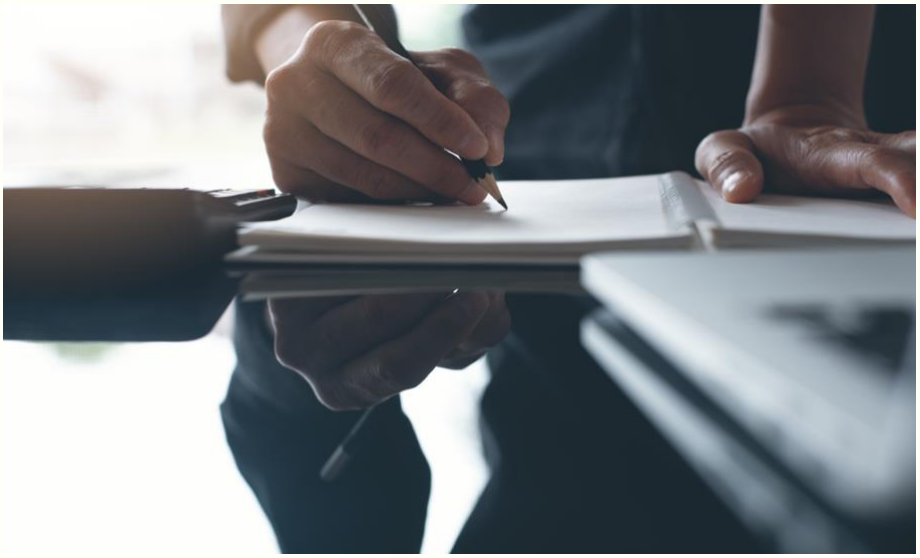
数据合规时事速递
NEWSLETTERS

2022 年 第七期 /总第四十一期



环球律师事务所
GLOBAL LAW OFFICE

2022 年 9 月 21 日

精彩导读

新规速递/ 国家网信办发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》

监管动态/ 全国 SDK 管理服务平台上线试运行

相关新闻/ 谷歌、Meta 未经同意跨平台收集信息，韩国开一千亿罚单

环球解读/对《网络安全法》修订征求意见稿的要点解读

环球律师事务所
GLOBAL LAW OFFICE

前　言

随着《网络安全法》、《数据安全法》、《个人信息保护法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

孟洁丨合伙人律师
直线：86-10-6584-6768
总机：86-10-6584-6688
邮箱：mengjie@glo.com.cn

孟洁律师为环球律师事务所常驻北京的合伙人，主要执业领域为网络安全、个人信息保护、互联网、电商合规、反腐败反商业贿赂合规。孟律师曾在诺基亚等世界五百强跨国公司和知名律师事务所工作超过十余年，担任知名人工智能独角兽公司总法律顾问、DPO。孟洁律师曾经及目前服务于大型跨国公司及知名互联网企业、车企、IoT、电信、云服务、AI、金融、医疗领域企业进行境内/境外的数据合规体系建设与数据合规专项，总结出不少可落地的实操方法论，颇受客户好评。

她被 China Business Law Journal 评为“2022 年度律师新星”；荣登钱伯斯大中华区 2022 年法律指南“数据隐私保护”榜单、“科技、媒体、电信”榜单；被 Legal 500 评为 2020 年“TMT 领域特别推荐律师”；2021 年“TMT 领域领军人物”、“数据保护领域领军人物”、“Fintech 领域头部律师”，被 LEGALBAND 评为“2022 年度顶级律师排行榜：网络安全与数据合规”、“2021 年中国律师特别推荐榜：消费与零售”、“2021 年中国律师特别推荐榜：汽车与新能源”、“网络安全与数据合规特别推荐 15 强”、“2020 年度 LEGALBAND 中国律师特别推荐榜 15 强：网络安全与数据合规”，被北京市律协评为全国千名涉外专家律师。在各大期刊、公号发表过数百篇专业文章、著作，例如有《SDK 安全与合规白皮书》，《个性化展示安全与合规报告》、《Cookie 合规指引报告（2021）》、《国内外标准兼容下的个人信息合规体系构建》等。

许国盛丨资深顾问
直线：86-010-6584-9306
手机：86-185-1085-6288
邮箱：xuguosheng@glo.com.cn

许国盛律师在金融服务与电信领域与合规官以及企业高管有丰富的合作经验。作为迪堡与诺基亚中国的前区域合规总监，许律师在数据保护规制以及中国监管事项方面有着多年经验。除此之外，他也经常协助跨国企业进行敏感的内部调查、监管检查、数据完整性问题检查以及应对政府执法。许律师曾负责管理整合来自不同国家的合规项目，并熟悉美国、欧盟以及亚洲国家的复杂法律法规。

许律师对如何运行合规项目有着极其深入的了解。在环球，许律师曾为客户的海外扩张提供数据合规方面的建议，包括国际数据隐私政策的本地化，员工或客户数据出境和共享，以及数据泄露的管理与向监管机构的自我报告等。许律师亦是《全球化与隐私保护指南（2020）》以及《GB/T 35273 与 ISO/IEC 27701 比较报告（2020）》的合著者。

本团队专门致力于为客户提供全面且专业的法律服务，包括以下业务领域：

- 网络安全与数据合规
- 互联网与电商合规
- 个人信息保护
- 反腐败/反商业贿赂合规

目录

新规速递

1. 国家网信办就《关于修改〈中华人民共和国网络安全法〉的决定》公开征求意见

9 月 12 日，国家网信办就《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（“下称《征求意见稿》”）向社会公开征求意见，意见反馈截止于 9 月 29 日。

《征求意见稿》拟对《中华人民共和国网络安全法》作如下修改：

一是完善违反网络运行安全一般规定的法律责任制度。结合当前网络运行安全法律制度实施情况，拟调整违反网络运行安全保护义务或者导致危害网络运行安全等后果的行为的行政处罚种类和幅度。

二是修改关键信息基础设施安全保护的法律责任制度。关键信息基础设施是经济社会运行的神经中枢，为强化关键信息基础设施安全保护责任，进一步完善关键信息基础设施运营者有关违法行为行政处罚规定。

三是调整网络信息安全法律责任制度。适应网络信息安全工作实际，对违反网络信息安全义务行为的法律责任进行整合，调整了行政处罚幅度和从业禁止措施，新增对法律、行政法规没有规定的有关违法行为的法律责任规定。

四是修改个人信息保护法律责任制度。鉴于《中华人民共和国个人信息保护法》规定了全面的个人信息保护法律责任制度，拟将原有关个人信息保护的法律责任修改为转致性规定。[1]

《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》全文请参见：

http://www.cac.gov.cn/2022-09/14/c_1664781649609823.htm

[1] 国家网信办官网。

2. 三部门联合发布《互联网弹窗信息推送服务管理规定》

9 月 9 日，国家互联网信息办公室、工业和信息化部、国家市场监督管理总局联合发布《互联网弹窗信息推送服务管理规定》（以下简称“《规定》”），自 2022 年 9 月 30 日起施行。

《规定》明确，互联网弹窗信息推送服务，是指通过操作系统、应用软件、网站等，以弹出消息窗口形式向互联网用户提供的信息推送服务；互联网弹窗信息推送服务提供者，是指提供互联网弹窗信息推送服务的组织或者个人。

