Dispute Settlement 争议解决, 2025, 11(12), 70-78
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.1112371

Hans汉斯

数字时代刑事证据合法性问题的案例比较研究

金海霞

山东建筑大学法学院，山东 济南

收稿日期：2025年11月12日；录用日期：2025年12月8日；发布日期：2025年12月17日

摘　要

数字技术的深度渗透使电子数据成为刑事诉讼中的“证据之王”，其合法性认定已成为决定案件裁判最终结果的重要因素。与普通证据种类相比，电子数据具有易篡改、依赖性强、形态多元等特征，导致其收集、固定、审查全流程的合法性判断深陷技术与法律的双重困境。本文以刑事证据合法性的核心构成要素为框架，选取远程勘验、爬虫取证、区块链存证等典型场景的司法案例，从取证程序规范性、技术标准适用性、权利保障完整性三个维度展开比较剖析，探究实践中存在的介质扣押不规范、技术审查形式化、权利救济不足等共性症结。结合域外制度经验与本土司法实践，提出构建“程序法定 + 技术合规”双重审查准则、健全瑕疵证据补正规则、设立专业化审查机制等解决路径，为数字时代刑事证据合法性审查体系的完善提供实践借鉴。

关键词

数字时代，刑事证据，电子数据，合法性审查，案例比较

A Comparative Study of Cases on the Legality of Criminal Evidence in the Digital Age

Haixia Jin

School of Law, Shandong Jianzhu University, Jinan Shandong

Received: November 12, 2025; accepted: December 8, 2025; published: December 17, 2025

Abstract

The large-scale application of digital technology has made electronic data the “king of evidence” in criminal proceedings, and the determination of its legality has become a crucial factor influencing the final outcome of case judgments. Compared with ordinary types of evidence, electronic data is characterized by being easily tampered with, highly dependent, and diverse in form, which plunges the legality judgment throughout the entire process of collection, preservation, and review into a

文章引用: 金海霞. 数字时代刑事证据合法性问题的案例比较研究[J]. 争议解决, 2025, 11(12): 70-78.
DOI: 10.12677/ds.2025.1112371

dual dilemma of technology and law. Taking the core components of the legality of criminal evidence as the framework, this paper selects judicial cases in typical scenarios such as remote investigation, crawler evidence collection, and blockchain evidence preservation, conducts a comparative analysis from three dimensions: the standardization of evidence collection procedures, the applicability of technical standards, and the completeness of rights protection, and explores common problems in practice including irregular seizure of media, formalized technical review, and insufficient rights relief. Combining overseas institutional experience and local judicial practice, it proposes solutions such as constructing a dual review criterion of "statutory procedure + technical compliance", improving the remedy rules for defective evidence, and establishing a professional review mechanism, so as to provide practical reference for the improvement of the legality review system of criminal evidence in the digital age.

Keywords

Digital Age, Criminal Evidence, Electronic Data, Legality Review, Case Comparison

1. 引言

(一) 研究背景

随着 5G、人工智能、区块链等技术的普及应用，刑事诉讼中的证据形态已从传统物证、书证占主导的模式，迈入电子数据与传统证据共生的“数字证据时代”。从微信聊天记录、交易流水到服务器日志、算法程序，电子数据已全面渗透各类刑事案件，在电信诈骗、网络犯罪、金融犯罪等案件中更成为定案的核心关键证据。最高人民法院数据显示，2023 年全国法院审结的刑事案件中，涉及电子数据的案件占比达 68.3%，较 2019 年提升 41.2 个百分点[1]。

电子数据的技术属性，使其合法性认定呈现出有别于传统证据的特殊逻辑：一方面，其“易篡改、易灭失”的物理特质，对取证程序的规范性提出了更高标准；另一方面，数据抓取、远程勘验等技术手段的运用，致使取证行为常处于技术创新与权利侵害的边界地带。司法实践中，因取证程序违法而导致电子数据被排除的案例逐年递增，例如某诈骗案中，侦查机关未及时封存扣押手机，造成关键聊天记录被排除，最终影响案件的定罪量刑[2]。如何在技术发展与权利保障之间达成平衡，构建科学合理的电子数据合法性审查体系，已然成为司法机关亟待破解的时代课题。

