

中国人民大学法学院 数字法学教研月报

2026年第1期（总第25期）

2026年3月16日



本期看点

【数字法治大事件】国家层面聚焦数字法治精准落地，个人信息保护与数据出境安全管理政策问答发布，为企业合规提供明确指引；《政务移动互联网应用程序规范化管理办法》出台整治“指尖上的形式主义”；《互联网平台反垄断合规指引》《网络交易平台规则监督管理办法》《直播电商监督管理办法》密集落地，筑牢平台经济公平竞争与消费者权益保护防线；《可能影响未成年人身心健康的网络信息分类办法》细化保护标准，构建多领域精细化数字治理制度体系。

【研究动态】本期研究覆盖数字法治核心领域，聚焦多维度前沿议题：个人信息保护围绕权利证成、数据保护、制度适配等展开；人工智能法治涉及治理路径、立法趋向、备案制度、著作权保护等核心内容；网络平台监管聚焦平台责任、元宇宙互操作治理等方向；数据确权研究涵盖权利登记、产权配置、财产权构造、数据访问制度等；新型数字技术法律应对聚焦物联网、人脸识别、流

量劫持、版权保护等议题；数字政府与智能司法围绕法治化建设、行政参与权、反垄断规制等展开；数字时代部门法研究涉及刑事证据、数字孪息、数字民生权、人机交互诈骗认定等，为数字法治实践提供理论支撑。

【教研活动】北大举办“数字时代的技术规制、法治变革与秩序转型”研讨会，第六届网络法治论坛聚焦数智法治与数字经济，对外经贸大学举办 AI 智能体安全研讨会及数字法学博士生论坛，中南大开展 AI 生成内容著作权保护沙龙，上海市法学会年会研讨网络平台版权侵权责任，推动学术交流与实务融合。

【数字法评】

《论人工智能时代肖像可识别性的判断标准》，《法学家》2026年第1期，作者：阮神裕。

《制度与场景：重构人脸识别与人脸图像信息保护》，《行政法学研究》2026年第1期，作者：丁晓东。

本期目录

数字法治大事件3	新型数字技术的法律应对.....44
个人信息保护政策法规问答（2026年1月）...3	数字政府与智能司法.....46
数据出境安全管理政策法规问答（2026年1月）.....4	数字时代的部门法研究.....47
国务院办公厅关于印发《政务移动互联网应用程序规范化管理办法》的通知.....5	教研活动51
《政务移动互联网应用程序规范化管理办法》答记者问.....7	北大举办“数字时代的技术规制、法治变革与秩序转型”研讨会.....51
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.....9	第六届网络法治论坛暨北京市网络法学研究会2025年年会及公益大讲堂在京成功举办.....54
《可能影响未成年人身心健康的网络信息分类办法》答记者问.....11	贸大举办“AI智能体行为安全与发展”研讨会.....60
网络交易平台规则监督管理办法.....12	贸大举办“中国数字法学自主知识体系构建：2025法学博士生学术论坛”.....61
直播电商监督管理办法.....17	中南大举办“人工智能生成内容的著作权保护”学术沙龙.....67
市场监管总局关于印发《互联网平台反垄断合规指引》的通知.....25	上海市法学会网络治理与数据信息法学研究会2025年年会暨“网络平台版权侵权责任”学术研讨会成功举办.....69
研究动态33	数字法评72
个人信息保护.....33	论人工智能时代肖像可识别性的判断标准.....72
人工智能法治.....36	制度与场景：重构人脸识别与人脸图像信息保护.....84
网络平台监管.....40	
数据确权研究.....40	

学术顾问：王利明

编委会：张新宝 丁晓东 王莹 张吉豫

编辑部：阮神裕 毕坤阳 来唯希 吕昊然 邓语鑫 梁因格 王昊

联系方式：RUCdigitallaw@163.com

本期编辑：梁因格

数字法治大事件

导言：

在数字中国建设向纵深发展的关键阶段，我国数字法治建设呈现出从“框架搭建”向“精准落地”与“精细治理”跨越的鲜明特征。2026年初，随着个人信息保护及数据出境安全管理政策法规问答的相继发布，我国在数据跨境流动与隐私保护领域进一步强化了政策执行的透明度与可预期性，通过常态化的权威解读，为企业合规经营提供了精准导航。与此同时，国务院办公厅印发《政务移动互联网应用程序规范化管理办法》，标志着政务数字化建设步入减负增效、规范有序的新阶段，通过制度化手段整治“指尖上的形式主义”，确保数字政府建设回归服务民生的本质。

在基础制度不断夯实的同时，数字经济核心领域的治理正向公平竞争与权责对等深度演进。市场监管总局发布《互联网平台反垄断合规指引》，为超大规模平台划定清晰的竞争红线，引导数字经济在公平竞争的轨道上实现高质量创新。针对日新月异的商业模式，《网络交易平台规则监督管理办法》与《直播电商监督管理办法》的并行出台，聚焦平台规则的透明度与直播生态的责任边界，通过体系化的监管规则，构建起保护消费者权益与激发市场活力的双重屏障。

在社会关切的特定领域，数字法治的温度与广度得到进一步彰显。《可能影响未成年人身心健康的网络信息分类办法》的印发及权威解读，不仅为未成年人网络保护筑起科学、动态的“防火墙”，更为内容平台履行主体责任提供了清晰的分类标准与执行依据。这一举措与平台治理政策相呼应，共同构成了多维度、立体化的数字生态治理体系，体现了法治在数字时代对社会公共利益的深度关切。

从跨境数据安全到政务应用规范，从平台反垄断合规到未成年人网络保护，一系列密集落地的法治举措共同勾勒出我国数字法治建设持续深化的清晰图景：以精准解读消除合规盲区，以制度约束净化政务生态，以公平竞争重塑平台秩序，以细腻关怀守护网络未来。这标志着我国正加速迈入一个安全有序、公平竞争、且更具人文温度的数字法治新生态，推动数字文明在规范与创新的良性互动中迈向更高水平。

个人信息保护政策法规问答 (2026年1月)

原载：“网信中国”微信公众号

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，通讯录、好友列表等联系人信息，网页浏览记录、软件使用记录等个人上网记录，国际移动设备识别码（IMEI）等个人设备信息，交通出行信息等个人位置信息，用户标签、画像信息等个人标签信息，步数、步频等个人运动信息，以及其他与已识别或者可识别的自然人有关的各种信息。

2. 什么是敏感个人信息？

敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

国家标准 GB/T 45574-2025《数据安全技术 敏感个人信息处理安全要求》明确了敏感个人信息识别和界定方法，并在附录 A 中给出常见的敏感个人信息类别，如人脸、基因、声纹等生物识别信息，

个人信仰的宗教、加入的宗教组织等宗教信仰信息，残疾人士身份信息、不适宜公开的职业身份信息 etc 特定身份信息，病症、既往病史、医疗就诊记录、检验检查数据等医疗健康信息，银行、证券、基金、保险账户的账号及密码等金融账户信息，连续精准定位轨迹信息、车辆行驶轨迹信息等行踪轨迹信息，居民身份证照片、征信信息、犯罪记录信息等其他敏感个人信息。

3. 应用人脸识别技术处理人脸信息前如何进行个人信息保护影响评估？

《人脸识别技术应用安全管理办法》第九条规定，使用人脸识别技术前应当进行个人信息保护影响评估，并对处理情况进行记录。个人信息保护影响评估由应用人脸识别技术的个人信息处理者组织开展，可有第三方机构参与。若有第三方机构参与，需在评估报告中说明第三方机构的基本情况 & 参与评估的情况。

主要评估四方面内容，一是人脸信息的处理目的、处理方式是否合法、正当、必要；二是对个人权益带来的影响，以及降低不利影响的措施是否有效；三是发生人脸信息泄露、篡改、丢失、毁损或者被非法获取、出售、使用的风险以及可能造成的危害；四是所采取的保护措施是否合法、有效 & 与风险程度相适应。

4. 符合什么条件的个人信息处理者需指定个人信息保护负责人和报送负责人信息？

《中华人民共和国个人信息保护法》第五十二条规定，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。《个人信息保护合规审计管理办法》第十二条规定，处理 100 万人以上个人信息的个人信息处理者应当指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作。

2025 年 7 月 18 日，国家互联网信息办公室发布《关于开展个人信息保护负责人信息报送工作的公告》，明确个人信息保护负责人信息报送要求、报送时间、报送方式等。个人信息保护负责人信息

报送采用线上方式。可直接访问“个人信息保护业务系统”（<https://grxxbh.cacdtsc.cn>），按照系统首页提供的《个人信息保护负责人信息报送系统填报说明（第一版）》，准备相关材料并履行信息报送手续，也可从中国网信网（<https://www.cac.gov.cn>）首页“全国网信政务办事大厅”栏目访问“个人信息保护业务系统”。

数据出境安全管理政策法规问答 (2026 年 1 月)

原载：“网信中国”微信公众号

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者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。如数据处理者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展个人信息出境活动。

已订立个人信息出境标准合同或通过个人信息出境认证，但自当年 1 月 1 日起累计出境超过 100 万人个人信息（不含敏感个人信息）或者超过 1 万人敏感个人信息的，数据处理者应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。数据处理者申报数据出境安全评估时，应当将自当年 1 月 1 日起通过订立个人信息出境标准合同或个人信息出境认证出境的个人信息，纳入申报评估范围，并按照数据出境安全评估结果开展个人信息出境活动。

属于《促进和规范数据跨境流动规定》第三条、第四条、第五条、第六条规定情形的，从其规定。

2. 境内数据处理者已订立粤港澳大湾区个人信息跨境流动标准合同，若个人信息出境情形发生变化，如何履行合规义务？

答：境内数据处理者订立并备案粤港澳大湾区个人信息跨境流动标准合同，应当按照《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》和《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》规定，在粤港澳大湾区内开展数据跨境活动，不得违法向粤港澳大湾区以外的组织、个人提供个人信息。

境内已备案粤港澳大湾区个人信息跨境流动标准合同的数据处理者，需要向粤港澳大湾区以外的组织、个人提供个人信息的，应当按照国家关于数据出境安全管理有关规定，将拟向粤港澳大湾区以外提供个人信息履行申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息出境认证等合规义务。

国务院办公厅关于印发《政务移动互联网应用程序规范化管理办法》的通知

原载：“网信中国”微信公众号

国务院办公厅关于印发《政务移动互联网应用程序规范化管理办法》的通知

国办函〔2026〕12号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

《政务移动互联网应用程序规范化管理办法》已经国务院同意，现印发给你们，请结合实际认真贯彻执行。

国务院办公厅

2026年1月25日

（此件公开发布）

政务移动互联网应用程序规范化管理办法

第一条 为规范政务移动互联网应用程序管理，统筹为基层减负和赋能，防治“指尖上的形式主义”和政务服务中的“面子工程”，根据《整治形式主义为基层减负若干规定》、《关于加强数字政府建设的指导意见》、《关于防治“指尖上的形式主义”的若干意见》等，制定本办法。

第二条 本办法所称政务移动互联网应用程序（以下简称政务应用程序），是指各级行政机关、群团组织、事业单位开发建设，或依托各类互联网平台搭建，运行在移动智能终端上，为内部工作人员办公、管理、学习提供支撑服务的应用软件，包括移动客户端（APP）、小程序、快应用等，不包括政务公众账号和工作群组。县以下（不含县级）单位原则上不得开发建设政务应用程序。

为经营主体和社会公众提供管理服务的政务应用程序，参照本办法管理。

第三条 国务院办公厅、国家网信办负责统筹协调政务应用程序管理工作。省级网信部门会同同级政务服务管理部门负责统筹协调本地区政务应用程序管理工作。

第四条 政务应用程序的主办（使用）单位按照“谁主办谁负责、谁使用谁负责”的原则，履行建设、使用、安全管理等环节的主体责任。

第五条 政务应用程序上线前，主办（使用）单位应按照本办法规定履行备案程序，并在显著位置以醒目方式标示主办（使用）单位及备案编号。禁止以任何形式要求用户下载、安装或使用未经备案的政务应用程序。法律、行政法规另有规定的，依照其规定。不承担行政职能的事业单位主办（使用）的应用程序，不纳入统一备案管理。

第六条 新建、改建政务应用程序，应纳入信息化项目审批范围，开展立项审核，避免同质化政务应用程序建设和运营。政务应用程序备案前原则上应对功能完整性、性能稳定性、交互便捷性等进行验收。

第七条 各地政务应用程序主办（使用）单位向所在地省级网信部门提交备案申请，由省级网信部门通过政务移动互联网应用程序规范化管理

系统向国家网信办申请备案。各部门主办（使用）的政务应用程序，由部门通过政务移动互联网应用程序规范化管理系统向国家网信办申请备案。

第八条 主办（使用）单位申请政务应用程序备案，应按要求提供备案申请材料，主要包括：

- （一）政务应用程序基本信息；
- （二）政务应用程序立项审核情况；
- （三）政务应用程序功能设置情况；
- （四）政务应用程序运维和安全保障情况；
- （五）政务应用程序验收情况；
- （六）政务应用程序备案需要的其他材料。

开发建设面向基层的政务应用程序，主办（使用）单位应在申请备案时单独说明。

第九条 省级网信部门应会同政务服务管理部门自收到备案申请材料之日起10个工作日内完成完备性审核。材料齐全的，报送国家网信办；材料不齐全的，退回主办（使用）单位并一次性告知需要补充的材料。

第十条 国家网信办应自收到备案申请之日起20个工作日内完成材料审核和技术检测，重点关注政务应用程序是否设置打卡签到、积分排名、统计在线时长等强制性功能，是否缺失必要功能等情况复杂或需要补充、更正材料的，可以适当延长办理期限，并告知主办（使用）单位延期理由和预计时间。

对通过材料审核和技术检测的政务应用程序，国家网信办予以备案并编号；对需要补充、更正材料或未通过技术检测的政务应用程序，通过政务移动互联网应用程序规范化管理系统反馈，主办（使用）单位应在收到反馈后10个工作日内补充提交备案申请材料或整改说明，逾期未提交的，视为放弃备案申请。

第十一条 政务应用程序重大功能变更的，主办（使用）单位应按照本办法第七条规定的程序，在变更发生10个工作日前提交备案变更申请，按要求说明变更情况，并重新进行材料审核和技术检测。

第十二条 政务应用程序关停注销的，主办

（使用）单位应在政务应用程序下线后10个工作日内，按照本办法第七条规定的程序进行报备。

第十三条 政务应用程序关停注销前，主办（使用）单位应发布公告，依法依规处置相关数据，防止数据泄露或流失。

第十四条 主办（使用）单位应规范政务应用程序建设、使用管理，不得出现下列情况：

- （一）随意或重复要求基层填表报数交材料；
- （二）除安保、应急等特殊场景规定外，政务应用程序设置打卡签到、积分排名、统计在线时长等强制性功能；

（三）强制推广下载使用政务应用程序，考核通报用户安装使用率，强制要求定期登录；

（四）把政务应用程序异化为工作考核日常化、督查检查线上化的主要载体，将点赞量、网络投票数、转发量、学习时长等作为考评依据，非必要情况下强制要求下级和基层单位通过政务应用程序上传工作照片、视频和轨迹等；

（五）使用政务应用程序从事经营性活动。

第十五条 鼓励在已备案移动互联网应用程序分发平台上架政务应用程序。

第十六条 主办（使用）单位应在确保安全的前提下，充分考虑政务应用程序对用户端软硬件的适配性，支持在不同操作系统环境下稳定运行。积极采用互联网协议第六版（IPv6）等创新技术，提升政务应用程序承载能力和用户体验。

第十七条 主办（使用）单位应组织做好政务应用程序运行监测，建立健全运维管理规范，严格巡查巡检，保障稳定可靠运行。

第十八条 主办（使用）单位应在政务应用程序中提供投诉建议功能，实现在线受理、跟踪反馈和回访评价等。

第十九条 各地区各部门应落实网络安全、数据安全、关键信息基础设施安全保护、个人信息保护、密码管理、移动互联网应用程序信息服务管理等有关法律法规规定，依法依规保护数据和个人信息安全等。

第二十条 各地区各部门应严格遵守国家保

密法律法规，完善保密自监管措施，定期开展安全保密检查和风险评估，及时发现处置违反保密法律法规行为。参与政务应用程序规范化管理工作的机构及其工作人员对在履行职责中知悉的国家秘密、工作秘密、商业秘密、个人隐私和个人信息应依法予以保密，不得泄露或非法向他人提供、非法使用。

第二十一条 各地区各部门应定期开展自查自评，主动发现强制使用、过度留痕、滥用排名、多头填报等问题并进行整改，对使用频率低、实用性不强的政务应用程序限期关停注销，对功能相近、重复的政务应用程序进行整合迁移。鼓励主办（使用）单位积极利用政务应用程序提高基层治理数字化智能化水平。各地区各部门应加强集约建设和数据共享，清理整合面向基层的政务应用程序，优化政务应用程序功能。

第二十二条 国家网信办会同有关方面定期组织对已备案政务应用程序进行抽查检测，推广先进做法，对违反本办法的典型问题、规范化管理工作落实不到位的单位予以通报。

第二十三条 政务应用程序存在违法违规或违反《整治形式主义为基层减负若干规定》、《关于加强数字政府建设的指导意见》、《关于防治“指尖上的形式主义”的若干意见》及本办法规定问题，整改不及时、不到位的，撤销备案。信息化项目审批部门应暂停主办（使用）单位政务应用程序项目审批，信息化项目运维经费管理部门应暂停主办（使用）单位政务应用程序运维经费拨付，待问题全部整改到位并重新备案后再按程序办理。

第二十四条 行政机关以外的其他国家机关可以参照本办法规范本单位、本系统政务应用程序管理。

第二十五条 本办法由国家网信办负责解释。

第二十六条 本办法自印发之日起施行。本办法施行前已上线的政务应用程序，应自本办法施行之日起6个月内完成备案。

《政务移动互联网应用程序规范化管理办法》答记者问

原载：“网信中国”微信公众号

日前，国务院办公厅印发《政务移动互联网应用程序规范化管理办法》（以下简称《办法》），自印发之日起施行，对政务移动互联网应用程序（以下简称政务应用程序）规范化管理作出了要求。国家网信办有关负责同志就《办法》相关问题回答了记者提问。

1. 问：《办法》出台的背景是什么？

答：随着网络信息技术在政务领域广泛应用，政务应用程序已成为政务部门提升政务服务与管理效能的重要载体。与此同时，形式主义顽瘴痼疾也渗透到线上，变异翻新出“指尖上的形式主义”问题，加重了基层负担，影响了基层政务工作效能。

以习近平同志为核心的党中央高度重视整治形式主义为基层减负工作。2024年7月，中共中央政治局会议强调，加强政务应用程序规范化管理，整治“指尖上的形式主义”。2024年8月，中共中央办公厅、国务院办公厅印发《整治形式主义为基层减负若干规定》，专章部署“规范政务移动互联网应用程序管理”，从清理整合面向基层的政务应用程序、严格建设管理、防止功能异化方面提出明确要求。2023年12月，中央网络安全和信息化委员会印发《关于防治“指尖上的形式主义”的若干意见》，提出规范政务应用程序管理，健全完善常态化监管措施和长效工作机制。

贯彻落实党中央决策，按照中央层面整治形式主义为基层减负专项工作机制统一部署，2024年10月以来，中央网信办会同有关部门开展“指尖上的形式主义”全国整治工作，着力纠治政务应用程序存在的过多过滥、多头填报、建设不规范和功能异化等突出问题。通过制定《办法》，巩固全国整治工作成果，明确政务应用程序管理要求，对于规范政务应用程序管理、防止“指尖上的形式主义”反弹回潮和隐形变异、提升政务服务和基层治理效

能具有重要意义。

2. 问：制定《办法》的总体思路是什么？

答：在《办法》的制定过程中主要把握以下几点：一是突出政治引领。深入学习贯彻习近平总书记关于力戒形式主义官僚主义的重要论述，认真落实中央层面整治形式主义为基层减负专项工作机制部署，统筹为基层减负和赋能，防治“指尖上的形式主义”和政务服务中的“面子工程”。二是聚焦突出问题。针对“指尖上的形式主义”突出问题，围绕政务应用程序建设、使用、安全等关键环节明确管理要求和工作职责，推动建立长效防治机制。三是坚持系统观念。落实《整治形式主义为基层减负若干规定》，从机制、制度、技术等方面综合施策，明确加强政务应用程序规范化管理的备案工作机制和技术能力支撑，将全国政务应用程序纳入统一技术监管。四是深化赋能增效。着眼便民利民、赋能增效，突出政务应用程序功能性能和用户体验，鼓励技术创新应用，推动提升政务服务效能。

3. 问：《办法》的适用范围是什么？

答：《办法》适用于政务应用程序全周期规范化管理。《办法》所称政务应用程序，是指各级行政机关、群团组织、事业单位开发建设，或依托各类互联网平台搭建，运行在移动智能终端上，为内部工作人员办公、管理、学习提供支撑服务的应用软件，包括移动客户端（APP）、小程序、快应用等。为经营主体和社会公众提供管理服务的政务应用程序，参照《办法》管理。行政机关以外的其他国家机关可以参照《办法》规范本单位、本系统政务应用程序管理。

4. 问：《办法》中对政务应用程序提出的备案管理要求和流程是什么？

答：《办法》对政务应用程序实施统一备案管理，要求主办（使用）单位上线政务应用程序前，按照《办法》规定履行备案程序，禁止以任何形式要求用户下载、安装或使用未经备案的政务应用程序。《办法》所提参照管理的情形，纳入统一备案管理。

《办法》提出了分级申请的工作原则。各地政

务应用程序主办（使用）单位向所在地省级网信部门提交备案申请，由省级网信部门会同政务服务管理部门对备案申请材料进行完备性审核后，通过政务应用程序规范化管理系统向国家网信部门申请备案。各部门主办（使用）的政务应用程序，由部门通过政务应用程序规范化管理系统向国家网信部门申请备案。

《办法》明确了主办（使用）单位申请、变更、注销政务应用程序备案的工作流程。政务应用程序上线前，主办（使用）单位应按分级申请原则提交备案申请，并按要求提供备案申请材料，主要包括政务应用程序基本信息以及立项审核、功能设置、运维和安全保障、验收等情况，开发建设面向基层的政务应用程序的，应单独说明。政务应用程序重大功能变更的，主办（使用）单位应按分级申请原则在变更发生前提交备案变更申请，按要求说明变更情况。政务应用程序关停注销的，主办（使用）单位应于关停注销前发布公告，依法依规处置相关数据，防止数据泄露或流失，并下线后进行注销报备。国家网信部门将适时发布备案工作指南，为主办（使用）单位申请、变更、注销政务应用程序备案提供操作指引。

备案管理中，由国家网信部门对政务应用程序进行材料审核和技术检测，重点关注政务应用程序是否设置打卡签到、积分排名、统计在线时长等强制性功能，是否缺失必要功能等，形成备案结果并编号。

5. 问：《办法》对政务应用程序提出哪些规范化管理要求？

答：《办法》对政务应用程序的建设、使用、技术、运维、安全和保密作出明确要求，全面加强政务应用程序规范化管理。一是明确建设要求。明确县以下（不含县级）单位原则上不得开发建设政务应用程序，同时提出立项、验收以及功能设置相关要求。二是明确使用要求。对政务应用程序填报数、推广下载、考核通报、从事经营等方面提出要求，严防功能异化。三是明确技术要求。在确保安全前提下，充分考虑对用户端软硬件的适配性，

支持在不同操作系统环境下稳定运行等。四是明确运维要求。加强政务应用程序运行监测，保障可靠稳定运行。五是明确安全要求。落实网络安全、数据安全等有关法律法规规定，依法依规保护数据和个人信息安全等。六是明确保密要求。严格遵守国家保密法律法规，完善保密自监管措施，定期开展检查评估。

6. 问：《办法》对政务应用程序监督管理作了哪些规定？

答：《办法》明确了日常监督管理要求。一是做好自查。各地区各部门应定期开展自查自评，主动发现强制使用、过度留痕、滥用排名、多头填报等问题并进行整改。二是强化抽查。国家网信部门会同有关方面定期组织对已备案的政务应用程序进行抽查检测，推广先进做法，对违反《办法》的典型问题、规范化管理工作落实不到位的单位予以通报。三是依规处置。政务应用程序存在问题且整改不及时、不到位的，撤销备案，并由有关部门暂停主办（使用）单位政务应用程序项目审批、运维经费拨付，待问题全部整改到位并重新备案后再按程序办理。

7. 问：《办法》对进一步提升政务应用程序效能提出哪些工作方向？

答：《办法》在加强政务应用程序规范化管理的基础上，提出了进一步发挥政务应用程序赋能增效作用的工作方向。一是更加注重用户体验。要求政务应用程序备案前原则上应对功能完整性、性能稳定性、交互便捷性等进行验收，保障好用、易用。二是更加注重技术创新。积极采用互联网协议第六版（IPv6）等创新技术，进一步提升政务应用程序承载能力。三是更加注重应用实效。积极运用政务应用程序提高基层治理数字化智能化水平。四是更加注重集约共享。加强集约建设和数据共享，清理整合面向基层的政务应用程序，优化政务应用程序功能。

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

原载：“网信中国”微信公众号

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

国家新闻出版署

国家电影局

教育部

工业和信息化部

公安部

文化和旅游部

国家广播电视总局

2025年12月26日

可能影响未成年人身心健康的网络信息分类办法

第一条 为了营造有利于未成年人身心健康的网络环境，进一步明确可能影响未成年人身心健康的网络信息的具体种类、范围、判断标准和提示办法，根据《中华人民共和国未成年人保护法》、《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》、《未成年人网络保护条例》、《互联网信息服务管理办法》、《网络信息内容生

态治理规定》、《网络暴力信息治理规定》等法律法规规定，制定本办法。

第二条 本办法所称的可能影响未成年人身心健康的网络信息，是指除法律法规规定的含有危害未成年人身心健康内容的违法信息外，通过互联网发布传播的可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生极端情绪、养成不良嗜好等的信息。

第三条 可能引发或者诱导未成年人模仿或者实施不良行为的信息包括但不限于：

（一）带有性暗示、性挑逗等易使人产生性联想的；

（二）存在指责嘲讽、贬低歧视等涉网络暴力不良信息的；

（三）煽动人群歧视、地域歧视、对立冲突等行为的；

（四）通过刻意刺激、恶意引导等方式，引发未成年人产生过度强烈或者持久的愤怒、恐惧、抑郁等极端情绪的；

（五）存在不安全驾驶等危险动作，诱导模仿高风险行为、进入危险区域等可能损害身体健康行为的；

（六）通过谐音梗、缩写词、拆解字、图文结合等形式传播不良网络用语的；

（七）宣扬未成年人抽烟（含电子烟）、饮酒、暴饮暴食、文身、不合理使用或者滥用药物等不良生活方式的；

（八）宣扬代写代抄、抄袭作弊、逃学旷课、学生欺凌等违反校纪校规行为的；

（九）诱导未成年人盲目追星、参与非理性极端“饭圈”行为的；

（十）诱导未成年人进行充值、打赏等非理性消费行为的；

（十一）教授未成年人制作具有伤害性的创意手工的；

（十二）向未成年人提供或者寻求陪玩陪聊、代练代打等服务的；

（十三）其他可能引发或者诱导未成年人模仿

或者实施不良行为的。

第四条 可能对未成年人价值观造成负面影响的信息包括但不限于：

（一）宣扬漠视生命、自我贬损等观念的；

（二）宣扬奢靡享乐、炫富拜金、消极颓废等不良价值观的；

（三）宣扬畸形审美、低俗恶俗文化的；

（四）宣扬荒诞离奇、危言耸听等伪科学内容的；

（五）宣扬不良交友、恋爱观的；

（六）宣扬“读书无用论”“唯分数论”“唯升学论”等观念的；

（七）其他宣扬违反公序良俗和社会公德的不良价值导向的。

第五条 不当使用未成年人形象的信息包括但不限于：

（一）利用未成年人形象摆拍演绎含有不良价值观或者不当言行的剧情内容的；

（二）利用未成年人形象展示营销不适宜未成年人的产品与服务的；

（三）利用未成年人声线传播不良内容的；

（四）通过恶搞未成年人、利用未成年人打造争议人设等方式博取关注的；

（五）借未成年人在短视频中长时间摆拍积累人气、牟取利益的；

（六）以不良方式或者目的对未成年人进行品行、道德方面测试的；

（七）歪曲或者炒作涉未成年人违法犯罪行为的；

（八）其他不当披露和使用未成年人形象的。

第六条 不当披露和使用未成年人个人信息包括但不限于：

（一）未经监护人同意不当展示不满十四周岁的未成年人学习、生活等可能暴露未成年人个人信息的；

（二）诱导未成年人发布可能泄露本人或者其他个人个人信息的；

（三）其他不当披露和使用未成年人个人信息

的。

第七条 对可能影响未成年人身心健康的网络信息，网络信息内容生产者以及网络产品和服务提供者应当按照《网络信息内容生态治理规定》、《网络暴力信息治理规定》等法律法规规定要求，采取防范和抵制措施，避免影响未成年人身心健康。

第八条 对于可能影响未成年人身心健康的网络信息，制作、复制、发布、传播该信息的组织和个人应当按照《未成年人网络保护条例》要求，在信息展示前，在明显位置作出显著提示。

网络产品和服务提供者应当为用户提供添加显著提示效果的标识功能，并引导和规范用户对相关信息作出提示。具体提示方式包括：

（一）在文本的起始、末尾或者中间适当位置添加文字提示或者通用符号提示等标识，或者在交互场景界面或者文字周边添加显著的提示标识；

（二）在音频的起始、末尾或者中间适当位置添加语音提示或者音频节奏提示等标识，或者在交互场景界面添加显著的提示标识；

（三）在图片的适当位置或者在交互场景界面添加显著的提示标识；

（四）在视频起始画面和视频播放周边的适当位置添加显著的提示标识，可在视频末尾和中间适当位置添加显著的提示标识，或者在交互场景界面添加显著的提示标识；

（五）呈现虚拟场景时，在起始画面的适当位置添加显著的提示标识，可在虚拟场景持续服务过程中的适当位置添加显著的提示标识；

（六）符合其他服务场景特点的显著提示标识方式。

第九条 网络产品和服务提供者应当落实《未成年人网络保护条例》要求，不得在首页首屏、弹窗、热搜、榜单、推荐、精选等处于产品或者服务醒目位置、易引起用户关注的重点环节，呈现可能影响未成年人身心健康的网络信息。

提供算法推荐、生成式人工智能等服务的，应当建立健全安全管理制度和技术措施，不得向未成年人推送可能影响其身心健康的网络信息。任何组

织和个人不得在专门以未成年人为服务对象的网络产品和服务中，制作、复制、发布、传播可能影响未成年人身心健康的网络信息。

第十条 违反本办法规定的，依据《中华人民共和国网络安全法》、《未成年人网络保护条例》等法律、行政法规的规定予以处理。

《可能影响未成年人身心健康的网络信息分类办法》答记者问

原载：“网信中国”微信公众号

近日，国家互联网信息办公室、国家新闻出版署、国家电影局、教育部、工业和信息化部、公安部、文化和旅游部、国家广播电视总局发布《可能影响未成年人身心健康的网络信息分类办法》（以下简称《办法》）。国家互联网信息办公室有关负责人就《办法》有关问题回答了记者提问。

问：请介绍一下《办法》的出台背景和意义？

答：党的十八大以来，以习近平同志为核心的党中央高度重视未成年人健康成长。习近平总书记多次就未成年人思想道德建设、加强未成年人网络保护作出重要指示批示，总书记在主持中央政治局第二十三次集体学习时强调，要健全网络生态治理长效机制，持续营造风清气正的网络空间。习近平总书记的重要讲话和重要指示精神，为我们进一步做好相关工作指明了前进方向、提供了根本遵循。当前，网络已经成为未成年人学习、生活、娱乐的重要空间，未成年人触网率持续攀升，在网络空间接触到的信息容易影响其身心健康和价值观塑造。社会各界对于加强未成年人网络保护，进一步净化未成年人网络环境的呼声日益强烈。《未成年人网络保护条例》第二十三条提出网信部门会同有关部门确定可能影响未成年人身心健康的不信息的具体种类、范围、判断标准和提示办法。制定《办法》是落实《条例》的重要举措，将法律法规要求进一步细化为具体制度规范，为网站平台、内容创作者等各方提供了清晰明确的指引。

问：制定《办法》的总体思路是什么？

答：起草过程中主要有三方面考虑：

一是注重制度衔接。《办法》依据《未成年人网络保护条例》第二十三条，进一步明确“可能影响未成年人身心健康的信息”的具体类别和情形，参考并延续前期多部管理规定，提出对相关信息作出显著提示的要求，实现治理连贯有效。

二是强化经验提炼。《办法》总结近年来“清朗”系列专项行动中整治的各类突出问题，结合常态化治理的实践经验，广泛征求相关部门、专家学者和社会公众意见，对可能影响未成年人身心健康的网络信息进行系统梳理，确保分类结果科学规范、体现共识。

三是坚持与时俱进。《办法》着眼网络发展中的新情况新问题，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、新应用可能带来的风险提出防范要求。

问：《办法》如何对可能影响未成年人身心健康的网络信息进行分类？

答：根据《未成年人网络保护条例》要求，从4个维度对可能影响未成年人身心健康的网络信息进行界定。

一是可能引发或者诱导未成年人模仿或者实施不良行为的信息。例如，带有性暗示、性挑逗等易使人产生性联想的；存在指责嘲讽、贬低歧视等涉网络暴力不良信息的；诱导未成年人进行充值、打赏等非理性消费行为的。

二是可能对未成年人价值观造成负面影响的信息。例如，宣扬奢靡享乐、炫富拜金、消极颓废等不良价值观的；宣扬畸形审美、低俗恶俗文化的。

三是不当使用未成年人形象的信息。例如，利用未成年人形象摆拍演绎含有不良价值观或者不当言行的剧情内容的；通过恶搞未成年人、利用未成年人打造争议人设等方式博取关注的。

四是不当披露和使用未成年人个人信息。例如，未经监护人同意不当展示不满十四周岁的未成年人学习、生活等可能暴露未成年人个人信息的。

问：《办法》对网络信息内容生产者、网络产品和服务提供者提出了哪些要求？

答：《办法》要求网络信息内容生产者以及网络产品和服务提供者应当按照《网络信息内容生态治理规定》、《网络暴力信息治理规定》等法律法规规定要求，对可能影响未成年人身心健康的网络信息，采取防范和抵制措施。

一是明确内容呈现管理。要求网络产品和服务提供者，不得在首页首屏、弹窗、热搜、榜单、推荐、精选等处于产品或者服务醒目位置、易引起用户关注的重点环节，呈现可能影响未成年人身心健康的网络信息。

二是添加显著提示标识。一方面，明确提示义务。要求制作、复制、发布、传播可能影响未成年人身心健康的网络信息的组织和个人，在信息展示前，在明显位置作出显著提示。例如在文本的起始、末尾或者中间适当位置添加文字提示或者通用符号提示等标识。另一方面，压实引导责任。要求网络产品和服务提供者应当为用户提供添加显著提示效果的标识功能，引导和规范用户对相关信息作出提示。

三是健全技术保障措施。要求提供算法推荐、生成式人工智能等服务的，应当建立健全安全管理制度和技术措施，不得向未成年人推送可能影响其身心健康的网络信息。任何组织和个人不得在专门以未成年人为服务对象的网络产品和服务中，制作、复制、发布、传播可能影响未成年人身心健康的网络信息。

问：如果违反《办法》规定，需要承担哪些法律责任？

答：对违反《办法》规定的，网信等有关部门可依据《中华人民共和国网络安全法》、《未成年人网络保护条例》等法律、行政法规的规定予以处理。

网络交易平台规则监督管理办法

原载：“网信中国”微信公众号

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。

第三条 本办法所称网络交易平台经营者,是指在网络交易活动中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务,供交易双方或者多方独立开展网络交易活动的法人或者非法人组织。网络社交、网络直播等网络服务提供者,为经营者提供网络经营场所、商品浏览、订单生成、在线支付等网络交易平台服务的,属于本办法规定的网络交易平台经营者。

第四条 本办法所称平台规则,是指网络交易平台经营者为服务不特定网络交易各方主体、管理平台内交易相关活动而预先拟定、供各方遵守的服务协议和交易规则的总称。平台规则包括网络交易平台服务协议、对平台内经营者的管理规则、平台内交易及纠纷处理规则、个人信息保护规则、知识产权保护规则等。网络交易平台经营者与特定主体单独协商达成的不具有广泛适用性的协议,不属于本办法规定的平台规则。

第五条 网络交易平台经营者制定、修改和执行平台规则应当遵循公开、公平、公正的原则,遵守法律、法规、规章和商业道德、公序良俗,不得利用平台规则实施危害国家利益、社会公共利益或者侵害网络交易各方主体合法权益的行为。

第六条 网络交易平台经营者应当通过平台规则的制定、修改和执行,加强对平台内经营者进入、退出平台以及平台内交易活动的管理,依法落实商品和服务质量保障、消费者权益保护、公平竞争、信用管理、信息安全管理、未成年人网络保护、个人信息保护、网络和数据安全保护等方面的责任。

第二章 平台规则的制定、修改和执行

第七条 网络交易平台经营者应当在其网站、应用程序首页显著位置,持续公示平台规则信息或者上述信息的链接标识,并保证经营者和消费者能够便利、完整地阅览和下载。

第八条 平台规则内容应当清晰明了,便于阅读和理解。网络交易平台经营者应当以字体加粗等显著方式提示经营者、消费者注意平台规则中涉及收费、争议解决等与其有重大利害关系的内容,保障其知情权,并按照经营者、消费者的要求对有关条款进行解释和说明。

第九条 网络交易平台经营者应当采取技术措施,在平台规则展示页面设置检索功能,为经营者和消费者检索、浏览平台规则中的特定内容提供便利。

第十条 网络交易平台经营者制定、修改平台规则,应当在其网站、应用程序首页显著位置公开征求意见。网络交易平台经营者应当预留必要时间并提供必要的技术支持,确保有关各方能够及时充分表达意见。

第十一条 网络交易平台经营者应当全面如实归纳整理平台规则征求意见过程中收到的意见,对于合理意见应当充分吸收采纳,不采纳意见应当有合理理由。相关资料应当留档备查,保存时间自征求意见结束之日起不少于三年。

第十二条 网络交易平台经营者制定、修改的平台规则,应当至少在实施前七日予以公示。对于涉及用户数量巨大、修改内容较多、关系有关各方重要权益的平台规则,应当至少在实施前十五日予以公示。

第十三条 网络交易平台经营者制定、修改平台规则,可能对有关各方重要权益造成重大影响

的，除依照本办法第十二条规定进行公示外，还应当根据其影响程度设置合理的过渡期，为有关各方妥善处理相关事宜提供便利条件。

第十四条 平台内经营者、消费者不接受平台规则修改的内容，要求退出平台或者终止相关服务的，网络交易平台经营者不得以设置不合理条件等方式阻止。平台内经营者、消费者依照前款规定，要求退出平台或者终止相关服务的，网络交易平台经营者应当按照修改前的平台规则承担据实退还费用等相关责任，不得故意拖延或者无理拒绝。

第十五条 网络交易平台经营者修改平台规则的，应当完整保存修改后的版本生效之日前三年的全部历史版本，并保证经营者和消费者能够便利、完整地阅览和下载。

第十六条 网络交易平台经营者不得强制或者诱导经营者和消费者对相关平台规则表示同意，不得将相关平台规则设定为默认同意的选项，但不增加经营者和消费者义务、不减损经营者和消费者权益的除外。

第十七条 网络交易平台经营者应当建立健全平台规则重大事项沟通协商机制，通过定期会商、座谈、问卷调查等方式，就涉及有关各方重大利害关系的平台规则的制定、修改和执行等事项进行常态化沟通协商，对沟通协商过程中收集的意见进行全面如实归纳整理，对于合理意见应当充分吸收采纳，不采纳意见应当有合理理由。

第十八条 网络交易平台经营者应当通过平台规则的制定、修改和执行，对网络交易活动中违反法律、法规、规章、商业道德、公序良俗的行为予以规制，防止有关各方主体合法权益受到侵害。

