Interdisciplinary Science Letters 交叉科学快报, 2025, 9(5), 669-675
Published Online September 2025 in Hans. https://www.hanspub.org/journal/isl
https://doi.org/10.12677/isl.2025.95083

Hans汉斯

数字空间理论下大数据证据审查的制度构建

周奕帆

西南民族大学法学院，四川 成都

收稿日期：2025年7月29日；录用日期：2025年8月22日；发布日期：2025年8月29日

摘　要

大数据证据在司法实践中面临数据基础可靠性存疑、算法黑箱等阻碍实质审查、分析结论与案件要素关联性认定困难等审查困境。“数字空间理论”将大数据证据解构为四个相互依赖的层级。构建适配的审查制度需要在程序层面，强化技术辅助体系、推动有限算法透明度规则、探索区块链存证技术应用，提升法庭审查能力；在实体规则层面，设定证明责任转移规则，将算法披露程度作为评价证据证明力的核心因素，促使大数据证据提出主体履行说明义务。

关键词

大数据证据，大数据证据审查，数字空间理论

Institutional Construction of Big Data Evidence Review under Digital Space Theory

Yifan Zhou

School of Law, Southwest Minzu University, Chengdu Sichuan

Received: Jul. 29th, 2025; accepted: Aug. 22nd, 2025; published: Aug. 29th, 2025

Abstract

Big data evidence faces challenges in judicial practice, including doubts about the reliability of the data foundation, algorithmic black boxes that hinder substantive review, and difficulties in determining the relevance of analytical conclusions to case elements. The “digital space theory” deconstructs big data evidence into four interdependent layers. To establish an appropriate review system, it is necessary to strengthen technical support systems, promote limited algorithm transparency rules, and explore the application of blockchain evidence storage technology at the procedural

文章引用: 周奕帆. 数字空间理论下大数据证据审查的制度构建[J]. 交叉科学快报, 2025, 9(5): 669-675.
DOI: 10.12677/isl.2025.95083

level to enhance court review capabilities. At the substantive rule level, rules for shifting the burden of proof should be established, with the degree of algorithm disclosure serving as a core factor in evaluating the probative value of evidence, thereby compelling the parties presenting big data evidence to fulfil their duty to explain.

Keywords

Big Data Evidence, Big Data Evidence Review, Digital Space Theory

1. 大数据证据及其审查困境

1.1. 大数据证据的定义及其表现形态

把握大数据证据的本质，关键在于理解它是算法对海量数据进行深度加工后输出的规律性结论。大数据证据在三个层面与传统证据不同：在数据基础上，从有限的局部样本转向力求全面的数据集合；在技术手段上，从人工主导的操作转向复杂的自动化运算；在论证逻辑上，从线性的因果推导转向对潜在复杂关联的挖掘。传统证据通常作为证明单个事实的独立单元存在，而大数据证据则构建于“原始数据集－算法模型－分析结论”这一独特的三层结构之上，通过这种框架实现了数据整体价值的提升[1]。

具体到数据层面，大数据证据的显著特征是追求覆盖范围的全面性。传统证据的价值在于单个数据点与待证事实之间清晰、直接的联系，例如一张具体的转账单据可以直接证明某次行贿行为的发生。相比之下，大数据证据的证明力来源于聚合大量表面上关联微弱甚至离散的数据单元，通过统计方法揭示出整体性的结论。单一数据点，比如一笔小额转账记录，其自身的证明价值可能微不足道；但当海量此类数据被整合分析，却能呈现出具有统计显著性的结果。为了保障结论的可靠性，支撑分析的数据集合需要尽可能包含与待证事实相关的所有数据类型和环节的信息。例如，要有效识别洗钱活动，就必须综合账户开立信息、高频交易记录、通讯关联对象以及异常行为模式等多维度数据。这种全面性的意义在于：数据量的激增放大了数据碎片化对结论准确性的威胁，而完整的数据集合是算法得出可靠判断的基础。

