Frontiers of Humanities and Social Sciences

Axon Connecting Ideas to Impact.

比较法视野下刑事电子数据取证的困境及完善

王奕儿*

同济大学，上海，200092

摘　要　刑事电子数据取证立法的缺失带来司法实践中的诸多困境，如取证主体不明确、取证范围过宽，非法证据排除规则缺失、一体式收集程序所引发的公民隐私权、财产权侵害问题等。借鉴域外合理经验，结合我国司法实际，未来修法时应注重明确电子数据的取证主体、限制取证范围，完善取证审批程序及救济途径的规定，并重视取证合法性的建设。

关键词　电子数据；侦查取证；刑事诉讼法修订；立法完善

Abstract The lack of legislation on criminal electronic data forensics has led to numerous dilemmas in judicial practice, such as unclear subjects of forensics, excessively broad scope of forensics, the absence of exclusionary rules for illegally obtained evidence, and violations of citizens' privacy and property rights caused by integrated collection procedures. Drawing on relevant international experience and considering China's judicial realities, future legislative revisions should focus on clarifying the subjects of electronic data forensics, restricting the scope of forensics, improving provisions for examination and approval procedures and remedies, and emphasizing the construction of legality in evidence collection.

Keywords electronic data; investigation and evidence collection; revision of the Criminal Procedure Law; legislative improvement

Received: January 28, 2026
Revised: February 10, 2026
Accepted: March 1, 2026
Published:February 7, 2026

1. 问题的提出

作为上层建筑的法律是由经济基础所决定并为之服务的，法律的基本形式不仅会受到经济发展的制约，更是会随着后者的变化而发生变化。2023年9月7日，全国人大常委会公布了第十四届人大任期内的立法规划，其中在“条件比较成熟、任期内拟提请审议的法律草案”一项中列出了《刑事诉

*王奕儿，同济大学博士研究生，研究方向：刑事法学;本文获得同济大学研究生国际交流基金项目资助

讼法》，标志着《刑事诉讼法》的再次修订工作即将启动。一方面，社会经济的不断发展变迁不仅会带来犯罪的进化演变，对刑事取证工作也产生了新的冲突和挑战；另一方面，随着《中华人民共和国网络安全法》（下文简称《网络安全法》）《中华人民共和国数据安全法》（以下简称《数据安全法》）《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）等顺应时代发展潮流的法律陆续颁布，《刑事诉讼法》也应完善立法衔接，作出立法完善。

2012 年修订的《刑事诉讼法》中首次将电子数据纳入证据种类，在裁判文书网以“电子数据”为关键词，并将案由限制为刑事案由，搜索可发现，2013 年使用电子数据作为证据的判决有 210 件，2014 年便增长至 2369 件，此后逐年呈现出指数倍增长的趋势，到 2020 年，相关案件数量竟达到了惊人的 34098 件[1]，可见，在大数据、云计算等技术飞速发展的数字时代，电子数据是当之无愧的“证据之王”，而其所涉及的案件远不止日益增加的网络犯罪，诸多传统犯罪中电子数据也是锁定案件事实的关键证据。2012 年《刑事诉讼法》仅将电子数据作为与视听资料并列的证据类型加以规定，最高人民法院随后出台的《关于适用〈中华人民共和国刑事诉讼法〉的解释》（以下简称《高法解释》）中第 93、第 94 条简要规定了电子数据作为证据使用时的审查与认定方法。2015 年《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》对电子数据的取证与审查做了进一步详细的规定，2016 和 2019 年，两高一部等机关均出台相关司法解释或指导规则不断对电子数据取证方式、条件以及现场提取、网络在线提取等方面进行细化，2021 年新出台的《高法解释》规定了电子数据真实性、完整度的审查标准以及瑕疵证据的补强或无法适用的情形，也对前述文件进行了纠正和补充。

