Journal of Security and Safety Technology 安防技术, 2026, 14(3), 122-126
Published Online September 2026 in Hans. https://www.hanspub.org/journal/jsst
https://doi.org/10.12677/jsst.2026.143013

Hans汉斯

基于生命周期理论的数字身份数据销毁策略研究

关　琳

江苏警官学院，江苏　南京

收稿日期：2026年8月15日；录用日期：2026年9月8日；发布日期：2026年9月15日

摘　要

数字身份数据的全生命周期管理是构建可信数字社会的基础，其销毁环节作为生命周期的终末阶段，直接关系到个人隐私保护、数据安全合规与企业风险管理。然而，现有主流数据安全标准在数字身份场景下的适用性仍需深入探讨。本文基于生命周期理论框架，构建了一个包含创建、验证/使用、更新/管理、撤销/停用、归档及销毁六个阶段的数字身份数据销毁模型。该模型明确了各阶段的数据状态与销毁要求，可有效解决“僵尸账户”带来的安全隐患，并为个人隐私保护、数据安全合规和企业风险管理提供具体指导。本文采用文献分析法和比较研究法相结合的研究方法，通过系统梳理国内外相关文献，构建数字身份数据销毁的策略理论框架，并探讨制度层面的实现路径，最后提出针对性的改进建议和未来研究方向。

关键词

数字身份，数据销毁，生命周期管理，隐私保护

Research on Digital Identity Data Destruction Strategy Based on Lifecycle Theory

Lin Guan

Jiangsu Police Institute, Nanjing Jiangsu

Received: August 15, 2026; accepted: September 8, 2026; published: September 15, 2026

Abstract

The full lifecycle management of digital identity data is the foundation for building a trustworthy

文章引用: 关琳. 基于生命周期理论的数字身份数据销毁策略研究[J]. 安防技术, 2026, 14(3): 122-126.
DOI: 10.12677/jsst.2026.143013

digital society. The destruction stage, as the final stage of the lifecycle, directly relates to personal privacy protection, data security compliance, and enterprise risk management. However, the applicability of existing mainstream data security standards in digital identity scenarios still needs in-depth discussion. This paper, based on the lifecycle theory framework, constructs a digital identity data destruction model comprising six stages: creation, verification/use, update/management, revocation/deactivation, archiving, and destruction. The model clarifies the data status and destruction requirements at each stage, effectively addressing the security risks posed by "zombie accounts" and providing specific guidance for personal privacy protection, data security compliance, and enterprise risk management. This paper employs a research method combining literature analysis and comparative research. By systematically reviewing relevant domestic and international literature, it constructs a theoretical framework for digital identity data destruction strategies, explores implementation paths at the institutional level, and finally proposes targeted improvement suggestions and future research directions.

Keywords

Digital Identity, Data Destruction, Lifecycle Management, Privacy Protection

1. 引言

数字身份作为个体在网络空间的身份标识，承载着大量敏感个人信息，包括身份基本信息、生物特征、行为轨迹和社交关系等。随着数字经济的发展，数字身份数据的生命周期管理已成为信息安全领域的核心议题。生命周期理论为理解数字身份数据从创建到销毁的全过程提供了理论框架。在数字身份生命周期管理的各个阶段中，数据销毁作为生命周期的最后环节，直接关系到个人隐私保护和数据安全。忽视数据销毁环节，大量“僵尸账户”成为安全攻击目标，进而引发个人信息泄露风险的情况，并不鲜见。

与传统数据相比，数字身份数据销毁具有以下特殊性：一是高敏感性，即数字身份标识符一旦泄露，可能导致身份冒用、金融诈骗等严重后果，销毁必须确保不可恢复性。二是关联性复杂，即数字身份与多种系统和服务关联，单一账户注销可能涉及多个关联系统的同步更新或清理。三是跨域共存性，即在分布式系统和去中心化网络中，身份信息可能分散存储于多个节点，彻底删除极具挑战。四是法律约束多元，不同司法管辖区对数字身份的留存期限和删除要求可能存在差异，企业需同时满足多重合规标准。

当前实践中，多数销毁策略仅依赖简单的数据删除操作，难以应对数字身份数据跨域共存与关联性复杂带来的技术难题[1]。现有研究在外包数据确定性删除、基于密码学的身份销毁、云存储安全删除等方面取得了进展[2]-[4]。本文基于生命周期理论构建六阶段模型，旨在为数字身份数据销毁提供系统性、可操作的理论指导与实践参考。

本文采用文献分析法和比较研究法相结合的研究方法，通过系统梳理国内外相关文献，构建数字身份数据销毁的策略理论框架，探讨制度层面的实现路径；最后提出针对性的改进建议和未来研究方向。

