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4月第4期（总第21期）

2025年4月17日

目　录

主办单位：公安部第三研究所网络安全法律研究中心

联合主办：北京网络空间安全协会

牵头组织：网安联秘书处

协办单位：网安联认证中心

技术支持：北京关键信息基础设施安全保护中心

广东关键信息基础设施保护中心

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。

境内前沿观察一：安全事件

导读：3月，适逢第十四届全国人民代表大会第三次会议，两会代表提出涉人工智能、可信数据空间等多项提案。

中央网信办、工业和信息化部、公安部、市场监管总局发布2025年个人信息保护系列专项行动的公告，将围绕App违法违规收集使用个人信息、SDK违法违规收集使用个人信息等重点问题开展系列专项行动。

我国七个数据标注基地数据标注规模再创新高，数据标注总规模达到17282TB，相当于中国国家图书馆数字资源总量的6倍左右。全国首个数据经纪人创新中心近日在深圳前海启动。《促进和规范数据跨境流动规定》实施一周年，数据出境安全管理工作取得数据出境安全评估用时大幅缩减，安全评估工作效率明显提升、多地发布自贸试验区数据出境负面清单，负面清单制度实施初见成效等。

中国网络安全产业联盟发布《美情报机构针对全球移动智能终端实施的监听窃密活动》，从针对SIM卡漏洞的高度复杂攻击，窃取收集SIM卡加密密钥，针对苹果手机的“零点击”攻击，对商用间谍软件的利用等11个方面展开，披露美情报机构针对全球移动智能终端和通讯体系的攻击渗透。

关键词：个人信息保护专项活动；数据标注；数据经纪人；数据跨境流动；监听窃密活动

1. 中央网信办、工业和信息化部、公安部、市场监管总局联合开展2025年个人信息保护系列专项行动

3月28日，中央网信办、工业和信息化部、公安部、市场监管总局发布2025年个人信息保护系列专项行动的公告，将围绕重点问题开展系列专项行动。

一是App（含小程序、公众号、快应用）违法违规收集使用个人信息。聚焦App未提供个人信息收集使用规则，未按照个人信息收集使用规则处理个人信息，无相关功能或未使用相关功能时调用位置、媒体文件、通讯录、设备等非必要权限或收集非必要个人信息，未提供个人信息相关投诉渠道，未提供有效的更正删除个人信息及注销账号功能，提供个性化信息推送等功能但未提供便捷的拒绝方式，以及开屏等场景频繁“意外”跳转广告页面等问题开展治理。

二是SDK违法违规收集使用个人信息。聚焦SDK未提供个人信息收集使用规则，未按照个人信息收集使用规则或与App明确的规则处理个人信息，未使用SDK相关功能时调用位置、媒体文件、通讯录、设备等非必要权限或收集非必要个人信息，未提供个人信息相关投诉渠道，提供个性化信息推送等功能但未向App提供停止收集个人信息或关闭该功能的选项等问题开展治理。

三是智能终端违法违规收集使用个人信息。聚焦智能手表、智能手环等穿戴产品，智能音箱、智能门锁、智能摄像头等家居产品，智能平板、

智能学习机等学习终端，未提供个人信息收集使用规则，高频次、高精度、长时段超范围收集非必要个人信息，以及相关功能开启后需在后台持续收集个人信息或者需在云端计算和分析的，但未向用户进行显著提示等问题开展治理。

四是公共场所违法违规收集使用人脸识别信息。聚焦交通运输、住宿旅游、教育培训、文化体育、物流商贸、休闲娱乐等公共场所使用人脸识别技术处理人脸信息，但未履行单独或书面告知同意等法律义务，未设置显著提示标识，未采取加密等严格保护措施，以及未依法开展个人信息保护影响评估等问题开展治理。

五是线下消费场景违法违规收集使用个人信息。聚焦自动售卖、扫码点餐、出行乘车、入场停车、商超支付、扫码充电、房屋租赁等线下消费场景中，强制关注公众号、强制注册会员，强制收集非必要的手机号、生日、性别等信息，物业前台收集个人信息用于用户授权以外的目的，未经同意向第三方提供用户个人信息，以及上述场景中个人信息处理者未尽有效保护义务造成泄露等问题开展治理。

六是个人信息相关违法犯罪案件。聚焦网络借贷、求职招聘、出行购票、教育、医疗、旅游住宿等领域个人信息违法犯罪活动，通过暗网电报等境外渠道以及境内渠道违规售卖公民个人信息，以及个人信息泄露或被攻击窃取等违法犯罪案件开展治理。（来源：网信中国）

2. 多名两会代表提出涉人工智能、可信数据空间等提案

3月，第十四届全国人民代表大会第三次会议期间，两会代表提出人工智能、可信数据空间等提案。

在人工智能方面，全国人大代表闫大鹏建议要加大人工智能政策支持力度，加强人工智能技术的基础研究和开发，鼓励人工智能相关企业，提高人工智能产品的研发水平和市场竞争力；针对人工智能企业，采取税收优惠政策，鼓励投资者和企业加大研发投入；建立完善监管体系，如知识产权保护机制等。全国政协委员齐向东建议，要建立适配大模型的纵深防御体系，筑牢人工智能的安全根基。通过构筑覆盖终端、应用、数据、模型、红域的多维度核心防护能力，打造适用于人工智能的立体纵深防御体系，并给予威胁情报、大网数据监测等情报赋能，实现“对外防攻击、对内防内鬼”，为人工智能大模型安全稳定运行保驾护航。

在可信数据空间方面，全国人大代表柳江建议，要加快可信数据空间技术标准化建设，加强互联互通。建议引导权威机构牵头，联合行业协会、科研机构和企业，共同制定可信数据空间相关技术标准，凝聚行业共识，有效降低数据流通利用技术壁垒，促进可信数据空间平台间互联互通互认。全国政协委员贺晗建议，要打造普惠型数字新基建，建设区域级、行业级等多层次的公共数据平台、产业数据平台、普惠算力调度平台，提供低成本AI、SaaS工具包，降低上云用数成本，推动民企数字化转型。（来源：赛博研究院）

3. 七个数据标注基地数据标注规模再创新高

3 月 19 日，数据标注基地先行先试现场会在成都举行，我国七个数据标注基地数据标注规模再创新高。

我国七个数据标注基地分别位于四川成都、辽宁沈阳、安徽合肥、湖南长沙、海南海口、河北保定和山西大同，数据标注总规模达到 17282TB，相当于中国国家图书馆数字资源总量的 6 倍左右。目前已形成医疗、工业、教育等行业的高质量数据集 335 个；赋能 121 个国产人工智能大模型研发；引进和培育标注企业 223 家；标注从业人员达 5.8 万人；带动数据标注行业相关产值超过 83 亿元。

数据标注是对数据进行添加标记、说明、解释、分类和编码的过程，是提升人工智能算法、模型核心能力的关键环节。国家数据局表示，未来将进一步畅通数据采集、标注、人工智能应用产业链，重点推动工业、金融、医疗、交通、教育等几大领域的高质量数据集建设，促进数据标注产业高质量发展。（来源：国家数据局）

4. 深圳市启动全国首个数据经纪人创新中心

3 月 18 日，全国首个数据经纪人创新中心——华为云（深圳·前海）数据经纪人创新中心在深圳前海启动。该创新中心由前海管理局与宝安区政府联合共建，由深圳市前海大数据资源管理中心有限公司运营。

根据规划，在未来三年内，该创新中心预计将取得一系列丰硕成果：带动数据交易额（含数据产品及数据服务）超过 30 亿元，推动数据要素相

关企业营业收入接近100亿元；累计赋能引入和本地培育数据经纪人企业超过100家，其中赋能新引入企业不少于30家；打造30个典型应用创新场景；培养数据要素相关专业人才不少于600人。

通过这些目标的实现，前海将打造成为数据要素生态高度汇聚、数据要素应用场景高度活跃、数据经纪产业品牌高度认可的产业高地。（来源：深圳政府在线）

5. 《促进和规范数据跨境流动规定》实施一周年 数据出境安全管理工作取得积极成效

为扩大高水平对外开放，激发数据要素价值，2024年3月22日，国家网信办出台实施《促进和规范数据跨境流动规定》（以下简称《规定》），促进数据依法有序自由流动。《规定》实施一年来，数据出境安全管理工作取得积极成效。

第一，一批数据跨境便利化措施陆续出台，企业普遍反响积极。《规定》明确了跨境购物、跨境寄递、跨境汇款、跨境支付、机票酒店预订、跨境人力资源管理、境外数据加工等免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境情形，放宽数据跨境流动条件，收窄数据出境安全评估范围。《规定》出台后，数据出境安全评估项目月均受理数量下降约60%，个人信息出境标准合同月均备案数量下降约50%，促进数据跨境流动的预期效果基本实现。此外，为做好《规定》实施，国家网信办配合中国人民银行、工业和信息化部等部门制定金

融、汽车等领域数据出境相关指引，为企业高效出境数据提供操作指南；指导全国网络安全标准化技术委员会发布《数据安全技术 数据分类分级规则》（GB/T 43697-2024），为企业识别重要数据提供参考；公布《个人信息出境个人信息保护认证办法（征求意见稿）》，明确个人信息出境个人信息保护认证的目的依据、适用情形、认证内容等。企业普遍反映数据出境管理政策不断优化，切实感受到《规定》带来的数据出境便利。

第二，数据出境安全评估用时大幅缩减，安全评估工作效率明显提升。国家网信办会同国务院有关部门建立国家数据出境安全管理专项工作机制，持续优化数据出境安全评估工作流程，强化部门协同，形成工作合力。一是更新发布《数据出境安全评估申报指南》，优化简化企业需要提交的材料。二是上线数据出境申报系统，面向企业提供在线提交材料通道，大幅缩减材料流转时间。三是组织北京、天津、上海、江苏、浙江、广东等6地省级网信办试点开展数据出境安全预评估，央地协同提升安全评估效率。四是商务部、国家网信办建立外商投资企业数据出境安全评估绿色通道机制，在合理范围内为在华经营的外商投资企业（含外资研发中心）数据出境提供便利。通过上述工作举措，目前数据出境安全评估平均用时少于30个工作日，相比《数据出境安全评估办法》规定的45个工作日大幅缩减。

第三，多地发布自贸试验区数据出境负面清单，负面清单制度实施初见成效。《规定》建立自贸试验区数据出境负面清单制度，鼓励自贸试验区结合实际制定数据出境负面清单，负面清单外数据出境将免予申报安全评估、订立标准合同、通过保护认证，是促进和便利自贸试验区数据跨境

流动的一项创新举措。落实《规定》，国家网信办、国家数据局联合印发通知，明确负面清单的政策定位、备案主体和备案流程。目前，天津、北京、海南、上海、浙江等地自贸试验区（港）数据出境负面清单已完成备案，对汽车、医药、零售、民航、再保险、深海业、种业等17个领域数据跨境流动发挥促进作用，部分在华企业已通过负面清单的模式实现高效便捷数据出境，数据出境负面清单制度实施初见成效。同时，按照“一地制定、多地适用”原则，指导自贸试验区做好数据出境负面清单适用衔接，针对同一领域，如果已有自贸试验区发布的负面清单，其他自贸试验区可参照执行。

第四，数据出境安全管理政策宣贯更加深入，企业数据出境合规能力持续提升。一是在中国网信网首页建立“数据治理”专栏，集中展示数据出境安全管理政策法规、标准指南、负面清单等文件，方便企业查阅使用。二是在北京、上海、深圳、杭州等16个城市举办政策宣讲会，面向全国2400多家企业机构解读数据出境安全管理政策标准，讲解实践案例；在北京举办欧盟在华企业数据跨境流动政策座谈会，与企业沟通交流，回应企业关切。三是公开发布《中国数据出境合规指引》，通过图解的形式系统阐述数据出境安全管理政策和合规要点。四是国家和各省级网信部门开通并公布数据出境咨询电话，常态化提供咨询服务，就企业遇到的常见问题进行解答。企业普遍反映，网信部门在促进和规范数据跨境流动方面不断探索，加强与企业互动，回应企业问题和诉求，持续优化数据出境安全管理机制，企业对相关政策的理解把握更加准确、合规能力显著增强。

第五，积极开展多双边数字治理对话交流，数据跨境对外合作稳步推进。发布《全球数据跨境流动合作倡议》，倡导各国政府共同构建高效便利安全的数据跨境流动机制，助力全球数字经济发展。积极开展多双边数字治理合作，按照对等互利原则，探索与有关国家和地区就数据跨境流动建立特殊制度性安排。中国国家网信办与欧盟委员会贸易总司建立中欧数据跨境流动交流机制并举行第一次会议；与德国数字化和交通部签署《关于中德数据跨境流动合作的谅解备忘录》，建立“中德数据政策法规交流”对话机制。国家网信办与香港特别行政区政府创新科技及工业局、澳门特别行政区政府经济财政司先后签署《关于促进粤港澳大湾区数据跨境流动的合作备忘录》，发布促进粤港澳大湾区数据跨境流动的相关政策文件。（来源：网信中国）

6. 中国网络安全产业联盟发布《美情报机构针对全球移动智能终端实施的监听窃密活动》

3 月 25 日，中国网络安全产业联盟（CCIA）立足网络安全专业视角，坚持科学、客观原则，根据全球网络安全厂商、研究机构和学者等披露的调查分析研究成果，编制《美情报机构针对全球移动智能终端实施的监听窃密活动》报告。

报告从 11 个方面披露美情报机构针对全球移动智能终端和通讯体系的攻击渗透：一是针对 SIM 卡漏洞的高度复杂攻击，二是窃取收集 SIM 卡加密密钥，三是针对苹果手机的“零点击”攻击，四是对商用间谍软件的利

用，五是通过运营商广泛预置软件收集数据，六是获取全球移动运营商技术参数，七是广泛使用伪基站监控手机，八是利用Regin软件攻击移动网络，九是“量子”系统对手机和上网PC的攻击能力，十是“怒触”计划的植入式攻击，十一是构建超级数据访问接口。（来源：中国网络安全产业联盟）

境内前沿观察二：政策立法

导读：3 月，网络安全、数据安全、个人信息保护、人工智能、密码管理仍是国家和地方政策立法重点关注内容。

网络安全方面，国家互联网信息办公室发布《中华人民共和国网络安全法（修正草案再次征求意见稿）》，对《网络安全法》多条法律责任进行修改与合并，以期更好起到维护网络安全的作用。全国网安标委拟修订、制定 15 项网络安全推荐性国家标准。云南省通信管理局、工业和信息化厅印发《云南省工业互联网安全分类分级管理办法实施细则》，包括企业分类分级、网络安全管理及风险处置、支持与保障等内容。

数据安全方面，市场监管总局印发《网络交易合规数据报送管理暂行办法》，规定网络交易平台经营者对平台内经营者违反市场监管法律、法规、规章的违法行为，应当自决定作出警示、暂停或者终止服务等处理措施之日起 5 个工作日内向住所地县级以上市场监管部门报告等。国家数据局 2025 年拟制修订 41 项数据领域国家标准，涵盖高质量数据集、数据基础设施建设、城市全域数字化转型等领域。安徽省合肥市发布全国首个数据标注产业规划《合肥数据标注产业发展规划（2025-2027 年）》，明确攻关数据标注关键共性技术、建设支撑项目、培育市场主体等任务。

个人信息保护方面，国务院发布《实施〈中华人民共和国反外国制裁法〉的规定》，强调《反外国制裁法》第六条第（四）项中的其他必要措施，包括但不限于“禁止或者限制向其提供数据、个人信息”。国家互联

网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》，明确应用人脸识别技术处理人脸信息的基本要求和处理原则，并指出人脸识别技术应用安全规范。

人工智能方面，《全国人民代表大会常务委员会工作报告》提出加强人工智能等新兴领域立法研究，指导地方探索区域协同立法。国家互联网信息办公室等四部门发布《人工智能生成合成内容标识办法》，明确人工智能生成合成内容标识主要包括显式标识和隐式标识两种形式。全国网安标委发布《网络安全标准实践指南——人工智能生成合成内容标识服务提供者编码规则》，指导人工智能生成合成内容服务提供者和网络信息内容传播服务提供者，开展人工智能生成合成内容的文件元数据隐式标识活动。广东省政府办公厅印发《广东省推动人工智能与机器人产业创新发展若干政策措施》，提出打造人工智能应用场景以及提出丰富数据要素供给等。

密码管理方面，国家密码管理局发布《电子认证服务使用密码管理办法（征求意见稿）》，规定采用商用密码技术提供电子认证服务，应当依法取得《电子认证服务使用密码许可证》。市场监管总局、国家密码管理局发布《商用密码产品认证目录（第三批）》，第三批目录共发布四种产品种类,包括基于 SM9 标识密码算法的密钥管理系统、PLC 控制器密码模块、DTLCP 密码模块、SSH 客户端密码模块、SSH 服务端密码模块。

关键词：网络安全；数据安全；个人信息保护；人工智能；密码管理

（一）国家层面动向

1. 《全国人民代表大会常务委员会工作报告》提出加强人工智能等新兴领域立法研究

3 月 14 日，《全国人民代表大会常务委员会工作报告》发布，对今后一年的任务进行部署。

报告提出高质量推进立法工作，预安排审议 34 件法律案。围绕完善国家安全体系和公共安全治理机制，修改网络安全法、治安管理处罚法、国家赔偿法等。围绕人工智能、数字经济、大数据、自动驾驶、低空经济、航天等新兴领域加强立法研究。启动法律清理工作。指导地方探索区域协同立法。（来源：新华社）

2. 国务院发布《实施〈中华人民共和国反外国制裁法〉的规定》

3 月 24 日，国务院发布《实施〈中华人民共和国反外国制裁法〉的规定》，共二十二条，自公布之日起施行。

《规定》强调，反外国制裁法第六条第四项中的其他必要措施，包括但不限于“禁止或者限制向其提供数据、个人信息”。第十三条规定，国务院有关部门对不依法执行反制措施的，有权责令改正，“禁止或者限制其从境外接收或者向境外提供数据、个人信息”。（来源：国务院）

3. 外交部：敦促美停止利用全球供应链实施恶意网络活动

3 月 25 日，外交部举行例行发布会。有记者提问，据报道，中国网络安全产业联盟今天发布《美情报机构针对全球移动智能终端实施的监听窃密活动》报告，披露了美国针对全球移动智能终端、移动产供链、运营商等开展网络攻击和监听窃密活动。请问中方对此有何评论。

郭嘉昆表示，中方注意到有关报告。根据这份报告，美国政府滥用其在信息技术和产供链上游的垄断优势地位，在全球范围内针对手机乃至整个移动产业生态体系开展大规模、长时间恶意网络活动，可谓无孔不入、无所不在。

值得注意的是，报告揭露出，美国是全球最主要的通过供应链和移动运营商实施网络攻击的国家。多年来，美方惯于在供应链安全问题上“贼喊捉贼”，操弄双重标准，不遗余力炒作所谓“5G 供应链安全问题”，同时却在自己国家大型互联网企业或设备供应商配合下，在全球信息设备产品中预设后门，服务于自身网络攻击行为。相信这份报告有助于国际社会认清美国的真实面目。

我们对报告曝光的美方恶意网络活动表示严重关切，敦促美方立即停止有关行为，特别是停止利用全球供应链实施恶意网络活动，以负责任的态度，给全世界一个交代。（来源：新华网）

4. 中共中央办公厅 国务院办公厅发布《中共中央办公厅 国务院办公厅关于健全社会信用体系的意见》

3 月 31 日，中共中央办公厅、国务院办公厅发布《中共中央办公厅 国务院办公厅关于健全社会信用体系的意见》，围绕构建覆盖各类主体的社会信用体系、夯实社会信用体系数据基础等五个方面，提出二十三条意见。

