法学研究 Chinese Journal of Law
Vol.46，No.5（2024）

数字证据及其阶梯式分类审查机制

郑　飞 *

内容提要：证据数字化呈现出五个基本面向——电子化、区块链化、大数据化、人工智能化和虚拟仿真化，从而形成电子数据、区块链证据、大数据证据、人工智能证据和虚拟仿真证据等五种基本的数字证据类型。由于数字技术的发展，传统电子数据概念和证据规则已不能有效涵盖和规制现有各种数字证据。基于数字空间理论以及不同类型数字证据在技术证明逻辑上的不同，应将2018年刑事诉讼法第50条第2款第8项中的“视听资料、电子数据”统一修改为一种整合开放的数字证据，以容纳因数字技术迭代升级而产生的各种数字化证据，并在司法解释中具体规定各种数字证据的审查判断规则，从而形成一种以电子数据证据规则为基础的阶梯式分类审查机制。同时，还应从证据采纳的必要性审查和实质性审查等层面，建立一种数字证据阶梯式审查的更新机制，以应对技术发展可能带来的对证据审查的冲击。

关键词：数字证据　电子数据　区块链证据　大数据证据　人工智能证据　虚拟仿真证据

随着数字技术不断迭代升级，产生了诸如区块链、大数据、人工智能和元宇宙等新数字技术。这些新数字技术在司法实践中得到广泛应用，学者们相继提出了区块链证据、〔1〕大数据证据、〔2〕人工智能证据、〔3〕算法证据、〔4〕元宇宙证据〔5〕等概念及其审查判断规则。数

* 北京交通大学法学院副教授。
本文系国家社科基金重大项目“中国特色刑事证据理论体系研究”（18ZDA139）的阶段性成果。

〔1〕 参见高奇：《〈证据新规〉下版权诉讼中的区块链证据：需求、规制及治理应对》，《电子知识产权》2020年第9期，第91页以下；杨继文：《区块链证据规则体系》，《苏州大学学报（哲学社会科学版）》2021年第3期，第86页以下；刘品新：《论区块链证据》，《法学研究》2021年第6期，第130页以下。

〔2〕 参见刘品新：《论大数据证据》，《环球法律评论》2019年第1期，第21页以下；林喜芬：《大数据证据在刑事司法中的运用初探》，《法学论坛》2021年第3期，第27页以下；郑飞、马国洋：《大数据证据适用的三重困境及出路》，《重庆大学学报（社会科学版）》2022年第3期，第207页以下。

〔3〕 参见马国洋：《论刑事诉讼中人工智能证据的审查》，《中国刑事法杂志》2021年第5期，第158页以下；李育林：《人工智能证据的表象之争与实质之辨——以刑事司法事实认定进路为视角》，《政法学刊》2022年第3期，第19页以下。

〔4〕 算法证据本身并未体现出独特的技术证明逻辑，根据算法的自动化和自主化程度不同以及具体应用场景和类型不同，可以分别纳入本文意义上的大数据证据和人工智能证据范畴。本文意义上的区块链证据和虚拟仿真证据也会用到算法，只是算法的自动化和自主化程度不同以及应用场景和类型不同。参见杨继文：《算法证据：作为证据的算法及其适用规则前瞻》，《地方立法研究》2022年第3期，第37页以下；张迪：《算法证据的独立：法理反思与制度方案》，《中国刑事法杂志》2023年第5期，第107页以下。

〔5〕 参见曹建军：《“元宇宙”司法与纠纷解决的智能化》，《政法论丛》2022年第2期，第101页；杨继文：《元宇宙证据：证据属性与适用规则》，《江海学刊》2024年第2期，第173页以下。

字技术日新月异，是否新出现一种技术及其证据应用，就要新设一种证据种类？本文即针对此问题展开系统性反思，并基于数字空间理论提出一种整合开放的数字证据概念及其审查规则体系，以容纳因技术迭代升级而产生的各种数字化证据类型，从而构建一种以电子数据证据规则为基础的阶梯式分类审查机制，也为未来新型数字证据构建一种开放的实质审查机制。

一、证据数字化的五个基本面向

数字技术的发展使人类活动逐渐从单一物理空间扩展到虚拟数字空间，数字空间相对于现实物理空间的附属性也有所消解，人类社会逐渐由单维社会系统分化为虚实共生的二维社会系统。〔6〕在此背景下，“人类的生产生活、社会关系不可避免地电子化、信息化、数据化，各种类型的司法案件亦是如此”，〔7〕尤其是在网络犯罪侦查与信息技术纠纷的审判过程中，带有数字因素的证据更是扮演了关键角色。〔8〕整体来看，司法证据在数字空间中逐渐呈现出电子化、区块链化、大数据化、人工智能化和虚拟仿真化等五个基本面向，从而形成了传统电子数据、区块链证据、大数据证据、人工智能证据和虚拟仿真证据等五种基本的数字证据类型。〔9〕

（一）证据的电子化与传统电子数据证据

随着计算机和信息网络技术的发展，证据的电子化逐渐形成了传统的电子数据证据类型。其产生方式有两种，一种是原生电子数据，另一种是其他类型证据的电子化。前者是纯粹的电子数据，而对于后者，虽然 2016 年最高人民法院、最高人民检察院、公安部《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》（以下称“电子数据规定”）第 1 条第 3 款对电子数据的界定排除了以数字化形式记载的言词证据等证据类型，但又规定这些相关证据的收集、提取、移送和审查可以参照适用电子数据证据规则。这实际上是将此类证据也视为电子数据的一种形式，因为从证据形成的动态过程看，此类以数字化形式记载的证据经历了从言词证据到电子数据的转化，拥有言词证据和电子数据的双重特征，显然应受到两种证据规则的双重规制。因此，不管是原生的电子数据，还是其他类型证据的电子化，均应一体适用电子数据证据规则。〔10〕从存储方式看，传统电子数据从最开始的电脑、硬盘、磁盘、U 盘等本地化、实体化存储形式，逐渐向网络远程化、云储存等形式发展。不管是哪种存储方式，相对于传统证据，电子数据都“具有虚拟空间性或者数字空间性”，“处在由 0 和 1 数字信号量构成的虚拟空间或数字空间，是办案人员不能直接进入的无形空间”，“是一种必须借助虚拟的‘机器’代理才能认识的证据”。〔11〕

〔6〕 参见郑飞、夏晨斌：《系统论法学视野下的元宇宙法律治理研究》，《河北学刊》2023 年第 2 期，第 207 页。

〔7〕 占善刚、王超：《从法定电子数据迈向电子数据法定》，《湖北大学学报（哲学社会科学版）》2021 年第 2 期，第 110 页。

〔8〕 参见左卫民：《迈向数字诉讼法：一种新趋势?》，《法律科学》2023 年第 3 期，第 56 页。

〔9〕 需要注意的是，证据数字化的五个基本面向并非完全按照时间顺序展开。在五种基本的数字证据类型中，电子数据最先产生，区块链证据、大数据证据、人工智能证据和虚拟仿真证据随着技术的迭代发展逐渐交错产生。

〔10〕 参见胡铭：《电子数据在刑事证据体系中的定位与审查判断规则——基于网络假货犯罪案件裁判文书的分析》，《法学研究》2019 年第 2 期，第 174 页。

〔11〕 参见刘品新：《电子证据的基础理论》，《国家检察官学院学报》2017 年第 1 期，第 152 页。

在法律正式规定电子数据之前，其早已在司法实践中大量运用了。〔12〕但直到2010年“两高”三部《关于办理死刑案件审查判断证据若干问题的规定》（以下称“办理死刑案件证据规定”）第29条，才首次从司法解释层面详细规定了“电子证据”及其审查判断规则。2012年修改刑事诉讼法时将“电子证据”改为“电子数据”纳入正式立法，而且在2012年《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》（以下称“刑事诉讼法解释”）中全面吸收了“办理死刑案件证据规定”中有关电子数据的审查判断规则。2016年“电子数据规定”和2019年公安部《公安机关办理刑事案件电子数据取证规则》从取证和审查判断两个角度，对电子数据证据规则作了更为系统详细的规定。2021年“刑事诉讼法解释”承继了上述司法解释规定。

