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7月第7期 （总第24期）

2025年7月15日

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

目　录

境内前沿观察一：政策立法

导读：6 月，网络安全、数据资源流通、数据跨境等方面仍是国家和地方政策立法重点关注内容，在配套规章、指南等层面规定更加细致。

全国人大常委会表决通过新修订的《治安管理处罚法》，新增关于计算机系统类以及违反国家有关规定向他人出售或者提供公民个人信息的违法行为。

国家互联网信息办公室发布《可能影响未成年人身心健康的网络信息分类办法（征求意见稿）》。征求意见稿指出，不得在专门以未成年人为服务对象的网络产品和服务中，呈现可能影响未成年人身心健康的网络信息等内容。国家互联网信息办公室发布《网信部门行政处罚裁量权基准适用规定》，明确网信部门适用行政处罚裁量权基准，应当遵循法制统一、公平公正、过罚相当、处罚与教育相结合等原则。

国家互联网信息办公室发布《数据出境安全评估申报指南（第三版）》，指导和帮助数据处理者规范有序申报数据出境安全评估。工信部、国家网信办、国家发改委等八部门联合发布《汽车数据出境安全指引（2025 版）（征求意见稿）》。征求意见稿适用于汽车数据处理者开展数据出境活动，明确列出汽车研发设计、生产制造、驾驶自动化等场景下，应当申报数据出境评估的重要数据。

国家卫生健康委办公厅、国家中医药局综合司、国家疾控局综合司发布《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》。

《通知》要求加强医疗机构内部管理，落实分级管理要求，遵循最小可用原则，明确临床诊疗、教学、管理等相关人员分级访问权限和时限等。

地方层面，山西、湖南、天津多省市推进数据安全与发展相关内容。山西省数据局发布《山西省数据流通安全治理工作实施办法（征求意见稿）》，规定数据基础、数据资源、数据授权运营等方面的安全义务。湖南省人民政府办公厅发布《湖南省国家数据要素综合试验区建设方案（2025—2027年）》，围绕打造数据制度共创示范标杆、打造数字设施共建示范标杆、打造数据要素共用示范标杆等五方面，提出多项措施。天津市数据局印发《2025年度政务数据共享责任清单》《2025年度公共数据开放清单》，贯彻落实《关于加快公共数据资源开发利用的意见》《政务数据共享条例》等部署要求。

关键词：治安管理处罚法；行政处罚裁量权；数据资源；数据安全

（一）国家层面动向

1. 全国人大常委会表决通过新修订的《治安管理处罚法》

6 月 27 日，十四届全国人大常委会第十六次会议表决通过新修订的《治安管理处罚法》，共 6 章 144 条，自 2026 年 1 月 1 日起施行。此次修订将一些新出现的影响社会治安的行为纳入管理范围，进一步优化和完善治安案件办理程序等方面内容。

新修订的《治安管理处罚法》增加三种关于计算机信息系统的违法行为：（1）采用其他技术手段，获取计算机信息系统中存储、处理或者传输的数据；（2）对计算机信息系统实施非法控制；（3）提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具的。第五十六条新增违反国家有关规定向他人出售或者提供公民个人信息的处罚，规定："违反国家有关规定，向他人出售或者提供个人信息的，处十日以上十五日以下拘留；情节较轻的，处五日以下拘留。窃取或者以其他方法非法获取个人信息的，依照前款的规定处罚。"

在提升执法效率与公正性方面，此次修订进一步规范和保障执法，完善有关处罚程序，对人民警察出示人民警察证、"一人执法"具体情形等作出规定。在执法监督方面，此次修订在建立治安违法记录封存制度、同步录音录像等方面作出细化规定。（来源：新华社）

2. 《上海合作组织成员国数字化转型行动计划》通过

6 月 17 日，第四次上海合作组织成员国信息通信技术发展部门负责人会议通过了《上海合作组织成员国数字化转型行动计划》，旨在落实 2023 年《上海合作组织成员国元首理事会关于数字化转型领域合作的声明》和 2024 年《上海合作组织成员国元首理事会阿斯塔纳宣言》，促进上海合作组织成员国数字化转型领域务实合作。

行动计划包括数字化转型政策合作行动、数字基础设施建设合作行动、数字政府合作行动、云计算合作行动、中小企业数字化行动、数字技术研发应用行动、数字技术人才交流行动七项具体行动。

在数字化转型政策合作行动中，各国强调数字化转型的重要性，一致同意加强数字化转型战略、规划、政策对接沟通，分享发展经验，促进相互借鉴，为数字化转型发展创造有利条件。

在数字基础设施建设合作行动中，各国将加强先进技术（包括绿色技术）合作，如新一代信息通信技术、骨干网络、数据中心及数字公共基础设施（DPI）等领域合作，积极开发、部署和利用普惠包容和可持续的数字基础设施，提升区域数字化水平，夯实数字化转型基础。

在数字政府合作行动中，各国将推广人工智能、大数据、云计算、智慧城市等数字技术在政务领域的应用，加强电子认证在跨境互认方面沟通合作，围绕应用系统、平台建设、数据治理等方面分享经验。

其他行动涉及内容包括：各国将推进云计算基础设施领域合作，促进云计算在经济关键领域的应用，共同提升人工智能算力；各国将鼓励中小

企业进行数字化转型，帮助更多中小企业对接资源、技术和资金，鼓励和支持数字技术在各经济领域的应用，分享数字化产品和解决方案，促进中小企业融入全球供应链和国际价值链；各国将加强理念互鉴和经验分享，鼓励企业、研究机构和智库在人工智能、大数据、云计算等前沿领域开展技术培训和学术交流，提升数字能力和数字素养，为数字化转型提供人才支撑等内容。（来源：克拉玛依政府网）

（二）部委层面动向

1. 全国数据标准化技术委员会秘书处发布 7 项全国一体化算力网技术文件征求意见稿

6 月 7 日，全国数据标准化技术委员会秘书处发布 7 项全国一体化算力网技术文件征求意见稿，包括《全国一体化算力网算力并网技术要求（征求意见稿）》、《全国一体化算力网算力资源管理与调度技术要求（征求意见稿）》、《全国一体化算力网算力多量纲计费技术要求（征求意见稿）》、《全国一体化算力网算力算效衡量技术要求（征求意见稿）》、《全国一体化算力网算力运营服务与撮合交易技术要求（征求意见稿）》、《全国一体化算力网算力监测接口要求（征求意见稿）》、《全国一体化算力网算力中心能力评估要求（征求意见稿）》。（来源：国家数据局）

2. 国家互联网信息办公室发布《可能影响未成年人身心健康的网络信息分类办法（征求意见稿）》

6 月 13 日，国家互联网信息办公室发布《可能影响未成年人身心健康的网络信息分类办法（征求意见稿）》。

征求意见稿指出，可能影响未成年人身心健康的网络信息是指除危害未成年人身心健康内容的违法信息外，通过互联网发布传播的其他可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生极端情绪、养成不良嗜好等的信息。

征求意见稿提出，可能引发或者诱导未成年人模仿或实施不良行为的信息包括但不限于：使用网络黑话烂梗等不文明用语的；宣扬代写代抄、抄袭作弊、逃学旷课、校园霸凌等违反校纪校规行为的；诱导未成年人盲目追星、参与“饭圈”行为；诱导未成年人参与网络主播、充值打赏、过度消费等博取关注或谋取利益行为等。

征求意见稿规定，网络产品和服务提供者应当落实《未成年人网络保护条例》要求，不得在首页首屏、弹窗、热搜、榜单、推荐、精选等处于产品或者服务醒目位置、易引起用户关注的重点环节，呈现可能影响未成年人身心健康的网络信息。提供算法推荐、生成式人工智能等服务的，应当建立健全安全管理制度和技术措施，防范和抵制传播可能影响未成年人身心健康的网络信息。不得在专门以未成年人为服务对象的网络产品和服务中，呈现可能影响未成年人身心健康的网络信息。（来源：网信中国）

3. 国家互联网信息办公室发布《网信部门行政处罚裁量权基准适用规定》

6 月 26 日，国家互联网信息办公室发布《网信部门行政处罚裁量权基准适用规定》，自 2025 年 8 月 1 日起施行。

规定明确，行政处罚裁量权基准是指网信部门在实施行政处罚时，按照裁量涉及的违法行为的事实、性质、情节、社会危害程度、当事人主观过错等因素，对法律、法规、规章中的原则性规定或者具有一定弹性的执法权限、裁量幅度等内容进行细化量化而形成的具体执法尺度和标准。明确网信部门适用行政处罚裁量权基准，应当遵循法制统一、公平公正、过罚相当、处罚与教育相结合等原则。

规定提出，网信部门行政处罚裁量权基准划分为不予处罚、减轻处罚、从轻处罚、一般处罚、从重处罚等裁量阶次。明确不予处罚、减轻处罚、从轻处罚、从重处罚等具体适用情形。规定违法行为不具有不予处罚、减轻处罚、从轻处罚或者从重处罚情形的，应当给予一般处罚。

规定明确，省、自治区、直辖市和设区的市、自治州网信部门可以结合工作实际制定本行政区域内的行政处罚裁量权基准。上级网信部门应当通过行政执法情况检查、行政执法案卷评查等方式，对下级网信部门行使行政处罚裁量权工作进行监督。（来源：网信中国）

4. 国家互联网信息办公室发布《数据出境安全评估申报指南（第三版）》

6 月 27 日，国家互联网信息办公室发布《数据出境安全评估申报指南（第三版）》，对数据处理者申报数据出境安全评估需要提交的相关材料进行优化简化，明确数据处理者申请延长数据出境安全评估结果有效期的条件、流程、材料等内容。

数据处理者因业务需要向境外提供重要数据和个人信息，符合数据出境安全评估适用情形的，应当根据《数据出境安全评估办法》和《促进和规范数据跨境流动规定》，按照申报指南申报数据出境安全评估。评估结果有效期届满，符合申请延长评估结果有效期条件的，数据处理者可以在有效期届满前 60 个工作日内提出延长评估结果有效期申请。（来源：网信中国）

5. 国家互联网信息办公室发布涉企行政检查事项清单

6 月 30 日，国家互联网信息办公室发布涉企行政检查事项清单，共五项检查事项，包括“清朗”系列专项行动回头看相关监督检查、对网站平台落实信息内容管理主体责任情况的监督检查、对互联网新闻信息服务活动的监督检查、对外国机构提供金融信息服务的监督检查、对互联网新技术新应用进行安全评估和监督检查、对数据安全和个人信息保护的管理制度建设、技术防护措施、数据出境合规等情况的检查评估。（来源：国家网信办）

6. 国家密码管理局等三部门发布《关键信息基础设施商用密码使用管理规定》

6 月 11 日，国家密码管理局、国家互联网信息办公室、公安部联合发布《关键信息基础设施商用密码使用管理规定》，自 2025 年 8 月 1 日起施行。

规定提出，关键信息基础设施运营者的主要负责人对关键信息基础设施商用密码使用管理负总责，负责关键信息基础设施商用密码使用和涉及商用密码的重大网络安全事件处置工作。

规定强调，关键信息基础设施建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。建设过程中需要调整商用密码应用方案的，应当重新开展商用密码应用安全性评估，评估通过后方可按照调整后的商用密码应用方案继续建设。关键信息基础设施运行前，其运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。关键信息基础设施未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。

目前，关键信息基础设施运营者已开展商用密码使用相关工作，但由于缺乏管理法规制度的具体指导和约束，部分网络与信息系统建设未深入分析商用密码使用需求并体系化加以解决，机械堆叠商用密码产品，或者简单实施外挂式、补丁式改造，商用密码应用的合规性、正确性、有效性难以保证；个别网络与信息系统仍然使用未经检测认证合格的商用密码产

品、服务或者未经审查鉴定的商用密码技术，存在较大安全隐患。《管理规定》出台为规范关键信息基础设施商用密码使用，保护关键信息基础设施安全提供指引。（来源：国家密码管理局）

7. 工业和信息化部等八部门联合发布《汽车数据出境安全指引（2025 版）（征求意见稿）》

6 月 13 日，工信部、国家网信办、国家发改委等八部门联合发布《汽车数据出境安全指引（2025 版）（征求意见稿）》。

征求意见稿适用于汽车数据处理者开展数据出境活动。汽车数据是指汽车设计、生产、销售、使用、运维等过程中涉及的个人信息和重要数据。汽车数据处理者是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、电信运营企业、自动驾驶服务商、平台运营企业、经销商、维修机构以及出行服务企业等。

征求意见稿列出汽车研发设计场景、生产制造场景、驾驶自动化场景、软件升级服务场景、联网运行场景下，应当申报数据出境评估的重要数据。例如在研发设计场景，征求意见稿指出，重要数据包括：（1）汽车数据处理者在整合全球研发资源、产品协同设计开发过程中，收集和产生的物料清单、研发设计文档、产品技术开发源代码数据。（2）汽车数据处理者开展汽车产品仿真、场地和实际道路测试过程中，收集和产生的标注场景数据、仿真场景数据、测试场景数据。

此外，征求意见稿还对汽车数据出境提出安全保护要求，包括管理要求、防护技术要求、日志要求以及应急处置要求四个方面。例如日志要求

方面，征求意见稿提出，汽车数据处理者应当：（1）记录日志。汽车数据处理者应当对汽车数据出境的网络通信行为、直接向境外传输汽车数据的主机的操作行为进行记录。（2）留存日志。汽车数据处理者应对网络流量日志、操作行为日志、安全日志进行防篡改留存，留存时间不少于3年。（3）审计日志。汽车数据处理者应当对网络流量日志、操作行为日志、安全日志进行审计，当发现存在非法操作等安全风险隐患时，及时响应处置。（来源：网信中国）

8. 国务院办公厅印发《关于进一步完善信用修复制度的实施方案》

6月22日，国务院办公厅印发《关于进一步完善信用修复制度的实施方案》，为完善信用修复制度提出六项措施，包括统一信用信息公示平台、完善失信信息分类标准、明确信用修复申请渠道等。

简化信用修复申请材料方面，方案提出，鼓励行业主管部门通过本部门信息系统直接获取证明材料。鼓励推广“两书同达”模式，即向信用主体送达行政处罚决定书或列入严重失信主体名单决定书时，同步送达信用修复告知书，确保信用主体第一时间知晓信用修复有关政策。

压实信用修复办理责任方面，方案提出，“信用中国”网站收到信用修复申请后，按照“谁认定、谁修复”原则，及时推送给有关行业主管部门办理修复。对已经建立信用修复制度和信息系统的部门和单位，有关系统要与“信用中国”网站深度联通；对尚未建立相应制度和系统的部门和单位，“信用中国”网站为其开设账号，由其通过“信用中国”网站办理修复。

