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6月第6期（总第23期）

2025年6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：5 月，网络安全、数据安全与发展、个人信息保护、公共安全视频图像仍是国家和地方政策立法重点关注内容，且规定更为细化，配套规章和标准密集发布。

国务院办公厅印发《国务院 2025 年度立法工作计划》，明确提出预备修订互联网信息服务管理办法，推进人工智能健康发展立法工作；预备制定网络安全等级保护条例。国务院总理李强签署国务院令公布《政务数据共享条例》，明确管理体制、目录管理、共享使用、平台支撑等内容。国务院、中央军委公布《重要军工设施保护条例》，明确重要军工设施范围、各方责任和保护措施，规范重要军工设施保护区划定。

中国人民银行相继发布《中国人民银行业务领域数据安全管理办法》《中国人民银行业务领域网络安全事件报告管理办法》，强化银行业务领域的网络和数据安全管理要求。公安部印发《公共安全视频图像信息系统监督管理工作规定》，提出公共安全视频系统管理单位可以通过线上或者线下方式办理备案。

标准层面，GB/T 45574-2025《数据安全技术 敏感个人信息处理安全要求》公布，规定敏感个人信息处理通用安全要求和特殊安全要求。全国网络安全标准化技术委员会秘书处发布个人信息保护合规审计方面的两个标准，对合规审计和专业机构服务能力要求进行规定。

关键词：政务数据共享；公共安全视频图像；个人信息保护

（一）国家层面动向

1. 全国人大常委会发布2025年度立法工作计划

5月14日，全国人大常委会发布2025年度立法工作计划，提出《治安管理处罚法（修改）》等14件继续审议的法律案，《网络安全法（修改）》等23件初次审议的法律案。（来源：全国人大）

2. 国务院办公厅印发《国务院2025年度立法工作计划》

5月4日，国务院办公厅印发《国务院2025年度立法工作计划》。

根据《计划》，国务院在推动高质量发展、构建高水平社会主义市场经济体制方面，预备提请全国人大常委会审议电信法草案。

在加强政府自身建设、深入推进依法行政方面，制定政务数据共享条例，修订行政复议法实施条例、行政法规制定程序条例。预备提请全国人大常委会审议人民警察法修订草案。预备制定行政执法监督条例、行政规范性文件制定和管理监督条例，预备修订政府信息公开条例、规章制定程序条例。

在实施科教兴国战略、建设社会主义文化强国方面，预备修订互联网信息服务管理办法，推进人工智能健康发展立法工作。

在健全国家安全法治体系、建设更高水平平安中国方面，提请全国人大常委会审议监狱法修订草案。预备制定网络安全等级保护条例、终端设

备直连卫星服务管理条例、卫星导航条例，预备修订反间谍法实施细则、企业事业单位内部治安保卫条例。（来源：国务院）

3. 国务院公布《政务数据共享条例》

5 月 28 日，国务院总理李强签署国务院令，公布《政务数据共享条例》，自 2025 年 8 月 1 日起施行。《条例》共八章四十四条，包括管理体制、目录管理、共享使用、平台支撑等内容。

目录管理方面，《条例》规定政务数据实行统一目录管理，明确政务数据目录编制、发布以及动态更新等要求。确定政务数据共享属性的分类，禁止擅自增设条件阻碍、影响政务数据共享。

共享使用方面，《条例》规定通过共享获取政务数据能够满足履职需要的，政府部门不得重复收集，明确牵头收集政务数据的政府部门的职责。细化政务数据共享申请、答复的流程及时限要求。明确政务数据质量管理、校核纠错及共享争议解决处理机制。规定上级政府部门应当根据下级政府部门的履职需要，在确保政务数据安全的前提下，及时、完整回流相关政务数据。

平台支撑方面，《条例》规定整合构建全国一体化政务大数据体系，要求已建设的政务数据平台纳入全国一体化政务大数据体系，原则上不新建政务数据共享交换系统。明确各级政府部门应当通过全国一体化政务大数据体系开展政务数据共享工作。（来源：中国政府网）

4. 国务院、中央军委公布实施《重要军工设施保护条例》

5月19日，国务院、中央军委公布《重要军工设施保护条例》，自2025年9月15日起施行。《条例》共七章五十一条，主要规定五方面内容。

一是明确重要军工设施范围和各方责任。规定依法保护的重要军工设施范围，明确国务院有关部门、地方人民政府、有关军事机关及重要军工设施管理单位等的职责。

二是规范重要军工设施保护区划定。明确重要军工设施通过划定重要军工设施保护区实施保护，规定重要军工设施保护区范围划定、调整的程序及要求。

三是明确重要军工设施的保护措施。规定重要军工设施保护区应当采取管控进入等安全防护措施，明确重要军工设施保护区外围安全控制范围的有关保护要求，并对利用重要军工设施开展重大科研试验活动等特殊情形的保护作出规定。

四是强化重要军工设施管理单位责任义务。明确建立健全保护责任制、实施全过程安全管理、制定应急预案、开展安全保护风险评估等职责，并明确内部治安保卫等方面的要求。

五是加强各方面保障监督。明确编制国民经济和社会发展规划等应统筹重要军工设施保护需要，强化行业主管部门和地方人民政府的监督检查、综合治理责任。（来源：国务院）

（二）部委层面动向

1. 国家发展改革委等三部门印发《关于全面推行以专项信用报告替代有无违法违规记录证明的通知》

4 月 29 日，国家发展改革委、公安部、国家数据局印发《关于全面推行以专项信用报告替代有无违法违规记录证明的通知》，全面推行“信用代证”工作。《通知》提出六个方面要求，包括夯实专项信用报告数据基础、明确适用对象和应用范围、畅通专项信用报告查询渠道等。

夯实专项信用报告数据基础方面，《通知》提出，各省（区、市）专项信用报告应至少涵盖行政处罚（含简易程序作出的行政处罚）、行政强制、严重失信主体名单和刑事裁判（犯罪记录）等信息。对地方政府产生的相关信用信息，各省级社会信用体系建设牵头部门要会同数据管理部门，按照国家有关数据共享标准，加强相关信用信息的归集共享；对中央国家机关产生的相关信用信息，通过全国信用信息共享平台推送给省级信用牵头部门。按照“谁产生、谁负责”原则，强化数据质量管理，建立数据异议反馈、核查修正机制，持续提高数据的全面性、真实性、准确性。对于已修复的信用信息，专项信用报告应予以展示，并标注“已修复”。

建立专项信用报告跨省互认机制方面，《通知》指出，“信用中国”网站要与省级信用平台网站建立信用信息互联互通机制，按照相关数据共享标准向各地区共享非本地区的信用主体基本信息，为实现专项信用报告跨省互认提供支撑。需要信用主体提供其他地区有无违法违规记录证明的，各地要明确认可相关地区出具的专项信用报告，不能再要求信用主体重复

提供相关证明。对于其他地区信用主体需要办理本地区有无违法违规记录证明的，省级信用牵头部门要积极为其查询、下载专项信用报告提供便利。完善信息异议处理机制方面，《通知》强调，省级信用牵头部门要建立专项信用报告异议申诉机制，除法律法规另有规定外，信用主体认为专项信用报告中的信用信息内容有误或者对信用修复结果存在异议的，可以通过省级信用平台网站提出异议申诉。省级信用牵头部门收到异议申诉申请后应及时推送给数源单位，督促数源单位及时核实相关情况，并将申诉处理结果及时反馈给申请人。（来源：国家发改委）

2. 中国人民银行发布《中国人民银行业务领域数据安全管理办法》

5 月 1 日，中国人民银行发布《中国人民银行业务领域数据安全管理办法》，自 2025 年 6 月 30 日起施行。《办法》共七章五十六条，包括业务数据分类分级与总体要求、全流程业务数据安全管理要求、全流程业务数据安全技术要求等内容。

《办法》规定，数据处理者应当建立业务数据资源目录，并从业务关联性、敏感性和可用性方面分别做好业务数据分类。具体而言，一是标识各数据项是否为个人信息、是否为外部收集产生、存储该数据项的信息系统清单和关联的业务类别；二是根据业务数据遭到泄露或者被非法获取、非法利用时，对个人、组织合法权益或者公共利益等造成的危害程度开展敏感性分类。三是根据业务数据遭到篡改、破坏后对业务正常运行造成的影响程度，明确信息系统差异化的数据恢复点目标，视为对业务数据的可用性分类。

《办法》强调，数据处理者收集业务数据应当采取安全保护管理措施。具体而言，一是除收集自行公开或者其他已经合法公开的业务数据的情形外，收集业务数据时应当依照法律、行政法规和中国人民银行相关规定取得个人同意或者组织授权，并落实相应告知义务；二是非直接面向个人、组织收集其尚未公开的业务数据的，应当在合同或者协议中明确数据提供方保障业务数据来源合法性、真实性的义务。三是采用人工录入方式收集业务数据的，应当采取必要校验措施保障业务数据录入的准确性，按照相关管理要求留存业务数据收集原始凭证；四是原则上不收集图像等原始个人生物识别信息；五是按照与数据提供方合同或者协议中约定的处理目的、方式、范围以及安全保护义务等开展收集和后续的业务数据处理活动。（来源：中国人民银行条法司）

3. 公安部等六部门联合公布《国家网络身份认证公共服务管理办法》

5 月 19 日，公安部、国家互联网信息办公室、民政部、文化和旅游部、国家卫生健康委员会、国家广播电视总局等六部门近日联合公布《国家网络身份认证公共服务管理办法》，自 2025 年 7 月 15 日起施行。

《办法》共十六条，主要规定了四个方面内容：一是明确了国家网络身份认证公共服务及网号、网证的概念、申领方式；二是明确了使用国家网络身份认证公共服务的效力、应用场景；三是强调了国家网络身份认证公共服务平台、互联网平台等对数据安全和个人信息保护的责任；四是对未成年人申领、使用国家网络身份认证公共服务作出特殊规定。

《办法》明确网号、网证的自愿使用原则，鼓励有关主管部门、重点行业、互联网平台按照用户自愿原则推广应用网号、网证，但同时保留、提供现有的或者其他合法方式进行登记、核验身份。鼓励互联网平台接入国家网络身份认证公共服务，但应当保障未使用网号、网证的用户与使用网号、网证的用户享有同等服务。

《办法》严格依照《个人信息保护法》等规定，充分保护公民个人信息权益。在信息收集方面，对用户选择使用网号、网证登记、核验真实身份的，除法律、行政法规另有规定或者用户同意外，互联网平台不得要求用户另行提供明文身份信息。国家网络身份认证公共服务平台所收集的信息仅限网络身份认证所必要的信息，不收集其他信息，不会影响用户正常使用互联网应用。

国家网络身份认证公共服务平台坚持“最小化提供”原则，对依法需要核验用户真实身份但无需留存法定身份证件信息的，仅向互联网平台提供核验结果；对依法确需获取、留存用户法定身份证件信息的，经用户单独同意，国家网络身份认证公共服务平台可以向互联网平台提供必要的明文身份信息。对法律、行政法规规定应当履行协助义务的，国家网络身份认证公共服务平台应当依法提供相关信息，但提供的信息仅限网号、网证对应的真实身份信息和认证日志信息。（来源：公安部）

4. 公安部印发《公共安全视频图像信息系统监督管理工作规定》

5 月 21 日，公安部印发《公共安全视频图像信息系统监督管理工作规定》，共二十二条，自印发之日起施行。

《规定》提出，公共安全视频系统管理单位可以通过线上或者线下方式办理备案。申请人通过线上方式备案的，县级公安机关应当在申请提交之日起5个工作日内，对备案信息齐全的，予以备案；对备案信息不齐全的，一次性告知申请人需要补正的信息。申请人通过线下方式备案的，县级公安机关应当在政务服务大厅公安窗口或者公安机关办事窗口接收备案申请材料。备案材料齐全的，由窗口工作人员录入公共安全视频图像信息系统备案平台，予以备案；备案材料不齐全的，应当当场一次性告知申请人需要补正的材料。

《规定》要求，公共安全视频系统管理单位办理备案时，应当提供经办人身份证件和加盖单位公章的委托办理备案授权书，并如实填写以下备案信息或者提交备案材料：一是公共安全视频系统管理单位基本信息，包括单位名称、类型、统一社会信用代码等；二是公共安全视频系统基本信息，包括系统建设位置（含图像采集设备相关信息）、数量及功能类型、视频图像信息存储期限等。（来源：公安部）

5. 中央网信办等三部门印发《2025年深入推进IPv6规模部署和应用工作要点》

5月20日消息，中央网信办、国家发展改革委、工业和信息化部近日联合印发《2025年深入推进IPv6规模部署和应用工作要点》。

《工作要点》明确了2025年工作目标：到2025年末，全面建成全球领先的IPv6技术、产业、设施、应用和安全体系。IPv6活跃用户数达到8.5

亿，物联网 IPv6 连接数达到 11 亿，固定网络 IPv6 流量占比达到 27%，移动网络 IPv6 流量占比达到 70%。

《工作要点》部署了九个方面四十二项重点任务。

一是增强内生发展动力。包括加大政策支持力度、发挥市场机制作用、释放 IPv6 技术优势、加强 IPv6 地址资源申请和规划。

二是强化网络服务保障。包括加大 IPv6 网络优化力度、提升 IPv6 业务服务水平、增强 IPv6 互联互通水平、加快广电网络 IPv6 应用。

三是加大应用基础设施供给。包括提高云服务产品 IPv6 易用性、优化内容分发网络 IPv6 服务质量、扩大数据中心 IPv6 支持范围、推动 IPv6 与人工智能融合发展。

四是深化单栈规模部署。包括提升 IPv6 单栈贯通能力、拓展 IPv6 单栈部署应用。

五是提高终端设备连通水平。包括加强终端设备 IPv6 检测、加快存量终端升级替换、扩大家庭智能终端 IPv6 支持范围、推广物联网 IPv6 应用。

六是深化融合应用。包括加大商业应用 IPv6 放量引流力度、深化政务应用 IPv6 演进升级、持续深化中央企业 IPv6 改造、拓展金融机构 IPv6 创新应用实践、深化农业农村部系统 IPv6 部署应用、提升教育系统 IPv6 网络性能和接入能力、推进人社部门 IPv6 升级改造、深化民政政务信息系统 IPv6 升级改造、加强卫生健康领域 IPv6 升级改造、推进交通数字化设施 IPv6 应用、拓展工业互联网 IPv6 应用、深化水利行业 IPv6 建设应用、加快自然资源和生态环境系统 IPv6 升级改造、推动应急管理业务系统全面接入 IPv6。

七是促进创新生态和标准体系建设。包括强化“IPv6+”创新产业生态建设、加强互联网体系结构创新研究和试点应用、持续推进 IPv6 国家标准制定与实施、提升 IPv6 国际标准影响力。

八是强化试点示范和宣传推广。包括深化实施重点城市 IPv6 专项行动、创新宣传形式和内容、丰富行业交流活动。

九是强化网络安全保障。包括加强 IPv6 网络安全防护和管理监督、提升 IPv6 安全风险研判及技术实践能力、推动 IPv6 安全产品研发应用。（来源：网信中国）

6. 中国人民银行发布《中国人民银行业务领域网络安全事件报告管理办法》

5 月 23 日，中国人民银行发布《中国人民银行业务领域网络安全事件报告管理办法》，自 2025 年 8 月 1 日起施行。《办法》共五章三十三条，包括网络安全事件分级、网络安全事件报告等内容。

网络安全事件分级方面，《办法》提出，金融从业机构应当在本机构网络安全管理制度或者操作规程中明确网络安全事件分级标准，将网络安全事件分为特别重大、重大、较大和一般四个等级。网络安全事件同时符合多个分级标准的，应当按照最高级别确定网络安全事件等级；事态发展情况已达到更高级别分级标准时，金融从业机构应当立即调整网络安全事件等级。因灾害或者信息基础设施故障，导致金融从业机构多个中国人民银行业务领域网络同时发生网络安全事件时，应当先分别确定网络安全事

件等级，再按照各网络安全事件等级中的最高级别，确定整体的网络安全事件等级。

网络安全事件报告方面，《办法》规定，金融从业机构发生较大等级以上网络安全事件后，应当于1小时内报送网络安全事件事发简要报告，并在24小时内报送网络安全事件事发报告。对于重大等级以上网络安全事件，金融从业机构应当至少每隔2小时进行事中进展报告，直至处置结束。处置过程中如出现调高网络安全事件等级、处置取得阶段性进展、发现新的问题等重要情况时，应当立即报告。网络安全事件处置结束后，金融从业机构应当于10个工作日内报送事后调查总结报告。无法按时报送事后调查总结报告的，金融从业机构应当先按时报送初步报告，说明承诺报送事后调查总结报告的日期并按时报送。承诺日期原则上应当在处置结束之日起40个工作日内。（来源：中国人民银行条法司）

7. 国家密码管理局发布《电子印章管理办法》（征求意见稿）

5月21日，国家密码管理局发布《电子印章管理办法》（征求意见稿）。征求意见稿共八章三十八条，包括管理和服务主体、使用管理、互信互认等内容。

征求意见稿指出，电子印章是指基于密码技术和相关数字技术表征印章的特定格式数据，用于实现电子文件的可靠电子签名，包含印章图像数据、印章名称、印章所有者信息、电子签名认证证书以及电子签名制作数据等。

电子印章使用管理方面，征求意见稿规定，电子签章应当使用有效的电子印章，遵照国家有关法律法规和标准规范，保证电子签章数据的真实性、完整性和不可否认性。电子签章过程信息应当被记录并保存，实现电子签章行为可追溯、可定责。

电子印章互认互信方面，征求意见稿提出，行政机关以及履行社会管理和公共服务职能的企业事业单位、社会组织在业务活动中需要使用电子印章时，其业务信息系统应当支持符合本办法的电子印章的接入使用，法律、行政法规另有规定的除外。经电子签章的电子文件应当实现跨层级跨地域跨系统跨部门跨业务互通互认。（来源：国家密码管理局）

8. 国家网信办发布《网信部门行政处罚裁量权基准适用规定（征求意见稿）》

5 月 30 日，国家网信办发布《网信部门行政处罚裁量权基准适用规定（征求意见稿）》，共二十条。

征求意见稿指出，规定所称行政处罚裁量权基准，是指网信部门在实施行政处罚时，按照裁量涉及的违法行为的事实、性质、情节、社会危害程度、当事人主观过错等因素，对法律、法规、规章中的原则性规定或者具有一定弹性的执法权限、裁量幅度等内容进行细化量化而形成的具体执法尺度和标准。

征求意见稿提出，网信部门行政处罚裁量权基准划分为不予处罚、减轻处罚、从轻处罚、一般处罚、从重处罚等裁量阶次。其中，一般处罚是

指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用适中的种类或者幅度，对当事人实施行政处罚。

征求意见稿规定，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、情节和本地区经济社会发展状况等因素，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。（来源：网信中国）

9. 国家互联网信息办公室就《个人信息保护合规审计管理办法》实施有关事项答记者问

5月27日，国家互联网信息办公室就《个人信息保护合规审计管理办法》实施有关事项答记者问。

关于个人信息保护合规审计参考操作指南问题，国家网信办指出，根据《个人信息保护合规审计管理办法》及附件《个人信息保护合规审计指引》，全国网络安全标准化技术委员会秘书处组织编制发布了《网络安全标准实践指南——个人信息保护合规审计要求》，对个人信息保护合规审计的实施流程、合规审计内容和方法、合规审计证据、底稿模板、报告模板等作出规范，个人信息处理者、专业机构可以参照该实践指南开展个人信息保护合规审计。

关于个人信息保护合规审计专业机构申请认证问题，国家网信办指出，根据《个人信息保护合规审计管理办法》第七条规定，专业机构的认证按照《认证认可条例》的有关规定执行。国家网信办数据与技术保障中心、中国网络安全审查认证和市场监管大数据中心、北京赛西认证有限责任公司3家单位，已向国家认证认可监督管理委员会备案相关认证规则，将依据认证规则和《网络安全标准实践指南——个人信息保护合规审计 专业机构服务能力要求》《网络安全标准实践指南——个人信息保护合规审计要求》实施认证。专业机构可向上述3家认证机构申请认证。