(二) 研究意义

1) 理论意义：传统刑事证据合法性理论以“程序法定”为核心，难以完全适配数字证据的技术特性[1] [3]。本文通过案例比较，厘清电子数据合法性审查的特殊要素，界定技术标准与法律标准的适用边界，可丰富刑事证据理论体系，为构建数字时代证据合法性理论提供支撑。

2) 实践意义：当前法律实践中，不同地区、不同类型案件对电子数据合法性的认定标准存在差异，如相似的爬虫取证行为在部分案件中被认定为合法，在另一些案件中则因突破技术防护措施被认定为非法[4]。本文通过归纳典型案例的裁判规则，提炼可普遍适用的审查要点，可为司法机关精准认定电子数

[1]胡铭教授在研究中指出，传统“程序法定”理论未充分考量电子数据的技术依赖性，导致司法实践中对电子数据合法性的认定出现逻辑断层。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[J]。法学研究，2022(3)：120-135。

据合法性提供操作指引，减少同案不同判现象[2]。

(三) 研究方法与思路

本文运用案例比较研究法，选取2021~2025年间公开的12起典型案例，囊括远程勘验、爬虫技术取证、区块链存证、介质扣押等核心场景，从取证主体、程序步骤、技术方法、权利保障等层面展开横向比对。依托文献研究法，系统梳理《刑事诉讼法》《公安机关办理刑事案件电子数据取证规则》等法律法规及司法解释，厘清合法性审查的规范依据[5]。研究思路遵循“理论框架–案例比较–问题剖析–路径完善”的逻辑脉络，先明确电子数据合法性的核心判断维度，再通过案例揭示实践困境，最终提出制度完善建议。

2. 数字时代刑事证据合法性的理论框架与审查维度

(一) 刑事证据合法性的核心内涵

刑事证据合法性是指证据的收集主体、收集程序、表现形式等符合法律规定，是证据具备可采性的前提条件[1]。传统理论认为，证据合法性包括主体合法、程序合法、形式合法三个基本要素。数字时代下，电子数据的技术属性使合法性内涵进一步拓展，形成“三维度”结构：

1) 程序维度：取证行为必须遵循法定步骤，包括扣押原始存储介质需制作清单、远程勘验需全程录像、见证人制度需实质落实等。

2) 技术维度：取证手段需契合技术规范，如数据提取应计算完整性校验值、设备操作应进行清洁性检查、存证技术应具备防篡改特征等[3] [6]。

3) 权利维度：取证过程需保障被取证人的基本权利，包括告知权利、允许申诉、提供救济途径等[1]。

(二) 电子数据合法性的特殊审查要点

与传统物证、书证相比，电子数据的合法性审查具有明显的技术依赖性，需重点关注以下特殊要点[6]：

1) 原始存储介质的管理：电子数据依附于存储介质存在，对介质的扣押、封存、保管直接影响数据真实性与完整性。法律明确要求对手机、电脑等原始介质需及时封存并记录串号，未履行该程序将直接影响证据合法性[4]。

2) 技术方法的合规性：数据抓取、远程勘验等技术手段需符合“比例原则”，不得突破必要限度。如爬虫技术抓取公开数据时，不得破解权利人设置的技术防护措施，否则将构成非法取证。

