



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3月第3期 (总第20期)

2025年3月15日

目 录

境内前沿观察一：安全事件	1
1. 张国清出席法国人工智能行动峰会并致辞	4
2. 首批 200 名缅甸妙瓦底地区的中国籍涉诈犯罪嫌疑人经泰国被押解回国	5
3. 国家互联网信息办公室举办欧盟在华企业数据跨境流动政策座谈会	6
境内前沿观察二：政策立法	7
(一) 国家层面动向	9
1. 中泰发布联合声明，强调打击跨境犯罪	9
2. 国务院公布《公共安全视频图像信息系统管理条例》	9
(二) 部委层面动向	11
1. 中共中央、国务院印发《国家突发事件总体应急预案》	11
2. 国家互联网信息办公室发布《个人信息保护合规审计管理办法》	12
3. 国家数据局综合司、公安部办公厅印发《全国数据资源统计调查制度》	13
4. 全国数据标准化技术委员会秘书处发布《关于发布 2025 年第一批数据领域国家标准需求的通知》	13
5. 自然资源部发布《导航电子地图安全处理技术基本要求（征求意见稿）》	14

6. 商用密码标准研究院开展新一代商用密码算法征集活动	14
（三） 地方层面动向	15
1. 上海市网信办等五部门印发自由贸易试验区数据出境负面清单管理办法、负面清单（2024 版）	15
2. 天津市工业和信息化局发布《天津市促进智能网联汽车发展条例（征求意见稿）》	16
境内前沿观察三：治理实践	18
（一） 公安机关治理实践	20
1. 山西省公安发布“净网 2024”专项行动打击网络违法犯罪 10 起典型案例	20
2. 湖北省松滋市公安侦破一起虚拟货币诈骗案	22
3. 江苏省徐州市公安破获一起有偿提供虚假流量服务的网络水军案	23
（二） 网信部门治理实践	24
1. 中央网信办发布“清朗·2025 年春节网络环境整治”专项行动治理成效	24
2. 中央网信办召开全国网络法治工作会议	24
3. 中央网信办发布 2025 年“清朗”系列专项行动整治工作重点	26
4. 中央网信办发布 2024 年全国网信系统打击网络违法违规行为工作成果	27

5. 国家网信办依法集中查处一批侵害个人信息权益的违法违规 App	27
6. 上海市委网信办召开属地 MCN 机构分类指导会，试行内容生态合规指引	28
7. 鄂尔多斯市委网信办对两家单位进行网络安全约谈	29
8. 聚焦保护“个人信息删除权”，上海市网信办依法约谈一批 App 运营者	30
(三) 通信管理部门治理实践	31
1. 上海、安徽等省通信管理局发布侵害用户权益 APP	31
(四) 其他部门治理实践	33
1. 最高人民法院发布六起依法惩治利用网络敲诈勒索犯罪典型案例	33
2. 最高检发布两起侵犯公民个人信息典型案例	38
3. 杭州互联网法院发布一起涉生成式人工智能平台侵害信息网络传播权案	40
4. 江苏高院发布涉外商事审判典型案例，涉境外虚拟货币投资	41
5. 杭州互联网法院发布一起操纵网络水军案	42
6. 北京互联网法院发布全国首例人工智能文生图著作权侵权案	43
境外前沿观察：月度速览十则	44

1. 美国白宫发布总统备忘录《美国优先投资政策》	46
2. 多个国家和国际组织签署巴黎人工智能宣言，英美拒签	47
3. 日本内阁通过《人工智能相关技术的研发及应用促进法》 草案	47
4. 英国政府发布《英国政府人工智能手册》	48
5. 欧盟《网络团结法》生效	49
6. 欧盟委员会发布网络安全蓝图提案，强化危机协调	50
7. 俄罗斯政府提议新惩罚措施打击网络犯罪	51
8. DeepSeek 遭到多国调查与禁止	52
9. 美国法院裁决或阻碍人工智能发展，禁止未经许可使用受 版权内容训练 AI	53
10. 因非法获取用户数据，苹果在韩被罚 24.5 亿韩元	54

行业前沿观察一：两部门联合发文加强智能网联汽车召回及软件在线 升级管理；四部门联合开展数字乡村强农惠农富农专项行动；工业和信息 化部发文提升卫星网络国内协调效率	55
---	-----------

1. 两部门印发关于进一步加强智能网联汽车产品准入、召回及软 件在线升级管理的通知	56
2. 中央网信办 农业农村部 商务部 中国人民银行联合开展数字 乡村强农惠农富农专项行动	61
3. 工业和信息化部发文提升卫星网络国内协调效率	62

行业前沿观察二：各地协会动态	64
-----------------------------	-----------

1. 广东省网络空间安全协会获评“广东省科普教育基地”	65
2. 甘肃省商用密码行业协会成功召开协会二届二次理事会	65
3. 武汉市网络安全协会成功召开协会第二届理事会第五次会议	66
4. 上海市信息安全行业协会“船舶网络安全，护航智慧海事”研 讨会顺利举办	66
5. 海南省网络安全和信息化协会两省协会联合开展“2025 冀琼新 一代信息技术交流活动”	67
6. 甘肃省商用密码行业协会组织开展 2024 年度商用密码应用推广 典型案例评选工作	67

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

顾问：严明 公安部第一、第三研究所 原所长、研究员
中国计算机学会计算机安全专业委员会 主任

指导专家：袁旭阳 北京网络行业协会 会长
公安部网络安全保卫局原 副局长

总编辑：黄道丽 公安部第三研究所网络安全法律研究中心 主任

副总编辑：鲍亮 公安部第三研究所网络安全技术研发中心 副主任

编委会主任：黄丽玲 北京网络空间安全协会 理事长

编委会副主任：（排名不分先后）

林小博 北京网络空间安全协会 秘书长

朱方园 上海市信息安全行业协会 副秘书长

于永丰 辽宁省信息网络安全协会 秘书长

闫东 辽宁省网络安全保障工作联盟 秘书长

孙甲子 黑龙江省网络安全协会 会长

吴文涛 安徽省网络安全协会 秘书长

刘长久 湖北省网络和数据安全协会 副秘书长

邓庭波 湖南省网络空间安全协会 秘书长

林勇忠 广东省网络空间安全协会 党支部书记

冯伟 广西网络安全协会 秘书长

李春报 海南省网络安全和信息化信协会 常务副理事长

戴勇 贵州省网络安全和信息化协会 副理事长

淡战平 陕西省信息网络安全协会 会长

卢建宙 甘肃省商用密码行业协会 会长

郑方 甘肃烽侦网络安全研究院 院长

李学锋 新疆维吾尔自治区互联网协会 秘书长

胡俊涛 郑州市网络安全协会 秘书长
乔 奇 武汉市网络安全协会 副秘书长
樊建功 南昌市网络信息安全协会 会长
王胜军 南宁市信息网络安全协会 会长
邓开旭 成都信息网络安全协会 副秘书长
陈建设 贵阳市信息网络协会 秘书长
杨建东 昆明市网络安全协会 秘书长
沈 泓 宁波市计算机信息网络安全协会 秘书长
卜庆亚 徐州市网络安全协会 理事长
孙 逊 佛山市信息协会 秘书长
谢照光 惠州市计算机信息网络安全协 常务副理事长
程 谦 河源市网络空间安全协会 秘书长
孔德剑 曲靖市网络安全协会 会长
李 丹 榆林市网络安全协会 秘书长

编委会委员：（排名不分先后）

黄汝锡 广东关键信息基础设施保护中心 党支部专职副书记
方满意 广东网络空间安全协会副会长
王 嫣 上海市信息网络安全管理协会 部长
贺 锋 广东中证声像资料司法鉴定所 主任
成珍苑 网安联认证中心 副主任
黎明瑶 广东新兴国家网络安全和信息化发展研究院 研究员
陈菊珍 广东计安信息网络培训中心
黄丽佳 揭阳网络空间安全协会 秘书长

编辑部主任：梁思雨

编辑部：何治乐 胡文华 李 坤 吴若恒 胡柯洋
李培刚 薛 波 孙翊伦 林 晴 徐瑞雪

发行部主任：周贵招

发行部：林永健 张 彦 高梓源

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：2月，针对当前缅甸妙瓦底地区涉中国电信网络诈骗犯罪严峻形势，公安部持续加强与缅甸、泰国执法部门间的合作，全力推动联合打击工作。中缅泰三国警方联手对妙瓦底地区电信网络诈骗犯罪开展集中打击，取得重大进展，大批缅甸妙瓦底地区的涉诈犯罪嫌疑人落网。

习近平主席特别代表、中共中央政治局委员、国务院副总理张国清近日在巴黎出席人工智能行动峰会并致辞。张国清表示，人工智能已成为新一轮科技革命和产业变革的重要驱动力量。中国以高度负责的态度参与人工智能全球治理。在法期间，法国总统马克龙会见张国清。张国清转达习近平主席亲切问候，表示中方愿同法方一道，落实好两国元首共识，推动中法关系在“新甲子”实现更大发展。马克龙感谢习近平主席派特别代表来法参会，表示法国坚持战略自主，愿同中方加强沟通合作，共促和平发展、共迎时代挑战。

国家互联网信息办公室在京举办欧盟在华企业数据跨境流动政策座谈会。相关负责同志介绍中国数据跨境流动政策法规及中欧数据跨境流动交流机制有关情况，回答欧盟在华企业关于数据跨境流动的有关问题。

关键词：数据跨境、电信诈骗、人工智能行动峰会

1. 张国清出席法国人工智能行动峰会并致辞

2月11日，习近平主席特别代表、中共中央政治局委员、国务院副总理张国清在巴黎出席人工智能行动峰会并致辞。

张国清表示，人工智能已成为新一轮科技革命和产业变革的重要驱动力。中国以高度负责的态度参与人工智能全球治理。2023年10月，习近平主席提出《全球人工智能治理倡议》，围绕“人工智能怎样发展与治理”的重大时代课题，提出了中国方案，贡献了中国智慧。面对人工智能发展的机遇和挑战，国际社会应携起手来，倡导智能向善，深化创新合作，强化包容普惠，完善全球治理。中国愿在人工智能领域与各国共推发展、共护安全、共享成果，共同构建人类命运共同体。欢迎各方来华出席上海2025世界人工智能大会。

在法期间，法国总统马克龙会见张国清。张国清转达习近平主席亲切问候，表示中方愿同法方一道，落实好两国元首共识，推动中法关系在“新甲子”实现更大发展。马克龙感谢习近平主席派特别代表来法参会，表示法国坚持战略自主，愿同中方加强沟通合作，共促和平发展、共迎时代挑战。（来源：国务院）

2. 首批 200 名缅甸妙瓦底地区的中国籍涉诈犯罪嫌疑人经泰国被押解回国

2月20日，缅甸向中国遣返的妙瓦底地区首批200名中国籍涉诈犯罪嫌疑人，经泰国被公安机关押解回国。

针对当前缅甸妙瓦底地区涉中国电信网络诈骗犯罪严峻形势，公安部持续加强与缅甸、泰国执法部门的执法合作，全力推动联合打击工作。今年1月底，在中国驻泰、驻缅使领馆的大力支持下，公安部派出工作组先后赴泰国、缅甸，与两国执法部门进行多轮次会谈磋商，就进一步加强中缅泰三方执法合作，探索建立联合打击犯罪机制，共同打击电信网络诈骗、人口贩运等跨国犯罪达成共识。

中缅泰三国警方加大工作力度，联手对妙瓦底地区电信网络诈骗犯罪开展集中打击。泰国对妙瓦底地区采取断电、断网、断油等措施，在泰缅边境加强巡查管控，坚决阻断涉诈人员偷渡、转移通道。缅甸部署对妙瓦底地区电诈园区开展集中清查，缉捕涉诈犯罪嫌疑人，解救被困中国公民。经三方密切协作、共同努力，打击工作取得重大进展，大批缅甸妙瓦底地区的涉诈犯罪嫌疑人落网。2月20日，缅方将向我遣返的首批200名中国籍涉诈犯罪嫌疑人移送至泰国湄索，公安部组织江苏公安机关民警执行包机押解任务，将相关人员全部押解回国。根据工作安排，预计还将有800余名中国籍涉诈犯罪嫌疑人被陆续押解回国。

