



LIFANG & PARTNERS
立 方 律 师 事 务 所

Data and AI Compliance Review

数据与人工智能合规观察月刊

No.2

Data and AI Compliance Review by Lifang & Partners**立方数据与人工智能合规观察月刊****2026. 9****No.2****目录**

Domestic News 境内动态	1
➤ Regulations Update 新规速递	1
CAC Issues the <i>Provisions of the State Council on Safeguarding the Healthy and Safe Use of the Internet by Minors (Draft for Comment)</i>	1
国家网信办发布《国务院关于保障未成年人健康安全使用网络的规定（征求意见稿）》	1
CAC Issues the <i>Notice on Strengthening the Management of Enterprise-Related Infringing Information and Continuously Promoting the Optimization of the Business-Oriented Online Environment</i>	2
国家网信办发布《关于加强涉企侵权信息管理 持续推动营商网络环境优化的通知》	2
CAC Issues Q&A on Policies and Regulations for the Security Management of Cross-Border Data Transfers	3
国家网信办发布数据出境安全管理政策法规问答	4
Ministry of Commerce Responds to the US Cybersecurity Notice Concerning Alleged Distillation Activities by Chinese AI Companies Against the United States	4
商务部回应美国发布中国人工智能企业对美国蒸馏活动相关网络安全公告	5
TC260 Issues the <i>Practical Guide to Cybersecurity Standards - Security Requirements for Cockpit Data Processing</i>	5
全国网安标委发布《网络安全标准实践指南——座舱数据处理安全要求》	6
Beijing Municipality Passes the <i>Regulations of Beijing Municipality on Surveying and Mapping Geographic Information</i>	6

北京市通过《北京市测绘地理信息条例》	7
➤ Regulatory Actions 监管行动	7
National Computer Virus Emergency Response Center Detects 82 Mobile Applications That Illegally Collect and Use Personal Information	7
国家计算机病毒应急处理中心检测发现 82 款违法违规收集使用个人信息的移动应用	8
CAC Reports 30 Apps with Issues Concerning the Collection and Use of Personal Information	8
中央网信办通报 30 款存在个人信息收集使用问题的 App	9
CAC Publishes Typical Law Enforcement Cases in the Fields of Cybersecurity, Data Security, and Personal Information Protection	9
国家网信办发布近期网络安全、数据安全、个人信息保护等领域执法典型案例	10
CAC Conducts In-Depth Implementation of the Second Phase of the “Qinglang · Rectifying Chaos in AI Applications” Special Campaign	10
中央网信办深入开展“清朗·整治 AI 应用乱象”专项行动第二阶段工作	11
Quality Supervision and Inspection Center for Computer Information System Security Products of the Ministry of Public Security Detects 42 Mobile Applications That Illegally Collect and Use Personal Information	11
公安部计算机信息系统安全产品质量监督检验中心检测发现 42 款违法违规收集使用个人信息的移动应用	12
Overseas News 境外动态	12
➤ Regulations Update 新规速递	12
EU: European Commission Publishes the Proposal for the <i>EU KIDS Act</i> ..	12
欧盟：欧盟委员会发布《欧盟儿童法案》提案	13
EU: Reporting Obligations under the CRA Take Effect	13
欧盟：CRA 报告义务生效	13
EU: CCPC Highlights the “Access by Design” Requirements under the <i>Data Act</i>	14
欧盟：CCPC 强调《数据法案》“设计即访问”要求	14

➤ Regulatory Actions 监管行动	15
UK: TikTok Withdraws Two Appeals in Children's Privacy Action and Accepts the £12.7 Million Fine.....	15
英国: TikTok 撤回两项儿童隐私上诉并接受 1270 万英镑罚款	15
Ireland: DPC Fines Google €403 Million over Violations Concerning the Processing of Location Data	16
爱尔兰: DPC 以位置数据处理违规对谷歌处以 4.03 亿欧元罚款	16
South Korea: PIPC Issues Recommendations for Improvement to Five Companies.....	17
韩国: PIPC 对五家企业提出改善劝告	17
EU: European Commission Designates ChatGPT, Reddit, and Roblox under the DSA.....	18
欧盟: 欧盟委员会依据 DSA 指定 ChatGPT、Reddit 和 Roblox	18

Domestic News 境内动态

➤ Regulations Update 新规速递

CAC Issues the Provisions of the State Council on Safeguarding the Healthy and Safe Use of the Internet by Minors (Draft for Comment)

On 18 September 2026, the Cyberspace Administration of China (CAC) issued the *Provisions of the State Council on Safeguarding the Healthy and Safe Use of the Internet by Minors (Draft for Comment)* (Provisions) for public comment, with the deadline for feedback being 17 October 2026. The Provisions comprise 25 articles and apply to the provision of internet services to minors within the territory of China, the research, development and manufacturing of smart terminal products, and the provision of applications to smart terminal users through application distribution platforms. The Provisions clarify that internet service providers shall not provide minors with online social networking services with strangers, services of virtual intimate relationships such as virtual relatives and virtual companions, and other such services, and prescribe relevant exceptional circumstances. It is proposed that internet service providers shall provide internet audio and video services, online live streaming services other than online live streaming publishing services, online game services, and online social networking services to minors under the age of 16 through a minors mode. The Provisions require that internet service providers shall have the capability to identify minor users and take necessary measures to safeguard the security of minors' personal information; with respect to users who have been authenticated through real-name registration or identified as minors, internet service providers shall take corresponding measures. ([More](#))