（二）证据的区块链化与区块链证据

因其独特的去中心化和加密可信特征，区块链技术也被运用到司法实践中。2018年，杭州互联网法院首次确认了区块链存证电子数据的法律效力，从而催生了区块链证据概念。依据产生方式，可将区块链证据分为三类：第一类是区块链原生电子数据，例如比特币、以太币、泰达币等各类数字货币的有币区块链原生电子数据，以及各种无币区块链应用平台如趣链科技、中国版权保护中心等搭建的各种数字作品区块链服务平台中产生的原生电子数据。第二类是区块链存证电子数据，即将传统的电子数据和其他类型证据电子化后直接完整地存储在区块链上。第三类是区块链核验电子数据，这种情况不是将电子数据直接完整地存储在区块链上，而是将电子数据的哈希值存储在区块链上，用以核验电子数据是否被修改并保持完整性。因此，区块链证据可以定义为借助区块链技术生成、存储、核验的一切证据。〔13〕相对于传统电子数据易被篡改，去中心化的、具有加密可信特征的区块链证据更不易被篡改，从而较大程度地保证了上链之后电子数据的真实性。当然，在不同类型的区块链上，链上电子数据的篡改难度是不一样的。一般来讲，公有链的篡改难度大于联盟链，联盟链的篡改难度大于私有链。除此之外，还有其他技术特征和相关因素，如共识机制、节点数量、节点权限设置等，也决定着不同区块链证据的篡改难度。〔14〕

基于区块链证据的广泛应用，司法解释层面已经初步确立并逐渐完善了相关证据规则。例如，2018年最高人民法院《关于互联网法院审理案件若干问题的规定》第11条首次概括性地规定了区块链证据的司法效力，随后2021年最高人民法院《人民法院在线诉讼规则》第16条至第19条进一步细化了区块链证据的效力、审查判断、上链前电子数据的真实性审查或通过鉴定等其他方式进行证据补强的规则。2022年，最高人民法院更是直接发布了《关于加强区块链司法应用的意见》，提出“形成全国统一、支持跨网系、跨链协同司法应用的区块链总体建设方案”，“构建基于分布式标识、互联互通、跨链互信的区块链联盟基础设施”，“加强司法区块链平台与各行业区块链平台跨链联盟建设”，“建设互联网司法区块链验证平台”。

（三）证据的大数据化与大数据证据

随着互联网和物联网的蓬勃发展，电子数据呈指数级增长，产生了对海量数据进行及时、系统、全面分析处理的需求。于是，运用统计学原理由计算机进行的数据统计、数据碰撞、数

〔12〕 参见郑飞：《证据种类法定主义的反思与重构》，《中国法学》2024年第1期，第111页。

〔13〕 参见前引〔1〕，刘品新文，第133页以下。

〔14〕 参见华为区块链技术开发团队编著：《区块链技术及应用》，清华大学出版社2021年版，第18页以下。

据挖掘与机器学习等大数据技术应运而生。随着大数据技术在司法领域的应用逐渐增多，例如对海量的资金流数据、通信数据、网络数据、轨迹数据等的大数据分析，产生了所谓大数据证据。从技术上讲，大数据证据的形成要经过三个环节："第一步是汇总数据并进行数据清洗，第二步是建构分析模型或机器算法，第三步是进行运算形成分析结论"。〔15〕因此，对大数据证据概念的理解可以有三种：第一种理解注重"本体"，即大数据证据就是海量数据本身；第二种理解注重"结果"，即大数据证据是基于海量数据本体运用大数据技术生成的大数据分析报告；第三种理解注重"本体与分析结果结合"，即大数据证据是由海量数据本体和大数据分析报告结果共同构成。

笔者倾向于"本体与分析结果结合"的综合性理解。尽管大数据证据的存储方式与传统电子数据并无区别，但其显著特征在于数据的海量化，以及运用大数据技术生成的大数据分析报告自带的二次生成性。"每一份具体的传统证据反映的是案件中具体的人、事、物、时、空等信息；与之不同的是，大数据反映的是案件整体或作为其很大一部分的人、事、物、时、空等信息"。〔16〕仅有海量数据，没有对海量数据进行分析处理的大数据技术及分析结果，普通人将无法窥见海量数据背后反映案件整体规律性的有效证据信息。此外，大数据分析报告很大程度上是调查取证人员利用机器模型和算法等对大数据作出的分析结果，分析过程具有更强的自动性和机器决定性，这与鉴定意见主要是鉴定人借助各种仪器设备深度介入分析过程而作出的分析结果有很大区别。〔17〕

（四）证据的人工智能化与人工智能证据

早期人工智能更多是人脸识别等判别式人工智能，随着大模型技术的发展，生成式人工智能（如 ChatGPT、文心一言）得以诞生，其基于机器学习的逻辑自动生成各种信息，更是催生了人工智能证据概念。〔18〕根据判别式人工智能与生成式人工智能的区分，人工智能证据也可以区分为判别式人工智能证据和生成式人工智能证据，前者如人脸识别证据，后者如生成式人工智能自动生成的各种虚拟文字、图片和音视频，其智能化程度更高，也是更典型的人工智能证据。〔19〕人工智能证据的显著特征实际上是一种从传统专家证据到机器证据的演变，或是一种从人类经验向机器经验的演变。其中会有连技术人员也无法完全解决的算法黑箱问题，因此在审查人工智能证据时，除依靠经验审查人工智能证据的真实性，还要依靠技术审查其真实性，尤其是人工智能算法的可靠性。

"大数据技术的重心在于对海量数据的处理和对相关性关系的发掘，是一种'寻找结果'的传统计算"，而"人工智能技术，是一种'允许机器执行认知功能'的计算方法，目的在于辅助或者替代人类完成某些任务，进行某些决定"，〔20〕具有更强的自主性和极强的机器决定

〔15〕 前引〔2〕，刘品新文，第 25 页。

〔16〕 同上文，第 24 页。

〔17〕 参见元轶：《大数据证据二元实物证据属性及客观校验标准》，《山西大学学报（哲学社会科学版）》2021 年第 5 期，第 147 页。

〔18〕 需要注意的是，这里的人工智能证据更多与生成式人工智能的应用相关，与马国洋所称的人工智能证据（参见前引〔3〕，马国洋文，第 161 页）是有区别的。从本质上讲，马国洋所谓的人工智能证据应属于上文所讲的大数据证据。

〔19〕 后文如无特别说明，均在生成式人工智能层面使用人工智能证据概念。

〔20〕 参见徐继敏、严若冰：《大语言模型材料的证据属性——以 ChatGPT 和文心一言为例》，《四川师范大学学报（社会科学版）》2024 年第 1 期，第 68 页。

性。因此，相对于大数据证据形成过程中专家对大数据分析的主动启动以及将统计学上的相关性向证据法上的相关性转化，人工智能证据的特点在于机器对证据信息的自主生成和深度学习算法的不可解释性。如果要进一步严格区分大数据证据和人工智能证据，笔者认为利用人工智能技术（如机器学习）对案件证据（包括海量数据）进行审查判断和分析所得的结果更符合上文对大数据证据的界定，也可称之为“人工智能证据审查方法”，判别式人工智能证据（如人脸识别证据）就属于这种情况。而典型的人工智能证据，应是将案件发生过程中由生成式人工智能生成的文字、图片和音视频等生成物作为案件证据，其有别于上述利用人工智能技术分析案件证据的“人工智能证据审查方法”以及由此形成的分析结果和报告。〔21〕