此外，涉中国公民王某等人被骗至境外失联被困、遭非法拘禁案的 10 名重要犯罪嫌疑人被泰国警方抓获后，已于 2 月 15 日凌晨被公安机关成功押解回国。（来源：公安部）

3. 国家互联网信息办公室举办欧盟在华企业数据跨境流动政策座谈会

2 月 25 日，国家互联网信息办公室在京举办欧盟在华企业数据跨境流动政策座谈会。国家互联网信息办公室相关局负责同志介绍中国数据跨境流动政策法规及中欧数据跨境流动交流机制有关情况，回答欧盟在华企业关于数据跨境流动的有关问题，商务部、工业和信息化部、自然资源部、国家卫生健康委员会、国家金融监督管理总局、北京网信办、上海网信办等部门相关负责同志介绍有关政策并参与交流。参会欧盟在华企业感谢国家互联网信息办公室举办本次座谈会，积极评价中方关于促进和规范数据跨境流动的政策举措，表示愿为中欧经贸合作作出更多贡献。23 家欧盟在华企业和中国欧盟商会相关负责人参加座谈。（来源：网信中国）

境内前沿观察二：政策立法

导读：2月，打击跨境犯罪、个人信息保护、公共安全视频图像、应急预案、数据资源统计管理仍是国家部委和地方政策立法的重点关注内容。

打击跨境犯罪方面。中泰发布联合声明提出，双方强调在双边、澜湄合作等地区合作机制下，以零容忍的坚决态度，加强打击人口贩运、电信网络诈骗、毒品走私、非法网络赌博、洗钱等跨境犯罪，开展湄公河联合巡逻执法行动。

个人信息保护方面。国家互联网信息办公室发布《个人信息保护合规审计管理办法》。《办法》明确，处理100万人以上个人信息的个人信息处理者应当指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作。《办法》强调，专业机构不得转委托其他机构开展个人信息保护合规审计。

公共安全视频图像方面。国务院公布《公共安全视频图像信息系统管理条例》，自2025年4月1日起施行。《条例》规定，人员聚集场所、交通枢纽等公共场所涉及公共安全区域的公共安全视频系统，由对相应场所负有经营管理责任的单位按照相关标准建设，安装图像采集设备的重点部位由县级以上地方人民政府各有关部门按照职责分工指导确定。

应急预案方面。中共中央、国务院印发《国家突发事件总体应急预案》，指导全国突发事件应对工作。《预案》规定，突发事件是指突然发生，造成或者可能造成严重社会危害，需要采取应急处置措施予以应对的自然灾

害、事故灾难、公共卫生事件和社会安全事件。在国家层面指挥体制层面，《预案》明确，中央网信办负责协调处理网络安全、网络数据安全与信息安全类突发事件。

数据资源统计管理方面。为贯彻落实《数字中国建设整体布局规划》工作部署，进一步摸清全国数据资源底数，国家数据局综合司、公安部办公厅印发《全国数据资源统计调查制度》，主要调查数据资源指标，包括数据生产、存储、计算、流通、应用和安全等内容。

地方层面，上海市五部门联合发布《中国（上海）自由贸易试验区及临港新片区数据出境负面清单管理办法（试行）》《中国（上海）自由贸易试验区及临港新片区数据出境管理清单（负面清单）（2024版）》。办法提出，在上海自由贸易试验区及临港新片区注册的数据处理者，属于已公布负面清单的行业、领域，向境外提供负面清单外的数据可以免于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。

标准制定方面。自然资源部发布强制性国家标准《导航电子地图安全处理技术基本要求》的征求意见稿，明确要求导航电子地图传输过程，应使用符合相关规定和文件要求的商用密码进行技术处理。商用密码标准研究院发布公告，将面向全球陆续开展新一代公钥密码算法、密码杂凑算法、分组密码算法征集活动

关键词：打击跨境犯罪、个人信息保护、公共安全视频图像、应急预案、数据资源

（一）国家层面动向

1. 中泰发布联合声明，强调打击跨境犯罪

2月8日，中泰发布《中华人民共和国政府和泰国政府关于面向未来、以人民为中心，加强全面战略合作伙伴关系，推进更为稳定、更加繁荣、更可持续的中泰命运共同体建设的联合声明》。

《声明》提出，双方强调在双边、澜湄合作等地区合作机制下，以零容忍的坚决态度，加强打击人口贩运、电信网络诈骗、毒品走私、非法网络赌博、洗钱等跨境犯罪，开展湄公河联合巡逻执法行动。双方将进一步讨论尽早确立适当协调合作机制，有效打击网赌电诈。双方同意积极参与“平安澜湄行动”，共同推进澜湄司法合作，维护地区人民群众生命财产安全。（来源：外交部）

2. 国务院公布《公共安全视频图像信息系统管理条例》

1月13日，国务院总理李强签署国务院令 第799号，公布《公共安全视频图像信息系统管理条例》，自2025年4月1日起施行。

《条例》指出，公共安全视频图像信息系统是指通过在公共场所安装图像采集设备及相关设施，对涉及公共安全的区域进行视频图像信息收集、传输、显示、存储的系统。

《条例》规定，城乡主要路段、行政区域道路边界、桥梁、隧道、地下通道、广场、治安保卫重点单位周边区域等公共场所的公共安全视频系

统，由县级以上地方人民政府按照建设规划组织有关部门建设，纳入公共基础设施管理，建设、维护经费列入本级政府预算。下列公共场所涉及公共安全区域的公共安全视频系统，由对相应场所负有经营管理责任的单位按照相关标准建设，安装图像采集设备的重点部位由县级以上地方人民政府各有关部门按照职责分工指导确定：（1）商贸中心、会展中心、旅游景区、文化体育娱乐场所、教育机构、医疗机构、政务服务大厅、公园、公共停车场等人员聚集场所；（2）出境入境口岸（通道）、机场、港口客运站、通航建筑物、铁路客运站、汽车客运站、城市轨道交通站等交通枢纽；（3）客运列车、营运营载客汽车、城市轨道交通车辆、客运船舶等大中型公共交通工具；（4）高速公路、普通国省干线的服务区。在上述规定的场所、区域内安装图像采集设备及相关设施，应当为维护公共安全所必需，除前两款规定的政府有关部门、负有经营管理责任的单位外，其他任何单位或者个人不得安装。

《条例》强调，禁止在公共场所的下列区域、部位安装图像采集设备及相关设施：（1）旅馆、饭店、宾馆、招待所、民宿等经营接待食宿场所的客房或者包间内部；（2）学生宿舍的房间内部，或者单位为内部人员提供住宿、休息服务的房间内部；（3）公共的浴室、卫生间、更衣室、哺乳室、试衣间的内部；（4）安装图像采集设备后能够拍摄、窥视、窃听他人隐私的其他区域、部位。对上述区域、部位负有经营管理责任的单位或者个人，应当加强日常管理和检查，发现在前款所列区域、部位安装图像采集设备及相关设施的，应当立即报告所在地公安机关处理。

相较于征求意见稿，《条例》适度减轻一般经营场所部署公共安全视频图像信息系统责任，适度放宽利害关系人查看公共安全视频图像信息系统的限制条件，理清了《条例》与《个人信息保护法》等的规范边界。（来源：国务院）

（二）部委层面动向

1. 中共中央、国务院印发《国家突发事件总体应急预案》

2月25日，中共中央、国务院印发《国家突发事件总体应急预案》，由总则、组织指挥体系、运行机制、应急保障、预案管理等部分组成，适用于党中央、国务院应对特别重大突发事件工作，指导全国突发事件应对工作。

《预案》明确，突发事件是指突然发生，造成或者可能造成严重社会危害，需要采取应急处置措施予以应对的自然灾害、事故灾难、公共卫生事件和社会安全事件。其中，事故灾难主要包括工矿商贸等生产经营单位的各类生产安全事故，交通运输、海上溢油、公共设施和设备、核事故，火灾和生态环境、网络安全、网络数据安全、信息安全事件等。

在国家层面指挥体制层面，《预案》明确，中央网信办负责协调处理网络安全、网络数据安全与信息安全类突发事件。《预案》要求工业和信息化部、广电总局等有关部门建立健全应急通信网络、应急广播体系，提升公众通信网络防灾抗毁能力和应急服务能力，推进应急指挥通信体系建设，强化极端条件下现场应急通信保障。（来源：国务院）

2. 国家互联网信息办公室发布《个人信息保护合规审计管理办法》

2月12日，国家互联网信息办公室发布《个人信息保护合规审计管理办法》，并附《个人信息保护合规审计指引》，自2025年5月1日起施行。

《办法》指出，处理100万人以上个人信息的个人信息处理者应当指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作。提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督。

《办法》规定，处理超过1000万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。国家网信部门和其他履行个人信息保护职责的部门在个人信息处理者存在发现个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险，或个人信息处理活动可能侵害众多个人的权益，或发生个人信息安全事件并导致100万人以上个人信息或者10万人以上敏感个人信息泄露、篡改、丢失、毁损时，要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计。

《办法》强调，专业机构不得转委托其他机构开展个人信息保护合规审计。同一专业机构及其关联机构、同一合规审计负责人不得连续三次以上对同一审计对象开展个人信息保护合规审计。（来源：网信中国）

3. 国家数据局综合司、公安部办公厅印发《全国数据资源统计调查制度》

2月18日，国家数据局综合司、公安部办公厅印发《全国数据资源统计调查制度》，自2025年1月开始实施，有效期3年。

《调查制度》所称数据是指任何以电子或其他方式对信息的记录。数据资源是指具有价值创造潜力的数据的总称，通常指以电子化形式记录和保存、可机器读取、可供社会化再利用的数据集合。统计范围为全国（不包括港澳台地区）。主要调查数据资源指标，包括数据生产、存储、计算、流通、应用和安全等内容。本年度全数据资源统计调查工作开展时间为2025年2月18日至3月14日，调查标准时点为2024年12月31日。调查对象包括合法拥有或控制数据的国家行政机关、事业单位、企业、社会团体等。

（来源：国家数据局）

4. 全国数据标准化技术委员会秘书处发布《关于发布2025年第一批数据领域国家标准需求的通知》

2月10日，全国数据标准化技术委员会秘书处发布《关于发布2025年第一批数据领域国家标准需求的通知》（全国数标委秘〔2025〕1号），共涉及四十七项数据领域国家标准需求，包括数据服务能力评估标准、面向分析和机器学习的数据质量标准、数据匿名化标准等。

2024年10月29日，全国数据标准化技术委员会成立大会暨第一次全体委员会议在京召开。全国数据标准化技术委员会编号TC609，由国家数据局筹建及进行业务指导。委员会负责专业范围为主要负责数据资源、数据

技术、数据流通、智慧城市、数字化转型等基础通用标准，支撑数据流通利用的数据基础设施标准，以及保障数据流通利用的安全标准等。（来源：全国数标委、人民网）

5. 自然资源部发布《导航电子地图安全处理技术基本要求（征求意见稿）》

2月5日，自然资源部发布强制性国家标准《导航电子地图安全处理技术基本要求》的征求意见稿，适用于公开出版、销售、传播、展示和使用的导航电子地图。征求意见稿规定了公开出版、销售、传播、展示和使用的导航电子地图在数据采集、制作和表示过程中，空间位置技术处理、传输安全技术处理、服务安全技术处理的要求，以及不应采集和表示的内容。

征求意见稿指出，导航电子地图是指，含有空间位置地理坐标，能够与空间定位系统结合，引导人或交通运输工具等从出发地到达目的地的电子地图或数据集。明确要求导航电子地图传输过程，应使用符合相关规定和文件要求的商用密码进行技术处理。（来源：自然资源部）

6. 商用密码标准研究院开展新一代商用密码算法征集活动

2月5日，为应对量子计算威胁，推动新一代商用密码算法标准制定，按照密码行业标准化技术委员会工作安排，商用密码标准研究院发布《关于开展新一代商用密码算法征集活动的公告》，将面向全球陆续开展新一代公钥密码算法、密码杂凑算法、分组密码算法征集活动，从安全性、性

