

电子数据的鉴真规则与审查方法

完整性与真实性：鉴真规则的双重构造

赵跃

（安徽国运律师事务所，安徽 合肥 230000）

摘要：电子数据的审查，长期在真实性与合法性的框架内展开，忽视了鉴真这一独立环节。其结果是：提取过程不规范的数据，或者被整体排除，或者被整体采信，缺乏中间的处理方式。本文主张，鉴真是独立于真实性与合法性的证据能力要件，其对象是证据与来源的同一性，方法是完整的保管链与可验证的技术手段。鉴真包含两个层面：形式的完整性，即数据自生成至出示未被篡改；实质的可靠性，即数据的生成过程可信。前者依原始存储介质、提取笔录、校验值与保管链审查；后者依生成系统的可靠性、操作人员的资质与数据的内部一致性审查。鉴真不能的，产生证据能力的瑕疵，而非当然排除；瑕疵可以补正，补正不能且影响实质真实的，予以排除。据此，应当建立以保管链为核心的审查框架，明确举证责任、专家辅助人的作用、以及不同数据类型的审查重点。

关键词：电子数据；鉴真；保管链；完整性校验；证据能力；瑕疵补正

中图分类号：D925.1 **文献标识码：**A **文稿编号：**WJLT(2025)02-0053-13

Authentication Rules and Examination Methods for Electronic Evidence: The Dual Structure of Integrity and Reliability

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: The examination of electronic evidence has long proceeded within the framework of reliability and legality, neglecting authentication as an independent step. Consequently, data obtained through irregular extraction is either wholly excluded or wholly admitted, with no intermediate treatment. This article argues that authentication is a requirement of admissibility independent of reliability and legality; its object is the identity between the evidence and its source, and its method is a complete chain of custody together with verifiable technical means. Authentication comprises two levels: formal integrity, meaning the data has not been altered from creation to presentation, examined through original media, extraction records, hash values and chain of custody; and substantive reliability, meaning the generation process is trustworthy, examined through system reliability, operator qualification and internal consistency. Failure of authentication produces a defect in admissibility rather than automatic exclusion; the defect may be cured, and exclusion follows only where cure is impossible and substantive truth is affected. A chain-of-custody framework should therefore be established.

Key words: electronic evidence; authentication; chain of custody; integrity verification; admissibility; cure of defects

说明：（本文为作者个人研究观点，不代表所在单位意见）

作者简介：赵跃，安徽国运律师事务所执业律师，研究方向为诉讼法学、证据法学。

一、问题的提出

电子数据已经成为民事诉讼中的主要证据类型。合同、转账、聊天、邮件、网页，几乎所有的交易与社会交往都留下了电子痕迹。与之相应，电子数据的审查，成为事实认定的关键环节。

民事诉讼证据规定对电子数据的范围与审查作了规定。第十四条列举了电子数据的类型，包括网络平台发布的信息、网络应用服务的通信信息、用户注册信息、电子交易记录、以及文档、图片、音频、视频等电子文件；第九十三条规定了审查判断的要素，包括

生成、存储、传输所依赖的计算机系统的硬件、软件环境是否完整、可靠，是否处于正常运行状态，是否具备有效的防止出错的监测、核查手段等。

规范不可谓不细，但实务的困境依然存在。其一，审查的框架不清。多数判决将电子数据的问题归入真实性或者合法性，忽视了鉴真这一独立的环节；其二，处理的方式两极化。提取过程不规范的数据，或者整体排除，或者整体采信，缺乏中间的处理方式；其三，技术的门槛较高。法官缺乏技术知识，往往依赖鉴定或者专家意见，而鉴定与专家的适用又有其局限。

本文的基本主张是：鉴真是独立于真实性与合法性的证据能力要件，其对象是证据与来源的同一性，方法是完整的保管链与可验证的技术手段；鉴真包含形式的完整性与实质的可靠性两个层面；鉴真不能的，产生证据能力的瑕疵，而非当然排除；瑕疵可以补正，补正不能且影响实质真实的，予以排除。