第十九条 网络交易平台经营者根据平台规则，对平台内经营者或者消费者采取对其权益有负面影响的措施的，应当告知其违反法律、法规、规章或者平台规则的事实、理由和依据，并设置便捷的申诉渠道。法律法规另有规定的，依照其规定。平台内经营者、消费者提起申诉的，网络交易平台经营者应当及时对申诉事项进行复核，客观公正作出处理；仅采用人工智能等技术手段处理，申诉人

提出人工判定要求的，应当采用人工判定的方式进行处理。网络交易平台经营者作出处理后，应当及时将处理结果告知申诉人。

第二十条 网络交易平台经营者在平台规则的制定、修改和执行过程中，不得对平台内经营者、消费者的申诉权利作出不合理限制。

第二十一条 网络交易平台经营者应当在平台规则中明确平台内交易纠纷解决机制，依照有关法律的规定公平设定平台内交易纠纷各方的举证责任。合理减轻一方举证责任的，网络交易平台经营者应当采取措施识别、防范和处置违反诚实信用原则滥用该规则侵害有关各方主体合法权益的行为。

第二十二条 网络交易平台经营者委托第三方机构和人员执行平台规则的，应当对其进行必要的培训，并依法承担因第三方机构和人员执行不当而产生的法律责任。

第三章 信息、网络和数据安全保护

第二十三条 网络交易平台经营者为平台内经营者、消费者提供信息发布服务的，应当在平台规则中以显著方式明确平台内商品和服务信息、交易信息、评论信息等信息安全条款，要求平台内经营者、消费者遵守法律法规和国家有关规定，不得制作、复制、发布、传播违法信息，应当采取措施防范和抵制制作、复制、发布、传播不良信息。

第二十四条 网络交易平台经营者应当遵循公开、公平、公正的原则，在平台规则中依法明确平台内经营者处理个人信息的规范，合理界定其与平台内经营者的个人信息保护权利和义务。

第二十五条 网络交易平台经营者通过平台规则明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务的，应当依法规定相关方的权利和义务，督促其加强网络数据安全保护。网络交易平台经营者不得利用平台规则从事非法处理用户网络数据、无正当理由限制用户网络数据权益等法律、行政法规禁止的活动。

第二十六条 未成年人用户数量巨大或者对未成年人群体具有显著影响的网络交易平台经营

者应当遵循公开、公平、公正的原则，制定专门的平台规则，依法明确平台内经营者的未成年人网络保护义务，并以显著方式提示未成年人用户依法享有的网络保护权利和遭受网络侵害的救济途径。

第四章 平台内经营者权益保护

第二十七条 网络交易平台经营者不得利用平台规则，实施下列对平台内经营者的自主经营活动进行不合理限制或者附加不合理条件的行为：

（一）强制或者变相强制平台内经营者承担退款不退货等售后责任，损害其合法权益；（二）强制或者变相强制平台内经营者开通非经营活动必需的增值服务，增加其经营成本；（三）强制或者变相强制平台内经营者参加推广、促销活动；（四）强制或者变相强制平台内经营者仅在特定平台开展经营活动；（五）其他对平台内经营者的自主经营活动进行不合理限制或者附加不合理条件的行为。网络交易平台经营者不得强制或者变相强制平台内经营者按照其定价规则，以低于成本的价格销售商品或者提供服务，扰乱市场竞争秩序。

第二十八条 网络交易平台经营者不得利用平台规则，实施下列向平台内经营者收取不合理费用的行为：

（一）重复收费；
（二）只收费不服务或者少服务；
（三）转嫁应当由平台自身承担的费用；
（四）向平台内经营者收取提供其基础经营数据的费用；
（五）强制或者变相强制平台内经营者购买服务或者参加推广、促销活动并收费；
（六）利用明显不合理的保证金等形式变相收费或者提高收费标准；
（七）收取其他不合理费用。网络交易平台经营者不得利用平台规则，在提供相同商品或者服务的情形下，对具有同等交易条件的平台内经营者实行价格歧视。

第二十九条 网络交易平台经营者在平台规则中对平台内经营者有关行为设置违约金或者损害赔偿金的，应当合理设置违约金的数额或者损害

赔偿金的计算方法；按照平台规则收取违约金或者损害赔偿金的，应当告知相应的计算依据和方法，不得利用平台规则收取明显超出合理水平的违约金或者损害赔偿金。

第五章 消费者权益保护

第三十条 网络交易平台经营者不得在平台规则的制定、修改和执行过程中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，具体包括下列情形：

（一）要求消费者承担的违约金或者损害赔偿金超过法定数额或者明显超过合理数额；
（二）排除或者限制消费者依法自主选择商品或者服务的权利；
（三）排除或者限制消费者依法请求支付违约金或者损害赔偿金的权利；
（四）排除或者限制消费者依法投诉、举报、请求调解、申请仲裁、提起诉讼的权利；
（五）其他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的情形。

第三十一条 网络交易平台经营者不得利用平台规则，在消费者不知情的情况下，对同一商品或者服务在同等交易条件下设置不同的价格或者收费标准。

第三十二条 消费者购买网络交易平台经营者提供的会员服务的，网络交易平台经营者不得在约定服务期内通过单方面修改平台规则的方式，擅自收取额外费用或者减损会员权益。在消费者继续购买会员服务前，网络交易平台经营者应当以显著方式告知消费者平台规则中与会员权益相关的变化情况。因无法预见的客观情况导致网络交易平台经营者无法按照原有平台规则对消费者提供相关服务，消费者提出终止会员服务的，应当依照本办法第十四条的规定处理。

第六章 监督管理

第三十三条 市场监督管理、网信部门应当依据职责对平台规则的制定、修改和执行活动加强监督管理，并建立健全线索移交、信息共享、会商研判等工作机制。市场监督管理、网信部门依法开

展监督管理活动，网络交易平台经营者应当予以配合，提供必要的数据、技术支持和协助，并确保所提供数据的真实性、准确性。

第三十四条 鼓励网络交易平台经营者建立平台规则社会共治制度，通过消费者组织、第三方机构和专家咨询、评议等方式，充分听取各方对平台规则的意见。

第三十五条 鼓励网络交易平台经营者发布年度平台规则合规报告，对平台规则的制定、修改和执行情况开展合规自评，并接受社会监督。鼓励网络交易平台经营者邀请或者委托第三方机构，出具平台规则外部合规评估报告。

第三十六条 省级以上市场监督管理、网信部门可以通过组织专家评审等方式，对本辖区内网络交易平台经营者制定、修改和执行平台规则的情况提出意见，并及时反馈相关网络交易平台经营者，指导其优化平台规则制定、修改和执行机制。

第三十七条 市场监督管理、网信部门在依照本办法规定履行平台规则监督管理职责过程中，应当确保行政检查于法有据、严格规范、公正文明、精准高效，避免对网络交易平台经营者、平台内经营者正常经营活动造成不必要的干扰。

第三十八条 网络交易平台经营者在平台规则的制定、修改和执行过程中有下列情形之一的，市场监督管理、网信部门可以依据职责对其有关负责人进行约谈，要求其说明情况、采取措施进行整改：

- (一) 履行网络交易相关法定义务不到位的；
- (二) 发生网络交易相关重大负面舆情事件的；
- (三) 市场监督管理、网信部门在日常监督管理中发现存在可能对网络交易秩序造成负面影响问题的；
- (四) 未保障平台内经营者、消费者等有关各方主体合法权益的；
- (五) 其他需要约谈的情形。

第七章 法律责任

第三十九条 网络交易平台经营者有下列行为之一的，依照《中华人民共和国电子商务法》第

八十一条的规定进行处罚：

(一) 违反本办法第七条规定，未在其网站、应用程序首页显著位置，持续公示平台规则信息或者上述信息的链接标识的；

(二) 违反本办法第十条规定，未按照要求公开征求意见的；

(三) 违反本办法第十二条第一款规定，未按照规定的时间提前公示平台规则内容的；

(四) 违反本办法第十四条第一款规定，平台内经营者不接受平台规则修改的内容要求退出，以设置不合理条件等方式阻止其退出的。

第四十条 网络交易平台经营者违反本办法第八条第二款、第十一条、第十四条第二款、第十六条、第二十条、第二十九条、第三十条、第三十二条第一款规定，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定，属于市场监督管理部门职责的，由市场监督管理部门责令限期改正，可以处一万元以上十万元以下罚款。

第四十一条 网络交易平台经营者违反本办法第二十三条至第二十六条规定，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定，属于网信部门职责的，由网信部门责令限期改正，可以处一万元以上十万元以下罚款。

第四十二条 网络交易平台经营者违反本办法第二十七条第一款、第二十八条第一款规定的，依照《中华人民共和国电子商务法》第八十二条的规定进行处罚。网络交易平台经营者违反本办法第二十七条第二款规定的，依照《中华人民共和国反不正当竞争法》第三十条的规定进行处罚。网络交易平台经营者违反本办法第二十八条第二款规定的，依照《中华人民共和国价格法》第四十条、《价格违法行为行政处罚规定》第四条的规定进行处罚。

第四十三条 网络交易平台经营者违反本办法第三十一条规定的，依照《中华人民共和国消费者权益保护法》第五十六条第一款的规定进行处罚。

第四十四条 网络交易平台经营者利用平台规则从事垄断行为的，依照《中华人民共和国反垄断法》的规定进行处罚。

第四十五条 市场监督管理部门依照本办法对网络交易平台经营者作出行政处罚决定后，应当依法通过国家企业信用信息公示系统向社会公示。

第八章 附 则

第四十六条 平台规则制定、修改和执行活动的监督管理依法属于其他有关部门职责的，由其他有关部门依照有关规定执行。

第四十七条 本办法自2026年2月1日起施行。

直播电商监督管理办法

原载：“网信中国”微信公众号

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、音频直播或者多种直播相结合等形式销售商品或者提供服务的经营活动。

本办法所称直播电商平台经营者，是指在直播电商活动中提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。

本办法所称直播间运营者，是指在直播电商平台上注册账号或者通过自建网站、其他网络服务，开设直播间从事直播电商活动的自然人、法人和非

法人组织。实际运营他人直播间的，也应当依照本办法规定履行直播间运营者的相应义务。

本办法所称直播营销人员，是指在直播电商活动中直接面向社会公众开展商品或者服务宣传、推介活动的自然人。本办法所称直播营销人员服务机构，是指为直播营销人员从事直播电商活动提供策划、运营、经纪、培训和技术支持等服务的机构。

第三条 从事直播电商活动，应当遵循自愿、平等、公平、诚信的原则，遵守法律、法规、规章和商业道德、公序良俗，公平参与市场竞争，接受政府监管和社会监督，营造良好直播电商生态。

第四条 直播电商监督管理应当坚持鼓励创新、严守底线、线上线下一体化监管的原则，营造有利于直播电商健康发展的市场环境，充分发挥直播电商在推动高质量发展、满足人民日益增长的美好生活需要等方面的重要作用。

第五条 鼓励直播电商平台经营者、直播间运营者建立健全首问负责、先行赔付、在线争议解决等制度，及时预防和解决直播电商领域消费争议。鼓励相关行业组织加强行业自律，建立健全行业规范，推动行业诚信建设，监督、引导本行业经营者公平参与市场竞争、自觉维护消费者合法权益。鼓励消费者组织加强对直播电商活动的社会监督，维护消费者合法权益。

第二章 直播电商平台经营者

第六条 直播电商平台经营者应当建立健全直播账号注册注销、平台内交易行为规范、商品和服务质量保障、消费者权益保护、个人信息保护、网络和数据安全保护以及直播间运营者、直播营销人员、直播营销人员服务机构管理等机制。

直播电商平台经营者应当加强直播电商信息内容管理，建立健全内容审核机制，营造良好直播电商生态。

第七条 直播电商平台经营者应当遵循公开、公平、公正的原则，制定平台服务协议和交易规则（以下简称平台规则），明确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等主体的权利和义务，并以显著方式提

醒相关主体注意与其有重大利害关系的内容。直播电商平台经营者应当在平台规则中要求直播间运营者、直播营销人员服务机构规范直播营销人员的招募、培训、使用、管理等工作。

第八条 直播电商平台经营者应当要求申请进入平台从事直播电商活动的直播间运营者提供其名称（姓名）、统一社会信用代码（身份证件号码）、实际经营地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并至少每六个月核验更新一次。

直播电商平台经营者应当要求直播间运营者在直播营销人员首次直播前，提供经核验无误的该人员姓名、身份证件号码、经常居住地址、联系方式、所属直播营销人员服务机构以及与直播营销相关的专业资质、职业职务等身份信息，对直播间运营者履行核验义务提供技术支持并进行监督。

直播电商平台经营者应当建立并落实直播营销人员真实身份动态核验制度，不得为与真实身份不符或者依照国家有关规定不得从事直播电商活动的人员提供相关服务。

第九条 直播电商平台经营者应当分别于每年一月和七月向平台住所地省级市场监督管理部门报送直播间运营者、直播营销人员的下列身份信息：

（一）已办理经营主体登记的直播间运营者的名称（姓名）、统一社会信用代码、实际经营地址、联系方式、直播账号等信息；

（二）未办理经营主体登记的直播间运营者的姓名、身份证件号码、实际经营地址、联系方式、直播账号等信息；

（三）直播营销人员的姓名、身份证件号码、经常居住地址、联系方式、所属直播营销人员服务机构以及与直播营销相关的专业资质、职业职务等信息。

第十条 直播电商平台经营者应当建立健全直播营销人员培训机制，每年对直播营销人员开展培训；在为首次从事直播电商活动的直播营销人员提供直播服务前，应当组织开展网络交易、网络信

息安全相关法律、法规、规章以及产品质量安全、消费者权益保护、平台规则等方面的培训。直播营销人员不得在接受培训时弄虚作假或者拒不参加培训。直播电商平台经营者应当每年组织直播间运营者、直播营销人员服务机构学习网络交易、网络信息安全相关法律、法规、规章，及时通报有关部门的工作要求。

第十一条 直播电商平台经营者应当通过平台规则建立健全直播间运营者分级分类管理制度，根据直播间运营者合规情况、关注和访问量、交易规模、所销售的商品或者服务种类以及其他指标，采取相应的管理措施。其中，对关注用户多、交易规模大、直播营销人员影响力强、多次出现违法行为或者从事关系消费者生命健康的商品或者服务的直播电商活动的直播间运营者，应当采取技术监测、实时巡查等管理措施。

鼓励直播电商平台经营者建立健全直播间运营者信用评价指标体系，将市场监督管理、网信部门依法共享或者通报的经营异常名录、严重违法失信名单、行政处罚、信用修复等信息纳入信用评价指标体系，并根据信用评价结果，采取相应的管理措施。

第十二条 直播电商平台经营者应当通过平台规则建立健全平台内违法行为处置制度，明确对违反法律、法规、规章的直播间运营者、直播营销人员、直播营销人员服务机构采取警示、限制功能、限制流量、暂停直播、限期停播、关闭账号、禁止重新注册账号、列入黑名单等处置措施的具体情形、程序以及相应的救济途径。采取处置措施的种类和幅度，应当与有关违法行为的事实、性质、情节、社会危害程度等相当。

市场监督管理、网信部门经调查核实，将相关直播间运营者、直播营销人员、直播营销人员服务机构违法情况通报直播电商平台经营者的，直播电商平台经营者应当根据相关法律、法规、规章以及平台规则，及时依照前款规定采取相应的处置措施。直播电商平台经营者采取处置措施的，应当保存有关记录，依法及时向平台住所地县级以上市场监督

管理、网信部门报告，并作为评价直播间运营者、直播营销人员、直播营销人员服务机构合规情况的参考。其中，采取关闭账号、禁止重新注册账号、列入黑名单等处置措施的，应当同时向平台住所地省级市场监督管理、网信部门报告。

第十三条 直播电商平台经营者应当建立健全风险识别制度，配备与其经营规模相适应的直播管理专业人员，加强对直播电商活动的动态监测，对直播中的违法行为及时采取警示、限制流量、暂停直播等处置措施。

第十四条 直播电商平台经营者应当通过平台规则建立健全黑名单制度，将严重违反市场监督管理、网信领域法律、行政法规的直播间运营者、直播营销人员、直播营销人员服务机构列入黑名单。

直播电商平台经营者将相关主体列入黑名单的，应当及时告知其违反法律、行政法规的事实、理由和依据，列入黑名单的具体期限以及相应的申诉途径；相关主体提起申诉的，应当对申诉事项进行必要的复核，客观公正作出处理，并及时将处理结果告知相关主体。

直播电商平台经营者应当加强对被列入黑名单的相关主体的管理，采取必要措施防止其在被列入黑名单期间，通过更换账号、重新注册账号等方式逃避惩戒；列入黑名单的期限届满的，应当将其移出并同步解除相应的处置措施。鼓励直播电商平台经营者之间共享黑名单相关信息，对相关主体采取信用管理措施。

第十五条 直播电商平台经营者应当为直播间运营者依法履行信息公示义务提供必要的技术支持。直播间运营者公示的信息发生变更的，应当在三个工作日内将变更情况报送直播电商平台经营者，直播电商平台经营者应当在七个工作日内进行核验，完成更新公示。

第十六条 直播电商平台经营者应当通过技术手段确保交易信息的完整性。交易信息应当包括直播账号，有关商品或者服务的直播视频回放记录、直播互动信息，消费者订单形成时的商品或者服务详情页面快照、客服记录、支付记录、物流快递、

退换货以及售后等信息。上述交易信息的保存时间自交易完成之日起不少于三年。法律、行政法规另有规定的，依照其规定。

第十七条 直播电商平台经营者应当采取有效措施，防范和处置直播间运营者、直播营销人员利用人工智能等技术手段，编造、传播虚假或者引人误解的商业信息，假冒他人进行商业宣传，欺骗、误导消费者和其他经营者。

第十八条 直播电商平台经营者应当建立健全消费者权益保护制度，明确消费争议解决机制。发生消费争议的，直播电商平台经营者应当根据消费者的要求提供直播间运营者、直播营销人员相关信息以及相关交易记录等必要信息。

第十九条 直播电商平台经营者知道或者应当知道直播间运营者、直播营销人员销售的商品或者提供的服务不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为的，应当依法采取必要措施。

第二十条 直播电商平台经营者应当建立健全投诉机制，明确处理流程和反馈时限，及时处理消费者投诉，并采取必要措施识别、防范和处置违反诚实信用原则滥用平台投诉机制的行为。

对于投诉集中的直播间运营者、直播营销人员，直播电商平台经营者应当及时采取技术监测、实时巡查等管理措施。

直播电商平台经营者应当将核查属实的投诉情况作为评价直播间运营者、直播营销人员、直播营销人员服务机构合规情况的参考。

第二十一条 直播电商平台经营者应当积极配合市场监督管理、网信部门依法开展的监督检查、案件调查、事故处置、缺陷消费品召回、消费争议处理等监管执法活动，如实提供有关直播间运营者、直播营销人员的身份信息、商品或者服务信息、交易信息等。

第二十二条 市场监督管理部门依法对直播间运营者、直播营销人员开展调查，发现上述主体通过实际经营地址、经常居住地址无法联系的，应当及时通报直播电商平台经营者。直播电商平台

经营者应当在接到市场监督管理部门通报后五个工作日内提醒相关直播间运营者、直播营销人员及时更新相关信息。

经提醒，相关直播间运营者、直播营销人员仍不及时更新相关信息的，直播电商平台经营者应当根据平台规则，对其采取相应的处置措施，并保存有关记录。

相关直播间运营者、直播营销人员更新相关信息后，可以根据平台规则，向平台申请解除处置措施。直播电商平台经营者收到申请并核验无误后，应当及时解除处置措施。

第二十三条 直播电商平台经营者对直播间运营者、直播营销人员采取处置措施的，应当对受影响的消费者的相关订单处理、售后服务、消费纠纷解决等作出妥善安排，协助消费者进行维权。

第二十四条 其他网络服务提供者在直播电商活动中，提供网络经营场所、交易撮合、信息发布等服务的全部或者部分内容的，应当根据其具体服务内容，依法履行本章规定的直播电商平台经营者应当履行的身份核验及登记、有关信息报送、违法行为处置及报告、交易信息保存、协助消费者维权和配合监管执法等相应义务；违反相关规定的，依法承担相应的责任。

第三章 直播间运营者、直播营销人员

第二十五条 直播间运营者为法人或者非法人组织的，应当在直播账号信息主页显著位置依法公示真实有效的名称、统一社会信用代码、住所、行政许可等信息，或者上述信息的链接标识。

直播间运营者为自然人，属于个体工商户的，应当在直播账号信息主页显著位置依法公示真实有效的名称、经营者姓名、统一社会信用代码、经营场所、组成形式等信息，或者上述信息的链接标识；属于依法不需要办理经营主体登记的其他自然人的，应当在直播账号信息主页显著位置依法公示实际经营地址、联系方式、所属直播营销人员服务机构等真实有效的信息，或者上述信息的链接标识。相关信息发生变更的，直播间运营者应当在三个工作日内将变更情况报送直播电商平台经营者。

直播间运营者依照本办法公示信息的，应当同时符合法律、行政法规和国家有关规定对展示账号相关信息的要求。

第二十六条 直播间运营者应当在其直播页面，以显著方式持续展示实际销售商品或者提供服务的经营者名称（姓名）、实际经营地址、联系方式等信息，或者该信息的链接标识。通过链接标识展示相关信息的，应当符合以下要求：

（一）在直播页面显著位置设置便捷入口，跳转页面应当真实、完整展示第一款规定的信息，不得多次跳转；

（二）不得设置连续多次验证、强制关注账号、打赏互动等不合理访问限制；

（三）不得以弹窗覆盖等技术手段干扰阅读。

第二十七条 直播间运营者应当核验实际销售商品或者提供服务的经营者的名称（姓名）、统一社会信用代码（身份证件号码）、实际经营地址、联系方式、行政许可、强制性产品认证、产品合格证明文件等信息，强化对直播选品、营销用语等的审核把关，并保存相关记录备查。保存记录自直播结束之日起不少于三年。

第二十八条 直播间运营者应当核验直播营销人员的姓名、身份证件号码、经常居住地址、联系方式、所属直播营销人员服务机构以及与直播营销相关的专业资质、职业职务等身份信息，并及时核验更新，保存相关记录备查，确保直播营销人员身份信息真实有效。保存记录自直播结束之日起不少于三年。直播间运营者应当在每次直播前将核验无误的直播营销人员身份信息报送直播电商平台经营者。

第二十九条 直播间运营者设置、展示的账号名称、头像、简介和直播间标题、封面、布景、道具等，应当符合法律、法规、规章的规定，不得含有损害国家利益和社会公共利益，违背公序良俗以及欺骗、误导消费者等内容的信息。

第三十条 直播间运营者应当建立健全事前合规审核机制，在直播前依照有关规定对展示内容、讲解内容、服装、布景、道具等进行审核。

第三十一条 直播间运营者应当建立健全直播营销人员纠错机制,发现直播营销人员出现口误、表述不完整、表述不当等情形时,应当现场进行纠正,并保存记录备查。保存记录自直播结束之日起不少于三年。直播间运营者应当对直播间互动内容进行实时管理,及时处置违法信息,并依法保存相关处置记录。

第三十二条 直播间运营者应当以显著方式展示所销售商品的品名、价格和计价单位或者提供服务的项目、内容、价格和计价方法等信息,或者上述信息的链接标识;采取价格比较、折价、减价等促销方式的,应当显著标明被比较价格或者折价、减价的计算基准等信息,或者上述信息的链接标识。

第三十三条 直播间运营者、直播营销人员不得通过直播间销售或者提供下列违法商品或者服务:

(一)不符合保障人身、财产安全的要求和环境保护要求的商品或者服务;

(二)掺杂、掺假、以假充真、以次充好等质量不合格的商品;

(三)法律、行政法规禁止交易,损害国家利益和社会公共利益,违背公序良俗的商品或者服务。

第三十四条 直播间运营者、直播营销人员不得对商品或者服务的经营主体以及性能、功能、质量、销售情况、用户评价、曾获荣誉、资格资质等作虚假或者引人误解的商业宣传,欺骗、误导消费者和其他经营者。直播间运营者、直播营销人员不得利用人工智能等技术手段,编造、传播虚假或者引人误解的商业信息,假冒他人进行商业宣传,欺骗、误导消费者和其他经营者。

第三十五条 直播间运营者、直播营销人员发布的直播内容构成商业广告的,应当依照《中华人民共和国广告法》的有关规定履行广告发布者、广告经营者或者广告代言人的义务。

下列情形一般构成前款所称的商业广告:

(一)商品经营者或者服务提供者以外有一定影响的自然人,在直播电商活动中以自己的名义或者形象对商品或者服务作推荐、证明的;

(二)为推销商品或者服务,将介绍商品或者服务的直播内容录制、剪辑、编辑后,以文字、图像、视频、音频等形式通过互联网或者其他媒介发布的;

(三)其他构成商业广告的情形。

第三十六条 直播间运营者、直播营销人员不得编造、传播或者指使他人编造、传播虚假信息或者误导性信息,损害其他经营者的商业信誉、商品声誉。

第三十七条 直播间运营者使用人工智能等技术生成的人物图像、视频从事直播电商活动的,应当符合有关法律、法规、规章和强制性国家标准的要求,并依照国家有关规定进行标识,持续向消费者提示该人物图像、视频由人工智能等技术生成。在直播电商活动中使用人工智能等技术生成的人物图像、视频,存在违反法律、法规、规章规定情形的,由管理或者使用该人物图像、视频的直播间运营者依法承担责任。法律、法规、规章另有规定的,依照其规定。

第四章 直播营销人员服务机构

第三十八条 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、管理等工作。

第三十九条 直播营销人员服务机构应当完善对直播营销人员的招募机制,核验直播营销人员的姓名、身份证件号码、经常居住地址、联系方式以及与直播营销相关的专业资质、职业职务等身份信息。

第四十条 直播营销人员服务机构应当与直播营销人员签订协议,明确各自应当履行的义务,不得减轻或者免除自身依法应当承担的责任。

第四十一条 直播营销人员服务机构应当加强对直播营销人员的培训,提醒其在直播电商活动中应当依法履行的义务。

第四十二条 直播营销人员服务机构应当加强对直播营销人员的日常管理和规范引导,建立健全直播营销人员违法行为处置制度,对发现的直播营销人员违法行为及时采取必要的处置措施。

第四十三条 直播营销人员服务机构与直播间运营者合作开展商业活动的，应当核验直播间运营者的名称（姓名）、统一社会信用代码（身份证件号码）、实际经营地址、联系方式、行政许可等信息，并与其签订书面协议，明确各自在直播营销人员管理、直播内容管理、产品质量审核、消费者权益保护等方面的义务。

第四十四条 直播营销人员服务机构不得通过组织虚假交易、虚假评价等方式，帮助直播间运营者、直播营销人员进行虚假或者引人误解的商业宣传。

第四十五条 直播营销人员服务机构提供直播选品服务的，应当核验实际销售商品或者提供服务的经营者的名称（姓名）、统一社会信用代码（身份证件号码）、实际经营地址、联系方式、行政许可、强制性产品认证、产品合格证明文件等信息，并保存相关记录备查。保存记录自直播结束之日起不少于三年。

第五章 监督管理

第四十六条 市场监督管理、网信部门应当依据职责加强对直播电商活动的监督管理，并建立健全线索移交、信息共享、会商研判等工作机制。市场监督管理、网信部门对直播电商平台经营者、直播间运营者、直播营销人员服务机构依法开展监督管理的，相关经营主体应当予以配合，提供必要的的数据、技术支持和协助，并确保所提供数据的真实性、准确性。

第四十七条 直播电商平台经营者，通过自建网站、其他网络服务从事直播电商活动的直播间运营者，以及直播营销人员服务机构违反本办法规定的行为，由其住所地县级以上市场监督管理、网信部门依据职责管辖。通过直播电商平台从事直播电商活动的直播间运营者违反本办法规定的行为，由其实际经营地县级以上市场监督管理、网信部门依据职责管辖。无法确定实际经营地，已办理经营主体登记的，由其住所地县级以上市场监督管理、网信部门依据职责管辖；未办理经营主体登记的，由直播电商平台经营者住所地县级以上市场监督管理、

网信部门依据职责管辖。直播营销人员违反本办法规定的行为，由依照前两款规定负责管辖其所在直播间的运营者违法行为的市场监督管理、网信部门依据职责管辖。

第四十八条 直播电商平台经营者住所地省级市场监督管理部门应当根据工作需要，及时将其掌握的直播间运营者、直播营销人员身份信息与直播间运营者实际经营地的省级市场监督管理部门共享。

第四十九条 市场监督管理、网信部门依据职责对涉嫌违法的直播电商活动进行查处时，可以依法采取下列措施：

（一）对与涉嫌违法的直播电商活动有关的场所进行现场检查；

（二）查阅、复制与涉嫌违法的直播电商活动有关的合同、票据、账簿等有关资料；

（三）收集、调取、复制与涉嫌违法的直播电商活动有关的电子数据；

（四）询问涉嫌从事违法的直播电商活动的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等当事人；

（五）向与涉嫌违法的直播电商活动有关的自然人、法人和非法人组织调查了解有关情况；

（六）法律、法规规定可以采取的其他措施。

第五十条 市场监督管理、网信部门发现直播间运营者、直播营销人员、直播营销人员服务机构有违反市场监督管理、网信领域法律、法规、规章的行为，依法要求直播电商平台经营者采取必要处置措施的，直播电商平台经营者应当予以配合。

第五十一条 市场监督管理部门依法对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等主体实施信用监管，将其注册登记、备案、行政许可、抽查核查结果、行政处罚、存续状态、列入经营异常名录和市场监督管理严重违法失信名单等信息，依法通过国家企业信用信息公示系统公示。对存在严重违法失信行为的，依法采取相应的惩戒措施。

前款规定的信息还可以通过市场监督管理部

门官方网站、网络搜索引擎、经营者从事经营活动的主页面显著位置等公示。网信部门依法将实施违法行为情节严重、影响恶劣的相关主体列入互联网严重失信名单，并采取相应的惩戒措施。

第五十二条 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有下列情形之一的，市场监督管理、网信部门可以依据职责对其有关责任人进行约谈，要求其说明情况、采取措施进行整改：

- (一) 履行直播电商相关法定义务不到位的；
- (二) 发生直播电商相关重大负面舆情事件的；
- (三) 市场监督管理、网信部门在日常监督管理中发现存在可能对直播电商秩序造成负面影响问题的；
- (四) 未保障消费者等有关各方主体合法权益的；
- (五) 其他需要约谈的情形。

第六章 法律责任

第五十三条 直播电商平台经营者有下列行为之一，属于市场监督管理部门职责的，由市场监督管理部门依照《中华人民共和国电子商务法》第八十条的规定进行处罚：

- (一) 不依照本办法第八条第一款规定对直播间运营者身份信息进行核验、登记的；
- (二) 不依照本办法第九条第一项、第二项规定报送有关信息的；
- (三) 不履行本办法第十六条规定的交易信息保存义务的。

第五十四条 直播电商平台经营者有下列行为之一，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定，属于市场监督管理部门职责的，由市场监督管理部门责令限期改正；拒不改正或者情节严重的，处一万元以上十万元以下罚款：

- (一) 不依照本办法第八条第三款规定对直播营销人员真实身份进行核验的；
- (二) 不依照本办法第九条第三项规定报送有关信息的；

(三) 不履行本办法第十条规定的培训义务的；

(四) 不依照本办法第十一条第一款规定建立健全直播间运营者分级分类管理制度的；

(五) 不依照本办法第十二条规定建立健全平台内违法行为处置制度的；

(六) 不依照本办法第十三条规定建立健全风险识别制度的；

(七) 不依照本办法第十四条规定建立健全黑名单制度的；

(八) 不依照本办法第十七条规定采取有效措施防范和处置有关虚假商业宣传行为的；

(九) 不履行本办法第二十二条规定的提醒、处置义务的。

第五十五条 直播电商平台经营者违反本办法第十八条规定，属于市场监督管理部门职责的，由市场监督管理部门依照《中华人民共和国消费者权益保护法实施条例》第五十条第一款的规定进行处罚。

第五十六条 直播电商平台经营者违反本办法第十九条规定，对直播间运营者、直播营销人员侵害消费者合法权益行为未采取必要措施的，由市场监督管理部门依照《中华人民共和国电子商务法》第八十三条的规定进行处罚。

第五十七条 直播间运营者不履行本办法第二十五条第一款至第三款规定的信息公示义务的，由市场监督管理部门依照《中华人民共和国电子商务法》第七十六条的规定进行处罚。

第五十八条 直播间运营者不履行本办法第二十六条规定的信息展示义务，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定，属于市场监督管理部门职责的，由市场监督管理部门责令限期改正；逾期不改正的，处一万元以下罚款。

第五十九条 直播间运营者有下列行为之一，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定，属于市场监督管理部门职责的，由市场监督管理部门责令限期改正；拒不改正或者情节严重的，处一万元以上十万元以下罚款：

(一)不履行本办法第二十七条、第二十八条规定的核验义务的;

(二)不依照本办法第二十九条规定设置、展示账号名称、头像、简介和直播间标题、封面、布景、道具等的;

(三)不依照本办法第三十条规定建立健全事前合规审核机制的;

(四)不依照本办法第三十一条规定建立健全直播营销人员纠错机制的;

(五)不履行本办法第三十七条第一款规定的标识义务的。

第六十条 直播间运营者违反本办法第三十二条规定的,由市场监督管理部门依照《中华人民共和国价格法》、《价格违法行为行政处罚规定》进行处罚。

第六十一条 直播间运营者、直播营销人员违反本办法第三十三条规定,通过直播间销售或者提供有关违法商品或者服务,法律、行政法规有规定的,依照其规定;法律、行政法规没有规定,属于市场监督管理部门职责的,由市场监督管理部门责令限期改正,处一万元以上十万元以下罚款。

第六十二条 直播间运营者、直播营销人员、直播营销人员服务机构违反本办法第三十四条、第四十四条规定的,由市场监督管理部门依照《中华人民共和国反不正当竞争法》第二十五条第一款的规定进行处罚;属于发布虚假广告的,依照《中华人民共和国广告法》第五十五条的规定进行处罚。直播间运营者、直播营销人员违反本办法第三十六条规定的,由市场监督管理部门依照《中华人民共和国反不正当竞争法》第二十八条的规定进行处罚。

第六十三条 直播营销人员违反本办法第三十三条、第三十四条、第三十六条规定,属于职务行为的,由其所在单位承担相应的行政责任;但是,有证据证明该直播营销人员的行为与其职务行为无关的除外。

第六十四条 直播营销人员服务机构不履行本办法第三十九条、第四十三条、第四十五条规定的核验义务,或者不依照本办法第四十二条规定加

强对直播营销人员的日常管理和规范引导,法律、行政法规有规定的,依照其规定;法律、行政法规没有规定,属于市场监督管理部门职责的,由市场监督管理部门责令限期改正;拒不改正或者情节严重的,处一万元以上十万元以下罚款。

第六十五条 在直播电商活动中制作、复制、发布、传播违法信息,或者未采取措施防范和抵制制作、复制、发布、传播不良信息的,由网信部门依据职责,依照《中华人民共和国网络安全法》、《互联网信息服务管理办法》等法律、行政法规的规定进行处罚。违反本办法第六条至第八条、第十条、第十一条第一款、第十二条、第十三条、第十四条第一款至第三款、第十六条、第十七条、第二十五条第四款、第二十七条、第二十九条至第三十一条、第三十四条、第三十六条、第三十七条、第四十一条至第四十四条,属于网信部门职责的,由网信部门依照《中华人民共和国网络安全法》、《互联网信息服务管理办法》等法律、行政法规的规定进行处罚;法律、行政法规没有规定的,由网信部门责令限期改正;拒不改正或者情节严重的,处一万元以上十万元以下罚款,并可以责令暂停提供相关服务。

第六十六条 妨害市场监督管理、网信部门依照本办法履行职责,拒绝、阻碍监管执法的,法律、行政法规、部门规章有规定的,依照其规定;法律、行政法规、部门规章没有规定的,由市场监督管理、网信部门依据职责责令改正,对个人可以处一千元以上一万元以下罚款,对单位可以处一万元以上十万元以下罚款。

第六十七条 违反本办法规定,涉嫌犯罪的,依法移送司法机关追究刑事责任。

第七章 附 则

第六十八条 直播电商活动的监督管理依法属于其他有关部门职责的,由其他有关部门依照有关规定执行。**第六十九条** 本办法自2026年2月1日起施行。

市场监管总局关于印发《互联网平台反垄断合规指引》的通知

原载：“国家市场监督管理总局”官网

各省、自治区、直辖市和新疆生产建设兵团市场监管局（厅、委）：

现将《互联网平台反垄断合规指引》印发给你们，请结合实际做好宣传和贯彻实施。

市场监管总局
2026年1月28日
（此件公开发布）

互联网平台反垄断合规指引

第一章 总则

第一条 目的和依据

为支持和引导平台经营者有效防范反垄断合规风险，健全反垄断合规管理制度，保护相关主体合法权益，维护市场公平竞争秩序，促进平台经济创新健康发展，根据《中华人民共和国反垄断法》（以下简称《反垄断法》）等法律规定，制定本指引。

第二条 相关概念

本指引所称互联网平台，是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交易或者其他活动，以此共同创造价值的商业组织形态。

本指引所称平台经营者，是指向自然人、法人以及其他市场主体提供经营场所、交易撮合、信息交流等互联网平台服务的经营者。

本指引所称平台内经营者，是指在互联网平台内提供商品或者服务（以下统称商品）的经营者。

本指引所称反垄断合规风险，是指平台经营者及其员工因违反《反垄断法》相关规定，引发法律责任、造成经济或者声誉损失以及其他负面后果的可能性。

本指引所称反垄断合规管理，是指以防控反垄断合规风险为目的，针对平台经营者的经营管理行

为和员工履职行为开展的有组织、有计划、全流程的管理活动。

第三条 合规管理必要性

互联网平台网络效应明显，涉及平台经营者、平台内经营者、消费者和从业人员等多方主体。平台经营者通常具有一定的管理者属性，通过数据和算法、技术、资本优势、平台规则等强化市场力量，影响平台竞争生态，要切实加强反垄断合规管理。

平台经营者违反《反垄断法》，将承担相应的法律责任，产生相关商业风险和信用风险。平台经营者加强反垄断合规管理，可以避免因从事垄断行为产生的风险，培育良好品牌形象和核心竞争优势。

平台经营者增强反垄断合规意识，健全反垄断合规管理制度，有利于提高竞争层次和水平，优化资源配置，提升运行效率，维护多方主体合法权益，推动平台竞争生态持续优化，实现平台经济创新发展。

第四条 基本原则

平台经营者遵循以下基本原则，参考本指引开展反垄断合规管理工作，实现规则公平、算法向善、竞争合规：

（一）针对性原则。结合所处行业、商业模式、治理结构、市场竞争状况等因素，有针对性地识别、评估和防控合规风险，开展反垄断合规管理。

（二）全面性原则。推进事前事中事后全链条合规，实现业务领域、部门、员工全覆盖，贯穿决策、执行、监督各环节，构建协同联动的全面合规体系。

（三）穿透性原则。贯通平台经营者总部和分公司、控股子公司等，完善总部指导、协调、监督机制，压实各分支机构等自身合规管理职责，实现层级穿透、业务穿透、规则算法穿透。

（四）持续性原则。健全反垄断合规长效机制，保障合规管理制度持续有效执行，防止“一次性”“阶段性”合规，定期评估自身合规经营情况，及时更新完善反垄断合规管理制度。

第五条 合规总体要求

平台经营者要切实承担反垄断合规主体责任，

健全反垄断合规制度，加强反垄断合规管理，依法竞争、合规经营，不得利用数据和算法、技术、资本优势、平台规则等从事《反垄断法》禁止的垄断行为。

第二章 风险识别

第一节 垄断协议

垄断协议，是指排除、限制竞争的协议、决定或者其他协同行为。《反垄断法》禁止经营者达成垄断协议。平台经营者要遵守《反垄断法》《禁止垄断协议规定》，避免在提供平台服务或者开展自营业务等过程中达成垄断协议，以及组织其他经营者达成垄断协议或者提供实质性帮助。

平台经营者识别垄断协议风险，通常首先分析相关行为是否属于《反垄断法》第十七条、第十八条第一款和第十九条规定的情形，再分析上述行为是否符合《反垄断法》规定的不予禁止或者豁免条件。

