 DOI: https://doi.org/10.12345/bdai.v6i5.32055

The Impact of Generative Artificial Intelligence on Personal Information and Countermeasures

Huaxuanshuo Wang

School of Law, Lanzhou University of Technology, Lanzhou, Gansu, 730050, China

Abstract

Exploring the risks faced in personal information protection in the era of generative artificial intelligence, this study employs a combination of case analysis and technical feasibility assessment to propose the construction of a collaborative governance framework involving users, regulatory authorities, and developers to address these risks. This tripartite collaboration ensures user data sovereignty while balancing technological innovation with risk mitigation. During the data governance transition period, an inclusive and prudent regulatory strategy should be adopted, integrating technical governance with institutional innovation to establish a dynamically balanced governance system. This approach ultimately aims to achieve mutual promotion between the benefits of technological innovation and societal public interests.

Keywords

generative artificial intelligence; data risk; digital divide; data governance frameworks

生成式人工智能对个人信息的冲击与应对

王化烜烁

兰州理工大学法学院，中国·甘肃 兰州 730050

摘　要

探讨生成式人工智能时代个人信息保护面临的风险，采用案例分析和技术可行性论证相结合的方法，提出构建由用户、监管机构、开发者三方共同参与的协同治理框架应对风险，三者结合既能保障用户数据主权，又可平衡技术创新与风险防控。在数据治理转型期，采取包容审慎的监管策略，通过技术治理与制度创新的有机融合，构建动态平衡的治理体系，最终实现技术创新红利与社会公共利益的双向促进。

关键词

生成式人工智能；数据风险；数字鸿沟；数据治理

1 引言

ChatGPT 是 OpenAI 在人工智能领域里程碑式成果，作为一种生成式人工智能模型，它所具有的自主学习并加工输出的能力，很好地契合了人们日常生活以及企业运转的需求。科技创新的洪流下通常伴随着未知的危险，随着生成式人工智能在医疗、科技、学术、办公等领域的普遍应用，模型算法的数据源头也愈发庞杂。而坐拥海量数据的人工智能厂商运行模型时无法达到《中华人民共和国个人信息保护法》（以下简称个人信息保护法）所要求的透明度，“算法黑箱”、滥用数据、数据诈骗等问题层出不穷，高新技术在惠及普罗大众的同时，也在用户、监管机构、模型设计者之间设立起高墙，加剧了数字鸿沟和数字不平等，冲击着个人信息保护法所维护的公民权益。当前我国对于数据风险的治理模式尚处于萌芽与探索阶段，如何规避生成式人工智能模型的负面影响，加强对个人信息的法律规制成了我国乃至其他国家迫在眉睫的课题。由此，本文从生成式人工智能的算法逻辑出发，探索处理个人信息过程中存在的风险，挖掘其深层次的原因，结合外域国家和组织的做法，本着包容审慎的原则，在立足于中国本土文化的基础上，就治理人工智能领域乱象提出个人意见，以待生成式人工智能产业的良性发展。

2 生成式人工智能对个人信息的冲击

2.1 技术特性与算法逻辑的双重影响

生成式人工智能 AIGC(AI Generated Content) 模型[①] 在面向用户之前会经历对数据（个人信息在作为软件程序处理对象时称为数据）的四个阶段训练：[②] 收集、处理、输出、储存。数据经历吸收和筛选重组，最后呈现在用户面前，其中掺杂着不仅仅是对数据品控的择优意识，还嵌入了模型设

① 谭佐财 .ChatGPT 的法律风险与治理路径 [J]. 湖南科技大学学报 (社会科学版),2023(3):117.

② 范为 . 大数据时代个人信息保护的路径重构 [J]. 环球法律评论 ,2016(5):92-115.

