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12月第12期 (总第17期)

2024年12月12日

目　录

主办单位：公安部第三研究所网络安全法律研究中心

联合主办：北京网络空间安全协会

牵头组织：网安联秘书处

协办单位：网安联认证中心

技术支持：北京关键信息基础设施安全保护中心

广东关键信息基础设施保护中心

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

境内前沿观察一：安全事件

导读：11 月，习近平主席在亚太经合组织第三十一次领导人非正式会议上提出《全球数据跨境流动合作倡议》，并在 2024 年世界互联网大会乌镇峰会正式发布倡议全文。倡议就各方普遍关切的数据跨境流动治理问题提出建设性解决思路，推动构建开放共赢的数据跨境流动国际合作格局，促进数据跨境高效便利安全流动。

世界互联网大会发布《2024 年全球发展倡议数字合作论坛主席声明》，重点聚焦“加强普惠合作，助力数字经济可持续发展”“推进数字治理，打造开放包容数字新格局”“深化交流互鉴，共创美好数字未来”三个方面提出九项对策举措。《中国互联网发展报告 2024》和《世界互联网发展报告 2024》蓝皮书正式发布。《中国互联网发展报告 2024》指出，一年来，中国关键信息基础设施安全不断强化，国家网络安全应急体系不断健全完善；网信重点领域相关立法加快完善。《世界互联网发展报告 2024》指出，数据治理成为网络空间国际治理的核心议题，但相关规则制度仍呈现碎片化、区域化、多极化特征等。

360 数字安全集团发布《大模型安全漏洞报告》，从模型层安全、框架层安全以及应用层安全三大维度探查安全问题，对多个开源项目进行代码梳理和风险评估，最终审计并发现近 40 个大模型相关安全漏洞，影响范围覆盖llama.cpp、Dify等知名模型服务框架，以及Intel等国际厂商开发的多款开源产品。字节跳动起诉前实习生田某某篡改代码攻击公司内部模型

训练一案已获北京市海淀区人民法院正式受理，字节跳动请求法院判令田某某赔偿公司侵权损失800万元及合理支出2万元，并公开赔礼道歉。

中国互联网联合辟谣平台对十月网络谣言进行梳理分析，发现十月网络谣言主要集中在假冒官方虚构政策、炮制谣言炒作话题、编造剧本打造虚假人设等方面。

公安部召开网络安全法律咨询委员会2024年年会暨第十四届中国信息安全法律大会。会议由公安部网络安全法律咨询委员会和中国信息安全法律大会专家委员会主办，公安部第三研究所承办。会议指出，2024年，全国公安机关在公安部党委的坚强领导下，在各有关部门的鼎力支持下，在各网络安全法律咨询委员的大力帮助下，深入推进网络安全立法、执法、司法工作，有效提升执法规范化水平。

关键词：数据跨境流动、数字经济发展、大模型安全、公安部网络安全法律咨询委员会

1. 中国提出《全球数据跨境流动合作倡议》

11 月 20 日消息，习近平主席近日在亚太经合组织第三十一次领导人非正式会议上提出《全球数据跨境流动合作倡议》，并在 2024 年世界互联网大会乌镇峰会正式发布倡议全文。

倡议就各方普遍关切的数据跨境流动治理问题提出建设性解决思路，明确中国促进全球数据跨境流动合作的立场主张，倡导秉持开放、包容、安全、合作、非歧视的原则，推动构建开放共赢的数据跨境流动国际合作格局，促进数据跨境高效便利安全流动。

倡议呼吁各国政府：鼓励因正常商业和社会活动需要而通过电子方式跨境传输数据，以实现全球电子商务和数字贸易为各国经济增长和可持续增长提供新的动力。

倡议提出，尊重各国为保护个人隐私等个人信息权益采取的措施，鼓励各国在保护个人信息的前提下为个人信息跨境传输提供便利途径，建立健全个人信息保护法律和监管框架，鼓励就此交流最佳实践和良好经验，提升个人信息保护机制、规则之间的兼容性，推动相关标准、技术法规及合格评定程序的互认。鼓励企业获得个人信息保护认证，以表明其符合个人信息保护标准，保障个人信息跨境安全有序流动。

倡议强调，禁止通过在数字产品和服务中设置后门、利用数字技术基础设施中的漏洞等手段非法获取数据，共同打击数据领域跨境违法犯罪活动，共同保障各国公民和企业的合法权益。（来源：外交部、中国网信网）

2. 2024年世界互联网大会发布《2024年全球发展倡议数字合作论坛主席声明》

11月21日，2024年全球发展倡议数字合作论坛于世界互联网大会乌镇峰会期间举行。会后，论坛发布《2024年全球发展倡议数字合作论坛主席声明》。声明重点聚焦“加强普惠合作，助力数字经济可持续发展”“推进数字治理，打造开放包容数字新格局”“深化交流互鉴，共创美好数字未来”三个方面提出九项对策举措。

加强普惠合作，助力数字经济可持续发展方面，声明要求深入开展包容普惠国际数字合作，大力推动科技创新与成果应用，推进数字技术同实体经济深度融合，加强产业链供应链国际合作，优化提升全球数字产业链供应链安全保障水平，促进全球数字经济高质量发展；积极开展数据要素的国际互通合作，加强数据互联互通，弥合数据流通分歧。倡导各方支持中方提出的《全球数据跨境流动合作倡议》《全球数据安全倡议》，推动全球数据跨境流动合作，携手构建开放共赢的数据领域国际合作格局。

在推进数字治理，打造开放包容数字新格局方面，声明提出加强国家间数字领域政策法规协调，推动数字国际规则和数字技术标准制定，推进全球数字治理体系更加公正合理，共同开创全球数字治理新局面，灵活应对数字时代挑战。声明鼓励引导人工智能等新技术新应用坚持“以人为本智能向善”，培育安全、可靠、公平、透明的人工智能技术研发和应用生态，持续深化在技术标准、伦理准则、法律法规方面的国际交流合作，推动形成具有广泛共识的全球人工智能治理体系。（来源：中国网信网）

3. 中国互联网联合辟谣平台发布十月辟谣榜综述

11 月 12 日，中国互联网联合辟谣平台近日对十月网络谣言进行梳理分析。

网上数据监测和网民举报显示，十月网络谣言主要集中在假冒官方虚构政策、炮制谣言炒作话题、编造剧本打造虚假人设等方面。一是自编自导骗取流量。一些造谣传谣者通过搭蹭社会民生话题，编造剧本、制造噱头，或打造虚假人设，或假借弱势群体形象卖惨，进而吸引网民关注，赚取流量、获取利益；二是假冒官方虚构政策。一些不法分子冒充权威机构，散布涉公共政策类谣言，误导公众认知。有的假借官方名义，伪造政策文件，实则行骗牟利，侵犯群众利益；三是危言耸听炒作话题。个别网民和自媒体编造虚假信息，炒作社会热点话题，并配以具有煽动性、误导性的标题，扩散传播，扰乱社会秩序。

面对各类网络谣言，各级网信和公安部门坚持重拳出击，加大打击力度。10 月以来，山西网民高某某利用 AI 技术生成虚假图像虚构剧情“网上寻娃”，重庆网民陈某某编造“喝酒开车警察不管”谣言，四川网民梅某编造“四川巴中频繁有青少年失踪”谣言，杭州网民段某某编造“杭州东站电车自燃烧死人”谣言等，均被当地警方依法予以罚款、行政拘留等处罚，网信部门亦对相关造谣账号予以禁言处罚或依法依约关闭。10 月 12 日，中央网信办通报，网信部门指导网站平台持续加大监测和处置力度，及时溯源并关闭谣言首发账号，累计处置相关违法违规账号 8583 个，同时公开

曝光第五批部分网络谣言典型案例，有力发挥了警示震慑作用。（来源：网信中国）

4. 《中国互联网发展报告 2024》和《世界互联网发展报告 2024》蓝皮书发布

11 月 21 日，《中国互联网发展报告 2024》和《世界互联网发展报告 2024》蓝皮书在 2024 年世界互联网大会乌镇峰会上正式发布。

《中国互联网发展报告 2024》总结一年来中国互联网发展情况。报告指出，一年来，信息基础设施建设提速升级，对于经济社会发展的战略性、基础性和先导性作用日益凸显；数字经济政策体系化布局加速推进；数字公共服务普惠化扩容加深；网络空间主流思想舆论不断巩固壮大，网络文明建设提质增效；数字文化产业蓬勃发展；关键信息基础设施安全不断强化，国家网络安全应急体系不断健全完善；网信重点领域相关立法加快完善；构建网络空间命运共同体迈向新阶段等。

《世界互联网发展报告 2024》指出，一年来，世界各国稳步推进信息基础设施建设，进入扩容升级新阶段；数字技术发展日新月异，进入加速创新的爆发期；全球数字经济迎来新一轮发展热潮；世界各国愈加重视数字政府建设，政府数字化治理水平不断提升；数据治理成为网络空间国际治理的核心议题，但相关规则制度仍呈现碎片化、区域化、多极化特征等。（来源：人民网、网信中国）

5. 公安部网络安全法律咨询委员会2024年年会暨第十四届中国信息安全法律大会召开

11月22日，公安部在京召开网络安全法律咨询委员会2024年年会暨第十四届中国信息安全法律大会。会议由公安部网络安全法律咨询委员会和中国信息安全法律大会专家委员会主办，公安部第三研究所承办。

会议指出，公安部依托网络安全法律咨询委员会加强网络法治建设，是学习贯彻习近平法治思想的必然要求，是应对网络安全新形势新任务的必然要求，是提升国际规则话语权和制定权的必然要求，是公安机关推进法治中国、平安中国建设的应有之义，对建设平安网络、法治网络具有重要意义。

会议指出，2024年，全国公安机关在公安部党委的坚强领导下，在各有关部门的鼎力支持下，在各网络安全法律咨询委员的大力帮助下，深入推进网络安全立法、执法、司法工作，有效提升执法规范化水平。

会议强调，公安部网络安全法律咨询委员会要牢牢把握公安网络法治建设的政治方向，始终同以习近平同志为核心的党中央保持高度一致。要积极协同为网络空间治理献言献策，及时反映网络空间治理新诉求、老百姓新期盼，助力公安机关网络法治建设工作提质增效、创新发展。（来源：公安部网安局）

6. 360 发布《大模型安全漏洞报告》，曝光近 40 个大模型相关安全漏洞

11 月 25 日消息，360 数字安全集团近日发布《大模型安全漏洞报告》，从模型层安全、框架层安全以及应用层安全三大维度探查安全问题，对多个开源项目进行代码梳理和风险评估，最终审计并发现近 40 个大模型相关安全漏洞，影响范围覆盖 llama.cpp、Dify 等知名模型服务框架，以及 Intel 等国际厂商开发的多款开源产品。

报告指出，大模型的开放性和可扩展性使其在训练和推理过程中面临着数据投毒、后门植入、对抗攻击、数据泄露等诸多安全威胁。近年来，各大知名厂商的大语言模型因隐私泄露和输出涉及种族、政治立场、公共安全等不合规信息而引起社会广泛关注的案例屡见不鲜，为加强模型本身的安全性，研究人员开始从模型的可检测性、可验证性、可解释性进行积极探索。

报告强调，随着大模型项目需求的不断增长，各类开源框架层出不穷。开源框架极大提升开发效率，降低构建 AI 应用的门槛，同时也打开新的攻击面。开源框架在各个层级都可能因接触不可信的输入而产生潜在的安全风险。比如利用非内存安全语言引发内存安全问题，或者通过影响正常业务流程向框架传递恶意数据进行攻击，以及利用物理或虚拟主机集群所暴露的服务接口进行恶意控制等。

报告提出，除模型本身外，人工智能应用是多项计算机技术的有机结合，通常还包含许多其它工程代码实践来落地整套业务逻辑。这些代码涉

及输入验证、模型驱动、后向处理等多个方面，而不同分工模块间的业务交互可能会引入额外的安全问题，既包含传统的 Web 问题，又涵盖大模型能力导致的新问题。（来源：360 数字安全）

7. 前实习生篡改代码攻击大模型训练，字节跳动起诉索赔 800 万

11 月 27 日消息，字节跳动起诉前实习生田某某篡改代码攻击公司内部模型训练一案，近日已获北京市海淀区人民法院正式受理。字节跳动请求法院，判令田某某赔偿公司侵权损失 800 万元及合理支出 2 万元，并公开赔礼道歉。

根据字节跳动公告指出，2024 年 6 月至 7 月，字节跳动集团商业产品与技术部门前实习员工田某某，因对团队资源分配不满，通过编写、篡改代码等形式恶意攻击团队研究项目的模型训练任务，造成资源损耗。字节跳动已与其解除实习协议，同步阳光诚信联盟及企业反舞弊联盟，并同步至其就读学校处理。（来源：隐私护卫队）

境内前沿观察二：政策立法

导读：11 月，推动数字经济发展与数据资源开发利用成为国家和地方政策立法的重点关注。此外，打击电信网络诈骗、关键信息基础设施安全保护相关制度建设也取得进展。

推动数字经济发展方面。作为数字经济的重要组成部分，数字贸易已成为国际贸易发展的新趋势和经济的新增长点。对此，中共中央办公厅、国务院办公厅发布《关于数字贸易改革创新发展的意见》，围绕支持数字贸易细分领域和经营主体发展、推进数字贸易制度型开放、完善数字贸易治理体系等四方面提出十八条意见。地方层面，山东省济南市、烟台市同日公布《济南市数字经济促进条例》《烟台市数字经济促进条例》。

数据资源开发利用方面。国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》。可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施；行动计划提出可信数据空间提出能力建设、培育推广、筑基三大行动。国家数据局还发布《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案（征求意见稿）》，提出政务数据共享过程中，供给方按照“谁主管、谁提供、谁负责”的原则，承担数据提供前的安全管理责任；接收方按照“谁经手、谁使用、谁管理、谁负责”的原则，承担数据接收后的安全管理责任。地方层面，山东省大数据局印发《山东省数据交易管理办法（试行）》、湖南省人民政府办公厅印发《湖南省加强数据资产管理工作方案》。

打击电信网络诈骗方面。公安部会同国家发展和改革委员会、工信部、中国人民银行联合印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》。办法坚持依法认定、预防为主，分级惩戒、过惩相当以及公开公正、保障权益的思路，明确列出针对哪些人实施惩戒、针对哪些行为实施惩戒，主要目的是为了让社会公众清楚认知实施电信网络诈骗及其关联违法犯罪行为将承担的法律责任，从而实现警示教育、预防犯罪的效果。

国家密码管理局发布《关键信息基础设施商用密码使用管理规定（征求意见稿）》，要求关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

此外，《网络安全技术 软件供应链安全要求》（GB/T 43698—2024）、《网络安全技术 网络安全众测服务要求》（GB/T 43741—2024）等 13 项国家标准于 11 月开始实施；《网络安全技术 网络弹性评价准则》（GB/T44862-2024）等三项国家标准获批发布，将为各主体保障网络安全、供应链安全等方面提供细化指引。

