第 3 章

电子数据的法律规则和标准体系

本章学习目标

- 英美法系的电子数据法律规则
- 大陆法系(我国)的电子数据法律规则
- 我国关于电子数据的相关立法
- 公安部门对电子数据取证程序的相关规定
- 电子数据与其他证据的区别
- 电子数据审查
- 国际电子数据取证的标准体系
- 我国电子数据取证的标准体系

电子数据对各国法律体系来说是个新生事物。近年来,各国根据实际情况出台了符合本国国情的关于电子数据的法律法规。这些法律法规是电子数据取证的根本依据。标准是法律的有力补充,标准具备很强的操作性,是电子数据取证具体工作的主要依据。电子数据取证要求取证人员既了解国内外关于电子数据的法律法规,又能熟悉现有国际及国内相关取证标准及取证指南,在工作中参照使用。

3.1 电子数据的法律规则

电子数据的类型和特点决定了其作为证据用于法庭展示的特殊性。电子数据需要将虚拟内容以物理形式展现给法庭。这就涉及电子数据的可视化。由于对电子数据这一证据本质的不了解,电子数据在司法实践中可能以勘验笔录、鉴定意见等形式出现,甚至可能以书证的形式出现。但是从未来发展和法律实践中看,电子数据应当作为独立的证据类型进行认定。

3.1.1 英美法系

英美法系并没有单独的电子数据法律法规。在以前的司法实践中,电子数据可能以其他证据形式,例如书证、传闻证据出现。英美法系的特点:一是证据规则数量多;二是相关判例多。这些证据规则和判例是英美法系证据制度的有机组成部分。网络犯罪的冲击使得英美法系国家纷纷进行证据法的相关修正、解释,或者进行新的立法。

美国没有统一的电子数据的相关法律。与电子数据相关的法律规定散见在证据法和其他相关法律中。就证据法而言，美国表现出成文法与判例法并存、联邦法与州法并存的特点。美国最重要的成文证据法典是《联邦证据规则》和《统一证据规则》，前者适用于联邦法庭、后者适用于各州。美国的证据规则，虽然没有单独的提出“电子数据”这一概念，但是在坚持“原件”原则的同时，通过增加例外条款，解决了电子数据作为证据使用的最后障碍。

美国通过一系列的法律来补充加强电子数据的使用，例如《计算机欺诈和滥用法》(Computer Fraud and Abuse Act)、《爱国者法》(Patriot Act)。同时州法也根据实际情况制定了关于电子数据的相关法律。例如，美国加利福尼亚州 2009 年颁布了《电子证据开示法》。

英国《警察与刑事证据法》(1984)规定：警察可以把存贮在计算机中的信息作为证据。《民事证据法》(1968)规定：证人可以通过音像媒体或者其他形式向法院提供证据。

加拿大 1998 年颁布了《统一电子证据法》(Uniform Electronic Evidence Act)，直接以电子记录(Electronic Record)和电子记录系统来界定电子数据，对电子数据的定义、适用范围作了具体的规定。2000 年加拿大证据法(Evidence Act of Canada)的修订第 31 节基本上全面吸收了《统一电子证据法》的内容。作为英美法系的重要分支，加拿大对“原件”进行概念的外延直接确定了电子数据的证据地位。除此之外，加拿大爱德华王子岛省[①]和育空省[②]都制定了相关的电子数据的本地法律。

英美法系最大的特色就是对程序的重视，如“正当程序”之类的概念就是起源于英美法系。总体上说，英美法系证据规则繁多，且内容比较复杂、具体。因此，即使成熟的英美法系，在电子数据作为证据进入到法律过程中，也遇到了一些现实的困难。这些困难主要包括证据的认定和证据有效性。电子数据在英美法系中主要面临以下证据规则的挑战。

1. 最佳证据规则

在英美法系，最佳证据规则(Best Evidence Rule)指的是“对于文书并以此证明案件真实情况的证据，证据法上要求通常必须出示原件，只有没有理由怀疑副本准确性的情况下，才可以作为例外不出示原件，出示副本”。这一规则就是著名的“最佳证据规则”(Best Evidence Rule)，有时候亦被称为“原本法则”(Original Document Rule)。最佳证据规则是一项非常古老的制度，并且在英美法系享有较高的地位。按照英美法系的最佳证据规则，只有文件的原件(Original)，才能作为证据被采纳。美国联邦证据规则原先规定，要证明文书的内容有必要提出文书的原件。加拿大证据法有关最佳证据规则也要求提供原件。

如果坚持须以原件才能作为证据，电子数据就会遇到难以克服的困难。因为计算机输出的书面材料很难说是原件，并不能做到表面内容和隐含内容与书证一致。按照上述最佳证据规则的要求，这种由计算机输出的资料是不能被采纳为证据的。

---

① 加拿大爱德华王子岛省《电子证据法》(2001)。

② 加拿大育空省《电子证据法》(2002)。

2. 传闻规则

传闻规则(Hearsay Rule)是英美法所特有的证据规则。所谓传闻是指证人在法庭内重述另一人以口头、文书或者其他方式所做的陈述。传闻规则规定“除了法律明文规定的例外情况,传闻证据原则上不具有可采纳性,不得提交法庭调查质证,已经在法庭出示的,不得提交陪审员”。这项原则应用于计算机便会遇到难以解决的问题,因为电子记录的产生过程不同于人的语言形成过程,电子记录系统本身无法对电子记录的产生为进行证明。电子记录通过计算机来传输和处理时,信息内容和状态很容易发生改变,而又不能对计算机进行交叉询问,因此,英美的传统理论和判例认为,由计算机输出的书面材料只是一种传闻证据,原则上是不能被采纳为证据的。

美国的最佳证据规则和传闻规则显然对电子数据的可采性产生了很多障碍。法官利用美国独特的“自由心证”制度在很多案件中巧妙、适当地避开了最佳证据规则和传闻规则对电子数据的限制。如在 1992 年的 Doe v. United States 案件中,原告起诉美国政府管辖的军事医院在给他输血的过程中,由于医院的不负责任使他感染了艾滋病病毒。美国政府提供的一份证据是从陆军航空队电子数据库打印出来的文书记录。原告认为这份证据有违最佳证据规则和传闻规则。法官向政府提出证实打印文书真实性的要求,随后政府补交了程序性证明资料,被法官采纳,并据此认定该文书是计算机数据的准确打印物。法官认为“这虽与典型的最佳证据规则不相符,但是也不构成对该规则的违反。”

