世界银行国际征信委员会《技术在征信业的负责任使用》报告摘要（下）

撰文_宋　扬

编者按

随着科技的迅猛发展，征信行业也在积极应用各种前沿技术提高效率和服务质量。然而，这种技术的广泛应用也引发了一系列潜在问题，涉及数据隐私、模型可信度、安全性等方面。本文为上期（2024 年第 1 期）同名文章的第二部分，继续介绍《技术在征信业的负责任使用》，深入探讨征信业中技术应用的挑战，并结合相关地区及组织的解决方案，提出确保技术负责任应用的原则建议。

宋　扬
供职于中国人民银行征信中心规划研究部。

征信领域新技术应用面临的风险与挑战

创新往往伴随着运营和网络层面的潜在风险。在这一背景下，征信机构作为网络攻击的潜在目标，面临着严重的数据泄露风险。在缺乏有效的信息安全管控环境和完备的风险管理制度的情况下，技术创新可能导致征信机构陷入网络安全事故的境地。此外，数据或模型的缺陷也使得消费者面临潜在的风险，因为其个人身份数据可能在非法市场上流通，使其成为勒索和欺诈行为的目标。与此同时，模型的缺陷还可能引发征信机构商业机密的泄露，从而失去竞争优势，并衍生声誉风险。更重要的是，数据泄露不仅对公众对征信系统的信心产生负面影响，还对整个信用体系产生深远的不良影响。

大数据

大数据的广泛应用引起了对隐私和数据安全合规性的担忧。联合国提出明确原则，包括合法获取和适度使用。国际信用报告委员会建议推动替代数据在信用报告中的应用，提高唯一标识符可用性，促进开放数据系统和标准的发展，并评估全球唯一标识符在跨界使用和数据共享中的角色。

开放银行与 API

开放银行生态系统涉及众多利益相关者，如数据提供商、第三方服务商、消费者和政府机构，其问题解决机制极具挑战性和复杂性。由于系统内部关系错综复杂多变，出现问题难以锁定对应环节，因此建立合理的问题诊断和解决机制至关重要。

征信机构通过开放 API 获得实时信息支持，减少了数据验证环节，但相关风险需引起关注，如网络钓鱼，网络犯罪分子通常伪装成想要收集客户敏感数据的金融科技公司实施犯罪。

此外，应推动统一开放 API 标准，减少与第三方合作伙伴在安全标准上的差异。各司法管辖区的开放银行生态系统有所不同，但在监管指引下，目标是建立可信任的环境，促进数据共享经验。

人工智能和机器学习

大多数人工智能和机器学习（AI/ML）系统都被认为是一个缺乏透明度的“黑匣子”，让人无从了解其决策机制或评分标准，并对潜在的歧视和偏差判断无法估量。

全球范围内，监管关注点集中在数据隐私、模型透明度、输出公平性和可解释性。美欧新加坡等地制定法规，要求模型满足风险评估、高质量数据、透明义务。新加坡推崇金融 AI 使用的公平、道德、问责和透明。世界银行国际征信委员会主张信用评分模型应可解释、透明、公平，教科文组织发布全球 AI 伦理标准，关注可靠性、问责制、透明度、公平性和伦理学，确保减少对消费者的潜在伤害。

数字身份证和生物识别技术

自动化的生物识别虽然简化了客户识别过程，降低了征信业风险，但仍需要有效监管和安全措施以防滥用和保护隐私。与此同时，对生物识别及数字身份的长期依赖将会导致对欺诈以及犯罪行为的忽视，并且伴随着大数据等技术的普及，生物识别技术也依然存在着潜在的歧视问题。

《数字时代可持续发展识别原则》由世界银行主导，得到联合国和多国认可，强调在提供广泛服务的同时避免歧视，通过开放标准构建可信身份。在征信机构在众多产品中使用生物识别技术的同时，生物识别协会（Biometrics Institue）也在生物识别技术领域制定了伦理原则，强调尊重生物特征所有权和个人数据，考虑公共利益、社区安全和个人净利益。这些原则集合体现了数字时代伦理和可持续发展的核心价值。

云计算

随着数据迁移到云平台，由于不同司法管辖区的数据法规不同，征信机构可能面临网络治理方面的种种挑战。伴随网络攻击、数据安全和合规风险，安全漏洞可能导致个人信息泄露，因此确保云服务商数据安全至关重要。

国际证券委员会的外包原则强调适当尽职调查云服务提供商，签订法律约束力合同，建立信息和服务保护措施，确保机密信息和数据安全，有效管理风险，确保监管和审计机构获取必要信息，规定明确的退出战略。