关键词：数字经济、数据资源、打击电信网络诈骗、关键信息基础设施

（一）国家层面动向

1. 中共中央办公厅、国务院办公厅发布《关于数字贸易改革创新发展的意见》

11 月 28 日，中共中央办公厅、国务院办公厅发布《关于数字贸易改革创新发展的意见》。意见围绕支持数字贸易细分领域和经营主体发展、推进数字贸易制度型开放、完善数字贸易治理体系等四方面提出十八条意见。

推进数字贸易制度型开放方面，意见强调，要促进和规范数据跨境流动。健全数据出境安全管理制度，完善相关机制程序，规范有序开展数据出境安全评估。在保障重要数据和个人信息安全的前提下，建立高效便利安全的数据跨境流动机制，促进数据跨境有序流动。

完善数字贸易治理体系方面，意见提出，加强数字领域安全治理。优化调整禁止、限制进出口技术目录。持续推动全球数字技术、产品和服务供应链开放、安全、稳定、可持续。发挥各类专业法院法庭作用，推动数字领域国际商事争端解决机制多元化发展。（来源：中国政府网）

（二）部委层面动向

1. 国家互联网信息办公室发布《移动互联网未成年人模式建设指南》

11 月 15 日，国家互联网信息办公室发布《移动互联网未成年人模式建设指南》。指南共七章，主要面向移动智能终端、移动互联网应用程序、

移动互联网应用程序分发平台，提出未成年人模式建设的总体方案，具体包括使用时段、时长、内容和功能等方面，适用于未成年人模式的研发、建设、运营和管理。

其中，指南针对移动智能终端未成年人模式提出基本要求、使用时长管理、防绕过要求等。指南要求未成年人模式的入口设置应当确保最简化原则。用户可通过开机提醒、桌面图标、系统设置等至少 3 种方式进入未成年人模式。模式入口应当在醒目位置、便捷易寻，方便用户一键切换。用户在首次登录未成年人模式时，移动智能终端应当在入口提供设置生日、选择年龄或年龄区间等多种方式供用户自行选择，并允许设置多个未成年人用户。用户可在首次开机或系统设置选择不需要未成年人模式，系统将不再出现相关提醒。退出未成年人模式时，需要家长进行验证同意。移动智能终端应当在符合个人信息保护的前提下，提供密码、指纹、人脸等单一或复合验证方式。（来源：中国网信网）

2. 公安部等四部门印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》

11 月 26 日消息，公安部近日会同国家发展和改革委员会、工信部、中国人民银行联合印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》。办法共十八条，主要包括惩戒原则、惩戒对象、惩戒措施、分级惩戒、惩戒程序、申诉核查等六方面内容。办法主要考虑如下：

一是办法坚持依法认定、预防为主。办法严格按照《反电信网络诈骗法》的规定，进一步细化惩戒对象范围，坚持依法惩戒，区分了设区的市

级以上公安机关和省级以上公安机关审核认定惩戒对象的范围，进一步明确认定标准，更具有操作性。同时，办法明确列出针对哪些人实施惩戒、针对哪些行为实施惩戒，主要目的是为了让社会公众清楚认知实施电信网络诈骗及其关联违法犯罪行为将承担的法律责任，从而实现警示教育、预防犯罪的效果。办法还规定，在惩戒期限内，相关企业对被惩戒人员本人的银行账户、互联网账户、电话卡的多项功能进行限制，从技术层面严防再犯。

二是办法坚持分级惩戒、过惩相当。办法规定因实施电信网络诈骗及其关联犯罪被追究刑事责任的人，适用金融惩戒、电信网络惩戒、信用惩戒措施，惩戒期限为 3 年；经设区的市级以上公安机关认定具有非法买卖、出租、出借电话卡、物联网卡、固定电话、电信线路、短信端口、银行账号、支付账户、数字人民币钱包、互联网账号等行为的单位、个人或相关组织者，适用金融惩戒、电信网络惩戒以及纳入金融信用信息基础数据库，惩戒期限为 2 年，明确对不同惩戒对象实施不同种类的惩戒，体现过惩相当。同时，办法在综合运用金融惩戒、电信网络惩戒、信用惩戒等惩戒措施的同时，保留被惩戒对象基本的金融、通信服务，确保满足其基本生活需求，充分体现惩戒的适度性。

三是办法坚持公开公正、保障权益。办法第十二条规定书面告知条款，明确要求将惩戒依据、期限、措施和申诉权利书面告知被惩戒对象。办法明确申诉、受理、核查、反馈和解除等工作的程序和时限。办法强化依法惩戒的同时，设立申诉渠道，对于发现惩戒认定确有错误的，要及时解除

惩戒措施，充分保障申诉人的合法权益。（来源：公安部刑侦局、中国警察网）

3. 国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》

11 月 21 日，国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》。行动计划指出，可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。行动计划主要包括三大行动：一是实施可信数据空间能力建设行动，二是开展可信数据空间培育推广行动，三是推进可信数据空间筑基行动。

实施可信数据空间能力建设行动方面，行动计划提出稳慎探索个人可信数据空间。研究制定个人数据开发利用政策文件，在切实保护个人数据合法权益的基础上，建立健全个人数据确权授权和合规利用机制。条件成熟时，在符合国家法律法规、充分尊重个人意愿、保护个人权益的前提下，稳慎探索个人可信数据空间建设试点，通过制度创新和技术创新，提供依场景授权许可的个人数据转移流动和开发利用服务。数据管理机构应会同相关部门加强监管，指导和规范个人数据依法合理有效利用。

推进可信数据空间筑基行动方面，行动计划提出强化可信数据空间规范管理。建立健全可信数据空间合规管理指引，明确可信数据空间参与各方的基本要求和责权边界，防范利用数据、算法、技术等从事垄断行为。探索开展可信数据空间备案管理，动态发布备案名录。可信数据空间参与各方须遵守网络安全法、数据安全法、个人信息保护法等法律规定，落实

数据分类分级保护、动态感知、风险识别、监测预警、应急处置、治理监管等要求，建立可信数据空间安全管理体系。按照国家标准，引导和规范第三方开展可信数据空间核心能力评估。（来源：国家数据局）

4. 国家数据局发布《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案（征求意见稿）》

11 月 29 日，国家数据局发布《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案（征求意见稿）》。征求意见稿共提出七项主要任务，分别是明晰企业数据流通安全规则、加强公共数据流通安全管理、强化个人信息流通保障、完善数据流通安全责任界定机制、加强数据流通安全技术应用、丰富数据流通安全服务供给和防范数据滥用风险。

加强公共数据流通安全管理方面。征求意见稿提出，政务数据共享过程中，供给方按照“谁主管、谁提供、谁负责”的原则，明确政务数据共享范围、用途、条件，承担数据提供前的安全管理责任，探索建立接收方数据安全管理风险评估制度，确保数据在安全前提下有序共享。接收方按照“谁经手、谁使用、谁管理、谁负责”的原则，承担数据接收后的安全管理责任。

完善数据流通安全责任界定机制方面，征求意见稿强调，数据供给方应当确保数据来源合法，数据需求方应严格按照要求使用数据，防止超范围使用。鼓励供需双方在数据流通交易合同中约定各自权责范围，清晰界定权责边界。探索建立数据流通安全审计和溯源机制，完善数据流通安全

治理标准，融合应用数字水印、数据指纹、区块链等技术手段，高效支撑数据流通过程中的取证和定责。

防范数据滥用风险方面。征求意见稿要求，强化部门协同，加强数据安全、个人信息保护等方面的执法协同，推动行政执法信息共享、情况通报和协同配合，提高监管效能。组织发布数据流通安全治理典型案例，充分发挥示范作用，营造“一地创新、全国共享”“一企创新、多企复用”的创新环境，促进数据安全有序流通。（来源：国家数据局）

5. 国家卫生健康委员会办公厅印发《卫生健康行业人工智能应用场景参考指引的通知》

11 月 6 日，国家卫生健康委员会办公厅印发《卫生健康行业人工智能应用场景参考指引的通知》，围绕“人工智能+医疗服务管理”“人工智能+基层公卫服务”“人工智能+健康产业发展”“人工智能+医学教学科研”四方面十三个子方面，提出八十四个卫生健康行业人工智能应用场景。

其中，“人工智能+基层公卫服务”中的“人工智能+养老托育服务”子方面，指引提出智能托育机构安全隐患预警场景。通过人工智能实时检测托育机构的安全场所，智能预警托育机构的安全隐患，提高托育机构的安全水平。具体而言，通过云端协同的智能分析能力，应用陌生人识别、人群密度检测、烟火捕捉等安全预警算法模型，实现托育机构安全隐患全方位、无死角实时监控与智能预警。在托育机构安全隐患检测中，综合分析托育机构门口、走廊、厨房等存在安全隐患场所的实时视频画面，精准

捕捉潜在风险点，预警托育机构安全隐患，及时将预警信息推送托育从业人员，方便托育机构快速展开人工干预，全方位筑牢托育机构安全屏障。

“人工智能+健康产业发展”中的“人工智能+医用机器人”子方面，指引提出医疗咨询机器人场景。利用语言大模型、智能算法和医学知识库，与患者进行智能对话，提供医疗信息咨询，协助完成就诊、检查预约等服务，提高患者就医便捷性和准确性。适用于医院网站、健康管理平台、移动应用、门诊导诊等场景，利用语言大模型、智能算法和医学知识库进行理解和分析，通过文字输入或语音交互的方式与患者进行智能对话，回答患者关于疾病症状、健康管理、医疗常识等方面的问题，提供医疗信息咨询与就诊服务。与医院信息系统对接，实现医疗预约、药品购买、健康档案管理等功能，为患者提供全方位的医疗服务和健康管理服务支持，提升患者就医体验，减轻医务人员负担。（来源：国家卫生健康委员会）

6. 国家密码管理局发布《关键信息基础设施商用密码使用管理规定（征求意见稿）》

11 月 15 日，国家密码管理局发布《关键信息基础设施商用密码使用管理规定（征求意见稿）》。征求意见稿共二十六条，包括运营者总体责任，商用密码技术、产品、服务使用要求，数据安全保护、个人信息保护要求等内容。

征求意见稿规定，关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码

技术应当通过国家密码管理部门审查鉴定。为关键信息基础设施提供的商用密码服务，其商用密码使用要求应当不低于其服务的关键信息基础设施。

征求意见稿规定，关键信息基础设施建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保关键信息基础设施商用密码的正确使用和商用密码保障系统的有效运行。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，并在改造期间采取必要措施保证关键信息基础设施运行安全。（来源：国家密码管理局）

7. 七部门联合印发《推动数字金融高质量发展行动方案》

11 月 27 日消息，中国人民银行、国家发展改革委、工信部、金融监管总局、中国证监会、国家数据局、国家外汇局近日联合印发《推动数字金融高质量发展行动方案》。方案围绕系统推进金融机构数字化转型、运用数字技术提升重点领域金融服务质效、完善数字金融治理体系等六方面提出二十三条行动。

夯实数字金融发展基础方面，方案提出要加强数字金融相关新型基础设施建设。指导有条件的金融机构规划建设绿色智能金融数据中心，推动新增算力向国家枢纽节点集聚，支持海量数据存储和实时数据调用。建设优化高可靠冗余的网络架构，提高金融网络健壮性和服务能力，为金融数字化转型架设通信高速公路。布局先进高效的算力体系，加快云计算、人工智能等技术规范应用，探索运用边缘计算和量子技术突破现有算力瓶颈，为金融数字化转型提供精准高效的算力支持。

完善数字金融治理体系方面，方案指出要加强数据和网络安全防护。指导金融机构严格落实数据保护法律法规和标准规范，完善数据安全管理体系，强化数据安全的商用密码保护，建立健全全流程数据安全管理机制。组织金融机构定期进行数据和网络安全风险评估，识别潜在风险，接入金融行业相关网络安全态势感知平台，推动相关平台互联互通。开展网络安全相关压力测试，提升网络安全防护体系建设水平。搭建证券业数据和网络安全公共服务平台，加强基础、共性安全支撑。（来源：中国人民银行）

8. 全国网安标委归口的 3 项网络安全国家标准获批发布

11 月 5 日，根据 2024 年 10 月 26 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 24 号），全国网安标委归口的 3 项国家标准正式发布，分别是：《网络安全技术 终端计算机通用安全技术规范》（GB/T 29240-2024）《网络安全技术 存储介质数据恢复服务安全规范》（GB/T 31500-2024）《网络安全技术 网络弹性评价准则》（GB/T44862-2024）。（来源：全国网安标委）

9. 全国网安标委秘书处、香港私隐公署发布《网络安全标准实践指南——粤港澳大湾区（内地、香港）个人信息跨境处理保护要求》

11 月 21 日，全国网络安全标准化技术委员会秘书处、香港个人资料私隐专员公署发布《网络安全标准实践指南——粤港澳大湾区（内地、香港）个人信息跨境处理保护要求》。

指南规定粤港澳大湾区（内地、香港）个人信息处理者或者接收方，在大湾区内地和香港间通过安全互认方式进行大湾区内个人信息跨境流动应遵守的基本原则和要求，适用于指导大湾区内个人信息处理者开展个人信息跨境处理活动。

指南提出个人信息处理要求，包括“个人信息处理合法性基础”“个人信息收集”“个人信息存储、使用、加工”“个人信息委托处理、提供、公开”“个人信息跨境”。

个人信息处理合法性基础方面，指南提出个人信息处理者、接收方处理个人信息应符合属地法律法规要求。粤港澳大湾区内内地的个人信息处理者、接收方处理个人信息应当符合下列情形之一：一是取得个人的同意；二是为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；三是为履行法定职责或者法定义务所必需；四是为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；五是为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；六是在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；七是法律、行政法规规定的其他情形。香港特别行政区的个人信息处理者、接收方而言，处理个人信息应符合香港《个人资料（私隐）条例》相关规定。（来源：全国网安标委）

10. 13 项网络安全国家标准于 11 月开始实施

11 月，《网络安全技术 信息技术安全评估准则》等 13 项网络安全国家标准开始实施。

《网络安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型》（GB/T 18336.1—2024）、《网络安全技术 信息技术安全评估准则 第 2 部分：安全功能组件》（GB/T 18336.2—2024）、《网络安全技术 信息技术安全评估准则 第 3 部分：安全保障组件》（GB/T 18336.3—2024）、《网络安全技术 信息技术安全评估准则 第 4 部分：评估方法和活动的规范框架》（GB/T 18336.4—2024）、《网络安全技术 信息技术安全评估准则 第 5 部分：预定义的安全要求包》（GB/T 18336.5—2024）、《网络安全技术 信息技术安全评估方法》（GB/T 30270—2024）6 项推荐性国家标准，是对软件、硬件、固件形式的 IT 产品及其组合进行安全测评的基础标准，为产品消费者、开发者、评估者提供了基本的安全功能和保障组件，内容吸纳了国际网络安全评估领域模块化评估、多重保障评估、供应链分析等最新理念，将为我国具有安全功能 IT 产品的开发、评估以及采购过程提供指导。