同步更新信用修复结果方面，方案提出，信用修复后，行业主管部门及时在本部门网站停止公示相关失信信息，同步向“信用中国”网站提供信用修复结果；“信用中国”网站同步停止公示相关失信信息，并将信用修复结果反馈申请人；有关部门更新信用评价结果，依法依规解除相应失信惩戒措施。“信用中国”网站统一汇总、每日更新、及时共享各类信用修复结果，并为信用主体提供信用修复决定书下载服务。（来源：中国政府网）

9. 国家卫健委发布《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》

6 月 23 日，国家卫生健康委办公厅、国家中医药局综合司、国家疾控局综合司发布《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》。

通知要求加强医疗机构内部管理。医疗机构需明确电子病历范围，压实主体责任，依法依规严格保护患者隐私，将电子病历信息规范使用管理情况纳入绩效评价。健全管理制度，建立电子病历使用长效监管机制和应急处置制度。落实分级管理要求，遵循最小可用原则，明确临床诊疗、教学、管理等相关人员分级访问权限和时限。

通知要求规范电子病历信息使用。医疗机构需规范相关人员使用权限和行为，不得违规收集、传输或泄露患者信息。加强短期人员培训与管理，确保权限与职责匹配，并与外部服务商签订保密协议。保障全流程可追溯，

采用数字水印等技术，确保使用过程留痕。确保数据安全，建立电子病历信息安全防护体系，防范潜在安全风险。

通知要求强化卫生健康行政部门监管。地方各级卫生健康行政部门(含中医药、疾控部门，下同)要加强对医疗机构指导和监管，组织推进落实，定期监测评估。各省级卫生健康行政部门要将医疗机构规范使用电子病历信息情况作为医院评审、医院巡查、智慧医院建设等相关工作重要评估依据。（来源：国家卫生健康委员会医政司）

10. 全国网安标委公开征求 6 项网络安全标准实践指南意见

6 月 23 日，全国网络安全标准化技术委员会公开征求《网络安全标准实践指南—人工智能生成合成内容标识方法文件元数据隐式标识文本文件》、《网络安全标准实践指南—人工智能生成合成内容标识方法文件元数据隐式标识图片文件》、《网络安全标准实践指南—人工智能生成合成内容标识方法文件元数据隐式标识音频文件》、《网络安全标准实践指南—人工智能生成合成内容标识方法文件元数据隐式标识视频文件》《人工智能生成合成内容标识方法 文件元数据隐式标识 文本文件（征求意见稿）》、《网络安全标准实践指南—人工智能生成合成内容检测技术指南》六项网络安全标准实践指南意见。（来源：全国网安标委）

11. 七部门联合倡议：守护青少年远离网络涉毒风险

6 月 20 日，中央网信办、教育部、公安部等七部门发布联合倡议《共同守护 让青少年远离涉麻精药品等成瘾性物质滥用危害——致青少年、家长和社会各界的倡议书》。

倡议提出，依托咪酯、右美沙芬、曲马多等既是治病的药品，同时也是我国规定管制的麻精药品，广大青少年务必遵医嘱使用，非医疗目的滥用即是吸毒违法行为。要警惕“无害”谎言骗术，面对诱惑勇敢说“不”。积极倡导家庭、社会共担禁毒责任，净化网络环境，为青少年健康成长织密无毒的铁壁铜墙。当孩子出现情绪异常、行为失控等情况时，应及时为他们提供专业帮助。以爱为盾，科学为剑，秉持“健康人生、绿色无毒”理念，全力防范青少年滥用涉麻精药品等成瘾性物质。（来源：网信中国）

（三）地方层面动向

1. 山西省数据局发布《山西省数据流通安全治理工作实施办法（征求意见稿）》

6 月 10 日，山西省数据局发布《山西省数据流通安全治理工作实施办法（征求意见稿）》，自印发之日起施行。征求意见稿包括安全职责、数据基础安全管理、数据资源安全管理、数据授权运营安全管理等内容。

数据基础安全管理方面，征求意见稿提出，数据基础设施建设应按照国家信息安全战略和相关法律法规，结合具体业务需求，通过可信接入、安全互联、跨域管控和全栈防护等安全管理，建立网络安全风险和威胁的

动态发现、实时告警、全面分析、协同处置、跨域追溯和态势掌控能力，提供应对芯片、软件、硬件、协议等内置后门、漏洞安全威胁的内生防护能力。

具体而言，在硬件安全方面，应按照法律法规要求采用符合国家安全标准的硬件设备。确保数据流通全过程中的物理安全。芯片、服务器、网络设备、存储介质等各类硬件设备应具备防篡改、防盗窃的防护能力，应定期进行硬件安全审计和维护，及时更换过时或存在安全隐患的设备，防止因硬件漏洞导致的数据泄露或损坏。

在软件安全方面，应部署满足安全等级防护要求的软件系统，采用加密技术、数据沙箱、数字签名等安全技术保障数据流通过程中的保密性与完整性，通过入侵检测和防御系统实现实时监控和应对潜在安全威胁。（来源：山西省数据局）

2. 山西省数据局发布《山西省公共数据资源登记管理实施细则（征求意见稿）》

6 月 16 日，山西省数据局发布《山西省公共数据资源登记管理实施细则（征求意见稿）》，自印发之日起施行，有效期 3 年。征求意见稿包括职责分工、登记要求、登记程序等内容。

登记要求方面，征求意见稿规定，登记主体应对纳入授权运营范围的公共数据资源以及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。已纳入山西省公共数据开放清单的数据资源和使用财政资金采购的公共数据以外的数据资源，应由数据持有或管理部门组织登记。

登记程序方面，征求意见稿规定，公共数据资源登记应按照申请、受理、形式审核、公示、赋码等程序开展。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。登记机构应对登记材料内容进行形式审核，自受理之日起20个工作日之内完成审核。审核未完成的，应当向登记主体说明原因。

登记管理方面，征求意见稿规定，省级数据管理部门按照统筹建设、集约使用的原则搭建山西省公共数据资源登记平台，与国家公共数据资源登记平台对接，实现登记信息互联互通和登记结果统一赋码。省级登记机构负责省公共数据资源登记平台运行和维护。登记平台应具备登记办理、登记信息查询和共享、存证溯源、安全保障等能力，支撑数据管理部门对登记业务进行全流程管理。（来源：山西省数据局）

3. 湖南省人民政府办公厅发布《湖南省国家数据要素综合试验区建设方案（2025—2027年）》

6月10日，湖南省人民政府办公厅发布《湖南省国家数据要素综合试验区建设方案（2025—2027年）》，围绕打造数据制度共创示范标杆、打造数字设施共建示范标杆、打造数据要素共用示范标杆等五个方面，提出二十项措施。

打造数据制度共创示范标杆方面，方案提出，要细化落地数据产权制度。探索建立数据持有权、使用权、经营权分置的产权运行机制，制定湖南省数据产权登记管理规定、数据产权登记审查指南、数据产权登记凭证应用管理规范等文件。建成全省统一的数据产权登记服务平台。探索先进

制造、音视频等特色行业的数据产权登记审查方法和产权登记凭证应用，形成一批典型案例。

打造数字设施共建示范标杆方面，方案提出，要构建数据安全防护体系。推进省数据安全防护及监控平台、省网络安全协调指挥平台、马栏山视频文创园数据安全防护平台、长沙数据网络安全大脑暨科创研发总部基地等建设，提升公共数据和企业数据安全风险分析、监测监管和处置能力。支持数据安全防护平台云服务化，发布服务目录清单，为中小企业提供数据安全合规服务。

打造数据要素共用示范标杆方面，方案提出，要加快公共数据资源开发利用。在医疗健康、文化旅游、金融服务等领域开展公共数据资源授权运营试点，以公共数据资源开发利用带动全社会数据资源融合应用。鼓励融合多源数据，对公共数据产品和服务进行再开发，提升数据产品和服务价值。（来源：湖南省人民政府）

4. 湖北省数据局印发《湖北省推进可信数据空间发展行动方案》

6 月 13 日，湖北省数据局印发《湖北省推进可信数据空间发展行动方案》，围绕分类推进可信数据空间建设、面向重点领域拓展可信数据空间应用、探索可信数据空间市场化运营机制等四个方面，提出二十三条措施。

分类推进可信数据空间建设方面，方案提出，着力构建合规便捷的跨境可信数据空间。支持湖北自由贸易试验区、鄂州花湖国际机场等针对跨境电商、跨境支付、供应链管理等场景应用，建立高效便利安全的数据跨

境流动机制，出台实施数据出境管理清单（负面清单），构建数据跨境监控、存证备案、出境管控等能力体系。

面向重点领域拓展可信数据空间应用方面，方案提出，服务人工智能产业发展，推动高质量数据集建设。推广在人工智能产业的应用，围绕工业制造、交通运输、医疗卫生、教育教学、文化旅游、生态环境等重点领域，依托武汉、宜昌、黄石数据标注城市创建，促进形成一批高质量数据集，丰富人工智能大模型训练推理“算料”。

探索可信数据空间市场化运营机制方面，方案提出，加强安全防护能力，保障数据安全。落实数据分类分级保护制度，构筑可信数据空间动态防御能力。通过数据安全监测、防护、审计等手段保障基础环境安全。建立健全信息报告、情报共享等安全监管能力。依托湖北信创产业生态，以国产数据库为核心，打造全栈信创技术体系。（来源：数据湖北）

5. 陕西省数据和政务服务局发布《陕西省公共数据资源授权运营实施细则（试行）》（公开征求意见稿）

6 月 16 日，陕西省数据和政务服务局发布《陕西省公共数据资源授权运营实施细则（试行）》（公开征求意见稿），包括职责分工、授权管理、运营实施等内容。

职责分工方面，公开征求意见稿规定，行业主管部门负责对本部门管理的公共数据资源开展授权运营；实施机构开展授权运营活动；运营机构负责对授权范围内的公共数据资源进行治理开发。

授权管理方面，公开征求意见稿规定，省级授权运营模式以整体授权为主，由数据管理部门在公共数据汇集共享和业务协同的基础上进行授权，

也可结合实际由数据管理部门会同行业主管部门开展分领域、依场景授权。省数据和政务服务中心为省级综合性实施机构，分领域、依场景授权的实施机构由数据管理部门会同行业主管部门确定。市级人民政府结合本地实际确定本区域公共数据授权运营模式。

运营实施方面，公开征求意见稿规定，实施机构应当根据审定同意后的实施方案，制定规范的运营机构遴选及退出流程。按照法律法规要求，以公开招标、邀请招标、竞争性谈判等公平竞争方式选择运营机构。实施机构应独立或会同本级有关业务主管部门，与依法选定的运营机构签订公共数据资源授权运营协议。授权运营协议内容应充分征求各方意见，经实施机构“三重一大”决策机制审议通过后签订，并报本级数据管理部门备案。市级数据管理部门应将本地区审议通过后的授权运营协议在一个月内报省级数据管理部门备案。（来源：陕西省数据和政务服务局）

6. 天津市数据局印发《2025 年度政务数据共享责任清单》《2025 年度公共数据开放清单》

6 月 26 日消息，为贯彻落实《关于加快公共数据资源开发利用的意见》《政务数据共享条例》等部署要求，建立健全全市政务数据资源目录体系，规范全市政务数据共享、公共数据开放，深化政务数据资源开发利用，提升政府数字化治理能力和政务服务效能，推动高质量发展。天津市数据局近日印发《2025 年度政务数据共享责任清单》《2025 年度公共数据开放清单》，清单汇总各市级部门、各区提供的政务数据和公共数据资源，为各单位更好实现政务数据资源共享和业务协同提供依据。（来源：天津市数据局）

境内前沿观察二：治理实践

导读：6 月，公安、网信、通信管理部门等机构持续发力，对网络安全、数据安全、个人信息安全等开展治理，助力提升网络安全防护能力，构建天朗气清的网络空间。

公安部网安局发布两起涉抗日战争网络谣言案例。上海警方今年以来依托“砺剑”“净网”系列专项行动，依法严厉打击涉企造谣抹黑、有偿删帖、舆情敲诈等违法犯罪活动。山东青岛公安网安部门侦破一起诱骗高校学生注册网络账号并层层倒卖的侵犯公民个人信息案，抓获涉案人员 151 人，涉案金额 4300 余万元。辽宁锦州网安部门成功侦破一起特大刷单类非法经营案，打掉一个涉及全国 6 省 14 市的特大犯罪团伙，涉案金额高达 9000 余万元，17 名主要犯罪嫌疑人已全部抓捕归案。

中央网信办发布中国互联网联合辟谣平台 2025 年 5 月辟谣榜综述，网络谣言集中在社会热点事件、公共安全、招考政策、旅游出行等领域。重庆市大渡口区网信办近日联合建委、公安、市场监管、检察院对属地某公司涉嫌违法违规处理个人（人脸）信息行为进行联合调查，依法对履行主体责任不到位的某公司作出行政处罚。

工业和信息化部信息通信管理局近日组织第三方检测机构进行抽查，共发现 57 款 APP 及 SDK 存在侵害用户权益行为。上海、江苏、浙江等多省市通信管理局发布侵害用户权益 APP/SDK 名单。

关键词：网络谣言；个人信息保护；数据犯罪

（一）公安机关治理实践

1. 公安部网安局发布两起涉抗日战争网络谣言案例

6 月 5 日，公安部网安局发布两起涉抗日战争网络谣言案例。

案例一：邓某杰散布网络谣言，歪曲抗日战争历史案。

公安机关网安部门工作发现，2025 年 4 月 28 日，网民邓某杰编造虚假的中国共产党领导的军队消灭日军数据，贬低、否定中国共产党在抗日战争中的中流砥柱作用，亵渎国家和民族情感，造成恶劣社会影响。邓某杰到案后，对其发布涉抗日战争网络谣言的违法行为供认不讳。根据相关法律法规，属地公安机关依法对违法行为人邓某杰处以行政处罚。

案例二：张某艺散布网络谣言，歪曲抗日战争历史案。

公安机关网安部门工作发现，2025 年 1 月 18 日，网民张某艺恶意编造“红军资助关东军”等不实信息，否定中国共产党领导下的东北抗日武装率先举起民族抗日大旗的历史事实，歪曲抗日战争历史，造成恶劣社会影响。张某艺到案后，对其发布涉抗日战争网络谣言的违法行为供认不讳。根据相关法律法规，属地公安机关依法对违法行为人张某艺处以行政处罚。（来源：公安部网安局）

2. 2025 年“净网”“护网”专项工作部署会召开

6 月 20 日，2025 年“净网”“护网”专项工作部署会在京召开。会议要求，要坚持以打开路，进一步构筑“净网”工作新格局。要加大打的力

度，紧盯人民群众反映强烈的各类网络乱象，持续依法严打侵犯公民个人信息、网络谣言、黑客犯罪、网络水军、网络黑灰产、网络暴力等突出网络违法犯罪，对重大典型案件要挂牌督办，确保打击质效。要提升打的能力，健全完善“专业+机制+大数据”新型警务运行模式，为高效开展网络线索核查、案件侦办等工作提供有力支撑。要形成打的合力，充分发挥国家网络与信息安全信息通报机制作用，强力推进网络空间安全综合治理，压实互联网企业主体责任，筑牢网络安全防线。