夯实社会信用体系数据基础方面，《意见》提出，建立全面完整准确的信用记录。严格界定公共信用信息范围，行业主管部门要根据法律、行政法规、地方性法规或党中央、国务院政策性文件确定本领域公共信用信息并形成行业信用记录，其中属于失信信息的，要分类明确其失信严重程度。对公共信用信息统一实行目录管理，国家发展改革委汇总建立相关主体的完整信用记录。

健全守信激励和失信惩戒机制方面，《意见》提出，依法依规开展失信惩戒。规范设定失信惩戒措施，依法依规合理确定惩戒范围和力度。设定失信惩戒措施、确定严重失信主体名单的设列领域必须以法律、行政法规、地方性法规或党中央、国务院政策性文件为依据，其中涉及设定对信用主体减损权利或增加义务的措施，必须以法律、行政法规、地方性法规为依据。行业主管部门应当以部门规章形式明确严重失信主体名单列入和退出的条件、程序。对被列入严重失信主体名单的，在申请政府资金、享受税收优惠、参与公共资源交易活动、股票债券发行、评先评优、公务员录用遴选调任聘任、事业单位公开招聘等方面，依法依规予以限制或禁止。

在房地产市场、互联网、人力资源市场、能源中长期合同领域增设严重失信主体名单。对失信惩戒措施和严重失信主体名单实行清单化统一管理。

健全以信用为基础的监管和治理机制方面，《意见》提出，以信用评价为基础实施分级分类监管。国家发展改革委牵头完善信用评价体系，各地区各行业主管部门以公共信用综合评价为基础健全本地区本行业信用评价机制，根据评价结果优化监管方式，对不同类型信用主体实施差异化监管。（来源：新华社）

（二）部委层面动向

1. 国家互联网信息办公室发布《中华人民共和国网络安全法（修正草案再次征求意见稿）》

3 月 28 日，国家互联网信息办公室发布《中华人民共和国网络安全法（修正草案再次征求意见稿）》，共八条。

修正草案再次征求意见稿提出，将《网络安全法》第五十九条修改为：“网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致

危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，由有关主管部门处二百万元以上一千万元以下罚款，并责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员处二十万元以上一百万元以下罚款。”

修正草案再次征求意见稿提出，将《网络安全法》第六十四条第一款、第六十六条、第七十条合并，作为第七十一条，修改为：“有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：

（一）发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的；

（二）违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的；

（三）违反本法第三十七条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。”（来源：网信中国）

2. 工业和信息化部印发《卫星网络国内协调管理办法（暂行）》

3 月 4 日，工业和信息化部印发《卫星网络国内协调管理办法（暂行）》，自 2025 年 5 月 1 日起实施。《办法》共六章三十三条，从卫星网络国内协调关系的建立、国内协调的开展、国内协调的完成等方面进行规定。

《办法》提出四项新的管理举措：一是加强国家统筹管理。强化国家无线电办公室统筹协调作用，提出对于重大、复杂协调事项由主管部门组织会议或函件征求意见开展协调。二是降低报送通知资料门槛。卫星操作单位报送卫星网络通知资料的条件为完成国内协调或提交频率兼容分析报告，并作出相关承诺。三是规范国内协调程序。明确国内协调需求征集、关系建立及开展协调各环节的时限要求，厘清申报协调双方的权利义务关系。四是减轻国内协调工作量。通过轨位间隔、技术限值等方式增加无需建立国内协调关系的情形，减少国内协调对象范围。（来源：国务院）

3. 国家互联网信息办公室等四部门发布《人工智能生成合成内容标识办法》

3 月 7 日，国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局联合发布《人工智能生成合成内容标识办法》，自 2025 年 9 月 1 日起施行。

《标识办法》明确，人工智能生成合成内容标识主要包括显式标识和隐式标识两种形式，显式标识是指在生成合成内容或者交互场景界面中添加的，以文字、声音、图形等方式呈现并可以被用户明显感知到的标识；

隐式标识是指采取技术措施在生成合成内容文件数据中添加的，不易被用户明显感知到的标识。

《标识办法》要求，服务提供者提供的生成合成服务属于《互联网信息服务深度合成管理规定》第十七条第一款情形的，应当按照要求对生成合成内容添加显式标识；服务提供者应当按照《互联网信息服务深度合成管理规定》第十六条的规定，在生成合成内容的文件元数据中添加隐式标识；提供网络信息内容传播服务的服务提供者应当采取技术措施，规范生成合成内容传播活动。

《标识办法》强调，任何组织和个人不得恶意删除、篡改、伪造、隐匿本办法规定的生成合成内容标识，不得为他人实施上述恶意行为提供工具或者服务，不得通过不正当标识手段损害他人合法权益。（来源：网信中国）

4. 国家互联网信息办公室、公安部联合发布《人脸识别技术应用安全管理办法》

3 月 13 日，国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》，自 2025 年 6 月 1 日起施行。

《办法》明确应用人脸识别技术处理人脸信息的基本要求。应用人脸识别技术处理人脸信息活动，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行个人信息保护义务，承担社会责任，不得危害国家安全、损害公共利益、侵害个人合法权益。

《办法》提出应用人脸识别技术处理人脸信息的处理规则。一是应当具有特定的目的和充分的必要性，采取对个人权益影响最小的方式，并实施严格保护措施。二是应当履行告知义务。三是基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。基于个人同意处理不满十四周岁未成年人人脸信息的，应当取得未成年人的父母或者其他监护人的同意。四是除法律、行政法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。除法律、行政法规另有规定外，人脸信息的保存期限不得超过实现处理目的所必需的最短时间。五是应当事前进行个人信息保护影响评估，并对处理情况进行记录。

《办法》指出人脸识别技术应用安全规范。一是实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。国家另有规定的，从其规定。二是应用人脸识别技术验证个人身份、辨识特定个人的，鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等渠道实施。三是任何组织和个人不得以办理业务、提升服务质量等为由，误导、欺诈、胁迫个人接受人脸识别技术验证个人身份。四是在公共场所安装人脸识别设备，应当为维护公共安全所必需，依法合理确定人脸信息采集区域，并设置显著提示标识。任何组织和个人不得在宾馆客房、公共浴室、公共更衣室、公共卫生间等公共场所中的私密空间内部安装人脸识别设备。五是人脸识别技术应用系统应当采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。（来源：网信中国）

5. 市场监管总局印发《网络交易合规数据报送管理暂行办法》

3 月 24 日，市场监管总局印发《网络交易合规数据报送管理暂行办法》，共二十一条，自 2025 年 4 月 25 日起施行。

《办法》所称网络交易合规数据，是指网络交易平台经营者依据《电子商务法》《网络交易监督管理办法》向市场监管部门提供的，产生于中华人民共和国境内的网络交易经营者身份信息、违法行为线索数据、行政执法协查数据、特定商品或者服务交易数据等网络交易监管相关数据。其中，网络交易平台经营者包括为经营者提供网络经营场所、商品浏览、订单生成、在线支付等网络交易平台服务的网络社交、网络直播等网络服务提供者。

《办法》规定，网络交易平台经营者对平台内经营者违反市场监管法律、法规、规章的违法行为，应当自决定作出警示、暂停或者终止服务等处理措施之日起 5 个工作日内向住所地县级以上市场监管部门报告，提供平台内经营者身份信息、网店名称、商品或者服务信息、违法行为描述、保存的有关记录、处置措施等违法行为线索数据。

《办法》提出，市场监管总局可以根据有关规定或者标准，探索开展公共数据开放和授权运营，依法合规向网络交易平台经营者提供政务数据服务，支持网络交易平台经营者更好地开展平台内经营者身份核实、许可信息验证、信用体系建设和平台内治理等工作。（来源：市说新语）

6. 国家密码管理局发布《电子认证服务使用密码管理办法（征求意见稿）》

3 月 21 日，国家密码管理局发布《电子认证服务使用密码管理办法（征求意见稿）》，共二十三条。

征求意见稿规定，采用商用密码技术提供电子认证服务，应当依法取得《电子认证服务使用密码许可证》。《电子认证服务使用密码许可证》有效期 5 年，内容包括：获证机构名称，住所，电子认证服务系统名称及版本号，证书编号，有效期限，发证机关和发证日期等。《电子认证服务使用密码许可证》禁止转让、出租、出借、伪造、变造、冒用、租借。

征求意见稿提出，电子认证服务机构应当按照国家有关密码管理要求履行电子认证服务使用密码安全管理义务，保证其电子认证服务使用密码持续符合要求。电子认证服务机构应当建立健全电子认证服务系统运行维护制度，明确关键岗位和岗位责任，制定操作规范，加强巡检和运行维护，提高监测预警和应急处置能力，及时消除电子认证服务系统运行安全隐患，保证电子认证服务系统安全可靠运行。

征求意见稿强调，电子认证服务机构应当自行或者委托专业机构每年至少进行一次电子认证服务使用密码合规性评估，对评估中发现的问题及时进行整改，并向住所地省、自治区、直辖市密码管理部门报送电子认证服务使用密码合规性评估报告。（来源：国家密码管理局）

7. 市场监管总局、国家密码管理局发布《商用密码产品认证目录（第三批）》

3 月 19 日，市场监管总局、国家密码管理局发布《商用密码产品认证目录（第三批）》，自发布之日起实施。第三批目录共发布四种产品种类，包括基于 SM9 标识密码算法的密钥管理系统、PLC 控制器密码模块、DTLCP 密码模块、SSH 客户端密码模块、SSH 服务端密码模块。（来源：国家密码管理局）

8. 工业和信息化部发布《工业和信息化部涉企行政检查事项表》

3 月 18 日，工业和信息化部发布《工业和信息化部涉企行政检查事项表》，列出四十项涉企行政检查事项。其中，工业和信息化部开展的涉企行政检查事项包括对非经营性互联网信息服务（含移动互联网应用程序）活动实施监督检查，网络运行安全检查，对电信业务经营者、互联网信息服务提供者保护用户个人信息的情况实施监督检查，网络产品安全漏洞检查，工业和信息化领域网络安全综合检查，工业和信息化领域数据安全监督检查等。（来源：工信部）

9. 15 部门办公厅联合发文，促进中小企业合规管理

3 月 13 日，工业和信息化部等 15 部门办公厅联合发布《关于促进中小企业提升合规意识加强合规管理的指导意见》，围绕明确合规管理重点领域、统筹推进中小企业合规管理体系建设提出十六条意见。

明确合规管理重点领域方面，《意见》提出，引导中小企业遵守网络安全、数据安全等方面法律法规，加强信息系统、网络、数据的安全防护和安全意识教育；制定实施数据安全合规管理制度，加强对数据的分类分级和权限管理，加强人员管理和技术控制，履行重要数据识别备案、分级防护、风险评估等责任义务，防范并及时应对和处理数据泄露、篡改、丢失事件；重点梳理向第三方输出、共享、委托、提供数据，从第三方接受数据，处理个人信息及跨境传输数据等活动中的合规要求和风险，落实特定类型信息收集与使用合规义务，保护企业数据及个人信息安全。

统筹推进中小企业合规管理体系建设方面，《意见》提出坚持因企制宜，引导企业完善合规制度。工业和信息化部将会同有关部门研究梳理中小企业合规相关标准和合规要点，为企业提供指引和参考。全国工商联将加强法治民企建设，制定实施工商联执委企业建立和完善中国特色现代企业制度指引。各地要结合实际，引导中小企业从自身实际情况出发，以风险防控为目标，建立完善覆盖重点领域、关键环节和重要人员的合规管理体系，在兼顾成本与效率的前提下加强合规管理。在选择合规管理模式、建立合规治理结构、培育合规文化理念、数字化转型推进合规等方面充分发挥企业自主性，以适合企业所需为宜。（来源：工信部）

10. 国家网信办发布第十批深度合成服务算法备案信息

3 月 12 日，国家网信办公布第十批深度合成服务算法备案信息，共计 395 项。

涉及的主要公司及算法有百川智能“百川教育大模型多模态算法”、腾讯“腾讯音乐文生图合成算法”、通义云启“阿里云云安全中心智能助手内容生成算法”、网易有道“有道子曰听记深度合成算法”等。根据《互联网信息服务深度合成管理规定》，具有舆论属性或者社会动员能力的深度合成服务提供者，应当履行备案和变更、注销备案手续。（来源：网信中国）

11. 全国网安标委发布《网络安全标准实践指南——人工智能生成合成内容标识服务提供者编码规则》

3 月 14 日，全国网安标委发布《网络安全标准实践指南——人工智能生成合成内容标识服务提供者编码规则》，指导人工智能生成合成内容服务提供者和网络信息内容传播服务提供者，开展人工智能生成合成内容的文件元数据隐式标识活动。

《实践指南》给出人工智能生成合成内容服务提供者和网络信息内容传播服务提供者的编码结构和赋码规则。其中，编码结构要求，服务提供者编码由二十七位的阿拉伯数字或大写英文字母组成，包括第 1 位~第 2 位标识格式定义码，第 3 位~第 22 位主体标识码，第 23 位~第 27 位服务扩展码三个部分。（来源：全国网安标委）

12. 全国网安标委拟修订、制定15项网络安全推荐性国家标准

3月19日，全国网络安全标准化技术委员会秘书处发布《关于下达15项网络安全推荐性国家标准计划的通知》，拟修订、制定15项网络安全推荐性国家标准。

拟修订的国家推荐标准有11项，包括《网络安全技术 SM2密码算法加密签名消息格式》、《网络安全技术 密码应用标识》、《网络安全技术 二元序列随机性检测方法》等。

拟制定的国家推荐性标准有4项，包括《网络安全技术 SM9密码算法加密签名消息格式》、《网络安全技术 事件调查原则和过程》、《网络安全技术 量子密钥分发的安全要求、测试和评估方法第1部分：要求》、《网络安全技术 量子密钥分发的安全要求、测试和评估方法第2部分：测试和评估方法》。（来源：全国网安标委）

13. 工信部人工智能标委会发布《工业和信息化部人工智能标准化技术委员会2025年标准制定指南（征求意见版）》

3月21日，工信部人工智能标委会发布《工业和信息化部人工智能标准化技术委员会2025年标准制定指南（征求意见版）》，围绕基础共性、关键基础技术、产品服务、赋能应用、安全治理五个方面，提出2025年标准制定工作指南。

安全治理方面，征求意见版提出，人工智能安全治理标准体系规范人工智能安全标准体系框架，明确标准体系的总体架构、分类和关键标准领域，为行业提供基本的安全规范和技术指导。具体而言，人工智能安全治

理标准体系包括治理能力标准、基础设施安全标准、数据安全标准、算法模型安全标准、应用安全标准、赋能安全标准。2025 年，应用安全标准拟制定智能移动终端产品安全防护与检测标准、人脸识别系统注入攻击防御能力要求及评估方法、生成式人工智能视频检测服务系统能力要求、生成式人工智能音频检测服务系统能力要求、数字人安全标准、智能体安全标准、合成鉴伪检测技术标准。（来源：工信部人工智能标委会）

14. 工业和信息化部、人工智能标准化技术委员会发布《工业和信息化领域人工智能安全治理标准体系建设指南（2025）（征求意见稿）》

3 月 27 日，工业和信息化部、人工智能标准化技术委员会发布《工业和信息化领域人工智能安全治理标准体系建设指南(2025)(征求意见稿)》。

征求意见稿提出，人工智能安全治理标准体系框架主要由治理能力、基础设施安全、网络安全、数据安全、算法模型安全、应用安全、赋能安全 7 个部分组成。

治理能力标准主要规范人工智能支撑能力和管理能力，为实现人工智能安全治理夯实基础底座。基础设施安全标准主要规范硬件平台、软件平台和智算中心等方面安全，确保人工智能基础设施安全稳定。网络安全标准主要规范网络安全的防护、监测、管理，以及供应链安全、网络安全风险评估，确保网络安全可靠运营。数据安全标准主要规范基础数据服务、训练数据、业务数据等方面安全，明确人工智能数据安全要求。算法模型安全标准主要规范算法、模型等方面安全，保障人工智能技术创新安全可

控。应用安全标准主要规范智能产品应用、智能服务应用、智能体、信息等方面安全，为推动产业智能化发展提供安全保障。赋能安全标准主要规范人工智能赋能新型工业化应用、行业应用，以及赋能网络、数据、信息、业务等方面安全，为人工智能赋能安全提供技术保障。（来源：工信部人工智能标委会）

15. 数据领域名词解释起草专家组发布《数据领域常用名词解释（第二批）》

3 月 29 日，数据领域名词解释起草专家组发布《数据领域常用名词解释（第二批）》，共二十条，包括数据产权、数据产权登记、衍生数据等名词解释。

其中，数据产权，是指权利人对特定数据享有的财产性权利，包括数据持有权、数据使用权、数据经营权等。

衍生数据，是指数据处理者对其享有使用权的数据，在保护各方合法权益前提下，通过利用专业知识加工、建模分析、关键信息提取等方式实现数据内容、形式、结构等实质改变，从而显著提升数据价值，形成的数据。

数据产业，是指利用现代信息技术对数据资源进行产品或服务开发，并推动其流通应用所形成的新兴产业，包括数据采集汇聚、计算存储、流通交易、开发利用、安全治理和数据基础设施建设等。

算力池化，是指通过算力虚拟化和应用容器化等关键技术，对各类异构、异地的算力资源与设备进行统一注册和管理，实现对大规模集群内计算资源的按需申请与使用。（来源：国家数据局）

16. 国家数据局 2025 年拟制修订 41 项数据领域国家标准

3 月 19 日，全国数据标准化技术委员会 2025 年第一次“标准周”全体会议在成都举行。记者从国家数据局获悉，2025 年拟制修订 41 项数据领域国家标准，涵盖高质量数据集、数据基础设施建设、城市全域数字化转型等领域，关系到人工智能、数据流通利用、智慧城市等产业行业的发展。

全国数据标准化技术委员会提出，要积极支持民营企业参与数据领域国家标准制定；加快推动数据治理、数字科技和基础设施建设等重点领域的标准研制。此外，全国数据标准化技术委员会联合多个国家级、行业、地方标准委员会发出全国数据标准化联合行动倡议，数据标准“协同共建，体系筑基”，国标践行“试点验证，经验推广”，标准落地“协同推进，实效提升”。（来源：央视新闻）

（三）地方层面动向

1. 新疆维吾尔自治区发布《新疆维吾尔自治区数据条例》

3 月 28 日，新疆维吾尔自治区发布《新疆维吾尔自治区数据条例》，自 2025 年 5 月 1 日起施行。《条例》共八章六十四条，包括数据基础设施、数据资源、数据流通、数据开发应用等内容。

《条例》规定，公共数据是指本行政区域内国家机关，法律、法规授权的具有管理公共事务职能的组织以及教育、医疗、供水、供电、供气、供热、公共交通等公共服务运营单位在履行法定职责或者提供公共服务过程中收集、产生的数据。

《条例》提出，公共数据共享分为无条件共享、有条件共享、不予共享三种类型。公共管理和服务机构应当按照国家和自治区规定对收集、产生的公共数据进行评估，科学合理地确定公共数据共享类型，并定期更新。公共管理和服务机构对列入有条件共享的公共数据，应当说明理由并明确共享条件；对列入不予共享的公共数据，应当提供相关法律、法规或者国家有关规定。公共管理和服务机构之间共享公共数据，应当以共享为原则，不共享为例外。

《条例》强调，对无条件共享的公共数据，公共管理和服务机构应当通过自治区公共数据平台直接获取，使用时不得超出履行法定职责或者提供公共服务必要范围，不得以任何形式提供给第三方，也不得用于其他任何目的。超出法定职责或者提供公共服务范围使用公共数据的，数据主管部门和数据提供单位应当在发现后立即终止其继续获取公共数据。对有条件共享的公共数据，公共管理和服务机构应当通过自治区公共数据平台提出共享申请，数据提供单位应当自收到申请之日起十个工作日内答复；不同意共享的，应当说明理由。（来源：新疆维吾尔自治区司法厅）

