法学研究 Chinese Journal of Law
Vol.41，No.2（2019）

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

胡　铭*

内容提要：互联网时代，电子数据在刑事审判中的重要性日益彰显。然而，在规则层面与审判实践层面，对电子数据的定位却呈现显著差异。通过对北大法意中国裁判文书库收录的2005－2015年网络假货犯罪案件裁判文书的分析发现，电子数据在刑事审判实践中存在定位泛化的问题，相关审查判断规则主要围绕电子数据的真实性展开，其关联性审查本质上也是真实性审查，其合法性审查亦主要是为了保障真实性。电子数据鉴定虽然被广泛适用，却未能发挥预期作用，而专家辅助人的引入尚处于初级阶段。为了准确定位电子数据并发挥其应有的作用，应在广义理解电子数据的基础上，在真实性与正当程序保障的价值权衡中，构建适应互联网时代需求的电子数据审查判断规则。

关键词：电子数据　证据体系　真实性　合法性　关联性

“互联网时代，尤其是社交网络、电子商务与移动通信把人类社会带入了一个以‘PB’（1024TB）为单位的结构和非结构数据信息的新时代。”〔1〕司法必须对此作出回应。例如，在技术层面，最高人民检察院2014年建设了电子数据云平台，实现首批全国检察机关31家电子数据实验室互联互通，用大数据服务办案。〔2〕在规则层面，2016年9月，最高人民法院、最高人民检察院、公安部联合发布《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》（以下简称“电子数据证据规定”）。在司法改革层面，继设立杭州互联网法院之后，〔3〕2018年7月，中央全面深化改革委员会决定增设北京互联网法院、广州互

* 浙江大学光华法学院、浙江大学司法鉴定中心教授。
本文系国家社科基金重大项目“深化司法体制改革和现代科技应用相结合的难点与路径研究”（18ZDA137）和国家“2011计划”司法文明协同创新中心成果。

〔1〕［英］维克托·迈尔—舍恩伯格、肯尼思·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社2013年版，第1页。

〔2〕参见许一航：《检察机关电子数据云平台建成使用》，《检察日报》2014年12月28日第1版。

〔3〕参见李英锋：《互联网法院：开启涉网纠纷解决新时代》，《人民法院报》2017年7月1日第2版。

联网法院；9 月，发布《最高人民法院关于互联网法院审理案件若干问题的规定》（以下简称“互联网法院审理案件规定”），成为司法主动适应互联网发展趋势的一项重大制度创新。

毋庸置疑，电子数据在互联网时代的审判实践中具有举足轻重的地位。关于电子数据的收集、保管、审查以及电子数据的真实性、合法性、关联性等问题，已经有不少研究成果。然而，现有成果主要从证据种类的角度展开研究，对于电子数据在刑事证据体系中的重要性，尚有认识上的不足；对于传统证据的电子化及其审查判断规则等问题，在研究深度上也有待加强。本文尝试在以审判为中心的刑事诉讼制度改革的背景下，重新审视电子数据在刑事证据体系中的定位与审查判断规则。

一、电子数据的法定化与传统证据的电子数据化

（一）作为法定证据种类的电子数据

2012 年修订后的刑事诉讼法第 48 条将电子数据列为法定证据种类之一，但未对电子数据作明确界定。《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》（以下简称“刑事诉讼法解释”）第 93 条指出电子数据具体包括：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。“电子数据证据规定”第 1 条则对电子数据作了明确界定：“电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。”这就意味着，以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等传统证据，被排除出了电子数据范畴。2019 年 1 月出台的《公安机关办理刑事案件电子数据取证规则》（以下简称“电子数据取证规则”）未对电子数据进行界定，实质上沿用了“电子数据证据规定”的相关规定。

值得注意的是，刑事诉讼法没有将电子数据予以单列，而是将其与视听资料并列为一类证据。有学者对此作了如下解释：“传统的视听资料与电子数据在其属性上既存在根本区别，但又存在密切的联系，新《刑事诉讼法》第 48 条采取将‘视听资料’和‘电子数据’合并作为一种证据种类进行规定的立法形式，既有效解决了司法实践中将电子数据作为证据使用的法律根据问题，也避免了在某些特殊情况下，如在计算机网页的视频文件，视听资料与电子数据难以截然分开的难题”。〔4〕这一解释恰好说明，电子数据与其他证据种类有明显交叉。实际上，不仅是视听资料，电子数据和书证、物证等其他证据也可能发生重合，如合同法第 11 条规定：“书面形式是指合同书、信件和数据电文（包括电报、电传、传真、电子数据交换和电子邮件）等可以有形地表现所载内容的形式。”对于证据种类交叉的问题，《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 116 条第 3 款明确指出：“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。”对于在一定程度上解决刑事诉讼中电子数据和视听资料难以界分的问题，这一规定具有借鉴意义。

（二）传统证据的电子数据化

从上述规定看，立法和司法解释采用的是狭义的电子数据概念，并力图将电子数据与其他传统证据种类予以区分。但是，从互联网时代的审判实践需求来看，广义的电子数据

〔4〕 陈光中主编：《〈中华人民共和国刑事诉讼法〉修改条文释义与点评》，人民法院出版社 2012 年版，第 52 页。

概念有其现实合理性。如“互联网法院审理案件规定”第 9 条在界定证据交换时，即采用广义的电子数据概念，即“当事人应当将在线电子数据上传、导入诉讼平台，或者将线下证据通过扫描、翻拍、转录等方式进行电子化处理后上传至诉讼平台进行举证，也可以运用已经导入诉讼平台的电子数据证明自己的主张”。〔5〕

从计算机及信息科学的角度看，电子数据，一般是指基于计算机应用、通信和现代管理技术等电子化技术手段形成的包括文字、图形符号、数字、字母等的信息。也就是说，从广义看，诸多信息都是以电子数据的形式存在，如以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人的供述和辩解等证据，都可以电子数据的形式存在，从而在技术层面等同于狭义的电子数据。也许正是看到了这一点，“电子数据证据规定”第 1 条在对电子数据作狭义界定时，也作了例外规定：“确有必要的，对相关证据的收集、提取、移送、审查，可以参照适用本规定。”但究竟什么是“确有必要”，却没有明确的解释，也很难进行科学的解释。

根据“电子数据证据规定”所确立的狭义电子数据概念进行分析，从本质上看，电子数据的主要特点不是“案件发生过程中形成的”，也不是“能够证明案件事实”，因为这两点和传统证据并无二致。电子数据的主要特点应当是“数字化形式存储、处理、传输的”信息。而物证、书证、证人证言等传统证据所承载的信息，都可以通过数字化处理转化为电子数据的形式。互联网法院的审判活动更是要求将传统证据转化为数字化证据，以便进行质证、认证。也就是说，在互联网时代，不仅大量证据以电子数据的形式存在，而且一些传统证据也必须转化为电子数据。这两类电子数据虽然存在差异，但由于二者均具备电子数据的属性，故应一体适用电子数据的审查判断规则。然而，“电子数据证据规定”对电子数据作了狭义界定，其确立的审查判断规则也是建立在狭义电子数据概念的基础之上。这样处理或许有简便之利，但恐怕不符合审判实际，也难以满足智慧司法、互联网审判的要求。

