Advances in Social Sciences 社会科学前沿, 2025, 14(12), 20-28
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2025.14121061

Hans汉斯

刑事诉讼法视阈下数字证据的审查认定与程序规制

鲁慧宇

澳门科技大学法学院，澳门

收稿日期：2025年10月10日；录用日期：2025年11月27日；发布日期：2025年12月5日

摘　要

随着数字时代发展，网络犯罪数量激增，数字证据成为定罪核心，但传统电子证据概念与规则已不适用，且《刑事诉讼法》相关程序规则原则化，导致证据排除问题频发，还存在取证授权模糊等困境。2012年《刑事诉讼法》将“电子数据”入法及后续规则细化，明确电子、网络、数字三类数据差异，指出数字技术催生五种新型数字证据，并阐述三大诉讼法原则对电子数据的约束。在取证存主体、地域、权利保护争议以及审查认定有真实性缺位与地域分歧。因此在立法上、司法上和技术上需要适配的应对措施，以构建适配数字时代的数字证据理论与规制体系。

关键词

电子数据，数字证据，数据取证，网络犯罪

Review, Determination, and Procedural Regulation of Digital Evidence from the Perspective of Criminal Procedure Law

Huiyu Lu

Law School, Macau University of Science and Technology, Macau

Received: October 10, 2025; accepted: November 27, 2025; published: December 5, 2025

Abstract

With the development of the digital era, the number of cybercrimes has surged, making digital evidence central to conviction. However, the traditional concept and rules regarding electronic evidence

文章引用: 鲁慧宇. 刑事诉讼法视阈下数字证据的审查认定与程序规制[J]. 社会科学前沿, 2025, 14(12): 20-28.
DOI: 10.12677/ass.2025.14121061

have become inadequate. Furthermore, the relevant procedural rules in the "Criminal Procedure Law" are often principle-based, leading to frequent issues of evidence exclusion and dilemmas such as ambiguity in forensic authorization. The 2012 "Criminal Procedure Law" incorporated "electronic data" into the legal framework, and subsequent rules have provided further details, clarifying the distinctions between three types of data: electronic, network, and digital. It points out that digital technology has given rise to five new types of digital evidence and elaborates on the constraints imposed by the three major procedural law principles on electronic data. Controversies exist regarding the subject and jurisdiction of evidence collection, as well as rights protection. In the review and determination process, challenges include the absence of authenticity verification and jurisdictional discrepancies. Consequently, adaptive countermeasures are needed in legislation, judiciary, and technology to construct a theoretical and regulatory system for digital evidence suited to the digital age.

Keywords

Electronic Data, Digital Evidence, Data Forensics, Cybercrime

1. 引言

当下网络犯罪的数量伴随着科技的飞速发展、互联互通的背景下而不断增加。公安部于 2024 年 9 月报道：全国公安机关继续开展“净网 2024”专项行动，对整治的各类网络违法犯罪活动，依法从严从重打击，累计侦办网络犯罪案件 11.9 万余。全年开展信息安全领域监督检查 20 万余次，办理行政案件 4.9 万余起，警告 3.5 万余次，责令整改 6500 余次，清理违法有害信息 50 余万条。从这些数据可以看出每年的网络犯罪数量之多，那么网络数字数据证据就成为侦破案件和定罪的核心关键证据，其重要性也日益凸显。

有学者认为《刑事诉讼法》对电子数据的程序规则过于原则化，所以在司法实践中因程序瑕疵导致证据排除的情况频出。从 2016 年“深圳快播案”的服务器取证争议到杭州华泰一媒“区块链存在第一案”的技术创新[1]，反映出我国刑事诉讼过程中电子数据程序规制存在取证授权模糊、审查标准欠缺、技术规制滞后的三种情况。与此同时，随着当下数字技术的发展，传统的电子数据概念和证据规则已经无法有效地覆盖和规范当前的数字证据[1]。对此我们将对新的电子数据证据进行新的范围界定，并探索新的数字证据审查机制，以及构建本土化的电子数据程序规制体系。

