Open Journal of Legal Science 法学, 2025, 13(8), 1969-1975
Published Online August 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.138272

Hans汉斯

数智时代经济犯罪电子数据取证困境解析与规则构建

米莉亚娜

中国政法大学证据科学研究院，北京

收稿日期：2025年7月15日；录用日期：2025年7月29日；发布日期：2025年8月29日

摘　要

数智时代的到来，使刑事犯罪形式与手段发生深刻变革，电子数据类证据在案件侦查与审理过程中起着愈发关键的作用。本文以经济犯罪为例，结合数智时代经济犯罪特点及电子数据证据特性，系统探讨电子数据证据鉴定中取证规则的现存困境，并提出相应规则的构建与完善，旨在为司法实践提供科学、合法的电子数据鉴定取证规则体系。

关键词

电子数据鉴定取证，经济犯罪，电子数据合法性

Analysis on the Dilemmas of Electronic Evidence Forensics in Economic Crimes and the Construction of Rules in the Digital-Intelligent Era

Marianna Mi

Institute of Evidence Law and Forensic Science, China University of Political Science and Law, Beijing

Received: Jul. 15th, 2025; accepted: Jul. 29th, 2025; published: Aug. 29th, 2025

Abstract

The advent of the digital-intelligent era has brought profound changes to the forms and means of criminal offenses. Electronic evidence has been playing an increasingly critical role in the investigation and trial of cases. Taking economic crimes as an example, this paper systematically explores

文章引用: 米莉亚娜. 数智时代经济犯罪电子数据取证困境解析与规则构建[J]. 法学, 2025, 13(8): 1969-1975.
DOI: 10.12677/ojls.2025.138272

the existing dilemmas in the forensics rules for electronic evidence authentication by combining the characteristics of economic crimes in the digital-intelligent era and the attributes of electronic evidence. It also puts forward proposals for the construction and improvement of relevant rules, aiming to provide a scientific and legitimate system of forensics rules for electronic evidence authentication in judicial practice.

Keywords

Electronic Evidence Authentication and Forensics, Economic Crimes, Legality of Electronic Evidence

Copyright © 2025 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

数智技术的迅猛发展推动经济活动的数字化，经济犯罪也呈现出智能化、隐蔽化、跨国化等新态势。在这类犯罪的侦查、起诉与审判过程中，电子数据类证据以其独特的证明价值，逐渐成为查明案件事实的核心依据。然而，由于电子数据证据具有数字化、易篡改性、技术依赖性强等性质，传统取证规则适配不良，导致司法实践中在电子数据证据鉴定面临诸多困境，如取证程序不规范、证据合法性存疑、技术手段落后等问题。因此，研究科学、合法的电子数据证据鉴定中的取证规则，对于保障司法公正、提高诉讼效率、打击数智时代经济犯罪具有重要的理论与实践意义。

2. 数智时代经济犯罪与电子数据证据特性

(一) 数智时代经济犯罪的特征

1) 智能化与技术化：犯罪手段采用前沿数智技术，如利用人工智能算法实施精准诈骗，通过区块链技术进行非法集资和洗钱活动。犯罪者借助复杂的加密技术、网络爬虫技术等，突破传统监管防线，使得犯罪行为隐蔽性和追踪难度大幅增加。

2) 犯罪地虚拟性与跨国性：经济犯罪通常在网络空间完成，跨越地域限制。跨国网络金融诈骗、跨境数据窃取等案件频发，犯罪组织通过在不同国家设立服务器、操控虚拟身份，利用各国法律差异和监管漏洞逃避制裁。

3) 犯罪形式多样性：数智技术的发展催生了如利用网络平台操纵金融市场、破坏数字经济基础设施等新型犯罪。这些新型犯罪涉及多个法律领域和行业监管范畴，增加了事实认定与法律适用的复杂性。

(二) 电子数据证据的特性

1) 数字化存在形式：以二进制代码存储于各类电子设备和存储介质中，需借助特定的硬件设备和软件程序进行读取、解析和展示，其物理形态与传统证据截然不同，证据的感知和理解依赖于技术工具。

