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）

2024年7月第7期（总第12期）

2024年7月11日

**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网安联发展工作委员会
**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。

# 目　录

**境内前沿观察一：安全事件 ..... 1**

1. 中巴发布联合声明，将持续拓展两国政府间科技合作 ..... 2

2. 网络法治保障高质量发展新闻发布会举行：我国已制定出台网络领域立法 150 多部 ..... 3

3. 国家互联网信息办公室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》 ..... 4

**境内前沿观察二：政策立法 ..... 5**

（一） 部委层面动向 ..... 7

1. 民航局发展计划司发布《民航数据管理办法（征求意见稿）》《民航数据共享管理办法（征求意见稿）》 ..... 7

2. 工信部等四部门联合印发《国家人工智能产业综合标准化体系建设指南（2024 版）》 ..... 8

3. 九部门印发《关于拓展跨境电商出口推进海外仓建设的意见》，允许跨境电商、跨境支付等应用场景数据有序自由流动 .. 9

4. 国家互联网信息办公室等四部门印发《网络暴力信息治理规定》 ..... 9

5. 全国网安标委发布《网络安全标准实践指南—敏感个人信息识别指南（征求意见稿）》 ..... 10

6. 全国网安标委发布《网络安全技术 关键信息基础设施安全保护能力指标体系（征求意见稿）》 ..... 11

7. 全国网安标委发布《数据安全技术 数据安全和个人信息保护社会责任指南（征求意见稿）》 ..... 12
（二） 地方层面动向 ..... 12
1. 广东省人民政府办公厅印发《广东省关于人工智能赋能千行百业的若干措施》 ..... 12
2. 广东省委办公厅、省政府办公厅印发《关于构建数据基础制度推进数据要素市场高质量发展的实施意见》 ..... 13
3. 陕西省工业和信息化厅印发《陕西省加快推动人工智能产业发展实施方案（2024—2026 年）》 ..... 14
4. 北京市人大常委会通过《关于进一步加强本市反电信网络诈骗工作的决定》 ..... 15
5. 北京市经济和信息化局发布《北京市自动驾驶汽车条例（征求意见稿）》，提出网络与数据安全保护要求 ..... 16
6. 四川省成都市人大常委会公布《成都市数据条例》 ..... 17
7. 内蒙古自治区人民政府印发《内蒙古自治区公共数据管理暂行办法》 ..... 18
8. 江西省工业和信息化厅印发《江西省工业领域数据安全能力提升实施方案（2024—2026 年）》，将强化数据安全监督执法 19
9. 海南省委网信办发布《数据出境安全评估申报工作指引（第二版）》《个人信息出境标准合同备案指引（第二版）》 ..... 20

10. 海南省委网信办发布《海南自由贸易港国际数据中心发展条例（公开征求意见稿）》 ..... 21
**境内前沿观察三：治理实践 ..... 22**
（一） 公安机关治理实践 ..... 24
1. 全国公安机关视频会议召开，要求对电信网络诈骗犯罪紧抓不放、乘胜追击 ..... 24
2. 因未落实网络安全保护义务导致违法信息传播，青海省西宁市警方对一公司进行处罚 ..... 24
3. 因网站被篡改等违法行为，甘肃甘州公安对两家公司进行处罚 ..... 25
4. 因未履行数据安全保护义务，甘肃甘州公安处罚 6 家酒店 26
5. 内蒙古乌兰浩特警方破获特大网络传播淫秽物品牟利案，涉案资金流水 15 亿元 ..... 26
6. 四川省南充市仪陇县公安破获一起特大破坏计算机信息系统案，涉案金额 1.2 亿余元 ..... 27
7. 四川省遂宁市大英县警方打掉一个为“标题党”恶意引流提供技术帮助的网络犯罪团伙 ..... 28
8. 四川省泸州市警方连续破获三起侵犯应届毕业生个人信息案件 ..... 29
9. 浙江丽水云和县警方破获一起非法利用软件抢购电商平台飞天茅台酒案 ..... 30

（二） 网信部门治理实践.....31
1. 中央网信办召开全国重点商业网站平台管理工作会议... 31
2. 国家网信办发布“清朗·优化营商网络环境一整治涉企侵权信息乱象”专项行动典型案例.....32
3. 北京市网信办严厉打击违法违规“自媒体”账号 9000 余个.....33
4. 上海市委网信办发布专项行动阶段性成果，属地网站平台清理违法外链上百万条.....34
5. 陕西网信部门依法查处一批网络违法违规案件.....34
（三） 通信管理部门治理实践.....35
1. 工信部、浙江省通信管理局通报问题 APP.....35
2. 上海市通信管理局印发通知，纵深推进“浦江护航”数据安全专项行动.....36
3. 上海市通信管理局印发通知，开展 2024 年上海市电信和互联网行业网络和数据安全检查.....37
4. 江苏省通信管理局印发方案，开展江苏省“龙磐 2024”网络和数据安全专项行动.....38
5. 浙江省通信管理局印发通知，开展 2024 年电信和互联网行业网络和数据安全检查.....39
（四） 其他部门治理实践.....40

1. 因数据安全管理不足等问题，国家金融监督管理总局对交通银行罚款160万元 ..... 40
2. 浙江省云和县法院审理一起侵犯公民个人信息案，一公司组织员工购买70余万条个人信息充数 ..... 41
3. 广东省湛江市启动“湛盾—2024”攻防演练活动 ..... 42
4. 因数据治理问题，农行、浦发银行、徽商银行宁波分行被处罚 ..... 43
5. 国家计算机病毒应急处理中心发布15款移动APP隐私不合规情况 ..... 44
**境外前沿观察：月度速览十则 ..... 46**
1. G7峰会国家联合发布《七国集团领导人普利亚公报》，涉及网络安全、人工智能等议题 ..... 47
2. 韩国个人信息保护委员会等六机构联合签署《网络钓鱼防范谅解备忘录》，强化跨机构合作治理 ..... 48
3. 欧盟数据保护监督机构发布《生成式人工智能数据合规指引》48
4. 美国国土安全部发布《2024-2025年战略指南》，对关键基础设施安全保护进行部署安排 ..... 50
5. 美国能源部发布《供应链网络安全原则》 ..... 50
6. 因使用个人数据训练人工智能模型被多次投诉，Meta暂停欧洲人工智能模型开发 ..... 51

7. 因在承包政府系统上线前未做安全测试，美国两家知名企业被罚 8200 万元 ..... 52
8. 印度特伦甘纳邦警察局应用程序遭网络攻击，大量警察和犯罪分子个人数据泄露 ..... 53
9. 美国联邦储备系统疑遭勒索软件攻击，泄露 33TB 敏感数据 . 53
10. 印尼国家数据中心遭勒索攻击，赎金 800 万美元 ..... 54
**行业前沿观察一：2024 网民网络安全感满意度调查活动样本采集工作于 7 月 17 日启动、中央网信办启动“清朗·2024 年暑期未成年人网络环境整治”专项行动、“第六届互联网辟谣优秀作品”揭晓、《中国互联网发展报告（2024）》正式发布 ..... 55**
1. 2024 网民网络安全感满意度调查活动样本采集工作于 7 月 17 日启动 ..... 56
2. 中央网信办启动“清朗·2024 年暑期未成年人网络环境整治”专项行动 ..... 57
3. “第六届互联网辟谣优秀作品”揭晓 ..... 59
4. 《中国互联网发展报告（2024）》正式发布 ..... 60
**行业前沿观察二：各地协会动态 ..... 63**
1. 湖北省信息网络安全协会：将在世界大安全博览会举办活动 64
2. 西藏自治区互联网协会：主办 2024 年第二届西藏自治区数字教育发展大会 ..... 64

3. 武汉市网络安全协会：举办在汉高校网络安全应用场景供需对接会 ..... 65

4. 北京网络行业协会：圆满举办协会第四届第三次会员代表大会暨理事会 ..... 66

5. 辽宁省信息网络安全协会：成功举办网络安全专场招聘会 .... 66

6. 上海市信息网络安全管理协会：发起 2024 年度“新耀东方”风采人物事迹征集活动 ..... 67

7. 上海市信息安全行业协会：圆满召开协会第五届第四次会员大会暨 2023 年度表彰大会 ..... 68

8. 湖南省网络空间安全协会：成立协会网络安全等级保护工作专委会 ..... 68

9. 揭阳网络空间安全协会：承办 2024 年“全国科技工作者日”网络数据安全学术交流会 ..... 69

10. 重庆信息安全产业技术创新联盟：成功举办软件供应链安全现状、发展及人才培养讲座 ..... 70

# 境内前沿观察一：安全事件

导读：6月，中国与巴基斯坦伊斯兰共和国发布联合声明。声明表示，双方愿加强人工智能领域政策协调，深化相关务实合作，协同促进人工智能技术发展。双方一致认为，国际社会应秉持发展和安全并重原则，通过对话协商与平等合作，携手构建开放、公正、有效的人工智能治理机制，使人工智能技术为造福各国人民、促进文明进步发挥积极作用。

国家互联网信息办公室与德国数字化和交通部部长签署《关于中德数据跨境流动合作的谅解备忘录》。双方将建立“中德数据政策法规交流”对话机制，加强在数据跨境流动议题上的交流，为两国企业营造公平、公正、非歧视的营商环境。

网络法治保障高质量发展新闻发布会在京举行。发布会上表示中国已经制定出台网络领域立法150多部，形成以宪法为根本，以法律法规为依托，以传统立法为基础，以网络专门立法为主干的网络法律体系，搭建中国网络法治的“四梁八柱”，为网络强国建设提供坚实的制度保障。同时，不断拓展网络普法新格局，加强优质普法作品创作传播，打造网络普法品牌，培育网络法治文化，形成亿万网民参与普法、普法惠及亿万网民的良好局面。

关键词：中巴联合声明、人工智能治理、网络法治、数据跨境流动

## 1. 中巴发布联合声明，将持续拓展两国政府间科技合作

6月4日至8日，巴基斯坦伊斯兰共和国总理夏巴兹·谢里夫对中国进行正式访问。期间，《中华人民共和国和巴基斯坦伊斯兰共和国联合声明》发布。

声明指出，双方对中巴信息技术产业联合工作组第二次会议取得的积极成果感到满意，愿在相关领域加大政策协调力度、提升经验交流和人才培训水平。双方同意持续加大对中巴信息通道开发力度，推动双方信息通讯技术领域基础设施融合对接，共同在巴基斯坦建设创新走廊。

声明表示，双方认为科技领域合作对深化中巴务实合作具有重要作用。双方同意持续拓展两国政府间科技合作，提升两国科技界在联合研究、技术转移、技术培训与人员交流等方面的合作水平，加强在通信基础设施、5G、大数据、云计算等新兴技术领域合作。

双方愿加强人工智能领域政策协调，深化相关务实合作，协同促进人工智能技术发展。巴方欢迎习近平主席宣布的《全球人工智能治理倡议》以及中方为增强发展中国家在人工智能全球治理中的权利所作努力。双方一致认为，国际社会应秉持发展和安全并重原则，通过对话协商与平等合作，携手构建开放、公正、有效的人工智能治理机制，使人工智能技术为造福各国人民、促进文明进步发挥积极作用。（来源：中国政府网）

## 2. 网络法治保障高质量发展新闻发布会举行：我国已制定出台网络领域立法150多部

6月18日，国务院新闻办公室举行新闻发布会，介绍网络法治保障高质量发展有关情况。

发布会上，国家网信办副主任王崧表示，2024年是习近平总书记提出网络强国战略目标10周年，是中国全功能接入国际互联网30周年，也是中国网络法治建设起步30周年。为此，国家网信办牵头专门组织力量编撰《中国网络法治三十年》，全面展现中国网络法治建设成就，总结中国网络法治建设经验，同时也展望中国网络法治的未来和前景。进入新时代，网络法治建设深入贯彻习近平法治思想和习近平总书记关于网络强国的重要思想，充分发挥固根本、稳预期、利长远作用，不断夯实经济社会高质量发展的法治基础。

王崧副主任表示，截至目前，中国制定出台网络领域立法150多部，形成以宪法为根本，以法律法规为依托，以传统立法为基础，以网络专门立法为主干的网络法律体系，搭建中国网络法治的“四梁八柱”，为网络强国建设提供坚实的制度保障。为了适应经济社会发展变化，不断加强网络领域行政执法统筹协调，探索网络领域综合执法和联合执法。同时，加大重点领域执法力度，切实保护人民群众合法权益，维护社会公共利益。不断拓展网络普法新格局，加强优质普法作品创作传播，打造网络普法品牌，培育网络法治文化，形成亿万网民参与普法、普法惠及亿万网民的良好局面。

对于在建设清朗网络空间、维护网民合法权益等方面主要开展的工作。国家网信办网络法治局局长李长喜表示，这些年来，国家网信办会同有关部门开展了一系列专项行动，通过这些行动加强互联网内容的建设和管理，切实推动网络生态治理，保护每个公民的合法权益，特别是一些特殊群体的权益。近年来，聚焦网络虚假信息、算法滥用等网络乱象，先后开展专项行动 40 余项，清理违法违规信息 200 多亿条。在有关部门积极履行管理责任的同时，注意督促网站平台履行主体责任，健全投诉举报机制，用这种方式保护用户的合法权益。（来源：国务院新闻办公室、中国网信网）

