中国人民大学法学院
数字法学教研月报

2025 年第 2 期（总第 14 期） 2025 年 2 月 23 日

本期看点

【数字法治大事件】国家发改委、国家数据局联合发布**《公共数据资源登记管理暂行办法》**，此举意在构建全国一体化的公共数据资源登记体系，推动公共数据资源的规范管理与合理利用。国务院颁布**《公共安全视频图像信息系统管理条例》**，明确划定四类区域为禁止安装图像采集设备的范围。国家网信办发布**《个人信息保护合规审计管理办法》**，对个人信息保护合规审计活动进行了细致规定，进一步提升了个人信息处理活动的合法合规程度。国家数据局印发**《国家数据基础设施建设指引》**，对保障国家数据基础设施建设行稳致远的关键作用。

在地方实践层面，北京市召开 2025 年政务服务和数据管理工作会议，积极推进地方政务服务与数据管理工作的开展。**相关部门发布关于向社会公开征求《数据领域常用名词解释（第二批）》意见的公告，推动数据领域术语规范统一。**这些政策举措和动态信息聚焦于数据资源管理、数据安全保障、个人信息保护等关键领域，进一步推动数据要素的市场化与价值化进程，切实维护数据安全与公民个人隐私权益，促进数据领域的健康、有序、可持续发展。

【研究动态】本期研究动态本期研究动态涵盖数字法学领域多个方面的问题，包括基础理论、个人信息保护、数据确权与流通、人工智能、平台治理、数字行政与司法，以及虚拟财产。学者们就、数据财产法的建构、数据跨境流动、个人信息处理者义务范围界定、人工智能的刑事法律治理、数字平台反垄断、平台义务等重要议题进行了讨论，对于保障公民、小生产者在数字时代的人格利益、经济利益具有重要意义。

【教研活动】涉案虚拟货币处置研讨会在京举行，本次研讨会分为四个单元，与会专家学者、实务届人士就虚拟货币处置的实践难题与应对举措、虚拟币的认定与证明等有关问题进行了充分讨论。

中国人民大学法学院成功举办全国高校涉外法治与数字法学师资公益研讨班。

申卫星教授及课题组成员赴 UNIDROIT 就数字资产法律问题研讨交流。

【数字法评】《重构“知情”：平台间接侵权责任反思》，《东方法学》2025 年第 1 期，作者：丁晓东；《从网络、个人信息到人工智能：数字时代的侵权法转型》，《法学家》2025 年第 1 期，作者：丁晓东。

【数字法案例分析】本期数字法案例分析，由中国人民大学法律硕士朱恬馨撰写。

本案作为技术伦理与法律碰撞的典型，通过界定肖像权边界和统一识别标准，在保护个体尊严与促进技术发展间实现平衡，为数字法治提供实践范本。

本期目录

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 卞 龙 艾 薇 邓语鑫 何 芮 梁因格 李佳丽 林诗敏 麻卓妍 乔彩霞 王 昊 朱恬馨

联系方式：RUCdigitallaw@163.com

本期排版：王昊

数字法治大事件

导言：近期，国家在数据领域出台多项重要政策并开展一系列相关工作，在数据管理、信息保护、资源共享等方面持续发力。国家发改委、国家数据局联合发布《公共数据资源登记管理暂行办法》，此举意在构建全国一体化的公共数据资源登记体系，推动公共数据资源的规范管理与合理利用。国务院颁布《公共安全视频图像信息系统管理条例》，明确划定旅馆客房、学生宿舍、公共浴室等四类区域为禁止安装图像采集设备的范围，有力地保障了公民个人隐私安全。国家网信办发布《个人信息保护合规审计管理办法》，对个人信息保护合规审计活动进行了细致规定，进一步提升了个人信息处理活动的合法合规程度。《人民日报》发文强调推进数据共享对于释放数据价值的重要意义；为贯彻落实党的二十届三中全会关于“建设和运营国家数据基础设施，促进数据共享”的改革任务，国家数据局印发《国家数据基础设施建设指引》，对保障国家数据基础设施建设行稳致远的关键作用。在地方实践层面，北京市召开 2025 年政务服务和数据管理工作会议，积极推进地方政务服务与数据管理工作的开展。《科技日报》发文提出加快建设人工智能高质量数据集，为人工智能发展提供有力支撑。相关部门发布关于向社会公开征求《数据领域常用名词解释（第二批）》意见的公告，推动数据领域术语规范统一。这些政策举措和动态信息聚焦于数据资源管理、数据安全保障、个人信息保护等关键领域，进一步推动数据要素的市场化与价值化进程，切实维护数据安全与公民个人隐私权益，促进数据领域的健康、有序、可持续发展。

国家发改委、国家数据局公布《公共数据资源登记管理暂行办法》

原载：“数据要素社”微信公众号

1 月 20 日，据国家发改委官网消息，国家发展改革委、国家数据局发布了《公共数据资源登记管理暂行办法》（以下简称《管理办法》），自 2025 年 3 月 1 日起施行，有效期 5 年。《管理办法》明确了公共数据资源登记的基本要求，形成全国一体化的公共数据资源登记体系，为建立公共数据资源底账、提高公共数据资源可用性奠定基础。

政策速览：

一、《管理办法》主要有哪些内容？

《管理办法》旨在规范公共数据资源登记工作，构建全国一体化的公共数据资源登记体系，从登记要求、登记程序、登记管理、监督管理等四个方面，明确了登记工作相关主体权利义务和工作流程。

一是针对“谁来登记、谁来负责登记”，确定了登记主体的范围，以及登记机构的基本条件。

二是针对“登记什么”，要求对纳入授权运营范围的公共数据资源进行登记，鼓励对未纳入授权运营范围的公共数据资源进行登记。

三是针对“怎么登记”，规定登记工作按照申请、受理、形式审核、公示、赋码等程序开展，明确首次登记、变更登记、更正登记、注销登记等登记申请类型，以及登记材料提交与审核要求。

四是针对“如何加强登记管理”，《管理办法》提出建设国家公共数据资源登记平台，登记结果统一赋码，推动登记信息互联互通，提高登记服务标准化、便利化。五是针对“如何加强监督管理”，《管理办法》确立了登记工作分级监督管理机制，明确了各级数据管理部门的监管职责，对登记机构、登记主体提出了明确的管理服务要求。

二、公共数据资源登记工作如何开展？

按照《管理办法》要求，开展公共数据资源登记工作重点从以下三个方面着手。

一是梳理纳入登记范围的公共数据资源。直接持有或管理公共数据资源的单位，梳理需要登记的公共数据资源，并按程序提出登记申请。鼓励运营

机构将加工治理形成的数据产品和服务进行登记。登记机构按要求受理审核。

二是依托全国一体化公共数据资源登记平台开展登记业务。加快“一个体系、两级平台”建设，国家公共数据资源登记平台重点支持中央和国家机关及其直属机构、中央企业的公共数据资源登记业务开展，并实现与省级平台的对接。省级平台重点支持本辖区公共数据资源登记工作。制定全国统一的登记结果编码规则，统一赋码，实现登记信息的互联互通。

三是建立登记工作的标准规范。组织力量编制登记制度落地所需的配套标准、规范和指南，细化登记的各项业务流程和标准，规范地方平台建设的技术要求，推进全国登记业务和服务标准化。

政策原文：

国家发展改革委 国家数据局关于印发《公共数据资源登记管理暂行办法》的通知

发改数据规〔2025〕26 号

中央有关部门，国务院各部委、各直属机构，最高人民法院，最高人民检察院，有关人民团体，各省、自治区、直辖市、新疆生产建设兵团发展改革委、数据管理部门，有关中央企业：

为贯彻落实《中共中央办公厅、国务院办公厅关于加快公共数据资源开发利用的意见》，规范公共数据资源登记工作，构建全国一体化公共数据资源登记体系，促进公共数据资源合规高效开发利用，我们制定了《公共数据资源登记管理暂行办法》。现印发给你们，请遵照执行。

国家发展改革委国家数据局

2025 年 1 月 8 日

公共数据资源登记管理暂行办法

第一章 总则

第一条 为促进公共数据资源合规高效开发利用，构建全国一体化公共数据资源登记体系，规范公共数据资源登记工作，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，按照《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》《中共中央办公厅、国务院办公厅关于加快公共数据资源开发利用的意见》要求，制定本办法。

第二条 在中华人民共和国境内开展公共数据资源的登记活动及其监督管理，适用本办法。第三条本办法中的术语含义：

（一）公共数据资源，是指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的具有利用价值的数据集合。

（二）登记主体，是指根据工作职责直接持有或管理公共数据资源的单位，以及依法依规对授权范围的公共数据资源进行开发运营的法人组织。

（三）登记机构，是指由国家和地方数据管理部门设立或指定的、提供公共数据资源登记服务的事业单位。

（四）登记平台，是指支撑公共数据资源登记全流程服务管理的信息化系统。

第四条 公共数据资源登记应当维护国家安全和公共利益，保护国家秘密、商业秘密、个人隐私和个人信息权益，遵循依法合规、公开透明、标准规范、安全高效的原则。

第二章 登记要求

第五条 直接持有或管理公共数据资源的党政机关和事业单位，应对纳入授权运营范围的公共数据资源进行登记，鼓励对未纳入授权运营范围的公共数据资源进行登记。鼓励经授权开展运营活动的法人组织，对利用被授权的公共数据资源加工形成的数据产品和服务进行登记。鼓励供水、供气、供热、供电、公共交通等公用企业对直接持有或管理的公共数据资源及形成的产品和服务进行登记。

第六条 登记机构负责实施公共数据资源登记，执行全国统一的登记管理要求，按照行政层级和属地原则提供规范化、标准化、便利化登记服务。登记机构应建立健全数据资源登记管理责任机制，履行数据安全保护义务，强化数据安全保护技术应用，妥善保管登记信息。中央和国家机关及其直属机构、中央企业的公共数据资源登记，由国家数据局指定所属事业单位负责办理。

第七条 登记主体经业务审核后，通过登记平台提出登记申请，如实准确提供登记材料，并对登记材料内容的真实性、完整性、合法性、有效性负责。涉及多个主体的，可共同提出登记申请或协商一致后由单独主体提出登记申请。

登记主体在申请登记前应在保障安全的前提下对公共数据资源进行存证，确保来源可查、加工可控。

第三章 登记程序

第八条 公共数据资源登记应按照申请、受理、形式审核、公示、赋码等程序开展。

第九条 公共数据资源登记申请类型主要包括首次登记、变更登记、更正登记、注销登记。

（一）首次登记：登记主体应按规定提交主体信息、数据合法合规性来源、数据资源情况、存证情况、产品和服务信息、应用场景信息、数据安全风险评估等申请材料。登记主体在开展授权运营活动并提供数据资源或交付数据产品和服务后，在 20 个工作日内提交首次登记申请。本办法施行前已开展授权运营的，登记主体应按首次登记程序于本办法施行后的 30 个工作日内进行登记。

（二）变更登记：对于涉及数据来源、数据资源情况、产品和服务、存证情况等发生重要更新或重大变化的，或者登记主体信息发生重大变化的，登记主体应及时向登记机构申请变更登记。

（三）更正登记：登记主体、利害关系人认为已登记信息有误的，可以申请更正登记。经登记主体书面同意或有证据证明登记信息确有错误的，登记机构对有关错误信息予以更正。

（四）注销登记：有下列情形之一的，登记主体应申请办理注销登记，登记机构自受理之日起 10 个工作日之内完成注销。

1. 公共数据资源不可复原或灭失的；

2. 登记主体放弃相关权益或权益期限届满的；

3. 登记主体因解散、被依法撤销、被宣告破产或因其他原因终止存续的；

4. 法律法规规定的其他情形。

第十条 登记机构应当自收到申请日起，3 个工作日内予以受理。申请材料不齐全或者不符合规定的，需一次性告知登记主体补充完善，并按新补充后重新提交申请之日起计算受理日期。不予受理的，应当向登记主体及时说明理由。

第十一条 登记机构应当对登记材料内容进行形式审核，自受理之日起 20 个工作日之内完成审核。审核未完成的，应当向登记主体说明原因。

第十二条 登记机构形式审核完成后应当将有关登记信息通过登记平台向社会公示，公示期为 10 个工作日。登记公示内容主要包括登记主体名称、登记类型、登记数据名称、数据内容简介。公示期内对公示信息有异议的，相关当事人应实名提出异议并提供必要证据材料，登记机构应当对提出的异议进行复核，异议成立的，应终止登记。

第十三条 公示期满无异议的，登记机构应按照国家数据局制定的统一编码规范向登记主体发放登记结果查询码。

第四章 登记管理

第十四条 国家数据局加强公共数据资源登记管理，推进登记服务标准化，依托登记信息和政务数据目录，建立健全公共数据资源目录。建设国家公共数据资源登记平台，实现与各省级公共数据资源登记平台对接，推动登记信息互联互通。在全国范围内实现登记结果统一赋码，支撑登记信息的查询和共享。省级数据管理部门应加强集约化建设，统筹开展本辖区公共数据资源登记平台使用管理工作，强化数据共享、应用服务和安全保障。

第十五条 登记结果有效期原则上为三年，自赋码之日起计算。对授权运营范围内的公共数据产品和服务登记，根据授权协议运营期限不超过三年的，登记结果有效期以实际运营期限为准。登记结果有效期届满的，登记主体可在期满前 60 日内按照规定续展。每次续展期最长为三年，自上一届有效期满次日起计算。期满未按规定续展的，由登记机构予以注销。

第十六条 登记机构应按照全国统一的登记要求，优化服务流程，提升登记便利化服务水平。

第十七条 国家数据局统筹开展公共数据资源

登记标准体系和登记工作评价机制建设。省级数据管理部门统筹开展对本辖区登记机构的服务水平评价。

第五章 监督管理

第十八条 全国公共数据资源登记工作实行分级监督管理。国家数据局主管全国公共数据资源登记工作。省级数据管理部门统筹负责本辖区的公共数据资源登记工作。各级数据管理部门应会同有关部门做好跨部门的协同监管。

第十九条 登记机构在登记过程中有下列行为的，由数据管理部门采取约谈、现场指导或取消登记机构资格等管理措施：

（一）开展虚假登记；

（二）擅自篡改、伪造登记结果；

（三）私自泄露登记信息或利用登记信息不当获利；

（四）履职不当或拒不履职的情况；

（五）其他违反法律法规的情况。

第二十条 登记主体有下列行为的，经核实认定后由登记机构撤销登记：

（一）隐瞒事实、弄虚作假或提供虚假登记材料；

（二）擅自篡改、伪造登记结果；

（三）非法使用或利用登记结果不当获利；

（四）其他违反法律法规的情况。

第二十一条 登记机构、登记主体存在违反有关法律行为的，依法承担相关责任；构成犯罪的，依法追究刑事责任。

第六章 附则

第二十二条 各省（自治区、直辖市）数据管理部门可依照本办法制定实施细则。

第二十三条 本办法由国家数据局负责解释。

第二十四条 本办法自 2025 年 3 月 1 日起施行，有效期 5 年，根据情况适时修订调整。

国务院明确！禁止在这些区域安装图像采集设施

原载：“央视新闻”微信公众号

国务院总理李强日前签署国务院令，公布《公共安全视频图像信息系统管理条例》，自 4 月 1 日起施行。《条例》旨在规范公共安全视频系统管理，维护公共安全，保护个人隐私和个人信息权益，共 34 条。要点如下：

严格规范建设，严禁非法乱建

明确县级以上地方人民政府加强统筹规划，避免重复建设，政府有关部门、经营管理单位按照规划、标准建设公共安全视频系统。

除负有经营管理责任、安全防范义务的部门、单位或者个人为维护公共安全所必需建设外，其他任何单位或者个人不得在公共场所安装图像采集设备设施。

禁止在民宿、宿舍、更衣室等能够拍摄、窥视、窃听他人隐私的区域、部位安装图像采集设备设施。

明确在军事禁区、军事管理区以及国家机关等涉密单位周边安装图像采集设备设施的，应当事先征得相关涉密单位同意。

明确各方责任，压实管理义务

明确公共安全视频系统的建设要求，公共安全视频系统管理单位的运行安全职责及视频图像信息使用要求，电信业务经营者对视频图像信息传输的安全管理义务，以及设计、施工、检验、验收、维护等单位对视频图像信息的保密义务。

加大保护力度，确保个人信息安全

明确对保存期限届满后已实现处理目的的视频图像信息应当予以删除。

严格规范国家机关、个人查阅调取视频图像信息的权限、程序。

要求公开传播视频图像信息时严格保护个人、组织相关信息。

明确在非公共场所安装图像采集设备设施不得危害公共安全或者侵犯他人合法权益。

加强监督管理，严格法律责任

明确公安机关的指导和监督管理职责，建立备案和举报制度。

对违法安装图像采集设备设施，或者非法对外提供、公开传播视频图像信息的，没收设备设施、

删除视频图像信息、给予罚款处罚；偷窥、偷拍、窃听他人隐私的，依法给予治安管理处罚；非法获取国家秘密、军事秘密的，依照有关法律规定处罚；构成犯罪的，依法追究刑事责任。

对未履行日常管理和检查义务并造成严重后果的经营管理单位或者个人，给予罚款处罚，根据情节轻重责令暂停业务或者停业整顿、吊销业务许可或者营业执照。

要求公安机关加强内部监督，并对公安机关、其他国家机关及其工作人员的违法违规行为规定了相应的法律责任。

个人信息保护合规审计管理办法

原载：“网信中国”微信公众号

国家互联网信息办公室令 第 18 号

《个人信息保护合规审计管理办法》已经 2024 年 5 月 20 日国家互联网信息办公室 2024 年第 15 次室务会会议审议通过，现予公布，自 2025 年 5 月 1 日起施行。

国家互联网信息办公室主任　庄荣文

2025 年 2 月 12 日

个人信息保护合规审计管理办法

第一条 为了规范个人信息保护合规审计活动，保护个人信息权益，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规，制定本办法。

第二条 在中华人民共和国境内开展个人信息保护合规审计，适用本办法。

本办法所称个人信息保护合规审计，是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动。

第三条 个人信息处理者自行开展个人信息保护合规审计的，应当由个人信息处理者内部机构或者委托专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第四条 处理超过 1000 万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。

第五条 个人信息处理者有以下情形之一的，国家网信部门和其他履行个人信息保护职责的部门（以下统称为保护部门），可以要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计：

（一）发现个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险的；

（二）个人信息处理活动可能侵害众多个人的权益的；

（三）发生个人信息安全事件，导致 100 万人以上个人信息或者 10 万人以上敏感个人信息泄露、篡改、丢失、毁损的。

对同一个人信息安全事件或者风险，不得重复要求个人信息处理者委托专业机构开展个人信息保护合规审计。

第六条 个人信息处理者自行开展或者按照保护部门要求委托专业机构开展个人信息保护合规审计的，应当参照本办法附件《个人信息保护合规审计指引》。

第七条 专业机构应当具备开展个人信息保护合规审计的能力，有与服务相适应的审计人员、场所、设施和资金等。

鼓励相关专业机构通过认证。专业机构的认证按照《中华人民共和国认证认可条例》的有关规定执行。

第八条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当为专业机构正常开展个人信息保护合规审计工作提供必要支持，并承担审计费用。

第九条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当按照保护部门要求选定专业机构，在限定时间内完成个人信息保护合规审计；情况复杂的，报保护部门批准后，可以适当延长。

第十条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，在完成合规审计后，应当将专业机构出具的个人信息保护合规审计报告报送保护部门。

个人信息保护合规审计报告应当由专业机构主要负责人、合规审计负责人签字并加盖专业机构公章。

第十一条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当按照保护部门要求对合规审计中发现的问题进行整改。在整改完成后 15 个工作日内，向保护部门报送整改情况报告。

第十二条 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。提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督。

第十三条 专业机构在从事个人信息保护合规审计活动时，应当遵守法律法规，诚信正直，公正客观地作出合规审计职业判断，对在履行个人信息保护合规审计职责中获得的个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供，在合规审计工作结束后及时删除相关信息。

第十四条 专业机构不得转委托其他机构开展个人信息保护合规审计。

第十五条 同一专业机构及其关联机构、同一合规审计负责人不得连续三次以上对同一审计对象开展个人信息保护合规审计。

第十六条 保护部门对个人信息处理者开展个人信息保护合规审计情况进行监督检查。

第十七条 任何组织、个人有权对个人信息保护合规审计中的违法活动向保护部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

第十八条 个人信息处理者、专业机构违反本办法规定的，依照《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。

第十九条 对国家机关和法律、法规授权的具有管理公共事务职能的组织的个人信息保护合规审计，不适用本办法。

第二十条 本办法自 2025 年 5 月 1 日起施行。

附件个人信息保护合规审计指引

一、本指引根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规制定。

二、对个人信息处理活动的合法性基础进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，是否取得个人同意，该同意是否由个人在充分知情的前提下自愿、明确作出；

（二）基于个人同意处理个人信息的，个人信息的处理目的、处理方式、处理的个人信息种类发生变更的，是否重新取得个人同意；

（三）基于个人同意处理个人信息的，是否依照法律、行政法规取得个人单独同意或者书面同意；

（四）处理个人信息未取得个人同意的，是否属于法律、行政法规规定不需要取得个人同意的情形。

三、对个人信息处理规则进行合规审计的，应当重点审查下列事项：

（一）是否真实、准确、完整地告知个人信息处理者的名称或者姓名和联系方式；

（二）是否以清单等便于查看的形式列明所收集的个人信息及其处理方式和种类；

（三）是否与处理目的直接相关，采取对个人权益影响最小的方式；

（四）是否明确个人信息保存期限或者保存期限的确定方法、到期后的处理方式，以及确定保存期限为实现处理目的所必要的最短时间；

（五）是否明确个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的途径和方法。

四、对个人信息处理者履行告知个人信息处理规则义务进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者在处理个人信息前，是

否以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理规则；

（二）告知文本的大小、字体和颜色是否便于个人完整阅读告知事项；

（三）线下告知是否通过标注、说明等多种方式向个人履行告知义务；

（四）在线告知是否提供文本信息或者通过适当方式向个人履行告知义务；

（五）个人信息处理规则发生变更的，是否将变更内容及时告知个人；

（六）处理个人信息不需要告知的，是否属于法律、行政法规规定应当保密或者不需要告知的情形。

五、对个人信息处理者与其他个人信息处理者共同处理个人信息进行合规审计的，应当重点审查下列事项：

（一）是否约定各自的权利义务；

（二）个人信息权益保护机制；

（三）个人信息安全事件报告机制；

（四）其他法律、行政法规规定需要约定的权利和义务。

六、对个人信息处理者委托处理个人信息进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者在委托处理个人信息前，是否开展个人信息保护影响评估；

（二）个人信息处理者与受托人签订的合同，是否与受托人约定了委托处理的目的、期限、方式、个人信息的种类、保护措施以及双方的权利义务等；

（三）个人信息处理者是否采取定期检查等方式，对受托人的个人信息处理活动进行监督。

七、个人信息处理者存在因合并、重组、分立、解散、被宣告破产等原因需要转移个人信息情形的，应当重点审查个人信息处理者是否向个人告知接收方的名称或者姓名和联系方式。

八、对个人信息处理者向其他个人信息处理者提供其处理的个人信息进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，是否取得个人的单独同意；

（二）是否向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，法律、行政法规规定应当保密或者不需要告知的除外；

（三）是否事前进行个人信息保护影响评估。

九、对个人信息处理者利用自动化决策处理个人信息进行合规审计的，应当重点审查下列事项：

（一）自动化决策的透明度，以及自动化决策的结果是否公平、公正；

（二）是否事前告知个人自动化决策处理个人信息的种类及可能带来的影响；

（三）是否事前进行个人信息保护影响评估；

（四）是否向用户提供保障机制，以便个人通过便捷方式拒绝通过自动化决策方式作出对个人权益有重大影响的决定，并要求个人信息处理者就通过自动化决策方式作出对用户个人权益有重大影响的决定予以说明；

（五）向个人进行信息推送、商业营销的，是否同时提供不针对个人特征的选项，或者提供便捷的拒绝自动化决策服务的方式；

（六）是否采取了有效措施，防止自动化决策根据消费者的偏好、交易习惯等对个人在交易条件上实行不合理的差别待遇；

（七）其他可能影响自动化决策的透明度和结果公平、公正的事项。

十、对个人信息处理者基于个人同意公开个人信息进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者公开其处理的个人信息前是否取得个人单独同意，该授权是否真实、有效，是否存在违背个人意愿将个人信息予以公开的情况；

（二）个人信息处理者公开个人信息前，是否进行个人信息保护影响评估。

十一、个人信息处理者在公共场所安装图像收集、个人身份识别设备的，应当重点对其安装图像收集、个人信息身份识别设备的合法性及所收集个人信息的用途进行审查。审查内容包括但不限于：

（一）是否为维护公共安全所必需，是否为商业目的处理所收集的个人信息；

（二）是否设置了显著的提示标识；

（三）个人信息处理者所收集的个人图像、身份识别信息用于维护公共安全以外用途的，是否取得个人单独同意。

十二、对个人信息处理者处理已公开的个人信息进行合规审计的，应当重点审查个人信息处理者是否存在下列违法违规行为：

（一）向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息；

（二）利用已公开的个人信息从事网络暴力、传播网络谣言和虚假信息等活动；

（三）处理个人明确拒绝处理的已公开个人信息；

（四）对个人权益有重大影响，未取得个人同意；

（五）收集、留存或处理已公开个人信息的规模、时间或使用目的超出合理范围。

十三、对个人信息处理者处理敏感个人信息进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息，是否事前取得个人的单独同意；

（二）基于个人同意处理个人信息的，处理不满十四周岁未成年人的个人信息，是否事前取得未成年人的父母或者其他监护人的同意；

（三）处理敏感个人信息的目的、方式、范围是否合法、正当、必要；

（四）是否在事前进行个人信息保护影响评估；

（五）是否向个人告知处理敏感个人信息的必要性以及对个人权益的影响，法律、行政法规规定应当保密或者不需要告知的除外；

（六）法律、行政法规规定应当取得书面同意的，是否取得书面同意；

（七）是否遵守法律、行政法规对处理敏感个人信息的限制性规定。

十四、对个人信息处理者处理不满十四周岁未成年人个人信息进行合规审计的，应当重点审查下列事项：

（一）是否制定专门的个人信息处理规则；

（二）是否向未成年人及其监护人告知未成年人个人信息的处理目的、处理方式、处理必要性，以及处理个人信息的种类、所采取的保护措施等，法律、行政法规规定不需要告知的除外；

（三）基于个人同意处理个人信息，是否存在强制要求未成年人或者其监护人同意处理非必要个人信息的行为。

十五、对个人信息处理者向境外提供个人信息进行合规审计的，应当重点审查下列事项：

（一）关键信息基础设施运营者向境外提供个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定的，从其规定；

（二）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 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定的，从其规定；

（三）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，是否按照国家网信部门的规定，经个人信息保护认证或者按照国家网信部门制定的标准合同与境外接收方签订合同并向所在地省级网信部门备案，或者符合法律、行政法规、国家网信部门规定的其他条件；

（四）存在向外国司法或者执法机构提供存储于中华人民共和国境内个人信息情形的，是否经过中华人民共和国主管机关批准；

（五）是否向被列入限制或者禁止个人信息提供清单的组织和个人提供个人信息。

十六、对个人信息删除权保障情况进行合规审计的，应当重点审查下列事项：

（一）个人信息处理目的是否已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者是否停止提供产品或者服务，或者个人是否已注销账号；

（三）保存期限是否已届满；

（四）个人是否撤回同意；

（五）个人信息处理者是否违反法律、行政法规或者违反约定处理个人信息；

（六）应当删除个人信息，但法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者是否停止除存储和采取必要的安全措施之外的处理。

十七、对个人信息处理者保障个人在个人信息处理活动中的权利情况进行合规审计的，应当重点审查下列事项：

（一）是否建立便捷的个人行使权利的申请受理机制和处理机制；

（二）是否及时响应个人行使权利的申请，是否及时、完整、准确告知处理意见或者执行结果；

（三）拒绝个人行使权利请求的，是否向个人说明理由。

十八、个人信息处理者应当响应个人申请，对其个人信息处理规则进行解释说明，合规审计时应当重点对下列内容进行评价：

（一）个人信息处理者是否提供便捷的方式和途径，接受、处理个人关于个人信息处理规则解释说明的要求；

（二）接到个人的要求后，个人信息处理者是否在合理的时间内，使用通俗易懂的语言对其个人信息处理规则作出解释说明。

十九、个人信息处理者应当依照法律、行政法规的规定制定内部管理制度和操作规程，明确组织架构、岗位职责，建立工作流程、完善内控制度，保障个人信息处理合规与安全。合规审计时，应当重点对个人信息处理者个人信息保护内部管理制度和操作规程进行审查，包括但不限于：

（一）个人信息保护工作的方针、目标、原则是否符合法律、行政法规规定；

（二）个人信息保护组织架构、人员配备、行为规范、管理责任是否与应当履行的个人信息保护责任相适应；

（三）是否根据个人信息的种类、来源、敏感程度、用途等，对个人信息进行分类；

（四）是否建立个人信息安全事件应急响应机制；

（五）是否建立个人信息保护影响评估制度、合规审计制度；

（六）是否建立畅通的个人信息保护投诉举报受理流程；

（七）是否合理制定个人信息处理操作权限；

（八）是否制定实施个人信息保护安全教育和培训计划；

（九）是否建立个人信息保护负责人及相关人员履职评价制度；

（十）是否建立个人信息违法处理责任制度；

（十一）法律、行政法规规定的其他事项。

二十、个人信息处理者应当采取与所处理个人信息规模、类型相适应的安全技术措施，并对个人信息处理者采取的技术措施的有效性进行评价，评价内容包括但不限于：

（一）是否采取相应安全技术措施实现个人信息的保密性、完整性、可用性；

（二）是否采取加密、去标识化等安全技术措施，确保在不借助额外信息的情况下，消除或者降低个人信息的可识别性；

（三）采取的安全技术措施能否合理确定有关人员查阅、复制、传输个人信息等的操作权限，减少个人信息在处理过程中未经授权的访问和滥用风险。

二十一、对个人信息处理者教育培训计划的制定和实施情况进行合规审计时，应当重点对下列事项进行评价：

（一）是否按计划对管理人员、技术人员、操作人员、全员开展相应的安全教育和培训，是否对相应人员的个人信息保护意识和技能进行考核；

（二）培训内容、方式、对象、频率等能否满

足个人信息保护需要。

二十二、对个人信息处理者指定的个人信息保护负责人履职情况进行合规审计的，应当重点审查下列事项：

（一）个人信息保护负责人是否具有相关的工作经历和专业知识，熟悉个人信息保护相关法律、行政法规；

（二）个人信息保护负责人是否具有明确清晰的职责，是否被赋予充分的权限协调个人信息处理者内部相关部门与人员；

（三）个人信息保护负责人在个人信息处理重大事项决策前是否有权提出相关意见和建议；

（四）个人信息保护负责人是否有权对个人信息处理者内部个人信息处理的不合规操作进行制止和采取必要的纠正措施；

（五）个人信息处理者是否公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送保护部门。

二十三、对个人信息处理者开展个人信息保护影响评估情况进行合规审计时，应当重点对影响评估开展情况和评估内容进行审查：

（一）是否依照法律、行政法规的规定，在进行对个人权益具有重大影响的个人信息处理活动前进行个人信息保护影响评估；

（二）是否对个人信息的处理目的、处理方式等进行合法、正当、必要评估；

（三）是否对个人权益的影响及安全风险进行评估；

（四）是否对所采取的保护措施的合法性、有效性，以及与风险程度的适应性进行评估。

二十四、个人信息处理者应当制定个人信息安全事件应急预案。合规审计时，应当对应急预案的全面性、有效性、可执行性作出评价，包括但不限于下列内容：

（一）是否结合业务实际，对面临的个人信息安全风险作出系统评估和预测；

（二）总体要求、基本策略，组织机构、人员，技术、物资保障，指挥处置程序，应急和支持措施等是否足以应对预测的风险；

（三）是否对相关人员进行应急预案培训，定期对应急预案进行演练。

二十五、对个人信息处理者个人信息安全事件应急响应处置情况进行合规审计的，应当重点审查下列事项：

（一）是否按照应急预案、操作规程及时查明个人信息安全事件的影响、范围和可能造成的危害，分析、确定事件发生的原因，提出防止危害扩大的措施方案；

（二）是否建立通报渠道，在安全事件发生后按照相关规定及时通知保护部门和个人；

（三）是否采取相应措施将个人信息安全事件可能造成的损失和可能产生的危害风险降低到最小。

二十六、对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者制定的平台规则进行合规审计的，应当重点审查下列事项：