《规定》要求，互联网弹窗信息推送服务提供者应当落实信息内容管理主体责任，建立健全信息内容审核、生态治理、数据安全和个人信息保护、未成年人保护等管理制度。

《规定》还强调，互联网弹窗信息推送服务提供者应当遵守优化推送内容生态、强化互联网信息服务资质管理、规范新闻信息推送、科学设定推送内容占比、健全推送内容审核流程、强化用户权益保障、合理算法设置、规范广告推送、杜绝恶意引流等九个方面要求。[2]

《互联网弹窗信息推送服务管理规定》全文请参见：

http://www.cac.gov.cn/2022-09/08/c_1664260384702890.htm

3. 国家网信办就《网信部门行政执法程序规定》公开征求意见

9 月 8 日，国家网信办就《网信部门行政执法程序规定（征求意见稿）》（以下简称“《规定》”）公开征求意见，征求意见截止日期为 10 月 8 日。

《规定》要求，网信部门实施行政处罚，应当遵循公正、公开的原则，坚持处罚与教育相结合，做到事实清楚、证据确凿、适用依据准确、程序合法、处罚适当、执法文书使用规范。网信部门应当加强

[2] 国家网信办官网。

执法队伍和执法能力建设，建立健全执法人员培训、考试考核、资格管理和持证上岗制度。

《规定》提出，网信部门应当依法以文字、音像等形式，对行政处罚的启动、调查取证、审核、决定、送达、执行等进行全过程记录，归档保存。网信部门应当建立健全对行政处罚的监督制度，实施行政处罚应当接受社会监督。公民、法人或者其他组织对网信部门实施行政处罚的行为，有权申诉或者检举；网信部门应当认真审查，发现有错误的，应当主动改正。[3]

《网信部门行政执法程序规定（征求意见稿）》全文请参见：

http://www.cac.gov.cn/2022-09/08/c_1664174174624227.htm

4. 国家网信办等发布《数据出境安全评估申报指南（第一版）》

8 月 31 日，为贯彻落实 9 月 1 日起正式生效的《数据出境安全评估办法》（以下简称“《办法》”），国家互联网信息办公室发布《数据出境安全评估申报指南（第一版）》（以下简称“《指南》”）。

《指南》在《办法》的基础上进一步明确了数据出境安全评估的适用范围、申报方式及流程、应当提交的申报材料以及申报咨询的官方渠道，并提供了数据出境安全评估申报书模板以及数据出境风险自评估报告模板等附件，以指导和帮助数据处理者规范、有序申报数据出境安全评估。

《指南》明确数据出境行为的具体情形，细化了省级网信办和国家网信办的两级分工，明确了数据出境安全评估的申报材料及要求，为数据处理者申报时需要准备的材料提供了模板。此外，《指南》还提供了网信办官方的申报咨询方式。[4]

[3] 法治日报。
[4] 国家网信办官网。

在全国性的《指南》发布之后，全国多个地区也陆续发布了本地区申报指南及咨询方式，目前已发布指南的有江苏省及浙江省。此外，河北、北京、上海、天津等地网信办也陆续公开咨询电话。

《数据出境安全评估申报指南（第一版）》全文请参见：

http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm

5. 国家卫健委发布《医疗卫生机构网络安全管理办法》

8 月 29 日，国家卫生健康委、国家中医药局、国家疾控局印发《医疗卫生机构网络安全管理办法》（以下简称“《办法》”），自印发之日起实施。《办法》明确了各医疗卫生机构网络及数据安全管理基本原则、管理分工、执行标准、监督及处罚要求，体现了统筹安全与发展的总体平衡，为医疗卫生机构指明了网络安全管理的总方向。

《办法》全文贯穿了全生命周期管理的主导思想。在网络安全方面，围绕信息系统全生命周期，提出落实等级保护制度、监测预警、应急实战、安全整改、人员管理、新技术应用、密码安全、医疗设备、供应链管理等方面的要求；在数据安全方面，以保障数据的机密性、完整性、可用性为目标，要求采取数据加密、数据备份、数据脱敏等技术，加强数据收集、传输、存储、使用、交换、销毁等全生命周期的安全防护。在实际运用中，应基于网络和数据的全生命周期视角，梳理安全策略架构，识别具体业务场景，有针对性的设计安全措施，实现安全防护。

《办法》强调医疗卫生机构安全管理应围绕顶层设计和制度保障两个要点着力推进。顶层设计方面，在整体网络安全体系的基础上，依据数据的特性建构网络和数据安全顶层设计，落实安全责任分工，明确数据管理部门、业务部门、信息化部门在网络和数据安全管理工作中的权责。制度保障方面，《办法》明确医疗卫生机构应建立健全安全管理制度、操作规程及技术规范。在执行过程中，应密切结合自身业务模式的变更，及时修订完善制度要求，保持网络和数据安全制度的有效执行力及充分协同。

《办法》要求建立网络安全管理制度体系，加强网络安全防护，通过管理和技术手段保障数据安全和数据应用的有效平衡。在实际运用中，应将总体安全策略拆解到具体安全管理要求，并通过安全技术实现管理要求，最终融入对应到安全运营体系中，形成融合管理、技术、运营三位一体的立体化网络安全管理模式。

《办法》指出要建立防护、监测、处置、保障四个体系协同的综合防控格局。在安全防护方面，要求建立“实战化、体系化、常态化”的安全防护体系；在安全监测层面，鼓励三级医院探索态势感知平台建设，及时收集、汇总、分析各方网络安全信息，并与国家及行业平台对接；在安全处置方面，要形成监督管理、安全检查、应急预案、联防联控协同体系；在安全保障方面，通过统筹领导和规划设计，在人才培养、安全培训、经费支持等方面实现全方位保障。[5]

《医疗卫生机构网络安全管理办法》全文请参见：

http://www.gov.cn/zhengce/zhengceku/2022-08/30/content_5707404.htm

6. 自然资源部发布《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》

8 月 30 日，自然资源部发布《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》（以下简称“《通知》”），明确测绘地理信息数据采集和管理等相关法律法规政策在智能网联汽车（包括智能汽车、网约车、智能公交以及移动智能配送装置等）相关活动中的适用问题。

《通知》明确，目前已在提供智能网联汽车售后和运营服务的企业，存在向境外传输相关空间坐标、影像、点云及其属性信息等测绘地理信息数据行为或计划的，应严格执行国家有关法律法规，依法履

[5] 国家卫健委官网。

行对外提供审批或地图审核程序等，在此之前应停止数据境外传输行为。

《通知》指出，当前，智能网联汽车（包括智能汽车、网约车、智能公交以及移动智能配送装置等）新业态迅猛发展，为方便出行、减少污染、改善交通提供了有效的解决方案，具有广阔的市场前景，同时其运行和服务高度依赖实时的高精度坐标、高清影像等数据支持。

为统筹发展与安全，在守牢安全底线的前提下，积极扶持智能网联汽车新技术、新业态的发展，扩大内需、促进消费，《通知》就测绘地理信息数据采集和管理等相关法律法规政策的适用与执行问题进行明确。[6]

