



LIFANG & PARTNERS
立 方 律 师 事 务 所

数据与人工智能合规观察月刊

Monthly Data and AI Compliance Review

No.1

立方数据与人工智能合规观察月刊

Monthly Data and AI Compliance Review by Lifang & Partners

2026 年 9 月

No.1

目录

境内动态 Domestic News 1

➤ 新规速递 Regulations Update 1

最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》 1

Supreme People’ s Court Issues *Opinions on Adjudicating Artificial Intelligence-Related Dispute Cases in Accordance with the Law*..... 1

《道路交通安全法（修订草案）》向社会公开征求意见..... 2

Road Traffic Safety Law (Revised Draft) Opened for Public Comment..... 2

两部门发布《关于加强知识产权数据资源开发利用的意见》 3

Two Authorities Issue the *Opinions on Strengthening the Development and Utilization of Intellectual Property Data Resources*..... 3

国家网信办发布《大型个人信息处理者个人信息保护规定（征求意见稿）》 4

CAC Issues the *Provisions on the Protection of Personal Information of Large-Scale Personal Information Processors (Draft for Comment)*..... 5

公安部发布《公安机关网络安全监督检查办法》 5

Ministry of Public Security Issues the *Measures of the Public Security Organs for Cyberspace Security Supervision and Inspection*..... 6

国家网信办发布个人信息保护政策法规问答..... 6

CAC Issues Q&A on Personal Information Protection Policies and Regulations..... 7

全国网安标委发布《网络安全标准实践指南——一个人用户使用人工智能服务安全指南》.....	7
TC260 Issues the <i>Practical Guide to Cybersecurity Standards – Security Guide for Individual Users Using Artificial Intelligence Services</i>	8
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（征求意见稿）》.....	8
TC260 Issues the <i>Practical Guide to Cybersecurity Standards – Security Requirements for Cockpit Data Processing (Draft for Comment)</i>	9
➤ 监管行动 Regulatory Actions	9
工信部通报 26 款 App（SDK）存在违规收集个人信息等行为.....	9
MIIT Reports That 26 Apps (SDKs) Are Found to Have Engaged in Acts Such as Illegal Collection of Personal Information.....	9
三部门通报 2026 年个人信息保护系列专项行动取得阶段性成效....	10
Three Authorities Report Phased Achievements in the 2026 Series of Special Campaigns on Personal Information Protection.....	10
国家计算机病毒应急处理中心检测发现 75 款违法违规收集使用个人信息的移动应用.....	11
CVERC Detects 75 Mobile Applications That Illegally Collect and Use Personal Information.....	11
公安部网安局公布打击侵犯公民个人信息犯罪 10 起典型案例.....	12
Cybersecurity Bureau of the Ministry of Public Security Releases 10 Typical Cases of Crackdown on Crimes of Infringing Upon Citizens’ Personal Information.....	12
网络安全审查办公室对派拓公司在华销售产品启动网络安全审查...	13
Cybersecurity Review Office Initiates Cybersecurity Review of Products Sold in China by Palo Alto Networks.....	13
常德市武陵区一公司超范围收集敏感个人信息被行政处罚.....	14

A Company in Wuling District, Changde City, Imposed Administrative Penalty for Collecting Sensitive Personal Information Beyond the Permitted Scope.....	14
境外动态 Overseas News.....	15
➤ 新规速递 Regulations Update	15
越南：越南颁布个人数据保护行政处罚新规.....	15
Vietnam: Vietnam Promulgates New Administrative Penalty Regulations on Personal Data Protection.....	15
菲律宾：NPC 发布关于在 AI 生成媒体中使用真人肖像的通知	16
Philippines: NPC Issues Notice on the Use of Real Individuals' Likenesses in AI-Generated Media.....	16
法国：CNIL 发布《关于识别和管理数据保护官利益冲突的指南》 ..	17
France: CNIL Issues <i>Guidelines on Identifying and Managing Conflicts of Interest for Data Protection Officers</i>	17
➤ 监管行动 Regulatory Actions.....	18
巴西：ANPD 因未成年人数据保护问题对 TikTok 处以 1.537 亿雷亚尔罚款.....	18
Brazil: ANPD Fines TikTok BRL 153.7 Million for Issues Concerning the Protection of Minors' Data.....	18
荷兰：AP 因自动化决策问题对 Uber 处以 8.25 亿欧元罚款	19
Netherlands: AP Fines Uber €825 Million for Issues Concerning Automated Decision-Making.....	19
英国：英国高等行政上诉法庭驳回 TikTok 上诉.....	20
UK: UK Upper Tribunal Dismisses TikTok' s Appeal.....	20

境内动态 Domestic News

➤ 新规速递 Regulations Update

最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》

2026年9月7日，最高人民法院发布了《关于依法审理涉人工智能纠纷案件的意见》（以下简称《意见》）。《意见》共五部分二十四条，是首部由国家最高审判机构发布的涉人工智能司法裁判规则文件。《意见》明确了审理涉人工智能纠纷案件应当坚持的指导思想，并明确提出坚持以人为本、支持创新发展、筑牢安全防线等三个基本原则。《意见》明确了涉人工智能案件归责原则及过错认定标准，即法律没有明确规定适用无过错责任或者过错推定责任的，应当依照民法典第一千一百六十五条第一款规定的过错责任原则认定行为人是否承担侵权责任。《意见》强调，为人工智能模型训练，在合理范围内处理个人自行公开的或者其他已经合法公开的个人信息，且个人未明确拒绝的，一般不认定为侵害个人信息权益的行为。对个人权益有重大影响的，应当依照法律规定取得个人同意。《意见》指出，生成式人工智能自动生成的内容侵害他人名誉权、隐私权等人格权益，经权利人通知，生成式人工智能服务提供者未及时采取停止生成侵权内容等必要措施的，应当对造成的损害依法承担侵权责任。

