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8月第8期 (总第13期)

2024年8月15日

主办单位：公安部第三研究所网络安全法律研究中心
联合主办：北京网络空间安全协会网安联发展工作委员会
牵头组织：网安联秘书处
协办单位：网安联认证中心
技术支持：北京关键信息基础设施安全保护中心
广东关键信息基础设施保护中心

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

目　录

境内前沿观察一：安全事件

导读：7 月 15 日至 18 日，中国共产党第二十届中央委员会第三次全体会议在北京举行。全会认为当前和今后一个时期是以中国式现代化全面推进强国建设、民族复兴伟业的关键时期。

全会提出，要健全因地制宜发展新质生产力体制机制，健全促进实体经济和数字经济深度融合制度。要完善意识形态工作责任制，优化文化服务和文化产品供给机制，健全网络综合治理体系，构建更有效力的国际传播体系。必须全面贯彻总体国家安全观，完善维护国家安全体制机制，实现高质量发展和高水平安全良性互动，切实保障国家长治久安。

全会审议通过《中共中央关于进一步全面深化改革、推进中国式现代化的决定》，是指导新征程上进一步全面深化改革的重要纲领性文献。决定提出，要健全促进实体经济和数字经济深度融合制度。加快建立数据产权归属认定、市场交易、权益分配、利益保护制度，提升数据安全治理监管能力，建立高效便利安全的数据跨境流动机制。

决定提出，完善行政处罚等领域行政裁量权基准制度，推动行政执法标准跨区域衔接。完善行政处罚和刑事处罚双向衔接制度。健全网络综合治理体系。深化网络管理体制改革，整合网络内容建设和管理职能，推进新闻宣传和网络舆论一体化管理。完善生成式人工智能发展和管理机制。加强网络空间法治建设，健全网络生态治理长效机制，健全未成年人网络保护工作体系。加强网络安全体制建设，建立人工智能安全监管制度。

《上海合作组织成员国元首理事会阿斯塔纳宣言》发布，成员国高度重视人工智能技术的发展与应用，愿在该领域开展合作，共同做好风险防范，不断提升人工智能技术的安全性、可控性、可靠性、可信性、公正性，确保人工智能造福全人类。

关键词：二十届三中全会、网络综合治理、网络安全体制建设、上合组织、人工智能

1. 二十届三中全会公报：要健全网络综合治理体系

7 月 18 日，中国共产党第二十届中央委员会第三次全体会议通过《中国共产党第二十届中央委员会第三次全体会议公报》。

全会提出，高质量发展是全面建设社会主义现代化国家的首要任务。必须以新发展理念引领改革，立足新发展阶段，深化供给侧结构性改革，完善推动高质量发展激励约束机制，塑造发展新动能新优势。要健全因地制宜发展新质生产力体制机制，健全促进实体经济和数字经济深度融合制度，完善发展服务业体制机制，健全现代化基础设施建设体制机制，健全提升产业链供应链韧性和安全水平制度。

全会提出，要完善意识形态工作责任制，优化文化服务和文化产品供给机制，健全网络综合治理体系，构建更有效力的国际传播体系。

全会提出，国家安全是中国式现代化行稳致远的重要基础。必须全面贯彻总体国家安全观，完善维护国家安全体制机制，实现高质量发展和高水平安全良性互动，切实保障国家长治久安。要健全国家安全体系，完善公共安全治理机制，健全社会治理体系，完善涉外国家安全机制。（来源：中国政府网）

2. 二十届三中全会通过《中共中央关于进一步全面深化改革 推进中国式现代化的决定》：加强网络安全体制建设

7 月 18 日，中国共产党第二十届中央委员会第三次全体会议通过《中共中央关于进一步全面深化改革 推进中国式现代化的决定》。

决定提出，要健全促进实体经济和数字经济深度融合制度。要加快构建促进数字经济发展体制机制，完善促进数字产业化和产业数字化政策体系。加快新一代信息技术全方位全链条普及应用，发展工业互联网，打造具有国际竞争力的数字产业集群。促进平台经济创新发展，健全平台经济常态化监管制度。建设和运营国家数据基础设施，促进数据共享。加快建立数据产权归属认定、市场交易、权益分配、利益保护制度，提升数据安全治理监管能力，建立高效便利安全的数据跨境流动机制。

决定提出，健全提升产业链供应链韧性和安全水平制度。抓紧打造自主可控的产业链供应链，健全强化集成电路、工业母机、医疗装备、仪器仪表、基础软件、工业软件、先进材料等重点产业链发展体制机制，全链条推进技术攻关、成果应用。建立产业链供应链安全风险评估和应对机制。

决定提出，深入推进依法行政。推进政府机构、职能、权限、程序、责任法定化，促进政务服务标准化、规范化、便利化，完善覆盖全国的一体化在线政务服务平台。完善重大决策、规范性文件合法性审查机制。加强政府立法审查。深化行政执法体制改革，完善基层综合执法体制机制，健全行政执法监督体制机制。完善行政处罚等领域行政裁量权基准制度，推动行政执法标准跨区域衔接。完善行政处罚和刑事处罚双向衔接制度。

决定提出，健全网络综合治理体系。深化网络管理体制改革，整合网络内容建设和管理职能，推进新闻宣传和网络舆论一体化管理。完善生成式人工智能发展和管理机制。加强网络空间法治建设，健全网络生态治理长效机制，健全未成年人网络保护工作体系。

决定要求，完善公共安全治理机制。加强网络安全体制建设，建立人工智能安全监管制度。（来源：中国政府网）

3. 《上海合作组织成员国元首理事会阿斯塔纳宣言》发布，主张建立安全的信息空间

7 月 4 日，上合组织成员国领导人在阿斯塔纳市举行元首理事会会议，并发表《上海合作组织成员国元首理事会阿斯塔纳宣言》。

宣言指出，成员国强调联合国在应对信息威胁方面的关键性作用，主张在尊重国家主权和不干涉他国内政原则基础上建立安全的信息空间。

宣言中，成员国强调，进一步深化数字经济领域互利合作具有重要意义，愿支持发展数字技术，利用数字转型机遇，促进数字基础设施建设，保障数字金融普及。

宣言表示，成员国指出，本组织成员国间科技领域合作符合全球技术发展的共同利益，愿在本组织框架内实施多边联合科研创新项目。成员国高度重视人工智能技术的发展与应用，愿在该领域开展合作，共同做好风险防范，不断提升人工智能技术的安全性、可控性、可靠性、可信性、公正性，确保人工智能造福全人类。（来源：中国政府网）

4. 2024 世界人工智能大会暨人工智能全球治理高级别会议发表《人工智能全球治理上海宣言》

7 月 4 日，2024 世界人工智能大会暨人工智能全球治理高级别会议发表《人工智能全球治理上海宣言》，从促进人工智能发展、维护人工智能

安全、构建人工智能治理体系、加强社会参与和提升公众素养、提升生活品质与社会福祉五个方面呼吁采取行动。

宣言指出，签署方高度重视人工智能的安全问题，特别是数据安全与隐私保护，愿推动制定数据保护规则，加强各国数据与信息保护政策的互操作性，确保个人信息的保护与合法使用。

宣言认识到加强监管，打造可审核、可监督、可追溯和可信赖的人工智能技术的必要性。将以发展的眼光看问题，在人类决策与监管下，以人工智能技术防范人工智能风险，提高人工智能治理的技术能力。鼓励各国结合国情，制定相应的法律和规范，建立风险等级测试评估体系和科技伦理审查制度，在此基础上，鼓励行业制定更为及时和敏捷的自律规范。

宣言同意加强人工智能相关的网络安全，增强系统与应用的安全性与可靠性，防止黑客攻击与恶意软件应用。在尊重运用国际国内法律框架前提下，共同打击操纵舆论、编造与传播虚假信息的行为。

宣言提出，合作防范恐怖主义、极端势力和跨国有组织犯罪集团利用人工智能技术从事非法活动，共同打击窃取、篡改、泄露和非法收集利用个人信息的行为。推动制定和采纳具有广泛国际共识的人工智能的伦理指南与规范，引导人工智能技术的健康发展，防止其被误用、滥用或恶用。来源：新华网）

境内前沿观察二：政策立法

导读：7月，修订后的《保守国家秘密法实施条例》公布。《条例》进一步规范网络信息和数据保密管理，加强网络使用保密管理，完善数据保密管理制度，压实机关、单位涉密数据安全保护主体责任，明确网络运营者对依法实施的保密违法案件调查和预警事件排查的配合义务。

公安部、国家互联网信息办公室发布《国家网络身份认证公共服务管理办法（征求意见稿）》。《网络安全法》《数据安全法》《个人信息保护法》《反电信网络诈骗法》明确国家实施网络可信身份战略、推进网络身份认证公共服务建设，国家组织建设网络身份认证公共服务基础设施，旨在建成国家网络身份认证公共服务平台，形成国家网络身份认证公共服务能力，为社会公众统一签发“网号”“网证”，提供以法定身份证件信息为基础的真实身份登记、核验服务，达到方便人民群众使用、保护个人信息安全、推进网络可信身份战略的目标。此次发布的征求意见稿明确使用“网号”“网证”进行网络身份认证的方式，并对“网号”“网证”的申领条件、公共服务的使用场景、法定身份证件范围、数据和个人信息安全保护义务等基础性事项作出规定。

数据安全方面，自然资源部印发《关于加强智能网联汽车有关测绘地理信息安全管理的通知》，要求地理信息数据必须存储于境内，所使用的存储设备、网络和云服务等必须符合国家有关安全和保密要求。广西、山东相继印发本省促进工业领域数据安全能力提升实施方案（2024—2026年），

提出推动数据安全行政执法，提升数据安全监督检查能力，推动数据安全纳入行政执法事项清单。

湖南省人民政府办公厅印发《湖南省省级政务云管理暂行办法》，明确非涉密政务信息系统部署到政务云后，安全管理遵守“安全管理责任不变、数据归属关系不变、安全管理标准不变、敏感信息不出境”的基本要求。北京市发改委等部门印发《北京市推动“人工智能+”行动计划（2024—2025 年）》，要求加快推动本市大模型按要求上线，编制大模型分级分类管理和安全评测标准，围绕真实场景开展大模型应用质量评估、伦理对齐等方面评测，促进大模型应用安全合规发展。

关键词：保守国家秘密法实施条例、网络身份认证、工业领域数据安全、政务云、人工智能+

（一）国家层面动向

1. 修订后的《保守国家秘密法实施条例》公布

7 月 10 日，国务院总理李强签署国务院令，公布修订后的《保守国家秘密法实施条例》，自 2024 年 9 月 1 日起施行。

条例规定，机关、单位应当加强信息系统、信息设备的运行维护、使用管理，指定专门机构或者人员负责运行维护、安全保密管理和安全审计，按照国家保密规定建设保密自监管设施，定期开展安全保密检查和风险评估，配合保密行政管理部门排查预警事件，及时发现并处置安全保密风险隐患。机关、单位应当按照国家保密规定，对绝密级信息系统每年至少开展一次安全保密风险评估，对机密级及以下信息系统每两年至少开展一次安全保密风险评估。

条例规定，网络运营者应当遵守保密法律法规和国家有关规定，建立保密违法行为投诉、举报、发现、处置制度，完善受理和处理工作机制，制定泄密应急预案。发生泄密事件时，网络运营者应当立即启动应急预案，采取补救措施，并向保密行政管理部门或者公安机关、国家安全机关报告。网络运营者对保密行政管理部门依法实施的保密违法案件调查和预警事件排查，应当予以配合。省级以上保密行政管理部门在履行保密监督管理职责中，发现网络存在较大泄密隐患或者发生泄密事件的，可以按照规定权限和程序对该网络运营者的法定代表人或者主要负责人进行约谈，督促其及时整改，消除隐患。

条例规定，机关、单位应当加强对互联网使用的保密管理。机关、单位工作人员使用智能终端产品等应当符合国家保密规定，不得违反有关规定使用非涉密信息系统、信息设备存储、处理、传输国家秘密。机关、单位应当承担涉密数据安全保护责任，涉密数据收集、存储、使用、加工、传输、提供等处理活动应当符合国家保密规定。机关、单位应当对汇聚、关联后属于国家秘密事项的数据依法加强安全管理，落实安全保密防控措施。（来源：中国政府网）

（二）部委层面动向

1. 三部门印发《关于办理跨境电信网络诈骗等刑事案件适用法律若干问题的意见》

6 月 26 日，最高人民法院、最高人民检察院、公安部印发《关于办理跨境电信网络诈骗等刑事案件适用法律若干问题的意见》。意见共十六条，主要包括依法惩治跨境电信网络诈骗等犯罪、全面加强追赃挽损等内容。