## 3. 国家互联网信息办公室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》

6 月 26 日，中国国家互联网信息办公室主任庄荣文在京会见德国数字化和交通部部长维辛一行，双方共同签署《关于中德数据跨境流动合作的谅解备忘录》。

中国国家互联网信息办公室将与德国数字化和交通部在《关于中德数据跨境流动合作的谅解备忘录》框架下，建立“中德数据政策法规交流”对话机制，加强在数据跨境流动议题上的交流，为两国企业营造公平、公正、非歧视的营商环境。（来源：中国网信网）

# 境内前沿观察二：政策立法

导读：6月，国家互联网信息办公室联合公安部、文化和旅游部、国家广播电视总局公布《网络暴力信息治理规定》。国家互联网信息办公室有关负责人表示，网络暴力信息严重侵害公民合法权益，受到社会各界高度关注。《规定》从明确网络信息内容管理主体责任、建立健全预防预警机制、规范网络暴力信息和账号处置、强化用户权益保护、加强监督管理、明确法律责任等方面，为加强网络暴力信息治理提供有力支撑。有关负责人还指出，网络暴力信息治理需要政府、企业、社会、网民等多方参与，促进形成积极健康、向上向善的网络文化，维护良好网络生态。

数据价值释放与安全利用仍是各部门和地方立法的重点关注。自今年3月国家互联网信息办公室发布《促进和规范数据跨境流动规定》以来，数据跨境流动监管模式更加灵活。6月，九部门联合印发《关于拓展跨境电商出口推进海外仓建设的意见》，提出在符合法律法规要求、确保安全的前提下，促进和规范数据跨境流动，允许跨境电商、跨境支付等应用场景数据有序自由流动。海南省委网信办发布《海南省数据出境安全评估申报工作指引（第二版）》《海南省个人信息出境标准合同备案指引（第二版）》，为有相应业务需求的主体落实数据出境安全评估和个人信息出境标准合同备案提供细化指引。

数据安全保障方面，广东省委办公厅、省政府办公厅印发《关于构建数据基础制度推进数据要素市场高质量发展的实施意见》，要求创新政府

数据治理模式，充分发挥政府有序引导和规范发展的作用，守住安全底线，明确监管红线。四川省成都市人大常委会公布《成都市数据条例》，强调本市各级各部门主要负责人是本单位数据工作第一责任人。江西省工业和信息化厅印发《江西省工业领域数据安全能力提升实施方案（2024—2026年）》，将强化数据安全监督执法，加强监管执法人员培训力度，强化数据安全监管力量。

人工智能法治保障方面，四部门联合印发《国家人工智能产业综合标准化体系建设指南（2024版）》，提出到2026年，新制定国家标准和行业标准50项以上，参与制定国际标准20项以上的工作目标。广东省人民政府办公厅印发《广东省关于人工智能赋能千行百业的若干措施》，提出将利用政务大模型智能化升级广东政务服务网、“粤系列”政务服务平台，提供全时在线问答和搜索服务。陕西省工业和信息化厅印发《陕西省加快推动人工智能产业发展实施方案（2024—2026年）》，要求在垂直行业领域主动布局，采用通用大模型泛化能力+行业标注数据集微调方式，加快行业大模型的持续突破和优化，不断提升适配性和精度。

关键词：网络暴力、数据跨境流动、人工智能法治保障、反电信网络诈骗

## （一）部委层面动向

### 1. 民航局发展计划司发布《民航数据管理办法（征求意见稿）》《民航数据共享管理办法（征求意见稿）》

6月4日，民航局发展计划司发布《民航数据管理办法（征求意见稿）》《民航数据共享管理办法（征求意见稿）》。

《民航数据管理办法（征求意见稿）》共九章四十四条，涉及数据共享、数据应用、数据安全等内容。其中，征求意见稿根据数据全生命周期处理活动场景，将民航数据处理主体主要分为四类：数据提供方、数据使用方、数据管理方、数据平台方。

征求意见稿规定数据提供方进行数据采集时应当遵循一数一源、一源多用的原则，规范本部门和本单位数据采集和维护流程，实现单位内数据的一次采集，共享使用。向外提供数据时应明确数据来源信息系统。民航各级行政机关、企事业单位应当加强数据应用，拓展应用场景，开展民航专业领域大模型训练，积极推进民航数据在决策支持、安全监管、生产运行、服务保障等领域中的应用，充分发挥数据要素乘数效应。安全监管中应进一步汇聚多元航空安全数据，开展多维度信息关联分析，加强安全预警与主动安全防护水平。

《民航数据共享管理办法（征求意见稿）》共七章三十条，涉及共享类型、数据归集等内容。其中，征求意见稿规定数据提供方、数据使用方、数据管理方和数据平台方应当依据国家和民航数据安全有关法律法规，按

照各自职责做好数据共享应用过程中的数据安全工作。数据提供方对其所提供数据具有解释权，应按照“谁提供，谁负责”的原则开展数据治理，保证所归集数据的完整性、准确性、时效性和可用性，接受数据质量评价考核。（来源：中国民用航空局）

## 2. 工信部等四部门联合印发《国家人工智能产业综合标准化体系建设指南（2024 版）》

6 月 5 日，工业和信息化部、中央网络安全和信息化委员会办公室、国家发展和改革委员会、国家标准化管理委员会联合印发《国家人工智能产业综合标准化体系建设指南（2024 版）》。

指南明确，人工智能标准体系结构包括基础共性、基础支撑、关键技术、智能产品与服务、赋能新型工业化、行业应用、安全/治理等 7 个部分。其中，基础支撑标准主要规范数据、算力、算法等技术要求，为人工智能产业发展夯实技术底座。安全/治理标准主要规范人工智能安全、治理等要求。安全标准规范人工智能技术、产品、系统、应用、服务等全生命周期的安全要求，包括基础安全，数据、算法和模型安全，网络、技术和系统安全，安全管理和服务，安全测试评估，安全标注，内容标识，产品和应用安全等标准。治理标准将结合人工智能治理实际需求，规范人工智能的技术研发和运营服务等要求以及人工智能全生命周期的伦理治理要求。（来源：工信部）

## 3. 九部门印发《关于拓展跨境电商出口推进海外仓建设的意见》，允许跨境电商、跨境支付等应用场景数据有序自由流动

6月8日，商务部、国家发展改革委、财政部等九部门印发《关于拓展跨境电商出口推进海外仓建设的意见》。

意见要求优化监管与服务，提升跨境数据管理和服务水平。在符合法律法规要求、确保安全的前提下，促进和规范数据跨境流动，允许跨境电商、跨境支付等应用场景数据有序自由流动。鼓励跨境电商、海外仓企业依法依规利用数据赋能产业链上下游，增强生产企业柔性化供应能力。（来源：中国政府网）

## 4. 国家互联网信息办公室等四部门印发《网络暴力信息治理规定》

6月12日，国家互联网信息办公室、公安部、文化和旅游部、国家广播电视总局印发《网络暴力信息治理规定》。规定共七章四十三条，涉及预防预警、信息和账号处置以及保护机制等内容。

规定对网络暴力信息加以定义，明确网络暴力信息是指通过网络以文本、图像、音频、视频等形式对个人集中发布的，含有侮辱谩骂、造谣诽谤、煽动仇恨、威逼胁迫、侵犯隐私，以及影响身心健康的指责嘲讽、贬低歧视等内容的违法和不良信息。

规定要求，网络信息服务提供者发现涉网络暴力违法信息的，或者在其服务的醒目位置、易引起用户关注的重点环节发现涉网络暴力不良信息的，应当立即停止传输，采取删除、屏蔽、断开链接等处置措施，保存有

关记录，向有关部门报告。发现涉嫌违法犯罪的，应当及时向公安机关报案，并提供相关线索，依法配合开展侦查、调查和处置等工作。

规定提出，网络信息服务提供者应当建立健全网络暴力信息预警模型，综合事件类别、针对主体、参与人数、信息内容、发布频次、环节场景、举报投诉等因素，及时发现预警网络暴力信息风险。网络信息服务提供者发现存在网络暴力信息风险的，应当及时回应社会关切，引导用户文明互动、理性表达，并对异常账号及时采取真实身份信息动态核验、弹窗提示、违规警示、限制流量等措施；发现相关信息内容浏览、搜索、评论、举报量显著增长等情形的，还应当及时向有关部门报告。

规定明确，网信、公安、文化和旅游、广播电视等有关部门依法监督检查网络信息服务提供者的网络暴力信息治理情况，建立健全信息共享、会商通报、取证调证、案件督办等工作机制，协同治理网络暴力信息。公安机关对于网信、文化和旅游、广播电视等部门移送的涉网络暴力信息违法犯罪线索，应当及时进行审查，并对符合立案条件的及时立案侦查、调查。（来源：中国网信网）

## 5. 全国网安标委发布《网络安全标准实践指南—敏感个人信息识别指南（征求意见稿）》

6 月 11 日，全国网络安全标准化技术委员会发布《网络安全标准实践指南—敏感个人信息识别指南（征求意见稿）》，提出敏感个人信息识别方法，给出常见敏感个人信息的类别和示例。

征求意见稿指出，既要考虑单项敏感个人信息识别，也要考虑多项一般个人信息汇聚或融合后的整体属性，分析其一旦泄露或非法使用可能对个人权益造成的影响。如果汇聚或融合后的一般个人信息在发生泄漏或非法使用时，影响达到敏感个人信息水平的，应将汇聚或融合后的个人信息整体参照敏感个人信息进行保护。

征求意见稿就个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息给出具体示例。其中，特定身份信息有残障人士身份信息、不适宜公开的职业身份信息（如军人、警察）等个人信息。其他敏感个人信息还包括精准定位信息、犯罪记录信息等。（来源：全国网络安全标准化技术委员会）

## 6. 全国网安标委发布《网络安全技术 关键信息基础设施安全保护能力指标体系（征求意见稿）》

6 月 20 日，全国网络安全标准化技术委员会发布国家标准《网络安全技术 关键信息基础设施安全保护能力指标体系（征求意见稿）》。

征求意见稿将关键信息基础设施安全保护能力分为 3 级，由低到高分别为：基本保护级、强化保护级、战略保护级。基本保护级侧重于满足相关法律法规要求，系统能够常态化安全稳定运行；强化保护级侧重于关键信息基础设施运营者与保护工作部门形成安全防御共同体，保障业务稳定运行，形成综合防御和协同防御的能力；战略保护级侧重于关键信息基础设施运营者、保护工作部门和国家层面三级协同，保障极限情况下关键业务最小化运行。（来源：全国网络安全标准化技术委员会）

### 7. 全国网安标委发布《数据安全技术 数据安全和个人信息保护社会责任指南（征求意见稿）》

6 月 20 日，全国网络安全标准化技术委员会发布国家标准《数据安全技术 数据安全和个人信息保护社会责任指南（征求意见稿）》。

征求意见稿为组织理解数据安全和个人信息保护社会责任和实施相关活动提供指南，主要围绕组织治理，合规性、创新性和价值体现，公平运行、竞争与合作，用户权益保护，公益参与和社会发展五大主题做出规定。（来源：全国网络安全标准化技术委员会）

## （二）地方层面动向

### 1. 广东省人民政府办公厅印发《广东省关于人工智能赋能千行百业的若干措施》

5 月 26 日，广东省人民政府办公厅印发《广东省关于人工智能赋能千行百业的若干措施》。

文件主要围绕三大方面进行规定：一是围绕夯实人工智能产业底座，加快形成新质生产力，提出加大人工智能核心芯片器件供给，推进人工智能软件迭代升级，系统构建算法产业矩阵，适度超前部署算力网络建设；二是围绕构筑智能终端产品新高地，塑造广东品牌新形象，提出提智做强高端装备，赋智壮大消费终端；三是围绕打造智能融合应用新引擎，形成经济增长新风口，提出赋能实体经济新动力，赋能智慧民生新体验，赋能社会治理新效能，赋能数字消费新业态，赋能各行各业新领域。

其中，赋能社会治理新效能方面，文件提出惠企利民建设智慧政府。利用政务大模型智能化升级广东政务服务网、“粤系列”政务服务平台，提供全时在线问答和搜索服务。建设面向全省各级党政机关的视频算力支撑基础平台，提升视频智能化水平。在“粤经济”平台融合经济算法模型，为政府在经济运行监测、分析研判、政策仿真等场景提供决策支撑。（来源：网信广东）

## 2. 广东省委办公厅、省政府办公厅印发《关于构建数据基础制度推进数据要素市场高质量发展的实施意见》

6 月 24 日消息，广东省委办公厅、省政府办公厅近日印发《关于构建数据基础制度推进数据要素市场高质量发展的实施意见》。

意见围绕六方面进行规定：一是围绕探索推进数据产权制度建设，提出探索数据产权结构性分置制度，建立健全数据确权授权机制、加强数据各参与方合法权益保护；二是围绕完善数据要素流通和交易制度，提出健全数据全流程合规与监管规则体系、培育数据要素流通和交易服务生态、构建数据要素市场基础运营体系等；三是围绕构建数据要素收益分配制度，提出更好发挥政府在数据要素收益分配中的引导调节作用、科学合理评估数据要素价值；四是围绕建立健全数据要素治理制度，提出创新政府数据治理模式、压实企业数据治理责任、发挥社会协同治理作用；五是围绕提升数据要素赋能高质量发展能力，提出赋能实体经济发展与制造业转型升级等；六是围绕构筑粤港澳大湾区数据协同发展新范式，提出构建数据安全合规有序跨境流通机制、推动粤港澳大湾区数据协同与交流。

