

企业中 AI 应用导致数据泄露的法律问题研究

刘奕文 常宝莲

南昌应用技术师范学院，江西南昌，330108；

摘要：随着人工智能（AI）在企业决策、操作优化和客户服务中的广泛应用，数据安全和隐私保护成为焦点。本文探讨 AI 在企业数据处理中的应用及其引发的潜在数据泄露风险，分析 AI 系统处理敏感信息时可能出现的技术漏洞和法律问题。研究概述了 AI 在数据分析和处理中的应用场景，讨论了算法漏洞、数据管理缺陷及合规性挑战等数据泄露原因。尽管 AI 提升了企业数据处理能力，但也带来了新的数据安全和隐私风险。因此，需要明确法律框架规范 AI 应用，保障数据主体权益，并为企业的数据泄露行为负责。本文强调，应制定更严格的法律规范，改进数据保护法规，强化 AI 系统的透明度和可解释性，建立全面的风险管理框架。最终，本文建议立法机构、企业和技术开发者共同合作，制定并执行有效措施，降低 AI 在数据处理中的泄露风险。

关键词：人工智能；数据泄露；数据安全；隐私保护；法律框架；

DOI: 10.69979/3029-2700.24.4.011

引言

在数字化转型中，AI 作为企业创新动力广泛应用于数据处理，提升决策和运营效率，但也带来了严重的数据泄露风险。本文探讨在中国法律框架下，AI 应用导致的数据泄露问题及其法律影响，旨在完善相关法律，保障数据安全与隐私。

在此之前，三星电子和微软等国际知名企业曾因 AI 应用导致数据泄露，引发对数据安全和隐私保护的关注。三星员工在使用 ChatGPT 时泄露公司信息，微软 AI 团队在 GitHub 上意外曝光大量私有数据，显示即便领先企业也面临 AI 数据泄露风险，涉及法律责任和隐私权等问题。随着中国 AI 技术的发展，企业在应用 AI 过程中数据泄露和隐私保护问题日益严重^[1]。

本文将分析企业使用 AI 处理数据可能带来的问题，并探讨如何在法律层面更好地规范 AI 应用，旨在促进我国 AI 相关法律法规的完善，保障数据安全和隐私保护。

1 AI 的应用与风险

企业中的 AI 应用带来了前所未有的效率和创新，但也暴露出更多风险，尤其是数据泄露领域的风险。本部分以中国法律为背景，论述 AI 在企业环境中的变革性应用以及相关的法律风险。

1.1 AI 在企业环境中的应用

1.1.1 提高生产力和创新能力

据 IBM 称，包括生成式 AI 在内的 AI 技术正在彻

底改变企业提高生产力、促进创新和激发创造力的方式。例如，生成式 AI 可以创建定制的文本、语音和视频内容，以此来满足特定客户的需求和文化上的细微差别，从而激发企业的创造力^[2]。

1.1.2 企业 AI 的定制化

企业 AI 的定制化趋势可以让公司开发整合专有数据的应用程序，从而确保更准确、更符合文化的客户互动和运营效率这种个性化延伸到客户的需求和运营效率，这可以更加贴合特定市场的文化价值观。

1.1.3 运营效率

AI 在农业、教育和医疗保健等领域实现复杂流程自动化的能力可转化为显著的运营效益，通过增强洞察力推动更好的决策^[3]。

2 AI 的风险

2.1 数据泄露

Rumala 的研究指出，AI 系统中尤其在医学图像处理领域的的数据泄露复杂。需实施稳健的数据管理策略，如细致的数据分割，以防泄漏并保障数据完整性。三星电子的数据泄露事件显示，AI 数据处理可能导致违规，凸显严格法律和合规机制的必要性^[4]。

2.2 AI 法律规范不明确

AI 带来的独特挑战要求加强现有的法律框架并制定新的法理方法，以保护企业数据免受 AI 相关漏洞的侵害缺乏明确的法律定义，尤其是关于敏感个人信息或

关键数据的定义，给 AI 实体的合规性带来了模糊性。

2.3 AI 的动态性质

AI 不断学习和适应的能力可能与法律法规的静态性质发生冲突，使 AI 持续合规成为一个可实现的目标。

2.4 法律对数据保护的挑战

如 OpenAI 和 ChatGPT 数据泄露事件所示。这些事件强调了建立健全的数据保护机制的必要性，尤其是在数据需上传至云端的情况下。然而，过于严格的本地化要求和跨境传输限制可能会限制全球数据流动和合作伙伴关系的企业运营灵活性。因此，如何在保证数据安全和隐私的前提下，适当放宽数据传输的限制，是法律制定者和企业需要共同考虑的问题。

