论数字证据之刑事程序规制*

詹羽洪

（中国社会科学院大学法学院，北京 102488）

[摘 要]数字时代深刻变革刑事证据体系，数字化证据的广泛应用在延续传统电子数据审查路径的同时，更催生以大数据、算法和人工智能证据为核心的数字证据的刑事程序规制需求。数字证据依托算法驱动，具有客观性与主观性的复合属性，推动司法认知由经验归纳向算法理性转型。然而，当前缺乏有效的规制，数字证据在证据能力上面临双重困境：一方面，控辩双方在证据的运用能力上失衡，导致质证形式化，证据能力难以有效通过严格证明的过程得到确认，法官也因证据主体虚化而难以审查；另一方面，“脏数据”、算法偏见、隐私权侵害及无罪推定原则受冲突等问题，引发证据可采性与合法性遭受质疑。从刑事程序规制视角出发，在侦查阶段应当保障犯罪嫌疑人的知情权，规范数字证据收集的启动程序；在审查起诉阶段，应当完善审前证据开示制度与释明义务；在审判阶段，应当扩大非法证据排除规则的适用范围，完善数字性最佳证据规则、技术性直接言词规则与技术性意见证据规则。

[关键词]数字证据 证据开示制度 无罪推定原则 隐私权 非法证据排除规则

[中图分类号]D925.2 [文献标识码]A [文章编号]2096-983X（2026）05-0125-14

一、引言

随着数字时代的到来，区块链证据、算法证据、大数据证据、人工智能证据等新型数字化证据在刑事司法中的运用日益广泛，并引发证据制度重大变革。然而，实践与学理层面对上述证据的定位尚未统一，导致证据审查规则模糊，具有共同性的证据适用不同的审查规则。目前，在司法实践中，存在将大数据视作电子数据、鉴定意见、书证、独立证据等各种情形。①在学理上，关于是否应当将数字证据作为独立于现有证据种类存在争议。持传统证据说的学者认为，基于技术发展所提出的数字证据等新的概念都缺乏具体的分析，计算机技术或其他类型的高科技直接记录实体事实的部分应加入物证、书证或鉴定意见之列，除此之外都属于认识证据的手段。[1-3]持电子数据说的学者认为，应当将数字证据纳入电子数据范畴，并扩大电子数据的概念。[4-5]持电子数据与数字证据结合说的学者认为，应当将电子数据作为最基础的数字证据类型，结合区块链、大数据、人工智能和虚拟仿真等技术，整合为数

收稿日期：2025-06-24；修回日期：2026-06-28

*基金项目：中国社会科学院大学研究生科研创新支持计划“数字证据之证据类型与审查规则研究”（2026-KY-210）

作者简介：詹羽洪，博士研究生，主要从事刑事诉讼法学研究。

①如在覃胜龙故意杀人案、刘冠、刘金秋、李艳冰诈骗案等案件中，判决书将大数据证据归为书证，参见广西壮族自治区来宾市中级人民法院〔2021〕桂13刑初16号刑事判决书。在朝某危险驾驶案中，判决书将大数据证据归为鉴定意见，参见沈阳市铁西区人民法院〔2021〕辽0106刑初488号刑事判决书。在李华进贩卖毒品案中，判决书中将大数据证据作为独立证据，参见云南省双江拉祜族佤族布朗族傣族自治县人民法院〔2020〕云0925刑初163号刑事判决书。

字证据。[6-7]持数字证据独立说的学者认为，应当根据证据生成空间、固定、移送空间与审查空间，将证据分为传统证据、传统证据数字化、数字证据的三元结构。[8]

针对目前实践中存在多种做法，以及学理中对于证据名称、证据内涵、证据规则等争议，笔者认为，应当将依托算法生成的证据材料整合为数字证据，并作为独立证据种类存在。然而，基于算法属于仍在不断发展的科技，其最终形成的证据内容具有不确定性，需要在刑事程序中设立专门的规制路径，以审查其来源是否合法、内容是否真实可信。本文拟通过界定数字证据之基本特征，论述其相较目前已有证据种类独立规制之必要性，并围绕证据能力，提出刑事程序规制方案。

二、数字证据之基本范畴

数字证据是基于客观数据经算法处理生成的新信息，兼具主观性与客观性特征，其独特价值在于内蕴的算法理性。

（一）数字证据之内涵

围绕数字证据是否应当独立于电子数据成为新的证据种类，核心争议在于其与电子数据的关系界定。厘清数字化证据的发展脉络和具体内涵，有助于揭示数字证据与电子数据的区别。

追溯历史，早在20世纪70年代，域外学者便提出了“计算机产生的证据”概念，用以描述计算机依据人类预设指令运行生成的结果证据。[9]此类证据的核心特征在于其内容反映人类意志或客观世界在数字领域的投射，而非机器自身的主观判断。随着技术认知深化，学界又区分出“计算机产生的证据”和“计算机储存的证据”。[10]受限于当时技术，二者本质上仍是数字化记录与呈现内容。《中华人民共和国刑事诉讼法》（以下简称《刑事诉讼法》）于2012年修订中正式将“电子数据”纳入法定证据种类，定义为“案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据”①。这一定义强调了电子数据由系统依据既定规则处理固定输入数据，内容边界清晰且不包含系统通过学习自主生成的推断，本质上属于对已有客观信息的数字化记录，因此在取证程序和审查规则上具备统一处理的基础。

随着技术迭代，数字化证据形态经历了从聚焦单机环境的电子数据到应对海量信息的新型证据的代际演进。[11]其中主要包括区块链证据、人工智能证据、大数据证据、算法证据。区块链证据的核心价值在于利用分布式存储和密码学技术确保原始数据记录的不可篡改性，通常被视为一种特殊机制下的存证凭证。[4]与之不同的是，人工智能证据是指基于人工智能分析形成的可用于证明案件事实的机器意见[12]；大数据证据是指通过应用算法对数据集进行深度分析和处理形成报告，其中该报告能够揭示数据之间的关联性、模式和趋势，具备一定的预测能力[13]；算法证据是将海量的案件信息数据进行计算整合，形成结构化和信息化的案件场景自动解读与自动推理结果[14]。这三者的共同核心在于都依赖复杂算法对基础数据进行加工处理以生成新的信息内容。

基于各项证据定义上与技术上的差异，本文将大数据证据、算法证据和人工智能证据作为“数字证据”的具体表现形式。据此，笔者认为，数字证据是指以客观数据为基础，通过算法对数据进行深度处理、演绎、推理或模拟后所生成的新证据材料。由于这些证据并非对客观事实的直接记录，而是算法对原始数据进行“二次加工”的产物，其可靠性与证明力依赖于三个要素：基础数据本身的真实性、算法处理逻辑的透明度与可验证性，以及数据加工操作全过程的合规性。正是这些独特的生成逻辑，构成了数字证据独立于传统电子数据的理论基础。