其中，创新政府数据治理模式方面，意见要求充分发挥政府有序引导和规范发展的作用，守住安全底线，明确监管红线。加强数据资源“一网共享”体系建设，健全数据目录清单，常态化开展数据普查。制定动态的数据流通和交易负面清单。强化行业监管和联合协同监管，建立数据联管联治机制。强化反垄断和反不正当竞争，营造公平竞争、规范有序的市场环境。加强网络和数据安全制度建设，强化网络和数据安全技术保障，提升网络和数据基础设施安全水平。（来源：广东省人民政府）

## 3. 陕西省工业和信息化厅印发《陕西省加快推动人工智能产业发展实施方案（2024—2026 年）》

5 月 30 日，陕西省工业和信息化厅印发《陕西省加快推动人工智能产业发展实施方案（2024—2026 年）》，围绕“强基”“创智”“赋智”“聚智”采取十一项行动。

方案要求以应用场景为牵引、智算中心为承载，积极吸引落地人工智能通用大模型。在垂直行业领域主动布局，采用通用大模型泛化能力+行业标注数据集微调方式，加快行业大模型的持续突破和优化，不断提升适配性和精度。

安全保障方面，方案要求围绕网络安全、数据安全、科技伦理等领域建立风险防范和应对机制，引导人工智能相关企业和组织健康发展。强化人工智能产品和系统的网络安全防护，坚持安全可信和创新发展并重。加强人工智能安全治理行业自律，积累大模型安全应用经验，探索可复制可推广的治理模式。（来源：陕西省工业和信息化厅）

## 4. 北京市人大常委会通过《关于进一步加强本市反电信网络诈骗工作的决定》

5 月 31 日，北京市第十六届人大常委会第十次会议通过《关于进一步加强本市反电信网络诈骗工作的决定》。

文件规定，市、区人民政府组织领导本行政区域内反电信网络诈骗工作，建立健全反电信网络诈骗工作机制，统筹力量资源，完善打击治理体系，确定目标任务，开展综合治理。公安机关牵头负责反电信网络诈骗工作。金融、电信、网信、市场监管等部门依照职责履行监管主体责任，负责本行业领域反电信网络诈骗工作，建立健全安全评估、行业准入、风险防控等制度，加强监测识别，强化技术反制。

文件要求，电信业务经营者应当依法全面落实真实身份信息登记制度，不得超出国家有关规定限制的数量开办电话卡；开展监测识别，对涉诈异常电话卡、物联网卡用户，依法采取重新核验、暂停服务等措施；及时识别、阻断非法设备、软件接入网络。电信业务经营者、互联网服务提供者应当依法落实互联网实名制管理有关规定；履行合理注意义务，在提供网络资源、网络推广、技术支持、支付结算等服务中，监测识别和处置涉诈支持、帮助活动。互联网服务提供者应当对涉诈异常互联网账号及涉案电话卡、涉诈异常电话卡所关联注册的互联网账号，进行监测、核验、处置。

文件要求，履行个人信息保护职责的部门、单位应当依法加强个人信息保护，对物流信息、交易信息、贷款信息、医疗信息、婚介信息等实施

重点保护，减少信息泄露风险，防止被电信网络诈骗利用。（来源：北京市人大常委会）

## 5. 北京市经济和信息化局发布《北京市自动驾驶汽车条例（征求意见稿）》，提出网络与数据安全保护要求

6 月 30 日，北京市经济和信息化局发布《北京市自动驾驶汽车条例（征求意见稿）》。征求意见稿共六章三十八条，从管理机制、产业创新发展、基础设施规划建设、创新活动规范、安全保障等方面进行制度设计。

网络安全方面，征求意见稿规定自动驾驶汽车企业应当依法落实网络安全等级保护制度，建立网络安全管理制度，依法制定网络安全事件应急预案，建立网络安全评估和管理机制，提高网络安全保护水平，保障网络安全稳定运行。

数据安全与个人信息保护方面，征求意见稿规定自动驾驶汽车企业应当依法建立健全数据安全和个人信息保护管理制度，开展数据分类分级保护和数据安全风险评估工作，重点加强重要数据和个人用户数据安全管理。不得非法处理个人信息，不得采集与本车辆行驶和交通安全无关的信息，不得非法采集涉及国家安全的信息。在发生或者可能发生涉及国家安全、用户个人信息等数据泄露、损毁、丢失等情况时，自动驾驶汽车企业应当立即采取补救措施，按照规定及时告知用户并向有关部门报告。自动驾驶汽车数据跨境传输活动按照国家有关规定执行。

测绘安全方面，征求意见稿规定具有相应导航电子地图制作测绘资质的单位利用非本单位所有的自动驾驶汽车开展测绘活动的，应当依法采取

技术措施、制定相关制度，以保障自动驾驶汽车传输到车外进行存储和处理的地理信息数据的安全。自动驾驶汽车企业应当依法采取技术措施、制定相关制度，保障其他单位和个人不得有利用自动驾驶汽车开展采集、存储、传输和处理地理信息数据的行为。（来源：北京市经济和信息化局）

## 6. 四川省成都市人大常委会公布《成都市数据条例》

6 月 4 日，四川省成都市人大常委会公布《成都市数据条例》。条例共七章四十六条，涉及数据收集与治理、数据流通与交易、数据应用与促进、数据安全与保护等内容。

条例规定，本市各级各部门主要负责人是本单位数据工作第一责任人，应当明确数据工作专（兼）职人员，做好数据资源管理、统建系统实施、应用场景推广、数据安全保护、线上线下融合等工作。政务部门和公共服务组织在法定职责或者提供公共服务范围内，可以依法直接收集或者委托第三方收集相关公共数据。委托第三方收集公共数据的，应当与受托人明确约定委托事项以及双方的权利义务，并对委托事项进行监督检查；受托人开展数据收集时，应当将委托情况告知被收集对象。

安全方面，条例规定政务部门和公共服务组织应当按照规定建立数据安全管理制度，按照要求对公共数据进行安全备份，编制并组织实施本单位的数据安全规划和数据安全应急预案，定期组织开展本单位的数据安全风险评估。数据处理者委托他人代为处理数据的，应当与其签订安全协议，明确数据安全保护责任。受托方完成数据处理任务后，应当及时有效销毁其存储的数据，不得擅自留存、使用、泄露或者向他人提供数据，但法律、

法规另有规定或者双方另有约定的除外。数据处理者对涉及个人信息的数据应当加密储存，不得采取一揽子授权、强制同意等方式处理个人信息，不得擅自变更数据授权用途，法律、行政法规另有规定的，从其规定。（来源：成都市人民政府）

## 7. 内蒙古自治区人民政府印发《内蒙古自治区公共数据管理暂行办法》

6月4日，内蒙古自治区人民政府印发《内蒙古自治区公共数据管理暂行办法》，规范自治区行政区域内公共数据采集、治理、归集、存储、加工、传输、共享、开放、开发及数据安全管理等活动。

办法指出，公共数据主管部门负责组织建立公共数据安全保障制度，会同有关部门在国家网络安全等级保护制度的基础上，研究制定公共数据安全保护工作措施，按照国家和自治区规定定期对公共数据共享数据库采用加密方式进行本地及异地备份，指导、督促公共数据采集、使用、管理全过程的安全保障工作，定期开展公共数据共享风险评估和安全审查。公共数据主管部门对外输出数据产品或者提供数据服务时，应当建立健全公共数据安全保障、监测预警和风险评估体系，明确数据要素流通全生命周期、各环节的责任主体和标准规范要求。

办法规定，公共数据安全实行“谁采集谁负责、谁使用谁负责、谁运行谁负责”的责任制。公共数据主管部门、公共管理和服务机构的主要负责人是本单位数据安全工作的第一责任人。公共数据主管部门、公共管理

和服务机构应当强化和落实数据安全主体责任，建立数据安全常态化运行管理机制。（来源：内蒙古自治区人民政府）

## 8. 江西省工业和信息化厅印发《江西省工业领域数据安全能力提升实施方案（2024—2026 年）》，将强化数据安全监督执法

6 月 5 日，江西省工业和信息化厅印发《江西省工业领域数据安全能力提升实施方案（2024—2026 年）》，将从企业数据保护、数据安全监管、数据安全产业支撑三方面采取能力提升行动。

提高数据安全监管能力方面，方案要求：（1）强化“以技管数”能力，推动江西省制造业重点产业链企业接入省工业数据安全监测平台；（2）强化风险监测与信息报送，建立重大风险事件案例库；（3）强化风险防控与应急处置，针对江西省制造业重点产业链企业的重点系统平台、重要数据集中开展风险排查和防范、远程检测、现场诊断等工作；（4）强化数据安全监督执法，将工业领域数据安全纳入江西省行政执法事项清单，加快完善江西省工业领域数据安全执法流程和工作机制，加强监管执法人员培训力度，强化数据安全监管力量。加强对各设区市的执法指导，开展执法案例宣介与警示教育，督促企业落实数据保护责任和义务，对发现的违法违规行为依法依规实施处罚。

提高企业数据保护能力方面，方案提出加强数据安全政策宣贯、开展数据安全业务培训、强化数据分类分级管理、强化重点企业数据安全管理。其中，方案表示将督促企业依法依规落实数据安全主体责任，建立健全数据安全管理体系和工作机制，引导企业将数据安全工作与业务发展同谋划、

同部署、同落实、同考核；将滚动编制江西省工业领域数据安全风险防控重点企业名录，督促其着重提升风险监测、态势感知、威胁研判和应急处置等能力。（来源：江西省工业和信息化厅）

## 9. 海南省委网信办发布《数据出境安全评估申报工作指引（第二版）》《个人信息出境标准合同备案指引（第二版）》

6月13日，海南省委网信办发布《海南省数据出境安全评估申报工作指引（第二版）》《海南省个人信息出境标准合同备案指引（第二版）》。

《海南省数据出境安全评估申报工作指引（第二版）》对数据、重要数据、个人信息、敏感个人信息及数据处理等术语进行定义，适用于注册地为海南的开展数据处理活动的法人、公共机构、政府机关等组织，或在海南开展数据处理活动的个人。数据出境安全评估申报工作主要包括以下步骤：（一）判断是否符合申报情形。数据处理者全面梳理处理和出境的数据，判断是否符合需要申报评估的情形；（二）开展数据出境风险自评估。数据处理者自行或委托第三方开展数据出境风险自评估；（三）提交申报材料。

《海南省个人信息出境标准合同备案指引（第二版）》适用于所在地为海南的个人信息处理者。个人信息处理者通过订立标准合同的方式向境外提供个人信息，同时符合下列情形的应当向所在地省级网信部门备案：（一）关键信息基础设施运营者以外的数据处理者；（二）自当年1月1日起，累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）的；（三）自当年1月1日起，累计向境外提供不满1万人敏感

个人信息的。属于《促进和规范数据跨境流动规定》第三条、第四条、第五条、第六条规定情形的，从其规定。指引同时明确备案方式、备案流程及备案材料。（来源：网信海南）

## 10. 海南省委网信办发布《海南自由贸易港国际数据中心发展条例（公开征求意见稿）》

6月26日，海南省委网信办发布《海南自由贸易港国际数据中心发展条例（公开征求意见稿）》。

征求意见稿适用于在海南自由贸易港内开展国际数据中心业务及其相关的监督管理活动。国际数据中心业务，是指企业在海南自由贸易港内利用高速便捷的跨境数据专用通道，仅面向境外提供数据存储、加工、交易等国际数据服务业务。

网络与数据安全方面，征求意见稿规定，海南省网信部门负责统筹协调国际数据中心网络安全和数据安全相关监管工作，指导有关部门和企业建设国际数据中心数据安全保障体系和监管体系，建立健全数据安全风险评估、信息共享、监测预警、应急处置等机制，保障国际数据中心网络安全和数据安全。国际数据中心业务运营者应当依照法律、法规的规定，落实安全管理制度和技术措施，建立健全全流程网络安全和数据安全管理制度及应急处置预案，保障网络安全和数据安全。海南省省级基础电信运营商应当依照法律、法规的规定，制定安全管理制度，履行网络安全和数据安全保护义务。（来源：网信海南）

# 境内前沿观察三：治理实践

导读：6 月，公安机关、网信部门、通信管理部门的多项重要工作会议或专项行动陆续展开。其中，全国公安机关视频会议召开，要求针对电信网络诈骗、跨境赌博等犯罪，紧抓不放、乘胜追击，有力推进专项打击、黑灰产治理、宣传防范和国际执法合作等工作。中央网信办召开全国重点商业网站平台管理工作会议，强调党的二十届三中全会召开在即，网信部门和网站平台必须全力以赴做好服务保障工作。

专项行动主要由地方通信管理部门组织开展。上海市将纵深推进“浦江护航”数据安全专项行动；江苏省将开展“龙磐 2024”网络和数据安全专项行动；上海市、浙江省将开展 2024 年电信和互联网行业网络和数据安全检查。其中，加强对电信和互联网行业第三方服务机构的管理成为保障专项行动顺利开展的重要措施之一。如上海“浦江护航”数据安全专项行动将强化机构管理纳入专项行动的保障措施，要求强化对在本市范围内开展电信和互联网行业数据安全服务的第三方机构的合规指导和监督管理，并建立数据安全服务责任追究机制，本市各电信和互联网企业发生数据安全事件的，倒查其近两年内委托开展数据安全风险评估服务的第三方机构及其评估结果。