2) 易修改性：电子数据存储于磁性或光介质，极易受到黑客攻击、恶意软件感染、人为误操作、硬件故障等因素影响而被篡改、删除或损坏，且修改痕迹往往难以察觉，这对证据的真实性和完整性构成严重威胁。

3) 海量性：数智时代经济活动产生海量数据，经济犯罪案件中的电子数据证据相互关联，形成复杂的证据网络。一条电子数据可能关联多个犯罪环节、多个主体和多种法律关系，需综合分析才能挖掘其证明价值。

4) 技术依赖性：电子数据的生成、存储、传输和获取依赖于计算机技术、网络技术、通信技术等多领域专业知识，取证人员需具备相应技术能力，掌握专业技术工具和操作方法才能开展取证工作。

3. 电子数据取证三重困境

(一) 电子数据取证的客观性困境

1) 电子数据存储稳定性之法律缺陷

以一起涉案金额巨大、受害数量众多的重大经济犯罪案件“e 租宝”非法集资案为例，用于存储关键交易记录、投资者信息等电子数据的服务器在警方调查取证过程中突发硬件故障，致使大量数据丢失。这些数据对于厘清涉案资金流向、确定犯罪金额等关键事实的认定起着不可代替的作用，数据的丢失严重阻碍了案件侦查进程，使得相关电子数据证据的证据效力大打折扣。

法律法规尚未强制要求数据存储方定期进行数据备份，亦未明确备份数据的存储方式、存储期限以及管理流程。这就导致一旦原始数据出现问题，难以迅速、准确地恢复，无法保障电子数据在整个诉讼过程中的稳定存在。

2) 电子数据完整性验证规则缺失

在证据审查要素体系中，证据完整性与证据基本属性中的客观性联系密切。周加海认为“电子数据完整性的功能是为证据做‘基础铺垫’，是电子数据真实性审查的一个前提性条件[1]。”2016 年“两高一部”《电子数据若干问题的规定》第 22 条，将证据完整与否作为真实性的审查要素。《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》规定在电子数据审查中，将完整性作为真实性审查的重要内容。由此可见电子数据证据的完整性是影响证据基本三性中客观性的重要因素之一。

而我国目前在电子数据审查领域，尚未构建起一套完备的、用以审查电子数据取证完整性的规则体系。完整性取证有三处困境：其一，电子数据证据海量的特性，使侦查人员在收集证据时难以全面收集而无遗漏。其二，电子数据往往跨越多个国家和地区，呈现出分散且庞杂的特点，跨境取证使完整取证难度极高。如跨国网络传销案件，犯罪组织通过搭建多个服务器，将数据分散存储在不同国家的服务器上，分别由不同的运营主体管理，数据格式和存储方式各异。在跨境取证过程中，不仅要协调不同国家的执法部门，还要应对不同的法律制度和司法协助程序，这使得获取完整证据困难重重。其三，受传统证据三性审查模式的影响，虽认识到数据完整性对证据客观性有重大影响，但我国尚未将电子数据完整性审查独立出来。龙宗智指出，单一证据完整性部分内容不能被真实性涵盖，证据群组完整性独立于真实性。完整性与证据充分性在语义、评价标准、适用对象和评价性质上也存在差异，因此证据完整性应作为相对独立的审查要素[2]。

(二) 电子数据取证的关联性困境

1) 海量电子数据筛选与关联性分析之规则空白

数智时代经济犯罪案件呈现涉案数据量大、存储分散的特点，这给证据的筛选与关联性分析带来巨大挑战。以“钱宝网”非法集资案为例，该案生成了海量资金交易记录、用户信息、推广宣传资料等电子数据，并存储于多个不同的存储介质中，分布于不同地区。

在筛选与案件具有关联性的数据时，现有规则没有提供明确、统一的指导标准。侦查人员在面对海量数据时，缺乏有效的筛选方法和工具，只能凭借经验和主观判断进行筛选。这可能导致在取证过程中遗漏关键证据，或者纳入过多与案件无关的证据，影响证据关联性的判断和案件侦查效率。