随着对于电子数据的逐步认可,电子数据作为证据的单独认定显得非常有必要。而且由于电子数据的特性,对其进行逐比特位的复制(Duplicate)形成的复制件,与原件并无二致。因此美国《联邦证据规则[①]》2015 版(Federal Rules of Evidence 2015)对证据进行了重新界定,其中 101 条规定,证据的范围包括“任何形式的书面材料或其他介质包括以电子形式存储的信息”。第 1001 条规定,“对于电子形式存储的信息,原始性意味着能够精确反映原始信息的打印输出以及其他可视化输出”;“副本意味着机械、图片、化学、电子和其他等同过程或技术的与原件完全一致”。第 1003 条规定了“副本”的法律效力,“在排除对原件有效性的质疑或者环境会对复制件造成影响的例外,副本与原件效力一致”。这就使得电子数据可以作为证据使用。英国也同期废止了传闻规则[②],同时在最佳证据原则中增加了例外条款。

3.1.2　大陆法系

大陆法系的证据法分为两种类型:一种是允许自行提出证据,德国、日本等国属于这种类型,这些国家,原则上可以提出任何证据,但是法院衡量采纳;另一种是明文规定证据的类型,例如中国。对于允许自行提出证据的国家,电子数据作为证据是毫无疑问的。对于明

① http://federalevidence.com/downloads/rules.of.evidence.pdf

② 1995 年制定的《民事证据法》取消传闻规则,第一条规定“在民事诉讼中,不得因为证据是传闻而予以排除”。

文规定证据的国家，如果电子数据不包含在证据类型中，就涉及证据转化和可采性的问题。但是，无论哪种证据法形式，都面临着电子数据的证明力和审查原则的问题。一般来说，大陆法系国家倾向提交证据“原件”，而电子数据的虚拟性很难提供原件。如果证据法只承认原件作为证据，复制件不作为证据，电子数据的证据效力将大打折扣。

我国属于大陆法系，并不存在英美判例法国家由判例中长期以来形成的例如“最优证据规则”与“传闻规则”的束缚，长期没有在证据类型中设立“电子数据”，但是某些立法却借鉴了英美法系的“最优证据规则”，给电子数据作为证据使用造成一定的障碍。例如 2012 年以前，最高人民法院在《关于执行〈中华人民共和国刑事诉讼法〉若干问题的解释》规定“收集、调取的书证应当是原件”和“收集、调取的物证应当是原物”。这实际将电子数据书证化和物证化，或者归于视听资料中，阻碍了电子数据作为证据在侦查、诉讼中的使用。将电子数据归于其他证据中，不但会有“原件与副本”、“直接证据与间接证据”、“文书化与虚拟化”等方面冲突，而且也不利于电子数据作为证据在司法诉讼中的应用。

随着《中华人民共和国刑事诉讼法》、《中华人民共和国民事诉讼法》和《中华人民共和国行政诉讼法》的改版。《中华人民共和国刑事诉讼法》第四十八条第八款、《中华人民共和国行政诉讼法》第三十三条、《中华人民共和国民事诉讼法》第六十三条第五款均规定“电子数据”作为证据类型之一。从而以三大法明文规定的形式确定了“电子数据”的法律证据地位。

3.2 我国关于电子数据的相关立法

随着我国信息安全意识的提高和司法进步，国家出台了一系列的涉及电子数据的法律法规。这些法律法规为打击网络犯罪，维护国家安全和公民权益提供了重要的法律支持。

3.2.1 法律

1.《中华人民共和国刑事诉讼法》第四十八条：可以用于证明案件事实的材料，都是证据。

证据包括：

（一）物证；

（二）书证；

（三）证人证言；

（四）被害人陈述；

（五）犯罪嫌疑人、被告人供述和辩解；

（六）鉴定意见；

（七）勘验、检查、辨认、侦查实验等笔录；

（八）视听资料、电子数据。

证据必须经过查证属实，才能作为定案的根据。

2.《中华人民共和国行政诉讼法》第三十三条证据包括：

（一）书证；

（二）物证；

（三）视听资料；

（四）电子数据；

（五）证人证言；

（六）当事人的陈述；

（七）鉴定意见；

（八）勘验笔录、现场笔录。

以上证据经法庭审查属实，才能作为认定案件事实的根据。

3.《中华人民共和国民事诉讼法》第六十三条证据包括：

（一）当事人的陈述；

（二）书证；

（三）物证；

（四）视听资料；

（五）电子数据；

（六）证人证言；

（七）鉴定意见；

（八）勘验笔录。

证据必须查证属实，才能作为认定事实的根据。

3.2.2　司法解释

最高人民法院制定并发布的司法解释，具有法律效力。最高人民法院进行司法解释的依据是全国人民代表大会常务委员会于 1981 年 6 月 10 日做出的《关于加强法律解释工作的决议》，该决议规定："凡关于法律、法令条文本身需要进一步明确界限或作补充规定的，由全国人民代表大会常务委员会进行解释或用法令加以规定。凡属于法院审判工作中具体应用法律、法令的问题，由最高人民法院进行解释。凡属于检察院检察工作中具体应用法律、法令的问题，由最高人民检察院进行解释。"基于该决议，最高人民法院于 1997 年发布了法发(1997)15 号《关于司法解释工作的若干规定》(以下简称《若干规定》)，进一步明确了司法解释的性质、效力、分类和程序。关于电子数据的司法解释主要有以下部分：

- 最高人民法院《关于审理非法出版物刊刑事案件具体应用法律若干问题的解释》(1998 年 12 月 17 日，法释[1998]30 号)，简称《非法出版物犯罪解释》。
- 最高人民法院《关于审理走私刑事案件具体应用法律若干问题的解释》(2000 年 9 月 26 日，法释[2000]30 号)，简称《走私犯罪解释》。
- 最高人民法院、最高人民检察院《关于办理利用互联网、移动通讯终端、声讯台制作、