青海、甘肃等地公安机关办理多起网络安全行政执法案件，涉及的违法行为集中在未进行联网备案、未落实网络安全保护义务导致网站被篡改为赌博网站或发布违法信息、未落实数据安全保护义务导致数据存在泄露

风险。内蒙古、四川、浙江等地警方破获多起刑事案件，涉及利用网络传播淫秽物品牟利、破坏计算机信息系统、侵犯应届毕业生个人信息、恶意引流等犯罪行为。

此外，多家银行因数据安全问题被处罚。因安全测试存在薄弱环节、数据安全管理不足、灾备管理不足等问题，国家金融监督管理总局对交通银行股份有限公司处以160万元罚款。因数据治理存在缺陷、数据治理不到位等问题，国家金融监督管理总局宁波监管局对农业银行宁波市分行、浦发银行宁波分行、徽商银行宁波分行分别处以罚款，罚款金额总计715万元。

关键词：电信网络诈骗、重点商业网站平台、电信和互联网行业专项行动、银行业数据安全治理

## （一）公安机关治理实践

### 1. 全国公安机关视频会议召开，要求对电信网络诈骗犯罪紧抓不放、乘胜追击

6 月 24 日，全国公安机关视频会议召开。会议强调，要全力捍卫政治安全，严密防范、严厉打击境内外敌对势力渗透颠覆捣乱破坏活动，确保国家政权安全、制度安全、意识形态安全。坚持和发展新时代“枫桥经验”，会同有关部门和基层组织滚动排查各类矛盾风险，推动落实属地管理责任和多元化解机制，努力做到源头化解。

会议指出，要全力打击治理突出违法犯罪。聚焦严重影响人民群众安全感的突出违法犯罪，运用集群战役、挂牌整治等多种方式，依法严厉打击、有效治理。针对电信网络诈骗、跨境赌博等犯罪，紧抓不放、乘胜追击，有力推进专项打击、黑灰产治理、宣传防范和国际执法合作等工作。

会议指出，建立完善“专业+机制+大数据”新型警务运行模式，把“情指行”一体化运行机制的作用发挥好，提高情报研判的精度、指挥协同的广度、行动处置的速度。（来源：公安部网安局）

### 2. 因未落实网络安全保护义务导致违法信息传播，青海省西宁市警方对一公司进行处罚

5 月 27 日，青海省西宁市公安局城东分局网安部门在日常工作中发现，辖区一家公司自开办网站以来，相关管理人员网络安全意识淡薄，缺乏日

常监管。该网站联网使用后，未在规定时间内到属地公安机关和全国互联网安全管理服务平台进行联网备案，未落实网络安全保护义务，未采取防范计算机病毒和网络侵入等技术措施，网站未对其发布的信息进行有效审核及管理，导致违法信息在网络上发布，造成不良影响。

针对上述违法违规行为，网安大队民警及时传唤该公司法人及网站负责人，普及网站日常管理和维护知识。同时，依据《网络安全法》第二十一条、第二十五条、第五十九条第一款，《计算机信息网络国际联网安全保护管理办法》第十二条、第二十三条等相关法律规定，对该公司给予行政处罚，并责令该公司及网站负责人限期内作出整改，进行网站备案登记，严格落实主体责任，合法合规开办网站。（青海网警）

## 3. 因网站被篡改等违法行为，甘肃甘州公安对两家公司进行处罚

6 月 13 日消息，甘肃省张掖市公安局甘州分局近日查处两起网络安全行政执法案件。

甘州分局网安大队在工作中发现，张掖市某信息科技公司网站由于长期未履行网络安全保护义务，该公司网站已被篡改为赌博网站，为网络犯罪埋下隐患；甘肃某信息科技有限公司网站未进行公安机关备案，违反计算机信息系统国际联网备案制度，根据《网络安全法》《计算机信息系统安全保护条例》相关规定，对以上 2 家公司依法给予行政处罚，责令立即整改。（来源：甘州公安）

## 4. 因未履行数据安全保护义务，甘肃甘州公安处罚 6 家酒店

6 月 25 日消息，甘肃省张掖市公安局甘州分局网安大队自“祁连 2 号”行动开展以来，持续对辖区企事业单位涉及公民个人信息的问题进行执法监督检查，于近日连续查处 6 起酒店行业未履行数据安全保护义务案。

甘州分局网安大队在工作中发现，张掖市某酒店管理服务有限公司等 6 家酒店的网络数据管理系统均存在数据泄漏的风险，未履行数据安全保护义务，严重影响公民个人信息安全。甘州分局根据《数据安全法》相关规定，对 6 家酒店依法给予行政处罚，责令立即整改。（来源：央广网）

## 5. 内蒙古乌兰浩特警方破获特大网络传播淫秽物品牟利案，涉案资金流水 15 亿元

6 月 15 日消息，在“净网 2024”专项行动中，内蒙古乌兰浩特警方成功破获一起特大网络传播淫秽物品牟利案，查获电子设备 333 台，冻结资金 356 万元。

2024 年初，内蒙古乌兰浩特网警在工作中发现，有人在微信群内大肆传播淫秽网站链接进行牟利。案件涉及人员多、涉案金额大、社会影响广，案件上报后，兴安盟、乌兰浩特市两级公安机关共同侦办该案。经查，该团伙向 2 万个微信群近千万人推广涉黄链接，涉及境外涉黄网站 5 个，涉及淫秽视频 40 余万部，涉案资金流水达 15 亿元。该团伙组织严密，分工明确，反侦查意识较强，5 个淫秽网站服务器分布在境外不同位置，国内成员采取分散办公的模式逃避打击，末端代理获利通过多级跑分平台逐步发放，组织者张某、李某等人的上线一直在变换身份，网站域名也经常变更。

乌兰浩特警方逐步掌握该犯罪团伙成员的身份信息、内部结构以及作案规律。通过两次收网行动会战，转战11省25市，打掉传播淫秽网站链接牟利窝点4个、扫码收款窝点2个、资金结算跑分窝点3个，采取刑事强制措施56人，扣押作案手机310部，电脑23台，银行卡122张，冻结资金356万元，查封房产2套。目前，该案还在进一步侦办中。（来源：光明网）

## 6. 四川省南充市仪陇县公安破获一起特大破坏计算机信息系统案，涉案金额1.2亿余元

6月18日消息，四川省南充市仪陇县公安近期破获一起特大破坏计算机信息系统案，打掉开发、销售和使用黑客破坏软件的犯罪团伙4个，查获黑客软件源码2套，涉案金额1.2亿余元。

此前，仪陇县公安局接群众举报，县城一家电器售后负责人老板徐某，经常使用“A助手软件”对国内某知名电器售后服务APP进行操作，频繁上传电器安装地址和照片，疑似有网络攻击行为。警方迅速开展工作，发现嫌疑人徐某使用这款软件突破安全防护，非法侵入该电器公司售后服务系统，并伪造、上传安装服务工单，用以骗取售后服务安装维护费用。经进一步侦查发现，该团伙除使用“A助手软件”外，还使用另一款具备非法侵入、控制售后服务系统伪造安装工单功能的黑客软件“B配置工具”。专案组经过4个月的不懈努力，研判出“A助手软件”开发人员张某及其销售运营团伙，“B配置工具”黑客软件开发人员白某及其销售运营团伙。

专案组立即组织警力分别赴黑龙江、山东、广东、广西等地，成功抓获两款黑客软件销售运营团伙15人，扣押涉案电脑21台、手机18部，查扣涉案资金360余万元。顺藤摸瓜，警方再赴山东、辽宁成功抓获该两款黑客软件开发者张某、白某二人，查获外挂软件源代码2套，查扣涉案资金200余万元。经过对两款黑客软件分析发现，犯罪嫌疑人利用国内某知名电器集团公司官方APP存在的安全漏洞，开发出能够侵入售后服务系统并非法控制进行数据修改的黑客工具。警方梳理出北京、浙江、广东等全国29省市共有800余人使用这两款软件，涉及售后合作网点700余个，涉案总金额高达1.2亿余元。

该案16名主要犯罪嫌疑人员因涉嫌提供侵入、非法控制计算机信息系统、破坏计算机信息系统、合同诈骗等犯罪被依法判处有期徒刑，并追缴违法所得。（来源：仪陇公安）

## 7. 四川省遂宁市大英县警方打掉一个为“标题党”恶意引流提供技术帮助的网络犯罪团伙

6月21日消息，四川省遂宁市大英县公安局近日成功打掉一个为“标题党”恶意引流提供技术帮助的网络犯罪团伙。

2022年5月以来，以张某为首的犯罪团伙成立成都某网络科技有限公司，明知向他人提供、出售的“系统”是用于编辑、制作虚拟文章内容，且明知该系统的源代码以及服务器内容中包含了仿公众号等数据，仍以1500至3800元不等的价格向他人出售，并根据购买者“建议”对该系统进行优化、升级、更改。

购买者则借助各类热点案事件编造各类虚假信息，通过添加“劲爆”“突发”“震惊”等字样的标题，再使用该公司“系统”生成链接后，在微信群、QQ群等社交平台大肆推送，以此骗取网民的“点击”和“关注”，赚取流量变现，收取广告费。通过甄别，绝大多数信息都是对热点案事件的歪曲解读、煽情、暗讽，文不对题，毫无“营养”，甚至有些就是谣言。

经过近2个月的侦查，四川遂宁市大英县公安局在省、市网安部门的大力支持和协助下，组织警力100余人（次），分赴山东、江西、广东等地抓获犯罪嫌疑人张某等21人，查获网络水军购买用户293个、场景数（有害信息）17966条，总点击量8664万余次。随即，警方在全国发起集群战役，全国各涉及省（市）据此共抓获涉案人员69人，关停账号18个，清理有害信息2000余条。（来源：公安部网安局）

## 8. 四川省泸州市警方连续破获三起侵犯应届毕业生个人信息案件

6月24日消息，四川省泸州市公安机关近日根据辖区居民报警，连续破获三起侵犯应届毕业生个人信息案件。

4月，泸州市网安部门接到辖区学生家长报警，近期频繁接到自称是某学校招生办的电话，对自己的姓名和电话掌握无误，自己小孩就读的学校、年级、姓名也了如指掌，自己及小孩的个人信息疑似被泄露。相关警情引起泸州公安机关高度重视，网安部门立即组织专业民警梳理案件线索，开展跟踪排查，以吴某兄弟、钟某某、陈某某为首的侵犯学生个人信息的犯罪团伙浮出水面。

经查，四川省内多个民办大中专、职业技术学院以及培训机构为拓宽招生渠道，将招生业务外包给吴某兄弟、钟某某、陈某某等人分别经营的教育咨询公司，并约定按照招生数量按比例抽成返利。为更好地开展招生业务，上述犯罪团伙自2018年3月起，从全国各地购买共计100万余条川渝片区各地市州初、高中应届生学籍信息，并分发给公司内部聘请的话务人员用于电话招生。

在成功查明团伙人员身份、组织架构后，专案组于5月开展集中收网工作，成功将3个犯罪团伙全部抓获，并在多个现场查获初、高中应届学生信息（学生姓名、家长姓名、家长电话）共计100余万条。目前，6名犯罪嫌疑人已被依法采取刑事强制措施，案件还在进一步侦办中。（来源：公安部网安局）

## 9. 浙江丽水云和县警方破获一起非法利用软件抢购电商平台飞天茅台酒案

6月28日消息，浙江丽水云和县公安局近日披露一起非法利用软件抢购电商平台飞天茅台酒案，涉及30余万条电商平台用户数据，涉案资金流水高达6000余万元。

2023年12月，云和县公安局网安大队接到辖区吴女士报案称，疑似有人通过外挂软件有偿帮人在电商平台上代抢茅台酒。案件受理后，云和公安立即组织警力开展侦查。民警在初步调查后发现，部分电商平台存在不法分子使用外挂软件秒杀“飞天茅台酒”的情况。

经过3个多月的缜密侦查和分析研判，民警锁定了5个分工明确、层级分明的犯罪团伙。随后，先后前往广东、江苏、陕西等地开展统一收网行动，在当地警方配合下，成功打掉犯罪团伙5个，抓获14名犯罪嫌疑人，查封涉案机房5处，涉案资金流水高达6000余万元。

据了解，犯罪嫌疑人郭某、刘某等人2021年以非法牟利为目的开发抢购软件，以有偿原价抢购电商平台飞天茅台酒为噱头，通过张某、李某等下级代理大量收集电商平台用户账号信息。郭某等人通过外挂软件批量登录账号进行抢购。在为用户成功抢购到茅台酒后，由代理向用户收取代抢费用，层级提交至软件开发人员郭某、刘某等人的手中。该案件中的5个犯罪团伙分工明确，截至目前，已为用户代抢到飞天茅台酒3万余瓶，非法获利2000余万元。