计者的主观价值理念。涉及到的数据来源合规、泄露、滥用风险不可小觑。而在各个阶段中，设计者添加的算法程序又会放大对数据安全侵蚀的风险，换句话说，在整个进程中数据风险与算法风险是并发的。

2.2 处理过程中的核心风险

基于生成式人工智能程序训练的固定性，下面从算法逻辑出发，探讨存在的风险，对症下药。

2.2.1 告知同意机制失效风险[①]

中国消费者协会 2018 年发布的《APP 个人信息泄露情况调查报告》显示，85.2% 的受访者遭遇过个人信息泄露，近七成认为手机 APP 在不必要情况下获取用户隐私权限，APP 过度采集个人信息呈现普遍趋势。

生成式人工智能其数据源的支持主要通过网络爬虫、自动识别算法等手段进行。在数据收集这一阶段，会有一个用户须知即知情同意的环节。[②]企业会通过操作隐私协议“制造同意”，寻求隐私收集与处理的合法化。通常授权与使用相互绑定，用户数据实际上被强制征用；应用权限和隐私政策内容过长、可读性差，导致很少有人仔细阅读；预先勾选、凸显或间接遮蔽部分关键条款，也是 APP 引导用户授权的惯用操作。ChatGPT 的训练数据库来源于 OpenAI, 在使用条款第 3（a）条指出 OpenAI 可能会根据需要使用用户信息，且在“隐私政策”中明确的说明会使用相关网络跟踪用户的关联浏览记录，[③]虽然用户仍然可以拒绝同意，但在开发者巧妙的程序设计下保持着默示同意为原则，拒绝同意为例外的秩序。且在特定情形下这种信息收集不会被 DNT（请勿跟踪）所限制，这意外着告知同意规则被架空，个人信息保护法第十三条成了一纸空文。

如若模型爬取的数据是属于公共领域的，个人信息保护法第二十七条也明确规定个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。法条中“重大影响”字眼的判定有待商榷，在训练的繁杂性影响下，每一条信息能被正确把控在合规范围内存在很大的不确定性。

2.2.2 数据处理合规性困境

个人信息保护法第六条、第七条以及第二十四条明确指出开发者在处理数据时应当遵守公开透明原则，而在实际情况中对数据的处理达到法理上的标准实属不易。大多数人都经历过在某些私人机构的调查问卷上留下联系方式后络绎不绝的推销电话，该机构超出收集目的的使用行为是对个人信息的绝对侵害。相对侵害的行为大多通过信息泄露或者贩卖的途径发生，比如在 OpenAI 的隐私政策中明确说明在某些情况下其会将个人信息提供给第三方，包括商用信息。

除了不正当的使用外，基于程序设计者的主观性以及对数据学习的全面性，生成式 AI 在输出过程中可能夹带不符合社会伦理甚至违反法律规范的信息。在对生成式人工智能模型是否能投放入社会的评估报告中显示，该模型对社会某一群体甚至是人种带有强烈敌意。[④]模型算法程序在学习阶段本身就无法对人类语言做到完全理解，在接触负面信息时也无法做到准确筛选，不可避免产生偏见，而在反复训练与学习中这种刻板印象会被逐渐加深，最终流入社会，潜移默化地影响那些懵懵懂懂未成年用户的身心健康。[⑤]这种风险的来源很大一部分是基于模型逻辑运转机制的不透明性，即“算法黑箱”风险[⑥]。计算机软件程序运行中有部分是靠 Bug 运转，即存在连开发者都无法解释的机制，[⑦]在各家人工智能公司互相竞争以及对知识产权保护的大环境下，披露模型细节更是天方夜谭。

2.2.3 虚假信息生成与传播风险

网上有一句流传已久的话：网上查病，癌症起步；网友断案，死刑起步。这是网友们的日常吐槽，却侧面反映出生成式人工智能的缺陷。作为一款商业性程序，生成式人工智能只是基于训练后专注于服务用户的程序，最终目的是给开发者增加创收，这就得通过“编造”令人满意的回答来得到用户的认可，在我用过的某款 AI 软件聊天框下有一行小字“AI 可能生成不准确信息，请谨慎使用”，不难看出生成式人工智能有生成虚假信息之嫌。近年来，通过 AI 换脸技术骗取老年人养老金退休金的案件频频发生。究其原因是人工智能深度合成技术的普及导致犯罪成本的低廉，投机分子可以随意在网络上完成换脸从而进行诈骗行为，此种行为不仅犯罪率高，还难以打击彻底，给网络空间以及社会治理带来了极大的负面影响。

3 风险成因多维解析

生成式人工智能产业链的秩序稳定性主要由三方构建：开发者、用户以及监管部门。任何一方内部的矛盾都会映射在这个系统中造成紊乱，即风险的诞生。下面笔者按照用户、监管部门、开发者的顺序逐个分析各个主体内部风险的源头。

3.1 技术崇拜与数据中心主义倾向

生成式人工智能相较于传统人工智能最大的区别就在于前期大量数据的训练，这也形成了无论是输入、处理、输出都是围绕数据这一要点展开，即数据中心主义。前面我们就提到该模型运行程序设计之初就包含了设计者的主观意

① 斜晓东 . 风险与控制：论生成式人工智能应用的个人信息保护 [J]. 政法论丛 ,2023(4):60.

