鉴 定 制 度
Forensic System

大数据背景下电子数据的审查与认定

王玉薇
(华东政法大学,上海 201620)

摘 要:随着大数据时代的到来,“数字化生存”的崭新挑战倒逼我们正面直视传统证据规则的网络“移植”风险。由此产生于“比特世界”的新型电子数据如何进行有效性的审查与认定成为网络证据理论及实务界面临的新任务。新型电子数据在真实性、合法性和关联性等网络证据规则的生成规律上异于传统证据并具有虚拟性、即时性、转化性等独立属性,由此使电子数据认定中“移植化”模式遭致合法化危机。为此,需要完善网络取证标准与原则,破解真实性认定的合理性困境;完善网络取证规则,破解客观性认定的合法性困境;完善非法网络证据的排除规则,破解关联性认定的有效性困境难题,以利于科学的网络电子数据认定体系的建构。

关键词:大数据;电子数据;非法证据排除;电子数据审查;电子数据认证
中图分类号:D915.13 **文献标志码**:A doi: 10.3969/j.issn.1671-2072.2017.06.002
文章编号:1671-2072-(2017)06-0010-08

The Examination and Identification of Electronic Data in the Background of Big Data

WANG Yu-wei
(East China University of Political Science and Law, Shanghai 201620, China)

Abstract: With the development of the big data age, the new challenge of “digital survival” forces us to look directly at the risk of “transplant” traditional evidence rules to the network. The way to carry out the review and identification of the validity of new electronic data which is generated in the “bit of the world” becomes a new task of people working on network evidence theory and practice. The new electronic data are different from the traditional evidence for their generation rules in authenticity, legitimacy, relevance and so on, and as a feature electronic data are virtual, prompt and transitional. It makes a legitimacy crisis of electronic data in the “transplant” model. In order to facilitate the construction of scientific identification system of network electronic data, we should improve standards and principles of obtaining network evidence to resolve the difficulties of confirmation of genuineness of network evidence. We should improve the rules of obtaining network evidence to resolve the problem of verification of network evidence. We should also improve the rules of excluding illegal network evidence to resolve the difficulties of determination of relevance of electronic evidence.

Keywords: big data; electronic data; exclusion of illegal evidence; examination; verification

1 问题的提出

随着大数据、云计算时代的到来,把人类带进了崭新的“数字化生存”的虚拟网络空间。这将使针对现实空间设计的物理化证据认定规则面临“比特世界”的数据化规则的严重挑战。

由此,产生于“比特世界”的新型电子数据如何进行有效性的审查与认定成为网络证据理论及实务界面临的新任务。目前的电子数据认定模式是将针对线下社会的证据理论及规则跨界照搬至新型的电子数据上。此种操作逻辑在三大诉讼法的不断修改及相关司法解释颁布中均有较为明显的规定。

不可否认,这种传统证据认定网络“移植”模式确实在电子数据的法律定位、概念明晰、类型列举等方面发挥了重要的决定功能。但事实上,大数据

收稿日期:2017-09-25
基金项目:“十三五”国家重点研发项目(2016YFC0800707);国家社会科学基金重大项目(14ZDB147);国家社会科学基金课题(15CFX022);华东政法大学 2017 年研究生创新能力培养专项资金项目(2017-1-006)
作者简介:王玉薇(1982—),女,博士,主要从事法理学、法社会学研究。E-mail:wangyuwei333@126.com。

背景下新型电子数据的虚拟性、即时性、转化性等新属性衍生出一系列自主运行的新规则。如差异化的网络认定规则、独立化的网络审查规则,网络非法证据排除规则等,这将从本质上动摇传统证据认定的合法性根基。我国目前围绕电子数据进行的一系列修法及颁布司法解释的活动为新型电子数据的研究开辟了新视野。新型电子数据的证据地位亦由最高人民法院《关于适用〈中华人民共和国民事诉讼法〉的解释》(法释[2015] 5号)(简称《民诉解释》)第一百一十六条、《关于适用〈中华人民共和国刑事诉讼法〉的解释》(法释[2012] 21号)第九十三条等明确规范。最高人民法院单独或联合其他部门发布的《关于办理死刑案件审查判断证据若干问题的规定》(法发 [2010]20号)(以下简称 (《刑证据规定》)、2016年《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)(以下简称《电子证据规定》)、2017年两高三部关于办理刑事案件严格排除非法证据若干问题的规定(法发[2017]15号),更是细致完善了是新型电子证据审查判断的标准和程序。以此为参照,本文试图从现代化网络证据规则认定的法治思维与方法上着手,为目前我国电子数据认定中的不合理、不合法、有效性不强的困境寻求解决问题的最佳出路。

