

第二章 中国数据涉外法治发展

梅夏英、许可、吴涵

第一节 大事记

一、《网络数据安全条例》生效

2024 年 9 月，国务院公布《网络数据安全条例》，并自 2025 年 1 月 1 日起施行。

¹作为《网络安全法》《数据安全法》《个人信息保护法》的配套行政法规，也是网络数据安全领域首个行政法规级文件，本条例对三部法律中规定的原则性规范和制度进行内容和流程方面的细化规定，解决制度衔接与规则落地问题，以协助做好法律实施，规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。

二、《公共数据资源授权运营实施规范（试行）》《公共数据资源登记管理暂行办法》出台

2025 年 1 月 20 日，国家发展改革委、国家数据局联合公布《公共数据资源授权运营实施规范（试行）》，旨在通过建立公共数据资源授权运营基础制度规则，指导相关单位规范化开展授权运营工作，重点从基本要求、方案编制、协议签订、运营实施、运营管理等五个方面，明确了授权运营工作的决策流程、实施路径和管理要求。²同日，两部门联合印发《公共数据资源登记管理暂行办法》，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 workflows。这份文件明确了公共数据资源登记的基本要求，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。³

三、《个人信息保护合规审计管理办法》生效

2025 年 2 月 12 日，国家网信办公布《个人信息保护合规审计管理办法》，自 2025 年 5 月 1 日起施行。⁴有关负责人表示，《个人信息保护法》《网络数据安全条例》对个人

¹ 国务院：《网络数据安全条例》，国令第 790 号，2024 年 9 月 30 日发布。

² 国家发展改革委、国家数据局：《公共数据资源授权运营实施规范（试行）》，发改数据规〔2025〕27 号，2025 年 1 月 20 日发布。

³ 国家发展改革委、国家数据局：《公共数据资源登记管理暂行办法》，发改数据规〔2025〕26 号，2025 年 1 月 20 日发布。

⁴ 国家互联网信息办公室：《个人信息保护合规审计管理办法》，国家互联网信息办公室令第 18 号，2025

信息处理者开展个人信息保护合规审计作了规定，本办法对合规审计活动的开展、合规审计机构的选择、合规审计的频次、个人信息处理者和专业机构在合规审计中的义务等作出细化规定，旨在为个人信息处理者开展个人信息保护合规审计提供系统性、针对性、可操作性的规范，提升个人信息处理活动合规水平，保护个人信息权益。

四、《中国人民银行业务领域数据安全管理办法》生效

2025 年 5 月 9 日，中国人民银行发布《中国人民银行业务领域数据安全管理办法》，并自 2025 年 6 月 30 日起施行。¹本办法全面衔接《数据安全法》《个人信息保护法》及《网络数据安全管理条例》等上位法，细化并加强中国人民银行业务领域数据安全合规要求的可操作性，以期在金融从业机构数字化转型的关键时期，更加有效地构建中国人民银行业务领域数据安全治理体系，督促指导相关数据处理器合规开展数据处理活动，并切实强化全流程风险防控能力，同时也平衡金融数据要素价值的充分释放，从而为现代化金融服务体系稳健运行提供坚实保障，筑牢国家金融安全与数据安全防线。

五、个人信息保护负责人报送工作启动

2025 年 7 月 18 日，国家互联网信息办公室发布《关于开展个人信息保护负责人信息报送工作的公告》，要求处理 100 万人以上个人信息的个人信息处理者，向所在地设区的市级网信部门履行个人信息保护负责人信息报送手续。²该公告正式启动个人信息保护负责人信息报送工作，表明个人信息保护工作将进入规范化、常态化的阶段：个人信息处理者处理个人信息数量已达到 100 万人的，需在规定期限前完成信息报送工作；公告发布之日后处理个人信息数量达到 100 万人的，应当自数量达到之日起 30 个工作日内完成信息报送。

六、《人工智能生成合成内容标识办法》施行

2025 年 9 月 1 日，国家网信办等多部委联合发布的《人工智能生成合成内容标识办法》正式施行。³该办法旨在促进人工智能健康发展，规范人工智能生成合成内容标识。具体而言，该办法主要适用于《互联网信息服务算法推荐管理规定》《互联网信息服务深度合

年 2 月 12 日发布。

¹ 中国人民银行：《中国人民银行业务领域数据安全管理办法》，中国人民银行令〔2025〕第 3 号，2025 年 5 月 9 日发布。

² 国家互联网信息办公室：《关于开展个人信息保护负责人信息报送工作的公告》，载中国国家互联网信息办公室网站，https://www.cac.gov.cn/2025-07/18/c_1754553420421538.htm，2026 年 2 月 28 日访问。

³ 国家互联网信息办公室、工业和信息化部、公安部：《人工智能生成合成内容标识办法》，国信办通字〔2025〕2 号，2025 年 3 月 7 日发布。

成管理规定》《生成式人工智能服务管理暂行办法》规定情形的网络信息服务提供者，就生成合成内容的标识类型（显式标识及隐式标识）、标识部署场景与部署方式等提出进一步细化规定，从而推动人工智能生成合成内容标识义务在实践中的落地。

七、《国家网络安全事件报告管理办法》生效

为规范网络安全事件报告管理、及时控制网络安全事件造成的损失和危害，2025年9月11日，国家网信办正式出台《国家网络安全事件报告管理办法》，并于2025年11月1日起施行。¹该办法全文共14条，主要对网络安全事件报告适用范围、监管职责、报告主体、报告流程、报告时限、报告内容等提出规范要求。该办法旨在强化网络安全事件报告机制，保证在意外情况下能够实现政企联动，有效应对网络安全事件，消除负面影响，同时也可以提示利益相关方采取措施，减少或者避免网络安全事件带来的损害。

八、《个人信息出境认证办法》发布

2025年10月14日，国家互联网信息办公室公布《个人信息出境认证办法》，自2026年1月1日起施行。²该办法旨在保护个人信息权益，规范个人信息出境认证活动，促进个人信息高效安全跨境流动。具体而言，该办法明确了个人信息出境认证的适用条件，同时对申请个人信息出境认证的程序做出了详细规定。本次国家网信办以规章立法的方式，专门明确了个人信息出境保护认证工作的要求、程序等，对我国提升数据出境管理水平，明确企业数据出境策略，扩大数字领域开放和保障个人信息出境安全等具有重要意义。

九、《网络安全法》迎来修订

2025年10月24日，十四届全国人大常委会第十八次会议表决通过关于修改《网络安全法》的决定，并将自2026年1月1日起施行。³这是2016年《网络安全法》出台以来的首次正式修订。此次修法，在深入总结网络领域相关立法实施经验的基础上，重点完善了危害网络运行安全、网络产品和服务安全、网络信息安全行为的法律责任，加大处罚力度，扩大法律的域外适用情形，并积极回应了人工智能治理和发展需要。

¹ 国家互联网信息办公室：《国家网络安全事件报告管理办法》，载中国国家互联网信息办公室网站，https://www.cac.gov.cn/2025-09/15/c_1759583017717009.htm，2026年2月28日访问。

² 国家互联网信息办公室、国家市场监督管理总局：《个人信息出境认证办法》，国家互联网信息办公室国家市场监督管理总局令第20号，2025年10月14日发布。

³ 《网络安全法》（2025年10月28日修正）。

十、《大型网络平台个人信息保护规定（征求意见稿）》发布

2025 年 11 月 22 日，国家网信办和公安部联合发布《大型网络平台个人信息保护规定（征求意见稿）》，向社会公开征求意见。¹该征求意见稿旨在规范大型网络平台个人信息处理活动，保护个人信息合法权益，促进个人信息依法合理利用。《征求意见稿》从数量、业务、风险和其他因素四个方面明确了认定大型网络平台的条件，同时强调了大型网络平台个人信息保护、数据安全的特别义务。具体而言，包括设立个人信息保护负责人和个人信息保护工作机构，提升大型网络平台个人信息保护合规审计要求，同时提出了个人信息本地存储和大型网络平台使用第三方数据中心存储个人信息时的额外要求。

十一、《人工智能拟人化互动服务管理暂行办法（征求意见稿）》发布

2025 年 12 月 27 日，国家网信办发布《人工智能拟人化互动服务管理暂行办法（征求意见稿）》，向社会公开征求意见。²该征求意见稿旨在促进人工智能拟人化互动服务健康发展和规范应用，鼓励拟人化互动服务创新发展，对拟人化互动服务实行包容审慎和分类分级监管，防止滥用失控。该征求意见稿提出了人工智能拟人化服务的概念，并提出了内容安全、主体责任、数据管理、高风险管控、特殊群体保护、安全评估等义务要求。

¹ 国家互联网信息办公室、公安部：《大型网络平台个人信息保护规定（征求意见稿）》，载中国国家互联网信息办公室网站，https://www.cac.gov.cn/2025-11/22/c_1765543463511624.htm，2026 年 2 月 28 日访问。

² 国家互联网信息办公室：《人工智能拟人化互动服务管理暂行办法（征求意见稿）》，载中国国家互联网信息办公室网站，https://www.cac.gov.cn/2025-12/27/c_1768571207311996.htm，2026 年 2 月 28 日访问。

第二节 综合分析

一、个人信息处理规则进一步完善

随着数字经济的持续演进，个人信息处理的合规性要求日益提升。《网络数据安全条例》（以下简称“《网数条例》”）的施行标志着我国个人信息处理规则进入新阶段，填补了此前法律与部门规章之间的衔接空白，在体系架构与具体要求上实现了双重完善，构建起包含法律、行政法规、部门规章、行业规范、国家标准在内的多层次个人信息合规体系，为个人信息主体权益保护提供了更坚实的制度保障。¹