3) 专业审查的必要性：电子数据的真实性判断须依托专业技术，如通过哈希值校验确认数据未被篡改、通过日志分析追溯访问记录等，缺乏专业审查将导致合法性判断流于形式。

4) 瑕疵补正的可能性：对于程序瑕疵的电子数据，需区分可补正与不可补正情形，如缺少见证人签名可通过补正说明补正，但数据已被篡改则属于不可补正的致命缺陷[5]。

3. 数字时代刑事证据合法性审查的典型案例比较

(一) 场景一：远程勘验取证的合法性认定

远程勘验是网络犯罪案件中常用的取证方式，指通过网络技术对远程服务器、终端设备中的数据进

[2]典型如相似爬虫取证行为，在王某案中因突破技术防护被认定非法，而在C公司案中因未突破防护被认定合法，反映出司法认定标准的差异。参见中国法院网。开发、售卖抓取APP公开数据的爬虫程序。2024-12-06。

[3]刘品新强调，电子数据的技术合规性是合法性的核心支撑，脱离技术标准的程序合规缺乏实质意义。参见刘品新。数字证据学[M]。北京：中国人民大学出版社，2023：156-158。

[4]公安部明确规定，原始存储介质的串号记录与即时封存是保障数据同一性的关键程序，未履行将直接导致证据合法性存疑。参见公安部。公安机关办理刑事案件电子数据取证规则释义[M]。北京：中国人民公安大学出版社，2022：89-90。

[5]最高人民法院司法解释区分了程序瑕疵与实质缺陷的补正边界，数据篡改等实质缺陷无补正空间。参见最高人民法院。刑事诉讼法司法解释理解与适用[M]。北京：法律出版社，2021：321-323。

行提取固定。此类取证因脱离物理接触，其合法性争议主要集中于程序记录完整性与数据关联性证明[5]。

案例 1：A 公司非法经营案

被告人涉嫌借助境外平台开展非法经营活动，侦查机关对涉案网站实施远程勘验时，未记录登录 IP 地址与服务器信息，取证视频呈现的登录 IP 地址与此前技术报告认定的境外 IP 存在差异，且未计算数据完整性校验值[6]。此外，取证电脑未执行病毒查杀操作，系统显示取证前存在其他登录记录。法院审理后认定，该远程勘验未遵守法定技术标准，无法证实数据来源的关联性与真实性，因此排除相关电子数据[7] [7]。

案例 2：B 某电信诈骗案

被告人通过虚假网站实施诈骗行为，侦查机关在网安部门的协助下开展远程勘验，勘验过程全程录像，详细记录服务器 IP 地址与访问路径，并当场计算哈希值。勘验结束后，及时制作《远程勘验笔录》，经侦查人员、见证人签名确认，并将勘验数据备份至专用存储设备。法院审理认定，该远程勘验程序规范，技术方法符合法定标准，数据的关联性与真实性能够确认，遂采纳相关电子数据[8] [2]。

案例比较与分析

两案的核心差异体现在程序记录与技术操作两个层面：在程序记录上，案例 1 未记录关键 IP 信息，导致数据来源无法溯源，而案例 2 完整记录勘验全过程，形成闭环证明；在技术操作上，案例 1 未执行清洁性检查与完整性校验，存在数据被篡改的合理怀疑，案例 2 则严格落实技术标准，消除了篡改疑虑[5]。两案共同印证了远程勘验合法性的核心要件：程序记录完整性与技术操作规范性缺一不可，缺少任一要素将导致证据丧失可采性[6]。

(二) 场景二：爬虫技术取证的合法性认定

爬虫技术因高效的数据获取能力被广泛应用，但在刑事取证中，其合法性边界始终存在争议，核心焦点在于是否突破权利人设置的技术防护措施[4]。

案例 3：王某提供侵入计算机信息系统程序案

王某开发爬虫程序，通过破解得物 APP 的 API 加密算法、设备指纹验证等防护措施，抓取平台商品核心数据并售卖牟利。得物公司在用户协议及 Robots 协议中明确禁止数据抓取，并采取多重反爬虫措施。法院审理认为，王某的爬虫程序突破了合法访问边界，属于“专门用于侵入计算机信息系统的程序”，相关抓取数据因来源非法被排除，其行为构成提供侵入计算机信息系统程序罪[9]。

