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11月第11期（总第16期）

2024年11月13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：10 月，我国在与东盟、上合组织、金砖国家的交流合作中，持续推动数字生态建设，深化信息安全领域合作。第 27 次中国-东盟领导人会议发布《关于推动建立可持续和包容性的数字生态合作联合声明》，提出在相互尊重的基础上，基于各方意愿、能力和需求，采取措施促进数字生态系统合作。《上海合作组织成员国政府首脑（总理）理事会第二十三次会议联合公报》强调，应加强相互协调与合作，高效利用数字经济和科技创新，为上合组织国家发展进步、提升地区经济竞争力和发展潜力注入新动力，强调技术应惠及全民。《金砖国家领导人第十六次会晤喀山宣言——加强多边主义，促进公正的全球发展与安全》呼吁采取全面、平衡、客观的方法来实现信息通信技术产品和系统的开发和安全，并制定和实施全球可互操作的供应链安全通用规则和标准。

同时，国家计算机病毒应急处理中心发布《“伏特台风”III —揭密美国政府机构实施的网络间谍和虚假信息行动》报告，进一步公开美国联邦政府、情报机构和“五眼联盟”国家针对中国和德国等其他国家及全球互联网用户联合实施的网络间谍窃听窃密活动。外交部发言人也在例行记者会上回应记者有关提问时表示，有关报告清楚表明了到底谁才是全球网络空间安全的最大威胁。中方奉劝美方停止“贼喊捉贼”等种种不负责任的言行，停止在全球范围内搞网络攻击，停止利用网络安全问题污蔑抹黑中国。此外，中国网络空间安全协会发文指出，英特尔存在安全漏洞问题

频发，可靠性差、漠视用户投诉，假借远程管理之名、行监控用户之实，暗设后门、危害网络和信息安全四类问题，应系统排查英特尔产品网络安全风险，并建议对英特尔启动网络安全审查。

字节跳动大模型训练据传被实习生攻击。因对团队资源分配不满，实习生利用HF漏洞在公司共享模型里写入破坏代码，导致模型训练效果忽高忽低。据悉，字节跳动内部已经调查明确此事为实习生所为。目前，该实习生已被辞退。

关键词：数字生态合作、网络间谍窃听窃密、网络安全审查、大模型攻击

1. 中国-东盟发布《关于推动建立可持续和包容性的数字生态合作联合声明》

10 月 10 日，第 27 次中国-东盟领导人会议在老挝万象举行，会后发布《关于推动建立可持续和包容性的数字生态合作联合声明》。

声明提出在相互尊重的基础上，基于各方意愿、能力和需求，采取七项措施促进数字生态系统合作，分别是加强政策交流和战略对接、推动数字基础设施建设、加快新兴数字技术创新应用、推动产业数字化转型、加强数字安全能力和韧性、提高数字素养和数字能力、推动更加包容普惠的数字化发展。

具体包括加强新兴技术相关信息交流，推动创新应用合作，包括但不限于 5G 技术和应用、云计算、数字政府和未来网络；推动人工智能准则、发展、安全和治理最佳实践的交流沟通；开展数字安全技术相关最佳实践的交流合作，包括但不限于政策、技术、标准、产业和能力建设。（来源：工信部）

2. 上海合作组织成员国政府首脑（总理）理事会第二十三次会议发布《联合公报》

10 月 15 日至 16 日，上海合作组织成员国政府首脑（总理）理事会第二十三次会议在伊斯兰堡举行，会后发布《联合公报》。

公报指出，当今世界经济正发生结构性变化，信息技术、数字化、人工智能、虚拟/数字资产、电子商务等领域快速发展、相互关联。各代表团

团长们对投资萎缩、供应链不稳定、各种保护主义措施和国际贸易壁垒引发的市场动荡等挑战表示担忧。

公报强调，应加强相互协调与合作，高效利用数字经济和科技创新，为上合组织国家发展进步、提升地区经济竞争力和发展潜力注入新动力，强调技术应惠及全民。深化信息安全领域合作十分重要，亟需弥合“数字鸿沟”，支持基于各自国内法律研究建立跨境数据交换机制，在经济和社会领域推广数字技术，发展电子政务、电子支付系统、电子商务及其他数字化业务。（来源：中国政府网）

3. 金砖国家领导人第十六次会晤发布《喀山宣言》

10 月 22 日至 24 日，金砖国家领导人在俄罗斯联邦喀山举行金砖国家领导人第十六次会晤，主题是“加强多边主义，促进公正的全球发展与安全”，会后发布《金砖国家领导人第十六次会晤喀山宣言——加强多边主义，促进公正的全球发展与安全》。

宣言指出，金砖国家认识到信息通信技术在弥合数字鸿沟、促进社会经济增长和人类发展方面具有巨大潜力，同时认识到来自数字领域和数字领域内部的挑战和威胁。金砖国家呼吁采取全面、平衡、客观的方法来实现信息通信技术产品和系统的开发和安全，并制定和实施全球可互操作的供应链安全通用规则和标准。

宣言强调，金砖国家对信息通信技术被更加频繁地恶意使用表示关切。金砖国家强调国际合作在预防和打击信息通信技术犯罪方面的重要性，因

此期待在第 79 届联合国大会通过《联合国打击网络犯罪公约》草案；加强国际合作，打击利用信息通信技术系统实施的某些犯罪，并以电子形式收集、保存和共享严重犯罪的证据。

宣言表示，金砖国家对包括传播虚假叙事和假新闻在内的虚假信息、错误信息和仇恨言论呈指数级蔓延和扩散表示严重关切，特别是在助长激进化和冲突的数字平台上。重申对国家主权的承诺，同时强调信息公正的重要性，并确保基于事实的准确信息能够自由流动并被公众获取，包括意见和言论自由以及数字和媒体素养，以便根据适用的国内法和国际法实现有意义的互联互通。（来源：中国政府网）

4. 国家计算机病毒应急处理中心发布《“伏特台风”III —揭密美国政府机构实施的网络间谍和虚假信息行动》

10 月 14 日，国家计算机病毒应急处理中心发布《“伏特台风”III —揭密美国政府机构实施的网络间谍和虚假信息行动》。

报告进一步公开美国联邦政府、情报机构和“五眼联盟”国家针对中国和德国等其他国家及全球互联网用户联合实施网络间谍窃听窃密活动，并通过误导溯源归因分析的隐身“工具包”实施“假旗行动”掩盖自身恶意网络攻击行为，嫁祸他国的铁证，以及美采取“供应链”攻击，在互联网产品中植入后门，“预先埋伏”的事实，彻底揭穿“伏特台风”这场由美国联邦政府自编自导自演的政治闹剧。

报告指出，长期以来，美国在网络空间积极推行“防御前置”战略并实施“前出狩猎”战术行动，也就是在对手国家周边地区部署网络战部队，对这些国家的网上目标进行抵近侦察和网络渗透。为适应这种战术需要，美国情报机构专门研发用于掩盖自身恶意网络攻击行为、嫁祸他国并误导溯源归因分析的隐身“工具包”，代号“大理石”（Marble）。该工具包是一个工具框架，可以与其他网络武器开发项目集成，辅助网络武器开发者对程序代码中各种可识别特征进行“混淆”，有效“擦除”网络武器开发者的“指纹”，使调查人员无法从技术角度追溯武器的真实来源。该框架还有一个更加“无耻”的功能，就是可以随意插入中文、俄文、朝鲜文、波斯文、阿拉伯文等其他语种的字符串，这显然是为了误导调查人员，并栽赃陷害中国、俄罗斯、朝鲜、伊朗以及众多的阿拉伯国家。

此外，报告指出，据美国国家安全局的资料显示，美国依托其在互联网布局建设中先天掌握的技术优势和地理位置优势，牢牢把持全球最重要的大西洋海底光缆和太平洋海底光缆等互联网“咽喉要道”，先后建立7个国家级的全流量监听站，与美国联邦调查局（FBI）和英国国家网络安全中心（NCSC）紧密合作，对光缆中传输的全量数据深度开展协议解析和数据窃取，实现对全球互联网用户的无差别监听。（来源：国家计算机病毒应急处理中心、新华社）

5. 中国网络空间安全协会：建议对英特尔启动网络安全审查

10 月 16 日，中国网络空间安全协会发文指出，英特尔安全漏洞问题频发、故障率高，应系统排查英特尔产品网络安全风险，并建议对英特尔启动网络安全审查。

文章指出英特尔存在四类问题，分别是安全漏洞问题频发；可靠性差，漠视用户投诉；假借远程管理之名，行监控用户之实；暗设后门，危害网络和信息安全。

安全漏洞问题频发方面，文章指出，2023 年 8 月，英特尔 CPU 被曝存在 Downfall 漏洞，该漏洞是一种 CPU 瞬态执行侧信道漏洞，利用其 AVX2 或者 AVX-512 指令集中的 Gather 指令，获取特定矢量寄存器缓冲区之前存储的密钥、用户信息、关键参数等敏感数据。该漏洞影响英特尔第 6 代至第 11 代酷睿、赛扬、奔腾系列 CPU，以及第 1 代至第 4 代至强处理器。实际上，早在 2022 年，就有研究者向英特尔报告过该漏洞，但英特尔在明知漏洞存在的情况下，既不予承认，也未采取有效行动，还持续销售有漏洞的产品，直至漏洞被公开报道，英特尔才被迫采取漏洞修复措施。

暗设后门，危害网络和信息安全方面，文章表示，英特尔公司开发的自主运行子系统 ME（管理引擎），自 2008 年起被嵌入几乎所有的英特尔 CPU 中，是其大力推广的 AMT（主动管理技术）的一部分，允许系统管理员远程执行任务。只要该功能被激活，无论是否安装了操作系统，都可以远程访问计算机，基于光驱、软驱、USB 等外设重定向技术，能够实现物理级接触用户计算机的效果。硬件安全专家 Damien Zammit 指出 ME 是一个后门，

可以在操作系统用户无感的情况下，完全访问存储器，绕过操作系统防火墙，发送和接收网络数据包，并且用户无法禁用 ME。

17 日，英特尔中国回应称，作为一家在华经营近 40 年的跨国公司，英特尔严格遵守业务所在地适用的法律和法规。 英特尔始终将产品安全和质量放在首位，一直积极与客户和业界密切合作，确保产品的安全和质量。将与相关部门保持沟通，澄清相关疑问，并表明对产品安全和质量的坚定承诺。（来源：中国网络空间安全协会、英特尔中国）

6. 外交部：奉劝美方停止利用网络安全问题污蔑抹黑中国

10 月 28 日，外交部发言人林剑主持例行记者会。有记者提问称，据报道，美国政府正调查据称与中国有关的行为体，该行为体侵入了美国通讯网络，尤其是对美方有关政客手机进行了黑客攻击。

外交部发言人林剑对此表示，不了解具体情况，但注意到有相关报道，特别提出所谓的黑客组织“盐台风”。林剑强调，美方近来似乎热衷于制造各种“台风”。针对此前美方热炒的所谓“伏特台风”事件，中国网络安全机构发布了真相系列报告，以确凿证据证明所谓“伏特台风”实为国际勒索软件组织，美国炮制网络溯源虚假叙事的真实目的是栽赃陷害中国。有关报告清楚表明了到底谁才是全球网络空间安全的最大威胁。中方奉劝美方停止“贼喊捉贼”等种种不负责任的言行，停止在全球范围内搞网络攻击，停止利用网络安全问题污蔑抹黑中国。（来源：外交部）

7. 字节跳动大模型训练被实习生攻击，涉事者已被辞退

10 月 18 日，多个微信群流传一则消息：“某头部大厂的大模型训练被实习生入侵，注入了破坏代码，导致其训练成果不可靠，可能需要重新训练。据称遭到入侵的代码注入 8000 多张卡，带来的损失可能超过千万美元。”

据知情人士表示，该头部大厂为字节跳动。2024 年 6 月，某高校的博士在字节跳动商业化技术团队实习，因对团队资源分配不满，使用攻击代码破坏团队的模型训练任务。该实习生利用了 HF（huggingface）的漏洞，在公司的共享模型里写入破坏代码，导致模型的训练效果忽高忽低，无法产生预期的训练效果，而且 AML 团队无法核查原因。

从知情人士处了解到，字节跳动内部已经调查明确此事为田姓实习生所为。目前，该实习生已被辞退，字节跳动同时把此事同步给阳光诚信联盟和企业反舞弊联盟，以及该实习生所在的学校。但这名实习生被辞退后到处“辟谣”甩锅，称是其他人所为。（来源：观察者网）

境内前沿观察二：政策立法

导读：10 月，数据资源开发利用和安全保障、人工智能健康应用仍是国家和地方政策立法的重点关注，体现重者恒重的治理理念。此外，两用物项出口管制相关立法也取得重要进展。

数字资源开发利用方面。因具有规模体量大、数据质量好、价值潜能大、带动作用强的特点，加快公共数据资源开发利用成为深化数据要素市场化配置改革的先导工程和重要抓手。对此，中共中央办公厅、国务院办公厅印发《关于加快公共数据资源开发利用的意见》。该意见是中央层面首次对公共数据资源开发利用进行系统部署，也是国家数据局成立以来研究起草的首个中央文件。意见出台后，预期将产生大幅扩大公共数据资源供给、进一步激发全社会用数活力、扩大社会有效投资、促进数据产业发展四方面效果。同时，国家发展改革委和国家数据局分别发布《公共数据资源登记管理暂行办法（公开征求意见稿）》和《公共数据资源授权运营实施规范（试行）（公开征求意见稿）》。

地方层面，江苏省政府办公厅印发《江苏省公共数据授权运营管理暂行办法》，提出公共数据授权运营采用“两级主体、分级授权”的模式；同日还印发《关于加快释放数据要素价值培育壮大数据产业的意见》，围绕夯实数据资源供给能力、促进数据资源开发利用等六方面提出 24 项具体措施。《广东省数据条例（草案征求意见稿）》《广州市数据条例（草案

修改稿·征求意见稿）》先后发布，围绕数据资源、数据流通、安全与保障方面进行规定。

人工智能健康应用方面。浙江省发展和改革委员会发布《浙江省“人工智能+”行动计划（2024—2027 年）（征求意见稿）》，围绕人工智能+科学、教育、交通、治理、能源、金融等 12 个重点领域提出具体行动要求。北京市发布《北京市教育领域人工智能应用指南》，是北京市教育研究部门研制的首份教育领域人工智能应用指南，将规范学校教育应用人工智能。

此外，《两用物项出口管制条例》公布，自 2024 年 12 月 1 日起施行。条例坚持总体国家安全观，统筹高质量发展和高水平安全，完善管理和服务，提升两用物项出口管制治理能力。条例给出“两用物项”定义，明确两用物项包括相关的技术资料等数据。

关键词：公共数据资源、数据安全事件、人工智能应用、两用物项出口管制

（一）国家层面动向

1. 中共中央办公厅、国务院办公厅印发《关于加快公共数据资源开发利用的意见》

9 月 21 日，中共中央办公厅、国务院办公厅印发《关于加快公共数据资源开发利用的意见》。意见是中央层面首次对公共数据资源开发利用进行系统部署，也是国家数据局成立以来研究起草的首个中央文件。

意见聚焦破除公共数据流通使用的体制性障碍、机制性梗阻，统筹发展和安全，兼顾效率和公平，从扩大资源供给、规范授权运营、鼓励应用创新、营造良好环境、强化组织保障等方面提出 17 项具体措施。

意见的主要创新点概括为“两个着力、一个规范”。一是着力激发供数动力。公共数据资源开发利用不足，主要矛盾在供给侧。意见明确共享、开放和授权运营三种开发利用方式，对资源供给进行体系化部署；二是着力释放用数活力。经济发展、社会治理等很多数据融合应用场景中，公共数据不可或缺。意见鼓励各方利用公共数据开发更多产品，提供更好服务，繁荣产业生态；三是规范授权运营活动。授权运营创新性强，亟需统一制度规则。意见要求建立公共数据资源登记制度、授权运营情况披露机制，提出监督管理要求，确立授权运营的制度规则框架。

加强安全管理方面，意见要求强化数据安全和个人信息保护，加强对数据资源生产、加工使用、产品经营等开发利用全过程的监督和管理。建立健全分类分级、风险评估、监测预警、应急处置等工作体系，开展公共

