第 51 卷第 5 期
2024 年 9 月
Vol. 51, No. 5
September, 2024

四川师范大学学报(社会科学版)
Journal of Sichuan Normal University
(Social Sciences Edition)

去中心化背景下数字身份识别的法律风险及其应对

靳梦戈

摘要:数字身份是数字化时代对个体传统身份的突破和超越的产物,是以数字化方式呈现的身份样态,具有唯一性与可验证性、动态性与跨界性、私有性与匿名性的特征。以用户自主控制身份数据为核心理念的去中心化身份识别技术已成为当下数字身份管理识别的主流。然而,去中心化背景下数字身份识别存在隐私与数据安全、身份盗用与身份欺诈、法律监管以及跨境数据流动等风险。构建安全、可靠、高效、公平的数字身份识别体系,应当注重激励隐私保护并强化数据安全规定,建立数字身份的法定技术标准,构建法律与技术相均衡的协调机制,推进数字身份国际合作的法律协调。

关键词:数字身份;去中心化;身份识别;数据安全;隐私保护

DOI: 10.13734/j.cnki.1000-5315.2024.0313

收稿日期:2024-04-25

基金项目:本文系国家社会科学基金重大项目"国家纵向治理体系化和法治化若干重大问题研究"(20&ZD159)的阶段性成果。

作者简介:靳梦戈,女,山西晋城人,山东大学法学院(威海)博士研究生,E-mail: 912592283@qq.com。

在传统熟人社会中,人的身份依靠社会交往的人际关系予以证明;在计算机时代,人的身份依靠公权力机构提供的身份证、护照等法定证件予以证明①。随着人类迈入"万物数字化、一切可计算"的信息新时代②,这种数字化浪潮剧烈地改变着人们的生活方式和存在样态,并对建立在传统物理世界基础上的身份识别观念产生了巨大的影响和冲击③,传统的身份识别方式(如身份证、驾驶执照等)在数字世界中面临诸多限制,促使了数字身份识别技术的快速发展。虽然数字身份识别技术及其相关应用已经得到了较为广泛的研究,但学界多数研究都集中在如何提高识别准确性或如何保护用户隐私等方面。未来,随着技术的不断进步和法律法规的逐步完善,数字身份识别将在保护个人隐私、提高交易效率等方面发挥更大作用。对于这一技术可能引发的法律风险及其应对措施,学界还缺乏比较系统和全面的研究。本文将在去中心化的背景下,以全新的视角探讨去中心化技术在数字身份识别中的应用,分析其法律风险,并提出针对性的应对措施。

一 数字身份的内涵及其可识别性

数字身份是对传统物理身份的迭代。在数字化时代,数字身份作为在数字社会中生存主体的重要表征,是了解个体与数字世界互动的关键,同时也是主体进入网络社交的基本门槛和准入凭证④。因此,理解数字身份的内涵、识别特征、发展演变以及识别技术,对于把握其在当代社会中的角色至关重要。

(一)数字身份的内涵

①金鸿浩《非法获取型数据犯罪的实务反思与规则重塑》,《中国政法大学学报》2023 年第 4 期,第 133 页。

②马长山《算法治理的正义尺度》,《人民论坛·学术前沿》2022 年第 10 期,第 68 页。

③郑智航《数字人权的理论证成与自主性内涵》,《华东政法大学学报》2023 年第 1 期,第 35 页。

④董兴彬、吴满意《思想政治教育主体数字身份:构成、认同及其价值》,《理论导刊》2024 年第 2 期,第 114—115 页。

身份是识别自我和其他主体的特定标识[①]。数字身份是指以数字化方式呈现的身份,是个体在数字空间中的唯一标识,通过一组电子数据涵盖了个人的基本信息、在线行为、社交网络互动等多维度信息。基于身份观念的复杂性,数字身份具有身份识别、身份认同和数字化身的多元面向[②]。它不仅是网络空间进行交易、社交、学习和工作的虚拟凭证,也是现代数字经济和社会运作的基石。与传统身份相比,数字身份具有明显的动态性和选择性特征,能够反映个体在数字空间中的行为变化和社交互动,具有更强的时效性和个性化特点。而传统身份通常依赖于静态的、非选择性的要素,如姓名、籍贯、性别等,这些要素大多在个人出生或成年早期确定,难以改变。

数字身份与传统身份的核心区别在于其构成元素的动态性和复杂性。数字身份的崛起意味着人与人之间的关系不再局限于特定的物理空间,在数字世界里,个体的身份不仅包括传统意义上的基本属性,还扩展到了个人的在线活动、偏好设置、交互数据等。这些数据是可变的,可以根据个人的活动和环境的变化而更新,从而使数字身份能够更准确地反映个体当前的状态和行为模式。此外,与传统身份依赖于政府或权威机构的颁发和认证不同,数字身份的建立和认证通常依赖于数字技术,如密码学、区块链和生物识别技术等,其认证过程和管理机制需要新的法律规范和技术标准来保障。总之,数字身份是对传统物理身份的重要补充和扩展,它通过整合个体在数字空间的多维度信息,提供了一种更为灵活且动态的身份识别方式。这种转变不仅影响了个人的社交互动和经济活动,也对法律制度和社会治理提出了新的要求和挑战。

(二)数字身份的可识别性特征

随着数字化生活的发展,越来越多的社会资源、社会关系均已迁移到网络场域,各种性质、功能和形态各异的网络场域是维系数字化生存的基本载体[③],数字身份的应用日益成为人们关注的焦点。与传统身份识别方式相比,数字身份具备了多样化的特征和功能,不仅体现了数字技术的进步,也代表了社会治理和个人隐私保护方法的变革。特别是在去中心化环境下,数字身份的可识别性特征变得更为复杂和多维,具有唯一性与可验证性、动态性与跨界性以及私有性与匿名性等属性,这些属性共同构成了数字身份的核心特征,并且在确保个人数据的安全性、促进跨域服务的整合以及保障用户隐私等方面发挥了至关重要的作用。