在体系架构上，《网数条例》处于承上启下的关键位置。一方面，《网数条例》向上衔接法律层面，以《网络安全法》《数据安全法》《个人信息保护法》构成的基础性法律框架为依据，将三部法律中关于个人信息处理的基本原则与权利义务框架转化为可落地的具体管理要求。另一方面，《网数条例》向下整合支撑部门规章、行业规范与国家标准。针对此前已出台的多领域、多时期规范以及实践中已经成熟的管理经验，《网数条例》形成了体系化的统筹与衔接：例如《网数条例》与《工业和信息化部关于开展信息通信服务感知提升行动的通知》中确立的个人信息保护“双清单”管理要求相互呼应，要求网络数据处理者以清单形式向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息。²同时，《网数条例》还为部门规章、行业规范与国家标准的出台提供了行政法规层级的依据，推动分散的领域规范与技术标准形成协同合力：2025年6月施行的《中国人民银行业务领域数据安全管理办法》在秉持《网数条例》合规导向的基础上，聚焦中国人民银行业务领域的特殊性，既进一步健全了该领域数据安全管理的具体规范，也为数据的合法开发利用锚定了方向。³

在具体要求上，《网数条例》既对既有立法规定予以细化完善，又回应了数据经济发展和数据治理实践的新需求。首先针对基于同意开展的个人信息处理活动，《网数条例》一方面对不同场景下个人同意的适用要求予以重申与细化，明确敏感个人信息需单独同意、未成年人个人信息需监护人同意等特殊规则；另一方面则划定了同意获取与行使的禁止性红线，如不得通过误导、欺诈、胁迫等方式取得同意，不得在个人拒绝后频繁征求同意等。其次，《网数条例》清晰界定了“个人信息转移权”行使的核心条件，同时对超出合理范围的

¹ 国务院：《网络数据安全条例》，国令第790号，2024年9月30日发布。

² 工业和信息化部信息通信管理局：《工业和信息化部关于开展信息通信服务感知提升行动的通知》，工信信管函〔2021〕292号，2021年11月1日发布。

³ 中国人民银行：《中国人民银行业务领域数据安全管理办法》，中国人民银行令〔2025〕第3号，2025年5月9日发布。

转移请求作出费用收取的补充规定。这一系列具体规则填补了此前相关立法在实践操作层面的空白，让个人信息转移权从原则性规定转化为可落地、可执行的制度安排，为我国个人信息权益保护与数据要素合理流通提供了更具针对性的法治保障。再次，针对自动化采集技术应用中易出现的非必要个人信息采集、未经同意获取个人信息以及注销账号情形下的个人信息保护问题，《网数条例》确立了以“删除或匿名化处理”为核心原则，以“停止主动处理并加强保护”为例外补充的分级合规要求，为相关场景下的数据处理行为划定了清晰明确的操作规范。最后，《网数条例》回应了实践中长期存在的争议，即个人信息达到特定敏感度与数量级是否将构成重要数据。条例明确规定处理 1000 万人以上个人信息的网络数据处理者需遵守《网数条例》项下的特定重要数据处理者合规义务。这一界定不仅为重要数据的判定提供了可量化的关键阈值，也从规模维度强化了对大规模个人信息集合的特殊保护。

值得注意的是，在个人信息保护方面，《网数条例》展现出与国际数据治理实践积极接轨的鲜明特点。例如，在个人信息保存期限的告知义务上，条例规定若保存期限难以确定，则应明确其确定方法；对于符合特定条件的大型网络平台，条例增设了更严格的外部监督与年度报告要求，强化了中国版“守门人”责任体系；在个人信息跨境流动的合法性基础上，条例在《促进和规范数据跨境流动规定》的基础上，明确将“履行合同所必需”纳入个人信息出境的合法情形之一。这些规则设计，既立足中国数据治理的实际需要，也反映了对欧盟《数字市场法案》(DMA) 等国际规则中成熟经验的合理吸收与本土化融合。

二、司法判决锚定个人信息处理的合规水位

数字时代下个人信息处理场景日趋多元复杂，个人信息保护合规基准的明晰亟待司法实践的助力。2025 年发布的一系列典型案例，聚焦个人信息处理合法性基础适用、个人信息主体行权响应等核心问题，为完善个人信息保护合规体系提供了关键司法支撑。

(一) 个人信息处理的合法性基础

在个人信息处理的合法性基础方面，尽管《个人信息保护法》第十三条明确提供了六类合法性基础，但在实践操作中，取得个人同意仍是应用最广泛的合规路径。¹究其原因，一方面在于“个人同意”本身的获取流程相对便捷，且认定标准与对应的法律效果清晰明确，便于个人信息处理者合规落地。另一方面则是其他合法性基础的适用场景、操作标准缺乏监管层面的细化指引，个人信息处理者在选择适用时易因界定模糊而面临合规风险，进而

¹ 《个人信息保护法》第十三条。

倾向于采取更为稳妥的“个人同意”模式。这一局面随着 2025 年 8 月最高人民法院第 265 号、266 号指导性案例的发布得以松动，两份案例共同划定了“为订立或履行合同所必需”这一合法性基础的理解边界与适用条件，划定合规底线。

在第 265 号指导性案例“罗某诉某科技有限公司隐私权、个人信息保护纠纷案”中，某科技公司运营英语学习网站及 APP，其在未征得罗某同意的情况下，通过线下合作体验店收集罗某手机号，为其创建网站账号密码并发送相关信息；随后罗某尝试登录账号时被强制要求填写职业、学习目的等信息，相关界面未提供“跳过”“拒绝”等选项，亦无授权同意收集个人信息的提示。罗某遂以隐私权、个人信息保护纠纷起诉，主张该公司未告知个人信息收集政策、强制收集并超范围使用用户画像等信息、发送营销短信侵扰其私人生活安宁等。该公司辩称，收集用户画像系提供个性化推荐服务所必需，无需用户个人同意。¹

针对“为订立、履行个人作为一方当事人的合同所必需”这一合法性基础的认定，法院明确，可以结合有关法律法规及规章、规范性文件等对必要个人信息范围的规定，并考量合同的类型、内容等作出认定：如果信息处理的缺位将使合同约定的基本功能服务或者用户自主选择的附加功能服务无法实现的，可以认定为订立、履行合同所必需，反之则不予认定。法院援引《常见类型移动互联网应用程序必要个人信息范围规定》（国信办秘字〔2021〕14 号）作为参考的行业规范，对案涉 APP 的基本服务功能及其所需必要个人信息进行释明后，结合产品功能设置，裁决认定收集用户画像信息并非提供网络服务所必需，且在未向用户提供不同意提交相关信息情况下的其他登录方式，属于用户非自愿同意提供个人信息的情形。

与之相对，在第 266 号指导性案例“黄某欢诉某信用管理有限公司个人信息保护纠纷案”中，针对某信用公司在提供“先享后付”服务时收集黄某欢个人信息的行为是否符合“履行合同所必需”的认定要件，法院结合“先享后付”功能与案涉信用服务开通的关联程度、信用服务的核心功能，以及信用服务商开展风控评估的业务刚需等多重因素综合研判，最终认定收集案涉个人信息属于履行“先享后付”合同所必需，实际无需取得个人同意。²但需注意的是，在案件中，根据告知同意规则，法院重申了即使是个人信息处理者不需要取得个人同意而开展处理活动的情形，也仍然需要履行告知义务。

上述两案分别从正反双向阐释了“履行合同所必需”的认定标准，通过司法判例的系统

¹ 最高人民法院：《指导性案例 265 号：罗某诉某科技有限公司隐私权、个人信息保护纠纷案》，载最高人民法院网站，<https://www.court.gov.cn/shenpan/xiangqing/474481.html>，2026 年 2 月 28 日访问。

² 最高人民法院：《指导性案例 266 号：黄某欢诉某信用管理有限公司个人信息保护纠纷案》，载最高人民法院网站，<https://www.court.gov.cn/zixun/xiangqing/474491.html>，2026 年 2 月 28 日访问。

论证，为该合法性基础下必要个人信息的范围确立了更为清晰的界定规则，体现了审慎、合理界定的司法立场。

（二）个人信息主体行权响应

在个人信息主体行权响应方面，司法裁判同样起到了关键作用，通过个案审理进一步明晰了合规标准。2025 年 10 月，北京市第四中级人民法院召开新闻发布会，发布个人信息保护类案件审判情况。同时，法院通报了 7 起个人信息权益保护典型案例，其中提及的“李某某与某科技公司网络侵权责任纠纷案”与“肖某与某科技公司网络侵权责任纠纷案”为个人信息查阅复制权的理解与适用提供了重要指引。

“李某某与某科技公司网络侵权责任纠纷案”为处理涉及多主体权益的衍生信息时，如何依法回应个人信息主体的查阅、复制请求提供了实践参照。¹本案中，李某某作为某科技公司运营的某短视频 APP 实名用户，要求该公司以书面形式向其提供其曾观看过的全部视频浏览记录，该公司一直未予答复，直至李某某起诉后，该公司方以 Excel 表格的形式提供了部分时间段内李某某浏览记录的副本，包括视频观看时间、观看完成度（百分比）、视频链接。

本案一审法院认为，针对浏览记录等衍生个人信息的查阅、复制请求，个人信息处理者可结合数据形式、存储能力、服务能力等因素，选择合理的提供方式与标准，但不得损害其他个人信息主体的合法权益，故判决被告科技公司向原告提供一定期间的浏览记录。二审法院在维持原判的同时进一步阐明，判断个人信息处理者是否履行查阅、复制义务，需综合考量信息类型、数量及请求形式等因素。对于浏览记录类信息，处理者既可以通过设置用户自主操作的系统指引，也可通过专门系统或人工渠道响应，两种方式均符合现行法律对保障知情权与决定权的要求。法院同时指出，该科技公司现有查阅方式在完整性与便捷性上存在不足，应向李某某提供浏览记录副本。基于浏览记录特性，提供准确的网络链接地址即可视为履行基本提供义务。

“肖某与某科技公司网络侵权责任纠纷案”则进一步厘清了个人信息查阅、复制权的保护属性与抗辩边界。²本案中，某科技公司系某网盘平台的运营主体，肖某为该平台的实名注册用户。肖某任职于某公司，负责招投标文件的制作工作，于 2022 年将其付费购置的投标文件资料存储至个人网盘账户。2023 年，肖某发现其网盘账号存在近年的不明登录记

