

doi:10.16060/j.cnki.issn2095-8072.2026.04.007

人工智能生成信息的刑事证据类型化认定^{*}

寿晓明

(安徽大学法学院, 合肥 230601)

摘要: 在生成式人工智能技术实现规模化应用后, 其生成的信息大量进入刑事侦查等场景, 成为了案件裁判的重要素材。此类信息具有算法黑箱性、主体模糊性、内容创造性等特征, 与以人类主导生成、客观事实记录、固定载体存储为要素的传统证据规则存在冲突, 带来了证据能力审查、证明力评估、证据认定实操等困境。在证据能力层面, 真实性审查遭遇来源资质无效、内容印证失灵的难题, 关联性认定因溯源困难而陷入实质关联判断的僵局, 合法性审查面临主体责任模糊、程序适配不足、内容合规风险并存的问题。在证明力层面, 判断标准缺失、层级定位模糊, 导致同案不同判的风险极大。在证据实操层面, 证据保存的完整性难以保证, 认证程序缺乏专门规则保障其可靠性。要破解上述困境, 应从证据的三性原理出发, 并衔接生成技术的特性, 以技术可追溯性为锚点, 构建底层逻辑、方法逻辑与价值逻辑的分析框架。在实践层面, 基于生成方式和证据用途将生成信息类型化为辅助生成型与自主生成型、事实证明型与程序辅助型, 分别构建证据能力三性审查、证明力差异化评估、实操流程适配等规则, 并厘清举证责任分配、质证程序规范、完整性保存技术路径及专家辅助机制。

关键词: 人工智能生成合成内容; 证据认定; 生成式人工智能; 刑事证据; 人工智能体

中图分类号: D915.3

文献标识码: A

文章编号: 2095-8072(2026)04-0097-13

一、引言

随着人工智能生成合成内容^①(以下简称“生成信息”)深度融入数字经济, OpenClaw等人工智能在司法领域的深度应用为审判工作高质量发展提供了新的技术路径(游劝荣, 2025)。最高人民法院在《关于规范和加强人工智能司法应用的意见》中提出, 要“加快推进人工智能技术与审判执行、诉讼服务、司法管理和法治社会服务等工作的深度融合, 规范司法人工智能技术应用”。然而, 生成信息被滥用的问题也日益凸显。人工智能技术生成的侵权文本、深度伪造的音视频、智能模型输出的数据分析报告, 已频繁出现在著作权纠纷、刑事侦查、举证等司法场景中, 且常被用作影响案件裁判结果的关键素材(丁国峰和寿晓明, 2025)。北京通州法院股权代持纠纷案、厦门海事法院涉外海事争议案等类似案件的涌现, 导致司法机关对该类证据审查陷入了认定困境。故此, 完善AI生成信息方面的裁判规则, 研究制定涉人工智能案件和数据产权司法保护的规范性文件迫在眉睫。人工智能在与司法工作融合时所面临的挑战, 根源在于传统证据法体系与生成信息特性间的冲突。传统证据规则以人类主导生成、客观事实记录、固定载体存储为前提, 而生成信息具有算法黑箱性、主体模糊性、内容创造性等特征, 难以被现有规则覆盖, 进而引发证据资格存疑、审查标准缺失与认证程序失灵等问题。

学界围绕人工智能与司法证据领域的融合展开研究, 生成式人工智能模型已从技术创新前沿走向经济社会塑造的中心地带(寿晓明, 2026)。徐继敏和严若冰(2024)的研究明确, 大语言模型材料可以成为证据, 但是否具有证据资格需要在具体个案中进行判断, 这为大语言模型材料进

^{*} 基金项目: 本文受江西省高校人文社会科学研究项目“去算法歧视的法理基础与规范展开研究”(项目编号: FX22107)的资助。

^① 《人工智能生成合成内容标识办法》第3条指出, “人工智能生成合成内容是指利用人工智能技术生成、合成的文本、图片、音频、视频、虚拟场景等信息”。

入司法证据范畴划定了标准。从人工智能的司法定位来看，现阶段的人工智能仍属于“弱人工智能体”，长于形式逻辑推理，但无法实现对人类认知思维的完整模拟，在司法证据推理之中处于辅助性地位（卓翔和崔世群，2023），这一认知界定了AI在证据推理中的功能边界。针对实践需求，程龙（2025）提出，应当将人工智能辅助量刑纳入司法审查对象范畴，对其进行证据化改造，通过聚焦AI辅助量刑的程序合规性，回应其融入司法审查体系的方向。在刑事司法领域，人工智能参与刑事证明，在一定程度上实现了统一证据标准、纠正证据瑕疵、输出辅助性司法决策结果等功能作用，能同时为刑事司法提供公正价值与效率价值（陆宇光，2025），凸显了AI在刑事证明中的功能优势与价值贡献。就技术介入方式而言，人工智能可以通过大数据及机器学习实现检索及统计分析、处理自然语言实现规划决策的方式介入科学证据的审查判断（潘金贵和熊用坪，2022），明确了AI参与科学证据审查路径。纵博（2019）强调，人工智能运用于证据判断时，应遵循辅助性原则、有限性原则、可反驳原则，为AI的实践应用设定了准则。此外，以大数据证据为代表的科学证据给刑事庭审的变革带来了机遇，同时也对传统的证据体系和规则产生了深刻影响（洪刚，2024），从宏观层面指出了大数据证据对刑事庭审及传统证据体系的变革意义。整体而言，现有研究围绕AI与司法证据的议题展开，形成了从微观资格判断到宏观体系影响的探讨。但多数聚焦于证据资格的抽象讨论，缺乏对真实性溯源、证明力层级、认证程序等困境的回应，虽提及类型化思路，但未构建出与AI技术特性、证据功能适配的认定规则。

本文遵循以下思路展开：首先，拆解生成信息在证据能力、证明力、实操认定的困境；其次，以技术可追溯性为锚点，衔接证据三性原理，构建“底层逻辑—方法逻辑—价值逻辑”的分析框架，为规则设计提供法理基础；最后，通过生成方式和证据用途的类型化划分，构建认定规则。