2. 广西壮族自治区工信厅印发《广西“人工智能+制造”行动方案（2025-2027 年）》

3 月 3 日，广西壮族自治区工业和信息化厅印发《广西“人工智能+制造”行动方案（2025-2027 年）》，围绕总体要求、工作目标、重点任务，重点实施人工智能产品突破、“智赋万企”、关键技术攻坚、企业培优育强、产业布局优化、资源要素保障六大行动。

资源要素保障方面，《行动方案》提出要夯实数据基础。持续推广《数据管理能力成熟度评估模型》（DCMM）等国家标准，鼓励企业开放数据，支持建设企业、行业、区域可信数据流通平台，支持行业链主企业、龙头企业及平台企业加快行业数据汇聚和分析应用，构建高质量工业数据语料库。（来源：广西壮族自治区工业和信息化厅）

3. 广东省政府办公厅印发《广东省推动人工智能与机器人产业创新发展若干政策措施》

3 月 9 日，广东省政府办公厅印发《广东省推动人工智能与机器人产业创新发展若干政策措施》，有效期至 2027 年 12 月 31 日。

《措施》提出打造人工智能应用场景。建立省级跨部门协调机制，压实“管行业管人工智能应用”责任，实施“人工智能+”行动，在教育、医疗、交通、民政、金融、安全等领域广泛拓展应用。组织开展“机器人+”行动，围绕工业、农业、城市管理、医疗、养老服务、特种作业等领域，深入挖掘开放应用场景。鼓励各地市挖掘开放各类应用场景，招引企业打造一批典型案例。

《措施》提出丰富数据要素供给。构建高质量人工智能数据集和语料库，形成一批高质量数据产品和服务。支持发展数据交易市场，推动广州、深圳数据交易所打造国家级数据交易场所。支持开展“数据要素×”行动，深化数据要素应用赋能。支持加快培育数据企业，依托优势打造广东数据要素集聚发展区。

《措施》提出建立包容审慎监管机制。探索创新人工智能与机器人“监管沙盒”等包容审慎监管模式，营造鼓励创新、大胆试错的制度环境。加大财政资金对人工智能与机器人领域相关软课题研究的支持力度。完善生成式人工智能发展和管理机制，加快建设粤港澳大湾区生成式人工智能安全发展联合实验室。支持人工智能与机器人安全性相关的检测认证平台建设，提供安全风险、伦理道德等方面的评估认证服务。加快推动人工智能与机器人领域立法工作，为人工智能与机器人产业发展提供制度保障。（来源：广东省政府）

4. 云南省通信管理局 工业和信息化厅印发《云南省工业互联网安全分类分级管理办法实施细则》

3 月 12 日，云南省通信管理局、云南省工业和信息化厅印发《云南省工业互联网安全分类分级管理办法实施细则》，共五章十七条，包括企业分类分级、网络安全管理及风险处置、支持与保障等内容。

《实施细则》指出，工业互联网企业网络安全由高到低分为三级、二级、一级。工业互联网企业应当按照工业互联网安全定级相关标准规范，结合企业规模、业务范围、应用工业互联网的程度、运营重要系统的程度、

掌握重要数据的程度、对行业发展和产业链供应链安全的重要程度以及发生网络安全事件的影响后果等要素，开展自主定级。

《实施细则》强调，工业互联网企业承担本企业网络安全主体责任，企业主要负责人为本企业网络安全第一责任人，要建立健全企业内部网络安全管理制度，主动开展自主定级、安全建设、风险评估、安全整改和应急保障等工作，落实安全防护标准，有效应对网络安全风险，保障本企业工业互联网安全。积极将网络安全纳入企业发展规划和工作考核，加大网络安全投入，加强网络安全防护能力建设，有效防范化解网络安全风险。企业应当积极配合主管部门的监督管理。（来源：云南省通信管理局）

5. 天津市数据局发布《天津市公共数据资源登记管理实施细则（试行）》

3 月 13 日，天津市数据局发布《天津市公共数据资源登记管理实施细则（试行）》，自 2025 年 3 月 1 日起实施，有效期 5 年。《细则》共六章二十九条，包括职责分工、登记要求、登记程序等内容。

《细则》规定，天津市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。登记主体按照国家和天津市要求，及时申请办理公共数据资源登记，签署诚信承诺书，对登记申请材料的真实性、完整性、合法性、有效性负责。在申请登记前，登记主体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。

《细则》提出，天津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，按照申请、受理、形式审核、公示、赋码等程序开展。其中，首次登记时，登记主体应按规定提交主体信息、数据合法合规性来源、数据资源情况、存证情况、产品和服务信息、应用场景信息、数据安全风险评估等申请材料。登记主体在开展授权运营活动并提供公共数据资源或交付公共数据产品和服务后，在20个工作日内提交首次登记申请。细则施行前已开展授权运营的，登记主体应按照首次登记程序于细则施行后的30个工作日内进行登记。

《细则》指出，登记结果有效期原则上为三年，自赋码之日起计算。对授权运营范围内的公共数据产品和服务登记，根据授权协议运营期限不超过三年的，登记结果有效期以实际运营期限为准。登记结果有效期届满的，登记主体可在期满前60日内按照规定续展。每次续展期最长为三年，自上一届有效期满次日起计算。期满未按规定续展的，由登记机构予以注销。（来源：天津市数据局）

6. 福建省数据管理局印发《福建省公共数据资源登记管理办法（试行）》

3月17日，福建省数据管理局印发《福建省公共数据资源登记管理办法（试行）》，自2025年4月1日起施行，有效期2年。《办法》共七章二十九条，包括责任分工、登记类型、登记程序、平台管理等内容。

《办法》提出，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、续展登记。登记主体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的20个工作日内应申请首次登记。申请首次登记时，登记主体应向登记机构提交首次登记申请表，包括主体信息、数据合法合规性来源、数据资源情况、存证情况、产品和服务信息、应用场景信息、数据安全风险评估情况等,并附相关佐证材料。

《办法》规定，公共数据资源登记一般按照申请、受理、形式审核、公示、赋码等程序开展。公示期满无异议的，登记机构按照国家数据局制定的统一编码规范，向登记主体发放登记结果查询码。登记结果有效期原则上为三年，自赋码之日起计算。对授权运营范围内的公共数据产品和服务登记，根据授权协议运营期限不超过三年的，登记结果有效期以实际运营期限为准。（来源：福建省数据管理局）

7. 湖北省数据局发布《湖北省公共数据资源登记实施细则（公开征求意见稿）》

3月18日，湖北省数据局发布《湖北省公共数据资源登记实施细则（公开征求意见稿）》。公开征求意见稿共七章二十八条，包括登记要求、登记类型、登记程序、登记管理等内容。

征求意见稿规定，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。经授权开展运营活动的法人组织，应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。

征求意见稿提出，根据工作职责直接持有或管理公共数据资源的单位，以及依法依规对授权范围的公共数据资源进行开发运营的法人组织为登记

主体。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。

征求意见稿强调，登记主体在申请办理首次登记时，应当提交存证情况材料。存证情况可由登记主体自证或委托第三方专业服务机构证明。自证由登记主体自行承担相应证明责任，自证文件应真实反映登记数据存储情况，包括但不限于数据存储位置截图、数据库查询结果截图、记录数据操作详细信息的日志文件等。委托第三方专业服务机构证明包括区块链平台存证、公证处公证、其他第三方专业服务机构测评。区块链平台存证、公证处公证证明文件包括电子版公证证书或扫描件；其他第三方专业服务机构测评证明文件包括但不限于数据资产评估中心、软件评测中心、律师事务所、会计师事务所等机构测评出具的权威报告。（来源：湖北省数据局）

8. 湖南省人民政府办公厅印发《湖南省 2025 年政务服务和数据工作要点》

3 月 18 日，湖南省人民政府办公厅印发《湖南省 2025 年政务服务和数据工作要点》，围绕深入推进政务数据共享、提升数字政务发展水平、持续提升政务服务效能等十二个方面，提出四十八条建议。其中，湖南省公安厅分工负责两项工作，一是推进湖南省政务数据统一管理，二是推动湖南省政务数据统一治理。

推进湖南省政务数据统一管理方面，《工作要点》提出，湖南省直单位要整合归集本行业、本系统、本单位数据，建立行业数据“一本账”，

按照“三不变”原则将非涉密业务系统数据库分类合规迁移上云并接入总枢纽，向总枢纽更新挂接目录资源，形成“系统—目录—数据”关系。持续推动共建共治共享自然人、法人、地理空间、信用信息、电子证照等基础数据库。各市州要推动本地区政务数据统一归集、治理、共享、应用。

推动湖南省政务数据统一治理方面，《工作要点》提出，推动政务数据统一治理。制定湖南省政务数据共享管理办法和工作指引。每季度开展数据目录和数据资源质检，推进政务数据综合治理。制定基础数据库等标准规范。（来源：湖南省政府）

9. 江西省发展改革委（江西省数据局）印发《江西省公共数据资源登记管理实施细则》

3 月 24 日，江西省发展改革委（江西省数据局）印发《江西省公共数据资源登记管理实施细则》，自 2025 年 5 月 1 日起施行，有效期 5 年。

《细则》明确公共数据资源登记的基本原则，包括依法合规、公开透明、标准规范、安全高效等，并详细规定职责分工，确保省级数据主管部门、登记机构、其他相关部门及各设区市数据管理部门等职责清晰，保障登记工作有序开展。

在登记要求方面，《细则》涵盖直接持有或管理公共数据资源的党政机关和事业单位等登记范围，并明确登记主体为直接持有或管理公共数据资源的单位，依法依规对授权范围内的公共数据资源进行开发运营的法人组织。各设区市、赣江新区设立或指定事业单位作为登记机构，负责具体登记工作。

此外，《细则》还明确四种登记申请类型，包括首次登记、变更登记、更正登记、注销登记，并规定了登记申请、受理、审核、公示、赋码等程序，以及登记异议处理流程、结果有效期、安全监管、法律责任等监管措施，形成了完整的登记管理体系。（来源：江西省公共资源交易平台）

10. 北京市互联网信息办公室等三部门印发《北京市数据跨境流动便利化综合配套改革实施方案》

3 月 27 日，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局印发《北京市数据跨境流动便利化综合配套改革实施方案》。《方案》提出六项主要任务，包括营造高效透明可预期的政策环境、强化可信流通技术赋能、优化全链条全领域安全监管等。

营造高效透明可预期的政策环境方面，《方案》提出负面清单倍增扩面。在国家数据分类分级保护制度框架下，按照自贸试验区数据出境负面清单动态管理机制，在评估完善首批汽车、医药、零售、民航、人工智能等 5 个领域负面清单基础上，聚焦北京市重点产业发展方向和企业实际需求，遴选若干重要领域制定出台第二批负面清单。全国其他自贸试验区正式发布的数据出境负面清单涵盖领域，北京市自贸试验区可参照使用，并按照《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》执行。

强化可信流通技术赋能方面，《方案》提出加快推进数据流通安全技术应用。针对不同市场主体间数据跨境流通交易风险和特定业务需求，利用可信数据空间、区块链、隐私计算等可信流通技术，提升数据跨境流通

效率和安全保障能力。探索开展个人信息匿名化试点，研究制定个人信息匿名化处理操作指南，指导个人信息匿名化技术在医疗、营销等典型场景优先落地。

优化全链条全领域安全监管方面，《方案》提出构建“综合+行业+属地”协同监管机制。数据安全监管部门发挥综合统筹作用，联合行业主管部门加强对各类市场主体违法违规出境数据情况的收集掌握，各自贸组团管理部门及属地相关职能部门配合开展数据出境情况摸排，依据投诉举报、转办移交、数据监测等线索，开展数据违规出境行为监督执法。建立网信部门与执法司法机关间的数据出境违法违规线索双向移交与会商研判机制，形成监管合力和典型判例。（来源：网信北京）

11. 上海市互联网信息办公室发布《上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）》

3 月 28 日，上海市互联网信息办公室发布《上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）》。征求意见稿共六章二十四条，包括网络数据分类分级、重要数据识别及目录管理、公共数据分类分级及开发利用等内容。

征求意见稿提出，网络数据分类应当根据网络数据管理和使用需求，结合网络数据所属行业领域已有的网络数据分类基础，灵活选择业务属性将网络数据逐级细化分类。涉及法律法规有专门管理要求的网络数据类别（如个人信息、公共数据），应按照有关规定和标准进行识别和分类。

征求意见稿强调，网络数据分级应当根据网络数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将网络数据从高到低分为核心数据、重要数据、一般数据三个级别。当网络数据业务属性、重要程度和可能造成的危害程度变化时，应当对网络数据的级别进行动态更新。

征求意见稿规定，重要数据识别主要依据相关法律法规，行业、领域重要数据识别指南，数据分类分级相关国家标准等。网络数据处理者应当对所处理的数据情况进行盘点、梳理和分类分级，并判断其对国家安全、经济运行、社会稳定、公共健康和安全可能造成的影响，按照国家有关规定识别、申报重要数据。各主管部门根据本行业、领域实际，审核申报情况，对确认为重要数据的，应当及时向网络数据处理者告知或者公开发布，同时将相关网络数据处理者纳入到重要数据处理者名单。（来源：网信上海）

12. 江苏省数据局等 12 部门联合印发《江苏省培育壮大数据企业行动方案（2025-2027 年）》

3 月 31 日，江苏省数据局、中共江苏省委金融委员会办公室、江苏省发展和改革委员会等 12 部门联合印发《江苏省培育壮大数据企业行动方案（2025-2027 年）》。《方案》明确 5 大重点任务，包括引导拓展新兴数据业务、增强数据企业核心能力等。

引导拓展新兴数据业务方面，《方案》提出，支持网络安全企业拓展数据安全业务。推动网络安全龙头企业拓展面向动态防护要求的数据安全业务，丰富数据安全产品，构建覆盖数据全生命周期的综合业务体系。支持创新型中小企业聚焦数据可信流通技术，加快成长为技术基础好、市场占有率高、核心竞争力强的数据安全企业。

加大数据企业招引力度方面，《方案》提出，加强重点数据企业招引。聚焦先进存储、大模型、智能算法等领域，招引一批行业领先的数据技术企业。加快在智能制造、新能源、大健康等领域，招引一批聚焦细分行业的数据应用企业。聚焦数联网、数据空间建设需求，招引一批数据基础设施领域的头部企业。围绕数据动态安全防护需求，招引一批在区块链、隐私计算等领域具有竞争力的骨干企业。鼓励各地招引影响力大、实力强的省外数据企业在江苏设立综合型总部、区域总部、研发机构或数据服务基地等分支机构。（来源：江苏省中小企业公共服务平台）

13. 安徽省合肥市发布全国首个数据标注产业规划

3 月 7 日消息，安徽省合肥市近日发布全国首个数据标注产业规划《合肥数据标注产业发展规划（2025-2027 年）》。

《规划》提出，力争到 2027 年底，合肥市多语种标注和语音标注能力达到国际领先水平，围绕“人工智能+”和“数据要素×”重点行业，标注数据规模达 3000TB，构建 11 个以上行业高质量数据集，拉动标注产业规模达 30 亿元，支撑相关产业规模超千亿，打造国际上有特色、有影响力的数据标注基地。

《规划》提出“一核引领、两区支撑、多园协同、区域联动”的产业空间布局。具体来看，高新区将被打造成数据要素核心引领区，力争成为全球领先的数据标注产业高地；蜀山与新站两大区域构建数据标注产业集聚区，推动区域协同发展；各县（市）区结合本地优势建设“数据标注+”特色产业园区，引导产业赋能传统产业、新兴产业和未来产业。同时，加强合肥数据标注基地顶层设计，带动合肥都市圈、皖北等地区发展，鼓励龙头企业在全国辐射发展分基地，形成协同发展大格局。

《规划》明确六大重点任务，一是攻关数据标注关键共性技术，加强数据预处理、智能化标注工具、数据安全等方向的技术创新；二是建设支撑项目，打造数据标注公共服务平台和人机协同多模态众智标注平台，提升数据开发能力；三是培育市场主体，招引培育龙头企业，助力中小企业专业化发展，建立健全第三方服务商体系；四是赋能行业发展，推动社会治理和服务数字化转型，强化数据要素的放大、叠加、倍增效应；五是营造发展生态，完善产业标准体系，加强人才培育招引，强化数据监管机制；六是创新运营机制，通过“四会一赛”生态运营、“政产学研用金”联合推进等措施，推动产业多方面、多层次发展。（来源：数字合肥）

境内前沿观察三：治理实践

导读：3 月，公安、网信、通信管理部门等机构持续发力，对网络空间安全进行全方位、多层次治理，旨在提升网络安全防护能力，构建更加安全的网络空间。

公安机关方面，公安部公布依法打击侵犯公民个人信息犯罪 10 起典型案例，主要包括：甘肃张掖公安机关侦破“1.23”侵犯公民个人信息案、四川凉山公安机关侦破宋某川等人侵犯公民个人信息案等。公安机关根据行为人社会危害性、主客观要素等内容做出相应的惩戒。因未履行数据安全保护义务，江西省萍乡市公安网安依法处罚某公司。江苏公安网安破获一起有偿提供“虚假流量”服务的“网络水军”案件。

网信部门方面，上海市委网信办会同市公安局、市市场监管局、上海互联网应急中心，对属地短视频类、生活服务类、论坛社交类等 12 家网站平台开展专项检查，指导整改工作。重庆市网信办依据《数据安全法》对属地存在个人信息泄露的重庆某公司作出行政处罚。青海省互联网信息办公室依法对海西州某公司存在的网络数据安全违法行为进行行政处罚。

通信管理部门方面，北京市通信管理局发布 2025 年第二期问题 APP 名单。安徽省通信管理局下架一款侵害用户权益的 APP“唱歌 K 歌大全”。针对 2025 年第 1 批次整改不到位的 APP,安徽省通信管理局近日已对相关 APP 予以公开通报，并要求限期整改。广东省通信管理局公开通报 8 款未按要求完成整改 APP 或小程序。浙江省通信管理局发布 2025 年第 2 批侵害用户

权益行为的APP名单。江苏省通信管理局发布2025年第2批侵害用户权益行为的APP名单。

国家公共数据资源登记平台正式上线运行，开展公共数据资源登记，是贯彻落实《中共中央办公厅、国务院办公厅关于加快公共数据资源开发利用的意见》的重要举措。国家网络安全通报中心通报大模型工具Ollama存在安全风险。通报指出，使用Ollma在本地部署DeepSeek等大模型时，会在本地启动一个Web服务，并默认开放11434端口且无任何鉴权机制。该服务直接暴露在公网环境，存在重大数据安全风险。

关键词：打击犯罪；数据安全；算法问题专项检查

（一）公安机关治理实践

1. 公安部公布依法打击侵犯公民个人信息犯罪 10 起典型案例

3 月 28 日，公安部公布依法打击侵犯公民个人信息犯罪 10 起典型案例。

案例一：北京海淀公安机关侦破刘某等人侵犯公民个人信息案。

北京海淀公安机关网安部门查明，2022 年 12 月以来，以刘某为首的犯罪团伙制作木马程序，组织人员入职目标教培机构，定向投放木马程序非法控制教培机构内部计算机，窃取客户资料等个人信息。2024 年 9 月，北京海淀公安机关依法抓获犯罪嫌疑人 8 名，指导 17 家受害企业清除木马程序，有效消除个人信息泄露风险隐患。