《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》全文请参见：

http://gk.mnr.gov.cn/zc/zxgfxwj/202208/t20220830_2757960.html

7. 信安标委就国标《信息安全技术 网络数据分类分级要求》公开征求意见

9 月 14 日，全国信息安全标准化委员会就国标《信息安全技术——网络数据分类分级要求》（以下简称“《要求》”）公开征求意见，征求意见截止日期为 11 月 13 日。

《中华人民共和国数据安全法》明确规定“国家建立数据分类分级保护制度”，而《要求》的设立正是为了支持数据分类分级保护工作的开展。《要求》给出了数据分类分级的原则和方法，用于指导各行业、各领域、各地方、各部门和数据处理者开展数据分类分级工作。

《要求》全文包括前言、引言、正文和 8 个附录，正文分为范围、规范性引用文件、术语与定义、基本原则、数据分类框架和方法、数据分级框架、数据分级确定方法、数据分类分级实施流程；附录分为

[6] 自然资源部官网

基于数据描述对象的行业领域数据分类参考示例、数据分级要素识别常见考虑因素、影响对象考虑因素、影响程度参考示例、衍生数据定级参考、动态更新情形参考、一般数据分级参考、个人信息分类示例。

《信息安全技术 网络数据分类分级要求》（征求意见稿）全文请参见：

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220914180530&norm_id=20211108000024&recode_id=48416

8. 上海经信委就《公共数据开放实施细则》公开征求意见

9 月 13 日，上海市经济信息委员会就《上海市公共数据开放实施细则（征求意见稿）》（以下简称“《细则》”）公开征询意见，征求意见截止日期为 10 月 12 日。

《细则》由上海市经济和信息化委员会起草，旨在贯彻落实《上海市数据条例》《上海市公共数据开放暂行办法》等有关法律法规，加快推进上海市公共数据更高水平开放。

《细则》共七章三十八条，主要规定了以下内容：（一）创新开放机制。明确制定开放年度计划、开展需求征集、建设示范项目，明确了场景要求、数据安全要求等开放条件，并将建立质量评估机制；（二）细化数据获取流程。主要包括材料告知、数据申请、申请处理与审核、签订数据协议、数据交付等；（三）鼓励数据利用。鼓励创新利用方式，鼓励数据产品进入流通交易市场，并将支持形成优秀成果名录、加强复制推广，鼓励数据赋能公共服务等。

《上海市公共数据开放实施细则（征求意见稿）》全文请参见：

http://sheitc.sh.gov.cn/gg/20220914/5b58744a4f4740fb8da5d003cd9b6d23.html

9. 《深圳经济特区人工智能产业促进条例》公布

我国首部人工智能产业专项立法——《深圳经济特区人工智能产业促进条例》（以下简称“《条例》”）经深圳市第七届人民代表大会常务委员会第十一次会议于 8 月 30 日通过，于 9 月 5 日公布，自 11 月 1 日起正式施行。

为破解人工智能产品落地难问题，《条例》提出创新产品准入制度，对于国家、地方尚未制定标准但符合国际先进产品标准或者规范的低风险人工智能产品和服务，允许通过测试、试验、试点等方式开展先行先试。

《条例》是全国首部人工智能产业专项立法，共设七章七十三条，包括总则、基础研究与技术开发、产业基础设施建设、应用场景拓展、促进与保障、治理原则与措施、附则等七个方面，从深圳人工智能产业发展实际出发，围绕“明确范围+补齐短板+强化支撑+抢抓应用+集聚发展+规范治理”等环节进行探索创新。其主要内容包括：（一）明确人工智能及人工智能产业的界定；（二）建立人工智能统计与监测制度；（三）补齐人工智能基础研究短板；（四）加强人工智能产业基础设施建设；（五）充分发挥应用场景驱动作用；（六）确立人工智能治理机制。[7]

《深圳经济特区人工智能产业促进条例》全文请参见：

http://www.szrd.gov.cn/rdlv/chwgg/content/post_834228.html

10. 上海市发布《上海市加快智能网联汽车创新发展实施方案》

9 月 5 日，上海市人民政府办公厅发布关于印发《上海市加快智能网联汽车创新发展实施方案》（以下简称“《方案》”）的通知。《方案》于 8 月 23 日印发，提出要坚持“创新引领、协同有序、需求牵引、包容开放”4 项基本原则。

[7] 深圳政府官网。

《方案》提出，到 2025 年，上海市初步建成国内领先的智能网联汽车创新发展体系。核心技术研发取得重大进展，核心装备初步实现自主配套。大规模、多场景、高等级、多车型应用初具规模，智慧交通生态加速融合。智慧道路基础设施实现重点区域覆盖，基本满足车路协同、智慧交通、智慧出行应用需求。规则、标准、监管体系实现突破优化，基本建成系统完善的智能网联汽车管理体系。

《方案》分为总体要求、重点任务、保障措施三部分，针对数据安全与数据利用提出坚持政府引导、推动数据信息等要素集聚、充分调动社会各界积极性、建立开源开放、资源共享合作机制等要求。[8]

《上海市加快智能网联汽车创新发展实施方案》全文请参见：

https://www.shanghai.gov.cn/nw12344/20220905/a6882b588ee14f1683d7b6873e668732.html

11. 瑞士新修订的《数据保护法》于 9 月 1 日正式生效

根据瑞士联邦委员会于 8 月 31 日的决定，全面修订的《数据保护法》（Data Protection Act）以及新《数据保护条例》（Data Protection Ordinances）和《数据保护认证条例》（Data Protection Certifications）（以下简称“《条例》”）中的实施条款将于 2023 年 9 月 1 日生效。在这段时间内，商业实体将有充分时间采取必要的措施来遵守新的法律。

对《数据保护法》和对《条例》相关条款的全面修订将确保更好地保护个人数据。该项立法适应了科技的进步，使个人对其数据的权利能得到充分保护，并且显著提升了数据收集方式的透明度。

联邦委员会在多个方面调整了《数据保护条例》。其中，彻底修改了关于数据控制者义务的章节：免除了私人数据控制者某些和个人数据传输通知有关的义务；免除了对于拒绝、限制或推迟传输原因的记录义务，由此访问权的行使方式被大大简化。联邦委员会还将数据处理的日志报告保留期调整为至少一年，并增加了一项新的规定，旨

[8] 安全内参。

在将数据安全保护目标与 2020 年 12 月 18 日有关信息安全的新联邦法的目标相协调。

该新法律确保了与欧盟法律的兼容性，并允许瑞士批准欧洲委员会关于数据保护的第 108 号公约（修订版）。此后，欧盟将继续承认瑞士是拥有充分数据保护水平的第三国，跨境数据交换仍然可以在不增加额外要求的情况下进行。[9]

[9] GDPR buzz.

