生成式人工智能时代个人信息保护的困境与路径

李波

沈阳工业大学文法学院，辽宁沈阳，110870；

摘要：随着生成式人工智能技术的快速迭代与广泛应用，个人信息的收集、处理、利用模式发生根本性变革，既催生了数据要素的价值释放，也对传统个人信息保护法律体系提出严峻挑战，面临权利边界模糊、责任认定困难、监管机制滞后等法学困境。本文通过剖析现行法律规范的适用局限，借鉴国内外先进经验，从权利体系完善、责任机制重构、监管模式创新三个维度，提出契合我国法治语境的完善路径，为数字时代个人信息保护提供法学理论支撑与实践指引，助力数字经济与法治建设协同发展。

关键词：生成式人工智能；个人信息保护；法学困境；责任认定；监管创新

DOI：10.69979/3029-2700.26.04.081

1 生成式人工智能场景下个人信息保护的核心法律界定

数字经济时代，个人信息已成为核心生产要素，其合理利用是法治建设的重要课题。当前，生成式人工智能技术广泛应用于各领域，个人信息的收集、处理、利用模式发生深刻变革，既推动了数据要素价值释放，也引发了一系列新型个人信息侵权问题，对我国现行个人信息保护法律体系提出新的挑战。

1.1 生成式人工智能场景下个人信息的范围界定

根据《个人信息保护法》第 4 条规定，个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。在生成式人工智能应用场景中，个人信息的范围呈现出“传统信息+衍生信息”的双重特征，既包括技术应用中直接抓取的自然人姓名、身份证号、联系方式等原始个人信息，也包括通过算法分析生成的衍生信息，如用户偏好、行为轨迹、信用评估等。

与传统场景相比，生成式人工智能应用中的个人信息具有两个显著特点：一是关联性更强，技术通过多维度数据整合，能够将分散的个人信息关联形成完整的个人画像，甚至实现“可识别性”的间接关联，例如通过用户的浏览记录、消费习惯等信息，精准识别出具体自然人；二是虚拟性突出，技术可基于原始个人信息生成虚拟个人信息，此类信息虽非直接来源于自然人，但与自然人具有高度关联性，一旦被滥用，仍会侵害自然人的人格权益与财产权益。

1.2 生成式人工智能场景下个人信息处理的法律特征

生成式人工智能场景下的个人信息处理，涵盖收集、存储、使用、加工、传输、提供、公开、删除等全流程，与传统个人信息处理相比，具有以下法律特征：其一，处理主体多元化，既包括技术研发者、使用者，也包括提供数据支撑的第三方平台，多主体参与导致责任划分难度加大；其二，处理行为自动化，技术通过算法自动完成个人信息的抓取、分析与生成，无需人工干预，使得侵权行为更具隐蔽性，难以被发现与追责；其三，处理目的泛化，个人信息处理的目的不仅包括提供服务、优化产品，还包括内容生成、商业推广等，部分处理行为超出用户预期，违背“目的明确”原则；其四，权利义务失衡，技术研发者与使用者凭借技术优势，掌握大量个人信息，而个人信息主体处于弱势地位，难以行使知情权、决定权等权利，形成不对等关系。

2 生成式人工智能时代个人信息保护的困境

2.1 权利体系不完善

我国现行法律虽明确了个人信息主体的知情权、决定权、查阅权、复制权、删除权等权利，但在生成式人工智能场景下，这些权利的实现面临诸多障碍，权利体系的不完善问题日益凸显。一方面，知情权流于形式，相关技术的算法具有黑箱性，个人信息主体难以知晓个人信息被抓取、处理的具体范围、方式与目的，即使平台提供了隐私政策，也多为冗长、晦涩的格式条款，用户难以全面理解，导致“知情同意”原则沦为形式化工