（五）证据的虚拟仿真化与虚拟仿真证据

随着虚拟仿真技术不断迭代升级，逐步产生了虚拟现实（Virtual Reality，VR）、增强现实（Augmented Reality，AR）、混合现实（Mixed Reality，MR）、扩展现实（Extended Reality，XR）等新数字技术。这些新数字技术在司法实践中应用，就产生了虚拟仿真证据。早在2018年3月，北京市人民检察院第一分院就在法庭上运用VR技术进行了证据展示。目击证人戴上VR眼镜，边陈述边操作手柄，“身临其境”地还原了杀人犯罪现场情况，并通过屏幕上的3D动画将整个犯罪过程完整地展示给法庭。〔22〕这里的证人当庭陈述无疑属于证人证言，但由证人戴着VR眼镜并操作手柄而生成的3D动画是什么证据？再如，在元宇宙虚拟空间中发生的对数字分身的强制猥亵，记录整个事件过程的虚拟现实交互仿真影像又属于何种证据？显然，它们都不属于传统的视听资料，前者更像是美国法上的示意证据，属于我国法上的证据展示方法。〔23〕后者虽然具有电子化特征，但其实是一种虚拟仿真证据，具有以往证据种类所不具备的沉浸式、交互式特征，需要综合运用区块链技术、大数据技术、人工智能技术和虚拟仿真技术等来呈现。不同于对真实情况进行记录的视听资料，由VR示证发展到元宇宙空间的虚拟仿真证据，是一种以虚拟现实交互仿真影像来证明案件事实的新数字证据类型。

显然，由于数字技术不断迭代升级，传统的电子数据概念已经不能完全涵盖数字空间这五个证据数字化基本面向，亟需一个崭新的整合开放型数字证据概念及相应审查判断规则来应对证据数字化趋势。需要说明的是，这五个基本面向只是基于当今数字技术发展所作的初步总结，随着数字技术的进一步发展，还会涌现其他新的证据数字化趋势。

二、基于数字空间理论迈向整合开放型的数字证据体系

（一）数字空间理论的提出

数字空间（cyberspace），通常被认为是除物理空间、生物空间之外的“第三空间”，其以数据形态内嵌于物理空间和生物空间，以数字表征形式对前二者进行“映射”或“重塑”。〔24〕数字空间存在三层次说和四层次说。所谓三层次，即物理层（physical layer）、逻辑层（logical

〔21〕 参见前引〔20〕，徐继敏等文，第69页。

〔22〕 参见赵春艳：《公诉机关庭审中首次用VR示证》，《民主与法制时报》2018年3月8日第4版。

〔23〕 2017年最高人民法院《人民法院办理刑事案件第一审普通程序法庭调查规程（试行）》第34条规定，“出示证据时，可以借助多媒体设备等方式出示，播放或者演示证据内容”。2018年最高人民检察院《人民检察院办理死刑第二审案件和复核监督工作指引（试行）》第35条规定，“重大、疑难、复杂的案件可以制作多媒体示证资料”。

〔24〕 参见黄其松：《数字时代的国家理论》，《中国社会科学》2022年第10期，第72页。

layer）和社交层（social layer），其中物理层主要由单机系统、路由、光纤等基础计算设备构成，也称为计算机空间；逻辑层主要由万维网（world-wide web）及底层协议构成，也称为信息网络空间；社交层则主要包括各类数字活动主体，〔25〕也称为内容层，主要是各类互动应用及信息内容。〔26〕四层次说则在三层次的基础上增加了数据层（data layer），包括计算机和网络存储、处理的数字化信息。〔27〕随着数字技术的发展，数字空间中的逻辑层、数据层和内容层发生了剧烈变革。例如，全新的去中心化分布式网络技术正在重塑逻辑层，区块链技术正让传统的“谎言网络”变为“可信网络”，让单纯的“信息网络”变为“信息+价值网络”；大数据技术则给数据层带来了深刻影响，实现了“用数据说话”到“让数据说话”的转变；人工智能技术、XR 扩展现实技术则丰富了内容层业态。

从证据数字化的五个基本面向看，证据的数字化完全映射于数字空间的四层架构之上，甚至与数字空间的发展趋势高度耦合，各类数字证据与四层数字架构存在一定的统一性关系。传统的电子数据证据理论对此未给予充分认识，其侧重于将基本电子介质——0 和 1 组成的二进制编码——作为电子数据证据的元特征。这一理论忽视了数字空间的层次属性和维度属性，将多维、多元数字结构扁平化、简单化为 0 和 1 的二进制编码。这一做法看似是对电子数据底层特征的“科学”抓取，实则是充满“偏见”的不充分特征提取。从数字空间和各类数字证据的发展历史，可以发现以下规律：一是数字空间具有层次性，数字空间不是扁平的，而是多维、多元的；二是数字空间层次具有延展性，随着技术的发展，数字空间层次也在不断变革；三是数字证据的发展与数字空间层次的演进具有耦合性，数字证据的演化与特定数字空间层次的变革息息相关。因此，更可行的做法是将各类数字证据统合在数字空间概念之下，基于数字空间的层次性、多维性及延展性来构建数字证据理论体系。不同类型的数字技术应用分属不同数字空间层次，进而产生不同的技术证明逻辑，形成数字空间中以传统电子数据证据为基础的不同数字证据类型。这就是奠定数字证据概念基础的“数字空间理论”。

（二）电子数据概念及其证据规则的局限性

电子数据是数字证据的初始形态，伴随着计算机和信息网络技术而生。首先，从概念上看，2010 年“办理死刑案件证据规定”第 29 条、2012 年“刑事诉讼法解释”第 93 条和 2016 年“电子数据规定”第 1 条，均将电子数据限于以数字化形式存储、处理和传输的数据。强调以数字化形式存储的数据所携带的证据信息来证明案件事实，并不能有效涵盖各种类型的数字证据。例如，大数据证据不仅包括海量数据本体，还包括基于海量数据运用大数据技术而生成的用以证明案件事实的大数据分析报告；人工智能证据也已超越训练数据和输入数据，而是基于深度学习的算法逻辑自动生成新的文字、图片和音视频等虚拟证据信息，然后以这种机器生成的证据信息来证明案件事实；虚拟仿真证据不仅是电子数据本身，还呈现出基于电子数据而生成的虚拟现实交互仿真影像，并以这种虚拟现实交互仿真影像来证明案件事实。

其次，从证据种类的角度讲，刑事诉讼法对证据种类采取了限制态度，秉持一种“不符合法定的证据种类，不得作为定案的根据”的证据种类法定主义。这导致大数据证据、人工智能证据和虚拟仿真证据等新型数字证据很难被传统的电子数据概念所涵盖，但现实中很多新

〔25〕 参见朱莉欣、武兰：《网络空间安全视野下的〈塔林手册 2.0〉评价》，《信息安全与通信保密》2017 年第 7 期，第 66 页。

〔26〕 参见刘晗、叶开儒：《网络主权的分层法律形态》，《华东政法大学学报》2020 年第 4 期，第 73 页。

〔27〕 参见王世忠、孙娉娉：《网络空间进攻机理初步研究》，《中国电子科学研究院学报》2015 年第 1 期，第 55 页。

型案件的司法证明又需要这些新型数字证据。因此，迈向整合开放的数字证据体系，本质上就是要打破证据种类法定主义的局限性。〔28〕

最后，从审查判断的角度讲，传统电子数据的相关性规则、真实性规则、合法性规则以及相关审查方法，已不足以审查判断新的数字证据类型。例如，对于大数据证据，原有的电子数据证据规则仅审查海量数据本体的三性，大数据分析报告的三性则需要新的审查判断规则。尤其是大数据分析报告的相关性，需要将统计学上的相关性转化成证据法上的相关性，才能进一步审查判断大数据分析报告的真实可靠性。再如，对于人工智能证据，不仅要审查相关电子数据的三性，还要审查生成内容的真实性和算法的可靠性，这就涉及了算法黑箱的问题。又如，虚拟仿真证据的底层也是电子数据，在审查判断电子数据三性的基础上，还要进一步审查判断虚拟仿真技术对虚拟仿真证据三性的影响。