（二）数字证据之特征

数字证据本质上是算法对数据集进行分

①《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》第1条。

析运算后生成的结果。其独特的、自动化程度更高的生成过程，使其区别于传统依赖人为观察、陈述或判断的证据，同时具备主观性与客观性的特征。

就其主观性而言，数字证据的可靠性深度依赖于人的设计、投入和操作，一些法院和学者认为，数字证据背后实质上反映的是其设计者或使用者的意图，人类的知识和意图是机器证据背后的真正“声明人”。[15]在此意义上，数字证据与人类证词一样，并非绝对客观的天然记录。因此，在刑事审判中，将机器证据作为证据提供时，必须确保其背景的充分审查和可信性测试。在诸多带有主观性特征的传统证据类型中，鉴定意见因其基于专业知识和技术的推理判断本质，与数字证据最具相似性。二者均非原始事实的直接记录，而是在基础证据之上，通过特定方法或技术演绎、分析后形成的意见，不同之处在于二者的生成机制。鉴定意见依赖具备特定资质的专家在审查时运用其专业认知和经验作出的个人化判断；数字证据是通过算法在既定规则下对数据进行智能化、自动化处理的产物，即在运算环节显著减少了人类的实时干预和个体主观因素的直接影响。这使得数字证据在一定程度上形成了独特的思考过程，与完全仰赖人工认知的主观证据存在差异。

就其客观性而言，机器明显缺乏道德判断或主动撒谎的能力，除非程序设计者有意为之。因此，相较于易受人类主观因素影响的证言证据，数字证据在一定程度上可被视为更稳定的“客观记录”，这与传统客观性证据有相通之处。例如，书证以书面形式记录原始的、未经加工的信息，并且以其记载的内容作为证据；电子数据则侧重于案件相关原始信息的数字化存储状态及其获取过程，通常涉及直接从案件现场获取的原始数据，以未经深度加工的形式提供信息。数字证据的本质不在于存储形态或原始记录，而是通过算法对数据进行加工后形成的信息产物。其核心价值在于通过算法增强数据的内在逻辑性、揭示其深层次的规律与关联性。这使得数字证据在揭示复杂事实、预测发展等方面，相比传统实物证据显示出独特效用。

综上所述，数字证据融合了基础数据的客观部分和算法对这些数据进行推理、演绎后形成的结论性部分，从而同时具备主观性与客观性属性。因此，将数字证据确立为独立的证据种类，不仅有助于明确其区别于传统电子数据、书证或鉴定意见的独特法律地位，而且能够促进司法实践中对数字证据形成合理的采纳、审查与运用规则。这种认定意味着数字证据的证明力和应用范围将得到更广泛的认可，其在司法证明过程中的作用也将被提升到一个新的层次。[16]

（三）数字证据之独特价值

在刑事诉讼证明过程中，常识常作为一种潜在的背景性知识而被法官下意识地运用，并且与直觉、逻辑推理和经验推理一道，共同构成了案件事实认定的认知框架。[17]188-189然而，在数字时代下，面对日益复杂的案件，法官依据自身的经验、常识与有限的逻辑推理去拼合离散证据，难以及时捕捉和理解海量信息之间的隐性关联，导致可能的关联性被忽略或遗漏。①

数字证据的独特价值，在于其内蕴的“算法理性”。算法理性是指通过预设或训练的算法逻辑，对输入的特定数据集进行自动化分析、处理、挖掘关联、推演模式，并输出具有逻辑一致性结论的能力。这种能力并非对原始事实的被动记录或存储，也不同于依赖专家个体认知的主观推论，而是通过算法模型主动构建证据间的结构性关系和逻辑链条。数字证据的引入，正是凭借这种算法理性改变了传统证明的局限性。算法不仅能构建揭示证据间复杂的关联，更能将证据的证明作用从传统的、点对点式的相互印证，提升至对整个证据体系进行

①例如，在许旋、张友刚侵犯公民个人信息案的一审程序中，需要核实的个人信息高达60万条，法官凭借个人能力难以对证据信息进行核查，参见安徽省淮北市相山区人民法院〔2020〕皖063刑初42号刑事判决书。

结构性、系统性验证的新高度。例如，在金融犯罪案件中，算法可在穿透表层交易记录后，识别并呈现复杂的资金流向拓扑结构，将资金池以动态可视化的形式予以呈现。[①]在此情形下，法官可更直观地观察到各类金融交易之间的关联与脉络，大幅提高对相关事实的认定效率与准确度。

此外，数字证据通过其算法理性推动了证据关联性判断基础转变，即从主要依赖个体的经验常识，向主要依靠基于数据和模型的逻辑推演转变。传统实物证据主要扮演客观事实原始记录的角色，言词证据则反映出主体性观点，其关联性需要法官通过自身认知框架去推理和发现。算法理性体现在其对海量数据的处理能力、对隐藏模式的挖掘能力，以及依据预设或学习模型进行逻辑推演的生成能力，并自动构建出具有内在逻辑一致性的结论。以车辆信息分析报告为例，算法生成的可视化输出不仅便于法官快速理解数据背后的逻辑关联，而且可满足证据内容公开与透明的程序保障。[②]此种算法理性的融入，本质上体现了证据科学化运动在数字时代的延续，即借助于算法模型对海量数据的分析与推演，法庭审查正在从“经验归纳”逐渐向“模型演绎”转型，为司法认定提供了更为系统与客观的认知图式，并在法律真实与客观真实之外进一步提出“算法真实”的这一认知论。

三、数字证据之证据能力问题

在我国证据审查规则重心全面由证明力转向证据能力的背景下[18]，应审视数字证据在获取证据能力上存在的问题。其应当满足积极条件与消极条件，积极条件要求法官在控辩双方举证质证的前提下，依照法定证据方法，通过法定程序进行审查；消极条件要求证据自身可靠且取证行为未违反法律。

（一）积极条件不足分析

1.控辩双方证据质证能力失衡

数字证据蕴含的技术壁垒，对不具备相关专业背景的诉讼主体构成显著质证障碍。在民事诉讼领域，由于诉讼主体处于平等地位、无公权力介入，双方当事人面临的数据获取难度与技术支持条件总体上相对平衡。质证能力的差异主要仰赖于诉讼主体自身的技术或经济实力，因此控辩质证能力失衡问题在民事诉讼中并不突出。然而，在刑事诉讼中，检察机关基于其公权力地位，天然具备强制调取关键数据资源和使用专业分析工具的技术能力，控辩双方在数据掌控与专业技术支撑上存在天然鸿沟。这种结构性失衡具体体现为辩方无法有效质证，质证环节形式化的问题。有学者对于15例涉及大数据证据质证案件的裁判文书进行了研究分析，仅有一个案例经辩方质证使得法院对大数据证据持怀疑态度，其余案件中控方提出的大数据证据均被认可为相关证据，最终成为了定案依据。[19]控方的优势体现在数据资源获取优势与技术分析能力优势两个方面。

