

刑事司法中大数据证据的适用风险与规制路径

唐 正

福建农林大学公共管理与法学院硕士研究生, 中国·福建 福州 350007

【摘 要】在刑事侦查、起诉与审判中, 通信、支付、轨迹等数据经算法处理日益被作为证据使用。现行规则多以电子数据一般规定兜底, 缺乏针对算法生成、海量关联的取证、保存与审查标准, 由此引发结果难以复核、算法黑箱、隐私过度收集及隐性偏见等风险, 甚至可能弱化质证与救济。应以可解释、可复核为准入门槛, 明确数据来源、处理流程与举证责任, 并允许专家参与复核, 同步建立数据合规与最小必要收集规则, 引入算法审计和程序性审查, 确保效率提升不以权利让步为代价。未来可通过刑诉法及司法解释细化统一标准, 并形成跨部门监督与责任追究机制, 促成数字时代证据制度的稳妥更新。

【关键词】刑事司法; 大数据证据; 隐私保护; 算法监管

1 绪论

1.1 研究背景及意义

科技进步、信息化生活为我们积累了海量的数据信息, 公安通过通信大数据、视频大数据、社会大数据、经济大数据等信息精准甄别违法犯罪线索、还原违法犯罪事实, 如“断卡行为”识别涉案可疑账户、抓取盗窃在逃人员等; 检察、司法通过算法识别分析海量的证据之间的关联并输出识别结果, 以可视化的方式呈现证据、事实之间的关联性, 提高审查效率、促进事实认定。这些应用为提高办案效率, 帮助办案人员甄别案件事实提供了便利, 但同时也存在很多问题, 如浙江“大数据错判公民吸毒案”、广东“算法风险高打追诉案”等案例反映出大数据证据的可采性、人权保障不足等问题。

1.2 文献综述

对于刑事司法领域大数据证据的研究, 目前国内有学者从不同的角度出发对其进行研究, 比如: 刘沛宏、万星辰(2025)认为对于刑事司法中的大数据证据的证明能力规则应当进行系统研究, 避免出现“技术审查”替代司法审查的现象^[1]。王燃(2025)从大数据证据的多重关联关系的角度, 认为关联关系会影响因果关系的判定, 应当完善关联度和证明力审查制度^[2]。肖沛权、周家驹(2025)认为在刑事诉讼法修改中对大数据证据在取证、保存和审查的证明责任进行明确的规定, 应当完善刑事诉讼法关于大数据证据证明的法律制度和司法解释, 完善刑事诉讼大数据证

据审查程序^[3]。谢登科(2025)认为要从人工智能证据的种类研究证据规则, 建立可理解性规则、审计规则、准入规则等, 确保证据的真实性、保障正当程序^[4]。总之, 国内对于刑事司法领域大数据证据的研究从理论、证据规则、立法规定、技术规制等进行了梳理, 但对于证据标准的制定、明确司法实践操作方式、建立各部委之间的监督机制等还需要进一步研究、实证分析。

2 大数据证据的性质与适用现状

2.1 大数据证据的概念

于刑事诉讼中, 大数据证据为, 对通信记录、支付流水、定位轨迹、社交动态、监控影像等海量结构化与非结构化数据开展提取、过滤、整合和算法分析后产生的, 用来证明案件事实、认定嫌疑人涉案相关联系的证据形式, 从法律属性的维度看, 其本质为电子数据的特殊样式, 完全合乎我国《刑事诉讼法》第50条规定的电子数据法定证据种类范畴, 跟以往传统的电子数据相比, 核心区别是其依赖算法对海量多元数据进行深度加工以及关联分析, 而不是直接把单一数据呈现。

2.2 大数据证据在刑事司法中的应用场景

2.2.1 侦查环节: 借助技术赋能线索挖掘与证据固定

大数据证据应用最集中的环节是侦查阶段, 核心是围绕犯罪线索发现、涉案关联确认以及证据初步固定展开, 就像胡铭讲的, 通信方面的痕迹、社交相关的动态、时空所处的位置、交易的流水明细等众多数字痕迹, 已成为侦查线索的

