



# 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9月第9期 (总第14期)

2024年9月12日

**主办单位：**公安部第三研究所网络安全法律研究中心

**联合主办：**北京网络空间安全协会

**牵头组织：**网安联秘书处

**协办单位：**网安联认证中心

**技术支持：**北京关键信息基础设施安全保护中心

广东关键信息基础设施保护中心

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

**指导专家：**袁旭阳 北京网络行业协会 会长  
公安部网络安全保卫局原 副局长

**总编辑：**黄道丽 公安部第三研究所网络安全法律研究中心 主任

**副总编辑：**鲍亮 公安部第三研究所网络安全技术研发中心 副主任

**编委会主任：**黄丽玲 北京网络空间安全协会 理事长

**编委会副主任：（排名不分先后）**

林小博 北京网络空间安全协会 秘书长

朱方园 上海市信息安全行业协会 副秘书长

于永丰 辽宁省信息网络安全协会 秘书长

闫东 辽宁省网络安全保障工作联盟 秘书长

孙甲子 黑龙江省网络安全协会 会长

吴晓文 安徽省计算机信息网络安全协会

刘长久 湖北省网络安全协会 副秘书长

邓庭波 湖南省网络空间安全协会 秘书长

林勇忠 广东省网络空间安全协会 党支部书记

冯伟 广西网络安全协会 秘书长

李春报 海南省网络安全和信息化信协会 常务副理事长

戴勇 贵州省网络安全和信息化协会 副理事长

孙大跃 陕西省信息网络安全协会 会长

卢建宙 甘肃省商用密码行业协会 会长

郑方 甘肃烽侦网络安全研究院 院长

李学锋 新疆维吾尔自治区互联网协会 秘书长

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

**编委会委员：（排名不分先后）**

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

**编辑部主任：梁思雨**

**编辑部：**何治乐 胡文华 王彩玉 王明一 胡柯洋  
李培刚 薛 波 孙翊伦 林 晴 徐瑞雪

**发行部主任：周贵招**

**发行部：**林永健 张 彦 高梓源

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

# 目 录

<b>境内前沿观察一：安全事件</b> .....	<b>1</b>
1. 澜湄合作第九次外长会议发布《澜湄合作框架下加强打击跨境犯罪合作的联合声明》 .....	3
2. 中俄共同发布《中俄总理第二十九次定期会晤联合公报》 .....	4
3. 中国与白俄罗斯共同发布《中华人民共和国政府和白俄罗斯共和国政府联合公报》 .....	5
4. 中欧数据跨境流动交流机制正式建立并举行首次会议 .....	5
5. 中央网信办、公安部就加强网络安全标准化工作进行答复 .....	6
6. 中国互联网络信息中心发布第 54 次《中国互联网络发展状况统计报告》 .....	8
7. 奇安信发布《网络安全威胁 2024 年中报告》 .....	8
<b>境内前沿观察二：政策立法</b> .....	<b>10</b>
（一） 国家层面动向 .....	12
1. 国务院审议通过《网络数据安全条例（草案）》 ..	12
（二） 部委层面动向 .....	12
1. 工信部印发《关于创新信息通信行业管理 优化营商环境的意见》 .....	12
2. 两部门印发《物联网标准体系建设指南（2024 版）》 ..	13
3. 两高发布《关于办理洗钱刑事案件适用法律若干问题的解释》，将通过“虚拟资产”交易明确列为洗钱方式 .....	14

4. 全国网安标委发布六项国家标准征求意见稿 .....	15
5. 全国网安标委发布《网络安全标准实践指南——互联网平台 台停用数据处理安全要求（征求意见稿）》 .....	15
（三） 地方层面动向 .....	16
1. 河南省发展和改革委员会等 20 部门印发《河南省“数据要素 X” 行动实施方案（2024—2026 年）》 .....	16
2. 贵州省公布《贵州省数据流通交易促进条例》 .....	17
3. 安徽省财政厅发布《关于规范和加强行政事业单位数据资 产管理的通知》 .....	18
4. 广州市政务服务和数据管理局发布《广州市公共数据授权 运营管理暂行办法（征求公众意见稿）》 .....	19
5. 北京市市场监督管理局发布《北京市直播带货合规指引》 .....	20
6. 北京市三部门印发《中国（北京）自由贸易试验区数据出 境负面清单管理办法（试行）》《中国（北京）自由贸易试验区 数据出境管理清单（负面清单）（2024 版）》 .....	21
7. 北京市三部门印发《北京市数据跨境流动便利化服务管理 若干措施》 .....	22
8. 上海市浦东新区数据局发布《浦东新区公共数据授权运营 管理若干规定（草案）》 .....	23
<b>境内前沿观察三：治理实践 .....</b>	<b>25</b>
（一） 公安机关治理实践 .....	27

1. 公安部公布 4 起打击整治涉体育领域“饭圈”违法犯罪典型案	27
2. 307 名在缅北佤邦地区实施跨境电信网络诈骗的犯罪嫌疑人被移交我方	28
3. 上海警方纵深推进打击整治网络谣言专项行动，查处网络谣言 1000 余起，关停违法账号 3.5 万个	29
4. 因不履行个人信息保护义务，甘肃酒泉一加油站被处罚	30
5. 甘肃酒泉网安部门查处一起擅自改变计算机信息网络数据案	31
6. 江西省公安部门发布“夏季行动”典型执法案例	31
7. 因信息系统存在弱口令漏洞，广西某高校被公安机关处罚	33
8. “浏览境外色情网站被网警罚款”？警方回应	34
9. 山东东营警方打掉多个“网络水军”团伙，涉及 2.3 万余个违法违规账号	34
10. 江西赣州警方破获一起贩卖个人微信账号侵犯公民个人信息案	35
11. 山东淄博警方侦破一起重大侵犯公民个人信息案，抓获犯罪嫌疑人 17 人	36
12. 福建福州警方破获“黑客”盗窃网游虚拟物品案	37
13. 河南新乡警方摧毁特大“网络水军”犯罪团伙，涉案金额达 5000 万元	38

14. 江西鹰潭警方破获一起制售游戏外挂案，3 人被刑拘..	39
(二) 网信部门治理实践 .....	40
1. 国家互联网信息办公室发布第七批深度合成服务算法备案信息 .....	40
2. 上海属地多平台集中整治体育“饭圈”，6000 多个违规账号被处置 .....	41
3. 广东深入开展“清朗”系列专项行动，推动网络生态治理取得积极成效 .....	41
4. 浙江网信通报 8 月执法处置情况，开展行政检查、行政指导 67 次 .....	43
5. 6 家咖啡企业依然存在违规采集消费者个人信息问题，上海网信办会同市场监管部门进行严肃约谈 .....	44
6. 重庆市网信办联合多部门约谈重庆汇才优聘科技有限公司负责人 .....	44
(三) 通信管理部门治理实践 .....	45
1. 工信部、多地通信管理局通报侵害用户权益行为的 APP(SDK) .....	45
2. 海南省通信管理局启动 2024 年信息通信业网络与信息安全中期执法检查 .....	47
3. 江苏省通信管理局启动 2024 年江苏省信息通信行业反诈骗落实情况执法检查暨涉卡涉用户数据安全检查 .....	47

(四) 其他部门治理实践 .....	48
1. 国家安全部发布一起境外间谍情报机关实施的网络安全攻击案件 .....	48
2. 安徽省合肥市发布《合肥市企业数据合规指引（试行）》 .....	49
3. 河南省商丘市组织开展未成年人网络保护专项执法行动 .....	50
4. 江西省高级人民法院发布一起个人信息保护典型案例 ... ..	51
5. 因数据安全管理的粗放等问题，交银信托公司被罚款 120 万元 .....	52
6. 北京市朝阳区法院审理一起非法获取公民个人信息案，涉及上亿条信息记录 .....	53
7. 杭州中级人民法院一审宣判首例涉数据产品商业秘密保护行政诉讼案件 .....	54
<b>境外前沿观察：月度速览十则 .....</b>	<b>56</b>
1. 联合国网络犯罪问题特设委员会通过《联合国打击网络犯罪公约》 .....	57
2. 俄罗斯国家杜马拟对使用深度伪造技术犯罪确立刑事责任 ... ..	58
3. 美国两部门发布《按需求安全指南：软件客户如何推动安全的技术生态系统》 .....	58
4. 新加坡 CSA：2023 年网络钓鱼、基础设施受感染和网站篡改事件有所下降，但绝对数字仍然很高 .....	59

5. 美国 CISA 披露 AVEVA、Ocean Data 和 Rockwell 自动化关键基础设施设备安全漏洞.....	60
6. 美国司法部起诉 TikTok 违反儿童隐私保护法.....	60
7. 美国国民公共数据公司面临数据泄露诉讼, 近 30 亿人隐私或遭暴露.....	61
8. 因违反政府合同规定的网络安全要求, 美国政府对佐治亚理工学院及其附属机构提起诉讼.....	62
9. 因违规跨境传输司机个人数据, 荷兰数据保护局对 Uber 处以 2.9 亿欧元罚款.....	63
10. 因违反安全措施等义务, 韩国对三家企业处以 2.3152 亿韩元罚款.....	64
<b>行业前沿观察一: “信创适配测试认证”战略合作签约仪式在广州举行; 国家网络安全宣传周开幕式在广州举行; 全国数字乡村建设工作现场推进会召开.....</b>	<b>66</b>
1. 2024 “国家网络安全宣传周”网络安全产品和服务供需洽谈会“信创适配测试认证”战略合作签约仪式在广州举行.....	67
2. 2024 年国家网络安全宣传周开幕式在广东广州举行.....	69
3. 2024 年全国数字乡村建设工作现场推进会在四川绵阳召开... ..	71
4. 国家发展改革委办公厅等发布关于推动车网互动规模化应用试点工作的通知.....	72
<b>行业前沿观察二: 各地协会动态.....</b>	<b>77</b>

1. 广东省网络空间安全协会：筑牢安全数字底座！数字经济高质量发展 的安全技术路径高级研修班顺利举行！ .....	78
2. 北京网络空间安全协会：“2024 信息技术应用创新与安全能力 提升”高研班在京成功举办 .....	79
3. 上海市信息安全行业协会：开展“2024 年度数据安全优秀案例 评选”活动 .....	80
4. 上海市信息网络安全管理协会主办数智创新系列高级研修班 (第二期) .....	81
5. 湖南省网络空间安全协会：赴贵阳调研大数据产业 .....	82
6. 西藏自治区互联网协会：开展“情暖雪域 e 起行”公益活动	82
7. 佛山市信息协会：承办“启沅杯”2024 年佛山市工业互联网安 全技能竞赛 .....	83
8. 南通市信息网络安全协会：“共建网络安全生态暨 2024 年全市 高校网络安全研讨会” .....	84

## 境内前沿观察一：安全事件

导读：8月，我国持续推动信息技术领域国际交流与合作，人工智能、数据跨境流动、开源及软件安全、网络与数据安全、网络犯罪打击等议题成为国际合作的重点关注。中国与俄罗斯共同发布《中俄总理第二十九次定期会晤联合公报》，双方商定将在信息技术和信息安全领域就开源、操作系统、软件和云服务等问题保持经常性沟通；在相互尊重、平等互利基础上积极开展人工智能领域务实合作，加强在全球治理问题上的协调；深化信息安全、数据安全、产业政策和标准、技术研究和人才培养等领域协作。《中华人民共和国政府和白俄罗斯共和国政府联合公报》发布，表明双方将在人工智能、通信、软件、物联网、开放源代码、网络和数据安全等领域开展互利合作，在确保安全的前提下推动低敏数据跨境流动；双方还将联合打击网络犯罪，共同保障两国合作项目及企业人员安全。我国与泰国、柬埔寨、老挝、缅甸、越南共同发布《澜湄合作框架下加强打击跨境犯罪合作的联合声明》，鼓励成员国将打击电信网络诈骗及各种形式的网络赌博犯罪作为优先合作事项。

作为互联网大国，我国的网民规模持续扩大。中国互联网络信息中心发布第54次《中国互联网络发展状况统计报告》，显示截至2024年6月，我国网民规模近11亿人（10.9967亿人），较2023年12月增长742万人。与此同时，我国面临的网络安全威胁形势依旧严峻。奇安信发布《网络安

全威胁 2024 年中报告》, 指出 2024 年上半年, 涉及我国的 APT 事件主要集中在信息技术、政府、科研教育领域, 受害目标集中在广东等地区。

此外, 中央网信办、公安部在新闻发布会上就加强网络安全标准化工作进行答复。中央网信办表示, 截至目前已制定发布 389 项网络安全国家标准, 涵盖关键信息基础设施安全保护、数据安全、产品管理等网络安全重点工作方方面面。公安部表示, 2019 年以来共发布行业标准 791 项, 国家标准 88 项, 公安工作高质量发展的标准体系更加健全。下一步, 公安部将围绕维护国家安全, 制修订网络安全治理等标准; 围绕加强公共安全治理, 研制新型犯罪预防打击、人工智能安全治理、公共视频建设运营等领域标准; 围绕新型警务模式建设, 制定数据分类分级等数据安全和数据实战应用标准, 促进形成和提升新质公安战斗力; 完善公安政务服务标准体系, 制修订网络身份认证公共服务等领域标准。

关键词: 跨境网络犯罪打击、人工智能、开源与软件安全、网络安全威胁、网络安全标准化

## 1. 澜湄合作第九次外长会议发布《澜湄合作框架下加强打击跨境犯罪合作的联合声明》

8月16日，澜沧江—湄公河合作（以下简称“澜湄合作”）第九次外长会在泰国清迈举行，并发布《澜湄合作框架下加强打击跨境犯罪合作的联合声明》。澜湄合作由我国、泰国、柬埔寨、老挝、缅甸、越南六国共同组成。

声明强调，当前跨境网赌电诈、毒品贩卖、人口贩运、恐怖主义、网络犯罪、武器走私等跨境犯罪活动的严重性及其带来的威胁持续上升，危害澜湄地区安全稳定和人民安全幸福。

声明提出，各国重申将坚决打击跨境犯罪，确保公共安全、次区域稳定及人民生命和财产安全，赞赏各方为此所付出的持续努力。各国期待在尊重国家主权、国际法及成员国法律框架的基础上密切各层级合作，加强同全球安全倡议等相关倡议的对接，以维护社会稳定、人民生命安全及地区繁荣发展。

声明鼓励成员国应将打击毒品走私、电信网络诈骗及各种形式的网络赌博犯罪作为优先合作事项，鼓励六国执法和安全部门为此密切配合，促进信息共享，加强边境管控。欢迎各方在“平安澜湄”行动和澜湄综合执法安全合作中心框架内开展自愿合作。（来源：中国政府网）

## 2. 中俄共同发布《中俄总理第二十九次定期会晤联合公报》

8月21日，中国与俄罗斯共同发布《中俄总理第二十九次定期会晤联合公报》。

公报提出，双方商定，将利用数字技术和自动驾驶技术创新货运交通运输新模式；深化移动、邮政等信息通信技术交流合作，加强跨境光缆铺设和维护合作，在电信、前沿技术、创新项目、标准化、电信设备测试领域开展互惠合作；扩大信息通信技术领域教育、研发、人才培养方面合作；在信息技术和信息安全领域就开源、操作系统、软件和云服务等问题保持经常性沟通。

公报提出，双方将在相互尊重、平等互利基础上积极开展人工智能领域务实合作，加强在全球治理问题上的协调。支持成立中俄总理定期会晤委员会通信与信息技术合作分委会人工智能工作组，围绕人工智能伦理治理、工业应用领域的经验和最佳实践分享开展合作。双方支持金砖国家就人工智能能力建设、联合研究、全球治理等开展合作，欢迎中方成立“中国—金砖国家人工智能发展与合作中心”，推动加强产业对接、能力建设等合作。

公报提出，双方将深化信息安全、数据安全、产业政策和标准、技术研究和人才培养等领域协作。加强国家治理数字化（电子政府）、公文流转电子化及电子签名跨境互认领域对话。加强中华人民共和国国家互联网信息办公室与俄罗斯联邦通信、信息技术和大众传媒监管署在相关领域的交流。（来源：中国政府网）