复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》(2004年9月3日,法释[2004]11号),简称《淫秽电子信息犯罪解释》。

- 最高人民法院、最高人民检察院《关于办理妨害信用卡管理刑事案件具体应用法律若干问题的解释》(2009年12月3日,法释[2009]19号),简称《妨害信用卡管理犯罪解释》。
- 最高人民法院、最高人民检察院《关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)》(2010年2月2日,法释[2010]3号),简称《淫秽电子信息犯罪解释(二)》。
- 最高人民法院、最高人民检察院《关于办理诈骗刑事案件具体应用法律若干问题的解释》(2011年3月1日,法释[2011]7号),简称《诈骗罪解释》。
- 最高人民法院、最高人民检察院《关于办理危害计算机信息系统安全刑事案件具体应用法律若干问题的解释》(2011年8月1日,法释[2011]19号),简称《危害计算机信息系统安全犯罪解释》。
- 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》(2012年12月20日,法释[2012]21号),简称《刑事诉讼法解释》。
- 最高人民法院、最高人民检察院《关于办理盗窃刑事案件具体应用法律若干问题的解释》(2013年4月2日,法释[2013]8号),简称《盗窃罪解释》。

3.2.3 规范性文件

- 最高人民法院、最高人民检察院、公安部、国家安全部、司法部《关于办理死刑案件审查判断证据若干问题的规定》(2010年6月13日,法发[2010]20号),简称《证据审查判断规定》。
- 最高人民法院、最高人民检察院、公安部、国家安全部、司法部《关于办理刑事案件排除非法证据若干问题的规定》(2010年6月13日,法发[2010]20号),简称《非法证据排除规定》。
- 最高人民法院、最高人民检察院、公安部《关于办理网络赌博犯罪案件适用法律若干问题的意见》(2010年9月15日,公通字[2010]40号),简称《网络赌博犯罪意见》。
- 《关于办理流动性团伙性跨区域性犯罪案件有关问题的意见》(公通字[2011]14号)(2011年1月1日,公通字[2011]14号),简称《流动性团伙性跨区域性犯罪意见》。
- 最高人民法院、最高人民检察院、公安部《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》(2011年1月10日,法发[2011]3号),简称《侵犯知识产权犯罪意见》。
- 最高人民法院、最高人民检察院、公安部《关于依法惩处侵害公民个人信息犯罪活动的通知》(2013年4月23日,公通字[2013]12号),简称《惩处侵害公民个人信息犯罪通知》。

- 最高人民法院、最高人民检察院、公安部《关于办理组织领导传销活动刑事案件适用法律若干问题的意见》(2013 年 11 月 11 日,公通字[2013]37 号),简称《组织领导传销活动刑事案件意见》。
- 最高人民法院、最高人民检察院、公安部《关于办理非法集资刑事案件适用法律若干问题的意见》(2014 年 3 月 25 日,公通字[2014]16 号),简称《非法集资刑事案件意见》。
- 最高人民法院、最高人民检察院、公安部《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》(2014 年 5 月 4 日,公通字[2014]10 号),简称《网络犯罪刑事诉讼程序意见》。

3.3　部门和行业对于电子数据的相关规定

- 最高人民检察院《人民检察院电子证据鉴定程序规则(试行)》(2009 年 4 月)。
- 国家工商总局《关于工商行政管理机关电子数据证据取证工作的指导意见》(工商市字[2011]248 号)。
- 国家税务总局关于贯彻《中华人民共和国税收征收管理法》及其实施细则若干具体问题的通知(国税发[2003]47 号)。
- 《海关稽查操作规程》(署调发 2003[142]号)。
- 《中华律师协会律师办理电子数据证据业务操作指引》。

3.4　电子数据与其他证据的区别

长期以来,由于电子数据没有成为独立的证据类型。电子数据被视为 1996 年刑事诉讼法七类证据的电子数据化,因此在司法实践中电子数据往往向其他证据类型转化使用,甚至被混淆。2013 年刑事诉讼法将电子数据列为证据类型之一,符合信息社会的发展趋势和司法进步。如果现在还将电子数据转化为其他证据使用,既不利于电子数据的司法实践,也不利于国家的法制进步和公平正义。因此有必要区分电子数据与其他证据类型的区别和联系。

3.4.1　电子数据与视听资料的区别

视听资料是指以“以录音磁带、录像带、光盘、电影胶片或其他设备存储的作为证明案件事实的音像、影像和图形”,又称为“声像资料”。传统理论有一种观点认为电子数据应当归于视听资料中。因为在数字化时代,模拟形式的视听资料已经逐渐被数字形式的视听资料所取代。同时数字形式的视听资料与电子数据在存在形式上类似,存储的视听资料和电子数据均需要一定的工具和手段转化为其他形式后为人们直接感知。二者的正本与副本均一

致。1996 年刑事诉讼法中只规定了“视听资料”作为证据类型，并未规定“电子数据”，因此很长一段时间内，“电子数据”是被视为“视听资料”来作为证据使用的。

但是电子数据与视听资料二者是有着本质区别的。一是电子数据范围更广，不但包含了视听资料的一部分，还涵盖网络数据、文本数据等诸多范围。二是视听资料一般是进行真实性鉴定，使用的方法手段与电子数据有较大区别。例如声纹鉴定，是将录音回放或者分析来确定真伪，电子数据鉴定则针对声音的元数据进行分析。根据最高人民法院关于适用《中华人民共和国民事诉讼法》的解释第一百一十六条规定“视听资料包括录音资料和影像资料……存储在电子介质中的录音资料和影像资料，适用电子数据的规定。”不但将视听资料与电子数据分离，而且还规定了电子数据适用的范围。

3.4.2 电子数据与物证的区别

物证是指“外部特征、物质属性和存在情况等能够证明案件真实情况的物品和痕迹”。物证因其客观存在的大小、数量、颜色、新旧等外部特征具有可靠性；因其质量、重量、材料、成分、结构等物质属性具有较强的稳定性；因其存在的空间、时间等物质的存在方式证明案件事实。电子数据与物证是截然不同的两种证据形式。这是因为：