案例二：甘肃张掖公安机关侦破“1.23”侵犯公民个人信息案

甘肃张掖公安机关网安部门查明，2023 年 2 月以来，以李某飞为首的犯罪团伙勾结快递行业工作人员，利用技术手段窃取快递订单相关个人信息，并出售牟利。2024 年 3 月，甘肃张掖公安机关依法抓获犯罪嫌疑人 18 名，查明涉案金额 300 余万元。公安部在本案基础上部署全国公安机关开展集群打击，共打掉犯罪团伙 12 个，抓获犯罪嫌疑人 65 名。

案例三：吉林长春公安机关侦破王某明等人侵犯公民个人信息案

吉林长春公安机关网安部门查明，2024 年 1 月以来，以王某明为首的犯罪团伙伪造工商营业执照，在招聘网站发布虚假招聘信息骗取求职者简历，并出售给电信网络诈骗等犯罪团伙牟利。2024 年 6 月，吉林长春公安机关依法抓获犯罪嫌疑人 27 名，查获伪造工商营业执照 1000 余张。

案例四：四川凉山公安机关侦破宋某川等人侵犯公民个人信息案

四川凉山公安机关网安部门查明，2023 年 1 月以来，以宋某川、费某扬和某宇等人为首的犯罪团伙，勾结教育行业供应链公司工作人员彭某，利用彭某开发运维在线学习平台的工作便利，非法获取、出售他人个人信息。2024 年 6 月，四川凉山公安机关依法抓获犯罪嫌疑人 45 名，并及时会同教育主管部门完善个人信息保护措施。

案例五：广东东莞公安机关侦破林某成等人侵犯公民个人信息案

广东东莞公安机关网安部门查明，2022 年 11 月以来，林某成等人成立法律服务公司，发展律师事务所及具有诉讼需求人员为客户，通过非法渠道获取他人个人信息牟利。2024 年 5 月，广东东莞公安机关依法抓获犯罪嫌疑人 21 名，查处涉嫌违法的法律服务公司 5 家。

案例六：江苏徐州公安机关侦破韩某珠等人侵犯公民个人信息案

江苏徐州公安机关网安部门查明，2020 年 12 月以来，以韩某珠、何某航为首的犯罪团伙利用黑客手段非法获取多款停车小程序中的停车数据，并通过安装定位设备方式，为他人提供车辆定位服务并牟利。2024 年 6 月，江苏徐州公安机关依法抓获犯罪嫌疑人 59 名，查扣定位设备 33 套。

案例七：山东青岛公安机关侦破张某等人侵犯公民个人信息案

山东青岛公安机关网安部门查明，2023 年 12 月以来，以张某、陈某静为首的犯罪团伙打着“自媒体工作室”的旗号，以招聘兼职工作人员的名义，骗取应聘人员的个人信息用于注册网络账号，并出售牟利。2024 年 5 月，山东青岛公安机关依法抓获犯罪嫌疑人 37 名。公安部在本案基础上部

署全国公安机关开展集群打击，共捣毁犯罪窝点21处，抓获犯罪嫌疑人114名。

案例八：河北承德公安机关侦破韩某等人侵犯公民个人信息案

河北承德公安机关网安部门查明，2022年12月以来，以韩某、黄某印为首的犯罪团伙，冒充医保部门工作人员，打着帮助开通“医保电子凭证”的幌子，骗取受害人个人信息注册网络账号并出售牟利。2024年4月，河北承德公安机关依法抓获犯罪嫌疑人43名，查获各类网络账号8万余个，查明涉案金额300余万元。

案例九：辽宁辽阳公安机关侦破朱某星等人侵犯公民个人信息案

辽宁辽阳公安机关网安部门查明，2023年10月以来，朱某星等人冒充某地图APP工作人员，打着免费帮助商户开通旺铺认证、提高知名度的旗号，骗取个体工商户个人信息，用于注册企业支付账号并出售牟利。2024年3月，辽宁辽阳公安机关依法抓获犯罪嫌疑人85名，查明涉案金额140余万元。

案例十：湖南湘潭公安机关侦破冯某等人侵犯公民个人信息案

湖南湘潭公安机关网安部门查明，2022年12月以来，以冯某、谭某红为首的犯罪团伙，通过在短视频平台发布免费领红包、游戏皮肤等虚假宣传视频，骗取他人的网络账号并出售牟利。2024年8月，湖南湘潭公安机关依法抓获犯罪嫌疑人35名，查获被盗网络账号6000余个，查明涉案金额200余万元。（来源：公安部网安局）

2. 江苏警方破获一起有偿提供虚假流量服务网络水军案

3 月 22 日消息，江苏公安网安近日破获一起有偿提供“虚假流量”服务的“网络水军”案件。

经查，犯罪嫌疑人安某某、臧某某、季某某等人违反国家法律规定，以营利为目的，搭建专门网站，配装手机机房，联系寻找各大网络社交平台上需要提升人气热度的网络直播间，非法向他人有偿提供虚假人气（在线人数）、涨粉、点赞、评论、播放量等服务，每次按不同服务数量收取几十元至几百元不等，涉嫌非法经营罪。目前，犯罪嫌疑人均已被依法刑事拘留，案件正在进一步办理中。（来源：公安部网安局）

3. 因未履行数据安全保护义务，江西省萍乡市公安网安依法处罚某公司

3 月 26 日消息，江西省萍乡市公安网安依法处罚某公司未履行数据安全保护义务的违法行为。

2025 年 2 月，江西省萍乡市公安局网安部门巡查发现，某机构查询系统存在重大泄露风险，极易被不法分子利用。调查发现，该机构为图方便，未按规定将手持终端采集的数据导入专网处理。涉事机构未履行数据安全保护义务，江西省萍乡市公安局网安部门依据《数据安全法》《个人信息保护法》有关规定对其予以警告处罚并责令限期整改。萍乡市委网信办联合公安机关对属地有关部门启动约谈问责程序，要求全面排查系统数据安全隐患。经过执法部门严肃查处、教育，机构方进行了深刻反省，第一时

间关停了相关页面，并组织开展了全面查究整改和网络安全培训。（来源：公安部网安局）

（二）网信部门治理实践

1. 上海市委网信办会同有关单位开展网络平台算法典型问题专项检查

3 月 7 日消息，上海市委网信办近日会同市公安局、市市场监管局、上海互联网应急中心等单位，对属地短视频类、生活服务类、论坛社交类等 12 家网站平台开展专项检查，指导整改工作。专项检查通过网上巡检、检查台账、线索比对、后台核验等方式，发现企业存在“信息茧房”、热搜榜单、算法向上向善、算法安全主体责任四个方面的共性问题。

“信息茧房”方面的共性问题有：一是标签管理机制不健全，导致算法推送内容类型多样性效果不明显；二是用户点击“不感兴趣”等负反馈功能后效果不突出，模型识别同质化内容能力需要进一步提高；三是部分平台算法推荐过程过于依赖用户已有兴趣点，潜在优质兴趣拓展不足，导致易形成负面低质内容“茧房”；四是个别平台强制用户选择兴趣标签，或者不支持用户对兴趣标签进行管理。

热搜榜单方面的共性问题有：一是部分平台榜单存在泛娱乐化情况；二是部分平台未有效对热搜榜单算法原理进行公示说明，榜单透明度和可解释性有待提高。

算法向上向善方面的共性问题有：一是违法不良信息检索过滤能力需进一步加强，部分平台把关不严，将违法和不良信息记入用户标签并据此推送信息；二是正向优质内容扶持力度不够，部分平台正能量优质内容池较小，未有效运用算法技术赋能优质内容识别与传播、提升正向内容在流量分发中的整体比重；三是个别平台未成年人模式下内容审核有待加强，存在不适宜未成年人浏览内容进入推荐池风险；四是AI生成信息的识别和审核能力不足，部分平台AI生成的文本、语音内容存在诱导性信息。

算法安全主体责任方面的共性问题有：一是平台内部算法安全组织架构不健全，未能有效搭建与业务量相适应的算法安全治理机构，内容安全管理部门在算法全生命周期管理中参与度不够；二是算法常态化评估机制不健全，未定期开展算法安全自评估；三是算法“应备尽备”落实不到位，部分平台算法尚未备案，或备案进度较为缓慢。（来源：网信上海）

2. 因泄露个人信息，重庆网信办依法处罚某公司

3月13日消息，根据国家网信办移交的问题线索，重庆市网信办近日依据《数据安全法》对属地存在个人信息泄露的重庆某公司作出行政处罚。

经查，该公司履行网络安全、数据安全保护义务不到位；执行网络安全、数据安全管理制度不到位；网络日志留存不符合法律法规规定；运行的系统未采取技术措施和其他必要措施保障数据安全，导致发生个人信息被窃取等违法情形，违反《网络安全法》《数据安全法》等法律法规。重庆市网信办依据《数据安全法》，对该公司作出责令改正，给予警告，并处五万元罚款的行政处罚，对其直接负责的主管人员和其他直接责任人员

分别处以一万元罚款处罚。目前该公司已按要求全面深入整改。（来源：网信重庆）

3. 因数据安全问题，青海省网信办依法处罚海西州某公司

3 月 21 日消息，青海省互联网信息办公室近日依法对海西州某公司存在的网络数据安全违法行为进行行政处罚，开出青海省首张网络数据安全“罚单”。

青海省互联网信息办公室针对有关问题线索充分调查取证，依法查明海西州某公司存在不履行网络安全、数据安全保护义务行为，其办公 OA 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，造成企业部分数据泄露。青海省互联网信息办公室依据《数据安全法》第四十五条第一款规定，对该公司作出责令改正，给予警告，并处 5 万元罚款的行政处罚，对直接主管人员和其他责任人员分别处以 1 万元罚款处罚。（来源：网信青海）

（三）通信管理部门治理实践

1. 北京、安徽、广东通信管理局发布侵害用户权益 APP 名单

（1）北京市

3 月 5 日，北京市通信管理局发布 2025 年第二期问题 APP 名单。北京市通信管理局近日通过抽测发现北京市部分 APP 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19款APP未整改或整改不到位。2025年1月26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APP并要求整改。截至通报，仍有4款APP未整改或整改不到位，现予以全网下架处置。（来源：北京通信管理局）

（2）安徽省

3月6日，安徽省通信管理局下架一款侵害用户权益的APP“唱歌K歌大全”。针对2025年第1批次整改不到位的APP，安徽省通信管理局近日已对相关APP予以公开通报，并要求限期整改。截至通报，尚有1款APP逾期未完成整改。安徽省通信管理局现组织对该APP进行下架，相关应用商店应在本通报发出后，立即对名单中的应用软件进行下架处理。（来源：安徽省通信管理局）

（3）广东省

3月25日，广东省通信管理局公开通报8款未按要求完成整改APP/小程序。广东省通信管理局近日发出《APP处置通知书》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7款APP、1款小程序未完成整改。被通报的APP/小程序应在2025年4月1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。（来源：广东信息通信业）

（4）浙江省

3月27日，浙江省通信管理局发布2025年第2批侵害用户权益行为的APP名单。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、即时通信、网络社区等类型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 5 款 APP 未按要求完成整改。未整改的 APP 开发运营者在 4 月 9 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）

（5）江苏省

3 月 31 日，江苏省通信管理局发布 2025 年第 2 批侵害用户权益行为的 APP 名单。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省内生活服务、休闲娱乐、实用工具等类型的 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。未整改的 APP 开发运营者在 4 月 14 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）

（四）其他部门治理实践

1. 国家公共数据资源登记平台上线运行

3 月 1 日，国家公共数据资源登记平台正式上线运行，登记工作全面展开，标志着数据要素市场化配置改革迈出重要一步。

开展公共数据资源登记，是贯彻落实《中共中央办公厅、国务院办公厅关于加快公共数据资源开发利用的意见》的重要举措。国家发展改革委、国家数据局联合印发《公共数据资源登记管理暂行办法》《公共数据资源授权运营实施规范》《关于建立公共数据资源授权运营价格形成机制的通知》后，国家信息中心积极搭建技术平台，地方、部门和相关企事业单位

主动对接落实资源登记工作，为平台如期上线创造了条件，也为逐步形成公共数据资源全国“一本账”，促进供需对接和公共数据规范化、透明化应用奠定基础。

公共数据资源登记平台是开展登记工作的信息化载体，实行“一个标准、两级架构”。国家登记平台主要负责办理中央和国家机关及其直属机构、中央企业的登记业务，同时暂时代为受理部分未完成平台建设省份的登记申请。登记首日，国家登记平台已有医保、气象、自然资源等多类国家级公共数据上线，北京、天津、河北、内蒙古、辽宁、上海、广东、海南、四川、陕西、宁夏、新疆生产建设兵团等地依托国家平台开展了登记工作。此外，山西、江苏、浙江、安徽、福建、江西、湖北等省级平台完成开发，与国家平台顺利对接，同步上线运行。国家登记平台与省级登记平台依托国家电子政务外网实现统一赋码、互联互通，将逐步构建起职责明确、分工负责、运转有序的全国公共数据资源登记体系。（来源：国家数据局）

2. 国家网络安全通报中心通报大模型工具 Ollama 存在安全风险

3 月 3 日，国家网络安全通报中心通报大模型工具 Ollama 存在安全风险。

据清华大学网络空间测绘联合研究中心分析，开源跨平台大模型工具 Ollama 默认配置存在未授权访问与模型窃取等安全隐患。鉴于目前 DeepSeek 等大模型的研究部署和应用非常广泛，多数用户使用 Ollama 私有

化部署且未修改默认配置，存在数据泄露、算力盗取、服务中断等安全风险，极易引发网络和数据安全事件。

通报指出，使用Ollma在本地部署DeepSeek等大模型时，会在本地启动一个Web服务，并默认开放11434端口且无任何鉴权机制。该服务直接暴露在公网环境，存在重大数据安全风险，包括：（1）未授权访问风险：未授权用户能够利用特定工具直接对模型及其数据进行操作，获取模型信息，甚至通过恶意指令删除模型文件或窃取数据；（2）数据泄露风险：通过特定接口可访问并提取模型数据，引发数据泄露风险；（3）数据破坏风险：攻击者可利用Ollama框架历史漏洞，直接调用模型接口实施数据投毒、参数窃取、恶意文件上传及关键组件删除等操作，造成模型服务的核心数据、算法完整性和运行稳定性面临安全风险。

通报还针对发现的安全风险提出相应安全加固建议。通报还建议广大用户加强隐患排查，及时进行安全加固，发现遭网络攻击情况第一时间向当地公安网安部门报告，配合公安网安部门开展调查处置工作。（来源：国家网络安全通报中心）

境外前沿观察：月度速览十则

导读：3 月，境外国家和地区在人工智能、加密货币、数据安全、个人信息保护、关基保护、网络安全等方面的政策法律、热点事件持续发生。

人工智能方面，欧盟委员会宣布通过《数字欧洲计划（2025-2027）》投入 13 亿欧元用于网络安全、人工智能及数字技能发展。《东盟负责任人工智能路线图（2025-2030 年）》正式发布，分为跨领域路线图与针对性路线图两类，旨在指导东盟政策制定者和利益相关者在 2030 年之前营造一个有利于负责任地开发和部署人工智能的环境。

加密货币方面，美国总统特朗普签署行政命令《建立战略比特币储备和美国数字资产储备》，主要内容包括战略储备创建与管理、资产核算等。

数据安全方面，美国总统特朗普签署行政命令《通过消除信息孤岛来阻止浪费、欺诈和滥用》，扩大对联邦机构非机密数据的访问，并促进机构间数据共享。法国竞争管理局宣布对美国苹果公司处以 1.5 亿欧元罚款，原因是该公司滥用其在设备定向广告中的主导地位。英国信息专员办公室（ICO）表示其正在调查中国短视频应用 TikTok 如何利用 13 岁至 17 岁青少年的个人信息，来对他们推荐内容。

个人信息保护方面，韩国《个人信息保护法》修正案获得国会通过，进一步强化跨境企业数据合规责任。对本地代表的工作范围提供了更清晰的界定，要求本地代表须具体负责“处理与个人信息处理相关的投诉和赔偿损害事宜”。

关基保护方面，香港特区立法会三读通过《保护关键基础设施（电脑系统）条例草案》，要求银行、能源、医疗保健和电信等关键行业加强网络安全防御，定期进行风险评估，并及时报告安全事件。瑞士联邦委员会引入针对关键基础设施的网络攻击的报告义务，要求关键基础设施运营商在发现网络攻击后 24 小时内向国家网络安全中心提交网络攻击初始报告，14 天内完成网络攻击报告表。

网络安全方面，加拿大政府推出了加拿大网络安全认证计划，以加强网络安全。该计划解决了针对该国国防工业的频繁网络攻击。

关键词：人工智能；加密货币；数据安全；个人信息保护；关基保护；网络安全

1. 欧盟委员会宣布通过《数字欧洲计划（2025-2027）》

3 月 28 日，欧盟委员会通过《数字欧洲计划（2025-2027）》，投入 13 亿欧元用于网络安全、人工智能及数字技能发展。该计划主要内容包括：（1）加速人工智能部署；（2）提高网络弹性；（3）扩展“目的地地球”计划；（4）扩展数字技能和创新；（5）发展欧盟教育和培训机构的数字技能；（6）欧盟支持实施并鼓励成员国采用新的欧盟数字身份钱包架构和促进“欧洲信任基础设施”的落地应用等。（来源：欧盟委员会）

2. 美国总统特朗普签署行政命令《通过消除信息孤岛来阻止浪费、欺诈和滥用》

3 月 20 日，美国总统特朗普签署行政命令《通过消除信息孤岛来阻止浪费、欺诈和滥用》，旨在扩大对联邦机构非机密数据的访问，并促进机构间数据共享。

行政令要求：（1）各机构负责人需采取措施，确保总统或其指定人员能够及时获取所有非密级机构记录和数据，以支持识别和消除浪费、欺诈及滥用行为的工作，包括促进非密级记录的共享与整合；（2）自命令发布之日起 30 日内，各机构需废除或修订阻碍非密级信息共享的指导文件，并向管理与预算办公室提交相关法规的审查报告；（3）各机构需确保联邦政府能够无阻碍获取所有接受联邦拨款的州级项目的完整数据，包括存储在

第三方数据库的数据；（4）劳工部长及其指定人员应在法律允许的范围内，访问所有失业数据和相关支付记录等。（来源：美国白宫）

3. 美国总统特朗普签署行政命令《建立战略比特币储备和美国数字资产储备》

3 月 6 日，美国总统特朗普签署行政命令《建立战略比特币储备和美国数字资产储备》，将美国定位为各国政府数字资产战略的领导者。行政令主要内容包括：

一是战略储备创建与管理，主要包括：（1）战略比特币储备。财政部设立专门办公室，管理由刑事或民事没收或罚款所得的比特币；（2）数字资产储备库。财政部应设立“数字资产储备库”管理机构，整合除比特币外的所有数字资产，整合标准同比特币；（3）增持限制。财政部与商务部应制定预算中性、不增加纳税人负担的比特币增持策略。非经立法或行政授权，不得不得使用纳税人资金购买除比特币外的其他数字资产；（4）资产处置例外。政府数字资产（含比特币及其他）原则上不得出售，除非用于：财政部长行使其合法权力并合理管理美国数字资产储备库；根据有管辖权的法院的命令，依法进行处置；赔偿犯罪受害者；执法行动；（5）评估报告财政部长应在本命令发布之日起 60 天内，提交一份评估报告，分析建立和管理战略比特币储备及美国数字资产储备库的法律和投资考虑因素。

二是资产核算。各机构负责人应在本命令发布之日起30天内，向财政部长和总统数字资产市场工作组全面报告该机构持有的所有政府数字资产情况

三是一般规定。本命令不削弱现有法律授权，实施需符合法定预算，且不创设任何法律权利。（来源：美国白宫）

4. 东盟发布《东盟负责任人工智能路线图（2025-2030年）》

3月5日，东盟发布《东盟负责任人工智能路线图（2025-2030年）》，分为跨领域路线图与针对性路线图两类，旨在指导东盟政策制定者和利益相关者在2030年之前营造一个有利于负责任地开发和部署人工智能的环境。