电子数据取证不规范时能否作为定案依据、法院如何审查、当事人如何质证，操作层面的规则可参见“电子数据取证不规范，能当认定证据吗”一文的梳理；本文不重复具体的操作步骤，只讨论鉴真的性质、审查的构造与瑕疵的处理。

（一）规范依据的梳理

电子数据的规范，经历了从“视为视听资料”到“独立证据种类”的转变。2012年民事诉讼法将电子数据列为独立的证据种类；此后的司法解释逐步细化了收集、提取、审查的规则。

规范的特点是：刑事领域细于民事领域。刑事电子数据规定对提取、封存、检查、侦查实验等环节作了详细规定；民事证据规定则较为简略，主要通过审查要素的列举，赋予法官裁量的空间。此点，与两类诉讼的性质有关：刑事诉讼涉及人身自由，程序的要求更为严格。

须注意，规范的参照适用。民事案件中，可以参照刑事电子数据规定的技术标准，例如完整性校验值的计算、原始存储介质的封存；但参照不等于照搬，民事案件应当结合其特点，避免过度的形式要求。

（二）与书证认证的比较

书证的认证，关注的是文书的制作人与制作时间；电子数据的鉴真，关注的是数据与来源的同一性。两者在结构上相似，都是先确认来源、再评价内容；但在方法上不同：书证依靠签名、印章、纸张，电子数据依靠校验值、日志、保管链。

须注意，方法的差异带来的难度差异。书证的形式特征直观，法官可以凭经验判断；电子数据的技术特征隐蔽，法官须借助工具或者专家。此点，是电子数据审查的技术门槛。

还须注意，证明责任的差异。书证的真实性，通常由提出方证明；电子数据的鉴真，

同样由提出方证明，但在特定的情形下可以转移，例如对方掌握原始数据而拒不提供。此点，是证明妨碍在电子数据中的运用。

实务中，有的判决直接援引书证的认证规则审查电子数据，忽视了技术特征。此种做法虽然简便，但容易遗漏关键的环节，例如校验值的比对、保管链的审查。正确的做法，是在书证规则的基础上，增加技术的审查。

（三）实务困境的梳理

困境之一，是审查的形式化。多数判决对电子数据的审查，停留于“来源合法、内容真实”的笼统表述，未就提取过程、保管链条、技术手段展开分析；当事人提出的质疑，往往以“不足以推翻”一语带过。

困境之二，是标准的不统一。同样的取证瑕疵，有的法院认定为“严重违反法定程序”，予以排除；有的认定为“轻微瑕疵”，予以采信；有的不作评价，径行采信。标准的不统一，使当事人难以预期。

困境之三，是技术能力的不足。法官普遍缺乏技术知识，难以判断哈希值是否可靠、时间戳是否可信、云端数据是否完整；其结果是，或者依赖鉴定，或者依赖经验，缺乏中间的分析路径。

困境之四，是救济的不平衡。电子数据的持有人往往是大企业或者平台，其掌握技术与资源；普通当事人难以获取、保存、出示电子数据，举证的能力悬殊。此点，是数字鸿沟在证据法上的体现。

二、鉴真的性质

（一）与真实性的区别

鉴真，指证明证据与来源的同一性，即出示的证据确实是其所主张的来源所产生的。真实性，指证据的内容与客观事实相符。两者不同：鉴真解决“是不是这个东西”，真实性解决“这个东西说的是不是真的”。

区分实益在于审查的顺序。先鉴真，后真实；鉴真不能的，无须审查真实。此点，与文书的认证相似：先确认文书的真实性（是否为其所主张的人所作），再审查其内容的证明力。

实务中，两者常被混淆。判决往往直接审查“内容是否真实”，未审查“数据是否来自其所主张的来源”。此种做法跳过了鉴真的环节，使来源不明的数据得以进入事实认定。

（二）与合法性的区别

合法性，指取证的主体、程序、方式符合法律的规定。鉴真，指证据与来源的同一性。两者不同：非法的取证可能仍然是真实的，合法的取证也可能是不可靠的。

区分实益在于后果的不同。非法的证据，依严重程度可能被排除；鉴真不能的证据，依补正的可能决定是否排除。两者的判断标准不同，不能相互替代。

须注意，两者的交叉。以非法方式提取的电子数据，往往同时存在鉴真的困难，因为提取过程缺乏记录，保管链条断裂。此时应当分别审查，先判断合法性，再判断鉴真；不能以合法性的判断替代鉴真的判断。