关于个人信息保护合规审计人员应当具备哪些能力问题，国家网信办指出，《网络安全标准实践指南——个人信息保护合规审计 专业机构服务能力要求》《网络安全标准实践指南——个人信息保护合规审计要求》将个人信息保护合规审计人员分为初级、中级、高级三个等级，明确了不同等级合规审计人员在法律法规、专业知识、专业能力、项目管理、报告撰写审核等方面的能力要求，可查询实践指南了解能力要求具体内容。

关于个人信息保护合规审计人员能力评价问题，国家网信办指出，中国网络空间安全协会根据《网络安全标准实践指南——个人信息保护合规审计 专业机构服务能力要求》《网络安全标准实践指南——个人信息保护合规审计要求》关于个人信息保护合规审计人员能力要求，编制了《个人信息保护合规审计人员能力评价要点》，明确不同等级个人信息保护合规审计人员的能力评价目标、方式、要点等，将开展个人信息保护合规审计人员能力评价，相关信息可在中国网络空间安全协会官网查询。（来源：网信中国）

10. 国家网信办发布数据出境安全管理政策问答（2025 年 5 月）

5 月 30 日，国家互联网信息办公室对近期收到的数据出境咨询问题进行研究，将有代表性的问题和答复公布。

关于识别申报重要数据的具体流程方面，国家网信办指出，《数据安全法》第二十一条规定，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，对列入目录的数据进行重点保护。《网络数据安全管理条例》第二十九条规定，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。

落实相关法律法规规定，各部门正在制定相关行业、领域的数据分类分级标准规范和重要数据识别申报规则，为本行业、领域的数据处理者识别申报重要数据提供具体依据和操作指导。部分行业、领域数据分类分级标准规范和重要数据识别申报规则已经公开发布，如工业领域的《工业领域重要数据识别指南》、电信领域的《电信领域重要数据识别指南》、自然资源领域的《地理信息数据分类分级工作指南（试行）》、统计领域的《统计数据安全管理办法》等，还有的通过召开会议、制发文件、一对一通知等形式告知到数据处理者。数据处理者应当按照相关标准规范、申报规则和有关主管部门的要求，及时做好重要数据识别、申报工作。相关行业主管部门对数据处理者申报重要数据进行认定，对确认为重要数据的，

将及时向数据处理者告知或者公开发布。如果数据处理者被告知掌握重要数据或者掌握的数据被公开发布为重要数据，应当按照相关法律法规的要求，履行重要数据安全保护责任。没有发布行业、领域的数据分类分级标准规范和重要数据识别申报规则，数据处理者也没有被有关部门告知应当进行重要数据识别申报的，未识别申报重要数据，未对相关数据进行重点保护，不会被认定为违反重要数据保护相关规定，不会因此受到行政处罚。

关于如何合规开展重要数据出境活动方面，国家网信办指出，根据《网络安全法》第三十七条、《数据安全法》第三十一条、《网络数据安全管理条例》第三十七条以及《数据出境安全评估办法》《促进和规范数据跨境流动规定》相关条款规定，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。申报数据出境安全评估的流程参考国家互联网信息办公室公开发布的《数据出境安全评估申报指南》。对于确需出境的重要数据，经数据出境安全评估认为不会危害国家安全和社会公共利益的，可以出境。

数据处理者应当按照相关规定识别、申报重要数据，未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估，相关数据出境活动不会被认定为违法违规出境重要数据，不会因此受到行政处罚。数据处理者被告知掌握重要数据或者掌握的数据被公开发布为重要数据后，如需继续开展相关数据出境活动的，应当在被告知或者公开发布后 2 个月内，通过所在地省级网信部门向国家网信部门申报数据出境安全评估。数据处理者应当按照国家网信部门出具的

安全评估结果合规开展数据出境活动，切实保障重要数据出境安全。（来源：网信中国）

11. 国家市场监督管理总局、国家标准化管理委员会公布国家推荐标准《数据安全技术 敏感个人信息处理安全要求》

5 月 23 日，国家市场监督管理总局、国家标准化管理委员会公布国家推荐标准 GB/T 45574-2025《数据安全技术 敏感个人信息处理安全要求》。

该标准确立了敏感个人信息识别和界定，规定了敏感个人信息处理通用安全要求和敏感个人信息处理特殊安全要求，适用于个人信息处理者开展敏感个人信息处理活动，也适用于监管部门和第三方评估机构对敏感个人信息处理活动进行监督、管理和评估。

标准在敏感个人信息处理通用安全方面，围绕基本要求、收集合法性、收集要求、告知同意、安全保护五个方面提出具体要求。例如，标准提出个人信息处理者在收集敏感个人信息前应符合以下要求：一是收集非敏感个人信息可实现处理目的的，不应收集敏感个人信息；二是应仅在个人信息主体使用业务功能期间，收集该业务功能所需的敏感个人信息；三是应按业务功能或服务场景，分项收集敏感个人信息；四是利用移动互联网应用程序收集应符合 GB/T 41391-2022《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》的要求。

标准在敏感个人信息处理特殊安全方面，提出生物识别信息、宗教信仰信息、特定身份信息、医疗健康信息、金融账户信息、行踪轨迹信息、不满十四周岁未成年人的个人信息等七类敏感个人信息处理的特殊要求。

例如，标准提出个人信息处理者处理生物识别信息，在符合敏感个人信息处理通用安全要求和 GB/T 40660-2021《信息安全技术 生物特征识别信息保护基本要求》要求的基础上，还需符合：一是基于生物识别信息进行身份识别时，应同时提供不基于生物识别信息的其他替代可选身份识别方式，并不应将基于生物识别信息的方式作为默认选项；二是除非个人信息主体主动要求或书面同意，不应公开生物识别信息；三是通过无需个人信息主体配合的方式收集生物识别信息用于身份识别前，应取得个人书面同意；四是在保证实现业务功能的基础上，应对所收集的生物识别信息直接进行特征和摘要信息提取；五是实现处理目的后，应删除所收集的原始生物识别信息，如原始图像、图片和视频等；六是将生物识别信息用于科学研究，应取得个人信息主体的书面同意。（来源：全国标准信息公共服务平台）

12. 全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——个人信息保护合规审计要求》

5 月 19 日，全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——个人信息保护合规审计要求》，提出了个人信息保护合规审计原则，规定了个人信息保护合规审计的总体要求、实施流程、内容和方法，适用于个人信息处理者和专业机构开展个人信息保护合规审计活动。

《指南》将个人信息保护合规审计实施流程分为五个阶段，包含审计准备、审计实施、审计报告、问题整改、归档管理。例如在审计准备阶段，一是要确定审计范围和依据，二是要建立审计组，三是开展审前调查，四是要确定审计方式方法，五是要编制和评审审计方案。

在审计内容和方法方面，《指南》根据处理个人信息的不同场景，分别提出审计要求。例如审计敏感个人信息处理情况时，应当参考个人信息保护管理制度、处理敏感个人信息情况说明、个人单独同意的实例记录，产品或服务的单独同意取得方式，个人信息处理规则或用户协议等资料。就审计方法而言，一是查看个人信息保护管理制度，是否明确基于个人同意处理个人信息的，事前需要取得个人单独同意；二是查看处理敏感个人信息情况说明，验证存在哪些处理敏感个人信息的情况；三是存在处理生物识别、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，查验征得个人同意的机制，以及个人信息处理者与个人之间签署的告知同意书、来往邮件等；四是使用 App 收集敏感个人信息的，查验个人信息处理者是否通过单独弹窗、单独告知等方式，征得用户的单独同意；五是抽查所处理的敏感个人信息，是否存在对应的征得个人单独同意实例记录。（来源：全国网络安全标准化技术委员会）

13. 全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——个人信息保护合规审计 专业机构服务能力要求》

5 月 19 日，全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——个人信息保护合规审计 专业机构服务能力要求》，规定了专业机构开展个人信息保护合规审计服务的能力要求，包括基本条件、管理体系、专业能力、人员能力、场所与设备资源能力，适用于指导与规范专业机构建设个人信息保护合规审计服务能力，还可为个人信息处理者选择合规审计专业机构提供参考。

《指南》围绕基本条件、管理能力、专业能力、人员能力四个方面，对个人信息合规审计机构提出具体要求。

在管理能力方面，《指南》提出，专业机构应充分考虑个人信息保护合规审计的特点，建立并执行合规审计管理机制和制度，包括建立专业机构管理责任制度，明确合规审计责任部门、责任范围、负责人、工作流程以及与其他部门的协调机制等。

在专业能力方面，《指南》提出，专业机构应具备开展个人信息保护合规审计的专业能力，包括：一是法律法规和标准规范知识，二是个人信息处理活动范围识别能力，三是个人信息识别能力，四是个人信息处理环节识别能力，五是个人信息处理活动相关方识别能力，六是个人信息处理活动保护措施识别和验证能力，七是个人信息处理活动检测能力，八是掌握国家标准《数据安全技术 个人信息保护合规审计要求》中个人信息保护合规审计内容的判别尺度，熟悉对应审计证据和审计方法，形成个人信息保护合规审计业务指导书。（来源：全国网络安全标准化技术委员会）

（三）地方层面动向

1. 北京市人民政府办公厅发布《关于严格规范涉企行政检查的实施意见》

5 月 20 日，北京市人民政府办公厅发布《关于严格规范涉企行政检查的实施意见》，围绕严格规范行政检查主体和人员、全面规范行政检查事

项和标准、强化行政检查源头管控、规范行政检查程序和行为、加强行政检查的执法监督五个方面，提出十八项建议。

严格规范行政检查主体和人员方面，《意见》提出，实施行政检查的主体必须具有法定资格。行政检查应当由行政机关、法律法规授权组织和依法受委托的组织实施。行政机关、法律法规授权组织应当按照法定职责或授权实施行政检查，依法受委托的组织应当在委托权限范围内以委托机关名义实施行政检查。行政检查主体名录经市、区司法行政机关审核确认后向社会公告并动态调整。

全面规范行政检查事项和标准方面，《意见》提出，各市级行政检查主体应当严格落实权责清单制度，清理、公布本领域行政检查事项并动态管理，接受企业和社会监督。未经公布的行政检查事项不得实施。除有法定依据外，不得将入企检查作为行政许可、行政给付等政务服务事项办理的前提条件。严禁以观摩、督导、考察等名义变相入企实施行政检查。实施行政处罚、行政强制确需入企开展的调查取证、文书送达、查封扣押、强制执行等活动，应当严格按照法定程序实施。

强化行政检查源头管控方面，《意见》提出，加快推广非现场监管，最大限度减少入企检查。实施入企检查，不得突破年度行政检查计划确定的入企检查总量，不得突破对同一检查对象的入企检查频次上限。实施入企勘验、复查、核查或者办理投诉举报、转办交办线索等实施的行政检查，不受总量和频次上限限制，但明显超过合理数量或者频次的，行政执法监督机关应当及时跟踪监督。（来源：北京市政府办公厅）

境内前沿观察二：治理实践

导读：5 月，公安、网信、通信管理部门等机构持续发力，对网络信息内容、数据安全、移动应用、个人信息安全等开展治理，助力提升网络安全防护能力，构建更加安全的网络空间。

公安部公布 8 起涉险情、灾情、警情等领域网络谣言案件。山东青岛公安网安部门侦破一起诱骗高校学生注册网络账号并层层倒卖的侵犯公民个人信息案，抓获涉案人员 151 人，涉案金额 4300 余万元。

中央网信办秘书局印发《关于开展“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动的通知》，重点整治四类突出问题。中央网信办推动“清朗·网络平台算法典型问题治理”专项行动，在算法透明度提升、破除“信息茧房”、完善推荐内容审核等方面取得新进展。中央网信办专门印发通知，督促各地网信部门、各网站平台进一步强化“开盒”问题整治工作。中央网信办通报 15 款 App 和 16 款 SDK 个人信息收集使用问题。中央网信办发布第六批涉公共政策、突发案事件、社会民生领域网络谣言典型案例。湖南省 2025 年度“亮剑湖湘·民生领域个人信息权益保护”专项执法行动正式启动。

上海市通信管理局印发电信和互联网行业数据安全专项行动通知，重点检查对象为在电信和互联网行业运营重要网络信息系统或处理重要数据、1000 万人以上个人信息的电信业务经营者。北京、上海等多省市通信管理局发布侵害用户权益 APP/SDK 名单

关键词：网络谣言；营商环境；算法治理；个人信息保护

（一）公安机关治理实践

1. 公安部公布 8 起涉险情、灾情、警情等领域网络谣言案件

5 月 26 日，公安部公布 8 起涉险情、灾情、警情等领域网络谣言案件。

案例一：刘某高编造传播“四川雅安发生 4.6 级地震”网络谣言案。近日，福建公安网安部门查明，刘某高（男，35 岁）为吸粉引流，在某社交平台发布“3 月 30 日凌晨 3 点 18 分，雅安市芦山县发生 4.6 级地震”的谣言信息，引发当地居民恐慌，误导大量网民关注，扰乱社会公共秩序。

案例二：袁某梅编造传播“湖北一水库设置为建筑生活垃圾填埋场”网络谣言案。近日，湖北公安网安部门查明，袁某梅（女，58 岁）编造内容为“冷水镇银钱村干部违规将村组水库设置为建筑生活垃圾填埋场”的网络谣言，发布在某短视频平台，误导大量网民关注和讨论，引发当地居民对生态环境的担忧。经核实，该村正组织挖机对四组水库进行扩容，方便后续蓄水，并非用水库作建筑生活垃圾填埋场。

案例三：陈某编造传播“四川自贡发生火灾”网络谣言案。近日，四川公安网安部门查明，陈某（男，37 岁）为吸粉引流，自行下载一段大火烧山视频后，进行剪辑拼接，并配文“艾叶镇发生火灾，具体情况坐等前方通告，关注我，了解自贡的新鲜事，突发事！”，在某短视频平台发布，引发当地居民恐慌，误导大量网民关注，扰乱社会公共秩序。

案例四：秦某路编造传播“四川一在建小区发生塔吊坍塌事故”网络谣言案。近日，山西公安网安部门查明，秦某路（女，35 岁）为吸粉引流，

利用 AI 工具，编造内容为“突发！四川某小区塔吊坍塌惊魂一刻，工人高空坠落重伤”的网络谣言并发布在其个人网络账号，误导大量网民关注，扰乱社会公共秩序。

案例五：谢某岳编造传播“杭州发生恶性刑事案件”网络谣言案。近日，浙江公安网安部门查明，谢某岳（男，27 岁）为吸粉引流，利用 AI 工具，编造内容为“4 月 7 日凌晨滨江区发生恶性刑事案件”的网络谣言并发布在某互联网平台，引发当地居民恐慌，误导大量网民关注，扰乱社会公共秩序。

案例六：曾某编造传播“大学城发生恐怖事件”网络谣言案。近日，重庆公安网安部门查明，3 月 26 日，重庆公安交管部门在重庆市大学城附近开展巡查酒驾工作，曾某（男，51 岁）为博取眼球，拍摄现场巡查视频并编造“大学城发生恐怖事件，整趴了几个，警车、武警全部出动”虚假警情，在某短视频平台发布，引发当地居民恐慌，误导大量网民关注，扰乱社会公共秩序。

案例七：朱某芳编造传播“重庆秀山打架致 5 人死亡”网络谣言案。近日，重庆公安网安部门查明，4 月 17 日，秀山县龙池学校门口发生一起两车相撞的交通事故，无人员伤亡。朱其芳（女，37 岁）为博取眼球，拍摄现场处置视频并编造“这里打死人了，警察都来了”“重庆秀山，死了 5 人”等虚假警情，在某短视频平台发布，引发当地居民恐慌，误导大量网民关注，扰乱社会公共秩序。

案例八：岑某勇编造传播“深圳地铁发生人员踩踏”网络谣言案。近日，广东公安网安部门查明，岑某勇（男，28 岁）4 月 3 日晚在“深圳北

站”乘坐地铁时，看到一老人弯腰捡东西，遂拍下视频。为博取眼球、吸粉引流，当晚编纂“深圳地铁发生人员踩踏”的谣言视频，发布到某短视频平台，误导大量网民关注，扰乱社会公共秩序。

以上人员均已被依法追究法律责任。（来源：公安部）

2. 山东青岛公安网安侦破一起侵犯公民个人信息案，扩线抓获涉案人员 151 人，涉案金额 4300 余万元

5 月 28 日消息，山东青岛公安网安部门近日侦破一起诱骗高校学生注册网络账号并层层倒卖的侵犯公民个人信息案，并据此发起 2 次集中收网行动，抓获涉案人员 151 人，涉案金额 4300 余万元。

2024 年 4 月，山东青岛公安网安部门工作中发现一重大侵犯公民个人信息案件线索。涉案犯罪团伙成立所谓“充场工作室”，承接各种手机软件和社交平台的“拉新”业务，并以招聘“兼职”的名义，哄骗兼职人员使用个人身份信息开展代为注册网络账号、实名手机号等“代实名注册”业务，涉案团伙通过贩卖个人信息获利。警方制定周密、详实的抓捕方案，历经三个多月多批次抓捕，37 名涉案人员全部落网。

警方侦破这起案件后，又筛查出 200 余个“号商中介”“充场工作室”线索，涉案人员遍布全国 6 个省 85 个地市。各地警方密切配合，共打掉网络黑产犯罪团伙 21 个，抓获违法犯罪嫌疑人 114 人，缴获电脑、手机等作案工具 531 台（部），查获各类网络账号 7 万余个，涉案金额总计 4300 余万元。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办发布侵害用户权益 APP/SDK 名单

5 月 6 日，中央网信办通报 15 款 App 和 16 款 SDK 个人信息收集使用问题。通报指出，墨迹天气 tv 版、医家等 15 款 App 存在未逐一列出收集使用个人信息的 SDK，未准确列出 SDK 收集使用个人信息的目的、方式、范围等问题；CTP 穿透采集、金仕达穿透采集等 16 款 SDK 收集使用个人信息，存在未提供个人信息收集使用规则，未说明自行或协助 App 响应用户个人信息权利请求的措施，未及时响应用户个人信息投诉举报等权利请求等问题。

通报强调，上述 App 和 SDK 运营者应当于通报发布之日起的 15 个工作日内完成整改，并将整改情况报中央网信办。中央网信办将会同有关部门进行核查，并结合整改情况依法依规开展处置处罚。（来源：网信中国）

2. 中央网信办发布第六批涉公共政策、突发案事件、社会民生领域网络谣言典型案例

5 月 12 日，中央网信办发布第六批涉公共政策、突发案事件、社会民生领域网络谣言典型案例。

案例一：“AI 预测彩票号码百分百中奖”谣言。一则“AI 预测彩票号码，百分百中奖”的消息在网络上流传。中国福彩发文提醒，所谓 AI 预测彩票号码均为骗局，请务必警惕。快手平台“落寞人生”“小红书平台”“快来带我吃饭”等账号已被依法依约关闭。

案例二：“广东冰雹比鸡蛋还大”等谣言。近期，有网民借广东冰雹天气，发布“冰雹比鸡蛋还大”“冰雹砸坏汽车”等图片。经广东省互联网举报中心核实，相关图片均为通过AI制作生成的虚假图片，画面明显夸大灾情。百度平台“童生在此”、小红书平台“遥遥雪中客”、今日头条平台“小糖热搜”等账号已被依法依约关闭。

案例三：“杭州滨江发生恶性刑事案件”谣言。网上有消息称“滨江区发生恶性刑事案，嫌疑人已被刑拘”，引发关注。经当地公安机关查证，该信息纯属虚构，系造谣者为博取流量，利用AI生成工具捏造虚假案情，经深度编辑后发布于社交平台，已依法对造谣者作出行政处罚。百度平台“小娱游游”、微信平台“憨憨小魔王”等账号已被依法依约关闭。