会议要求，要坚持打管衔接，进一步健全“护网”综合治理新体系。要全力保护网络安全，加强关键信息基础设施保护、重要系统安全检测。要全力保护数据安全，加强数据安全问题集中整治、重点行业监督检查，及时整改问题、堵塞漏洞。要全力保护信息安全，加强互联网平台安全监管、人工智能平台安全监管和网络信息内容的全链条监管。（来源：公安部网安局）

3. 陕西西安网警破获一起非法控制计算机信息系统案

6 月 4 日消息，陕西西安网警近日破获一起非法“薅羊毛”案件。两男子一个开发制作非法“薅羊毛”外挂软件出售，一个在网上利用非法“薅羊毛”外挂软件骗取商家优惠券牟利，目前警方已对涉案人员采取刑事强制措施。

西安网警工作中发现有人利用“薅羊毛”软件，伪造虚假网购信息，绕开某电商平台风控，获取新人福利券，以 0.01 元、1.01 元等极低价格批

量下单，套取商家优惠补贴，涉及订单 6 万余笔，造成商家极大经济损失。西安网警迅速开展调查工作。

通过分析，警方掌握了嫌疑人犯罪活动的基本方式，成功抓获涉案嫌疑人王某超，并查获电脑、手机、银行卡等大量作案工具。经查，王某超利用非法外挂软件绕过电商平台风控机制，下单 6 万余次，涉案资金 1000 余万元。

通过对涉案非法外挂软件进行深入研判，警方调取、固定大量证据，线索指向了制作软件的王某，民警随即将嫌疑人抓获归案，现场查获电脑 5 台、手机 24 部、手机卡 64 张等大量涉案物品，同时查获其制作的软件脚本和制作工具。经查，王某自 2024 年 10 月起，制作外挂软件，组建“互联网群组”进行推销及售后服务，引导购买者以“薅羊毛”形式在某平台低价购买商品再转售牟利。

目前，王某超因涉嫌诈骗罪被依法批准逮捕，王某因涉嫌提供侵入、非法控制计算机信息系统程序、工具罪被依法刑事拘留。案件仍在进一步侦办中。（来源：公安部网安局）

4. 安徽网警公布 8 起打击整治网络谣言典型案件

6 月 12 日，安徽网警公布 8 起打击整治网络谣言典型案件。

案例一：2024 年 11 月中旬，网民谢某某为吸引关注，在多个网站上散布“车企收购”等不实信息，并发布利用 AI 软件制作的虚假“股权分布图”，对相关企业正常经营造成负面影响。公安机关已依法对该网民予以行政拘留。

案例二：2025 年 2 月中旬，网民徐某为发泄个人情绪，冒充某车企公司员工，在网上杜撰发布不实信息，并编造“身边就有 3 名同事被 HR 约谈”谣言信息，引发网民关注、热议，对相关企业正常经营造成负面影响。公安机关已依法对该网民予以行政处罚。

案例三：2025 年 4 月上旬，网民周某为吸引关注，网上发布一段外地火灾视频并编发“舒城蜜雪着火了”谣言信息，引发网民关注，造成当地居民恐慌。公安机关已依法对该网民予以行政拘留。

案例四：2024 年 10 月下旬，网民陶某某为发泄个人情绪，多次在网上编发某连锁超市“蔬菜肉类有问题”谣言信息，引发网民关注和对该超市食品安全的担忧，对该超市正常经营造成影响。公安机关已依法对该网民采取刑事强制措施。

案例五：2025 年 1 月上旬，网民陈某为吸引关注，在未经核实的情况下网上编发“前两天濉溪某小区有个小孩往化粪池扔炮竹被炸死了”谣言信息，引发网民关注、热议，造成负面影响。公安机关已依法对该网民予以行政处罚。

案例六：2025 年 1 月下旬，网民宋某为吸引关注，网上编发“发生交通事故，受伤 40 多人”虚假警情，引发网民关注、热议，造成负面影响。公安机关已依法对该网民予以行政处罚。

案例七：2025 年 3 月上旬，网民徐某为吸引关注，网上编发“小吃街有餐饮老板感染艾滋病”谣言信息，引发当地网民关注、热议、恐慌，对相关餐饮商户造成不良影响。公安机关已依法对该网民予以行政处罚。

案例八：2025 年 5 月中旬，网民朱某为吸引关注，网上编发“马上要泄洪了”“大闸水满了，要放水”谣言信息，引发当地网民关注、热议、恐慌，造成负面影响。公安机关已依法对该网民予以行政处罚。（来源：公安部网安局）

5. 上海警方严厉打击涉企舆情敲诈犯罪

6 月 19 日消息，上海警方今年以来依托“砺剑”“净网”系列专项行动，依法严厉打击涉企造谣抹黑、有偿删帖、舆情敲诈等违法犯罪活动。从已侦案件中，上海警方提炼出不法分子对企业实施舆情敲诈的三个步骤。

首先，不法分子会搜集编发负面、不实信息。不法分子通常在短视频平台、社交平台注册账号，以自媒体身份经营积累一定影响力后，打着“舆论监督”旗号，通过网络有针对性搜集目标企业的所谓“负面信息”，随后采取“无中生有”“移花接木”“断章取义”等手段重新拼凑成文后冠以“吸睛标题”发布。这些负面、不实文章一般都滥用极端词汇，刻意制造公众对企业的不满情绪，极易快速引发舆论关注。不法分子舆情敲诈的目标，多为社会关注度高的经济、民生领域的知名企业，尤其是处于上市、融资等关键节点的大型企业。例如，在青浦警方侦办的涉企舆情敲诈案件中，犯罪嫌疑人以发布有关“服务点倒闭”“公司车辆发生重大交通事故”等负面不实信息抹黑企业，进而以此为要挟进行敲诈勒索。

其次，不法分子会利用网络炒作形成舆论压力。不法分子利用其经营的自媒体账号的影响力，编发的涉企负面、不实信息又刻意贴靠社会关注和网络热点，极易在短时间内大量转发评论，形成网络舆情。同时，为了

进一步向目标企业施压，有的不法分子还会雇佣“网络水军”短时间多账号同步炒作负面信息，人为制造舆情发酵假象，逼迫企业主动联系不法分子，花钱息事宁人。例如，在普陀警方侦办的一起案件中，犯罪嫌疑人故意将外地发生的持刀伤人案件“张冠李戴”到某上海公司，暗示是该公司逼迫借款人还款才导致对方报复伤人，该篇文章迅速引发舆情，嫌疑人趁机以信息服务费名义向该公司勒索“公关费”。

最后，不法分子以舆论胁迫敲诈企业索取费用。在负面舆情发酵后，有的不法分子采取直接威胁的方式，要求企业“有偿解决”，明示若不支付“删帖费”就继续发帖放大舆情；也有的不法分子打着“商业合作”旗号，以签署“合作推广”“舆论支持”等服务协议为名间接逼迫企业“付费删帖”，企图为敲诈勒索披上“合法”外衣。例如，在刑侦总队侦办的一起敲诈勒索案中，犯罪嫌疑人发布负面信息后，以寻求协助运营合作的机会为由，逼迫相关公司签订付费合同，达到非法牟利的目的。（来源：公安部网安局）

6. 江西横峰公安网安部门打击低俗直播

6 月 23 日消息，江西横峰公安网安部门近日在工作中发现，5 月 8 日至 14 日期间，若干名本地主播在横峰县某工业园区等地多次组织直播 PK，为博取流量、诱导打赏，竟公然实施“订书机钉肢体”“皮带抽打”“别针穿唇”等极端低俗体罚表演，并恶意传播至粉丝群，造成极其恶劣的社会影响。5 月 14 日，横峰县公安局网安大队依法传唤主要违法行为人鲍某、

刘某、徐某、夏某到案调查。目前，公安机关依据《治安管理处罚法》对4人依法作出行政处罚。（来源：公安部网安局）

7. 辽宁锦州网警侦破一起特大刷单非法经营案，涉案金额9000余万

6月25日消息，辽宁锦州网安部门近日成功侦破一起特大刷单类非法经营案，打掉一个涉及全国6省14市的特大犯罪团伙，涉案金额高达9000余万元，17名主要犯罪嫌疑人已全部抓捕归案。

辽宁锦州公安网安部门在工作中发现，某电商平台大量店铺存在异常交易记录，遂立即组织力量开展深入调查。经查，有一犯罪团伙以“网络兼职”为诱饵，利用社交软件招募刷手，虚构交易流水和虚假好评。该团伙组织严密、层级分明，通过伪造物流信息、虚假购物代刷好评等手段逃避监管。

掌握充分证据后，公安机关精准锁定犯罪窝点分布，并于2025年2月13日在统一指挥下对辽宁省内多个窝点同步实施收网行动，现场查获各类作案工具一批，固定电子证据10万余条。随后，专案组乘胜追击将涉及江西、福建、湖南、湖北、吉林等地的犯罪嫌疑人全部抓捕归案。经查明，该团伙累计为700余家网店提供非法刷单服务，单笔虚假交易金额最高达万元，严重扰乱了正常的市场秩序，损害了广大消费者的合法权益。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办发布中国互联网联合辟谣平台2025年5月辟谣榜综述

6月9日，中央网信办发布中国互联网联合辟谣平台2025年5月辟谣榜综述。5月，网络谣言集中在社会热点事件、公共安全、招考政策、旅游出行等领域，造谣者通过张冠李戴、移花接木等手段，编造灾情汛情或虚假社会事件，扰乱正常社会秩序。

涉公共安全谣言方面，涉灾害事故谣言多发，渲染情绪、制造混乱。5月中旬，多个自媒体账号密集发布“云南德宏州4.5级地震，余震超千次”“芒市地震4.7级”“山西临汾发生4.1级地震”等不实信息，渲染恐慌情绪；新疆伊犁霍城县山洪灾害后，有账号散布“洪水冲入主城区”“牲畜大批死亡”等不实视频，将其他地区洪灾画面与某养殖场病死牲畜处理场景拼凑，严重误导公众；所谓“安徽含山河道泄洪”的视频经核实为捏造，“河南安阳冰雹致小麦颗粒无收”虽拍摄下了当地冰雹天气片段，嫁接的却是虚假结论。此外，个别网民为博取流量，自导自演、虚构事实，扰乱公共秩序。如“百万粉丝网红在成都自杀”事件，当事人为博关注编造戏剧性情节，伪造遗书、操纵评论，消耗社会同情心。

教育、文旅等领域谣言方面，部分账号假冒官方发布，在中考、公共假期等时点散布虚假信息。如“江西南昌2025年中考取消选择题和填空题”谣言，打着“教育部官宣”的旗号，引发家长群体过度担忧；另有部分商家瞄准社会公众对升学备考的关心，声称“中考体测使用‘氮泵’可提升

成绩”“用体考神器考试开挂”，诱导家长购买对青少年身体可能造成伤害的产品。五一假期期间，有自媒体为蹭热点、涨流量，散布“广西漓江断流，游客徒步江底”谣言，实为对往年枯水期画面的恶意剪辑；“五一登顶泰山得3万奖金”“成都6月1日起公路停车位全面免费”等不实信息，误导广大游客，扰乱社会秩序。更有甚者，编造“5·12北川地震遗址收费”等虚假信息，引发公众议论和忧虑。5·12汶川特大地震纪念馆等机构快速回应、澄清谣言，出示免费政策文件，有效回应了网民关切。

针对谣言，各级网信、公安部门协同联动，强化技术监测与溯源打击，合力整治谣言乱象。网信部门公开曝光第六批涉公共政策、突发案事件、社会民生领域网络谣言典型案例，累计处置相关违法违规账号2210个。上文中故意编造“自杀离世”虚假信息的孙某，因涉嫌虚构事实扰乱公共秩序，已被公安机关依法立案调查，其账号被平台无限期封禁。除此之外，深圳警方对编造“深圳发生多车火灾事故”的宋某某、重庆警方对编造“巫溪建机场”的梁某均已依法给予行政处罚。天津、广州等多地开展网络举报辟谣宣传活动，提高公众对网络谣言的辨别能力和防范意识。（来源：网信中国）

2. 国家网络与信息安全信息通报中心通报64款违法违规收集使用个人信息的移动应用

6月18日，国家网络与信息安全信息通报中心通报2025年5月23日至2025年6月11日，检测发现的64款移动应用违法违规收集使用个人信息情况。

（1）10 款移动应用在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理者的名称或者姓名、联系方式、个人信息的保存期限等。例如《星巴克》（版本 3.4.0，微信小程序）、《太平洋咖啡会员》（版本 3.3.0，微信小程序）、《古茗茶饮点单》（版本 6.0.40，微信小程序）。

（2）25 款移动应用隐私政策未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等。例如《黑岩阅读》（版本 4.2.1，微风下载站）、《乐教乐学》（版本 1.0.281，PP 助手）、《听》（版本 2.8.0.008，红旗 EQM5 车载 App）。

（3）14 款移动应用个人信息处理者向其他个人信息处理者提供其处理的个人信息的，未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。例如：《诚通证券》（版本 6.0.3.0，百度手机助手）、《海峡银行》（版本 4.0.0，VIVO 应用商店）、《找朋友》（版本 1.2.3，应用宝）。

（4）2 款移动应用未在征得用户同意后才开始收集个人信息或打开可收集个人信息的权限。例如：《微博 SDK（Android）》（版本 13.10.5，官网）、《太平洋咖啡会员》（版本 3.3.0，微信小程序）。

（5）8 款移动应用未提供有效的更正、删除个人信息及注销用户账号功能；虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内完成核查和处理。例如：《手机游戏联运 SDK》（版本 3.2.3，官网）、《OnewaySdk-Android》（版

本 2.6.3，官网）、《云飞扬 SDK》（版本 1.6.14，官网）、《乌海银行》（版本 5.0.1，华为应用市场）。

（6）5 款移动应用投诉、举报未在承诺时限内受理并处理。例如：《手机游戏联运 SDK》（版本 3.2.3，官网）、《云飞扬 SDK》（版本 1.6.14，官网）、《声音转换 Android SDK》（版本 2.1.2，官网）。

（7）30 款移动应用未向用户提供撤回同意收集个人信息的途径、方式；个人信息处理者未提供便捷的撤回同意的方式。例如：《黑岩阅读》（版本 4.2.1，微风下载站）、《Deep 人工智能 AI》（版本 1.0.7，OPPO 软件商店）、《OnewaySdk-Android》（版本 2.6.3，官网）。

（8）4 款移动应用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。例如：《云听》（版本 2.8.0.008，红旗 EQM5 车载 App）、《畅达金城》（版本 1.2.2，VIVO 应用商店）、《NOWWA 挪瓦咖啡》（版本 5.77.15，微信小程序）。