（三）鉴真与推定

在特定的情形下，电子数据的鉴真可以推定。例如，由公证机关公证提取的数据、由中立第三方存证平台保存的数据、以及由国家机关制作的公文性电子数据，可以推定其鉴真成立；对方有异议的，应当提出反证。

推定的正当性，在于这些数据的保管与提取有第三方的监督，篡改的成本较高、被发现的可能性较大。此点，与公文书证的推定相似。

须注意，推定的可推翻性。推定不是终局，对方提出合理异议并提供线索的，举证方仍须就鉴真举证；不能举证的，推定被推翻。此点，是推定的相对性。

实务中，有的当事人将公证提取的数据视为“绝对真实”，不作任何审查。此种理解不当，因为公证只证明提取的过程，不证明数据的内容真实；内容的真实性，仍须结合其他证据判断。

（四）独立要件的证成

本文主张，鉴真是独立的证据能力要件。其独立性体现在三方面：其一，对象独立，其对象是证据与来源的同一性，而非内容或程序；其二，方法独立，其方法是保管链与技术校验，而非合法性审查；其三，后果独立，其后果是瑕疵的补正或者排除，而非非法证据的排除。

独立的实益在于审查的精细化。将鉴真独立出来，法官便有了明确的分析路径：先查来源，再查内容；先查形式，再查实质；先查瑕疵，再查补正。路径清晰，结论自然可靠。

须注意，鉴真与证据能力的整体关系。鉴真是证据能力的积极要件，即证据须经鉴真才能进入事实认定；真实性与证明力是消极要件与程度问题，即在鉴真之后评价其证明作用。三者的层次不同，不能颠倒。

三、完整性的审查

（一）原始存储介质

原始存储介质，是电子数据首次生成的载体，例如手机、电脑、服务器、存储卡。其审查的要点有三：其一，介质是否被封存，封存的状态是否完整；其二，介质的提取是否有记录，记录是否经当事人确认；其三，介质的内容是否被修改，修改是否有正当理由。

须注意，原始介质的例外。介质不便封存或者封存会影响其正常使用的，可以提取数据后封存数据；但应当制作笔录，说明理由，并由见证人签字。此点，是原则与例外的平衡。

实务中，有的取证人员直接操作原始介质，未作封存，也未记录操作过程。此时数据的完整性难以证明，应当由取证方举证；举证不能的，认定为鉴真不能。此点，是举证责任的分配。

（二）网络在线提取

网络在线提取，是指通过网络远程访问目标系统，提取其中的数据。其特点是：不接触物理介质，数据在传输过程中可能被修改；故其完整性依赖于提取的工具与过程的记录。

须注意，在线提取的记录。应当记录：访问的地址、使用的工具、提取的时间、数据的范围、以及校验值；有条件的，应当全程录像。此点，是在线提取的规范要求。

实务中，有的取证人员使用普通的浏览器下载数据，未记录工具与过程。此时数据的完整性难以证明，因为浏览器可能缓存、转换、或者截断数据。正确的做法，是使用专用的取证工具，并记录工具的名称与版本。

还须注意，境外网站的提取。境外网站的数据可能因网络原因无法完整获取，也可能因服务商的配合而获得后台数据；两种来源的可靠性不同，应当分别审查。此点，是跨境取证的特殊性。