国家网信办发布《国务院关于保障未成年人健康安全使用网络的规定（征求意见稿）》

2026年9月18日，国家互联网信息办公室（以下简称“国家网信办”）发布了《国务院关于保障未成年人健康安全使用网络的规定（征求意见稿）》（以下简称《规定》），向社会公开征求意见，意见反馈截止时间为2026年10月17日。《规定》共二十五条，适用于中国境内向未成年人提供网络服务，研发、制造智能终端产品，通过应用程序分发平台为智能终端用户提供应用程序。《规定》明确，网络服务提供者不得向未成年人提供陌生人网络社交服务、虚

拟亲属和虚拟伴侣等虚拟亲密关系服务等，并规定了相关例外情形。提出网络服务提供者向未满十六周岁的未成年人提供网络音视频服务、网络直播发布服务以外的其他网络直播服务、网络游戏服务和网络社交服务等，应当通过未成年人模式提供。《规定》要求，网络服务提供者具备未成年人用户识别能力，并采取必要措施保障未成年人个人信息安全；对经实名认证或者识别为未成年人用户的，网络服务提供者应当采取相应的措施。（[查看更多](#)）

CAC Issues the Notice on Strengthening the Management of Enterprise-Related Infringing Information and Continuously Promoting the Optimization of the Business-Oriented Online Environment

On 18 September 2026, the CAC issued the *Notice on Strengthening the Management of Enterprise-Related Infringing Information and Continuously Promoting the Optimization of the Business-Oriented Online Environment* (Notice). The Notice clarifies that website platforms shall proactively clean up and dispose of the following enterprise-related infringing information: (1) Personal information category. Including the disclosure of entrepreneurs' personal identity and contact information such as ID cards, home addresses, and phone numbers, as well as sensitive personal information such as biometric information, medical and health information, financial account information, and movement trajectories. (2) Insult and denigration category. Including insulting and abusing enterprises and entrepreneurs, and making fun of or defacing enterprise logos, products, and entrepreneurs' portraits. (3) Counterfeiting and impersonation category. Including enterprise-related supervisory information counterfeited or impersonated as being produced and published by news organizations. (4) False and misleading category. Including taking remarks of entrepreneurs out of context or distorting the interpretation of their past statements, and presenting search keyword associations and search landing page results inconsistent with the facts. (5) Other categories. Including enterprise-related content inciting rivalries or provoking confrontation, and collected and rehashed old news, old matters, and negative information about enterprises. ([More](#))

国家网信办发布《关于加强涉企侵权信息管理 持续推动营商环境优化的通知》

2026年9月18日，国家网信办发布了《关于加强涉企侵权信息管理 持续推动营商环境优化的通知》（以下简称《通知》）。《通知》明确，网站平台对

以下涉企侵权信息，应当积极主动清理处置：（1）个人信息类。包括泄露企业家身份证、家庭住址、电话号码等个人身份及联系信息，以及生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息。（2）侮辱贬损类。包括侮辱谩骂企业、企业家，恶搞丑化企业标识、产品和企业家肖像等。（3）假冒仿冒类。包括假冒仿冒新闻单位制作发布的涉企监督信息等。（4）虚假误导类。包括断章取义、歪曲解读企业家过往言论，呈现与事实不符的搜索关键词联想、搜索落地页结果等。（5）其他类。包括涉企拉踩引战信息，集纳翻炒的企业旧闻旧事、负面信息等。（[查看更多](#)）

CAC Issues Q&A on Policies and Regulations for the Security Management of Cross-Border Data Transfers

On 11 September 2026, the CAC issued a Q&A on policies and regulations for the security management of cross-border data transfers. The CAC emphasized that where a non-operator of critical information infrastructure has, cumulatively since 1 January of the current year, provided overseas the personal information of more than 100,000 but fewer than 1 million individuals (excluding sensitive personal information), or the sensitive personal information of fewer than 10,000 individuals, and such information does not include important data, it may fulfill its compliance obligations for cross-border data transfers through the means of personal information protection certification. Of note, the CAC clarified that a personal information processor that engages in the cross-border transfer of personal information may apply to a professional certification institution for personal information protection certification regardless of the scale of the personal information transferred. When filing an application for a data export security assessment, the personal information processor may attach the relevant information concerning the certification obtained, to demonstrate the level of personal information protection of the personal information processor and the overseas recipient, the safeguarding of personal information rights and interests, and other such matters, and the cyberspace administration will take such information into reference during the security assessment process. The CAC stated that a personal information processor may apply to any professional institution that has completed filing for personal information protection certification. Before applying for certification and providing personal information overseas, the personal information processor shall, in accordance with the relevant provisions, perform its obligations such as notifying the individual, obtaining

the individual's separate consent, and conducting a personal information protection impact assessment. ([More](#))

国家网信办发布数据出境安全管理政策法规问答

2026年9月11日，国家网信办发布了数据出境安全管理政策法规问答。国家网信办强调，非关键信息基础设施运营者自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息，且不包括重要数据的，可以通过个人信息出境认证方式履行数据出境合规义务。值得关注的是，国家网信办明确个人信息处理者存在个人信息出境行为，不论出境个人信息规模大小，均可向专业认证机构申请个人信息出境认证；个人信息处理者申报数据出境安全评估时，可以将通过个人信息出境认证有关情况附后，说明个人信息处理者和境外接收方的个人信息保护水平、个人信息权益保障等情况，网信部门将在安全评估过程中予以参考。国家网信办指出，个人信息处理者可以向已通过备案的任何一家专业机构申请个人信息出境认证。个人信息处理者在申请认证向境外提供个人信息前，应当按照规定履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。（[查看更多](#)）