跨领域路线图方面，涵盖技能与能力建设、公平与包容、治理与参与、整合与合作四个关键支柱。针对性路线图方面，依据各国人工智能生态系统的准备程度分为新兴、有前景和发达三个层级，每个层级围绕内部治理结构和措施、负责任的人工智能辅助决策的技能与知识、风险缓解和运营管理、利益相关者协调与区域合作四个支柱制定具体行动。（来源：东南亚国家联盟）

5. 韩国国会通过《个人信息保护法》修正案

3月13日，韩国国会通过《个人信息保护法》修正案，进一步强化跨境企业数据合规责任。

修正案明确要求：（1）如果境外企业在韩国设有本地实体，则应当指定其作为本地代表，不得将该职责外包给其他第三方机构；（2）境外企业总部须管理和监督本地代表履行其职责；（3）隐私政策中须包含本地代表的名称、地址、电话号码和电子邮件地址；（4）对本地代表的工作范围提供了更清晰的界定，要求本地代表具体负责“处理与个人信息处理相关的投诉和赔偿损害事宜”。

修正案进一步引入了违反上述要求的具体罚则，违反上述要求的企业可能会被处以高达 1000 万或 2000 万韩元的行政罚款。修正案目前待总统批准并刊登政府公报后正式生效。（来源：韩国国会）

6. 香港特区立法会三读通过《保护关键基础设施（电脑系统）条例草案》

3 月 19 日，香港特区立法会三读通过《保护关键基础设施（电脑系统）条例草案》，要求银行、能源、医疗保健和电信等关键行业加强网络安全防御，定期进行风险评估，并及时报告安全事件。

《条例草案》对关键基础设施（CI）和关键基础设施组织（CIO）进行了定义。CI 是指那些对香港的社会和经济活动至关重要的基础服务和设施，涵盖能源、信息技术、银行和金融服务、航空运输、陆路运输、海上运输、医疗保健服务以及电信和广播服务等行业。CIO 还必须在香港设有办事处，如地址有任何变更，必须根据条例内容以书面形式通知监管机构，并设立和维持计算机系统安全管理单位。

《条例草案》规定，在关键计算机系统的移除，向基础设施添加计算机系统等事件发生后 1 个月内，CIO 应当向监管机构报告；CIO 在指定日期后的 3 个月内向监管机构提交一份保护 CI 的计算机系统安全计划；在指定日期后的 12 个月内以及此后每 12 个月进行一次计算机系统安全风险评估。

香港特区政府保安局局长邓炳强表示，条例核心功能是为维护电脑系统安全，绝非针对个人资料或者相关机密。执行时如要向营运者和相关机构索取资料，须合理行使条例中规定的权利，符合相关条文所定义的条件和程序，并只可索取符合相关条文目的的资料。此外，受规管的关键基础设施营运者大部分为大型机构，中小型企业和一般市民不受规管和影响。他也强调，条例并无域外效力。

邓炳强期望条例于 2026 年 1 月 1 日正式生效，并设立专责办公室。（来源：香港特区立法会）

7. 瑞士联邦委员会引入针对关键基础设施网络攻击的报告义务

3 月 7 日，瑞士联邦委员会引入针对关键基础设施的网络攻击的报告义务，要求关键基础设施运营商在发现网络攻击后 24 小时内向国家网络安全中心（NCSC）提交网络攻击初始报告，14 天内完成网络攻击报告表。承担报告义务的机构和组织主要包括能源和饮用水供应商、运输公司以及州和社区政府等。

当网络攻击威胁到关键基础设施运行、导致信息泄露，或涉及勒索、威胁或胁迫时，未报告网络攻击的关键基础设施运营商可能会被罚款。必

须报告的事件主要包括：（1）已成功在系统上安装恶意软件；（2）加密木马；（3）可用性攻击；（4）通过利用安全漏洞获得对计算机系统的未经授权访问等。（来源：瑞士联邦委员会）

8. 加拿大推出网络安全认证计划，以加强网络安全

3 月 12 日，加拿大政府推出了加拿大网络安全认证计划（CPCSC），以加强网络安全。该计划解决了针对该国国防工业的频繁网络攻击，这些攻击威胁到承包商和分包商持有的非机密联邦信息的安全。从 3 月开始，将实施一项新的行业标准，以保护国防合同中的敏感政府数据。

加拿大国防部门经常遇到针对承包商和分包商的网络攻击，从而危及非机密的联邦信息，保护这些关键供应链至关重要。CPCSC 将逐步实施，使公司能够调整其运营以满足新的要求。第一阶段将涉及发布新的加拿大工业网络安全标准，开启认证流程，并引入 1 级认证的自我评估工具。这将有助于企业在今年晚些时候更广泛地推出该计划之前了解该计划。（来源：加拿大政府）

9. 苹果因滥用主导地位被法国监管机构罚款 1.5 亿欧元

3 月 31 日，法国竞争管理局宣布对美国苹果公司处以 1.5 亿欧元罚款，原因是该公司滥用其在设备定向广告中的主导地位。

法国竞争管理局指出，苹果公司于2021年4月发布“应用程序跟踪透明度”机制，宣称以保护个人数据为目标，但其实施方式“既无必要，也不适当”。该机制有偏袒苹果自身服务之嫌，损害了第三方应用程序利益。

法国竞争管理局表示，此次处罚针对的是2021年4月至2023年7月之间苹果的违规行为。除罚金外，该局还要求苹果公司连续七天在其网站上发布该处罚决定的摘要。（来源：法国竞争管理局）

10. 英国信息专员办公室对TikTok等平台儿童数据保护问题展开调查

3月3日，英国信息专员办公室（ICO）表示其正在调查中国短视频应用TikTok如何利用13岁至17岁青少年的个人信息，来对他们推荐内容。ICO也在调查网络讨论平台Reddit和图片分享网站Imgur，了解它们如何评估未成年用户的年龄。

社媒平台使用复杂的推荐算法确定内容的优先级并吸引用户参与。然而，ICO认为平台的相似内容推荐可能导致儿童受到有害内容愈发严重的不利影响。ICO在声明中称，如果我们有足够证据证明上述任何一家公司违法，我们会向它们提出这个问题，并在得到它们的陈述后，得出最终结论。

2023年，ICO曾因TikTok未经父母同意使用13岁以下儿童的个人数据的行为违反了数据保护法，进而对TikTok处以1270万英镑（约合人民币1.19亿元）的罚款。（来源：英国信息专员办公室）

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.从大模型工具Ollama互联网暴露态势浅析大模型行业落地的初步画像

摘要：目前，各类大模型的落地应用越来越广泛，本文从公开的资产测绘数据分析出发，通过Ollama大模型工具在互联网上暴露的情况初步窥见当前大模型行业应用与落地的特征画像。此外，Ollama大模型工具大规模在互联网暴露态势，反映出企业、个人开发者在大模型工具部署时对安全风险的忽视，其安全配置管理能力和风险管控意识亟需提升，以在充分发挥人工智能技术价值的同时，有效保障数据安全与AI模型安全。

关键词：人工智能安全、数据安全、业务安全

随着人工智能特别是大模型技术的迅猛发展，各类大模型的落地应用越来越广泛。开源跨平台大模型部署工具Ollama，由于其灵活、便捷、快速一键部署大模型的功能，在企业界和学术界迅速得到普及。2025年3月

3 日，国家网络安全通报中心发布关于大模型工具 Ollama 存在安全风险的情况通报，指出 Ollama 在默认配置下暴露于公网时，存在严重的安全隐患，例如未授权访问、数据泄露和模型窃取风险等。本文从 Shodan、Censys、FOFA、ZoomEye 等互联网公开资产测绘数据分析出发，浅析大模型工具 Ollama 互联网暴露态势，并初步勾勒大模型在行业落地画像。

一、从模型家族分布看行业落地倾向

根据互联网资产测绘平台公开资产数据显示，目前国内暴露在公网环境中的大模型以 qwen2、llama、bert、nomic-bert、deepseek2 等家族居多，其中 qwen2 与 llama 两大家族占据绝对优势，从暴露的数据显示来看，当前大模型应用的典型特点整体呈现如下态势：

（一）生成式场景需求旺盛，qwen2 与 llama 居于主导地位

qwen2 是阿里云通义千问团队开发的开源模型，该模型是被认为是中文及多语言场景下的热门之选，根据百度等搜索引擎检索结果显示，其部署、调试、应用，在国内开源社区讨论热度突出，针对中文对话、智能客服、搜索推荐、智慧政务等应用领域需求强劲。另外，根据国内暴露在公网数据显示，qwen2 的部署量略高于 llama，而 llama 是由 Meta 主导的开源大模型家族，由于 llama 模型家族发布较早于 qwen 家族，仍然获得了广泛部署量。

（二）传统特征提取型模型仍保持应用热度

BERT 及其衍生模型在数量上仍然占据了一定比例，在文本分类、命名实体识别、特征提取和信息检索等相对传统的 NLP 应用中，企业、研究机

构、个人开发者仍继续采用经典的BERT架构，在资源有限、对生成式需求相对较弱的场景下，特征提取型模型从算力成本投入和部署规模仍然有重要价值。

（三）多样化小众模型反映场景细分趋势

目前，人工智能通用技术供应商聚集并向头部涌现，如deepseek2、chatglm、baichuan、minicpm、rwkv等来自不同人工智能通用技术供应商的模型家族的出现，数量虽然不多，但围绕细分领域或定制化需求或已经开始呈现不断探索趋势。在实际应用场景下，上述模型可能针对特定行业的法律、医疗、教育场景进行微调和优化，大模型在垂直应用上的精细化发展已逐渐显露趋势。

二、从参数规模分布看部署资源考量

根据互联网资产测绘平台公开资产数据显示，暴露在公网环境的模型参数规模分布，呈现明显的阶梯化趋势：

（一）中等规模模型成为产业落地主流选择

8.0B、7.6B、7.2B等参数规模的模型数量占据绝对优势，占据目前暴露在互联网的绝大部分比例。7B-8B左右的模型被广泛视为功能性和性价比最优的“甜点区”，单卡或双卡GPU便可满足大多数企业和个人开发者的测试、调试、部署、开发需求。此类规模的模型不仅能够提供足够好的对话生成能力，同时推理成本和资源消耗也较为可控，非常适合金融、医疗、政务、教育等领域构建知识库的私有化部署需求。

（二）数十亿级参数模型活跃，高端场景需求旺盛

参数规模为 32.8B、14.8B、70.6B 等数十亿参数级别的模型也有明显占比，这类规模的大模型一般运行在专用服务器，以及为运行大模型而构建的计算资源中，能满足更高的推理精度、复杂场景的要求，通常被用于高端对话机器人、精准推荐系统以及高级推理和分析任务，代表了企业普遍已经额外投入算力资源，积极探索更强的 AI 智能化应用。

（三）小规模与超大规模参数模型同时存在，呈多元化部署趋势

1B～4B 的小规模模型如 1.8B、3.2B、4B 等，尽管在互联网中暴露的数量不占绝对优势，但可能在企业内部知识库检索、FAQ 机器人、移动端本地部署等轻量场景中仍然保持一定需求。

最后，从互联网暴露资产数据中还能观测到极大规模（如 671B、235.7B、405.9B 等数百亿以上参数规模）的模型暴露情况，虽然整体数量不多，占比也相对较低，但此类模型由于其部署所需算力成本极高，且通常仅部署在具有高 GPU 性能的服务器或云环境中，当前面临的安全挑战可能会更为严峻，一方面，攻击者可利用这些极大模型的未授权访问漏洞，非法占用高价值的算力资源，另一方面，攻击者可通过持续的恶意请求导致资源耗尽或服务中断，进而影响正常研究或生产业务，甚至造成服务瘫痪。故大模型在调试、部署、应用过程中的“配置安全”和“安全配置”仍然是不可忽视的第一道防线。

三、综合模型分布画像与行业应用特征

基于上述模型家族和参数规模的分布画像，我们能够通过大模型工具 Ollama 互联网暴露态势初步勾勒出大模型的行业应用画像：

（一）行业应用以生成式为主，辅以传统任务并行

大量 qwen2 和 llama 模型的部署代表行业内以智能问答、生成式对话、辅助决策为代表的生成式 AI 应用已成为主流。而 BERT 系列模型的持续存在，意味着行业内也并未完全放弃传统 NLP 任务，特征抽取、分类检索等任务与生成式应用形成了并行发展的趋势。

（二）部署规模体现行业资源差异与应用需求的多样性

7B-8B 的广泛部署规模表明当前大多数企业、机构、个人的计算资源满足中等规模模型应用的必要资源，通常来说在不需要额外购买或增加计算资源的前提下，完成部署和应用，在实际场景中也能够在必要的模型性能与资源投入取得平衡。

而 7B～32B 左右是典型的“产业适配”区间，对于大多数企业、机构、个人来讲，仅需要额外少量投入专用计算资源，便可获得可观的理解与生成能力，又不至于像百亿级以上那样苛求顶级算力及计算资源的成本投入。

同时，互联网上少量暴露出的超大规模模型，也间接印证了头部企业和研究机构在内部可能部署了更多、更大规模的大模型，也说明了行业实力企业、研究机构在进行深入、复杂的探索，产业逐步出现资源投入差距化的状态。而一般企业、个人开发者则受限于资源和算力成本，更多选择中等规模模型进行部署，进一步反映出产业界在大模型应用上的资源投入差距日益扩大，产业生态呈现明显的层次化趋势。

（三）细分场景模型兴起，反映行业应用精细化趋势

各类小众模型家族的出现，体现了企业、研究机构、个人开发者正积极进行细分场景探索和模型定制化。行业应用开始由早期的“一模走天下”逐步向“场景细分和个性化定制”方向发展，这种趋势将可能进一步带动产业内大模型精细化落地。

（四）大模型互联网暴露态势凸显，大模型安全使用与安全管理面临挑战

当我们重新审视当前Ollama大模型工具在互联网大量暴露现象时，折射出的是大模型技术在近两年迅猛普及，作为相对新颖的技术应用，许多企业、机构、个人开发者急于尝试部署新兴的AI模型以抓住技术红利，却在实践过程中普遍忽略了安全部署与管理的重要性。

这种“重应用、轻安全”的心态和实践，导致部署、调试过程中配置不当、接口直接暴露、未授权访问等问题发生，进而给攻击者提供了便利条件，易引发数据泄露、模型窃取、算力盗用及服务中断等多重安全事件，同时，随着大模型的规模和种类越来越丰富，安全管理的复杂度不断攀升，尤其是极大规模模型一旦遭受未授权访问，不仅会造成巨大的算力资源浪费，甚至带来数据投毒和算法污染等严重后果。因此，在大模型迅速普及落地的同时，对AI安全风险的认知，安全标准与规范，在其大模型安全使用与安全管理过程中仍然面临艰巨挑战。

四、安全风险和落地挑战不容忽视

根据Shodan、Censys、FOFA、ZoomEye等公开资产测绘数据分析来看，随着大模型技术快速普及、技术门槛逐渐降低，越来越多企业、机构及个

人开发者能够低成本、快速地尝试和部署最新的AI模型,尤其是类似Ollama的工具能够完成大模型的一键部署和运行，以期迅速享受“技术平权”带来的新“技术红利”。然而，这种快速普及与广泛部署的趋势也造成了大模型无意间在互联网暴露数量呈现指数级增长，在积极部署应用的同时，行业内暴露出的严重安全隐患也不得不引起高度关注：

（一）部署配置不当，带来极高的安全风险

无意识的将开源或私有大模型部署于互联网，直接暴露于公网环境，且未采用有效的鉴权、加密手段，极易导致被未授权访问模型，无需认证即可调用模型服务，甚至导致数据泄露、模型投毒等恶意攻击，企业和机构在大模型私有部署时，务必要对可能潜在安全风险保持高度敏感和风险评估。

（二）大模型普及造成的安全治理复杂性显著提升

随着大模型家族、版本与部署场景的多样化发展，企业和机构在安全治理方面正面临空前的挑战。一方面，模型数量增加、多版本并行部署以及频繁迭代更新，使传统的安全管理模式和审计机制变得捉襟见肘；另一方面，大模型在不同业务场景中的定制化程度越来越高，带来了安全风险边界难以界定的问题。由于大模型在训练、微调与推理阶段涉及的数据类型、来源、敏感程度各异，传统的安全审计规则难以覆盖这种复杂的数据流通场景。此外，定制化大模型在应用中与业务系统的集成深度增加，使模型数据与业务数据、训练环境与生产环境、内部接口与外部接口之间的界限日渐模糊，增加了安全审计和权限管理的难度。这些因素导致企业在

界定模型访问权限、明确数据保护范围、设定数据访问边界等方面面临实际困难，进而造成数据泄露、未授权访问、权限滥用等风险不断增加，传统的安全治理策略已不能有效应对上述日趋复杂的安全场景。

综上，在大模型快速普及应用的背景下，企业和机构不仅要加大安全管理投入，还应全面提升技术团队对新兴 AI 技术的认知与适应能力。

五、结语

从 Ollama 互联网暴露态势中所反映的模型家族与参数规模分布画像，我们能够初步了解到当前行业内大模型部署的主流方向，以中等规模生成式大模型为主体，兼顾传统特征抽取型模型，并积极探索细分场景与定制化需求。在 AI“技术平权”、AI “技术红利”的驱动下企业、机构、个人在大模型私有部署已成快速爆发增长趋势，积极落地的同时，企业、机构、个人开发者必须对由此产生的数据安全与网络安全风险高度重视，尤其是对 AI 开源工具链的安全方面，需要重点通过加强配置管理、安全策略制定以及定期风险评估，才能在充分发挥大模型潜能的同时，确保网络和数据安全得到有效保障。（作者：雷承霖　烽台科技（北京）有限公司）

2. 如何打造安全可控的数据库安全网关

在信息化高度发展的今天，数据库系统作为存储和处理关键业务数据的核心组件，其安全性直接关系到数据资产的完整、保密和可用性。随着《网络安全法》和《数据安全法》等法律法规的颁布，关基、企事业单位

更加注重和加强了对其数据库的防护。很多网络安全厂商也都推出了数据库安全网关系统，协助用户保护数据库系统。

数据库安全网关定义

数据库安全网关通过对数据库客户端访问数据库服务的网络报文的解析，还原出访问数据库的用户、SQL 访问操作等，形成审计日志，并对非法的异常的 SQL 访问操作做管控，实现“事中管控、事后审计”的要求。数据库安全网关一般由基本核心组件和应用系统组成。基本核心组件包括硬件元器件、操作系统和数据库，应用系统实现数据库的审计与防护功能。

数据库安全网关主要用于关基单位、企事业单位，部署在单位的核心数据库资产之前，系统还原出针对数据库的 SQL 访问操作并记录。系统部署的环境以及系统所能接触的数据都是核心和机密的，因此系统本身的安全性和保密性尤为重要。针对系统的安全和保密性考虑，涉及五大安全服务，包括鉴别服务、访问控制服务、数据机密性服务、数据完整性服务和抗抵赖性服务。鉴别服务保证了系统的认证安全，访问控制服务确保系统的访问权限可控，数据机密性和完整性保证了系统存储数据的机密、不被篡改等。除此之外，系统的重要基本核心组件，还应当考虑国产化和自主可控，确保这些组件不会有“后门”。

数据库安全网关一般是 “软硬一体”的，根据这一特点及其功能点，应该从基本核心组件安全、应用系统安全、持久化数据安全三个方面设计系统的安全和保密性，打造其安全可控。