（三）提取笔录

提取笔录，是记录提取过程的法律文书。其内容应当包括：提取的时间、地点、人员、方法、设备、数据的范围与格式、以及当事人的确认。笔录的完整性，是鉴真的基础。

须注意，笔录的形式要求。笔录应当由提取人、见证人、持有人签名；持有人拒绝签名的，应当注明；无见证人的，应当说明理由。形式的欠缺，可能导致鉴真不能。

实务中，有的笔录只写“提取了相关数据”，未写明数据的范围与格式。此种笔录无法证明提取的内容与出示的内容是否一致，鉴真难以完成。正确的做法，是详细记载数据的名称、数量、格式、以及校验值。

（四）完整性校验值

完整性校验值，是通过哈希算法对数据计算得出的固定长度的值。数据被修改，校验值即变化；故校验值是判断数据是否被篡改的技术手段。常用的算法有消息摘要算法与安全散列算法。

须注意，校验值的局限。其一，校验值只能证明数据在计算之后未被修改，不能证明计算之前的状态；其二，校验值相同的两个数据，理论上可能不同（碰撞），但概率极

低；其三，校验值本身也可能被伪造，须有保管链的佐证。

实务中，有的取证人员计算了校验值，但未在笔录中记载，也未随案移送。此时校验值失去了证明作用，因为无法确认其对应的数据。正确的做法，是将校验值记入笔录，并在出示时再次计算比对。

（五）第三方存证平台

第三方存证平台，是为用户提供数据保存、固化的服务机构。其特点是：平台独立于当事人，具有一定的中立性；但其资质、技术、管理的水准参差不齐，不能一概推定可靠。

须注意，平台资质的审查。应当审查：平台是否具备相应的资质、其技术方案是否可靠、其数据是否可验证、以及其是否与当事人存在利害关系。资质的欠缺，可能影响存证的可信度。

实务中，有的平台仅提供“时间戳”服务，未保存原始数据。此时时间戳只能证明某一时刻存在某个哈希值，不能证明数据的内容；故其证明力有限，应当结合原始数据审查。

还须注意，平台的退出风险。平台停止运营的，其保存的数据可能无法访问；此时应当审查平台是否提供了数据的导出与验证方案。此点，是存证服务的可持续性问题。

（六）保管链

保管链，是记录证据从提取到出示的全过程链条。其内容包括：每一次移交的时间、地点、人员、方式、以及证据的状态。链条完整，才能证明证据未被替换或者篡改。

须注意，链条的断裂。链条中断的，例如某一环节无移交记录、保管人变更未记录、保管条件不明，鉴真即出现瑕疵。瑕疵是否影响证据能力，取决于断裂的环节是否关键、是否有其他证据佐证。

实务中，有的电子数据由一方当事人自行保存，未经第三方保管。此时保管链的可靠性较低，应当结合其他证据审查；对方提出异议的，保存方应当就保管的条件与过程举证。此点，是自助保存的证明难题。

四、真实性的审查

（一）内容的真实性

内容的真实性，指数据所记载的信息与客观事实相符。其审查的要点有三：其一，数据的内容是否完整，有无删改；其二，数据的上下文是否连贯，有无断章取义；其三，数据与其他证据是否印证。

须注意，截图的局限。截图只呈现数据的一部分，未呈现上下文；且截图易于伪造。故仅有截图的，应当要求提供原始载体或者完整的记录；不能提供的，截图的证明力较

低。

实务中，有的当事人仅提供聊天记录的截图，未提供原始载体。此时应当审查截图的内容是否连贯、双方的身份证是否可识别、以及是否有其他证据佐证；综合判断后，决定其证明力。此点，是自由心证的运用。

（二）深度伪造的挑战

深度伪造，是利用人工智能技术生成的、难以辨别的虚假音视频或者图像。其出现，使“眼见为实”的经验失效，也使电子数据的鉴真面临新的挑战。

须注意，识别的困难。深度伪造的内容在视觉与听觉上高度逼真，普通人难以识别；即使专业人员，也须借助技术工具。故对存疑的音视频，应当委托专业机构鉴定，而非凭经验判断。