数据利用的安全风险评估和应用业务规范性审查。运营机构应依据有关法律法规和政策要求，履行数据安全主体责任，采取必要安全措施，保护公共数据安全。加强技术能力建设，提升数据汇聚关联风险识别和管控水平。依法依规予以保密的公共数据不予开放，严格管控未依法依规公开的原始公共数据直接进入市场。

10 月 10 日，国务院新闻办公室举行新闻发布会。发布会表示，意见出台后，预期产生四方面效果，分别是将大幅扩大公共数据资源供给、将进一步激发全社会用数活力、将扩大社会有效投资、将促进数据产业发展。（来源：中国政府网、国务院新闻办公室）

2. 李强签署国务院令公布《两用物项出口管制条例》

9 月 30 日，国务院总理李强签署国务院令，公布《两用物项出口管制条例》，自 2024 年 12 月 1 日起施行。条例共六章五十条，主要包括管制政策、管制措施、监督检查等内容。

条例给出“两用物项”定义，明确两用物项，是指既有民事用途，又有军事用途或者有助于提升军事潜力，特别是可以用于设计、开发、生产或者使用大规模杀伤性武器及其运载工具的货物、技术和服务，包括相关的技术资料等数据。

条例保持现行两用物项出口管制管理体制稳定，对国家出口管制工作协调机制、国务院商务主管部门、海关和国家其他有关部门，以及省、自治区、直辖市人民政府商务主管部门各自职责作出规定。同时，取消两用物项出口经营者登记制度。增强两用物项出口管制政策的透明度和规范性，

明确拟定出口管制政策的考量因素和程序规定。细化两用物项出口管制许可便利措施及其适用条件、程序等。

条例以出口管制法为基础，细化两用物项出口管制清单制定和调整的程序，要求国务院商务主管部门及时公布清单，并在制定、调整过程中以适当方式征求有关企业、商会、协会等方面意见，必要时开展产业调查和评估。此外，条例还细化实施临时管制的程序性要求，规定实施临时管制的次数和期限，以及对实施临时管制的评估要求。（来源：中国政府网）

（二）部委层面动向

1. 国家发展改革委发布《公共数据资源登记管理暂行办法（公开征求意见稿）》

10 月 12 日，国家发展改革委发布《公共数据资源登记管理暂行办法（公开征求意见稿）》。公开征求意见稿共六章二十七条，包括登记要求、登记程序、登记管理等内容。公开征求意见稿规定，公共数据资源登记申请类型主要包括首次登记、变更登记、更正登记、注销登记。

首次登记要求，登记主体应按规定提交主体信息、数据合法合规性来源、数据资源情况、存证情况、产品和服务信息、应用场景信息、数据安全风险评估等申请材料。登记主体在开展授权运营活动并提供数据资源或交付数据产品和服务后，在 20 个工作日内提交首次登记申请。本办法施行前已开展授权运营的，登记主体应按首次登记程序于本办法施行后的 30 个工作日内进行登记。

变更登记要求，对于涉及数据来源、数据资源情况、产品和服务、存证情况等发生重要更新或重大变化的，或者登记主体因机构重组等原因导致主体信息发生变化的，登记主体应及时向登记机构申请变更登记。

更正登记要求，登记主体、利害关系人认为已登记信息有误的，可以申请更正登记。经登记主体书面同意或有证据证明登记信息确有错误的，登记机构对有关错误信息予以更正。

注销登记要求，登记主体应申请办理注销登记，登记机构自受理之日起10个工作日之内完成注销，包括公共数据资源不可复原或灭失的；登记主体放弃相关权益或权益期限届满的；登记主体因解散、被依法撤销、被宣告破产或因其他原因终止存续的；法律法规规定的其他情形。（来源：国家发展改革委）

2. 国家数据局发布《公共数据资源授权运营实施规范（试行）（公开征求意见稿）》

10月12日，国家数据局发布《公共数据资源授权运营实施规范（试行）（公开征求意见稿）》。公开征求意见稿共七章二十七条，包括基本要求、方案编制、协议签订、运营实施、运营管理等内容。

公开征求意见稿规定，县级以上地方各级人民政府、国家行业主管部门可将依法持有的公共数据资源，在不危害国家安全、公共利益，不侵犯商业秘密和个人隐私、个人信息权益的前提下，纳入授权运营范围。以政务数据共享方式获得的其他地区或部门的公共数据，用于授权运营的，应征得共享数据提供单位同意。

公开征求意见稿强调，实施机构应建立健全管理制度，强化数据治理，提升数据质量，明确数据分类分级安全保护要求，加强技术支撑保障和数据安全管理，严格防控纳入授权运营范围的原始公共数据资源直接进入市场，强化对运营机构涉及公共数据资源授权运营的内控审计。运营机构应履行数据安全主体责任，加强内控管理、技术管理和人员管理，不得超授权范围使用公共数据资源，严防数据加工、处理、运营、服务等环节数据安全风险。实施机构、运营机构应通过管理和技术措施，加强数据关联汇聚风险识别和管控，保障数据安全。（来源：国家数据局）

3. 国家数据局发布《可信数据空间发展行动计划（2024—2028 年）（征求意见稿）》

10 月 18 日，国家数据局发布《可信数据空间发展行动计划（2024—2028 年）（征求意见稿）》，围绕实施可信数据空间能力建设行动、开展可信数据空间培育推广行动、推进可信数据空间筑基行动提出十三项行动。

征求意见稿指出，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。

行动计划方面，征求意见稿要求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，落实数据安全分类分级、动态感

知、风险识别、应急处理、治理监管等要求，建立可信数据空间安全管理体系。引导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. 国家数据局向社会公开征求《数据领域名词解释》意见

10 月 21 日，国家数据局就《数据领域名词解释》向社会公开征求意见。征求意见稿给出原始数据、数据资源、数据要素市场化配置、数字经济高质量发展等 41 项名词的解释。

其中，数据要素是指能直接投入到生产和服务过程中的数据，是用于创造经济或社会价值的新型生产要素。

隐私计算是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私计算的常用技术方案有多方安全计算、联邦学习、可信执行环境、密态计算等；常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

多方安全计算是指在无可信第三方的条件下，通过特殊设计的密码学算法和协议，允许多个参与方在不泄露各自隐私数据的前提下，协同完成计算任务。（来源：国家数据局）

5. 三部门印发《新材料大数据中心总体建设方案》

10 月 16 日，工信部、财政部、国家数据局联合印发《新材料大数据中心总体建设方案》，搭建形成“1+N”的新材料大数据中心架构体系（1 个新材料大数据中心主平台、N 个数据资源节点）。

根据方案，新材料大数据中心定位为促进新材料产业创新发展的新型研发基础设施，旨在立足机制创新、协同创新、成果转化，构建新材料数据资源中心、数据产品研发中心、数据基础产品和定制化服务提供中心，主要功能为构建材料数据汇聚标准和融通平台、加强共性和前沿技术研究、开展材料数据软件产品开发应用、提供材料数据公益服务、加强材料基因领域创新人才队伍建设、推进材料数据和技术国际合作。

方案明确新材料大数据中心的建设任务：一是搭建新材料大数据中心架构体系。建立以公益性服务为主的中心主平台，统筹建门户、出标准、定规则；布局以商业化运营为主的数据资源节点，负责采数据、用数据、保质量。二是建立数据流通应用技术体系，包括标准规范体系、管理共享机制、数据安全保障体系。三是优化新材料大数据技术应用生态。着力研发关键技术和软件，开展重点领域应用示范，创新人才队伍建设和公益服务。（来源：中国政府网）

6. 工信部印发《工业和信息化领域数据安全事件应急预案（试行）》

10 月 29 日，工信部印发《工业和信息化领域数据安全事件应急预案（试行）》。

预案共八章四十条，重点明确以下八方面内容：一是界定预案适用范围，明确数据安全事件以及事件分级的相关概念定义；二是明确工业和信息化领域数据安全应急处置工作的组织体系，规定领导机构、办事机构、地方行业监管部门、数据处理者、应急支撑机构等单位的构成及职责；三是明确开展数据安全风险监测预警工作的具体流程和要求；四是明确不同

级别数据安全事件应急处置工作的具体流程和要求；五是规定重大及以上数据安全事件应急工作结束后，地方行业监管部门和数据处理者的具体工作要求；六是提出预防保护、应急演练、宣传培训、手段建设、重大活动期间保障共五项预防措施；七是提出落实责任、奖惩问责、经费保障、工作协同、物资保障、国际合作、保密管理共七项保障措施；八是规定应急预案修订原则和排除条款等要求。

此外，预案在附件中细化数据安全事件分级方法、事件上报模板、事件总结报告模板、应急处置流程图等内容，为各方开展应急处置工作提供细化实操指导。（来源：工信部）

7. 国家密码管理局发布《关于做好〈电子政务电子认证服务管理办法〉实施工作的公告》

10 月 31 日，为做好《电子政务电子认证服务管理办法》实施工作，国家密码管理局发布《关于做好〈电子政务电子认证服务管理办法〉实施工作的公告》。

公告明确，国家密码管理局委托各省、自治区、直辖市密码管理部门，新疆生产建设兵团密码管理部门负责受理本行政区域的电子政务电子认证服务机构资质申请，对申请材料进行形式审查，出具受理通知书或者不予受理通知书。自 2024 年 11 月 1 日起，申请人可以向住所地省级密码管理部门提出资质申请。（来源：国家密码管理局）

8. 十项网络安全国家标准获批发布

10 月 9 日，全国网络安全标准化技术委员会归口的十项国家标准正式发布，包括：《数据安全技术 互联网平台及产品服务个人信息处理规则》《网络安全技术 实体鉴别 第 2 部分：采用鉴别式加密的机制》《网络安全技术 消息鉴别码 第 2 部分：采用专门设计的杂凑函数的机制》《网络安全技术 杂凑函数 第 1 部分：总则》《网络安全技术 杂凑函数 第 2 部分：采用分组密码的杂凑函数》《网络安全技术 杂凑函数 第 3 部分：专门设计的杂凑函数》《网络安全技术 网络和终端隔离产品技术规范》《网络安全技术 信息安全控制》《网络安全技术 办公设备安全规范》《网络安全技术 智能门锁网络安全技术规范》。（来源：全国网安标委）

（三）地方层面动向

1. 广东省政务服务和数据管理局发布《广东省数据条例（草案征求意见稿）》

10 月 8 日，广东省政务服务和数据管理局发布《广东省数据条例（草案征求意见稿）》。草案征求意见稿共八章六十七条，包括数据权益保护、数据资源、数据流通等内容。

数据资源方面，草案征求意见稿规定，公共管理和服务机构应当根据公共数据资源目录，完整、准确、及时地向公共数据平台汇聚公共数据。省数据主管部门应当会同省有关部门在省公共数据平台建立完善自然人、法人和非法人组织、自然资源和空间地理、电子证照、经济治理等基础数

据库。公共管理和服务机构应当按照应用需求在本级公共数据平台建立和完善跨地域、跨部门专题数据库。

数据流通方面，草案征求意见稿指出，在保障国家秘密、国家安全、公共利益、商业秘密、个人隐私和数据安全的前提下，省和市人民政府及其有关部门可以授权符合条件的法人或者非法人组织运营公共数据，并与被授权运营主体签订授权运营协议。鼓励有条件的县（区）、乡（镇）按照规定开展公共数据授权运营。授权主体负责对被授权运营主体实施日常监督管理。

安全与保障方面，草案征求意见稿指出，公共管理和服务机构依法委托第三方服务机构开展平台建设以及运行维护的，应当按照国家和省有关规定对服务提供方进行安全审查；经安全审查符合条件的，签订服务协议时应当同时签订服务安全保护协议以及保密协议，约定违约责任。

草案征求意见稿规定，公共管理和服务机构及其工作人员在数据交易流通、应用创新等先行先试工作中出现偏差失误或者未能实现预期目标，但是符合国家确定的改革方向，决策程序符合法律、行政法规规定，且勤勉尽责、未牟取私利，能够及时纠错改正，未造成重大损失或者社会负面影响的，应当按照有关规定从轻、减轻或者免予追责。（来源：网信广东）

2. 广州市人大常委会法工委发布《广州市数据条例（草案修改稿·征求意见稿）》

10 月 23 日，广东省广州市人大常委会法工委发布《广州市数据条例（草案修改稿·征求意见稿）》。草案修改稿·征求意见稿共八章四十五条，

包括数据资源、数据要素市场、数据产业发展、南沙深化数据开发合作、数据安全等内容。

南沙深化数据开发合作方面，草案修改稿·征求意见稿提出，广州市南沙区人民政府及其有关部门应当按照国家有关规定，开展数据跨境流动安全管理创新和试点应用，建立面向企业的数据跨境安全管理指导机制。南沙区人民政府应当建立数据出境负面清单管理机制，制定相关数据安全保障预案，及时掌握数据安全风险状况，强化数据安全风险管控能力，探索构建数据跨境服务和安全保护体系。

数据安全方面，草案修改稿·征求意见稿规定，网信、公安、数据等有关部门应当探索建立数据相关的新技术运用安全评估机制，防止数据相关的新技术运用危害国家安全和公共利益、扰乱经济秩序和社会秩序、侵犯他人合法权益等。此外，发生突发事件时，有关行业主管部门可以依法要求自然人、法人和非法人组织提供突发事件应对工作所必需的数据，并明确告知数据使用的目的、范围、方式。对在突发事件应对过程中获取的数据，有关行业主管部门及相关主体应当履行数据安全保护职责，不得擅自向第三方提供或者用于突发事件应对以外的其他用途。突发事件应对结束后，有关行业主管部门及相关主体应当对涉及国家秘密、商业秘密和个人隐私的数据进行封存或者销毁等安全处理。（来源：广东省政务服务和数据管理局）

3. 四川省十三部门印发《四川省数据知识产权登记办法（试行）》

10 月 8 日，四川省市场监督管理局、四川省高级人民法院、四川省经济和信息化厅等十三部门印发《四川省数据知识产权登记办法（试行）》。办法共四章三十条，包括登记程序、运用与管理等内容。

办法明确数据知识产权登记对象、原则和主管部门。办法明确登记对象为依法收集、经过一定算法加工、面向具体场景、具有实用价值和智力成果属性的数据，登记原则为依法合规、自愿登记、安全高效、公开透明、诚实信用，登记主管部门为四川省市场监督管理局（省知识产权局）。

加强数据知识产权登记监管和运用方面，办法明确数据知识产权证书作为数据知识产权流通、交易、收益分配和权益保护等初步证明文件的法律地位，加强数据知识产权登记工作、登记证书运用等方面的管理，要求市场监管（知识产权）部门依照有关规定将违规违法行为信息记入信用档案。（来源：四川省市场监督管理局）

4. 浙江省发展和改革委员会发布《浙江省“人工智能+”行动计划（2024—2027 年）（征求意见稿）》

10 月 8 日，浙江省发展和改革委员会发布《浙江省“人工智能+”行动计划（2024—2027 年）（征求意见稿）》。

征求意见稿提出“到 2027 年，培育形成 10 个以上全国一流的垂直行业大模型，500 个以上可复制推广的标杆应用场景，1000 个以上融合示范案例，全力打造人工智能创新发展和融合应用高地”的总体目标。

征求意见稿围绕人工智能+科学、教育、交通、治理、能源、金融等12个重点领域提出具体行动要求。其中，人工智能+治理领域，征求意见稿提出，构建智慧型政府，推进大模型技术在政务咨询、业务办理等场景应用，提升公共服务效能。建设浙江省法治知识服务中心，全面构建服务政府合规、社会治理的权威、互惠法治大数据共享体系。（来源：浙江省发展和改革委员会）

5. 北京市教育委员会印发《北京市教育移动互联网应用程序备案实施细则》

10月11日，北京市教育委员会印发《北京市教育移动互联网应用程序备案实施细则》。细则共九章三十五条，包括提供者备案、使用者备案、选用制度、评议推荐制度等内容。

细则所指的教育APP是以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的互联网移动应用程序。教育APP的备案分为提供者备案和使用者备案。提供者备案按照“全国统一标准、各省分头实施、单位属地备案”的原则开展。使用者备案根据隶属关系向主管教育行政部门备案。

细则规定，提供者应在完成互联网信息服务（ICP）备案和网络安全等级保护定级备案后，进行提供者备案。住所地或注册地为北京市的企业、社会组织和平台方均向市教委进行提供者备案。各子公司（分公司）或分支机构开发的教育APP，由总公司统筹进行备案。