第六条 横向垄断协议

具有竞争关系的平台经营者，要避免通过以下方式达成固定或者变更价格、限制产（销）量、分割市场、限制新技术（产品）、联合抵制交易等横向垄断协议：

（一）利用会议、电话、短信、电子邮件、共享文档、即时通讯工具、共享数据池、互操作协议、云存储平台、人工智能等就竞争性敏感信息进行意思联络和信息交流；

（二）收集并且交换定价模式、佣金比例、优惠政策、客户名单、流量分配机制以及研发、投资、生产、营销、推广策略等竞争性敏感信息；

（三）利用数据、算法、技术、平台规则等实现用户分类、动态定价、流量分配、商品排序等方面的协调一致行为。

风险示例：平台间算法共谋

具有竞争关系的平台经营者利用算法，通过意思联络、交换敏感信息、行为协调一致等方式，达成垄断协议。比如：平台经营者甲、乙之间具有竞争关系，甲和乙通过算法进行共谋，统一定价机制、抽佣比例等，达成横向垄断协议，排除、限制市场

竞争。

第七条 纵向垄断协议

平台经营者要避免通过以下方式与交易相对人达成固定转售价格、限定最低转售价格等纵向垄断协议：

（一）利用大数据分析、人工智能等技术手段对转售价格进行自动化设定；

（二）利用接口调用、数据使用、流量分配、促销活动、店铺管理、用户服务等方面的平台规则对转售价格进行统一；

（三）利用用户画像、预测算法等对转售价格进行直接或者间接限定。

第八条 组织与实质性帮助

平台经营者要避免通过以下方式组织平台内经营者等其他经营者达成垄断协议或者为达成垄断协议提供实质性帮助：

（一）通过共享数据、发布通知、签署协议等组织、协调平台内经营者之间或者与其他经营者进行意思联络；

（二）为平台内经营者等其他经营者获取竞争性敏感信息、实现协调一致行为提供必要支持、创造关键性便利条件等。

风险示例：组织帮助平台内经营者达成垄断协议

平台经营者组织、协调具有竞争关系的平台内经营者达成横向协议，或者通过提供必要支持、创造关键性条件进行实质性帮助。比如：平台经营者甲与平台内具有竞争关系的经营者分别签署内容相同或者相似的调价协议，在此过程中，促成平台内经营者进行了意思联络，交换了竞争性敏感信息，最终形成一致的定价行为，排除、限制市场竞争。

第二节 滥用市场支配地位行为

滥用市场支配地位行为，是指具有市场支配地位的经营者从事的以不公平高价销售、以不公平低价购买或者没有正当理由低于成本销售、拒绝交易、限定交易、搭售、附加其他不合理条件、差别待遇等行为。《反垄断法》禁止具有市场支配地位的经营者从事滥用市场支配地位行为。鼓励市场份额或

者市场力量较大的平台经营者定期评估是否对相关市场具有市场支配地位。平台经营者要遵守《反垄断法》《禁止滥用市场支配地位行为规定》，避免在提供平台服务或者开展自营业务等过程中从事滥用市场支配地位行为。

平台经营者识别滥用市场支配地位行为风险，通常首先界定相关市场，评估在相关市场是否具有市场支配地位、是否实施相关行为，再结合是否具有正当理由以及相关行为是否排除、限制市场竞争，具体分析是否构成滥用市场支配地位行为。

第九条 市场支配地位的考虑因素

平台经营者评估在相关市场是否具有市场支配地位，可以考虑以下因素：

(一)平台经营者的市场份额以及相关市场竞争状况。确定平台经营者市场份额，可以考虑交易金额、交易数量、销售额、注册用户数、活跃用户数、点击量、使用时长、平台内经营者数量或者其他指标在相关市场所占比重，同时考虑该市场份额持续的时间。分析相关市场竞争状况，可以考虑相关市场的发展状况、竞争性平台经营者数量以及市场份额、平台竞争特点、平台差异程度、规模经济、潜在竞争性平台经营者情况、创新和技术变化等。

(二)平台经营者控制市场的能力。可以结合线上和线下业务多样性、纵向一体化等因素考虑平台经营者控制上下游市场或者其他关联市场的能力，阻碍、影响其他平台经营者进入相关市场的能力，相关经营模式、网络效应，以及影响或者决定价格、流量或者其他交易条件的能力等。

(三)平台经营者的财力和技术条件。可以考虑投资者情况、资产规模、资本来源、盈利能力、融资能力、技术创新和应用能力、拥有的知识产权、掌握和处理相关数据的能力，以及该财力和技术条件能够以何种程度促进业务扩张或者巩固、维持市场地位等。

(四)平台内经营者等其他经营者对该平台经营者在交易上的依赖程度。可以考虑平台内经营者等其他经营者与该平台经营者的交易关系、交易量、

交易持续时间，锁定效应、用户黏性，以及转向其他平台的可能性以及转换成本等。

(五)其他平台经营者进入相关市场的难易程度。可以考虑市场准入、平台规模效应、资金投入规模、技术壁垒、用户多栖性、用户转换成本、数据获取的难易程度、用户习惯等。

(六)基于平台经济特点认定平台经营者具有市场支配地位的其他因素。

第十条 不公平高价或者不公平低价

具有市场支配地位的平台经营者，要避免通过以下方式滥用市场支配地位，以不公平的高价销售商品或者以不公平的低价购买商品：

(一)向平台内经营者收取明显高于其他同类业务平台经营者在相同或者相似市场条件下的佣金、注册费、手续费、会员费、技术服务费、信息服务费、营销推广费等费用，或者在成本基本稳定的情况下，超过正常幅度提高向平台内经营者收取的上述费用；

(二)通过拆分服务项目、增加收费名目等，变相向平台内经营者收取不公平的高额费用；

(三)向平台内经营者支付明显低于其他同类业务平台经营者在相同或者相似市场条件下的商品价格。

认定市场条件相同或者相似，一般可以考虑平台类型、经营模式、交易环节、成本结构、交易具体情况等因素。

风险示例：平台不公平高价

具有市场支配地位的平台经营者，借助平台规则、技术和算法等，滥用市场支配地位，向平台内经营者收取不公平的高额费用。比如：具有市场支配地位的平台经营者甲，在成本基本稳定的情况下，连续多年超过正常幅度提高服务费用，对平台内经营者收取不公平的高额费用，损害平台内经营者利益。

第十一条 低于成本销售

具有市场支配地位的平台经营者，要避免滥用市场支配地位，没有正当理由，通过过度补贴、交叉补贴等方式，以低于成本的价格销售商品或者提

供服务，排除、限制市场竞争。

分析是否构成低于成本销售，一般重点考虑平台经营者是否以低于成本的价格排挤竞争性平台经营者，以及是否可能在将竞争性平台经营者排挤出市场后，获取非公平竞争水平下的不当利益、损害市场公平竞争和消费者合法权益等情况。

在计算成本时，可以综合考虑平台涉及多边市场中各相关市场之间的成本关联情况及其合理性。

风险示例：平台低于成本销售

具有市场支配地位的平台经营者，滥用市场支配地位，没有正当理由，通过过度补贴、超过合理限度的优惠政策等方式，以低于成本的价格提供服务，排除、限制市场竞争。比如：具有市场支配地位的平台经营者甲，明显超出符合商业惯例的合理期限，给予平台内经营者免费入驻、大额补贴优惠，待竞争性平台经营者退出相关市场后，大幅提高入驻费等相关费用，获取不当利益，损害了市场公平竞争和消费者合法权益。

第十二条 拒绝交易

具有市场支配地位的平台经营者，要避免通过以下方式滥用市场支配地位，没有正当理由，拒绝与交易相对人进行交易，排除、限制市场竞争：

（一）通过下架商品、封禁账号、设置复杂的交易流程、限制流量、关闭接口、中断数据共享等，停止、拖延、中断与交易相对人的交易；

（二）通过设置不合理的交易条件、显著高于市场合理水平的服务费、停止提供应用程序更新、中断数据更新、拖延签署合作协议等，拒绝与交易相对人进行交易；

（三）利用流量分配算法、商品发布规则等，限制获取流量、接受订单，实质性削减与交易相对人的交易数量；

（四）制定不合理的营销、研发等平台规则，或者使用歧视性算法设置不合理的限制和障碍，使交易相对人难以开展交易；

（五）通过控制构成必需设施的特定数据、模型、应用平台等，拒绝与交易相对人以合理条件进行交易。

风险示例：封禁屏蔽

具有市场支配地位的平台经营者，滥用市场支配地位，没有正当理由，对交易相对人在应用层、传输层、网络层等进行封禁屏蔽，导致其无法进入相关市场，排除、限制市场竞争。比如：具有市场支配地位的平台经营者甲，没有正当理由，通过限制链接跳转或者端口接入等方式，导致交易相对人无法开展特定业务、参与市场竞争。

第十三条 限定交易

具有市场支配地位的平台经营者，要避免通过以下方式滥用市场支配地位，没有正当理由，限定交易相对人只能与其或其指定的经营者进行交易，或者不能与特定经营者进行交易，排除、限制市场竞争：

（一）在商家入驻、平台服务、内容发布、应用开发等平台规则中设置独家合作条款，要求平台内经营者只能与本平台合作，或者只能将特定商品、内容在本平台发布；

（二）通过活动规则、合作协议、站内通知等，要求平台内经营者不能与特定竞争性平台合作，或者不能参与特定竞争性平台的促销活动；

（三）通过屏蔽店铺、搜索降权、流量限制、技术障碍、扣取保证金、罚款、取消参加促销活动资格、拖延上线、差别费率、延迟账期、降低评分等级等惩罚性措施实施限制；

（四）通过补贴、折扣、优惠、流量资源支持、赠送增值服务、提高评分等级等激励性措施变相实施限制。

风险示例：“二选一”行为

具有市场支配地位的平台经营者，滥用市场支配地位，没有正当理由，强迫交易相对人在该平台经营者和其他竞争性平台经营者间作出选择，并通过惩罚性措施或者激励性措施保障实施前述“二选一”行为，排除、限制市场竞争。比如：具有市场支配地位的平台经营者甲，没有正当理由，要求平台内经营者承诺不与竞争性平台开展合作，并对不遵守承诺的平台内经营者采取搜索降权、下架商品、限制流量、扣取保证金等方式予以惩戒，限制

平台内经营者自由选择权，产生了排除、限制市场竞争的效果。

第十四条 搭售或者附加其他不合理条件

具有市场支配地位的平台经营者，要避免通过以下方式滥用市场支配地位，没有正当理由，搭售或者附加其他不合理交易条件，排除、限制市场竞争：

（一）利用难以选择、更改、拒绝的格式条款、弹窗、操作必经步骤等，要求平台内经营者、消费者在使用其服务时，必须搭配使用指定商品；

（二）通过采取搜索降权、流量限制、技术障碍、关停服务、取消授权等惩罚性措施，强制平台内经营者、消费者等接受其他商品；

（三）强制或者变相强制平台内经营者、消费者等参加推广、促销、优惠活动，接受不合理的撮合价格，或者承担应当由平台经营者承担的费用、风险等；

（四）对交易条件和方式、服务提供方式、付款方式和手段、售后服务等附加不合理的限制；

（五）在交易价格之外强制收取未经明确公示的技术服务费、流量推广费等不合理费用，或者通过重复收费等收取交易价格之外的不合理费用；

（六）强制收集非必要的用户信息或者附加与交易标的无关的交易条件、交易流程、服务项目。

风险示例：“全网最低价”

具有市场支配地位的平台经营者，滥用市场支配地位，没有正当理由，要求平台内经营者向其提供全网最低价格，排除、限制市场竞争。比如：具有市场支配地位的平台经营者甲，没有正当理由，要求平台内经营者在该平台销售的商品价格不得高于其他竞争性平台，若在其他平台降价，须在甲平台内降价至相同或者更低水平，并采取措施确保相关要求的执行，产生排除、限制竞争的效果。

不具有市场支配地位的平台经营者，要求平台内经营者在商品价格、数量等方面向其提供等于或者优于竞争性平台的交易条件，可能构成垄断协议。

第十五条 差别待遇

具有市场支配地位的平台经营者，要避免通过

以下方式滥用市场支配地位，没有正当理由，对交易条件相同的平台内经营者、消费者等交易相对人实施差别待遇，排除、限制市场竞争：

（一）对商品类别、订单数量、评分等级等交易条件相同的交易相对人，在进入平台、收取费用、营销推广等方面实行差异性标准、规则、算法；

（二）基于用户偏好、交易历史、终端设备、使用习惯等数据，利用支付能力、用户黏性、价格敏感度等分析算法，实行差异性交易价格、付款条件、交易方式等。

前款所称交易条件相同，是指交易相对人之间在交易安全、交易成本、信用状况、所处交易环节、交易持续时间等方面不存在实质性影响交易的差别。平台经营者在交易中获取的交易相对人的隐私信息、交易历史、个体偏好、消费习惯等方面存在的差异不影响认定交易相对人条件相同。

风险示例：平台差别待遇

具有市场支配地位的平台经营者，滥用市场支配地位，没有正当理由，对交易条件相同的平台内经营者、消费者等交易相对人，实施价格、政策等方面的差别待遇，排除、限制市场竞争。比如：平台经营者甲具有市场支配地位，没有正当理由，对规模、商品、信用等方面交易条件均相同的平台内经营者，按明显不同的抽佣比例收取佣金，产生排除、限制市场竞争的效果。

第十六条 正当理由

平台经营者在评估是否具有本指引第十一条至第十五条规定的正当理由时，可以考虑以下因素：

（一）在合理期限内，为发展平台内其他业务、为促进新商品进入市场、开展促销活动等；

（二）符合公平、合理、无歧视的平台规则，或者为防止平台经济领域经营者利益发生不当减损；

（三）为保护交易相对人、消费者、从业人员合法权益或者维护合理的经营模式所必需；

（四）符合正当的行业惯例和交易习惯，或者为提升商品使用价值或者效率所必需；

（五）为保护知识产权、商业秘密、个人信息

或者针对交易进行的特定资源投入所必需；

(六)为保护交易安全、数据安全或者网络安全所必需；

(七)存在不可抗力等客观因素；

(八)能够证明行为具有正当性的其他理由。

与竞争性平台经营者做法一致、顺应消费趋势、保护市场价格稳定性、维持平台生态整体性等理由一般不属于本指引第十一条至第十五条规定的正当理由。

第三节 经营者集中

经营者集中包括以下情形：(一)经营者合并；

(二)经营者通过取得股权或者资产的方式取得对其他经营者的控制权；(三)经营者通过合同等方式取得对其他经营者的控制权或者能够对其他经营者施加决定性影响。

第十七条 经营者集中申报

经营者集中达到《国务院关于经营者集中申报标准的规定》的申报标准的，经营者应当事先向国务院反垄断执法机构申报，未申报的不得实施集中。对于违法实施经营者集中的，国务院反垄断执法机构将依法进行处理。

第十八条 经营者集中合规

平台经营者可以参考《经营者反垄断合规指南》《经营者集中反垄断合规指引》，识别、评估和管控经营者集中反垄断合规风险，避免具有或者可能具有排除、限制竞争效果的经营者集中，防范因违法实施集中承担法律责任。

第四节 滥用行政权力排除、限制竞争

《反垄断法》禁止行政机关和法律、法规授权的具有管理公共事务职能的组织(以下称行政主体)滥用行政权力排除、限制竞争。平台经营者可以参考《关于平台经济领域的反垄断指南》，避免主动或者被动在行政主体协调、推动或者要求下从事垄断行为。平台经营者认为行政机关滥用行政权力排除、限制竞争的，可以向反垄断执法机构举报，或者依法向行政复议机关提出行政复议申请。

第十九条 行政主体协调、推动的垄断行为

平台经营者要避免主动参与行政主体协调或

者推动的《反垄断法》禁止的垄断行为，或者利用与行政主体签订合作协议、备忘录等实施垄断行为。

第二十条 行政主体要求的垄断行为

平台经营者收到行政主体要求执行的办法、决定、公告、通知、意见、函件、会议纪要等文件时，要重点关注文件内容是否存在反垄断合规风险，存在风险的，必要时向反垄断执法机构反映。

第三章 风险管理

第二十一条 风险评估

平台经营者可以根据所处行业特点和市场竞争状况，结合自身经营规模、商业模式等因素，建立风险评估指标体系，全面评估反垄断合规风险。鼓励平台经营者基于风险评估施行分类分级管理，对不同类别、等级的风险采取不同措施。

第二十二条 风险提醒

鼓励平台经营者对员工施行分岗分级提醒，根据不同岗位、级别和工作范围的员工所面临的不同风险，针对性开展风险提醒。重点做好以下人员的风险提醒：

(一)法定代表人、董事、高级管理人员；

(二)主要业务负责人、新业务负责人；

(三)可能与竞争性平台经营者或者上下游经营者接触的人员；

(四)负责销售、采购、价格和商务政策制定、并购管理、销售网络管理以及联络行业协会等事项的部门中知晓竞争性敏感信息的人员；

(五)曾为竞争性平台经营者工作可能知晓其竞争性敏感信息的人员；

(六)负责企业并购项目的人员；

(七)其他反垄断合规高风险人员。

第二十三条 事前风险防控

平台经营者可以在制定规则、设计算法、签订协议、商业洽谈、投资并购、调整业务模式、组织营销活动等重要事项前，对有关事项进行反垄断风险识别评估，并依据本指引第二十二条进行风险提醒。

第二十四条 事中风险防控

平台经营者在经营过程中要根据法律法规、行

业情况、市场结构、业务布局等发生的变化，及时更新风险评估指标体系，重新评估反垄断合规风险，提出关于平台经营者风险防控工作的合规建议。

第二十五条 事后风险防控

平台经营者可以在营销活动、投资交易、商贸合作等完成结束后对反垄断合规风险进行复盘，提出关于加强和改进自身风险防控工作的反馈意见，防范化解反垄断合规风险。

第二十六条 平台规则审查

平台经营者可以重点对账户管理规则、终端用户政策、平台内经营者协议和管理办法、第三方服务商合作协议、流量分配规则、促销活动政策等平台规则进行全量审查，避免发生反垄断合规风险。

第二十七条 算法筛查

平台经营者可以对互联网平台内使用的各类计价算法、推荐系统、排序逻辑、广告投放策略等核心算法模型进行定向筛查和动态监测，重点关注是否存在歧视性设计、不公平交易导向、价格过度调整、统一定价推送、策略性算法共享等问题，避免发生反垄断合规风险。

鼓励平台经营者通过技术手段与人工复核相结合的方式，确保算法逻辑透明可解释，避免算法黑箱破坏市场竞争秩序、损害消费者利益和社会公共利益。鼓励平台经营者建立算法迭代纠偏机制，发现风险后及时下线调整相关算法，并留存完整审计记录。

第二十八条 配合调查

平台经营者及其员工、平台内经营者要配合反垄断执法机构的调查，如实提供反垄断执法机构要求提交的证据材料，避免以下拒绝或者阻碍调查的行为：

- (一) 拒绝、阻碍执法人员进入经营场所；
- (二) 拒绝提供相关文件资料、信息或者其获取权限；
- (三) 拒绝回答问题；
- (四) 隐匿、销毁、转移证据；
- (五) 提供误导性信息或者虚假信息；
- (六) 其他拒绝、阻碍反垄断调查的行为。

第二十九条 合规整改

平台经营者按照《提醒敦促函》《约谈通知书》《立案调查通知书》《行政处罚决定书》等反垄断“三书一函”要求进行整改的，要注意及时提交整改方案，有序推进整改工作，按时提交整改报告。平台经营者可以采取适当方式对整改效果进行评估，持续完善合规管理制度、改进合规管理体系。

平台经营者可以主动向社会公开整改措施和成效，接受监督。

第三十条 合规激励

平台经营者要建立完善的反垄断合规管理制度，并真实、有效实施。平台经营者遇到反垄断调查时，可以依据《经营者反垄断合规指南》规定，向反垄断执法机构申请合规激励。反垄断执法机构可以依法酌情考虑平台经营者反垄断合规制度的建设实施情况，给予必要合规激励。

第四章 合规保障机制

第三十一条 合规管理机构

反垄断合规管理机构负责统筹、组织和推进反垄断合规管理工作，可以专设，也可以由有关部门承担相应职责。鼓励平台经营者为合规管理机构独立履职提供必要的资源，保障反垄断合规管理有效实施。鼓励平台经营者设立首席合规官。

平台经营者总部可以要求分公司、控股子公司等配合开展风险排查、举报调查、监督检查和问题整改等反垄断合规管理工作。

第三十二条 合规汇报

鼓励平台经营者建立反垄断合规汇报机制，由反垄断合规管理负责人听取合规管理牵头部门报告合规管理落实情况和合规风险，并定期向平台经营者主要负责人汇报反垄断合规管理情况，及时报告反垄断合规重大风险。合规管理牵头部门可以组织业务以及职能部门汇报本部门的反垄断合规工作情况和合规风险。

鼓励平台经营者总部定期听取分公司、控股子公司等合规管理牵头部门汇报反垄断合规管理落实情况和重大风险，收集反垄断合规管理工作所需的资料和信息，及时掌握合规风险事项。

第三十三条 合规培训

鼓励平台经营者投入有效资源,建立反垄断合规培训机制,将反垄断合规培训纳入员工培训计划和常态化合规培训机制,结合不同岗位的合规管理要求针对性地开展培训。鼓励平台经营者建立合规培训台账,结合反垄断法相关规定及时更新培训内容,定期评估培训效果。

第三十四条 合规考核

鼓励平台经营者建立健全反垄断合规人事考核以及奖惩机制,将考核结果作为员工及其所属部门绩效考核的重要依据,激励和督促员工自觉遵守反垄断合规管理要求。对于考核结果不合格、涉及投诉举报的人员或者部门,采取相应纠正整改措施。

平台经营者总部可以对分公司、控股子公司等反垄断合规管理工作进行考评和指导。

第三十五条 合规监督

鼓励平台经营者建立反垄断合规举报处理和反馈机制,积极响应员工、平台内经营者、消费者、从业人员等的反垄断合规投诉和举报,并组织开展核查。

鼓励平台经营者建立平台内经营者、消费者、从业人员等平台用户以及独立第三方等的外部评

价机制,自觉接受社会监督,不断完善平台治理规则。

第三十六条 合规管理信息化

鼓励平台经营者加强合规管理信息化建设,将合规要求和风险防控机制嵌入业务信息化流程,支持业务以及职能部门对本部门日常工作开展信息化合规管理,强化对经营管理行为合规情况的过程管控和运行分析,记录和保存相关信息,提高合规工作效率。

第五章 附则

第三十七条 指引的效力

本指引是关于互联网平台的专项反垄断合规指引,旨在对平台经营者反垄断合规提供一般性指引,不具有强制性。

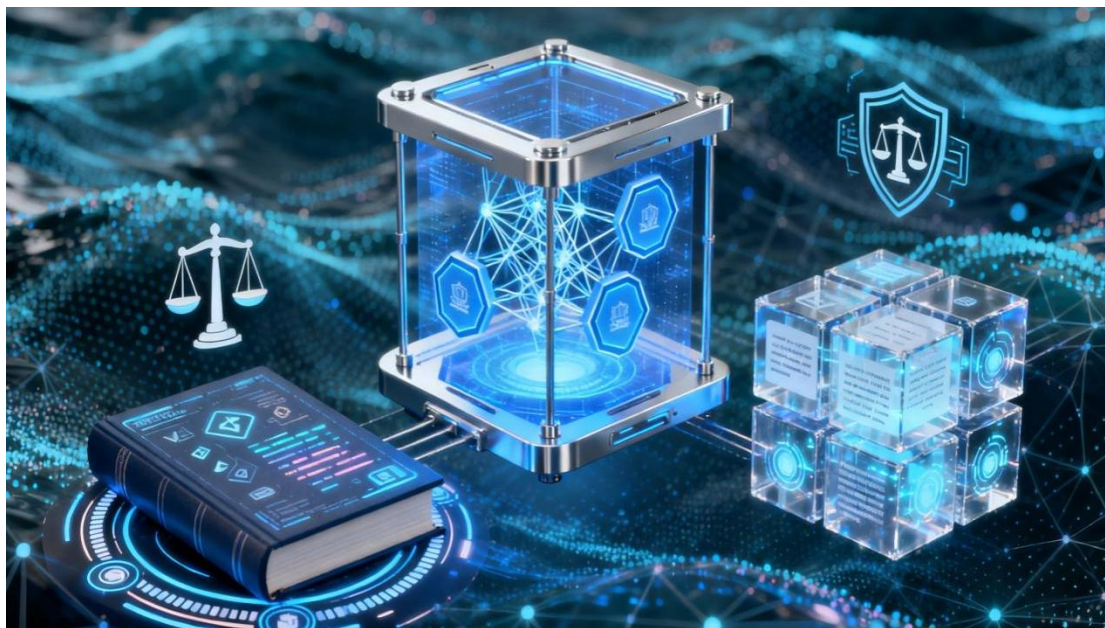
平台经营者、有关行业协会可以参考本指引,根据反垄断法律法规规章指南等的规定,结合自身特点,建立健全反垄断合规制度,优化合规工作体系。

第三十八条 指引的解释

本指引由市场监管总局负责解释。

(技术编辑:来唯希)

研究动态



个人信息保护

1、也论个人信息权的道德证成:理由之重构(黄圆胜)

来源:《法制与社会发展》2026年第1期

在法律层面证成个人信息权,虽然有助于描述个人信息权的法律性质,却难以揭示其背后的价值来源。权利模式的反对者因而批评个人信息权只是保护了权利人的意志或利益,与公共利益并无任何概念关联。要想强有力地批判权利模式的反对者,就必须在道德层面证成个人信息权,揭示其共同善面相。为更好地完成这一工作,应在理论逻辑上依据拉兹的弱版本的共同善权利观,在方法论上采纳阿隆·哈勒尔的内在/外在理由的二分证成框架,明确个人信息权属于一般人格权的衍生权利。在内在理由方面,将弱至善主义的自治作为内在理由,能够更好地突出国家促进个人信息自治的辅助性义务。在外在理由方面,将自由公共文化和情境关联价值作为外在理由,能够更好地说明辩护个人信息权保护强度的共同善理由。经由这种证成理由之重构,个人信息权的最佳道德证成才是可能的。

2、数字行为痕迹数据保护的刑法展开(赵拥军)

来源:《法学论坛》2026年第1期

数字行为痕迹数据与个人信息之间不是相互包容关系而是交叉关系。数字行为痕迹数据从生成及价值角度划分,可分为原生型和衍生型,以及是否可作为数据资源持有的数字行为痕迹数据。可作为数据资源持有的数字行为痕迹数据不可能是原生型而只能存在于衍生型的数据中。对于数字行为痕迹数据的刑法保护,应认可并赋予其独立的“客体”属性地位,从一种数据资源的视角出发,通过原生型与衍生型以及是否可作为数据资源持有而划定不同类型的动态分层进行,确保其作为数据资源的流通利用与刑法保护之间的价值平衡,以凸显数字行为痕迹数据的独立属性,最大限度地对其数据资源的实质角色进行开发利用并实现价值。

3、论已公开个人信息的保护模式(边琪)

来源:《东方法学》2025年第6期

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”。

4、“知情同意”与侵犯公民个人信息罪的出罪机制（姚万勤）

来源：《东方法学》2025年第6期

为了保护个人信息不被滥用，《个人信息保护法》确立了“知情同意”作为处理个人信息的核心原则。既然前置法中的“知情同意”作为他人责任豁免的重要事由，在刑法中也应当积极承认其免责效果。虽然通说将其视为阻却违法性事由，但是目前将被害人承诺作为排除构成要件符合性事由加以看待的见解越来越有力，应当重新赋予其作为出罪事由的体系性地位。因此，处理经过他人同意的个人信息数据，因不符合构成要件符合性而予以出罪。对于已经公开的个人信息，不仅需要理论中确定“已公开”“合理处理”等语词的规范含义，而且还需要通过推定的同意理论对其予以出罪。

5、算法正义的法理基础及制度实现（罗有成）

来源：《法商研究》2026年第1期

算法正义指为算法时代人与人之间的关系提供一种良好安排的价值原则。算法正义的提出，源于算法背后不同主体之间的利益冲突，目标在于划定算法参与决策的正当边界。在算法时代背景下，正义本质并未发生根本改变，但正义的内容在算法深度

介入条件下呈现出新的内涵。因此，算法正义是对传统正义理论的一种时代性拓展。算法正义的内容包括数据分配正义、算法程序公平、人机关系和谐与可行能力保障四个方面。实现算法正义，应基于算法正义的上述内容，从公平分配数据权益、确立算法正当程序、构建和谐人机关系以及提升数字可行能力方面作出相应制度安排。

6、人工智能背景下个人信息保护制度的挑战与应对（丁晓东）

来源：《政治与法律》2026年第1期

人工智能对个人信息保护制度提出了一系列挑战。究其根源，个人信息保护制度起源于档案化个人信息时代，其针对的典型场景是行政机关低频处理少量档案类个人信息。在以互联网与信息技术为代表的前人工智能时代，个人信息处理的典型场景就已经转换为企业高频处理大规模行为类个人信息。在人工智能背景下，个人信息处理的典型场景进一步演化为海量个人信息的融合汇聚型处理，其对数据的处理类似水库对海量水滴的汇聚与融合利用。人工智能背景下的个人信息保护原理与制度应当与人工智能处理的典型场景对齐，其原则应从静态预防迈向动态发展思维，从激化对抗迈向信任互惠，从个体主义迈向群体主义。在此基础上，其具体制度模块也应进行相应调整与重构。人工智能处理个人信息应成为个人信息保护制度改革的试验田，个人信息保护的一般原理与制度也应借机进行改革与完善。

7、个人信息侵权损害赔偿酌定规则的反思与重构（李喜莲）

来源：《政治与法律》2026年第1期

在个人信息侵权纠纷中，酌定损害赔偿已成为法院裁判的主要路径。然而，我国实践中法院适用这一规则仍面临着损害范围窄、酌定尺度不一和酌定说理不清等难题。这主要是由于，传统侵权法中的损害填平原则与新型数字权益保护需求之间存在张力，非物质损害难以纳入酌定赔偿的范围；《民法

典》与《个人信息保护法》在个人信息保护上存在竞合，法院尚未形成清晰的法律适用顺位，在缺乏具体酌定规则的背景下，裁判过程常面临价值排序与利益平衡的双重考验；加之酌定赔偿尚无适配的程序规则，其在程序法上的行为性质尚不明晰。要破解这些难题，需从实体与程序协同改革切入。在实体法层面，应在厘清个人信息权属的基础上，将实质性风险损害纳入法院酌定赔偿的范围；针对不同类型的个人信息和不同侵权行为，可以建构分类分层的动态酌定赔偿标准，使法院酌定有法可依。在程序法层面，应强化信息主体的初步证据提出义务，在降低证明标准的同时保持必要的证明责任约束，并强化法院对酌定赔偿的说理义务。

8、刑事在线庭审证人个人信息保护的程序论（自正法）

来源：《法律科学（西北政法大学学报）》2026年第1期

目前刑事在线庭审对证人的个人信息保护主要有三种模式，即严格保护模式、相对保护模式和开放保护模式。实践中对证人个人信息的保护主要以开放保护模式为主，严格保护和相对保护模式为辅。然而，以开放保护为主的刑事在线庭审模式容易侵犯证人个人信息权益，而加强对证人个人信息保护又会妨碍被告人对质权的行使，且证人在线身份识别与个人信息保护之间存在一定冲突，这些问题在一定程度上加剧了刑事在线庭审与证人个人信息保护之间的紧张关系。未来我国刑事在线庭审证人个人信息保护制度的构建，可依据横向与纵向程序构造相结合的原理，确立以相对保护为主的证人个人信息保护模式，并通过程序设计以及细化证人在线出庭规则等一系列程序构造来缓解证人在线身份识别与个人信息保护之间的紧张关系。

9、法定职责作为国家机关处理个人信息的边界（郑春燕）

来源：《中外法学》2025年第6期

《个人信息保护法》为国家机关确立了“告知同意”

规则的豁免适用条件——“法定职责”和配套的必要性原则。借鉴个人信息权益的基础性权能与工具性权能的二分法，可将个人信息处理行为区分为核心信息处理行为与辅助信息处理行为。对于核心信息处理行为，“法定职责”中的“法”应限定为规章以上的规范性文件，且必须明确授权；对于辅助信息处理行为，在上位法已经授予核心信息处理权限的前提下，“法”的范围可扩展至所有合法规范，且无需明确授权。此外，应承认创设对等权利的行政协议和组织规范前提下的行政惯例，作为职责来源的补充。鉴于数字化改革推进的整体政府进程，必要性原则的适用不应局限于静态的“最小化”，而应根据公共数据收集、共享与开放的阶段特征，结合个人信息处理活动对信息权益的具体影响，构建起情境化的必要性原则内涵，以实现职责履行与个人信息权益之间的动态平衡。

10、个人信息权益与数据产权的关系释论（王年）

来源：《法学家》2025年第6期

个人信息权益与数据产权关系阐释的前提是在承认人格利益专属个人的基础上明确个人数据财产利益的归属。个人数据财产利益由数据主体与处理者共同生成，并分别形成纵向和横向共生关系。基于个人数据财产利益的“共生理理”，数据主体与数据处理者之间的关系应从“对立竞争”转向“双向依赖”，权益位阶应从“绝对优先”转向“同步生成”，调整模式应从“排他赋权”转向“治理规范”。由此，个人信息权益与数据产权是将个人数据的不同利用权能分别赋予数据主体与处理者形成的两项平行权利。数据主体可通过个人信息权益实现个人数据财产利益的管理，数据处理者则因合法处理行为享有包括持有、使用权、经营权等在内的数据产权。针对个人信息权益与数据产权的冲突，一方面应通过限缩同意撤回权的适用条件、细化删除规则并引入匿名化替代机制，协调数据未转移时的冲突；另一方面可依据转移目的合法性约束转移权行使，并以处理方式实质性变化或特别约定作为目的变更认定标准，协调数据转移时的冲突。

人工智能法治

1、风险与危险区分下的人工智能治理（林涓民）

来源：《比较法研究》2025年第6期

风险与危险在人工智能治理中常被混用，引起法律适用的混乱。风险是抽象的、延迟的与不确定的，往往与收益并存；危险则是一种具体、紧迫与相对确定的威胁，对应明显的不利益。人工智能风险活动应借助行政法中的风险预防机制予以调整，具体包括容错与纠错模式下的风险评估规则、促进多系统沟通的风险交流规则以及作为授权基础的实验主义治理制度等。风险本身并不构成侵权法意义上的损害，只有当风险转化为危险与损害时，才有侵权法适用的空间。人工智能侵权原则上应适用过错归责，只是可通过证据开示、特殊的因果关系推定等规则平衡两造之间的诉讼力量。风险在概念内涵与治理机制方面均与危险有所不同，侵权行为符合监管沙箱、真实测试等法律实验要求的，并不当然产生民事责任减免效力。

2、全球人工智能立法的重要关切与未来趋向（支振锋）

来源：《比较法研究》2025年第6期

人工智能技术的特殊性，使得人工智能立法也具有极大的特殊性。从世界各国的立法实践来看，人工智能立法呈现出讨论热烈但行动审慎，风险规制是关注焦点但发展促进才是立法重心的悖论性特征。目前世界各国多就人工智能某个领域的具体问题，出台问题导向的专项立法，而且立法层级一般较低。制定并通过人工智能综合性统一立法的国家或地区，仍为极少数。这种状况既体现了人工智能作为颠覆性技术的重大影响，也彰显了国家战略博弈的理性选择。鉴于人工智能技术和产业对国家竞争力可能具有的关键性作用，各国在推进人工智能立法时既要统筹发展与安全，也要协调国内与国际。在全面把握人工智能技术和产业发展状况之前，各国在出台人工智能国家层面综合性统一立法上，仍将呈现出“探索积极、立法审慎”的姿态，尤其会

着眼于国际竞争的整体背景，重视立法的国内外影响。作为人工智能技术和应用领先的大国，中国的人工智能立法立足本国实际，坚持问题导向，秉持人类命运共同体理念，推动全球人工智能治理，体现出显著优势。

3、构建风险分级导向的人工智能系统备案制度（郭雨婷）

来源：《东方法学》2025年第6期

算法透明治理的需要催生了我国算法备案制度。要确保算法备案制度真正落地生根，不仅需要坚实的理论基础作为支撑，更需要回归备案文本进行实践反思，优化制度设计。算法备案制度已实现了生成合成类算法的独立以及检索过滤类算法的拆分两大重要转变，但是目前类型化的算法备案制度面临类型难以界分、与生成式人工智能备案范围的重叠以及备案信息质量难以保障的治理难题。对此，未来我国应以风险为导向，从类型化算法备案逐步转向风险分级人工智能系统备案，并基于包容审慎的监管理念制定一套科学、合理的运行机制，包括完善备案填报指导机制、健全备案审核与责任机制、实行备案继承机制等，以保障备案制度良好运行。

4、大语言模型开发应用中作品使用法定许可制度研究（程迈）

来源：《政治与法律》2026年第1期

大语言模型的开发应用需要利用大量作品。这些利用行为在对作者财产与人身权益造成侵权风险的同时，也在挤压作者群体的经济与艺术生存空间，使得作者群体处于不利境地。目前的法律制度在应对这些侵权风险、保护作者利益方面存在着规范供给短缺、调整方案解释力不足的情况。作品对于大语言模型的完善与提高具有重要的科研、经济、社会乃至文化价值。大语言模型能够充分利用大量优秀作品、新作品，不仅事关大语言模型技术提高，而且事关人类社会持续健康发展。为了打通目前制约大语言模型合法利用作品的法律制度堵点，应以促进作者权益实现与作品使用成本内化为原则，扩

展著作权法中的作品使用法定许可制度，引入侵权争议首问最终用户原则，针对营利型大语言模型开发应用方设置特别企业所得税，降低作者个人所得税率并设立出版资助基金，以将大语言模型开发应用中的红利反哺作者群体。

5、人工智能时代创作风格的价值重勘与著作权制度因应（代晓焜）

来源：《法学研究》2026年第1期

将创作风格长期不受著作权法保护的原因归于“思想与表达二分”框架，是对著作权法治理逻辑的误读。创作风格的“思想”标签根植于自然人之间市场替代性有限、正外部性显著的学习模仿范式，服务于著作权法平衡私权激励与创作自由的规范功能。人工智能技术的介入打破了创作风格之上固有的利益平衡结构。在财产维度，创作风格由依附于作品载体的审美要素，嬗变为具有稀缺性与独立交易价值的“数字生产资料”，其衍生利益亟待合理分配。在人格维度，创作风格由“创作者人格的符号存在”矮化为被批量调用、任意改造的参数代码，引发创作者人格尊严与创作主体性的时代危机。著作权制度既有“不予干预”的治理立场难以适配人机协作的实践语境。应回归著作权法激励创新和以人为本的价值本位，为创作风格构建以单纯获酬权为核心的利益分配机制，矫正因技术变革导致的结构性利益失衡，为人工智能时代健康、可持续的创作生态提供制度保障。

6、人工智能强制责任保险的法律构造——以智能驾驶为例（齐萌）

来源：《东方法学》2025年第6期

在人工智能应用模式下，传统保险产品的算法与网络安全风险被显著放大，打破了多元主体参与下的责任划分格局，导致受害人获取证据的难度持续攀升。人工智能强制责任保险以“强制投保”为核心机制，能够有效化解受害人“举证难”与“损失获赔”之间的核心矛盾，且具备坚实的理论支撑：国家干预理论为强制责任保险的介入提供正当性基

础，科斯定理所倡导的“社会总成本最小化”理念与强制责任保险保障消费者的目标高度契合，汉德公式的引入为保险制度中的风险评估、责任界定提供客观量化的依据。人工智能强制责任保险的构建需从三方面精准发力：内容设计上，以“产品责任风险”与“网络安全风险”为双重核心；技术支撑上，依托“黑匣子技术”实现算法过程的可追溯，结合“多模态融合识别技术”提升风险监测与定损的精准度，为保险理赔提供技术赋能；程序构建上，建立“过错推定原则+人工智能司法鉴定”的联合认定机制的同时，不断健全保险公司的追偿权制度。