数据资源获取优势是指在控方能够通过行政或司法权力从政府部门及第三方公司高效调取数据。由于数据集通常包含敏感的个人信息，我国对此类信息的流通实施了严格监管。其中，公权力机关处理信息有据可依，但辩方缺乏调取渠道，安全例外常被用以拒绝辩方查阅数据。此外，即使辩方经申请获取相关证据，司法实践中亦存在检察机关向辩方倾倒数据，使得其在审前阅卷不能，进而加剧质证不能的问题。[19]例如，在“快播案”中，控方从被告公司的服务器中提取了上万条视频文件，辩方甚至连粗略浏览这些视频的时间都不够，更

①在王国强开设赌场案，公诉机关提交了物证抓获经过、微信账单交易明细、行政处罚决定书、交易情况及数据分析报告、情况说明，以分析资金流向，参见云南省龙陵县人民法院〔2021〕云0523刑初180号刑事判决书。

②在王路维交通肇事案中，主要通过对过车记录、卫星定位等数据认定当时经过事故发生地的车辆，以此证明行为人与犯罪行为发生地点的关联性，参见吉林省长春市朝阳区人民法院〔2021〕吉0104刑初479号刑事判决书。

不用说对这些证据进行有效的质证了。[20]

技术分析能力优势体现在控方客观上在算法技术运用中占据优势地位。面对数字证据所蕴含的海量信息和专业技术门槛，控方能够凭借公权力支撑，利用专业技术设备和算法技术，有效地从大量数据中提取有价值的信息，形成有力的证据。而辩方对算法的具体运作机制缺乏了解，也就无法评估算法逻辑是否合理、假设是否科学，更谈不上通过技术审查来质疑结果的真实性和可靠性。正如在“快播案”①中，控方不仅能够自由调取海量视频文件，还能使用专业技术设备和分析算法对其进行高效比对与甄别，而辩方在算法和技术层面均无力参与或反驳。

2.法官证据审查困难，直接审理原则难以落实

数字证据对传统证据审查规则的冲击，核心在于技术壁垒加剧了诉讼程序失衡的风险。在民事诉讼中，诉辩双方地位平等、资源配置总体对等，双方均可借助聘请专家证人的方式弥补技术短板进行质证。然而，在刑事诉讼中，控方依托政府资源的强力支持，拥有获取先进技术设备、专业人才及昂贵算法服务的优势。这种资源配置的根本差异，使得控方在庭审中能够高效、有力地提出和展示数字证据，而辩方难以对数字证据提出有效质疑。法官在缺乏强有力的反向论证情况下，通常也缺乏充分的动力去主动深入审查控方所提出的数字证据的真实性与可靠性。与之相似的是，在刑事诉讼中，辩方难以对存在技术壁垒的鉴定意见展开有效质证，法官亦对此倾向形式审查。[21]

在证据审查中，主观性证据的审查侧重于当事人的可信度，而包括电子数据在内的客观性证据则侧重于证据的鉴真，以确保其同一性和真实性。[22]数字证据因其双重属性而加剧形式化审查问题。一方面，就主观性证据的审查方式而言，传统质证方法，如观察证人的表情和肢体语言，并不适用于算法生成的证据。算法决策的黑箱性使证据生成过程脱离具体人类意志的直接控制，导致证据陈述主体虚化，证据无法直接追溯到某个可被质询的、负责任的主体。另一方面，客观性证据的鉴真主要验证证据载体的完整性和来源合法性即可。[23]然而，这种审查模式适用在数字证据中体现为仅关注最终的报告结果，而未能深入验证背后的数据集和算法的真实性和可靠性。《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》第22条所要求的“完整性校验”亦只针对数据介质是否被篡改，而忽视算法模型等其他要素。

在上述困境下，法官在庭审中所面对并据以裁判的，通常仅是一份由算法处理输出的结论性报告。在此过程中，法官既未能直接亲历基础数据的范围确定与收集过程，也未能直接观察算法的核心运行逻辑与推理步骤。这种基于报告而非其底层数据和核心算法的审查定案模式，实质上违背了严格证明所要求的直接审理原则。直接审理原则禁止法院使用“证据的替代品”，即除特殊情况外，禁止法院依靠间接证据对与犯罪事实相关的事实进行认定。[24]15-19在直接审理原则的要求下，法官应当在数字证据的举证质证中，见证数据集的范围，了解分析报告的运算过程，建立心证形成的事实基础。

（二）消极条件不足分析

1.数字证据数据集与算法真实性问题

数字证据的可靠性基础来源于其数据集以及算法分析的可靠性。然而，这一可靠性基础却存在重大挑战。

数据集的问题在于数据挖掘的过程中所产生的“脏数据”，其中“脏数据”一般是指“缺失数据、错误数据以及相同数据的非标准表示”等问题。[25]侦查机关在调查案件时，常通

①2013年11月，北京市海淀区文化委员会在执法检查中查获快播公司托管的四台服务器。2014年4月，海淀公安分局以涉嫌传播淫秽物品牟利罪对快播公司其高管立案侦查，案件于7月移送审查起诉。法院一审判决快播公司及王欣等高管构成传播淫秽物品牟利罪，分别判处有期徒刑和罚金。被告上诉后，北京市一中院于12月裁定维持原判。参见北京市海淀区人民法院〔2015〕海刑初字第512号刑事判决书；北京市第一中级人民法院〔2016〕京01刑终592号刑事裁定书。

过合法途径向互联网企业调取相关信息。然而，由于源自商业平台的原始数据质量无法得到官方统一标准的保障，因此这种从传统直接取证到借助第三方服务提供商的模式转变，在丰富侦查手段的同时，也带来了数据真实与完整性的问题。然而，即使来自官方的数据也往往因为当事人隐瞒或者警方偏见甚至数据造假等原因而缺乏可靠性。例如在美国，2006年至2010年期间，基于当事人隐瞒的原因，只有不到一半的暴力犯罪被警方统计[26]；而2005年至2012年，基于警方偏见的原因，有14000起严重袭击犯罪被记载为轻伤[27]。更甚者，为了迎合社会或上级对“降低犯罪率”的要求，部分警察部门可能会故意操纵或篡改犯罪数据。纽约相关调查显示，为了实现年度犯罪率下降的目标，一些主管及辖区指挥官会操纵犯罪统计数据。[28]在数据集不断被运用的过程中，“脏数据”不但难以进行数据清洗，更是“越洗越脏”。相较之下，在民事诉讼中，涉案数据集通常源自特定企业在其日常业务活动中自行积累的数据资产。此类数据在来源上具有相对的单一性与封闭性，内容通常更为聚焦、格式相对统一且管理流程明晰。这种内在的“相对纯净性”大大降低了因多源异构数据混杂带来的复杂关联性问题。

除数据本身的原因，算法自身也存在虚假编程与不当加工问题。虚假编程是指机器本身不具备感知能力或道德观念，但它们可以被人为编程来提供不准确的信息，或编程以某种方式引导机器本身学习撒谎。[15]不当加工是指为迎合用户需求或提高模型输出的可读性，部分生成式人工智能系统可能在运行过程中对个人数据进行不恰当的处理，包括编造从未存在的数据、错配信息等。[29]这种做法不仅违反个人信息保护的基本原则，也会在刑事诉讼中破坏对证据真实性的认定。

