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6月第6期（总第11期）

2024年6月15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

导读：5 月，人工智能是我国开展国际交流与合作的重要议题。我国与法国就人工智能和全球治理发表联合声明，双方一致认为促进人工智能的开发与安全，并为此推动适当的国际治理至关重要。中法两国将充分致力于促进安全、可靠和可信的人工智能系统，坚持“智能向善（AI for good）”的宗旨。中美人工智能政府间对话首次会议举行，同样强调“智能向善”理念。中方强调将始终坚持以人为本、智能向善理念，确保人工智能技术有益、安全、公平，并就美方在人工智能领域对华限制打压表明严正立场。

我国与俄罗斯在两国建交 75 周年之际发布联合声明，商定在人工智能等信息通信技术领域开展互利合作。同时，双方愿就人工智能的发展、安全和治理加强交流与合作。双方同意建立并用好定期磋商机制加强人工智能和开源技术合作，在国际平台上审议人工智能监管问题时协调立场，支持对方举办的人工智能相关国际会议。此外，双方重申在维护信息通信技术领域安全问题上的一致立场，同意协作应对包括与人工智能相关的各类网络安全风险。反对利用技术垄断、单边强制措施恶意阻挠他国人工智能发展、阻断全球人工智能供应链。

5 月 31 日，《网络安全法》实施七周年活动在苏州顺利举行。30 余位专家围绕人工智能产业发展及立法、数据治理挑战和探索、密码法治保障高质量发展、供应链安全与生态构建、《网络安全法》实施成效及修改等议题展开深度研讨。《网络安全法》实施周年活动是中国信息安全法律大

会专家委员会的重要年度活动，已连续七年在苏州举办，赋能苏州数字经济安全发展，对助力数智化时代的中国网络安全法治构建、以高质量法治促进新质生产力发展具有重要意义。

关键词：人工智能、智能向善、人工智能供应链、《网络安全法》实施七周年活动

1. 中法发布人工智能和全球治理联合声明，达成十大共识

5 月 5 日至 7 日，国家主席习近平对法国进行国事访问。期间，两国元首在 2023 年《中法联合声明》达成共识的基础上，发布《中华人民共和国和法兰西共和国关于人工智能和全球治理的联合声明》，在人工智能方面达成十大共识。

其中，中法两国认识到人工智能在发展与创新中的关键作用，同时考虑到人工智能的发展和使用可能带来的一系列挑战，一致认为促进人工智能的开发与安全，并为此推动适当的国际治理至关重要。为了充分利用人工智能带来的机遇，中法两国致力于深化关于人工智能国际治理模式的讨论。这一治理既应顾及技术不断快速发展所需的灵活性，同时应对个人数据、人工智能用户的权利以及作品被人工智能使用的用户的权利提供必要保护。中法两国充分致力于促进安全、可靠和可信的人工智能系统，坚持“智能向善（AI for good）”的宗旨，通过全面和包容性的对话，挖掘人工智能的潜力，降低其风险。（来源：外交部）

2. 中美人工智能政府间对话首次会议举行，中方阐明人工智能立场

5 月 14 日，中美人工智能政府间对话首次会议在瑞士日内瓦举行。双方围绕人工智能科技风险、全球治理、各自关切的其他问题深入、专业、建设性地交换意见。

中方强调人工智能技术是当前最受关注的新兴科技，中方始终坚持以人为本、智能向善理念，确保人工智能技术有益、安全、公平。中方支持加强人工智能全球治理，主张发挥联合国主渠道作用，愿同包括美方在内的国际社会加强沟通协调，形成具有广泛共识的全球人工智能治理框架和标准规范。中方就美方在人工智能领域对华限制打压表明严正立场。

双方均认识到人工智能技术发展既面临机遇也存在风险，重申继续致力于落实两国元首在旧金山达成的重要共识。（来源：央视新闻）

3. 中俄发布联合声明，将加强人工智能和开源技术合作

5 月 16 日至 17 日，俄罗斯联邦总统普京对我国进行国事访问。访问期间，中俄双方发布《中华人民共和国和俄罗斯联邦在两国建交 75 周年之际关于深化新时代全面战略协作伙伴关系的联合声明》。

声明强调，双方商定在信息通信技术领域开展互利合作，包括人工智能、通信、软件、物联网、开源、网络和数据安全、电子游戏、无线电频率协调、职业教育和专业科学研究等领域。双方高度重视人工智能问题，愿就人工智能的发展、安全和治理加强交流与合作。俄方欢迎中方提出《全球人工智能治理倡议》，中方欢迎俄方在人工智能领域提出治理准则。双方同意建立并用好定期磋商机制加强人工智能和开源技术合作，在国际平台上审议人工智能监管问题时协调立场，支持对方举办的人工智能相关国际会议。

同时，双方重申在维护信息通信技术领域安全问题上的一致立场，同意协作应对包括与人工智能相关的各类网络安全风险。双方鼓励全球共同推动人工智能健康发展，共享人工智能红利，加强人工智能能力建设国际合作，妥善应对人工智能军事应用问题，支持在联合国、国际电信联盟、金砖国家、上海合作组织、国际标准化组织等机制平台开展人工智能交流合作。反对利用技术垄断、单边强制措施恶意阻挠他国人工智能发展、阻断全球人工智能供应链。

此外，双方肯定联合国在制定国际信息安全领域共同规则中发挥主导作用，支持联合国2021—2025年信息安全开放式工作组作为该领域无可替代的全球谈判平台并开展经常性工作。双方指出，应制定信息空间新的、负责任的国家行为准则，特别是制定普遍性法律文书可为建立旨在防止国家间冲突的信息空间国际法律调解机制奠定基础，有利于构建和平、开放、安全、稳定、互通、可及的信息通信技术环境。双方认为应履行联合国大会第74/247号决议，在联合国特设委员会框架内完成制定打击以犯罪为目的使用信息和通信技术的全面国际公约。双方支持在确保各国网络体系安全稳定的前提下打造多边、民主、透明的全球互联网治理体系。双方愿在上海合作组织、金砖国家及其他多边机制下加强协作。双方主管部门愿在现行法律条约框架下，深化国际信息安全领域双边合作。（来源：中国新闻社）

4. 《网络安全法》实施七周年活动在苏州顺利举行

5 月 31 日，《网络安全法》实施七周年之际，以“智能风险 法治可能”为主题的研讨活动在苏州举行。

30 余位专家围绕人工智能产业发展及立法、数据治理挑战和探索、密码法治保障高质量发展、供应链安全与生态构建、《网络安全法》实施成效及修改等议题展开深度研讨。与会专家认为，人工智能、量子计算等颠覆性技术以前所未有的速度、广度和深度影响人类社会生产生活，网络空间安全态势愈加复杂，我国网络安全法治面临新变革、新挑战。推动网络安全法治建设，应当既立足当前又着眼未来，审慎回应科技与法治、科技与人之间的关系，平衡个人与国家、政府与产业、发展与安全、国内与国际等多重价值目标，以法治的无限可能助推新质生产力发展。

《网络安全法》实施周年活动是中国信息安全法律大会专家委员会的重要年度活动，已连续七年在苏州举办，赋能苏州数字经济安全发展，对助力数智化时代的中国网络安全法治构建、以高质量法治促进新质生产力发展具有重要意义。（来源：新华财经）

境内前沿观察二：政策立法

导读：5 月，国务院、全国人大常委会 2024 年立法工作计划相继发布，明确本年度立法工作要点。网络数据安全管理条例列入国务院 2024 年拟制定、修订的行政法规；《网络安全法（修改）》列入全国人大 2024 年初次审议法律案，人民警察法修改列入预备审议项目。

行政执法监督成为国家层面政策立法重点关注。继国务院办公厅在 2023 年 9 月发布的《提升行政执法质量三年行动计划（2023—2025 年）》中要求完善行政执法监督制度、健全行政执法监督机制、创新行政执法监督方式后，5 月，预备制定行政执法监督条例列入国务院 2024 年立法工作计划；中共中央办公厅、国务院办公厅印发《关于加强行政执法协调监督工作体系建设的意见》，提出到 2024 年年底，基本建成省市县乡四级全覆盖的比较完善的行政执法监督工作体系，实现对行政执法工作的全方位、全流程、常态化、长效化监督的工作目标。

网络安全方面，中央网络安全和信息化委员会办公室等四部门联合发布《互联网政务应用安全管理规定》，规范机关事业单位建设运行的互联网政务应用。对于委托外包环节，明确未经委托的机关事业单位同意，外包单位不得转包、分包合同任务，不得访问、修改、披露、利用、转让、销毁数据。此外，供应链安全方面，国家标准《网络安全技术 软件供应链安全要求》正式发布，明确软件供应链安全目标，提出软件供应链安全风险管理要求和供需双方的组织管理和供应活动管理安全要求。《网络安全

技术 软件物料清单数据格式（征求意见稿）》发布，为软件供应链安全保障的重要环节，即软件物料清单的生成、共享和使用提供指引。

促进数字经济发展、激发数据要素潜能方面，《数字中国建设 2024 年工作要点清单》《2024 年数字福建工作要点》《数字广东建设 2024 年工作要点》等文件发布，深入推动数字经济创新发展与提升数字安全保障能力并重仍是核心理念。国家数据局提出将加强数字技术协同创新运用，稳步增强数字安全保障能力，不断完善数字领域治理生态；福建表示将在数字政府建设、重要行业领域信息化建设、关键信息基础设施保护中落实安全可靠技术和产品应用要求；广东表示将常态化开展安全培训、测评、检查、审计、漏洞排查和供应链安全管理。

针对数据出境安全，《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》、上海临港新片区三个领域的《数据跨境场景化一般数据清单》发布，进一步细化数据出境安全监管模式。

关键词：网络安全法（修改）、行政执法监督、互联网政务应用安全、供应链安全、数字经济发展

（一）国家层面

1. 国务院办公厅印发《国务院 2024 年度立法工作计划》

5 月 6 日，国务院办公厅印发《国务院 2024 年度立法工作计划》。

法律案层面，预备提请全国人大常委会审议电信法草案、人民警察法修订草案、人工智能法草案。

行政法规层面，拟制定、修订的行政法规包括网络数据安全管理条例（国家网信办起草）、两用物项出口管制条例（商务部起草）。预备制定行政执法监督条例、政策发布条例、行政规范性文件制定程序条例。预备修订行政复议法实施条例、规章制定程序条例、互联网信息服务管理办法、保守国家秘密法实施条例、反间谍法实施细则。（来源：中国政府网）

2. 全国人大常委会公布《2024 年度立法工作计划》

5 月 8 日，全国人大常委会公布《2024 年度立法工作计划》。本次立法计划共安排 16 件继续审议的法律案、23 件初次审议的法律案，以及若干预备审议项目和 3 件 2024 年实施期限届满的授权决定。

其中继续审议的法律案包括治安管理处罚法（修订）（6 月）；初次审议的法律案包括《反不正当竞争法（修改）》和《网络安全法（修改）》；预备审议项目包括制定电信法，修改人民警察法，以及研究网络治理和人工智能健康发展方面的立法项目，由有关方面抓紧开展调研和起草工作，视情安排审议。（来源：中国人大网）

3. 中共中央办公厅、国务院办公厅印发《关于加强行政执法协调监督工作体系建设的意见》，加强行政执法监督工作

5 月 14 日，中共中央办公厅、国务院办公厅印发《关于加强行政执法协调监督工作体系建设的意见》，对加强新时代行政执法协调监督工作作出系统部署。

意见指出，要持续完善监督制度、严格落实监督职责、不断创新监督方式，充分发挥行政执法监督对行政执法工作的统筹协调、规范管理、指导监督、激励保障作用，到 2024 年年底，基本建成省市县乡四级全覆盖的比较完善的行政执法监督工作体系，实现对行政执法工作的全方位、全流程、常态化、长效化监督。

意见要求，要健全行政执法监督工作体制机制，推动行政执法监督与其他各类监督有机贯通、相互协调。要完善行政执法监督法规制度体系，推进行政执法监督立法，健全行政执法监督工作制度，完善行政执法行为规范，健全行政执法管理制度。要严格履行行政执法监督职能，开展行政执法常态化监督，抓好行政执法专项监督，可根据工作需要对重要法律、法规、规章的执行情况组织开展行政执法检查，强化涉企行政执法监督，强化对行政执法工作的综合协调，做好对跨领域跨部门综合行政执法改革以及基层综合行政执法改革的指导工作。（来源：中国政府网）

（二）部委层面动向

1. 国家密码管理局印发《商用密码领域违法线索投诉举报处理办法（试行）》

4 月 12 日，国家密码管理局印发《商用密码领域违法线索投诉举报处理办法（试行）》，自 2024 年 6 月 1 日起施行。

办法规定商用密码领域违法线索的投诉举报处理工作的主管机关及其处理原则、投诉举报渠道、投诉举报者应当提供的信息、管辖权事宜、审查期限、审查结果、审理期限等。办法明确，由国家密码管理局主管全国投诉举报处理工作，指导并监督地方各级密码管理部门的投诉举报处理工作。县级以上地方各级密码管理部门负责本行政区域内的投诉举报处理工作。密码管理部门应当自受理之日起 90 日内办结投诉举报。投诉举报情况复杂，难以在 90 日内办结的，经密码管理部门负责人或者其授权的相关负责人批准，可以延长办理期限，延长期限不得超过 30 日。延长办理期限的，应当告知投诉举报人并说明理由。法律、法规、规章另有规定的，从其规定。（来源：国家密码管理局）

2. 两部门印发《会计师事务所数据安全管理暂行办法》

4 月 15 日，财政部、国家网信办印发《会计师事务所数据安全管理暂行办法》，加强会计师事务所数据安全管理，规范会计师事务所数据处理活动。

办法适用于在我国境内依法设立的会计师事务所开展下列审计业务相关的数据处理活动：（1）为上市公司以及非上市的国有金融机构、中央企业等提供审计服务的；（2）为关键信息基础设施运营者或者超过100万用户的网络平台运营者提供审计服务的；（3）为境内企业境外上市提供审计服务的。此外，会计师事务所从事的审计业务不属于上述规定的范围，但涉及重要数据或者核心数据的，适用本办法。办法所称数据是指会计师事务所执行审计业务过程中，从外部获取和内部生成的任何以电子或者其他方式对信息的记录。

办法规定，会计师事务所存储核心数据的信息系统要落实四级网络安全等级保护要求，存储重要数据的信息系统要落实三级及以上网络安全等级保护要求。此外，会计师事务所应当对审计业务相关的信息系统、数据库、网络设备、网络安全设备等设置并启用访问日志记录功能。涉及核心数据的，相关日志留存时间不少于三年。涉及重要数据的，相关日志留存时间不少于一年；涉及向他人提供、委托处理、共同处理重要数据的相关日志留存时间不少于三年。

办法要求，审计工作底稿应当按照法律、行政法规和国家有关规定存储在境内。相关加密设备应当设置在境内并由境内团队负责运行维护，密钥应当存储在境内。会计师事务所应当建立数据备份制度。会计师事务所应当确保在审计相关应用系统因外部技术原因被停止使用、被限制使用等情况下，仍能访问、调取、使用相关审计工作底稿。会计师事务所不得在业务约定书或者类似合同中包含会计师事务所向境外监管机构提供境内项目资料数据等类似条款。（来源：中国网信网）

3. 两部门印发《关于规范移动互联网程序中登载使用地图行为的通知》

4 月 24 日，自然资源部办公厅、工业和信息化部办公厅近日联合印发《关于规范移动互联网程序中登载使用地图行为的通知》，规范移动互联网应用程序（简称“APP”）登载使用地图的行为。

