 DOI: https://doi.org/10.12345/cjygl.v8i9.21091

The Current Situation, Problems and Countermeasures of Digital Social Identity management

Zhiyi Cai

City University of Hong Kong, Hong Kong, 999077, China

Abstract

The paper focuses on the current situation, problems, and countermeasures of digital social identity management. Through multidimensional analysis, it reveals the current situation of technology application, institutional construction, and social cognition, points out the main problems of information security, inconsistent standards, and regulatory difficulties, and proposes innovative measures such as building a multi-level protection system, promoting inclusive strategies, enhancing system resilience, and exploring new models of collaborative governance. Research has shown that digital identity management requires a balance between technological innovation and privacy protection, promoting social equity, improving system reliability, and establishing a multi-party governance mechanism. The paper aims to conduct an in-depth analysis of the current situation of digital social identity management, identify the main problems it faces, and propose innovative strategies to provide theoretical basis and practical guidance for promoting the healthy development of digital social governance.

Keywords

digitalization; society; identity management

数字化社会身份管理的现状、问题及对策

蔡智怡

香港城市大学，中国·香港 999077

摘　要

论文聚焦数字化社会身份管理的现状、问题及对策，通过多维度分析，揭示了技术应用、制度建设和社会认知的现状，指出信息安全、标准不统一和监管难度等主要问题，提出构建多层次保护体系、推动包容性战略、增强系统韧性和探索协作治理新模式等创新对策。研究表明，数字身份管理需要平衡技术创新与隐私保护，促进社会公平，提高系统可靠性，并建立多方参与的治理机制。论文旨在深入分析数字化社会身份管理的现状，剖析其面临的主要问题，并提出创新对策，为推动数字化社会治理的健康发展提供理论依据和实践指导。

关键词

数字化；社会；身份管理

1 引言

数字化浪潮正深刻改变着社会治理的方方面面，其中数字化社会身份管理成为关键议题。随着区块链、生物识别等新技术的广泛应用，数字身份管理面临前所未有的机遇与挑战。如何在提高管理效率的同时，保护公民隐私、促进社会公平、应对安全威胁，成为亟待解决的问题。

2 数字化社会身份管理现状分析

2.1 技术层面：区域联、生物识别等新技术的应用

在数字化社会身份管理领域，区块链技术正逐步发挥其独特优势。该技术通过去中心化、不可篡改的特性，为身份信息的存储和验证提供了新的可能性。多个国家已开始探索基于区块链的数字身份系统，如爱沙尼亚的 e-Residency 项目，通过区块链技术为全球公民提供数字身份服务，实现跨境身份认证和商业活动。生物识别技术在社会身份管理中的应用日益广泛。指纹识别、面部识别、虹膜扫描等方法不仅提高了身份验证的准确性，还大大简化了认证流程。中国在这一领域走在前列，多个城市已实现刷脸支付、刷脸进站等应用场景。然而，生物识别技术的广泛应用也引发了公众对隐私保护的担忧，如何在便利性和安全性之间取得平衡成为亟待解决的问题。人工智能和机器学习技术在身份管理系统中的应用正在深化。这些技术可以通过分析海量数据，识别潜在的身份欺诈行为，提高身份验证的准确性和效率。例如，一些金融机构已经开始使用 AI 算法来分析客户的行为模式，实时检测异常交易，从而有效防范身份盗用和金融欺诈。然而，AI 技术的应用也带来了算法偏见等新的挑战，

【作者简介】蔡智怡（2001–），女，中国河南夏邑人，硕士，从事大数据社会公共人力资源管理研究。

需要在技术发展的同时加强伦理约束和监管。

2.2 制度层面：相关法律法规和政策的制定与实施

数字化社会身份管理的法律法规框架正在逐步完善。欧盟于 2016 年实施的《通用数据保护条例》（GDPR）为个人数据保护设立了全球标杆，明确了数据主体的权利和数据控制者的责任。该法规对数字身份管理产生了深远影响，促使全球范围内的组织重新审视其数据处理实践。中国在数字身份管理法规方面也取得了显著进展。2021 年实施的《中华人民共和国个人信息保护法》为数字时代的个人信息保护提供了法律依据，规定了个人信息处理的基本原则和规则。此外，《网络安全法》《数据安全法》等法律的出台，进一步完善了数字社会的法律体系，为数字身份管理提供了制度保障。在政策层面，多个国家已将数字身份管理纳入国家战略。印度的 Aadhaar 计划是全球最大规模的生物特征识别系统，为超过 12 亿印度公民提供了唯一的数字身份。该计划不仅提高了政府服务的效率，还促进了金融普惠。然而，Aadhaar 也面临着隐私保护和数据安全的挑战，引发了社会各界的广泛讨论。这些实践经验为其他国家制定数字身份政策提供了宝贵参考。