[\(查看更多\)](#)

Supreme People's Court Issues *Opinions on Adjudicating Artificial Intelligence-Related Dispute Cases in Accordance with the Law*

On 7 September 2026, the Supreme People's Court issued the *Opinions on Adjudicating Artificial Intelligence-Related Dispute Cases in Accordance with the Law* (Opinions). Comprising five parts and 24 articles, the Opinions are the first document on judicial adjudication rules concerning artificial intelligence issued by the country's highest judicial organ. The Opinions clarify the guiding ideology to be upheld in adjudicating AI-related dispute cases, and explicitly put forward three basic principles: adhering to a people-oriented approach, supporting innovative development, and firmly establishing a security defense line. The Opinions clarify the principles of liability attribution and the standards for determining fault in AI-related cases: where the law does not explicitly provide for the application of strict liability or presumed fault liability, whether an actor shall bear tort liability shall be determined in accordance with

the principle of fault liability prescribed in Article 1165, Paragraph 1 of the Civil Code. The Opinions emphasize that, for the purpose of AI model training, processing, within a reasonable scope, personal information voluntarily disclosed by the individual or otherwise lawfully made public, where the individual has not explicitly refused, shall generally not be deemed an act infringing upon personal information rights and interests. Where such processing has a significant impact on the rights and interests of the individual, the individual's consent shall be obtained in accordance with the law. The Opinions state that where content automatically generated by generative artificial intelligence infringes upon personality rights and interests such as the right to reputation and the right to privacy of others, and the generative artificial intelligence service provider, upon notification by the rights holder, fails to promptly take necessary measures such as ceasing the generation of infringing content, it shall bear tort liability in accordance with the law for the damage caused. ([More](#))

《道路交通安全法（修订草案）》向社会公开征求意见

2026年8月28日，《道路交通安全法（修订草案）》（以下简称“修订草案”）经第十四届全国人大常委会第二十四次会议审议后，向社会公开征求意见，意见反馈截止时间为2026年9月26日。修订草案共九章一百七十条，设置了“自动驾驶汽车的特别规定”专章，明确自动驾驶汽车和辅助驾驶功能的概念、上道路行驶条件、违章处理原则、保险制度、数据处理活动等。修订草案规定，自动驾驶汽车登记后上道路行驶，可以在设计运行条件下激活自动驾驶功能。自动驾驶汽车生产企业、进口企业应当确保自动驾驶汽车在不符合设计运行条件时不能激活自动驾驶功能。任何单位和个人不得擅自改变自动驾驶功能。修订草案明确，自动驾驶汽车在自动驾驶功能激活状态下发生道路交通安全违法行为的，由自动驾驶汽车生产企业、进口企业接受处理。自动驾驶汽车生产企业、进口企业认为道路交通安全违法行为与自动驾驶功能无关的，应当承担举证责任。（[查看更多](#)）

Road Traffic Safety Law (Revised Draft) Opened for Public Comment

On 28 August 2026, the *Road Traffic Safety Law (Revised Draft)* (Revised Draft) was opened for public comment following its deliberation at the 24th Session of the Standing Committee of the 14th National People's Congress. The deadline for submitting comments is 26 September 2026. The Revised Draft comprises nine

chapters and 170 articles, and includes a dedicated chapter on “Special Provisions on Autonomous Driving Vehicles,” which clarifies the concepts of autonomous driving vehicles and driver-assistance functions, the conditions for travelling on roads, the principles for handling traffic violations, the insurance system, and data processing activities. The Revised Draft provides that an autonomous driving vehicle may, after registration, travel on roads and activate its autonomous driving function within its operational design domain. Manufacturers and importers of autonomous driving vehicles shall ensure that the autonomous driving function cannot be activated when the vehicle does not meet the operational design domain conditions. No entity or individual may alter the autonomous driving function without authorization. The Revised Draft clarifies that where a road traffic safety violation occurs while an autonomous driving vehicle is operating with its autonomous driving function activated, the manufacturer or importer of the autonomous driving vehicle shall be subject to the handling of such violation. Where the manufacturer or importer contends that the road traffic safety violation is unrelated to the autonomous driving function, it shall bear the burden of proof. ([More](#))

两部门发布《关于加强知识产权数据资源开发利用的意见》

2026年8月26日，国家知识产权局和国家数据局发布了《关于加强知识产权数据资源开发利用的意见》（以下简称《意见》），旨在更好发挥数据要素作用、加快公共数据资源开发利用的决策部署，进一步加强知识产权数据资源开发利用。《意见》提出：（1）夯实知识产权数据资源基础，包括健全知识产权数据资源管理制度、完善知识产权数据资源标准体系、加强知识产权数据基础设施建设、推进人工智能等新技术应用。（2）扩大知识产权数据资源供给：推进知识产权数据共享、推动知识产权数据开放、探索知识产权公共数据授权运营。

（3）深化知识产权数据资源应用：支撑政府决策、优化信息服务、赋能企业创新。（4）强化组织实施：国家知识产权局会同国家数据局统筹知识产权数据开发利用，地方协同释放价值。（[查看更多](#)）

Two Authorities Issue the Opinions on Strengthening the Development and Utilization of Intellectual Property Data Resources