7、生成式人工智能背景下作品风格的著作权保护（姚叶）

来源：《清华法学》2025年第6期

风格长久以来被视为“思想”而不受著作权法保护，但生成式人工智能的“风格迁移”技术挑战了这一传统观念。追溯艺术学基本原理，可以发现风格是所有作品的构成要素，是作者“个性”的客观表现。所有“可版权性表达”均为“表现”，但并非所有表现均受著作权法保护，何种表现可以构成可版权性表达体现了法律的政策考量并受到技术的限制。生成式人工智能发掘了作品数据的集聚价值，能够快速从作品中习得风格的默会知识，在技术上以风格损失函数的方式实现了风格的确定性、可分性与可复制性，使风格具有可版权性。应在此基础上划定风格的保护范围，厘定风格的保护环境和条件，明确风格合法使用的边界。

8、论作为新型邻接权的人工智能生成内容创作者权（焦和平）

来源：《法商研究》2026年第1期

人工智能在内容创作领域的深度介入，改变了知识产品由自然人创作的传统方式。人工智能生成内容作为新型知识产品，将其纳入财产范围具有正当性。但作为一种新型的财产权客体，将其纳入传统的财产法保护范畴存在障碍。考虑到知识产权客体

的包容性与知识产权法体系本身的变迁性，应当在知识产权制度框架下寻求合适的人工智能生成内容的财产法保护方案。囿于专门立法模式的弊端，著作权客体二分体系下的制度设计能够为人工智能生成内容提供充分保护。具体来说，将人工智能生成内容纳入邻接权体系，并设立作为新型邻接权的人工智能生成内容制作者权，不失为一种合理方案。该权利的客体为缺乏人格性且不具有独创性的人工智能生成内容，主体为人工智能使用者；权能仅配置财产权而不设立人身权，权利限制可从保护期限和公共利益两个维度设定。

9、人工智能生成内容的阶梯式保护体系（孙靖洲）

来源：《法商研究》2026年第1期

人工智能正逐步嵌入文化创作的各个场景和环节，其协同创作范式与规模化生产机制正在重塑内容产业的生产方式与组织结构，并使人工智能生成内容的经济价值与人类创造力之间的内在关联日趋弱化，传统著作权制度显然难以有效应对这一变革。赋予人工智能生成内容以特殊保护形式，可与著作权制度共同构建起阶梯式的创意内容保护体系，形成以人类创造性劳动参与程度为依据的差异化激励机制，在鼓励技术投资的同时，确保人类创造力的制度优先地位。在建立与著作权“强弱有别、获取难易程度不同”的权利类型的基础上，还需通过权利克减、开放许可与“安全港规则”等机制实现权利与责任的再分配，进而引导技术向善，保障公众在文化资源获取与数字收益分配中的基本权利，为人类创造力与“机器创造力”的协同共进奠定制度基础。

10、人工智能法律主体问题的法理辨析（支振锋）

来源：《法律科学(西北政法大学学报)》2026年第1期

可否赋予人工智能法律主体地位，是一个学术界颇为重视但又存在理论争议的问题。法律主体是权利的享有者、义务的承担者，必须符合特定的条件。在法律史上，法律主体的范围的确存在过混乱，对

法律主体的认知曾似是而非。但随着理性化、世俗化和现代化的发展，法律主体逐渐呈现出以人类为中心的纯净化的特点，体现为自由意志、有限实体和可社会性三者有机统一的理论框架。只有人类或由人类结成的特定组织，才有可能成为法律主体。通过梳理人工智能领域的权威科学文献，人工智能发展的技术路线，当前主流大语言模型的技术方案，可以发现，人工智能没有自由意志，不具备有限实体，也不可能结成可作为社会有机体的组织。赋予人工智能法律主体地位既不符合基本法理，也不具备实践上的可能性。

11、渐进式法律人格理论与人工智能体的部分权利能力（申卫星、鲍伊帆）

来源：《华东政法大学学报》2026年第1期

基于功能主义意志理论，人工智能体已在一定程度上具备自由意志，其功能表现亦逐步超越传统工具属性。有限认可人工智能体的法律人格，对于实现利益的合理配置与填补责任归属中的制度空缺具有重要意义。回顾民事主体制度的历史演进，可以观察到主体概念由“人可非人”发展至“人皆为人”，并进一步延伸至“非人亦可为人”，呈现出历时性与共时性的双重渐进式特征。作为对传统“人—物”二分范式的修正，渐进式法律人格理论强调法律人格并非不可分割的先验资格，而可依据功能与风险结构作层级化配置，其认定标准由自然属性导向转向功能主义导向。人工智能体的法律地位应结合意思能力与系统功能水平作综合判断。当人工智能体能够理性形成意思表示，并在感知、决策与执行等方面达到较高的功能成熟度时，可在与其自主性程度相匹配的范围内赋予有限法律人格，使其在特定范围内具备有限的权利能力和责任能力。同时，要通过领域限定与外部监督对其行权范围加以约束。

12、人工智能提供者的产品责任（曹建峰）

来源：《法律科学(西北政法大学学报)》2026年第1期

随着对AI系统的控制权日益从使用者转向提供者，

AI 提供者的责任问题已成为 AI 侵权责任制度讨论的核心议题。作为最低成本的事后规避者，提供者应对其开发、提供的 AI 系统因存在缺陷而造成的损害承担侵权责任。为此，有必要构建人工智能产品责任规则：一是革新产品概念，将软件、AI 系统等数字化产品纳入产品责任法；二是扩大可赔偿损害范围，涵盖心理健康损害、数据损害、精神性人格权损害等；三是以合理算法标准取代传统缺陷认定模式，并以上市后监测义务等作为辅助规则；四是排除发展风险抗辩，建立算法解释与信息获取等程序性保障机制。总体而言，以产品责任视角来构建 AI 监管框架，是减轻 AI 风险和救济 AI 损害最有前景的方法，有助于激励安全创新，强化消费者保护，促进人工智能产业健康发展。

13、人工智能生成发明创造的可专利性及其权利归属（詹映）

来源：《法律科学（西北政法大学学报）》2026 年第 1 期

人工智能生成发明创造是指人工智能对发明成果作出了实质性贡献的发明创造，包括“人机协作生成发明”和“AI 主导生成发明”两类。人工智能生成发明创造的可专利性审查应聚焦人类而非人工智能的实质性贡献。人工智能生成发明创造具备可专利性的前提条件是人类对发明成果作出了实质性贡献。人类实质性贡献的判定，应遵循创造性贡献、人类主导性等基本原则，并结合不同的人工智能应用场景进行具体分析。多数场景下，有资格成为发明人的是人工智能系统的使用者，特殊场景下也可能包括人工智能系统的开发者。无论现在还是未来，专利制度都无须赋予人工智能发明人身份。在人工智能生成发明创造中，一旦确认了人类的实质性贡献，就可以依据人类贡献程度确定发明创造的发明人，并以发明人为中心，按照法律规定或合同约定确定专利权归属。

14. 人工智能介入语境下的司法公信力研究——基于认知实验的考察（林喜芬）

来源：《政法论坛》2026 年第 1 期

评估人工智能介入语境下的司法公信力，有助于厘清民众对司法和技术的认同逻辑与信任关系，为我国数字司法制度建设提供理论支撑。通过采用认知实验方法，让 1 076 名被试者在不同的启动信息条件下对 50 个案例中的商标组进行形式混淆判定。实验数据表明，民众对司法裁判结果有较高的认同度，但人工智能的介入会对其认知过程产生干预。即使法官在裁判中使用了人工智能，民众对司法裁判依然保持较高的信任度，但相较无人工智能介入情景下的司法裁判，信任度有所下降；强调人工智能的辅助定位，可以缓解民众疑虑但效果有限。数字化是司法现代化的趋势之一，未来有必要强化“民众—AI”与“法官—AI”的双向协同：既要着力构建法律领域的垂直大模型，为公众提供更精准的法律服务，防止人工智能介入对司法认同产生负面影响；又要健全人工智能应用的制度体系，规范并保障法官对人工智能的合理运用，增强司法人工智能的信任基础。

15、人工智能国际治理的三重维度 产品责任、伦理价值与国家安全（万方）

来源：《中外法学》2025 年第 6 期

当前人工智能国际治理主要涵盖产品责任、伦理价值与国家安全三个目标维度。欧盟、中国和美国在人工智能国际治理中分别代表了个体权利主导、平衡多元目标与国家安全主导的三种典型路径，不同路径下三个目标维度的追求位阶与制度侧重存在显著差异。全球人工智能治理应以上述三个目标维度为核心，通过制度衔接与规则对话，构建层次分明、协调有序的治理体系。具体而言，应以共同伦理为前提，从产品责任与系统安全入手，通过技术标准、行业规则与合规指引形成基础性共识。在此基础上，逐步推动权利义务具体化的区域性伦理协议和软法工具的形成，培育更高层次的价值认同与制度合作框架。而在涉及国家安全的议题上，则需在人工智能军民两用场景不断深化的背景下，探索建立跨国危机管理与风险沟通机制，以防止因过度

强调人工智能军事化或技术封锁而造成国际共识受阻,从而实现以安全为底线、以合作为导向的全球人工智能国际治理秩序。

16、论人工智能时代肖像可识别性的判断标准（阮神裕）

来源：《法学家》2025年第6期

肖像可识别性要件发挥作用的典型场景,主要集中在争议形象“去面部特征”的肖像权纠纷中。随着人工智能生成虚拟形象的广泛应用,肖像可识别性要件越发凸显其重要性。“综合判断法”过度依赖法官自由裁量权,不仅导致法律适用的不确定性,而且忽视了肖像权所要保护的不同法益对可识别性判断标准的差异化要求,难以成为理想的判断路径。肖像权保护的终局性法益包括尊严利益、同一性利益和财产性利益。针对不同法益,肖像可识别性的判断标准亦应有所区分:在保护尊严利益时,应当采取最为宽松的标准,只要肖像权人本人可以识别即可;在保护同一性利益时,应当以一定范围内的熟人可以确信争议形象只能是肖像权人为准;而在保护财产性利益时,则应当采用最为严格的标准,即在隔离对比的情境中,社会公众能够一眼认出争议形象为肖像权人,由此形成肖像可识别性的多元化判断标准体系。

网络平台监管

1、第二代互联网规则?——从欧盟《数字服务法》看平台责任的未来（丁晓东）

来源：《华东政法大学学报》2026年第1期

欧盟《数字服务法》在域外被视为“第二代互联网规则”的代表,对治理著作权网络侵权、网络暴力、网络谣言等行为具有重要启示。《数字服务法》主要回应避风港规则的不足,对不同平台施加梯级增长内容审查责任,同时对不同平台适用正当程序。

《数字服务法》的洞见在于认识到了平台的公权力特征,但其方案也存在不合理性。欧盟与美国的平台责任制度反映了各自独特政治与法律背景,相较

而言,我国的平台责任制度整体具有合理性,但需要避免过度规制。关于平台责任,应根据不同类型,重构避风港制度、审查责任与正当程序制度。对于平台参与特定个案的第三方侵权,应适用共同侵权制度。对于大规模第三方侵权和违法内容,应按照平台治理的必要性、治理难度、治理代价、治理比较优势、治理善意等判定责任。法律应避免简单将平台视为公权力组织,对其适用正当程序,但法律可以将平台正当程序作为平台治理的信号机制与治理工具。

2、元宇宙平台互操作实现的激励型治理（毕文轩）

来源：《东方法学》2025年第6期

元宇宙作为当前典型的新兴技术领域,具有广泛的商业用途和巨大的经济潜力,但是,缺乏互操作性已然成为桎梏当前元宇宙平台经济进一步发展的主要障碍之一。元宇宙平台在数据结构、数字身份、经济系统及治理模式上与传统平台具有差异,导致其在实现互操作的过程中存在技术标准不足、企业商业利益冲突、用户隐私伦理风险以及治理协作机制缺失等多重困境。建立在以传统竞争法为基础上的命令控制型法律治理模式,无法有效引导元宇宙平台的互操作实施,也难以防范因互操作而可能产生的风险,进而会削弱元宇宙平台互操作的实施效果。基于对提高元宇宙平台互操作规制效率的显性需求、规避互操作信息不对称的隐性需求以及实现互操作良好控制的发展需求的考量,规范元宇宙平台互操作需要引入激励型治理模式。基于分层规制理论从基础设施层、数字要素层和商业生态层分别构造相应的激励治理机制,在更好地发挥出制度功能、激励元宇宙平台互操作的同时,能够对可能引发的激励失灵给予及时的矫正,并构建促进元宇宙平台互操作实现的创新容错机制,形成科学的法律激励结构。

数据确权研究

1、数据权利登记的误区及其矫正（孙清白）

来源：《法制与社会发展》2026年第1期

数据权利登记是破解数据交易难题、推动数据交易规范化的关键。数据权利登记的对象是数据资源持有人、数据加工使用权和数据产品经营权。数据来源者权并非数据权利登记的对象。数据资源持有人、数据加工使用权和数据产品经营权的登记彼此之间并不存在简单的包含与被包含关系。对于数据权利登记的法律效力，需要在区分数据权利取得方式的基础上，进行类型化分析，并在我国现有财产权登记制度框架内寻找解决方案。如果数据权利系原始取得，则数据权利登记可以作为权利人享有数据权利的证明。如果数据权利系继受取得，则需要区分数据转让、数据许可使用和数据服务三种不同数据交易类型的基础上，对数据权利登记的法律效力展开分析。现有财产权登记法律效力体系中的登记证明效力、登记对抗效力和登记生效效力都有应用空间。

2、衍生数据的识别标准与产权配置（申卫星）

来源：《法学研究》2026年第1期

衍生数据是数据处理者在原始数据的基础上，通过深度分析、过滤与提炼整合等处理活动生成的高附加值数据形态，具有显著的经济价值与社会价值。衍生数据构成与原始数据相互独立的新数据，其识别标准是衍生数据产权配置规则得以展开的前置性问题。衍生数据应同时满足实质改变、价值显著增值与不可逆转三重标准。实质改变标准是指衍生数据与原始数据在数据结构、内容或形式等维度存在实质差异；价值增值标准意味着衍生数据的使用价值和交换价值相较原始数据显著提升；不可逆转标准则要求衍生数据无法在经济成本或技术难度的合理范围内通过逆向工程还原为原始数据。衍生数据的产权配置规则可以类推适用民法典第322条，遵循意思自治原则确定权属，在当事人没有约定或约定不明确时，则可基于贡献赋权原则与“数尽其用”原则，由数据处理者享有持有人、使用权和经营权等数据权利。在数据处理者未取得原始数据使用权而实施加工行为的情形，在先权利人有权

依个人信息权益请求权、不当得利返还请求权或侵权损害赔偿请求权获得救济。

3、论个人数据来源者财产权的法律构造（侯跃伟）

来源：《法学论坛》2026年第1期

明确数据来源者的权利内涵及边界，是构建数据产权制度的核心议题之一。当前学界探讨多集中于个人信息保护这一非财产性自决权，而忽视了对其财产性权益的保障。事实上，数据价值并非完全由收集者或加工者创造，其源头亦凝结着数据来源者的劳动贡献。因此，在制度层面确立数据来源者的财产性权利，通过明晰权属，可以有效激励数据供给、促进数据自由流通与价值创造。在实现路径上，相较于依赖个体行使权利的“分散式路径”，我国更适合采用以制度化、集体化方式运作的“集中式路径”，通过数据信托、数字税、数据入股等方式，聚合分散的个体权益，降低大规模数据交易中的协商成本，提升数据来源者的整体议价和维权能力。因数据来源者的财产权并非绝对化，必须同步构建科学的权利限制和公共利益平衡机制，在数据采集、加工、流通等环节，依法对数据来源者财产权加以必要限制，以确保数据在个人权益、商业价值和公共利益之间实现动态平衡。

4、竞争法视域下数据访问制度构建研究（王煜婷）

来源：《法学论坛》2026年第1期

使用互联产品或机器产生的使用数据和在使用在线服务产生的行为数据可以说是数据驱动型市场的重要输入，对此类数据的占有和控制引发了一系列市场失灵的问题。竞争法视域下的数据访问制度旨在确保产品或服务的相关用户能够有权访问他们通过使用产品或服务“共同生成”的数据，从而缓解基于数据的“锁定”效应，促进相关市场的创新和竞争，保障数据的公平获取和使用，并在数据驱动型市场中为“择优竞争”建立新的基准。我国应当建立双轨制的数据访问制度，即在建立全国性数据基本法律制度时确立对数据的一般访问权，同时结合不同行业使用数据、不同种类数据、不同数

据主体等多样化因素，再制定具体的定制化数据访问规则。数据访问制度应兼顾多元利益平衡，创设可放弃的数据访问、使用和可携性权利。强化独立数据中介商作用，进一步补充、完善数据访问制度。

5、企业产权同等化保护的刑法要义（孙万怀）

来源：《法学》2025年第12期

同责同罪同罚以平等为基础。基本自由是平等产生的前提，机会均等是平等实现的核心，差异原则则是防止平等最终被消解的保障，也是同责的具象表达。司法机关在追求平等的氛围下，所要寻找的规则就是如何公正处理个体所遇到的“运气”，在此框架之内确认或保证个体的道德责任和社会义务能够公正表达。经营主体地位以主体意思自治为基础，主体地位的不同和发展阶段的不同决定了必须有差异性补足。运气平等主义要求经营主体在对资源进行占有时，要考虑相关行为是否对自己的不利负有责任。有必要将责任主义纳入平等主义概念中，考察主体在努力和选择过程中的责任是刑事责任的基础。如果说法益是一个规范层面的概念，损害原则则更倾向于司法过程的适用功能，更具有个案的适用价值。损害原则与市场伦理相呼应，构成对经营主体进行保护的基准。遵循原旨解释的第二层含义，寻找规范字里行间的内在立法原始意图是理解民营企业背信犯罪处理的平衡性依据。在没有严重损害债权人权益情形下，公司人格问题的讨论并无公司法的实质意义。在前置法没有实际处罚意义的前提下，刑法的处罚自然无价值。在存在损害——权益侵犯情形下，通过人格否认落实为民事责任，且无法排除对财产性质的合理怀疑时，也不属于刑法评价的对象。

6、企业数据财产化的刑法保护（王铎）

来源：《法学论坛》2026年第1期

数字经济浪潮之下，海量企业数据创造了丰富的经济价值，形成了扩充的财产利益增量，从而进一步财产化成为刑法意义上的财物。基于企业数据的财产价值，其逐渐成为犯罪的攻击对象，而既有的数

据信息化保护路径与知识产权保护路径无法全面保护企业数据的财产法益，造成企业数据的刑法保护漏洞，并可能产生定罪量刑不科学的影响，有必要加强企业数据的财产化刑法保护。由于企业数据的刑法财产属性的争议与犯罪数额认定的困难，企业数据财产化刑法保护受阻，刑法有必要确认企业数据的财产属性、分类分级限定财产化保护范围、结合现有规范构建犯罪数额认定机制，并明确财产化保护路径与其他保护路径的配合机制，完善企业数据保护的刑事法网。

7、数据财产的独立性构造与刑法保护（熊波）

来源：《东方法学》2025年第6期

进入数字经济时代，我国理论界和实务界对数据财产的刑法保护表现出依附性或独立性理论构造的混杂化特点，并采取截然相反的保护做法，这不利于精准定罪量刑。依附性保护构造在对象要件层面依附于侵犯财产罪的有体财物和无形财产性利益，在法益内容层面依附于侵犯财产罪的财产所有权和占有权。依附性理论违背了罪刑法定的基本原则，违反了法秩序统一性原理，容易导致罪刑失衡，并不可取。刑法应当明确数据财产的独立性理论构造，将数据财产的刑法保护独立于侵犯财产罪的财物和财产性利益、财产所有权和占有权。在独立对象要件层面，数据财产具有外在无形性特点，以及非统一性、不稳定性、货币无法等价衡量性的内在价值特点。在独立法益内容层面，数据财产权具有有限缩性和持有权的双重法益构造。基于数据财产的独立性理论构造，在对象要件层面，刑法应当明确数据财产的特质在于数据载体所承载的经济利益，并区分适用计算机数据类个罪和侵犯知识产权类个罪。在法益保护层面，刑法应当构建经济损失和违法所得的法益侵害的二元入罪标准，塑造并列且择一的独立适用关系。

8、动产担保视角下数据担保的体系定位与解释论展开（赵申豪）

来源：《当代法学》2026年第1期

数据具有经济价值与可让与性，是适格的担保财产。虽然数据没有实物形态，但它是现实世界的客观存在，可通过数字技术控制与支配。因此，数据在民法上的定位应当是无体物，可比照适用动产物权的规则。尽管如此，数据在竞争性、时效性、是否涉及他人利益等方面均有别于动产与智力成果，所以应就数据担保构建专门性的调整规则。在担保物权的类型上，基于数据的非消耗性、可复制性等特征，数据担保原则上应采取数据抵押，亦不排除设置数据质押的可能。在担保财产的范围上，鉴于数据具有强时效性与经济价值上的规模效应，数据担保多采取集合担保的交易模式，而这会与物权客体特定原则产生抵牾。对此，可通过将担保物权客体的“特定性”解释为“可得特定性”予以缓和。在担保物权的实现上，由于个人信息类数据承载着信息主体的个人信息权益，其转让受到“知情—同意”规则的限制，应将强制管理制度作为数据担保的实现方式。

9、数据财产担保的体系构建（钱子瑜）

来源：《法商研究》2026年第1期

数据财产担保以载体层面的数据为标的，应解释为数据的担保而非权利担保。对于担保权人来说，数据具有可复制性，数据交付无法发生排他性移转占有的效果，数据持有的留置增信效力有限，无法排斥担保人利用数据。对于担保人来说，数据交换价值具有时效性，担保人在担保期间具有利用数据的现实需求。数据财产担保属于固定担保，应当借鉴动产抵押规则进行体系构建。数据财产担保采用“合同设立、登记对抗、交付互信”的基本框架：合同是担保设立的方式，登记是担保权对抗效力的要件，交付数据复制件是协助担保权人明确担保标的范围、便于价值评估的方式。此外，针对数据价值的波动，主要通过价值评估权获悉变化、通过价值保全权提供保证；针对数据可重复变价的特征，建议通过构建“强制管理制度”来充分发挥数据价值、保障债权实现。

10、数据产权的营业权属及其体系效应（林涓民）

来源：《华东政法大学学报》2026年第1期

在缺乏数据产权专门立法的背景下，唯有将数据产权归为一种既有权利，才能实现保障权益、合规使用的数据产权制度目标。数据产权化的功能有二：一是通过化解数据交易的合规风险促进数据交易，二是在不阻碍数据流通的前提下保护企业对数据资源的合法持有。为实现上述功能，数据产权应被界定为数字时代的新型营业权。将数据产权界定为营业权，既与数字时代营业观念扩张相一致，也不会干扰个人信息保护规则的适用。作为新型营业权的数据产权与数据产权登记相结合，能够表征数据供方合规地持有数据，使数据需方免于承担因无法自证无过错而被问责的风险，有效促进数据流通。当数据产权受到不法侵犯时，权利人可以依据《民法典》第1165条第1款请求损害赔偿，但不得依据《民法典》第1167条主张停止侵害、排除妨碍、消除危险等防御性侵权请求权。

11、数据财产权与个人信息权益的冲突与调适（巩姗姗）

来源：《中外法学》2025年第6期

数据确权是数据要素市场化改革的基础。当法律向数据处理者配置数据财产权，涉及可识别个人数据时，便形成数据财产权与个人信息权益并存的共生权利结构。当前，二者未能清晰界分。以“知情同意”为核心、贯穿“全生命周期控制”的个人信息保护体系，构成对数据财产权行使的制度性约束，制约数据高效流通与数字经济深化发展。个人信息权益本质是旨在防范数据处理风险的防御性权利，而非个人对数据的排他性支配权。个人信息权益体系应从全程控制向“剩余控制+风险防控”转向，通过限缩可携带权等工具性权利的适用空间，强化行为规制与分级治理，重构更具适应性的保护范式；科学界分两类权益属性，合理协调个人与公共利益，明确可市场化数据的边界；承认数据来源者的“数字劳动”及其在数据生成中的基础性价值，依据分配正义原则，构建以“贡献度”为基准的数据收益分配机制，实现数据价值与收益的公平分享，

最终形成兼顾保护、流通与创新的数据治理新格局。

12、反不正当竞争视角下商业数据的类型化确权进阶（侯利阳）

来源：《法商研究》2026年第1期

随着数字经济的兴起，如何通过权益配置激发商业数据的市场活力成为各国需要面对的问题。通说认为应当在反不正当竞争法的框架中进行商业数据的确权，但存在两种不同的确权思路：一是采用商业秘密的保护路径来确权，二是适用实质性替代原则来确权。这两种解决思路看似存在冲突，但均旨在保护数据持有人的财产性权益，只是在保护方式上存在强保护与弱保护的差异。商业数据的构成复杂，难以对其确权形成统一的解决方案，宜对之作类型化处理，区分非公开商业数据与公开商业数据；前者宜作为商业秘密进行保护，后者应适用实质性替代原则予以保护。

13、论数据产权分置的体系构造：以数据持有为中心（徐化耿）

来源：《清华法学》2025年第6期

数据产权的价值取向在于助推数据流通，应以“卡—梅框架”之下的责任规则取代财产规则作为数据利用的一般原理，即以事后定价取代事先同意作为数据流通的基本规则。数据产权以实际控制数据并能决定其利用方式为本质特征，其与传统所有权制度并不冲突，二者可以“控制”为连接点，实现有机契合。传统所有权的控制效果起源于占有，而数据产权的控制效果既发端于也呈现为持有。持有是形成于技术基础之上的事实状态，贯穿于数据利用的全周期，同时持有的来源应符合数据合规要求。在权利配置上，数据产权应以持有为中心，以“数据所有权加数据持有”的二元结构具体展开构建。数据所有权是一种虚置性权利，仅在数据生产阶段具有现实意义，而数据持有才是数据利用的一般性正当权源。数据持有的内容具有开放性，包括但不限于《关于构建数据基础制度更好发挥数

据要素作用的意见》中的数据加工使用权、数据产品经营权等子权利。

新型数字技术的法律应对

1、物联网产品范围的界定及其对民事责任的影响（周学峰）

来源：《比较法研究》2025年第6期

物联网产品的典型特征在于其集硬件、软件与服务为一体，而且随着产品智能化功能的加强，以及软件和服务的价值在物联网产品中所占比例的上升，其重要性日益凸显。传统法律制度中的瑕疵担保责任制度和产品责任制度都是以有形物为典型的适用对象而进行规则设计的，未能考虑到物联网产品的特性。在当前数字化、网络化和智能化的背景下，为了充分保护物联网用户、消费者的权益，应当通过扩张“商品”和“产品”的概念范围，将物联网产品功能发挥所必需的软件、服务纳入其中，使其与硬件一体适用瑕疵担保责任和产品质量责任。随着软件、服务因素的纳入，其对于瑕疵担保责任中瑕疵的认定、卖方的售后义务，以及产品责任中产品缺陷认定、损害赔偿范围和免责抗辩等都会产生重要影响。

2、人脸识别技术治理的另一种理论范式：透明度、可问责与信息关联消除（赵精武）

来源：《政治与法律》2026年第1期

人脸识别技术的广泛应用实现了信息服务的便捷化，但同时也引发一系列争议：部分信息服务提供者变相强制自然人接受人脸识别技术，使得社会公众对于各类“刷脸”应用产生不信任，质疑这类技术应用是否确有必要。尽管现有研究针对这类问题提出各类风险治理机制，但是仍然存在人脸图像与人脸数据、身份识别风险与其他风险、差异性隐私泄露风险混同的问题，并且这些概念混同也使得相关治理规则或是停留于个人信息保护规则重述，或是泛化该类技术应用的特殊性。现阶段，人脸识别技术治理依然是围绕人脸数据展开，只不过治理逻辑

辑有别于一般个人信息，需要实现运作方式、权益影响程度、安全风险等重要事项的透明化。一方面，基于可问责理论延伸出公示问询、评估、备案、审计等治理规则，以权威机构的审查结果简化透明信息，实现社会公众对透明信息的可理解；另一方面，基于信息关联消除理论，义务主体无法确保人脸识别应用透明化时，应当消除人脸数据与其他个人信息的关联状态。

3、流量劫持的刑法治理：技术类型与规范评价（王华伟）

来源：《法学论坛》2026年第1期

流量劫持是数字时代备受关注的议题，它在不同法律领域中都存在很大争议。流量劫持具有复杂多样的技术形态，核心内涵是影响和控制用户数据访问路径。结合流量劫持的技术原理与规范评价，可将其分为系统内劫持和系统外劫持，系统内劫持可进一步区分为显性劫持与隐性劫持。流量劫持不宜按照财产犯罪或数据获取型犯罪论处，对此也无需设立新罪，破坏计算机信息系统罪和非法控制计算机信息系统罪足以应对。系统外的流量劫持不构成犯罪，宜作为不正当竞争案件处理。系统内的隐性劫持可以构成非法控制计算机信息系统罪。系统内的显性劫持可能同时构成非法控制计算机信息系统罪和破坏计算机信息系统罪，应按照想象竞合处理。

4、数字技术驱动下版权刑事保护的范式转型（陈超）

来源：《法学论坛》2026年第1期

在数字化和网络化推动下，通过数字化创作、数字媒体获取信息、传播分享内容已经成为日常生活工作中不可或缺的部分。然而技术发展带来生活便利的同时也引发了数字时代版权治理的诸多问题，尤其是在积极主义刑法治理立场下，版权刑事治理不断扩张不仅冲击着传统刑法理论基础，更侵蚀着著作权利益平衡的基本格局。基于对知识产权法哲学以及相应的刑法解释立场的考察，数字时代版权刑

事保护范式亟待转型，应遵循审慎功能主义治理机制，在规范适用时恪守限缩解释的立场，在法律运行机制上通过消极司法平衡积极立法，在法律适用上以主观解释限制客观解释，在犯罪判定思维上以实质出罪中和形式入罪。同时，明确审慎功能主义下限缩立场的前提、实质和定位，对具体犯罪构成要件解释作出适当限制，从而在著作权犯罪社会治理中适度限制刑法的介入，以充分提高数字时代作品利用的积极性。

5、元宇宙平台互操作实现的激励型治理（毕文轩）

来源：《东方法学》2025年第6期

元宇宙作为当前典型的新兴技术领域，具有广泛的商业用途和巨大的经济潜力，但是，缺乏互操作性已然成为桎梏当前元宇宙平台经济进一步发展的主要障碍之一。元宇宙平台在数据结构、数字身份、经济系统及治理模式上与传统平台具有差异，导致其在实现互操作的过程中存在技术标准不足、企业商业利益冲突、用户隐私伦理风险以及治理协作机制缺失等多重困境。建立在以传统竞争法为基础上的命令控制型法律治理模式，无法有效引导元宇宙平台的互操作实施，也难以防范因互操作而可能产生的风险，进而会削弱元宇宙平台互操作的实施效果。基于对提高元宇宙平台互操作规制效率的显性需求、规避互操作信息不对称的隐性需求以及实现互操作良好控制的发展需求的考量，规范元宇宙平台互操作需要引入激励型治理模式。基于分层规制理论从基础设施层、数字要素层和商业生态层分别构造相应的激励治理机制，在更好地发挥出制度功能、激励元宇宙平台互操作的同时，能够对可能引发的激励失灵给予及时的矫正，并构建促进元宇宙平台互操作实现的创新容错机制，形成科学的法律激励结构。

6、数实融合产品出卖人主给付义务的重构（吴逸越）

来源：《东方法学》2025年第6期

数实融合产品作为数字技术与实体硬件深度融合

的新型产品，对“数实分治”的现行法律规制模式提出根本性挑战。传统买卖合同法以有体物为中心构建的义务体系，难以对其进行有效规制。数实融合产品买卖突破了传统买卖合同一时性给付的特征，形成了“实体商品交付并转移所有权+数字产品给付+持续性服务”的复合义务结构。通过扩充无瑕疵给付义务的内涵，可以有效承载数字产品相关义务，具体包括：将数字元素纳入瑕疵考察范围，构建主客观并行的瑕疵判断标准，确立差异化的瑕疵认定时间节点，通过约定由第三人履行机制解决数字产品提供主体多元化问题等。这种义务重构既保持了与传统理论的连续性，又能有效回应数实融合产品的特殊需求，为消费者权益保护和数实融合经济健康发展提供法治保障。

数字政府与智能司法

1、政策试验视域下数字政府建设的法治化图景（赵龙）

来源：《东方法学》2025年第6期

在全面深化改革的背景下，政策试验已成为推动数字政府建设的重要工具。然而，数字政府对治理效能的过度推崇，使得“数治”与“法治”在长期结构耦合中张力凸显。传统理论如工具理性、价值理性与制度理性在解释此类张力时渐显局限，而以卢曼社会系统理论为代表的系统理性对化解内生于社会功能分化的此类张力展现出更强的解释力。当前推行的数字法治政府系统改革，旨在回应政府治理现代化对复杂性进行化约的深层需求。鉴于规则、程序与组织共同塑造了数字政府与法治政府两大系统的“共振界面”，应从规则设计、程序控制及组织保障等维度将数字法治政府建设政策命题再具体化。

2、数字化治理背景下行政参与权遮蔽的生成逻辑与制度因应（娄金炜）

来源：《法学》2025年第12期

权利遮蔽是指法定权利由于客观情势变更造成的

权利内容无法被完全实现的现象，环境变动和介质基础变化是其关键成因。在数字化治理中，具体行政行为中的相对人面临着行政参与权遮蔽的困境，需要系统探讨其生成逻辑。就技术引发的环境变动而言，数字化治理引发了公开行政异化、协商行政萎缩及责任行政混沌，造成了行政参与权遮蔽的不良结果；就数字化治理引发的程序介质变化而言，程序折叠下的流程结构再造和法律关系隐匿均带来了相应的行政参与权遮蔽问题。对此，宜分别从保障义务补位和权利迭代发展出发寻求解题思路，包括以实质可理解为落脚点、以有效交互为内核、以切实可问责为方向强化治理部门的行政参与权保障义务。同时，从推进技术与知情权融合、完善陈述申辩权的保障性制度群、设置人工服务可及权三方面推动行政参与权的迭代发展。

3、公共数据授权运营的反垄断规制（钟颖）

来源：《比较法研究》2025年第6期

公共数据授权运营是推动数据要素市场化配置、促进数据要素潜能释放的重要举措。然而，实施主体授权特定主体经营公共数据，将导致公共数据资源高度集中于少数运营主体，可能形成经营者进入相关市场的数据壁垒，衍生滥用公共数据市场支配地位行为等风险。对此，现有公共数据授权运营的竞争治理仍然主要依靠传统的事后反垄断监管，其在价值层面和方法层面均存在较大局限。鉴于公共数据授权运营的市场结构具有自然垄断属性及其运营主体的数字平台特征，加强事前反垄断规制成为可行的方向。具体而言，通过自然垄断业务的结构性拆分、设置运营主体的互操作义务、限制市场准入以及合理的价格规制等措施，提前防范垄断风险，弥补传统反垄断监管的不足。

4、数字监察及其制度建构（张震、刘栋阳）

来源：《华东政法大学学报》2026年第1期

数字监察是在数字中国法治建设场景中提炼的理论命题。技术要素与规范要素是厘清数字监察基本内涵的双重维度。技术要素遵循“工具理性”的内

在逻辑，主要功能是为监察范式革新提供技术赋能；规范要素遵循“价值理性”的内在逻辑，主要功能是为数字技术的运用确立法治秩序、提供价值指引。对数字技术的运用应同时秉持工具理性和价值理性，以防技术异化风险。数字技术的场景化运用驱动监察理念革新，进而撬动监察概念再造、监察原则焕新、监察方法迭代等，最终推动监察体系的数字化转型，从而以数字化监察体系对接数字化治理体系。当前，宜采取先由国家监察委员会进行实施性立法，待时机成熟后再由全国人大进行基础性立法的制度路径。数字监察的制度内容，主要包括对既有监察规范体系的法理承继与价值赓续、针对数字治理场景的制度调适与重塑、契合数字时代发展特征的全新制度建构等三个方面。

5、人脸识别侦查的场景规制与全景启示（张迪）

来源：《华东政法大学学报》2026年第1期

大数据侦查法律规制是重要的时代议题，传统宏观的整体研究忽视对其具体实践的考察和分析，聚焦人脸识别侦查的场景化研究可为大数据侦查之规制提供新视角。人脸识别侦查指借助人脸识别技术所进行的侦查活动。实践中，人脸识别侦查的主要问题是前期数据获取和算法运用尚未被法律规范，中期人脸识别侦查的用途多元但缺少体系控制，后期人脸识别侦查证据的使用处于失范样态。人脸识别侦查的复杂性、创新性和侵权隐蔽性、传统侦查规制框架的局限性和规范衔接难题、网络犯罪治理需求与大公安格局等导致人脸识别侦查未被法律规制。立足人脸识别侦查运用流程，应通过数据规范、算法规范、程序规范和证据规范等对其进行四维规制。人脸识别侦查场景的规制思路对大数据侦查的全景规制具有启示意义：不同大数据侦查在运用环节上存在共性，四维规制理论可推广为大数据侦查法律规制的基本框架；但不同场景下的大数据侦查具有自身特性，四维规制理论需结合具体侦查场景针对性地展开。中国应构建基于多场景的大数据侦查四维规制体系，这既能维护法律的体系性，也可保持法律的开放性。

6、数字法院构建的价值取向及其实现（解志勇）

来源：《现代法学》2025年第6期

构建数字法院的主要目标，是破除司法体制机制中的公平、效率障碍，实现人民法院系统性、整体性的数字化变革，以满足中国式现代化的司法需求。数字法院以审判工作现代化为导向，以宪法和法律规范为尺度，融合了审判经验技艺与客观性数理逻辑。静态层面以贯通联动的组织体系为支撑，在具体运行中以“解析式”数据链接搭建“数助式”办案系统，服务于审判权行使和司法政务管理，展现出“立体化”的业务流程。构建数字法院需秉持数字正义、司法效率、审判工作现代化等价值取向，以数字理念的融合维度、数字逻辑的遵循程度、数字技术的应用程度和数字办案的质效程度作为评价标准。通过预设数字司法的不同场景，坚持数字技术的工具属性并明确数字司法的救济途径，实现数字法院的制度重塑，并对全球数字司法变革提出中国方案。

数字时代的部门法研究

1、数字时代刑事证据合法性再思考及相关规则完善——以刑事诉讼法修改为契机（李学军）

来源：《法学杂志》2026年第1期

科技的进步，在助力公民生命、财产安全等物理层面人权保障的同时，极大程度地对公民精神层面的人权保障带来新的挑战，即公民的隐私权等正在不断被碾压。考虑科技发展带来的此等双刃剑效应，理应重思刑事证据合法性保障的人权内涵。检视我国现行非法证据排除规则以及司法实践现状可知，对证据非法性的审查认定基本上只在意是否侵犯公民的生命、健康、自由等人权，却极少关注是否侵犯公民的隐私权。随着物理空间与网络空间的进一步交融，电子数据已成为数字时代最基础、最核心的证据，若依然将其合法性“误定”为如同物证、书证合法性那般的客观真实性，固守于传统的物理层面人权侵害标准，必然难以满足新形势下精神层

面隐私权等人权保障的需求。因此，基于刑事证据合法性之“法”的动态性及其所保障人权的多维性，应在刑事诉讼法第四次修改时，增设搜查手机等电子设备中电子数据的法律规定，修正电子数据合法性的审查判断规则，同时更新迭代技术侦查的相关规定、正清电子数据等实物证据的合法性所在，适当扩大排除非法证据的证据种类并明确证据排除程序，以进一步完善我国刑事证据合法性相关规定及规则，助力人权保障。

2、数字孪息分配的解耦与类型化策略（邵怿）

来源：《政治与法律》2026年第1期

数字孪息是衍生于数字财产的附属增值收益，对于数字孪息的分配，传统规则由于物理依附缺失、价值来源异常以及权利边界模糊等困境，已经无法有效应对数字化的纠纷场景。因而，逐步实现从“依附性标准”向“价值贡献标准”的转变便具有了现实的紧迫性与必要性。价值贡献的判断需要建立在孪息与原物解耦的基础之上，同时也需要针对不同类别的数字财产，采取区别化的规制策略。此外，对于链上增值这一特殊经济现象，在引入全新标准之外，应重点理清法律规则与技术规则二者的效力位阶，避免出现规则的错位适配与跨层级冲突。同时，也应提前布局国家治理与自动化决策间的功能衔接与角色互补，以实现技术发展的成果可享与风险可控。