② 任龙龙 . 论同意不是个人信息处理的正当性基础 [J]. 政治与法律 ,2016(1):126-134.

③ 谭佐财 .ChatGPT 的法律风险与治理路径 [J]. 湖南科技大学学报 (社会科学版),2023(3):117.

④ 毕文轩 . 生成式人工智能的风险规制困境及其化解：以 ChatGPT 的规制为视角 [J]. 比较法研究 ,2023(3):158.

⑤ 徐露 . 算法透明的法律规制研究 [D]. 郑州大学博士学位论文 ,2022:10.

⑥ 许可 . 人工智能的算法黑箱与数据正义 . 社会科学报 ,2018(6).

⑦ 郑晓华 . 算法时代网络意识形态风险防范与实践逻辑 [J]. 重庆邮电大学学报 (社会科学版),2023(3):163-170;189.

志，而在训练阶段基于数据接受的全面性也难免混杂着形形色色的价值观，进而模拟人类语言进行对话，既包含人类良性的一面，也不可避免有着人类的阴暗面。随着 ChatGPT 初代到 4.0 的迭代更新，算法的进一步加强，机器聊天的痕迹逐渐淡化，语言模型与人类无异。人们在一次次的求助中放下内心尚存的质疑，最终对其过度信任。[①] 对虚拟程序的信任无疑是一切风险的来源，无论是在点击告知同意书时，还是在判断数据诈骗时。即便人工智能程序的交互页面都会有风险提示，用户也不以为然。我们需要清楚的一点是，人工智能模型的开发者是追本逐利的，即便设计者最初目的是服务社会、造福人类，但在巨量的开发成本、紧迫的同行竞争等现实压力影响下，后期的开发过程中难免掺杂经济因素考量从而忽视掉一些合规方面的权益保障，对个人、社会乃至国家造成难以估量的影响。

3.2 法律滞后性与治理转型期的张力

我国对于人工智能产业的规制历经两个阶段，即从包容到集中。[②] 在人工智能发展早期，2017 年 7 月 8 日，国务院发布《新一代人工智能发展规划》，提出加快建设创新型国家和世界科技强国的目标，既要清醒的认识到自身的不足，也要把握人工智能成为经济发展的新引擎。同年 12 月 13 日为贯彻落实《中国制造 2025》和《新一代人工智能发展规划》，加快人工智能产业发展，推动人工智能和实体经济深度融合，制定《促进新一代人工智能产业发展三年行动计划（2018 — 2020）》。[③] 此阶段可以概括为包容放权模式：这种模式主要依靠行业组织和企业自身来制定行为规范，实现行业自律，而监管部门只制定软性规则进行引导推动，对于现实事件也基本上采取事后处理的态度。该种模式的优点是可以适应快速变化的市场环境，同时给方兴未艾的人工智能领域留存更多空间进行开拓创新。但该模式无法进行事前预防，若事态升级到无法控制的局面，对社会会造成不可估量的后果。且依靠企业自觉性这种过于依赖市场的治理模式，也同样是对企业逐利性考虑的欠缺。

现如今我国正处于自上而下的监管模式，换言之属于集中统一管理模式。我国已基本建立起一个由法律、部门规章、地方性法规、国标、行业自律标准等组成的多层次治理规范体系。这个体系从中央到地方，从政府到行业组织，涵盖了不同级别和层次的治理内容，同时还融合了具有强制约束力的法定规范（硬法）和新型的行业自律准则（软法），形成了一个综合全面的治理体系。[④] 此种模式的优点是执行力强，可以在短期内迅速解决问题，人工智能产业在国家监管的范畴发展，其潜在的风险能够得到有效的把控。但同样过于强硬、缺乏弹性的管理会带来监管过度、限制创新的问题。

回望 2017 — 2024 年我国对人工智能与实体经济双轨制发展的历程，仍然可以看出我国尚处于治理模式的过渡转型期，究竟何种模式适合我国经济结构有待商榷，但风险不等人。

