

数字科技与人工智能

**Digital Technology
and Artificial Intelligence**

每月资讯 2026 年 01 月

上海市律师协会数字科技与人工智能专业委员会

上海市律师协会
数字科技与人工智能专业委员会
每月资讯

(2026年01月)

主任

张逸瑞（北京市金杜律师事务所上海分所）

副主任

吴卫明（上海市锦天城律师事务所）

徐凯（上海市君悦律师事务所）

编委会

本期责任编辑：朱培、李然

目录

新规概览.....	4
1. 国家互联网信息办公室关于《互联网应用程序个人信息收集使用规定(征求意见稿)》公开征求意见的通知.....	4
2. 关于开展第二批个人信息保护合规审计人员能力评价工作的通知.....	5
3. 数据出境安全管理政策法规问答(2026年1月).....	6
4. 《网络犯罪防治法(征求意见稿)》公开征求意见.....	7
5. 《可能影响未成年人身心健康的网络信息分类办法》.....	8
6. 个人信息保护政策法规问答(2026年1月).....	9
7. 国家互联网信息办公室关于《金融信息服务数据分类分级指南(征求意见稿)》公开征求意见的通知.....	10
8. 《直播电商监督管理办法》.....	11
9. 《网络交易平台规则监督管理办法》.....	12
域外规范.....	14
1. 英国 ICO 发布更新版个人信息跨境传输指引以简化 UK GDPR 合规要求.....	14
2. 德国发布合法利益评估(LIA)模板.....	14
3. 西班牙数据保护机构发布关于 AI 语音转录对数据保护影响的指导意见.....	15
4. 韩国 MOIS 宣布国会通过《公共人工智能法》.....	16
案例研讨.....	17
一、域内相关案例.....	17
1. 上海发布 2025 年执法典型案例.....	17
2. 律师用 AI 生成虚假案例.....	17
3. 全国首例生成式 AI “幻觉”引发侵权之诉.....	18
二、域外相关案例.....	19
1. 越南对 TikTok Pte. Ltd 公司罚款 8.8 亿越南盾.....	19
2. 法国 CNIL 因未能保护个人数据而对 France Travail 处以 500 万欧元的罚款.....	20
3. 美国加州隐私保护局对数据经纪商发起执法行动.....	21
4. 意大利 Garante 发布针对 Grok 及类似 AI 服务的正式警告通报.....	22
实务研究.....	24
1. 数字法院：历史、现在与未来.....	24
2. 论世界模型的隐私机制及其法律规制.....	24
3. 生成式人工智能算法“失控”：风险景象、治理困境与规制进路.....	25
4. 论已公开个人信息的保护模式.....	25
数字科技产品发展.....	27
1. 阿里发布千问旗舰推理模型 Qwen3-Max-Thinking.....	27
2. 美国英伟达发布四大开源人工智能模型.....	27
3. 银河通用重磅发布工业重载机器人 S1.....	28

新规概览

1. 国家互联网信息办公室关于《互联网应用程序个人信息收集使用规定（征求意见稿）》公开征求意见的通知



国家互联网信息办公室关于《互联网应用程序个人信息收集使用规定（征求意见稿）》公开征求意见的通知

2026年01月10日 16:00 来源: 中国网信网 【打印】【纠错】

为规范互联网应用程序个人信息收集使用活动，保护个人信息权益，促进个人信息合理利用，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，国家互联网信息办公室起草了《互联网应用程序个人信息收集使用规定（征求意见稿）》，现向社会公开征求意见。公众可以通过以下途径和方式提出反馈意见：

1. 登录中国网信网 (www.cac.gov.cn)，进入首页“网信要闻”查看文稿。
2. 通过电子邮件方式发送至: shujuju@cac.gov.cn。
3. 通过信函方式将意见寄至: 北京市海淀区阜成路15号国家互联网信息办公室网络数据管理局，邮编100048，并在信封上注明“互联网应用程序个人信息收集使用规定征求意见”。

发布机构: 国家互联网信息办公室

公布/生效时间: 2026年1月10日发布

内容概要/法规、政策文件的原文:

2026年1月10日，为规范互联网应用程序个人信息收集使用活动，保护个人信息权益，促进个人信息合理利用，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，国家互联网信息办公室起草了《互联网应用程序个人信息收集使用规定（征求意见稿）》，现向社会公开征求意见。

来源: 中国网信网，https://www.cac.gov.cn/2026-01/10/c_1769603446094128.htm。

2. 关于开展第二批个人信息保护合规审计人员能力评价工作的通知



The screenshot shows the official website of the Cyberspace Administration of China (CAC). The header includes the CAC logo and name in Chinese and English, along with a search bar. A navigation menu contains links for Home, Timely News, Network Administration, Interactive Services, and Hot Topics. The main content area displays the title of the notice: "关于开展第二批个人信息保护合规审计人员能力评价工作的通知". Below the title, it shows the date (2026年01月09日 21:41), source (中国网信网), and options for printing and reporting errors.