2.5 全球合作和标准化风险

由于全球各国在 AI 的法律规制方面存在不一致性，并且 AI 的数据传输与处理常跨国界进行，缺乏国际间的协调可能导致不同国家在 AI 应用和监管上采取各异的方法。所以由各国之间交流并建立一个关于 AI 的标准是十分有必要的。

3 中国 AI 法律框架面临的挑战与漏洞

3.1 对 AI 伦理和偏见的监管不足

中国现行法律广泛涵盖了数据隐私和网络安全，但缺乏针对 AI 伦理因素的具体规定。如算法偏见和决策透明度。随着 AI 系统越来越多地在创作、数据处理和信用评分等敏感领域发挥作用，完善这一漏洞至关重要。

3.2 对动态 AI 系统的覆盖不足

随着 AI 技术不断拥有更高的自主性，中国现有的法律并不能很好地应对 AI 系统所带来的挑战。具体来说，当 AI 在没有人类监督下所做出的决策时，现有的《网络安全法》或《数据安全法》等现行法律没有很好的规范由 AI 完全自主做出的决策。

3.3 AI 安全的模糊定义和标准

对于什么是“安全”的 AI 操作，中国的法律缺乏准确的定义和标准。“安全”一词在自动驾驶等 AI 技术的运用中尤为重要，在这些企业中的 AI 应用，可能对人类安全构成重大危险，而在随后执行有关安全的法律法规、追究失职责任的主体时就会面临较大挑战。

3.4 国际合作

国际合作是 AI 发展的关键步骤。虽然《数据安全法》和《网络安全法》为保护国家安全和公民隐私，对跨境数据传输进行了严格限制，但这些规定与国际标准差异较大，阻碍了中国与全球的合作和技术创新。中国的 AI 法律应与国际接轨，不仅为了更好地规范数据传输问题，更为了使中国的 AI 技术走向世界。

4 对策与建议

针对企业 AI 应用导致的数据泄露的法律问题，本文提出重点加强中国法律框架的数据保护和隐私保障的若干对策和建议。

4.1 加强中国关于 AI 的法律框架

4.1.1 完善现有法律框架

在人工智能快速发展的时代，中国已通过《个人信息保护法》《网络安全法》和《数据安全法》等法规对 AI 技术进行了基本覆盖。但由于 AI 的独特性，我们仍需对其进行特别的法律调整和细化，因其在数据收集、处理和跨境传输方面需要更高的安全和保护要求。

拿《个人信息保护法》来说，虽然规范了个人信息的收集和使用，并对敏感信息提供了额外规定，但对 AI 技术在企业应用中泄露隐私数据的责任归属尚不明确。因此，建议在法律中明确 AI 处理个人信息的界定和限制，以及如何处理 AI 生成的衍生数据。《网络安全法》和《数据安全法》在 AI 层面的应用也存在模糊性，导致法律实践中的困难，包括数据保护的保守性和数据分类标准不明确等问题。

综上所述，现有法律各有侧重，互为补充，但对于复杂的 AI 技术，没有一部法律能清晰规范其应用风险。因此，完善相关法律，甚至制定新的专门法律，十分重要。

4.2 企业责任与合规

4.2.1 明确的责任准则

制定透明的 AI 数据泄露责任归属准则，明确企业、AI 开发者和第三方服务提供商的责任。这种方法应考虑到 AI 运营的各种细微差别。正如 Borner 强调的数据泄露的多方面影响，包括经济和声誉损失，以及迅速、有效的应对机制对最大限度地减少长期负面影响的重要性^[5]。

4.2.2 合规协议

为 AI 系统实施健全的合规协议，确保企业遵守数据保护和违规管理的法律标准。笔者认为这些应协议旨在防止外泄，确保在发生外泄时迅速采取行动。Naik 等人所讨论的法律和道德考虑因素，他们在医疗行业强调了合乎道德地使用 AI、保护隐私的重要性，以及不断适应医疗保健和其他行业不断发展的数字环境的必要性^[6]。

4.3 加强国际合作与标准

4.3.1 双边和多边协定

G20 的《大阪数字经济宣言》和欧盟的《人工智能协调计划》是促进国际合作的典范。这些国际宣言和计划突出了全球在 AI 治理方面共同努力的必要性。《大阪宣言》强调在信任基础上促进数据自由流动的重要性，对 AI 发展至关重要。它倡导国际合作，利用数字经济的机遇，应对隐私、数据保护、知识产权和安全等挑战。欧盟的计划展示了全面的 AI 发展和监管方法，重点关注投资、研究、技能培养，以及道德和法律框架。该计划强调大量公共和私人投资的必要性、培养 AI 人才的重要性，并将道德准则作为可信赖 AI 的核心。

