网安联
Wang An Lian

网络与数据安全治理

FRONTIERS OF REGULATORY OVERSIGHT IN CYBERSECURITY AND DATA GOVERNANCE

前沿洞察（月刊）

2025年12月第12期 (总第29期)

2025年12月15日

声明：本刊定位于网络与数据安全前沿动态梳理，侧重全面跟踪、及时掌握，如需针对特定领域或前沿动态进行针对性专题研究，请将需求发送至 cinsabj@163.com。

目　录

境内前沿观察一：政策立法

导读：11 月，公安机关监督检查、数据安全、大型网络平台以及数据要素等成为中央和地方发布政策法律标准的重要着力点，相关制度从原则性要求加速走向可操作、可落地的细化规则。

部委层面，国家互联网信息办公室发布《网络安全标识管理办法（征求意见稿）》，构建基础级、增强级、领先级“三档”网络安全标识体系，明确产品目录、实施规则及与国内外标准的衔接路径。国家互联网信息办公室、公安部发布《大型网络平台个人信息保护规定（征求意见稿）》，对大型平台认定标准、专门机构设置、境内数据中心要求等作出专门规定，强化平台—数据中心一体化监管。公安部发布《公安机关网络空间安全监督检查办法（征求意见稿）》，细化线上巡查、漏洞探测、渗透性测试等监督方式及程序边界，明确对被检查对象履行法定网络安全、信息安全、数据安全义务等情况进行监督检查。全国网络安全标准化技术委员会发布《数据安全技术 数据安全保护要求（征求意见稿）》，从通用保护、重要数据保护、核心数据保护三层提出分类分级和全生命周期保护要求，强化与等保和关保制度衔接。

地方层面，广东发布《广东省工业和信息化领域企业信息安全事件应急预案（试行，征求意见稿）》，以五级事件分级为基础，完善监测预警、应急处置和事后评估的全流程机制。广西印发《广西推动工业高质量数据集建设实施方案》，提出梳理数据集应用需求、推动高质量数据汇聚、分

级推动高质量数据集构建等多项措施。北京发布《中共北京市委、北京市人民政府关于建设数据要素综合试验区 深化数据要素市场化配置改革的实施意见》《北京市公共数据资源登记管理实施细则》，推动数据要素和公共数据资源开发利用。

关键词：数据安全；网络安全标识；大型网络平台；公安机关监督检查；数据要素

（一）部委层面动向

1. 国家认监委印发《国家认监委关于提升认证机构数字化管理能力的指导意见（2025—2029 年）》

10 月 21 日，国家认监委印发《国家认监委关于提升认证机构数字化管理能力的指导意见（2025—2029 年）》，围绕建立健全数字化管理手段和运行机制、强化数字化管理支持工具的赋能作用、加强数字化基础设施和数据安全保障能力建设三个方面，提出十条措施。

建立健全数字化管理手段和运行机制方面，《意见》提出建立规范认证流程的数字化管理工作制度。认证机构应围绕认证流程的规范管理，建立清单化的数字化管理工作制度和更新机制，通过制定业务流程管理规范、平台操作使用规范等内部管理性文件，保证认证流程和要素的完整性，强化数字化管理工作制度对规范认证流程的约束作用。

强化数字化管理支持工具的赋能作用方面，《意见》提出认证审核管理数字化支持工具。认证审核活动的实施与管理是确保认证有效性的关键环节。鼓励认证机构开发和使用数字化审核管理支持工具，更好支撑审核活动的可追溯性，减少人员工作量和出错率。一是实现审核活动关键过程的数字化协同与信息确认，做到从审核计划到审核问题关闭过程的多方线上协同，以及审核工作实施与取证环节的线上线下融合等。二是实现审核计划与报告的辅助性自动生成，做到基于线上任务管理的审核任务自动分配和跟踪管理，基于结构化数据的审核方案和报告的自动编制等。三是实

现审核问题描述与整改验证措施的智能化匹配和闭环管理。四是实现审核计划、审核结果等应上报信息的自动化、无人工操作的即出即报。

加强数字化基础设施和数据安全保障能力建设，《意见》提出加快数字化基础设施建设。算力、存储与网络是数字化管理平台安全稳定运行的核心资源保障。鼓励认证机构通过国家公共数字化基础设施的有效供给，利用云计算、大数据、人工智能等成熟的数字化产品，构建满足认证机构自身发展需要的高效、安全、可扩展的数字化基础设施。一是使用具有充足算力和扩展性的自建或云端服务器等方式，保障各类数字化业务平台的高效运行。二是利用互联网数据中心（IDC）资源，采用多链路组网等技术，实现全国范围高效稳定的网络和存储技术保障。三是主动使用我国自主可控的操作系统、数据库等软件工具。（来源：国家认证认可监督管理委员会）

2. 全国网络安全标准化技术委员会秘书处发布《数据安全技术 数据安全保护要求（征求意见稿）》

10 月 31 日，全国网络安全标准化技术委员会秘书处发布《数据安全技术 数据安全保护要求（征求意见稿）》。

征求意见稿提出了数据安全保护原则、目标和框架，规定了数据安全保护的通用要求，及重要数据、核心数据安全保护的专门要求，适用于指导各行业领域、各地区、各部门和数据处理者开展数据分类分级保护工作，也可为主管（监管）部门、第三方评估机构等组织对数据安全进行监督、管理和评估提供参考，不适用于涉及国家秘密的数据和军事数据。

数据安全通用保护要求方面，征求意见稿围绕数据安全责任、数据分类分级、数据安全保护制度、数据处理安全、风险监测及应急处置提出要求。例如征求意见稿在“数据安全责任”部分提出，委托他人处理或者与他人共同处理重要数据的，数据安全责任不因委托而改变；数据接收方应当按照数据提供方根据所属行业领域有关标准规范确定的数据级别，对数据进行有效保护；数据处理者因合并、分立、解散、破产等原因需要转移数据的，数据接收方应继续履行数据安全保护义务等要求。

重要数据保护要求方面，征求意见稿围绕数据安全管理、数据全生命周期防护、数据安全风险评估、数据共享调用、数据委托处理等九个方面，提出要求。例如征求意见稿在“数据全生命周期防护”部分提出，重要数据的收集、存储、使用、加工、传输、提供、公开、删除等环节，综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护等要求。

核心数据保护要求方面，征求意见稿提出，核心数据的处理者应在满足重要数据保护要求基础上，采取存储和处理核心数据的信息系统，涉及关键信息基础设施的，应在网络安全等级保护制度的基础上，落实关键信息基础设施安全保护要求，不涉及关键信息基础设施的，应落实四级网络安全等级保护要求等措施。（来源：国标委）

3. 国家发展改革委等九部门以及中国国家铁路集团有限公司联合印发《关于推动物流数据开放互联 有效降低全社会物流成本的实施方案》

11 月 3 日，国家发展改革委、国家数据局、中央网信办等九部门以及中国国家铁路集团有限公司联合印发《关于推动物流数据开放互联 有效降低全社会物流成本的实施方案》，围绕夯实物流数据开放互联基础、推动物流公共数据开放互联、促进企业物流数据市场化流通利用三个方面，提出九项措施。

夯实物流数据开放互联基础方面，《方案》提出健全物流数据标准规范，构建物流数据标准体系，研究制定物流数据分类分级保护、采集汇聚、共享开放、质量评价等标准规范，强化数据标准衔接，统一数据共享交换规则，加强国内国际标准接轨。推进物流数据标准宣贯实施，开展标准实施效果评价，提升标准的有效性和适用性。围绕产品数字化和业务协同，推广标准化数据接口和解决方案，持续提升物流数据标准化水平。

推动物流公共数据开放互联方面，《方案》提出加强物流公共数据共享开放，建立国家物流公共数据共享开放清单，根据行业管理和政务服务需要，明确物流公共数据共享范围，加强企业资质、从业人员、车船注册、通关物流等数据归集共享。对已在国家有关部门实现集中管理的物流公共数据，加大“总对总”共享力度，健全信息更新维护机制，提升物流公共数据共享质效。加大基础设施、运力、价格等物流公共数据开放力度。（来源：国家发展改革委）

4. 国家互联网信息办公室发布《网络安全标识管理办法（征求意见稿）》

11 月 21 日，国家互联网信息办公室发布《网络安全标识管理办法（征求意见稿）》，共四章二十一条，包括标识实施、监督管理等内容。

征求意见稿指出，网络安全标识是指能够反映产品本身网络安全能力水平的信息标识。国家互联网信息办公室、工业和信息化部负责网络安全标识管理工作，分批制定公布《实施网络安全标识的产品目录》，明确每类产品的具体实施规则和依据的国家标准或技术文件，授权中国电子技术标准化研究院承担网络安全标识备案、信息发布、违规行为处置等工作。

征求意见稿规定，网络安全标识对应的网络安全能力由低到高依次为基础级、增强级、领先级，相应的标识等级分别用一星、二星、三星表示。基础级要求产品应当满足相关国家标准的基本安全要求，如不存在弱口令或通用默认口令、建立漏洞管理机制并动态修复漏洞、保持软件更新等；增强级要求产品网络安全能力达到国内先进水平；领先级要求产品网络安全能力达到国际先进水平，同时还应通过渗透性测试方法，检测抵御高级别网络攻击的能力。每类产品的标识等级具体安全要求，在实施规则中确定。安全要求应当和现行国家标准、国际标准做好衔接，充分借鉴吸收其它实施网络安全标识制度国家和地区的相关经验。（来源：网信中国）

5. 国家互联网信息办公室、公安部发布《大型网络平台个人信息保护规定（征求意见稿）》

11 月 22 日，国家互联网信息办公室、公安部发布《大型网络平台个人信息保护规定（征求意见稿）》，共二十四条。

征求意见稿提出，国家网信部门会同国务院公安部门等有关部门制定发布大型网络平台目录并动态更新。对大型网络平台的认定主要考虑：（1）注册用户 5000 万以上或者月活跃用户 1000 万以上；（2）提供重要网络服务或者经营范围涵盖多个类型业务；（3）掌握处理的数据一旦被泄露、篡改、损毁，对国家安全、经济运行、国计民生等具有重要影响；（4）国家网信部门、国务院公安部门规定的其他情形。

征求意见稿规定，大型网络平台服务提供者应当明确个人信息保护工作机构，在个人信息保护负责人领导下开展个人信息保护相关工作，包括但不限于：（1）制定实施内部个人信息保护管理制度、操作规程以及个人信息安全事件应急预案，合理确定个人信息处理的操作权限，对大型网络平台的个人信息处理活动进行安全管理；（2）组织开展个人信息安全风险监测、风险评估、合规审计、影响评估、应急演练、宣传教育培训等活动，及时处置个人信息安全风险和事件；（3）明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务，并对其个人信息处理活动和履行个人信息保护义务情况进行监督；（4）明确专人负责未成年人个人信息保护工作；（5）受理并处理个人信息保护投诉、举报；（6）每年编制发布大型网络平台服务提供者个人信息保护社会责任报告。

征求意见稿强调，大型网络平台服务提供者应当将在中华人民共和国境内运营中收集和产生的个人信息存储在符合下列条件的数据中心：（1）设立在中华人民共和国境内；（2）主要负责人具有中华人民共和国国籍，无境外永久居留权或者长期居留许可；（3）安全性符合国家有关标准要求。（来源：网信中国）

6. 公安部发布《公安机关网络空间安全监督检查办法（征求意见稿）》

11 月 29 日，公安部发布《公安机关网络空间安全监督检查办法（征求意见稿）》，共二十三条。

征求意见稿规定，公安机关可以通过网络信息巡查、信息审核能力测试、漏洞扫描等不危害网络空间安全的方式，对被检查对象的网络安全、信息安全、数据安全等情况进行线上巡查，以发现风险隐患。对线上巡查发现的风险隐患，应当通过现场检查等方式进行线下核查。上级公安机关可以组织开展本辖区范围内的线上巡查。开展信息审核能力测试的，应当事先告知被检查对象巡查时间、巡查范围等事项。设区的市级以上公安机关可以通过漏洞探测、渗透性测试等方式，对本辖区范围内关键信息基础设施以外的网络设施、信息系统进行网络空间安全监督检查，但应当事先告知被检查对象检查时间、检查范围等事项，不得干扰、破坏被检查对象网络设施、信息系统的正常运行。

征求意见稿提出，公安机关根据网络空间安全防范需要，可以对下列对象依法开展监督检查：（1）提供互联网接入、数据中心、内容分发、域

名服务、信息服务等的互联网服务提供者；（2）公共上网服务提供者；（3）网络运营者及其建设者、维护者；（4）关键信息基础设施运营者及其建设者、维护者；（5）网络产品、服务的提供者；（6）数据处理者；（7）个人信息处理者；（8）其他依法可以监督检查的对象。对开展前款规定的服务未满一年的，两年内曾发生过网络安全、数据安全事件、违法犯罪案件的，或者因未履行法定网络安全、信息安全、数据安全义务被予以行政处罚的，应当开展重点监督检查。

征求意见稿强调，公安机关应当对被检查对象履行法定网络安全、信息安全、数据安全义务等情况进行监督检查，重点检查以下内容：（1）是否依法办理联网单位备案手续，并报送接入单位和用户基本信息及变更情况；（2）是否依法制定并落实网络安全、信息安全、数据安全管理制度和操作规程；（3）是否依法记录并留存用户注册信息和上网日志信息；（4）是否依法履行网络安全等级保护定级备案、等级测评、建设整改、自查等安全保护义务；（5）是否依法履行关键信息基础设施安全保护义务；（6）是否依法采取防范计算机病毒和网络攻击、网络侵入等技术措施；（7）是否依法针对网络安全漏洞、隐患采取相应的整改措施，消除风险隐患；（8）是否依法在公共信息服务中对法律、行政法规禁止发布或者传输的信息采取防范措施；（9）是否依法落实算法安全主体责任，建立健全算法推荐管理制度和技术措施；（10）是否依法履行数据安全、个人信息保护义务；（11）是否依法为公安机关维护国家安全、防范调查恐怖活动、侦查犯罪等提供技术支持和协助。（来源：公安部）

（二）地方层面动向

1. 广东省工业和信息化厅发布《广东省工业和信息化领域企业信息安全事件应急预案（试行，征求意见稿）》

11 月 2 日，广东省工业和信息化厅发布《广东省工业和信息化领域企业信息安全事件应急预案（试行，征求意见稿）》，适用于广东省辖区内发生的工业和信息化领域企业信息安全事件应急处置活动。

征求意见稿所称工业和信息化领域企业信息安全事件，是指由于人为原因、软硬件缺陷或故障等，对工业和信息化领域企业数据安全、工业互联网安全、工业控制系统信息安全等造成危害，导致或可能导致企业网络和信息系统、工控系统或者其中的工业数据遭篡改、破坏、泄露或者非法获取、非法利用，影响正常工业生产，对国家安全、公共利益或者个人、组织合法权益造成危害的事件。

征求意见稿根据工业和信息化领域企业信息安全事件对国家安全、企业网络和信息系统、生产运营、经济运行等造成的影响范围和危害程度，将企业信息安全事件分为五级：特别重大、重大、较大、次级、一般。

征求意见稿提出应急预案包括监测与预警、应急处置、事后总结、保障措施四个方面，其中监测与预警包括预警监测和报告、预警分级、预警发布、预警响应等内容，应急处置包括事件报告、先行处置、应急响应、响应级别调整、舆情监测、应急结束等内容，预防工作包括日常管理、应急演练、安全检查、宣传与培训等内容。（来源：广东省工业和信息化厅）

2. 广东省人民政府印发《广东省国家数字经济创新发展试验区建设方案（2025—2027 年）》

11 月 8 日，广东省人民政府印发《广东省国家数字经济创新发展试验区建设方案（2025—2027 年）》，围绕推进数据要素市场化配置改革、优化数据基础设施建设布局、加快关键核心技术突破等七个方面，提出二十三项措施。

推进数据要素市场化配置改革方面，《方案》提出构建数据基础制度新范式。完善数据要素市场化配置制度规则体系，加快出台《广东省数据条例》。健全数据产权制度，推动数据产权登记与公共数据资源登记、公共数据资源产品和服务登记等 3 类登记事项协同办理。建立公共数据、企业数据、个人数据分类分级确权授权机制，制订公共数据授权运营实施细则。建立数据流通交易与合规体系，健全场内数据交易流通标准体系，开展数据交易纠纷调解机制试点，健全数据领域纠纷调节机制，构建全省一体化数据市场。开展数据资产核算研究，探索将数据资产等投资纳入固定资产投资统计。

推进适数化改革方面，《方案》提出以数字政府改革提升营商环境质效。开展“人工智能+政务”行动，推动人工智能大模型在政务服务、政府治理和政府运行领域深度应用。推进政务服务“智办”，推进“高效办成一件事”。推进政府治理“智管”，提升风险识别、趋势分析、辅助决策、场景模拟、指挥调度等智能化水平。深化“民意速办”改革，开展民生诉求事项清单化管理。推进政府运行“智联”，完善一体化协同办公体系。

推动核心业务数据化改革，完善“块数据”平台建设，健全核心业务指标全流程管理机制。建立基层报表准入退出和清单管理机制，强化政务数据依需回流和有序开放，健全数据质量审查、监测和纠正机制。探索创新数字政府建设运营模式，推动有条件的公共平台社会化运营。（来源：网信广东）

3. 广西壮族自治区工信厅印发《广西推动工业高质量数据集建设实施方案》

11 月 3 日，广西壮族自治区工信厅印发《广西推动工业高质量数据集建设实施方案》，提出梳理数据集应用需求、推动高质量数据汇聚、分级推动高质量数据集构建等六项措施。

推动高质量数据汇聚方面，《方案》提出聚焦重点特色优势产业，汇聚企业研发、生产、管理等关键环节数据。例如支持企业对客户需求信息、专利信息、行业技术标准、产品数据、工艺数据、研发设计数据、开发测试数据等研发数据进行归集，形成生产研发数据集。