2 电子数据认定中的"移植化"走向

目前我国对电子数据的认定主要围绕真实性、合法性、客观性三个方面的内容展开。其惯性的认定逻辑是将线下证据认定的原件理论、最佳证据规则、非法证据排除规则扩张适用于新型的电子数据。其目的在于,借助司法对电子数据的审查与认定,补足网络证据规则的不足与滞后,实现其对电子数据证明力的采信与排除。

2.1 真实性认定的网络"移植"

电子数据真实性的认定以终极实在为价值目标,秉承传统证据认定的原件理论和基本理念,主要用来证明案件待证网络事实的真实性。以此为基础,目前理论通说一般认为,如若用于证明案件事实的电子数据,存在伪造、增加、删除、修改等无法证明真实性的情形出现时,其通常不会被法院认定并采纳,也随之丧失证明力。

异于传统证据真实性的认定,新型电子数据具有虚拟性和易逝性等独特属性。这些具有新属性特征的电子数据更多存储在虚拟化的云系统中。这将导致海量电子数据的直接提取困难并易遭受攻击。如备受热议的E租宝案、快播案等庭审过程的证据展示,其间涉及到的很多具有较强证明力的电子数据都是从云系统提取的。诸如此类的特殊性,我国三大诉讼法的多次完善和司法实践都做出了新的规定和相应调整。具体来讲主要体现在电子数据真实性的形式认证和实质认证两方面的内容。前者主要涉及电子数据类型的真实性审查;后者主要涉及电子数据内容的真实性审查。

从电子数据真实性认证的形式看,整体上,三大诉讼法及相关司法解释较为一致地赋予了电子数据独立的网络法律地位。2012年修改的《刑事诉讼法》第四十八条、2012年修改的《民事诉讼法》第六十三条以及2014年修改的《行政诉讼法》第三十三条均对此做出了相应的规定。随后,2015年《民诉法解释》、2016年《刑事电子数据规定》第一条、第二十二条等规定进一步对电子数据的形式真实性认定标准和程序做了较为详尽的描述。如原始存储介质及数字签名、数字证书等特殊标识有无的形式要件。其中,根据《民事诉讼法》第六十九条和最高人民法院《关于民事诉讼证据的若干规定》第七十七条,被依法公证的文件会被法院采纳,并直接作为案件证据。这与国际电子数据真实性认定的"功能等同法"标准也是较为类似的。

在国际电子数据认定上,基本确定了对电子数据"原件"的要求和"功能等同法"原则,只要电子数据在功能上等同或基本等同于书面原件,那么可以依此"原件"理论标准判断电子数据的证据效力。与此相类似,英美等国家对于电子数据的要求确立了传闻规则和最佳证据规则。美国法将"商务记录例外"作为传闻证据的例外。相类似的做法还有以法国、德国等为代表的大陆法系国家也基本认为,只要电子数据能够确保其真实可靠性就可以作为证据被接受并采纳[1]。如《法国民法典》第1361-1条的规定。以上国际通行的做法表明,我国目前对新型电子数据扩张适用原件理论在一定程度上可以获得国外电子数据认定理论的支持,具有一定程度上的普遍适用效力。对此,需要指出的是,新型电子数据的易篡改、易攻击等特有属性必然会减弱原件理

论适用的网络合理性。

从电子数据真实性认证的实质认证上看，主要聚焦三个事项：电子数据是否可以重现、是否附有说明及证据的完整性等要求。除了新修改的三大诉讼法及相关司法解释对此做了相应的规定外，2016年《刑事电子数据规定》就电子证据的鉴真部分变动的条款很多。其中第五条规定了电子数据完整性保护的方法；第八条规定了原始存储介质的认定原则；第九条规定了计算完整性校验值的要求；第二十二条规定了对真实性的审查判断内容、第二十三条规定了验证完整性的方法；第二十七条规定了瑕疵处理的补强规则、第二十八条规定了未能鉴真的排除性规则等。其中第九条明确规定基于原始存储介质不便封存或位于境外等例外情况出现时，可以在线提取。据此，从以上分析不难发现，目前我国电子数据实质真实性的认定比重越来越重，证明力也随之增强。