（9）3 款移动应用处理敏感个人信息未取得个人的单独同意；个人信息处理者处理敏感个人信息的，未向个人告知处理敏感个人信息的必要性以及对个人权益的影响。例如：《厦心健康管理中心》（版本 4.36，微信小程序）、《找朋友》（版本 1.2.3，应用宝）、《本地陌交友》（版本 6.8.1，华为应用市场）。

（10）7 款移动应用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。例如：《黑岩阅读》（版本 4.2.1，微风下载站）、《拓词》（版本 14.23，PP 助手）、《找朋友》（版本 1.2.3，应用宝）。

（11）29 款移动应用未采取相应的加密、去标识化等安全技术措施。例如：《手机游戏联运 SDK》（版本 3.2.3，官网）、《微博 SDK（Android）》（版本 13.10.5，官网）、《Deep 人工智能 AI》（版本 1.0.7，OPPO 软件商店）。

（12）2 款移动应用没有关闭标志或者计时结束才能关闭广告。例如：《戏曲多多》（版本 3.9.1.0，搜狗应用）、《OnewaySdk-Android》（版本 2.6.3，官网）。

（13）6 款移动应用无隐私政策。例如：《SpeechSDK》（版本 1.04，官网）、《天气》（版本 3.01.02.059，红旗 EQM5 车载 App）、《访客端 SDK-Android 端》（版本 3.6_231128，官网）。

2025 年 5 月 29 日通报的国家计算机病毒应急处理中心检测发现的 63 款违法违规移动应用，经复测仍有 28 款存在问题，相关移动应用分发平台已予以下架。（来源：公安部网安局）

3. 重庆大渡口区、巴南区网信办开展违规收集人脸信息整治活动

6 月 3 日消息，重庆市大渡口区网信办近日联合建委、公安、市场监管、检察院对属地某公司涉嫌违法违规处理个人（人脸）信息行为进行联合调查，依法对履行主体责任不到位的某公司作出行政处罚。经查，该公司在售楼处私自安装人像采集设备，在未真实、准确、完整地向个人告知采集人脸信息，以及未取得个人单独同意情况下，累计收集、存储客户信息 1.2

万余条，含人脸信息5000余条，并主要用于与购房人身份信息、中介机构、置业顾问匹配营销，违反《个人信息保护法》《网络数据安全管理条例》等有关规定。大渡口区网信办依据《网络数据安全管理条例》，对该公司作出责令限期整改，给予警告，并处1万元罚款的行政处罚。

6月18日至19日，重庆市巴南区委网信办对物业小区、写字楼、学校、景区、健身房等7个重点场所开展专项检查，整治人脸识别技术应用中的违法违规行为。检查围绕人脸信息采集、使用全流程，发现多项违规操作：采集环节，部分场所未在采集区域设置显著标识，未经用户明示同意擅自采集人脸信息，甚至在未取得监护人同意的情况下采集14岁以下未成年人信息；管理环节，缺乏便捷撤回同意渠道，未对人脸信息进行加密存储和传输，未经用户同意通过互联网传输人脸数据；使用环节，在有其他验证方式情况下，仍强制将人脸识别作为唯一验证途径。针对上述问题，检查组当即下达整改通知书，要求相关单位限期整改到位。（来源：网信重庆）

4. 北京市网信办加强数据安全领域执法工作，依法查处两家违法企业

6月13日，北京市网信办发布2起违反数据安全保护的典型案例。

案例一：北京某科技公司在开展业务过程中，因技术人员缺乏数据安全保护意识，未对后台业务系统的接口配置访问控制和身份认证等安全措施，导致该系统存在未授权访问漏洞，使储存于其中的姓名、身份证号、手机号等个人信息数据暴露于互联网，并被境外IP访问窃取。该公司未依法履行数据安全保护义务，未建立健全全流程数据安全管理制度，相关系

统未采取技术措施和其他必要措施保障数据安全，造成部分个人信息数据遭窃取，违反《数据安全法》第二十七条规定。针对以上违法情况，北京市网信办依据《数据安全法》第四十五条，对北京某科技公司作出警告，并处五万元罚款的行政处罚。

案例二：北京某有限公司在开展业务过程中，为方便系统测试，将ES数据库的9200端口对外开放且未限制访问，导致ES数据库存在未授权访问漏洞，使储存于其中的姓名、手机号等个人信息数据暴露于互联网，并被境外IP访问窃取。该公司数据安全保护意识淡薄，未依法履行数据安全保护义务，未建立健全全流程数据安全管理制度，相关系统未采取技术措施和其他必要措施保障数据安全，造成部分个人信息数据遭窃取，违反《数据安全法》第二十七条规定。针对以上违法情况，北京市网信办依据《数据安全法》第四十五条，对北京某有限公司作出警告，并处五万元罚款的行政处罚。（来源：网信北京）

5. 江西省鹰潭市互联网信息办公室公布三起网信领域典型案例

6月30日，江西省鹰潭市互联网信息办公室公布三起网信领域典型案例。

案例一：某新型材料集团有限公司未履行数据安全保护义务，致视频监控数据被境外黑客窃取。

接上级转办线索，某新型材料集团有限公司所属IP向境外多个IP传输数据，行为异常。经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：该公司未采取相应的技术措施和其他必要措施保

障数据安全，未在开展数据处理活动时加强数据安全缺陷、漏洞等风险监测，导致其所属的视频监控系统多次被境外黑客组织登录并窃取视频监控数据，相关行为违反了《数据安全法》第二十七条、第二十九条规定。鹰潭市网信办依据《数据安全法》、《行政处罚法》等法律法规，责令该公司限期改正，并给予警告。

案例二：某科技有限公司未履行网络安全保护义务，致所属 IP 被黑客远控对外发起攻击。

监测发现，某科技有限公司所属 IP 频繁对外发起 SMB 服务通联，疑似为爆破攻击行为。经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：该公司未采取防范计算机病毒和网络攻击等危害网络安全行为的有效技术措施，未及时处置计算机病毒、网络攻击等安全风险，所属终端感染木马病毒，持续对外发起网络攻击，相关行为违反了《网络安全法》第二十一条规定。鹰潭市网信办依据《网络安全法》、《行政处罚法》等法律法规，对该公司网络安全工作主管人员和直接责任人员开展约谈，并责令限期改正。

案例三：某机关单位网络安全工作责任制落实不力，违规委托第三方运营新媒体账号。

巡查发现，某机关单位长期委托不具备运营资质的第三方运营微信视频和抖音视频账号。经过调查取证、现场问询等工作，查明：该机关单位委托第三方的审批与监管存在漏洞，导致其政务新媒体信息安全防护方面存在缺陷、内容质量与导向存在风险，相关行为违反了《互联网政务应用安全管理规定》第二十五条规定。鹰潭市网信办依据《网络安全法》，联

合市委宣传部依法对该机关单位分管领导、主管人员及直接责任人员开展约谈，并责令限期改正。（来源：网信鹰潭）

（三）通信管理部门治理实践

1. 部省通信管理部门通报侵害用户权益 APP（SDK）

（1）工信部

6 月 26 日消息，工业和信息化部信息通信管理局近日组织第三方检测机构进行抽查，共发现 57 款 APP 及 SDK 存在侵害用户权益行为。上述 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，工业和信息化部信息通信管理局将依法依规组织开展相关处置工作。（来源：工业和信息化部信息通信管理局）

（2）上海

6 月 5 日，上海市通信管理局近日组织第三方检测机构对本市 APP（SDK）进行抽查，共发现 50 款 APP（SDK）存在侵害用户权益行为。上述 APP（SDK）应对存在的问题立即整改，并对该 APP（SDK）个人信息和用户权益保护工作开展全面自评估，自通报之日起 30 日内将整改报告和自评估报告书面报告上海市通信管理局。对未能在限期内完成整改并提交报告的，上海市通信管理局将依法依规予以处理。（来源：上海通信圈）

（3）江苏省

6 月 17 日，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实用工具、旅游出行等类型的 APP、小程序进行检查，并通报相关违

规 APP、小程序主办者限期整改。截至目前，尚有 11 款 APP、小程序未完成整改。请上述 APP、小程序开发运营者在 6 月 18 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）

（4）浙江省

6 月 25 日，浙江省通信管理局通报 2025 年第 5 批侵害用户权益行为的 APP（小程序）。浙江省通信管理局近日组织第三方检测机构对群众关注的网上购物、即时通信等类型 APP、小程序进行检查，书面要求违规 APP、小程序开发运营者限期整改。截至目前，尚有 3 款 APP 及小程序未按要求完成整改。上述 APP 及小程序开发运营者在 7 月 3 日前按有关规定进行整改，整改落实不到位的，浙江省通信管理局将依法依规组织开展相关处置工作。（来源：浙江省通信管理局）

（四）其他部门治理实践

1. 最高法发布利用网络、信息技术侵害人格权典型案例

6 月 12 日，最高人民法院发布利用网络、信息技术侵害人格权典型案例。

案例 1：擅用他人肖像供用户“换脸”，应承担肖像权侵权责任——彭某某诉某软件运营公司肖像权纠纷案

某软件运营公司开发运营一款软件，用于供付费会员使用他人的照片进行面部替换（俗称“换脸”），进而生成面部为该他人的作品。该公司

未经彭某某同意，自行在软件中上架彭某某的肖像供会员“换脸”并牟利。审理法院认为，自然人的肖像权受法律保护。未经自然人同意，他人不得制作、使用、公开自然人的肖像。自然人的肖像权受到侵害的，有权要求停止侵害、消除影响、赔礼道歉，并可以要求赔偿损失。某软件运营公司未经彭某某授权同意，以营利为目的使用含有彭某某肖像的照片、视频，侵害了彭某某的肖像权，应承担相应民事责任。审理法院判决某软件运营公司向彭某某赔礼道歉并赔偿损失3千元。

案例2：利用网络账号“挂人”并号召粉丝投诉和网暴，构成名誉权侵权——陈某与孟某等人名誉权纠纷案

涉案账号系某知名相声演员的粉丝超话账号（即粉丝基于对该演员的关注聚集在该账号中，形成特定的讨论组），由孟某手机绑定、高某身份信息实名注册，孟某、高某对该账号共同管理使用。陈某观看前述相声演员的演出后通过自己的社交账号发布观后感，因意见不合与该相声演员的粉丝在网络社交平台发生争执。涉案账号发布多条信息，将陈某的社交账号等个人信息置顶公示（俗称“挂人”），列出陈某的多条与粉丝争执的消息网址链接，并置顶公开投诉模板，号召该相声演员的其他粉丝投诉陈某的社交账号。陈某的社交账号还收到众多粉丝的私聊辱骂。审理法院认为，陈某仅是针对某相声演员的演出发表观后感，后与个别粉丝发生言语争执。涉案账号借维护相声演员声誉为由，号召其他粉丝投诉陈某社交账号，持续对其网暴，严重侵犯陈某的名誉权。孟某、高某作为账户的共同使用人，应当对涉案账号的行为承担相应责任。审理法院判决孟某、高某删除涉案相关信息、公开赔礼道歉，并赔偿陈某损失。

案例 3：非法买卖人脸信息情节严重的，构成侵犯公民个人信息罪——徐某、李某侵犯公民个人信息案

2021 年 6 月起，徐某通过其社交账号自他人处购买约 130 套公民个人身份信息（包括公民的动态人脸图等信息）和 1 套软件。在未经游戏账号所有人同意的情况下，徐某用购买的公民个人信息和该软件解封多人的游戏账号，还对外有偿出租该软件、出售公民个人信息给社会人员，用于解封社交账号、游戏账号。徐某获利约 6 千元。2021 年 8 月起，李某通过使用徐某提供的软件，采取人脸识别、完成观看任务视频等方式为他人解封社交账号，还将从多个渠道购进的公民个人信息（包括人脸照片、视频等）转卖，获利约 3 万元。徐某、李某被检察机关提起公诉。审理法院认为，徐某、李某违反国家有关规定，非法获取、出售或提供公民个人信息，情节严重，其行为均已构成侵犯公民个人信息罪，应依法惩处。两人归案后如实供述犯罪事实，自愿认罪，积极退缴违法所得，依法可以从轻处罚。审理法院判决李某犯侵犯公民个人信息罪，判处有期徒刑九个月，并处罚金人民币 3 万元；徐某犯侵犯公民个人信息罪，判处有期徒刑六个月，并处罚金人民币 6 千元；违法所得及手机、电脑等作案工具予以没收。

案例 4：非法获取他人家庭监控摄像头控制权，情节严重的，构成非法控制计算机信息系统罪——韩某非法控制计算机信息系统案

2020 年，韩某通过聊天软件，非法获取他人家中网络监控摄像头账号、密码等信息，添加到自己手机或电脑上，非法获取他人家庭监控摄像头的控制权限，远程观看他人家中画面，并将部分画面截图保存。截至 2022 年 5 月，韩某登录并控制的监控摄像头共 193 个。韩某被检察机关提起公诉。

审理法院认为，非法控制计算机信息系统罪是指违反国家规定，对计算机信息系统实施非法控制，情节严重的行为。在案证据证实，2020 年至 2022 年 5 月，韩某非法控制监控摄像头设备 193 个，窥探他人隐私，保存了大量其窥探到的他人家中画面影像的截图，属于情节特别严重，其行为构成非法控制计算机信息系统罪。最终判决：韩某犯非法控制计算机信息系统罪，判处有期徒刑三年一个月，并处罚金人民币 1.3 万元。（来源：最高人民法院新闻局）

2. 审计署通报 6 省市 147 个数源部门拒绝数据共享申请或提供失效数据

6 月 24 日，第十四届全国人民代表大会常务委员会第十六次会议，审计署报告《国务院关于 2024 年度中央预算执行和其他财政收支的审计工作报告》。报告指出，2024 年，审计署重点审计的 18 省市在数据资源利用和公共资源交易平台运行方面主要存在 2 方面问题。

一是数据资源底数不清、共享应用存在梗阻。至 2024 年底，9 省市 1091 个政府部门的信息系统未按要求编制政务数据目录，9717 个政府部门已编制的数据目录因未关联信息系统、未注明共享条件等，不符合规范要求，降低数据赋能作用。6 省市的 147 个数源部门以各种理由拒绝其他部门正当共享申请，或提供已过时失效数据等共计 577 项。5 省市的 134 个用数部门 375 个服务事项“应用未用”相关数据，相关地区在办理公积金缴存、中小学入学等民生事项时，仍需提交纸质材料或手工填报上传 10 余项证明材料，影响群众获得感。