不难看出，上述司法解释和规范性文件旨在保障电子数据的真实性和可靠性，却忽视了电子数据取证的法律适用条件和正当程序规则[2]。电子数据的实质是一些二进制代码的排列组合，随着日新月异的发展，可作为证据使用的电子数据主要演变出如下几种形式：其一为可存储于特定介质或载体内的电子数据，是最为原始的一种电子数据形态，通常储存在计算机终端或移动设备中，可以直接进行复制或备份；其二为电子通信设备中的电子数据，如移动终端设备中的通讯录、短信，抑或是传真机、电子监控中留存的数字资料等，此类电子数据往往真实性和客观性较高，因此也具有更强的证明力；其三为基于云计算技术下存储在云端的电子数据，云端数据具备共享性，不仅可以通过私人账户登录查看，也可以通过提供云存储服务的供应商处提取到相应数据；其四为网络信息交互中产生的电子数据，即用户在适用微信、

微博、邮箱等即时通信软件时产生的电子资料，此类数据往往直接通过图片或文字形式进行呈现，直观性较强，并可通过技术手段进行恢复，是当下电子数据取证中的主要对象之一。由此可见，当前电子数据的种类和存储方式愈发复杂且仍在不断更新演变，在进行电子数据的取证工作时，所涉及的主体不再仅有取证人员和案件当事人或证人，服务器提供者、社交平台运营者等均有可能成为被搜查的主体，不仅如此，在同一云端上被存储的与案件完全无关的众多第三人的数据或本案当事人与案件完全无关的其他私人数据也会暴露在取证人员的搜查工作之下，因此在电子数据取证规则的立法中，应特别注意尽量减少对此类主体隐私权、财产权等私人权利的侵害。而就当前立法现状来看，无论是《刑事诉讼法》中的条文还是相关司法解释中规定的滞后性都较为严重，尽管滞后性是立法的天然属性，但现行立法中关于电子数据搜查、提取等的规定显然不能与现实情况相适应，不仅不能给司法实践提供明确指引，致使司法工作人员取证不规范、程序不合法，更是给公民个人信息安全带来了隐患。基于此，本文拟针对电子数据取证这一角度，结合证据法和侦查法的相关理论知识，发掘司法实践中的问题所在，对比域外视野，将比例原则、权利保障理论与程序正义理论作为核心分析工具，对电子数据取证中的问题进行立体化的审视，试图构建一个以权利保障为核心、以比例原则为尺度、以程序正义为路径的规范分析范式，进而为未来我国构建更为精细、平衡且符合法治精神的电子数据取证制度提供坚实的理论支撑与具体的完善方向。

2. 当下法律困境

在数字时代，受科技发展、社会变革等因素的影响，犯罪的种类、手段以及其所发生的时间、空间均发生实质改变，犯罪人也可通过习得相关技术知识使自己具备更强的反侦察意识，另一方面，在智能生活助手不断发展并被广泛应用的背景下，数字技术真真切切地渗透到人们的日常生活之中，在衣食住行等方面均会留下大量的电子数据[3]。因此，无论是传统犯罪还是网络犯罪，电子数据在所采证据中的地位均不容小觑，而以往传统的刑事诉讼手段显然无法完全适应当下稍显复杂的侦查需要，也面临着如下困境。

2.1. 取证主体困境

一般而言，刑事侦查活动必然会伴随着一定程度的对被侦查者隐私权等权利的侵害，因此各国在立法上均对取证主体加以限制。2014 年公安部发布的《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》中规定，对电子数据进行取证时，应当由二名以上“具备相关专业知识”的侦查人员进行。而 2016 年两高一部《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》在取证主体上则取消了对侦查人员应当具备相关专业知识的限定。19 年公安部《公安机关办理刑事案件电子数据取证规则》（下文简称《电子数据取证规则》）延续了该规定，对侦查人员的专业知识不作要求，但补充了必要时可以指派或者聘请专业技术人员在侦查人员主持下进行收集、提取电子数据的规定。