通知明确，APP 主办者合规登载使用地图应遵守下列义务：（1）依法履行行政审批。从事互联网地图服务的 APP 主办者应当向自然资源主管部门、电信主管部门履行地图审核程序、ICP 备案手续。地图内容发生变化或者进行更新的，应依法重新履行地图审核程序；（2）严格落实主体责任。APP 主办者应落实安全主体责任，确保在登载使用地图时准确反映中国领土范围、行政区域界线、重要岛屿等并标示审图号；引用地图时要注明地图来源和审图号；对违反法律法规登载使用地图的注册用户要依法依约采取警示、限制功能、关闭账号、保存记录并上报等处置措施；（3）强化国家版图意识宣传。APP 主办者应按照自然资源主管部门、电信主管部门要求，积极参与国家版图意识宣传工作，知悉了解地图管理相关法律法规，牢固树立“地图无小事”的观念，在 APP 开发、上线审查阶段明确规范使用地图的要求，从源头上防止“问题地图”的出现，以实际行动维护国家主权、安全。

此外，通知明确增强协同联动的三方面工作机制，即优化行政审批和备案服务、构建多部门协同监管机制及强化违法违规行为的整治处置措施。（来源：自然资源部）

4. 两部门印发《关于支持引导公路水路交通基础设施数字化转型升级的通知》

4 月 29 日，财政部、交通运输部印发《关于支持引导公路水路交通基础设施数字化转型升级的通知》，支持引导公路水路交通基础设施数字化转型升级，计划用三年时间打造一批示范通道及网络。通知围绕推动基础设施智慧扩容、推动基础设施安全增效、推动跨领域产业融合、推动体制机制创新四个方面提出具体实施措施。

其中，推动基础设施安全增效方面，通知要求围绕行业管理提升，对通道基础设施安全监测、运行管控和应急指挥调度体系进行数字化改造，加快应用新一代信息采集、智慧分析与处理系统等，推进实施数字化管养系统、运行监测预警平台、数字治超及大件运输全链条监管系统、应急指挥调度系统等建设，推动开展业务流程和运行机制优化重构，有效提高安全风险识别预警、快速响应和联动处置能力，持续提升公共服务和行业治理水平。（来源：交通运输部）

5. 国家市场监督管理总局发布《网络反不正当竞争暂行规定》

5 月 6 日，国家市场监督管理总局发布《网络反不正当竞争暂行规定》。

规定要求，经营者不得采用财物或者其他手段，贿赂平台工作人员、对交易有影响的单位或者个人，以谋取交易机会或者在流量、排名、跟帖服务等方面的竞争优势。经营者不得利用互联网、大数据、算法等技术手段，通过影响用户选择或者其他方式，实施流量劫持、干扰、恶意不兼容等行为，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行。

规定优化执法办案，针对网络不正当竞争行为辐射面广、跨平台、跨地域等特点，对监督检查程序作出特别规定。明确网络不正当竞争行为举报较为集中，或者引发严重后果或者其他不良影响的，可以由实际经营地、违法结果发生地的设区的市级以上地方市场监督管理部门管辖。同时，创设专家观察员制度，为解决重点问题提供智力支撑和技术支持。（来源：国家市场监督管理总局）

6. 工业和信息化部印发《工业和信息化领域数据安全风险评估实施细则（试行）》

5 月 10 日，工业和信息化部印发《工业和信息化领域数据安全风险评估实施细则（试行）》，自 2024 年 6 月 1 日起施行。实施细则明确数据安全风险评估的适用对象、评估内容、评估期限、评估开展方式、评估报告的提交与管理等关键环节，为工业和信息化领域数据安全风险评估提供具体操作指南。

实施细则规定，重要数据和核心数据处理者每年至少开展一次数据安全风险评估，评估结果有效期为一年，以评估报告首次出具日期计算。评估报告应当包括数据处理者基本情况、评估团队基本情况、重要数据的种类和数量、开展数据处理活动的情况、数据安全风险评估环境，以及数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等。

实施细则明确，重要数据和核心数据处理者可以自行或者委托具有工业和信息化数据安全工作能力的第三方评估机构开展评估。重要数据和核心数据处理者委托第三方评估机构开展数据安全风险评估的，可以通过订

立合同或者其他具有法律效力的文件，明确双方的权利和责任，向第三方评估机构提供必需的材料和条件，确保相关材料的真实性和完整性，并确认评估结果。（来源：工业和信息化部）

7. 四部门印发《关于深化智慧城市发展 推进城市全域数字化转型的指导意见》

5 月 14 日，国家发展改革委、国家数据局、财政部、自然资源部联合印发《关于深化智慧城市发展 推进城市全域数字化转型的指导意见》。指导意见围绕全领域推进城市数字化转型、全方位增强城市数字化转型支撑、全过程优化城市数字化转型生态三方面提出十二项具体举措。

安全方面，指导意见要求提升城市安全韧性水平。加强城市物理空间安全管理和安全风险态势感知，强化应急广播等城市安全风险预警信息发布手段，围绕“高效处置一件事”，完善城市常态事件和应急事件分类处置流程，打破城市管理条块分割和信息壁垒，构建全链条、全环节联动应急处置体系，实现弹性适应、快速恢复。加强城市数字空间安全管理，健全完善网络安全监测预警和应急处置机制，构建城市网络运行安全管理体系，提升通信网络韧性。加快推进城市数据安全体系建设，依法依规加强数据收集、存储、使用、加工、传输、提供、公开等全过程安全监管，落实数据分类分级保护制度，压实数据安全主体责任。加强个人隐私保护。推进建设有韧性的城市数据可信流通体系，健全数据要素流通领域数据安全实时监测预警、数据安全事件通报和应急处理机制。（来源：中国政府网）

8. 国家能源局印发《电力网络安全事件应急预案》

5 月 16 日，国家能源局印发《电力网络安全事件应急预案》。

文件明确，根据电力网络安全事件造成停电等后果的影响程度，电力网络安全事件分为特别重大、重大、较大和一般四级。电力网络安全事件发生后，事件发生单位应立即启动应急预案，实施处置并立即向其上级电力调度机构、当地派出机构、属地公安部门及当地网信部门报告。全国电力安全生产委员会企业成员单位同时报告国家能源局。发生较大及以上电力网络安全事件的，应 1 小时内报告，一般电力网络安全事件应 12 小时内报告。

后期处置方面，文件要求事件发生单位应查明事件起因、性质、影响、责任等情况，提出防范、整改措施和处理建议，于应急响应结束后 5 天内完成自查，向组织事件调查的机关提交自查报告。事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。（来源：国家能源局）

9. 国家数据局印发《数字中国建设 2024 年工作要点清单》

5 月 21 日消息，国家数据局近日印发《数字中国建设 2024 年工作要点清单》，对 2024 年数字中国建设工作作出部署。

按照《数字中国建设整体布局规划》要求，工作要点围绕高质量构建数字化发展基础、数字赋能引领经济社会高质量发展、强化数字中国关键能力支撑作用、营造数字化发展良好氛围环境四个方面部署重点任务。主

要包括：加快推动数字基础设施建设扩容提速，着力打通数据资源大循环堵点，深入推进数字经济创新发展，健全完善数字政府服务体系，促进数字文化丰富多元发展，构建普惠便捷的数字社会，加快推进数字生态文明建设，加强数字技术协同创新运用，稳步增强数字安全保障能力，不断完善数字领域治理生态，持续拓展数字领域国际合作交流空间。（来源：国家数据局）

10. 四部门发布《互联网政务应用安全管理规定》

5 月 15 日，中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部联合发布《互联网政务应用安全管理规定》，规范各级党政机关和事业单位（简称机关事业单位）建设运行的互联网政务应用。

规定共八章四十四条，涉及信息安全、网络和数据安全、电子邮件安全、监测预警和应急处置、监督管理等方面。规定所称互联网政务应用，是指机关事业单位在互联网上设立的门户网站，通过互联网提供公共服务的移动应用程序（含小程序）、公众账号等，以及互联网电子邮件系统。

网络和数据安全方面，规定要求，建设互联网政务应用应当落实网络安全等级保护制度和国家密码应用管理要求，按照有关标准规范开展定级备案、等级测评工作，落实安全建设整改加固措施，防范网络和数据安全风险。其中，中央和国家机关、地市级以上地方党政机关门户网站，以及承载重要业务应用的机关事业单位网站、互联网电子邮件系统等，应当符合网络安全等级保护第三级安全保护要求。

规定明确，机关事业单位委托外包单位开展互联网政务应用开发和运维时，应当以合同等手段明确外包单位网络和数据安全责任，并加强日常监督管理和考核问责；督促外包单位严格按照约定使用、存储、处理数据。未经委托的机关事业单位同意，外包单位不得转包、分包合同任务，不得访问、修改、披露、利用、转让、销毁数据。机关事业单位应当建立严格的授权访问机制，操作系统、数据库、机房等最高管理员权限必须由本单位在编人员专人负责，不得擅自委托外包单位人员管理使用；应当按照最小必要原则对外包单位人员进行精细化授权，在授权期满后及时收回权限。（来源：中国网信网）

11. 三部门发布《信息化标准建设行动计划（2024—2027 年）》

5 月 29 日，中央网信办、市场监督管理总局、工业和信息化部联合发布《信息化标准建设行动计划（2024—2027 年）》，围绕四方面部署主要任务：

一是建立创新信息化标准工作机制。计划要求完善国家信息化标准体系、优化信息化标准管理制度，以及强化信息化标准实施应用；

二是推进重点领域标准研制。计划要求在关键信息技术、数字基础设施、数据资源、产业数字化、电子政务、信息惠民、数字文化、数字化绿色化协同发展等 8 个重点领域推进信息化标准研制工作。例如，针对关键信息技术，要强化通用技术标准研制和布局新兴技术领域标准；针对数字基础设施，要完善网络基础设施标准、推进算力基础设施标准研制和提升应用基础设施标准化水平；针对数据资源，要强化数据资源基础标准建设

和强化数据资源基础标准建设；针对电子政务，要强化服务业信息化标准、完善政务应用标准建设、加强政务治理标准建设等；

三是推进信息化标准国际化。计划要求深化国际标准化交流合作、国际标准化交流合作和推动国际国内标准协同发展。

四是提升信息化标准基础能力。计划要求优化标准供给结构、加强标准化人才培养和推动标准数字化发展。（来源：中国网信网）

12. 16项网络安全国家标准正式发布

5月9日，全国网络安全标准化技术委员会宣布16项国家标准正式发布，包括《网络安全技术 信息技术安全评估方法》《网络安全技术 软件供应链安全要求》《数据安全技术 应用商店的移动互联网应用程序（App）个人信息处理规范性审核与管理指南》《网络安全技术 网络安全众测服务要求》《网络安全技术 软件产品开源代码安全评价方法》等。（来源：全国网络安全标准化技术委员会）

13. 全国网安标委发布《网络安全技术 软件物料清单数据格式（征求意见稿）》

5月16日，全国网络安全标准化技术委员会发布《网络安全技术 软件物料清单数据格式（征求意见稿）》，为软件供应链相关方之间进行软件物料清单信息的生成、共享和使用提供指引。

征求意见稿针对软件供应链愈发复杂、软件嵌套引用组件数量庞大、国内的软件物料清单建设没有统一规范等问题，制定软件物料清单（SBOM）

格式规范，识别软件组件及其依赖关系，提高软件全生命周期的可见性和透明度，增强软件供应链安全管理能力。

征求意见稿规定软件物料清单数据格式，包括清单组成、文件格式要求和清单元素，以及清单中各元素的属性和属性值格式等信息。征求意见稿明确软件物料清单由基本信息、软件组成信息、外部依赖信息、安全信息、扩展信息和签名信息六大类信息组成，每类信息包括若干清单元素，并对每个清单元素所涉及的字段进行规定。软件物料清单文件格式应支持人类容易理解和解释的需求、支持自动化工具解析处理、支持独立于编程语言的通用格式，以及清单文件的命名应以SBOMDF为后缀等。（来源：全国网络安全标准化技术委员会）

14. 全国网安标委发布《网络安全技术 生成式人工智能服务安全基本要求（征求意见稿）》

5月23日，全国网络安全标准化技术委员会发布《网络安全技术 生成式人工智能服务安全基本要求（征求意见稿）》，细化《生成式人工智能服务管理暂行办法》中的安全要求，旨在帮助服务提供者明确生成式人工智能服务网络安全基线、提高服务安全水平。

征求意见稿针对当前生成式人工智能服务面临的网络安全、数据安全、个人信息保护等关键问题，提出覆盖服务全生命周期的安全要求，防范化解服务过程中的应用场景安全风险、软硬件环境安全风险、生成内容安全风险以及权益保障安全风险等。其中，针对生成式人工智能服务上线前的模型研发过程，征求意见稿重点关注训练数据来源安全、训练数据内容安

全、数据标注安全，以及模型安全。针对面向公众开放后的服务提供过程，征求意见稿重点关注在提供服务过程中应采取的安全措施。（来源：全国网络安全标准化技术委员会）

15. 全国网安标委发布《网络安全技术 关键信息基础设施边界确定方法（征求意见稿）》

5 月 30 日，全国网络安全标准化技术委员会发布《网络安全技术 关键信息基础设施边界确定方法（征求意见稿）》，指导关键信息基础设施运营者确定关键信息基础设施边界，及关键信息基础设施安全保护其他相关方使用。

征求意见稿给出关键信息基础设施边界确定方法，包括基本信息梳理、关键信息基础设施功能识别、关键业务链与关键业务信息识别、关键业务信息流识别与资产识别、关键信息基础设施要素识别和边界确定的流程、步骤等内容。（来源：全国网络安全标准化技术委员会）

16. 自然资源部（国土）就智能网联汽车时空数据安全发布两项强制性国家标准征求意见稿

5 月 21 日，自然资源部（国土）发布两项强制性国家标准《智能网联汽车时空数据安全处理基本要求（征求意见稿）》《智能网联汽车时空数据传感系统安全基本要求（征求意见稿）》。

《智能网联汽车时空数据安全处理基本要求（征求意见稿）》规定，智能网联汽车处理位置类数据和构图类数据时，应在存储和向车外传输前

按照国家认定的地理信息保密处理技术完成处理。其中，车端不应存储：（1）军事禁区、军事管理区及其内部的建筑物、构筑物和道路；（2）武器弹药、爆炸物品、剧毒物品、麻醉药品、精神药品、危险化学品、铀矿床和放射性物品的集中存放地，核材料战略储备库、核武器生产地点及储备品种和数量，高放射性废物的存放地，核电站；（3）国家安全等要害部门；（4）军民合用机场、港口、码头的重要设施；（5）监狱、看守所、拘留所、强制隔离戒毒所和强制医疗所（名称除外）；（6）国家战略物资储备库、中央储备库（名称除外）；（7）公路的路面铺设材料；（8）国家禁止公开的其他信息等目标的构图类数据。

《智能网联汽车时空数据传感系统安全基本要求（征求意见稿）》规定，时空数据传感器指的是安装在智能网联汽车上，采集、存储、向车外传输时空数据的器件或装置。时空数据包括具有时间、空间特征的地理信息数据。标准要求时空数据传感器应具备独立的、可检测的关闭功能。时空数据传感系统的存储模块和向车外传输模块在运行时，应具备地理信息保密处理功能，并应符合国家认定的地理信息保密处理技术要求。针对其存储功能，要求时空数据传感系统外部接口（USB 接口、诊断接口和其他接口等）应具有访问控制和身份鉴别的机制，确保存储的时空数据不被任意获取。（来源：自然资源部（国土））