分级推动高质量数据集构建方面，《方案》提出应用规模以上工业企业智改数转诊断分级和数据管理能力成熟度评估结果，分级推进高质量数据集建设，提高企业数据开发能力，同步推进设备更新与数据治理。针对数字化水平较低的木材加工、纺织服装、糖业等行业，推动企业智改数转，实施大规模设备更新，加装智能传感器、通信模块等硬件设备，应用工业物联网技术，实现设备联网与互联互通，提升数据采集稳定性。针对数字化智能化水平较高的有色金属、汽车、机械、石化化工等行业，引导企业

建立健全企业数据管理制度，构建数据资源架构体系，建设数据管理目录，系统性开展数据治理，实现数据共享和业务协同。针对数据管理成熟度高的企业、国家和自治区级智能工厂企业，按照循序渐进、先易后难原则，建设面向研发、生产、运维等具体应用场景数据集，示范带动全面推进行业高质量数据集建设。（来源：广西工业和信息化厅）

4. 《中共北京市委、北京市人民政府关于建设数据要素综合试验区 深化数据要素市场化配置改革的实施意见》印发

11 月 6 日，《中共北京市委、北京市人民政府关于建设数据要素综合试验区 深化数据要素市场化配置改革的实施意见》印发，围绕夯实数据要素基础环境、加强多主体数据资源供给、推动多层次数据资源流通等七个方面，提出十八项措施。

夯实数据要素基础环境方面，《意见》提出建立健全数据基础制度，组织推动数据产权结构性分置制度落地，鼓励数据复用融合、创新创造及有序流转。创新数据流通交易制度，完善场内场外结合的交易规则体系，培育壮大场内交易，规范引导场外交易。引导形成数据要素由市场评价贡献、按贡献决定报酬的收益分配机制，保障各参与方依法依规享有收益权利。健全数据安全治理制度，完善数据流通交易责任界定机制，提升数据流通风险防范能力。推动数据要素综合性立法。围绕重点行业领域数据流通合规指引、数据资产管理、平台数据合规供给、数据跨境流动等制定一批特色创新制度。发挥北京市数据标准化技术委员会作用，率先在数据基础设施、数据技术、数据流通、安全保障等方面出台系列标准。

加强多主体数据资源供给方面，《意见》提出有效扩大公共数据供给，推动公共数据资源开发利用政策落地，完善政务数据共享、公共数据开放和授权运营等配套制度。深化公共数据目录管理机制，推动各行业领域、各区公共数据上链汇聚。完善“一数一源一标准”治理机制，加强公共数据供给质量评估和监督检查。加强数据共享协调，依法推动政务数据应共享、尽共享，促进市级数据下沉和基层数据反哺。建立开放数据接诉即办机制，及时响应社会主体数据需求和应用反馈。探索以政企合作方式开展开放平台基础设施建设和运营，提升数据产品的开发效率和价值转化能力。积极推动分领域授权、依场景授权，探索整体授权运营。建立公共数据资源授权运营价格形成机制，制定最高准许收入和上限收费标准。深化金融公共数据专区运营，加快建设医疗、医保、医药“三医”及气象、时空等一批公共数据专区。加强央地协同，推进与国家部委、央企建立数据合作机制，加快形成权责清晰、部市协同的授权运营模式。（来源：北京市政府）

5. 北京市政务服务和数据管理局发布《北京市公共数据资源登记管理实施细则》

11 月 10 日，北京市政务服务和数据管理局发布《北京市公共数据资源登记管理实施细则》，共六章二十七条，包括登记要求、登记程序、登记管理等内容。

《细则》提出，直接持有或管理公共数据资源的党政机关和事业单位，应对纳入授权运营范围的公共数据资源进行登记，鼓励对未纳入授权运营

范围的公共数据资源进行登记。鼓励经授权开展运营活动的法人组织，对利用被授权的公共数据资源加工形成的数据产品和服务进行登记。鼓励供水、供气、供热、供电、公共交通等公用企业对直接持有或管理的公共数据资源及形成的产品和服务进行登记。

《细则》强调，登记主体在申请登记前应在保障安全的前提下对公共数据资源进行存证，确保来源可查、加工可控。党政机关、企事业单位的公共数据资源在登记前应依托北京市大数据平台完成数据目录上链。登记主体经业务审核后，通过市登记平台提出登记申请，如实准确提供登记材料，并对登记材料内容的真实性、完整性、合法性、有效性负责。涉及多个主体的，可共同提出登记申请或协商一致后由单独主体提出登记申请。登记主体可以自行申请登记，也可以委托代理机构办理登记申请手续。

《细则》规定，北京市公共数据资源登记申请类型主要包括首次登记、变更登记、更正登记、注销登记。首次登记时，登记主体在开展授权运营活动并提供数据资源或交付数据产品和服务后，应在20个工作日内提交首次登记申请。（来源：北京市政务服务和数据管理局）

6. 天津市数据局等八部门印发《天津市关于加快数据标注产业发展促进行业高质量数据集建设的行动方案（2025—2027年）》

11月11日，天津市数据局、天津市教委、天津市科技局等八部门联合印发《天津市关于加快数据标注产业发展促进行业高质量数据集建设的行动方案（2025—2027年）》，围绕培育壮大产业、强化创新驱动、统筹产业布局等六个方面，提出十六项措施。

强化创新驱动方面，《方案》提出推动标准制定和应用，支持企事业单位参与数据标注、数据集相关标准的制定和验证，承接国家级行业高质量数据集建设先行先试任务，促进数据标注和数据集领域相关标准、技术专利在重点行业领域的协同创新和成果转化。鼓励企业探索数据标注与区块链、隐私保护计算等技术的融合应用，提升数据安全与标注质量。

建设行业高质量数据集方面，《方案》提出扩大公共数据供给，建立健全全市政务数据资源目录体系，规范全市政务数据共享、公共数据开放，深化政务数据资源开发利用，推动数据开放共享。升级数据资源统一共享交换平台，依法有序推进数据资源流通使用，推动跨部门、跨地区、跨层级公共数据融合应用。鼓励政府部门和企业协同开展政务大模型所需数据的标注业务，并利用标注处理后的高质量数据集进行训练。

健全服务平台方面，《方案》提出打造数据标注公共服务平台，鼓励开发建设集数据加工处理、数据集质量评估、模型基准测试、产教融合实训为一体的数据标注公共服务平台，提升数据标注自动化、智能化水平，支持服务行业龙头企业、中小企业等不同层次数据标注需求。（来源：天津市数据局）

7. 湖南省互联网信息办公室发布《湖南省网信行政处罚裁量权基准（征求意见稿）》

11 月 19 日，湖南省互联网信息办公室发布《湖南省网信行政处罚裁量权基准（征求意见稿）》，共二十四条。

征求意见稿规定，当事人同时存在减轻处罚、从轻处罚或者从重处罚等情形的，应当根据案件具体情况综合考量进行处罚。涉及未成年人权益或英雄烈士名誉荣誉的案件，若同时存在从宽和从严情形，应当优先考量对未成年人、英雄烈士的保护需求。

征求意见稿强调，罚款有一定幅度的，在相应的幅度范围内分为从轻处罚、一般处罚、从重处罚。从轻处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间低于30%的数额；一般处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间的30%至70%的数额；从重处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间超过70%的数额。在确定具体处罚数额时，综合考量违法行为的性质、情节和湖南省经济社会发展水平、地区差异等因素，结合执法实践和执法案例，可以以前款规定的百分比为基础上下浮动十个百分点。

征求意见稿提出，单位实施违法行为的，对直接负责的主管人员和其他直接责任人员的处罚，应当综合考量相关责任人员的岗位职责、任职时间、履职行为与违法行为的关联性、主观过错程度、主次责任，以及是否对违法行为采取整改措施等因素，参照对单位行政处罚裁量阶次，确定适当的行政处罚。（来源：网信湖南）

境内前沿观察二：治理实践

导读：11 月，公安、网信、通信管理部门等机构持续发力，强化网络安全、数据安全、个人信息保护监督检查力度，公布一批刑事打击和行政执法典型案例，提升网络和数据安全水平。

国家网络与信息安全信息通报中心通报 40 款违法违规收集使用个人信息的移动应用。福建、山东、陕西等地公安网安部门发布涉及帮助信息网络犯罪活动、处置网络安全漏洞隐患、查处平台数据泄露等典型案例。

中央网信办部署开展“清朗·十五运会和残特奥会网络环境整治”专项行动，聚焦涉赛事舆论传播、账号运营和个人信息保护等重点领域，从严打击编造传播涉赛事及相关地区虚假信息、滥用人工智能制作传播虚假赛事内容以及泄露隐私、组织网络暴力等突出问题。国家网信办会同工业和信息化部等部门深入开展汽车行业网络乱象专项整治行动，从严整治散布虚假不实信息，恶意抹黑诋毁汽车企业、汽车产品等违法违规行为。中央网信办近日深入推进“清朗·整治网络直播打赏乱象”专项行动，针对低俗团播引诱打赏问题，督促网站平台持续加强团播内容管理，从严处置一批顶风作案的违规账号。

最高人民法院发布三例涉未成年人网络保护与违法犯罪惩处典型案例，涉及未经许可擅自使用未成年人肖像、未成年人网络侵权、敲诈勒索等违法行为。

关键词：网络安全漏洞；网络环境整治；未成年人网络保护

（一）公安机关治理实践

1. 国家网络与信息安全信息通报中心通报 40 款违法违规收集使用个人信息的移动应用

11 月 17 日，国家网络与信息安全信息通报中心发布消息称，在 2025 年 9 月 28 日至 2025 年 10 月 16 日期间，检测发现 40 款违法违规收集使用个人信息的移动应用。40 款移动应用存在的安全问题如下：

（1）16 款移动应用未逐一列出收集、使用个人信息的目的、方式、范围，包括《壹达外卖》（版本 6.0.202509021，应用宝）等。

（2）1 款移动应用在申请打开可收集个人信息的权限时，未同步告知用户其目的，包括《掌上药店》（版本 6.3.9，百度手机助手）。

（3）2 款移动应用征得用户同意前就开始收集个人信息，包括《返利淘联盟》（版本 8.6.9，豌豆荚）、《e 看牙》（版本 4.37.2，豌豆荚）。

（4）16 款移动应用实际收集的个人信息超出用户授权范围，包括《壹达外卖》（版本 6.0.202509021，应用宝）等。

（5）1 款移动应用个人信息保护政策中描述需要收集的个人信息超出相关功能的必要范围，包括《药安食美》（版本 1.1.5.3，应用宝）。

（6）2 款移动应用配置文件中声明的可收集个人信息的权限超出相关功能的必要范围，包括《手机血压血糖管理》（版本 1.0.16，应用宝）等。

（7）10 款移动应用实际收集的个人信息超出相关功能的必要范围，包括《熊猫霸王餐》（版本 1.3.6，应用宝）等。

（8）5 款移动应用未向用户提供个人信息相关投诉渠道或功能，包括《赏帮赚》（版本 5.2.7，豌豆荚）等。

（9）3 款移动应用未向用户提供更正或补充其个人信息的具体途径，包括《金牌护士》（版本 5.1.10，华为应用市场）等。

（10）3 款移动应用未向用户提供删除其个人信息的具体途径，包括《金牌护士》（版本 5.1.10，华为应用市场）等。

（11）1 款移动应用未向用户提供注销账户的途径和方式，包括《游戏接单》（版本 2.0.4，应用宝）。

（12）1 款移动应用注销账户的流程中设置不合理的条件或提出额外要求，包括《护士通》（版本 3.4.5，vivo 应用商店）。

（13）1 款移动应用未提供退出或关闭个性化展示模式的选项，包括《Party Play》（版本 3.16.0，vivo 应用商店）。

（14）2 款移动应用广告存在误导、欺骗用户行为，包括《血压血糖免费测》（版本 1.3.0，华为应用市场）等。（来源：国家网络安全通报中心）

2. 公安部网络安全法律咨询委员会 2025 年年会暨第十五届信息安全法律大会在京召开

11 月 27 日至 28 日，公安部网络安全法律咨询委员会 2025 年年会暨第十五届信息安全法律大会在京召开。

会议指出，近年来，面对不断严峻复杂的网络安全新形势、新挑战，网络安全法律咨询委员会充分发挥作用，帮助公安机关大力推进网络法治

建设、深入参与网络空间国际治理，进一步提升公安机关履职尽责、主动担当的能力水平，为推进平安中国、法治中国建设贡献了积极力量。

会议强调，2025 年，网络安全法律咨询委员会立足职责任务，在全国人大常委会法工委、中央网信办、最高人民法院、最高人民检察院、工业和信息化部、司法部等部门和相关高校院所、互联网企业的积极支持下，紧密贴合公安机关实战需求，通过主题沙龙、立法研讨、专题会议、闭门讨论等多种形式，凝聚共识、贡献智慧，助力公安机关网络安全立法工作取得新进展、网络犯罪打击治理取得新战果、网络安全行政执法取得新成效。

会议要求，公安部网络安全法律咨询委员会要牢牢把握公安网络法治建设的政治方向，始终同以习近平同志为核心的党中央保持高度一致。要积极协同为网络空间治理献言献策，及时反映网络空间治理新诉求、老百姓新期盼，助力公安机关网络法治建设工作提质增效、创新发展。

会议设“打击网络犯罪‘净网’”、“网络安全监管‘护网’”、密码法治创新发展、数据安全与个人信息保护、生成式人工智能风险防范等分论坛。来自有关部委、高校院所、公检法部门、企事业单位的咨询委员在分论坛上作了交流发言，相关咨询委员及地方公安网安民警参加了论坛。（来源：公安部网安局）

3. 福建网警侦破一起帮助信息网络犯罪活动案

11 月 3 日消息，福建莆田网警近日在“净网—2025”专项工作中成功侦破一起诱骗收购未成年人实名手机卡为境外诈骗分子提供通讯通道的帮助信息网络犯罪活动案，抓获犯罪嫌疑人 8 名。

2025 年 4 月，福建莆田公安网安部门工作中发现，辖区内有一犯罪团伙盗窃、收购中小学生实名手机卡，并提供给境外诈骗分子使用。经查，该犯罪团伙通过盗窃中小学生通讯设备和高价引诱未成年人办理手机卡等方式大量获取实名手机卡，并按照境外诈骗分子要求利用非法获取的手机卡联系受害者实施诈骗。

全面掌握该犯罪团伙组织架构、人员身份和窝点位置等信息后，莆田公安机关组织警力在多地开展统一抓捕行动，抓获主犯李某某、吴某某等犯罪嫌疑人 8 名，查获涉案手机 80 余部、手机卡 150 余张、电脑及相关设备 18 套。目前，案件正进一步侦办中。（来源：公安部网安局）

4. 因未按规定发布漏洞信息，某平台被依法处罚

11 月 6 日，公安网安部门在“护网—2025”专项工作中发现，某具有交互式信息发布功能的网络产品安全漏洞发现、收集平台掌握了某网络产品存在安全漏洞，但在网络产品提供者发布安全漏洞修补措施前，公开了该漏洞细节信息及利用该漏洞从事危害网络安全活动的程序和工具。公安机关依据《网络安全法》，对该平台运营者予以行政处罚，并责令整改。（来源：公安部网安局）

5. 因未及时修复安全漏洞，山东青岛某科技公司被依法处罚

11 月 10 日消息，山东青岛公安网安部门在日常工作中发现，某机构对外提供公共服务的网络平台长时间持续存在 SQL 注入漏洞、越权访问漏洞，存在网络数据安全隐患。

经查，某科技公司在为该机构提供系统运行、维护时，未按照法律法规相关规定和合同约定履行网络数据安全保护义务，未采取必要的技术措施，未及时修复安全漏洞，存在数据泄露风险。青岛崂山网安部门依据《网络数据安全管理条例》对该公司予以行政处罚。（来源：公安部网安局）

6. 陕西网警依法查处一起涉无人机管理平台遭攻击导致数据泄露案

11 月 23 日消息，陕西某无人机技术公司开发、使用的无人机管理平台近日遭黑客网络攻击，平台内存储的部分数据被窃取。陕西西安公安网安部门依法立案侦查。

在案件办理过程中，陕西西安公安网安部门发现，该公司无人机管理平台存在安全漏洞，且公司内部未建立全流程数据安全管理制度，未组织开展数据安全教育培训，缺乏必要的技术防护措施。针对该公司不履行数据安全保护义务的违法行为，陕西西安公安机关依据《数据安全法》，依法追究了该公司的法律责任并责令其限期改正。同时，指导该公司建立健全相关安全管理制度，修复平台安全漏洞，开展网络和数据安全专项培训，提升员工安全防范意识，加强内部网络和数据安全防护。目前，案件仍在进一步侦办中。（来源：公安部网安局）

7. 网站未按规定审核，导致违法信息传播，网警依法处罚

11 月 26 日消息，山东青岛公安网安部门近日在工作中掌握，辖区某网站平台未按照有关规定对发布的信息进行审核，未及时发现用户在网站上发布的违法信息，导致违法信息在互联网传播、扩散。青岛市公安局李沧分局依据《网络安全法》，对该网站予以行政处罚。（来源：公安部网安局）

8. 宁夏网警侦破一起“网络水军”诈骗案

11 月 26 日，宁夏中卫市沙坡头区网警近日侦破一起“网络水军”以提供“直播推流”服务为名实施诈骗的案件，打掉以张某某为首的 5 人犯罪团伙。

犯罪嫌疑人张某某长期伪造某网络平台官方工作人员身份并在全国范围内招募超 80 余名水军成员及技术人员，打造虚假流量“手机墙”。以“包上热门”“内部渠道”“快速涨粉”等话术为饵，诱使渴望提升直播人气的主播支付高额服务费，并强制要求主播每日参加所谓“流量密码授课”。当主播识破虚假人气要求退款时，张某某团伙便采取拖延推诿等手段迫使其放弃并拒绝退款。

目前，该犯罪团伙已对全国 300 余名网络主播实施诈骗，金额累计 360 余万元。其行为严重扰乱平台正常经营秩序和网络市场经济环境，侵害广大消费者及合法经营者的权益。