### 3. 中国与白俄罗斯共同发布《中华人民共和国政府和白俄罗斯共和国政府联合公报》

8月22日，中国与白俄罗斯两国共同发布《中华人民共和国政府和白俄罗斯共和国政府联合公报》。

公报提出，双方将在信息和通信技术领域开展互利合作，包括人工智能、通信、软件、物联网、开放源代码、网络和数据安全、电子游戏、无线电频率协调、专业教育和行业科学研究工作等领域。为发展两国数字经济，双方将在确保安全的前提下推动低敏数据跨境流动。双方愿加强数字经济政策协调、传统产业数字化转型发展及数字经济新业态新模式培育等领域合作，共同推进绿色低碳发展。双方愿加强数字贸易等领域多层次交流互鉴，深化务实合作。

公报提出，双方将在防务、司法、执法安全领域加强合作，深化包括军事人员培训，联合打击网络犯罪、跨国犯罪以及打击“东伊运”等“三股势力”在内的合作，共同保障两国合作项目及企业人员安全。（来源：中国政府网）

### 4. 中欧数据跨境流动交流机制正式建立并举行首次会议

8月27日，中欧数据跨境流动交流机制第一次会议以视频方式举行，正式宣布建立中欧数据跨境流动交流机制。

会议就双方企业关于数据跨境流动的具体问题以及数据跨境流动监管框架进行坦诚、深入、富有建设性的交流。中欧数据跨境流动交流机制由

中国国家互联网信息办公室和欧盟委员会贸易总司牵头，通过召开会议等方式交流相关政策和实践，促进中欧数据跨境流动。（来源：国家互联网信息办公室）

## 5. 中央网信办、公安部就加强网络安全标准化工作进行答复

7月31日，市场监管总局召开实施公共安全标准化筑底工程专题新闻发布会。

发布会上，就加强网络安全标准化工作方面，中央网信办表示，近年来，中央网信办组织开展网络安全标准化工作，基本构建起统一权威、科学高效的网络安全标准体系和标准化工作机制，截至目前已制定发布389项网络安全国家标准，涵盖关键信息基础设施安全保护、数据安全、产品管理等网络安全重点工作方方面面，为网络强国建设提供了有力有效标准保障。

下一步，中央网信办将从以下四个方面大力推进国家网络安全标准化工作。一是构建适应大网络安全工作格局的标准化工作机制。强化网络安全标准化工作统筹协调和顶层设计，推动各相关部门、机构、企业、专家通过网安标委这个机制和平台，加强技术沟通交流，群策群力、求同存异，形成国家网络安全标准化工作的强大合力；二是体系化推进重点领域标准研制。紧紧围绕国家战略需求、网络安全管理工作和技术产业发展亟需，持续完善关键信息基础设施安全保护、数据安全和个人信息保护、网络产品和服务特别是产品互联互通、人工智能安全等重点领域标准体系，形成

分领域体系化的标准成果；三是强化标准实施应用。以“标准周”模式为载体持续推进标准研制和宣贯实施，多渠道、多层次、多形式开展网络安全标准宣传解读。围绕当前国家网络安全重点工作，针对重点标准做好标准测试验证、宣贯培训、应用实施、试点示范等；四是推进标准化国际交流合作。

公安标准化工作推进方面，公安部表示，2019年以来，共发布行业标准791项，国家标准88项，公安工作高质量发展的标准体系更加健全。针对打击网络犯罪和保护公民个人信息，建立健全网络安全等级保护、互联网交互式服务安全、公共安全视频图像安全等标准体系，构筑网络空间标准防火墙。

下一步，公安部将重点加强以下工作：一是聚焦防范化解各类安全风险隐患，开展重点领域标准建设。围绕维护国家安全，制修订重要基础设施反恐怖防范、网络安全治理、民用爆炸物品管理、生态环境资源犯罪侦查等标准；围绕加强公共安全治理，加快完善社会治安防控标准体系，健全交通安全系列标准，研制新型犯罪预防打击、人工智能安全治理、公共视频建设运营等领域标准；围绕新型警务模式建设，制定数据分类分级等数据安全标准和数据实战应用标准，促进形成和提升新质公安战斗力；二是统筹发展和安全，以标准升级服务经济社会发展。完善公安政务服务标准体系，制修订治安户政管理、道路交通管理、移民出入境管理、网络身份认证公共服务等领域标准；三是突出标准实施监督，夯实行业标准化发展基础。（来源：国家市场监督管理总局）

## 6. 中国互联网络信息中心发布第 54 次《中国互联网络发展状况统计报告》

8 月 29 日，中国互联网络信息中心（CNNIC）发布第 54 次《中国互联网络发展状况统计报告》。报告显示，截至 2024 年 6 月，我国网民规模近 11 亿人（10.9967 亿人），较 2023 年 12 月增长 742 万人，互联网普及率达 78.0%。

报告指出，上半年，我国互联网行业保持良好发展势头，互联网基础资源夯实发展根基，数字消费激发内需潜力，数字应用释放创新活力，更多人群接入互联网，共享数字时代的便捷和红利。（来源：新华网、中国互联网络信息中心）

## 7. 奇安信发布《网络安全威胁 2024 年中报告》

8 月 19 日，奇安信发布《网络安全威胁 2024 年中报告》。报告指出，2024 上半年网络威胁活动呈现出以下特点：攻击者积极挖掘新攻击面并更新技战术，恶意软件的快速迭代和跨平台攻击的增加对防御者提出了新的挑战；随着 AI 技术的发展，AI 不仅成为网络安全人员的重要工具，也带来了新的攻击手段和挑战，如用 AI 生成的误导信息内容和 AI 本身引入的软件漏洞。

报告指出，2024 年上半年，涉及我国的 APT 事件主要集中在信息技术、政府、科研教育领域，受害目标集中在广东等地区。未知威胁组织（UTG）也对新能源、低轨卫星、人工智能等领域构成威胁。

勒索软件方面，全球勒索软件家族数量众多，新型变种频出，采用“双重勒索”模式，利用漏洞、恶意软件等手段进行攻击。2024年上半年全球范围内的勒索软件攻击波及包括中国在内的多个国家，受害者中既有个人用户，也有各种规模的组织机构，政府、医疗、制造、能源等行业屡次遭到勒索攻击团伙染指。

互联网黑产方面，报告指出，不法分子利用网络技术形成黑色产业链，攻击手法多样，目标包括 IT 运维人员、线上考试系统等，目的为获取经济利益。

0day 漏洞利用方面，上半年 0day 漏洞数量达 25 个，攻击焦点从传统三巨头（微软、谷歌、苹果）转向边界设备，且攻击者在尝试新攻击角度。

（来源：奇安信威胁情报中心）

## 境内前沿观察二：政策立法

导读:8月,国务院常务会议审议通过《网络数据安全条例(草案)》。会议指出,要对网络数据实行分类分级保护,明确各类主体责任,落实网络数据安全保障措施。要厘清安全边界,保障数据依法有序自由流动,为促进数字经济高质量发展、推动科技创新和产业创新营造良好环境。

作为落实《网络安全法》《数据安全法》《个人信息保护法》三大立法的一项重要行政法规,条例的制定修改始终是各界关注的重点。自2022年起,条例作为行政法规连续三年写入国务院立法工作计划,《国务院2024年度立法工作计划》再次提到“围绕健全国家安全法治体系,制定《网络数据安全条例》等”。下一步,条例草案经修改后将报请总理签署国务院令公布施行。

工信部印发《关于创新信息通信行业管理 优化营商环境的意见》,提出营商环境既是重要软实力,也是核心竞争力。《意见》从准入环境、竞争环境、监管环境和服务环境四方面提出十二项意见,表示将进一步打造规范透明可预期的监管环境。意见提出将推广行政指导、行政约谈等柔性监管手段,按照合法、科学、审慎的原则,细化信息通信领域“轻微违法不罚”的具体标准,完善配套监管制度,依法给予经营主体容错纠错空间;加快探索大数据、区块链、人工智能等新技术在监管中的应用,推行远程监管、线上监管方式,进一步提升监管效能;强化综合监管,进一步完善

互联网领域综合监管体制机制，积极探索跨地区、跨部门综合执法，推进监管信息共享互认和执法协作，避免多头检查和重复执法。

自数据与土地、劳动力、资本、技术等传统要素并列为生产要素以来，数据要素利用与价值挖掘成为国家和地方制度建设的重点。贵州通过《贵州省数据流通交易促进条例》，明确数据流通交易应当坚持政府引导、市场主导，合法合规、优质供给，鼓励创新、释放价值，保障安全、包容审慎的原则。作为特殊的一类数据，公共数据成为多地促进数据流动的重要抓手。国家数据局有关负责人曾表示“公共数据的特点是数据基础好、管理相对规范，同时经济价值和社会价值高，所以市场和社会都高度期待。”8月，广州市、上海浦东新区在公共数据授权运营管理方面持续探索，分别发布《广州市公共数据授权运营管理暂行办法（征求意见稿）》和《浦东新区公共数据授权运营管理若干规定（草案）》。

数据跨境流动方面，北京市发布《北京市数据跨境流动便利化服务管理若干措施》《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》和《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》，其中，负面清单（2024版）是首个场景化、字段级数据出境负面清单，选择汽车、医药、零售、民航、人工智能5个领域，详细列明23个业务场景和198个具体字段，便于企业准确识别判断。

关键词：网络数据安全条例、优化营商环境、数据流动交易、公共数据授权运营、数据出境负面清单

## **（一）国家层面动向**

### **1. 国务院审议通过《网络数据安全条例（草案）》**

8月30日，国务院总理李强主持召开国务院常务会议，审议通过《网络数据安全条例（草案）》。

会议指出，要对网络数据实行分类分级保护，明确各类主体责任，落实网络数据安全保障措施。要厘清安全边界，保障数据依法有序自由流动，为促进数字经济高质量发展、推动科技创新和产业创新营造良好环境。（来源：中国政府网）

## **（二）部委层面动向**

### **1. 工信部印发《关于创新信息通信行业管理 优化营商环境的意见》**

7月22日，工业和信息化部印发《关于创新信息通信行业管理 优化营商环境的意见》。意见围绕持续优化高效开放统一的准入环境、积极营造健康公平有序的竞争环境、进一步打造规范透明可预期的监管环境、着力构建便捷可靠优质的服务环境四方面提出十二条意见。

其中，进一步打造规范透明可预期的监管环境方面，意见提出：（1）创新包容审慎监管方式。健全以信用为基础的长效监管机制，推动实施事前信用承诺、事中信用分类监管、事后信用修复的行业管理新模式，引导企业自觉合规经营。推广行政指导、行政约谈等柔性监管手段，按照合法、

科学、审慎的原则，细化信息通信领域“轻微违法不罚”的具体标准，完善配套监管制度，依法给予经营主体容错纠错空间；

(2) 构建“以网管网”监管能力。强化技术赋能监管，推进现有技术监管能力迭代升级，建设互联网数据中心等重点电信业务大数据综合监管平台、面向移动互联网应用程序检测及认证公共服务平台，强化业务合规经营情况的线上监测分析、调查取证能力，健全技术监管体系。加快探索大数据、区块链、人工智能等新技术在监管中的应用，推行远程监管、线上监管方式，进一步提升监管效能；

(3) 严格规范行政监管执法。严格落实行政执法三项制度，持续开展专项执法培训，不断完善行政执法程序，优化执法方式，确保执法过程公正公开、执法程序严谨规范。强化综合监管，进一步完善互联网领域综合监管体制机制，积极探索跨地区、跨部门综合执法，推进监管信息共享互认和执法协作，避免多头检查和重复执法。（来源：工信部）

## 2. 两部门印发《物联网标准体系建设指南（2024版）》

7月22日，工业和信息化部、国家标准化管理委员会印发《物联网标准体系建设指南（2024版）》。指南包括建设思路、重点方向等内容，共提出四个重点建设方向：基础标准、技术标准、建设运维标准、应用标准。

基础标准包括术语与分类、架构、标识、测评、安全可信、管理等标准；技术标准包括感知技术、网络与通信技术、数据处理技术、融合技术、射频与电磁兼容技术、边缘计算技术、物联网操作系统、数字孪生技术等标准；建设运维标准包括规划设计、部署实施、运行维护等标准；应用标

准是指结合农业、工业、服务业等产业发展特点，提出面向各行业的物联网应用指南。（来源：工信部）

### 3. 两高发布《关于办理洗钱刑事案件适用法律若干问题的解释》，将通过“虚拟资产”交易明确列为洗钱方式

8月19日，最高人民法院、最高人民检察院联合发布《关于办理洗钱刑事案件适用法律若干问题的解释》，其中将通过“虚拟资产”交易明确列为洗钱方式之一。

据最高法介绍，随着互联网技术的广泛应用，洗钱手法不断翻新升级，虚拟币、游戏币、“跑分平台”、直播打赏等成为新型洗钱载体和方式，对打击洗钱犯罪提出了新的更高的要求。对此，司法解释明确了刑法中“以其他方法掩饰、隐瞒犯罪所得及其收益的来源和性质”的七种具体情形，其中包括通过“虚拟资产”交易、金融资产兑换方式，转移、转换犯罪所得及其收益等。

同时，司法解释明确了“自洗钱”“他洗钱”犯罪的认定标准，以及“他洗钱”犯罪主观认识的审查认定标准。司法解释同时明确，洗钱数额在五百万元以上，且具有多次实施洗钱行为；拒不配合财物追缴，致使赃款赃物无法追缴；造成损失二百五十万元以上；或者造成其他严重后果情形之一的，应当认定为“情节严重”。

最高法刑三庭庭长陈鸿翔表示，人民法院将依法从重从严惩处洗钱犯罪，加大对涉地下钱庄洗钱犯罪、利用虚拟币、游戏币等洗钱犯罪的打击力度。依法惩处“自洗钱”犯罪。加大罚金刑判处和执行力度，依法追缴

洗钱行为人的违法所得，不让任何人从犯罪行为中非法获利。同时，切实贯彻宽严相济的刑事政策，区分情况、区别对待，确保取得最佳的政治效果、社会效果和法律效果。（来源：新华社）

#### 4. 全国网安标委发布六项国家标准征求意见稿

8月，全国网络安全标准化技术委员会共发布六项国家标准征求意见稿，分别是：

- (1) 《网络安全技术 标识密码认证系统密码及其相关安全技术要求》（征求意见稿）；
- (2) 《数据安全技术 数据接口安全风险监测方法》（征求意见稿）；
- (3) 《网络安全技术 安全技术 网络安全 第7部分：网络虚拟化安全》（征求意见稿）；
- (4) 《数据安全技术 二手电子产品信息清除技术要求》（征求意见稿）；
- (5) 《网络安全技术 网络安全试验平台 体系架构》（征求意见稿）；
- (6) 《网络安全技术 网络空间安全图谱要素表示要求》（征求意见稿）。（来源：全国网安标委）

#### 5. 全国网安标委发布《网络安全标准实践指南——互联网平台停用数据处理安全要求（征求意见稿）》

8月7日，全国网络安全标准化技术委员会发布《网络安全标准实践指南——互联网平台停用数据处理安全要求（征求意见稿）》。征求意见稿

提出互联网平台停用数据处理基本要求，规定重要数据处理的要求，适用于指导互联网平台数据处理者开展数据安全保护工作，也可为主管监管部门实施安全监管或安全评估提供参考。

征求意见稿对互联网平台运营者停用数据处理提出 7 项通用要求，包括：（1）应按照国家 and 行业分类分级要求，参照 GB/T43697 区分核心数据、重要数据和一般数据；（2）应参照敏感个人信息国家标准，区分敏感个人信息和一般个人信息；（3）应采取必要措施保障数据安全，切实履行数据安全和个人信息保护职责；（4）自停用之日起停止收集个人信息和重要数据；（5）涉及未成年人个人信息的，应保障未成年人及其监护人对不满十四周岁未成年人个人信息的查阅、复制、更正、补充、删除的权利；（6）应及时处置长期未对外提供服务的 App、小程序等；（7）因停用需要转移数据的，应明确数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。（来源：全国网安标委）

### （三）地方层面动向

#### 1. 河南省发展和改革委员会等 20 部门印发《河南省“数据要素 X”行动实施方案（2024—2026 年）》

7 月 23 日，河南省发展和改革委员会、中共河南省委网络安全和信息化委员会办公室、中共河南省委金融委员会办公室等 20 部门印发《河南省“数据要素 X”行动实施方案（2024—2026 年）》。

方案围绕数据要素 X 工业制造、现代农业、商贸流通、交通运输、科技创新、应急管理 etc 十二个领域部署重点行动，同时要求从强化数据要素供给、优化数据流通环境、加强数据安全保障三方面强化保障支撑。