（三）地方层面动向

1. 福建印发《2024 年数字福建工作要点》

4 月 30 日，福建省数字福建建设领导小组印发《2024 年数字福建工作要点》。文件围绕着力夯实数字福建发展基础、坚持“五位一体”全面赋能、强化数字化发展两大关键能力、营造良好数字化发展环境、健全保障措施五方面部署十四项主要任务。

安全方面，文件要求提升公共数据安全防护能力。建设省一体化公共数据平台监测监管系统，加强公共数据基础平台安全防护，完善数据全生命周期防护体系。规范公共数据开发主体活动，完善一级开发行业管理，常态化开展数据安全隐患自查自纠。持续深化信息技术应用创新。在数字政府建设、重要行业领域信息化建设、关键信息基础设施保护中落实安全可靠技术和产品应用要求，持续提升自主可控的数字安全能力。制定实施支持信创产业高质量发展若干政策措施，推动信创产业高质量发展。加快推进密码应用安全。完成福建省政务云统一商用密码服务平台建设，推动省级重要政务信息化系统加快接入。落实“三同步一评估”要求，提升密码体系化应用覆盖率。（来源：网信福建）

2. 天津印发《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》

5 月 8 日，中国（天津）自由贸易试验区管理委员会、天津市商务局印发《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》。

《负面清单》列明天津自贸试验区企业向境外提供数据需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形。天津自贸试验区企业向境外提供《负面清单》外的数据免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。涉及国家秘密的数据、核心数据、政务数据不纳入《负面清单》管理，相关数据出境按照有关法律、法规和规定执行。

《负面清单》明确共计 13 大类、45 项小类数据，需要通过数据出境安全评估，包括：（1）战略物资和大宗商品类，包括石油、石化、天然气、农产品；（2）自然资源和环境类，包括基础地理信息、遥感影像、气象等；（3）工业类，包括国防军工、化学工业等；（4）金融类，包括银行、保险、融资租赁；（5）统计类，包括经济统计、社会统计；（6）通信传播类，包括电信、新媒体等；（7）住房建设类，包括住房公积金；（8）交通运输类，包括邮政、交通；（9）公共卫生类，包括食品、药品、疾控数据等；（10）公共安全类，包括物理安全、网络安全、应急管理；（11）互联网服务和电子商务类，包括服务外包、互联网平台服务；（12）科学

技术类，包括出口管制物项、禁止出口限制出口技术等；（13）个人信息。（来源：天津市商务局）

3. 北京发布《2024 年度北京地区电信和互联网行业数据安全管理实施方案》

5 月 10 日，北京市通信管理局发布《2024 年度北京地区电信和互联网行业数据安全管理实施方案》。方案明确推进北京地区电信和互联网行业数据安全管理工作的总体目标、组织方式、重点任务、工作要求。

方案在总体目标中提出，将组织开展北京地区电信和互联网行业“三提升一示范”专项行动，着力加强北京地区数据安全风险治理能力、数据安全事件应急处置能力、数据安全管理能力。

方案提出四项重点任务，分别是持续推进数据安全风险治理能力提升、全面助力数据安全事件应急处置能力提升、重点推进行业数据安全管理能力全面提升、部署开展数据安全管理和应用试点示范。

其中，北京市通信管理局将推动数据安全风险评估制度全面落地实施。在 2023 年数据安全风险评估试点的基础上，对名录内已备案重要数据的企业全面部署风险评估工作要求，解读数据安全风险评估制度要求和方法模型，严格开展评估报告备案审核，敦促企业系统性、综合性、全面性识别数据安全风险，并针对性开展风险处置，有效防范化解重大风险。

此外，北京市通信管理局还将深入开展数据安全风险隐患排查与监督检查。统筹基础电信企业考核、“双随机一公开”“数安护航”专项行动等工作，科学设计风险排查与监督检查方案，以“重点对象回头看、重点

要求督落实，热点事件深入查”为原则，针对合作方管理、权限管理、用户数据使用安全、数据中心和云业务安全、大模型数据安全等重点场景，采用现场检查、远程技术监测、随机飞行检查等多种检查方式，全面排查数据安全风险问题，切断风险源头。（来源：北京通信业）

4. 海南发布《海南自由贸易港数字经济促进条例（草案·公开征求意见稿）》

5 月 14 日，海南省工业和信息化厅发布《海南自由贸易港数字经济促进条例（草案·公开征求意见稿）》。草案共八章二十五条，涉及数字产业化、产业数字化、数据要素、数字经济安全和治理数字化等内容。

草案规定，数字经济是指以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进公平与效率更加统一的新经济形态。

草案要求，引进跨国公司和大型互联网企业在海南自由贸易港建设数据中心，探索发展国际数据中心，支持开展跨境数据处理、算力租售等服务。推动建设算网融合的新型互联网交换中心。积极部署人工智能基础设施，支持建设面向海南特色行业应用的算法模型平台和数据集，推动人工智能赋能新型工业化、智慧旅游等重点领域升级，鼓励依托跨境专线开展跨境人工智能训练和应用服务。

草案规定，县级以上人民政府及有关部门应当落实数字经济发展过程中的网络安全保障责任，建立网络安全风险评估、监测预警和应急处置机制，加强对重要网络、信息系统和硬件设备安全保障。鼓励使用自主可控

产品，提高产业链供应链韧性。海南自由贸易港应当在国家数据跨境传输安全管理制度框架下，建立数据跨境流动管理机制，探索推行数据跨境流通“负面清单”制度，加快实现医疗、航天、深海、贸易、投资、教育、旅游、金融等领域数据跨境安全有序流动。（来源：海南省工业和信息化厅）

5. 广东印发《数字广东建设 2024 年工作要点》

5 月 15 日，广东省政务服务和数据管理局印发《数字广东建设 2024 年工作要点》，围绕十三个方面部署主要任务。

安全方面，文件提出加强网络和数据安全管理，筑牢安全防线。一是健全安全工作机制。推动建立健全数字广东全方位网络安全联防联控机制，加强党政机关（事业单位）网络安全工作调度协调，健全“粤数安”安全运营中心工作机制。加强网络和数据安全信息共享通报，开展数字政府网络安全指数评估工作，强化考核评估结果运用。

二是强化网络安全保护。建立党政机关（事业单位）重要网络、系统、核心数据台账，加强关键信息基础设施安全保护。建设网络和数据安全信息采集汇聚平台，强化省、市一体化网络安全运营，加强保密审查，积极防范数据关联分析和数据汇聚产生的失泄密风险。组织开展网络安全实战攻防演练，持续开展“粤盾”攻防演练活动。

三是加强数据安全管理。健全数据安全管理体系，推动建立数据分类分级保护制度，完善数据安全监测预警和应急处理机制。加快推动密码应用，增强数据安全保障能力。常态化开展安全培训、测评、检查、审计、

漏洞排查和供应链安全管理。组织开展全省政务 APP 数据安全专项演练活动。（来源：广东政数）

6. 浙江印发《关于推进浙江数商高质量发展的实施意见》，重点培育数据安全服务

5 月 15 日，浙江省制造业高质量发展（数字经济发展）领导小组办公室印发《关于推进浙江数商高质量发展的实施意见》，明确浙江数商培育对象，围绕做强数商企业群体、提升数商发展能力、推动数商深度赋能、强化标准规范导引、优化数商发展生态、做强发展支撑平台六个方面提出十五项重点任务。

实施意见指出，要重点培育数据安全服务，主要包括为保障数据持续处于有效保护、合规利用、有序流通状态提供数据安全技术、产品、服务等业务。重点支持浙江数商从事针对数据全生命周期提供敏感数据识别、API 安全管理、数据加密、数据脱敏、数据防泄漏、隐私计算、量子保密、监测预警、安全管理咨询等数据安全保障业务。（来源：浙江省经济和信息化厅）

7. 上海临港新片区发布三个领域《数据跨境场景化一般数据清单》

5 月 16 日，中国（上海）自由贸易试验区临港新片区管理委员会发布《中国（上海）自由贸易试验区临港新片区智能网联汽车领域数据跨境场景化一般数据清单（试行）》《中国（上海）自由贸易试验区临港新片区生物医药领域数据跨境场景化一般数据清单（试行）》《中国（上海）自

由贸易试验区临港新片区公募基金领域数据跨境场景化一般数据清单（试行）》（简称“一般数据清单”）。

一般数据清单包含智能网联汽车、公募基金、生物医药三个领域，涉及智能网联汽车跨国生产制造、医药临床试验和研发、基金市场研究信息共享等11个场景，划分成64个数据类别600余个字段。其中，智能网联汽车领域包括跨国生产制造、全球研发测试、售后服务、二手车全球贸易4个场景；公募基金领域包括市场研究、内部管理2个场景；生物医药领域包括临床试验和研发、药物警戒和医疗器械不良事件监测、医学问询、产品投诉、商业合作伙伴管理5个场景。

数据处理者可向临港新片区管委会申请咨询一般数据清单各数据类别项下的数据字段，并按照《中国（上海）自由贸易试验区临港新片区数据跨境流动一般数据清单操作指南（试行）》的管理要求开展数据跨境流动。（来源：上海临港）

8. 山东省济南市发布《济南市推动数据要素市场化配置改革 加快数字经济发展行动方案（2024—2025年）（征求意见稿）》

5月20日，山东省济南市大数据局发布《济南市推动数据要素市场化配置改革 加快数字经济发展行动方案（2024-2025年）（征求意见稿）》。

征求意见稿主要包括总体要求、工作目标、重点工作三部分。其中，工作目标提出构建数据要素市场化流通体系、持续提升算力支撑能力、探索推进数据基础设施建设、培育数商发展、推动数据要素相关产业发展五个具体目标。

征求意见稿明确十方面重点工作任务，包括成立数据要素流通服务中心、开展数据要素产权登记、推进公共数据授权运营、培育数商生态、开展“数据要素×”行动、推进人工智能数据应用体系建设、强化数据要素相关政策支持等。其中，提出拟制定多项制度文件，如《济南市数据登记暂行办法》《济南市政务元数据规范》《济南市公共数据开放利用办法》《济南市行政事业单位数据资产管理试点实施方案》《济南市公共数据授权运营指南》。（来源：济南市大数据局）

9. 内蒙古公布《内蒙古自治区数字经济促进条例》

5 月 30 日，内蒙古自治区第十四届人民代表大会常务委员会第十次会议通过《内蒙古自治区数字经济促进条例》。条例共九章七十七条，涉及数字基础设施建设、数据资源开发利用、数字产业化、产业数字化、治理数字化、 数字经济安全内容。

条例要求，自治区人民政府及科技、工业和信息化、市场监督管理、数据管理等有关部门应当统筹规划软件产业发展，推进软件产品更新迭代、适配测试和产业化应用，构建安全可控、共建共享的软件产业生态。旗县级以上人民政府及发展改革、商务、市场监督管理、数据管理等有关部门应当培育互联网平台企业，支持利用互联网平台推进资源集成共享和优化配置。依法明确平台企业定位和监管规则，促进平台经济和共享经济规范有序健康发展。

安全方面，条例规定，数据的采集人、持有人和使用人应当采取技术手段和其他必要措施，确保其收集储存的数据安全，防止数据泄露、篡改、

丢失。发生或者可能发生数据泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知用户和相关权利人，并向有关信息监管部门报告。旗县级以上人民政府及公安机关等有关部门应当依法加强对个人信息数据收集、存储、使用、加工、传输、提供、公开等活动的监管，查处危害个人信息安全的违法活动。（来源：内蒙古自治区工业和信息化厅）

10. 湖南公布《湖南省数字经济促进条例》

5 月 30 日，湖南省人民代表大会常务委员会公布《湖南省数字经济促进条例》。条例共二十六条，涵盖数字基础设施建设、数据资源开发利用、数字技术和数字生态创新、数字产业化和产业数字化以及为数字经济提供支撑保障等内容。

数据资源开发利用方面，条例一方面强调政府及其部门的作用，要求县级以上人民政府及其有关部门应当编制公共数据开放目录，依法依规、分类分级开放公共数据，加强公共数据治理和运营，有序推动公共数据资源开发利用。另一方面，条例要求加强对企业和其他组织的引导，明确引导企业和其他组织通过产业政策引导、社会资本引入、应用模式创新、强化合作交流等方式，依法有序开放自有数据资源。

安全方面，县级以上人民政府及其有关部门应当履行安全保障职责，健全安全风险评估和安全保障制度，建立监测预警和应急处置机制，采取安全保障措施，保护数据、网络以及相关设施、设备等方面的安全。县级以上人民政府及其有关部门应当建立健全与数字经济发展相适应的服务与监管体系，完善有关标准体系、评价体系，创新基于数字技术手段的数字

经济监管模式，对数字经济领域新技术、新产业、新业态、新模式实行包容审慎监管，建立相应容错免责机制，提高数字经济监管和治理水平，优化数字经济营商环境，完善数字经济治理体系。（来源：湖南省人民政府、湖南人大）

境内前沿观察三：治理实践

导读：5 月，重庆市南岸区警方公布“胖猫”案件调查细节，系“胖猫”姐姐刘某通过抖音账号多次发布“胖猫”与其女友谭某的私聊记录、转账截图等个人隐私信息。后又在发布怀念“胖猫”信息时，采取另注册账号在评论区点评引导、邀约亲友跟评的方式，继续曝光谭某相关地址、抖音账号等信息。刘某的行为导致谭某被网民攻击辱骂，网络出现多起威胁谭某人身安全的言论，严重影响谭某正常生活，并造成网络空间秩序混乱。目前，刘某认识到自己行为的违法性并认错，警方将根据进一步的调查情况依法作出处理。

广东省、浙江省、天津市网信办公布网络执法工作成效。广东省网信系统 2024 年第一季度依法约谈网站平台 48 家，警告 7 家，罚款处罚 10 家，下架移动互联网应用程序 46 款，会同全省通信管理局等部门依法处置违法违规网站 17 家。浙江省网信部门 2024 年 5 月聚焦网络直播、短视频等领域乱象，依法依规约谈网站账号 22 个，责令整改网站平台 46 家，注销网站备案 27 家，开展行政检查、行政指导 57 次，对 8 家无备案或虚假备案的网站移交省通信管理局作进一步处置。天津市网信部门 2024 年 4 月督促属地网站平台清理各类违法和不良信息 31637 条、平台依据用户服务协议处置违规账号 12163 个；依法约谈、警告网站、账号 24 家，取消网站许可、备案 140 家，移送相关部门线索 8 条。

浙江省通信管理部门公布依法治网工作情况。杭州亚运会期间，累计监测拦截DDoS攻击流量535T，处置移动恶意程序和僵木蠕攻击56万次，封堵高危IP 4200个，圆满完成保障任务。提升行业网络安全防护能力方面，2023年累计处置网络安全威胁6.3万个，印发工业互联网安全预警通报53期，完成20个车联网平台定级备案审核。

此外，服务型政府的治理思路更加凸显。上海市网信办会同市市场监管局组织开展“咖啡消费场景下个人信息保护”合规指导会，围绕6大类违法违规问题以案释法，开展普法教育，下发《咖啡消费场景下常见个人信息保护问题自查清单》；北京市网信部门会同交通部门推行停车缴费“安心码”，确保商家必须遵循个人信息收集最小必要原则，有效避免诱导或强制收集消费者个人信息等违规行为；杭州互联网法院发布《引导企业数据健康发展行为指引》，聚焦市场主体在大数据产业发展中的热点和难点问题，引导企业数据健康发展。