目前，14名犯罪嫌疑人因涉嫌提供侵入、非法控制计算机信息系统程序工具罪，被移送起诉至云和县人民检察院。（来源：公安部网安局）

## （二）网信部门治理实践

### 1. 中央网信办召开全国重点商业网站平台管理工作会议

6月27日，中央网信办在四川成都召开全国重点商业网站平台管理工作会议。

会议强调，党的二十届三中全会召开在即，网信部门和网站平台必须全力以赴做好服务保障工作。要坚持正确的政治方向、舆论导向和价值取

向，持续整治网上各类乱象问题，维护网络传播秩序，为会议召开营造良好网络舆论氛围。

会议要求，要正确处理好安全与发展的关系，做到以管理促安全、以安全促发展。既要发挥平台主体作用，以科技创新催生新产业、新模式、新动能，推动网站平台高质量发展，也要加强网络内容建设和管理，防范各种风险隐患，促进网络生态健康有序。（来源：中国网信网）

## 2. 国家网信办发布“清朗·优化营商网络环境一整治涉企侵权信息乱象”专项行动典型案例

6月8日，国家网信办发布“清朗·优化营商网络环境一整治涉企侵权信息乱象”专项行动中依法处置的一批典型案例：

（1）“墨子商业论”等账号散布谣言信息，恶意诋毁企业形象。微信视频号“墨子商业论”“兆基弟弟”、今日头条账号“老百姓那点事儿”、百家号“一条鱼影评”、微博账号“奶茶甜度超标 kk ”等，恶意解读某饮用水企业股权结构、产品包装图案，散布虚假信息和极端言论，抹黑诋毁企业形象。涉及的账号已被依法依约关闭。

（2）“奇偶派”等账号歪曲解读涉企公开信息，谋取非法利益。某文化传播有限公司在抖音、网易、知乎等多个网站平台上注册“奇偶派”账号，蓄意发布对某信息科技公司年度财务报表进行负面解读的信息，并在该信息科技公司与其沟通信息内容真实性问题时，借机胁迫要求签订商业合作协议。涉及的账号及其“转世”账号已被依法依约关闭，账号主体被纳入平台黑名单管理。

（3）“小牛说车”等账号故意夸大歪曲事实，抹黑诋毁企业及其创始人。抖音账号“小牛说车”、懂车帝账号“小牛说车 new ”、今日头条账号“黄小牛 new ”，为博眼球、吸流量，多次发布短视频，歪曲捏造事实、恶意诋毁某品牌汽车质量和该汽车企业、创始人形象声誉。涉及的账号已被依法依约关闭。

（4）“刘步尘”等账号发布虚假不实信息，恶意诋毁企业、企业家形象。微博账号“刘步尘”、抖音账号“我是东爷”、百家号“步尘观察”，发布涉某企业及其高管人员虚假不实信息，并与低俗话题关联。微信视频号“星宇卡车帝”，散布某品牌汽车因发动机存在环保超标问题被强制召回的不实信息。涉及的账号已被依法依约禁言。

（5）“橡果商业评论”等账号蹭炒涉企热点，抹黑攻击企业。腾讯新闻账号“橡果商业评论”、网易号“橡果商业”，蹭炒涉企热点，以“独家对话”形式，发布涉企虚假不实信息。微博账号“数码帅姐”“就喜欢跑跑跑”“熊哥爱车”，存在刷帖控评等网络水军行为，恶意抹黑攻击某企业产品。涉及的账号已被依法依约关闭。（来源：中国网信网）

## 3. 北京市网信办严厉打击违法违规“自媒体”账号 9000 余个

6 月 11 日，北京市网信办公布“自媒体”乱象治理工作情况。自 5 月起，北京市网信办贯穿全年开展“自媒体”综合治理。近期，北京市网信办深入开展“清朗京网•整治‘自媒体’无底线博流量”专项行动，督促指导属地网站平台依法依约处置“风趣的只说实话”等账号 9000 余个。

同时发布八起典型案例，涉及传播涉企虚假信息、散布同质化不实信息、自导自演摆拍造假、蹭炒热点博取流量、制造虚假人设炫富、滥发“新黄色新闻”、拉踩引战“饭圈”乱象等违法行为。（来源：网信北京）

## 4. 上海市委网信办发布专项行动阶段性成果，属地网站平台清理违法外链上百万条

6月14日，上海市委网信办发布“清朗浦江·打击违法信息外链”专项行动阶段性成果。根据中央网信办统一部署，上海市委网信办4月底起开展为期2个月的专项行动，重点针对账号、评论、群圈、直播和短视频、生活服务、浏览器和搜索引擎、电商、涉未成年人版块等八大环节出现的违法信息外链引流问题进行集中整治。截至目前，属地网站平台共清理有害信息103.8万余条，处置违法违规账号超过24.3万个。

为进一步创新专项行动开展形式，建立健全专项整治长效机制，上海市委网信办将2023年以来开展的分类指导会运用于专项治理工作中，召开打击违法信息外链专项行动分类指导会。拼多多、得物、大众点评、携程、饿了么、小红书、虎扑、soul、哔哩哔哩等15家属地电商、生活服务类、网络社交、网络音视频和未成年人用户较多的网站平台参加会议。（来源：网信上海）

## 5. 陕西网信部门依法查处一批网络违法违规案件

6月21日消息，今年以来，陕西网信部门联合相关部门持续深化“从严整治‘自媒体’乱象”专项行动，不断加大网络执法力度，依法查处一

批网络违法违规典型案件。截至目前，共依法依规关停网站122家，关闭互联网平台账号39个，警告、约谈网站和账号160家（个），下架违法违规移动应用程序77个，向有关部门移交线索44件。

陕西网信部门依法关闭一批网站、账号传播涉政治类有害信息，网站违规开展互联网新闻信息采编发布服务，网站、账号传播淫秽色情赌博违法违规信息；约谈一批“自媒体”账号违规传播虚假信息；禁言处罚一批网络账号发布造谣污蔑信息。（来源：陕西网警巡查执法）

## （三）通信管理部门治理实践

### 1. 工信部、浙江省通信管理局通报问题APP

（1）工信部

6月19日，工信部通报2024年第4批，总第39批侵害用户权益行为的APP（SDK）。通报指出，工信部近期组织第三方检测机构进行抽查，共发现22款APP及SDK存在侵害用户权益行为，涉及违规收集个人信息、强制频繁过度索取权限、超范围收集个人信息、强制用户使用定向推送功能、信息窗口未提供关闭或退出标识等问题。相关APP及SDK应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

6月28日，工信部通报2024年第5批，总第40批侵害用户权益行为的APP（SDK）。通报指出，工信部近期组织第三方检测机构进行抽查，共发现24款APP及SDK存在侵害用户权益行为，涉及违规收集个人信息、强制频繁过度索取权限、超范围收集个人信息、强制用户使用定向推送功能、

信息窗口未提供关闭或退出标识、信息窗口摇一摇乱跳转、SDK 使用说明不完整等问题。相关 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）浙江省通信管理局

6 月 25 日，浙江省通信管理局通报 2024 年第 5 批 11 款侵害用户权益行为的 APP。通报指出，浙江省通信管理局近期组织第三方检测机构对群众关注的实用工具、本地生活、电子图书等类型 APP 进行检查，并书面要求违规 APP 开发运营者限期整改。截至目前，尚有 11 款 APP 未按要求完成整改，涉及违规收集个人信息、强制频繁过度索取权限问题。相关 APP 开发运营者在 7 月 4 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：工信部、浙江省通信管理局）

## 2. 上海市通信管理局印发通知，纵深推进“浦江护航”数据安全专项行动

6 月 20 日，上海市通信管理局印发《关于纵深推进“浦江护航”数据安全专项行动的通知》。

专项行动的主要对象为本市电信和互联网行业数据处理者。其中，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 100 万人以上个人信息等重要数据的电信业务经营者。

专项行动涉及七项重点任务，包括促进行业数据要素高效流通和利用、深化行业首席数据官制度实施、深入推进重要数据识别认定及目录管理、

实施人工智能应用领域数据安全管理等。其中，各单位要进一步加强数据安全风险排查和防范工作，落实工业和信息化部“数安护航”行动要求，对照《电信领域数据安全风险排查和防范指导手册》，重点防范数据非法收集、数据非法利用、防护措施不到位、人员违规操作等突出问题引发的数据泄露、滥用、勒索攻击等风险。各企业要统筹做好行业数据的开发利用和安全保护、新型技术的高效应用和风险防范等工作，对利用“人工智能+”应用和模型进行数据处理活动的场景加强备案记录和安全管理。

专项行动提出四项保障措施，分别是强化统筹协调、强化制度衔接、强化机构管理、强化人才培养。其中，将强化对在本市范围内开展电信和互联网行业数据安全服务的第三方机构的合规指导和监督管理。建立数据安全服务责任追究机制，本市各电信和互联网企业发生数据安全事件的，倒查其近两年内委托开展数据安全风险评估服务的第三方机构及其评估结果。（来源：上海市通信管理局）

## 3. 上海市通信管理局印发通知，开展 2024 年上海市电信和互联网行业网络和数据安全检查

6 月 24 日，上海市通信管理局印发《关于开展 2024 年上海市电信和互联网行业网络和数据安全检查的通知》。

检查对象为提供公共互联网网络信息服务的基础电信企业、互联网企业（含云平台服务提供商、APP 和小程序运营企业、车联网企业、工业互联网平台和标识解析节点企业等）、域名注册服务机构等。重点检查相关网络运行单位的重要网络单元及承载重要数据的信息系统，包括但不限于关

键信息基础设施、通信网络基础设施、公共云服务平台、域名服务系统、工业互联网平台、标识解析系统、车联网平台及应用等。

检查内容涉及六方面，包括网络和数据安全保障体系建设落实情况、车联网安全防护管理情况、数据安全保护落实情况、个人信息和用户权益保护工作情况等。其中，将在重大活动前，组织开展系统定级评测评估情况核查和远程网络安全检查，重点对2023年以来通报过通信网络安全防护管理问题的系统及其运营者进行复查。对未落实整改要求、未开展定级评测评估工作以及发现系统存在安全隐患、安全事件的企业，将依法依规予以处置，必要时依法采取暂停其网络接入等措施。

检查分为自查自纠、重点抽查、整改问责三个阶段。其中，重点抽查环节，市通信管理局将选取部分企业和相关系统，委托专业技术机构通过现场询问、查阅资料、现场检测、远程渗透、源代码检测等方式进行网络安全抽查。对检查时发现的薄弱环节、安全漏洞和安全风险，专业技术机构要及时形成检查结果记录报告，并上报市通信管理局。（来源：上海市通信管理局）

## 4. 江苏省通信管理局印发方案，开展江苏省“龙磐2024”网络和数据安全专项行动

6月28日，江苏省通信管理局印发《江苏省“龙磐2024”网络和数据安全专项行动方案》。

方案明确四项重点任务，分别是筑基赋能，固本强基构筑安全管理基石；技术赋能，关口前移防范化解安全风险；实战赋能，靶向施策提升应急处突水平；服务赋能，创新构建安全共享共治生态。

其中，方案要求各企业的三级网络、系统和定级为三级的工业互联网企业每年至少开展一次符合性评测和风险评估，二级网络、系统和定级为二级的工业互联网企业每两年至少开展一次符合性评测和风险评估。各企业要结合自身情况，聚焦典型突出风险，组织开展网络和数据安全实网攻防演练。江苏省通信管理局将组织相关企业开展网络和数据安全攻防演练，以攻促防，检验各企业应急预案的科学性、实用性和可操作性，提升实战化应对能力。

方案提出提高思想认识、层层压实责任、加强工作落实、强化风险防控四项工作要求。其中，方案要求演练过程中，参演红方不得对授权以外的资产进行渗透，不得进行破坏性测试；参演蓝方应做好防护准备，参照应急预案科学有效地开展应急处置；未经江苏省通信管理局允许，不得将发现的网络安全漏洞、演练方案、检查结果等信息进行泄露；如发生重大事件，及时向江苏省通信管理局报告。（来源：江苏省通信管理局）

## 5. 浙江省通信管理局印发通知，开展 2024 年电信和互联网行业网络和数据安全检查

6 月 28 日，浙江省通信管理局印发《关于开展 2024 年电信和互联网行业网络和数据安全检查的通知》，决定在 2024 年 7 月至 10 月开展 2024 年电信和互联网行业网络和数据安全检查。

检查对象为相关企业建设运营的网络、系统、平台、应用、业务，重点检查电信和互联网行业重要网络单元及承载的信息系统，包括但不限于：5G 行业应用、互联网接入服务系统、互联网数据中心、网上营业厅、企业门户网站、网络管理系统、网络交易系统、计费系统、域名系统、电子邮件系统、移动应用商店、公共服务云平台、网络预约出租汽车信息服务平台、移动智能终端及移动应用分发平台等。

检查内容包括网络和数据安全制度机制落实情况、网络安全技术防护情况、重大活动网络安全防护情况、数据安全保护落实情况、个人信息保护工作情况四方面。其中，网络安全技术防护情况将检查企业设备和服务供应链安全管理情况，企业网络和系统定级备案等。重大活动网络安全防护情况将围绕庆祝新中国成立 75 周年网络安全保障任务，对省内 11 地市相关互联网企业开展网络安全现场检查和远程检测，通过攻防演练等方式，实战检测各单位网络安全防护能力，及时发现并修复薄弱环节、安全漏洞和安全风险。（来源：浙江省通信管理局）