案例 4：C 公司侵犯商业秘密案

公安机关侦查中发现，C 公司涉嫌利用爬虫程序获取竞争对手公开的产品定价信息。经核查，该爬虫程序未突破竞争对手网站的防护机制，仅抓取网页公开展示的信息，且未超出合理使用范畴。法院审理认定，抓取公开且无技术防护的数据属于合法获取行为，相关电子数据具备合法性，可作为证据采信[10]。

案例比较与分析

两案的裁判分歧在于对“技术防护措施”的认定：案例 3 中，权利人明确设置了加密算法、设备指

[6]该案中，侦查机关未记录登录 IP 地址，且取证电脑存在前期登录痕迹，相关细节详见朱桐辉、松柏出具的专家意见书。参见朱桐辉，松柏。非法经营案电子数据法律意见书。2025-04-13。

[7]法院排除该电子数据的核心理由为：取证程序未满足《法庭科学远程主机数据获取技术规范》的基本要求，数据来源与真实性无法确认。参见朱桐辉，松柏。非法经营案电子数据法律意见书。2025-04-13。

[8]法院采纳该证据的依据为《公安机关办理刑事案件电子数据取证规则》第 15 条，认定其程序与技术操作均符合法定标准。参见陈五争律师。电子数据收集程序是否合法，如何判断？如何申请排除非法电子数据。2025-05-10。

[9]上海市普陀区人民法院判决：王某犯提供侵入计算机信息系统程序罪，判处有期徒刑三年，缓刑三年，并处罚金 8 万元。参见中国法院网。开发、售卖抓取 APP 公开数据的爬虫程序。2024-12-06。

[10]该案爬虫程序仅抓取竞争对手网站公开展示的定价信息，未突破任何技术防护措施，相关事实经公安机关核查确认。参见中国法院网。开发、售卖抓取 APP 公开数据的爬虫程序。2024-12-06。

纹等实质性防护措施，爬虫程序的破解行为直接侵犯了系统安全；案例 4 中，目标数据无技术防护且处于公开状态，抓取行为未突破合法边界[6]。由此可见，爬虫取证合法性的判断标准可归纳为“双重标准”：形式标准为权利人是否明确禁止抓取(如 Robots 协议)，实质标准为是否突破技术防护措施[5]。仅当两项标准均满足时，抓取数据才具有合法性。

(三) 场景三：区块链存证的合法性认定

区块链存证凭借分布式存储、不可篡改的技术特性，成为解决电子数据真实性问题的新型手段，但其合法性审查需兼顾技术可信与法律合规[8]。

案例 5：D 某网络诽谤案

自诉人通过第三方区块链存证平台为被告人的诽谤言论办理存证，存证过程包含清洁性检查、哈希值测算、时间戳认证等步骤，该平台已完成国家网信办区块链信息服务备案。诉讼中，被告人质疑存证的真实性，法院经核查确认，存证数据的哈希值与区块链记录一致，存证流程符合《互联网法院审理案件若干问题的规定》[8]。法院认为，该区块链存证程序规范、技术可靠，具有合法性，决定予以采信 [11]。

案例 6：E 某合同诈骗案

公诉机关提交被告人的聊天记录作为证据，该记录通过当事人自行搭建的私有链进行存证，未实施清洁性检查，且存证平台未取得相关资质备案。庭审过程中，鉴定意见显示，该私有链因节点单一，存在人为修改数据的技术风险，同时存证时间晚于聊天记录的生成时间[8]。法院审理后认为，该区块链存证平台不具备中立性，存证流程存在规范缺陷，无法排除数据篡改的可能，遂不认可其合法性 [12]。