本文主张，面对深度伪造，应当强化源头审查：其一，审查数据的生成设备与软件，是否有合成的痕迹；其二，审查数据的元数据，是否有异常；其三，审查数据的传播链条，是否有合理的来源。三者的结合，可以提高识别的准确性。

实务中，有的当事人以“可能是深度伪造”为由，否定一切不利的音视频。此种主张缺乏依据，因为怀疑不等于证明；其应当提供具体的线索或者申请鉴定。此点，是异议的具体性要求。

（三）生成过程的可靠性

生成过程的可靠性，指数据在生成时未受干扰，其内容能够反映真实情况。其审查的要点有三：其一，生成系统的可靠性，即系统是否正常运行、有无故障或者异常；其二，操作人员的资质与操作规范；其三，数据的内部一致性，即各字段之间是否矛盾。

须注意，系统的可靠性难以直接证明。此时可以借助系统的日志、第三方的认证、以及行业的惯例；必要时可以申请鉴定。此点，是技术问题与法律问题的交界。

实务中，有的电子数据来自自动化的系统，例如门禁记录、交易系统日志。此类数据的可靠性较高，因为系统自动生成，人为干预的空间小；但仍须审查系统的运行状态与数据的完整性。

（四）与其他证据的印证

电子数据往往不是孤立的，其与其他证据的印证，是判断真实性的方法。印证的方式包括：与书证的印证、与证人证言的印证、与当事人陈述的印证、以及电子数据之间的相互印证。

须注意，印证的限度。印证只能提高证明力，不能替代鉴真；来源不明的数据，即使内容与其他证据吻合，也不能径行采信，因为其可能是伪造的。此点，是鉴真优先的原则。

实务中，有的判决以“与其他证据吻合”为由，回避鉴真的审查。此种做法混淆了证

据能力与证明力：前者是入口，后者是权重；入口未通过，权重无从谈起。

五、举证与质证

（一）举证责任

电子数据的举证责任，依主张者举证的原则分配。提出电子数据的一方，应当证明其来源、提取过程、保管链条；对方提出异议的，应当说明理由；有合理理由的，举证方应当进一步说明或者补充证据。

须注意，举证的程度。举证方无须证明数据的绝对真实，只须证明其来源可靠、过程完整、内容未被篡改；达到高度可能性的，即为已足。此点，与民事证明标准一致。

实务中，有的法院要求举证方提供“原始载体、提取笔录、校验值、保管链”四项俱全，缺一不可。此种要求过高，因为并非所有的电子数据都有完整的记录；正确的做法，是结合数据的重要性、异议的理由、以及补正的可能，综合判断。

（二）当事人的获取能力

电子数据往往由一方或者第三方掌握，普通当事人难以获取。例如，平台的交易记录、通讯的后台数据、企业的系统日志，均非当事人可以自行取得。获取能力的悬殊，影响了举证的可能。

缓和的方法有三。其一，申请法院调查收集；其二，申请证据保全；其三，申请责令对方提交。三种方法，均有其条件与限度，应当根据具体情况选择。

须注意，责令提交的适用。对方掌握证据而拒不提交的，法院可以推定申请方的主张成立；但申请方应当证明对方掌握该证据，且该证据对证明事实有必要。此点，是证明妨碍的构成。

实务中，有的法院对调查收集的申请一律不予准许，理由是“当事人应当自行举证”。此种做法忽视了电子数据的特殊性，可能使弱势方无法举证。正确的做法，是审查申请的必要性与可行性，必要的应当准许。

（三）专家辅助人

专家辅助人，是当事人申请出庭、就专门性问题提出意见的人。其作用在于弥补当事人与法官的技术知识不足，帮助质证与认证。民事诉讼法第八十二条规定，当事人可以申请人民法院通知有专门知识的人出庭，就鉴定人作出的鉴定意见或者专业问题提出意见。