(1) 从特点上看，传统物证具备物质属性，包括法医物证、微量物证、文书物证等。他们的存在形式都是有形的，是物理存在的。但是电子数据是使用“0、1”的数字形式存储的，看不见、摸不到，不能等同于以外观形式分类的传统物证。“电子物证”是相对传统物证提出来的一个概念，广泛为刑侦部门采用。过多使用这个称呼，会导致执法人员对其概念的理解错误，不能理解其本质意义。

(2) 从法律规定上看，根据《中华人民共和国刑事诉讼法》、《中华人民共和国民事诉讼法》、《中华人民共和国行政诉讼法》，物证与电子数据是两种不同形式的证据，不能混为一谈；最高人民法院在《关于执行〈中华人民共和国刑事诉讼法〉若干问题的解释》第七十条规定“收集、调取的物证应当是原物”，而电子数据规定允许提取复制。这就从实质上证明电子数据和传统物证是两种不同的证据形式，在取证中也需要根据各自特点进行有针对性的工作。

3.4.3 电子数据与书证的区别

书证是“以文字、符号、图画等记载的内容和表达的思想来证明案件事实的书面或其他形式的文件”。任何书证，举要借助一定的物质材料而存在，例如纸张、布帛、竹木等。

电子数据由于其虚拟性，可以通过专用设备予以呈现，或者以勘验笔录或者鉴定意见呈现其关联性。实践中，也往往以书证的形式出现，这分为两种可能，一种可能是数据在认可范围内打印输出，一种是将电子数据转化为书证，侦查人员为了能够快速固定证据，将电子数据打印出来让嫌疑人签字。认为电子数据作为书证的观点，是借鉴英美法系相关法律的基础上得来的。但是作为大陆法系国家，我国已经从法律层面上规定了电子数据是单独的

证据类型。而且从电子数据的本质来看，其与书证有着截然不同的特点和取证方法，应当是单独的证据形式。

（1）存在形式上，书证是物理展示，电子数据是虚拟存在。书证具有物质性，一般为纸张，也有其他形态，其内容明确，形式固定，稳定性较强。电子数据因其虚拟特点，输出的硬拷贝往往不能体现其所有的内容。例如，对于 Word 电子文档，电子数据的分析不但要分析内容，还要分析其元数据，比如修改时间、打印时间、修改次数。这都是隐藏的无法显示的重要的信息。如果转化为书证，会造成大量数据丢失。

（2）法律规定上，最高人民法院在《关于执行〈中华人民共和国刑事诉讼法〉若干问题的解释》第七十一条规定“收集、调取的书证应当是原件”，这就将书证限制到“原件”原则，这一点与英美法系一致。而“电子数据可以提取、复制”，这就说明电子数据是与书证截然不同的证据形式。

将电子数据转化为书证，往往缺乏监管的，有些操作人员不具备相应电子数据专业取证知识。最高人民法院在《关于执行〈中华人民共和国刑事诉讼法〉若干问题的解释》第九十三条规定，“提取、复制电子数据是否由二人以上进行，是否足以保证电子数据的完整性，有无提取、复制过程及原始存储介质存放地点的文字说明和签名”。这些要求在电子数据转化为书证时往往不被遵守，电子数据在转化过程中丢失或被篡改，导致其转化的书证和原始电子数据都没有证据效力。

3.4.4　电子数据与勘验、检查笔录的关系与区别

在电子数据取证的实际应用中，电子数据有时以勘验、检查笔录的形式出现。这种情况出现的背景是，1996 年刑事诉讼法中并未将电子数据作为证据的种类。这在司法实践中对当时蓬勃发展的电子数据的运用产生了两难境地：一方面，根据刑诉法的要求，一切可以证明案件事实的材料都是证据，与案件相关的电子数据自然属于证据的范畴；另一方面，作为大陆法系国家明文规定证据类型的我国，1996 年刑诉法又将证据限定为七种，并未涉及电子数据，又导致电子数据的应用无法律依据。面对这一局面，司法实践中采取了两类权宜之计：一类是在规范性文件中将电子数据作为证据类型，侧面的对刑事诉讼法加以补充。例如最高人民法院、最高人民检察院、公安部、国家安全部和司法部联合制定《关于办理死刑案件审查判断证据若干问题的规定》的第二十九条中规定：“对于电子邮件、电子数据交换、网上聊天记录、网络博客、手机短信、电子签名、域名等电子证据，应当审查”。另一类是将电子数据转化为法定证据类型予以使用，例如勘验、检查笔录。最高人民法院、最高人民检察院、公安部《关于办理网络赌博犯罪案件适用法律若干问题的意见》[①]在“关于电子证据的收集和保全”规定：“侦查机关对于能够证明赌博犯罪案件真实情况的网站页面、上网记录、电子邮件、电子合同、电子交易记录、电子账册等电子数据，应当作为刑事证据予以提取、复制、固

① 简称《刑事诉讼法解释》。

定。侦查人员应当对提取、复制、固定电子数据的过程制作相关文字说明，记录案由、对象、内容以及提取、复制、固定的时间、地点、方法，电子数据的规格、类别、文件格式等，并由提取、复制、固定电子数据的制作人、电子数据的持有人签名或者盖章，附所提取、复制、固定的电子数据一并随案移送。”从这一规定可以看出，该规范性文件实际上是要求将电子数据按照勘验、检查笔录这一法定证据类型进行提取和转换的。

但是，在 2013 版《刑事诉讼法》中，电子数据已经成为证据类型之一。与勘验、检查笔录并列为有效证据。同时在实践中，勘验、检查笔录与电子数据还是有一定区别的。勘验、检查笔录一般是如实陈述现场或者封存物品的状态、将电子数据以笔录的形式记录在案，虚拟的电子数据被物理化，并不能完整体现电子数据的完整信息，因此其证明力也大打折扣；同时《刑事诉讼法解释》也同时规定“所提取、复制、规定的电子数据一并随案移送”。这是符合现行的司法实践中，要求电子数据具有完整性和唯一性，并可以在法庭上呈现的实际需求。这都是勘验、检查笔录所不具备的。因此要充分注意到电子数据的“虚拟性”，不能够简单地用勘验、检查笔录或者其他证据类型来完全代替电子数据，以免影响案件侦查和诉讼过程。