2. 理论基础与研究现状

2.1. 生命周期理论与数据销毁的关联

生命周期理论最初源于生物学领域，后被引入计算机科学和管理学，用于描述信息系统从创建到退役的全过程控制。在云计算领域，李兴国等人提出了资源生命周期的三个核心阶段：置备、日常维护与

销毁，强调了销毁阶段的自动化、可追溯与安全可控特性[5]。在数据销毁阶段，数据销毁义务的理论根基在于信息保密方式的拓展，即从维系信息保密状态转变为维系数据安全风险的可控性。数据销毁不仅是技术操作，更是法律义务的履行。当义务主体无法保障暂时不使用的重要数据和个人信息处于安全状态时，应当采取适当的数据销毁范式降低数据泄露或非法复原的安全风险[6]。

2.2. 现有销毁策略综述

数字身份数据作为个人信息的核心组成部分，其安全销毁对保护隐私至关重要。当前国外国内研究围绕外包数据确定性删除、基于密码学的身份销毁、云存储安全删除等方向展开。

国外研究方面，Cachin 等(2013)提出基于策略的安全删除模型，通过加密和密钥管理实现数据彻底删除，支持任意删除策略，适用于各类存储系统[7]。Reardon 等(2013)从系统角度对安全数据删除进行知识梳理，分析删除机制的技术实现与局限性[8]。Dahshan 建立数据生命周期威胁模型，系统分析各阶段安全风险，特别指出销毁阶段存在数据恢复、元数据篡改等威胁[9]。Victor 等提出基于数据安全风险等级的电子废弃物处置决策模型，根据设备状态和风险等级制定不同销毁流程[10]。Davidson 等提出“设计即销毁”理念，将数据销毁规划纳入系统设计的初期阶段[11]。

国内研究方面，张逢喆等(2011)在云计算领域提出数据隐私性保护与自我销毁机制，通过密钥管理模块实现密文数据的可控销毁，确保密钥销毁后数据无法恢复[12]。熊金波等(2014)针对网络内容隐私保护，提出基于身份加密的自毁方案，通过属性撤销机制实现可控的数据销毁[13]。任正伟等(2022)系统综述云存储中外包数据的确定性删除研究，涵盖密码学方法、访问控制策略和验证机制等技术路线，为数字身份数据删除提供理论框架[2]。徐小龙等提出面向云端融合计算的防御性数据销毁机制，采用移动 Agent 检测技术对潜在危险数据进行及时销毁，包含更新、封装、检测和策略 4 个功能模块[14]。赵精武(2022)从法律视角探讨数据销毁义务的理论逻辑，强调“删除权”不等于“数据销毁”，提出数据销毁应作为维持数据安全风险的最终保障手段[6]。

总体而言，数字身份数据销毁策略呈现多维度发展：技术上形成清除、擦除、销毁三类技术体系；方法上发展加密删除、策略删除、密钥销毁等多种机制；制度上推进数据销毁义务与隐私保护的衔接。对于数字身份数据的规范化、流程化销毁尚未建立起制度性标准。

3. 数字身份数据销毁六阶段模型

基于通用数据生命周期理论，并结合数字身份数据的独特性，本文构建了一个包含六个核心阶段的数字身份数据生命周期模型。该模型旨在为制定精细化的销毁策略提供一个清晰的流程框架，如图 1 所示。

(1) 创建(Creation)阶段：用户有包括用户注册、身份信息采集、初始凭证(如密码、密钥)生成以及身份绑定等活动，即进入数字身份数据的创建阶段。该阶段是数字身份数据生命周期的初始阶段，数据状态为初始活跃状态。从数据销毁考量，在此阶段，需明确数据收集的最小化原则，并预先设定数据的保留期限和销毁策略。对于创建失败或中途放弃的临时数据，应立即触发销毁程序。

(2) 验证/使用(Verification/Use)阶段：当用户进行登录、身份认证、授权访问、交易签名或信息共享等活动时，即进入数字身份数据的验证/使用阶段。该阶段数字身份数据较为活跃，通常被高频访问。从数据销毁考量，此阶段产生大量的日志和行为数据，需制定这些衍生数据的生命周期策略，例如，安全审计日志需按法规要求保留一定期限后销毁，而临时会话数据则应在使用结束后立即销毁。

(3) 更新/管理(Update/Management)阶段：当用户进行修改个人资料、重置密码、更新密钥、变更权限、添加或移除绑定设备等操作时，即进入数字身份数据的更新/管理阶段。该阶段数字身份数据较为活跃，开始呈现版本化。从数据销毁考量，此阶段每次更新都会产生旧版本数据，因此必须制定明确的策略来处理这些历史数据，是立即销毁还是作为历史版本保留一段时间。例如，旧密码的哈希值应立即被