为保障个人信息保护合规审计工作的落地落实，依据《个人信息保护合规审计管理办法》第三条、第四条、第五条、第七条规定，在中央网络安全和信息化委员会办公室指导下，中国网络空间安全协会根据《个人信息保护合规审计人员能力评价要点》，面向个人信息处理者和自愿申请认证的专业机构等有意从事个人信息保护合规审计工作的人员，开展个人信息保护合规审计人员能力评价工作，确保从事个人信息保护合规审计人员有与考试等级相适应的能力水平。

根据有关工作部署，现开展第二批个人信息保护合规审计人员能力评价工作。有关事项通知如下：

一、评价目标

发布机构：中国网络空间安全协会

公布/生效时间：2026年1月9日发布

内容概要/法规、政策文件的原文：

2026年1月9日，为保障个人信息保护合规审计工作的落地落实，依据《个人信息保护合规审计管理办法》第三条、第四条、第五条、第七条规定，在中央网络安全和信息化委员会办公室指导下，中国网络空间安全协会根据《个人信息保护合规审计人员能力评价要点》，面向个人信息处理者和自愿申请认证的专业机构等有意从事个人信息保护合规审计工作的人员，开展第二批个人信息保护合规审计人员能力评价工作。

来源：中国网信网，

https://www.cac.gov.cn/2026-01/09/c_1769689281653351.htm。

3. 数据出境安全管理政策法规问答（2026年1月）



The screenshot shows the official website of the Office of the Central Cyberspace Affairs Commission (CAC). The header includes the CAC logo and name in Chinese and English, along with a search bar. The navigation menu contains links for Home, News, Network Governance, Interactive Services, and Hot Topics. The main content area displays the title '数据出境安全管理政策法规问答 (2026年1月)' and the date '2026年01月30日 19:00'. The source is listed as '中国网信网'.

国家互联网信息办公室持续加强数据出境安全管理政策法规宣介，指导和帮助数据处理器高效合规开展数据出境活动。经对近期收到的咨询问题进行研究，现将一些有代表性的问题和答复公布如下。

1. 订立个人信息出境标准合同、通过个人信息出境认证与申报数据出境安全评估如何衔接？

答：根据《网络安全法》《个人信息保护法》《网络数据安全条例》《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》《个人信息出境认证办法》等法律法规规章要求，关键信息基础设施运营者以外的数据处理器自当年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的，可以通过订立个人信息出境标准合同或个人信息出境认证方式出境个人信息。如数据处理器将前述个人信息出境事项申报数据出境安全评估，应当按照数据出境安全评估结果开

发布机构：国家互联网信息办公室

公布/生效时间：2026年1月30日

内容概要/法规、政策文件的原文：

2026年1月30日，国家互联网信息办公室发布了《数据出境安全管理政策法规问答（2026年1月）》，旨在宣介数据出境安全管理政策法规，指导数据处理器合规开展数据出境活动。该问答明确了订立个人信息出境标准合同、通过个人信息出境认证与申报数据出境安全评估的衔接规则，以及粤港澳大湾区个人信息跨境流动标准合同的适用范围和合规要求。

来源：中国网信网，

https://www.cac.gov.cn/2026-01/30/c_1771505108953002.htm。

4. 《网络犯罪防治法（征求意见稿）》公开征求意见



The screenshot shows the official website of the Ministry of Public Security of the People's Republic of China. At the top, there is a navigation bar with links for 'Home', 'Institutional Settings', 'Police Information', 'Public Services', and 'Police-Citizen Interaction'. A search bar is also present. The main content area features a breadcrumb trail: 'Home > Police-Citizen Interaction > Investigation Collection > Text'. The central heading is '《网络犯罪防治法（征求意见稿）》公开征求意见的公告'. Below the heading, the date is listed as '2026年01月31日'. The text of the announcement explains the purpose of the draft law: to curb network crime sources, improve public internet security, and after thorough research, the Ministry has drafted the law and is now seeking public input. Two methods for providing feedback are listed: logging into the official website (www.mps.gov.cn) to view the draft, or emailing the draft to wajfzc@sina.com.

发布机构：公安部

公布/生效时间：2026 年 1 月 31 日

内容概要/法规、政策文件的原文：

《网络犯罪防治法（征求意见稿）》由公安部起草，旨在构建网络犯罪综合防治体系。草案共 7 章 68 条，重点包括：强化网络基础资源实名制管理，遏制黑灰产物料供应；明确网络犯罪生态治理制度，打击支付、引流等黑灰产业链；规定电信、金融、互联网等服务提供者的防治义务；并针对跨境网络犯罪制定防治措施。现公开征求意见至 2026 年 3 月 2 日。

来源：公安部，

<https://www.mps.gov.cn/n2254536/n4904355/c10386242/content.html>。

5. 《可能影响未成年人身心健康的网络信息分类办法》



关于印发《可能影响未成年人身心健康的网络信息分类办法》的通知

2026年01月23日 17:00

来源: 中国网信网

【打印】【纠错】



关于印发《可能影响未成年人身心健康的网络信息分类办法》的通知

国信办通字〔2025〕5号

各省、自治区、直辖市互联网信息办公室、新闻出版局、电影主管部门、教育厅（局）、通信管理局、公安厅（局）、文化和旅游厅（局）、广播电视局，新疆生产建设兵团互联网信息办公室、新闻出版局、电影主管部门、教育局、公安局、文化体育广电和旅游局：

现将《可能影响未成年人身心健康的网络信息分类办法》印发给你们，自2026年3月1日起施行，请认真贯彻执行。

国家互联网信息办公室

发布机构：国家互联网信息办公室

公布/生效时间：2026 年 1 月 23 日

内容概要/法规、政策文件的原文：

《可能影响未成年人身心健康的网络信息分类办法》落实《未成年人网络保护条例》要求，明确可能影响未成年人身心健康的网络信息的 4 种类型及具体表现形式，将不当使用未成年人形象等近年来突出问题纳入治理范围，对算法推荐、生成式人工智能等新技术、新应用、新业态可能带来的内容风险提出防范要求，确保《办法》科学严谨、与时俱进。《办法》要求，对可能影响未成年人身心健康的网络信息，网站平台和内容生产者应当采取防范和抵制措施，避免对未成年人产生负面影响。