3.5 电子数据审查

在刑事案件中，电子数据如要作为证据使用，必须符合刑事证据的三个基本特征，即证据的真实性、关联性和合法性。由于电子数据与传统证据的实物性或者言词性不同，具有虚拟性、隐蔽性和易篡改等特性，检察和审判人员必然审查电子数据的来源、电子数据的收集是否合法，公安机关是否采用了符合电子数据特性的技术手段收集，电子数据的内容有无被破坏、是否真实等。为保障刑事案件的采信率，公安机关必须正确理解电子数据审查的标准。

2010 年 5 月 30 日，最高人民法院、最高人民检察院、公安部、司法部、国家安全部联合颁布了《关于办理死刑案件审查判断证据若干问题的规定》，该规定首次专门条款确定了电子数据的运用规则。其第二十九条规定“对于电子邮件、电子数据交换、网上聊天记录、网络博客、手机短信、电子签名、域名等电子证据，应当主要审查以下内容：（一）该电子证据存储硬盘、存储光盘等可移动存储介质是否与打印件一并提交；（二）是否载明该电子证据形成的时间、地点、对象、制作人、制作过程及设备情况等；（三）制作、储存、传递、获得、收集、出示等程序和环节是否合法，取证人、制作人、持有人、见证人等是否签名或者盖章；（四）内容是否真实，有无剪裁、拼凑、篡改、添加等伪造、变造情形；（五）该电子证据与案件事实有无关联性。对电子证据有疑问的，应当进行鉴定。对电子证据，应当结合案件其他证据，审查其真实性和关联性。”

2013 年 1 月 1 日起施行的《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》第 93 条详细阐述了对电子邮件、电子数据交换、网上聊天记录、博客、微博客、手机短信、电子签名、域名等电子数据，应从五个方面进行真实性、完整性等的审查：（一）是否随原始

存储介质移送；在原始存储介质无法封存、不便移动或者依法应当由有关部门保管、处理、返还时，提取、复制电子数据是否由二人以上进行，是否足以保证电子数据的完整性，有无提取、复制过程及原始存储介质存放地点的文字说明和签名；(二)收集程序、方式是否符合法律及有关技术规范；经勘验、搜查等侦查活动收集的电子数据，是否附有笔录、清单，并经侦查人员、电子数据持有人、见证人签名；没有持有人签名的，是否注明原因；远程调取境外或者异地的电子数据的，是否注明相关情况；对电子数据的规格、类别、文件格式等注明是否清楚；(三)电子数据内容是否真实，有无删除、修改、增加等情形；(四)电子数据与案件事实有无关联；(五)与案件事实有关联的电子数据是否全面收集。对电子数据有疑问的，应当进行鉴定或者检验。

刑诉法解释第 93 条在五部委《关于办理死刑案件审查判断证据若干问题的规定》第 29 条规定的基础上，对电子数据的审查判断作了进一步修改完善[①]。

(1) 不存在“原始电子数据”的概念。与传统证据种类不同，电子数据没有“原始电子数据”的概念，只有“原始存储介质”的概念。由于电子数据的电子性，电子数据不同于物证、书证等其他证据种类，其可以完全同原始存储介质分离开来。例如，存储于计算机中电子文档，可以同计算机这一存储介质分开来，存储于移动硬盘、U 盘等存储介质之中。而且，对电子数据的复制可以确保与原数据的完全一致性，复制后的电子数据与原数据没有任何差异。与此不同，物证、书证等证据无法同原始存储介质完全区分开来，更无法采取确保与原物、原件完全一致的方式予以复制。例如，一封作为书证使用的书信，书信的原始内容无法同原始载体完全分离开来，只能存在于原始的纸张这一载体之上，即使采取彩色复印等方式进行复制，也无法确保复制后的书信同原件的完全一致性。不仅物证、书证等传统证据如此，视听资料这一随着技术发展而兴起的新型证据亦是如此。基于上述考虑，使用“原始电子数据”这个概念没有任何意义，对于电子数据而言，不存在“原始电子数据”的概念。但是，电子数据原始存储介质这个概念是有意义的，这表明电子数据是存储在原始的介质之中，即取证时是将存储介质予以扣押，并作为证据移送，而非运用移动存储介质将该电子数据从原始介质中提取，如直接从现场扣押行为人使用的电脑。因此，可以将电子数据区分为电子数据是随原始存储介质移送，还是在无法移送原始存储介质的情况下(如大型服务器中的电子数据)通过其他存储介质予以收集。为了确保随原始存储介质移送的电子数据的真实性、完整性，针对此种情形，审判人员要审查电子数据随原始存储介质移送的，是否采取了技术措施保证原始存储介质数据的完整性，如通过加只读锁确保数据不被修改，应当审查侦查机关是否对电子数据采取记录电子数据完整性校验值等方式保证电子数据的完整性。

(2) 远程调取电子数据的问题。需要特别注意的是，如果电子数据位于境外，难以通过国际司法协助获取相关数据，通常通过远程调取的方式获取数据。而且，即使在国内，也可能在个别案件中采取异地远程调取电子数据的情况。此种情况下，应当注明相关情况。审

① 喻海松：刑事证据规则司法适用解读《人民司法》2013 年第 3 期。

判人员应当根据注明的情况予以审查，判断电子数据提取过程的合法性，判断所提取电子数据的真实性和完整性。

（3）电子数据的鉴定和检验。在法庭审查过程中，审判人员应当通过听取控辩双方意见、询问相关人员等多种方式审查电子数据的内容和制作过程的真实性，必要时可以进行庭外调查。但是，由于电子数据的技术性较强，一般的删除、修改、增加等情形难以通过审判人员的观察作出认定，因此，刑诉法解释第九十三条第二款规定："对电子数据有疑问的，应当进行检验或者鉴定。"这里的检验或者鉴定，主要针对的是计算机程序功能（如计算机病毒等破坏性程序的功能）和数据同一性、相似性（如侵权案件需要认定盗版软件与正版软件的同一性、相似性）的问题等。

刑诉法解释第九十四条规定："电子数据经审查无法确定真伪，或者制作、取得的时间、地点、方式等有疑问，不能提供必要证明或者作出合理解释的，不能作为定案的依据。"

