E-Commerce Letters 电子商务评论, 2024, 13(4), 2830-2834
Published Online November 2024 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2024.1341464

Hans汉斯

人工智能驱动的个性化推荐系统法律问题分析

范美林

贵州大学法学院，贵州 贵阳

收稿日期：2024年8月31日；录用日期：2024年11月6日；发布日期：2024年11月13日

摘 要

数字经济时代，人工智能驱动的个性化推荐系统在电子商务，新闻，社交等领域应用广泛，同时也带来了数据隐私保护、数据泄露、算法透明性与公平性、以及新兴技术与现行法律框架的冲突等问题，为实现法律之治，可从数据最小化与匿名化、加强监督与处罚、用户知情权的加强、算法可解释性提升、保持对新兴技术的敏感度与规制几方面对人工智能驱动的个性化系统进行法律约束，切实保障用户权益。

关键词

人工智能，个性化推荐系统，法律分析

Analysis of Legal Issues of Personalized Recommendation Systems Driven by Artificial Intelligence

Meilin Fan

School of Law, Guizhou University, Guiyang Guizhou

Received: Aug. 31st, 2024; accepted: Nov. 6th, 2024; published: Nov. 13th, 2024

Abstract

In the digital economy era, AI-driven personalized recommendation systems are widely used in e-commerce, news, social networking and other fields. At the same time, they also bring about problems such as data privacy protection, data leakage, algorithm transparency and fairness, and conflicts between emerging technologies and the current legal framework. In order to achieve the rule of law, AI-driven personalized systems can be legally constrained from the aspects of data minimization and anonymization, strengthening supervision and punishment, strengthening user right to know, improving algorithm interpretability, maintaining sensitivity and regulation to emerging technologies, and effectively protecting user rights.

文章引用: 范美林. 人工智能驱动的个性化推荐系统法律问题分析[J]. 电子商务评论, 2024, 13(4): 2830-2834.
DOI: 10.12677/ecl.2024.1341464

Keywords

Artificial Intelligence, Personalized Recommendation System, Legal Analysis

1. 引言

互联网技术的发展极大地改变了传统的商业模式及我们的生活方式，其中个性化推荐系统更是在电子商务、社交媒体、新闻等领域得到了广泛的应用，通过分析用户行为数据，个性化推荐系统能够针对性地提供内容和产品，提升用户体验和商业收益[1]。个性化的推荐的实现需要对用户数据进行收集、分析、标记，以及利用人工智能算法进行用户画像，并将平台的商品或服务等内容与用户倾向进行匹配，这个过程中往往涉及数据隐私、算法透明性和公平性等法律问题，影响用户的基本权利和利益。个性化推荐服务在便利人类生活的同时，同样需要受到法秩序的干预和规制[2]。

2. 个性化推荐的法律问题

2.1. 数据隐私保护的法律挑战

2.1.1. 用户同意的有效性

在数据隐私保护方面，获取用户的明确和知情同意是基础。但是，实践中同意的有效性往往会受到质疑[3]。根据 2022 全国网民网络安全感满意度《个人信息保护和数据安全专题报告》调查结果显示，36.7%的公众网民认为对个人信息保护现状认为一般，22.93%的公众网民对个人信息保护现状持负面评价。在公众网民在对 APP 运营者在个人信息保护方面表现的评价中，认为一般的占 51.43%，认为有所变差或者明显变差的占 3.72%。同时 40.36%的公众网民认为其遭遇“比较多”甚至“非常多”信息泄露，仅有 21.98%的公众网民认为其近一年来“没有遇到”或“很少遇到”个人信息泄露。数据搜集者和平台用户不具有对等地位，技术力量悬殊，在用户协议或隐私政策中，企业所提供的隐私条款文字通常晦涩难懂、繁杂至极，用户往往琢磨不透，企业借此过度收集个人信息。用户只有按下“同意”键，才被允许使用相关应用程序，否则只会被拒之门外[4]。这种“霸王条款”导致用户在使用应用程序时，无法真正知晓自己的个人信息将如何被收集、公开和交易，使得数据搜集的同意过程流于形式。

2.1.2. 数据安全与泄露责任

数据泄露事件频发，使得数据安全问题备受关注并成为重要的法律议题。2013 年，斯诺登曝光了美国的“棱镜计划”，震惊全球[5]。曝光内容显示，从 2007 年开始，美国政府便通过微软、谷歌、苹果等大型互联网公司的服务器，对全球用户的隐私进行监控。监控范围广泛、持续时间长、侵犯程度深，引发了广泛的抗议和对个人信息保护的强烈关注。尽管这一丑闻被揭露，信息泄露的威胁仍未消失。随着时间的推移，一些更加隐秘的网络攻击事件逐渐显现，其背后往往涉及跨国黑客组织。除了非法收集个人信息，另一严重问题是非法出售这些信息。犯罪团伙将用户的个人数据卖给数据经纪人、黑市等非法渠道以牟取暴利。