环球律师事务所
GLOBAL LAW OFFICE

监管动态

1. 全国 SDK 管理服务平台上线试运行

软件开发工具包（SDK）是移动互联网应用程序用户权益保护全链条中的关键一环，SDK 在为 APP 开发者带来便利性的同时，也面临选择配置功能不完善、处理个人信息不规范等问题。

为提升 SDK 合规水平和服务能力，中国信通院在工业和信息化部的指导下，牵头搭建了全国 SDK 管理服务平台（sdk.caict.ac.cn），为 SDK 和 APP 开发运营者提供 SDK 政策标准发布、产品信息公示、监管问题处置、用户使用反馈等服务。同时，平台作为移动互联网应用程序检测及认证公共服务平台中的重要组成部分，将逐步建成开放的 SDK 个人信息保护技术检测服务能力。

目前已有 50 余家企业的 400 余款 SDK 向平台报送产品信息，涵盖广告类、支付类、安全风控类、第三方登录类等 15 个 SDK 类型，公示信息包括 SDK 名称、版本、隐私政策、接入文档、开发者、官网信息等内容。

据悉，公示服务汇总公示广告类、安全风控类、地图类、第三方登录类、支付类、认证类、社交类、客服类、框架类、实时音视频类、统计类、推送类、性能监控类、人工智能类、平台服务类等 15 类共 322 款 SDK 信息，包括 SDK 名称、类型、收费性质、基本介绍、支持平台、开发者、版本、官网信息及 SDK 隐私政策、SDK 接入文档。[10]

2. 最高法发布电信网络诈骗犯罪及其关联犯罪典型案例

9 月 6 日，最高人民法院召开新闻发布会，通报人民法院依法惩治电信网络诈骗犯罪的相关工作情况，同时发布十起电信网络诈骗犯罪及其关联犯罪典型案例。

此次发布的典型案例，包括“被告人易扬锋、连志仁等三十八人诈骗、组织他人偷越国境、偷越国境、帮助信息网络犯罪活动、掩饰、

[10] 中国通信院官方微信账号。

隐瞒犯罪所得案”“被告人罗欢、郑坦星等二十一人诈骗案”“被告人施德善等十二人诈骗案”“被告人陈凌等五人侵犯公民个人信息案”“被告人隆玖柒帮助信息网络犯罪活动案”等十起。

最高法刑三庭庭长马岩介绍，此次发布的典型案例打击重点突出。马岩介绍，当前，电信网络诈骗犯罪境外作案占比达80%，跨境电信网络诈骗犯罪案件社会危害更重，打击难度更大。人民法院打击电信网络诈骗犯罪的首要原则是从严惩处，而从严惩处的“重中之重”，正是跨境电信网络诈骗犯罪，特别是对于跨境电信网络诈骗犯罪集团首要分子和骨干成员，必须用足用好现有法律武器，坚决依法从严惩处，最大限度彰显刑罚的功效。例如，此次发布的“被告人易扬锋、连志仁等三十八人诈骗、组织他人偷越国境、偷越国境、帮助信息网络犯罪活动、掩饰、隐瞒犯罪所得案”，法院认定系跨境电信网络诈骗犯罪集团，对该集团的首要分子、骨干成员，以及为该集团提供支付结算帮助和转移赃款服务的犯罪分子，均依法予以严惩，集团首要分子易扬锋被依法判处无期徒刑。[11]

3. 北京市通信管理局通报41款问题App

9月5日，北京市通信管理局依据《网络安全法》《数据安全法》《个人信息保护法》《网络产品安全漏洞管理规定》等法律法规，组织第三方检测机构对北京地区App开展技术检测工作。检测后通报41款存在侵害用户权益和安全隐患等问题的App，并要求相关App运营企业立即进行整改并于9月15日前提交整改报告。逾期仍整改不到位的，北京市通管局将依法依规予以处置。

41款App主要来源于vivo应用商店、华为应用市场等手机厂商内置软件下载平台，涵盖“最美证件照”等拍照修图类App，“灵兰中医”等医疗保健App，“Keep”、“薄荷轻断食”等健身类App等。通报问题涉及未经用户同意收集使用个人信息、强制用户使用定向推送功能、未明示收集使用个人信息的目的、方式和范围、账号注销困难、App强制、频繁、过度索取权限等。[12]

[11] 最高人民法院官网。
[12] 北京通信管理局官网。

4. 湖北省持续开展网络数据安全专项检查

9月7日，从省通信管理局数据安全政策标准宣贯培训会上获悉，湖北省将用“严标准”建立数据安全管理制度，用“高标准”建设数据安全技术能力，并持续开展电信和互联网行业网络数据安全专项检查，确保“数字湖北”持续安全稳定运行。

当前，数据安全问题日益凸显，数据泄露事件逐年增长，数据安全问题影响范围从个人权益、企业利益辐射到产业安全甚至国家主权。2021年，我国违规采集个人信息、勒索攻击、数据泄露等在数据安全事件中占比达78%。

省通信管理局数据显示：从去年11月至今，湖北省工业互联网安全监测与态势感知平台，监测发现被攻击事件涉及1964家企业。较为集中的行业分别为汽车制造业（占比22%），软件和信息技术服务业（占比16%），研究和试验发展行业（占比7%），批发业（占比5%），专业技术服务业（占比5%）。从地域分布看，分别为武汉（占比76%）、宜昌（占比8%）、荆门（占比3%）、襄阳（占比3%）、十堰（占比3%）。

湖北省通信管理局表示，“安全发展、标准先行”，我省通信行业将以贯标工作为抓手和切入点，在5G、云计算、车联网、物联网等重点领域推进数据安全标准体系建设，并持续开展电信和互联网行业网络和数据安全检查，强化行业风险防范及主体责任落实，促进湖北网络和数据安全工作再上新台阶。[13]

5. 北京开展2022年工业互联网企业网络安全分级分类管理工作

近日，北京市经济和信息化局、通信管理局联合发布《关于开展2022年工业互联网企业网络安全分类分级管理工作的通知》（以下简称“《通知》”）。

[13] 湖北省人民政府网站。

《通知》明确，到2022年底，组织50家以上代表性企业开展网络安全分类分级管理工作，进一步完善定级核查、风险评估、整改落实等工作机制，提升企业网络安全防护水平；初步建成北京市工业互联网企业网络安全分类分级管理体系，建立管理名录，培育遴选一批分类分级管理典型解决方案和优秀示范企业，持续加强工业互联网安全保障体系能力建设。

本次分类分级管理工作依托全国工业互联网企业网络安全分类分级管理服务平台组织实施。本次工作流程主要包括企业自主定级、组织定级核查、落实防护要求、开展评估整改、组织安全抽查、开展工作总结。《通知》随附件发布了《工业互联网企业网络安全分类分级管理指南（试行）》、《防护系列规范（试行）》及相关信息表。[14]

《关于开展2022年工业互联网企业网络安全分类分级管理工作的通知》全文请参见：

http://jxj.beijing.gov.cn/jxdt/tzgg/202209/t20220909_2812188.html

6. 英国电信公司面临严厉网络安全新规

英国定于10月出台的严厉政府新规规定，若在保护网络免遭攻击方面未遵循行业最佳实践，电信公司将面临高达营业额10%的罚款。

8月30日，英国数字、文化、媒体和体育部（DCMS）发布公告称，“新的电信安全法规将成为世界上最严格的法规之一”，将为英国提供更严格的保护，使英国免遭网络威胁，防止网络故障或敏感数据被盗。根据现行立法，电信公司自我监管其网络安全标准，但近期电信供应链审查发现，在网络安全方面，供应商毫无动力采用最佳安全实践。