2.2 合法性认定的网络“移植”

电子数据的合法性认定以权利保障为司法的终极目标，秉承程序正义和方法科学为理论的基本要义。主要规定用来证明案件待证事实的电子数据必须按照法规所规定的内容和法定程序取得的。电子数据合法性的认定是证据的核心，是证据在法律上成为能否允许其作为证据的资格和能否成立及被采用的关键因素[2]。据此，几乎三大诉讼法及相关的司法解释规定都指出，采用非法方式收集的电子数据通常不被采纳。详细来讲主要体现在形式合法性和实质合法性的认定两方面。前一方面主要强调电子数据在形式上的合法性；后一方面主要强调收集方式的合法性。

从电子数据合法性认证的形式上看，三大诉讼法及相关司法解释都已明确电子数据属于合法的证据形式并在不同部门立法中分别列举了电子数据合法性存在的具体类型。概括而言，主要指电子数据的制作、存储、收集等程序是否合法以及是否有相关的取证人签名或盖章等形式构成要件的要求，特别体现于其生成、存储、传递以及显现、收集等方面。电子数据是2012《刑事诉讼法》修改第四十八条新增的一种法定证据。规定指出“可以用于证明案件事实的材料，都是证据。证据包括……（八）视听资料、电子数据。”

在刑诉法修改前，2010年《死刑案件证据规定》第二十九条先行对电子数据的范围进行了列举式规定。随后，2015年《民诉法解释》第一百一十六条以不完全列举的方式，进一步详细列举了民事领域电子数据的范围与涵义。如将电子数据表述为，通过电子邮件、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、域名等形成或存储在电子介质中的信息，具体包括网页等网络平台发布的信息、通讯群组等网络应用服务的通信信息等情形。从国际层面看，在英美法上，证据具有两个重要的特征，即“关联性”和“可采纳性”，其实就是指证据所应当具备的法律要件，即“法律性”[3]，为我国电子数据合法性的认定提供了可参照的标准与原则。《死刑案件证据规定》第二十三条明确规定审查判断鉴定意见时应当着重考察的10项内容，旨在通过对鉴定意见的全面审查判断，明晰其证据能力和证明力。

从电子数据合法性认证的方式看，主要指获取电子数据手段的合法性。“证据必须与需要证明的案件事实或其他争议事实具有一定的联系，具有证明性”[4]。此种手段合法性对于电子数据收集的操作标准至关重要。三大诉讼法及相关司法解释都较为一致地认为，凡足以影响重大权益实现的，均视为实质非法性，均予以排除，这与2015《民事诉讼证据规定》的预期相一致，其中第二十四条、第六十八条对此做出了详细的规定。第六十八条指出：“以侵害他人合法权益或者违反法律禁止性规定的方法取得的证据，不能作为认定事实的依据。”综合起来看，电子数据合法性的网络“移植”在一定程度上，确定了网络证据合法性认定的标准和形式，具有积极的法治意义。

2.3 关联性认定的网络“移植”

电子数据关联性的认定，主要是指电子数据证据必须与案件的待证事实有关。从理论上讲，电子数据与待证案件事实的关联性越强，其证明力也越强，被审判人员接受并被采纳的概率越高。通常情况下，电子数据关联性的有无及大小直接决定电子数据能否被作为证据以及证明力的大小。与事实联系越紧密、越直接相关，其证明力越大。反之，如果与待证案件事实是间接相关的，逻辑上距离较远，则证明力越小。