在技术层面，算法是处理和解读庞杂数据的关键。其运作过程大体遵循清洗数据、降维特征、挖掘关联的流程。数据清洗环节旨在过滤噪音和干扰项，例如剔除异常值；特征降维的目标是提炼关键指标，例如识别出关键的行为模式；最后的关联规则挖掘则致力于发现数据中隐藏的、非直观的规律，例如定位异常交易集群。整个过程是非线性的，它将原始、混杂且海量的超出人类直接认知能力的数据转化为了能够指向案件事实的认知成果。

在呈现方式上，大数据证据最终表现为算法加工后形成的分析报告或结论性意见，而非原始数据的直接堆砌。它呈现的是经过提炼的结果，如同展示一份精炼的报告，而非庞杂的原始数据。常见的表现形式包括可视化的关系图谱，例如犯罪组织网络图，或量化的风险评估数值。这种形式上的转换意味着司法审查的重点必须转移到结论的生成过程及其可靠性上。

实践中，大数据证据的具体表现形态主要有以下几类：一是数据库比对结论，这是基础且常见的形态，通过计算特定数据特征的匹配程度来确认身份或物品的同一性，例如利用指纹或面部特征进行人员

身份确认。其可靠性依赖于数据库是否尽可能完整和算法能否有效过滤干扰信息。它在司法中的主要优势是将海量信息浓缩为一个关键判断，但需要注意算法本身可能存在的系统偏见；二是算法分析报告，这类报告依托复杂算法模型，如深度学习网络，从图像、文本等非结构化数据中抽取出行为规律。支撑其证明力的要素包括特征权重的可理解性解释、多种验证方法体现的模型稳健性以及结果的可信区间范围。然而，算法本身难以透视的黑箱特性，即内部决策逻辑的不可解释性，构成了对其可靠性质疑的主要来源。三是预测性判断，其运用统计模型对未来的可能性进行推断，例如评估个体再犯罪的风险。在刑事诉讼中引入这类证据必须极其审慎，遵循严格的适用原则。四是生成式内容输出，这是最前沿的应用，利用大模型“生成”新的内容来辅助认知，例如通过三维场景模拟还原事故过程。对其审查的关键在于原始数据来源是否清晰可溯、生成内容的逻辑是否可解释，以及需要与案件中的其他实质证据进行印证，防止技术模拟的逼真性误导了事实判断[2]。

这四种形态在技术介入的深度和目标导向上存在差异。数据库比对主要解决“身份、物品是否同一”的基础事实问题；算法分析报告和预测性判断则深入一步，分别聚焦于解释“行为如何运作”和评估“风险是否可能”的未来推断；生成式内容则是更深层次的技术介入，通过场景重构模拟来辅助理解事件“如何发生”的过程。

1.2. 大数据证据的审查难点

大数据证据具有数据量大、依赖算法、结论存疑等不同于现有证据种类的特征，大数据证据在司法实践中的应用日益增多，亟需理论与实践的协同。当前对大数据证据的审查主要存在以下难点。

“数据不牢靠”和“结论生成过程难以被理解和审查”的问题严重。当前审查实践往往侧重于文书齐备、见证人在场等收集程序的合规性，而对原始记录的准确性、全面性、是否存在历史偏见或商业干扰等数据本体质量的关注相对不足。洪涛教授指出，数据规模本身无法弥补其基础质量的缺陷。大数据证据的算法黑箱特征明显，技术公司提供的资质证明仅能反映机构能力，却难以揭示算法内部的运行逻辑、决策依据以及是否存在基于地域、性别或职业的歧视性设定等潜在的偏见。这种不透明性使得法庭难以实质性验证分析过程的合理性与结论的可靠性，审查容易流于形式[3]。

“数据对不上人或事”和“结论讲不清道理”的关联难题。大数据证据常常根据 IP 地址、设备 ID 等数据的算法分析结论建立与特定案件主体或行为的关联，但在实践中常遭遇关联失效问题。例如，公用设备、代理服务器或 VPN 的普遍使用，使得基于单一标识的对应关系变得脆弱且易被技术手段干扰。郑飞教授强调的基础层验证在此环节易受阻。此外，算法揭示的如特定药品购买频率与保险欺诈的关联性等非常规统计关联往往超出生活经验范畴，法官缺乏有效方式对其进行心证。预测性证据则是对未来可能性的推测与刑事证明要求的“证明过去已发生事实”及“排除合理怀疑”标准存在冲突，同时预测模型所依赖的训练数据标签本身可能隐含社会偏见，难以在审查中被有效识别和排除[4]。