能、特点等方面组织评估，遴选出优胜算法开展标准化工作。（来源：商用密码标准研究院）

（三）地方层面动向

1. 上海市网信办等五部门印发自由贸易试验区数据出境负面清单管理办法、负面清单（2024版）

2月8日，上海市互联网信息办公室、上海市数据局、上海市发展和改革委员会、中国（上海）自由贸易试验区管委会、中国（上海）自由贸易试验区临港新片区管委会联合印发《中国（上海）自由贸易试验区及临港新片区数据出境负面清单管理办法（试行）》《中国（上海）自由贸易试验区及临港新片区数据出境管理清单（负面清单）（2024版）》，自发布之日起实施。

《办法》共六章二十一条，包括工作机制与职责、负面清单实施与管理、数据出境促进措施、监督管理等内容。办法提出，在上海自由贸易试验区及临港新片区注册的数据处理者，属于已公布负面清单的行业、领域，向境外提供负面清单外的数据可以免于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。

《办法》强调，使用负面清单开展数据出境活动的数据处理者，应按照规定所属区域及时向上海自贸试验区管委会、临港新片区管委会报告数据出境情况，包括但不限于数据出境业务场景、出境数据目录、出境数据规模、境外接收方等情况。数据处理者向境外传输重要数据和个人信息，应当遵

守法律、法规的规定，履行数据安全保护义务，采取技术措施和其他必要措施，保障数据出境安全。发生数据出境安全事件或者发现数据出境安全风险增大的，应当采取补救措施，并及时向上海市互联网信息办公室、上海市数据局、上海市公安局、上海市国家安全局、上海自贸试验区管委会、临港新片区管委会报告。

《负面清单（2024版）》提出，再保险领域、国际航运领域、商贸领域（零售与餐饮业、住宿业）中，需要通过数据出境安全评估的数据清单，以及需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单。（来源：网信上海）

2. 天津市工业和信息化局发布《天津市促进智能网联汽车发展条例（征求意见稿）》

2月14日，天津市工业和信息化局发布《天津市促进智能网联汽车发展条例（征求意见稿）》，共七章四十七条，包括产业发展、基础设施建设、创新应用、安全保障等内容。

征求意见稿指出，天津市网信部门应当统筹协调智能网联汽车网络安全事件监督管理工作。市工业和信息化、公安、交通运输等部门按照各自职责加强全市智能网联汽车的网络安全风险管理工作。智能网联汽车生产、车联网软件提供、通信运营等相关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、网络安全评估和管理机制，按照有关规定及时优化升级智能网联汽车系统软件，依法落实网络安全相关管理要求。

征求意见稿强调，智能网联汽车生产、车联网软件提供、通信运营等智能网联汽车相关企业，应当建立健全数据安全保护管理制度，依法履行数据安全保护义务，并遵守下列规定：（1）收集的数据应当与车辆行驶和交通安全有关；（2）评估数据安全风险，分类分级保护有关数据；（3）处理个人信息应当遵守个人信息保护法的有关规定；（4）处理重要数据应当按照规定开展风险评估，并向市网信部门和有关部门报送风险评估报告；（5）为车辆所有人、管理人等查阅车辆运行数据，使用人查阅本人使用期间与事故、故障相关的数据提供查询工具和路径；（6）国家和本市规定的其他要求。（来源：天津市工业和信息化局）

境内前沿观察三：治理实践

导读：2月，公安机关、网信部门、通信管理部门、检察机关、法院等持续发力，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。

公安机关治理方面，山西省公安发布“净网2024”专项行动打击网络违法犯罪10起典型案例，对多起利用信息网络进行犯罪的行为人给予处罚。湖北省松滋市公安侦破一起虚拟货币诈骗案，帮助被害人及时追回损失。江苏省徐州市公安破获一起有偿提供虚假流量服务的网络水军案件，已将多名涉案犯罪嫌疑人依法刑事拘留。

网信部门治理方面，中央网信办召开全国网络法治工作会议，回顾总结2024年网络法治建设成效经验，分析面临的形势任务，研究部署2025年网络法治工作。中央网信办发布“清朗·2025年春节网络环境整治”专项行动治理成效，从严查处一批违法违规典型案例，确保整治工作取得扎实成效，为营造春节良好网络氛围提供了有力保障。国家网信办针对广大人民群众反映强烈的App未公开收集使用规则、未按法律规定提供删除或更正个人信息功能等问题，依据《个人信息保护法》《网络数据安全管理条例》《App违法违规收集使用个人信息行为认定方法》等法律规范，依法依规查处82款违法违规App。上海市委网信办通报2024年网信部门开展涉MCN机构管理工作情况，并部署《上海MCN机构内容生态合规指引（试行）》实施要求。

通信管理部门治理方面，上海、安徽、广东等省通信管理局发布侵害用户权益 APP，要求违规 APP 进行整改，逾期不整改的将依法依规组织开展相关处置工作等。

其他部门治理方面，最高人民法院发布六起依法惩治利用网络敲诈勒索犯罪典型案例，最高检发布两起侵犯公民个人信息典型案例。杭州互联网法院发布一起涉生成式人工智能平台侵害信息网络传播权案，对帮助侵害信息网络传播权的认定进行说理。北京互联网法院发布全国首例 AI 文生图著作权侵权案，对认定利用 AI 文生图的著作权问题进行界定。江苏高院判定涉境外虚拟货币投资不受我国法律保护。

关键词：行政处罚、专项行动、个人信息保护、典型案例

（一）公安机关治理实践

1. 山西省公安发布“净网 2024”专项行动打击网络违法犯罪 10 起典型案例

2 月 10 日，山西省公安发布“净网 2024”专项行动打击网络违法犯罪 10 起典型案例。

案例一：马某某等人非法利用信息网络为赌博集团洗钱案

2024 年 3 月，运城公安机关工作发现，犯罪嫌疑人马某某、王某等 8 人成立网络科技有限公司，并注册电商平台店铺为境外网络赌博集团洗钱，涉案资金达 1.5 亿元。目前，运城公安机关已查封犯罪团伙注册的网络科技公司 10 家，依法对马某某等 8 人采取刑事强制措施。

案例二：史某编造“受父辈庇护，入职相关单位”网络谣言案

2024 年 5 月，太原公安机关工作发现，犯罪嫌疑人史某为寻求网络关注，多次发布辱骂中国人、侮辱中国等信息并编造“受父辈庇护，入职相关单位”虚假消息，造成严重不良社会影响。目前，太原公安机关已依法对史某采取刑事强制措施。

案例三：荆某某等人非法利用信息网络组织、介绍卖淫案

2024 年 6 月，朔州公安机关工作发现，有人利用网络社交软件发布招嫖信息，组织人员长期为他人介绍卖淫并从中获利。朔州公安机关立即成立专案组开展深入侦查，开展了 2 轮次收网工作，捣毁了一个利用信息网

络组织卖淫团伙，共抓获犯罪嫌疑人 53 人，其中依法采取刑事强制措施 28 人。

案例四：付某某等人组织“网络水军”刷量控评案

2024 年 6 月，太原公安机关工作发现，犯罪嫌疑人付某某通过网络有偿提供刷量控评服务非法谋利，扰乱网络秩序，太原公安机关通过层层深挖，最终摧毁作案窝点两处，打掉作案网站平台 4 个和非法网络店铺 100 余个，依法采取刑事强制措施 8 人，查明涉案金额 1000 余万元。

案例五：宋某某等人侵犯公民个人信息案

2024 年 7 月，晋城公安机关工作发现，犯罪嫌疑人宋某某等人非法从事公民个人信息买卖行为，随即开展立案侦查，成功破获一起本地教培行业人员购买公民个人信息案，依法采取刑事强制措施 4 人。

案例六：张某某非法侵入计算机信息系统案

2024 年 8 月，忻州公安机关工作发现，忻州市某系统平台存在文件上传漏洞，疑似被非法侵入，忻州公安机关对该线索立案侦查，成功侦破一起非法侵入信息系统案，依法对犯罪嫌疑人张某某采取刑事强制措施，并及时采取安全措施修复平台漏洞。

案例七：于某某等人破坏计算机信息系统案

2024 年 8 月，运城公安机关工作发现，运城某加油站擅自改动燃油加油机主板芯片，存在加油作弊嫌疑。运城公安机关对该线索立案侦查，成功抓获 3 名利用修改加油机税控芯片实施加油机作弊的犯罪嫌疑人。目前，运城公安机关已依法对于某某等 3 人采取刑事强制措施。

案例八：郑某某等人侵犯公民个人信息案

2024年9月，长治公安机关工作发现，犯罪嫌疑人郑某某存在非法获取公民个人信息行为，长治公安机关对该线索立案侦查，成功打掉一从事非法获取公民信息、非法买卖账号、非法提供资金结算的黑灰产业团伙。目前，长治公安机关依法对9名犯罪嫌疑人采取刑事措施。

案例九：高某某编造“网上寻娃”网络谣言案

2024年10月，大同公安机关工作发现，违法嫌疑人高某某为博取流量便于直播带货，利用AI技术生成虚假图像，编造“孩子走失”的虚假信息，扰乱公共秩序，造成不良社会影响，大同公安机关依法对高某某采取治安拘留处罚。

案例十：李某某等人侵犯公民个人信息案

2024年11月，运城公安机关工作发现，运城市部分财税代记账公司疑似非法获取公民个人信息，运城公安机关通过深入扩线侦查，成功抓获犯罪嫌疑人7人，查扣非法买卖的公民个人信息一批。省公安厅在该案基础上，统筹全省发起集群战役，一举破获侵犯公民个人信息刑事案件18起、行政案件40起，抓获违法犯罪嫌疑人99人。（来源：公安部网安局）

2. 湖北省松滋市公安局侦破一起虚拟货币诈骗案

2月19日消息，湖北省松滋市一男子近日购买虚拟货币被骗走31400元，松滋市公安局新江口水陆派出所凭借“两队一室”警务模式迅速行动，仅用一日便成功侦破此案，及时为受害群众追回损失。

2月12日15时，雷先生报案称，被老同学彭某某诈骗31400元。经详细了解，事情缘起于1月23日，雷先生受朋友委托，找老同学彭某某购买5000个USDT（泰达币）虚拟货币，并支付31400元。彭某某收款后，以购买USDT货币手续繁琐为由，拖延交货时间，随后失联。雷先生与朋友察觉异常，遂来派出所报案。经综合指挥室对案件相关信息深入研判，很快锁定彭某某的活动轨迹。随后，快反队依据指挥室提供的线索循线追踪。

2月13日，在武汉某小区内，快反队成功将嫌疑人彭某某抓获。彭某某到案后供述，其因偿还外债，遂将雷先生托购买USDT的31400元扣下以缓解债务压力。在办案民警的耐心劝导与教育下，彭某某认识到错误，已将所骗金额如数退回。（来源：平安松滋）

3. 江苏省徐州市公安破获一起有偿提供虚假流量服务的网络水军案

2月28日消息，江苏省徐州市公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，2023年2月份至今，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抖音人气（在线人数）、抖音涨粉、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：江苏网警）

（二）网信部门治理实践

1. 中央网信办发布“清朗·2025年春节网络环境整治”专项行动治理成效

2月13日，中央网信办发布“清朗·2025年春节网络环境整治”专项行动治理成效。“清朗·2025年春节网络环境整治”专项行动启动以来，网信部门针对挑起极端对立、炮制不实信息、宣扬低俗恶俗、鼓吹不良文化、违法活动引流、侵害消费者权益等6类问题，从严查处一批违法违规典型案例，确保整治工作取得扎实成效，为营造春节良好网络氛围提供了有力保障。截至目前，微博、抖音、快手、腾讯、小红书、百度、知乎、豆瓣、哔哩哔哩等重点平台累计清理违法违规信息103万余条，处置账号9.7万个。（来源：网信中国）

2. 中央网信办召开全国网络法治工作会议

2月21日，中央网信办在贵州贵阳召开全国网络法治工作会议，回顾总结2024年网络法治建设成效经验，分析面临的形势任务，研究部署2025年网络法治工作。

会议指出，2024年，全国网信系统深入学习贯彻习近平总书记关于网络法治的重要论述，勠力同心、担当作为，全面深化推进网络法治统筹、网络立法、网信法治政府建设、网络法治宣传、涉外网络法治建设、网络