因此，以广义概念来界定电子数据并在此基础上形成相应的审查判断规则，恐怕是更加符合审判实际、也更加合理的选择。即，只要与计算机及信息技术相关的能够证明案件事实的材料，原则上均应纳入电子数据范畴，并应在此基础上形成基于互联网、数字化时代要求且符合电子数据自身特点的审查判断规则。

二、从裁判文书看电子数据在刑事证据体系中的定位

（一）数据来源与样本情况

本研究以网络假货犯罪（网络售假案件中涉及侵犯知识产权的犯罪）案件的电子数据应用情况为分析样本，这是考虑到此类案件的审判涉及电子数据的情况较多，尤其是网络购物平台涉及假货犯罪的案例具有典型性。而且笔者所在的杭州是互联网法院和阿里巴巴公司所在地，以此类案件为样本，便于开展相关调研和访谈工作。

〔5〕“互联网法院审理案件规定”虽然只适用于北京、广州、杭州的互联网法院，且不适用于刑事案件，但该规定对于完善互联网时代的审判制度和证据规则显然具有参考意义。

案例的来源是，通过北大法意的中国裁判文书库（http://www.lawyee.org/Case/Case.asp）进行检索，提取2005－2015年相关裁判文书的全样本，共计877个案例。〔6〕排除24个无效样本（审理段或证据段中为空白内容，或者是二审法院对一审法院审理的事实及证据进行确认而无实质内容），有效样本共计853个。〔7〕

将所有这些案例编号并输入SPSS软件，进行统计分析。为对比法律修改和司法解释出台对司法实践的影响，特别是2016年“电子数据证据规定”出台对司法实践的影响，又随机选取了该规定实施后2016－2017年的30个案例，作为对照样本。〔8〕

如图1所示，样本中案件数量排名前五的罪名是：销售假冒注册商标的商品罪、侵犯著作权罪、假冒注册商标罪、侵犯商业秘密罪以及销售侵权复制品罪。其中，以销售假冒注册商标的商品罪为涉案事由的案件数量最多，远远大于其他种类。

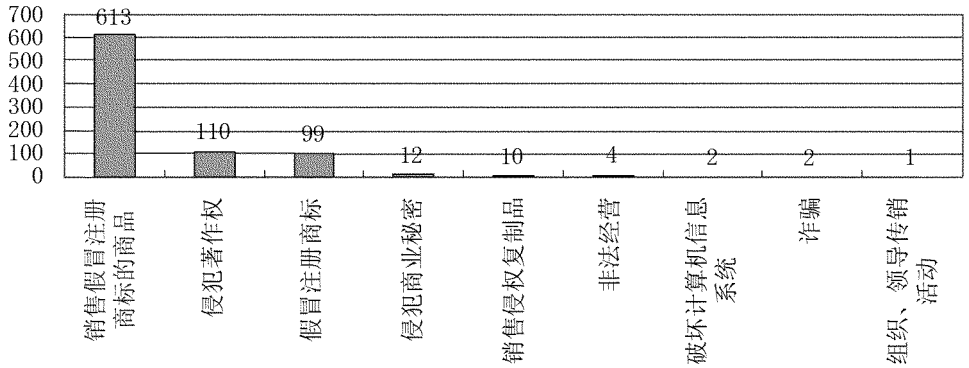

图1　罪名分布情况

（二）电子数据的取证方式与在法庭上展示的形式

1．电子数据的取证方式

从裁判文书中可以看出，涉案的电子数据通常并不唯一，表现形式也很多样，因此，对不同类型的电子数据会运用不同的取证手段。对样本案件中不同取证方式出现次数的统计结果见下文图2。打印是侦查机关采用最多的取证方式，通过打印输出方式取证有148件次。这主要是因为打印方式简便易行，但其单纯通过打印方式取证，也很容易引起争议。类似的取证方式还有直接导出、截图，分别有128、105件次。

观察2016年“电子数据证据规定”出台后的案例，取证方式与上述情况基本一致。这可能与“电子数据证据规定”对复印件、打印件等便捷取证方式的肯定有关。其第18条规定：“人民法院、人民检察院因设备等条件限制无法直接展示电子数据的，侦查机关应当随案

〔6〕 检索方式如下：在案例高级检索处点击检索说明栏的“参考案由”，在案由检索区的案由树中勾选“刑事→破坏社会主义市场经济秩序罪→侵犯知识产权罪”，分别进行以下检索：（1）全文关键词“网店 假”＋案由“侵犯知识产权罪”；（2）全文关键词“电脑 假”＋案由“侵犯知识产权罪”；（3）全文关键词“互联网 假”＋案由“侵犯知识产权罪”；（4）全文关键词“网络 假”＋案由“侵犯知识产权罪”－全文关键词“网络联系”；（5）全文关键词“网上 假”＋案由“侵犯知识产权罪”；（6）全文关键词“微信 假”＋案由“侵犯知识产权罪”。

〔7〕 一审裁判文书809份，二审裁判文书44份。

〔8〕 2016－2017年的网络假货犯罪案件裁判文书已上网的数量较少，在统计学上不具有显著意义，但从个案角度可以反映一定的实际情况。

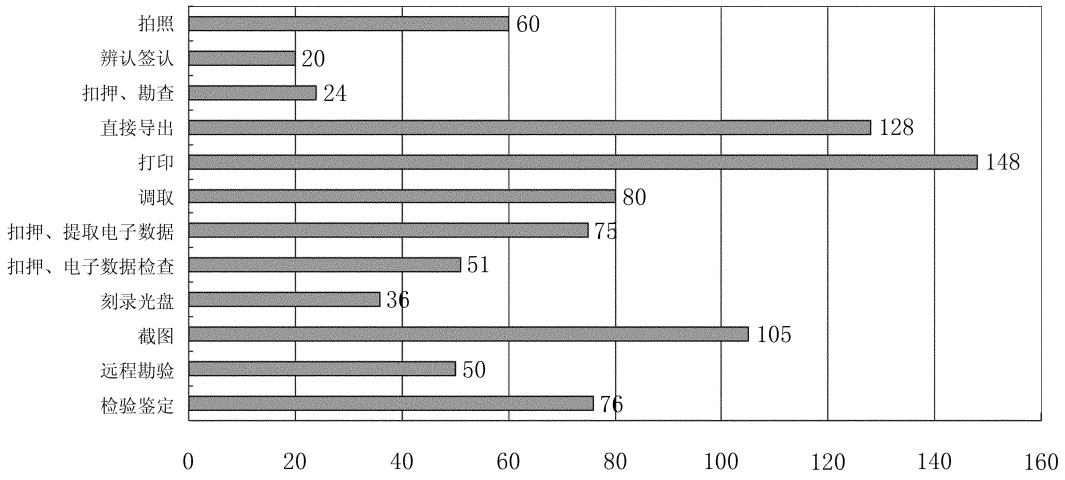

图 2　取证方式的运用情况

移送打印件，或者附展示工具和展示方法说明”。

在取证方式中，向第三方有关机构调取证据仅有 80 件次，比笔者预期的要少。具体取证情况例如：向腾讯财付通后台调取交易数据；向淘宝公司调取涉案网店信息；向支付宝公司调取账号注册信息及交易记录；向人人网调取账号充值记录；向奇虎公司调取云盘存储数据等。第三方机构通常向侦查机关提供数据光盘或者盖章的书面记录，上述材料的获得和真实性十分依赖第三方机构的配合与诚信。此外，在样本中只有一例显示对电子数据作了公证，可见在电子数据取证中很少使用公证方法。