¹ 北京日报：《北京四中院通报个人信息保护类案件审判情况及典型案例》，载北京日报网站，<https://xinwen.bjd.com.cn/content/s69032cfee4b0221b9beee6ce.html>，2026 年 2 月 28 日访问。

² 北京日报：《北京四中院通报个人信息保护类案件审判情况及典型案例》，载北京日报网站，<https://xinwen.bjd.com.cn/content/s69032cfee4b0221b9beee6ce.html>，2026 年 2 月 28 日访问。

录，且账户内出现陌生文件夹。肖某因此怀疑账号遭他人异常登录、网盘文件已泄露，遂通过多种投诉渠道向该科技公司申请调取异常登录时段的账号登录详情，但均未果。

一审法院认为该科技公司已通过系统功能提供部分个人信息查询，且肖某未在诉前提出具体请求，同时该科技公司在诉讼中已对相关问题作出解释，结合《信息安全技术 个人信息安全规范》(GB/T 35273-2020) 中关于技术成本的规定，认定公司拒绝提供具有合理性，未侵害肖某权利。二审法院则指出，公司提供的查询功能存在信息不完整、条件受限等问题，无法满足用户对个人信息的完整查阅需求。同时二审法院强调，处理者的解释说明不能替代提供信息的法定义务，推荐性国家标准中的成本考量亦不得对抗《民法典》与《个人信息保护法》的强制性规定。鉴于该公司具备提供能力，二审改判其应在指定期限内向肖某提供完整登录记录副本。

上述案例体现出法院在个人信息主体行权响应场景下对于主体合法权益、立法目的与现实可行性等因素的多方考量，彰显了数字治理中的司法审慎与平衡智慧。此外，相关案例还涉及告知义务履行、最小必要原则适用、依法获取主体单独同意、员工个人信息保护等重要维度，体现了司法机关在确立个人信息保护合规尺度中的关键地位。

三、个人信息保护合规审计正式启动

如前所述，《个人信息保护合规审计管理办法》(以下简称“**《审计办法》**”) 于 2025 年 5 月 1 日起施行。该办法共 20 条，明确了个人信息保护合规审计的基本要求、审计类型、审计程序、专业机构资质、各方责任义务等核心内容，明确了审计报告与整改要求。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；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，负责个人信息保护合规审计工作。¹《审计办法》将审计分为两类：一是个人信息处理者自行定期开展的合规审计，二是依据履行个人信息保护职责的部门要求开展的合规审计，同时将《个人信息保护法》中的抽象指标转化为 27 项具体的合规审计标准。这一重要法规的出台，不仅是《个人信息保护法》的关键配套制度，更是我国在个人信息保护合规治理方面迈出的实质性一步。

《审计办法》的出台体现了我国个人信息保护监管的战略导向：一是从形式合规转变为实质合规，提升了个人信息权益保护；二是政府监管、企业自治、行业自律与社会监督多元共治，促进数字治理的良性发展；三是以规范制度营造公平竞争环境，促进数字产业

¹ 同前注 4，《个人信息保护合规审计管理办法》。

创新，为数字经济的可持续发展注入新动力。从国际视角看，《审计办法》的出台使我国在个人信息保护领域的制度建设走在了世界前列，通过建立科学、规范、可操作的审计制度，展现我国在数字治理的积极姿态，更有助于提升我国在全球数据治理中的话语权和影响力。

《审计办法》出台以来，受到各地监管与私营部门的高度重视。一方面，各地监管部门纷纷推动个人信息保护审计制度在基层落地生根。2025年7月4日，浙江省开展“之江数安-2025”专项行动，要求各企业全面排查业务系统平台访问登录日志、数据处理日志、服务器/主机设备日志以及数据传输日志等留存审计的合规情况。¹2025年9月12日，吉林省人民政府发表《吉林省人民政府关于加快推进人工智能创新发展的实施意见》，敦促提升人工智能安全治理水平，贯彻落实网络和数据安全防护相关法律法规，加快推动落实个人信息保护认证、合规审计等要求。²2025年11月25日，上海市网信办、市场监管局、卫健委联合发布《上海市医疗服务类互联网企业网络数据安全和个人信息保护合规指引》，该指引第17条规定了处理100万人以上个人信息的企业，应当根据《个人信息保护法》和《审计办法》规定，向上海市互联网信息办公室履行个人信息保护负责人信息报送手续。³另一方面，个人信息保护审计工作也受到我国私营部门的积极响应。早在2024年9月，苏州市轨道交通集团率先响应国家加强个人信息保护合规治理的水平号召，启动个人信息保护合规审计项目规划，对个人信息处理活动开展合规审计和整改。⁴可以预期，个人信息保护审计将逐步成为我国数字治理以及企业内部合规治理的常规环节，进一步促进我国行业监管和企业个人信息保护工作的开展，形成良性循环。

此外，在个人信息保护合规审计工作中，第三方专业机构和人员的资质要求也始终倍受关注。《审计办法》第7条要求，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，并鼓励相关专业机构通过认证。2025年5月26日，全国网络安全标准化技术委员会进一步发布《网络安全标准实践指南——个人信息保护合规审计要求》(TC260-PG-20255A)和《网络安全标准实践指南——个人信息保护合规审计专业机构服务能力要求》(TC260-PG-20254A)，明确了个人信息保护合规

¹ 浙江通信管理局：《浙江省通信管理局关于开展“之江数安-2025”专项行动的通知》，载浙江通信管理局网站，https://zjca.miit.gov.cn/zwgk/zcwj/wjfb/art/2025/art_c6778c1e955d407e88a2616a9ff5e452.html，2026年2月28日访问。

² 吉林省人民政府：《吉林省人民政府关于加快推进人工智能创新发展的实施意见》，吉政发〔2025〕9号，2025年9月12日发布。

³ 上海市互联网信息办公室、上海市市场监督管理局、上海市卫生健康委员会：《上海市医疗服务类互联网企业网络数据安全和个人信息保护合规指引》，载澎湃新闻网站，https://www.thepaper.cn/newsDetail_forward_32044221，2026年2月28日访问。

⁴ 苏州市审计局：《苏州轨道集团开展个人信息保护合规审计》，载苏州市审计局官方网站，<https://audit.suzhou.gov.cn/audit/jyjl/202503/6e3d519c7c06423aa3c70ae18b83bcb2.shtml>，2026年2月28日访问。

审计人员和机构应当具备的能力。¹5月27日，网信办在答记者问中公布，将个人信息保护合规审计人员能力评价工作，交由其指导下的中国网络空间安全协会组织实施；该协会同时根据前述两份指南为依据，编制《个人信息保护合规审计人员能力评价要点》，为开展个人信息保护合规审计人员的能力评价提供参考。²此外，7月18日，国家网信办公布《关于开展个人信息保护负责人信息报送工作的公告》，进一步推进《审计办法》中“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”的个人信息保护工作。³由此，审计制度、现有各项法律法规、部门规章与各项个人信息保护系列专项行动形成了监管闭环，标志着我国个人信息保护进入全方位、立体化的治理新阶段。

四、人工智能涉外布局持续拓展

2025年，人工智能已成为重塑全球竞争格局的关键变量。作为全球人工智能发展的重要一极，中国在这一年展现出前所未有的国际参与度和影响力。从倡议成立世界人工智能合作组织到推动“人工智能+”国际合作，从深化与东盟、上合组织的区域合作到拓展与欧美、非洲、拉美等地区的双边伙伴关系，中国正以更加开放、包容、普惠的姿态，在全球AI治理体系中发挥引领作用。

（一）开局起势：多边机制与双边合作同步推进

2025年伊始，中国AI涉外布局便展现出强劲势头，多边机制建设与双边务实合作取得实质性进展。

2025年1月3日，中国—金砖国家人工智能发展与合作中心运营基地在上海西岸大剧院正式启用，为金砖国家AI合作搭建了重要平台，标志着中国在国际多边AI合作机制建设上迈出重要一步。⁴

2025年2月10日至11日，习近平主席特别代表、中共中央政治局委员、国务院副

¹ 全国网络安全标准化技术委员会秘书处：《网络安全标准实践指南——个人信息保护合规审计要求》，载全国网络安全标准化技术委员会官网，2025年5月19日，<https://www.tc260.org.cn/portal/article/2/20250519172429>；全国网络安全标准化技术委员会秘书处：《网络安全标准实践指南——个人信息保护合规审计专业机构服务能力要求》，载全国网络安全标准化技术委员会官网，<https://www.tc260.org.cn/portal/article/2/20250519172332>，2026年2月28日访问。

² 国家互联网信息办公室：《〈个人信息保护合规审计管理办法〉实施有关事项答记者问》，载中国网信网，https://www.cac.gov.cn/2025-05/27/c_1750056480898746.htm；中国网络空间安全协会：《个人信息保护合规审计人员能力评价要点》，载中国网络空间安全协会官网，<https://www.cybersac.cn/detail/1927994773663158273>，2026年2月28日访问。

³ 国家互联网信息办公室：《关于开展个人信息保护负责人信息报送工作的公告》，载中国网信网，https://www.cac.gov.cn/2025-07/18/c_1754553420421538.htm，2026年2月28日访问。

⁴ 上海市经济和信息化委员会：《上海市“人工智能+”行动推进大会暨中国—金砖国家人工智能发展与合作中心基地启用仪式顺利举办》，载上海经信委微信公众号，<https://mp.weixin.qq.com/s/4k7gPZ62GceayV4v90anaw>，2026年2月28日访问。

总理张国清出席在巴黎举行的人工智能行动峰会并致辞。张国清副总理强调，中国以高度负责的态度参与人工智能全球治理，2023年10月习近平主席提出的《全球人工智能治理倡议》为全球AI治理贡献了中国智慧。来自30多个国家的国家元首、政府首脑或高级别代表出席峰会，共同发布《关于发展包容、可持续的人工智能造福人类与地球的声明》，体现了中国作为负责任大国的全球视野和国际担当。¹