1.唯一性与可验证性

数字身份的唯一性,是指在数字环境中,每个身份标识符都是独一无二的,确保了每个主体在网络空间的独立性和不可替代性。这种唯一性的建立基于复杂的算法和加密技术,以确保每个数字身份的独特性不能被复制或重复使用。在去中心化的身份系统中,唯一性不仅是身份验证的前提,也是维护系统完整性和防止身份被盗用的关键。数字身份的可验证性,指其真实性和合法性可以通过技术手段进行验证。在传统的中心化系统中,这种验证通常依赖于中心服务器或认证中心的确认。而在去中心化系统中,可验证性通过使用公钥基础设施(Public Key Infrastructure,PKI)[④]、数字签名等加密技术实现,任何人都可以验证数字身份的真实性而无须依赖第三方机构。这种机制大大增强了系统的安全性和透明度,但同时也对加密技术和算法安全性提出了更高的要求。

2.动态性与跨界性

数字身份的动态性,体现在其能够反映和适应主体在数字空间中的行为和属性的变化。这不仅包括基本信息的更新,如地址变更、职务变动等,还涉及到信誉评分、交易历史、行为习惯等更为复杂的维度。动态性要求数字身份管理系统具备高度的灵活性和适应性,能够实时更新和维护身份信息,确保信息的准确性和时效性。数字身份的跨界性,则指其可以跨越不同的平台、网络和应用进行识别和验证。这种特性在促进信息共享和服务整合方面具有重要价值,但同时也带来了安全性、隐私保护和数据一致性的挑战。在去中心化的身份系统中,跨界性的实现依赖于标准化的协议和互操作性机制,从而使得不同系统间的身份信息可以安

①武文颖、王鑫《数字身份构建的伦理困境及其超越》,《学习与实践》2023年第6期,第30页。

②陆青《数字身份的多元面向及其法律保护》,《社会科学辑刊》2022年第6期,第77页。

③管其平《数字化生存中的时空逻辑、时空剥夺及其时空权利》,《昆明理工大学学报(社会科学版)》2022年第1期,第133页。

④PKI使用公钥理论和技术为用户提供安全服务,将用户公钥与身份信息绑定在数字证书中,实现了大规模网络环境中可靠的信息交换与身份认证。参见:黄保华等《基于MPT索引的高效链上PKI模型》,《信息网络安全》2022年第8期,第73页。

全、高效地共享和验证。

3. 私有性与匿名性

数字身份的私有性或称隐私性，是指个体具有在数字环境中控制自己的个人信息并决定这些信息如何被收集、使用和分享的属性。它涉及到个人数据的各个方面，包括但不限于个人身份信息、位置数据、通信记录、在线行为习惯等。私有性保护的核心是赋予个体对自己信息的控制权，确保个人信息只在用户明确同意的情况下才能被访问和使用，采取适当的安全措施保护个人信息不被未授权访问、泄露或滥用。数字身份的匿名性，是指在进行数字活动时，个体的身份不被揭露或不与其真实身份直接关联。匿名身份认证是指用户在注册过程中无须提供身份信息便可以获得身份标识并用于系统认证①。通过匿名性机制，用户可以在网络上发表意见、进行交易或参与活动，而不必担心个人身份信息的泄露。匿名性的关键在于隐藏或掩盖个人身份的标识符，利用加密技术和匿名通信协议（如 Tor 网络②）保护用户在网络上的活动不被追踪，使得个人行为不能轻易地被追溯到特定的个体。因此，对于某些网络安全事件而言，用户身份匿名性阻碍了对该事件的追踪溯源③。

（三）数字身份识别方式的演变

数字身份识别是指通过数字化手段验证和管理个体在数字空间中的身份标识过程。随着数字化时代的深入推进，数字身份识别方式也在不断演变与革新。这一变革不仅反映了技术的飞速发展，更彰显了社会对身份识别安全性、便捷性、隐私保护的多重需求。数字身份作为个体在数字空间中的标识与表征，其产生及发展与数字技术密切相关，经历了较为长期的演化过程，其识别方式经历了从简单认证到复杂验证、从中心化到去中心化的转变。

1. 简单认证的初始阶段

在早期的互联网和数字技术应用中，数字身份通常为用户名和密码的组合，这种识别机制易于实现，但随着互联网的普及和数字交易的增加，其安全性和功能性的局限逐渐显现。简单的认证识别机制无法有效地防止身份盗窃、欺诈等问题，黑客通过各种手段获取用户的登录信息，从而进行未经授权的访问和操作，这不仅威胁到用户的隐私和数据安全，还可能导致严重的经济损失。而且，简单认证机制缺乏对用户行为的跟踪和分析能力，无法提供个性化的服务。用户必须在每个平台上重复输入凭证，增加了操作的复杂性和不便性。这种认证机制也无法有效区分合法用户和恶意行为者，限制了用户高级安全需求的实现。

2. 多因素认证与整合身份管理的发展阶段

为了解决安全性和功能性的问题，数字身份管理引入了多因素认证（Mult-Factor Authentication, MFA）机制，如短信验证码、电子邮件确认、生物识别等，与单一的用户名和密码不同，MFA 要求用户在登录时提供多个独立的凭证，大大增加了黑客破解的难度。同时，随着互联网服务的增多，用户需要在多个平台和服务中认证自己的身份，这促进了整合身份管理（Identity and Access Management, IAM）系统的发展。IAM 系统通过提供单一登录（Single Sign-On, SSO）等功能，使用户能够使用一组凭据访问多个系统和服务；通过集中管理和监控用户访问权限，能够及时检测和处理潜在的安全威胁，并确保用户数据的安全。

3. 区块链与去中心化身份识别技术的转型阶段

随着区块链技术的兴起，数字身份识别迎来了转型。与传统分布式网络相比，区块链更多关注如何自治、平等、安全地实现网络服务④，通过提供去中心化的数据管理框架，使得数字身份能够在去中心化、不可篡改的分布式账本上进行注册和验证。这种去中心化身份（Decentralized Identity, DID）识别技术，不仅提

---

①参见：李馥娟、马卓、王群《区块链系统身份管理机制研究综述》，《计算机工程与应用》2024 年第 1 期，第 64 页。

②Tor（The onion route）是指通过采用不定数量节点、不定路由建立通信链路，并且在通信过程对通信数据进行层层加密，从而保证数据通信过程的隐蔽、匿名和防溯源性。参见：龙军、王轶骏、薛质《重要 Tor 暗网站点的验证码快速识别和数据采集》，《计算机应用与软件》2022 年第 7 期，第 315 页。

③Gautami Tripathi, Abdul A M, and Sathiyarayanan M, "The Role of Blockchain in Internet of Vehicle (IoV): Issues, Challenges, and Opportunities," In *2019 International Conference on Contemporary Computing and Informatics* (IC3I, Singapore, 2019), 26-31.