这些实践难点凸显了现有规则体系与技术发展之间的脱节，对构建适配大数据证据特性的审查规则提出了迫切需求。

2. 数字空间理论下对大数据证据审查的重点

郑飞教授提出的“数字空间理论”为应对大数据证据审查的挑战，提供了重要的理论支撑和实践路径。“数字空间理论”将大数据证据解构为物理层(硬件载体)、逻辑层(处理规则)、数据层(信息本体)和内容层(分析结论)四个层级，这一分层视角不仅揭示了数据从物理基础到分析结论的生成链条，更强调了各层级间的相互依赖关系，即底层的安全与质量是上层结论可靠性的根基[5]。

物理层关注的是硬件基础，比如服务器、硬盘、传感器这些设备本身是否运行良好、安全可靠。设

备的状态直接关系到原始数据的完整性和真实性，如果存储交易记录的服务器维护不当，原始数据就可能出问题。这个层面呼应了卫晨曙等学者强调的“载体鉴真”需求，也涉及洪涛教授提出的数据全面性问题。审查时需要关注设备的维护记录、存储环境的安全措施等。

逻辑层关注的是怎么收集、清洗、转换和整合的数据处理的规则和流程，这个层面常常面临因规则不透明存在隐藏偏差的难题，在反洗钱分析中如果判断可疑交易的规则设定不合理或没解释清楚，就可能漏掉真正的问题交易。洪涛教授主张的算法科学性在这里体现为几个审查重点：数据处理路径是否清楚可查？关键步骤的规则，如过滤掉哪些数据是否合理？技术方案本身有没有设计缺陷？技术文档的完整性和关键参数的透明度？

数据层直接对应作为分析基础的海量数据本身。这个层面的审查核心是数据的质量和相关性。它需要平衡洪涛教授强调的“数据整体真实性”原则和卫晨曙教授警示的数据质量系统性瑕疵风险。审查要点包括：数据来源是否合法，数据获取是否符合规定？数据质量是否可靠，有没有明显的错误或矛盾值？数据样本是否有代表性，覆盖的时段、范围是否足够？

内容层是最终呈现的报告或图表等分析结论，这是直接用来证明案件事实的部分，但它的可靠性完全依赖于前面几个层级的支撑。内容层的审查有两个关键挑战：一是如何把统计上的关联(比如 A 商品和 B 商品销量一起涨)转化为法律上认可的事实关联，这往往需要结合其他信息来解释；二是结论本身是否说得清楚、能使法庭充分理解。洪涛教授强调的“可印证性”在这里特别重要，即大数据分析结论需要与通讯记录、证人证言等其他证据相互印证，不能孤立存在。

这个理论框架的价值不仅在于分层审视大数据证据，更在于揭示了各层之间紧密的联系。物理层是基础，逻辑层的算法处理规则影响数据层质量，而高质量的数据层才能支撑可靠的内容层结论。反过来，如果对最终结论有疑问，也可以一层层往回查，看问题出在数据本身、处理规则还是硬件基础上。这种系统性的视角，结合洪涛、卫晨曙等学者对数据真实性、算法科学性、载体可靠性等关键问题的深入探讨，共同为法官和办案人员审查复杂的大数据证据，提供更清晰、更可操作的理论支撑和方法指引。

3. 程序协同机制的构建

大数据证据的审查面临诸多复杂难题，学者们对此提出了深刻见解。郑飞教授构建的“数字空间理论”列明了大数据证据审查的内容。洪涛教授则着重分析了数据的真实性规则，指出不能被其庞大的数据量迷惑，要深究大数据证据的原始来源和质量[6]。卫晨曙教授则结合郑飞的理论框架，探讨了刑事审判中大数据证据审查的特殊挑战和应遵守的原则[7]。基于这些理论分析和实践中的痛点，本章聚焦程序性环节，尝试提出一些更便于操作的完善建议。

3.1. 审查技术辅助体系

面对大数据证据审查的技术门槛，构建一个有效的技术辅助体系至关重要。这套体系的核心在于，为法庭和诉讼参与方提供必要的专业支撑，以穿透复杂技术，保障法庭审查的实质有效。具体可从三个方面入手：