来源：中国网信网，

https://www.cac.gov.cn/2026-01/23/c_1770728781060093.htm。

6. 个人信息保护政策法规问答（2026年1月）



个人信息保护政策法规问答（2026年1月）

2026年01月09日 16:30

来源：中国网信网

【打印】【纠错】



国家互联网信息办公室持续加强个人信息保护相关政策法规宣贯，指导帮助个人信息处理者规范开展个人信息处理活动，保护个人信息权益。现将一些具有代表性的问题和答复公布如下。

1.什么是个人信息？

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息包括但不限于以下类型，如个人姓名、生日、年龄等个人基本资料，身份证、军官证、护照等个人身份信息，人脸、基因、声纹、虹膜、指纹等生物识别信息，用户账号、用户标识符（用户ID）等网络身份标识信息，教育经历、职业、职位等个人教育工作信息，金融账户、消费记录、收入状况、借款信息等个人财产信息，账号口令、数字证书等身份鉴别信息，通信记录、短信、电子邮件等个人通信信息，

发布机构：国家互联网信息办公室

公布/生效时间：2026年1月9日

内容概要/法规、政策文件的原文：

国家互联网信息办公室持续加强个人信息保护相关政策法规宣贯，指导帮助个人信息处理者规范开展个人信息处理活动，保护个人信息权益，在《个人信息保护政策法规问答（2026年1月）》中针对一些具有代表性的问题和答复进行公布。其中主要包括：明确个人信息的定义与范围（如基本资料、生物识别信息等）；界定敏感个人信息（如生物识别、金融账户、未成年人信息等）及其特殊保护要求；规定应用人脸识别技术前需进行个人信息保护影响评估的四个方面；以及说明处理百万人以上信息的个人信息处理者需指定并报送个人信息保护负责人的相关法规与具体报送方式。

来源：中国网信网，

https://www.cac.gov.cn/2026-01/09/c_1769688003183197.htm。

7. 国家互联网信息办公室关于《金融信息服务数据分类分级指南（征求意见稿）》公开征求意见的通知



为规范金融信息服务数据处理活动，提升金融信息服务的数据安全水平，依据《中华人民共和国网络安全法》、《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》、《网络数据安全条例》、《金融信息服务管理规定》等法律法规规章和政策规定，国家互联网信息办公室会同有关部门组织起草了《金融信息服务数据分类分级指南（征求意见稿）》，现向社会公开征求意见。公众可以通过以下途径和方式提出反馈意见：

- 1.通过电子邮件方式发送至：shujuju@cac.gov.cn。
- 2.通过信函方式将意见寄至：北京市海淀区阜成路15号国家互联网信息办公室网络数据管理局，邮编100048，并在信封上注明“金融信息服务数据分类分级指南征求意见稿”。

发布机构：国家互联网信息办公室

公布/生效时间：2026年1月24日

内容概要/法规、政策文件的原文：

为规范金融信息服务数据处理活动，提升金融信息服务的数据安全水平，依据《中华人民共和国网络安全法》、《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》、《网络数据安全条例》、《金融信息服务管理规定》等法律法规规章和政策规定，国家互联网信息办公室会同有关部门组织起草了《金融信息服务数据分类分级指南（征求意见稿）》，现向社会公开征求意见。该指南规定了金融信息服务数据的分类分级规则，旨在规范数据处理、提升安全水平。数据分为业务、用户、企业三大类，细分为多级子类；按安全重要程度分为核心数据、重要数据、敏感一般数据、常规一般数据四级，并明确了分级要素、影响对象与级别判定标准。指南适用于境内金融信息服务提供者，要求其进行分类分级、识别重要数据并动态更新管理。

来源：中国网信网，

https://www.cac.gov.cn/2026-01/24/c_1770812246428118.htm。

8. 《直播电商监督管理办法》



国家市场监督管理总局规章

[下载文字版](#)[下载pdf版](#)

直播电商监督管理办法

(2025年12月18日国家市场监督管理总局、国家互联网信息办公室令第117号公布 自2026年2月1日起施行)

第一章 总 则

第一条 为了加强直播电商监督管理,保护消费者和经营者的合法权益,促进直播电商健康发展,根据《中华人民共和国电子商务法》、《中华人民共和国消费者权益保护法》、《中华人民共和国网络安全法》等法律,制定本办法。

第二条 在中华人民共和国境内从事直播电商活动以及市场监督管理、网信部门依据职责对其进行监督管理,适用本办法。

本办法所称直播电商,是指通过互联网站、应用程序等,以视频直播、音频直

发布机构: 国家市场监督管理总局、国家互联网信息办公室

公布/生效时间: 2026年1月7日

内容概要/法规、政策文件的原文:

《办法》聚焦直播电商平台经营者、直播间运营者、直播营销人员、直播营销人员服务机构四类主体,压实责任义务,划定行为红线,完善监管机制。

《办法》结合直播电商活动的具体场景,从事前、事中、事后三个维度,系统规定了平台在身份信息核验登记、信息报送、直播营销人员培训、直播间运营者分级分类管理、平台内违法行为处置、风险识别及处置、交易信息保存、消费者权益保护等方面的责任义务。《办法》明确了直播间运营者在信息公示、核验实际经营者信息和直播营销人员身份信息、实时管理直播间互动内容、事前合规审核、实施明码标价等方面的义务,划定了直播间运营者、直播营销人员不得进行虚假宣传、不得进行商业诋毁、不得销售或者提供违法商品或者服务等行为红线。《办法》规定直播营销人员服务机构应当建立健全内部管理制度,规范直播营销人员的招募、培训、使用、管理工作,在与直播间运营者的商业合作以及直播选品中履行必要的核验义务。

来源：国家市场监督管理总局，

https://www.samr.gov.cn:8080/zw/zfxxgk/fdzdgknr/fgs/art/2026/art_ce66ea61fcc4583b5dbd677f470088b.html。