2.数字证据的运用与无罪推定原则冲突

与之形成鲜明对比的是，在刑事诉讼领域，数字证据的算法推演特性对无罪推定原则构成重大冲击。数字证据基于其预测功能，能够将犯罪的应对方式从被动的事后追惩转变为主动的事前预防，将个体行为数据转化为未来犯罪概率，从而违背无罪推定原则。这种违背体现的是公民所处的状态介于无罪与疑罪之间。其本应享有无罪下的自由权利，却被迫在未立案之际即承担忍受义务。

预测性司法虽然能够有效控制犯罪的发生，但亦容易使侦查人员对在特定时间出现在特定地点的个人产生先入为主的罪犯判断。例如，2013年，芝加哥警察局通过大数据指标预测特定区域部分人员成为枪支暴力受害者或者犯罪者的可能性，并加派警力在特定区域以对处在“犯罪热名单”上的人进行监管。[30]又如2019年，荷兰在全国范围内推广了“犯罪预测系统”，通过多源数据和风险模型运算，绘制出一张可以预测不同区域犯罪“热点时间”的“热点地图”。[31]犯罪预测系统通过数据画像将公民异化为风险对象，使刑事诉讼从“行为惩罚”转向“身份管控”。[32]这种“数字污名化”效应，背离了无罪推定原则的精神，也影响了人权的进一步保障。

3.数字证据对隐私权侵犯所导致的证据非法性

数字证据在数据收集和分析过程中往往表现出全面监控与尊严侵害两大特征，从而引发对个人隐私的侵犯。数据收集的全面监控体现在通过手机、智能设备等物联网技术实现数据捕获，使个人空间保护形同虚设，人际交往关系数据化。数据分析的尊严侵害体现为算法根据庞大的数据库推断出个人敏感信息，构成对人格尊严的“预测性侵犯”。相较之下，在民事诉讼场景下所涉数字证据所包含的个人数据，通常局限于特定企业依据其具体业务目的所收集的用户信息范畴，不涉及与其他来源或平台的数据集影响。因此，数字证据在民事诉讼中可能引发的隐私权影响相较刑事诉讼显著受限。

我国《刑事诉讼法》第56条针对非法证据作出了排除性规定，但仅限于供述、证人证

言、被害人陈述、物证、书证。由于法定证据种类的范畴较为狭窄，司法实践往往对数字证据或与数字证据相似的证据采取两种处理方式：其一，以缺乏相关法律依据为由拒绝排除；其二，以存储介质作为非法物证依附排除。[33]然而，时任最高人民法院刑事审判第三庭庭长戴长林法官指出："非法证据排除规则所关注的对象是基本人权，如果收集实物证据的行为故意违反法定程序，并且侵犯了宪法规定的公民隐私权……等基本人权，就可以被视为严重影响司法公正。"[34]由此可见，非法证据排除规则的目的在于规制取证行为的合法性，而不是某一证据种类的合法性。如果控方在收集、处理或使用数字证据时，已经构成对公民隐私权的严重侵犯，那么无论其以何种证据种类作为证据呈交法庭，均应适用非法证据排除规则。

四、数字证据之规制路径

对于数字证据，应分别从侦查、审查起诉和审判三个阶段予以规制。侦查阶段重在限制数据碰撞范围，避免侦查范围任意扩大；审查起诉阶段重在建立证据开示制度，使控辩双方庭审质证能力相当；审判阶段重在确立证据能力的审查规则，强化庭审对证据的审查效力。

（一）侦查阶段规制

1.保障公民个人信息权利

公民的个人数据权利包括数据信息调取的知情权、收集分析的同意权以及修改的申请权。[35]然而，数字证据基于数据收集与碰撞需求，往往会超越案件需求。为兼顾打击犯罪的现实需求与保障公民权利，有必要对不同主体的同意权进行区别对待。对于犯罪嫌疑人而言，因涉嫌犯罪，对执法机构收集和储存其个人敏感信息负有一定的忍受义务，可适度限制其个人数据的同意权；但对于不涉案的被害人或证人，原则上应充分尊重其对个人数据使用的知情权与同意权。[36]

在采集与应用具体数据时，知情权与同意权的权利范围应遵循"隐私合理性期待"原则。该原则系美国联邦最高法院于1967年办结的Katz v. United States案确立的标准，其将隐私权的空间无限扩张化，具体的范围取决于当事人对于隐私权的主观期待。①对于公民没有合理隐私期望的部分证据，侦查人员对其进行收集属于合理的范畴。例如，侦查人员通过监控对于故意将自己暴露在公众场合的人的观察以及从社交媒体中提取当事人公开发表的信息等均不构成对隐私的侵犯。但对于当事人有合理隐私期望的部分信息，侦查人员原则上仅能针对犯罪嫌疑人展开收集活动。

在收集有合理隐私期望的信息时，应尊重宪法赋予公民的个人信息自决权，以有效制衡对其个人隐私权的潜在侵犯。②借鉴德国联邦宪法法院通过"人口普查案"确立的"信息自决权"，数据收集行为若侵犯公民对个人信息的实质性控制权，即公民自行决定何时并在何种限度内披露其个人生活的事实，则构成对基本权利的侵害。③数字证据中对数据的采集、分析等处理皆属于个人信息自决权所保护的范围，赋予公民该权利能够保障数字证据收集行为仅以侦破犯罪为目的，并防止侵犯公民核心权利领域。[37]尤其是在平衡国家侦查犯罪的需

①See Katz v. United States, 389 U.S. 347 (1967). Harlan大法官在案中所指出："某人如果故意将自己的事情展示在社会公众面前，即便是在家里或者在办公室，其也不受宪法第四修正案的保护；但即便是在公共场所，如果个人像保护隐私一样处理自己的事务，则其也受宪法第四修正案的保护。"

②对于我国是否赋予公民个人信息自决权，学界从解释论角度出发，认为我国宪法第33条人权条款以及第38条人格尊严条款以公民个人信息受保护权作为公民个人信息自决权的内涵之一。参见赵宏：《信息自决权在我国的保护现状及其立法趋势前瞻》，载《中国法律评论》2017年第1期，第154页；王锡锌、彭錞：《个人信息保护法律体系的宪法基础》，载《清华法学》2021年第3期，第13页。本文持相同观点。

③See BverfGE65, 1.