二、人工智能生成信息的证据认定困境

（一）证据能力审查困境

1. 证据真实性审查困境

在来源审查层面，人工智能的虚拟主体属性使资质审查遭遇瓶颈。传统来源审查以证据生成主体资质为考察对象，主体资质作为判断来源可靠性的关键，但AI不具有主体资格，无法符合资质的法定要件，导致主体资质审查陷入困境。同时，算法生成环境的高度复杂性及封闭性，使得难以判断生成过程是否有外部干预、算法本身是否存在偏见或漏洞，以及训练数据中是否混入虚假信息。在内容核对层面，生成信息是对客观事实的创造性重构，其内容与传统证据或已知事实的关联性极弱，不能单纯以比对方式进行真实性验证。深度伪造辩护的出现，可能消解刑事诉讼中对证据的信任基础（刘学敏，2024）。依据《中华人民共和国刑事诉讼法》（以下简称《刑事诉讼法》）第55条“只有被告人供述，没有其他证据的，不能认定被告人有罪”的规定，传统内容核对方法依赖证据链印证，但生成的创造性信息没有对应的客观事实证据，与其他证据之间没有印证关系。生成式人工智能具有生成表面真实、实则虚假信息的能力，而传统内容核对标准只能审查内容的表面合理性，无法识别技术层面的虚假性。这导致真实性审查流于形式，不能实质过滤虚假证据，违反了《刑事诉讼法》第56条非法证据排除规则的要求。虚假证据虽不是非法收集，但其对事实认定的误导性不亚于非法证据，若不予以排除，案件事实认定必然出错。

2. 证据关联性审查困境

由于算法决策、数据筛选标准及参数调整对输出结果的影响机制，难以用可视化方法呈现，法

律人工智能面向法律大数据和法律知识,运用机器学习算法与符号逻辑(魏斌,2022),即便引入算法解释工具,也只能就生成过程的局部环节进行有限拆解,不能做到全链路追溯。而关联性审查的前提恰恰需要厘清证据的事实来源,因此黑箱特性切断了生成信息与原始事实间的追溯路径,使得审查者无法确认信息生成所依据的数据是否与案件事实存在关联,亦无法判断算法是否基于案件事实进行运算。《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》(以下简称《电子数据规定》)第5条要求电子数据审查时要注意原始性、完整性,但溯源障碍阻碍了生成信息满足关联性审查对事实来源的要求。同时,溯源技术的适配缺陷加剧了关联性认定困境。电子数据溯源技术以存储载体及传输路径为对象,从存储介质中提取元数据以确定信息生成的时间、主体及环境,但生成信息具有动态生成、瞬时运算的特点,并不依赖固定存储介质即可完成输出,极易出现元数据缺失或碎片化的情形。而元数据作为描述数据来源、结构、上下文的信息,其缺失便意味着审查者无法厘清信息生成背景,也无法判断信息与案件事实在时间、空间、逻辑等要素上是否有可证明的关联点。依据《刑事诉讼法》第50条证据经查证属实的要求,关联程度不明的信息理应排除于定案根据之外。但正因缺乏溯源手段,法官难以就关联性进行裁判。此外,溯源能力的缺失导致审查者无法排查信息生成过程中是否存在外部干预或算法偏差,算法偏差极有可能导致信息内容偏离客观事实,人为构造虚假、伪造的关联。这种技术异化形成的关联关系脱离了经验法则,而外部干预本身就会让生成信息刻意指向或回避某案件事实。

3. 证据合法性审查困境

主体合法性方面,传统证据合法性要求生成主体具有法律资格且能独立承担责任,而生成信息是以算法执行预设程序的方式作出的,故其并无独立意思表示与实质性责任能力。AI开发者、使用者、平台的责任边界既难以厘清,又难以确定符合法律规定的证据生成主体。生成式人工智能生成的信息在某些情况下可以作为诉讼证据,但需满足可靠性、相关性、合法性等条件(韩旭,2025)。程序合法性方面,《电子数据规定》设定了电子数据收集、提取、固定的程序要求,但电子数据具有信息动态生成、瞬时运算的特性,导致其收集程序极难适配。实践中对此类信息尚无收集、固定规范,导致在收集过程中没有可遵循的法定程序以及完整记录生成环境与参数,违反了《刑事诉讼法》第52条严禁以非法方法收集证据的规定。内容合法性方面,生成信息的内容以训练数据及算法模型为基础,若训练数据中包含非法获取的个人信息、虚假信息或侵权内容,生成信息本身即违法,也违反了《中华人民共和国个人信息保护法》(以下简称《个保法》)确立的个人信息处理的合法性要求,以及《中华人民共和国数据安全法》(以下简称《数据安全法》)有关数据使用合规性的规定。更严重的是,某些生成信息涉及危害国家安全、侵害他人合法权益的内容,不符合证据内容不得违反禁止性规定的要求,但审查体系难以排查此类内容的违法风险。

(二) 证据证明力评估困境

1. 证明力判断标准缺失

生成信息的来源可靠性判断缺乏法定标准。《电子数据规定》第22条要求,审查电子数据真实性关注是否具有数字签名、收集提取过程是否可重现等,但生成信息的算法黑箱特性导致其生成无法进行可视化检验,没有传统证据生成主体的资质背书,也难以满足提取过程可重现的要求。传统标准中来源可靠与人类主体的中立性、专业性相关,但生成信息的来源是算法模型与训练数据,《电子数据规定》虽对电子数据来源审查有规范,却未针对算法模型的合规性、训练数据的真实性设置审查条款。未来科技对传统司法的冲击不仅是人工作业的替代,更可能在深度学习的场合取代

人作为决策者的主体地位（胡铭和宋灵珊，2021）。同时，生成信息的内容一致性与印证程度判断缺乏指引。《刑事诉讼法》第55条规定，证据确实、充分需满足综合全案证据排除合理怀疑，《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》（以下简称《刑诉法司法解释》）第139条和第140条要求结合全案证据综合判断，排除矛盾和疑问，但生成信息可能是对客观事实的创造性重构，与传统证据的关联性较弱，难以通过证据链形成印证。由于没有明确生成信息在印证体系中的权重以及采信所需的印证标准，也未明确其与其他证据冲突时的取舍规则，导致法官无法依据法定标准判断其证明价值。

此外，差异化判断标准的空白进一步加剧了证据证明力评估的困境。不同技术复杂度、生成方式的生成信息在可靠性上存在差异，但《刑事诉讼法》及相关司法解释均未确立差异化的证明力判断规则。《电子数据规定》虽然针对电子数据的不同类型设置了审查要点，但未区分传统电子数据与生成信息的差异，也未对弱AI、强AI生成信息的证明力判断进行区分规定，这导致法官缺乏统一的法定指引，只能依赖自由心证作出判断，违背了《刑诉法司法解释》第140条“运用证据进行的推理符合逻辑和经验”的要求，也容易引发同案不同判的风险。