Ministry of Commerce Responds to the US Cybersecurity Notice Concerning Alleged Distillation Activities by Chinese AI Companies Against the United States

On 9 September 2026, the Ministry of Commerce responded to the cybersecurity notice issued by the United States concerning alleged distillation activities by Chinese artificial intelligence companies against the United States. On 8 September 2026, the United States issued a notice accusing Chinese AI companies of conducting “industrial-scale” distillation against the United States to obtain US frontier model capabilities, and suggesting relevant defensive measures to US companies. The Ministry of Commerce responded that distillation is a common practice in the field of artificial intelligence through which models learn from one another, and is by nature a neutral technical means used by model companies worldwide, including US companies. Such a technical means can help models improve learning efficiency and achieve more efficient utilization of human knowledge, and is of positive significance for countries in developing their AI industries, unleashing the potential of AI technology, bridging development gaps, and more broadly benefiting developing countries and the general public. The US practice is a typical case of striking at distillation in name but practicing industrial monopoly in reality. By issuing the notice through a security agency, the

United States is tying the interests of individual enterprises and capital to national security, and using state coercive institutions to interfere with normal commercial activities. The Ministry of Commerce noted that certain US AI companies abuse their dominant competitive position by setting hegemonic clauses such as broad geographical restrictions in user agreements, and the relevant US distillation allegations have the appearance of endorsing such hegemonic clauses. ([More](#))

商务部回应美国发布中国人工智能企业对美国蒸馏活动相关网络安全公告

2026年9月9日，商务部回应了美国发布中国人工智能企业对美国蒸馏活动相关网络安全公告。2026年9月8日，美国发布公告，指责中国人工智能企业对美国开展“工业规模”蒸馏，获取美国前沿模型能力，并向美企提出相关防御措施建议。商务部回应，蒸馏是人工智能领域各个模型间互相学习的通行做法，本质是中性技术手段，包括美企在内的全球模型企业都在用。这种技术手段可以帮助模型提升学习效率，实现人类知识的更高效利用，对各国发展人工智能产业、释放人工智能技术潜力、弥补发展鸿沟、更广泛惠及发展中国家和社会大众有积极意义。美国的做法是典型的以打击蒸馏为名，行产业垄断之实。美国由安全部门发布公告，是将个别企业和资本利益与国家安全相捆绑，动用国家强权机构干涉正常商业活动。商务部注意到，美国个别人工智能企业滥用竞争优势地位，在用户协议中设置宽泛的地域限制等霸王条款。美国相关蒸馏指控，有为这些霸王条款背书之嫌。（[查看更多](#)）

TC260 Issues the *Practical Guide to Cybersecurity Standards - Security Requirements for Cockpit Data Processing*

On 15 September 2026, the National Technical Committee 260 on Cybersecurity of SAC (TC260) issued the *Practical Guide to Cybersecurity Standards - Security Requirements for Cockpit Data Processing* (Requirements). The Requirements apply to cockpit data processing activities and may also serve as a reference for the design and development of automotive cockpit functions. The Requirements provide that a cockpit data processor is an organization that conducts cockpit data processing activities, including automobile manufacturers, component and software suppliers, or in-vehicle application service providers. The Requirements set out clear security technical requirements for voice wake-up, intelligent voice dialogue, driver status monitoring systems, and remote viewing. For example, a cockpit data processor that processes data related to the driver status monitoring system function shall disclose the

location of the cameras used for the driver status monitoring system function; the camera capture range shall cover only the area directly above the driver's seat; cockpit data involving human faces shall be stored in an independent space on the vehicle side and shall not be stored together with personal identity information; and the collected facial data of drivers shall be processed within the vehicle. ([More](#))

全国网安标委发布《网络安全标准实践指南——座舱数据处理安全要求》

2026 年 9 月 15 日，全国网络安全标准化技术委员会（以下简称“全国网安标委”）发布了《网络安全标准实践指南——座舱数据处理安全要求》（以下简称《要求》）。《要求》适用于座舱数据处理活动，也可为汽车座舱功能设计研发提供参考。《要求》规定，座舱数据处理者是开展座舱数据处理活动的组织，包括汽车制造商、零部件和软件供应商或车载应用服务提供者。《要求》对语音唤醒、智能语音对话、驾驶员状态检测系统、远程查看的安全技术作出明确要求，例如座舱数据处理者处理驾驶员状态监测系统功能相关数据的，应告知用于驾驶员状态监测系统功能的摄像头位置、摄像头采集范围应仅覆盖主驾驶座椅正上方区域、涉及人脸的座舱数据应在车端独立空间存储，不应与个人身份信息一起存储、所收集驾驶员人脸数据应在车内处理。（[查看更多](#)）

Beijing Municipality Passes the Regulations of Beijing Municipality on Surveying and Mapping Geographic Information