案例四：“扫码领取‘五险一金补贴’”谣言。近日，有网民反映收到“扫码领取‘五险一金补贴’”的通知。人力资源和社会保障部表示，通知信息不实且涉嫌诈骗，从未面向普通群众发放过所谓的“五险一金补贴”。微信平台“尼吉特”等账号已被依法依约关闭。

案例五：“故意捏造并传播虚假‘死亡率’”系列谣言。近期，“截至2024年末，80后死亡率突破5.2%”“70后死亡率却低于80后”等信息在网上流传。经公安机关查证，上述信息系个别网民为挑拨情绪、售卖保健品而借机编造的谣言，已对造谣者依法予以行政处罚。知乎平台“江南”、哔哩哔哩平台“晶晶说-”等账号已被依法依约关闭。

案例六：“重庆一工业园区着火10人遇难上百人失联”谣言。近日，有网民散播“10人遇难，16人受伤，上百人失联，重庆一工业园区着火”的信息，引发关注。经重庆市互联网违法和不良信息举报中心向重庆市应

急管理局和重庆市消防救援总队核实，重庆近期未发生此类事故，网传信息系谣言。抖音平台“霞姐”、微博平台“官疯雨”等账号已被依法依约关闭。

案例七：“云南德宏芒市发生5.8级地震”谣言。近日，有网民发布视频称“云南芒市发生5.8级地震”。经芒市委网信办核实，相关视频系造谣者为蹭流量，将缅甸地震视频标注为“云南芒市地震废墟”的不实信息。抖音平台“爱一个人要好好的对她”、快手平台“相识是缘033”等账号已被依法依约关闭。

案例八：“中国残疾人联合会宣传文化部开展APP线上试点”谣言。有网络传言称“中国残疾人联合会宣传文化部开展APP线上试点”，中国残联宣文部严正声明，从未授权任何组织或个人成立所谓“中国残联线上试点线下工作室”，从未组织开展过所谓“APP线上试点精准扶贫助残”等活动。微信平台“然然的”等账号已被依法依约关闭。（来源：网信中国）

3. 中央网信办开展“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动

5月21日，中央网信办秘书局印发《关于开展“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动的通知》，集中整治网络“黑嘴”伤企乱象，督促网站平台健全涉企信息内容管理机制。

专项行动聚焦网络“黑嘴”伤企乱象，重点整治四类突出问题：

一是恶意抹黑诋毁攻击企业问题，包括诋毁攻击企业产品质量、经营状况，捏造虚假信息抹黑企业声誉，对企业进行恶意投诉；组织、操纵“网络水军”“黑公关”，联动发布涉企负面信息，恶意攻击企业或企业家；开展以商养测、以测养商、商测结合的虚假不实测评等

二是对企业进行敲诈勒索问题，包括发布涉企负面信息后，以“删帖”“撤稿”等名义，向企业索取“删稿费”“公关费”；利用自身话语权和影响力，以“舆论监督”“新闻监督”等名义，要挟企业提供“保护费”；在企业新品发布、上市、融资等重要时间节点，发布涉企虚假不实信息或负面信息，胁迫企业开展商务合作。

三是恶意营销炒作问题，包括恶意集纳企业负面信息，唱衰企业或行业发展前景；歪曲解读企业股权结构、财务报表、产品包装等涉企公开信息或新闻报道；翻炒企业旧闻旧事，蹭炒涉企热点事件进行恶意营销。

四是泄密侵权类问题，包括在公众账号名称、头像和简介中假冒仿冒企业家姓名肖像，假借企业家名义发布信息，断章取义企业家过往言论；散布地域歧视、人群歧视言论，对企业家进行污名化或恶意贬损；炒作、泄露企业家个人隐私等。（来源：网信中国）

4. 中央网信办发布信息推荐算法治理新进展

5 月 22 日消息，中央网信办近日推动“清朗·网络平台算法典型问题治理”专项行动取得新进展。

在提升算法透明度方面，中央网信办推动平台公开算法运行规则，推进透明展示工作，保障用户知情权。抖音通过开设“安全与信任中心”网

站、举办开放日活动等方式，向公众阐释推荐逻辑、干预机制及治理成效。微博提升热搜算法透明度，公示上榜规则、数据规则，上线热搜热度标签，标示热度背后的推动因素。微信视频号通过通俗易懂的图文、视频方式向用户公示，发布《一图读懂微信视频号算法推荐》《算法破茧系列》。

在破除“信息茧房”方面，中央网信办推动平台创新推出“茧房评估”“一键破茧”等功能，帮助用户防范“信息茧房”风险。抖音全面升级“使用管理助手”，创新内容偏好评估功能，以可视化形式呈现用户近期浏览内容。小红书设置“内容偏好评估与调节”、“探索更多”功能，方便用户一键操作，浏览更多元丰富的推荐内容。快手依托正能量算法增加对“正向”“有用”“温暖”“信任”等内容挖掘，在算法推荐中充分呈现。

在完善推荐内容审核方面，中央网信办要求平台不断健全推荐内容审核机制，加强正能量内容推送，防范算法推荐低俗不良信息。微信视频号完善“好友推荐”和“算法推荐”双重机制，不断迭代升级识别打击模型，严禁低俗恶俗等典型不良信息进入推荐池。抖音创新推出热点当事人核实机制，防止摆拍造假、仿冒蹭热、拼凑剪接等恶意传播行为。在用户赋权方面。持续优化兴趣偏好管理、内容负反馈等功能设置，便于用户自主调节优化算法推荐内容。快手为用户提供便捷、精细的兴趣偏好管理功能，用户可根据自身喜好，滑动对应兴趣标签，调节不同内容推送强度。微博设置不感兴趣、不看此博主、内容质量差等多种负反馈选项供用户选择，精准响应用户需求。（来源：网信中国）

5. 中央网信办部署进一步加强“开盒”问题整治工作

5 月 27 日消息，中央网信办近日专门印发通知，从阻断“开盒”信息传播、完善预警机制、加大惩治力度、优化保护措施、加强宣传引导等多个维度明确工作要求，督促各地网信部门、各网站平台进一步强化“开盒”问题整治工作。

“开盒”问题整治工作从以下三个方面开展：

一是全力阻断传播渠道。督促网站平台深入清理各类违法发布个人信息，诱导网民跟进泄露隐私，借机进行攻击谩骂、嘲讽贬低的内容，清理教授、买卖或者提供“开盒”方法、教程和服务等信息内容，对于组织煽动“开盒”、提供“开盒”服务等账号、群组，一律予以关闭或者解散。

二是升级完善保护措施。指导网站平台在前期治理网络暴力的基础上，进一步升级完善防护措施，加大“开盒”风险提示力度，设置涉“开盒”举报快速入口，及时核实网民投诉举报，最大限度帮助网民防范和处置“开盒”问题风险。

三是加大打击惩治力度。结合个人信息保护系列专项行动，深入治理违法违规收集使用个人信息等问题，会同有关部门严厉打击泄露、盗取、贩卖个人信息，以及利用个人信息开展违法犯罪活动等行为。此外，也希望广大网民提高防“开盒”意识，强化个人信息保护，自觉抵制相关行为，共同营造清朗有序的网络空间。（来源：网信中国）

6. 湖南省2025年度“亮剑湖湘·民生领域个人信息权益保护”专项执法行动正式启动

5月21日，湖南省2025年度“亮剑湖湘·民生领域个人信息权益保护”专项执法行动正式启动。专项执法行动时间为2025年5月至10月，聚焦个人信息安全问题突出的教育培训、医疗健康、金融理财、房产物业等民生领域，重点整治违规采集人脸信息、采集范围过度、获取方式不当、保护措施不力、违法使用问题突出等五类违法违规收集使用个人信息的问题。（来源：网信湖南）

（三）通信管理部门治理实践

1. 北京、上海等多省市通信管理局发布侵害用户权益APP/SDK名单

（1）上海市通信管理局

5月8日，上海市通信管理局发布2025年第3批侵害用户权益行为APP。近日，上海市通信管理局组织第三方检测机构对上海市移动互联网应用程序进行抽查，共发现15款APP及小程序存在侵害用户权益行为。上述APP及小程序应按有关规定在5月16日前落实整改工作。整改落实不到位的，上海市通信管理局将依法依规组织开展处置工作。（来源：上海通信圈）

（2）安徽省通信管理局

5月7日，安徽省通信管理局宣布下架3款侵害用户权益APP。通报指出，针对2025年第2批次整改不到位的APP，安徽省通信管理局已对相关

APP 予以公开通报，并要求限期整改。截至通报，尚有 3 款 APP 逾期未完成整改。安徽省通信管理局将组织对上述 APP 进行下架，相关应用商店应在通报发出后，立即对名单中的应用软件进行下架处理。

5 月 20 日，安徽省通信管理局通报 2025 年第 3 批侵害用户权益 APP。通报指出，安徽省通信管理局近日对省内 APP 进行了拨测检查，检测发现 16 款 APP 存在违法违规收集使用个人信息的问题，2025 年 4 月 23 日对上述违规 APP 企业下达了责令改正通知书，要求限期完成整改工作。截至通报，尚有 4 款 APP 未完成问题整改，相关 APP 企业应在 2025 年 5 月 26 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。（来源：安徽省通信管理局）

（3）北京市通信管理局

5 月 9 日，北京市通信管理局通报 2025 年第 4 期问题移动互联网应用程序。通报指出，北京市通信管理局近日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 7 款移动互联网应用程序未整改或整改不到位。

2025 年 3 月 31 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 9 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。（来源：北京通信业）

（4）江苏省通信管理局

5月8日,江苏省通信管理局通报2025年第3批侵害用户权益行为APP。通报指出，江苏省通信管理局近日组织第三方检测机构对群众关注的江苏省内地图导航、即时通信等类型的APP进行检查，并通报相关违规APP主办者限期整改。截至通报，尚有5款APP未完成整改。上述APP开发运营者在5月19日前完成整改，整改落实不到位的，江苏省通信管理局将视情采取下架、关停、行政处罚等措施。（来源：江苏通信业）

（5）浙江省通信管理局

5月26日消息，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网上购物、实用工具等类型APP进行检查，书面要求违规APP开发运营者限期整改。截至通报，尚有14款APP未按要求完成整改。请上述APP开发运营者在5月30日前完成整改落实工作，整改落实不到位的，浙江省通信管理局将视情采取下架、关停、行政处罚等措施。（来源：浙江省通信管理局）

2. 上海市通信管理局组织开展“浦江护航”2025年电信和互联网行业数据安全专项行动

5月14日，上海市通信管理局印发《关于开展“浦江护航”2025年电信和互联网行业数据安全专项行动的通知》，对上海市电信和互联网行业数据处理者开展数据安全专项行动。重点对象为在电信和互联网行业运营重要网络信息系统或处理重要数据、1000万人以上个人信息的电信业务经营者。

《通知》提出七项工作重点，一是促进行业数据要素安全流通和利用，二是深化行业首席数据官制度落地实施，三是深入推进重要数据识别认定及目录管理，四是加强行业数据安全风险评估管理，五是加强数据对外共享安全管理，六是加强互联网数据中心客户数据安全保护，七是加强数据安全风险防范及应急处置。

在深入推进重要数据识别认定及目录管理方面，《通知》提出，电信和互联网企业应动态结合国家出台的最新法律法规及其他规范性文件定期进行数据梳理盘点，依据相关标准规范开展重要数据及1000万人以上个人信息识别工作，形成并定期更新本单位重要数据目录，在7月31日前向市通管局备案。当重要数据条目数量或者存储总量等变化30%以上，或者其他备案内容发生重大变化时，企业应在三个月内向市通管局更新备案。

在加强互联网数据中心客户数据安全保护方面，《通知》提出，互联网数据中心企业应依据《关于加强互联网数据中心客户数据安全保护的通知》《互联网数据中心客户数据安全保护实施指引》要求，明确客户数据安全责任边界及管控要求，开展自查自纠；互联网数据中心企业可自行或委托第三方专业机构定期开展客户数据安全保护能力评价。市通管局对互联网数据中心企业数据安全保护工作进行监督检查。（来源：上海通信圈）

（四）其他部门治理实践

1. 国家网络与信息安全信息通报中心通报 3 批违法违规移动应用清单

5 月，国家网络与信息安全信息通报中心通报 3 批违法违规移动应用清单。

经国家计算机病毒应急处理中心于 2025 年 4 月 8 日至 2025 年 4 月 28 日期间检测发现，65 款移动应用存在违法违规收集使用个人信息情况。其中，9 款移动应用存在首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则等问题；43 款移动应用存在隐私政策未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等；16 款移动应用存在个人信息处理者向其他个人信息处理者提供其处理的个人信息的，未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。通报指出，2025 年 4 月 18 日通报的违法违规移动应用 67 款，经复测仍有 31 款移动应用存在问题，相关移动应用分发平台已予以下架。

经公安部计算机信息系统安全产品质量监督检验中心于 2025 年 4 月 16 日至 2025 年 5 月 15 日期间检测，35 款移动应用存在违法违规收集使用个人信息问题。其中，12 款移动应用未以结构化清单的方式逐一列出收集、使用个人信息规则；18 款移动应用实际收集的个人信息超出用户授权范围；2 款移动应用个人信息保护政策中描述收集的个人信息与业务功能无直接关联；8 款移动应用在配置文件中声明与移动应用的所有业务功能均没有直

接关联的权限；1 款移动应用申请的可收集个人信息的权限与业务功能没有直接关联；2 款移动应用提前要求用户授权当前未使用的特定功能所需的权限；2 款移动应用提前要求用户填写当前未使用的特定功能需要的个人信息；2 款移动应用实际收集的个人信息与业务功能没有直接关联；10 款移动应用实际收集个人信息的频率与业务功能没有直接关联；1 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；5 款移动应用广告存在误导、欺骗用户行为。

经国家计算机病毒应急处理中心于 2025 年 4 月 29 日至 2025 年 5 月 23 日期间检测，63 款移动应用存在违法违规收集使用个人信息情况。其中，8 款移动应用存在投诉、举报未在承诺时限内受理并处理，未建立便捷的个人行使权利的申请受理和处理机制；34 款移动应用存在未向用户提供撤回同意收集个人信息的途径、方式，以及未提供便捷的撤回同意的方式；9 款移动应用未采取相应的加密、去标识化等安全技术措施。通报指出，2025 年 5 月 12 日通报的 65 款违法违规移动应用，经复测仍有 16 款存在问题，相关移动应用分发平台已予以下架。（来源：国家网络安全通报中心）

2. 国家版权局等四部门启动“剑网 2025”专项行动

5 月，国家版权局、工业和信息化部、公安部、国家互联网信息办公室四部门联合启动打击网络侵权盗版“剑网 2025”专项行动。

专项行动聚焦六个主要方面开展重点整治：一是以视听作品版权整治为重点，加强对电影、电视剧、网络剧、微短剧、短视频的版权保护，重

点打击非法搬运、传播、售卖视听作品的侵权行为，加强对网站平台帮助侵权治理，为网络视听产业健康发展提供良好版权保障。

二是以动漫及游戏领域版权整治为重点，加强对动漫及游戏相关作品及衍生品的版权保护，严厉打击非法复制传播动漫作品、生产销售侵权盗版动漫 IP 衍生品以及实施侵害游戏版权的私服、“外挂”等行为，推动动漫、游戏相关作品的版权转化运用。

三是以计算机软件版权整治为重点，重点打击通过虚假授权、超范围授权销售侵权盗版软件非法牟利行为，持续净化软件产业发展环境，维护软件市场公平竞争秩序和消费者合法权益，推进软件正版化工作深入开展。

四是以网络存储+传播领域的版权整治为重点，重点打击相关平台直接侵权、故意为侵权盗版提供网络服务的帮助侵权，以及教唆、诱导、鼓励用户侵权等违法行为，有效加强浏览器+搜索引擎+网盘商业模式的版权监管。

五是以网络销售版权整治为重点，重点打击网络销售侵权盗版制品及资源链接等行为，加大对涉及青少年权益、通过隐蔽渠道分销等新型侵权盗版销售模式的关注，着力规范电商平台、直播平台、短视频平台网络销售版权秩序。

六是以流媒体智能终端版权整治为重点，重点打击智能终端破坏技术措施非法接入正版 APP 提供作品资源、直接提供侵权盗版资源或链接的违法行为，强化对交互式网络电视、智能电视机顶盒、佩戴式智能终端等流媒体软硬件的版权监管，净化流媒体智能终端市场版权环境。（来源：国家版权局）

3. 北京市海淀区法院发布一起涉互联网医疗平台数据搬运案

5 月 12 日，北京市海淀区法院发布一起涉互联网医疗平台数据搬运案。

因认为海洋公司经营的平台大量爬取、搬运其平台的患者点评数据、医生科普文章数据等平台数据（以下合称涉案数据）的行为构成不正当竞争，时代公司将海洋公司诉至法院，要求海洋公司消除影响、赔偿经济损失及合理开支 500 万元。

海洋公司辩称，其运营的乙平台与时代公司运营的甲平台分属互联网医疗领域不同赛道，二者之间不存在竞争关系。涉案数据归属于用户，时代公司不享有相应权益。时代公司证据无法证明海洋公司实施了被诉行为，即便海洋公司实施了被诉行为，其使用的系甲平台中的公开信息，未超过“必要、合理”的限度，未违背行业通行的商业道德，不存在不当目的，且已及时删除处理，未给时代公司合法权益造成损害。时代公司主张的经济损失和合理开支亦缺乏依据且明显过高，不应得到支持。

法院经审理后认为，时代公司与海洋公司同处互联网医疗领域，所面向的用户群体、提供的服务内容以及开展的经营活动均有重合之处，属于具有竞争关系的同业经营者。时代公司合法地对用户生成的内容进行收集，并通过不同分类，对涉案诊疗问答、就医评价和涉案医学科普文章进行收集、存储、编排、整理后，以内容集合形式整体向用户和社会公众传播并加以利用，进一步吸引患者和医生用户聚集，由此获得了交易机会和市场竞争优势。时代公司对于涉案就医评价和涉案医学科普文章合集所享有的

竞争性权益，独立于平台用户对其创作内容所享有的权利，应受反不正当竞争法保护。

海淀法院经审理，认定海洋公司被诉行为构成不正当竞争，判决海洋公司就其不正当竞争行为消除影响，赔偿时代公司经济损失200万元及合理开支30万元。宣判后，海洋公司提起上诉，二审法院维持原判。该判决现已生效。（来源：北京海淀法院）

境内观察三：人工智能安全专题

导读：5 月，世界互联网大会人工智能专委会主办的“数字转型创新、智绘健康未来”研讨会在北京国家会议中心召开。会议就促进人工智能赋能医疗健康提出三点建议，包括鼓励融合创新，激发跨界发展活力；严守安全底线，筑牢风险防控屏障；加强国际合作，实现协同普惠发展。

中英人工智能对话在北京举行。双方围绕人工智能发展机遇、挑战和各自政策深入交换意见，支持继续加强交流互鉴及务实合作，促进两国人工智能健康安全有序发展。

上海警方侦破一起利用人工智能技术编造、传播网络谣言损害企业权益案，抓获姚某、陈某等 8 名犯罪嫌疑人。

关键词：人工智能赋能；人工智能发展；网络谣言传播

1. 世界互联网大会人工智能专委会召开“数字转型创新、智绘健康未来”研讨会

5 月 17 日，由世界互联网大会人工智能专委会主办的“数字转型创新、智绘健康未来”研讨会在北京国家会议中心召开。

会议认为，当前数字技术正以前所未有的深度和广度重塑医疗健康生态系统，数字化转型和人工智能技术是推动医疗健康迈向高质量发展的关键引擎。会议就促进人工智能赋能医疗健康提出三点建议：