公安机关精准锁定辖区嫌疑人及上线张某某犯罪窝点，现场查获手机、电脑等作案工具 140 余部，查获用于制造虚假流量直播账号 4300 余个，用

于注册账号公民个人信息4100多条（包含手机号，身份证信息），固定电子证据10万余条。彻底斩断这一危害网络生态的黑色产业链。5名主要犯罪嫌疑人均已采取刑事强制措施。（来源：公安部网安局）

9. 山东网警侦破一起非法控制计算机信息系统案

11月28日消息，山东济南网警近日侦破一起非法控制计算机信息系统案，抓获9名犯罪嫌疑人，对其中4名主犯依法采取刑事强制措施。

经查，犯罪团伙利用内部人员运维权限，在网吧监管平台中植入恶意插件，实现对全省3000余家网吧、10万余台计算机的非法控制。犯罪嫌疑人通过强制弹出广告引流，将用户引导至恶意网站，非法牟利，形成了依托监管平台掩蔽，实施非法活动的黑灰利益链条。（来源：公安部网安局）

10. 因不履行个人信息保护义务，某公司被依法处罚

11月29日消息，山东烟台公安机关网安部门近日在日常工作中掌握，某公司在其运营的新媒体账号发布由其负责的某区域内约上百条用户姓名、住址信息等，造成公民个人信息泄露。

经查，系公司员工系统操作不当，将用户信息表上传至公司公众号，公司对公民信息数据未尽到保护责任，存在数据泄露隐患。该公司接到通知后，第一时间删除了相关内容。属地公安机关网安部门依据《网络安全法》第六十四条，对其依法依规作出处罚。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办部署开展“清朗·十五运会和残特奥会网络环境整治”专项行动

10 月 31 日，中央网信办印发《关于开展“清朗·十五运会和残特奥会网络环境整治”专项行动的通知》，决定自 11 月 4 日至 12 月 20 日开展“清朗·十五运会和残特奥会网络环境整治”专项行动，集中整治 6 类突出问题。

（1）散布涉十五运会和残特奥会及相关地区公共政策、社会民生领域虚假信息，捏造可能引起恐慌的灾难事故、违法犯罪、食品产品质量问题、疫情防控等谣言，特别是在权威辟谣信息发布后仍大肆造谣传谣的行为。

（2）片面、歪曲传播赛事期间可能出现的突发事件信息，假冒当事人或相关人员身份发声，关联翻炒旧闻旧事。

（3）发布抹黑“一国两制”制度言论，散布有关人群、民族、地域歧视的信息，挑拨地域对立、煽动群体对立，恶意损害香港、澳门、广州、深圳等主要赛事举办地及相关地区形象。

（4）未经许可擅自开展涉十五运会和残特奥会相关互联网新闻信息服务活动。利用人工智能技术制作和发布有关虚假赛事视频，以及关联赛事和运动员、教练员、裁判员等的不实信息。

（5）使用相同或者相似名称、域名、标识、页面等假冒仿冒十五运会和残特奥会的网站、移动应用程序、快应用、小程序；在账号名称、头像、简介、直播间或短视频背景等环节假冒仿冒相关地区官方机构、新闻媒体等。

（6）组织“人肉搜索”，故意泄露运动员、教练员、裁判员等个人隐私信息，诱导实施网络暴力；实施拉踩引战、互撕谩骂等体育饭圈不良行为，影响运动员备战和赛事举办。（来源：中国网信）

2. 国家网信办发布处置涉退役军人违法违规账号典型案例

11 月 12 日消息，根据“网上涉退役军人不当行为和有害信息内容专项整治”工作安排，国家网信办近日指导各网站平台从严整治以退役军人名义售卖假冒伪劣商品、进行低俗表演、消费军旅情怀、损害退役军人形象等问题，处置一批违法违规账号。

其中，典型案例包括四个方面：（1）发布低俗内容。网络账号“颜班长（退役女兵）”“小颜班长（退役女兵）”“漠九”等，自称退役军人，发布穿着暴露，含有性暗示、性挑逗的低俗擦边内容。网络账号“王兴奇”等，穿着我国武装力量现行或曾经装备的制式服装及其仿制品，在直播过程中开展低俗舞蹈表演吸引用户打赏。

（2）传播有害言论。网络账号“宋班长（正能量）”“睿智人生”等，以讲授从军经验、咨询部队情况等名义，发布“在某地服役有什么危害”“在部队患上这样那样的疾病”等导向不良言论。

（3）散布虚假信息。网络账号“防炎炎夏日”“中国梦#”等，利用人工智能、深度合成等技术，制作发布“边疆站岗 20 年，如今带着有病的孩子走在路上”等谣言信息，以及虚假退役军人图片、视频等，误导公众认知。

（4）不当营销牟利。网络账号“A-后勤仓库正品协调”“迷彩仓”“贩卖人间快乐”等，借退役军人身份，违规售卖军服及其仿制品，或发布提供各类定制服务的营销信息。网络账号“红旗白鸽”等，以提供“转业安置咨询”等为噱头，歪曲解读涉军政策，违规提供收费咨询服务。（来源：网信中国）

3. 国家网信办发布汽车行业网络乱象专项整治行动典型案例

11 月 12 日消息，国家网信办近日会同工业和信息化部等部门深入开展汽车行业网络乱象专项整治行动，从严整治散布虚假不实信息，恶意抹黑诋毁汽车企业、汽车产品等违法违规行为。

其中，典型案例包括四个方面：（1）“大眼哥说车”等账号发布贬损性信息，侵害企业商誉和产品信誉。抖音账号“大眼哥说车”、今日头条账号“电电加电”、快手账号“森哥电车”等，随意发布贬损性言论，恶意诋毁某汽车企业品牌、辱骂企业家并持续炒作。涉及的账号已被依法依约采取关闭等处置措施。

（2）“高见观潮”等账号散布虚假不实信息，恶意诋毁攻击企业。今日头条账号“高见观潮”、微信公众账号“象视汽车”、微博账号“大 D 有态度”等，编发涉某汽车企业虚假信息，诋毁攻击企业产品质量，恶意唱衰企业经营状况。涉及的账号已被依法依约采取处置措施。

（3）“我是大彬同学”等账号恶意集纳企业负面信息，诋毁攻击企业产品。微博账号“我是大彬同学”、抖音账号“石头搞机”、哔哩哔哩账

号“赛车星冰乐”等，为博眼球、吸流量，集纳企业负面信息、蹭炒涉企热点事件、煽动群体对立。涉及的账号已被依法依约采取处置措施。

（4）“易车榜”等账号巧立名目发布汽车销量榜单，干扰企业正常生产经营。微博账号“易车榜”“孙少军09”、微信公众账号“数典汽车排行榜”“中汽数研”“大侠侃车”等，频繁发布未经核实，甚至捏造、杜撰的汽车销量数据，误导消费者，干扰汽车企业正常生产经营。涉及的账号已被依法依约采取处置措施。

（5）“王武松”等“转世”账号继续发布不实信息，抹黑诋毁汽车企业。抖音账号“王悟空说车”“987疯狂奶爸”因多次歪曲事实诋毁新能源汽车性能，恶意抹黑某汽车企业形象声誉被依法依约关闭。上述账号使用主体，在抖音、小红书、百度等平台注册“王武松”“疯狂斯坦森”等账号，继续发布主观测评信息，抹黑攻击某新能源汽车企业产品质量。涉及的账号已被依法依约采取关闭措施。（来源：网信中国）

4. 国家网信办发布打击涉学术论文买卖违法违规账号典型案例

11月13日消息，国家网信办近日针对部分网络账号违规提供学术论文买卖、代发、代投服务，严重扰乱网络秩序，污染网络生态的情况，严惩一批违法违规账号。

其中，典型案例包括三个方面：（1）明码标价实施学术论文买卖行为。网络账号“琪瑞派论文咨询”“苏苏老师论文辅导咨询”“本硕博毕业服务旗舰店”等，利用“毕业论文全天加急”“文章代笔”“辅导至毕业”

等宣传营销话术，明码标价提供学术论文买卖、代发、代投服务。上述账号已依法予以关闭。

（2）引流圈群实施学术论文买卖行为。网络账号“木木学姐论文咨询”“GYuan-论文指导”“A1 孙编辑”等，以“论文辅导”“期刊咨询”“论文降重”等隐晦话术，诱导用户添加微信、QQ 等私域圈群联系方式，违规提供学术论文买卖、代发、代投服务。上述账号已依法予以关闭。

（3）利用话题暗示提供违规服务。网络账号“司徒说创业”“官子随笔”等，发布“AI 代写业务招商”“招募兼职写手”等话题，在其简介、评论互动等环节暗示提供学术论文买卖、代发、代投服务。上述账号已依法予以关闭。（来源：网信中国）

5. 中央网信办严惩一批网络直播低俗团播账号

11 月 26 日，中央网信办近日深入推进“清朗·整治网络直播打赏乱象”专项行动，针对低俗团播引诱打赏问题，督促网站平台持续加强团播内容管理，从严处置一批顶风作案的违规账号。

部分典型案例包括三个方面：（1）低俗内容吸引打赏。团播账号“HN-三世烟火”“Top-长安城”“YC-热舞青春 6.0”等，在直播过程中穿着暴露，频繁做出抖胸、扭动臀部、淋湿衣物展示湿身效果等带有性暗示、性挑逗的动作，渲染低俗不良氛围，诱导用户打赏。相关账号已依法予以永久禁言或永久封禁直播权限。

（2）低俗惩罚诱导打赏。团播账号“心动女孩”“好多表妹哟”“YZB 女团”等，在直播过程中使用抽打脚底板、击打臀部、成员之间互相电击

等引人不适的惩罚方式，以及发出不雅声音，诱导用户通过打赏与主播进行低俗互动。相关账号已依法予以禁言或永久封禁直播权限。

（3）低俗玩法拉票打赏。团播账号“Vibe-002”“亿江南-后宫”“蔚蓝海岸”等，在直播过程中采用送礼物排名选妃玩法，刻意展示团播成员礼物金额，通过金额攀比、镜头聚焦高排名主播敏感部位等形式，诱导用户为主播送礼物提高排名。相关账号已依法予以禁言或永久封禁直播权限。（来源：网信中国）

6. 网信部门从严整治利用 AI 仿冒公众人物开展直播营销问题乱象

11 月 14 日消息，网信部门近日针对网络账号利用 AI 技术仿冒公众人物形象，在直播、短视频等环节发布营销信息误导网民的情况开展整治活动。网信部门严厉处置“百货超市小店”“娜娜好物联盟”“环球护肤美妆甄选”等一批违法违规网络账号。同时，督促网站平台发布治理公告，举一反三，开展集中清理整治，目前已累计清理相关违规信息 8700 余条，处置仿冒公众人物账号 1.1 万余个。（来源：网信中国）

7. 浙江省互联网信息办公室开展 2025 年度汽车数据安全管理情况报送工作

11 月 14 日，浙江省互联网信息办公室发布《浙江省互联网信息办公室关于报送 2025 年度汽车数据安全管理情况的通知》。《通知》指出，注册地为浙江省且开展重要数据处理活动的汽车数据处理者，包括汽车制造商、

零部件和软件供应商、经销商、维修机构以及出行服务企业等主体，在2025年12月15日前，向浙江省互联网信息办公室报送《2025年度汽车数据安全管理情况报告》、《风险评估报告》、《汽车数据处理者情况汇总表》。（来源：网信浙江）

8. 北京市网信办、市公安局、市通管局联合约谈18款小众通联APP运营主体

11月21日消息，北京市网信办、市公安局、市通管局近日依法联合约谈18款小众通联APP运营主体，通报其存在的涉诈风险，责令限期整改，切实履行主体责任。

依据《反电信网络诈骗法》《网络安全法》等法律法规，三部门提出明确管理要求。一是全面落实实名制。在与用户签订协议或确认提供服务时，依法要求用户提供真实身份信息，用户不提供真实身份信息的，不得提供服务。二是完善监测识别机制。对利用其服务从事涉诈支持、帮助活动进行监测识别和处置，对监测识别的涉诈异常账号立即重新核验，并根据风险等级采取限制功能、暂停服务等处置措施。三是健全内部管理制度。完善反诈内部防控机制和安全责任制度，防范被不法分子利用。积极配合监管执法工作，为公安机关办案提供技术支持和协助。四是加强反诈宣传提示。在APP注册、使用环节的显著位置，通过公告栏等方式加强反诈宣传，提高用户反诈意识。同时，完善用户投诉通道，及时受理处置用户举报。（来源：网信北京）

9. 北京市网信办启动“清朗京华•金融守护”专项行动，重点整治六类金融领域网络乱象

11 月 26 日，北京市网信办会同北京金融监管局联合部署开展为期 3 个月的“清朗京华·金融守护”金融领域网络乱象治理专项行动。专项行动聚焦短视频、社交、直播等重点网站平台，集中整治假冒仿冒专业人员误导公众、以隐蔽方式违规引流、为非法存贷款中介提供推介服务、开展非法代理维权“黑灰产”活动、恶意抹黑诋毁金融机构、捏造虚假信息唱衰经济等六类突出问题。（来源：网信北京）

10. 湖南省长沙市网信办发布个人信息保护部分执法案例

11 月 28 日，湖南省长沙市网信办发布个人信息保护部分执法案例。2025 年 5 月以来，长沙市网信办联动市公安局、市住建局、市卫健委等部门共同开展“亮剑湖湘▪民生领域个人信息权益保护”专项行动，依法惩处了一批违法违规主体。

专项行动聚焦群众反映强烈的教育培训、医疗健康、金融理财、房产物业等行业应用程序和公共场所违规收集使用人脸识别信息的行为，通过线索摸排、技术检测、现场勘验等方式，依法查处违法违规线索 79 条，约谈单位企业 52 家，进行现场勘验 24 次，立案处罚 5 起。

案例一：某医院数据泄露案

长沙某医院有限公司相关系统未采取技术措施和其他必要措施保障数据安全，存在未授权访问漏洞、个人敏感信息在传输及存储过程中未进行

加密或脱敏处理等问题，导致数据泄露。长沙市网信办依法对该公司作出行政处罚，责令其在规定期限内完成整改。

案例二：某金融小程序违规收集使用个人信息案

湖南某融资担保有限公司微信小程序存在未明示收集使用个人信息的目的、方式和范围，未按法律规定提供有效的更正、删除个人信息及注销用户账号功能等问题。芙蓉区网信办依法对该公司负责人进行约谈，并下发责令改正通知书，责令其在规定期限内完成整改。

案例三：某餐饮公司小程序违规收集使用个人信息案

长沙某记餐饮管理有限公司微信小程序未按法律规定提供有效的更正、删除个人信息及注销用户账号功能。望城区网信办联合区市场监管局依法对该公司负责人进行约谈，并下发责令改正通知书，责令其在规定期限内完成整改。

案例四：某售楼部违规采集个人（人脸）信息案

长沙某房地产有限公司某楼盘售楼部存在未充分告知、未征得购房人或访客明确同意的情况下，违规收集、使用个人（人脸）信息，用于购房人身份确认及分销佣金结算认定的行为。长沙市网信办联合市住建局依法对该公司负责人进行约谈，并下发责令改正通知书，责令其在规定期限内完成整改。（来源：网信湖南）

（三）通信管理部门治理实践

1. 安徽、山东、浙江等省市通信管理局通报问题 APP（SDK）名单

（1）北京

11 月 3 日，北京市通信管理局通报 2025 年第十期问题移动互联网应用程序名单。近日，北京市通信管理局通过抽测发现北京市部分移动互联网应用程序存在“违反必要原则收集个人信息”“未明示收集使用个人信息的目的、方式和范围”等侵害用户权益和安全隐患类问题。截至通报，尚有 8 款移动互联网应用程序未整改或整改不到位。2025 年 10 月 10 日，北京市通信管理局通报北京市部分存在侵害用户权益行为的移动互联网应用程序并要求整改。截至通报，仍有 7 款移动互联网应用程序未整改或整改不到位，现予以全网下架处置。

（2）江苏

11 月 3 日，江苏省通信管理局通报 2025 年第 8 批侵害用户权益行为的 APP。江苏省通信管理局近日组织第三方检测机构对省内本地生活等类型的 APP 进行检查，并通报相关单位限期整改。截至通报，尚有 14 款 APP 未完成整改。相关单位于 11 月 14 日前完成整改并反馈，整改落实不到位的，江苏省通信管理局将依法依规组织开展相关处置工作。

（3）安徽

11 月 6 日，安徽省通信管理局通报 2025 年第 7 批侵害用户权益的 APP。安徽省通信管理局近日对省内 APP 进行拨测检查，检测发现 28 款 APP 存

在违法违规收集使用个人信息的问题，2025 年 9 月 23 日对上述违规 APP 企业下达责令改正通知书，要求限期完成整改工作。截至通报，尚有 10 款 APP 未完成问题整改，相关 APP 企业应在 2025 年 11 月 14 日前落实整改要求。逾期不整改的，安徽省通信管理局将依法依规组织开展相关处置工作。

（4）浙江

11 月 12 日，浙江省通信管理局通报 2025 年第 9 批侵害用户权益行为的 APP（小程序）。浙江省通信管理局近日组织第三方检测机构对群众关注的实用工具、网上购物等类型 APP、小程序进行检查，书面要求违规 APP、小程序开发运营者限期整改。截至通报，尚有 13 款 APP、小程序未按要求完成整改。上述 APP、小程序开发运营者在 11 月 24 日前按有关规定进行整改，整改落实不到位的，浙江省通信管理局将依法依规组织开展相关处置工作。

（5）广东

11 月 13 日，广东省通信管理局公开通报 3 款未按要求完成整改 APP，通报下架 5 款 APP。

广东省通信管理局近日持续开展移动应用程序专项治理工作，发出《APP 整改通知书》责令 APP 运营者限期整改，并通知相关应用商店协助督促 APP 运营者整改。截至通报，尚有 3 款 APP 未完成整改。被通报的 APP 主办者应在 2025 年 11 月 21 日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施，切实维护 APP 用户合法权益和网络安全秩序。