（三）不同类型数字证据的技术证明逻辑

不同数字证据类型的技术特征，决定了它们在技术证明逻辑上的差异性。首先，电子数据与传统书证在一般证明逻辑上并没有实质不同，都是以其承载的信息内容来证明案件事实。但是，电子数据之所以成为一种与书证不同的证据类型，是因为其电子化形式和载体具有独特的技术特征，即以 0 和 1 的二进制编码数字化形式存储的数据所携带的证据信息来证明案件事实。这种数字化形式的证据信息要经过复杂的转化，才能成为类似书证这样易于普通人理解的文字、符号和图表等证据信息。〔29〕而且，相对于书证，电子数据的数字化技术特征导致其更容易被篡改却不易被普通人发现，且具有无损的无限可复制性。因此，如果要用电子数据证明案件事实，就要先对电子数据进行特殊的技术性鉴真，〔30〕并采用特殊的调查取证程序和方法。这就是电子数据相对于书证的独特技术证明逻辑。

其次，相对于传统电子数据，区块链证据的证明逻辑亦无本质区别，都是以电子数据所携带的证据信息来证明案件事实。但是，区块链具有去中心化、加密可信的技术特征，相较于传统电子数据，其保证了区块链上的电子数据不易被篡改。通常来讲，区块链上电子数据的篡改难度与去中心化程度成正比，不同区块链类型上电子数据的可篡改难度不同。一般而言，可篡改难度从高到低依次为公有链、联盟链和私有链。因此，需要着重审查区块链技术的可靠性和区块链存证平台的可信性等因素及其对区块链证据三性的影响。这就是区块链证据相对于传统电子数据在真实可靠性方面的不同技术证明逻辑。

再次，大数据证据的证明逻辑与传统电子数据相比也无实质区别，都是以电子数据所携带的证据信息来证明案件事实。但大数据证据的不同技术证明逻辑在于，需要运用大数据技术来揭示海量电子数据所携带的潜在证据信息。尽管大数据证据因其海量数据本体与案件事实有关联而可以用来证明案件事实，但这种相关性的有无和程度通常是普通人无法探知和测量的，需借助基于统计分析原理的大数据技术进行深度处理，并转换成普通人能够理解的证据法上的相关性。因此，“大数据证据的实质是揭示海量数据背后的规律性结论，以及该结论与待证事实的关联性”。〔31〕由此可见，大数据证据的技术证明逻辑实际上是运用统计学上的相关性来揭

〔28〕 参见前引〔12〕，郑飞文，第 122 页。

〔29〕 参见常怡、王健：《论电子证据的独立性》，《法学》2004 年第 3 期，第 87 页。

〔30〕 参见谢登科：《电子数据的技术性鉴真》，《法学研究》2022 年第 2 期，第 209 页以下。

〔31〕 倪春乐、陈博文：《大数据证据的刑事诉讼应用机理研究》，《中国人民公安大学学报（社会科学版）》2022 年第 2 期，第 43 页。

示海量数据所携带的潜在的有效证据信息，体现的是与传统电子数据不同的大数据证据的二次生成性。

复次，人工智能证据的技术证明逻辑实际上是以相对于人类经验的机器经验的逻辑来证明案件事实。尽管人工智能生成的证据信息仍然以电子数据的形式表现出来，但其生成过程已经超越了以往各种证据信息的形成机制。人类经验是基于人类学习总结而产生的经验概括或经验法则，机器经验则是基于深度学习而形成的普通人甚至专家都不易理解的数据特征规律和算法法则。现有生成式人工智能的一个显著缺陷是其生成信息的真实性难以保证，因此，使用人工智能生成的人工智能证据来证明案件事实，不仅要审查训练人工智能的大数据的可靠性，更要审查人工智能算法的可靠性和生成信息的真实性。

最后，尽管虚拟仿真证据也是基于电子数据而生成，但其因虚拟仿真技术的加持已经具备了普通电子数据所不具有的虚拟现实交互仿真影像。虚拟仿真证据与视听资料不同，其并非对真实情况的如实记录，而是对真实情况的虚拟仿真（如 VR 示证）或者对虚拟仿真世界的记录（如元宇宙虚拟仿真证据）。这类虚拟仿真证据并不是以电子数据本身来证明案件事实，而是以其虚拟仿真的动态场景来证明案件事实。这就是虚拟仿真证据不同于传统电子数据的技术证明逻辑。

（四）整合开放型的数字证据体系

基于前述对数字空间理论和不同数字证据技术证明逻辑的阐释，可以发现数字证据的类型与数字空间的层级具有对应性，五种数字证据皆是对数字空间不同层级技术迭代改造应用而形成的。如表 1 所示，电子数据作为最基础的数字证据类型，通过区块链、大数据、人工智能和虚拟仿真等技术的加持和融合，逐步形成了新的数字证据体系。

表 1　数字证据体系

数字证据类型	数字空间层级	技术证明逻辑
电子数据	第 1 层：物理层	以 0 和 1 的二进制编码数字化形式存储的数据所携带的证据信息来证明案件事实，需要经过复杂的转化
区块链证据	第 2 层：逻辑层	借助区块链技术的去中心化和加密可信等特征来保证区块链上的电子数据不易被篡改
大数据证据	第 3 层：数据层	借助大数据分析技术并运用统计学上的相关性来揭示海量数据所携带的潜在的有效证据信息
人工智能证据	第 4 层：内容层	以人工智能生成的信息和相对于人类经验的机器经验的逻辑来证明案件事实
虚拟仿真证据	第 4 层：内容层	以虚拟仿真的动态场景来证明案件事实

所有其他类型数字证据的底层都是电子数据，电子数据主要对应的是数字空间的物理层。本质上讲，区块链证据并不是独立的证据类型，因为其只是利用区块链技术保证上链后的电子数据不易被篡改，主要对应的是去中心化网络的区块链技术对传统中心化网络的数字空间逻辑层的改造。〔32〕为了审查判断的便利，可将其视为独立的数字证据类型。大数据证据与传统电

〔32〕 参见前引〔1〕，刘品新文，第 137 页。

子数据有显著区别，是一种独立的证据类型。这是因为大数据证据既包括海量数据本体，还包括大数据分析报告，主要对应的是大数据技术对数字空间数据层的改造。人工智能证据基于机器逻辑与人类逻辑的差异，特别是其生成式人工智能的特点，需要“大数据+算法+算力”的加持，也应当是一种新型数字证据，其主要对应的是人工智能技术（尤其是生成式人工智能技术）对数字空间内容层的改造。虚拟仿真证据综合运用了区块链、大数据、人工智能和虚拟仿真等技术，并以虚拟仿真影像的形式来呈现和证明案件事实，属于一种集大成的数字证据形态，是对数字空间内容层的进一步虚拟仿真化改造。由此可见，数字证据与数字空间具有层级对应性，以电子数据为基础，基于不同的数字技术生成了不同类型的数字证据。

构建基于数字空间理论提炼的数字证据概念及类型体系，可在法律层面将 2018 年刑事诉讼法第 50 条第 2 款第 8 项中的“视听资料、电子数据”统一修改为大类的数字证据，并在司法解释中对不同类型的数字证据作进一步细化规定。甚至可以直接将视听资料纳入电子数据的范畴，因为随着数字技术的迭代升级，其在应用层面几乎已经完全取代模拟技术。1979 年刑事诉讼法并没有规定视听资料，后来为应对录音录像的普遍应用，才在 1982 年民事诉讼法（试行）和 1996 年刑事诉讼法中相继将视听资料规定为独立的证据种类，并把录音、录像、计算机存储资料等都划归其中。〔33〕在 20 世纪 80 年代以前，“崭露头角的电子信息技术并不发达，电子信息技术的应用一般也仅限于录音、录像、电话、传真等，视听材料能大致囊括基于信息技术产生的证据形式”。“随着电子信息技术的进一步发展，特别是互联网的兴起，新型的数字技术逐渐淘汰和取代了原有的模拟技术。也正是在这个过程中，电子数据逐步取得独立于视听资料的地位”。〔34〕2012 年以后，三大诉讼法相继规定了电子数据，并将其与视听资料并列。随着移动互联网等网络信息技术的不断发展，采用传统模拟技术的录音带、录像带等视听资料，几乎完全被采用数字技术的音视频所取代。因此，现在完全可以将视听资料归入电子数据，“电子数据证据规定”第 1 条第 2 款第 4 项就将“音视频”纳入了电子数据的规制范围。同样地，可以将 2018 年刑事诉讼法第 50 条第 2 款第 6 项“鉴定意见”修改为大类的专家意见，并对各种类型的专家意见如鉴定意见、专门性问题报告、事故调查报告中涉及专门性问题的意见和专家辅助人意见等，在司法解释中作进一步细化规定。类似地，还可以将同款第 7 项修改为大类的笔录证据，将同款第 3 项“证人证言”、第 4 项“被害人陈述”和第 5 项“犯罪嫌疑人、被告人供述和辩解”修改统一为大类的普通言词证据。最终形成具有层级性和整合开放性的法定证据种类（见表 2），这样处理有三个好处：