2) 间接电子数据证据关联性认定之规则缺失

在电子数据证据中，存在大量间接证据，这些证据需要通过法律推理和分析，才能确定其与案件要件事实的关联性。以借助 P2P 平台非法吸收公众存款案为例，嫌疑人的网络聊天记录、财务转账记录等

电子数据为间接证据，这些间接证据看似孤立，但实际隐藏着与非法吸储行为相关的关键线索。美国在电子数据证据领域建立了较为完善的关联性交叉验证规则，联邦证据规则明确规定了电子数据关联性的判断标准和交叉验证的方法。例如，对于电子存储信息(ESI)，要求在收集、保存和出示过程中，确保其完整性和可靠性，并通过证据间相互印证的方式进行交叉验证。

而我国现有规则未对如何判断间接电子数据与案件主要事实的逻辑联系提供清晰指引。在司法实践中，对于这些间接证据的采信与否，往往存在较大争议。不同的法官、检察官可能基于不同的经验和判断标准，对同一间接证据的关联性得出不同结论。

除了间接证据与案件的关联性分析规则空白，不同类型的间接电子数据证据之间的关联性交叉验证规则也处于空白状态。例如合同诈骗案件中，电子合同与邮件往来记录同作为间接证据，其间可能存在相互印证或相互矛盾的关系。但由于缺乏相应的规则，无法通过两者之间的关联性分析来强化或削弱它们的证明作用，使得司法人员在判断证据关联性和证明力时缺乏足够依据。

3) 新兴技术电子数据关联性判断规则滞后

随着大数据分析、人工智能算法等新兴技术在经济活动中的广泛应用，对基于新型技术产生的电子数据证据与案件关联性的判断也变得更加复杂。如利用大数据精准预选受害人实施网络诈骗的案件中，犯罪团伙通过大数据分析客户偏好数据、营销行为轨迹数据等，以此为依据筛选目标诈骗用户。这些基于大数据分析产生的数据虽然与网诈行为存有潜在关联，但现有规则无法直接认定其与犯罪行为之间关联性强度。这些数据往往是经过复杂算法处理后的结果，司法人员在面对此类新型证据时，对数据的来源、处理过程难以直观判断证明价值。

在一些金融诈骗案件中，人工智能生成的风险评估数据、信用评级数据等被用于迷惑投资者。由于人工智能算法具有“黑箱性”，数据可能在形式上看似合情合法，但实际上是犯罪分子实施诈骗的工具，现有规则无法有效应对这种新型证据带来的挑战，给案件侦破和审判带来巨大困难。

(三) 电子数据取证的合法性困境

《电子数据规定》《公安机关取证规则》中规定了电子数据的取证要求“侦查机关应当遵守法定程序，遵循有关技术标准，全面、客观、及时地收集、提取电子数据[1]。”而我国电子数据取证的合法性规则仍有三大难点。

1) 电子数据取证中当事人权利保障规则的不足与权益侵害问题

电子数据取证合法性规则的理论基础是保障当事人的基本权利，然而现有规定在电子数据证据取证过程中对当事人的知情权、隐私权、财产权等权益保护不足。有研究者提出，电子数据取证可能影响财产权、隐私权、通信自由权和言论自由权[3]。例如侵犯商业秘密案件中，侦查人员在对嫌疑人电脑进行扣押时，未隔离电脑中与案件无关的个人隐私数据，导致嫌疑人个人隐私泄露。这不仅侵犯了当事人的隐私权，也引发了公众对侦查、鉴定人员取证行为合法性、规范性的质疑。

再如电商平台刷单炒信、非法经营案中，执法机关扣押了平台服务器。平台因数据被扣押无法正常运营，产生巨大经济损失。由于缺乏对当事人财产权保护的规则，如明确的价值评估前置程序，当事人请求赔偿的诉求难以界定。