2．电子数据在法庭上展示的形式

统计结果显示，样本中 57.21% 的案件（488 个），公诉机关提交了电子证据。其中，法院或公诉机关将这些证据明确认定为电子数据的占 17.01%（83 个）；也有将其归为书证（40 个）、视听资料（4 个）、勘验笔录（1 个）的情况；而大多数法院即 73.77% 的法院（360 个），未对此类证据作直接归类。这表明大量司法机关并未将电子数据定位为独立的证据种类，而是将其与其他证据种类相混同，适用类似的审查判断规则。

即使在 2012 年修订刑事诉讼法，明确将电子数据规定为法定证据种类之后，电子数据的表现形式也并不清晰。如在泰勒、沈某等销售假冒注册商标的商品案中，判决书列明了公诉机关作为电子数据举证的证据：“广州市公安局经济犯罪侦查支队四大队穗公经电检 2012005 号电子物证检验报告，证明公安机关对在广州市番禺区祈福新村 B 区十三街 B112 号提取的兼容组装电脑主机一台进行电子物证检验，并将‘DailyOrders. csv’电子数据刻录到光盘。”〔9〕该案并没有将移动硬盘、电脑、电子邮件、网页截图等纳入电子数据的举证种类，而是将其纳入物证、书证和勘验、检查笔录等证据种类。

从 2012 年电子数据成为法定证据种类之后的裁判文书看，将电子数据作为专门一类证据的比例明显提高。但案例显示，检察官更多是从有利举证的角度来对证据进行归类；并且在不少案例中，是围绕待证事实来列举证据，而没有明确按照法律的分类来举证。在

〔9〕 广东省高级人民法院（2013）粤高法刑二终字第 42 号刑事判决书。

2018 年 6 月笔者于浙江大学对杭州市公诉检察官进行的个别访谈中，检察官表示，不少被告人及其律师对电子数据的信任度不高，只有将电子数据转化成书证等传统证据才能沿用传统的质证方法。因此，将电子数据归入传统证据种类是常见现象，也并不影响电子数据的证明力。

裁判文书显示，公诉机关提交的电子数据主要有以下几种形式：（1）实物形式，如电脑、硬盘、光盘等。只有一成左右的案件中存在电子数据的原始载体，三成左右的案件中存在电子数据的复制件（如光盘）。（2）书面形式，如打印件、扣押清单、截图、各类工作记录等。在接近一半的案件中，电子数据以打印件的形式存在；在超过六成的案件中，电子数据完全以书面形式呈现。（3）笔录形式，这表现为与电子数据紧密相关的各种笔录，如搜查笔录、检查笔录、辨认笔录、提取笔录、远程勘验笔录、现场勘验笔录等。（4）鉴定意见形式，实际表现为鉴定意见书、鉴定说明书、鉴定结论书、检查意见书等。这些统计表明，向法庭提供原始载体的比例显然偏低，甚至连提交复制的光盘和相关笔录也没有成为普遍做法。

在“电子数据证据规定”出台以后，电子数据的举证形式仍然延续了原来的便利做法。这显然与“电子数据证据规定”的要求不一致。该规定第 22 条第 1 项明确指出，审查电子数据的举证形式应主要围绕以下事项展开：是否移送原始存储介质；在原始存储介质无法封存、不便移动时，有无说明原因，并注明收集、提取过程及原始存储介质的存放地点或者电子数据的来源等情况。值得注意的是，在审判阶段，居然有超过 60% 的案件，电子数据最后完全是以转化为控方书面材料的形式存在的；还有部分案件中是以公安机关出具“证明”“情况说明”“笔录”等来证明相关电子数据的存在。这表明，电子数据在法庭上展示的形式与法律、司法解释的规定有较大差距。

三、以真实性为导向的电子数据审查判断

（一）电子数据审查判断的表象：围绕真实性、合法性、关联性展开

审查判断证据，一般围绕证据的真实性、合法性、关联性来展开。电子数据的审查判断同样如此，只是侧重有所不同。从裁判文书看，对电子数据的质证主要包括四类（表 1）。

表 1　对电子数据的质证类型

案例	控方举证	被告方质证理由及类型	法官不采信质证的理由
陈某销售假冒注册商标的商品案〔10〕	网页截图、注册资料、交易明细记录、支付宝账户等书证及视听资料等	不真实：仅将网店销售记录导出打印统计，没有进行审计，无法证实该证据的客观、公正、真实	数据从服务器中提取，由淘宝网及支付宝公司提供，无法删改
符某等销售假冒注册商标的商品案〔11〕	司法鉴定意见书及其附件所列的交易明细表等	真而不实：犯罪金额中应当扣除虚拟交易（刷单）金额和快递费	没有事实依据

〔10〕 参见广东省广州市海珠区人民法院（2012）穗海法刑初字第 302 号刑事判决书。

〔11〕 参见上海市第二中级人民法院（2013）沪二中刑（知）终字第 1 号刑事判决书。

续表

案例	控方举证	被告方质证理由及类型	法官不采信质证的理由
顾某、张某销售假冒注册商标的商品案〔12〕	某某公司出具的材料，证明账户的注册人为张某，银行卡照片、活期存款历史明细清单等	无相关性：张某只是借身份证给他人开网店，不知道卖出货物的真假，也不知道销售的数量	张某与被告人顾某以及相关证人的证言能够相互印证
黄某销售假冒注册商标的商品案〔13〕	公安机关出具的扣押物品、文件清单及情况说明，司法鉴定意见书和货值金额情况、补充说明等	程序违法：立案、扣押赃物、鉴定的程序违法及公安机关超越职权	对于本案的侦破情况，公安机关已在工作情况中作详细阐述

在样本案件中，辩护方对控方提交的电子数据的质疑内容主要包括：电子数据的原始性、真实性；依电子数据得出的犯罪数额是否准确；电子数据提取、存储和固定等程序的合法性；电子数据鉴定意见的合法性，等等。然而，辩护方异议获得法院支持的比例极低。从获得法院支持的少量个案看，有效的质证主要集中于对犯罪数额的异议。比如，辩护方准确分析电子数据所含信息，致使法院对犯罪数额作了从轻认定；对提取电子数据时程序严重不合法提出质证意见，从而否定了据此认定的犯罪数额。针对辩护方提出的质疑，多数裁判文书未详细说明理由，往往笼统采信控方证据，比如，“本院认为，上述证据间相互关联、相互印证，证据具有真实性、合法性、有效性，可予以认定。”〔14〕这种表述显然难以令辩护方信服。