On 13 September 2026, the Standing Committee of the Beijing Municipal People's Congress passed the *Regulations of Beijing Municipality on Surveying and Mapping Geographic Information* (Regulations), which shall come into effect on 1 January 2027. The Regulations comprise nine chapters and 66 articles, and apply to activities such as conducting surveying, mapping and geographic information activities, utilizing surveying, mapping and geographic information results, and implementing surveying, mapping and geographic information administration within the administrative area of Beijing Municipality. The Regulations provide that where surveying, mapping and geographic information data become state secrets after being aggregated and associated with relevant data, security and confidentiality prevention and control measures shall be implemented to guard against the risk of leakage. The Regulations state that units that transmit surveying, mapping and geographic information data through networks, such as satellite navigation and positioning reference station construction and operation and maintenance units and internet map service units, shall, in accordance with the

security and confidentiality management requirements, regularly carry out security testing of equipment, facilities and network environments to ensure data security. The Regulations clarify that where surveying, mapping and geographic information data such as autonomous driving maps and internet maps are updated in a crowdsourced manner, such updating shall be implemented by surveying and mapping units with relevant qualifications, who shall, in accordance with the law, ensure the security of data collection and transmission, protect personal information, refrain from disclosing personal privacy, and refrain from endangering national security. ([More](#))

北京市通过《北京市测绘地理信息条例》

2026年9月13日，北京市人民代表大会常务委员会通过了《北京市测绘地理信息条例》（以下简称《条例》），自2027年1月1日起实施。《条例》共九章六十六条，适用于在北京市行政区域内开展测绘地理信息活动、利用测绘地理信息成果、实施测绘地理信息管理等活动。《条例》规定，测绘地理信息数据与相关数据汇聚、关联后属于国家秘密的，应当落实安全保密防控措施，防范泄密风险。《条例》指出，卫星导航定位基准站建设和运行维护单位、互联网地图服务单位等利用网络传输测绘地理信息数据的单位，应当按照安全保密管理要求定期开展设备设施和网络环境安全检测，保证数据安全。《条例》明确，以众源方式更新自动驾驶地图、互联网地图等测绘地理信息数据的，应当由具备相关资质的测绘单位实施，依法确保数据采集和传输安全，保护个人信息，不得泄露个人隐私，不得危害国家安全。（[查看更多](#)）

➤ Regulatory Actions 监管行动

National Computer Virus Emergency Response Center Detects 82 Mobile Applications That Illegally Collect and Use Personal Information

On 23 September 2026, the National Computer Virus Emergency Response Center detected 82 mobile applications that illegally collect and use personal information. The issues identified include but are not limited to: (1) Failing to prompt users, through conspicuous means such as pop-up windows upon the first launch of the App, to read collection and use rules such as the privacy policy; seeking users' consent through non-explicit means such as defaulting to consent to the privacy policy; the privacy policy being difficult to access; and the personal information processor failing, before processing personal information, to inform the individual in a conspicuous manner and in clear, easy-to-understand language, truthfully, accurately, and completely of the

name of the personal information processor, its contact information, the retention period of the personal information, etc.; (2) The privacy policy failing to list item by item the purposes, methods, and scope of collection and use of personal information by the App (including entrusted third parties or embedded third-party code and plugins); (3) Where a personal information processor provides the personal information it processes to another personal information processor, failing to inform the individual of the name of the recipient, its contact information, the processing purpose, the processing method, and the categories of personal information, and failing to obtain the individual's separate consent; (4) Failing to adopt effective security technical measures to prevent unauthorized access as well as the leakage, tampering, and loss of personal information. ([More](#))

国家计算机病毒应急处理中心检测发现 82 款违法违规收集使用个人信息的移动应用

2026 年 9 月 23 日，国家计算机病毒应急处理中心检测发现了 82 款违法违规收集使用个人信息的移动应用，所涉问题包括但不限于：（1）在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；以默认选择同意隐私政策等非明示方式征求用户同意；隐私政策难以访问；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理者的名称或者姓名、联系方式、个人信息的保存期限等；

（2）隐私政策未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等；（3）个人信息处理者向其他个人信息处理者提供其处理的个人信息的，未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；（4）未能采取有效安全技术措施，防止未经授权的访问以及个人信息泄露、篡改、丢失。（[查看更多](#)）

CAC Reports 30 Apps with Issues Concerning the Collection and Use of Personal Information

On 20 September 2026, the CAC reported 30 Apps with issues concerning the collection and use of personal information. The issues identified include: (1) failing to disclose the rules for the collection and use of personal information; (2) frequently requesting non-necessary permissions; (3) failing to list item by item the SDKs that collect and use personal information; (4) failing to list item by item the purposes,

methods, and scope of the collection and use of personal information, etc.; and (5) failing to provide an effective account cancellation function. The operators of the relevant Apps shall complete rectification within 15 working days from the date of publication of the report, and report the rectification status to the CAC, which will, together with the relevant departments, carry out verification and, in light of the rectification status, conduct disposition and penalties in accordance with laws and regulations. ([More](#))

中央网信办通报 30 款存在个人信息收集使用问题的 App

2026 年 9 月 20 日，中央网信办通报了 30 款存在个人信息收集使用问题的 App，所涉问题包括：（1）未公开个人信息收集使用规则；（2）频繁索要非必要权限；（3）未逐一系列出收集使用个人信息的 SDK；（4）未逐一系列出收集使用个人信息的目的、方式、范围等；（5）未提供有效账号注销功能。相关 App 运营者应当于通报发布之日起的 15 个工作日内完成整改，并将整改情况报中央网信办，其将会同有关部门进行核查，并结合整改情况依法依规开展处置处罚。

([查看更多](#))

CAC Publishes Typical Law Enforcement Cases in the Fields of Cybersecurity, Data Security, and Personal Information Protection