（一）平台规则是否与法律、行政法规相抵触；

（二）平台规则个人信息保护条款的有效性，是否合理界定了平台、平台内产品或者服务提供者的个人信息保护权利和义务；

（三）平台规则的执行情况，是否通过抽样等方式验证平台规则被有效执行。

二十七、对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者发布的个人信息保护社会责任报告进行合规审计的，应当重点审查社会责任报告披露下列内容的情况：

（一）个人信息保护组织架构和内部管理情况；

（二）个人信息保护能力建设情况；

（三）个人信息保护措施和成效；

（四）个人行使权利的申请受理情况；

（五）独立监督机构履职情况；

（六）重大个人信息安全事件处理情况；

（七）促进个人信息保护社会共治的科普宣传、公益活动情况；

（八）法律、行政法规规定的其他事项。

人民日报 | 推进数据共享 释放数据价值

原载：“国家数据局”微信公众号

今年全国数据工作的一个重要方向，是大力推进数据要素的市场化价值化。如何推动公共数据资源开发利用、更好发挥数据要素作用？怎样打造更多数据应用场景？国家数据局 2 月 18 日举行“数据价值化，我们在行动”系列新闻发布会第一场，国家数据局等有关部门负责人介绍了相关情况。

推进政务数据共享应用

“推动数据价值化，公共数据要先行一步，真正把公共数据资源供出来、用起来。”国家数据局副局长陈荣辉说。

去年 10 月，《中共中央办公厅 国务院办公厅关于加快公共数据资源开发利用的意见》公开印发。据介绍，全国数据系统在配套制度建设、政务数据共享、数据授权运营、应用创新实践等方面开展一系列工作，有些方面取得初步进展。

在推进政务数据共享应用方面，明确数据治理和共享责任，推动“一次填报，多方共用”，推动数据由“向基层要”变为“从系统取”，切实减轻基层干部重复报数负担。同时推动数据回流，支持基层干部利用数据更好为企业和百姓服务，助力提升基层治理水平。

以福建为例，2020 年，福建入选国家公共数据资源开发利用 8 个试点省份之一。该省依托省市两级公共数据汇聚共享平台，接入全省 2000 余个政务信息系统、汇聚 1800 多亿条有效数据，基本实现全省政务信息系统“应接尽接”和全省公共数据“应汇尽汇”。并以汇聚共享平台为枢纽，常态化开展公共数据共享申请、授权、对接、应用，目前平台日均批量交换数据 1.5 亿多条，有效支撑各地各部门 800 多个应用场景。

探索公共数据授权运营

探索公共数据授权运营，这是近来数据领域的热词，如何理解？

陈荣辉表示，授权运营是一种新的数据供给方式，目的是通过引入专业化力量，对公共数据进行治理、加工，形成数据产品和服务，在保障安全的前提下更好满足社会用数需求、更好促进数字经济发展。目前，很多部委都在按政策文件要求，梳理拟授权运营的数据资源，编制数据授权运营方案，积极推进数据资源和产品登记工作。

据介绍，国家公共数据资源登记平台将于 3 月 1 日正式上线试运行。“这个平台不仅是公共数据资源的管理系统，也是信息披露和资源发现的窗口，全社会都可以来这里找数据、找产品。”陈荣辉说。

根据会上发布的信息，直接持有或管理公共数据资源的党政机关和事业单位，应对纳入授权运营的公共数据资源进行登记。未纳入授权运营范围的数据资源，以及利用被授权数据资源加工形成的数据产品和服务，也鼓励进行登记。

陈荣辉介绍，登记平台上线运行后，将发挥两个方面的作用：一是服务性功能，供数单位可以通过登记平台发布数据资源和产品信息，用数单位可以来这里查找数据资源，未来还可以发布数据需求，从而更好地实现供需对接，为降低全社会用数成本、促进数据资源价值释放创造条件。二是管理功能，通过登记工作，掌握全国公共数据资源底账，加强授权运营信息披露，促进授权运营规范化、透明化。

打造更多数据应用场景

数据价值化，要在场景应用中得以实现。

例如，气象数据与经济社会千行百业息息相关，应用场景广阔、发展潜力巨大。深圳市围绕低空物流企业需求，为起降点及航线提供 1 公里分辨率，分钟级更新的大风、降水等精细化服务，减少因恶劣天气导致的延误或损失，让配送计划更合理、经济。上海基于气象数据决策开展无人机消减雾试验，能见度可从 500 米快速提升至 2 公里以上，为降低大雾天气对飞行“窗口期”影响提供了支持。

中国气象局预报司副司长张洪政介绍，中国气象局还积极对接新能源规划选址、高效消纳和安全运行对精细化气象数据的需求，引导鼓励各方加入示范场景共建，创新新能源气象服务产品和解决方案，为国家能源绿色低碳转型、能源安全提供支撑。

各地区各部门对发挥数据要素作用都高度重

视，比如，今年福建省政府工作报告提出，深化“千行百业”行动，聚焦重点领域，培育更多数字应用场景。重庆市提出要扩大数据流通和价值示范，培育实数融合新业态。国家数据局会同相关地方和部门重点打造一批示范性数据应用场景，探索形成可复制、可推广模式。

陈荣辉表示，下一步，将加快推动公共数据资源管理和运营机制改革落地见效，进一步增强数据资源价值释放的驱动力，以公共数据开发利用引领撬动各方数据的融合应用，打造数据利用的多应用场景和模式，更好释放数据要素价值。

专家解读之六 | 扎实推进数据标准化工作 保障国家数据基础设施建设行稳致远

原载：“国家数据局”微信公众号

文 | 中国电子技术标准化研究院院长 杨旭东

为贯彻落实党的二十届三中全会关于“建设和运营国家数据基础设施，促进数据共享”的改革任务，近日，国家数据局印发《国家数据基础设施建设指引》（以下简称《建设指引》）。《建设指引》阐述概念内涵，描绘发展愿景，提出总体功能、总体架构与重点方向，构建算力底座，给出网络支撑、安全防护与组织保障的工作方向，是夯实数字经济发展基础的重要指导性文件，有效支撑构建促进数字经济发展体制机制，推进数据服务千行百业、深度融入社会生产生活，推动数据要素“供得出、流得动、用得好，保安全”。标准是国家竞争力的基本要素，是规范经济和社会发展的重要技术制度，是统筹数据工作的重要抓手。《建设指引》中提出，“国家数据基础设施是从数据要素价值释放的角度出发，面向社会提供数据采集、汇聚、传输、加工、流通、利用、运营、安全服务的一类新型基础设施，是集成硬件、软件、模型算法、标准规范、机制设计等在内的有机整体”，标准规范已成为国家数据基础设施的重要组成，在国家数据基础设施建设中起到了关键的支撑作用。

一、标准规范是国家数据基础设施建设的“先手棋”

（一）夯实数据互联互通基础

数据流通利用设施是国家数据基础设施的重要组成部分，建设数据流通利用设施底座以统一目录标识、统一身份登记、统一接口为前提。《建设指引》提出，“制定统一目录标识、统一身份登记、统一接口要求的标准规范，夯实数据基础设施互联互通技术基础”。通过对数据流通利用设施参考架构、能力基本要求、应用成熟度评价、数据目录通用要求、数字合约与使用控制协议要求等方面进行规范，以标准为手段将目录标识管理、数字身份管理和接入、跨平台接口等技术要求在数据流通利用设施建设初期予以明确，助力实现数据基础设施的互联互通。

（二）促进数据资源有效供给

高质量数据是国家数据基础设施建设、赋能人工智能等新兴产业发展的根基。《建设指引》提出，“研究制定高质量数据集建设相关标准”，通过制定训练数据集采集处理、标注、合成等标准，从数据生成、注释定义到数据管理的全过程，确保数据标注的准确性和数据模型的专业性，为数据资源应用水平提升提供标准支撑。

（三）保障数据流通安全合规

《建设指引》提出，“建立数据流通准入标准规则，鼓励探索数据流通安全保障技术、标准、方案”。通过建立数据流通准入标准规则体系，规范数据流通安全合规相关要求，预防数据滥用和泄露，增强不同行业、不同机构、不同部门对数据流通的信任度，支持保障数据在跨行业和跨领域间的大规模、低成本、安全自由流通，为数据要素市场安全高效运行提供基础保障。

二、标准规范是国家数据基础设施建设的“助推器”

（一）标准规范推动数据有序采集汇聚

以标准为手段统一数据格式、定义和质量，可实现组织、行业间不同来源和类型数据的有效整合和利用，通过数据标准的贯彻实施，对数据分类、术语、数据元和代码集等关键数据进行统一管理，

使数据从产数源端到消费终端均能够准确识别理解其代表的结构和含义，减少数据冗余，消除数据孤岛，促进数据资源的共享与互认。

（二）标准规范推动数据可信流通利用

标准可为数据的合法、合规使用提供框架，通过对可信数据空间的参考架构及组件、连接协议、数据传输网络、可信安全能力、数据交易系统等方面进行标准化，统一标准通信交互协议，明确通信安全、系统安全以及身份认证安全等级别和能力，并通过记录和执行数据流通过程中的规则定义、标准符合性检测以及质量要求，有效降低数据流通中的安全风险。

（三）标准规范推动数据高效传输加工

通过制定并应用规范统一的数据标准，对数据结构和含义进行数字化建设与管理，可有效支撑数据使用方快速定位和使用所需的数据元，提高数据应用的效率和准确性，确保数据在处理和使用的传输供给过程中的一致性，降低数据传输和加工成本，推动数据多场景应用、跨主体复用。

三、标准规范是国家数据基础设施建设的“顶梁柱”

（一）积极探索数据基础设施标准化建设

我国在数据基础设施建设上已开启了积极探索，仍存在数据流通利用基础设施架构待统一、数据算力度量和资源调度难度大等问题。目前正在研制数据流通利用设施总体框架、对接要求、统一数字身份管理和接入规范、统一标识管理规范、跨平台互联互通接口要求、接入连接器通用能力要求、接入连接器互操作规范以及数据算力调度、数据算力度量等标准，逐步形成统一目录标识、统一身份登记、统一接口要求，进而夯实数据流通利用设施底座。

（二）充分发挥全国数标委的布局规划作用

2024 年 9 月，《国家数据标准体系建设指南》正式印发，提出了数据标准体系建设及落实落地的目标要求，强调了数据基础设施重点标准的研制和推广。2024 年 10 月，全国数据标准化技术委员会（以下简称“全国数标委”）正式成立，明确支撑数据流通利用的数据基础设施标准化建设要求，下设数据基础设施标准工作组（WG6），务实推进数据基础设施标准研制及推广，进一步发挥标准在数据基础设施建设、数据高效有序流通利用等方面的基础支撑作用。

（三）扎实推进数据基础设施标准化重点任务

2024 年 10 月，全国数标委第一次全体委员会议召开，明确数据基础设施标准工作组主要负责调研数据基础设施标准现状与发展趋势，开展支撑数据流通利用的数据基础设施标准制修订工作，推动相关标准宣传推广及应用实施。同时，通过 2024—2025 年工作要点，规划重点工作任务，要求研究制定数据目录标识、数字身份登记、互联互通接口、算力度量、算力并网、算力调度等标准，为全国一体化算力网及数据流通利用基础设施建设提供支撑，为加快推进数据基础设施标准化工作提供助力。

四、充分发挥标准规范的支撑作用，推动《建设指引》贯彻落实

（一）强化数据基础设施标准组织运营支撑

做好全国数标委数据基础设施标准工作组的运营工作，按照《建设指引》，建立健全数据基础设施标准化路径，加快重点任务部署，深化重点方向研究。鼓励技术创新探索，加快数据基础设施关键技术攻关和重大成果转化。

（二）明确数据基础设施重点标准研制方向

《建设指引》提出，“强化标准支撑，研究制定数据基础设施相关标准规范”。按照“急用先行”的原则，加快推进数据算力、数据流通利用基础设施、可信数据空间、数据质量管理系统、数据登记平台通用技术等方面重点标准研制，扎实做好全国数标委 2024—2025 年工作要点部署的数据基础设施标准化重点工作任务。

（三）大力推进数据基础设施标准应用推广

推动数据算力、数据流通利用基础设施、可信数据空间、数据质量管理系统、数据登记平台通用技术等标准的试验验证，及时总结数据标准化典型做法和实践经验，服务标准制修订。广泛开展地区、

行业重点数据标准应用试点，打造可复制、可推广的数据基础设施标准化示范案例，进一步繁荣数据产业生态。推动数据与行业应用融合发展，探索研究一批融合应用的数据基础设施标准，推进数据基础设施标准工作向各行业、区域衍伸发展。

（四）探索数据格式标准符合性检测先行先试

探索形成从标准文档、标准术语、数据元、数据模型完整统一的数据标准数字化管理体系，运用标准符合性检测工具建立数据格式规范化校验和数据质量检测能力，充分落实数据领域各类数据元、数据集标准的执行，为数据的源头治理、质量管理提供支撑，加快形成可复制推广的工作模式，助力数据基础设施建设的标准化、规范化。

（五）深化数据基础设施标准国际合作

《建设指引》提出，“鼓励企业、社会团体、科研机构参与数据基础设施国际标准的制定工作。加强与 ISO、IEC、ITU、IEEE、3GPP 等国际标准化组织的合作，推动数据领域高水平专家在国际组织任职”。要积极关注国际标准化组织动态，加强与国际标准组织的交流与合作，深入参与并积极承担国际组织工作，主动承接国际标准化活动。联合国内外专家、学者共同开展数据领域国际标准研制，推动我国标准成为国际标准，建立国际标准化工作生态圈，深化数据领域的多边合作互利共赢。

地方动态 | 北京市召开 2025 年政务服务和数据管理工作会议

原载：“国家数据局”微信公众号

2 月 19 日，北京市召开 2025 年政务服务和数据管理工作会议。会议深入贯彻习近平新时代中国特色社会主义思想，全面贯彻党的二十届三中全会、中央经济工作会议和全国数据工作会议精神，落实市委市政府决策部署，总结 2024 年工作，部署 2025 年重点任务。围绕全市数据工作，会议指出，2024 年我市提出数据要素“一区三中心”发展思路和定位，各项工作取得新突破。会议强调，2025 年要以更高起点推进数据管理工作。一是要充分发挥首都数据优势禀赋，推进“一区三中心”落地见效，围绕数据要素市场化配置改革这条主线，健全数据基础制度，超前布局数据基础设施，不断激活数据要素价值，做大做强数据产业，加快培育新质生产力，全面赋能经济社会发展。二是要加快国家数据要素综合试验区建设，构建适应数据要素特征、符合市场规律、契合发展需要的基础制度，促进数据“供得出、流得动、用得好、保安全”，力争取得一批标志性成果，为全国数据要素市场化配置改革提供经验借鉴。三是要贯通推进各项重点任务，强化智慧城市协同创新仿真实验平台、数据流通利用增值协作网络、“数据要素×”行动、大数据平台等工作协同联动，深化“三京”“三个一网”应用，打造智慧城市场景创新和综合应用示范。四是要落实京津冀协同发展战略，构建三地数据互信互认、交易所互联互通、政策互融互补合作机制。五是要加强国际交流互鉴，打造数据领域国际交流合作窗口，积极参与国际数据标准体系建设。各区、各相关部门主管负责同志，部分央（市）属企业和数商企业有关代表参加会议。

科技日报 | 加快建设人工智能高质量数据集

原载：“国家数据局”微信公众号

文|中国科学院科技战略咨询研究院研究员 王晓明

当前，人工智能处在快速发展的关键时期，正在重塑经济社会发展模式。2024 年中央经济工作会议指出，开展“人工智能+”行动，培育未来产业。数据作为人工智能发展的三大核心要素之一，是人工智能模型训练的基础要素，也是人工智能模型应用的核心资源，加快建设人工智能高质量数据集，对于推动“人工智能+”场景落地具有重要意义。

高质量数据集建设存在的问题

高质量数据供给是推动新一代人工智能加快发展的关键要素。当前，面向新一代人工智能的数据供给仍有不足，数据处理专用技术有待进一步突破，数据产业和数据生态有待丰富，高质量数据集的整体规划和支持政策还有待完善。

首先，通用领域、垂直领域以及具身智能领域的高质量数据供给仍有不足。一方面，中文公开数据在质量和数量方面落后于英文数据。另一方面，我国公共数据开放利用程度有待提高，各地开放标准不统一，专门面向人工智能发展的高质量行业数据集仍较匮乏。具身智能领域真实交互数据采集不足，主要原因在于智能机器人与环境的交互数据获取困难且成本高昂，同时，企业采集数据缺乏统一的参照标准。

其次，高质量数据的合成、处理和利用技术亟待提升。利用深度学习和强化学习生成高精确度、多样化合成数据的技术在成熟度和应用范围上急需突破。随着社会自动化和智能化程度的不断提高，对数据处理的要求也不断提升，因此急需针对结构化、半结构化和非结构化数据的处理技术进行迭代优化，进一步提高数据处理效率。

再次，数据主体和商业模式发展尚不成熟。我国缺乏类似美国 Databricks 和 Snowflake“数据+人工智能”模式的高质量数据汇聚和治理主体，具备大规模数据汇聚管理分析能力的公司数量不足。医疗、法律、保险、金融、工业、科研等多个领域的公共数据授权运营主体目前仍在培育中，数据集构建和运营利用的商业模式发展还不够成熟。

最后，高质量数据集的专项规划和支持政策有待完善。我国已出台一系列数据发展相关指引政策，但是面向新一代人工智能模型训练和场景应用的高质量数据集专项规划和支持政策尚未出台，其建设、运营、流通、利用等方面举措有待进一步细化。在数据采集方面，各领域数据缺乏适用的标准规范；在数据使用方面，缺少面向大模型和具身智能模型训练的数据共享和流通促进机制，一定程度上限制了模型能力的快速提升。

多措并举建设高质量数据集

针对当前存在的资源、技术、模式、制度等方面问题，结合新一代人工智能发展的需要，建议发挥政府和市场的协同作用，多措并举推进高质量数据集建设。

一是加快公共数据开放和企业数据流通，建设面向新一代人工智能的高质量数据集。建议形成部门、行业、地区共同参与的协同机制，围绕高质量数据集建设，扩大数据供给范围和规模，完善公共及行业数据标准，加速可信数据空间建设。面向医疗、教育、科研、法律、工业、农业、物流、金融、能源、交通等重点领域建设大数据中心及大模型行业应用创新（工程）中心，打破信息孤岛，构建完备数据生态，构建高质量数据集，提升垂直领域人工智能模型能力。着眼自动驾驶、具身智能等未来产业需求，开放相关公共数据，制定行业数据标准，探索企业间数据流通机制，鼓励企业和研究机构创建高质量行业数据集。

二是围绕建设行业高质量数据集关键技术问题加大攻关力度。面向数据合成和处理，加快开发数据合成、数据治理的关键共性技术；面向数据流通汇聚，大力推广隐私计算、区块链等技术；面向“数据+人工智能”应用模式，着力开发数据管理技术，探索新型模型结构和训练架构。鼓励面向人工智能的数据产品、数据服务企业牵头承担国家重大项目，开展应用基础研究和关键核心技术攻关。推动产学研合作和创新联合体建设，打造数据技术、产品和服务深度融合的新型合作模式。面向重点场景，打造数据技术“测试场”，提供真实数据环境、模拟应用场景，建设中试基地，吸引企业、高校和科研机构参与数据技术的创新和验证，加速新技术推广和应用。

三是引导企业和商业模式创新，构建人工智能数据产业生态。大力培育人工智能数据资源、技术、服务、应用、安全、基础设施等多领域企业，重点建设面向人工智能行业的数据产业创新平台。鼓励企业基于“数据+人工智能”探索多领域商业模式，支持企业与各方合作，打造基于高质量数据集的产业创新链和生态系统。鼓励企业探索大模型和具身智能应用场景，驱动数据产业发展。支持模型应用、模型开发、数据服务、数据产品等相关企业组建创新联合体，开发高质量数据集，发展“数据即服务”“知识即服务”“模型即服务”等新业态。

四是加大人工智能高质量数据集建设政策支

持力度。面向新一代人工智能技术开发和应用发展需求，完善数据资源构建体系，培育数据产业，支持数据技术发展，系统推进高质量数据集建设，强化行业应用。统筹中央和地方财政资金、产业引导基金和各类政策性投资，加大对高质量数据集建设的投入。鼓励金融机构创新产品和服务，增加对数据相关企业的融资支持。引导社会资本有序参与人工智能高质量数据集的开发利用。

关于向社会公开征求《数据领域常用名词解释（第二批）》意见的公告

原载：“国家数据局”微信公众号

为进一步凝聚共识，推动社会各界对数据领域术语形成统一认识和理解，现就《数据领域常用名词解释（第二批）》向社会公开征求意见。

此次征求意见的时间是 2025 年 1 月 23 日至 2 月 16 日。欢迎社会各界人士提出意见，请通过电子邮件方式将意见发送至 gjsjjzcs@126.com。

感谢您的参与和支持！附件：数据领域常用名词解释（第二批）

数据领域名词解释起草专家组

2025 年 1 月 23 日

附件

数据领域常用名词解释（第二批）

1.**数据产权**，是指权利人对特定数据享有的财产性权利，包括数据持有权、数据使用权、数据经营权等。

2.数据产权登记，是指数据产权登记机构按照统一的规则对数据的来源、描述、合规等情况进行审核并记载，并出具登记凭证的行为。

3.数据持有权，是指权利人自行持有或委托他人代为持有合法获取的数据的权利，旨在防范他人非法违规窃取、篡改、泄露或者破坏持有权人持有的数据。

4.数据使用权，是指权利人通过加工、聚合、分析等方式，将数据用于优化生产经营、形成衍生数据等的权利。一般来说，使用权是权利人在不对外提供数据的前提下，将数据用于内部使用的权利。

5.数据经营权，是指权利人通过转让、许可、出资或者设立担保等有偿或无偿的方式对外提供数据的权利。

6.衍生数据，是指数据处理者对其享有使用权的数据，在保护各方合法权益前提下，通过利用专业知识加工、建模分析、关键信息提取等方式实现数据内容、形式、结构等实质改变，从而显著提升数据价值，形成的数据。

7.企业数据，是指企业在生产经营过程中形成或合法获取、持有的数据。

8.数据交易机构，是指为数据供需多方提供数据交易服务的专业机构。

9.数据场内交易，是指数据供需方通过数据交易机构达成数据交易的行为。

10.数据场外交易，数据供需方不通过数据交易机构达成数据交易的行为。

11.数据撮合，是指帮助数据供需方达成数据交易的行为。

12.第三方专业服务机构，为促进数据交易活动合规高效开展，提供数据集成、数据经纪、合规认证、安全审计、数据公证、数据保险、数据托管、资产评估、争议仲裁、风险评估、人才培训等第三方服务的专业化组织。

13.数据产业，是指利用现代信息技术对数据资源进行产品或服务开发，并推动其流通应用所形成的新兴产业，包括数据采集汇聚、计算存储、流通交易、开发利用、安全治理和数据基础设施建设等。

14.数据标注产业，是指对数据进行筛选、清洗、分类、注释、标记和质量检验等加工处理的新兴产业。

15.数字产业集群，是指以数据要素驱动、数字技术赋能、数字平台支撑、产业融通发展、集群生态共建为主要特征的产业组织新形态。

16.可信数据空间，是指基于共识规则，联结多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，

是支撑构建全国一体化数据市场的重要载体。可信数据空间须具备数据可信管控、资源交互、价值共创三类核心能力。

17. 数据使用控制，是指在数据的传输、存储、使用和销毁环节采用技术手段进行控制，如通过智能合约技术，将数据权益主体的数据使用控制意愿转化为可机读处理的智能合约条款，解决数据可控的前置性问题，实现对数据资产使用的时间、地点、主体、行为和客体等因素的控制。

18. 数据基础设施，是从数据要素价值释放的角度出发，面向社会提供数据采集、汇聚、传输、加工、流通、利用、运营、安全服务的一类新型基础设施，是集成硬件、软件、模型算法、标准规范、机制设计等在内的有机整体。

19. 算力调度，本质是计算任务调度，是基于用户业务需求匹配算力资源，将业务、数据、应用调度至匹配的算力资源池进行计算，实现计算资源利用效率最大化。

20. 算力池化，是指通过算力虚拟化和应用容器化等关键技术，对各类异构、异地的算力资源与设备进行统一注册和管理，实现对大规模集群内计算资源的按需申请与使用。

君合法评丨要点简析：《个人信息保护合规审计管理办法》正式出台

原载：“君合法律评论”微信公众号

2025 年 2 月 14 日，国家互联网信息办公室正式发布《个人信息保护合规审计管理办法》（以下简称“《审计办法》”），自 2025 年 5 月 1 日起施行。《审计办法》的发布，标志着《个人信息保护法》（以下简称“《个保法》”）所设立的个人信息保护合规审计制度正式进入落地实施阶段。

下文中，我们将通过问答的形式简析《审计办法》的核心要点，为企业开展个人信息保护合规审计（以下简称“合规审计”）提供参考。

一、合规审计是企业必须开展的吗？

个人信息保护合规审计是所有在中国境内处理个人信息的企业应当履行的合规义务。该义务明确规定于《个保法》第 54 条、第 64 条和《网络数据安全管理条例》第 27 条。

因此，所有在境内处理个人信息的企业都应定期开展合规审计，以对个人信息保护合规落实情况进行审查、评价和监督。

二、合规审计与企业日常合规管理工作有什么差别？

根据《审计办法》，个人信息保护合规审计，是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动。因此，合规审计本质是监督工作，与企业日常开展的合规管理工作（例如个人信息保护影响评估、风险评测等）存在区别。

从制度逻辑上看，独立性是审计的核心特征。一般认为，合规审计独立于日常合规管理，并作为企业的最后一道风险管理防线。从内容上看，日常合规管理工作的执行情况和有效性是合规审计的对象，日常合规管理工作所形成的评估报告、评测结果、处理记录亦为合规审计提供了重要的证据。从开展形式上看，日常合规工作往往针对特定项目或单个信息处理活动而启动，合规审计则是对企业的个人信息处理活动是否遵守法律、行政法规的情况进行的整体审查和评价。

三、企业应当在何时开展合规审计？

整体上，合规审计的开展分为两种情形：一是企业自行开展的合规审计，二是监管机关在特定情形下要求企业开展合规审计。

1. 企业自行开展的合规审计

对于企业自行开展的合规审计，《个保法》第 54 条及《网络数据安全管理条例》第 27 条仅要求合规审计应“定期”开展，但未明确具体开展的频率。《审计办法》根据个人信息处理者的处理活动规模，进一步要求处理超过 1000 万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。但对于处理个人信息数量低于 1000 万人的个人信息处理者，《审计办法》并未设置强制性的合规审计开展频率的要求。

对此，企业在判断自行开展合规审计的频率时，我们建议企业关注和考虑以下事项：

“1000 万人个人信息”的计算。《审计办法》并未明确“1000 万人个人信息”的计算标准。我们理解，实践中，企业在不同的业务场景下可能有不同的数据处理身份，例如针对 A 场景构成个人信息处理者，而针对 B 场景构成受托处理者。就 B 场景中企业作为受托处理者所处理的个人信息规模是否要纳入“1000 万人个人信息”的计算范围，有待监管部门的进一步澄清。

处理未成年人个人信息的特别审计要求。根据《未成年人网络保护条例》第 37 条，个人信息处理者应当自行或者委托专业机构每年对其处理未成年人个人信息遵守法律、行政法规的情况进行合规审计，并将审计情况及时报告网信等部门。因此，企业需要结合自身的业务模式和个人信息处理活动，评估是否触发未成年人个人信息的定期合规审计要求。

对于信息处理规模少于 1000 万人个人信息的企业，在确定合规审计的频率时，我们建议企业综合考虑：自身处理个人信息的规模和敏感程度、业务和个人信息处理活动的变化情况、集团的统一的合规安排、自身数据违规、安全及泄露的情况、面临的内外部环境相关情况（如立法执法趋势、已有的监管行动、行业自律行为、过往风险评估记录等），设置合理的审计计划安排和工作体系。

考虑到《个保法》已经生效实施 3 周年，我们建议企业可以考虑在《审计办法》生效后（即 2025 年 5 月 1 日后），根据自身的情况，考虑在适当的时间点进行首次审计，以满足《个保法》的合规审计要求。

2. 监管机关要求企业发起的合规审计

除了企业自行开展的合规审计，监管机关有权在发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。该等情形包括：（1）发现个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险的；（2）个人信息处理活动可能侵害众多个人的权益的；（3）发生个人信息安全事件，导致 100 万人以上个人信息或者 10 万人以上敏感个人信息泄露、篡改、丢失、毁损的。

在监管部门要求企业发起的合规审计中，按照《审计办法》的规定，企业应当：

（1）协助配合审计：为专业机构正常开展个人信息保护合规审计工作提供必要支持，并承担审计费用。

（2）按时完成审计：在限定时间内完成个人信息保护合规审计；情况复杂的，报保护部门批准后，可以适当延长。

（3）开展整改：应当按照专业机构给出的整改建议进行整改。

（4）成果报送：将专业机构出具的合规审计报告及整改情况报送履行个人信息保护职责的部门。

四、合规审计应当由谁来具体开展？

对于企业自行开展的合规审计，可以由企业内部，或者企业自行委托第三方专业机构来完成。但对于监管部门要求企业开展的合规审计，企业必须委托第三方专业机构开展审计。

另外，《审计办法》进一步规定，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。由于此前《个保法》第 52 条仅规定“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”而未明确规定数量，《审计办法》则明确了该等数量标准。就《个保法》关于个人信息保护负责人进一步规定的“个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门”。后续如何执行则可待监管部门另行指引。

《审计办法》也规定了，对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，其应当成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督。在实践之中，哪些企业可能会认定为该类个人信息处理

者，以及该等独立机构如何设立、监督方式，也是值得继续观察的问题。

如果企业内部自行开展合规审计，企业需要注意审计团队的独立性设置。参考国家标准《数据安全技术 个人信息保护合规审计要求（征求意见稿）》，就内部审计而言，内部机构审计人员应回避自身负责的业务内容，不应直接参与被审计对象的日常业务运营、个人信息安全保护工作；未设置专职个人信息保护合规审计团队的，应在保持独立原则的前提下，分别从内审团队、安全团队、法务团队等具有审计或个人信息保护相关专业能力的团队中选派人员，来自各团队的人员比例应保持在合理范围内，并由审计组长审批人员名单。