围绕电子数据的真实性、合法性、关联性展开质证，得到了“电子数据证据规定”第 2 条的明确肯定：“人民检察院、人民法院应当围绕真实性、合法性、关联性审查判断电子数据”。但这只是规则层面的表象，从裁判文书看，真实性一直是电子数据审查判断的重点，合法性与关联性审查虽然在“电子数据证据规定”出台后有所增加，但仍然主要是为真实性审查起辅助作用。

（二）以信息的真实性为重点展开审查判断

从裁判文书看，法庭质证主要围绕电子数据的真实性来展开。辩护方对真实性的质疑，如表 1 所示，主要有两类：（1）电子数据不真实，包括电子数据是否为虚假信息或被篡改等。质疑电子数据不真实，很大程度上是因为控方在法庭上举证采用的是打印件、情况说明、笔录等形式，这样做虽然简便、直观，却很难将电子数据所承载的信息以充分、可信的方式展现出来。但是，此类质疑的成功率并不高。（2）电子数据真而不实，这主要表现为，在大量案件中被告方对犯罪事实无异议，但对犯罪数额有不同意见。例如，在耿某销售假冒注册商标的商品案中，律师对被告人构成犯罪没有异议，但对犯罪数额提出如下意见：“耿某在经营网店过程中，为争揽客户采取了在第三方网站进行虚假交易的模式来提高

〔12〕 参见上海市浦东新区人民法院（2011）浦刑初字第 2079 号刑事判决书。

〔13〕 参见上海市闵行区人民法院（2012）闵刑（知）初字第 83 号刑事判决书。

〔14〕 “董某、毛某销售假冒注册商标的商品案”，福建省福州市鼓楼区人民法院（2014）鼓刑初字第 74 号刑事判决书。

网店信誉度与知名度，故存在应予扣除的虚假交易部分计人民币 13111.6 元。”法院采纳了质证意见：“辩护人提交的虚假交易记录，证明耿某的淘宝网店销售记录中存在虚假交易部分；辩护人提交的耿某淘宝网店销售记录，证明鉴定金额存在计算错误部分。”〔15〕

围绕电子数据的真实性展开审查判断，有其必然性。一方面，我国的刑事证据体系本身就以保障真实性为主要宗旨。电子数据虽然是新型证据种类，但我国的电子数据证据规则受上述理念影响，也主要围绕保障真实性来展开。另一方面，电子数据的真实性审查与传统证据有较大差别。例如，一个书证和一个电子文档，从内容上看是很相似的，而且可以相互转化，但在真实性的审查判断上，二者却有很大差异。比如，对于书证的审查判断，主要从其来源、是否原件、具体内容等角度进行，而电子文档包含有副本文件、位置信息、系统信息等多个数据信息；书证易被损毁但不易篡改、伪造、变造，而电子文档即使被删除也会留下可还原的信息从而很难被彻底抹去，却很容易被修改，难以区分是原始文档还是曾被篡改、伪造、变造的文档。这些技术特点决定了，电子数据的真实性相比传统证据更容易被质疑。因此，在司法实践中，要证明电子数据的真实性，相关基础性工作就更为复杂，例如证据保管链的鉴真等。

在规范层面，“刑事诉讼法解释”第 93 条明确规定了电子数据的审查要点，也主要体现了保障真实性的倾向：（1）是否是原始介质；（2）是否有文字说明和签名；（3）是否附有笔录、清单；（4）是否符合技术规范；（5）是否完整；（6）是否真实；（7）与案件事实有无关联；（8）是否全面收集，等等。“电子数据证据规定”第 22 条至第 28 条对电子数据的真实性、完整性、网络身份与现实身份的同一性、瑕疵补正等作了详细规定，体现了对保障真实性的具体要求。〔16〕上述司法解释从取证过程、举证形式、内容本身、完整性审查等方面规定了较为详实的真实性审查规则，这与裁判文书所展示的电子数据真实性审查简单化、与传统证据审查判断趋同化，有较大差异。

虽然司法解释的相关规定实际上给了被告方作详细比对从而发现取证瑕疵的机会，但司法实践中针对电子数据的质疑，实效并不明显。这是因为：一方面，“电子数据证据规定”第 20 条确立了庭前补正规则，即法院庭审前发现电子数据不符合相关要求，“应当”通知检察院。这就给了控方通过说明情况或补充手续等方式补正瑕疵的机会。另一方面，法院易偏向控方，在裁判文书中往往采用模糊表述来否定此种质疑。如徐某等诈骗案的裁判文书即指出：“公安人员对扣押的伪基站、设备进行检查，符合‘电子数据证据规定’的要求，并有检查人员的签名，程序合法。辩护人该意见与事实不符，本院不予采纳。”〔17〕

（三）电子数据的关联性审查本质上仍然是保障真实性

电子数据的关联性，是指电子数据所承载的信息与案件事实存在客观的内在联系，从而能够起到证明作用。这种内在联系具体表现为，电子数据所承载的信息应当是证明待证

〔15〕 上海市第二中级人民法院（2012）沪二中刑（知）终字第 2 号刑事判决书。

〔16〕 对于电子数据是否真实，“电子数据证据规定”第 22 条指出应当着重审查以下内容：（1）是否移送原始存储介质；在原始存储介质无法封存、不便移动时，有无说明原因，并注明收集、提取过程及原始存储介质的存放地点或者电子数据的来源等情况；（2）电子数据是否具有数字签名、数字证书等特殊标识；（3）电子数据的收集、提取过程是否可以重现；（4）电子数据如有增加、删除、修改等情形的，是否附有说明；（5）电子数据的完整性是否可以保证。

〔17〕 广西壮族自治区柳州市柳南区人民法院（2016）桂 0204 刑初 449 号刑事判决书。

案件事实的全部或一部分信息。关联性“旨在向事实裁判者展现将有助于作出决定的全部信息。对不相关证据的排除也遵从于发现事实真相的价值，因为它使事实认定者的注意力集中于适当的信息，且仅仅集中于适当的信息。”〔18〕从本质上看，电子数据的关联性也体现了保障真实性的价值趋向。

网络空间中的任何行为都会在虚拟空间留下痕迹，从而为查明真相提供重要信息。但是，这些信息究竟是谁留下的、是怎么留下的等问题，却引发了与现实世界的关联性疑问。比如，在裁判文书中，QQ 聊天记录是十分常见的电子数据，其记载的内容虽然明确，但被告人常常辩称该记录与自己无关：QQ 被盗号；别人也有密码；不是自己说的话；所说的话并非真实意思表达，等等。司法实践显示，电子数据的关联性审查主要分为两个方面：一是从内容来看，电子数据所承载的信息是否同案件事实有关；二是从载体来看，主要审查虚拟空间的身份、行为、介质、时间与地址同物理空间中的当事人或其他诉讼参与人能否关联起来。〔19〕上述关联性审查实际上是一个推理过程，即由电子数据的内容及虚拟空间的身份、行为、介质、时间与地址等已知的判断，推导出电子数据与案件事实具有相关性。这是审查电子数据关联性的主要方法，也是电子数据审查判断保障真实性的难点所在。由于关联性主要是一个经验问题，在很大程度上依赖于经验与常识，这就使得对关联性审查很难提出具有可操作性的标准。因此，如前文表 1 所示，在裁判文书中，对于电子数据的关联性审查，很容易作含糊其辞或简单化的处理。