On 15 September 2026, the CAC recently reported 10 typical law enforcement cases in the fields of cybersecurity, data security, and personal information protection, covering typical cases such as web page tampering, setting up malicious programs, data leakage, personal information leakage, illegal collection and use of personal information, illegally transferring personal information abroad, failure to implement the labeling requirements for AI-generated synthetic content, and providing services through new technologies and new applications launched online without assessment. Among them, a WeChat mini program operated by one enterprise provides services such as AI text dialogue and image generation, but failed to add explicit labels to AI-generated synthetic content, failed to add implicit labels to file metadata, failed to add explicit labels to generated synthetic content when providing the export function, and also failed to implement the security assessment requirements as prescribed, posing content security risks; the cyberspace administration has, in accordance with the law, ordered the mini program to be taken offline. Two websites operated by another enterprise call the interfaces of multiple large model products in the manner of an “API relay station”

to provide services such as dialogue and Q&A, and failed to carry out security assessment work as prescribed, posing content security risks; the local cyberspace administration has, in accordance with the law, ordered it to make corrections, strictly handle the responsible persons, and imposed a warning penalty. ([More](#))

国家网信办发布近期网络安全、数据安全、个人信息保护等领域执法典型案例

2026 年 9 月 15 日，国家网信办近期通报了 10 起网络安全、数据安全与个人信息保护领域典型执法案例，包括网页篡改、设置恶意程序、数据泄露、个人信息泄露、违法收集使用个人信息、违法出境个人信息、未落实人工智能生成合成内容标识要求、新技术新应用未经评估上线提供服务等典型案例。其中，某企业运营的微信小程序提供 AI 文本对话、图片生成等服务，但未对人工智能生成合成内容添加显式标识，未在文件元数据中添加隐式标识，未在提供导出功能时对生成合成内容添加显式标识，同时未按规定落实安全评估要求，存在内容安全风险，网信部门已依法责令下线该小程序；某企业运营的 2 个网站以“API 中转站”方式调用多个大模型产品接口，提供对话、问答等服务，未按规定开展安全评估工作，存在内容安全风险，属地网信办已依法责令其改正、从严处理责任人，予以警告处罚。（[查看更多](#)）

CAC Conducts In-Depth Implementation of the Second Phase of the “Qinglang • Rectifying Chaos in AI Applications” Special Campaign

On 2 September 2026, the CAC reported on the achievements of the second phase of the “Qinglang • Rectifying Chaos in AI Applications” special campaign. The campaign focuses on prominent issues such as using AI to create and publish false information, disseminating violent and vulgar content, counterfeiting and impersonating others, and infringing upon the rights and interests of minors. It deploys local cyberspace administrations to advance the key rectification tasks in depth, urges website platforms to centrally clean up all kinds of illegal and harmful information generated by AI, investigates and penalizes illegal accounts and mobile applications in accordance with the law, effectively curbs the chaos of AI-generated synthetic information content, and promotes the healthy and orderly development of AI application services. As of now, more than 5.61 million items of illegal and harmful information have been cleaned up cumulatively, more than 49,000 accounts have been investigated and penalized, and more than 2,400 illegal websites and applications have been disposed of. Since the launch of the special campaign, local cyberspace

administrations have effectively fulfilled their territorial supervision responsibilities and introduced a series of targeted governance measures in light of local conditions. Website platforms have also actively responded to the deployment arrangements of the special campaign and continuously improved routine governance mechanisms for AI content. ([More](#))

中央网信办深入开展“清朗·整治 AI 应用乱象”专项行动第二阶段工作

2026 年 9 月 2 日，中央网信办通报了“清朗·整治 AI 应用乱象”专项行动第二阶段工作成果。行动聚焦利用 AI 制作发布虚假信息、传播暴力低俗内容、假冒仿冒他人、侵害未成年人权益等突出问题，部署各地网信部门深入推进重点整治任务，督促网站平台集中清理 AI 生成各类违法不良信息，依法查处违规账号和移动应用程序，有效遏制 AI 生成合成信息内容乱象，推动 AI 应用服务健康有序发展。截至目前，累计清理违法违规信息 561 万余条，查处账号 4.9 万余个，处置违规网站、应用程序等 2400 余个。专项行动开展以来，各地网信部门切实履行属地监管责任，因地制宜推出一系列针对性治理措施。网站平台也积极响应专项行动部署安排，持续健全 AI 内容常态化治理机制。 ([查看更多](#))

Quality Supervision and Inspection Center for Computer Information System Security Products of the Ministry of Public Security Detects 42 Mobile Applications That Illegally Collect and Use Personal Information

On 1 September 2026, the Quality Supervision and Inspection Center for Computer Information System Security Products of the Ministry of Public Security detected 42 mobile applications that illegally collect and use personal information. The issues identified include: (1) Failing to disclose the rules for the collection and use of personal information. (2) Collecting and using personal information without the user's consent. (3) Failing to completely and accurately inform users of the collection and use of personal information, or the stated purposes, methods, and scope of the collection and use of personal information being inconsistent with the actual collection and use. (4) Failing to specify the categories, purposes, and methods of providing personal information to third parties, as well as the names and contact information of the recipients. (5) Failing to inform users of the purposes at the same time when applying to open permissions that may collect personal information or applying to collect users' personal sensitive information such as user profiles. (6) Collecting and using personal information beyond the necessary scope, collecting personal information such as

location, contacts, and SMS messages in unrelated scenarios. (7) Failing to provide an effective function for users to cancel their accounts. (8) Failing to establish and publish channels for complaints and reports regarding personal information security, etc. ([More](#))