求时，公民的知情权与同意权往往仅具形式上的程序制约效力，而个人信息自决权则能提供更深层、更具实质性的反向约束力，从源头上规范数字证据的收集行为，从而降低公民数据权利遭受滥权的风险。这一权利的行使，要求公权力机关遵守目的约束原则，即对公民个人信息数据的处理不得背离最初目的，从而防止权利滥用。[38]

2.规制数字证据收集的启动程序

为应对犯罪和恐怖主义的威胁，许多政府采取了大规模信息收集策略。但在没有具体犯罪嫌疑的情况下，政府监控公民的行为引发了争议，即犯罪预防功能与刑事侦查功能的混合引发公民的不满。如欧洲人权法院在Szabó and Vissy v. Hungary案中裁定，无差别数据监控因缺乏“具体嫌疑”，而违反《欧洲人权公约》第8条。①通常，在公民日常生活中，行政机关会通过大数据监管以进行一定程度的犯罪预防，而严重侵犯公民隐私的侦查行为应在刑事诉讼启动后进行。“大陆法系国家通常严格区分犯罪预防和犯罪侦查，前者被视为预防性的行政调查，后者则被视为强制性的刑事侦查。”[39]然而，在数字化时代，犯罪预防和犯罪侦查的界限变得模糊，尤其是警察使用数据库检索、电子监控等技术时，预防性行政调查与刑事侦查的职能开始重叠。[40]在美国，刑事侦查通常需要合理怀疑，执法部门才会收集信息，但数字时代使得个人信息自动收集和存储成为常态，这些行为往往在犯罪发生前就已进行，引发了合法性问题。[41]我国立案制度是国家追诉犯罪的起点，在此之前侦查机关不得采取强制性侦查措施，即不得采取侵犯公民基本权利的侦查措施。然而，在数字时代，个人信息不可避免地被自动化地收集、储存以及分析。因此，亟待进一步明确在何种情况下相关数据可以用于刑事立案。

在规制方式上，应当以行政规制和刑事规制分别的二元制亦或是二者统一规制的一元制目前仍然存在争议。在域外，英美国家采取一元制，其以是否存在特定的指控对象为根据启动刑事诉讼程序，没有专门的启动手续；大陆法系国家采取二元制，其以是否存在犯罪事实为根据启动刑事诉讼程序，其中法国以检察官向法院提起指控为启动标志，德国以提起刑事追诉的请求开始。[42]526-527笔者认为，鉴于我国存在独立的刑事诉讼法启动程序，应当采取由刑事诉讼法与行政法规分别进行规制的二元制。二元制的模式能够有效规制侦查机关在采取可能侵犯公民基本权利的措施时，需要在刑事诉讼活动启动后依照法律授权，并通过严格审批方可开展相关活动。具体而言，可以参照德国立法的假定替代干预原则。根据该原则，在行政程序或者其他刑事程序中合法收集的证据，可以作为其他案件的证据使用；即使系违法收集的证据，法官仍有权根据个案裁决其证据能力的权力。[43]即“犯罪预防性情报”与“侦查性情报”若依照合法程序收集，即可以作为立案依据，即使非法收集，亦待法官个案裁决。

在二元制规制模式下，行政机关在日常管理中获取的数字证据可以作为立案的“必要但不充分条件”。这一部分证据的取证规范受到行政法规的监管。在刑事领域，数字证据常带有“预测”性质，缺乏明确的犯罪事实，故其不能单独作为立案的充分依据，必须辅以其他客观证据来达到立案标准。正如欧盟2024年颁布的《人工智能法案》第42条所指出：“根据无罪推定原则，除非根据客观可验证的事实合理怀疑该人参与了犯罪活动，否则不得根据人工智能来评估其犯罪的可能性或推测实际或潜在刑事犯罪的发生。”因此，侦查机关在决定是否立案的过程中，无论数字证据有多么充分，基于当事人受无罪推定原则的保护，还需要借助其他证据才能形成合理怀疑。否则，侦查机关可能会利用先进技术预测犯罪，并在评估立案条件时使用信息检索和比对技术快速

①See Szabó and Vissy v. Hungary, [2016] ECHR, 37138/14.

确定犯罪嫌疑人，这实际上削弱了立案程序的重要性，也违背了无罪推定原则的要求。

（二）审查起诉阶段规制

控辩平等原则要求在诉讼程序中赋予双方同等的对抗能力，以确保辩方能够充分行使质证权。在审查起诉阶段，应当通过完善审前证据开示制度和强化控方释明义务，从而平衡控方与辩方在信息与技术方面的差距。

1.完善审前证据开示制度

在数字时代，审前证据开示制度强调的是控方面向辩方的单向且全面开示，其具体内容包括阅卷权、数据访问权以及适度的算法开示。[44]首先，应当延长阅卷时间，扩大阅卷范围，允许律师接触案件中所有可能涉及数字证据的关键材料。其次，就数据访问权而言，为了核实数字证据的真实性，应当允许辩方以数据接口的方式获取数据，并对数据进行独立审查。最后，建立适度的算法开示制度，解释常用算法的整体思路、核心逻辑、关键参数及其与案件事实相关性等。

2.完善释明义务

控方释明义务的实质化，是平衡控辩证据优势的关键机制。具体而言，控方应当简要释明数字证据的获取方式以及数据集基础来源。此外，控方应当重点释明其所采用的算法技术与算法逻辑。

（三）审判阶段规制

相较于美国、德国、俄罗斯等国未将电子数据单列为法定证据种类、主要参照书证规则处理的做法[45]，我国虽明确将电子数据列为独立证据种类，但在可采性审查传统上仍囿于传统的关联性、合法性、真实性框架，且忽视程序权利保障。[46]针对数字证据的特殊性，严格证明的证据规则应当围绕以下四个方面展开。

1.扩大非法证据排除规则适用范围

传统意义上认为非法证据排除规则是一种制裁手段。制裁是针对违背社会规范的行为采取的措施，旨在通过施加负面后果来阻止行为人继续此类行为，其本质是对行为人施加损失或不利，以促使其遵守规范。[47]5-6然而，制裁的基本前提在于有法可依。例如，就收集手机数据而言，美国联邦最高法院于2014年Riley v. California案和United States v. Wurie案中，正式确立了无证搜查不适用于收集手机数据的规定，对手机搜查属于强制性措施。①目前我国非法证据排除规则并未在明文上将数字证据纳入其中，从而导致实践中存在争议，进而无法制约侦查机关非法取证行为。司法实践中仍然存在着侦查人员径直没收并要求犯罪嫌疑人解锁手机，从而直接将手机内容拷贝并获取其中相关信息的情形。我国刑事诉讼法第52条规定“不得强迫任何人证实自己有罪”。这一条款的保障内涵目前德国通说以及欧洲人权法院均采主动基准，即犯罪嫌疑人没有义务为认定自身犯罪而主动提供协助，协助内容包括作出供述或提供其他证据。[48]112-113侦查人员强制要求犯罪嫌疑人交出手机并配合解锁，无异于让犯罪嫌疑人主动配合侦查机关认定其犯罪事实。

在此条款未发挥作用且缺乏专门的规制法律的前提下，将非法证据排除规则视作一种救济手段，则有助于法官针对侦查机关的非法取证行为进行有效规制，同时能够保障被追诉人的权益。权利救济不足使得我国刑事诉讼程序呈现典型的权力裁量特征。[49]而救济理论相较于制裁理论，其强调的是侵害权利后的矫正或补偿，其目的在于使受侵害的权利恢复至应有状态。[50]即通过程序性救济，能够加强法官的中立性，确保审判程序能够关注对象从侦查机关的取证行为转变成被追诉人在审前是否受到权利侵害，进而能够有效作出判断。此外，这一救济模式能够有效扩张辩护权的行使条件，契合辩护权发展脉络的方向。[51]

将救济理论作为非法证据排除规则的理论的显著作用在于填补法律空缺。目前，我国规定侦查机关在搜查犯罪嫌疑人住宅时应当

①See Riley v. California, 573 U.S. 373 (2014); See also United States v. Wurie, 728 F.3d 1 (1st Cir.2013).