第一，在证据种类的大类划分上，都是以证明方法和证明逻辑的差异来区分证据种类，更具有逻辑融贯性和稳定性。例如以物理和化学特征来证明案件事实的物证；以文字、符号等反映的思想内容来证明案件事实的书证；基于对案件的亲身知识而以言词方式证明案件事实的普通言词证据；以专门性知识结合具体案件证据来证明案件专门性事实问题的专家意见；以调查取证过程中形成的记录来证明案件事实的各种笔录证据；以数字空间中的数字信息内容来证明案件事实的数字证据。

第二，在法律对证据进行大类划分的基础上，再通过司法解释基于不同分类标准对每一大

〔33〕 参见前引〔29〕，常怡等文，第 86 页。

〔34〕 前引〔7〕，占善刚等文，第 112 页。

类证据作进一步细分，这样的层级划分更有利于证据的精细化审查判断。例如，基于诉讼身份的不同可将普通言词证据进一步细分为证人证言、犯罪嫌疑人、被告人供述和辩解、被害人陈述；基于专家的来源和诉讼身份的不同，可将专家意见进一步细分为鉴定人的鉴定意见、鉴定人以外的专家出具的专门性问题报告、事故调查组出具的事故调查报告中涉及专门性问题的意见；基于调查取证对象和程序的不同，可将笔录证据进一步细分为勘验、检查、辨认、侦查实验等笔录；基于技术证明逻辑的不同，可将数字证据进一步细分为电子数据、区块链证据、大数据证据、人工智能证据和虚拟仿真证据等。

表 2　层级性和整合开放性的法定证据种类

一级大类划分（法律）	二级小类划分（司法解释）
物证	
书证	
普通言词证据	证人证言
	犯罪嫌疑人、被告人供述和辩解
	被害人陈述
	……
专家意见	鉴定意见
	专门性问题报告
	事故调查报告中涉及专门性问题的意见
	……
笔录证据	勘验笔录
	检查笔录
	辨认笔录
	侦查实验笔录
	……
数字证据	电子数据
	区块链证据
	大数据证据
	人工智能证据
	虚拟仿真证据
	……

第三，这种证据大类规定的层级性实际上形成了证据种类的整合开放性。从法律层面看，证据大类的区分更具有稳定性，对于每种证据大类之下的次级证据类型，则可以通过司法解释不断容纳新的细分证据类型。这与数字技术不断迭代升级、数字证据应用快速发展的特点十分契合。随着数字技术的发展，必然不断产生新的数字证据类型，这些新的数字证据类型都以电子数据为基础，以数字证据的技术证明逻辑来体现，因此都可以将其放到数字证据的细化分类

中，从而形成整合开放型的数字证据体系。此外，数字证据的概念也更符合国际趋势，尤其是在国际刑事诉讼的研究中，学者们越来越多地使用“数字证据”（digital evidence）一词。〔35〕数字证据的概念内核具有双重属性，不仅强调证据所包含信息的存储、传输格式，即数字格式，还体现多维、多元、多层次的数字空间特征。无论是区块链技术、大数据技术，还是人工智能技术、虚拟仿真技术，都无法脱离数字格式和数字空间单独成型，各种数字技术加持下的数字证据类型也无法脱离数字证据的概念从属关系。例如，英国国家犯罪局（National Crime Agency，NCA）颁布的《国家数字与实物证据保留指南》（National Digital and Physical Evidence Retention Guidance）便将证据信息的存储方式以两分法划分为实物化与数字化（physical or digital）。可见作为上位概念，“数字化”一词具备更强的统领性。相对而言，电子数据（electronic evidence）概念更强调证据获取、呈现过程中与电子设备（如计算机、智能手机）的关联性。例如，欧洲法律合作委员会（European Committee on Legal Co-operation，CDCJ）制定的《民事和行政诉讼中的电子数据指南》（Guidelines on Electronic Evidence in Civil and Administrative Proceedings）便将电子数据定义为“从任何设备中包含或生成的数据中获得的证据，这些设备的运行依赖软件程序，或依赖存储在计算机系统或网络中的数据”。这一定义强调了电子数据的设备依赖性，数字证据概念则不局限于设备类型或技术手段，而是着眼于信息本身的数字格式和数字空间的层次性。这使得数字证据概念具有更强的适应性和灵活性，能够适用于快速变化的技术环境，因此，以数字证据为基础构建的证据规则也将具有更强的开放性。

三、数字证据的阶梯式分类审查机制

笔者认为，基于数字证据的层级性特征，应当构建一种阶梯式的分类审查机制。首先，基于数字空间理论，所有类型的数字证据都应以传统的电子数据证据规则为审查判断的基础。其次，对于不同的数字证据类型，应基于各自不同的技术证明逻辑建立不同的审查判断机制。有的数字证据（如虚拟仿真证据）的审查判断，还可能要以其他数字证据（如区块链证据、大数据证据、人工智能证据等）的规则为基础，受到多重证据规则的规制。最后，应当为未来可能出现的新数字证据类型构建一种开放的实质审查判断机制。

（一）阶梯式审查的原理：基于两个不同层面的分析

数字证据审查的阶梯性涉及两个层面：一是不同种类数字证据之间的阶梯关系，二是同一种数字证据内部的阶梯关系。因此，对数字证据的审查也就存在两项需要判断的内容：一是待审查的证据属于哪一层级的证据，这主要是为了帮助事实认定者准确识别数字证据类型，进而有效判断可能使用的证据规则和审查方法；二是待审查的证据如何在本层级中进行审查，这涉及对证据本身的技术复杂性和难度的识别，这同样是为了帮助事实认定者在多种层次的证据规则和审查方法中进行有效选择。

〔35〕 以《国际刑事法评论》（International Criminal Law Review）为例，过去十年该刊刊载了一系列以“数字证据”（digital evidence）为题的论文，例如 Kristina Hellwig, *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings*, 22（5-6）International Criminal Law Review 965-988（2022）; Rafael Braga da Silva, *Updating the Authentication of Digital Evidence in the International Criminal Court*, 22（5-6）International Criminal Law Review 941-964（2022）; Riccardo Vecellio Segate, *Cognitive Bias, Privacy Rights, and Digital Evidence in International Criminal Proceedings: Demystifying the Double-Edged AI Revolution*, 22（2）International Criminal Law Review 242-279（2021）。