9. 《网络交易平台规则监督管理办法》



国家市场监督管理总局规章

下载文字版
下载pdf版

网络交易平台规则监督管理办法

（2025年12月18日国家市场监督管理总局、国家互联网信息办公室令第116号公布 自2026年2月1日起施行）

第一章 总 则

第一条 为了规范网络交易平台规则（以下简称平台规则）的制定、修改和执行，维护网络交易秩序，保护网络交易各方主体合法权益，促进平台经济健康可持续发展，根据《中华人民共和国电子商务法》、《中华人民共和国消费者权益保护法》、《中华人民共和国网络安全法》等法律，制定本办法。

第二条 网络交易平台经营者开展平台规则制定、修改和执行活动以及市场监督管理、网信部门依据职责对其进行监督管理，适用本办法。

发布机构：国家市场监督管理总局、国家互联网信息办公室

公布/生效时间：2026年1月7日

内容概要/法规、政策文件的原文：

《办法》聚焦网络交易平台经营者（以下简称平台）这一“关键少数”，结合近年来监管实践，以平台规则为切入点，进一步压紧压实平台责任。

一是明确平台在制定、修改和执行平台规则过程中应当履行的责任义务。

《办法》规定了平台在信息公示、公开征求意见、过渡期设置、申诉渠道设置等方面的义务，要求平台建立健全平台规则重大事项沟通协商、平台内交易纠纷解决等机制。

二是细化平台在保障信息、网络和数据安全，保护平台内经营者和消费者合法权益等方面的具体要求。《办法》要求平台在其平台规则中明确信息安全条款，明确平台内经营者处理个人信息的具体规范以及平台内经营者的未成年人网络保护义务等。同时，《办法》明确不得利用平台规则对平台内

经营者的自主经营活动进行不合理限制，收取不合理费用、不合理的违约金或者损害赔偿金；不得利用平台规则排除或者限制消费者权利、减轻或者免除自身责任、不合理加重消费者责任、实施大数据“杀熟”、提供会员服务时单方面随意变更平台规则损害会员权益等。

三是强化执法协作，完善监管机制。《办法》要求市场监管、网信部门加强部门协作，建立健全两部门线索移交、信息共享、会商研判等工作机制。规定两部门可依据职责对平台有关负责人进行约谈，要求其说明情况，采取措施进行整改。倡导社会共治，鼓励平台发布平台规则合规报告，主动开展合规自评或者引入第三方进行合规“体检”。

来源：国家市场监督管理总局，

https://www.samr.gov.cn/zw/zfxxgk/fdzdgknr/fgs/art/2026/art_85b474fc5a08494bb60ca6a280b98d7d.html。

域外规范

1. 英国 ICO 发布更新版个人信息跨境传输指引以简化 UK GDPR 合规要求

内容概要: 2026 年 1 月 15 日, 英国信息专员办公室 (ICO) 发布个人信息跨境传输更新版指南, 旨在帮助企业快速理解并遵守《英国通用数据保护条例》(UK GDPR) 项下的跨境传输规则。

新版指南精简规则条款, 明确核心合规要求, 增设“三步核验法”供机构判断是否涉及受限数据传输; 针对企业高频疑问领域补充阐释内容, 新增权责划分章节以适配多层次传输场景。同时配套推出简明操作指引、速查问答手册及术语表, 帮扶非专业机构合规。

此次更新为阶段性成果, 后续将进一步细化传输风险评估方法、补充《国际数据传输协议》及云服务专项指引, 还计划上线交互式工具及新增案例研究。

来源: ICO,

<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/01/updated-guidance-on-international-transfers-published/>。

2. 德国发布合法利益评估 (LIA) 模板

内容概要: 2026 年 01 月 06 日, 汉堡数据保护和信息自由专员 (HmbBfDI) 现提供一份全面的问题目录, 用于确定合法利益。该文件提供众多示例和提示, 可作为机关、企业和组织的指南。问题目录支持负责人仔细审查和记录其数据处理的利益所在, 以及数据主体的权利和利益是否得到适当考虑。它逐步引导完成以下主要检查点: 确定合法利益: 数据处理追求的目标是什么, 这些目标是否合法? 必要性: 数据处理是否必要, 是否仅收集所需数据? 利益平衡: 数据主体的权利和利益是否得到充分考虑和保护? 记录和合规: 如何记录审查并定期更新?

来源: HmbBfDI,

<https://datenschutz-hamburg.de/news/hmbbfdi-veroeffentlicht-fragenkatalog->

[zur-interessenabwaegung-nach-dsgvo](#)。

3. 西班牙数据保护机构发布关于 AI 语音转录对数据保护影响的指导意见

内容概要：2026 年 1 月 14 日，西班牙数据保护机构（AEPD）发布了一份题为利用人工智能（AI）进行语音转录对数据保护影响的指导意见。

AEPD 指出，自然人语音因具备直接或间接识别身份的特性，应被认定为个人数据；与语音关联的通信内容、电话号码、IP 地址、Cookie 等元数据，同样属于个人数据范畴，需纳入 GDPR 合规考量。而通过技术手段实现匿名化的语音，其身份识别属性可被消除。

在 AI 语音转录系统的操作流程中，存在生成会议纪要等转录服务、利用语音样本微调模型两类常见处理方式。数据控制者引入相关服务时，需审慎筛选合作方，核查其关于额外数据处理操作、保密措施、安全防护、数据留存期限、数据最小化等方面的合规保障，确保符合 GDPR 第 28 条要求。若转录服务涉及情绪推断、生物特征识别等特殊类别数据处理，需遵循更严格的监管规则，且不得使用欧盟《人工智能法》（2024/1689 号条例）明令禁止的 AI 系统。