可见，自 12 年电子数据成为证据种类之后，相关机关在制定司法解释或意见规定时均对取证主体的适格性进行了考量，这也侧面反映出电子数据取证时有别于传统物证的特殊性和专业性。就当前立法而言，一方面，绝大多数侦查人员的教育背景隶属于侦查学、法学等专业，缺乏互联网、大数据、云计算等领域的相关专业技术知识，加之有关学科技术革新较快，即使具备相关专业背景的侦查人员也很难在工作后及时补充领域的最新前沿技术；另一方面，《电子数据取证规则》中侦查人员指派或聘请专业技术人员的规定亦有待推敲，其一在于此种规定在《刑事诉讼法》中于法无据，根据其规定，我国的侦查主体主要包括公安机关为主，人民检察院、国家安全机关等在内六个机关，其他个人或组织团体均不具有法定的侦查资格；其二，在部分案件中，无法保证所聘请专业技术人员与涉案人员不存在商业竞争等利害关系，如在“快播案”中，辩护人提出取证程序违法的辩护意见，理由之一在于涉案的服务器是由文创动力公司开启，之二则为文创动力公司还在为快播公司的竞争对手服务，涉案服务器在文创动力公司长期保存原始数据存在被污染的可能[4]。综上不难看出当下立法在电子数据取证主体规定上的漏洞与矛盾之处，司法解释中的处理也会产生电子数据取证主体权限合法性与取证技术资质合法性的冲突[1]。

2.2. 取证范围困境

《公安机关规定》第 66 条规定，收集、调取电子数据，能够扣押电子数据原始存储介质的，应当扣押原始存储介质，并制作笔录、予以封存；因客观原因无法扣押原始存储介质的，可以现场提取或者网络在线提取电子数据。以上两种提取方式都无法实现时，才可采取打印、拍照或者录音录像等方式固定相关证据。可见，对电子数据进行收集时，取证手段呈现出扣押原始储存介质优先于现场提取或在线提取，再优先于打印、拍照、录音录像的阶梯式结构。此种以扣押储存介质为主的取证方式显然值得商榷，因为电子数据天然具有和存储介质的可分离性，且即使经过多次复制仍与原始形态几乎无任何差别，更何况在计算机科学领域已存在如利用哈希值进行文件校验等判断数据有无被损坏或修改风险的成熟技术。而无视电子数据可分离性特征的统一扣押模式背后所隐含的是对公民财产权和隐私权的肆意侵犯，同时

所提取的实物载体也与案件本身的关联性不高。早在上个世纪，美国大法官 Louis D.Brandeis 便指出，在未来，政府即使不去当事人家中翻阅私人抽屉中的任何文件，也可在法庭上出示相关内容，从而使得一个家庭中最为隐私的部分直接暴露于公众的目光之下[5]。可见，此种提取方式不仅会对公民的个人信息自决权造成预防性的侵犯，更是会引发无关信息滥用的风险，而上述隐患均远超于查明特定案件事实的必要限度。不仅如此，正如上文所言，由于电子数据的交互性和开放性等特征，在以特定的存储介质中除可能的涉案信息以外，还会有大量与案件无关数据的存在，甚至于存储载体在运转过程中也会自动处理并产生一些信息，且这些数据信息的分享与披露绝非出于当事人意愿[6]，如果将其一并进行扣押，极大可能将大量无关第三人的数据信息同时扣押，并对与案件无关的设备拥有者或信息提供者的日常经营活动产生负面影响。此外，扣押原始电子设备看似保留了证据的完整性，但从技术层面来看，收集到的海量数据可能会模糊关键证据的生成时间、修改轨迹等，也存在“淹没”关键证据的可能，不仅可能会导致相关证据证明力的削弱，海量数据的长期安全存储与管理都需要硬件投入与运维成本，与侦查经济原则相悖。