2. 网络数字证据的刑事诉讼法基础

2.1. 法律规范与法律体系

2012 年《刑事诉讼法》将“电子数据”正式纳入到法定证据的范围，代表了刑事证据数字化开始被采纳作为破案依据。对于那时候的网络数字环境来说，互联网还没有广泛的普及，网络犯罪也没有很频繁，那时的“电子数据”也仅仅是停留在以广播、电视、电话或录音机等为媒介的所记录的固定的电子数据，还不具有较强的传播性和易变性。但是这项立法规定对此来说也是具有一定前瞻性的，截至目前

[1]https://baike.baidu.com/item/快播案/19259333

的电子证据的内涵和外延已经有了很大的变化，随着大数据和人工智能技术的兴起，电子证据及其衍生品的使用，都逐渐渗透到刑事案件中[2]。由于立法只规定了概念性和原则性，司法实践中对电子证据的应用存在一定盲区[3]。

在电子数据正式被列入法律条文之前，在司法实践中早已开始被大量运用了[4]。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 [2]，首次从司法解释的层面详细规定了“电子证据”的内容及其审查判断规则。2012 年对刑事诉讼法进行修改时将“电子证据”改为“电子数据”纳入正式立法，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定。[3]2016 年发布的《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》[4]与 2019 年公安部出台的《公安机关办理刑事案件电子数据取证规则》[5]，共同涉及了取证和审查的相关内容。检查并比较两个角度。对电子数据证据规则进行了更加系统和详尽的规定。2021 年的“刑事诉讼法解释”延续了之前的司法解释规定[1]。

2.2. 法律体系下“电子数据”的外延

目前《刑事诉讼法》第 50 条和第 54 条的规定视听资料和电子数据可以作为证据，但我国法定证据种类主要根据证据的外在表现形式做出划分，既与英美法系对证据形式的开放性规定不同，也与大陆法系对“证据方法”和“证据资料”的划分有所区别。传统的说法是把电子证据归入视听资料，部分学者在 1982 年第一次以法律形式肯定视听资料的名称和地位时，对包括录音资料、录像资料和电脑储存资料等视听资料的名称和地位，在我国 1982 年《民事诉讼法(试行)》中，大致主张“视听资料”包括录音、录像、计算机存储资料及其他音像证据[5]。也有学者从其他方面定义，从载体形式来看，在保证该类介质的内容能够固定、不会消失或修改的情况下，如果在硬盘、磁盘、光盘等介质上记录了输入和存储的信息，即为准书证；经计算机处理过的资料，如在上述介质中存储，则同一种情况下，仍按准书证、书证等方式处理；若输出至印纸，则以书证为宜。从输出形式上看，若表现在纸上，则为书证；若表现为声像，即视听资料[6]。

综合以上学者的观点，传统的电子数据所涵盖范围已经跟不上目前数字时代更迭下产生新的数字技术。关于电子数据、数字数据与网络数据三者之间都应该有着相应区分，数字数据是底层形式，电子数据和网络数据是在不同场景中的具体应用，电子数据侧重“存储”，网络数据侧重“传输”，而数字数据是两者的共同技术基础。表 1 和图 1 分别是它们的特点和关系，因此现在因应日益繁杂的网路犯罪，传统的电子资料也就是包含影音资料和网路资料，无法作为案件的充分证据来处理。

Table 1. Characteristics of the three types of data
表 1. 三种数据的特点

纬度	电子数据	网络数据	数字数据
核心属性	强调存储介质(电子设备)	强调传输环境(网络)	强调数据形式(二进制编码)
存在形式	静态存储或本地处理	动态传输或远程存储	抽象的逻辑表示
依赖技术	存储技术(SSD、HDD)	网络协议(HTTP, TCP, IP)	编码技术(ASCII, Unicode)
覆盖范围	电子设备中的全部数据	网络交互中的部分数据	所有电子化数据的底层形态