细则强调，自主开发、自主选用和上级部门要求使用的教育 APP 均需进行使用者备案。使用者应登陆教育部教育移动互联网应用程序备案管理平台，在已完成提供者备案的教育 APP 中进行勾选，完成使用者备案。（来源：北京市人民政府）

6. 北京市教育研究部门研制发布《北京市教育领域人工智能应用指南》

10 月 26 日，《北京市教育领域人工智能应用指南》发布，指导学校和师生稳妥有序开展应用实践。

指南是北京市教育研究部门研制的首份教育领域人工智能应用指南，将规范学校教育应用人工智能，为教育工作者提供系统化指导。结合国内外政策、理论研究和实践应用，以及面向本市中小学师生家长开展的调研分析，指南明确以“智”助教、以“智”助学、以“智”助评、以“智”助育、以“智”助研、以“智”助管六大重点应用领域 29 个典型场景，覆盖人工智能在学校教育中的所有关键应用层面。

本市还将设置动态调整机制，确保指南内容随技术发展和教育需求变化而优化，帮助学校持续改进人工智能应用策略。教育领域人工智能高质量数据集和人工智能应用测试场同步启动建设。（来源：网信北京）

7. 山东省大数据局发布《山东省数据交易管理办法（试行）（征求意见稿）》

10 月 14 日，山东省大数据局发布《山东省数据交易管理办法（试行）（征求意见稿）》。征求意见稿共八章二十九条，包括交易标的、交易主体、交易方式、交易行为等内容。

征求意见稿指出，数据交易标的主要为数据产品，包括 API 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、算法模型类等其他类型。

征求意见稿规定，数据供需双方开展数据交易，可以自主选择：通过数据交易机构交易；数据供需双方直接交易；其他法律法规允许的交易方式。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、行政事业单位采购的数据产品、国有企业采购或出售的数据产品在数据交易机构开展数据交易。

征求意见稿强调，数据供需双方可以选择成本定价、收益定价、协商定价、拍卖定价、评估定价等方式，自主定价。用于数字化发展的公共数据有偿使用，执行政府指导定价。（来源：山东省大数据局）

8. 江苏省政府办公厅印发《江苏省公共数据授权运营管理暂行办法》

10 月 23 日，江苏省政府办公厅印发《江苏省公共数据授权运营管理暂行办法》。办法共六章二十九条，包括授权程序、主体责任、数据运营、监督管理等内容。

授权程序方面，办法指出，公共数据授权运营采用“两级主体、分级授权”的模式。两级主体是指运营主体和开发主体，分级授权是指省、设区的市人民政府授权本级数据主管部门试点确定本级运营主体。其中，运营主体是指承担公共数据授权运营，包括授权运营平台建设、数据加工处理、开发利用管理、服务能力支撑、市场生态培育和安全保障等工作的经营主体；开发主体是指依托公共数据授权运营平台，依场景开发利用经协议授权的公共数据，形成数据产品并向社会提供的经营主体。

数据运营方面，办法规定，公共数据授权运营平台应当在授权运营域中建设运行，并依托政务云部署，确保公共数据申请、加工处理、开发利用不出域。在数据主管部门和行业主管部门指导监督下，运营主体应当基于公共数据资源目录，结合应用场景登记形成授权运营数据资源目录，依据目录向数据主管部门申请数据。开发主体结合应用场景申请数据资源，运营主体确认后提供。

监督管理方面，办法明确，网信部门会同数据主管部门、公安及行业主管部门等建立健全数据安全协同监管机制，明确公共数据授权运营各主体全过程的安全责任，加强对两级主体安全监督检查，包括安全管理组织机构、制度、技术及安全评估、应急预案、个人信息保护、数据出境安全等情况，推动公共数据授权运营安全有序规范开展。（来源：江苏省人民政府）

9. 江苏省政府办公厅印发《关于加快释放数据要素价值培育壮大数据产业的意见》

10 月 23 日，江苏省政府办公厅印发《关于加快释放数据要素价值培育壮大数据产业的意见》。意见围绕夯实数据资源供给能力、促进数据资源开发利用、深化数据要素市场建设、培育多元化产业经营主体等六方面提出 24 项具体措施。

夯实数据资源供给能力方面，意见提出，加强公共数据高水平供给。开展全省公共数据攻坚三年行动，推进公共数据资源体系建设。坚持“一数一源”，加强源头治理，健全公共数据标准规范。优化省市公共数据平台，实现省市平台统一纳管、数据目录统一编制、资源分层分级管理。发布高价值数据清单，推进公共数据综合治理和整合共享。聚焦基层亟需，推动数据回流。

增强产业发展综合支撑方面，意见要求，强化数据安全治理监管。落实国家数据分类分级保护制度，加强对涉及国家安全、商业秘密、个人隐私等数据的保护。强化数据全生命周期的可信可控可溯源，建立健全数据安全风险评估、监测预警和应急处置等机制，开展公共数据利用的安全风险评估和应用业务规范性审查。探索建立便利化的数据跨境流动安全管理机制，加强跨部门协同监管。强化跨境数据专线安全管理。（来源：江苏省人民政府）

境内前沿观察三：治理实践

导读：10 月，公安、网信、工信、检法等部门持续强化网络空间安全治理，通过部署专项行动、强化行政执法、加强犯罪打击、总结治理成效等方式净化网络空间、保障网络安全、提升安全意识。

专项行动方面，中央网信办部署开展“清朗·整治违规开展互联网新闻信息服务”“清朗·规范网络语言文字使用”“清朗·同城版块信息内容问题整治”专项行动，进一步规范互联网新闻信息服务活动，整治网上国家通用语言文字不规范使用乱象，集中治理同城版块易发多发问题，压紧压实网站平台主体责任。

行政执法方面，各部门综合运用监督检查、行政处罚、约谈、合规培训教育等手段提升行政执法效能。重庆市南岸区委网信办、区审计局组建联合审计（检查）组，对相关审计单位开展网络安全联合检查，重点关注网络安全工作责任制落实情况、网络安全制度建设及执行情况等。海南省通信管理局组织开展“海盾行动——2024”网络和数据安全实网攻防演练，此次演练首次加入供应链企业。广东省通信管理局对省内 14 家电信领域企业开展“数安护航”专项行动数据安全现场诊断工作，聚焦企业在数据非法收集、数据非法利用、防护措施不到位、人员违规操作等突出问题引发的数据安全风险。

总结治理成效方面，上海市检察院通报全链条打击网络犯罪情况，上海市杨浦区检察院、北京互联网法院通报个人信息相关案件办理情况。具体来说，上海市检察机关 2023 年以来受理审查逮捕网络犯罪案件 4550 件

8099 人，受理审查起诉网络犯罪案件 9838 件 16146 人；审查起诉案件数量前三名犯罪分别为帮助信息网络犯罪活动罪，诈骗罪（电信网络诈骗）和掩饰、隐瞒犯罪所得、犯罪所得收益罪。上海市杨浦区检察院自 2020 年以来共受理侵犯公民个人信息罪审查逮捕案件 19 件 20 人，起诉案件 34 件 44 人；案件呈现总体数量下降但出现新犯罪方法、个案涉及信息数量较多且呈现针对性、购买群体涉及行业多非法牟利速度快三大特点。北京互联网法院自 2023 年 10 月以来共受理 113 件涉及个人信息保护的案件，涉及行业领域较为广泛，以互联网企业为被诉主体的案件最多，涉诉个人信息类型和侵权形态较为多样。

此外，全国数据标准化技术委员会（SAC/TC609）获批成立，工作范围是对数据领域国家标准进行统一技术归口，统一组织申报、送审和报批。国家安全部还发布一起境外公司非法开展地理信息测绘案件，某境外公司通过与我国具有测绘资质的公司合作，以开展汽车智能驾驶研究为掩护，在我国内非法开展地理信息测绘活动。

关键词：清朗专项行动、实网攻防演练、联合执法、全国数据标准化技术委员会、地理信息非法测绘

（一）公安机关治理实践

1. 国家网络与信息安全信息通报中心发现一批境外恶意网址和恶意 IP

10 月 21 日消息，国家网络与信息安全信息通报中心近日发现一批境外恶意网址和恶意 IP，有多个具有某大国政府背景的境外黑客组织，利用这些网址和 IP 持续对中国和其他国家发起网络攻击。这些恶意网址和 IP 都与特定木马程序或木马程序控制端密切关联，网络攻击类型包括建立僵尸网络、网络钓鱼、勒索病毒等，以达到窃取商业秘密和知识产权、侵犯公民个人信息等目的，对中国国内联网单位和互联网用户构成重大威胁，部分活动已涉嫌刑事犯罪。相关恶意网址和恶意 IP 归属地主要涉及：美国、波兰、荷兰、保加利亚、土耳其、日本等。（来源：国家网络与信息安全信息通报中心）

2. 因未履行个人信息保护义务，广西钦州一机构被处罚

10 月 13 日消息，广西钦州网警近日在日常检查时发现，灵山县某机构对用户个人信息管理不规范，其通过租用 APP 共收集 6600 多名会员信息数万条，包括姓名、身份证号码、手机号码、家庭住址等个人敏感信息。

经进一步检查发现，该机构未按要求制定内部管理制度和操作规程，未采取相应的加密和去标识化等安全技术措施，未合理确定个人信息处理的操作权限，未定期对从业人员进行安全教育和培训，未履行个人信息保

护义务，存在公民个人信息泄露或非法提供、出售公民个人信息的风险。钦州公安机关依法予以行政处罚。（来源：公安部网安局）

3. 因非法获取个人信息用于电话推销，甘肃警方对一家具专卖店作出行政处罚

10 月 23 日消息，因非法获取有装修房屋家具需求群体的个人信息用于电话推销，甘肃省张掖市网安部门近日对一家具专卖店进行行政处罚。

2024 年 1 月，甘肃省张掖市网安部门在宣传和执法工作过程中，多名群众反映接到本地企业的推销电话“骚扰”，影响个人生活。民警根据此线索核查发现，某某家具专卖店在售卖家具过程中为提高业绩，存在非法获取公民个人信息的违法行为。民警发现，该家具专卖店为提高家具店销售业绩，非法获取一批装修房屋家具需求群体个人信息，进行电话推销家具业务。公安机关依照《网络安全法》第四十四条、第六十四条之规定，对非法获取、向他人提供个人信息的违法人员依法给予处罚。（来源：公安部网安局）

4. 甘肃警方破获一起侵犯公民个人信息案，实现全链条打击

10 月 12 日消息，夏季治安打击整治行动期间，甘肃公安机关网安部门在工作中发现，有人在网上贩卖电商订单数据，涉及多名公民个人信息，引起网警高度警觉。

随着案件深入调查，发现被泄露信息的公民多次接到陌生推销电话和各类虚假购物信息，严重影响个人日常生活。办案民警发现，个别不良商

家为实现精准营销，违反电商平台相关行为规范将订单信息提供他人进行数据解密后贩卖，由此衍生出一条以企业单位内部工作人员为内鬼、订单解密技术人员为上线、层级代理为中间商、个别不良商家为下线的侵公黑灰产业链。鉴于案件涉及地域广、案情重大，该案被甘肃省公安厅列为挂牌督办案件。

专案组经过攻坚，先后辗转多地，抓获犯罪嫌疑人 18 人，查获一批公民个人信息，收缴涉案资金 35 万余元。案件侦破后，梳理出全国多地涉案人员 200 余人，发起集群打击，支撑破获刑事案件 63 起，行政案件 19 起，累计抓获犯罪嫌疑人 84 人，批评教育 176 人，实现全链条生态打击。（来源：公安部网安局）

5. 福建福州警方打掉一利用虚拟币洗钱团伙

10 月 14 日消息，福建省福州警方近日在工作中发现一条为网络诈骗等黑灰产平台提供资金转移和支付结算的案件线索，涉案金额巨大，警方迅速成立专案组开展案件侦查。

经过研判，警方查明该犯罪团伙系通过运营第四方支付平台，采用虚拟货币稳定币为非法期货平台黑灰产业提供资金转移支付，并从中赚取返佣。2024 年 7 月，福州警方奔赴各地开展统一收网行动，一举抓获以潘某某为首的犯罪嫌疑人 11 名。目前，潘某某等 11 人已被公安机关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）

6. 新疆警方侦破一起电信网络诈骗案件，抓获犯罪嫌疑人 58 人

10 月 15 日，新疆生产建设兵团第二师铁门关市公安机关近日通过侦破一起电信网络诈骗案件，串并 168 起案件，涉案金额 6200 余万元，办案民警奔赴全国 10 个省市，抓获 58 名涉案嫌疑人。

本案中，赵清茉女士（化名）遭受网络诈骗后，向第二师乌鲁克垦区公安局刑侦大队报警。经公安机关侦查发现，该诈骗团伙利用赵清茉的银行卡进行取现，然后由专人通过当面交易的方式取走现金。民警根据其提供的交易地点迅速排查，锁定了交易车辆的车牌号。经过侦查发现，该车辆为犯罪嫌疑人租赁的车辆，民警又通过租车行的租车信息进一步侦查，锁定了犯罪嫌疑人为广东籍，每次交易都是乘飞机从广东飞到新疆，然后租车前往赵清茉处取钱。在锁定犯罪嫌疑人后，办案民警立即赶往广东当地落地打击，成功抓获了该涉案团伙的“车手”。

在成功抓获一名“车手”后，另一组民警也根据赵清茉被诈骗的账号进行线上追踪。通过对该案件信息流、资金流等进行全要素串并发现，诈骗分子通过在境外利用境内“号商”提供的 QQ 号、微博账号、抖音账号等社交账号接触受害人，然后引诱受害人线上购买虚假投资理财产品并相互转账，再从线下取走受害人取出的现金，交给指定的虚拟币交易商，最后通过线上迅速将诈骗资金转移境外。

根据研判线索和掌握情况，专案组对诈骗团伙使用的多个社交账号进行线上追踪分析，关联锁定为诈骗集团提供社交账号的犯罪嫌疑人周某，继而深挖锁定孟某等为骨干成员的“号商”团伙，并根据这个“号商”团

伙循线追踪发现串并全国168起电信网络诈骗案件，涉案金额达6200余万元。另一方面，专案组根据“车手”供述，也成功锁定了伍某等“币商”和“车手”团伙。

专案组制定周密计划，组织办案民警辗转山东、安徽、福建等全国10个省市开展集中落地抓捕行动，成功抓获“币商”团伙5人，“号商”团伙53人，共抓获58名涉案嫌疑人。同时，专案组在案件侦办中还将3名境外诈骗集团人员的真实身份成功锁定并核实。目前，该案警方仍在进一步侦办中。（来源：首都网警）

7. 新疆公安机关侦办一起侵犯公民个人信息案件

10月19日消息,新疆公安网安部门近日破获一起侵犯公民个人信息案，斩断一条帮助信息网络犯罪活动的黑色利益链。

2022年12月，阿勒泰网民叶某在网上看到一条“收购网络账号”的信息，随即添加对方QQ号并将本人注册使用的微信账户出售，此后叶某主动加入非法网络账号黑产群组，结识多名“收号”上家，联系对方将非法收购的微信账号、QQ账号进行售卖。为进一步非法获利，叶某伙同巴某、依某、米某等人在微博、微信、QQ群等多个网络平台通过个人账号发布收购网络账号信息，并发展在校学生等多名下线成员收购他人网络账号，再按照网络账号实名认证、使用年限、网络支付权限等，转售至违法犯罪团伙用于电信诈骗、网络犯罪引流、网络暴力、网络谣言等违法犯罪行为，逐渐形成一条组织严密、分工明确的网络黑灰产犯罪链条。目前，该团伙违

法行为构成侵犯公民个人信息罪，经公安机关侦查终结移送起诉，叶某四人被福海县人民法院依法判处有期徒刑并处罚金。

为确保侵犯公民个人信息违法犯罪打深、打透、打彻底，新疆网安部门对该团伙网上违法行为持续开展侦查，顺线深挖涉及全国 22 省 99 人的犯罪链条，会同属地网安部门开展打击惩治，目前共立案 26 起，打击处理 109 人，涉及互联网虚拟账号 1300 余个，涉案金额百万余元。（来源：新疆网警）