2.2. 算法透明性与公平问题

随着人工智能技术的发展，算法特别是深度学习模型在各类应用中得到了广泛的使用，但也引发了

一个问题，即“黑箱问题”。该问题指算法的内部决策机制由于高度的复杂性和非线性结构，会变得难以解析和理解，在深度学习模型中尤为明显，这些模型往往包含多层神经网络和大量的参数调整，其决策过程往往超过人类直观理解的范畴，并且由此带来了许多问题。第一，它使得算法的决策逻辑不透明，用户、开发者以及监管机构无法直接观察或解释模型的内部运作，更难以判断这些决策是否基于合理的数据模式，是否受到了某些偏差或噪声的影响，这种不透明性直接威胁到算法的合法性和可信度，特别是在涉及个人隐私时。第二，因为缺乏对算法内部决策过程的清晰理解，难以识别和纠正其中潜在的偏见，黑箱问题还会影响算法的公平性。例如，在自动化招聘系统、信用评分等领域，算法可能会基于训练数据中的历史偏见做出歧视性决策，这些偏见往往不易被察觉和修正，即使算法表面上表现良好，其内在决策可能仍存在系统性的不公平。

2.3. 新兴技术与现行法律框架的冲突

2.3.1. 技术发展速度与法律滞后

在新兴技术的推动下，社会发展进入了一个快速变革期。以人工智能技术为例，随着其在数据处理、自动化决策和自我学习能力方面的突破，使得过去许多依赖于人类判断的任务实现了机器化，但同时带来了现行法律体系的滞后。法律的制定和修改通常需要经过详细的调研、广泛的社会讨论和严格的立法程序，这一过程本身就具有较长的时间周期，而与此形成鲜明对比的是技术的迅速迭代和扩展应用。这一滞后现象带来的直接后果是，现行法律体系难以涵盖新兴技术所带来的新型行为模式和伦理挑战。例如，AI 技术的广泛应用催生了新的数据处理方式和自动化决策系统，而这些新模式往往不在现行数据保护和隐私法律的有效范围之内。AI 算法对用户数据的深度分析、预测和行为引导在法律上可能缺乏明确的界定和限制，导致用户隐私权和数据安全面临风险。同时，AI 自动化决策可能涉及歧视性偏见、责任归属不清等问题，而这些问题往往超出了现行法律对传统决策体系的规制范围[6]。

2.3.2. 法律滞后带来的具体挑战

数据隐私保护问题。随着 AI 技术对大规模数据的依赖，传统的数据保护法律显得捉襟见肘。我国对于个性化推送技术的现行立法多集中于从个人隐私保护、平台及服务提供商行为规范等角度开展的，法律分布较为分散，高位阶专门法律尚未制定，低位阶规范性文件的法律效力较弱，尚未形成完整的针对个性化推送行为的法律体系。我国现有关于个性化推送技术的立法主要侧重于个人隐私保护和对平台及服务提供商行为的规范。然而，这些法律分散在多个领域，高层次的专门法律尚未出台，低层次的规范性文件法律效力较弱，因此尚未形成一个针对个性化推送行为的完整法律体系。国外，《欧盟通用数据保护条例》等法律虽已对个人数据的保护做出较为详细的规定，但面对 AI 驱动的复杂数据处理和分析模式，其效力仍显不足。这些法规大多聚焦于数据收集、使用和存储的基本原则，但 AI 技术所涉及的深度学习和预测分析往往打破了传统数据使用的界限，使得法律在实际执行中面临巨大的解释空间和漏洞。责任归属问题。AI 系统的决策自动化使得传统的责任分配规则面临挑战，当 AI 系统做出错误决策导致损害时，责任应由系统开发者、使用者还是算法本身承担？现有法律体系尚未能明确解决这一问题，这种法律责任的不确定性影响了相关当事人的权益。

3. 法律对策与建议

3.1. 数据隐私保护对策

3.1.1. 数据最小化与匿名化

数据最小化要求平台在收集和处理数据时，确保只获取实现业务目的所需的数据，并在不再需要时

及时删除有关数据，减少对用户隐私的影响。数据匿名化则要求对个人数据进行去标识化和数据分割，以确保数据无法被直接或者间接用于识别个体[7]。

3.1.2. 加强监督与处罚

第一，加强个人信息泄露风险的监督检查。相关部门要通过常态化的监督、抽查，确保平台切实履行对用户数据安全的保障义务，确保信息系统的安全防护措施实施到位，并且将相关的检查结果及时向社会公众公布，以督促平台加强个人信息的安全管理，防止个人信息泄露事件的发生[8]。