④斯雪明、潘恒、刘建美、祝卫华、姚中原《Web3.0 下的区块链相关技术进展》，《科技导报》2023 年第 15 期，第 37 页。

高了身份管理的安全性和透明度,而且赋予了用户对自己身份数据的控制权。在这种模式下,用户可以自主管理自己的身份信息,选择性地与服务提供者共享必要的数据,有效地保护了个人隐私。

4.人工智能与智能合约的未来趋势

未来,数字身份的发展将更加依赖于人工智能(Artificial Intelligence, AI)和智能合约技术。AI能够通过分析用户行为、交易模式等数据,提供更为精准的身份验证和个性化服务。智能合约则可以在满足预设条件时自动执行合约条款,为数字身份的使用提供了新的可能性,比如自动化的信用评估、权限管理等。此外,在区块链的PKI中,每个存储的证书都不能被丢弃或卸载,但智能合约允许用户替换自己的证书或存储的信息,而不会影响以前存储的数据①。

(四)数字身份监管技术的发展

探讨去中心化背景下数字身份识别的法律风险及其应对策略,关键在于理解中心化身份识别技术与去中心化身份识别技术在核心理念、管理架构及其安全性能上的根本差异。这些差异不仅影响着技术实施的可行性和效率,也涉及到隐私保护、数据安全、法律责任等多个方面。

首先,在核心理念层面,中心化身份识别技术依靠一个受信任的中心机构去维护一个全面的、可靠的身份数据库的支持,个人或实体必须通过这个中心机构来验证他们的身份信息。例如,银行可能需要通过政府数据库来验证个人的社会保障号码,或者在线平台可能要求用户通过电子邮件验证来确认其身份。而去中心化身份识别技术则是对数字身份管理的一次重大革命,其核心理念是赋予用户对自己身份数据的完全控制权②,从根本上改变了传统的中心化身份验证机制。

其次,在管理架构层面,传统的中心化身份识别技术建立在一个核心的权威机构或机构集群上,这些机构负责管理和存储个人身份信息。这种机制在许多国家的政府机构、金融服务和在线服务提供商中被广泛采用。与之不同的是,去中心化身份识别技术不再存储于任何单一的中心化数据库中,而是分布式地存储在区块链上,赋予每个用户独立控制和使用数字身份的能力,确保了数据的不可篡改性和持久性。去中心化身份识别技术没有单一的管理主体,由网络的多个节点共同地维护和验证,从而实现身份信息的去中心化管理。

最后,在安全性能方面,中心化身份识别技术将用户的身份信息集中地存储于单一的数据库中,这种方式虽然便于管理,但同时也集中了风险。例如,中心化身份识别技术的隐私保护依赖于中心机构的安全措施,这种依赖关系使得用户隐私保护存在潜在风险。此外,在应对法律风险的能力上,中心化身份识别技术将风险集中于中心机构,使得责任更为明确,但这也可能导致在遇到法律问题时整个系统陷于被动停滞。而去中心化身份识别技术通过在网络的多个节点上分散地存储身份信息,极大地增强了数据的安全性和可靠性。具体而言,去中心化身份识别技术使得个人身份信息的存储变得透明而安全,同时也提高了数据的抗审查性。用户通过持有与其数字身份关联的一对密钥(公钥和私钥)来管理自己的身份信息。公钥广泛分布,而私钥则由用户安全保管,未经用户授权,任何人都无法访问或更改用户的身份信息。例如,去中心化身份识别技术通过加密和匿名机制,让用户能够更好地控制自己的身份信息,从而有效地减少了隐私泄露的风险。此外,去中心化身份识别技术的法律风险则分散于网络的多个节点,虽然这使得法律责任的界定更为复杂,但同时也保证了单一节点问题不会影响到整个系统的运行。

综合而言,中心化身份识别技术与去中心化身份识别技术从生成理念到实践运用等多个维度存在着本质区别。这些差异不仅对技术选择有着重要影响,也对确保数字身份识别的法律风险得到有效应对提出了挑战。

二 数字身份识别面临的法律风险

数字技术与现实社会的深度融合,在传统的物理空间之外发展出无限延展的虚拟空间,由此形成虚实同

①B. K. Mohanta, S. S. Pan, D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," In *2018 9th International Conference on Computing, Communication and Networking Technologies* (ICCCNT, Bengaluru, India, 2018), 1-4.

②李馥娟、马卓、王群《区块链系统身份管理机制研究综述》,《计算机工程与应用》2024年第1期,第62页。

构的双层社会架构[①]。数字身份识别技术作为现代信息社会的核心技术，既是实现数字化转型的关键推动力，也随之产生了一系列复杂的法律与伦理问题。去中心化作为一种技术和管理理念，虽然在提升系统透明度、增强用户自治方面具有显著优势，但同时也带来了一系列法律风险。包括但不限于去中心化背景下的数字身份识别，面临着用户隐私权和数据安全、身份盗用与身份欺诈、法律监管及跨境数据流动等风险。

（一）隐私泄露与数据安全的挑战

大数据的追溯功能创造了空间和时间“圆形监狱”的幽灵[②]，使每个人都深陷在这个由大数据构成的监狱中，受到抽丝剥茧般的严密监控，任何一点隐私的信息，都会成为大数据的一个片段，最后被整合成人们的数字身份[③]。去中心化系统尽管以其较高的安全性获得推崇，但并非绝对安全，其中技术漏洞的存在为黑客攻击提供了机会，使他们取得存储在去中心化网络中的敏感信息。这些漏洞可能出现在智能合约的编码中，或因区块链平台本身的安全缺陷而产生。尽管去中心化网络提供了一定程度的匿名性，但通过交易行为和模式的分析，恶意分子可能追踪到特定用户的身份及其进行中或已完成的活动。去中心化的特性使得一旦信息被上传至区块链，就很难被删除或撤回，这也会对用户的数据删除权带来挑战。