8. 四川警方打掉一个涉案金额超 1 亿元的“网络水军”团伙

10 月 18 日消息，四川内江市中区警方近日打掉一个涉案金额超 1 亿元的“网络水军”团伙。

2024 年 3 月，内江市中区网警在工作中发现一款名为“某某战队”的微信小程序打着“99 看播”“躺赚”等噱头，招募全国各地人员充当“网络水军”从事网络虚假刷单行为。进一步侦察发现，“某某战队”的新会员入会时须缴纳 199 至 2999 元不等的会员费。根据缴纳会员费的多少获得创始人、董事、学员等不同层级称号，从而分配业务员、刷手、客服等不同职务，并用类似传销的手法通过网络快速发展新会员。

同时，为规避风险，“某某战队”都会按照购物平台的要求进行完整的流程交易，但从不实际购买商品。刷单任务开始后，商家会邮寄空包裹进行虚假发货。待快递显示签收，客服立即联系刷手给予商品五星好评。创始人、董事、刷手则分别从商家支付的刷单费中获取每单 1-50 元不等的佣金。

今年4月至8月，内江市中区公安组织骨干民警成立专案组赴多地对刷手、代理、推广、技术维护平台经营等人员进行抓捕，抓获嫌疑人23名，查扣资金300万余元，查获大量手机、电脑、电话卡、银行卡等作案工具。经查，该团伙自2022年3月以来通过虚假下单、刷好评等方式已为抖音、小红书、拼多多、淘宝等平台1000余户商家“刷单控评”，其涉案金额高达1亿元。

目前，涉案犯罪嫌疑人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）

9. 四川南充仪陇公安破获一起特大破坏计算机信息系统案，涉案金额1.2亿元

10月30日消息，四川南充仪陇公安近日破获一起特大破坏计算机信息系统案，打掉开发、销售和使用黑客破坏软件的犯罪团伙4个，查获黑客软件源码2套，涉案金额1.2亿余元。

仪陇县公安网安部门工作中发现，一家电器售后负责人老板徐某，经常使用“A助手软件”对国内某知名电器售后服务APP进行操作，频繁上传电器安装地址和照片，疑似有网络攻击行为。警方迅速开展工作，发现嫌疑人徐某使用这款软件突破安全防护，非法侵入该电器公司售后服务系统，并伪造、上传安装服务工单，用以骗取售后服务安装维护费用。经进一步侦查发现，该团伙除使用“A助手软件”外，还使用另一款具备非法侵入、控制售后服务系统伪造安装工单功能的黑客软件。

专案组研判出黑客软件开发人员及其销售运营团伙。专案组立即组织40名精干力量分别奔赴多地，成功抓获两款黑客软件销售运营团伙15人，扣押涉案电脑21台、手机18部，查扣涉案资金360余万元。顺藤摸瓜，警方再赴2地成功抓获该两款黑客软件开发者张某、白某二人，查获外挂软件源代码2套，查扣涉案资金200余万元，彻底斩断两条黑客犯罪团伙链条。

经调查，犯罪嫌疑人利用国内某知名电器集团公司官方APP存在的安全漏洞，开发出能够侵入售后服务系统并非法控制进行数据修改的黑客工具。警方梳理出全国29省市，涉及售后合作网点700余个，涉案总金额高达1.2亿余元。

日前，该案嫌疑人徐某、白某等14名主要犯罪嫌疑人员因涉嫌非法获计算机信息系统数据、提供侵入、非法控制计算机信息系统、破坏计算机信息系统等犯罪被分别依法判处有期徒刑，并追缴违法所得。（来源：公安部网安局）

10. 浙江警方破获一起制造、售卖非法控制停车场车辆道闸系统权限工具案

10月21日消息，浙江遂昌县公安网安部门近日破获一起制造、售卖非法控制停车场车辆道闸系统权限工具案。

公安网安部门工作中发现，一电商平台专门从事制造、推广、销售具备非法控制车闸遥控功能的设备。民警在初步侦查后发现该团伙生产的车闸遥控设备可以获取停车场车辆道闸系统使用权限。用户在购得该遥控设

备后只需将设备带至车辆道闸附近，打开设备对附近信号进行自动搜索扫描，道闸信号自动匹配成功后即获取车闸控制权限。用户出入时通过遥控设备控制车闸开关即可任意进出停车场，从而逃避停车场道闸收费，严重破坏正常的市场经济秩序。

经查，自 2021 年 6 月起，犯罪嫌疑人周某某伙同吴某某注册了一家电子科技公司专门生产销售具有自动扫码功能的车闸遥控设备，并通过多个电商平台进行线上销售。同时为获取更大的市场份额，周某某、吴某某积极发展代理商。

公安机关迅速组织警力分别前往多地开展统一收网行动，成功抓获犯罪嫌疑人周某某等 14 人，查获车闸遥控设备 12000 余套，捣毁制造窝点 2 处、仓库 3 个，扣押涉案手机 25 部、电脑 18 台，涉案金额达 1000 余万元。2024 年 8 月，被告人周某某等 6 人均被遂昌县人民法院以提供非法控制计算机信息系统工具罪追究刑事责任，现本案已依法宣判。（来源：公安部网安局）

11. 沈阳警方成功破获一批“号贩子”非法倒卖医院稀缺号源案件

10 月 22 日消息，沈阳警方近日成功破获一批“号贩子”非法倒卖医院稀缺号源案件，共打掉犯罪团伙 9 个，抓获犯罪嫌疑人 112 名，扣押涉案计算机、手机 245 台（部），涉案金额达 300 余万元。

2024 年 8 月初，沈阳警方在工作中获悉：自沈阳各大医院推行网上预约挂号以来，一些“黄牛”人员通过多种科技手段恶意抢占号源，再大幅

加价倒卖，最高收费达3000元，给广大患者造成“一号难求”“买号认宰”等困难，严重扰乱正常医疗秩序，损害患者的合法权益。

获取线索后，沈阳市公安局便衣警察支队联合网络安全保卫支队等警种部门组成专案组，立即展开案件侦办工作。专案组经多方搜集信息，深入排查走访、循线深挖，迅速掌握王某君等9个犯罪团伙的组织架构和作案手段。团伙以亲属、朋友关系为主，并广泛发展下线，团伙之间人员交叉、相互串联，主要通过“使用软件反编译破解挂号系统中传输的加密数据”和“架设模拟器使用点击软件代替人工频繁点击进行抢号”等方式作案。在2024年1月至9月期间，9个团伙共计抢号23000余次，涉及6家医院。

专案组历时2个月的缜密侦查，在全面掌握上述团伙的犯罪证据后，决定开展集中收网行动，抽调612名精干警力实施抓捕，将王某君等9个犯罪团伙全部打掉，并奔赴北京、河北廊坊、辽宁朝阳等地，将制作、售卖外挂抢号软件，向全国各地售卖的尹某某、陈某、魏某某3名犯罪嫌疑人抓获，截至目前，共抓获相关涉案人员112人，扣押涉案计算机、手机245台（部），涉案金额达300余万元。

目前，112名犯罪嫌疑人因涉嫌侵犯计算机信息系统相关犯罪、寻衅滋事罪，已被警方依法采取刑事强制措施，案件正进一步办理中。（来源：法治日报）

12. 广东警方公布打击整治网络黑灰产十起典型案例

10 月 24 日，广东警方公布打击整治网络黑灰产工作成效。据悉，今年以来，广东省公安机关持续深入推进“净网 2024”专项行动，坚持以打开路、以打促管、以打促治，重拳打击利用技术手段搭建发卡平台非法出售网民账号、非法获取网民账号、开发销售外挂软件等一系列突出犯罪，共侦破相关案件 1328 起，刑事拘留 1489 人，打击整治工作取得阶段性成效。

广东警方公布打击整治网络黑灰产 10 起典型案例，分别是：（1）珠海公安机关侦破一起利用酒店设备搭建 VOIP 设备的帮助信息网络犯罪活动案；（2）肇庆公安机关侦破一起“恶意索赔”的侵犯公民个人信息案；（3）东莞公安机关破获一起架设“猫池”从事养号卖号的侵犯公民个人信息案；（4）东莞公安机关破获一起开发销售网约车抢单外挂软件的提供侵入、非法控制计算机信息系统程序、工具案；（5）惠州公安机关破获一起为开设赌场提供技术支持的帮助信息网络犯罪活动案；（6）江门公安机关侦破一起售卖虚拟定位软件的提供入侵、非法控制计算机信息系统程序、工具案；（7）清远公安机关侦破一起销售虚拟定位打卡软件的提供入侵、非法控制计算机信息系统程序、工具案；（8）佛山公安机关破获一起制作销售网约车抢单外挂软件的提供侵入、非法控制计算机信息系统程序、工具案；（9）广州公安机关破获一起“搭建交易平台”为各类黑灰产行业提供实名账号的侵犯公民个人信息案；（10）深圳公安机关破获一起使用黑客工具抢购演唱会门票的提供侵入、非法控制计算机信息系统程序、工具案。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办部署开展“清朗·整治违规开展互联网新闻信息服务”专项行动

10 月 3 日消息，为进一步规范互联网新闻信息服务活动，提升主流新闻舆论影响力，营造清朗网络空间，中央网信办近日部署开展为期 3 个月的“清朗·整治违规开展互联网新闻信息服务”专项行动。

本次专项行动针对违法违规开展互联网新闻信息服务行为，集中整治五类突出问题：一是编发虚假不实新闻信息，使用与新闻信息内容严重不符的夸张标题，或者恶意篡改、断章取义、拼凑剪辑、合成伪造新闻信息，误导社会公众；二是借舆论监督名义，通过采编、发布、转载、删除新闻信息，干预新闻信息呈现或搜索结果等手段，威胁、要挟他人提供财物、开展商业合作，谋取不正当利益；三是仿冒、假冒新闻网站、报刊社、广播电视机构、通讯社等新闻单位，或者擅自使用“新闻”“报道”等具有新闻属性的名称、标识开设网站平台、注册账号、发布信息；四是未经许可或超越许可范围开展互联网新闻信息采编发布服务、转载服务、传播平台服务。未取得互联网新闻信息采编发布服务资质，违规开展新闻采访、发布新闻信息；五是伪造、倒卖、出租、出借、转让互联网新闻信息服务许可资质。出售、出租或以其他形式委托第三方主体运营互联网新闻信息服务频道等。通过不正当手段、虚假材料等取得互联网新闻信息服务许可。（来源：中国网信网）

2. 中央网信办、教育部部署开展“清朗·规范网络语言文字使用”专项行动

10 月 11 日消息，为整治网上国家通用语言文字不规范使用乱象，塑造有利于未成年人健康成长的网络环境和育人生态，中央网信办、教育部近日部署开展“清朗·规范网络语言文字使用”专项行动。

专项行动聚焦部分网站平台在热搜榜单、首页首屏、发现精选等重点环节呈现的语言文字不规范、不文明现象，重点整治歪曲音、形、义，编造网络黑话烂梗，滥用隐晦表达等突出问题。

专项行动要求，各地网信、教育部门要强化协同联动，形成依法管理和正面引导合力，坚持问题导向，聚焦群众反映集中的问题，聚焦未成年人等特殊群体权益保护，畅通举报渠道，集中清理不规范、不文明网络语言文字相关信息，严格落实整治任务。鼓励各地结合工作实际，加强语言文字相关法律法规科普宣传，倡导文明用语用字，营造全社会重视和参与的良好氛围。（来源：中国网信网）

3. 中央网信办发布《全民数字素养与技能发展水平调查报告（2024）》

10 月 25 日，中央网信办发布《全民数字素养与技能发展水平调查报告（2024）》。报告从我国全民数字素养与技能发展的总体情况、地区情况、群体情况等进行分析，并描述区域、城乡、年龄、受教育程度等方面的具体情况。

此次系首次全国范围全民数字素养与技能发展水平调查。此次调查面向全国31个省（区、市）开展问卷调查，调查对象为18-69周岁成年公民和12-17周岁未成年公民，共回收样本288万份，其中有效样本272万份。

报告显示，我国六成以上公民具备初级及以上数字素养与技能；数字素养与技能水平和区域经济发展态势相符；城乡居民数字素养与技能水平协同提升；各年龄段人群数字素养与技能发展态势持续向好；受教育程度是影响数字素养与技能的关键因素；我国劳动者适应数字时代职业发展需要的能力逐步增强，全国就业人员具备初级及以上数字素养与技能水平的占比为67.85%、高级水平占比为19.75%。（来源：中国政府网）

4. 中央网信办部署开展“清朗·同城版块信息内容问题整治”专项行动

10月31日，为集中治理同城版块易发多发问题，压紧压实网站平台主体责任，切实净化同城版块网络生态环境，中央网信办部署开展“清朗·同城版块信息内容问题整治”专项行动。

本次专项行动覆盖社交、短视频、直播、资讯、电商、搜索引擎、团购点评、婚恋交友、地图导航、旅游出行、本地生活、天气日历、运动健康等平台同城（本地）榜单、版块、栏目、频道，以及各类基于地理位置提供同城信息内容或服务的移动互联网应用程序，重点整治散播网络戾气、制造网络谣言和虚假信息、呈现色情低俗信息、为同城违法活动引流、提供网络水军服务五类突出问题。（来源：中国网信网）

5. 中央网信办发布“清朗·2024年暑期未成年人网络环境整治”专项行动典型处置案例

10月9日，中央网信办发布“清朗·2024年暑期未成年人网络环境整治”专项行动成果及典型处置案例。专项行动期间，网信部门累计清理拦截涉未成年人违法不良信息430万余条，处置账号13万余个，关闭下架网站平台2000余个。部分典型案例有：

一是从严处置各类危害未成年人身心健康的“毒视频”。专项行动以涉未成年人主题、未成年人出镜内容为重点，深入整治各类传播不良导向、诱导危险行为的直播和短视频内容。网信部门指导重点平台完善涉未成年人内容审核标准，将管理要求以治理公告、站内信等形式触达网络主播，从严处置2.1万余个相关违规账号，关停直播3.2万余场。

二是集中整治针对未成年人的“开盒挂人”乱象。密切关注涉未成年人网暴风险，深入排查“校园墙”、“留言板”等环节“开盒挂人”问题。北京、河南、贵州等地网信部门深入核查问题线索，解散关闭1500余个提供挂人服务的话题、超话、贴吧，对存在突出问题的平台予以从重处罚，相关违法线索已转公安机关。

三是严厉打击隔空猥亵等网上恶性违法犯罪行为。天津、广东等地网信部门及时核查网民举报线索，督促平台加大评论区引流信息管理力度，链条式打击隔空猥亵、性引诱等问题，累计关闭相关违规群组1000余个，配合公安机关查办案件70余起。

四是深入整治网上涉未成年人违规售卖问题。上海、江苏、浙江等地网信部门督促属地电商平台，深入摸排打击售卖涉未成年人违规商品问题。专项行动期间，重点网站平台累计下架相关违规商品4.2万余个，对1400余个店铺采取关闭、扣除违约金等处置措施。

五是排查下架一批涉未成年人违规应用。专项行动期间，应用商店落实上架审核、日常管理、应急处置等管理责任，对面向未成年人提供服务的应用程序强化内容和功能安全审核。专项行动期间，重点应用商店累计排查下架900余个违规APP，对1000余个APP采取上架审核不通过措施，对部分涉严重问题的APP开发者，依约采取封禁账号、冻结账号下所有应用等措施。（来源：中国网信网）

6. 中央网信办发布涉公共政策、突发案事件、社会民生领域网络谣言典型案例

10月12日，中央网信办发布十二起涉公共政策、突发案事件、社会民生领域网络谣言典型案例，分别是：（1）“冷藏车内发现15名被拐儿童”谣言；（2）“女生在泳池被男生轮流抱摔霸凌”谣言；（3）“留学生将享受申请自费留学奖学金等六大政策扶持”谣言；（4）“中国高铁一公里耗一万度电”谣言；（5）“扫码可领‘2024年个人劳动补贴’”谣言；（6）“安徽省关于实施《公司法》注册资本登记管理制度的规定”谣言；（7）“上海虹口足球场举办活动时发生持刀伤人案件”谣言；（8）“游客在贵州旅游被‘噶腰子’”谣言；（9）“太原一学校开学第一天人去楼空”谣言；（10）“重庆红绿灯热燃了”谣言；（11）“杭州东站电车自燃烧死