异于传统证据的关联性的认定方式,电子数据关联性的认定中除了必须与案件待证事实有实质性关联外,更为重要的还必须与电子数据生成的环境有动态的客观性关联,只有这种双关联的结构同时具备才能从系统上更有效、更有意义地识别信息的关联性。从本质上看,主要肇因于大数据时代的电子数据具有人与人、人与物、物与物之间即时互联的结构属性。因而仅凭单一性的电子数据很难建构和支撑起证明力,需要其他相关性的辅助或印证方式才能实现。2016年新颁布的《刑事电子数据规定》第二十五条确定了对网络身份与现实身份同一性及犯罪嫌疑人、被告人与存储解释关联性的审查的标准,破解了电子数据客观性关联认定标准缺失带来的不规范采信困难。

具体而言,电子数据的形式关联性主要指电子数据间的物理关联,解决的是人与有形物的关联性问题,是人与物的外在形式上的关联性问题。而电子数据的实质关联性是指电子数据间的内容关联,电子数据的内容直接影响着案件性质,即必须与系统环境相耦合才可能与待证案件事实发生实质性关联。许多部门规章对电子证据的关联性提出明确的要求,如2010年《死刑案件证据规定》第二十九条指出:"对于……电子证据,应当主要审查以下内容:……(五)该电子证据与案件事实有无关联性。"就此项规定在司法实践适用的效果而言,在胡某某等涉嫌破坏计算机信息系统罪一案中,辩护意见认为,"鉴定书的鉴定材料来源不明,鉴定意见不具有关联性。[5]"可见,在司法实践中,审判人员以电子数据与待证案件事实的关联性有无而判断电子数据的证明力的判决还是较为常见的。

3 网络"移植"走向给电子数据认定带来的现实困境

不可否认的是,上述网络证据"移植"模式确实在电子数据的法律定位、概念明晰、类型列举等方面发挥了重要的决定功能。但事实上,新型电子数据的新属性衍生出一系列自主运行的新规则将从本质上给网络"移植"模式带来不客观、不合法、不正当等困境,势必影响电子数据证明力功能的客观实现。

3.1 真实性认定的网络合理化不足

大数据背景下电子数据的即时性、虚拟性和数字化等新型属性因未获相关立法理论和司法实践的特别关注而将其混同于传统证据的认定方法及程序,进而导致庭审中被采信的法律资格陷入合理性困境。

相较于传统证据真实的认定而言,新型电子数据真实性的认证具有"双重独立性。[6]"此种双重独立性的形成依托于"案件事实中的真实性因素与客观世界的真实性因素两相竞合后并将这种真实性顺次传递至证据生成、保存、递交法庭全过程的一种集合属性。[6]"据此,电子数据真实性认定的形式与实质两方面内容具有同等的重要地位并且其证明对象具有同一性特征。而我国目前的立法规定和理论学说尽管明确了电子数据独立地位的同时,却将其与传统证据典型的书证、视听资料相等同,并将制定于现实社会的书证和视听资料跨界穿越到虚拟化的网络空间,直接适用于电子数据的审查与认定。其真实性的认定是司法实践中常遇的难题。在庭审过程中,未经实名认证的微信聊天记录作为证据被采纳的概率不高,证据采信的说理机制相对不完善。

不可否认,电子数据确实与传统的证据类型及形式某种程度上具有相类似的特征。但由于本质属性及生成规律的显著差异决定了现实与虚拟证据的认定并非一一的对应关系, 也即绝非完全等同。比如,传统证据的原件书证是可以通过人的肉眼识别的,而电子数据数字化特质决定其非直接观察属性。因为电子数据体现为以0和1的二值数字组成的数字化信息化的虚拟单元,此时现实社会的物理人被编码为虚拟化的电子人。在网络空间中,"其生活主要是由代码来规制的,人们同样要在代码的规制下生活。[7]"在一定范围和功能上,代码实则成为了网络证据收集行为规制的基本法律,并有效制约审判权的正确行使。这将使种种围绕身份相关的事务不再迫切,同时由于互联网没有守门人—互联网不存在类似编辑部的机构"[8], 从根本上动摇了以"身份"为基础的传统证据真实性认定规则的根基。

进一步说,异于传统证据,电子数据必须经过合法的程序转化都会生成一份新的文件,突破了原件理论的基本要求。而对于这些自动生成的电子数据的证明力及证据能力,我国目前电子数据的认定恰恰关注较少。在虚拟化的数字化生存空间中,其