具，与“选择同意原则”的立法初衷相悖。

另一方面，权利行使缺乏有效保障，个人信息主体难以对个人信息处理行为进行有效监督与干预。例如，当相关技术生成虚假个人信息、滥用个人信息时，个人信息主体难以证明自身权益受到侵害，也难以要求相关责任主体删除信息、承担侵权责任；此外，该场景下的个人信息多为多主体共同处理，当权益受到侵害时，个人信息主体难以确定责任主体，导致权利救济陷入困境。同时，现行法律未明确个人信息主体的算法知情权、算法解释权，个人信息主体无法知晓算法的运行逻辑，难以判断算法是否存在歧视、滥用个人信息的情况，进一步加剧了权利实现的难度。

2.2 追责机制不健全

生成式人工智能场景下，个人信息处理的多主体参与、行为自动化等特征，导致侵权责任认定面临“主体难确定、因果关系难证明、责任难划分”的困境。责任主体界定模糊，技术研发者、使用者、数据提供方、平台运营者等多主体共同参与个人信息处理，各主体的权利义务边界不清晰，当发生个人信息侵权行为时，难以确定具体的责任承担者。例如，技术研发者提供算法技术，使用者利用该技术抓取、处理个人信息，平台提供数据支撑，一旦发生信息泄露，各主体相互推诿，导致追责无门。同时因果关系证明困难，相关技术的算法具有黑箱性，个人信息侵权行为具有隐蔽性、间接性，个人信息主体难以证明自身权益受到侵害与个人信息处理行为之间存在直接因果关系。例如，技术通过算法分析个人信息生成虚假内容，导致个人名誉受损，个人信息主体难以证明虚假内容的生成与自身个人信息被滥用之间存在因果关系，也难以举证证明算法运行存在过错。

2.3 监管机制滞后

我国现行个人信息保护监管机制以政府监管为主，辅以行业自律与社会监督，但在生成式人工智能场景下，该监管机制呈现出明显的滞后性，难以适应技术快速发展的需求。首先，监管主体不明确，相关技术涉及多个行业、多个领域，目前我国尚未明确专门的监管主体，各监管部门之间的职责划分不清晰，存在监管重叠、监管空白等问题，导致部分个人信息处理行为处于无人监管的状态。现行监管方式以事后监管为主，缺乏事前预防与事中控制机制，难以防范相关技术带来的个人信息安全风险。相关技术迭代速度快，侵权行为具有隐蔽性、突发性，事后监管往往难以挽回损失，也难以形成有效的震慑作用；此外，监管技术落后，面对算法的黑箱性，监管部门难以对个人信息处理行为进行有效监测与监管，无法及时发现算法滥用、信息泄露等问题。

3 生成式人工智能时代个人信息保护的完善路径

3.1 完善权利体系

针对生成式人工智能场景下个人信息主体权利实现困难的问题，需进一步完善个人信息权利体系，明确权利内容与行使方式，为权利实现提供法律保障。细化知情权与同意权的规定，要求技术研发者、使用者在处理个人信息前，以清晰、明确、易懂的方式，向个人信息主体告知个人信息处理的范围、方式、目的、算法逻辑等内容，避免使用晦涩的格式条款；同时，建立动态同意机制，允许个人信息主体根据自身需求，随时变更、撤回同意，确保同意权的真正实现，落实“选择同意原则”与“公开透明原则”。

同时，增设算法知情权与算法解释权，明确个人信息主体有权知晓算法的运行逻辑、决策依据、数据来源等内容，技术研发者、使用者有义务向个人信息主体作出清晰、易懂的解释，尤其是当算法决策对个人信息主体的权益产生重大影响时，必须提供充分的解释说明，打破算法黑箱。此外，完善个人信息主体的删除权、更正权，明确当个人信息处理行为违反法律规定、超出同意范围，或者个人信息主体撤回同意时，相关责任主体必须及时删除、更正相关个人信息，确保个人信息主体对自身信息的控制权。