二是公共资源交易平台体系不健全、监管不严格、收费不规范。在平台整合共享方面，5 省 130 个县级平台未按要求整合至市级，其中 7 县还违规新设 7 个平台。部分平台对专家信息共享不充分，一方面地方难以获取异地优质专家资源，另一方面造成“污点”专家继续参评。如天津有 43 人 2021 年至 2024 年 5 月被住房城乡建设、财政等部门处罚期间，仍参与了其他部门 292 个项目评标。在平台监管方面，5 省 6 个平台交易审查不严，363 项交易存在违规设置不合理限制性条件等问题，加剧行业垄断。7 省 10 个平台和 8 省部分行政监督部门未有效监测线上交易，部分项目涉嫌围标串标。4 省 5 个平台对存在国有资产挂牌价格畸低等异常交易情况的 70 个项目，未按要求向行政监督部门报告，相关国有权益面临损失风险。在服务收费方面，9 省 47 个平台借助行政垄断地位，直接或协助第三方企业违规收费等 7.47 亿元。如吉林省平台 2022 年至 2024 年 5 月，违规允许其建设厂商向在该平台开展电子保函业务的金融机构，按收入 45%至 50%的比例收取分成 2196.3 万元。（来源：国家审计署）

3. 江苏南京中院审结一起数据侵权案，判赔 3000 万元

6 月 12 日，南京市中级人民法院对“小旺神”数据侵权案作出一审判决，依法裁定“小旺神”相关公司立即停止侵权行为，并赔偿淘宝、天猫、淘软三家公司 3000 万元。该案被称为《数据安全法》实施后的“数据资源法治第一案”。

淘宝天猫等三原告主张对其搜集、整理、加工的各类数据享有数据权益和竞争性权益，通过与用户签订一系列协议，获得用户授权取得了相关

数据的“持有使用权”，经过计算、统计、分析而形成的诸如交易数据、营销数据、浏览数据、收藏数据等经营数据，享有该类数据的“加工使用权”，且该类数据经过访问限制和技术防护手段等加密处理，不为公众所知悉，应当认定为反不正当竞争法意义上的经营信息商业秘密。

淘宝天猫认为被告一方面通过“小旺神”的“指数一键还原”功能，寄生于原告的“生意参谋中，增加被告访问量，引流用户至被告网站；另一方面，通过破坏性技术手段“监控”获取相关经营数据，实质性替代“生意参谋”，获取流量利益和直接经济利益，给原告造成了难以弥补的巨大损失，遂索赔3000万元等。

南京中院审理认为，淘数公司利用了相关技术手段获得了与淘天平台真实数据高度近似的数据。该功能将平台用户的真实数据隐私、平台的真实经营数据商业秘密，完整地甚至超过“生意参谋”查询次数及数量的限制对外披露，突破了“生意参谋”的数据安全底线，颠覆了“生意参谋”的商业模式，破坏了数据安全与数据利用的平衡，直接损害了淘天平台利益及用户权益。

小旺神“指数一键还原”功能以免费引流破坏“生意参谋”商业模式的代价提升了小旺神”的不当竞争优势等，违反了反不正当竞争法第九条的规定，侵害了原告的经营信息商业秘密。小旺神的“竞品监控”功能、“素材下载”功能等违反了反不正当竞争法第十二条的规定，构成不正当竞争。

2025年6月，南京中院作出一审判决，适用两倍惩罚性赔偿，全额支持了原告3000万元等。（来源：新华日报）

4. 辽宁多家银行因网络安全与数据安全问题被罚

6 月 17 日，中国人民银行辽宁省分行对部分金融机构的网络安全与数据安全问题进行了处罚，主要针对金融机构在数据安全管理、网络安全防护以及客户信息保护等方面的违规行为。

其中，交通银行股份有限公司辽宁省分行存在：（1）未按规定落实网络安全相关管理规定；（2）未按规定落实数据安全相关管理规定；（3）违反信用信息采集、提供、查询及相关管理规定；（4）未按规定履行客户身份识别义务等违法行为。

中国光大银行股份有限公司沈阳分行存在：（1）未按规定落实反电信网络诈骗相关管理规定；（2）未按规定落实网络安全相关管理规定；（3）违反信用信息采集、提供、查询及相关管理规定；（4）未按规定履行客户身份识别义务等违法行为。

抚顺银行股份有限公司存在：（1）未按规定落实反电信网络诈骗相关管理规定；（2）未按照规定落实数据安全相关管理规定；（3）违反信用信息采集、提供、查询及相关管理规定；（4）未按规定履行客户身份识别义务等违法行为。（来源：中国人民银行）

5. 上海市静安区检察院办理一起非法获取计算机信息系统数据罪案

6 月 17 日消息，上海市静安区检察院近日办理一起非法获取计算机信息系统数据罪案。

A公司成立于2018年，是一家提供信息网络服务的技术公司，自主研发一款P系统用于整合分析相关数据，并以收费方式提供服务。2023年6月，A公司监测系统突发异常，P系统在48小时内遭高频访问6万余次，约有1700余万条某专业领域相关重要数据被非法下载。A公司系统被迫关停，数据服务业务陷入瘫痪。2023年7月，A公司报案。经立案侦查，侦查人员发现Y公司存在重大作案嫌疑。同年8月25日，该公司负责人杨某某自动投案。然而，其到案后拒不供述，辩称已获得授权。

鉴于本案涉及计算机信息系统犯罪，专业性强，静安区检察院依法提前介入。经初步侦查查明，犯罪嫌疑单位Y公司成立于2019年，犯罪嫌疑人杨某某系法定代表人。2023年5月，Y公司中标了M公司“某某规划项目”，合同总价为人民币25万元（以下币种均为人民币）。在开展项目合作期间，M公司向A公司借用P系统临时账号，供Y公司查询上述项目的相关数据。杨某某在使用临时账号期间，发现该系统某些专业领域数据全面、细致，资源蕴含巨大经济价值，遂指示公司员工非法使用爬虫软件抓取、下载大量数据。经鉴定，爬取数据量高达1800余万条。

2024年6月3日，案件移送至静安区检察院审查起诉。在审查过程中，检察官在回溯Y公司员工孙某某与负责人杨某某的聊天记录过程中发现，早在2022年7月，杨某某就曾与A公司接触，明知A公司系统的商业性质，也明知系统数据属于具有高度市场价值的商业资产。为查明“授权是否等于合法”的问题，检察官开展自行补充侦查，通过询问第三方技术公司工作人员，依法询问被害单位业务负责人、调取被害单位提供的书证、充分听取第三方鉴定机构的意见等，查明关键两点事实：一是权限限制，A

公司提供的临时测试账号明确设限（登录时间、查询条数、单次导出数据量等），但Y公司却在48小时内高频访问，爬取1800余万条数据，远超临时账号的授权范围；二是技术突破，A公司通过密码验证、下载范围、条数速度等对系统数据设置反爬措施，并且即使是付费用户也仅能获取页面数据，而杨某某公司利用爬虫绕过防护，直接窃取系统底层原始数据。杨某某看似通过合法渠道实现了账户登录，却在使用账号过程中，以技术手段突破授权边界，利用爬虫软件将导出权限提升覆盖至对全库底层原始数据的获取，该行为严重违背被害单位的授权意志、范围，本质上是超越授权非法获取信息数据。

2025年6月3日，静安区法院以非法获取计算机信息系统数据罪作出一审判决，判处Y公司罚金五万元；判处杨某某有期徒刑三年，缓刑三年，并处罚金三万元。（来源：静安检察）

6. 浙江省杭州市滨江区检察院发布一起典型非法控制计算机信息系统案

6月26日，浙江省杭州市滨江区检察院发布一起典型非法控制计算机信息系统案。

施某某于2019年前后，开发出某云解析软件。通过使用该软件可以在未经授权将视频上传至互联网公司的服务器，以此“省服务器的存储、网络的带宽、流量的费用”。互联网上租用的服务器费用，根据服务器的配置、容量、流量、带宽的不同，会有不同的价格。视频网站的流量特别巨大，架设视频网站流量费用非常高。因此，施某某认为有利可图，开始在

社交群里兜售云解析软件。2020 年 6 月，郭某某加入施某某，并由施某某更新维护软件，郭某某招募客户。2022 年 7 月，由于原解析域名被封，王某某向两人提供多个子域名用于解析，帮助软件正常运行。

直至 2023 年 6 月，被害某互联网公司发现服务器被人非法控制，造成大量流量费用亏损，故向公安机关报案。经统计，截至 2023 年 8 月案发，施某某、郭某某二人通过售卖上述软件获利 171 万余元。2025 年 5 月底，经滨江区检察院提起公诉，滨江区法院审结本案，三名被告人被判处有期徒刑 4 年至有期徒刑一年六个月、缓刑两年不等，并处罚金。（来源：杭州滨江检察）

境内观察三：人工智能安全专题

导读：6 月，中央网信办发布“清朗 • 整治 AI 技术滥用”专项行动第一阶段工作成果。各地网信部门多措并举，扎实推进，积极履行属地管理责任等。上海市网信办联合上海市市场监督管理局及相关行业主管部门在本年度继续开展“亮剑浦江 • 2025”个人信息权益保护专项执法行动，专项行动聚焦三大领域八项重点任务，“抵制 AI 滥用”是本年度治理重点之一。广东省委网信办发布“清朗 • 整治 AI 技术滥用”专项行动阶段性成果。

北京市通州区人民检察院提起公诉的北京市首例利用人工智能侵犯著作权刑事案件获法院判决支持，4 人利用人工智能侵犯著作权被判刑。

利用 AI 炮制“政府工作人员因买方便面被通报”网络谣言，炮制人被属地公安机关依法采取刑事强制措施。

关键词：人工智能技术滥用；侵犯著作权；网络谣言

1. 中央网信办发布“清朗·整治 AI 技术滥用”专项行动第一阶段工作成果

6 月 20 日，中央网信办发布“清朗·整治 AI 技术滥用”专项行动第一阶段工作成果。

自 2025 年 4 月启动以来，中央网信办聚焦 AI 换脸拟声侵犯公众权益、AI 内容标识缺失误导公众等 AI 技术滥用乱象，深入推进第一阶段重点整治任务。第一阶段累计处置违规小程序、应用程序、智能体等 AI 产品 3500 余款，清理违法违规信息 96 万余条，处置账号 3700 余个，各项工作取得积极进展。

各地网信部门多措并举，扎实推进，积极履行属地管理责任。北京网信办开设 AI 技术滥用治理举报渠道，形成“用户标记—平台核查—联合处置”工作模式，处置有关举报 26 篇。上海网信办推动标识要求落地示范，组织开展 4 场法规宣贯和专题交流，覆盖企业 400 余家，属地内重点企业已基本完成显式标识规范上线。浙江网信办加大对属地 AI 应用和网站平台的督导力度，各平台共拦截清理各类违法违规信息及提问 2550 万余条。江苏网信办加强统筹协调，联合省通信管理局等部门排查 AI 风险域名 163 个，封堵和取消接入域名 18 个。天津网信办采用“人工+技术”方式，开展大模型安全监测，通报 4 批次 14 个风险问题。

重点网站平台积极履行主体管理责任，加强 AI 技术滥用源头治理。在处置违规 AI 产品方面，腾讯规范应用程序管理，提高准入门槛，优化巡查机制，驳回、处置违规小程序、应用程序等共计 570 余款。在清理违规 AI

产品教程和商品方面，微博通过策略识别、用户举报等多渠道审核，累计处置违规内容4800余条，并公布典型案例。在加强训练语料管理方面，通义平台围绕数据生命周期建立安全管理体系，在数据采集、训练、使用等阶段加强训练语料管理。在强化安全管理措施方面，抖音建立“红蓝对抗”机制，模拟攻击案例，修复潜在安全漏洞，优化模型对虚假信息的识别能力。在落实内容标识要求方面，阿里、快手、稀宇等重点平台积极推进元数据隐式标识落地落实。在防范重点领域安全风险方面，小红书在模型后置训练阶段输入专业领域数据，提升模型对医疗、金融、未成年人等重点领域问题的理解能力。（来源：网信中国）

2. .北京首例利用AI侵犯著作权案审结，4人利用AI侵犯著作权被判刑

6月13日，北京市通州区人民检察院提起公诉的北京市首例利用人工智能（AI）侵犯著作权刑事案件获法院判决支持。通过审理，法院认定被告单位福州市某电子商务有限公司犯侵犯著作权罪，判处罚金10万元；被告人罗某某、姚某某等4人因犯侵犯著作权罪，分别被判处有期徒刑一年六个月至缓刑，并处罚金6万元至2.5万元不等。

2024年5月27日，张某报警称其画作被人盗用，牟取利益。经查，被告人罗某某、姚某某等4人，于2024年3月至7月间，共谋从互联网平台下载他人美术作品后，使用开源软件生成侵权图片，制成拼图对外销售。经比对，被告人销售的多类拼图图样与张某、刘某某等多名著作权人享有

著作权的美术作品关键元素一致，属于实质相同。经查，上述各被告人于涉案期间共售出侵权拼图产品3000余件，非法经营数额共计27万余元。

检察机关还查明，罗某某实际控制的福州市某电子商务有限公司除为同案姚某某生产拼图外，另存在其他合法生产经营业务。办案人员通过查明公司实际经营情况，明确涉案公司参与复制发行他人美术作品犯罪活动体现单位意志，相关违法所得用于公司生产经营，且公司并非以实施犯罪为主要活动，后依法追加单位犯罪。2025年5月，北京市通州区人民检察院对罗某某、姚某某等4名被告人提起公诉，同时对生产侵权拼图的福州市某电子商务有限公司追加单位犯罪，一并提起公诉。据此，法院一审作出上述判决。（来源：法治日报）

3. 广东深入开展“清朗·整治AI技术滥用”专项行动取得阶段性成效

6月16日消息，广东省委网信办发布“清朗·整治AI技术滥用”专项行动阶段性成果。

（1）聚焦重点平台，压实主体责任

广东省委网信办制定专项行动工作方案，建立政企直联机制，深入指导华为、腾讯、网易、夸克、OPPO、vivo、荣耀、唯品会、金山办公、迅雷等20余个重点平台集中开展专项治理，围绕违规AI产品宣推、训练语料管理不严、内容标识要求落实不力、安全审核措施薄弱等重点风险问题，深入开展自查自纠，集中清理“一键脱衣”、未经授权的人声或人脸克隆编辑等违规AI功能和应用，严厉打击违规售卖AI账号、教程及传授技术

规避手段、利用 AI 技术刷量涨粉、虚假互动、恶意引流等违法违规行为。截至目前，各重点网站平台拦截清理售卖违规 AI 产品教程或商品、假冒仿冒、不当营销等信息 8260 余条，处置违规账号 470 余个。

广东省委网信办充分发挥广州、深圳以及横琴等地大模型服务中心作用，靠前指导属地企业建立健全大模型安全体系，服务企业高效开展大模型上线合规工作。截至目前，已完成 66 款大模型备案，17 款应用登记。对 6 款未履行上线合规手续、存在违规风险的 AI 应用依法约谈并督促整改。