新法规包括由英国国家网络安全中心（NCSC）和英国通信管理局（OFCOM）制定的行业行为规范，旨在规定运营商应采取的具体行动，确保其遵守并履行该法案规定的法律职责。作为《电信（安全）法案》的一部分，新法规赋予政府制定移动和宽带网络安全标准的权

[14] 北京市经信局官网。

力，涵盖处理互联网流量和电话呼叫的基站和电话交换机里的硬件和软件。

负责监督和执行新行为准则的是英国通信管理局，该部门有权检查营业场所和各个系统，确保其合规。如果有公司未能达到标准，最高可处以营业额 10%的罚款。如果持续违反此项法律，公司可能面临高达每日 10 万英镑的罚款，一直罚到问题得到解决。

运营商应识别和评估直接暴露给潜在攻击者的任何“边缘”设备所面临的风险，包括无线基站和提供给客户的调制解调器和 Wi-Fi 路由器等互联网设备。运营商还需要严格控制谁可以做出全网更改，并防止恶意信令进入网络而导致中断。公司层面上也需有所投入，包括通过适当的董事会级责任确保业务流程支持安全等。

尽管该立法于 10 月生效，但供应商必须在 2024 年 3 月之前确保已实现上述所有目标。一旦落实到位，将有进一步的时间表供未来采取其他措施保护网络基础设施。[15]

[15] 安全内参。

环球律师事务所
GLOBAL LAW OFFICE

相关新闻

1. 美方将审计中概股，互联网巨头将首批接受审计底稿检查

根据中美在 8 月底就中概股审计达成的审计监管合作协议，中国证监会将安排在美上市的中国公司及其会计师事务所将其审计底稿和其他数据从内地转移到香港，在 9 月中旬接受美方检查。

美国 2020 年年底出台的《外国公司问责法》规定，在美上市的中概股如果连续三年未能提交美国公众公司会计监督委员会（PCAOB）所要求的报告，美国证券交易委员会（SEC）有权将其从美国的交易所摘牌。迄今为止已有超过 160 家中国公司被 SEC 认定未遵守美国的审计规则，其中包括中国互联网巨头阿里巴巴、京东和拼多多。美国证监会网站显示，9 月 14 日，又一家中概股公司被列入“预摘牌”名单。此次中美在审计监管的合作被认为是在美上市的中概股迎来的重要转机。

根据美国《华尔街日报》9 月 16 日的报道，SEC 主席加里·根斯勒披露，美国 PCAOB 的工作人员预计将于 9 月 19 日开始检查在美上市中概股的审计底稿。根斯勒在参议院银行委员会听证会上称，整个过程需要 8 到 10 周，或在 2022 年 12 月初得出检查结果。他还表示，中方监管机构表示会遵守协议规定。[16]

2. 买卖微信账号侵犯公民个人信息，法院认定合同无效且违法

9 月 5 日，中国法院网公布一起微信账号买卖合同纠纷案判决结果，法院认定买卖微信账号构成买卖他人个人信息，合同无效，且涉嫌侵犯公民个人信息罪。

本案原告程某系一网红医美顾问，曾为发展粉丝以自己或他人名义注册多个微信账号，每个账号内均包含大量微信好友。本案被告赵某经营医美项目，希望以 50 万元向程某购买微信账号，以获取潜在客户并进行商业推广，但被告赵某并未在约定的时间缴纳中期款项 10 万元，因此原告程某向法院起诉，要求赵某支付全部尾款及逾期利息。

[16] 环球网。

法院在审理中追加了腾讯公司作为第三人，三方就买卖合同是否有效及买卖账号行为的性质进行了辩论。

法院认为，微信账号承载了使用者个人特有的可识别信息和微信好友的大量个人信息，买卖微信账号构成了买卖他人个人信息，进而认定微信账号买卖合同无效。法院不仅驳回了原告程某的全部诉讼请求，还因程某的行为涉嫌侵犯公民个人信息罪而将相关线索移送公安机关侦查。[17]

3. 工信安全中心发布《2022 年数据交易平台发展白皮书》

9 月 2 日，国家工业信息安全发展研究中心（以下简称中心）信息政策所数字经济研究室发布了智库成果洞察系列报告《2022 年数据交易平台发展白皮书》（以下简称《白皮书》），从成立时间、所在区域、注册资本、盈利模式、技术应用等多个角度对我国数据交易平台进行分析和比较，探究了其发展现状，发展趋势，分析了发展中面临的问题，提出了对策建议。

《白皮书》指出，我国数据交易平台经历了两大发展阶段，第二波平台建设浪潮方兴未艾。平台的注册资本多数介于 5000 万至 1 亿元间，华东、华南、华中地区为主要集聚地。各大平台形成了佣金收取、会员制、增值式交易服务等多种盈利模式。

从发展趋势上看，数据产权制度日趋受到关注，各大数据交易平台将以数据登记、技术赋能数据权益使用等多种形式探索破解数据确权难题。数据应用场景不断拓展，参与交易流通的数据类型从金融数据将逐步扩展到医疗、交通、工业等多种类型的数据。隐私计算等技术加速应用，将进一步助力数据要素安全流通。公共数据日益成为交易平台数据的重要供给源，而数据交易平台也彰显出越来越大的公共价值，开始反哺数据产业发展。数据交易上下游产业链开始浮现，有望在未来形成商业生态。

[17] 中国法院网。

然而，我国数据交易平台在不断发展的同时，也仍然面临数据产权不清、数据交易活跃度不高、新技术支撑不充分、出现平台同质化竞争苗头等问题。

针对这些问题，《白皮书》建议加强统筹布局，推动各数据交易机构错位发展；结合各地数据资源禀赋，建立数据交易良好发展生态；加大技术研发，建立统一规范的标准体系；完善数据基础制度，推动数据高质量供给。[18]

《白皮书》详细内容请见：

https://www.secrss.com/articles/46611

4. 因不当处理未成年人个人信息，Meta 被罚 4.02 亿美元

9 月 5 日，因允许 13 岁至 17 岁的用户在该平台上操作商业账号，并默认公开显示用户的电话号码和电子邮件地址，Meta 旗下社交平台 Instagram 被爱尔兰数据保护委员会（DPC）处以 4.05 亿欧元罚款。据悉，这是 Meta 迄今收到的最大《通用数据保护条例》（GDPR）罚单，数额超越了旗下另一软件 WhatsApp 在去年 9 月被处以的 2.25 亿欧元罚款。

DPC 对 Instagram 的调查始于 2020 年，重点关注在 Instagram 对运营商业账号的青少年用户的数据处理方式及该平台的用户注册系统。DPC 在调查中发现，Instagram 允许年龄在 13 岁至 17 岁之间的青少年用户在该平台上操作商业账户，而这些青少年用户的账户状态会被默认设置为“公开”。同时，平台用户注册系统允许儿童用户填写他们的电话号码或电子邮件地址。这一设置为获取青少年用户的电话号码或电子邮件地址数据提供了便利。