On 26 August 2026, the China National Intellectual Property Administration and the National Data Administration issued the *Opinions on Strengthening the Development*

and Utilization of Intellectual Property Data Resources (Opinions), aiming to better leverage the role of data elements, accelerate the decision-making and deployment on the development and utilization of public data resources, and further strengthen the development and utilization of intellectual property data resources. The Opinions propose the following: (1) Consolidate the foundation of intellectual property data resources, including improving the management system for intellectual property data resources, refining the standards system for intellectual property data resources, strengthening the development of intellectual property data infrastructure, and promoting the application of new technologies such as artificial intelligence. (2) Expand the supply of intellectual property data resources: promoting the sharing of intellectual property data, advancing the opening of intellectual property data, and exploring the authorized operation of intellectual property public data. (3) Deepen the application of intellectual property data resources: supporting government decision-making, optimizing information services, and empowering enterprise innovation. (4) Strengthen organization and implementation: the China National Intellectual Property Administration, together with the National Data Administration, shall coordinate the development and utilization of intellectual property data, and local authorities shall work in coordination to unlock value. ([More](#))

国家网信办发布《大型个人信息处理者个人信息保护规定（征求意见稿）》

2026 年 8 月 7 日，国家互联网信息办公室（以下简称“国家网信办”）发布了《大型个人信息处理者个人信息保护规定（征求意见稿）》（以下简称《规定》），共六章五十条，向社会公开征求意见，意见反馈截止时间为 2026 年 9 月 7 日。《规定》确立了大型个人信息处理者的认定申报机制：处理 1000 万人以上个人信息，且自评估符合“提供涉及个人信息处理的重要网络服务或经营范围涵盖多种相关业务”、“个人信息处理活动对国家安全、经济运行、社会稳定、公共健康和安全等具有重要影响”的，应通过所在地省级网信部门向国家网信部门申报认定。在告知义务方面，《规定》要求被认定者以结构化清单形式逐项披露各功能服务的个人信息收集使用情况、嵌入 SDK 的名称及完整处理规则访问途径、个人已同意的信息种类与处理目的方式等内容。此外，大型个人信息处理者应自认定之日起 6 个月内成立主要由外部成员组成的个人信息保护监督委员会，国家网信办同步发布了该委员会工作规则制定指引。（[查看更多](#)）

CAC Issues the *Provisions on the Protection of Personal Information of Large-Scale Personal Information Processors (Draft for Comment)*

On 7 August 2026, the Cyberspace Administration of China (CAC) issued the *Provisions on the Protection of Personal Information of Large-Scale Personal Information Processors (Draft for Comment)* (Provisions), comprising six chapters and 50 articles. The Provisions are open for public comment, with the deadline for feedback being 7 September 2026. The Provisions establish a declaration and recognition mechanism for large-scale personal information processors: where a processor handles the personal information of more than 10 million natural persons and, following self-assessment, meets the criteria of either “providing important internet services involving personal information processing or having a business scope covering multiple relevant businesses” or “its personal information processing activities have a significant impact on national security, economic operation, social stability, public health and safety, etc.,” it shall declare for recognition as a large-scale personal information processor to the CAC through the provincial cyberspace administration at its locality. Regarding the obligation to inform, the Provisions require recognized processors to disclose, item by item in the form of a structured list, the collection and use of personal information for each functional service, the names of embedded software development kits (SDKs) and the access channels to their complete processing rules, the categories of personal information to which the individual has consented and the purposes and methods of processing, and other relevant content. In addition, a large-scale personal information processor shall, within six months from the date of recognition, establish a personal information protection supervisory committee composed mainly of external members. The CAC has simultaneously issued guidelines for formulating the working rules of such committee. ([More](#))

公安部发布《公安机关网络空间安全监督检查办法》

2026年8月6日，公安部发布了《公安机关网络空间安全监督检查办法》（以下简称《办法》），自2026年10月1日起实施。《办法》共二十三条，适用于公安机关依法对网络运营者、数据处理者、个人信息处理者等履行法律法规规定的网络安全、数据安全、信息安全义务情况开展的监督检查。《办法》明确，对曾发生网络安全、数据安全等事件，或者因未履行法定网络安全、数据安全、信息安全义务被行政处罚且未按照要求整改的，应当重点开展监督检查。《办

法》规定，对网络安全等级保护第三级（含）以上的网络运营者、关键信息基础设施运营者，每年开展一次日常性的现场检查。《办法》指出，公安机关开展网络空间安全现场检查，可以采取进入查阅、复制与监督检查事项相关的信息等措施。（[查看更多](#)）

Ministry of Public Security Issues the *Measures of the Public Security Organs for Cyberspace Security Supervision and Inspection*

On 6 August 2026, the Ministry of Public Security issued the *Measures of the Public Security Organs for Cyberspace Security Supervision and Inspection* (Measures), which shall come into effect on 1 October 2026. The Measures comprise 23 articles and apply to the supervision and inspection conducted by public security organs in accordance with the law on the performance by network operators, data processors, and personal information processors of their obligations regarding cybersecurity, data security, and information security as prescribed by laws and regulations. The Measures clarify that priority shall be given to conducting supervision and inspection in respect of entities that have previously experienced cybersecurity, data security, or other incidents, or that have been subject to administrative penalties for failing to perform their statutory obligations regarding cybersecurity, data security, and information security and have not rectified the situation as required. The Measures provide that routine on-site inspections shall be conducted once a year in respect of network operators at Level 3 (inclusive) or above of the classified protection of cybersecurity, and operators of critical information infrastructure. The Measures state that, when conducting on-site cyberspace security inspections, public security organs may take measures such as entering premises to inspect, and copying information related to the matters under supervision and inspection. ([More](#))

国家网信办发布个人信息保护政策法规问答

2026年8月12日，国家网信办发布了个人信息保护政策法规问答。问答从反面列举了违法违规处理已公开个人信息的具体情形，进而明确了处理此类信息的合规底线，包括：（1）向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息；（2）利用已公开的个人信息从事网络暴力、传播网络谣言和虚假信息等活动；（3）处理个人明确拒绝处理的已公开个人信息；（4）对个人权益有重大影响，未取得个人同意；（5）收集、留存或处理已公开个人