2.3 社会层面：公众对数字身份的认知与接受度

公众对数字身份的认知和接受度呈现出复杂的态势。一方面，数字化带来的便利性得到了广泛认可。移动支付、在线身份验证等服务大大简化了日常生活中的身份认证流程，提高了效率。调查显示，超过 70% 的用户认为数字身份服务改善了他们的生活质量。特别是在新冠疫情期间，数字身份在远程工作、在线教育等领域发挥了关键作用，加速了公众对数字身份的接受。另一方面，随着数据泄露事件的频发，公众对数字身份安全的担忧日益加剧。2018 年，Facebook-Cambridge Analytica 数据泄露丑闻暴露了大规模数据滥用的风险，引发了公众对个人数据保护的广泛讨论。这一事件不仅影响了公众对社交媒体平台的信任，也让人们开始反思数字身份的脆弱性。调查显示，超过 60% 的用户担心自己的数字身份信息可能被盗用或滥用。数字素养的差异也导致了公众对数字身份的接受度存在显著差异。年轻一代普遍表现出对数字身份的高度接受和熟练使用，而老年群体在适应数字化身份管理时面临较大困难。这种“数字鸿沟”不仅体现在年龄上，在城乡、不同教育水平群体之间也存在明显差距。如何缩小这一差距，确保数字身份管理的普惠性，成为政策制定者面临的重要挑战。

3 数字化社会身份管理面临的主要问题

3.1 信息安全与隐私保护的困境

数字化社会身份管理面临的最严峻挑战之一是信息安全与隐私保护。随着个人信息数字化程度的提高，数据泄露的风险与日俱增 [1]。2019 年，一家主要信用报告机构遭遇数据泄露，影响了 1.47 亿美国消费者，暴露了现有数据保护措施的脆弱性。这类事件不仅造成直接经济损失，还严重损害了公众对数字身份系统的信任。隐私保护方面，数字身份管理系统面临着如何平衡信息共享与个人隐私的难题。过度收集和使用个人数据可能导致隐私侵犯，而信息不足又可能影响服务质量和安全性。

3.2 身份认证标准不统一

身份认证标准的不统一是数字化社会身份管理面临的另一个重要问题。不同国家、地区甚至不同机构之间采用的身份认证标准和技术各不相同，导致身份信息难以互通和互认。这种标准的碎片化不仅增加了系统开发和维护的成本，也给用户带来了诸多不便。跨境身份认证尤其面临挑战。在全球化背景下，国际旅行、跨国商务活动日益频繁，但各国数字身份系统的互操作性不足，导致用户需要多次进行身份认证。如何建立全球认可的数字身份标准，实现跨境身份互认，成为国际社会面临的重要议题。

3.3 监管难度加大

数字化社会身份管理的快速发展给监管带来了前所未有的挑战。技术创新的速度往往超过了法律法规的制定速度，导致监管存在滞后性 [2]。例如，区块链技术的去中心化特性使得传统的中心化监管模式面临挑战，如何在保护隐私的同时确保必要的监管，成为一个棘手问题。此外，数字身份管理涉及多个领域和部门，如何协调不同利益相关方，建立有效的监管机制，也是一大难题。例如，在处理跨境数据流动时，各国法律法规的差异增加了合规的复杂性。一些跨国公司发现自己陷入了遵守一国法律可能违反另一国法规的困境。如何在全球范围内建立协调一致的监管框架，平衡创新、安全和隐私保护，成为各国政府和国际组织面临的重要课题。

4 数字化社会身份管理的创新对策

4.1 构建多层次的数字身份保护体系

构建多层次的数字身份保护体系是应对当前挑战的关键策略。这一体系应涵盖技术、法律和伦理三个维度，形成全方位的保护网络。在技术层面，加密技术的创新至关重要。零知识证明（Zero-Knowledge Proof）技术为保护隐私提供了新的可能性，它允许在不泄露具体信息的情况下证明某一声明的真实性。例如，荷兰的数字身份系统 IRMA 就采用了这一技术，使用户能够选择性地披露身份信息，大大降低了隐私泄露的风险。法律层面需要建立更加细化和灵活的规范体系。欧盟的《通用数据保护条例》（GDPR）为个人数据保护树立了新标准，但在实施过程中也暴露出一些问题。针对这些问题，可以考虑引入“分级管理”的概念，根据数据敏感程度和使用场景制定差异化的保护措施 [3]。例如，对于高度敏感的生物识别数据，可以要求采用更严格的加密和存储标准，并限制其使用范围。同时，建立动态调整机制，使法规能够及时响应技术发展和社会需求的变化。在伦理层

面，需要建立数字身份管理的伦理准则。这不仅涉及隐私保护，还包括公平性、透明度和问责制等方面。可以借鉴医疗伦理委员会的模式，成立专门的数字伦理委员会，对数字身份管理的重大决策进行伦理审查。新加坡政府在推广人工智能应用时，就设立了专门的伦理委员会，为 AI 在各领域的应用制定伦理指南，这一做法值得借鉴。