去中心化系统的数据保护面临的挑战主要源自传统法律框架与去中心化技术之间的适应性差异。首先，当前大多数数据保护法律，如欧盟的通用数据保护条例（General Data Protection Regulation，GDPR），是基于中心化数据处理模式设计的，使得这些法律难以直接适用于去中心化的数据处理环境。例如，GDPR规定了数据处理者和数据控制者的责任和义务，但在去中心化系统中，由于缺乏明确的数据控制者，这些规定难以实施。而且，从全国性立法层面来看，我国也并未对数据确权作出回应[④]。其次，区块链网络所有用户共享一个公共区块链，不会存在因为单点失效而导致系统故障的情况，因此，除掌握区块链网络51%的算力能够进行信息修改外，区块链网络可以被视为是绝对安全的[⑤]。这表明，数据安全可能面临51%攻击，这种攻击虽在大型网络中难以实施，但理论上是能够篡改区块链信息、影响数据完整性的。最后，中间人攻击（Man in The Middle Attack，MiTM）[⑥]可能在数据传输过程中发生，尤其是当通信未充分加密时，中间人可截获并篡改数据。重放攻击和时间戳攻击则分别通过重新发送交易信息和操纵时间戳来欺骗网络和影响交易顺序，威胁网络的完整性。

（二）身份盗用与身份欺诈的风险

去中心化背景下，个人身份盗用和欺诈的具体情形及所面临的风险和挑战展现出了明显的多样性和复杂性。身份盗用指的是不法分子通过非法手段获取他人的身份信息，并在未经他人同意的情况下，冒充他人进行各种活动。在去中心化的数字身份系统中，身份盗用包括但不限于私钥的窃取、身份证明文件的伪造等行为，其动机主要包括经济利益的获取、逃避法律制裁、破坏和干扰系统正常运行等。因此，设计新颖、安全的身份认证方案至关重要[⑦]。

首先，私钥的安全问题是去中心化系统中身份安全的核心。用户的数字身份和访问权限几乎完全依赖于私钥，其安全性直接关系到身份安全。私钥一旦被盗或丢失，攻击者便能轻易冒充身份主体，获得对其数字资产、个人信息和服务的无限制访问权。这使得个人身份被盗用的风险极高，攻击者可能利用被盗身份进行各种欺诈活动，如非法转移资产、发布虚假信息等。

其次，智能合约的安全问题日益凸显，成为亟待解决的重要课题。智能合约是一种执行合约条款的计算

①马长山《智能互联网时代的法律变革》，《法学研究》2018年第4期，第21页。

②维克托·迈尔－舍恩伯格《删除：大数据取舍之道》，浙江人民出版社2013年版，第117页。

③董军、程昊《大数据时代个人的数字身份及其伦理问题》，《自然辩证法研究》2018年第12期，第77页。

④王利明《数据何以确权》，《法学研究》2023年第4期，第56页。

⑤何沛军、郭志远《有机融合与双向升级：区块链技术下的个人信息保护研究》，《广西社会科学》2023年第9期，第139页。

⑥中间人攻击是一种间接的入侵攻击，攻击者通常窃取合法用户拥有的唯一身份证、密码、密钥和其他敏感数据。参见：闫青乐、朱慧君《基于区块链智能合约的大数据安全》，《计算机应用与软件》2023年第12期，第336页。

⑦M. Hussain, A. Mehmood, S. Khan, et al., “Authentication Techniques and Methodologies Used in Wireless Body Area Networks,” *Journal of Systems Architecture* 101 (October 2019): 1-28.

机交易协议,它是区块链 2.0 的代表性技术,允许无第三方的可信交易,交易可追溯且不可逆①。去中心化应用和服务的运作依赖于智能合约的自动化操作,但这些合约可能存在编码漏洞或设计缺陷。这为攻击者提供了机会,他们可以通过这些漏洞修改合约中的身份验证逻辑,获得未经授权的访问或操作权限,从而进行身份欺诈或其他恶意活动。

再次,随着人工智能应用范围的不断扩大,社会工程学攻击的智能化和高仿真特征不断增强,其威胁不容小觑②。尽管去中心化技术本身具备较高的安全性,但用户可能会成为钓鱼攻击、欺骗或其他形式操纵的目标。攻击者通过诱导用户泄露个人密钥或点击恶意链接,实现对用户身份的控制,自动学习并构造虚假信息,使用户自愿上钩,进而对其实施身份盗用和欺诈。

最后,跨境身份欺诈问题因其复杂性和跨国界的特点使得治理更加困难,同样需要高度关注。去中心化身份技术的跨境特性,意味着身份验证和使用不再受地理限制。这一特点虽然带来了便利性,但同时也为跨境身份欺诈提供了可能。攻击者可以利用不同国家或地区之间的法律和监管差异,进行身份盗用,实施跨境诈骗或其他非法活动。在这种情况下,受害者往往面临着追踪攻击者和对其进行法律追责的双重困难,尤其是当涉及到多个司法管辖区时。

人工智能技术的发展与信息数据技术的进步相辅相成,其风险与问题也同根而生③。面对这些挑战,法律责任的界定难度显著增加。由于去中心化环境缺乏中心化的身份管理和验证机构,当发生身份盗用或欺诈事件时,责任归属的确定变得异常复杂。去中心化的匿名性和伪匿名性特征进一步加剧了这一问题治理的难度,使得追踪攻击者和实施法律制裁变得更加困难。