其中，加强数据安全保障方面，方案要求贯彻落实《数据安全法》《网络安全法》《个人信息保护法》，全面落实数据分类分级保护、数据安全审查、网络安全等级保护、关键信息基础设施安全保护、个人信息保护等制度。面向数据采集、存储、流通、加工处理各环节，开展隐私计算、数据空间等数据安全有关技术研发和服务创新，构建制度、技术相协同的数据安全治理体系。强化个人信息收集、存储、使用、传输各环节的规范管理，重点监测电信、金融等重点行业数据和个人信息安全，深入排查个人信息泄露风险。（责任单位：省委网信办、省工业和信息化厅、省科技厅、省发展改革委）。（来源：河南省发展和改革委员会）

## 2. 贵州省公布《贵州省数据流通交易促进条例》

7月31日，贵州省人大常委会公布《贵州省数据流通交易促进条例》。条例共八章四十条，包括数据交易场所、数据授权使用、数据权益保护、数据流通交易生态培育等内容。

条例明确，数据流通交易应当坚持政府引导、市场主导，合法合规、优质供给，鼓励创新、释放价值，保障安全、包容审慎的原则。依法保护数据流通交易主体在数据流通交易活动中享有的数据资源持有、数据加工使用、数据产品经营等合法权益，以及基于法律规定或者合同约定流转数据相关财产性权益。

条例规定，省人民政府数据主管部门应当会同网信、公安、国家安全等部门定期对数据交易场所履行数据流通交易安全责任、落实数据流通交易安全管理制度和保护技术措施等情况进行检查，发现数据交易场所存在安全风险的，应当提出整改要求并督促落实。

条例指出，数据交易场所应当建立健全信息化系统运行维护制度和应急处置预案。信息化系统应当依法通过网信、公安、国家安全等部门组织的网络安全审查，符合国家信息安全等级保护等相关要求。

条例强调，数据授权运营按照谁授权谁负责、谁运营谁负责、谁使用谁负责的原则确定安全责任。数据授权机构应当严格控制授权范围，数据运营机构应当加强数据安全使用管理，不得违反法律、法规规定或者超出授权范围运营数据，确保数据来源可溯、去向可查、行为留痕、责任可究。

（来源：贵州人大）

### 3. 安徽省财政厅发布《关于规范和加强行政事业单位数据资产管理的通知》

8月1日，安徽省财政厅发布《关于规范和加强行政事业单位数据资产管理的通知》。通知从以下四个方面提出10条要求：健全体制机制，推动数据资产管理协同共治；规范全程管理，有效促进数据资产赋能增值；严格安全监管，确保数据资产全过程安全合规；统筹推进实施，积极探索数据资产管理路径。

其中，严格安全监管，确保数据资产全过程安全合规要求方面，通知提出：（1）防范各类风险。行政事业单位应严格落实数据资产安全管理责

任，把安全贯穿数据资产管理全生命周期，依法依规加强涉密数据资产管理。强化对信息化系统运维机构等相关主体的监督，有效识别和管控数据资产泄露、违规使用等各类潜在安全风险。行政事业单位不得利用数据资产进行担保，新增政府隐性债务。数据资产管理涉及的安全、价值评估等，应按照市场化原则选聘有关社会中介服务机构；（2）建立监督机制。行政事业单位应建立健全数据资产管理内部控制制度，严格落实数据资产管理各项制度，加强全过程日常监督管理。逐步将数据资产管理情况纳入行政事业性国有资产管理情况报告，接受同级人大常委会监督。加强监督检查，确保数据资产安全完整。（来源：安徽省财政厅）

#### 4. 广州市政务服务和数据管理局发布《广州市公共数据授权运营管理暂行办法（征求意见稿）》

8月1日，广州市政务服务和数据管理局发布《广州市公共数据授权运营管理暂行办法（征求意见稿）》。征求意见稿共八章三十八条，包括数据供给、运营管理、安全管理、运营监管与激励机制等内容。

征求意见稿指出，公共数据授权运营，是指市人民政府授权参与本市公共数据运营工作的企事业单位（简称公共数据运营机构）对公共数据进行加工使用，公共数据运营机构为数据商提供安全可信的数据开发利用环境以及数据商开发利用形成公共数据产品和服务并向社会提供使用的行为。数据商，是指提供数据产品开发、发布、承销和数据资产合规化、标准化、增值化的数据处理者。公共数据运营机构与数据商功能分离，公

共数据运营机构不得从事可能影响数据商公平公正准入的活动及应由数据商开展的相关营利性活动。

安全管理方面，征求意见稿规定，市公共数据主管部门组织开展公共数据授权运营的安全监管，公共数据产品和服务需经核查后方可出域，形成运营全过程可记录、可审计、可追溯的管控机制。除从公开途径合法获取或者法律法规授权公开的公共数据外，原始公共数据不得从公共数据运营平台直接导出。不可导出可通过可逆模型或算法还原出原始公共数据的公共数据产品和服务。（来源：广州市政务服务和数据管理局）

## 5. 北京市市场监督管理局发布《北京市直播带货合规指引》

8月8日，北京市市场监督管理局发布《北京市直播带货合规指引》。指引共4章31条，包括直播带货平台经营者合规要求、直播带货从业人员合规要求等。

指引提出，直播带货平台经营者应当积极履行入驻登记核验义务，依法对申请开通商品或者服务推广功能的直播间运营者提供的身份、地址、联系方式、行政许可等信息进行登记，建立登记档案，并积极采取技术措施进行核验。直播带货直播间运营者的上述信息发生变化的，应当及时更新信息，并向平台报备。

指引提出，直播带货直播间运营者、直播带货人员和直播带货服务机构应当坚持正确政治方向、舆论导向和价值取向，不得违反公序良俗或者制造社会舆论等开展商业营销。积极践行社会主义核心价值观，坚持健康格调品位，自觉反对违法失德、流量至上、畸形审美、“饭圈”乱象、拜

金主义、食物浪费、泛娱乐化等不良现象。（来源：北京市市场监督管理局）

## 6. 北京市三部门印发《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》

8月26日，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局三部门印发《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》。

办法规定，负面清单应至少包含以下两方面：（1）需要通过数据出境安全评估的数据清单，主要包括：1. 关键信息基础设施运营者向境外提供个人信息或者重要数据；2. 关键信息基础设施运营者以外的数据处理器向境外提供重要数据，或者向境外提供达到负面清单要求申报数据出境安全评估的个人信息；（2）需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单，主要包括：关键信息基础设施运营者以外的数据处理器向境外提供达到负面清单要求订立个人信息出境标准合同或者通过个人信息保护认证的个人信息。

办法规定，数据处理器在数据出境活动中，应及时备案，各自贸组团应组织专业技术机构就数据实际出境情况与备案材料进行一致性抽验，对于数据处理器在数据出境活动中未严格履行相关承诺，或出现瞒报、虚报、故意造成实际出境数据与备案数据不一致等违规行为的，各自贸组团可责

令其暂停数据出境活动，要求限期整改，整改完成后重新履行负面清单申请、备案程序；情节严重的，终止其数据出境活动，对其采取重点监管措施，并及时向市级管理部门上报有关情况。

负面清单（2024版）是首个场景化、字段级数据出境负面清单，选择汽车、医药、零售、民航、人工智能5个领域，详细列明23个业务场景和198个具体字段，便于企业准确识别判断。（来源：北京市商务局）

## 7. 北京市三部门印发《北京市数据跨境流动便利化服务管理若干措施》

8月26日，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局印发《北京市数据跨境流动便利化服务管理若干措施》。文件围绕畅通数据合规出境通道、细化服务措施、优化监管措施、强化保障措施四个方面提出十八条措施。

优化监管措施方面，文件提出，要强化重要数据出境保护。依据《数据安全法》及相关法律、法规和规定，在北京市数据安全工作协调机制的统筹协调下，重点行业主管部门加快推进数据分类分级管理，指导企业开展重要数据识别、申报工作，构建企业与行业主管部门间重要数据申报反馈通道，加强对重要数据出境安全的保护支撑。

文件强调，要提升数据跨境基础设施监管能力。鼓励引导企业合规使用国际数据传输专线，传输国际贸易、学术合作、跨国生产制造、跨境购物、跨境支付、考试服务等活动中收集和产生的数据，促进数据合规高效跨境流通。网信、工信等部门按照各自职责强化对国际数据传输专线的安

全管理，落实个人信息或者重要数据出境申报要求，加强数据违规跨境传输处置。

文件提出，要实施事前事中事后全链条全领域综合监管。落实国家及行业数据安全要求，加强对数据出境活动的指导监督，建立数据出境合规抽验、出境活动风险研判、安全事件发现通报机制，强化安全风险预警、处置能力建设，提升全过程数据安全治理监管能力。（来源：北京市商务局）

## 8. 上海市浦东新区数据局发布《浦东新区公共数据授权运营管理若干规定（草案）》

8月16日，上海市浦东新区数据局发布《浦东新区公共数据授权运营管理若干规定（草案）》。草案共二十条，涉及职责分工、授权运营模式、运营主体资质要求、数据安全保障等内容。

草案规定，公共数据授权运营主要采取整体授权、领域授权的方式，整体授权由区数据主管部门实施，领域授权由区行业主管部门会同区数据主管部门实施。整体运营主体采取技术措施保障数据安全，向领域运营主体提供基础公共数据产品，并可以在授权运营范围内进行公共数据产品开发。领域运营主体开发符合产业发展、市场需求的数据产品，向社会提供。领域运营主体有能力提供数据产品的，整体运营主体不得以直接或者间接的方式提供。

草案规定，运营主体应当符合以下基本条件和要求：（1）单位及其法定代表人或者负责人无重大违法记录，未被列入失信被执行人名单、重大

税收违法案件当事人名单、严重违法失信企业名单；（2）明确首席数据官、数据安全负责人和管理部门，具备公共数据授权运营内部管理和安全保障制度；（3）具备接入政务外网的环境和条件，具备对公共数据获取、管理和应用的软硬件环境；（4）具有符合网络安全等级保护三级标准的系统开发和运行维护实践经验；（5）法律、法规、规章规定的其他条件。

草案指出，公共数据授权运营实行“谁授权谁监管、谁运营谁负责”安全责任制。区数据主管部门应当建立健全公共数据授权运营全过程安全管理机制，组织制定授权运营安全管理规范和技术标准，实施公共数据授权运营安全监管，监督运营主体落实公共数据开发利用和安全管理责任。运营主体应当按照授权运营安全管理规范、技术标准和授权运营协议，采取必要措施保障公共数据安全，接受区数据主管部门的监督检查，并定期报告运营安全情况。运营主体应当做好应急预案，在发生数据安全事件时启动应急预案并采取相应处置措施。（来源：法治浦东）

## 境内前沿观察三：治理实践

导读：8月，巴黎奥运会期间，公安机关网安部门密切关注涉巴黎奥运会相关动态，切实加强针对性工作措施，高度重视“饭圈”乱象，持续会同有关部门依法严厉打击相关领域违法犯罪行为。公安部公布4起打击整治涉体育领域“饭圈”违法犯罪典型案例，包括两起涉诋毁行为的刑事案件和两起网络暴力行政处罚案件。

7月底至8月，海南省、江苏省通信管理局分别启动执法检查 and 专项行动。其中，海南省通信管理局启动2024年信息通信业网络和信息安全中期执法检查，检查范围涵盖省内基础电信企业、互联网企业、增值电信企业等各类主体，重点检查网络和数据安全管理制度落实情况、技术手段建设运维情况及保护措施的有效性以及用户个人信息的收集、使用和保护等。江苏省通信管理局启动2024年江苏省信息通信行业反诈法落实情况执法检查暨涉卡涉用户数据安全专项检查。检查组将依据《反电信网络诈骗法》各项规定和要求，深入基础电信企业省市公司、省内移动通信转售企业，采取听取工作汇报、查看书面文件、现场业务演示、系统拨测等方式，重点检查各企业“制度机制建设、电信治理、互联网治理、综合措施落实、法律责任落实”等《反电信网络诈骗法》规定及涉卡涉用户数据安全工作情况。

国家安全部发布一起境外间谍情报机关实施的网路攻击案。某反间谍安全防范重点企业的网络设备多次遭受境外木马病毒的网络攻击。国家安

全机关锁定网络攻击来源于境外间谍情报机关，随即指导该企业采取一系列针对性安全防范措施。同时，国家安全机关依法对该企业落实反间谍安全防范措施情况进行检查，就检查中发现的问题组织相关责任人员进行专门培训指导。

关键词：“饭圈”乱象、信息通信业执法检查、《反电信网络诈骗法》、境外网络攻击

## （一）公安机关治理实践

### 1. 公安部公布 4 起打击整治涉体育领域“饭圈”违法犯罪典型案例

8 月 5 日，公安部公布 4 起打击整治涉体育领域“饭圈”违法犯罪典型案例。

案例一：北京公安机关侦办的贺某某涉嫌诋毁案。查明犯罪嫌疑人贺某某（女，29 岁，江苏苏州人）在网络社交平台发布诋毁乒乓球运动员和教练员的信息，造成恶劣社会影响。8 月 6 日，北京公安机关依法对其采取刑事强制措施。

案例二：广东公安机关侦办的王某涉嫌诋毁案。查明犯罪嫌疑人王某（女，38 岁，广东广州人）多次在网络社交平台发布辱骂、诋毁乒乓球运动员和教练员的信息，造成恶劣社会影响。8 月 13 日，广州公安机关依法对其采取刑事强制措施。

案例三：山东、河北公安机关侦办的盖某、徐某某涉嫌网络暴力案。查明盖某（男，23 岁，山东烟台人）于 8 月 3 日晚，编造所谓的《五问 XX》（内容主要为质问巴黎奥运会某项目冠军），徐某某（男，23 岁，河北石家庄人）在网络社交平台公开发布，该文章在网上大量扩散传播，造成不良社会影响。山东、河北公安机关分别对该 2 人予以行政处罚。

案例四：河南公安机关侦办的杨某某涉嫌网络暴力案。查明杨某某（女，18岁，河南焦作人）在网络社交平台公开辱骂体操运动员，造成不良社会影响，河南公安机关依法对其予以行政处罚。（来源：公安部网安局）

## 2. 307名在缅北佤邦地区实施跨境电信网络诈骗的犯罪嫌疑人被移交我方

8月21日消息，为持续深入推进打击缅北涉我电信网络诈骗犯罪专项行动，进一步清剿犯罪窝点、缉捕涉诈人员，公安部近日部署云南省公安机关与缅甸相关地方执法部门开展边境警务执法合作，成功抓获307名实施跨境电信网络诈骗的中国籍犯罪嫌疑人，其中网上在逃人员20名。目前，全部嫌疑人已被移交我方，打击行动取得又一重大战果。

2023年以来，为坚决遏制缅北涉我电信网络诈骗犯罪多发高发态势，公安部持续深化与缅甸执法部门的国际警务执法合作，联合开展了一系列打击行动，累计5万余名中国籍涉诈犯罪嫌疑人被移交我方，缅北涉我电信网络诈骗犯罪形势持续向好。为全面清除缅北电信网络诈骗犯罪，在公安部的指挥部署下，云南省公安机关与缅甸相关地方执法部门开展边境警务执法合作，在缅北佤邦地区成功抓获307名实施跨境电信网络诈骗的中国籍犯罪嫌疑人，其中包括20名网上在逃人员，查扣一大批手机、电脑等作案工具。经查，该团伙藏匿于佤邦，通过搭建虚拟币网络投资平台，诱导受害人在平台“低买高卖”虚拟币的方式实施诈骗。目前，全部犯罪嫌疑人及涉案证据物品已通过云南孟连县孟连口岸顺利移交我方，同时云南

省公安机关对境内9名同案犯罪嫌疑人开展同步收网，案件侦办工作正紧张进行。（来源：公安部）

### 3. 上海警方纵深推进打击整治网络谣言专项行动，查处网络谣言1000余起，关停违法账号3.5万个

8月22日，上海市公安局召开新闻发布会，通报上海警方深入推进打击整治网络谣言专项行动的措施成效和典型案例。

2024年是打击整治网络谣言专项行动年，公安部部署全国公安机关开展为期一年的专项行动，持续加大全链条、全平台、全领域打击力度，营造清朗网络空间。行动以来，上海公安机关坚持打防管控一体推进，持续严厉打击涉灾情、险情、民生等领域网络谣言，深挖彻查幕后“网络水军”，依法打击造谣传谣违法犯罪行为，累计查处网络谣言案件1000余起，打掉“网络水军”团伙42个，清理网络谣言信息35万余条，关停违法账号3.5万余个，行政处罚相关单位60家次，守护了网络空间的清朗有序。