最后，对于当事人在电子数据证据取证过程中的知情权、参与权保障不足。马长山学者认为“随着数字经济和智慧社会的深入发展，开启了以‘数字人权’为代表的‘第四代人权’，包括知情同意权、数据采集权、数据修改权、数据可携权、数据被遗忘权(删除权)、数据管理权、数据支配权、数据使用权、数据收益权等等数字人权内涵，由此导致侵犯人权的方式更加技术化[4]。”由于侦查机关取证技术手段的隐秘性要求，当事人无法了解取证的详细技术过程和方法，难以对取证行为的合法性进行有效监督。在权利受到侵害时，当事人也缺乏明确的救济途径和程序。当事人作为利害关系人，应有权参与取证过

程，有权了解取证的依据、方法和程序，亦有权对非法取证行为提出异议，并获得有效的法律救济。然而，现有规则在这方面存在明显短板，导致当事人合法权益无法得到充分保障。

2) 数据与介质相分离应对应特殊规则缺失

电子数据取证主要有两种方式：一是调取存储该数据的介质(包括原始的和用来传输复制的)，二是直接调取电子数据。因此类证据中，电子数据和存储介质可相互分离，这两种取证方式在合法性规定应有所差异。“由于电子数据与载体的可分离性特征，带来了不同层面的电子数据真实性问题，由此需要分

别制定取证合法性规则，现有法律规定尚未对此作出规定[5]。”“电子数据的取证活动可能通过调取存储介质的方式实现，也可能采取直接调取电子数据的方式，对于存储介质和电子数据的调取，在合法性方面的要求是不同的[5]。”例如，在调取实物存储介质时，应严格遵循法定程序，确保从扣押、封存到后续保管的全流程都符合法律规定，保障证据来源的合法性与完整性。直接调取电子数据时，取证技术手段应具有合法性，如需采用经法律授权的软件工具、数据提取技术符合法律规定等[5]，因此，鉴于电子数据取证的复杂性以及两种取证方式合法性要求的显著差异，理应依据电子数据证据的双重客体的特性分别制定专门的合法性规则。然而，我国在这一领域尚缺失规则，亟待完善相关法律体系，以适应数智化时代司法实践的需求。

3) 电子数据非法证据排除规则细化不足

针对电子数据证据的非法取证情形、排除标准和程序缺乏细化规则。首先，电子数据证据并未被纳入《刑事诉讼法》第 56 条所规定的应当受到排除的非法证据的范围。现行立法《刑事诉讼法》第 56 条对于非法证据排除规则的适用对象作出了一般性规定：采用刑讯逼供等非法方法收集的犯罪嫌疑人、被告人供述和采用暴力、威胁等非法方法收集的证人证言、被害人陈述，应当予以排除。收集物证、书证不符合法定程序，可能严重影响司法公正的，应当予以补正或者作出合理解释；不能补正或者作出合理解释的，对该证据应当予以排除。从文字表述来看，适用对象仅包括犯罪嫌疑人、被告人供述、证人证言、被害人陈述、物证、书证这五类证据，而未明确电子数据是否适用扩张解释。“目前电子数据问题无法在《刑事诉讼法》的条文范围内进行解释，相关司法解释也未对此作出扩展。由此可以认为，在《刑事诉讼法》的层面没有规定电子数据违法取证的法律后果规则[5]。”