法治研究等各方面工作，取得一系列新进展新成效，有力服务了网信事业高质量发展、保障了网络空间高水平安全。

会议强调，2025年是贯彻落实网信工作“十四五”规划和法治领域“一规划两纲要”的收官之年，网络法治工作要突出抓好主题主线、着力强化网络法治统筹协调，以“网信为民、法治担当”为主题主线，以人民群众满意为评判标准，以解决人民群众急难愁盼为努力方向，以践行全过程人民民主为目标宗旨，统筹开展关于加强新时代网络法治工作相关指导意见、网信系统“八五”普法规划等总结评估，起草发布中国网络法治发展年度报告；要突出重点新兴领域、着力完善网络法律规范体系，积极营造清朗网络空间，持续筑牢网络安全屏障，有力保障新质生产力发展，加强网信领域党内法规建设；要突出规范化程序化、着力提升网信法治政府建设水平，强化顶层设计和监督实施，加快完善行政裁量权基准制度，发挥“五大”审核职能；要突出法治内容供给、着力增强网络法治宣传实效，坚持内容为王、效果导向，加强指导协调、丰富手段方式，构建更加完善的网络法治宣传格局；要突出内外法治贯通、着力拓展涉外网络法治工作成效，做好国外跟踪研究和国内立法应对，积极参与网络空间国际规则制定和网络法治国际交流合作；要突出体系能力建设、着力夯实网络法治工作基础，科学设计谋划，强化督促落实，加强研究支撑。（来源：网信中国）

3. 中央网信办发布 2025 年“清朗”系列专项行动整治工作重点

2月21日，中央网信办发布2025年“清朗”系列专项行动整治工作重点。重点整治任务主要包括：

一是整治春节网络环境，集中打击挑起极端对立、炮制不实信息、宣扬低俗恶俗、鼓吹不良文化、违法活动引流等问题。

二是整治“自媒体”发布不实信息，包括发布干扰舆论、误导公众内容，不做信息标注、内容以假乱真问题，缺失资质、提供伪专业信息等问题，规范重点领域信息内容传播。

三是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、炒作争议性话题等问题，强化信息来源标注、虚构和演绎标签标注。

四是整治AI技术滥用乱象，突出AI技术管理和信息内容管理，强化生成合成内容标识，打击借AI技术生成发布虚假信息、实施网络水军行为等问题，规范AI类应用网络生态。

五是整治涉企网络“黑嘴”，处置集纳负面信息，造谣抹黑企业和企业家，从事虚假不实测评，诋毁产品质量等问题，进一步优化营商网络环境。

六是整治暑期未成年人网络环境，强化涉未成年人不良内容治理，净化儿童智能设备、未成年人模式、未成年人专区等重点环节信息内容，防范线上线下交织风险。

七是整治网络直播打赏乱象，打击利用高额返现吸引打赏、情感伪装诱导打赏、低俗内容刺激打赏、未成年人打赏等突出问题，加强直播打赏功能管理。

八是整治恶意挑动负面情绪，包括借热点事件等挑起群体极端对立情绪，通过夸大炒作不实信息和负面话题，宣扬恐慌焦虑情绪，借血腥暴力画面挑起网络戾气等问题，严肃查处违规营销号、网络水军和 MCN 机构。

（来源：网信中国）

4. 中央网信办发布 2024 年全国网信系统打击网络违法违规行为工作成果

2 月 25 日，中央网信办发布 2024 年全国网信系统打击网络违法违规行为工作成果。2024 年，全国网信系统依法对 11159 家网站平台予以约谈，对 4046 家网站平台实施警告或罚款处罚，责令 585 家网站暂停有关功能或信息更新，下架移动应用程序 200 款，处置小程序 40 款，会同电信主管部门取消违法网站许可或备案、关闭违法网站 10946 家，督促相关网站平台落实主体责任，依法依约关闭账号 107802 个。（来源：网信中国）

5. 国家网信办依法集中查处一批侵害个人信息权益的违法违规 App

2 月 19 日消息，国家网信办近日针对广大人民群众反映强烈的 App 未公开收集使用规则、未按法律规定提供删除或更正个人信息功能等问题依

据《个人信息保护法》《网络数据安全条例》《App违法违规收集使用个人信息行为认定方法》等法律法规，依法依规查处“开个密室馆”等 82 款违法违规 App（含小程序）。

经查，“开个密室馆”等 4 款 App 存在未公开收集使用规则问题，违反《个人信息保护法》等法律法规，依法依规予以下架处置；“动态壁纸帝”等 78 款 App 存在未按法律规定提供删除或更正个人信息功能问题，违反《个人信息保护法》等法律法规，依法依规责令限期 1 个月完成整改，逾期未完成整改的，依法依规予以下架处置。（来源：网信中国）

6. 上海市委网信办召开属地 MCN 机构分类指导会，试行内容生态合规指引

2 月 18 日，上海市委网信办召开属地 MCN 机构分类指导会。美腕、百秋、宝尊、萤火虫文化、仙梓文化、艺寻传媒、美聚传媒、丽人丽妆等 16 家属地 MCN 机构以及浦东、静安、长宁等区委网信办参会。

上海市委网信办通报 2024 年网信部门开展涉 MCN 机构管理工作情况，并部署《上海 MCN 机构内容生态合规指引（试行）》实施要求。市委网信办依据相关法律法规和规范性文件，结合前期行业调研，综合行业主管部门、重点 MCN 机构以及网络平台等意见建议于去年 11 月底制定《上海 MCN 机构内容生态合规指引（试行）》，并于 2025 年起在属地 MCN 机构实施，主要要求属地 MCN 机构在建立健全内容合规管理体系，加强账号、内容安

全、直播、未成年人网络保护四大重点环节管理以及积极履行社会责任等方面不断探索、勇于实践。（来源：网信上海）

7. 鄂尔多斯市委网信办对两家单位进行网络安全约谈

2月25日消息，鄂尔多斯市委网信办近日依据《网络安全法》《数据安全法》《党委（党组）网络安全工作责任制实施办法》等有关法律法规，就网络安全问题对两家单位进行约谈。

监测发现，某市直部门的信息系统存在弱口令高危漏洞，经查该单位网络安全工作责任落实不到位，涉事信息系统未经网络安全风险评估上线运行，网络安全管理制度和操作规程不规范，网络安全责任不明晰，导致系统带病运行，造成严重网络安全隐患。鄂尔多斯市委网信办依法对该单位相关责任人进行约谈，要求该单位严格落实网络安全工作责任制，立即开展网络安全风险隐患排查整改，全面梳理本单位网络资产，建立完善网络安全管理制度，明晰责任人，切实维护单位信息系统网络安全和数据安全。

检查发现，某市属国有企业网站存在个人信息泄露安全风险，经查该单位在网站公示人员名单时，将人员姓名、身份证号等个人敏感信息未进行匿名化处理，造成个人信息泄露安全风险。鄂尔多斯市委网信办依法对该单位相关责任人进行约谈，要求该单位严格落实《数据安全法》《个人信息保护法》要求，立即开展风险隐患排查整改，加强网络数据和个人信息保护。

被约谈单位表示，将按照约谈要求立即整改，认真履行网络安全监管责任，举一反三，严格落实网络安全主体责任，加强《网络安全法》《数据安全法》等法律法规和网络安全知识技能学习培训，加强网络安全和数据安全风险防范和处置力度，有效杜绝属地网络安全事件频发现象。（来源：网信鄂尔多斯）

8. 聚焦保护“个人信息删除权”，上海市网信办依法约谈一批 App 运营者

2月27日消息，上海市网信办近日依法约谈吉米猫英语、美职篮英雄、帕为患者、上海都市旅游卡、遇见市北、专家门诊、云尚心理、车轮-掌上车服务、饱饱有赏、3DM游戏等在沪 App 运营者。

针对此前《国家网信办依法集中查处一批侵害个人信息权益的违法违规 App》通报中指出的“无用户账号注销功能、未提供有效的用户账号注销功能、为用户账号注销设置不合理条件”等问题，上海市网信办提出整改指导意见，要求企业立即改正相关问题，切实保障好用户个人信息删除权，并举一反三开展自查自纠，全面制定、完善内部管理制度和操作规程，切实采取有效保护措施，确保用户个人信息全生命周期安全可靠。同时，上海市网信办要求企业加强《个人信息保护法》《网络数据安全管理条例》《App 违法违规收集使用个人信息行为认定方法》等法律法规的学习和培训，真正树立依法办网、诚信经营的理念。（来源：网信上海）

（三）通信管理部门治理实践

1. 上海、安徽等省通信管理局发布侵害用户权益 APP

（1）上海

2月8日，上海市通信管理局通报2025年第1批侵害用户权益APP。上海市通信管理局近日组织第三方检测机构对本市移动互联网应用程序进行抽查，共发现31款APP及小程序存在侵害用户权益行为。上述APP及小程序应按有关规定在2月14日前落实整改工作。整改落实不到位的，上海市通信管理局将依法依规组织开展处置工作。（来源：网信上海）

（2）安徽

2月8日，安徽省通信管理局通报2025年第1批侵害用户权益APP。安徽省通信管理局近日对安徽省内APP进行拨测检查，检测发现14款APP存在违法违规收集使用个人信息的问题，2025年1月6日对上述违规APP企业下达了责令改正通知书，要求限期完成整改工作。截至目前，尚有5款APP未完成问题整改，相关APP企业应在2025年2月14日前落实整改要求。逾期不整改的，安徽省通信管理局将依法依规组织开展相关处置工作。（来源：安徽省通信管理局）

（3）广东

2月14日，广东省通信管理局通报12款未按要求完成整改APP/小程序。广东省通信管理局近日开展APP隐私合规和数据安全专项整治行动，发出《违法违规APP处置通知》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。截至目前，尚有 11 款 APP、1 款小程序未完成整改。被通报的 APP 应在 2025 年 2 月 21 日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施。（来源：广东信息通信业）

（4）江苏

2 月 20 日，江苏省通信管理局通报 2025 年第 1 批侵害用户权益 APP。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。截至目前，尚有 20 款 APP 未完成整改。请上述 APP 开发运营者在 2 月 28 日前完成整改，整改落实不到位的，江苏省通信管理局将视情采取下架、关停、行政处罚等措施。（来源：江苏通信业）

（5）浙江

2 月 28 日，浙江省通信管理局通报 2025 年第 1 批 2 款侵害用户权益 APP。浙江省通信管理局近日组织第三方检测机构对群众关注的网上购物、实用工具、求职招聘等类型 APP 进行检查，书面要求违规 APP 开发运营者限期整改。截至目前，尚有 2 款 APP 未按要求完成整改。请上述 APP 开发运营者在 3 月 7 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）

（四）其他部门治理实践

1. 最高人民法院发布六起依法惩治利用网络敲诈勒索犯罪典型案例

2月11日，最高人民法院发布六起依法惩治利用网络敲诈勒索犯罪典型案例。

案例一：孙某媛敲诈勒索案——制造、散播网络谣言敲诈勒索

被告人孙某媛系某网络主播的“粉丝”，被害人侯某经营的培训机构与该主播有业务合作。2022年6月，孙某媛自认为侯某与主播关系暧昧，遂在网络直播间辱骂侯某，并通过自媒体平台找到侯某家人联系方式，借用他人电话向侯某家人宣称侯某婚内出轨。侯某要求孙某媛停止人身攻击，孙某媛索要人民币100万元，被侯某拒绝后，孙某媛给侯某的培训机构员工、学员家属打电话、发短信，散布侯某婚内出轨、偷税漏税、猥亵儿童等虚假信息。孙某媛还匿名拨打电话向相关政府部门、公安机关举报侯某的培训机构存在没有办学资质、偷税漏税等违法行为，并在多个知名网站论坛发布涉及前述虚假内容的帖子。侯某不堪其扰轻生自杀，幸被人发现获救，孙某媛又发布侯某“畏罪自杀”的帖子，并继续向侯某索要钱财。侯某向公安机关报案，孙某媛被抓获。

法院审理认为，被告人孙某媛以非法占有为目的，采取威胁、要挟手段索要他人数额特别巨大的财物，其行为已构成敲诈勒索罪。孙某媛未能取得财物，系犯罪未遂，可以比照既遂犯从轻或者减轻处罚。孙某媛捏造