安全销毁，不可恢复。

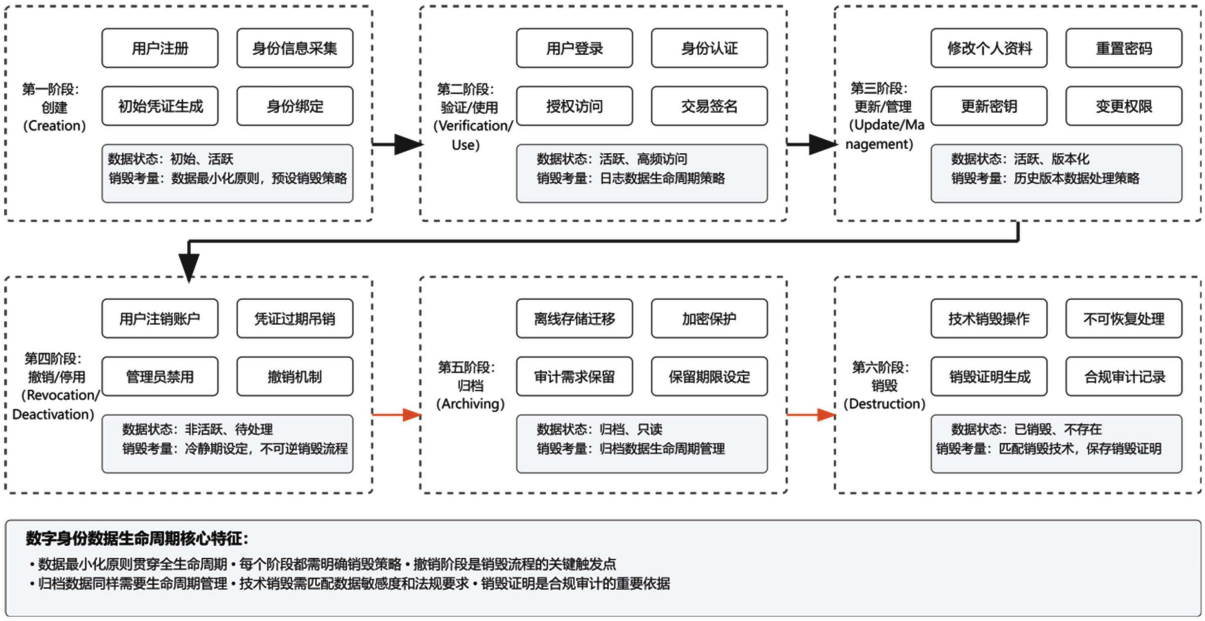

Figure 1. Six-stage model of digital identity data lifecycle
图 1. 数字身份数据生命周期六阶段模型

(4) 撤销/停用(Revocation/Deactivation)阶段：当用户进行注销账户，或发生凭证过期、被吊销、管理员禁用等情况时，数字身份数据触发销毁流程。该阶段数字身份数据状态不活跃或已标记为待处理。从数据销毁相关考量，身份进入此阶段后，其主体数据应立即停止对外提供服务，并进入预销毁或归档流程。需设定一个明确的“冷静期”或“缓冲期”，在此期间数据可被恢复，期满后则进入不可逆的销毁流程。

(5) 归档(Archiving)阶段：当用户将非活跃但因法律、审计或业务需要必须长期保留的数据，从在线生产系统迁移到低成本、安全的离线存储中时，数字身份数据进入归档阶段。该阶段数字身份数据处于归档只读状态，不可修改。从数据销毁考量，归档数据同样有其生命周期，必须为归档数据设定明确的保留期限，并在期限届满时执行销毁。归档数据的存储应采用加密等强保护措施，确保在销毁前的数据安全。

(6) 销毁(Destruction)阶段：当执行技术操作，使目标数据在任何存储介质上都无法被恢复时，数字身份数据进入销毁阶段。这一阶段数据状态为已销毁且不存在。这是生命周期的终点，必须选择与数据敏感度、存储介质和法规要求相匹配的销毁技术。同时，需要生成并安全保存销毁证明(如销毁日志、第三方证书)，以备审计和合规检查。