一是鼓励融合创新，激发跨界发展活力。相关机构应积极拥抱人工智能等新技术，主动适配医疗行业需求，探索人才联合培养和学科共建，促进产学研深度融合。

二是严守安全底线，筑牢风险防控屏障。坚持“以人为本”理念，确保人工智能技术在符合法律法规、医学伦理、公众利益的前提下发展。

三是加强国际合作，实现协同普惠发展。发挥国际组织平台作用，加强智慧医疗领域交流，探索打破数据壁垒，助力孵化全球普惠的国际公共产品。（来源：网信中国）

2. 中英举行人工智能对话

5 月 20 日，中英人工智能对话在北京举行。外交部军控司司长孙晓波和英国外交发展部科技司司长琼斯共同主持，国家发展改革委、科技部、工业和信息化部、国家网信办及英国科学创新和技术部、内阁办公室、商业贸易部、驻华使馆官员等参加。

双方围绕人工智能发展机遇、挑战和各自政策深入交换意见，支持继续加强交流互鉴及务实合作，促进两国人工智能健康安全有序发展。双方同意就人工智能全球治理保持沟通协调，推动落实联合国未来峰会通过的《全球数字契约》，帮助发展中国家加强能力建设，确保人工智能向善普惠发展。（来源：外交部）

3. 上海警方侦破一起利用人工智能技术编造、传播网络谣言损害企业权益案

5 月 29 日，上海警方侦破一起利用人工智能技术编造、传播网络谣言损害企业权益案，抓获姚某、陈某等 8 名犯罪嫌疑人。

2025 年年初，上海长宁警方接辖区茶饮企业报案称，多个自媒体平台出现大量针对该企业及创始人的不实信息，损害了企业品牌形象，影响了企业正常运营，部分区域门店单日营业额同比下降超 20%。接报后，长宁警方立即成立专案组开展侦查。

经查，嫌疑人姚某系职业自媒体人，运维某财经类账号，靠文章植入广告赚取广告费，但长期以来收入不佳。为提高账号流量获取广告收益，姚某花费 800 元在网上找到卢某代笔。卢某接单后，利用 AI 生成了一篇涉及霸王茶姬茶饮的文章，文中包含大量不实信息。姚某未经核实便在十余个自媒体平台账号上发布，全网浏览量迅速上涨，引发网民对该茶饮企业的质疑。

嫌疑人陈某平时主要经营 AI 网络培训，为了推广培训课程，其主动联系好友赵某，告知其在某平台发布文章的阅读量达到一定程度可以获取现

金提现。随后陈某将从网络上搜集的各类关于霸王茶姬企业创始人的身世及创业过程的传言，未经核实即用 AI“洗稿”后生成的文章在赵某个人账号上发布，短时间内即获得了较高阅读量。其余嫌疑人也分别通过 AI 洗稿、盲目转载等方式参与谣言传播，以达到引流博取热度、实现快速涨粉等目的。目前，8 名犯罪嫌疑人均已被长宁警方依法采取刑事强制措施。（来源：新京报）

五、境外前沿观察：月度速览十则

导读：5 月，境外国家和地区在人工智能、网络安全、数据安全等方面的政策法律和热点事件持续发生。

人工智能方面，日本参议院通过《人工智能相关技术研究开发及应用推进法案》。乌克兰数字化转型部副部长签署欧洲委员会关于《人工智能与人权、民主和法治框架公约》。美国商务部宣布正式撤销拜登政府发布的《人工智能扩散规则》，商务部工业与安全局发布三项强化半导体技术出口管制的措施，强化对中国先进计算芯片及人工智能模型相关技术的出口管制。美国众议院“美中战略竞争特别委员会”主席联合两党多位议员共同引入《芯片安全法案》，旨在限制美国先进人工智能芯片对华出口。

网络安全方面，美国总统特朗普签署《删除法》，旨在把发布未经同意的私密影像的行为定为犯罪。美国司法部公布美国国防承包商 Raytheon Companies 和其分拆企业 Nightwing Group 需支付 840 万美元和解金，以解决其未能达到联邦网络安全标准的指控。

数据安全方面，欧盟与新加坡签署《欧盟—新加坡数字贸易协定》，致力于消除跨境数据流动壁垒，明确双方不得以数据本地化为由限制信息传输。欧洲数字权利中心向 Meta 发出禁止令，质疑其在未经选择同意的情况下使用欧盟用户个人数据进行人工智能训练的计划，违反欧盟 GDPR。TikTok 因向中国传输个人数据被处以 5.3 亿欧元罚款。欧盟委员会初步认定 TikTok 的广告存储库违反《数字服务法》。

关键词：人工智能；深度伪造；跨境数据流动；个人数据保护

1. 欧盟与新加坡签署《欧盟－新加坡数字贸易协定》

5 月 7 日，欧盟与新加坡签署《欧盟－新加坡数字贸易协定》。本协定是在 2019 年签署的《欧盟－新加坡自由贸易协定》基础上进一步拓展的成果。协定致力于消除跨境数据流动壁垒，明确双方不得以数据本地化为由限制信息传输。同时，协定重申各方有权在本国领土内实施合理监管，以实现公共健康、安全、数据保护等合法政策目标。协定强调个人数据保护的重要性，要求双方维持高水平的法律框架，鼓励在不同法规体系下寻求互认和合作。

在促进数字贸易便利化方面，协定承认电子合同与电子签名的法律效力，明确不得对电子化传输行为征收关税，不得仅因服务以电子方式提供而设立前置许可要求。此外，协定规定双方不得强制要求转让或披露软件源代码，除非为保障国家安全或执法需要，且须具备相应保密机制。协定还涵盖了电子支付、电子发票、无纸化贸易、网络安全、消费者权益保护以及打击垃圾邮件等具体内容，鼓励采用国际通用标准，推动系统互通与监管协同。为增强中小企业在数字贸易中的参与度，协定还提出将加强信息共享、数字能力建设和数字包容性。

此外，协定建立了明确的争端解决机制，确保条款执行的透明度与可预期性，同时预留了对协定内容进行审查与更新的空间，以期与不断演进的技术与市场保持同步。（来源：欧盟委员会）

2. 美国商务部废除拜登时代的《人工智能扩散规则》，发布三项管制措施

5 月 13 日，美国商务部宣布正式撤销拜登政府于年初发布的《人工智能扩散规则》，此外美国商务部工业与安全局同时发布三项强化半导体技术出口管制的措施：《关于可能适用于先进计算芯片及其他用于训练人工智能模型商品的管制的政策声明》；《关于通用禁令 10（GP10）对中国先进计算芯片适用的指南》；《关于防止先进计算芯片转移的行业指南》，旨在进一步细化并强化对中国先进计算芯片及人工智能模型相关技术的出口管制。

《政策声明》强化对先进芯片及人工智能技术流向特定国家（尤其是包括中国在内的 D:5 国家组）的出口管制，以防止其用于军事、情报或大规模杀伤性武器等威胁美国国家安全的领域。《芯片适用指南》提醒业界使用中国先进计算芯片（如华为昇腾系列）的风险，这类芯片可能在违反美国出口管制下开发或生产。指南指出，根据 GP10 的规定，使用此类先进计算芯片可能构成违反美国出口管制的行为，并可能导致公司面临商务部的执法行动。《行业指南》列出新的交易和行为“红旗”警示清单，帮助公司评估相关方或活动是否与出口管制规避有关；规定实施尽职调查行动及最佳实践等。（来源：美国商务部）

3. 乌克兰签署《人工智能与人权、民主和法治框架公约》

5 月 15 日，乌克兰数字化转型部副部长 Oleksandr BORNIAKOV 签署欧洲委员会关于《人工智能与人权、民主和法治框架公约》。《公约》主要内容包括：

一是缔约方的一般性义务，包括：（1）保护人权。缔约方应采取或维持措施，确保人工智能系统生命周期内的活动符合适用国际法和其国内法规定的保护人权义务；（2）尊重法治。缔约方应采取或维持措施，确保人工智能系统不被用于破坏民主机构和进程的完整性、独立性和有效性等。

二是缔约方应遵守的相关原则，包括：（1）个人自主权原则。各缔约方应采取或维持措施，在人工智能系统生命周期内的活动中尊重人的尊严和个人自主权；（2）确保透明度原则。各缔约方应采取或维持措施，确保针对人工智能系统生命周期内的活动制定适合具体情况和风险的充分透明度和监督要求，包括识别由人工智能系统生成的内容，提高公众对人工智能系统的信任，促进其合理应用；（3）落实问责制原则。各缔约方应采取或维持措施，确保对人工智能系统生命周期内的活动对人权、民主和法治造成的不利影响负责，包括明确责任主体，建立相应的问责机制，确保在出现问题时能够及时追究责任等。（来源：欧洲委员会）

4. 美国国会引入《芯片安全法案》，强化芯片出口管制

5 月 15 日，美国众议院“美中战略竞争特别委员会”主席联合两党多位议员共同引入《芯片安全法案》，旨在限制美国先进人工智能芯片对华出口。

该法案主要包括三项机制：（1）人工智能芯片位置验证。美国商务部将被授权在180日内建立位置验证机制，对先进人工智能芯片的最终使用地点进行核实，确保其不会被非法转移至敏感地区；（2）强制报告。芯片制造商将被要求对敏感技术可能被转运至受限对象的情况向商务部工业与安全局进行强制报告；（3）执行评估。商务部还需在该法案实施1年内对法案进行全面评估，考虑是否需要设置额外安全机制和修改出口管制标准。

美中战略竞争特别委员会主席发表声明表示，长期以来，中国政府通过多种手段将敏感的美国技术引入中国以强化对美竞争，这一趋势已对美国国家安全构成威胁，削弱了美国在人工智能领域的全球领导地位。此前，美中战略竞争特别委员会已就相关事件发布DeepSeek相关报告。5月8日，参议院也引入同名法案，表明这一立法已获得国会两院的广泛支持。（来源：美中战略竞争特别委员会）

5. 美国总统特朗普签署《删除法》，把发布未经同意的私密影像的行为定为犯罪

5月19日，美国总统特朗普在白宫签署《通过阻止网站和网络上技术生成的深度伪造影像来应对已知剥削工具法》，即《删除法》，使其正式成为法律。该法旨在把发布未经同意的私密影像的行为定为犯罪，并要求科技平台在收到删除要求时，48小时内删除相关内容，否则将被联邦贸易委员会处罚。

该法禁止在满足以下三点的情形下，未经同意发布成年人或未成年人的私密影像：（1）影像在隐私情境下获取；（2）影像是非自愿公开或公

众关注内容；（3）意图或实际对成年人造成心理、财务或声誉损害或意图虐待、性剥削未成年人。此外，对于使用人工智能等技术生成或篡改的私密影像，未经同意发布，且符合上述真实影像条件的行为也被禁止。同时，法案规定以下例外情形：（1）执法或情报机构的合法活动；（2）基于举报、医学用途等的合法目的披露；（3）个人自愿发布（不包括发布包括儿童色情内容）等。

对于违反上述规定的个人主体，最高可被判处 3 年监禁和罚款；未履行相关删除义务的科技平台将被视为“不公平或欺诈行为”,面临调查和处罚。（来源：美国白宫）

6. 日本参议院通过首部人工智能法案

5 月 28 日，日本参议院全体会议通过《人工智能相关技术研究开发及应用推进法案》（人工知能関連技術の研究開発及び活用の推進に関する法律案）。这是日本首部专门针对人工智能的法案，旨在促进人工智能相关技术研发和应用并防止其滥用。

该法案指出人工智能技术是日本经济社会发展的基础，从安全保障的角度来看也是重要的技术。依据本法，拟设立以日本首相为首、全体内阁成员参加的“人工智能战略本部”作为日本人工智能政策的“司令部”，并制定“人工智能基本计划”。该法案提出，日本应在人工智能领域保持研究开发能力，并提高相关产业的国际竞争力。日本政府有责任全面且系统地制定和实施推动人工智能研发和应用的措施。

为防止人工智能技术被滥用而引发侵权问题，缓解公众对生成式人工智能制造虚假信息等的不安，该法规定，日本政府要对侵权行为展开调查，并给涉事企业以建议和指导，企业有义务配合相关调查。对于使用人工智能制作虚假视频、侵犯著作权等行为，日本政府将进行分析调查，并可公开相关企业的名称。（来源：新华网）

7. 美国司法部公布国防承包商需因网络安全违规支付 840 万美元和解金

5 月 1 日，美国司法部公布美国国防承包商雷神公司 Raytheon Companies 和其分拆企业夜翼集团 Nightwing Group 需支付 840 万美元和解金，以解决其未能达到联邦网络安全标准的指控。

根据美国司法部披露的和解协议，从 2015 年 8 月至 2021 年 6 月期间，雷神公司旗下 CODEX 部门（网络攻防专家团队）使用的网络系统未能符合国防部网络安全要求，且存储着非机密的国防信息。此外，该公司虽未承认过错，但被指控未能制定必要的“系统安全计划”，且在 2020 年 5 月才向政府坦承其网络系统不符合美国国家标准与技术研究院（NIST）的安全标准。

本案由雷神公司前工程总监作为举报人发起，其将获得超过 150 万美元的和解金分成。涉事的夜翼公司原为雷神技术旗下部门，于 2024 年完成分拆独立运营。目前，雷神和夜翼公司均未对和解协议作出回应。（来源：美国司法部）

8. TikTok 因向中国传输个人数据被处以 5.3 亿欧元罚款

5 月 2 日，爱尔兰数据保护委员会（DPC）公布对 TikTok 的调查最终决定，主要关注 TikTok 将欧洲经济区（EEA）用户个人数据传输至中国的合法性，以及其在透明度方面的合规性。调查结果显示，TikTok 在数据传输和透明度义务方面违反《通用数据保护条例》（GDPR），因此被处以 5.3 亿欧元的罚款，并要求在 6 个月内整改，否则将暂停对中国的数据传输。

DPC 副专员格雷厄姆·道尔指出，GDPR 要求在数据跨境传输时必须保持欧盟的高数据保护标准。TikTok 未能证明其在中国的员工对 EEA 用户数据的访问能够维持与欧盟相同的保护水平。此外，TikTok 在调查期间曾表示未在中国服务器上存储 EEA 用户数据，但后来承认确有少量数据存储在中国，这与其之前提供的信息不符。

DPC 表示将考虑是否需要采取进一步的监管措施，并将在适当时候公布完整决定及相关信息。（来源：爱尔兰数据保护委员会）

9. 欧洲 NOYB 要求 Meta 停止使用用户数据训练人工智能

5 月 14 日，欧洲数字权利中心（NOYB）向 Meta 发出禁止令，质疑其在未经选择同意的情况下使用欧盟用户个人数据进行人工智能训练的计划，违反欧盟《通用数据保护条例》（GDPR）。

起因为 Meta 宣布从 5 月 27 日起，它将使用来自 Instagram 和 Facebook 用户的欧盟个人数据训练其新开发的人工智能系统。Meta 并未征求消费者的明确同意（即“选择加入”机制），而是基于所谓的“合法利益”主张，

直接吸纳所有用户数据。欧盟新出台的《集体救济指令》（Collective Redress Directive）授权 NOYB 等实体在欧盟范围内提起禁止令。

NOYB 认为 Meta 在未经用户选择同意的情况下使用欧盟个人数据，违反 GDPR 第 6 条第（1）款，并且 Meta 限制用户的反对权，违反 GDPR 第 21 条。同时，Meta 也可能无法遵守其他 GDPR 的规定，如被遗忘权、纠正错误数据的权利，或允许用户在人工智能系统中访问其数据的权利。（来源：欧洲数字权利中心）

10. 欧盟委员会初步认定 TikTok 的广告存储库违反《数字服务法》

5 月 15 日，欧盟委员会初步认定 TikTok 的广告存储库违反《数字服务法》。TikTok 没有提供有关广告内容、广告针对的用户以及广告付费商的必要信息。此外，TikTok 的广告库不允许公众根据这些信息全面搜索广告，从而限制该工具的有用性。

2024 年 2 月 19 日，委员会启动正式程序，以评估 TikTok 是否可能违反《数字服务法》。除了广告透明度外，诉讼还涵盖 TikTok 算法系统设计产生的负面影响（例如“兔子洞效应”和行为成瘾）、年龄保证、确保未成年人高度隐私、安全和保障的义务以及研究人员的数据访问等。

委员会建立一个举报工具，允许员工和其他知情者以匿名方式联系委员会,通过指定的超大型在线平台(VLOP)和超大型在线搜索引擎(VLOSE)为委员会的合规性监控做出贡献。（来源：欧盟委员会）

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. 基于区块链与联邦学习的中医循证可信数据空间构建

摘要：在中医药现代化进程中，中医循证研究对跨机构、多源异构数据共享提出了迫切需求，但数据隐私泄露、信任缺失与安全风险等问题成为主要障碍。本文创新性地提出基于区块链与联邦学习技术的可信数据空间架构，旨在解决中医循证研究中的数据安全与隐私保护难题。通过构建基于联盟链的中医药数据目录和权属体系，利用智能合约实现数据访问的细粒度控制，并结合分布式协同计算，该架构在确保数据不出医院的前提下，实现了跨院间中医联合循证分析，为提升中医临床数据的利用效率和共享安全性提供了切实可行的解决方案。

关键词：区块链、中医循证、联邦学习、可信数据空间

在数字时代，医疗数据已成为国家基础性战略资源，在疾病诊治、新药研发及医学研究等领域展现出巨大价值。中医药临床数据作为中医诊疗经验的直观体现，对挖掘中医隐形诊疗经验、构建显性诊疗知识体系具有重要意义。然而，中医药数据的多源异构特性、数据标准不一致、质量难以保证等问题，严重制约了数据的利用效率。同时，数据权属不明确、隐私保护不足等问题，阻碍了数据的流通与共享，成为制约中医循证研究发展的瓶颈。在此背景下，如何构建一个安全、可信、高效的中医药数据共享环境，成为亟待解决的问题。

一、传统中医药数据跨医院共享的痛点

随着国际上对传统医学的关注度不断提高，中医药作为一种具有独特理论和实践体系的传统医学，面临着更严格的科学评估和验证要求。中医

循证即是遵循证据的中医医学诊疗方法，旨在依据可靠的证据制定临床决策，其核心在于系统性收集、评估和应用中医药临床数据以验证中医诊疗的有效性与安全性，这要求打破单个医疗机构的数据局限，整合多源异构的中医药数据资源，从而为跨医院的数据共享带来迫切需求，但传统中医药数据跨医院共享面临以下痛点问题：

1、数据安全与隐私保护存在较大风险

随着医疗数据系统逐步实现数字化，在数据生产、数据存储、数据传输、数据利用等过程中，始终面临着多重安全风险。由于医疗数据本身含有大量患者隐私，对数据的安全性和隐私性具有较高需求，一旦发生数据窃取、泄露、篡改或恶意删除等安全问题，都将会对患者和医疗机构造成巨大的损失。

2、医疗健康数据所有权和使用权界定不清

由于缺乏统一的法律框架和标准，患者、医疗机构、数据平台等各方在数据归属、使用权限和利益分配上存在分歧。这导致医疗机构在数据共享时顾虑重重，担心侵犯患者隐私或承担法律责任，而患者则担心个人信息泄露。同时，数据的不流通也限制了医疗研究和临床决策的效率，影响了医疗服务的质量和创新。