同时，重拳出击，严查快处违法行为方面，上海警方严格落实7\*24小时网络巡查，及时发现查处违法犯罪活动。对于编造不实信息等扰乱社会秩序或可能引发社会危害的谣言线索，多方核实、及时查证并公开辟谣。同时，对造谣引流、刷量控评、有偿删帖等“网络水军”发起集群战役，全力挤压“网络水军”违法犯罪活动空间；源头治理，压实平台主体责任方面，上海警方依法履行网安管理职能，加强互联网安全监督检查，排查网站平台漏洞问题，采取警告、责令整改、罚款等措施查处了一批不履行主体责任和义务的平台，督促指导互联网平台落实网络安全主体责任，健

全网络平台实名制度，规范内容发布的审核标准及流程，坚决整治恶意摆拍、炮制谣言等违法违规行爲；协同共治，促进行业自律意识方面，上海警方积极发动社会各界参与到打击整治网络谣言行动中，共同维护健康清朗的网络舆论环境。今年，警方指导帮助互联网企业提升异常问题发现能力，提前化解处置各类风险隐患，营造法治化营商环境。（来源：上海市公安局）

#### 4. 因不履行个人信息保护义务，甘肃酒泉一加油站被处罚

7月26日，甘肃酒泉网警对一加油站不履行个人信息保护义务的行为依法作出行政处罚，并要求现场整改。

酒泉网警在开展网络安全执法检查过程中，发现酒泉金塔县一加油站对用户个人信息管理不规范，未履行个人信息保护义务，存在个人信息泄露安全隐患。民警在检查中发现，该加油站在工作过程中大量登记公民个人信息共计600余条，包含姓名、身份证号码、电话、家庭住址等，但未对存储公民个人信息的计算机进行安全管理，未制定内部管理制度和操作规程。同时，该加油站还将部分公民个人信息登记成册随意放置在前台，未进行专人管理和保密设置，他人可以随意查阅使用，存在公民个人信息被泄露的严重风险。该加油站涉嫌违反《个人信息保护法》之规定，构成不履行个人信息保护义务。（来源：甘肃网警）

## 5. 甘肃酒泉网安部门查处一起擅自改变计算机信息网络数据案

8月6日消息，甘肃酒泉敦煌公安近日查处一起擅自改变计算机信息网络数据案，违法人员娄某被依法给予警告，并处1000元罚款，非法所得已被全部没收。

敦煌市某检验检测有限公司负责人报案称，该公司使用的气瓶充装质量追溯信息系统未经允许被他人非法入侵登陆，且对该信息系统内车载气瓶检验数据进行删除、修改、增加等操作，请求公安机关查处。接报后，敦煌市公安局迅速开展调查，并第一时间进入该公司开展电子证据数据侦查、取证工作。通过调查，最终锁定违法行为人娄某，并于当日传唤至公安局进行询问。

经审查，娄某如实交代了利用某检验检测有限公司在气瓶充装质量追溯信息系统的账号和密码非法进入系统，将两个气瓶编号录入气瓶充装质量追溯系统中，使气瓶取得加气资质，从中获利500元的违法行为。（来源：甘肃网警）

## 6. 江西省公安部门发布“夏季行动”典型执法案例

8月12日，江西网警发布多起“夏季行动”涉网络安全典型执法案件。

### (1) 严打侵犯公民个人信息行为

案例一：新余市公安局渝水分局网安大队查处1家MCN机构

近日，新余市公安局渝水分局网安大队联合辖区派出所开展互联网企业、场所安全检查时，发现一家MCN机构公司存在违法行为，该公司通过网络购买大量能够直接关联自然人身份信息的自媒体账号用于公司经营，

涉嫌非法获取公民个人信息。目前，该自媒体公司因非法获取公民个人信息，已被渝水公安依法处以行政处罚。

案例二：赣州市信丰县公安局网安大队查处 9 家 MCN 机构

近日，赣州市信丰县公安局网安大队在工作中发现，辖区内有 9 家 MCN 机构存在违法行为。经民警分析发现，上述 9 家 MCN 机构通过非法途径购买大量能够直接关联自然人身份信息的自媒体账号用于公司经营，共计非法获利 30 余万元，涉嫌侵犯公民个人信息。目前，犯罪嫌疑人刘某、陈某等 5 人因涉嫌侵犯公民个人信息罪，已被信丰警方依法采取刑事强制措施。

(2) 严打编造网络谣言违法行为

案例一：新余市分宜县公安局网安大队侦办 1 起发布网络谣言案件

近日，新余市分宜县局网安大队巡查到一条网络谣言线索，发现一抖音网民发布“分宜电厂螺蛳小镇要改名杀猪小镇，1 元的润田矿泉水卖 7 元”的短视频，浏览播放量达 10 余万。后经民警核实，确认短视频所描述内容系谣言。目前，违法行为人刘某因散布谣言扰乱社会秩序，已被分宜县公安局予以罚款 500 元的行政处罚，涉事短视频已被刘某删除且重新发布澄清致歉短视频。

案例二：鹰潭市贵溪市公安局网安大队侦办 1 起网络谣言案件

近期，鹰潭市贵溪市公安局网安大队民警在日常网络巡查中发现一则“鹰潭火车站涨大水”的抖音视频，网民黄某为了博取关注、赚取流量，周顾事实在网上下载涨大水视频，移花接木、随意剪辑，并配上“鹰潭火车站”字样，在抖音短视频平台发布故意编造的虚假信息，严重扰乱公共秩序。目前，黄某因虚构事实扰乱公共秩序被公安机关依法行政拘留五日。

### (3) 严打网络直播领域低俗、违规现象

案例一：上饶市婺源县公安局网安大队依法约谈 1 名网络主播

近日，上饶市婺源县公安局网安大队民警巡查发现辖区内某平台一网络主播在直播过程中存在低俗、违规行为后，迅速联合县委网信办对该网络主播进行依法依规约谈和批评教育，并当场签订《规范网络行为承诺书》，该主播表示已充分认识问题的严重性和社会危害性，承诺今后将严格遵守国家相关法律法规，坚守网络直播的道德底线。

案例二：赣州市兴国县公安局网安大队侦办一起涉嫌制作、贩卖淫秽物品案

近日，赣州兴国县公安局网安大队在日常巡查工作中发现，有人自制淫秽视频和图片在网上收费贩卖，网安大队联合工业园派出所立即开展侦查，成功锁定并抓获嫌疑人李某。截至案发，李某拍摄制作并贩卖，淫秽视频 58 个及图片 207 张，非法获利 12000 余元。目前，犯罪嫌疑人李某，因涉嫌制作、贩卖淫秽物品牟利罪，被警方依法采取刑事强制措施。（来源：江西网警）

## 7. 因信息系统存在弱口令漏洞，广西某高校被公安机关处罚

8 月 21 日消息，因信息系统存在弱口令漏洞，广西某高校近日被公安机关处罚。

广西梧州网警于 2024 年 6 月 12 日在工作中发现，某学校运营的信息系统存在弱口令漏洞的情况，遂前往现场进行网络安全检查及技术检测。经查，该学校涉及安全隐患的信息系统是一款记录学校师生考试成绩信息

的系统，该学校为方便老师进入系统查询，设置了弱密码。进一步检查发现，该学校网络安全制度缺失，无网络安全防护技术措施，无网络安全应急预案，漏洞扫描显示信息系统存在大量高危漏洞，被网络攻击及数据泄露的安全隐患极大。根据相关法律法规，梧州网警对其进行行政处罚，并责令其立即整改。（来源：公安部网安局）

## 8. “浏览境外色情网站被网警罚款”？警方回应

8月24日消息，广东清远英德市公安局民警近日在工作时发现，一网民于2024年8月7日11时14分许，在短视频平台发布一则图文视频。视频内容为一张付款页面截图，显示“2024年8月7日10时36分，扫二维码付款—英德市网警200元，付款方留言‘浏览境外色情网站’”。

英德警方立即介入调查，发现该视频为网民卜某修图编造的虚假信息。经民警普法宣传和教育，网民卜某表示诚恳接受批评，当场删除该视频，并承诺不再编造不实信息吸引关注，做到知法守法，坚决杜绝此类无底线博流量事件再次发生。（来源：红星新闻）

## 9. 山东东营警方打掉多个“网络水军”团伙，涉及2.3万余个违法违规账号

8月5日消息，按照公安部“净网2024”专项行动和打击整治网络谣言专项行动部署要求，山东省东营市公安局近日成功打掉多个“网络水军”犯罪团伙，抓获违法犯罪嫌疑人54名，查获违法违规账号2.3万余个，封堵虚假引流视频、图文120万余条。

今年4月份以来，东营网安部门工作发现，辖区内存在多个利用实名制自媒体账号和AI技术自动生成帖文的方式造谣引流的“网络水军”犯罪团伙。经对大量数据进行分析研判，逐步梳理出位于东营市的10个自媒体公司的法人、直接负责人、财务及相关工作人员的身份和明确的组织架构。

今年4月和6月，东营警方抽调50余名警力，分多组在嫌疑人经常活动的10个地点开展两次集中统一抓捕行动，一举打掉10个利用非法购买的实名自媒体账号实施网络营销、造谣引流、侵犯公民个人信息的“网络水军”犯罪团伙，抓获违法犯罪嫌疑人54名，扣押作案手机、电脑76台（部），查获百家号、今日头条等各类互联网平台实名账号2.3万余个，封堵利用AI技术编辑的虚假引流视频、图文120万余条。

经查，该犯罪团伙通过互联网非法购买实名制的自媒体账号，通过账号群控软件控制该批自媒体账号，利用群控软件的AI功能自动生成网络帖文实施精准网络营销，赚取相关网络平台的流量分成。同时还利用自动生成的帖文为相关网络犯罪行为实施引流和炒作敏感案事件，严重污染网络环境。目前，案件正在进一步侦办中。（来源：山东网警）

## 10. 江西赣州警方破获一起贩卖个人微信账号侵犯公民个人信息案

8月5日消息，江西赣州警方近日成功破获一起通过贩卖个人微信账号侵犯公民个人信息的案件。

江西赣州警方工作中获悉，网民邹某在网上通过贩卖实名认证的微信账号非法获利。随即迅速展开调查并立即组织警力将其成功抓获。经查，

犯罪嫌疑人邹某从网上购买实名认证的微信账号，再将微信账号转售给他人用于违法犯罪活动，非法获利共计1万余元。

经审讯，犯罪嫌疑人邹某对其侵犯公民个人信息的犯罪事实供认不讳。目前，犯罪嫌疑人邹某已被依法刑事拘留，案件正在进一步侦办中。（来源：公安部网安局）

## 11. 山东淄博警方侦破一起重大侵犯公民个人信息案，抓获犯罪嫌疑人17人

8月9日消息，山东省淄博市公安局临淄分局近日侦破一起重大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，抓获犯罪嫌疑人17人，扣押作案电脑18台、手机86部。

临淄公安分局网安大队民警在工作中发现，某网站上显示多条公民个人信息广告及交易截图。民警敏锐认识到，这背后可能是一起违法贩卖公民信息的案件。民警顺藤摸瓜，对线索开展深度分析研判，最终在某平台中发现其背后的“主角”。临淄警方成功固定抓捕犯罪嫌疑人的证据，还原该犯罪链条运营模式，摸清犯罪团伙组织脉络，将涉嫌非法出售公民个人信息的作案团伙成员乔某、刘某、王某、马某、刘某某等5人被抓获归案。随后，民警乘胜追击，网上网下同频发力，经过1个多月的持续奋战，警方组织集中抓捕收网行动，专案组辗转奔赴各地，成功打掉这一以陈某为首的侵犯公民个人信息犯罪团伙，一举抓获犯罪嫌疑人12名。

经审讯，自2019年底以来，该团伙作为贩卖公民个人信息的“中间商”，通过多个聊天软件与卖家及买家取得联系，根据买家需要，从卖家手中购

买公民个人手机号码倒卖给买家从中获利。这些手机号码均源自各网赌平台，买家均为网赌网站幕后老板，购买手机号码就是为了向使用者精准推送赌博网站广告，达到引流的目的。

目前，乔某、陈某等 17 人均因涉嫌侵犯公民个人信息罪被依法采取刑事强制措施。（来源：公安部网安局）

## 12. 福建福州警方破获“黑客”盗窃网游虚拟物品案

8 月 21 日消息，福州市警方近期破获一起“黑客”盗窃网游虚拟物品案。

某游戏运营公司近期密集收到关于账号内虚拟物品被盗的投诉以及国内某第三方虚拟物品交易平台上存在大量低于正常价格出售的游戏装备的举报。接线索后，福州警方迅速开展综合研判，通过缜密侦查，判断这其中藏着一伙利用黑客技术手段侵害某游戏运营公司以及某款游戏玩家的犯罪团伙。该团伙系通过将木马程序植入游戏玩家所使用的电脑，监测游戏玩家客户端与游戏服务器之间交互的数据，操纵玩家的游戏账户将装备出售变现牟利。

2024 年 6 月，福州警方组织警力在福建本省以及广西、四川等地进行统一收网行动，一举抓获以陈某某为首的犯罪嫌疑人 23 名。经审查，该团伙对其利用黑客技术手段针对某款网络游戏账户进行盗窃的犯罪事实供认不讳，目前案件正在进一步侦办中。（来源：公安部网安局）

### 13. 河南新乡警方摧毁特大“网络水军”犯罪团伙，涉案金额达5000万元

8月21日消息，河南新乡警方近期成功摧毁一个拥有大量“网红”“大V”账号的特大“网络水军”犯罪团伙，抓获犯罪嫌疑人276人，涉案金额达5000万元。

新乡网警在网上巡查时发现，多个微博账号异常活跃，频繁发布推广广告，大肆宣扬其团队可以帮助客户大幅提高账号内容的浏览量，提升账号热度，甚至可以根据客户要求上微博热搜榜单。民警判断，微博账号都是实名认证，如果这家公司利用非法手段操控大量微博账号转发、点赞、评论的话，很有可能涉嫌非法经营罪。发现情况异常后，新乡市公安局汇聚网安等力量，迅速成立打击“网络水军”违法犯罪专案组；经缜密侦查，一个以非法盈利为目的、披着文化传媒公司外衣的“网络水军”团伙被抓获。警方在工作室里发现，10台电脑上都安装大量的手机模拟器，每个手机模拟器上都登录微博账号，并且都安装一个名为“千语中控”的软件，可以对微博账号自动进行点赞、评论、转发。据统计，张某工作室每台电脑装有50个手机模拟器，10台电脑就可控制500个微博账号。随着深入调查，警方发现，像这样的“网络刷手”在全国还有很多，仅这家河南某文化传媒有限公司，在全国各地招募的“网络刷手”已达千人。

如此大量的业务，警方判断应有多家公司参与。通过分析涉案公司资金流水，设在厦门、天津的两家网络公司浮出水面。这两家网络公司均掌握大量“大V”账号，这些账号少则几十万粉丝，多则上百万粉丝。警方通

过梳理案件犯罪链条，摸清涉案公司作案手法。例如，某品牌方需要项目推广，这些网络公司会为品牌方提供热搜推广的规划方案，以广告合同的形式签约。签约后，网络公司将任务以固定价格打包给下游的文化传媒公司，下游公司再组织“网络刷手”通过批量转发、点赞、评论将品牌方要求的内容推上热搜。

掌握相关犯罪事实后，警方开展收网行动，先后在河南、福建、天津、上海等地抓获赖某、张某等 276 名犯罪嫌疑人，同时缴获作案手机和电脑若干。经查，该“网络水军”犯罪团伙涉及虚假微博“转赞评”操作达 8 亿次，内容涵盖社会舆论、热点事件、明星形象、广告推广及账号运营等多个领域，严重扰乱网络生态。

目前，警方已采取刑事强制措施 94 人，移送起诉 19 人，打掉“网络水军”公司 6 家，查获自动批量“转评赞”软件 4 个。案件正在进一步办理中。（来源：新华社）

#### 14. 江西鹰潭警方破获一起制售游戏外挂案，3 人被刑拘

8 月 22 日消息，江西省鹰潭市公安局网安部门近期接到某游戏运营方和游戏用户的举报，称有大量玩家使用“全防”游戏外挂，这款外挂软件不仅能让玩家免费获取游戏角色和道具，还能在竞赛中达到“无敌”状态，严重破坏游戏的公平性。