《网络安全技术 无线局域网客户端安全技术要求》（GB/T 33563—2024）、《网络安全技术 无线局域网接入系统安全技术要求》（GB/T 33565—2024）两项推荐性国家标准，规定了无线局域网客户端与接入系统的安全功能要求和安全保障要求，给出了无线局域网客户端与接入系统面临安全问题的说明，能够为无线局域网客户端产品与接入系统的测试、研制和开发提供指导。

《网络安全技术 零信任参考体系架构》（GB/T 43696—2024）、《网络安全技术 证书应用综合服务接口规范》（GB/T 43694—2024）两项推荐性国家标准，分别规定了零信任参考体系架构以及面向证书应用的综合服务接口要求和相应验证方法，对于采用零信任体系框架的信息系统的规划、设计，公钥密码基础设施应用技术体系下证书应用中间件和证书应用系统的开发，以及密码应用支撑平台的研制和检测具有重要意义。

《网络安全技术 软件供应链安全要求》（GB/T 43698—2024）、《网络安全技术 网络安全众测服务要求》（GB/T 43741—2024）、《网络安全技术 软件产品开源代码安全评价方法》（GB/T 43848—2024）3 项推荐性国家标准，分别确立软件供应链安全目标，规定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，描述网络安全众测服务的角色以及职责、服务流程、安全风险、服务要求，规定软件产品中的开源代码成分安全评价要素和评价流程，对软件供应链中的供需双方开展风险管理、组织管理和供应活动管理具有引领和促进作用，将为网络安全众测服务活动提供帮助指导，助力各方对软件产品包含的开源代码成分进行静态安全评价。（来源：网信浙江）

（三）地方层面动向

1. 山东省大数据局印发《山东省数据交易管理办法（试行）》

11 月 5 日，山东省大数据局印发《山东省数据交易管理办法（试行）》，自 2024 年 12 月 6 日起施行，有效期至 2026 年 12 月 5 日。办法共八章二十七条，包括交易标的、交易主体、交易方式、交易行为等内容。

交易标的方面，办法规定，数据交易标的主要为数据产品，包括数据接口类、数据集类、数据报告类、数据服务类、数据工具类、数据应用类、算法模型类等类型。

交易主体方面，办法鼓励数据供需双方通过数据交易机构开展数据交易，鼓励公共数据授权运营方式加工形成的数据产品在数据交易机构开展交易。数据交易机构应当对在本机构交易的数据供需双方身份和交易标的进行审核，出具交易凭证，做到交易过程可控制、风险可防范、责任可追溯。此外，办法还规定第三方专业服务机构的义务。第三方专业服务机构是指提供数据集成、数据经纪、合规认证、数据检测、安全审计、数据公证、数据保险、数据托管、资产评估、争议仲裁、风险评估等专业服务的机构，应当具备从事相关业务的资质，在安全可控的前提下，提供第三方专业服务。（来源：山东省大数据局）

2. 山东省济南市人大常委会公布《济南市数字经济促进条例》

11 月 21 日，山东省济南市人大常委会公布《济南市数字经济促进条例》，自 2025 年 1 月 1 日起施行。条例共七章六十条，包括数字基础设施建设、

数字产业化与产业数字化、政务与公共服务数字化、数据开发利用与保护等内容。

条例强调，市、区县人民政府应当推进数据空间、隐私计算、区块链、精准授权、数据沙箱等技术应用，增强数据利用可信、可控、可计量能力。网信、公安、工业和信息化、大数据等部门应当按照职责分工，采取数据分类分级、标识登记、资产权益凭证等安全措施，加强安全产品的拓展应用。建立网络安全监测、预警、应急响应联动机制，提升网络安全态势感知、威胁发现、应急指挥、协同处置和攻击溯源能力。

条例规定，严格落实个人信息授权使用、数据安全使用承诺和重要数据出境安全管理等相关制度。网信、公安等部门发现数据安全缺陷、漏洞等风险时，应当督促其立即采取补救措施。（来源：济南人大）

3. 山东省烟台市人大常委会公布《烟台市数字经济促进条例》

11月21日,山东省烟台市人大常委会公布《烟台市数字经济促进条例》,自2025年1月1日起施行。条例共十章六十二条，包括数字化治理、服务推进体系、数据安全、数字基础设施等内容。

条例提出，市、区（市）人民政府及其有关部门应当对数据资源实施全生命周期管理，挖掘数据资源要素潜力，提升数据要素质量，培育数据要素市场，促进数据资源开发利用，充分发挥数据的关键资源和创新引擎作用。

条例强调，市、区（市）人民政府应当推动数字技术在经济调节、市场监管、社会治理、公共服务、生态环境保护、政府自身运行等领域的应

用，逐步实现政府履职全业务、全流程数字化，提高政府科学决策、高效监管、精准治理水平。应急管理、卫生健康、公安等部门应当加强数字技术在突发自然灾害、事故灾难、公共卫生事件和社会安全事件中的应用，推动应急救援信息共享共用，提高应急监测预警、应急救援处置能力。（来源：烟台人大）

4. 安徽省通信管理局等十二部门印发《关于推动新型信息基础设施协调发展有关事项的通知》

11 月 6 日，安徽省通信管理局联合省工业和信息化厅、省委网信办、省教育厅等十一部门印发《关于推动新型信息基础设施协调发展有关事项的通知》。

通知从八个方面作出工作部署：一是加强全省统筹规划布局。统筹规划骨干网络设施，优化布局算力基础设施，合理布局新技术设施；二是推动省域均衡普惠发展。推进基础设施开放发展，深化地区间均衡协调发展，促进城乡融合普惠发展；三是加强跨网络协调联动发展。推进多种网络端到端协同升级，鼓励网络与算力设施协同发展；四是加强跨行业融合共享发展。推进信息设施与传统设施融合发展，深化电信基础设施跨行业共建共享；五是构建绿色低碳发展方式。推进重点设施绿色低碳发展，促进设施与环境协调发展；六是增强全方位安全保障能力。提升网络和数据安全保障能力，增强跨行业安全服务赋能，增强信息基础设施稳定安全运行能力；七是加强跨部门政策协调。发挥要素配置牵引作用，协同推进跨领域

标准化工作，加大投融资支持；八是加强组织实施。加强组织领导，强化协同落实，跟踪评估问效。（来源：安徽省通信管理局）

5. 广东省广州市促进智能网联与新能源汽车产业发展工作专班印发《在不同混行环境下开展智能网联汽车（自动驾驶）应用示范运营的工作方案（第二版）》

11 月 11 日，经广州市人民政府同意，广州市促进智能网联与新能源汽车产业发展工作专班印发《在不同混行环境下开展智能网联汽车（自动驾驶）应用示范运营的工作方案（第二版）》。方案包括智能网联汽车混行范围及场景、示范运营主体准入条件、示范运营区域事故和违法处理要求、运营主体退出机制等内容。

准入条件方面，方案要求，应用示范运营主体须配备智能网联汽车（自动驾驶）安全保障团队，具备应急处理能力；配备网络和数据安全专家团队，建立数据安全管理制度，通过相应技术措施建立全面立体的安全防护体系。应用示范运营车辆准入方面，方案要求，车辆应当安装车辆行驶数据记录设备、车载视频设备、车辆位置设备和车联网设备等车载设备，全程连续记录和存储车辆运行状态、驾驶模式、车内外视频等数据，并将相关数据接入且存储在广州市智能网联汽车（自动驾驶）应用示范运营监控平台。

示范运营区域事故和违法处理要求方面，方案提出应用示范运营区域须建立迅速报告机制、事故技术评估机制、先行赔付机制。事故发生后，运营主体应当立即抢救伤者、固定现场证据并报警（报警需说明时间、地

点、是否有伤亡或车损、是否是无人驾驶车辆等信息），于事发后 15 分钟内向市承担智能网联汽车（自动驾驶）示范运营具体组织工作的第三方机构报告。第三方机构接到事故报告后，应立即通过智能网联汽车（自动驾驶）监控平台锁定车辆信息，固定现场证据，于 1 小时内向运营主体注册地区政府和市专项工作组口头汇报，于 3 小时内提交书面报告。（来源：广州市人民政府）

6. 湖南省人民政府办公厅印发《湖南省加强数据资产管理工作方案》

11 月 14 日，湖南省人民政府办公厅印发《湖南省加强数据资产管理工作方案》。方案围绕建立数据资产管理机制、推动数据资产开发利用、加强数据资产管理协同共治、开展数据资产管理试点、加强数据资产风险防控五方面提出十八条工作任务。

建立数据资产管理机制方面，方案提出规范数据资产处置管理。建立健全公共数据资产处置审批流程，依据处置事项批复等相关文件及时处置数据资产，严禁擅自处置，防范数据资产流失或泄露等造成法律和安全风险。对经过认定失去价值、没有保存要求的数据资产，进行安全和脱敏处理后及时有效销毁，严格记录数据资产销毁过程相关操作。

加强数据资产管理协同共治方面，方案提出构建跨部门合作机制。协同建立统一的公共数据标准体系，全面识别和分类数据资源，维护并动态更新公共数据资源目录。协同推动数据资源汇聚，实现数据资源的挂接和共享，提升共享意愿和价值。协同推动数据治理提质，明确数据质量责任

主体，定期实施数据质量核查与反馈，确保数据资产的准确性、完整性和时效性，形成“谁生产、谁治理、谁提供、谁负责”的闭环管理体系。（来源：网信湖南）

境内前沿观察三：治理实践

导读：11 月，公安、网信、工信、市场监督管理等部门持续开展行政执法，从平台算法治理、信息内容治理、网络安全保护、个人信息保护等方面消除风险隐患，强化主体责任。

治理对象方面，网络平台仍是各部门重要治理对象，平台算法安全成为 11 月重点治理视角。中央网信办、工信部、公安部、国家市场监督管理总局联合开展“清朗·网络平台算法典型问题治理”专项行动，提出包括落实算法安全主体责任在内的六个主要任务，旨在实现算法导向正确、算法公平公正、算法公开透明、算法自主可控、算法责任落实五项工作目标。北京互联网法院首例“搜索提示词”算法侵权案宣判，法院认为搜索排序、搜索提示、搜索联想是典型的算法推荐与搜索功能相结合的应用场景。平台生成的搜索排序、搜索提示、搜索联想是否侵权，应当综合考虑是否有人工参与生成或审核、侵权内容是否明显或易于判定、平台的审核技术能力、平台是否因此盈利等因素，认定平台是否知道或者应当知道侵权内容，并结合平台是否采取删除、屏蔽、断开链接等必要措施最终判定。

治理方式方面，随着《网络安全法》《数据安全法》《个人信息保护法》均明确有关部门有权开展约谈，约谈逐渐成为引导督促主体落实安全保护义务、提升主体安全意识的重要手段。湖南省网信办联合湖南省市场监管局集中约谈 17 款问题 App 和微信小程序运营企业负责人，聚焦餐饮外卖、房屋租售、商超购物、停车约车等社会关注度较高、个人信息被滥用

和过度索取乱象突出的四类消费场景。某医疗公司因网站域名到期后未续费使用，亦未及时注销备案等违法行为，导致网站主页被篡改为网络赌博页面，违反《网络安全法》，江西警方对该公司网站业务负责人进行约谈。江西赣州警方联合网信部门约谈多名涉低俗内容的网络主播。

个案方面，快手公司因存在对法律、行政法规禁止发布或者传输的信息未及时处置，以及落实青少年模式不到位等情况，导致违法信息扩散，危害未成年人身心健康，违反《网络安全法》，公安机关依法对快手公司给予行政处罚，并依法依规处置违法违规账号。此外，福建警方发布两起涉“两高一弱”行政执法案例，并围绕高度关注高危漏洞、高危端口、弱口令问题，建立网络安全应急协调工作机制，加强网络安全教育三方面提出解决方案。

此外，我国公安部与美国国土安全部相关执法部门联合处置一起跨国电信网络诈骗案件，帮助一家浙江企业及其美方合作伙伴追回被骗资金170余万美元，有力维护相关企业合法权益。目前，中美两国执法部门正积极推进案件侦办工作。

关键词：网络平台、算法治理、约谈、两高一弱

（一）公安机关治理实践

1. 公安部公布三起涉网金融犯罪典型案例

11 月 6 日，公安部公布三起涉网金融犯罪典型案例。

案例一：上海张某鹏等人涉嫌非法经营案

2024 年 7 月，上海公安机关依法立案侦办张某鹏等人涉嫌非法经营案。经查，2022 年 10 月以来，犯罪嫌疑人张某鹏组织招揽技术开发、App 运营、黑灰产引流等数十人组成职业化非法放贷犯罪团伙，以“高利放贷”非法营利为目的，在境外开发运营 26 款网贷 App，向境内非法提供贷款业务，收取借款金额 30%-35%的高额周息，截至案发，累计向 5 万余人非法放贷 5.6 亿元。今年 8 月，办案单位开展收网打击，抓获以张某鹏为首的 22 名犯罪嫌疑人。随后，公安部经侦局在本案基础上部署全国公安经侦部门开展集群打击，抓获犯罪嫌疑人 29 名，相关案件正在进一步侦办中。

案例二：安徽赵某等人涉嫌妨害信用卡管理案

2024 年 3 月，安徽省宿州市公安局依法立案侦办赵某等人涉嫌妨害信用卡管理案。经查，以犯罪嫌疑人赵某为首的犯罪团伙，利用社交软件招募卡商，并实时指使下线卡商人员在全国范围内大量非法买卖、持有、使用他人银行卡 3000 余张，涉案金额达 8000 余万元。今年 8 月，公安部经侦局在本案基础上部署全国公安经侦部门开展集群打击，抓获赵某等犯罪嫌疑人 38 名，相关案件正在进一步侦办中。

案例三：广东李某等人涉嫌窃取、收买、非法提供信用卡信息案

2024 年 6 月，广东省佛山市公安局依法立案侦办李某等人涉嫌窃取、收买、非法提供信用卡信息案。经查，自 2022 年 1 月以来，犯罪嫌疑人李某等人在互联网上销售信用卡信息，相关信息被购买者购得后无需信用卡密码便可直接用于网上消费、游戏平台充值、购物消费等变现。截至案发，该犯罪团伙共销售信用卡数万张，从中非法获利超 400 万元。公安部经侦局在本案基础上部署全国公安经侦部门开展集群打击，共抓获李某等犯罪嫌疑人 54 名，相关案件还在进一步侦办中。（来源：公安部）

2. 中美两国执法部门联合处置一起跨国电信网络诈骗案件

11 月 7 日，公安部发布消息称，与美国国土安全部相关执法部门近日联合处置一起跨国电信网络诈骗案件，帮助一家浙江企业及其美方合作伙伴追回被骗资金 170 余万美元，有力维护相关企业合法权益。目前，中美两国执法部门正积极推进案件侦办工作。（来源：公安部）

3. 江苏南京警方破获一起假冒余华英儿子造谣案

11 月 5 日消息，江苏省南京市公安机关网安部门近日工作中发现，有网民自称是余华英的儿子，在多个社交平台相继发布数条视频，引发大量网民关注、议论。南京公安网安部门迅速开展调查，经查，网民吴某某（男，24 岁，现住南京，网名“奶声奶气的咖啡”“魔鬼苏慧伦”）出于吸粉引流、赚取广告收益的目的，通过某社交平台自带软件剪辑视频，造谣称自己是余华英当年被卖掉的儿子，在网上恶意制作、发布虚假视频，扰乱网