## （四）其他部门治理实践

### 1. 因数据安全管理不足等问题，国家金融监督管理总局对交通银行罚款 160 万元

6 月 3 日，因安全测试存在薄弱环节、运行管理存在漏洞、数据安全管理不足、灾备管理不足问题，国家金融监督管理总局依据《银行业监督管

理法》第四十六条和相关审慎经营规则，对交通银行股份有限公司处以160万元罚款。（来源：国家金融监督管理总局）

## 2. 浙江省云和县法院审理一起侵犯公民个人信息案，一公司组织员工购买70余万条个人信息充数

6月5日消息,浙江省云和县法院近日以侵犯公民个人信息罪判处刘某、朱某等14名被告人有期徒刑三年至六个月不等，缓刑五年至一年不等，各并处罚金，判处信息公司罚金500万元。与此同时，检察机关对其他涉案的11人作出相对不起诉处理。

本案中，刘某是湖南省长沙市某信息技术服务有限公司总经理。2020年11月，该公司中标了一项市场调研型项目，项目的主要工作就是通过账号密码登录某App，通过浏览获取指定酒店的价格、房型、是否提供早餐等信息。随后，该公司成立项目组，刘某作为总经理直接负责整个项目。

项目初期，由于甲方公司的需求量不大，该公司就让采集员自己注册账号进入某App进行人工采集并录入甲方公司的相关系统。但随着甲方公司的需求量逐渐变大，员工注册的单个账号已经无法满足需求。与此同时，某App也发现信息被采集的情况，启动风控措施，导致员工此前注册的许多账号无法登录继续采集相关信息。2021年5月，该公司决定通过向卡商购买公民个人信息及相关密码完成采集任务。该公司购买的公民个人信息均来自卡商朱某等人。

2022年1月，云和县公安局在办案中发现朱某等人出售公民个人信息的行为，随后对朱某等卡商立案侦查，于同年7月掌握刘某等人购买公民

个人信息的行为，其中涉及买卖公民个人信息70余万条，涉案金额达1800万余元。

2022年10月至2023年5月，公安机关陆续以刘某等25人涉嫌侵犯公民个人信息罪移送检察机关审查起诉。云和县检察院认定该公司构成单位犯罪，且公司获利570余万元。对负责项目决定审批、项目整体管理等核心工作的刘某等6人，认定为单位犯罪中直接负责的主管人员，依法提起公诉。对该公司中实施项目具体工作的业务组长或组员11人，认定为单位犯罪中其他直接责任人员，依法作出不起诉处理。而对出售公民个人信息的卡商朱某等8人，认定为侵犯公民个人信息的行为人，属于情节特别严重，依法提起公诉。

2023年8月至11月，云和县检察院以该公司及刘某等14人涉嫌侵犯公民个人信息罪陆续向法院提起公诉。截至今年3月，法院经陆续开庭审理后，对该公司及14名被告人判处相应刑罚，其中刘某被判处有期徒刑十个月，缓刑一年二个月，并处罚金5万元。（来源：检察日报正义网）

## 3. 广东省湛江市启动“湛盾—2024”攻防演练活动

6月12日，“湛盾—2024”湛江市数字政府网络安全攻防演练活动正式启动。本次活动由广东省政务服务和数据管理局指导，湛江市政务服务和数据管理局、市委网信办、市公安局共同主办，中国电信股份有限公司湛江分公司协办。

活动以“筑牢本质安全防线，护航数字湛江发展”为主题，邀请由国内专业网络安全企业和高校组成的15支高水平网络安全攻击队伍，对全市

非涉密重要政务信息系统开展为期5天的实兵、实网、实战攻防演练，挖掘网络安全突出问题和深层次漏洞隐患，以练促建、以练促改、以练促管、练建结合，全面提升数字政府网络和数据安全保障水平。

全市79个政务单位将以此次演练为契机，全面摸清网络安全“家底”，按活动设定规则积极进行防御和处置各类攻击入侵事件，查找突出问题、薄弱环节和潜在风险，对演练发现的问题及时整改，全面提升“人防”“物防”“技防”相结合的安全防控水平，共同打造可信可控的数字安全体系。（来源：网信广东）

## 4. 因数据治理问题，农行、浦发银行、徽商银行宁波分行被处罚

6月7日，因涉及数据治理等问题，国家金融监督管理总局宁波监管局对3家银行分别处以罚款。

农业银行宁波市分行因“授信管理不审慎、数据治理存在缺陷”等四项主要违法违规事实，国家金融监督管理总局宁波监管局依据《银行业监督管理法》第四十六条对其罚款180万元。

浦发银行宁波分行因“数据治理存在缺陷、授信业务管理不到位”等六项主要违法违规事实，国家金融监督管理总局宁波监管局依据《银行业监督管理法》第四十六条对其罚款275万元。

徽商银行宁波分行因“数据治理不到位、员工行为管理不到位”等七项主要违法违规事实，国家金融监督管理总局宁波监管局依据《银行业监督管理法》第四十五条、第四十六条对其罚款260万元。（来源：国家金融监督管理总局宁波监管局）

## 5. 国家计算机病毒应急处理中心发布15款移动APP隐私不合规情况

6月14日，国家计算机病毒应急处理中心发布15款移动APP隐私不合规情况，主要涉及十类不合规行为，分别是：

(1) 隐私政策未逐一列出App收集使用个人信息的目的、方式、范围等；未声明App运营者的基本情况。

(2) App客户端向第三方提供个人信息，未经过用户同意，未做匿名化处理；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，未取得个人的单独同意。

(3) App在征得用户同意前开始收集个人信息或打开可收集个人信息的权限。

(4) App未提供有效的更正、删除个人信息及注销用户账号功能，或为更正、删除个人信息或注销用户账号设置不必要或不合理条件；向用户提供撤回同意收集个人信息的途径、方式，未在隐私政策等收集使用规则中予以明确；注销用户账号的人工处理（承诺）时限超过 15 个工作日。

(5) App未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内受理并处理的。

(6) 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者未提供便捷的撤回同意的方式。

(7) 通过自动化决策方式向个人进行信息推送、商业营销，未同时提供不针对其个人特征的选项，或者未向个人提供便捷的拒绝方式；隐私政策未声明收集的用户个人信息用于定向推送、精准营销；隐私政策明示存在定向推送功能，页面中未见显著区分个性化推送服务。

(8) 处理敏感个人信息未取得个人的单独同意。

(9) 个人信息处理者处理不满十四周岁未成年人个人信息的，未制定专门的个人信息处理规则；收集未成年人信息未取得监护人单独同意。

(10) App 未向用户明示未经用户同意，且无合理的使用场景，存在频繁自启动或关联启动的行为。（来源：国家计算机病毒应急处理中心）

# 境外前沿观察：月度速览十则

导读：6 月，G7 峰会国家联合发布《七国集团领导人普利亚公报》，涉及网络安全、人工智能等议题，对当前 G7 国家如何应对网络安全和人工智能相关问题提出关注要点。韩国个人信息保护委员会、金融监督局等六部门签署《网络钓鱼防范谅解备忘录》，强化跨机构合作治理。美国国土安全部发布《2024-2025 年战略指南》，对关键基础设施安全保护进行部署安排。欧盟数据保护监督机构发布《生成式人工智能数据合规指引》，为欧盟机构使用生成式人工智能系统处理个人数据提供实操建议和指南。美国能源部发布《供应链网络安全原则》，明确能源行业自动化和工控系统供应链安全治理的基本路径。

美国两家知名企业在承包政府系统上线前未做安全测试，被罚 8200 万元。Meta 因使用个人数据训练人工智能模型收到多起投诉，目前因隐私问题暂停欧洲人工智能模型开发。美国联邦储备系统疑遭勒索软件攻击，泄露 33TB 敏感数据。印度特伦甘纳邦警察局应用程序遭网络攻击，导致数据信息泄露。印尼国家数据中心遭勒索赎金 800 万美元。

关键词：网络钓鱼、供应链网络安全、人工智能数据合规、勒索攻击、安全测试

## 1. G7 峰会国家联合发布《七国集团领导人普利亚公报》，涉及网络安全、人工智能等议题

6 月 14 日，G7 峰会国家在意大利联合发布《七国集团领导人普利亚公报》，内容涉及网络安全、人工智能等议题。

公报指出，面对日益复杂的战略性网络威胁，各国应展现出坚决的抵抗态度，并追究网络恶意行为者的法律责任。具体策略包括：（1）改善网络空间中负责任的国家行为；（2）在私营领域提升网络安全防护；（3）制定并应用措施以遏制和回应恶意国家行为及网络犯罪，破坏其基础设施，加强国际合作；（4）加大对同盟国家网络安全能力建设的支持。鉴于勒索软件攻击的猖獗，G7 峰会国家将高效执行国际反勒索软件倡议，并减少赎金支付行为，同时考虑对恶意实体施加制裁。

公报指出，人工智能在促进社会进步和发展中发挥关键作用。为促进安全可信的人工智能发展，应关注以下要点：（1）安全可靠性。推动安全、可靠和可信的人工智能发展；（2）数字转型。追求包容性、以人为本的数字转型，支持经济增长和可持续发展；（3）治理合作。促进包容性的人工智能治理方法，加强全球性合作；（4）互操作性和协调。提高不同人工智能治理方法间的互操作性，推动建立问责机制和提高透明度；（5）风险管理。采取基于风险管理的方法，促进创新和可持续增长；（6）军事应用。采取负责任的方式在军事领域开发和使用人工智能，确保军事应用人工智

能符合国际法；（7）司法独立。确保人工智能系统的使用不会侵犯法官的决策权进而影响司法独立。（来源：欧洲委员会）

## 2. 韩国个人信息保护委员会等六机构联合签署《网络钓鱼防范谅解备忘录》，强化跨机构合作治理

6 月 3 日，韩国个人信息保护委员会、科学和信息通信技术部、金融委员会、金融监督院、国立科学搜查研究院和韩国互联网振兴院联合签署《网络钓鱼防范谅解备忘录》，旨在扩大机构间在应对语音网络钓鱼活动方面的合作范围和深度。

备忘录要点包括：（1）数据共享。政府机构将与私营公司共享语音钓鱼通话数据，以帮助开发测试预防语音钓鱼的人工智能模型。同时，私营公司会对数据进行去标识化处理，强化个人信息保护；（2）行业合作治理。政府机构正在推动电信和金融行业合作，共同开发防范语音钓鱼的人工智能技术，并建立健全相关法律法规，推动人工智能技术在合法合规的情况下进行部署应用；（3）政府主导技术开发。科学和信息通信技术部、韩国个人信息委员会正在规划和推动政府主导的技术开发项目，开发语音网络钓鱼检测和预防技术。（来源：韩国个人信息保护委员会）

## 3. 欧盟数据保护监督机构发布《生成式人工智能数据合规指引》

6 月 3 日，欧洲数据保护监督机构（EDPS）发布《生成式人工智能数据合规指引》，旨在为欧盟机构使用生成式人工智能系统处理个人数据提供

实操建议和指南。指引对生成式人工智能的概念进行界定，明确生成式人工智能是人工智能的子集，通过使用专门的机器学习模型生成文本、音视频等内容。

指引针对生成式人工智能场景下的数据保护提出一系列基本要求，要点包括：（1）欧盟机构在符合法律要求的前提下，原则上可以开发、部署、使用生成式人工智能系统提供公共服务。公共部门使用新技术时应当充分尊重个人的基本权利和自由，在生成式人工智能模型供应链中，需要明确各参与者的责任，确保合规；（2）生成式人工智能系统中的个人数据处理可能发生在不同阶段，若开发者或服务提供者的系统不处理个人数据，应要求开发者或服务提供者提供具体控制措施的详细信息，确保未处理个人数据；（3）强调数据保护官（DPO）的作用。DPO 负责提供有关数据保护的建议，监控内部合规，提供有关数据保护影响评估的建议，并作为数据主体和欧洲数据保护监管机构的联络点，与组织内部各职能部门保持联络；（4）生成式人工智能系统的个人数据处理涵盖系统生命周期内的所有处理活动，欧盟机构处理个人数据应当依据相关法律，在特定情况下处理个人数据时应征求当事人同意。（来源：欧洲委员会）

## 4. 美国国土安全部发布《2024-2025 年战略指南》，对关键基础设施安全保护进行部署安排

6 月 14 日，美国国土安全部（DHS）发布《2024-2025 年战略指南》，旨在提升美国关键基础设施面临人工智能等系统带来新兴威胁时的安全性和弹性。

指南指出，在全球数字化加速发展的背景下，电网、水处理、交通和医疗等关键基础设施的自动化与数字化程度加深，使得关键基础设施安全防护成为迫切需求。DHS 致力于将人工智能纳入战略考量，指出人工智能作为变革性技术在关键基础设施保护中的潜力与挑战。尽管人工智能技术能够提高关键基础设施的防御能力，提升网络运营安全水平，但同时也需警惕人工智能技术滥用对关键基础带来的风险。因此，DHS 鼓励关键基础设施运营者探索在内部部署人工智能技术，辅助网络安全和威胁监测。

此外，指南还强调量子计算对现有密码体系构成的安全风险，DHS 将与 NIST 合作制定指南文件，帮助关键基础设施实体应对量子计算带来的密码和数据安全挑战。（来源：美国国土安全部）