2025年2月23日，中国与老挝在万象签署共建中国—老挝人工智能创新合作中心协议，旨在系统化提升老挝在智能时代的基础能力，为老挝产业发展全面赋能，体现了中国对东盟AI合作的战略重视。²

（二）纵深拓展：聚焦能力建设与治理共识

进入年中，中国在多边AI合作机制建设上取得突破性进展。

2025年5月6日，中国、赞比亚常驻联合国代表团和中国科协在纽约联合国总部共同举办人工智能能力建设国际合作之友小组专题会议，来自70多个国家和国际组织的100多位代表参会，共商人工智能发展现状和前景，为发展中国家在AI领域的能力建设提供了重要平台。该会议也彰显了中方将坚持智能向善、公平普惠、协同共治，与各方共同推进人工智能全球治理与合作的决心。³

2025年5月29日，国家发展改革委、天津市人民政府联合主办的“2025中国—上海合作组织人工智能合作论坛”在天津成功召开。本次论坛以“智汇中国 智慧上合”为主题，旨在推动中国同上合组织成员国加强人工智能发展和治理务实合作，共享人工智能发展红利。⁴

2025年6月17日至20日，中国政府同禁化武组织在上海合作举办“AI向善，共享未来：人工智能助力履行《禁化武公约》”国际研修班，同全球来自40多个国家的代表分享中国人工智能发展治理经验，用实际行动回应了国际社会对中国AI技术在全球安全治理方面应用的期待。⁵

¹ 新华社：《张国清出席法国人工智能行动峰会并致辞》，载外交部官网，https://www.mfa.gov.cn/web/wjdt_674879/gjldrhd_674881/202502/t20250211_11553050.shtml，2026年2月28日访问。

² 新华社：《中国—老挝人工智能创新合作中心签约》，载新华网，<https://www.news.cn/world/20250224/4620c6ce18b34829b936fbc6a3643074/c.html>，2026年2月28日访问。

³ 常驻联合国代表团：《常驻联合国代表傅聪大使出席人工智能能力建设国际合作之友小组专题会议》，载外交部官网，https://www.mfa.gov.cn/web/wjdt_674879/zwbdt_674895/202505/t20250508_11617323.shtml，2026年2月28日访问。

⁴ 政策研究室：《中国—上海合作组织人工智能合作论坛在津召开》，载国家发展和改革委员会官网，https://www.ndrc.gov.cn/fzggw/wld/hr/zyhd/202505/t20250530_1398181.html，2026年2月28日访问。

⁵ 人民日报：《计利天下，推动人工智能赋能禁化武履约》，载人民周刊网，https://www.peopleweekly.cn/html/2025/renminzhiku_0613/249873.html，2026年2月28日访问。

2025 年 7 月，国家发展改革委与巴西科技创新部正式签署《关于共建中国—巴西人工智能应用合作中心的谅解备忘录》，计划在夯实人工智能发展的多方面开展务实合作。¹同月，中欧数据跨境流动交流机制第二次会议在布鲁塞尔举行，双方同意设立工作组，就汽车领域数据跨境流动开展合作，展现了我国在数据安全领域与国际社会积极合作、齐头并进的姿态。²

（三）峰会引领：提出“中国方案”与构建开放生态

2025 年下半年成为中国 AI 涉外布局的关键时期，多项重大倡议相继发布，推动全球治理体系变革。

2025 年 7 月 6 日，李强总理在金砖国家第十七次峰会全体会议上宣布，中国将在全球发展倡议（GDI）框架下发起“数字南方”倡议，未来五年将为全球南方国家举办 200 个数字经济和人工智能领域的培训项目，展现了中国为推动共同发展、完善全球治理、促进世界持久和平繁荣作出更大贡献的决心。³

2025 年 7 月 26 日至 28 日，在上海举办的 2025 世界人工智能大会暨人工智能全球治理高级别会议（WAIC），以“智能时代、同球共济”的主题，明确传递了中国反对技术脱钩、主张多边主义的信号。本次大会的场地规模和嘉宾阵容创造了历史之最，汇聚了来自 70 多个国家和地区的 800 多家人工智能企业，展出 3000 余项前沿技术成果，同时吸引了 30 多个国家和地区超过 1200 位嘉宾参会，其中包括图灵奖、诺贝尔奖等共 12 位国际顶尖奖项得主，以及超过 80 位国际顶尖学术代表，并推出《人工智能全球治理行动计划》13 项举措。这无疑展现了上海以及中国在国际 AI 产业的国际影响力和号召力，标志着中国从 AI 技术应用者向全球治理规则制定者的重要转变。⁴同时，中国政府在本次会议上倡议成立世界人工智能合作组织（WAICO），初步考虑总部设在上海。这一倡议旨在加强人工智能领域的国际合作，推动共商共建共享全球治理，是中国坚持践行多边主义、响应全球南方呼声、推动共商共建共享全球治理的重要举措。⁵

在会议期间，在 2025 年 7 月 26 日，工业和信息化部还推动中国—金砖国家人工智

¹ 政策研究室：《国家发展改革委与巴西有关部门签署合作文件》，载国家发展和改革委员会官网，https://www.ndrc.gov.cn/fzggw/wld/lss/zygz/202507/t20250707_1399017.html，2026 年 2 月 28 日访问。

² 国家互联网信息办公室：《中欧数据跨境流动交流机制第二次会议在布鲁塞尔举行》，载中国网信网，https://www.cac.gov.cn/2025-07/18/c_1754549064237501.htm，2026 年 2 月 28 日访问。

³ 央视网：《李强出席金砖国家领导人第十七次会晤第二及第三阶段会议》，载 CCTV 节目官网，<https://tv.cctv.com/2025/07/08/VIDEz82XsajC1mqn7FTWCTn6250708.shtml>，2026 年 2 月 28 日访问。

⁴ 新华社：《共探未来——从 2025 世界人工智能大会看 AI 发展新动向》，载新华网，<https://www.news.cn/tech/20250730/3281a99e69014cd68a721a7f1a590e36/c.html>，2026 年 2 月 28 日访问。

⁵ 新华社：《中国政府倡议成立世界人工智能合作组织》，载中国政府网，https://www.gov.cn/yaowen/liebiao/202507/content_7033957.htm，2026 年 2 月 28 日访问。

能发展与合作中心联合多家开源社区共同发布《国际人工智能开源合作倡议》，倡导 AI 技术的开放共享，携手打造“中国主导、金砖协同、全球辐射”的开源开放生态体系。这标志着中国正式举起“开源”大旗，为全球技术民主化迈出重要一步。¹7 月 27 日，由司法部指导，中国政法大学和联合国教科文组织联合主办的 2025 世界人工智能大会“人工智能规则全球对话与协同发展”论坛同时举办，发布了《全球人工智能治理规则地图 2025》，启动了“全球人工智能规则合作研究平台”，深化全球人工智能治理合作。²

2025 年 8 月，国务院发布《关于深入实施“人工智能+”行动的意见》，将“人工智能+”全球合作作为六大重点行动之一，围绕推动人工智能普惠共享、共建人工智能全球治理体系两方面任务，坚持智能向善，把人工智能作为造福人类的国际公共产品。³9 月 8 日，国家发展改革委、国家能源局印发《关于推进“人工智能+”能源高质量发展的实施意见》进一步坚持全球合作理念。这一国内政策与中国在国际上提出的各项 AI 合作倡议形成了完美呼应，体现了中国以中国智慧促全球发展的大国担当。⁴

2025 年 9 月 2 日，在 2025 年上海合作组织峰会期间，中国作为 2024-2025 年轮值主席国，推动通过了《上海合作组织成员国元首理事会关于进一步深化人工智能国际合作的声明》。⁵中国正在与世界各国共同努力推动人工智能在国际范围内向更加开放、包容、普惠、公平、向善的方向发展。

2025 年 9 月 23 日，中国国务院总理李强在纽约联合国总部出席全球发展倡议高级别会议时，强调 AI 必须服务于联合国的 2030 可持续发展目标，反对将技术政治化，并正式提出《“人工智能+”国际合作倡议》，呼吁各国结合自身国情积极推进“人工智能+”行动，彰显中国坚持开放、包容、合作的姿态。⁶

2025 年 11 月 27-28 日，在深圳举办的“2025 大湾区—东盟经济合作（前海）论坛”上，多项具有深远意义的创新产业与人工智能的合作机制相继发布，中国将以更开放的胸怀、

¹ 中国信息通信研究院：《工信部推动中国—金砖国家人工智能发展与合作中心发布〈国际人工智能开源合作倡议〉》，载央视网，<https://gongyi.cctv.com/2025/07/27/ARTIsTVWLBbYFrDFyIqc3QVo250727.shtml>，2026 年 2 月 28 日访问。

² 中国日报：《中国政法大学与联合国教科文组织联合举办 WAIC 2025“人工智能规则全球对话与协同发展”论坛》，载中国日报网，<https://caijing.chinadaily.com.cn/a/202507/27/WS68860634a310028a84abff9c.html>，2026 年 2 月 28 日访问。

³ 国务院：《国务院关于深入实施“人工智能+”行动的意见》，国发〔2025〕11 号，2025 年 8 月 21 日发布。

⁴ 国家发展改革委、国家能源局：《国家发展改革委 国家能源局关于推进“人工智能+”能源高质量发展的实施意见》，国能发科技〔2025〕73 号，2025 年 9 月 4 日发布。

⁵ 新华社：《上海合作组织成员国元首理事会关于进一步深化人工智能国际合作的声明》，载中国政府网，https://www.gov.cn/yaowen/liebiao/202509/content_7038710.htm，2026 年 2 月 28 日访问。

⁶ 外交部：《李强出席全球发展倡议高级别会议》，载外交部官网，https://www.mfa.gov.cn/web/wjdt_674879/gjldrhd_674881/202509/t20250924_11714592.shtml，2026 年 2 月 28 日访问。