截至通报规定时限，经核查复检，尚有 5 款 APP 未按照要求完成整改反馈。为严肃处理上述 APP 的违规行为，广东省通信管理局决定对 APP 予以下架。3 款 APP 未按要求完成整改，予以通报。5 款 APP 未按要求完成整改，予以下架。

（6）上海

11 月 26 日，上海市通信管理局通报 2025 年第十批侵害用户权益行为的 APP（SDK）。上海市通信管理局近日组织第三方检测机构对上海市 APP（SDK）进行抽查，共发现 71 款 APP（SDK）存在侵害用户权益行为。上述 APP（SDK）应对存在的问题立即整改，并对该 APP（SDK）个人信息和用户权益保护工作开展全面自评估，自通报之日起 5 个工作日内将书面整改报告和自评估报告报送上海市通信管理局。对未能在限期内完成整改并提交报告的，上海市通信管理局将依法依规予以处理。

（7）山东

11 月 28 日，山东省通信管理局通报 2025 年第 6 批不合格整改情况 APP。

山东省通信管理局近日对山东省各类 APP 进行合规性检测。截至 11 月 28 日，有 3 款存在问题并被通知限期整改的 APP 未按要求在限期内完成整改反馈。12 月 5 日前，上述 3 款 APP 开发运营者务必完成整改与情况反馈工作。如再次逾期仍未整改到位，山东省通信管理局将视情采取下架等措施。

截至 11 月 28 日，有 4 款存在问题的 APP 经书面要求整改、通报再次要求整改后，仍未在规定时限内完成整改反馈，现予以下架。相关应用商店应立即对有关 APP 进行下架处理，并举一反三，排查反复出现问题的 APP

开发运营者，严格落实分发平台主体责任，把好上架审核关。山东省通信管理局将对下架情况进行持续跟踪。（来源：北京通信业、江苏通信业、安徽省通信管理局、浙江省通信管理局、广东信息通信业、上海通信圈、山东省通信管理局）

（四）其他部门治理实践

1. 最高法发布三例涉未成年人网络保护与违法犯罪惩处典型案例

11 月 20 日，最高法发布三例涉未成年人网络保护与违法犯罪惩处典型案例。

案例一：未经许可擅自使用未成年人肖像，网络店铺承担侵权责任——陈某某诉苏州某公司侵权责任纠纷案

陈某某是一名小学学生。2023 年，陈某某母亲发现某网络平台上一家店铺在未经授权许可的情况下，将陈某某在艺术节的参赛表演图片擅自用于所售卖舞蹈服饰的效果展示中。苏州某公司系该网络店铺的经营者。陈某某以苏州某公司侵犯其肖像权为由提起民事诉讼，请求法院判令苏州某公司赔礼道歉并赔偿损失。

审理法院认为，经比对案涉网络店铺使用的被诉图片，以社会一般人的认知标准，能够确认图片中的肖像为陈某某的形象，陈某某对该图片再现的肖像享有肖像权。陈某某系未成年人，苏州某公司未经陈某某监护人同意，擅自使用陈某某肖像用于商品宣传，侵犯了陈某某的肖像权。据此，审理法院判决苏州某公司向陈某某赔礼道歉并赔偿损失。

案例二：未未成年人网络侵权，监护人应当承担侵权责任——小王诉小李及父母侵权责任纠纷案

小王与小李是小学同班同学。因与小王发生矛盾，小李将自己在班级群中的昵称设置为“小王你好可怜”，个性签名设置为“小王你散架了”，其他人@小李时，群成员均能看到该昵称。小李还在其他平台账号个人主页简介中标注“主挂小王，你好棒”，在有班级同学的群聊中以贬损、嘲讽的口吻发布有关双方校园矛盾的信息。小王因此在班级群、其他平台等网络环境以及校园中受到他人的嘲笑，遭受极大心理压力。小王认为小李的行为侵害了其名誉权，遂将小李及其父母诉至法院，要求小李及其父母赔礼道歉和赔偿损失。

审理法院认为，小李的行为导致小王社会评价降低，构成对小王的侮辱，侵害了小王的名誉权。小李是未成年人，其父母作为监护人未尽到监护责任，应承担侵权责任。据此，审理法院判决小李的父母以书面形式向小王赔礼道歉并赔偿小王经济损失，同时明确，如果小李有财产，从其财产中支付赔偿费用，不足部分由父母赔偿。

案例三：未成年人受网络不良影响犯罪，依法承担刑事责任——被告人李某某、穆某某等敲诈勒索案

2023 年 11 月至 2024 年 3 月间，被告人李某某（18 周岁）、穆某某（17 周岁）伙同张某（另案处理）以某网络游戏代练为名，诱骗他人登录事先准备的账户，后修改账户密码，以远程锁定手机相威胁，向多名被害人敲诈勒索钱财，共计 7.5 万余元。案发后，李某某、穆某某被抓获归案，赔偿

被害人损失并取得谅解。经调查了解到，被告人李某某、穆某某等人系通过短视频平台发布的不良信息习得犯罪方法。

审理法院认为，被告人李某某、穆某某以非法占有为目的，多次敲诈勒索他人财物，已构成敲诈勒索罪。李某某敲诈勒索财物数额巨大，穆某某敲诈勒索未成年人，属于有其他严重情节，均应依法惩处。综合考虑二被告人的犯罪事实、情节，穆某某系未成年人，以及二人退赃退赔等因素，依法对被告人李某某判处有期徒刑一年八个月，并处罚金人民币五千元；对被告人穆某某判处有期徒刑一年三个月，并处罚金人民币二千元。

法院在案件审结后，鉴于案涉短视频平台的未成年人模式未能发挥实质保护作用，内容审核存在疏漏，可检索到大量不良信息，违法风险提示机制不健全，难以对未成年人实现有效警示等问题，依法向短视频平台发送关于规制短视频内容的司法建议，并对服刑的穆某某组织开展回访帮教。（来源：最高人民法院）

2. 北京互联网法院发布一起“搜索提示词”算法侵权案

11 月 26 日，北京互联网法院发布一起“搜索提示词”算法侵权案“深圳某公司与操某、北京某公司网络侵权责任纠纷案”。

深圳某公司是一家从事新能源模式电站开发、设计、建设、智能运维和专业咨询服务的企业。操某在北京某公司运营的网络平台发布十余篇文章、视频，含有如“招摇撞骗”“坑害老百姓”等侵犯深圳某公司名誉权的内容。其中一篇文章所在页面下端的“搜索”框中包含“深圳某公司骗局”等提示词。在涉案网络平台搜索框中输入深圳某公司名称时，也会出

现“骗局”“被骗”等提示词。深圳某公司诉至法院，主张操某发布的涉案文章、视频侵犯其名誉权，北京某公司利用算法在其网络平台“搜索”框中添加设置“深圳某公司骗局”等提示词系人为干预，扩大了涉案侵权内容的传播和影响范围，亦构成侵权，并要求北京某公司对相关算法进行解释说明。在法院的要求下，北京某公司先后两次书面说明涉案搜索提示技术的服务生成机制和页面提示词展示的基本原理、目的意图、运行规则。一审法院判决操某向深圳某公司赔礼道歉并赔偿经济损失。一审判决作出后，双方当事人均未提起上诉，判决已发生法律效力。

法院生效判决认为，操某在涉案文字、视频等内容中多次提及深圳某公司的字号、品牌，如果涉案内容确实构成侵权，深圳某公司的品牌商誉即会受到损害。本案中，被诉侵权言论主要围绕深圳某公司的业务模式，操某在陈述事实之外还作出了超过一般评价限度的侮辱性、贬损性言论。一般而言，公众认知会将企业及其品牌作为一个整体。企业名誉权与品牌商誉紧密相关，故可能会因品牌商誉受损而受到相应损害。故操某的评论降低了深圳某公司产品和服务在所属行业的社会评价，构成名誉侵权。北京某公司应诉后已在合理期限内采取必要措施，尽到了网络服务提供者的事后义务。同时，北京某公司还根据法院要求两次对被诉侵权的搜索提示算法的基本原理、运行逻辑、作用结果作出书面解释说明，即涉案搜索提示词系利用算法根据不特定用户搜索的历史记录自动生成并更新变化，没有人为加入新的内容或者专门聚合负面内容，亦无人工参与事前审核。经过对算法的审查，法院认定北京某公司的搜索提示技术服务不构成对深圳某公司名誉权的侵犯。（来源：北京互联网法院）

境内前沿观察三：人工智能安全专题

导读：11 月，我国人工智能政策立法和监管行动主要关注“人工智能+”、人工智能产业发展和人工智能合成内容标识方面。

国家卫生健康委办公厅等五部门发布《关于促进和规范“人工智能+医疗卫生”应用发展的实施意见》，提出“人工智能+行业治理”、丰富医疗数据供给，推动“三医”协同和跨部门数据共享等多项意见。地方层面，福建、山东、安徽分别印发《福建省推动人工智能产业发展和赋能应用若干措施》《山东省机器人产业科技创新行动计划（2026—2028 年）》《安徽省智能机器人产业发展行动方案（2025—2027 年）》，推动人工智能及机器人产业创新发展。

网信部门针对部分网站平台未有效落实人工智能生成合成内容标识规定要求相关问题，集中查处一批违法违规移动互联网应用程序，依法依规予以约谈、责令限期改正、下架下线等处置处罚。重庆市网信办发布一批违规从事生成式人工智能服务的案例。

关键词：“人工智能+”；人工智能产业发展；人工智能生成合成内容标识

1. 国家卫生健康委办公厅等五部门发布《关于促进和规范“人工智能+医疗卫生”应用发展的实施意见》

10 月 20 日，国家卫生健康委办公厅、国家发展改革委办公厅、工业和信息化部办公厅等五部门发布《关于促进和规范“人工智能+医疗卫生”应用发展的实施意见》，围绕深化重点应用、夯实应用基础、规范安全监管等四个方面，提出十六项意见。

深化重点应用方面，《意见》提出“人工智能+行业治理”。加强卫生健康行业智能监管，促进医疗、医保、医药协同发展和治理，融合推进深化医改与数智赋能。开展关键信息个案数据实时采集分析，实现医疗卫生资源、服务、质量、安全和能级水平的智能监测、分析与预警，建立应对突发公共事件医疗资源紧急调配处置的省级区域智能辅助决策系统。

夯实应用基础方面，《意见》提出丰富医疗数据供给，推动“三医”协同和跨部门数据共享，优化数据收集和标注流程，完善医疗卫生领域数据标注，促进数据要素合规高效、安全有序互通互联、强化应用；优化人工智能算力算法，根据国家算力基础设施总体规划和布局，结合国家人工智能应用中试基地，支持省级统筹建立行业公共支撑服务平台，提供统一、高效、开放的人工智能算力服务。

规范安全监管方面，《意见》提出创新监管方式和预警机制，加强对人工智能研发、审评、准入、应用等各环节监管，开展应用监测评估。建立大模型应用评测验证，从医疗质量安全、个人隐私和数据

安全等方面开展穿透式监管，加强动态监测和预警。（来源：国家卫健委规划发展与信息化司）

2. 福建省政府办公厅印发《福建省推动人工智能产业发展和赋能应用若干措施》

11 月 4 日，福建省政府办公厅印发《福建省推动人工智能产业发展和赋能应用若干措施》，提出支持行业模型攻关、促进研发创新落地、打造行业创新平台等十项措施。

支持行业模型攻关方面，《措施》提出聚焦行业场景需求，引导开发拥有行业数据集、高水平任务处理能力的人工智能行业垂直模型，推动行业“人工智能+”赋能应用。围绕工业、教育、医疗、交通运输、农业、海洋、气象等各领域，发挥行业主管部门作用，强化数据供给，开放应用场景，支持企业、高校、科研院所开展人工智能行业垂直模型产学研用攻关，加快技术开发和应用拓展。

强化数据资源供给，《措施》提出深化公共数据汇聚治理，依托省公共数据资源统一开放平台和省公共数据资源开发服务平台，持续推动公共数据资源开发应用和对外开放。建设省高质量数据集管理服务平台，建立数据集资源库，提供基础信息、技术指导、开放合作等服务，结合人工智能需求每年推动开发 10 个以上高质量数据集。建立数据产品供需对接机制，各地各部门主动协调推动本领域数据资源汇聚储备和治理开发，丰富数据产品和服务供给。支持建设省数据标注基地，培育数据标注产业生态。引导各地打造一批“小而精、小而

优”的数据要素产业园，对入选的省数据要素产业园按规定给予奖励。支持企业、高校、科研院所等探索建设可信数据空间，促进数据要素合规高效流通使用。对入选国家可信数据空间创新发展试点的项目按规定给予奖励。（来源：福建省政府）

3. 贵州省大数据局公开征求《贵州算力券管理办法》（2025年修订版）意见

10月31日，贵州省大数据局公开征求《贵州算力券管理办法》（2025年修订版）意见。征求意见稿共五章二十五条，包括算力券相关主体、算力券相关要求等内容。

征求意见稿指出，贵州算力券是经贵州省人民政府批准，由贵州省大数据发展管理局实施的一种政策工具和数字化凭证，用于购买符合条件的贵州算力服务、国产化算力适配服务、模型训练服务或贵州数据交易等产品服务时，给予综合政策激励。

征求意见稿提出，算力服务由需求方申领。国产化算力适配服务、模型训练服务均由提供方集中申领。数据交易服务需求方和提供方均可申领，同一业务只能一方申领。算力券仅限于申领方自己使用，不得转让、赠送、买卖、出借、重复使用等。（来源：贵州省大数据发展管理局）

4. 山东省科技厅等十九部门印发《山东省机器人产业科技创新行动计划（2026—2028 年）》

11 月 2 日，山东省科学技术厅、中共山东省委组织部、中共山东省委金融委员会办公室等十九部门印发《山东省机器人产业科技创新行动计划（2026—2028 年）》，提出机器人核心技术“筑基”行动、机器人重大产品“焕新”行动、机器人场景应用“拓展”行动、机器人产业发展“提质”行动四项重点任务。

聚力实施机器人核心技术“筑基”行动方面，《计划》提出加快基础理论创新。瞄准机器人基础理论研究与源头创新，加快机器人新型仿生机理、智能传感与认知理解、模型和数据混合驱动控制、集群智能协同等基础研究，脑机或肌电高通量接口与实时交互、高保真数字物理仿真引擎、大模型驱动的具身智能等应用基础研究，催生原创性、前瞻性、引领性成果，形成机器人基础理论研究的相对优势。

机器人重大产品“焕新”行动方面，《计划》提出推出先进整机产品。持续巩固新一代智能协作机器人、高速高精度重载工业机器人、重载移动机器人等工业机器人产品优势；针对性开发应急救援、智慧农业、地质勘探、深空深地深海作业机器人等特种机器人；加快研制养老服务机器人、康复机器人、外骨骼机器人、微创手术机器人等服务机器人，推动机器人整机及相关产品迭代焕新、提“智”向新。（来源：山东省科学技术厅）

5. 安徽省人民政府办公厅印发《安徽省智能机器人产业发展行动方案（2025—2027 年）》

11 月 10 日，安徽省人民政府办公厅印发《安徽省智能机器人产业发展行动方案（2025—2027 年）》，围绕攻关核心技术、打造标志性产品、拓展高价值场景等五个方面，提出十五项措施。

攻关核心技术方面，《方案》提出支持关键技术攻关。围绕智能机器人本体设计、环境感知、运动控制、动态执行和人机交互等环节，突破一批关键共性技术。聚焦智慧“大脑”、敏捷“小脑”等智能决策与控制技术和强健“肢体”的高动态、高爆发、高精度运动结构，突破一批前沿引领技术。对牵头承担智能机器人领域国家重大专项项目的企业予以配套支持。

打造标志性产品方面，《方案》提出开发多类型机器人大模型。研发融合视觉、听觉、触觉等多模态大模型，构建数据驱动的高精度世界模型，突破群体智能等技术，提升动态环境下复杂任务规划、执行和多机协作能力。推动基于模型的运动控制算法、灵巧操作、人机交互算法等成果转化，实现适应不同任务场景的垂类应用。研发通用技术底座，包括机器人专用操作系统、高保真仿真平台、高质量数据集及开发环境等，推动与具身智能大模型深度融合，系统打造智能机器人应用生态。（来源：安徽省政府）

6. 网信部门依法集中查处一批存在人工智能生成合成内容标识违法违规问题的移动互联网应用程序

11 月 25 日消息，网信部门近日针对部分网站平台未有效落实人工智能生成合成内容标识规定要求相关问题，集中查处一批违法违规移动互联网应用程序，依法依规予以约谈、责令限期改正、下架下线等处置处罚。

主要违法违规情形包括两个方面：（1）人工智能生成合成服务提供者未对生成合成的内容添加显式标识；提供生成合成内容导出功能时，未在文件中添加显式标识；在生成合成内容的文件元数据中，未添加包含属性信息、服务提供者名称或者编码、内容编号等制作要素信息的隐式标识；隐式标识添加位置不规范等。（2）网络信息内容传播服务提供者未落实隐式标识核验、在发布内容周边添加显著提示标识相关要求；未在生成合成内容传播活动涉及的文件元数据中添加属性信息、传播平台名称或编码、内容编码等传播要素信息；未向用户提供声明生成合成内容的功能等。（来源：网信中国）

7. 重庆市网信办发布一批违规从事生成式人工智能服务典型案例

11 月 12 日，重庆市网信办发布“清朗巴渝”专项行动典型案例。其中，涉及一批违规从事生成式人工智能服务的案例。结合“清朗·整治 AI 技术滥用”专项行动，依据《网络信息内容生态治理规定》，针对“*语”“AI·*ote”“灵*AI”等 APP 提供制作发布违背伦理、

法律相关功能的行为，责令其深入整改；情节严重的，依法予以下架；对利用人工智能技术制作的“重庆河里出现**”“奉节发生**事件”等谣言信息依法清理。

同期还通报了违规从事互联网信息服务网站，假冒仿冒网站，发布不实信息的账号，传播低俗色情、网络赌博信息网站、账号，涉企网络“黑嘴”，短视频恶意营销等典型案例。（来源：网信重庆）