2.3. 审批程序困境

《电子数据取证规则》的第二章将收集提取电子数据分为扣押、封存原始存储介质、现场提取电子数据、网络在线提取电子数据、冻结电子数据以及调取电子数据五种手段，却只针对冻结电子数据、调取电子数据规定了批准程序，即采取上述两种方法取证时，应经过相关负责人批准，并制作相关文书，对其余三种手段则不做审批必要性的规定。值得注意的是，针对冻结电子数据的行为，应当经“县级以上公安机关负责人”批准，而针对调取电子数据的行为，则要经“办案部门负责人”批准，而公安部 2012 年公布施行的《公安机关办理刑事案件程序规定》（下文简称《公安机关规定》）第 61、62 条也规定，公安机关收集证据无需特定批准程序，调取证据则需经办案部门负责人的批准。诚然，审批程序存在与否与取证活动可能侵犯被取证人权利大小有着直接的关联，但由于电子数据所蕴含的特殊技术属性，对其进行收集调取更容易引发侦查权的滥用，也更容易侵害到涉案当事人或案外人员的隐私权，更何况，侦查人员对网络空间中的数据开展搜查活动，应属搜查活动的一种，理应经过特定的审批和授权[7]。

在诉讼理论中，根据侦查行为是否侵害个人的重要法益（如身体、住所、财产等）可将其分为强制侦查和任意侦查，而前者通常要伴随令状主义加以共同适用[8]。而令状主义的实质就在于通过对侵入、搜查、扣押等行为的发

动进行事先明示从而以限制侦查权的肆意行使[9]。我国当前的刑事诉讼法中并未对令状主义进行明文规定，但在关于勘验、检查、以及强制措施中的规定均透露出令状主义的内涵所在。与传统的侦查方法相比，通过技术侦查调取电子数据对个人权利的侵害形态必然有所不同[10]。同样地，与物证不同，电子数据特殊的存储介质使其单位存储容量更大、更复杂且更分散，其中不仅会包含以往会存储在传统物证之上的敏感记录，更是会涵盖众多不可能以任何形式承载于物理场所中的隐私信息[11]，这就会导致其整体上与某一特定案件的关联性变弱，侦查人员需要在更大体量中的信息中分析并筛选与案件相关的数据以作为证据使用，无形之中便会侵害到当事人更多的权益。因此即使是现场提取证据，若收集物证则直接可直接定位并现场封存，而对电子数据的提取——以智能手机上的信息为例——侦查人员不仅可能会要求当事人提供解锁密码或其他生物验证信息，后续更是会对一系列云端数据进行查询和分析，这种取证方式显然打破了传统物证中的时空壁垒，当然需要对其进行更为严格的审批。

2.4. 非法证据排除困境

根据《刑事诉讼法》第 56 条，当前可适用法条被排除的非法证据仅限于犯罪嫌疑人、被告人供述、证人证言、被害人陈述、物证及书证五种，21 年《高法解释》第九节中虽列举了部分应被排除的取证手段，但仍明文将可被排除证据种类限制为上述五种，由此可见，当前立法中非法证据排除规则并没有覆盖到全部的八种法定证据类型，即在《刑事诉讼法》的层面没有规定电子数据违法取证的法律后果规则[12]。

21 年《高法解释》中仅对电子数据的瑕疵补正做了说明，然而不能进行补正的瑕疵证据绝不等同于应被排除的非法证据，无论就收集手段、程序还是证据的真实性或完整性等角度而言，瑕疵证据的可采纳性均明显高于非法证据。易言之，当前在刑事诉讼立法及配套司法解释中仅对违法程度较低的取证手段所产生的瑕疵电子数据证据的适用进行规定，却缺少违法程度较高的取证手段导致的非法电子数据证据的排除规定，这种缺乏递进层次的规定就会使得电子数据取证的合法性缺乏必要的保障机制和制裁机制，属于法律后果规则的重大缺失[12]。一方面，相关人员在取证时会滥用侦查手段，影响所提取电子数据的完整性和真实性，另一方面，当被告人因非法手段调取的证据受到指控时，其也缺少法律明文规定的救济手段，致使其诉讼权利受到侵害。