公安部计算机信息系统安全产品质量监督检验中心检测发现 42 款违法违规收集使用个人信息的移动应用

2026 年 9 月 1 日，公安部计算机信息系统安全产品质量监督检验中心检测发现了 42 款违法违规收集使用个人信息的移动应用，所涉问题包括：（1）未公开个人信息收集使用规则。（2）未经用户同意收集使用个人信息。（3）未完整准确告知收集使用个人信息情况，或告知收集使用个人信息目的、方式、范围与实际收集使用情况不一致。（4）未列明向第三方提供个人信息的种类、目的、方式以及接收方的名称、联系方式。（5）在申请打开可收集个人信息的权限或申请收集用户等个人敏感信息时，未同步告知用户其目的。（6）超出必要范围收集使用个人信息，在无关场景收集位置、通讯录、短信等个人信息。（7）未提供有效注销用户账号功能。（8）未建立、公布个人信息安全投诉举报渠道等。（[查看更多](#)）

Overseas News 境外动态

➤ Regulations Update 新规速递

EU: European Commission Publishes the Proposal for the *EU KIDS Act*

On 17 September 2026, the European Commission published the proposal for the *EU KIDS Act*, aiming to protect minors from high-risk digital services and AI systems, uphold the digital single market, and establish a coherent regulatory framework and enforcement structure for the protection of minors online. The proposal recognizes the risks that minors face when using certain online social networking services and video-sharing platforms, and therefore provides that children below the age of 15 shall not autonomously create accounts on the aforementioned specific platforms and systems. By providing one uniform age standard across the European Union, the proposal removes obstacles arising from diverging rules among Member States, thereby facilitating the implementation of the Digital Single Market and ensuring that all

children in the European Union enjoy an equivalent level of legal protection and safeguards. ([More](#))

欧盟：欧盟委员会发布《欧盟儿童法案》提案

2026 年 9 月 17 日，欧盟委员会发布了《欧盟儿童法案》提案，旨在保护未成年人免受高风险数字服务及人工智能系统的侵害，维护数字单一市场，并为未成年人网络保护建立连贯一致的监管框架与执法结构。该提案承认了未成年人使用某些在线社交网络和视频分享平台时所面临的风险，因此规定 15 岁以下儿童不得在上述特定平台和系统上自主创建账户。通过在欧盟全境统一年龄标准，该提案消除了各国之间不同的规定差异，从而促进了数字单一市场的实施，确保所有欧盟儿童都能获得同等的法律保护和保障。（[查看更多](#)）

EU: Reporting Obligations under the CRA Take Effect

On 11 September 2026, the reporting obligations under the EU *Cyber Resilience Act* (CRA) took effect. Manufacturers are required to report actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements. Manufacturers shall submit an early warning within 24 hours of becoming aware, and a full notification within 72 hours. A final report shall be submitted no later than the following deadlines: within 14 days after a corrective measure becomes available, for actively exploited vulnerabilities; and within one month after the 72-hour notification, for severe incidents. Pursuant to Article 24(3) of the CRA, open-source software stewards also bear reporting obligations. Manufacturers report only once through the CRA Single Reporting Platform (SRP). The notification shall be addressed to the Computer Security Incident Response Team (CSIRT) of the Member State where the manufacturer has its main establishment and, unless particularly exceptional circumstances apply, the relevant information shall be made available to the European Union Agency for Cybersecurity (ENISA) at the same time. The CSIRT initially receiving the notification shall share the notification without delay with all other CSIRTs on the territory of which the product has been made available. ([More](#))

欧盟：CRA 报告义务生效

2026 年 9 月 11 日，欧盟《网络韧性法案》（CRA）的报告义务生效，制造商须就遭主动利用的漏洞及影响含数字元素产品安全的严重事件履行报告义务。制

造商须在知悉后 24 小时内提交预警信息，72 小时内提交完整通知；最终报告需不迟于以下时限提交：对于已被主动利用的漏洞，在纠正措施可用后 14 天内；对于严重事件，在 72 小时通知后一个月内。根据 CRA 第 24（3）条，开源软件管理人也负有报告义务。制造商仅通过 CRA 单一报告平台（SRP）报告一次。通知应发送至制造商主要营业地所在的计算机安全事件响应小组（CSIRT），且除非存在特别例外情形，相关信息应同时提供给欧盟网络安全局（ENISA）。最初收到通知的 CSIRT 应毫不迟延地将该通知分享给产品已在其境内提供的所有其他 CSIRT。（[查看更多](#)）

EU: CCPC Highlights the “Access by Design” Requirements under the *Data Act*

On 12 September 2026, the EU *Data Act* took effect across the European Union. It covers a range of data-related activities, such as how data from connected products (e.g., smart watches or smartphones) are used, and the right to switch cloud data storage service providers. The Irish Competition and Consumer Protection Commission (CCPC) emphasized in particular that data holders must ensure that all products and related services placed on the EU market from 12 September 2026 are designed with direct data access in mind. Instead of users needing to request access to the data generated from connected products, data holders are required, where technically feasible, to design products and services that allow users to access relevant data directly, by default. In practice, enabling users to access data more easily through, for example, a built-in interface, an application, or another technical tool moves the *Data Act* from an access-on-request model to an access-by-design approach. Moreover, data holders should assess whether data access is provided to users directly or provided indirectly through a request mechanism. If direct access is not provided, data holders should be able to demonstrate and document the reasons. ([More](#))