对于此次罚款，Meta 发言人辩称，早在一年多前，为保护儿童的安全与隐私，Instagram 就更新了相关设置。此外，Instagram 在过去的一年多里也陆续发布了多项未成年保护新功能。目前，18 岁以下的未成年新用户在注册 Instagram 时，其账户会被默认设置为“私人”状

[18] 安全内参。

态——陌生用户无法向未成年用户发送的信息，未成年用户发布的内容也不会陌生用户看到。[19]

5. 谷歌、Meta 未经同意跨平台收集信息，韩国开一千亿罚单

9 月 14 日，韩国个人信息保护委员会召开会议，对谷歌和 Meta 未经用户同意收集个人信息、用于个性化推荐广告的违法行为进行审议，并对谷歌处以 692 亿韩元（约合人民币 3.46 亿元）、对 Meta 308 亿韩元（约合人民币 1.54 亿元）的罚款。委员会要求，平台若要收集、利用第三方行为信息，必须提前通知用户并取得同意，让用户容易、明确地了解情况，并自由行使其决定权。据悉，这是韩国首次就个性化推荐广告平台收集个人信息行为进行罚款，也是对企业违反韩国《个人信息保护法》开出的最大罚单。

自 2021 年 2 月起，韩国个人信息保护委员会开始调查韩国国内外主要线上定向广告平台的行为信息收集和利用情况，重点为平台在收集第三方行为信息时是否得到了用户同意。调查发现，谷歌在至少 6 年的时间内，在注册服务时没有明确告知用户第三方行为信息收集和使用事实细则，使用了“更多选项”隐藏部分设置，以及将隐私相关选项默认为“同意”。Meta 则在约 4 年的时间内，将注册时需要告知用户的内容以不容易看懂的形式放在数据政策全文中。

委员会公告指出，第三方行为信息是在用户访问其他网站或应用程序时自动收集的，因此用户很难预测自己在“哪些网站中的哪些行为信息”会被收集。特别地，在用户账号登录的所有设备上，平台都能监控在线活动，日积月累，可能收集或生成包括用户的“思想、信仰、政治见解、健康状况、生理数据、行为特征等”敏感信息。因此，平台在收集第三方行为信息时，要明确告知用户具体内容并得到同意。

对此，韩国个人信息委员会委员长尹钟仁表示：“希望通过此次处分，纠正平台以提供免费服务为名，在用户不知情的情况下擅自收集、利用用户信息的行为。让这次处分成为一个契机，保障用户自主

[19] 新浪科技网。

决定个人信息收集与利用的情况。……希望今后大型在线广告平台在收集和利用个人信息的过程中，能够显著提高透明度，尽到社会责任。”

韩国以外，其他国家也有类似案例。2019 年 1 月，法国个人信息监管机构（CNIL）裁定谷歌在个性化广告方面“缺乏透明度，信息提供不充分，且未获得用户的有效同意”，对谷歌处以高达 5000 万欧元的罚款，是当时监管机构依据欧盟《一般数据保护条例》（GDPR）开出的最高金额罚单。2019 年 2 月，德国反垄断监管机构（FCO）认为，Facebook 在未经用户同意的情况下收集和利用了第三方行为信息，命其停止在德国境内的数据收集行为。[20]

6. 美国海关复制大量公民私人信息

据《华盛顿邮报》当地时间 9 月 15 日报道，美国海关和边境保护局（CBP）的负责人在今年夏天的一次简报会上告诉国会工作人员，美国政府官员每年在机场、海港和边境口岸旅客手中查获多达约 1 万台电子设备，并从中拷贝数据至一个庞大的数据库。

据报道，约 2700 名海关和边境保护局官员无需通行证即可访问该数据库，且数据库正在迅速扩大，数据包含旅客手机和电脑等设备中的照片、联系人、通话记录和信息等。这些此前不为人知的细节已经引起国会警惕。据海关和边境保护局表示，这些数据将保存 15 年，复制的数据大部分来自没有任何犯罪嫌疑的普通公民。

俄勒冈州民主党参议员罗恩·怀登（Ron Wyden）15 日给美国海关和边境保护局局长克里斯·马格努斯（Chris Magnus）的一封信中披露了数据库的细节，他批评该机构“允许不分青红皂白地搜查美国人的私人记录”，并呼吁加强隐私保护。[21]

[20] 安全内参。
[21] 安全内参。

环球律师事务所
GLOBAL LAW OFFICE

环球解读

1. 对《网络安全法》修订征求意见稿的要点解读

前言

2022 年 9 月 14 日，国家互联网信息办公室（下称“网信办”）发布了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（下称“《决定（征求意见稿）》”）。本次修订为《中华人民共和国网络安全法》（下称“《网安法》”）自 2017 年正式实施以来的首次修订。根据网信办的说明，本次修订的目的在于做好《网安法》与 2021 年相继修订或制定实施的《中华人民共和国行政处罚法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》（下称“《个人信息保护法》”）等法律的衔接协调，拟通过调整、整合网络运营者的网络信息安全保护义务，将违法后果可能产生的危害与应当通过行政处罚进行惩戒的措施种类和幅度相协调，处罚标准也有意识地与《个人信息保护法》下的刻度进行了对齐，并对原法中没有规定的违法行为补充了法律责任条款，从而能够更有力地保障国家网络运营安全，进一步完善网络安全法律责任制度，也重点强化了关键信息基础设施运营者对系统和运营安全的保护管理责任。结合此背景，本次《决定（征求意见稿）》主要针对《网安法》“第六章 法律责任”部分作出修订，涉及的具体条文包括《网安法》第五十九条至第七十条。

一、对《网安法》第五十九条、第六十条、第六十一条、第六十二条的修订（下称“条款一”）

根据《决定（征求意见稿）》，“条款一”将《网安法》第五十九条、第六十条、第六十一条、第六十二条修改为：“违反本法第二十一条、第二十二条第一款和第二款、第二十三条、第二十四条第一款、第二十五条、第二十六条、第二十八条、第三十三条、第三十四条、第三十六条、第三十八条规定的网络运行安全保护义务或者导致危害网络运行安全等后果的，由有关主管部门责令改正，给予警告、通报批评；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节特别严重的，由省级以上有关主管

部门责令改正，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令停止相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。”

（一）责任内容

“条款一”修订并融合了《网安法》的第五十九条至第六十二条的规定，这些规定所包含的具体责任为：

- 网络产品、服务应当符合相关国家标准的强制性要求（第二十二条第一款），网络产品、服务的提供者提供安全维护的责任（第二十二条第二款）
- 网络运营者应按照网络安全等级保护制度的要求，履行安全保护义务（第二十一条）；
- 网络产品、服务应当符合相关国家标准的强制性要求（第二十二条第一款），网络产品、服务的提供者提供安全维护的责任（第二十二条第二款）；
- **网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供（第二十三条）；**
- 网络运营者要求用户提供真实身份信息的义务（第二十四条第一款）；
- 网络运营者按要求履行网络安全事件相关义务（第二十五条）；
- 遵守国家规定开展网络安全认证、检测、风险评估、发布等活动（第二十六条）；
- **网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助（第二十八条）；**
- 关键信息基础设施运营者履行安全技术措施（第三十三条）、额外安全保护义务（第三十四条）、签订安全保密协议（第三十六条）、年度检测评估及报送义务（第三十八条）。