基本核心组件安全可控

基本核心组件安全，涉及硬件元器件、操作系统和数据库三个部分。

硬件元器件方面，首先考虑CPU的国产化，综合考虑国产化程度、自主可控技术以及供货持久度，可以采用鲲鹏、飞腾、海光等国产化CPU，其性能也能达到实用程度。网卡芯片方面，因涉及网络通讯和数据采集，也需要选择诸如网讯之类的国产化芯片。此外，内存、电源和存储介质等元器件也都都应该选择国产化供应商。

其次在操作系统方面，麒麟、统信、欧拉等厂商推出了符合中国信息安全测评中心要求的国产化操作系统，可以选择合适的操作系统或者内核。为提升可靠性，应该对系统的文件系统进行处理，一般地，文件系统应以自研格式加密形式存储，系统每次启动时解密、解压并以只读方式挂载文件系统，确保文件系统不会被篡改。系统应无root用户，受控用户可以通过命令行方式登录系统进行维护，保证了系统不会被越权操作。文件系统中应仅保留必需的服务，裁剪不需要和可能带来安全隐患的服务和命令，做到文件系统的最小化。

最后，在数据存储方面，审计日志需要持久化存储，而且审计日志是关于用户的数据库访问行为，应该选择符合中国信息安全测评中心要求的数据库，确保用户数据的安全。

应用系统安全可控

应用系统安全主要从系统的鉴别服务和访问控制来保证。

在鉴别服务方面，因为系统一般采用B/S架构风格实现，可通过浏览器管理系统，系统应强制使用国密通讯，保证网络通讯的安全性。系统应

采用改进型的 JWT 方式进行认证，在 JWT 中增加了盐和时间戳，保证系统不会被重放攻击。系统还应支持多种认证方式，包括密码、Ukey、证书等，并强制使用验证码，防止机器人攻击。此外，系统应对密码强度做要求，并要求用户首次登录修改密码、定期修改密码。

在访问控制方面，首先，系统应以 RBAC 方式进行权限控制。系统应内置系统管理员、审计员和业务操作员三种角色。系统管理员具备系统配置相关权限，业务操作员具备业务功能管理权限，审计员具备对系统管理员和业务操作员的操作日志查看权限。其次，系统应内置防火墙实现访问行为的控制。系统限制对外提供除 HTTPS 和 SSH 外的其他服务，限制可访问系统的 IP、接口，并对允许访问系统的 IP、Mac 进行绑定，防止非法未授权用户访问系统。通过鉴别服务和访问控制，可极大的提升系统的安全性和保密性。

持久化数据安全可控

持久化数据安全方面，根据持久化数据的类型不同选择不同的安全保密方式。持久化数据包括系统配置数据和审计日志数据两部分。

对于系统配置数据，因为数据量不会很大，则采用全量加密方式存储，系统启动后解密到内存中使用。如果配置中涉及到密码信息，则计算 MD5 后进行加密存储，系统不直接存储明文的密码。

对于审计日志数据，在存储到数据库前，先对敏感信息（如用户访问数据库的密码）脱敏处理，保证用户信息不泄露。为保证审计日志数据的安全性，系统应支持将审计日志数据备份到外置存储（如 SAN、NAS）上。

备份方式支持增量备份和全量备份；备份时机支持定期备份和即时备份。此外，系统应内置多块数据存储介质，每块存储介质可独立提供存储服务，审计日志数据以非冗余的方式分布式存储在多个存储介质上，以降低单块存储介质损坏带来的数据丢失风险。对系统中需要持久化的数据加密、备份、分布式存储，实现了数据的保密性和安全性。

结语

随着数据安全法律法规、条例的实施与推进，随着用户对“数据“的安全意识越来越突出，数据库安全网关也将会进一步发挥作用。中美贸易战、科技战、网络战等无处不在，安全无小事，用户在选择数据库防护设备的时候，除考虑功能外，也应该将安全可控放在首位。目前，有很多的安全厂商已发布相关产品,如天融信发布的数据库审计与防护系统(TopDAP)即是一款专业的数据库安全防护产品，具备功能丰富、国产化程度高、安全可控等特点。（作者：刘勇 北京天融信网络安全技术有限公司 高级工程师）

3. 白盒密码技术简介

摘要：密码系统的安全性通常由密钥的安全性决定，攻击者总是试图采用各种方法找到密钥。当密码算法运行在不可信平台上时，尤其是密码

算法软件实现时，攻击者完全具有监控密码系统运行过程的能力，白盒密码作为白盒攻击中保护密钥的关键技术手段。

关键词：白盒攻击、密钥、白盒加密

Abstract: The security of a cryptosystem is usually determined by the security of the key, and attackers always try to find the key by various methods. When the cryptographic algorithm runs on an untrusted platform, especially when the cryptographic algorithm is implemented by software, the attacker has the ability to monitor the process of the cryptographic system. White-box cryptography is the key technical means to protect the key in the white-box attack.

Key words: white box attack, key, white box encryption

1.背景

随着网络和计算机技术应用的快速发展，信息安全问题已经成为关乎国计民生的大事。传统密码学建立在黑盒模型下，该模型假设算法运行在一个可信的终端，其运行子结果、内存等均处在不可查看和不可更改的可信任环境中——即假设攻击者不知道密钥，但是知道密码算法,能够控制明文并获得密文输出，但是加密的动态过程是隐藏的，攻击者无法观察算法的运行。

密码系统的安全性通常由密钥的安全性决定，攻击者总是试图采用各种方法找到密钥。根据攻击者攻击密码系统所具有的能力的不同，通常将密码学安全攻击模型分为：黑盒模型、灰盒模型与白盒模型。

在黑盒攻击中，密码系统运行在一个不可见的黑盒里，攻击者只能获取黑盒的输入输出信息，而无法获取任何其它信息（图 1）。此时密码算法的安全强度完全由密码算法本身的安全强度决定。

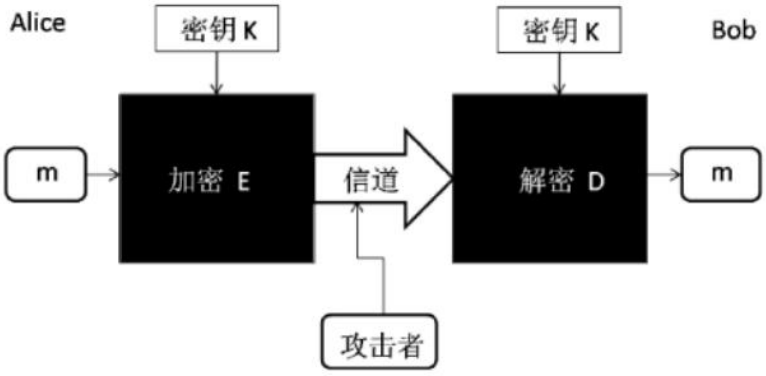


图 1 黑盒攻击

在灰盒攻击中，攻击者不仅能获取密码系统的输入输出信息，还可以获取密码系统运行时所泄露的一些旁路信息，如电磁信息、时间信息等（图 2）。此时密钥的安全性不仅与算法本身的强度有关，还与运行时泄露的信息有关。

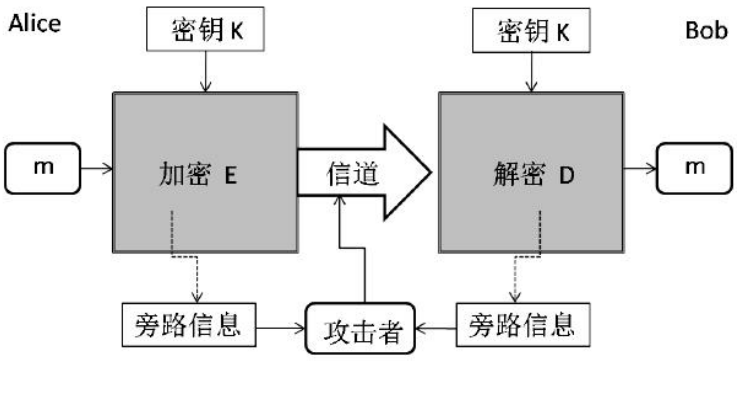


图 2 灰盒攻击

在白盒攻击中，攻击者具有完全控制密码系统运行的能力，密码系统运行过程中产生的一切信息都对攻击者可见（图 3）。当密码算法运行在不

可信平台上时，攻击者完全具有监控密码系统运行过程的能力，如何在此种情况下保护密钥的安全正是白盒密码所要解决的问题。

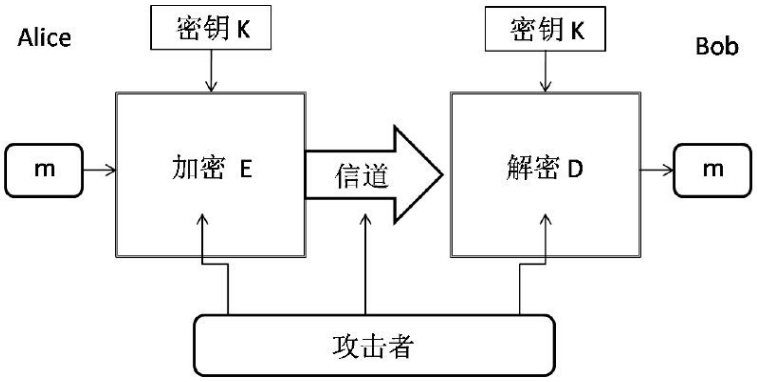


图 3 白盒攻击

2.白盒密码概念

白盒密码学[1-3]（White-box cryptography）由 Chow 等人在 SAC 2002 年会上首次提出，其核心思想是通过白盒密码实现技术，使得密码算法的软件实现与运行环境在对攻击者完全开放的前提下，密码算法所使用的用户密钥仍然不能被攻击者所获取。在提出白盒密码学概念的同时，Chow 等人也针对国际分组密码算法标准 AES 和 DES 给出了相应的白盒实现方案。根据其描述，我们归纳出 Chow 等人对白盒密码的理论定义：

定义 1[1,2]. 白盒密码学是一种混淆技术，即使敌手能对密码学原语的实施和执行平台有完全的控制能力，也无法提取密钥信息。

但是 Brecht Wyseur 则认为，这个定义是在加密算法的背景下提出的，并不具有通用的意义，他们建议白盒实现应该在具体密码学原语的相关安全概念下考虑，因此，他们给出一个新的定义：

定义 2[1-5]. 白盒密码学的目标是实施一个密码学原语，在这个过程中，对于一个计算能力有限的敌手来说，即便是能够完全控制密码学原语的执行，也不会比黑盒模型下的敌手具有任何的优势。

由于白盒密码算法具有良好的兼容性和可维护性，目前已得到了密码学界和工业界的广泛研究与关注。在防火墙、无人机、APP 等应用中，白盒密码算法已作为软件完整性保护、身份认证、密钥管理与分发等功能的关键信息安全保护技术加以实际应用。在白盒密码定义上，我们将能够抵抗白盒攻击的密码算法及其实现称为白盒密码。白盒密码包括了已有密码算法的白盒实现和白盒密码算法。但是，目前在白盒密码上的研究主要都集中在密码算法的白盒实现上，而通常会将密码算法的白盒实现作为白盒密码来看待。

（1）已有密码算法的白盒实现

已有密码算法的白盒实现是指，将已知的密码算法通过白盒密码技术进行设计，使得在白盒攻击环境下，不改变原算法的功能且原算法所希望保证的安全性不受破坏。例如，加密算法希望保证其密钥不会泄露、签名算法希望其签名不会被伪造等。

（2）白盒密码算法

白盒密码算法其实是指一种新的密码算法，它与传统的密码算法不同的是，它能够抵抗白盒攻击环境下敌手的攻击，其本身是一个新的算法，而不是在已存在的算法上的进行白盒安全实现的设计。

3. 白盒密码应用前景

白盒密码致力于构造密码学算法的软件安全实现，使得该实现能够为抵抗白盒攻击提供足够的安全水平。与使用硬件的方式相比，密码算法软实现具有容易扩展、使用便捷、传输方便等优点。随着越来越多的应用软件和运行平台呈现出多元化的趋势，其执行环境也越来越复杂和恶劣，在这种复杂异构的应用环境下，白盒密码发挥作用的舞台也越来越大。发展白盒密码技术具有以下几方面的优势：

提高安全性。终端设备通常是处于一个白盒攻击环境中，传统的密码算法在白盒攻击环境中不再安全，很容易通过对二进制文件的反汇编、静态分析，对运行环境的控制结合使用控制 CPU 断点、观测寄存器、内存分析等来获取密钥。安全的白盒密码方案可在终端完成数据处理，并同时保护密钥安全，可极大提高安全性。

有效的降低成本。可穿戴设备、智能家居等应用场景下的终端设备通常对成本较敏感，若采用硬件密码设备保护这些终端设备必然会增加厂商的成本，甚至导致因为成本而忽略了安全问题。密码算法的软实现将是大势所趋，安全的白盒方案相对于密码硬件具有很大的价格优势。

纯粹的可信关系。移动支付当前通常采用硬件 SE 与 TEE 来保存与执行敏感的数据和进程，以保证安全性，但是 SE 和 TEE 作为安全元件是需要进行管理的，比如 TSM 平台，而平台管理者可能是第三方、芯片厂商、手机厂商等；再如 TEE 开发上提供的 SDK，也常常由第三方提供；还有作为安全元件它们是共享的，上面一般都运行着多家金融机构的程序。采用这些硬件来保护敏感数据和进程的过程中有太多的参与者，太复杂的信任关系。

采用白盒密码则在可以完成硬件相同功能时，无需各类提供商的参与，可以一个应用独享，数据与安全可更好的由应用开发商控制，该技术无论从管理上还是技术上，都构建了一个更简化、更纯粹的可信关系。

4.总结

白盒密码技术具有广泛的应用前景。例如：白盒密码最早是应用在数字版权保护领域，视频行业目前面临最主要的信息安全问题是盗播盗看、广告屏蔽、刷量作弊等盗版带来的版权问题。因此，在非可信的环境下，传统标准加密技术和依赖硬件加密都无法完全有效的保障大规模应用场景下的视频版权安全，而白盒密码成为版权保护的密码技术的重要原因。（作者：秦体红 汪宗斌 北京信安世纪科技股份有限公司）

参考文献

[1] CHOW S, EISEN P, JOHNSON H, et al. White-box cryptography and an AES implementation[C]. In: Selected Areas in Cryptography—SAC 2002. Springer Berlin Heidelberg, 2003: 250－270.

[2] CHOW S, EISEN P, JOHNSON H, et al. A white-box DES implementation for DRM applications[C]. In: Digital Rights Management—DRM 2002. Springer Berlin Heidelberg, 2003: 1－15.

[3] LEPOINT T, RIVAIN M, MULDER Y D, et al. Two attacks on a white-box AES implementation[C]. In: Selected Areas in Cryptography—SAC 2013. Springer Berlin Heidelberg, 2013: 265－285.

[4]MULDER Y D, ROELSE P, PRENEEL B. Revisiting the BGE attack on a white-box AES implementation[J]. IACR Cryptology ePrint Archive, 2013: 2013/450.

[5]XIAO Y Y, LAI X J. A secure implementation of white-box AES[C]. In: Proceedings of 2009 2nd International Conference on Computer Science and Its Applications—CSA 2009. IEEE, 2009: 1－6.

4.2024年暗网态势研究报告：数据泄露趋势与治理挑战

摘要：本报告基于绿盟科技威胁情报中心对2024年暗网数据交易市场的监测和分析，深入探讨了当前数据泄露的现状、趋势及其对国家安全和社会稳定的影响。报告显示，尽管国内数据泄露事件数量有所减少，但泄露数据量却有所增加，特别是在金融、电商、物流、教育等行业以及重要单位组织机构领域。此外，报告还分析了泄露数据的类型、涉及的人群和地区分布，揭示了暗网活跃账号的变化趋势和泄露事件的主要类型。最后，报告提出了加强数据安全治理的建议，以应对日益复杂的网络安全威胁。

引言

随着互联网的快速发展，数据已成为现代社会的重要资产。然而，数据泄露事件的频发不仅威胁个人隐私，还对国家安全和社会稳定构成严重挑战。暗网作为网络犯罪的主要温床，其上的数据交易市场更是各种非法

活动的聚集地。本报告旨在通过对2024年暗网数据泄露态势的全面分析，揭示当前数据安全面临的严峻形势，并为数据相关治理工作提供科学依据。

一、数据泄露总体态势

1.1 数据泄露事件数量与数据量变化

2024年，绿盟威胁情报中心共监测到国内数据泄露事件3,510起，涉及泄露数据量高达581亿条。与去年相比，数据泄露事件数量有所减少，但泄露数据量却呈现上升趋势。这一变化表明，尽管数据安全治理取得了一定成效，但大规模数据泄露的风险依然存在。

1.2 数据交易次数与售卖人员变化

数据显示，2024年数据交易次数减少了37.66%，数据售卖人员减少了34.41%。这一变化反映出国家在数据安全治理方面的努力取得了一定效果，但同时也提示我们，数据交易市场的活跃度仍然较高，需持续加强监管。

1.3 泄露数据涉及人群变化

泄露数据涉及人群整体减少了20.35%。如图1所示，脆弱人群、高净值人群和关键人群仍然是数据泄露的主要目标。这些人群的信息泄露可能导致严重的社会和经济后果，需引起高度重视。人员信息作为许多软件、平台在注册、 登记时的必填项，应用广泛，是数据窃取的主要目标之一。

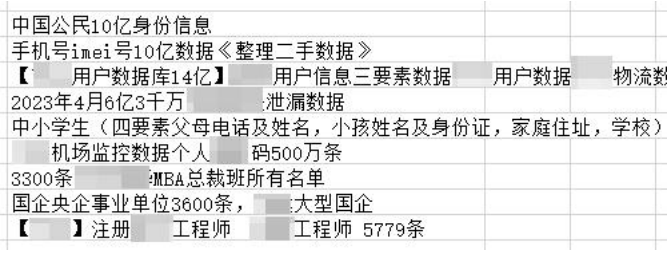


图 2.29 泄露清单示例

二、数据泄露行业分析

2.1 金融、电商、物流、教育等行业的数据泄露情况

如图 2 所示，从泄露事件量角度，2024 年金融、电商、物流和教育行业仍然是数据泄露的重灾区。其中，金融领域的泄露事件尤为严重，主要包括银行用户信息、贷款信息、股票证券投资信息等，这些信息的泄露可能导致直接的经济损失。电商和物流领域的数据泄露则主要涉及平台用户信息、网购订单数据和详细地址信息，覆盖面极广。