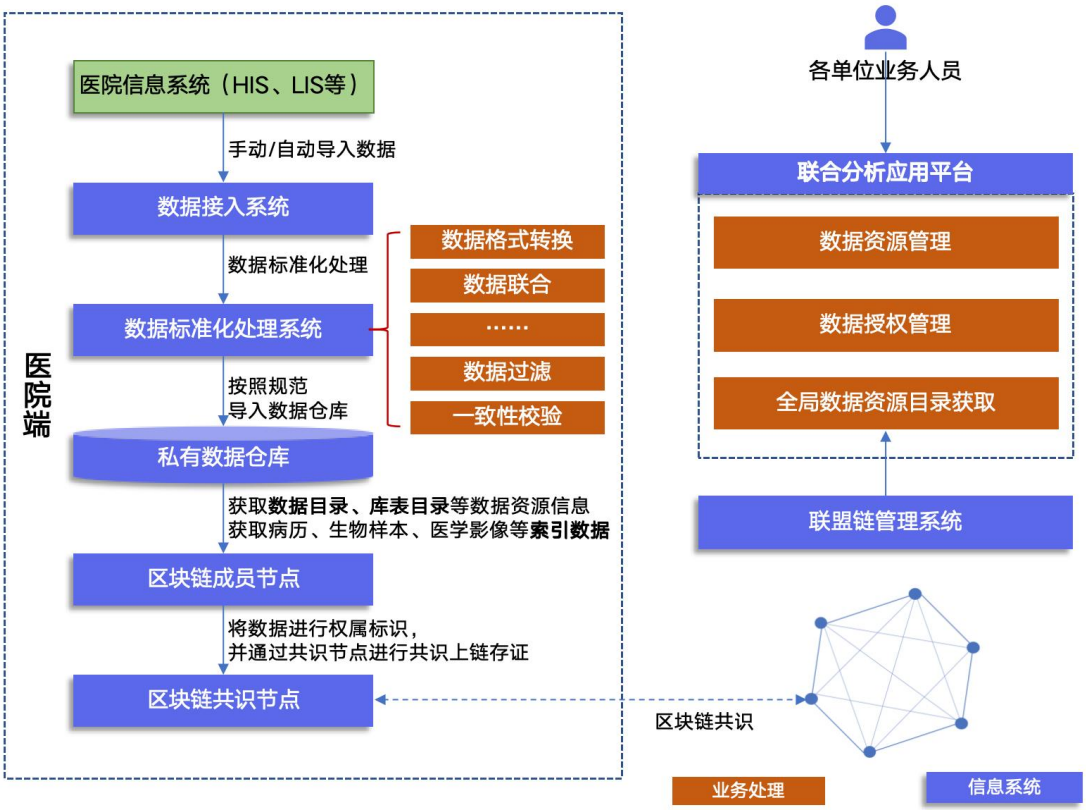
二、“一链、一平台、多端”分布式协同数据共享框架

针对上述痛点，本文提出“一链、一平台、多端”（1+1+N）的中医循证可信数据空间架构，依托区块链技术多方共识、分布式记账、防篡改、国密化加密、智能合约等特性，综合运用大数据分析、隐私计算等技术，

将本地、中心式处理转变为联邦学习、群体协作的创新模式，实现在数据不出医院的前提下完成跨机构间的多源数据共享与分析应用。

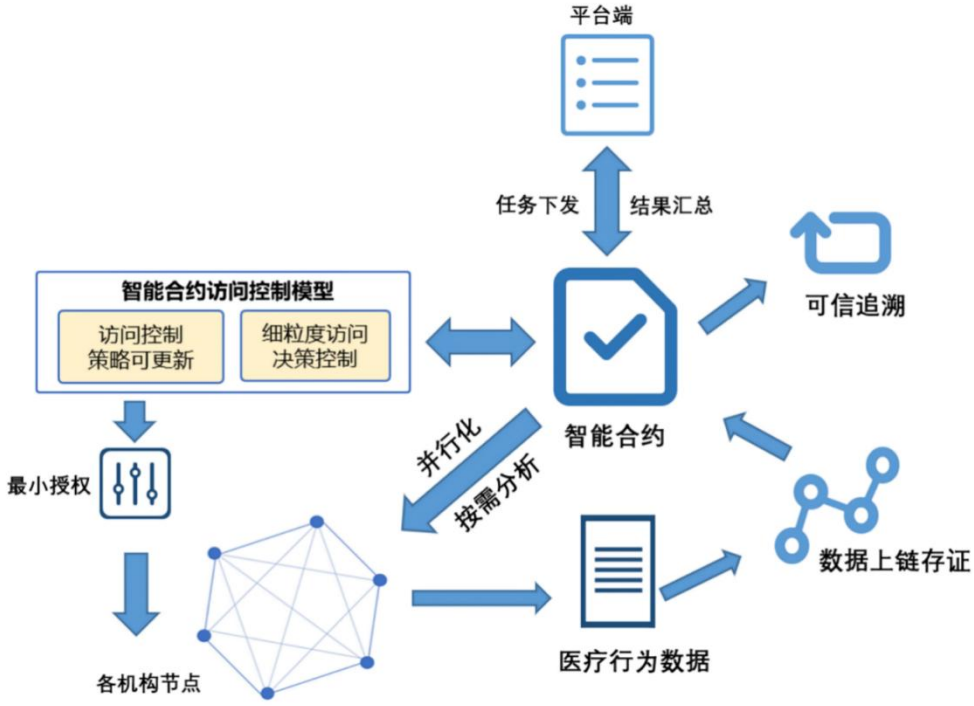
1、依托联盟链的中医药数据目录和权属体系

联盟链以其去中心化、不可篡改、可追溯等特性，为中医药数据共享提供了一个安全可信的基础设施，通过将患者主索引、入出院记录、诊断结果、检验数据等的条目、元数据、索引、Hash 特征等信息上链存证，而非直接存储原始数据，可以有效保护数据隐私；同时，基于联盟链的共享账本，各医疗机构可以平权共建数据目录和权属体系，实现数据信息的全面归集，为跨机构数据共享奠定坚实基础。



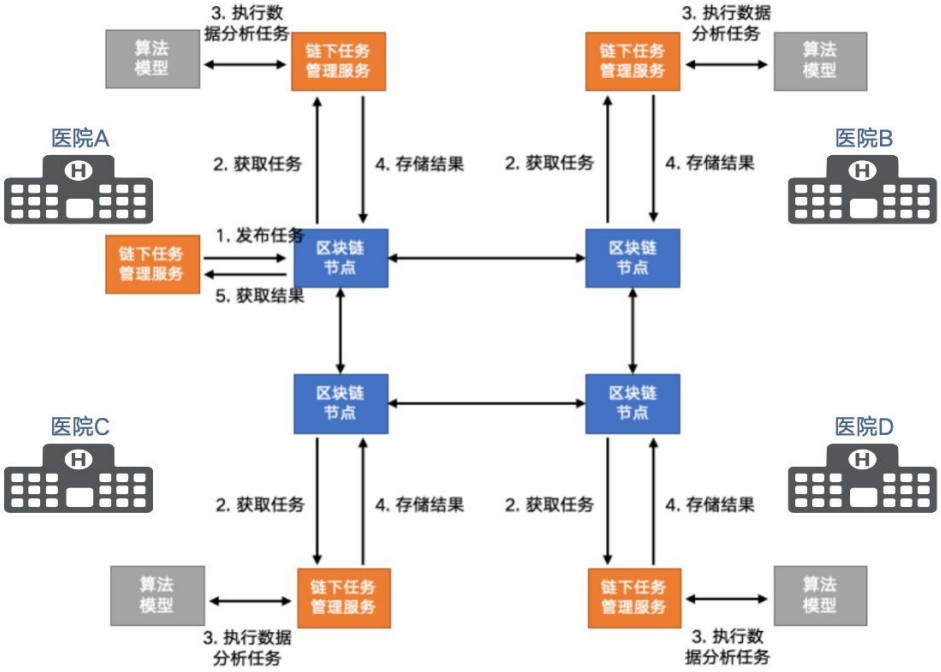
2、依托智能合约对数据访问进行细粒度控制

基于智能合约构建多机构间自动化、细粒度的身份管控，对数据进行确权和最小粒度的授权使用。在中医循证研究的多机构数据共享场景中，借助智能合约，各参与机构可以根据自身的角色、权限以及数据使用目的，制定精细化的访问控制策略。例如，对于不同的研究项目、不同的数据类型，设置差异化的访问权限级别，只有满足特定条件如经过严格的授权审批流程、具备合法的研究资质等，才能获得相应数据的访问权；同时，通过智能合约对数据的使用权进行精确划分，确保数据使用仅限于授权范围内，防止数据被滥用和过度访问。



3、基于联盟链网络的分布式协同计算

在联盟链网络的支撑下，结合分布式统计、联邦学习、群体学习等先进算法，可以将任务需求、计算模型参数、计算结果中间状态等数据进行链上流转；通过链上链下协同计算范式，实现数据在不出医院的前提下，完成跨院间的分布式协同计算。具体而言，各医疗机构在本地对数据进行处理和分析，仅将加密后的计算结果和模型参数上传至联盟链网络，从而实现数据的分布式协同利用，确保数据的隐私性和安全性，同时提升数据的利用效率和价值挖掘深度。



三、结语

在中医药现代化发展的进程中，数据共享与安全保护之间的矛盾日益突出。通过创新性地构建基于区块链与联邦学习的可信数据空间架构，为中医循证研究中的数据安全与隐私保护问题提供了一种可行的解决方案。这一架构不仅能够打破医疗数据孤岛壁垒，还能够建立一个自主、安全、智能、高效、平等、开放的中医药数据共享生态。

展望未来，随着区块链、联邦学习等技术的不断成熟和完善，以及相关法律法规和标准的逐步健全，该架构有望在更广泛的医疗领域得到推广应用，这将有力推动医疗数据的安全共享与高效利用，助力医疗服务质量和创新能力的提升，构建更加安全可信、高效、可持续的医疗数据价值化发展生态系统。（作者：李青山 博雅正链（北京）科技有限公司）

2.5G NTN 标准化进展及关键安全技术

摘要：随着天地一体化网络融合标准化工作的推进，5G NTN 在满足海量物联网设备接入及高速低时延业务需要的同时，面临着信令过载和敏感信息泄露等风险。为此，5G NTN 提出了临时 UID、星载核心网功能等关键技术，这些技术有助于提升 5G NTN 网络的安全及可用性。

关键词：非地面网络；卫星通信；安全与隐私；

引言

非地面网络具有网络覆盖面广、容灾能力强、组网成本低的特点，使其可以作为地面网络的有力补充。天地一体化融合网络可以实现全天候，全地域的覆盖。在个人移动通信、物联网、交通运输及应急救灾等领域具有广泛的应用前景。

2022 年 3GPP Rel-17 版本正式确定了 5G NTN 标准，加速了天地一体化网络的标准化工作。从 3GPP Rel-17 的基础架构搭建到 Rel-19 的新场景适配，5G NTN 技术逐步实现从概念验证向商用场景的跨越，形成空天地一体化的泛在接入网络体系。

5G NTN 与地面 5G 网络有着不一样的网络结构及特点，在高带宽、低时延，支持海量机器通信应用场景下，面临着许多技术挑战及安全风险。

本文主要介绍了 3GPP Rel17~Rel19 标准中 5G NTN 的技术进展及关键安全技术。

1 5G NTN 网络介绍及标准化进展

1.1NTN 网络介绍

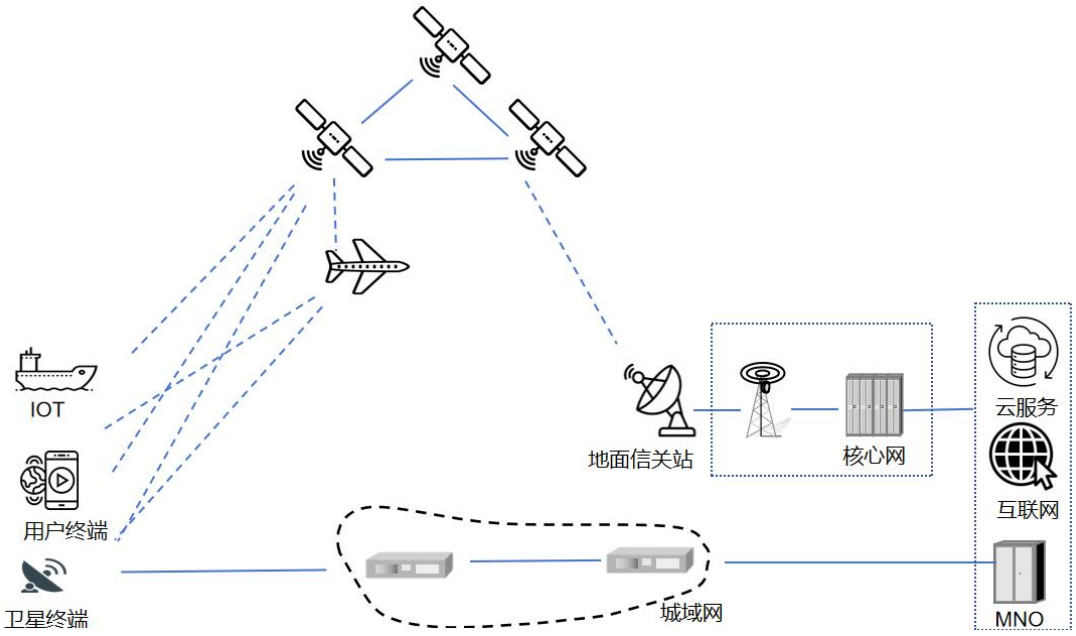


图 1　天地一体化融合网络

非地面网络（Non-Terrestrial Network，NTN）是由卫星通信网络与高空/空中平台网络共同构成的立体化通信体系，NTN 包括低地球轨道（LEO）、中地球轨道（MEO）和地球同步轨道（GEO）卫星、高空/空中平台网络包括飞行器（飞机、无人机），浮空器（气球、飞艇）等。

非地面网络作为地面移动通信系统的空间延伸，旨在实现空间、空中和地面三维协同的移动宽带覆盖。星地融合一体化网络能够实现“任何人，任何地点，任何时间”都可以通信的愿景。

基于 3GPP 标准的 5G NTN 是重要的星地融合通信技术。5G NTN 主要分透明转发及可再生两大模式。

在透明转发模式中，卫星作为中继器，提供信号中继转发功能。地面信关站完成星地信号转化功能。基站及核心网部署在地面，承载地面网已有业务及 5G 业务。

基于透明转发组网模式充分利用现有的卫星及地面网络资源，可以快速组网。

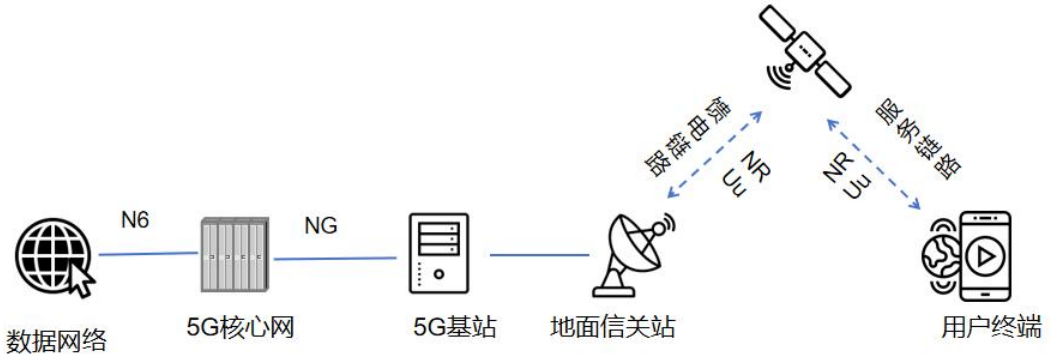


图 2　基于透明转发模式的 NTN 网络

在可再生模式中，卫星直接进行信号处理并承载基站或部分核心网功能（如 AMF、UPF），从而降低时延，提升实时业务处理能力及泛在连接能力。

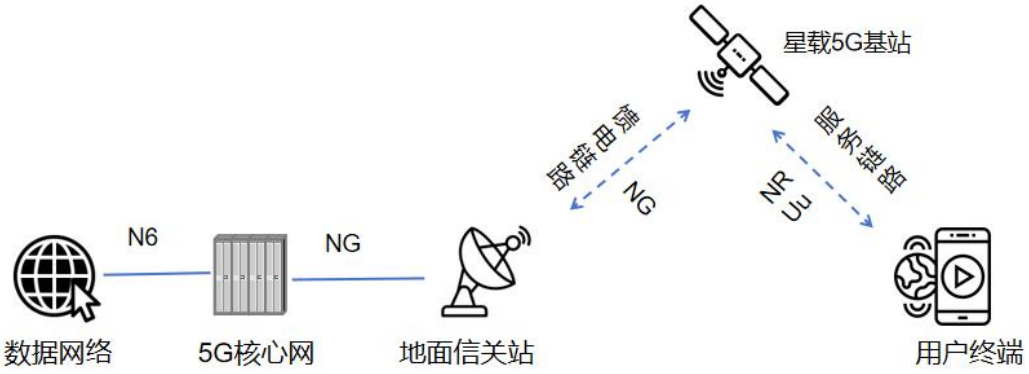


图 3　基于再生模式的 NTN 网络

在 3GPP Rel-17 和 Rel-18 版本标准中只支持透明转发模式，而规划中的 Rel-19 版本已开始支持再生模式，旨在提高星上处理能力和泛在连接能力[1]。

1.2 国内外标准化进展

1.2.1 国内标准化及研究进展

2023 年 1 月，中国电信完成了全球首次 S 频段 的 5G NTN 技术外场上星实测验证。

CCSA TC5 WG5 于 2024 年完成《面向 5G 网络及 5G 增强的天地一体化网络安全风险与安全能力需求研究》项目结题，该项目研究了基于 5G/5G-A 的天地一体网络典型安全风险及安全能力需求，推进对星地接入认证与隐私保护的关键技术、基站上星、核心网上星场景下存在的安全风险与安全需求的研究[2]。

中国移动在 2024 年发布了《面向 6G 的天地一体融合网络技术白皮书》，对天地一体融合组网的应用场景、目标、面临的挑战及创新技术进行了阐述[3]。

1.2.2 国际标准化进展

2019 年 ITU 组织在 NAT-SAT 项目中，提出了星地网络融合的四种应用场景。

ITU-TSG17 在 2024 年通过立项了首个星地融合安全标准的项目 X.5G_Sec-FMSC，研究固定、移动及卫星融合网络架构下安全需求与安全指南。

2025 年，ITU-TSG13 推动了《面向 IMT-2030 的固定、移动、卫星网络融合安全》国际标准/项目立项。

在标准方面，3GPP Rel-17 标准正式将非地面网络（NTN）技术纳入 5G 标准框架，为终端直连卫星通信提供了系统化技术规范。3GPP Rel-18 版本

对NTN覆盖增强、移动性增强、10GHz以上频谱支持、物联网增强、UE位置服务规范进行了改进。3GPP Rel-19 作为 5G-A 的关键版本，聚焦于网络性能优化与新场景适配能力提升，主要在基站上星、上行链路容量增强、下行覆盖增强、广播服务的服务区域通知能力、NTN+(e)RedCap 及引入IoT-NTN TDD模式等方面进行了增强。

2 关键问题及安全技术

2.1 关键问题

由于星地距离远，卫星移动速度快的特点，非地面网络存在高时延、星地路径损耗大及多普勒频移的问题。相比地面5G网络，5G NTN在高带宽、低时延，支持海量机器通信应用场景，面临许多挑战。

文献4提出了不连续覆盖场景下涉及的UE安全上下文存储的问题[4]。

文献5针对5G NTN提出了三个关键需求[5]：

1.支持再生式卫星接入。研究在 LEO/MEO 卫星上部署基站的可行性，支持卫星端信号再生处理，以降低传输时延并提升灵活性。

2.支持存储转发卫星操作。为非实时业务设计卫星“存储-转发”机制，适应卫星断连或不连续覆盖场景。

3.支持 UE-卫星-UE 直连通信，实现 UE 间通过卫星直接通信（无需地面核心网转发），支持 IMS 语音/视频、MCPTT（关键任务一键通）等业务。

为了上述需求及场景，需要在卫星端部署基站及部分核心网功能，并定义数据缓存、重传策略，同时对现有5G认证流程进行调整适配。

现阶段的5G NTN，在安全方面聚焦在以下方面：

1.不连续覆盖场景下，如何保持UE的安全上下文及为UE存储和/或转发的数据？

2.如何规避卫星快速移动导致大量UE频繁注册/注销带来的信令过载的风险?