4. 实施与讨论

4.1. 模型的应用路径

六阶段模型的落地实施需要技术手段与制度规范的双重保障。在技术层面，企业应建立自动化的数据销毁管理系统，根据各阶段的数据敏感度和法规要求，预设销毁策略与触发条件。例如，在更新/管理阶段，系统可在接收到密码更改事件后自动调用安全擦除函数处理旧哈希值；在撤销/停用阶段，系统应在冷静期结束后自动进入不可逆销毁流程。在制度层面，企业应制定数据销毁管理制度，明确各岗位的数据销毁职责与操作规范，并建立定期的审计验证机制，确保销毁操作的合规性与完整性。同时，企业应将销毁义务纳入数据治理体系，将设计即销毁理念融入系统架构的初期规划中。

4.2. 挑战与展望

六阶段模型在跨系统数据关联清理方面仍面临技术难题。数字身份数据的高关联性意味着单一账户可能关联数十个外部系统与服务，实现自动化的同步清理需要建立统一的接口规范与协调机制。此外，动态的法规环境也要求销毁策略模型具备自适应调整能力。未来研究可向以下方向深入：一是跨领域协同机制，探索不同系统与服务间数据关联的自动识别与同步销毁技术；二是动态策略调整模型，根据数据价值变化、安全威胁态势演变以及法规更新，自动调整数据保留期限与销毁方式；三是新兴技术应用，研究区块链技术(如智能合约自动触发销毁)、同态加密(在密文状态下实施销毁)等在数据销毁领域的创新应用，以进一步提升数字身份数据管理的安全性与合规性。

5. 结语

本文基于生命周期理论，构建六阶段数字身份数据销毁策略模型，明确各阶段数据状态与销毁要求，为数字身份数据安全销毁提供系统化框架。数字身份数据销毁需兼顾技术手段与制度规范，未来需进一步探索跨领域协同机制、动态策略调整模型及新兴技术在销毁中的应用，以提升数字身份数据管理的安全性与合规性。

基金项目

本文系江苏高校哲学社会科学研究项目“网络社会综合治理身份管理机制研究”(2022SJYB0467)阶段性成果。

参考文献

[1] Lee, Y., Shin, H. and Choi, D. (2026) A Survey on Credential Revocation and DID Deactivation in Self-Sovereign Identity Systems. *IEEE Access*, **14**, 16089-16115. https://doi.org/10.1109/access.2025.3649792

[2] 任正伟, 李雪婷, 王丽娜, 等. 云存储中外包数据确定性删除研究综述[J]. 电子学报, 2022, 50(10): 2542-2560.

[3] 邵俊通. 云存储数据的确定性删除方案研究[D]: [硕士学位论文]. 保定: 河北大学, 2019.

[4] 周由胜, 陈律君. 基于区块链的细粒度云数据安全存储与删除方案[J]. 电子与信息学报, 2021, 43(7): 1856-1863.

[5] 李兴国, 林夏, 任益枚. 一种基于微服务的云计算资源生命周期管理框架设计[J]. 深圳大学学报(理工版), 2020, 37(S1): 207-211.

[6] 赵精武. 从保密到安全: 数据销毁义务的理论逻辑与制度建构[J]. 交大法学, 2022(2): 28-41.

[7] Cachin, C., Haralambiev, K., Hsiao, H. and Sorniotti, A. (2013) Policy-Based Secure Deletion. *Proceedings of the* 2013 *ACM SIGSAC Conference on Computer & Communications Security—CCS*'13, Berlin, 4-8 November 2013, 259-270. https://doi.org/10.1145/2508859.2516690

[8] Reardon, J., Basin, D. and Capkun, S. (2013) SoK: Secure Data Deletion. 2013 *IEEE Symposium on Security and Privacy*, Berkeley, 19-22 May 2013, 301-315. https://doi.org/10.1109/sp.2013.28

[9] Dahshan, M.M. (2014) Data Security in Cloud Storage Services. Master's Thesis, American University in Cairo.

[10] Victor, A., Arunkumar, G., Rajkumar, S., *et al*. (2024) Survey on Effective Disposal of E-Waste to Prevent Data Leakage. *Computer Assisted Methods in Engineering and Science*, **31**, 187-212.

[11] Davidson, S.B., Gershtein, S., Milo, T. and Novgorodov, S. (2022) Disposal by Design. University of Pennsylvania.

[12] 张逢喆, 陈进, 陈海波, 等. 云计算中的数据隐私性保护与自我销毁[J]. 计算机研究与发展, 2011, 48(7): 1155-1167.

[13] 熊金波, 姚志强, 马建峰, 等. 面向网络内容隐私的基于身份加密的安全自毁方案[J]. 计算机学报, 2014, 37(1): 139-150.

[14] 徐小龙, 龚培培. 面向云端融合计算的防御性数据销毁机制[J]. 北京理工大学学报, 2017, 37(3): 281-286.