AEPD 强调，利用转录数据开展模型再训练的主体，将被认定为独立数据控制者，其处理行为需具备独立的合法性依据。数据处理的合法基础包括履行合同、合法利益、数据主体同意等，其中同意需通过明确主动行为作出，不得设置为默认选项，且用户撤回同意的方式应与提供同意同样简便。

此外，数据控制者需履行透明度义务，在处理前告知数据主体服务用途、额外处理操作、第三方参与情况及相关权利风险。合规分析同时明确，GDPR 不适用于合成语音或经源头匿名化处理的语音，但服务元数据及关联自然人的通信内容仍受该条例约束。

来源：AEPD，

<https://www.aepd.es/en/press-and-communication/blog/ai-voice-transcription>。

4. 韩国 MOIS 宣布国会通过《公共人工智能法》

内容概要：2026年1月29日，韩国行政安全部（MOIS）宣布，《人工智能与数据化行政管理促进法》（以下简称《公共人工智能法》）于同日在韩国国会全体会议表决通过。该法为公共部门推广、应用人工智能奠定制度基础，助力打造人工智能驱动的民主政府。

《公共人工智能法》的规制对象为各类公共机构，要求其推行人工智能与数据化行政管理，同时保障相关工作的安全性、可靠性，恪守伦理准则，维护公民基本权利。

《公共人工智能法》对以下概念作出全新界定：人工智能；人工智能化行政管理；训练数据。上述定义与2025年1月21日颁布的《人工智能发展与信任基础构建基本法》保持统一。

来源：MOIS，

<https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do;jsessionid=PJcLHICu39TIDB6IoTdzut-5Fpho2OcbeXSZu43q.node40?bbsId=BBSMSTR%5F000000000008&nttId=123514>。

案例研讨

一、域内相关案例

1. 上海发布 2025 年执法典型案例

时间：2026 年 1 月 16 日

内容概要：

上海市网信办依据《网络安全法》《数据安全法》《个人信息保护法》，以及《网络数据安全条例》(以下简称《条例》)等法律法规，持续加大执法力度，规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益。发布典型案例如下：

一、未依法履行网络数据安全主体责任，导致发生数据泄露：

案例 1：某物流运输网络科技企业数据泄露案

案例 2：某物联网科技企业用户数据泄露案

案例 3：某事务中心档案查询系统信息泄露

二、未落实网络数据跨境安全管理要求，导致数据违法违规出境

案例 4：某酒店管理企业违法违规出境用户数据案

案例 5：某物业管理企业违法违规出境用户数据案

三、未有效履行个人信息安全保护义务，导致个人信息权益受到侵害

案例 6：某咖啡企业违法违规收集使用个人信息案

案例 7：某 SDK 网络科技企业违法违规收集个人信息案

案例 8：某酒店管理企业存在个人信息泄露风险案

来源：网信上海，https://mp.weixin.qq.com/s/W_EDyn0NIltRWO72L7dVyA。

2. 律师用 AI 生成虚假案例

时间：2026 年 1 月 15 日

内容概要：

北京通州法院审理一起代持股民事纠纷时，原告律师为支持其诉讼请求，在庭审后提交了两份“参考案例”（标注为最高法、上海一中院案例）。法官审核发现案例格式异常，经核实，案例虽真实存在，但内容与提交版本完

全不符（如其中一份实为民间借贷案）。律师承认案例是通过向 AI 大模型提问生成后未经核实直接提交。法院认定该行为属提交虚假参考案例，因情节轻微、无恶意且未造成严重后果，在判决书中对律师予以批评，并对原告部分请求不予采纳。一审判决生效。诉讼参与者应遵循诚信原则，对提交材料真实性负责；提交 AI 生成且未经核实的虚假案例应承担法律后果；情节轻微可批评教育，情节较重可参照《民事诉讼法》第一百一十四条第一款处理。

来源：网信上海，<https://mp.weixin.qq.com/s/SCzIf2oMT565mRRDiqqyJg>。

3. 全国首例生成式 AI “幻觉” 引发侵权之诉

时间：2026 年 1 月 26 日

内容概要：

某生成式人工智能应用程序（以下简称某生成式人工智能应用），是某科技公司基于自研大语言模型，开发并运营的文本生成、信息查询类通用型智能对话应用程序。2025 年 3 月，梁某在同意用户协议后，注册并开始使用某生成式人工智能应用。2025 年 6 月 29 日，梁某在某生成式人工智能应用中输入提示词询问某高校报考的相关信息时，某生成式人工智能应用生成了关于该高校某校区的不准确信息。梁某发现后，在对话中进行了纠正和指责，某生成式人工智能应用仍继续回复称该高校确实存在这一校区，并生成了对争议问题的解决方案，提出若生成内容有误将向用户提供 10 万元赔偿。之后，梁某将从该高校官网查询到的招生信息提供给某生成式人工智能应用，此时某生成式人工智能应用承认其生成了不准确信息，并建议梁某到杭州互联网法院起诉索赔。

梁某认为，某生成式人工智能应用生成不准确信息对其构成误导，使其遭受侵害，并承诺对其进行赔偿，遂起诉要求某科技公司赔偿损失 9999 元。某科技公司辩称，对话内容由人工智能模型生成，不成立意思表示；某科技公司已充分履行了注意义务，无过错；原告未产生实际损失，某科技公司不构成侵权。

案件结果：

法院裁判要点如下：1. AI 不具有民事主体资格，其生成的“承诺”不构成

服务提供者的意思表示。2. AI 服务属于“服务”而非“产品”，侵权责任适用过错责任原则，而非产品无过错责任。3. 法院认定服务提供者已通过显著提示、采用检索增强生成等技术履行合理注意义务，无过错；原告未能证明实际损害及因果关系。故不构成侵权，驳回诉请。