2. 证明力层级定位模糊

生成信息与传统证据的层级对比缺乏法定依据。当前由人工智能系统分析形成的证据已经出现在法庭上，对传统的刑事诉讼程序和证据制度提出了新挑战（余鹏文，2024）。生成信息作为数字化形式呈现的证据，一般被归入电子数据范畴，但目前尚未厘清其与书证、物证、证人证言等证据间的证明力层级关系。传统电子数据的证明力可依据《电子数据规定》第22条至第24条所列标准予以认定，而生成信息的黑箱化、动态性特点使其不满足标准，但尚无法条明确其证明力是否低于传统电子数据或其他证据。同时，生成信息内部层级划分缺乏立法依据。不同类型生成信息的技术特性差异明显，辅助生成型信息规则明确、逻辑可追溯，可靠性较高；而自主生成型信息以深度学习自主运算为基础，黑箱化程度极高，可靠性风险大。但《电子数据规定》没有对不同类型生成信息的证明力层级进行区分，且其对电子数据的完整性、真实性虽有校验要求，却未针对AI技术复杂度设计差异化的审查标准，法官难以依据法定规则确定二者的采信优先级。更根本的问题是证据类型定位模糊，生成信息表面看似证明了案件事实，但因生成逻辑不明、真实性存疑，不能达到直接证据的要件标准。若作为间接证据，该证据与案件事实的关联强度未满足《刑诉法司法解释》第140条所列的与其他证据结合形成证明体系的判断标准。此外，《司法鉴定程序通则》第5条要求司法鉴定应遵循科学、客观原则，但针对生成信息的鉴定标准尚不存在，无法基于鉴定意见补强其证明力。

（三）证据认定实操困境

1. 证据保存完整性困难

生成信息的数字属性导致证据篡改的成本极低、隐蔽性极强。算法模型可以用微调参数、替换训练数据片段、加入外部干扰因子等方式对所生成的信息作局部修改或整体重构，而修改后的信息在形式、外观上都与原始信息几乎一致，肉眼难以察觉篡改痕迹。人工智能的司法应用暴露出技术程式歧视、算法黑箱和无法灵活裁判的弊端（刘妍，2022）。更重要的是，篡改无需专业设备，普通用户用简单的AI工具便能实现。

完整性验证技术在处理生成信息时存在缺陷。传统电子数据的完整性验证采用哈希值校验、数字签名等方法，以信息内容的固定性为前提，通过比对信息生成前后的特征值来判别数据是否被篡改。但生成信息具有动态性特征，其内容常因算法模型迭代、运算环境变化而作细微调整，哈希值

等特征值必然随之发生变化,因此传统完整性验证技术极易误判信息完整性状态。同时,针对生成式人工智能的完整性验证技术没有形成标准化体系,不同技术方案对信息完整性的判断标准各不相同,部分技术甚至不能覆盖复杂类型的生成信息。正因缺乏统一、可靠的技术手段保障生成信息的完整性,虚假信息进入司法程序的风险大大增加。《刑事诉讼法》第55条规定了“证据确实、充分”的要求,故完整性存疑的信息不能作为定案根据。但由于缺乏统一的验证标准,法官难以认定信息的完整性,虚假信息极有可能被错误采信。

2. 证据认证程序缺失

从质证程序来看,传统质证围绕证据的生成主体、来源、内容展开,但生成信息的技术特性使得质证难以触及核心问题,当事人通常缺乏对算法原理、生成过程的专业认知,无法就技术层面的争议展开辩论,这与《刑事诉讼法》第198条控辩双方可以对证据和案件情况发表意见且可以互相辩论的要求不符,质证也就失去了意义。同时,证人出庭制度无法适配该类信息,AI无法作为证人出庭,而开发者或使用者对生成过程的了解往往局限于操作层面,无法解释算法运算逻辑,这就导致证人出庭无法提供有效证言,质证无法深入审查证据生成的技术细节,难以发现潜在的技术缺陷或虚假风险。人工智能在证据审查中的应用存在证据审查建构模型数据样本不充分、证据规则结构化转换不完整、证据审查程序缺乏可视性等风险和问题(谢登科和周鸿飞,2024)。从认证辅助机制来看,现有程序没有强制引入技术专家的规定。生成信息的审查必然涉及专业技术知识,应当由技术专家提供专业意见,当事人亦可申请人民法院通知有专门知识的人出庭,就鉴定人所作鉴定意见或专业问题发表意见。但司法实践中技术专家出庭多依当事人申请,且对专家资质的认定标准、专家意见的法律效力都没有规定,因而专家意见的专业性、客观性都难以保证。同时,目前尚无针对生成信息鉴定的鉴定机构及鉴定标准。《司法鉴定程序通则》第5条规定司法鉴定应遵循客观、独立、公正的原则,但现有鉴定机构缺乏处理生成信息所需的鉴定技术及设备,又没有统一、可操作的鉴定标准,故其作出的鉴定意见尚不具备公信力。该类证据难以达到《刑事诉讼法》第50条所规定的证据须经查证属实的要求,认证程序也因此陷入僵局。

三、人工智能生成信息的证据类型化认定逻辑

(一) 技术适配与法理遵循的底层逻辑

1. 以技术可追溯性为锚点

技术可追溯性是破解算法黑箱与证据溯源困境的前置条件,其源于《刑事诉讼法》第50条“证据必须经查证属实,才能作为定案的根据”的要求。来源可靠与生成透明原则是证据查证属实的前提,构建AI裁判模型算法审查制度成为智能裁判体系建设的根本保障(杨延超,2022)。技术可追溯性的要求是完整、连续、不可篡改地记录生成全链路信息,进而形成完整还原生成过程的技术档案,其中包括算法模型的版本参数、训练数据的来源与筛选标准、生成指令的发起主体与时间节点、运算过程的中间变量变化以及输出结果的初始状态等要素。

技术档案作为技术层面的溯源依据,承担衔接传统证据规则的功能,回应了《电子数据规定》第5条对电子数据原始性、完整性的审查要求。通过技术档案的核查,审查者能够打通生成信息与原始案件事实间的关联路径,明确信息生成所依据的数据是否与案件事实存在实质关联,排查生成过程中是否存在外部干预或算法偏差的可能性,以此减少因算法黑箱导致的虚假关联风险。更为重要的是,完备的技术档案能够转换生成信息的来源审查路径,将审查重心从虚拟主体资质核验转移