3. 比较法视野下的域外经验考察

由于我国《刑事诉讼法》当前在电子数据取证方面的立法有较多空白，在未来修法时，参照域外成型经验，结合我国现实国情与司法实际取其精华，去其糟粕，不仅可以规避既有弊端，也可促使修法成熟化。在指导原则方面，1995 年成立的计算机证据国际组织（IOCE）曾于千禧年在报告中提出计算机取证过程中应遵守的六项基本原则，为计算机数据取证提供了基本遵循，至于具体立法规范，本部分也将介绍有代表意义的国家或地区的立法现状及可借鉴之处。

3.1. 日本

关于直接就存储电子数据的计算机进行直接扣押的问题，日本学者认为，侦查机关被授予的执行强制措施的权利并不能及于计算机本体，计算机的使用权或管理权应只属于其拥有者[13][14]。日本于 2011 年对其刑事诉讼法进行了修改，并回应了此前实务界争议较大的关于电子记录物的搜查和查封问题。修改后的《刑事诉讼法》第 99、第 218 条规定，当应对涉及电子数据的载体或存储介质进行扣押时，扣押执行人可根据涉案数据的种类、数量、存储载体的性质以及被取证者的态度进行判断，必要时应采取把相应电子数据复制或转存到其他载体上进行扣押的代替扣押措施，而不直接扣押原介质[10]。如此一来被处分者手里还留存原始信息，不会影响其正常工作生产。此外，在对云端存储系统或网络通讯系统这种内部承载大量无关人员或无关信息的数据进行取证时，应由系统管理者进行操作，筛选并输出有关的数据并复制在新的载体之上，侦查人员只需扣押新的介质即可。此种扣押行为被称做“附带记录命令的扣押”，从其性质上看应纳入强制措施的范畴[15]，当然需要配合相应的令状一并执行。

对于不了解计算机技术的办案人员来说，在进行电子数据取证时不仅会耗费大量时间，更是可能对调取对象造成权利上的侵犯，因此关于取证主体的问题，日本修改后的《刑事诉讼法》第 111 条规定，侦查人员可以要求被处分者对证据提取进行协助。当然，法典中并未明确协助的条件或限度仍是一个遗留的、值得研究的问题，对此，有学者指出，若协助指令超出了操作者知识或技术可能达致的范围或会对其业务工作产生较大影响时，被处分者可以拒绝侦查人员提出的协助要求[16]。

可见，日本 11 年修改的《刑事诉讼法》关于电子数据取证的部分，创设了电子数据复制品替代扣押的机制，并明确了侦查人员可要求运营商协作配合的程序，此种立法不仅贴合电子数据虚拟性、可复制性的特殊属性，也在尝试构建一种市民参加协助机制，对我国日后修法有一定的借鉴意义。

3.2. 德国

《德国刑事诉讼法》中没有对可能成为证据或没收对象的物品的扣押设立实质的限制或保障[17]，但起到统帅作用的比例原则还是在某些特殊物证上进行了特定的限制，以搜查扣押电子数据为例，比起复制这一侵入性较小的措施，直接对存储硬件进行扣押很显然与比例原则相违背[18]，故一般来言，应禁止为寻求某项轻罪的证据来扣押大量计算机的取证手段。此外，基于预防犯罪的需要，对于尚处于服务器之间传输途中而未被存储于私人服务器或由私人所有的信息系统[19]的数据而言，警方也可采取对通信进行监控的手段以获取传输中的电子数据，但出于对公民隐私权利的保护，此种获取电子数据的方式仅限于在事关公民生命、健康、迁徙自由等宪法性权利及国家存亡等重大风险时[20]才能被加以适用。而对一般公民私人设备中存储的数据而言，因调取私人数据所带来的比例原则上的冲击，因此德国刑事诉讼法第 100 条规定，司法机关在将移动电话中的电子数据进行记录并用于刑事侦查之前必须得到司法授权，且只有在侦查行为确有重大意义时才能得到允许[21]。至于非案件嫌疑人的数据信息，只有在确属必要时才可进行调取，并需在记录使用后立即删除。