意见指出，对于跨境实施的电信网络诈骗、敲诈勒索等犯罪，确因客观条件限制无法查明被害人的，可以依据账户交易记录、通讯群组聊天记录等证据，结合犯罪嫌疑人、被告人供述，综合认定犯罪数额。犯罪嫌疑人、被告人参加境外诈骗犯罪集团或犯罪团伙，实施电信网络诈骗犯罪行为，犯罪嫌疑人、被告人及所在犯罪集团、犯罪团伙的犯罪数额均难以查证，但犯罪嫌疑人、被告人一年内出境赴境外犯罪窝点累计时间 30 日以上或者多次出境赴境外犯罪窝点的，应当认定为刑法第二百六十六条规定的

“其他严重情节”，以诈骗罪依法追究刑事责任。但有证据证实其出境从事正当活动的除外。

意见提出，犯罪嫌疑人、被告人在境外实施电信网络诈骗、敲诈勒索等犯罪，犯罪情节轻微，依照法律规定不起诉或者免予刑事处罚的，由主管部门依法予以行政处罚。（来源：最高人民检察院）

2. 国家密码管理局发布《国家密码管理局商用密码随机抽查事项清单（2024 年版）》

7 月 19 日，国家密码管理局发布《国家密码管理局商用密码随机抽查事项清单（2024 年版）》，自发布之日起施行。2024 年版随机抽查事项包括四大类别五类事项，分别是：

（1）商用密码检测，抽查事项包括商用密码产品检测随机抽查、商用密码应用安全性评估随机抽查，抽查对象分别是商用密码检测机构的商用密码产品检测业务和商用密码应用安全性评估业务；

（2）商用密码应用，抽查事项为商用密码应用随机抽查，抽查对象是法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统运营者；

（3）电子认证服务使用密码，抽查事项为电子认证服务使用密码随机抽查，抽查对象是电子认证服务使用密码许可单位；

（4）电子政务电子认证服务，抽查事项为电子政务电子认证服务随机抽查，抽查对象是电子政务电子认证服务机构。（来源：国家密码管理局）

3. 自然资源部印发《关于加强智能网联汽车有关测绘地理信息安全管理的通知》

7 月 26 日，自然资源部印发《关于加强智能网联汽车有关测绘地理信息安全管理的通知》。

通知要求落实地理信息数据存储和出境要求。要加强地理信息数据全流程监管，确保智能网联汽车采集、收集的用于导航相关活动以及地图制作、更新的地理信息数据，直接传输至具备导航电子地图制作测绘资质的单位管理，其他单位或个人不得接触。地理信息数据必须存储于境内，所使用的存储设备、网络和云服务等必须符合国家有关安全和保密要求。申请向境外提供地理信息数据的，必须严格履行对外提供审批或地图审核程序，并落实数据出境安全评估等有关规定。

通知提出，要强化地理信息安全监管。要着力健全智能网联汽车地理信息安全风险防控体系，组织研发地理信息保密处理、及时预警与处置等技术，建立完善分类分级、安全风险评估等管理制度和地理信息安全风险监测预警机制。开展地理信息安全风险监测和全周期跟踪，及时查处有关案件。（来源：自然资源部）

4. 两部门发布《国家网络身份认证公共服务管理办法（征求意见稿）》

7 月 26 日，公安部、国家互联网信息办公室发布《国家网络身份认证公共服务管理办法（征求意见稿）》。

征求意见稿共16条，主要包括四个方面的内容：一是明确公共服务和“网号”“网证”等概念；二是明确公共服务的使用方式和场景；三是强调公共服务平台和互联网平台的数据和个人信息保护义务；四是明确公共服务平台和互联网平台违反数据和个人信息保护义务的法律责任。

征求意见稿指出，国家网络身份认证公共服务，是指国家根据法定身份证件信息，依托国家统一建设的网络身份认证公共服务平台，为自然人提供申领网号、网证以及进行身份核验等服务。网号是指与自然人身份信息一一对应，由字母和数字组成、不含明文身份信息的网络身份符号；网证是指承载网号及自然人非明文身份信息的网络身份认证凭证。

征求意见稿规定，网号、网证可用于在互联网服务及有关部门、行业管理、服务中非明文登记、核验自然人真实身份信息。根据法律、行政法规规定，在互联网服务中需要登记、核验用户真实身份信息的，可以使用网号、网证依法进行登记、核验。（来源：中国网信网）

（三）地方层面动向

1. 北京市印发《北京车联网安全筑基工作方案》

6月19日，北京市通信管理局、北京市经济和信息化局印发《北京车联网安全筑基工作方案》。

方案明确，北京市通信管理局、北京市经济和信息化局统筹推进车联网网络安全和数据安全管理工作，指导督促北京地区车联网企业落实落细网络安全、数据安全各项管理要求；结合工作需求，开展网络和数据安全

政策宣贯及标准培训，帮助企业完成风险排查、威胁治理和问题整改等工作。车联网企业应按照通知要求，结合企业实际情况，抓好工作落实。

方案提出提升企业网络安全水平、强化车联网网络安全分级防护、深化车联网网络安全威胁治理、推动企业数据安全保护、促进产业创新发展五大项十八小项主要任务。其中，方案要求各车联网企业应当加强合作方数据安全管理，建立合作方管理台账，记录合作方名称、共享数据的类别、级别、规模、用途、提供方式、安全保障措施等信息并及时更新。结合具体业务场景通过签订数据安全合同协议等方式，明确所涉数据情况及双方数据安全管理责任划分、保障措施、违约责任等；涉及数据提供、委托处理等合作的，应要求合作方提供所在地省级通信管理局审核通过的数据安全风险评估报告或审核通过的相关证明材料，涉及重要数据的，应当对合作方数据安全保护能力开展核验，保障其数据安全履约能力。（来源：北京市通信管理局）

2. 北京市发改委等部门印发《北京市推动“人工智能+”行动计划（2024—2025 年）》

7 月 18 日，北京市发展和改革委员会、北京市经济和信息化局、北京市科学技术委员会、中关村科技园区管理委员会印发《北京市推动“人工智能+”行动计划（2024—2025 年）》。

行动计划打造标杆应用工程。依托首都优势行业资源和科技创新能力，围绕机器人、教育、医疗、文化、交通等 5 个领域组织实施一批综合型、标杆性重大应用工程；围绕科研探索、政务服务、工业智能、金融管理、

空间计算、数字营销、司法服务、广电传媒、电力保障、内容安全等10个行业细分领域，支持市级行业主管部门、相关区、行业应用企业与大模型企业联动结对，突破场景落地共性难点，探索标准化、可复制、可推广的大模型行业应用落地路径。

行动计划要求统筹高质量发展和高水平安全，督促指导大模型企业落实国家关于生成式人工智能服务的法律要求，坚持包容审慎监管原则，加快推动本市大模型按要求上线，编制大模型分级分类管理和安全评测标准，围绕真实场景开展大模型应用质量评估、伦理对齐等方面评测，促进大模型应用安全合规发展。

行动计划要求夯实数据安全和个人隐私保障能力，完善面向大模型行业的数据漏洞、隐私泄露等风险监测体系，支持权威机构开发大模型风险监测平台，形成“安全态势感知+风险评估预警”运作机制。压实大模型服务开发者、使用方的主体责任，引导各方依法依规使用生成式人工智能技术，注意保护个人隐私、知识产权和秘密信息，促进人工智能产业向上向善发展。（来源：北京市发展和改革委）

3. 湖南省人民政府办公厅印发《湖南省省级政务云管理暂行办法》

6月28日，湖南省人民政府办公厅印发《湖南省省级政务云管理暂行办法》。办法共十章四十三条，包括建设管理、使用管理、运维管理、安全管理等内容。

办法规定，政务云采取“政府按需统一购买服务、企业建设和运维”的方式进行建设运维。省级各单位应当充分利用政务云开展政务信息化建

设，原则上不得新建非涉密数据中心、机房等通用基础设施，不得自行采购政务云已具备服务能力的软、硬件产品及网络、安全服务，已建网络安全等级保护第三级及以下的非涉密政务信息系统应当逐步迁移到政务云，相关法律法规另有规定的除外。

办法规定，非涉密政务信息系统部署到政务云后，安全管理遵守“安全管理责任不变、数据归属关系不变、安全管理标准不变、敏感信息不出境”的基本要求。任何单位和个人不得利用政务云侵犯国家、公民、法人及其他组织的合法权益，不得利用政务云从事违法犯罪活动。各政务部门自行采购拟部署至政务云的产品，不满足政务云安全管理要求的，不得部署至政务云。

办法明确，云服务商负责其提供的产品和服务的安全，协助云使用单位开展非涉密政务信息系统等保测评和商用密码测评等工作。云服务商提供的云平台应当通过国家云计算服务安全评估、网络安全等级保护第三级测评、商用密码应用安全性评估，并按《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》（国务院令第 745 号）、《商用密码管理条例》（国务院令第 760 号）、《云计算服务安全评估办法》（公告 2019 年第 2 号）等要求定期开展评估并备案。（来源：湖南省人民政府网）

4. 湖南省数据局发布《湖南省数据条例（草案）（征求意见稿）》

7 月 16 日，湖南省数据局发布《湖南省数据条例（草案）（征求意见稿）》。征求意见稿包括七章四十条，包括数据权益、数据资源、数据流通交易、数据发展应用、数据安全监管等内容。

征求意见稿指出，要依法保护自然人对其个人信息享有的合法权益。数据处理者所处理的数据中包含个人信息的，取得个人信息主体授权或者经过匿名化处理的，可以依法进行开发利用，但应当保护个人信息主体获取、复制或者转移个人信息数据的权益。

征求意见稿依法保护数据处理者在数据处理活动中形成合法财产权益，探索建立数据持有权、使用权、经营权结构性分置机制。数据处理者对合法获取的数据进行实际持有或委托他人代为持有、依法进行自主管控并排除他人干涉的权益，通过加工、聚合、分析等方式对合法持有的数据进行使用的权益，通过转让、许可或者设立担保等方式对外提供数据的权益，受本条例保护。法律、法规另有规定的，从其规定。数据处理者对在生产经营活动中采集加工的不涉及个人信息和公共利益的数据，享有依法持有、使用、获取收益的权益。数据处理者对在不违反法律、法规规定，不侵犯其他主体合法权益的前提下收集的公开数据，享有依法持有、使用的权益，并可在不违反市场秩序或当事人约定的前提下加工生产数据产品对外提供。（来源：湖南省人民政府）

5. 河南省印发《2024 年河南省大数据产业发展工作方案》

7 月 3 日，河南省工业和信息化厅、河南省发展和改革委员会、河南省科学技术厅、河南省通信管理局印发《2024 年河南省大数据产业发展工作方案》。

方案提出，要提高数据安全保障水平。开展 2024 年度工控系统安全检查，指导工业互联网企业强化安全管理，完善安全策略，确保网络安全、

平台安全和数据安全。持续推进工业企业数据分类分级管理，开展重要数据和核心数据识别并形成目录。深化隐私计算、数据脱敏、区块链等技术应用，提升各环节的数据安全水平。试点建设一批行业、企业可信数据空间，实现行业数据按需接入、安全共享、可管可控。（来源：河南省工业和信息化厅）

6. 海南省通信管理局印发《海南省公共互联网网络安全突发事件应急预案》

7月4日，海南省通信管理局印发《海南省公共互联网网络安全突发事件应急预案》。

预案根据社会影响范围和危害程度，将公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。建立公共互联网网络突发事件预警制度，按照紧急程度、发展态势和可能造成的危害程度，公共互联网网络突发事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全突发事件。公共互联网网络安全突发事件应急响应分为四级：Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级，分别对应已经发生的特别重大、重大、较大、一般事件的应急响应。

预案指出，省内基础电信企业、域名机构、互联网企业和网络安全专业机构应加强对木马查杀、漏洞检测、网络扫描、渗透测试等网络安全应急装备、工具的储备，及时调整、升级软件硬件工具。鼓励研制开发相关技术装备和工具。（来源：海南省通信管理局）

7. 贵州省大数据局发布《贵州省公共数据授权运营管理办法（试行）（征求意见稿）》

7 月 5 日，贵州省大数据局发布《贵州省公共数据授权运营管理办法（试行）（征求意见稿）》。征求意见稿共六章三十一条，包括公共数据授权、公共数据运营、行为规范、安全监管等内容。

征求意见稿规定，原始公共数据不得导出公共数据平台。可通过可逆模型或算法还原出原始数据包的数据产品和服务，不得导出公共数据平台。符合有关法律法规要求的网络安全等级保护标准和商用密码安全性评估要求的非公共数据承载系统，可以接入公共数据平台。