8. 上海市委网信办发布“亮剑浦江·2025”专项行动成果

11 月 28 日，上海市委网信办发布“亮剑浦江·2025”专项行动成果。

“亮剑浦江·2025”专项执法行动期间，上海市区两级网信、市场监管部门巡查属地 APP 超 2100 款，对 20 款、总下载量达 1.04 亿的 APP 展开集中培训与精准指导，督导属地 2.5 万家自动售货机柜、246 个售楼处规范应用人脸识别技术，指导属地平台累计清理涉违规偷拍帖文 1.2 万余条，处理违规账号 170 余个，督导 375 家医疗服务类互联网企业完成隐患排查和问题整改，组织 100 余家重点企业开展普法培训。

专项行动期间，网信部门牵头出台《上海市人脸识别技术应用安全治理专项工作协同机制（1.0 版）》和人脸识别“六不得”合规倡议；发布《偷拍内容网上传播专项整治负面清单》，提出 10 项平台具体整改要求；推出《医疗服务类互联网企业数据安全合规指引》等行业规范；制定《未成年人网络保护四方协同机制》等。（来源：网信上海）

境外前沿观察：月度速览十则

导读：11 月，境外国家和地区持续推动网络安全领域政策法律与执法活动，重点关注人工智能、个人信息保护等方面。

人工智能方面，欧盟数据保护监督局发布《人工智能系统风险管理指南》，重点聚焦人工智能系统在数据处理链条中引入的技术性风险，并提出全流程风险管理方法与合规建议，旨在帮助数据控制者在开发、采购和部署人工智能系统时进行数据保护风险评估。欧盟委员会发布用于报告具有系统性风险的通用用途人工智能模型严重事故的统一模板，以促进成员国及相关企业在执行《人工智能法》及《通用用途人工智能行为准则》时实现一致且透明的事故通报。

个人信息保护方面，印度政府正式公布《2025 年数字个人数据保护规则》，标志着印度在个人数据管理和隐私保护领域迈入新的制度阶段。根据规则，印度新的数据保护体系将依法采取分阶段实施方式，以确保制度平稳落地。美国德克萨斯州总检察长办公室宣布与谷歌就隐私索赔达成 13.75 亿美元和解协议，涉及谷歌对地理位置数据、无痕浏览活动数据及生物特征识别符的不当处理。韩国科学技术信息通信部与个人信息保护委员会宣布，将就电商企业 Coupang 个人信息大规模泄露事件开展全面调查，并迅速采取监管措施。

关键词：人工智能；个人信息保护

1. 欧盟委员会发布具有系统性风险通用人工智能模型严重事故报告模板

11 月 4 日，欧盟委员会发布用于报告具有系统性风险的通用用途人工智能模型严重事故的统一模板，以促进成员国及相关企业在执行《人工智能法》及《通用用途人工智能行为准则》时实现一致且透明的事故通报。根据《人工智能法》《通用用途人工智能行为准则》《通用用途人工智能模型提供者指南》等法律文件的规定，相关人工智能模型提供者有义务向欧盟人工智能办公室以及在适当情况下向各成员国主管部门报告涉及严重事故的相关信息。此次模板以 DOCX 和 PDF 格式向公众开放下载，旨在推动欧盟范围内人工智能监管的统一化实施，提高事故报告质量，并强化对具有系统性风险人工智能模型的预警和监管能力。（来源：欧盟委员会）

2. 欧盟数据保护监督局发布《人工智能系统风险管理指南》

11 月 11 日，欧盟数据保护监督局发布《人工智能系统风险管理指南》，聚焦人工智能系统在数据处理链条中引入的技术性风险，并提出全流程风险管理方法与合规建议。指南旨在帮助数据控制者在开发、采购和部署人工智能系统时进行数据保护风险评估。

指南强调，风险管理是指一个组织控制风险的过程，而该活动的核心是风险评估。在风险管理过程中，组织需要连续地识别、分析和评估风险，然后进入风险处理阶段。风险管理过程的步骤如下：（1）风险识别。要求系统性地寻找可能影响组织目标的风险来源，并建立

风险登记册；（2）风险分析。在定性基础上评估风险发生的概率及其对数据主体的潜在影响；（3）风险评估。需要将分析结果与组织的风险偏好进行比较，以判断风险是否可接受；（4）风险处理。包括制定与实施风险缓解措施、评估其成效。如剩余风险仍不可接受，则需进一步处理。指南强调，风险管理应是持续性的迭代过程。

指南指出，风险可能出现在人工智能系统开发周期的不同阶段，因此组织需要了解人工智能系统开发周期与传统系统开发周期的差异。指南将生命周期划分为九个阶段：（1）构思/分析：明确系统目标、任务场景与模型架构；（2）数据采集与准备：获取并格式化训练数据，确保其质量、合规性与代表性；（3）开发：训练模型、调参、测试，可结合内部开发与外部预训练模型；（4）验证与确认：确保模型满足功能与非功能需求，评估准确性、鲁棒性与泛化能力；（5）部署：将模型上线至设备或服务器；（6）运行与监控：持续监控系统表现并根据反馈调整；（7）持续验证：对于采用持续学习的系统，需要定期检测性能并更新测试集；（8）复审机制：根据实际运行数据重新评估风险，并纳入下一周期；（9）退休：安全退役系统，确保不留风险。针对许多组织通过外部采购模型与服务，指南强调采购环节需确保透明性、公开招标、明确技术要求并严格监督执行。

指南强调人工智能系统的可解释性与可说明性在人工智能治理中的基础作用：（1）可解释性：侧重理解模型内部结构与输入输出关系，主要面向技术人员；（2）可说明性：聚焦对具体预测给出易懂理由，更面向用户和监管者。对于深度神经网络等黑箱模型，由于

难以真正解释内部机制，因此需要采用事后可说明技术。（来源：欧盟数据保护监督局）

3. 印度发布《2025 年数字个人数据保护规则》

11 月 13 日，印度政府正式发布《2025 年数字个人数据保护规则》，标志着印度在个人数据管理和隐私保护领域迈入新的制度阶段。根据规则，印度新的数据保护体系将采取分阶段实施方式，以确保制度平稳落地。

规则明确数据处理主体在向数据主体提供告知时的义务，要求以清晰、易懂的语言说明所收集的个人数据种类、处理目的及相关服务，并提供便捷的渠道以便数据主体撤回同意、行使权利或向数据保护委员会提出投诉。同时，规则建立了“同意管理人”的注册与监管机制，规定其申请条件、职责义务及可能的暂停或取消注册情形，以保障数据主体的合法权益。

数据安全方面，规则规定数据处理者必须采取强化的安全措施，包括加密、数据掩码、访问控制、日志记录与监控、数据备份及持续处理保障机制，并须在与数据处理方的合同中加入合理的安全防护条款。若发生数据泄露，数据处理者必须在 72 小时内向主管机构提交完整报告，并立即通知受影响的个人。企业若未能及时披露违规行为，最高可面临 20 亿卢比（约合 2200 万美元）的罚款。

规则还规定数据保存期限与删除机制，要求数据处理者在特定目的完成后在规定时间内删除相关数据及日志，除非法律另有要求。同

时，数据处理者必须至少保存相关记录一年，并在数据删除前至少48小时通知用户，以便用户登录账户或采取措施阻止删除。数据处理者须公开其数据保护官员或相关负责人的联系方式，以便数据主体咨询。对于儿童及残障人士，规则要求在处理其个人数据前必须取得可验证的父母或合法监护人同意，并规定了验证方式及相关机构的职责等。（来源：印度政府）

4. 欧盟就数字一揽子政策发布情况说明

11月19日，欧盟就数字一揽子政策发布情况说明。说明指出，欧盟近期的数字政策主要包括：（1）《数字综合监管改革提案》，集中简化人工智能、网络安全和数据领域规则；（2）《数据联盟战略》，旨在为人工智能释放更多高质量数据；（3）“欧洲商业数字钱包”系统，为企业提供可在全欧盟范围使用的统一数字身份工具，使跨境运营更为顺畅。

《数字综合监管改革提案》旨在通过统一和简化欧盟在数据保护、网络安全及人工智能领域的多项规则体系，预计可减少15亿欧元的合规成本。在数据领域，提案将优化企业的数据访问能力，从而增强欧洲企业在全球的竞争力，同时在维护高水平个人数据保护的前提下，使隐私框架更加清晰、可预期、并促进创新。在网络安全方面，提案将建立统一的事件报告入口，使企业能够在单一系统内履行所有相关报告义务。在人工智能监管上，提案将更明确《人工智能法》与其他法律之间的衔接关系，并将高风险规则的生效时间与相关支持工具

（如技术标准）的可用性相挂钩；同时，通过扩展监管沙箱与人工智能素养等支持性措施，减少企业合规成本，并强化监管工作的集中协调，由欧盟人工智能办公室统一开展监督。《数据联盟战略》进一步提出扩大人工智能训练和应用所需的高质量数据供给，通过对数据规则的整合、更新与精简，在确保基本权利保护的基础上提升数据共享效率，并强化欧洲数据主权。

“欧洲商业数字钱包”系统旨在为企业和公共机构提供快速、安全的数字身份识别、认证与信息交换机制。该系统将使企业能够在整个欧盟范围内更便捷地运营，减少繁琐的行政程序与合规成本，并可能为企业每年节省高达 1500 亿欧元。该机制将进一步促进欧盟单一市场的数字化转型，提高跨境经营效率，并为经济活动提供更高的安全性与可靠性。（来源：欧盟委员会）

5. 美国白宫发布《启动创世纪计划》行政命令，通过人工智能加速国家科学发现进程

11 月 24 日，美国白宫发布《启动创世纪计划》行政命令，提出“创世纪计划”，将以人工智能加速科学发现为核心，通过训练科学领域基础模型、打造人工智能科研代理、推动自动化与智能化实验和制造，显著提升科研效率和创新能力，并放大联邦研发投入的社会回报。行政命令主要内容如下：

一是设立“创世纪计划”总体框架，明确能源部与白宫科技决策链条的职责分工：行政命令正式设立“创世使命”，将其定义为围绕

紧迫国家挑战的人工智能赋能科学发现国家行动。能源部部长负责在能源部内部具体实施“使命”，包括设定优先事项，并在法律授权范围内将涉“使命”的能源部资源整合为一个安全、统一的平台；部长可指定高级政治任命官员负责日常运行。总统科学技术事务助理通过国家科学与技术委员会对“使命”提供总体领导和跨部门协调，确保该使命与美国整体国家战略目标相一致。

二是建设“美国科学与安全平台”，打造统一的人工智能科研基础设施：行政命令要求能源部建立并运营“美国科学与安全平台”，作为“使命”的核心基础设施，以一体化方式提供人工智能赋能科研的关键能力，包括：（1）高性能计算资源：整合能源部国家实验室超级计算机和安全云端人工智能计算环境，用于大规模模型训练、仿真和推理；（2）人工智能建模与分析框架：开发用于探索设计空间、评估实验结果和自动化科研工作流程的人工智能代理和工具；（3）计算与优化工具：构建人工智能赋能的预测模型、仿真模型和设计优化工具，服务多学科科研需求；（4）领域基础模型：面向先进制造、生物技术、能源、量子与半导体等多种科学领域，开发相应的领域特定基础模型；（5）安全数据访问体系：在遵守保密要求、隐私保护、知识产权和联邦数据管理标准的前提下，整合专有、联邦整理、开放科学数据集以及利用能源部算力生成的合成数据，提供安全访问渠道；（6）实验与生产工具：布局支持自主与人工智能增强实验和制造的实验室与生产设施，推动“机器人实验室”和智能制造体系建设。

三是梳理和动态更新“国家科学与技术挑战”清单，引导人工智能科研资源聚焦重大领域。为确保“创世使命”聚焦国家战略重点，行政命令要求：（1）60 日内，能源部需提出至少 20 项具有国家重要性的科学与技术挑战，重点围绕与《国家科学与技术备忘录第 2 号》一致的优先领域，包括先进制造、生物技术、关键材料、核裂变与核聚变能源、量子信息科学以及半导体与微电子等；（2）在此基础上，总统科学技术事务助理通过国家科学与技术委员会，与参与机构协同制定扩展版挑战清单，将其他部门提出的优先课题纳入其中，形成“创世纪计划”首批重点攻关任务；（3）参与“使命”的各联邦机构须在法律和职责范围内，依托“美国科学与安全平台”开展与上述挑战清单相一致的科研开发；（4）能源部每年需会同行政部门对挑战清单进行评估与更新，结合已取得进展、新兴国家需求以及现政府研发优先事项，动态调整攻关方向。（来源：美国白宫）

6. 美国德克萨斯州与谷歌就隐私问题达成 13.75 亿美元和解协议

10 月 31 日，美国德克萨斯州总检察长办公室宣布与谷歌就隐私索赔达成 13.75 亿美元和解协议，该协议涉及该州于 2022 年针对谷歌提起的两起诉讼。这两起诉讼分别指控谷歌对地理位置数据、无痕浏览活动数据及生物特征识别符的不当处理。

在第一起诉讼中，德州依据《德克萨斯州欺骗性贸易行为法》指控谷歌存在系统性欺骗行为，声称该公司“蓄意误导、欺骗并隐瞒关

键事实”，涉及对用户地理位置数据的追踪、使用和商业化操作。起诉书特别指出，即便用户启用“无痕模式”，谷歌仍持续追踪、收集并利用用户数据，此举与其公开声明相悖。诉状援引谷歌自身隐私政策的内容作为支持《德克萨斯州欺骗性贸易行为法》指控的证据。

第二起诉讼指控谷歌通过 Google Photos、Google Assistant 和 Nest Hub Max 智能家居设备收集语音特征、面部轮廓等生物特征识别符，违反德州《生物特征识别符捕获与使用法》。（来源：JDSUPRA）

7. 法国巴黎检察院就内容审核与算法风险对 TikTok 启动初步调查

11 月 4 日，法国巴黎检察院发布通告，表示其于 2025 年 9 月 11 日收到国会调查委员会关于 TikTok 心理影响问题的相关正式报告后，决定对其启动初步调查。该报告向司法机关移交了委员会收集的多项材料，指出 TikTok 在内容审核方面存在不足，未能有效限制未成年人使用，并凭借其复杂算法使处境脆弱者迅速陷入特定内容循环，从而可能被推向自杀等极端风险。

目前，调查已交由巴黎警察局下属的网络犯罪打击大队负责。调查重点围绕多项潜在刑事违法行为展开，包括：以有组织形式提供在线平台以促成非法交易；以有组织形式破坏自动化数据处理系统正常运行；宣传被视为助长自杀的产品、物品或方法。调查内容涵盖平台对相关违法行为的法定通报义务、算法实际运行机制与向用户展示方

式的一致性，以及与促进自杀相关内容的编辑与传播情况。（来源：法国巴黎检察院）

8. 爱尔兰媒体委员会依据《数字服务法》对社交平台 X 启动正式调查

11 月 12 日，爱尔兰媒体委员会宣布，依据欧盟《数字服务法》正式对在线平台 X 的运营方立案调查，以评估其是否违反该法第 20 条规定。此次调查源于该机构平台监督团队对 X 履行用户申诉权保障义务的担忧，并得到非政府组织 HateAid 及一名用户投诉所提供信息的补充。

《数字服务法》第 20 条明确要求，平台必须向用户提供有效的内部投诉处理系统，使用户能够对平台所作出的删除、屏蔽内容或暂停、终止账户等决定提出申诉。本次调查的重点包括：用户在举报认为违反平台服务条款的内容后，是否能够对平台不予删除的决定提出申诉；用户是否被充分告知举报处理结果及其享有的申诉权；以及 X 是否具备一个便捷、易用的内部投诉处理机制。若平台被认定违反《数字服务法》，媒体委员会可处以最高相当于全球营业额 6%的行政罚款，相关罚款须由巡回法院或高等法院确认。在调查过程中，监管机构与平台亦可签订具有约束力的“承诺协议”，由平台承诺采取措施解决合规问题。

爱尔兰媒体委员会数字服务专员表示，根据前期监督以及多方信息分析，有合理理由怀疑 X 可能未遵守该法第 20 条第 1 款和第 3 款

的义务。调查将重点审查 X 是否充分告知用户相关决定及其申诉权，确保用户能够行使法律赋予的基本权利。（来源：爱尔兰媒体委员会）

9. 欧盟委员会就谷歌涉嫌违反《数字市场法》启动正式调查

11 月 13 日，欧盟委员会宣布，已正式对谷歌在搜索结果中下调媒体出版商内容排序的做法启动调查程序，以评估是否遵守《数字市场法》关于向出版商提供公平、合理、非歧视性网站访问条件的义务。

委员会在持续监测中发现迹象显示，谷歌依据其所谓的“站点信誉滥用政策”，对包含商业合作伙伴内容的新闻媒体及其他出版商网站实施搜索排名下调。谷歌称该政策旨在打击涉嫌操纵搜索排名的行为，但委员会注意到，该规则可能直接影响出版商依赖商业合作实现网站与内容变现的普遍且合法的经营模式。因此，委员会将重点调查谷歌母公司 Alphabet 是否通过下调相关网站和内容的排序，损害出版商开展合法业务、促进创新或与第三方内容提供商合作的自由。

委员会强调，启动程序并不预设任何不合规结论，而是意味着委员会将进一步深入审查该案。如调查显示存在不合规证据，委员会将向 Alphabet 通报初步调查结果，并阐明拟采取的整改措施或 Alphabet 需实施的补救措施。委员会计划在程序启动后的 12 个月内完成调查。若确认存在违规行为，委员会可对企业处以其全球年营业额最高 10% 的罚款；如为重复违规，罚款幅度可提高至 20%。在系统性违规情况下，委员会还可施加额外补救措施，包括要求“守门人”出售相关业