结合《网安法》的第五十九条至第六十二条的规定可知，“条款一”新增了**违反《网安法》第二十三条与第二十八条的法律责任**。这意味着，若网络运营者未按要求认证或检测并销售或提供网络关键设备或网络安全专用产品，则企业及直接责任人员均面临着较高的处罚风险。根据 2022 年年初工信部等四部门发布的《关于统一发布网络关键设备和网络安全专用产品安全认证和安全检测结果的公告》可知，网络关键设备或网络安全专用产品的认证和检测结果通过中国网信网、工业和信息化部网站、公安部网站和认监委网站同步公布和更新，企业可保持关注。此外，对于公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动，网络运营者应当提供技术支持和协助，否则将面临处罚。

除上述新增的法律责任外，“条款一”并未把《网安法》第五十九条至第六十二条规定的所有法律责任囊括在内，例如《网安法》第四十八条第一款规定的电子信息及应用软件不得设置恶意程序不得含有禁止发布或传输的信息。结合《决定（征求意见稿）》的其余修订可知，此处修订进一步调整了相应法律责任的逻辑，将用户信息管理所涉及的相关法律责任汇总在新的条款之中，下文将详细说明。

（二）处罚标准

“条款一”在融合了上述责任内容的同时，对违反上述法律责任的行为均提高了处罚标准。具体分为三级：

- 违反网络运行安全保护义务或者导致危害网络运行安全等后果的，由有关主管部门责令改正，给予警告、**通报批评**；
- 拒不改正或者情节严重的，**处一百万元以下罚款**，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员**和其他直接责任人员**处一万元以上十万元以下罚款；
- **情节特别严重的，由省级以上有关主管部门责令改正，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令停止相关业务、停业整顿、关闭网站、**

吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

据此可知，对于一般的违法行为，“条款一”新增了“通报批评”的处罚方式。对于“拒不改正或者情节严重的”的违法行为，“条款一”将对企业的罚款上限调整至了一百万元，同时，除“直接负责的主管人员”，“其他直接责任人员”也面临着一万元以上十万元以下的罚款。这意味着在实践中，除管理层外直接接触相关工作的企业员工（例如信息安全部门、数据管理部门）若未履行《网安法》下的义务受处罚的几率有所增加。此外，“条款一”新增了“情节特别严重的”最高级处罚，罚金最高上限等同于《个人信息保护法》第六十七条的规定，即五千万元以下或者上一年度营业额百分之五以下罚款，以及停止相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等严厉的行政处罚措施。而对于直接负责的主管人员和其他直接责任人员而言，则不仅面临着最高一百万元的罚款，还可能受“从业禁止”的处罚，在一定期限内禁止担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

二、对《网安法》第六十三条、第六十七条的修订（下称“条款二”）

根据《决定（征求意见稿）》，“条款二”将《网安法》第六十三条、第六十七条修改为：“违反本法第二十七条、第四十六条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，或者设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。”

（一）责任内容

“条款二”修订并融合了《网安法》的第二十七条及第四十六条的规定，具体为：

- 任何个人和组织禁止从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动，禁止为上述活动提供程序、工具、技术支持、广告推广、支付结算等帮助（第二十七条）；

- 任何个人和组织不得设立用于违法犯罪活动的网站、通讯群组，不得利用网络发布违法犯罪活动的信息（第四十六条）。

“条款二”将《网安法》中涉嫌利用网络实施违法乃至犯罪行为的责任内容整合至一处，逻辑上更为清晰。

（二）处罚标准

“条款二”在融合了上述责任内容的同时，整合了相应违法内容的处罚标准，具体分为以下情况：

- 违反《网安法》第二十七条、第四十六条规定，构成犯罪的，则由相关刑事法律法规及司法解释予以规制；

- 尚不构成犯罪的：a）对个人：由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；

b）对企业：由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

- 尚不构成犯罪但情节较重的：a）对个人：处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款；b）对企业：由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

- 违反第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

根据上述处罚标准可知，“条款二”在规定了相应行政处罚措施的同时，也按照《行政处罚法》第八条第二款的要求，保留了追究相关主体刑事责任的规定。此外，“条款二”提高了对个人的罚款上限，也即一般情况下的五十万元以下罚款以及情节较重时的一百万元以下罚款（原规定为十万元/五十万元）。对单位的违法行为，则保留了原处罚措施与力度。同时，“条款二”延续了《网安法》第六十三条第三款规定中的“禁业规定”，也即受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。此处的“禁业规定”应区别于“条款一”中企业直接负责的主管人员和其他直接责任人员的“从业禁止”，前者在处罚力度更为严厉的同时，其针对群体也并非仅为企业的责任人员，“任何个人和组织”均可能成为处罚对象，且需满足 “受到治安管理处罚”及“受到刑事处罚”的条件。

三、对《网安法》第六十四条的修订（下称“条款三”）

根据《决定（征求意见稿）》，“条款三”将《网安法》第六十四条修改为：“网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十四条规定，侵害

个人信息依法得到保护的权利的，依照有关法律、行政法规的规定处罚。”

（一）责任内容

“条款三”延续了《网安法》第六十四条所涉及的具体责任内容：

- 网络产品、服务具有收集用户信息功能的，应遵守关于个人信息保护的规定（第二十二条第三款）；
- 网络运营者收集、使用个人信息所遵循的原则及规定（第四十一条）；
- 网络运营者确保个人信息安全及未经被收集者同意不得提供的义务（第四十二条）；
- 网络运营者应保障个人删除及更正个人信息的权利（第四十三条）；
- 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息（第四十四条）。

根据上述责任内容可知，“条款三”将《网安法》中涉及个人信息的相关责任汇总至一起，在逻辑上更为清晰。

（二）处罚标准

“条款三”取消了原《网安法》第六十四条中规定的具体处罚标准，而代之以“依照有关法律、行政法规的规定处罚”。结合网信办“关于修改《中华人民共和国网络安全法》的决定（征求意见稿）的说明”可知，《决定（征求意见稿）》所体现的趋势为，《网安法》中有关个人信息保护的法律责任将修改为转致性规定。也即，存在未来《网安法》中涉及个人信息保护的责任

内容以《个人信息保护法》或其他个人信息保护法律法规的处罚标准直接适用的可能性。

四、对《网安法》第六十五条（下称“条款四”）及六十六条的修订（下称“条款五”）

（一）“条款四”的解读

根据《决定（征求意见稿）》，“条款四”将《网安法》第六十五条修改为：“关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下或者上一年度营业额百分之五以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

“条款四”并未改变《网安法》第六十五条所规定的责任内容，即根据《网安法》第三十五条，关键信息基础设施运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。根据 2022 年 2 月正式实施的《网络安全审查办法》可知，关键信息基础设施运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险，影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。而在网络安全审查视野下的“网络产品和服务”，主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。