3.在卫星存储转发操作下，认证流程将分为多个阶段进行，在这过程中如何保护UE的隐私不被泄露？

4.星载能力增强后带来的跨域攻击风险。当卫星被攻击者控制后，卫星可以被攻击者做为跳板来入侵地面其他5G核心网元，实现从接入域到核心域的攻击。

5.针对mMTC场景中海量连接需求与有限卫星资源的矛盾，需采用轻量级接入、轻量级加密算法及密钥管理、分布式认证等解决方案。

2.2 关键安全技术

1.移动性管理优化

（1）信令过载控制，为了避免大量的UE在离开范围或重入网时对网络造成过多的信令负载，AMF根据网络配置、接入优先级及优先级范围确定一个最大的时间偏移，用于在非连接覆盖情况下，作为UE与网络进行NAS信令交互的时间窗口。UE在最大时间偏移范围内随机访问网络，避免出现短时集中访问导致的资源竞争和信令过载的情况。

（2）支持分离功能的MME/AMF星载部署，提前缓存UE的安全上下文。卫星上部署MME/AMF部分功能，卫星在信关站的馈电链路正常时，星载

MME/AMF 提前向地面核心网获取 EPS/5GS 认证向量，并在服务链路不可用时存储 EPS/5GS 认证向量。当服务链路可用时，利用存储的认证向量完成后续的认证，从而缩短重新连接时的认证延迟，提升端到端安全连续性。

（3）针对频繁卫星切换场景，5G NTN 通过预测不可达周期，协调 AMF/MME 与 UE 的行为，优化信令流程。

UE 在初始注册或注册更新时上发节能参数。AMF 基于运营商策略和覆盖预测结果，对 UE 请求的参数进行修正，并通过注册接受（Registration Accept）消息下发最终参数，完成节能参数协商。

在预测的不可达周期内，UE 根据协商参数关闭射频模块进入低功耗状态，跳过无覆盖时段的寻呼监听与注册更新。AMF 基于覆盖预测结果暂停对 UE 的下行寻呼，避免无效信令开销，同时缓存待传数据直至覆盖恢复，从而减少因覆盖中断导致的重复认证及寻呼请求。

2.不连续覆盖场景下的认证增强

（1）增加 UE 与星载 MME/AMF 的认证。TR 33700-29 提出了多种用于 UE 和卫星的互认证方法[5]。在 UE 与核心网开始主认证流程之前，新增 UE 与卫星 MME/AMF 的认证流程，只有双方完成互认证后，UE 才会上报注册信息，同时星载 MME/AMF 才会缓存 UE 的安全上下文信息。新增的认证流程避免了卫星馈电链路中断时 UE 信息过量存储及 UE 等待时间过长引发的拒绝服务攻击。

（2）卫星本地化 AUSF/UDM 功能，通过星载分布式认证机制减少 UE 与核心网的交互次数，解决不连续覆盖场景下的鉴权延迟问题。

3.通过临时UID实现UE身份信息的匿名化

在不连续覆盖场景下，网络在异常流程会明文传输GUTI，而长期有效的GUTI可能会导致UE被跟踪。TR 33700-29提出了临时UID的方案，在方案中UE建立NAS安全之前生成临时UID。核心网基于临时UID为UE分配一次性临时GUTI，这个临时GUTI以明文形式发送并多次重复使用。UE收到临时GUTI后，基于临时UID信息进行比对，验证成功后才开始NAS认证流程。这样避免了信息泄露的风险。

4.再生组网模式的跨域攻击风险防护

随着星载能力不断增强，5G NTN下核心网动态化及开放化发展的趋势。核心网的功能由地面和卫星共同承载。开放部署及防护能力有限的卫星如果被入侵，N3/N4/N9接口将成为新的攻击面，这将对核心网造成很大的威胁。需要研究5G核心网元可信启动、零信任及内嵌异常监测机制，构建跨域协同防护及微隔离机制，实现安全策略联合生成与自适应快速重构，以快速阻断跨域攻击的风险。

5.面向mMTC场景的安全技术

针对物联网海量连接需求，5G-A通过RedCap/eRedCap技术优化了信令流程。未来通过轻量级密钥管理与轻量级密码算法（如ASCON）的结合，有望能降低终端计算开销，适配无源物联网等低功耗场景。

在NTN方面，通过星间高速互联，巨型星座组网，实现算力及安全能力分布式调度也是解决海量连接需求的关键。

结语

5G NTN是面向卫星通信和低空通信场景的5G演进技术，具有广阔应用前景。为满足场景拓展需求并保持技术兼容性，当前5G NTN网络安全机制基于地面5G安全框架进行了增强，仍面临许多挑战。未来6G具有全域覆盖、极致性能与泛在连接的发展目标，基于开放架构的6G将完全实现地面网络与非地面网络的有机融合，6G安全将向内生安全，分布式认证部署与智能化的方向协同演进。（王启泽 北京启明星辰信息安全技术有限公司）

参考文献：

[1]Joern Krause. Non-Terrestrial Networks (NTN), https://www.3gpp.org/technologies/ntn-overview,2024-03-14

[2] IMT-2020(5G)推进组.《5G-A安全关键技术及标准化进展》,2024-12.

[3]中国移动.《面向6G的天地一体融合网络技术白皮书》.

https://mp.weixin.qq.com/s/UNKrCDE1h6Ael7zx_0dJBA.

[4] xiaoming. "Security for Satellite Access and NTN".

https://www.3gpp.org/ftp/Email_Discussions/SA3/TSG3_Rel18/Discussion%20on%20Security%20Aspects%20for%20Satellite%20Access%20and%20NTN.pdf.

[5] 3GPP. TR 23.700-29: "Study on integration of satellite components in the 5G archite cture; Phase 3".

3.大模型安全行业影响分析及企业安全规划思路

大模型作为新兴起的IT应用技术，受技术发展前景、政策鼓励多方因素推动，得到广泛的应用与推广。安全行业作为信息技术领域的专业子行业，大模型不但作为底层创新能力，成为驱动产品架构革新和服务升级的重要技术；同时也因其极强的智能生成与推理能力，获得监管机构乃至黑色产业的重点关注，加剧了安全与发展的对立统一关系，也使得保障大模型安全成为实现产业应用健康发展必须关注的问题。了解大模型安全对产业多方的影响，进而科学规划大模型安全，是企业机构确保大模型技术稳步推进的可行路径。

鉴于大模型作为一项基本技术，其不能类似等级保护以系统为单位进行管理，也不宜类似ISMS以机构为单位单独进行顶层规划。但组织机构针对大模型应用，依然可以从顶层参考GRC（治理、风险、合规）框架，基于当前市场的现状，首先聚焦大模型合规，后期伴随业务发展，同步不断充实治理、风险场景用例与细节粒度。其次，再从系统层面，对于应用了大模型技术的系统，可以参照等级保护管理、技术的二维逻辑进行规划，尤其是重点关注大模型技术安全的特殊性，加以设计。所以本文基于如上逻辑，结合市场与技术现状，分别对大模型安全的合规规划与技术规划展开阐述。

一、大模型安全行业影响

大模型安全对行业的影响，可以从三类主体展开分析。按照行业供需关系，分为大模型安全供给方、大模型安全需求方以及特殊第三方，如图1

所示。大模型安全供给方以安全行业厂商为代表，是提供大模型安全技术、产品、服务的关键主体；大模型安全需求方以各应用行业机构为代表，依据场景划分为独立部署大模型、外联商业大模型两类群体；特殊第三方主要考虑了黑色产业，也是针对大模型防护过程中必须考虑的主体。

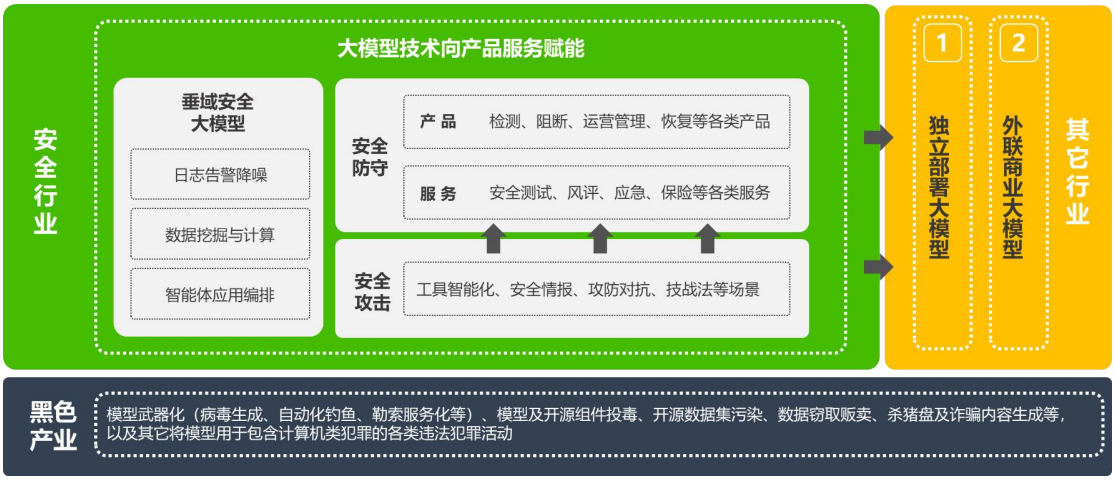


图 1 大模型安全三方模型

针对大模型安全供给方，大模型技术从三个方面带来影响。首先，大模型技术于安全行业进行二次应用，经过训练、微调，实现垂域安全大模型孵化。垂域大模型的场景能够应用于日志告警降噪、数据挖掘与计算、智能体应用编排，伴随相关技术的不断进步，安全数据质量的不断提升，该技术对安全智能运营产生大的影响；其次，安全攻击作为带动安全防守升级的基础，攻击类工具不断向智能化发展，关联安全情报、攻防对抗、技战法涉及的流程及平台化技术也对应提升；最后，安全防守作为向其它行业输出的接口，既要融合大模型技术实现功效提升，也要以大模型为保护标的进行对应能力转化，其涉及检测、阻断、运营管理、恢复等各类安全产品，以及测试、风评、应急、保险等各类安全服务。

大模型安全需求方，是大模型安全市场组织机构数量最为庞大的主体，也是大模型技术场景化应用不断丰富的核心源泉。因行业监管要求以及大模型应用成熟度各不相同，本文未按照行业类型进行划分，而是划分为两类应用场景。两类场景分别为独立部署大模型场景，即企业组织机构自行部署大模型，能够控制模型的训练、部署、应用的部分或全部阶段；以及外联商业大模型场景，指企业组织机构通过互联网访问开放的商业模型，对模型不具有控制权。独立部署大模型因赋予组织机构更大的自由度，对于孵化本行业垂域模型、研发特色应用、探索高价值场景提供了更多机会，也是传统行业数字化转型的亮点应用领域。该场景也面临更大风险，需要更细致的安全责任划分和防护策略，也是大模型应用进行商业化的前提；外联商业模型，主要从风险管理原则与实践需要出发，更符合企业组织机构急迫需要外联商业模型并提升自身业务能力、处理效率的背景。该场景一般由安全部门进行总体设计，并区分 API 外联、WEB 外联两类调用模式，尽速部署安全策略，防止组织内部商业敏感数据、个人信息乃至涉密数据的外发上传。

大模型安全特殊第三方，主要考虑了黑色产业，源于安全行业本身对抗的特殊属性，其既是安全厂商产品技术不断升级迭代的驱动力，也是限制制约大模型技术应用的一大关键。黑色产业利用大模型优秀的推理、生成能力，一方面不断进行模型武器化和攻击手段智能体化，以实现病毒生成、钓鱼、勒索等任务的智能化与自动化；另一方面，黑色产业利用大模型产业的开源生态，通过对模型及开源组件、开源数据集进行投毒和污染，

以进一步诱导或渗透。除计算机类犯罪，黑色产业利用大模型进行杀猪盘设计与诈骗内容生成，辅助数据窃取贩卖等违法犯罪活动，也是需要关注的内容。

二、大模型安全合规规划

大模型安全规划从两个方面展开，首先为合规规划，其次是技术规划。组织机构对外提供大模型服务，相关安全合规规划必须加以重视，且一般于项目可行性研究阶段就加以考虑。该规划一般由业务部门牵头，联合组织机构法律团队、风控团队、安全团队共同完成。以国内大模型合规为例，对大模型应用法律法规及规范标准梳理过程中，可从两个方向开展。纵向可以从法律法规效力层级逐层分析，以保证全面覆盖相关要求；横向关注区域、行业性要求，如图 2 所示。

纵向法律及行政法规层面，当前还未发布直接以人工智能、大模型应用为主题的相关文件，但存在涉及生成式人工智能数据安全的条款。该方向以规范性文件、标准及技术文件内容较多，而且伴随时间推移，围绕大模型主题的内容会持续充实细化，所以组织机构需要持续跟进。横向有关区域、行业性规范，当前针对人工智能及大模型技术，均以鼓励发展类文件为主，关系到企业组织机构申报政府奖励、补贴、奖项等工作。

组织机构涉及境外业务的，国内除履行大模型合规备案手续，还需要单独针对数据、个人信息出境进行合规评估或备案。同时，于服务使用国（国外），单独评估相关业务于该国是否存在人工智能与大模型相关的专

门法规，并可能涉及向未成年人提供服务、开源接入知识产权、金融与医疗数据等，特殊人群、行业与场景的专门合规评估与规划。

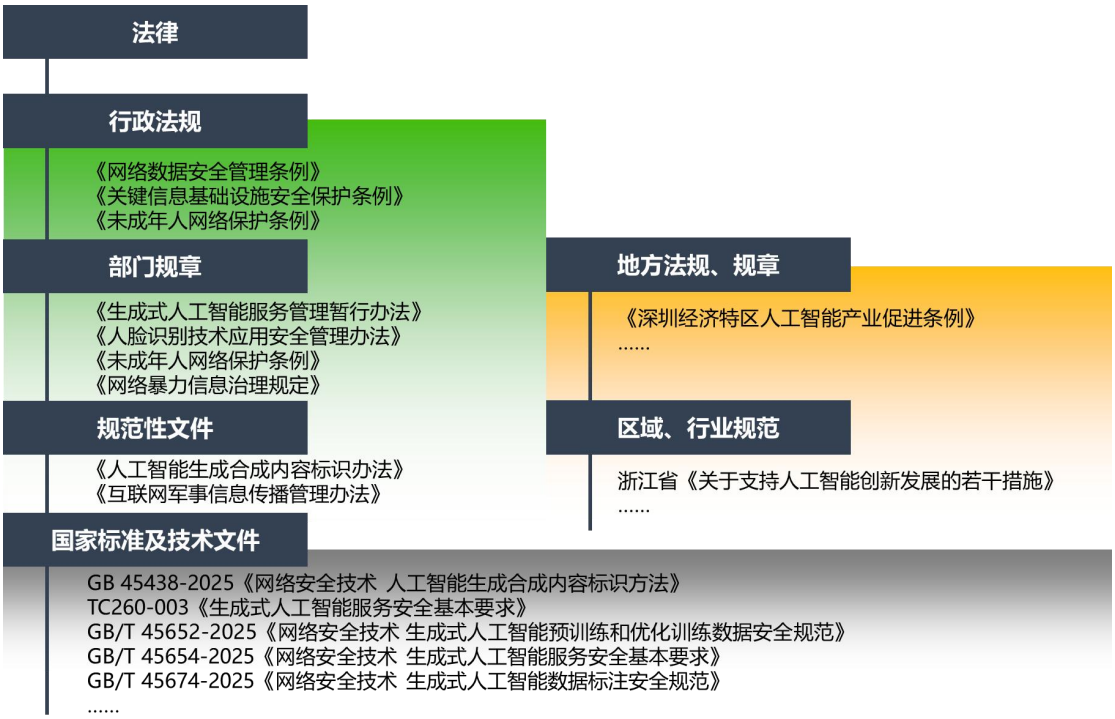


图 2 大模型安全合规框架

三、大模型安全技术规划

大模型安全技术规划一般由安全或 IT 团队主导，需要与大模型业务遵循安全技术措施同步规划、同步建设、同步使用原则，同时可基于模型安全功能实践，分阶段实现内容安全护栏、Prompt 工程、模型微调、模型训练、数据安全，如图 3 所示。之所以分阶段实现，首先考虑了当前大模型应用场景异常活跃、监管要求持续细化，需要通过技术手段实现内容安全合规，其次再考虑模型应用自身及应用环境安全要求。内容安全包含了模型输入、输出两个方面，尤其需要重点考虑输出内容的合规审计；其次，五阶段规划考虑了大模型技术以及相关安全技术的发展成熟度，同时兼顾工程成本和实现难度，所以从内容安全护栏开始，分阶段实现大模型安全

工程化落地也更满足实践现状。伴随未来大模型及大模型安全技术不断发展成熟，五阶段安全规划可以平滑转换为大模型纵深防御架构，采取从中心到边缘的总体设计。

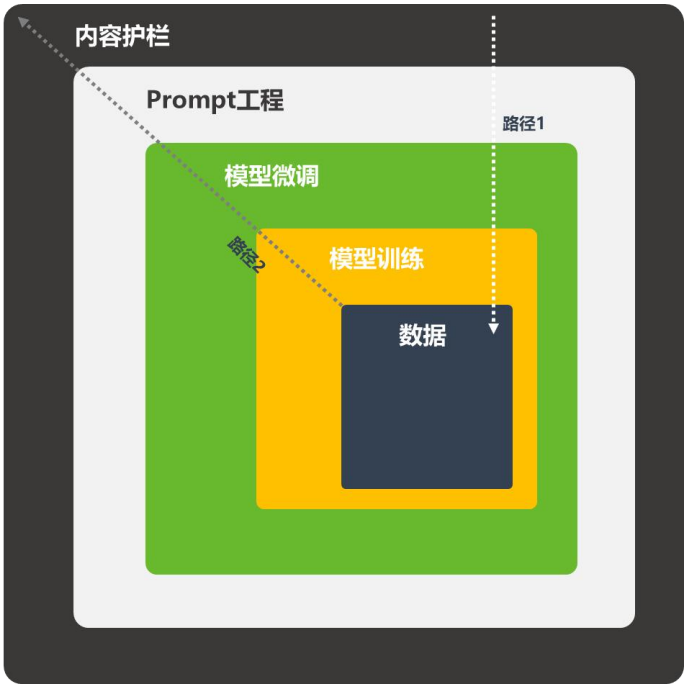


图 3 大模型安全技术规划路径

安全技术措施实现上，内容护栏主要为验证检查和过滤功能。在最终用户输入和大模型输出上执行所需安全检测、阻断控制措施。内容安全护栏充当用户和模型之间的代理和中介角色，使大模型能够专注于内容生成，而安全护栏则使应用程序安全、合规、可靠。

Prompt 工程是通过创建 Prompt 模板、检测并调整 Prompt，进而控制最终用户输入、输出的角色，控制相关角色的权限，以及控制数据类型、Token 长度等内容，Prompt 模板提供了预定义安全控制的能力。

模型微调是指基于既有安全需求，单独对模型执行额外微调，以保证模型在其指定应用领域、情景下按预期工作，尤其是满足国家、行业监管机构对于模型输出的要求。同时，也可基于业务场景、角色，进行微调。

模型训练从更早阶段，明确定义模型领域、角色、语气、场景，以针对性训练。如以网络安全领域为例，可以训练垂域模型，并且可进一步划分为攻击类场景和防守类场景，攻击场景大模型需以更严格的安全使用要求进行设计，防止模型滥用。以防守场景大模型为例，如设定“你是一个安全防守工程师，只回答防护建议，不回答攻击手段，基于你知道的回答，不确定的以及不知道拒绝回答”。

若进一步溯及大模型安全上游，必须对训练数据、微调数据进行安全设计，其涉及数据清洗、标注、脱敏、匿名化等工作，在分析模型的使用业务场景需求的前提下，定义数据范围、所有权、权限，涉及公开的需要预先评估数据风险，涉及商业推荐的，还需联合业务场景进行防歧视等算法合规层面的落实。（张睿 绿盟科技集团资深总师）

4. 浅析网络安全风险量化评估模型 FAIR

摘要：在全球数字经济加速发展的背景下，网络安全风险已成为企业数字化转型的核心挑战。当前企业数字化建设与业务运营加速融合，网络安全风险管理已从传统的技术保障层面跃升为企业风险管理框架的战略性支柱。如何提升网络安全风险的精益化管理能力，对网络安全风险进行可量化的分析，以支持企业在风险管理的过程中进行更严格和广泛的决策，成为业内关注的热点问题。信息风险因子分析（FAIR, Factor Analysis of