人”谣言；（12）“四川达州洪灾致多人死亡”谣言。（来源：中国网信网）

7. 浙江省网信办发布十月执法处置情况

10 月，浙江网信系统坚持严格规范公正文明执法，围绕网络生态、网络安全、数据安全等重点领域，依法查处违法违规行为，督促指导网站平台整改落实，积极营造清朗网络空间。

浙江省各级网信部门依法依规约谈“lycn0570.com”“铁娘子 love”等网站账号 33 个，责令整改“网趣贸易”“一品生物”等网站平台 70 家，注销“米言”“锡兰茶叶网”等网站备案 16 家，开展行政检查、行政指导 73 次。各级网信部门及属地重点平台总计受理处置网民举报 3.3 万件，对 16 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）

8. 湖南省长沙市网信办发布第三季度网络管理执法情况

10 月 9 日，湖南省长沙市网信办发布第三季度网络管理执法情况。2024 年第三季度，长沙市网信系统深入推进网络综合治理，扎实开展“清朗”系列、未成年人网络保护等专项行动。全市网信系统共清理网络违法违规信息 527 条，警告约谈平台账号 79 个，责令注销网站或停止网站域名解析 20 家，关闭自媒体账号 12 个，封禁直播账号 19 个，对 3 家网站予以行政处罚罚款；指导属地应用商店下架违法违规应用程序 25 款，向有关部门移交案件线索 8 条。

其中，“湖南**科技股份有限公司”所属系统有多处安全漏洞，存在等保制度未落实、日志不健全、未履行数据安全保护义务等问题，7 月 26 日，长沙市网信办依据《数据安全法》第四十五条第一款之规定，对该公司作出警告、罚款五万元的处罚，对该公司直接负责的主管人员及其他直接责任人共计罚款三万元。（来源：网信长沙）

9. 重庆市南岸区委网信办、区审计局联合开展网络安全检查

10 月 10 日消息,重庆市南岸区委网信办、区审计局近日依托部门预算、经责审计等部分年度审计项目，对相关审计单位开展网络安全联合检查。

据介绍，从今年 5 月开始，两部门组建联合审计（检查）组对相关单位开展网络安全联合检查,今年共有 9 个单位纳入 2024 年度联合检查计划，截至目前，已完成 6 个单位的联合检查，其余 3 个单位正在按进度实施。

联合审计（检查）组重点关注网络安全工作责任制落实情况、网络安全制度建设及执行情况等，通过现场询问、查阅资料、远程扫描、渗透测试等方式，对被审计单位党委（党组）履行网络安全主体责任、网络意识形态工作落实、网络安全技术防护、数据安全和个人信息保护、数字化项目服务外包和公共 LED 电子显示屏等方面进行全面检查评估，充分发挥双方专业优势，提高工作成效。

针对查出的问题，逐一建立问题清单，提出整改建议，并将相关问题纳入审计报告，严格按照审计发现问题整改要求督促相关审计单位整改落实；针对面上普遍共性问题，由南岸区委网信办通报全区所属单位学习、

自查自纠，并从区级层面追本溯源、建章立制、规范管理，发挥主管部门监督管理作用。（来源：网信重庆）

10. 北京网信办组织召开自动售货机收集使用个人信息合规培训会

10 月 18 日消息，北京网信办于 10 月上旬选取 30 个自动售货机进行实地检测，测试扫码支付、刷脸支付等不同付款模式下收集个人信息情况。经查，先付制自动售货机多数只需选品后扫码付款即可弹出货物，一般不收集个人信息，出现问题率较低。后付制自动售货机因需要先授权打开柜门，消费者选品关闭柜门后再进行支付，容易出现强制或诱导刷脸支付、先采集人脸信息再弹出隐私政策、过度收集个人信息等问题。

10 月 17 日，北京网信办会同市市场监管局、国家互联网应急中心北京分中心，对北京市 18 家自动售货机运营企业开展收集使用个人信息合规培训。培训围绕“三个一”目标，结合前期现场检查实际案例情况，帮助企业学会一部法律——《个人信息保护法》，掌握一套标准——自动售货机消费场景收集使用个人信息合规标准，开展一次自查——按照培训要求进行深度自查，限时整改。

下一步，北京网信办将分批分类对更多自动售货机运营企业进行合规指导，在企业完成自查整改后，组织开展“回头看”检查，依法处置仍存在违法违规收集使用个人信息问题的企业。（来源：网信北京）

11. 四川省南充市、区两级网信、公安部门依法约谈两名违规账号负责人

10 月 14 日消息，为抵制“三俗”营造清朗清爽网络环境，四川省南充市、区两级网信、公安部门近日依法约谈两名违规账号负责人。

南充市顺庆区互联网信息办公室在工作中发现，某网络平台账号“某哥”（某阔技城）在该平台发布行为低俗、渲染暴力的短视频，涉嫌违反《网络安全法》《网络信息内容生态治理规定》等相关法律法规，扰乱正常网络秩序，造成不良社会影响。南充市互联网信息办公室、顺庆区互联网信息办公室、南充市公安局顺庆区分局网安大队依法对该账号负责人王某开展约谈教育。约谈中，执法人员组织该账号负责人认真学习相关互联网法律法规，结合典型案例以案说法，并对其进行了批评教育。通过教育引导，该账号负责人深刻认识到自身错误，表示将严格遵守相关法律法规，依法上网、文明上网，主动维护良好的网络生态环境，并写下了责任保证书。目前，该账号负责人已主动删除相关违规短视频。

接到多名群众举报，某网络平台账号“社恐阿某”在该平台发布庸俗、软色情信息。经查，该账号负责人为博人眼球、赚取流量，以男扮女装、奇装异服、模仿影视剧不良画面等为噱头，在网络平台发布宣扬庸俗、软色情内容的短视频，其行为涉嫌违反《网络安全法》《网络信息内容生态治理规定》等相关法律法规，对网络生态造成负面影响。南充市互联网信息办公室、南充市公安局网安支队、顺庆区互联网信息办公室依法对该账号负责人黄某开展约谈教育。约谈中，执法人员明确指出该账号存在的问

题，并对其进行了严肃的批评教育，责令其立即整改，严格落实账号管理主体责任，坚决抵制不良行为，切实维护网络秩序。被约谈人表示已深刻认识到自己的错误，写下责任保证书，保证今后将严格遵守相关法律法规，主动弘扬主旋律、传播正能量，自觉接受管理与监督，坚决杜绝此类问题再次发生。目前，该账号负责人已主动删除相关违规短视频。（来源：网信南充）

12. 因个人信息数据泄露，上海市网信办对某医疗科技企业作出行政处罚

10 月 14 日消息，上海市网信办近日接到线索，反映属地某医疗科技公司所属系统存在网络安全漏洞，致使系统大量个人信息数据发生泄漏被境外 IP 访问窃取。针对这一问题线索，上海市网信办立即赴涉事企业开展现场核查。经查实，该企业的确存在数据泄漏问题，暴露出公司未能履行好网络安全、数据安全保护义务，上海市网信办依据《数据安全法》对该公司予以立案调查。

通过调查核实，涉事医疗科技公司为民营医疗机构，主要从事医疗领域教育培训的技术开发服务，涉事系统为该企业内部生产测试系统，部署于云服务平台，系统数据库内存储大量个人信息数据，包含姓名、单位名称、所属省市、所在乡镇/街道、手机号（已采取加密措施）等。该系统未采取有效网络安全防护措施，存在未授权访问漏洞，网络和数据安全管理制度不完善，网络日志留存不足 6 个月，造成数据泄漏被窃取，违反《数据安全法》第二十七条规定。针对以上违法情况，上海市网信办依据《数

据安全法》第四十五条规定对该医疗科技公司给予警告，并处以罚款的行政处罚。（来源：网信上海）

13. 因违反《数据安全法》，河南郑州市网信办对两家公司作出行政处罚

10 月 23 日消息，河南省郑州市网信办近日工作中发现，郑州市两家公司未履行网络安全保护义务，未采取必要的安全防护，导致大量敏感数据被窃取。郑州市网信办依据《数据安全法》分别对两家公司作出责令改正，给予警告，并处人民币 5 万元罚款的行政处罚。两起案例具体情况如下：

案例一：经调查核实，郑州市某互联网信息服务有限公司在数据库中配置增加远程登录空口令账户，导致黑客利用该空口令账户成功登录数据库，并窃取数据库中的数据，被窃取的数据包含姓名、身份证号、手机号、邮箱地址等敏感信息。该公司在网络安全意识方面淡薄，未建立健全全流程数据安全管理制度，未采取相应的技术措施和其他必要措施保障数据安全，造成部分敏感数据泄露。针对以上违法情况，郑州市网信办依据《数据安全法》第二十七条、第四十五条，对该互联网信息服务公司作出责令改正，给予警告，并处人民币 5 万元罚款的行政处罚。

案例二：经调查核实，郑州市某科技有限公司缺乏网络安全意识，没有正确配置数据库，导致数据库存在未授权访问漏洞。攻击者通过漏洞登录数据库，查看、下载数据，导致敏感数据泄露。该公司系统访问日志功能未开启、重要的通联日志留存不足六个月，数据库系统配置不当，存在未授权访问漏洞，在网络安全管理方面存在缺失，未能按照《数据安全法》

要求对企业重要数据进行分级分类管理，系统日志存储时未对用户个人敏感信息进行脱敏处理，存在安全风险。针对以上违法情况，郑州市网信办依据《数据安全法》第二十七条、第四十五条，对该科技公司作出责令改正，给予警告，并处人民币5万元罚款的行政处罚。（来源：网信郑州）

14. 因网站停用后未及时注销备案，重庆市璧山区网信办对属地某企业作出行政处罚

10月25日消息，重庆区璧山区网信办近日依据《网络安全法》对属地一企业未履行网络安全义务行为进行立案调查并作出行政处罚。

据了解，该网站未严格履行网络安全保护义务，未建立网络安全事件应急预案，未落实网络安全责任人，网站停用后未及时注销备案，导致域名被非法盗用篡改为博彩类网站，其行为违反《网络安全法》第二十一条之规定。璧山区网信办依据《网络安全法》第五十九条规定责令其限期改正，并给予警告处罚。（来源：网信重庆）

15. 因未履行数据安全保护义务，湖南省网信办对某信息公司作出行政处罚

10月29日消息，湖南省互联网信息办公室近日在工作中发现，湖南某信息技术有限公司未落实网络安全等级保护制度，未采取相应的技术措施和其他必要措施保障数据安全，系统存在未授权访问漏洞，网络安全日志大量缺失，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，并处对该公司、主管人员和直接责任人员分别罚款五万元、二万元和一万元的行政处罚。（来源：网信湖南）

（三）通信管理部门治理实践

1. 海南信息通信业“海盾行动-2024”网络和数据安全实网攻防演练圆满落幕

10月18日，由海南省通信管理局主办的为期两周的“海盾行动——2024”网络和数据安全实网攻防演练圆满落幕。

本次演练活动共遴选出4支综合素质强、技术水平高的专业队伍参与渗透测试，靶向覆盖10家单位的86个重要信息系统和门户网站，在真实网络环境中运用多种技术手段，深入探索各防守方系统的安全漏洞；各防守方运用流量分析、蜜罐技术等手段实施全面监控与应急响应，主动发现并修补安全弱点。

演练过程结合实网对抗与录屏审计，既确保渗透测试方能够充分揭示系统安全隐患，又保障目标系统的稳定运行，实现演练的安全、可控、有序与有效监督。本次演练中首次加入供应链企业。（来源：工信部）

2. 广东通信管理局组织开展“数安护航”专项行动数据安全现场诊断工作

10 月 29 日消息，广东省通信管理局近日组织技术力量对省内的基础电信企业、数据中心和云业务企业、车联网服务平台企业、“人工智能+”大模型业务企业等 14 家电信领域企业开展“数安护航”专项行动数据安全现场诊断工作。

本次现场诊断在企业安全风险自查整改、防范处置的基础上，通过访谈交流、查阅资料、技术核验等方式，聚焦企业在数据非法收集、数据非法利用、防护措施不到位、人员违规操作等突出问题引发的数据安全风险，开展现场诊断工作。（来源：工信部）

3. 上海、浙江通信管理局通报侵害用户权益行为的 APP

（1）上海市

10 月 15 日，上海市通信管理局通报下架 12 款侵害用户权益行为的应用。通报指出，2024 年 8 月，上海市通信管理局向社会公示了一批共 26 款存在侵害用户权益行为的应用。在规定的二次整改期限内，经核查复检，尚有 12 款应用未按照要求落实整改，存在违规收集个人信息、超范围收集个人信息、APP 自启动和关联启动、未合理申请使用权限、未明示个人信息处理规则等。为严肃处理上述应用的违法违规行为，上海市通信管理局依据有关法律和规范性文件要求，已对上述应用在全国范围内主流应用市场进行下架处理。

（2）浙江省

10 月 23 日，浙江省通信管理局通报 2024 年第 9、10 批 4 款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。目前尚有 4 款 APP 未按要求完成整改，存在违规收集、使用个人信息问题。上述 APP 开发运营者应在 11 月 1 日前完成整改落实工作，整改落实不到位的，浙江省通信管理局将视情采取下架、关停、行政处罚等措施。（来源：上海市通信管理局、浙江省通信管理局）

（四）其他部门治理实践

1. 市场监管总局、国家数据局选取八个城市试点开放信用监管数据

10 月 15 日消息，市场监管总局、国家数据局近日联合印发《关于开展向平台企业开放信用监管数据试点 推动平台经济规范健康发展的通知》，选取八个城市向平台企业开放信用监管数据，以提高境外来华人员移动支付的便利性，强化平台企业落实主体责任，推动平台经济规范健康发展。八个城市分别是江苏苏州、浙江杭州、山东济南、湖北武汉、湖南长沙、广东深圳、四川成都和陕西西安。

在当前消费场景中，境外来华人员习惯绑定信用卡进行移动支付，境内个体工商户普遍使用的微信、支付宝等个人收款码不支持信用卡支付。由于移动支付平台不掌握个体工商户登记信息，造成个体工商户开通商户

收款码流程复杂、周期较长，严重影响境外来华人员支付便利性。此次印发通知旨在解决上述难点。

通知明确要求，数据开放将按照最小必要原则，采用“原始数据不出域、数据可用不可见”的方式开展数据核验，并严格限定仅用于个体工商户开通商户收款码，以及为平台企业核查个体工商户信用风险提供参考。通知还要求，加强系统、接口的安全防护，制定应急处置方案，严防数据安全问题和商业秘密泄露问题。（来源：国家市场监督管理总局）

2. 国家安全部发布一起境外公司非法开展地理信息测绘案

10月16日，国家安全部发布一起境外公司非法开展地理信息测绘案件。国家安全机关工作发现，某境外企业A公司通过与我国具有测绘资质的B公司合作，以开展汽车智能驾驶研究为掩护，在我国内非法开展地理信息测绘活动。

A公司为某国重点敏感领域项目承包商，根据《测绘法》规定，并不具备在国内单独开展地理信息测绘活动的资质。为规避我国行业主管部门监管，该公司以汽车智能驾驶研究为由，将项目多次外包，最终委托具备测绘资质的国内B公司具体实施。为尽可能直接获取原始测绘数据，A公司越过项目转包的层层节点，全程主导测绘项目进展，直接指挥B公司人员在我国内多省份开展测绘，专门委派外籍技术专家对B公司的测绘人员开展实操指导，重点把控测绘数据的存储、处理和流转等环节。最后在A公司的操控指使下，B公司将测绘所得数据转移出境。

经鉴定，A公司采集的数据多项属于国家秘密。国家安全机关会同有关部门开展联合执法活动，依法追究涉事企业和有关责任人员的法律责任。（来源：国家安全部）

3. 112家机构通过国家密码管理局商用密码检测机构（商用密码应用安全性评估业务）资质申请技术评审

10月28日，国家密码管理局发布商用密码检测机构（商用密码应用安全性评估业务）资质申请通过技术评审的机构名单，共112家机构通过评审，包括北京国家金融科技认证中心有限公司、公安部网络安全等级保护评估中心等。（来源：国家密码管理局、苏州信息安全法学所）