多条虚假负面信息，匿名向被害人亲属、同事、客户以及社会公众散布，多次威胁、要挟被害人给付巨额钱财，并在被害人有自杀举动后继续人身攻击、索要钱财，犯罪情节恶劣，依法予以从严惩处。据此，对孙某媛以敲诈勒索罪判处有期徒刑八年七个月，并处罚金人民币十万元。

案例二：赵某杰敲诈勒索案——利用网络敲诈勒索未成年人

2020年7月至8月期间，被告人赵某杰用QQ添加14至18周岁未成年女性40余人为好友。在聊天过程中，赵某杰故意找茬称对方把自己气病，以到被害人学校和家中持刀捅人相威胁，要求被害人“拿钱治病”，先后向4名被害人（13至16周岁）索要共计人民币18964元。案发后，赵某杰向被害人退赔违法所得并取得了谅解。

法院审理认为，被告人赵某杰以非法占有为目的，采取以暴力相威胁的手段索要他人数额较大的财物，其行为已构成敲诈勒索罪。赵某杰对多名未成年人实施敲诈勒索，依法应当从重处罚；其到案后如实供述罪行，自愿认罪认罚，积极退赔并取得被害人谅解，依法可以从轻处罚。据此，对赵某杰以敲诈勒索罪判处拘役六个月，并处罚金人民币二万元。

案例三：相某漫敲诈勒索案——编造事由向网络平台商家恶意索赔敲诈勒索

2021年1月至2023年4月期间，被告人相某漫在多个线上外卖平台购买食品并投放异物，随后拍照反馈给平台和商家，以不赔偿就投诉相威胁先后向4家餐饮店铺索要共计人民币3169元。

法院审理认为，被告人相某漫以非法占有为目的，以投诉相威胁勒索多家被害单位钱款，数额较大，其行为已构成敲诈勒索罪。相某漫到案后如实供述罪行，依法可以从轻处罚；其自愿认罪认罚，依法可以从宽处理。据此，对相某漫以敲诈勒索罪判处有期徒刑七个月，并处罚金人民币四千元，并责令其退赔违法所得。

案例四：罗某甲等人敲诈勒索案——制造、散播负面信息并以有偿删帖方式敲诈勒索

被告人罗某甲、徐某、聂某某、杨某均系新闻媒体从业人员。2019年11月至2022年2月期间，罗某甲注册成立公司，并与徐某、聂某某、杨某以及被告人罗某乙、罗某丙等人共谋通过自媒体发布企业负面消息进而勒索财物。受罗某甲安排，罗某乙注册微信公众号“××经”并在多家知名网络平台注册第三方账号。罗某甲、杨某负责收集企业负面信息并撰写帖文，徐某负责审核，聂某某、罗某乙、罗某丙负责在微信公众号和第三方媒体账号发布、删除帖文。罗某甲还负责与被害单位谈判，罗某乙负责收款。2022年3月至7月期间，罗某甲等人利用“××经”微信公众号及相关网络平台账号发布6家互联网企业的负面帖文，迫使上述企业联系罗某甲等人，罗某甲等人以不支付“商务合作”费用就不删帖相要挟，索要被害单位钱款人民币29.6万元。

法院审理认为，被告人罗某甲、罗某乙、徐某、罗某丙、聂某某、杨某以非法占有为目的，在网上发布企业负面信息，以有偿删帖的方式多次勒索他人财物，数额巨大，其行为均已构成敲诈勒索罪。在共同犯罪中，

罗某甲是主犯，罗某乙、徐某、罗某丙、聂某某、杨某是从犯。罗某甲、徐某、罗某丙、聂某某、杨某有自首情节，罗某乙有坦白情节，依法可以从轻处罚。各被告人均认罪认罚，依法可以从宽处理。据此，对罗某甲以敲诈勒索罪判处有期徒刑三年十个月，并处罚金人民币五万元；对罗某乙等五人分别判处有期徒刑并适用缓刑，并处罚金；对违法所得予以追缴。

案例五：李某等人敲诈勒索案——以“裸聊”为诱饵敲诈勒索

2020年7月至9月，被告人李某与胡某（另案处理）共谋以“裸聊”方式敲诈勒索，分别提供场地、设备、技术、支付结算账户，并通过层层联系招募“客服”“枪手”，纠集了被告人王某佳、谷某、钟某龙及谢某雄、谢某军、谢某勇（均另案处理）等人先后偷渡到缅甸。同年9月中旬至11月底，在李某指使下，“客服”谢某雄、谢某军、谢某勇等人使用王某佳收购的网络社交账号，冒充女性引诱被害人进行“裸聊”，并趁机录制不雅视频，向被害人手机植入病毒，读取手机内的通讯录信息，之后将不雅视频、手机通讯录交由“枪手”李某、梁某祥、梁某浩（另案处理）等人，再由李某等人以散布不雅视频相要挟索要钱款，先后从30余名被害人处索要人民币70余万元。所得钱款由李某进行分赃。

法院审理认为，被告人李某、王某佳、谷某、钟某龙结伙以散布“裸聊”视频相要挟，向多名被害人勒索财物，数额特别巨大，其行为均已构成敲诈勒索罪。在共同犯罪中，李某负责策划、组织、指挥，提供场地、设备、技术，分配犯罪所得钱款等，起主要作用，系主犯，依法应当按照其组织、指挥及参与的全部犯罪处罚；王某佳、谷某、钟某龙起次要作用，

系从犯，依法应当从轻或者减轻处罚。根据本案的犯罪事实、性质、情节、对社会的危害程度以及各被告人在共同犯罪中的地位、作用，对李某以敲诈勒索罪判处有期徒刑十二年，并处罚金人民币十万元，与尚未执行完毕的前罪掩饰、隐瞒犯罪所得罪判处的刑罚并罚，决定执行有期徒刑十二年六个月，并处罚金人民币十万五千元；对王某佳、谷某、钟某龙以敲诈勒索罪判处九年至六年不等的有期徒刑，并处罚金；共同退赔被害人财产损失。

案例六：贺某武敲诈勒索案——为网络敲诈勒索犯罪分子提供技术支持

2022年5月，被告人贺某武与通过聊天软件结识的龙某鹏（在逃）共谋后，向网络资源商蔡某智（另案处理）购买IP地址非法搭建跨境网络专线，出售给缅甸某专门从事“裸聊”敲诈勒索犯罪的窝点，并雇佣技术人员对跨境网络专线进行维护。为规避打击，龙某鹏用泰达币及现金泰铢与上述犯罪窝点结算、与贺某武分成。至2023年2月，贺某武、龙某鹏获利共计人民币857万余元。2023年2月，某学院学生吴某明（被害人）被“裸聊”敲诈勒索人民币34.4万元。同年7月贺某武被抓获，之后贺某武主动上交违法所得，并返还了被害人吴某明的部分损失，获得吴某明的谅解。

法院审理认为，被告人贺某武明知他人利用信息网络实施敲诈勒索犯罪，仍为他人提供技术支持，致使被害人吴某明被敲诈勒索数额巨大的财物，其行为已构成敲诈勒索罪。贺某武有坦白情节，认罪认罚，退缴违法所得，退赔被害人部分损失并取得谅解，依法可以从宽处罚。据此，对贺

某武以敲诈勒索罪判处有期徒刑四年五个月，并处罚金人民币五万元。（来源：最高人民法院）

2. 最高检发布两起侵犯公民个人信息典型案例

2月18日，最高检近日发布两起侵犯公民个人信息典型案例。

案例一：史某某等人侵犯公民个人信息案

天津W科技有限公司史某某等人研发投放助贷APP和H5网页，吸引有贷款意向的用户填写个人信息，并将上述信息提供给线下信贷机构和贷款中介，为双方提供信息服务，并收取费用。2023年3月11日，H省Y县公安局对史某某等人以涉嫌侵犯公民个人信息罪立案侦查。同年3月17日，Y县公安局抓获史某某等19人，冻结公司相关账户资金1572万余元，并扣押史某某、任某某存单、手机等财物。同年3月18日，史某某等12人被Y县公安局以涉嫌侵犯公民个人信息罪刑事拘留。3月22日，任某某等7人被Y县公安局取保候审。

2023年4月17日，公安机关对被羁押的史某某等12人提请批准逮捕，Y县检察院审查认为史某某等12人构成侵犯公民个人信息罪证据不足，对史某某等人不予逮捕不致发生社会危险性，遂作出不批准逮捕决定。2023年9月20日，公安机关将史某某等19人以侵犯公民个人信息罪移送起诉。

2024年6月14日最高检将此案列为重点交办案件，四级检察机关同步展开工作。2024年9月2日至6日，最高检派出工作组赴H省阅卷审查、现场督导本案。Y县检察院经审查认为，本案犯罪嫌疑人的行为不构成侵犯

公民个人信息罪。经检察机关依法监督，公安机关于2024年9月26日撤销案件，全部解除查扣冻并全额返还涉案财物。（来源：最高人民检察院）

案例二：林某某等侵犯公民个人信息案

吴某某通过电脑程序非法获取大量QQ号码，并在QQ群组中发布广告予以出售。林某某通过上述广告联系到吴某某，2022年6月至2023年3月间，吴某某向林某某出售QQ账号共计6万条，实名认证率为91%，非法获利折合人民币500万余元。2022年8月至2023年3月，林某某将购买的QQ号码转化为包含姓名、电话、地址等信息，在TG网络社交平台上发布以招揽买家，其中属于公民个人信息的5000余条。通过林某某发布的广告，邵某某向林某某购买包含手机号码、性别的公民个人信息8万余条，出售给他人，非法获利7500元；王某某向林某某购买包含手机号码、QQ号码的公民个人信息28万余条，出售给他人，非法获利3万元；李某某向林某某购买具有贷款需求的公民个人信息5万余条。

2023年10月27日、2024年1月22日，山西省长治市屯留区人民检察院先后以林某某、吴某某、邵某某、王某某、李某某犯侵犯公民个人信息罪提起公诉。2024年1月15日、3月8日，长治市屯留区人民法院先后以侵犯公民个人信息罪，判处林某某有期徒刑三年六个月，并处罚金505万元；判处吴某某、邵某某、王某某、李某某有期徒刑三年，缓刑三年，并处罚金1.5万元至505万元不等。后林某某提出上诉，长治市中级人民法院裁定驳回上诉，维持原判。

另查明,2021年开始,梁某某雇佣牟某某在TG网络社交平台上建立“黄站长”聊天群组,该群组为买卖公民个人信息等非法交易进行推广并提供担保,非法交易金额折合人民币2500万余元,已全部追缴。2024年3月27日,长治市屯留区人民检察院以梁某某犯非法利用信息网络罪提起公诉。6月20日,屯留区人民法院以非法利用信息网络罪,判处梁某某有期徒刑十个月,并处罚金30万元。3月28日,因牟某某犯罪情节轻微、犯罪时系未成年人、从犯,长治市屯留区人民检察院对牟某某相对不起诉。(来源:最高人民检察院)

3. 杭州互联网法院发布一起涉生成式人工智能平台侵害信息网络传播权案

2月10日,杭州互联网法院发布一起涉生成式人工智能平台侵害信息网络传播权案。原告系奥特曼系列形象的知识产权权利人。被告运营某AI平台,该平台提供Checkpoint基础模型和LoRA模型,支持图生图、模型在线训练等诸多功能。在该平台首页及“推荐”“IP作品”项下存在有关奥特曼的智能生成图片以及LoRA模型,可应用、下载、发布或分享链接。奥特曼LoRA模型系由用户上传奥特曼图片,选择平台基础模型,调整参数进行训练后生成。其后,其他用户可通过输入提示词,选择基础模型、叠加奥特曼LoRA模型进行训练后生成与奥特曼形象实质性相似的图片等。

杭州互联网法院就该案作出一审判决，认定被告杭州某智能科技有限公司构成侵害信息网络传播权的帮助侵权，判决被告立即停止侵权并赔偿经济损失及合理费用3万元。日前，该案已生效。（来源：杭州互联网法院）