至生成过程可追溯性核查，符合电子数据审查完整性优于主体资质单一验证的证据理念。

2. 衔接证据三性认定原理

通过要素式审查、附条件相关性、技术性鉴真和双重可靠性分析，分别对生成式人工智能证据的合法性、相关性、真实性和可靠性作出有效判断（熊晓彪，2025）。重构真实性审查，将审查划分为技术层面的生成真实性及内容层面的客观事实关联性。依据《刑诉法司法解释》第139条“综合全案证据审查证据真实性”的要求，先以技术档案核查的方式确定生成过程没有外部干预、训练数据没有虚假成分、算法运算连贯稳定，继而考察所生成的信息内容是否与客观事实或其他查证属实的证据存在合理关联，避免生成信息的创造性重构导致传统证据印证规则失灵。此外，“客观事实关联”允许在客观事实的基础上作合理的创造性整合，但必须恪守事实本质，所涉事实要素不得虚构或歪曲。通过厘清技术关联及事实关联的审查标准，完成关联性审查的分层递进。技术关联审查用于核验生成数据与算法模型是否匹配，确保信息从与案件相关的算法运算中生成，排除因数据、模型不匹配所致的生成偏差，避免无关数据进入生成过程。事实关联审查用于核验生成信息内容与待证事实的对应关系，即该信息能否就案件事实的存在或不存在起到证明作用，排除算法偏差所致的虚假关联，符合《电子数据规定》第8条对电子数据来源及案件关联性的审查要求。

通过明确合法性审查底线，保证主体、程序、内容合规。就主体合法性而言，要突破单一主体资格的审查框架，需要先厘清主体合法，即要件在于责任可归属性，再确认存在能够承担责任的主体，最后以技术档案、使用记录明确主体间的责任边界。具体而言，开发者就算法模型合规性、训练数据合法性负责，使用者就生成指令合法性、信息使用正当性负责，平台承担审核义务及安全保障责任。就程序合法性而言，需设计适配人工智能特点的收集、提取流程，参照《电子数据规定》中所列电子数据收集、提取的程序要求，明确生成信息的收集需完整、客观地记录生成环境、算法版本、训练数据来源等参数。就内容合法性而言，确立训练数据及生成结果合规的底线标准，即依照《个保法》第13条的规定，审查训练数据中是否含有非法获取的个人信息、国家秘密、商业秘密等内容，以及生成结果是否违反禁止性规定、危及国家安全、侵害他人名誉权或隐私权等权益，并据此建立内容违法风险排查机制。

（二）多元验证与分层认定的方法逻辑

1. 多元验证方法整合

依托技术验证化解证据完整性、真实性审查难点。通过技术手段还原生成过程的客观事实，为法律审查提供技术事实基础。鉴于生成信息易篡改、传统完整性验证技术适用性不足的问题，引入区块链存证技术固化生成全过程。依据《最高人民法院关于互联网法院审理案件若干问题的规定》（以下简称《互联网法院审理案件规定》）第11条的规定，利用区块链去中心化存储、时间戳固化、哈希值校验等不可篡改的特性，促使生成信息自产生之时即被固定。因此区块链存证可以验证信息内容的完整性，以及记录信息的生成时间、生成主体、运算环境等要素，以此强化信息的原始性及可追溯性。同时，技术验证还包含对生成日志及元数据的审查，参照《电子数据规定》第8条对电子数据原始存储介质的审查要求，提取算法运行记录、参数调整轨迹、数据输入输出明细、运算环境变量等信息，再以比对分析的方式验证生成逻辑的一致性及稳定性。若事实认定缺乏准确性，法律就会变得不可测，继而人们便无法高效地按照法律规定行事（艾伦和汪诸豪，2020）。从法律验证层面破解证明力标准缺失及合法性困境。在查明技术事实的基础上进行价值判断，厘清相关主体责任及证据效力。再就主体责任模糊问题，适用谁主张、谁举证的规则，确定差异化的举证

责任分配规则。辅助生成型信息因人类对其控制程度高、责任归属明确，故由使用者承担主要举证责任，就生成指令的合法性、生成过程的可控性、内容的真实性予以证明。自主生成型信息因人工智能自主性强、技术复杂度极高，故由使用者与开发者承担举证责任，使用者就信息使用目的及与争议事实的关联性举证，开发者就所涉算法模型的合规性、训练数据的合法性举证，平台若未尽审核义务则承担补充举证责任及赔偿责任。

针对程序合规性问题，在遵循《电子数据规定》对电子数据收集、提取程序要求的基础上，制定生成信息收集规范，从而明确收集过程必须记录生成环境、算法版本、训练数据来源等参数。针对内容合法性审查的难点问题，结合《数据安全法》第21条与《个保法》第13条的要求，构建源头审查和结果审查的合规审查机制，源头审查聚焦训练数据的收集是否合法、是否经过必要的授权以及是否存在非法收集个人信息、窃取国家秘密等违法情形；结果审查聚焦生成信息的内容是否存在违法性、是否危害国家安全、损害社会公共利益以及是否侵害他人合法权益。

2. 分层认定规则

从人类对生成过程控制的程度及责任归属的明确性出发，按生成方式分层需要赋予人工智能证据独立的法律地位，将人工智能证据列入法定证据种类中（谢登科，2025）。辅助生成型信息的生成过程由人类以指令形式控制，人工智能仅起辅助作用，故此类证据可控制度高、责任归属清晰，审查重点则聚焦人类指令的合法性及所生成内容的一致性，应当验证指令文本的完整性、人类修改痕迹的真实性，无需介入算法底层逻辑。此时算法的功能与传统文字处理软件等工具没有本质区别，故审查应回归人类行为的合法性及真实性。人类对自主生成型信息的生成过程控制度低，人工智能以深度学习的方式自主生成信息，故责任归属相对模糊、技术风险突出，需强化对训练数据真实性、算法无偏性的审查。具体而言，举证主体应提供训练数据来源证明及算法无偏见性报告，并依照《刑事诉讼法》第55条与其他非AI证据形成印证链。从信息与案件事实的关联程度及对裁判结果的影响出发，按证据用途分层。事实证明型信息关系案件实体裁判，故其真实性、合法性关乎案件事实的认定结果，应适用《刑事诉讼法》第55条“证据确实、充分”的标准，做到技术上生成真实、内容完整，法律上形式合法，且与其他证据形成闭环印证。程序辅助型信息只需服务司法程序的推进，并不证明案件事实，对实体裁判结果没有实质影响，故可简化技术审查流程，仅就其关联性是否具有事实误导性予以审查。只要验证信息内容与程序环节相关且无事实误导性即可，无需进行技术鉴定或专家评审。