需要指出的是，电子数据的关联性包括直接关联和间接关联两种形式。直接关联类似于传统证据关联性中的直接与待证案件事实相关；间接关联则是指，因无法准确把握因果关系，故不能用该关联性直接认定案件事实。例如，大数据证据的运用便具有间接关联的特点。在具体的司法证明中，全样本数据所反映出的规律，在多大程度上能够影响案件事实的证明，目前仍然缺乏足够的实证支撑，而仅能体现间接层面的关联性。

（四）电子数据的合法性审查围绕保障真实性来展开

电子数据的使用应符合正当程序并保障被追诉人的基本权利，这是电子数据合法性审查的应有内涵。但裁判文书显示，辩护方对电子数据合法性的质疑往往比较宽泛，多以“没有鉴定人员签名”“送检人显示为无”这样的取证瑕疵以及没有多少具体线索的一般性程序不合法为理由。质疑的结果多为两种情况：一是法院按照普通物证的非法证据排除进行判断，例如，“公安机关虽未严格依照有关规定的程序提取涉案电子数据，但……证据存管是以完全封闭方式……相关证据能相互印证……对电子数据的制作提取过程……公安机关作出了必要说明……属于合理解释”。如此一来，控方较容易对证据的合法性进行补正。二是以辩护方就非法取证问题未提供线索或者材料为由予以否定。裁判文书显示，辩护方对合法性提出异议的成功率比较低，此类辩护意见并未有多少实际效果。

从规范层面看，现有的电子数据合法性审查判断规则主要围绕保障真实性来展开。“刑事诉讼法解释”第 93 条对于电子数据的合法性仅笼统提到“收集程序、方式是否符合法律及有关技术规范”，缺乏具体的审查程序和标准。“电子数据证据规定”第 24 条对电子数据

〔18〕［美］戴维·伯格兰：《证据法的价值分析》，张保生、郑林涛译，载何家弘主编：《证据学论坛》第 13 卷，法律出版社 2007 年版，第 244 页以下。

〔19〕参见刘品新：《电子证据的关联性》，《法学研究》2016 年第 6 期，第 175 页。

的合法性审查作了四项具体规定，但内容主要涉及对电子数据真实性而非正当程序的保障。[20] 其中，第 1 项是审查侦查人员人数及取证方法是否符合技术标准。要求取证须由两名以上侦查人员进行，并无法律上的明确依据，是否有必要也存在争议；是否符合技术标准，主要涉及电子数据的真实性是否得到保障。第 2 项至第 4 项分别规定了笔录记载情况，见证和过程录像，存储介质、数据备份和录像等情况，这些内容在侦查取证的合法性问题中并非关键所在，也不涉及基本权利，反而是对保障电子数据的真实性具有一定的意义。

通过裁判文书的对比可以看到，在 2016 年以后的案例中，被告人及其律师质疑电子数据合法性的比例明显提高。在 2016－2017 年的 30 个案例中，有 4 个案例辩护方明确提出电子数据的合法性问题，而在此前的 800 多个案例中，仅有 8 个案件涉及电子数据的合法性问题。当然，这与“电子数据证据规定”明确强调电子数据合法性的要求是有关系的。在这 4 个案例中，辩护律师都是依据“电子数据证据规定”提出质疑的。如在林某等非法经营案中，辩护律师指出：“电脑账单是确定犯罪数额的主要证据，而储存该电脑账单的电脑主机公安机关不是直接从被告人处扣押，而是由安监部门移送。电脑账单属电子数据，其收集和提取应严格按照‘电子数据证据规定’操作，但本案电脑账单的收集和提取未按该规定操作。”法官未认可该意见：“‘电子数据证据规定’是从 2016 年 10 月 1 日起施行，而本案电脑账单是在 2016 年 6 月 21 日提取，故该规定并不适用于本案。”[21] 这一案件从侧面说明，侦查人员的取证行为存在不规范，出台司法解释对电子数据的合法性审查提出明确要求，对于严格电子数据取证的合法性、规范性显然是有所助益的。

四、电子数据的检验鉴定与真实性审查盲点

有别于传统的证据种类，电子数据的真实性审查与现代科技紧密相关。为保障电子数据的真实性，无外乎两条路径：一是通过严格的正当程序规定，对电子数据的收集、保存等进行规制；二是通过检验、鉴定、专家意见等技术手段来审查电子数据的真实性。对于前者，“电子数据证据规定”等司法解释作了积极探索，但和司法实践的需求仍有较大差距。而后者正成为司法实践中电子数据真实性审查的难点，并存在诸多盲点。

（一）真实性审查与电子数据的司法鉴定

电子数据的司法鉴定与传统证据的司法鉴定有较大区别。裁判文书显示，电子数据的司法鉴定被广泛使用，但遭遇了较多质疑，未达到预期作用。在 488 个明确列明有电子数据的案例中，241 个案例存在司法鉴定意见书，占了将近 50%。在是否有鉴定人出庭的统计中，明确提到鉴定人出庭对电子数据进行说明的，占14.34%（70 个）。与一般案件相比，

〔20〕“电子数据证据规定”第 24 条规定的审查判断内容包括：（1）收集、提取电子数据是否由二名以上侦查人员进行，取证方法是否符合相关技术标准；（2）收集、提取电子数据，是否附有笔录、清单，并经侦查人员、电子数据持有人（提供人）、见证人签名或者盖章；没有持有人（提供人）签名或者盖章的，是否注明原因；对电子数据的类别、文件格式等是否注明清楚；（3）是否依照有关规定由符合条件的人员担任见证人，是否对相关活动进行录像；（4）电子数据检查是否将电子数据存储介质通过写保护设备接入到检查设备；有条件的，是否制作电子数据备份，并对备份进行检查；无法制作备份且无法使用写保护设备的，是否附有录像。

〔21〕浙江省玉环市人民法院（2017）浙 1021 刑初 285 号刑事判决书。

这个比例相当高,[22] 体现了司法鉴定对于电子数据审查判断的独特作用。

电子数据本身具有科技属性，审查其真实性离不开以科技为基础的鉴定。这种证明价值建立在特定科学知识或者技术原理之上的鉴定意见，因其体现相关专业知识并由得到国家资质认可的专业技术人员作出，故能够有效弥补侦查人员和司法人员对相关专业知识的欠缺。司法解释也特别强调鉴定对于电子数据审查判断的重要性。“刑事诉讼法解释”第 93 条第 2 款规定：“对电子数据有疑问的，应当进行鉴定或者检验。”需要注意的是，司法解释将电子数据的鉴定和检验并列在一起。从内涵来看，鉴定和检验是不一样的。鉴定的主体是具有鉴定资质的独立第三方，而检验的主体是侦查机关指定的机构。但是，从真实性审查的角度看，两者是共通的，即均为运用专门知识对电子数据的真实性进行审查。