接到线索后，鹰潭网警高度重视，迅速进行深入调查。经查，该犯罪团伙主要由 3 名年轻人组成，三人通过游戏认识后，发挥各自“特长”，共同谋划制作游戏外挂赚点“零花钱”，并通过建立稳定的客户群体和多

个千人规模的QQ群，利用卡网销售的方式，自动分发“永久卡”“周卡”“天卡”等产品牟取利益。

2024年6月，公安机关辗转多地侦查取证，先后将3名主要嫌疑人抓捕归案。经审讯，3名嫌疑人对制售游戏外挂的违法犯罪行为供认不讳。目前，犯罪嫌疑人均已被依法刑事拘留。（来源：公安部网安局）

## （二）网信部门治理实践

### 1. 国家互联网信息办公室发布第七批深度合成服务算法备案信息

8月5日，国家互联网信息办公室发布第七批深度合成服务算法备案信息，共487项。

其中包括：（1）中国司法大数据研究院有限公司备案“中国法研法律服务内容生成算法”，应用于文本生成场景，根据用户输入的文本信息，生成符合用户需求的文本内容；（2）北京抖音信息服务有限公司备案“小荷医疗大模型算法”，应用于文本生成场景，根据用户输入的文本问题，生成符合用户需求的文本内容，实现知识问答、多轮对话、逻辑推理等功能；（3）智己汽车科技有限公司备案“智己多模态AI视觉图像生成式算法”应用于图片生成场景，根据用户输入的图片信息，深度解析用户绘制的涂鸦，捕获形状、线条，生成符合用户需求的图片内容。（来源：网信中国）

## 2. 上海属地多平台集中整治体育“饭圈”，6000多个违规账号被处置

8月7日消息，为加强网上体育“饭圈”问题整治，上海市委网信办近日在中央网信办统一部署下，指导属地重点网站平台主动履行网络信息内容管理主体责任，加强巡查清理力度，防止赛场外噪音杂音滋扰中国运动员正常比赛，努力营造清朗网络空间。

截至8月6日，小红书发布6期治理公告，清理相关违规信息1.9万余条，下线违规话题24个、对“梦里啥都有”“两百万”等749个违规账号进行禁言处置。哔哩哔哩清理跟评、弹幕等违规互动信息58652条，对1639个违规稿件采取管控措施，封禁4553个违规账号。虎扑清理相关违规内容18323条，对946个账号根据违规程度予以阶梯封禁、永久禁言处理。咪咕视频处置违规互动信息77万余条，对“雏\*\*\*雷”“平\*\*\*音”“淘\*夕”等24个违规账号予以禁言处置。（来源：网信上海）

## 3. 广东深入开展“清朗”系列专项行动，推动网络生态治理取得积极成效

8月30日，广东省委网信办公布“清朗”系列专项行动工作成效。今年以来，根据中央网信办统一部署，广东省委网信办扎实开展“优化营商环境—整治涉企侵权信息乱象”“整治‘自媒体’无底线博流量”“打击违法信息外链”“2024年暑期未成年人网络环境整治”“网络直播领域虚假和低俗乱象整治”等“清朗”系列专项行动，腾讯、网易、UC、YY直播、vivo、OPPO、唯品会等广东属地重点网站平台主动作为、多措并举，

依法依规依约从严清理各类有害信息 326.4 万余条，处置违法违规账号 6 万余个，下架违法违规 APP184 款，推动网络生态持续向好。

“清朗·优化营商网络环境—整治涉企侵权信息乱象”专项行动方面，加强网上涉企信息内容管理，重点整治无事实依据凭空抹黑诋毁企业和企业家形象声誉、炮制传播虚假不实信息、敲诈勒索谋取非法利益、干扰企业正常生产经营秩序和恶意炒作涉企公开信息等突出问题，累计清理涉广东企业和企业家虚假不实信息 2.2 万余条，处置违法违规账号 1390 个，下架违法违规 APP32 款。

“清朗·整治‘自媒体’无底线博流量”专项行动方面，进一步加强“自媒体”管理，从严整治自导自演式造假、不择手段蹭炒社会热点、以偏概全设置话题、违背公序良俗制造人设、滥发“新黄色新闻”等突出问题，累计清理违法违规“自媒体”信息 4.9 万余条，处置相关账号 1817 个。

“清朗·打击违法信息外链”专项行动方面，重点聚焦账号、评论、群圈、直播和短视频、生活服务、浏览器和搜索引擎、电商、涉未成年人版块等违法信息外链问题易发多发的八大重点环节，加强违规内容审核拦截管理，推动建设共享违法外链样本库，累计清理违法外链信息 306.4 万余条，处置违法违规账号、群组 3.4 万余个，暂停功能或信息更新 1083 个，下架违法违规 APP66 款，移交问题线索 470 余条。

“清朗·2024 年暑期未成年人网络环境整治”专项行动方面，全面加强未成年人网络保护，集中整治有害内容隐形变异、沙雕动画、摆拍卖惨、网络暴力、隔空猥亵、低俗擦边等网上涉未成年人突出问题，坚决维护未成年人网络合法权益，累计清理涉未成年人有害信息 3.8 万余条，处置违

法违规账号、群组 4800 余个，关闭未成年人违规直播 146 场次，下架违法违规 APP86 款、涉未成年人软色情商品 21 个。

“清朗·网络直播领域虚假和低俗乱象整治”专项行动方面，坚决制止网络直播领域“流量向善”和“劣币驱逐良币”，重点整治编造虚假场景人设无底线带货营销、“伪科普”“伪知识”、传播“软色情”、侵犯他人权益、销售假冒伪劣商品等网络直播领域五类突出问题，强化网络主播行为管理，累计清理相关有害信息 9.1 万余条，处置违法违规用户账号 1.8 万余个、主播账号 4053 个，关闭违规直播 2.9 万场次。（来源：网信广东）

#### 4. 浙江网信通报 8 月执法处置情况，开展行政检查、行政指导 67 次

8 月，浙江网信强化省域网络执法一体化建设，体系化推进、服务型执法、闭环式监管，积极营造清朗网络空间，为优化营商环境提供强有力的支撑、服务和保障。

依法依规约谈“生死狙击”“爱搜”等网站账号 34 个，责令整改“爱吾信息”“甬矽电子”等网站平台 78 家，注销“红枣电影网”“极品教师”等网站备案 39 家，开展行政检查、行政指导 67 次。网信部门及属地重点平台总计受理处置网民举报 4.9 万件，对 10 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）

## 5. 6家咖啡企业依然存在违规采集消费者个人信息问题，上海网信办会同市场监管部门进行严肃约谈

8月7日消息，经上海市网信办近期复核巡查发现，太平洋咖啡、瑞幸咖啡、COSTA COFFEE、M Stand、挪瓦咖啡、一尺花园等6家企业仍然存在问题整改不到位情况，反映出部分企业仍没有真正有效落实《个人信息保护法》相关要求。8月6日下午，上海市网信办会同市市场监管局依法约谈上述咖啡企业负责人。

约谈中，上海市网信办对于6家企业存在隐私政策缺失、不实或不完整，强制或频繁诱导收集精准位置信息，强制或诱导加入会员，未提供关闭定向推送等违法违规问题进行了严肃批评，要求企业务必认真履行个人信息保护义务，不折不扣落实好个人信息处理“最小必要”和“告知—同意”原则，真正做到隐私政策清晰完整、个人信息收集合法合规。市市场监管局要求企业采取有效措施保障消费者合法权益，落实《消费者权益保护法》《消费者权益保护法实施条例》相关要求，履行企业对消费者个人信息保护的主体责任，切实做好守法经营、规范经营。（来源：网信上海）

## 6. 重庆市网信办联合多部门约谈重庆汇才优聘科技有限公司负责人

8月16日消息，重庆市网信办近日联合重庆市人力社保局、大渡口区网信办、大渡口区人力社保局依法对重庆汇才优聘科技有限公司负责人进行约谈。

该公司运营的“重庆招聘网”微信小程序、“重庆招聘网”App、“重庆招聘网”网站、“重庆招聘会”“大渡口招聘”等11个微信公众号，擅自使用县级以上行政区划地理名称误导公众，存在以夸张、虚假信息诱导消费者等违规情形，违反《互联网用户公众账号信息服务管理规定》《网络信息内容生态治理规定》等相关规定。现该公司已按要求修改微信小程序、微信公众号等名称，查删虚假不实信息内容。（来源：网信重庆）

### （三）通信管理部门治理实践

#### 1. 工信部、多地通信管理局通报侵害用户权益行为的 APP（SDK）

##### （1）工信部

8月27日，工信部信息通信管理局通报2024年第7批，总第42批侵害用户权益的APP（SDK）。通报指出，工信部近期组织第三方检测机构进行抽查，共发现21款APP及SDK存在侵害用户权益行为，包括违规收集个人信息，信息窗口“摇一摇”乱跳转，超范围收集个人信息，APP强制、频繁、过度索取权限等。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）上海市通信管理局

8月16日，上海市通信管理局通报2024年第一批侵害用户权益的APP。通报指出，上海市通信管理局近期组织第三方检测机构对上海市移动互联网应用程序进行抽查，共发现26款APP及小程序存在侵害用户权益行为，包括违规收集个人信息、超范围收集个人信息、未合理申请使用权限等。

上述 APP 及小程序应按有关规定在 8 月 23 日前落实整改工作。整改落实不到位的，上海市通信管理局将依法依规组织开展处置工作。

### (3) 浙江省通信管理局

8 月 28 日，浙江省通信管理局通报 2024 年第 7 批侵害用户权益的 APP。通报指出，浙江省通信管理局近期组织第三方检测机构对群众关注的房屋租赁、网上购物等类型 APP 进行检查，发现上述 APP 存在侵害用户权益行为，包括 APP 强制、频繁、过度索取权限、违规收集个人信息。浙江省通信管理局书面要求违规 APP 开发运营者限期整改。截至 8 月 28 日，尚有 11 款 APP 未按要求完成整改。上述 APP 开发运营者必须在 9 月 6 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。

### (4) 山东省通信管理局

8 月 12 日，山东省通信管理局发布 2024 年第 7 批侵害用户权益的 APP。通报指出，山东省通信管理局持续开展 APP 侵害用户权益专项整治工作，常态化组织专业机构对山东省各类 APP 进行合规性检测，对违规 APP 书面要求限期整改。截至 8 月 12 日，有 25 款 APP 存在 APP 强制、频繁、过度索取权限、违规收集个人信息、超范围收集个人信息等问题，被通知限期整改但未按要求完成整改。（来源：工信部、上海市通信管理局、浙江省通信管理局、山东省通信管理局）

## 2. 海南省通信管理局启动 2024 年信息通信业网络与信息安全中期执法检查

7月29日，海南省通信管理局启动2024年信息通信业网络和信息安全管理中期执法检查，旨在进一步加强网络和数据安全管理，保障公民个人信息安全，维护清朗稳定网络空间，不断赋能千行百业新质生产力发展和助力海南自贸港在高质量发展的道路上行稳致远。

本次执法检查的检查范围涵盖省内基础电信企业、互联网企业、增值电信业务企业等各类主体；重点检查网络和数据安全管理制度落实情况、技术手段建设运维情况及保护措施的有效性以及用户个人信息的收集、使用和保护等。

在检查过程中，执法人员将采取现场检查、技术检测、查阅资料、询问相关人员等多种方式，对被检查单位的网络和数据安全状况进行深入细致评估。对发现的问题和隐患，将依法责令相关单位限期整改，并对整改情况进行跟踪复查。对存在严重违法违规行为的单位，将依法予以严肃处理，绝不姑息。（来源：海南省通信管理局）

## 3. 江苏省通信管理局启动 2024 年江苏省信息通信行业反诈法落实情况执法检查暨涉卡涉用户数据安全检查

8月9日，江苏省通信管理局启动2024年江苏省信息通信行业反诈法落实情况执法检查暨涉卡涉用户数据安全检查。

根据工作方案，检查组将依据《反电信网络诈骗法》各项规定和要求，深入基础电信企业省市公司、省内移动通信转售企业，采取听取工作汇报、

查看书面文件、现场业务演示、系统拨测等方式，重点检查各企业“制度机制建设、电信治理、互联网治理、综合措施落实、法律责任落实”等《反电信网络诈骗法》规定及涉卡涉用户数据安全工作落实情况。

江苏省通信管理局高度重视防范治理电信网络诈骗工作，坚持行业违法违规“零容忍”。今年上半年，持续开展数据稽核、“一案双查”和现场督导，针对违反《反电信网络诈骗法》情形，综合运用法律、行政和经济手段加大处罚问责力度，累计对电信企业下发行政指导类文件2个、风险提示函2次、责令改正通知书5次，开展现场调查4次，实施行政约谈6次、行政处罚1次。（来源：江苏省通信管理局）

## （四）其他部门治理实践

### 1. 国家安全部发布一起境外间谍情报机关实施的网络安全攻击案件

8月19日，国家安全部发布一起境外间谍情报机关实施的网络安全攻击案。

某反间谍安全防范重点企业的网络设备多次遭受境外木马病毒的网络攻击。国家安全机关连夜对该企业遭受网络攻击的设备进行取证，对木马病毒进行清除和风险评估。综合分析木马病毒特征、网络攻击手法和境外IP地址等，锁定网络攻击来源于境外间谍情报机关，随即指导该企业采取一系列针对性安全防范措施，包括指导该公司技术人员对系统漏洞进行修复，升级杀毒防护软件，加强网络安全防范措施。

同时，国家安全机关依法对该企业落实反间谍安全防范措施情况进行检查，就检查中发现的问题组织相关责任人员进行专门培训指导，进一步

提升相关人员的保密意识和安全防范意识，确保安全防范措施落地见效，切实降低间谍窃密风险隐患，保障该企业掌握的国家秘密安全。（来源：国家安全部）

## 2. 安徽省合肥市发布《合肥市企业数据合规指引（试行）》

8月1日，安徽省合肥市数据资源管理局、合肥市司法局、合肥市律师协会联合发布《合肥市企业数据合规指引（试行）》。指引共7章90条，包括数据合规管理组织体系、数据合规管理制度体系、数据全生命周期合规、数据合规运行及保障、数据跨境流动合规等。

指引将企业数据合规管理组织体系分为三层，决策层、管理层和执行层。其中，决策层是指由企业主要负责人担任企业数据合规负责人，对数据合规负领导责任；管理层是指企业应当设立专门的数据合规管理部门，或由合规管理、法务、审计、监督等相关部门承担该职能，并配备数据合规专员。数据合规管理部门对数据合规决策层负责。执行层是指企业内部开展数据处理工作的各职能部门负责本部门业务范围内的数据合规工作。

指引提出，企业应当建立监管执法配合机制，受到监管部门调查时应立即通知数据合规负责人、数据合规管理部门负责人和相关职能部门负责人等人员，启动必要的内部调查程序并明确监管调查对接人员，必要时应当暂停相应的数据处理活动。企业应当对监管部门的监管执法予以协助、配合，不得拒绝、阻挠，不得提供虚假材料、信息或隐匿、销毁、转移证据。企业积极配合监管并主动开展合规整改采取措施有效减轻、消除危害后果的，可以向监管部门申请酌情从轻或减轻行政处罚。

指引建议，企业应当加强对合作方的合规管理，明确信息系统开发及运维、数据存储、数据处理等合作方的准入标准和资格审查机制，并通过签订合规协议等形式明确双方的权利和义务，以及合作方的数据处理权限、应采取的安全保护措施等事项。企业应当定期对合作方进行合规检查和审计，并结合风险特征对合作方进行合规分级、分类管控，对不同风险级别的合作方采取相适应的合规管理措施。发现合作方存在严重违法、违规、违约行为或发生重大数据安全事故、丧失数据安全保障能力、故意不履行数据安全保护职责等情形的，应及时终止与其合作。（来源：合肥市数据资源管理局）

### 3. 河南省商丘市组织开展未成年人网络保护专项执法行动

8月14日至15日，为进一步加强未成年人网络权益保护工作，河南省商丘市委网信办联合市公安局、市文化广电和旅游局、市市场监督管理局开展未成年人网络保护专项执法行动，对商丘市部分县区互联网上网服务营业场所、从事MCN业务单位、未成年人智能终端产品销售商家、互联网文化经营单位进行实地检查。

执法人员重点检查互联网上网服务营业场所线上平台是否存在影响未成年人健康成长的网络违法和不良信息，是否允许未成年人进入，是否设置未成年人禁入标志，是否在规定的营业时间以外营业等；电竞酒店是否严格执行未成年人进入的管控措施，是否落实“五必须”“四警示”规定，是否实施网络安全技术措施和图像采集技术措施等；互联网经营服务单位是否涉及未成年人直播，诱导未成年人打赏，诱导未成年人应援集资、投