第二，要加大对个人信息泄露事件的处罚力度。有关部门对于个人信息泄露事件，在查清事件情况下，依据泄露事件的规模、企业是否采取有关安全措施、为减少个人损失所采取的补救措施等，对企业实施相应程度的行政处罚，并采取灵活的处罚方式[9]。最后要加强数据安全普法宣传，提高公众的安全意识。通过开展各种形式的宣讲会，讲座，法律知识竞赛等教育活动，向社会普及个人数据安全知识。

3.1.3. 用户知情权的加强

平台应提供简明易懂的隐私政策，详细说明数据收集、处理和使用的目的及方式。在隐私声明中，应使用户对平台收集的数据的范围，收集的目的、方法以及数据收集后的用途有明确的了解，对与用户的关键个人信息，还需要着重提示并解释，并告知用户相应的权利，包括访问、修改、删除数据的权利，并提供便捷的渠道以行使这些权利。

3.2. 算法透明性与公平性对策

平台应开发和采用能够提供清晰决策解释的算法，确保用户和监管机构能够理解算法的决策过程。可以通过多种方式实现算法可解释性，例如利用模型可解释性技术(如局部可解释模型解释(LIME)和Shapley Additive explanations (SHAP)来揭示模型的决策逻辑还应建立透明的文档和报告系统，详细记录算法的设计和训练过程，为用户和监管机构提供必要的解释和信息。

3.3. 保持对新兴技术的敏感度

要建立动态立法机制，保持对新兴技术的敏感度。可以尝试通过设立专门的技术法律委员会或加快技术法规的立法流程来应对快速变化的技术环境[10]。在立法过程中，也要坚持对技术中立原则的坚持，即在法律制定过程中应避免对具体技术的过度干预，而应关注技术应用的伦理和社会影响，为新兴技术的发展留有足够的空间和弹性。

与此同时，有关立法机构还应该强化对技术风险的前瞻性评估机制，通过与技术专家、企业、社会公众的广泛合作，可以更好地预见和规制新兴技术可能带来的负面影响。

4. 结论

人工智能驱动的个性化推荐系统在法律上面临着数据隐私，算法透明性与公平性以及新技术与现行法律落后性之间的矛盾。其中，数据隐私保护的核心在于采取数据最小化以及匿名化措施，确保仅收集必要数据并有效保护用户隐私。更重要的是加强用户知情权，通过明确的隐私政策和简化的同意管理提升用户对数据处理的信任。针对算法透明性与公平性，可以提升算法可解释性和实施偏见检测与修正流程，以此来增加算法决策过程的透明度，保障算法对所有用户群体的公平性。最后，针对新兴技术与现行法律框架之间的冲突，应引入合规性技术工具，并实现法律法规与技术标准的协调，以应对法律与技术的快速变化带来的挑战。

参考文献

[1] 武腾. 人工智能时代个人数据保护的困境与出路[J]. 现代法学, 2024, 46(4): 116-130.

[2] 郭诗怡. 智媒时代算法技术对把关机制的冲击及防范策略[J]. 新闻世界, 2024(7): 32-35.

[3] 文静. 算法个性化推荐下消费者权益保护研究[D]: [博士学位论文]. 上海: 上海师范大学, 2024.

[4] 施涵杰. 消费者自动化决策拒绝权研究[J]. 中国价格监管与反垄断, 2024(6): 37-39.

[5] 徐玉梅, 王欣宇. 我国重要数据安全法律规制的现实路径——基于国家安全视角[J]. 学术交流, 2022(5): 37-48, 191.

[6] 丁国峰, 寿晓明. 生成式人工智能算法的法律风险及其规范化防控[J]. 云南大学学报(社会科学版), 2024, 23(3): 107-119.

[7] 韩璇君. 个性化算法推荐平台的私法规制[D]: [硕士学位论文]. 济南: 山东政法学院, 2024.

[8] 张晟昊. 大数据时代个人数字身份的法律保护研究[D]: [硕士学位论文]. 杭州: 浙江农林大学, 2024.

[9] 聂广川. 数据权利的权利属性研究[D]: [硕士学位论文]. 济南: 山东师范大学, 2024.

[10] 姚旭. 个性化推荐算法应用的法律风险规制[D]: [硕士学位论文]. 济南: 山东政法学院, 2024.