## 5. 美国能源部发布《供应链网络安全原则》

6 月 19 日，美国能源部（DOE）发布《供应链网络安全原则》，旨在明确能源行业自动化和工控系统（ICS）供应链安全治理的基本路径。

文件针对供应商提出一系列指导原则，要点包括：（1）基于影响驱动的风险管控。供应商应将产品全生命周期存在的安全风险、上游供应链节

点带来的安全风险都纳入考量，进行一体化管控；（2）安全防御设计。供应商应吸收既有网络安全框架中的防御理念和最佳实践，融入关键功能和基础设施设计之中；（3）安全开发和部署。遵循国际认可的框架和指南，对系统进行安全开发；（4）透明度。向用户和公众提供网络安全态势和产品安全信息；（5）实施指南。提供包括默认设置和行为的管理在内的安全实施指南；（6）积极漏洞管理。采用符合行业最佳实践和协同漏洞披露程序的漏洞管理框架，对发现的漏洞进行负责任处置和披露。

文件针对最终用户提出一系列指导原则，要点包括：（1）基于影响驱动的风险管控。最终用户应考虑产品全生命周期带来的网络安全风险；（2）防御措施。最终用户应整合网络安全框架，设计关键功能和信息防护；（3）透明度和信任建设。最终用户与供应商签订的合同应包含安全条件和测试要求；（4）产品全生命周期支持和运营。最终用户进行商业规划和资源配置，确保产品在全生命周期得到维护和更换。（来源：美国能源部）

## 6. 因使用个人数据训练人工智能模型被多次投诉，Meta 暂停欧洲人工智能模型开发

6 月 6 日，因计划使用客户数据训练人工智能，Meta 公司面临来自 11 个欧洲国家的数据保护机构的投诉，这些投诉由隐私维权组织 Noyb 发起。

Meta 意图利用用户的历年帖子来发展人工智能技术，未明确征求用户同意，用户需主动选择才能退出此默认设置，且一旦数据用于模型则似乎无法删除。根据 GDPR 第 22（2）条规定，欧洲用户可通过特定步骤选择退

出，非欧洲用户则无法行使此权利。Noyb 的创始人批评 Meta 的政策与 GDPR 相悖，担忧数据用途不明且可能被广泛分享。

6 月 17 日消息，Meta 因隐私问题暂停欧洲 GenAI 开发。（来源：英国路透社）

## 7. 因在承包政府系统上线前未做安全测试，美国两家知名企业被罚 8200 万元

6 月 17 日消息，因在执行纽约州紧急租赁援助计划（ERAP）时未能确保适当的网络安全措施，美国知名咨询公司 Guidehouse 和 Nan McKay and Associates（NMA）近日同意支付共计 1130 万美元的罚款。Guidehouse 承担其中 760 万美元，NMA 承担 370 万美元。这一和解源于前 Guidehouse 员工的举报，后者将获得 194.925 万美元的奖励。

ERAP 是在 2021 年初由美国国会设立的全国性项目，旨在疫情期间为低收入家庭提供住房相关财政援助。纽约州选择 Guidehouse 作为主要承包商，NMA 作为其分包商，共同负责 ERAP 系统的实施与服务。然而，两家公司在未充分测试网络安全的情况下上线系统，导致申请人的个人信息暴露于互联网。尽管事后调查未发现未经授权的个人身份信息（PII）使用情况，但小范围的 PII 仍被商业搜索引擎捕获，构成信息泄露。Guidehouse 还被发现未经批准使用第三方云软件存储敏感信息，进一步违反合同规定。

纽约北区检察官强调，接收联邦资金的承包商有责任严格遵守网络安全义务，否则将面临法律责任。NMA 在回应中表示，尽管与政府达成和解，

但并未承认在《虚假申报法》下的任何责任，并坚称其在住房计划管理方面的声誉不受影响。（来源：英国科技新闻）

## 8. 印度特伦甘纳邦警察局应用程序遭网络攻击，大量警察和犯罪分子个人数据泄露

6 月 5 日消息，印度特伦甘纳邦警察局的 TSCOP 应用程序近日遭到黑客攻击，造成大量警察和犯罪分子的个人数据泄露。此次攻击由不法分子 Adm1nFr1end 策划，此人被认为是 HawkEye 应用程序数据泄露事件的幕后黑手。此次泄露的信息包括反腐败局、反毒品局、情报局等多个部门的警察姓名、电话号码和电子邮件地址。此外，黑客曝光了近期登记的罪犯数据及其详细信息，以及申请枪支许可证的公民的个人信息。网络安全专家指出，特伦甘纳邦警察局的网络系统存在身份验证和编码问题，易受到黑客攻击。目前，特伦甘纳邦警方尚未对此次攻击事件做出回应。（来源：Cyber Express）

## 9. 美国联邦储备系统疑遭勒索软件攻击，泄露 33TB 敏感数据

6 月 24 日消息，美国联邦储备系统的名字近日出现在勒索软件组织 LockBit3.0 的数据泄露网站受害者清单中，LockBit 在勒索通知中宣称 2024 年 6 月 23 日入侵美联储系统，窃取了 33TB 的金融信息，其中包含“美国金融业的秘密”。LockBit 给出的赎金支付截止日期是 UTC 时间 6 月 25 日晚八点半。根据勒索通知，LockBit 勒索软件组织要求美联储更换谈判专家，

因为后者的出价仅为5万美元。截至目前，美联储尚未公开确认此次入侵事件，也未提供有关响应工作的详细信息。

LockBit3.0是近年来最危险和多产的与俄罗斯有关的勒索软件组织，曾攻击过中国工商银行和波音公司等大型组织。此次针对美联储的攻击不排除是报复性行为。拜登政府近期全面禁止销售和使用卡巴斯基反病毒软件，并制裁12名卡巴斯基高管。（来源：SC Media）

## 10. 印尼国家数据中心遭勒索攻击，赎金800万美元

6月24日消息，印尼国家数据中心近日遭到黑客组织攻击，该组织索要800万美元赎金（约合1310亿印尼盾），以交换201份被盗数据，但印尼政府表示不会支付。印尼通信和信息部表示，自6月20日以来，网络攻击已经扰乱了国家和地区200多个政府机构的服务，其中一些政府服务已经恢复，机场和其他地方的移民服务现已正常运转，但仍在努力恢复投资许可等其他服务。国家网络和密码局承认国家数据中心遭到黑客攻击，黑客疑似使用最新的勒索软件LockBit 3.0攻击政府服务器，服务器管理着各部委和机构以及地方政府的国家数据。（来源：网空闲话）

# 行业前沿观察一：2024 网民网络安全感满意度调查活动样本采集工作于 7 月 17 日启动、中央网信办启动“清朗·2024 年暑期未成年人网络环境整治”专项行动、“第六届互联网辟谣优秀作品”揭晓、《中国互联网发展报告（2024）》正式发布

导读：近日，中央网信办专门印发通知，在全国范围内部署开展为期 2 个月的“清朗·2024 年暑期未成年人网络环境整治”专项行动。

网民网络安全感满意度调查活动组委会发布《关于开展 2024 网民网络安全感满意度调查活动样本采集工作的通知》，公布将于 7 月 17 日正式启动 2024 年度调查样本采集工作，届时全国将同步开通样本采集通道。

7 月 5 日，第六届互联网辟谣优秀作品发布会在四川成都举行。第六届互联网辟谣优秀作品分为“文字类”“图片类”“动漫音视频类”“重大辟谣专题”四个类别。自今年 3 月启动作品征集以来，得到社会各界积极支持和踊跃参与，共收到 1700 余家单位和个人报送的 2600 多部作品。

7 月 11 日，由中国互联网协会主办的 2024（第二十三届）中国互联网大会在京闭幕。中国互联网协会副秘书长裴玮在大会闭幕式上发布《中国互联网发展报告（2024）》。

关键词：数字乡村、信息化、工信部、网络安全、网络谣言、网络强国

## 1. 2024 网民网络安全感满意度调查活动样本采集工作于 7 月 17 日启动

近日，网民网络安全感满意度调查活动组委会发布《关于开展 2024 网民网络安全感满意度调查活动样本采集工作的通知》，公布将于 7 月 17 日正式启动 2024 年度调查样本采集工作，届时全国将同步开通样本采集通道。此次采集工作将持续 10 天，于 7 月 26 日结束。

通知提到，为全面贯彻落实习近平总书记关于“网络安全为人民、网络安全靠人民”的重要讲话精神，在各级党政相关主管部门的关心指导和各发起单位的共同努力下，网民网络安全感满意度调查活动（以下简称“调查活动”）已连续成功举办六届，累计采集调查有效样本量突破千万份，收集汇总网民意见建议近百万条，浏览和点击数据量 2 亿多次，发布全国总报告、专题报告、行业报告、区域报告等专业性调查报告近千份。调查数据被政府部门、研究机构广泛引用、权威发布，成为我国网络安全研究、互联网综合治理工作的有力支撑。

通知强调，各发起单位可向组委会推荐本地有意愿、有能力的相关机构加入调查活动发起单位和支持单位。为保障各地顺利开展工作，组委会今年推出了全面、详尽的志愿服务支持，可通过“网安联小程序”了解调查活动以及网安联志愿服务站（队）、公益讲师、公益宣传员、志愿者等相关工作。

通知就2024调查活动的相关安排、发起/支持单位报名方式、样本采集工作指引、资料提供、“网安联”小程序介绍（含志愿服务功能操作介绍）、总结表彰等进行了说明。（来源：网安联）

## 2. 中央网信办启动“清朗·2024年暑期未成年人网络环境整治”专项行动

为切实加强未成年人网络保护，营造更加健康安全的网络环境，近日，中央网信办专门印发通知,在全国范围内部署开展为期2个月的“清朗·2024年暑期未成年人网络环境整治”专项行动。

本次专项行动将重点整治6个环节突出问题。一是短视频、直播平台。“二次包装”经典动画或儿歌，集中展示暴力血腥内容。摆拍校园霸凌视频，将校园霸凌行为娱乐化。利用“网红儿童”牟利，恶搞儿童博取关注、卖惨引流。采取剧情电台、语音旁白等方式，诱导胁迫未成年人变相参与直播等问题。二是社交平台。在未成年人照片分享、交友信息等页面，发布诱导不良交友、引流非法网站等信息。对未成年人实施“网络厕所”“人肉开盒”等行为。恶意编造网络黑话、低俗流行语，向未成年人传播不良价值观。创建专门话题、群组等，恶意发布反击攻略、进行恶意P图，煽动亲子、师生对立等问题。三是电商平台。向未成年人售卖软色情手办文具、动漫周边等商品。利用儿童模特摆出不雅姿势、做性暗示动作，借未成年人形象进行无底线营销。提供有偿代骂，制作恶搞同学、学校的图文

视频等服务。以售卖动漫剧作、电子游戏等为名，引流未成年人至第三方平台，违规提供涉黄涉暴资源等问题。四是应用商店。利用相似标志和名称信息，仿冒未成年人喜爱的APP，传播违法不良信息。通过内嵌非法软件或违规马甲包等方式，恶意“变身”为涉黄涉赌平台。学习类、工具类APP偏离主责主业，传播打擦边球违规信息。具有匿名、加密等属性的小众APP，存在网络诈骗、隔空猥亵等问题。五是儿童智能设备。设备自带APP包含可能影响未成年人身心健康的内容。对第三方APP提供的信息内容审核把关不严，存在不良导向内容。提供相貌PK、运势测算等不适宜未成年人的应用或功能。以积分排行、功能解锁、背景更新等为名，诱导未成年人过度消费。六是未成年人模式。提供“虚假模式”，用户进入未成年人模式后无内容、无法使用。模式下存在诱导未成年人模仿不安全行为、养成不良嗜好等内容。模式防逃逸措施不完备，无需验证即可退出。模式下存在诱导未成年人投票打榜、刷量控评等功能。

中央网信办有关负责同志强调，清朗的网络环境对未成年人健康成长至关重要。各地网信部门要按照通知要求，认真部署、精心组织、扎实推进，抓好专项整治任务落实。要密切关注涉未成年人问题新特点新表现，对各类违规行为，保持高压态势，从严处置违规平台、账号及相关MCN机构。要压实平台主体责任，健全平台未成年人网络保护机制，共同维护良好网络生态。（来源： 中国网信网）

## 3. “第六届互联网辟谣优秀作品”揭晓

7 月 5 日，第六届互联网辟谣优秀作品发布会在四川成都举行。中央网信办副主任、国家网信办副主任杨建文，新华社副社长、党组成员刘健，四川省委常委、宣传部部长郑莉，成都市委常委、宣传部部长辜学斌出席发布会并致辞。

第六届互联网辟谣优秀作品分为“文字类”“图片类”“动漫音视频类”“重大辟谣专题”四个类别。自今年 3 月启动作品征集以来，得到社会各界积极支持和踊跃参与，共收到 1700 余家单位和个人报送的 2600 多部作品。经过作品初审、网络投票、专家复审和综合评定，最终推选出《社保卡有四种颜色？看这篇，拒绝误传！》《条漫：新“武松打虎”》《大魔术师》《三星堆问答》等 60 部优秀辟谣作品。这些作品聚焦社会热点、回应群众关切，在揭示谣言套路、传递事实真相、创新辟谣方式、提升传播效果方面发挥良好示范作用。

第六届互联网辟谣优秀作品征集发布活动由中央网信办违法和不良信息举报中心、四川省委网信办、成都市委网信办主办，新华网、成都市广播电视台承办。来自中央和国家机关有关单位、地方网信部门、基层单位、行业协会、新闻媒体、网站平台的嘉宾和获奖作者代表 180 余人参加发布会。（来源：中国网信网）