络空间秩序，造成不良社会影响。目前，南京公安网安部门已依法对违法行为人吴某某给予行政处罚，相关账号已被封禁。（来源：中国警察网）

4. 浙江温州警方公布一起利用人工智能造谣案

11 月 11 日消息，浙江省温州市公安网安部门近日在工作中发现，一则《***市近期面临着一场严峻的天然气供应危机》的文章在网络流传。该信息迅速引发网民关注和议论，造成不良社会影响。温州网安部门立即开展核查，经核实此信息为谣言。

温州公安网安部门迅速找到发布该谣言的叶某。叶某到案后自述，其在网上浏览信息时看到“文章创作兼职”。后叶某按照流程向运营方提供注册好的文章平台账号，由运营方全权负责。该账号在运营过程中，产生的文章创作收益由双方均分。

温州公安网安部门将平台运营方负责人余某抓获归案。余某承认使用非法爬虫软件批量采集互联网公开文章，并通过 AI 工具批量改写后发布，造成大量谣言信息传播。余某利用上述方式，先后与多人达成“兼职合作协议”，由其运营他人的账号。目前，温州公安网安部门已依法对余某行政处罚，并对叶某进行批评教育。（来源：公安部网安局）

5. 福建警方发布两起涉“两高一弱”典型案例

11 月 18 日，福建警方发布两起涉“两高一弱”典型案例。

案例一：前期，宁德市公安机关网安部门接报案，某单位数据遭泄露，公安机关网安部门高度重视，经现场检查发现，该单位为方便系统日常维

护，将信息管理系统外联互联网，外联软件设置弱口令导致被黑客破解。该单位未建立全流程数据安全管理制度、未落实网络安全等级保护制度、未履行数据安全保护义务，违反《网络安全法》相关规定，宁德市公安机关对该单位处以行政处罚。

案例二：近期，宁德市公安机关网安部门在工作中发现某旅游公司门户网站存在任意文件上传高危漏洞，网页被黑客篡改。经查，该公司网站未制定相应的网络安全管理制度，未采取必要的安全技术防范措施，存在严重网络安全隐患。宁德市公安机关依据《网络安全法》第二十一条、五十九条，对该公司处以行政处罚。

对此，福建警方提出三项解决方案：一是要高度关注高危漏洞、高危端口、弱口令问题，定期升级系统，强化密码策略，关闭非必要端口。合理配置防火墙、入侵检测系统（IDS/IPS）、防病毒软件等，有效防范黑客攻击；二是建立网络安全应急协调工作机制，制定网络安全事件应急预案，定期组织安全演练，发现被黑客入侵，及时切断网络，保存好相关证据，并向当地公安机关报案；三是加强网络安全教育，党政机关企事业单位应定期组织安全培训，提高员工的安全意识和防范能力。（来源：公安部网安局）

6. 因公司网站主页被篡改，江西警方依法约谈某公司

11 月 21 日消息，江西警方近日在工作中发现，某公司网站被篡改，存在较大风险。经查，该公司主营业务为医疗、保健品类生产销售，建设网站用于公司产品业务宣传。该网站域名到期后未续费使用，亦未及时注销

备案，日常网络安全管理义务履行不到位，导致网站主页被篡改为网络赌博页面，相关行为违反《网络安全法》有关规定。

公安机关网安部门依法对该网站业务负责人进行约谈，责令对到期不再使用的域名及时注销备案，要求依法依规办网，切实履行网站平台主体责任。该公司网站业务负责人表示，已深刻认识到问题严重性，将配合公安网安部门的监管，立即进行整改。（来源：公安部网安局）

7. 因短视频存在违法信息，公安机关依法处罚快手公司

11 月 22 日消息，公安机关近日依据《网络安全法》规定，针对快手公司短视频中存在违法信息等问题，依法给予快手公司警告处罚。

经查，快手公司存在对法律、行政法规禁止发布或者传输的信息未及时处置，以及落实青少年模式不到位等情况，导致违法信息扩散，危害未成年人身心健康，违反《网络安全法》相关规定。公安机关依法对快手公司给予行政处罚，责令其全面落实青少年模式，全面排查清理违法信息，并依法依规处置违法违规账号。（来源：国家网络安全通报中心）

8. 江西省赣州市两地公安机关联合网信部门约谈多名网络主播

11 月 25 日消息，江西省赣州市两地公安机关近日联合网信部门约谈多名网络主播。

江西省赣州市石城县公安网安部门近日在日常工作中发现，某平台主播董某（女）与孔某（男）为搏眼球、吸引流量，在直播中言语污秽、内容低俗，违反《互联网直播服务管理规定》《网络信息内容生态治理规定》

等，污染网络空间环境，造成不良社会影响。石城县公安机关网安部门随即依法对2名网络主播进行约谈教育。约谈中，民警带领主播学习相关规定，责令全面清理网络账号违规信息，要求遵守法律法规，遵循公序良俗，依法规范上网行为。通过约谈教育，2名主播深刻认识到了自己的错误，承诺今后将汲取教训、引以为戒，并当场写下了《规范网络行为保证书》。

江西省赣州市南康区公安机关近日联合区网信办对网民何某进行约谈。此前，南康区公安机关网安部门在工作中发现，网民何某长期在短视频平台发布低俗表演视频以此博人眼球、赚取流量。其行为严重扰乱网络秩序，造成恶劣社会影响。民警及网信办工作人员依法对其约谈教育。约谈中，民警及网信办工作人员组织何某认真学习相关法律法规，结合典型案例以案说法，对何某进行批评教育。通过教育引导，何某深刻认识到了自身错误，删除违规短视频，并签订《网络自律承诺书》，表示会严格遵守相关法律法规。（来源：公安部网安局）

9. 新疆警方公布打击整治网络黑灰产违法犯罪5起典型案例

11月1日，新疆警方公布5起打击整治网络黑灰产违法犯罪典型案例。

案例一：2024年3月，阿勒泰地区阿某加入一电信网络诈骗团伙群组，受电诈团伙成员拉拢，先后向对方累计出售他人社交平台实名注册网络账户130余个，非法获利12万余元。目前，阿某已被依法刑事立案。

案例二：2024年4月，乌鲁木齐市张某通过搭建中介平台，有偿为他人提供“直播间刷虚假人气”“网络账号增加虚假粉丝数”“短视频和文

章刷转评赞”等，从中赚取“中介费”，非法获利5万余元。目前，张某已被依法刑事立案。

案例三：2024年4月，克孜勒苏柯尔克孜自治州吾某伙同阿某等人，使用本人和亲友手机帮助境外电信网络诈骗团伙累计发送涉诈短信30万余条，非法获利23万余元。公安机关警串并同类案件，连带破获电信网络诈骗案件6起。目前，吾某、阿某2人因涉嫌帮助信息网络犯罪活动罪被分别判处有期徒刑。

案例四：2024年6月，吐鲁番市邓某方伙同邓某康、胡某某等人流窜各地，利用扫码送礼品等方式引诱群众在个人群组内大量转发诈骗信息，涉嫌从事推广引流网络黑产违法犯罪活动。目前，邓某方已被依法刑事立案，邓某康、胡某萍等人已被依法行政拘留。

案例五：2024年8月，阿勒泰地区胡某某伙同刘某、弟某某、杨某某等人通过网络联系，购买、安装加油机作弊设备，并利用该作弊设备对移动加油机面板进行参数配置远程修改，人为影响加油机正常加油，非法获利200万余元。目前，上述4名犯罪嫌疑人已被依法刑事立案。（来源：公安部网安局）

10. 四川警方公布一起冒充公职人员造谣案

11月3日，四川警方成功打掉一个冒充公职人员，伪造政府“红头文件”，诱骗他人转发谣言，蛊惑群众购买网络课程的犯罪团伙。

四川警方发现磨某全等人冒充国家公职人员，编制话术，伪造政府“红头文件”，蒙骗诱导相关单位工作人员，转发谣言信息以及定制的网络课

程链接至互联网通讯群组，诱导网民购买其网络课程并从中牟取非法利益。四川警方分赴两地开展同步收网行动，将磨某全等 8 人抓获归案。捣毁犯罪窝点 2 个，抓获犯罪嫌疑人 8 名，扣押涉案电脑 6 台，手机 168 部，印章 6 个，话术本 19 本。

磨某全等人均对犯罪事实供认不讳，并主动积极配合公安机关调查。目前磨某全等人均被依法采取刑事强制措施。（来源：公安部网安局）

11. 江苏常州警方破获一起老年机“无端扣费”案

11 月 18 日消息，江苏省常州市金坛警方近日破获一起老年机“无端扣费”案。

2023 年 2 月，金坛警方接到多名老人报案称，老人机被无端扣费。经过对“自动扣费”手机数据的分析和追踪，警方发现手机网络数据指向一台架设在深圳的服务器。老人机被该台服务器远程操控，导致“自动订购”增值业务。经调查发现，全国有 98 万部手机存在非机主本人订购额外增值业务的情况，涉案金额高达 347 万元。警方立即赶赴深圳将服务器控制人张伟生抓获，并第一时间提取服务器数据，将服务器关闭。

经查，2019 年 9 月，张伟生找到深圳宇舟科技公司负责人李明，由李明负责联系代理商，并将他们的服务短信、语音电话的服务通道号码、控制指令等参数发送给张伟生，张伟生则通过服务器后台向功能机发出指令，扣取话费，扣除给代理商的费用后，所得利润二人按八二分。2019 年 10 月，张伟生结识专门开发手机主板的易通达科技公司员工方凯。张伟生联合方凯，将控制老年机的代码植入公司开发的主板。被植入恶意扣费软件的主

板被卖给专门生产老人机的厂家。此后，张伟生招聘2名程序员陈贤、朱锡帮他搭建、维护手机销售管理系统。该系统可以控制载有恶意扣费代码的老人机，并能给手机发送短信、屏蔽资费提示、删除短信、拨打语音电话，达到在手机用户不知情的情况下自动订购增值服务、秘密扣取资费的目的。

2023年3月，张伟生、李明等人因涉嫌盗窃罪被金坛区检察院批准逮捕。2024年2月，张伟生、李明等人盗窃案经江苏省常州市金坛区法院依法审理，张伟生被判处有期徒刑十二年，并处罚金30万元；李明被判处有期徒刑十年，并处罚金18万元。一审判决后，被告人提出上诉。近日，常州市中级人民法院裁定驳回上诉，维持原判。2024年5月，公安机关以方凯、陈贤、朱锡涉嫌盗窃罪移送至检察机关审查起诉。（来源：江苏警方）

12. 福建南平警方侦破一起针对某电商购物平台刷单控评非法营利的“网络水军”全链条案件

11月22日消息，福建省南平市公安网安部门近日成功侦破一起针对某电商购物平台刷单控评非法营利的“网络水军”全链条案件，一举捣毁犯罪窝点4个，抓获犯罪嫌疑人15名。

南平公安网安部门工作中发现，有辖区居民在为某电商购物平台商户虚刷销量和好评，从中赚取佣金。通过深入调查，一个分工明确且有完整利益链条的网络水军犯罪团伙浮出水面。

公安网安部门快速行动，组织警力分赴多地，将以林某、丁某为首的15名犯罪嫌疑人悉数抓获，并在其窝点查获大量电脑、手机等作案工具。

经查，该犯罪团伙在某电商购物平台“网络刷单”高达3000余万次，涉案金额上千万元，严重扰乱市场公平竞争秩序，损害消费者合法权益。

经查，曾为某电商购物平台商户的林某发现利用平台虚假刷单有利可图，于是招募人员开发多款刷单软件，发布虚刷销量和好评的广告，通过网络发布刷单任务，广泛招募刷手使用软件批量刷单，按刷单量结算佣金，逐步形成了一个覆盖技术开发、推广运营、招揽客户、网络刷手等多环节的犯罪链条。目前，涉案犯罪嫌疑人均已被依法采取刑事强制措施，案件正在进一步侦办中。（来源：公安部网安局）

13. 浙江慈溪警方全链条摧毁一“网络水军”团伙

11月25日消息,浙江省慈溪市警方近日重拳出击,全链条摧毁一个“网络水军”团伙，抓获多级中介以及刷手等犯罪嫌疑人7人，涉案资金流水高达千万元。

慈溪市公安网安部门在工作中发现，在慈溪一出租房内，一男子购置30余部工作机，试水接单，为他人提供刷流量服务以此牟利。民警顺藤摸瓜，发现一个网站，该网站正是能为他人提供虚假刷人气、点赞、评论、增粉等服务的中介平台。通过这个网站，注册用户可以直接在网站中下单，也可以设立自己的代理分站，进一步发展分销商。

民警发现，这个网站下设有30多个代理网站。这些注册用户通过层层增设代理的方式来实现获利最大化。该网站每天的成交量可能达成千上万单，交易对象又分布在全国各地。经查，公安机关最终确定实际运营者为

党某堂和刘某浩二人。慈溪公安组织警力，将正在实施虚假点评赞服务的两人成功抓获。

据党某堂二人交代，两人为亲戚关系，在党某堂的提议下，由党某堂搭建、维护中介平台，刘某浩作为网站客服对接上下级。两人一方面通过他人代理的抽成得利，另一方面自己也充当中介接单，随后将需求提供给上级转包商或直接给刷手工作室，实现虚假刷量。

经工作，慈溪警方进一步锁定吴某成、吴某伟和杨某宣等三名经营此类中介平台的嫌疑人，以及一个专门帮助党某堂实施虚假刷人气的刷手团伙李某、吴某飞。警方再次开展收网工作，成功抓获以上人员。截至目前，警方共抓获犯罪嫌疑人 7 人，扣押用于虚假刷量的“云控虚拟机”3 台、“线控水军手机”623 部，捣毁“水军工作室”4 处，及时关停涉案“网络水军”虚假刷量接单网站总站 3 个、二级代理站点 32 个。（来源：公安部网安局）

14. 山西长治警方破获特大侵犯公民个人信息案

11 月 26 日消息，山西省长治市公安机关近日成功打掉一个特大侵犯公民个人信息及掩饰、隐瞒犯罪所得的犯罪团伙，抓获犯罪嫌疑人 10 名，扣押涉案资金 500 余万元。

长治公安网安部门工作发现，辖区女子郑某燕在多个小区以赠送小礼品、小礼物为诱饵，诱骗群众扫描二维码、推广码注册各类 APP，通过窃取群众手机号码及验证码非法获利 3 万余元，涉嫌侵犯公民个人信息犯罪。掌握确凿证据后，民警将郑某燕抓获归案。

以此为突破口，长治市公安网安部门全力展开侦查。经过分析研判、深挖扩线，循线追踪辗转各地展开收网行动，共抓获涉嫌侵犯公民个人信息以及掩饰、隐瞒犯罪所得的犯罪嫌疑人10名。经查，该特大侵犯公民个人信息犯罪团伙以赠送小礼品、小礼物等地推形式，诱骗普通群众使用自己的手机号码注册各类APP的虚拟账号，后窃取公民个人信息用于上游犯罪分子实施网络诈骗、网络敲诈、网络刷单等违法犯罪活动。