如果企业委托第三方专业机构开展合规审计，《审计办法》要求同一专业机构及其关联机构、同一合规审计负责人不得连续三次以上对同一审计对象开展个人信息保护合规审计，以保证合规审计工作的客观中立性。

五、合规审计中应当审查什么事项？

《审计办法》在其附件《个人信息保护合规审计指引》（以下简称“《审计指引》”）中详细列举了个人信息处理者或其委托的专业机构在开展合审计工作时应当重点审查的事项，涉及个人信息处理规则、个人信息跨境提供规则、个人信息主体权利保障、个人信息处理者的义务、大型互联网平台特殊责任五大模块，细分为二十七个方面的核查要求。

《审计指引》中的重点审查事项与《个保法》中各章节的具体规定相对应，同时纳入了《网络数据安全管理条例》、《未成年人网络保护条例》、《信息安全技术 个人信息安全规范》等法规和国家标准的要求。

六、合规审计工作应当如何具体开展？

《审计办法》并未对合规审计的具体流程、实施管理和人员要求、证据文件要求进行规定。

在《审计办法》正式出台前，全国网络安全标准化技术委员会于 2024 年 7 月 12 日发布了关于国家标准《数据安全技术 个人信息保护合规审计要求（征求意见稿）》（以下简称“《审计要求征求意见稿》”），在国家标准层面对个人信息保护合规审计的原则、要求、流程、审计内容和方法、审计证据进行规定，并提供了审计底稿模板和审计报告模板。虽然该国家标准目前尚未发布最终版本，但其中的细化规定和文本模板对审计工作的开展具有一定的参考价值。关于国家标准《审计要求征求意见稿》的主要内容的分析，请见《君合法评丨个人信息合规审计落地又进一步——国家标准发布征求意见》。

此外，根据公开报道，全国网络安全标准化技术委员会正在研制一批个人信息保护合规审计重点标准和实践指南。该等标准和指南也将《审计办法》的落地实施提供支撑 1。我们也会持续跟进相关进展。

（技术编辑：何芮）

研究动态

基础理论

1. 国家治理体系现代化语境下的数字检察

（胡骋）

来源：《华东政法大学学报》2025 年第 1 期

数字检察历经“起步—起势—成势”，走出了“个案办理—类案监督—系统治理”的法律监督路径，推动了“数字赋能监督，监督促进治理”的法律监督模式变革重塑，是以检察工作现代化支撑和服务中国式现代化的重要依托。面对数字检察纵深推进中的高质量发展瓶颈，应当强化数字检察基础理论研究，从推进国家治理体系、治理能力现代化的视角，阐释数字检察逻辑的根本支点，明晰数字检察的演进方向和宏观策略，促推数字检察再提升、再深化、再突破。

2. 数字贸易中的隐私权保护

（李姝卉）

来源：《华东政法大学学报》2025 年第 1 期

数字贸易发展与隐私权保护相互促进、相互制约。数字时代隐私权保护机制的创新和发展，对建立可信的数字经济发展环境、提升贸易效率和质量、扩大贸易自由范围等，均有较大促进作用。我国 TikTok 等数字产品和服务，常被域外政府以隐私权保护等机制存在不足为由加以非难；中国在隐私权保护领域的国际话语权不强，也因此受到部分国家的不公平对待。面对国际数字治理和数字贸易竞争日益加强的态势，针对未来数字贸易的隐私权保护立法，我国应以兼收并蓄的发展理念，进一步提升数字产品和服务的隐私权保护水平与竞争能力，积极推动隐私权保护、公平、安全的国际贸易规则的完善；同时，应推进数字领域软法与行业规则的完善，扩大相关规则适用的范围，进而充分实践、积极提炼隐私权保护的制度创新经验，构筑全球数字贸易中的隐私权保护法律制度，提升中国隐私权保护立法的国际影响力，促进数字贸易的繁荣与发展。

3. 公共大模型决策的法治化约束

（余圣琪）

来源：《国家检察官学院学报》2025 年第 1 期

随着数字政府建设的纵深推进，大模型日渐成为一种重要的公共决策方式，代表着新型的“数字公权力”，凭借超强高效的算法决策来提升公共服务质效和促进社会治理。公共大模型决策反映着计算理性和数字治理逻辑，已经突破了工商社会的法治化规制范围，甚至成为一块权力技术化的“飞地”。因此亟需纳入数字法治框架予以有效约束，即应当厘清决策的适用边界，构建决策的正当程序，确立价值对齐的基本原则，探索算法科层制的监督机制，

从而促进数字正义和数字法治建设。

4. 数字法学范畴体系的分层结构与逻辑展开

（任颖）

来源：《中国法学》2025 年第 1 期

作为跨法律部门的融合型学科，数字法学范畴体系并不局限于单一层次的范畴结构，而是遵循范畴分层法则的要求，形成基石范畴、基本范畴、具体范畴三阶构造。基石范畴层级的本体论范畴、价值论范畴、方法论范畴，在基本范畴层级转化为对象范畴、价值范畴、方法范畴，在具体范畴层级转化为要素范畴、宗旨范畴、技术范畴。数字法学范畴的分层逻辑，在部门法到领域法范畴、数字法治实践到数字法学理论、法学范畴到法治实践三个层次的演化中，发展出以数字要素为单位的法律规制路径，最终回归于数字私益、数字众益、数字公益的整体协同，数据财产安全、自然人信息人格、算法程序公平区分保护，以及数字私权利、私权力、公权力配置的差序平衡。

5. 论数字时代刑事证据的三元结构

（胡铭）

来源：《中外法学》2025 年第 1 期

随着数字技术的发展，数字空间正在逐步“侵蚀”现实空间。刑事证据也因此面临从传统二元结构向三元结构转移之趋势。传统二元结构下，言词证据与实物证据二分，口供被视为证据之王；新二元结构下，传统证据与电子数据二分，数字证据成为新的证据之王。证据生成空间的数字化形成了数字证据，证据移送、审查空间的数字化形成了传统证据数字化，传统证据、传统证据数字化、数字证据并存呈现出新的三元结构，这会对现行证据审查原则、规则等造成颠覆性影响。在此背景下，刑事证据法有必要通过专门立法构建起稳定的体系框架，并以证据真实性、关联性、合法性为基础，梳理三元证据审查的共性规则和差异性规则，通过传统证据、传统证据数字化和数字证据的协调发展来形塑数字时代的刑事证据体系。

6. 面向“三维世界”的数字法学

（马长山）

来源：《中国社会科学》2024 年第 11 期

数字法学立足于“三维世界”的系统创生，在其中展开自身的核心范畴。它呈现着“数字人类”的主体性再造、人类生活的数字逻辑和数字契约的共享赋权，因而生成了流动性、场景性、穿透性、交互性的数字权利；基于契约论向“三方论”的转型，构筑了传统数字化权力、新生数字权力和技术性数字权力的复杂权力结构；从“二维世界”迈进“三维世界”，使得数字正义摆脱了道德推理的分配策略，它在属性上是计算正义，在过程上基于认知计算，在方式上是可视正义，因而是一种计算分析的匹配正义。由此可见，数字法学负有重要的时代使命与担当，应致力于提炼“中国式现代化”中的法学命题，创新自主的数字法学理论，从而塑造新时代的自主法学知识体系。

7. 大数据背景下育种创新成果知识产权保护

（李菊丹）

来源：《知识产权》2024 年第 11 期

以特定种质资源改进与创新所形成的育种创新成果，具有与特定植物材料难以分离、具备繁殖能力且与特定名称相对应等特点，从而在国家种业监管链条中形成大量与育种创新成果有关的数据信息。这些数据信息是证明育种创新成果权利及归属、认定侵权行为成立与否、确定损害赔偿数额的重要证据。数字技术的广泛应用使得对上述数据信息进行针对性和关联性分析利用成为可能。考虑到相关数据应用与创新保护的紧密关联性，种业监管部门应优化不同监管环节数据信息的衔接，推动数据信息共享共用及向公众公开；育种创新主体应重视育种创新数据信息管理，提升数据应用能力，增强核心种质资源开发应用，构建多元保护机制。

8. 数据产权制度构建的方法论——以知识产权基础理论为起点 **（初亦周）**

来源：《知识产权》2024 年第 11 期

虽然技术的发展日新月异，但其变化并没有冲击到最底层的法律体系。由于数据产品与知识产品有着极强的共性，对于数据产权的制度构建往往可以借鉴已经较为成熟的知识产权基础理论，不必

“白手起家”，也不必“旧瓶装新酒”。洛克劳动财产理论在证立知识产品与数据产品的赋权时存在着相同的难点未予解决；“客体—对象”区分论不仅可以解释“唯数据不足以确权”的问题，也能解释“未产生新的利益关系也不足以设权”的问题；邻接权制度可以在数据产权相关问题悬而未决之时为数据产品提供栖身之所。在新时代出现新问题之时，法学研究应退回到其背后的法律体系中寻找与现有问题的共通之处，不必急于另立山头。

9.在互联网受众经济中推进数字权利的战略性诉讼的机遇和困难 （Swee Leng Harris）

来源：German Law Journal,Vol.25,Issue 6 (2024)

互联网科技巨头受到多个重叠但不同的欧盟立法的监管，这些立法为互联网用户建立了一系列实质性的数字权利，并在其执法架构中为战略诉讼提供了不同的法律机会结构。我的文章重点介绍了欧盟新《数字服务法》和《数字市场法》与《通用数据保护条例》的数字权利和执行架构的比较。对有关现有法规的关键战略诉讼的考虑为我探索新法案下战略诉讼的机会和障碍提供了信息。对这些战略诉讼机会的分析必然包括欧盟根据《代表行动指令》提出的集体索赔新制度，以及互联网用户的数字权利与消费者保护法之间的互动。我认为，新法案相对地将公共执法权集中在欧盟委员会，将公民社会边缘化，并有效地排除了公民社会在公共执法方面的大多数战略性诉讼。此外，新法案可能会通过在现有机构和制度之外建立额外的监管机构和能力，从而增加监管碎片化和法律不一致的风险。我认为，针对互联网科技巨头的私人执法战略诉讼可以增强公民社会影响数字权利发展的能力。私人执法战略诉讼作为一种执行机制，允许同时提出和解决多个法律领域，而不是孤立地提出和解决，这也有助于法律的一致性。然而，此类诉讼存在相当大的障碍，包括跨境管辖权和地位等法律问题，以及有效战略诉讼所需的资源。总的来说，关于战略诉讼的法律分析，我的文章表明，我们必须考虑跨多个法律领域的执法架构的公共和私人维度，同时考虑到不同执法机制的不同权力动态，以了解战略诉讼在互联网注意力经济中推进数字权利的机会。

10.通过战略诉讼对系统和无差别数据收集的挑战：欧盟法院审理的乘客姓名记录案

（Catherine Forget）

来源：German Law Journal,Vol.25,Issue 6 (2024)

当欧盟及其成员国不断采取措施打击严重犯罪和恐怖主义时，特别是通过数据保护规则的棱镜，欧盟法院通过强制遵守严格的条件来充当堡垒，从而侵犯了最初由成员国负责的国家刑事诉讼规则。在这篇文章中，我们将研究 Ligue des Droits Humains 如何以及基于什么能够让欧盟法院对乘客姓名记录指令做出裁决，以及这一行动在多大程度上确实具有“战略性”。

个人信息保护

1.个人医疗健康数据处理者信义义务的证成与制度建构 （邓辉，孙挥）

来源：《华东政法大学学报》2025 年第 1 期

在信息社会，医疗机构在持有医疗健康数据时也在事实上获取了患者的医疗健康信息，双方的权力势差不断放大。现行个人信息保护规则中无论是对医疗健康数据不可识别性使用时的匿名化要求，还是可识别性处理时以“告知—同意”为核心的赋权规则，均受到近代民法形式理性正义观的惯性影响，在实践中多流于形式。承认个人医疗健康数据处理者与信息主体间的持续性显著不平等关系，对数据处理者课以信义义务，使其成为个人医疗健康信息受信人，将“同意”解释为基于信赖的授权，可以有效克服形式主义正义观的不足，向实质正义迈进。信义义务的引入应避免对数据利用的过度掣肘，无论是信义义务的证成还是规范内容的构建，皆应遵循基于场景的分析。在医疗健康数据场景下，信义义务中的忠实义务应界定为约束信义关系的核心规范，为受信人划定行为之边界；注意义务则是在此基础上为受信人设定的行为之标准，可通过动态场景化的比例原则将其进一步具体化。如此，不仅可化解匿名化及“告知—同意”困境，重新在

个人医疗健康数据处理者与信息主体间注入信任，亦可对现行过于严苛与僵化的其他个人信息保护规则进行完善，以适应不断变化的数字社会的实践需求。

2. 侵犯公民个人信息罪的违法性认识错误出罪路径 （陈禹衡）

来源：《中国刑事法杂志》2024 年第 6 期

侵犯公民个人信息罪违法性认识错误易产生但难出罪。在侵犯公民个人信息案中，指导理念的差别、规范落实的滞后以及保护诉求的混乱导致了违法性认识错误的产生，而法规衔接的细化则导致违法性认识错误产生碎片化。侵犯公民个人信息罪违法性认识错误能够实质出罪的依据在于其难以避免。法律规范衔接不畅、实质法益内涵不明以及个人信息场景复杂导致了侵犯公民个人信息罪违法性认识错误难以避免，可以因此阻却责任并尝试实质出罪。行为人在知情同意机制中因为实质法益混淆而产生违法性认识错误，同时并未侵害个人信息自决权，可以实质出罪；行为人对合理处理流程产生争议而咨询权威机关获得错误答复，因此产生违法性认识错误不可避免，可以实质出罪；当个人与平台间存在客观的认知势差，个人受平台指示而产生不可避免的违法性认识错误，则也可以实质出罪。

数据确权与流通

1. 公共数据权属配置的再结构化

（包晓丽）

来源：《环球法律评论》2025 年第 1 期

公共数据概念呈扩张性演进的趋势，并可被类型化区分为公共管理数据和公共服务数据。由公共数据之“公共性”使然，各国立法政策均对公共数据开发利用有所规定，这也就对公共数据的权属配置提出一定要求。公共数据在主体身份、处理目的、权利基础和行权方式等方面均与企业数据存在较大差异，企业数据的产权结构性分置规则不能完全与之适配。公共数据权属配置的再结构化强调，应区分公共管理数据和公共服务数据设置差异化的产权结构性分置规则。具体而言，公共管理数据上存在三元权利结构，并可细化为国家的数据管理权、原始收集者的数据持有权和定限使用权、运营机构的数据经营权。公共服务数据上的产权结构与企业数据类似，提供公共服务的组织对数据同时享有持有权、使用权和经营权。数据的公共性越高，其开放共享的法定义务越强，经营权的受限程度越深。

2. 数据产权登记的基本问题研究

（孙莹）

来源：《中国法学》2025 年第 1 期

数据登记是数据产权制度体系建设中的关键环节。数据知识产权登记与数据产权登记在内核上其实是殊途同归，基于对法秩序统一性的维护，将数据登记制度统一命名为数据产权登记制度更为合适。应建立“专职登记机关—数据交易所”二元登记机构，并采取“登记机构形式审查—第三方机构实质审查”的二元审查模式。在效力模式的选择上，登记对抗主义将自愿原则之精髓贯彻始终，更为符合数据的价值实现规律。数据产权变动中存在两种法律事实协同发挥作用，其中数据交付具备生成效力，而推定效力、对抗效力、公信效力等与公示紧密相关的效力只有在完成数据登记后才能发生。数据产权登记的对抗效力需借助不完全权利变动理论进行周全解释。数据善意取得构成要件的认定应更为严格，制度效力宜从法定失权改造为强制授权。

3. 数据交易安全法益的刑事保护

（张勇）

来源：《中国刑事法杂志》2024 年第 6 期

在数据交易过程中存在非法获取数据、违法交易数据、不当泄露或滥用数据等安全风险，数据权属不清、交易规则不统一、安全监管不足，刑事立法也存在静态化、分散化、碎片化等缺陷。数据安全犯罪是以数据为对象、直接或间接危害数据安全法益的犯罪，可分为纯正的和不纯正的数据安全犯罪，与侵犯公民个人信息、危害计算机信息系统的犯罪存在交叉重合。在数据交易安全风险防控中，

需要确立风险预防刑法观、罪群生态化和刑事一体化治理理念。数据交易安全法益具有确定性和独立性，可分为私法益与公法益两种类型。在法益识别过程中，需要依据前置法运用法益还原方法，将公法益还原为私法益予以认定。同时，在分类分级的基础上予以不同层次的刑法保护。在刑事法领域，应合理分配和设定数据交易参与主体的数据安全保护义务，强化数据商和第三方服务机构的安全保护义务，赋予数据交易所“看门人”的安全监管义务。同时，加强刑法与前置法的刑行衔接，将被害人同意作为出罪免责事由，运用以刑制罪方法进行需罚性判断，合理把握涉罪行为的刑事责任边界。

4. 数字经济时代数据要素的法益识别与刑法保护——从公共秩序到财产安全、市场秩序

（郭旨龙）

来源：《财经法学》2025 年第 1 期

我国刑法在十几年前就开始设立公共秩序犯罪来保护数据的机密性，但这主要是回应信息经济中社会成员对于数据内容的关切。在当下的数字经济中，数据不再仅仅是直接提供给人类的信息，来支撑起供应链协同和大规模定制，而主要是以大数据的形式给云计算和人工智能提供生产要素性的原始数据。个人数据、企业数据和公共数据都进入了这个价值链，也都面临着威胁。数据的财产、经济性质日益凸显，社会成员愈发重视数据资源持有权、数据加工使用权、数据产品经营权等数据产权本身的保护。对于数字经济中对数据资源持有权、数据加工使用权的侵犯，应当根据具体情形认定为盗窃、毁坏财产或破坏生产经营的行为。鉴于盗窃行为排除占有的固有形象，对盗取数据的行为最好有特别立法以示区别和公平。在出现成熟市场之后，数据的财产性质必然嵌入到整个经济活动中，涉及竞争利益和市场秩序。侵犯数据产品经营权更多是严重扰乱数字经济市场秩序的行为，而非侵犯知识产权的行为。

人工智能

1. 数字司法与人工智能治理的中国方案

（韩旭至）

来源：《华东政法大学学报》2025 年第 1 期

数字司法与人工智能治理是数字社会法律治理变革中的两大核心议题，是我国近年来法治实践探索的前沿阵地。就前者而言，从 20 世纪 90 年代起，我国司法机关就开始了信息化的初步探索，至今已经历了“信息化—智慧化—数字化”三个发展阶段。当前，以数字法院、数字检察为主要内容的数字司法已经成为数字中国总体战略的一部分。就后者而言，随着人工智能的“第三次勃兴”，人工智能技术成为发展新质生产力的关键，世界主要发达国家均将大力发展人工智能定位为国家战略。

2. 人工智能治理的全球变革与中国路径

（张欣）

来源：《华东政法大学学报》2025 年第 1 期

人工智能领域的国际角力已然超越了技术和产业层面，实质上拓展至以法律规制和制度构建为核心的治理竞争。面对人工智能技术应用中的失序现象，人工智能治理步入全球化时代。纵观全球趋势，人工智能治理呈现出以分类分级为内核、软法与硬法动态衔接、监管主体跨域协同的特征。为积极应对人工智能带来的多元复杂影响，我国逐步形成了以人工智能安全为内核，以分类分级为依托，以人工智能安全主体责任为支点，以个体权利体系为外部约束的治理路径。当前，我国人工智能治理正逐步迈向以系统化立法为标志的新阶段。在此背景下，可从领域、主体、结构、技术视角构建多维协同的人工智能分类分级治理、全域构建软法与硬法深度耦合的规则体系以及推进技术赋能监管智能化等方面探索现阶段提升治理效能的方案。

3. 算法透明机制的局限性及其克服

（戴维，王锡锌）

来源：《华东政法大学学报》2025 年第 1 期

在算法治理语境中，算法透明被视为一种解决算法黑箱问题的主要机制。算法透明机制已得到广泛讨论，在理论上发展出以技术披露和决策解释为

核心的双线模式。双线模式要求算法技术能够被公众“看透”或“理解”。但该模式未能充分考虑算法可解释性障碍和公众认知局限，在实践层面遭遇来自技术和制度的双重挑战，这可能导致透明机制的失效和透明度期待落空。鉴于可解释人工智能的技术属性，伴随以算法信任为核心的治理理念的兴起，我们需要反思算法透明机制的局限，完善面向公众的算法透明机制。这种“面向公众的算法透明机制”应当以提升公众信任为目标，将透明机制作为信任沟通的工具，向公众传递有助于算法可信度评估的重要信息，建立真正服务于公众的算法透明机制。

4. 人工智能时代联邦学习隐私保护的局限及克服 （刘泽刚）

来源：《中外法学》2025 年第 1 期

人工智能立法通常会对特定技术有所偏重。联邦学习属于主流的机器学习技术，最大的优势就在于其架构设计充分考虑了隐私需求。联邦学习在金融、数据公开等领域的应用已经比较广泛，并对自然人权益产生了重大影响。目前以隐私保护为目标的联邦学习不断暴露各种隐私揭示了个人数据隐私保护路径的法律缺陷：规范稀疏导致联邦学习缺乏明确隐私需求，“隐私设计”优势很难得到发挥；分布式架构导致联邦学习隐私保护责任难以落实；过度强调保密性和安全性，导致隐私保护的人格性被弱化和转化；技术权衡缺乏规范导致隐私保护缺乏透明性和确定性。这些问题揭示了人工智能隐私保护与个人数据保护在保护对象、保护流程、保护责任、保护框架等方面存在的巨大鸿沟。为了适应人工智能隐私保护的特殊要求，未来可在整合规范依据、调整规范重点、探索归责机制、构建沟通机制等方面对人工智能隐私保护规范进行升级和完善。

5. 伦理人格与技术人格：人工智能法律主体地位的理论框架 （梅夏英）

来源：《中外法学》2025 年第 1 期

目前人工智能法律主体地位的理论探讨遵循两种路径：一是将人工智能作为具有高级智能的类人“种群”来进行理论预判；一是探讨赋予当前弱人工智能某种法律拟制人格来承担责任和享有权利。对此有必要提出“伦理人格”和“技术人格”的区分理论，来界定人工智能主体地位的不同理论面向。人格区分现象在传统民法中已然存在，它呈现为以人格抽象程度为标志的人格递进序列，其中存在着两种人格的“渐变”和“断裂”现象。人工智能作为伦理主体遇到了“自我意识”的难题，目前的弱人工智能尚不能获得独立的伦理人格，规制技术开发者的科技伦理起主导作用，同时不排除人机交互伦理可能会赋予机器人某种道德性“权利”。就人工智能的技术性人格而言，如果只是将人工智能作为“个体”进行研究，并无自然人的意思表示机制和机器人自身财产的支撑，赋予机器人技术人格便不完全具备条件。未来人工智能的主体性将依照两种人格的路径各自发展，以技术人格的探索先行，逐渐进行伦理人格的塑造，人类或机器人的伦理人格最终成为技术人格的依归。

6. 人工智能法律治理的框架选择：从“分类分级”到“模块组合” （苏宇）

来源：《中国法律评论》2025 年第 1 期

对人工智能实行适当的区分式治理，是人工智能立法中最为基础而关键的问题之一。人工智能立法不宜采取分类分级式框架，因为容易产生高昂的错误划分成本，亦难以回应超越单纯风险治理的立法目标。考虑人工智能演化过程中出现的重要分支、人工智能技术发展的开放性与叠加性特征以及人工智能技术本身的模块化特点，人工智能立法宜采取模块组合式框架。这一框架应至少包含参数模块、生成模块、开源模块、隔离模块和运动模块，相关规则模块根据治理对象的特点而针对性地适用，并且可以根据未来人工智能技术的发展而动态增减。《人工智能法》应以专门性的章节进行制度设计。

7. 论人工智能训练数据高质量供给的制度建构 （赵精武）

来源：《中国法律评论》2025 年第 1 期

人工智能训练数据的高质量供给直接关系到人工智能产品或服务的功能提升。尽管学界针对训

练数据供给问题试图通过著作权合理使用认定、数据安全保护义务履行等方式纾解训练数据供给的制度障碍，但未能从促进科技创新的视角论及如何实现训练数据的高质量供给的问题。人工智能训练数据高质量供给的法律内涵是市场供给的训练数据本身满足“质”和“量”的要求，同时，训练数据供给方式、供给渠道具有多元化的特征。结合促进科技创新所遵循的协同治理方式，需要从满足不同科技创新主体需求和塑造实质公平的科技创新资源配置两个方向出发，建构层次化、多元化的训练数据高质量供给保障体系。

8. 大模型价值对齐的法治进路

（韩旭至）

来源：《中国法律评论》2025 年第 1 期

价值对齐是大模型伦理风险防控的核心手段，是构建可信人工智能的关键。大模型价值对齐的运行机理展现了人机协同的技术治理逻辑。人工智能治理的制度规范蕴含了价值对齐的要求。然而，价值对齐的标准模糊对商业自由、言论自由造成冲击，价值对齐的义务责任不明引起开发者与提供者的权责失衡，大模型自主性与可控性、可解释性的法律要求之间又存在一定张力。针对上述困境，大模型价值对齐的理念应从绝对安全转向合理成本的模型安全，从单一维度规制转向共建共享的合作治理。在此基础上，大模型价值对齐应以体系融贯为原则，构建目标限缩与标准解释机制；以分类分级为基础，设计伦理风险评估、审计与应对机制；同时，以责任豁免与公共数据供给机制，形成对价值对齐的激励。

9. 人工智能伦理的机制设计

（郑戈）

来源：《中国法律评论》2025 年第 1 期

到目前为止，关于人工智能伦理的学术和政策讨论仍然沿袭了传统科技伦理的路径，以提出“以人为本”“科技向善”等抽象伦理原则为主要形式，而缺乏实施这些原则的有效机制。本文借助经济学中机制设计理论所提供的分析框架，从激励兼容、显示原理和实施机制三个方面梳理人工智能伦理从潜在性向现实性转化的动力机制，以期为负责任、可信任的人工智能技术和产业的发展提供一个可操作的理论模型。

10. 论生成式人工智能版权侵权“双阶”避风港规则的构建 （黄玉烨，杨依楠）

来源：《知识产权》2024 年第 11 期

生成式人工智能的作品使用具有海量化及算法化特征，面临侵权责任认定与分配难题。避风港规则以满足特定条件给予免责为构造，可以回应机器训练的行为转变，契合风险分配的规制目标，具有事前预防效果。基于生成式人工智能服务提供者的技术能力、大模型版权侵权的规制需求和版权人的获益需求，为其新设“双阶”避风港规则具有必要性。在训练阶段，可以通过设置信息披露、权利保留的识别尊重、非直接获得经济利益和整体性补偿义务，使生成式人工智能服务提供者无须经事先许可使用作品，且不必承担解除学习等责任；在输出阶段，可以为生成式人工智能服务提供者配置建立投诉处理机制、消除重复作品数据、优化模型过度拟合、干扰用户恶意引导、基于请求的版权过滤等义务，使其免受抽象侵权标准影响。

11. 人工智能生成内容著作权规制的全球趋向与本土路径 （熊琦，张文窈）

来源：《知识产权》2024 年第 11 期

生成式人工智能技术的普及对著作权制度的影响主要体现在两个方面：一是输出端生成内容的可版权性与权利归属，二是输入端基于机器学习大规模使用他人作品的合法性认定。对于前者而言，在普遍坚持和认同自然人参与创作为可版权性前提的同时，全球各国对权利归属仍存在使用者和设计者的认知差别。对于后者而言，人工智能技术领先型和追赶型国家的制度选择存在较大差异：技术领先型国家更多借助判例法传统，等待传统版权产业与人工智能产业双方的充分博弈，延续以往平衡应对新旧产业冲突的路径，期待双方在充分表达利益的基础上实现产业合作途径的创新；技术追赶型国家的立法选择则更偏向于为人工智能产业提供发展空间。鉴于现阶段的技术水平和产业地位，我

国有必要选择将技术追赶型国家的制度经验融入本土“三步检验法”，在机器学习的合理使用适用上破除“非营利性”和“适度性”局限。

12.机器学习著作权法定许可的适用基础与规则构建 （蔡元臻）

来源：《知识产权》2024 年第 11 期

人工智能模型训练（机器学习）侵权是人工智能著作权冲突中的重要问题。扩张适用合理使用制度和加强损害赔偿救济难以解决社会利益失衡的难题，法定许可模式仍具有难以替代的利益调和功能。机器学习法定许可的使用行为仅限于复制，商业性数据挖掘必须遵守法定许可，合理使用仅适用于公益性明显强于商业性的情形。法定许可费用的制定可以参考损害赔偿许可使用费的裁定方法，费用的收转仍需通过著作权集体管理组织配合执行，但是需要提高作品使用者的信息标注义务和完善人工智能法定许可信息机制。机器学习孤儿作品的特殊情形可以采用责任限制为主、法定许可为辅的二元治理模式。人工智能研发者负有数据过滤和信息披露的注意义务，后者应当遵循强制公开和公平合理原则；人工智能服务提供者则是在避风港规则的基础上，承担研发者信息披露的形式审查等义务。

13.人工智能训练的版权困境及其出路：模块化许可机制探析 （孙靖洲）

来源：《知识产权》2024 年第 11 期

创作者对人工智能利用其作品进行训练的抵制，缘于利益分配机制付之阙如。在调整因新技术带来的作品使用形式变化所引发的新的社会关系时，既要确保创作者能公平地参与到由创作带来的收益分配中，维护其劳动尊严和劳动收入，又要防止版权人通过杠杆优势制约技术发展。可考虑从知识产权制度为解决市场失灵而创设的四种特殊许可模式中汲取经验，为人工智能训练建立一套整体协调但内部区隔的模块化授权许可机制：大型人工智能企业应尽最大努力获取授权，主动建立版权许可机制，与版权人分享收益；中小企业同时面临被大型内容平台拒绝许可与缔约成本高的双重困境，应要求大型内容平台作出以公平、合理、无歧视方式进行授权的声明，并发挥其中介组织的优势，保障个体创作者的合法利益、企业获得充足训练语料，同时防止掌握海量内容数据的大型内容平台封锁人工智能产业。

14.解决数据驱动的边境管制程序中的算法错误 （Mirko Forti）

来源：German Law Journal, Vol. 25, Issue 4 (2024)

欧盟移民政策的逐步数字化正在将外部边界变成人工智能驱动的过滤器，根据风险指标限制来自第三国的人员享有基本权利。人们对技术设备的可靠性及其预测入境外国人未来行为的能力有着不可动摇的信心，这种信心正导致欧盟外部边界的数据化。如果所谓的无懈可击的算法出错了会怎样？本文旨在了解算法错误对抵达欧盟的移民、难民和寻求庇护者生活造成的影响。这篇文章调查了在边境部署数据驱动解决方案的社会政治影响，试图对欧盟移民政策的技术解决方法及其对受影响个人基本权利的影响提出质疑。

15.布鲁塞尔的副作用：人工智能法案如何缩小欧盟政策的全球影响力

（Marco Almada, Anca Radu）

来源：German Law Journal, Vol. 25, Issue 4 (2024)