3.2 明确责任划分与追责路径

针对生成式人工智能场景下责任认定模糊、追责机制不健全的问题，需重构个人信息侵权责任机制，明确责任主体、责任划分标准与追责路径，确保侵权行为能够得到有效追责。首先，明确责任主体的范围与权利义务，将技术研发者、使用者、数据提供方、平台运营者等均纳入责任主体范围，明确各主体的责任边界：技术研发者对算法的安全性、合法性负责，需对算法进行安全检测与风险评估，防范算法滥用带来的个人信息安全风险；技术使用者对个人信息的处理行为负责，需严格

按照法律规定与同意范围处理个人信息，不得滥用个人信息；数据提供方需确保提供的个人信息真实、合法、有效，不得提供虚假、非法的个人信息；平台运营者需履行监管义务，对平台内个人信息处理行为进行监督，及时制止侵权行为。

其次，明确责任划分标准与承担方式，针对不同的侵权情形，制定不同的责任划分规则：若因算法缺陷导致侵权，由技术研发者承担主要责任，使用者承担次要责任；若因使用者滥用技术导致侵权，由使用者承担全部责任；若多主体共同侵权，按照各自的过错程度承担连带责任。同时，扩大惩罚性赔偿的适用范围，对故意滥用技术侵害个人信息、造成严重后果的行为，依法适用惩罚性赔偿，提高侵权成本，形成有效震慑；此外，明确技术生成虚假个人信息的法律责任，对故意生成虚假个人信息、侵害他人权益的，依法追究相关主体的民事责任、行政责任，情节严重的，追究刑事责任。

3.3 创新监管模式

针对生成式人工智能场景下监管机制滞后的问题，需创新监管模式，构建“政府监管+行业自律+社会监督+技术监管”的多元协同监管体系，提升监管效能，适应技术发展的需求。应明确监管主体与职责划分，设立专门的监管机构，统筹协调该场景下的个人信息保护监管工作，明确各监管部门的职责，避免监管重叠与监管空白；同时，建立跨部门监管协作机制，加强各监管部门之间的沟通协作，实现信息共享、联合执法，提高监管效率。并构建“事前预防—事中控制—事后追责”的全链条监管机制。事前预防方面，建立算法备案制度与安全评估制度，要求技术研发者在推出相关产品前，将算法模型、数据来源、个人信息处理方案等向监管部门备案，并进行安全评估，不符合个人信息保护要求的，不得推出使用；事中控制方面，运用大数据、人工智能等技术，构建智能化监管平台，对个人信息处理行为进行实时监测，及时发现算法滥用、信息泄露等问题，采取约谈、责令整改等措施，防范风险扩大；事后追责方面，加大对侵权行为的处罚力度，对违反个人信息保护法律规定的主体，依法处以罚款、吊销营业执照等行政处罚，情节严重的，追究刑事责任。

4 结论

生成式人工智能技术的快速发展，为数字经济的发展注入了新的活力，但也对个人信息保护的法律体系提出了严峻挑战。要破解这些法学困境，需立足生成式人工智能的技术特征，结合我国的法治实践与学术研究成果，从完善权利体系、重构责任机制、创新监管模式三个维度，构建契合我国国情的个人信息保护法律体系。通过细化个人信息主体的权利内容、明确责任主体的边界与责任划分、构建多元协同监管体系、能够有效防范相关技术带来的个人信息安全风险，保障个人信息主体的合法权益，同时为技术创新发展预留合理空间，实现个人权益保护与数字产业发展的平衡，助力数字中国建设的法治化进程。

参考文献

[1]王利明.和而不同:隐私权与个人信息的规则界分和适用[J].法学评论,2021,39(02):15-24.

[2]张新宝.论个人信息权益的构造[J].中外法学,2021,33(05):1144-1166.

[3]顾云辉.个人信息民法保护研究[J].合作经济与科技,2025,(14):182-184.

[4]周汉华.平行还是交叉个人信息保护与隐私权的关系[J].中外法学,2021,33(05):1167-1187.

[5]高富平.同意≠授权——个人信息处理的核心问题辨析[J].探索与争鸣,2021,(04):87-94+178.