目前，犯罪嫌疑人均已被依法采取刑事强制措施，案件正在进一步侦办中。（来源：公安部网安局）

15. 云南曲靖警方破获一起倒卖网络账号案

11月29日消息，云南省曲靖市警方近日破获一起倒卖网络账号案。截至案发，该团伙共倒卖社交账号4000余个，获利近50万元。

云南曲靖警方经过两个多月的调查，于7月份先后在曲靖沾益区、经开区将犯罪嫌疑人王某、孙某、冀某抓获，捣毁犯罪窝点3处，缴获作案使用手机7部、电脑2台。

经查，王某等人如实交代开办工作室，由孙某、冀某在网上发布兼职广告，王某负责指导应聘人员用自己的手机号实名注册各互联网平台社交账号，进行收购后，再转售给他人进行获利的犯罪事实。目前，王某、孙某、冀某3人因涉嫌侵犯公民个人信息罪已被移送检察院提起公诉。（来源：公安部网安局）

（二）网信部门治理实践

1. 四部门联合开展“清朗·网络平台算法典型问题治理”专项行动

11 月 12 日，中央网络安全和信息化委员会办公室秘书局、工信部办公厅、公安部办公厅、国家市场监督管理总局办公厅联合印发通知，开展“清朗·网络平台算法典型问题治理”专项行动。

专项行动包括六个主要任务：一是深入整治“信息茧房”、诱导沉迷问题；二是提升榜单透明度打击操纵榜单行为；三是防范盲目追求利益侵害新就业形态劳动者权益；四是严禁利用算法实施大数据“杀熟”；五是增强算法向上向善服务保护网民合法权益；六是落实算法安全主体责任。

提升榜单透明度打击操纵榜单行为方面，专项行动要求全面公示热搜榜单算法原理，提升榜单透明度和可解释性。完善榜单日志留存，提高榜单算法原理可验证性。健全水军刷榜、水军账号等违规行为、账号检测识别技术手段，严管不法分子恶意利用榜单排序规则操纵榜单、炒作热点行为。

落实算法安全主体责任方面，专项行动强调健全算法机制机理审核、数据安全的管理制度和技术措施。确保算法的训练数据具有合法来源，及时检测修复代码安全漏洞和算法逻辑缺陷，定期对算法模型的可用性、可控性、可解释性以及数据处理、模型训练、部署运行等环节开展安全评估。

专项行动还提出算法导向正确、算法公平公正、算法公开透明、算法自主可控、算法责任落实五项工作目标。（来源：网信中国）

2. 重庆市巴南区六部门联合开展网络安全检查

11 月 22 日消息，重庆市巴南区委网信办近日牵头联合经信、公安、文旅、卫健、审计、大数据等六部门组成联合检查组，在全区范围内深入开展网络安全现场检查。

本次检查覆盖政务、文化、教育、医疗、企业等多个关键领域，通过现场访谈、资料查阅、技术扫描等多种检查方式，对区内 23 家重点单位进行了全面细致的检查评估。检查发现部分单位在落实网络安全工作责任制、互联网政务应用管理及技术防护等方面存在问题。检查组已第一时间向相关单位提出整改意见，明确整改期限，确保问题得到彻底、有效解决。（来源：网信重庆）

3. 湖南省网信办、省市场监管局联合执法约谈 17 家应用程序运营企业负责人

11 月 8 日，湖南省网信办联合湖南省市场监管局聚焦全省餐饮外卖、房屋租售、商超购物、停车约车等社会关注度较高、个人信息被滥用和过度索取乱象突出的四类消费场景，依法对存在“超范围收集、频繁索取个人信息”“未经用户同意或默认收集个人信息、强制收集个人信息”等问题的 17 款问题 App 和微信小程序运营企业负责人进行集中约谈。

约谈要求以上应用程序运营企业充分提高思想认识，切实加强个人信息全生命周期保护，认真落实企业主体责任。对存在的问题，从制度、管理和技术等方面提出针对性整改方案，做到个人信息采之有界、用之有度、护之有责。以上应用程序运营公司负责人均表示，将严格按照网信、市监

等部门工作要求，切实提高政治站位，认真组织学习互联网相关法律法规，对违法违规问题限期整改，严格落实平台主体责任，切实履行个人信息保护义务。（来源：网信湖南）

4. 因履行个人信息保护义务不到位，重庆市武隆区网信办对某物业公司依法处罚

11 月 22 日消息，重庆市武隆区网信办近日对武隆区某物业公司收集个人信息未履行个人信息保护义务依法处罚。

经查，该公司收集个人信息数据量较大，未制定内部管理制度和操作规程，未对个人信息实行分类管理，未采取去标识化安全技术措施，未合理确定个人信息处理的操作权限，未建立个人信息安全事件应急预案等相关管理制度，未按规定落实个人信息保护措施，存在个人信息泄露风险隐患，履行主体责任不到位，违反《个人信息保护法》第五十一条的规定。武隆区网信办依据《个人信息保护法》第六十六条的规定，责令该公司限期整改，并给予警告的行政处罚。（来源：网信重庆）

5. 因多次泄露数据，湖南省网信办对某信息技术公司作出行政处罚

11 月 29 日消息，湖南省互联网信息办公室近日依法查明，湖南某信息技术有限公司存在不履行网络安全、数据安全保护义务行为，其相关系统未采取技术措施和其他必要措施保障数据安全，存在未授权访问漏洞，造成部分数据多次泄露，严重损害数据安全。湖南省互联网信息办公室依据

《数据安全法》《湖南省网络安全和信息化条例》对该公司责令改正，给予警告，对该公司、主管人员和直接责任人员分别并处罚款二十万元、三万元和二万元的行政处罚。（来源：网信湖南）

（三）通信管理部门治理实践

1. 工信部、多地通信管理局通报侵害用户权益行为的 APP

（1）工信部

11 月 13 日，工信部通报 2024 年第 9 批，总第 44 批侵害用户权益行为的 APP（SDK）。通报指出，工信部近日组织第三方检测机构进行抽查，共发现 27 款 APP 及 SDK 存在侵害用户权益行为，涉及信息窗口“摇一摇”乱跳转或误导用户滑动乱跳转、违规收集个人信息、APP 频繁自启动和关联启动、信息窗口误导用户点击乱跳转等问题。上述 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）北京

11 月 1 日，北京市通信管理局通报 2024 年第 10 期问题 APP。通报指出，北京市通信管理局近日通过抽测发现北京市部分 APP 存在侵害用户权益和安全隐患类问题。截至目前，尚有 8 款 APP 未整改或整改不到位，涉及违反必要原则收集个人信息、违规向他人提供个人信息、账号注销难、未经用户同意收集使用个人信息、未明示收集使用个人信息的目的、方式和范围等问题，予以公开通报。

（3）山东

11 月 12 日，山东省通信管理局通报 2024 年第 9 批下架侵害用户权益 APP。通报指出，山东省通信管理局于 9 月 20 日向社会公开通报 22 款经检测发现存在侵害用户权益和安全隐患问题，且下发整改通知书后未在规定时限完成整改的 APP，并再次要求限期整改。截至再次要求的规定时限，仍有 6 款 APP 未完成整改反馈。山东省通信管理局决定对上述 6 款 APP 予以下架。相关应用商店应立即组织对名单中的 APP 进行下架处理，并举一反三，排查反复出现问题的 APP 开发运营者，严格落实分发平台主体责任，把好上架审核关。山东省通信管理局将对通报 APP 持续跟踪，视情况进一步采取断开网络、行政处罚、纳入电信业务经营不良名单等措施。

（4）浙江

11 月 26 日，浙江省通信管理局通报 2024 年第 11 批存在侵害用户权益行为的 APP。通报指出，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、本地生活、即时通信等类型 APP 进行检查，并书面要求违规 APP 开发运营者限期整改。截至目前，尚有 17 款 APP 未按要求完成整改，涉及违规收集个人信息、APP 强制、频繁、过度索取权限两方面问题。上述 APP 开发运营者在 12 月 5 日前完成整改落实工作，整改落实不到位的，浙江省通信管理局将视情采取下架、关停、行政处罚等措施。

（5）安徽

11 月 27 日消息，安徽省通信管理局通报 2024 年第 8 批存在侵害用户权益行为的 APP。通报指出，安徽省通信管理局近日对安徽省 APP 进行拨测检查，检测发现 19 款 APP 存在违法违规收集使用个人信息的问题，2024 年 11 月 1 日对上述违规 APP 企业下达责令改正通知书，要求限期完成整改工

作。截至目前，尚有5款APP未完成问题整改，相关APP企业应在2024年12月3日前落实整改要求。逾期不整改的，安徽省通信管理局将依法依规组织开展相关处置工作。（来源：工信部，上海市、浙江省、山东省等地通信管理局）

（四）其他部门治理实践

1. 国家标准《数据安全技术 个人信息保护合规审计要求》试点启动会在京召开

11月12日，全国网络安全标准化技术委员会秘书处组织召开国家标准《数据安全技术 个人信息保护合规审计要求》试点启动会。本次试点工作旨在验证标准的科学性、合理性、可操作性和适用性，形成个人信息保护合规审计典型案例和应用经验，为标准推广应用积累经验，为个人信息保护合规审计工作提供标准支撑。

本次试点工作在互联网、金融、交通、医疗、电信等重点行业和领域选取36家单位作为标准应用首批试点单位，试点专家、试点单位、技术支撑单位等共70余人参加试点启动会议。会后，网安标委秘书处将按照试点工作方案，指导相关方有序开展试点各项工作。（来源：全国网安标委）

2. 上海市市场监管局发布“2024 网络市场监管促发展保安全专项行动”成果

11 月 1 日，上海市市场监管局发布“2024 网络市场监管促发展保安全专项行动”成果。

专项行动期间，上海市市场监管局督促平台加强经营者资质审核，对上海市交易类网站和平台内经营者的亮照亮证情况开展监测，发现涉嫌违法线索 338 条，调查后责令改正 166 条；严格规范网络营销和集中促销行为，组织开展无底线营销、互联网违法广告等网络和广告监测，查办互联网广告、不正当竞争等案件近 1600 件；严查网售危害生命健康的重点商品，加大对药品、医疗器械、特殊食品以及网络餐饮服务企业线上线下同步监管力度，查处相关网络案件 500 余件；严厉打击网售侵权假冒伪劣商品行为，开展一老一小用品、电动自行车和配件、燃气用具产品网络监督抽查 189 批次，发现不合格 27 批次，不合格产品均依法实施后续处理；依法清理处置网络禁限售商品，组织开展特供酒、假冒检验检测报告等禁限售商品专项监测，发现并处置涉嫌违法线索 286 条。（来源：国家市场监督管理总局）

3. 湖北孝感市市场监管局发布“2024 网络市场监管促发展保安全专项行动”成果

11 月 12 日，湖北省孝感市市场监管局发布“2024 网络市场监管促发展保安全专项行动”成果。自专项行动以来，湖北省孝感市市场监管局发现并处置涉嫌违法线索 103 条，查处涉网案件 88 件，清理网上违法违规信

息301条，处置网站平台违法违规账号10个，督促互联网企业关停违法违规账号7个。

针对社会关注度高、涉及面广、群众反映强烈的问题，湖北省孝感市市场监管局围绕督促指导平台强化经营者资质审核、持续规范网络营销和集中促销行为、严厉查处网售危害生命健康的重点商品、从严打击网售侵权假冒伪劣商品行为和依法清理处置网络禁限售商品5个方面，开展在线检查和第三方定向监测，严厉查处相关违法违规问题。截至目前，湖北省孝感市市场监管部门通过第三方机构共监测各类网店、网站、App、微信公众号3.9万余家次，监测商品信息链接204.96万余条。

专项行动强化线上线下一体化智慧监管和跨部门、跨层级、跨区域协同监管，形成监管合力。湖北省孝感市市场监管局先后联合其他部门对网络文化经营单位、网络经营旅行社等相关经营单位开展“双随机、一公开”监管，开展各类网络线索与隐患排查。参与江汉流域鄂豫陕甘15城市网络市场监管与服务跨区域协作联盟，与东西湖区市场监管局签订区域合作协议，与美团、饿了么等知名平台签订政企合作协议，推动监管端口前移。（来源：国家市场监督管理总局）

4. 北京互联网法院首例“搜索提示词”算法侵权案宣判

11月11日，北京互联网法院一审开庭宣判首例因“搜索提示词”引发的网络侵权纠纷案。

本案中，被告一夏某某在被告二北京某信息服务公司运营的网络平台发布十余篇涉案文章、视频，含有被诉侵犯名誉权的内容。在该平台搜索

框中输入原告名称，也会出现“骗局”“被骗”等搜索提示词。原告深圳某科技公司认为，被告一夏某某发布的涉案文章、视频侵犯了其名誉权；被告二北京某信息服务公司明知被告一的侵权行为，但在被告一涉案侵权内容中有选择性地添加设置搜索提示词条，具有主观过错，应当承担侵权责任，请求法院判令二被告共同向其赔礼道歉，并赔偿经济损失及合理维权支出。

法院经审理认为，原告名誉与品牌商誉紧密相关，有权主张名誉权侵权；被告一言论用词不当，超出了一般批评的范围，侵犯原告的名誉权；原告没有作出有效通知，被告二作为网络服务提供者不与被告一承担连带责任。

其中，被告二提供的搜索提示技术服务不侵犯原告名誉权。搜索排序、搜索提示、搜索联想一般由平台基于用户的搜索记录等个人信息及衍生的统计数据，利用某种特定算法处理而生成，是典型的算法推荐与搜索功能相结合的应用场景。平台生成的搜索排序、搜索提示、搜索联想是否侵权，应当综合考虑是否有人工参与生成或审核、侵权内容是否明显或易于判定、平台的审核技术能力、平台是否因此盈利等因素，认定平台是否知道或者应当知道侵权内容，并结合平台是否采取删除、屏蔽、断开链接等必要措施最终判定。

本案中，涉案搜索提示系被告二利用算法根据不特定用户搜索、浏览的历史记录自动生成并更新变化。被告二并不会人为加入新内容或是专门聚合负面内容，亦无人工事前审核。鉴于庞大的用户量、搜索量，要求被告二对此进行事前的验证审核，超出当前技术发展的水平，属于不当扩张

被告二作为网络服务提供者的注意义务。搜索提示服务目的在于优化用户搜索体验及内容获取体验，并不直接以营利为目的。此外，被告二收到相关诉讼材料后在合理期限内已采取必要措施，已经尽到网络服务提供者的事后义务，并无过错或扩大损害的侵权情形。综上所述，被告二的搜索提示技术服务行为不具有主观过错，不构成对原告名誉权的侵犯。