欧盟：CCPC 强调《数据法案》“设计即访问”要求

2026 年 9 月 12 日，欧盟《数据法案》在欧盟全境生效，其涵盖一系列与数据相关的活动，例如联网产品（如智能手表或智能手机）数据的使用方式，以及切换云数据存储服务提供商的权利。爱尔兰竞争与消费者保护委员会（CCPC）重点提示，数据持有者必须确保，自 2026 年 9 月 12 日起投放欧盟市场的所有产品和服务在设计时即考虑直接数据访问。数据持有者无需用户请求访问联网产品生成的数据，而是被要求在设计上（在技术可行的情况下）默认允许用户直接访问相关数据。在实践中，通过例如内置接口、应用程序或其他技术工具

使用户更容易访问数据，将《数据法案》从“按请求访问”模式转变为“设计即访问”方式。并且，数据持有者应评估数据访问是直接提供给用户，还是通过请求机制间接提供。如果未提供直接访问，数据持有者应能够证明并记录其原因。（[查看更多](#)）

➤ Regulatory Actions 监管行动

UK: TikTok Withdraws Two Appeals in Children’s Privacy Action and Accepts the £12.7 Million Fine

On 24 September 2026, the UK Information Commissioner’s Office (ICO) announced that TikTok has agreed to pay the £12.7 million fine it imposed in 2023, withdrawing its appeal against the underlying penalty notice. TikTok has also withdrawn its appeal against another information notice requiring it to provide relevant documents and details concerning its processing of the personal information of 13- to 17-year-olds in its recommender systems. The 2023 fine arose from the ICO’s finding that TikTok had committed numerous breaches of data protection law, including failing to use children’s personal data lawfully. Based on economic analysis, the ICO estimated that up to 1.75 million UK children under 13 used TikTok in 2020, despite the platform’s rules prohibiting users of that age from creating accounts. TikTok failed to carry out adequate checks to identify and remove underage users, failed to provide users with clear information about how their data was collected, used, and shared, and also failed to obtain parental consent. TikTok’s earlier appeal was based on the claim that the data processing served “special purposes” (such as artistic purposes). In August 2026, the UK Upper Tribunal dismissed that claim, establishing a precedent for the withdrawal of the appeals. The ICO launched its recommender systems investigation in February 2025, concerned that young people were being served inappropriate or harmful content through such systems. However, TikTok’s appeal against the information notice had once impeded the progress of the investigation; with the appeal now withdrawn, the investigation can continue. ([More](#))

英国：TikTok 撤回两项儿童隐私上诉并接受 1270 万英镑罚款

2026 年 9 月 24 日，英国信息专员办公室（ICO）宣布，TikTok 已同意支付其 2023 年开出的 1270 万英镑罚单，撤回对该罚款通知的上诉；同时撤回对另一项信息通知的上诉，该通知要求 TikTok 就其在推荐系统中处理 13 至 17 岁青少年个人信息的情况提供相关文件和细节。2023 年罚款源于 ICO 认定 TikTok 多项违

反数据保护法律，包括未能合法使用儿童个人数据。ICO 基于经济分析估计，2020 年英国有多达 175 万名 13 岁以下儿童使用 TikTok，尽管平台规则禁止该年龄段用户创建账户，TikTok 未能开展充分检查以识别和移除未成年用户，未向用户清晰说明数据收集、使用和分享方式，也未取得家长同意。TikTok 此前的上诉以数据用于“特殊目的”（艺术等）为由提出，2026 年 8 月英国高等行政上诉法庭驳回该主张，为本次撤诉奠定先例。ICO 于 2025 年 2 月启动推荐系统调查，担忧青少年通过该系统被推送不当或有害内容，但 TikTok 对信息通知的上诉一度阻碍调查推进，如今撤诉后调查可继续。（[查看更多](#)）

Ireland: DPC Fines Google €403 Million over Violations Concerning the Processing of Location Data

On 21 September 2026, the Data Protection Commission (DPC) announced the conclusion of its inquiry into Google Ireland Limited and its final decision, imposing administrative fines totaling €403 million on Google and ordering it to bring its processing into compliance within 6 months. The inquiry was launched by the DPC on its own volition in February 2020, in its role as the Lead Supervisory Authority for Google, following complaints from several European consumer rights organizations concerning Google’s processing of location data in connection with certain services and products. The scope of the inquiry concerned Google’s processing of location data in three features – “Web & App Activity”, “Location History”, and “Location Accuracy” - between the date of application of the GDPR, 25 May 2018, and 4 February 2020. The DPC found that Google infringed the GDPR: its processing of location data in “Web & App Activity” and “Location History” lacked lawfulness and fairness; it failed, in respect of “Location Accuracy”, to demonstrate compliance with the lawfulness, fairness, and transparency principle, in breach of its accountability obligations; it breached its transparency obligations in respect of all three features; and it retained location data in “Web & App Activity” and “Location History” for longer than necessary. ([More](#))

爱尔兰：DPC 以位置数据处理违规对谷歌处以 4.03 亿欧元罚款

2026 年 9 月 21 日，爱尔兰数据保护委员会（DPC）宣布结束对谷歌爱尔兰有限公司的调查并作出最终决定，对其处以总计 4.03 亿欧元的行政罚款，并责令其在 6 个月内完成合规整改。该调查由 DPC 作为谷歌的主导监管机构于 2020 年 2 月主动发起，起因是多个欧洲消费者权益组织投诉谷歌在部分服务和产品中的

位置数据处理行为。调查范围涵盖 2018 年 5 月 25 日 GDPR 适用之日起至 2020 年 2 月 4 日期间，谷歌在“网页与应用活动”“位置记录”及“位置精确度”三个功能中的位置数据处理。DPC 认定谷歌违反了 GDPR：在“网页与应用活动”和“位置记录”中处理位置数据缺乏合法性与公平性；未能在“位置精确度”方面证明其处理符合合法、公平、透明原则，违反问责义务；三个功能均存在透明度义务违反；且在“网页与应用活动”和“位置记录”中超期保留位置数据。（[查看更多](#)）