电子数据认定的惯例为,提交电子数据不仅要移送可移动存储介质而且要提交打印件等转化材料。这意味着,对电子数据真实性认定本质不在于提交的是原件还是复印件,比如是原始的纸质借条还是微信借条截图,而应凭借微信借条所载内容判断能否证明借款事实的真实存在。据此,电子数据真实性的证明力常常招致司法实践的怀疑或拒绝采纳。尽管很多规范性的法律及司法解释都较为一致地规定了网络用户的"后台实名、前台自愿"注册的基本原则,如2014年出台《即时通信工具公众信息服务发展管理暂行规定》第六条规定等。但多数情况下,一元化的现实真我极易不受限制地任意注册为多元化网络假我,给电子数据真实的认定带来更多的复杂性。

3.2 合法性认定的网络规范性不足

电子数据的合法性,是电子数据能否被赋予法定证据资格的关键因素。对此,除了通过相关的立法修改及司法解释出台的方法肯定电子数据的法律证据地位外,还通过"功能等同说"、"法律拟制说"、"混同标准说"、"结合打印说"等现实理论的网络扩张来对电子数据的证明力和证据能力进行深层次说理及补强。三大诉讼法修改后的新规定均有相关的内容呈现。例如《行政诉讼证据规定》第六十四条指出:"以有形载体固定或者显示的电子数据,其制作情况和真实性经对方当事人确认,或者以公正等其他有效方式予以证明的,与原件具有同等的证明效力。"这一解释规定显然是将电子数据的"复制件"等同于传统证据的"原件",并强调二者间具有证明力上的同一性,但却忽视了电子数据的"法定原件"的非唯一化及独立性的创生规律,再次使电子数据认定陷入新型合法性困境。

异于电子邮箱、博客等以微信、云盘等为代表的新型电子数据,其即时性、虚拟性、系统性等特征较为突出。由此特征带来的易删改性、易污染性、易丢失性现象普遍存在,并大大削弱了自身的证据能力。诚如有学者认为,电子数据的证明力弱,原因是电子数据具有"高度易删改性和隐蔽性"[9]。而事实上,电子数据的证明力不在于将其归属于哪一种证据形式,而在于其实质上的与待证案件事实间的关系强弱。关系越强,证明力越强,忽视了电子数据具有不受限制的"天然证据能力",导致对其认定标准的不规范乱象。

就本质而言,新型电子数据或者产生于数字化的虚拟网络空间,或者在现实与虚拟两个空间中来回穿梭。这种虚拟场域的法治意义在于,它是一个巨大的转换器和追求责任的必经之路。但终究因其经过的环节较多,不确定成分较多等偶然性可能性增加,致电子数据的被法庭采纳的合法性不足,给法律认定带来困扰。

在司法实践中,常常碍于相关法律的缺位或不到位等客观存在,常常把网页截图、QQ聊天记录、手机短信等电子数据转化成传统的书证、物证、视听资料等类型,然后根据传统证据类型的认定规则确定电子数据证明力的有无及大小。通常的做法只是在判决书中笼统地说"上述事实,有……网页截图等证据证实,足以认定。"显然,对电子数据采信的说理机制极为不充分,认证过程相对简单。然而"在审判活动中运用电子证据最大的挑战就是不能轻易地将其划归传统的证据类型"[10]。整体而言,从网络证据理论和司法审判实践观察,电子数据被采信的标准不规范,网络程序规则缺位,因此非法性认定的网络规范性不足,是电子数据认定有效性低下的又一重要原因。

3.3 关联性认定的网络有效性不足

电子数据关联性认定的有效性要旨在于,如何从海量的电子数据中挑选出与待证案件事实具有较大关联性的数据,并将其选择出来作为证据在庭审中出示并被法官采纳,而排除非关联性信息或关联性较少的信息的干扰。这将直接决定了电子数据的关联性被法官采纳的概率或机会,同时决定了电子数据证明力的大小或强弱。进一步说,新型电子数据关联性的认定不再是或有或无的二选一模式,"结论"的权威性时代已经过去,其电子数据的证据能力与证明力必须通过庭审加以检验,法官在此基础上依法进行综合审查判断,经此过程反复进行说理机制的建立才是现代电子数据关联性认定的有效性之所在。