首先，在法院内部，特别是审理涉复杂技术案件较多的法院，可考虑设立专门的技术顾问，这些顾问的主要职责是充当法官的“技术助手”，他们并非鉴定人或专家证人，而是服务于法庭理解力的专业桥梁。在庭前准备阶段，技术顾问帮助梳理证据材料中数据收集、算法模型等技术争议焦点，过滤非核心细节，使庭审聚焦关键技术问题。在庭审过程中，他们则协助法官理解专业术语和争议的技术实质，促进法庭与技术相关方之间更顺畅的沟通。

其次，规范和激活专家辅助人机制，确保能对大数据证据进行有效质证。在诉讼活动中应明确告知

当事人拥有聘请专家辅助人的权利。同时，需明晰在大数据证据质证过程中，专家辅助人的核心作用在于提供质疑算法设计的合理性、分析数据关联的统计可靠性、指出预测模型的潜在局限等专业解读和批判性质证意见，帮助法庭审查相关技术问题，明确其定位是技术支持者，防止其演变为当事人的代理人进行事实陈述或法律辩护。此外，可探索建立由司法行政部门管理的公益技术专家库，对无力聘请专家辅助人的当事人提供免费或低成本的基础技术分析支持。

第三，推动形成有限的算法透明度规则，为技术质询奠定基础。应要求大数据证据提供方披露直接影响分析结论的核心信息。这并非要求公开所有商业秘密，而是说明算法模型主要依赖的决策依据，如在风险评估模型中，指明最重要的几个特征变量，以及其做出判断的基本逻辑类型和关键阈值，如达到何值会触发高风险判定。此类有针对性的信息披露，为当事人和法庭有效地审查算法的合理性及其潜在偏差提供了条件，使技术辩论能有据可循。

3.2. 引入区块链存证流程

底层数据是大数据证据的基石，数据在流转过程中的真实性与完整性是审查面临的重点，区块链具有不可篡改和可追溯特点，恰好能为数据的流转和数据状态变化提供可靠的独立验证。为了有效应对这一难题，使法庭对数据操作全程可追溯，引入区块链存证技术是一种值得探索的辅助路径。具体而言，这套辅助流程可以这样运作。

在数据操作启动的源头，就建议技术公司进行存证，当执行首次远程访问涉案服务器，或者启动核心数据分析程序等关键步骤时，应即时将此刻的操作指令和目标数据的关键状态标识同步记录到由法院或公证机构等可信第三方管理的区块链上。这一步自动生成带有精确时间戳的链上记录，为数据的原始状态和操作的起点打下了一个清晰的数字戳，为后续审查数据来源和操作规范提供了客观的起点。

随着数据处理分析的推进，系统会持续产生诸如清晰记录操作人、时间点和具体行为等详细的操作日志。为了保证整个处理链条的可信，可以将这些日志的核心内容取其哈希值，以及最终分析报告的关键结论摘要同样取其哈希值，定期或按需锚定到区块链上。这样，区块链上就形成了一条连贯的、可公开验证的操作时间链，任何试图在事后篡改原始日志或报告内容的行为，都会导致其哈希值与链上记录不符，从而被发现。

为了让法庭能够便捷高效地利用这些链上存证信息进行验证，还需配套开发便捷的验证工具。这类工具可以集成在法院办公系统中，或设计成简易的应用程序，允许法官或技术人员在法庭上直接导入需要核验的操作日志或分析报告等文件，能够自动计算文件的当前哈希值，并与之前存储在区块链上的对应记录进行快速比对，便捷直观地显示文件内容是否自存证后发生过改变，从而简化法庭对数据的验证流程，降低大数据证据审查的技术门槛和时间成本[8]。

通过引入这样的区块链存证辅助流程，在不过度增加程序负担的前提下，借助技术力量提升对大数据证据从生成到提交全流程的真实性、完整性等的验证能力，为法官审查数据的真实流转轨迹和完整性，提供相对客观且高效的技术支撑手段。