信息的规模、时间或使用目的超出合理范围。同时，问答列举了导致个人信息泄露的常见原因，例如个人信息明文存储和传输，未采取适当的加密、去标识化等安全技术措施等原因。（[查看更多](#)）

CAC Issues Q&A on Personal Information Protection Policies and Regulations

On 12 August 2026, the CAC issued a Q&A on personal information protection policies and regulations. The Q&A enumerates, by way of negative examples, specific circumstances of unlawful processing of already public personal information, and thereby clarifies the compliance baseline for processing such information, including: (1) sending commercial information unrelated to the purpose of disclosure to email addresses, mobile phone numbers, etc. contained in already public personal information; (2) using already public personal information to engage in activities such as cyberbullying, dissemination of online rumors and false information; (3) processing already public personal information that the individual has explicitly refused to have processed; (4) processing that has a significant impact on the rights and interests of the individual without obtaining the individual's consent; and (5) the scale, duration, or purpose of use of collecting, retaining, or processing already public personal information exceeding a reasonable scope. Meanwhile, the Q&A lists common causes of personal information leaks, such as the storage and transmission of personal information in plaintext, and the failure to adopt appropriate security technical measures such as encryption and de-identification. ([More](#))

全国网安标委发布《网络安全标准实践指南——个人用户使用人工智能服务安全指南》

2026 年 8 月 24 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——个人用户使用人工智能服务安全指南》（以下简称《指南》）。《指南》适用于指导个人用户安全地通过互联网使用人工智能服务，也可为人工智能服务的技术提供者、服务开发者、服务运营者保障个人用户的安全使用提供参考。《指南》明确，个人用户在使用人工智能服务的过程中，应使用从正规渠道获取的人工智能服务，优先选用最新版本；涉及生成式人工智能服务的，应选择已通过生成式人工智能服务备案的大模型，不通过来源不明的中转站、未授权代理等方式使用相关服务。《指南》强调，个人用户在使用人工智能生成合成内容时，应积极履行生成合成内容标

识义务，关注相关服务输出内容是否具备生成合成内容标识，不恶意裁剪、删除标识。（[查看更多](#)）

TC260 Issues the Practical Guide to Cybersecurity Standards - Security Guide for Individual Users Using Artificial Intelligence Services

On 24 August 2026, the National Technical Committee 260 on Cybersecurity of SAC (TC260) issued the *Practical Guide to Cybersecurity Standards - Security Guide for Individual Users Using Artificial Intelligence Services* (Guide). The Guide applies to guiding individual users in securely using artificial intelligence services via the internet, and may also serve as a reference for technology providers, service developers, and service operators of artificial intelligence services in ensuring the secure use by individual users. The Guide clarifies that, in the course of using artificial intelligence services, individual users shall use artificial intelligence services obtained from legitimate channels and prioritize the latest versions; where generative artificial intelligence services are involved, they shall select large models that have completed the generative artificial intelligence service filing, and shall not use relevant services through relay stations of unknown origin, unauthorized proxies, or other such means. The Guide emphasizes that, when using artificial intelligence to generate synthetic content, individual users shall actively fulfill the obligation to label generated synthetic content, pay attention to whether the content output by relevant services bears a generated synthetic content label, and shall not maliciously crop or delete such labels. ([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（征求意见稿）》

2026年8月20日，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（征求意见稿）》（以下简称《要求》），向社会公开征求意见，意见反馈截止时间为2026年9月3日。《要求》适用于座舱数据处理者开展非运营车辆的座舱数据处理活动，也可作为汽车座舱功能设计研发提供参考。《要求》明确，座舱数据处理者处理者应满足以下方面的安全要求：（1）语音唤醒：除驾驶人自主设定外，车内传声器应默认不收集座舱数据等。（2）智能语音对话：应为用户提供开启和关闭车载智能语音对话功能的方式等。（3）驾驶员状

态监测系统：应告知用于驾驶员状态监测系统功能的摄像头位置等。（4）远程查看：应对申请远程查看者进行身份认证等。（[查看更多](#)）

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

On 20 August 2026, TC260 issued the *Practical Guide to Cybersecurity Standards - Security Requirements for Cockpit Data Processing (Draft for Comment)* (Requirements), which is open for public comment with the deadline for feedback being 3 September 2026. The Requirements apply to cockpit data processing activities conducted by cockpit data processors in respect of non-commercial vehicles, and may also serve as a reference for the design and development of automotive cockpit functions. The Requirements clarify that cockpit data processors shall satisfy the following security requirements: (1) Voice wake-up: unless independently configured by the driver, in-vehicle microphones shall, by default, not collect cockpit data, etc. (2) Intelligent voice dialogue: users shall be provided with a means to enable and disable the in-vehicle intelligent voice dialogue function, etc. (3) Driver status monitoring system: the location of cameras used for the driver status monitoring system function shall be disclosed, etc. (4) Remote viewing: identity authentication shall be performed on applicants for remote viewing, etc. ([More](#))

➤ 监管行动 Regulatory Actions

工信部通报 26 款 App（SDK）存在违规收集个人信息等行为

2026 年 8 月 25 日，工信部通报了 26 款 App（SDK）存在违规收集个人信息等行为，所涉问题包括：（1）违规收集个人信息；（2）超范围收集个人信息；（3）违规使用个人信息；（4）信息窗口无法关闭；（5）信息窗口点击乱跳转；（6）强制用户使用定向推送功能；（7）App 强制、频繁、过度索取权限；（8）App 频繁自启动和关联启动；（9）违规提供自动续费服务；（10）欺骗误导用户下载 App；（11）SDK 信息公示不到位。上述 App（SDK）应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。（[查看更多](#)）