在过去几年里，人工智能（AI）技术已经深入到社会生活的各个领域，促使国家和国际层面的立法努力。在欧盟（EU），这种立法动力体现在各种法律文书中，特别是拟议中的《人工智能法》，该法有望通过“布鲁塞尔效应”成为全球标准。本文认为，虽然《人工智能法》很可能会产生自己的“布鲁塞尔效应”，但这种结果将伴随着一种副作用，即破坏欧盟在人工智能治理方面传播立法文本和价值观的雄心。由于《人工智能法》沿用了欧盟的产品安全立法，其条款对欧盟政策意图保护的某些价值观（如基本权利保护）提供了有限的保护。欧盟积极努力制定替代文书，如欧洲委员会按照《人工智能法》的思路提出的人工智能公约，使这些缺陷变得更加复杂。因此，《人工智能法》作为全球标准的推广将对欧盟的人工智能政策议程和布鲁塞尔效应的概念化产生影响。

16.人工智能法案中的风险管理

（Jonas Schuett）

来源：European Journal of Risk Regulation, Vol.15, Issue 2 (2024)

拟议的人工智能法案（AI Act）是在主要司法管辖区监管人工智能（AI）的首次全面尝试。本文分析了 AI 法案中的关键风险管理条款第 9 条。它概述了规范背后的监管概念，确定了其目的和适用范围，对具体的风险管理要求进行了全面解释，并概述了执行这些要求的方式。本文可以帮助高风险系统的提供商遵守第 9 条中规定的要求。此外，它还可以为 AI 法案当前草案的修订以及制定 AI 风险管理协调标准的努力提供信息。

17.欧洲拟议的 AI 法案中的可接受风险：决定多少风险管理才算足够的合理性和其他原则

（Henry Fraser, José-Miguel Bello y Villarino）

来源：European Journal of Risk Regulation, Vol.15, Issue 2 (2024)

本文批判性地评估了欧盟委员会拟议的人工智能法案对对基本权利和安全构成风险的高风险人工智能系统的风险管理和风险可接受性的方法。该法案旨在促进具有适当监管负担的“可信”人工智能。其关于风险可接受性的规定要求在考虑“最新技术”的情况下，“尽可能”减少或消除高风险系统的剩余风险。这个标准，特别是如果狭义地解释，是行不通的，既不促进成比例的监管负担，也不促进可信度。相比之下，议会最新的风险管理条款修正案草案引入了“合理性”和成本效益分析，并且在风险可接受性判断的价值和背景性质方面更加透明。本文认为，议会的方法更可行，并且更好地平衡了相称性和可信度的目标。它借鉴了过失法和欧洲医疗器械法规的原则，解释了风险可接受性判断的合理性。它还认为，风险可接受性判断的方法需要公民合法性的坚实基础，包括监管机构的详细指导或参与，以及受影响利益相关者的有意义意见。

18.ChatGPT：生成式人工智能系统版权挑战的案例研究 （Nicola Lucchi）

来源：European Journal of Risk Regulation, Vol.15, Issue 3 (2024)

本文重点介绍与生成式人工智能（AI）系统有关的版权问题，特别强调 ChatGPT 案例研究作为主要示例。为了生成高质量的结果，生成式 AI 系统需要大量的训练数据，这些数据通常可能包含受版权保护的信息。这促使人们询问合理使用、创作衍生作品以及数据收集和使用合法性的法律原则。将输入数据用于训练和增强 AI 模型，这引起了对潜在侵犯版权的严重担忧。本文为保护版权所有者和竞争对手的利益提供了建议，同时解决了法律挑战并加快了 AI 技术的发展。本研究以 ChatGPT 平台为例进行分析，以探讨版权法规必须进行的必要修改，以充分解决 AI 生成的创意内容领域中作者身份和所有权的复杂性。

19.“More than Words”：由生成式人工智能提供支持的商业聊天机器人风险的法律方法

（Sara Migliorini）

来源：European Journal of Risk Regulation, Vol.15, Issue 3 (2024)

最近发布的新一代聊天机器人系统，尤其是那些利用基于 Transformer 的大型语言模型（LLM）（如 ChatGPT）的系统，让世界感到惊讶，并引发了关于它们对社会的潜在影响的辩论。虽然人们经常讨论对这些技术构成的生存威胁的担忧，但将我们的注意力转移到与部署这些技术相关的更直接的风险上至关重要。由于缺乏解决用户识字问题的积极措施以及这些聊天机器人的传播营利性模式，这些风险进一步加剧了这种风险。借鉴计算机科学和其他领域的研究，本文着眼于这些产品引发的直接风险，并反思了法律在旨在引导生成式人工智能技术走向共同利益的更广泛政策中的作用。它还审查了欧洲议会对欧盟委员会 AI 法案提案提出的相关修正案。

20.将安全标准的执行编码到智能机器人中，以利用其计算复杂性和协作潜力：欧盟政策制定者的法律风险评估

（Riccardo Vecellio Segate, Angela Daly）

来源：European Journal of Risk Regulation, Vol.15, Issue 3 (2024)

在机器人和人类大部分时间都在快节奏但相互独立的环境中工作之前，职业健康与安全（OHS）规则可以在很大程度上独立于机器人的行为来解决工人的安全问题。现在情况不再是这样了：与人类一起工作的协作机器人（cobots）需要制定相关政策，确保在共享空间和合作工作流程交付时，人类和机器人的安全。在欧盟（EU）内部，适用的监管框架处于国际行业标准与欧盟及成员国立法之间的交叉点。当前的标准和法律不仅未能令人满意地应对人机交互（HRI）带来的身心健康挑战，而且在智能机器人（“SmaCobs”）方面也存在重大差距。事实上，SmaCobs 将机器学习带来的黑箱不可预见性与更普遍的与 HRI 相关的风险结合在一起，使操作界面和生产链变得越来越复杂、移动和互联。在此背景下，基于生产力和健康的动机，我们敦促将职业健康安全政策的执行直接编码到 SmaCobs 中。首先，SmaCobs 可以利用量子计算的复杂性，以适应各种情况下的突发需求的方式调整复杂的规范架构。其次，委托它们对自己和人类执行职业健康安全标准，可能会证明比由人类来执行更安全，也更符合成本效益。这种情况引发了对 SmaCobs 法律人格、责任分配和算法可解释性的深刻法律、伦理和哲学关注。为解决这些问题，我们提出了第一个系统性建议。对于欧盟，我们建议通过针对 SmaCobs 时代的新的具有约束力的职业健康安全条例来实现这一目标。

21.《欧盟人工智能法》：在产品安全与基本权利之间徘徊

（Marco Almada, Nicolas Petit）

来源：Common Market Law Review, Vol.62, Issue 1 (2025)

欧盟（EU）人工智能法案（简称“AI 法案”）规定了混合监管框架。AI 法案结合了欧盟法律的两个经典传统，即产品安全和基本权利保护。然而，如果拟议的合并没有考虑到两种法律传统之间的结构性差异，它可能会失败。本文使用法律和技术文献的三个经典主题——节奏问题、监管视角和制度路径依赖性——来说明为什么 AI 法案的设计会产生实践和理论挑战，这些挑战需要在法案的实施和未来的欧盟立法中解决。

22.欧盟《人工智能法》对基于人工智能的移民技术的监管：（仍）在阴影中运行？

（Ludivine Sarah Stewart）

来源：European Law Journal, Vol.30, Issue 1-2 (2024)

虽然人工智能（AI）正在成为支持欧盟及其成员国移民和边境管理政策的关键要素，但迄今为止，基于人工智能的移民技术在测试和实施过程中受到的公众监督十分有限。在此背景下，欧盟《人工智能法》有望成为一项符合基本权利保护和法治的法规。虽然成员国在部署人工智能时受到现有欧盟立法的约束，但该法案是首次尝试在移民和边境管理中对这一技术进行监管。本文探讨了该法案在整个谈判过程中的演变，以及它在追究参与人工智能驱动的移民技术的行为者的责任，从而促进法治方面的潜力。本文认为，虽然该法规提供了大有可为的重要内容，但仔细研究后会发现其在确保问责能力方面存在重大问题。

平台治理

1.平台劳动者自动化决策拒绝权实现路径的公私法协同 （程凌）

来源：《华东政法大学学报》2025 年第 1 期

平台劳动者自动化决策拒绝权是解决平台劳动者“困在系统里”问题的必要路径。该权利作为宪法个人信息权权利束体系的组成部分，与其他宪法基本权利的实现密切相关。该权利具有双重功能，主观防御功能在于保障平台用工自动化决策的私法自治，客观价值秩序功能要求国家对平台用工自动化决策进行积极干预。相应地，该权利的实现需要私法与公法的协调配合。在私法视野下，平台劳动者以请求权的方式行使自动化决策拒绝权，权利行使须满足“仅通过自动化决策的方式作出”、对

平台劳动者权益有“重大影响”两项要件，从而达到拒绝完全自动化决策、获得人工干预的法律效果，此路径注重平台劳动者个人层面的权益影响或损害救济。在公法视野下，主要通过有意义信息的强制性披露、自动化决策的风险评估与人工监控来规制自动化决策信息不对称风险及平台劳动者生命健康权、平等权等基本权利被侵害的风险，此路径注重平台劳动者整体层面的风险预防。

2. 论平台用工算法透明的制度实现

（班小辉）

来源：《清华法学》2025 年第 1 期

算法黑箱对平台从业者权益保障带来多重挑战，促进算法透明是化解风险的重要路径。从算法介入用工管理方式来看，算法透明涉及平台从业者的个人信息处理、用工算法规则公示以及自动化决策解释三重问题。在个人信息处理方面，平台从业者“知情同意”真实性的判断、算法环境下敏感个人信息的保护以及个人信息访问权范围的厘定面临挑战。在用工算法规则公示方面，当前公示的事项范围与方式不清，且职工民主参与机制难以适应平台用工实践。在算法自动化决策解释方面，解释的范围与时间亦存在争议。为此，应明确平台用工算法处理平台从业者个人信息的合法标准，设置个人信息处理红线，加强对算法监控系统的监管，并合理判断信息访问权的范围；强化用工算法规则公示的可操作性，优化新业态协商协调机制，落实职工民主管理和集体协商在算法规则公示上的功能；设置差异化的用工算法自动化决策解释义务，并落实相关配套机制。

3. 超级平台权力的进化与规制——以“微信小程序”为例

（马平川）

来源：《政法论坛》2025 年第 1 期

小程序作为超级平台权力的再进化方式，消解了人们原有线下交互的生活方式，构建了网络化、数字化、智能化的生活模式，但其中也隐藏着不容忽视的法律风险。超级平台在权力资源系统集成、市场力量跨界扩张的基础上，通过小程序重塑了数字应用市场结构，把控了公民数字生活，并在一定意义上成为新型的“数字利维坦”。为制约这种复合型的超级平台权力，应采用权力制衡、数据限制和市场规制的三重路径，同时对平台“守门人”义务进行优化设计，通过优化其内部治理义务、算法合规义务、平台中立义务和风险防控义务来限制平台权力的滥用，并防止超级平台利用小程序继续汲取权力，以塑造安全、可控的数字市场秩序。

数字行政与司法

1. 数字时代在线诉讼模式特有原则与制度构建

（景汉朝）

来源：《华东政法大学学报》2025 年第 1 期

数字时代在线诉讼的深入发展对传统民事诉讼提出了革命性挑战。从其产生的社会基础、表现形态和运行模式、实践需要及创建中国特色原创性诉讼理论话语体系等方面分析，深刻把握在线诉讼特点及规律，研究确立其特有原则与制度，是完善在线诉讼理论，探索形成原创性自主知识体系，实现法治理论“弯道超车”的突破口。具体而言，应确立线上纠纷线上审原则、证伪不证真原则、倾斜保护原则、公开审判与信息保护并重原则、数据安全优先原则，创建通域管辖、准代表人诉讼、多元审级、送达即时生效等特有制度。这些特有原则制度与传统诉讼模式中有关原则制度相结合，共同构成了在线诉讼模式的原则制度体系，丰富了民事诉讼理论内涵。

2. 智能行政中自动化决策拒绝权的证成与适用

（翁明杰）

来源：《财经法学》2025 年第 1 期

随着数字技术的迭代更新，自动化决策的应用范围不断扩大、应用程度不断加深，给现代行政法治带来新的挑战。《个人信息保护法》第 24 条第 3 款规定的“自动化决策拒绝权”虽然构造相对粗糙，条文设计弹性不足，但是该规定似乎给智能行政情境下研究如何保障行政相对人合法权益提供了新方向。在智能行政中嵌入自动化决策拒绝权不仅是权力与权利不对等的必要化解路径、智能行政要求

嵌入更高强度人工干预的必然举措，还与自动化决策“人在回路”的治理路径相契合。禁令路径或权利路径因不同程度上的局限被排除在自动化决策拒绝权的进路选择范围之外。折中进路以其宏观性、弱对抗性和动态性的优点，弥补其他两种路径的局限，成为自动化决策拒绝权的进路选择。在折中进路指引下，自动化决策拒绝权中的适用场域应当拓宽、“对个人利益有重大影响”的适用前提需要划定、自动化决策拒绝权的适用衔接应当优化。

虚拟财产

1. 数据资产的刑法保护模式

（姚万勤）

来源：《中国刑事法杂志》2024 年第 6 期

关于数据资产的刑法保护，我国刑法当前并无直接规定，只能以极个别罪名对少部分个人数据进行间接保护。然而，数据资产的间接刑法保护模式并不妥当。数据资产不是著作权法规定的作品，也不都是商业秘密，因而知识产权犯罪保护模式不可行。数据资产具有财产属性，因而纯粹保护数据的扰乱公共秩序犯罪保护模式没有做到全面评价。新型财产权保护模式的保护成本较高。传统财产犯罪保护模式具有一定优势，但须先明确数据资产的属性及其存在形态。数据资产具有财产属性，其存在形态为无体物。基于此因应数字资产的刑法保护，应当重塑财产犯罪中的占有概念。财产犯罪中的占有，不局限于事实性的占有或者观念上的占有，而是非法获取，支配的效力范围可扩展至间接支配。如此，便可通过传统财产犯罪对侵犯数据资产的行为予以规制。对尚未涉及的其他行为类型，可以增设“窃取、骗取、抢劫或者以其他方式侵犯他人数据资产”及其与其他财产犯罪竞合的罪刑规范予以规制。

2. 数字藏品受贿犯罪的数额认定规则研究

（王剑波）

来源：《法律适用》2024 年第 12 期

数字藏品作为一种新型网络虚拟财产，属于刑法意义上的财物，可以成为受贿犯罪的对象。但是，受数字藏品市场属性与法律属性的影响，对于数字藏品受贿犯罪的数额认定，现行法律规范尚未明确适用规则，因而存在着理论上的争论与实务适用困难的问题。对数字藏品受贿犯罪的数额认定，有必要引入同类型数字藏品在同期市场的交易价格作为参照，并结合犯罪数额认定的一般标准进行综合考量。如果涉案贿赂属于未公开发行的数字藏品，数额认定可考虑以成本价格为基础，以处置价格为补充，同时参照同类型数字藏品的同期市场交易价格。如果涉案贿赂属于已公开发行的数字藏品，数额认定可考虑以受贿行为完成时的市场价格为基础，以处置价格为补充，同时参照同类型数字藏品的同期市场交易价格。

（技术编辑：李佳丽、麻卓妍）

教研活动

涉案虚拟货币处置研讨会在京举行

为贯彻落实党的二十届三中全会精神，充分发挥法治在国家治理体系和治理能力现代化建设中的依托保障作用，1 月 19 日，由中国人民大学法学院、中国人民大学刑事法律科学研究中心和北京中银律师事务所联合主办的“涉案虚拟货币处置”研讨会在京举行。来自全国人大常委会法工委、最高人民法院、最高人民检察院、公安部等实务部门代表，法学理论界、律师界、企业代表近 60 人参加会议。

研讨会现场

第一单元 虚拟币法律规制现状与前瞻

第一单元“虚拟币法律规制现状与前瞻”由中国人民大学法学院副院长、教授程雷主持。

中国人民大学法学院院长、教授杨东，中国人民大学刑事法律科学研究中心主任时延安，海克斯康集团大中华区法务总裁、首席合规官薛海滨，成都链安科技有限公司董事长、电子科技大学副教授杨霞女士，中银律师事务所管委会主席、高级合伙人刘晓宇分别发表了主题发言。最高人民法院研究室副主任喻海松担任本单元的与谈人。

第二单元 虚拟币处置的实践难题与应对举措（一）

第二单元“虚拟币处置的实践难题与应对举措（一）”由中银律师事务所管委会委员、高级合伙人张晓君主持。

北京市公安局法制总队涉案财物管理支队相关负责人曹文建，中国政法大学诉讼法学研究院教授郭烁，中南财经政法大学国家治理学院副院长陈实，西北政法大学刑事法学院副院长刘仁琦分别发表了主题发言。最高人民检察院第四检察厅金融办案组负责人王拓、北京师范大学刑事法律科学研究院副院长、教授何挺进行了与谈。

第三单元 虚拟币处置的实践难题与应对举措（二）

第三单元“虚拟币处置的实践难题与应对举措（二）”由中银律师事务所党委书记、高级合伙人李征主持。

中国社会科学院法学研究所研究员董坤，南开大学法学院副教授朱桐辉，华东师范大学法学院副教授聂友伦，盈科律师事务所全球总部合伙人郭志浩分别发表了主题发言。中央财经大学法学院副教授李伟、全国人大常委会法制工作委员会刑法室干部张宇翔进行了与谈。

第四单元 虚拟币的证明与认定

第四单元“虚拟币的证明与认定”由中银律师事务所合伙人郑佳主持。

南开大学法学院教授高通，德恒律师事务所高级合伙人刘扬，中国海洋大学法学院副教授潘侠，北京交通大学法学院讲师王熠珏分别发表了主题发言。北京网络行业协会信息安全应急响应与处置中心主任高显嵩和西北政法大学刑事法学院讲师陈建军进行了与谈。

程雷和李征进行了小结。与会专家从多重维度深入探讨了涉案虚拟货币处置，涵盖了虚拟货币的概念、法律属性、域外立法现状以及各地的处置实践做法等。但我国目前在虚拟货币处置过程中，存在立法不完善和法解释空间缺失等问题，使得虚拟货币处置面临较大法律风险和实践困难。虚拟货币作为新兴资产类别，亟须通过立法完善以确保其合法性与安全性，同时可以加强跨国协作、增强监管力度，为涉案虚拟货币规范处置提供切实法律保障。

中国人民大学法学院成功举办全国高校涉外法治与数字法学师资公益研讨班

2025 年 1 月 11 日至 13 日，由中国人民大学法学院主办的全国高校法学教师涉外法治与数字法学公益研讨班顺利举行，本次研讨班由中国人民大学未来法治研究院、中国人民大学涉外法治研究院、教育部哲学社会科学创新团队“新科技革命与未来法治创新团队”协办。来自 25 个省份、62 所高校的 108 名高校法学教师参加了本次公益研讨班。

本次研讨班内容丰富，涵盖了涉外法治和数字法学的多个前沿议题。来自全国各地的法学教师齐聚一堂，共同学习分享、相互切磋研讨。

研讨班现场

中国人民大学法学院党委书记**杜焕芳**教授、中国人民大学法学院院长**杨东**教授与研讨班学员分别进行了交流研讨。杜焕芳教授围绕习近平总书记对中国法学会第九次全国会员代表大会致信精神，对高校教师如何进一步加强自身建设、如何培养法治人才谈了自己的看法。杨东教授就高校法学院系如何在国家战略中挺膺担当，如何培养涉外法治和数字法学领域的专门法律人才谈了自己的见解。

中国人民大学法学院党委书记杜焕芳教授

中国人民大学法学院院长杨东教授

在为期三天的研讨中，多位专家学者为学员们带来了精彩的讲座。中国人民大学法学院**张新宝**教授、**韩立余**教授、**余民才**教授、**丁晓东**教授、**熊丙万**教授等老师以及北京师范大学法学院廖诗评教授就一些前沿问题做了专题报告。

除专题讲座外，研讨班还设置了研讨环节，中国人民大学未来法治研究院执行院长**张吉豫**副教授、中国人民大学法学院普通法研究中心副主任**吴至诚**副教授分别主持了“数字法学的教与学”、“涉外法治的教与学”的研讨环节，中国人民大学法学院**黄尹旭**副教授等老师参与了研讨。

1 月 13 日下午，研讨班举行了简短的结业仪式，北京物资学院**白硕**老师作为学员代表发言，中国人民大学法学院**程雷**副院长出席结业仪式并做总结发言。

中国人民大学法学院始终牢记肩负的社会责任与使命，多年来一直坚持开展高校教师的专业培训和公益讲座。近五年来，针对高校法学专业教师

线上开展了习近平法治思想公益讲座、民法典高校教师公益讲座等。此次研讨班旨在进一步加强高校法学教师职业共同体建设，共同研讨以提升涉外法治和数字法学的教研水平，更快更好地培养具有国际视野和竞争力的法治人才，加快构建我国涉外法治、数字法学的知识体系、学科体系和教学体系。

检校同行，打开数字检察新“视”界——海淀区检察院与中国人民大学开展交流研讨

为深入贯彻落实最高检、市院关于深化数字检察战略的部署要求，赋能新时代法律监督工作提质增效，不断推动法学研究与检察实践双向奔赴、融合发展，促进“检校共建”产出更多有益成果，1 月 6 日，海淀区检察院与中国人民大学召开数字检察工作交流研讨会。中国人民大学国家治理大数据和人工智能创新平台主任、交叉科学研究院副院长、数学学院教授**龚新奇**，国家治理大数据和人工智能创新平台执行主任、大型科学仪器共享平台副主任、信息学院教授**陈跃国**等专家老师一行 9 人应邀参加本次会议。海淀区检察院党组成员、政治部主任**辛东卿**，各部门相关负责同志及信息化工作专员参加会议。

研讨会现场

会上，数字办同志介绍了海淀区检察院数字检察工作当前进展、推广成效及下一步发展设想，各业务部门相关负责同志就自主研发建用的大数据法律监督模型逐一进行汇报展示，围绕模型创建、数据调取、数据处理、本地化应用、平台研发等方面进行了详细介绍，并就未来与中国人民大学合作的空间、领域及项目进行展望。

国家治理大数据和人工智能创新平台执行主任、大型科学仪器共享平台副主任、信息学院教授**陈跃国**，国家治理大数据和人工智能创新平台副主任**代文林**，法学院助理教授**彭雅丽**，国家治理大数据和人工智能创新平台工程师**尹珺**、**王安顶**结合海淀区检察院数字检察模型建用需求、可视化分析方法、非结构化数据处理等方面进行交流发言，并表示会在技术攻关、模型创建、学术研究等领域给予海淀区检察院有力支持和坚实保障。

中国人民大学国家治理大数据和人工智能创新平台主任、交叉科学研究院副院长、数学学院教授**龚新奇**表示，国家治理大数据和人工智能创新平台会通过发挥优质师资力量和科研团队优势，结合海淀区检察院丰富案例资源，助推大数据、人工智能等技术在检察工作中深度应用，不断优化数字检察理论体系和实践模式，努力形成案例数据系统化、模型场景体系化、案件办理智能化的工作机制，为海淀区检察院“打开小切口，达成深治理”全力提供智力支撑和技术支持。期待检校双方在已有共建成果的基础上，继续携手并进，畅通优化供需对接，促进相互赋能、双向奔赴，形成更多有特色亮点的合作成果，有力推动法学教育与检察实践相融互促。

龚新奇教授发言

海淀区检察院党组成员、政治部主任**辛东卿**表示，海淀区检察院与中国人民大学合作共建历史悠久，友谊源远流长，此次交流研讨会为加强检校互动、拓展视野思维、推动数字检察工作深入发展注入了新的动力和活力。检察机关具有丰富的案件资

源、数据优势和数字应用需求，高校具有理论研究优势和技术优势，检校双方可以通过联合组建研发团队、定期开展交流研讨等方式，不断推动科研成果与司法实践紧密结合，加快数字检察提档升级，力争形成更多“海淀经验”，充分实现检校“优势互补、合作共赢”。下一步，希望与中国人民大学持续加强联动协作，不断挖掘共建契合点，在人才培养、理论研究、资源共享、项目建设等多个方面实现深度交流合作，共促“检校共建”迈上新台阶。

辛东卿主任发言

研讨会成员合照

门头沟区检察院、门头沟区司法局 赴中国政法大学数据法治实验室调研交流

为进一步推动数字检察高质量发展，深化检校共建合作，提升新质法律监督能力，推进检察工作高质量发展，2025 年 1 月 20 日，门头沟区检察院、门头沟区司法局来到教育部哲学社会科学实验室——中国政法大学数据法治实验室开展调研交流活动。

门头沟区检察院党组书记、检察长闫俊瑛，党组副书记、副检察长石磊，党组成员、副检察长霍丽娜、滕英杰等相关同志；门头沟区司法局副局长魏晓东、魏丽娜等相关同志；中国政法大学党委常委、副校长、教授时建中，中国政法大学数据法治研究院教授王立梅等参加活动。

调研成员合照

活动伊始，门头沟区检察院、司法局一行参观了中国政法大学校史馆与中国政法大学数据法治实验室。

时建中教授为与会人员讲述了数据法治研究院、数据法治实验室的建设历程，发展现状与未来规划，对数智技术与数据引发的新兴法律问题做了主题讲解，并对实验室的一系列最新研究成果和技术产品进行了介绍。王立梅对实验室研发的公平竞争审查系统、智能调解平台等产品进行了进一步的讲解和展示。

时建中教授讲述实验室建设历程

参观结束，一行人针对数字检察监督的建设开展交流会议。与会人员就数据法治建设、数据赋能基层治理中存在的问题等方面进行了深入交流，对实验室研究成果在执法监督、“两法”衔接以及知识产权保护等方面的应用进行了深度探讨。

交流会议现场

双方一致认为，本次交流是数据法治研究与数字检察实践的一次深度碰撞，数字技术将在检察工作中发挥越来越重要的赋能作用。数据法治实验室将继续加强与检察实务部门的合作交流，进一步推动大数据、人工智能等科技创新成果同检察工作的深度融合，推动数字检察高质量发展，推进检察改革走深走实。

申卫星教授及课题组成员赴 UNIDROIT 就数字资产法律问题研讨交流

2025 年 1 月 28 日-29 日，清华大学法学院教授、智能法治研究院院长申卫星应国际统一私法协会（UNIDROIT）之邀，带领课题组成员前往意大利罗马出席 1 月 28 日召开的“数字资产及其在亚洲的法律应用和发展”研讨会，并于 1 月 29 日再次召开工作交流会，与国际统一私法协会秘书长 Ignacio Tirado 教授、副秘书长 Anna Veneziano 教授、国际统一私法协会首席法律官黄美玲教授及《数字资产与私法原则》（Principles on Digital Assets and Private Law，简称“DAPL Principles”）起草组成员就数字财产及数据交易领域的立法活动进行深入交流，取得了丰硕成果。

申卫星教授及课题组成员与国际统一私法协会秘书处成员合影

2025 年 1 月 28 日下午，“数字资产及其在亚洲的法律应用和发展”研讨会正式开始。这也是国际统一私法协会亚洲跨国法律研究中心（ATLC）系列研讨会的首场会议，此次研讨会由国际统一私法协会法律顾问 Theodora Kostoula 担任主持人。

研讨会首先由国际统一私法协会秘书长 Ignacio Tirado 教授致欢迎词，随后由 ATLC 联合主任 William Brydie-Watson 对 ATLC 作简要介绍。此后，来自土耳其 MEF 大学法学院的 K. Berk Kapanci 教授，K. Berk Kapanci 教授分别发表了主题演讲。

与谈环节紧随其后。申卫星教授与意大利罗马一大（Sapienza University） 法学院的 Luca di Donna 教授受邀作为与谈嘉宾。

随后，在主持人 Theodora Kostoula 的邀请下，申卫星教授就中国法对数字资产的性质、中国法下“控制”和“占有”概念区别分享了观点。

申卫星教授就数字资产在中国的理解适用发表看法

接下来，来自中国香港的国际统一私法协会法律官员 Chi wing cheuk 就香港法律如何理解和保护数字资产予以回应。

最后，意大利罗马一大法学院的 Luca di Donna 教授结合意大利法律和欧盟法与谈。

与谈嘉宾各自发言结束后，国际统一私法协会秘书长 Ignacio Tirado 教授、副秘书长 Anna Veneziano 教授以及现场听众热情高涨，纷纷踊跃提问。

研讨会结束后，国际统一私法协会秘书长 Ignacio TIRADO 教授、副秘书长 Anna Veneziano 教授以及国际统一私法协会首席法律官黄美玲教授对申卫星教授的观点及中国在数据领域的发展表达了浓厚兴趣。1 月 29 日上午受黄美玲教授邀请和组织，申卫星教授再次携课题组成员前往国际统一私法协会，开始了第二轮的工作交流会。

申卫星教授、刘云助理研究员与国际统一私法协会秘书处成员深入交流

交流会后，国际统一私法协会秘书长 Ignacio Tirado 教授表示希望可以继续保持沟通合作，在进一步深入了解中国数据政策的同时，求同存异，共同推动促进数字财产领域交易规则的国际化和协调化发展。

技术编辑：林诗敏

数字法评

重构“知情”：平台间接侵权责任反思

原载：《东方法学》2025 年第 1 期，第 75-89 页

作者：丁晓东

摘要：知情状态在平台间接侵权中被赋予重要地位，共同侵权制度中的过错判断与避风港制度中的通知都与知情状态密切相关。但以知情状态判断平台过错与责任，只适合分析平台平等参与特定个案的侵权。在此类侵权中，可以分析平台在个案中是否“知道”或“应知”，是否存在过错和尽到合理注意义务。而典型的平台间接侵权是大规模治理下所产生的问题，其“知道”“应知”或注意义务应当以是否具有整体性治理过错为依据，其判断因素包括危害性与治理必要性、治理可能危及的合法性活动、平台辨识合法与非法活动的难度、直接侵权制度是否更有效等。从典型平台间接侵权的大规模治理型侵权特征出发，可以对传统共同侵权与避风港制度进行协调，通过分领域和案例积累而破解算法推荐等场景下知情分析的不确定性，同时消除平台“不做不错”“做多错多”的悖论。

一、问题的提出

在网络平台间接侵权制度中，平台的知情状态被视为关键因素。[1]一方面，传统的共同侵权制度都将知情状态作为判断平台是否存在间接侵权的标准。以我国相关制度为例，《信息网络传播权保护条例》第 22 条、《消费者权益保护法》第 44 条、《电子商务法》第 38 条、《民法典》第 1197 条、《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》（以下简称《信息网络传播权司法解释》）第 7、9 条，《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（以下简称《网络人身权益司法解释》）第 6 条都以“知道”“明知”“应当知道”等作为判断平台责任的依据。另一方面，以“通知－删除”规则为代表的避风港制度也与平台的知情状态密切相联。“通知－删除”规则规定，平台只有在接到被侵权人的通知后，才有履行删除侵权内容的义务。在某种程度上，这一制度可以被解释为“知情－删除”规则，即平台对于平台内的一般间接侵权并不知情，只有平台在被告知和处于知情的状态下，平台才应当承担责任。[2]