其次，现行法规未明确何为非法电子数据，即未明确何为非法取证手段。《最高法解释》第 13、14 条和《电子数据规定》第 27、28 条中规定了电子数据排除规则。以《电子数据规定》第 28 条为例，其中规定，“电子数据具有下列情形之一的，不得作为定案的根据：(一) 电子数据系篡改、伪造或者无法确定真伪的；(二) 电子数据有增加、删除、修改等情形，影响电子数据真实性的；(三) 其他无法保证电子数据真实性的情形。”规则制定者在对该条文进行解读时，将其界定为电子数据的排除规则，而不是非法电子数据的排除规则，并且明确说明，“对于电子数据应当着重审查其真实性，如果通过综合审查判断，仍然无法保证真实性的，则应当排除”。由此可见，制定该规则的本意是保障电子数据的真实性，与电子数据的合法性无关，不是违反取证合法性规则的法律后果[5]。例如网络诈骗案例中，执法人员在未获得合法搜查令的情况下，擅自进入嫌疑人的网络云盘获取电子数据证据，由于电子数据取证非法证据排除规则的不完善，该证据是否应被排除有较大争议。一方面，对于这种未经合法授权获取电子数据的行为，现有规则未明确其是否属于绝对排除的情形，还是可以根据具体情况进行裁量。另一方面，在排除程序上，缺乏明确的操作流程，如谁来启动排除程序、如何进行举证质证等。这就导致在司法实践中，非法证据可能因规则漏洞而进入诉讼程序，影响案件的审理效率和公正性。值得探究的另一问题是电子数据跨境取证，例如近些年日益严峻的网络诈骗案件，绝大部分都涉及境外取证需求。由于涉及不同国家和地区的法律制度、司法协助程序，电子数据取证的合法性面临更多的不确定性。缺乏统一的跨境电子数据取证规则和非法证据排除标准，使得司法机关在处理此类证据时无所适从。

同时，由于缺乏明确的非法电子证据排除规则，导致司法实践中存在操作不规范和法律适用争议的问题。在利用技术侦查措施打击网络金融犯罪的案件中，如果违反了法定的审批程序或程序条件，所获取的电子数据证据是否应被排除，以及如何排除，都缺乏具体规定。技术侦查措施在打击网络金融犯罪中发挥着重要作用，但必须在合法的框架内实施。

4. 电子数据取证规则的构建与完善

(一) 客观性困境的解决对策

1) 完善存储稳定性相关法律

数字经济犯罪频发，数据存储稳定性是案件侦查审理的关键。立法应规定定期备份涉案数据，且备份频率与数字经济犯罪的风险程度相匹配，如存储期限参照数字经济犯罪的最长追诉期设定，确保数据长期可查可用。建立严格的数据备份操作规范、数据存储环境要求、定期检测机制等，以保障数据存储安全。

2) 构建完整性验证规则体系

利用区块链技术的不可篡改和可追溯特性，对数字经济犯罪相关电子数据进行全流程记录，确保数据完整性。但需注意的是，区块链证据仅能保证证据上链后难被篡改，而其上链前的真实性难以查证。相较于传统物证，电子数据及存储介质对取证规范性和证据保存环境有更高要求。一方面，取证人员的不当技术操作可能导致电子数据原件毁损灭失。另一方面，电子数据和存储介质可能面临电子病毒、硬件物理性损毁、不良储存环境等诸多风险[6]。因此还需制定相应规则，如预先审查上链前的证据真实性、完整性，再如严格把控操作证据上链的传输人员采用的技术手段及流程等。

依据数字经济犯罪的类型特点，如网络传销、虚拟货币诈骗等，预先设计关键数据筛选逻辑，借助大数据分析技术自动筛选并收集相关电子数据，进行预防警示。

加强国际司法合作，与各国司法部门建立协作机制，共享跨境取证经验和资源，共同制定跨境电子数据完整性取证标准和流程，提升跨境取证成功率和效率。

(二) 关联性困境的解决对策

1) 填补海量数据筛选规则空白

根据不同类型的数字经济犯罪，分别制定详细的数据筛选标准指南。明确不同犯罪场景下(如电商平台刷单炒信、网络金融诈骗等)应重点关注的数据类型、关键信息及筛选优先级，为执法人员提供清晰指引。运用人工智能算法开发专门的数据筛选软件，针对数字经济犯罪数据的特点进行优化训练，协助分析海量电子数据，精准识别与案件相关的数据，并按照关联性程度进行排序，提高筛选效率和准确性。

2) 建立间接证据关联性认定规则

出台司法解释，针对电子数据中的间接证据，明确其与案件要件事实关联性认定标准，包括证据所反映的行为模式、时间节点、交易对象等与案件核心事实要素。构建间接证据交叉验证规则，要求司法人员从多维度分析验证，通过不同间接证据之间的相互印证或矛盾分析，判断其关联性和证明力，形成完整证据链条甚至证据网。