MIIT Reports That 26 Apps (SDKs) Are Found to Have Engaged in Acts Such as Illegal Collection of Personal Information

On 25 August 2026, the Ministry of Industry and Information Technology (MIIT) reported that 26 Apps (SDKs) were found to have engaged in acts such as illegal collection of personal information. The issues identified include: (1) illegal collection of personal information; (2) collection of personal information beyond the permitted scope; (3) illegal use of personal information; (4) information windows that cannot be closed; (5) random redirection upon clicking information windows; (6) forcing users to use targeted push notification functions; (7) Apps forcibly, frequently, and excessively requesting permissions; (8) Apps frequently self-starting and associated-starting; (9) illegally providing auto-renewal services; (10) deceiving or misleading users into downloading Apps; and (11) inadequate disclosure of SDK information. The aforementioned Apps (SDKs) shall carry out rectification in accordance with relevant provisions. Where rectification is not properly implemented, the MIIT shall, in accordance with laws and regulations, organize and carry out relevant disposition work. ([More](#))

三部门通报 2026 年个人信息保护系列专项行动取得阶段性成效

2026 年 8 月 19 日，中央网信办、工信部、公安部通报了 2026 年个人信息保护系列专项行动取得阶段性成效，包括：（1）累计对 2 万余款 App、SDK 个人信息收集使用情况开展核查检测，督促 4000 余款完成合规整改，公开通报 1100 余款存在违法违规问题的 App、SDK，对 400 余款采取下架等处置处罚措施。（2）针对个人信息处理规则未明确收集个人信息用于广告、用户画像，未提供个性化广告关闭选项等问题，对 1000 余家企业和机构的相关产品开展核查检测并督促整改。（3）开展教育、交通、卫生健康、金融等领域个人信息风险排查，累计摸排 9 万余家企业和机构，发现并督促整改各类隐患问题 1.2 万余个。（4）加大个人信息违法犯罪打击力度，加强线索监测发现，严打涉信息泄露、信息倒卖等违法犯罪行为，严惩行业“内鬼”。（[查看更多](#)）

Three Authorities Report Phased Achievements in the 2026 Series of Special Campaigns on Personal Information Protection

On 19 August 2026, CAC, MIIT, and the Ministry of Public Security reported the phased achievements of the 2026 series of special campaigns on personal information protection, including: (1) Having conducted verification and testing on the collection and use of personal information by more than 20,000 Apps and SDKs in total, urged

more than 4,000 to complete compliance rectification, publicly reported more than 1,100 Apps and SDKs with illegal and non-compliant issues, and imposed disposition and penalty measures such as delisting on more than 400. (2) In response to issues such as personal information processing rules failing to specify that personal information is collected for advertising and user profiling, and the failure to provide an option to disable personalized advertising, having conducted verification and testing on relevant products of more than 1,000 enterprises and institutions and urged rectification. (3) Having carried out personal information risk screening in sectors such as education, transportation, health, and finance, investigating and screening a total of more than 90,000 enterprises and institutions, and identifying and urging the rectification of more than 12,000 hidden dangers and problems of various types. (4) Having intensified the crackdown on personal information-related illegal and criminal acts, strengthened the monitoring and discovery of leads, severely cracked down on illegal and criminal acts involving information leaks and illegal trading of information, and severely punished industry “insiders.” ([More](#))

国家计算机病毒应急处理中心检测发现 75 款违法违规收集使用个人信息的移动应用

2026 年 8 月 14 日，国家计算机病毒应急处理中心检测发现了 75 款移动应用存在违法违规收集使用个人信息的问题，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；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）隐私政策未逐一系列出 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；App 客户端向第三方提供个人信息，未经用户同意，未做匿名化处理；（4）未采取相应的加密、去标识化等安全技术措施；（5）无隐私政策。（[查看更多](#)）

CVERC Detects 75 Mobile Applications That Illegally Collect and Use Personal Information

On 14 August 2026, the National Computer Virus Emergency Response Center (CVERC) detected that 75 mobile applications had issues of illegally collecting and using personal information, including but 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; 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; and the App client providing personal information to third parties without the user's consent and without anonymization; (4) Failing to adopt corresponding security technical measures such as encryption and de-identification; and (5) Having no privacy policy. ([More](#))

公安部网安局公布打击侵犯公民个人信息犯罪 10 起典型案例

2026 年 8 月 11 日，公安部网安局发布了打击侵犯公民个人信息犯罪 10 起典型案例。此次公布的案件涉及非法注册贩卖实名账号、利用黑客技术搭建社工库非法查询、批量窃取电商订单信息、以科技公司为掩护盗取房产中介数据等多种违法犯罪手法。犯罪链条覆盖信息窃取、倒卖、利用等环节，涉案金额从数十万元至数百万元不等，单个案件涉及公民个人信息数量最高达 600 余万条。目前，相关犯罪嫌疑人已被依法采取刑事强制措施或移送起诉。公安部网安局表示，将持续深入推进“净网”专项行动，依法严厉打击侵犯公民个人信息违法犯罪活动，切实维护公民个人信息安全与合法权益。（[查看更多](#)）

Cybersecurity Bureau of the Ministry of Public Security Releases 10 Typical Cases of Crackdown on Crimes of Infringing Upon Citizens' Personal Information

On 11 August 2026, the Cybersecurity Bureau of the Ministry of Public Security released 10 typical cases of crackdown on crimes of infringing upon citizens' personal information. The cases released involve a variety of illegal and criminal *modi operandi*, including the illegal registration and sale of real-name accounts, the use of hacking techniques to build social engineering databases for illegal queries, the bulk theft of e-commerce order information, and the theft of real estate agency data under the cover of a technology company. The criminal chains cover the links of information theft, resale, and exploitation. The amounts involved in the cases range from hundreds of thousands to millions of yuan, with the highest number of citizens' personal information involved in a single case reaching more than 6 million items. At present, the relevant criminal suspects have been subject to criminal compulsory measures in accordance with the law or transferred for prosecution. The Cybersecurity Bureau of the Ministry of Public Security stated that it will continue to thoroughly advance the "Clean Net" special campaign, severely crack down on illegal and criminal activities infringing upon citizens' personal information in accordance with the law, and earnestly safeguard citizens' personal information security and lawful rights and interests. ([More](#))