不过，以知情状态分析平台间接侵权责任，却存在种种困境。其一，间接侵权与避风港制度虽然都涉及知情，但前者以传统共同侵权中的角色判断与责任分担为基础，后者则以合规免责为基础，两者存在紧张甚至冲突。其二，何谓知情具有很大弹性。法律对于知情状态的要求各不相同，既包括事实上的“知道”，也包括规范意义上的“明知”或“应知”等要求。在司法实践中，对于知情的判断常常具有很大的不确定性。例如在算法推荐等技术等背景下，平台是否对第三方侵权知情再次引发争议。其三，通过知情状态判断平台责任，也可能带来平台作为与平台审查的悖论。平台可能故意无视，以避免相关责任，从而导致“不做不错”的悖论。平台也可能因为积极履责而对平台内的侵权行为知情，从而承担责任，导致“做多错多”的悖论。

本文对平台间接侵权中的知情困境进行分析与反思，指出困境的根源在于典型平台间接侵权与传统的个案性侵权、非治理型的共同侵权存在根本性不同。在传统共同侵权中，其典型形态是特定个案的侵权，在这类侵权中，共同侵权人的知情状态可以作为判断平台注意义务与责任的依据。但典型的平台侵权具有大规模治理特征，平台注意义务应当是整体性和概率性的，而非仅仅是个案性的。从典型平台侵权的大规模治理特征出发，本文对平台间接侵权责任进行重构。

二、问题的分析与展开

本文第一部分指出，以知情状态分析与判断平台责任，可能存在种种困境。本部分首先对本文引言所提到的若干困境进行系统化分析与展开。

（一）两种制度中的知情

平台间接侵权中的知情问题首先涉及两种制

度。一方面，平台间接侵权可以适用帮助侵权、教唆侵权、替代责任等传统共同侵权法制度。例如我国《民法典》在第 1168 条规定了一般共同侵权责任。第 1169 条第 1 款规定了教唆、帮助侵权责任，第 2 款规定了替代责任，第 1171 和 1172 条规定了可分割的共同侵权责任。此外，《民法典》在第 1197 条规定，“网络服务提供者知道或者应当知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任”，这一条款也可以被视为传统共同侵权制度在网络领域的应用。这一条款虽然被置于《民法典》互联网专条部分，但与传统共同侵权制度并无不同。[3]另一方面，平台间接侵权也适用以“通知－删除”规则为代表的避风港规则。例如我国《民法典》在第 1195 和 1196 条引入了以美国数字千禧年版权法案为基础的通知－删除规则，[4]要求网络服务提供者在收到权利人的侵权通知后及时“采取必要措施”。

传统共同侵权与避风港制度虽然都将知情状态视为是否应当承担责任的重要标准，但二者对于知情状态的理解并不相同。一方面，传统共同侵权以过错或过失来理解平台的知情状态，其对平台所施加的责任相对较重。当平台“知道”或者“应当知道”平台内存在侵权时，都应当承担共同侵权责任。另一方面，避风港规则以合规免责的立场理解平台的知情状态，其对平台所施加的责任相对较轻。以我国为例，只要平台履行《民法典》第 1195、1196 条所规定的义务，就不应承担侵权责任。《美国数字千禧年版权法案》的规定则更为具体，如果网络服务提供者“并不实际知道”侵权行为，或者“不知道存在明显侵权活动的事实或情况”，那么网络服务提供者就不应当承担责任。[5]这两种知情状态常常被总结为“实际知情”与“红旗知情”。[6]此外，《美国数字千禧年版权法案》还规定，网络服务提供者不必承担对侵权行为的一般审查义务。[7]

在法律实践中，法院对知情的理解与判断常常在两种制度间摇摆，经常出现不一致的理解。以我国司法为例，法院一方面以传统共同侵权来理解知情状态，要求平台承担合理注意义务。例如，韩某诉北京某度网讯科技有限公司案中，法院认为某度公司应有合理的理由知道相关文档侵权；[8]某果公司诉北京某铁数盟信息技术有限公司案中，法院认为某果公司应当能够知道相关侵权行为。[9]另一方面，法院在其他案件中也利用避风港规则来理解平台的知情状态。例如，某健（中国）日用品有限公司诉浙江某宝网络有限公司侵犯商标专用权纠纷案中，法院认为，对于平台内的疑似商标侵权，对平台提出过高的审查义务与注意义务，会导致对“避风港规则的否定”。[10]相对而言，美国对平台的注意义务与侵权责任采取相对宽松的立场，但也面临两种制度的紧张。一方面，美国法院不断解释与适用《数字千禧年版权法案》中的“实际知情”与“红旗规则知情”标准，将其解释为需要对某一特定侵权具体知情。[11]另一方面，美国法院也不断适用普通法间接侵权上的知情标准。例如，维亚康姆公司诉油管一案中，法院指出，普通法上的“故意无视”原则并未被避风港规则所取代。[12]MGM 工作室公司诉格罗克斯特案等一系列案件中，法院引入了普通法上的教唆侵权的教义，对平台施加了一定的“应知”责任。[13]

（二）知情的不确定性

知情状态面临的另一问题是其判断标准高度不确定。这不仅是因为上文提到的两种制度对于知情状态的理解不同；还因为即使在两种制度内部，法律对知情的规定、理解与判断也存在巨大弹性。

以我国为例，2006 年公布并于 2013 年修订的《信息网络传播权保护条例》规定，如果网络服务提供者“不知道也没有合理的理由应当知道”，则其可以免责；而处于“明知或者应知”的状态下则应当承担责任。2009 年制定的侵权责任法规定，网络服务提供者处于“知道”的状态下应当承担连带责任。2013 年制定的《消费者权益保护法》规定，网络交易平台提供者“明知或者应知”销售者或者服务者利用其平台侵害消费者合法权益，未采取必要措施的，依法与该销售者或者服务者承担连带责任。2018 年制定的《电子商务法》规定，电子商务平台经营者“知道或者应当知道”平台内经营者销售的商品或者

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，未采取必要措施的，依法与该平台内经营者承担连带责任。2020 年制定的《民法典》采取与《电子商务法》类似表述，规定网络服务提供者“知道或者应当知道”网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。[14]此外，《网络传播权司法解释》和《网络人身权益司法解释》则更明确地规定，认定网络服务提供者是否属于“应知”或“知道或者应当知道”，应当考虑多重因素。

在法律解释上，我国对于知情状态的理解与适用也存在争议与不确定性。例如有观点认为，我国法律中的“应知”或“应当知道”应当解释为类似美国法上的“推定知道”，即根据已有证据与事实可以反证平台处于知情状态。[15]但也有观点为，“应知”或“应当知道”不应解释为限于证据层面的推定知道，而应当解释为包括其过失状态所导致的“应知而未知”。[16]此外，对于平台内的疑似侵权行为，法院对于平台的知情状态的判断也不同。例如在某健（中国）日用品有限公司诉浙江某宝网络有限公司侵犯商标专用权纠纷案中，对于平台内的网店经营者所进行疑似专利侵权行为，法院认为平台对于此类行为不属于知道或明知。[17]而在杭州某广告有限公司与深圳市某科科技股份有限公司侵害发明专利权纠纷再审案中，法院认为，对于平台内疑似专利侵权的行为不必以法院的判决为基础，某广告有限公司“明知”其平台上的疑似侵权行为而不采取有效的措施，应当对权利人扩大的损失承担连带责任。[18]

域外国家对于知情的法律规定与判断也存在不确定性。以美国为例，美国成文法在著作权领域制定了“通知－删除”规则，平台在“实际知情”与“红旗规则知情”的情形中应当承担连带责任。在司法实践中，对于何谓“实际知情”与“红旗规则知情”，法院的司法解释不仅不断变化，而且与立法意图也存在较大差异。在不涉及知识产权的言论侵权领域，美国则在其《通讯风化法》230 条款及其司法解释中对网络服务提供者完全免责，这就意味着即使平台对平台内侵权完全知情，平台也不承担任何责任。[19]而在普通法上，美国法院对于间接侵权在不同领域的知情要求也并不相同。例如在专利帮助侵权中，美国法院一般要求对侵权行为实际知情，[20]但在著作权帮助侵权中，美国法院倾向于认为，对侵权行为“推定知情”即可，即“知道或有理由知道”存在侵权行为。[21]

近年来，随着算法推荐技术在网络领域的广泛应用，有关于平台知情状态与责任的分析再次成为争议焦点。有观点认为平台既然可以利用算法技术进行个性化推荐，就对存在侵权的算法推荐知情，或者至少“应当知道”相关侵权行为。[22]而相反的观点则认为，算法推荐技术并没有改变平台责任的基本原理。既然避风港制度将平台知情限定在有限范围内，那么平台就没有责任利用算法技术进行一般审查。因此，利用算法技术的平台并不需要承担更高的注意义务。[23]

（三）平台作为的悖论

以知情状态来分析和判断平台责任，不仅面临上文提到的两种制度协调与不确定性困境，而且还会导致平台作为的悖论。一方面，以知情状态分析与判断平台责任，可能导致平台不作为或“不做不错”的悖论。如果以我国法上的“知道”或美国法上的“实际知情”“红旗规则知情”界定知情，那么一些平台可能会故意无视平台内的侵权行为。上文提到，美国法院认定“故意无视”无法得到避风港的保护，就是为了避免平台承担过低的注意义务。而且，即使以我国法律中的“应当知道”或平台过失来界定知情，法律也可能对平台设置过低的责任。例如，当平台对于平台内侵权的审查与预防措施远低于同类平台或行业的一般技术水平时，可能导致平台内侵权行为的大量出现，对被侵权人与社会造成严重负担。在人身损害等严重侵权类型中，此类问题将更为突出，平台所产生的大量侵权行为将给社会带来严重的负外部性。

另一方面，更为重要的是，平台作为可能出现“做多错多”的悖论。因为平台越注意审查与防范平台内的侵权行为，平台就越可能处于知情状态。例

如在上海某网络科技有限公司与北京某信息技术有限公司侵犯著作财产权纠纷案中，法院认为，从某视频网站的后台页面来分析，被告在对网站进行日常维护和管理过程中，会对网络用户上传的节目进行审批和推荐，这说明其有权利和能力去掌握和控制侵权活动的发生。[24]

事实上，互联网领域的避风港制度之所以被提出，正是因为知情悖论所导致的种种乱象。1995 年，在互联网发展之初，美国法院在斯特拉顿·奥克蒙特诉奇迹服务公司案中认定，互联网平台对平台内的内容进行了删除、编辑和管理，这说明互联网平台对侵权内容知情，应当被视为类似出版商的角色，对平台内的言论侵权承担连带责任。[25]这一判决引发了平台的巨大担忧和不作为，为了避免可能承担的侵权责任，互联网企业索性不再作为，任由互联网上的各类违法信息泛滥，以此来证明自己对侵权信息不知情和不具有控制力。正是在这样的背景下，美国国会在 1996 年制定了《通讯风化法》230 条款，免除了网络服务提供者在言论领域的侵权责任，以保护对网络内容进行治理的“好心人”。[26]

在法律对平台施加公法审查义务的背景下，“做多错多”的悖论会更突出。我国在若干法律法规中都规定了审查义务，例如 2000 年制定的《互联网信息服务管理办法》规定，互联网信息服务提供者不得制作、复制、发布、传播九类个人信息，其中除了危害国家安全等具有明显公法属性的信息，还将“侮辱或者诽谤他人，侵害他人合法权益的”也包括在内。[27]《电子商务法》《食品安全法》也规定了相应的资质资格审核义务，要求网络平台对平台内的商业主体进行实名登记、审查许可证。当平台履行其公法审查义务，平台就可能在审查过程中接触了相关内容，从而可能被认定为对相关侵权内容“知情”。[28]

三、困境根源：大规模治理型侵权

平台间接侵权的知情分析之所以面临挑战与困境，与平台间接侵权的典型形态密切相关。典型的平台间接侵权是一种大规模治理型侵权，与传统特定个案型、共同侵权人相互独立的侵权形态非常不同。[29]一方面，平台间接侵权具有大规模的整体性特征，难以被分解为多个独立、特定个案的共同侵权。另一方面，平台与平台内主体具有治理关系，平台既对于平台内主体有一定的控制能力和侵权预防能力，同时又需要建立容错机制。平台间接侵权的形态变迁使得传统共同侵权中的知情与过错分析难以直接适用。

（一）侵权形态的变迁

就小型、各自独立的传统间接侵权而言，此类侵权形态可以视为传统一对一侵权的复合形态。一方面，传统间接侵权不具有显著的大规模性或外溢性，即该间接侵权行为是一个相对独立发生的事件，该间接侵权行为与其他侵权行为并不具有联动性。例如，一个人撞伤他人或打破他人物品往往是偶发事件，侵权人并不对被侵权人或被侵权人亲属之外的一般人群产生影响。另一方面，传统间接侵权行为中的共同侵权人彼此具有独立性，相互之间并不存在管理或支配性关系。也因此，传统间接侵权行为可以被拆分或被视为两个独立侵权行为的叠加。

但平台间接侵权的形态则非常不同。一方面，平台间接侵权典型形态具有大规模或外溢性特征。在平台间接侵权中，平台所扮演的角色是普遍性而非特定的。平台不仅与某一侵权行为有关，而且涉及大量的同类侵权行为，是一种典型的一对多或一对海量的侵权关系。只有在少数情形下，平台才会对某一特定对象进行帮助侵权或教唆侵权。例如平台对某一特定个体进行言论诽谤，或者精准化打击平台内的某一商家，或者故意将某一热点视频编辑推送至网站首页播放，此时平台可能对平台内的侵权主体提供特殊帮助或进行教唆。在此类情形中，平台所参与的间接侵权就与传统侵权具有类似性，也是偶发独立事件，而且不会对平台内的一般主体产生影响。另一方面，平台与平台内的经营者、消费者、创作者等各类主体之间的关系并非完全独立或平等，平台与共同侵权人具有管理性或从属性关系。[30]两者的这种关系使得平台既可以对平台内主体进行一定的风险预防，又需要避免在管理过程中对平台内主体造成伤害。

（二）知情状态的相关性

从间接侵权的形态出发，就可以发现知情状态分析为何曾经具有重要意义，又为何会在平台间接侵权中陷入泥沼。传统间接侵权虽然比直接侵权复杂，但其基本原理与直接侵权并无区别，都以过错（包括故意或过失）为前提。在此背景下，分析间接侵权人在个案中知情状态就具有重要意义。在道德正当性层面，判断间接侵权人在个案中是否对直接侵权知情，是否在个案中故意促成直接侵权或放任直接侵权事件发生，可以对间接侵权人的过错与责任进行较为合理的判断。[31]在效率与功利主义层面，分析知情状态可以更为合理地对间接侵权人的一般行为进行免责，对故意或放任参与侵权行为的间接侵权人进行威慑预防，从而维持人们行动自由与预防侵权之间的平衡。[32]

但在平台间接侵权中，分析间接侵权人在特定个案中的知情与过错已经不再契合。在经典的平台间接侵权案件中，平台并不参与个案性的帮助侵权或教唆侵权，平台在间接侵权中并没有个案性的意图。[33]因此，以个案中的知情状态来判断平台间接侵权，并不能反映平台在间接侵权中所扮演的角色。相反，更为合理的方式是分析与判断平台在治理意义上是否履行合理注意义务，是否平衡了各方利益。按照这一判断标准，平台在间接侵权中的知情与过错应当从大规模和整体性的意义上进行分析，也应当从兼顾预防与容错的治理意义上进行分析。平台间接侵权应当避免仅仅关注特定个案，也不能仅仅从预防侵权的角度进行分析。

大规模治理型侵权并非完全为平台共同侵权所特有，一些非平台侵权也可能具有部分类似特征。在这些类型的侵权中，以知情状态分析侵权中的过错也面临问题。第一，工业化时代产品缺陷等侵害所导致的大规模侵权不再注重个案意义上的知情状态。在此类侵权中，判断侵权者是否应当承担责任，重要是产品制造者是否存在履行社会义务上的过失。美国学者威廉·普罗西（William Prosser）将这一变化视为以个案知情与过错为基础的传统侵权法“城堡的崩溃”。[34]在我国，过失仍然被视为一种过错，但这种过错已经“客观化”，与侵权方在特定个案中的知情与过错具有本质区别。第二，很多侵权也具有管理型侵权的特征。例如当劳动者在履行工作职责时侵犯他人权益、[35]跳蚤市场中的商家出售假冒伪劣商品，[36]音乐厅允许他人演奏未获版权的作品，[37]此时用人单位、跳蚤市场的组织者、音乐厅组织者都可能因为其管理角色而承担连带侵权责任。在此类侵权中，法律往往不需要考虑管理者是否知情，而是分析管理者是否从被管理者那里获得直接经济收益。如果管理者从被管理者那里获得直接经济收益，那么管理者将承担替代责任。[38]

不过，平台间接侵权与一般过失侵权以及传统管理型侵权仍具有重大区别。首先，就过失侵权而言，产品制造者在侵权中主要扮演的直接侵权角色，这与平台所扮演的间接侵权角色不同。只有在少量的专利侵权中，才会出现生产者的共同侵权或间接侵权问题。[39]因此，各国对于产品责任的规定都限于直接侵权责任，排除了产品缺陷所导致的间接侵权责任。而对于专利间接侵权中的产品责任，法律也排除了制造“通用商品”的生产者责任。[40]这使得产品生产者的间接侵权责任仍然限于与传统的间接侵权形态。此外，产品缺陷所引发的主要是人身财产侵害，而平台间接侵权除了在一部分情形中涉及人身安全，其他更多的情形主要涉及言论侵权、著作权侵权、商标侵权等侵权类型。在言论与知识产权等侵权形态中，其侵害程度较低，而且平台更需要维持言论自由、知识产权合理使用与保护权利人之间的平衡。基于这些原因，平台间接侵权与产品责任中的知情与过错分析仍然非常不同。产品责任可能适用过失责任（negligence）或严格责任（strict liability），[41]即要求产品责任承担过失意义上的注意义务或更高的严格责任。但对于平台而言，要求平台承担类似产品生产者的责任，对其适用产品责任法上的知情与过错分析并不合理。[42]

第三，就管理型侵权而言，用人单位、跳蚤市场的组织者、音乐厅组织者的用户规模一般较小，这些管理者往往能够对其管理的主体进行个案性

监管。而平台则往往涉及海量用户的管理，不太可能对平台内的主体进行一一监管。平台间接侵权如果适用替代责任，要求平台承担严格责任意义上的知情与注意义务，也只能限定在平台能够直接获益的特定案件中。在司法实践中，美国法院认定，替代责任只能适用于平台能够识别特定侵权，并且具有直接经济利益的情形中。[43]我国的《信息网络传播权司法解释》第 11 条规定，“网络服务提供者因提供网络服务而收取一般性广告费、服务费”，并不属于“获取经济利益”。《信息网络传播权司法解释》第 22 条规定，平台“未从服务对象提供作品、表演、录音录像制品中直接获得经济利益”，将不需要承担赔偿责任。这些规定都反应了平台间接侵权与传统替代侵权的不同，不能将传统替代侵权中的个案知情状态与注意义务简单移植到平台上。

四、原理重构

上文已经指出，判断典型间接侵权中的平台责任，应当分析大规模治理意义上的合理注意义务，而非分析特定个案中的平台知情状态。本部分对平台注意义务的具体标准进行分析，指出其判断标准应当结合治理的必要性、治理的代价、治理难度、治理的比较优势等角度进行分析。综合而言，平台的注意义务应当分析平台是否在整体治理意义存在过错。就平台的间接侵权赔偿责任而言，平台在同一类型案件中的赔偿总额应当与平台因为治理过错而需要受到的罚款保持一致。

（一）注意义务的判断标准

首先，平台的注意义务应当结合侵权的危害程度进行判断。平台间接侵权所造成的社会危害性越大，平台所应承担的注意义务就越大。平台间接侵权的类型很多，包括但不限于侵犯隐私权和个人信息、侮辱诽谤、著作权、商标、专利、侵犯个人财产与人身安全。当平台间接侵权仅仅造成偶发性的微型损害时，此时平台一般不需要承担注意义务与相应责任。相反，当平台间接侵权造成了他人人身财产安全损害，特别是造成了大范围的人身财产安全损害时，平台就应当承担较高的注意义务，防止此类事件的发生。[44]我国法律在共同侵权与避风港规则之外，进一步规定了平台的安全保障义务，正是因为安全保障义务涉及严重侵权。[45]例如我国《电子商务法》第 38 条规定：“对关系消费者生命健康的商品或者服务，电子商务平台经营者对平台内经营者的资质资格未尽到审核义务，或者对消费者未尽到安全保障义务，造成消费者损害的，依法承担相应的责任。”美国一直是平台免责的坚定支持者，但在刑事犯罪领域，美国仍然于 2015 年制定了《停止广告剥削受害者法案》，要求平台对在线性贩卖（Sex trafficking）承担责任。[46]

其次，平台的注意义务应结合其促进的合法活动与社会利益进行判断。其提供的公共服务和促进的合法活动越多，其注意义务越低。平台的兴起不仅带来了侵害，也同时带来了收益。对平台的注意义务与责任进行分析，需要同时考虑二者。而此处需要强调的是，要求平台对侵权承担间接侵权责任，也会同时导致平台对一般内容与用户活动进行审查，伤害平台内的正常活动。因为只有对平台内进行一般审查，平台才有可能避免承担间接侵权责任。菲利克斯·吴将这种现象称为平台责任常常导致的“附带伤害”，即平台常常会因为避免其间接侵权责任而进行过度审查，附带对平台内的合法活动与合法用户造成伤害。[47]例如，如果要求平台对所有疑似著作权侵权行为承担责任，那么平台就会加大对平台内的各类言论、图片与视频的审查，删除或下架很多表面侵权但实质并非侵权的作品。[48]因此，在判断平台注意义务时，法律不仅应当关注其可能造成的侵权，而且应关注预防侵权所带来的“附带伤害”。

再次，平台的注意义务应当通过平台辨识侵权活动的难度、改善平台内生态的成本进行判断。平台越能够以较小的技术与管理成本减少侵权行为，同时不影响平台内的合法活动，其注意义务就越高。[49]以信息核验义务为例，此类辨识技术与管理方式难度较小，也不会对平台内的合法活动造成影响，将其纳入法定义务就具有更高的合理性。例如上文提到的《消费者权益保护法》第 44 条和《食品安全法》第 131 条都规定，如果平台不能提供平台内经

营者的“真实名称、地址和有效联系方式的”，平台应当承担连带责任。《电子商务法》第 38 条则规定，“对关系消费者生命健康的商品或者服务，电子商务平台经营者对平台内经营者的资质资格未尽到审核义务”，“造成消费者损害的，依法承担相应的责任”。而在其他很多情形下，平台精确辨识侵权活动的难度或成本常常非常高。有的平台间接侵权常常需要高度专业化的知识，例如，专利侵权、个人信息侵权具有很强的专业性，平台很难凭借自身力量判断某一主体是否侵犯了专利，[50]某一平台内的信息处理者是否侵犯个人信息。[51]平台对此类间接侵权承担的责任相对较低，其通知删除义务常常以法院的生效判决为前提。还有的平台间接侵权则常常需要权衡侵权与合理使用的边界。例如侮辱诽谤等言论侵权常常需要考虑言论自由的抗辩，[52]著作权侵权常常遭受合理使用的抗辩。[53]在此类间接侵权中，平台很难通过算法技术或人工审查对言论侵权进行精准识别与删除。如果平台对疑似言论侵权或著作权侵权内容都进行删除，那就会导致大量正常表达的内容遭受删除，影响平台内用户的言论自由。

最后，平台的注意义务应分析是否首要侵权者承担责任比平台承担责任更有效。首要侵权者责任与平台责任的关系大致可以视为侵权与规制的关系，[54]首要侵权者承担责任越有效，平台所需要履行的注意义务就越低。例如，当平台内的商家为消费者提供侵权损害保险，消费者可以较为便利地获得损害赔偿；或者当平台履行信息核验与资质审查义务、为被侵权方提供侵权起诉的途径，且平台内商家具有足够的赔偿资金时，直接侵权制度就可以有效地应对平台内的侵权行为；而让平台承担较高注意义务和承担间接侵权责任，则会逆向激励平台，促使平台对平台内内容与活动进行过度规制与审查。反之，当直接侵权制度无法有效发挥作用，此时平台需要承担更高的注意义务。例如直接侵权者从事高风险行为，但不具有足够资金、无力履行损害赔偿，使得受害人无法得到赔偿，此时平台就需要对此类行为承担较高的注意义务，防止平台内将大量的负外部性损失转移给社会。[55]在此类情形中，由平台承担间接侵权责任，可以激励平台将负外部性内部化，弥补直接侵权制度的不足。[56]

（二）作为治理的侵权

关注平台责任域外研究的读者可能会发现，本文所论述的平台注意义务的四大要素与道格拉斯·李其曼（Douglas Lichtman）教授和威廉·兰德斯（William Landes）教授的研究具有一定的相似性。在 20 年前关于著作权帮助侵权的一篇研究中，两位教授指出，平台是否应当承担帮助侵权责任，取决于四大要素：（1）第三方侵权的危害越大，平台越应当承担责任；（2）合法使用平台的收益越少，平台越应当承担责任；（3）改进平台治理以不实质性干扰合法活动、减少侵权活动的成本越低，平台越应当承担责任；（4）在执法与预防侵权过程中，间接侵权责任制度相比直接责任制度的成本越低，平台越应当承担责任。[57]本文的分析大致对应两位教授所提出的四种考虑因素。

需要指出的是，李其曼和兰德斯的分析并未从平台侵权的性质层面对平台间接侵权进行分析。对于读者来说，其分析的论点与结论可能具有启发性，但难免会让人对其论述逻辑感到难以把握。尤其对于其提到的四点要素，一般读者可能会感到困惑：为何是这四大因素，而不是其他因素？这四大因素之间有何逻辑联系？

从本文所论述的大规模治理型侵权出发，就可以理解其中的逻辑与原理。首先，第三方侵权的危害性越大，即平台在此类情形中的大规模治理义务越重。其次，合法使用平台的收益越少，即平台在此类情形中的治理间接侵权的附带损失越小。再次，改进平台治理以不实质性干扰合法活动、减少侵权活动的成本越低，即平台在此类情形中的治理改进难度越小。最后，间接侵权责任制度相比直接责任制度的成本越低，即平台治理相对于侵权制度的优势越大。综上所述，这四种要素分别从治理的必要性、治理的代价、治理难度、治理的比较优势角度进行分析。从大规模治理的角度理解间接侵权，上述困惑就会迎刃而解。

需要指出的是，司法实践中对于平台间接侵权责任的判断也同样纳入了这些因素。例如《信息网络传播权司法解释》第 9 条对判断网络服务提供者是否属于“应知”，列举了六项因素：（一）基于网络服务提供者提供服务的性质、方式及其引发侵权的可能性大小，应当具备的管理信息的能力；（二）传播的作品、表演、录音录像制品的类型、知名度及侵权信息的明显程度；（三）网络服务提供者是否主动对作品、表演、录音录像制品进行了选择、编辑、修改、推荐等；（四）网络服务提供者是否积极采取了预防侵权的合理措施；（五）网络服务提供者是否设置便捷程序接收侵权通知并及时对侵权通知作出合理的反应；（六）网络服务提供者是否针对同一网络用户的重复侵权行为采取了相应的合理措施。这六项因素除了第（二）（三）项可能属于特定个案侵权外，[58]其他都属于大规模治理型侵权中的考虑要素。[59]

从本文所论述的大规模治理型侵权出发，平台在间接侵权中所承担赔偿责任也可以得到更为合理的解释。平台的赔偿责任应当以平台的治理过错为前提，当平台不存在治理过错，平台无需承担赔偿责任。当平台存在治理过错，则其承担的赔偿责任应当首先从整体性的角度进行考虑，其对于某一类型的侵权赔偿数额应当与平台因为治理过错而需要受到的罚款保持一致。[60]例如某一平台企业对平台内的某类大规模侵权存在治理过错，理想情况下应对其处以 5000 万元罚款，那么其在所有此类间接侵权案中的整体赔偿额也应当维持在 5000 万元。至于此类间接侵权案中的个案赔偿额度，法院则可以考虑权利人受到的损失、对权利人进行救济的必要性等因素进行综合考虑，对赔偿总额进行合理分配。

五、制度重构

从平台间接侵权中知情问题的一般原理出发，可以对本文开篇所提到的制度挑战与制度困境进行分析。本文开篇提到，平台间接侵权中的知情面临三大问题：共同侵权与避风港制度中的知情要求不一致；知情判断存在不确定性；知情判断存在“做的少、知道的少、错的少”“做的多、知道的多、错的多”的悖论。克服这三大问题的关键是区分特定个案型侵权与大规模治理型侵权，对前者适用传统共同侵权的知情与过错分析，对后者适用治理意义上的注意义务与责任分析。

（一）两种制度中的知情

在特定孤立的平台侵权案件中，无论是共同侵权还是避风港制度，都可以按照传统侵权中的知情过错进行分析。以 2020 年修订的《信息网络传播权司法解释》为例，其中的若干条款属于此类情形。例如，第 4 条规定“有证据证明网络服务提供者与他人以分工合作等方式共同提供作品、表演、录音录像制品”的情形；第 10 条规定“网络服务提供者在提供网络服务时，对热播影视作品等以设置榜单、目录、索引、描述性段落、内容简介等方式进行推荐，且公众可以在其网页上直接以下载、浏览或者其他方式获得的”情形，第 12 条规定“将热播影视作品等置于首页或者其他主要页面等能够为网络服务提供者明显感知的位置的”“对热播影视作品等的主题、内容主动进行选择、编辑、整理、推荐，或者为其设立专门的排行榜的”情形。在上述情形中，平台都主动参与了特定的侵权案件。当平台间接侵权存在上述情形，就应当推定平台知道侵权行为和具有过错，应当承担责任。

在特定孤立的平台侵权案件中，基于通知－删除规则的平台免责制度则不应适用。因为此类案件与传统的共同侵权案件类似，平台无论是作为还是不作为，都具有显著的主观意志。在避风港规则中，各国也将存在“明显侵权事实”排除在保护范围之外。避风港规则整体上是一种合规免责制度，其主要功能是为平台的自我治理提供法律保护。[61]而特定、孤立的平台侵权案件并不涉及自我治理，与传统共同侵权无异，其制度适用也就不应受到避风港规则的保护。

在典型的大规模治理型侵权中，首先应避免套用传统共同侵权制度的逻辑分析平台的注意义务。上文提到，《民法典》第 1197 条、《信息网络传播权保护条例》第 22 和 23 条、《电子商务法》第 38

和 45 条、《消费者权益保护法》第 44 条都使用了“应当知道”或“应知”的表述，这些表述常常被视为要求平台承担更高注意义务。此处需要强调，此类注意义务应当是治理意义上的，而非传统个案侵权中的注意义务，也非产品责任等过失侵权中的注意义务。[62]正如本文一再强调，平台的注意义务是整体性而非个案性的，其对平台治理的注意义务需要考虑治理的必要性、治理的代价、治理难度、治理的比较优势等综合性因素，而不能仅仅注意预防侵权事故。