4. 军地职能部门处置一批网上违法违规信息及自媒体账号，并通报典型案例

10月28日消息，军地职能部门近日依法依规处置一批网上违法违规信息及自媒体账号，典型案例有：

一是捏造军事谣言。一些自媒体账号打着“军事评书”、“军事演义”旗号，以军事科普为幌子消费群众爱国情怀。微信公众号“裂变研究所”、“王婆卖瓜呀”等散布“我舰艇击沉四艘外军军舰”等谣言。有的账号通过拼凑、嫁接、剪辑等方式，炮制军事“爽文”、“自嗨”解读，编造“南海电子战12小时”、“边境爆发冲突”等虚假内容。

二是杜撰军事史实。一些账号以“科学论证”、“解密探秘”等名义搞历史虚无主义，知乎账号“六月末狂想”、“陈必红”等编排“在中国

战场上被游击战打死的日军只占很小一部分”、“长津湖之战的历史事实有一个不通的地方”等错误论调，歪曲史实、误导认知。

三是抹黑军队形象。B站UP主“图腾战术方案”恶意发布现役军人姓名、部职别、身份证号等涉密信息。抖音账号“凯玉正能量”、“峰哥正能量”等，编造“儿子不顾反对去当兵，几年后母亲却见到儿子的骨灰盒”等谣言信息；抖音账号“小团子乖宝”、“莲雾”、“小楠不难”等，散布“儿子从‘军中清华’国防科大毕业一年了，没有一家愿意录用”等虚假信息。

四是曲解军事政策。有的账号臆测散布“军队参与金融战”等不实信息。百度贴吧一些用户发布歪曲文职人员制度等不实信息，成为负面情绪集散地。一些微信公众号散布所谓“内幕消息”，称部队将重启“军转文”，妄加解读福利待遇、转业安置等政策。

五是煽动军地对立。头条账号“干一杯鸭”、“老张聊当下事”等炒作“养一支军队耗费海量资金”，鼓噪“裁军20万缓解财政压力”，挑动军地矛盾。有的账号在高考季、征兵季，对军地高校招生、军地职业发展等进行不当对比，渲染涉军校招生、部队征兵等负面信息误导舆论。

六是消费拥军情怀。抖音账号“国防发布”、“国防布发布”等恶意关联冒用军队官方账号信息，开设虚假账号。淘宝商家“咱家的百货铺”违规使用“冰雕连”图片，恶意开展营销宣传。一些淘宝、闲鱼账号使用军队特定含义字样和图案，兜售“军中茅台”、“军队专供”、仿制军服等假冒伪劣商品。一些微信小程序发布虚假招考信息，打着军队旗号诱导报考人员购买服务。（来源：中国网信网）

5. 全国数据标准化技术委员会在京成立

10 月 29 日消息，全国数据标准化技术委员会（SAC/TC609）近日获批成立。委员会由来自政府部门、高等院校、科研机构、企业、行业和地方等 98 名各界代表组成。

委员会的工作范围是对数据领域国家标准进行统一技术归口，统一组织申报、送审和报批，具体包括：（1）数据资源、数据技术、数据流通、智慧城市、数字化转型等基础通用标准；（2）支撑数据流通利用的数据基础设施标准；（3）保障数据流通利用的安全标准。

委员会的工作职责包括：（1）提出数据领域标准化工作的政策和措施建议；（2）组织制定和持续完善国家数据标准体系，研究提出数据领域制修订国家标准的规划、年度工作要点和采用国际标准的建议；（3）组织开展数据领域国家标准的起草、征求意见、技术审查、复审及国家标准外文版的翻译和审查工作；（4）组织开展数据领域国家标准的宣贯和培训工作、重点标准的试点验证和应用推广；（5）承担数据领域相关国际标准化组织的对口业务工作，组织参与国际标准化工作，组织开展对外交流活动。

委员会的未来重点方向是：（1）强化顶层设计，加强重点方面标准化前瞻研究；（2）围绕关键领域，加快推进标准制修订工作。推进数据治理标准研制，保障数据要素价值发挥；推进数据流通利用标准研制，保障数据高效流动；推进数字化转型标准研制，赋能城市和产业高质量发展；推进数据技术标准研制，强化技术服务能力；推进数据基础设施标准研制，夯实数据流通利用底座；（3）推动标准试点，有效促进标准质量及应用；

（4）加强国际交流合作，打造国际竞争新优势。（来源：国家标准化管理委员会）

6. 上海市检察院介绍打击网络犯罪等相关情况：网络犯罪主体年轻化特征明显

10 月 11 日，上海市检察院召开新闻发布会，通报 2023 年以来全市检察机关全链条打击网络犯罪、持续开展网络综合治理、推动互联网法治建设情况。

据统计，2023 年以来，全市检察机关受理审查逮捕网络犯罪案件 4550 件 8099 人，受理审查起诉网络犯罪案件 9838 件 16146 人。网络犯罪主体年轻化特征明显，“90 后”“00 后”涉案人员合计占起诉总人数的近 70%。此外，办理涉未成年人网络犯罪案件共计 309 件 338 人。

审查起诉案件数量前三名犯罪分别为帮助信息网络犯罪活动罪 3963 件，诈骗罪（电信网络诈骗）1759 件，掩饰、隐瞒犯罪所得、犯罪所得收益罪 1190 件，上述三罪名共占审查起诉案件数的 70.4%。随着打击治理跨境电信网络诈骗犯罪、“净网”等专项行动开展，诈骗罪，非法利用信息网络罪，破坏计算机信息系统、数据类犯罪，侵犯公民个人信息罪，销售假冒注册商标的商品罪等五类罪名审查起诉案件数增幅较大。

发布会表示，近年来，直播行业的兴起孵化催生出了“流量经济”，与此伴生的新型网络犯罪趋多态势明显，除“网络水军”利用网络流量实施非法刷单炒信、刷量控评等犯罪外，不法分子还借用人工智能、区块链等新技术新业态“热度”，通过流量变现获取违法所得。传统犯罪活动向

网络世界加速渗透，财产犯罪向虚拟财产领域扩展蔓延；经济金融犯罪借助网络通讯群组、直播平台等媒介，实现精准引流，快速锁定目标对象；传统“黄、赌、毒”等犯罪“线上化”趋势明显，利用网络虚拟身份、社交软件进行联络沟通、不法交易、资金支付，犯罪行为隐蔽性强、查处难度大。网络犯罪黑灰产业内核不断升级，逐步向规模化、公司化运营转型，境外加密通讯技术被广泛使用，虚拟币成为网络洗钱的重要黑产工具。电信网络诈骗犯罪跨境化、集团化、产业化程度加深，逐步从境内向境外转移，境外诈骗窝点呈现园区化特征，并持续从境内外招募、诱骗人员。

此外，企业网络安全风险持续上升，企业信息系统遭受外部及内部人员攻击案件日益增多，组织“网络水军”利用网络谣言敲诈勒索企业、利用网络暴力侵犯企业合法权益、诋毁商业信誉、商品声誉等案件频发。网络犯罪还持续向教育、食药、消费等民生领域侵蚀蔓延，如某些打着在线教培机构名义侵犯客户个人信息、付费退赔讹诈；不法分子通过网络移动端自媒体、社交软件等渠道非法销售假药劣药、有毒有害食品；不良商家发布虚假网络广告诱导消费，侵害消费者财产利益等。（来源：上海检察）

7. 上海市闵行区人民检察院公布一起流量劫持案件

10 月 18 日消息，上海市闵行区人民检察院近日提起公诉，被告单位某信息科技有限公司犯非法控制计算机信息系统罪，被法院判处罚金 20 万元；被告人王某、李某基、肖某、李某磊犯非法控制计算机信息系统罪，被法院判处有期徒刑一年九个月至三年不等，均适用缓刑，各并处罚金。

闵行区检察院介绍，周先生使用电脑时发现被流量劫持，于是前去派出所报案，一个专门靠劫持流量敛财的信息科技公司进入警方视野。经调查，2015 年末，被告四人从某互联网公司离职，决定合作创办一家信息科技公司，主要是做软件或者小程序，比如桌面清理软件或者购物平台返利软件等。2022 年，王某等人了解到可以通过静默安装插件，更改用户电脑中浏览器的计费名获得流量收益。

王某供述，计费名是搜索平台公司给的推广渠道号。王某之前有通过商务推广渠道向某知名搜索平台申请过数十个计费名。如果用户使用的搜索平台的网站链接中带有公司的计费名，平台就知道是公司介绍来的客户，就会给流量费。被问及如何实现替换电脑用户计费名时，王某供述，当时公司开发的一些桌面工具软件自带插件安装包。每次用户安装完自家公司开发的软件后，就会静默在用户的浏览器中安装浏览器插件，实现浏览搜索平台时，自动添加或更改公司申请注册的计费名。

整个犯罪流程不仅环环相扣，涉案公司内部也层级严密、分工明确。在王某提出大概的业务框架后，肖某、李某磊负责开发电脑端的相关软件，李某基负责公司所有服务器的运营维护。经鉴定，涉案公司的两款软件可进行静默安装浏览器插件，具有流量劫持功能，违法所得共计 8 万余元。

闵行区检察院认为被告单位某信息科技公司，被告人王某、李某基、肖某、李某磊违反国家规定，采用技术手段非法控制他人计算机信息系统，其行为已触犯刑法相关规定，涉嫌非法控制计算机信息系统罪。近日，经闵行区检察院提起公诉，被告单位某信息科技有限公司，王某、李某基等

四名被告人因犯非法控制计算机信息系统罪，被法院判处前述刑罚。（来源：网信上海）

8. 上海市杨浦区检察院通报2020年以来侵犯公民个人信息隐私案件办理情况

10月28日，上海市杨浦区检察院召开新闻发布会，通报2020年以来侵犯公民个人信息隐私案件办理情况，并发布相关案例。据统计，自2020年以来，杨浦区检察院共受理侵犯公民个人信息罪审查逮捕案件19件20人，起诉案件34件44人。

发布会指出，此类案件主要呈现以下特点：（1）案件总体数量下降但出现新犯罪方法。随着对侵犯个人信息类犯罪打击力度的不断加大和对个人信息数据安全的宣传力度不断提升，杨浦区此类案件的总体数量近年来呈明显下降趋势，但是犯罪方法更加新颖，犯罪分子充分利用了互联网、区块链、人工智能等技术，通过买卖、交换、利用职务便利获取、非法下载、拷贝窃取等多种手段非法获取公民个人信息，再利用门户网站、社区论坛、聊天APP、网络邮箱等途径买卖公民个人信息；（2）个案涉及信息数量较多且呈现针对性。大部分案件涉及公民个人信息的数量超过1万条，个别案件侵犯个人信息数量惊人。除了常见的身份证号码、手机号、微信号、QQ号、住址等信息外，还包括职务信息、车辆信息、理财信息等，甚至有些是特定身份群体信息，如某行业工作人员的住址、联系方式、工作岗位等信息；（3）购买群体涉及行业多非法牟利速度快。不法分子获得公民个人信息后，向多人重复提供或售卖，谋取丰厚的利益。购买者多从事

中介、推销、保险、理财等行业，甚至有的利用公民个人信息进行不法活动，这些人员利用获取的公民个人信息，拓宽业务渠道和客源，再谋取更多的利益。更有犯罪分子之间通过互相贩卖、交换等手段不断扩充信息“数据库”，从而在短时间内获利数十万元。

发布会还对犯罪原因展开分析，认为是犯罪手段隐蔽侦查困难、企业行业监管存在漏洞以及涉案人员法律意识不强。对此，聚焦人民群众关切的个人信息保护领域，杨浦区检察院就持续深入加大对公民个人信息安全的司法保护力度，提出以下建议：（1）全方位打击犯罪链条，切实保障信息安全；（2）全流程监管重点行业，合力整治突出问题；（3）全覆盖进行法治宣传，实现从治罪到治理。（来源：杨浦检察）

9. 因通过外网非法获取公民个人信息 1 亿余条，某科技公司员工获刑

10 月 28 日，上海市杨浦区人民检察院通报一起侵犯公民个人信息典型案件。

被告人吴某是某安全科技有限公司员工。2024 年 2 月，被告人吴某通过翻墙软件违规访问境外 Telegram 平台，并在该软件“ling 某”群的“资源共享”内下载含有公民个人信息的文件，储存在其持有的移动硬盘中，同时将上述下载渠道提供给他人。经鉴定，被告人吴某非法获取的公民个人信息共计 1 亿余条。

本案争议点之一在于通过境外网络平台下载公民个人信息的行为是否属于“非法获取”行为。经审查认为，侵犯公民个人信息罪中，对于“非

法”的认定，可以将是否违反国家有关规定作为判断标准。根据《计算机信息网络国际联网管理暂行规定》第六条第二款，任何单位和个人不得自行建立或者使用其他信道进行国际联网。吴某作为网络安全从业者，没有法律授权对个人信息收集、储存或使用的权利，也没有获得相关当事人的许可，其违反国家规定违规访问国际互联网的行为属于“非法获取”。

最终，考虑到吴某尚未将非法获取的信息投入使用，亦未谋取不法利益，同时具有自首情节，给予轻缓处理，法院以侵犯公民个人信息罪判处吴某有期徒刑一年六个月，缓刑一年六个月，并处罚金人民币二千元。（来源：央视网）

10. 北京互联网法院发布一起网络信息“搬运”侵权责任纠纷案件

10 月 18 日，北京互联网法院发布一起网络信息“搬运”侵权责任纠纷案件。

原告小王偶然发现，被告运营的公众号搬运北京某企业拟录用人员名单（在姓名处作出打码处理，但仍可识别出原告姓名，其余院校、专业与学历信息未作打码）与递补人选名单（姓名处作出打码处理，无法识别具体姓名，院校、专业、学历未作打码处理）。小王通知微信公众号运营者其行为已构成侵权。被告虽表示道歉，但双方就道歉和消除影响的方式未达成一致意见，涉案文章并没有修改或删除。

法院审理认为，涉案录用名单截图包含原告姓名、院校、专业与学历，属于个人信息范畴，同时不属于私密信息，应适用个人信息保护相关规定。被告在发布上述个人信息之时，未取得原告同意，但上述个人信息已经公

示程序合法公开，原告未举证证明其在文章发布之前明确拒绝他人处理相关个人信息，也未举证证明该信息侵害原告的重大利益，因此，被告无需就其发布涉案文章的行为承担侵害个人信息权益的民事责任。但同时，原告已于2023年6月向被告明确其姓名信息在涉案文章中清晰可见，并表示被告行为构成侵权，属于明确拒绝被告处理其个人信息。在此情况下，被告未举证证明其对于涉案文章内容进行修改或者删除处理，被告应对此行为承担侵害原告个人信息权益的民事责任。

法院判决被告删除涉案侵权文章，在涉案微信公众号发布致歉声明向原告赔礼道歉，向原告支付维权合理支出。（来源：北京互联网法院）

11. 北京互联网法院通报2023年以来涉个人信息及数据相关案件审理情况

10月30日，北京互联网法院召开涉个人信息及数据相关案件审理情况新闻通报会，通报此类案件的审理情况。自2023年10月至今，北京互联网法院共受理113件涉及个人信息保护的案件，涉及的行业领域较为广泛，以互联网企业为被诉主体的案件最多，涉诉个人信息类型和侵权形态较为多样。

调研发现，数字经济下个人信息权益和其他人格权错综交织，呈现出较为复杂的权益形态，涉诉案件中单独以个人信息权益受到侵害为由起诉的不足40%。另外，个人信息保护案件涉诉信息类型较为丰富，既包含基础个人信息，如手机号、身份证号等，也有因人工智能技术引发的“AI换脸”等新类型侵权案件，还包括多种衍生信息，亦包括大量法律未明确列举的

个人信息，如电子商务平台上形成的用户订单交易详情、客服沟通记录等，反映出个人信息与企业的衍生数据相互交织，呈现复杂化的状态和趋势。

从侵权形态来看，涉及侵害个人信息的知情权与决定权的案件最多，主要侵权形式为未经同意收集、公开、提供个人信息，或超范围收集个人信息。部分案件中反映网络平台运营者未尽到保障用户个人信息安全的法定义务，导致用户个人信息遭受泄露、篡改、冒用。例如，网络平台未经有效审查，导致侵权人盗用他人身份信息用于企业账号认证。

通报会还围绕AI换脸侵犯个人信息权益、个人信息处理的知情同意规则、个人信息处理者安全保障义务、去标识化处理后的个人信息利用、妥善保管网络账号中的个人信息等问题，通报八起涉个人信息及数据典型案例。（来源：北京互联网法院）