来源：网信上海，<https://mp.weixin.qq.com/s/JaB0BPBHgP265YA7aElwuw>。

二、域外相关案例

1. 越南对 TikTok Pte. Ltd 公司罚款 8.8 亿越南盾

时间：2026 年 1 月 22 日

内容概要：

在 1 月 22 日，越南国家竞争委员会宣布已对 TikTok Pte. Ltd 公司进行行政处罚。

根据该委员会的说法，通过检查该公司遵守消费者权益保护法律的情况，国家竞争委员会已对 TikTok Pte. Ltd 公司（总部位于新加坡莱佛士码头 1 号，#26-10）处以 8.8 亿越南盾的罚款，原因是该公司存在以下违规行为：

1. 没有机制允许用户选择是否允许使用其信息进行广告宣传、产品推荐。
2. 规定了一般交易条件中不得规定的条款。
3. 通过提供不完整的用户与组织、个体经营者之间交易的内容、特点信息，误导消费者。
4. 没有发布适合每个易受伤害消费者对象的流程、程序、方法或措施，以保障易受伤害消费者的申诉权、争议解决请求权和其他权利。

国家竞争委员会已要求该公司停止违规行为，主动审查并完善内容、政策，确保完全、准确地遵守消费者权益保护法律规定。

来源：越南政府新闻网，

<https://baochinhphu.vn/xu-phat-vi-pham-hanh-chinh-810-trieu-dong-cong-ty-va-n-hanh-nen-tang-zalo-10226012215522757.htm>。

2. 法国 CNIL 因未能保护个人数据而对 France Travail 处以 500 万欧元的罚款



时间：2026 年 1 月 29 日

内容概要：

2026 年 1 月 29 日，法国国家信息与自由委员会（CNIL）公布其 SAN 专委会于 2026 年 1 月 22 日作出的第 2026-003 号决议，就法国劳工局（France Travail）发生的大规模个人数据泄露事件作出行政处罚决定。

CNIL 查明，2024 年 2 月至 3 月期间，攻击者通过社会工程学手段入侵法国劳工局信息系统，利用被攻陷的残障求职者帮扶机构（CAPEMPOI）顾问及外部合作机构的合法账户，持续近一个月非法访问并窃取数据。涉案系统中存储了过去约 20 年的注册用户信息，数据泄露规模约 3680 万名自然人，被窃取的数据包括姓名、出生日期、法国社保号、联系方式、求职者身份状态及注册期限等高度敏感的身份识别信息。

CNIL 认定，尽管攻击未涉及完整求职者档案或健康数据，但法国劳工局未能有效保障其处理的个人数据安全，其行为构成对 GDPR 第 32 条“处理安全”的违反。具体违规情形包括：

- (1) 身份验证安全不足：账户在连续 50 次登录失败后才会锁定，且高风险账户未部署多因素认证，尽管该要求已在其此前的数据保护影响评估中明确；
- (2) 日志监控与异常检测缺失：系统虽留存日志，但未对异常访问和大规模数据外传行为进行有效监控和预警；
- (3) 访问权限配置过宽：顾问账户可访问全国范围内求职者数据，违反最小权限原则；
- (4) 对已识别风险未采取整改措施：相关安全缺陷早在 2022 年的数据保护影响评估中已被识别，但长期未落实整改。


案件结果：

鉴于涉案数据规模巨大、数据敏感性高，且机构对已知风险存在明显疏忽，CNIL 认定法国劳工局存在重大过失，对其处以 500 万欧元行政罚款，并责令其采取整改措施，包括强化密码策略、全面部署多因素认证、建立有效的日志监控与预警机制，以及严格限制数据访问权限。

来源：CNIL，

<https://www.cnil.fr/fr/violation-de-donnees-sanction-5millions-france-travail>。

3. 美国加州隐私保护局对数据经纪商发起执法行动



**California Privacy
Protection Agency**

[Announcements](#)
[Meetings & Events](#)
[Laws & Regulations](#)
[FAQ](#)
[Resources](#)
[Career Opportunities](#)
[File a Complaint](#)
[Data Broker Registry](#)

[Home](#) | [Announcements](#) | [2026](#) | 20260108

CalPrivacy Brings New Round of Enforcement Actions Against Data Brokers

Marketing firm that sold lists of people with serious health conditions must pay fine and stop selling Californians' personal information

News: January 8, 2026

SACRAMENTO, CA – The California Privacy Protection Agency Board has issued two new decisions following settlements reached by the Enforcement Division's [Data Broker Enforcement Strike Force](#).

The [first decision](#) requires Rickenbacher Data LLC, d/b/a Datamasters, a Texas-based reseller of personal information for targeted advertising, to pay a \$45,000 fine for failing to register as a data broker in violation of California's Delete Act. The decision also orders the company to stop selling all Californians' personal information.

According to the decision, Datamasters bought and resold the names, addresses, phone numbers, and email addresses of millions of people with Alzheimer's disease, drug addiction, bladder incontinence, and other health conditions for targeted advertising. In addition, Datamasters bought and resold lists of people based on age and perceived race, offering "Senior Lists" and "Hispanic Lists," as well as lists based on political views, grocery store purchases, banking activity, and health-related purchases.