关键词：“胖猫”案件、网络执法工作成效、服务型政府

（一）公安机关治理实践

1. 浙江杭州上城警方打掉一出售应聘者简历信息的犯罪团伙，涉案简历数据 26 万条

5 月 6 日消息，浙江省杭州市上城网警近日打掉一出售应聘者简历信息的犯罪团伙，涉案招聘简历信息数据 26 万条。

本案中，上城网警在工作中发现，有人利用某招聘平台注册公司非法收集应聘者简历信息。经调查，2023 年 11 月，意图出售手中掌握的简历信息的某公司 HR 边某在其亲戚袁某的拉拢下加入一条由杭州本地辐射安徽、河南、贵州等地包括多层级料商在内的为境外诈骗团伙提供黑料的灰产链。黎某与邓某二人也在边某亲戚拉拢下成为下线，利用所开的人力资源公司招聘收集更多简历，以此牟利。这几人从未见过面，所有的交易通过微信进行。在上线的鞭策下，几人开始通过伪造公章和营业执照，注册虚假企业并在招聘软件投放虚假招聘广告的方法来获得更多简历。袁某还提供专门的简历提取软件，可以批量收集平台简历。几人在社交群组进行公开出售，甚至利用境外软件勾结境外诈骗团伙大量出售应聘者信息。

近日，杭州上城网警集结警力开展集中收网行动。行动抓获袁某杰、郭某波等犯罪嫌疑人 11 名（刑拘 5 名），查获伪造印章 21 枚、伪造工商营业执照 27 张，扣押涉案泰达币 19 万枚（折合人民币 136 万元），固定招聘简历信息数据 26 万条。目前案件还在进一步办理中。（来源：公安部网安局）

2. 辽宁警方打掉一利用 AI 技术帮助境外电诈犯罪洗钱的犯罪团伙，涉案金额 7000 万元

5 月 11 日消息，辽宁警方近日成功打掉一个利用 AI 技术制作人脸识别验证视频，帮助境外电诈犯罪分子洗钱的犯罪团伙。

前段时间，辽宁网安部门接到群众报案，称自己的银行账户里少了三千块钱，还多了几笔向陌生账户转账的记录。接到线索后，辽宁网警迅速开展工作。在侦查过程中，网安部门又多次接到类似警情，都是以零零散散的方式向陌生账户转账，金额不等，大多在 5 万元以下。警方意识到，这很有可能是一起有组织有预谋的团伙作案。

经过几个月的持续侦查，一个以 AI 技术为支撑的犯罪团伙浮出水面。该犯罪团伙以任某某为头目，4 名“信息员”“联络员”为骨干成员，另有 27 名“辅助人员”进行支撑。他们责任分工明确，由“信息员”赵某某与刘某某负责收购载有公民面部照片、手机号、银行卡号的公民个人信息三要素；“联络员”刘某负责联系境外不法分子“秋某”售卖这些要素；“秋某”则利用 AI 软件将人脸图片做成人脸识别验证视频，连同手机号及银行卡号，打包卖给境外赌博或电信网络诈骗组织牟取利益。因嫌疑人具有一定的反侦察意识，不仅使用境外即时聊天工具勾结联络，还定期删除聊天记录，同时也频繁更换住所。

近期，辽宁网安抽调 20 余名干警，奔赴 2 省 5 市，将犯罪嫌疑人全部抓捕归案。经查，该团伙非法收购公民面部照片 50 余个，银行卡、电话卡

100 余张，帮助境外电诈犯罪分子洗钱流水 7000 万元并从中非法获利。（来源：公安部网安局）

3. 重庆南岸区警方公布涉及侵犯个人隐私“胖猫”案件调查细节

5 月 19 日，重庆市公安局南岸区分局发布“胖猫”事件调查情况。今年 4 月 11 日，一位网名叫“胖猫”的男子因感情问题在重庆跳江身亡，该事件随后在网络上持续发酵，“胖猫”女友谭某被视为利用感情骗取钱财，网上出现大量针对谭某的人肉搜索、造谣、谩骂等行为。

根据警方调查，谭某（女，27 岁，重庆石柱人）和刘甲（男，21 岁，网名“胖猫”，湖南临武人）以真实身份交往两年多，互见亲友，并在一定范围公开双方恋爱关系，经济上互有往来，共同攒钱谋划未来生活，双方存在真实恋爱关系，谭某未实施虚构事实或隐瞒真相、以恋爱为名骗取“胖猫”财物的行为，不构成诈骗犯罪。

5 月 11 日，重庆市公安局南岸区分局对刘乙（女，28 岁，湖南临武人，“胖猫”姐姐，下文以“刘某”代称）报案称谭某诈骗其弟“胖猫”钱财依法作出不予立案决定，刘某对不予立案决定表示认可。同时，经调解，近日刘某父母与谭某已达成和解，谭某全额退还了与“胖猫”恋爱期间经济往来的差额。

警方经依法调查查明，“胖猫”跳江后，刘某翻阅“胖猫”遗留的手机后，通过抖音账号多次发布“胖猫”与谭某私聊记录、转账截图等个人隐私信息。后又在发布怀念“胖猫”信息时，采取另注册账号在评论区点评引导、邀约亲友跟评的方式，继续曝光谭某相关地址、抖音账号等信息。

刘某的行为导致谭某被网民攻击辱骂，网络出现多起威胁谭某人身安全的言论，严重影响谭某正常生活，并造成网络空间秩序混乱。调查过程中，刘某认识到自己行为的违法性并认错，警方将根据进一步的调查情况依法作出处理。（来源：新华网）

4. 四川泸州市警方破获一起涉民营企业黑客攻击案，成功解密恢复 16TB 数据

5 月 21 日消息，四川省泸州市公安机关网安部门近日成功侦破一起涉民营企业黑客攻击案。

2024 年 2 月 1 日，泸州市江阳区某摄影公司发现公司电脑硬盘被加密，技术人员多次尝试解密和数据恢复均以失败告终，导致公司业务全面停滞，面临客户投诉、高额违约金、数据泄露和倒闭的风险。公司内部排查无果，遂报警。

经泸州市公安机关网安部门调查，最终锁定犯罪嫌疑人罗某斐。罗某斐精通电脑，就职于某科技公司，负责向全国多家摄影公司提供软件及维护服务。为报复该摄影企业拒绝购买其推销的设备，罗某斐通过远程控制系统，恶意加密锁定摄影公司服务器硬盘，导致系统无法正常使用。罗某斐还利用此类手段，控制全国各地摄影公司服务器电脑终端 90 余台。

在泸州市公安机关网安部门的帮助下，摄影公司已成功解密恢复数据 16TB，挽回经济损失一百万余元。目前，犯罪嫌疑人罗某斐被依法采取强制措施，案件正在进一步侦办中。（来源：公安部网安局）

5. 内蒙古鄂尔多斯市警方打掉一个网络水军团伙，13 人获刑

5 月 23 日消息，内蒙古鄂尔多斯市准格尔旗人民法院近日对审理的一起涉网恶势力案件进行公开宣判，13 名被告人因犯敲诈勒索罪、强迫交易罪、非法经营罪、妨害作证罪分别被依法判处有期徒刑 10 年 6 个月至 11 个月不等，并处人民币 24.19 万元至 2 千元不等罚金。

2022 年 7 月底，鄂尔多斯市网安部门接到上级线索：网民“马某某”通过新浪微博发布涉某企业大量负面信息，并涉嫌敲诈勒索。接报后，鄂尔多斯市网安部门依据该线索进行专案经营，并会同属地准格尔旗公安局成立联合工作专班开展深入调查。

经查，以宋某为首的犯罪团伙盘踞在陕西、山西和内蒙古等省份，在 2021 年至 2023 年 1 月期间，利用各类自媒体平台发布、转载企业负面帖文，进而对企业实施敲诈勒索等违法犯罪活动。该团伙结构清晰、组织严密，在实施犯罪过程中，由宋某统一指挥、管理，并按照其意志给团伙成员分赃。该团伙成员将自己伪装成新闻工作者，并在其注册的 30 多个网络自媒体账号撰写发布厂矿企业不实信息，再通过互相转发等方式扩大影响，迫使企业“花钱删帖”，大肆实施敲诈勒索、非法经营等犯罪活动。

该团伙在内蒙古、陕西等地疯狂作案 20 多起，以网络为载体，捏造夸大事实，集体成员间相互交叉作案，充当“网络水军”，严重扰乱经济、社会、生活秩序，造成较为恶劣的社会影响。先后有 30 余家厂矿企业遭受该犯罪团伙敲诈勒索、强迫交易，涉案金额达 1200 万元。

该案通过信息网络实施犯罪，整个犯罪链条、空间突破传统犯罪的地域时空限制，渗透力强、波及面广、受害企业多，危害大。专案组民警辗转陕西、甘肃、山西、河北、河南及内蒙古等6省区25个市县调查取证，行程10余万公里，成功抓获以宋某为首的恶势力网络水军犯罪团伙成员16人，破获刑事案件26起，为受害企业避免损失910万元，冻结涉案资金20.8万元，追赃8.35万元。（来源：公安部网安局）

6. 云南怒江市警方侦破一起破坏计算机信息系统案

5月29日，云南省怒江市警方公布近期侦破的一起破坏计算机信息系统案件细节。

2024年3月4日，怒江网警接到报警，某小区网络瘫痪，门禁系统、视频监控系统、停车收费系统失灵，业务被迫中断，造成财产损失。经警方调查，犯罪嫌疑人为此前与该小区物业合作的一信息技术有限公司离职员工马某某。马某某因与信息技术有限公司存在劳资纠纷，遂临时起意，通过小区一弱电井连接笔记本电脑，清除系统的配置信息，导致小区计算机系统瘫痪，与之相连的监控系统、门禁可视电话系统、地下停车管理系统均无法正常运转。

马某某因涉嫌违反《刑法》第286条破坏计算机信息系统罪，已移送人民检察院审查起诉。（来源：云南网警）

7. 山东青岛市警方发布四起网络暴力典型案件

5 月 31 日，山东省青岛市警方发布一起涉网络暴力刑事案件和三起涉网络暴力行政案件。

案件一：主播侮辱致网友自杀。2023 年 4 月份开始，一名为“青岛薛姐”的主播开直播对贾某某进行持续辱骂。10 月 11 日晚，贾某某因不堪受辱，精神崩溃，用修眉刀割腕自杀，后被就医抢救。近日，“青岛薛姐”薛某某（女）依法受到刑事处罚。

案例二：吸粉博眼球开地域黑。2023 年 12 月至 2024 年 5 月，李某某为了增加其粉丝数量、提升账号关注度，通过 APP 账号多次发表关于抹黑河南人，引起“地域黑”的负面信息和评论，造成恶劣影响。近日，李某某因寻衅滋事被依法行政处罚。

案例三：拼接视频传播淫秽。2024 年 1 月至 2024 年 5 月，在多个社交平台出现李某某的裸照及不雅视频，称李某某私生活不检点，引发大量网民热议，对李某某正常生活及个人名誉造成恶劣影响。经查，照片及视频系违法行为人孙某某经过软件拼接处理，上传至网络进行传播。近日，孙某某被依法行政处罚。

案例四：恶意造谣中伤他人。2023 年 12 月，名为“帅哥一枚”的网民发布视频称一名市民出轨抛弃结发妻，欠钱不还，早晚遭报应。经查，违法行为人李某某发布上述谣言视频，视频内容对报案人造成不良影响，构成诽谤。近日，李某某被依法行政处罚。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办发布第十五批境内区块链信息服务名称及备案编号

5 月 16 日，中央网信办发布第十五批共 74 个境内区块链信息服务名称及备案编号。根据《区块链信息服务管理规定》，区块链信息服务提供者应当在提供服务之日起十个工作日内通过国家互联网信息办公室区块链信息服务备案管理系统填报服务提供者的名称、服务类别、服务形式、应用领域、服务器地址等信息，履行备案手续。区块链信息服务提供者未履行备案手续或者填报虚假备案信息的，由国家和省、自治区、直辖市互联网信息办公室依据职责责令限期改正；拒不改正或者情节严重的，给予警告，并处一万元以上三万元以下罚款。（来源：中国网信网）

2. 广东省网信部门：2024 年第一季度约谈网站平台 48 家

5 月 7 日，广东省网信办通报 2024 年第一季度网络举报处置与执法情况。2024 年第一季度，广东省网信系统受理处置网络举报线索 8000 余件，依法约谈网站平台 48 家，警告 7 家，罚款处罚 10 家，下架移动互联网应用程序 46 款，会同全省通信管理局等部门依法处置违法违规网站 17 家。同步公布七起行政执法典型案例。（来源：网信广东）

3. 上海市委网信办“清朗浦江·2024”网络生态治理旬行动

5 月 10 日，由上海市网信办主办、区委网信办承办的为期十天的上海市“清朗江·2024”网络生态治理旬行动正式启动。

本次网络生态治理旬行动期间，总计将开展28项凸显生态治理特色的主题日和网站开放日活动。特色主题日包括优化营商网络环境主题日、“自媒体”治理主题日、反对网络暴力主题日、防范非法证券期货活动主题日和未成年人网络保护主题日，与今年上海市委网信办聚焦网络营商环境、“自媒体”、网络暴力、未成年人网络保护等重点领域的“清朗浦江”五大专项整治行动紧密结合。（来源：网信上海）

4. 上海市网信办、市市场监管局联合举办咖啡行业合规指导和普法培训

5月10日，上海市网信办会同市市场监管局组织开展“咖啡消费场景下个人信息保护”合规指导会，星巴克、瑞幸咖啡、Manner Coffee、麦咖啡、Tims天好咖啡、挪瓦咖啡、COSTA COFFEE 、M Stand、Seesaw Coffee、niiice café、Peet's Coffee、库迪咖啡等24家连锁咖啡企业负责人参加，涉及全市超过3600家门店。

上海市网信办以前期网民举报、巡查发现的问题线索以及典型案例为抓手，围绕企业强制或默认消费者同意隐私政策，隐私政策缺失、不实或不完整，强制或频繁诱导收集精准位置信息，诱导收集手机号码或关注公众号，未提供关闭定向推送，未提供删除个人信息渠道等6大类违法违规问题以案释法，开展普法教育。要求咖啡企业提高个人信息保护意识，履行个人信息保护义务，严格遵循个人信息收集“最小必要”“告知同意”原则，认真对照梳理下发的《咖啡消费场景下常见个人信息保护问题自查

清单》进行自查整改，采取有效措施确保个人信息收集、存储、使用、删除等全生命周期合法合规。（来源：网信上海）

5. 上海市委网信办等四部门联合开展打击网上非法证券期货行为专项行动

5 月 15 日，上海市委网信办、上海证监局、上海市检察院、上海市公安局四部门联合开展“清朗浦江·e 企共治”打击网上非法证券期货行为专项行动。

专项行动将督促上海属地东方财富网、小红书、哔哩哔哩等重点网站平台开展全面自查，集中删除、屏蔽“非法推荐股票、基金、期货”“股市黑嘴”“场外配资”等违法活动信息，对相关账号采取阶梯处置措施。建立健全证券期货基金违法活动信息日常监测、清理长效机制，对以“暗语”、图片等形式传播的非法外链信息加大识别打击力度，切断证券期货基金违法活动信息网络传播渠道；探索当用户在搜索、群聊、私信等环节发布上述内容时，网站平台自动推送警示提醒信息。