(三)数字身份引发的法律监管难题

去中心化技术的发展,使得数字身份引发的法律监管难题变得日益复杂。这种技术转变推动了对传统法律概念的重新审视,特别是在隐私权、数据安全和身份认证领域。去中心化的特性虽然强化了个人隐私保护和数据主权,却也带来了监管的不确定性,尤其是在确保合规、防止身份盗用和明确法律责任方面。此外,去中心化系统的跨境特性和国际法律差异进一步增加了监管的复杂度,因此,国内外层面均需加强法律协调和合作。

1.监管框架与去中心化技术的冲突

去中心化技术,特别是基于区块链的应用,通过分布式账本技术提供了一种无需信任中介即可实现信息和价值传递的方式。这种技术架构的核心优势在于其匿名性或至少是伪匿名性,以及确保数据的不可篡改性。这些特性在一定程度上增强了用户隐私保护,但同时也为传统监管技术的应用带来了挑战。

一方面,匿名性与监管透明性的矛盾。去中心化技术中的匿名性或伪匿名性特征,意味着用户可以在网络上进行交易而无需透露其真实身份。这种匿名性虽然保护了用户的隐私权,但也为非法活动提供了可乘之机,如洗钱、资金逃避监管等。因此,如何在不破坏去中心化本质的前提下,实现对于非法活动的有效监管,成为监管科技(RegTech)④面临的一大挑战。

另一方面,分布式技术与集中式监管的冲突。去中心化技术的另一大特点是其分布式特性,这意味着没有中央控制点或单一的故障点。这种分布式的特性虽然提高了系统的稳定性和抗攻击能力,但也使得传统基于中心化的监管机制难以奏效。监管机构通常习惯于通过监管中心化的机构来间接监管整个市场,但在去中心化的环境下,这种方法不再适用。

2.法律跟进与技术发展的脱节

首先,法律制定与更新的滞后性。目前,我国已经形成了以《个人信息保护法》、《数据安全法》和《网络安全法》三法为核心的网络法律体系,为保障数字时代良好的网络环境提供了较为完善的法律基础。然而,

①王苗苗、芮兰兰、徐思雅《面向文化资源可信共享的多因子身份认证方案》,《通信学报》2023 年第 10 期,第 36 页。

②方滨兴等《人工智能赋能网络攻击的安全威胁及应对策略》,《中国工程科学》2021 年第 3 期,第 63 页。

③邱遥堃《走出虚拟世界:元宇宙热的批判性解释》,《中外法学》2023 年第 4 期,第 1081 页。

④监管科技是指一种搭载科技创新的监管新方法,主张融合法律和技术来共同提高政府的监管能力。参见:许多奇《论监管科技的双层容错机制》,《政治与法律》2024 年第 1 期,第 139 页。

当前的三法体系中涉及数字身份权利的内容较少①。相对于区块链、人工智能等技术的快速发展以及新兴、复杂的去中心化数字身份识别技术的不断涌现，法律的制定和更新通常需要经过长时间的立法调研、讨论和审议过程，这种时间差导致了法律对新兴技术的规制往往处于滞后状态。例如，当前的法律体系可能还在讨论如何针对传统的中心化数字身份识别技术进行规制，而去中心化身份识别技术等新兴技术已经广泛应用，法律的滞后性使得新兴技术引发的风险得不到及时的控制和应对处理。

其次，法律条款的泛化与模糊性。为了应对技术发展的不确定性，法律往往采取泛化和抽象的表述方式，试图覆盖尽可能多的情况和技术形态。然而，这种做法在实践中往往导致法律条款的模糊性，使其在法律适用和执行过程中出现诸多困境。例如，在去中心化数字身份识别技术的法律规制中，如何界定“去中心化”的标准、如何判断数据处理行为是否符合“最小必要性原则”，这些都是在实际操作中难以准确把握的问题。模糊的法律规定不仅增加了执法的难度，也给技术的开发和应用带来了不确定性。

再次，跨界性技术的法律适用问题。去中心化背景下的数字身份识别技术具有强烈的跨界性，既涉及信息技术领域，也涉及金融、医疗、教育等多个行业领域。这种跨界性给法律适用带来了挑战，不同领域的法律规定可能存在差异甚至冲突，如何在去中心化技术应用中统一法律规范、协调不同领域法律之间的关系成为棘手难题。此外，去中心化技术的应用往往跨越国界，而不同国家的法律体系、监管标准不一，如何建设具有整体性、协同性的跨界治理体系②，处理跨国法律适用和冲突，也是法律跟进与技术发展脱节中的一个重要问题。

最后，技术特性与法律规制的矛盾。去中心化数字身份识别技术的一些核心特性，如匿名性、不可篡改性等，与当前的法律规制存在天然的矛盾。例如，匿名性虽然可以保护用户隐私，促进社会平等③，但同时也给身份验证、数据追溯等带来了难度，这与法律对于身份明确性、数据可追溯性的要求相冲突。如何在保障技术发展和创新的同时，确保数据安全、维护社会公共利益，是法律规制需要解决的矛盾。

（四）跨境数据流动面临的法律障碍

在去中心化技术迅速发展的背景下，全球数字身份认证领域的复杂性不仅涉及技术层面的创新，也涉及法律、政治、经济和文化等多个维度的相互作用。

1. 去中心化身份识别技术对现有国际法律框架的挑战

去中心化身份识别技术的核心优势在于提供了一种去中心化、不依赖于单一权威机构的身份验证方式。然而，这种去中心化的特性在跨国应用时却遇到了重大的法律障碍。不同国家对于个人数据的保护、网络安全、身份认证等方面有着截然不同的法律规定和实施标准。例如，欧盟的 GDPR 与美国的信息隐私法律在许多方面存在根本性的差异。在这种情况下，如何在保障个人隐私和数据安全的同时，实现一种全球通用的去中心化身份认证系统，成为了一个亟待解决的国际性问题。

2. 国际合作与法律协调面临着国际政治和经济因素的复杂影响

不同国家和地区在政治体系、经济发展水平、技术实力等方面的差异，导致它们在面对数字身份识别及其法律规制时持不同的立场。这不仅使国际标准的制定变得困难，而且即使达成了一定的国际共识，其执行和监督也充满挑战。例如，在去中心化身份认证技术的应用中，发达国家可能更加重视个人隐私保护和数据安全，而发展中国家则可能更加关注技术的普及和经济效益。这种差异在试图建立一个全球统一的法律和技术标准时会产生显著的分歧。