时间：2026 年 1 月 8 日

内容概要：

2026 年 1 月 8 日，美国加利福尼亚隐私保护局（CalPrivacy）理事会发布在其执法部门“数据经纪商执法特别行动组”达成和解后，作出了两项新的执法决定。

第一项决定要求 Rickenbacher Data LLC（以 Datamasters 名义经营）支付 45,000 美元罚款。该公司是一家总部位于德克萨斯州的个人信息转售商，主要为定向广告用途提供数据。由于其未按照《删除法案》（Delete Act）的规定注册为数据经纪商，构成违法，理事会同时责令其停止出售所有加州居民的个人信息。

第二项决定要求总部位于纽约的数据与技术服务提供商 S&P Global, Inc. 支付 62,600 美元罚款。该公司因一次行政性错误而未能依法注册为数据经纪商。除罚款外，该决定还要求 S&P Global 建立数据经纪商注册及合规审计程序，以防止类似错误再次发生。

来源：CPPA，

<https://cppa.ca.gov/announcements/2026/20260108.html>。

4. 意大利 Garante 发布针对 Grok 及类似 AI 服务的正式警告通报



The screenshot shows the official website of the Garante per la Protezione dei Dati Personali (Italian Data Protection Authority). The main header includes the logo and the text "GARANTE PER LA PROTEZIONE DEI DATI PERSONALI". Navigation links include "L'Autorità", "Temi", "Normativa e provvedimenti", "News e comunicazione", and "Amministrazione Trasparente".

The main content area features a press release titled "COMUNICATO STAMPA - Deepfake, il Garante avverte: a rischio diritti e libertà fondamentali". Below the title are icons for "Ascolta", "Stampa", "PDF", and "Condividi". The text of the press release reads: "Deepfake, il Garante avverte: a rischio diritti e libertà fondamentali. Dopo il blocco di Clothoff, l'Autorità richiama l'attenzione sull'uso di Grok e altri servizi analoghi. Il Garante per la protezione dei dati personali ha adottato un provvedimento di avvertimento nei confronti degli utilizzatori di servizi basati sull'intelligenza".

On the right side, there is a "Scheda" (Card) section with the following details: "Doc-Web 10207147", "Data 08/01/26", and "Tipologie Comunicato stampa".

时间：2026 年 1 月 8 日

内容概要：

2026 年 1 月 8 日，意大利个人数据保护机构（Garante）向 Grok 及其他人工智能工具的用户和提供方发布了正式警告，重点关注这些服务在未获得当事人同意的情况下，可能生成基于真实内容的深度伪造图像等风险。

Garante 特别关注一类可基于真实图像或声音生成并传播内容的人工智能服务，包括能够在未经本人同意的情况下对个人进行“数字脱衣”等深度伪造操作的功能。Garante 在该决定中明确要求相关服务的提供方在应用和平台的设计、开发与上线阶段即落实隐私保护要求，确保用户能够在符合法律规定的前提下使用相关服务。

Garante 进一步表示，就 X 平台所提供的相关服务，其已与爱尔兰数据保护机构开展协作（鉴于 X 在欧盟的主要设立地位于爱尔兰），并保留采取进一步监管或执法行动的权利。

来源：GPDP，

<https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10207147>。

实务研究

1. 数字法院：历史、现在与未来

作者：陈增宝

时间：2026年1月16日

内容概要：

数字法院是在大数据、区块链、人工智能等前沿技术推动下，为落实“数字中国”战略、推进审判工作现代化而发展起来的现代化法院新样态。它超越了以往信息化建设的工具属性，以“数据驱动”为核心，通过平台化、无纸化、智能化实现从技术赋能到模式变革、制度重塑和认知升级的一体化迭代。文章回顾了数字法院的由来与历史沿革，强调其起源于浙江“全域数字法院”的实践，并经历了从信息化 1.0 到 4.0 版的演进。数字法院的建设理念坚持一体化、开放式、智能化发展，以数字正义和司法为民为导向，注重数字赋能与伦理守正的协调。其实施路径涵盖从技术嵌入到模式变革、从碎片化到体系化、从程序化输出到智慧化生产等多维变革。未来展望包括深化人工智能应用、加强司法数据全生命周期质量管控、强化关键信息基础设施和安全保护，最终推动司法方法论变革，勾勒司法文明新图景。

来源：法律适用，<https://mp.weixin.qq.com/s/Ar2VTQ3ullGTf65-uDgNPQ>。

2. 论世界模型的隐私机制及其法律规制

作者：岳林

时间：2026年1月29日

内容概要：

所谓世界模型，是指能够对物理世界和人类社会进行模拟和理解的人工智能技术图景。Sora、V-JEPA 和 Genie 等新兴人工智能技术，皆以世界模型作为它们的技术原理和发展方向。本文试图从世界模型的整体发展趋势出发，研究其技术机制将如何影响人类社会的隐私机制，进而探讨隐私权以及相关法律制度可能给予的回应。目前人工智能领域存在两种主流世界模型路径，可分别把它们概括为“模拟式世界模型”和“理解式世界模型”。进而

指出，世界模型的技术机制可以类比理解为人类社会的四种隐私机制，即：对世界现象的还原，对因果关系的探究，对世界现象的虚构，对社会人格的伪装。并预测随着世界模型的技术发展以及相应社会变迁，现有隐私权制度将进一步被弱化，而个人信息法和数据法将承担起更主要的隐私法律规制功能。因此提出以下建议：国家应该加强对个人信息的行政规制，即在公法层面细化个人信息的类型和行为规范；针对世界模型应用的具体场景和媒介，立法者和监管者应当提供差异化的行为规范和主体责任模式；法律应该针对世界模型隐私问题建立“多方参与治理模式”，鼓励所有社会主体积极参与技术和法律的互动过程。

来源：上海市法学会，https://mp.weixin.qq.com/s/2pdJExscDz8g1T6co_NLZw。

3. 生成式人工智能算法“失控”：风险景象、治理困境与规制进路

作者：孙逸啸、彭成龙

时间：2026年1月20日

内容概要：

生成式人工智能在深度嵌入人类生产生活的同时，算法“失控”问题也日益凸显。从生成式人工智能的底层算法及其应用趋势来看，算法“失控”可能引发生成内容风险、加剧技术安全风险和升级“黑箱”风险等。当前，我国算法治理面临备案体系不完善、监督检查精准度不足以及责任界定不清晰等诸多挑战。面对这一系统性治理难题，应当转变治理路径，构建以风险防范为核心、全生命周期监管为框架、场景性规制为路径的多维治理框架，并从事前备案、事中监督检查、事后追责三个层面完善具体措施，打破算法治理孤岛，实现生成式人工智能算法的整体可控。