3) 更新新兴技术数据关联性判断规则

针对大数据分析、人工智能算法等新兴算法技术产生的电子数据，制定专门的关联性判断细则：如要求提供此类数据平台详细说明数据来源、采集方式、算法原理及处理过程，确保数据合法性和关联性。司法机关应建立技术专家库，遇到复杂的新兴技术电子数据关联性判断时，遴选鉴定专家提供技术解读和分析，为司法判决说理提供技术支持。

(三) 合法性困境的解决对策

1) 强化当事人权利保障规则

电子数据取证规则应保障当事人知情权。侦查机关取证前应以书面形式详细告知当事人取证的目的、范围、方式及可能对其权益的影响。保障当事人隐私权，扣押电子设备或获取数据时，采用加密、匿名化等技术手段隔离与案件无关的隐私数据。维护当事人财产权，针对取证扣押数据造成的经营受损等情况，建立相应的赔偿评估和执行机制。赋予当事人参与取证过程的权利，允许其或委托代理人在不影响案件侦查的前提下进行监督，发现非法取证可当场异议，并向上级部门或司法机关申诉。

2) 制定数据与介质分离的特殊规则

鉴于存储介质和电子数据相分离的双重客体性，应当分别制定取证要求，有不同的侧重点。“扣押原始存储介质的情况下，应当对电子数据和原始存储介质的来源进行双重审查[7]。”对于调取存储介质的取证方式，制定严格的程序规范，包括扣押前审批流程、扣押时现场记录要求、封存时密封标准和标识规范、保管期间存储环境要求和定期检查制度等，确保存储介质在取证过程中的完整性和安全性。并且还需建立有效的扣押前置评估规则，将可能因扣押实物介质而给当事人造成的经营损失预先评估，维护当事人合法财产权益。

对于直接调取电子数据的方式，应明确列出合法技术手段和软件工具清单，要求侦查人员使用清单内工具提取数据，并详细记录操作步骤、数据来源、提取时间等信息，保证数据来源合法、提取过程规范。

3) 细化电子数据非法证据排除规则

将电子数据明确纳入非法证据排除范围，详细列举数字经济犯罪中的非法取证情形，如未经授权侵入数智平台获取数据、利用恶意软件篡改电子数据等。

制定非法电子数据证据排除的具体操作流程，明确排除程序启动主体、启动时间、启动流程等。规定庭审前或庭审中对争议电子数据进行专门举证质证，由举证方承担证据合法性的举证责任，无法证明则予以排除。

积极参与国际规则制定，推动建立统一的跨境电子数据鉴定取证规则和非法证据排除标准，加强跨境取证合作，签订双边或多边司法协助协议。“欧盟改造跨境电子取证机制的前述经验，可以启发我国对国家主权原则下跨境电子取证方案作出有理有据的教义解释[8]。”明确跨境取证程序、合法性标准及非法证据排除措施，确保跨境取证合法规范。

参考文献

[1] 周加海, 喻海松. 《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》的理解与适用[J]. 人民司法(应用), 2017(28): 31-38.

[2] 龙宗智, 唐云阳. 论证据完整性及其审查规则[J]. 国家检察官学院学报, 2024(5): 22-40.

[3] 谢登科. 刑事电子数据取证的基本权利干预——基于六个典型案例的分析[J]. 人权, 2021(1): 72-88.

[4] 马长山. 智慧社会背景下的“第四代人权”及其保障[J]. 中国法学, 2019(5): 5-24.

[5] 褚福民. 电子数据合法性规则体系研究[J]. 证据科学, 2023(4): 389-404.

[6] 叶翔宇. 论电子数据复制件的证据能力及其司法适用[J]. 证据科学, 2024(4): 484-496.

[7] 杜邈, 田坤. 论网络犯罪案件的电子数据审查方法[J]. 证据科学, 2024(1): 28-38.

[8] 刘品新. 跨境电子取证的欧盟方案及启示[J]. 国家检察官学院学报, 2022(5): 3-23.