持有搜查令，这意味着我国通过法律规制的方式保护着公民的隐私，然而隐私权的保护对象没有随着数字化时代的到来通过法律的形式予以扩张。相比之下，美国确立的“隐私合理性期待”标准值得我国在针对数字证据的非法证据排除规则的完善上加以借鉴。在该标准中，隐私权的空间不再局限于公民的私人空间，如其住宅，而是将该空间扩展至任何一个公民希望予以保护的地方。例如，公民认为手机、电脑等电子设备属于其隐私范围，亦或者公民认为其低声与他人说话、交流时所传播出来的声音属于其隐私范围，针对这些隐私，其不得被他人任意侵犯。在救济理论的视角下，隐私权的保护范围应当取决于被告人的主观期待，从而能够对于在非紧急情况下任意侵犯被告人个人敏感数据的行为予以排除。

2.完善数字性最佳证据规则

最佳证据规则以“原始性”为核心，旨在确保证据载体与信息内容的真实性。在传统司法实践中，对于书证、物证通常要求出示原件，对于证人证言则要求证人出庭，对于鉴定意见则要求鉴定人出庭作证。数字证据展现的不是原始物，而是基于算法对原始数据集进行处理后生成的“报告型”证据。与传统鉴定意见由鉴定人出庭相比，数字证据背后往往是算法运算的结果，缺少单一且明确的“生成主体”。一旦在诉讼过程中对结果产生质疑，难以通过传统的交叉询问来有效检验结论的可靠性。

最佳证据规则适用于数字证据时，需将审查重点放在对初始数据集的真实性以及收集程序的合规性上。在数据集的信息审查上，为了验证数据的真实性，法官在面对“脏数据”时，可要求控方提交未经任何处理的原始数据，并借助第三方专业机构对该数据进行独立清洗或验证，以判断其完整性与真实性。如果数据来源于第三方平台或商业机构，法官还需重点考察该数据的收集及处理方式是否符合相关法律法规要求。特别是在商业环境中，常见“僵尸粉”“水军”“刷单”等虚假数据，会导致对真实市场交易情况或经济往来情况的误判。

在数据集的收集程序审查上，首先应当审查原始存储介质扣押与保全。数字证据在获取过程中，需审查取证部门是否对原始存储介质进行了依法扣押或封存，以保障后续数字证据的可信度。然而，电子数据的精确复制件难以与原件区分，且经由多次传输或基于云计算生成的电子数据通常不存在传统意义上的单一物理“原件”因此，僵化套用传统最佳证据规则要求必须提交原始存储介质已不切实际。为因应数字技术特性并维护证据可靠性核心，电子数据的“原件”规则应进行适应性调整，将经过严格验证、具有完整性与客观性的副本纳入法律认可的“原件”范畴。其次，为保证原始数据在取证到庭审之间不被篡改或替换，应当利用区块链所具有的不可篡改、分布式存储、全程可追溯的技术特性，构建高度可信的存证链。通过将数据的哈希值与时间戳等信息，固化于区块链之上，形成难以变更的存证记录。最后，从程序到具体证据的全流程审查。通过对取证环境、取证人员资质、取证软硬件、操作规程、数据固化方式等方面的综合审查，判断数字证据是否符合最佳证据规则。若发现程序环节存在严重缺陷，应考虑对该证据予以排除或降低其证明力。构建有效的证据保管链，核心在于建立完整可验证的记录机制。既要制作详尽的取证笔录形成基础追溯文本，也要通过拍照、录像及见证人等方式确保记录客观；更需在关键节点即时生成并固定数据特有的校验码，以此形成环环相扣的验证闭环。

3.完善技术性直接言词规则

司法实践中法官往往对科学证据抱有一种不加分析的信任，甚至一些法官可能会在没有进行充分审查的情况下，将数字证据作为定案的依据。例如，在杨某盗窃案中，辩方以人脸对比数据结果未达到100%为由认为该大数据证据证明能力不足，在控方未提出其他证据的基础上，法官则直接以视频中人脸清晰、对比度高达96%为理由确认其为被告人。[①]这种

过度依赖数字证据的倾向，反映出当下对新型科技证据审查不足的问题。

为确保法官能够对数字证据进行实质性审查，在数字技术背景下“主体虚化”的前提下，应当完善技术性直接言词规则，构建由“有专门知识的人”组成的陈述主体。“有专门知识的人”包括两类专家，分别是技术专家与研发专家。技术专家主要负责审查算法的可靠性，如评估算法的理论基础、技术成熟度、数据输入输出的准确性等。一旦发现算法存在重大缺陷或潜在风险，可及时指出并帮助法官排除相应的错误结论。例如，美国在审查丰田凯美瑞意外加速问题诉讼中的源代码时，一名技术专家审查了酒精呼吸机“Alcotest 7110”的源代码，他发现该代码无法通过软件开发和测试的行业标准，其包含了19500个错误，其中9个最终会影响呼气酒精读数。[15]研发专家能够解释算法原理并构建透明流程，帮助法官与控辩双方理解程序设计思路以及算法在具体情境下的适用性。这类专家可被视为机器的“顾问”，其证词有助于提升算法测算结果的说服力。类似于早期摄影技术尚未成熟时，只有在摄影师对照片成像过程作证并证明照片的准确性后，法院才会采信该照片作为证据。[52]

然而，在司法实践中，控方申请出庭的有专门知识的人常常扮演“纯粹的侦探”角色，机械性地重复机器传送的内容，造成证据已进行证伪的假象。[15]因此，由辩方申请出席法庭的有专门知识的人，往往能够从一个更加公正客观的视角去审查数字证据的真实性，并通过与其他专家之间的辩论以确保得到的结果客观真实，使得裁判者能够在对比两方专家意见的基础上作出判断。在德国，为保障辩方在技术证据方面的质证能力，制度设计上不仅允许辩护人在审前调查结束后查阅全部案卷，而且可以请求法院传唤与法官、检方意见不同的专家出庭作证。[53]我国可在此基础上进行借鉴，通过为辩方提供申请技术专家或研发专家出庭的保障程序，使其具备与控方对等的技术审查能力，从而真正实现庭审实质化与程序公正。具体而言，可以由诉讼双方围绕案件事实与证据提出各自的解释方案；法官则依据理性标准对这些方案进行比较、评估，最终采纳其中对现有证据最具说服力最合理的解释作为裁决基础。