同时，专项行动强化证券、期货投资咨询业务“亮牌”执业监管要求。要求属地网站平台落实主体责任，有关账号在发表证券、期货投资咨询文章、报告或者意见时，要在前台“亮牌”执业。加强对“亮牌”信息的实质性审核，通过要求账号注册人提供所在证券、期货投资咨询机构相关信息、上传个人执业资质等方式，加强与公示从业信息的比对。比对不一致的，要求限期整改，完成整改前暂停其证券、期货投资咨询信息发布功能。（来源：网信上海）

6. 北京、上海网信部门公布生成式人工智能服务已备案信息

5 月 15 日，北京网信办发布 19 款生成式人工智能服务已备案信息。涉及的主要公司及产品有：快手“可图”、小米公司“小米”、腾讯云“行业大模型”、高德“千寻”、爱奇艺“奇智”及海尔“HomeGPT”等。

20 日，上海市网信办发布《生成式人工智能服务已备案信息公告》。截至 5 月 20 日，上海市新增 1 款已完成备案的生成式人工智能服务，是上海携程商务有限公司的“问道”模型。目前累计已完成 29 款生成式人工智能服务备案。

已上线的生成式人工智能应用或功能，应在显著位置或产品详情页面公示所使用已备案生成式人工智能服务情况，注明模型名称及备案号。（来源：网信上海、网信北京）

7. 北京市网信办等部门聚焦十大领域扫码缴费场景，开展“清朗•长安”个人信息保护行动

5 月 28 日消息，北京市网信办联合市交通委、市商务局、市市场监管局等部门聚焦十大领域扫码缴费场景，开展“清朗•长安”个人信息保护行动，以解决用户个人信息被商家过度采、强制要、诱导取的情况比较突出问题。截至目前，682 家停车场已实现停车缴费“安心码”改造。

由网信部门会同交通部门推行的停车缴费“安心码”，提供直接缴费渠道，扫码后只需要输入车牌号、点击缴费 2 个步骤，就可以完成缴停车费。对于有会员优惠服务的商家，在提供直接缴费的基础上，还可以提供

会员优惠缴费通道。“安心码”的设计确保商家必须遵循个人信息收集最小必要原则，有效避免诱导或强制收集消费者个人信息等违规行为。

北京市从“十大场景”之一的经营性停车场扫码缴费场景开展宣传治理，后期还将针对餐饮、商超、酒店、影院、剧院、景区、理发、公园、洗衣等涉及人民群众日常生活消费的领域扫码缴费场景，扎实开展“清朗·长安”个人信息保护行动。下一步，“安心码”将在全市开展扫码缴费经营活动的公共停车场全面推行。市区两级网信、交通、商务、市场监管等部门将持续跟踪问效，定期对停车缴费“安心码”落实情况进行巡查抽查，并接受公众举报监督，防止违法违规问题隐形变异和反弹回潮。（来源：北京日报）

8. 浙江省网信部门：5 月开展行政检查、行政指导 57 次

2024 年 5 月，浙江省网信部门聚焦网络直播、短视频等领域乱象，依法依规约谈“乐刻”“悟饭游戏厅”等网站账号 22 个，责令整改“护工来啦”“超维信息”等网站平台 46 家，注销“智能单”“同城约炮”等网站备案 27 家，开展行政检查、行政指导 57 次。网信部门及属地重点平台总计受理处置网民举报 6.2 万件，对 8 家无备案或虚假备案的网站移交省通信管理局作进一步处置。（来源：网信浙江）

9. 天津市网信部门：4 月清理各类违法和不良信息 31637 条

5 月 17 日，天津市委网信办通报“海河净网 2024”4 月份网络生态治理成果。

2024 年 4 月，天津市委网信办持续深入开展“海河净网”网络生态治理系列专项行动，围绕自媒体乱象、网络谣言、侵害企业和未成年人合法权益等影响网络生态的突出问题开展集中整治。全市各级网信部门督促属地网站平台清理各类违法和不良信息 31637 条、平台依据用户服务协议处置违规账号 12163 个；依法约谈、警告网站、账号 24 家，取消网站许可、备案 140 家，移送相关部门线索 8 条；受理违法和不良信息举报 5.82 万余件，处置侵权举报信息 2554 条。

其中，属地网站“宇恩源科技”“东方席居装饰”等因长期放弃运营被篡改发布色情、赌博信息，依法予以注销；属地平台依据用户服务协议对发布低俗色情、电信诈骗和恶意营销广告的“悦悦”“夜场”“独角兽”“薇薇看世界”“海外助孕”等账号予以封禁处置。报请国家有关部门对发布涉相关案事件虚假谣言信息、涉天津市殡葬不实政策信息、诅咒谩骂网络戾气有害信息和恶意诋毁天津上市企业非法勒索谋利、冒用天津地铁集团公司名称或标识、违反“双减”政策发布违规教育培训广告的微信、抖音、快手、微博、网易、今日头条、西瓜视频、小红书等 60 个“自媒体”账号予以关闭处置。（来源：网信天津）

10. 天津市召开新闻发布会，明确“海河净网 2024”网络生态治理系列专项行动重点

5 月 24 日，天津市政府新闻办举行“海河净网 2024”网络生态治理系列专项行动新闻发布会。发布会指出，2023 年的“海河净网 2023”专项行动中，累计清理违规有害信息 30.6 万条，依据用户服务协议处置违规账号

18.2 万个，每月向社会公开治理成果，有力震慑互联网内容领域违法违规行为，维护网民合法权益。

今年的“海河净网 2024”网络生态治理专项行动主要包括以下三个方面：一是“优化营商网络环境”专项行动，主要针对互联网上出现的发布涉企业、企业家虚假不实信息，侵害企业合法权益获利等违法违规行为，会同有关部门积极受理核实、依法快速处置；二是“整治房地产领域虚假不实信息”专项行动。将会同有关部门，针对传播虚假不实信息的违法违规行为予以坚决打击；三是“保护未成年人网络环境”专项行动。着眼于贯彻落实《未成年人网络保护条例》，严厉打击发布低俗色情内容、诱导未成年人沉迷网络和实施网络欺凌、网络暴力等侵害未成年人合法权益行为，全面压缩有害信息、违规行为生存空间。

“海河净网 2024”网络生态治理系列专项行动紧紧围绕上述 3 个重点方面，由市委网信办会同公安、政务服务、住建、教育、共青团等十余个部门在市、区两级同步开展。（来源：网信天津）

11. 西部航空通过国家网信办数据出境安全评估，系重庆首家

5 月 17 日，重庆市网信办发布消息称，西部航空有限责任公司近日通过国家网信办数据出境安全评估，是重庆市首家通过评估的企业。截至目前，重庆市已正式完成数据出境安全评估企业 1 家，通过个人信息出境标准合同备案 6 家，标志着重庆市在智能制造、物流等领域形成行业数据出境合规示范案例。（来源：网信重庆）

12. 因未履行数据安全保护义务，江西省南昌市网信办对某集团作出行政处罚

5 月 15 日消息，江西省南昌市网信办近日接上级网信部门通报，南昌某集团有限公司所属 IP 疑似被黑客远程控制，频繁与境外通联，向境外传输大量数据。

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：该公司未履行数据安全保护义务，未采取相应的技术措施和其他必要措施保障数据安全，所属的服务器遭境外黑客攻击并植入可获取服务器文件管理权限和命令执行权限的木马程序，大量数据疑似泄露或被窃取，相关行为违反《数据安全法》第二十七条规定。同时，该公司开展数据处理活动未加强风险监测，在发现数据安全漏洞风险和事件时未采取补救措施，未履行风险监测、补救处置等义务，相关行为违反《数据安全法》第二十九条规定。

南昌市网信办依据《数据安全法》第四十五条的规定，对南昌某集团有限公司处以警告、罚款 10 万元，对直接负责的主管人员处以罚款 2 万元的行政处罚。（来源：网信南昌）

13. 因涉嫌发布违法违规内容，海南省网信办对“薯条漫画”APP 作出行政处罚

5 月 28 日，海南省网信办发布对“薯条漫画”APP 的行政处罚公告。近期，海南省网信办在监督检查中发现，海南新指引网络科技有限公司运营的“薯条漫画”APP 涉嫌发布违法违规内容。经查，海南新指引网络科技

有限公司未严格落实网络信息内容管理主体责任，发布的漫画中含有性描写、暴力等危害未成年人身心健康内容，且相关内容可在该APP青少年模式下呈现，严重影响未成年人网络安全环境和网络信息内容生态秩序。

根据《未成年人保护法》《网络信息内容生态治理规定》《移动互联网应用程序信息服务管理规定》，海南省网信办决定对该公司和直接责任人分别进行经济处罚，同时对“薯条漫画”APP责令整改30日。（来源：网信海南）

14. 因未尽到审核管理义务，重庆市渝中区网信办对属地一公司作出行政处罚

5月28日消息，重庆市渝中区网信办近日依法对“律师服务网”运营主体重庆法云科技有限公司未尽到审核管理义务、履行主体责任不到位的行为作出行政处罚。

经查，重庆法云科技有限公司运营的“律师服务网”履行主体责任不到位，对用户发布的信息未尽到审核管理义务，存在法律、行政法规禁止发布或者传输的信息，违反《网络安全法》第四十七条的规定。渝中区网信办依据《网络安全法》第六十八条的规定，责令该公司限期改正，给予行政警告的处罚。（来源：网信重庆）

15. 因未尽到审核管理义务，重庆市九龙坡区网信办对一AI写作网站运营主体作出行政处罚

5月29日，重庆九龙坡区网信办依法对属地“开山猴”AI写作网站运营主体重庆初唱科技有限公司未尽到审核管理义务、履行主体责任不到位的行为作出行政处罚。

经查，该企业运营的“开山猴AI写作大师”网站违规生成法律法规禁止的信息，未尽到主体责任义务，违反《网络安全法》《生成式人工智能服务管理暂行办法》等相关法律法规。九龙坡区网信办依据《网络安全法》第六十八条的规定，给予其行政警告处罚，并责令该公司限期全面整改，加强信息内容审核，健全信息内容安全管理相关制度，暂停网站信息更新及AI算法生成式写作功能15日。（来源：网信重庆）

（三）通信管理部门治理实践

1. 工信部、多地通信管理部门通报存在问题的APP

（1）工信部

5月24日，工业和信息化部信息通信管理局通报侵害用户权益行为的APP（SDK）名单。

经组织第三方检测机构进行抽查，共发现50款APP及SDK存在侵害用户权益行为。违法违规事由主要包括违规收集个人信息，APP强制、频繁、过度索取权限、弹窗乱跳转和关不掉、SDK使用说明不完整，以及误导用户

下载等。这些APP及SDK应按有关规定进行整改，整改落实不到位的，将依法依规组织开展相关处置工作。

（2）广东省

5月30日，广东省通信管理局通报16款未完成整改的问题APP名单。

此前，针对存在问题的APP，广东省通信管理局发出《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16款APP未完成整改，现予以通报。违规事由主要包括违规收集个人信息、账号注销难，以及APP强制、频繁、过度索取权限等。被通报的APP应在6月6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。

（3）北京市

5月30日，北京市通信管理局通报2024年第五期存在侵害用户权益和安全隐患等问题的APP名单。

一是，北京市通信管理局近期通过抽测发现部分APP存在“违反必要原则收集个人信息”“未明示收集使用个人信息的目的、方式和范围”等侵害用户权益和安全隐患类问题。截至目前，尚有2款APP未整改或整改不到位，现予以公开通报。

二是，4月30日，该局通报本市部分存在侵害用户权益行为的APP并要求整改。截至目前，仍有5款APP未整改或整改不到位，并予以全网下架处置。（来源：工信部、广东省通信管理局、北京市通信管理局）

2. 浙江省通信管理局：2023 年累计处置网络安全威胁 6.3 万个

5 月 23 日，浙江省通信管理局公布依法治网工作情况。

聚焦互联网专项行动，强化网络生态治理方面，浙江省通信管理局强化 APP 个人信息保护。积极开展“浙里跃升”移动互联网应用服务能力专项行动，聚焦人民群众急难愁盼，集中整治超范围收集个人信息、强制索取权限等群众密切关注的问题，纵深推进 APP 专项治理工作，维护用户权益。专项行动开展以来，下发核查处置通知书 509 份，向社会公告问题 APP152 款，下架 42 款，指导 548 款百万用户以上 APP 建立个人信息保护“双清单”，有效改善用户服务感知。

聚焦行业能力提升，强化网络安全保障方面，一是提升重大活动安全保障能力。通过健全保障机制、建强保障队伍、提升技术能力等多种方式强化重大活动安全保障。杭州亚运会期间，累计监测拦截 DDoS 攻击流量 535T，处置移动恶意程序和僵木蠕攻击 56 万次，封堵高危 IP 4200 个，圆满完成保障任务；二是提升行业网络安全防护能力。加强基础电信网络安全防护，深化行业关键信息基础设施保护，完善供应链安全评估闭环机制，强化网络安全防护检查和威胁处置，2023 年累计处置网络安全威胁 6.3 万个，印发工业互联网安全预警通报 53 期，完成 20 个车联网平台定级备案审核，有效提升行业网络安全防护能力；三是提升数据安全风险治理能力。开展“之江数安”专项行动，组织 21 家电信和互联网重点企业进行重要数据识别认定和目录管理，对 12 家企业开展合规性评估和现场检查，常态化开展安全风险预警处置工作，2023 年共研判风险线索 286 条，印发数据安全预

警通报 234 份，不断强化数据安全风险治理能力。（来源：浙江省通信管理局）

3. 上海市通信管理局公开通报通信网络安全防护管理情况

5 月 30 日，上海市通信管理局公开通报通信网络安全防护管理情况。

通报指出，上海市通信管理局定期对本市电信和互联网企业的通信网络安全防护管理情况进行督查审查，并对在本市行政区域内提供通信网络安全评测、评估服务的网络安全专业机构及其信息通信领域安全服务资质予以备案登记。

近期，通管局针对 2023 年度通报存在安全威胁问题、通信网络定级备案等情况开展审查，发现仍有 19 家单位未整改网络安全威胁且未完成通信网络定级备案。通管局要求，上述单位应当于本通报发布之日起 5 个工作日内完成安全威胁整改，30 日内完成通信网络安全防护定级备案、符合性评测和安全风险评估工作，并将网络威胁整改报告及相应系统的通信网络定级备案证明及时报送该局。未按期落实整改工作的，通管局将依法依规予以处置。（来源：上海通信圈）

（四）其他部门治理实践

1. 国家密码管理局公布通过商用密码检测机构（商用密码应用安全性评估业务）资质申请材料审查的机构名单

5 月 28 日，国家密码管理局根据《商用密码管理条例》《商用密码检测机构管理办法》有关规定，组织对新一批商用密码检测机构（商用密码应用安全性评估业务）资质申请材料进行审查，公布 12 个省市共 19 个通过商用密码检测机构（商用密码应用安全性评估业务）资质申请材料审查的机构。（来源：四川省密码管理局）

2. 广州首例跨境数据产品“离岸易”完成数据资产入表

5 月 6 日，广州市政务服务和数据管理局指导广电运通集团股份有限公司，完成首例跨境数据产品“离岸易”的数据资产入表工作。

数据资产入表是指将数据确认为企业资产负债表中“资产”一项，即数据资产入资产负债表，在财务报表中体现其真实价值与业务贡献。“离岸易”数据产品利用区块链和 AI 技术，对 19 个国家和地区的报关数据、全球大部分集装箱数据，以及相关海运提单数据等进行整合加工处理。