[2]https://www.spp.gov.cn/spp/flfg/sfjs/201212/t20121228_52202.shtml
[3]https://baike.baidu.com/item/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/15898472?fr=aladdin
[4]https://www.spp.gov.cn/spp/zdgz/201609/t20160921_167425.shtml
[5]https://www.spp.gov.cn/zdgz/201609/t20160921_167425.shtml

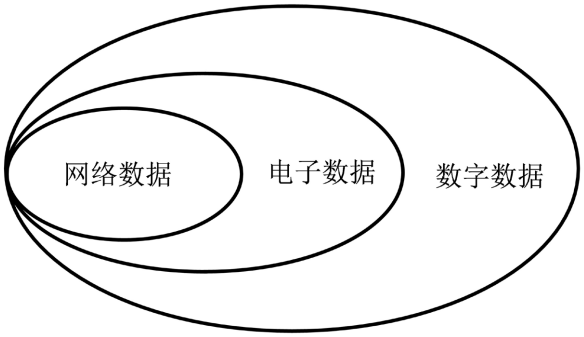

Figure 1. The relationship between the three types of data
图 1. 三种数据之间的关系

数字技术的发展引领人们进入虚拟数字空间领域，突破了传统的物理空间，使人类社会由单维的社会系统逐渐分化为二维的社会系统，这种社会系统是虚实共生的[7]。电子化、信息化、数据化的生产生活和社会关系必然使人类的生产生活、社会关系，各种类型的司法案件也随之产生。证据对案件事实的复原和描述，证据与载体的结合方式决定了证据的存在形式[8]。在司法案件的证据体系中，电子数据的数量日益增加，形式多样化，其重要性也日益增强。同时在网络犯罪侦查和信息技术纠纷的审判时的数字证据也就更加关键[9]。因此在当下的数字环境中，司法证据逐渐按照数字空间的分化趋势表现出电子化、区块链化、大数据化、人工智能化和虚拟仿真化五个基本方面，在此基础上就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这五种主要的数字证据形式。因此相关学者建议针对不同的类型，分别构建阶梯式分类审查机制和开放的实质审查机制[1]。

2.3. 刑事诉讼法基本原则对电子数据的约束

首先是合法性原则的遵守，在刑事诉讼过程中应当保证取证主体和取证所采用的技术手段是符合法律规定的，尽量避免“非法证据”的产生。在技术上对于使用没有认证的程序或软件获取的证据，法院应该合理排除，所以应将技术合规纳入程序合法性的审查犯罪中。

其次是直接言词原则的调适，电子数据依赖技术鉴定的间接性，无论是取证的过程还是对于呈现出的电子证据都不能清楚知道其真实性和完整性，应该充分保障被告人的质证权。比如法院在审理过程中就应当要求侦查人员出庭对取证和远程勘验过程等环节进行说明，来弥补电子数据取证环节的言词证据缺失。

最后是证据裁判原则的严格要求，对于作为证据的电子数据其真实性应该通过相应的技术验证，就比如通过哈希值来验证数据是否被篡改，相同数据的哈希值始终是一致的，任何微小乃至一个字符的改动都会造成哈希值的改变。哈希值作为电子数据的“数字指纹”在司法实践中广泛使用，常用 MD5、SHA-256 等哈希算法进行比对，来验证电子数据的完整性。

3. 网络数字证据的刑事诉讼程序困境

3.1. 取证程序合法性争议

3.1.1. 取证主体和程序的合法性

目前《刑事诉讼法》第 54 条规定“人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。”那么有权进行取证的就只有我国的审判机关、检察机关和侦查机关，取证的范围包括了所有类型的证据。由于互联网的发展，网络犯罪的案件数量逐渐增长，因为网络载体与其它证据载体之间存在着很大的不同，这就给司法工作人员在取证程序中带来了巨大的困难，利用传统的证据收集方式很