（2）聚焦重点环节，强化全链管理

广东省委网信办指导腾讯应用宝、微信小程序、华为应用市场、OPPO 软件商店、vivo 应用商店等属地重点应用程序分发平台严格落实安全管理责任，建立健全“事前、事中、事后”全链条管理体系。强化“事前”准入把关，加大 AI 服务和应用上架审核力度，重点核验相关应用主体算法备案、大模型备案等资质。强化“事中”巡查整改，优化专项巡查机制，对未履行大模型备案或登记程序、提供不合规功能、未按要求标识等违规 AI 服务的 APP 及时采取限期整改、下架等措施处置。强化“事后”复核检查，结合本次专项整治重点，采取“人工+技术”巡查手段对在架应用程序开展复核，持续畅通用户投诉举报渠道，发现问题及时督促主体整改。专项行动开展以来，应用程序分发平台审核驳回存在违法违规内容、未落实内容标识要求、未提供有关资质等问题的小程序及 APP 共 760 余款，巡查发现并整改处置违规小程序及 APP 共 350 余款。

（3）聚焦重点领域，筑牢安全屏障

广东省委网信办加强对医疗、金融、教育以及涉未成年人等重点领域的AI服务应用的督导，要求平台根据行业领域特点针对性完善安全审核和管控措施，严防“AI处方”“诱导投资”“低俗恶俗”等不当回答，避免对病人患者、中老年人、学生等群体产生错误引导。加强生成合成内容标识管理，督促属地AI服务提供者按照规定在生成合成内容及文件元数据中按要求添加标识，确保生成合成数据信息标识可见、来源可溯；督促内容传播平台陆续推动“虚构内容请谨慎识别”“疑似生成合成内容”等AI生成内容标识选项提示上线，引导形成作者主动声明、有效提示用户辨别相关内容的社区氛围。

在第二阶段工作中，广东省委网信办将聚焦AI技术制作发布谣言、不实信息、色情低俗内容等突出问题，持续深入开展专项整治，切实提高全省AI治理水平，促进广东AI技术产业安全发展。（来源：网信广东）

4. AI智能体对话存在低俗擦边内容，筑梦岛APP被上海市网信办依法约谈

因近期有媒体报道,筑梦岛APP等AI聊天软件存在虚拟角色互动生成低俗内容等问题，经核实属实，6月19日，上海市网信办依法约谈筑梦岛APP运营企业主要负责人，要求平台立即整改，健全AI生成合成内容审核机制，提升技术把关能力，加强涉未成年人不良内容的整治清理，切实落实未成年人网络保护义务。企业负责人表示，将按照约谈要求，对照问题举一反三、全面整改。（来源：网信上海）

5. 上海市网信办对一批拒不整改的生成式人工智能服务网站予以立案处罚

6 月 24 日消息，上海市网信办联合上海市市场监督管理局及相关行业主管部门在本年度继续开展“亮剑浦江·2025”个人信息权益保护专项执法行动，专项行动聚焦三大领域八项重点任务，“抵制 AI 滥用”是治理重点之一。

上海市网信办在专项行动中发现，部分对外提供生成式人工智能服务功能的网站，未按法律要求开展安全评估工作、未采取必要的安全措施防范违规信息生成、未采取限制措施防止生成式人工智能功能被滥用，导致相关生成功能侵犯个人信息权益、产出“开盒”“洗钱”等违法违规内容、生成色情低俗图片等信息内容，存在较大安全风险。上海市网信办督促企业自行下线相关功能，在通过安全评估后方可重新上线。上海市网信办“回头看”巡查发现，在未通过安全评估、未采取必要安全防护措施等情况下，被要求下线的 3 家企业自行重新上线存在安全风险的生成式人工智能功能。上海市网信办依法约谈企业，进行严肃批评，要求全面整改，并依法对涉事企业进行立案查处。其中，典型问题有：

（1）生成侵害他人个人信息权益的违规信息。个别企业未按照《个人信息保护法》《互联网信息服务深度合成管理规定》等法律法规要求，提示用户在编辑他人生物识别信息时，应依法告知被编辑个人并取得其单独同意。如某网站在未取得被编辑个人同意的情况下，克隆其声纹信息并进行语音合成提供其他用户使用。

（2）生成侵犯他人名誉权、隐私权等合法权益的违规信息。个别企业未采取必要措施防止用户生成侵犯他人名誉权、隐私权等合法权益的信息。

如某网站根据输入信息，可生成包含公众人物形象的虚假图片；某网站可根据用户要求生成“开盒教程”“他人隐私信息曝光教程”等违规内容。

（3）生成色情、暴力等法律法规禁止的违规信息。个别企业未按照《网络安全法》《生成式人工智能服务管理暂行办法》等法律法规要求，在平台出现违法违规内容时及时采取停止生成、停止传播、消除等措施。如某网站依据输入信息，可生成色情、暴力等有害图片；某网站根据需求，可生成具有明显“性暗示”的文字信息。（来源：网信上海）

6. 利用 AI 炮制“政府工作人员因买方便面被通报”网络谣言，曹某林被依法采取刑事强制措施

6 月 24 日消息，近日网上流传一份通报，称“泰州姜堰顾高镇政府办公室两名干部张某某、李某某在三令五申严禁违规吃喝、厉行节约反对浪费的纪律要求下，未能严于律己、以身作则，在镇政府周边一便利店消费方便面 2 份，行为逾越了公职人员的廉洁规范，造成了不良影响，予以通报批评”，引发大量网民关注和讨论。经属地核查，相关内容完全虚假，顾高镇政府从未发布类似通报，镇政府工作人员也无文中提到的“张某某（男，31 岁）、李某某（女，29 岁）”，也不存在相关便利店。

公安网安部门查明，曹某林（男，28 岁）在看到“全党开展深入贯彻中央八项规定精神学习教育”有关新闻后，为蹭热点、博眼球、吸引流量，利用 AI 工具炮制了相关谣言，引发大范围传播扩散，严重扰乱公共秩序。目前，曹某林已被属地公安机关依法采取刑事强制措施。（来源：公安部网安局）

境外前沿观察：月度速览十则

导读：6 月，境外国家和地区在人工智能、网络安全、数据安全等方面的政策法律和热点事件持续发生。

人工智能方面，七国集团领导人发布声明，指出在确保尊重人权、隐私、公平问责等的前提下，共同推进公共部门人工智能部署，提升公共服务质量、增强企业与民众福祉，同时提高政府运作效率。美国国会议员提出《禁用敌对人工智能法案》，禁止联邦机构使用由外国对手控制的人工智能技术。

网络安全方面，欧盟理事会通过修订后的网络安全危机管理蓝图。该蓝图是指导各成员国提升网络安全事件准备、检测及响应能力的重要纲领。美国总统特朗普签署《维持加强国家网络安全的特定努力并修订第 13694 号行政命令和第 14144 号行政命令》的行政命令，对往届政府的网络安全政策进行部分调整。

数据安全方面，英国《数据（使用与访问）法》被国王签署成为法律，旨在规范客户数据和业务数据的访问权限，建立数字验证服务框架，完善国家地下资产登记制度，并对出生和死亡登记、数据保护与隐私等领域提出新的监管要求。欧盟委员会发布《执法部门有效合法获取数据路线图》，为欧盟执法部门提供有效且合法的数据获取途径。美国总统特朗普签署《关于进一步延长 TikTok 执法宽限期》行政命令，将 TikTok 执法宽限期延长至 2025 年 9 月 17 日。

关键词：人工智能；网络安全；数据安全

1. 欧盟委员会制定国际数字战略

6 月 5 日,欧盟委员会制定国际数字战略。该战略旨在提高欧洲竞争力,推动以欧洲及其合作伙伴安全为重点的数字议程，并塑造全球数字治理和标准。战略核心内容包括:

一是加强合作伙伴网络。通过部长级贸易和技术委员会、数字伙伴关系和数字对话等形式，与全球伙伴建立合作。计划扩大其全球伙伴网络，深化现有合作关系，并建立新的数字伙伴关系和对话。与伙伴国家合作，推动政策协调、安全连接和创新投资。

二是确定优先合作领域，主要包括：（1）安全和可信的数字基础设施，推动 5G/6G 网络、海底电缆、卫星连接等基础设施的部署；（2）人工智能、半导体、量子技术等新兴技术领域的合作和标准化；（3）网络安全，加强全球网络安全合作，打击网络犯罪，提升关键基础设施的网络安全弹性；（4）数字身份和数字公共基础设施，推广欧盟的数字身份钱包和互操作性框架；（5）在线平台，推动保护儿童在线安全、消费者保护和公平竞争。

三是推动全球数字治理，继续通过多边和多利益相关者的方式，推动全球数字治理。积极参与联合国全球数字契约的实施，并支持开放互联网架构。利用标准化体系，在关键数字技术的国际标准制定中发挥更大影响力。（来源：欧盟委员会）

2. 欧盟理事会通过修订后的《网络安全危机管理蓝图》

6 月 6 日，欧盟理事会通过修订后的《网络安全危机管理蓝图》，是指导各成员国提升网络安全事件准备、检测及响应能力的重要纲领。该蓝图在 2017 年发布的蓝图基础上，进一步纳入近期通过的重要立法，如《NIS2 指令》和《网络团结法》。该蓝图旨在通过强化欧盟现有网络、促进成员国及相关主体间合作、消除既有障碍，应对日益复杂的网络威胁形势。

蓝图强调，数字技术与全球互联互通是欧盟经济增长与竞争力的基石。然而，日益数字化和互联的社会也加剧了网络安全事件与网络攻击的风险。混合型攻击行动和网络攻击可能直接影响欧盟的安全、经济和社会。尽管成员国在应对网络安全事件和网络危机中承担首要责任，但大规模事件引发的破坏可能超出单个成员国的应对能力，或对多个成员国产生连锁影响。鉴于此类事件可能演变为全面危机，扰乱欧盟内部市场运行或造成重大公共安全风险，从技术、行动和政治层面开展合作对有效危机管理至关重要。

为明确界定“大规模网络安全事件”和“欧盟层面网络危机”，蓝图清晰阐释危机管理框架的触发条件，明确欧盟层面各网络主体与机制的职责分工——包括欧盟网络安全局和欧洲网络危机联络组织网络。蓝图还强调网络危机管理中军民协同的重要性，提出在必要时通过强化信息共享机制，与北约等组织深化合作。最后，文件设立专门章节探讨灾后恢复机制建设，着力推动成员国间网络安全经验教训的交流共享。（来源：欧盟理事会）

3. 欧盟委员会发布《执法部门有效合法获取数据路线图》

6 月 24 日，欧盟委员会发布《执法部门有效合法获取数据路线图》，旨在为欧盟执法部门提供有效且合法的数据获取途径。该路线图是欧盟今年 4 月公布的内部安全战略“保护欧盟”的重要成果之一。

路线图重点关注六大领域：（1）数据留存。欧盟将于 2025 年开展影响评估，旨在更新数据留存规则；（2）合法拦截。为实现跨系统和司法管辖区取证，欧盟委员会拟于 2027 年前探索完善数据合法拦截的跨境合作机制，涵盖部门间协作及部门与服务提供商合作；（3）数字取证。执法人员与司法部门需具备分析保存电子设备数字证据的能力。欧盟委员会将联合欧洲刑警组织协调开展数字取证技术需求差距分析，并通过欧盟资金和公私合作支持取证工具研发；（4）解码技术。欧盟委员会将于 2026 年出台加密技术路线图，评估执法部门合法访问加密数据的解决方案；（5）标准化建设。欧盟委员会将联合欧洲刑警组织、行业利益相关方、专家等，制定聚焦数字取证、合法披露与合法拦截的欧盟内部安全标准化实施方案；（6）执法领域的人工智能解决方案。至 2028 年，欧盟委员会将推动开发部署人工智能工具，协助执法部门合法高效处理海量查获数据，提升数字证据筛选分析效率。（来源：欧盟委员会）

4. 七国集团领导人发布声明，促进人工智能和量子技术发展

6 月 17 日，七国集团领导人发布声明，促进人工智能和量子技术发展。

促进人工智能繁荣方面，声明主要内容包括：（1）推动公共部门人工智能应用。在确保尊重人权、隐私、促进透明、公平问责的前提下，共同

推进公共部门人工智能部署，提升公共服务质量、增强企业与民众福祉，同时提高政府运作效率；（2）以人工智能促进经济繁荣。支持中小微企业在尊重个人数据和知识产权的前提下应用开发人工智能技术，增强其效率、生产力与竞争力；（3）构建面向未来的人工智能劳动力体系。为应对人工智能驱动的转型，将落实 2024 年 G7《以人为本安全可信人工智能职场应用行动计划》，帮助劳动者应对人工智能技术转型，制定自愿性最佳实践指南等；（4）解决人才短缺问题，确保机会平等。通过鼓励女性和全球化进程中的弱势群体参与科学、技术、工程和数学（STEM）教育，提高女性在各级人工智能人才库中的占比，缓解人才短缺并确保平等机会。

促进量子技术发展方面，声明主要内容包括：（1）促进对量子科学和技术的公共和私人投资；（2）促进量子技术在各个领域的有益应用的开发和采用；（3）支持合作伙伴之间建立开放公平的市场环境和值得信赖的生态系统；（4）促进对量子技术的信任；（5）加强值得信赖的国家测量机构间的合作；（6）提高对不同行业量子技术相关风险的理解。（来源：欧盟委员会）

5. 美国总统特朗普签署《维持加强国家网络安全的特定努力并修订第 13694 号行政命令和第 14144 号行政命令》的行政命令

6 月 6 日，美国总统特朗普签署《维持加强国家网络安全的特定努力并修订第 13694 号行政命令和第 14144 号行政命令》的行政命令，对往届政府的网络安全政策进行部分调整。

该命令修正了奥巴马与拜登时期行政令（14144 号与 13694 号）中存在的不合理条款，主要举措包括：（1）指示联邦政府推进安全软件开发；（2）要求各部门机构加强边界网关安全以抵御网络互联劫持攻击；（3）要求各部门机构部署后量子加密技术以防范基于下一代计算架构的威胁；（4）强制采用最新加密协议标准；（5）将人工智能网络安全重心转向漏洞识别管控，摒弃审查导向；（6）推行技术化网络安全政策实施手段，包括制定机器可读的政策标准，建立“物联网”设备信任标识体系，确保美国家庭智能设备符合基础安全工程准则；（7）严格限定网络制裁仅针对境外恶意行为体，防止该机制被滥用于打压国内政治对手，并明确选举相关活动不适用网络制裁；（8）剔除与网络安全核心使命无关的越权条款，废止此前要求为非法移民颁发政府数字身份证的规定，该政策存在福利欺诈等系统性滥用风险等。（来源：美国白宫）

6. 美国总统特朗普签署《关于进一步延长 TikTok 执法宽限期》行政命令

6 月 19 日，美国总统特朗普签署《关于进一步延长 TikTok 执法宽限期》行政命令，将原定于 2025 年 4 月到期的 TikTok 执法宽限期进一步延长至 2025 年 9 月 17 日。在此期间，司法部不得采取任何行动来执行《保护美国人免受外国对手控制应用程序法》，并禁止对 TikTok 及其他“外国对手控制应用”的分发、维护、更新行为施加处罚。（来源：美国白宫）