更务实的举措，共同开创 AI 国际合作新篇章。¹

总体而言，2025 年中国在 AI 涉外布局方面交出了一份令人瞩目的成绩单。从倡议成立世界人工智能合作组织到推动“人工智能+”国际合作，从深化区域合作到拓展全球伙伴关系，中国以更加自信、开放、包容的姿态参与全球 AI 治理，为构建人类命运共同体贡献了中国智慧和方案。

¹ 人民网：《2025 大湾区—东盟经济合作（前海）论坛成功举行》，载人民网，<https://hm.people.com.cn/n1/2025/1129/c42272-40614064.html>，2026 年 2 月 28 日访问。

第三节 热点聚焦

一、数据出境监管体系基本完善

(一)《个人信息出境认证办法》正式出台

2025年10月，随着《个人信息出境保护认证办法》（简称“认证办法”）的正式出台，并将于2026年1月1日起正式实施，我国的个人信息出境认证路径基本具备了完整、可操作、可监督的制度安排，与安全评估、标准合同备案共同构成了完整的跨境传输合规框架，使我国数据出境监管体系从“制度框架搭建阶段”迈入“机制成熟与规则成型阶段”。这一变化不仅填补了制度空缺，更标志着监管体系开始形成可分级适用、可灵活选择、可动态校准的立体化治理模式。

在认证办法出台之前，我国的跨境数据合规体系中长期存在一个结构性的问题：虽然法律层面确立了安全评估、标准合同备案、认证三类路径，但其中“认证”机制始终缺乏法律法规层面的制度文本，导致企业在实际操作中的选择空间有限，往往只能在前两者之间做出抉择。对于跨国公司、区域性共享服务中心、境内外一体化运营的科技平台而言，动辄覆盖数十个国家、涉及上百项业务流程的跨境数据调用，往往无法完全被标准合同所覆盖，而安全评估的前置性、单点审查性和周期长等特点又难以适配“持续、动态、大规模”的跨境处理需要。因此，企业的合规路径在早年间呈现出“实践复杂、规则单一”的矛盾，监管机构也难以通过有限的工具对复杂跨境场景进行精细化管理。

认证办法的出台正是在这一背景下完成的制度化补位。此次办法不仅明确了认证的适用范围、实施程序、管理责任和监督机制，更与同期发布的国家标准 GB/T46068-2025

《数据安全技术 个人信息跨境处理活动安全认证要求》形成体系化对应，使认证成为能够在实践中落地运行、可供企业主动申请的制度路径。特别是对于跨国企业集团、境外委托处理情形以及长期稳定的跨境业务安排而言，认证路径提供了一种可持续、可预测、可循环适用的合规机制，使跨境数据活动可以借助制度化的治理体系获得持续稳定性。

从制度内容上看，本次认证机制的最大特点在于，它强调对跨境处理活动的“体系化评估”而非“单一行为审查”。认证不是对某一次传输行为进行备案，而是对企业整体个人信息治理能力、跨境处理组织结构、境外接收方安全能力、数据再转移控制、个人权利保障机制等多个维度进行综合判断。这意味着，认证不再仅是跨境行为的许可，而是对企业整个数据治理体系是否能够承载跨境活动的系统性评估。这种制度设计使认证机制适用于大型科技公司、跨国集团总部—子公司体系、区域性数据管理中心，以及需要频繁共享数据的

全球业务协作模式，从而弥补了标准合同难以覆盖“长期、复杂、链路多节点”场景的不足。

此外，认证办法还建立了区别于标准合同的“持续监督机制”。认证证书有效期为三年，但并非“一证三年无监管”，而是要求认证机构对认证后的企业进行周期性的监督审核，并对企业在跨境活动中出现的重大变更进行动态评估。例如，境外接收方新增应用场景、处理目的发生变化、集团数据架构调整等情形均可能触发重新评估甚至暂停认证。这种动态监管机制使认证路径具有“持续校准”的能力，与安全评估的一次性审查、标准合同备案的事后性管理形成互补，更符合跨境数据流动本身的动态特征。

值得注意的是，认证办法将“境外再转移控制”作为关键审查要素之一。境外接收方不得随意将个人信息再次提供给第三国或其他实体，必须有完备的再转移审批和风险控制机制，并接受境内企业与认证机构的协同监督。这一要求在制度逻辑上与欧盟 GDPR 的 BCR 机制高度一致，体现了我国监管体系向国际高标准规则体系靠拢的趋势，对于当前普遍依赖全球统一 IT 架构、跨国风控模型与全球客服资源的企业而言，提供了更加清晰的制度边界。

从监管体系视角来看，认证办法的出台并非单一制度的增加，而是整体治理体系完善的重要一环。随着认证机制的落地，数据出境在我国开始形成豁免及“标准合同、认证、安全评估”多层次、全场景可覆盖的合规体系。企业可以根据数据类型、跨境目的、处理规模、集团架构、境外接收方能力等因素灵活选择路径，监管机构也可以根据风险分类精准施策，实现“高风险强约束、低风险优便利”的资源优化配置。

认证办法的推出，使我国跨境数据治理体系实现了关键性制度完善，既补齐了监管体系的功能，也为企业提供了更加稳定、可控、可预期的跨境合规选项。随着认证机制开始在实践中逐步实施，跨境治理的精细化程度、制度可操作性以及监管的可持续性均将显著提升，我国在全球数字经济体系中的规则制定力和参与度也将在此基础上进一步增强。

（二）跨境合规执法落地：未履行数据出境义务的风险具象化

2025 年，我国在跨境数据监管领域的制度建设与执法实践实现了衔接。一方面，多项数据出境合规机制已实现制度化落地，使企业具备了清晰且可选择的跨境路径；另一方面，监管部门也开始将制度要求转化为实际执法行动，对未按规定履行跨境义务的企业作出明确处理，其中标志性案例即为某国际奢侈品公司发生的个人信息泄露事件，不仅揭示了跨境数据活动的风险点，也为企业合规提出了现实警示。

该公司在中国大陆长期开展高端奢侈品零售业务，其运营过程中会收集大量消费者的姓名、联系方式、消费偏好、预约记录等个人信息。2025 年 5 月，监管部门通报该公司在

境内运营的子公司因个人信息保护措施不到位，发生了涉及大量消费者个人信息的泄露事件。有关部门在调查过程中发现，该公司在将中国境内收集的消费者信息传输至境外总部的过程中，未按照我国法律规定履行数据出境的必要义务，包括但不限于：未开展数据出境安全评估、未签署并备案个人信息出境标准合同、未通过个人信息出境认证、未充分告知消费者境外接收方的处理方式、未取得“单独同意”；以及未对收集的个人信息采取加密、去标识化等安全技术措施。换言之，该事件本质上并非单一的网络安全事故，而是典型的“跨境链路存在系统性合规缺失”所引发的后果。

最终，监管机构依据《网络安全法》《数据安全法》《个人信息保护法》的相关规定，对该公司在华子公司作出行政处罚。该事件清晰传递了一个信号：跨境合规是必须被严格履行的法定义务；不履行跨境合规程序的风险不仅体现在可能的泄露后果，更体现在监管部门对企业整体数据治理体系的整体性审查。首先，该案例表明企业不能以“集团内部调用”“国际通行惯例”等理由免除数据跨境的合规义务。在我国法律框架下，只要发生个人信息从境内向境外提供的事实，就必须按照规定选择相应的合规路径或确认存在豁免情形，且不同路径具有不同的履责重点，任何缺位均可能导致合规力度受到负面影响。其次，即使存在豁免情形，也并不意味着企业无需履行任何合规义务：对收集、跨境传输的个人信息采取去标识化措施、开展因跨境传输个人信息而触发的个人信息保护影响评估仍是企业的法定义务。

该事件也标志着我国跨境数据治理从“建制度”走向“强监管”，监管机构已开始将制度化要求转化为具体执法行动，跨境合规义务已不再停留在纸面；同时，该案例也为国内外企业提供了现实教训：即便企业品牌知名度高、国际业务成熟，若未按我国法律履行跨境合规义务，依旧会被严格追责。随着认证机制、安全评估机制与豁免机制逐步成熟，未来跨境数据监管将更加可预期，也将更注重对企业“实际执行能力”的检验。对企业而言，必须从内部治理、技术能力、境外链路管理等多方面建立起符合我国法律要求的跨境安全体系，否则跨境数据流动的业务便利可能随时转化为法律风险与声誉损害。

二、数据及人工智能系列执法活动持续展开

2025 年，随着个人信息保护与算法治理立法与规范的逐步完善，国家网信办联合工业和信息化部、公安部、市场监管总局等部门在全国范围内持续组织开展了一系列有针对性的执法行动与专项整治，重点聚焦移动应用（含小程序、公众号、快应用）违法违规收集使用个人信息、SDK 违规扩散、信息推荐算法典型问题以及生成式人工智能与深度合成服

务的合规性审查。从总体来看，2025 年的执法节奏呈现出从“发现—通报—责改—问责”到“常态化、制度化治理”的转变：既有大规模的批次检测与通报，也有针对算法治理的专项整治与推动平台自我修正的政策引导，监管治理方式更加立体化、常态化与精细化。

在 APP 及 SDK 领域，中央网信办会同相关部门对移动应用收集使用个人信息的行为进行了系统检测并多次通报典型问题。2025 年的集中通报显示，监管部门依托技术检测与行政协同，对若干流行 App、小程序以及 SDK 的个人信息收集规则、权限调用、用户告知与权利响应机制等方面存在的合规缺陷进行了公开披露，并责令平台采取下架、整改、限期完善功能等处置措施。例如，在 2025 年 5 月的通报中，监管机关点名披露了 15 款存在未准确列出或未充分说明所含 SDK 收集使用个人信息的 App，以及 16 款存在合规缺失的 SDK，要求相关责任主体限期整改并依法依规接受后续监管。¹早在 2 月的另一轮集中处置中，网信办亦依法对若干款存在未依法公开个人信息收集使用规则、未按规定履行主体责任的应用实施了下架和整改要求，显示出对移动端个人信息合规问题的持续高压态势。²