3、论数字民生权及其法律救济（宋保振）

来源：《法学》2025年第12期

伴随数字科技全面融入人们日常生活，技术控制和资本垄断引发众多民生利益新挑战，这使得数字社会中的民生保障需求显得尤为迫切。数字民生权作为数字人权的基本权利类型，是既有民生权的数字化转型与升级，其成立具有道德性、正当性和规范性依据。数字民生权隶属“二阶性”公民基本权利体系，以“全体社会成员”为权利主体，既包括民生权基础权能，也包括技术赋权逻辑下的信息无障碍权、互联网断开权、数字决策参与权和技术帮助

权。数字民生权法律救济以明确个人、平台和国家义务为前提：一方面，可通过行政解释将涉及数字民生利益的诉求纳入行政复议受案范围；另一方面，可通过行政和公益诉讼机制，实现对数字民生权的有效法律救济。

4、人机交互中的诈骗：基于相当性原则的建构（王华伟）

来源：《法学研究》2026年第1期

在智能机器全面普及的人机交互时代，在相关案件中一概适用盗窃罪，会使盗窃罪构成要件的定型性面临挑战，也与人们的观念和司法实践相背离。智能机器不具有独立主体地位，不能脱离人而受骗。在人人交互与人机交互并存的社会沟通方式中，诈骗罪作为沟通犯的法解释学构造应当与时俱进地发展。我国刑法规定的诈骗罪构成要件涵摄力强，在规范论的视阈下，由于智能机器扮演了类似代理的角色，行为人可以在特定条件下通过对智能机器实施功能性欺骗，从而实现对机器背后人的欺骗。这种理解的基本目标定位在于维护盗窃罪和诈骗罪的行为定型，并且避免可能出现的处罚漏洞。针对智能机器实施的功能性欺骗，应当与针对人实施的心理性欺骗具有相当性。对于人机交互中的诈骗，欺骗行为、错误认识、财产处分、财产损失等要件的理解与适用，都应当在相当性原则的指引下加以限定。

5、数字时代人格权商业化利用的法理重构：身份分层理论的展开（陆青、万子怡）

来源：《法学研究》2026年第1期

数字技术的发展正深刻重塑人格特质的呈现、传播与利用方式，致使人格权商业化利用实践呈现出高度的融合性与流动性，这对传统以“权利客体清单”为核心的人格权商业化利用理论范式构成系统性挑战。人格权商业化利用的本质，并非对个别人格要素的简单授权使用，而是对主体基于人格特质综合建构的“个人身份”所进行的符号化再生产。基于身份分层理论，数字语境中的身份呈现可以解析

为三个层面：作为人格尊严之根基与自主性基础的本真身份，作为社会互动中角色扮演与公众形象建构的社会身份，以及作为可脱离物理实体并由算法与数据驱动的数字存在的虚拟身份。三者构筑了从人格内核向外围延伸的“差序格局”，各层之间存在着持续的渗透、互动与制约关系。身份分层理论并不旨在提出一种复杂概念分类标准，而意于提供一种实质的结构化的分析框架。经由对各身份层的规范检视与整合分析可知，该理论框架能够为评估人格权益受侵害程度、界定商业化利用边界提供更为精细的指引，有助于实现人格尊严保护与数字技术创新的动态平衡。

6、迈向程序正义：平台用工场景中算法自动化决策的人工控制（陈靖远）

来源：《法制与社会发展》2026年第1期

互联网用工平台对算法自动化决策系统的广泛运用催生了新的社会问题。在现行应对举措中，“算法取中”的实质性规则调整与权利视角下的“脱离自动化决策”等主要方案对于现实问题的解决仍然存在局限。因此，有必要引入“有意义的人工控制”作为互联网用工平台使用算法自动化决策系统应当履行的一般程序性义务。在正当性方面，“有意义的人工控制”是对平台算法权力的程序矫正，在维护社会共同体的整体价值与人性尊严方面具有独立价值。在义务内容方面，互联网用工平台应当在应用算法自动化决策系统的全周期内，通过事前一般禁止、事中流程监督和事后异议申诉等方式实现有意义的人工控制。在机制建构方面，可以借鉴“守门人”模式划定适格主体范围，设置公法与私法上的双重法律后果，并将程序性义务的履行纳入《数据安全法》等法律法规相协调，为数据安全提供一体化法律保护。数据犯罪具有独立的构成特征，具有不同于现有犯罪的、独立的侵害法益、犯罪对象和危害行为，应属于扰乱公共秩序罪。数据犯罪立法体系内部是二元、立体结构，包括侵犯数据本身安全犯罪和妨害数据安全秩序犯罪，其保护的重点应当是国家核心数据和重要数据。

算法合规审计。

7、人工智能时代我国儿童色情的刑法规制（朱光星）

来源：《中国刑事法杂志》2025年第5期

我国现行刑法对儿童色情的规制存在法益定位偏差、规制对象混同以及因儿童年龄差异导致的定罪处刑失衡等问题。人工智能生成虚拟儿童色情，具有制作门槛低、生产批量化、客体虚拟但仿真度高、传播便捷等特点，严重违反“不得性化儿童”的文明底线，对全球儿童色情犯罪治理构成严峻挑战。我国现行刑法尤其面临虚拟儿童年龄识别困境以及对持有行为非罪化的规制缺憾。域外国家的新探索否定了虚拟儿童色情系“无被害人犯罪”的观点，其共通经验值得借鉴。应当确立儿童色情与成年色情的二元规制模式，明确儿童色情侵害法益是儿童人格尊严与性健康发展权。应当将持有儿童色情予以犯罪化，并同步建构下列三类内容的出罪机制：基于正当目的的抗辩、未成年人合意性行为的私密影像记录、执法司法机关依法调查所用的虚拟儿童资料。

8、论数据安全的独立刑法保护（皮勇）

来源：《法商研究》2026年第1期

当前我国数据安全的刑法保护具有附属性、有限性和不完全性，需要改进。为数据安全提供独立、全面的刑法保护既是社会安全发展的要求，也是国际立法趋势。《中华人民共和国数据安全法》确立了数据安全法益的独立性，其内容是数据本身安全和数据安全秩序。数据犯罪立法应当秉持发展、协调、平衡的立法理念，与《中华人民共和国数据

9、数字贸易制度型开放的基石：数字信任体系之构建（梅傲）

来源：《东方法学》2025年第6期

数字贸易是数字经济和高水平对外开放的重要组成部分，但目前我国在数字贸易领域存在信任危机、开放限制过高两大问题，推动数字贸易制度型

开放成为经济发展的重要任务。数字贸易的制度型开放可以分为贸易制度层面的高标准经贸规则对接和贸易本体层面的高水平对外开放。贸易制度层面的开放分为国内制度完善与国际高标准制度衔接，重点任务在于解决市场的信任与公平透明问题；贸易本体层面的开放主要在于贸易要素流通的开放，重点任务在于解决贸易主体、标的、过程的信任问题。数字贸易制度型开放的核心要素是数字信任体系的搭建，由此提出“信任建立—信任保障

—信任维护”三步搭建模式，通过利用权益授权证明算法的特性，依托区块链技术建立贸易主体的数字信任；依赖可信数据空间方案，利用隐私保护计算技术保障贸易标的的数字信任；构建新型数据托管理论，通过放宽精神损害认定、采用风险性损害赔偿的责任承担模式强化数据责任的方式，搭建数字贸易中的数字信任体系，以期推进数字贸易的制度型开放。

（技术编辑：毕坤阳）

教研活动

北大举办“数字时代的技术规制、法治变革与秩序转型”研讨会

2025年12月25日，“北大文研论坛”第212期在静园二院208会议室举行，主题为“数字时代的技术规制、法治变革与秩序转型”。本次论坛的引言人为厦门大学法学院助理教授、北京大学人文社会科学研究院邀请学者毛海栋；参与讨论的学者包括北京大学法学院长聘副教授戴昕、清华大学法学院长聘副教授鲁楠、北京大学法学院副教授胡凌、对外经济贸易大学法学院教授许可、北京大学法学院长聘副教授左亦鲁、清华大学公共管理学院长聘副教授陈天昊、北京大学新闻与传播学院助理教授刘金河、同济大学法学院助理教授朱悦；主持人为北京大学法学院长聘副教授、北京大学人文社会科学研究院副院长阎天。

论坛伊始，毛海栋老师以“技术规制、法治变革与秩序转型”为题做引言，介绍了本场论坛的主旨。毛老师首先回顾了其对数字时代的法律-技术关系的研究缘起，认为在数字时代，网络和数字技术作为规制手段和模式逐渐崛起，对法治、伦理和社会秩序等都产生了重要影响。毛老师认为，法律和技术之间存在两类关系：一是将技术作为规制的对象，即对技术进行规制（regulation of technology）；另一是将技术作为规制的工具或手段，即通过技术进行规制（regulation by technology）。技术规制有两种意涵。首先是在一般意义上，技术本身具有独特的规制机制，通过要求、强制、抑制或禁止人们做出特定行为来约束人的行动，对人产生广泛的规制效应；这种规制的特点是通过技术物的功能可供性对人的知觉和行动进行媒介，实现人与世界的互构。而法律意义上的技术规制则是指，技术像法律一样规制人的行为，具有法律上的意义和影响，涉及权利义务和权力关系；技术支持、补充、替代着法律。法律意义上的技术规制可以分为公共部门的技术规制和私人部门的技术规制：在公共部门的技术规制中，人们最常关注到的是行政部门的技术规

制；而私人部门的技术规制则主要涉及近年来平台利用算法、大数据分析、物联网等技术来规制消费者、劳动者、内容创作者等群体。



与会学者合影

毛老师认为，技术规制的崛起引发了法治变革。当前，规制主体呈现出公共部门与私人部门的互动融合，规制的效应也呈现出从调节性技术规制到构成性技术规制的规范性光谱，技术之治（Rule of Technology）与法治（Rule of Law）存在竞争与张力。毛老师比较了技术的规制机制和法律的规制机制，认为其存在四方面的区别。在规制方式方面，法律主要依靠规则的“内化”或“主观化”机制来对行为进行规制，技术则通过“物化”或“客观化”机制来规制行为。在规制所依赖的媒介方面，法律主要通过语言文字和法律文本这样的符号媒介进行规制，而技术则主要通过物质性媒介进行规制。在规制过程方面，法律是一种控制论意义上的规制过程，遵循“设定标准—持续监控—采取矫正措施”的三阶段过程，而技术则将这三个过程合而为一并自动执行。在规制的效果和影响方面，法律规制需要行为人的理解与配合，而技术规制则是自动化的，行为人难以质疑、难以拒绝，因此也难以救济。因此，毛老师认为随着技术规制的兴起，作为一项规范性、因果性、道德性事业的法律正在消亡。基于此，数字时代的法治变革在对象方面需要同时考量法律规则和技术措施，在约束主体方面需要同时考虑公共部门和私人部门，在法治维度上需要兼顾形式正义、程序正义和实质正义，而在媒介方面需要考虑将文本之外的技术物（artifacts）也作为法律规则的表达形式和法治的载体。

毛老师认为，技术规制崛起引发的法治变革推

动人们去反思法律何为。传统的以文本为基础的法律的特征在于保留了阐释学空间，法律告诉行为体何为可为和不可为，行为体可以选择如何行动；但在技术规制的条件下，行为体可能失去了这样一种能动性。因此，技术时代的法治设计需要考虑将法律的规范性和价值转译到技术系统中；在此基础上，毛老师提出了技术时代法治设计的透明度原则、自主权原则、对称性原则、情境公平原则、可争议性和人类监督等重要原则。最后，毛老师提出一系列问题供大家思考和讨论：是否总能通过更为有效的技术手段来替代文本法律规则？技术是对法律的辅助、补充还是替代？如果技术可以作为法律的媒介形式和具身化体现，那么应该如何重新理解“什么是法律”？“技术规制”这一概念/框架是否有益？是否应承认一种更弱意义上的规范性，如规制效应或功能可供性？法治设计与形式、程序、实质法治之间的关系是怎样的？等等。

随后，鲁楠老师聚焦数治是否可能取代法治这一问题，以“数治、法治与人的自主性”为主题发言。鲁老师主要讨论了三个问题。第一，关于规制（Regulation）的翻译演进及其背后所体现的社会变迁。鲁老师指出，Regulation的本意强调柔性调解，涉及多元主体相互配合，以及传统意义上的公私主体相互渗透和配合；Regulation的汉语翻译自改革开放以来经历了管制—规管—监管—规制的变化，这背后体现的是随着市场化转型深入，政府在社会发展中逐渐放权退出。鲁老师认为，规制一词使用的泛化可能同样存在风险：规制仍然是在管理的意义上思考法治，而法治本身则具有更丰富的意涵。第二，关于法律与代码之间的关系问题。鲁老师引述卢曼（Niklas Luhmann）的观点，即将法律视为在合法和非法的二进制代码区分基础上所建立起来的一个自创生系统，在这个意义上法律本身就是一套代码。鲁老师认为其所隐喻的社会秩序是一种黑客帝国式的秩序，即法律通过匿名化的方式自主运转，而人不被视为拥有独立自主意志的主体。第三，关于技术的规范性问题。鲁老师认为，法律的规范性建立在人的合理选择的基础之上，即

法律尊重每个人对自己生活方式的选择；而如果考虑技术的规范性，就需要考虑技术是否是建立在承认人的尊严和自主性的基础之上的。

胡凌老师以“信息增加或减少之后：透过技术看本质”为主题发言，讨论了信息爆炸时代以及当下人们试图减少信息的尝试如何影响人们的选择。胡老师认为，信息（技术）是（法律）规则的内生条件，因为信息本身是一套规则系统，需要对外释放信号、传递信息，特别是关于特定行为及其后果，以及发现概率。信息也是市场有效运行的条件，因为市场需要强有力的信息披露。胡老师认为，信息传统上以不同类型的数据和内容及其载体呈现出来，用于指引社会主体行动，产生激励效果；但一旦信息生产突破既有形态、数量限制，就会产生新的治理效果。在过去二十年间，随着信息生产方式的演化，平台企业形成了围绕人工生产信息和服务的商业模式。胡老师区分了两类信息：一类信息是展示性信息，包括版权内容、价格、用户职业、头像等；另一类信息是辅助性信息，包括认证信息、匹配信息和评价信息。胡老师认为，信息增加之后，信息结构发生了变化：认证信息的范围从基础身份信息拓展到行为信息，评价信息的范围从单纯的评分排名拓展到披露声誉信息，匹配信息的范围则从静态连接拓展到动态匹配。

戴昕老师以“法律与技术的相互隐喻”为主题发言，讨论了法律和技术如何相互隐喻及其原因。戴老师列举了石蕊测试、防火墙、模块、监管沙盒、人在回路等法律中的技术隐喻，认为法律专业中之所以会引入技术术语作为隐喻，主要是为了突出法律的科学严谨，即法律就像工程一样是被专业设计出来的；而这种法律中的技术隐喻的缺点则在于言过其实。戴老师也列举了权限、程式、联邦学习、合宪智能等技术中的法律隐喻，认为工程领域之所以会引入法律术语作为隐喻，主要是为了强调这些工程项目的权威性、正当性、可控性、人性化等；而其缺点则在于夸大了技术的同理心，并试图以此掩饰伦理的不确定性。戴老师认为，法律和技术之间的这种借势修辞存在着双向动机，法律借助技术

话语增加了自己外观上的科学性和形式上的稳定性，而技术借助法律话语提高了自身的规范性以及由此而来的社会的可接受性。作为结论，戴老师认为，虽然当前技术与法律之间有各种比喻，但机器和人的最大的差别在于人不仅是通过“训练”，而且也通过“意会”来了解和理解社会，新知识无法仅通过程式化的理论和程式化的方法获得，灵感涌现需要丰富的涉猎与经验的积累。

许可老师以“技术法的雅努斯：从 RegTech 到 GovernTech”为主题发言，讨论了治理如何从技术作为工具向技术作为构成要素与方法转向。从雅努斯（Janus）的隐喻引入，许老师指出技术的影响具有两面性，悲观主义认为技术进步会导致监控国家、法治黑箱、数字鸿沟、平台垄断等问题，乐观主义则认为技术进步会带来国家治理进步、直接民主、个体赋权、颠覆性创新等积极影响。许老师回顾了从 1G 到 4G 时代的主要技术架构和特征，以 Uber 的“灰色名单筛选”和大众汽车排放测试时的“作弊装置”为例，许老师指出在监管科技（RegTech）不断发展的同时，企业也会相应地规避监管，发展出反监管科技（Anti-Regtech）。许老师认为，当前技术变化的核心在于，技术已经不只是人们日常使用的工具，它实际上成为理解法律和规制的一种重要的环境和方法。因此从监管的视角上，许老师认为需要引入以技术作为构成要素和方法的治理科技（GovernTech）作为以技术作为工具的监管科技（RegTech）的补充。治理科技的特点在于强调整体性治理（Holistic Governance）和网络治理（Governance as Networks）并重，经过仔细设计并符合伦理标准；在此基础上许老师提出了科技治理的三项原则，即对称原则、互动原则和共同优化原则。

左亦鲁老师以“‘新’言论自由与内容管理”为主题发言，讨论了当代技术环境对言论自由的影响。左老师认为，平台企业的兴起带来了两项变化：第一，平台企业改变了经典的言论自由理论所预设的政府—公民二分模式，形成了政府—平台—公民的三角模式；第二，在前互联网时代，不管是限制

言论自由还是保护言论自由基本都采取的是一事一议、人工干预的做法，但在互联网时代，算法会介入审核过程。左老师认为，当前最重要的问题是，AI 对互联网而言，到底是一项革命性的进步还是现有技术的延续。如果 AI 是一项革命性进展，其可能影响包括：第一，人和 AI 对话生成的内容是否是人具有主体性的成果；第二，AI 直接影响人们获取信息的方式和媒介，从根本上影响言论自由；第三，在 AI 时代，信息泛滥而非表达稀缺将更成为常态，这对传统上基于表达稀缺的言论自由的定义提出了挑战。

陈天昊老师以“数字时代何以法治？——技术规制对规范体系的冲击与替代”为主题发言，讨论了数字技术对法治的复杂影响。陈老师认为，法治有两重目的，其一是保障人的尊严，其二是提供行为预期。而为了实现这两个目的，法治提供了三项手段，一是将基本权利刚性化，注入规范体系；二是建立成文明确的规范体系；三是通过权力及其制衡来实施法治。陈老师认为，数字时代出现了三项新的变化：一是治理对象是表现为黑箱一样的技术；二是技术本身的发展也处于加速之中；三是产业生态根据技术的变化而不断演化。陈老师回顾了当前大语言模型的技术进展，认为当前数字时代社会治理的特征包括：第一，发展成为比基本权利具有更高显示度的目标；第二，成文法被大量的规章、其他规范性文件、技术标准架空；第三，社会治理仍然依靠权力及对权力的制衡，但转变为平台权力和监管权力之间的平衡，立法和司法的影响力弱化。作为结论，陈老师认为，在数字时代，规范和行为之间存在着一个日益厚重且完全不透光的技术层；如何平衡个人尊严和人类发展，如何将成文法转化为具体行动，如何真正制衡权力，最终都只能依靠技术。

刘金河老师以“技术空间中的理性进程与私人秩序”为主题发言，讨论了马克思和韦伯视角下的当代技术环境。刘老师认为，早期网络空间是一种由技术社群和互联网公司主导的秩序，当前线上平台时代则是商业平台企业主导的秩序，而未来的科

技社会可能是科工复合体主导的秩序，其共同的特征都是一种私人秩序（private order），即在私人力量和私有主体主导的规则体系下运行的社会状态。刘老师认为，平台权力正在创造一种新的社会秩序，即平台私人秩序。在马克思的视角下，平台权力是受制于工业生产力的结果。私营性和私有化是市场经济的基本逻辑，私营性是平台权力发生的根基，私有化是平台权力实现的基础，互联网平台作为产品是企业财产，具有私有性。而在韦伯的视角下，平台权力作为社会私有化的结果，是社会整体理性化进程的必然。在此基础上，刘老师进一步追问如何在平台权力秩序中寻求价值的可欲性，指出一种可能性是用文化涵化并超越理性，另一种可能性是在私有结构中实现公共价值。

朱悦老师以“迈向法学研究的网络与信息化转型”为主题发言，聚焦法学研究的发表如何更好匹配当前的技术进展。朱老师主要谈及三个问题。第一，算法（模型）是否是黑箱？朱老师认为，大数据模型并不完全是一个黑箱，其数据清洗过程等是可以被研究的，因此法学研究不应该放弃其中和知识产权等与法学有关的部分的研究。第二，算法（模型）可以被引注吗？朱老师认为，当前期刊的引注格式仍然相对传统，对网络资源的引注格式仍停留在网页引用上，可以考虑与时俱进增加 APP、移动页面等数字资料的引用格式支持。第三，算法（模型）可以被纳入法学研究吗？朱老师认为，面对当前的技术进展，法学研究的范围需要与时俱进，将一些网络与信息化的人造物纳入法学研究的范畴。

第六届网络法治论坛暨北京市网络法学研究会 2025 年年会及公益大讲堂在京成功举办

2025 年 12 月 28 日，第六届网络法治论坛暨 2025 北京市网络法学研究会年会、数智法治与数字经济高质量发展公益大讲堂在北京隆重召开。本届论坛由北京市法学会指导、北京市网络法学研究会主办，中国政法大学互联网金融法律研究院、中国政法大学数字经济与法治研究中心、北京邮电大学互联网治理与法律研究中心共同承办。

本届论坛深入贯彻落实党的二十届四中全会

及《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》精神，深刻把握新一轮科技革命和产业变革的历史机遇，以“数智法治与数字经济高质量发展”为主题，来自高校、科研机构、公检法、政府机关、企业的专家学者和青年学子共 41 人就本届论坛主题发表真知灼见，并集中围绕“建立合理有效的数据产权与治理制度”“健全人工智能法治规范，促进新质生产力发展”议题深入研讨，分享前沿研究成果与创新思路，为与会者带来一场学术盛宴。

主题发言

中央网信办网络法治局李民处长介绍了数据跨境流动法律体系的构建成果，我国已基本形成了“三法一条例四规章”为主体的多层次、全覆盖的数据跨境流动中国模式，构建了覆盖不同类型和数据场景的管理制度体系，地方性法规和规章也对数据跨境规则和法律体系构建作出了重要贡献。



李民 中央网信办网络法治局局长

研究会副会长、中国政法大学民商经济法学院刘继峰教授围绕“数据法的学科建构问题”，指出数据法学科的确立需要具备概念和概念体系、理论与理论体系、方法与方法论三大要素。数据法学科的发展可以从坚持客体中心主义、数据全生命周期视角、利益平衡原则以及技术与法律的结合四个方面建立起学科范式。



刘继峰 中国政法大学民商经济法学院教授

研究会副会长、中国社会科学院法学研究所研究员**席月民**以“积极适应高水平对外开放，加快中国数字经济法治建设”为题，提出数字经济时代法治与开放之间是互促共进的关系，数字经济法治建设的核心是开放与安全、创新与监管、自主与对接三对关系的有机平衡，数字经济法治建设应精准发力于高水平对外开放的重点领域与核心场景。并结合我国数字经济法治建设的基本制度现状分析了数字经济法治建设的未来发展走向与基本路径。



席月民 中国社会科学院法学研究所研究员

研究会副会长、人类命运共同体研究院副院长、中国传媒大学**王四新**教授从互联网内容治理的人民性出发，指出网络生态治理的治理实践和理论研究均应当以人民为中心，把人民的数字权益放在首位，为全体人民、为整个民族创造良好的精神家园。



王四新 中国传媒大学人类命运共同体研究院副院长、教授

研究会副会长、北京航空航天大学法学院副院长**周学峰**教授以“人工智能产品责任的范围界定”为题，指出人工智能存在多种样态，对应的侵权责

任归责原则也存在多样性，不宜一概适用产品责任。人工智能产品责任的适用应当限定在功能实现所必需的软件和服务范围内，并应当通过立法明确人工智能产品责任损害赔偿的范围。



周学峰 北京航空航天大学法学院副院长、教授

中国一上司法培训基地反洗钱与金融安全研究中心主任、上海政法学院**王铎**教授以“我国公共数据汇聚关联风险的系统解构与治理进路”为题，归纳总结公共数据汇聚模式的类型，并从治理思路、治理过程、治理情景、治理机制、治理结构等多方面进行系统分析，指出风险治理应当坚持总体国家安全观。



王铎 上海政法学院教授

议题一“建立合理有效的数据产权与治理制度”

研究会会长、中国政法大学民商经济法学院**李爱君**教授围绕“数据产权与数据价值释放”主题，明确了数据的定义、特征、数据的双层结构，厘清了数据和信息之间的关系，分析了数据产权的内容与未来数据产权制度的立法趋势，指出对数据的科学认知是未来数据法学体系的研究、数据法学科建设的基础。



李爱君 中国政法大学民商经济法学院教授

研究会理事、中国政法大学仲裁研究院秘书长、涉外法治研究院**李良**副教授以“反垄断法中的数据规制与竞争促进”为题，分析数据在市场活动和竞争中的角色，从经济性损害与非经济性损害的角度出发，探讨与数据相关的反垄断问题，提出竞争促进与个人信息保护之间存在冲突，应由部门法处理剥削型滥用相关的问题。



李良 中国政法大学仲裁研究院秘书长、涉外法治研究院副教授

《大连理工大学学报（社会科学版）》执行主编**张秀萍**以“教育领域数据立法：构建安全、可信的数字教育未来”为题，谈到教育数据的重要性，比较分析我国和欧盟、美国对教育数据的保护的立法实践，指出我国的教育数据保护面临数据本地化要求、合规成本高、大数据分析 with 预测风险等挑战，未来应当细化规定、技术赋能、严格问责机制、提升数据素养，进行教育数据保护的专门立法。



张秀萍 《大连理工大学学报（社会科学版）》执行主编

北京师范大学法学院**时业伟**副教授以“算法透明义务中的数据出境判断及其在 FTA 框架下的法律协调”为题，提出在现有 FTA 框架下算法披露行为不是受保护的数据自由流动，本质上是自由贸易规则在数字监管问题上系统性不足的边缘行为，此问题是法律适用范围的结构不兼容导致的，可以从建立审查的中立机制、明确算法披露义务的定位、实施分类管控等方面进行制度重构。



时业伟 北京师范大学法学院副教授

研究会理事、北方工业大学文法学院**陈兰兰**副教授以“汽车数据出境监管问题研究”为题，从法律规定与实践衔接、出口管制和数据出境管理规定的协调角度分析了汽车数据出境监管实践中面临的具体问题，涉及负面清单制定、重要数据范围认定等方面。



陈兰兰 北方工业大学文法学院副教授

北京环球律师事务所合伙人**王艺**律师围绕“基于司法审查背景下数据产权登记体系构建应注意的若干问题”，指出《民事案件案由规定》新增数据纠纷案由对于数据司法审理、数据合规、权益救济的意义，在此背景下分析数据产权登记可能存在的问题，未来应当通过出台国家数据产权登记办法、充分调研对地方产业的影响、及时更新地方配套规则、发布司法解释，为数据产权登记提供更为明确的指引。



王艺 北京环球律师事务所合伙人

北京市炜衡（重庆）律师事务所党委委员、合伙人**温灏洁**以“在跨境贸易场景下，数据产权制度的构建”为题，指出跨境贸易数据存在确权难、流通难、协同难问题，跨境贸易数据具有多维属性、高时效性、高敏感性，应通过推行场景化确权、构建数据流转的规则框架、建立数据合规权益激励机制，建立以问题为导向的数据产权制度。



温灏洁 北京市炜衡（重庆）律师事务所合伙人

议题二“健全人工智能法治规范，促进新质生产力发展”

研究会常务理事、中国政法大学财税金融法研究所所长**翁武耀**教授以“AI时代下平台企业课税的几点思考”为题，指出在AI时代财富分配可能会更不公平，税收需要在此种变化下发挥再分配的作用，税制改革可从间接税的角度降低对劳动的税赋，通过对个人征收财富税等方式提高对资本的税赋。



翁武耀 中国政法大学财税金融法研究所所长、教授

北京市社会科学院法治所副研究员**王伟伟**从“自动驾驶汽车‘云控平台’交通事故责任”的视角，分析了云控平台运营主体的公私法定位，讨论了云控平台运营主体与驾驶人在不同情形下的责任划分。



王伟伟 北京市社会科学院法治所副研究员

研究会理事、北京信息科技大学**梁力军**副教授以“科技伦理视阈下人工智能的‘有所为’与‘有所不为’”为题，指出“有所为”体现在科技伦理应从“人机技数行”五维角度引导，以法律为红线，关注重点场景，实现科技向善；“有所不为”体现在围绕“尊重人类主体地位、保障社会公平正义、维护社会公共利益”三个维度构建伦理边界。



梁力军 北京信息科技大学副教授

研究会理事、北方工业大学文法学院讲师**尚志红**围绕“生成式人工智能服务提供者著作权侵权问题的思考”的主题，从人工智能网络服务商承担侵权责任的合理性、用户和服务商之间侵权责任分配与侵权主体确定、服务商注意义务等问题出发，指出侵权责任的认定和分配需结合具体生成场景进行分析，生成内容的侵权不仅和生成式人工智能服务有关，也和用户行为有关，需要结合行为的主导者具体判断。



尚志红 北方工业大学文法学院讲师

北京师范大学(珠海校区)讲师**魏志栋**围绕“数字安全治理的困境与破局：从算法黑箱到人才战略——兼及数字治理的概念谱系建构”，对数字治理、数字人才相关的核心概念作解释，认为数字监察数据建模存在三重矛盾，并由此引出算法黑箱问题，提出问题解决依赖于法律专业人才的培养，并提出数字法治人才的三级培养模式。



魏志栋 北京师范大学(珠海校区)讲师

江苏省太仓市人民检察院第六检察部干警**尹志豪**以“数智法治护航数字经济高质量发展：刑事涉案虚拟货币的处置困境与协同破解路径”为题分享实践中的思考，指出虚拟货币兼具财物与数据双

重属性，需以法治确权为基础，针对不同类型的虚拟货币设置差异化处置规则，以机制完善为支撑，通过统一资质、公允定价、安全保管规范处置流程，以协同共治为核心，凝聚治理合力，最终实现犯罪惩治和权益保护的双重目标。



尹志豪 江苏省太仓市人民检察院第六检察部干警

研究会常务理事、中央财经大学法学院副院长、中央财经大学数字经济与法治研究中心执行主任**刘权**教授以“人工智能的包容审慎监管”为题，指出包容审慎是人工智能监管的基本原则，包容审慎监管的目标是统筹发展和安全，应通过有效市场和有为政府的结合、引入试验机制、完善数据安全和个人信息保护认证、以容错机制激励市场与政府探索创新、法治与科技伦理规范并行等方式落实包容审慎监管。



刘权 中央财经大学法学院副院长、教授

研究会常务理事、中国数字治理研究会秘书长、北京师范大学互联网发展研究院研究员**杨煜东**围绕“AI与新质生产力”，指出技术发展包括技术涌现和技术扩散两个阶段，法律作为规制社会的手

段，在技术涌现阶段不应过于干预技术的发展，监管的包容性是回应目前技术发展的关键。



杨煜东 北京师范大学互联网发展研究院
研究员

中国信息通信研究院互联网法律研究中心研究员**杜安琪**以“《网络安全法》修改思路与制度设计”为题，分析了《网络安全法》的立法定位与实施成效，以及修改的思路与要点，指出应以落实总体国家安全观为工作指导，适应技术应用发展的新趋势，回应网络监管执法实践的需求，提升网络安全法律体系的协同性，进而发挥法律的引领规范保障作用。



杜安琪 中国信息通信研究院互联网法律研究中心
研究员

研究会理事、中国政法大学民商经济法学院**刘东辉**副教授从“人工智能驱动型程序化交易的证券监管转型”着眼，聚焦人工智能从执行者到决策者的身份转变，提出需要根据自主化程度对交易报告监管制定差异化策略、调整归责原则、规范对人工智能开发者的监管、合理分配举证责任等监管建议。



刘东辉 中国政法大学民商经济法学院副教授

研究会副秘书长、北京邮电大学人文学院**潘静**副教授以“生成式人工智能中算法黑箱的风险与治理”为题，分析域外的司法案例，梳理人工智能算法可能产生的风险类别，指出算法可能产生程序不公与歧视风险，需要进行针对性治理。



潘静 北京邮电大学人文学院副教授

对外经济贸易大学法学院助理研究员**谭伟杰**围绕“论数智时代的法律：从‘技术的’到‘实践的’法律观”，指出传统的技术法律观在数智时代的法律实践中难以回应事实与规范不对称的问题，而根据实践对法律进行续造的实践法律观才是数智时代法律观的更优解。



谭伟杰 对外经济贸易大学法学院助理研究员

贸大举办“AI智能体行为安全与发展”研讨会

2025年12月28日,对外经济贸易大学数字经济与法律创新研究中心联合清华大学科技发展与治理研究中心,在对外经济贸易大学宁远楼729会议室举办了“AI智能体行为安全与发展”研讨会。该会议汇聚了法学、公共管理、计算机、实务界等多领域专家,围绕“AI智能体跨APP操作的边界与底线”“AI智能体安全交互路径”“构建以安全为前提的多方共治生态”三大关键议题展开深度研讨,旨在凝聚多学科智慧,聚焦科技向善之维,探索AI智能体的未来发展之道。

清华大学公共管理学院长聘副教授、科技发展与治理研究中心主任助理**陈天昊**基于操作系统融合度和交互路径两个指标,划分出技术路线的四象限,并对国内外厂商开发的智能体进行归类。他指出,端侧智能体的广泛部署将对现行法律秩序构成严峻挑战:在网络安全方面,面临认知层攻击(如提示词注入)及模型内部目标劫持的新风险;在信息隐私方面,智能体的全域感知需求与《个人信息保护法》的“最小必要原则”存在冲突,且端云协同加剧了数据出域风险;在产业生态方面,GUI自动化操作引发了流量分配争议及“自我优待”垄断风险。针对上述问题,建议明确避免逐底竞争、培育市场力量、维护创新生态的三方面治理目标,并采取专门规章、软法、产业实践作为治理手段。

北京理工大学法学院研究员**王磊**指出,AI智能体高权限特征带来的四个方面的治理新挑战,一是责任分担问题,二是数据权益与互联互通存在竞争性壁垒,三是个人信息收集的合规标准挑战,四是高权限与不诚信的矛盾性。他指出,对AI智能体对“无障碍权限”的启用必然涉及对“最小必要原则”的突破,同时,AI智能体执行任务的关键节点缺乏必要透明度,有可能背离技术应用的应然方向。因应智能体的冲击,需建立“机制—技术”融合的复合型治理方案,树立主动引导的监管理念,

推动多元主体共治格局的形成,注重技术治理与法律治理的协同,发挥技术伦理与商业道德的作用。

恒安嘉新(北京)科技股份有限公司安全业务总监**雷小创**介绍了智能体应用场景中的主要风险点,如提示词注入、记忆投毒、隐私泄露等,特别介绍了其被诈骗分子应用时存在的潜在风险。关于智能体安全建议,他提出,一是推动智能体安全政策法规建设,完善监管制度框架;二是建立多元协作机制,提升智能体安全治理合力,三是推动“以技治技”,增强智能体动态防护能力;四是加强智能体应用本身防护能力。为此,建议在法规上明确责任红线,规范智能体应用高危权限(通讯录,短信、无障碍等权限)申请,技术上贯彻“隐私原生”与数据最小化,相关APP应强化安全边界管理。

哈尔滨工业大学(深圳)网络空间安全研究院智能体研究方向负责人**刘斌**介绍了豆包手机的系统架构,指出豆包手机实现自动化全流程控制的核心是:读取屏幕+动作执行,并研判了豆包手机助手存在权限和代码层面的安全风险。他认为国内外智能体发展策略取向存在差异,豆包的系统级注入策略属于非常规实现,而用户同意无法弥补底层代码的脆弱性,导致安全风险不可控。建议各方通过标准化、可审计的API接口开展合作,降低终端智能体对系统底层权限的依赖,形成技术与制度的多重安全防护。

对外经济贸易大学数字经济与法律创新研究中心主任、法学院教授**许可**从亚马逊诉Perplexity案切入,分析AI智能体与第三方平台之间的权责边界问题,其争议核心在于如何平衡平台自主权、用户授权与新兴技术特性。他认为,智能体代理下的访问呈现出隐名、机器、高频等特征,其合法性来自用户授权,有效性来自对用户意思表示真实、准确、完整的理解;但在数据爬取上,其单方、大批量、不受限制地复制与转移数据的行为,超出用户授权范围;在数据使用上,可能存在云储存、商业利用的风险。许可教授建议,在制度上采取用户和平台双重授权,在技术上采用模型上下文协议

(MCP)实现握手，最终从互害共生走向“人一机一平台”互利共生。

在总结环节，对外经济贸易大学副校长、法学院教授**梅夏英**指出：作为讨论主题的智能体具有多重面向，涵盖委托代理，数据保护、公共安全等多方面问题，参会的实务人士、专家学者的观点让人受益匪浅。梅夏英教授认为，应将人工智能的出现视为百年不遇的大事件，它会给社会带来根本性的变革，因而不能落入传统法律关系的窠臼，必须从更宏观的社会结构和技术系统角度重新思考治理方案。智能体自动化系统的本质决定了应首先从技术层面思考问题，应基于系统思维分析技术综合体，关注客观规律、机器智能等问题。梅夏英教授认为，智能体问题的实质是风险问题，在技术具有高度自主性的时代，应重视国家引导的作用，发展不能以牺牲安全为代价，在智能体技术安全、透明、可控等底线确立的基础上，再考虑市场中的博弈和技术路线的选择。

贸大举办“中国数字法学自主知识体系构建：2025 法学博士生学术论坛”

为深入贯彻落实党中央关于加快构建中国特色哲学社会科学战略部署，积极回应数字技术迅猛发展对法治理论与制度体系提出的时代课题，推动中国数字法学自主知识体系的系统建构与创新，引导青年法学研究者立足中国法治实践、聚焦数字时代的真问题、深问题，“中国数字法学自主知识体系构建：2025 法学博士生学术论坛”于2025年12月31日成功举办。本次论坛受到对外经济贸易大学科研处、研究生院的指导和支持。本次论坛邀请来自北京大学、中国人民大学、武汉大学、上海交通大学、日本大阪大学、中国政法大学、中国人民公安大学、中央财经大学、山东大学、天津大学、西南政法大学、首都经济贸易大学、对外经济贸易大学的23位博士后、博士研究生受邀参会并进行专题报告。

论坛开幕式由对外经济贸易大学法学院院长**冯辉**教授主持。对外经济贸易大学党委常委、副校长**梅夏英**教授出席开幕式并致辞。梅校长对2025年法学博士生学术论坛的顺利召开表示热烈祝贺，对与会专家学者和青年学者的到来表示诚挚欢迎，并简要介绍了对外经济贸易大学在数字法学领域的学科布局、研究特色与人才培养情况。他指出，数字技术正在深刻重塑社会运行方式和法治形态，数字法学研究应从数据、算法、人工智能、平台治理等关键议题的内在机理与制度逻辑出发聚焦真问题，数字法学研究者应夯实理论根基，在回应时代命题中不断提升研究能力，为构建数字法学自主知识体系贡献智慧与力量。

单元一：数智经济健康发展的法治保障

单元一以“数智经济健康发展的法治保障”为主题，由北京理工大学法学院讲席教授**齐延平**主持。

北京大学博士生**何炆**围绕“数字资产增值的权属配置：以借名直播中的添加工规则类推为视角”这一主题，聚焦直播账号“借名”引发的权属冲突，指出实际使用人运营投入致账号价值激增。为破解“静态定性无能、动态裁量失范”，主张合同法规则失灵时类推添加工：账号类为“原物”，演绎运营界定为“加工”。并提出效率导向加工主义：原则归加工人，例外以价值对比修正，并以债权补偿保护无过错方。