目前我国电子数据关联性有效性低的主要原因是,电子数据产生的特殊网络语境环境未能得到传统理论及实务界应有的关照和证据资源的投放,而将这种特殊化虚拟生存仍混同于物理化证据的认定方法,势必只有较少电子数据作为证据被采纳

的资格,因此认定的有效性低下。究其原因,电子数据的产生具有专属或特定的网络语境。如若将其混同于物理世界的研究方法与形成它的系统相分离时,可能会变得无法理解。譬如,支付宝、蚂蚁花呗等即时通讯软件的司法认定常常成为困扰审判人员有效性认定的现实难题。在以支付宝、蚂蚁花呗等为典型的现代电子数据常常开启了阅读即焚的功能,用户在点击阅读后该信息自动删除或被覆盖,难以恢复,因此其作为证据被审判人员采纳的概率不高。

不仅如此,新型电子数据的流动性属性更是常常给传统证据固定性的认定带来较大的难度,因此证明力的有效性较为不稳定。如办理危害计算机信息系统安全刑事案件过程中,经常会涉及对计算机病毒、计算机程序功能、数据统计数量、数据同一性认定等问题。现实情况是,具有相应鉴定资质的机构较少,难以满足办案需求,难以对海量的、多元的、异质化的新型电子数据进行较为客观、充分和有效性认定。

除此之外,从新型电子数据的独立属性看,"高科技性、复合性、脆弱性"等新特征凸显[11],这也是司法人员主观认定电子数据的证明力低的重要原因。此种审判人员主观决定的经验采信机制,似乎从电子数据的形式合法性上观察是相对"保险"的,但实则披上了"法定证据效力优先"的合法性外衣,陷入更深的实质合法性危机。由于电子证据本身是一种数字化的证据,目前法律还不能穷尽所有的关联性法则,这就需要司法机关工作人员在司法证明活动中予以具体的适用。诸如此类的诸多新型特质势必使传统证据关联性认定规则的有效性大打折扣。

需要指出的是,在司法实践中新型电子数据关联度的认定,很大程度上取决于电子证据同案件事实是否存在客观内在联系及存在联系的程度[12]。而这一实质关联性认定的决定权恰巧掌握在庭审中的法官手里。这样庭审法官的知识结构及对电子数据的认知能力直接影响了认定结果的主观价值属性及电子数据证明力的有无及大小。从司法实践中司法人员对电子数据被应用及采纳的总体来看,采信质量并不高,"不说理"的现象较为普遍。显然,简单套用现实社会传统证据关联性认定的规则,势必导致其实质性审查面临有效性不足的窘境。

4 大数据背景下电子数据的规范性认定与排除

大数据背景下新型电子数据认定的照搬或移植模式给司法实践带来诸多负效应。其缘由恰是将新型的电子数据纳入传统证据认定的规则体系当中,从而遮蔽了新型电子数据独立性的生成规律,进而加重了司法机关对证据采信的主观化倾向。基于此,有效解决新型电子数据认定的路径应是规范化、法治化的方式与方法,试图构建网络证据认定的新规则体系。

4.1 完善规范性标准与原则,实现对电子数据真实性认定的网络合理性

大数据背景下新型电子数据真实性的认定规定更为复杂化,并衍生出双重标准和双重原则。此双重标准和原则的形成主要解决电子数据真实性认定的同一性及形式化困境。前项双重标准主要包括确定"视同原件"的标准[13]和客观化标准。后项双重原则主要指无差异原则和补强原则。

从"视同原件"的标准和"无差异"原则看,着重审查该电子数据原本形态是否保留了最初生成时的全部信息的确定状态。该项基本原则和标准的基本要义强调,对于决定新型电子数据的证明力有无及大小的关键看,只要是保留了最初生成时全部的事实信息和鉴定信息,无论其下载于何处,均构成原件。依此而言,不论是原件还是复印件,具有同等的证明力。

从"客观"化标准看,着重解决电子数据的整体性和动态性带来的真实性困境。为此,赞同学者主张构建客观化的采信机制,注重经验判断转向追求客观量化[14]。具体要求我们必须要遵循电子数据客观演进的认识论规律、尊重新型电子数据本身特有的独立属性和客观属性,进一步细化客观化采信机制的制度标准和可操作原则,纠正过往抽象化、模糊化的规则不足带来的审判人员恣意采信的主观化问题,并尝试建立法官对证据新型电子数据采信的说理机制,做到规范化采信。