4.2 推动包容性数字身份战略

推动包容性数字身份战略是缩小数字鸿沟、实现社会公平的重要举措。这一战略的核心在于确保所有社会群体都能平等地获取和使用数字身份服务，不因年龄、教育程度、经济条件或身体状况而被排斥在数字社会之外。实现这一目标需要从教育、技术和政策三个方面着手。在教育方面，普及数字素养教育是关键。可以借鉴爱沙尼亚的做法，将数字技能教育纳入国民教育体系，从小学开始培养学生的数字能力。对于成年人，特别是老年群体，可以通过社区学习中心、移动教育站等形式提供针对性的培训。技术层面需要开发适应性强的身份认证方式。传统的密码认证对于某些群体来说可能存在困难，因此需要探索更加直观、易用的认证方式。例如，印度的 Aadhaar 系统采用了生物识别技术，使得即便是文盲群体也能方便地进行身份认证。然而，在推广生物识别技术时，需要充分考虑隐私保护和文化敏感性。对于残障人士，可以开发特殊的辅助技术，如语音控制、眼动追踪等，确保他们能够平等地使用数字身份服务。在政策层面，建立数字身份援助机制非常重要。这包括为经济困难群体提供免费或低成本的数字设备和网络接入，以及设立专门的数字身份服务站，为不熟悉数字技术的群体提供面对面的帮助。肯尼亚的 M-PESA 移动支付系统就通过广泛的代理网络，使得即便是偏远地区的居民也能方便地进行身份验证和金融交易。

4.3 增强身份管理系统的韧性

增强身份管理系统的韧性是应对技术依赖性增强和系统脆弱性的关键策略。韧性强的系统能够在面对各种挑战和威胁时保持稳定运行，并快速恢复。实现这一目标需要从系统架构、数据管理和应急响应三个方面入手。在系统架构方面，发展分布式身份管理架构是提高系统韧性的有效方法。区块链技术为此提供了新的可能性。例如，加拿大政府正在探索基于区块链的数字身份系统，通过去中心化的方式存储和验证身份信息，大大降低了单点故障的风险。数据管理方面，提高系统间的互操作性至关重要。这不仅能提高系统效率，还能增强整体韧性。欧盟的 eIDAS 规则为跨境电子身份认证提供了框架，促进了成员国之间身份系统的互操作性。借鉴这一经验，可以建立国内不同部门和地区之间的数据共享机制，在保护隐私的前提下，实现身份信息的有效流通和验证。同时，采用数据冗余和备份策略，确保在部分系统出现故障时，仍能维持基本的身份验证功能。构建应急响应机制是增强系统韧性的另一关键环节，包括：建立实时监控系统，及时发现和响应潜在威胁；制定详细的应急预案，明确各方职责和处置流程；定期进行应急演练，提高相关人员的应对能力。

4.4 探索协作治理新模式

探索协作治理新模式是应对数字身份管理复杂性增加的有效策略。传统的自上而下的管理模式已难以应对日益复杂的数字社会需求，需要建立一个多方参与、协同合作的治理框架。这一框架应包括政府、企业、学术机构和公民社会组织等多个利益相关方，通过共同参与决策和监督，实现更加透明、公平和高效的数字身份管理。在实践中，可以借鉴多利益相关方互联网治理模式的经验。例如，互联网名称与数字地址分配机构（ICANN）就采用了这种模式，通过定期的公开会议和工作组，让各方共同参与互联网关键资源的管理。引入第三方监管机制是协作治理模式的重要组成部分。独立的第三方机构可以提供客观、公正的监督和评估，增强公众对数字身份管理系统的信任。英国的信息专员办公室（ICO）就是一个很好的例子，它作为独立的监管机构，负责监督个人数据的使用，并有权对违规行为进行处罚。在数字身份管理领域，可以考虑设立类似的专门机构，负责审核身份验证系统的安全性和隐私保护措施，处理相关投诉，并定期发布评估报告。

5 结语

数字化社会身份管理是一个复杂的系统工程，需要技术、法律、伦理等多领域的协同创新。论文提出的多层次保护体系、包容性战略、系统韧性增强和协作治理新模式等对策，为应对当前挑战提供了新的思路。然而，数字化进程是动态演进的，未来还将面临新的挑战。我们需要持续关注技术发展趋势，及时调整管理策略，在保护个人权益与促进社会发展之间寻求平衡。

参考文献

[1] 唐三幸.论数字化社会“身份信用卡”的构建及广域作用[J].零陵师范高等专科学校学报,2002(2):40-41.

[2] 饶钰玮.数字政府背景下公民身份管理研究[D].广州:华南理工大学,2021.

[3] 陈爱丹.公共事业单位人力资源管理创新分析[J].商业文化,2021(32):78-79.