务或禁止其收购与系统性不合规相关的新增服务。（来源：欧盟委员会）

10. 韩国政府就 Coupang 大规模个人信息泄露事故启动联合调查

11 月 29 日，韩国科学技术信息通信部与个人信息保护委员会宣布，将就电商企业 Coupang 个人信息大规模泄露事件开展全面调查，并迅速采取监管措施。

Coupang 于 11 月 19 日首次向当局报告称，共 4536 个用户账号的姓名、电子邮件、地址等信息疑似泄露。但在后续调查中，泄露规模被大幅修正，超过三千万个账号被判定存在信息外泄，事态严重性显著提升。基于泄露规模巨大且可能引发进一步损害的判断，韩国科学技术信息通信部决定自 11 月 30 日起组建并运作“民官联合调查团”，全面查明事故原因并制定再发防止措施。委员会方面表示，已于 11 月 20 日和 11 月 29 日两次接收 Coupang 提交的泄露申报，并自 11 月 21 日起展开调查。鉴于泄露信息中包含大量公民的联系方式和住址等敏感资料，委员会将迅速查清泄露规模与经过，一旦确认违反《个人信息保护法》规定的安全措施义务，将依法进行严格制裁。

为防止泄露信息被不法分子用于发送诈骗短信、构建钓鱼页面或实施语音诈骗等二次攻击，科学技术信息通信部和委员会已通过相关专题网站向公众发布安全警示，提醒用户警惕以“受害补偿”“受害事实查询”“退款”等关键词伪装的短信钓鱼、通过搜索结果恶意曝

光的钓鱼网站，以及假借通知泄露情况和指导补偿程序的语音诈骗，并提供了举报方式及应对指引。有关部门亦公布了举报和咨询渠道，提醒用户提高警觉并采取必要防护措施。（来源：韩国个人信息保护委员会）

行业前沿观察一：高工专栏

导读：全球经济承压，网络空间安全行业却在逆境中崛起。生成式人工智能、低空经济等新兴技术的涌现，为网络安全产业带来新机遇。习近平总书记强调，广大工程技术人员应坚定科技报国理想，推动发展新质生产力。在此背景下，北京网络空间安全协会推出“高工专栏”，以“网络空间安全-新技术、新引擎、新发展”为主题，邀请新晋“网络空间安全专业高级工程师”撰稿。

专栏旨在传播网络安全新技术、新思想和新理念，优秀稿件将在全国范围宣传，并在相关活动中做主题交流。稿件内容可涵盖业务安全、数据安全、信息内容安全及网络与系统安全等方向，需为创新性技术分析文章，字数约 2000 字，个人署名，可配照片。

请于每月 15 日前投稿至 bjcsa@bjcsa.org.cn，审稿通过后，将在本月或下月刊载。

联系人：薛老师

联系方式：17200383428、010-67741727

关键词：人工智能、网络安全、高工专栏、互联网

1.大模型幻觉分析与治理路径研究

摘要：本文基于“构建安全可信的网络生态：技术协同与治理路径探索”系列培训内容，系统分析大模型幻觉问题的分类、成因及治理路径，旨在为人工智能安全治理提供理论支持与实践参考。研究通过文献梳理与培训内容归纳，将幻觉问题划分为忠实性幻觉与事实性幻觉两类：前者体现为模型输出与输入指令或上下文逻辑相悖，后者表现为生成内容与客观事实不符。针对这两类问题，本文对比了检索增强生成（RAG）与模型微调两类技术路径的优劣。RAG 通过外部知识库实时检索增强生成内容的准确性，尤其适用于动态知识场景，但其效果高度依赖检索质量与分块策略；模型微调则通过参数优化使模型内化领域知识，从根源上提升输出的可靠性，但面临训练成本高与伦理对齐挑战。本研究提出“微调+RAG”协同治理框架，通过微调塑造模型的领域认知能力，再结合 RAG 注入实时知识，形成优势互补，构建“微调奠基，RAG 增强”的综合框架，成为兼顾模型内生能力与外部知识时效性的最优解。

关键词：大模型幻觉；RAG；模型微调；人工智能安全

引言：随着大模型在文本生成、跨模态合成等领域的广泛应用，其“幻觉”问题已成为制约 AI 可信度的核心挑战。本次培训以“构建安全可信的网络生态”为主题，从技术协同与治理路径角度，深入探讨了人工智能赋能网络空间治理的伦理边界、安全风险及应对策略。本文结合培训内容，系统分析大模型幻觉的分类与成因，并针对性地提出改善路径，以期为行业实践提供参考。

大模型幻觉的类型与危害

大模型的“幻觉”问题，即模型生成不忠实于输入源或不符合客观事实的内容，不仅影响用户体验，更在特定场景下可能引发严重的实际危害。根据其本质特征，幻觉主要可分为“忠实性幻觉 1”与“事实性幻觉 2”两大类，二者在核心问题、验证依据及危害层面上均有显著差异。

1.1 忠实性幻觉

忠实性幻觉，特指大语言模型生成的内容未能忠实于其接收到的输入信息。这种不忠实性并非指内容违背了世界知识，而是指其与用户给定的指令、提供的上下文背景或内部的逻辑链条产生了矛盾[1]。根据文档中的分类，其具体表现形式可归纳为以下三种：

（1）指令不一致

这是最为直观的一种幻觉类型，表现为模型的输出完全偏离或未能执行用户的明确指令。例如，用户明确指令：“请用日语总结一下这篇关于日本茶道的文章。”而模型输出却可能是用中文开始详细解释茶道的历史，并未总结文章要点。这种幻觉直接反映了模型在指令理解与遵循能力上的缺陷，使其无法成为可靠的任务执行工具。

（2）上下文不一致

在长文本生成或多轮对话等需要维持上下文一致性的场景中，模型后续的陈述可能与之前自己提供的信息产生矛盾。例如，在对话历史中，模型在前一轮回答中已确认：“故事的主角小明没有兄弟姐妹。”但在后续几轮对话后，模型却可能说出：“小明的弟弟建议他……”

这种前后信息的冲突会严重破坏对话的逻辑连贯性与可信度，让用户感到困惑与不信任。

（3）逻辑不一致

当任务涉及数学解题、逻辑分析等需要严谨推理的环节时，模型的推理过程或最终结论可能存在内部矛盾。一个典型的例子是，用户提问：“如果 A 大于 B，B 大于 C，那么 A 和 C 谁更大？”模型可能给出这样的推理：“因为 A>B，B>C，所以 A<C。”其结论与前提条件发生了根本性的逻辑冲突。这类幻觉揭示了模型在深层推理能力上的不足。

此类忠实性幻觉在摘要生成、对话系统、内容创作等应用中尤为突出。它可能导致生成的信息与用户需求南辕北辙，或者在关键决策过程中提供相互矛盾的依据，从而引发信息误导与决策错误，降低了模型的可信度与实用性[2]。

1.2 事实性幻觉：违背客观知识

与忠实性幻觉不同，“事实性幻觉”是指大语言模型生成的内容与可验证的现实世界事实不一致的现象。它是大模型“胡说八道”的主要表现之一，即模型非常自信地输出一些看似合理但实际上是错误或虚构的信息[3]，如表 1 所示。

事实性幻觉的核心问题在于其输出内容不符合客观事实或世界知识。验证其是否存在，需要依靠外部真实世界知识库进行交叉验证。例如，模型可能声称“爱因斯坦在 1905 年发现了相对论”（事实是提出了狭义相对论），或断言“长江发源于青海省玉树藏族自治州”

（实际源头是唐古拉山脉）。这些错误看似细微，却直接动摇了模型作为信息提供源的权威性。

表 1 事实性幻觉与忠实性幻觉对比表

特征	事实性幻觉(Factualness Hallucination)	忠实性幻觉(Faithfulness Hallucination)
核心问题	输出内容不符合客观事实或世界知识	输出内容偏离了用户的指令或提供的上下文
验证依据	需要依靠外部真实世界知识进行验证	仅需对照用户输入的原始内容或指令进行验证
典型示例	声称“爱国斯坦在 1905 年发现了相对论”(事 实是提出了狭义相对论);或将“长江发源于 青海省玉树藏族自治州”(实际源头是唐古山脉) 。	用户要求总结一篇关于“人工智能在医疗中的应 用”的文章,模型却生成了关于“人工智能在金融领域”的内容。

1.3 幻觉对网络生态安全的威胁

综上所述，无论是偏离输入的忠实性幻觉，还是违背客观事实的事实性幻觉，都对构建安全可信的网络生态构成了直接威胁。治理大模型幻觉绝非仅仅是提升模型性能的技术问题，更是关乎人工智能赋能网络空间治理的伦理边界与安全底线的核心议题[4]。它是构建“安

全可信网络生态”不可或缺的技术基石，后续的治理路径必须针对这两种幻觉的不同特性，采取针对性的技术与管理措施。

幻觉治理的技术路径

大模型幻觉治理的技术路径主要可分为两类：一是通过检索增强生成（RAG）技术，借助外部知识库实时校正模型输出；二是通过模型微调，使模型内部参数更适应特定领域与任务需求，从根源上提升生成内容的可靠性[4]。两者各有优势，且在实践中有互补作用。

2.1 RAG：基于检索的实时知识增强

RAG（Retrieval Augmented Generation）的基本思想是在大语言模型生成答案之前，先从外部知识源中检索相关信息，并将检索结果作为上下文与用户问题一并输入模型，从而增强生成内容的准确性与事实一致性。如图 1 所示，RAG 核心流程包括：

索引：将外部知识源（如文档、数据库）进行分块并编码为向量，存入向量数据库。

检索：将用户查询同样编码为向量，在向量数据库中进行相似度搜索，找出最相关的文本片段。

增强生成：将检索到的文本片段与原始查询组合成增强提示（Prompt），输入大语言模型生成最终答案。

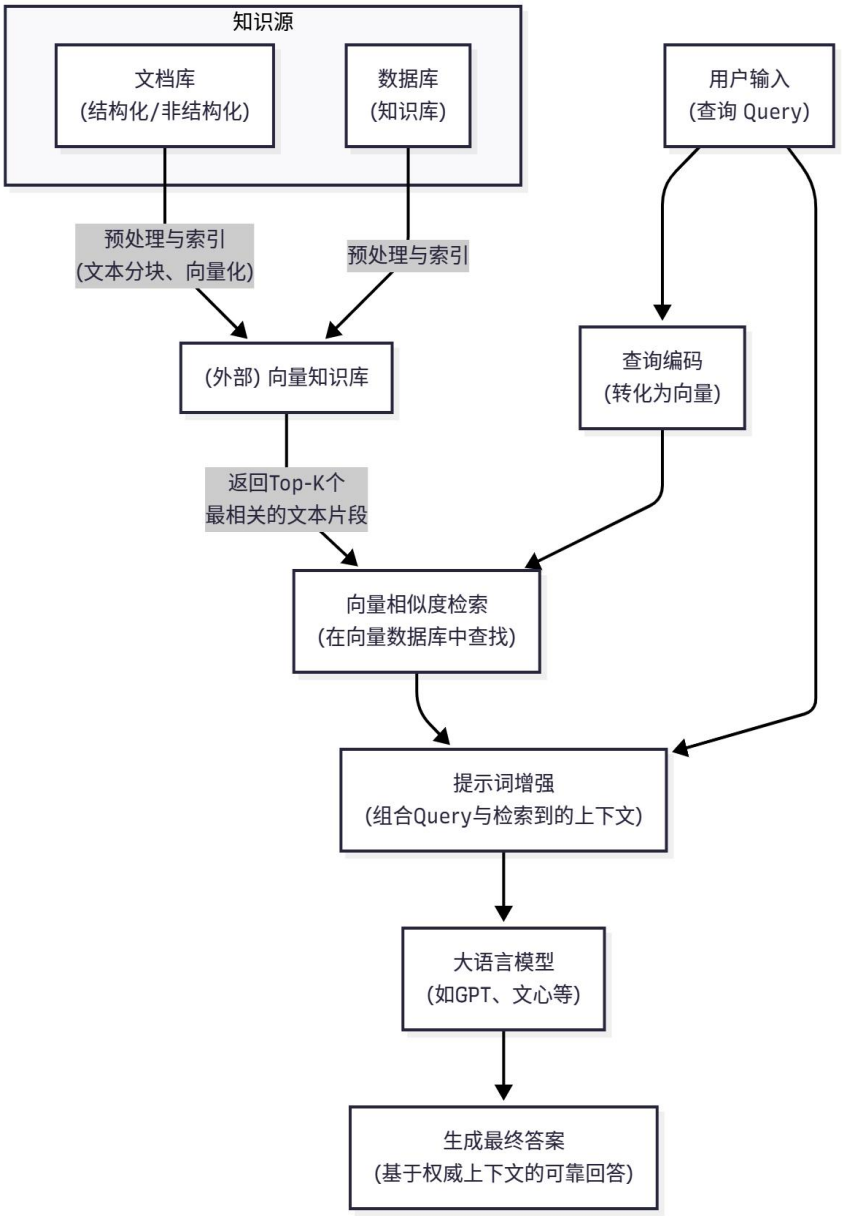


图 1　RAG 处理流程图

这一机制能有效抑制事实性幻觉，因为它要求模型的回答严格建立在检索到的权威信息基础上。为了提升 RAG 系统的性能，以下优化策略至关重要：

文本分块优化：针对专业领域文档（如电力施工手册），采用符合其内容结构的动态分块策略至关重要。例如，不采用固定的字符长度分块，而是按文档的“章-节”结构进行划分，确保每个文本块（Chunk）

承载一个相对完整的语义单元，从而显著提升检索的准确性和上下文的相关性。

GraphRAG 应用：对于需要复杂推理的查询，传统 RAG 可能表现不佳。GraphRAG 通过构建知识图谱，将实体和关系结构化，支持基于图结构的检索与推理。它能更好地处理“多跳推理”问题，通过遍历实体关联路径，合成分散在多个数据点中的深层信息，从而提供更全面、连贯的答案。

然而，RAG 技术也存在其局限性。其效果高度依赖于检索质量，若外部知识库不完整或检索算法不精准，则可能引入错误信息或无法提供有效上下文。此外，检索步骤会增加系统的响应延迟。因此，RAG 常需与模型微调技术结合使用，以弥补其不足。

2.2 模型微调：参数优化与伦理对齐

与 RAG 借助外部知识进行“外挂式”修正不同，模型微调旨在通过训练，将特定领域的知识、任务规范与价值准则内化到模型参数中，从而从根本上提升模型的内在可靠性与安全性。这是一种“外科手术式”的参数优化，使通用大模型转变为适应特定场景的领域专家。其核心实践主要围绕参数高效微调与价值对齐微调两个维度展开。

2.2.1 LoRA 高效微调：低成本适配的工程实践

面对拥有数百亿乃至万亿参数的大模型，传统的全参数微调需耗费巨大的计算资源与存储成本，难以推广。低秩自适应（LoRA, Low-Rank Adaptation）技术为此提供了一种高效、轻量的解决方案。其核心假设是：模型在适应新任务时，其权重矩阵的更新具有较低的

“内在秩”（Intrinsic Rank）。因此，LoRA 不直接更新原始的巨大权重矩阵 W∈Rd×k，而是冻结其参数，并注入一个可训练的低秩分解矩阵 ΔW=BA，其中 B∈Rd×r,A∈Rr×k，且秩 r≪min(d,k)。

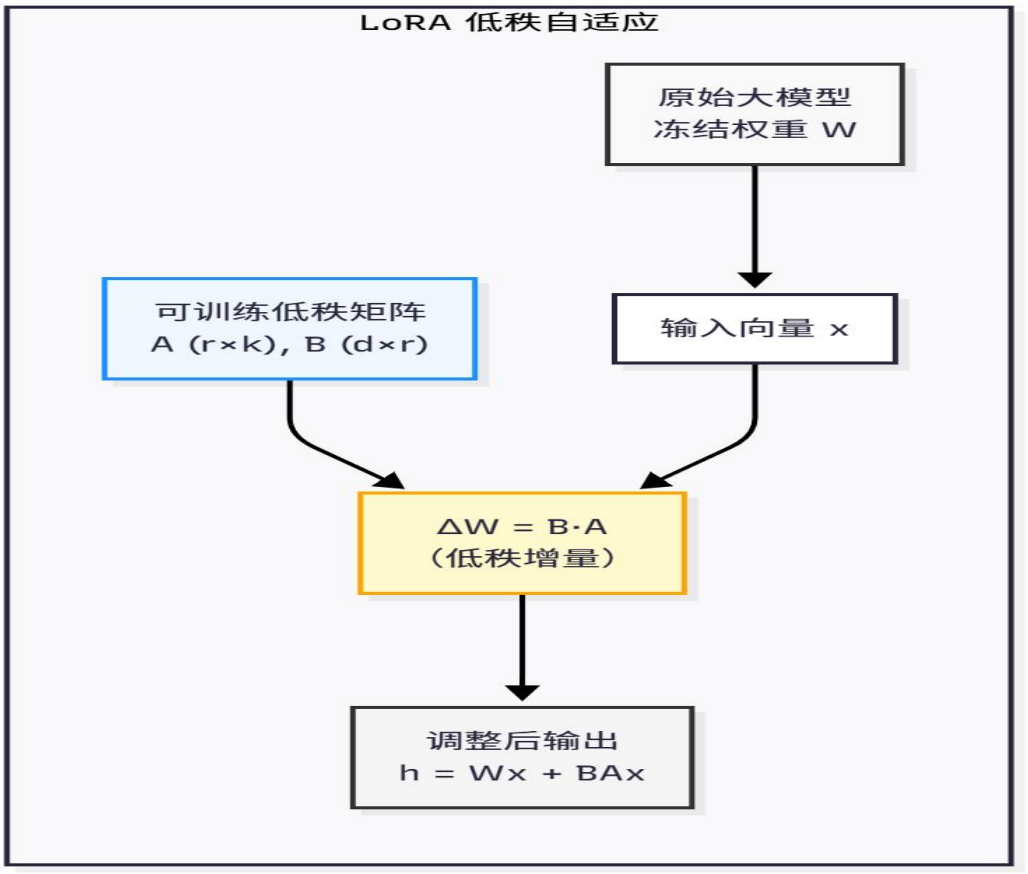


图 2 LoRA 自适应流程图

如图 2 所示，在前向传播过程中，调整后的输出为 h=Wx+ΔWx=Wx+BAx。训练时，仅需更新小矩阵 A 和 B 的参数，其参数量通常不到原模型的 0.1%。这种方法的优势显著： 首先，它极大降低了计算和存储开销，使得在消费级 GPU 上微调大模型成为可能；其次，它实现了模块化的任务适配，通过加载不同的 LoRA 适配器，同一个基座模型可快速切换为法律、医疗、金融等不同领域的专家；最后，它避免了灾难性遗忘，由于基座模型参数被冻结，其