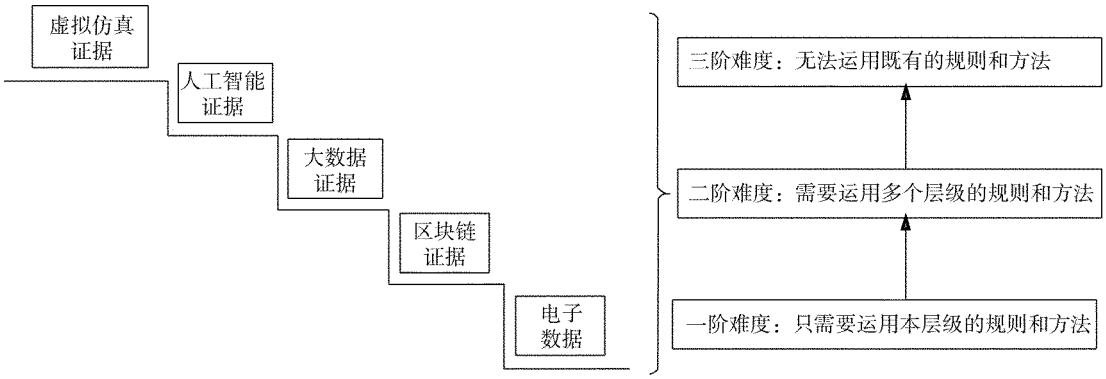

图 1　数字证据的阶梯式分类审查机制

首先，之所以将不同种类的数字证据称为阶梯式关系，主要是由于在证据审查的过程中，高层级的证据审查可能需要运用低层级的证据规则和审查方法。例如，对区块链证据的审查，就需要运用电子数据的证据规则和审查方法；对虚拟仿真证据的审查，有时需要运用人工智能证据的证据规则和审查方法。由此，可以将不同种类的数字证据进行层级划分。第一层是电子数据。电子数据是所有数字证据类型的最底层，各种数字证据类型的审查判断都必须以电子数据证据规则为基础。第二层是区块链证据。这是在传统电子数据的基础上增加了区块链技术，提升了证据的加密性和不易篡改性。第三层是大数据证据。大数据证据的核心特征是需要运用大数据技术对海量数据进行分析，这使得对大数据证据的审查必然要运用电子数据的证据规则和审查方法。此外，大数据技术的应用有时需要区块链技术作为保障，此时对大数据证据的审查，也要适当考量区块链证据的证据规则和审查方法。第四层是人工智能证据。此类证据的核心特征是机器决定性，而机器判断与分析所依托的基础仍然是电子数据。此外，新一代人工智能的发展很大程度上依托于大数据技术，海量数据的出现有效提升了机器分析的准确性。当然，这些数据有时需要通过区块链技术进行加密。因此，人工智能证据的审查很多时候需要引入电子数据、区块链证据和大数据证据的证据规则和审查方法。第五层是虚拟仿真证据。虚拟仿真证据同样以电子数据甚至是大数据为基础，这些数据有时也涉及加密问题，因此也可能要运用区块链技术。当前虚拟仿真技术的运行往往依托于人工智能技术，以实现虚拟仿真的效果。〔36〕因此，虚拟仿真证据的审查，除了要运用与自身技术相关的证据规则和审查方法，还可能要运用电子数据、区块链证据、大数据证据和人工智能证据的证据规则和审查方法。

其次，数字证据层级分类的依据主要是技术的复杂性和难度。即使对于同一层级的证据，也存在不同的审查要求。一是只需运用本层级证据的规则和审查方法，而无需运用其他层级证据的规则和审查方法；二是既要运用本层级证据的规则和审查方法，也要运用其他层级证据的规则和审查方法；三是由于新型数字技术的发展和应用，运用既有数字证据的规则和审查方法，仍然无法有效审查当前证据的，就需要针对新型数字技术的技术证明逻辑开发新的证据规则和审查方法。

基于上述分析，对数字证据的审查就需要采取“三步审查法”。第一步，识别数字证据属于哪一层级；第二步，识别数字证据的技术复杂性和难度级别；第三步，根据前两步识别的结

〔36〕 例如虚拟仿真教学对人工智能辅助技术的引入。参见彭秀程等：《“AI 智能+VR 技术”支持下虚拟仿真教学的设计与应用》，《数字技术与应用》2023 年第 5 期，第 89 页以下。

果进行证据的审查判断。

（二）阶梯式审查方法的设计：基于不同的审查步骤

就阶梯式审查而言，其方法设计可以分为证据类型识别和具体证据审查。前者主要是建立证据类型的识别方法，后者主要是开发不同层级证据的审查方法，其中以后者为关键。因为证据类型的识别很多时候可以根据证据所依托的技术“一目了然”，至于具体的审查方法，则要对技术证明逻辑作更深入的了解。

1．数字证据类型的识别方法

在对数字证据进行类型识别的过程中，通常会要求证据提供者详细说明证据所依托的技术背景信息。具体来说，证据提供者要详细描述证据生成过程中涉及的各种技术的运行机制和原理。基于这些技术信息，事实认定者应首先分析证据具体依托哪些技术手段，然后选择涉及最高层级的技术定义来界定此项证据。在此基础上，事实认定者还应进一步判断该证据是否还依托其他技术。例如，一项基于人脸识别技术的证据，证据提供者应深入阐释生成该证据的具体原理和过程。在这个过程中，可能涉及的证据规则和审查方法包括但不限于人工智能证据、大数据证据、区块链证据和电子数据的证据规则和审查方法。因此，这项证据应当被定义为人工智能证据。然而，仅仅将其归类为人工智能证据还不足以全面反映其技术复杂性，还应评估其难度等级——其难度为二阶难度（见图 1）。这意味着在评估这项证据时，除了要考虑人工智能证据规则和审查方法，还应综合运用大数据证据、区块链证据和电子数据的证据规则和审查方法，以确保对证据的全面、准确评估。

2．不同层级的基础证据审查方法

在明确了证据类型的识别方法之后，要进一步考虑不同层级证据的审查方法。此时要就每一种证据类型设计最基础的审查方法，如表 3 所示。

表 3　数字证据的层级性与阶梯式审查路径

数字空间层级	数字证据类型	相关性审查	真实性审查	合法性审查
物理层	电子数据	一般相关性审查	一般真实性审查：载体、内容、数据等	一般合法性审查：取证过程是否合法、是否侵犯公民基本权利等
逻辑层	区块链证据	一般相关性审查	特殊真实性审查：技术信赖规则；区块链的类型；平台技术特征等	一般合法性审查
数据层	大数据证据	特殊相关性审查：数据来源；输出结果；算法技术等	特殊真实性审查：数据来源的可靠性；算法技术、数据分析报告的真实性	特殊合法性审查：数据隐私权的保护；数据采集和处理的合法性
内容层	人工智能证据	特殊相关性审查：机器生成的相关性问题	特殊真实性审查：技术的可检验性、同行评议、普遍接受度、准确率	特殊合法性审查：数据来源、使用及隐私保护
	虚拟仿真证据	特殊相关性审查：虚拟仿真技术与案件事实的匹配	特殊真实性审查：技术原理的可靠性；数据的完整性；系统运行的稳定性	特殊合法性审查：证据开示和技术援助制度

首先是电子数据的审查方法。处于物理层的电子数据是数字空间的基石，因此电子数据是所有数字证据类型的最底层，各种数字证据类型的审查判断都必须以电子数据证据规则为基础。从电子数据证据的审查样态看，主要包括相关性、真实性和合法性审查。电子数据关联性（相关性）的审查判断要素既包括信息或内容的关联性，也包括载体或形式的关联性。前者是经验上的关联性，体现了电子数据所携带的信息内容与案件事实之间的证明关系，其审查判断机制与其他传统证据并无不同；而后者通常是一种技术上的关联性，这是由电子数据的技术证明逻辑所决定的。〔37〕电子数据的真实性包括电子数据载体的真实性、电子数据本身的真实性和电子数据内容的真实性。〔38〕电子数据的合法性则主要考虑电子数据取证的过程是否符合法律程序、是否侵犯公民的基本权利等。