（三）效率与公正平衡导向的价值逻辑

1. 兼顾司法效率需求

首先，构建标准化的审查流程。针对生成信息认定环节，明确划分技术初审、法律审查和综合认定阶段，实现分层推进。技术初审由司法技术部门或委托的第三方技术机构完成，核查技术档案的完整性、区块链存证的有效性以及生成日志的一致性，形成客观上不涉及法律的技术报告；法律审查由承办法官主导，聚焦证据三性与证明力判断，依据技术初审报告并结合当事人质证意见审查合法性与关联性，综合判断证明力大小，从而完成法律价值判断；综合认定阶段由法官结合技术初审报告与法律审查意见，在庭审中组织当事人进行最终辩论后作出认定结论。故此，应当秉持证据裁量的基本立场，用证据裁量能动主义克服证明标准客观化的缺憾（徐阳和魏溢男，2024）。

其次，制定统一的技术及法律审查标准。在技术标准层面，通过明确区块链存证的技术参数、生成日志要素、哈希值校验的操作规范等要求，确保不同地区、不同法院对同类信息的技术验证标

准一致，从而避免因技术标准不统一所引发的争议及重复验证。在法律标准层面，明确不同类型生成信息的举证责任分配规则、合法性审查要点以及证明力判断要素等要求，从而避免法官因缺乏统一标准而导致自由裁量过大。

最后，建立低风险信息快速审查通道。针对程序辅助型、辅助生成型的低风险信息采用简化的审查流程，只就要件予以审查，技术上先核查生成指令与所涉信息是否有关联、是否完整，由此确定信息与程序推进相关且未篡改，再从法律角度核查主体责任是否明确、内容是否无违法性，确保责任可归属、无法律瑕疵。因此无需技术鉴定或专家评审，仅以人工审查结合简单技术校验即可认定。

2. 保障司法公正底线

首先，强化高风险信息风险防控。就自主生成型、事实证明型等高风险信息而言，应建立全链条风险防控机制。在真实性风险防控上，由举证主体提供算法合规证明及训练数据抽样验证报告，以专业技术手段排除深度伪造风险，继而根据《刑事诉讼法》第56条将技术上无法确认真实性、有明显篡改痕迹或者所载内容彼此矛盾的信息，作为虚假证据排除，即便该信息系合法收集，其对事实认定的误导性不亚于非法证据。在合法性风险防控上，对训练数据的合法性及生成程序的合规性予以审查，对存在训练数据非法收集、生成程序违法等情形的信息，适用非法证据排除规则。其次，坚守关联性底线，防范虚假关联对事实认定的不利影响。依据《刑事诉讼法》第50条，先用技术档案核查确定生成数据与案件事实的关联性，排除无关数据介入生成过程，再作内容审查，判断所涉信息是否指向待证事实、是否对事实的存在或不存在有实质性证明效果，由此排除虚假关联信息。

此外，通过保障当事人的程序参与权，破解质证困境。以人为中心的经验理性主义以及算法数据、过程、结果的可解释性等措施进行体系矫正（龚善要，2023），针对生成信息技术专业性强、当事人难以质证的问题，可依据《刑事诉讼法》第197条的规定，明确技术专家出庭的强制性义务，对于自主生成型、事实证明型信息的认定，若当事人提出异议，法院应通知技术专家出庭，就算法原理、生成逻辑、技术验证结果等问题进行通俗易懂的说明，并接受控辩双方的询问与质证。同时，细化专家辅助人的资质标准与意见效力，明确专家辅助人需具备技术领域的专业资质，其意见可以作为质证依据与法官认定的参考资料。

四、人工智能生成信息的证据类型化认定进路

（一）类型化适配的证据能力审查

1. 证据真实性审查

对辅助生成型信息的真实性审查，应围绕人类控制痕迹展开。一是审查生成指令的完整性，要求举证主体提交指令链路材料，即初始需求文本、中间修改意见、最终确认文件，继而根据《电子数据规定》第5条所列电子数据原始性要件，以指令文本的连贯性验证生成方向的可控性，排除指令模糊导致的生成失控风险；二是溯源人类修改痕迹，从生成日志中提取人类操作元数据，诸如修改时间戳、修改内容对比、修改意图说明等，凭借日志的完整性、连续性证明人类对生成结果的支配地位，符合《刑诉法司法解释》第139条综合全案证据审查真实性的要求；三是简化技术工具合规性审查，核查AI工具是否按照《生成式人工智能服务管理暂行办法》的规定完成备案手续，要求开发者提交技术合规声明，就工具是否含算法偏见或功能性漏洞予以验证。在法律层面，要求使用

者签署真实性承诺函, 书面说明指令合法性、修改痕迹真实性、内容与客观事实的关联性等事项, 若作出虚假陈述, 即按《刑事诉讼法》第54条承担伪证或者妨碍诉讼的责任。

对自主生成型信息的真实性审查, 应以全链路算法溯源作为基础。一是算法模型合规性审查, 要求举证主体提交所涉模型的备案材料、算法原理说明书, 审查模型是否存在偏见性训练或重大技术漏洞。二是训练数据真实性及合法性审查, 举证主体需提供训练数据的来源证明、数据清洗及筛选规则、涉密或敏感数据脱敏报告, 再根据《个保法》第13条查验训练数据是否包含非法获取的个人信息或虚假数据, 从源头上排除数据污染所致的信息失真风险。三是生成日志完整性审查, 参照《电子数据规定》第6条提取生成全流程实时日志, 通过区块链存证技术固化日志信息, 继而根据《互联网法院审理案件规定》第11条的规定, 以时间戳、哈希值等技术手段确保证据不可篡改。在法律层面, 建立开发者及使用者的真实性担保责任机制, 开发者就算法合规性、训练数据真实性负担担保义务, 使用者就信息使用范围的正当性负担担保义务, 任一主体未尽担保责任, 将致使案涉证据的真实性要件无法成立。

事实证明型信息的真实性审查需要叠加内容实质性的关联验证, 通过研判所生成内容与已知客观事实以及其他查证属实的证据是否存在合理关联, 由此排除创造性重构导致的印证失灵问题。程序辅助型信息需要简化真实性审查标准, 人机间更合适的定位应当是由法官承担说理责任, 机器予以全面辅助(周翔, 2024), 仅需验证信息无明显失真、无事实误导性即可, 无需过度介入技术细节。