作为广州市属国有企业首例数据资产入表项目，“离岸易”数据产品经过数据资源权属论证、合规确权、资产论证、成本归集和分摊等技术工作，选择以存货作为数据资产核算类型，计入相应会计科目，并于近期获得广州数据交易所颁发的数据资产登记凭证。（来源：广州市人民政府）

3. 江西省鹰潭市余江区人民法院审判全国首例利用“AI 外挂”修改游戏数据案

5 月 6 日，江西省鹰潭市余江区人民法院公开宣判全国首例“AI 外挂”案。经审理查明，被告人王某合通过制作出售“AI 外挂”的方式牟利，2022 年，其先后联系万某至、张某（另案处理）等人编写“AI 外挂”程序。程序制作完成后，王某合利用网络平台招聘陈某勇、张某文（另案处理）等人作为代理销售程序，并通过出售“AI 外挂”点卡密码等获利。至案发，王某合非法获利共计 629 万余元，支付万某至制作费用 84 万余元，支付张某制作费用 42 万余元。

经鉴定，案涉“AI 外挂”中“cvc”等程序对多款游戏中游戏画面数据进行未授权获取，对游戏中处理的鼠标数据指令进行未授权的修改，增加游戏中“自动瞄准”和“自动开枪”的功能，干扰游戏的正常运行环境，属于破坏性程序。盒子程序源代码具有接收计算机 USB 端口传输的鼠标数据指令，并对指令进行计算解析，再将计算结果发送至计算机 USB 端口，从而实现控制计算机鼠标指针自动移动和点击的功能。

鹰潭市余江区人民法院认为，被告人王某合提供专门用于侵入、非法控制计算机信息系统的程序、工具，并获取巨额利润，其行为构成提供侵入、非法控制计算机信息系统程序、工具罪，且情节特别严重。被告人王某合归案后如实供述自己的罪行，属坦白，依法可以从轻处罚；其自愿认罪认罚并退缴违法所得，依法可以从宽处理。法院依法对被告人王某合以提供侵入、非法控制计算机信息系统程序、工具罪判处有期徒刑三年，缓

刑五年，并处罚金；已退缴的违法所得及扣押的作案工具予以没收，上缴国库；剩余未退缴的个人违法所得继续追缴。宣判后，被告人王某合表示服从判决，不上诉。（来源：鹰潭市余江区人民法院）

4. 苏州数据资源法庭揭牌成立

5 月 8 日，江苏苏州高新技术产业开发区（苏州市虎丘区）人民法院狮山人民法庭（苏州数据资源法庭）揭牌成立。

苏州数据资源法庭实行三审合一体系，主要负责审理由虎丘区人民法院管辖的与数据资源相关的一审刑事、民事、行政案件。法庭将聚焦数据采集、存储、处理、销毁等全生命周期合规需求，通过数据资源类案件的管辖集中化、案件类型化、审理专业化的优势，不断为数据收集、开发、开放全过程明确行为规范和责任体系，探索数据产权制度应用和数据纠纷优化处理，激励数据创新，合理界分数据权利，促进数据流通利用，维护数据使用秩序，为营造开放、健康、安全的数字生态提供有力司法保障。

活动中，发布由苏州互联网法庭、苏州数据资源法庭和苏州大数据交易所联合制定的《苏州企业数据合规管理指引》和《企业数据全生命周期负面行为清单》。《合规管理指引》涵盖企业数据合规管理组织体系、制度体系、数据交易与数据出境等多个方面内容，为企业在数据处理活动中提供合规管理法律意见参考。《负面行为清单》聚焦企业数据收集、存储、使用、加工、传输、提供、公开、销毁等维度数据全生命周期合规需求，归纳合规风险，并列出企业在数据处理过程中常见的违法违规行为。（来源：苏州发布）

5. 北京市数据出境“绿色通道”首家试用企业数据出境全部获批

5 月 21 日消息，由北京自贸试验区（大兴）数据跨境服务中心支撑完成的拜耳（中国）有限公司数据出境安全评估项目近日顺利通过国家互联网信息办公室的出境批准。这是我国首个外资生物医药行业企业获批的数据出境安全评估案例，也是北京市打造跨国药企数据出境“绿色通道”首例成功案例。

生物医药领域数据出境存在数据敏感度高、类型识别难、风险判定难度高等特点，其中在药物警戒、临床试验等场景因涉及大量敏感个人健康生理信息，对企业数据出境合规体系建设提出更高要求。为了解决生物医药企业在数据合规出境方面的难题，北京自贸试验区（大兴）数据跨境服务中心充分利用北京市外资企业数据出境“绿色通道”机制，发挥其在数据治理领域的专业实力，协助拜耳开展数据出境合规自查及整改工作，仅用两个月时间，高效完成场景申报，并顺利通过国家网信办评估，其中临床试验和药物警戒全字段通过，为整个医药行业打造数据出境合规标杆。

截至目前，北京自贸试验区（大兴）数据跨境服务中心已服务北京、上海等 7 省市 70 余家企业的近百种复杂数据出境业务场景,并在外资药企、人工智能、跨境清算、征信查询等领域形成全国首例合规出境案例。（来源：北京市人民政府）

6. 杭州互联网法院发布《引导企业数据健康发展行为指引》

5 月 24 日，杭州互联网法院发布《引导企业数据健康发展行为指引》，聚焦市场主体在大数据产业发展中的热点和难点问题，引导企业数据健康发展。

指引分为数据收集与存储、数据开发利用与加工处理、数据交易、数据出境、数据风险识别与安全保护、附则六大部分。其中，第一部分着眼于数据处理全流程的起点，明确数据收集与存储的原则及方式；第二部分引导企业挖掘和提升数据价值，稳步推动数据资源到数字资产的跃迁；第三部分探索企业数据授权使用新模式、数据交易服务体系，强调合法性审查问题，发挥数据要素的乘数效应；第四部分瞄准企业数据出境行为及申报流程合规问题，促进企业合理有序进行数据跨境流动；第五部分聚焦数据安全风险防控问题，明确企业应当建立数据分类分级保护制度及履行数据安全保护义务。

指引提出，企业在经营管理过程中向第三方获取数据时，还应对第三方收集数据的方式是否合法、合规进行审查。企业应当对数据存储进行分域分级管理，选择安全性能、防护级别与安全等级相匹配的存储载体。对敏感个人数据和国家规定的重要数据还应当采取加密存储、授权访问或者其他更加严格的安全保护措施。（来源：杭州互联网法院）

7. 杭州互联网法院发布《青少年网络权益司法保护白皮书》

5 月 31 日，杭州互联网法院发布《青少年网络权益司法保护白皮书》。白皮书指出，2020 年 5 月至 2024 年 5 月，杭州互联网法院共受理涉未成年

人民事纠纷案件259件。其中，未成年人涉网络案件类型集中度高，259件案件中，案由集中在网络服务合同纠纷（181件，占比69.88%）、信息网络买卖合同纠纷（39件，占比15.06%）、网络侵权责任纠纷（39件，占比15.06%）。

白皮书指出，未成年人涉网络案件主要呈现以下特点：（1）涉诉未成年人年龄跨度大，总体呈现低龄化；（2）涉诉场景逐渐增多，未成年人网络活跃程度提高；（3）涉诉未成年人及其监护人维权能力普遍薄弱；（4）充值打赏类案件数量呈上升趋势，且标的额普遍较大；（5）侵害未成年人非物质性人格权的案件增多，但精神损害抚慰金的赔偿数额不高；（6）案件法律关系复杂、适用法律具有特殊性。

白皮书认为，未成年人涉网案件原因有四个方面：（1）未成年人自身网络观念尚未成型；（2）未成年人用网的家庭监管有所欠缺；（3）网络服务提供者未成年人网络保护意识不足；（4）未成年人网络素养系统化教育缺位。（来源：杭州互联网法院）

境外前沿观察：月度速览十则

导读：5 月，美国国家网络主任办公室发布《2024 年美国网络安全态势报告》，对美国网络安全态势、网络政策和战略的有效性以及网络安全执法成效进行整体性评估。英国国王签署《数字市场、竞争和消费者法》，构建数字市场监管新制度。欧洲委员会正式通过首部具有法律约束力的人工智能国际条约《人工智能与人权、民主和法治框架公约》。

欧洲警察署遭遇黑客组织 IntelBroker 入侵，导致内部安全数据受损。印度大量军警人员生物特征数据被泄露，引发民众对身份信息泄露以及选举安全的担忧，同时，印度多个政府网站被黑客篡改成推广加密货币的赌博平台。

关键词：网络安全态势、数字市场监管、人工智能安全、勒索攻击、数据泄露

1. 欧洲委员会正式通过《人工智能与人权、民主和法治框架公约》

5 月 17 日，欧洲委员会正式通过《人工智能与人权、民主和法治框架公约》。公约是第一部具有法律约束力的人工智能国际条约，由欧洲委员会 46 个成员国、欧盟以及美国等 11 个非欧洲国家作为观察员国共同起草，68 名私营部门、民间社会和学术界代表也作为观察员参与其中。公约第 16 条“风险和影响管理框架”规定，缔约方应采取安全措施，识别、评估、预防并缓解人工智能系统带来的风险，并考虑其对人权、民主和法治的实际影响、潜在影响。安全措施应根据需要渐进式、差异化推进，并将下列因素纳入考量：（1）适当考虑人工智能系统的应用领域和预期用途，特别是对人权、民主和法治带来风险的情况；（2）适当考虑潜在影响的严重性和可能性；（3）在适当情况下，考虑相关利益相关者的观点，尤其是权利可能受到影响的人的观点；（4）对人权、民主和法治的风险和负面影响进行监测；（5）对风险、实际和潜在影响以及风险管理方法进行记录；（6）在适当情况下，要求在首次使用人工智能系统前以及对其进行重大修改时进行测试。（来源：欧洲委员会）

2. 英国国王签署《数字市场、竞争和消费者法》

5 月 23 日，英国国王签署《数字市场、竞争和消费者法》，旨在构建一套数字市场监管新制度，通过加强监管、促进竞争和保护消费者权益，防范大型科技公司滥用市场支配地位。该法适用于拥有“战略市场地位”

的公司。“战略市场地位”被定义为“在数字活动方面拥有实质性的、根深蒂固的市场力量和具有战略意义的地位”。

根据该法，拥有“战略市场地位”公司的认定标准包括：（1）企业的全球营业额或企业所在集团在一定时期内的全球营业额超过250亿英镑；或（2）企业在英国境内的营业额，或企业所在集团在一定时期内在英国境内的营业额超过10亿英镑。该法赋予消费者免受不公平交易的权利；禁止误导性、强制性销售活动，赋予消费者追索权，并明确订阅合同的具体要求，包括提前通知、取消权和冷静期等，保护消费者在订阅服务中的权益。（来源：英国议会）

3. 美国ONCD发布《2024年美国网络安全态势报告》

5月7日，美国国家网络主任办公室（ONCD）发布《2024年美国网络安全态势报告》，这是美国首份联邦网络安全态势报告。报告明确2023年美国网络安全态势，包括：（1）关键基础设施面临不断演变的安全风险。对手国家的攻击者利用网络破坏关键基础设施，实现自身战略目标。并且攻击目标不再局限于具有间谍价值的系统，而是扩展到更广泛的基础设施；（2）勒索软件威胁持续升级。勒索软件团伙不断开发复杂策略，逃避防御措施，对国家安全、公共安全和经济发展带来威胁；（3）供应链攻击日益严重。软件、IT服务等供应链成为主要攻击目标；（4）商业间谍软件泛滥。私营供应商向国家行为者出售网络监控工具；（5）人工智能技术风险。人工智能技术快速发展带来挑战，技术恶意利用可能造成大规模网络风险。

报告列举美国政府采取的网络安全行动，包括：（1）强化关键基础设施防护。建立并应用网络安全技术保护关键基础设施，制定并统一关键基础设施监管要求；（2）提升协作与信息共享。提高行业风险管理机构能力，整合联邦网络防御力量，快速共享威胁信息，优先为受害者提供支持；（3）打击网络犯罪活动。利用国家力量干扰、削弱不法分子的恶意网络活动；（4）建设现代化网络防御体系。大规模、快速构建联邦网络防御机制，在整个联邦范围内升级传统技术系统，扩大共享服务的使用范围；（5）培养网络安全人才。加强国家网络安全人才培养，与企业家、学生和教育工作者强化合作。（来源：美国 ONCD）

4. 美国 CISA 联合多部门发布《防范 Black Basta 勒索软件》

5月10日,美国网络安全和基础设施安全局(CISA)与联邦调查局(FBI)、卫生与公众服务部（HHS）以及多州信息共享和分析中心（MS-ISAC）联合发布网络安全咨询《防范 Black Basta 勒索软件》，旨在指导关键基础设施组织采取行动，缓解 Black Basta 勒索软件带来的网络威胁。

Black Basta 是一种勒索攻击软件，已影响北美、欧洲和澳大利亚等地的企业和关键基础设施。2022 年 4 月至 2024 年 5 月期间，Black Basta 入侵 500 多个组织，并加密、窃取多个关键基础设施行业的数据。文件向关键基础设施组织提出应对建议，要点包括：（1）资产管理和安全。组织内的网络安全人员应当识别并了解每个设施的功能、运转和控制情况，确保关键数据和系统得到合理保护，并定期进行资产盘点，对关键资产进行风

险评估，落实安全加固措施，修复已知漏洞，加强系统安全配置；（2）防范钓鱼攻击。组织应当安装反恶意软件系统，自动更新签名，防范钓鱼攻击；（3）漏洞管理和风险评估。组织应当建立漏洞管理机制，定期扫描系统漏洞，发现漏洞后根据内部风险策略评估并优先处置高风险漏洞；（4）账户管理。组织应当将多因素身份验证优先应用于最高风险账户，例如关键资产的特权管理账户。（来源：美国 CISA）

5. 英国 NCSC 发布《组织勒索攻击事件赎金支付指南》

5 月 14 日，英国国家网络安全中心（NCSC）与英国三大保险协会 ABI、BIBA、IUA 合作，联合制定《组织勒索攻击事件赎金支付指南》，鼓励受害组织遵循指南指引，更好应对勒索攻击赎金支付问题。指南不具备强制性。

指南指出，受害组织在遭遇网络勒索时应：（1）不要惊慌，谨慎决策；（2）审查替代方案。是否付款应基于对事件影响的全面了解，选择备份方案恢复系统和数据；（3）记录决策过程。仔细记录事件响应、做出的决策、采取的行动以及受影响的数据，这对于事后审查、吸取经验教训或向监管机构提供证据至关重要；（4）评估影响。全面评估勒索攻击对于自身业务运营、敏感数据保护、金融风险的影响，再决定是否支付赎金；（5）调查事件的根本原因，避免在未明确损害原始来源的情况下付款；（6）向英国当局求助。遭受勒索软件攻击的组织可以向英国当局报告该事件，寻求帮助。指南指出，支付赎金会鼓励犯罪分子继续开展犯罪活动，NCSC 不鼓励、认可或纵容组织支付赎金。（来源：英国 NCSC）

6. 美国 FBI 网络犯罪投诉中心发布《2023 年涉老诈骗报告》

5 月 2 日，美国联邦调查局网络犯罪投诉中心（IC3）发布《2023 年涉老诈骗报告》，回顾美国 2023 年 60 岁以上老年人遭受诈骗的情况。报告指出，对于老年受害者，投资型诈骗涉案金额最多，损失总额高达 12 亿美元；而技术支持型诈骗数量最多，诈骗者通过冒充特定公司的技术支持人员，告知受害者账户存在涉诈风险、账户有订阅服务退款等，引诱受害者下载恶意软件，获取其银行账户信息。