3.3 数据殖民主义：技术垄断下的新型剥削逻辑

生成式 AI 的风险不仅源于技术缺陷和法律滞后，更植根于数据殖民主义的权力结构。数据殖民主义揭示了数字时代技术垄断者通过数据掠夺实现权力扩张的本质。科技公司通过用户协议模糊化数据所有权（如 ChatGPT 使用公开论坛内容训练模型），本质是将个人数据视为无主资源进行圈占，形成“数据原料地（用户）- 技术加工中心（企业）- 利润垄断者（平台）” 的殖民链条，延续了殖民主义的资源掠夺逻辑。通过“数据圈地运动”将个人信息转化为私有生产资料，而用户沦为“数字佃农”。例如，Meta 利用用户社交数据训练 LLaMA 模型却未支付任何对价；2023 年 OpenAI 被曝使用肯尼亚廉价劳工标注敏感数据，但未向数据提供者（用户或劳工）分享商业收益。数据殖民主义因而成为算法风险与数据合规困境的深层诱因，揭示了个体赋权（如知情同意）必须与结构性改革（如数据主权立法）同步推进的必要性。现有的个人信息保护法侧重个体知情同意，但数据殖民主义揭示的结构性剥削需突破“个人 - 企业”二元框架，只有通过重构数据所有权、重建利益分配机制，才能避免人工智能时代沦为新殖民秩序的数字复刻。

4 风险应对本土化路径构建

4.1 法律规制模式的国际启示：敏捷治理的探索

欧盟的严格合规模式在个人信息保护上彰显了制度刚性，但其冗长的立法程序难以匹配生成式 AI 的迭代速度。相较而言，日韩等国探索的敏捷治理路径，为技术不确定性下的数据权益平衡提供了新思路。

敏捷治理摒弃“一刀切”的刚性监管，转而通过阶段性规则迭代与多元主体协同应对技术不确定性。在生成式 AI 场景中根据应用场景实时调整监管强度，避免过度压制创新。通过“监管沙盒”允许企业在可控环境下测试数据合格方案，如匿名化计算，积累经验后再推广普适规则。正如 Brownsword 所言“生成式 AI 的技术黑箱与快速进化，要求法律从静态合规检查转向动态风险共治。敏捷治理通过小步快跑的规则更新，填补了传统立法在响应速度上的鸿沟”。[⑤]

“活文书机制”指的是在法律文本中嵌入触发修订的客观指标，自动启动规则升级程序。如韩国《个人信息保护法》增设“AI 特别条款”，规定若生成式 AI 用户投诉量连续 3 个月超过阈值，则强制实施算法源代码备案制度。适应

① 袁康 . 可信算法的法律规制 [J]. 东方法学 ,2021(3).

② 薛澜 . 人工智能治理 -- 过去是回应式治理，现在是集中治理，应尽快进入敏捷治理 http://gfagz27172ce1fca64726hop0bnbko5cqv6c6f.fzfy.oca.swupl.edu.cn/archives/64542.

③ 参见工业和信息化部关于印发《促进新一代人工智能产业发展三年行动计划 (2018—2020 年)》的通知 .

④ 毕文轩 . 生成式人工智能的风险规制困境及其化解：以 ChatGPT 的规制为视角 [J]. 比较法研究 ,2023(3):161.

⑤ Brownsword, R. Law, technology, and society: Reimagining the regulatory environment. Law, Innovation and Technology, 2017(1),p12-15.

性立法除了拥有“活文书机制”工具，还有“模块化立法框架”，该制度设计是将 AI 法律拆解成独立功能模块。如数据采集合规模块、内容生成追责模块等，允许针对技术进展单独修订，在日本《AI 社会原则指南》中就采用“核心原则＋技术附件”结构，2023 年针对生成式 AI 新增训练数据透明度附件，要求公开数据来源地域分布，如 Stable Diffusion 披露 Lasion-5B 数据集构成。

日韩这种适应性立法智慧，对中国在个人信息保护法框架下细化 AI 规则具有重要借鉴意义。我们可以构建“原则坚守 - 细则弹性”的混合立法体系，刚性方面在《网络安全法》《个人信息保护法》中确立“数据最小必要”“用户控制权优先”等不可突破的红线，弹性方面授权国家网信办制定《生成式 AI 数据合规实施细则》，按年度发布更新版本，如 2024 版重点规制深度伪造数据采集。以上举措可在经济发达地区试点“数据治理特区”，如在雄安新区、深圳先行示范区允许企业采用“区块链存证＋智能合约”替代传统书面同意，用户通过数字分身代理行使数据权利，同时也要建立试验区退出机制，若个人信息泄露事件超阈值则暂停创新条款使用。 正如 Fischer 的“参与式技术评估”理论所示，生成式 AI 的治理需打破“专家 - 官僚”垄断，使公众从被保护对象转化为规则共治者。