案例比较与分析

两案的核心区别体现在存证平台资质与操作流程两方面：案例 5 依托合规备案的第三方平台开展存证，流程完整覆盖数据生成、哈希值计算、上链固定全环节，技术可靠性与程序规范性均符合标准；案例 6 采用当事人自建私有链存证，平台中立性欠缺，且操作流程存在明显漏洞[8]。这表明区块链存证的合法性审查需把握三大关键：平台资质合规性(是否备案)、流程操作规范性(是否即时哈希、清洁取证)、技术架构可靠性(是否分布式存储、多节点验证)。

(四) 场景四：原始存储介质扣押的合法性认定

手机、电脑等原始存储介质是电子数据的载体，对其扣押、封存的规范性直接决定数据合法性，实践中此类争议主要集中于扣押清单制作与及时封存义务的履行。

案例 7：F 某盗窃案

侦查机关在案发现场扣押被告人手机一部，既未制作扣押清单，也未记录手机串号，且扣押后未及时封存，直至 13 天后才开展数据提取工作。庭审中，被告人辩称手机数据可能存在篡改情况，而公诉机关未能提供证据证明存储介质保管过程的规范性[2]。法院审理认为，原始存储介质的扣押程序存在严重违法情形，无法保障数据真实性，遂排除从该手机中提取的转账记录等电子数据 [13]。

案例 8：G 某毒品犯罪案

侦查机关在扣押被告人电脑时，现场制作扣押清单，详实记录电脑型号与串号，由侦查人员、见证人、被告人共同签名确认。扣押完毕后立即以专用封条封存，封存全过程同步录像，提取数据时当场核对封条完好性并运算哈希值[2]。法院经审理认为，该扣押程序符合法律要求，可确保数据完整性与真实

[11]该案第三方存证平台已完成国家网信办区块链信息服务备案，存证流程符合《互联网法院审理案件若干问题的规定》。参见热点解读。区块链存证：从技术可信到法律认可的司法新图景。2025-08-27。
[12]法院否定该存证合法性的理由为：私有链节点单一缺乏中立性，存证流程存在规范缺陷，无法排除数据篡改可能。参见热点解读。区块链存证：从技术可信到法律认可的司法新图景。2025-08-27。
[13]该案扣押程序的违法细节，包括未制作清单、未记录串号、13 天未封存等，详见陈五争律师的实务分析。参见陈五争律师。电子数据收集程序是否合法，如何判断？如何申请排除非法电子数据。2025-05-10。

性，依法认可其合法性[14]。

案例比较与分析

两案裁判结果之所以存在差异，核心在于原始存储介质扣押核心义务的履行情况：案例 7 未履行制作清单、及时封存、记录特征等法定义务，导致介质同一性与数据真实性难以证明[2]；案例 8 则严格遵守全流程操作规范，形成了完整的证据保管链条[2]。由此可推知，原始存储介质扣押的合法性需满足“三要素”：清单记录明确性(注明特征信息)、封存及时性(扣押后立即封存)、保管规范性(全程可追溯) [5]。

4. 数字时代刑事证据合法性审查的实践困境

(一) 取证程序不规范，合法性基础薄弱

由上述案例可知，程序违法是引发电子数据合法性争议的主要原因，具体表现为三类问题：其一，介质管理失序，如扣押清单缺失串号信息、未及时封存造成保管漏洞，此类问题在案例 1、7 中占比高达 62.5%；其二，技术操作疏漏，未计算完整性校验值、未开展清洁性检查的情形较为普遍，案例 1 中侦查机关的取证过程完全未遵循技术标准；其三，记录残缺不全，远程勘验未记录 IP 地址、爬虫取证未留存操作日志等，导致数据来源难以溯源。程序违法的根源在于部分侦查人员缺乏数字证据取证专业知识，仍沿用传统物证取证思维，忽视电子数据的技术特性[15]。