征求意见稿规定，运营主体、开发利用主体违反网络安全、数据安全、个人信息保护有关法律法规的，由网信、公安、国家安全、保密、密码管理等部门按照职责依法予以查处，相关不良信息依法记入其信用档案。未经同级人民政府数据主管部门审核确认，政府部门私自开展公共数据授权运营相关工作，由网信、公安、国家安全、保密、密码管理等部门按照职责依法予以查处。（来源：贵州省大数据发展管理局）

8. 广西壮族自治区印发《广西促进工业领域数据安全能力提升实施方案（2024—2026 年）》

7 月 12 日，广西壮族自治区工业和信息化厅印发《广西促进工业领域数据安全能力提升实施方案（2024—2026 年）》，围绕提升工业企业数据保护能力、提升数据安全监管能力、提升数据安全产业支撑能力，提出八项重点任务。

提升工业企业数据保护能力方面，方案提出，要压实企业数据安全主体责任。督促企业依法依规落实数据安全主体责任，压实各单位法定代表人或主要负责人数据安全第一责任，推动企业建立健全适应行业和企业实际数据安全责任制，落实各级各有关部门有关人员的数据安全责任。遴选和推广一批各行业领域数据安全管理制度完备的企业案例，组织行业企业学习借鉴。指导企业建立健全数据分类分级安全保护等工作机制，配齐、配足、配强数据安全岗位和人员队伍。推动数据安全专家团队与重点企业开展结对联学，协助企业做好数据安全教育培训。

提升数据安全监管能力方面，方案指出，要推动数据安全行政执法。依据《数据安全法》《工业和信息化领域数据安全管理办法（试行）》，根据工业和信息化部统一安排部署，推动将工业领域数据安全纳入行政执法事项清单，建立健全行政执法队伍，依法依规处置违法行为。指导地市依法严格处置违法行为，打造专业化、规范化监管执法队伍。（来源：广西壮族自治区工业和信息化厅）

9. 山东省印发《山东省促进工业领域数据安全能力提升实施方案（2024—2026 年）》

7 月 12 日，山东省工业和信息化厅印发《山东省促进工业领域数据安全能力提升实施方案（2024—2026 年）》，围绕实施工业企业数据保护能力提升工程、实施数据安全科学监管能力提升工程、实施数据安全产业支撑能力提升工程三个方面，实施十项重点任务。

工业企业数据保护能力提升方面，方案提出，要提升企业数据安全防护能力。指导企业依据工业领域数据安全保护实践系列指南，强化数据异常监测、数据加密、数据脱敏、数据防泄露等安全防护手段建设，提升企业风险监测、态势感知、威胁研判和应急处置等综合能力，及时报告重大风险事件。引导企业将数据安全融入业务数据化、数据业务化全过程，加快建设基于隐私计算的可信工业大数据平台和企业数据仓，构建企业可信数据空间，提升企业数据汇聚、流通和应用等数据处理场景安全保护能力。面向供应链上下游协作、服务外包、上云上平台等典型业务场景，厘清多主体数据安全责任界面和衔接模式，建立全链条全方位数据安全保护体系。

数据安全科学监管能力提升方面，方案提出，要完善数据安全管理工作机制。落实国家工业领域数据安全风险评估实施细则、应急预案、行政处罚裁量指引等政策文件，推动各级工业和信息化主管部门完善重要数据备案、风险监测、监督检查与应急处置等工作流程，结合实际制定细化工作方案，加强与网信、公安等相关部门协作力度，共同提升区域数据安全管理水平。（来源：山东省工业和信息化厅）

10. 湖北省通信管理局印发《湖北省信息通信行业网络运行安全综合管理能力评估机制（试行）》

7 月 15 日消息，湖北省通信管理局近日印发《湖北省信息通信行业网络运行安全综合管理能力评估机制（试行）》，指导企业开展网络运行安全综合管理能力评估工作，督促电信运营企业严格落实企业主体责任。

评估机制以筑牢安全防线、消除风险隐患、夯实技术能力为目标，对省内各基础电信运营企业、铁塔公司开展年度网络运行安全综合管理能力评估。重点围绕企业在网络稳定安全运行保障体系、风险隐患排查化解、重要系统保障、技术管控、运行事故应急处置及运行事故整改等六方面能力、67 项任务落实情况开展能力评估工作。分为企业自查评估、第三方审查评估和管局督查评估三个阶段。（来源：湖北省通信管理局）

境内前沿观察三：治理实践

导读：7月，中央网信办部署开展为期2个月的“清朗·2024年暑期未成年人网络环境整治”专项行动，聚焦短视频、直播平台，社交平台，电商平台，应用商店，儿童智能设备以及未成年人模式六个重点环节；并部署开展为期1个月的“清朗·网络直播领域虚假和低俗乱象整治”专项行动，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”混淆视听等五类突出问题。

公安部、最高检分别围绕针对企业财会人员实施电信网络诈骗、利用网络暴力侵犯企业合法权益两方面发布典型案例，提高相关企业和人员防骗意识能力，保障企业合法权益。公安部刑侦局有关负责人表示，公安部已部署各地公安机关结合典型案例对企业相关人员开展反诈宣传，指导排查清除钓鱼软件，提升系统安全防护能力，切实消除风险隐患。同时，公安机关提醒广大企业和群众切实提高防范意识，定期对电脑进行杀毒，一旦发现伪装成好友的诈骗账号立即删除并更改聊天软件登录密码。如遇到单位领导、企业老板、公司客户在聊天软件中要求转账汇款的，一定要当面或者电话核实，以免遭受财产损失。

行政执法个案方面，广西、内蒙古、河南、湖南等地公安机关和网信部门公开披露多起行政执法案件。所涉及的违法行为包括但不限于：1. 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范；2. 将业主个人信息打印成册随意放置，未进行专人管理和保密设置；

3. 外网路由器密码复杂程度不够；4. 未在公安机关进行网络安全等级保护备案；5. 未及时发现处置系统漏洞；6. 未明示收集使用个人信息的目的、方式、范围；7. 在执行实名认证流程时，未将个人隐私政策向用户深度解读，取得用户独立同意；8. 系统存在安全漏洞，经网信部门多次通报后认为落实安全保护义务。

关键词：网络生态治理、电信网络诈骗、网络暴力、系统漏洞

（一）公安机关治理实践

1. 公安部公布 5 起针对企业财会人员实施电信网络诈骗的典型案例

7 月 30 日，公安部公布 5 起针对企业财会人员实施电信网络诈骗的典型案例。

公安部表示，近期，通过投放木马病毒入侵公司电脑，从而冒充企业老板或客户诈骗财会人员的“精准投毒”类电信网络诈骗案件高发，造成相关企业巨大损失。公安部对此高度重视，部署各地公安机关迅速行动、重拳出击，成功侦破一批重点案件，打掉一批诈骗团伙。经查，此类诈骗案件中，诈骗分子通常将研发的木马病毒伪装成报税工具、办公软件、电子发票、涉税文件等，通过发送电子邮件或推送下载链接等方式，诱骗企业人员点击下载，从而实施木马攻击。相关企业电脑一旦被木马病毒入侵，诈骗分子即可对电脑远程监控，进而通过办公文件、聊天记录等信息“精准”分析出企业基本情况和财会、管理、销售等人员信息。随后，诈骗分子通过远程控制财会等人员的 QQ、微信等社交软件，在本人未发觉的情况下，将用于诈骗的账号添加至其好友列表。时机成熟后，诈骗分子再将诈骗账号“摇身一变”，伪装成该企业老板或客户的 QQ、微信，编造多种理由要求财会等人员转账汇款，从而实施诈骗。作案过程中，诈骗分子无论是前期利用木马病毒入侵电脑，还是后期假冒老板、客户要求转账汇款，

都极为隐蔽，迷惑性极强，甚至通过长期潜伏逐步摸清相关人员聊天习惯和企业财务审批流程，稍有不慎就可能落入诈骗陷阱。

案例1：2023年9月21日，浙江省台州市天台县公安局接报一起电信网络诈骗案件，受害人朱某系一科技公司财会人员，被诈骗分子冒充公司老板拉入微信群后转账1000余万元。案件发生以后，浙江省市县三级公安机关联合成立专案组，紧急开展资金止付和案件侦办等工作。接报后，公安机关仅用6小时就抓捕到第1名涉案犯罪嫌疑人，成功为该公司挽回损失600余万元。后经专案组缜密侦查、深挖拓线，在全国多地成功抓获涉及该案资金、通讯等环节的犯罪嫌疑人41名，实现全链条打击。

案例2：2023年10月25日，福建省武夷山市公安机关接群众郑某报警称，其公司财务张某疑似被电信网络诈骗1480余万元。接报后，公安机关立即开展涉案资金止付挽损工作，当天成功止付冻结涉案资金930余万元，涉及529个账户。经查，案发前，诈骗分子通过对张某电脑投放木马病毒程序实现远程控制，进而将其微信好友中的公司老板账号秘密删除，再将假老板微信添加为其好友。随后，假老板将张某拉入一微信工作群，让张某提前支付合作公司货款，从而实施诈骗。目前，全案共抓获犯罪嫌疑人51名，打掉黑灰产团伙8个，累计挽回损失1200余万元。

案例3：2024年5月22日，安徽省阜阳市公安机关接到某公司人员报警称，公司财务疑似被电信网络诈骗。经查，该公司财务王某在工作微信群中下载运行一不明文件后，电脑被植入木马病毒。境外诈骗分子通过木马病毒远程控制王某电脑，秘密窃取相关信息，利用伪装的“公司领导”微信号要求其向指定账户转账。王某信以为真，向该账户转账100万元，

直至公司领导询问时才发觉被骗。案发后，阜阳市公安机关第一时间开展追赃挽损、循线打击，成功为该公司挽回损失85万元，抓获犯罪嫌疑人6名。

案例4：2024年3月21日，山东省烟台市公安局蓬莱分局海港海岸派出所接到国家反诈中心下发的见面劝阻指令：辖区内一公司存在被骗风险。接指令后，派出所民警立即开展见面劝阻工作。据悉，该公司工作人员迟某伟安装了一款在网上购买的激活软件后，其电脑被植入木马病毒并被诈骗分子远程控制，自动进行打字、发送消息等操作。随后，诈骗分子利用伪装成公司工作人员的微信向会计发送信息，要求向指定账户转账100万元。了解情况后，民警迅速组织对该公司电脑进行木马病毒查杀，同时对相关人员开展反诈知识宣传，成功为企业避免财产损失。

案例5：2024年5月27日，上海市松江区公安机关接到一公司经理李某求助称，其公司员工疑遭遇电信网络诈骗。经了解，该公司财务总监熊某当日收到一条微信好友申请，头像和姓名均为其公司老板。添加好友后，对方以老板日常说话语气与熊某聊天，后以支付货款为由要求其向指定公司账户转账498.6万元。熊某想起公安机关反诈宣传中“转账前要当面或电话确认”的防范提示，并未仓促转账而是立即致电公司老板。因多次未联系上老板，熊某遂将相关情况告知李某。随后，公安机关协助熊某与公司老板取得联系，成功拆穿骗局，避免公司遭受财产损失。经查，熊某公司电脑近日中了木马病毒，诈骗分子通过木马病毒逐步摸清公司人员和经营情况，伪装潜伏后伺机实施诈骗。（来源：公安部）

2. 广东省公安厅公布打击整治网络谣言和网络水军十大典型案例

7月2日，广东省公安厅公布打击整治网络谣言和网络水军十大典型案例，分别是：

案例一：刘某某为提升其名下房产中介公司知名度编造“广东一公司有员工因讲粤语被罚款5000元”网络谣言案。

案例二：刘某某利用AI视频软件制作并发布虚假视频网络谣言案。

案例三：林某修改官方通报发布涉“广州一交通事故造成11人死亡”网络谣言案。

案例四：黄某某通过对旧视频“移花接木”编造“东莞暴雨，8人死亡事件”网络谣言案。

案例五：林某某散布“中国血液制品出口”虚假信息抹黑无偿献血政策网络谣言案。

案例六：周某某冒充记者利用“负面新闻”敲诈勒索案。

案例七：郑某某等人非法查询外卖平台匿名评价客户信息后通过联系、骚扰客户的方式为商家提供删除差评服务侵犯公民个人信息案。

案例八：刘某某搭建网站有偿提供虚假点赞破坏市场公平竞争环境非法经营案。

案例九：黄某等人组织“刷单控评”扰乱电商平台信用评价体系非法经营案。

案例十：郭某搭建刷单平台组织“刷量控评”虚假提升商家曝光度并赚取佣金非法经营案。（来源：广东公安）

3. 因不履行个人信息保护义务，广西一物业服务公司被处罚

7 月 8 日，广西河池市东兰县公安局对一物业服务公司涉嫌不履行个人信息保护义务依法进行行政处罚，并要求现场整改。

在全国夏季治安打击整治专项行动中，河池市东兰县公安局民警收到群众反映，购房后经常收到装修公司的电话或短信骚扰，怀疑个人信息被泄露。民警走访发现，东兰县某物业服务公司在物业管理过程中大量采集业主公民个人信息共计 400 余条，包含姓名、身份证号码、电话、家庭住址等，但公司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范。同时，该公司还将部分业主个人信息打印成册随意放置在前台，未进行专人管理和保密设置，他人可以随意使用，存在公民个人信息被泄露的严重风险。