4. 实体规则的补强路径

大数据证据的审查需层层把关，对大数据证据的真实性审查不能只停留在收集程序合规的层面，必须深入数据本身的质量和可靠性。突破这些困境还需在实体规则层面围绕责任分配、科学评价证明力等进行相应完善[9]。

4.1. 设定数据质量问题的证明责任转移规则

针对大数据证据审查中数据源头真实性保障的难题，特别是洪涛教授所警示的核心原始数据系统性

缺陷可能引发的可靠性风险，有必要设定特别的证明责任转移规则。当可靠证据证明支撑大数据分析结论的原始数据存在基础性、系统性的质量缺陷，并且该缺陷经评估存在实质性地扭曲分析结论的现实可能性时，传统的证明责任分配规则应当进行适当调整。

此类系统性缺陷包括但不限于：权威报告证实的特定数据集存在广泛性错误，如历史数据录入错误率超出可接受范围，或者技术公司采集的数据存在普遍性问题，如爬取数据包含显著比例的重复项或存在结构性缺失，且这些问题可能影响算法模型的关键输出。一旦缺陷情况被初步证实，则法律上应确立对该大数据证据可靠性的合理怀疑推定。基于此推定，举证责任需相应转移至证据提供方，这意味着，在刑事诉讼中控方不再仅享有证据优势地位，而是负有积极责任，需提供充分且有效的证据以证明即使存在上述已知的数据缺陷，其拟通过该大数据证据证明的核心指控事实或主要结论仍然成立，或未受实质性影响。

为履行证明大数据证据数据可靠的责任，证据提供方可进行针对性的数据清洗与重复验证，对已知缺陷数据进行专项清洗、修正或剔除后，重新运行关键的分析流程，观察核心结论是否发生显著变化；其次，实施基于可靠子样本的验证，仅采用原始数据中经评估明确可靠的部分数据，重新分析以验证关键结论的稳健性及其统计意义强度。

若证据提供方未能成功履行此证明责任，即未能以有效方法消除该证据可靠性的合理怀疑，那么法官应对该大数据证据的证明力进行减等评价，如将其降格为辅助性、补强性证据；若数据缺陷极为严重，足以动摇分析结论的根基，法官则应当遵循审慎进行心证考虑排除该证据作为认定案件事实的依据。设定数据质量问题的证明责任转移规则，能够在数据质量风险显著存在时，促使证据提供方切实进行大数据证据分析结论可靠性验证，保障大数据证据审查的严谨与公正。

4.2. 推行“算法透明度－证明力等级”挂钩的证明力减等规则

大数据证据的算法运作的特性使得其结论的可靠性难以被实质性检验。洪涛教授所倡导的对证据真实性进行深度审查的理念启示我们，破解此困境的关键，在于构建一种程序性约束机制，通过证明力杠杆，激励证据提出方履行必要的披露义务，可以将算法透明度作为评价其衍生证据证明力的核心考量因素，当信息披露不足时，即对该证据的证明价值进行相应的阶梯式减等评价。

数据和算法模型的透明程度决定了审查的可能边界。可大致对大数据证据的算法模型透明程度分为四个层级：对于披露最为充分的例如算法完全开源可查的情形，或虽未开源但通过特定授权，允许独立审计方在安全环境中进行“白盒式”深入验证(包括提供可复现关键结论的标准测试数据集)。次之者，虽无法对源代码进行完全的审查，但披露了对结果起决定性作用的特征变量及其选取依据、模型的核心参数设定详情、训练数据集的关键统计特性分布、以及模型逻辑框架的说明性解释等左右结论的核心决策要素。若披露仅限于算法模型类型名称及最终报告，而对上述核心决策要素语焉不详，则意味着其运作逻辑实质处于难以被外界审验的状态。最不透明者，仅凭公司资质与结论性报告支撑，对算法模型运作机理几无任何解释，则已构成实质意义上的技术黑箱。

不同层级的透明度，必然匹配差异化的证明力评价。

当证据仅处于上述第三种透明度水平，即核心决策信息缺失时，其内在可靠性验证已存在显著障碍，即使其数据采集过程符合规范，该大数据证据的可靠程度也因技术不透明而难以确认。因此，在法律上应预设其证明力等级较低。此类证据原则上不宜作为认定案件关键事实的依据，除非有证明力强的、独立的证据能够对其进行高度印证。尤其在涉及当事人如定罪量刑等重大实体权利的判断中，如需采纳，则必须在裁判文书中详尽论证其审慎考量的过程及理由。