北京互联网法院判决被告一夏某某向原告深圳某科技公司赔礼道歉，赔偿经济损失及合理支出共计 40400 元。驳回原告的其他诉讼请求。（来源：北京互联网法院）

5. 北京互联网法院发布一起网络侵权责任纠纷典型案例

11 月 29 日，北京互联网法院发布一起网络侵权责令纠纷典型案例。本案中，李某某诉北京某科技有限公司网络侵权责任纠纷案，就网络服务提供者对严重侵害未成年人权益的违法信息审查义务的认定问题作出判决。

李某某为未成年人，与同学黄某某在学校学习期间因琐事产生矛盾。黄某某委托另外一名同学刘某某通过被告某科技公司运营的某社交软件制作了一段视频，该视频包含李某某的肖像、姓名、微信号等个人信息，并包含造黄谣、招嫖广告等内容，该视频在社交软件中发布后迅速传播，一天内浏览量即超过三万次。李某某发现黄某某在朋友圈发布该视频后报警，案涉视频也在他人投诉后下架。因黄某某和刘某某均为未成年人，经李某某及其监护人同意，公安机关未作出行政或刑事案件处理。北京互联网法院判决被告某科技公司赔偿原告李某某精神损害抚慰金 8000 元和律师费 2000 元。

北京互联网法院认为，网络服务提供者对涉及未成年人个人隐私、涉性谣言等严重侵害未成年人权益的违法信息审查，应当尽到更高的注意义务。对于短时间内浏览量飙升的前述侵权信息，网络服务提供者未采取必要措施及时处理的，应当按照民法典第一千一百九十七条与网络用户承担连带责任。（来源：北京互联网法院）

境外前沿观察：月度速览十则

导读：11 月，澳大利亚议会批准《网络安全法案 2024》，要求组织必须在 72 小时内报告向黑客支付的勒索软件攻击款项，评估对国家安全的潜在威胁等。美国国土安全部人工智能安全与保障委员会发布《关键基础设施中人工智能的角色和责任框架》，以现有风险框架为基础，使各实体能够评估在某些系统或应用中使用人工智能是否会对关键基础设施资产、部门、国家重要系统或由此类系统提供服务的个人造成危害。

加拿大政府下令关闭 TikTok Technology Canada 在加拿大开展的业务，但并未阻止加拿大民众访问 TikTok 应用程序或在该平台创作内容。因非法收集个人信息，韩国个人信息保护委员会决定对 Meta 处以 216 亿多韩元行政罚款。

此外，五眼联盟国家网络安全机构发布公告《2023 年最常被利用的漏洞》，称零日漏洞已经成为黑客最常利用的漏洞类型。德国联邦信息安全局发布《2024 年网络安全态势》报告，指出勒索软件、APT 攻击以及混合威胁等风险正在持续增加。澳大利亚信号局发布《2023-2024 年度网络威胁报告》，指出企业和个人面临的三大网络犯罪威胁分别是电子邮件入侵、网上银行欺诈和商业电子邮件欺诈，分别占网络事件的 20%、13%和 13%等。

关键词：勒索攻击、关键基础设施、非法收集个人信息、零日漏洞

1. 澳大利亚议会批准《网络安全法案 2024》，要求支付勒索赎金后必须按时报告

11 月 25 日，澳大利亚议会批准《网络安全法案 2024》，要求组织必须在 72 小时内报告向黑客支付的勒索赎金，旨在提高澳大利亚网络弹性，帮助澳大利亚信号局（ASD）监控勒索软件趋势，评估对国家安全的潜在威胁，并帮助执法部门追踪网络犯罪。

法案扩大《2018 年关键基础设施安全法》适用范围，以涵盖与关键基础设施相关的系统。随着公用事业、医疗保健和金融等行业对数字系统的依赖程度越来越高，这些系统已成为网络攻击的主要目标。法案将使监管机构能够更好地保护与关键基础设施资产相关的数据系统。法案还将建立网络事件审查委员会，负责审查影响国家安全或公共安全的重大网络事件，包括勒索软件攻击；委员会将评估各组织如何应对事件，并提出未来应对措施改进建议，但不会追究责任或损害相关组织的合法权益。法案特别指出，虽然不鼓励向网络犯罪分子付款，但在某些特殊情况下支付赎金是合理的。（来源：澳大利亚议会、橙说安全）

2. 美国国土安全部发布《关键基础设施中人工智能的角色和责任框架》

11 月 14 日，美国国土安全部人工智能安全与保障委员会发布《关键基础设施中人工智能的角色和责任框架》。本框架以现有风险框架为基础，使各实体能够评估在某些系统或应用中使用人工智能是否会对关键基础设

施资产、部门、国家重要系统或由此类系统提供服务的个人造成危害。框架主要内容包括：（1）建设基于风险和用例的缓解措施；（2）在开发和部署人工智能驱动的服务时，提出一套自愿性责任；（3）建议民间社会和公共部门承担一系列自愿责任；（4）依靠现有的风险框架进行风险评估。

框架的预期成果主要包括：（1）加强基础安全实践的协调统一；（2）改进关键服务的规划和交付；（3）提升整个人工智能生态系统的信任度和透明度；（4）推进关键基础设施的人工智能安全成果研究；（5）尊重公民权利等。（来源：美国国土安全部、天极智库）

3. 因非法收集个人信息，Meta 被罚款 216 亿韩元

11 月 4 日，韩国个人信息保护委员会在第 18 次全体会议上决定，因违反韩国《个人信息保护法》，对美国互联网公司 Meta 处以 216 亿多韩元（约合人民币 1.12 亿多元）的行政罚款。

调查显示，2018 年 7 月至 2022 年 3 月，Meta 通过旗下社交平台 Facebook 个人简介非法收集了约 98 万名韩国用户的宗教观、政治观、是否与同性结婚等敏感信息。根据韩国《个人信息保护法》，涉及个人思想及信念、政治见解、性生活等的信息被列为须得到严格保护的敏感信息，原则上禁止加以处理。外媒报道称，Meta 向广告客户提供了擅自收集的个人敏感信息，约 4000 家广告商利用了这些敏感信息。Meta 在未获得用户同意的情况下收集并利用用户敏感信息，且未采取保护个人信息的措施。此外，Meta 还以非《个人信息保护法》所规定的调阅对象为由拒绝用户调阅个人信息的要

求。对于处于已停用或未激活状态的网站，Meta 也未采取删除或关闭等安全措施，导致 10 名韩国用户的个人信息遭到外泄。

据报道，虽然 Meta 曾在 2021 年 8 月中断了在“个人简介”功能中收集敏感信息的行为，并于 2022 年 3 月主动废除了与敏感信息有关的广告，但韩国个人信息保护委员会还是确认了其违法事实并处以罚款。这也是 Meta 继 2020 年起第五次因涉嫌违反《个人信息保护法》被韩国罚款，累计缴纳的罚款额约达 730 亿韩元。（来源：环球时报热点、央广网）

4. 加拿大政府禁止 TikTok 运营，称出于国家安全考虑

11 月 6 日，加拿大创新、科学和工业部部长发表声明称，经过多步骤的国家安全审查程序，加拿大政府已下令关闭 TikTok Technology Canada, Inc. 在加拿大开展的业务。声明称，这一决定是根据《加拿大投资法》作出的，该法允许对“可能损害加拿大国家安全”的外国投资进行审查。声明称，加拿大政府并未阻止加拿大民众访问 TikTok 应用程序或在该平台创作内容，使用社交媒体应用程序或平台是个人的选择。

对此，TikTok 加拿大发言人回应称，“关闭 TikTok 加拿大办公室将毁掉数百个当地高薪工作岗位，不符合任何人的最佳利益，公司将在法庭上挑战这一命令。TikTok 平台仍将帮助创作者寻找观众、探索新商机，并帮助企业茁壮成长。”（来源：CBS 新闻官网、界面新闻）

5. 因勒索攻击，美国知名军工芯片厂商损失超 1.5 亿元

11 月 7 日消息，美国知名军工半导体厂商微芯科技近日发布最新财报披露，因近期发生网络安全事件，该公司已产生 2140 万美元（约合 1.53 亿元人民币）的相关费用。此次安全事件于 8 月首次曝光，当时该公司发现，其网络系统中出现了可疑活动，并导致公司部分制造设施的生产中断。大约一周后，勒索软件团伙 Play 宣称对此次攻击负责，并表示已窃取了数几 GB 的数据。9 月初，在恢复大部分运营后，该公司确认，威胁行为者确实从其系统中窃取了一些信息，其中包括员工的联系方式和密码哈希值。（来源：安全内参）

6. 德国发布《2024 年网络安全态势》报告：勒索软件、APT 攻击以及混合威胁等风险持续增加

11 月 12 日，德国联邦信息安全局发布《2024 年网络安全态势》报告，强调网络安全对社会稳定的重要性，指出勒索软件、APT 攻击以及混合威胁等风险正在持续增加。据统计，2023 至 2024 年，德国平均每日发现 309000 个新恶意软件变种，较前一年增长 26%，其中针对 64 位 Windows 系统和 Android 设备的攻击显著上升。尽管支付赎金的比例有所下降，但勒索软件的威胁依旧严峻。

报告注意到 APT 组织的威胁持续激增，其中许多组织都有国家支持。在地缘政治紧张的背景下，这些组织越来越多地将政党、政府机构和企业

作为网络间谍活动的目标。报告敦促公共和私营部门采取主动的威胁情报和保护措施，以防御持续复杂攻击。

报告给出的网络安全建议包括：（1）采取治理和基于风险的政策；（2）增强监控和检测；（3）加强事件响应和恢复；（4）增强公众意识和恢复措施；（5）加强与国际安全标准的协调一致。（来源：德国联邦信息安全局、安全内参）

7. 五眼联盟国家的网络安全机构联合发布公告：零日漏洞已经成为黑客最常利用的漏洞类型

11 月 12 日，美国、英国、加拿大、澳大利亚和新西兰的网络安全机构联合发布公告《2023 年最常被利用的漏洞》，公布 2023 年最常被利用的漏洞清单。报告称零日漏洞已经成为黑客最常利用的漏洞类型。

与 2021 年、2022 年发布的同类公告相比，此次公告有明显不同。此前，这些机构警告称，恶意网络攻击者更常利用旧软件的已知漏洞，而不是新披露的漏洞。在此次发布的公告中，网络安全机构列出了 2023 年最常被黑客利用的前 15 个漏洞，其中影响思杰公司（Citrix）NetScaler 网络产品的 CVE-2023-3519 漏洞位居榜首。

公告指出，自美国网络安全和基础设施安全局及其合作伙伴开始发布年度漏洞清单以来，这是首次在年度清单中确认，大部分漏洞首次利用即被作为零日漏洞。尽管公告仅涵盖 2023 年情况，但根据英国国家网络安全中心的数据，零日漏洞利用的趋势已持续到 2024 年。（来源：安全内参）

8. 澳大利亚信号局发布《2023—2024 年度网络威胁报告》

11 月 20 日，澳大利亚信号局发布《2023—2024 年度网络威胁报告》，揭示澳大利亚当前面临的网络安全挑战。报告指出，澳大利亚信号局在过去一年应对超过 1100 起网络安全事件，网络犯罪威胁不断增加。报告指出，企业和个人面临的三大网络犯罪威胁包括电子邮件入侵、网上银行欺诈和商业电子邮件欺诈（BEC），分别占网络事件的 20%、13%和 13%。个人最关注的是身份欺诈，影响 26%的澳大利亚公民，其次是网上购物欺诈和网上银行欺诈。报告通过案例研究展示了网络安全事件的多样性，包括医院网络事件和能源供应商 DDoS 攻击。（来源：澳大利亚信号局）

9. 澳大利亚公司董事协会等机构发布第 2 版《网络安全治理原则》

11 月 25 日，澳大利亚公司董事协会和网络安全合作研究中心发布第 2 版《网络安全治理原则》，以应对 2022 年首次发布原则以来的新兴网络威胁和监管需求。第 2 版原则涵盖了数字供应链风险、数据治理以及网络事件响应和恢复应对等内容，主要包括：（1）明确角色和职责；（2）制定、执行并持续完善网络战略；（3）将网络安全嵌入现有风险管理实践；（4）培养网络弹性文化；（5）为重大网络安全事件制定预案。（来源：澳大利亚公司董事协会）

10. 俄黑客组织通过“近邻攻击”远程入侵美国企业 WiFi 网络

11 月 25 日消息，网络安全公司 Volexity 近日曝光一起网络攻击事件，俄罗斯黑客组织 APT28 成功突破物理攻击范围，入侵万里之外的一家美国企业的 Wi-Fi 网络。

APT28 是隶属于俄罗斯军事情报总局（GRU）第 26165 部队的黑客组织，早在 2004 年便开始活跃，主要攻击目标是西方政府、军事部门。据报道，2022 年 2 月，美国华盛顿一家企业的 WiFi 网络被发现遭遇攻击，这次攻击被归因于 APT28（亦称 Fancy Bear/Forest Blizzard/Sofacy），该组织通过一种名为“近邻攻击”的新技术，远程入侵了该美国企业的 WiFi 网络。（来源：安全内参）

行业前沿观察一：工业和信息化部等十二部门印发《5G 规模化应用“扬帆”行动升级方案》；2024“安满周”即将全国开幕！系列重磅调查报告发布！“第三届广东信创大赛”总决赛暨第三届信创生态融合发展与数字安全创新大会在广州成功召开

导读：为深入贯彻习近平总书记关于加快 5G 发展的重要指示精神，落实党中央、国务院决策部署，大力推动 5G 应用规模化发展，工业和信息化部等十二部门印发《5G 规模化应用“扬帆”行动升级方案》。

近日，网民网络安全感满意度调查活动组委会、北京网络空间安全协会联合发出《关于举办 2024 网民网络安全感满意度调查报告发布周的通知》，正式公布将于 2024 年 12 月 21 日-27 日在全国线上线下同步举办 2024 网民网络安全感满意度调查报告发布周（安满周）系列活动。

在广东省教育厅、广东省人民政府国有资产监督管理委员会、广东省政务服务和数据管理局 、广东省科学技术协会指导下，经省人社厅批准，由广东省网络空间安全协会、广州网络空间安全协会、广东省科协信创联合体、广东新兴国家网络安全和信息化发展研究院主办的“第三届广东信创大赛”总决赛暨第三届信创生态融合发展与数字安全创新大会在广州举行。

关键词：网安周、信息化、数字乡村、网络安全、大湾区、新能源

1. 工业和信息化部等十二部门印发《5G 规模化应用“扬帆”行动升级方案》

近日，工业和信息化部等十二部门关于印发《5G 规模化应用“扬帆”行动升级方案》，内容如下：

5G 规模化应用“扬帆”行动升级方案

为深入贯彻习近平总书记关于加快 5G 发展的重要指示精神，落实党中央、国务院决策部署，大力推动 5G 应用规模化发展，加快培育新质生产力，带动新一代信息技术全方位全链条普及应用，壮大经济社会高质量发展新动能，制定本行动方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的二十大和二十届二中、三中全会精神，统筹高质量发展和高水平安全，发挥 5G 牵引作用，着力推动数字技术融合创新，实现更广范围、更深层次、更高水平的多方位赋能，持续增强 5G 规模应用的产业全链条支撑力、网络全场景服务力和生态多层次协同力，支撑新型工业化和信息通信业现代化，为建设网络强国、推进中国式现代化构筑坚实物质技术基础。