警方查明，该物业服务公司涉嫌违反《个人信息保护法》之规定，涉嫌不履行个人信息保护义务。在民警的指导下，该物业服务公司对存储的公民个人信息安全隐患进行整改。（来源：广西网警）

4. 内蒙古通辽网警公布 4 起不履行网络安全保护义务处罚案例

7 月 11 日，内蒙古自治区通辽市公安机关网安部门公布 4 起不履行网络安全保护义务处罚案例。

案例一：2024 年 1 月 9 日，内蒙古自治区通辽市科尔沁左翼后旗公安局警务支援大队接到上级下发线索，科尔沁左翼后旗 X 有限责任公司存在网络安全隐患。经查，该公司外网路由器密码复杂程度不够，系统未在公安机关进行网络安全等级保护备案，未落实网络安全保护义务，未采取防

范计算机病毒和网络侵入等技术措施。科左后旗公安局根据《网络安全法》第二十一条、第五十九条之规定，责令该公司整改并给予警告的行政处罚。

案例二：2024 年 1 月 11 日，内蒙古自治区通辽市科左后旗公安局警务支援大队深入辖区 X 公司进行网络安全检查，对该公司业务系统进行安全检测，发现多个漏洞，存在网络安全隐患，容易造成年检车辆人员的大量信息泄露。科左后旗公安局根据《网络安全法》第二十一条第一项、第二项、第五十九条第一款之规定，责令该公司整改并给予警告的行政处罚。

案例三：内蒙古自治区通辽市奈曼旗公安局警务支援大队在执法检查中发现，某中心业务系统存在多个高危漏洞隐患，该中心网络责任和义务落实不到位，网络安全管理制度和技术措施不完善，网络安全保护意识淡薄，未制定网络安全事件应急预案，未能及时发现处置其业务系统漏洞。通辽市奈曼旗公安局依据《网络安全法》第二十五条、第五十九条之规定给予警告的行政处罚。

案例四：2024 年 4 月 1 日，通辽市奈曼旗公安局警支大队在执法检查时发现，奈曼旗某单位操作系统存在多个网络安全漏洞。经查，该单位对其内部操作系统未做到定期检查，未及时发现处置系统漏洞。通辽市奈曼旗公安局依据《网络安全法》第二十五条、第五十九条之规定，责令该单位整改并给予警告的行政处罚。（来源：通辽网警）

5. 河南郑州警方依法办理一起 APP 超范围采集公民信息案

7 月 24 日消息，河南省郑州市公安局高新分局网安大队近日在开展网络安全执法检查中发现，辖区某网络科技公司开发运营的一款游戏类 App

在搜集用户个人信息时，未明示收集使用个人信息的目的、方式、范围；在执行实名认证流程时，未将个人隐私政策向用户深度解读，取得用户独立同意，存在违规搜集行为；同时该公司存在网络安全意识不强、未制定网络安全管理制度、未开展网络安全培训工作、网络日志保存时间不足等问题，违反《网络安全法》相关规定。

针对该公司不履行网络安全义务的违法行为，郑州市公安局高新分局根据《网络安全法》相关规定，分别对该网络科技有限公司和主管人员李某某依法予以行政处罚，并责令其限期整改。（来源：河南网警）

6. 北京海淀警方破获三起涉网违法犯罪案件

7 月 14 日消息，北京海淀警方近日持续加大对涉网违法犯罪的打击力度，破获三起涉网违法犯罪案件。

案例一：利用网络直播传播有害信息案

近日，海淀警方经细致侦查，成功破获一起以成立 MCN 传媒公司的方式，非法利用信息网络传播违法信息的案件，刑事拘留 16 人。2024 年 3 月中旬，海淀警方接群众举报，称在某直播平台发现一主播有传播淫秽视频的行为。接警后，海淀分局警务支援大队立即开展工作，通过调查，发现该公司多名主播均存在此类情况。民警立即成立攻坚小组开展多维度侦查，梳理团伙成员，固定相关证据。

2024 年 4 月中旬，民警锁定李某、魏某等 16 名有重大作案嫌疑人，随即立即开展抓捕工作，最终将涉案人员全部抓获。目前，犯罪嫌疑人李某、魏某等 16 人已被海淀警方依法刑事拘留，案件正在进一步审查中。

案例二：企业“内鬼”非法获取计算机信息系统数据案

日前，海淀警方经过缜密侦查，与辖区企业密切配合，成功破获一非法获取计算机信息系统数据案件，刑事拘留 2 人，涉案金额 8 万余元。2024 年 3 月，海淀警方接辖区企业报警称，公司在内部日常巡检时，发现员工吴某操作行为异常，存在违法嫌疑。接警后，警务支援大队立即开展侦办。

民警循线追踪侦查，于 2024 年 4 月将犯罪嫌疑人吴某抓获，当场扣押作案工具，在其办公电脑中发现大量作案证据。经审讯，吴某承认为牟取非法利益，利用职务便利，进行网络犯罪的事实。随即，民警加大工作力度，深挖扩线，分析研判其同伙赵某藏身地并将其抓获。目前，吴某、赵某因非法获取计算机信息系统数据罪，已被海淀警方依法刑事拘留，案件正在进一步审查中。

案例三：非法获取公民个人信息案

2023 年 12 月，海淀警方在办理一起案件时，发现非法出售公民个人信息的线索。随即，警务支援大队联合上地派出所民警扩线侦查。经工作，民警发现犯罪嫌疑人翁某和黄某有重大作案嫌疑。2024 年 4 月，民警连日摸排蹲守，最终将两人抓捕归案。目前，翁某、黄某因涉嫌侵犯公民个人信息罪，已被海淀警方依法刑事拘留，案件正在进一步侦办中。（来源：公安部网安局）

7. 辽宁阜新警方成功打掉一个非法控制计算机信息系统犯罪团伙

7 月 23 日消息，辽宁省阜新市网安支队近日成功打掉一个非法控制计算机信息系统犯罪团伙，斩断一条研发网约车外挂销售非法获利的犯罪链。

经工作得知，阜新市居民李某在多个司机群以“外挂”软件能实现虚拟定位、优先抢单、随意变换计费路程等名义，发布出售“朱雀”、“猪猪侠”、“钵钵鸡”等多款网约车外挂非法获利。警方立即对该线索进行梳理，涉嫌非法控制计算机信息系统罪，作案团伙人数众多，分工明确，有的专门负责编写外挂软件，有的负责寻找下线代理人员，有的负责销售。

阜新网安支队抽调分局警力成立专案组，对该团伙实施抓捕工作，但嫌疑人反侦察意识很强，又居无定所，给抓捕工作带来很大困难。专案组决定转换思路，奔赴多个省市，开展大量走访摸排工作，充分固定证据后，组成5个抓捕组，出动40余名警力，分赴四省多地将李某等5名销售外挂软件嫌疑人抓获，随即立即对其突击审讯，根据李某等提供的线索顺藤摸瓜，终于锁定以吴某为首的犯罪团伙位置。

专案组连夜奔赴广州、深圳、盐城、扬州、南京等市，经过十多个小时的集中收网，成功将另外12名犯罪嫌疑人抓获，封停网约车外挂账号22万余个，涉案金额高达800余万元，目前犯罪嫌疑人已被采取强制措施，案件正在进一步侦办中。（来源：阜新网警）

8. 浙江警方成功侦破3起重大“网络水军”虚假转评赞案件，累计涉案金额超过千万元

7月30日消息，浙江警方近日成功侦破3起重大“网络水军”虚假转评赞案件，累计涉案金额超过千万元。

案例一：台州三门——跨省“网络水军”团伙覆灭，涉案金额高达两百万

2024年6月，台州三门县公安局成功破获一起以刘某辉为首的“网络水军”案件，抓获犯罪嫌疑人3名，涉案金额逾200万元。该团伙利用“某乐”网站平台，为网络平台主播提供虚假流量、虚假好评等非法服务，严重破坏了网络直播市场的公平竞争环境。警方查明，该团伙作案范围广泛，涉及多个省份，累计为万余家商户提供刷好评服务，危害极大。

案例二：宁波慈溪——全链条摧毁“网络水军”团伙

2024年6月至7月间，宁波慈溪市公安局经过精心部署，连续两次收网行动，成功捣毁一个专门从事虚假刷人气、点赞、增粉服务的“网络水军”团伙，抓获多级中介以及刷手等犯罪嫌疑人7人，涉案资金高达千万元。该团伙通过搭建多个网络平台，为抖音、小红书、淘宝等多家平台的商户提供虚假增粉、评论、点赞等增值服务，严重扰乱网络市场秩序。警方共查获虚假信息记录超4000万条，实现对“网络水军”团伙全链条打击。

案例三：金华永康——网络水军头目获刑五年三个月

2024年6月20日，金华永康市法院对一起“网络水军”案件作出判决，被告人朱某某因利用网络贩卖虚假播放量、浏览量等非法服务，被判处有期徒刑五年三个月，并处罚金二十五万元。此案源于永康市公安局网安大队接到的群众举报，经调查发现朱某某通过搭建运营“网红24小时自助下单平台”，向微信、抖音等社交平台客户出售虚假推广服务，非法获利20余万元，累计交易订单超50万条，涉案金额上百万元。（来源：浙江网警）

（二）网信部门治理实践

1. 中央网信办启动“清朗·2024 年暑期未成年人网络环境整治”专项行动

7 月 13 日消息，中央网信办近日印发通知，在全国范围内部署开展为期 2 个月的“清朗·2024 年暑期未成年人网络环境整治”专项行动。专项行动重点整治 6 个环节突出问题：

一是短视频、直播平台。“二次包装”经典动画或儿歌，集中展示暴力血腥内容。摆拍校园霸凌视频，将校园霸凌行为娱乐化。利用“网红儿童”牟利，恶搞儿童博取关注、卖惨引流。采取剧情电台、语音旁白等方式，诱导胁迫未成年人变相参与直播等问题。

二是社交平台。在未成年人照片分享、交友信息等页面，发布诱导不良交友、引流非法网站等信息。对未成年人实施“网络厕所”“人肉开盒”等行为。恶意编造网络黑话、低俗流行语，向未成年人传播不良价值观。创建专门话题、群组等，恶意发布反击攻略、进行恶意 P 图，煽动亲子、师生对立等问题。

三是电商平台。向未成年人售卖软色情手办文具、动漫周边等商品。利用儿童模特摆出不雅姿势、做性暗示动作，借未成年人形象进行无底线营销。提供有偿代骂，制作恶搞同学、学校的图文视频等服务。以售卖动漫剧作、电子游戏等为名，引流未成年人至第三方平台，违规提供涉黄涉暴资源等问题。

四是应用商店。利用相似标志和名称信息，仿冒未成年人喜爱的APP，传播违法不良信息。通过内嵌非法软件或违规马甲包等方式，恶意“变身”为涉黄涉赌平台。学习类、工具类APP偏离主责主业，传播打擦边球违规信息。具有匿名、加密等属性的小众APP，存在网络诈骗、隔空猥亵等问题。

五是儿童智能设备。设备自带APP包含可能影响未成年人身心健康的内容。对第三方APP提供的信息内容审核把关不严，存在不良导向内容。提供相貌PK、运势测算等不适宜未成年人的应用或功能。以积分排行、功能解锁、背景更新等为名，诱导未成年人过度消费。

六是未成年人模式。提供“虚假模式”，用户进入未成年人模式后无内容、无法使用。模式下存在诱导未成年人模仿不安全行为、养成不良嗜好等内容。模式防逃逸措施不完备，无需验证即可退出。模式下存在诱导未成年人投票打榜、刷量控评等功能。（来源：中国网信网）