核心根源, 侦查工作更多借助数据关联分析和时序还原对犯罪事实进行追溯^[5]。公安机关凭借多维度数据整合创建侦查模型: 借助通信大数据追踪嫌疑人在通话时基站的切换轨迹, 重现作案路线跟同伙的联络关系; 利用支付数据去排查涉案资金的走向, 正如“断卡行动”期间, 去分析银行流水和第三方支付账单, 精准挑出涉诈账户及资金转移链条; 运用人脸识别技术对监控视频做大量对比, 迅速锁定盗窃、诈骗等相关案件嫌疑人; 以社交平台数据挖掘涉案人员的关系网络, 结合行为分析及关系图谱技术确认犯情的关联, 达成对可疑个体的精确排查和线索连贯^[6]。

2.2.2 起诉环节: 提升证据审查及程序推进的效率

检察机关在起诉阶段的大数据运用, 主要围绕证据关联性的审核、量刑建议的辅助与办案流程的规范开展。借助“智慧检务”系统对侦查移送的大量证据开展算法筛选与关联性确认, 自动辨认可疑证据、书证与电子数据的矛盾所在, 改善证据审查的全面性与精确水平; 就盗窃、故意伤害等普遍存在的刑事案件, 依靠历史判例数据及量刑规范, 生成量刑建议的参考区间范围, 为精准提出量刑建议提供数据后盾; 依靠自然语言处理技术自动生成审查报告、起诉书等检察相关文书, 提取案件核心要点并规范文书规格, 减轻办案人员事务性工作的压力值。

2.2.3 审判环节: 事实呈现及裁判辅助的多方支持

审判阶段的大数据应用把重点放在案件事实可视化呈现与裁判决策科学化辅助上, 为法官精准认定事实、顺利作出裁判提供技术后盾, 余鹏文觉得, 大数据在审判中的应用不只是围绕证据审查展开, 更延伸至庭审可视化、量刑参考等多种情形, 需要重新厘定其证据性质和法律地位^[7]。在庭审开展期间, 借助数据可视化技术把复杂涉案关系转变为时空图谱、资金流向图等直观图表, 明白呈现被告人在场时间、行为轨迹跟案件事实的关联, 使法官在事实认定上的难度降低; 在量刑这个阶段, 法院凭借“智慧法院”系统整合起同类案件裁判数据以及量刑指导意见, 把本案犯罪情节、被告人悔罪表现等数据进行结合, 给出量刑参考方案, 为裁判给出量化支撑; 部分法院探索采用算法对案件证据链的完整性进行检验, 辅助法官找出证据里的漏洞, 但正如谢佑平所害怕面对的, 技术赋能背后悄悄

藏着程序正义的挑战, 数据获取的全面性状况、部门间数据共享的规范性水平, 以及被告人落实对大数据证据质证等相关问题, 都给审判程序的公正性带来了新要求^[8]。

2.3 现行适用中的法律框架与实践问题

当前我国大数据证据的司法适用尚未形成专门化、体系化的规则体系, 仍主要依托证据法基本原则兜底调整, 导致规则适用困难与实践障碍并存, 其核心症结在于法律框架的层级缺失与规范缺口, 且直接映射为司法实践中的具体问题。

《刑事诉讼法》把电子数据归为法定证据种类, 为大数据证据的法律定位提供了基础支撑, 但没有针对其算法生成、海量关联等特殊情况作出专门规定, 在证明标准、举证责任分配等核心问题上缺少明确的引导; 《个人信息保护法》虽说明了司法机关为办案收集个人信息的合法边界所在, 但跟刑事诉讼里的证据收集程序衔接程度不足, 未对“必要范围”的具体判断标准作出界定; 《数据安全法》针对数据分类分级保护所做规定, 无法直接转成刑事司法里数据采集、存储、分享的操作规范, 造成安全要求跟司法效率需求难以统一。

3 大数据证据适用的风险分析

3.1 证据可靠性与可解释性风险

将大数据证据引入刑事司法, 其可靠性以及可解释性问题更为突出。数字证据种类繁多复杂, 处理流程过于复杂繁琐, 传统的审查方式无法处理, 要构建阶梯式审查分类机制, 区分不同种类证据的不同证明能力, 并增强处理可解释性。应在证据提交前对大数据进行证据化处理, 做好数据预处理、特征提取、模型检验等, 避免由于技术不正确导致对案件结果的错误解释。算法在司法领域的适用应当兼顾高效与可解释, 通过算法解释、可审查的记录、司法审查接口等, 让法官、当事人了解清楚算法形成的推论, 确保事实认定主体合法性。如果不以立法或司法解释的形式确立算法可证伪、算法可解释的原则或标准, 那么技术判断将替代法官的裁判判断, 进而使得正当程序和被告人权利被架空, 因而应当以法律的形式确立算法的可解释原则和举证负担原则。在技术方面提高可审查性、可跟踪性同时还要从制度上保障司法主体对技术输出的审查、