报告建议公众采取以下安全防范措施：（1）在识别诈骗分子的诈骗意图后，及时终止与诈骗分子的通信；（2）保持冷静，在受到威胁时及时报警；（3）谨慎对待陌生来电、邮件和上门服务；（4）不向未经确认的个人和企业提供个人身份信息以及支票或电汇等信息。（来源：美国 IC3）

7. 美国 FBI 就人工智能犯罪风险发出警告

5 月 8 日，美国联邦调查局（FBI）旧金山分部发布警告，提醒个人和企业防范网络攻击者利用人工智能工具实施的网络钓鱼、语音和视频克隆诈骗等违法犯罪活动。FBI 建议企业采取以下安全防范措施：（1）使用技术手段拦截人工智能伪造信息，避免员工遭受侵害；（2）加强员工教育培训，使员工了解网络钓鱼的危险性以及验证数字通信信息的重要性，谨慎向外提供敏感信息；（3）实施多因素验证，提升账户和系统的安全性。（来源：美国 FBI）

8. 黑客组织 IntelBroker 入侵欧洲警察署并窃取机密数据

5 月 10 日消息，黑客组织 IntelBroker 近日公开表示已成功侵入欧洲警察署并访问各种敏感数据，包括：欧洲警察署各机构工作人员的个人数据、仅供官方使用的源代码、作战文件、用于侦查任务和作战指南的文件等。此次入侵导致欧洲警察署内部安全数据受损，受影响机构包括网络犯罪中心（EC3）、专家平台、执法论坛等。

IntelBroker 已公开售卖从欧洲警察署数据库中提取的样本数据集，并命名为 EC3-Space.csv。数据集涵盖欧洲警察署工作人员的详细信息，如名字、姓氏、职务、组织、国家和地区、专业领域和职责范围等。IntelBroker 尚未透露数据集的出售价格，但已邀请感兴趣的各方提交报价。目前，欧洲警察署尚未就此次泄露事件发表正式声明。（来源：安全内参）

9. 印度大量军警人员生物特征数据泄露

5 月 23 日消息，在印度全国大选期间，近日发生一起大规模数据泄露事件，数百万人的生物特征信息遭到暴露，引发印度民众对身份信息泄露以及选举安全的担忧。

被泄露的数据库共约 166159 个文件（496.4GB），内含警察、军人、教师、铁路工人的面部扫描图像、指纹、签名和识别标记等敏感生物特征信息。除生物识别数据外，出生证明、照片、电子邮件地址、就业申请、毕业证书、资格证书和其他教育相关文件等重要个人信息也在泄露之列。该数据库涵盖 2021 年至 2024 年期间的数据记录。其中约有 284535 份文件

记录了警察和执法人员的体能测试信息，包括签名图像、PDF 文件、移动应用程序和安装数据，部分以压缩包 zip 格式存储。泄露数据来源于 ThoughtGreen Technologies 和 Timing Technologies 两家印度科技公司，两家公司均提供应用开发、射频识别（RFID）和生物特征验证服务。但是，目前尚不清楚这两家公司中哪一家拥有该数据库的托管服务器。（来源：安全内参）

10. 印度多个政府网站遭黑客篡改，成为推广加密货币的赌博平台

5 月 13 日消息，安全研究人员近日发现 40 个带有“gov.in”域名的链接，指向自称“亚洲最受欢迎的在线博彩平台”和“印度领先的板球博彩应用程序”。被篡改的链接属于印度各地的政府网站，包括比哈尔邦、果阿邦、卡纳塔克邦、喀拉拉邦、米佐拉姆邦和泰伦加纳邦等，部分警察局和财税部门等重要机构的官方页面被篡改。发现该问题后，TechCrunch 立即向印度计算机紧急响应小组（CERT-In）报告，并主动提供受影响站点的样本。收到报告后，CERT-In 启动调查程序，并表示已采取相关应对措施。目前，漏洞修复工作正在进行，黑客在政府网站上植入广告的方法以及重定向链接存续的时间尚未明确。（来源：安全内参）

行业前沿观察一：中央网信办等四部门印发《2024年数字乡村发展工作要点》、中央网信办等三部门印发《信息化标准建设行动计划（2024—2027年）》、2024年全民数字素养与技能提升月活动启动、中国互联网联合辟谣平台发布2024年5月辟谣榜

导读：近日，中央网信办、农业农村部、国家发展改革委、工业和信息化部联合印发《2024年数字乡村发展工作要点》。《工作要点》明确了工作目标：到2024年底，数字乡村建设取得实质性进展。

为深入落实《“十四五”国家信息化规划》《国家标准化发展纲要》任务部署，近日，中央网信办、市场监管总局、工业和信息化部联合印发《信息化标准建设行动计划（2024—2027年）》（以下简称《行动计划》），要求加强统筹协调和系统推进，健全国家信息化标准体系，提升信息化发展综合能力，有力推动网络强国建设。

5月24日，2024年全民数字素养与技能提升月活动在第七届数字中国建设峰会开幕式上启动。全民数字素养与技能提升月活动（简称“提升月”）已连续举办两届，本届提升月以“数字赋能 全民共享”为主题。

近日，中国互联网联合辟谣平台对5月网络谣言进行了梳理分析。网上数据监测和网民举报显示，当月网络谣言主要集中在涉公共政策、社会民生、科技与健康等领域，一些不法分子或假冒官方编造谎言实施诈骗行

为，或杜撰事实博眼球蹭流量，或传播伪科普误导公众认知，扰乱公共秩序、造成不良影响。

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. 中央网信办等四部门印发《2024 年数字乡村发展工作要点》

近日，中央网信办、农业农村部、国家发展改革委、工业和信息化部联合印发《2024 年数字乡村发展工作要点》。通知要求，深入贯彻落实习近平总书记关于乡村振兴的重要指示批示精神和中央经济工作会议、中央农村工作会议精神，认真落实《中共中央 国务院关于学习运用“千村示范、万村整治”工程经验 有力有效推进乡村全面振兴的意见》（中发〔2024〕1 号）部署要求，深入实施《数字乡村发展战略纲要》《数字乡村发展行动计划（2022—2025 年）》，以信息化驱动引领农业农村现代化，促进农业高质高效、乡村宜居宜业、农民富裕富足，为加快建设网络强国、农业强国提供坚实支撑。

《工作要点》明确了工作目标：到 2024 年底，数字乡村建设取得实质性进展。数字技术保障国家粮食安全、巩固拓展脱贫攻坚成果更加有力。农村宽带接入用户数超过 2 亿，农村地区互联网普及率提升 2 个百分点，农产品电商网络零售额突破 6300 亿元，农业生产信息化率进一步提升，培育一批既懂农业农村、又懂数字技术的实用型人才，打造一批示范性强、带动性广的数字化应用场景，抓好办成一批线上线下联动、群众可感可及的实事。

《工作要点》部署了 9 个方面 28 项重点任务。一是筑牢数字乡村发展底座。包括提升农村网络基础设施供给能力，加大农村基础设施改造升级力度，加快推进涉农数据资源集成共享。二是以数字化守牢“两条底线”。包括强化确保粮食安全数字化支撑，强化防止返贫监测和帮扶举措。三是

大力推进智慧农业发展。包括加强农业科技创新与应用推广，提升农业全产业链数字化水平，以数字技术深化农业社会化服务。四是激发县域数字经济新活力。包括加快推进农村电商高质量发展，多措并举推动农文旅融合发展，释放涉农数据要素乘数效应，运用数字技术促进农民增收。五是推动乡村数字文化振兴。包括加快乡村文化文物资源数字化，丰富乡村公共文化服务数字供给。六是健全乡村数字治理体系。包括稳步推进农村“三务”信息化建设，提升农村社会治理数字化效能，增强农村智慧应急管理能力。七是深化乡村数字普惠服务。包括着力提升乡村教育数字化水平，持续推进乡村数字健康发展，增强农村数字普惠金融服务实效，加强农村特殊人群信息服务保障。八是加快建设智慧美丽乡村。包括加强农村人居环境整治数字化应用，提升农村生态环境保护监管效能。九是统筹推进数字乡村建设。包括加强跨部门跨层级协调联动，健全多元化投入保障机制，培养壮大乡村数字人才队伍，推进重点领域标准化建设，讲好新时代数字乡村故事。（来源：中国网信网）

2. 中央网信办等三部门印发《信息化标准建设行动计划（2024—2027 年）》

为深入落实《“十四五”国家信息化规划》《国家标准化发展纲要》任务部署，近日，中央网信办、市场监管总局、工业和信息化部联合印发《信息化标准建设行动计划（2024—2027 年）》（以下简称《行动计划》），要求加强统筹协调和系统推进，健全国家信息化标准体系，提升信息化发展综合能力，有力推动网络强国建设。

《行动计划》强调，信息化标准是国家标准体系的重要组成部分，是以信息化驱动引领高质量发展的重要支撑，要以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，深入贯彻党的二十大精神，认真落实党中央、国务院关于信息化发展和标准化工作的决策部署，完善信息化标准体系、提升标准化基础能力、健全工作机制、强化标准实施、增强国际影响力，以标准建设支撑引领信息化发展，为加快建设全国统一大市场，培育壮大新质生产力提供有力支撑。

《行动计划》提出，要坚持系统观念、坚持需求导向、坚持重点推进、坚持开放合作。到 2027 年，信息化标准工作机制更加健全，信息化标准体系布局更加完善，标准研制、服务等基础能力进一步夯实，发布一批高质量的信息化标准，形成一支专业化、职业化、国际化的标准化人才队伍，标准质量显著提升，实施效果明显增强，信息化标准在引领技术创新、驱动经济社会发展中的作用充分发挥，国际标准贡献度和影响力明显提升。

《行动计划》围绕4个方面部署了主要任务。一是创新信息化标准工作机制，包括完善国家信息化标准体系、优化信息化标准管理制度、强化信息化标准实施应用。二是推进重点领域标准研制，在关键信息技术、数字基础设施、数据资源、产业数字化、电子政务、信息惠民、数字文化、数字化绿色化协同发展等8个重点领域推进信息化标准研制工作。三是推进信息化标准国际化，包括深化国际标准化交流合作、积极参加国际标准组织工作、推动国际国内标准协同发展。四是提升信息化标准基础能力，包括优化标准供给结构、加强标准化人才培养、推动标准数字化发展。

《行动计划》从加强统筹协调、强化政策支持、营造良好氛围等3方面提出组织保障要求，确保目标任务落到实处。（来源：中国网信网）

3. 2024年全民数字素养与技能提升月活动启动

5月24日，2024年全民数字素养与技能提升月活动在第七届数字中国建设峰会开幕式上启动。

全民数字素养与技能提升月活动（简称“提升月”）已连续举办两届，本届提升月以“数字赋能 全民共享”为主题，由中央网信办、中央党校（国家行政学院）、教育部、科技部、工业和信息化部、民政部、人力资源社会保障部、农业农村部、国家卫生健康委、国务院国资委、全国总工会、全国妇联、中国科协、中国残联等14个部门共同主办，以助力提高人口整

体素质、服务现代化产业体系建设、促进全体人民共同富裕为目标，强化数字教育培训，优化教学资源供给，丰富数字应用场景，完善数字环境保障。

提升月期间，将组织举办全民数字素养与技能培训基地开放日活动、数字素养与技能专题课、师生数字素养与技能提升专项行动、数字科技普及活动、企业数字化转型人才队伍建设行动、数字助老爱心帮扶公益活动、数字技术工程师培育项目和社会保障卡居民服务“一卡通”应用宣传教育活动、农民手机应用技能培训、数字健康普及宣传活动、国有企业数字化转型行动计划、职工数字素养与技能提升活动、女性数字素养与技能提升行动、数字科普系列活动、信息无障碍建设行动等系列主题活动，突出赋能增效和便民惠民，加强对人工智能等新技术新应用的教育培训，不断提升全民数字素养与技能水平，夯实新质生产力发展的人力资源基础。

全国各省、自治区、直辖市和新疆生产建设兵团有关部门将同期举办本地区2024年全民数字素养与技能提升月活动。（来源：中国网信网）

4. 中国互联网联合辟谣平台发布2024年5月辟谣榜

近日，中国互联网联合辟谣平台对5月网络谣言进行了梳理分析。网上数据监测和网民举报显示，当月网络谣言主要集中在涉公共政策、社会民生、科技与健康等领域，一些不法分子或假冒官方编造谎言实施诈骗行

为，或杜撰事实博眼球蹭流量，或传播伪科普误导公众认知，扰乱公共秩序、造成不良影响。

假冒官方行骗敛财。5 月以来，一些不法分子通过伪造“红头文件”、虚构官方项目等方式，打着“领取补贴”“投资项目”“发放国债”等旗号，设置骗局，实施诈骗。如冒充国家部委发布“扫码可领‘2024 年个人劳动补贴’”邮件，伪造“官方”小程序或网站，骗取钱财；打着国家工程或项目的幌子谎称“‘藏水入疆’工程将于 9 月正式开工”“新疆 5G 机站管网线路预埋项目施工”，发布所谓投资项目帖文，诱骗投资；假借财政部发行国债之名，伪造“红头文件”，声称“收到‘国债发放通知书’便有机会申请提款 288 万”，诱导转账。此外，还有人造谣称“文旅部门帮某农家乐推荐引流”，实则是为博取眼球、吸引游客故意编造的不实言论。

捏造事实搬弄是非。个别自媒体和网民或虚构杜撰、捏造事实，或捕风捉影、夸大其词，或混淆视听，颠倒黑白，造谣传谣，造成不良社会影响。比如，谣言“广东交通最落后的县没有国道”“四川凉山最落后山村不通电”与事实严重不符，歪曲当地经济社会发展和脱贫攻坚成果，对涉事地方形象造成不良影响；谣言“‘中国最贵景区’楼兰故城门票 3500 元”“新疆克拉玛依有风力机着火损失千万”“河南郑州地标建筑‘大玉米’楼被大风刮歪”等纯属捕风捉影，刻意博人眼球，徒增网民担忧情绪。还有个别自媒体利用网民对大熊猫的关注和喜爱，编造“旅美大熊猫‘洋洋’口吐白沫、饿得啃墙皮”“大熊猫国际合作是‘将大熊猫送给外国人做黑

实验’”等谣言，抹黑我国大熊猫保护和国际合作工作，伤害社会信任。此外，根据国家安全部微信公众号披露，所谓“所有人入境中国都会被查手机”的谣言，出自境外反华敌对势力故意造谣抹黑、搬弄是非，实属荒谬至极。

胡乱科普误导认知。一些自媒体为博眼球、引流量，利用人们对各类科学知识的好奇和需求，制作散布网络伪科普，不仅误导社会公众，有些甚至借机兜售各种保健品、营养品、化妆品，令网民上当受骗。比如谣言“河南小麦单产破2500公斤”无视农业生产和科技发展客观规律，信口开河炒作小麦产量，严重搅乱公众认知；“发生在我国的红色极光是‘假极光’？”“太阳耀斑会导致头痛、失眠？”等说法看似新奇，实则缺少科学依据和严谨论证。另有“靠吃减脂餐就能轻松变瘦”“结石患者不能吃豆制品”“每天只需睡2个钟头，其余都是浪费时间？”等说法，打着“科学”的幌子传播似是而非的观点，渲染焦虑情绪，误导人们日常健康生活。

进入6月，恰逢端午、中高考、毕业季等重要节点，涉旅游出行、节庆民俗、中高考政策、求职就业等领域的话题关注度高，各类谣言亦或随之增多。中国互联网联合辟谣平台提醒广大网民，天气日渐炎热、头脑务必冷静，面对海量网上信息，始终保持理性客观态度，切实增强识谣辨谣能力，共建共享清朗网络空间。（来源：网信中国）