此外，“条款四”新增了“上一年度营业额百分之五以下罚款”的处罚标准，关键信息基础设施运营者应当格外注意。

（二）“条款五”的解读

“条款五”将《网安法》第六十六条修改为：“关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，

或者向境外提供网络数据的，依照有关法律、行政法规的规定处罚。”

“条款五”调整了关键信息基础设施运营者违反境内存储与安全评估义务（第三十七条）所涉及的处罚标准，取消了《网安法》第六十六条中的具体处罚措施规定，代之以“依照有关法律、行政法规的规定处罚”。《数据安全法》第四十六条规定，违反本法第三十一条规定（关键信息基础设施运营者应履行境内存储或数据出境安全评估义务），向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

五、对《网安法》第六十八条、六十九条的修订（下称“条款六”）

根据《决定（征求意见稿）》，“条款六”将《网安法》第六十八条、第六十九条修改为：“违反本法第四十七条、第四十八条、第四十九条规定的网络信息安全保护义务，或者不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息采取停止传输、消除等处置措施的，或者不按照有关部门的要求对网络存在较大安全风险和发生安全事件采取措施的，由有关主管部门责令改正，给予警告、通报批评，没收违法所得；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。”

（一）责任内容

“条款六”修订调整了《网安法》第六十八条、第六十九条的相关内容，其具体责任内容为：

- 网络运营者对用户发布信息的管理（第四十七条）；
- 任何个人和组织发送的电子信息、提供的应用软件不得设置恶意程序，不得含有禁止传输的信息，相关服务提供者应当履行安全管理义务（第四十八条）；
- **网络运营者应当建立网络信息安全投诉、举报制度**（第四十九条）。
- **网络运营者应按照有关部门的要求对法律、行政法规禁止发布或者传输的信息采取停止传输、消除等处置措施的，或者按照有关部门的要求对网络存在较大安全风险和发生安全事件采取措施**（“条款六新增”）

在责任内容方面，“条款六”延续了网络运营者对用户发布信息的管理的义务内容，同时将《网安法》第四十八条的内容归纳为统一的责任内容，改变了原先第四十八条第一款的责任内容与第二款的责任内容分属不同法条的情况。同时，“条款六”将网络运营者建立网络信息安全投诉、举报制度也新增纳入了责任范围，这意味着网络运营者未建立相关制度、公布投诉、举报方式等信息，或未及时受理并处理有关网络信息安全的投诉和举报或配合监管部门检查的行为，可能面临处罚。

此外，“条款六”删除了《网安法》第六十九条规定情形，并将其细化新增在条文中。这意味着，网络运营者若不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息采取停止传输、消除等处置措施的，或者不按照有关部门的要求对网络存在较大安全风险和发生安全事件采取措施的，即便符合《网安法》第四十七条、第四十八条、第四十九条规定的网络信息安全保护义务，也面临着处罚风险。

（二）处罚标准

“条款六”在融合了上述责任内容的同时，对违反上述法律责任的行为均提高了处罚标准。具体分为三级：

- 由有关主管部门责令改正，给予警告、通报批评，没收违法所得；

- 拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；

- **情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。**

对于一般的违法行为，“条款六”新增了“通报批评”的处罚方式。对于“拒不改正或者情节严重的”的违法行为，“条款六”将对企业的罚款上限调整至了一百万元。此外，“条款六”类似“条款一”的情况，新增了“情节特别严重的”最高级处罚，罚金最高上限等同于《个人信息保护法》第六十七条的规定，即五千万元以下或者上一年度营业额百分之五以下罚款，以及停止相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等严厉的行政处罚措施。而对于直接负责的主管人员和其他直接责任人员而言，则不仅面临着最高一百万元的罚款，还可能受“从业禁止”的处罚，在一定期限内禁止担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

六、对《网安法》第七十条的修订（下称“条款七”）

根据《决定（征求意见稿）》，“条款七”将《网安法》第七十条修改为：“发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

法律、行政法规没有规定的，由有关主管部门责令改正，给予警告、通报批评，没收违法所得；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。”

（一）责任内容

“条款七”所涉及的《网安法》第十二条第二款，并规定禁止发布、传输危害网络安全，危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

除《网安法》第十二条第二款所涉及内容外，“条款七”延续了《网安法》第七十条的规定，同时将“其他法律、行政法规禁止发布或者传输的信息”也纳入了责任内容范围。

（二）处罚标准

“条款七”补充扩展了《网安法》第七十条有关处罚标准的规定，也即相关主体触犯本条规定，但法律、行政法规没有规定时：

- 由有关主管部门责令改正，给予警告、通报批评，没收违法所得；

- 拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；

- **情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。**

据此可知，“条款七”补充了在没有相关法律法规规定时的处罚标准，同时类似“条款一”及“条款六”，规定了“情节特别严重”的最高标准，应当引起相关主体关注。

七、结语

本次《决定（征求意见稿）》的发布，进一步完善了对网络安全、数据安全与个人信息保护法律责任制度体系。一方面，针对网络运营者、关键信息基础设施运营者的责任内容逻辑更加紧凑清晰，另一方面，适应了最新立法趋势并调整了处罚幅度及处罚种类。同时，对于个人信息保护的法律责任，《决定（征求意见稿）》也显现出将原有《网安法》项下关个人信息保护的法律责任修改为转致性规定的趋势。目前，《决定（征求意见稿）》尚处于征求意见阶段，在社会各界的热烈讨论与监管部门的进一步调整下，我们相信“三驾马车”中最早发布实施的《网安法》

的法律责任体系将更加清晰，不同法律适用之间的不协调问题将进一步得到解决。

值得大家关注的是，网信办除了对“实体法”有上述修订外，2022 年 9 月 8 日亦发布了关于《网信部门行政执法程序规定（征求意见稿）》（下称“《规定（征求意见稿）》”）的通知[22]，代表着国家网信部门也正在同步完善包括对网络安全违法行为进行行政处罚等执法“程序”（如立案、调查取证、听证、约谈、行政处罚决定、送达等）。我们建议企业及各相关主体在关注《网安法》法律责任部分修订的同时，也同时关注网信部门按照《规定（征求意见稿）》拟将施行的行政执法最新趋势，以求在“实体”与“程序”两大维度上满足监管部门的最新监管要求。同时，《规定（征求意见稿）》也赋予了当事人主体所享有的相关权利（如要求举行听证、申请行政复议、申请延期或分期缴纳罚款等），以满足当事人主体在最新程序框架内实现权利与义务的统一。

[22] 《网信部门行政执法程序规定（征求意见稿）》是在《互联网信息内容管理行政执法程序规定》（2017 年 5 月 2 日发布，2017 年 6 月 1 日正式实施，现行有效）的基础上进行的修订。《网信部门行政执法程序规定（征求意见稿）》全文共五十六条，分为总则、管辖和适用、行政处罚的普通程序（包括四节：立案；调查取证；听证、约谈；行政处罚决定、送达）、执行与结案、附则五章。

2022 年 第七期 /总第四十一期

数据合规时事速递
NEWSLETTERS

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

若您有任何疑问和建议，欢迎随时与我们联系，联系邮箱：tianziyi@glo.com.cn。您也可以扫描上方二维码，关注我们的公众号“M 姐 数据合规评论”获取更多资讯。