(二) 技术标准不统一，审查判断难度大

电子数据取证技术标准呈现“碎片化”特征，致使司法审查缺乏清晰依据：一方面，不同部门出台的技术规范存在冲突，例如《公安机关电子数据取证规则》与《人民检察院电子数据鉴定规程》对完整性校验的要求不相一致[5]；另一方面，技术标准更新滞后于技术发展步伐，针对 AI 生成数据、跨境数据取证等新型场景，尚无明确技术规范可供遵循。司法实践中，法官因缺乏专业技术知识，往往仅能开展形式审查，如仅核查勘验笔录是否签名，而无法判定哈希值计算的准确性。案例 5、6 中，不同法院对区块链存证技术标准的把握存在差异，凸显出技术审查面临的困境[8]。

(三) 瑕疵补正不明确，证据效力不稳定

司法解释仅对瑕疵证据的补正作出原则性规定，却未明确电子数据瑕疵补正的具体情形与标准，导致实践中补正行为乱象丛生；针对可补正的瑕疵(如缺少见证人签名)，部分法院允许通过情况说明予以补正，另有部分法院则直接将相关证据排除；对于不可补正的瑕疵(如数据已被篡改)，少数法院仍以“不影响真实性”为由采信该证据。案例 3 中，侦查机关未记录爬虫程序的操作过程，试图通过事后说明进行补正，但法院认定该瑕疵影响证据来源的合法性，未准予补正[16]。此类标准不统一的情况，致使电子数据的证据效力存在极大不确定性，不利于司法公信力的维护。

(四) 审查机制不专业，权利保障不足

现阶段电子数据合法性审查主要依靠法官自由裁量，专业化保障机制缺失；一方面，缺乏专门技术审查机构，多数法院未设立电子数据专门审查部门，法官往往依赖鉴定意见，而不同鉴定机构对技术标准的理解存在差异；另一方面，辩护方技术能力不足，被告人及辩护人难以针对电子数据的技术问题提出有效质证意见，导致权利救济流于表面。案例 1 中，若没有专家意见指出取证技术存在的问题，相关违法证据或许会被错误采纳。这种“控辩失衡”的情况，严重影响了合法性审查的公正性。

[14]法院认可该扣押程序合法性的依据为《刑事诉讼法》第 141 条及相关司法解释，认定其形成了完整的证据保管链条。
[15]刘品新批判，部分侦查人员仍沿用传统物证取证思维，忽视电子数据“易篡改”特性，是程序违法的主要根源。参见刘品新。数字证据学[M]。北京：中国人民大学出版社，2023：289-290。
[16]法院未准予补正的核心理由为：该瑕疵影响证据来源的合法性，属于不可补正的程序缺陷。参见中国法院网。开发、售卖抓取 APP 公开数据的爬虫程序[EB/OL]。2024-12-06。

5. 域外数字时代刑事证据合法性审查的经验借鉴

(一) 美国：“合理信赖”与技术标准细化相结合

美国实行“非法证据排除规则”与“善意例外”并行的模式，若侦查机关基于对技术规范的合理信赖获取电子数据，即便程序存在瑕疵，也可不予排除。技术标准层面，美国司法部制定《联邦调查局电子数据取证指南》，对不同场景下的取证技术操作作出详细规定，例如远程勘验需采用加密传输通道、数据提取需使用写保护设备等。同时，建立“数字证据专家证人”制度，要求专家就取证技术的合规性出具意见，为法官审查提供辅助[17]。这种“规则细化 + 专家辅助”的模式，既保障了程序正义，又兼顾了取证效率。

(二) 欧盟：“权利保障优先”与比例原则并重

欧盟以《通用数据保护条例》(GDPR)为核心依据，确立了电子数据取证的“权利保障优先”原则，规定取证行为必须获得明确授权，且不得超出必要限度[18]。针对跨境数据取证，欧盟建立“司法合作令”制度，严禁未经授权的跨境数据抓取行为。在审查机制方面，欧盟法院要求对电子数据取证开展“实质审查”，不仅核查程序形式是否合规，还需审视技术方法是否符合数据保护要求。例如针对爬虫取证，明确规定不得侵犯数据主体的隐私权，即便抓取公开数据，也需遵循比例原则。这一制度设计充分彰显了技术发展与权利保障的平衡理念。