其次，处于逻辑层的区块链证据的审查判断机制应从分布式网络即可信网络的底层逻辑出发，主要包括以下几个方面：（1）除了要受到传统电子数据证据规则的调整，还要受到区块链证据专门规则的调整。（2）需要区分上链前与上链后的数据，上链前电子数据的真实性由传统电子数据证据规则规制，其真实性信赖依靠“经验信赖”产生；上链后的电子数据才属于区块链证据，其真实性信赖依靠“技术信赖”产生。因此，基于区块链的可信网络技术特性，区块链证据的真实性审查将从主观主义下的“经验信赖”，转向客观主义下的“技术信赖”。（3）“技术信赖”亦有层次之分。一是要区分区块链证据的类型，建立相应的审查判断机制。例如，区块链原生数据是自然意义上的区块链证据原件，其真实性程度较高，一般可以直接推定真实性；区块链存证数据实际上是传统电子数据和其他类型证据的复制件，要受到双重或多重证据规则的规制；区块链核验证据实际上是一种鉴真方法，受鉴真规则规制。二是要区分区块链证据所在的区块链类型，建立不同信赖层级的审查判断机制。一般而言，公有链、联盟链、私有链的篡改难度是依次递减的，因此要着重审查不同区块链技术对区块链证据真实性的影响。三是基于客观主义逻辑，区分不同的区块链平台并建立相应的审查判断机制。尤其是用于区块链存证的各类平台，既有由私营公司搭建的区块链存证平台，也有由各级法院发起搭建的司法区块链平台，等等。不同区块链平台的技术特征和相关因素（如共识机制、节点数量、节点权限设置等）都会影响对区块链证据的审查判断，因此，应在综合考虑上述多种因素的基础上，通过司法解释构建更为细致的“区块链+推定”“区块链+司法认知”的新型审查判断机制。〔39〕

再次，处于数据层的大数据证据的审查判断机制，应从大数据“容量大”“种类多”“低价值密度”“非线性分布”的基本特征出发，主要包括以下几个方面：（1）大数据的“低价值密度”“非线性分布”特征决定了大数据证据在相关性审查方面面临严峻考验。这意味着，对于大数据证据，不仅要运用传统电子数据证据规则审查判断海量数据本体与案件事实的相关性，还要将大数据分析报告所揭示的统计学上的相关性转化成证据法上的相关性，也就是将大数据的机器经验（大数据经验）转化成人类经验（经验法则）。换句话说，需要处理“大数据发现的相关关系在证据法上为什么相关”这个问题，并将对该问题的解释转译为日常语言。（2）既要运用传统电子数据证据规则审查判断海量数据本体的真实性，还要审查判断大数据

〔37〕 参见刘品新：《电子证据的关联性》，《法学研究》2016 年第 6 期，第 178 页以下。
〔38〕 参见褚福民：《电子证据真实性的三个层面》，《法学研究》2018 年第 4 期，第 121 页以下。
〔39〕 参见前引〔1〕，刘品新文，第 146 页以下。

分析报告的真实性。前者既包括海量数据整体的来源可靠性，例如大数据收集渠道和程序的合法性（这是大数据证据真实性的程序保障）、数据传输过程的安全性以及数据存储环境的稳定性和保密性，也包括经过大数据分析确认的具体数据的真实性。（3）除了遵循传统电子数据的合法性审查判断规则，还要特别注意大数据证据在合法性审查方面的特殊性。大数据证据的获取和数据挖掘均有可能对公民隐私权造成威胁，对于前者要构建适当的大数据侦查程序和程序性制裁规则，对于后者要构建适当的机器算法和大数据分析报告审查机制。需要注意的是，目前的实践案例中，大数据分析报告的证据形式不会直接出现，而是转化为司法鉴定意见书、〔40〕工作情况说明、〔41〕电子版数据分析报告〔42〕等形式出现。由于运用了大数据碰撞、分析和比对等侦查方式，其本质上都是大数据分析报告，法院大多数情况下都会对其进行认定且作为事实认定的基础，并注意到该类证据是建立在电子数据的基础之上。

复次，处于内容层的人工智能证据的特征，实质上取决于人工智能的技术特性，即“机器决定性”“机器生成性”以及“局部最优性”。“机器决定性”意味着人工智能证据的产生往往不需要人为选择与干预，“机器生成性”意味着人工智能证据通常是基于原始数据“二次开发”的产物。〔43〕“机器决定性”和“机器生成性”决定了人工智能证据的产生具有一定的不可知与不可控属性，这就削弱了其与原始数据之间的相关性。考虑到当下人工智能以数据驱动为主，其在运行逻辑上与大数据分析有诸多相似之处，人工智能证据的相关性审查可以借鉴大数据证据的“数据、结论与算法”相关性审查规则。此外，基于人工智能的“局部最优”属性，还要对人工智能证据的可靠性（即真实性）进行审查。人工智能证据的真实性审查在美国已有司法先例，有学者将其总结为四大标准：人工智能技术可被检验；人工智能技术经过同行评议；人工智能技术被普遍接受；人工智能技术准确率高。〔44〕

总之，人工智能证据的审查判断机制应主要包括以下几个方面：（1）尽管人工智能证据有文本、图像和音视频等多种形态，但其底层仍然是电子数据，因此首先要受到电子数据证据规则的规制。（2）应区分不同人工智能技术所产生的人工智能证据，构建不同的审查判断机制。例如，判别式人工智能证据更多是基于数据库的比对原理，应主要审查其判别的历史正确率、数据集的代表性、算法的偏见性以及更新迭代的时效性。生成式人工智能证据的大模型技术更为复杂，如基于深度学习大模型技术而生成的文本、图像或音视频等，不仅要审查其生成的直接结果，还要深入探究大模型背后的算法逻辑、训练数据来源与质量、模型的可解释性等因素。（3）对于生成式人工智能证据，因其大模型技术的复杂性，即使开示大模型的所有源代码也可能无法有效审查其可靠性，因此需要结合经验、逻辑、技术、规则和制度等构建一种综合性的专门针对生成式人工智能证据的审查判断机制。目前，人工智能证据的称谓也没有在实践案例特别是判决书中直接表现出来，取而代之的是对涉人工智能类证据的直接应用。对于这一类证据的审查，法院一般既关注人工智能所使用的数据，也关注人工智能技术本

〔40〕 参见陕西省咸阳市中级人民法院（2018）陕04刑终131号刑事裁定书。
〔41〕 参见黑龙江省哈尔滨市香坊区人民法院（2017）黑0110刑初549号刑事判决书。
〔42〕 参见四川省成都高新技术产业开发区人民法院（2018）川0191刑初94号刑事判决书。
〔43〕 参见前引〔3〕，马国洋文，第161页。
〔44〕 同上文，第167页。

身的性质。〔45〕

最后，虚拟仿真证据同样处于内容层，其审查判断机制应主要包括以下几个方面：（1）虚拟仿真证据是一种特殊类型的数字证据，需要在遵循传统电子数据证据规则的基础上，首先着重审查建构虚拟现实交互仿真影像的电子数据的完整性，以及虚拟仿真技术（尤其是元宇宙技术）的独特技术原理的可靠性，包括验证仿真模型的科学性、算法逻辑的合理性、数据输入的准确性、系统运行的稳定性等，以确保虚拟仿真技术生成的影像能够真实反映案件事实，而非技术偏差或人为操控的结果。（2）虚拟仿真本质上是一种视觉技术，可以通过虚拟现实交互仿真影像来证明案件事实，具有极大的视觉冲击性和“眼见为实”的确定感。文生视频大模型 Sora 的出现会极大地强化这一虚实融合趋势，这种趋势存在误导事实认定者的风险，例如在 VR 示证中举证方可能在虚拟仿真演示中自觉或不自觉地加入本方的一些臆测观点而非事实陈述，文生视频大模型 Sora 所创造的虚拟世界会进一步模糊虚拟与真实的界限。因此，需要事实认定者对虚拟仿真证据的证明价值和危险性进行权衡，从而决定是否采纳该证据。〔46〕（3）应建立完善的虚拟仿真证据开示和技术援助制度。前者包括应开示虚拟仿真证据的完整数据集，含原始数据、处理过程、算法逻辑等全部信息。后者包括对符合条件的辩护方进行技术援助以实现控辩平衡，防止辩护方因技术门槛过高而难以有效质证。在我国的 NFT 侵权第一案中，〔47〕不仅涉及数字作品在区块链中的存储问题，还涉及元宇宙数字藏品问题。由于其争议涉及传统的知识产权侵权问题——只是将侵权行为转移到了元宇宙空间，所以法院需要在著作权法、2020 年《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》等法律、司法解释的基础上，进一步厘清该类型证据的区块链技术和元宇宙技术基础，以及原被告双方提交的一系列有关技术的释明材料。但纵观全案，始终没有摆脱通过公证等方式将新数字证据类型转化为传统证据种类的固定流程，这说明我国亟需完善虚拟仿真证据开示和技术援助制度。