然而，专家证人存在超越其证明范围发表意见的内在风险。当前的明确共识是专家只能就专业性问题发表意见，不能对超出其专业性部分作出推论，更不能取代裁判者的地位作出证据是否可以采纳的决定。当法庭争议聚焦于“某一事实是否实际发生”时，专家的作用在于阐述和论证其所依据的专门性证据与该待证事实之间关联性知识的科学性与可靠程度。[54]54-56专家不了解案件的整体背景，也缺乏必要的法律知识储备，不得直接断言该待证事实为“真”，事实真伪的认定权依法专属于裁判者。据此，专家证人的核心地位与作用在于辅助事实裁判者，帮助其理解专业性证据本身的技术含义与科学基础，以及帮助理解数字证据与待证事实关系的认识与判断。[55]

4.完善技术性意见证据规则

意见证据规则要求证人必须就所见、所闻的客观事实进行陈述，不得在证言中随意夹杂个人主观推断或评价。然而，在数字证据中，人类专家意见往往被预先压缩至算法设计阶段。这使证据融合了专家预设判断与机器计算结果，因此对其生成内容的可靠性审查尤为重要。

为提高对数字证据的审查质量，我国法院可与第三方专业机构合作，建立独立的评估机制。该机制应基于控方所提供的大数据集，由第三方机构运用自身成熟的算法模型对证据的内容与生成进行审查与评估。评估机制应当包含评估流程、评估标准、保密义务三个方面。在评估流程上，应当根据争议点的重要程度以及法官的内心确信度，对具备争议的证据必须进行独立评估。对于无争议且法官认为能

①参见台州市椒江区人民法院〔2020〕浙1002刑初467号刑事判决书。

够确认其可靠性的证据，可以在其他证据的佐证下予以采信。在保密义务上，法院需对第三方评估机构的审查过程进行监督，对评估所涉数据、算法细节以及商业机密严格保密。

在评估标准上，美国联邦最高法院于1993年确立的多伯特标准曾为传统电子数据审查提供了重要框架。①然而，当审查对象转向依赖算法的数字证据时，多伯特标准便无法满足审查需求。其基于实验验证的方法论无力揭示算法运行机制本身存在的“黑箱”隐患。[15]强制公开源代码被视为解构黑箱的重要途径，[56]但鉴于商业秘密的保护需求，此方案现实可行性极低。有鉴于此，证据审查方式应当转向标准化流程规范与生命周期管理相结合的综合路径。标准化流程是指裁判者可以通过数字证据的标准化生成过程去判断证据的可靠性。[57]裁判者既可通过审阅证据生成过程是否遵循既定的行业技术标准以确认其可信度；亦可根据专家依据标准化框架对证据的技术原理与关联性进行阐释的规范程度作出判断。这使得证据的核心价值取决于流程本身的合规性，而非个体专家的主观判断能力，法庭只需评估解释流程是否符合预设的标准化要求即可。[58]同时，对机器证据可采性的全面评估必须纳入全生命周期管理的视角。电子数据本质上是过程性与结果性的统一体，其可靠性高度依赖整个生成、收集、固定、存储、传输、分析直至呈现于法庭的全链条能否被有效追溯和验证。[59]51-52这种“生命周期管理”聚焦于证据从源头到终点的全流程监管轨迹，包括关键环节是否依法定或技术规范执行。

五、结语

纵观人类科技与法律的交织历程，每一次重大的技术革新都会引发对既有司法制度的深层次冲击，也会为司法公正与效率的提升带来新的契机。数字证据的出现，正是数字时代对司法实践的一项深远考验。其以算法与数据为基础，深度介入从侦查、审查起诉到审判的全过程，为事实认定提供了更精细、更立体的信息支撑。面对这种新型证据的涌现，我们应当采取开放的姿态，并认识到其在揭示案件真相中的价值。然而，开放不等于盲目相信、崇拜。只有当其被纳入合法、透明、有序的司法轨道时，才能真正造福于公众、维护社会正义。具体而言，在审前阶段，应当加强当事人对数据调取、运用的知情权，并强化相关侦查行为的规范要求，检察机关应当履行告知数据来源以及释明算法运用等义务确保法庭调查环节的平等。法官在审查数字证据时，必须遵守证据方法，依照严格证明的要求对其进行审查。展望未来，我国应及时跟进科技发展态势，秉持对技术理性与程序正义的平衡，为数字证据的收集、提取、开示与质证提供全面而明确的操作指引，在波澜壮阔的数字时代始终坚守住公正与信赖的底线。

参考文献：

[1]裴苍龄. 论证据的种类[J]. 法学研究，2003(5)：45-50.

[2]张嘉军，李保茹. 论我国证据种类之重构[J]. 黑龙江省政法管理干部学院学报，2005(2)：86-90.

[3]何家弘，邓昌智，张桂勇，等. 大数据侦查给证据法带来的挑战[J]. 人民检察，2018(1)：54-57.

[4]刘品新. 论区块链证据[J]. 法学研究，2021，43(6)：130-148.

[5]冯俊伟. 机器生成的电子数据之可采性[J]. 中国刑事法杂志，2024(3)：60-76.

[6]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.

[7]张中. 刑事证据制度现代化的中国标准与制度安排[J]. 国家检察官学院学报，2024，32(5)：3-21.

①多伯特标准从四个层面界定评估的标准，分别是：(1)检验鉴定所依据的科学理论和技术方法必须能够得到检验；(2)该项科学理论和技术方法经必须公开发表并得到同行认可；(3)有基础研究证明其错误率；(4)鉴定专家必须有资格进行该项鉴定，鉴定的结果是否可由其他专家用同样方法获得。(5)专家必须能够以通俗、简洁的语言向法庭解释该科学原理和鉴定的结果，使法庭和陪审员能够正确理解。See Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 U.S. 579 (1993).