对于实质处于难以验证和审查状态的证据，即第四种透明度水平，其证明力应视为极其有限，仅在

证明对权利影响甚微的辅助性、程序性事项时，方可审慎考虑其微弱价值，且判决中必须明确记载该证明力因不透明性所受的限制。其应不能作为实体权利处分的依据。

对于披露了核心决策要素的情形(第二种透明度水平)，可认为其具备中等的初步证明力等级。但这仅为起点，该证明力的最终强度尚需结合以下维度进行复合评估：(1) 基于已披露信息，模型中是否残留可能导致歧视的潜在设计偏见且未能妥善处理；(2) 模型面对合理解释范围内的输入波动，是否呈现稳定的逻辑输出一致性；(3) 证据提出方是否就技术结论如何逻辑推演至待证法律事实的要件，提供了清晰而有说服力的论证。

透明度最高的大数据证据具备获得较高证明力的基础条件，其为法官理解大数据证据、进行实质有效的可靠性检验创设了客观的可能性与便利性。但绝非当然推定其效力，其仍须经受证据资格的严格审查，并需考察其与全案其他证据的印证关系。

这种算法透明度与证明力的挂钩规则设计，本质上是通过规则的杠杆效应，促使在技术上占优的证据提供方，为大数据证据的可靠性提供可被实质检验的基础，为解决算法结论难以被理解、审查的困境具有操作性的方案。

5. 结语

大数据证据在司法实践中的应用，在拓展证明手段的同时，也带来了数据基础可靠性、算法过程透明度、结论关联性认定及预测性判断适配性等方面的审查挑战。郑飞教授提出的“数字空间理论”提供了一个有益的分析框架，该理论将大数据证据解构为物理层、逻辑层、数据层和内容层四个层级，这一分层视角清晰地揭示了最终结论的可靠性对其他三层质量的深度依赖，提示审查工作应贯穿证据生成的整个过程，关注每一层级。

针对上述挑战，本文探讨了相应的完善路径。在程序机制上，建议强化技术辅助、推动核心算法信息的有限披露、探索区块链等存证技术的应用，以提升审查透明度和可操作性。在实体规则上，提出在基础数据存在系统性缺陷风险时，可考虑转移证明大数据证据可靠性的责任；主张将证据提供方对算法逻辑及决策依据的披露程度，作为评价该证据证明力的重要考量因素，披露的充分性与核心性，应与其证明力评价正相关。

总之，有效应对大数据证据的审查难题，需依托分层框架系统审视其生成链条，并通过程序协同提升审查能力、实体规则明晰评价标准，从而在释放大数据证据证明价值的同时，审慎管控潜在风险，维护司法公正。

参考文献

[1] 刘品新. 论大数据证据[J]. 环球法律评论, 2019, 41(1): 21-34.

[2] 林喜芬. 大数据证据在刑事司法中的运用初探[J]. 法学论坛, 2021, 36(3): 27-36.

[3] 杨继文, 范彦英. 大数据证据的事实认定原理[J]. 浙江社会科学, 2021(10): 46-54, 156-157.

[4] 郑飞, 马国洋. 大数据证据适用的三重困境及出路[J]. 重庆大学学报(社会科学版), 2022, 28(3): 207-218.

[5] 郑飞. 数字证据及其阶梯式分类审查机制[J]. 法学研究, 2024, 46(5): 169-186.

[6] 洪涛. 大数据证据真实性审查规则的建构[J]. 苏州大学学报(法学版), 2024, 11(1): 69-82.

[7] 卫晨曙. 论刑事审判中大数据证据的审查[J]. 安徽大学学报(哲学社会科学版), 2022, 46(2): 77-86.

[8] 熊晓彪. 生成式人工智能证据认定的困境与规范进路[J]. 法律科学(西北政法大学学报), 2025, 43(1): 72-93.

[9] 丰叶. 刑事大数据证据的证据化路径研究[J]. 大连理工大学学报(社会科学版), 2024, 45(5): 93-101.