针对算法治理方面，中央网信办继续组织开展“清朗”系列专项行动，将网络平台算法典型问题治理作为 2025 年重点任务之一。专项行动既强调对平台算法在推荐逻辑上可能产生的低俗化、极端化与“信息茧房”效应进行整治，也推动平台在算法透明、用户可控、内容多样性保障等方面采取具体技术与管理改进。监管要求包括公开算法基本规则原理、完善用户兴趣偏好管理与拒绝/屏蔽机制、开展“茧房评估”、探索“一键破茧”等功能，以及优化内容多样性策略；同时，督促重点平台签署行业自律承诺，推动“算法向善”治理意识在行业内落地。此类专项行动侧重从源头与机制端抑制算法带来的舆论风险，并通过约谈、通报、整改乃至行政处罚的手段实现治理闭环。

在生成式人工智能与深度合成服务监管方面，网信办加大了对“深度合成”技术服务提供者的备案与合规检查，重点关注未对深度合成内容作显著标识、未按规定开展安全评估、以及将深度合成功能作为便捷消费工具而忽视合规治理的问题。官方公开的执法案例中，监管部门对若干提供深度合成换脸或配音等服务的 App 做出下架处置，并以相关法律法规点名其未落实技术标识、未建立风险提示与用户权限管控为主要违规事实。这一执法方向

¹中华人民共和国国家互联网信息办公室关于 15 款 App 和 16 款 SDK 个人信息收集使用问题的通报 https://www.cac.gov.cn/2025-05/06/c_1748239411359045.htm，2025 年 12 月 4 日访问。

² 国家网信办依法集中查处一批侵害个人信息权益的违法违规 App https://www.cac.gov.cn/2025-02/19/c_1741664476228611.htm，2025 年 12 月 4 日访问。

表明，生成式 AI 服务的“准入—标识”链条已成为监管关注的常态化内容。¹相较于既有的生成式 AI 监管，最新出台的 AI 拟人化互动服务的监管则更为强调服务提供者对用户的心理健康与情感认知方面的安全保护能力，并拟以具有强制性效力的法规形式明确服务提供者采取必要干预措施的义务，而非企业承担社会责任的自愿性举措。尽管这一政策还仅是征求意见稿，但可以预见的是，未来很有可能针对该领域开展具体的执法行动，以此实现对该类 AI 服务的精准化监管。

总体而言，2025 年中央网信办及有关部门在 APP 执法、SDK 监管、算法治理和生成式人工智能合规等方面持续展开集中行动，既通过公开通报与下架处置清理短板，又通过专项治理与制度建设推动平台自我修复与长效合规机制的形成。对企业而言，2025 年的执法态势强调了合规的系统性要求：技术防护、产品设计、第三方治理与用户权利响应需同步到位；对监管机构而言，未来治理将更侧重于构建风险预警、动态监督与跨部门联动的全链条合规体系，以适应数据与 AI 快速演进带来的复杂监管挑战。

三、数据合规领域多项国家标准细化落地：数据及 AI 监管规则通过系列标准得以明确

多项国家标准在 2025 年密集出台并逐步落地，形成了以“分类分层、风险导向、可操作化”为特征的数据与人工智能合规规则体系。与此前以法律为主、标准为辅的格局相比，2025 年的标准体系体现出更强的技术细化能力和更高的可执行性：既将抽象的法律义务拆解为可测量的技术指标和治理流程，也为监管执法、第三方评估与企业自查提供了统一的衡量尺度，从而在实践中显著提升了合规的透明度与可预测性。

首先，在个人信息与敏感个人信息领域，国家标准 GB/T45574-2025《数据安全技术 敏感个人信息处理安全要求》细化了敏感个人信息的分类示例、处理全生命周期的安全控制点及相应的技术与管理要求，包括但不限于最小必要性原则、强制性加密与去标识化要求、访问控制与审计链路、以及对高风险处理活动的事前评估和事后追溯机制。该标准自 2025 年 11 月 1 日起实施，为企业在界定与处置敏感个人信息时提供了清晰的操作性指引，有助于解决实践中关于“何为敏感信息”“如何保障敏感信息安全”的认定与实施难题。

其次，在数据跨境与个人信息出境合规方面，配合此前出台的法律法规，国家标准层面推出了面向个人信息跨境处理活动的认证与技术要求文件，为监管部门、认证机构与企业提供了统一的评估框架。GB/T46068-2025《数据安全技术 个人信息跨境处理活动安全认

¹ 国家网信办发布近期网络安全、数据安全、个人信息保护相关执法典型案例
https://www.cac.gov.cn/2025-09/16/c_1759741437315419.htm, 2025 年 12 月 4 日访问。

证要求》明确了跨境处理活动应遵循的基本原则、评估维度与认证技术指标，并对境外接收方能力审查、再转移控制、个人权益保障等关键点给出具体化要求。该标准的发布为个人信息出境认证机制提供了国家层面的技术参照，推动认证从政策设想向可操作的合规工具转化。

再次，在人工智能与生成式内容治理方面，中央网信办、工信部等部门围绕“标识、透明、责任”三大原则，出台并推动实施了人工智能生成内容（AIGC）标识方法与管理办法的配套标准。国家标准 GB45438-2025《网络安全技术 人工智能生成合成内容标识方法》对生成内容的显著标识方式、可追溯的元数据格式、服务提供者的标识义务以及与用户提示机制的技术实现路径进行了规范，且自 2025 年 9 月 1 日实施后，成为监管深度合成、换脸、语音合成等敏感场景的重要技术依据。国家关于 AIGC 的管理办法同时要求服务提供者在用户界面、下载保存等关键触点主动标注生成内容来源与可疑风险提示，形成了“产品设计—使用提示—监管留痕”的合规链条。更宏观地看，2025 年国家在人工智能领域推动的标准化呈现出“多层次覆盖、应用导向强、治理工具化”的特点。一方面，国家标准体系不再仅停留于基础算法或模型性能的评估，而是扩展到模型可解释性、可审计性、数据集治理、偏见评估、多模态融合风险等治理要素；另一方面，标准化的推进与监管政策形成了相互促进的格局：标准为监管提供具体可检的技术指标，而监管实践又反过来推动标准的修订与细化。国家层面已发布与拟定的人工智能国家标准数量显著增长，覆盖从基础软硬件到行业应用与安全治理的完整链条，这一态势表明国家正在以标准化为抓手，引导产业在合规轨道上实现规模化应用。

最后，在标准对企业实践的直接影响方面，三类典型变化尤为显著。其一，在产品设计与上线阶段，企业必须将合规嵌入到模型训练数据治理、隐私保护设计、以及生成内容的标识与用户提示机制中，监管不再仅在事后“找问题”，而是通过标准要求企业在事前建立可追溯的治理链条。其二，第三方服务生态（包括数据供应商、模型托管方、算法推荐平台、SDK 提供商等）须承担更明确的合规责任，标准明确了第三方能力评估、合同条款与再转移限制的技术要求，从而推动产业链上下游的合规分工与风险隔离。其三，监管与认证机构获得了可落地的评价工具，诸如敏感信息处理安全基线、AIGC 标识检测流程、跨境处理认证条目等，均可用于监督检查、合规审计与行政执法，从而提高了执法的操作性和判定的可重复性。

总体而言，2025 年国家标准在数据安全、敏感个人信息处理、个人信息出境认证和人工智能生成内容标识等关键领域的密集出台，为数据与 AI 的合规治理提供了技术化、程

序化的支撑。这些标准既为企业合规提供了操作指引，也为监管执法提供了可执行的审查维度，从而在制度层面推动了“从规则到实施”的跃迁。未来，随着标准的持续完善与产业实践的累积，数据与人工智能治理有望在更高的确定性与透明度下与创新发展并行。

四、数据产权登记制度逐步建立

（一）数据产权制度建设火热开展

近年来，随着数据成为数字经济时代的关键生产要素，我国在“数据产权”制度构建上的探索不断加深。2025 年，伴随监管部门与地方政府推动、标准制度不断完善，数据产权登记制度开始从试点探索迈向全国推广，并在制度设计、法律承认、司法实践与市场应用等方面取得显著进展，标志着数据要素市场化与规范化基础制度正在稳步落地。

“数据产权登记”制度，顾名思义，是指将数据资源或数据产品的权利状况通过登记系统予以确认和记载，并对权利归属、权利内容、权利流转及交易使用等予以制度化管理的一种机制，其建设对推动数据资源合法合规流通、激发数据要素价值、促进数据资产交易、维护数据权利主体合法权益具有基础性作用。

2025 年，制度落地的进展首先体现在我国官方机构对“数据产权制度”的系统规划与制度设计进程中。在 2025 年 8 月召开的全国“十四五”规划收官之际，国家数据局局长公开表示，今年将推出“数据产权”等十多项制度，以完善数据基础制度体系。这一表态，意味着国家层面对“数据产权”制度的重视已上升为战略部署，并将通过制度化手段推动数据要素的市场化配置与规范流动。

具体来说，数据产权登记制度应当包括以下几个关键环节：首先，对“权利客体”的界定，即明确什么样的数据 / 数据集 / 数据产品可以作为登记对象——这既可能涵盖采集生成数据、清洗加工后的数据，也可能涵盖以数据为基础的“数据服务产品”或“数据资产包”；其次，对“权利主体”的认定与登记：即谁对该数据资源享有权利（原始采集者、加工者、平台运营者、数据交易机构等）；再者，对“权利内容与权利边界”的确认，包括持有权、使用权、交易权、收益分配权等；最后，对“权利限制与公共利益保障机制”的制度设计——在尊重数据产权性质的同时，必须兼顾个人隐私、安全、公共利益与行业规范。学界强调，这样的登记制度为构建公平、有序、透明、可监督的数据交易与数据治理体系奠定制度基础。