4.2 制度优化：从数据掠夺到数据正义

4.2.1 建立数据资源税收制度

生成式 AI 的“数据圈地运动”将个人信息异化为私有生产要素，而数据资源税通过税收杠杆调节数据生产要素收益，矫正数据殖民主义下的结构性剥削，其理论正当性来自于经济产权理论。[①] 对调用超量个人数据训练模型的企业征收专项税，税率按数据密集度（训练数据量 / 模型参考量）动态浮动。例如，GPT-4 调用 1.2 万亿条社交媒体数据，需按 0.005 美元 / 条标准缴税，其中 60% 注入省级公共数据池，供中小 AI 企业调用。欧盟的数字服务税（DST）已经部分体现这一制度，只是其侧重平台营收而非数据用量 ,2025 年起对跨境数据调用征收数字资源税，Meta 因使用欧盟用户数据训练 LLaMA-3 模型缴纳首笔税款 2.3 亿欧元。中国可创新“数据用量 * 敏感度系数”计税模式以此倒逼企业优先使用低风险数据。

4.2.2 重构知识产权规则

传统知识产权制度将数据视为无主资源或企业资产，忽视了用户作为数据生产者的劳动属性。然而根据数字劳动价值理论 [②] 生成式 AI 训练数据的价值创造包含双重劳动：一重是显性劳动，包括用户主动生成文本、图片等；另一重是隐性劳动，包括 AI 系统捕获的用户行为轨迹并用于模型优化。因此知识产权规则应该突破创作者中心主义，确定用户对衍生数据的收益权，该思路早在 2020 年就有所提及。[③]

该数据分红机制由三部分构成：确权机制、分红模式、纠纷解决方式。首先在《中华人民共和国著作权法》中增设“数据衍生权益”条款，明确用户对 AI 训练数据的署名权与收益权，同时参考欧盟 Data Act 第 12 条承认数据利他主义者的补偿请求权，即约定用户对训练数据享有“有限排他权”，允许企业非独占使用但保留收益主张权。分红模式分为直接分红与间接分红两种，直接分红按照数据使用量分配 AI 模型营收，如用户获取 GPT-4 利润的 0.001%，间接分红则是抵用 AI 服务，如免费 API 调用额度之类，法国 CNIL 就要求 AI 企业将 2% 的利润注入数据公益基金，国内可利用区块链存证用户数据流向，如蚂蚁链“数据要素流转平台”，智能合约自动执行分红。那么在用户与企业发生纠纷时应该采取何种措施呢？欧盟会通过欧洲数据保护监督局（EDPS）协调跨境数据分红纠纷，在国内可采取设立“数据版权集体管理组织”，如音乐版权协会，代理用户执行维权与收益分配事宜。

4.3 治理转型：从集中管控到协同共治

4.3.1 “枫桥经验”下的多元主体参与机制

枫桥经验其核心理念是充分发动和依靠群众，坚持矛盾不上交，实现基层问题就地解决。将枫桥经验融入到生成式人工智能对个人信息的侵害治理中，是基层治理模式在人工智能时代的适应性创新。工作重点应从两个方面开展：一个是社区和基层组织的参与。社区和基层组织在个人信息保护方面具有独特的优势，可以通过设立个人信息保护专员、开展个人信息保护培训措施，实现对个人信息的实时监控和保护。另一个就是建立举报机制。鼓励民众对侵犯个人信息的行为进行举报，设立举报热线和网络平台，对举报线索进行认真核查，对侵权行为进行严厉打击。

4.3.2 包容审慎政策试点

前文已然提到我国正处于数据治理的过渡转型期，如今横在我国立法人员以及学者面前最大的问题就是如何平衡科技发展与监管策略之间的冲突。

笔者以为总的方向上应该采取包容审慎 [④] 的态度，其主张在防范风险的同时，鼓励创新和发展。通过制定适当的政策措施，支持生成式人工智能领域的技术创新和应用，提高生成式人工智能的竞争力。具体来说，包容性是指尊重和包容不同的利益相关方，包括监管机构、科研机构、用户等，听取他们的建议，共同推动生成式人工智能的发展。审慎性是指在制定政策和监管措施时，要充分考虑生成式人工智能可能带来的风险和挑战，采取必要措施降低风险，确保行业

① Zuboff, Shoshana. The Age of Surveillance Capitalism: The Flight for a Human Future at the New Frontier of Power. Public Affairs.2019,p125.