2. 证据关联性审查

首先, 进行技术关联审查。先就生成信息与案件事实的技术关联性加以审查, 防止因算法偏差带来的无关信息介入。具体而言, 对辅助生成型信息作指令进行关联性审查, 考察人类所输入的生成指令是否为待证事实作出, 并检验指令与生成结果的一致性程度, 由此通过指令文本与生成结果的比对排除无关指令驱动生成的信息。对自主生成型信息作训练数据与算法匹配度的审查, 核实生成信息所依托的训练数据是否含有案件相关要素, 算法模型是否具备处理此类案件数据的功能, 再借助技术档案核查生成时所调用数据的关联性, 防止无关数据介入产生的虚假关联。其次, 进行事实关联审查。首先确定生成信息内容与待证事实的实际关系, 针对辅助生成型信息的事实关联审查分析, 只需就生成内容与指令要求的一致性、与案件事实的表面契合度予以验证, 无需介入技术细节。自主生成型信息的事实关联审查, 需结合案件背景、事实要素判断生成信息是否符合客观事实, 防止算法自主运算中所形成的虚假关联。最后, 事实证明型信息的关联性审查需达到实质影响证明效果的标准, 需证明所生成的信息直接或者间接证明待证事实的存在或不存在, 由此通过技术关联和事实关联的方式予以检验并排除虚假关联风险。程序辅助型信息的关联性审查可简化为程序适配性检验, 辅助裁判模型是智能司法基础理论的核心内容(高翔, 2021)。只要证明信息内容与推进的程序环节直接相关即可, 无需就其与案件事实的关联作审查, 且应明确列举无关联性的排除情形, 包括技术关联缺失、事实关联虚假以及关联程度微弱的信息等。

3. 证据合法性审查

主体合法性审查围绕责任归属展开, 需要突破传统单一主体资格的审查框架, 按生成方式实现类型化责任分配。辅助生成型信息需明确举证主体为人类使用者或指令发出者, 由其承担指令合法性、修改行为合法性的责任, 若存在违法指令或恶意修改, 则依据《刑事诉讼法》第54条承担责任; AI工具开发者仅承担工具本身的合规责任, 若工具存在未备案或已知漏洞却未告知的情形, 需承担补充责任。自主生成型信息需建立开发者和使用者的责任体系, 开发者承担算法合规性、训练

数据合法性的责任，若因算法缺陷或训练数据非法导致信息违法，需依据《数据安全法》第45条承担赔偿责任；使用者承担生成指令合法性与信息使用范围合法性的责任，若指令违法或超范围使用信息，则依据《刑事诉讼法》第54条承担责任；平台未尽到审核义务的，需承担补充责任。同时，程序合法性审查需匹配AI特性设置审查流程，按生成方式及用途对程序要求加以细化。对于辅助生成型信息，程序审查简化为指令及收集记录的完整性，即收集过程应完整记录生成指令、修改痕迹、使用者身份等信息，且参照《电子数据规定》中所列的电子数据收集的要求，以此保证过程可追溯、可重现。对于自主生成型信息，程序审查贯彻全流程规范记录的原则，要求收集过程记录生成环境、算法版本、训练数据来源、生成日志等要素，必要时由第三方机构对收集过程的合规性予以见证。同时，根据证据用途补充适配性要求，事实证明型信息需另行提交程序合规性说明，由法官结合质证意见就程序合法性予以审查，而程序辅助型信息则简化程序审查，只需检验收集过程是否存在明显违法情形即可。

此外，内容合法性审查需厘清训练数据及生成结果合规的底线标准，按类型化方式适用不同强度的审查规则。应当从防范虚假信息、限制生成式人工智能裁判、保护数据安全等多个层面着手对生成式人工智能进行规制（郑曦，2023），所有类型的生成信息都需符合训练数据中不得含有非法获取的个人信息、国家秘密、商业秘密等内容的要求，并根据《个保法》第13条及《数据安全法》第21条的规定，提交训练数据合规证明。相应地，生成结果不得违反禁止性规定、危害国家安全、侵害他人合法权益，从而规避内容违法风险。具体而言，事实证明型信息应委托专业机构予以核查，确保没有隐性违法内容，而程序辅助型信息只需作形式审查，排查是否存在事实误导性内容，若存在模糊表述或虚假暗示，允许修改后重新提交，无需否定其合法性。

（二）类型化适配的证据证明力评估

1. 证明力判断标准

辅助生成型信息的证明力判断标准需从人类控制程度及内容一致性考察，要素包括生成指令的完整性与明确性、人类修改痕迹的真实性与合理性、技术工具的合规性，以及与其他证据的印证程度。若各要素都符合标准且彼此印证，其证明力等同于传统电子数据，有部分要素瑕疵时应以其他证据补强，要素根本缺失时应直接否定其证明力。同时，自主生成型信息的证明力判断标准以算法可靠性、多证据印证为根本，首先要厘清算法证据的法律地位，继而设计审查规则，由官方主导并优化算法证据的生成、监督与公开（张迪，2023）。通过审查算法模型的合规性及透明度、训练数据的真实性及合法性、生成日志的完整性及非AI证据的印证程度，所有要素都须达标，且要与至少两项非AI证据形成印证链，方能确认其证明力。若任一要素缺失或者印证不足，原则上都应借助第三方鉴定或专家评审予以补强，不能合理补强的，直接予以否定。此外，事实证明型信息适用证据确实、充分的标准，判断要素均需达到排除合理怀疑的程度，且印证链需形成闭环，无任何矛盾或遗漏；程序辅助型信息简化为无误导性与关联性标准，仅需验证信息内容无事实误导性、与程序环节直接相关即可，不要求过高的印证程度，证明力仅作为程序推进的辅助参考，并不影响实体裁判。在更多领域开发专用型司法人工智能技能，让其在辅助法官决策、替代事务性工作以及预测裁判结果等方面，为法官提供更多帮助（胡昌明和张吟，2025）。明确否定证明力的情形包括：存在算法偏见或漏洞、训练数据虚假、生成日志篡改以及无法与其他证据形成印证等，均应否定证明力。