（二）数据产权制度落地的预期法律效果有待观察

一方面，数据产权登记将可能成为数据资产入表和流通交易的“软门槛”。数据产权登

记与数据资产入表、流通交易的逻辑衔接和规范关系，将在未来的数据资产保护相关制度文件中得以厘清和强调。从目前来看，事实上数据产权登记凭证可能并不具有强制性法律效力，也即，即便是未申请产权登记的数据资产或数据产品，也依然可成为企业资产负债所厘定的范围，并进入数据要素流通市场进行自由交易。但可以预见的是，未经产权登记的数据资产将在数据资产价值链的实现环节付出相同乃至更多的自证成本以说明数据权属的明确性和合法性。

另一方面，数据产权登记在司法判决中的效力仍有待实践检验。数据产权登记与数据知识产权登记类似，与前者目前主要作为权利人享有合法数据权利的重要手段不同，数据知识产权登记目前已初步具备行政执法和司法裁判活动中的“准证据”效力。2024年8月26日，北京互联网法院发布的“服务保障新质生产力十大典型案例”中，全国首个涉《数据知识产权登记证》效力认定案备受关注。在该案中，法院首次在司法裁判中确认《数据知识产权登记证》对数据持有的证明效力，即数据知识产权登记可以作为原告享有数据财产权益的初步证据，也可以作为其数据收集行为或数据合法性来源的初步证据。然而，数据产权登记和数据知识产权登记的关系，尚且不明。有观点认为，数据知识产权登记是数据产权制度的一个分支。

除了登记机制本身的发展，伴随着制度设计与司法实践，数据资源、数据资产的交易与流通也正逐步活跃。国家数据局在2025年推动包括公共数据资源授权运营机制、数据基础设施建设、数据交易机构互认互通、数据产品需求目录发布等一系列配套措施，意在为数据产权制度提供基础设施与市场支撑。

总体而言，2025年我国数据产权登记制度正在从政策倡导与理论探索，迈入制度设计、地方试点、司法认可与市场实践的综合阶段。其主要进展与特征可以总结如下：一是国家层面将数据产权纳入基础制度体系，并明确发展路径与政策推进节奏；二是多地试点落地，形成不同地区可操作的登记办法，为全国推广积累经验；三是司法实践开始承认登记证书的法律效力，为权利保护、交易担保与纠纷解决提供参考；四是交易机制、基础设施、市场配套同步推进，为数据要素市场建设奠定制度与技术基础；五是与此同时，也存在登记标准不统一、跨域适用难、权利与公共利益平衡复杂等制度性挑战。

第四节 展望与建议

一、立足本国国情，结合最新国际经验，适时制定完善的 AI 监管体系

2024 年 8 月 1 日，欧盟《人工智能法案》分阶段生效：AI 的一般条款及禁止的 AI 实践已于 2025 年 2 月 2 日生效；通用 AI 模型治理相关条款、各国通知机构等条款于 2025 年 8 月 2 日生效。然而，欧盟委员会在审查《人工智能法案》的执行准备情况时发现各成员国在指定国家主管机构和符合性评估机构方面的进展迟缓。同时，在高风险 AI 系统合规条款将生效的现阶段，市场上普遍缺乏针对《人工智能法案》高风险要求的统一标准、明确指南及合规工具，委员会认为此类延误可能导致企业和公共部门的合规成本显著增加，不利于法案规则的具体落地，因此有必要在《人工智能法案》正式实施前进行结构性“微调”。

在此背景下，2025 年 11 月，欧盟委员会发布了《关于简化人工智能法案规则》的提案（以下简称“该提案”）。该提案旨在对《人工智能法案》进行技术性修订，核心目的是简化其实施，减轻企业（尤其是中小企业）的合规负担，同时确保监管的有效性。修改核心包括：移除企业确保自身员工具备 AI 素养的普遍性义务，转而要求欧盟委员会和成员国承担鼓励和促进员工 AI 素养发展的责任；加入“小型中间市值企业”（SMC）定义，拓宽可使用简化规则的企业范围；顺延高风险 AI 系统相关规则的生效时间，并重点提出相关规则需在可落地、可执行的配套执行规则例如协调标准等出台后的一定期间内方可生效。

现阶段，中国 AI 治理已形成“发展—应用—安全—治理”同向发力的清晰路径，并确立了“包容审慎、分类分级”的核心原则，也将立法与标准建设作为保证“人工智能+”可持续落地的重要制度保障。¹立足中国数据及 AI 治理的当前实践，结合欧盟《人工智能法案》的简化思路，未来可考虑从以下方面制定和优化我国现有 AI 监管规则：

（一）构建符合技术发展逻辑的 AI 监管体系

在 AI 领域，我国始终坚持以实际风险为导向的“小切口法”，及时针对算法及 AI 应用事件频发的算法推荐领域、深度合成领域以及生成式人工智能领域发布部门规章，通过“敏捷治理”的方式对具体算法及 AI 应用的具体领域进行初步治理，并逐步制定《人工

¹ 张凌寒：《筑牢深入推进“人工智能+”行动的政策制度之基》，载中华人民共和国国家发展和改革委员会政策解读，https://www.ndrc.gov.cn/xxgk/jd/jd/202508/t20250828_1400103.html，2026 年 2 月 28 日访问。

智能生成合成内容标识办法》等专门规定，以进一步落实前期 AI 监管体系建立的初步合规义务并为相关适格义务主体提供具体操作指引。在此基础上，我国也将建立统一的人工智能法纳入立法计划，不仅在党的二十届三中全会通过的《中共中央关于进一步全面深化改革 推进中国式现代化的决定》中提出完善生成式人工智能发展和管理机制、建立人工智能安全监管制度的整体要求，将人工智能法明确列入国务院的立法计划之中，实践中也已出现了《人工智能示范法 1.0》《人工智能示范法 2.0（专家建议稿）》等学者、专家版，其中可窥见我国部分 AI 监管治理思路。

然而，在我国暂未发布正式的人工智能法草案的现阶段，欧盟对已部分生效的 AI 法案进行大幅修订，其修订思路清晰地标志着欧盟从“规则刚性”到“系统性适应”的转变，且这种转变的核心在于，欧盟的立法者已深刻地认识到，面对 AI 这类快速更迭、边界模糊的数字技术，试图通过一部法律预先设定所有技术细节和合规路径，不仅是低效的，更可能因规则脱离技术现实而扼杀创新或引发系统性合规危机。这一转变为我国的 AI 治理提供了关键的镜鉴。通常而言，立法者可能期待建立“一步到位”、兼具完备性和稳定性的监管体系，然而如何确保监管体系能够具备应对未知技术的灵活性、如何建立一个能够自我调整并与技术发展同步演进的适应性监管系统成为了当前 AI 领域的立法难题。究其根本，在 AI 等具有超强技术迭代性的创新领域，技术的未知性远大于确定性，过于追求立法的早期完备性，可能带来双重风险：一是规则可能基于对技术路径的当前现状及未来想象，加之立法需要较长的程序，从而在颁布时即已滞后，或锁定了发展路径；二是为应对所有可能性而制定的冗杂、刚性的义务（例如欧盟 AI 法案的第一版草案）可能会加剧企业的合规成本与不确定性，最终扼制创新的活力，且相关规则落实本身也可能变为不现实。

因此，欧盟的“适应性转向”启示我们，在面对高度不确定的技术前沿时，立法的智慧或许不在于“筑高墙”式的过早详尽规定，而在于“划跑道、设路标”，即优先建立明确的风险分类、治理原则和权责框架，同时为具体技术标准的形成、监管工具的试错，以及规则的动态更新预留制度接口，从而实现发展与规范在动态过程中的平衡。

（二）在“保安全”的前提下平衡中小企业的 AI 合规负担

无论是 GDPR 还是欧盟 AI 法案的简化提案，均放宽了企业适用豁免措施的范围，例如最新的 AI 法案修改草案将中小企业全部合规优惠扩展至“小中型企业”，即扩大到包含员工大于 250 且小于 500 人（原为 250 人以下），或者年营业额不超过 5 亿欧元（原为 5000 万欧元），或者资产负债表总额不超过 4.3 亿欧元（原为 4300 万欧元）的企业。

因此，更多的中小型企业亦可以享受包括在高风险 AI 合规时适用简化的文档管理、质量管理要求，以及违规罚款计算时的减轻系数等简化措施。

我国也有类似的视企业规模制定合规要求的情形，例如，《个人信息保护合规审计管理办法》第 4 条规定，处理超过 1000 万个人信息的个人信息处理，应当每两年至少开展一次个人信息保护合规审计。同时，该办法第 12 条规定，要求处理个人信息达到 100 万人的个人信息处理者必须指定个人信息保护负责人，并负责个人信息保护的年度合规审计。另外，2025 年 11 月刚发布的《大型网络平台个人信息保护规定（征求意见稿）》也对“大型网络平台”的服务提供者（认定因素包括：注册用户 5000 万以上或月活跃用户 1000 万以上；提供重要网络服务或业务类型复杂；数据安全影响重大等）提出了特殊的信息保护要求。