4. 江苏高院发布涉外商事审判典型案例，涉境外虚拟货币投资

2月11日，江苏高院发布涉外商事审判典型案例，其中涉及一起境外虚拟货币投资案件，指出其不受我国法律保护。

相关案例中，新加坡公民潘某某、中国公民田某某与案外人签订了合作协议约定共同经营“MFA区块链”项目，潘某某向田某某转帐1574万元用于购买MFA虚拟货币。然而，随着时间推移，由于一直未见到资金回笼，潘某某心里开始打鼓，催促田某某归还款项。起初田某某以市值紧张为由推诿，在潘某某的多次催促下，田某某陆续向其返款1060万元人民币。2020年9月，MEXC（新加坡交易平台）下线MFA/USDT现货交易，案涉虚拟账户被锁定而无法交易，本金全部损失。潘某某向法院提起诉讼，请求法院依法判决田某某向其返还剩余款项并按银行间贷款市场报价利率支付利息。

盐城市中级人民法院审理后认为，田某某与潘某某签订合作协议的目的是投资案涉“MFA区块链”项目，双方均明知该项目实际是炒作虚拟货币，该合同应认定为无效，相应损失由当事人自行承担，遂判决驳回潘某某的诉讼请求。潘某某不服该判决，提起上诉。江苏高院二审认为，潘某某是新加坡公民，本案具有涉外因素，根据我国法律适用法，涉及我国金融安全以及社会公共利益的，应当直接适用我国法律法规的强制性规定。我国

法律法规规定禁止虚拟货币投资，因此投资境外虚拟货币及相关衍生品违反我国法律法规强制性规定，违背公序良俗，合作协议应认定为无效，由此引发的损失由当事人自行承担。遂判决驳回上诉，维持原判。（来源：江苏高院）

5. 杭州互联网法院发布一起操纵网络水军案

2月27日，杭州互联网法院发布一起全国首例操纵“网络水军”案。2019年9月至2022年5月间，被告杨某鹏利用其注册的公司研发的平台，招募数量庞大的兼职人员充当“网络水军”，并通过组织、操纵“网络水军”“养号”等方式，开展有偿“转评赞”“直发”“投诉举报”等业务，即在未核实信息真实性的情况下，实施包括对客户指定的影视作品、网络视频、游戏作品、商品的宣发等正面点赞、转发、评论，按客户要求的相关网络平台发布关于特定作品、商品的具体内容等提升热度的业务，以及通过在信息发布平台进行投诉举报等方式删帖以降低针对特定作品、商品负面信息热度的业务。经调查，共“养号”1294个，完成“转评赞”“直发”任务24万余条，任务金额合计896万余元；完成“投诉举报”任务1200余条，任务金额合计19万余元。

杭州互联网法院作出判决：杨某鹏等于本判决生效之日起十日内支付公益损害赔偿金100万元，删除已发布的虚假信息并注销相关网络账号1294个，在国家级媒体上向社会公众刊发赔礼道歉声明。宣判后，双方均未上

诉。另，杨某鹏等以营利为目的，有偿提供删帖服务的行为已被生效刑事判决认定构成犯罪。（来源：杭州互联网法院）

6. 北京互联网法院发布全国首例人工智能文生图著作权侵权案

2月28日，北京互联网法院发布全国首例AI文生图著作权侵权案。原告使用人工智能模型，通过输入提示词的方式生成了涉案图片后发布在某网络平台。被告在另一网络平台上发布文章，文章配图使用了涉案图片。

法院经审理认为，涉案图片体现出与在先作品存在可以识别的差异性。涉案图片生成过程中，原告对于人物及其呈现方式等画面元素通过提示词进行设计，对于画面布局构图等通过参数进行设置，体现原告的选择和安排。在无相反证据的情况下，可以认定涉案图片由原告独立完成，体现出原告的个性化表达，因此涉案图片具备“独创性”要件。涉案图片是以线条、色彩构成的有审美意义的平面造型艺术作品，属于美术作品，受到著作权法的保护。就涉案作品的权利归属而言，涉案图片是基于原告的智力投入直接产生，体现出原告的个性化表达，因此原告是涉案图片的作者，享有涉案图片的著作权。被告侵害原告享有的权利，应当承担侵权责任。最终法院判决被告赔礼道歉并赔偿损失。（来源：北京互联网法院）

境外前沿观察：月度速览十则

导读：2月，境外各国在对外投资、人工智能、网络安全、数据安全等方面的政策法律、热点事件持续发生。

对外投资方面，美国白宫发布总统备忘录《美国优先投资政策》，明确美国政府在维护国家安全、保护技术创新和关键基础设施方面的战略意图，特别是针对“竞争对手国家”的投资。

人工智能方面，中国、法国、印度、欧盟在内的多个国家和国际组织签署《关于发展包容、可持续的人工智能造福人类与地球的声明》，美国和英国未签署。声明倡导加强全球人工智能协调治理，承诺推动“开放、包容、透明、合乎道德、安全、可靠”的人工智能发展，鼓励有利于未来劳动市场和可持续发展的人工智能部署，确保该技术更加普及和可及。中国人工智能 DeepSeek 在日本、澳大利亚等多国遭到调查与禁止。印度新德里的德里高等法院发布一份通知，回应一项公益诉讼，该诉讼要求限制使用中国人工智能聊天机器人 DeepSeek，这是 DeepSeek 遭遇的全球首场诉讼。日本内阁通过《人工智能相关技术的研发及应用促进法》草案。该法案是日本政府为应对 AI 技术快速发展而制定的综合性法律框架，旨在通过系统化的政策推动人工智能技术的研究、开发和应用。英国政府发布《英国政府人工智能手册》，规定要合法、道德和负责任地使用 AI，以及确保 AI 系统的安全性等。人工智能行动峰会在法国巴黎闭幕，美国地方法院美国法院裁决或阻碍人工智能发展，禁止未经许可使用受版权内容训练 AI。

网络安全方面，欧盟《网络团结法》生效。该法着眼于提升欧盟的网络安全应对能力，特别是通过加强跨国合作来应对网络威胁。欧盟委员会公布一项《欧盟网络安全危机管理蓝图》提案，旨在应对日益复杂的网络威胁和危机。俄罗斯政府修订 30 多项现行法律，增加监禁期限、扩大资产没收程序以及强制公开审判网络罪犯等内容，以实现俄罗斯网络安全框架的现代化。

数据安全方面，韩国个人信息保护委员会宣布，对苹果公司和韩国移动支付平台卡卡奥支付因非法获取和传输用户数据的行为进行处罚。其中，苹果公司被处以 24.5 亿韩元（约合 1240.9 万元人民币）的罚款，而卡卡奥支付则面临 59.68 亿韩元（约合 3022.8 万元人民币）的罚款。

关键词：优先投资政策、人工智能、网络安全、数据传输、DeepSeek

1. 美国白宫发布总统备忘录《美国优先投资政策》

2月21日，美国白宫发布总统备忘录《美国优先投资政策》，加强对外国尤其是来自中国的投资。备忘录主要包括：

一是原则与目标。美国致力于维护强劲、开放的投资环境，以使美国的经济和人民受益，同时提高保护美国的能力，使其免受可能伴随外国投资而来的新的、不断变化的威胁。然而，不计一切代价的投资并不总符合国家利益。包括中华人民共和国（PRC）在内的某些外国对手，系统性地操控及推进对美国公司和美国资产的投资，以获取尖端技术、知识产权以及在战略产业的影响力。

二是政策。美国的相关政策主要包括：（1）美国的政策是保持开放的投资环境，以帮助确保未来的人工智能和其他新兴技术在美国本土建成、创造及发展；（2）对于涉及关键技术、关键基础设施、个人数据和其他敏感领域的美国公司企业的投资，对外国投资者获取美国资产的限制将根据其与PRC和其他外国对手或威胁行为体的掠夺性投资和技术收购行为的可核实距离和独立性而相应地放宽；（3）本届政府还将加快对在美国的任何超过10亿美元投资的环境审查；（4）美国将减少公共和私营部门的资本、技术和技术知识被诸如PRC等外国对手利用；（5）为了进一步削弱美国个人投资于外国竞争对手的激励，特朗普政府正在审视是否暂停或废止1984年签署的《美国-中华人民共和国所得税协定》。这项税收协定，加上中国加入世界贸易组织以及美国对中国的商品和服务承诺无条件最惠国待遇，被认为是导致美国去工业化和中国军事技术现代化的因素。特朗普政府致

力于扭转这两种趋势，鼓励美国投资者将资金投向美国的未来，而非中国的未来等。（来源：美国白宫）

2. 多个国家和国际组织签署巴黎人工智能宣言，英美拒签

2月11日，人工智能行动峰会在法国巴黎闭幕，中国、法国、印度、欧盟在内的多个国家和国际组织签署《关于发展包容、可持续的人工智能造福人类与地球的声明》，美国和英国未签署。声明倡导加强全球人工智能协调治理，承诺推动“开放、包容、透明、合乎道德、安全、可靠”的人工智能发展，鼓励有利于未来劳动力市场和可持续发展的人工智能部署，确保该技术更加普及和可及。

声明指出，参会各国的行动基于科学、解决方案（聚焦符合各国框架的开放人工智能模型）和政策标准三大原则，与国际框架保持一致。声明认可现有的关于人工智能的多边倡议，包括联合国大会决议、全球数字契约、联合国教科文组织关于人工智能伦理的建议、非洲联盟大陆人工智能战略、经济合作与发展组织（OECD）、欧洲理事会和欧盟、七国集团（G7）包括广岛人工智能进程以及二十国集团（G20）的工作，并确认推动人工智能的可及性以减少数字鸿沟等六项优先事项。（来源：法国总统官网）

3. 日本内阁通过《人工智能相关技术的研发及应用促进法》草案

2月28日，日本内阁通过《人工智能相关技术的研发及应用促进法》草案。该法案是日本政府为应对AI技术快速发展而制定的综合性法律框架，

旨在通过系统化的政策推动人工智能技术的研究、开发和应用，确保日本在这一领域的国际竞争力。值得注意的是，为避免过度监管，法案未设惩罚性条款，而是鼓励企业自主提升人工智能运用中的安全性和透明度。但也提到如果人工智能技术的使用损害国民权利，将公布涉事企业名单，增强对侵犯人权行为的威慑。

法案主要内容包括：（1）法案清晰界定国家、地方政府、研究机构、企业及国民在人工智能技术研发与应用中的职责分工；（2）法案提出包括研发、人才培养、普及教育及国际合作等多项基本施策，并作为政府推动人工智能发展的行动蓝图，确保政策体系的系统性和连续性，全面助力人工智能技术健康发展。（来源：japan news）

4. 英国政府发布《英国政府人工智能手册》

2月10日，英国政府发布《英国政府人工智能手册》，为政府实体安全和负责任地使用AI提供指导方针。手册主要包括以下内容：

一是该手册规定十项原则，具体包括：（1）了解AI及其局限性。确保使用者对AI技术有基本的理解，知道其能力边界和潜在风险；（2）合法、道德和负责任地使用AI。确保AI的应用符合法律法规，并且在道德上是可接受的；（3）确保AI系统的安全性。采取措施保护AI系统不受网络攻击，并确保数据安全；（4）在关键阶段实施有意义的人类控制。确保在AI系统的决策过程中有适当的人类监督和干预等。

二是 AI 简介。该部分对 AI 及其主要领域进行了概述，包括神经网络、机器学习、深度学习、语音识别、计算机视觉、自然语言处理、生成式 AI 等。

三是构建 AI。这部分详细介绍了构建 AI 解决方案的步骤，包括团队组建、技能获取、与商业同事合作、确定目标、用户研究、识别用例、创建支持结构等。它为政府组织提供了实用的指导，帮助他们在项目初期就考虑到 AI 系统的全生命周期管理，确保 AI 项目的顺利实施和可持续发展等。（来源：英国政府官网）

5. 欧盟《网络团结法》生效

2月4日，欧盟《网络团结法》生效。该法着眼于提升欧盟的网络安全应对能力，特别是通过加强跨国合作来应对网络威胁。该法建立了一个名为“网络安全警报系统”的泛欧基础设施，涵盖了来自欧盟各成员国的国家和跨境网络中心，这些中心将协同工作，检测和应对网络安全威胁。利用先进的技术，包括人工智能（AI）和大数据分析，这些网络中心能够及时发现并共享网络威胁和事件警报，提升整体应对效率。