须注意，专家辅助人意见的性质。其不是鉴定意见，不具有法定的证据形式；但其可以作为法官判断的参考，也可以作为质证的依据。此点，是与鉴定意见的区别。

实务中，有的当事人申请专家辅助人出庭，法院以“无必要”为由不予准许。此种做法限制了当事人的质证权，应当纠正。正确的做法，是审查申请的理由；理由正当的，应当准许。

（四）鉴定的适用

电子数据的鉴定，包括真实性鉴定、同一性鉴定、以及恢复鉴定。鉴定的启动，依当事人的申请或者法院的依职权决定；鉴定的事项，应当具体明确，避免笼统的“是否真实”。

须注意，鉴定的局限。鉴定只能就技术问题作出判断，不能就法律问题作出判断；鉴定的结论，仍须经法庭质证，法官可以结合其他证据决定是否采信。此点，是鉴定意见的证据地位。

实务中，有的法院将鉴定意见作为“铁证”，不加审查即予采信。此种做法放弃了法官的认证职责，不符合证据规则。正确的做法，是审查鉴定的资质、方法、过程、以及结论的合理性。

六、瑕疵与补正

（一）技术与法律的衔接

电子数据的审查，是技术问题与法律问题的交织。技术解决“数据是否被修改”，法律解决“修改是否影响证据能力”。两者的分工，应当清晰：技术判断由专家完成，法律判断由法官完成。

须注意，法官的职责。法官不必掌握技术的细节，但须理解技术的意义：校验值的作用、保管链的价值、以及系统日志的证明力。理解意义，才能正确地评价专家的意见。

实务中，有的法官将技术问题完全交给鉴定，自己不作品断。此种做法放弃了认证的职责；正确的做法，是审查鉴定的方法是否可靠、结论是否合理、以及是否与其他证据吻合。此点，是法官的技术素养要求。

（二）取证主体与见证

取证的主体，包括行政机关、公证机关、以及当事人的代理人。不同主体的取证，其可靠性不同：行政机关的取证有公权力的保障，公证机关的取证有中立的监督，代理人的取证则依赖其自律。

须注意，见证人的作用。见证人应当与案件无利害关系，其作用是监督取证的过程；见证人的签名，是取证合法性的证明。无见证人的，应当说明理由。

实务中，有的取证由一方当事人的员工见证，其与案件有利害关系。此时见证的效力存疑，应当结合其他证据审查。此点，是见证人资格的审查。

（三）瑕疵的类型

电子数据的瑕疵，可以分为三类：其一，形式的瑕疵，例如笔录未签名、封存不规范；其二，程序的瑕疵，例如未通知当事人到场、未制作清单；其三，技术的瑕疵，例如未计算校验值、未记录系统的状态。

须注意，三类瑕疵的可补正性不同。形式的瑕疵，一般可以补正；程序的瑕疵，视其对当事人权利的影响决定；技术的瑕疵，若数据已被修改或者丢失，往往无法补正。

实务中，有的法院对所有的瑕疵一概不予补正，径行排除。此种做法过于严苛，与证据规则的弹性不符。正确的做法，是区分瑕疵的类型，分别处理。

（四）补正的可能

补正，指通过补充证据或者重新取证，消除瑕疵。补正的可能，取决于三个因素：其一，瑕疵是否可以通过其他证据弥补；其二，补正是否损害当事人的质证权；其三，补正的成本是否合理。

须注意，补正的限度。补正不得改变证据的内容，也不得替代原件；以重新制作的“数据”替代原数据，不属于补正，而是新的证据。此点，是补正与造假的界限。

实务中，有的取证方在诉讼中重新提取数据，主张“补正”。此种做法是否准许，应当审查：原数据是否仍然存在、重新提取的条件是否相同、以及是否损害对方的质证权。三个条件具备的，可以准许。

（五）排除的后果

鉴真不能且无法补正的，电子数据应当排除。排除的后果，是该数据不得作为认定事实的根据；但排除不影响其他证据的效力，也不影响当事人以其他方式证明同一事实。

须注意，排除的范围。排除应当限于有瑕疵的部分，不及其余；同一载体中的其他数据，若鉴真无疑，仍可以采用。此点，是部分排除的原则。

实务中，有的法院因一份数据的瑕疵，将整批数据一概排除。此种做法过度，损害了证据的完整性。正确的做法，是分别审查各部分的数据，仅排除有瑕疵的部分。

七、类型化的展开

（一）即时通讯记录

即时通讯记录，包括微信、短信、其他通讯应用的聊天记录。其特点是：数据存储于双方的终端与平台服务器，易于删除与伪造；其审查的重点，是账号的归属、内容的完整、以及上下文的连贯。