South Korea: PIPC Issues Recommendations for Improvement to Five Companies

On 19 September 2026, the Personal Information Protection Commission (PIPC) of South Korea published the results of its follow-up inspection of the 2025 personal information processing policy evaluation. The inspection showed that Luton Technologies failed to reply to inquiries concerning the exercise of rights, while Tesla Korea and DeepSeek replied to Korean users' inquiries in English and Chinese respectively. The PIPC required the aforementioned three companies to improve their operational systems so that the requests of Korean data subjects to exercise their rights can be smoothly received and processed. With respect to the operation of domestic representatives, OpenAI and Nike provided separate email addresses during telephone inquiries but failed to reply to the relevant inquiries. The PIPC required the two companies to strengthen management and supervision to ensure that personal information-related complaints and inquiries are smoothly handled through domestic representatives. In addition, the inspection also identified issues such as partial inconsistency between the processing bases stated in the processing policies and the actual processing methods, complex access paths to the processing policies, and the failure to disclose previous versions of the processing policies. The PIPC has individually notified the relevant companies of the inspection results and will continue to guide them to carry out their own rectification. ([More](#))

韩国：PIPC 对五家企业提出改善劝告

2026 年 9 月 19 日，韩国个人信息保护委员会（PIPC）公布了 2025 年个人信息处理方针评估后续检查结果。检查显示，Luton Technologies 对权利行使咨询未予回复，特斯拉韩国与 DeepSeek 分别以英语、中文回复韩国用户的咨询。PIPC 要求上述 3 家企业完善运营体系，确保韩国信息主体的权利行使请求能够顺利受理和处理。在韩国国内代理人运营方面，OpenAI 与 Nike 在电话咨询时提供了

单独邮箱但未回复相关咨询，PIPC 要求两家企业强化管理与监督，确保通过国内代理人顺畅处理个人信息相关投诉与咨询。此外，检查还发现处理方针记载的处理依据与实际处理方式存在部分不一致、处理方针访问路径复杂、未公开旧版处理方针等问题。PIPC 已向相关企业个别通报检查结果，并将持续引导其自行整改。（[查看更多](#)）

EU: European Commission Designates ChatGPT, Reddit, and Roblox under the DSA

On 31 August 2026, the European Commission issued an announcement designating ChatGPT, Reddit, and Roblox under the *Digital Services Act* (DSA). These services declared that they have at least 45 million average monthly active users in the EU, and therefore reach the designation thresholds. ChatGPT is an AI system capable of interacting and responding to users' prompts and queries, including through web searches. Accordingly, ChatGPT is a hybrid service and is designated as a Very Large Online Search Engine (VLOSE). Reddit is a discussion-based platform that enables users to create, share, and interact with content in topic-based communities. Roblox is an immersive gaming and creation platform that enables users to create, publish, and play games developed by other users. Since these services enable users to disseminate third-party content to the public, they are designated as Very Large Online Platforms (VLOPs). Following their designation, the aforementioned services shall, within four months (i.e., before January 2027), comply with the additional obligations under the DSA, such as assessing and mitigating systemic risks arising from their services and algorithmic systems, relating to the dissemination of illegal content, negative effects on minors, users' physical and mental well-being, fundamental rights, electoral processes, and public security. The European Commission will be competent to supervise DSA compliance, in cooperation with the Irish media regulator, Coimisiún na Meán, for ChatGPT, and with the Dutch Authority for Consumers and Markets (ACM) for Reddit and Roblox. ([More](#))

欧盟：欧盟委员会依据 DSA 指定 ChatGPT、Reddit 和 Roblox

2026 年 8 月 31 日，欧盟委员会发布公告，依据《数字服务法》（DSA）指定 ChatGPT、Reddit 和 Roblox，这些服务声明其在欧盟至少达到 4500 万平均月活跃用户，因此达到指定门槛。ChatGPT 是一种 AI 系统，能够与用户的提示和查询进行交互并作出回应，包括通过网络搜索。因此，ChatGPT 是一种混合服务，

被指定为超大型在线搜索引擎（VLOSE）；Reddit 是一个基于讨论的平台，使用户能够在基于主题的社区中创建、分享内容并与之互动；Roblox 是一个沉浸式游戏与创作平台，使用户能够创建、发布并游玩由其他用户开发的游戏。由于这些服务使用户能够向公众传播第三方内容，因此它们被指定为超大型在线平台（VLOP）。被指定后，上述服务须在 4 个月内（即 2027 年 1 月前）履行 DSA 项下的额外义务，例如评估和缓解由其服务及算法系统所引发的系统性风险，这些风险涉及非法内容传播、对未成年人的负面影响、用户身心健康、基本权利、选举进程和公共安全。欧盟委员会将有权监督 DSA 合规情况，就 ChatGPT 与爱尔兰媒体委员会（Coimisiún na Meán）合作，就 Reddit 和 Roblox 与荷兰消费者与市场管理局（ACM）合作。（[查看更多](#)）

立方律师事务所编写本刊的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

This Newsletter has been prepared for clients and professional associates of Lifang & Partners. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.



北京 | 上海 | 武汉 | 广州 | 深圳 | 海口 | 首尔

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Haikou | Seoul

www.lifanglaw.com

Tel: +86 10 64096099

Email: info@lifanglaw.com

Fax: +86 10 64096260/64096261