难获取电子证据[10]。因为电子证据并不是所见即所得，也不是“眼见为实”的存在，需要通过较高的计算机技术来获取，那么大多数的司法工作人员中是不具备在计算机领域中的较高水平和相关的专业知识。因此在网络犯罪的案件取证过程中，就需要相应的计算机专业技术人员或专家的协助，但是专业技术人员一方面不具备取证的法律上的主体资格，《刑事诉讼法》第 146 条仅规定：“为了查明案情，需要解决案件中某些专门性问题的时候，应该指派、聘请有专门知识的人进行鉴定。”对于专业人员是否可以直接参与和接触取证的内容是有待讨论的。

另一方面即使通过授权主体资格，专业人员也不具备相应的法律知识，他们的取证方法也不一定会符合法律规范，取证的内容是否会有误差，从而导致辛苦获取的证据最后被作为“非法证据”给排除了。这种授权流程繁琐和聘请专业人员费时的冲突情况下，在实际司法实践中必然会导致办案取证的时间浪费。因为电子证据易丢失、易销毁和难保存的特点，时间上的耽误便会给不法分子提供了销毁证据的时间，造成电子证据的永久性灭失，且难以恢复。网络数据在互联网环境中，任何群体都可以与之构建相应的联系，访问其中的内容。这就会存在如果被害人及其家属，自己通过黑客技术和其他技术自行去获取证据的问题。成功获取也会因为违反《刑事诉讼法》被合理排除，获取失败便会引起不法分子的警觉而设置加密程序或销毁程序，导致后期司法人员的工作开展困难。

在裁判文书网中检索“境外电信网络诈骗”的词条，可以检索出 157 篇文书，从文书中可以看到大部分都是犯罪嫌疑人主动投案自首或在他人劝告下自首的。以及网上查阅的诸多境外电信诈骗案例，基本都需要犯罪嫌疑人的帮助才能掌握关键信息。这也从侧面反映出对于这种跨境的网络犯罪证据的获取相当困难，耗时之久。[6]

3.1.2. 地域取证的阻碍因素

网络犯罪比传统犯罪类型在侦查上困难的地方在于，网络犯罪对地域没有要求，借助网络平台犯罪人可以对任何地点的受害人实施犯罪行为。传统犯罪的第一时间基本就可以确定犯罪发生的地点和时间，而网络犯罪因网际网路复杂的特点，犯罪人可以通过虚拟的账号、虚假的定位、虚构的网域和设置定时程序等方式来掩盖自己犯罪的地点和时间，给侦查带来了巨大的难度。

此外犯罪人实行网络犯罪会设法将云端服务器存储在境外，这样即使锁定了犯罪人的地址，但是相关的数据却都存储在境外，没有办法第一时间获取或封存数据，增加极大的不稳定因素。更不用说犯罪人直接在境外通过网络对国内被害人实施犯罪行为的，不仅无法获取证据，而且不能在第一时间就锁定犯罪人地址。同样如果所有相关数据都是虚假的，对此犯罪人的搜索将犹如大海捞针。

2023 年全球网络安全峰会披露，跨国网络犯罪造成的经济损失巨大，但是跨境电子证据调取的成功率不足 27%。国际刑警组织的调查显示，67%的跨国网络犯罪因电子证据获取受阻而无法起诉。某勒索软件攻击案中，关键日志存储于俄罗斯服务器，依据当地法律需总统特批才能调取，最终导致追查中断。[7]同时国内的大部分跨境诈骗案，服务器基本都在菲律宾、越南和缅甸等国家，调取数据耗时之久很容易造成关键证据灭失，所以“数据主权”与“司法协作”之间很难协调统一。

根据 2018 年通过的《中华人民共和国国际刑事司法协助法》第 25 条和第 26 条规定，向外国请求调查取证不仅要先经国内的机关审核同意，再去通过对外联系机关向国外提出请求，而且所需要准备的材料也很繁多。据司法部统计，通过中央机关向境外提出请求，平均周期就需要 14~18 个月。[8]时间上的损