3. 技术的快速发展变化也为国际法律协调带来了巨大挑战

区块链的身份认证技术正以惊人的速度发展和演变，然而，法律制度的建立和修改通常需要较长的时间，这种滞后性使得现有的法律难以有效应对快速发展的技术需求。例如，去中心化身份认证系统在提供高度安全和匿名性的同时，也可能被用于国际非法活动，如跨国洗钱或国际恐怖主义融资。这就要求国际社会

①张峰、杨丽《数字身份的泛在形态及其伦理风险治理研究》，《河海大学学报（哲学社会科学版）》2023 年第 6 期，第 15 页。

②刘祺《跨界治理理论与数字政府建设》，《理论与改革》2020 年第 4 期，第 117 页。

③张富利《智慧治理抑或数字规训？——智慧城市如何消解匿名性》，《宁夏社会科学》2023 年第 1 期，第 151 页。

不仅要制定适应新技术的法律规范,还要建立有效的监管和执法机制。

4.跨境数据流动所引发的法律问题也是一个重要的讨论点

在全球化的今天,数据的跨境流动已成为常态,但这也带来了复杂的法律问题。不同国家对数据的存储、处理和传输有着不同的法律要求。在去中心化身份认证系统中,数据需要在全球范围内传输和存储,这就会触及到多国的数据保护法律。如何保证数据在多规则框架下自由流动,是一个亟待解决的问题①。

三 数字身份识别法律风险的应对措施

数字时代需要有前瞻性的立法,立法者要深刻理解数字技术背后的多重道德缺失与资本逐利的陷阱,平衡好技术发展与人类发展的法律和伦理的天秤②。技术日新月异,法律也需要随之调整,不能拘泥于传统的法律框架,而应当在保障基本权益的前提下,确保法律与技术的同步发展。

(一)激励隐私保护并强化数据安全规定

1.创新隐私保护技术的激励措施

创新隐私保护技术的激励措施,应当以稳定为导向③。政府可以设立专门的技术创新基金,支持开发和应用新的隐私保护技术,如区块链和 AI 在数据保护中的应用。此外,政府可以为采用先进隐私保护技术的企业或研究机构提供税收减免或财政补贴,以鼓励他们在隐私保护方面的投入和创新。同时,政府应积极与高校、企业之间加强合作,建立伙伴关系和协作平台,共同开发和推广隐私保护技术,从而分享最佳实践研究成果和技术解决方案。在隐私保护技术的发展上,我国还应积极参与国际合作的标准制定,与其他国家和国际组织合作,共同推动全球隐私保护技术的发展和应用。

2.强化个人数据保护的法律规定

数据是数字社会的基本物理要素,数字社会的权利义务分配均围绕数据展开④。在强化个人数据保护的法律规定方面,首要任务是制定一套全面的数据保护法律体系。参考欧盟的 GDPR 及《人工智能法案》,覆盖个人数据的整个处理周期,包括收集、处理、存储、传输和销毁。在此基础上,法律规定还应当明确数据主体的权利,如访问权、更正权、删除权和反对处理权。此外,处理大量个人数据的企业或机构,应被强制要求设立数据保护官(DPO)⑤,以监督数据处理活动的合法性,并将其作为监管机构和数据主体之间的桥梁。对于敏感信息,如种族、宗教信仰、生物特征等,数据企业或机构应实施更严格的保护措施,只在绝对必要时才能收集和使用这类数据。

(二)建立数字身份识别的法定技术标准

建立数字身份识别的法定技术标准,重点在于三个方面:去中心化数字身份识别合法性认定,建立数据加密及匿名化处理标准,监管沙箱和风险评估机制的建立。合法性认定关注技术与法规的一致性,确保用户权利不受侵犯;制定并实施统一的数据加密标准至关重要,以降低数据泄露的风险;监管沙箱与风险评估则为新技术提供测试环境,同时确保其应用的安全性和合规性。从整体上讲,这些措施共同建立起确保技术进步与个人权益保护相均衡的法律技术标准,以促进数字技术的健康发展和广泛应用。

1.去中心化数字身份识别合法性认定

在去中心化身份(DID)识别的合法性认定方面,首先需要制定一套明确的、符合法律要求的技术标准,这些标准和要求应详细规定 DID 识别系统必须遵循的安全性、透明性和可靠性原则。例如,可以要求 DID 识别系统必须具备高级别的加密技术,确保数据的安全传输和存储,同时还需明确用户身份信息的采集、存储和使用必须基于用户的明确同意,并赋予用户随时撤回同意的权利。此外,合法性认定还应涵盖数据保护和隐私法规的整合,确保去中心化身份识别技术的实施不会侵犯用户的隐私权和数据安全。去中心化身份

---

①梁燕妮《企业数据合规治理:从个人数据保护到跨境数据流动》,《社会科学家》2023 年第 12 期,第 81 页。

②李建新《数字社会人权保护的伦理进路》,《河北法学》2022 年第 12 期,第 145 页。

③唐林垚《Web3.0 治理:制度机理与本土构建》,《华东政法大学学报》2023 年第 6 期,第 61 页。

④彭诚信《数字法学的前提性命题与核心范式》,《中国法学》2023 年第 1 期,第 87 页。

⑤数据保护官制度起源于欧洲,是 GDPR 规定的在特定条件下强制要求企业或组织应聘任的保护个人数据的专职岗位。参见:刘江山《欧盟通用数据保护条例中的数据保护官制度》,《中国科技论坛》2019 年第 12 期,第 173-174 页。

识别应用应当符合《个人信息保护法》的规定，如实现对个人数据的最小化收集，提供数据主体访问、更正和删除其信息的权利等。考虑到技术的快速发展，制定合法性认定的技术标准时，应预留足够的灵活性，以适应未来技术的发展，同时定期评估和修订法律规定，以保持其适应性和时效性。