到 2027 年底，构建形成“能力普适、应用普及、赋能普惠”的发展格局，全面实现 5G 规模化应用。

——5G 规模赋能成效凸显。5G 个人用户普及率超 85%，5G 网络接入流量占比超 75%，5G 新消费新体验不断丰富。面向工厂、医院、景区等重点行业领域打造一批 5G 应用领航者，带动行业数字化转型升级。5G 物联网终端连接数超 1 亿，大中型工业企业 5G 应用渗透率达 45%。

——5G 产业供给不断丰富。5G-A 国际标准参与度持续深化，5G 国内行业标准体系加快完善，5G 融合应用标准超 150 项。5G 融合应用产业体系不断健全，5G 与数字技术融合持续深入，芯片模组、行业终端、虚拟专网、共性能力平台等关键环节供给能力升级，打造形成超 1000 款创新行业终端模组产品。

——5G 网络能力显著增强。5G 覆盖广度深度不断拓展，每万人拥有 5G 基站数达 38 个，5G 网络驻留比超 85%，全面支持 IPv6 技术。按需推进 5G 网络向 5G-A 升级演进，全国地级及以上城市实现 5G-A 超宽带特性规模覆盖。建成 7 万个 5G 行业虚拟专网，带动 5000 个边缘计算节点建设，构筑“通感算智”深度融合的新型数字底座。

——5G 应用生态加速繁荣。推动建设一批 5G 应用规模发展城市，培育 200 家 5G 应用解决方案供应商，打造 50 个特色鲜明的 5G 应用创新载体。面向重点领域锻造 5 项以上 5G 应用安全标杆，构建与 5G 发展相适应的安全保障体系。大中小企业融通发展、梯度成长的良好态势逐步形成，全球开放合作生态日益完善。

二、应用升级，推动多方位深度赋能

（一）5G 带动新型消费扩大升级

1.培育新终端。推动基于5G的智能机器人、智能移动终端、云设备等研发应用，鼓励融合5G的XR业务系统、裸眼3D、智能穿戴、智能家居等产品创新发展。推动“5G上车”，鼓励汽车前装5G通信模块，助力智能网联汽车智驾、智舱提质升级。

2.丰富新体验。加速5G新通话、裸眼3D、云手机、5G消息等应用创新，实现5G新通话用户规模突破1亿。推动5G与AI深度融合，提升互动视频等新型交互体验。鼓励基础电信企业面向公众不同需求提供差异化服务，终端企业加快推进手机支持超高清视频显示及拍摄，促进5G超高清视频及直播在娱乐、赛事、电商等领域规模发展。

3.营造新环境。支持互联网企业、基础电信企业和终端企业联合建设5G新型应用创新工场和体验中心，开展AI大模型、面向公众应用的网络切片等新技术试点，促进网络、内容、终端协同创新，为5G新业务新产品研发提供试验环境。强化低成本、适老化5G智能手机供给能力，提升5G普惠服务能力。

（二）5G赋能生产经营提质升级

1.5G+工业互联网。打造“5G+工业互联网”升级版，推进“5G+工业互联网”高质量发展和规模化应用。面向大中小企业深化重点行业领域5G工厂建设，推广一体化、集约化解决方案，打造5G工厂建设标杆。加速5G+工业互联网重点产品研发推广，加快新型工业网络建设。推进5G专用网络建设，探索5G毫米波在制造、采矿、铁路、国防工业等领域创新应用。

2.5G+智慧电力。加速5G智能巡检、分布式能源管理等场景规模推广。面向新能源发电并网、高质量配电网、新型调节性电源等需求，推动5G应用场景创新，培育一批5G电厂，加快电力5G轻量化终端规模上量。

3.5G+智能矿山。加快5G远程掘进、远程综采、无人矿卡等场景规模推广，推动5G与矿山行业系统融合，构建一体化数智矿山方案，建设一批5G矿山。加速5G本质安全网络设备研制，推动5G赋能矿山采掘等成套装备改造和升级。

4.5G+智能油气。推动智能无人巡检、环境信息采集等5G应用推广，促进5G在智能勘探与新能源融合、生产数据采集共享、绿色低碳管理等环节创新应用，打造一批5G油气园区，推进5G与油气装备联合研发部署。

5.5G+智慧交通。推进5G智能交通信号控制等应用场景规模部署，深化基于5G的编队行驶、远程驾驶等高级别自动驾驶应用场景。加快5G技术与AGV、RGV等物流终端融合，探索低空航空器交通运输等5G创新应用服务场景。推动5G在港机远程控制、自动导引运输、集卡自动驾驶等场景中形成标准化解决方案，加速5G海港解决方案向河港、内陆场站、空港等场景复制推广。

6.5G+智慧农业。加速5G在种植、养殖等场景创新应用。推进5G与智能农机深度融合，提升基于5G的农业传感器、控制器、机器人、无人机等智能化装备研发生产水平。

7.5G+智慧海洋。加速5G在海洋渔业、智能船舶、海上交通、海上执法、海上能源、海洋生态环境、海上救助打捞等领域创新应用。推动适用

于海洋环境的5G网络设备及终端研发，深化5G与无人艇、海洋监测浮标、钻井平台等海洋设备融合应用。

（三）5G助力公共服务普惠升级

1.5G+政务服务。面向法律服务、社会保障、社区服务、外网移动办公等需求，加快5G巡回法庭、线上审批、独居老人看护、远程视频会议等应用推广，探索开发5G政务智能终端。

2.5G+数字教育。加强5G与室外实践教学科研、虚拟仿真实验实训、校园体育体测等重点场景深度融合应用，加速5G在在线教学、教育综合评价、校园管理等环节应用。加快5G网络与校园网络协同部署，实现内外网业务跨域融合，支持5G教育终端设备创新研发，推进5G校园建设。

3.5G+社会治理。加快安全生产、应急救援管理、智能指挥调度、灾害事故监测预警等场景5G规模应用，加大5G监测预警终端、智能防护装备、无人化救援装备等安全应急装备的研发创新和推广应用。推动5G摄像头、5G智慧表计等规模部署，探索基于5G的建筑、桥梁、道路等微形变监测应用。推进5G在水利监测感知、智能预报调度、水利工程管控等智慧水利场景应用。

4.5G+智慧文旅。加快旅游治理和服务、文物保护、公共文化服务等领域5G规模化应用。推进5G与人工智能、虚拟现实等融合，探索新型内容生产、传播和体验方式，加快演艺、娱乐、文化会展、文博等行业数字化转型，打造沉浸式文旅体验新场景。加强5G应用、内容生成和装备升级协同创新，完善XR、虚拟交互、智能文化装备等产业链，提升文化装备智能

化水平和产业化能力。持续开展5G+智慧旅游应用试点，培育一批5G景区。打造5G+数字文博标杆项目。增强大型演唱会、音乐节等演出现场5G通信服务能力。

5.5G+卫生健康。推广急诊救治、远程诊断、公共卫生防控等5G应用场景，培育5G智慧健康养老、医药制造、医疗器械制造、远程手术等应用场景。打造一批5G智慧医院，深化多院区医院、医联体、医共体、公共卫生机构等的5G行业虚拟专网及边缘云部署应用。

6.5G+广电视听。加快超高清、沉浸式等高新视听内容智能生产、云上制播、快捷分发、大小屏联动以及车载音视频、应急广播等场景5G规模应用，支持视频平台加大高清视频和4K/8K超高清视频内容供给。创新5G广播服务，强化媒体资源协同，加快推进智慧广电及新型广电网络建设，打造一批5G+广电视听创新应用。

7.5G+数字体育。推动5G在体育训练、健身指导、运动培训、赛事直播、智慧场馆等重点场景规模应用，培育5G数字运动、5G体育赛事互动等服务新模式，强化5G体育器材研发能力。

三、产业升级，构筑全链条发展支撑

（一）升级5G核心产业基础能力

构建5G-A产业链，持续推进上下行超宽带、通感一体、无源物联、高精度低功耗定位、网络智能等关键技术研发试验，加快推进基站、核心网、终端、芯片和仪器仪表等设备研发及产业化。推进5G NR广播技术验证与

试点示范，推动产业端到端支持5G NR广播功能。加快5G毫米波端到端产业链成熟，打造适配多类场景的终端创新生态。

（二）加强5G融合应用技术研发

深化5G+AI赋能行业智能化变革，加快5G+北斗在定位、授时等领域的技术能力提升及应用推广，推进5G与边缘计算、云计算、大数据等技术深度融合。强化5G与行业技术融合研发，推动供需双方加强跨领域技术联合创新，健全5G融合应用技术研发体系。

（三）健全5G融合应用产业体系

加速5G与行业融合产品落地，着力提升芯片/模组、融合终端/装备、行业虚拟专网、解决方案等关键环节低成本高质量供给能力，指导开展“5G Inside”（5G内置）等产业供需对接活动，研发推广基于5G技术的“小快轻准”数字化技术产品，持续丰富5G行业应用解决方案，打造5G应用关键共性能力平台，推进5G与行业内网、设备等融合改造及更新。

（四）完善5G融合应用标准体系

加快5G-A国际标准研制，推进网络、基站、终端等标准体系建设。健全重点行业5G融合应用标准体系，加速行业虚拟专网、行业终端模组、融合装备、解决方案等关键标准制定、完善和推广，鼓励行业联盟开展标准宣贯。

（五）筑牢5G应用安全防护屏障

完善通信网络安全防护管理，加快新兴行业5G终端安全、网络设备安全、数据安全、密码安全等关键技术研究，推动研制具备虚拟化、智能化、

自适应能力的安全产品。发挥5G应用安全创新推广中心集智攻关优势，打造5G应用安全产业核心竞争力。面向重点行业开展5G应用安全标杆锻造，提炼30项以上原子化5G应用安全能力。

四、网络升级，提升全场景服务能力

（一）夯实全域优质5G网络覆盖

纵深推进“宽带边疆”建设，加速5G网络向乡镇、行政村、近海、边疆等区域延伸，积极利用卫星通信技术增强网络覆盖能力。深入实施“信号升格”专项行动，深化政务中心、文旅场所、卫生健康机构等重点场景覆盖，为公众提供更高品质网络服务。加速推动5G RedCap县级以上城市连续覆盖。加快5G-A商用网络部署，推进5G网络向5G-A升级演进。

（二）加强5G行业虚拟专网供给

大力推进5G行业虚拟专网在工业、能源、医疗、教育等领域规模部署，带动云平台、边缘计算节点、智算基础设施等建设，充分发挥公网切片、网元下沉等技术能力，增强定制化服务水平，满足行业低成本、高安全应用需求。探索5G行业虚拟专网在海洋、低空等新兴场景部署。扩大5G RedCap、5G LAN、定位增强、无源物联、通感一体等技术应用，推动5G行业虚拟专网与NB-IoT、4G、IPv6等协同应用。探索建立基础电信企业和行业企业网络共管共维新模式，持续增强网络运维、监测和服务能力，强化网络与终端协同管理，提升网络能力开放水平。

五、生态升级，强化多层次协同创新

（一）打造5G规模应用地方样板

持续开展5G应用“扬帆之城”总结评估，建设5G应用规模发展城市，鼓励地方对推动5G规模化应用成绩突出的企事业单位等给予政策倾斜，加大对5G应用发展支持力度。依托中小企业特色产业集群打造一批具备地方、行业特色的5G产业园区，加速形成集约高效、方案成熟的中小企业5G应用创新发展模式。

（二）培育5G应用创新企业梯队

支持龙头企业带动创新型中小企业成长，培养一批面向行业5G应用的芯片、模组和终端等专精特新企业。指导开展5G应用解决方案供应商征集活动，培育集成类和行业特色5G应用解决方案供应商。鼓励供需双方加强协同，联合攻关5G应用关键环节，完善龙头引领、梯队协同的融通创新模式。

（三）构建5G应用推广平台矩阵

发挥5G应用产业方阵等平台作用，培育一批协同创新和应用推广载体，支持供需双方共建5G融合应用测试床。搭建5G应用“出海”交流合作平台，推动关键产品和服务向全球推广。依托“绽放杯”5G应用征集大赛，加速典型方案和成熟模式规模复制。

六、保障措施

（一）强化统筹联动。工业和信息化部联合相关部门完善协同机制，协调推动网络统筹规划、技术标准研制、产业生态培育、应用场景开放等重点工作。健全部省联动机制，鼓励各地积极出台5G规模化应用相关政策。

（二）优化频谱供给。科学统筹现有频谱资源，依法合规、稳妥有序地通过重耕、共享等方式，持续提升5G频率供给。开展5G工业专用频率需求以及其他无线电系统兼容性研究，适时启动5G专用频率规划。

（三）完善要素保障。深化产融合作，鼓励地方政府、大型企事业单位、各类投资基金等加大对5G创新产品和设备应用的支持力度。发挥重点高校、科研机构优势，加强复合型人才培训，构建多层次人才队伍。

（四）加强动态监测。加强对5G规模化应用统计监测指标研究，及时将成熟指标纳入信息通信业统计调查制度，开展常态化统计监测。进一步完善5G发展监测平台，持续跟踪5G-A等新技术应用进展，定期发布5G新终端、新体验等发展情况。发挥5G应用产业方阵等组织作用，及时总结应用典型案例经验成效，加大宣传推广力度。

2.2024“安满周”即将全国开幕！12月21-27日，系列重磅调查报告发布！

近日，网民网络安全感满意度调查活动组委会、北京网络空间安全协会联合发出《关于举办2024网民网络安全感满意度调查报告发布周的通知》，正式公布将于2024年12月21日-27日在全国线上线下同步举办2024网民网络安全感满意度调查报告发布周（安满周）系列活动。

2024年调查活动共收获全国34个省（直辖市、自治区、特别行政区）323.9470万份网民意见，形成全国总报告、专题报告、区域报告、分析报告等170多份调查报告和各类数据成果。

《通知》公布，本届安满周以“网络安全为人民、网络安全靠人民”为主题，联合公安部第三研究所法律研究中心、教育部教育管理信息中心、12321 网络不良与垃圾信息投诉受理中心、中国互联网协会、密码科技国家工程研究中心、复旦大学、上海交通大学、浙江大学、西安电子科技大学、海南大学、广州大学、郑州大学、北京联合大学、粤港澳网络空间治理创新研究院等专业权威机构及部分网安联成员单位，集中一周时间，密集发布 2024 年调查活动各类成果报告。

《通知》提到，2024“安满周”主会场设在北京香山，相关活动定于 12 月 21 日-24 日举行，由北京网络空间安全协会联合北京网络行业协会、中国计算机学会计算机安全专业委员会、中国互联网协会网民权益保护工作委员会主办。

北京香山主会场系列活动内容包括：发布《2024 年全国网民网络安全感满意度调查统计总报告》和部分行业报告、专题报告、区域报告，重磅发布 2024 年全国网民安全感满意度指数。同期举办“第四届网络志愿服务大会”、启动“网络空间安全志愿守护者行动”公益活动、召开“网安联理事扩大会议”、开展党建联学暨主题党日和考察交流等活动。期间组委会还将联合中国互联网协会发布《12321 年度投诉受理工作报告》和《12321 举报助手 APP 鸿蒙版》。