[8]胡铭. 论数字时代刑事证据的三元结构[J]. 中外法学, 2025, 37(1): 45-64.
[9]Younger I. Computer printouts in evidence: ten objections and how to overcome them[J]. Litigation, 1975, 2(1): 97-132.
[10]Kurzban S A. Authentication of computer-generated evidence in the united states federal courts[J]. The Journal of Law and Technology, 1995, 35(4): 437-466.
[11]刘品新, 陈丽. 电子证据的迭代与立规[N]. 人民法院报, 2020-10-22(5).
[12]马国洋. 论刑事诉讼中人工智能证据的审查[J]. 中国刑事法杂志, 2021(5): 158-176.
[13]张吉喜, 孔德伦. 论刑事诉讼中的大数据证据[J]. 贵州大学学报(社会科学版), 2020, 38(4): 82-88.
[14]杨继文. 算法证据: 作为证据的算法及其适用规则前瞻[J]. 地方立法研究, 2022, 7(3): 37-51.
[15]Roth A. Machine testimony[J]. Yale Law Journal, 2016, 126(7): 1972-2053.
[16]刘品新. 论大数据证据[J]. 环球法律评论, 2019, 41(1): 21-34.
[17]吴宏耀, 魏晓娜. 诉讼证明原理[M]. 北京: 法律出版社, 2002.
[18]易延友. 以可采性为中心的刑事证据规则之建构[J]. 国家检察官学院学报, 2025, 33(1): 131-149.
[19]程龙. 论大数据证据质证的形式化及其实质化路径[J]. 政治与法律, 2022(5): 96-114.
[20]刘品新. 电子数据的鉴真问题: 基于快播案的反思[J]. 中外法学, 2017, 29(1): 89-103.
[21]顾永忠. 以审判为中心背景下的刑事辩护突出问题研究[J]. 中国法学, 2016(2): 65-85.
[22]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.
[23]陈瑞华. 实物证据的鉴真问题[J]. 法学研究, 2011, 33(5): 127-142.
[24]林钰雄. 严格证明与刑事证据[M]. 北京: 法律出版社, 2008.
[25]Kim W, Choi B J, Hong E K, et al. A taxonomy of dirty data[J]. Data Mining and Knowledge Discovery, 2003, 7(1): 81-99.
[26]Lynn L, Marcus B, Christopher K, et al. Victimizations not reported to the police, 2006-2010 [R/OL]. (2012-08-09)[2024-09].https: //bjs.ojp.gov/content/pub/pdf/vnrp0610. pdf.
[27]Josh S. Los angeles police underreported crime stats for 8 years[EB/OL]. (2015-10-15)[2024-09-28]. https: //time. com/4074896/los-angeles-crime-rates-higher-assaults/.
[28]Rashbaum, William K. Retired officers raise questions on crime data[EB/OL]. (2010-02-06)[2024-09-28]. https: //www. nytimes. com/2010/02/07/nyregion/07crime. html.
[29]刘艳红. 生成式人工智能的三大安全风险及法律规制——以ChatGPT为例[J]. 东方法学, 2023(4): 29-43.
[30]Ferguson A G. Big data and predictive reasonable suspicion[J]. University of Pennsylvania Law Review, 2014, 163(2): 327-410.
[31]Strikwerda L. Predictive policing: the risks associated with risk assessment[J]. The Police Journal, 2021, 94(3): 422-436.
[32]詹羽洪. 论轻罪案件附条件不起诉制度的数字化改革路径[J]. 中国刑警学院学报, 2025(1): 117-128.
[33]谢登科. 非法电子数据排除的理论基点与制度建构: 以数字权利的程序性救济为视角[J]. 上海政法学院学报(法治论丛), 2023, 38(3): 62-80.
[34]戴长林. 非法证据排除规则司法适用疑难问题研究[J]. 人民司法, 2013(9): 22-31.
[35]程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122.
[36]陈永生. 大数据预测警务的运作机理、风险与法律规制[J]. 中国法学, 2024(5): 165-184.
[37]施鹏鹏. 论大数据侦查: 以信息自决权为主线[J]. 法治研究, 2024(6): 15-25.
[38]赵宏. 告知同意在政府履职行为中的适用与限制[J]. 环球法律评论, 2022, 44(2): 36-51.
[39]卢莹. 刑事侦查中人脸识别技术的应用与规制[J]. 法治研究, 2022(6): 144-160.
[40]程雷. 大数据侦查的法律控制[J]. 中国社会科学, 2018(11): 156-180.
[41]Brayne S. Big data surveillance: The case of policing[J]. American Sociological Review, 2017, 82(5): 977-1008.
[42]王敏远. 刑事诉讼法学[M]. 2版. 北京: 知识产权出版社, 2023.
[43]李倩. 同一数据在诉讼程序转化后的使用限制及证成[J]. 环球法律评论, 2024, 46(4): 176-191.
[44]郑曦. 数字时代刑事证据开示制度之重塑[J]. 华东政法大学学报, 2023, 26(4): 38-48.
[45]Custers B, Stevens L. The use of data as evidence in dutch criminal courts[J]. European Journal of Crime, Criminal Law and Criminal Justice, 2021, 29(1): 25-46.
[46]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.
[47][日]佐伯仁志. 制裁论[M]. 丁胜明, 译. 北京: 北京大学出版社, 2018.
[48]王士帆. 不自证己罪原则[M]. 台北: 冠顺印刷事业有限公司, 2007.
[49]詹羽洪. 重新追诉案件的并案处理程序问题研究[J]. 北方法学, 2026, 20(1): 149-160.
[50]赵常成. 非法证据排除的规范原理新论——以“制裁—救济”为分析框架[J]. 中外法学, 2023, 35(1): 241-259.
[51]詹羽洪. 审查起诉阶段律师讯问在场制度研究[J]. 现代法学, 2025, 47(6): 116-131.
[52]Mnookin J L. The image of truth: Photographic evidence and the power of analogy[J]. Yale Journal of Law & the Humanities, 1998, 10(1): 1-74.
[53]Gless S. AI in the courtroom: A comparative analysis of machine evidence in criminal trials[J]. Georgetown Journal of International Law, 2020, 51(2): 195-254.
[54]Roberson B, Vignaux G A, Berger C E H. Interpreting evidence: Evaluating forensic science in the courtroom[M]. Chichester: Wiley, 2016.
[55]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.
[56]Coble M D, Buckleton J, Butler J M, et al. DNA commission of the international society for forensic genetics: Recommendations on the validation of software programs performing biostatistical calculations for forensic genetics applications[J]. Forensic Science Intenational: Genetics, 2016, 25(0): 191-197.
[57]Imwinkelried E J. Computer source code: A source of the growing controversy over the reliability of automated forensic techniques[J]. Depaul Law Review, 2016, 66(1): 97-132.
[58]郑国良, G·亚历山大·纳恩, 卫晨曙. 证人之外: 将程式化视角引入现代证据法[J]. 证据科学, 2022, 30(3): 322-355.
[59]Caianiello M, Camon A. Digital forensic evidence: Towards common european standards in antifraud administrative and criminal investigations[M]. Utah: CEDAM, 2021.

【责任编辑 邱佛梅】

On the Criminal Procedural Regulation of Digital Evidence

ZHAN Yuhong

Abstract: The digital age is changing criminal evidence systems. Digital evidence is now widely used. Some types can be reviewed using traditional methods for electronic data. But new rules are needed for big data evidence, algorithm evidence, and AI evidence. This new evidence relies on algorithms. It has both objective facts and subjective analysis. It moves court decisions from relying on experience to using algorithms. However, in the absence of effective regulation, digital evidence encounters a dual predicament regarding its admissibility: on one hand, the imbalance in evidentiary capabilities between prosecution and defense leads to a formalistic cross-examination process, rendering strict proof difficult to achieve and causing judges to struggle with the intangible source of such evidence. On the other hand, issues such as “dirty data,” algorithmic bias, privacy infringements, and conflicts with the presumption of innocence principle cast doubts on its admissibility and legitimacy. From the perspective of procedural regulation, it is recommended that: during the investigation phase, suspects should be granted the right to know about the data involved, and the initiation procedure for collecting digital evidence should be standardized; during the prosecution review phase, the pretrial evidence disclosure system and the duty of explanation should be strengthened; and during the trial phase, the scope of the exclusionary rule for illegal evidence should be expanded, while rules on digital best evidence, technical direct oral testimony, and technical opinion testimony should be further refined.

Keywords: digital evidence; evidence disclosure system; presumption of innocence; privacy; exclusionary rule of illegal evidence