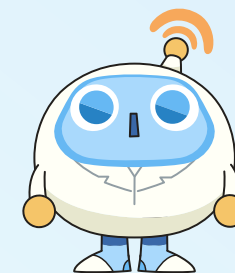
第九条 网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，并对所处理网络数据的安全承担主体责任。

2.《中华人民共和国密码法》

第二条 本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

“沪”航安全指南：

- 1.企业应定期排查数据库端口，关闭不必要的公网访问，避免数据直接暴露。
- 2.企业要设置严格的访问控制，落实网络安全等级保护测评，堵住管理漏洞。
- 3.市民选择物流服务时可隐藏面单上的姓名、电话、地址，优先选择有数据加密承诺和安全资质的平台。



https://mp.weixin.qq.com/s/W_EDyn0NIltRW072L7dVyA



案例解析



案例一

2026年3月，某地一位独居老人接到一通自称“医保局”的电话，对方称其名下有两个医保账户需注销一个，否则将影响医保使用。电话随后被转接至“经侦民警”，对方准确说出她的个人信息。老人信以为真，在对方的诱导下，一步步填写了银行卡信息、取消免密支付、输入密码，配合人脸录入，并下载了一款某远程操控软件，对方声称用于账户安全检测。案发时已有近6万元资金被转走，但因处置及时，200余万元养老存款得以保全。



展示图片均由ai模组生成

面向银龄群体

法律法规条例：

1. 《中华人民共和国网络安全法》

第四十三条 网络运营者收集、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。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

2. 《中华人民共和国反电信网络诈骗法》

第二十九条 个人信息处理者应当依照《中华人民共和国个人信息保护法》等法律规定，规范个人信息处理，加强个人信息保护，建立个人信息被用于电信网络诈骗的防范机制。

履行个人信息保护职责的部门、单位对可能被电信网络诈骗利用的物流信息、交易信息、贷款信息、医疗信息、婚介信息等实施重点保护。公安机关办理电信网络诈骗案件，应当同时查证犯罪所利用的个人信息来源，依法追究相关人员和单位责任。

“沪”航安全指南：

- 1.凡是来电自称官方工作人员要求转账或其他行为，须保持戒备，并拨打官方电话进行核实。
- 2.不要随意让陌生人对手机进行远程操作。
- 3.不要向任何陌生来电提供银行卡信息、配合人脸录入等操作。
- 4.收集个人信息的组织、个人，应当加强对个人信息泄露风险的防范。



<https://www.jfdaily.com/wx/detail.do?id=1090119>



案例解析



案例二

2024年起，一团伙身着某通信公司制服，在某地多个村镇以“通信公司做活动，办卡送米送油”为名，专门针对农村老人实施诈骗。江某要求老年人提供身份证、配合人脸认证办理手机卡，声称“只为完成公司指标，办完就销毁”。为打消顾虑，当面掰断一张废卡谎称“卡已销毁”，实际上，真正开通的手机卡已被截留，江某将截留的手机卡以每张约200元的价格出售，用于批量注册APP网络账号。截至案发，6000余名老人被骗完成人脸认证，江某被依法提起公诉。



展示图片均由ai模组生成

面向银龄群体

法律法规条例：

1. 《中华人民共和国个人信息保护法》

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

2. 《中华人民共和国网络安全法》

第四十六条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

“沪”航安全指南：

- 1.人脸信息十分重要，一旦泄漏无法补救。切勿为“一点小利”随意配合陌生人刷脸，不轻信“当面掰断废卡”等伪装操作。
- 2.看到“送米送油”等街头活动，先核实主办单位真实身份，不轻易交出身份证和手机供他人操作。
- 3.子女应及时提醒父母保护个人信息，避免造成不可逆的损失。



https://law.cnr.cn/zx/20251004/t20251004_527385421.shtml



案例解析



案例一

2026年5月，某地检察机关接到志愿者反映，当地智慧停车管理平台存在信息泄露隐患。经查，该平台注册用户七万余人，联网本地区五百余个停车场，留存1600万余条车辆停车轨迹、缴费记录等敏感信息，用户仅输入车牌号即可无验证查询他人完整行踪，平台存储的敏感个人信息未落实安全防护，未做脱敏处理，存在大规模个人信息泄露风险。检察机关随即启动行政公益诉讼，联合相关部门督促平台增设身份核验功能。整改后，平台已隐藏原始停车记录，敏感信息完成去标识化处理，消除信息“裸奔”隐患。