境外前沿观察：月度速览十则

导读：10 月，欧盟委员会通过《网络弹性法案》，旨在确保带有数字组件的产品在整个供应链和生命周期中都是安全的。美国白宫发布《推进人工智能在国家安全领域的治理与风险管理框架》，给出禁用人工智能用例、高影响人工智能用例、影响联邦人员的人工智能用例。

安全威胁方面，加拿大网络安全中心发布《2025—2026 年国家网络威胁评估报告》，指出网络犯罪对加拿大个人、组织和政府构成持续威胁，勒索软件是关键基础设施面临的最大网络犯罪威胁。微软公司发布《2024 年微软数码防御报告》，强调国家行为者和网络犯罪分子之间的界限变得模糊，关键基础设施成为现代混合冲突中物理攻击和网络攻击的主要目标。美国最大的受监管水务公共事业公司遭遇网络攻击，使得公司 MyWater 账户系统瘫痪。名为 GoldenJackal 的 APT 黑客组织攻破欧洲政府机构气隙隔离系统，涉及某南亚国家驻白俄罗斯大使馆和某欧洲政府机构。

监管行动方面，俄罗斯针对 VPN 服务的监管力度持续加大，现已封禁近 200 个 VPN。因在回复信息自由请求时泄露全体员工个人信息，英国信息专员办公室对北爱尔兰警察局处以 75 万英镑罚款。因将用户个人数据用于行为分析和定向广告违反 GDPR，爱尔兰数据保护委员会宣布，对职业社交平台 LinkedIn 处以 3.1 亿欧元罚款。

关键词：网络产品安全、人工智能治理、APT 攻击、VPN 监管

1. 欧盟委员会通过《网络弹性法案》，提高数字产品网络安全

10 月 10 日，欧盟委员会通过《网络弹性法案》，旨在确保带有数字组件的产品，例如物联网产品，在整个供应链和生命周期中都是安全的。

法案主要内容包括：（1）对硬件和软件产品的设计、开发、生产和在市场上提供引入欧盟范围内的网络安全要求，以避免欧盟成员国的不同立法导致要求重叠；（2）该法规将适用于直接或间接连接到其他设备或网络的所有产品。对于现有欧盟规则中已有网络安全要求的产品，例如医疗器械、航空商品和汽车，存在一些例外情况；（3）法案将允许消费者在选择和使用包含数字元素的产品时考虑网络安全，使其更容易识别具有适当网络安全特征的硬件和软件产品。（来源：欧盟委员会）

2. 美国白宫发布《推进人工智能在国家安全领域的治理与风险管理框架》

10 月 24 日，美国白宫发布《推进人工智能在国家安全领域的治理与风险管理框架》，旨在落实 2023 年 10 月 30 日发布的第 14110 号行政命令《安全、可靠和值得信赖的人工智能开发与使用》。

框架给出禁用人工智能用例、高影响人工智能用例、影响联邦人员的人工智能用例。其中禁止使用人工智能的情形包括但不限于使用人工智能意图或旨在开展以下活动：（1）仅根据《宪法》和适用的受美国国内法保护的权利（包括言论自由、结社自由和集会自由），对个人的活动进行画

像、锁定或追踪；（2）非法压制言论自由权或获得法律咨询的权利，或对其造成负担；（3）基于个人的种族、民族、性别、性别认同、性取向、残疾状况或宗教信仰，非法将个人置于不利地位；（4）仅依靠生物特征数据推断或确定个人的宗教、民族、种族、性取向、残疾状况、性别认同或政治认同；（5）除出于合法且正当的理由外，从获取的个人数据中检测、测量或推断其情绪状态。

框架细化高风险人工智能用例监管措施。框架通过分类分级，为高风险人工智能使用场景设立更为严格的标准和限制，尤其是对于影响联邦人员和公众的重大决策。同时，强调人类监督重要性，重视人工智能和人类监督的平衡，确保人类在决策过程中仍然拥有关键的控制权，以防止机器完全代替人类决策的风险。此外，框架加强数据管理与透明度，对数据管理进行专门要求，保证模型透明度和公平性，避免模型在实际应用中产生偏差。（来源：美国白宫、网安寻路人、大道简行）

3. 加拿大发布《2025—2026 年国家网络威胁评估报告》

10 月 30 日，加拿大通信安全局下属的加拿大网络安全中心发布《2025—2026 年国家网络威胁评估报告》，以应对日益扩大且复杂的网络威胁。

报告指出，网络犯罪对加拿大个人、组织和政府构成持续威胁，勒索软件是关键基础设施面临的最大网络犯罪威胁。报告分为三部分，涵盖国家对手的网络威胁、网络犯罪威胁以及塑造加拿大网络威胁格局的趋势。报告强调，国家支持的网络威胁行为者可能试图通过破坏性网络攻击和信

息战来影响公众舆论。加拿大政府已将网络安全作为优先事项，提高预算以增强情报和网络运营计划。（来源：加拿大网络安全中心）

4. 微软公司发布《2024 年微软数码防御报告》

10 月 15 日，微软公司发布《2024 年微软数码防御报告》，指出微软客户每天遭受超过 6 亿次网络犯罪和国家支持的攻击，包括勒索软件、网络钓鱼和身份盗窃。报告强调国家行为者和网络犯罪分子之间的界限变得模糊，关键基础设施成为现代混合冲突中物理攻击和网络攻击的主要目标。

报告指出需要更强大的威慑框架，以促进稳定，保护关键基础设施，并避免有害的网络攻击。报告还指出，国家支持的黑客出于经济利益开展活动，招募网络犯罪分子收集情报，并使用网络犯罪社区青睐的工具。

此外，报告还强调国际规范在网络空间行为的重要性，并指出国际规范缺乏对违规行为的处罚规定，导致国家支持和网络犯罪分子的攻击有增无减。报告呼吁政府深化跨利益相关者群体的合作，以识别关键基础设施，并采取行动对最有害的网络攻击施加后果。（来源：微软）

5. 美国水务巨头遭网络攻击，水计费系统瘫痪

10 月 7 日，美国水务公司（American Water Works）发布声明，表示其供水和废水设施未受到上周开始的网络攻击事件影响。该公司向美国证券交易委员会（SEC）提交了相关文件，向公众通报此事件。公司管理层在

其网站上警告，由于为遏制此次攻击采取了措施，客户目前无法访问用于管理个人账户和支付水费的门户网站。

根据公司网站公告，目前公司的MyWater账户系统已瘫痪，所有客户预约的服务将被重新安排。此外，所有账单处理已暂停，直至另行通知。但是，系统恢复上线之前不会产生逾期费用或停止服务。公司的呼叫中心也已无法正常运作。

在向SEC提交的文件和网站公告中，该公司表示于10月3日发现此次攻击。公司已通知执法部门，并聘请网络安全专家协助遏制和缓解这一事件的影响。声明指出，公司已采取并将继续采取措施保护其系统和数据，包括断开或停用部分系统。对于是否正在应对勒索攻击或是否收到勒索要求，该公司未回应相关评论请求。SEC文件中写道，公司“目前认为其供水或废水设施及运营未受到此次事件的负面影响”。但也指出尚无法“预测此次事件的全部影响”。该公司在其网站上表示正通过断开和停用部分系统来保护客户数据并防止进一步的损害。

美国水务公司是美国最大的受监管水务公共事业公司，总部位于新泽西州，为14个州及18个军事设施的约1400万人提供饮用水、废水处理及其他相关服务。（来源：安全内参）

6. 多个政府机密系统遭 APT 组织攻破

10 月 9 日消息，名为 GoldenJackal 的 APT 黑客组织近日成功攻破欧洲政府机构的气隙隔离系统。黑客使用两套自定义工具集窃取大量敏感数据，包括电子邮件、加密密钥、图像、档案以及文件。

根据欧洲安全厂商 ESET 的报告，至少有两波重大事件与此有关。第一波发生在 2019 年 9 月和 2021 年 7 月，目标是某南亚国家驻白俄罗斯大使馆；第二波事件针对的是一个欧洲政府机构，具体发生在 2022 年 5 月至 2024 年 3 月之间。

2023 年 5 月，卡巴斯基发布关于 GoldenJackal 活动的警告，指出该威胁行为者专注于政府和外交机构，主要目的是进行间谍活动。虽然早已知晓 GoldenJackal 通过 USB 闪存驱动器传播自定义工具，例如“JackalWorm”，但此前并没有确认过成功攻破气隙隔离系统的案例。气隙隔离系统常用于关键操作，专门管理机密信息。作为一种安全措施，这类系统与开放网络完全隔离。（来源：安全内参）

7. 俄罗斯封禁近 200 个 VPN 服务，监管持续加码

10 月 25 日消息，俄罗斯近日针对 VPN 服务的监管力度持续加大，现已封禁近 200 个 VPN。Roskomnadzor 公共通信网络监控和管理中心主任在 Spectrum2024 论坛上透露，目前共有 197 个 VPN 服务被屏蔽，此前在 2023 年 10 月的论坛上，该数字为 167 个。

自 2024 年 3 月 1 日起，俄罗斯实施一项禁令，禁止传播任何宣传或推广绕过封锁以访问非法内容的方法的信息。该措施旨在进一步强化对互联网内容的控制。（来源：TECHRADAR）

8. 因泄露全体员工个人信息，英国 ICO 对北爱尔兰警察局处以 75 万英镑罚款

10月3日,英国信息专员办公室(ICO)宣布,已对北爱尔兰警察局(PSNI)处以 75 万英镑罚款，原因是泄露全体员工个人信息。

2023 年 8 月 3 日，PSNI 收到通过名为 WhatDoTheyKnow（WDTK）网站提交的来自同一人的两份信息自由请求，分别要求提供各级别警官人数和各级别员工人数，以及正式、临时或代理的人数信息。这些信息以 Excel 文件形式（内含一个工作表）从 PSNI 的人力资源管理系统（SAP）中下载，其中数据包括姓氏和名字首字母、职务、职级、等级、部门、岗位所在地、合同类型、性别以及 PSNI 服务和员工编号。

分析这些信息以进行披露时，在下载的 Excel 文件中创建了多个其他工作表。完成后，所有屏幕上可见的工作表标签均从 Excel 文件中删除。然而，包含个人详细信息的最初工作表未被注意到，质量检查中也未能发现这一问题。随后，该文件于 8 月 8 日上传至 WDTK 网站。PSNI 内部警员于当日告知此次数据泄露，WDTK 随后隐藏该文件，并将其从网站上删除。

PSNI 表示，将继续推进 ICO 提出的建议以及独立审查小组在 2023 年 12 月发布的调查结果中提出的建议，包括设立副首席警官作为高级信息风

险负责人（SIRO），并建立战略数据委员会和数据交付小组，确保信息安全和数据保护事项得到应有的支持和关注。（来源：英国 ICO）

9. 美国四家上市公司因网络安全信息披露违规被罚 5000 万元

10 月 22 日，美国证券交易委员会（SEC）宣布，因在 2019 年“太阳风”数据泄露事件中做出误导性披露，决定对四家公司处以民事罚款。被处罚的四家公司分别是网络安全公司 Check Point（罚款 99.5 万美元）、Mimecast（罚款 99 万美元），科技公司 Unisys（罚款 400 万美元）和 Avaya（罚款 100 万美元）。

SEC 指出，四家公司各自存在不同的违规之处。Avaya 宣称黑客仅访问了“有限数量”的公司电子邮件，却未提及黑客还访问了其云文件共享环境中的至少 145 个文件。Check Point 在明知漏洞存在的情况下，仅以“泛泛之辞”描述了网络入侵和潜在风险。Mimecast“拒绝披露”被盗代码及公司加密凭证的数量，企图淡化攻击的严重性。Unisys 则将其网络安全事件的风险描述为假设性的，尽管该公司遭遇了与“太阳风”相关的两次攻击。（来源：美国证券交易委员会）

10. 因非法使用用户数据，爱尔兰数据保护委员会对 LinkedIn 处以 3.1 亿欧元罚款

10 月 24 日，爱尔兰数据保护委员会（DPC）宣布，对职业社交平台 LinkedIn Ireland Unlimited Company（LinkedIn）处以 3.1 亿欧元罚款，原因是其将用户个人数据用于行为分析和定向广告的行为违反 GDPR 规定。

DPC 指出，在收到法国一家非营利组织“网络公民权利保护组织”投诉后，于 2018 年 8 月 20 日对涉事数据控制者 LinkedIn 启动调查。经调查，DPC 认定 LinkedIn 存在下列违法行为：（1）未能就第三方数据的处理获得有效同意；（2）虽然声称基于合法利益进行数据处理，但用户有权利对此进行反驳；（3）声称数据处理在合同上具有必要性的说法不成立；（4）未能就数据处理活动向用户提供足够的信息；（5）以用户不完全理解的方式处理数据，违反公平处理原则。

鉴于此，DPC 最终决定向 Linedln 发出以下纠正令：（1）给予谴责；（2）处以总额为 3.1 亿欧元的三项行政罚款；（3）命令 LinkedIn 使其处理符合 GDPR 相关规定。（来源：欧盟数据保护委员会、赛博研究院）

行业前沿观察一：中央第十五巡视组巡视中央网络安全和信息化委员会办公室工作动员会召开、中国将牵头制定抗量子攻击的通信网络安全协议设计指南、13项网络安全国家标准开始实施

导读：根据中央关于巡视工作的统一部署，近日，中央第十五巡视组巡视中央网络安全和信息化委员会办公室工作动员会召开。中央第十五巡视组组长习骅作了动员讲话，对深入学习贯彻习近平总书记关于巡视工作重要讲话精神，扎实开展巡视工作提出要求。

日前从 WAPI 产业联盟获悉，近日在瑞典斯德哥尔摩举行的 ISO/IEC JTC1/SC6（系统间远程通信和信息交换）会议上，中国专家就如何设计抗量子攻击的通信网络安全协议提交提案并获会议一致通过，会议决议成立预备工作项目，由中国专家牵头推进制定协议设计指南。

11 月 1 日起，《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，将为引领网络安全产业高质量发展，增强广大人民群众的获得感、幸福感和安全感提供标准支撑。

关键词：网安周、信息化、数字乡村、网络安全、大湾区、新能源

1. 中央第十五巡视组巡视中央网络安全和信息化委员会办公室工作动员会召开

根据中央关于巡视工作的统一部署，近日，中央第十五巡视组巡视中央网络安全和信息化委员会办公室工作动员会召开。中央第十五巡视组组长习骅作了动员讲话，对深入学习贯彻习近平总书记关于巡视工作重要讲话精神，扎实开展巡视工作提出要求。中央宣传部副部长、中央网信办主任、国家网信办主任庄荣文主持会议并讲话。

中央网信办领导班子成员，中央纪委国家监委驻中央宣传部纪检监察组有关负责同志，中央第十五巡视组、中央巡视办有关同志出席会议；中央网信办退出现职的办领导，中央网信办总工程师、副总工程师，各局各单位主要负责同志，巡视工作联络组成员列席会议。

习骅强调，中央和国家机关是践行“两个维护”的第一方阵，在中国式现代化建设中肩负重要使命，必须在履职担当上走在前、作示范，敢作善为、攻坚克难，主动为党分忧、为国尽责。对中央和国家机关单位开展巡视，充分体现了以习近平同志为核心的党中央的高度重视和关心爱护，是加强党的政治建设、促进履行职责使命、进一步全面深化改革、深入推进党风廉政建设和反腐败斗争的重要举措。中央网信办室务会要切实提高政治站位，深刻领会党中央精神，坚持同题共答，自觉接受监督，坚决完成好党中央交给的巡视任务。

习骅指出，巡视是重要的政治工作，肩负“两个维护”的重大政治责任。中央巡视组将坚持以习近平新时代中国特色社会主义思想为指导，深

入贯彻党的二十大和二十届二中、三中全会精神，认真落实二十届中央纪委三次全会部署，全面贯彻巡视工作方针，精准有效开展政治监督。坚持政治巡视定位，围绕中心、服务大局，聚焦贯彻落实党中央重大决策部署和习近平总书记重要讲话精神，重点检查履行职能责任，落实重大改革部署，防范化解重大风险，纵深推进全面从严治党，加强领导班子、干部人才队伍和基层党组织建设，以及巡视、审计等监督发现问题整改等情况。坚持严的基调，紧盯权力和责任，紧盯“一把手”和领导班子，紧盯群众反映强烈的问题，强化立行立改、边巡边查，着力推动解决突出问题，切实发挥巡视利剑作用，为高质量发展提供有力保障。