网络安全审查办公室对派拓公司在华销售产品启动网络安全审查

2026年8月6日，国家网信办发布公告称，为保障关键信息基础设施安全稳定运行，防范网络安全风险隐患，维护国家安全，依据《国家安全法》《网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对派拓公司（Palo Alto Networks）在华销售的产品实施网络安全审查。根据派拓公司官网介绍，其在华主营产品为网络安全平台，提供“实时人工智能驱动的网络安全”“云交付的安全服务”“新一代防火墙”等服务。（[查看更多](#)）

Cybersecurity Review Office Initiates Cybersecurity Review of Products Sold in China by Palo Alto Networks

On 6 August 2026, CAC issued an announcement stating that, in order to ensure the secure and stable operation of critical information infrastructure, prevent cybersecurity risks and hidden dangers, and safeguard national security, the Cybersecurity Review Office, in accordance with the *National Security Law* and the *Cybersecurity Law* and pursuant to the *Cybersecurity Review Measures*, has implemented a cybersecurity review on products sold in China by Palo Alto Networks. According to the introduction

on Palo Alto Networks’ official website, its main products in China are cybersecurity platforms, providing services such as “real-time AI-driven cybersecurity,” “cloud-delivered security services,” and “next-generation firewalls.” ([More](#))

常德市武陵区一公司超范围收集敏感个人信息被行政处罚

2026年8月25日，武陵区网信办通报了一公司超范围收集敏感个人信息被行政处罚。经核查发现，该公司在与骑手签订管理合同后，要求骑手拍摄一段含人脸手持合同的视频，该公司员工再通过微信上传至总公司留存。该行为违反了《个人信息保护法》《常见类型移动互联网应用程序必要个人信息范围规定》的相关规定，存在超范围、过度收集敏感个人信息，未采取必要措施保障所处理的个人信息安全的问题。武陵区网信办依法对该公司作出责令改正、警告的行政处罚。该公司负责人承诺，将严格落实监管要求，清理存量人脸视频数据，规范个人信息全流程管理，严守数据安全合规底线。（[查看更多](#)）

A Company in Wuling District, Changde City, Imposed Administrative Penalty for Collecting Sensitive Personal Information Beyond the Permitted Scope

On 25 August 2026, the Wuling District Cyberspace Administration reported that a company had been imposed an administrative penalty for collecting sensitive personal information beyond the permitted scope. Upon verification, it was found that, after signing management contracts with delivery riders, the company required the riders to shoot a video showing their face while holding the contract, and the company’s employees then uploaded the videos via WeChat to the headquarters for retention. This act violated the relevant provisions of the *Personal Information Protection Law* and the *Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications*, and involved the issues of collecting sensitive personal information beyond the permitted scope and excessively, as well as failing to take necessary measures to ensure the security of the personal information being processed. The Wuling District Cyberspace Administration, in accordance with the law, imposed on the company an administrative penalty of ordering rectification and issuing a warning. The person in charge of the company undertook that it would strictly implement regulatory requirements, clear the existing stock of facial video data, standardize the full-process management of personal information, and strictly adhere to the bottom line of data security compliance. ([More](#))

境外动态 Overseas News

➤ 新规速递 Regulations Update

越南：越南颁布个人数据保护行政处罚新规

2026 年 8 月 19 日，越南政府颁布第 330/2026/ND-CP 号法令，自颁布之日起生效。该法令适用于在越南领域内实施相关违规行为的越南及外国个人与组织，包括向越南公民提供跨境服务并处理其个人数据的外国企业。覆盖违规类型涵盖个人数据保护原则与禁止行为、数据主体同意、数据主体权利行使、数据处理行为等全链条环节。罚款幅度方面，超范围或超目的处理数据、未保证数据准确性、超期存储等行为，处 2000 万至 4000 万越南盾；阻挠个人数据保护活动、利用他人数据从事违法行为，处 4000 万至 6000 万越南盾；未经同意处理数据、捆绑同意、默认勾选同意、未按目的分别取得同意、未留存同意记录、未告知敏感数据处理等同意类违规，处 3000 万至 5000 万越南盾；在数据主体要求停止或主管机关责令后仍继续处理、将沉默视为同意的，处 5000 万至 7000 万越南盾。此外，法令还规定了没收违法工具与所得、强制不可恢复地删除违规数据、公开赔礼道歉、强制更正数据等附加处罚与补救措施。（[查看更多](#)）

Vietnam: Vietnam Promulgates New Administrative Penalty Regulations on Personal Data Protection

On 19 August 2026, the Government of Vietnam promulgated Decree No. 330/2026/ND-CP, which shall take effect from the date of promulgation. The Decree applies to Vietnamese and foreign individuals and organizations that commit relevant violations within the territory of Vietnam, including foreign enterprises that provide cross-border services to Vietnamese citizens and process their personal data. The types of violations covered encompass the full chain of links, including the principles of personal data protection and prohibited acts, consent of data subjects, exercise of data subject rights, and data processing activities. Regarding the range of fines: processing data beyond the permitted scope or purpose, failing to ensure data accuracy, and storing data beyond the required period shall be subject to a fine of VND 20 million to 40 million; obstructing personal data protection activities and using others' data to engage in illegal acts shall be subject to a fine of VND 40 million to 60 million; consent-related violations, including processing data without consent, bundling consent, pre-ticked

consent, failing to obtain separate consent for each purpose, failing to retain records of consent, and failing to notify sensitive data processing, shall be subject to a fine of VND 30 million to 50 million; and continuing to process data after a data subject requests cessation or a competent authority so orders, or treating silence as consent, shall be subject to a fine of VND 50 million to 70 million. In addition, the Decree also provides for additional penalties and remedial measures such as confiscation of illegal tools and proceeds, compulsory irreversible deletion of violating data, public apology, and compulsory correction of data. ([More](#))