2.建立数据加密与匿名化处理标准

在建立数据加密与匿名化处理标准方面，制定并实施统一的数据加密标准，以确保所有个人数据在传输和存储过程中都经过加密处理，从而降低数据泄露的风险。推广匿名化和假名化技术在个人数据处理中的应用，可以有效保护数据主体的隐私。将传统云中心身份技术与区块链技术相结合，能够有效提高互联网建立信任关系的能力和效率①，并增强数据库的抗攻击性②。例如，将真实身份信息转换为不可逆的代码，在不暴露个人身份的情况下使数据分析成为可能。

为确保法律规定的必须使用加密和匿名化技术的正确实施，首先应确定关键数据类别，如身份信息、财务信息和健康记录等，需要通过加密和匿名化技术进行保护。同时，制定加密和匿名化的使用标准，特别是在数据传输和存储过程中，应当明确指出在哪些业务操作或数据处理过程中必须使用这些技术。此外，强制执行对企业和组织的数据处理活动进行数据安全评估定期检查，确保符合法定要求。政府或监管机构应在数字法律制度建设方面做出前瞻性的投入和努力，包括推荐的加密算法、匿名化技术和最佳实践，并建立一个有效的监督机制，通过定期的合规性审查和对违规行为的处罚，确保企业和组织遵守相关法律规定。同时，政府应支持培训和资源开发，帮助企业和组织理解和实施这些技术。最后，考虑到技术的快速发展，相关法律和标准应定期审查并更新，以保持与最新数据保护技术的同步。通过这些综合措施，可以确保在必要的情况下正确应用数据加密和匿名化技术，有效保护个人隐私与数据安全。

3.设立监管沙箱与风险评估机制

数据要素只有在安全可控、合规有序的流通环境中才能充分实现其价值③。起源于英国的“监管沙箱”为新兴技术提供了可控制的试验环境，以便在现实世界条件下测试其应用并评估其潜在影响④。在设立实验区域时，首先，需要明确实验的目标和范围，例如可以将目标设定为测试去中心化身份识别技术在提高金融服务效率方面的潜力。其次，制定严格的参与资格条件，如只允许那些具备一定技术实力和合规记录的企业参与试验。对于参与实验区的实体，应明确其在实验期间的责任和义务，确保用户数据的安全性，并遵守临时的监管要求。再次，实施有效的风险评估和管理机制，包括对参与实验的技术和服务进行全面的安全评估，以及时识别和处理潜在风险。最后，建立透明的监管反馈和调整机制，根据实验结果适时调整和完善相关的法律和政策。

（三）构建技术与法律相均衡的协调机制

构建技术与法律相均衡的协调机制，关键在于平衡技术创新与法律监管的需求，确保法律体系能够适应快速发展的去中心化技术。这要求立法不仅要中立，避免偏向特定技术形式，还要具备前瞻性，能够预见技术趋势并据此更新法律规范。通过构建一个包含灵活性原则、技术中立规制、进行专门立法及分层次监管体系的框架，能够有效应对数字身份识别技术所带来的复杂挑战，促进其健康发展，并确保社会秩序和个人权益得到妥善保护。

1.确立灵活性与适应性原则

数字技术正处于根本性的社会形态变革之中，法学知识有可能获得全面、彻底而不是局部、浅层的更新。因此，法律体系内部应做好充足准备以应对数字化、智能化等重大变革的冲击⑤。在构建适应性强的法律框

①Zhengquan Zhang et al., “6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies,” *IEEE Vehicular Technology Magazine* 14, no.3 (September 2019): 28-41.

②李川、王智《大数据环境下用户隐私数据多级加密仿真研究》，《计算机仿真》2019年第11期，第159页。

③刘艳红《数据要素全生命周期安全风险的刑事保障制度研究——以数字经济安全法益观为视角》，《法学论坛》2024年第1期，第40页。

④张永亮《金融科技监管的原则立场、模式选择与法制革新》，《法学评论》2020年第5期，第117页。

⑤胡铭《数字法学：定位、范畴与方法——兼论面向数智未来的法学教育》，《政法论坛》2022年第3期，第121页。

架中,首要任务是制定灵活性与适应性原则。动态立法机制是此原则的核心,其中“日落条款”[①]和“自动更新机制”可以确保法律随技术的快速发展而适时调整。同时,可以建立技术评估机构,以监测数字身份技术的发展并评估其对法律体系的影响,这一机构可以收集公众和企业的反馈,向立法机构提供改进建议。立法时还应当考虑不同利益相关者(如技术提供者、用户、监管机构)的需求,以实现多元利益的平衡。

2.基于技术中立的法律规制措施

不必过分担忧智能科技的负面影响,以免误用规则阻碍其发展进步[②]。有学者指出,“法律系统对自动决策算法的规范,就应克服科技系统与经济系统的弊端,将风险识别与防范内化于算法的研发和应用之中”[③]。这种将技术研发和风险识别结合起来的深刻见解,应当引起规范研究者的重视。基于技术中立的法律规制,意味着法律应专注于规制技术的使用和影响,而非特定技术形态。为实现这一目标,法律条文应采用功能性定义,关注技术的功能和使用结果。这样能够确保法律适用于各种技术,即使在技术迅速发展变化的情况下也能保持法律的适应性。同时,法律应具备预见性,能考虑技术未来可能的发展方向。这要求立法者与技术专家进行持续对话,以防范技术发展的潜在风险。