中国人民大学博士生**王嘉徽**以“平台内经营者‘内卷式’过度竞争：困境、原因及对策”为主题，指出平台内经营者陷入内卷式过度竞争，但传统理论难解释、传统方案难奏效。其关键在纵向控制：平台对经营者价格决策权施加不合理约束，诱发低价竞逐与成本转嫁。治理上，应以法律规制与市场约束并行，聚焦遏制平台不当控制，恢复公平竞争秩序。

中国人民大学博士生**赵栩**围绕“数字时代个人电商经营者识别标准研究”主题，指出数字经济催

生“人的商个人化”，个人电商经营者识别成为现实难题。现有司法解释规定有限、适用边界与标准仍待细化。她主张回归实质判断：登记仅具确认效力；重构“营业性”标准；组织性、职业性非必要要件，改以持续性、反复性、计划性并结合频次、模式、品类等指标综合认定，并将“公开性”纳入实质审查。

中国政法大学博士生**洪一凡**围绕“论平台内容治理的‘用户决策性参与’——基于合作规制模式”这一主题，指出用户决策性参与缺位，致规制过度与不足并存。其因在既有思路忽视用户角色。她主张在合作规制框架下增强参与：通过公开征求与吸纳意见、宣传解读参与平台“准立法权”；以用户标记、判断嵌入“准行政权”；政府承担激励引导与监督约束双重职能，实现权利保障与治理效能兼顾。

西南政法大学博士生**张宇迪**围绕“算力产业经营者集中的反垄断规制研究”主题，指出算力资源高度集中带来潜在垄断风险与生态封闭，削弱创新并扰乱竞争秩序。她据算力市场自我修正受限与生态系统特性提出优化：事前审查完善启动机制、市场界定与竞争损害评估；事后救济实行分类分级结构性救济，行为性救济引入产业监管部门，并借助数字孪生开展场景模拟，以科学选择救济措施，促进行业健康发展。

中央财经大学博士生**肖浩然**围绕“平台企业用工数据报送的义务证立与规则型构”主题，指出数据报送义务系数字时代雇主法定义务延伸，数据承载公共利益决定平台应承担协助义务。其规则建构强调必要与目的限制，合理设置时限程序、避免过重负担；采取“常规信息及变动定期主动报送、非常规信息按需被动报送”的混合模式；并以清晰责任机制与安全保障约束平台与政府，防范泄漏风险，实现合规监管与公共利益协同。



专家评议环节，中国人民大学法学院教授**熊丙万**认为，本单元六位博士生选题“颗粒度高”、问题意识鲜明，能够回应数字经济发展中的真实议题。就何焯“借名直播账号”研究，他肯定以添附加工规则类推讨论的方法的启发性，并建议细化争议结构：区分“借名人一出名人”权属争议与“平台—用户”网络服务合同关系，澄清“被添附”对象究竟是债权债务关系中的权利还是更接近商号权益。同时提示对“效率优先、兼顾公平”需更精确论证，说明二者在场景中能否同步实现。就王嘉徽的研究，他建议明确规制路径是偏规制、偏市场或“双管齐下”，结合电商法厘清责任，并补充价格法与竞争法/反垄断法在执法中的衔接，以消费者福利等维度强化解释与规制论证。

北京交通大学法学院副教授、数据法学研究中心主任**付新华**认为，赵栩与洪一凡两位同学选题问题意识鲜明、颇具启发。就赵栩关于个人电商经营者识别标准的研究，她指出“行为导向的灵活判断”可能导致尺度不一，建议把结论与操作路径讲透，可引入“三步综合认定”：先排除明显民事行为，再审查核心要素，最后允许以非营利目的等反证。同时建议加强案例实证，扩充判例样本，观察法院实际关注指标，提炼“隐形标准”，并压缩背景性铺陈、聚焦法律要件重构。就洪一凡关于“用户决策性参与”的研究，她提示需更细化可行性与风险防范：用户差异下如何实现实质参与仍具挑战；除技术工具外，还应就制度设计、责任豁免前提及适用边界作更严格论证。

对外经济贸易大学法学院助理教授**尚博文**认为，张宇迪与肖浩然两位同学论文聚焦前沿、论证扎实，具创新性与现实意义。就张宇迪关于算力产业集中反垄断规制的研究，他肯定文章系统呈现集中带来的垄断风险及对结构、创新、隐私与秩序的影响，并以错误成本理论、非经济价值目标与生态系统损害理论构建框架，提出复合审查标准与特殊申报机制等建议，尤其将生态系统损害理论引入算力分析，拓展传统单边/双边市场视角。同时建议提升严谨性：明确“算力产业/市场”等核心概念，强化理论之间的逻辑衔接，完善文献综述与问题提出以凸显学术增量。就肖浩然关于用工数据报送义务的研究，他肯定其从雇主义务延伸、数据公共属性与协助义务论证正当性，并提出以必要原则与目的限制界定范畴等思路；同时建议聚焦报送边界，讨论报送/共享链条中数据错误、更新不及时的责任配置，并加强与个保法、数据安全法等规范的衔接论证。



单元二：人工智能风险治理与归责方案

单元二以“人工智能风险治理与归责方案”为主题，由中国社会科学院法学研究所编审、《环球法律评论》编辑部主任**姚佳**教授主持。

中国人民大学博士生**何泽昊**以“追寻产品责任的替代方——从人工智能事故切入”为主题，指出学界多以产品责任应对 AI 安全隐患，但其回应工业社会信息失衡的逻辑在 AI 时代受限。经历史分析，他提出三条替代路径：瑕疵担保责任适配直销模式；过失责任借行业惯例缓解“黑箱”举证难；

绝对责任结合画像与订阅定价以降低道德风险与逆向选择。

中国政法大学博士生**逯政阳**围绕“告知同意规则在高校处理学生个人信息中的适用与限制”展开，指出高校在个保法中定位不明。借鉴德国公法人制度，他按学术/非学术事务划分高校—学生关系，并据此配置处理规则。针对学生信息权与学术自由冲突，提出以告知同意为调和：强化单独/书面同意，限制同意无效，并引入场景一致性理论设计分级分段同意与事后补救。

日本大阪大学博士生**魏琪**以 ChatGPT 为例，探讨“生成式人工智能服务提供者过失规制的归责路径”，指出生成式 AI 引发数据违规、违法内容等风险，责任应主要由服务提供者承担。她以新过失论重构注意义务：预见义务以一般提供者认知与技术水平为基准；回避义务贯穿全生命周期，研发嵌入伦理与数据质量控制，在使用阶段开展内容监控与风险提示，以平衡创新与规制。

中国人民公安大学博士生**邱光耀**以“区块链证据的真实性、关联性补强”为主题，指出相关裁判文书至 2025 年 12 月已近 3500 份，集中于知识产权与合同纠纷。区块链证据虽具分布式与可验证特征，但实践偏重真实性，忽视关联性与合法性。他提出两阶段鉴真：上链前审查来源与机制，上链后核验哈希与时间戳；并主张破除“技术即真实”，以相关性为准入底线并强化非法证据排除。

中国政法大学博士生**汪会瑶**聚焦“数字权利的发生逻辑与体系化建构”，指出数字权利具主体二元性、客体数据化与技术依赖性，源于数字文明转型及平台私权力扩张等权利诉求。她提出“数字人权—工具性权利束—场景化权利”的开放框架：以人的主体性与技术向善为原则，以数字人权为基础层，算法与数据权利束为核心层，场景化权利为衍生层。

首都经济贸易大学博士生**张锡汪**以“动态体系论下生成式人工智能风险监管的路径优化”为主题，指出分级分类监管标准僵化，全生命周期监管资源配置亦可能失衡。他引入动态体系论，提出“要

素一效果”优化路径：理念上兼顾动态响应与常态约束，对象上设置动态评价要素，规则上明确满足度与统计标准，并以裁量基准与类案指导作为中介，实现创新与权利保护的动态平衡。



评议环节，中国人民大学纪检监察学院**邓矜婷**教授重点评议何泽昊博士与逯政阳博士的发言。她肯定何泽昊研究的问题意识与论述的完整性，认为其突破产品责任路径依赖、提出替代方案契合AI事故特征；同时指出传统理论回应AI问题易陷“似是而非”，建议引入更精准的量化支撑以提升科学性与精准度。对逯政阳的研究，她认可其聚焦高校个人信息保护的现实意义与论证逻辑，建议进一步聚焦行政职责履职中的权力滥用，并结合纪检监察相关议题寻求突破，增强研究深度。

中国政法大学习近平法治思想研究院**宋烁**副教授重点评议魏琪博士与邱光耀博士的发言。她肯定魏琪聚焦生成式AI服务提供者过失规制的前沿性，建议细化责任主体的定义与分类，明确不同提供者的责任边界，并结合具体罪名展开分析，避免选题过宽以增强实操性。对邱光耀研究，她建议适度收束议题、聚焦核心问题，重点围绕区块链证据的实质审查规则，与传统电子数据及司法鉴定规则对比，突出区块链证据的特殊性，从而提升创新性与针对性。

对外经济贸易大学法学院助理教授**李昊林**老师重点评议汪会瑶博士与张锡汪博士的发言。他肯定汪会瑶研究的系统性与完整性，建议突出中国数字权利建构的国别特色，结合我国数字经济与法治实践，选取具体权利（如个人信息保护）深入解析

其发生路径，避免框架过于泛化以增强独特贡献。对张锡汪研究，他认可引入动态体系论的创新性，但指出部分概念新潮而阐释不足，建议厘清其与传统法理概念的差异，并以更易形成共识的话语表达，提升方案的可理解性与可操作性。

单元三：数智时代公共治理的革新与趋势

单元三以“数智时代公共治理的革新与趋势”为主题，由中国政法大学比较法研究院副院长、教授、《比较法研究》常务副主编**孙海波**主持。

对外经济贸易大学博士后**谭伟杰**以“论数智时代的法律：从技术法律观到实践法律观”为题，意欲明确数智时代法律观。他指出法律实践面临事实与规范不对称，两类技术法律观各有偏失：转译型强调将法律转成技术指令、法律先行介入；扩张型试图将技术指令纳入法律体系、淡化预设规范。为避免“要么偏规范、要么倒向事实”，他主张实践法律观：区分法律1.0（预设规范）与法律2.0（续造且具约束力的法律），由1.0出发按事实需求动态续造，实现规范与事实融合。

中国人民大学博士生**王懋祺**以“人工智能算法删除责任的规范构成”为题，探讨模型出现问题时能否要求部署者、开发者删除模型本体。他指出仅靠侵权或刑事责任易出现“人被罚而模型仍在运行”，因此提出“算法删除责任”（追缴/销毁）：当模型存在显著合法缺陷时，强制销毁、删除或重新训练。其研究梳理必要性、境外实践与我国规范基础及边界，并借鉴美国FTC两阶段监管与欧盟梯度化措施，建议我国沿权益保障型与缺陷矫正型双路径建构，并细化要件与执行机制。

上海交通大学博士生**施文予**以“数据流通视角下实质性替代规则的司法价值”为题，聚焦数据抓取中的权益平衡。她指出实质性替代规则虽存在标准不清等局限，但可解释竞争损害客体与权利保护的衔接。为增强规则在数据流通场景的可用性，她将其类型化为“抓取即产品”和“抓取即原料”两类不正当竞争行为，分别适用一般性与特殊性要

件，以扩大法益衡量维度，进而拓展实质性替代规则的司法适用价值。

山东大学博士生**张滕**以“裁判语境中法律解释的数字化转型”为题，从静态载体数据化与动态过程计算化两维度提出路径。他强调解释数字化本质是定量分析，但须以定性分析为基础并服务规范判断。数据层面可通过案例群构建数字支持系统，辅助文义与社会学解释；动态层面可借助双向计算模型择取更优解释结论，但应确保计算规则与法律思维衔接，计算结果仅作认知参考，不能替代裁判。

天津大学博士生**张弛**以“未成年人数字身份验证的平台义务构造”为题，指出平台虽法定验证义务，但实践存在验证被动、一次性通过率高、身份冒用多发等失灵现象。为此他提出建立分级验证机制，依据服务类型与用户风险动态调整验证强度，并综合运用年龄核实、年龄评估与年龄声明等手段，构建过程与效果并重的验证体系，将身份验证定位为未成年人网络保护的系统性起点。



评议环节，中央财经大学法学院副院长、副教授**殷秋实**对前两位发言人进行点评。针对谭伟杰博士的研究，殷秋实副教授指出实践法律观若具有方法论普遍性，则对传统法学亦具整合价值，但需进一步澄清“什么是法”这一前提性问题；对王懋祺

博士的研究，建议明确其研究定位，即究竟是对现行法的解释还是新规范的创设，并建议依据文章重点确定分析详略。

北京师范大学法学院副教授**郭晔**评议第三、四位发言人的论文。郭晔副教授对张滕博士的研究区分数据化形式与过程、定性与定量的思路表示肯定，但指出缺乏实例支撑易使论证趋于理想化；对施文予博士的研究，郭晔副教授赞同其对抓取模式的类型化分析，但认为文末回归不正当性判断，偏离了对实质性替代标准的具体建构，建议进一步明确司法适用路径。

中国政法大学人权研究院（当代法治研究院）讲师**王也**点评张弛博士的论文，指出平台动力不足是验证失灵的关键，仅强调平台义务略显单一，应纳入家长与未成年人行为等因素进行系统考察；并指出，身份验证应与内容审核、分类管理等环节衔接，形成协同治理机制。



单元四：数据治理的新路径与新趋势

单元四以“数据治理的新路径与新趋势”为主题，由北京外国语大学法学院副院长、教授**万方**主持。

中国政法大学博士生**王小源**以“数字时代公共数据授权运营的风险挑战与刑法应对”为题，指出公共数据常涉国家安全、公共安全等重大法益，应将其刑法保护作为独立议题。在相对数据控制模式下，他提出“一阶本体安全+二阶功能安全”的二阶框架；并就功能法益按侵害主体区分内部侵害与外部侵害的规制路径，强调对个人信息、财产与市场秩序等利益实行前置化保护。

上海交通大学博士生**牛钰彤**以“数据跨境流动视阈下的主权嬗变：从属地主义到功能主义”为题，指出各国普遍“严出宽进”，规则差异致全球治理碎片化，并引发管辖权冲突与数字贸易壁垒，使我国跨国平台面临双重合规风险。她主张数据主权转向功能主义，强调以实质安全合规替代数据本地化；并建议细化分类分级分区规则，强化基础设施与安全技术，通过多边合作参与规则协商以化解冲突。

西南政法大学博士生**樊皓**以“政府数据授权运营收入的预算约束与制度建构”为题，指出授权运营推动政府数据由行政内部走向市场循环、由免费开放走向增值利用，但预算制度对相关收入形成多重约束难题。他提出构建特殊预算框架：零基预算编制、嵌入主动监督、厘清衔接边界；实行任务导向列式收支预算并明确财政部门参与；细化复式预算管理，将成本性收入与盈利性收入分别纳入不同预算盘子，并建立跨部门协调与共享机制。

中央财经大学博士生**黄一川**以“国家所有制度下公共数据产权的法律构造”为题，提出公共数据产权应采“公私法协同”框架：初始归属由宪法、行政法确认国家所有与行政机关主导；具体实现层面由私法搭建市场化规则以容纳私主体利用。他主张区分信息来源者与数据生产者、控制者、使用者四类主体，通过产权结构性分置的授权机制，明确持有者、使用权与经营权边界，并强调国家所有不等于国家垄断，国家负有成果共享与防侵害义务。

武汉大学博士生**彭紫婷**以“深度伪造性影像的刑法规制”为题，以2017年Reddit事件为引，分析深度伪造通过对抗网络生成高度逼真影像的技术逻辑，指出现有刑法规制易忽视个人法益、评价不足。她将深度伪造界定为未经授权却具高度真实外观的“数字再现”，系对身份的虚构性模拟与人格形象扭曲，直接侵害人格权。据此主张构建专门规制体系，明确对象、方式与主观要件，并设计入罪路径及正当化事由。

中国人民公安大学博士生**王丽爱**以“数据侦查法律性质的判定标准”为题，指出数据比对、轨迹

重构等已成基础侦查工具，但传统“强制—任意”二分法在数据侦查中失灵，且我国缺乏性质判定标准，导致程序规制失去起点。她比较美“合理隐私期待”、德“信息自决权干预标准”、日“重要权益侵害说”，提炼以基本权利干预强度为核心要素，构建同心圆结构，并提出两阶路径：单一维度达质变阈值即属强制侦查；多维叠加产生“马赛克”质变亦认定为强制。



评议环节，清华大学公共管理学院长聘副教授、清华大学科技发展与治理研究中心主任助理**陈天昊**对第四单元发言人的论文进行评议。他指出，王小源关于公共数据授权运营的刑法应对，在实践尚未普及时过度预设风险并搭建复杂体系，可能脱离现实，应回到具体场景论证规制必要性。对牛钰彤研究，他建议澄清功能主义转向是实然还是应然，并强化理论论证与对策之间的对应关系。对樊皓研究，他认为公共数据收入入预算更偏会计议题，宜聚焦防范政府借授权运营“美化”资产负债表、滋生新债务风险。对黄一川研究，他肯定体系完整，但指出仅靠产权构造难解现实问题。对彭紫婷研究，他提示深度伪造风险不限于性影像，还涉名誉、身份等多元法益，需覆盖更全面场景。对王丽爱研究，他肯定其问题意识明确、方案较具可操作性。

清华大学智库中心助理研究员**刘云**点评第三位、第四位两位发言人的论文。针对樊皓博士的研究，陈老师指出数据短期内难成财政主要方式，研究应注意区分货币性与非货币性收入，预算编制方

法需与完不成预算的责任机制契合；针对黄一川博士的研究，陈老师认为因数据具有可复制性、非限制性、弱排他性，其将数据视为传统不动产存在误解，并指出主体权能划分需重新思考。

对外经济贸易大学法学院助理教授**周瑞珏**对第五位、第六位发言人进行评议。针对彭紫婷博士的研究，周老师建议应将技术逻辑、规制起点与不法内涵整合，加强与刑法规制衔接；针对王丽爱博士的研究，他指出应在问题提出部分明确数据侦查行为类型，围绕具体数据侦查实践活动论证，增强说服力。

会议闭幕式由对外经济贸易大学法学院助理教授**李依怡**主持，对外经济贸易大学法学院副院长、教授**张欣**作闭幕致辞。张欣教授对出席本次论坛的专家学者表示衷心感谢，感谢兄弟院校对本次论坛和对外经贸大学法学院、数字法学团队的长期支持。同时，张欣教授由衷感谢积极投稿、参会的博士生，本届论坛投稿数量多、质量高充分体现了青年学者对学术研究的热情以及对贸大法学院的信任，青年学者的积极参与让“中国数字法学自主知识体系建构”的发展前景更加清晰、令人振奋。

中南大举办“人工智能生成内容的著作权保护”学术沙龙

2026年1月9日上午，中南财经政法大学知识产权学院、知识产权研究中心在文泓楼一楼报告厅成功举办“人工智能生成内容的著作权保护”学术沙龙，聚焦人工智能技术发展背景下著作权保护的前沿争议与实践难题，吸引了校内外学者、司法实务界人士及师生代表参与，现场交流氛围热烈。本次沙龙由中南财经政法大学知识产权学院副院长**徐小奔**教授主持，英国牛津大学知识产权研究中心主任**德夫·甘吉**教授、中南财经政法大学知识产权学院院长**黄玉烨**教授、**刘云开**副教授、**李安**老师、**杨依楠**老师，湖北省武汉市东湖新技术开发区人民法院审判员**许冬冬**担任与谈嘉宾。



德夫·甘吉 牛津大学知识产权研究中心主任、教授

德夫·甘吉教授以“Training AI Models: Copyright Implications”为题发表主旨演讲。他围绕英国最新判例“Getty Images 诉 Stability AI 案”展开深度解析，详细梳理了案件核心争议，指出案件的关键分歧集中在“模型是否构成侵权复制品”“训练行为的管辖权认定”“输出内容与原始作品的相似性判断”三大问题。他介绍，英国法院最终采纳了被告方观点，认定 AI 模型仅存储统计关系，未再现原始作品的核心特征，不构成侵权复制品；而训练行为因发生在英国境外，规避了管辖权约束。此外，他还对比了德国“GEMA 诉 ChatGPT 案”的相反判决，德国法院认为模型可通过提示词还原完整歌词，构成记忆性复制，应认定侵权。通过两大判例的对比，甘吉教授揭示了全球范围内 AI 版权保护的司法分歧，引发了现场对技术特性与法律适用关系的深入思考。



黄玉烨 中南财经政法大学知识产权学院
院长、教授

与谈环节中，**黄玉烨**教授指出 AI 技术对版权制度是“挑战而非颠覆”，著作权法的基本理念与原则仍需坚持，但需针对技术特性进行制度调试。她以中国“奥特曼图形”相关案例为例，介绍了司

法实践的探索：广州互联网法院认定 AI 平台专门输出侵权图形构成侵权；杭州互联网法院则认为用户上传图片用于模型训练不构成侵权，但商业性输出需承担责任，两个案例均体现了利益平衡的核心思想。她强调 AI 版权保护需加强理论与实践对话，学者应关注司法实务中的成本困境与裁判逻辑，司法者也需吸收学术研究的技术洞察，共同构建适配中国产业发展的制度框架。



徐小奔 中南财经政法大学知识产权学院
副院长、教授

徐小奔教授系统梳理了 AI 生成内容著作权保护的两大核心争议：一是训练阶段，作品用于数据训练是否构成复制权侵害；二是输出阶段，生成内容是否构成著作权法意义上的作品，以及与在先作品相似时的侵权认定标准。结合甘吉教授介绍的英美判例，他强调法律应正视 AI 作为辅助创作工具的普及事实，既要避免过度限制技术应用，也要防止漠视在先权利人合法权益，需在权利人与开发者、使用者之间重塑共赢的利益关系。



李安 中南财经政法大学知识产权学院讲师

李安老师将目光投向技术迭代与侵权争议的关联，提出当前 AI 输出内容的实质性相似争议，

本质是技术不成熟阶段的“记忆复制”现象。随着技术发展，模型的内容转化能力将持续提升，记忆复制问题会逐渐弱化，因内容高度相似引发的侵权争议也将逐步解决。李安老师强调，AI 版权保护需预留制度弹性，模型从“笨拙”到“智能”的进化依赖多元数据供给，法律规制不应因过度限制训练数据使用而阻碍技术进步，应聚焦长期平衡而非短期争议。



刘云开 中南财经政法大学知识产权学院院长、副
教授

刘云开副教授从 AIGC 输出端切入，聚焦版权定性与侵权责任分配问题，认为 AIGC 应采用版权保护模式，反对将其纳入公有领域或采取分类审核模式，认为这两种模式要么违背市场交易逻辑、降低用户创作积极性，要么执行成本高昂、缺乏实践可行性；他提出人工智能时代可适度突破著作权法人格理论，秉持实用主义哲学观，只要有人类参与且 AIGC 与现有表达存在差异即可给予版权保护，而在侵权责任方面，因 AIGC 生成逻辑与传统规则适配性不足，无过错责任仍有适用空间，搭配停止侵害请求权限制与防御机制可实现著作权主体与 AI 产业主体的利益平衡。



杨依楠 中南财经政法大学知识产权学院讲师

杨依楠老师提出“著作权法是技术之法”的核心主张，认为人工智能技术已从底层逻辑颠覆传统著作权制度的适用前提，机器阅读替代人类阅读、海量作品的微量价值贡献替代单件作品的深度利用、概率映射关系替代直接复制关系，传统侵权认定路径已难以适配。他强调，AI时代需探索新的作品交易模式与许可机制，在保障作者权益的同时，降低模型训练的合法许可成本；著作权法功能应向职业创作场景聚焦，正视作者劳动力转移现象，通过制度创新实现技术发展与权利保护的动态平衡。



许冬冬 湖北省武汉市东湖新技术开发区人民法院
审判员

许冬冬法官结合司法实务分享观点。他以2023年武汉首例AI文生图案为切入点，指出当前AI图片类纠纷呈现“数量多、标的小、裁判少”的特点——多数纠纷通过商业和解、撤诉解决，真正进入司法裁判视野的案件有限。许冬冬法官表示，AI生成内容的著作权保护仍处于立法与裁判规则未明确的探索阶段，核心争议集中在“思想与表达的分界”：人类提供素材、AI加工润色的创作形式是否应受保护，不同法院存在观点分歧。他提到，韩国已明确“有人工因素介入且人类提供主要素材”的AI作品受版权保护，而中国司法实践中，市场逻辑在消化部分纠纷，暂时未出现大规模诉讼潮，未来需平衡司法成本与权利保护的关系。

上海市法学会网络治理与数据信息法学研究会2025年年会暨“网络平台版权侵权责任”学术研讨会成功举办

开幕式

2026年1月25日，上海市法学会网络治理与数据信息法学研究会2025年年会暨“网络平台版权侵权责任”学术研讨会在上海交通大学凯原法学院成功举办，上海市法学会专职副会长施伟东、上海市法学会网络治理与数据信息法学研究会会长孔祥俊，以及来自北京大学、同济大学、华东政法大学、浙江省高级人民法院等单位的专家学者出席了本次研讨会。本次研讨会由上海交通大学知识产权与竞争法研究院、同济大学上海国际知识产权学院承办。

上海交通大学讲席教授、知识产权与竞争法研究院院长、网信法研究会会长孔祥俊首先作开幕致辞，对出席的各位嘉宾表示衷心的感谢和热烈的欢迎。他指出，过去一年，研究会上海市法学会的指导下，严格按照计划和法学会的要求，开展了一系列活动与工作，始终秉持服务国家战略和地方发展的宗旨，在数字治理、平台经济法制等前沿领域深耕细作，努力发挥专业智库的独特作用。随后，就本次年会聚焦网络平台版权侵权责任这一核心议题，他提出信息网络传播权的产生是网络时代撬动知识产权规则变革的关键起点，自上世纪90年代起，该领域便在国际范围内引发持续关注与制度演进，美国、欧洲等地相继形成各具特色的规则体系，我国也在立法与司法层面逐步构建起适应本土发展的制度框架。他进一步提出，历经二三十年发展，传播技术、产业形态与版权生态不断变化，相关法律的核心逻辑与利益平衡机制仍需“变”与“不变”、“守正”与“创新”之间审慎把握。当前，在某种程度上，国际上已呈现出以美国、欧盟和中国为代表的三足鼎立态势，各国在平台责任、技术治理等议题上存在不同取向。在此背景下，深入探讨网络版权制度的底层逻辑与发展方向，具有重要的理论价值与现实意义。最后他预祝此次研讨会圆满成功。



孔祥俊 上海交通大学讲席教授、知识产权与竞争法研究院院长、网信法研究会会长

上海市法学会党组书记、专职副会长、《东方法学》主编**施伟东**出席会议并发表致辞。首先，他代表上海市法学会对本次年会的胜利召开表示热烈的祝贺，向莅临会议的各位专家学者与业界同仁表示诚挚的欢迎和感谢。随后，他指出当前平台经济发展已经成为生产力发展的重要引擎。习近平总书记多次强调，要妥善处理平台活力与经济秩序，创新发展与风险规范，平等保护与平衡保障的关系，推动平台经济规范健康持续发展。上海是我国改革开放的前沿窗口，也是平台经济最为活跃，要素聚集度最高的区域之一。对此，他充分肯定了本次年会聚焦网络平台版权侵权责任这一主题进行深入研讨，具有深刻的理论前瞻性和现实紧迫性。他还指出2025年上海市法学会网络治理信息法学研究会，在理事会特别是孔祥俊会长的带领下，完成了很多卓有成效的研究工作，并对研究会2026年的进一步发展提出了殷切期望。最后，他也期待与会各方通过此次研讨，能取得更为丰硕的研究成果。



施伟东 上海市法学会党组书记、专职副会长、《东方法学》主编

年度观察

华东政法大学教授、网信法研究会副会长**王艳芳**作了关于网络平台注意义务认定的演讲。她基于2025年北京、上海、浙江、江苏、广东、湖北、重庆等法院近26份典型司法文书和4篇核心文献，从审查义务、注意义务与过错认定、明知应知的认定、盈利对侵权行为判定的影响、合格通知的认定、必要措施的认定，以及平台通知规则与用户个人信息保护之间的关系等方面进行了系统梳理。从收集到的文书来看，法院普遍认为平台对侵权行为不承担一般性的审查义务，责任认定需回归具体过错判断。她提出，从近年司法案例和文献研究看，平台责任整体仍与2012年的司法解释基本契合，未出现明显加重倾向，法律逻辑和法律价值始终保持稳定。



王艳芳 华东政法大学教授、网信法研究会副会长

浙江高院知识产权庭庭长**王亦非**结合2025年司法实践，对“必要措施”认定标准作出系统解读。她指出，网络平台版权侵权场景出现了案件主体、侵权行为和案件争议焦点的三大新变化。她总结了三类新型场景的司法探索，即短视频及算法推荐场景、云盘和网盘服务场景、生成式人工智能场景。她指出，对于必要措施的认定，目前呈现出标准难以统一、边界难以把握和利益平衡难以实现的复杂态势。她强调，必要措施认定核心在于“守正与创新”，在保持制度的必要性和标准的动态性的同时，应当建立及时、有效、合理的审查框架。未来需要强化司法裁判的规则引领作用，构建数字生态中协同共治的格局。



王亦非 浙江高院知产庭庭长

北京大学法学院教授**刘银良**从惩罚性赔偿制度的渊源引入，指出惩罚性赔偿本质是“准刑事责任”，核心功能在于惩罚与威慑；惩罚性赔偿在维护公共秩序的同时，也暴露出合理性和不合理性共存的问题。他指出，大陆法系国家普遍缺失惩罚性赔偿制度，英美法系国家对该制度的适用也受到严格限制；我国当前在知识产权领域引入惩罚性赔偿，存在过度扩张风险，知识产权的模糊边界易导致惩罚性赔偿制度的过度威慑。因此，在法律适用上应当严格限制适用范围，并警惕行政与刑事责任的叠加；科学处理补偿性赔偿与惩罚性赔偿的倍数关系等问题。



刘银良 北京大学法学院教授

主题论坛

议题一“过滤拦截的技术和成本问题”，由蚂蚁集团首席隐私官、网信法研究会副会长**聂正军**主持。北京林业大学教授**刘宁**，抖音集团法律研究中心研究员**赵一洲**，冠勇科技创始人兼 CEO **吴冠勇**，集佳上海分所主任、网信法研究会理事**李文红**依次作主题发言。华东政法大学特聘副研究员、网信法研究会理事**童云峰**，网信法研究会理事**谭俊**进行评议。

议题二“注意义务认定问题”，由上海知识产权法院二庭庭长、网信法研究会理事**钱光文**主持。武汉中院知产庭副庭长**周书博**，广州知识产权法院三级高级法官**江闽松**，上海徐汇法院知产庭副庭长**于是**，上海松江法院商事庭审判长**毛水龙**依次作主题发言。上海市市场监管局价监竞争处副处长、网信法研究会理事**黄伟丰**，上海市高院知产庭三级高级法官、网信法研究会理事**朱佳平**进行评议。

议题三“侵权损害赔偿问题”，由同济大学上海国际知识产权学院教授、网信法研究会理事**许春明**主持。南京中院知产庭庭长**徐新**，杭州中院知产庭法官助理**项一城**，同济大学法学院教授、网信法研究会理事**袁秀挺**、腾讯集团视频版权维权负责人**谭乃文**依次作主题发言。苏州知识产权法庭副庭长**徐飞云**，华东政法大学知产院副教授、网信法研究会理事**兰磊**进行评议。

（技术编辑：吕昊然）

数字法评

论人工智能时代肖像可识别性的判断标准

此处删除了原文脚注，全文请参见《法学家》2026年第1期，转载或引用请注明出处。

作者：阮神裕

内容提要：肖像可识别性要件发挥作用的典型场景，主要集中在争议形象“去面部特征”的肖像权纠纷中。随着人工智能生成虚拟形象的广泛应用，肖像可识别性要件越发凸显其重要性。“综合判断法”过度依赖法官自由裁量权，不仅导致法律适用的不确定性，而且忽视了肖像权所要保护的不同法益对可识别性判断标准的差异化要求，难以成为理想的判断路径。肖像权保护的终局性法益包括尊严利益、同一性利益和财产性利益。针对不同法益，肖像可识别性的判断标准亦应有所区分：在保护尊严利益时，应当采取最为宽松的标准，只要肖像权人本人可以识别即可；在保护同一性利益时，应当以一定范围内的熟人可以确信争议形象只能是肖像权人为准；而在保护财产性利益时，则应当采用最为严格的标准，即在隔离对比的情境中，社会公众能够一眼认出争议形象为肖像权人，由此形成肖像可识别性的多元化判断标准体系。

引言

在前人工智能时代，肖像通常通过摄影、摄像、雕塑或者绘画等方式固定于一定载体上，其核心功能在于反映特定自然人可被识别的外部形象。这类外部形象往往直接呈现了自然人的真实面貌。因此在司法实践中，肖像的可识别性要件逐渐淡化。只有在个别“去面部特征”的场景中，肖像的可识别性要件才会成为争议焦点。然而，在人工智能时代，随着信息技术的迭代和艺术创作手段的多样化，肖像的表现形式日益复杂。AI换脸、数字人产品、AI生成卡通图像以及合成语音等技术，催生了大量虚拟形象，这些虚拟形象在生成过程中可能依赖于真实肖像，但是其输出结果又不完全等同于原始肖

像。肖像信息的来源主体主张该虚拟形象侵害其肖像权时，肖像的可识别性遂成为裁判的核心争点之一。可以说，在人工智能时代，肖像的可识别性问题的理论与实务意义较之以往更显重要。

在现有理论研究中，对于肖像可识别性问题的主流解决路径可以被总结为“综合判断法”，即考虑争议形象呈现的方法、特征、场合、相关文字说明等客观要素，以决定其是否具备可识别性。该方法固然可以应对绝大多数的肖像权纠纷，但由于过度依赖法官自由裁量，难免带来法律适用上的不确定性。本文拟在既有研究的基础上，推动肖像可识别性问题往法律确定性的方向发展，即建构一个以肖像权所欲保护法益类型为基点的多元化判断标准体系。为此，本文将围绕以下三个核心问题展开论证：其一，肖像可识别性的判断难题通常发生于何种场景？其二，肖像权究竟旨在保护哪些终局性法益？其三，为更有效保护上述法益，应如何建构肖像可识别性的判断标准？

一、肖像可识别性的判断难题

肖像可识别性作为肖像权的核心要件之一，在大多数直接使用完整面部形象的案件中并不构成实质争议，因而在早期司法实践中其重要性一度被淡化。然而，随着“去面部特征”的争议形象不断出现，尤其是在人工智能生成虚拟形象、AI换脸、数字人等新型场景中，肖像可识别性问题越发成为裁判关键。然而，理论上占主导地位的“综合判断法”似乎无法充分解决有些肖像可识别性的认定难题。

（一）肖像可识别性发挥作用的场景

肖像是特定自然人可以被识别的外部形象。通常认为，外部形象不以面部形象为限，只要外部形象可以识别出特定自然人，应当受到肖像权的保护。在实践中，争议形象包含面部特征的，可识别性不成问题，无需详加检讨；但是，争议形象没有面部特征的，其可识别性问题就会成为争议焦点。可以说，肖像的可识别性发挥作用的场景，主要是争议形象“去面部特征”的场景，具体包括：

其一，争议形象包含部分面部特征，或者面部

以外之其他身体特征。争议形象中的面部特征不完整的，肖像可识别性往往成为争议焦点。例如，在被告使用一幅只有眼部以下的局部面部特征的照片用于商业广告的案件中（“叶璇案”），该照片是否满足肖像的可识别性要件，乃是该案争议焦点。又如被告发布的照片中只有眉眼部的影像、照片中的人物佩戴口罩，照片中的人物眼部作了马赛克处理的，或者被告发布的照片是侧面照等情形，可识别性要件亦是核心争点。此外，争议形象包含面部特征以外之其他身体特征的，如被告使用的照片涉及原告的背影、被告在网站上使用的是眼部以下至腰部以上局部照片等情形中，法院亦需判断争议形象是否具有可识别性。

其二，争议形象涉及妆造、服饰、剪影等非身体特征的元素。肖像权的客体范围甚至可以延伸至权利人身体特征之外的外在表现，如妆容、服饰或剪影等，只要这些元素具有典型性，足以成为识别特定自然人的依据，即应受到肖像权的保护。最为典型的案例是“迈克尔·乔丹与国家工商行政管理总局商标评审委员会商标争议行政纠纷案”（简称“乔丹案”），该案的争议焦点之一便是中国乔丹的商标图形部分的人体剪影是否可以识别出迈克尔·乔丹。又如在“AI换脸案”中，有的运营商未经同意在其应用程序或者网站上发布可供换脸的模板视频，消费者只需上传自己的肖像即可替换脸部信息、生成含有消费者面部特征的新视频。替换前模板视频含有原告完整的面部特征，当然具有可识别性；但是，替换后的新视频是否具有可识别性，不乏争议。有的运营商对模板视频进行了预处理，删去了其中的面部特征后提供给消费者，或者预先替换了视频发布者的面部特征。这些“去面部特征”的模板视频是否侵害肖像权，存在较大争议。一种观点认为，尽管预处理后的视频仅保留了身体形象，但是通过对比原视频素材，仍能通过未被修改的衣着服饰、肢体动作及相应场景细节识别出该身体形象乃是原告，因此认定预处理后的视频具有可识别性。相反观点则认为，经过删除或替换面部特征的预处理，衣着服饰、肢体动作以及相应的场景

细节不具有可识别性。由此可见，涉及妆造、服饰、剪影等非身体特征的争议形象是否具有可识别性，在实践中仍有较大争议。

其三，争议形象是漫画、数字人产品等虚拟形象。在争议形象为漫画人物或者卡通形象的场合，因艺术表现与风格化的需要，其面部特征往往经过一定程度的“异化”处理，即通过夸张、变形或符号化的手法，脱离现实形象以增强视觉表达力，因此其是否具备可识别性，成为诉讼双方的核心争点。例如，有的卡通形象虽然没有标志性特征，但是配上了姓名、艺名或者昵称，使得涉案卡通形象的整体认知明确指向了肖像权人的，该卡通形象应当被认定为具备可识别性。又如，被告使用的卡通形象配上了“贾女士”以及打拳击的场景，加之原告主演的电影社会关注度极高，该卡通形象具有较强的可识别性。再如，一个卡通形象加上“您有才”及“咱不差钱”这两句经典台词作为旁白，可以认定该卡通形象可以识别出特定自然人“赵本山”。

值得注意的是，随着人工智能的飞速发展，肖像权的侵权纠纷呈现出了全新样态。例如，被告使用原告的声音信息训练文本转语音产品（Text—To—Speech），该产品的音色音调与原告声音高度相似，但是相比于视觉形象的辨认，声音的可识别性判断存在更大的争议（“声音权案”）。又如，被告使用生成式人工智能处理原告的真实肖像，将真实肖像转化为局部特征被异化处理的3D卡通形象，但是仍然保留相似的构图、服饰或者背景，该3D卡通形象的可识别性亦有争议（“AI生成图案”）。再如，使用人工智能训练生成的数字人是否具有可识别性，同样成为争议焦点（“数字人案”）。所谓数字人，是指通过AI技术，对采集到的真人视频进行处理，提取面部特征和声音特征，进而生成对应数字形象和声音的虚拟主体。根据数字人形象是否还原真人肖像，数字人可以分为两类：（1）有的平台致力于发展与真人形象高度相似的数字人，生成结果尽可能还原真人形象，该数字人形象若是没有取得真人同意，当然构成肖像权侵害。（2）有的平台则致力于随机生成全新的、虚构的数字人

形象，该生成结果不与特定自然人形象匹配。但是由于该数字人形象是基于真人肖像训练而成的，因此在一定程度上保留了真人的局部面部特征。于此场合，该数字人形象是否具备可识别性成为难题。