票打榜、互撕谩骂、刷量控评等不当行为；未成年人智能终端产品是否在出厂前安装未成年人网络保护软件，是否具有预防未成年人沉迷网络、便于监护人履行监护职责等功能。（来源：网信商丘）

#### 4. 江西省高级人民法院发布一起个人信息保护典型案例

8月5日，江西省高级人民法院发布2023年度全省法院贯彻实施民法典十大典型案例，其中有一起涉个人信息保护典型案例：曹某与江西某文化传播公司等个人信息保护纠纷案——未经同意发送商业短信属于侵害个人信息权益。

本案中，被告某创起翼公司系短信息端口10685583的使用单位。2022年10月13日傍晚5:27，被告江西某文化传播公司使用某创起翼公司106855839159999短信息平台，向原告曹某使用的手机号发送一条短信息，内容为“【招联金融】您好！根据综合评估已为您授信一笔168900元！可享受三个月免息，点jowincarnetwork.com领取，退订回T”。原告曹某收到该短信息后，即向中国银保监会投诉被告招联公司。曹某认为某创起翼公司、江西某文化传播公司和某招联公司共同侵害其生活安宁权、个人信息保护权，遂诉至法院，要求三被告赔偿损失并书面道歉。

江西省九江市濂溪区人民法院经审理认为，个人信息的核心特征在于“可识别性”。案涉手机号码为原告实名注册的手机号码，与原告本人特定相关。从该手机号码已识别或可识别出原告本人，故案涉手机号码属于原告的个人信息。被告江西某文化传播公司作为短信平台的运营商，与被告某招联公司之间存在商业合作关系。案涉短信由被告江西某文化传播公

司委托被告某创起翼公司从其掌握的码号端口发出。综合相关因素，在无证据证明短信内容提供者的情况下，法院认定短信平台端口提供者、平台运营商均为个人信息处理者。双方未告知并取得原告的同意即处理其个人信息，侵害原告个人信息权益，应当依法承担连带责任。且二者之间关于权利义务的内部约定，不影响对外侵权责任的承担。故判决被告江西某文化传播公司、被告某创起翼公司以书面形式向原告曹某公开赔礼道歉，并赔偿原告曹某诉讼合理支出 500 元。

法院表示，本案是依法规制商业短信侵害个人信息权益的典型案列。本案判决认定未经接收人同意向其发送商业短信属于侵犯个人信息权的行为。同时，短信服务平台往往经过多次转包，无证据证明短信内容的提供者，法院认定短信平台端口提供者、平台运营商均构成个人信息侵权，被侵权人可向任意一方主张权利，要求侵权行为人停止侵害、排除妨碍、消除影响、恢复名誉、赔礼道歉、赔偿损失等，如果该侵权行为造成严重精神损害的，被侵权人还有权请求精神损害赔偿。（来源：江西法院）

## 5. 因数据安全管理的粗放等问题，交银信托公司被罚款 120 万元

8 月 16 日，国家金融监督管理总局湖北监管局公布一则行政处罚信息，对交银国际信托有限公司（以下简称“交银信托”）处以罚款 120 万元。其中，交银信托的违法违规事实包括数据安全管理的粗放存在风险隐患以及数据治理体系不健全，监管报送数据存在漏报和错报。湖北监管局依据《银行业监督管理法》第二十一条、第四十六条及相关审慎经营规则对交银信托进行处罚。（来源：国家金融监督管理总局）

## 6. 北京市朝阳区法院审理一起非法获取公民个人信息案，涉及上亿条信息记录

8月19日消息，北京市朝阳区人民法院近日审理一起侵犯公民个人信息案件。

2022年4月至8月间，天某某伙同他人通过爬取、交换、购买等方式获取大量公民个人信息后，利用境外聊天软件向他人有偿提供公民信息查询。经鉴定，在起获的被告人天某某的电脑内，共存储上亿条信息记录，其中包含姓名、手机号、证件号以及交易信息，车辆信息，用户密码等多种个人信息，部分信息较为敏感，给不特定公民的人身、财产安全造成极大的风险和隐患。天某某还让张某担任聊天软件客服负责解答客户问题，让陈某某帮助存储、转发部分公民个人信息。

法院认为，被告人天某某、张某、陈某某违反国家有关规定，向他人出售或者提供公民个人信息，情节特别严重，三被告人的行为均已构成侵犯公民个人信息罪，依法均应予惩处。被告人天某某、张某、陈某某均表示认罪认罚，被告人张某、陈某某系从犯，被告人天某某、张某积极退缴违法所得，依法对被告人天某某予以从轻处罚，对被告人张某、陈某某予以减轻处罚。故判决，被告人天某某犯侵犯公民个人信息罪，判处有期徒刑5年，罚金100万元；被告人张某犯侵犯公民个人信息罪，判处有期徒刑1年8个月，缓刑2年，罚金3万元；被告人陈某某犯侵犯公民个人信息罪，判处有期徒刑1年半，缓刑2年，罚金4万元。（来源：朝阳法苑）

## 7. 杭州中级人民法院一审宣判首例涉数据产品商业秘密保护行政诉讼案件

8月29日，杭州市中级人民法院对原告缪某某诉被告杭州市余杭区市场监督管理局、杭州市余杭区人民政府、第三人某软件有限公司行政处罚及行政复议一案进行公开宣判。

涉案“生意参谋”系某软件有限公司开发的数据产品，为平台商家提供经营分析和决策参考等数据服务。商家在订购“生意参谋”数据产品时需签署相关软件服务协议，服务协议中约定了保密条款，商家登录平台主账号或子账号进行实名认证后，方可查看相关数据信息。针对商家违规获取或者使用“生意参谋”数据的行为，某软件有限公司采取扣分、限制或取消数据访问权限等违规处罚措施。

缪某某将其掌握的“生意参谋”子账号提供给案外人杨某某登录使用，供其登录浏览“生意参谋”内商业信息。余杭区市场监督管理局经调查认定缪某某违反保密义务，披露其所掌握的商业秘密，构成侵害商业秘密的行为，遂作出行政处罚决定，责令缪某某停止侵害商业秘密行为，处罚款5万元。上述决定作出后，缪某某向余杭区人民政府申请行政复议，余杭区人民政府维持该决定。缪某某不服上述决定，向杭州中院提起行政诉讼，要求撤销上述行政处罚决定及行政复议决定。

杭州中院审理后认为，涉案“生意参谋”数据产品具备不为公众所知悉、采取相应保密措施、具有商业价值之要件，符合商业秘密构成要件，应作为商业秘密予以保护。缪某某违反保密义务，向他人披露或者帮助他

人获取“生意参谋”数据，应当认定其行为构成对某软件有限公司商业秘密的侵害。余杭区市场监督管理局对缪某某所作的行政处罚决定执法程序合法，认定事实清楚，证据确实充分，适用法律正确，处罚结果并无不当。余杭区人民政府复议程序合法，予以维持的复议决定适用法律正确，处理适当。杭州中院据此判决驳回原告缪某某的诉讼请求。（来源：杭州中院）

## 境外前沿观察：月度速览十则

导读：8月，联合国网络犯罪问题特设委员会全体成员一致通过首个专门针对网络犯罪的国际条约——《联合国打击网络犯罪公约》，为全球范围内打击网络犯罪提供系统性法律框架。公约预计将在秋季提交联合国大会表决。一旦获得40个联合国成员国的批准，该公约将正式生效。

俄罗斯国家杜马拟对使用深度伪造技术犯罪确立刑事责任，旨在打击利用深度伪造技术进行犯罪的行为。美国CISA和联邦调查局发布《按需求安全指南：软件客户如何推动安全的技术生态系统》，通过确保软件制造商从一开始就优先考虑安全技术，帮助组织推动安全的技术生态系统。

新加坡网络安全局发布《2023年新加坡网络形势》报告，指出AI技术被威胁行为者用来增强网络攻击。美国CISA披露多项涉关键基础设施设备安全漏洞，建议相关组织尽快升级受影响的产品版本。

美国政府对佐治亚理工学院及其附属机构提起诉讼，指控这些机构故意未能遵守与美国国防部订立的合同相关的网络安全要求。美国司法部对TikTok及其母公司字节跳动提起诉讼，指控其严重违反《儿童在线隐私保护法》（COPPA）。因违规将欧洲地区司机的个人数据跨境传输至美国，严重违反GDPR，荷兰数据保护局宣布对Uber公司处以2.9亿欧元罚款。

关键词：网络犯罪公约、深度伪造犯罪、软件供应链安全、网络安全形势、数据跨境传输

## 1. 联合国网络犯罪问题特设委员会通过《联合国打击网络犯罪公约》

8月8日，联合国网络犯罪问题特设委员会全体成员一致通过首个专门针对网络犯罪的国际条约——《关于打击为犯罪目的使用信息和通信技术行为的全面国际公约》草案，简称《联合国打击网络犯罪公约》。

公约主要内容包括：（1）确立通用罪名，公约第二章包含15个条文，详细规定与网络犯罪定罪相关的各个方面。其中，第7条至第17条具体描述11类网络犯罪的构成要件行为；（2）确立程序权力，要求缔约国采取必要的立法或其他措施，开展快速保全电子数据、快速保全和部分披露流量数据、提交令、搜查和扣押电子数据等；（3）促进国际合作，合作目的包括刑事犯罪相关侦查、起诉和司法程序以及相关电子证据的收集、获取、保存和分享，合作方式包括引渡、被判刑人员移管等；（4）鼓励制定和实施预防措施，加强执法机构与私营部门合作、开展公众宣传活动、提高刑事司法系统的能力、鼓励服务提供商加强安全、制定受害人援助方案等；（5）开展技术援助和信息交流，鼓励缔约国针对犯罪方法和技术、政策立法、电子证据、国际法规等方面相互提供广泛的技术援助和能力建设，交流相关经验和知识，实施技术转让，同时要特别考虑发展中缔约国的利益和需求；（6）确立实施机制，设立公约缔约国会议，以促进公约的实施和审查工作。（来源：联合国网络犯罪问题特设委员会、CAICT国际治理观察）

## 2. 俄罗斯国家杜马拟对使用深度伪造技术犯罪确立刑事责任

8月9日，俄罗斯国家杜马劳动、社会政策和退伍军人事务委员会主席雅罗斯拉夫·尼洛夫提议调整《刑法》“诽谤”“欺诈”“盗窃”“敲诈勒索”“计算机信息领域的欺诈”和“通过欺骗或滥用信任造成财产损失”等条款，使其适用于使用深度伪造技术从事上述违法行为的情形，将利用深度伪造技术进行的盗窃和诽谤等行为确立为刑事犯罪。

法案指出，计算机技术的发展使得伪造视频和音频材料变得容易，现代技术如神经网络和人工智能让伪造品难以被非专业人士识别。尼洛夫认为人的图像和声音常用于身份识别，但并不总是被视为生物识别数据，建议将其单独分类以应对日益增多的欺骗行为。尽管政府对该法案提出批评，认为需要进一步改进，尼洛夫表示将考虑这些反馈，对法案进行必要的调整后提交国家杜马审议。（来源：security lab）

## 3. 美国两部门发布《按需求安全指南：软件客户如何推动安全的技术生态系统》

8月6日，美国网络安全和基础设施安全局（CISA）和联邦调查局发布《按需求安全指南：软件客户如何推动安全技术生态系统》，通过确保软件制造商从一开始就优先考虑安全技术，帮助组织推动安全技术生态系统。

指南建议在软件采购生命周期的各个阶段融入安全考虑，从采购前评估软件制造商的安全策略，到合同中纳入安全要求，再到采购后的持续安全评估。CISA强调，客户应通过采购决策推动软件制造商签署CISA发布的

《安全设计承诺》和落实“安全设计”，并应在日志管理、第三方依赖性管理和漏洞报告等关键领域保持透明性和及时性。（来源：美国网络安全和基础设施安全局、国际治理观察）

#### 4. 新加坡 CSA：2023 年网络钓鱼、基础设施受感染和网站篡改事件有所下降，但绝对数字仍然很高

7 月 30 日，新加坡网络安全局（CSA）发布《2023 年新加坡网络形势》报告，全面介绍新加坡 2023 年面临的网络安全威胁形势。报告指出，2023 年，作为诈骗和其他恶意网络活动主要途径的网络钓鱼活动数量较 2022 年大幅下降；平均每三天报告一起勒索软件案件，这一频率与 2022 年相似。新加坡受感染的基础设施数量也有所下降。

报告发现，AI 技术越来越多地被威胁行为者用来增强网络攻击。报告强调 AI 崛起是一个值得关注的趋势。AI 迭代和社会应用规模在 2023 年达到前所未有的水平，预计还会进一步增长，恶意行为者也可能从中受益。例如，恶意行为者正在利用 AI 来增强网络攻击的各个方面，包括用于社会工程或侦察。随着数据存储量的持续增大，这种情况可能会增加，这些数据可用于训练 AI 模型以获得更高质量的结果。CSA 对 2023 年向 SingCERT 报告的网络钓鱼电子邮件样本分析发现，大约 13% 的样本包含 AI 辅助/生成的内容。这些 AI 辅助/生成的电子邮件在语法和句子结构上都更好，还具有更好的流程和推理能力。（来源：新加坡网络安全局）

## 5. 美国 CISA 披露 AVEVA、Ocean Data 和 Rockwell 自动化关键基础设施设备安全漏洞

8 月 15 日消息，美国网络安全与基础设施安全局（CISA）发布十项涉及工业控制系统的安全公告，警示 AVEVA、Ocean Data Systems 及 Rockwell Automation 等关键基础设施设备中的多项安全漏洞。这些漏洞包括 AVEVA SuiteLink 服务器的资源分配漏洞（CVE-2024-7113）、Rockwell AADvance Standalone OPC-DA 服务器的输入验证漏洞（CVE-2024-40619），以及 Rockwell ControlLogix5580 设备的拒绝服务漏洞等。

这些漏洞可能导致任意代码执行、敏感数据泄露、拒绝服务等严重后果。CISA 建议相关组织尽快升级受影响的产品版本，以防范潜在威胁，并强调全面可见性和资产管理在多阶段攻击中的重要性。（来源：industrial cyber）

## 6. 美国司法部起诉 TikTok 违反儿童隐私保护法

8 月 2 日，美国司法部宣布已对流行社交媒体平台 TikTok 及其母公司字节跳动提起诉讼，指控其严重违反儿童隐私保护法。

诉讼称，TikTok 未经父母同意收集 13 岁以下儿童的个人信息，违反《儿童在线隐私保护法》（COPPA）。自 2019 年以来，TikTok 还允许儿童在未启用“儿童模式”的情况下创建账户，并未有效实施删除儿童账户的政策和流程。司法部指出，TikTok 暴露大量年轻用户的个人信息，允许他们接触成人内容并与成人用户互动。此外，TikTok 在家长要求删除个人信息时

未遵守规定，为家长设置重复和不必要的障碍且未能准确告知数据收集和使用情况。

诉讼主要内容包括，TikTok 未能：（1）通知父母他们从儿童那里收集的所有个人数据；（2）获得父母同意以收集和使用该数据；（3）限制收集、使用和披露儿童的个人信息；（4）在父母要求或不再需要时删除儿童的个人信息。司法部要求对 TikTok 及字节跳动处以民事处罚，并下达永久禁令，以防止未来违反 COPPA。TikTok 回应称不同意指控，并表示将继续改进保护儿童的措施。（来源：美国司法部）

## 7. 美国国民公共数据公司面临数据泄露诉讼，近 30 亿人隐私或遭暴露

8 月 7 日消息，美国背景调查服务提供商——国民公共数据公司（National Public Data）正面临集体诉讼，指控其数据泄露事件可能影响近 30 亿人。这一诉讼于 2024 年 8 月在佛罗里达州南区联邦地区法院提起，指控该公司因安全漏洞导致 29 亿人的个人信息被泄露，泄露的信息包括全名、地址和社会安全号码（SSN），这些数据被以“USDoD”为别名的攻击者免费发布在暗网。

诉讼称，国民公共数据公司通过一种名为“抓取”的技术，从非公开来源大量收集数据，包括 SSN 和个人地址信息。尽管抓取技术本身并不非法，但该公司采集的数据规模和来源问题引发争议。此前，国民公共数据公司也曾被黑客攻击，数据库曾被以 200 万美元的价格出售。原告要求法