民事案件中，主要依据《电子签名法》来审查电子数据的有效性。《电子签名法》第八条规定："审查数据电文作为证据的真实性，应当考虑以下因素：（一）生成、储存或者传递数据电文方法的可靠性；（二）保持内容完整性方法的可靠性；（三）用以鉴别发件人方法的可靠性；（四）其他相关的因素。"这一规定参照了联合国的《电子商务示范法》的有关规定而作出的。检验电子数据还需要对其生成过程、存储、传递流程以及相关设备的情况进行审查。

3.6 国际电子数据取证的标准体系

3.6.1 国际电子数据取证标准体系概述

电子数据取证的结果是法律诉讼活动重要的证据。对电子数据取证来说，电子数据作为证据使用有两个必要条件：

- 可复现性。可复现性指的是运用相同的方法或标准重复取证，得出的结论一致。包括相同人员的重复取证或不同人员的比对取证；
- 可回溯性。利用相同的方法或标准，能够回溯到取证的各个环节和流程，确保取证的质量值得推敲。

因此，电子数据作为证据使用，必须保证输入和输出稳定可靠。这个过程由标准或指南来保证。

1. 标准

标准，是为了在一定范围内获得最佳秩序，经协商一致制定并由公认机构批准，共同使用的和重复使用的一种规范性文件[①]。

电子数据取证程序或者方法的技术相关标准，其中影响较大的主要为 ISO 系列。如

① GB/T 20000.1—2002《标准化工作指南第 1 部分：标准化和相关活动的通用词汇》。

ISO/IEC 27000:2014[①] 信息安全管理体系基础和术语(Information security management system fundamentals and vocabulary)。提供了 ISMS(Information Security Management System)标准族中所涉及的通用术语及基本原则,是 ISMS 标准族中最基础的标准之一。ISMS 标准族中的每个标准都有"术语和定义"部分,但不同标准的术语间往往缺乏协调性,而 ISO/IEC27000 则主要用于实现这种协调。

2012 年 10 月 15 日,ISO 组织发布了 ISO/IEC 27037:2012 信息技术-安全技术-电子证据识别、收集、获取和保存指南[②](Information technology-Security techniques-Guidelines for identification, collection, acquisition, and preservation of digital evidence),作为 ISO/IEC 27000:2014 信息安全管理体系必要的模块。ISO/IEC 27037:2012 标准为在电子数据处置中的特定活动提供了指南,包括可能具有证据价值的潜在电子数据识别、收集、获取和保存。此标准为取证人员提供整个电子数据处理过程中遇见的常见情况的指南,协助组织处理他们的纪律处分程序,并促进不同司法部门的潜在电子数据的交换。这个标准特别是现场勘验的取证环境具有极其重要的参考意义。

标准中还有一系列对电子数据取证实验室进行运行管理以及认证认可的标准程序,其中影响较大的主要是 ISO/IEC 17025《检测和校准实验室能力的通用要求》(ISO/IEC 17025: 2005 General requirements for the competence of testing and calibration laboratories[③]),是国际标准化组织和国际电工委员会联合发布的国际标准,是全球通用的检测和校准实验室质量管理标准,也是认可机构实施认可的基础。

2. 指南

标准制定相对严谨,因此一段时间内不会更新。而电子数据取证的相关技术和流程却在时刻变化之中。因此国外执法部门以"指南"(guide)作为标准的良好补充,指南可以看作"准标准"。

电子数据取证的相关指南西方国家起步较早,制定的也较为频繁。主要是规定取证方法和流程的操作指南,例如美国国家标准与技术研究院(National Institute of Standards and Technology,NIST[④])的系列标准集,其中较为重要的有《SP 800-101 Rev. 1 移动设备取证指南》(Guidelines on Mobile Device Forensics[⑤]);《SP 800-86 应急响应中取证技术应用指南》(Guide to Integrating Forensic Techniques into Incident Response[⑥])。美国司法部发布的《现场人员操作指南——电子犯罪现场调查》(Electronic Crime Scene Investigation, A

① http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411
② http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381
③ http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39883
④ http://www.nist.gov/
⑤ http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf
⑥ http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

guide for first responders[①])、《刑事调查中的搜索、扣押电脑和获取电子证据指南》(Searching and seizing computers and obtaining electronic evidence in criminal investigations[②])、互联网工程任务组(IETF)发布的备忘录《RFC-3227 电子证据收集及归档指南》(Guidelines for evidence collection and archiving[③])等。英国首席警官协会(Association of Chief Police Officers,ACPO[④])发布的《基于计算机的电子证据取证最佳实践》(Good Practice for Computer-based Electronic Evidence)。

3.6.2 国际电子数据取证指南简介

对于电子数据取证实际应用,指南更具备指导意义。通过了解西方国家的取证指南,不但可以对我国的电子数据取证工作提供指导,而且还对我国的电子数据取证的相关标准和指南的制定提供借鉴。

1. 国际通行的指南

国际标准化委员会(ISO)颁布的 ISO/IEC 27037:2012《信息技术-安全技术-电子证据识别、收集、获取和保存指南》[⑤]是符合国际标准的取证指南。ISO/IEC27037 的主要内容不但包括电子数据的科学原则与理念,而且对于电子数据取证中的各类检材的取证提供了具体的方法与技术细节,其内容涵盖了电子数据识别、收集、获取和保存的完整过程。指南的主要内容有:

(1) 对于电子数据而言,该指南认为可审核性、可重复性、可再现性、正当性是很重要的四大原则。

- 可审核性,是指独立的评测人或其他授权有关方应能评估电子数据取证第一响应人员和鉴定专家进行的活动,活动被记录在案。
- 可重复性,是指在相同的条件下,使用相同的设备产生相同的结果。同时使用相同的程序和方法,可以在任意时候重复,则会产生重复性:一个拥有熟练技能、经验丰富的电子数据取证人员应该能够在没有指导或解释下,通过操作记录中所描述的所有流程,得出同样的结果;同时应注意到在有些环境下,结果不可重复,例如当原始硬盘被复制后返还使用时,或者涉及易失性存储器的资料时。在这种情况下,取证人员应确保获取过程是可靠的。为了实现可重复性,应记录所有操作。
- 可再现性,是指使用相同的方法,在不同的条件下,使用不同的设备,产生相同的结果,会产生可再现性。
- 正当性,是指电子数据取证人员应能证明处理潜在电子数据的所有行动和方法正确。