然而，这并非代表中国在 AI 监管方面必须完全参照或移植欧盟的“规模豁免”路径。其审慎性源于两点现实考量：其一，在 AI 乃至整体数字经济领域，企业的数据处理规模与其人员、资产规模时常脱钩。典型的轻资产型企业，如某些程序化广告技术公司，其人员规模可能符合“中小”甚至“小微”标准，但实际处理、流转的个人信息数量与敏感度却极为庞大。例如，央视 2025 年“3·15”晚会曾曝光的“精准获客”软件产业，该产业中的公司声称他们研发的大数据获客软件，可为商家精准获取目标人群的消费习惯、手机号码等联系方式，方便商家拨打电话推广自己的业务和产品。根据公开的企业信息，多数被点名的企业均属于小微企业或科技型中小企业，然而其获取的数据量极为庞大，部分公司据称拥有 20 亿条精准人群画像，甚至号称每日处理数据量达 100 亿条数据。因此，若机械地依据人员或营业额指标给予其核心合规义务的宽免，可能诱发监管盲区，增加系统性数据安全风险。其二，基于品牌声誉维护、用户信任构建及资本市场预期等多重因素，中国的大型企业或知名企业的主动合规意愿与投入能力往往较高，往往拥有针对合规的专项资金、专业团队（法务、合规、安全）和成熟的内部合规体系。此外，在 2025 年 8 月，阿里巴巴、百度、腾讯、华为等 18 家我国行业领军企业更是联合签署《人工智能安全承诺》，共同发布并主动披露安全实践发布 AI 安全承诺书等合规行动转化为新的“信任状”与市场壁垒。与之相对，部分小型企业反而因生存压力、成本考量、侥幸心理，加之对繁杂而专业的监管要求认知不足，其合规问题识别能力较差、合规动力更是相对薄弱，更可能游走于规则边缘。

因此，在 AI 监管方面，如需考虑不同规模主体的差异化合规要求，应审慎权衡，更应聚焦于其业务活动本身的数据处理量级、风险性质以及对个人权益的实际影响程度，因

地制宜地设计豁免或延期履行条款（例如，可延期履行的或是某些程序性、文档类义务，而对于涉及 AI 安全底线或算法透明度的核心义务，则不宜简单因规模而豁免），而非完全照搬以企业规模为核心的豁免框架。

二、个人信息识别标准变革的审慎方案

2025 年 11 月，欧盟委员会公布了一项全面修订 GDPR 的提案，提案拟对个人数据（即中国《个人信息保护法》项下的个人信息）进行再定义：信息只有在相关实体能够使用其自身手段合理识别数据主体的情况下，才会被视为个人数据。该提案改变了此前 GDPR 的客观识别立场，转向“主观判断标准”——如果某一特定公司无法识别数据主体，则该数据对该公司而言不属于“个人数据”。如该修订实际通过，则将大幅度限缩个人数据的范畴，为数据驱动下商业模式带来更多的可能性，但也将导致 GDPR 的规则在许多情况下不再适用。例如，一家广告科技公司收到经过哈希处理的电子邮件地址后无法对其自行解析并识别至个人，即使其合作伙伴可以，该公司也可辩称这些数据对其而言不是个人数据。这可能会在某些情况下显著缩小数据保护的范围，为数据驱动的商业模式在更少的监管审查下运作提供了更大空间。

我国《个人信息保护法》定义个人信息为“以电子或其他方式记录的与已识别或者可识别的自然人有关的各种信息”，并明确采纳了“匿名化”概念将其排除在个人信息范围之外，这与既有 GDPR 的立法精神一致。然而，中国实践中对于个人信息匿名化的标准莫衷一是，对个人信息采取何种技术处理才能主张匿名化缺乏统一、有效的执行规则，业务侧与法务侧也可能据此产生分歧，对企业的数据流通效率可能产生负面影响。尽管我国陆续发布《个人信息保护 个人信息去标识化指南（征求意见稿）》《个人信息保护 个人信息匿名化指南（征求意见稿）》《数据安全技术 个人信息匿名化处理指南及评价方法》，但相关规则目前基本仅为征求意见稿，即使正式发布也仅是推荐性国家标准，而非正式的法律法规，其认可度与影响力较之 GDPR 拟从法律层面修改个人信息的识别标准也存在较大差距。目前，我国已有司法案例对个人信息的识别标准进行裁判：在北京互联网法院裁判的夏某诉北京某电子公司网络服务合同纠纷案中，原告要求作为个人信息处理者的被告披露特定时段内获取个人信息的访问记录。法院认为，企业已对相关访问记录中涉及的用户身份证号码等个人信息的展示采取了内容替换、SHA256 等脱敏、加密技术，访问者难以识别该身份证号码属于原告；另一方面，相关访问记录也不具备关联特征，不是本案原告在其活动中产生的信息。因此，个人信息处理者对个人信息的访问记录无论是从识别还是关联角度来看，

难以被定义为个人信息，仅为被告企业的内部管理信息。尽管中国并非判例法国家，但既有司法判决中有关个人信息识别的论述，仍能在识别与匿名化标准保持现状的情况下为相关企业提供指引。

因此，在对实践中个人信息识别态度及匿名化操作进行充分调研的基础上，如有必要，可在观察欧盟 GDPR 后续对个人信息识别标准的修改态度后，谨慎评估考虑是否需因地制宜修订或完善我国的个人信息识别及匿名化标准，在对个人信息进行保护的同时最大程度发挥非个人信息的能动性。但需注意的是，尽管欧盟简化提案引入的“主观判断标准”为识别个人信息提供了一种新思路，但由于其对个人信息将带来根本上的影响，直接影响企业在特定情况下是否应遵守个人信息保护规则，因此对识别标准的更新应进行充分、谨慎地全面评估；在欧盟仅提出简化提案、缺乏实践经验检验的现阶段，不宜过早跟随。较之直接对个人信息识别标准进行修改，为促进数据流动和合规商业化利用，在确保当前个人信息保护法律体系稳固实施的前提下关注欧盟提案最终结果的同时，可考虑尽快构建、完善我国的个人信息匿名化体系，通过确立匿名化标准划分个人信息和非个人信息的边界。

三、完善网络生态治理中国特色社会体系

2025 年 11 月 28 日，二十届中央政治局第二十三次集体学习，主题聚焦加强网络生态治理。习近平总书记开宗明义：“网络生态治理是网络强国建设的重要任务，事关国家发展和安全，事关人民群众切身利益”。¹该体系以一套核心原则为引领，通过特定的治理机制，构建了一个立体化的综合治理框架，其中特别提及“促使网络平台、自媒体和多频道网络机构‘担负社会责任’……‘责任层层压实’”以及“大力弘扬社会主义核心价值观，推出更多有内涵、有温度、有影响的网络作品”。

目前，我国已通过压实大型网络平台的个人信息保护责任等方式推动网络平台担负更多的社会责任。例如，国家网信办与公安部联合发布《大型网络平台个人信息保护规定（征求意见稿）》、单独发布《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》，前者要求注册用户达 5000 万以上或者月活跃用户 1000 万以上、提供重要网络服务或者经营范围涵盖多个类型业务等的大型网络平台明确个人信息保护负责人及个人信息保护机构并开展相应个人信息保护工作，后者对大型网络平台设立、运行个人信息保护监督委员会提出了具体的执行细则，例如个人信息保护监督委员会成员人数应与大型网络平台

¹ 《网络生态治理是网络强国建设的重要任务，事关国家发展和安全，事关人民群众切身利益》，载中华人民共和国国家互联网信息办公室，https://www.cac.gov.cn/2025-11/29/c_1766155754164858.htm，2026 年 2 月 28 日访问。

业务规模、用户数量等相匹配，一般不少于 7 人，外部成员占比不低于三分之二。健康的网络生态环境绝非监管部门单一作用即可实现，上述征求意见稿均旨在强化大型网络平台的个人信息保护职责，确保涉及复杂业务、海量用户规模的网络平台能够形成内驱的个人信息保护体系，维护良好的个人信息保护网络环境。未来，在既有立法基础上，宜进一步提出大型网络平台的具体目录，明确“提供重要网络服务或者经营范围涵盖多个类型业务”的范畴，压实网络平台主体责任。内容治理是网络生态治理的重要一环，网信办发布《网络信息内容生态治理规定》，详细列举禁止、防范和抵制生成的具体违法与不良信息类型，旨在构建“清朗”的网络空间。在此基础上，《互联网信息服务深度合成管理规定》和《生成式人工智能服务管理暂行办法》均强调了服务提供者的信息发布审核、不得生成虚假有害信息等法律、行政法规禁止内容的内容审核义务，并在《生成式人工智能服务管理暂行办法》中进一步强调了发现违法内容时的处置措施，包括但不限于停止生成、停止传输等。2025 年，相关部门也已在专项监管行动中加强对内容审核的监管力度。例如，2025 年，中央网信办持续开展“清朗·网络平台算法典型问题治理”专项行动，要求相关平台不断健全推荐内容审核机制，加强正能量内容推送，防范算法推荐低俗不良信息；严禁低俗恶俗等典型不良信息进入推荐领域；同时，网信办同年召开专项整治 AI 技术滥用的行动，并计划在专项行动的第二阶段聚焦利用 AI 制作发布谣言、不实信息、色情低俗内容等突出问题，集中清理相关违法不良信息。

面对技术浪潮，治理需保持开放心态以利用技术红利，同时坚持自主可控以确保安全发展。目标是化“变量”为“增量”；鼓励支持新技术发展与应用，同时确保其安全、可控，为我所用，使互联网成为事业发展的助推器。因此，在未来，宜合理利用《人工智能生成合成内容标识办法》等手段，对技术浪潮引发的各类信息进行来源追溯，并通过模型训练、内容过滤等方式将违法与不良信息扼杀在源头。此外，网络空间的攻击层出不穷，企业除了语料选择等自我防范机制，还应积极采取有效的外部技术管控措施，抵御外部攻击，尽可能降低因外部攻击引发的内容风险，或将内容安全事件造成的影响降低至最小范围，维护清朗的网络空间。

【版权声明】

《中国涉外法治发展报告（2025）》对外经济贸易大学版权所有，侵权必究。未经版权方正式书面许可，任何单位及个人不得擅自转载、摘抄、改编、汇编、商用传播或以其他方式使用本报告全部或部分内容。合法转载须完整标注原文出处与来源信息，严禁篡改内容、

隐匿来源。凡违反本声明擅自侵权使用的，我方将依法追究其全部法律责任。

如需规范引用本报告内容，请统一采用以下标准格式：

梅夏英、许可、吴涵：第二章，对外经济贸易大学涉外法治研究院、法学院编《中国涉外法治报告（2025）》

<https://law.uibe.edu.cn/zt/2025xfzczzt/69bfb14dd64840a8a33b543b84b8145a.htm>