裁判文书显示，电子数据的鉴定结果在个案中被质疑的情况较为普遍。这与电子数据鉴定的特点和现状有关：（1）电子数据的司法鉴定并未纳入司法行政机关统一管理的三大类鉴定，从而对其缺乏有效管理。根据全国人大常委会《关于司法鉴定管理问题的决定》第 2 条，明确列举并纳入统一管理的是三大类司法鉴定，即国家对法医类、物证类、声像资料司法鉴定业务的鉴定人和鉴定机构实行登记管理制度。[23] 电子数据的司法鉴定并不在上述范围内，这导致对电子数据司法鉴定的管理呈现混乱状态：有的地方将其归入声像资料类，有的地方根本就没有进行电子数据鉴定的司法鉴定机构，更多的地方则以公安检察机关工作人员的检验来代替鉴定。（2）要求专门知识，但缺乏统一的鉴定资质要求。在实践中，既有鉴定机构出具的鉴定意见，也有某些专门机构出具的鉴定证明书，还有涉案单位出具的说明材料。如在顾某、张某销售假冒注册商标的商品案中，被告方对博邦公司的鉴定资质提出质疑。法院最终认定：“博邦公司出具的鉴定情况说明并非刑事诉讼证据中的鉴定结论，其内容为被害单位的辨认，其证据属性应当归类于刑事诉讼证据中的被害人陈述……故对博邦公司出具的鉴定情况说明予以采纳。”[24]（3）关于电子数据检验的具体办法，“电子数据证据规定”第 17 条第 2 款仅规定：“具体办法由公安部、最高人民检察院分别制定。”这意味着公安机关和检察机关对于电子数据的检验握有掌控权。在 2017 年 8 月笔者于浙江大学对杭州市公安局侦查人员进行的个别访谈中，侦查人员坦言，他们依据的标准就是内部规定，而不是司法解释。被追诉方对这些内部规定显然缺乏了解，也无法获得有效救济。（4）电子数据鉴定的专业性很强，法官缺乏必要的审查判断能力。通过对样本的相关性统计，对电子数据是否进行鉴定，对法官是否采纳电子数据的影响微乎其微。[25] 之所以出现这种现象，可能与法官审查判断电子数据的能力总体较弱有关。无论对电子数据是否进行鉴定，法官都较难实质性地对其进行有效审查。从统计数据看，法院显然极度偏向采纳控方提交的电子数据（采纳比例高达 96%），所以是否进行鉴定对电子数据的采纳

〔22〕 据浙江省司法厅统计，2013 年该省办理涉及诉讼的司法鉴定 36832 件，鉴定人出庭作证只有 167 次，出庭率仅为 0.45%。参见俞世裕、潘广俊、林嘉栋、余晓辉：《鉴定人出庭作证制度实施现状及完善》，《中国司法鉴定》2014 年第 5 期，第 167 页。

〔23〕 2015 年，最高人民法院、最高人民检察院、司法部联合出台的《关于将环境损害司法鉴定纳入统一登记管理范围的通知》，将环境损害司法鉴定也纳入了统一管理。

〔24〕 上海市第一中级人民法院（2012）沪一中刑（知）终字第 3 号刑事判决书。

〔25〕 两者相关性的显著性 P 值 = .55 > 0.05（P 表示显著性水平），表明鉴定情况与法院采纳电子数据情况的相关性不显著。

几乎没有影响。

（二）专家辅助人的准确定位及其作用的发挥

专家辅助人的引入，为审查电子数据的真实性提供了重要支持。但分析样本发现，在电子数据的审查判断中，司法实践尚未对专家辅助人作出准确定位，其作用也未充分发挥。

裁判文书统计显示，电子数据的鉴定包含三种形式：（1）一般意义上的司法鉴定；（2）侦查机关指定的机构出具的检验报告；（3）具有专门知识的人的意见。由于电子数据的真实性审查涉及专门知识，这就为专家辅助人发挥作用提供了广阔空间。专家辅助人的引入，也可以有效解决电子数据司法鉴定所面临的鉴定机构与鉴定人资质等问题。

裁判文书显示，在司法实践中，法官对这些专家意见给予了等同于司法鉴定意见的地位。但是，从规范层面看，专家辅助人意见并不是一种证据，在电子数据领域也应如此。“电子数据证据规定”第 26 条第 3 款规定：“公诉人、当事人或者辩护人、诉讼代理人可以申请法庭通知有专门知识的人出庭，就鉴定意见提出意见。”〔26〕也就是说，专家辅助人的制度定位是协助质证，这就极大地限制了专家辅助人的作用。笔者对此曾作过专门研究，主张“如果要充分发挥专家辅助人在庭审中的作用，就需要超越质证权，从整体上重新思考专家辅助人的定位，而其中的关键是专家辅助人意见的证据能力问题”。〔27〕

至于电子数据的检验报告，应当统一纳入专家辅助人制度。“电子数据证据规定”第 17 条第 1 款规定：“对电子数据涉及的专门性问题难以确定的，由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。对于人民检察院直接受理的案件，也可以由最高人民检察院指定的机构出具报告。”该规定进一步明确了电子数据的检验报告制度，即由侦查机关指定的机构出具检验报告，这与“电子数据取证规则”第 55 条是一致的。“电子数据证据规定”第 26 条第 4 款规定：“对电子数据涉及的专门性问题的报告，参照适用前三款规定。”〔28〕这就使得检验报告具有了与司法鉴定和专家意见同等的作用，在电子数据的取证、举证抑或质证中都可以广泛应用。侦查机关指定的机构显然不是司法鉴定机构，否则没有必要作此特别规定；也不应当是侦查机关的内部机构，否则很难摆脱自侦自检的质疑；而且侦查机关本身有鉴定机构，也没有必要将侦查机关的鉴定机构纳入这里的指定机构。基于控辩平等对抗的诉讼构造，由指定机构的专家出具的检验报告，应当统一作为专家辅助人意见来适用和规范，并解决其证据能力问题。

（三）现代科技带来的真实性审查盲点

电子数据的真实性审查要善于利用互联网、云计算、人工智能、区块链等技术手段。“互联网法院审理案件规定”第 11 条对此作了积极探索，即通过电子签名、可信时间戳、

〔26〕 与“电子数据证据规定”不同，“互联网法院审理案件规定”第 11 条第 3 款规定：“当事人可以申请具有专门知识的人就电子数据技术问题提出意见。互联网法院可以根据当事人申请或者依职权，委托鉴定电子数据的真实性或者调取其他相关证据进行核对。”即当事人可以申请专家辅助人出庭，无需以存在鉴定意见为前提。

〔27〕 胡铭：《鉴定人出庭与专家辅助人角色定位之实证研究》，《法学研究》2014 年第 4 期，第 205 页。

〔28〕 “电子数据证据规定”第 26 条第 1 款至第 3 款规定的内容如下：公诉人、当事人或者辩护人、诉讼代理人对电子数据鉴定意见有异议，可以申请法院通知鉴定人出庭作证。法院认为鉴定人有必要出庭的，鉴定人应当出庭作证。经法院通知，鉴定人拒不出庭作证的，鉴定意见不得作为定案的根据。对没有正当理由拒不出庭作证的鉴定人，法院应当通报司法行政机关或者有关部门。公诉人、当事人或者辩护人、诉讼代理人可以申请法庭通知有专门知识的人出庭，就鉴定意见提出意见。

哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证。然而，技术上的进步仍然难以避免诸多盲点。比如，云技术环境给电子数据取证带来的深远影响和现实困难。在云技术环境下，世界任何角落的某个用户都可以利用云服务实施网络诈骗、身份窃取等犯罪活动，而不留下能够追踪其真实身份的信息。云平台的数据如何收集提取、分析、定位等都是难题，此外还涉及跨境管辖权、安全基础设施建设、云服务商责任等问题。再如，VPN（虚拟专用网络）、VPS（虚拟专用服务器）带来的电子数据取证难问题。在 2018 年 7 月笔者于浙江大学与阿里巴巴安全部门技术人员的个别访谈中了解到，在 VPN、VPS 环境下，IP 地址随时可以更换从而很难查实，这会给网络犯罪案件的电子数据取证带来重重困难。

五、真实性与正当程序保障并重的电子数据审查判断规则

上述分析表明，为因应互联网时代的要求和司法实践的需要，应对电子数据作广义定位：以数字化方式存在的可用于证明案件事实的信息。在此基础上，应当在真实性与正当程序保障的价值权衡中，确立电子数据的审查判断规则。

（一）规范层面：共性规则与差异性规则

规范层面的重点应当是，辨识哪些是电子数据与传统证据的共性规则，哪些是电子数据所特有的规则，对二者作分门别类的研究。

1. 共性规则

共性规则是指，电子数据应遵循正当程序和证据法的一般要求，以避免出现电子数据不受现有规则限制的情况。从西方国家的情况看，电子数据的收集包括从被告人处收集和从第三方收集，两者适用不同的程序。若从被告人处收集电子数据，主要有四种情形：搜查令、同意搜查、“一览无遗”原则以及紧急情况；从第三方收集电子数据，主要包括自愿披露和强制披露两种情形。电子数据在法庭中的适用，则涉及电子数据的鉴定、传闻证据规则以及专家证人等问题。〔29〕这些问题往往可以在既有的证据制度和规则中找到处理依据，如美国联邦证据规则中就有不少相关规定。

从我国电子数据的现有规范来看，电子数据的审查判断并未与初查、技术侦查、搜查、非法证据排除等制度有效衔接。如“电子数据证据规定”主要是围绕电子数据的真实性审查进行规范，而忽视了电子数据的提取与强制性侦查行为具有共性。相关共性规则的缺失，使得这些直接涉及公民基本权利的电子数据取证行为缺乏必要的制度规范。〔30〕又如 2017 年出台的《关于办理刑事案件严格排除非法证据若干问题的规定》，未直接规定非法电子数据的排除问题。实际上，按照传统的理论逻辑就可以厘清电子数据中的不少问题。比如，电子数据的取证过程涉及公民基本权利和正当程序，以侵害他人合法权益或者违反法律禁止性规定的方式取得的电子数据，不能作为认定案件事实的依据。而规范电子数据取证的关

〔29〕 See Major Jacqueline J. DeGaine, *Digital Evidence*, 2013 (5) The Army Lawyer 7 – 25.

〔30〕 参见龙宗智：《寻求有效取证与保障权利的平衡——评“两高一部”电子数据证据规定》，《法学》2016 年第 11 期，第 7 页以下。

键在于法庭上对电子数据的审查判断，即通过司法审查来实现电子数据取证的正当化，并将其转化为非法电子数据的审查和排除问题。

2．差异性规则

电子数据的审查判断应当建立在电子数据自身的物理属性和特点上，这就使得电子数据的审查判断具有区别于传统证据的特殊性。这些差异性规则是审查所有数字化信息时都可以适用的。比如，应基于电子数据的特点确立真实性审查规则。与传统证据相比，电子数据具有很多显著特点，〔31〕对其进行真实性审查，就必须对电子数据的收集、保存、鉴定等制定符合其特点的规则。审查内容则应包括电子数据生成平台、存储介质、保管方式、提取主体、传输过程和验证形式等多个方面，并应鼓励和引导运用电子签名、可信时间戳、哈希值校验、区块链等技术手段进行审查。〔32〕“电子数据证据规定”等现有规范性文件，多侧重于电子数据取证的技术规范而非程序规则，多围绕电子数据的提取、固定、审查判断等证据问题展开，而对电子数据的初查以及勘验、搜查、调取、扣押、鉴定等涉及公民基本权利的侦查程序少有规定，这使得对于电子数据取证并未形成充分的程序性规制。

为避免电子数据资料受损或者发生变动，执法人员在收集或保存电子数据的过程中，应重视证据保管链条的完整性，需要建立一套每一步骤都有相关记录的标准处理程序，以确保电子数据的原貌与完整性。如国际计算机组织（IOCE）曾公布一套“处理计算机证据的国际标准”，其中包括处理电子数据的基本规则：（1）扣押电子数据时，不可改变证据的内容；（2）有必要存取原始的电子数据时，应由有鉴识能力的人员处理；（3）所有关于电子数据的扣押、存取、储存或搬运的行为，应完整记录、保存以及可供审查；（4）在持有电子数据期间发生的任何与该证据有关的行为，皆由电子数据的持有人负完全的责任；（5）任何负责扣押、存取、储存或搬运电子数据的机构，皆应遵守以上处理原则。〔33〕这不仅是行业标准，更是司法机关能够较为简易地审查电子数据真实性的依据，应由法律或司法解释对此作出统一规范，而不应授权侦查机关自行制定。

电子数据的鉴真过程就是审查电子数据真实性的过程，即通过审查检材的可靠性、检材提取的规范性以及保管过程的完整性等来为鉴定提供基本的前提条件。〔34〕其中的重点在于：（1）保管链审查。需要审查电子数据的收集、运输、保管、鉴定等环节形成完整的保管链，这是保障控方提交的电子数据不被污染、损坏、篡改或替换的基本要求。从获取电

〔31〕 从优势看，电子数据更难被破坏，几乎不需要任何物理空间进行存放；可以被精确复制，因此其副本可以代替原件来证明案件事实；只要经由合适的工具，很容易分析电子数据是否被修改。从劣势看，与传统证据相比，电子数据不易被理解、被感知；虽然可以被复制，但如何证明该复本与原本具有相同的证明力，需要审查其可靠性和具体的来源；虽然可以用专门技术来分辨是否被修改，但易于修改的特性也增加了技术上的成本；网络的发达，使得电子数据可轻易通过网络被人修改、操控或传送。

〔32〕 “互联网法院审理案件规定”第11条规定，互联网法院应当结合质证情况，审查判断电子数据生成、收集、存储、传输过程的真实性，并着重审查以下内容：（1）电子数据生成、收集、存储、传输所依赖的计算机系统等硬件、软件环境是否安全、可靠；（2）电子数据的生成主体和时间是否明确，表现内容是否清晰、客观、准确；（3）电子数据的存储、保管介质是否明确，保管方式和手段是否妥当；（4）电子数据提取和固定的主体、工具和方式是否可靠，提取过程是否可以重现；（5）电子数据的内容是否存在增加、删除、修改及不完整等情形；（6）电子数据是否可以通过特定形式得到验证。