## 4.《中国互联网发展报告（2024）》正式发布

7 月 11 日，由中国互联网协会主办的 2024（第二十三届）中国互联网大会在京闭幕。中国互联网协会副秘书长裴玮在大会闭幕式上发布《中国互联网发展报告（2024）》。

《报告》显示，2023 年以来，我国互联网行业深入贯彻党的二十大精神，坚决落实《数字中国建设整体布局规划》等战略部署，我国网络基础设施建设日益完备，关键前沿技术创新发展，关键领域数字化水平稳步提高，网络综合治理框架加速构建，网络安全产业高质量发展，数字中国发展呈现出良好态势。

具体来看，我国互联网行业呈现如下发展特征，一是在基础资源与技术方面，我国 5G、千兆光纤网络等新型信息基础设施建设日益完备，下一代互联网 IPv6 用户和流量规模显著提升，卫星互联网建设稳步推进，光纤宽带网络服务能力不断增强；算力基础设施建设达到世界领先水平，智能算力规模占比提升至 30%，云计算市场规模快速增长；数据要素统筹管理体制更加完善，分类推进数据要素发展成为共识；人工智能产业应用进程持续推进，多种服务模式逐渐涌现，高质量数据需求日益凸显；移动物联网络用户数量大幅增长，物联网应用进入规模化爆发期。二是在互联网应用与服务方面，工业互联网进入规模发展新阶段，数实深度融合服务新型工业化建设；电子商务市场稳定增长，数字消费新动能愈加强劲；商务交易类应用模式业态持续迭代，跨境电商等新业态迅猛发展；数字文娱用户规模持续攀升，AIGC 赋能数字文娱发展，垂直大模型应用纷纷落地。三是在

网络治理与环境方面，互联网治理体系进一步完善，基层社会治理增“数”赋“智”；网络安全产业进入快速成长阶段，数字安全成为数字发展战略保障。

展望未来，我国互联网行业将继续深入贯彻数字中国建设部署要求，一是数字基础设施建设进一步提速发展，以6G、卫星互联网等为代表的新式网络基础设施加快部署，算力基础设施布局进一步优化，算力资源配置更加合理有序。二是数字技术创新将逐步推动互联网向智能化迈进，“人工智能+”行动的实施和多模态大模型的快速发展将推动新一代人工智能技术加速拓展应用场景。三是算法、算力与数据的核心作用将更加凸显，算力发展需求推动高端芯片自主研发和制造能力不断提升，数据资源将与人工智能技术耦合发展，不断催生新产业、新模式、新业态，生成新的经济增长点。四是中国式网络治理框架加快构建，人工智能等重点领域与新技术治理将逐渐走向制度化、法律化的道路，监管框架与原则性治理规则更加明确，多部门共同治理格局逐渐形成。五是行业融合应用将赋能价值互联，推动人、机、数据等关键要素进一步融合，加速制造业数字化、智能化升级。六是数字领域国际合作空间将进一步拓展，“数字丝绸之路”建设继续稳步推进，“丝路电商”伙伴国的范围将进一步扩大。

中国互联网协会组织编撰的《中国互联网发展报告》（以下简称“《报告》”）是中国互联网领域的大型编年体研究报告，是中国互联网行业发展忠实的记录者和见证者。《报告》自2002年开始出版，每年一卷，目前已连续发布23年。中国互联网协会持续跟进我国互联网发展历程，总结现

状、深化研究、探索规律，中国互联网发展描绘全新场景，为政府部门、行业机构、业界专家了解和掌握中国互联网发展情况提供全面参考，共同把握数字化发展机遇，推进网络强国、数字中国建设。（来源：中国互联网大会）

# 行业前沿观察二：各地协会动态

导读：各地协会活动精彩纷呈，举行博览会、教育发展大会、表彰会等，助推网络安全发展。湖北省信息网络安全协会：将在世界大安全博览会举办活动；西藏自治区互联网协会：主办 2024 年第二届西藏自治区数字教育发展大会；武汉市网络安全协会：举办在汉高校网络安全应用场景供需对接会；北京网络行业协会：圆满举办协会第四届第三次会员代表大会暨理事会；辽宁省信息网络安全协会：成功举办网络安全专场招聘会；上海市信息网络安全管理协会：发起 2024 年度“新耀东方”风采人物事迹征集活动；上海市信息安全行业协会：圆满召开协会第五届第四次会员大会暨 2023 年度表彰大会；湖南省网络空间安全协会：成立协会网络安全等级保护工作专委会；揭阳网络空间安全协会：承办 2024 年“全国科技工作者日”网络数据安全学术交流会；重庆信息安全产业技术创新联盟：成功举办软件供应链安全现状、发展及人才培养讲座。。

关键词：数字教育、招聘、数据安全、信息安全、网络安全、信息安全、网络强国

## 1. 湖北省信息网络安全协会：将在世界大安全博览会举办活动

6 月 25 日，武汉国际安全应急博览会活动各主承办协办单位负责人一起召开了筹备工作对接会，研究讨论世界大安全博览会筹办工作。湖北省信息网络安全协会会长王耀发、秘书长刘莉参加筹备会并提出意见和建议。

王耀发在会上首先热烈欢迎各位嘉宾的到来，并衷心感谢他们在安全应急领域的辛勤付出。他指出，作为连续四届武汉国际应急博览会主办方之一，未来举办的第五届世界应急博览会应当以创新为主旨，办出品牌、办出特色，结合中部地区的安全应急管理特色和产业优势，举办一场与历届安全应急博览会不同特色的活动。

## 2. 西藏自治区互联网协会：主办 2024 年第二届西藏自治区数字教育发展大会

6 月 20 日，由西藏自治区教育厅、区通信管理局、区党委网信办指导，西藏自治区互联网协会、区通信行业协会联合区电化教育馆主办的 2024 年第二届西藏自治区数字教育发展大会在拉萨顺利召开。

大会内容丰富，亮点纷呈。教育部信息中心公共平台处、中国信息通信研究院技术与标准研究所、电信、移动等单位企业的专家分别作主题演讲和分享，从不同角度讲述了教育数字化转型升级的应用实践和发展前景。

并举行对话数字教育研讨会，就当前西藏自治区数字教育案例和行业前沿应用展开交流研讨。

除了丰富的主题分享、研讨会外，大会现场布置了数字教育暨“5G+”行业应用展区。此次大会是数字赋能千行百业三年行动计划启动后，首次与教育行业联合开展数字赋能相关工作，为西藏自治区教育行业发展增添助力。

## 3. 武汉市网络安全协会：举办在汉高校网络安全应用场景供需对接会

6 月 25 日，武汉市临空港经开区现代服务产业建设管理办公室会同武汉市网络安全协会在国家网络安全人才与创新基地网安创新中心成功举办了“在汉高校网络安全应用场景供需对接会”。

活动旨在搭建一个高校与企业深入交流、供需精准对接的平台，共同探索网络安全产学研用创新发展之路。活动吸引了在汉六十余所高校网信工作负责人及部分计算机与网络安全院系负责人，同时汇集了四十家网络安全领域的领军企业参与。

对接会上，各方代表们就网络安全领域的最新技术趋势、应用场景需求、人才培养等方面进行了深入交流和探讨。各企业的展台设计新颖、内容丰富，充分展示了最新的网络安全技术、产品和解决方案。现场还举办

了多场技术交流和对接活动，为高校与企业之间搭建了直观、高效的沟通平台。

## 4. 北京网络行业协会：圆满举办协会第四届第三次会员代表大会暨理事会

北京网络行业协会第四届第三次会员代表大会暨理事会于近期圆满召开，协会理事单位以及会员单位代表参加了大会。

会议通过线上和线下相结合的方式，审议并投票通过了《北京网络行业协会 2023 年度工作报告》；《北京网络行业协会 2023 年度财务收支情况报告》；《北京网络行业协会章程》修正案；以及《北京网络行业协会会费收取和管理办法》修正案；增补国源天顺科技产业集团有限公司为协会常务理事单位；增设北京网络行业协会网络与数据安全专业委员会等决议。

## 5. 辽宁省信息网络安全协会：成功举办网络安全专场招聘会

在辽宁省公安厅网安总队的指导和大力推动下，辽宁大学信息学部联合辽宁省信息网络安全协会于 6 月 24 日下午，在崇山校区成功举办了网络安全专场招聘会。

此次专场招聘会汇聚19家网络安全领域知名企业，吸引120余人参加，现场收取简历400余份。招聘会现场气氛活跃，秩序井然。用人单位与学生面对面交流，介绍企业情况和岗位信息，深入了解学生求职需求，实现供需的高效对接。学生以积极态度和充分准备参加招聘会，展现了良好的专业素养和求职热情。

## 6. 上海市信息网络安全管理协会：发起2024年度“新耀东方”风采人物事迹征集活动

为持续展示网络安全领域专业人士在推动行业创新发展中的突出贡献和独特风采，上海市信息网络安全管理协会、上海公益新媒体中心联合发起2024年度“新耀东方”风采人物事迹征集活动，旨在进一步弘扬网络安全行业的正能量，树立优秀标杆，激励广大从业者奋发向前，共同推动行业的蓬勃发展。

活动面向全行业广泛征集网络安全从业者的优秀事迹，鼓励广大从业者积极申报并分享创新成果、实践经验及行业贡献。表彰结果将通过媒体宣传和网络传播等多种方式，全面展示优秀事迹，提升网络安全行业的社会认可度和影响力。

2024年8月2日，将在“新耀东方-2024上海网络安全博览会暨发展论坛”开幕式期间举行2024年度“新耀东方”风采人物表彰仪式。

## 7. 上海市信息安全行业协会：圆满召开协会第五届第四次会员大会暨 2023 年度表彰大会

5 月 30 日下午，上海市信息安全行业协会第五届第四次会员大会暨 2023 年度表彰大会顺利召开。上海市经信委综合规划处处长赵广君、上海市经信委软件和信息服务业处华宇涵、上海市普陀区科学技术委员会科技产业科张凤，以及协会会员单位代表共计 200 余人参加会议。大会由协会副会长石坚主持。

大会汇报了协会《2023 年工作总结及 2024 年工作计划》和《2023 年度监事会报告》等内容，并对新入会的会员单位进行了介绍，为 2023 年度在推进上海市网络和信息安全行业健康、可持续发展中作出贡献的会员单位及个人进行表彰，包括【优秀会员单位】、【优秀成果】、【优秀工作者】、【优秀联络员】四项荣誉。

## 8. 湖南省网络空间安全协会：成立协会网络安全等级保护工作专委会

湖南省网络空间安全协会网络安全等级保护工作专委会（以下简称“等保专委会”）于近日正式成立。

据悉，等保专委会将着力推动等保测评报告抽检常态化，进一步健全完善等保测评与测评机构高质量发展考核评价体系，加强网络安全等级保

护测评机构监督管理，规范测评行为，提高测评机构技术能力和规范化、标准化水平，促进我省网络安全等级保护测评体系健康发展。

等保专委会将于6月份由主任及副主任单位组织召开成员大会,对2024年工作作出部署安排，明确全年工作目标、内容及措施，严明工作纪律，确保等保测评检查工作出成效、促规范。

## 9. 揭阳网络空间安全协会：承办2024年“全国科技工作者日”网络数据安全学术交流会

2024年5月30日是第八个全国科技工作者日。当天，由揭阳市科学技术协会主办、揭阳网络空间安全协会承办的2024年“全国科技工作者日”网络数据安全学术交流会在中国电信揭阳分公司信息化展厅举办，主题是“科技创新和高质量发展”。

活动会场设置了屠呦呦、黄旭华、邓稼先等我国优秀科学家先进事迹展板，营造了浓厚的弘扬科学家精神氛围；会议传达学习了习近平总书记关于科技创新的重要论述精神，并向所有科技工作者致敬。

## 10. 重庆信息安全产业技术创新联盟：成功举办软件供应链安全现状、发展及人才培养讲座

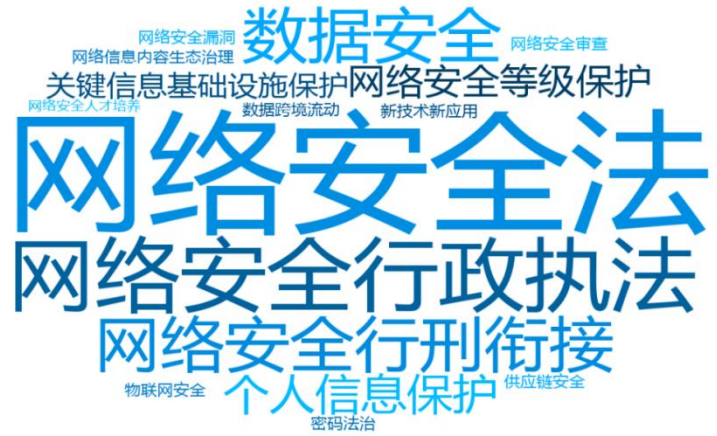
5 月 29 日，重庆信息安全产业技术创新联盟特邀深圳开源互联网安全技术有限公司副总经理王颉，在重庆人文科技学院举办“软件供应链安全现状、发展及人才培养”讲座。

讲座围绕软件安全基本知识、软件供应链安全国内外现状、软件供应链安全国标框架及要点、建设实践、软件供应链安全人才培养模式等方面进行了深度阐述。

# 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

**02 风险评估** — 3 - 5 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

**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

……