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，举行党建联学活动、举行网络安全论坛等，助推网络安全发展。广东省网络空间安全协会党支部等 6 家单位在广州开展党建联学；上海市信息安全行业协会开展 2024 年度上海市网络信息安全行业“网安工匠”评选工作；安徽省网络安全协会成功主办数字政府安全建设大会；陕西省信息网络安全协会、北京网络空间安全协会在西安成功举办第八届丝绸之路网络安全论坛；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；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；佛山市信息协会顺利举行 2024 年佛山市中小企业服务机构宣贯服务活动（第二期）；武汉市网络安全协会入选湖北省第一批优质团体标准制定主体重点培育名单；南宁市信息网络安全协会成功举办企业数字化服务同行沙龙；肇庆市计算机学会、肇庆市信息协会成功举办 2024 年知识产权进校园活动等。

关键词：信创、大学生网络安全、信息安全、网络安全、企业数字化、网络强国

1. 广东省网络空间安全协会党支部等 6 家单位在广州开展党建联学

6 月 6 日，中共北京网络空间安全协会流动联合支部、中共广东省网络空间安全协会支部委员会、中共南宁市信息技术学会支部、南宁市信息网络安全协会、广西高校教育技术专业委员会、广州网络空间安全协会等 6 家单位在广州开展党建联学，举行习近平总书记关于网络强国的重要思想学习会。

党的十八大以来，我国网络安全和信息化事业取得重大成就，党对网信工作的领导全面加强，网络空间主流思想舆论巩固壮大，网络综合治理体系基本建成，网络安全保障体系和能力持续提升，网信领域科技自立自强步伐加快，信息化驱动引领作用有效发挥，网络空间法治化程度不断提高，网络空间国际话语权和影响力明显增强，网络强国建设迈出新步伐。

此次党建联学重点重温学习领会习近平总书记对网络安全和信息化工作作出重要指示。大家表示要深刻领会习近平总书记关于网络强国重要思想的重大意义，进一步增强学习宣传贯彻的政治自觉、思想自觉和行动自觉。（来源：广东省网络空间安全协会）

2. 上海市信息安全行业协会开展2024年度上海市网络信息安全行业“网安工匠”评选工作

5月20日，上海市信息安全行业协会发布《关于开展2024年度上海市网络信息安全行业“网安工匠”评选工作的通知》。

《通知》公布，为进一步弘扬工匠精神，树立行业标杆，增强从业人员的敬业感和荣誉感，助推本市网络信息安全、数据安全产业发展，根据上海市总工会《关于在本市开展“上海工匠”培养选树千人计划的实施意见》（沪工总经〔2015〕260号）精神，上海市信息安全行业协会将与上海市浦东新区信息安全行业工会联合会开展2024年度上海市网络信息安全行业“网安工匠”评选工作。

《通知》中就申请对象及评选条件、评选名额、评选程序、选手命名、申报要求、联系方式等进行了详细说明。（来源：上海市信息安全行业协会）

3. 安徽省网络安全协会成功主办数字政府安全建设大会

近日，由中国计算机学会计算机安全专委会指导，国家信息中心《信息安全研究》杂志、安徽省网络安全协会主办的数字政府安全建设大会在安徽合肥成功举行。会议聚焦数字政府建设，以促进安全建设为目的，着

力提升相关单位从业人员的业务能力。来自国家部委、各地信息中心、大数据局等单位代表参会。

会上，多位与会领导、专家及企业代表发言、演讲。其中，国家信息中心办公室副主任吕欣表示，大力推进以数字经济为代表的新质生产力快速发展有三个关键点。一是要大力发展数据基础设施；二是要大力发展数据产业；三是持续加强数据安全能力建设。

安徽省网络安全协会会长俞能海表示，协会将进一步加强与国内网络安全企事业单位和专家互动交流，强化安徽省网络安全教育技术产业融合发展，在主管单位安徽省公安厅网安总队支持下，用网络安全创新成果服务政府部门和企事业单位，推动安徽网络安全产业发展壮大。（来源：安徽省网络安全协会）

4. 陕西省信息网络安全协会、北京网络空间安全协会在西安成功举办第八届丝绸之路网络安全论坛

5 月 23 日，2024 第八届丝绸之路网络安全论坛在陕西宾馆会议中心成功举办，本次论坛以“汇聚万千智慧 夯实安全堤坝”为主题，由主论坛及密码技术与密评、教育行业网络安全、卫健行业网络安全三个平行分论坛组成，论坛邀请业内专家学者、企业代表、行业代表共计 400 余人参加。

本届论坛由陕西省信息网络安全协会主办，北京网络空间安全协会网安联发展工作委员会特约指导，西安市信息网络安全协会、榆林市网络安

全协会、渭南市互联网协会、商洛市信息网络安全协会协办，本次论坛还得到12家网络安全企业的大力支持。（来源：陕西省信息网络安全协会）

5. 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。（来源：上海市信息安全行业协会）

6. 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。（来源： 湖南省网络空间安全协会）

7. 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。（来源：重庆信息安全产业技术创新联盟）

8. 佛山市信息协会顺利举行2024年佛山市中小企业服务机构宣贯服务活动（第二期）

5月23日-24日,由佛山市工业和信息化局指导、佛山市中小企业服务中心主办、佛山市信息协会承办的“2024年佛山市中小企业服务机构宣贯服务活动（第二期）"顺利举行。来自产业集群、示范平台、示范基地、产业园区、商协会、涉企服务机构、企业代表约50人参加了活动。

本次宣贯活动以创业创新专题为主题，邀请了多位业界精英和行业专家担任讲师，通过《自媒体运营合规管理要点》《概念验证，通过工程化服务让科技成果走向产业市场》、《企业人才职称晋升发展方向与规划》、《外贸数字化平台赋能中小企业出海》、《佛山市金融扶持政策解读》、《直播项目创投的管理流程》的主题分享，为参会人员提供了大量实用性的经验和实践案例。（来源：佛山市信息协会）

9. 武汉市网络安全协会入选湖北省第一批优质团体标准制定主体重点培育名单

近日，湖北省市场监督管理局联合其他九个相关部门印发了《关于实施以标准升级服务保障大规模设备更新和消费品以旧换新行动的工作方案》的通知。该方案中决定实施团体标准培优计划。

其中，在湖北省第一批优质团体标准制定主体重点培育名单中，武汉市网络安全协会成功入选。协会表示，未来将按照国家标准化法规要求和省工作方案精神，不断加大高质量优质团体标准供给，带领广大会员为本省市网络安全标准化工作提供有力支撑、服务和保障。（来源：武汉网络安全）

10. 南宁市信息网络安全协会成功举办企业数字化服务同行沙龙

为了更好地推动企业数字化服务的发展，加强产教融合与交流合作，5月 17 日下午，“同心聚力 产教同行——企业数字化服务同行沙龙”成功举办。活动由南宁市信息技术学会、南宁市信息网络安全协会、广西布道天下信息产业有限公司共同主办。

活动活动邀请了广西中小企业公共服务平台、南宁市信息技术学会、南宁市信息网络安全协会相关领导，南宁职业技术大学教授，及各企业数字化服务同行单位，以《广西企业数字化转型政策解读》为主题进行交流，

对政策见解进行了充分探讨，为以后的业务推进及公司发展提供了强有力的支持。（来源： 南宁市信息网络安全协会）

11. 肇庆市计算机学会、肇庆市信息协会成功举办 2024 年知识产权进校园活动

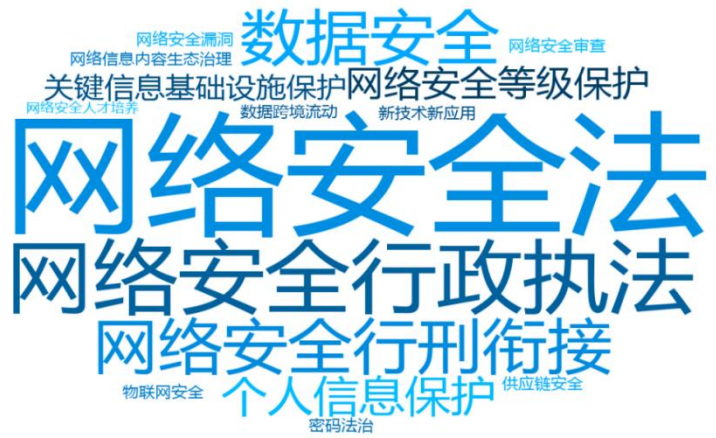
为加强知识产权宣传普及，培养小学生的知识产权保护意识，营造尊重知识、勇于创新的校园文化氛围。6 月 4 日，在市市场监督管理局（知识产权局）和高要区科学技术协会的指导下，由市计算机学会主办，市信息协会承办的 2024 年知识产权进校园活动在白诸中心小学举办，活动由我会副会长兼秘书长梁永志主持。

活动邀请广东睿立知识产权专家梁子军老师现场授课，梁老师围绕着知识产权的概念、分类等相关知识，用通俗易懂的语言、案例列举等方式，深入浅出地向学生们进行知识产权科普，帮助学生们进一步加深对知识产权的理解和认识。（来源：肇庆市信息协会）

公安部第三研究所网络安全法律研究中心

2016年2月，公安部第三研究所正式成立“网络安全法律研究中心”。 中心成立以来，聚焦前瞻性研究，切实践行理论研究与立法实践深度结合，跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用发展及安全风险，并持续推动科研成果应用于网络安全相关立法活动，在国内网络安全法律方面的影响力逐步提升。同时投身警务实践活动和公安一线服务，为公安部门提供立法动态研判和决策研究支撑。

基础性	专业性	针对性



推动立法、服务实务、智库支撑

联系方式

电子邮箱：cslaw@gass.ac.cn　　咨询电话：王老师 18817309169

网络与数据安全法律合规咨询服务

提供《网络安全法》《数据安全法》《密码法》《个人信息保护法》及配套制度为核心的数据安全保护合规体系建设，包括但不限于帮助企业落实网络安全等级保护、关键信息基础设施安全保护、网络安全审查、数据出境安全风险评估、数据交易安全保障、安全事件应急处置等要求。
开展个人信息、重要数据、核心数据等数据安全合规自查、合规差距性分析，发现、识别、分析、研判、控制数据收集、存储、使用、加工、传输、提供、公开等全生命周期的法律风险，提供法律意见和整改建议。

数据安全合规体系构建

为企业提供网络安全漏洞发现与披露、漏洞扫描与渗透测试等安全测试、“白帽子”与众测等业务场景下的合规体系构建，帮助企业厘清行为边界，避免经营风险。

安全测试法律合规体系构建

开展情况调研，评估拟出境活动风险，发现安全风险并提供整改建议，根据客户整改落实情况，出具数据出境安全风险评估报告。

数据出境安全风险评估咨询服务

帮助企业构建事先防范网络安全、数据安全行政与刑事风险框架，指导企业如何正确配合监督检查、理解执法要求等。

网络安全、数据安全执法调查与刑事风险的防范与处置意见

针对《个人信息保护法》第五十五条规定的个人信息处理情形，帮助企业开展个人信息保护影响评估，履行个人信息保护义务。

个人信息保护影响评估/合规审计咨询服务

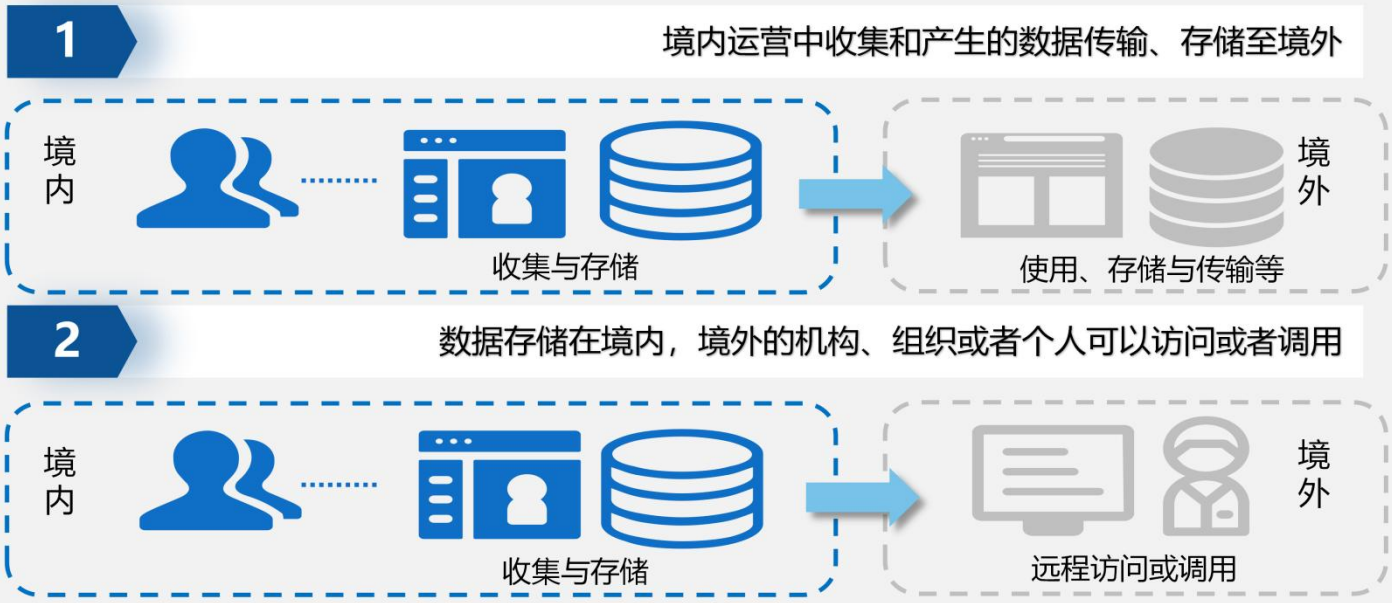
结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

网络安全、数据安全法律法规专业培训

数据出境安全风险评估咨询服务

近年来，我国在国家数据安全和个人信息保护的顶层设计布局下，加快数据出境相关立法，数据出境规则体系不断完善，数据出境安全评估成为数据出境的重要路径。2022年7月7日，国家互联网信息办公室发布《数据出境安全评估办法》，落实《网络安全法》《数据安全法》《个人信息保护法》上位法要求，明确数据出境安全评估相关规定。在此形势下，企业普遍面临出境数据识别难、出境风险评估难、申报材料填报难等难题。为帮助企业解决以上难题，及时履行数据出境安全评估申报义务，公安部第三研究所网络安全法律研究中心特推出**数据出境安全风险评估咨询服务。**

数据出境活动



数据出境安全风险评估咨询服务流程

- 开展合规差距分析
- 识别安全风险并划定风险等级
- 针对安全风险提供整改建议

- 结合客户落实整改情况，出具《数据出境风险评估报告》

合规咨询服务项目

中心已为互联网、银行、服装、签证、传统制造业等分属不同行业类别的企业提供APP合规咨询、个人信息保护（隐私政策）评估、个人信息保护合规整改、数据出境安全风险自评估等方面的合规咨询服务，合规咨询服务能力得到客户一致认可。

典型项目

- 某互联网公司APP合规咨询
- 某银行个人信息保护（隐私政策）评估
- 某跨国服装零售企业个人信息保护合规整改
- 某签证跨国集团数据出境安全风险评估咨询
- 某传统制造业跨国集团数据出境安全风险评估咨询

……