3. “第三届广东信创大赛”总决赛暨第三届信创生态融合发展与数字安全创新大会在广州成功召开！

11 月 29 日，在广东省教育厅、广东省人民政府国有资产监督管理委员会、广东省政务服务和数据管理局 、广东省科学技术协会指导，中国创新创业成果交易会办公室、中国教育技术协会网络安全专业委员会联合指导下，经省人社厅批准，由广东省网络空间安全协会、广州网络空间安全协会、广东省科协信创联合体、广东新兴国家网络安全和信息化发展研究院主办，北京网络空间安全协会联合主办的“第三届广东信创大赛”总决赛开幕式暨第三届信创生态融合发展与数字安全创新大会在广州广东亚洲国际大酒店举行。

中国工程院院士沈昌祥，欧洲科学院外籍院士、华南理工大学计算机科学与工程学院院长陈俊龙，广东省政务服务和数据管理局党组成员魏文涛，广东省教育厅二级巡视员陈健生，广东省市场监督管理局标准化处处长郑文涛，广东省政务服务和数据管理局处长罗奇伟，广东省国资委科技创新处二级调研员张怀有，广东省市场监督管理局标准化处副处长蔡捷章，广东省公安厅科技信息化处三级调研员李伟明，广东省科学技术协会四级调研员邓梅，广东省教育厅事务中心办公室副主任苏卫，广州市公用事业技师学院副院长梁峰，广东省公安厅原常务副厅长张圣钦，广东省人力资源和社会保障局原二级巡视员魏建文，广东省公安厅原副巡视员、网警总队原总队长栾广生，广州市公安局原副巡视员、网监分局原局长高中孝，广州市公安局网监分局原局长蒋兆明，广东省网络空间安全协会会长黄丽

玲，启明星辰华南战略服务副总经理李昕，中电科金仓(北京)科技股份有限公司广东事业部总经理陈晨等领导出席活动。来自教育、金融、能源、交通、水利、公共通信、信息服务等行业的专家代表和部分赛项获奖选手600余人现场参加活动；活动还采用直播形式线上同步举行，约有20万人次线上参加。

“第三届广东信创大赛”共设5个赛项，包括信息系统信创改造方案竞赛、数据安全管理员竞赛、数据库管理员竞赛、信创标准竞赛、信创知识竞赛。其中，信息系统信创改造方案（效果）竞赛、信息系统信创改造方案竞赛、信创知识竞赛已成功完成各项赛事；数据安全管理员赛项、数据库管理员赛项经过激烈角逐，最终有274名优秀选手脱颖而出，于今日（11月29日）进行总决赛。本次大赛吸引了全省21个地市，超3000人报名参与，参赛人员行业分布广泛，涵盖信创“2+8+N”各领域。

活动现场广东省市场监督管理局对广东省网络空间安全协会颁发“省级地方标准实施情况统计分析点（网络安全和信息化）承担单位”牌匾。协会作为广东省网安标委秘书处承担单位，在标准化工作方面做了大量工作，积极主导或参与地方标准、行业标准、国家标准的制修订；培训宣贯和实施推动团体标准的制定、发布、落地、实施；将标准化工作与工程职称评定、博士站等工作紧密挂钩，为我省网络空间安全标准化工作与专业技术人才培养评价和使用有了更成熟的运转模式做出了极大贡献。

总决赛现场同期举办了第三届信创生态融合发展与数字安全创新大会，邀请到多位行业权威专家，围绕数字经济发展、智算模型落地应用、国产数据库发展与建设、信创产业服务等内容进行主题分享。

与前两届信创大赛相比，本届大赛不仅规模持续扩大，品质也大幅度升级，全面考察参赛选手在数据安全与管理、数据库管理方面的综合素质和创新能力。竞赛内容由理论知识和实操技能两部分组成，参赛选手最终名次依据选拔赛和总决赛两部分成绩按比例累加的综合成绩进行排名，其中选拔赛成绩占 20%、总决赛成绩占 80%。

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，召开理事会、召开博览会等活动。北京网络行业协会成功举行“数据要素赋能新质生产力·共建实数融合新生态”活动；上海市信息安全行业协会成功举办上海信息安全管理师（红帽认证）培训班；西藏自治区互联网协会“党建领航 网众e心”活动圆满闭幕；上海市信息网络安全管理协会四届六次理事会召开；甘肃省商用密码行业协会成功举办甘肃省第二届大学生密码知识竞赛；福建省互联网协会成功主办2024福建互联网大会；湖北省网络和数据安全协会召开2025武汉网络与数据安全博览会启动仪式说明会；深圳市网络与信息安全行业协会成功主办第26届中国国际高交会网络安全前沿技术产业发展论坛等。

关键词：大讲堂、信创大赛、技能竞赛、AI、信息安全

1. 北京网络行业协会成功举行“数据要素赋能新质生产力·共建实数融合新生态”活动

为深入探讨数据要素在推动高质量发展中的关键作用，北京网络行业协会、中国技术创业协会孵化分会联合北京普天德胜科技孵化器有限公司于11月22日共同主办的“数据要素赋能新质生产力·共建实数融合新生态”活动顺利举行。

活动邀请了众多行业专家、企业代表和政府领导，聚焦于“数据要素赋能新生产力，共建实数融合新生态”的主题，探讨了网络数据安全保护的重要意义和创新之路。50余家单位近百人参加，现场气氛热烈。

活动期间，多位特邀专家和行业代表进行了主题演讲。并进行了圆桌对话，围绕着数据要素在企业数字化转型中的应用、数据要素在创新生态中的角色和模式、数据资产化的实施路径与模式案例等诸多内容展开深入的探讨。

2. 上海市信息安全行业协会成功举办上海信息安全管理师（红帽认证）培训班

11月27日，上海市信息安全行业协会携手印度国家信息技术学院（NIIT）,在上海浦东软件园三林园成功举办了信息安全管理师（红帽认证）培训班。吸引了来自银行、证券、汽车、卫生健康、互联网、航空航天等行业领域的信息安全管理人员、专业技术和研发人员以及高校学生参加，

共同学习和探索信息安全前沿知识与实践技能。由红帽全球技术培训部资深交付经理贺正刚老师授课。

培训配套了红帽结业证书，旨在通过专业、系统的培训与交流，为广大从业者提供一个学习、分享与合作的平台，共同应对信息安挑战，守护数字世界的安全与稳定。

3. 西藏自治区互联网协会“党建领航 网众 e 心”活动圆满闭幕

为深入学习贯彻党的二十届三中全会和自治区党委十届六次全会精神，在自治区互联网行业党委的指导下，11 月 27 日，西藏自治区互联网协会牵头承办的“党建领航 网众 e 心”主题活动在拉萨中心书城成功举办。

活动包括学习贯彻党的二十届三中全会、区党委十届六次全会精神主题演讲及知识竞答活动，“E 心向党共绘蓝图”才艺教学展示活动。参加活动的有区管重点互联网企业、拉萨市互联网企业、网络社会组织党员及员工共 50 余人。

活动围绕学习贯彻党的二十届三中全会、区党委十届六次全会精神展开。各支部通过内部选拔，推荐出优秀选手进行主题演讲。活动为互联网企业和网络社会组织提供了交流合作平台，促进资源共享与优势互补。

4. 上海市信息网络安全管理协会四届六次理事会召开

近日，上海市信息网络安全管理协会四届六次理事会成功召开。协会副会长以及理事单位代表共计 80 人参会。监事会成员、高研班学员、打谣

联盟成员代表列席会议。上海市公安局网络安全保卫总队陆明副总队长、市公安局普陀分局网安支队周健支队长出席会议并讲话。

会议进行了多项议程。协会会长薛质在会议总结时表示，理事会积极创新，下沉到区，联合属地单位，共同举办健步走及打谣展示活动，内容丰富多样、形式新颖独特，得到了各方大力支持。此模式成效显著，期望能在更多区域推广，有兴趣的理事可与协会对接合作事宜。协会正在紧锣密鼓地筹办第四届新耀东方上安会、第三期数智创新高研班等重要活动，衷心希望继续得到大家一如既往的支持与积极参与。

5. 甘肃省商用密码行业协会成功举办甘肃省第二届大学生密码知识竞赛

近日，由甘肃省国家密码管理局指导，甘肃省商用密码行业协会、西北师范大学主办，甘肃烽侦网络安全研究院提供技术支持的“甘肃省第二届大学生密码知识竞赛”在西北师范大学成功举办，省国家密码管理局相关领导出席颁奖仪式并进行颁奖。

此次竞赛活动为推动甘肃省商用密码应用创新发展提供了重要契机，进一步检验和锻炼了参赛学生在密码政策理论研究、分析和应用等方面的能力。在未来实践中，甘肃省将进一步探索新载体新手段，深化“政校企”协同，推进“产学研”融合，持续锚定自主创新，加强基础理论研究，加快拓展技术应用。

6. 福建省互联网协会成功主办 2024 福建互联网大会

11 月 15 日，在石狮市人民政府的支持下，由福建省互联网协会主办的 2024 福建互联网大会在福建石狮圆满落幕。大会以“新质生产力，注力新发展”为主题，设有 1 场开幕式、2 场分享会，共同围绕人工智能、AI 大模型、低空经济、新质生产力等行业热点，展开深度交流，为福建的经济发展和产业升级注入新的活力。

相关政府部门领导、专家学者、社会组织主要负责人、行业精英、互联网及相关领域从业者、地市互联网协会领导、媒体等超过 800 人次齐聚大会现场，共同探讨互联网行业前沿发展新机遇，凝聚智慧和力量，搭建交流合作平台，推动数智赋能与数实融合，助力加快形成新质生产力，帮助福建省在互联网产业的激烈竞争中抢占先机，为福建省数字经济产业高质量发展注入新力量。

7. 湖北省网络和数据安全协会召开 2025 武汉网络与数据安全博览会启动仪式说明会

11 月 15 日，2025 武汉网络与数据安全博览会启动仪式说明会成功举行。此次说明会旨在向社会各界详细介绍博览会的筹备情况、特色亮点以及未来规划。

会上，博览会组委会负责人、湖北省网络和数据安全协会会长王耀发发表讲话，对出席说明会的嘉宾表示热烈欢迎，并就博览会的背景和意义进行了深入阐述。他表示，本次博览会的举办，将为行业搭建一个交流合

作、展示创新成果的高端平台，促进网络与数据安全技术的进步和应用的普及。此外，协会秘书长刘莉详细介绍了博览会的筹备进展。

说明会的成功举行，标志着 2025 武汉网络与数据安全博览会的筹备工作进入了一个新的阶段。

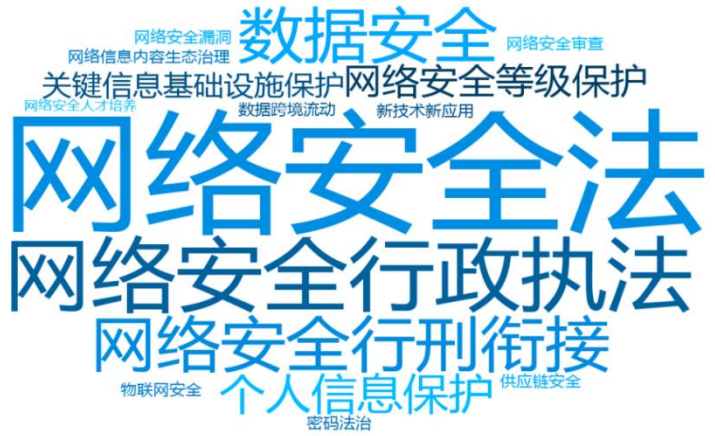
8. 深圳市网络与信息安全行业协会成功主办第 26 届中国国际高交会网络安全前沿技术产业发展论坛

11 月 14 日，由深圳市网络与信息安全行业协会主办的第二十六届中国国际高新技术成果交易会网络安全前沿技术产业发展论坛在深圳国际会展中心召开，协会创始会长王智、副会长林鲁冰、秘书长白健等莅临活动现场。论坛特邀多位行业资深专家、学者大咖、企业掌舵人，围绕“AI”、“大模型”、“韧性网络”、“商密”、“网络安全保险”等当下最前沿技术，共议网络与信息安全热点话题，探讨网络安全行业现状、技术创新及未来发展方向。

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

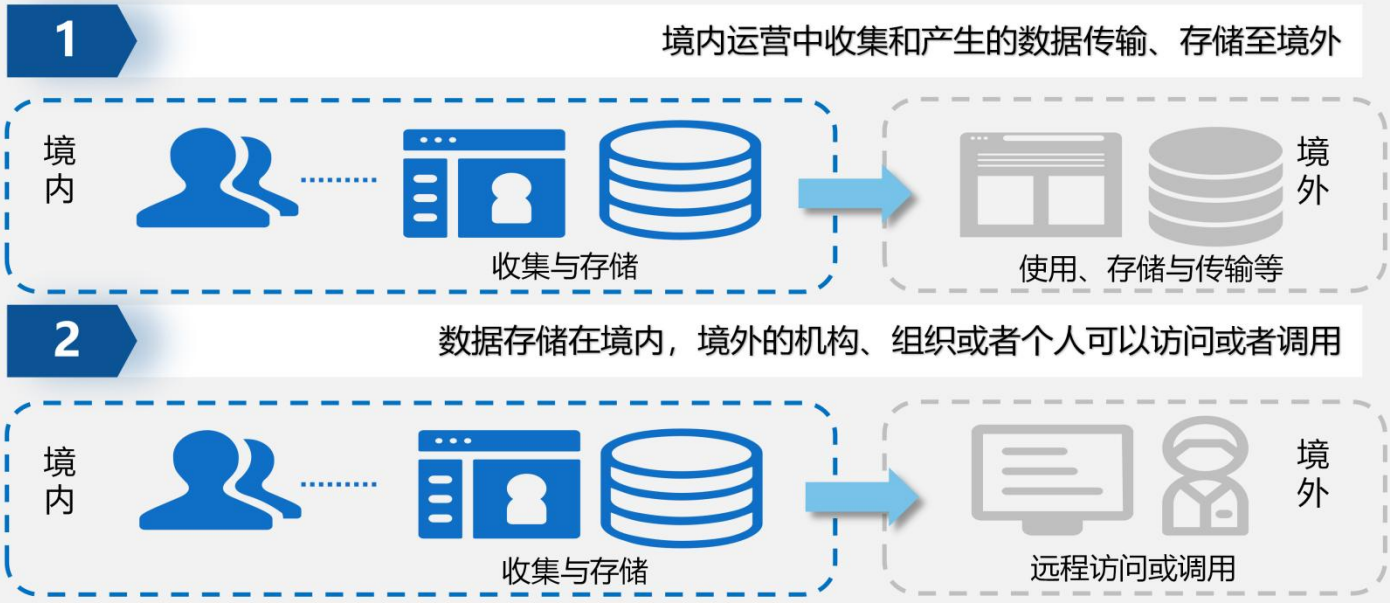
结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

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

……