3．“三阶难度”证据的审查方案

如前所述，某一特定层级数字证据的“三阶难度”（见图 1）主要体现在，在对既有本层级和其他层级证据规则和审查方法进行彻底探究之后，仍然无法有效审查当前证据。在这种情况下，事实认定者并无现成方案可以用来审查这些证据。为了应对这一挑战，事实认定者可以尝试以下几种方法来探索新的审查方案：首先，可以邀请相关领域的专家就这些证据进行深入解释，并指出证据中可能存在的技术审查风险点；其次，可以要求原被告双方就证据的相关性、真实性和合法性提出详细的分析和解释，以便更好地理解证据的含义；再次，可以利用现代科技手段，如大数据分析、人工智能辅助等，对证据进行更加深入和细致的分析，提出基于机器经验的相关证据意见；最后，可以要求熟知相关技术的人员作为证人出庭，对证据进行专业解释和说明。通过上述一个或多个方法，法官可以综合各种信息对证据进行深入分析和判断。如果在穷尽所有可能的方法之后，法官仍然无法理解相关证据，为了确保法官在审判过程中的主体性和公正性，避免可能存在真实性、合法性等风险的证据未经审查便进入法庭，应当

〔45〕 参见王新雷、秦文豪：《涉人工智能案件的审判难点及应对思路——基于对 220 件司法裁判结果的实证研究》，《北京航空航天大学学报（社会科学版）》2023 年第 6 期，第 45 页以下。

〔46〕 美国《联邦证据规则》403 条就确立了“危险性实质上超过证明力的相关证据排除规则”。

〔47〕 参见浙江省杭州市中级人民法院（2022）浙 01 民终 5272 号民事判决书。

排除该证据，以防止因法官无法理解证据而导致的误判。当然，上述只是司法实践在初次应对新兴数字证据类型时的权宜之计，为了更好地应对数字技术迭代所可能产生的新数字证据类型，需要构建一种数字证据阶梯式审查的更新机制，即开放的实质审查机制。

（三）数字证据阶梯式审查的更新机制：一种开放的实质审查机制

从视听资料到电子数据，数字技术的每一次更新发展和司法应用，都可能产生新的数字证据形式。是否每产生一种新数字技术及其证据应用，就要在法律或司法解释中设立一种新的数字证据类型？答案当然是否定的。只有当一种新的数字技术在司法中大量应用后产生了与以往各种数字证据不同的技术证明逻辑之后，才有可能产生一种新的数字证据类型。因此，数字证据及其审查应当保持开放性，对于今后可能产生的新数字证据类型，应当构建一种有效的开放的实质审查机制。〔48〕

第一，采纳新数字证据类型的必要性审查。对于既有证据类型以外的新数字证据类型，首先要从以下几个方面进行证据采纳前的必要性审查：（1）新的数字证据类型是否实质上有助于准确认定事实。如果仅是非必要的辅助证明手段，就没有必要采纳为定案根据。（2）新的数字证据类型是否不可替代。如果案件中的传统证据类型就足以证明案件事实，就没有必要采纳为定案根据。（3）新的数字证据类型是否影响关系人的精神自由。例如，现在的测谎证据之所以不可采，不仅因为其不可靠，更重要的是它影响了关系人的精神自由。〔49〕未来脑机接口技术成熟并广泛应用之后，与之相关的证据能否作为定案的根据，就必须依据此规则进行审查判断。（4）采纳新的数字证据类型是否会严重影响审判效率和其他重要价值。这取决于新型数字技术的技术逻辑是否复杂到需要付出更大的诉讼成本，是否会严重危及公正、和谐等重要价值。（5）在采纳新的数字证据类型前，要征求控辩双方的意见，尤其要考虑新型数字技术的应用是否可能造成新的控辩失衡。如果可能造成，就要对辩方进行技术法律援助以扭转这种控辩失衡，否则不能采纳该数字证据。

第二，采纳新数字证据类型的实质性审查。针对既有证据类型以外的新数字证据类型，要基于证据法的一般原理，结合新型数字技术的特征，审查其证据三性和相关影响因素，并遵循一般的证据能力规则，对采纳新数字证据类型进行实质性审查。这一过程不仅要遵守证据法的基本原则与普遍规律，还要深入剖析新型数字技术的独特属性和运作机制。以在涉及生态环境和地矿资源的案件中广泛应用的卫星遥感数据为例，其本质上是数字证据，应遵循一般的电子数据证据规则。这意味着卫星遥感数据的收集过程需符合法定程序，以确保其来源的合法性和真实性，同时数据的完整性、一致性和未被篡改的状态也是审查重点。除此之外，卫星遥感数据的生成、传输、处理和存储有其技术特殊性，因此应运用证据法的一般原理审查其证据三性，尤其是卫星遥感数据的技术原理，包括其采用的遥感成像技术类型、传感器的精度与分辨率、数据处理算法的有效性和准确性等。除了在证据能力的审查上要注意结合新型数字技术的特征，在证明力的判断方面亦应如此，因为新型数字技术的特征也会在不同程度上影响证据三性，从而影响法官对证据证明力的判断。〔50〕

第三，新数字证据类型的审查在既有阶梯式审查中的位置。考虑到对高层级证据的审查判

〔48〕 参见前引〔12〕，郑飞文，第120页以下。

〔49〕 参见施鹏鹏：《意大利刑事诉讼与证据制度专论》，中国政法大学出版社2020年版，第215页。

〔50〕 参见郑飞：《证据属性层次论——基于证据规则结构体系的理论反思》，《法学研究》2021年第2期，第128页。

断可能会使用低层级证据的审查规则，在明确了新型数字证据的审查方式之后，应进一步考量其在数字证据阶梯式审查中的位置。这需要根据其依托的技术以及基于相关技术而形成的证据的特点进行综合判断，如果某种新型数字证据的形成需要依托区块链技术、大数据技术、人工智能技术和虚拟仿真技术，那么该证据就应处于数字证据阶梯式审查的更高层级。这种情况下，可以根据实践需要逐步增设各种应用成熟的新数字证据类型的实质审查判断规则。例如，对于上文所述的卫星遥感数据，〔51〕就需要在深入分析卫星遥感数据特性、技术原理及在法律适用中面临的具体问题的基础上，制定一套既符合证据法基本原理，又适应新技术特点的实质审查判断规则，以涵盖数据的收集、保全、真实性验证、相关性分析、合法性评估以及证明力判断等多个方面。

Abstract: The digitization of evidence gradually presents five basic aspects of electronization, blockchainization, big digitalization, artificial intelligentization, and virtual simulation, thus forming five basic types of digital evidence, i. e., electronic data, blockchain evidence, big data evidence, artificial intelligence evidence, and virtual simulation evidence. However, with the development of the digital technology, the traditional concepts and rules of electronic data can no longer effectively cover and regulate the existing digital evidence. Based on the theory of digital space and the differences in the logic of technical proof of different types of digital evidence, audio-visual materials and electronic data provided for in Article 50 Paragraph 2 (8) of the Criminal Procedure Law should be uniformly modified into an integrated and open digital evidence to accommodate various kinds of digital evidence generated by the iterative upgrading of digital technology. In the judicial interpretation, the review of and judgment rules on various kinds of digital evidence should be specified to form a hierarchical classification review mechanism based on electronic data evidence rules. At the same time, China should also establish an update mechanism for digital evidence hierarchical review at the levels of necessity review and substantive review, so as to cope with the impact of technological development on evidence review.

Key Words: digital evidence, electronic data, blockchain evidence, big data evidence, artificial intelligence evidence, virtual simulation evidence

〔51〕 虽然卫星遥感数据不像五种基本数字证据类型一样运用广泛，但其在特定类型的案件中经常运用，为便于实务操作，可以将其总结提炼为一种新的数字证据类型。