Information Risk）模型为上述问题的解决提供了有意的参考。本文将从概念、建模方法等方面对FAIR模型进行解读分析。

关键词:网络安全、风险评估、量化分析、FAIR模型、风险管理

一、引言

网络安全风险天然具备不确定性的特征，其不确定性的程度依赖于信息的可获得性。对风险进行度量的目标应通过构建清晰的场景假设、选择合理的模型、更好地利用所拥有的数据，将风险评估的不确定性降低到有用且合理的水平，进而为决策分析提供有益参考。

有效的网络安全风险管理依赖于严格的风险度量。网络安全风险量化技术在企业风险管理中有着广泛的应用：通过网络安全风险量化分析确定风险处置优先级，最大限度降低网络安全风险、评估网络安全技术和服务的投资回报率以优化网络安全投入、帮助客户充分了解和管理网络安全风险及其潜在的财务损失以保持业务价值、优化网络安全保险投资组合策略等方面的均具备实用的指导价值。2018年Gartner在其首个集成风险管理象限(Integrated Risk Management Magic Quadrant)中，就将风险量化技术列为集成风险管理解决方案的关键能力之一。

FAIR模型通过识别和定义构成风险的因子及其关系来分析风险，风险因子或因子之间的关系可以用数学方法进行表达，并将网络安全风险的影响转化为财务术语，以帮助决策者更好的理解、分析和度量网络安全风险，使企业组织在非网络世界中进行常规业务规划提供了一种可行的路径。

二、FAIR风险分析框架及核心概念

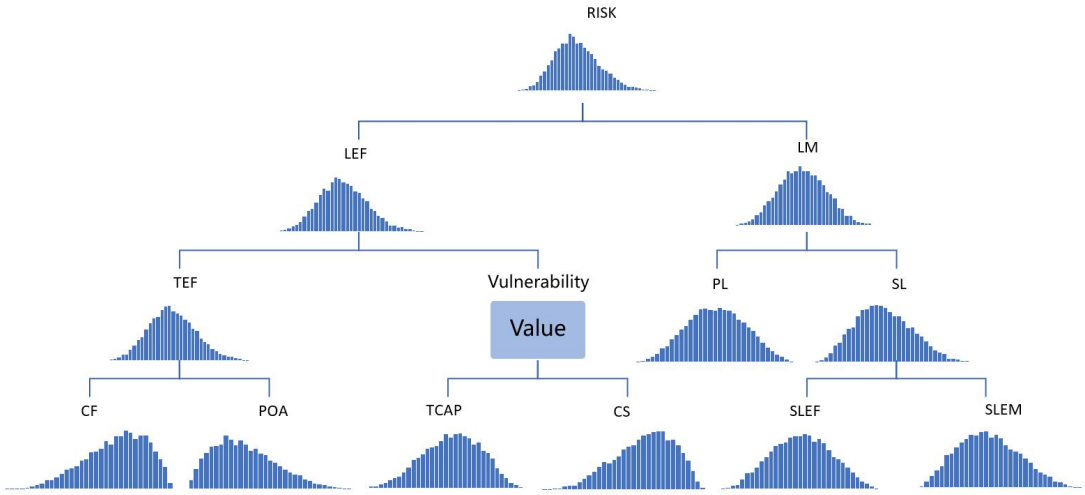


Figure 1 FAIR 模型风险因子关系图

为帮助用户理解使用该框架，The Open Group 发布了两个关于 FAIR 的标准：开放风险分类技术标准（Open Risk Taxonomy Technical Standard, O-RT）以及开放风险分析技术标准（Open Risk Analysis Technical Standard, O-RA），前者规范了 FAIR 风险分析中使用的术语、定义和关系，后者对有效进行风险分析相关的流程进行了描述。结合 FAIR 因子的定义，对 FAIR 因子及关系描述如下：

风险（RISK）：未来一段时间内，损失事件可能发生的频率与损失幅度。在该定义中，FAIR 特别强调时间的概念，也即在对风险因子进行估计时，首先要确定对评估的时间段，通常在业务操作中选择对未来一年内的风险进行分析。

威胁（Threat）和威胁代理(Threat Agent)：在 FAIR 的标准术语中，严格区分了威胁和威胁代理的概念。简而言之，威胁代理是指从事对资产、系统或网络构成潜在风险行为的实体或个人。这些威胁代理可以是人类，如黑客或内部人员，也可以是非人类，如恶意软件或病毒。另一方面，威

胁是指可能对资产、系统或网络造成损害的行为。威胁代理是负责实施这些威胁的具体实体。在后续的场景分析中，可以对威胁代理实体的能力、意图、规模等进分析，也可以对威胁行为进行明确的分类。

损失事件频率(LEF，Loss Event Frequency)：在给定的时间段内，威胁代理对资产产生实际损失的可能频率。LEF 通常是年度损失事件发生的频率，如 Max(LEF)=0.5，Min(LEF=0.1)，代表损失事件最多 2 年发生一次，至少 10 年发生一次。在进行风险估计时，对 LEF 的相关数值可直接给出，也可由威胁事件发生的频率以及威胁事件转化为损失事件的概率计算得出。在 FAIR 标准术语定义中，定义了三类事件：接触事件、威胁事件和损失事件。举例而言，黑客登录网站查询信息是接触事件，一旦黑客对该网站采取攻击行为，即演变为威胁事件，若破坏了网站或窃取了数据，即转化为损失事件。

威胁事件频率（TEF，Threat Event Frequency）：在给定的时间段内，威胁代理对资产采取攻击行为的频率。TEF 可直接估计得出，也可由接触频率因子和行动概率因子计算得出。

脆弱性概率（V，Vulnerability）：威胁事件转化为损失事件的概率，也表示威胁能力大于防御强度的概率。在进行风险估算时，脆弱性概率可直接进行估计，也可由威胁源能力以及抵抗强度因子进行计算得出。需要注意的是，在 FAIR 模型中脆弱性概率 V 是一个数值表达，需要与常规语境中的漏洞、脆弱性等术语加以区分。

接触频率（CF，Contact Frequency）：在给定的事件段内，威胁代理与资产接触的可能频率。

行动概率（POA， Probability of Action）：一旦接触发生，威胁代理对资产采取行动的概率。

威胁能力（TCAP，Threat Capability）：威胁代理的能力水平。其数值范围为[0,1]，通常用百分比表示。

防御强度（RS，Resistance Strength）：可抵御威胁的水平。与威胁能力对应，其数值范围为[0,1]，通常用百分比表示。

损失幅度（LM，Loss Magnitude）：一次损失事件可能导致的损失范围。如一次损失事件导致的损失范围在10万-20万之间。损失幅度由主要损失（PL，Primary Loss）和间接损失（SL，Secondary Loss）构成。间接损失可由间接损失事件发生的频率（SLEF，Secondary loss event frequency）以及间接损失发生的幅度(SLM，Secondary loss magnitude)计算得出。常见的主要损失类型包括生产力成本、替换成本、响应成本等，常见的间接损失包括声誉损失、罚款等。损失事件一旦形成一定包含主要损失，但是否会产生间接损失则是概率性事件。如发生网络勒索类事件，导致制造生产线宕机，会带来生产力下降的直接损失，但未必会导致声誉损失。因此，间接损失由间接损失发生的频率以及间接损失的幅度构成。

上述的风险因子及其关系构成了FAIR风险分析的主要框架。

三、FAIR建模与分析

（一）FAIR建模分析的主要流程

使用 FAIR 进行建模和分析，主要步骤包括定义风险场景、进行风险因子的选择、对选择的风险因子进行估计、对风险因子通过 PERT 函数进行模拟、根据因子关系进行蒙特卡洛模拟，最终得出风险结论及分析结果。

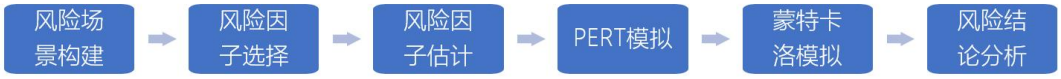


Figure 2 FAIR 风险分析主要的流程

（二）FAIR 分析概要计算过程

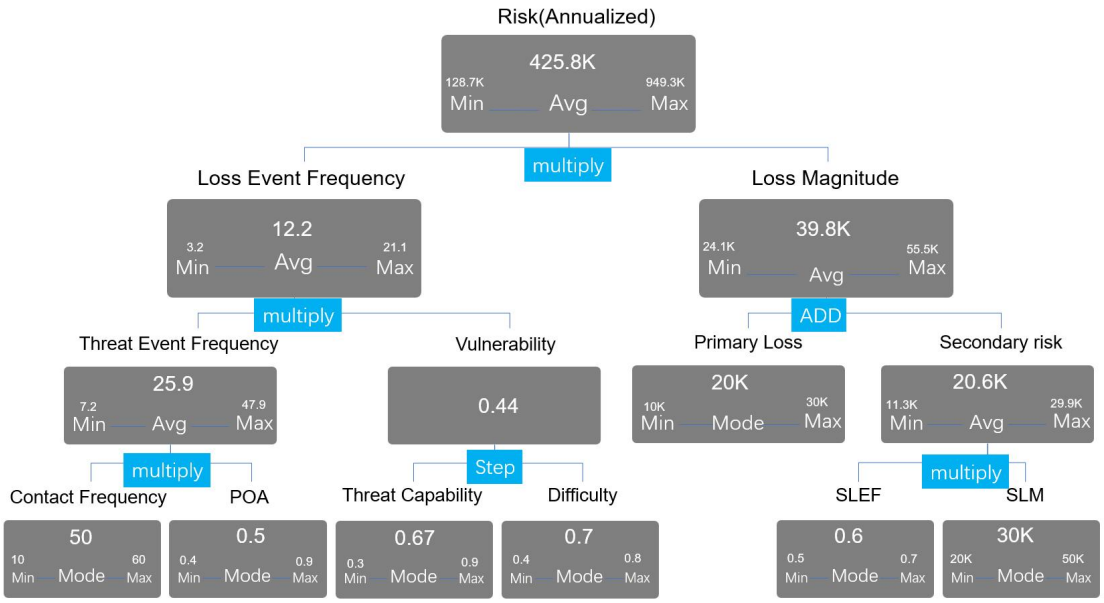


Figure 3 FAIR 总体计算过程

使用 FAIR 进行风险分析的过程，首要的任务是明确风险评估的场景，对场景中的威胁源、攻击方法、资产、事件影响等进行分析，为风险因子的估计提供分析输入。

在使用 FAIR 进行风险分析的过程中，有一个非常核心的理念，即风险是不确定性的，很难使用单个确定的数值对风险中的因子进行估算。如让我们估算勒索事件的损失：假如发生此类事件，恰好花费 40 万元的说法并

不准确。而表达为“未来发生一次勒索事件，其损失幅度可能在 20 万到 70 万之间，最有可能是 40 万左右”更为客观、准确，也为评估分析者提供了合理的评估准则。在 FAIR 框架中，对风险因子的数值估计，通常由 4 个核心数值构成：最大值、最小值、最有可能值、以及对最有可能值的信心程度决定，以帮助评估者更好的表达对风险的认知。比如对一次损失事件发生的损失幅度进行估计，可估计为最小损失 20 万，最大损失 60 万，最有可能损失 40 万，信心程度为高。

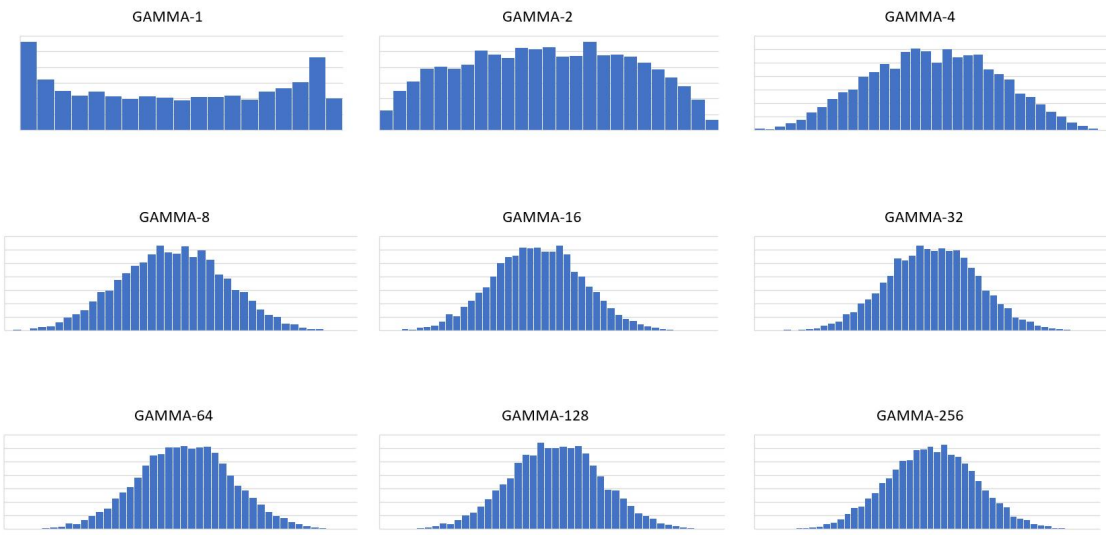


Figure 4 信心程度变量对风险因子拟合的影响

FAIR将根据上述四个数值采用PERT 算法进行单个风险因子的数值模拟，并根据因子之间的关系采用蒙特卡洛模拟算法得到风险分析结论。图 3 为选择风险因子到第四层的整体初始值估计过程示例，在实际应用过程中用户可根据实际场景，选择合适的因子和层级进行评估。图 1 显示了整个计算过程的模拟结论。图 4 反映了对最有可能数值估计的信心程度对该风险

因子拟合的影响，通过图 4 说明对最有可能值估计的信心程度越高，在对该风险因子进行 PERT 模拟时，分布向最有可能值集中。

（三）FAIR 分析结论的解读及应用

Figure 5 年度风险敞口损失超越曲线

完成风险计算后，可得到图 5 年度风险敞口损失超越曲线，X 轴代表年度风险敞口，Y 轴代表概率，曲线上的点表示该场景下年度风险敞口超过特定损失数值 X 的概率为 Y。如图 5 的红色标记处，根据风险计算的结论显示，未来一年内，损失超过 4000000 元的概率为 7%。

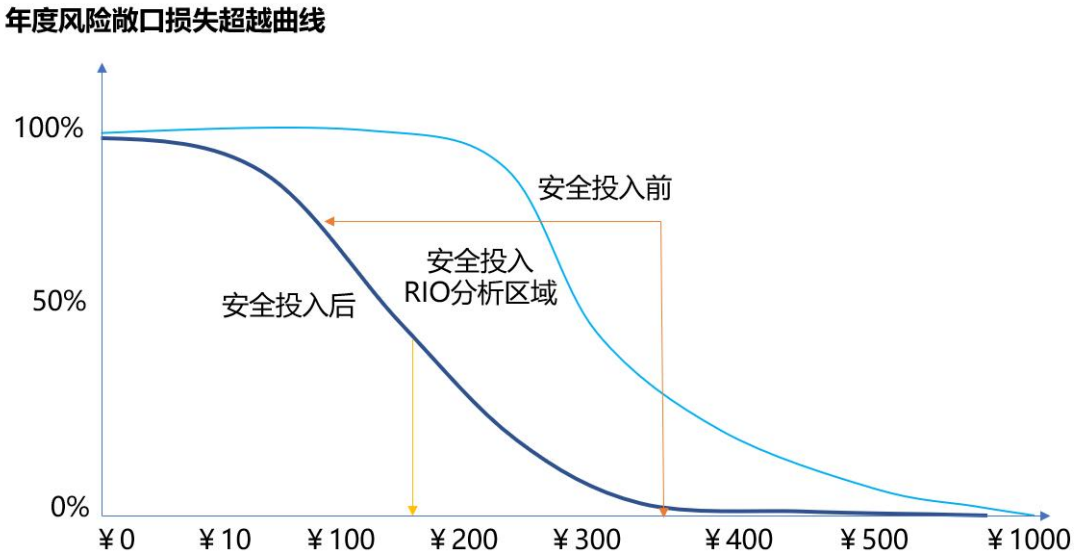


Figure 6 使用FAIR分析结论进行安全投入分析应用示意图

用户通过FAIR分析，将安全语境和财务语境的风险度量使用货币化表达方式进行了统一，使网络风险的影响转化为财务术语，支持企业在非网络世界中进行的常规业务规划成为可能。用户可根据FAIR输出的结论，根据自身企业经营情况，对网络安全风险承受水平进行分析、开展风险自留及风险转移（如通过购买网络安全保险等方式）策略的分析、安全投入产出的绩效分析（如图6所示）等应用场景的支持。

四、总结与展望

对网络安全风险进行量化评估是企业进行精益化风险管理的重要依据。FAIR模型为网络安全风险量化评估提供了具有启发性的思路和方法，可帮助决策者从财务视角理解、分析和度量网络安全风险。在利用FAIR进行场景化网络安全风险量化分析的过程中，分析者需要重点构建风险分析的场景，结合风险量化分析的目标，充分利用现有的数据，作出合理的分析结论，这对网络安全量化分析者提出了较高的技能要求，也是FAIR在场景化应用落地中需要重点关注和研讨的问题。（作者：赵远杰 北京源堡科技有限公司高级工程师）

行业前沿观察二：国家网信办开展人脸识别技术应用备案工作；《智能社会发展与治理标准化指引（2025版）》印发；《网信部门行政处罚裁量权基准适用规定（征求意见稿）》公开征求意见

导读：近日，国家网信办发布关于开展人脸识别技术应用备案工作的公告，自2025年6月1日起，应用人脸识别技术处理的人脸信息存储数量达到10万人的，应当自数量达到之日起30个工作日内履行备案手续。2025年6月1日前，应用人脸识别技术处理的人脸信息存储数量已经达到10万人的，应当在2025年7月14日前履行备案手续。

为进一步规范网信部门行政处罚行为，保护公民、法人和其他组织的合法权益，国家互联网信息办公室研究起草了《网信部门行政处罚裁量权基准适用规定（征求意见稿）》，向社会公开征求意见。

为贯彻落实中共中央、国务院《关于加快建设全国统一大市场的意见》和《国家标准化发展纲要》，准确把握社会智能化转型趋势，发挥标准化的基础性、引领性作用，深化智能社会发展与治理，中央网信办秘书局、市场监管总局办公厅近期联合印发《智能社会发展与治理标准化指引（2025版）》。

关键词：互联网、人脸识别、网络安全、网信办、标准化

1. 中央网信办秘书局、市场监管总局办公厅联合印发《智能社会发展与治理标准化指引（2025 版）》

为贯彻落实中共中央、国务院《关于加快建设全国统一大市场的意见》和《国家标准化发展纲要》，准确把握社会智能化转型趋势，发挥标准化的基础性、引领性作用，深化智能社会发展与治理，中央网信办秘书局、市场监管总局办公厅近期联合印发《智能社会发展与治理标准化指引（2025版）》（以下简称《指引》）。

《指引》旨在建立健全科学合理的智能社会发展与治理标准研究制定、实施反馈、优化完善的工作机制，建成覆盖智能技术主要社会应用场景、有效保障技术全生命周期良性健康发展的标准体系，从而适应技术创新需要、满足产业发展需求、支撑智能社会建设，助力国家治理体系和治理能力现代化。

《指引》提出了智能社会发展与治理的基本原则和要求，明确了常见智能技术应用场景、社会影响及其观测评估指标，规定了人工智能社会实验的一般程序和要求，构建了包括基础通用、发展与治理原则、场景应用、技术和方法、效果评价等五部分内容的智能社会发展与治理标准体系，为各地方、各部门、科研院所、企事业单位等开展智能社会发展与治理理论研究和实践活动提供技术支撑和规范指引。