[6]http://www.gxhepu.jcy.gov.cn/html/ajjj/detail_2024_07/26/1825.html，依法惩治跨境电信网络诈骗及其关联犯罪典型案例。
[7]https://blog.csdn.net/m0_71322636/article/details/147671474，《跨国黑客攻击的取证困局：云端日志的司法管辖权博弈》。
[8]参见百态老人：《跨境黑网贷案件的法律与技术治理体系》。
https://xueqiu.com/6916781846/327398427?md5__1038=110279f682e-%2B9ykVahalod%2BwDL%2BaFaYmaC9L9do9Li-Hek302Hu4Gs9IWqUxkB4ka%2BdI1uplqbpuY30abwX9LuYaaRajkaW3au0dKau9LcnZ0YiYaG0amaR0dA%2Bzaurya-VzPLQaE0yFMJKxwxiad9dwYaYWaztrVawYGauegyue60KYHnDkzqW0EqHYa0P0CydcRYLY9%3Dpa

失，极易造成关键证据因境外服务器数据无法及时调取而灭失。

目前虽然按照属地管辖原则可以扩大解释，但只要涉及资金交割、信息互通等行为在国内发生，即使服务器在国外，也可以主张管辖。犯罪人将服务器存储在境外，也是要通过境内 IP 地址才能完成特定的程序，所以对于犯罪行为地是没有争议的。根据属人管辖原则，对于处于境外的犯罪人仍是用于管辖权的。但是这些只能针对犯罪人本身的抓捕工作，对于数据证据的获取和固定无法提供帮助。对此有学者认为可以通过“服务器镜像技术”复制境外服务器数据至境内司法鉴定中心，实现“数据主权”的延伸[10]。2018 年的“区块链存证第一案”即华泰一媒文化传媒有限公司诉深圳道同科技发展有限公司侵犯著作权案，法院首次确认了区块链技术固定电子数据和镜像类数据的效力，进一步说明了该操作的可行性。

3.1.3. 证据取证与个人权利保护的界限

现代人将互联网作为自己存储数据资料和文件等载体工具，所有的交流学习都转移到了网络平台，网络的使用逐渐成为人们日常生活习惯，用户的一切行为模式就以数据的形式记载在网络中。有学者认为个人资料与个人隐私又是密切相关的，在收集涉案证据的同时，电子证据往往涉及与案件无关的一些文献资料，极有可能构成对材料所有人的隐私权的侵害，因此，在搜集涉案证据时，电子资料与个人资料之间存在着密切的联系。各国刑事诉讼共同面临的任务就是打击犯罪，保障个人权利，现在各国的刑事诉讼不可能只追求一个方面，而要尽量在保护个人权利的前提下对犯罪进行打击，当然在个案中也会有所调整，在数据保护措施是否得到必要的限制。一个国家的个人权利保障状况，应该反映一个国家对数据保护措施的必要限制是否予以限制。电子证据刑事侦查措施要达到打击犯罪、保障个人权利的平衡[11]。《关于网络犯罪的公约》[9]对调查措施的适用条件和权力保障的要求作了规定，在法律上的有效实施以及个人权利保障方面，缔约方应当将有关措施规定在本国法律中，并体现在相互称谓原则上，以达到平衡。

对于个人权利保护目前没有详细的措施，对于网络服务的提供者也没有相应的数据保存要求和义务。但是可以看到现在注册 APP 或者浏览一些网页的时候，总是会说根据相关法律规定，要求用户同意授权自己的个人信息才能完成注册使用，因此许多非法平台总是以此为借口收集用户的个人信息。《刑事诉讼法》要求尊重和保障个人权利，那么就不会把让侦查机关的权利过分凌驾于个人权利之上，而应该按照相称性的原则，对个人权利的保护，还是应该给予相应的保障，使公民的正当权利和自由得到保护。