展示图片均由ai模组生成

面向全体市民

法律法规条例：

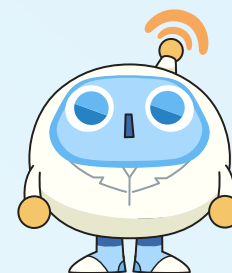
《中华人民共和国个人信息保护法》

第五十一条 个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

- (一) 制定内部管理制度和操作规程；
- (二) 对个人信息实行分类管理；
- (三) 采取相应的加密、去标识化等安全技术措施；
- (四) 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；
- (五) 制定并组织实施个人信息安全事件应急预案；
- (六) 法律、行政法规规定的其他措施。

“沪”航安全指南：

1. 在使用APP前，应仔细阅读APP的《隐私政策》，确定个人数据将会被如何使用，有不合理的条款应及时停止使用，以防个人信息泄露。
2. 在使用APP、软件过程中若发现仅凭车牌号即可查询他人停车记录等类似的侵犯个人隐私信息的情况，及时向有关部门举报。
3. 建议广大市民定期清理闲置的平台的授权权限，降低行踪信息泄露风险。



https://www.spp.gov.cn/zd gz/202508/t20250803_702952.shtml



案例解析



案例二

2025年底，某市某区人民检察院接到志愿者反映，部分餐厅扫码点餐存在强制收集个人信息问题。公益诉讼检察官们化身普通食客，亲身调查了多家餐饮门店。调查发现：部分商家在扫码点餐时强制收集手机号、微信昵称、位置信息等非必要个人信息，以“不同意无法点餐”等方式变相强迫用户授权，且授权后消费者无法自主删除个人信息。经检察机关督促，2026年初回访时发现，部分门店已增设纸质菜单，扫码小程序也已修改为无需授权即可直接点餐支付。



展示图片均由ai模组生成

面向全体市民

法律法规条例：

1. 《中华人民共和国个人信息保护法》

第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

2. 《中华人民共和国网络安全法》

第四十三条 网络运营者收集、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。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

“沪”航安全指南：

- 1.可优先选择“无授权”直接点餐或索要纸质菜单。
- 2.扫码点餐前留意隐私协议，若要求填写手机号、位置等个人信息，可拒绝授权。
- 3.点餐后留意个人信息删除功能，及时清理授权。



<https://export.shobserver.com/toutiao/html/1068674.html#1>



深化拓展“人工智能+”——AI从突破期转入应用爆发期

2026年，我国深化拓展“人工智能+”行动，推动人工智能商业化规模化应用。如果说过去几年是大模型能力突破期，那么接下来很可能是AI真正进入工作与生活的应用爆发期——从对话式AI到多媒体内容生成，普通人触达AI的门槛已大大降低。央视发布2026年AI十大趋势，一个由更聪明的“AI伙伴”全面融入工作、家居和娱乐的新时代正加速到来。随着应用的普及，个人信息被采集和滥用的风险也越高。使用AI服务前，留意隐私政策，谨慎上传个人敏感信息，不随意授权AI读取通讯录、相册等非必要权限。



AI智能体让生活更智能——普通人可借力的实用场景

对话式AI已成为普通人接触最频繁的智能交互形态，支持多轮对话、上下文记忆和跨领域知识调用。

例如，智能家居将进入“无感自动化”阶段——AI通过家中的传感器学习你的作息，在固定时间自动调节空调、灯光等设备。不过我们需要定期检查智能家居设备的隐私设置，关闭非必要的数据共享，并且定期更新设备固件、修改登录密码，让AI成为生活的“左膀右臂”，而非安全隐患。





AI “情商” 大进化——情绪感知型AI助手正不断走进日常生活

新一代AI在理解人类情感上取得突破，能够识别语气中的焦虑、疲惫或喜悦，并用更贴合人类的方式回应。与此同时，我们需要建立同AI相处时必要的“边界感”，不随意向AI透露个人敏感信息，警惕要求“屏幕共享”“授权相册”等过度权限，并且定期清理聊天记录。