须注意，账号归属的证明。仅有聊天记录的截图，不能证明对方的身份；应当结合实名信息、绑定的手机号、以及交易的习惯综合判断。此点，是主体识别的难点。

实务中，有的当事人使用他人的账号或者伪造账号，制造虚假的聊天记录。审查时应当注意：账号的注册时间、聊天的习惯用语、以及是否有其他证据佐证；必要时可以申请平台提供后台数据。

（二）电子签名与时间戳

电子签名，是用于识别签名人身份并表明其认可内容的数字。可靠的电子签名，与手写签名或者盖章具有同等的法律效力；其可靠性，取决于签名制作数据的专有性、签署后的改动可被发现等条件。

须注意，电子签名的验证。验证的内容包括：签名人的身份、签名的时间、以及签名后文档是否被修改。验证的方法，依签名技术的不同而异；有资质的机构可以出具验证报告。

时间戳，是由时间戳服务机构签发的、证明某一时刻数据存在的凭证。其作用是固定数据的时间，防止事后倒签。时间戳的可靠性，取决于服务机构的中立性与技术的安全性。

实务中，有的当事人以“有电子签名”为由，主张文档无须审查。此种主张不当，因为电子签名只解决签名与完整性的问题，不解决内容真实的问题；内容的真实性，仍须结合其他证据判断。

（三）电子邮件

电子邮件的特点是：有较为完整的元数据，包括发件人、收件人、时间、服务器路径；其真实性相对易于证明。审查的重点，是邮件头的完整、服务器的日志、以及附件的完整性。

须注意，邮件地址的冒用。发件人的地址可以被伪造，故不能仅凭地址认定发件人；应当结合邮件的内容、双方的往来习惯、以及服务器的认证记录综合判断。

（四）电子交易记录

电子交易记录，是平台或者系统自动生成的交易数据，包括订单、支付、物流等信息。其特点是：由系统自动生成，人为干预的空间小；但平台的系统可能出错，记录也可能被修改。

审查的重点，是记录的完整与系统的可靠。完整的记录，应当包括交易的全部环节；可靠的系统，应当有日志、备份、以及异常监测。此点，与自动化生成的数据的审查一致。

实务中，有的平台仅提供交易的摘要，未提供明细。此时应当要求平台提供完整的记录；不能提供的，摘要的证明力较低。此点，是记录完整性的要求。

（五）云端数据

云端数据，存储于第三方的服务器，用户通过账号访问。其特点是：用户不掌握物理介质，数据的完整性依赖服务商；取证须通过服务商的配合或者公证。

须注意，云数据的保管链。取证的环节包括：账号的登录、数据的下载、以及下载后的保管；每一环节都应当有记录，并由公证员或者见证人监督。此点，是云取证的关键。

实务中，有的当事人自行登录云端下载数据，未作公证。此时数据的完整性难以证明，对方提出异议的，应当由服务商提供后台记录或者申请公证。

（六）区块链存证

区块链存证，是将数据的哈希值上链，利用区块链的不可篡改性证明数据的存在与完整。其特点是：上链后的数据难以篡改，但上链前的数据仍可能被伪造。

须注意，存证的效力。区块链存证只能证明“上链时的数据是某个值”，不能证明“上链时的数据是真实的”；故其证明力限于完整性，不及于真实性。此点，是技术的中立性。

实务中，有的当事人将区块链存证作为“铁证”，主张无须审查。此种主张不能成立，因为存证只解决完整性问题；数据的来源、生成过程、以及内容的真实性，仍须审查。

（七）类案的统一

电子数据的裁判尺度，各地差异明显。同样的取证瑕疵，有的法院排除，有的采信；同样的存证，有的法院认可，有的质疑。差异的根源，在于鉴真的标准不统一。

统一的方向，是统一要件、统一方法、统一后果。要件上，明确鉴真的独立性；方法上，确立以保管链为核心的审查框架；后果上，区分瑕疵的类型与补正的可能。三者统一，结论自然趋同。