此外，该法还提出建立网络安全应急机制，增强欧盟对网络安全事件的准备和响应能力。这一机制包括：为关键行业（如医疗、交通、能源等）提供潜在漏洞测试的准备行动；建立由私营部门应急响应服务组成的“欧盟网络安全储备”，这些服务可在发生重大网络安全事件时迅速介入；以及推动成员国间的技术互助。（来源：欧盟委员会）

6. 欧盟委员会发布网络安全蓝图提案，强化危机协调

2月24日，欧盟委员会公布一项《欧盟网络安全危机管理蓝图》提案，旨在应对日益复杂的网络威胁和危机。蓝图不仅为欧盟成员国及相关机构构建了清晰简洁的管理框架，还着重强调了网络安全危机管理全周期中的合作与协调机制，涵盖信息共享、联合演练、资源调度及国际合作等关键环节。蓝图主要内容包括：

一是网络危机的定义与触发机制。根据《NIS2指令》的定义，大规模网络安全事件是指那些干扰程度超出成员国应对能力或对至少两个成员国造成重大影响的事件。

二是制定危机管理框架。蓝图提出一个全面的网络危机管理框架，涵盖预防、检测、响应和恢复四阶段，着重强调成员国与欧盟机构在信息共享、联合演练及资源调配等领域的紧密协作。蓝图的重点在于确保各行为体能够理解如何在整个危机管理生命周期中互动，并充分利用现有机制。

三是信息共享与态势感知。建议成员国和欧盟机构加强信息共享，建立共同的态势感知，特别是在关键基础设施（如能源、交通、金融等领域）的网络安全方面。通过共享高质量数据集和实时信息，成员国与欧盟机构能更有效地预测网络攻击，做好防范，并及时检测攻击等。（来源：欧盟委员会）

7. 俄罗斯政府提议新惩罚措施打击网络犯罪

2月19日消息，俄罗斯政府公布一项全面立法方案，旨在通过严厉惩罚措施打击网络犯罪。此次改革修订30多项现行法律，通过增加监禁期限、扩大资产没收程序以及强制公开审判知名网络罪犯，以实现俄罗斯网络安全框架的现代化。这一举措旨在应对近年来与国家相关的黑客活动激增，包括对德克萨斯州水利设施和波兰工业系统的攻击。新立法大幅加强了俄罗斯刑法的处罚力度，特别是针对未经授权的访问、恶意软件传播和对关键信息基础设施（CII）的损害。

入侵政府或企业系统的刑期从最高6年提升至5至15年，而网络欺诈的刑期也翻倍至12年。此外，法律授权法院没收与非法活动相关的加密货币和其他数字资产，解决了追踪区块链交易的执法漏洞。

针对有组织网络犯罪的关键条款包括：（1）资产冻结和就业禁令。金融机构必须在发现可疑交易后的24小时内冻结账户；被定罪的黑客将面临10年内禁止从事IT、金融或公共部门职务的禁令；（2）公开审判。重大网络犯罪案件将公开审判，以威慑潜在犯罪者；（3）增强引渡框架。俄罗斯承诺加强与国际刑警组织合作，引渡居住在海外的黑客等。（来源：cyber security news）

8. DeepSeek 遭到多国调查与禁止

2月3日，日本个人信息保护委员会事务局就 DeepSeek 公司提供的生成式 AI 服务发布使用 DeepSeek 等的注意事项。（来源：日本个人信息保护委员会）

2月3日消息，荷兰数据保护机构已对中国人工智能公司 DeepSeek 的数据收集行为展开调查。（来源：雅虎财经）

2月4日，澳大利亚联邦政府以国家安全为由发布强制性指令，禁止在所有政府网络和设备上使用 DeepSeek。（来源：澳大利亚政府内政事务部）

2月5日消息，印度财政部发布内部通知，要求雇员避免在执行公务时使用包括 DeepSeek、ChatGPT 在内的人工智能工具，理由是对政府文件和数据的保密性构成风险。（来源：reuters）

2月6日，美国两党议员提出《禁止在政府设备上使用 DeepSeek 法案》，该法案将禁止从政府设备使用和下载 DeepSeek 软件。（来源：Josh Gottheimer 众议员官网）

2月6日，波兰个人数据保护办公室建议谨慎使用 DeepSeek。波兰个人数据保护办公室还提醒，基于生成式人工智能的技术本质上依赖于对大量数据的处理，这些数据可能会被用于与用户最初意愿不符的目的，例如用于进一步训练模型或营销目的。（来源：波兰个人数据保护办公室）

2月10日，美国纽约州州长霍赫尔宣布在全州范围内禁止在纽约州信息与技术服务部管理的政府设备和网络上下载 DeepSeek 人工智能应用程序。（来源：美国纽约州政府）

2月13日，印度新德里的德里高等法院发布一份通知，回应一项公益诉讼，该诉讼要求限制使用中国人工智能聊天机器人 DeepSeek，这是 DeepSeek 遭遇的全球首场诉讼。（来源：新浪财经）

2月15日消息，美国德克萨斯州宣布正在调查人工智能公司 DeepSeek，因其涉嫌违反该州的数据隐私法。（来源：新浪新闻）

2月18日消息，韩国下架 DeepSeek，确认 DeepSeek 与字节跳动共享用户数据。（来源：朝鲜日报）

9. 美国法院裁决或阻碍人工智能发展，禁止未经许可使用受版权内容训练 AI

2月11日，美国特拉华州地方法院对“汤森路透”诉法律 AI 公司 Ross Intelligence 版权侵权诉讼作出部分简易判决”，汤森路透赢得美国首例 AI 训练版权诉讼，法院裁判内容如下：

一是 headnotes 和 Key Number System 具有独创性。法官确认汤森路透对 Westlaw 的 headnotes 和 Key Number System 享有版权。

二是版权侵权成立，主要包括：被告实施复制行为和实质性相似。

三是被告合理使用等抗辩不成立。被告围绕目的与性质、作品性质、使用数量比例以及市场影响合理使用等四大因素提出抗辩。

法官最终没有采纳被告构成合理使用的抗辩理由，对于被告提出的其他抗辩，也均予以驳回。同时，法官在本案裁决中也强调独创性和转换性在合理使用判断中的重要性。（来源：美国特拉华州地方法院）

10. 因非法获取用户数据，苹果在韩被罚 24.5 亿韩元

2月27日消息，韩国个人信息保护委员会（PIPC）宣布，对苹果公司和韩国移动支付平台卡卡奥支付（Kakao Pay）因非法获取和传输用户数据的行为进行处罚。其中，苹果公司被处以 24.5 亿韩元（约合 1240.9 万元人民币）的罚款，而卡卡奥支付则面临 59.68 亿韩元（约合 3022.8 万元人民币）的罚款。

据 PIPC 调查，卡卡奥支付在未经用户明确同意的情况下，向苹果公司提供了约 4000 万用户的个人信息。这些信息包括用户的唯一识别码、手机号码、电子邮件地址等敏感数据，以及与资金不足可能性相关的 24 项数据。

PIPC 指出，苹果公司和卡卡奥支付的行为严重违反了韩国的个人信息保护法。在未经用户同意的情况下，擅自收集、传输和使用用户数据，不仅侵犯了用户的隐私权，也损害了用户的合法权益。（来源：观察者网）

行业前沿观察一：两部门联合发文加强智能网联汽车召回及软件在线升级管理；四部门联合开展数字乡村强农惠农富农专项行动；工业和信息化部发文提升卫星网络国内协调效率

导读：近日，工业和信息化部、市场监管总局联合发布《关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知》（以下简称《通知》），旨在进一步规范智能网联汽车准入、召回及软件在线升级（OTA）管理，切实保障车辆安全，提升智能网联汽车产品安全水平，推动汽车产业高质量发展。

中央网信办、农业农村部、商务部、中国人民银行近日联合印发《关于开展数字乡村强农惠农富农专项行动的通知》，在浙江省、安徽省、福建省、山东省、河南省、重庆市、四川省、陕西省等8个重点省市部署开展数字乡村强农惠农富农专项行动。

工业和信息化部近日印发《卫星网络国内协调管理办法（暂行）》，进一步优化卫星网络国内协调程序，提升国内协调效率。办法明确了国内协调基本原则，就国内协调地位判定标准、各单位职责分工、干扰处置和监督措施等方面进行了规定，同时规范了国内协调程序，明确了建立国内协调关系的条件和流程，国内协调需求征集、汇总和公示，以及协调反馈等环节的时限要求。

关键词：人工智能、网络安全、智能汽车、数字乡村

1. 两部门印发关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知

工业和信息化部 市场监管总局关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知

工信部联通装〔2025〕45号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，市场监管局（厅、委），有关汽车企业和单位：

为落实《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于试行汽车安全沙盒监管制度的通告》《关于进一步加强汽车远程升级（OTA）技术召回监管的通知》，进一步做好搭载组合驾驶辅助系统和具备软件在线升级（以下称OTA升级）功能的智能网联汽车产品（以下简称智能网联汽车产品）准入与召回管理，规范汽车生产企业OTA升级活动，现将有关事项通知如下：

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大和二十届二中、三中全会精神，落实全国新型工业化推进大会部署和《质量强国建设纲要》，统筹发展和安全，坚持问题导向，强化管理协同，落实汽车生产企业生产一致性和质量安全主体责任，加强智能网联汽车产品准入和召回管理，进一步规范汽车生产企业OTA升级活动，提升智能网联汽车产品安全水平，维护公民生命、财产安全和公共安全，促进新技术规范应用，推动汽车产业高质量发展。

二、加强智能网联汽车产品准入与召回管理

(一) 强化企业产品质量安全主体责任。汽车生产企业应当主动履行产品质量安全主体责任，要根据《智能网联汽车产品准入、召回及软件在线升级管理与技术指南》（详见附件1），加强与研发生产智能网联汽车产品及开展OTA升级活动相适应的能力建设。企业要对智能网联汽车产品及OTA升级活动开展充分的测试验证，明确系统边界和安全响应措施，确保控制策略合理，严格履行告知义务，确保在开发、生产、运行等阶段进行有效的安全管理，不断提升产品功能、性能和质量安全水平。

(二) 细化产品准入与召回管理要求。在车辆产品主要技术参数表中，补充增加组合驾驶辅助系统和OTA升级信息有关技术参数（详见附件2）。补充增加的技术参数，纳入工业和信息化部产品准入和生产一致性管理，并向市场监管总局备案，保障汽车产品缺陷调查和召回管理顺利实施。企业申报智能网联汽车产品准入，应当完整、准确填报有关技术参数，涉及产品功能和性能的，还应当提交相关检验检测报告等验证材料。尚无国家标准对应的检验检测项目，允许依据企业产品技术规范提供自我检验报告，并承诺检验结果真实有效。工业和信息化部加强产品准入技术审查，强化生产一致性监督管理；市场监管总局加强产品安全风险研判，强化产品召回管理，促进智能网联汽车产品安全应用。已取得准入的智能网联汽车产品，企业应当在2025年6月1日前分别向工业和信息化部、市场监管总局补充报送有关技术参数及验证材料。工业和信息化部、市场监管总局根据

技术发展情况和管理需要，加快推进相关标准制修订，适时调整有关技术参数。

（三）深化产品沙盒监管。智能网联汽车产品取得道路机动车辆生产企业及产品准入许可等生产准入后，企业及时向市场监管总局提交搭载的组合驾驶辅助系统深度测试方案、质量安全风险评估方案及前期测试报告等材料。市场监管总局深化汽车安全沙盒监管，组织召回技术机构督促、指导企业开展深度测试、查找安全问题、完善技术标准、加强技术研判，不断提升组合驾驶辅助系统安全性能。

（四）健全事件事故报告与研判机制。企业在获知其生产销售的智能网联汽车产品发生组合驾驶辅助系统失效导致功能退出等事件或搭载组合驾驶辅助系统车辆发生碰撞等事故的，根据有关要求向工业和信息化部、市场监管总局报告（内容详见附件3）。工业和信息化部加强事件事故报告分析和研判，及时优化调整准入要求和技术标准。市场监管总局联合有关部门加强事故深度调查，强化智能网联汽车产品安全与召回管理。