庄荣文表示，中央巡视组对中央网信办开展常规巡视，是对中央网信办室务会的全面“政治体检”，充分体现了以习近平同志为核心的党中央对网信工作的高度重视和亲切关怀，对网信干部的严格要求和关心爱护，室务会坚决拥护党中央决定。中央网信办是党的机关、政治机关，全办各级党组织和全体党员干部要深入学习贯彻习近平总书记关于巡视工作的重要论述，充分认识政治巡视的重大意义，要自觉接受巡视监督、服从巡视工作安排、严守纪律规矩，以最坚决的态度、最严明的纪律、最有力的措施、最优良的作风，全力配合中央巡视组做好各项工作，以实际行动践行“两个维护”。以巡促改、以巡促治，深入查摆问题，强化立行立改，统筹做好网信各项工作，不断开创网络强国建设新局面，为全面推进强国建设、民族复兴伟业作出应有贡献。

中央巡视组将在中央网信办工作2个月左右。巡视期间设专门值班电话：010-68337705，每天受理电话的时间为8:00至18:00；专门邮政信箱：北京市西城区A04433号信箱。巡视组受理信访时间截止到2024年12月30日。根据巡视工作条例规定，中央巡视组主要受理反映中央网信办室务会领导班子及其成员、下一级党组织主要负责人和重点岗位人员问题的来信来电来访，重点是关于违反政治纪律、组织纪律、廉洁纪律、群众纪律、工作纪律和生活纪律等方面的举报和反映。其他不属于巡视受理范围的信访问题，将按规定由中央网信办和有关部门认真处理。（来源：中国网信网）

2.中国将牵头制定抗量子攻击的通信网络安全协议设计指南

日前从WAPI产业联盟获悉，近日在瑞典斯德哥尔摩举行的ISO/IEC JTC1/SC6（系统间远程通信和信息交换）会议上，中国专家就如何设计抗量子攻击的通信网络安全协议提交提案并获会议一致通过，会议决议成立预备工作项目，由中国专家牵头推进制定协议设计指南。

量子时代到来后，现有通信网络安全协议变得不再安全。此次我国针对协议设计问题提交提案，将促进全球数据通信系统更平稳地从传统密码算法时代过渡到后量子密码算法时代，避免量子计算机给现有使用传统公钥密钥体系的通信系统带来较大安全威胁。

据介绍，随着量子计算的发展，全球基于传统密码算法的通信协议和系统皆面临颠覆性挑战。虽然可商用量子计算机的发布尚无确切时间表，

但其给全球网络空间带来的挑战已经切实存在，目前已有攻击者开始收集和存储一些重要数据，留待未来使用量子计算机进行破解以获取重要信息。

“为此全球标准组织和各国均在推进行动计划，应对量子计算机带来的安全挑战。本次中国专家提交的国际提案，旨在为全球通信网络向后量子密码迁移提供引导。”WAPI 产业联盟秘书长张璐璐表示。

据悉，WAPI 产业联盟参加了提案论证，西电捷通公司是提案的主要技术贡献者。

西电捷通公司总经理曹军表示，西电捷通公司数年前就开始研究抗量子攻击的网络安全协议，此次正式提交国际提案，是在向后量子时代迁移的历史进程中，中国科技创新力量为构建共享共治的网络空间命运共同体做出的贡献。

记者从 2024 量子科技标准与产业化大会了解到，西电捷通公司等中国企业已经在无线局域网领域开展了抗量子攻击的通信安全协议设计实践，发布了具有抗量子攻击能力的新一代 WAPI 技术。（来源：新华网）

3.13 项网络安全国家标准开始实施

11 月 1 日起，《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，将为引领网络安全产业高质量发展，增强广大人民群众的获得感、幸福感和安全感提供标准支撑。

《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）等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，分别确立了软件供应链安全目标，规定了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，描述了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，规定了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：央视网）

行业前沿观察二：各地协会动态

导读：各地协会活动精彩纷呈，举行大讲堂、技能竞赛等活动。广州网络空间安全协会协同广州市越秀区公安分局、政数局举办等保工作会议暨网安大讲堂活动；西藏自治区互联网协会开展“中华民族一家亲、同心共筑中国梦”主题党日活动；新疆互联网协会成功举办读书会活动；广西网络安全协会协办2024年广西数据跨境流动管理政策宣讲活动；北京网络行业协会承办“AI 赋能关键信息基础设施保护论坛”；佛山市信息协会将承办2024徐州市“移动杯”5G+无人机应用技术职业技能竞赛；揭阳网络空间安全协会成功举办2024年揭西县教育系统网络安全业务培训班；徐州网络公共安防技术协会积极筹备徐州市无人机应用技术职业技能竞赛等。

关键词：大讲堂、信创大赛、技能竞赛、AI、信息安全

1. 广州网络空间安全协会协同广州市越秀区公安分局、政数局举办等保工作会议暨网安大讲堂活动

为贯彻落实习近平总书记关于网络安全的重要指示精神，进一步推进全区信息系统网络安全等级保护工作，有效防范化解网络安全风险，着力提升网络安全保障水平，11 月 8 日，由广州市越秀区公安分局、越秀区政数局主办，广州网络空间安全协会承办的“2024 年越秀区网络安全等级保护工作会议暨网络与信息安全大讲堂”在数字广东公司广东厅成功举办。

会议通过“常见网络攻击类型及其有效防御措施”主题分享、“网络安全保护新诠释”主题分享、网络安全培训、2024 年越秀区网络安全等级保护工作开展情况通报等议程，面向 120 余名来自越秀区辖区内行业相关单位分管信息安全的负责人，开展了网络安全教育宣讲。

此次活动的开展进一步增强了参会负责人的网络安全意识，提升了他们的网络安全防护技能，营造了安全、健康、文明的网络环境。下一步，协会将继续携手各方力量，为维护国家网络安全贡献力量。（来源：广州网络空间安全协会）

2. 西藏自治区互联网协会开展“中华民族一家亲、同心共筑中国梦”主题党日活动

近日，西藏自治区互联网协会党支部在西藏自治区互联网行业党委的指导下，开展了“中华民族一家亲、同心共筑中国梦”联合主题党日活动。

活动的举办，进一步增强了各党支部之间交流，实现共同学习、相互提高。今后，协会党支部将继续发挥好支部的战斗堡垒作用和党员的先锋模范作用，推动全区互联网行业发展，助力构建和谐社会。同时，协会党支部将不断加强自身建设，提高党员素质，确保党的路线方针政策在互联网行业得到全面贯彻和落实。通过开展形式多样、内容丰富的主题党日活动，进一步激发广大党员的积极性和创造性，为建设团结富裕文明和谐美丽的社会主义现代化新西藏贡献力量。（来源：西藏自治区互联网协会）

3. 新疆互联网协会成功举办读书会活动

为了丰富会员单位职工的精神文化生活，加强会员间的交流与沟通，提升文化素养，新疆互联网协会于近期举办了以“从《瓦尔登湖》到《我的阿尔泰》”为主题的读书会活动，来自会员单位的30余人参加了此项活动。此次“读书会”推荐书籍《我的阿勒泰》，围绕此书籍分享阅读心得，深入剖析书中精髓，展开讨论，拓展思维世界。大家结合自己的人生经历谈体会谈感悟，互动交流，畅所欲言，气氛温馨宁静又不乏热烈活跃。读书会活动的举办，不仅为了分享一本好书带来的感动与启迪，更是为了构建一个学习交流、思想碰撞的平台，让智慧的光芒在相互启发中更加耀眼。愿我们都能在书籍的陪伴下，不断成长，不断前行，共同书写属于我们自己的精彩篇章。（来源：新疆互联网协会）

4. 广西网络安全协会协办2024年广西数据跨境流动管理政策宣讲活动

近日，2024年广西数据跨境流动管理政策宣讲活动在南宁成功举办。活动以“建设中国—东盟信息港打造‘数字丝绸之路’”为主旨，由广西壮族自治区党委网信办、自治区商务厅、自治区数据局联合主办，南宁市委网信办、南宁市数据局承办，广西网络安全协会协办。活动主会场设在南宁，区内其他设区市同步设置分会场，近300人参加。宣讲活动上，来自中央网信办及专业领域部门的专家，对我国数据出境安全管理政策进行了总体介绍，并详细解读了《促进和规范数据跨境流动规定》、《个人信息出境标准合同办法》、《数据出境安全评估办法》、数据出境安全管理相关国家标准以及自由贸易试验区数据跨境流动相关政策。参会代表与专家们进行了面对面的交流互动，现场气氛活跃。（来源：广西网络安全协会）

5. 北京网络行业协会承办“AI 赋能关键信息基础设施保护论坛”

近日，“第39次全国计算机安全学术交流会”在西安顺利召开。作为第39次大会的重要分论坛之一,“AI 赋能关键信息基础设施保护论坛”在大会期间顺利举行。该分论坛由中国计算机学会计算机安全专业委员会主办，北京网络行业协会等3家单位/企业承办。论坛由公安部网络安全保卫局原常务副局长、北京网络行业协会会长袁旭阳担任主持人。多位来自关键信息基础设施领域的重要单位和高端专家，以“AI+大模型”等前沿技术

在国内关键信息基础设施保护中的实践与应用为核心议题，共同审视当前安全态势的新变化，深入探讨如何通过技术创新与融合应用为关键信息基础设施筑起更加牢固的安全防线。（来源：北京网络行业协会）

6. 佛山市信息协会将承办 2024 徐州市“移动杯”5G+无人机应用技术职业技能竞赛

10 月 19 日，由佛山市信息协会承办的“2024 年佛山市职工职业技能大赛第四届开发者大赛暨佛山市制造业数字化转型成果发布会”圆满落下帷幕！大赛以“‘AI+’赋能新质生产力”为主题，分为技术创新专题和“AI+”应用专题两个环节，吸引了众多来自佛山市制造业企业的优秀技术人才同台竞技，充分展现了佛山在推动制造业数改智转方面坚实的人才基础和出色的技术创新能力。大赛期间，佛山市制造业数字化转型成果发布会同期举行。会上，佛山市人民政府为 200 多家数字化智能化示范工厂、车间进行授牌，表彰其在佛山制造业数字化转型中的示范引领作用。同时，为优秀数字化服务商、金融机构、产业集群牵引单位等进行颁奖，充分肯定他们近三年在佛山制造业数字化转型中的支撑作用，激励企业接下来积极适配制造业数字化转型需要，汇聚整合资源要素，加强技术创新和产品研发，合力探索创新服务型制造新业态、新模式。（来源：佛山市信息协会）

7. 揭阳网络空间安全协会成功举办2024年揭西县教育系统网络安全业务培训班

10月19日,由揭西县教育局主办,揭阳网络空间安全协会承办的“2024揭西县教育系统网络安全业务培训班”在揭西县第一中学学术报告厅成功举办，各中、小学校校长，教育组组长等约230人参加培训。开班仪式上，县教育局分管领导作动员讲话，强调当前网络安全形势严峻，在教育系统中做好网络安全工作具有重要的意义，希望通过本次培训，大家能够意识到网络安全和保密工作的重要性并运用到实际的工作生活中。培训会上，揭阳市国家保密局有关同志作《新修订的保守国家秘密法解读和案例分享》,揭西县公安局网警大队副大队长谢春青作《增强网络安全防范意识共筑网络安全墙》分享，网络空间安全公益讲师、协会秘书长黄丽佳作《网络安全风险防范措施》分享，分别从法律法规、典型案例、数据分析等方面向大家讲解和强调网络安全和保密工作的重要性，以及相关知识。（来源：揭阳网络空间安全协会）

8. 徐州网络公共安防技术协会积极筹备徐州市无人机应用技术职业技能竞赛

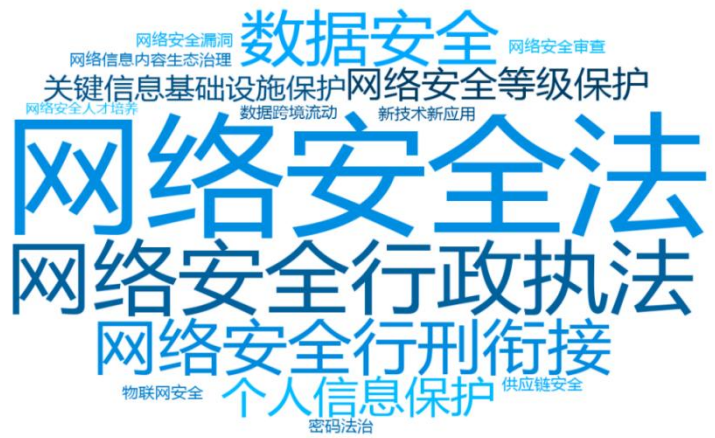
由徐州市公安局、徐州市人力资源和社会保障局、徐州市总工会主办，徐州网络公共安防技术协会无人机分会、中国移动江苏公司徐州分公司、淮海人才集团有限公司承办的2024徐州市“移动杯”5G+无人机应用技术职

业技能竞赛活动紧张筹备中，活动举行时间拟定于 2024 年 11 月 23 日至 24 日，截至目前，共有超过60名考生报名参加此次竞赛，内部推荐9名裁判，已向人社部门提交相关材料，等待审核。协会正在积极组织更多的人员参与报名，以确保竞赛的广泛参与。开将继续加强与各相关部委办局的沟通，以确保竞赛的顺利进行。（来源：徐州网络公共安防技术协会）

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

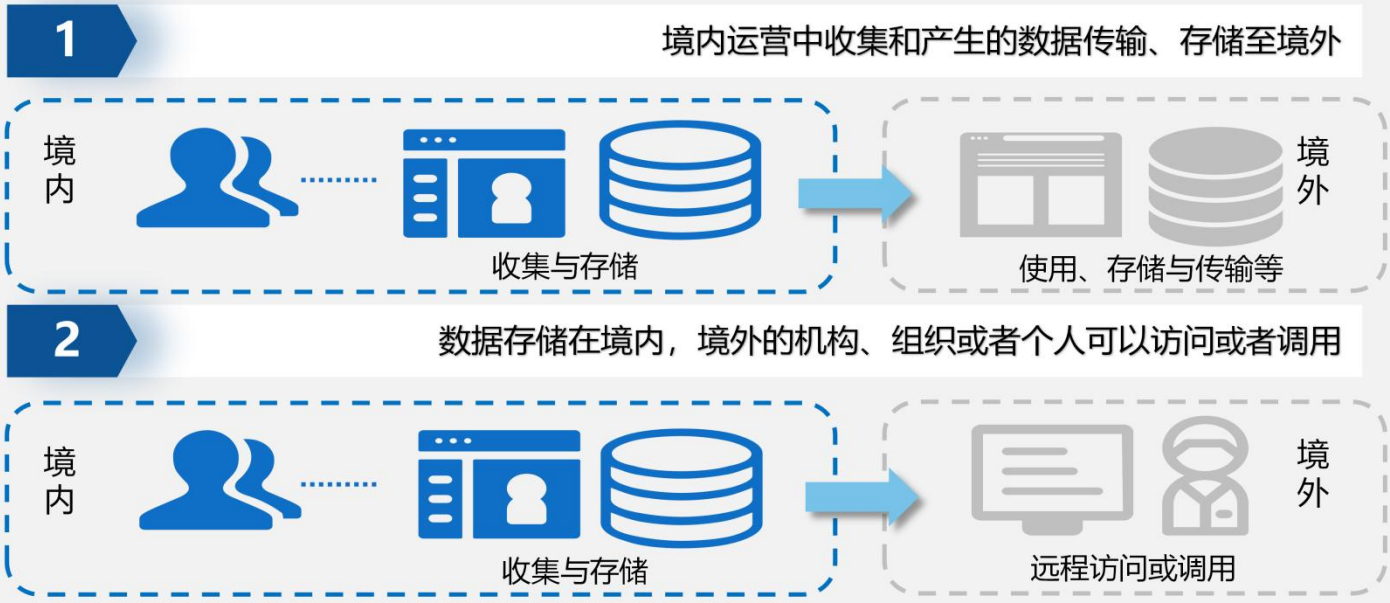
结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

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

……