对于电子证据的侦查取证有时还需要在很大范围或在侦查案件的早期适用，但是这些措施在刑事案件发生后是必须要适用的，而且必须是合乎法定的程序，在数字网络空间里严禁作为防御犯罪的手段，不能违背司法的公正性，也不能违背社会公共利益的客观需要，更是不能作为监控数字网络空间的正常社会生活的手段。权利的释放下，必然会引起对个人信息和数据的过度监管，但凡有风吹草动便会以预防为由随意调取。同样如果与商业挂钩，以“技术侦查”等理由利用商业爬虫抓取平台数据给第三方，这样不仅个人隐私安全得不到保障，而且商业主体也会迎来严重的经济损失。那么应该考虑受到电子证据调查影响的第三人的权利和正当利益，尽量避免对其造成不良影响，如果必然，就应该采取尽量减少这种影响的措施，避免给第三人造成损害，从而引起第三人的损害的补偿[11]。

3.2. 证据真实性的审查缺位和证据认定分歧

信息与大数据时代，电子证据毋庸置疑的成为新的“证据之王”[12]，随着杭州、北京和广州等地的互联网法院的陆续成立，电子证据的应用也越来越频繁[13]。所有的纸面证据和材料都将转化为电子数据

[9]https://www.spp.gov.cn/spp/zdgz/202508/t20250827_704693.shtml

的形式，以及网络犯罪的愈发频繁，相关数据作为证据的范围面也越来越广。由于数据载体的复杂性和专业性，以及数据本身的可变性、复合性和再生性[14]，对此电子证据的审查就应具有一定的技术性。真实性审查可以利用哈希校验的方法，关联性审查可以利用 IP 地址为链和数据行为链的方式进行审查。但是基本上的法官或者其他司法工作人员必然不具备如此专业的技术水平，那么他们自身就没有办法对数据的真实性做出判断。

检察机关技术审查能力不足，就会导致检察机关可以以“技术复杂性”为由要求辩方自证数据真实性，这就导致举证责任的错位。同时辩方和辩护律师也不一定具有能够验证真实性的能力，那边导致诉讼程序遇到了僵局。

有学者调查研究发现地域之间也会存在差异，就比如优先建立互联网法院的广州、杭州和北京，法官对“区块链存证”了解的就比其他地区的要深入详细。据数据统计已经有司法区块链平台的互联网法院，也仅有 24.02%的裁判者比较了解，其他地区的法院了解率仅不到 3% [15]。同时涉及区块链证据的案件中，仅有 24%的判决书详细说明了哈希值校验过程，而非互联网法院地区这一比例低于 5%。这表明技术审查标准在实践中严重依赖于地区司法资源与法官认知水平。因为不了解和技术水平的问题，就造成大多数电子数据的审查仅核对提取笔录的签名，没有审查原始的储存媒介。受各地经济和科技水平发展影响，造成审查标准的割裂和司法判决的差异。对此可以借鉴《民事诉讼法》中的专家辅助人制度来弥补技术上的空缺，但仍需注意地区之间的不平衡，司法资源的不平等的情况，否则就只会导致该制度的虚置。

4. 程序法视角下的完善路径

4.1. 立法层面：细化取证程序和构建层次化程序规制

4.1.1. 义务提供原则下的程序细化

义务提供原则是指人民法院、人民检察院、公安机关在依法收集、调取证据过程中，掌握电子证据的单位、组织和个人对涉案电子证据有义务及时全面地提交。电子证据的义务提供原则的含义，一是电子证据正好掌握了与案件有关的电子证据，电子证据与其他传统证据一样，在任何单位或个人手中都有可能被掌握；二是网络服务商等法律法规规定的电子证据第三方保存部门的义务来源，法律对此有规定[16]。也是来源于《刑事诉讼法》中现有的规定，其优势在于可以减少上述提到的技术障碍，提高侦查的效率，这些数据由单位、组织或个人自行维护存储，遵守真实原则，自行解决技术问题。在后期司法机关取证过程中就可以直接获得其提供的解码过的数据，在交由相应的机关审查，便可被直接采纳。对比于额外聘请专业技术人员，司法机关自行取证审查等，由第三方主动提供数据证据，是要节约较多的时间和精力的[17]。