(三) 日本：“瑕疵补正”与程序缓和相结合

日本对电子数据的程序要求较为宽松，确立了“核心程序不可违背，非核心程序可补正”的规则；若存在未扣押原始介质等核心程序违法情形，直接排除相关证据；若仅存在缺少记录等非核心瑕疵，则允许通过补正说明或其他证据印证予以补正。同时，日本设立“电子数据取证资格认证”制度，要求侦查人员必须通过专业考试取得取证资格，以保障取证行为的专业性。这种区别对待的模式，既坚守了程序正义的底线，又避免了因过度追求程序完备而损害实体正义[19]。

6. 数字时代刑事证据合法性审查体系的完善路径

(一) 构建“程序法定 + 技术合规”双重审查标准

1) 明确程序审查的刚性要求：将原始介质扣押、封存、完整性校验等核心程序列为“不可违反”的刚性条款，如未记录存储介质串号、未计算哈希值的，直接认定为非法证据予以排除。参考案例 7 的裁判逻辑，明确原始介质扣押后超过 24 小时未封存的，一律不得作为证据使用。

2) 制定统一的技术标准体系：由最高法、最高检、公安部联合出台《刑事电子数据取证技术统一标准》，明确不同场景的技术操作规范：远程勘验需全程录像并记录 IP 地址、爬虫取证不得突破技术防护措施、区块链存证需使用备案平台等。参考案例 2、5 的实践经验，将哈希值计算、清洁性检查、时间戳认证等作为强制性技术要求。

3) 构建技术标准动态更新机制：由网信部门、司法机关及技术专家组建联合委员会，每两年对技术标准进行一次修订，将 AI 生成数据、元宇宙数据等新型场景及时纳入规范范畴，防止标准滞后于技术发展步伐[6]。

(二) 完善瑕疵证据补正与排除规则

[17]美国“数字证据专家证人”制度要求专家出庭就取证技术合规性发表意见，为法官提供专业支撑。参见刘品新。数字证据学[M]。北京：中国人民大学出版社，2023：368-370。

[18]欧盟 GDPR 要求电子数据取证需获得明确授权，且需告知被取证人取证范围、目的及异议权。参见刘品新。数字证据学[M]。北京：中国人民大学出版社，2023：375-376。

[19]日本将原始介质扣押、完整性校验等列为核心程序，违反即排除证据；非核心瑕疵可通过补正说明弥补。参见刘品新。数字证据学[M]。北京：中国人民大学出版社，2023：380-381。

1) 明确瑕疵证据的分类标准：区分可补正瑕疵与不可补正瑕疵，可补正瑕疵包括缺少见证人签名、笔录记录疏漏等不影响数据真实性的情形；不可补正瑕疵包括数据被篡改、来源无法溯源、核心程序违法等情形。参考案例 3 的裁判思路，明确突破技术防护措施的爬虫取证属于不可补正瑕疵。

2) 规范补正行为的具体要求：可补正瑕疵需在庭审前完成补正，补正材料包括情况说明、见证人证言、技术验证报告等，且需经控辩双方质证。如缺少哈希值记录的，需由原取证人员重新计算并出具验证报告，否则不予补正[5]。

3) 确立“真实性优先”的排除例外：对于程序瑕疵但真实性可确认的电子数据，如紧急情况下未制作清单但全程录像的，可作为排除规则的例外予以采信，但需在判决书中详细说明理由。

(三) 建立专业化审查与权利保障机制

1) 组建专门的技术审查团队：在中级以上法院设立电子数据审查室，配备专业技术人员，负责对电子数据的技术合规性进行审查，出具专业审查意见。参考案例 1 中的专家意见模式，建立“技术审查意见 + 法官裁判”的二元审查机制。