② Fuchs Christian. Digital Labour and Karl Marx. New York: Routledge.2013,p45.

③ Stahl, Bernd Carsten. Ethics of Artificial Intelligence. Springer.2020,p112.

④ 李克强 . 李克强详解为何对新业态实施“包容审慎”监管？，载中国政府网 http://gfagzc112eefb48ed4fffhop0bnbko5cqv6c6f.fzfy.oca.swupl.edu.cn/guowuyuan/2018-09/12/content_5321209.htm.2024 年 5 月 21 日访问。

发展的稳定性和安全性。[①]

在软法层面进行分级式的风险管理，包容审慎的核心是该松的松，该紧的紧。将用户信息按照隐私程度进行层级划分，隐秘性较高且涉及较大经济效益的为最高等级，给予最大的监管资源倾斜，然后逐级递减。这样可以减少工作人员的强度，合理配置法律资源。

4.4 技术赋能：数据主权和反垄断措施

生成式人工智能的“黑箱”特性加剧了个人信息滥用风险。当前我国透明度规则偏重程序公开而忽视实质可理解性，公开的算法公式仍无法被公众解读。因此我们在风险应对中需立足本土制度优势与技术能力，构建“规则约束—技术赋能—社会监督”三位一体的透明度治理框架，推动算法可解释性。

《互联网信息服务算法推荐管理规定》第 12 条鼓励算法推荐服务提供者综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的透明度和可解释性，避免对用户产生不良影响，预防和减少争议纠纷。在规则层面需要将透明度义务分级化处理。在诸如医疗诊断、金融风控等高风险场景中，强制要求企业在上线生成式人工智能前需提交算法说明书与数据来源报告，通过网信办备案核心算法逻辑，如特征权重、决策阈值，备案信息脱敏后向社会公开。而在娱乐聊天之类的低风险场景中可以简化披露要求，仅公开数据总量与去标识化比例即可。实际生活中企业会以商业秘密为由拒绝披露算法细节，如字节跳动称推荐算法涉及核心竞争力拒绝披露时，我们可以允许企业向监管部门提交加密版算法说明，由第三方机构审查后发布摘要。

在具体审计算法透明度中运用高新技术，如可解释性插件，该插件可视化展示生成式人工智能模型的决策路径；偏见检索引擎，该引擎可以扫描训练数据中的地域、性别偏差，筛查出存在歧视风险的 AI 应用并给出负面清单。

生成式人工智能时代实现社会监督离不开用户对数据的控制力，其本质是用户数据主体赋能。由政府设立统一政务平台，用户可实时查看哪些 AI 模型使用了自己的数据以及数据使用的地理分布与商业用途，并实时调整数据授权范围。由政府主导开发个人数据主权工具，用户授权 AI 代理监控数据流向，自动执行维权动作，如检测到未经授权的数据调用时，触发区块链存证并发送律师函，同时消费者协会、工会等可代表不特定用户起诉 AI 企业数据滥用，胜诉赔偿金注入“数据公益基金”，用于资助弱势群体维权。

从“弱同意”到“强控制”，将用户从数据剥削的客体转化为治理共同体中的平等主体，打破“平台资本主义”的数据圈地，践行“数据属于人民”的社会主义治理观。

5 结语

冰冻三尺非一日之寒，我们应正视自身法律制度的不足，生成式人工智能技术的快速发展对现行的个人信息保护法提出了挑战，我们可以通过建立数据治理框架、应用高新技术提高技术安全性、促进各方合作等方式来应对这些挑战。在保护个人隐私的同时，我们也要关注生成式人工智能技术的发展，以实现技术创新与法律监管之间的平衡。只有充分保障个人信息安全，才能确保生成式人工智能技术在未来得到健康、可持续的发展。

① 王东方.生成式人工智能对个人信息权益的侵害风险及其法律规制[J].征信,2024(2):[34，35].