在典型的大规模治理型侵权中，避风港制度中的注意义务也应按照治理的原则进行理解与建构。就事前而言，避风港制度虽然免除了平台的一般审查义务，但这并不意味着平台完全没有治理意义上的事前注意义务。例如，当平台内的严重侵权行为导致受害人无法获得正常赔偿，而平台本可以利用很低的成本就此类侵害行为，且不会影响平台内的正常活动，此时平台就应被认定为未履行治理意义上的注意义务。[63]当然，平台的此类事前注意义务也应当是有限度的，并且应结合本文所提到的要素进行分析，这也是为何避风港制度具有强大生命力的原因所在。[64]就事中而言，应避免将权利人通知等同于平台知情。如果将权利人通知等同于平台知情，平台间接侵权将会回到传统共同侵权的逻辑：平台在接到通知前处于不知情和没有过错的状态，在接到通知后则参与到特定个案的共同侵权中。但这种理解并不合理。事实上，权利人所发出的通知可能是错误通知，很多通知还可能是由权利人通过机器所发出的批量通知，[65]甚至有的通知可能不是权利人所发出。无论何种情形，平台在收到通知后都并未直接进入完全确定的知情状态。相反，平台在收到通知后仍然需要对平台内侵权行为的事实进行判断，例如平台需要判断权利人所发出的通知是真诚的还是恶意的？[66]其平台内侵权行为有多大概率是真实的？从治理型侵权的视角看，平台所接收到的通知更类似于举报。对于举报，平台需要对其性质、概率进行综合性判断，而非简单将某一方的举报认定为事实。就事后而言，平台所采取措施中的知情状态也应按照平台治理的逻辑进行理解。平台在接到权利人或法院通知后，可能需要采取删除之外的多种不同措施。例如欧盟著作权法采取了较为严格的要求，要求对确定侵权的内容进行“屏蔽”，以确保侵权内容不会重复上传。[67]这一规则实际上要求平台对于预防侵权采取更高的注意义务，因为只有对平台内容进行一定程度的审查才能避免侵权内容重复上传。加拿大著作权法则采取较为宽松的规则，仅要求平台进行反通知，但不要求平台删除相应侵权内容。[68]这一规则实际上将平台视为消极被动的裁决者，免除了平台的积极注意义务。限于篇幅，本文在此无法对避风港的具体制度进行详细论述。但可以指出的是，典型平台间接侵权中的避风港制度应当按照治理与举报的原理进行理解，而非转换为传统特定个案的共同侵权进行理解。

（二）走出知情的不确定性

就知情分析的不确定性而言，通过区分个案特定型侵权与治理型侵权，可以破解知情标准的统一性问题。首先，无论是传统共同侵权制度还是避风港制度，其知情判断的标准都应当是一致的，即在个案特定型侵权中按照传统侵权法中的知情与过错进行判断，在治理型侵权中按照治理意义上的注意义务进行判断。如果对于同一侵权类型与侵权形态，采用共同侵权制度与避风港制度对其进行分析导致了不同答案，那只能表明相关制度设计或制度适用出现了偏差。

其次，平台注意义务的分析应避免法律解释学上的语义学之刺，[69]不必过于关注具体语词与表述。上文提到，我国立法在知情问题上采取了不同表述，例如《信息网络传播权保护条例》使用了“不知道也没有合理的理由应当知道”，《消费者权益保护法》使用了“明知或者应知”，《电子商务法》和《民法典》使用了“知道或者应当知道”。《信息网络传播权司法解释》则除了使用“明知或应知”，还规定了“明显感知”的表述。在本文看来，对这些不同表述进行词义辨析意义不大。一方面，很多表述的区别不大，立法者在进行表述选择的时候并没有特别清

晰的考虑，甚至在立法草案与终稿中也不断变化表述。[70]另一方面，更为重要的是，对于知情状态与注意义务的分析主要与本文所提到的侵权形态与其涉及要素相关。如果相关侵权形态属于特定个案型侵权，则可以利用平台在个案中的知情状态来判断平台的过错与责任。相反，如果相关侵权属于治理型侵权，则其注意义务分析取决于本文所提到的治理的必要性、治理的代价、治理难度、治理的比较优势等因素。平台是否具有过错与是否承担责任取决于其大规模治理意义上的注意义务，而非个案中的知情。

再次，平台注意义务的分析应当根据不同领域而进行建构。[71]对于不同领域，平台治理特征非常不同，而同一领域的平台治理特征则具有相似性。例如在涉及人身财产安全特别是公民健康的侵权中，法律所要保护的权利属于绝对性权利，对其进行治理具有很强的必要性。而在知识产权领域，法律所要保护的权利常常需要与他人的合理使用权利进行平衡。因此对于涉及人身财产安全的侵权与涉及知识产权的侵权，平台的注意义务就应当有所不同，法律应当对前者施加更高的注意义务或安全保障义务，对后者则应当施加较轻的注意义务，赋予平台更大的自治权。而且，即使在知识产权内部，针对著作权、商标、专利、商业秘密的平台侵权也具有差异，对不同类型的平台间接侵权也应建构不同规则。目前，我国一方面在知识产权、消费者权益保护、人身财产安全、食品安全等不同领域确立了不同的注意义务，这种设置具有其合理性。另一方面，我国的平台注意义务也面临碎片化与不协调问题。例如《电子商务法》对涉及知识产权的间接侵权做出了特殊规定，[72]这一规定有可能引起法律解释的不一致。更为合理的方式是根据著作权、商标、专利等不同领域的间接侵权进行特殊规定，实现同一领域的规则统一性。

最后，平台的注意义务应借助个案认定实现其确定性。本文关于知情不确定性的分析可能会让一部分读者感到，平台的知情标准处在高度不确定性状态，无论是个案特定型侵权还是治理型侵权都面临不确定性。对于孤立与特定型侵权，平台在个案中的知情与过错很难统一判断。对于治理型侵权，综合考虑治理的必要性、治理的代价、治理难度、治理的比较优势等因素，也同样无法避免知情标准不确定的问题。上述担忧不无道理。不过需要指出，现实场景中的间接侵权形态虽然千变万化，但法律通过案例仍然可以形成较为确定的规则。尤其是一些典型案例，例如涉及网站分享软件侵权的案例、涉及用户公开共享型平台的著作权侵权案例，这些案例可以为判断平台注意义务提供基准。当这些典型案例被法律实践与社会广泛接受后，由案例所创造的规则也可以进一步凝练为司法解释或成文法。

从上述进路出发，平台间接侵权中知情分析的不确定性难题就可以迎刃而解。以本文开篇所提到的算法推荐问题为例，算法推荐本身并不能作为判断平台是否对个案知情的标准，但是算法也并非天然中立，算法仍然应当承担大规模治理意义上的注意义务。[73]此外，算法推荐中的平台责任也应当区分不同领域与类型，并通过案例来确定平台的治理责任。例如对于《互联网信息服务管理办法》第 15 条第（一）至（七）款规定的严重违法型言论，平台应当具有更高的算法治理责任；对于第 15 条第（八）款规定的“侮辱或者诽谤他人，侵害他人合法权益的”，平台的算法治理责任相对较低。总之，算法推荐虽然是新技术，但并未改变其基本原理，其治理义务也应当综合考虑本文所归纳的若干因素进行判断。[74]

（三）破解平台作为的悖论

就知情悖论而言，按照本文所区分的个案与特定型侵权与治理型侵权进行分析，相关问题就将不复存在。就个案特定型侵权而言，“不做不错”“做多错多”的推理并不存在问题。由于平台在个案中具有较为显著和可以辨析的主观意志，利用传统侵权法中的知情与过错概念对平台责任进行判断具有合理性。就像在传统共同侵权中，帮助侵权或教唆侵权者在共同侵权案件中知道的越少、介入越少，其承担连带侵权责任的可能性就越少。

在治理型侵权中，无论是“不做不错”“做多错

多”，还是“不做就错”“做了免责”都不合理。判断平台是否存在治理上的注意义务，关键是判断平台在治理意义上作为的合理性，而不是判断平台是否作为，是否对个案或一般侵权知情。就平台不作为而言，如果平台内存在大量侵权，而且平台主要用于侵权用途、平台本可以以较小成本阻止侵权却不作为，那么即使平台对个案侵权不知情，平台也需要承担责任。这正是美国法院在 Napster 案等 P2P 软件侵权案件中所采取的立场，[75]也是我国司法所采取的立场。[76]而当平台可以被用于大量非侵权用途，例如面向公众（public－facing）的视频分享网站可以被用于普通用户创造、交流与公共空间建构，那么即使平台不作为或采取与 P2P 类软件案件中同等的审查过滤措施，平台也可能被认定不需要承担责任。这正是美国在维亚康姆公司诉油管案中的立场，[77]也是我国司法所采取的立场。[78]各国司法之所以在 P2P 类软件案件中与面向公众的视频中采取不同立场，表面原因在于二者的法律分析框架与适用不同，但深层原因在于前者主要用于侵权活动，而后者则具有广泛的社会合法用途，因此法律对于后者的注意义务要求更低。在 Napster 案中，Napster 公司曾经提出愿意采取积极审查措施，将其软件中的侵权率降至很低，但法院仍然宣布 Napster 应当对平台内侵权承担责任。[79]

另一方面，平台作为也应根据治理意义上的注意义务进行判断。平台作为无疑会提高平台对于间接侵权的知情程度，但知情程度并不意味着平台就一定需要承担责任。如果平台越知情，就越应当承担治理责任，则此类制度设计将会导致平台对间接侵权行为的消极应对或过度规制。[80]一方面，平台可能会取消本来已有的审查措施，[81]以证明自己对平台内的间接侵权并不知情。另一方面，平台也可能会采取严厉的审查措施，过滤很多本来合法的用户内容与用户活动，以防止自己承担间接侵权责任。对于平台作为，更为合理的制度应当是看平台的作为是否符合其治理义务。如果平台的积极作为或积极审查从其合理治理出发，则无论这种积极作为是属于自我规制还是法定审查义务，则平台都应基于其积极作为而免责。相反，如果平台未从治理出发进行积极作为，则其积极作为是武断和非理性的，那么平台的积极作为或积极审查可能伤及平台内的正常活动。此时，平台反而可能需要因为其积极作为而对本文所提及的“附带伤害”承担责任。

结语

平台间接侵权中的知情问题是一个困扰法律实践与法学学术的老大难问题。本文研究指出，造成这一问题的根源在于典型的平台侵权具有与传统共同侵权非常不同的形态。在传统共同侵权中，共同侵权人具有平等、特定的关系，因此对间接侵权人适用知情分析与过错判断具有合理性。但在典型的平台侵权中，平台所扮演的是大规模治理的角色，即使平台面对的是一个侵权个案，平台所采取的行动也会引起大规模的连锁效应，具有整体性或一般性的意义。此外，平台不仅导致第三方侵权事件的发生，而且带来了大量的合法活动，面对平台内的侵权活动或权利人状态不确定的通知投诉，平台所采取的行动需要考虑其治理意义上的合理性，而不能仅仅考虑预防侵权事件发生。

从大规模治理型侵权的特征出发，本文指出在典型平台侵权中，平台知情状态分析需要走出特定侵权个案的泥沼，转而从大规模治理是否存在过错分析平台的注意义务。具体而言，平台在此类侵权中的注意义务与责任应当综合分析治理的必要性、治理的代价、治理难度、治理的比较优势。首先，无论是传统共同侵权制度中的“应知”或“应当知道”，还是避风港制度中的通知－删除规则，平台的注意义务都必须按照大规模治理型侵权的原理进行重构。其次，平台的注意义务超越个案知情分析和知情规定的语义分析，重点按照分领域、案例建构的方式构建相关规则。最后，平台作为与不作为的责任也要超越个案知情判断，既需要避免“不做不错”“做多错多”的悖论，也需要避免简单适用“不做就错”“做了免责”。综合而言，在典型平台侵权中，平台间接侵权的制度需要按照大规模治理侵权的原则重新建构。

参考文献

[1] See Laura A. Heymann, *Knowing How to Know: Secondary Liability for Speech in Copyright Law*, 55 Wake Forest Law Review 333, 347-349 (2020).

[2]对于我国网络侵权条款的性质，学界存在争议，有学者将其理解为避风港规则，也有学者将其理解为传统共同侵权制度。参见薛军：《民法典网络侵权条款研究：以法解释论框架的重构为中心》，载《比较法研究》2020 年第 4 期；王迁：《＜信息网络传播权保护条例＞中“避风港”规则的效力》，载《法学》2010 年第 6 期。

[3]参见刘金瑞：《“避风港”规则的实践困境与完善路径》，载《云南社会科学》2024 年第 1 期。

[4]需要指出，避风港规则并不等同于“通知－删除”规则，其还包括以美国通讯风化法 230 条款为模版的完全免责规则，以及“通知—通知”“通知—屏蔽”等其他多种不同模式。

[5] 17 U.S.C. Section 512(c), (d).

[6]对两种知情的综合性分析，参见美国版权局 2020 年 5 月的报告“U.S. Copyright Office Section 512 Report”，pp．113－123。

[7] 17 U.S.C. Section 512(c)(A)(i) (ii). 这一规定也被欧盟等国家和地区所采纳，我国的立法与司法也大致体现了这一原则。Also see E-Commerce Directive, 2000, Article 15.

[8]北京市海淀区人民法院（2012）海民初字第 5558 号民事判决书。

[9]北京知识产权法院（2018）京 73 民终 534 号民事判决书。

[10]浙江省杭州市西湖区人民法院（2009）杭西知初字第 11 号民事判决书。

[11] See UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).

[12] See Viacom International Inc et al v. YouTube Inc et al, 676 F.3d 19 No. 13-1720, para. 60 (2nd Cir. 2012). 需要指出，美国法院对于“故意无视”的认定是非常严格的，在 Viacom International 一案中，法院就认定 YouTube 平台存在的大量侵权内容不属于“故意无视”。

[13] See MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); Columbia Pictures, Inc. et al. v. Gary Fung et al., 710 F.3d 1020 No.10-55946 (9th Cir. 2013).

[14]分别参见《信息网络传播权保护条例》第 23 条；侵权责任法第 36 条；消费者权益保护法第 44 条；《电子商务法》第 38、45 条。

[15]参见孔祥俊：《网络著作权保护法律理念与裁判方法》，中国法制出版社 2015 年版。

[16]参见易健雄：《从算法技术看网络服务提供者的“应当知道”———也谈＜民法典＞第 1197 条的适用》，载《知识产权》2021 年第 12 期。

[17]浙江省杭州市西湖区人民法院（2009）杭西知初字第 11 号民事判决书。

[18]最高人民法院（2019）最高法民申 5954 号民事判决书。

[19]美国法院对通讯风化法 230 条款的解释强化了平台责任豁免，参见 Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997); Doe v. MySpace, Inc., 528 F.3d 413 (2008);Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009)等。

[20] See Aro Mfg. v. Convertible Top Replacement Co., 377 U.S. 476, 488 (1964).

[21] See A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[22]参见邓宏光：《信息流推荐服务提供者的行为定性——兼评＜延禧攻略＞案》，载《中国版权》2022 年第 3 期。

[23]参见熊琦：《算法推送与网络服务提供者共同侵权认定规则》，载《中国应用法学》2020 年第 4 期；崔国斌：《论算法推荐的版权中立性》，载《当代法学》2024 年第 3 期。

[24]上海市高级人民法院（2008）沪高民三（知）终字第 62 号民事判决书。

[25] Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995).

[26] 47 U.S.C. § 230(e)(3) (2012).

[27]参见《互联网信息服务管理办法》第 15 条第（八）

项。

[28]参见姚志伟：《公法阴影下的避风港——以网络服务提供者的审查义务为中心》，载《环球法律评论》2018 年第 1 期。

[29]参见丁晓东：《从网络、个人信息到人工智能：数字时代的侵权法转型》，载《法学家》2025 年第 1 期。

[30] See Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 Harvard Journal of Law & Technology 395, 397 (2003).

[31] See John C.P. Goldberg, Benjamin C. Zipursky, *Torts as Wrongs*, 88 Texas Law Review 917, 917-986 (2010).

[32] See Guido Calabresi & Spencer Smith, *On Tort Law's Dualism*, 135 Harvard Law Review Forum 184, 184-193 (2022).

[33] See Felix T. Wu, *The Structure of Secondary Copyright Liability*, 61 Houston Law Review 385, 385 (2023).

[34] See William L. Prosser, *The Assault upon the Citadel (Strict Liability to the Consumer)*, 69 Yale Law Journal 1099, 1112 (1960).

[35] See Hinman v. Westinghouse Elec. Co., 471 P.2d 988, 990 (Cal. 1970).

[36] See Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263-264 (9th Cir. 1996).

[37] See Gershwin Publ'g Corp. v. Columbia Artists Mgmt., 443 F.2d 1159, 1162 (2d Cir. 1971).

[38] See 17 U.S.C. § 512(c)(1)(B). 我国并未直接规定网络服务提供者或平台替代责任，但在司法解释中也同样引入了平台替代责任。参见《信息网络传播权司法解释》第 22 条第（四）项、《信息网络传播权司法解释》第 11 条。

[39] See Aro Mfg. v. Convertible Top Replacement Co., 377 U.S. 476, 488 (1964).

[40] 35 U.S.C. § 271 (2010).

[41]产品缺陷包括设计缺陷、制造缺陷和警示缺陷。严格责任主要适用于制造缺陷，而设计缺陷与警示缺陷则主要适用过失责任。See James A. Henderson, Jr. & Aaron D. Twerski, *Achieving Consensus on Defective Product Design*, 83 Cornell Law Review 867, 867 (1998).

[42]另一个问题是平台是否应当承担产品责任法上的销售者责任，由于篇幅所限不再展开。See Christoph Busch, Rethinking, Product Liability Rules for Online Marketplaces: A Comparative Perspective, available at: https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3897602, December 1, 2024.

[43] Perfect 10, Inc. v. Giganews, Inc., No. 15-55500 (9th Cir. 2017) p. 27 et seq.

[44]参见王磊：《安全保障义务的解释论展开》，载《现代法学》2024 年第 3 期；吴越：《安全保障义务人侵权补充责任的理论反思》，载《法学研究》2024 年第 4 期。

[45]我国民法典第 1198 条规定："宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所的经营者、管理者或者群众性活动的组织者"，"经营者、管理者或者组织者未尽到安全保障义务的，承担相应的补充责任。"民法典并未明确规定这一条所规定的安全保障义务是否可以适用于网络平台。 按照本文的分析，民法典第 1198 条所规定的安全保障义务应当按照本文所分析的大规模治理责任进行判断。

[46] 18 U.S.C. Sec. 1591.

[47] See Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 Notre Dame Law Review 293, 308 (2011).

[48]当然平台间的竞争可能会减少平台的此类行为，因为保留表面侵权但实质并非侵权的作品可以让平台内的作品更为丰富，可以为用户提供更好的服务与体验。但这种市场竞争力量是有限的，当平台需要承担的间接侵权责任较重时，平台就可能会更愿意删除表面侵权但实质并非侵权的作品，而非保留它们。

[49]有学者据此提出平台应当采用"有可能获取的

最佳技术”对平台进行管理。See Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 Columbia Law Review 1194, 1195 (2011).

[50]参见王迁：《论“通知与移除”规则对专利领域的适用性——兼评＜专利法修订草案（送审稿）＞》第 63 条第 2 款》，载《知识产权》2016 年第 3 期。

[51]参见姚志伟：《大型平台的个人信息“守门人”义务》，载《法律科学（西北政法大学学报）》2023 年第 2 期。

[52]在言论侵权中，侵权与言论自由之间的边界更难统一确定。美国的 CDA230 条款之所以对平台采取完全免责的态度，就与言论侵权的这一特征相关。对平台言论自我管理的分析，参见 Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harvard Law Review 1598, 1625-1630 (2018).

[53]参见焦和平：《算法私人执法对版权公共领域的侵蚀及其应对》，载《法商研究》2023 年第 1 期。

[54] See Steven Shavell, *Liability for Harm versus Regulation of Safety*, 13 Journal of Legal Studies 2, 357-374(1984)；丁晓东：《数字法学：多维知识的组织方式》，载《华东政法大学学报》2024 年第 3 期。

[55] See Miriam Buiten & Alexandre de Streel & Martin Peitz, *Rethinking Liability Rules for Online Hosting Platforms*, 28 International Journal of Law and Information Technology 2, 139-166 (2020).

[56]在著作权领域，有学者提出了“导管理论”（conduit theory），即著作权人可以通过平台这一“导管”而从直接侵权者那里收取许可费，而非对某一个个体侵权者收取费用。See Tun-Jen Chiang, *The Conduit Theory of Secondary Liability in Patent and Copyright Law*, 23 Nevada Law Journal 65, 65-114 (2022).

[57] See supra note 30, p.396.

[58]第（二）（三）项是否属于特定个案侵权，也需要判断“侵权信息的明显程度”是个案型还是大规模治理型，以及网络服务提供者的“选择、编辑、修改、推荐”是属于孤立特定型，还是具有大规模治理性质。如果是后者，则网络服务提供者的责任仍然应当按照治理型侵权进行判断。

[59]《网络人身权益司法解释》第 6 条对判断网络服务提供者是否属于“知道或者应当知道”具有类似项，除了第（一）项可能属于特定个案侵权，第（二）至第（六）项都属于大规模治理型侵权中的考虑要素。

[60]在个人信息保护中，也存在同样的从个体救济到公共治理的逻辑，参见丁晓东：《从个体救济到公共治理：论侵害个人信息的司法应对》，载《国家检察官学院学报》2022 年第 5 期。

[61] See Jonathan Band & Matthew Schruers, *Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act*, 20 Cardozo Arts & Entertainment Law Journal 295, 295 (2002).

[62]就此而言，典型间接侵权中的平台责任不能简单适用“最小成本避免者”（least cost avoider）理论，因为“最小成本避免者”理论主要用于纯粹损失的产品责任等领域。关于“最小成本避免者”理论，参见 Guido Calabresi & Jon T. Hirschoff, *Towards a Test for Strict Liability in Torts*, 81 Yale Law Journal 1055, 1060 (1972)。

[63] See A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001); MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). 美国在这些案例中引入了引诱侵权的制度进行分析，但实质上是借用这一制度来对平台施加一定的事前治理义务。

[64]近年来学界对避风港制度存在众多批判，在本文看来，避风港制度存在的问题在于其制度的复杂性并未得到合理阐释与合理适用，对避风港制度的批判并不意味着需要回到传统的共同侵权制度。

[65]对于通知导致的错误删除，参见 Daniel Seng, *Copyrighting Copywrongs: An Empirical Analysis of Errors with Automated DMCA Takedown Notices*, 37 Santa Clara High Technology Law Journal119, 119-

190 (2020)。

[66]在涉及著作权合理使用的案例中，法院还需要判断对著作权的合理使用是否属于“真诚相信”，参见 Lenz v. Universal Music Corp., 815 F.3d 1145 (9th Cir. 2016) 。

[67] Martin Husovec, *The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?*, 42 Columbia Journal of Law & the Arts 53, 53-84 (2018).

[68] Copyright Act, R.S.C. 1985, c C-42 §§ 41.25, 41.26 (Can.).

[69] See Ronald Dworkin, *Law's Empire*, 45-46 (1986).

[70]参见张新宝、任鸿雁：《互联网上的侵权责任：<侵权责任法>第 36 条解读》，载《中国人民大学学报》2010 年第 4 期。

[71]Mark Lemley 教授曾经尝试提出避风港规则的统一建构，参见 Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 Journal on Telecommunications and High Technology Law 101, 101 (2007)。不过 Lemley 教授主要是认为《数字千年版权法案》的通知删除规则对平台保护不够，其希望为平台免责提供更多保护。

[72]参见王英州：《论电子商务领域知识产权保护的司法介入》，载《法律适用》2021 年第 4 期；毕文轩：《电商平台涉知识产权侵权治理的困境与纾解——基于司法裁判的实证分析》，载《南开学报（哲学社会科学版）》2024 年第 1 期。

[73]参见徐俊：《互联网平台算法推荐的版权侵权责任研究》，载《政法论坛》2024 年第 1 期；宋建立：《推荐算法运用下的平台义务与责任》，载《法律适用》2024 年第 7 期。

[74]参见张吉豫、汪赛飞：《数字向善原则下算法推荐服务提供者的著作权注意义务》，载《知识产权》2022 年第 11 期。

[75] See A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545

U.S. 913 (2005); in re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020 (9th Cir. 2013).

[76]参见《信息网络传播权司法解释》第 3 条。

[77] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012)

[78]参见《信息网络传播权司法解释》第 4 条。

[79]很多学者对法院在 Napster 案等案件中的这一立场持批评态度，认为法院的完全禁止分享软件，这给分享软件施加了过重的责任。See Lawrence Lessig, Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity, 33, 60, 105 (2004).

[80] 参见 Jennifer M. Urban ET AL., Notice and Takedown in Everyday Practice, available at: https://osf.io/preprints/socarxiv/59m86, Mar. 2, 2017, pp.95-96.

[81]在市场环境下，平台具有自我审查与治理的动力，因为第三方侵权可能会导致平台被投诉，可能导致被侵权方离开平台；过多的第三方侵权也可能损害平台的市场声誉。

从网络、个人信息到人工智能：数字时代的侵权法转型

原载：《法学家》2025 年第 1 期，第 40-54 页，第 191-192 页

作者：丁晓东

摘要：数字时代，网络侵权、个人信息侵权以及人工智能侵权等新型侵权形式涌现，对传统侵权法的损害认定、过错判断、因果关系分析、救济措施应对提出挑战。传统侵权法植根于传统观念社会，以不具外溢性的小范围故意侵害行为为典型场景。数字时代的新型侵权则表现出大规模微型侵权、大规模汇聚型侵权、大规模治理型侵权、风险侵权等特征。数字时代的侵权法应进行转型升级与发挥其公法治理功能：从主观过错与因果关系判断转向责任分配分析，从损害填补转向合理威慑预防，从个体救济迈向群体福利保护，在此基础上建构具体制度。侵权法的公法治理功能可能面临外部与内部批评，但相关批评均可反驳。我国《民法典》侵权责任编同时包含传统与现代侵权法，应注重其双重结构，强化对现代侵权法公法治理功能的理解与适用。

引言

数字时代，互联网、大数据与人工智能的兴起促成了社会合作与数字经济发展，也带来了大量新型侵权形态和侵权法争议。首先，网络间接侵权或第三方侵权大量出现，互联网上的第三方主体在网络平台上对他人进行诽谤，侵害他人著作权、商标权、专利权。对于此类侵权，网络平台应当承担何种责任成为争议焦点。其次，大数据带来的个人信息处理行为日益普遍。信息处理者违规处理个人信息在侵权法上承担何种责任，成为中外侵权法学术研究的热点与难点。最后，人工智能的兴起带来了一系列新型侵权，例如生成式人工智能可能侵犯隐私权、个人信息、名誉权等人格性权益，服务型人工智能可能提供错误决策建议，产品构成类人工智能可能造成一系列人身伤害。人工智能由于具有众创性、智能涌现、人机交互、软硬件结合等特征，其侵权判断更具争议。面对数字互联的新场景，传统侵权法在损害认定、过错判断、因果关系、救济措施等方面面临着一系列挑战。[1]

本文对数字时代的侵权法挑战与回应进行分析，选取网络平台间接侵权、个人信息侵权、人工智能侵权这三个典型场景，指出数字时代的很多侵权形态与传统社会的典型侵权场景具有根本性差别。在传统社会中，侵权法主要以小范围、具有主观过错的侵权为典型场景。在这种场景下，围绕损害、过错、因果关系、补偿建构起来的侵权法制度具有高度合理性，与其背后的道德哲学与功利主义考量高度吻合。但数字化时代的侵权场景发生了巨大变化，表现出大规模微型侵权、大规模汇聚型侵权以及大规模治理侵权等特征。为了回应数字化时代的侵权法挑战，侵权法应在借鉴工业化时代侵权法的基础上，注重发挥侵权法的公法治理功能。在原理层面，数字时代的侵权法应注重责任分配而非过错与因果关系认定；注重合理威慑而非损害填补；注重群体福利保护而非个体救济。在制度层面，数字时代的侵权法应当注重侵权法制度的二重结构。对于数字时代的传统侵权形态，侵权法可以沿用传统侵权法制度工具；但对于数字时代的新型侵权形态，侵权法应当主动转型升级，积极发挥其公法治理功能。

一、数字时代的侵权与挑战

以网络间接侵权、个人信息侵权、人工智能侵权为例，可以发现数字时代的侵权对于传统侵权法提出了一系列挑战。这类侵权中的损害、过错、因果关系、救济措施都面临争议、两难或不确定性。

（一）网络平台侵权

针对网络间接侵权，各国主要通过传统共同侵权制度以及“避风港”制度应对。以我国为例，一方面《民法典》在第 1168 条规定了一般共同侵权责任，第 1169 条第 1 款规定了教唆、帮助侵权责任，第 2 款规定了替代责任，第 1171 和 1172 条规定了可分割的共同侵权责任；另一方面，《民法典》第 1194 至 1197 条引入了基于“通知—删除”规则的避风港制度，确立了网络平台侵权的特殊制度。[2]此外，我国在《信息网络传播权保护条例》《电子商

务法》《食品安全法》等法律法规中也采取了某种形式的避风港规则。[3]美国和欧盟也采取了类似的措施。例如美国法院在利用普通法中的帮助侵权、引诱侵权、替代责任等制度对网络平台责任进行调整的同时，通过《通讯风化法》（CDA）230 条款、《数字千年版权法案》（DMCA）确立了避风港规则。

网络间接侵权制度虽然已有法律规定，但在理论与实践上却仍面临争议。首先，平台对于第三方间接侵权的过错难判，甚至陷入两难。在我国与域外的法律中，分析过错都与分析平台是否知情密切相关，例如我国《民法典》第 1197 条规定，如果“网络服务提供者知道或者应当知道”存在侵权，则平台应当承担责任。[4]避风港规则中的“通知”，也被视为是一种提醒平台知情的机制。但是，以知道或知情来判断平台是否存在过错、是否应当承担责任，很难对平台施加合理责任。

一方面，如果将知情界定为知道特定侵权，则将意味着平台在绝大多数情况都应属于不知情或不存在过错。只有平台内的侵权行为属于“红旗原则”（red flag principle）所述的“侵权活动明显的事实或情况”，或者被侵权人对于平台发出通知，告知平台存在第三方侵权，平台才能被判定为存在知情与过错。在实践中，这种对知情与过错的界定导致了过于宽松的平台责任。因为按照这种界定，网络平台即使对平台内的各类侵权现象装作不知道或故意无视（willful blindness），[5]也不用承担责任。而网络平台本来可以对某些侵权现象进行预防，防止某些本可以发现的第三方侵权。另一方面，如果将“知情”界定为一般知情，则将导致网络平台责任无限扩张。平台可能会为了避免被认定为知情而放任各类违法活动滋生，以证明自己未介入内容管理。[6]平台也可能对所有内容进行严格审查，进而影响合法活动的正常开展。[7]如果我们进行极端推理，假设平台积极利用其算法技术对平台内的所有内容进行人工审查，平台将知晓所有平台内发生的侵权行为，对所有侵权行为承担责任。这显然会对平台施加过重的法律责任。

网络平台第三方侵权中的因果关系与救济措施也同样面临挑战与争议。就因果关系而言，网络平台的相关行为虽然可以被视为侵权结果的原因，但并非引起侵权行为的直接原因或主要原因。因此，对平台间接侵权中的因果关系进行判断，实际上取决于对平台的法律责任进行判断。无论将网络平台视为教唆帮助侵权的主体或作为替代责任的主体，还是不用承担责任的信息中介，法律都是通过判断平台的法律责任来判断因果关系，而非通过因果关系判断平台责任。就救济措施而言，网络平台对于间接侵权行为应当采取何种措施，也存在很多不同的方案。例如我国《民法典》第 1195 条互联网专条规定平台在“通知—删除”规则下对侵权内容采取“删除、屏蔽、断开链接等必要措施”。美国《通讯风化法》第 230 条对网络平台采取了完全免责的救济责任，《数字千年版权法案》的“通知—删除”规则（notice-takedown）要求网络平台对侵权内容进行删除；欧盟部分领域的“通知—屏蔽”规则（notice-stay down）不仅要求网络平台对侵权内容进行删除，还要求网络平台采取预防措施，防止重复侵权；[8]加拿大的避风港规则则采取了“通知—通知”（notice-notice）规则，仅要求网络平台对于侵权内容告知涉嫌侵权的一方。[9]在网络间接侵权中，由于存在大量的虚假通知与反通知、错误通知与反通知、重复侵权等现象，平台在间接侵权中采取何种救济措施更为合理，成为一个争议焦点。[10]