3.制定专门的《数字身份法》

为适应去中心化技术背景下数字身份识别的发展,特别是应对其带来的法律风险及挑战,制定一部专门的“数字身份法”显得尤为必要。该法律应当全面覆盖数字身份的生成、使用、管理、保护及责任追究等方面,为数字身份的健康发展提供法律保障。第一,确立“数字身份法”的法律地位和作用范围。“数字身份法”应作为数字法律体系中的一个重要组成部分,与《网络安全法》、《数据安全法》、《个人信息保护法》等法律形成有效衔接,共同构建一个综合的、多层次的数字法律体系。第二,明确数字身份的法律定义及分类。“数字身份法”需明确给出数字身份的法律定义,区分不同类型的数字身份[④],并明确各类型身份的适用范围和基本规范,以便于法律的具体适用和执行。第三,规定数字身份的生成、使用和管理规则。包括但不限于身份信息的收集、处理和存储标准,用户身份验证的方法和流程,数字身份的更新、注销及其安全保护措施等,以确保数字身份的合法性、安全性和可靠性。第四,强化数字身份的保护措施。该法律需明确个人数字身份信息的保护范围,包括个人隐私权、数据所有权等方面的保护,禁止未经授权收集、使用、泄露个人数字身份信息的行为,以及相关违法行为的法律责任。第五,明确责任主体、法律责任和救济渠道。应明确数字身份管理的责任主体,包括数字身份的提供者、使用者以及监管机构等,分别规定各自的权利义务,以及在数字身份被滥用、泄露等情况下的法律责任,确保违法行为可以得到制裁,被侵权的主体可以得到救济。第六,推动国际合作。考虑到数字身份的全球性特点,该法律还应鼓励和促进国际合作,推动跨境数据流动和数字身份互认的法律框架建设,以适应全球化背景下的法律挑战和需求。

4.构建分层次法律监管体系

推动完善数据保护法治框架,应当将构建分层次的法律监管体系作为应对数字身份法律风险的另一关键环节[⑤]。这要求立法者根据技术的复杂度、使用范围和潜在风险,制定不同层次的法律规制标准。例如,对涉及高隐私或安全风险的技术应用,实施更严格的监管。监管方法应根据技术特性和应用场景的不同而灵活多变,对快速发展的技术采取更灵活的监管策略,包括实施临时许可或试点项目。同时,建立国家级、地区级和行业级等多层次监管机构至关重要。这些机构的协调和合作,能够更有效地应对跨区域和跨行业的技术应用挑战,确保监管的有效性和及时性。通过这种分层次的监管体系,可以确保法律既能促进技术创新,又能有效应对和减轻新技术带来的风险和挑战。

(四)推动数字身份国际合作的法律协调

---

①日落条款的功能在于,虽然市场环境已经发生变化,但是东道国仍然可以根据需求,灵活地通过赋予适当的剩余权利,确保投资法律环境的稳定,使投资者在新形势下平稳过渡。参见:魏艳茹《国际投资协议日落条款研究》,《法商研究》2022年第3期,第43页。

②张文显《构建智能社会的法律秩序》,《东方法学》2020年第5期,第9页。

③林洹民《自动决策算法的风险识别与区分规制》,《比较法研究》2022年第2期,第199页。

④如基于区块链的去中心化身份、基于中心化管理的数字身份等。

⑤陈统《欧盟数据治理中的“一站式”监管:运行机制、实施困境及启示》,《学术探索》2024年第1期,第60页。

随着数字全球化加速，跨境数据流动和去中心化技术的普及，要求各国超越单一法域，共同建立统一的认证标准和法律框架。这不仅涉及技术标准的协同，更触及全球范围内对隐私保护、数据安全等关键法律问题共识的形成。有效的国际法律协调，能够促进技术互通，保障用户权益，并为打击跨国犯罪、维护网络安全提供强有力的法律支撑，是推进数字社会健康发展的关键。

1.建立统一的国际数字身份认证标准

统一的国际数字身份认证标准的建立，首先需要基于共同的价值观和道德观①。保护隐私权、确保数据安全、维护用户权益，应当成为这些标准制定的基础。在这个基础上，技术规范与交互操作性成为关键。不同国家和地区的数字身份系统需要能够互相认证和交互，这要求建立标准化技术协议和数据格式，支持包括区块链等去中心化技术在内的多种技术路径。此外，认证流程与标准的统一是保障系统安全性和效率的前提。包括用户身份验证、数据加密、信息交换等环节都需要明确的国际标准来指导，以防止出现数据泄露和身份盗用等问题。

国际组织在这一过程中扮演着不可或缺的角色。联合国、国际电信联盟、世界贸易组织等机构可以提供一个平台，领导和协调数字身份认证标准的制定和推广。通过这些机构的共同努力，可以建立多边合作机制，促进政府间及非政府组织之间的合作。各国政府也需要在本国法律框架内引入和完善国际数字身份认证标准，确保法律政策的一致性和连续性。通过政策激励措施，如税收优惠、资金支持等，可以鼓励企业和机构采用和推广这些国际标准。

2.完善数字身份跨境流动的协调与合作

在数字身份认证领域，跨境法律协调与合作的完善是一个复杂的过程，建立数字身份认证法律体系与监管机制的互认是基础。这意味着各国需要通过双边或多边协议，相互认可彼此的数字身份认证系统和监管框架，简化跨境交易和合作的法律程序。同时，还应当制定统一的跨境数据流动法律框架。这一框架应当能够平衡数据流动的自由与个人隐私的保护，为数据跨境传输提供法律依据和保障。

国家与世界的联系越来越频繁并难以被物理边界所阻隔②，因此，建立国际法律协调机制也是推进跨境合作的关键。这包括通过双边和多边协议来明确各方在数字身份认证和数据保护方面的权利与义务，以及建立有效的国际争端解决机制，为数字身份相关的跨境问题提供法律途径和解决方案。跨国合作与信息共享是促进国际合作的另一个重要方面。建立国际信息共享平台，促进关于数字身份认证的技术、政策、法律等信息的交流和共享，对于提高全球数字身份认证体系的透明度和效率具有重要意义。此外，鼓励国际联合研究与开发项目，共同探索数字身份认证的新技术、新方法，可以加快技术进步和应用普及。

考虑到各国法律文化和实践的差异，在推进国际合作的过程中应当采取灵活的方法和策略。尊重各国的法律文化差异，通过逐步推进和试点项目，逐渐解决合作中的技术、法律和政策问题，积累经验和信任，从而构建一个全球化的、高效的、安全的数字身份识别体系。

［责任编辑：苏雪梅］

①Nicholas Epley, David Tannenbaum ., "Treating ethics as a design proble," *Behavioral Science&Policy* 3, no.2 (November 2017): 73-84.
②绍莉莉《绿色元宇宙的法律规制——国内法治与国际法治协同发展》，《东方法学》2023年第1期，第82页。