---

① http://www.ncjrs.gov/pdffiles1/nij/219941.pdf

② http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

③ http://www.rfc-base.org/rfc-3227.html

④ 已经改组为国家警察局长理事会(NPCC)

⑤ http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381

(2) 电子数据面对的检材种类主要有以下几类：

① 计算机设备中使用的存储介质，例如硬盘、软盘、光盘及类似功能的数据存储设备。

② 移动电话、个人数字助理(PDA)、个人电子设备(PED)、存储卡。

③ 移动导航系统。

④ 数字照相或录像机。

⑤ 有网络连接的计算机设备。

⑥ 基于 TCP/IP 的网络和其他数字协议的数据。

⑦ 有上述功能的其他设备。

(3) 指南提出了在进行电子数据取证时，执行顺序应有一个优先级的思想。执行优先级以减少潜在电子数据被损坏的风险，并将收集的电子数据的证据价值最大化。因此对于取证过程，取证人员还应：

① 记录所有的行动。

② 为了确定潜在电子数据副本与原始证据相比的准确性和可靠性，确定和应用方法。

③ 认识到潜在电子数据的保存行动不能总是非侵入式的。

2. 美国制定的指南

美国执法部门一直强调执法人员应对犯罪现场的能力。因此执法部门，包括军方、警方和标准化部门，都积极参与到电子数据取证指南的制定。典型的是美国司法部专门编写了《电子犯罪现场调查指南》(US-DOJ-Electronic Crime Scene Investigation, A Guide for First Responders Second Edition[①]，目前已经出到第二版，以下简称指南)，编写这个指南的目的是为了让第一时间到达现场的执法人员能有效应对日益复杂的犯罪现场电磁环境，并按照符合法律规范的要求进行电子数据的扣押和获取。根据反恐类案件以及网络环境的巨大改变和复杂性，在其最新一版内大幅增加了对现场网络环境及其设备、应用进行识别收集获取的内容。

该指南对现电子数据取证提出了三条通用原则：不改变原则、专业训练原则、证据监督链原则。

- 不改变原则，是指应确保在电子数据收集、扣押、传递过程中，都不应该造成电子数据证物的改变。
- 专业训练原则，是指对电子数据证物从收集到扣押、传送、分析都应该由受到专业训练的人员来进行。
- 证据监督链原则，指电子数据证物从收集到扣押、传送、分析都应该有完整的文档记录以备事后查验。

这三条原则不仅适用于美国的法律体制，同样对我们开展电子数据取证工作也有借鉴意义。

---

① http://www.nij.gov/publications/Pages/publication-detail.aspx? ncjnumber=219941

对于现场电子数据证物的搜查，该手册提出了四个步骤：

（1）辨认、确定、封存并保护犯罪现场中的电子数据；

（2）记录整个犯罪现场并特别注明电子数据发现的位置；

（3）集中标记电子证物并保存电子数据；

（4）以安全的方式包装并运输电子数据。

指南的第一章对常见的电子数据的类型进行了逐一描述，并附有照片，便于现场执法人员对照识别，对每一类证物可能包含的证据信息。特别是对每类证据需要注意的细节都描述非常详细。比如对移动设备，其手册内专门提示，移动设备的取证需要注意以下三点：

- 电池耗尽可能会导致数据丢失。
- 保持开机状态有可能会导致数据丢失或删除。
- 手持设备可能会被远程删除或者锁定。因此，执法人员在现场应尽可能将易丢失数据提取、保存。

对于网卡、路由器等网络设备，该指南特别提出，应特别关注网络设备的 MAC 地址以及设备所携带的存储介质上所可能含有的网络应用信息。

指南的第二章列出了电子数据现场勘验应准备的物品清单可供参考；第三章描述了对现场进行保护和评估的方法，并列出了对现场人员的询问提纲。其中特别提到要注意对现场电子设备的网络摄像头和可能的远程连接进行评估和记录，对于在线已经登录的聊天室、即时通讯等要做好提取和固定；第四章则对如何记录犯罪现场的细节进行了阐述；手册的第五章主要阐述电子数据收集步骤。该章的体例更像一个流程图，根据现场遇到的电子数据的不同状态可以选择不同场景的操作步骤。该章的最后一节特别提到，如果遇到复杂系统环境，现场执法人员切勿轻易关机；手册的第六章则建立了电子数据的包装、运输、存储的程序。在包装的程序中，该手册特别提到应注意不要污染电子数据可能潜在的生物证据（如指纹、DNA 等）；第七章则针对美国常见的虐待儿童、入侵计算机、伪造、死亡调查、家庭暴力、电子邮件威胁（骚扰）、绑架、身份偷窃、麻醉品犯罪、网络诈骗、卖淫、盗版、电信诈骗以及涉及国家安全的恐怖主义等 14 类案件的搜查重点进行了阐述。不同的案件搜查的重点不完全一样，如恐怖主义案件，搜查重点专门提到了 voip 语音电话及 GPS 设备。

综上所述，该手册内容浅显却紧扣实战，使现场人员即使不熟悉电子取证技术也能借助手册完成工作。该手册的写作方法和内容值得国内执法人员借鉴。

3. 英国制定的指南[①]

英国是世界上最重要的科技强国之一，它的电子数据取证标准化研究也是仅次于美国。英国的指南最为典型的是英国首席警官协会（Association of Chief Police Officers，

① 郭弘，电子数据取证标准。

ACPO[①])发布的指南,这是最经典的电子数据取证指南之一。ACPO 是一个非营利性组织,监管英格兰、威尔士和北爱尔兰的警务实践。参与了计算机证据国际组织(IOCE)的计算机取证过程中应该遵守的 6 项一般原则的制定。为使实践工作能符合取证的原则和标准,ACPO 推出的《电子数据检查的最佳实战指南》(Guidelines for Best Practice in the Forensic Examination of Digital Technology)和《电子证据最佳操作指南》《Good Practice Guide for Digital Evidence[②]》等多个指南,并随着实践工作的转变而新增、修订和完善指南内容。