2. 中央网信办启动“清朗·网络直播领域虚假和低俗乱象整治”专项行动

7月31日消息，中央网信办近日印发通知，在全国范围内部署开展为期1个月的“清朗·网络直播领域虚假和低俗乱象整治”专项行动。专项行动重点整治五类突出问题：

一是编造虚假场景人设，无底线带货营销。编造虚假“扶贫”“助农”“患病”等场景，通过“扮穷”“卖惨”诱导网民购买低质伪劣商品。利用未成年人、残障人士、孤寡老人等形象吸粉引流。摆拍编造虚假社会热点，浪费公共资源。

二是“伪科普”“伪知识”混淆视听。冒充金融、教育、医疗卫生、司法等领域专业人员，借提供所谓“专业服务”带货卖课，开展不当营销。打着“情感咨询”“婚恋军师”等名义歪曲婚姻观念。

三是传播“软色情”信息。直播过程中衣着暴露，刻意展示带有性暗示或性挑逗的动作，言语挑逗，发布“软色情”“擦边”“泛黄”内容，严重破坏直播生态。通过在直播中展示二维码、在评论区发布联系方式或网址链接等形式违规引流，传播违法和不良信息。

四是扰乱社会秩序，侵犯他人权益。直播互动中污言秽语，拉踩引战、互相挑衅、攻击谩骂，刻意营造冲突对抗氛围，刺激打赏。追逐、拦截、骚扰他人直播搭讪，扰乱公共秩序。使用侮辱性、暴力性、低俗无底线的惩罚方式博眼球、赚流量，违背社会公序良俗，诱导高额打赏。

五是欺骗消费者，销售假冒伪劣商品。炮制虚假粉丝量、浏览量、点赞量和交易量等数据，制造抢单爆款假象。过度渲染商品“功效”，夸大食品、保健用品功能，误导坑害消费者。打着“特供”等旗号销售仿冒假冒商品。（来源：中国网信网）

3. 江西省南昌市网信办通报 2024 年上半年网络管理与执法工作情况

7 月 3 日，江西省南昌市网信办通报 2024 年上半年网络管理与执法工作情况。2024 年上半年，南昌市网信系统不断推进网络综合治理体系建设，强化属地监管，提升网络管理和执法能力，围绕网络安全、数据安全、互联网信息内容监管、个人信息保护四大领域，用好约谈、停更、罚款、关

停四种手段，打好统筹抓总、主动亮剑、协调联动的“组合拳”，始终保持对网络违法违规行为的高压态势，切实营造清朗健康的网络空间。

南昌市网信办针对备案域名涉黄涉赌、低俗不良直播、传播虚假谣言信息等问题依法约谈相关运营主体20家；开展个人信息权益保护专项执法行动。扫码点餐领域，现场检查餐饮类企业33家，点餐系统供应商3家，发现问题75个，下达《责令限期改正通知书》15份；针对自媒体在直播期间散布虚假信息、传播不良导向、语言低俗粗俗等无底线博流量行为，下达《责令限期改正通知书》5份，对多个违法违规账号主体处于7—14天的停更处罚；针对“感染恶意程序并对外发起网络攻击”“大量敏感信息泄露或存在泄露风险”等类型案事件，开具《行政处罚决定书》6份，作出行政警告2起，累计罚没款18万元。

同时，南昌市各县区网信办在网络管理和执法工作上纷纷“亮剑”。如：针对App出现非法获取、超范围收集、过度索取权限等侵害公民个人信息的违法违规行为，南昌县网信办对App开发运营企业作出警告的行政处罚；西湖区、青山湖区、红谷滩区网信办分别约谈属地履行个人信息保护义务不到位的企业；针对履行网络安全保护义务不到位，导致网站被植入非法暗链，青云谱区网信办依法对相关企业进行约谈并责令限期改正。（来源：网信南昌）

4. 江西省南昌市网信办启动“洪城亮剑·个人信息权益保护”专项治理行动

7月4日，江西省南昌市网信办启动“洪城亮剑·个人信息权益保护”专项治理行动，聚焦餐饮外卖、房屋租售、酒店服务、用车服务等社会关注度较高、个人信息被滥用和过度索取乱象突出的领域，采取举报监督、执法检查、跟踪问效、媒体曝光等多种措施，惩戒针对个人信息“过度采、强制要、诱导取、违规用”等问题。

专项治理行动重点整治8类问题：（1）没有隐私政策，或者隐私政策中无收集使用个人信息规则，或者没有通过明显方式提示用户阅读隐私政策等收集使用规则的；（2）没有逐一列出，或者通过其他方法明示收集使用个人信息的目的、方式和范围的；（3）未经用户同意、默认用户同意、强制收集个人信息，或者诱导用户提供个人信息的；（4）违反必要原则，超范围收集、频繁索取个人信息的，或者用户不同意收集非必要个人信息，拒绝提供业务功能的；（5）未经用户同意、也未做匿名化处理，即向第三方提供个人信息，致使用户频繁收到定向推送广告营销信息的；（6）未提供删除、更改个人信息功能，或者未公布投诉、举报方式等信息的；（7）对用户个人信息管理责任不到位、存在泄露风险的；（8）利用互联网各种渠道非法买卖公民个人信息的。（来源：网信南昌）

5. 重庆市网信办启动扫码消费领域个人信息保护专项治理行动

7 月 4 日，重庆市网信办针对消费领域个人信息过度采集、强制收集、诱导索取、违规使用等问题，会同行业主管部门开展为期三个月的个人信息保护专项治理行动。

专项治理行动聚焦停车、餐饮、商超购物三类社会关注度高、个人信息保护问题突出的扫码消费场景，采取举报监督、执法检查、公益诉讼、媒体曝光等多种措施，打击消费场景个人信息过度采集和肆意滥用乱象，整治侵害个人信息权益的违法违规行为。

根据工作掌握的问题线索，专项治理行动重点整治以下 4 类问题：（1）违反“公开”原则，未公开个人信息收集使用规则，未明示收集使用的目的、方式、范围；（2）违反“同意”原则，未经用户同意收集使用个人信息，非法向他人提供个人信息；（3）违反“必要”原则，收集与提供的服务无关的个人信息；（4）违反“安全”原则，未履行保护责任，未对用户个人信息采取必要保护措施，发生个人信息安全事件。（来源：网信重庆）

6. 北京市网信办发布“自媒体”乱象综合治理情况

7 月 11 日消息，北京市网信办近日聚焦优化营商网络环境、清理违法信息外链、打击网络暴力行为、净化未成年人网络环境等重点领域，集中开展“自媒体”乱象综合治理，推动属地网站平台积极履行主体责任，重拳打击“自媒体”账号违法违规行为。6 月以来，督促指导属地网站平台依法依约处置违法违规账号 1.5 万余个。

针对网络信息内容泛在化、网络表达情绪化、网络生态复杂化等网络治理新形势新挑战，北京市网信办指导属地网站平台进一步夯实主体责任，采用内容标注、全链路智能识别等方式加强技术赋能，加大违规“自媒体”典型案例警示公告，强化“自媒体”管理效能。比如抖音等平台发布指导手册要求用户通过剧情演绎方式创作、发布虚构内容时，需在显著位置或以显著形式明确标注相关视频系演绎，同时建立热点当事人仿冒账号核验机制，净化热点流量，打击不择手段蹭炒热点行为；快手等平台针对违法信息外链变体变异快、流窜性强等特点，通过多模型识别治理模式，强化OCR异常内容检测等能力，对账号信息场景、评论场景、视频场景、直播场景等多环节进行违法信息外链全链路的识别打击；新浪微博等平台定期发布公告，针对网络黑产、体育领域“饭圈乱象”等违规“自媒体”典型案例进行通报，警示“自媒体”做好自我管理。

同步围绕严重侵犯企业合法权益类、违法信息外链引流导流类、恶意诽谤实施网络暴力类、不良社交诱骗未成年人类违法行为发布典型案例。（来源：网信北京）

7. 上海市网信办发布属地21款App收集使用个人信息情况

7月30日，上海市网信办发布消息称，2024年4月至7月，上海市网信办对属地21款App开展收集使用个人信息专项检查，共发现80余项问题。经过通报和跟进指导，截至目前，各App运营单位均已完成问题整改。

检查发现常见10种收集使用个人信息问题是：隐私政策内容不完整、强制收集非必要个人信息、收集用户敏感信息未同步告知目的及必要性、

未主动提示用户阅读隐私政策、收集与业务无关的个人信息、收集个人信息的频度超出业务功能实际需要、未公开收集使用规则、注销机制无效、未经用户同意收集个人信息、超范围使用个人信息。（来源：网信上海）

8. 因信息系统存在安全漏洞，湖南省长沙市长沙县网信办对一公司进行处罚

7 月 2 日，湖南省长沙市长沙县网信办依法对长沙某软件开发有限公司作出行政处罚，开出长沙县网络执法首张罚单。

经查，该企业信息系统存在目录遍历等安全漏洞，在多次收到网信部门的网络安全通报后，仍未按照网络安全等级保护制度的要求履行保护义务，存在网络安全风险隐患，违反《网络安全法》第二十一条、第二十五条相关规定。长沙县网信办依据《网络安全法》第五十九条规定，对该企业及相关责任人分别作出罚款一万元和五千元的行政处罚，并督促企业在规定期限内完成整改，切实履行网络安全主体责任。（来源：网信长沙）

（三）通信管理部门治理实践

1. 工信部、多地通信管理局通报问题 APP

（1）工信部

7 月 29 日，工信部信息通信管理局通报 2024 年第 6 批，总第 41 批侵害用户权益行为的 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 17 款 APP 及 SDK 存在侵害用户权益行为，所涉问题包

括APP强制、频繁、过度索取权限，APP频繁自启动关联启动，违规收集个人信息，违规使用个人信息，信息窗口摇一摇乱跳转，强制用户使用定向推送功能等。

（2）江苏省通信管理局

7月17日,江苏省通信管理局通报2024年第1批侵害用户权益的APP。江苏省通信管理局近期组织第三方检测机构对群众关注的省内生活服务、休闲娱乐、实用工具等类型的APP进行检查，并通报相关违规APP主办者限期整改。截至目前，尚有28款APP未反馈整改报告或未完成整改。上述APP开发运营者在7月23日前完成整改，整改落实不到位的，江苏省通信管理局将视情采取下架、关停、行政处罚等措施。

28款APP所涉问题包括强制、频繁、过度索取权限，违规收集、使用个人信息，违规处理个人信息，欺骗误导用户下载APP等。

（3）浙江省通信管理局

7月23日,浙江省通信管理局通报2024年第6批侵害用户权益行为的APP。通报指出，浙江省通信管理局组织第三方检测机构对群众关注的实用工具、运动健身、拍摄美化等类型APP进行检查，并书面要求违规APP开发运营者限期整改。截至目前,尚有11款APP未按要求完成整改。上述APP开发运营者在7月31日前完成整改落实工作，整改落实不到位的，将视情采取下架、关停、行政处罚等措施。11款APP所涉问题包括APP强制、频繁、过度索取权限，违规收集个人信息，违规使用个人信息，超范围收集个人信息等。

（4）北京市通信管理局

7 月 31 日，北京市通信管理局通报 2024 年第七期问题 APP。

一是北京市通信管理局近期通过抽测发现本市部分 APP 存在“违反必要原则收集个人信息”“未明示收集使用个人信息的目的、方式和范围”等侵害用户权益和安全隐患类问题。截至目前，尚有 1 款 APP 未整改或整改不到位，予以公开通报。二是 6 月 30 日，北京市通信管理局通报本市部分存在侵害用户权益行为的 APP 并要求整改。截至目前，仍有 4 款 APP 未整改或整改不到位，予以全网下架处置。

（5）广东省通信管理局

7 月 31 日，广东省通信管理局公开通报 37 款未按要求完成整改 APP。通报称，广东省通信管理局持续开展 APP 隐私合规和数据安全专项整治行动，发出《违法违规 APP 处置通知》责令 APP 运营者限期整改，并通知相关应用商店协助督促 APP 运营者整改。截至目前，尚有 37 款 APP 未完成整改。所涉问题包括强制用户使用定向推送功能，APP 强制、频繁、过度索取权限，APP 频繁自启动和关联启动等。被通报的 APP 应在 8 月 7 日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施。

同日，广东省通信管理局还通报下架 1 款 APP。通报指出，截至通报规定时限，经核查复检，尚有 1 款 APP“美甲帮”未按照要求完成整改反馈，所涉问题为超范围收集个人信息。广东省通信管理局决定对该 APP 予以下架。相关应用商店应立即组织对该 APP 进行下架处理，并举一反三，排查反复出现问题的 APP 开发运营者，严格落实分发平台主体责任，把好上架审核关。广东省通信管理局将对通报 APP 持续跟踪，视情况进一步采取断