来源：上海市法学会，

<https://mp.weixin.qq.com/s/viky-RYjuchUPSP42BmBCQ>。

4. 论已公开个人信息的保护模式

作者：边琪

时间：2026 年 1 月 7 日

内容概要：

已公开个人信息保护应从“严进宽出”模式转向“宽进严出”模式，在此基础上，已公开个人信息处理规则的解释应被更新。所谓“宽进严出”模式，是指在信息收集上放宽对目的限制的要求，但在信息处理上强化对处理结果的控制。我国《个人信息保护法》第 24 条已在自动化决策场景中初步确立“宽进严出”模式，该模式在价值判断、理论准备、规则设置上亦能得到支持。“宽进严出”模式下，认定已公开个人信息处理在“合理的范围”内应降低目的限制要求，以处理结果倒推处理方式的关联性与合理性。个人信息处理者无需履行告知义务，个人信息主体行使拒绝权的时间和方式应尊重所在场景的信息处理技术特性。“对个人权益有重大影响”的评估应被置于整体风险评估中，具体为对处理结果和系统风险的评估。从“合理的范围”和“对个人权益有重大影响”中亦可推出，已公开个人信息也应“严出”。

来源：上海市法学会，<https://mp.weixin.qq.com/s/5BqOG6ZLzy3I0e70rO7s1g>。

数字科技产品发展

1. 阿里发布千问旗舰推理模型 Qwen3-Max-Thinking

发布机构、企业等：阿里巴巴

时间：2026 年 1 月 26 日

内容概要：

阿里正式发布千问旗舰推理模型 Qwen3-Max-Thinking。Qwen3-Max-Thinking 是目前阿里规模最大、能力最强的千问推理模型，其总参数量超万亿（1T），预训练数据量高达 36T Tokens。

此前，预览版 Qwen3-Max-Thinking 斩获数学推理 AIME 25 和 HMMT 25 的国内首个双满分，推理性能已让人惊艳；在此基础上，阿里通义团队进行了更大规模的强化学习后训练，全面提升了正式版 Qwen3-Max-Thinking 性能。其中，在涵盖事实知识、复杂推理、指令遵循、人类偏好对齐、Agent 能力等 19 个公认的大模型基准测试中，千问旗舰推理模型刷新了数项最佳表现（SOTA）纪录，整体性能可媲美国际顶尖 AI 大模型。

来源：Qwen, <https://qwen.ai/blog?id=qwen3-max-thinking>。

2. 美国英伟达发布四大开源人工智能模型

发布机构、企业等：NVIDIA

时间：2026 年 1 月 6 日

内容概要：

美国英伟达在 2026 年国际消费电子展上推出覆盖智能体人工智能、物理人工智能、自动驾驶、生物医疗四大领域的开源模型。四大模型分别为 Nemotron 系列、Cosmos 平台、Alpamayo 系列及 Clara 模型，可实现语音性能提升 10 倍、机器人物理推理、自动驾驶决策解释、原子级蛋白质设计等功能。此举将使英伟达成为全球开源训练框架和最大开放多模态数据集的贡献者，其中包括 10 万亿个语言训练 tokens、50 万条机器人轨迹、45.5 万个蛋白质结构以及 100TB 的车辆传感器数据，标志着英伟达正全力构建一个涵盖语言处理、机器人技术、科学研究及自动驾驶的开放生态系统，加

速从硬件向 AI 生态构建者转型。目前，博世、Uber、Salesforce 等企业已采用相关技术。

来源：NVIDIA，

<https://blogs.nvidia.cn/blog/open-models-data-tools-accelerate-ai/>。

3. 银河通用重磅发布工业重载机器人 S1



发布机构、企业等：银河通用

时间：2026 年 1 月 18 日

内容概要：

银河通用机器人正式发布具身智能重载机器人 Galbot S1，作为全行业首个实现零遥操、全自主、可持续作业的重载机器人，其双臂最大负载能力达 50 公斤，树立了行业新标杆。值得关注的是，该产品核心的具身搬运模型已作为北京人工智能重要成果，由北京大学助理教授，银河通用机器人创始人及首席技术官王鹤博士在北京人工智能+创新示范高地大会上向市领导、发改委领导正式发布汇报，彰显其技术与战略双重价值。目前，Galbot S1 已在宁德时代等先进制造龙头企业实现规模化产线应用，标志着具身智能正式迈入工业级重载新时代。

Galbot S1 从设计之初就瞄准真实工业场景，以工规级标准严格锻造，具备 IP54 防水防尘与耐高温性能，能可靠应对粉尘、震动、温变等复杂工况。

其作业高度达 2.3 米，覆盖超大工作区间，真正适配从仓储到产线的多样化工业环境。

它面向高强度、长周期、连续运行的工业节拍，也能适应粉尘、震动、遮挡、光照变化等非理想工况，并在复杂流程中与人机混行、物流交叉、任务频繁调整的环境中稳定作业。

更为关键的是，它的负载能力在行业中前所未有：双臂最大负载达 50kg。此指标不仅刷新了行业认知，更意味着 Galbot S1 能够直接进入生产流程的关键搬运与转运环节，成为影响节拍、效率与安全的核心节点，而非外围辅助设备。

来源：环球网，<https://tech.huanqiu.com/article/4Q1K6g22crM>。