〔33〕 参见法思齐：《美国法上数位证据之取得与保存》，台湾《东吴法律学报》第22卷（2010年）第3期，第96页以下。

〔34〕 参见陈瑞华：《实物证据的鉴真问题》，《法学研究》2011年第5期，第127页以下。

子数据起至该电子数据被提交到法庭，该电子数据流转和放置的基本信息以及保管和检验该电子数据的人员的信息，应当是完整且连续的。（2）司法鉴定与专家辅助人意见。电子数据的司法鉴定作为检验电子数据真实性的重要手段，应纳入统一司法鉴定管理体制；为充分发挥专家辅助人的作用，应赋予专家辅助人意见以证据能力。（3）第三方取证存证平台。应建立中立的第三方电子数据存管制度，明确电子数据取证存证平台的审查认定标准。比如，杭州安存公司构建了基于全数据生命周期的电子数据存管与证明体系，从数据生成与创建、数据存储与传输、数据取证的数据生命环节，闭环解决电子数据与司法证据间的要求差异，使之符合司法要求。〔35〕这一方法已在司法实践中得到有效应用，如判决书指出："确认涉案商品信息不存在的安存证据保全图片打印件一份，用以证明天猫公司在收到起诉状后已删除了相关信息，确认涉案信息已不存在，履行了相应的法律义务"。〔36〕

（二）司法层面：从真实性审查到正当程序保障

从裁判文书和访谈中均可清晰地看到，公安司法人员对电子数据的审查判断均侧重于真实性审查，即便是审查关联性也仍然围绕真实性问题来展开。然而，从裁判文书所显示的趋势来看，将来庭审抗辩的焦点很可能会从电子数据的真实性审查转向合法性、关联性等问题，从侧重真实性审查走向真实性审查与正当程序保障的平衡。

如前所述，电子数据的关联性审查主要是一个经验问题，这就意味着对于电子数据的关联性审查，司法层面比规范层面更重要。侦查人员对于电子数据的关联性要想建立证明锁链，就必须超越传统的人和行为的两要素分析，而要锁定人、机（云空间）、数据、行为这四个要素。由于技术上存在盲点和缺陷，这就要求加强在电子数据取证中对关联性证据的收集与固定，同时降低对言辞证据的依赖，善于运用间接证据证明案件事实。这就要求侦查人员须掌握互联网、数据挖掘、数据保存等技术标准规范，公诉人员也应具备审查技术性证据的经验和能力。

司法实践的情况表明，我国电子数据的使用，其短板是欠缺全面、充分的电子数据合法性审查。电子数据合法性审查的重点是对公民基本权利的保护，尤其是电子数据所承载的信息会涉及公民的隐私权。如美国的《爱国者法》一经通过，便被执法人员视为针对恐怖分子和计算机犯罪的最有力武器。该法强化了对互联网和电子邮件的监控，如政府能够在无需合理根据或者合理怀疑的情况下，获得被监控对象访问的互联网地址和发送、接受电子邮件的地址。这固然有利于打击特定犯罪，但对于公民自由和隐私权的保护显然极具负面影响，从而受到诸多批评。〔37〕又如韩国大法院（韩国的最高法院）近期明确指出：打印或复制电子设备载体上存储的犯罪事实相关文件的过程，可视为根据扣押、搜查令状进行的搜查行为。因此，打印或复制的电子文件对象与搜查、扣押的对象应当相同，应将其

〔35〕 杭州安存网络科技有限公司创建于 2008 年。基于全数据生命周期的电子数据存管与证明体系，该公司研发了八大产品系：语音保全系、邮件保全系、凭证保全系、合同保全系、版权保全系、电子政务保全系、医疗数据保全系、即时通讯保全系。安存公司与全国 28 个省（市、自治区）200 多个地区的公证机构及阿里云、百度云、腾讯云等建立了深度合作关系，提供一站式电子数据证明解决方案服务，努力构建全方位电子数据证明体系。http://www.ancun.com，2018 年 12 月 23 日访问。

〔36〕 "江苏源燊动漫产业有限公司诉浙江天猫网络有限公司等著作权侵权纠纷案"，浙江省杭州市余杭区人民法院（2015）杭余知初字第 1137 号民事判决书。

〔37〕 参见胡铭：《价值抉择：反恐措施与刑事诉讼》，《政法论坛》2006 年第 6 期，第 29 页以下。

限定为与犯罪事实相关的电子文件。〔38〕这实际上是强调电子数据取证应遵循正当程序原则、令状主义和比例原则。为减少国际争议，“电子数据取证规则”第23条规定：“对公开发布的电子数据、境内远程计算机信息系统上的电子数据，可以通过网络在线提取。”即将境外数据在线提取的对象限定于“公开发布的电子数据”；对于远程计算机信息系统上的电子数据，则仅限于针对“境内”系统进行网络在线提取。这说明，对于远程电子数据取证，公安机关已经认识到公民权利保障作为国际通行规则的重要性。但是，国内国际适用不同标准显然只能是过渡办法，从长远看应当并轨。

电子数据的合法性审查主要围绕程序问题展开，关键是应当明确违法的程序性后果。对于电子数据的收集、保管等违反程序规则，足以影响其他人的重大权益的，应适用非法证据排除规则。从司法实践看，排除的情形主要应包括：（1）通过非法搜查、扣押获得的电子数据；（2）私自拦截取得的传输中的电子数据；（3）非法侵入计算机信息系统获得的电子数据；（4）私自破解的已加密的电子数据；（5）以植入木马、病毒等侵害他人合法权益的手段获得的电子数据，等等。实证研究表明，我国侦查机关电子数据取证中的程序性违法往往并未导致证据被排除的后果，而是被视为瑕疵证据予以补正。这里不仅存在完善非法证据排除规则的问题，更重要的是司法实践应正确认识违法电子监控、违法电子搜查等行为的危害性，严格依法排除非法的电子数据。

Abstract: The importance of electronic data evidence in criminal justice has become more and more prominent in the Internet era. There is a significant difference between the location of electronic data at the normative level and that at the level of trial practice. An analysis of written judgments on cases of online counterfeiting from 2005 to 2015 in the Lawyee Chinese Judgement indicates that, firstly, the definition of electronic data evidence in criminal trial practice is imprecise, secondly, authentication rules, including those on relevance review and legal examination, are only pursuing the truth as their main value, and thirdly, the widespread existence of electronic data appraisal has not played its expected role, and the application of expert assistance is still at its preliminary stage. Judicial practice shows that, in the future, the focus of court debate in criminal trial would shift from the authenticity of electronic data evidence to the relevancy and legitimacy of such evidence. Therefore, the improvement of the rules on the authentication of electronic data evidence is urgently needed. On the basis of understanding electronic data in a broad sense, we should strike a balance between the value of “pursuing the truth” and that of “pursuing the good”, so as to construct electronic data authentication rules that meet the needs of the Internet era.

Key Words: electronic data, evidence law system, authentication rule, legal examination, relevance review

〔38〕 参见［韩］丁雄奭：《认定电子证据等电子设备载体证据能力》，《第九届中韩刑事司法学术研讨会论文集》，成都，2016年7月28－29日，第2页。