综上，肖像的可识别性问题往往出现在被告使用“去面部特征”的外在形象的场景。很长一段时间以来，此类场景在司法实践中只是偶有发生。在绝大多数肖像权纠纷中，被告未经同意使用的是原告的真实肖像，肖像的可识别性问题通常不会成为争议焦点。诚如“章某莱与蓝港在线（北京）科技有限公司人格权纠纷上诉案”的判决所云：“纵观二十几年的司法实践，涉及侵犯肖像权的纠纷多是与人的自然相貌紧密相关，即例如自然人的照片被擅自使用等情形，……久而久之，由于实务中涉及的侵犯肖像权的纠纷多是直接反映自然人的体貌特征，在适用法律时，肖像权中蕴含的可识别性也被逐渐淡化了。”尽管如此，随着人工智能技术的发展，AI换脸案、声音权案、AI生成图案和数字人案的出现，再一次凸显了肖像的可识别性的重要性。

（二）肖像可识别性的综合判断法及其问题

理论界在回答肖像的可识别性应当如何判断时，通常采取列举若干考虑因素交由法官自由裁量的综合判断法。例如有的论者主张，一方面应就争议形象呈现的方法、特征、场合、相关文字说明等客观要素加以综合认定，另一方面还应结合个人之交往范围、社会知名度等不同综合予以判断。又如“可识别性理论追求的是肖像与自然人外部形象之间的关联性，应就外部形象呈现之方法、特征、场合、相关文字说明等客观要件加以综合认定。”再如有的论者主张结合个人的面部特征、其他身体部分、肖像在图片或录像等载体中的位置以及所配图片、文字等进行综合判断。本文认为，综合判断法存在以下问题：

其一，综合判断法尽管具有一定的灵活性，但是缺少确定性和稳定性。综合判断法的优点是灵活性。诸如外部形象呈现之方法、特征、场合、相关文字说明等参考要素，只是以“论题目录”的方式

提示裁判者在具体个案中应当予以权衡，而未以法律规则的形式对裁判者作出事先指令，使得裁判者可以结合案件要素作出具体判断，最终作出合乎个案正义的裁判。

然而，综合判断法的灵活性也带来了一定的缺陷。一方面，若是裁判者在每次面临新的案件时，总是重新回到抽象的参考要素中，针对具体个案作出新的自由裁量，那么以往的裁判就没有发挥其指导性意义，不同的裁判者可能作出截然不同的裁量结果。上文提到的AI换脸案即属此例，同样是去面部特征的妆容、服饰和场景，有的判决认定其具有可识别性，而有的判决则认定其不具有可识别性。另一方面，肖像可识别性的判断容易受到人类认知机制系统性偏差的影响。肖像权人主张争议形象具有可识别性时，通常提供其肖像照片和争议形象进行比对。若按此种方式进行比对，裁判者很容易过分高估或者夸大肖像照片和争议形象的相似度，陷入“锚定效应”（Anchoring Bias）的系统性认知偏差，即裁判者先看到某一张照片，再对比另一张，第一张照片可能成为对比的“锚点”，从而影响对第二张照片的解读，使其更倾向于发现相似之处。在司法实践中，有的法院通过照片比对，发现肖像权人提供的肖像照片和争议形象具有同一性，据此认定争议形象具有可识别性。例如，伽美公司未经同意使用了眼部经过马赛克处理的女性照片，黄某提交了百度图片中的有关照片，证明该照片中的女性是其本人。法院对比两张照片后，发现二者具有同一性，据此认定眼部经过马赛克处理的女性照片具有可识别性。这一认定方法有待商榷。由于“锚定效应”的影响，在肖像权人提供肖像照片进行参照比对的场景下，争议肖像的可识别性程度将会显著高于社会一般人仅仅通过争议形象进行联想时的程度。

其二，综合判断法虽然需要考虑数个因素，但是其实质上遵循的是单一的肖像可识别性判断标准，没有根据肖像权所要保护的法益类型不同而采用不同的判断标准。

在论及肖像的可识别性时，当前学说通常不问

肖像权所要保护的法益为何，而是采取单一的可识别性判断标准。例如有的论者主张，只要特定载体所呈现的形象足以使人在该载体与某一自然人之间发生当然联想，那么就应当认定该形象具有可识别性，而不论该肖像为何种表现形式，以及肖像的呈现方法、手段或载体为何。肖像可识别性的单一标准，尤其体现在“识别主体”问题上。所谓识别主体，是指在判断争议形象是否可以识别出特定自然人时，应当由谁作出判断？一种常见的观点是，在判断肖像是否具有可识别性时，应当以社会一般人能否识别作为判断标准，即识别主体是社会一般人。也有观点主张，识别主体应当是“一定范围内的特定主体”，即肖像权人自身生活、工作范围内的群体作为识别标准。以上观点虽有差异，但是它们在识别主体的问题上均采取了单一标准。

只要稍微考虑以下两种情形，就会发现单一标准存在一定问题：情形一，原告的肖像被漫画化，内容涉及丑化和侮辱原告；情形二，原告的肖像同样被漫画化，不过该漫画只是用于常见商品的推广活动。两种情形均涉及可识别性的判断问题。假设原告不是名人，也没有什么显著特征，即便采取“一定范围内的特定主体”标准，也不足以识别漫画是原告。但是，原告本人可以识别出该漫画就是指向自己，尤其是考虑到该漫画创作者与自己具有一定的交往乃至过节，原告更加确信该漫画就是自己。按照该单一标准，两种情形中的原告都无法得到救济。然而在法感情上，不对情形一中的原告提供救济，似乎有违《民法典》人格权编保护人格尊严之宗旨。这个思想实验初步说明了，肖像权所要保护的法益对肖像可识别性的判断标准有一定的影响，后文将对此予以详述。

当然，不乏论者尝试对肖像可识别性问题进行类型化分析。一种常见的思路是区分名人和非名人认定可识别性。该思路结合不同案型将抽象的法律标准予以类型化，相比于“综合判断法”有所前进。但是这一类型化的思路存在两个方面的问题。一方面，在自媒体时代，名人与非名人之间的界限日趋模糊。今日还是默默无闻的某甲，明日可能因MCN

公司的包装推广而成为“网红”。在大多数人看来，不为人知的某乙，可能在某个特定领域拥有百万粉丝。另一方面，仅以肖像权人是否出名为依据进行类型化，忽视了肖像权保护的不同法益对可识别性判断标准的影响。例如，行为人使用生成式人工智能将某丙的真实肖像动漫化，但是因为人工智能技术不成熟，某丙的真实肖像被丑化为四肢不健全的动漫形象，即便是某丙之亲属、邻居或同事亦无法识别，此时若以该照片不具有可识别性为由不予救济，那么某丙的尊严利益将会受到严重侵害。

综上，在肖像的可识别性较少成为争议焦点时，“综合判断法”为法官的裁判和说理提供了指引。但是，随着该问题在司法实践中的逐渐积累，理论界就不应该仅仅满足于列举若干参考要素，而是要在总结涉及肖像可识别性的案件类型的基础上，对肖像可识别性的问题作出进一步的类型化。唯有如此，法律才能在实践中“生长”。

二、肖像可识别性判断标准的建构方法

在肖像可识别性成为争议焦点的疑难案件中，裁判者不得不进一步追问：肖像的可识别性判断应当遵循何种标准？本文尝试基于法益类型化的方法，建构针对不同法益之肖像可识别性的判断标准。为此，需要界定肖像权究竟保护何种法益。

（一）法益类型化视角下的建构路径

肖像可识别性的判断标准，是指裁判者在判断争议形象是否具备肖像权意义上的可识别性时应当遵循的标准。裁判者在判断肖像可识别性时，应当实施两个步骤的作业，第一步是明确肖像可识别性的判断标准，第二步则是判断具体个案是否符合该标准。综合判断法实际上没有回答肖像的可识别性应当遵循何种法律标准，其只是列举了若干参考要素供裁判者进行权衡。也就是说，综合判断法始终遵循单一判断标准，没有考虑保护不同法益时应当适用不同标准的可能性。例如，在判断肖像是否具备可识别性时，首要问题在于确定“识别主体”应当是谁。这正是肖像可识别性的判断标准所要回答的核心问题。然而，综合判断法往往将识别主体笼统地界定为“社会一般人”或“一定范围内的熟

人”。二者是否存在本质差别，以及在不同情境下究竟应当确立何种识别主体，仍有待进一步阐明。

肖像可识别性判断标准的建构，应当同时兼顾两个层面：一是肖像可识别性标准所要服务的规范目的，即肖像权所要保护的终局性法益；二是肖像可识别性的判断标准通常应当包含的要素。详言如下：

一方面，建构肖像可识别性的判断标准时，需要考虑肖像权所要保护的终局性法益。法律解释的基本前提在于理解法律规范的结构与功能。任何法律规范的设立，均非偶然，而是立法者基于特定社会关系的需要，为实现某种规范目的而创设。因而在法律解释的作业中，首先需要确定立法者所追求的规范目的，才能确定实现规范目的之适当且均衡的法律手段。肖像权的目的是，乃是保护肖像这一人格要素之上承载的终局性法益。正如程啸教授所言：“人格利益是人格权所保护的内容。对于自然人来说，人格权的最终目的都是维护人的尊严和自由，但是，不同的人格权所保护的具体的人格利益却是不同的。”可以说，《民法典》第1018条至第1023条共同服务于肖像权所要保护的终局性法益。《民法典》第1018条第2款对肖像的定义亦不例外，其中“可以被识别的”也应当契合肖像权的规范目的。肖像可识别性的判断标准的建构，亦应回到肖像权的规范目的，即立足于肖像权所要保护的法益，根据法益类型之不同，而适用不同的肖像可识别性判断标准。

另一方面，建构肖像可识别性的判断标准时，还需要明确其通常应当包含何种要素。结合理论与实践经验可知，肖像可识别性的判断标准通常涉及以下三个要素：（1）识别主体，即“谁”可以识别出争议形象为权利人的肖像。识别主体可能是肖像权人本人、一定范围内的熟人或者社会一般公众，对此下文将予以详细阐释。在此需要明确的是，肖像可识别性判断中的识别主体应当为“人类”，而非“机器”。这是因为：肖像权所要防范的风险，发生于肖像信息在社会交往中自由流通的场景，即肖像信息在违背权利人的意愿而被随意传播时，可

能引发的人格尊严遭到侵害、人格自由发展受到限制、身份发生混淆或社会评价失真等风险。故此，肖像的可识别性应当以人类识别为准。与此不同，个人信息权益所要防范的风险，乃是个人信息被大规模处理后引发的风险，即信息过度集中造成的、对信息主体的人格权益以及人身、财产安全的威胁。这种风险尤其体现在处理者使用信息技术手段进行大数据处理的场景中。在这个意义上，个人信息的可识别性可以采取机器识别的方法。（2）识别依据，即识别主体究竟依据何种特征来判断争议形象是否可识别。肖像的识别依据呈现出不断扩张的趋势。早期观点认为肖像仅指自然人的面部特征，不包括其他能够反映其外部形象的身体特征。但是《民法典》第1018条第2款并未作此限定，不论是面部特征，还是躯干、造型、衣着、发式、手势等均可成为识别依据。（3）肖像可识别性的判断标准还要界定明确识别程度，即识别需要达到何种程度才是肖像权意义上的可识别性。所谓的识别程度，是指识别主体根据识别依据在判断某一争议形象是否为特定自然人时，其内心在多大程度上予以确信。在不同情境中，争议形象的可识别性呈现出明显差异：有时识别主体可以一眼确认该形象必然对应某特定自然人，无需任何比对即可直接联想到该人；有时识别主体仅能产生怀疑，认为“可能是某人，也可能不是”，缺乏辅助手段便无法做出确定判断；而在可识别性最低的情形中，即便识别主体手持特定自然人的真实照片进行比对，仍无法得出该争议形象与该自然人相同的结论。建构肖像可识别性的判断标准，需要明确识别需达到何种程度。

综上所述，基于法益类型建构肖像可识别性判断标准，其实质是：根据肖像权所要保护的终局性法益之不同，针对识别主体、识别依据和识别程度进行一一界定，建构出契合不同法益保护需求的肖像可识别性的判断标准。

（二）肖像权保护的法益类型

在大多数肖像权纠纷案件中，裁判者没有必要深入检讨肖像权所要保护的法益为何，但是在疑难

案件（hard case）中，在判断系争行为是否侵害肖像权时，则应当回到肖像权所要保护的终局性利益。肖像权所要保护的利益，通常被笼统概括为精神性利益和财产性利益。本文尝试依据距离内心感受的远近将肖像权所要保护的利益进一步区分为尊严利益、同一性利益和财产性利益三类。

1. 尊严利益

《民法典》第1019条规定：“任何组织或者个人不得以丑化、污损……等方式侵害他人的肖像权。”根据这一规定，丑化或者污损肖像的行为，构成了对肖像权人的尊严利益的侵害，因而构成对肖像权的侵害行为。肖像具有标表功能，肖像代表权利人之人格，对肖像的丑化、污损，就是对权利人的尊严进行贬损，侵害了肖像权人的尊严利益。对此，《民法典》编纂工作人员撰写的释义中明确指出：“肖像权涉及肖像权的人格尊严，是具有极强精神属性的权利，以丑化、污损……等方式侵害他人的肖像权，都有可能对肖像权人的精神造成严重损害，必须禁止。除此之外，有的学者提出，在他人肖像上打叉或添画胡须、痣、疖、眼镜等，或焚烧、撕扯、倒挂他人的肖像等行为，损害了肖像权人在公众中的良好形象，影响了公众对其的良好社会评价，该行为同时侵害了他人的肖像权和名誉权。这一观点实质上建立在肖像权保护尊严利益的基础上。有的论者主张，丑化、污损他人肖像并未妨碍肖像的同一性，难以构成肖像权侵权，应当将其认定为侵害一般人格权。这一观点恐怕忽视了肖像权对尊严利益的保护。依体系解释之方法，《民法典》第109条规定“自然人的人身自由、人格尊严受法律保护”，紧随其后的第110条规定了各项具体人格权，这一体系安排表明具体人格权乃是人身自由与人格尊严的具体化。《民法典》第990条第2款规定“除前款规定的人格权外，自然人享有基于人身自由、人格尊严产生的其他人格权益”，亦表明了“前款规定的人格权”，即肖像权等具体人格权，乃是基于人身自由、人格尊严产生的人格权益。故此，肖像权实际上是人格尊严之具体化，因而具备保护尊严利益之功能。”

在司法实践中，著名的“冰心合影案”也凸显肖像权对尊严利益的保护。在该案中，被告利用原告与冰心的合影照片，经电脑技术将合影照片中原告躯体部分影像保留，头部影像更换成被告的头部影像，形成被告与冰心的合影照片，该照片被用于著作出版。原告主张其肖像权遭受侵害。二审法院均支持了原告的诉讼请求，其中二审法院的裁判理由是“维护肖像完整权，自然人对自己的肖像有维护完整性的权利，有权禁止他人非法毁损，维护自己的尊严，公民的人格尊严受法律保护。”尽管法院提到了维护肖像完整权，但是不能简单地将破坏、毁损肖像的行为都认定为侵害了肖像权，否则诸如保管不善等任何因过失毁损肖像载体的行为都将被认定为侵害肖像权。在该案中，法院之所以要保护“肖像完整权”，其终局性理由是：“在中华文化传统中，社会公众一般比较重视照片中自身影像的完整性，特别是将头部与躯干视为一个整体，不可分离，尤其忌讳将已成影像中的头部从躯干上人为地去除。根据这一观念，破坏肖像完整性的行为，具有贬损肖像所代表的人格的含义。法院所要保护的”肖像完整权“实质上是肖像所代表的尊严利益。”

值得讨论的是，是否可以将“维护肖像的完整权”单独作为肖像权所要保护的利益？这个问题随着人工智能的发展而日益突出。有的判决书认为，“被告将原告视频中的形象‘换脸’后上架供其注册用户换脸使用，破坏了原告肖像的完整性”，并且据此认定为对肖像权的侵害。这一观点有待商榷，肖像权的法律权能不应包括“肖像完整权”。“冰心合影案”虽然提到了维护肖像完整权，但是维护肖像完整权的目的是保护尊严利益。在二十余年前，“将影像中的头部从躯干上人为地去除”被认定为触犯了忌讳，因此侵害了权利人之尊严利益。但是，在美图秀秀、PS以及AI换脸软件等新兴技术广泛运用的今天，换脸行为不宜再像过去一样被认定为触犯了忌讳，从而构成对尊严利益的侵害。故此，纯粹的破坏肖像完整性不足以构成对肖像权的侵害，只有在破坏行为具有贬损权利人尊严

严利益的前提下，才能被认定为侵害肖像权。

2. 同一性利益

肖像作为人格的外在表征，具有显著的标表功能，其与权利人之人格之间存在稳定的联系。权利人肖像一旦被置于特定的社会语境中，往往会被解读为其本人持有某种观点、立场或品味。可以说，肖像就代表了一个人的人格形象。基于此，法律赋予自然人对其肖像一定的自主控制权，使其能够审慎决定在何种语境下允许其肖像被使用。倘若他人未经同意将权利人肖像置入某一语境，则可能导致社会公众基于该语境误将特定观点、立场或品味归属于权利人，引发“归属混淆”（Zuordnungsverwirrung），进而侵害权利人之人格同一性利益。同一性利益与上文提到的尊严利益有所不同。尊严利益是人之为他人享有的最为基本的人格利益，其保护的是肖像权的人格不受贬损的法益；对尊严利益的侵害方式表现为丑化、污损肖像。而同一性利益是指肖像与其主体具有形象同一性的利益，对同一性利益的侵害方式不一定是丑化、污损肖像，更加常见的是未经同意将肖像用于陌生语境中，从而使他人对肖像权人产生人格形象的误解或混淆。例如，在某大学的学术研讨会上，组织方未经许可，把一位教授的照片放在会议宣传海报上，并配上“××倡议”的字样。该教授从未公开表态过相关立场，但由于肖像与标语同时出现，社会公众会自然将这种观点“归属”到该教授本人身上。因而这一行为侵害了权利人肖像的同一性利益。

《民法典》第1019条第1款第1句规定“任何组织或者个人不得以……利用信息技术手段伪造等方式侵害他人的肖像权”。从历史解释的角度来看，该规定旨在保护同一性利益。随着现代信息科技的迅速发展，特别是语音合成、人脸替换、视频生成等人工智能技术的兴起，“深度伪造”（deepfake）技术使得“眼见为实”“有图有真相”的观念不再可靠，社会公众在网络中所见所闻往往可能完全虚构。深度伪造技术使得肖像权所保护的同一性利益面临前所未有的威胁。在轻微的违法行

为中，行为人利用深度伪造技术将人工合成的虚构音频嵌入肖像权人的演讲视频，使观众误以为其发表了相关言论，而这些言论可能严重违背其真实立场或观点。此类行为侵害了肖像权人的同一性利益。在严重的违法行为中，不法分子可能利用深度伪造技术生成虚假的色情视频，例如将明星的面部替换至色情演员的身体上。此类行为不仅侵害了同一性利益，同时严重侵害了尊严利益。《民法典》编纂过程中，有的单位提出：“利用信息技术手段‘深度伪造’他人的肖像、声音，不仅侵害自然人的的人格权益，严重的还可能造成恶劣的社会影响，危害国家和社会公共利益，建议法律对深度伪造技术带来的‘换脸’等问题予以回应。”全国人民代表大会宪法和法律委员会经研究，建议采纳这一意见。故此，《民法典》第1019条第1款第1句规定，任何组织或者个人不得利用信息技术手段伪造等方式侵害他人的肖像权，该规定所要保护的，正是肖像权人的同一性利益。

当然，肖像权保护同一性利益并非《民法典》第1019条第1款第1句所创。在“叶璇案”中，法院提到“这里所说的形象，是指原形人相貌综合特征给他人形成的、能引起一般人产生与原形人有关的思想或感情活动的视觉效果”。法院认为，被告使用的照片只显示了原告的鼻子和嘴等部分面部特征，该照片不是法律意义上的肖像。这是因为，该照片既不能反映特定人相貌的综合特征，也不能引起一般人产生与特定人有关的思想或感情活动”。其中第一个理由指向的是争议照片与权利人肖像的客观相似性，而第二个理由则指向了肖像权的保护目的，即肖像权旨在保护社会公众产生的、与特定人有关的思想或感情活动。在德国法中，肖像权之所以受到法律保护，是因为现实中存在“将一个人在特定情境中的形象与其本人相剥离，并在任何时候向无法预测的人群加以复制，以及随着情境的变化改变图像表达的意义的可能性。”上述案例中提到的肖像可以引起社会公众关于特定人的思想或感情活动，就是肖像所具有的同一性利益的具体表现。”

3. 财产性利益

在人格权的“一元保护模式”下，肖像权等特殊人格权既保护精神利益，也保护财产性利益。肖像之所以具有财产价值，源于其所承载的人格形象本身具有独特的商业吸引力。尤其是明星的肖像能够引发社会公众的关注，从而推动相关产品或服务的消费。正因如此，法律将肖像所产生的注意力效应及其所转化的经济利益，归属于肖像权人所有。他人若未经许可擅自使用他人肖像，即是在攫取原本应当由肖像权人享有的财产性利益，因而构成对肖像权的侵害。

对于肖像权所要保护的财产性利益，需要注意的是：一方面，该财产性利益，不同于尊严利益、同一性利益。他人未经同意使用明星肖像用于正面产品的广告代言，并不会侵害肖像权人的尊严利益。尽管该广告代言可能因不符合肖像权人的观念或者品味而侵害同一性利益，并且可能造成一定的精神痛苦，但不会直接剥夺本该归属于肖像权人的经济利益。美国法直接区分了公开权和隐私权，其中公开权之所以应受保障，乃在激励个人投资，收取其努力的回报，而与个人情感的保护几乎没有关联。另一方面，该财产性利益应当来自肖像所具备的吸引注意力的功能，而非肖像作为原始数据的数据价值。后者应当纳入个人信息权益或者数据来源者权中进行保护。例如，有的企业未经授权将原告发布的国风视频进行“去面部特征”的预处理，再制作成视频模板，供消费者替换为自己的面部特征，从而生成新的国风视频。该预处理行为是侵害肖像权，还是侵害个人信息权益？又如，有的企业未经自然人同意，使用自然人的肖像视频训练“数字人”产品，提供给消费者自主生成口播特定内容的“数字人”视频。假设数字人产品不具有可识别性，该企业未经同意使用肖像视频进行训练的行为，应当被认定为侵害肖像权，还是侵害个人信息权益？对此，本文主张以上训练行为侵害的是个人信息权益或者数据来源者权利，而非肖像权。这是因为：肖像权的财产性利益，应当来自肖像所具备的吸引注意力的能力。但在以上案中，训练行为

并非利用肖像获取注意力进而盈利，而是将肖像作为数据进行训练，故此，该行为并未攫取本该归属于肖像权人的财产性利益。

综上，肖像权保护的法益可以进一步细分为尊严利益、同一性利益和财产性利益。当然，上述法益之间具有彼此牵连、相互交叉的关系。一项加害行为可能同时侵害多种法益。如未经同意将肖像用于广告代言，既在该肖像与某种商品之间建立联系，使人误以为肖像权人使用、欣赏或喜欢该项商品，侵害了同一性利益；也褫夺了本来应当归属于肖像权人的财产性利益。又如，将某一明星的肖像替换到色情作品中，亦同时侵害了尊严利益和同一性利益。

三、肖像可识别性判断标准的具体展开

肖像权所要保护的法益包括尊严利益、同一性利益和财产性利益。在肖像可识别性成为争议焦点的疑难案件中，裁判者需要回顾肖像权所要保护的终局性法益，根据法益类型之不同，适用不同的肖像可识别性判断标准。唯有如此，方可最大限度地实现肖像权的规范目的。

（一）保护尊严利益之肖像可识别性判断标准

肖像权所要保护的法益，首先是尊严利益。肖像代表人格，丑化、污损肖像，就是侵害肖像权人的尊严利益。他人通过丑化、污损肖像或其他方式贬损尊严利益时，肖像的可识别性应当采取“本人识别”标准。详言之，识别主体应当为肖像权人本人，只要肖像权人本人识别，即便他人无法识别，亦可认定为具有可识别性；识别依据应当仅限于肖像权人的面部特征或者其他身体特征，不得扩张至肖像权人的妆造、服饰或者剪影等，即一个人不能因为自己惯用的妆造被人丑化而主张肖像权受到侵害；而识别程度则应当采取最为严格的、百分之百确信争议形象是肖像权人的程度。

上文提到，“冰心合影案”实际上保护了肖像权背后的尊严利益。二审法院之所以认定被告实施的“换头”行为侵害了肖像权，是因为在中华文化传统中，社会公众一般比较重视照片中自身影像的完整性，尤其忌讳将影像中的头部从躯干上人为地

去除，因此被告实施的行为因为触犯忌讳而被认定为侵害了肖像权。这个裁判理由实际上保护了肖像权背后的尊严利益。但是，该案判决书没有检讨案涉争议形象，即原告的躯干与被告的头部组合成的照片，是否具有肖像可识别性。通常而言，除非原告的躯干具有显著特征，否则常人难以根据案涉争议形象识别出原告。事实上，二审法官在评论该案件时，明确指出：“肖像最基本的功能是识别功能，一审法院将不具有识别特征的躯干作为肖像归类于法律保护的范畴，显然在语义上存在逻辑错误。”

问题在于，倘若“冰心合影案”中的争议形象真的不具有可识别性，任何主体均无法从争议形象中识别出原告，那么该案二审何以判决被告行为侵害了原告肖像权？在本文看来，二审法院实质上采取了一个不同于一审法院的可识别性的判断标准，即“本人识别”的标准。若是采取“他人识别”的标准，那原告的躯干的确不具有可识别性；相反，若是采取“本人识别”的标准，则原告可以识别出案涉合影中的躯干为其本人。在“冰心合影案”中，尽管他人无法识别案涉合影照片中的躯干为原告，但是原告本人可以识别。故此，“冰心合影案”保护的是肖像权背后的尊严利益，而该案采取的肖像可识别性的判断标准则是“本人识别”的标准。

根据本人识别的标准，若是他人侵害肖像权的行为触及尊严利益，则只要本人可以识别争议形象系肖像权人即可。在一则案例中，被告未经原告同意，使用人工智能将原告肖像丑化为一幅四肢残缺的三维卡通图像。法院认定该图像不具有可识别性。本文认为，尽管他人难以根据争议形象识别出原告，但是由于被告系将争议形象单独发送给原告，并且该争议形象的构图、服饰与原告肖像相似，因而原告可以识别出争议形象系其本人。鉴于被告侵害肖像权的行为触及尊严利益，故此应当根据本人识别的标准认定该争议形象具有可识别性。

（二）保护同一性利益之肖像可识别性判断标准

肖像权保护同一性利益。肖像代表人格，某一肖像出现在特定语境中，就意味着肖像权人持有某

种观点、立场或者品味。然而肖像权人可能并无此观念。因此行为人未经同意将肖像用于某一场景侵害了肖像权人的同一性利益。于此场景，肖像的可识别性应当采取一定范围内的熟人确信识别的标准。对此，需要说明的是：

其一，识别主体应当是一定范围内的熟人。在被告行为可能侵害同一性利益的场景中，原告担心的是将不恰当的观念归之于原告，产生归属混淆，进而侵害同一性利益。这种归属混淆的不利后果只可能发生在认识原告的社交圈子中。陌生人本就不知道其观念为何，甚至不会形成与原告有关的思想或感情活动，因此这些人是否可以识别原告，实则无关紧要。当然，一定范围内的熟人可多可少。对于名人来讲，认识他的人范围广泛，因此其更容易被识别，识别主体实际上等同于社会一般人；而对于非名人来讲，可能只有其亲属、邻居、朋友或者同事属于熟人的范畴，识别主体应当以此为限。例如，某医院刊登的医疗广告图案中，包含一名医生的正面形象和一名男性患者的侧身背影，原告提供三名证人出庭作证，证明同村人可以通过该侧身背影识别出系原告本人；加之广告内容涉及男科疾病，可能会使他人误以为原告患有相关疾病。故此，二审法院认定该广告图案具有可识别性。

其二，识别程度应当达到确信识别的程度，即达到“争议形象只能是权利人”，而不能仅仅停留在“争议形象可能是权利人，也可能是其他人”的层次。原告主张争议形象具有可识别性时，其应当通过提交本人的真实肖像，以及一定范围内的熟人认为争议形象具有可识别性的证言证词等证据材料，使法官确信争议形象只可能是原告。倘若法官的心证程度停留在“争议形象可能是权利人，也可能是其他人”，那么就不足以认定争议形象具有可识别性。例如，在“赵本山案”中，卡通人物形象以该特殊识别性为特征，并且配上了“您有才”及“咱不差钱”等赵本山在春节文艺晚会上小品节目的经典台词作为旁白，使一定范围内的熟人认为“那只能是赵本山”，因此该卡通形象具有可识别性。与此相反，在“乔丹案”中，乔丹商标之所以

不具有肖像可识别性，是因为即便配上“乔丹”的中译名，充其量只能形成该商标中的黑色人形剪影“既有可能是迈克尔·乔丹，也有可能是其他黑人篮球明星乔丹”的心证程度，而无法形成“那只能是迈克尔·乔丹”的心证程度。

被告在抗辩过程中只要提交证据拉低心证程度，使法官无法形成“争议形象只能是权利人”，只能形成“可能是权利人，也可能是其他人”的程度即可，而不必达到“不可能是权利人”的程度。故此，被告的抗辩方法，不应该是在原告提供的真实肖像和争议形象之间“找不同”，而是提供更多的其他主体的肖像，向法官证明“争议形象可能是权利人，也可能是其他人”。事实上，在刑事侦查中，为了确保被害人、证人等辨认人在侦查辨认时不受偏见或者先入为主的观念的影响，《公安机关办理刑事案件程序规定》第260条第1款规定，应当将辨认对象混杂在特征相类似的其他对象中，不得在辨认前向辨认人展示辨认对象及其影像资料，不得给辨认人任何暗示。同样，裁判者在判断争议形象是否具有可识别性时，也不能仅仅对照肖像权人提供的真实肖像进行对比，还要考虑“陪衬对象”。倘若争议形象既有部分特征与肖像权人相似，又有部分特征与陪衬对象相似，那么就无法形成“争议形象只能是权利人”的确信，不能认定争议形象具有可识别性。例如，在制作数字人产品的过程中，虽然行为人使用了肖像权人录制的肖像视频提取面部特征，但是在3D建模阶段使用了基于AI的融合算法（如生成对抗网络），替换或者融合了多个肖像视频中的面部特征，最终生成了含有全新面部形象的数字人产品。该数字人产品可能有部分特征与肖像权人相似，但是其他特征则与其他人相似。于此情形，只要裁判者无法形成“争议形象只能是权利人”的心证，就应当认定该数字人产品不具有可识别性。

（三）保护财产性利益之肖像可识别性判断标准

肖像权保护肖像承载的财产性利益。若是未经同意使用权利人的真实肖像获取财产性利益，则无

检讨可识别性的必要。只有在被告未经同意使用去面部特征的形象获取财产性利益时，才有必要检讨该争议形象是否具有可识别性。于此场景，肖像可识别性应当采取社会公众一眼即可识别的标准。

之所以采取这一标准，是因为肖像的财产价值源自其吸引社会公众注意力的能力。在传统的品牌代言、广告宣传等商业活动中，使用某一名人的肖像，可以借助该名人的影响力和粉丝基础，迅速扩大某一品牌或者商品的知名度。而在互联网经济中，肖像同样通过吸引注意力获得财产性利益，并且不再仅限于传统意义上的影视明星的肖像，也可能是依靠外貌特征、个性标签或独特风格而走红的网络红人的肖像。因此，只有当社会公众能够一眼就认出争议形象所指向的正是特定权利人，才能说明该形象正在利用权利人的个人特质吸引社会公众的注意力，进而转化为财产性利益。反之，如果公众无法在第一眼就明确识别出权利人，则不足以认定争议形象满足财产性利益保护下的肖像可识别性判断标准。

事实上，保护财产性利益之肖像可识别性判断标准，在逻辑结构上与商标法中关于相似性的判断标准具有高度一致性，均强调社会公众基于直观印象的可识别性。《最高人民法院关于审理商标民事纠纷案件适用法律若干问题的解释》第10条规定，认定商标相同或者近似时，应当以相关公众的一般注意力为标准，在比对对象隔离的状态下分别进行商标的整体比对和主要部分的比对，即所谓的“隔离比对法”或“隔离观察法”。之所以采取隔离比对法，是因为消费者不会将商标放在一起进行比较，而是在商店看到侵权商标后，错误地将带有侵权商标的商品当作他真正想买的商品。同样，在未经同意使用去面部特征的争议形象的场景中，只有相关消费者在未进行对比的情况下，就将争议形象误认作权利人时，方可认定被告使用争议形象的行为攫取了本应归属于权利人的财产性利益。例如在一个德国判例中，一则电台广告使用了模仿著名演员和作家海因茨·埃尔哈特（Heinz Erhardt）的声音，还使用了专属于埃尔哈特的词句来为某产品

做广告。汉堡上诉法院（OLG Hamburg）认为：“此案中人格权的受侵害程度并不亚于肖像和姓名的使用。不论听众是否能识别出声音模仿，对于任何听到广播广告的听众来说，都会生动地回忆起他的艺术人格。事实上，这种回忆效果正是广告追求的目的所在，即借此达到吸引注意力的效果。”在这个案件中，电台广告使用的声音使德国的社会公众“一听就知道那是埃尔哈特”，从而吸引了社会公众的注意力，因此符合保护财产性利益之肖像可识别性判断标准。作为反例，在“数字人案”中，被告生成的数字人产品并不足以使社会公众立即识别出该形象与权利人之间的对应关系。换言之，社会公众之所以关注该数字人产品，并非因为其体现了权利人的个体特质，而可能是出于对该数字人产品的新颖性、技术感或其他独立吸引力的兴趣。因此，该类产品不应当被认定为满足保护财产性利益之肖像可识别性判断标准。又如，被告商户在网络平台上发布了一幅女子佩戴口罩的照片，并将其用于相关商品的广告宣传。法院虽承认争议照片存在一定程度的面部遮挡，但经与原告的原始照片比对后，认定二者构成实质性相似。据此，法院认为争议照片具有可识别性。本文认为，该法院的认定标准尚有商榷之处。该案实质上涉及肖像财产性利益的保护，而在此类案件中，肖像可识别性应当采取社会公众一眼即可识别的标准。然而，争议照片中的女子佩戴了口罩并且不是知名人物，其形象并不足以使社会公众一眼即可辨识为特定主体，显然难以满足前述肖像可识别性的判断标准。

（四）肖像可识别性的多元化判断标准体系

肖像权保护的法益具有多元性，这一特征决定了肖像可识别性的判断标准亦不宜拘泥于单一标准，而应当被建构为一个多元化的标准体系：（1）在尊严利益保护层面，肖像可识别性的判断标准应当相对宽松。只要肖像权人本人可以识别出被丑化、污损的争议形象系其肖像，即可满足肖像可识别性的要求。然而，鉴于该层面所要保护的是尊严利益，识别依据原则上应限于肖像权人的身体特征，而不宜扩张至非身体特征。（2）在同一性利

益保护层面，肖像可识别性的判断标准应当相对严格。识别主体应当限定为一定范围内与肖像权人存在稳定交往关系的熟人团体；识别依据不仅包括身体特征，还可以涵盖与肖像权人具有稳定联系的非身体特征；识别程度应当达到完全确信争议形象是肖像权人的层次。（3）在财产性利益保护层面，肖像可识别性的判断标准应当最为严格，须达到社会一般人能够凭直观印象一眼认出争议形象所指向的特定身份的程度。

肖像可识别性的多元化判断标准体系的合理性，在于其系以肖像权所欲保护的不同类型法益及其位阶差异为基础而建构，从而实现法益保护与判断标准之间的对应关系。尊严利益最具保护价值，因而肖像可识别性的判断标准应当最为宽松，以便尽可能将争议形象被丑化、污损的案件纳入肖像权的救济范围。尽管肖像所承载的财产性利益应当受到法律保护，但行为人的一般行为自由亦有保护价值，因此肖像可识别性的判断标准应当最为严格，以避免肖像权对他人行为自由产生过度干涉。

当然，肖像权所欲保护的各类终局性法益之间存在交织和重叠，一个侵权行为往往同时指向数个终局性法益。在此情况下，肖像可识别性的判断标准应当采取如下思路：首先，《民法典》第1019条第1款的规定已经涵盖了肖像权所欲保护的终局性法益，因而在简单案件（easy case）中，裁判者不需要检讨被告行为具体侵害了哪一项法益，只需确认被告行为违反了《民法典》第1019条第1款，即可认定其侵害了肖像权。但是，在疑难案件中，尤其是在肖像可识别性成为争议焦点的案件中，裁判者有必要回溯至肖像权的规范目的，通过目的解释的方法，界定肖像可识别性的判断标准。其次，尊严利益、同一性利益和财产性利益均是肖像权所要保护的终局性法益，无论被告行为侵害其中何种法益，均可构成对肖像权的侵害。由此，在一个行为同时涉及数个法益的场景中，可以优先适用较为宽松的识别性判断标准。例如，在“AI换脸案”中，运营商未经同意发布去面部特征的换脸模板，该行为既可能侵害同一性利益，也可能侵害

财产性利益。由于保护同一性利益的可识别性判断标准宽于保护财产性利益的标准，故此裁判者只要认定前一标准得到满足，即可认定争议形象具有肖像可识别性。最后，倘若争议形象满足侵害较为宽松的肖像可识别性的判断标准，而不满足最为严格的判断标准，那么原告有权主张的损害赔偿项目将受到一定的影响。详言之，被告未经同意使用的争议形象可能满足了本人识别或一定范围内的熟人可以识别的标准，但是无法满足社会公众一眼即可识别的标准，因此被告使用争议形象的行为可以被认定为侵害了肖像权所欲保护的尊严利益或者同一性利益，但是难以认定为侵害了财产性利益。这是因为，争议形象没有达到社会公众一眼即可识别的程度，因此该争议形象难谓褫夺了本应归属于肖像权人的财产性利益。于此场合，原告固然可以主张其肖像权遭受了侵害，也可以主张精神损害赔偿请求权，但是不得主张基于肖像权侵害而产生的财

产损害赔偿请求权，如肖像的许可使用费等。

结语

肖像可识别性要件发挥作用的场景，主要是去面部特征的争议形象引发的肖像权纠纷。由于人工智能的迅速发展，去面部特征的虚拟形象在商业活动和社会交往中日益普遍，肖像可识别性要件重要性越发凸显。本文提出，应当以肖像权所保护的终局性法益为基点，建构一个肖像可识别性的多元化判断标准体系。在尊严利益层面，宜采取宽松标准，以最大限度制止丑化和污损肖像的行为；在同一性利益层面，应当采纳相对严格的标准，以保障主体形象的稳定性与完整性；在财产性利益层面，则需坚持最为严格的标准，以避免肖像权过度扩张对他人自由造成不当限制。通过在不同法益维度上确立差异化标准，既可以回应人工智能时代肖像表现形式多样化带来的挑战，又能在法益保护与行为自由之间实现更为均衡的制度安排。

制度与场景：重构人脸识别与人脸图像信息保护

此处删除了原文脚注，全文请参见《行政法学研究》2026年第1期，转载或引用请注明出处。

作者：丁晓东

内容提要：已有法律制度对通过技术识别的人脸识别信息适用个人信息保护，将其视为生物识别信息或敏感个人信息；对可以自然识别的人脸图像信息适用隐私权保护，将其视为公开个人信息与非私密信息。此类基于信息区分的二分保护具有一定合理性，但也存在困境。法律应转向基于制度区分的保护，在侵权隐私、信息隐私、执法隐私的制度模块下保护不同场景下的人脸信息。侵权隐私制度具有横向性特征，主要针对违反社会关系的人脸信息获取场景；信息隐私制度具有倾斜性特征，主要针对信息能力不平等主体之间的人脸信息处理场景；执法隐私制度具有纵向性特征，主要针对人脸信息的公共执法场景。人脸信息保护的关键是实现制度与场景的对齐。应将不同制度模块适用于与其相匹配的典型场景；对于与制度模块不匹配的非典型场景，则应对制度模块进行改造与转型升级。