从新型电子数据的"补强"原则看。该原则的构建着重解决电子数据形式要件认定上的瑕疵困境。解决上述形式瑕疵困境的具体路径,第一,可以通过创设关于电子证据的"孤证绝对否定、不同节点

印证、属性痕迹补强”[14]等规则，为新型电子数据形式要件的瑕疵认定提供可操作化的审查路径。第二，在前述条件缺位的情况下，可以增加法官对电子数据采信的说理机制，促进经验办案向知识办案转型。具体“补强”证据的效力途径可以通过自认、推定、辨认与鉴真和专家鉴定四种方式予以认定。对此相关的立法及司法实践均有规定。比如电子签名法第九条等。实践中，电子数据或其复制件通常要经过公证才能得到法院认可。整体而言，经过补强后的电子证据的证明力更强，被采纳的概率更大。

4.2 完善规范性取证方法和程序规则，实现对电子数据认定的网络合法性

从规范化的程序认定看，一是，完善规范化电子数据认证的制度，保障法官依法审查并判断。实践中，快播案的庭审涉及“辩护人对涉案淫秽视频的鉴定标准的判断和把握无明确依据，鉴定材料的来源和保管缺乏具体明确的记录”等一系列规范化鉴定程序问题。二是，坚持动态的规则演变理论。建议将电脑打印出文件，虽属法庭外的陈述，仍得作为证据，并可认为复制原本，该适用于独立电子数据认定的规则应得到肯定。同时，对电子数据的搜查、扣押应严格按照法律规定的程序，否则会对公民权利造成巨大伤害。有学者指出“在未来的刑事诉讼法修改时特别建立电子数据搜查、扣押的司法审查制度，[15]” 提高审判人员审判案件的责任心，促进规范化办案质量的有效提高。

从规范化的方法认定看，第一，培养以“方法型”法官为主导的认证主体。在程序认定的选择方法上，必须通过正当、合法的方法获得的电子数据才具有法律上的意义并被采纳。提高法官使用信息化的水平和能力，调整审判人员的知识结构，使其具有运用法治思维和选择法治方式认定电子数据的证明能力。第二，网络法律方法认定的清单，必须审查选择方法申请的理由做出明确的限定。在未来电子数据立法中应“侦察机关在搜查、扣押电子数据之后，应当就设备中存储的点至数据制作一个完整的‘比特流备份’，并将该备份材料交给辩护方”[15]，依此制作规范性审查的清单和具体标准。对此，最高法刑诉法《解释》九十三、九十四条对电子数据证明的合法性审查判断较少关注证据运输、存储等环节的问题，建议区分静态存储和动态演示两类电子证据来审查方法。但因有“排除合理怀疑”证明标准相冲突之嫌的，司法认定应保持谨慎态度，倾向从严适用为宜。第三，建立以审判为中心的网络证据改革的系列配套措施，进一步维护宪法和法律尊严，保障网络公民的合法权利。同时，限制网络侦查权的恣意行使，禁止网络非法取证的方式和手段，从根本上遏制网络非法电子证据生产的诱因并从源头上防止冤假错案的发生。对此，建议参照“两高三部”联合发布 2017 年《关于办理刑事案件严格排除非法证据若干问题的规定》，细化非法网络电子数据取证方法与程序规则，推进全面以网络审判为中心的程序制度的改革。

4.3 完善非法网络证据的排除程序，实现对电子数据认定的网络有效性

电子数据关联性认定的有效实现，依托于对“非法”的关联证据的规范化排除，规范性确定“非法”的排除理念与具体的排除事项。较于前者主要包括客观关联和主观关联两项。后者主要以列举的方式明细了具体的排除内容。