其次，这可以有效减轻对合法权益的侵害，从而最大程度地保障个人权利。自己掌握数据，履行义务提供原则，便可以自行对涉及犯罪内容的部分数据进行截取，提供给相应的司法工作人员。就不需要司法工作人员，对所有的数据进行审查，涉及公司的数据往往包含着大量的商业秘密，价值巨大。同时这些多方数据混杂的情况下，对全部的数据进行核查，不仅会妨碍正常的生产经营程序，也是浪费大量的司法资源。所以这样可以更好避免私密数据的泄露，更好的保护第三方合法权利和用户的个人信息安全。

最后在跨境协作的构建上，涉外电子程序的及时获取可以避免繁琐的司法程序。同样因为国家的主动介入，需要层层申请审批，准备繁琐材料信息，极度的损耗时间。义务提供原则下跨国公司自行准备好需要提供的相应数据，在两国沟通完成后，由该国司法机关直接转交给我国，综合节省了多方面的成

本。

4.1.2. 授权机制分级和操作流程法定

首先按照部分学者的物理层、逻辑层、数据层和内容层的数字空间层级将数字证据类型分为电子证据、区块链证据、大数据证据、人工智能证据和虚拟仿真数据。根据数字证据不同的类型和特点，分层级的构建相应的取证和审查机制。也可以根据技术侦查审批标准，建议对应的电子数据取证的等级审批制度。依据证据的关键程度，分为普通数据、敏感数据和核心数据，依照关键程度和私密等级对审批主体和取证程序都进行层层递进的严格要求。操作流程的法定化上，可以在法律规定中增加电子数据的专门章节内容，依据现在数字环境背景下，对电子证据的界定、性质、取证和审查等相关内容详细罗列，并且规定原始数据存储介质优先提取和远程勘验同步录像等强制性程序。

4.2. 司法层面：完善审查认定体系

在司法上，可以构建如图 2 展示的“形式和实质”的复合审查模式，通过专业技术对证据进行真实性和有效性的实质审查，依据侦查申请材料和取证主体审查符合法定形式，两者相互配合，就可以保障审查的全面性和准确性。

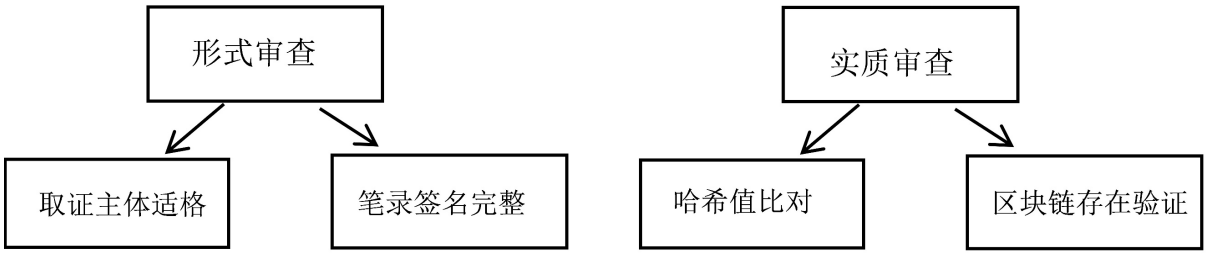

Figure 2. Composite review mode
图 2. 复合审查模式

通过建立国家级电子数据专家库，按照法院指定和政府付费的模式，破解辩方聘请能力不足的问题，解决地区专业水平差距过大问题，充分激活专家辅助机制。还可以在国家的专业研究机构和院校中，成立双领域专业复合型研究小组，培养复合型人才，随时可以投身到案件取证程序实践中。