院指示该公司清除所有受影响人员的个人信息，并对未来收集的数据进行加密，同时实施数据分段、数据库扫描、威胁管理程序，并委任第三方进行年度网络安全评估。（来源：cyber express）

## 8. 因违反政府合同规定的网络安全要求，美国政府对佐治亚理工学院及其附属机构提起诉讼

8月22日消息，美国政府近日对佐治亚理工学院及其附属机构佐治亚理工学院研究公司（GTRC）提起诉讼，指控这些机构故意未能遵守与美国国防部（DoD）订立的合同相关的网络安全要求。GTRC是佐治亚理工学院的签约机构，负责执行与政府机构签订的合同。

该诉讼是由克里斯托弗·克雷格和凯尔·科扎根据《虚假申报法》提起的举报人诉讼，两人曾是佐治亚理工学院网络安全合规团队的高级成员。违反《虚假申报法》的被告将被要求承担政府损失三倍的责任，外加适当的处罚。诉讼指出，至少在2020年2月之前，佐治亚理工学院的Astrolavos实验室未能制定和实施国防部网络安全法规所要求的系统安全计划。即使在2020年2月实施系统安全计划，也未能适当地将所有相关的笔记本电脑、台式机和服务器纳入计划的范围。此外，直到2021年12月，Astrolavos实验室未能在其台式机、笔记本电脑、服务器和网络上安装、更新或运行防病毒或反恶意软件工具。佐治亚理工学院批准该实验室拒绝安装防病毒软件，这违反联邦网络安全要求和佐治亚理工学院自己的政策。

此外，DoD 要求承包商提交汇总分数，反映他们对用于存储或访问所涵盖国防信息的承包系统适用网络安全要求的遵守情况。诉讼称，佐治亚理工学院和 GTRC 于 2020 年 12 月向国防部报告的佐治亚理工学院校园总分 98 分是错误的，因为佐治亚理工学院实际上没有校园范围的 IT 系统，且该分数是针对“虚拟”环境的。（来源：美国司法部）

## 9. 因违规跨境传输司机个人数据，荷兰数据保护局对 Uber 处以 2.9 亿欧元罚款

8 月 26 日，荷兰数据保护局宣布，对美国网约车服务运营商 Uber 公司处以 2.9 亿欧元罚款，原因是 Uber 违规将其欧洲地区司机的个人数据跨境传输至美国，严重违反 GDPR。

荷兰数据保护局对 Uber 的调查，起源于 2020 年 6 月法国人权组织(LDH)代表 170 多名法国 Uber 司机向法国数据保护局 (CNIL) 提交的投诉，主张 Uber 将司机个人数据违规跨境传输至美国。随后该投诉被转交至 Uber 欧洲总部所在国家的监管机构—荷兰数据保护局，与 CNIL 共同开展调查。

经调查，荷兰数据保护局发现，Uber 从欧洲司机收集敏感个人数据后将其存储在美国的服务器上。这些敏感数据包括但不限于账户信息、出租车执照信息、位置数据、照片、付款信息、身份证件信息，甚至是司机的犯罪记录和医疗数据等，并且传输这些数据至其位于美国总部的公司时未采取适当的保障措施，如未签署标准合同等。因此，荷兰数据保护局认定，在 2021 年 8 月 6 日至 2023 年 11 月 21 日期间，因违规跨境传输司机个人

数据，对 Uber 进行相应处罚。目前，Uber 已经停止违规行为。（来源：荷兰数据保护局）

## 10. 因违反安全措施等义务，韩国对三家企业处以 2.3152 亿韩元罚款

8 月 28 日，韩国个人信息保护委员会（PIPC）宣布，对韩华大酒店与度假村有限公司、Thingsflow 有限公司、现代汽车有限公司处以 2.3152 亿韩元罚款，原因是这三家运营商提供互联网服务违反韩国《个人信息保护法》下的安全措施义务、同意义务、个人信息泄露举报和通知义务。

韩华大酒店与度假村有限公司更改其在线预订程序，以便在线会员也可以使用优惠券进行住宿预订，但未进行合适的系统开发和事先验证，导致非预订人的预订信息被查看多达 1818 次。因此，PIPC 认定，因该公司在更改登录程序时未对他人个人信息被查看的可能性进行事先验证，违反《个人信息保护法》下的安全措施义务，并决定对其处以 1.8531 亿韩元罚款和 300 万韩元滞纳金。

被 Thingsflow 有限公司合并的 Between Us 有限公司运营情侣社交网络服务平台“Between”，该平台未经法定代理人同意收集了 38633 名未满 14 岁儿童的个人信息，且个人信息处理者没有保存和管理个人信息处理系统的访问记录，亦未在规定时间内 10 天内回应访问个人信息的请求。因此，PIPC 认定，因未经年龄验证或法定监护人同意擅自收集未满 14 岁以下儿童

的个人信息行为违反《个人信息保护法》，决定对 Thingsflow 公司处以 2743 万韩元的罚款和 360 万韩元滞纳金并在 PIPC 官网公布处罚结果和整改令。

现代汽车有限公司在推行新车试驾营销服务时，拒绝向未同意以营销为目的收集个人信息的客户提供试驾服务。此外，该公司未及时对用于客户支持应用程序“My Hyundai”商用软件进行安全补丁，导致将他人的个人信息泄露给用户，并且对个人信息泄露事件存在延迟举报和通知的事实。因此，PIPC 决定对该公司处以 329 万韩元罚款和 900 万韩元滞纳金并在 PIPC 官网上公布处罚结果。（来源：韩国个人信息保护委员会）

## 行业前沿观察一：“信创适配测试认证”战略合作签约仪式在广州举行；国家网络安全宣传周开幕式在广州举行；全国数字乡村建设工作现场推进会召开

导读：9月8日，2024年国家网络安全宣传周开幕式在广东省广州市举行，本届网安周在全国范围内以会议、论坛、竞赛、展览等多种形式展开，强调全民参与，着力创新成果展示，注重发挥粤港澳大湾区的区位优势，推动网络安全宣传辐射全国。

9月9日，2024年全国数字乡村建设工作现场推进会在四川省绵阳市召开，会议强调，数字乡村战略实施以来取得了积极成效，形成了一批典型经验做法，也面临不少困难和挑战。

9月10日，国家发展改革委办公厅等发布关于推动车网互动规模化应用试点工作的通知。其中提到，按照“创新引导、先行先试”的原则，全面推广新能源汽车有序充电，扩大双向充放电（V2G）项目规模，丰富车网互动应用场景，以城市为主体完善规模化、可持续的车网互动政策机制，以V2G项目为主体探索技术先进、模式清晰、可复制推广的商业模式，力争以市场化机制引导车网互动规模化发展。

关键词：网安周、信息化、数字乡村、网络安全、大湾区、新能源

## 1. 2024 “国家网络安全宣传周”网络安全产品和服务供需洽谈会 “信创适配测试认证”战略合作签约仪式在广州举行

9月8日，2024年国家网络安全宣传周开幕式在广东省广州市举行，本届网安周在全国范围内以会议、论坛、竞赛、展览等多种形式展开，强调全民参与，着力创新成果展示，注重发挥粤港澳大湾区的区位优势，推动网络安全宣传辐射全国。9月9日上午，2024“国家网络安全宣传周”网络安全产品和服务供需洽谈会“信创适配测试认证”战略合作签约仪式在广州南沙举行，广东省网络空间安全协会副会长、华南信创适配测试认证中心副主任成珍苑，广东省网络空间安全协会会长助理黄丽佳、广东新兴国家网络安全和信息化发展研究院博士工作站办公室主任吴一丰与10家从事信创服务的机构合作方代表参加签约仪式。

签约现场，广东新兴国家网络安全和信息化发展研究院博士工作站办公室主任吴一丰作了题为《供应链安全与信创适配测试》的演讲，重点解读软件供应链标准的第三方测评相关部分，分享广东省政数局对信息系统的信创要求和相关适配测试要求，介绍华南信创适配测试认证中心以及与本次签约甲方——华南信息安全技术（广东）有限公司之间的关系，为战略合作协议的签订做了预热铺垫。

随后，华南信创适配测试认证中心、华南信息安全技术（广东）有限公司与广东广晟通信技术有限公司、惠州市计算机信息网络安全协会、广东申腾信息技术有限公司、广东比特豹科技有限公司、广东天安信信息技术有限公司、广州东华职业学院产业链合作研究院、网安世纪科技有限公

司广东分公司、深圳市广思德科技有限公司、广东方昱网络有限公司、杭州领信数科信息技术有限公司 10 家公司现场举行“信创适配测试认证”战略合作项目签约仪式，并合影留念。

据介绍，此次签约本着资源共享、优势互补、合作共赢的原则，达成在产品与技术交流、供需对接、人才培养、科研成果转化、信息共享、标准制定六方面的战略合作协议，为建立信息共享平台，推动信创适配、网络安全等相关技术创新和产业升级、培养行业优秀人才奠定坚实基础。

以广东省政务服务数据管理局为主管单位，依托广东省网络空间安全协会、广州华南检验检测中心有限公司，由华南信息安全技术（广东）有限公司牵头，联手生态合作伙伴（网安联认证中心有限公司、麒麟软件有限公司、统信软件技术有限公司、北京人大金仓信息技术股份有限公司、武汉达梦数据库股份有限公司、天津南大通用数据技术股份有限公司、金蝶国际软件集团有限公司、北京东方通科技股份有限公司），打造从省辐射至市/区/县的信创适配中心，为广东省提供优质的信创适配资源及服务支撑。

此次“信创适配测试认证”战略合作项目签约仪式的成功举行，加强了多方力量的紧密合作，促进技术、人才等资源的有效整合，为进一步推动信息技术应用创新工作，加快新技术新产品应用推广，促进新质生产力的形成和发展，推动我国信创产业高质量发展注入新的活力。（来源：广东省网络空间安全协会）

## 2. 2024 年国家网络安全宣传周开幕式在广东广州举行

9月8日，2024年国家网络安全宣传周开幕式在广东省广州市举行。中共中央政治局委员、广东省委书记黄坤明出席开幕式并致辞。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出席开幕式并致辞。广东省委副书记、省长王伟中主持开幕式。

与会嘉宾认为，党的十八大以来，习近平总书记从事关党的长期执政、事关国家长治久安、事关人民群众福祉的战略高度，谋划推动网络强国建设，强化网络安全工作，指引网信事业与党和国家各项事业同步发展，取得历史性成就、发生历史性变革。党的二十届三中全会就加强网络安全体制建设作出专门部署，向网信战线发出新的动员令，必将指引我们在新征程上开启网络安全工作的崭新篇章。我们要深入学习领会习近平总书记关于网络强国的重要思想，全面落实党中央决策部署，全方位推进网络安全建设，为加快建设网络强国作出更大贡献。

与会嘉宾表示，要深入学习贯彻党的二十届三中全会精神，坚持方方面面齐动手，突出体系建设，着力强化关键信息基础设施防护；突出重点防范，着力提高数据安全保护能力水平；突出兴利除弊，着力激发新技术新应用发展活力；突出系统思维，着力夯实国家网络安全工作基础；突出共建共享，着力增强维护网络安全社会共识，构建大网络安全工作格局，全面推进国家网络安全体系和能力现代化。

公安部党委委员、副部长陈思源，香港特别行政区创新科技及工业局局长孙东，澳门特别行政区网络安全委员会秘书、司法警察局局长薛仲明

出席开幕式并发言。中央网信办副主任、国家网信办副主任王京涛，工业和信息化部党组成员、副部长张云明，国家广播电视总局党组成员、副局长杨国瑞，全国妇联副主席、书记处书记冯玲，广东省委、省政府及广州市有关领导，全国总工会、共青团中央有关负责同志，中央宣传部、中央网信办、中央港澳办、中国人民银行有关部门负责同志等出席开幕式。

开幕式上，粤港澳三地有关部门签署了《关于促进粤港澳网络安全领域交流合作备忘录》。开幕式后，与会领导嘉宾还参观了网络安全博览会。

本届网安周以“网络安全为人民，网络安全靠人民”为主题，由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、国家广播电视总局、全国总工会、共青团中央、全国妇联等十部门联合举办。中央和国家机关有关部门负责同志，香港、澳门特别行政区政府代表，广东省及有关省（区、市）有关方面负责同志，专家学者、企业和高校代表、媒体记者等参加开幕式。

网安周期间，还将举行网络安全技术高峰论坛，校园日、电信日等六大主题日活动，网络安全人才招聘专场活动、网络安全创新创业投资专场活动、中国网络安全创新创业大赛总决赛、“羊城杯”粤港澳大湾区网络安全大赛决赛、网络安全进基层等活动。

9月9日至15日，2024年国家网络安全宣传周在全国范围内统一开展。

（来源：中国网信网）

### 3. 2024 年全国数字乡村建设工作现场推进会在四川绵阳召开

9月9日，2024年全国数字乡村建设工作现场推进会在四川省绵阳市召开，中央网信办副主任、国家网信办副主任王崧出席会议并作总结讲话。四川省人大常委会副主任宋朝华出席会议。

会议指出，发展数字乡村是数字时代推进农业农村现代化进程的必由之路，要深入贯彻落实党的二十届三中全会精神和习近平总书记关于网络强国的重要思想，着眼全面建设社会主义现代化国家全局，深刻认识推进数字乡村建设的重要性、必要性、紧迫性，认真学习运用“千万工程”经验，推进数字乡村建设走深走实，加快以信息化培育乡村振兴新动能。

会议强调，数字乡村战略实施以来取得了积极成效，形成了一批典型经验做法，也面临不少困难和挑战。要深化改革创新，推进数字乡村建设再上新台阶，建强乡村数字基础设施和涉农数据平台“两个基础”，着力补齐乡村信息化发展短板；抓住培育乡村新产业新业态和壮大信息化人才队伍“两个关键”，培育发展新质生产力；提升乡村数字治理能力和乡村信息服务能力“两大能力”，推进乡村治理体系和治理能力现代化；强化粮食安全数字化支撑和防止返贫动态监测“两条底线”，增强乡村信息化支撑保障能力；抓好第二批国家数字乡村试点和数字乡村强农惠农富农专项行动“两个行动”，探索数字乡村发展长效机制。要坚持系统观念，正确把握统筹推进与重点突破、智慧城市与数字乡村、有为政府与有效市场、埋头实干与学习借鉴的关系，以钉钉子精神抓好各项任务落实。

会上，山东省委网信办、新疆维吾尔自治区党委网信办，重庆市潼南区、福建省泉州市石狮市以及中国邮政集团有关负责同志进行交流发言；商务部、中国人民银行相关司局负责同志作政策解读；文化和旅游部、四川省分别发布“乡村旅游数字提升行动”“四川数字点亮万村计划”成果；中央网信办、农业农村部、商务部、中国人民银行、全国供销合作总社等部门联合启动“数字乡村强农惠农富农专项行动”；农业农村部市场与信息化司负责同志作有关工作部署。（来源：中国网信网）

#### 4. 国家发展改革委办公厅等发布关于推动车网互动规模化应用试点工作的通知

9月10日，国家发展改革委办公厅等发布关于推动车网互动规模化应用试点工作的通知。其中提到，按照“创新引导、先行先试”的原则，全面推广新能源汽车有序充电，扩大双向充放电（V2G）项目规模，丰富车网互动应用场景，以城市为主体完善规模化、可持续的车网互动政策机制，以V2G项目为主体探索技术先进、模式清晰、可复制推广的商业模式，力争以市场化机制引导车网互动规模化发展。参与试点的地区应全面执行充电峰谷分时电价，力争年度充电电量60%以上集中在低谷时段，其中通过私人桩充电的电量80%以上集中在低谷时段。参与试点的V2G项目放电总功率原则上不低于500千瓦，年度发电量不低于10万千瓦时，西部地区可适当降低。

## 国家发展改革委办公厅等关于推动车网互动

### 规模化应用试点工作的通知

发改办能源〔2024〕718号

各省、自治区、直辖市、新疆生产建设兵团发展改革委、能源局、工业和信息化主管部门、市场监管部门，北京市城市管理委员会、上海市交通委员会、河南省住房和城乡建设厅，国家能源局各派出机构，国家电网有限公司、中国南方电网有限责任公司，中国电力企业联合会：