原有的通用知识能力得以完整保留。在实践中，针对“电力施工安全规程”等专业文档，通过 LoRA 微调，可使模型精准掌握专业术语与规范逻辑，显著减少在该领域的事实性幻觉。

2.2.2 对齐微调：塑造负责任的 AI 价值遵循

仅仅拥有专业知识不足以确保模型的安全可信。大模型可能生成偏见、有害或不符人类伦理的内容。因此，对齐微调的目标是使模型的输出与人类价值观保持一致，通常遵循“有用、诚实、无害”的原则。实现这一目标的核心技术是人类反馈强化学习。

RLHF 通常包含三步：首先，利用高质量的指令数据对模型进行有监督微调，使其初步学会遵循指令；接着，收集人类标注员对模型多个输出结果的偏好排序数据，训练一个“奖励模型”来模拟人类的评判标准；最后，通过强化学习算法，以该奖励模型为引导，优化 SFT 模型的策略，使其输出能获得更高奖励，即更符合人类偏好。通过 RLHF，模型能学会在复杂情境中做出更负责任的价值判断。例如，在面对“农村是否适合发展污染产业”的提问时，未经对齐的模型可能仅从经济效益角度给出肯定分析。而经过充分对齐微调的模型，则能综合权衡经济发展、环境保护、公众健康与社会公平等多重伦理维度，生成一种平衡、负责任、具有建设性的分析，明确指出其潜在环境风险与替代性绿色产业发展路径，从而避免传播片面或有害的观点。

3 “RAG+微调”技术协同

尽管 RAG 与模型微调是两种独立的幻觉治理路径，但其在原理与功能上高度互补，存在天然的协同空间。单一技术均存在固有局限：

RAG 高度依赖检索质量，对模型内在的逻辑与知识能力提升有限；而模型微调（尤其是高效参数微调）虽能内化专业知识，但难以覆盖所有动态更新的外部信息，且训练成本限制了其知识更新的频率。因此，将两种技术协同融合，构建“微调奠基，RAG 增强”的综合框架，成为兼顾模型内生能力与外部知识时效性的最优解。

该协同框架的核心逻辑分为两个层次：首先，通过微调塑造领域专家。利用高质量的专业语料，对基座模型进行 LoRA 等高效微调，使其深入掌握特定领域的核心概念、专业术语、推理范式与价值规范，从根本上降低生成内容的领域无关幻觉与逻辑错误，成为一个具有深度领域认知的“专家大脑”。其次，通过 RAG 提供动态知识外挂。为微调后的专家模型，接入一个实时更新的外部知识库（如政策法规库、前沿论文库、最新漏洞数据库等）。在处理具体查询时，模型优先基于其内化的专家知识进行推理，同时通过 RAG 机制检索并整合外部知识库中的最新、最具体的信息，确保输出的内容兼具深度与时效性。

4 结论与展望

本文基于“构建安全可信的网络生态”系列培训的核心内容，对大模型幻觉问题的治理路径进行了系统性分析与探讨。

研究表明，大模型幻觉主要体现为忠实性幻觉与事实性幻觉，在技术层面的改善，主要通过检索增强生成（RAG）与模型微调（特别是 LoRA 高效微调与对齐微调）构成了互为补充的治理基石。RAG 通过引入外部知识库有效保障信息的准确性与时效性，而模型微调则从参数层面内化专业知识与价值对齐，从根本上提升模型的可靠性与

安全性。二者的协同应用，能够实现“专家能力”与“动态知识”的结合，为构建可信 AI 系统提供了坚实的技术框架。（作者：中国大唐集团科学技术研究总院有限公司　丁朝晖）

注释

1 忠实性幻觉定义参考自 Joshua Maynez 等《On Faithfulness and Factuality in Abstractive Summarization》（2020）。

2 事实性幻觉，亦称为“事实性 hallucination”，是指大语言模型生成的内容与可验证的客观事实或世界知识不一致的现象。其核心在于模型看似流畅、自信地输出了错误或虚构的信息

参考文献

郭全中,张磊,韦薇.AI 幻觉的生成机理与敏捷治理[J/OL].新闻爱好者,1-15[2025-12-08].https://doi.org/10.16017/j.cnki.xwahz.20251205.001.

徐琦,孙智蒲.大模型智能体幻觉难题：成因、风险与应对[J].中国传媒科技,2025,(05):7-14.DOI:10.19483/j.cnki.11-4653/n.2025.05.001

刘泽垣,王鹏江,宋晓斌,等.大语言模型的幻觉问题研究综述[J].软件学报,2025,36(03):1152-1185.DOI:10.13328/j.cnki.jos.007242..

何静,沈阳,谢润锋.大语言模型幻觉现象的分类识别与优化研究[J].计算机科学与探索,2025,19(05):1295-1301

行业前沿观察二：2025 网民网络安全感满意度调查报告发布周（简称“安满周”）在全国线上线下同步开幕；网信部门依法查处网络名人账号违法违规行为；网络数据安全风险评估办法向社会公开征求意见

导读：近期，网信部门指导有关网站平台，依法处置网络名人账号违法违规行为，通报其中典型案例。

12 月 15 日上午，2025 网民网络安全感满意度调查报告发布周（简称“安满周”）在全国线上线下同步开幕，将用为期一周的时间举办 15+场调查报告发布会及系列重磅大会，公布 2025 年度网民满意度指数。

为规范网络数据安全风险评估活动，保障网络数据安全，促进网络数据依法合理有效利用，根据《中华人民共和国数据安全法》《网络数据安全管理条例》等法律法规，国家互联网信息办公室起草了《网络数据安全风险评估办法（征求意见稿）》，向社会公开征求意见。

关键词：人工智能、网络安全、高工专栏、互联网

1.2025 网民网络安全感满意度调查报告发布周（简称“安满周”）在全国线上线下同步开幕

征程万里阔，蓝图再铺展。12 月 15 日上午，2025 网民网络安全感满意度调查报告发布周（简称“安满周”）在全国线上线下同步开幕，将用为期一周的时间举办 15+场调查报告发布会及系列重磅大会，公布 2025 年度网民满意度指数，揭示 2025 年度网民在网络空间治理方面新的关注点、痛点以及期望，展示我国网络安全发展新态势，为有关各方开展网络空间安全治理研究和治理实践提供新一年的网情民意数据参考。

2025“安满周”由网民网络安全感满意度调查活动组委会指导，全国 135 家网络社会组织及相关机构(网安联)发起，全国 228 家网安联志愿服务机构及相关志愿服务团队联合发起，北京网络空间安全协会、北京网络行业协会主办，中国计算机学会计算机安全专业委员会、中国互联网协会网民权益和个人信息保护工作委员会联合主办。主会场设于北京，上海、广州、杭州、郑州等城市设置线下分会场，全国多省市设置线上分会场，线上线下同步直播。

此外，中关村可信计算产业联盟、网安联（北京）国际人才交流中心、香港网络空间安全协会、香港国际人才交流协会、澳门国际科技产业发展协会为本届安满周支持单位，广东新兴国家网络安全和信息化发展研究院、北京关键信息基础设施安全保护中心为承办单位，国源天顺科技产业集团有限公司、广州华南检验检测中心有限公司提供技术支持。

15+份调查报告发布：百万网民心声和诉求集中呈现

“安满周”是一个以发布系列调查报告为主，同时集学术问题深研、行业趋势把脉、专家学者交流、企业融资发展、人才供需服务等的多元化平台，聚焦于“发现问题，指出问题，给出解决方案”，助力提升网民群众获得感、幸福感、安全感和满意度。

2025“安满周”以“网络安全为人民，网络安全靠人民”为主题，将在2025年12月15日-21日期间发布“1+13+3+N”份调查报告，集中展示“2025网民网络安全感满意度调查活动”中采集到的164.5154万份网民意见所揭示的调查结果和各类数据分析成果。

其中，“1”是指《2025年全国网民网络安全感满意度调查统计总报告》，将于12月20日上午在北京发布，届时将公布2025年度网民满意度指数。

“13”是指2025调查活动13个专题调查的调查报告——《网络安全法治社会建设专题报告》《网络诚信建设专题报告》《遏制网络违法犯罪专题报告》《个人信息保护和数据安全专题报告》、《网络购物安全权益保护专题报告》《特殊人群（未成年人和老年人等）网络权益保护专题报告》《互联网平台监管与企业自律报告》《数字政府服务与治理能力提升专题报告》《智能社会发展与治理挑战专题报告》《2025中国网民权益保护调查报告》《行业治理与企业合规专题报告》《行业发展与科技创新报告》《新技术挑战与网络安全专题报告》。

“3”是指《商用密码专题报告》《2025 教育行业网民（学生）网络安全感满意度调查分析报告》《2025 年北京地区学生网民网络安全感满意度调查分析报告》这 3 份行业调查报告。

“N”是指 2025 网民网络安全感满意度调查部分省市区域报告。

系列重磅大会：凝心聚力助力新时代网络强国建设

除发布系列调查报告之外，2025“安满周”期间还将同期举行第五届网络志愿服务大会、京港网络空间安全职业资格互认签约、北京市网络空间安全人才培养评价及国际职业资格互认工作成果发布、教育分会会员代表大会暨教育行业网络安全痛点及解决方案研讨会、2025 安满周·教育行业分论坛、网安联党建联学暨主题党日活动、网安联理事扩大会议、“第二期网络空间安全志愿守护者行动”启动、网安联 20 周年庆系列活动、2025 安满周成果分享会暨闭幕仪式，以及各主题研讨会、座谈会、表彰等系列重磅活动。

活动期间邀请有关党政主管部门领导、中国工程院院士、科研院所专家学者、网安专业技术人员、头部企业精英、社会组织代表、志愿服务团队代表、网民代表以及港澳有关社团、高校、企业代表等汇聚线上线下，共同探讨 2025 网民反映的网络安全问题，探索新时代网络空间安全治理和监管新路径，服务国家网络安全和信息化事业高质量发展。

智库汇聚：行业权威学术合作单位、龙头企业撰写发布报告

调查活动历年全国总报告由承办单位广东新兴国家网络安全和信息化发展研究院撰写编制。此外，为加强政、产、学、研、用等方

面的合作，深挖活动数据价值，进一步为党政有关部门进行网络空间安全治理提供决策参考，提升网络安全行业技术水平，调查活动组委会每年联合相关学术合作单位撰写与发布系列重磅主题报告。

在调查活动组委会授权下，公安部第三研究所网络安全法律研究中心、高速铁路网络管理教育部工程研究中心、乌镇数字文明研究院、互联网实验室等专业权威机构，中国教育技术协会、中国互联网协会网民权益和个人信息保护工作委员会等行业组织，复旦大学、浙江大学、北京交通大学、上海交通大学、海南大学、郑州大学、广州大学等高校，长扬科技(北京)股份有限公司、北京关键信息基础设施安全保护中心、国源天顺科技产业集团有限公司、广州华南检验检测中心有限公司等企业，以及部分网安联成员单位，作为2025“安满周”学术合作单位，撰写、发布2025年度调查活动各大专题调查报告、行业报告、区域报告，为网安领域行业发展赋予新一年的智慧参考。

2025年是国家“十四五”规划收官之年和“十五五”规划谋篇布局之年。在深入贯彻学习党的二十大和二十届二中、三中全会精神，深入贯彻落实“网络强国”“数字中国”重要战略部署和思想指引的热潮中，2025网民网络安全感满意度调查活动于2025年7月至8月在全国范围内面向全社会网民开展了问卷调查，为了解、分析2025年我国网络空间安全现状以及网民对网络治理的评价和诉求等提供了宝贵且丰富的数据。

2.网信部门依法查处网络名人账号违法违规行为

近期，网信部门指导有关网站平台，依法处置网络名人账号违法违规行为。现将其中典型案例通报如下：

一、网络账号“户晨风”在多个平台长期编造所谓“安卓人”“苹果人”等煽动群体对立言论，各平台相关账号已关闭。

二、微博账号“郭美 May 努力努力”、小红书账号“亿颜 LuLu”、快手账号“忘川”、抖音账号“Ayuki_888”、微信视频号“周熙凯 XK”等持续宣扬炫富拜金等不良价值观，相关账号已关闭或长期禁言。

三、微博账号“阑夕”发布宣介境外色情影片内容，抖音主播“张雪峰”在直播中长时间使用污言秽语，相关账号已限期禁言、停播。

四、根据税务部门通报的网络主播偷税案件情况，抖音、快手等平台账号“小影夫妇”“曳步舞鑫鑫”已长期禁言停播、暂停带货营利权限。网络主播“王子柏”相关账号此前因偷逃税款、炫富拜金行为被关闭，近期发现重新注册，网信部门已督促相关平台开展核查处置。

网络名人账号影响力大、社会关注度高，运营者更应自觉依法用网、文明上网，规范网上言行，合理使用流量。各级网信部门持续督促相关网站平台履行主体责任，健全社区规则、用户协议，加强对运营者的教育提醒，依法依约开展账号和信息管理工作，防止已查处的问题反弹复发。

3.网络数据安全风险评估办法向社会公开征求意见

国家互联网信息办公室关于《网络数据安全风险评估办法（征求意见稿）》公开征求意见的通知

为规范网络数据安全风险评估活动，保障网络数据安全，促进网络数据依法合理有效利用，根据《中华人民共和国数据安全法》《网络数据安全管理条例》等法律法规，国家互联网信息办公室起草了《网络数据安全风险评估办法（征求意见稿）》，现向社会公开征求意见。公众可以通过以下途径和方式提出反馈意见：

1.登录中国网信网（www.cac.gov.cn），进入首页“网信要闻”查看文稿。

2.通过电子邮件方式发送至：shujuju@cac.gov.cn。

3.通过信函方式将意见寄至：北京市海淀区阜成路15号国家互联网信息办公室网络数据管理局，邮编100048，并在信封上注明“网络数据安全风险评估办法征求意见”。

意见反馈截止时间为2026年1月5日。

附件：网络数据安全风险评估办法（征求意见稿）

国家互联网信息办公室

2025年12月6日

网络数据安全风险评估办法

（征求意见稿）

第一条 为了规范网络数据安全风险评估活动，保障网络数据安全，促进网络数据依法合理有效利用，根据《中华人民共和国数据安全法》、《中华人民共和国网络安全法》、《网络数据安全管理条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内开展网络数据安全风险评估，应当遵守本办法。法律、行政法规、部门规章另有规定的，依照其规定。

本办法所称网络数据安全风险评估（以下简称风险评估），是指对网络数据和网络数据处理活动安全进行的风险识别、风险分析和风险评价等活动。

第三条 国家网信部门在国家数据安全工作协调机制指导下，统筹各地区、各部门开展风险评估，加强工作协调、信息共享。

第四条 各有关主管部门应当按照“谁管业务、谁管业务数据、谁管数据安全”的原则，定期组织开展本行业、本领域风险评估，可以根据工作需要对本行业、本领域的重要数据处理者开展风险评估情况进行检查，并于每年1月底前向国家网信部门报送年度风险评估及检查计划。

省级网信部门统筹省级有关部门制定本行政区域年度风险评估及检查计划，按照前款要求报送国家网信部门。

第五条 国家网信部门在国家数据安全工作协调机制指导下，统筹有关主管部门和省级网信部门报送的年度风险评估及检查计划，避免重复评估、重复检查。

各有关部门开展检查不得向被检查的网络数据处理者收取费用。

第六条 处理重要数据的网络数据处理者（以下简称重要数据处理者）应当每年度对其网络数据处理活动开展风险评估。重要数据安全状态发生重大变化可能对数据安全造成不利影响的，应及时对发生变化及其影响的部分开展风险评估。

鼓励处理一般数据的网络数据处理者（以下简称一般数据处理者）至少每 3 年开展一次风险评估。

第七条 风险评估工作应当按照《网络数据安全管理条例》有关要求和《数据安全技术 数据安全风险评估方法》（GB/T 45577）等有关国家标准开展。有关主管部门对本行业、本领域风险评估工作另有规定的，从其规定。

第八条 网络数据处理者可以自行或者委托第三方评估机构（以下简称评估机构）开展风险评估。

网络数据处理者自行开展风险评估，应当指定专人负责。网络数据处理者委托评估机构开展风险评估，应当优先选择通过认证的评估机构，并通过订立合同或者其他具有法律效力的文件等方式明确双方的权利、责任和保密义务等。

第九条 经国务院认证认可监督管理部门依法批准的具有数据安全服务认证资质的认证机构，可按照《数据安全技术 数据安全评估机构能力要求》（GB/T 45389）等有关国家标准、行业标准对评估机构开展认证。

第十条 评估机构开展风险评估应当遵守法律法规，公正客观地作出风险判断，并对所出具的风险评估报告真实性、有效性、完整性负责，不得再委托其他机构开展风险评估。

第十一条 同一评估机构及其关联机构不得连续3次以上对同一网络数据处理者开展风险评估。

第十二条 评估机构在风险评估过程中发现网络数据处理活动存在重大数据安全风险的，应当及时通报网络数据处理者，并按照有关规定向省级以上网信部门、有关主管部门报告。

评估机构及其工作人员应当对在风险评估过程中获得的数据、商业秘密、保密商务信息等依法予以保密，不得泄露或者非法向他人提供，在风险评估工作结束后及时删除相关信息。

第十三条 重要数据处理者开展年度风险评估应当按照本办法附件模板编制评估报告，一般数据处理者可以参照本办法附件模板编制评估报告。有关主管部门对风险评估报告模板另有规定的，从其规定。