7. 英国《数据（使用和访问）法》被国王签署成为法律

6 月 19 日，英国《数据（使用与访问）法》被国王签署成为法律。该法旨在规范客户数据和业务数据的访问权限，建立数字验证服务框架，完善国家地下资产登记制度，并对出生和死亡登记、数据保护与隐私等领域提出新的监管要求。

在客户数据和业务数据的访问方面，该法明确了客户数据和商业数据的范畴，规定了数据持有者在客户要求或授权第三方的情况下，需向客户提供数据或允许其访问数据；要求数据持有者在必要时提供、收集或保留客户数据，并在客户请求时进行数据更正，以及规定了接口设施或服务的建立、管理及使用标准；赋予监管机构权力以监督法规执行，包括调查、信息获取、罚款和合规通知等权力。

在数字验证服务方面，该法主要内容包括：（1）要求国务大臣制定数字验证服务的信任框架和补充准则，确保服务的可靠性和安全性；（2）建立数字验证服务提供商的注册制度，规定注册条件、拒绝注册的权力以及注册信息的管理；（3）允许公共权力机构在特定条件下向注册的数字验证服务提供商披露信息。

在国家地下资产登记方面，该法要求国务大臣建立和维护英格兰和威尔士以及北爱尔兰的国家地下资产登记制度；规定相关方在规定时间内将资产信息上传至登记系统，并允许授权方访问。（来源：英国议会）

8. 美国国会议员提出《禁用敌对人工智能法案》

6 月 25 日，美国国会议员提出《禁用敌对人工智能法案》，禁止联邦机构使用由外国对手控制的人工智能技术。

法案要求制定外国敌对人工智能系统清单，具体内容包括：（1）清单制定。自本法案颁布之日起 60 日内，联邦采购安全委员会须制定一份包含所有由外国对手生产或开发的人工智能系统清单；（2）清单公布。自本法案颁布之日起 180 日内，管理与预算办公室（OMB）主任应协同联邦采购安全委员会，在公开网站上发布前款清单；（3）清单更新。联邦采购安全委员会应至少每 180 天更新一次清单。此外，若某人工智能的所有者提交书面证明，说明其产品非外国对手开发，且联邦采购安全委员会审核后确认无误，则可从清单中移除该人工智能。

法案明确要求禁止获取和使用外国对手人工智能。自法案颁布之日起 90 日内，各行政机构负责人须协同联邦采购安全委员会，审查并考虑移除清单所列外国对手实体提供的人工智能系统。各行政机构负责人应依据《美国法典》第 41 编第 4713 条赋予的权限，对清单所列人工智能采取禁用措施。同时规定，经向 OMB 主任及国会相关委员会提交书面备案，行政机构负责人可批准以下例外情形，包括：（1）基于《2002 年教育科学改革法案》第 102 条界定的科研需求；（2）用于评估、培训、测试或分析；（3）反恐或反间谍行动需要；（4）保障关键职能运行的必要情况。（来源：美国参议院）

9. 爱尔兰社会保障部因使用面部匹配技术处理敏感生物识别数据，被处以 55 万欧元罚款

6 月 12 日，爱尔兰数据保护委员会（DPC）宣布对爱尔兰社会保障部（DSP）使用面部匹配技术处理敏感生物识别数据行为的调查决定。

DPC 于 2021 年 7 月启动调查，发现 DSP 使用“Safe 2”系统在无合法依据且未充分告知公众的情况下收集、存储并比对数百万人的面部扫描数据，严重违反 GDPR 关于生物识别数据处理的透明度、合法性和对影响评估的规定，因此决定对其处以 550000 欧元的罚款。

DPC 指出，尽管 DSP 的技术安全措施在技术和组织层面没有问题，但其法律基础缺失、透明度不足以及未进行足够详尽的数据保护影响评估（DPIA）构成违规，属高风险不当处理。DPC 要求 DSP 在 9 个月内确定有效的合法依据，否则必须停止使用该技术。同时，DSP 还被责令删除相关生物识别数据，以确保用户隐私权不再继续受到侵害。（来源：爱尔兰数据保护委员会）

10. 中国台湾地区经济部国际贸易署将华为、中芯纳入《战略性高科技货品出口实体管理名单》

6 月 15 日，中国台湾地区经济部国际贸易署做出新闻回应，确认将华为、中芯纳入《战略性高科技货品出口实体管理名单》属实，并说明该举措是在跨部会实体清单审查机制下作出的决定。台湾地区称此举是依据台湾地区《贸易法》第 13 条，出于“防止武器扩散及其他国安考量”，参考联合国安理会和“友盟”制裁与管制名单，要求台湾厂商向名单内实体出口时，

必须事先取得战略性 高科技货品输出许可证，否则海关将不予放行。此举是台湾地区首次正式将华为与中芯国际纳入出口管制体系，延续了自 2020 年台积电应美国要求停止向华为供货以来的一系列对大陆科技限制措施，配合美国技术封锁政策。（来源：中国台湾地区经济部）

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.密钥派生机制简介--- PRF vs HKDF

概述：密钥派生技术（Key Derivation Function，常缩写为KDF）是密码学中的一项重要技术，它的主要作用是使用一个秘密值（例如主密钥、口令或共享秘密）通过伪随机函数导出一个或多个新的密钥。这些新生成的密钥被称为派生密钥。密钥派生可以认为是一种特殊的hash函数，因为它具有与哈希一样的特点，甚至某些密钥派生算法本身就使用了哈希或HMAC算法。

1.为什么需要密钥派生技术？

密钥派生技术在信息安全领域具有广泛的应用，主要有以下几个目的：

密钥扩展和格式转换：

有时我们拥有一个较短的秘密值，但加密算法需要一个更长的密钥，或者需要特定格式的密钥。KDF可以将短密钥扩展成指定长度和格式的密钥，同时保持其密码学强度和随机性。例如，在DH(Diffie Hellman)密钥交换协议中，双方协商得到一个共享秘密，但这个秘密可能不直接适用于SM4等对称加密算法，此时就需要KDF将其转换为适合SM4的密钥。

密钥多样化：从一个主密钥中派生出多个不同的密钥，用于不同的目的（例如一个用于加密，一个用于完整性保护）。这样做可以避免“一钥多用”带来的风险，即使其中一个派生密钥泄露，也不会直接影响其他密钥的安全性。

密码杂凑（密钥扩展和强化）：这是密钥派生最常见的应用之一。用户输入的口令通常较短且规律性强，容易被暴力破解或彩虹表攻击。KDF通过引入“盐值”（一个非秘密参数）和大量的迭代计算，使得从口令派生密钥的过程变得缓慢且耗费资源。这大大增加了攻击者进行离线破解的难

度，即使攻击者获得了口令哈希值，也需要花费大量时间和计算资源才能破解原始口令。

多方密钥协商协议的组成部分：在多方通信中，KDF 可以作为密钥协商协议的一部分，从协商出的共享秘密中生成会话密钥或其他加密所需的密钥数据。

2.常见的密钥派生函数

根据派生源的不同，我们可以将密钥派生算法简单分为两种：

（1）从一个密钥派生出一个或多个新的密钥，如 HKDF(HMAC-based key derivation)， 基于 HMAC 的密钥派生算法。

（2）从一个密码派生出一个或多个密钥，即由用户使用的一个密码、口令等派生出一个或多个密钥，如 PBKDF2、Bcrypt、Scrypt、Argon2 等。

目前有多种成熟的 KDF 算法，其中一些常用的包括：

PBKDF2 (Password-Based Key Derivation Function 2)：这是目前广泛使用的基于密码的 KDF，由 IETF 制订的文件 RFC 8018 对 PBKDF2 的过程进行了详细规定。它通过多次迭代哈希（通常是 HMAC）和引入“盐值”来增加计算复杂度，从而有效抵御暴力破解和彩虹表攻击。我国密码行业标准 GM/T 0091 也规定了利用口令来派生密钥的方法，该方法与 PBKDF2 类似。

HKDF (HMAC-based Key Derivation Function)：HKDF 是一种基于 HMAC（带有密钥的哈希消息认证码）的 KDF，HKDF 由 IETF 制订的 RFC 5869 进行了详细的规定。它通常分为两个阶段：

提取 (Extract)：将原始的输入密钥材料（可能不够随机）与盐值结合，通过 HMAC 生成一个高强度的伪随机密钥。

拓展（Expand）：使用提取阶段生成的伪随机密钥，通过HMAC和计数器的方式，生成多个或任意长度的派生密钥。

HKDF的这种设计使其在密钥多样化和密钥扩展方面表现出色。

scrypt：scrypt是一种内存密集型的KDF，RFC 7914对scrypt的过程进行了详细规定，除了计算量，它还需要大量的内存才能派生密钥。这使得它更有效地抵抗GPU（图形处理器）和ASIC（专用集成电路）的暴力破解，因为这些设备通常在内存方面受限。scrypt通过调整参数（如迭代次数、块大小和并行性）可以根据不同的安全需求和硬件性能进行优化。

Argon2：Argon2是口令哈希竞赛（Password Hashing Competition）的最终获胜者，旨在提供比PBKDF2和scrypt更高的安全性，IETF的RFC 9106对Argon2的过程进行了详细规定。它通过结合时间成本（迭代次数）、内存成本和并行成本来抵抗各种攻击，包括暴力破解、彩虹表攻击以及GPU和ASIC加速攻击。

3.密钥派生函数特点

密钥派生函数是一种利用已有密钥从中派生出新的密钥的算法。其主要特点包括以下几点：

密钥派生函数可以根据输入的原始密钥生成更加复杂和安全的派生密钥。

密钥派生函数通常使用哈希函数作为其基本构建块，通过多次迭代哈希来实现密钥的派生过程。

密钥派生函数可以根据不同的输入参数生成不同的派生密钥，以满足不同的应用场景需求。

4.密钥协商与密钥派生的区别

很多人会混淆密钥协商和密钥派生，但它们是两个不同的概念：

密钥协商（Key Agreement)：密钥协商协议（如迪菲-赫尔曼密钥交换）的目的是让通信双方在不直接传输秘密密钥的情况下，共同计算出一个共享的秘密值。这个共享秘密值是双方都知晓的，但第三方无法推断出来。密钥协商解决的是“如何安全地建立一个共享秘密”的问题。

密钥派生（Key Derivation)：密钥派生的目的是从一个已有的秘密值（可能是协商得来的共享秘密，也可能是用户密码或主密钥）中生成一个或多个实际用于加密、签名或其他密码学操作的密钥。KDF 将这个秘密值转换成适合具体应用场景的密钥形式和长度。密钥派生解决的是“如何从现有秘密中获得可用密钥”的问题。

简单来说，密钥协商是为了“得到一个原始秘密”，而密钥派生是为了“将这个原始秘密加工成可用的密钥”。在许多实际应用中，密钥协商和密钥派生是紧密结合的，例如在 TLS/SSL 协议中，双方通过密钥协商建立共享秘密，然后通过 KDF 从这个共享秘密派生出会话密钥用于后续的数据加密。

5.总结

总的来说，密钥派生在实际系统中的应用案例丰富多样，涵盖了密码存储、加密通信、身份验证等多个领域。同时，作为密码学领域的重要组成部分，密钥派生在密码学研究中扮演着关键的角色，对提高密码学系统的安全性和推动密码学领域的发展具有重要意义。（作者：北京信安世纪科技股份有限公司 汪宗斌 秦体红）

行业前沿观察二:2025 调查活动 7 月 22 日正式启动；网信部门大力整治假冒仿冒“自媒体”账号；部署开展“清朗·2025 年暑期未成年人网络环境整治”专项行动；整治涉企网络‘黑嘴’”专项行动典型案例公开

导读：网民网络安全感满意度调查活动组委会发出通知，公告将于 7 月 22 日正式启动“2025 网民网络安全感满意度调查活动”样本采集工作，届时全国同步开通问卷样本采集通道，采集工作历时 10 天，于 7 月 31 日结束。

中央网信办印发通知,在全国范围内部署开展为期 2 个月的“清朗·2025 年暑期未成年人网络环境整治”专项行动。网信部门会同相关部门依法处置一批假冒仿冒账号，督促重点平台加强账号审核、畅通举报渠道、深入自查自纠，累计处置违规账号 3008 个。

国家网信办扎实组织开展“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动，部署地方网信办积极受理处置涉企网络侵权不法行为，督促重点网站平台强化涉企信息内容管理，从严从快处置一批涉企违法违规账号。

关键词：互联网、人脸识别、网络安全、网信办、标准化

1. 2025 网民网络安全感满意度调查活动样本采集工作将于 7 月 22-31 日开展

6 月 25 日，网民网络安全感满意度调查活动组委会发出通知，公告将于 7 月 22 日正式启动“2025 网民网络安全感满意度调查活动”样本采集工作，届时全国同步开通问卷样本采集通道。采集工作历时 10 天，于 7 月 31 日结束。

通知提到，为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，在各级党政有关部门的关心指导和各发起单位的共同努力下，调查活动已连续成功举办七届，累计采集有效样本量突破 1300 万份，收集网民意见近 100 万条，发布全国总报告、专题报告、区域报告、行业分析报告等系列调查报告 1200 多份。调查数据被党政有关部门、研究机构广泛引用和权威发布，为我国网络安全研究、互联网综合治理工作提供了有力支撑。

通知提出，2025 年是国家“十四五”规划收官之年和“十五五”规划谋篇布局之年，也是调查活动第二个五年计划(2023-2027)实施的关键之年。各发起单位接到通知后，要及时组织开展相关工作。

通知公布了 2025 调查活动样本采集工作领导小组成员名单，明确了四大工作内容，就支撑服务和总结表扬等做了说明。

2. 网信部门大力整治假冒仿冒“自媒体”账号

近期，一些网络账号以“XX 报”“XX 新闻”“XX 文旅推荐官”“XX 官方直播间”为名假冒仿冒新闻媒体、政府机构、企事业单位，虚假宣传、

售卖假货，扰乱社会秩序。网信部门会同相关部门依法处置一批假冒仿冒账号，督促重点平台加强账号审核、畅通举报渠道、深入自查自纠，累计处置违规账号3008个。现将部分典型案例通报如下。

1.“动态新闻”“上海午报”等账号仿冒新闻媒体名称、标识，违规开展互联网新闻信息服务，扰乱网络传播秩序。涉及的账号已被依法依约关闭。

2.“安徽省教育考试招生院”等账号假冒教育招生部门官方名称，为涉考涉招培训、咨询业务违规引流，严重干扰招生考试秩序。涉及的账号已被依法依约关闭。

3.“日照文旅推荐官”等账号未获相关文化和旅游行政部门授权，账号名称仿冒地方文旅官方认证账号，误导公众。涉及的账号已被依法禁言、暂停营利权限、关闭等处置。

4.“邮政精选”等账号名称、头像、简介、背景图中含有“邮政”元素，未经授权利用“中国邮政”品牌和邮政机构的公信力、影响力、权威性引流带货，损害消费者合法权益，破坏网络生态。涉及的账号已被依法禁言、暂停营利权限、关闭等处置。