开网络、行政处罚、纳入电信业务经营不良名单等后续处理措施。（来源：工信部、浙江省通信管理局、北京市通信管理局、江苏省通信管理局、广东省通信管理局）

2. 两部门开展“网络去NAT”专项工作，进一步深化IPv6部署应用

7月2日，工业和信息化部办公厅、中央网信办秘书局印发《关于开展“网络去NAT”专项工作 进一步深化IPv6部署应用的通知》，旨在加快IPv6规模部署和流量提升。IPv4到IPv4网络地址转换（NAT44）设备是将少量公网IPv4地址转换为较多的私网IPv4地址的网络设备。

通知要求，基础电信企业要认真摸排NAT44设备部署应用情况并建立NAT44设备信息台账，制定“网络去NAT”工作方案和时间表，有序推进全网NAT44设备使用规模逐步降低。工业和信息化部、中央网信办将组织选取部分区域开展“网络去NAT”试点，到2025年7月底前实现试点区域基础电信企业NAT44设备总容量停止增长，主要移动互联网应用（APP）固网侧IPv6流量占比不低于70%。

通知要求强化运行维护，确保网络安全稳定。基础电信企业、互联网企业要科学合理推进“网络去NAT”专项工作，进一步强化网络日常运行维护管理，加强重要指标监测。针对开展IPv6升级改造的网络系统，要持续强化网络安全防护管理，定期开展风险评估，做好重要系统网络安全风险监测预警和应急处置。对于影响范围较大的设备升级、配置变更、服务变

动，要制定预案，加强关键节点性能监测，保障网络安全稳定运行。（来源：工信部）

（四）其他部门治理实践

1. 最高检发布检察机关依法惩治利用网络暴力侵犯企业合法权益典型案例

7 月 28 日，最高人民检察院发布检察机关依法惩治利用网络暴力侵犯企业合法权益典型案例，涉及利用网络敲诈勒索企业、损害商业信誉、寻衅滋事等罪名。

该批典型案例共 5 件，分别是：李某某等人敲诈勒索案，王某某、张某敲诈勒索案，黄某某、吕某某敲诈勒索案，李某某等人损害商业信誉、商品声誉案，刘某某寻衅滋事案。（来源：最高人民检察院）

2. 浙江省发布 2024 浙江网络空间依法治理重点成果

7 月 30 日，浙江省政府新闻办举行 2024 年浙江省“之江净网”网络空间依法治理新闻发布会。发布会指出，今年以来，浙江省聚焦“健全网络综合治理体系，推动形成良好网络生态”，深入开展“之江净网”网络生态治理。网络空间依法治理取得重要成果，主要体现在网络生态治理成效凸显、营商网络环境持续优化、网络法治保障更加坚实三个方面。

网络生态治理成效凸显方面，浙江省围绕网络信息内容安全，各地各部门组织开展“浙里清朗”“清网 2024”、网络市场监管促发展保安全等

系列专项行动，迭代升级“网络直播监测”“浙里心安·互联网信息服务管理”等系统，累计清理有害信息61万余条，处置账号近5万个，发现涉嫌违规线索12万余条、直播风险信息3万余条。今年以来，依法查处“寒假作业丢巴黎”摆拍引流案、“某抖音账号假冒属地文化和广电旅游体育局官方账号”“某‘自媒体’账号直播期间发布自导自演式低俗视频”等一批典型案例。

浙江省围绕网络安全和数据安全，开展民营企业网络安全能力提升行动，累计举办培训693场次，培训企业人员5.1万余人次，举办2024年浙江省网络安全行业职业技能竞赛，强化网络安全人才队伍建设，综合施策提升企业网络安全意识和防护能力；开展“数安之江”重要行业网络数据安全、App违法违规收集使用个人信息等专项行动，举办“数据要素×”大赛浙江分赛，持续推进新技术新应用安全评估、算法安全检查等工作，压实数据安全主体责任。

网络法治保障更加坚实方面，加快《浙江省未成年人保护条例（修订）》《浙江省实施〈中华人民共和国反电信网络诈骗法〉办法》的立法进程；研究制订《重要行业网络数据分类分级指南》，出台《浙江省数据出境自评估索引指南》《浙江省汽车数据处理管理规定》。各地各部门组织开展“浙E执法”“净网”、打击整治网络谣言等系列行动，建设“浙江省文化市场执法在线”平台，累计检查网络文化市场企业1万余家次，侦办网络犯罪案件1200余起，依法查处造谣传谣网民1万余人。（来源：今日浙江）

境外前沿观察：月度速览十则

导读：7 月，《欧盟人工智能法》最终文本正式公布，这是世界上首部此类立法，试图为人工智能监管设定全球标准。《欧盟与日本跨境数据传输协议》正式生效，主要规定缔约双方须承诺以电子方式跨境传输数据，且不得采取禁止或限制缔约双方跨境传输数据的措施。北约发布新版《人工智能战略》，旨在以安全和负责任的方式推进北约内部人工智能技术的使用。

欧盟委员会发布新版《数字十年状况》报告，指出各成员国当下的共同努力尚未达到欧盟的预期目标，在数字技术、高质量连通、企业使用人工智能和数据分析以及半导体生产等方面尚存较大差距。

执法行动方面，俄罗斯政府开展迄今最大规模的非法 VPN 清剿行动，大量知名非法 VPN 几乎全军覆没。因违反个人信息跨境传输规定等，韩国个人信息保护委员会对阿里巴巴全球速卖通处以 19.78 亿韩元罚款和 780 万韩元滞纳金。

微软软件更新导致“蓝屏”等问题，对全球多国包括航空、铁路、医疗、金融、媒体等在内的多领域造成影响。经查，系美国电脑安全技术公司 CrowdStrike 为微软视窗系统发布的软件更新存在“缺陷”，非黑客袭击或网络安全威胁导致，预估影响全球近 850 万台设备。

关键词：数据跨境传输、人工智能法、非法 VPN 清缴、全球蓝屏事件

1. 《欧盟与日本跨境数据传输协议》正式生效

7 月 1 日，欧盟委员会宣布《欧盟与日本跨境数据传输协议》正式生效，同时该协议被纳入《欧盟与日本经济伙伴关系协定》。

跨境数据传输协议主要规定在协定第 8.81 条，即以电子方式进行跨境数据传输。该条款主要规定缔约双方须承诺以电子方式跨境传输数据，且不得采取下列禁止或限制缔约双方跨境传输数据的措施：（1）要求使用缔约方境内的计算机设备进行数据处理；（2）要求在缔约方境内本地化存储或处理数据；（3）禁止在另一方境内存储或处理数据；（4）规定跨境传输数据取决于计算机设备的位置以及数据存储和处理本地化；（5）规定数据跨境传输前须获得批准等。此外，该条款还规定数据跨境传输的例外情形，即可以为实现合法公共政策目的而禁止或限制数据跨境传输。（来源：欧盟委员会）

2. 北约发布新版《人工智能战略》

7 月 10 日，北约发布新版《人工智能战略》，旨在以安全和负责任的方式推进北约内部人工智能技术的使用。新版战略的主要目标是：（1）为北约及其盟国树立榜样，鼓励以负责任的方式发展和使用人工智能，支持盟国的国防和安全；（2）加速人工智能交互能力的发展，强化互操作性；（3）加强对人工智能技术的防护和监控，解决安全使用问题；（4）识别并防范使用人工智能所带来的威胁。

此外，战略还指出对未来人工智能发展的预期：（1）北约正推动一系列符合北约标准和要求的人工智能实际应用，提高北约的数字技术和能力，跟上数字化大趋势；（2）通过北约防务计划过程中的承诺，采取可量化步骤，将高质量数据支持下的人工智能技术整合到盟国军事能力中；（3）建立一支懂得使用人工智能的人才队伍，并通过人工智能人才发展计划提供支持；（4）制定一系列标准、评估模板、审查流程及其他工具，以促进北约负责任使用人工智能；（5）深化北约及其盟国对人工智能机遇和风险影响的理解；（6）构建全北约同盟范围内的人工智能测试、评估、验证和确认体系，以支持负责任使用人工智能系统；（7）通过与合作伙伴、国际组织和学术界的合作，为制定人工智能在国防和安全领域负责任地使用规范和标准做出贡献。（来源：北大西洋公约组织）

3. 《欧盟人工智能法》最终文本正式发布，自 8 月 2 日生效

7 月 12 日，欧盟官方公报正式公布《欧盟人工智能法》最终文本。这是世界上首部此类立法，试图为人工智能监管设定全球标准。

该法遵循“基于风险”的方法，这意味着对社会造成危害的风险越高，规则就越严格。该法旨在促进欧盟单一市场中公共和私营行为者开发和采用安全和值得信赖的人工智能系统。同时，该法还旨在确保尊重欧盟公民的基本权利，并刺激欧洲对人工智能的投资和创新。该法仅适用于欧盟法律范围内的领域，并为部分系统规定了豁免，例如专门用于军事和国防目的以及研究目的的系统。

该法将自 2024 年 8 月 2 日正式生效。根据该法规定，2024 年 11 月 2 日之前，各成员国应指定人工智能监管机构；2025 年 2 月 2 日开始，禁止使用人工智能的清单将在法律生效六个月后适用；2025 年 5 月 2 日之前，欧洲人工智能办公室将发布业务守则。（来源：欧盟委员会）

4. 英国推出《网络安全与弹性法案》，更新国家网络安全法规

7 月 17 日，英国新政府宣布计划推出《网络安全与弹性法案》，更新国家网络安全法规。英国现行法律《网络与信息系统条例》（NIS 法规）根据欧盟命令于 2018 年通过实施，NIS 法规为关键基础设施和基本数字服务提供商制定安全标准。

新法案与 NIS 法规相比，主要更新以下几点：（1）扩大监管范围，以保护更多的数字服务和供应链。数字服务与供应链攻击是网络攻击者日益青睐的攻击对象，新法案将填补防护空白，防止英国关键公共服务部门遭受类似攻击；（2）为监管机构奠定坚实基础，确保实施必要的网络安全措施。措施包括潜在的成本回收机制，为监管机构提供资源，并赋予主动调查潜在漏洞的权力；（3）强制增加事件报告，以便政府能够获得更全面的网络攻击数据，包括组织被勒索赎金的情况。该措施将通过扩大受监管实体必须报告的事件类型和性质，更早察觉到潜在的网络攻击。

目前，尚不清楚该法案将何时提交议会。尽管勒索软件事件在英国持续创下新高，但 NIS 法规对报告门槛设定较高，导致报告数量较低。对于配电网络基础设施，可报告的 NIS 事件必须涉及至少 50000 名客户的计划

外供应损失超过三分钟。影响全国重要的互联网流量DNS解析器的事件将导致该服务的带宽在15分钟或更长时间内下降25%以上。不影响供水的勒索软件攻击也不被视为可报告事件。新法案的出台可能会降低这些门槛，提高网络安全整体标准。（来源：英国总理办公室）

5. 欧盟发布新版《数字十年状况》报告：进展未达到预期目标

7月2日，欧盟委员会发布新版《数字十年状况》报告，全面概述在实现数字十年政策计划（DDPP）为2023年设定的数字目标和指标方面取得的进展。报告指出，各成员国当下的共同努力尚未达到欧盟的预期目标，在数字技术、高质量连通、企业使用人工智能和数据分析以及半导体生产等方面尚存较大差距。

报告基于欧盟各成员国积极采取行动促进数字技术传播且确保公民具备足够数字技能的背景下，呼吁各成员国加强行动，保持斗志为在数字基础设施、企业采用人工智能等方面实现“数字十年”目标而不懈努力。此外，在当前地缘政治格局中，采用和开发新技术对于提高欧洲竞争力至关重要，特别是由于网络安全威胁增加，需要具有更大弹性和更强的安全防护措施。报告强调，成员国和委员会应共同努力，促进建立一个真正有效的数字市场。2023年，欧洲公司对人工智能、云和大数据的采用率远低于75%的数字十年目标。按照目前趋势，到2030年，只有64%的企业将使用云，50%的企业将使用大数据，17%的企业将使用人工智能。实现商业部门的数字化要激励中小企业采用创新的数字工具，并动员私营部门进一步投资高

增长的初创企业。这对于欧洲保持在数据驱动的创新、效率和增长方面的竞争力至关重要。

报告最后指出,成员国必须立即审查和调整其国家路线图,以符合 2024 年 12 月 2 日之前数字十年政策计划的目标。根据 DDPP 的规定，委员会将监测和评估这些政策计划的实施情况，并在 2025 年的下一份《数字十年状况报告》中报告所取得的进展。（来源：欧盟委员会）