风险评估报告至少保存3年。

第十四条 重要数据处理者应当在年度风险评估完成后的10个工作日内按照有关主管部门要求报送评估报告。主管部门不明确的，向省级网信部门或者国家网信部门报送。

有关主管部门应当公开评估报告报送渠道和联系方式，及时接收重要数据处理者报送的评估报告，自收到评估报告之日起的10个工作日内将报告通报同级网信部门。国家网信部门汇总相关报告并报送国家数据安全工作协调机制。

省级以上网信部门和有关部门可对网络数据处理者的评估报告真实性、准确性进行抽查核验，网络数据处理者应当配合开展抽查核验。

第十五条 省级以上网信部门和有关部门在风险评估报告核验、监督检查等工作中发现网络数据处理者有以下情形之一的，应当要求其委托通过认证的评估机构开展风险评估：

（一）网络数据处理活动存在较大安全风险的；

（二）发生网络数据安全事件，导致重要数据或者大规模个人信息泄露、被窃取的；

（三）网络数据处理活动可能危害国家安全、公共利益的；

（四）国家网信部门或者有关部门规定的其他情形。

对同一网络数据安全事件或者风险，不得重复要求网络数据处理者委托评估机构开展风险评估。

第十六条 网络数据处理者按照有关部门要求委托评估机构开展风险评估的，应当履行下列义务：

（一）为评估机构开展风险评估工作提供必要支持，包括为风险评估人员提供访问网络数据设施、网络数据、系统及操作日志记录权限等；

（二）在限定时间内完成风险评估，承担评估费用，情况复杂的，报有关部门批准后可以适当延长；

（三）在完成风险评估后将评估机构出具的评估报告报送有关部门，评估报告应当由评估机构主要负责人、风险评估负责人签字并加盖机构公章；

（四）按照有关部门要求对风险评估中发现的问题进行整改，在整改完成后15个工作日内，向有关部门报送整改情况报告。

网络数据处理者不得以任何方式要求或者示意评估机构出具不实或者不当的评估报告。

第十七条 有关部门在组织风险评估工作中发现存在可能危害国家安全、公共利益的网络数据处理活动，应当责令网络数据处理者进行整改；对整改不到位、拒不整改的网络数据处理者，可以采取要求其停止处理重要数据等措施。

第十八条 各地区、各部门应当加强风险信息共享和协同处置，及时处置风险评估工作中发现的安全风险和问题，并按照有关规定及时报告。

省级网信部门统筹协调本行政区域内风险信息共享和协同处置工作，于每年3月底前向国家网信部门报送上一年度风险信息处置情况，国家网信部门汇总相关情况报送国家数据安全工作协调机制。

第十九条 任何组织、个人有权对风险评估中的违法违规活动向有关部门进行投诉、举报，收到投诉、举报的部门应当依法及时处理。

第二十条 省级以上网信部门和有关部门发现网络数据处理者未按规定开展风险评估的，应当依据《中华人民共和国数据安全法》等法律法规予以处置处罚。

发现评估机构违反本办法开展风险评估的，省级以上网信部门和有关部门应当责令其进行整改；情节严重的，可以限制或者禁止其开展风险评估活动，追究相关人员责任，并予公布；构成犯罪的，依法追究刑事责任。

第二十一条 风险评估、网络安全等级保护测评、数据安全管理认证、个人信息保护合规审计、商用密码应用安全性评估等内容重合的，相关结果可以互相采信，避免重复评估、审计、认证。

第二十二条 重要数据处理者提供、委托处理、共同处理重要数据前进行风险评估，可以参照本办法有关规定执行。

第二十三条 核心数据处理者的风险评估，按照国家有关规定执行。

第二十四条 开展涉及国家秘密、工作秘密的风险评估活动，按照《中华人民共和国保守国家秘密法》等法律、行政法规及国家保密规定执行。

第二十五条 本办法自 年 月 日起生效。

行业前沿观察三：各地协会动态

导读：各地协会活动精彩纷呈，举办高级研修班，举行职业技能决赛，举办主题党日、研讨会活动等。北京网络空间安全协会成功举办人社部 2025 人工智能安全保障能力提升高级研修班；2025 年北京市职工数据安全管理员职业技能决赛成功举办；广东省网络空间安全协会科技服务站获评广东省科协服务产业科技创新十佳案例；信创软件供应链安全与风险管理高级研修班在广州成功举办；中关村可信计算产业联盟成功举办 2025 院士大讲堂；海南省网络安全和信息化协会信息安全管理员职业技能竞赛圆满收官；海南省计算机学会组织党员赴海口“二次口岸”考察学习；湖南省网络空间安全协会开展省委网信办网络执法与监督处党支部赴协会支部联基层主题党日活动；上海市信息网络安全管理协会举行“安澜·她界网络安全分会”成立仪式；西藏自治区互联网协会举办党的二十届四中全会精神主题党日活动；湖南省网络空间安全协会成功举办“数据要素流通安全与基础设施建设前沿解读培训”；武汉市网络安全协会成功举办 2025 中国 5G+工业互联网大会工业数据安全防护平行论坛等。

关键词：年会、会长会议、团体标准、网

1.北京网络空间安全协会：人社部2025人工智能安全保障能力提升高级研修班成功举办

依照《人力资源社会保障部办公厅关于印发专业技术人才知识更新工程2025年高级研修班项目计划的通知》的精神，“人工智能安全保障能力提升高级研修班”于2025年11月24-28日在北京网络空间安全协会培训中心（中国锦32层）成功举办。

本次培训由人社部主办、北京市人社局协办、北京网络空间安全协会承办，来自全国各地党政部门、央企/国企、科研机构、高校和民企及社会组织等从事人工智能产品和服务的高级专业技术人才踊跃报名，109名学员按时来到会场学习。

2.2025年北京市职工数据安全管理员职业技能决赛成功举办

2025年11月23日上午，由北京市总工会、北京市人力资源和社会保障局主办，北京网络空间安全协会、北京市总工会职工服务中心、北京市职工技术协会联合承办，人民网北京分公司和北京劳动午报作为媒体支持的“2025年北京市职工职业技能大赛数据安全管理员竞赛暨‘网安联杯’首届数据安全管理员职业技能竞赛”决赛，在北京网络空间安全协会报告厅顺利闭幕。经过初赛、复赛的严格筛选，从全市642名参赛者中脱颖而出的优秀选手齐聚一堂，在决赛中展开了激烈角逐。

3.广东省网络空间安全协会科技服务站获评广东省科协服务产业科技创新十佳案例

12 月 2 日，广东省科学技术协会举办的 2025 年服务产业科技创新站点工作交流活动顺利召开。广东省网络空间安全协会（网安联认证中心）科技服务站凭借在服务产业科技创新中的突出表现、兼具创新性与示范价值的丰硕成果，获得“2025 年广东省科协服务产业科技创新站点十佳案例”荣誉，为网络安全领域科技服务赋能产业发展树立了标杆。

广东省网络空间安全协会（网安联认证中心）科技服务站以机制创新为引擎，以服务实效为导向，已经初步构建起覆盖培训、认证、赛事、调研、科普等多维度的网络安全服务体系，形成了可复制、可推广的“广东模式”。此次获评十佳案例，既是省科协对服务站工作成效的高度认可，更是对网络安全领域科技服务工作的激励与期许。

4.信创软件供应链安全与风险管理高级研修班在广州成功举办

2025 年 11 月 11 日至 11 月 15 日，由广东省人力资源和社会保障厅主办、广东省网络空间安全协会承办的“信创软件供应链安全与风险管理高级研修班”在广州成功举办。本次高研班围绕信创产业发展核心，旨在为我省培养一批高素质、专业化的软件供应链安全技术和管理骨干，共同筑牢数字经济发展的安全底座。

本次高研班课程设置科学合理，内容丰富实用。在为期三天的集中培训中，围绕“信创软件供应链安全”这一主题，设置了八大核心模块，包括软件供应链安全前沿动态及趋势、风险管理体系构建、基础软件供应链安全挑战与国产化路径、软件组件安全评估与选型策略等关键内容。

5.中关村可信计算产业联盟成功举办 2025 院士大讲堂

11 月 10 日，中关村可信计算产业联盟主办的 2025 可信计算院士大讲堂在北京警察学院成功举行。北京警察学院师生和可信联盟成员单位代表约二百人在现场参加会议，线上直播在教育部网络安全与执法专业虚拟教研室平台、北京工业大学、北京交通大学设立分会场。

中国工程院沈昌祥院士莅临现场，以《构建安全可信智能网络新生态，促进数字经济高质量发展》为题做主旨报告。

6.海南省网络安全和信息化协会信息安全管理员职业技能竞赛圆满收官

应 12 月 6 日，由海南省人力资源开发局、海南省网络安全和信息化协会联合主办的 2025 年海南省行业职业技能竞赛（信息安全管理员）职业技能竞赛在海口顺利完成全部赛程，圆满落幕。

此次竞赛面向全省公开征集选手，共吸引约 20 支队伍、60 多名选手参赛，覆盖党政机关、重点企业、科研机构及通信运维等多个关键领域。竞赛秉持“公平、公正、实战” 原则，设置理论考核与

实操攻坚双重赛制，紧密结合自贸港建设中的政务服务、数据安全、关键信息基础设施防护等实际场景，全面检验选手的专业知识储备与实战应对能力。

7.海南省计算机学会组织党员赴海口“二次口岸”考察学习

近日，海南省计算机学会组织十多名党员和积极分子前往海口新海港和南港“二次口岸”货运集中查验场，开展“党建引领促发展，实地调研强担当”主题活动。活动通过实地考察货物通关流程、专题学习党的二十届四中全会精神，实现理论学习与业务实践深度融合，为学会党员服务海南自贸港建设注入新动力。

8.湖南省网络空间安全协会开展省委网信办网络执法与监督处党支部赴协会支部联基层主题党日活动

近日，湖南省委网信办网络执法与监督处党支部书记、处长严颂一行赴湖南省网络空间安全协会，开展了以“党建引领聚合力 数智安全谱新篇”为主题的基层主题党日活动，推动了党建与协会业务的深度融合。

在新法响应与交流研讨环节，双方围绕党支部建设、党管互联网、新修正的《网络安全法》贯彻落实等内容进行交流研讨。未来，协会将持续强化党建引领核心作用，凝聚共识，增进交流，有力促进党建与业务工作双提升。

9.上海市信息网络安全管理协会举行“安澜·她界网络安全分会”成立仪式

应上海市普陀区妇女联合会邀请，上海市信息网络安全管理协会牵头组建的“安澜·她界网络安全分会”，将作为上海市普陀区女性人才促进会的第九个分会。

为推进分会筹备工作，并明确班子成员，近期，分会筹备会在协会普陀办公点——长风网络安全产业园启幕。20 余位来自会员单位的女性从业者齐聚于此，共同描绘分会职能与发展的新蓝图。此外，12 月 16 日将举办分会成立仪式，开启全新篇章。

10.西藏自治区互联网协会举办党的二十届四中全会精神主题党日活动

为深入学习宣传贯彻党的二十届四中全会精神，以党建引领西藏互联网行业高质量发展，近日，在区互联网行业党委的精心指导下，西藏自治区互联网协会与西藏自治区通信行业协会联合党支部成功举办“党建领航·网众 e 心”—深入学习宣传贯彻党的二十届四中全会精神主题党日活动。

活动创新采用“理论学习+沉浸式体验”模式，区互联网行业党委相关领导、所属支部党员同志及行业代表共计 30 余人齐聚一堂，在学思践悟中筑牢思想根基，在红色浸润中凝聚奋进力量。

11.湖南省网络空间安全协会成功举办“数据要素流通安全与基础设施建设前沿解读培训”

近日，由湖南省网络空间安全协会协办的“数据要素流通安全与基础设施建设前沿解读培训”在国家网络安全产业园区（长沙）成功举办。

此次培训以“理论赋能+实地感知”为特色精心设计为参训学员带来全方位、深层次的专业分享。活动伊始，参训人员在工作人员引导下参观了国家网络安全产业园展示厅，近距离接触网络安全前沿技术与应用成果，实时了解长沙市网络安全运营核心数据，直观感受数据安全防护体系的构建逻辑。

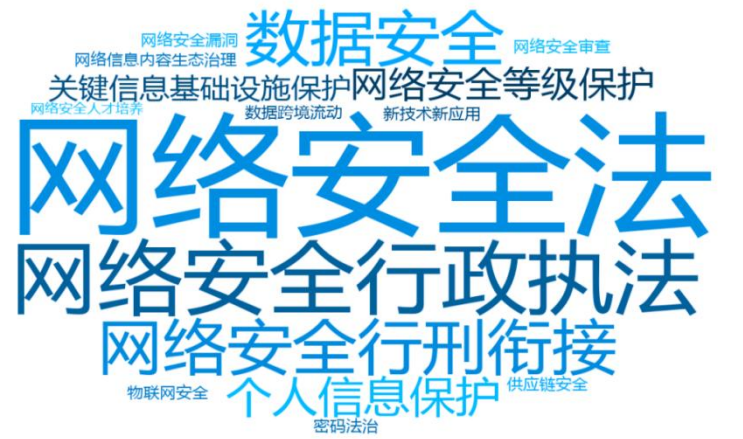
12.武汉市网络安全协会成功举办 2025 中国 5G+工业互联网大会工业数据安全防护平行论坛

11 月 23 日，由武汉市网络安全协会承办的中国 5G+工业互联网大会工业数据安全防护平行论坛在武汉光谷科技会展中心成功举办。该论坛以“筑盾工业数安护航”为核心指引，聚焦工业数据安全风险防控、重要数据分级分类、技术实践与生态协同三大关键议题，搭建起“政策解读-技术创新-产业落地”三位一体的高端交流平台，为推进制造强国、网络强国、数字中国战略落地筑牢安全支撑。汇聚了来自政府部门、高校科研院所、工业制造及网络安全领域的近两百位嘉宾，共话工业数据安全治理新路径。

公安部第三研究所网络安全法律研究中心

2016年2月，公安部第三研究所正式成立“网络安全法律研究中心”。 中心成立以来，聚焦前瞻性研究，切实践行理论研究与立法实践深度结合，跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用发展及安全风险，并持续推动科研成果应用于网络安全相关立法活动，在国内网络安全法律方面的影响力逐步提升。同时投身警务实践活动和公安一线服务，为公安部门提供立法动态研判和决策研究支撑。

基础性	专业性	针对性



推动立法、服务实务、智库支撑

联系方式

电子邮箱：cslaw@gass.ac.cn　　咨询电话：王老师 18817309169

网络与数据安全法律合规咨询服务

提供《网络安全法》《数据安全法》《密码法》《个人信息保护法》及配套制度为核心的数据安全保护合规体系建设，包括但不限于帮助企业落实网络安全等级保护、关键信息基础设施安全保护、网络安全审查、数据出境安全风险评估、数据交易安全保障、安全事件应急处置等要求。
开展个人信息、重要数据、核心数据等数据安全合规自查、合规差距性分析，发现、识别、分析、研判、控制数据收集、存储、使用、加工、传输、提供、公开等全生命周期的法律风险，提供法律意见和整改建议。

数据安全合规体系构建

为企业提供网络安全漏洞发现与披露、漏洞扫描与渗透测试等安全测试、“白帽子”与众测等业务场景下的合规体系构建，帮助企业厘清行为边界，避免经营风险。

安全测试法律合规体系构建

开展情况调研，评估拟出境活动风险，发现安全风险并提供整改建议，根据客户整改落实情况，出具数据出境安全风险评估报告。

数据出境安全风险评估咨询服务

帮助企业构建事先防范网络安全、数据安全行政与刑事风险框架，指导企业如何正确配合监督检查、理解执法要求等。

网络安全、数据安全执法调查与刑事风险的防范与处置意见

针对《个人信息保护法》第五十五条规定的个人信息处理情形，帮助企业开展个人信息保护影响评估，履行个人信息保护义务。

个人信息保护影响评估/合规审计咨询服务

结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

网络安全、数据安全法律法规专业培训

数据出境安全风险评估咨询服务

近年来，我国在国家数据安全和个人信息保护的顶层设计布局下，加快数据出境相关立法，数据出境规则体系不断完善，数据出境安全评估成为数据出境的重要路径。2022年7月7日，国家互联网信息办公室发布《数据出境安全评估办法》，落实《网络安全法》《数据安全法》《个人信息保护法》上位法要求，明确数据出境安全评估相关规定。在此形势下，企业普遍面临出境数据识别难、出境风险评估难、申报材料填报难等难题。为帮助企业解决以上难题，及时履行数据出境安全评估申报义务，公安部第三研究所网络安全法律研究中心特推出**数据出境安全风险评估咨询服务。**

数据出境活动

1 境内运营中收集和产生的数据传输、存储至境外

2 数据存储在境内，境外的机构、组织或者个人可以访问或者调用

数据出境安全风险评估咨询服务流程

01 情况调研 — 1 - 3 周

- 开展合规差距分析
- 识别安全风险并划定风险等级
- 针对安全风险提供整改建议

02 风险评估 — 3 - 5 周

03 指导落实整改 — 周期视情况而定

04 出具风险评估报告 — 1 - 2 周

- 结合客户落实整改情况，出具《数据出境风险评估报告》

合规咨询服务项目

中心已为互联网、银行、服装、签证、传统制造业等分属不同行业类别的企业提供APP合规咨询、个人信息保护（隐私政策）评估、个人信息保护合规整改、数据出境安全风险自评估等方面的合规咨询服务，合规咨询服务能力得到客户一致认可。

典型项目

- 某互联网公司APP合规咨询
- 某银行个人信息保护（隐私政策）评估
- 某跨国服装零售企业个人信息保护合规整改
- 某签证跨国集团数据出境安全风险评估咨询
- 某传统制造业跨国集团数据出境安全风险评估咨询

……