最高人民法院可以通过发布典型案例，明确若干争点：截图的证明力；保管链断裂的后果；第三方存证的可信度；深度伪造的识别。规则明确，才能减少争议。

还须强调说理的完整。采信电子数据的判决，应当说明来源的可靠、过程的完整、内容的可信；排除的判决，应当说明瑕疵的具体情形、补正的不可能、以及对实质真实的影响。仅以“真实性存疑”一语带过，难以服人。

从更长的时段看，电子数据的审查，正在从“经验判断”走向“规则审查”。这一转向，与证据法整体的发展趋势一致：从自由心证的单极，走向规则约束与自由心证的结合。鉴真规则的建立，正是这一转向的体现。

需要补充的是，规则的落地依赖技术的普及。取证工具的标准化、审查指引的细化、以及法官的技术培训，都是制度运行的基础。技术的门槛不能成为正义的障碍；唯有降低门槛，才能使电子数据的审查既准确又公平。

还有一点须提及：电子数据的审查，应当兼顾效率。技术审查的成本较高，若对每一份数据都要求完整的保管链与校验值，将使诉讼难以为继。故应当根据数据的重要性、争议的程度、以及金额的大小，确定审查的强度。此点，是比例原则在证据审查中的运用。

对简单的案件，可以采用简化的审查：核对数据的来源、内容的连贯、以及对方的认可；对复杂的案件，则应当采用完整的审查：保管链、校验值、系统日志、专家意见。分

级审查，既能保障准确，又能兼顾效率；反之，若不分轻重一律苛求，则形式完备而实质拖延，正义反而迟到。

最后须指出，鉴真的最终目的，是使事实认定建立在可靠的基础之上。技术只是手段，可靠才是目的；脱离目的的技术追求，不过是新的形式主义，于事实认定无所增益。

八、结语

电子数据的鉴真，可以概括为三句话：性质上，是独立的证据能力要件，区别于真实性与合法性；构造上，包含形式的完整性与实质的可靠性两个层面；后果上，鉴真不能产生瑕疵，瑕疵可以补正，补正不能且影响实质真实的，予以排除。

本文的三个主张，都围绕“鉴真”展开。性质解决定位的问题，构造解决审查的问题，后果解决处理的问题。三者依次展开，电子数据的审查便从形式的罗列，变为可操作的作业。

对裁判者而言，这一框架的实益是使审理有了顺序：先审查来源与提取；再审查保管链；再审查校验值；再审查内容的完整；再审查生成过程的可靠；最后决定采信与否。六步依次展开，结论自然清晰。

最后须指出，鉴真规则的完善，不能仅靠个案的裁判。取证规范的统一、技术标准的制定、以及跨部门的数据共享，都是制度运行的基础。司法的功能，在于为这些制度提供审查的框架；框架的清晰，才能使电子数据真正成为可靠的事实基础。

参考文献

- [1] 《中华人民共和国民事诉讼法》（2023年修正）第六十六条、第八十二条。
- [2] 《最高人民法院关于民事诉讼证据的若干规定》（法释〔2019〕19号）第十四条、第十五条、第九十三条、第九十四条。
- [3] 《最高人民法院、最高人民检察院、公安部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》（法发〔2016〕22号）。
- [4] 《人民法院在线诉讼规则》（法释〔2021〕12号）第十六条至第十九条。
- [5] 刘品新：《电子数据的鉴真问题》，《法学研究》2021年第5期。
- [6] 谢登科：《电子数据完整性的审查》，《中国法学》2022年第3期。
- [7] 褚福民：《区块链存证的证据法地位》，《政法论坛》2023年第2期。