区块链技术

分布式记账技术（DLT）提供去中心化、开放和无须许可的服务，这是行业监管空白，尤其是在无法认定主要责任人的情况下其弊端尤为突出。

同时，DLT 创建了一个不可变的数据库，这是它的主要优点之一，也是它的主要缺点。不可变的数据库意味着信息一旦存储，就不能

被删除，任何更新都会被永久记录。

国际电信联盟（ITU）提出应对 DLT 监管挑战的建议，包括确保分布式控制和账本共享，设立链上争议解决工具，加强消费者保护。同时，强化密码学标准、避免明文数据存储、采用零知识证明、进行数据保护影响分析，以对抗篡改。在数字资产方面，制定互操作性规范，并调整 DLT 协议的透明度，以符合相关行业及地区规定。

新技术负责任使用的十项原则

为确保在征信业务活动中负责任地应用技术，国际征信委员会提出十项原则。通过采纳这些原则，征信行业可以最佳、最负责任地采用颠覆性技术，以造福所有利益相关方。考虑到征信系统会随着技术进步而不断演进，这些原则的目标是确保在征信活动中使用的所有技术类型都能达到这一目标，而不仅仅是特定技术或特定类型的征信机构。具体如下：

公平性原则

1. 征信系统要确保技术应用公平，不歧视个体、消费者群体或中小企业。

2. 保证技术解决方案和征信机构的公平性，包括实质上和程序上的公平。

3.AI/ML 技术使用不得偏袒个人或受保护群体，需要通过预处理技术确保系统基础数据无偏差。

4. 建立评分模型治理框架和 AI/ML 特定风险管理框架，确保评分的公平性。

道德性原则

1. 征信机构要确保使用的所有技术符合其企业价值观、行为准则和最高道德标准。

2. 建立和保持最高水平的道德标准，包括行为准则和以人为本的企业价值观。

3. 尊重个人尊严和平等权利，以为人类服务为目的使用技术。

问责制原则

1. 征信系统参与者应对使用的技术负责，建立相应的治理机制，监督技术驱动型产品的流程。

2. 建立内部问责机制，对 AI/ML 系统进行测试、监控、审批和授权。

3. 提高 AI/ML 系统可解释性、可追溯性和可审计性，允许独立第三方进行评估。

透明性原则

1. 向公众披露征信业务活动、技术政策、道德价值观和行为准则。

2. 向公众公开 AI/ML 系统的运用、影响以及风险防控措施。

3. 向数据主体解释决策的基础因素，提供足够的解释说明。

安全稳健性原则

1. 建立适当的数据安全管理框架，确保信息的保密性、完整性和可用性。

2. 加强数据管理的控制和风险防范措施，防范潜在风险。

3.AI/ML 系统应是可验证的和安全的，可防范攻击和漏洞。

合法性原则

1. 确保数据和技术的使用符合相关法律法规和行业标准。

2. 采取合法手段获取、收集、分析、处理和使用数据。

3.具备有效的合规职能，确保技术使用符合相关法规。

隐私性原则

1. 在数据的访问、收集、分析、处理和对外提供中保护数据主体的隐私。

2. 建立有效的数据治理框架，评估隐私风险和益处。

3. 遵循最小化原则，实施强有力的技术和组织保障措施。

可持续性原则

1. 技术的使用应有利于

人类福祉，具有可持续性。

2. 评估技术发展和运用对可持续性和环境的影响。

3. 分布式存储技术的使用要优化资源和能源的消耗，降低对环境的影响。

包容性原则

1. 征信系统的技术创新不得导致或加重对任何个人或群体的排斥。

2. 征信机构进行技术创新应采用包容性技术，确保产品设计能够服务所有消费者群体，特别是弱势群体。

> ***征信系统的技术创新不得导致或加重对任何个人或群体的排斥。***

3. 在模型设计和 AI/ML 系统使用过程中，特别关注纳入服务水平较低的经济部门的数据集。

4. 数字识别系统应服务于所有客户，不能因个人身体特征或读写水平等个人属性拒绝服务，确保收集的资料符合人权保护要求。

可信赖原则

1. 征信系统采用的技术应当被数据主体和金融机构等利益相关方所信任。

2. 新技术引入不应损害征信系统的可靠性和可信度，应提高效率而不损害服务质量。

3. 在新技术实施之前，需要关注和预测最终用户的感受，尤其考虑到征信业对金融部门的关键性作用。

关于在实务中落实上述原则的进一步探讨

在应用过程中，上述原则并非僵化的规则，而是应随实际情况在整个组织内调整的指导方针。它们不仅需要征信机构的领导层和整个行业的共同努力，还需要持续努力理解技术的影响，最大限度地提高技术的效益，公正分配利益和责任，并采用多元视角解决困难和冲突。