一、问题的提出：人脸识别与人脸图像信息二分

人脸信息保护是一个老生常谈的社会与法律热点问题，每隔一段时间，新闻媒体就会报道我国和域外有关人脸信息的立法与相关案例。例如，在杭州的“人脸识别第一案”中，杭州野生动物园仅允许游客使用人脸识别的方式入园，游客据此向法院提起诉讼，引发全社会关注。又比如，在山东济南的一个楼盘售楼处，部分看房人为躲避售楼处的面部识别监控技术，头戴摩托车头盔前去看房，引发媒体广泛报道。而随着人工智能技术的兴起，利用网络技术在互联网空间爬取人脸图片、创建人脸识别信息库并用于人工智能训练，也引发了法律风险与争议。这一做法目前在美国被认定为合法活动，但却被欧盟多个国家的数据保护机构认定为违法。此外，涉及人脸信息拍摄、监控的案件也层出不穷。

例如有人从事街拍活动，将拍到的人像图片和视频上传至网络，引发了被拍摄者的不满；有的居民在自家门口安装监控视频，拍到其邻居的人脸信息，引起邻居的投诉与不满；一些网民的人脸被他人用AI技术移花接木到淫秽色情图片与视频上，并遭遇敲诈勒索。

为了合理保护人脸信息，我国、域外国家和地区均出台了相关法律法规或指南。例如，我国最高人民法院于2021年出台了《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，国务院于2024年发布了《公共安全视频图像信息系统管理条例》，对采集与处理包括人脸信息在内的个人信息进行规范。同年，我国国家互联网信息办公室、公安部联合发布了《人脸识别技术应用安全管理办法》，对利用人脸识别技术处理人脸信息进行规范。域外国家和地区也发布了相应指南。美国于2025年通过了《删除法案》，其中相关条款规定，平台需要采取技术措施删除利用AI技术进行换脸的私密或裸露图像。欧盟早在2019年就发布了《关于通过视频设备处理个人数据的准则》的指南，对通过视频监控方式处理人脸信息的行为进行规范。欧洲理事会《关于个人数据自动化处理中的个人保护公约》（第108号公约）咨询委员会发布《人脸识别指南》的报告，就人脸识别对立法与政策制定者、制造商、使用者和个人给出了全方位的建议。欧盟于2024年通过的《人工智能法案》也对人脸识别进行了规定，将从互联网或监控视频中“爬取人脸图像来创建或扩展人脸识别数据库”列入禁止性人工智能实践。

对于人脸信息保护，学界已经从不同角度进行了深入分析，但仍有一些关于人脸信息保护的核心问题尚未得到分析与探讨。首先，人脸信息保护应当适用何种制度？是否可以说，经过技术识别的人脸识别信息适用《个人信息保护法》，而未经技术识别的人脸图像信息则不适用？如果人脸信息保护适用《个人信息保护法》的框架，则个人可以行使《个人信息保护法》中的一系列权利，例如，个

体知情决定权、查阅复制权、携带转移权、更正补充权、删除权、解释说明权等权利；信息处理者则要遵守一系列义务，例如，安全保护措施、合规审计、影响性评估、个人信息泄露等情形中的补救措施。相反，则上述《个人信息保护法》的一般制度将不适用。当人脸图像信息不适用个人信息保护时，法律又应当采取其他何种保护制度？例如，在摄影街拍、监控录像的场景下，法律是否以及如何保护人脸图像信息？

其次，如何看待人脸信息的敏感性、公开性与私密性等属性与特征？敏感个人信息与公开个人信息的概念为各国的个人信息保护法所规定。对于敏感个人信息，各国都采取强化保护措施。对于处理公开个人信息，各国则对其进行弱化保护。而私密信息则与传统隐私权密切相关，《中华人民共和国民法典》（以下简称《民法典》）规定：“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。”是否可以说，经过技术识别的人脸信息都是生物识别个人信息，因此属于敏感个人信息、非公开个人信息、私密信息，而未经技术识别的人脸信息则是非敏感个人信息、公开个人信息、非私密信息？但在人脸图像信息和人脸识别信息相互转换的背景下，又应当如何看待人脸信息的属性及其法律适用？

上述问题环环相扣，密不可分。例如人脸信息适用何种制度，将决定或影响法律对敏感个人信息、公开个人信息与私密信息概念的讨论。反之，人脸信息是否具有敏感性、公开性与私密性特征，又会影响法律采取何种制度保护人脸信息。此外，人脸信息的敏感性、公开性与私密性也会相互影响。本文对上述问题进行讨论，指出人脸识别信息与人脸图像信息二分保护面临着重大挑战与困境。为应对这些挑战与困境，本文引入域外法学界最近二十多年来广受关注的制度模块理论（modularity theory），指出这些挑战与困境的根源在于制度模块与场景的不匹配。法律需要区分不同制度与场景，将不同功能的制度模块适用于与其相匹配的典型场景；而对于与制度模块不匹配的非典型场景，

则需要对制度模块进行拆分、重组、改造或转型升级，使得新制度能够适应非典型场景或新场景。本文提出信息隐私、侵权隐私与执法隐私这三种不同制度模块，对这三种制度模块的制度设计、功能与基本原理进行分析，在此基础上对人脸信息保护的制度进行重构。

在行文方面，本文第二部分对人脸信息保护的制度适用与信息属性展开分析；第三部分阐述信息隐私、侵权隐私与执法隐私的不同制度模块，借此分析与重构人脸信息保护的基本原理；第四部分对人脸信息保护的具体制度进行重构；结语部分对制度与场景的对应问题进行法理学反思。在术语使用方面，为了简便起见，本文将把经过技术识别的人脸信息称为人脸识别信息，把暂时未经技术识别的人脸信息称为人脸图像信息，把人脸识别信息和人脸图像信息统称为人脸信息。同时，本文所称的信息隐私制度与个人信息保护制度是同一制度，但在不同语境中采用不同表达。

二、人脸信息二分保护的困境与争议

人脸信息收集与利用的场景多元，既包括人脸识别信息，也包括人脸图像信息。前者又包括一对一的个体验证、多对一的个体识别、多对多的身份归类。后者则包括摄影拍照、录像监控、网络爬取等多种不同场景。对人脸信息进行分析，可以发现其适用的制度与人脸信息的特殊性都存在争议。

（一）人脸信息二分保护的制度困境

对于人脸识别信息，一对一的人脸识别主要用于身份验证，例如，有的大学和小区门口设置刷脸设备，对进入其中的学生、老师和访客进行验证；酒店在旅客入住、银行在顾客开户时通过公安机关身份信息数据库进行比对。在此类场景中，人脸识别技术的使用者与个人具有显著的信息处理关系，而且利用个人信息保护制度可以有效规制此类信息处理关系。一方面，赋予个人信息主体相关权利可以有效维护个人权益，例如，个人信息更正权可以有效防止个体人脸识别出现差错。另一方面，对信息处理者施加相关责任则可以有效维护用户的信息安全、金融账户安全、公共安全等各类权益。

但在多选一、多选多的人脸识别场景下，法律是否应当对其适用个人信息保护法存在疑问。多选一的个人人脸识别主要用于从人群中识别个人，例如，公安机关可能利用此类识别技术进行打拐，寻找走失儿童，在侦查过程可能调取摄像头，从摄像头中比对识别犯罪嫌疑人。也有的商家可能利用人脸识别技术对顾客进行精准识别，对其进行持续追踪与精准营销。多选多的人脸群体归类主要指群体特征识别，即通过人脸识别技术将某人归纳为某一群体，例如，执法部门或娱乐场所、烟酒企业商家利用人脸识别技术，筛查其所交易的对象是否为未成年人。还有的商家和经营实体利用人脸识别技术，识别进入其商店的顾客有多少人是女性，有多少人是老年人。本文开篇提到的售楼处利用人脸技术识别顾客，就属于此类情形。但无论是多选一还是多选多，对其完全适用个人信息保护制度都存在问题。一方面，人脸技术的应用者和个人都缺乏直接交互的界面与持续性的信息关系。因此，人脸技术应用者很难保障个人的知情同意权、查阅复制权、携带转移权、更正补充权、删除权、解释说明权等权利。人脸技术应用者最多只能在某些场景下对个体进行提示，例如，竖立警示标识，但无法保障每个个人都能对其进行充分告知，更难以获取其同意。另一方面，在筛查犯罪嫌疑人、娱乐场所未成年等执法场景下，法律则更加不可能赋予个体以知情同意权，对个体进行事前告知将使得执法失去意义。

人脸图像信息所涉及的场景也非常复杂。有的人脸图像信息收集利用明显不具有信息处理关系的特征，把这些场景排除在个人信息保护制度之外，具有合理性。例如，当个体在街拍时拍到他人人脸，或者利用AI技术对他人照片视频进行换脸，那么法律应当对此类行为适用传统隐私权与侵权法进行保护。除非个人是专业性的街拍人员，其拍摄的人脸信息已经具备处理特征，则此时法律可以适用个人信息保护制度。但在其他很多涉及人脸图像信息的场景中，个人信息保护制度是否适用存在争议。以餐厅、宾馆、咖啡馆等场所的视频监控为

例，很多监控视频不会直接被用于人脸生物性识别，但也可能在未来被用于一对一、多选一、多选多的人脸生物性识别。而且，即使是排除人脸生物性识别的监控视频，个人信息保护中的很多制度也未必能够完全适用。对于视频监控，个人应当有一定的知情权，也可以要求信息处理者确保此类视频的安全，防止数据泄露，但个人却未必可以主张决定权、查询复制权、删除权、携带权等权利。因为监控视频缺乏交互场景，个人无法行使同意。而且此类视频往往包含了其他个体的信息，在查询、复制、删除或转移此类视频时，很可能会威胁他人的信息安全。

（二）人脸信息二分保护的属性争议

首先，人脸识别信息与人脸图像信息的敏感性二分存在争议。法律一般将人脸识别信息视为生物识别类的敏感个人信息。例如我国最高人民法院2021年出台《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》指出，人脸识别信息属于《民法典》第1034条规定的“生物识别信息”。美国伊利诺伊州的《生物识别信息隐私法案》（Biometric Information Privacy Act）规定：“脸部印记（包括从照片中提取的任何脸部印记）”属于“生物识别标示（biometric identifier）”。对于生物识别类个人信息，各国也对其适用特殊保护制度。例如，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）将生物识别数据与种族、民族、宗教信仰、医疗健康、金融账户、个人行踪等信息并列，归入“个人敏感信息”的范畴，并对其制定了特殊的处理规则。欧盟则将生物识别数据归入“特殊类型个人数据”的范畴，规定除了一些例外情况，原则上禁止对其进行处理。美国伊利诺伊州《生物识别信息隐私法案》要求，任何私人实体收集生物识别信息，必须向个人提供书面告知，并且获取个人同意。相反，如果个人或企业拍摄他人照片或安装摄像头进行监控，但并不使用技术手段为个人设置唯一的人脸标识，则此类人脸图像信息仍然属于普通个人信息。《最高人民法院关于审

理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》明确指出，“使用人脸识别技术处理人脸信息、处理基于人脸识别技术生成的人脸信息”，是该司法解释适用前提。《一般数据保护条例》也有较为清晰的认定，“重述”指出，“照片的处理不应系统地被视为特殊类别个人数据的处理，因为只有通过允许对自然人进行唯一识别或认证的特定技术手段进行处理时，生物特征数据的定义才涵盖这些数据”。

但人脸信息敏感性的上述二分保护面临争议。法律对非技术识别的人脸图像信息进行一般保护，对技术识别的人脸识别信息进行特殊保护，其理由是人脸识别信息具有唯一性和敏感性。但无论是识别的唯一性还是信息的敏感性，此类区分都并非绝对。就识别性而言，人脸技术识别信息固然具有相对唯一性，可以通过此类信息识别到个人，但此类识别是针对机器而言。对于自然人的肉眼而言，技术与机器处理后的信息，例如，鼻子与嘴唇的距离，其实反而不具有识别性。自然人所能一眼识别的人脸信息，恰巧是未经技术处理的人脸照片或人脸视频。因此，在有的情形下，人脸图片或视频信息反而受到比人脸识别信息更多的保护。例如，1998年的美国《儿童在线隐私保护法》(Children's Online Privacy Protection Act, COPPA)将儿童的“照片、视频或音频文件”视为儿童个人信息，但并未将未成年人的生物特征数据明确纳入其保护范围。

就不同国家的文化背景与个人感受而言，人脸技术识别信息也很难说就比人脸照片与视频更敏感。欧盟将生物性识别数据纳入“特殊类型个人数据”，与种族或民族背景、政治观念、宗教或哲学信仰等类型的数据并列，这与欧盟的历史和种族问题有密切联系，反映了欧盟对于借助生物性识别信息进行种族歧视和种族排斥的高度警惕。但这一历史与文化背景并不一定适用于其他国家，尤其未必适用于中国等非西方国家。对于普通中国人而言，可能某些场景下的人脸照片或视频更为敏感，此类信息的收集与储存可能会让很多人感到更为焦虑和紧张。相反，经过机器识别与处理的人脸信息则

由于其技术性，只能为机器以及很少部分技术人员所识别，人们可能并不担心其为机器所识别，而更担忧这类信息泄露后被用于身份伪造等非法行为。

其次，人脸识别信息与人脸图像信息的公开性二分也存在争议。法律一般将人脸图像信息视为公开个人信息，将人脸识别信息排除在公开个人信息之外。因为在社会交往中，人脸图像信息经常以公开为原则，以不公开为例外。例如，在关于蒙面的宪法争论中，很多国家和地区的宪法判决认为，对脸部信息的遮挡违背了人格尊严，阻碍了社会交往与个人的公共责任。而人脸识别信息由于需要进一步识别，具有较强的私密性，因此不少国家的法律都明确将其排除在公开个人信息范围之外。例如美国《加州隐私权利法案》(California Privacy Rights Act, CPRA)规定，“‘公开可用’并不意味着企业有权在消费者不知情的情况下收集有关消费者的生物特征信息”。对于公开个人信息，各国法律也对其进行弱化保护甚至是豁免保护。例如，我国《民法典》规定，合理处理“自然人自行公开的或者其他已经合法公开的信息”，信息处理者并不承担责任，除非“自然人明确拒绝或者处理该信息侵害其重大利益”。我国《个人信息保护法》也规定，“在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息”可以被视为处理个人信息的合法性基础。并且对处理公开信息进行了单独规定。

人脸信息公开性的二分保护框架也存在问题。《个人信息保护法》对公开个人信息弱化保护，其基本预设是公开个人信息已经经过个人信息主体或其他合法途径公开，因此对其进行处理对个人权益和社会利益造成的影响较小。但无论是在公开性层面还是在风险层面，人脸图像信息处理的风险都未必会比人脸识别信息的风险更小。就公开性而言，人脸图像信息的公开性主要针对其线下交往或活动范围，除非是公众人物，其人脸图像信息并非对全社会完全公开。而人脸识别信息也已经越来越容易获取，其公开属性也越来越强。人脸识别技术于2000年前后仍然主要处于实验层面，但随着过

去二十年来卷积神经网络（CNN）等算法技术的突破，人脸识别技术被快速商业化运用。今天，人们只要用很低的费用就可以购买具有人脸识别功能的各类技术应用。尤其对于包含人脸的照片、视频，人们可以很轻松地将此类人脸图像信息转换为人脸识别信息。就风险而言，人脸识别信息虽然在技术层面更为精确，但这种精确识别主要用于手机解锁、移动支付、银行开户、小区进出、机场安检等少量场景，而这些场景中的人脸识别信息往往受到较高层级的安全保护，其信息处理的风险未必很高。相较之下，人脸图像信息虽然难以直接被技术所精准识别，但其可以被用于不特定的具体场景。例如，人脸可能被不法分子用于各类移花接木的PS、AI换脸，其所产生的风险可能远大于人脸识别信息。

最后，就个人信息的私密性而言，人脸图像信息与人脸识别信息的二分保护也存在类似问题。个人信息的私密性常常被用于判断其是否受隐私权保护的依据。从直觉上看，人脸图像信息具有公开性，应当属于非私密信息，仅受个人信息或公开个人信息的法律保护；而人脸识别信息则较为隐蔽，可以归入私密信息范畴，受到隐私权保护。但正如上文所言，人脸图像信息并非完全公开，人脸识别信息也越来越容易公开获取。从原理层面看，个人信息的私密性与公开性并非非黑即白，而是一个连续性光谱，取决于具体场景。例如，互联网公共论坛上的个人信息可能公开性很强，微信朋友圈的个人信息具有半公开性；而线下公共场所、商业街的个人信息公开性较强，各种餐厅、咖啡馆、街角的个人信息公开性则相对较弱。当某人出现在某些私密场所，其人脸信息就具有私密性。相反，一些获取人脸识别信息的行为，在某些国家和地区也被认为并不侵犯个人的隐私权。例如，美国Clearview AI公司从Facebook、YouTube、Venmo和其他网站“抓取”了海量人脸图像，创建了一个30多亿张人脸识别数据库供人工智能企业训练之用，这一行为也被认为符合美国法律规定。

三、迈向人脸信息的制度模块保护

人脸信息之所以在法律制度和个人信息属性问题上存在争议，与隐私和个人信息保护的不同制度模块设计有关。隐私和个人信息保护采取了侵权隐私、信息隐私与执法隐私三种不同的制度模块，而每种制度模块对应不同的典型场景，人脸信息的保护场景有的和典型场景一致，有的则并不一致，这导致了人脸信息保护很难在法律制度和个人信息属性上给出没有争议的答案。本部分阐述这三种制度模块及其对应场景，并分析人脸信息保护的场景与其对应和不对应之处。

（一）侵权隐私制度模块

法律保护隐私与个人信息的第一种制度模块是具有横向关系特征的侵权隐私。这种制度模块的发展历史与基本制度已经为学界所熟知。19世纪末，随着摄影技术的发展，一些记者开始用相机拍摄可以识别个人人脸的照片，并将此类照片和留言八卦刊登在媒体小报上。1890年，沃伦（Samuel Warren）与布兰代斯（Louis Brandeis）发表《隐私权》一文，首先在论文中提出隐私权的概念，主张法律保护“个人独处的权利”，保证个人的“思想、情绪和感受”这些构成人格的要素不受侵害。其后，隐私权的概念在美国、德国等国家被认可，我国也将其纳入人格权的保护范畴，并利用侵权法进行保护。

在适用侵权隐私制度模块时，侵权隐私所要保护的隐私权是一种合理的社会关系，而非某一个体的固定空间。沃伦与布兰代斯虽然在《隐私权》一文中提出了作为独处的隐私，但他们也同时强调在社会关系中理解隐私，认为隐私的边界必须结合“每个具体案例的多种情境”来进行考虑。沃伦与布兰代斯指出，之所以要确立个人的隐私权，是因为新闻媒体已经“在各个方面都脱离了规矩（propriety）和体面（decency）”，流言蜚语已经成为一种“厚颜无耻的工业化生产”。因此正如波斯特教授在评论沃伦与布兰代斯时指出，隐私权并不意味着秘密、匿名和独处，而是意味着我们作为社会群体中的个体应当给予彼此的空间。侵犯隐私意味着打破了社会精神上的宁静。当法院将某些

行为认定为隐私侵权，法院在此类认定过程中其实并非认定某个人固有的权利边界，而是界定一个社会共识性的交往规则，即一个社会的“社会规范（social norms）”或“文明规则（rules of civility）”。

（二）信息隐私制度模块

法律保护隐私与个人信息的第二种制度模块是具有倾斜性关系特征的信息隐私或个人信息保护制度，主要针对“信息处理者”与个人之间的关系。在适用前提与调整关系方面，这一制度模块的适用前提是存在倾斜性的“信息处理关系”，即信息处理者利用信息技术处理个人信息。例如，欧盟《一般数据保护条例》将“处理”（processing）界定为“自动化”“半自动化”，或者对“存档系统”进行“结构化”的手动处理。美国各州的立法也将其法律适用范围界定在专业化或商业化的个人信息处理场景。我国《个人信息保护法》并未对“处理”概念进行明确界定，但也将纯粹私人性质的个人信息处理排除在外，表明我国也采取了与欧美类似的法律制度。在制度设计方面，这一制度也具有倾斜性保护特征，法律一方面对个人信息主体进行赋权，另一方面对信息处理者施加责任，以合作治理的方式对信息处理关系中的信息主体进行保护。

需要指出和强调的是，个人信息保护制度模块所针对的典型信息处理关系不仅具有倾斜性保护特征，而且具有大规模微型权益保护与持续性信息关系的特征。大规模微型权益保护的原因不难理解，如果信息处理关系是一对一、具有明确损害的侵权关系，则法律完全可以利用侵权隐私的框架进行保护。而在大规模微型权益保护中，个体利用侵权法进行救济的动力和能力非常有限，社会又需要对此类大规模微型侵权进行治理。在侵权隐私制度无法适应此类侵权的背景下，信息隐私或个人信息保护法的制度才得以诞生。同时，如果信息处理关系不具有持续性和交互性，而是一次性、侵入性的，则《个人信息保护法》中的若干制度也无法发挥作用。在缺乏信息关系与交互界面的情形下，个体将

无法向信息处理者行使知情决定权、查阅复制权、携带转移权、更正补充权、删除权、解释说明权等权利。只有当信息处理者和个人建立持续性和交互性的关系，《个人信息保护法》中的主要制度才能发挥其功能。

（三）执法隐私制度模块

法律保护隐私与个人信息的第三种制度模块则是纵向性的执法隐私制度。在中文学界的隐私或个人信息保护领域，这一制度模块受到的关注主要限于宪法研究与刑事诉讼研究。最初，执法隐私所针对主要是国家执法机构，例如，国家执法机构对个人进行侦查、监控所引发的个人隐私保护问题。在我国，《中华人民共和国刑事诉讼法》（以下简称《刑事诉讼法》）等法律法规对其进行了规定。在美国，这一问题则主要被放置在美国《宪法第四修正案》和《监控法》（surveillance law）的框架下进行规范。不过需要指出，美国的《监控法》仅针对有限的窃听等问题进行规范；而美国宪法的框架又过于简单和僵化，很难适应信息与数字时代的执法隐私问题。在美国《宪法第四修正案》的“第三人理论”（third party doctrine）框架下，当事人对于自己对外披露的信息均不具有合理隐私期待（reasonable expectation of privacy），执法机构可以任意获取公共信息或这类当事人向第三人披露的信息。这使得美国执法部门可以广泛获取大量私人企业等主体所保存的个人信息和其他具有隐私属性的个人信息。在执法隐私的学术研究中，美国的制度设计受到了学者们的广泛批判。执法隐私制度需要超越美国《宪法第四修正案》的制度，对执法部门处理所有个人信息进行规范。

此外，执法隐私制度模块还应当针对私人主体执法。很多私人主体不仅获取并拥有大量的个人信息，而且直接承担了政府所要求的部分执法职能，例如上文提到的娱乐场所利用人脸识别机构筛查未成年人。这类关系由于其执法属性，私人主体与个人或公众之间也形成纵向性关系，也应当利用执法隐私的制度加以规范。本文开篇提到的我国《公共安全视频图像信息系统管理条例》，除了对国家

执法机构和公共场所管理组织应用公共安全视频进行规范,也同时对旅馆、饭店、宾馆、招待所、民宿等私人主体应用公共安全视频做出规定。我国的相关立法更为符合执法隐私的基本原理与制度设计。

执法隐私也有若干特殊性需要指出和进行强调。首先,执法隐私的主体是公共机构或代表公共利益进行执法的私人机构,而公共执法本身就具有正当性,法律常常需要平衡执法信息与个人隐私保护,寻求与侵权隐私和信息隐私不同的理论基础。从目前的法学理论与法律实践看,学者提出了多种不同的论证。例如,保罗·葛维宝(Paul Gewirtz)教授认为,隐私保护有利于人民自治。如果人民“害怕被人偷听,害怕被公众曝光,害怕自己的言辞成为流言蜚语的话题,害怕自己的亲密关系被公开审查,害怕自己所说的话被认可或不被认可时”,那么人民就不会参与公共讨论,人民意志就难以形成。内尔·理查德(Neil Richard)教授认为,执法中的隐私保护有利于公民个体的自主性,特别是个人的智性发展不受干扰。此外,还可以看到国家对私人信息的过度获取反而会造成执法部门的信息过载,削弱国家的执法能力。国家执法能力的传统研究主要针对传统社会或工业化社会,其主要聚焦点是国家信息汲取能力的不足与国家能力建设的必要性。但在信息与数据化时代,对国家执法能力的研究尤其需要关注信息过载所造成的国家能力下降问题。

从典型场景来看,典型执法隐私制度模块所针对的场景具有一次性或持续性的侵入型特征,区别于个人信息保护典型场景中的信息处理关系。一次性侵入的执法隐私典型是刑事案件中的个案侦查,而持续性侵入的执法隐私典型是公共安全监控。但无论是具有一次性还是持续性特征的执法隐私,执法者与个人之间都具有侵入性或对抗性,二者主要是侦查、预防等关系。而在典型的个人信息保护所针对的信息处理关系中,信息处理者与个人之间形成了兼具互惠与侵害的关系。执法隐私中的侵入性与对抗性特征,使得执法隐私也难以适用《个人信

息保护法》中的很多制度。例如,在刑事侦查中,赋予个体知情决定权、查阅复制权等权利,将会严重干扰或彻底破坏执法机构的执法努力。整体而言,执法隐私主要通过对执法者进行规范而非赋予个体信息权利来保障个人隐私。

(四) 小结:从信息区分到制度区分

从个人信息保护的三种制度模块出发,就能理解为何人脸识别信息与人脸图像信息的二分保护框架存在问题。这种二分保护框架从人脸信息本身的特征分析相关问题,忽略了人脸信息保护应当首先分析不同制度所适用的场景与制度功能。从人脸信息区分转向制度区分,上述问题则会迎刃而解。

就制度适用而言,无论是人脸识别信息还是人脸图像信息,其制度适用取决于其信息处理的场景是否与某一制度相对应。如果某一场景与侵权隐私、信息隐私与执法隐私中的某一制度高度对应,则该场景就应完全适用其中的某一制度。而在场景与制度不对应的情形中,则应进一步分析某一制度的具体功能,并对该制度进行拆分、重组、改造或转型升级,以更好地应对无法与制度完全匹配的场景。

就人脸信息的属性而言,无论是人脸信息的敏感性、公开性还是私密性,都首先是特定制度工具的一部分,都必须结合具体制度及其制度功能来进行判断。其中,敏感性与公开性是个人信息保护制度的组成部分,某一信息是否敏感与公开,取决于将这类信息纳入敏感个人信息与公开个人信息,是否可以有效对这类信息进行治理。而私密个人信息则是侵权隐私制度中的相关制度,人脸信息是否属于侵权隐私中的私密信息,取决于隐私侵权中的个人处于何种场景,获取人脸信息的主体与个人之间的关系如何,其获取的人脸信息在多大范围公开、被用于何种目的等因素。

四、制度模块视野下的人脸信息保护

在原理反思的基础上,本部分进一步对人脸信息保护进行制度建构。具体而言,本部分将按照上一部分所提出的侵权隐私、信息隐私与执法隐私制度对涉及人脸信息的场景进行分类建构。正如上一

部分所述,有的场景与制度高度契合,有的场景则与制度存在错位,法律需要对制度整体进行重构。

(一) 人脸信息的侵权隐私保护

首先,侵权隐私可以适用于拍照录像、个人视频监控等各类与该制度相对应的典型场景。在这些场景下,判断相关人脸信息处理是否构成隐私侵权,取决于相关行为是否违反社会规范或一个社会中理性个体的合理预期。以拍照录像为例,利用手机进行拍照录像,拍到他人人脸;在公共广场、商业街道、旅游景区拍摄包含一般人脸图像的视频并上传至社交网络,都不应被视为侵权。在这类场景中,每个个体都应当能够预期自己的人脸信息有可能被他人拍摄与分享。但是,如果此类拍照录像是对特定个体进行跟踪拍摄,或者是针对未成年人进行未经允许的人脸特写拍照并将其广泛分享,则相关行为可能构成隐私侵权。再以个人视频监控为例,当普通个体在其房屋外或家门口安装视频监控,如果这类视频监控的区域属于社会理性个体所能预期的范围,则其视频监控到的人脸信息不属于侵权。但是如果此类监控可以拍摄到他人房屋内的活动,或者此类监控可能构成对邻居等特定个体的行踪轨迹的监控,则此类视频监控就属于侵犯他人隐私。

侵权隐私中的人脸信息保护也常常需要考虑其他合法权益。例如,在涉及媒体报道、公共人物与公共事件的情形中,法律需要平衡隐私权与舆论监督、公共讨论的需求。而且即使是个人从事此类行为,其侵权行为的边界也应当有所变化。例如2019年,有父母将一名6岁的小女孩绑在树上进行教育,一位路人担忧小女孩情况,对这一情形进行了录像,并将视频私信给新浪微博大V进行传播,此案最终引发了相关诉讼。在本文看来,此案对未成年人的人脸信息进行法律保护具有合理性。但此案与一般拍摄未成年人的行为不同之处在于,此案中的路人是因为担忧未成年人的安全而进行的拍摄和传播,具有见义勇为和社会监督的性质。虽然事后证明该案中的父母并没有伤害其孩子的意图,但在当时的情形下,该名路人的拍摄与传播行为不

应受到法律的否定。

其次,在非典型场景下,侵权隐私也可以适用于信息隐私或执法隐私对应的场景。尽管侵权隐私是一种横向保护的制度,但当事人仍然可以将信息处理者或执法者视为侵权法上的侵权者。当然正如上文所述,在信息隐私或执法隐私的人脸保护场景中,适用侵权隐私可能面临制度失效的困境。例如,信息处理者违规处理大量人脸信息、执法者违规对个人人脸信息进行识别。在这些场景中,个体很难对自身权益进行有效救济,在绝大多数情形下,个体既难发现其权益受到侵害,也难对造成的损害进行举证。而且即使极少数个体能够对自身权益进行救济,其他被违规处理的海量个体权益也无法得到保护。

面对非典型场景下制度与场景的错位,一种方案是直接诉诸信息隐私或执法隐私保护制度,寻求与场景更相对应的制度工具。而另外一种方案则是对侵权隐私制度进行改造与升级,使得侵权隐私制度仍然能够发挥其作用。例如,在综合性个人信息保护制度仍然缺位的美国,很多学者就主张降低隐私侵权中“损害”的认定标准,允许更多的隐私侵权被法院接受与认可,以重新发挥侵权法对于大规模侵权的治理作用。不过,这种制度的改造也是双刃剑,降低隐私侵权中“损害”的认定标准,可能导致法院的案件大量增加、监管过度等“私人执法”问题。

(二) 人脸信息的信息隐私保护

首先,正如上文所述,信息隐私高度对应一一对人脸识别验证这一场景。在一对一的人脸识别场景下,处理者与个人之间不但具有不平等的信息处理关系,而且人脸识别信息又具有很强的个体属性。人脸识别信息的这种特征使得这类信息具有类似早期档案类个人信息的属性。个人信息保护法的早期制度,即公平信息实践制度,起源于对个人税收记录等个人档案类信息的保护。对于此类较为重要和处理频次较低的信息,个体具有较强的自我保护动力,赋予个人信息权利和强化个体的信息自我控制,不会陷入“隐私悖论”(privacy paradox)

或隐私自我管理的困境。就一对一的人脸识别本身而言，这一制度适用信息隐私制度应无疑议。

其次，对于一些与信息隐私保护不完全匹配的非典型场景，信息隐私制度模块应当进行改造和适用。以上文提到的商业化多对一或多对多的人脸识别场景为例，当商场对顾客进行人脸识别并进行商品推荐、顾客服务，此类场景中的商场与个人之间仅具有有限的交互性，而且其交互性是针对进入商场的顾客，而非针对特定个人。针对其场景的特殊性，法律应当赋予个体以个人信息权利中的知情权，但不应要求商场保证个体的决定权等其他权利。商场如果选择使用人脸识别技术，就需要在入口等显著位置对顾客进行提示，告知其使用了人脸识别技术，但商场不太可能无法获得顾客的事前明示同意，对于已经进行人脸信息识别的顾客。而且由于商场是与整体顾客进行有限交互，商场也很难保证某个个体用户的人脸信息可以被查阅复制、携带转移、更正补充或删除。当然，由于顾客对于人脸图像或人脸识别信息处理往往较为敏感，商场应当遵守信息处理者责任中的相关制度，特别是严格遵守“目的限定”“数据最小化”等要求。一旦商场的人脸识别突破“目的限定”与“数据最小化”要求，将其应用于跨商场追踪，个人的隐私合理期待就会受到严重挑战。

再以目前争议较大的人工智能人脸识别训练为例，人工智能人脸训练所依赖的人脸识别数据早期主要依赖个体授权，但随着人工智能对于数据量的需求暴增，目前的人工智能人脸识别训练数据主要源于对互联网上可公开获取的人脸图片进行爬取、识别与标注。在本文看来，信息隐私的制度模块应避免对此类场景适用个人信息权利部分，但应当适用信息处理者责任部分。就个人信息权利而言，人工智能企业与个人之间完全没有交互场景，而且其对人脸信息的训练型利用也不会对个体直接产生侵害，此时个人信息权利中的知情决定权等权利都无法有效行使。就个人信息处理原则而言，人工智能人脸识别训练的目的也往往和其人脸信息在互联网上公开的初始目的并不一致。在个人信

息权利与个人信息处理原则方面对个人信息保护制度进行调整，允许人工智能企业对互联网公开途径获取的人脸图像与人脸识别信息进行训练，既符合我国《个人信息保护法》的相关规定，也有利于大规模数据的聚合与人工智能的发展。当然，人工智能企业处理此类人脸信息也会带来社会风险，例如，大规模泄露人脸数据可能造成安全风险、人脸数据训练不当可能对特定人群造成歧视。基于这些考虑，法律应对人工智能企业适用人脸信息安全保护、合规审计、影响性评估、信息泄露补救措施等法律责任。

（三）人脸信息的执法隐私保护

执法隐私制度涉及的人脸保护典型场景包括个案侦查与公共监控。二者的共同之处在于均基于公共利益需求，且执法者与个体均构成纵向执法关系。从二者的共同性出发，执法隐私制度在这两种场景中都应当注重对执法者收集、传输、显示、存储、使用人脸信息进行全流程规范，而非通过信息隐私制度中的个人信息权利而保护人脸信息。正如上文所述，执法隐私中的执法者与个人之间具有纵向侵入性与对抗性关系，这种关系不同于典型信息隐私场景下兼具互惠性与侵入性的信息处理关系。

当然，个案侦查与公共监控中的人脸信息保护也有不同之处。个案侦查涉及刑事案件，往往需要对具有私密性或秘密性的人脸信息进行侵入性侦查。这决定了个案侦查中的人脸信息保护需要法律对执法者进行更为特定具体的授权，对执法者进行更为严格的程序性规范。我国《刑事诉讼法》规定，采取“技术侦查措施”需要“根据侦查犯罪的需要，经过严格的批准手续”“必须严格按照批准的措施种类、适用对象和期限执行”。美国宪法也规定法院发出的搜查令（warrants）必须“有合理根据（probable cause），以宣誓或代誓宣言保证，并具体说明搜查地点和扣押的人或物”，一般性的搜查令（general warrants）与美国宪法相抵触。中美等国家和地区的此类规定，都反映了法律需要对人脸信息的侦查进行严格规范。而且正如上文所述，此类规范需要突破美国法仅关注非公开场所的

制度模块，将人脸信息侦查的全流程纳入法律规范框架。

相较而言，公共监控中的人脸信息具有事前一般预防的特征。就人脸视频监控对象而言，公共监控所收集的人脸信息涉及公共空间的所有个人，而非仅仅刑事个案所涉及的人脸信息。因此就制度而言，人脸视频监控并不需要获得一般性授权，整体坚持“统筹规划、合理适度、标准引领、安全可控”的原则。不过也正是因为其权限较广，其部署应当仅限于公共空间，排除“安装图像采集设备后能够拍摄、窥视、窃听他人隐私”的区域、部位。就监控目的而言，人脸公共视频监控包含了维护公共安全、信息追溯、威慑犯罪与侵权等目的。因此人脸公共视频监控虽然无法获得个体或公众授权，但应该在显著位置设置显著标识，告知公众存在监控视频。公共监控的显著标识除了可以有效威慑犯罪与侵权，对于获取公众信任也有重要意义。如果公共监控视频没有相关提示，甚至在公共空间秘密部署，则公共监控视频就可能变为一般性技术侦查措施，公众可能反而会因此类秘密监控而感到不安全。

对于执法隐私制度涉及的非典型人脸保护场景，执法隐私制度也应进行改造性适用。例如，在企业等私主体的执法场景中，很多企业不仅进行人脸公共视频监控和维护其内部营业安全，而且对此类监控视频进行人脸识别与违法人员筛查。例如，上文提到的娱乐场所利用人脸识别技术筛查未成年人，网约车利用人脸识别技术筛查可疑犯罪分子。此类情形构成私人执法或委托执法（delegated enforcement）。在本文看来，对于私人执法是否应当被允许，私人执法应当遵守何种程序，需要考虑多种因素。就执法权限而言，人脸识别所涉及的违法行为的严重性程度越严重，私人执法者越难找到人脸识别之外替代性的执法方法，人脸识别执法造成的执法错误或附带侵害越小，私人利用人脸技术进行执法就越应当被允许。就执法规范而言，法律需要对私人执法进行严格规范，以避免私人执法对公众权益造成侵害。《公共安全视频图像信息系

统管理条例》对此已经做出若干规范，例如，“建立系统监看、管理等重要岗位人员的入职审查、保密教育、岗位培训等管理制度”“采取授权管理、访问控制等技术措施，严格规范内部人员对视频图像信息的查阅、处理”“建立信息调用登记制度，如实记录查阅、调取视频图像信息的事由、内容及调用人员的单位、姓名等信息”。当私人主体进一步利用此类视频图像进行人脸识别，法律应当在私人主体遵守这些规定的同时，进一步制定其人脸识别执法的程序与制度。

五、结语：制度与场景如何对齐

本文对人脸信息保护进行整体图景分析，指出将人脸信息区分为技术性识别的人脸识别信息和自然识别的人脸图像信息，并对其进行二分保护，会带来很多问题。有的人脸识别场景并不适合适用信息隐私或个人信息保护制度，有的人脸图像信息也可以部分适用信息隐私或个人信息保护制度。人脸图像并不必然具有公开性、非私密性，而人脸识别信息也未必因为其生物性特征而变得具有敏感性、非公开性、私密性特征。这些现象产生的根源在于，人脸信息和其他所有个人信息保护一样，其保护取决于人脸信息流通与利用的场景。如果人脸信息本身进行保护与属性认定，其结果就会导致制度适用悖论，很多制度将无法发挥作用或带来负面效果。

为了超越人脸信息保护的悖论，本文区分了隐私与个人信息保护的三种典型制度模块：侵权隐私、信息隐私与执法隐私。其中侵权隐私是一种横向性制度，这一制度主要维护横向社会主体之间的关系；信息隐私是一种倾斜性制度，这一制度主要维护信息能力不平等主体之间的关系；执法隐私则是一种纵向的制度关系，这一制度主要维护执法者与个体或公众之间的关系。无论是侵权隐私、信息隐私还是执法隐私，法律都需要通过对人脸图像信息或人脸识别信息的保护而实现合理的信息关系，促进横向性、倾斜性与纵向性关系中不同主体的信任。本文将人脸信息保护放置在这三种不同的制度模块下进行分析。其中有的场景完全对应某一制度

模块的典型场景，因此其制度与场景高度对应。但更多的场景则并非完全对应某一制度，对于这些场景，应当对制度模块进行拆分、重组、改造或转型升级，并将改造后的制度适用于这些非典型场景。

人脸信息保护看似是一个小问题，但揭示了具体场景与法律制度对齐的一般原理。在法学研究与法律制度设计中，人们常常会根据直觉对法律适用对象进行分类。例如，在本文的例子中，人们的第一直觉往往区分人脸信息属于人脸识别信息还是属于人脸图像，同时对其进行二分保护。但正如本

文研究所表明的，直觉性的分类可能反而带来更多问题。究其原因，直觉性的分类是人们根据日常经验所形成的第一反应，是人们理解与应对现实世界的表象性认识，而法律制度所要处理的问题往往具有复杂性，需要超越此类直觉性或表象性认识。法律需要既全面深入了解相关场景，又对制度的分类与功能进行更为准确地把握。如此，法律才可以在匹配的场景中适用相关制度，在不匹配的场景中改造与升级相关制度，场景与制度才能真正对齐。

（技术编辑：邓语鑫）