菲律宾：NPC 发布关于在 AI 生成媒体中使用真人肖像的通知

2026 年 8 月 11 日，菲律宾国家隐私委员会（NPC）发布了关于在 AI 生成媒体中使用真人肖像的通知。NPC 提醒公众，根据 2012 年《数据隐私法》（DPA），个人的面部和肖像属于个人信息。在某些情况下，摄影和视频媒体也可能构成直接识别个人身份的生物识别信息。使用 AI 工具从真实个人的面部和肖像生成图像或视频，并发布或分享由此产生的图像和/或视频，属于个人数据的处理形式，无论所生成媒体的性质或目的如何。与任何个人数据处理一样，这些行为必须具有合法目的，并且必须符合 DPA 中规定的合法处理标准之一。在没有合法依据的情况下使用他人的面部和肖像创建合成媒体，可能构成 DPA 第 25 条下的未经授权处理，并且根据此类处理的程度（包括发布和分享此类 AI 生成媒体），还可能构成违反 DPA 其他处罚条款的行为。这些违法行为将带来刑事处罚以及可能的民事和行政责任，且不影响其他法律规定的救济措施。（[查看更多](#)）

Philippines: NPC Issues Notice on the Use of Real Individuals' Likenesses in AI-Generated Media

On 11 August 2026, the National Privacy Commission (NPC) of the Philippines issued a notice on the use of real individuals' likenesses in AI-generated media. The NPC reminds the public that, under the *Data Privacy Act of 2012* (DPA), an individual's face and likeness constitute personal information. In certain circumstances, photographic and video media may also constitute biometric information that directly identifies an individual. The use of AI tools to generate images or videos from the face and likeness of a real individual, and the publication or sharing of the resulting images and/or videos, constitute a form of processing of personal data, regardless of the nature or purpose of

the generated media. As with any processing of personal data, such acts must have a lawful purpose and must comply with one of the criteria for lawful processing prescribed in the DPA. The creation of synthetic media using another person's face and likeness without a lawful basis may constitute unauthorized processing under Section 25 of the DPA, and, depending on the extent of such processing (including the publication and sharing of such AI-generated media), may also constitute acts violating other penal provisions of the DPA. Such violations will entail criminal penalties as well as potential civil and administrative liability, without prejudice to remedies provided under other laws. ([More](#))

法国：CNIL 发布《关于识别和管理数据保护官利益冲突的指南》

2026 年 8 月 10 日，法国国家信息自由委员会（CNIL）发布了《关于识别和管理数据保护官利益冲突的指南》。数据保护官（DPO）除履行《通用数据保护条例》（GDPR）第 39 条规定的职责外，还可以在指定机构内承担其他职能（兼职 DPO），前提是这些任务或工作的执行不得损害其作为 DPO 行使职能，包括不得使其缺乏履行职责所需的时间，并且这种职责叠加不得使其陷入利益冲突境地。以下问题可帮助机构识别利益冲突：（1）对于机构/集团内部 DPO：与 DPO 职责叠加的其他职能和/或任务是什么？DPO 是否承担管理职务？DPO 和/或其团队成员是否在决定机构实施的数据处理的目的和/或方式方面拥有决策权？（2）对于外部 DPO：担任律师或受雇于律师事务所的 DPO，是否曾参与代表该机构处理与数据保护相关的诉讼？DPO 是否属于可能与指定机构存在利益冲突的机构的人员或管理层？（3）多个机构共用 DPO：DPO 是否也被可能与指定机构存在利益冲突的机构指定？（[查看更多](#)）

France: CNIL Issues *Guidelines on Identifying and Managing Conflicts of Interest for Data Protection Officers*

On 10 August 2026, the French National Commission on Informatics and Liberty (CNIL) issued the *Guidelines on Identifying and Managing Conflicts of Interest for Data Protection Officers*. In addition to performing the tasks prescribed in Article 39 of the *General Data Protection Regulation* (GDPR), a Data Protection Officer (DPO) may also undertake other functions within the appointing organization (a part-time DPO), provided that the performance of such tasks or duties does not impair the exercise of the DPO's functions, including by depriving the DPO of the time necessary

to perform his or her duties, and that such accumulation of functions does not place the DPO in a situation of conflict of interest. The following questions may assist organizations in identifying conflicts of interest: (1) For an in-house DPO within an organization/group: What other functions and/or tasks overlap with the DPO's duties? Does the DPO hold a management position? Do the DPO and/or members of his or her team have decision-making power in determining the purposes and/or means of the data processing implemented by the organization? (2) For an external DPO: Has the DPO, acting as a lawyer or being employed by a law firm, previously been involved in representing the organization in data protection-related litigation? Is the DPO a member of the staff or management of an organization that may have a conflict of interest with the appointing organization? (3) For a DPO shared by multiple organizations: Has the DPO also been appointed by an organization that may have a conflict of interest with the appointing organization? ([More](#))