2. 关于公开征求《网信部门行政处罚裁量权基准适用规定（征求意见稿）》意见的通知

为进一步规范网信部门行政处罚行为，保护公民、法人和其他组织的合法权益，国家互联网信息办公室研究起草了《网信部门行政处罚裁量权基准适用规定（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式反馈意见：

1. 通过电子邮件将意见发送至：law@cac.gov.cn。

2. 通过信函将意见寄至：北京市西城区车公庄大街11号（邮编：100044）。请在信封上注明“《网信部门行政处罚裁量权基准适用规定（征求意见稿）》意见反馈”。

意见反馈截止时间为2025年6月14日。

附件：网信部门行政处罚裁量权基准适用规定（征求意见稿）

国家互联网信息办公室

2025年5月30日

网信部门行政处罚裁量权基准适用规定

（征求意见稿）

第一条 为了规范网信部门行政处罚行为，保护公民、法人和其他组织的合法权益，根据《中华人民共和国行政处罚法》、《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》、《网信部门行政执法程序规定》等法律、法规、规章和国家有关规定，结合网信工作实际，制定本规定。

第二条 网信部门依据行政处罚裁量权基准行使行政处罚裁量权，适用本规定。法律、法规、规章另有规定的，从其规定。

第三条 本规定所称行政处罚裁量权基准，是指网信部门在实施行政处罚时，按照裁量涉及的违法行为的事实、性质、情节、社会危害程度、当事人主观过错等因素，对法律、法规、规章中的原则性规定或者具有一定弹性的执法权限、裁量幅度等内容进行细化量化而形成的具体执法尺度和标准。

第四条 网信部门适用行政处罚裁量权基准，应当遵循法制统一、公平公正、过罚相当、宽严相济、处罚与教育相结合等原则。

第五条 网信部门行政处罚裁量权基准划分为不予处罚、减轻处罚、从轻处罚、一般处罚、从重处罚等裁量阶次。

不予处罚是指因法定原因对实施违法行为本应给予行政处罚的当事人不再给予行政处罚。

减轻处罚是指减少并处法律、法规、规章规定的行政处罚种类或者低于最低限度的处罚幅度，对当事人实施行政处罚。

从轻处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用较轻、较少的种类或者较低的幅度，对当事人实施行政处罚。

一般处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用适中的种类或者幅度，对当事人实施行政处罚。

从重处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用较重、较多的种类或者较高的幅度，对当事人实施行政处罚。

第六条 有下列情形之一的，应当不予处罚：

（一）违法行为轻微并及时改正，没有造成危害后果的；

（二）当事人有证据足以证明没有主观过错的，法律、法规另有规定的，从其规定；

（三）法律、法规规定的其他情形。

初次违法且危害后果轻微并及时改正的，可以不予处罚。

依法不予处罚的，网信部门可以根据情节采取相应的行政监管措施，并应当对当事人进行教育。

第七条 有下列情形之一的，应当从轻或者减轻处罚：

（一）主动消除或者减轻违法行为危害后果的；

（二）受他人胁迫或者诱骗实施违法行为的；

（三）主动供述网信部门尚未掌握的违法行为的；

（四）配合网信部门查处违法行为有立功表现的；

（五）法律、法规、规章规定的其他情形。

第八条 有下列情形之一的，应当从重处罚：

（一）违法行为严重危害网络信息内容安全、网络运行安全、网络数据安全的，违法处理个人信息或者处理个人信息未履行个人信息保护义务情节严重的；

（二）因同种违法行为一年内受到网信部门两次以上行政处罚的；

（三）教唆、胁迫、诱骗他人实施违法行为的；

（四）拒不配合、阻碍、以暴力威胁网信部门执法人员依法执行公务的；

（五）隐匿、毁损、伪造、篡改有关证据的；

（六）对证人、举报人、网信部门工作人员进行打击报复的；

（七）违法行为引起群众强烈反映，引发群体性事件或者造成其他不良社会影响的；

（八）违反未成年人保护相关规定情节严重的；

（九）性质恶劣、情节严重、社会危害性较大的其他情形。

第九条 违法行为不具有不予处罚、减轻处罚、从轻处罚或者从重处罚情形的，应当给予一般处罚，法律、法规、规章另有规定的除外。

第十条 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。

第十一条 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、情节和本地区经济社会发展状况等因素，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。

第十二条 依法单独处警告、通报批评、没收违法所得的，仅适用不予处罚、一般处罚两种裁量阶次。

第十三条 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。

第十四条 网信部门适用行政处罚裁量权基准，判断违法行为性质、情节以及社会危害程度等，应当综合考量以下因素：

（一）违法行为的具体方法或者手段，当事人实施违法行为的主观过错程度；

（二）违法行为的持续时间、发生次数，违法行为造成的社会影响、危害后果；

（三）违法行为的危害对象及其数量；

（四）当事人本年度内的处罚情况；

（五）当事人获取的违法所得；

（六）当事人的生产经营类型规模、经营情况及其影响力；

（七）当事人改正违法行为的主观态度、配合检查的情况、所采取的整改措施及效果；

（八）法律、法规、规章规定的其他因素。

第十五条 对当事人的同一个违法行为，不得给予两次以上罚款的行政处罚。同一个违法行为违反多个法律规范应当给予罚款处罚的，按照罚款数额高的规定处罚。有两个以上应当给予行政处罚违法行为的，应当分别裁量，合并处罚。

第十六条 市（地、州）级以上网信部门可以结合工作实际制定本行政区域内的行政处罚裁量权基准。对同一行政执法事项，上级网信部门已经制定行政处罚裁量权基准的，下级网信部门原则上应当直接适用；如下级网信部门不能直接适用，可以结合本地区经济社会发展状况，在法律、法规、规章规定的行政处罚裁量权范围内进行合理细化量化，但不能超出上级网信部门划定的阶次或者幅度。下级网信部门制定的行政处罚裁量权基准与上级网信部门制定的行政处罚裁量权基准冲突的，应当适用上级网信部门制定的行政处罚裁量权基准。

第十七条 网信部门作出行政处罚决定前，应当告知当事人拟作出的行政处罚的内容及事实、理由、依据，并在行政处罚决定书中对行政裁量权基准的适用情况予以明确。

第十八条 网信部门实施行政处罚，适用本部门制定的行政处罚裁量权基准可能出现明显不当、显失公平，或者行政处罚裁量权基准适用的客观

情况发生变化的，经本部门主要负责人批准或者集体讨论通过后可以调整适用，批准材料或者集体讨论记录应当列入处罚案卷归档保存。

适用上级网信部门制定的行政处罚裁量权基准可能出现前款情形的，报请上级网信部门批准后，可以调整适用。

第十九条 上级网信部门应当通过行政执法情况检查、行政执法案卷评查等方式，对下级网信部门行使行政处罚裁量权工作进行监督。

因不规范适用行政处罚裁量权基准造成严重后果的，应当依规依纪依法严格追究有关人员责任。

第二十条 本规定自 年 月 日起施行。

3. 国家网信办：开展人脸识别技术应用备案工作

国家网信办发布关于开展人脸识别技术应用备案工作的公告，自2025年6月1日起,应用人脸识别技术处理的人脸信息存储数量达到10万人的，应当自数量达到之日起30个工作日内履行备案手续。2025年6月1日前，应用人脸识别技术处理的人脸信息存储数量已经达到10万人的，应当在2025年7月14日前履行备案手续。全文如下：

根据《人脸识别技术应用安全管理办法》（国家互联网信息办公室、中华人民共和国公安部令第19号，以下简称《办法》）规定，现就开展人脸识别技术应用备案工作有关事项公告如下：

一、备案对象

根据《办法》第十五条规定，应用人脸识别技术处理的人脸信息存储数量达到10万人的个人信息处理者，应当向所在地省级网信部门履行备案手续。

二、备案时间

（一）自2025年6月1日起，应用人脸识别技术处理的人脸信息存储数量达到10万人的，应当自数量达到之日起30个工作日内履行备案手续。

（二）2025年6月1日前，应用人脸识别技术处理的人脸信息存储数量已经达到10万人的，应当在2025年7月14日前履行备案手续。

（三）备案信息发生实质性变更的，应当在变更之日起30个工作日内办理备案变更手续。

三、备案方式

人脸识别技术应用备案采用线上方式。请直接访问“个人信息保护业务系统”（https://grxxbh.cacdtsc.cn），按照系统首页提供的《人脸识别技术应用备案系统填报说明（第一版）》，准备相关材料并履行备案手续，也可从中国网信网（https://www.cac.gov.cn）首页“全国网信政务办事大厅”栏目访问“个人信息保护业务系统”。

四、法律责任

未按照《办法》规定履行备案手续的，依照有关法律、行政法规的规定处理。

特此公告。

国家互联网信息办公室

2025年5月28日

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，开展主题当日活动，开设大讲堂，举行培训会等。陕西省网络信息安全协会：2025 第九届丝绸之路网络安全论坛成功举办；广州网络空间安全协会：承办“202 年越秀区网络安全等级保护工作会议暨网络与信息安全大讲堂”；上海市信息安全行业协会：2025 海事及船舶网络安全与数智化大会在沪召开；西藏自治区互联网协会联合开展廉政警示教育活动；惠州市计算机信息网络安全协会：“惠聚美好”人工智能网络安全与发展公益培训举行；南宁市信息网络安全协会：南宁市第十五届学术年会开幕式暨 2025（第四届）网络空间安全合作与发展论坛成功举办；南昌市网络信息安全协会：南昌市网络信息安全标准化技术委员会扬帆起航；湖南省网络空间安全协会：第 1 期网络与信息安全管理员高级研修班圆满收官；湖北省网络和数据安全协会：承办 2025 年湖北卫生健康行业网络安全攻防培训等。

关键词：年会、会长会议、团体标准、网络安全、信息安全

1. 陕西省网络信息安全协会：2025 第九届丝绸之路网络安全论坛成功举办

5 月 29 日，由陕西省网络信息安全协会主办的 2025 第九届丝绸之路网络安全论坛在陕西宾馆成功举办，本届论坛以“AI 赋能安全 共筑数字未来”为主题，汇聚行业专家、学者与企业代表，全面聚焦 AI 时代下网络安全行业面临的机遇与挑战，共同探讨 AI 技术在网络安全中的创新应用、风险治理及未来发展方向，助力构建安全可信的数字生态。来自省内外 500 余名专家、行业代表、企事业单位相关负责人出席大会。

活动设置主论坛和密码及其应用分论坛、教育行业网络安全分论坛、低空经济与卫星互联网安全专题论坛三个分论坛。为了更好地促进行业交流，在 2025 第九届丝绸之路网络安全论坛会场外还设置了产品展示区、技术交流区，并设置了固定的观展时间，促进企业与行业客户的近距离交流。

2. 广州网络空间安全协会：承办“202 年越秀区网络安全等级保护工作会议暨网络与信息安全大讲堂”

为贯彻落实习近平总书记关于网络安全的重要指示精神，深入贯彻落实国家网络安全等级保护制度，近日，由广州市越秀区委网信办、越秀区公安分局、越秀区政数局共同主办，广州网络空间安全协会承办的“2025 年越秀区网络安全等级保护工作会议暨网络与信息安全大讲堂”在协会报告厅成功举办。

会议面向70余名来自越秀区辖区内相关联网单位分管信息安全的负责人或代表，通报了越秀区2024年等保工作情况及2025年工作部署，并解读网络安全等级保护新规、分享大数据和AI时代常见的信息安全风险和问题，以进一步推进越秀区信息系统网络安全等级保护工作，有效防范化解网络安全风险，着力提升网络安全保障水平。

3. 上海市信息安全行业协会：2025海事及船舶网络安全与数智化大会在沪召开

5月29日，以“安全航运新未来，数聚船舶新动能”为主题的2025海事及船舶网络安全与数智化大会在上海半马苏河国际会议中心隆重举行。大会由上海市普陀区科学技术委员会、上海市信息安全行业协会、上海船舶工业行业协会主办，汇聚了国内外航运、船舶制造、网络安全及数智化领域近千名专家学者、企业代表，共探船舶行业安全防护与智能化转型路径。

大会通过主论坛战略引领与分论坛实践剖析，全面呈现船舶行业“安全为基、数智为翼”的发展图景。随着AI、大模型等技术与船舶场景加速融合，产业链上下游协同创新、标准共建与生态培育将成为破题关键。活动主办方表示，未来将持续搭建产学研用对接平台，助力我国航运业在智能安全赛道实现领跑。

4. 西藏自治区互联网协会联合开展廉政警示教育活动

5 月 28 日，在西藏自治区互联网行业党委的指导下，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、西藏自治区互联网行业党委所属各党支部，联合组织全体党员干部职工前往拉萨市党员干部廉政警示教育中心开展参观学习活动。此次活动作为西藏自治区互联网行业党委“党建领航，网众 e 心”系列活动之一，旨在增强党员干部的廉洁自律意识，筑牢拒腐防变的思想防线。

5. 惠州市计算机信息网络安全协会：“惠聚美好”人工智能网络安全与发展公益培训举行

5 月 29 日上午，由中共惠州市委网信办、惠州市工业和信息化局主办，惠州市计算机信息网络安全协会参与承办的“惠聚美好”人工智能网络安全与发展公益培训成功举行。

活动上，来自行业内的专家对人工智能大模型备案政策进行解读，详细介绍备案的目的、适用范围、流程与标准，分析政策出台对企业和行业的影响。技术专家以《人工智能安全挑战和应对》，通过真实案例，揭示人工智能大模型在应用中面临的安全挑战和应对策略。人工智能专家以《人工智能赋能智能制造与工业安全》，分享人工智能及安全发展趋势、大模型安全防护体系、智能制造与工业安全解决方案。

6. 南宁市信息网络安全协会：南宁市第十五届学术年会开幕式暨2025（第四届）网络空间安全合作与发展论坛成功举办

5月23日，由南宁市信息网络安全协会参与主办的“南宁市第十五届学术年会开幕式暨2025（第四届）网络空间安全合作与发展论坛”，在广西工业职业技术学院隆重举行。

论坛以“智能安全新生态——人工智能场景应用　网络安全保驾护航”为主题展开分享交流。广西网络安全和信息化联合会常务副会长、原自治区广播电视局副局长、一级巡视员朱日荣，广西工业职业技术学院党委副书记、校长黄政艳和南宁市科协党组成员、副主席李锦伟进行了大会致辞。会议邀请资深专家众多，旨在汇聚多方力量，共探网络安全前沿趋势。

7. 湖南省网络空间安全协会：第1期网络与信息安全管理员高级研修班圆满收官

近日，湖南省网络空间安全协会2025年第一期网络与信息安全管理员高级研修班在协会网络空间安全人才培训专委会主任单位湖南云畔网络科技有限公司正式开班，20余名来自企业从事网络安全从业者、行业精英进阶者、网络安全部门负责人、技术总监等人才参加培训。培训结束后开展职业技能等级认定。

此次培训为期2天，采用“理论+实操”相结合的教学模式，围绕当前网络安全面临的问题与挑战、我国大力推进网络安全建设的重要性、网络安全的防范与建设等内容进行了重点讲述。培训内容针对性强，指导性高，

有效帮助学员进一步规范网络安全行为、安全防范意识，为创建安全、和谐、稳定的工作环境打下了坚实的基础。

8. 湖北省网络和数据安全协会：承办 2025 年湖北卫生健康行业网络安全攻防培训

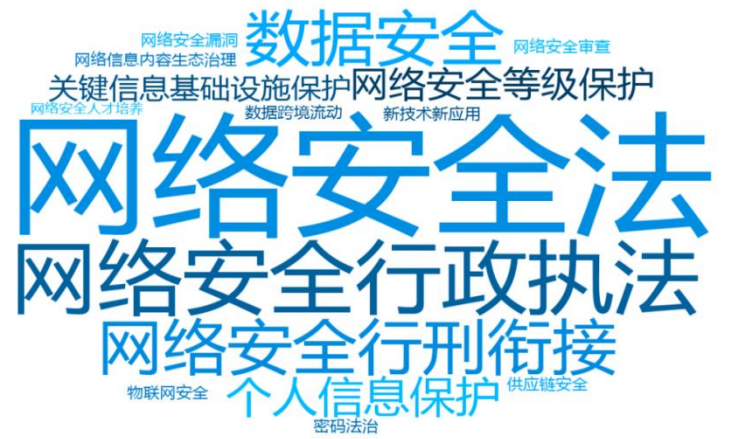
5 月 6 日，由湖北省卫健委指导、湖北省网络和数据安全协会医卫分会承办的 2025 年湖北卫生健康行业网络安全攻防培训顺利开展，湖北省内卫生健康行业专业人士参训。

培训中，专家以医疗数据泄露事件为例，剖析攻击路径与防御策略，并组织“红蓝对抗”模拟演练，让学员沉浸式体验漏洞挖掘、攻击溯源及应急处置全流程。学员结合工作实际，就“老旧系统安全加固”“移动医疗设备管控”等痛点与专家交流，形成 20 余项可落地解决方案。

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

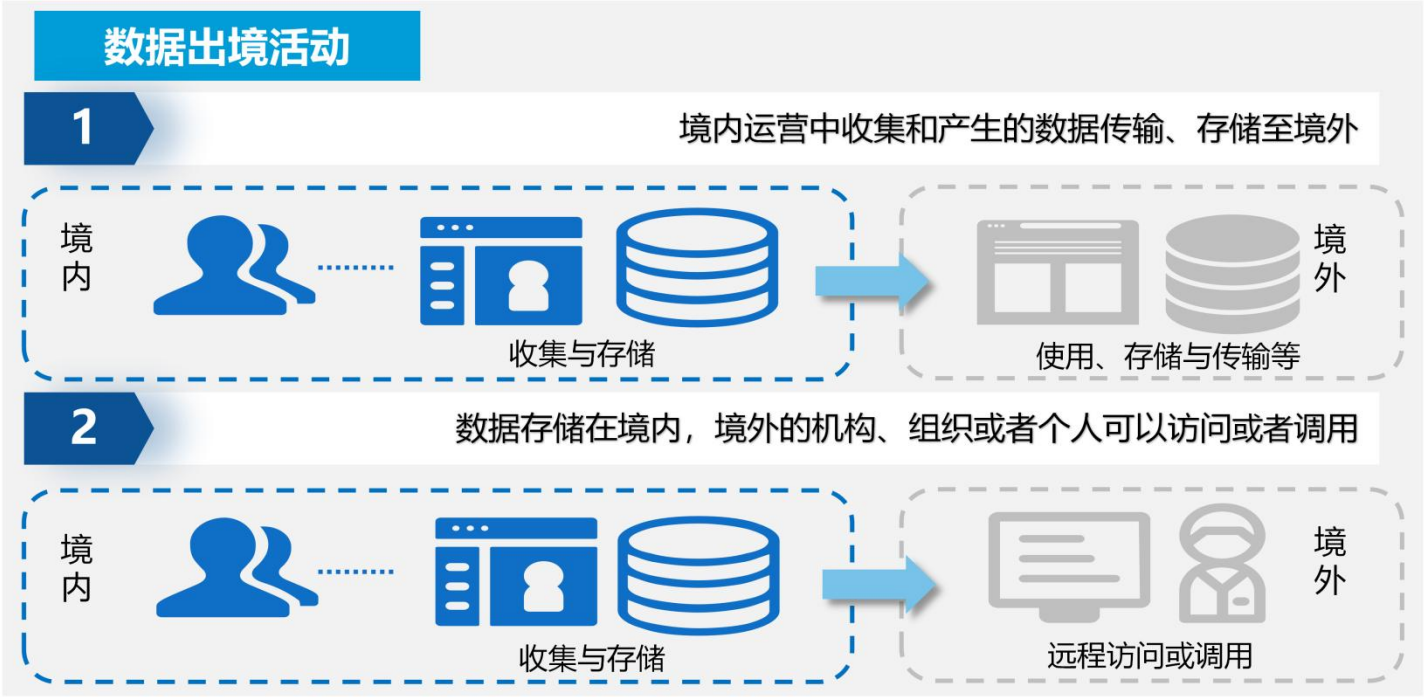
结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

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



数据出境安全风险评估咨询服务流程

- 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

- 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

……