4.3.2 通过全球 AI 标准

(1) 推广国际法律标准

推广国际 AI 法律标准对确保 AI 开发和使用的安全、道德及隐私保护至关重要。全球机构如电气与电子工程师协会 (IEEE) 制定的“伦理对齐设计”指南，鼓励在 AI 开发中优先考虑伦理、人权和社会福祉，强调透明、责任和尊重用户隐私。该指南帮助专业人士和组织设计有益社会、无害个人的 AI 技术，促进问责、透明和以用户为中心的方法。中国应在国际层面持续推进相关 AI 法律原则。

(2) 彼此建立协议

各国可以通过双边和多边协议开展合作，为 AI 创建一个超越国界、连贯一致的法律和伦理框架。这种采用全球 AI 标准可进一步确保全球 AI 发展遵守商定的原则，在国际上营造信任与合作的环境。

4.4 促进公私伙伴关系

4.4.1 合作制定 AI 政策

(1) 建立 AI 伦理战略合作伙伴关系

正如 Wirtz 等人的工作中所强调的那样^[7]，在政

府、行业、学术界和民间社会之间建立战略合作伙伴关系对于制定 AI 伦理政策非常重要，并且这些合作应以平衡创新与伦理考虑为目标。

(2) 包容性政策框架

伙伴关系有助于制定融合不同观点的包容性 AI 政策框架，确保政策的全面性和道德基础。Jobin 等人的研究提供了对全球 AI 伦理准则现状的洞察，他们认为在 AI 政策制定中采用包容性和整体性方法是十分必要的。

4.4.2 联合研究计划

(1) AI 伦理研究

发展公共和私营实体之间的联合研究计划对于探索 AI 伦理实践和应对社会影响十分重要。Hagendorff 的研究强调了 AI 伦理考虑因素的重要性，以及合作研究在确定和应对伦理挑战方面的作用^[8]。

(2) 通过合作实现创新解决方案

Cath 等人的工作讨论了跨部门合作如何能够带来负责任的、符合伦理的 AI 创新，他强调了共享知识和专业知识在解决复杂伦理问题方面的益处。这让我们认识到，合作可以推动创新，为 AI 带来的伦理挑战制定解决方案。

结语

综上，我们认识到技术进步和完善的法律框架对降低风险至关重要。法律必须不断完善，紧跟 AI 的快速发展，确保数据安全和隐私保护是主动的。随着 AI 深度融入企业流程，立法需动态更新，不仅要为 AI 合规提供明确指导，还要促进 AI 创新，不阻碍技术发展。立法者、企业和技术专家的合作对于营造负责任、道德的 AI 法律环境至关重要，保障个人隐私权，维护公众对 AI 的信任。将法律严谨性与技术前瞻性相结合，是在管理和利用 AI 技术与防范其风险之间取得平衡的基础。

参考文献

- [1] Ben-Sasson, H., & Greenberg, R. (2023, September 18). 38TB of data accidentally exposed by Microsoft AI researchers. Wiz Research. Retrieved from <https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers>

[2]Dave Bergmann, "Artificial intelligence trends," IBM Blog, February 9, 2024, accessed April 17, 2024, <https://www.ibm.com/blog/artificial-intelligence-trends/>.

[3]Peter Giger, "We need to move faster to regulate AI, say CROs," World Economic Forum, July 27, 2023, Accessed April 17, 2024, <https://www.weforum.org/agenda/2023/07/ai-biggest-risks-how-to-manage-them/>.

[4]Rumala, D. J. (2023). Subject Characteristics Studies in Longitudinal Brain MRI Analysis, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia.

[5]Peter Borner, "The Legal Implications and Consequences of a Data Breach"

[6]Nithesh Naik et al, Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?

[7]Wirtz, B. J., Weyerer, J. C., & Geyer, C. (2019). Artificial Intelligence and the Public Sector-Applications and Challenges. International Journal of Public Administration

[8]Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. Minds and Machines

作者简介：刘奕文（2004-），男，汉族，江西省赣州市瑞金市，学生，本科，南昌应用技术师范学院，专注知识产权法、国际商法与人工智能法律交叉，探讨科技进步对法律体系的影响与挑战。

常宝莲（1969-），女，汉族，河南省人，副教授，法学博士毕业于西南政法大学，现任河南师范大学副教授，并受聘于南昌应用技术师范学院。专注于民事诉讼法与经济法的研究，致力于分析法院与当事人在民事诉讼中的权限分配，探讨当事人主义与职权主义的交错适用，推动法律理论与实践的进步。