（二）个人信息侵权

数字时代的个人信息侵权是对传统侵权的另一挑战。首先，个人信息侵权中的个体损害往往不明显或属于轻微侵权。个人信息侵权所造成的损害大致可以分为两种情形：第一种情形是信息处理者侵犯个人信息权益，但并未造成明显人身或财产损害。例如，信息处理者在没有获得个人同意的情形下收集个人信息，或者违规处理个人信息，但这些行为并未直接对个体造成损害，也没有导致信息泄露。第二种情形是信息处理者在处理个人信息过程中造成了某些实际的损害，例如个人信息泄露导致了人身或财产损害。但即使在第二种情形中，个人

信息侵权也具有风险性特征，如个人信息泄露导致了诈骗和巨额财产损失，此类损失的直接原因是诈骗行为，而个人信息泄露仅是风险来源之一。

个人信息侵权中的过错判断、因果关系、救济措施也存在难题。就过错认定而言，除了少量主体之外，绝大多数信息处理者可能都没有主观意志上的过错。通常情况下，侵害个人信息的收益非常小，绝大多数信息处理者不具有直接侵害个人信息的动机。就因果关系而言，侵害个人信息造成损害的因果关系非常复杂。造成侵害的主体可能是个人信息处理者，也可能是非法倒卖个人信息的中间数据商。此外，很多个人信息侵害都是各类信息处理叠加后所产生的“聚合效应”（aggregation effect），即某一个人信息处理行为并未产生危害，但大量信息处理使得风险最终积聚并造成损害。[11]在这类情形中，法院都难以就因果关系进行认定。就救济措施而言，在损害认定、过错判断均不存在争议的情形下，[12]对个人信息主体提供合理的救济措施也是一大难题。

个人信息侵权使得传统侵权法面临两难。一方面，有的国家和地区将一些个人信息侵权排除在侵权法救济之外。例如，美国最高法院在过去几年的判决中一再否定一般的个人信息侵权存在损害，仅仅认定个人信息泄漏中的风险可以被认定为侵权法上的损害。[13]此种做法具有一定的合理性，毕竟如拉丁法谚所言，“法律不理琐事”（De minimis non-curat lex）。但另一方面，完全将个人信息侵权排除在侵权法救济之外，忽略了个人信息侵权的大规模性。虽然单个案例中个人受到的损害是微型或不确定性的，但海量个人信息侵权所带来的风险不应被忽视。[14]在大规模微型侵权的背景下，如何发挥侵权法的个人信息保护功能，已经成为一个全球性的挑战。

（三）人工智能侵权

人工智能侵权在损害认定、过错判断、因果关系分析、责任认定方面也存在挑战。首先，人工智能侵权是否存在损害具有不确定性。例如，生成式人工智能的训练数据很大一部分源自对公开数据或半公开数据的大量爬取，常常包含大量未经获得个人明确授权的数据。这类数据处理在大多数情形下可能不会带来明确损害，因为此类处理一般不会向第三方提供或泄露。但在特殊情形下，这类处理也可能带来一定的侵害风险，例如这类处理可能导致个人特征被用于合成各类声音、图片，侵犯个人的人格等相关权益。同时，人工智能也可能因为训练数据以及其智能化导致输出不实言论、诽谤言论或歧视言论。这些言论可能对个体造成的损害并不特别明显，但同样具有大规模侵权的特征。针对人工智能的言论侵权，有观点认为，应当对此类侵权损害适用避风港规则；但也有学者认为，生成式人工智能已经成为“大型诽谤模型”（Large Libel Models），应当承担侵权法上的相应责任。[15]

其次，人工智能侵权中的过错判断存在难题。在传统社会，人类与物之间的交互主要是人类使用工具。因此传统侵权法认为，只有人类存在主观意志与过错的问题，而物或工具的问题主要是产品安全与产品质量问题。但在人工智能所形成的交互场景下，很多决策都由人工智能这一工具做出，而人类则在其中扮演了消极或辅助性决策角色。[16]例如，在自动驾驶场景中，自动驾驶车辆是各类决策的主体，而司机则扮演了安全监管员或乘客的角色。[17]在人工智能决策权重增加与人机交互形态变换的背景下，人工智能用户所应承担的责任与人工智能系统责任的关系成为判断难题。[18]此外，如果考虑到产品责任问题，人工智能侵权中的过错与归责原则将更为复杂。在传统侵权法上，法律一般对硬件产品适用产品责任和无过错责任，对软件适用过错责任。[19]其原因在于，硬件产品可能对消费者或用户造成人身、财产等物理伤害，而且硬件产品常常可以通过设计、制造、预警等方式来预防风险，为消费者提供安全冗余。相反，软件系统则主要提供信息服务，其造成的伤害一般较小或可以通过其他信息服务而规避，而且软件系统很难避免漏洞（bugs），无法达到硬件系统那样的准确性与安全性。[20]但在人工智能时代，很多人工智能构成类的产品都具有软硬件高度融合的特征，可能带来侵权

风险。

最后，人工智能侵权中的因果关系与责任认定存在界定难题。一方面，人工智能具有“众创性”特征，参与人工智能系统生成的主体众多。这些主体既包括数据产业的数据收集者、数据清洗者与标注者，也包含人工智能算法或代码的设计者、调试者与训练者。人工智能的侵权结果可能是海量主体“众创”的结果，就如同雪花的积累最终导致了雪崩，或者海量水滴汇聚导致了水库污染，很难说哪一片雪花或水滴具有“过错”与责任，与侵权结果之间存在因果关系。另一方面，人工智能决策具有“涌现性”（emergent）特征与黑箱（black box）属性，人们常常无法直接理解人工智能做出决策的机制。例如，在个性化推荐中，人工智能算法为何给某些人推荐某类视频，搜索为何会将有些搜索结果排在前面？随着机器学习等算法的崛起，人工智能决策的黑箱特征愈发明显，这使得传统侵权法对于因果关系的判断更加困难。

二、侵权法原理重构：从传统侵权到现代侵权

数字时代的侵权法之所以面临争议与挑战，与侵权法所要应对的侵权形态变化密切相关。相比传统社会，数字时代的侵权形态发生了巨大变迁，这引发了传统侵权法的不适应。为回应数字时代的侵权形态，侵权法应进行转型升级，从纯粹私法功能的侵权法迈向兼具公法治理功能的侵权法。

（一）侵权形态的变迁

在传统社会，侵权形态大多与人们的日常生活经验相对应。例如，某人打翻了他人的一个贵重花瓶，造成了他人的财产损失；某人骑车撞到了他人，造成了他人的人身伤害。在这类侵权形态中，损害事实、侵权人过错、行为与结果之间的因果关系往往都比较清晰。此外，这些案件的影响也往往只局限于原告、被告或与原告和被告的家庭；除非某些案件成为公共性事件，一般的侵权法案件对社会整体的影响不大，不具有外溢性或外部性（externality）。共同侵权、教唆帮助侵权等连带侵权的情形要更为复杂，但也可以视为一对一侵权的复合形态。基于这些原因，传统侵权法中的制度工具可以帮助法律人或一般民众有效地分析相关案件、判断侵权责任。

但在数字时代，侵权形态的典型场景发生了根本性变化，一系列大规模微型侵权、大规模汇聚型侵权以及大规模治理型侵权开始兴起。以网络侵权为例，网络平台侵权之所以存在挑战，根本原因在于这类侵权形态具有大规模治理型侵权的特征，与传统帮助侵权、教唆侵权等共同侵权具有本质不同。在传统共同侵权中，共同侵权者或帮助侵权者仅参与特定个案，而且其与主要侵权主体之间为平等关系或小型社会的管理关系。对于共同侵权者或帮助侵权者是否具有共同侵权的主观意志、是否存在过错、是否存在因果关系，人们凭借日常经验就能够判断。而在网络间接侵权中，网络平台所扮演的角色并非个案，网络服务既带来了大量的一般性侵权，增加了社会风险，同时也促成了社会合作与数字经济发展，增加了社会福利，[21]特别是为广大普通用户提供了创造、交流与交易的机会。[22]网络平台间接侵权的这种特征使得法律对其过错、因果关系与责任认定很难套用基于传统经验的侵权法。如果侵权法仅仅关注个案中的被侵权者损害、平台是否知情与存在过错，就无法理解平台间接侵权的整体图景。

个人信息侵权、人工智能侵权则具有大规模微型侵权、大规模汇聚型侵权的特征。就大规模侵权而言，个人信息处理一方面对个体的侵害具有微型、不确定性特征，但另一方面又涉及海量个体。人工智能由于涉及海量数据主体，其输入端具有显著的大规模风险汇聚特征，其输出端则可能对海量个体造成微型侵权。[23]整体而言，数字时代带来了一系列新的侵权形态，这类侵权的侵权方与被侵权方都变得高度不确定，二者不再是一对一或小范围的引起与被引起关系。同样，如果法律依赖传统侵权法中的损害、过错、因果关系、救济措施对其进行分析，则将很难准确分析相关侵权案件，对各方施加合理责任。

在工业化时代，大规模侵权与风险侵权等新型侵权形态已经出现。[24]例如，工业化时代带来了一系列意外伤害，侵权法不得不开始面对由工业化生

产所带来的工伤等风险侵权或事故侵权。在产品侵权与消费者保护领域，由食品、日用品、家电、机动车等产品所引起的侵权也具有大规模微型侵权与风险侵权的部分特征。[25]在环境侵权中，大规模侵权与风险侵权的现象非常明显，企业所排放的污水、气体也可能对不特定的个体产生侵害。[26]数字时代无疑延续了工业化时代的某些风险特征，但相比工业化时代，数字时代的侵权形态与传统侵权更为明显。数字时代的侵权由于涉及海量主体，往往具有大规模微型侵权或大规模汇聚型侵权的特征。此外，网络平台、信息处理者与人工智能对于私人主体具有更多的控制性，这使得数字时代的侵权也呈现更多的大规模治理型特征。

（二）侵权法的迭代升级

为应对数字时代的侵权挑战，侵权法需进行转型和升级。首先，侵权法应从传统的主观过错与因果关系判断，转向更注重责任的分配。在传统侵权法中，侵权行为人的过错通常与其主观意志紧密相连，能够从道德角度将其行为认定为过错。[27]即便是过失行为，其主观意图和道德过错依然可以被识别，而且在我国侵权法上也被归入过错范畴。同样，传统侵权中的因果关系也与人们的日常经验吻合。尽管哲学意义上的终极因果关系一直存在争议，但人们凭借因果关系这一思维工具，仍然可以对传统与日常类的因果关系进行较好分析。数字时代的新型侵权形式则从根本上改变了主观过错与因果关系分析的意义。在数字时代的典型侵权中，侵权人主观意图的识别变得非常困难，侵权行为中的因果关系也不再是简单的一一对应。因果关系很大程度取决于对责任的归属进行判断。二者的关系是通过后者反推前者，而非通过前者推论后者。在此背景下，更合理和可行的方式是在不同主体之间进行责任分配，而不是继续依赖主观过错和因果关系来分析和判断侵权责任。事实上，工业化时代的过错判断已经逐渐淡化对主观意志的判断。工业化时代由于产生了大量产品与风险侵权，过失侵权成为侵权的重要形态，美国、欧盟等国家或地区都以违反注意义务对过失进行客观性判断。[28]与此同时，工业化时代因果关系分析的重要性也显著降低，因为工业化时代的因果关系本质是一种责任判断。在数字时代的新型侵权形态中，这种转变更为必要，侵权法应进一步朝着责任分配方向发展。这种责任分配也包括超越侵权法中的直接涉案主体，将社会保险、责任保险等制度纳入分析框架。

其次，侵权法的目标应从单纯的损害填补转向合理威慑。在传统侵权中，侵权法主要采取“向后看”（backward-looking）的视角，重点在于通过损害填补和矫正不公来恢复被侵权人的权利，修复侵权行为所造成的损害。[29]然而，在数字时代，以损害填补为主要目标面临诸多困境。一方面，数字时代的大规模微型侵权案件中，侵权造成的损害往往极为轻微或难以精确定义，这使得损害填补难以充分发挥作用，且难以惠及那些未提起诉讼的群体。如果侵权法仅仅以赔偿为主要手段，可能威慑效果不足，无法有效预防大量潜在风险。另一方面，数字时代的侵权行为往往伴随科技进步和技术发展，而这些进步和发展本身也是社会所追求的目标。如果仅依赖损害填补为主导，将科技进步前的状态作为参考基准，可能会导致侵权法产生过度威慑，抑制技术创新。因此，为了避免传统侵权法的困境，数字时代的侵权法应当采取“向前看”（forward-looking）的视角，[30]既合理威慑潜在的违法行为，又为科技进步和技术创新提供包容性发展的空间。

最后，侵权法应注重从个体救济转向关注群体福利的保护。传统的侵权行为通常发生在一对一或小范围内，不具有显著的外部性，因此对个体进行救济和维护群体福利往往是高度一致的。然而，随着数字时代新型侵权形态的出现，单纯的个体救济不足以实现群体福利的全面保障。为了更好地促进群体福利，数字时代的侵权法不仅应当关注个体的救济需求，还应赋予个体更广泛的公共治理功能，将其视作能够促进群体利益的“私人总检察长”（private general attorney）。[31]这种重心的转变并不意味着放弃对个体的救济，而是将个体救济纳入群体福利的整体框架进行考量。例如，在某些情况下，可以通过惩罚性赔偿或法定赔偿的方式激励个体

提起诉讼，以打击侵权行为并形成对潜在侵权者的威慑。而在其他情况下，则可能需要对某些微型侵权行为进行限制，以防止滥诉，确保科技创新和发展具有一定的试错空间。侵权法还应积极引入保险机制，为可能遭受侵害的个体提供社会层面的风险分担，从而弥补个体在侵权中所造成的损害。[32]

综合而言，数字时代的侵权法应从纯粹私法转向具有一定公法属性与治理功能的法。正如格雷戈里·基廷（Gregory Keating）教授所言，如果说传统侵权责任法关注的重心是“单数的行为世界（world of act）”，那么现代侵权责任法关注的重心则是“复数的活动世界（world of activities）”。[33]对于“复数的活动世界的侵权”，侵权法应当更注重责任分配、风险合理预防、促进群体福利等治理功能。如果继续延续传统和套用侵权法，侵权法将出现制度工具与现实世界脱节的困境。

三、制度建构：数字时代的侵权法转型

在重构数字时代侵权法原理的基础上，可以对网络平台侵权、个人信息侵权、人工智能侵权的具体制度进行建构。从大规模治理型侵权的特征出发，数字时代新型侵权中的损害认定、过错判断、因果关系分析、救济措施都应当采取不同于传统侵权法的制度结构。

（一）平台侵权制度

就网络平台侵权而言，其过错认定和知情状态的判断不应仅仅基于个案中是否知悉间接侵权行为，而应基于其是否履行了大规模治理层面的合理注意义务来判断过错。[34]一方面，当平台上存在显而易见的严重侵权行为，或平台在不影响合法活动的情况下本应知晓并采取预防措施但未能预防，则无论被侵权方是否通知，平台都应当承担间接侵权责任。因为在大规模治理层面，此类行为属于平台可以以较小成本进行有效治理的行为。另一方面，如果采取措施对平台内合法活动造成的损害大于阻止侵权的收益，则即使被侵权人通知平台，平台除了履行信息提供和核实义务外，也可以不承担赔偿责任。因为在大规模治理层面，对平台施加责任可能带来寒蝉效应，阻碍平台内的大量合法活动。总之，通过分析大规模治理意义上的合理注意义务，侵权法可以在网络间接侵权问题上摆脱“知情”问题的泥沼，直接判断网络平台是否存在违法性和是否应当承担责任。

因果关系和救济措施的设计也应遵循大规模治理型侵权的逻辑。首先，在因果关系和责任认定上，网络平台的责任不应基于个案中的行为与侵权结果之间的因果关系，而应评估平台是否履行了治理义务。具体而言，法律可以参照国家行政法律法规对平台施加的审查责任、已有技术发展水平、成本收益分析等要素，分析平台是否合理地控制了平台内的大规模侵权行为。其次，在救济措施方面，平台应根据不同情形采取不同措施。目前各国对网络平台的规则各不相同，既有完全免责制度，也有“通知—删除”“通知—通知”“通知—屏蔽”等机制。我国《民法典》也规定了“删除、屏蔽、断开链接”等必要措施。平台应在平衡预防间接侵权和保护合法活动之间找到适当的应对方案，而非一刀切或仅根据个案损害进行救济。一方面，如果平台过度激进地应对侵权行为，比如对微小侵权行为采取屏蔽、断开链接甚至删除账户的措施，这将使大量合法用户受到不当影响，带来附带损害（collateral damage），[35]使社会整体福利受损。另一方面，如果平台的措施过于消极，例如对所有侵权行为都援引《通讯风化法》第 230 条下的完全免责，[36]或对严重且可预防的侵权行为仅适用“通知—通知”或“通知—删除”规则，则平台将逃避其治理责任。

（二）个人信息侵权制度

个人信息侵权制度应该进行优化设计。个人信息侵权可以分为两类：一类是未造成实际损害的个人信息权利之诉，另一类是已造成损害的个人信息侵害之诉。[37]之所以进行这种区分，一方面是因为我国《个人信息保护法》第 50 条第 2 款和第 69 条已经对二者设立不同制度。另一方面，虽然两类个人信息侵权都可能属于大规模侵权，但前者的个体损害难以确定，而后者的损害则相对明显和易于识别。因此，这两种类型的侵权应当分别构建不同的法律制度加以应对。

首先，对于没有造成实际损害的个人信息权利之诉，应将其视为含有申诉举报性质的诉讼。当信息处理者侵害个人的信息权利，如知情同意权、查阅复制权、更正补充权、删除权和解释说明权时，此时信息处理者侵害的不仅是个体权利，更涉及法律秩序中的公共利益或法益。在这类情形中，信息处理者的行为虽然没有给个人造成明确的损害，但由于此类侵害涉及海量个体，此时法院仍然可以对此类侵权进行救济与回应。不过也正是因为此类侵权属于大规模微型侵权，法院在回应此类案件中，应将个人信息权利视为实现公共治理的工具性权利或程序性权利，而非绝对性权利。[38]此外，法院还需考虑这些权利的实际可行性以及其行使是否会对其他合法权益产生影响，包括对个人信息进行合理利用与促进数据流通。[39]

其次，个人信息侵权损害之诉也应进行制度优化。在损害认定和可诉性方面，当个人信息侵权导致了明显的损害，侵权责任的认定通常不存在争议。争议较大的情况是当个人信息侵权仅造成微小或不确定损害时，如信息处理者违规处理信息并导致敏感个人信息泄露，但未造成直接的人身或财产损害。[40]在这些情形中，法院应根据侵权法的治理功能来设计损害认定制度。一方面，法院应要求存在实质性损害或实质性风险，避免将个人的焦虑或担忧视为损害。如果对损害进行过宽界定，个人信息侵权损害之诉将引发滥诉，进而对信息处理者施加过度威慑与不合理责任。另一方面，法院应将那些可能造成重大风险的个人信息泄露案件视为侵权损害，并纳入救济范围，以提供行政监管之外的法律保护途径。[41]

最后，个人信息侵权损害之诉的过错判断、因果关系、救济措施也应进行优化设计。就过错而言，个人信息侵权损害之诉中的过错应结合个人信息处理的违法性、公共危害程度进行分析。[42]我国《个人信息保护法》第 69 条引入了过错推定原则。在适用这一条款时，法院应当将违反《个人信息保护法》和《民法典》个人信息条款的相关处理行为视为存在过错，在此基础上允许信息处理者进行抗辩。在因果关系判断方面，应当避免过度纠缠于传统因果关系分析，转而从违法性、事故发生的可能性和合理威慑等角度综合判断责任。如果信息处理者的行为违法且具有较高的事故发生概率，则可视其为应承担责任的主体。[43]在救济措施方面，个人信息侵权损害之诉除了可以适用《个人信息保护法》中规定的损失赔偿制度，还应依据《民法典》第 1167 条的规定，采用“停止侵害、排除妨碍、消除危险”等不同救济手段，具体措施应根据信息处理者违法行为的严重性和其对社会风险的影响程度来确定。[44]

（三）人工智能侵权制度

对于人工智能侵权，可首先将人工智能分为生成式人工智能、决策服务型人工智能和产品构成类人工智能，分别建构相关制度。

对于生成式人工智能造成的侵权，可以类比出版商、搜索引擎与平台的侵权责任进行分析。首先，生成式人工智能不宜采取与出版商相同的侵权责任，因为生成式人工智能的输出内容由海量用户数据汇聚、融合和训练而成，[45]在此过程中生成式人工智能企业固然可以对有关数据进行清洗或审查，但难以达到与图书编辑对内容审查相同的精细度。再加上生成式人工智能本身就具有“一本正经胡说八道”的特征，用户未必完全相信其输出内容。其次，生成式人工智能的内容主要源于网络或用户数据，在不少场景下，其数据来源具有出处或标志性。当用户可以较为清晰地辨识其信息输出内容的来源时，此时生成式人工智能具有搜索引擎或信息查找工具的特征，应当和搜索引擎一样免于承担侵权责任。不过在用户无法辨识其信息输出内容来源时，生成式人工智能的侵权责任就应区别于搜索引擎。最后，就平台而言，生成式人工智能与平台的共同特点在于二者均涉及大量用户，具备众创与数据汇聚等特征。其不同之处在于，人工智能对于信息输出具有更强的控制性，且用户不像在网络平台下可以直接控制内容的生成。[46]当用户通知生成式人工智能存在侵权内容时，这类特定侵权内容也很难被删除。基于上述原因，生成式人工智能可以借鉴“通知—删除”的避风港规则，[47]采取“通知—屏蔽”机

制，即生成式人工智能在收到侵权通知后，应通过关键词过滤等手段阻止相关内容输出。[48]当然，“通知—屏蔽”规则也应采取大规模治理的进路。在过错认定上，生成式人工智能不应通过判断其在个案中的主观意图或知情状态来评估责任，而应评估其是否履行了大规模治理意义上的注意义务，即其技术措施与人工审查是否合理平衡了生成式人工智能的发展与大规模侵权预防。在因果关系方面，生成式人工智能也应从寻求客观因果关系转向责任分配分析。

决策服务型人工智能主要应用于劳动招聘、信贷评估、法律服务等场景，这类人工智能一般为商业主体或公共机构提供服务，并不直接面向消费者。对于这类人工智能侵权中的过错判断、因果关系分析、救济措施等难题，可以参考企业顾问或政府顾问的侵权责任进行分析。首先，对于决策服务型人工智能造成的侵害，应对其应用者追究责任，对其提供者则应当适用合同违约责任和过错侵权责任。因为此类人工智能所提供决策仅具有建议性，最终的决策仍然由人工智能的应用者作出。当然，当决策服务型人工智能所提供的服务产生公共影响时，此时法律也应利用行政监管等手段对其进行合理规制。

产品构成类人工智能与决策服务型人工智能具有一定的类似性，二者都面对商家系统而非普通用户，而且二者也都具有人工智能决策的不确定性、黑箱性等特征。然而，产品构成类人工智能由于与硬件深度融合，风险更大，如自动驾驶、医疗器械中的人工智能系统失效可能直接危及人身安全。因此，法律应首先对这类嵌入人工智能的终端产品设定风险基准与市场准入门槛。为确立社会对人工智能构成产品的信心，监管部门还可以适当提高终端产品的风险预防标准。例如，国外有关监管部门认为，自动驾驶车辆只有将其事故率控制在人工驾驶事故率的一半时方可上路行驶。[49]其次，法律应对人工智能所构成的终端产品施加产品责任或严格责任。至于人工智能系统的提供者，则应当区分标准化的人工智能系统与非标准化的人工智能系统。对少量可以标准化的人工智能系统，可以对其适用产品责任或严格责任；而对绝大部分无法标准化的人工智能系统，则应对其仍适用过错责任。其原因在于，非标准化的人工智能系统很难对相关风险进行类似硬件产品的风险预防。[50]在法律对终端产品已经进行规制的背景下，终端产品制造者可以更为精准地对相关风险进行内化（internalize），对人工智能系统的风险进行控制。只有当人工智能系统成为标准化产品，例如人工智能系统被制作成为标准化的导航系统并进行大规模销售的背景下，此时法律才应当对其施加严格责任。

四、可能面临的批评与回应

侵权法的转型与重构可能会引发各种批评意见。历史上，在工业化时代的侵权法转型过程中，相关批评早已存在，这些批评同样可能延续到本文所讨论的数字时代侵权法的变革中。总体来看，批评可分为两类：外部批评和内部批评。外部批评者认为，行政规制比侵权法在应对现代大规模治理型侵权、大规模微型侵权、大规模汇聚型侵权，以及风险侵权等方面更加有效。而内部批评者则认为，即便面对现代侵权形式的变化，侵权法既没有也不应该进行重大调整。本部分指出，相关批判可以为行政法与侵权法的互动、为侵权法的多维视角提供启示，但并非否定侵权法的现代转型。

（一）外部批评与回应

外部批评的核心观点是，在应对数字时代的新型侵权问题时，应该优先依靠行政监管而非侵权法。[51]理由主要包括以下几方面：首先，数字时代的新型侵权，例如平台侵权、个人信息侵权、人工智能侵权等，通常涉及大量主体，这类侵权的本质是一种公共安全风险，因此应由政府通过监管进行事前预防，而非依赖侵权法的事后惩戒。一些学者如西奥多·艾森伯格（Theodore Eisenberg）认为，即使有惩罚性赔偿，侵权法仍难以产生足够的威慑效果。[52]其次，数字时代的侵权往往是广泛的、不确定的，涉及公共利益而非个人利益。因此，政府机构作为民主代议制的体现，政府监管更具正当性，政府有能力更好地衡量公共利益。此外，监管机构可以制

定更为普适的规则，为相关主体提供明确的行为指引，而侵权法则依赖于个案裁决，法官与陪审团的判断具有较大的不确定性。最后，数字时代的侵权通常伴随技术复杂性，专门的监管机构比法院更有能力评估相关风险。[53]

这些外部批评可以逐一回应。首先，虽然行政监管可以在一定程度上预防风险，但过度监管也可能导致正常的社会活动受到不当限制，特别是在数字时代，这可能抑制科技创新，将潜在造福社会的技术视为需要规避的风险，影响新技术和应用的市场化进程。侵权法的事后监管则有其比较优势。侵权法要等到损害发生后才进行回应，这种回应虽然具有“马后炮”的特征，但也因此对风险规制更加审慎和具有针对性。而且与事前风险监管所预设的各类可能发生的风险不同，侵权法所应对的是已经发生和被证实的风险，这就大大降低了风险过度预防的可能性。

其次，数字时代的社会风险固然涉及公共利益，但这并不意味着政府机构就一定比法院更适合应对这类风险。现代监管与规制研究的大量文献指出，政府监管可能对专业风险问题做出错误判断，[54]或者可能遭遇“监管俘获”（regulatory capture）。[55]就此而言，监管机构虽然看似具有民意代表机构的特征或代表机构授权，但其制定的规则与作出的判断却未必具有更强的民主正当性。相反，司法机构虽然常常被认为是非代议制机构，但其个案判决的公开性、对抗性程序可能赋予其更强的正当性，更有利于实现公共利益。[56]

再次，尽管行政规制具有规则确定性的优势，但这些规则也容易因时间变化失去合理性，或与现实社会脱节。[57]当监管机构制定的规则不再合理或与时俱进，那么其所进行的监管活动就可能导致监管过度或监管不足。一些本来已经不再具有风险的行为将无法正常展开，一些主体可能满足于监管合规，不再积极采取措施避免相关事故风险。[58]对于这些问题，侵权法都具有自身的相对优势。侵权法具有个案性与灵活性的特征，可以在具体案件中判断相关主体责任。同时，侵权案件往往更贴近当前的现实风险，可以避免监管规则的滞后所带来的问题。

最后，监管机构在应对专业问题时，未必具备显著的优势。现代社会专业领域日益分化，行政人员在诸多技术性问题上难以做出准确的风险评估。例如，他们可能难以评估平台算法的审查技术是否足以防止侵权，或是判断个人信息泄露的风险，以及人工智能医疗器械的安全性。无论是监管机构还是法院，都需要依赖外部专家进行风险判断。两者在专家的使用方式上有所不同：监管机构通常通过统一的专家论证和集体决策，对特定规则或标准进行风险评估；而法院则在个案审理中做出专业判断。此外，专家在风险评估中也并非总是科学或完全中立的，可能存在派系倾向或偏见。专家的风险判断可能仅仅反映精英人士的风险认知，与民众的认知具有较大差距；专家的认知也可能反映了某一学派或利益集团的观点，并非完全中立。[59]因此，这些认知差异使得监管机构与法院在使用专家方面的优势与劣势更加复杂，难以简单得出谁更占优的结论。

针对这些外部批评的反驳并不是要否定行政监管在数字时代的作用，而是要强调侵权法与行政监管在不同场景中的互补性。两者的优劣需要在具体情况下进行分析。早在 40 年前，史蒂文·夏维尔（Steven Shavell）教授就曾经作出一项经典分析，从监管机构与私人的风险认知能力、损害赔偿能力、逃脱制裁或被诉讼的机会、诉讼成本与监管成本四个要素对行政与侵权的比较优势进行分析。夏维尔教授认为，侵权法在多数情况下比行政监管更具优势。[60]我们当然不必完全认同夏维尔教授的观点，但也不能忽视侵权法的独特功能。[61]此外，我们还需要重视行政监管与侵权法在风险预防中的协调配合，避免风险规制中的“合成谬误”。[62]

（二）内部批评与回应

侵权法的转型升级还可能面临来自侵权法学界的内部批评。批评意见的代表性理论之一是朱尔斯·科尔曼（Jules Coleman）和欧内斯特·温瑞布（Ernest Weinrib）提出的矫正正义（corrective justice）

理论。矫正争议理论认为，侵权法的核心在于侵权方对被侵权方的损失进行补偿，而非承担风险预防或社会治理的职责。这一理论借鉴了亚里士多德与康德的思想，强调侵权法是一种“向后看”的损害填平机制，而非“向前看”的预防性制度；[63]侵权法的重点在于解决原告与被告之间的双边关系，而不涉及其他不特定社会群体。[64]此外，矫正争议理论认为，侵权法应当注重道德理论，而非社会治理、风险分担或合理威慑等公共政策层面的考量。[65]矫正正义理论不仅可以对侵权法的制度与历史进行更为准确的事实性描述，而且可以为具体的侵权法判决提供更为合理准确的规范性指引。