2. 证明力层级定位

结合生成方式与证据用途构建证明力层级排序体系，明确不同类型生成信息与传统证据的采信

优先级,通过技术理性规则制约司法任意性(赵杨,2021),从而确保层级定位精准可操作。第一层级是原始书证、物证及传统电子数据,该层级证据因原始性、可靠性最高,采信优先级高于所有类型的生成信息,当生成信息与该层级证据存在矛盾时,以该层级证据为准。第二层级是辅助生成型事实证明信息,该类信息因人类控制度高、生成逻辑可追溯,经完整验证与印证后,证明力等同于传统电子数据,采信优先级仅次于原始证据。若其与其他第二层级证据形成印证,可作为定案依据;若与原始证据存在矛盾,需重新核查验证过程。第三层级是自主生成型事实证明信息,该类信息即便经完整验证与印证,证明力仍低于辅助生成型事实证明信息与传统电子数据,需与至少两项非AI证据形成印证链才可作为定案依据,且不得单独作为认定事实的唯一依据。若其与第二层级及以上证据存在矛盾,优先采信第二层级及以上证据,除非有充分的技术验证与鉴定意见证明自主生成型信息的真实性。第四层级是程序辅助型信息,该类信息仅服务于司法程序的推进,不具备独立证明案件事实的证明力,采信优先级最低,仅作为辅助参考依据。若其内容与其他层级证据存在矛盾,一律以其他层级证据为准,不得因程序辅助型信息否定事实认定。同时,明确层级排序的例外规则,若辅助生成型信息存在严重技术瑕疵,证明力可降格至第三层级;若自主生成型信息经权威第三方鉴定确认算法完全合规、生成透明,且与多项原始证据形成完美印证,证明力可提升至第二层级;程序辅助型信息无论验证情况如何,均不得提升至第三层级及以上。

(三) 类型化适配的证据认定操作

1. 证据保存完整性

就自主生成型、事实证明型等高风险信息,采用区块链存证及全链路日志固化的强化保存规则。所有生成的信息从产生之时起就通过符合国家标准的区块链存证平台予以存证,同时依据《互联网法院审理案件规定》第11条的规定,区块链存证所载时间戳、哈希值、节点共识记录均可作为认定生成时间、内容完整性的依据,借此解决单方存证中篡改证据的风险。同时,完整提取全流程日志并以双重哈希值校验技术保证日志不可篡改。保存主体方面,自主生成型信息由开发者、使用者本人保存技术档案,事实证明型信息由法院指定的第三方机构代为保存,以此避免保存主体单方篡改的风险。就辅助生成型、程序辅助型等低风险信息,采用简化哈希校验和主体责任担保的保存规则。辅助生成型信息以简单哈希值校验内容完整性,只需保存生成指令、修改痕迹等材料,由使用者予以保存并作出完整性承诺。程序辅助型信息以人工肉眼直接核查信息完整性,无需进行复杂技术验证,保存主体可以是使用者或办案机关,但必须保证所保存材料可随时核查。

自主生成型信息需定期进行哈希值比对,若出现哈希值不一致,则委托第三方机构核查是否存在篡改或算法迭代导致的内容变化;事实证明型信息应在庭审前重新进行区块链存证有效性验证,确保庭审中使用的信息与原始存证信息一致;辅助生成型与程序辅助型信息仅需在提交司法机关时进行一次完整性验证,后续若出现完整性争议,由保存主体承担举证责任。经验证存在篡改痕迹或信息缺失的,则直接否定证据能力;制度上应将算法治理融入诉讼法规范治理体系,创新人工智能辅助司法裁判应用场景下的程序权利保障机制(杜雨钊和唐力,2025),因算法迭代或环境变化导致的内容细微调整,需提交技术说明并经第三方验证,证明调整不属于篡改所致,否则仍否定其完整性。

2. 证据认证程序

自主生成型信息的认证程序细化完善为技术质证、专家出庭和第三方鉴定三类流程。质证焦点围绕算法合规性、训练数据真实性、生成日志完整性以及区块链存证有效性等技术问题展开;依

据《刑事诉讼法》第197条的规定,明确技术专家强制出庭义务,若当事人对生成信息的真实性或可靠性提出异议,法院必须通知技术专家出庭,就算法原理、生成逻辑、技术验证结果等专业问题进行说明,并接受控辩双方询问;对于复杂类型的自主生成型信息,应强制要求提交第三方鉴定意见,鉴定内容包括信息是否存在篡改、算法是否合规、内容与客观事实的偏差度等,且鉴定意见应作为认证的必要依据,无鉴定意见的不得作为定案根据。法官审查时,则结合技术质证意见、专家说明和鉴定意见综合判断。辅助生成型信息的认证程序可以简化为指令及修改痕迹质证、常规审查环节,应强调司法工作人员的主体地位(陈灵峰,2021),故其质证焦点为生成指令是否清楚、修改痕迹是否真实、所用技术工具是否符合规范。当事人可以申请AI工具开发者出庭就技术原理作出说明,而无需第三方鉴定,法官依质证意见及技术审查报告即可进行判断。

事实证明型信息的认证程序需遵循庭审实质化要求,所有质证环节均需在庭审中公开进行,技术专家与鉴定人出庭接受交叉询问,法官需在裁判文书中说明认证理由;有效发挥司法人员的主观能动性,避免对人工智能的过度依赖(黄巍巍,2022),程序辅助型信息的认证程序简化为书面审查和当庭说明,无需组织专门的技术质证,仅需举证主体当庭简要说明信息的生成过程与用途,法官进行书面审查后即可作出认定。此外,构建认证程序的救济机制。当事人对自主生成型信息的鉴定意见或专家说明有异议的,可申请重新鉴定或要求补充专家出庭;对辅助生成型信息的认证结果有异议的,可提交补充技术材料证明自身主张;法官未按类型化认证程序进行审查的,当事人可将其作为上诉理由。

五、结语

生成信息对传统证据法体系的挑战,本质是数字时代技术创新与司法秩序适配的典型命题。从更宏观的视角看,生成信息的刑事证据认定不仅是对单一证据类型的规制,更是司法机关适应数字时代的制度探索。从司法实践落地与政策完善层面看,仍需完善配套制度。一是推动专门司法解释与裁判规则细化,明确生成信息的证据定位,细化不同类型生成信息的审查标准、举证责任分配规则、非法证据排除细则;二是构建司法与技术协同的审查机制,引入第三方技术存证、算法合规鉴定、专家辅助出庭机制,统一证据完整性校验、算法溯源、真实性鉴真的技术标准;三是建立动态化风险规制体系,结合人工智能迭代趋势,更新证据审查规范与技术认定标准;四是强化司法裁判统一指引,通过发布典型案例、细化裁判文书说理规范,明确不同场景下生成信息的采信标准与证明力层级。唯有坚持技术为用、法律为体的原则,方能为司法公正注入数字时代的新动能。