4.3. 技术层面：嵌入刑事诉讼程序与数字法治融合

飞速发展的数字时代下的 AI 和人工智能技术的应用，也可更好的帮助在证据领域的发展。人工智能证据是机器意见，可以用 AI 分析形成的证据来证明案件事实。人工智能证据作为一种新型的科学证据，主要包括相关性和可靠性两个方面，在使用时审查内容，是由机器而非人类做出的实质性判断。关联性是由三个层次构成的，即技术关联性、数据关联性和结论关联性，在复习关联性的时候要按照“适当”的标准[18]。通过高级的算法计算，同样可以弥补技术能力不足的问题，我们不应当畏惧人工智能的发展，担心被其取代，而是应该更好的去利用这个先进的工具，帮助我们去解决疑难问题。区块链存证入法以及对专业取证工具的认证是我们当下需要去完善和普及的问题。

5. 结语

时代的发展总是伴随着新鲜事物的产生，对于落后的事物，通过新的解读为其赋予新的生命。正如梁静教授所说，我们把证法从神证转化为人证，再转化为物证为主的证法，使证法在飞跃中不断向前发展。我们现在已经从传统的电子数据时代进入了更加广泛的数字证据解释的时代，我们已经进入了一个

更新的司法证明的时代。科技迭代发展不应该阻止我们进步的步伐，对于新起的证据类型也不应该避之不及，面对问题更应该迎难而上，积极面对。

面对自身在数字证据领域的知识和技术的不足，要立足于自身实际出法，借鉴他国的丰富经验，总结出符合自己的模式。充分利用好科技发展的趋势，也不盲目依赖科技，在传统证据和传统电子证据结合的基础上，利用不同证据之间的关联性和优缺点，构建新时代的刑事诉讼中数字证据理论。

参考文献

[1] 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.
[2] 左卫民. 数字化背景下刑事诉讼法修改的重要方向[J]. 中国刑事法杂志, 2024(4): 39-52.
[3] 奚玮. 我国电子数据证据制度的若干反思[J]. 中国刑事法杂志, 2020(6): 135-154.
[4] 郑飞. 证据种类法定主义的反思与重构[J]. 中国法学, 2024(1): 105-123.
[5] 刘品新, 张斌. 电子证据在我国的法律地位[J]. 证据法论坛, 2003, 6: 183-200.
[6] 戴莹. 电子证据及其相关概念辨析[J]. 中国刑事法杂志, 2012(3): 73-77.
[7] 郑飞, 夏晨斌. 系统论法学视野下的元宇宙法律治理研究[J]. 河北学刊, 2023, 43(2): 205-215.
[8] 占善刚, 王超. 从法定电子数据迈向电子数据法定[J]. 湖北大学学报(哲学社会科学版), 2021, 48(2): 110-119.
[9] 左卫民. 迈向数字诉讼法: 一种新趋势? [J]. 法律科学, 2023, 41(3): 53-61.
[10] 裴兆斌. 论刑事诉讼中电子数据取证模式[J]. 东方法学, 2014(5): 87-95.
[11] 梁静. 电子证据在刑事诉讼中的收集与认证[J]. 河南财经政法大学学报, 2012, 27(4): 117-123.
[12] 刘品新. 中国电子证据立法研究[M]. 北京: 中国人民大学出版社, 2005: 8-9.
[13] 许晓彤, 肖秋会. 电子文件与证据法学中相关概念的比较及其演化脉络分析[J]. 理论纵横, 2019(2): 23-28.
[14] 徐燕平, 吴菊萍, 李小文. 电子证据在刑事诉讼中的法律地位[J]. 法学, 2007(12): 131-135.
[15] 段莉琼, 吴博雅. 区块链证据的真实性认定迷局与规制重构[J]. 法律适用, 2020(19): 149-163.
[16] 樊崇义, 李思远. 论我国刑事诉讼电子证据规则[J]. 证据科学, 2015, 23(5): 517-530.
[17] 皮勇. 网络安全法原论[M]. 北京: 中国人民公安大学出版社, 2008: 641.
[18] 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.