为落实党中央、国务院关于碳达峰、碳中和的战略部署，支撑新型能源体系和新型电力系统构建，促进新能源汽车与电网融合互动，根据《国务院办公厅关于进一步构建高质量充电基础设施体系的指导意见》（国办发〔2023〕19号）和《国家发展改革委等部门关于加强新能源汽车与电网融合互动的实施意见》（发改能源〔2023〕1721号）有关要求，国家发展改革委、国家能源局、工业和信息化部、市场监管总局将在全国开展车网互动规模化应用试点。现将有关事项通知如下。

#### 一、总体要求

按照“创新引导、先行先试”的原则，全面推广新能源汽车有序充电，扩大双向充放电（V2G）项目规模，丰富车网互动应用场景，以城市为主体完善规模化、可持续的车网互动政策机制，以V2G项目为主体探索技术先进、模式清晰、可复制推广的商业模式，力争以市场化机制引导车网互动规模化发展。参与试点的地区应全面执行充电峰谷分时电价，力争年度充

电量 60%以上集中在低谷时段，其中通过私人桩充电的电量 80%以上集中在低谷时段。参与试点的 V2G 项目放电总功率原则上不低于 500 千瓦，年度发电量不低于 10 万千瓦时，西部地区可适当降低。

## 二、重点任务

（一）发挥电力市场的激励作用。逐步完善车网互动资源聚合参与电力市场的交易规则，推动充电负荷规模化、常态化参与电力市场交易，支持探索负荷聚合商参与电力市场的商业模式，推动电力市场各类新业态主体培育，逐步形成模式清晰、发展稳定、具备推广条件的负荷聚合商业模式。鼓励 V2G 项目聚合参与电力现货、绿电交易以及储能容量租赁等市场，验证 V2G 资源的等效储能潜力。

（二）完善价格与需求响应机制。建立健全居民充电峰谷分时电价机制，鼓励围绕居民充电负荷与居民生活负荷建立差异化的价格体系，优化峰谷时段设置，合理扩大峰谷价差；探索新能源汽车和充换电场站对电网放电的价格机制。创新需求响应机制，丰富需求响应品种，提升用户参与频次和响应规模。

（三）加强智能有序充电应用推广。制定完善充换电设施智能化相关技术要求，推动智能有序充电桩建设、替代或改造。推动建设智能有序充电试点社区，建立居住社区智能有序充电管理体系，在保障电网安全运行的基础上，有效提升个人智能桩接入能力。提升充换电场站互动能力，研究优化报装容量核定方法和并网运行规则，开展智能充换电场站接入容量优化提升试点。

（四）促进 V2G 技术与模式协同创新。探索与园区、楼宇、住宅等场景高效融合的 V2G 技术和模式，满足公共领域和私人车辆的 V2G 应用需求。支持有关企业联合开展 V2G 项目申报，鼓励车企和电池企业完善电池质保体系和提升电池技术。探索依托新能源汽车国家监测与动力蓄电池回收利用溯源综合管理平台开展 V2G 项目电池状态评估。

（五）强化工作保障和有效引导。强化标准实施应用，支撑车网互动规模化应用有效推进。积极发挥充电设施监测服务平台作用，建立健全车网互动数据接入和评估机制。加强用户权益保障，强化宣传科普，提升用户参与意愿。加大电网企业保障力度，做好资源接入、入网检测、并网计量、调度运行、清分结算等服务。

### 三、组织实施

（一）请各省（区、市）牵头负责充电设施发展的部门会同相关部门和国家能源局派出机构，推荐本地区有意愿参与车网互动规模化应用的城市和 V2G 项目。原则上各省（区、市）推荐的城市不超过 1 个，长三角、珠三角、京津冀鲁、川渝等条件相对成熟的区域可适当放宽至 2 个。原则上各省（区、市）推荐的 V2G 项目不超过 5 个（换电项目不超过 1 个），单个项目可为同一实施主体在同一城市的分散设施集合。

（二）请各省（区、市）牵头负责充电设施发展的部门按照附件要求汇总编写相关材料，并于 2024 年 10 月 31 日前将纸质版材料盖章后寄至国家能源局电力司。国家发展改革委、国家能源局、工业和信息化部、市场

监管总局将适时组织专家审查，选取不少于5个发展基础好、政策力度大、带动效应强的城市及不少于50个V2G项目列入本次试点范围。

（三）各级牵头负责充电设施发展的部门要严格落实主体责任，加大与相关部门的协同力度，积极创新政策机制和监管方式，鼓励相关企业探索车网互动新技术、新产业、新业态、新模式。省级价格主管部门要研究完善峰谷分时等配套电价政策；电力运行主管部门要逐步完善需求响应机制；国家能源局派出机构要推动完善辖区内电力市场准入条件和交易规则，丰富电力交易品种，发挥市场机制和电价政策的协同作用，支持车网互动工作开展。

（四）国家发展改革委、国家能源局、工业和信息化部、市场监管总局将统筹指导各省（区、市）车网互动规模化应用试点工作，会同地方相关部门协调解决工作中的实际问题，适时推动典型经验和成熟模式在全国范围内推广。

国家发展改革委办公厅

国家能源局综合司

工业和信息化部办公厅

市场监管总局办公厅

2024年8月23日

## 行业前沿观察二：各地协会动态

导读：导读：各地协会活动精彩纷呈，举行高级研修班、进行调研活动等。广东省网络空间安全协会举行数字经济高质量发展的安全技术路径高级研修班；北京网络空间安全协会举行“2024 信息技术应用创新与安全能力提升”高研班；上海市信息网络安全管理协会主办数智创新系列高级研修班；上海市信息安全行业协会开展“2024 年度数据安全优秀案例评选”活动；湖南省网络空间安全协会赴贵阳调研大数据产业；西藏自治区互联网协会开展“情暖雪域 e 起行”公益活动；佛山市信息协会承办“启沅杯”2024 年佛山市工业互联网安全技能竞赛；南通市信息网络安全协会举办共建网络安全生态暨 2024 年全市高校网络安全研讨会等。

关键词：高研班、技能竞赛、数据安全、信息安全、网络安全

## 1. 广东省网络空间安全协会：筑牢安全数字底座！数字经济高质量发展的安全技术路径高级研修班顺利举行！

为推动新质生产力在数字经济中的应用和发展，为数字经济的发展提供强有力的人才支撑和智力支持，由广东省人力资源和社会保障厅主办、广东省网络空间安全协会承办的“数字经济高质量发展的安全技术路径”高级研修班于8月27日至8月31日在广州顺利举行。广东省人力资源和社会保障厅一级主任科员杨斌彬，广东省网络空间安全协会常务副会长方满意，协会副会长黄志豪、成珍苑等领导出席高研班开班仪式。来自省内从事数字化管理、数字技术应用及数据安全相关工作，具有中高级职称的专业技术人员或高层管理人员129人通过线上和线下的方式参加高级研修班开班仪式。

在三天的课程中，安排了11场研修专题教学，从新质生产力助力数字经济高质量可持续发展，数字经济与实体经济融合高质量发展案例，人工智能是新质生产力的关键引擎，数字经济高质量发展安全风险等等……丰富多彩的课程确保每位学员都能学有所得，学以致用，大家纷纷感慨收获满满，不虚此行。

2024年“数字经济高质量发展的安全技术路径”高级研修班在30日晚落下帷幕。许多学员表示，此次深入学习了数字经济与新质生产力的融合发展、数据安全与隐私保护的实践经验等等，这些知识和技能的积累，为

提升自己的专业素养，提高技能水平打下坚实基础。今后要学以致用，为推动数字经济的高质量发展贡献更多的力量。

## 2. 北京网络空间安全协会：“2024 信息技术应用创新与安全能力提升”高研班在京成功举办

为深入学习贯彻党的二十届三中全会精神，不断提升专业技术人才自主创新能力，2024年8月26日至30日由国家人社部批准、北京市人社局主办、北京网络空间安全协会承办的专业技术人才知识更新工程“2024 信息技术应用创新与安全能力提升”高级研修班在北京圆满举行。

本次高研班采取了线下线上学习相结合的形式，全国24个省（市、自治区）237名从事信息技术应用创新和网络安全相关工作、具有中高级职称的专业技术人员和高级管理人员报名，其中来自全国10个省（市、自治区）的86名学员参加了线下培训。

8月27日上午，主办单位北京市人社局专技处处长、二级巡视员刘武出席开班仪式并致辞。国家网信办原网络应急管理局局长方楠、中国科学院信息工程研究所研究员查达仁、教育部教育管理信息中心网络安全处副处长孙强等专家领导出席开班仪式。承办单位北京网络空间安全协会理事长黄丽玲致欢迎词，公安部网络安全保卫局原二级巡视员唐前临主持了开班仪式。

本次高研班的研修课程，内容设计紧密聚焦学员需求，围绕服务国家重大战略、重点领域、重点工作，相继邀请了中国工程院方滨兴院士以及中国科学院、北京大学、中央网信办、公安部、国家互联网应急中心、中国信息通信研究院、中国电信集团等专家领导授课，以专题演讲、分组讨论、现场教学等形式，开展了理论基础、关键技术、应用场景、安全挑战及解决方案等方面内容的深入研修和讨论。

研修课程结构也充分集合发展现状+前景预测+实践应用等多个实用模块，从政策前瞻到技术要领给予大家最丰富详实的学习体验，并安排了国家信创园及信创展厅、头部信创企业、信创适配测试及系统迁移实践等现场教学。高研班汇聚了全国各地信创领域的专家和专技人才，对大家来说，是一次难得的同行深入交流探讨的机会。（来源：北京网络空间安全协会）

### 3. 上海市信息安全行业协会：开展“2024年度数据安全优秀案例评选”活动

为响应国家鼓励数据安全领域技术创新的号召，发掘数据安全领域的优秀产品和应用，链接数据安全领域的供给与需求，促进数据安全产业发展，上海市信息安全行业协会将联合其余4家单位主办“2024年度数据安全优秀案例评选”活动。此次评选活动继续获得上海市普陀区科学技术委员会的大力支持，由上海市信息安全行业协会数据安全与隐私计算专业委员会、网安创新中关村专业委员会具体承办，获奖案例将由主办方提报相

关行业主管部门备案，向潜在用户和行业进行推荐，并通过媒体、行业主管部门、产业发展部门等进行广泛传播。评选将面向全社会发起征集（不限地域，不限行业），相关的产品厂商、服务单位和用户单位均可参与。征集数据安全相关的应用案例，包括但不限于数据采集、数据存储、数据传输、数据流通、数据使用、数据防泄漏、数据销毁、数据治理等各个环节。

#### 4. 上海市信息网络安全管理协会主办数智创新系列高级研修班（第二期）

近日，由上海市信息网络安全管理协会、上海交通大学终身教育学院联合主办的数智创新系列高级研修班（第二期）在上海交大长宁校区隆重开班。

中央网信办国家计算机网络与信息安全管理中心上海分中心顾问顾嘉福带来开班第一课《树立总体国家安全观，确保网络与数据安全》，强调并采取一系列必要的措施，确保网络与数据安全。教育部长江学者、上海交通大学终身教育学院院长胡洁做主题报告《人工智能时代的产业创新》，深入浅出地阐述了人工智能在各产业的广泛应用和未来的发展趋势。此次数智创新高级研修班将深度整合业界、学界的优质资源，通过系统的专业学习、交流研讨、参访实践，致力于赋能学员们掌握新理念，拓宽新视野，

激活新动能，构建新思路，开拓新赛道。（来源：上海市信息网络安全管理协会）

## 5. 湖南省网络空间安全协会：赴贵阳调研大数据产业

近日，湖南省网络空间安全协会受湘江新区及长沙市国链安全可靠计算机产业促进中心邀请，携手国家新一代自主安全计算系统产业集群促进组织及重点企业前往贵阳调研大数据产业。调研团一行首先走进中国电信云计算贵州信息园，就园区建设规划、业务发展情况展开调研。调研团在全国一体化算力网络国家（贵州）主枢纽中心，了解贵州响应国家战略构建的全国一体化算力网络枢纽的重大战略工程，深入考察了包含通算、智算、超算等在内的复合型算力枢纽建设情况。通过观看视频演示、听取案例解析，调研团全面深入了解了大数据战略行动以及“数字贵州”的发展成果。并通过座谈会就推动两地的先进计算产业和大数据产业发展展开了深入讨论。

## 6. 西藏自治区互联网协会：开展“情暖雪域 e 起行”公益活动

8月27日，西藏自治区互联网协会党支部秉承服务群众的宗旨，联合西藏自治区党委网信办、上海市志愿者协会中小企业家志愿服务队前往那曲市申扎县巴扎乡，开展了以“情暖雪域 e 起行”为主题的公益活动。活

动中，协会党支部了解到当地实际情况后，积极统筹行业内部资源，主动服务、主动参与，为巴扎乡的群众和儿童筹集到价值12万元的爱心物资，包括全新衣物、生活用品以及学习用品。在自治区党委网信办的积极协调下，物资已顺利送达申扎县巴扎乡的帮扶对象手中。自“情暖雪域e起行”公益项目启动以来，西藏自治区互联网协会党支部通过该项目已向全区37个偏远乡村、学校捐赠各类物资价值180万余元，发放网络安全、反诈、网络文明、数字素养、农村电商等互联网科普宣传材料6000余份。

## 7. 佛山市信息协会：承办“启沅杯”2024年佛山市工业互联网安全技能竞赛

近日，由佛山市信息协会参与承办的“启沅杯”2024年佛山市工业互联网安全技能竞赛第一次线上公开课圆满结束。作为“启沅杯”赛事筹备的重要内容，组委会精心策划线上公开课，邀请业内大咖围绕CTF赛事进行精彩分享，旨在为广大职工和院校学生提供一个交流与学习的平台，进一步拓宽网络安全人才培养渠道。据悉，“启沅杯”线上初赛采用CTF解题赛的方式进行。CTF比赛是一种在网络安全领域广泛开展的竞技形式，旨在通过模拟的网络攻击和防御活动来测试和提高参与者的网络安全技能。今年是佛山市连续第五年举办全市工业互联网安全技能竞赛，经过五年的积累与沉淀，“启沅杯”的影响力逐年增强，竞赛形式也不断丰富。今年

赛事更是首次辐射粤港澳大湾区，旨在搭建网络安全高技能人才交流互鉴的平台。

## 8. 南通市信息网络安全协会：“共建网络安全生态暨 2024 年全市高校网络安全研讨会”

为进一步增强各高校的网络安全意识、提升网络安全防护能力，共同构建安全可靠的网络环境，近日，南通市信息网络安全协会在南通·中关村信息谷举办“共建网络安全生态暨 2024 年全市高校网络安全研讨会”主题活动。相关领导为活动致辞，要求各单位把网络安全工作摆在突出位置，既要加强技术上的检测防护，又要落实制度上的管理责任，共同推进网络安全打击治理工作。会议带领大家学习习近平总书记关于网络强国的重要思想，号召各单位用底线思维扎牢织密网络安全防护网，打造安全可靠的网络安全空间。同时以《共建网络安全生态》为主题，就增强网络安全意识、筑牢网络安全防线等要点进行讲解，探讨降低网络安全风险的经验。会议中还穿插高校网络安全工作经验分享环节。南通大学代表讲授生活中遇到的网络安全问题与处置经验，大家积极参与讨论，深感网络安全无处不在，协会的主题活动不仅丰富了大家的网络安全知识，更增强了网络安全意识，收获颇丰。

# 公安部第三研究所网络安全法律研究中心

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

基础性

专业性

针对性

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

推动立法、服务实务、智库支撑



## 联系方式

电子邮箱: [cslaw@gass.ac.cn](mailto:cslaw@gass.ac.cn)

咨询电话: 王老师 18817309169

# 网络与数据安全法律合规咨询服务

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

## 数据安全合规体系构建



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

## 安全测试法律合规体系构建



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

## 数据出境安全风险评估咨询服务



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

## 网络安全、数据安全执法调查与刑事风险的防范与处置意见



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

## 个人信息保护影响评估/合规审计咨询服务



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

## 网络安全、数据安全法律法规专业培训



# 数据出境安全风险评估咨询服务

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

## 数据出境活动

1

境内运营中收集和产生的数据传输、存储至境外



2

数据存储在国内，境外的机构、组织或者个人可以访问或者调用



## 数据出境安全风险评估咨询服务流程

1 - 3 周

周期视情况而定

01 情况调研

02 风险评估

03 指导落实  
整改

04 出具风险  
评估报告



3 - 5 周



1 - 2 周

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

- 结合客户落实整改情况，出具《数据出境风险评估报告》

# 合规咨询服务项目

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

## 典型项目

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

.....