征信机构领导层的责任是确保这些原则得到遵守，通过评估现状、识别改进点，并公开传达合规评估的结果来实现。评估的责任可以由道德委员会、类似机构或外部评估承担，他们应基于明确定义的问题收集必要的事实依据，从而形成对每个原则的结论。

在特定技术方面，比如 AI/ML 算法、数据使用、数据治理等，评估人员应关注各项原则的实际应用。例如，在模型设计中，要确保 AI/ML 模型适用且符合道德，开发团队接受培训并具有多样性。对于数据使用，需确保数据合法、正当，并采取预防措施来识别和消除潜在的敏感数据。在数据治理方面，关注数据质量、准确性，并评估和管理风险。模型文档、结果分析、控制、调试和监控等方面也有相应的问题需要关注。

能力建设是成功实施新技术的关键，需要所有利益相关者了解和接受培训。决策者和从业人员的技术熟练程度至关重要，而征信行业协会可以在技术的负责任使用方面提供支持。此外，特定技术的建议包括对 AI/ML 算法的自主程度的定义，大数据治理和风险管理准则的制定，以及生物识别系统的安全性和以人为本的设计。对第三方云服务提供商和分布式账本技术的关注也是必要的，以确保它们符合相同的道德和技术标准。

公平性和包容性原则要求征信机构定期审查其基于人工智能 / 机器学习的信用评

分模型，确保其公平性。通过维护数据映射、排除受保护属性，并使用具有包容性的数据集，模型开发团队努力确保评分的公正性。同时，对模型输出结果的跟踪和公平性审查的定期进行，有助于保证模型的可靠性和准确性，并降低可能存在的差异性影响。

道德性原则在征信机构中体现为创建道德委员会，该委员会在技术的道德原则制定和实施方面提供指导。该委员会鼓励员工提供关于技术输出偏差的反馈，以增强人们对人工智能 / 机器学习系统的信任。员工在决策时适当地参考和使用人工智能 / 机器学习模型的输出结果，有助于确保决策过程是明智和负责任的。

问责制原则涵盖了高级管理层的参与，他们为基于人工智能的决策流程制定相关的战略、指南和规则。培训关键工作人员以提高对技术使用原则的认识，并建立内部和外部审计机制，确保人工智能 / 机器学习系统的运行合乎责任。这一原则还包括确保数据主体受到伤害或不利影响时采取适当的补救措施，并鼓励第三方报告潜在的漏洞、风险或偏见。

透明性原则体现在使 AI 信用评分模型的输出结果可解释，从而提供对消费者获得低信用评分的原因的直观解释。此外，透明度也包括确保用户能够获得关于他们信用评分的详细解释，以及提供与其他类似贷款申请的比较，以增强整个流程的透明性。

安全稳健性原则涉及建立完善的数据安全标准，通过预防措施确保数据完整性和弹性。为了应对网络风险事件，强调业务连续性和编制应急方案，同时要求员工参与不断优化的培训计划，提高员工对信息安全的重视和认识。

合法性原则要求采用合法收集替代数据的数据管理标准，明确政策和流程，以确保数据与目的相关，并提供了征得消费者同意、访问和更正信息的机制。

隐私性原则包括建立数据治理标准，设置专门负责保护数据主体隐私的工作人员，采用 ISO、IEEE 等认证标准来管理数据，以及使用最少个人数据来训练模型，从而加强隐私保护。

可持续性和社会福祉原则涵盖将可持续性纳入公司战略和政策。征信活动根据可持续发展目标进行，并制定政策来衡量其技术对环境和社会的影响。这强调了征信机构在其技术实践中整合环境、社会和治理因素的承诺。

征信行业正处于十字路口，技术进步为效率、准确性和包容性提供了巨大潜力。然而，这些好处必须与围绕数据隐私、透明度和算法偏差的伦理和人权问题相权衡。

展望未来，需要各方的共同努力。监管机构、行业领导者和技术开发人员必须携手合作，建立负责任的人工智能使用的稳健框架。这包括实施有关数据收集、存储和访问的清晰准则，以及培养可解释的人工智能模型，为信用决策提供清晰的依据。最终，负责任的技术采用可以为更具包容性和公平的信用报告生态系统铺平道路。通过优先考虑公平、透明和问责制，以确保技术进步赋予个人权利，并整体加强金融体系。

□ 责任编辑：古炳鸿