另一种对侵权法治理功能的批评来自戈德堡（John C. P. Goldberg）和奇普斯基（Benjamin C. Zipursky）提出的民事救济（civil recourse）理论。这一理论近年来颇具影响力，主张侵权法的核心功能是“确认过错”（recognizing wrongs）并提供救济，而不是如霍姆斯（Holmes）、普罗西（Prosser）及现代侵权法主流理论所认为的那样，赋予其社会治理功能。民事救济理论认为，侵权法首先是一种关系性的（relational）法律制度，处理的是侵权方与被侵权方之间的关系，而非涉及侵权方与非侵权方之外的社会主体的关系。[66]其次，侵权法的目标是为被侵权者提供国家公权力所保护的私人权利救济，这种权利具有深厚的自由主义权利哲学背景，也是侵权法赖以存在的基础。[67]最后，侵权法的核心问题在于过错，其与具体个案中的道德规范（moral norms）或社会规范（social norms）具有密切关联，其本质都是对过错进行救济，其不同之处在于侵权法将一部分道德规范上升为法律规范。[68]综合而言，民事救济理论从自由主义权利理论出发，将侵权法视为国家对个体权利被侵犯后的救济机制。民事救济理论与矫正正义理论具有一定的区别，其视角主要关注个体权利、救济程序、道德规范，而矫正正义理论则更关注侵害矫正、损害填平。[69]但二者在反对与批评现代侵权法理论方面具有一致性，都强调从内部视角看待侵权法，反对从治理功能的角度看待侵权法。

尽管矫正正义理论与民事救济理论各有其独特的学术贡献，它们对侵权法治理功能的批评却难以成立。从描述层面看，侵权法的现代转型已经是不争的事实，无论是域外还是我国，侵权法中的严格责任、危险责任和惩罚性赔偿等制度都得到了广泛认可。矫正正义理论与民事救济理论或许可以较好地描绘传统社会的侵权法，但很难对现代侵权尤其是数字时代的侵权形态进行解释与回应。[70]有学者尖锐地指出，民事救济理论更适合解释西方 18 世纪的侵权法。[71]在规范性层面，矫正正义理论和民事救济理论也难以为现代侵权法的立法与司法实践提供有效指引。矫正正义理论将损害的修复视为侵权法的核心原则，但在现代侵权中，侵权法常常偏离这一目标。例如，平台侵权中的避风港规则为平台设置了较低的责任标准，而惩罚性赔偿则对侵权者施加了较高责任。现代侵权法制度设计无可避免地会引入公共治理的要素考虑，与民事救济理论将权利救济与过错认定视为侵权法的核心并不一致。

当然，矫正正义理论与民事救济理论仍为我们提供了有价值的内部视角。[72]这两种理论提醒我们，即使在数字时代，某些侵权行为可能依然保持传统的侵权特征，法官与当事人可能仍然倾向于从个案角度出发处理侵权问题，期待更多从个案角度对侵权行为进行判断与救济。在这些情况下，侵权法应当继续聚焦于个案的权利救济功能，而不必过度强调其社会治理的角色。[73]相反，如果某一侵权类型具有大规模微型侵权、大规模汇聚型侵权、大规模治理型侵权、风险侵权等新型侵权特征，那就应当超越矫正正义理论与民事救济理论，避免仅仅关注侵权方与被侵权方而带来的“隧道视野”（tunnel vision）。只有将侵权法置于社会治理的整体视野，以事物相互联系的眼光看待具体侵权行为，才能更为有效地发挥侵权法的功能。[74]

结语

针对数字时代的侵权型态，我国《民法典》已经提供较为完备的制度工具箱。综观《民法典》的侵权责任编，可以发现其既包括传统侵权法制度，

又包含大量现代侵权法制度，凸显了侵权法的治理功能。例如，在归责原则方面，《民法典》第 1165 和第 1166 条规定了过错责任、过错推定责任和严格责任等不同的过错认定原则；在救济措施上，第 1182 条规定了不同的赔偿方案，如基于损失和侵权人所得利益的赔偿方式；第 995 条、第 1167 条和第 1205 条等条款规定了停止侵害、排除妨碍、消除危险、消除影响、恢复名誉、赔礼道歉等救济方案。此外，《民法典》第 1194 至 1197 条规定了“通知—删除”规则为基础的网络侵权责任，并引入了网络用户的“反通知”规则，进一步完善了网络避风港规则。与此同时，《民法典》人格权编将个人信息纳入法律保护范围，奠定了个人信息侵害、大数据“杀熟”、人工智能算法歧视等数字时代大规模微型侵权的法律救济基础。

与《民法典》侵权法的双重结构与转型升级相适应，数字时代的侵权法制度适用与侵权法研究也应当迭代升级。[75]在适用层面，数字时代的侵权法应首先区分传统型侵权与现代型侵权：前者通常无外溢性和社会性影响，仍适用传统侵权法的损害认定、过错责任、因果关系及损害填补等基本制度；后者则涉及社会治理功能，需要对这些侵权法制度进行重构，注重风险预防与责任合理分配。[76]此外，数字时代的侵权法还应当注重侵权法与行政监管、领域法及行业规则的协调，避免重复监管与过度威慑，充分发挥侵权法的比较优势。在研究层面，数字时代的侵权法研究需要深化对现代侵权法的理论探讨，尤其是加强与法理学及其他部门法的衔接研究，破解部门法交叉性不足、法理学与部门法研究存在“两张皮”的困境。本文的研究指出，侵权法本身就具有公法因素。随着数字时代的不断发展、新型侵权型态的不断出现，突破传统侵权法的二维想象，以多维视角理解与发挥侵权法的公法治理功能已经刻不容缓。[77]

参考文献

[1]侵权法理论对于是否将违法性作为要件存在一定争议，但对于损害、因果关系与过错都有一定共识。相关论述参见王利明：《侵权责任法》（第 2 版），中国人民大学出版社 2021 年版，第 1-4 页；梁慧星：《侵权责任法讲义》，法律出版社 2023 年版，第 1–3 页；张新宝：《侵权责任法》（第 5 版），中国人民大学出版社 2020 年版，第 1-3 页；杨立新：《侵权责任法》（第 2 版），高等教育出版社 2021 年版，第 1-2 页；程啸：《侵权责任法》（第 3 版），法律出版社 2021 年版，第 1-5 页。

[2]参见张新宝：《侵权责任编：在承继中完善和创新》，载《中国法学》2020 年第 4 期，第 109-129 页；程啸：《论我国〈民法典〉网络侵权责任中的通知规则》，载《武汉大学学报（哲学社会科学版）》2020 年第 6 期，第 137-149 页；余佳楠：《网络服务提供者的妨害人责任——以合比例性为中心》，载《中外法学》2021 年第 6 期，第 1638-1657 页。

[3]参见何炼红：《论算法时代网络著作权侵权中的通知规则》，载《法商研究》2021 年第 4 期，第 186-200 页；熊琦：《著作权法“通知—必要措施”义务的比较经验与本土特色》，载《苏州大学学报（法学版）》2022 年第 9 期，第 97-109 页；薛军：《〈电子商务法〉平台责任的内涵及其适用模式》，载《法律科学（西北政法大学学报）》2023 年第 1 期，第 57-68 页。

[4]除了《民法典》，我国的相关法律法规以及被废止的《侵权责任法》对知情问题进行了不同规定，引起了对知情标准的很多讨论，参见刘文杰：《网络服务提供者的安全保障义务》，载《中外法学》2012 年第 2 期，第 495-410 页；陈锦川：《网络服务提供者过错认定的研究》，载《知识产权》2011 年第 2 期，第 56-62 页；冯术杰：《论网络服务提供者间接侵权责任的过错形态》，载《中国法学》2016 年第 4 期，第 179-197 页；朱开鑫：《网络著作权间接侵权规则的制度重构》，载《法学家》2019 年第 6 期，第 121-122 页。

[5] See Viacom International Inc et al. v. YouTube Inc et al. ,676 F. 3d 19 No. 13-1720 (2nd Cir. 2012).

[6]这种情况正是避风港制度出现前所发生的现象。See Stratton Oakmont, Inc. v. Prodigy Services

Co. ,1995 WL 323710 (N. Y. Sup. Ct. 1995).

[7]这正是欧盟《数字单一市场版权和相关权利指令》（DSM 指令）所引发的争议。See Annemarie Bridy, "The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform", *Vanderbilt Journal of Entertainment and Technology Law*, Vol.22(2020), p. 343.

[8] Council Directive (EU) 2019 /790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market,2019 O. J. (L 130), Art. 17 (4).

[9] See Copyright Act, R. S. C. 1985, c C-42 §§ 41. 25,41. 26 (Can.).

[10] See Martin Husovec, "The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?", *Columbia Journal of Law & The Arts*, Vol.42 (2018), p. 53.

[11] See Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press,2004, pp. 44-47.

[12]参见马更新：《数据交易中个人信息保护制度之完善——以"知情—同意"规则为核心》，载《河北学刊》2024 年第 2 期，第 193-204 页。

[13] See Spokeo, Inc. v. Robins,136 S. Ct. 1540,1549 (2016); TransUnion LLC v. Ramirez,141 S. Ct. 2190(2021) .

[14]参见王利明、丁晓东：《论〈个人信息保护法〉的特色、亮点与适用》，载《法学家》2021 年第 6 期，第 13 页；龙卫球：《〈个人信息保护法〉的基本法定位与保护功能——基于新法体系形成及其展开的分析》，载《现代法学》2021 年第 5 期，第 84-104 页；彭诚信：《论个人信息权与传统人格权的实质性区分》，载《法学家》2023 年第 4 期，第 146-159 页。

[15] See Eugene Volokh, "Large Libel Models? Liability for AI Output?", *Journal of Free Speech Law*, Vol. 3 (2023), p. 489.

[16] See Gerhard Wagner, "Robot, Inc.: Personhood for Autonomous Systems?", *Fordham Law Review*, Vol. 88, No. 2 (2019), p. 602.

[17]参见冯珏：《自动驾驶汽车致损的民事侵权责任》，载《中国法学》2018 年第 6 期，第 109-132 页； Nora Freeman Engstrom, "When Cars Crash: The Automobile′ s Tort Law Legacy" ,*Wake Forest Law Review*, Vol. 53 (2018), pp. 294-336.

[18] See Andrew D. Selbst, "Negligence and AI′ s Human Users", *Boston University Law Review*, Vol. 100 (2020), p. 1315.

[19] See Michael Scott, "Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?", *Maryland Law Review*, Vol. 67(2008), pp. 469-470.

[20] See Jay P. Kesan, Carol M. Hayes, "Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Soft- ware Vulnerabilities", *Arizona Law Review*, Vol. 58 (2016), p. 780.

[21]就此而言，网络平台责任也不能简单套用"最小成本避免者"理论，将平台视为"最小成本避免者"。See Catherine M. Sharkey, "Products Liability in the Digital Age: Online Platforms as 'Cheapest Cost Avoiders'", *Hastings Law Journal*, Vol. 73 (2022), pp. 1327-1351.

[22] See Pamela Samuelson, "Pushing Back on Stricter Copyright ISP Liability Rules", *Michigan Technology Law*, Vol. 27 (2021), pp. 334-342.

[23]参见丁晓东：《人工智能促进型的数据制度》，载《中国法律评论》2023 年第 6 期，第 175-191 页。

[24] See Oliver Wendell Holmes, "The Path of the Law", *Harvard Law Review*, Vol.100, No.5(1997), pp. 991-1009.

[25] See John Fabian Witt, "Speedy Fred Taylor and the Ironies of Enterprise Liability", *Columbia Law Review*, Vol.103(2003), pp. 1-49.

[26] See Peter Cane, "Using Tort Law to Enforce Environmental Regulation?", *Washburn Law Journal*, Vol.41(2002), p. 402.

[27] See John C. P. Goldberg, "Twentieth-Century Tort

Theory", *Georgetown Law Journal*, Vol.91, No.3(2003), pp. 513-584.

[28]我国也有学者呼吁区分故意与过失，参见叶名怡：《侵权法上故意与过失的区分及其意义》，载《法律科学》2010 年第 4 期，第 87-98 页。

[29]参见石佳友：《论侵权责任法的预防职能——兼评我国〈侵权责任法（草案）〉（二次审议稿）》，载《中州学刊》2009 年第 4 期，第 100-103 页。

[30]关于向后看的视角与向前看的视角，See Michael L. Rustad, Thomas H. Koenig, "Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory", *Brooklyn Law Review*, Vol.68(2002), pp. 12-13.

[31] See Danielle K. Citron, "The Privacy Policymaking of State Attorneys General", *Notre Dame Law Review*, Vol.92(2017), p. 748.

[32] See Gary T. Schwartz, "Auto No-Fault and First-Party Insurance: Advantages and Problems", *Southern California Law Review*, Vol.73(2000), pp. 611-676.

[33] See Gregory C. Keating, "Is Tort Law 'Private'?", in Oberdiek, J., Miller, P.(eds.), *Civil Wrongs and Justice in Private Law*, Oxford: Oxford University Press, 2019, p. 367.

[34] See Felix Wu, "The Structure of Secondary Copyright Liability", *Houston Law Review*, Vol.61(2023), p. 401.

[35] See Tun-Jen Chiang, "The Conduit Theory of Secondary Liability in Patent and Copyright Law", *Nevada Law Journal*, Vol.23(2022), pp. 87-93.

[36] COMMUNICATIONS DECENCY ACT,47 U. S. C. § 230.

[37]参见丁晓东：《从个体救济到公共治理：论侵害个人信息的司法应对》，载《国家检察官学院学报》2022 年第 5 期，第 103-120 页。

[38] See Margot E. Kaminski, "Binary Governance: Lessons from the GDPR′s Approach to Algorithmic Accountability", *Southern California Law Review*, Vol.92(2019), p. 1529.

[39]参见申卫星：《数字权利体系再造：迈向隐私、信息与数据的差序格局》，载《政法论坛》2020 年第 3 期，第 89-102 页。

[40] See Seth F. Kreimer, "Spooky Action at a Distance: Intangible Injury in Fact in the Information Age", *Journal of Constitutional Law*, Vol.18 (2016), p. 745; Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms", *Texas Law Review*, Vol.96(2018), pp. 756-774.

[41] See Peter C. Ormerod, "A Private Enforcement Remedy for Information Misuse", *Boston College Law Review*, Vol.60(2019), pp. 1893-1948.

[42]参见蔡立东、展海晴：《论个人信息权益保护范围的厘定——以行为违法判断为核心》，载《吉林大学社会科学学报》2023 年第 2 期，第 5-18 页。

[43]参见谢鸿飞：《个人信息处理者对信息侵权下游损害的侵权责任》，载《法律适用》2022 年第 1 期，第 43-44 页。

[44]参见梅夏英：《社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度》，载《环球法律评论》2022 年第 1 期，第 5-20 页。

[45]生成式人工智能的新型侵权形态还包括数据侵权问题。参见丁晓东：《企业数据的合同法与侵权法保护》，载《法制与社会发展》2024 年第 4 期，第 190-204 页；赵新潮：《企业数据权利的法律保护与侵权救济》，载《河北学刊》2023 年第 4 期，第 208 页。

[46] See Peter Henderson, Tatsunori Hashimoto and Mark Lemley, "Where's the Liability in Harmful AI Speech?", *Journal Free Speech Law*, Vol.3(2023), pp. 592-593.

[47] See Jane Bambauer, "Negligent AI Speech: Some Thoughts About Duty", *Journal of Free Speech Law*, Vol.3(2023), pp. 343-362.

[48] See Eugene Volokh, "Large Libel Models? Liability for AI Output?", *Journal of Free Speech Law*, Vol.32023), pp. 514-518.

[49] See Bryant Walker Smith, "Automated Driving

and Product Liability", *Michigan State Law Review*, Vol.2017(2017), pp. 1-74.

[50]参见丁晓东：《人工智能风险的法律规制——以欧盟〈人工智能法〉为例》，载《法律科学》2024 年第 5 期，第 3-18 页。限于篇幅，无法就人工智能产品销售者是否应当承担产品责任的问题展开讨论，相关讨论参见高圣平：《论产品责任的责任主体及归责事由——以〈侵权责任法〉"产品责任"章的解释论为视角》，载《政治与法律》2010 年第 5 期，第 2-9 页。

[51] See Richard C. Ausness et al., "Providing a Safe Harbor for Those Who Play by the Rules: The Case for a Strong Regulatory Compliance Defense", *Utah Law Review*, Vol.2008(2008), pp. 115-157; Richard B. Stewart, "Regulatory Compliance Preclusion of Tort Liability: Limiting the Dual-Track System", *Georgetown Law Journal*, Vol.88(1999), pp. 2167-2186.

[52] See Theodore Eisenberg, "Measuring the Deterrent Effect of Punitive Damages", *Georgetown Law Journal*, Vol.87(1998), pp. 347-357.

[53] See Richard B. Stewart, "Regulatory Compliance Preclusion of Tort Liability: Limiting the Dual-Track System", *Georgetown Law Journal*, Vol.88(1999), p. 2177.

[54] See Richard Goldberg, *Medicinal Product Liability and Regulation*, Oxford: Hart Publishing, 2013, pp. 1-210.

[55] See Anthony Ogus, *Regulation: Legal Form and Economic Theory*, Oxford: Oxford University Press, 1994, pp. 57-58.

[56] See Douglas A. Kysar, "The Public Life of Private Law: Tort Law as a Risk Regulation Mechanism", *European Journal of Risk Regulation*, Vol.9, No.1(2018), pp. 48-65.

[57] See Teresa Moran Schwartz, "Regulatory Standards and Products Liability: Striking the Right Balance Between the Two", *University of Michigan Journal of Law Reform*, Vol.30(1997), pp. 444-445.

[58] See W. Page Keeton, Dan B. Dobbs, Robert E. Keeton and David G. Owen, *Prosser and Keeton on the Law of Torts*, Minnesota: West Group, 1984, p. 229.

[59] See Marcia Angell, Science on Trial: *The Clash of Medical Evidence and the Law in the Breast Implant Case*, New York: W. W. Norton & Company, 1996, pp. 109-132.

[60] See Steven Shavell, "Liability for Harm versus Regulation of Safety", *The Journal of Legal Studies*, Vol.1, No.2(1984), pp. 358-364.

[61] See Clayton P. Gillette and James E. Krier, "Risk, Courts, and Agencies", *University of Pennsylvania Law Review*, Vol.138(1990), pp. 1027-1109; Michael D. Green, "Statutory Compliance and Tort Liability: Examining the Strongest Cas", *University of Michigan Journal of Law Reform*, Vol.30(1997), pp. 461-510; Robert L. Rabin, "Reassessing Regulatory Compliance", *Georgetown Law Journal*, Vol.88(2000), pp. 2049-2084.

[62]中文领域也已经积累了大量研究，参见朱虎：《规制法与侵权法》，中国人民大学出版社 2018 年版。

[63] See Ernest J. Weinrib, "Corrective Justice in a Nutshell", *The University of Toronto Law Journal*, Vol.52, No.4(2002), pp. 349-356.

[64] See Ernest J. Weinrib, "Deterrence and Corrective Justice", *UCLA Law Review*, Vol.50(2002), p. 623.

[65] See Jules L. Coleman, "The Mixed Conception of Corrective Justice", *Iowa Law Review*, Vol.77(1992), p. 428.

[66] See John C. P. Goldberg and Benjamin C. Zipursky, *Recognizing Wrongs*, Cambridge: The Belknap Press of Harvard University Press, 2020, pp. 1-24.

[67] See Benjamin C. Zipursky, "Rights, Wrongs, and Recourse in the Law of Torts", *Vanderbilt Law Review*, Vol.51(1998), pp. 1-100.

[68] See John C. P. Goldberg and Benjamin C. Zipursky,

"Torts as Wrongs", *Texas Law Review*, Vol.88(2010), pp. 917-986.

[69] See Benjamin C. Zipursky, "Civil Recourse, Not Corrective Justice", *Georgetown Law Journal*, Vol.91(2003), pp. 695-756.

[70] See Richard A Posner, "Instrumental and Noninstrumental Theories of Tort Law", *Indiana Law Journal*, Vol.88(2013), pp. 487-519.

[71] See Michael L. Rustad, "Torts as Public Wrongs", *Pepperdine Law Review*, Vol.38(2011), pp. 433-550.

[72] See John C. P. Goldberg, Benjamin C. Zipursky, "Seeing Tort Law from the Internal Point of View: Holmes and Hart on Legal Du- tie", Fordham Law Review, Vol.75(2006), pp. 1563-1592.

[73] See Guido Calabresi and Spencer Smith, "On Tort Law's Dualism", *Harvard Law Review Forum*, Vol.135(2022), pp. 184-193.

[74] See Michael L. Rustad, "Twenty-First-Century Tort Theories: The Internalist/Externalist Debate", *Indiana Law Journal*, Vol.88(2013), pp. 419-447.

[75]参见王利明、丁晓东：《数字时代民法的发展与完善》，载《华东政法大学学报》2023 年第 2 期，第 6-21 页。

[76]民法的形式主义与功能主义之争，参见熊丙万：《法律的形式与功能——以"知假买假"案为分析范例》，载《中外法学》2017 年第 2 期，第 300-339 页。

[77]关于法学知识的想象与组织方式，参见丁晓东：《数字法学：多维知识的组织方式》，载《华东政法大学学报》2024 年第 3 期，第 84-97 页。

（技术编辑：艾薇）

案例分析

未经授权进行 AI 换脸的侵权法探究——廖某诉某科技文化有限公司网络侵权责任纠纷案

撰写人：朱恬馨

1. 案件事实

原告廖某是一名古风短视频博主，在全网拥有较多粉丝。被告某科技文化有限公司在未经原告授权同意的情况下，使用原告出镜的系列视频制作换脸模板，并上传至其运营的涉案软件中，提供给用户付费使用并以此牟利。原告诉称，被告的行为侵犯其肖像权与个人信息权益，要求被告书面赔礼道歉、赔偿经济损失与精神损失。被告某科技文化有限公司辩称，其运营的平台发布的视频均有合法来源，并且面部特征并非原告，并未侵害原告肖像权；此外，，涉案软件所使用的“换脸技术”实际由第三方提供，故被告并未处理原告的个人信息，并未侵害原告的个人信息权益。经审理查明，涉案换脸模板视频与原告创作的系列视频的妆容、发型、服饰、动作、灯光及镜头切换呈现一致特征，但出镜人的面部特征均不相同且并非原告。法院判决被告不构成对原告肖像权的侵害，但构成对原告个人信息权益的侵害。[1]

2. 法律问题

本案的的争议是，被告是否侵害了原告的肖像权？就此需要讨论两个问题：1.肖像如何定义？被告没有使用原告的面部特征，而是在抹去面部特征后使用了原告的其他外在形象制作视频，这是否符合肖像的定义？2.肖像权的特征是具有可识别性，应当以什么作为法院判断可识别性的参照？

3. 案例分析

（1）肖像的定义

关于肖像的定义，学界主要存在两种观点。“面部中心说”认为，只有含有自然人面部特征的形象，才能称为肖像，自然人的面部特征以外的能够反映自然人的其他特征的形象，不属于肖像。[2]“外部形象说”则认为，肖像系作为人的外部形象的客观再现，[3]以面部形象为主，但不局限于此，凡足以呈现个人外部形象的均包括在内。[4]

司法实践中的主流观点认为肖像的定义已不局限于面部特征，还包括能被一般大众所识别的身体其他外部形象。比如赵某某与某某公司，黄某某肖像权纠纷一案5、米某某与北京某某科技有限公司肖像权纠纷一案6与魏江、北京及力科技有限公司肖像权纠纷一案7，其基本案情都是某公司作为被告，在未经原告允许的情况下，在其换脸软件中使用原告肖像为原内容的短视频作为模版提供给用户换脸使用，并提供融脸功能，利用信息技术手段变造原告的肖像视频，法院都认为被告侵犯了原告的肖像权，这就承认了肖像的定义是包括面部以外的其他身体特征的。《民法典》第 1018 条第 2 款 8的规定也支持了“外部形象说”的观点。

然而，即使支持“外部形象说”，不同法院就“换脸”这类案件的判决却截然不同。认为不侵权的法院给出的理由是去除掉面部信息后剩下的是妆容、发型、服饰等要素，它们并非无法与特定自然人所分割的要素，不具有可识别性。在林某某与北京某科技有限公司网络侵权责任纠纷一案9中，法院认为被告没有侵犯原告的肖像权，其理由是，虽然随着时代和技术的发展，肖像权保护的范围不局限于面部，但仍应符合法律规定的“反映特定自然人可以被识别的外部形象”，但在该案中，原告视频中人物的面部不仅被去除，并且被替换，本质

1 《北京互联网法院涉个人信息及数据典型案例》“AI 换脸”案：未经授权对包含他人肖像的视频进行“AI 换脸”处理，构成对他人个人信息权益的侵害——廖某诉某科技文化有限公司网络侵权责任纠纷案。
2 郭明瑞、张玉东：“肖像权三题”，载《浙江工商大学学报》2014 年第 1 期。
3 陈甦、谢鸿飞主编：《民法典评注•人格权编》，中国法制出版社 2020 年版，第 226-227 页。
4 王泽鉴：《人格权法》，北京大学出版社 2013 年版，第 141 页。
5 重庆市巴南区人民法院（2024)渝 0113 民初 1435 号。
6 成都铁路运输第一法院（2024)川 7101 民初 5615 号。
7 成都铁路运输第一法院（2022)川 7101 民初 5472 号。
8 《民法典》第 1018 条第 2 款：“肖像是通过影像、雕塑、绘画等方式在一定载体上所反映的特定自然人可以被识别的外部形象。”
9 北京互联网法院（2023）京 0491 民初 12766 号。

上已经将视频中具有识别性的核心部分替换成为他人极具识别性的面部肖像，消解甚至破坏了肖像所具有的“个体识别”特征，一般公众通过涉案换脸模板视频可以直接识别到的实为模板中的人物而非原告。在本案中，法院给出的理由与林某某与北京某科技有限公司网络侵权责任纠纷一案类似。

而认为侵权的法院则多从人格权的精神利益出发，认为公民形象的完整性受法律保护，任何人不得非法损毁、恶意玷污，被告换脸的行为侵犯了肖像权人的人格尊严。在陆永兴诉薛仲良肖像权纠纷案中10，被告未经同意，利用原告与冰心的合影照片，通过图片编辑软件将原告躯体部分影像保留，头部影像更换成被告的头部影像，形成了被告与冰心的合影照片，并将编辑后的照片刊登在《冰心与江阴》内发行。一二审法院均认为被告侵犯了原告的肖像权，但原因却不同：一审法院认为，肖像权保护范围不限于人的五官，还包括人的躯体，因此被告行为侵犯了原告肖像权。二审法院认为，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，在语义上存在逻辑错误。二审法院之所以认为被告侵犯了肖像权，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，尤其忌讳将已成影像中的头部从躯干上人为地去除，被告未经原告的许可，擅自通过电脑技术将视为具有特定价值的照片中的头部影像从其整体影像中分离，破坏了原告肖像在该合影照片中的完整性，其行为侵害了原告最基本的肖像完整展现的专有权益，已经构成侵权。在北京及力科技有限公司肖像权纠纷一案中，法院提到“该软件通过 AI 换脸技术替换了原视频中的角色用于软件用户的娱乐，系利用信息技术伪造的方式侵害了原告的肖像权，这侵犯了肖像权人的人格尊严。故被告未经原告的同意，使用技术手段伪造原告视频中的肖像并以营利为目的，侵犯了原告的肖像权。”

笔者认为，精神利益的判断标准过于抽象，不具有说服力，仍应当以可识别性为标准判断是否侵权，接下来将讨论肖像权可识别性的参照于判断标准。

（1）肖像权可识别性的判断标准

可识别性强调肖像的本质在于指向特定的人，通过技术手段再现的肖像要能够使一般公众辨认出该肖像为何人的形象。虽然随着时代和技术的发展，肖像权保护的范围不局限于面部，但仍应符合法律规定的“反映特定自然人可以被识别的外部形象”，即应指向自然人与生俱来的、区别于其他自然人的特定个体形象。这种形象应主要集中于自然人的生理特征所形成的外部形象，以面部为核心，也可能涉及独特的身体部位、声音、识别性较高的特定动作等，能与特定自然人形成一一对应。

肖像是否可以被识别，一种观点认为，应以社会一般人能否识别作为判断标准[11]；另一种观点认为，一般人识别的标准难以确立，应当以肖像权人自身生活、工作的群体作为认定标准；[12]还有观点认为，依据是否直接体现个人形象来利用肖像进行认定。[13]笔者认为，需要区分名人和普通人分别讨论。对于名人，由于其社会影响度较高，被大众所熟知，印象应当以一般人能否识别作为判断标准；对于普通人则可以放宽标准，以肖像权人自身生活、工作的群体作为认定标准；最后，如果某个个体的知名度仅限于某一行业（例如京剧界），则以该业界的普通受众能否识别来进行判断。[14]

再来看本案，涉案视频去除了原告的面部特征，剩下的身体外部形象主要包括妆容、发型、服饰、灯光、镜头切换等，不同于声音、身体部位等自然人与生俱来的人格要素，它们极易被模仿、复制、伪造，即使以肖像权人自身生活、工作的群体作为认定标准，也无法将它们与特定自然人形成一一对应关系，因此无法成为肖像权客体。

此外，在本案审理过程中，原告是用自己的照

[10] 江苏省无锡市中级人民法院（2009）锡民终字第 0168 号。

[11] 王利明、程啸：《中国民法典释评·人格权编》，中国人民大学出版社 2020 年版，第 280 页。

[12] 石冠彬：“司法视域下民法典肖像权新规的教义学展开”载《甘肃政法大学学报》2020 年第 5 期 第 106-115 页。

[13] 王叶刚：“论肖像的可识别性及其认定”，载《四川大学学报（哲学社会科学版）》2018 年第 3 期 第 27-31 页。

[14] 同注 12。

片进行参照后发现被告使用的框架和原告的视频很相似，法院认可了这种参照方式，而有学者认为不能用原告照片作为参照标准，因为不特定陌生人在看到视频时并不认识原告，应当在没参照照片的时候也能识别出原告身份，这样才符合可识别性。在林某某与北京某科技有限公司网络侵权责任纠纷一案中，法院否定了原告直接将自己视频与涉案视频进行对比以此来论证被告侵权的行为。

笔者认为应当在没参照照片的情况下也能识别出原告身份才符合可识别性，理由是，以社会一般人能否识别为判断标准，意味着只有社会一般人在没有原照可供参照对比的情况下可以识别出特定自然人，才满足可识别性要求；若是以自然人自身生活、工作的群体能否识别作为判断标准，那么由于这个群体脑海里实际上是有该自然人之肖像信息的，因此他们实际上是将脑海中的肖像信息与涉案视频进行了一番对比，发现了涉案视频可以识别出该自然人。由此可知，无论是以哪类人能否识别作为判断可识别性的标准，都不需要参照原照。

4. 小结

AI 换脸与个人肖像密切相关，不免引起公众对肖像权与个人信息权益的担忧。本案明确了肖像权“可识别性”不局限于面部，但应当主要集中于自然人的个人生理特征，避免肖像权的任意扩张影响妆容、造型等领域的合法使用及创作传播。其次，在判断是否具备可识别性的时候，应当将“AI 换脸”后的视频与原告本人进行对比，而不应与原告进行过特定妆造后拍摄的照片进行对比，以符合可识别性的定义。本案围绕“AI 换脸”这一新商业模式，对肖像权、个人信息权益及基于劳动创造投入的合法权益进行准确区分，既维护自然人的合法权益，又为人工智能技术和新兴产业发展留有合理空间，对于服务和保障数字经济规范健康发展有重要意义。

（技术编辑：朱恬馨）