质证性，化解大数据证据的根本风险。

3. 2隐私保护与数据滥用风险

在刑事司法适用大数据证据时，隐私保护、数据滥用等成为制度风险。侦办过程中对通信记录、位置信息、消费轨迹等信息的搜集适用，超出了案件侦办的必要性需求，模糊了比例原则、目的限制，将案件以外的第三者大量私人生活纳入其中。部门、省份之间数据的交换共用缺乏监管，使收集的用于公共安全目的的数据被用于其他未知的或不当的目的，使数据采集、存储、分析过程去标识化，重识别没有实质性突破，当事人隐私依然处于裸露状态，数据主体的知情权、异议权在刑事司法程序难以行使，受侦查秘密、举证规则限制，个人无从得知数据被怎样使用的答案，无从寻求救济途径。

4 大数据证据适用的规制路径

4. 1证据价值判断与可解释性标准构建

构建证据价值判断与可解释性标准，首先需要理论和实务对大数据证据自身的特点及评价维度进行梳理。算法生成的证据与传统证据不同，具有技术性强的“黑箱”特征明显，对于证据价值的认定，需要关注算法原理、数据来源和数据处理流程是否可以回溯，而非结果输出。需将质证程序与技术审查程序相结合，实现证据质证形式化与实质化，从程序上保障信息披露、专家参与、复核机制，在实质上设置可解释性门槛，防止出现用技术判断代替了司法判断的现象。

4. 2强化数据保护与个人权利救济机制

刑事司法中大数据证据必须以健全的数据保护和个人权利救济制度作为前提，追求办案效率不能以牺牲权利为代价，明确数据收集的合法界限，遵循目的性、必要性原则，禁止超范围收集、留存不涉及案件事实的信息以及超期存储；提高敏感数据保护标准，要求公安机关收集数据前须审查合法性、必要性。明确告知和异议机制，保障当事人知道真相、有提出、更正、删除的权利。确保个人对数据来源、用途、后果作出合意。规范数据访问、数据开放权限，建立授权许可、审计留痕制度，各部门或委托机构进行数据加工须严格履行审批手续并进行登记。同时，建立救济途径，包括复议、刑事司法救济、第三方组织投

诉等，救济途径应具有便捷性、可得性。为执法部门和第三方服务提供商明确法定责任和赔偿义务，落实责任制，防止滥用，构建制度保护权利机制。

5 结论与展望

通过对刑事司法大数据证据属性、适用情况及风险分析，本文认为，大数据证据海量、关联、算法生成等特点为侦查办案、庭审发现新证据事实提供路径，降低传统证据裁判科技水平和程序运用难度；但其证明价值性、可审查性、来源合法性困境对证据裁判科技含量要求和诉讼风险高，超出法官及当事人认知能力，阻碍司法正义；其隐私保护、数据滥用与算法植入对当事人权利和社会正义的威胁无法靠传统证据化解。需从立法、司法解释明确其定位与审查规则，从算法说明、第三方技术审查、数据保护强化机制与程序设计，从庭审介入、救济路径引入技术与救济机制。总之，只有复合型多主体多层次治理才能在刑事司法效益中坚守程序公正和基本人权底线。

参考文献：

- [1] 刘沛宏, 万星辰. 论刑事审判中大数据证据的证据能力规则设置[J]. 湖南社会科学, 2025, (05): 102-112.
- [2] 王燃. 论大数据证据的多元关联性[J]. 法制与社会发展, 2025, 31 (05): 191-206.
- [3] 肖沛权, 周家驹. 《刑事诉讼法》再修改背景下刑事证据制度之完善[J]. 东北师大学报(哲学社会科学版), 2025, (04): 167-175.
- [4] 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, (03): 62-72+175+2.
- [5] 胡铭. 论数字时代刑事证据的三元结构[J]. 中外法学, 2025, 37 (01): 45-64.
- [6] 潘金贵. 数字时代刑事证据运用的风险及其规制——以算法证据为分析视角[J]. 法治研究, 2024, (06): 26-42.
- [7] 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, (05): 36-54.
- [8] 谢佑平. 人工智能时代我国刑事司法改革的双重使命[J]. 政法论丛, 2024, (05): 84-98.

作者简介：

唐正 (2000.12.14-), 汉族, 男, 福建省漳州市。