6. 俄罗斯开展史上最大规模非法 VPN 清剿行动

7 月 8 日消息,俄罗斯政府近日开展迄今最大规模的非法 VPN 清剿行动,大量知名非法 VPN 几乎全军覆没。应俄罗斯电信监管机构 Roskomnadzor 要求，苹果公司已从其俄罗斯区苹果应用商店下架多达 25 款 VPN 应用，此举针对的是可以访问俄罗斯境内被标记为非法内容的多个应用程序，包括知名 VPN 服务商 NordVPN、ProtonVPN、Red Shield VPN 等。

早在 2017 年 7 月，俄罗斯总统已签署禁止 VPN、代理和 Tor 的相关立法，但直到 2019 年 3 月，当局才开始尝试执行该法。当时，Roskomnadzor 通知了十家 VPN 服务商,要求他们将系统连接到俄罗斯国家信息系统(FGIS),以确保用户无法自动访问被屏蔽的网站。（来源：BleepingComputer）

7. 因涉嫌违反《数字服务法》，X 公司遭欧盟调查

7 月 12 日，欧盟委员会宣布，因涉嫌违反《数字服务法》（DSA），马斯克旗下的 X 公司可能面临高达其全球年营业额 6%的罚款。

欧盟委员会表示，与内容审核、广告相关的透明度和问责制是DSA的核心。对X公司的调查是依据DSA条款，通过审查内部文件、专家访谈以及欧盟数字服务协调员调查三种方式进行，调查时长共计七个月。

欧盟委员会指出X违反DSA的关键点：（1）X平台的相关规则使任何用户都可以轻易获得“已验证账户”的蓝色标记，违反行业惯例。已经有恶意行为者滥用“已验证账户”来欺骗用户；（2）X不符合广告透明度要求，X没有提供可检索且可靠的广告存储库，而是设置访问障碍，使存储库未达到对用户的透明度要求。该设计限制了对在线广告分发带来的新风险进行必要监督；（3）X未能按照DSA中规定的条件向研究人员提供对其公共数据的访问权。X禁止符合条件的研究人员通过抓取等方式独立访问其公共数据。（来源：欧盟委员会）

8. 因违反个人信息跨境传输规定等，韩国PIPC对阿里巴巴全球速卖通处以19.7亿韩元罚款

7月24日，韩国个人信息保护委员会（PIPC）在第13次全体会议上决定，对阿里巴巴全球速卖通（Alibaba.com Singapore E-Commerce Private Limited）处以19.78亿韩元（约合143万美元）罚款和780万韩元（约合5640美元）滞纳金，责令改正并提出改善建议，原因是违反韩国《个人信息保护法》（PIPA）第28（8）条关于跨境传输个人信息规定以及第31（2）条和第38条关于难以行使数据主体权利的规定等。

PIPC 指出，阿里巴巴全球速卖通采用“开放市场”模式，提供在线平台供入驻商家向用户销售商品并从中收取一定比例的产品销售额作为中介费。在此跨境交易过程中，韩国用户的个人信息传输至海外发货卖家，故隐私被侵犯风险日益增加。经调查，PIPC 发现，阿里巴巴全球速卖通向海外中国卖家传输约 18 万名韩国用户的个人信息，且并未向韩国用户告知个人信息传输的目的地国家、接收个人信息的个人或法人的姓名、联系方式等 PIPA 规定的应告知事项，也未在卖家须知中体现应采取的个人信息保护措施。此外，阿里巴巴全球速卖通还通过使会员退出菜单难以查找、账户删除页面以英文显示等方式，增加用户行使 PIPA 下的权利的难度。（来源：韩国个人信息保护委员会）

9. 微软发生全球“蓝屏”事件，系安全技术公司 CrowdStrike 产品缺陷引发

7 月 19 日，微软公司旗下部分应用和服务出现访问延迟、功能不全或“蓝屏”无法访问问题。在全球范围内，许多微软用户反映称搭载 Windows 系统的公司电脑出现“蓝屏”故障，无法正常启动。多国机场、加油站、超市、银行等机构的微软电脑出现严重技术故障。全球数千架次航班取消、数万架次航班延误。

20 日，微软公司介绍，美国电脑安全技术公司“众击”（CrowdStrike）为微软视窗系统发布的软件更新中存在“缺陷”，由此引发的故障据估算

影响全球近850万台安装了该系统的设备。21日，“众击”公司表示已有相当大一部分受影响设备恢复正常运行。

路透社报道称，“众击”公司网络安全防护软件在此次更新时使用了错误的代码，但在审查流程中并未被发现。专家称，为确保用户能得到及时的网络安全保护，安全软件通常会保持高频率的更新，而较高的更新频率，或许是导致“众击”公司未在向用户推出更新前先进行充分测试的原因。有分析师表示，万幸的是，问题出自软件更新，不是由黑客袭击或网络安全威胁导致。（来源：央视网）

10. 国际ERP软件大厂云泄露超7亿条记录，内含密钥等敏感信息

7月25日消息，根据安全研究人员近日最新发现，墨西哥最大的企业资源规划（ERP）技术提供商之一ClickBalance拥有的一个包含7.69亿条记录的云数据库未设置任何密码或安全认证，恶意威胁行为者可以轻而易举地访问这些数据。安全研究人员向WebsitePlanet报告了这一问题。该报告指出，该数据库包含了潜在的敏感信息，如访问令牌、API密钥、密钥、银行账号、税号和381224个电子邮件地址。目前尚不清楚数据库暴露了多长时间，也不清楚是否有其他主体访问过。（来源：安全内参）

行业前沿观察一：2024 网民网络安全感满意度调查样本采集工作圆满收官；2024 年中国网络文明大会将于 8 月举行；多部门发布行动方案，助力行业发展

导读：近日，以“网络安全为人民，网络安全靠人民”为主题的 2024 网民网络安全感满意度调查活动圆满收官，截至 26 日 24 时，全国网民参与答题总样本量达 323.9470 万份，创历史新高，其中主问卷总样本量 130.8402 万份、专题问卷总样本量 193.1068 万份。

国家发展改革委、市场监管总局、生态环境部联合印发《关于进一步强化碳达峰碳中和标准计量体系建设行动方案（2024—2025 年）》，要求加快研制新型基础设施能效标准，加强重点产品和设备循环利用标准研制，鼓励企业利用 5G 等技术手段建立能源和碳排放数据采集和分析系统。

国家发展改革委、国家能源局、国家数据局联合印发《加快构建新型电力系统行动方案（2024—2027 年）》。聚焦近期新型电力系统建设亟待突破的关键领域，提升电网对清洁能源的接纳、配置、调控能力。

2024 年中国网络文明大会新闻发布会在京举行，宣布大会将于 8 月 28 日至 29 日在四川成都举办。

关键词：数字乡村、信息化、工信部、网络安全、网络谣言、网络强国

1. 创新高！2024 网民网络安全感满意度调查样本采集工作以 323 万余份的佳绩圆满收官

在深入学习贯彻党的二十届三中全会精神热潮中，以“网络安全为人民，网络安全靠人民”为主题的 2024 网民网络安全感满意度调查活动于 7 月 17-26 日开展了样本采集工作，面向广大网民征求意见。截至 26 日 24 时，全国网民参与答题总样本量达 323.9470 万份，创历史新高，其中主问卷总样本量 130.8402 万份、专题问卷总样本量 193.1068 万份。为维护网络安全，共建网络文明，全面了解、反映广大网民对我国网络安全状况的感受和看法，向各级党政有关部门开展互联网治理与监管提供详实的网情民意支撑作出了新贡献。

2024 网民网络安全感满意度调查活动（以下简称“2024 调查活动”）覆盖我国 34 个省级行政区以及部分海外地区，百万网民通过填写此次调查问卷，表达了自己上网用网的感受和评价，提出了关于网络安全的诉求、意见、建议，为分析研究 2024 年及未来我国网络空间综合治理和互联网产业发展提供了宝贵且丰富的数据。

作为全球最庞大的网民群体，我国网民们的上网感受如何？他们面临过哪些网络安全问题？他们渴望哪些问题得到解决、哪些网络服务得到改进？他们对于网络空间治理有着什么样的诉求和建议？网络从业人员们对于我国的互联网产业发展又是怎么样的想法？自 2018 年启动开展以来，调查活动每年都在致力于凝聚社会各界力量收集这些意见。

在深入贯彻落实党的二十大精神和积极践行国家“大兴调查研究之风”等部署的大背景下，调查活动在2023年启动了“第二个五年计划（2023-2027）”，进入高质量发展新轨道。

向“新”而行，以“质”致远。2024年作为调查活动“第二个五年计划”实施的奋进之年，在采用新机制和新模式、执行新标准的新里程上，延续了去年第二个五年开局之年的目标和要求，以“更贴近民心、深入一线”的方式开展样本采集工作，以“更高质量开展调查”的要求收录样本数据，最终共收集到323.9470万份网民意见，在突破历史数据新高的同时保障了样本的高质量，并取得系列亮眼的新成果。（来源：网安联）

2. 三部门：利用5G等技术建立能源和碳排放数据采集和分析系统

近日，国家发展改革委、市场监管总局、生态环境部联合印发《关于进一步强化碳达峰碳中和标准计量体系建设行动方案（2024—2025年）》（以下简称《方案》），要求加快研制新型基础设施能效标准，加强重点产品和设备循环利用标准研制，鼓励企业利用5G等技术手段建立能源和碳排放数据采集和分析系统。

《方案》明确了16项重点任务及5方面保障措施。《方案》提出，2025年，面向企业、项目、产品的三位一体碳排放核算和评价标准体系基本形成，重点行业和产品能耗能效技术指标基本达到国际先进水平，建设100家企业和园区碳排放管理标准化试点。2025年底前，研制20项计量标准和

标准物质，开展25项关键计量技术研究，制定50项“双碳”领域国家计量技术规范，关键领域碳计量技术取得重要突破，重点用能和碳排放单位碳计量能力基本具备，碳排放计量器具配备和相关仪器设备检定校准工作稳步推进。

《方案》提出，加快产品能效标准更新升级。对标国际先进水平，修订升级工业通用设备、制冷和供暖设备、办公设备、厨房电器、照明器具产品能效标准，扩大能效产品覆盖范围，加快研制电动汽车充电桩、第五代移动通信（5G）基站设备等新型基础设施能效标准，将高压电机、服务器等产品纳入能效标识管理，研究出台数据中心能效标识实施细则。

加强计量对碳排放核算的支撑保障。制定重点排放单位碳计量器具配备和管理规范，推动企业碳排放计量器具配备。优化相关行业温室气体排放核算和报告指南，强化碳核算数据优先来源于计量器具的要求。充分发挥国家能耗在线监测系统作用，鼓励企业利用第五代移动通信（5G）、区块链等技术手段建立能源和碳排放数据采集和分析系统。按照国家温室气体排放因子数据库建设需求，探索建立国家温室气体排放因子计量实测验证平台。

3.《加快构建新型电力系统行动方案（2024—2027 年）》重磅发布

8 月 6 日，国家发展改革委、国家能源局、国家数据局联合印发《加快构建新型电力系统行动方案（2024—2027 年）》（以下简称《方案》）。

《方案》提出，聚焦近期新型电力系统建设亟待突破的关键领域，提升电网对清洁能源的接纳、配置、调控能力。在 2024-2027 年重点开展 9 项专项行动，推进新型电力系统建设取得实效。

其中包括：

电力系统稳定保障行动：推进构网型技术应用。根据高比例新能源电力系统运行需要，选择典型场景应用构网型控制技术，具备主动支撑电网电压、频率、功角稳定能力，提升系统安全稳定运行水平。

智慧化调度体系建设行动：加强智慧化调度体系总体设计。适应大规模高比例新能源和新型主体对电力调度的新要求，全面推进调度方式、机制和管理的优化调整。研究新一代电力调度系统的基本定义、主要特征、分阶段实现路径、关键技术等内容，加快新型调度控制技术应用，做好调度与电力市场的衔接。

电力系统调节能力优化行动：建设一批共享储能电站；探索应用一批新型储能技术，围绕不同应用场景对爬坡速率、容量、长时间尺度调节及经济性、安全性的需求，探索建设一批液流电池、飞轮、压缩空气储能、重力储能、二氧化碳储能、液态空气储能、钠离子电池、铅炭电池等多种