除此之外,英国标准协会(British Standards Institution,BSI[③])、英国内政部科学发展处(Home Office scientific development branch,HOSDB[④])和英国数字保存联盟(Digital Preservation Coalition,DPC[⑤])都制定了电子数据取证的指南。

4. 香港地区制定的指南

香港资讯保安及法证公会(Information Security and Forensics Society, ISFS[⑥])成立于 2000 年,是香港电子取证专家专业团体,主要目标是推广计算机法证公众意识,提升专家专业能力,创立公正规范的规程,促进法证技术的发展。该公会人员包括香港海关、香港警务处、廉政公署、律政司、企业信息安全人士、院校学者。ISFS 积极推动与内地的合作与交流,目前已经和国内联合举办了十届 CCFC 计算机法证技术峰会。ISFC 发布的和电子数据取证相关的出版物有:

(1) 2004 年 4 月,Computer Forensics Part 1: An Introduction to Computer Forensics

(2) 2009 年 8 月,Computer Forensics Part 2: Best Practices

(3) Computer Forensics Glossary

3.7　我国电子数据取证标准

长期以来,由于电子数据在我国不属于法定证据,其标准化工作无法可依,处于停滞状态。2013 年电子数据由国家法律确定为证据类型之一后,国内对于电子数据取证标准的研究和制定逐步走上正轨。

目前,国内的取证标准体系主要分为三个层级:国家标准(GB/T)、行业标准(由司法鉴

---

① 2015 年成立的国家警察局长理事会(The National Police Chiefs' Council,NPCC)取代了英国首席警官协会(Association of Chief Police Officers,ACPO)

② http://site.npcccms.coraider.com/documents/FoI%20publication/Disclosure%20Logs/Information%20Management%20FOI/2013/031%2013%20Att%2001%20of%201%20ACPO%20Good%20Practice%20Guide%20for%20Digital%20Evidence%20March%202012.pdf

③ http://www.standardsuk.com

④ http://webarchive.nationalarchives.gov.uk/20091207123234/http://crimereduction.homeoffice.gov.uk/cpindex.htm

⑤ http://www.dpconline.org/

⑥ http://www.isfs.org.hk

定主管部门、司法鉴定行业织或者相关行业主管部门制定的行业标准和技术规范)以及各相关实验室自制的标准。电子数据取证的标准主要以行业标准为主,行业标准发布较多的相关政府部门主要是公安部网络安全保卫局、公安部第三研究所、公安部刑侦局和公安部第二研究所等单位。

目前,电子数据取证国家标准仅有三个:《GB/T 29360—2012 电子物证数据恢复检验规程》、《GB/T 29361—2012 电子物证文件一致性检验规程》、《GB/T 29362—2012 电子物证数据搜索检验规程》。

行业标准在近年来得到了快速的发展。如 2008 年发布的行业标准仅四个,《GA/T 754—2008 电子数据存储介质复制工具要求及检测方法》、《GA/T 755—2008 电子数据存储介质写保护设备检测方法》、《GA/T 756—2008 数字化设备证据数据发现提取固定方法》、《GA/T 757—2008 程序功能检验方法》,到 2014 年发布的行业标准数就达到了 7 个。

2008 年发布

- GA/T 754—2008《电子数据存储介质复制工具要求及检测方法》
- GA/T 755—2008《电子数据存储介质写保护设备检测方法》
- GA/T 756—2008《数字化设备证据数据发现提取固定方法》
- GA/T 757—2008《程序功能检验方法》

2009 年发布

- GA/T 825—2009《电子物证数据搜索检验技术规范》
- GA/T 826—2009《电子物证数据恢复检验技术规范》
- GA/T 827—2009《电子物证文件一致性检验技术规范》
- GA/T 828—2009《电子物证软件功能检验技术规范》
- GA/T 829—2009《电子物证软件一致性检验技术规范》

2012 年发布

- GA/T 976—2012《电子数据法庭科学鉴定通用方法》
- GA/T 977—2012《取证与鉴定文书电子签名》
- GA/T 978—2012《网络游戏私服检验技术方法》

2014 年发布

- GA/T 1770—2014《移动终端取证检验方法》
- GA/T 1771—2014《芯片相似性比对检验方法》
- GA/T 1772—2014《电子邮件检验技术方法》
- GA/T 1773—2014《即时通讯记录检验技术方法》
- GA/T 1774—2014《电子证据数据现场获取通用方法》
- GA/T 1775—2014《软件相似性检验技术方法》
- GA/T 1776—2014《网页浏览器历史数据检验技术方法》

司法行政管理部门也发布了司法鉴定技术规范,主要有 2014 年发布的 2014 年发布

SF/Z JD0400001—2014《电子数据司法鉴定通用实施规范》、SF/Z JD0401001—2014《电子数据复制设备鉴定实施规范》、SF/Z JD0402001—2014《电子邮件鉴定实施规范》、SF/Z JD0403001—2014《软件相似性检验实施规范》等 4 个。

3.8　本 章 小 结

电子数据取证不仅要具备技术能力，更要了解相关的法律法规，并按照标准方法和指南进行工作，这样才能保证证据的有效性。本章通过对比英美法系与大陆法系（我国）关于电子数据的法律规则，阐述了电子数据的作为证据的效力问题。同时介绍了我国和相关部门对于电子数据的法律和法规，以及电子数据作为证据使用的审查标准。对于法律实践有着现实指导意义。通过介绍国外发展完善的标准和指南，指出未来电子数据取证的发展要遵循标准化的方法和操作指南，来保证取证的质量，确保电子数据作为证据使用的有效性。

思　考　题

1. 简述美国和英国关于电子数据的法律。
2. 简述美国的最优证据规则以及对于电子数据进行的修订。
3. 我国关于电子数据的相关立法有哪些？
4. 电子数据与视听资料的区别是什么？
5. 电子数据与物证的区别是什么？
6. 电子数据与书证的区别是什么？
7. 电子数据与勘验、检查笔录的关系与区别是什么？
8. 电子数据的审查在法律和司法解释上有哪些规定？
9. 电子数据取证的标准体系分为几个层次，具有什么含义？
10. ISO/IEC 27037:2012《信息技术-安全技术-电子证据识别、收集、获取和保存指南》提出的电子数据的四大原则是什么？
11. 我国出台的关于电子证据的三个国家标准是哪些？