从“非法”网络电子数据的排除理念看，第一，基于客观关联理念的考量。如若将新的电子数据欲做入罪裁判时，必须首先考虑犯罪嫌疑人的网络身份和现实身份是否具有同一性，人机对应是排除合理性怀疑的基本限度。对此可以参照《刑事电子数据规定》第三十五条规定综合判断犯罪嫌疑人的双重身份的同一性问题，建立具体配套的规定。第二，基于实质关联性的考量。一般认为，与待证案件事实存在的联系越直接、越相关，证明力就越强；反之，证明力就越小。当存在多份电子证据指向同一待证事实的复杂情况下，经过公证的、鉴定的、自认的电子数据证明力相对较大。

从“非法”网络电子数据的具体排除事项看，原则上与可参照 2017 年 6 月 27 日“两高三部”联合发布的《关于办理刑事案件严格排除非法证据若干问题的规定》，使网络非法证据排除的规则更加明确，积极落实人权保障理念。如对“反对强迫自我归罪的权利、获得律师帮助的权利、住宅不受任意侵犯的权利等实质性程序瑕疵应采取强制排除的立场”[16]，但建议做出新的非法网络电子数据排除的创新规定。

第一，网络孤证绝对排除。相较于传统证据的

认定而言,电子数据“是由一系列命令或程序遵循一定及技术规则的海量电子数据组成的系统整体”[17]。实践也表明孤立的电子数据是不存在的。例如快播案的庭审的证据认定关键在于第三方协助的合法性、数据提取的及时性及数据提取的完整性问题。

第二,网络瑕疵证据不能补正并做出合理解释的情形。对此可以参照2016年《刑事电子数据规定》第二十七条内容,列举网络瑕疵证据的具体情形。当上述所列举的瑕疵情形出现并已补正或者做出合理解释的,原则上可以采用并赋予证明资格。相反则不具有证据资格和证明力,不得作为定案的根据。

第三,网络非法证据排除的法定情形,即不得作为定案根据的电子数据。可以参照《刑事电子数据规定》第二十八条规定,制定不得作为定案根据的电子数据的类型化标准及事项。一是确实能够认定电子数据确系篡改、伪造或者无法确定真伪的;二是确实影响电子数据电子数据真实性的增加、删除、修改等情形。三是其他无法保证电子数据真实性的情形。[18]”相反,如若进行排除合理怀疑,又附带充分的说明理由,应属于合法电子数据的认证的范围。

参考文献:

[1] 谢勇.论电子数据的审查和判断[J].法律适用,2014,(1):118.

[2] 李汉昌.论证据的合法性[J].法商研究,1999,(5):8-9.

[3] 叶自强.民事证据研究[M].北京:法律出版社,2002: 6.

[4] 何家弘,刘品新.证据法学[M].北京:法律出版社,2013:114.

[5] 刘品新.电子证据的关联性[J].法学研究,2016,(6):175-190.

[6] 陈浩. 即时通讯记录作为证据的司法认定研究[J].证据科学 2017(1):54 -64.

[7] [美]劳伦斯·莱斯格.代码 2.0:网络空间中的法律[M].李旭,沈伟伟,译.北京:清华大学出版社,2009:94.

[8] 南帆.虚拟的意义:社会与文化[J].东南学术,2009,(1):4-11.

[9] 王春.论电子证据补强规则确立及补强机制建构[J].湖北社会科学,2012,(8):160-164.

[10] lan M. Gahtan. Electronic Evidence [M].Toronto .Ontario: Carswell ,1999:138.

[11] 樊崇义,李思远.论电子证据时代的到来[J].苏州大学学报,2016,(2):99-106.

[12] 李主峰,刚继斌.从立法到司法:刑事诉讼中电子证据之认证[J].学术交流,2013,(7):35-37.

[13] 汪闽燕.电子证据的形成与真实性认定[J].法学,2017,(6):183-192.

[14] 刘品新.证与概率:电子证据的客观化采信[J].环球法律评论,2017,(4):126 : 109-127.

[15] 陈永生. 电子数据搜查扣押的法律规制 [J]. 现代法学,2014,(5):111-127.

[16] 易延友.非法证据排除规则的立法表述与意义空间—《刑事诉讼法》第54条第1款的法教义学分析[J].当代法学,2017,(1):38-55.

[17] 刘品新.论电子证据的定案规则[J].人民检察,2009,(6):37-40.

[18] 万春,王建平,吴孟栓,等.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理解与适用[J].人民检察,2017,(1):45-59 .

(本文编辑:朱晋峰)