➤ 监管行动 **Regulatory Actions**

巴西：ANPD 因未成年人数据保护问题对 TikTok 处以 1.537 亿雷亚尔罚款

2026 年 8 月 25 日，巴西国家数据保护局（ANPD）在《联邦官方公报》公布处罚决定，对 TikTok 母公司字节跳动处以 1.537 亿雷亚尔罚款，理由是其在处理儿童与青少年个人数据时违反《通用数据保护法》。ANPD 在调查中认定，TikTok 在“免注册浏览”和“注册浏览”两种模式下，均无法定依据处理未成年人个人数据，且未采取有效措施防止该类数据被处理。处罚同时要求删除违规收集的数据，并实施合规整改计划。字节跳动承诺的整改措施包括：对 16 岁以下账户自动适用最严格隐私设置（仅可经监护人同意变更）、强化家长监控与内容过滤；免注册模式下全面暂停广告、限制使用时长 12 小时、禁止评论、私信、直播、关注等社交功能、仅展示全龄适宜内容，并将数据收集降至最低。
([查看更多](#))

Brazil: ANPD Fines TikTok BRL 153.7 Million for Issues Concerning the Protection of Minors' Data

On 25 August 2026, the National Data Protection Authority (ANPD) of Brazil published its penalty decision in the *Federal Official Gazette*, imposing a fine of BRL 153.7 million on ByteDance, the parent company of TikTok, on the grounds that it violated the *General Data Protection Law* (LGPD) in the processing of personal data

of children and adolescents. In its investigation, the ANPD found that, under both the “feed without registration” and “feed with registration” modes, TikTok processed the personal data of minors without a legal basis and failed to adopt effective measures to prevent such data from being processed. The penalty also requires the deletion of the data collected in violation of the law and the implementation of a compliance rectification plan. The rectification measures committed by ByteDance include: automatically applying the strictest privacy settings to accounts of users under 16 (which may only be changed with guardian consent), and strengthening parental controls and content filtering; under the no-registration mode, completely suspending advertising, limiting usage duration to 12 hours, prohibiting social functions such as comments, direct messages, live streaming, and following, displaying only content suitable for all ages, and minimizing data collection. ([More](#))

荷兰：AP 因自动化决策问题对 Uber 处以 8.25 亿欧元罚款

2026 年 8 月 21 日，荷兰数据保护局（AP）作出决定，对美国网约车平台 Uber 处以 8.25 亿欧元罚款，理由是其通过自动化系统停用司机账户且未充分告知，违反 GDPR。经查，2020 年至 2022 年间，Uber 自动化系统在欧洲对多名涉嫌欺诈的司机实施临时停权，部分低评分司机遭永久停用。AP 认定，该做法侵犯了司机免受具有重大影响的自动化决策约束的权利，以及知情权——司机赖以谋生的平台账户被停用属于重大影响。该案源于法国 Uber 司机的投诉，因 Uber 欧洲总部位于荷兰而由 AP 管辖。Uber 表示将提起上诉，称其从未在无人工审核的情况下永久停用账户，且现行政策已包含人工复核与司机申诉机制，并认为罚款金额过高。（[查看更多](#)）

Netherlands: AP Fines Uber €825 Million for Issues Concerning Automated Decision-Making

On 21 August 2026, the Dutch Data Protection Authority (AP) issued a decision imposing a fine of €825 million on Uber, the US ride-hailing platform, on the grounds that it deactivated driver accounts through automated systems without adequately informing the drivers, in violation of the GDPR. Upon investigation, it was found that between 2020 and 2022, Uber’s automated systems temporarily suspended multiple drivers suspected of fraud in Europe, and some low-rated drivers were permanently deactivated. The AP found that this practice violated the drivers’ right not to be subject

to automated decision-making with significant effects, as well as their right to be informed - the deactivation of platform accounts on which drivers depend for their livelihood constitutes a significant effect. The case originated from a complaint by French Uber drivers and fell under the AP's jurisdiction because Uber's European headquarters is located in the Netherlands. Uber stated that it will appeal, claiming that it has never permanently deactivated accounts without human review, that its current policies already include human review and a driver appeal mechanism, and that the fine amount is excessive. ([More](#))

英国：英国高等行政上诉法庭驳回 TikTok 上诉

2026 年 8 月 4 日，英国高等行政上诉法庭驳回了 TikTok 就其逾 1200 万英镑罚款提出的上诉。英国信息专员办公室（ICO）于 2023 年向 TikTok 开出了 1270 万英镑罚单，此前调查发现该平台在处理 13 岁以下儿童数据时违反了英国数据保护法律。TikTok 试图提出上诉，辩称其数据处理活动服务于“特殊目的”——该术语在《英国数据保护法》中被定义为包括新闻、学术、艺术或文学目的。若该主张成立，则 ICO 在针对 TikTok 采取行动时必须满足额外的法律前提条件，这实际上会使得最初的罚款变得无效。然而，英国高等行政上诉法庭认定，TikTok 的数据处理并非出于“特殊目的”，称仅托管包含新闻、学术、艺术或文学价值的用户生成内容，并不满足该门槛标准。（[查看更多](#)）

UK: UK Upper Tribunal Dismisses TikTok's Appeal

On 4 August 2026, the Upper Tribunal (Administrative Appeals Chamber) of the United Kingdom dismissed TikTok's appeal against its fine of over £12 million. The UK Information Commissioner's Office (ICO) issued a £12.7 million fine against TikTok in 2023, following an investigation that found the platform had violated UK data protection laws in processing the data of children under 13. TikTok sought to appeal, arguing that its data processing activities served a "special purpose" - a term defined in the UK Data Protection Act as including journalistic, academic, artistic, or literary purposes. Had this argument succeeded, the ICO would have been required to satisfy additional legal preconditions when taking action against TikTok, which would in effect have rendered the original fine ineffective. However, the Upper Tribunal found that TikTok's data processing was not carried out for a "special purpose," stating that

merely hosting user-generated content containing journalistic, academic, artistic, or literary value does not meet the threshold standard. ([More](#))

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