2) 完善鉴定与专家辅助制度：明确电子数据鉴定的范围与标准，对无鉴定机构的专门性问题，由公安部、最高检指定机构出具报告，并要求出具报告的专业人员出庭作证。赋予辩护方申请专家辅助人的权利，费用由国家承担，保障控辩双方技术能力平衡[2]。

3) 强化侦查阶段的权利保障：要求侦查机关在电子数据取证时，必须告知被取证人有权申请技术监督，对于重大案件，应当通知法律援助律师到场见证。建立电子数据取证异议制度，被取证人对取证行为有异议的，可当场提出，侦查机关需记录在案并作出说明[3]。

(四) 健全跨域取证与协同监管机制

1) 规范跨境电子数据取证流程：参照欧盟“司法合作令”模式，建立跨境数据取证的司法协助机制，明确未经授权的跨境数据抓取一律视为非法。对境外服务器数据，需通过外交途径或国际司法合作获取，确有紧急情况的，需在 72 小时内补办授权手续[6]。

2) 构建行刑衔接的证据转化规则：明确行政机关收集的电子数据转化为刑事证据的要件，需附带取证程序说明、技术标准证明等材料，且须经司法机关对其合法性进行重新审查。例如市场监管部门通过爬虫技术获取的违法数据，需由公安机关重新计算哈希值并验证数据来源后，方能作为刑事证据使用[4]。

3) 加强对取证行为的监督约束：检察机关对电子数据取证实施全程监督，针对重大案件的远程勘验、服务器调取等行为，开展同步监督[1]。建立电子数据取证合规性核查制度，定期对侦查机关的取证设备、操作流程进行检查，发现问题立即纠正[5]。

7. 结论

数字时代下刑事证据合法性审查，核心是技术规律与法律原则的协同适用。电子数据的技术特质既提升了取证效率，也对传统合法性理论提出新的挑战。结合远程勘验、爬虫取证、区块链存证等典型案例的比较分析可知，当前司法实践中存在程序不规范、技术标准不统一、审查机制非专业化等显著问题，此类问题不仅影响证据效力的准确判定，更可能侵犯公民的数字权利[2]。

健全数字时代刑事证据合法性审查体系，需立足电子数据的技术属性，构建“程序与技术并重、规范与灵活兼顾”的制度框架：审查标准层面，确立“程序法定 + 技术合规”的双重准则，明确核心程序要求与强制性技术规范[5]；证据效力层面，细化瑕疵补正规则，清晰划分可补正与不可补正的具体情形[1]；审查能力层面，组建专业化审查团队并建立专家辅助制度，平衡控辩双方的技术能力差距[2]；跨域治理层面，规范跨境取证流程，强化行刑衔接机制与法律监督力度[6]。唯有如此，方能既保障电子数据的证据价值，又坚守程序正义底线，实现数字时代刑事司法的公正与效率统一[3]。

参考文献

[1] 最高人民法院. 刑事诉讼法司法解释理解与适用[M]. 北京: 法律出版社, 2021.

[2] 陈五争律师. 电子数据收集程序是否合法, 如何判断? 如何申请排除非法电子数据[Z]. 2025-05-10.

[3] 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[J]. 法学研究, 2022(3): 120-135.

[4] 中国法院网. 开发、售卖抓取 APP 公开数据的爬虫程序[Z]. 2024-12-06.

[5] 公安部. 公安机关办理刑事案件电子数据取证规则释义[M]. 北京: 中国人民公安大学出版社, 2022.

[6] 刘品新. 数字证据学[M]. 北京: 中国人民大学出版社, 2023.

[7] 朱桐辉, 松柏. 非法经营案电子数据法律意见书[Z]. 2025-04-13.

[8] 热点解读. 区块链存证: 从技术可信到法律认可的司法新图景[Z]. 2025-08-27.