（五）加强认证服务和管理。推动构建智能网联汽车质量认证体系，围绕组合驾驶辅助系统的数据安全、网络安全、功能安全、预期功能安全等领域积极推行自愿性认证，服务智能网联汽车产业健康发展。根据智能网联汽车标准制修订情况，及时将相关强制性国家标准纳入汽车强制性产品认证。

三、强化汽车软件在线升级活动协同管理

(六) 加强 OTA 升级活动监督管理。企业实施 OTA 升级活动，应当按要求向工业和信息化部、市场监管总局备案，并确保实施 OTA 升级活动后的汽车产品符合国家法律法规、技术标准及技术规范等相关要求。市场监管总局及时开展备案评估与监督检查，规范 OTA 升级应用方式，避免企业通过 OTA 升级隐瞒车辆缺陷或规避责任。

(七) 强化 OTA 升级活动分类管理。不涉及产品主要技术参数变更的 OTA 升级活动，企业在完成备案后，即可实施升级；涉及产品主要技术参数变更的，企业应当在取得产品变更许可并完成备案后，方可实施升级。涉及汽车自动驾驶功能的 OTA 升级活动，应当按照准入管理有关规定，取得相应许可。企业实施 OTA 升级活动消除汽车产品缺陷、实施召回的，应当按照《缺陷汽车产品召回管理条例实施办法》组织实施，并立即停止生产、销售缺陷汽车产品。若消除缺陷的措施涉及产品主要技术参数变更，企业应当在取得产品变更许可后，方可恢复相应汽车产品的生产。

(八) 强化管理协同。工业和信息化部、市场监管总局建立汽车 OTA 升级活动备案信息共享机制。按照协同管理的原则，根据技术发展情况及时优化备案要求，探索开展汽车 OTA 升级活动联合备案，推动 OTA 升级活动备案信息联通共用，联合开展 OTA 升级活动监督管理。

四、保障措施

(九) 强化责任落实。企业要落实智能网联汽车产品生产一致性和质量安全主体责任，持续确保汽车产品符合网络安全和密码应用安全、数据安全和个人信息保护等国家有关规定，严格履行 OTA 升级活动管理要求，

规范营销宣传行为，健全产品售后服务管理体系。企业存在未按规定申报或备案、隐瞒真实情况、提供虚假材料的，工业和信息化部、市场监管总局依据有关规定处理。

（十）加强监督管理。各地工业和信息化主管部门、市场监管部门要加强协同配合，按照《道路机动车辆生产企业及产品准入管理办法》《缺陷汽车产品召回管理条例》有关要求，做好对本通知落实情况的监督检查，督促企业落实主体责任。各地市场监管部门根据市场监管总局部署，协助开展缺陷调查、事故调查与沙盒监管等工作。

（十一）夯实能力建设。工业和信息化部、市场监管总局组织有关技术机构加强新产品、新技术的管理技术研究，夯实新技术参数分析与测试验证、事件监测与分析、事故深度调查与缺陷研判、场景数据研究与应用等能力建设，联合有关部门加快推进组合驾驶辅助、OTA升级等标准规范制修订及实施，不断提升智能网联汽车技术和安全水平。

本通知自印发之日起施行。

工业和信息化部

市场监管总局

2025年2月25日

2. 中央网信办 农业农村部 商务部 中国人民银行联合开展数字乡村强农惠农富农专项行动

近日，中央网信办、农业农村部、商务部、中国人民银行联合印发《关于开展数字乡村强农惠农富农专项行动的通知》（以下简称《通知》），在浙江省、安徽省、福建省、山东省、河南省、重庆市、四川省、陕西省等8个重点省（市）部署开展数字乡村强农惠农富农专项行动。

《通知》要求，要以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大和二十届二中、三中全会精神，坚持农业农村优先发展，坚持城乡融合发展，突出目标导向和问题导向，以学习运用“千万工程”经验为引领，以建立完善乡村振兴长效机制为目标，把增加农民收入作为中心任务，把农民是否真正受益作为衡量标准，充分发挥信息化赋能作用，千方百计推动农业增效益、农民增收入、农村增活力，为推进乡村全面振兴提供强有力支撑。

《通知》明确了行动目标。通过2年左右时间，重点省（市）数字乡村建设取得突出进展。农业生产信息化水平进一步提升，乡村新产业新业态持续壮大，农村网络零售额稳步增长，城乡数字鸿沟加速弥合，基本公共服务更加均衡可及，乡村治理效能显著提高，农村集体经济和农民实现“双增收”，带动全国数字乡村发展迈上新台阶。重点省（市）结合所辖县（市、区）经济基础、资源禀赋、参与意愿等实际情况，确定纳入专项行动范围的县（市、区）比例。

《通知》部署了6项重点任务。一是大力推进智慧农业发展，包括积极打造智慧农业发展高地，加快5G与智能农机深度融合等内容。二是培育壮大新产业新业态，包括深化“数商兴农”，因地制宜发展乡村新业态，开展乡村旅游数字提升行动等内容。三是建强乡村数字基础设施，包括按需推进农村5G网络和千兆光网建设，完善农村寄递物流体系等内容。四是深化数字惠农便民服务，包括构建线上线下相结合的乡村信息服务体系，深化实施金融科技赋能乡村振兴示范工程等内容。五是打造智慧乡村治理体系，包括推进涉农数据汇聚共享和开放开发，深化整治“指尖上的形式主义”，切实为基层减负赋能等内容。六是拓宽农民增收致富渠道，包括进一步完善联农带农机制，有效增加农民经营性收入，因地制宜发展新型农村集体经济等内容。

下一步，中央网信办将会同有关部门、重点省（市）建立完善工作机制，加强政策支持、人才保障、跟踪监测和宣传推广，营造各地互学互鉴、共促共进的良好氛围。（来源：中国网信网）

3. 工业和信息化部发文提升卫星网络国内协调效率

3月11日消息，工业和信息化部近日印发《卫星网络国内协调管理办法（暂行）》，进一步优化卫星网络国内协调程序，提升国内协调效率。

办法明确了国内协调基本原则，就国内协调地位判定标准、各单位职责分工、干扰处置和监督措施等方面进行了规定，同时规范了国内协调程

序，明确了建立国内协调关系的条件和流程，国内协调需求征集、汇总和公示，以及协调反馈等环节的时限要求。

与此同时，办法优化了国内协调机制，强化了国家无线电办公室统筹协调作用，提出了无需建立国内协调关系的情形，减少国内协调对象范围，引入五种完成国内协调的形式，降低国内协调复杂度。

记者了解到，办法自 2025 年 5 月 1 日起施行。下一步，工业和信息化部将加强办法宣传和解读、制定配套制度，确保办法各项措施落到实处，进一步激发航天企业活力，推动航天产业高质量发展。（来源：新华网）

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，举办研讨会、召开理事会议，开展技术交流活动等。广东省网络空间安全协会获评“广东省科普教育基地”；甘肃省商用密码行业协会成功召开协会二届二次理事会；武汉市网络安全协会成功召开协会第二届理事会第五次会议；上海市信息安全行业协会“船舶网络安全，护航智慧海事”研讨会顺利举办；海南省网络安全和信息化协会两省协会联合开展“2025 冀琼新一代信息技术交流活动”；甘肃省商用密码行业协会组织开展 2024 年度商用密码应用推广典型案例评选工作等。

关键词：理事会议、商用密码、团体标准、网络安全、信息安全

1. 广东省网络空间安全协会获评“广东省科普教育基地”

近日，广东省科学技术协会和省科学技术厅联合发布《关于命名“广东省科普教育基地（2025-2029年）”的通知》，公布“广东省科普教育基地（2025-2029年）”认定名单。由广东省网络空间安全协会申报的“广东省网络安全和信息化科普教育基地”成功入选！

此次被命名“广东省科普教育基地”，是“广东省网络安全和信息化科普教育基地”的新起点也是协会发展道路上的重要一步。协会将以此为契机，持续完善科普设施，提升科普服务质量，通过系列科普教育活动，弘扬科学精神，传播网络空间安全知识，为我国网络安全行业高质量发展贡献力量。

2. 甘肃省商用密码行业协会成功召开协会二届二次理事会

3月5日，甘肃省商用密码行业协会二届二次理事会在兰州成功召开。会议全面总结2024年工作，谋划部署2025年重点工作。协会全体理事、部分会员单位代表及省国家密码管理局业务处室同志和相关工作人员共100余人参加会议。

会议由协会秘书长主持，审议通过了2024年度工作报告及财务情况报告、《甘肃省商用密码行业协会财务管理办法》等8项内部管理制度、新增会员名单和专业委员会专家名单，同时还通报了2024年度商用密码应用推广典型案例及优秀会员单位。

3. 武汉市网络安全协会成功召开协会第二届理事会第五次会议

武汉市网络安全协会第二届理事会第五次会议于2025年2月27日在协会新设立的会员活动中心顺利召开。此次会议在主管部门的指导下，全面总结协会2024年度工作成果，审议通过2025年工作计划及多项重要提案，为全市网络安全事业高质量发展凝聚共识、擘画蓝图。主管部门相关处室负责人到会指导，协会会长、副会长、监事、理事参会，各专（工）委会负责人、部分会员代表以及秘书处全体成员均列席参加。

4. 上海市信息安全行业协会“船舶网络安全，护航智慧海事”研讨会顺利举办

2月20日，以“船舶网络安全，护航智慧海事”为主题的研讨会在上海宝山举办。本次研讨会由上海市信息安全行业协会主办，北京六方云信息技术有限公司和上海佳文昇科技有限公司联合承办，汇聚了来自政府、高校、船级社、设计院、船东、船厂及网络安全供应商等各界精英，共同探讨船舶网络安全的前沿议题。中国海事局和上海市经信委软信处领导莅临并致辞。

本次会议的成功举办，为参会各方提供了一个深入交流、共同探讨的平台，更为推动船舶网络安全技术的发展和應用注入了新的动力和活力。据悉，2025年5月，上海市信息安全行业协会将在有关部门和企业的支持下，在上海举办船舶网络安全高峰论坛。

5. 海南省网络安全和信息化协会两省协会联合开展“2025 冀琼新一代信息技术交流活动”

为贯彻落实党中央建设海南自贸港的决策部署和河北、海南两省加强战略合作精神，2025年2月18日，河北省信息产业与信息化协会和海南省网络安全和信息化协会联合主办“2025 冀琼新一代信息技术交流活动”。此次活动以“协同创新 共谋合作发展新生态”为主题，两地协会会员、企业家共40人参与。

活动中，两省协会还签署了战略合作协议，将在技术创新、人才交流、成果转化、产业合作等方面，携手共进，为两省高质量发展做出新贡献。

6. 甘肃省商用密码行业协会组织开展2024年度商用密码应用推广典型案例评选工作

为深入贯彻落实《中华人民共和国密码法》、《商用密码管理条例》，甘肃省商用密码行业协会在省国家密码管理局指导下，组织开展了全省2024年度商用密码应用推广典型案例征集工作，力求通过系统梳理特色做法、搭建交流互鉴平台，促进经验共享与成果转化，切实提升商用密码创新应用能力。

经过前期申报、审查、初筛等环节，近期，甘肃省商用密码行业协会组织召开了2024年度商用密码应用推广典型案例专家评审会，邀请省市密码管理部门、省内重点高校及行业相关企业的5名专家组成评审组，重点评估典型案例的技术突破性、场景适配性和社会效益，通过“材料审阅-交

流研讨-量化评分”全流程闭环评审，最终 12 个涵盖政务、民生、产业的商用密码应用项目分获一、二、三等奖。

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，切实践行理论与实践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

网络安全漏洞
网络信息内容生态治理
关键信息基础设施保护
网络安全等级保护
网络安全人才培养
数据跨境流动
新技术新应用
数据安全
网络安全审查
网络安全法
网络安全行政执法
网络安全行刑衔接
物联网安全
个人信息保护
密码法治
供应链安全

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

数据存储在国内，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

1 - 3 周

周期视情况而定

01 情况调研

02 风险评估

03 指导落实
整改

04 出具风险
评估报告



3 - 5 周



1 - 2 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

- 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

.....