技术路线的储能电站。通过合理的政策机制，引导新型储能电站的市场化投资运营。

需求侧协同能力提升行动：建设一批虚拟电厂。结合电力保供、新能源发展等需求，利用当地源荷储资源，建设一批虚拟电厂。建立健全虚拟电厂技术标准体系，完善虚拟电厂的市场准入、安全运行标准和交易规则，常态化参与系统调节，提升电力保供和新能源就地消纳能力。

4. 2024 年中国网络文明大会将于 8 月 28 日至 29 日在四川成都举办

7 月 29 日下午，2024 年中国网络文明大会新闻发布会在京举行，宣布大会将于 8 月 28 日至 29 日在四川成都举办。中央网信办副主任、国家网信办副主任杨建文，中央精神文明建设办公室专职副主任胡凯红，四川省委常委、宣传部部长郑莉，以及中国网络社会组织联合会、成都市委负责同志出席发布会，介绍大会有关情况，并回答记者提问。

杨建文表示，党的十八大以来，习近平总书记高度重视网络文明建设，围绕加强网络文明建设、共建网上美好精神家园等作出一系列重要论述，为我们做好工作提供了科学指引，引领和推动网络文明建设取得显著成效。在全党全国深入学习宣传贯彻党的二十届三中全会精神之际，举办本届中国网络文明大会具有特殊重要意义。大会将旗帜鲜明地体现思想引领，着力做好党的二十届三中全会精神的宣传贯彻；聚焦全会部署和社会关切，

精心设置议程；强化成果产出，发布网络文明建设优秀案例、网络文明家风倡议等一批网络文明建设成果；充分调动各方面力量，多视角共同讲好新时代网络文明建设的生动故事。

胡凯红表示，刚刚胜利召开的党的二十届三中全会，对深化文化体制机制改革作出全面部署，要求加快适应信息技术迅猛发展新形势，激发全民族文化创新创造活力。8月下旬，我们将举办2024年中国网络文明大会，这是落实习近平总书记重要讲话精神和党中央决策部署，培育时代新风新貌、提高社会文明程度，建设社会主义文化强国的重要举措。

郑莉介绍，在全国上下深入学习贯彻党的二十届三中全会精神的重要时刻，网络文明领域最高规格的中国网络文明大会，首次进入中西部，将在四川成都召开，这是对四川现代化建设的极大鼓舞和强力支持，也将对中西部网络文明建设起到极大的辐射带动作用。四川正全力以赴、精益求精做好筹备工作。诚邀大家相聚天府之国，共襄网络文明盛会。

本次大会以“弘扬时代精神 共建网络文明”为主题，由中央网信办、中央精神文明建设办公室、中共四川省委、四川省人民政府共同主办，中国网络社会组织联合会、四川省委网信办、四川省文明办、中共成都市委、成都市人民政府联合承办。大会将举办开幕式及主论坛、11场分论坛和“让科技之光点亮网络文明”网络互动引导活动。目前，大会各项筹备工作已基本就绪。

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，举行培训会、学习会、举行创新论坛等，助推网络安全发展。北京市中关村社团第一联合党委所属社会组织党支部书记、主要负责人新质服务力培训班成功举办；广东省网络空间安全协会党支部举行党的二十届三中全会精神学习会；安徽省网络安全协会：2024 智能网联车安全发展与创新论坛成功举办；“新赋能-法治护航科技创新”分论坛圆满落幕；徐州网络公共安防技术协会赴江苏淮海人力资源服务产业园运营公司考察学习；南通市信息网络安全协会举办“构建安全稳定的软件供应链环境——党纪印我心”主题活动；肇庆市计算机学会组织会员企业参加 S-CIO 2024 华南 CIO 大会。

关键词：数字教育、招聘、数据安全、信息安全、网络安全、信息安全、网络强国

1. 北京市中关村社团第一联合党委所属社会组织党支部书记、主要负责人新质服务力培训班成功举办

2024 年 7 月 9 日至 10 日，在北京市总工会、北京市行业协 会商会综合党委、北京市科委、中关村管委会的指导和支持下， 北京市中关村社团第一联合党委所属社会组织党支部书记、主要负责人新质服务力培训班成功举办。

北京市总工会社会联络部一级调研员巫继恒、北京市总工会基层组织建设部副部长张晶晶、北京市总工会职工服务中心社会组织服务部部长李熙靖出席活动。活动由北京市中关村社团第一联合党委书记、中关村社会组织联合会常务副会长兼秘书长戴键主持。北京网络空间安全协会副理事长林勇忠与近 100 名中关村社团党支部书记、会长、秘书长等主要负责人参加活动。（来源：网安联）

2. 广东省网络空间安全协会党支部举行党的二十届三中全会精神学习会

7 月 29 日，广东省网络空间安全协会党支部举行党的二十届三中全会精神学习会，认真学习党的二十届三中全会精神特别是习近平总书记在全会上所作的关于《中共中央关于进一步全面深化改革、推进中国式现代化的决定》的说明和全会《决定》，学习中央宣讲团成员、广东省委书记、

学习贯彻党的二十届三中全会精神省委宣讲团团长黄坤明作宣讲主题报告精神。

学习会以线下线上形式举行。协会党支部书记、副会长林勇忠在线学习；协会党支部专职副书记黄汝锡主持学习会；协会党支部委员黎明瑶与协会党员、预备党员和入党积极分子参加学习。

学习会指出，党的二十届三中全会是在以中国式现代化全面推进强国建设、民族复兴伟业的关键时期召开的一次十分重要的会议。全会的举行，彰显了以习近平同志为核心的党中央将改革进行到底的坚强决心和强烈使命担当，是对新时代新征程举什么旗、走什么路的再宣示，是新的历史起点上进一步全面深化改革、推进中国式现代化的总动员、总部署，对以中国式现代化全面推进强国建设、民族复兴伟业具有重大而深远的意义。（来源：广东省网络空间协会）

3. 安徽省网络安全协会：2024 智能网联车安全发展与创新论坛成功举办

8 月 8 日，由安徽省发展改革委（省汽车办）指导，安徽省网络安全协会主办，新华三信息安全技术有限公司与中国科学技术大学网络空间安全学院联合承办的“智在必行，安全随行——智能网联车安全发展与创新论坛”在中国科学技术大学隆重召开。本次论坛聚焦智能网联车安全技术创

新与实践，汇聚顶尖高校学者、权威机构专家和各方产业领军企业代表，共同探讨智能时代下的车联网安全发展新路径。

高校作为科研创新的前沿阵地，在知识积累、人才培养及基础科学研究方面具备显著优势。作为车联网前沿技术创新探索的高校代表，中国科学技术大学、合肥工业大学从“自动驾驶”和“智能车联网隐私安全”技术研究方面做了主题分享。

合肥市发改委、合肥市委网信办、合肥市工信局、合肥市高新区管委会等相关单位领导出席本次论坛，来自十余个地市级发改委汽车办领导，大众安徽、安凯汽车、江淮汽车等知名车企代表，以及安徽大学、安徽理工大学、合肥大学、蚌埠学院等各大高校嘉宾参加本次活动。（来源：安徽省网络安全协会）

4. “新赋能-法治护航科技创新”分论坛圆满落幕

由上海市信息网络安全管理协会互联网安全法律服务专家委员会出品的“新赋能-法治护航科技创新”分论坛于 8 月 3 日在上海新国际博览中心成功举行。本次分论坛得到了上海法治报、公安部第三研究所网络安全法律研究中心等单位的大力支持。

上海市法学会党组副书记、专职副会长施伟东在致辞中指出，互联网因创新而生、因创新而兴，网络法治工作尤其需要创新，以创新引领网络法治实践，以法治护航科技创新。

上海市公安局网络安全保卫总队政委金黎钢希望以本次分论坛召开为契机，凝聚与会各位专家和嘉宾们的专业优势，群策群力，找到不断提升本市网络安全治理能力的新办法、新路径。

为深化网络强国战略实施，强化网络安全责任体系，上海市信息网络安全管理协会成立了互联网安全法律服务专家委员会，并精心构建了跨领域、跨行业的专家库，依托深厚的专业背景和丰富的实践经验，为企业提供精准高效的法律服务，为网络安全领域的政策制定与社会治理贡献前瞻性的建议与策略。（来源：上海市信息网络安全管理协会）

5. 徐州网络公共安防技术协会赴江苏淮海人力资源服务产业园运营公司考察学习

为了深入贯彻落实习近平总书记关于“科技是第一生产力、人才是第一资源、创新是第一动力”的讲话精神，进一步落实徐州市委书记宋乐伟提出的“打造人才强市，为高质量建设区域中心城市提供坚实支撑”的指示精神，8 月 9 日上午，我协会卜庆亚理事长一行 13 人赴江苏淮海人力资源服务产业园运营公司考察学习。

秉承“为了人才一切，一切为了人才”的宗旨，江苏淮海人力资源服务产业园运营公司作为徐州经济技术开发区重点打造的人力资源龙头企业集聚区，致力于为入园企业提供全面的专业服务和产业发展服务，推动人力资源服务产业的快速发展。通过引进国内外知名人力资源服务机构，产

业园不仅在淮海经济区中处于领先地位，而且成功晋升为省级人力资源服务产业园，全面提升了徐州人力资源服务行业的整体水平。（来源：徐州网络公共安防技术协会）

6. 南通市信息网络安全协会举办“构建安全稳定的软件供应链环境——党纪印我心”主题活动

为深入贯彻落实党中央关于网络安全工作的决策部署，进一步提升各相关单位的“供应链安全意识”，加强网络安全保障，7 月 30 日下午，南通市信息网络安全协会在南通·中关村信息谷举办“构建安全稳定的软件供应链环境——党纪印我心”主题活动。

南通市公安局一级高级警长、南通市信息网络安全协会秘书长张建为本次活动致辞，强调软件供应链安全是网络安全建设的重要内容，党纪学习教育在当今时代具有深远意义，号召参会人员以昂扬的斗志和不懈的努力，共同开创南通网络和数据安全事业发展新局面。

协会会员单位、软件供应链企业、软件应用单位、网络安全服务企业、运营商相关负责同志共计 80 余人参加本次活动，大家认真聆听授课，积极交流，活动取得了良好成效。（来源：南通市信息网络安全协会）

7. 肇庆市计算机学会组织会员企业参加 S-CIO 2024 华南 CIO 大会

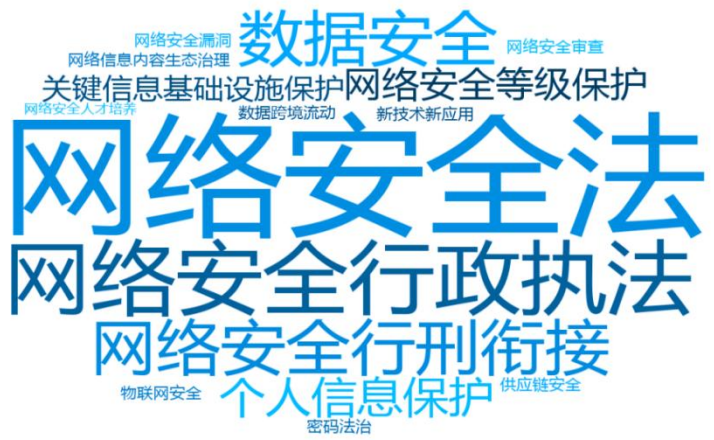
由广州市首席信息官协会、珠海市首席信息官协会、佛山市 CIO 联盟、中山市首席信息官协会、肇庆市信息协会等华南地区二十多个 CIO 组织联合主办的第七届华南 CIO 大会（以下简称：大会）在中国·珠海、隆重召开。

本届大会以"新质驱动、数智未来"为主题，紧扣时代脉搏，聚焦数字经济领域的最新成果与前沿思考，探索数字经济与实体经济的深度融合。大会特邀华为、新加坡工程院、温氏集团、三花控股集团、樊文花、美的集团、广东亚太创新经经济研究院、德赛西威、都市丽人集团、天章集团等（排名不分前后）知名企业/机构的总裁、CIO、专家等，和参会的企业董事长、总经理、首席信息官（CIO）等深入探讨了如何抓住数字经济发展机遇，分层次、多角度地分享了各自在数字化转型中的成功路径、方法、案例实践和成果，助力企业实现高质量发展。（来源：肇庆市计算机学会）

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

1 境内运营中收集和产生的数据传输、存储至境外

2 数据存储在境内，境外的机构、组织或者个人可以访问或者调用

数据出境安全风险评估咨询服务流程

01 情况调研 — 1 - 3 周

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

02 风险评估 — 3 - 5 周

03 指导落实整改 — 周期视情况而定

04 出具风险评估报告 — 1 - 2 周

- 结合客户落实整改情况，出具《数据出境风险评估报告》

合规咨询服务项目

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

典型项目

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

……