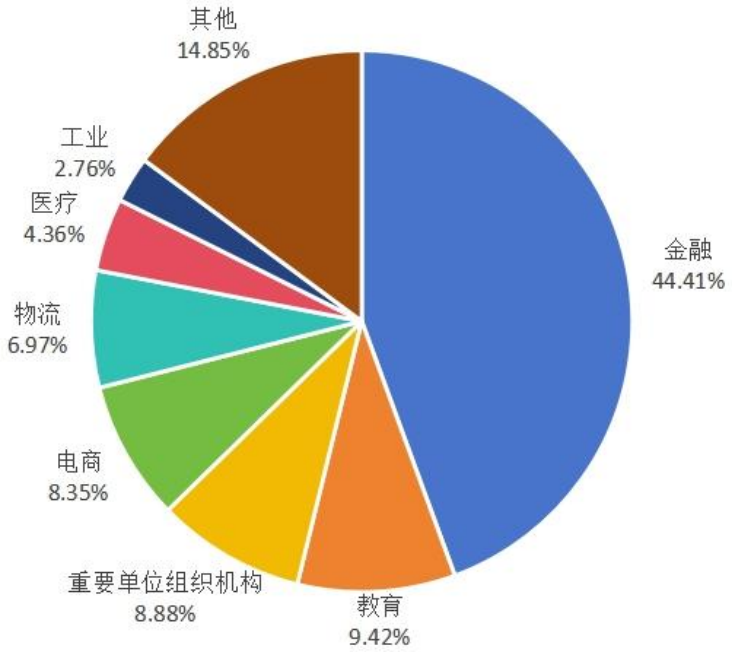


图 2　2024 年国内数据泄露行业统计（泄露事件量）

如图 3 所示，从泄露数据量角度，2024 年泄露数据量较多的行业为电商、物流、金融、重要单位组织机构、教育。

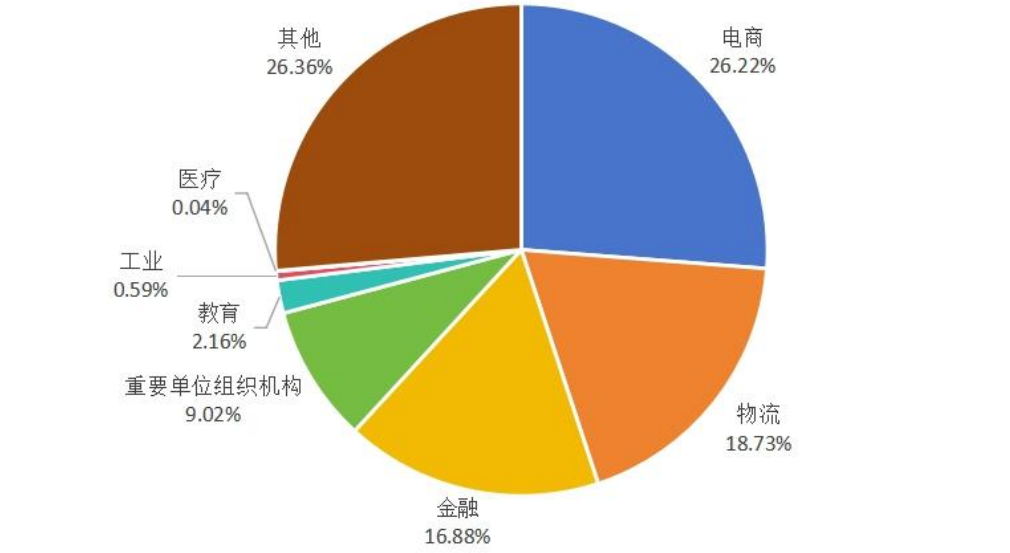


图 3 2024 年国内数据泄露行业统计（数据量）

2.2 重要单位组织机构领域的数据泄露增加

值得注意的是，重要单位组织机构领域的数据泄露事件和泄露数据量均有增加。这些数据主要包含公民信息和内部人员信息，涉及政府机关、研究所、大型企业等。由于其覆盖面广、可靠性强，不法分子很容易在其基础上采取加工、关联等操作，因此这类数据的泄露往往会造成极大的隐患。

三、数据泄露涉及群体分析

3.1 脆弱人群、高净值人群和关键人群的泄露情况

如图 4 所示，脆弱人群（如儿童、老年人、宝妈和大学生）因其消费习惯和防范意识较弱，容易成为不法分子的重点关注对象。高净值人群（如拥有豪车、豪宅的人群）的信息泄露可能导致显著的经济损失。关键人群（如政府工作人员、大型企业员工）的信息泄露则可能对国家和社会造成严重影响。

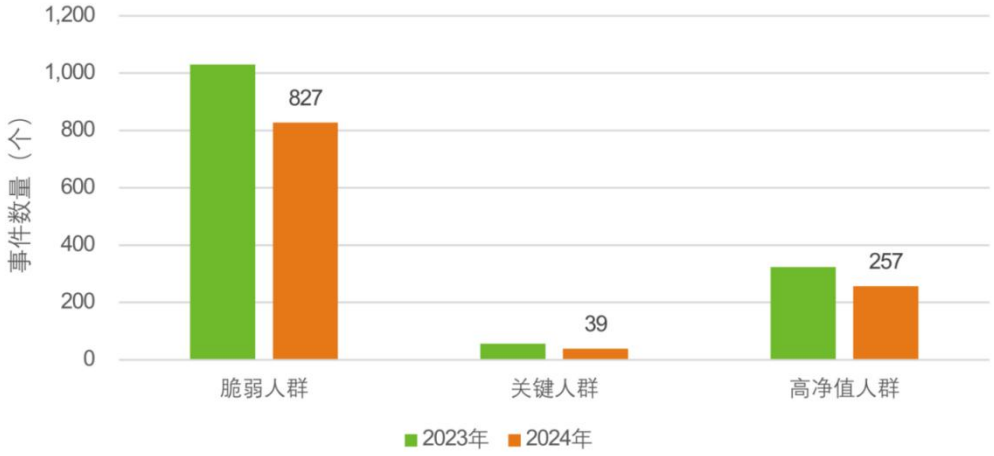


图 4 数据泄露针对人群分布

3.2 不同人群信息泄露的潜在影响

脆弱人群的信息泄露可能导致诈骗、身份盗用等犯罪活动；高净值人群的信息泄露可能导致经济损失；关键人群的信息泄露则可能影响国家安全和社会稳定。因此，针对不同人群的信息保护措施需有所侧重。

四、数据泄露地区分布

4.1 经济发达和人口密集省份的数据泄露情况

如图 5 所示，对比去年来看，数据泄露事件涉及的地区分布没有较大的变化，仍易发生在经济发达和人口密集的省份，如上海市、广东省。从整体数量来看，数据泄露次数有所下降，体现出我国在数据安全领域的治理力度。

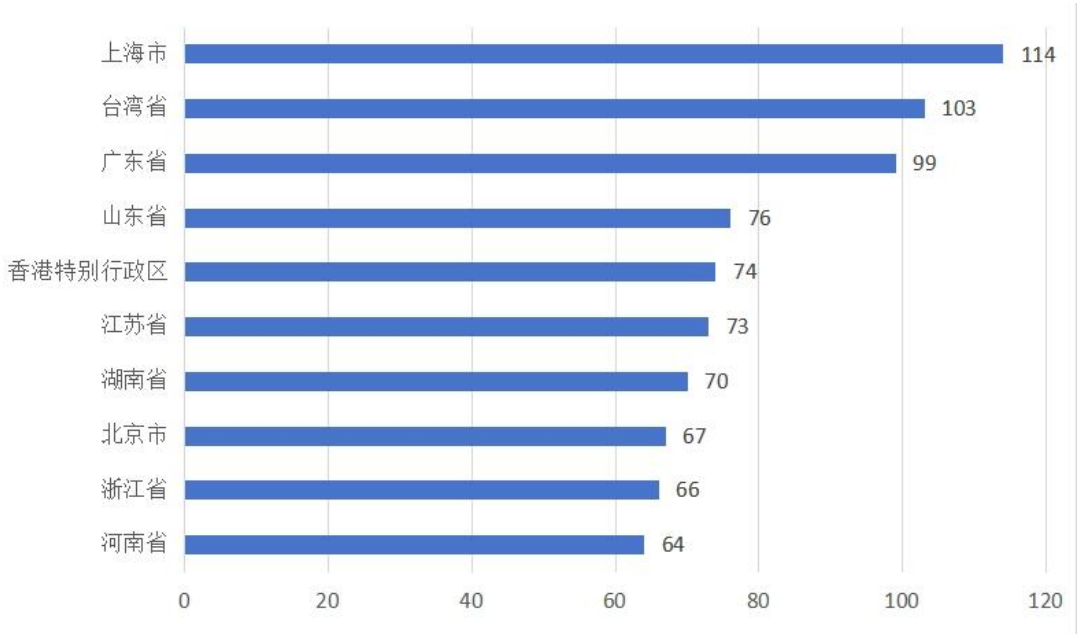


图 5 数据泄露相关省份 TOP10

4.2 各地区数据泄露次数变化及原因分析

与 2023 年相比，上海市的数据泄露次数从第七名上升到了第一名，主要由于几年前泄露的几批重点领域数据被反复售卖。广东省、北京市、四川省的数据泄露次数有所下降，而香港则有所上升。这一变化提示我们，数据安全治理行动需长期持续推进。

五、数据泄露内容分析

5.1 手机号、身份证号等个人信息泄露情况

如图 6 所示，交易者在泄露数据信息中手机号、身份证号、地址、邮箱等涉及个人信息数据字段的泄露较多。其中，手机号、身份证号分别出现了 793 次和 660 次。这两类数据作为许多软件、平台在注册、登记时的必填项，发生泄露的可能性 更大；其中身份证号的重要性更是不言而喻，不法分子更倾向于窃取此类内容。这些内容的 泄露很容易造成电信诈骗、身份盗用等严重后果。

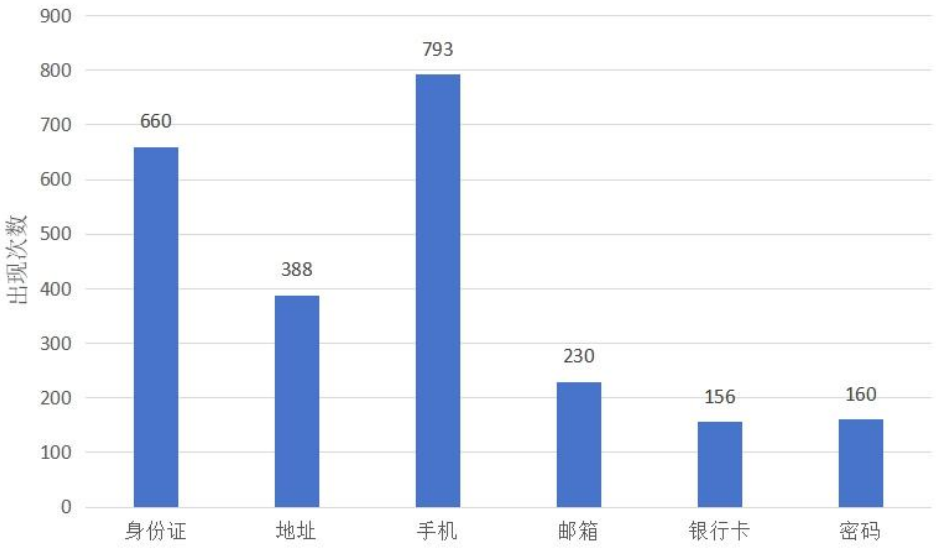


图 6 数据泄露中的已知字段

5.2 数据泄露中的已知字段分布

据绿盟威胁情报统计，交易者在泄露数据信息中手机号、身份证号等涉及个人信息数据的泄露较多。这些内容的泄露很容易造成电信诈骗、身份盗用等严重后果，应该引起相关部门的重视。

六、暗网活跃账号分析

6.1 发布交易信息的账号数量变化

如图 7 所示，据绿盟威胁情报中心统计，2024 年，共发现 509 个账号发布过交易信息，其中 350 个账号只发布过 1～3 次泄露数据，4 个账号发布频次超过 100 次，账号数量约 占 68.76%。与上一年相比，发布者数量明显减少，极端活跃者的发布数量也有所减少。

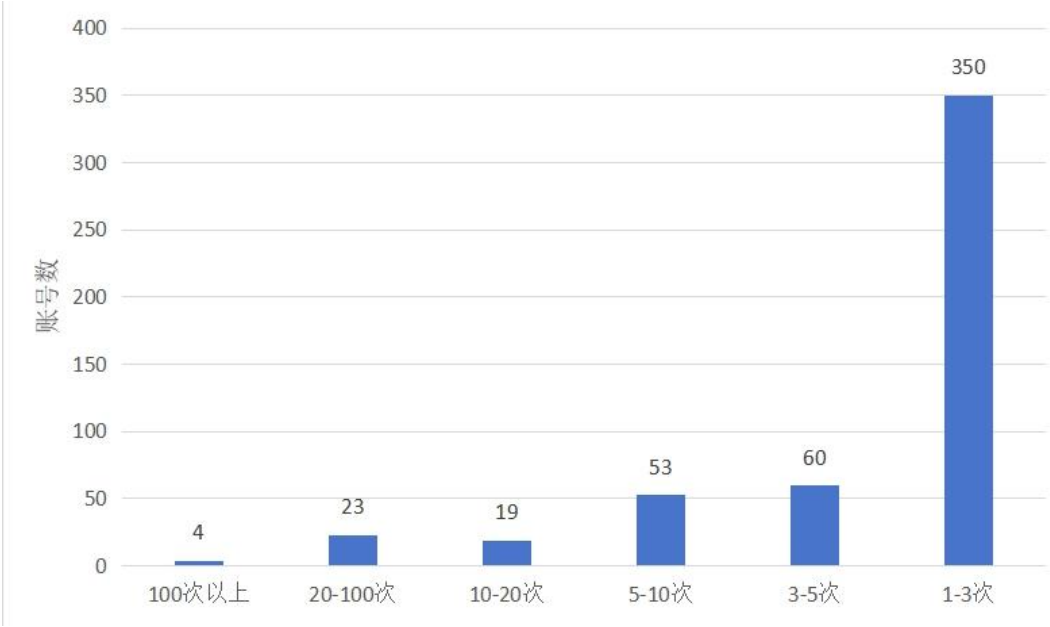


图 7 不同账号发布泄露数据的次数分布

6.2 活跃账号的类型与发布内容

活跃账号主要分为数据代理商账号和特定数据售卖账号。数据代理商账号所售数据的领域分布广泛，通常进行各类数据的转卖、代售等；特定数据售卖账号售卖的数据一般都集中在同一领域内，其背后可能是相关行业的从业人员。

七、数据泄露事件类型分析

7.1 历史数据泄露事件与新数据泄露事件

2024 年的数据泄露事件中，大多为历史数据的二次售卖。历史泄露事件中数据形态除了未售出或已发售但无人购买的数据、数据早已传播但缺乏热度等之外，还包含经过一定的数据处理，如简单去重、分析、提取、加工、组合、混淆等方式，再次进行售卖的情况。

7.2 数据泄露事件类型占比情况

如图 8 所示，据绿盟威胁情报中心统计，在 2024 年数据泄露事件中，历史泄露事件数量超过总量的一半，占比约为 60.45%。无论是新数据泄露，还是历史数据的多次售卖，数据交易市场往往是真假参半的。

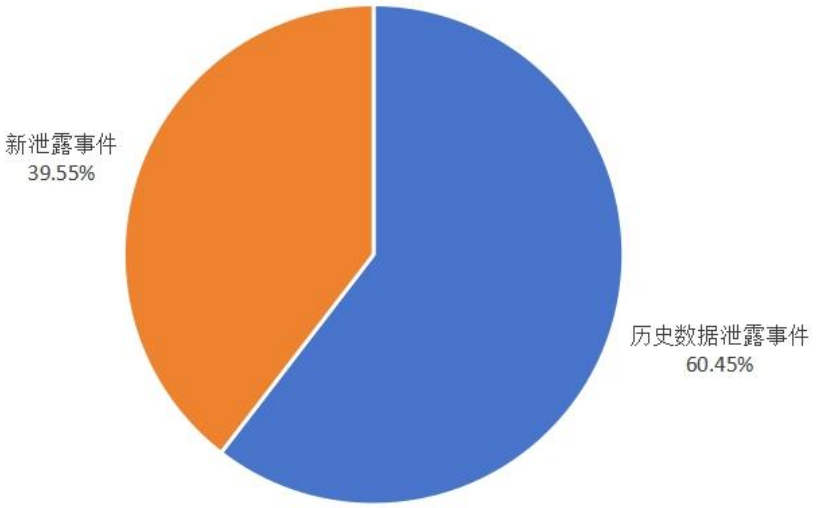


图 8 数据泄露事件类型占比

八、结论与建议

8.1 数据泄露风险下降趋势的积极意义

国内数据泄露风险呈现下降趋势，反映出国家在数据安全治理方面取得的效果。然而，泄露数据量的增加提示我们，数据安全治理仍需加强。

8.2 加强数据安全治理的建议

针对当前数据泄露的严峻形势，建议从以下几个方面加强数据安全治理：一是完善数据安全法律法规，加大执法力度；二是加强数据安全技术研发，提升数据保护能力；三是提高公众数据安全意识，增强自我保护能力；四是加强国际合作，共同应对跨境数据泄露威胁。（作者：郑开发　绿盟科技集团股份有限公司研究员）

特别感谢，绿盟科技威胁情报实验的全体研究员。

参考文献

[1] 绿盟科技威胁情报中心. (2024). 2024 年暗网态势报告.

[2] 国家互联网信息办公室. (2023). 数据安全管理办法.

[3] 中国信息安全测评中心. (2024). 数据泄露事件分析与应对策略.

行业前沿观察二：有关部门严厉打击网上体育“饭圈”问题；网信部门依法查处一批低俗炒作娱乐明星信息账号；国家网信办就 MCN 机构相关业务活动管理规定征求意见 给 MCN 机构戴上监管“紧箍咒”

导读：近日，国家互联网信息办公室发布《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》（以下简称《草案稿》）并公开征求意见。《草案稿》明确了 MCN 机构的法律地位和责任义务，明确禁止其直接或组织、教唆、委托、协助签约的网络账号实施发布网络谣言、煽动网民情绪等行为，给 MCN 机构戴上了监管“紧箍咒”。

网信部门会同体育主管部门持续加大对网上体育饭圈问题治理力度，依法严惩拉踩引战和攻击谩骂等行为，清理违法违规信息 160 万余条，处置账号 7.6 万个，其中关闭账号 3767 个，切实维护清朗网络空间，为运动员积极备战和体育赛事顺利举办营造良好舆论氛围。

此外，网信部门还持续打击文娱领域“饭圈”乱象，近期，督促网站平台依法依约关闭和长期禁言处置“超能摄影阳阳”“摄影刘大锤”“老板王大发”“娱乐有饭”“追星少女卓小宴”“贴小君”“娱三少”“ba 哥专用”“Real 皮皮王”“八酱日常”“明星娱乐一线”“明星娱乐最前线”“娱蜀黍”等一批低俗炒作绯闻丑闻八卦的违法违规账号。

关键词：互联网、MCN、网络安全、网信办、“饭圈”

1. 有关部门严厉打击网上体育“饭圈”问题

近期，网信部门会同体育主管部门持续加大对网上体育饭圈问题治理力度，依法严惩拉踩引战和攻击谩骂等行为，清理违法违规信息160万余条，处置账号7.6万个，其中关闭账号3767个，切实维护清朗网络空间，为运动员积极备战和体育赛事顺利举办营造良好舆论氛围。

严打挑动互撕、引战的“大粉”“粉头”账号。工作中发现，“时**安”“李**干”“乌**冰”等“粉头”账号频繁侮辱谩骂运动员、教练员，设置所谓“唯粉”标准鼓动“捧一踩一”，有些还打着“维权”等旗号恶意批量举报投诉，甚至组织扰乱公共秩序的线下聚集活动等。网信部门要求网站平台依法依约对存在上述问题的1376个违法违规账号予以关闭处置，同步解散相关违规群组5803个。

惩处编造谣言、恶意炒作的“自媒体”账号。“贺*龙”“杜*言”“舜**Sean”“春**影”“星**梦”等“自媒体”账号多次炮制有关人员选拔、赛事保障等谣言信息，通过恶意解读赛场行为挑动评论区“骂战”，虚构拼接低俗图文信息炒作“运动员CP”，煽动网民情绪，无底线博取流量。网信部门指导网站平台依法依约对1500余个相关“自媒体”账号采取关闭、禁言和暂停营利权限等措施。

清理冒用运动员名义的账号群组。据反映，一些人员打着国家队运动员、教练员等旗号开设或者组建专门账号、群组、贴吧和超话，诱导非理性应援，挑动群体对立，甚至借此敛财牟利，对广大网民特别是未成年人造成负面影响。国家队运动员、教练员纷纷发声，明确表示解散粉丝群组，