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《互联网用户账号信息管理规定》《关于加强“自媒体”管理的通知》等要求，持续整治假冒仿冒“自媒体”账号，加大网络执法力度，努力营造积极向上的网络环境。同时，网信部门将持续保持高压严打态势，欢迎广大网民积极参与监督举报，共同营造清朗网络空间。

3. 中央网信办部署开展“清朗·2025 年暑期未成年人网络环境整治”专项行动

为强化未成年人网络保护，营造良好网络环境，近日，中央网信办印发通知，在全国范围内部署开展为期 2 个月的“清朗·2025 年暑期未成年人网络环境整治”专项行动。

落实《未成年人网络保护条例》，本次专项行动将进一步拓展治理深度和范围，持续深入整治网上危害和影响未成年人身心健康的问题乱象，严肃查处涉暴力迷信、淫秽色情、引诱自杀自残、侵害未成年人隐私等违法信息，全面清理低俗庸俗、炫富拜金、极端情绪等不良内容，严厉打击涉嫌针对未成年人的违法犯罪行为。在此基础上，聚焦各类新情况新表现，做好四方面问题整治。一是实施网络侵害行为。以未成年人为对象，借绝版“谷子”、明星周边、免费学习搭子、图片定制等名义，侵扰未成年人，实施网络欺凌、隔空猥亵等恶性违法行为。二是隐蔽传播违法不良信息。借卡牌、故事、动漫等未成年人喜爱的新载体、新手法，炮制网络黑话烂梗，虚构放大血腥暴力情节，包装美化不良亚文化，鼓吹不良价值观，危害未成年人身心健康。三是诱导参与线下危险活动。引诱提供陪聊、陪玩、陪游等违规服务，教授制作“笔枪”“牙签弩”等所谓“创意手工”，鼓动未成年人模仿“楼梯跳跃”“窒息挑战”等危险动作，可能造成线下伤害。四是利用未成年人形象牟利。恶意发布导向不良的未成年人出镜内容，炮制软色情、软暴力“毒流量”，炒作儿童 CP，摆拍“整蛊儿童”“姐弟互殴”等虚假剧情，炫耀未成年人不良行为，博取眼球、营销牟利。

在开展专项整治的同时，网信部门将重点关注三个方面情况。一是未成年人模式的使用情况以及内容建设存在的问题。二是儿童智能设备的内容安全以及功能规范。三是AI功能在未成年人领域不当应用以及诱导沉迷问题。

中央网信办有关负责同志强调，开展专项行动是净化网络空间、护航未成年人健康成长的有力保障。各地网信部门要准确把握未成年人网络保护新情况、新问题、新特点，压实网站平台主体责任，加大巡查力度，从严处置处罚存在突出问题的平台、账号和MCN机构，公开曝光典型案例，强化警示震慑。同时，也呼吁社会各界以及广大网民共同抵制网上涉未成年人乱象问题，共同营造安全健康的网络环境。

4.“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动公开曝光一批典型案例

近期，国家网信办扎实组织开展“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动，部署地方网信办积极受理处置涉企网络侵权不法行为，督促重点网站平台强化涉企信息内容管理，从严从快处置一批涉企违法违规账号。现将部分典型案例通报如下。

1.“柴怼怼”等账号编造涉企虚假不实信息，恶意诋毁攻击企业。抖音账号“柴怼怼”“怼怼柴”，小红书账号“柴怼怼”等，无事实依据蓄意抹黑某企业的产品质量，恶意诋毁某企业和企业家形象声誉，并借机吸粉引流带货。涉及的账号已被依法依约关闭。

2.“孟栖笔谈”等账号发布涉企负面信息，谋取非法利益。微信公众账号“孟栖笔谈”“辉常观察”，微博账号“-孟永辉-”，百家号“孟永辉”等，长期集纳发布涉企负面不实信息。在企业与其沟通删除不实信息时，要挟开展商务合作。涉及的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.“车说道”等账号蹭炒涉企热点，发布虚假不实信息。懂车帝账号“CHE 车说道”、易车账号“CHE 车说道”、搜狐账号“车说道”等，为博眼球、吸流量，恶意蹭炒智能驾驶、辅助驾驶等汽车行业热点话题，发布某品牌汽车不实信息，捏造人员伤亡事故，虚构法院判决，恶意诋毁企业产品质量。涉及的账号已被依法依约关闭。

4.“物联网咨询室”等账号散布企业商业秘密，传播虚假不实信息。微信公众账号“物联网咨询室”“物联网咨询室号外”为博取流量，长期发布某高科技企业的商业秘密，并恶意传播虚假信息，干扰企业正常生产经营和发展。涉及的账号已被依法依约关闭。

5.“兴德旺业”等账号冒用企业、企业家身份，开展市场营销。微信公众账号“兴德旺业”“杭州娃小哈”，微信视频号“兴德旺业书院”，抖音账号“王少甫-瀚慈”等，在账号名称、简介中假冒仿冒企业名称或假借企业家名义发布信息，开展商业活动。涉及的账号已被依法依约处置，侵权信息已被清理。

行业前沿观察三：各地协会动态

导读：各地协会活动精彩纷呈，开展主题当日活动，开设大讲堂，举行培训会等。广东省网络空间安全协会：成功召开 2025 网民网络安全感满意度调查活动高校合作说明会；甘肃省商用密码行业协会：甘肃省“密码法治陇原行”——嘉峪关站活动成功举办；沈阳市网络安全协会：顺利召开会员大会暨第四届换届选举大会；苏州市互联网协会：“苏州市网络和数据安全公益大讲堂”正式揭牌；惠州市计算机信息网络安全协会：开展网络安全公益行企业“体检”活动；中关村可信计算产业联盟 ：“2025 地理信息技术创新大会”将于 9 月召开；海南省计算机学会成功举办 2025 中国高校计算机大赛-移动应用创新赛暨海峡两岸创新作品赛海南省赛；东莞市信息与网络安全协会党支部正式授牌成立；“新耀东方”2025 第四届上海网络安全博览会暨发展论坛圆满落幕；湖北省网络和数据安全协会：协会 2025 年第二期网络与信息安全管理员考试圆满收官等。

关键词：选举、调查活动、论坛、网络安全、信息安全

1. 广东省网络空间安全协会：成功召开 2025 网民网络安全感满意度调查活动高校合作说明会

近日，为深入贯彻“网络安全为人民，网络安全靠人民”的重要理念，广泛凝聚高校智慧力量，共同推动国家网络安全事业发展，由网民网络安全感满意度调查活动组委会指导，全国 135 家网络社会组织及相关机构（网安联）发起，北京网络空间安全协会、广东省网络空间安全协会主办，北京关键信息基础设施安全保护中心、广东新兴国家网络安全和信息化发展研究院承办的“凝聚高校力量，共筑网络安全”——2025 网民网络安全感满意度调查活动高校合作说明会成功召开。

调查活动组委会秘书处副秘书长周贵招对 2025 年调查活动相关工作情况进行汇报，他详细介绍了 2025 年调查活动的整体规划、核心目标及重点工作任务。他表示，高校是培养网络空间建设者和守护者的摇篮，是调查活动获取真实、多元声音的重要阵地，期待高校发挥自身优势，深度融入本次调查活动。

2. 甘肃省商用密码行业协会：甘肃省“密码法治陇原行”——嘉峪关站活动成功举办

甘肃省“密码法治陇原行——嘉峪关站”暨《商用密码管理条例》施行两周年活动成功举办。活动由甘肃省国家密码管理局指导，甘肃省商用密码行业协会主办，嘉峪关市、甘肃矿区国家密码管理局承办。嘉峪关市与甘肃矿区相关部门、各重要网络与信息系统运营单位负责同志及行业专

家等 200 余人参加活动，甘肃省国家密码管理局、嘉峪关市相关领导出席并致辞。

活动以展板宣传、商密产品展示、集中授课等方式举办。活动聚焦《密码法》、《商用密码管理条例》的深化落实，就当前形势与政策、密评实施经验、政务信息系统密码应用建议以及人工智能发展态势进行了专题讲授，切实强化了政策普及实效。

3. 沈阳市网络安全协会：顺利召开会员大会暨第四届换届选举大会

7 月 4 日，沈阳市网络安全协会会员大会暨第四届换届选举大会在辽宁大厦一楼多功能厅隆重举行。100 多名会员齐聚一堂，共商沈阳网络安全事业发展大计，擘画行业发展新蓝图。

会上，参会人员认真听取并审议通过第三届理事会工作报告。会议现场，书面审议了第三届理事会财务工作报告、监事工作报告。大会同时还审议通过了换届选举办法及章程修订案。此次换届大会的成功举办，标志着协会在推动沈阳市网络安全事业发展的征程上迈入新阶段。未来，协会将继续发挥桥梁纽带作用，凝聚行业智慧与力量，为沈阳市网络安全生态建设及数字经济高质量发展保驾护航。

4. 苏州市互联网协会：“苏州市网络和数据安全公益大讲堂”正式揭牌

7 月 3 日下午，苏州市网络安全志愿讲师领航赋能活动暨网络和数据安全公益大讲堂揭牌仪式在苏州大学举行。

现场，苏州市互联网协会与三家高校共建的“苏州市网络和数据安全公益大讲堂”正式揭牌，标志着苏州网络安全宣传教育向“校协合作、资源共享”迈出关键一步。

苏州市委网信办、苏州大学继续教育学院、苏州市职业大学、西交大苏州信息安全法学所等相关单位领导和 30 余位志愿讲师出席活动。

5. 惠州市计算机信息网络安全协会：开展网络安全公益行企业“体检”活动

7 月初，惠州市委网信办全面统筹，按照广东省委网信办要求精心组织了网络安全公益行企业“体检”活动，惠州市计算机信息网络安全协会携手技术支撑单位，为广大企业提供了一系列高质量的网络安全公益性服务。

“体检”团队实地调研多家企业网络安全发展情况，针对企业网络及数据安全方面存在的问题，为各企业提供一对一的免费网络安全“体检”服务，帮助企业及时发现问题、修复漏洞、消除隐患。同时，针对企业在数字化发展中存在的网络安全问题，开展网络安全培训，提高企业网络安全意识和防范能力。

6. 中关村可信计算产业联盟 ：“2025 地理信息技术创新大会”将于 9 月召开

近日，中关村可信计算产业联盟发布消息，公布“2025 地理信息技术创新大会”将于 2025 年 9 月 16-17 日在北京国际会议中心召开。

作为地理测绘领域极具影响力的活动之一，该大会以时代发展为背景，聚焦政策趋势解读、前沿技术发展、技术应用创新、方案成果展示、人才教育方法等，通过 2 天的时间，为参会者奉献立足于技术驱动未来变革与影响的饕餮盛宴。以推动地理信息技术不断创新，应用不断普及、深入，助力地理信息产业可持续发展，增进地理信息技术在各个应用领域成功经验交流，提升国产 GIS 平台软件的自主创新水平。

7. 海南省计算机学会成功举办 2025 中国高校计算机大赛-移动应用创新赛暨海峡两岸创新作品赛海南省赛

近日，由海南省计算机学会作为实施单位的“2025 年中国高校计算机大赛-移动应用创新赛暨海峡两岸创新作品赛”海南省赛成功举办。大赛旨在激发大学生创新精神，提升移动应用设计与开发实践能力，深化高校学子在科技创新领域的交流。比赛吸引了省内 29 所高校 1100 多名师生共计 220 个项目参赛。

此次海南省赛是全国赛的重要选拔环节，参赛作品涵盖了移动应用、人工智能、信息安全、算法设计、语言识别、大数据、图像处理、虚拟现实、三维可视化应用、游戏设计、动漫创意设计等多个领域，充分展现了

当代大学生对科技赋能社会发展的深刻洞察力和创造力。优秀团队将代表海南省角逐全国总决赛，参与海峡两岸的创新交流活动。

8. 东莞市信息与网络安全协会党支部正式授牌成立

近期，东莞市信息与网络安全协会党支部正式成立，并在南城街道新建两新党组织书记培训班（第二批）上成功举行授牌仪式。

接下来，在南城街道“两新”组织党委的带领下，协会党支部将以创新的指导思想引领党员，将党建工作与网络安全工作深度融合，充分发挥专业优势，为东莞市网络安全事业的健康发展提供坚强有力的组织保障，为筑牢数字时代的安全防线贡献力量。

9. “新耀东方”2025 第四届上海网络安全博览会暨发展论坛圆满落幕

近日，由上海市信息网络安全管理协会参与主办的“新耀东方-2025 第四届上海网络安全博览会暨发展论坛”，在上海新国际博览中心成果举办。在连续三届成功举办的基础上，精心构建多元融合的交流平台，采用“论坛+展览”的形式，共设 1 个主论坛与 4 个分论坛，旨在激发数字安全领域的创新潜能，共同探索应对网络安全挑战的创新策略。

其中，上海市信息网络安全管理协会网络信息内容安全专委会和人工智能安全专委会在开幕式上正式揭牌成立，旨在发挥平台优势，整合行业优质资源，凝聚专业智慧力量，为构建更加安全可靠的网络空间提供有力支撑。

10. 湖北省网络和数据安全协会：协会 2025 年第二期网络与信息安全管理员考试圆满收官

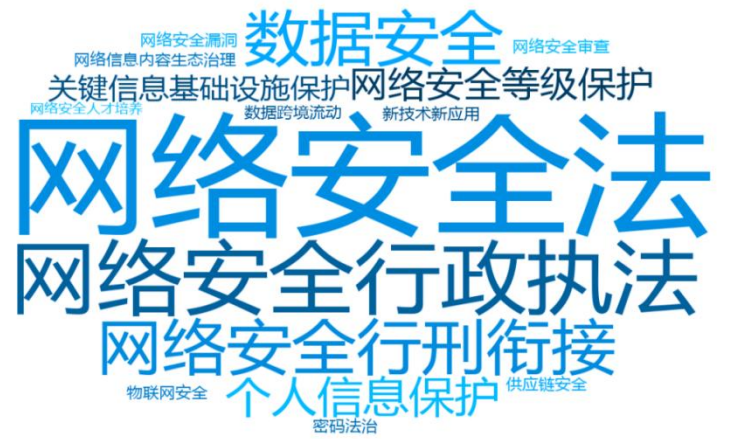
近日，湖北省网络和数据安全协会 2025 年第二期网络与信息安全管理员考试圆满落幕。此次考试以提升从业者专业素养为核心，聚焦网络安全基础知识、攻防技术、信息安全管理等核心领域，吸引全省数百名跨行业网安人才参与，全方位检验从业者技能与实践能力。

考试现场秩序规范，考生严守纪律、专注作答，展现扎实专业功底；监考团队严格执行流程，确保公平公正。作为湖北网安领域重要行业组织，协会未来将持续开展培训、考试等活动，搭建学习交流平台，紧跟行业前沿，以创新路径推动网安人才培育与行业高质量发展，诚邀更多从业者携手共建安全网络空间。

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

……