参考文献

- [1] 艾伦·汪诸豪.人工智能与司法证明过程:来自形式主义和计算的挑战[J].证据科学,2020(5):588-599.
- [2] 陈灵峰.司法人工智能的技术效应与应用边界[J].求索,2021(6):182-190.
- [3] 程龙.人工智能辅助量刑的证据化改造[J].现代法学,2025(2):174-188.
- [4] 丁国峰,寿晓明.经营者滥用人工智能生成合成信息不正当竞争的技术治理路径[J].福建论坛(人文社会科学版),2025(5):47-67.
- [5] 杜雨钊,唐力.人工智能辅助司法裁判的正当性边界与制度约束[J].新疆大学学报(哲学社会科学版),2025(3):106-118.
- [6] 高翔.智能司法的辅助决策模型[J].华东政法大学学报,2021(1):60-75.
- [7] 龚善要.人工智能司法应用的实践审思与完善[J].国家检察官学院学报,2023(5):95-108.
- [8] 韩旭.以DeepSeek为代表的生成式人工智能信息证据能力问题研究[J].湖南大学学报(社会科学版),2025(4):131-139.
- [9] 洪刚.大数据证据在刑事庭审中运用的隐忧与防范[J].法治论坛,2024(2):37-52.
- [10] 胡昌明,张吟.中国司法人工智能面临的挑战及应对[J].学习论坛,2025(2):128-136.
- [11] 胡铭,宋灵珊.“人工+智能”:司法智能化改革的基本逻辑[J].浙江学刊,2021(2):12-23.
- [12] 黄巍巍.证据标准的理论阐述与实践思考[J].中国人民公安大学学报(社会科学版),2022(1):110-118.

- [13] 刘学敏.人工智能时代“深度伪造辩护”对刑事诉讼的挑战及其应对[J].厦门大学学报(哲学社会科学版),2024(1):109-120.
- [14] 刘妍.人工智能的司法应用及其挑战[J].河南财经政法大学学报,2022(4):136-145.
- [15] 陆宇光.人工智能技术参与刑事证明的实践与进路[J].江汉论坛,2025(8):137-144.
- [16] 潘金贵,熊用坪.人工智能介入科学证据审查判断的可行性与作用路径[J].学术交流,2022(3):34-45.
- [17] 寿晓明.生成式人工智能模型竞争的反垄断监管因应[J].中国矿业大学学报(社会科学版),2026(1):121-142.
- [18] 魏斌.法律人工智能:科学内涵、演化逻辑与趋势前瞻[J].浙江大学学报(人文社会科学版),2022(7):49-67.
- [19] 谢登科,周鸿飞.司法人工智能在证据审查中的功能定位与风险规制[J].吉林大学社会科学学报,2024(3):61-72.
- [20] 谢登科.人工智能证据的类型分析与规则建构[J].学习与探索,2025(3):62-72.
- [21] 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(1):72-93.
- [22] 徐继敏,严若冰.论大语言模型材料的证据属性——以ChatGPT和文心一言为例[J].四川师范大学学报(社会科学版),2024(1):60-73.
- [23] 徐阳,魏溢男.人工智能时代证明标准客观化的负效应及其克服[J].齐鲁学刊,2024(1):82-96.
- [24] 杨延超.算法裁判的理论建构及路径选择——基于若干人工智能实验的启示[J].治理研究,2022(4):108-122.
- [25] 游办荣.人工智能赋能新时代审判工作高质量发展的机遇、挑战及应对[J].中国应用法学,2025(3):1-15.
- [26] 余鹏文.刑事诉讼中人工智能证据的法律性质和运用规则[J].中国刑事法杂志,2024(5):36-54.
- [27] 张迪.刑事诉讼中的算法证据:概念、机理及其运用[J].河南大学学报(社会科学版),2023(3):36-42.
- [28] 赵杨.人工智能时代的司法信任及其构建[J].华东政法大学学报,2021(4):73-82.
- [29] 郑曦.生成式人工智能在司法中的运用:前景、风险与规制[J].中国应用法学,2023(4):81-93.
- [30] 周翔.司法人工智能对裁判说理的辅助价值和实现路径[J].法学杂志,2024(1):111-127.
- [31] 卓翔,崔世群.论人工智能在证据推理中的辅助性定位[J].治理研究,2023(1):136-156.
- [32] 纵博.人工智能在刑事证据判断中的运用问题探析[J].法律科学(西北政法大学学报),2019(1):61-69.

【作者简介】寿晓明:安徽大学法学院博士研究生。研究方向:竞争法、数字法。

Classification of Criminal Evidence for Information Generated by Artificial Intelligence

SHOU Xiao-ming

(School of Law, Anhui University, Hefei 230601, China)

Abstract: After the large-scale application of generative artificial intelligence technology, a large amount of information generated by it enters criminal investigation and other scenes, becoming an important material for case adjudication. This kind of information has the characteristics of black box algorithm, fuzzy subject and creative content, which conflicts with the traditional evidence rules with human dominant generation, objective fact record and fixed carrier storage as elements, thus bringing difficulties such as evidence ability examination, proof evaluation and evidence identification. At the level of evidence ability, authenticity examination encounters the difficult problems of invalid source qualification and failure of content verification; relevance identification falls into the deadlock of substantial association judgment due to difficulty in traceability; legality examination faces the problems of vague subject responsibility, insufficient procedure adaptation and coexistence of content compliance risks. At the level of probative power, the lack of judgment standard and vague hierarchical positioning lead to great risk of different judgments in the same case. At the practical level of evidence, it is difficult to guarantee the integrity of evidence preservation, and the authentication procedure lacks special rules to ensure its reliability. In order to solve the dilemma, we should start from the three principles of evidence, link up the characteristics of generative technology, and take the traceability of technology as the anchor point to construct the analysis framework of underlying logic, method logic and value logic. At the practical level, based on the generation mode and evidence use, the classification is carried out: the auxiliary generation type is distinguished from the independent generation type, the fact proof type and the procedure auxiliary type, the rules such as the three-nature examination of evidence ability, the differential evaluation of proof power, the adaptation of practical operation process, etc. are constructed respectively, and the distribution of burden of proof, the standardization of cross-examination procedures, the technical path of integrity preservation and the expert auxiliary mechanism are clarified.

Keywords: artificial intelligence generated content; evidence identification; generative artificial intelligence; criminal evidence; artificial agents

(责任编辑:马莹)