呼吁聚焦赛场、支持体育活动本身。在此基础上，网信部门会同体育主管部门加大管理力度，督促网站平台关闭假冒运动员、教练员开设的账号531个，解散违规建立的粉丝群组3226个、超话1264个、贴吧336个。

查处一批违规售卖涉运动员商品的商家店铺。在电商和社交平台发现，一些不法分子违法售卖运动员联系方式、证件号码、行程安排等个人信息，一些账号违规提供运动员有偿代拍、私拍活动等商品服务，一些店铺假冒仿冒运动员签名制作所谓“限量版”球拍、运动鞋借机牟取暴利。网信部门督促网站平台进行跨平台联动处置，累计下架违规售卖商品123件，关闭店铺6家。

及时处置存在不良导向的产品功能。网信部门督促网站平台密切跟踪研究网上体育饭圈问题新情况、新表现，动态调整优化产品功能和社区规则。工作发现，个别平台违规上线对运动员容貌、人气进行恶意评比的榜单，推出诱导网民刷量控评、应援集资的“签到”“打卡”等功能。网信部门督促相关平台深入开展整改，及时下线违规产品功能，有力遏制相关问题反弹风险。

强化线上线下联动处置工作。为防范化解网上体育饭圈问题风险，网信部门与体育主管部门召开会议，就体育饭圈问题整治工作进行专门部署，并建立协同联动工作机制，围绕体育领域重要赛事活动举办，加强线索移交、问题研判和会商处置，切实形成工作合力。将发现的涉违法犯罪问题线索，及时移交有关部门查处。

下一步，网信部门将会同体育主管部门持续深化网上体育饭圈乱象治理，督促网站平台切实履行主体责任，严惩违法违规账号，对问题突出、治理不力的平台，将依法从严采取处置处罚措施。同时，也鼓励广大网民更多关注和支持体育赛事活动本身，自觉抵制体育饭圈不良行为，积极参与监督举报，共同营造清朗网络空间。（来源：中国网信网）

2. 网信部门依法查处一批低俗炒作娱乐明星信息账号

网信部门持续打击文娱领域“饭圈”乱象，近期，督促网站平台依法依约关闭和长期禁言处置“超能摄影阳阳”“摄影刘大锤”“老板王大发”“娱乐有饭”“追星少女卓小宴”“贴小君”“娱三少”“ba 哥专用”“Real 皮皮王”“八酱日常”“明星娱乐一线”“明星娱乐最前线”“娱蜀黍”等一批低俗炒作绯闻丑闻八卦的违法违规账号。

一段时间以来，相关账号通过偷拍、跟拍明星非公开行程，发布未经核实的“爆料”信息；或以“知情人”名义编造、转发不实信息，或借“标题党”和虚假预告等形式，制造噱头，恶意博取流量；或使用暗语、隐喻等手段，无底线炒作明星八卦信息，严重破坏网络生态。

下一步，网信部门将继续压实网站平台主体责任，督促严格落实《网络信息内容生态治理规定》《关于进一步加强娱乐明星网上信息规范相关工作的通知》等要求，聚焦泛娱乐化倾向和低俗炒作现象，坚决整治流量至上和“饭圈”乱象，加大网络执法力度，努力营造积极向上的网络环境。

同时，欢迎广大网民积极参与监督举报，共同营造清朗网络空间。（来源：中国网信网）

3.国家网信办就MCN机构相关业务活动管理规定征求意见 给MCN机构戴上监管“紧箍咒”

随着短视频平台和网红经济的快速发展，MCN机构（网络信息内容多渠道分发服务机构）的市场规模迅速扩大。与此同时，部分MCN机构因过度追求流量，屡屡挑战公序良俗甚至法律底线，行业乱象亟待整治。

近日，国家互联网信息办公室发布《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》（以下简称《草案稿》）并公开征求意见。《草案稿》明确了MCN机构的法律地位和责任义务，明确禁止其直接或组织、教唆、委托、协助签约的网络账号实施发布网络谣言、煽动网民情绪等行为，给MCN机构戴上了监管“紧箍咒”。

行业乱象亟待整治

MCN机构是指在网络信息内容服务平台入驻，为网络信息内容创作者提供策划、制作、营销等相关服务的机构。

简单来说，MCN机构就像是网络信息内容创作者的“经纪人”，他们负责管理、运营创作者的网络账号，帮助账号提高曝光度、扩大受众群体，以及提供专业的内容制作，并协助账号与广告主、品牌方合作对接。

从MCN机构的盈利方式看，广告发布、直播打赏、知识付费等都很常见，还有一些MCN机构通过自创品牌、推出技术服务等新模式盈利，但不

论哪种形式，最终都离不开流量：账号是否成功，看流量；有没有广告合作，看流量……伴随行业的激烈竞争，在“唯流量论”驱使下，部分MCN机构的“骗人套路”层出不穷。

“越苦越惨，流量越大”，这是有的MCN机构策划视频情节时遵循的原则。近几年，“假冒骑手摆拍卖惨”等涉外卖员群体的谣言事件频繁出现，有的谣言贴上“失业被迫送外卖”等标签抓眼球，有的摆拍捏造“骑手深夜带患儿跑单”等桥段博同情。相关调查显示，从道具采购到剧本设计，再到视频拍摄、炒作传播，一条营造“骑手苦情人设”的灰色产业链已经形成。

专家指出，这些“卖惨”方式能够有效调动用户的共情情绪，且这类“剧本”的编写成本也很低。倘若平台没有对这些以流量为导向的算法推荐机制进行约束和调整，很有可能就会诱发这类“卖惨”的网络信息快速传播。

部分MCN机构还从事侵害用户个人信息等违法行为。不久前，江西省赣州市信丰公安依法查处了8家涉嫌非法获取公民个人信息的MCN机构，这些机构利用非法软件购买实名账号并批量登录，在某网络平台上转发搬运其他平台文章，获取网络流量从而牟利。

中国社会科学院大学互联网法治研究中心主任刘晓春评论称，MCN机构的这些行为不仅扰乱了网络秩序，也对社会风气和公众利益造成不良影响，严重破坏网络内容生态，必须严厉整治并通过规范化的管理，促进其健康有序发展。

监管覆盖全链条

加大对网络不法行为的打击，已成社会各方共识。为遏制MCN行业的种种乱象，有关方面一直在行动。例如，中央网信办部署2025年“清朗”系列专项行动，重点整治短视频领域恶意营销，打击虚假摆拍、虚假人设、虚假营销、炒作争议性话题等。

此次，国家网信办出台专门的规范性规定，将为MCN机构的规范化发展提供有力指引，也令监管部门开展工作更加有章可循、有据可查。

笔者梳理发现，《草案稿》明确了MCN机构的法律地位和责任义务，为MCN机构的行为边界和责任承担建立了全面、清晰的规范体系，要求其在提供策划、制作、营销、经纪等相关服务时，必须遵守法律法规，尊重社会公德。

在准入门槛方面，《草案稿》提出，从事表演、节目等活动的MCN机构应当依法依规取得相关从业资格或服务资质。

内容管控方面，《草案稿》为MCN机构划定了明确的红线，列出了禁止其直接或组织、教唆、委托、协助签约的网络账号实施翻炒旧闻旧事、利用“网红儿童”牟利、宣扬不良价值观、渲染炒作突发案事件等12种行为，覆盖内容生产全链条。

《草案稿》明确了MCN机构的信息披露等机制。要求MCN机构应当与旗下网络账号进行绑定，在网络账号注册、拟变更账号信息等环节进行适当的信息披露，增加透明度。刘晓春表示，通过一系列绑定和披露的要求，能够实质性建立MCN机构和旗下账号关联关系的管理、披露、治理规范体

系，有效提高面向公众和监管机关的透明度，有效防范MCN机构不当批量操纵账号导致的乱象。

值得一提的是，《草案稿》还强化了网络平台在落实MCN机构规范和管理过程中的主体责任，要求平台建立对于MCN机构规范和管理的一整套治理机制。比如，平台应当根据MCN机构合规情况、旗下账号数量及其粉丝总数量等指标维度，建立分级管理制度，并采取相应管理措施防范信息内容风险。业内人士指出，这将督促平台完善内部管理流程，既有助于提升平台自身的治理能力，也能提升MCN机构的专业水平和服务质量。

“《草案稿》的出台标志着中国互联网内容产业将从‘野蛮生长’步入‘精细化治理’阶段。”中国政法大学网络与新媒体研究所所长郑满宁说，“这些新规的实施将大幅减少虚假信息和不良内容的传播，从而净化网络环境，提升行业的公信力。”

规范治理促健康发展

MCN机构的规范化发展是其长远发展的必由之路，也是互联网内容生态健康发展的必然要求。专家指出，《草案稿》的出台，将为整个行业带来诸多利好。

在内容质量提升方面，新规将促使MCN机构更加注重内容的合规性和质量，减少低俗、虚假、误导性内容的传播，提升整体内容质量。

相应地，内容审核加强，也将增加机构的运营成本，未来，中小型MCN机构将面临洗牌。业内人士分析，新规正是通过制定严格的规则，筛选符

合要求并愿意合规发展的MCN机构，唯有主动拥抱合规、深耕内容价值的MCN机构方能发展壮大。

在新规的管理下，一些机构的不规范运营模式或将调整。

“新规出台后，以往依赖流量造假等不规范商业模式的MCN机构，需要摒弃旧模式，重新探索可持续的变现方式。”郑满宁建议，未来，MCN机构一方面要依托技术赋能实现“节流”，强化合规体系与技术能力建设，采用AI审核、区块链存证等合规技术降低企业成本；另一方面，要积极探索广告、电商、知识付费等多种变现模式以求“开源”。

刘晓春指出，通过规范MCN机构和网络平台，不仅有利于提升网络空间的整体质量，还能为用户创造更好的网络体验，促进网络信息内容生态良性发展。“期待《草案稿》经法定程序后落地实施，为MCN机构的健康有序发展提供制度支撑，也希望MCN机构和网络平台都能以此为契机，更加聚焦内容创新与价值传递，为网络内容行业的发展和治理注入源源不断的正能量。”（来源：人民日报海外版）

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，进行评选活动，开设培训会，举行税宣会等。广东省网络空间安全协会：税企“面对面”税宣会在协会顺利举行；北京网络空间安全协会开展京粤汇"网安精英系列培训班（第五期）---"数据安全保护培训；广东省网络空间安全协会举行广东省科协信创联合体主席团工作会议；湖北省网络和数据安全协会：深化跨国合作！新加坡代表团与协会共谋发展新机遇；西藏自治区互联网协会：2024 年度西藏自治区“最美通信人”评选活动圆满完成；苏州举办“海棠花红 e 心向党”网络人士红色基地行活动等。

关键词：年会、会长会议、团体标准、网络安全、信息安全

1. 广东省网络空间安全协会：税企“面对面”税宣会在协会顺利举行

为深入学习贯彻党的二十届三中全会精神，践行致力服务会员、服务社会，帮助广大会员单位、相关企业纳税人及时了解掌握税务政策，4 月 8 日，由广东省网络空间安全协会、国家税务总局广州市越秀区税务局联合举办的税企“面对面”税宣会在协会举行。越秀区税务局多个部门派员参加宣讲，广东省网络空间安全协会常务副会长方满意，秘书长周贵招，副秘书长吴一丰、蔡舒婷参加税宣会。受协会党支部书记林勇忠委托，协会党支部专职副书记、执行秘书长黄汝錫主持税宣会时代表协会向越秀区税务局表示感谢。

本次宣讲会以《服务粤港澳大湾区建设科技创新税收优惠政策宣讲》为主题，从软件产品增值税即征即退政策、高新企业企业所得税优惠政策、个人所得税优惠政策、“走出去”税收指引介绍四方面，通过分析举例、流程演示等方式，全方位开展政策解读，回应企业涉税费诉求，为粤港澳大湾区“走出去”纳税人提供全方位的参考。（来源：广东省网络空间安全协会）

2. 广东省地方标准批准发布公告 网络安全合规咨询服务规范等13项标准发布

近年来，全球掀起数据安全、网络安全与个人信息保护的立法热潮，对企业提出了更高的网络安全合规性等要求。随着我国《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》为核心的网络安全法律法规体系逐步建立健全，我国多部数据及网络安全标准也已经发布或者正在制定中，相关的标准体系正趋向完善，但聚焦于研究网络安全合规咨询服务标准的甚少，基于前期标准研究成果起草规范网络安全合规咨询服务标准，以填补网络安全合规咨询服务在地方标准上的空白，针对数据安全合规咨询、个人信息保护合规咨询等网络安全合规咨询服务，进一步明确其应具备的基本能力、专业能力和服务过程能力要求。《网络安全合规咨询服务规范》的发布，填补了这一空白。

近日，《网络安全合规咨询服务规范》由广东省市场监督管理局批准发布，同期发布的地方标准涵盖网络安全合规咨询服务规范、乡村旅游民宿质量规范、危险化学品储存装置安全使用技术规范等13项地方标准。

《网络安全合规咨询服务规范》由广东省网络空间安全协会作为主导单位，广东省科学技术厅作为标准归口省级行政主管部门和提出单位，广东省网络空间安全标准化技术委员会作为归口标准化技术委员会。本标准由广东省网络空间安全协会、公安部第三研究所、广东电网有限责任公司广州供电局、网安联认证中心有限公司、广州华南检验检测中心有限公司等单位共同参与了该标准的起草工作。该标准规定了网络安全合规咨询服

务类型、通用评价要求和专业评价要求等内容，填补了网络安全合规咨询服务在地方标准上的空白，具有较高的实用性和可操作性。

3. 北京网络空间安全协会开展京粤汇"网安精英系列培训班（第五期）---"数据安全保护培训

为深入贯彻2025年全国网信工作会议"打造新时代网络强国战略支点"精神，落实专业技术人才继续教育要求，北京网络空间安全协会与广东省网络空间安全协会联合主办的"京粤汇"网安精英系列培训班（第五期）——数据安全保护培训于2025年4月10日通过线上直播形式成功举办。来自京粤两地网络安全领域的技术骨干齐聚云端，共同探讨数字经济时代下的数据安全保护策略，助力构建全域数据安全防护体系。

作为"京粤汇"品牌的深化实践，本期培训进一步强化了京粤两地网络安全协同创新机制。通过专家资源共享、技术经验互通，两地正加速构建覆盖数据全生命周期的安全防护生态，为数字经济高质量发展筑牢安全底座。未来，双方将持续聚焦行业热点，优化培训体系，培育更多复合型网络安全精英，为推进网络强国战略注入新动能。（来源：北京网络空间安全协会）

4. 广东省网络空间安全协会举行广东省科协信创联合体主席团工作会议

为进一步凝聚共识、注入动能，拓展工作新领域，助力推动广东省信创产业高质量发展，3 月 28 日，广东省科协信创联合体主席团工作会议在广东省网络空间安全协会举行，会议总结联合体阶段性成果，谋划下一阶段重点工作。联合体主席单位广东省网络空间协会创会会长黄丽玲，副会长方满意、黄志豪、成珍苑，秘书长周贵招，监事长张伟以及副主席单位广东省民营医院行业协会会长何奔，广东省电子信息行业协会副秘书长张静玲，省高性能计算学会秘书戴思正，省机器人协会秘书处办公室副主任禤慧洁，协会党支部专职副书记、执行秘书长黄汝锡，副秘书长程晓峰、吴一丰、蔡舒婷等参加会议。

会议指出，广东省科协信创联合体要在广东省科协的支持指导下积极开展工作，围绕中心服务大局，面向国家重大发展战略，面向省委、省政府的发展重点，聚焦 AI 新热潮，找准信创联合体工作的切入点，为创新驱动发展服务，在实现高质量发展中展现新作为；发挥大联合大协作的集成优势，将五个工作委员会的优质资源结合起来，在学术交流、科学普及、人才培养、科技成果评价、标准研制等方面发挥重要作用；要按照联合体的工作规范，建立良好的运行机制，确保联合体正确的发展方向，建立责任共担，利益共享的合作发展模式，努力形成相互促进相辅相成的合作共赢发展机制。

工作会议上，联合体的主席团成员针对省科协信创联合体的章程与2025年信创联合体的工作规划进行了讨论与征集修改意见，对信创联合体以及相关工作委员会的具体工作目标达成初步意见。（来源：广东省网络空间安全协会）

5. 湖北省网络和数据安全协会：深化跨国合作！新加坡代表团与协会共谋发展新机遇

近日，新加坡代表团远赴湖北，与湖北省网络和数据安全协会展开深入交流，围绕网络与数据安全的前沿发展、人才培养及产业合作等议题，共同探讨创新模式，为未来合作奠定坚实基础。

交流会上，协会会长王耀发　先生对代表团的到来表示热烈欢迎，并介绍了协会在网络安全技术研究、人才培养及安全防护体系建设方面的最新进展。新加坡代表团分享了网络数据安全领域的先进经验，强调产学研深度融合的必要性。并从文化交流与企业社会责任的角度，探讨如何通过文化纽带深化中新两国的网络安全合作，为行业发展提供新思路。（来源：湖北省网络和数据安全协会）

6. 西藏自治区互联网协会：2024年度西藏自治区“最美通信人”评选活动圆满完成

为全面贯彻落实党的二十大精神，弘扬通信人的职业精神和社会责任，集中展示近年来西藏自治区通信人在行业建设发展过程中的突出贡献和优

秀事迹，在西藏自治区党委宣传部、西藏自治区总工会　的指导下，西藏自治区通信行业协会、西藏自治区互联网协会在全区组织开展的2024年度西藏自治区“最美通信人”评选活动于2025年3月26日圆满完成。

经过各位评委严格初评和终评，最终有20位从中脱颖而出，被评为“最美通信人”。此次评选活动的圆满完成，不仅为西藏自治区通信行业树立了榜样，更激励着我区广大通信工作者向先进看齐、向榜样学习，在新时代的征程中，勇挑重担，砥砺前行，为西藏通信事业的发展贡献更多的智慧和力量。（来源：西藏自治区互联网协会）

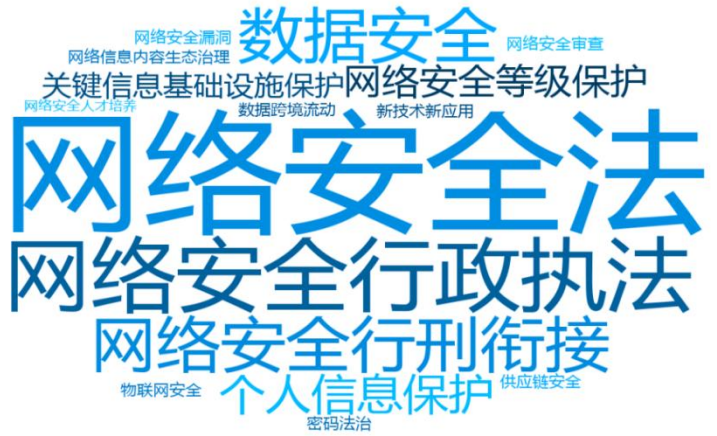
7. 苏州举办“海棠花红 e心向党”网络人士红色基地行活动

为深入学习贯彻习近平总书记在江苏代表团审议时的重要讲话和全国两会精神，深刻领会内涵实质，进一步激励全市网络人士不断提升政治自觉、思想自觉和行动自觉，4月2日，由市委网信办、市互联网企业行业党建专委会主办，张家港市委网信办、苏州市互联网协会承办的“海棠花红e心向党”网络人士红色基地行活动在张家港顺利举行。全市行业企业、网络人士代表30余人参加。（来源：苏州市互联网协会）

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

……