不仅如此，德国在电子数据取证中对人权的保障不仅体现在比例原则中，更是渗透于令状规则之中。根据德国刑事诉讼法第 145 条的规定，实施涉及个人隐私的侦查行为如搜查、扣押、监听监控等，必须事先取得法官的司法授权，即需申请实施相关侦查措施的令状，令状中必须清楚列明所要搜查、扣押的物品。此处的法官为特定的侦查法官，由侦查所在地的地方法院加以任命。而如果侦查人员因迟延危险等特殊原因径自实施取证活动的，需向联邦宪法法院说明具体理由，若后续查明当时侦查人员有等待法官签发令状的机会而谎称情况紧急直接行动，则此种无令状侦查行为是违宪的。为了能够及时对侵权性侦查措施进行司法审查与授权，联邦宪法法院正积极推进司法应急服务组织的建设工作[22]。另一方面，作为利益相关人的普通公民也可以向法院提出对警察扣押行为是否合法的裁量请求，如果该扣押行为被认定违法，警察必须返还扣押物，政府也许提供一定的金钱赔偿。

取证违法往往和非法证据的排除密切相关，但德国刑事诉讼法中关于排除非法证据的明文规定并不多，实践中法官也更愿意将查明真相立于前置之位。但值得肯定的是，德国刑事诉讼法第 100 条中规定了对私人住宅进行搭线窃听或音频监控而得到的证据不能用作定罪依据，相较于我国，德国的非法证据排除程序并不局限于传统证据的桎梏，而是更倾向于考察侦查行为是否对受法律保护的个人隐私领域的侵犯。除此之外，通过上文分析不难看出德国刑事诉讼程序以比例原则为指导，其中特别重视对被调取信息者个人隐私的保护，着重考量对当事人个人权利的侵犯是否与为查明真相而采取的侦

查行为的重要性成比例[23]，对于新技术下产生的对新证据的提取手段也会进行违宪性审查并对不合适者及时叫停或加以限制。其对人权的保护、在侦查阶段的司法控制以及对比例原则的贯彻落实均可为我国下一步修法提供思路。

3.3. 美国

为保障被扣押人的财产利益，美国联邦司法部曾发布指导性文件，建议为减少搜查扣押行动对当事人的影响，在不影响侦查活动正常进行和不过分增加司法成本的前提下，当被扣押人提出合法营业或自身需要的请求时，相应机关应对之作出响应，发还相应数据的复制品于被扣押人[24]，而实践中也确有法院履行该文件精神[25]：当被扣押人以影响其日常营业为理由向法院提出归还被扣押物的申请时，法院通常会同意该申请并责令侦查机关将扣押的相关设备返还被扣押人。而在案件审理结束前出现被扣押物已不再被需要的情况时，法院也可能会要求侦察机关将扣押物返还。

至于扣押物的范围，早期美国刑事诉讼理论曾提出单纯证据原则（Mere Evidence Rule）[26]，所谓“单纯证据”，指除犯罪工具、犯罪所得及违禁物以外的对起诉或定罪量刑有价值的证据，对单纯证据不能进行扣押，而需由大陪审团或法院签发命令，后由所有人自行提交证据。此规则于 1967 年被美国联邦最高法院推翻，理由在于比起财产权搜查工作应更注重当事人的隐私权，与犯罪工具等相比，单纯证据并不一定具有更强的隐私属性[27]。有判例认为，当事人如果在主观上对特定物品或信息抱有一定的隐私期待，且此种期待从一般社会大众的角度来看为合理时，当事人便可主张宪法上的隐私权[28]。而单纯证据原则的废止直接扩大了警察的搜查和扣押范围，在美国的司法实践中存在大量侦查人员对物证进行过量扣押的现象，对此，美国联邦第九巡回上诉法院判决提出警察在进行搜查工作时应按照搜查令状上所申请记载的范围实施扣押工作，若所扣押之物远超于搜查令上标注的内容，则有违反宪法第四修正案之嫌。对于以记载内容为证据的客体，如果警察在现场无法判断哪些应该被扣押，可现场对其进行翻阅之后再进行判断。对于特殊案件，若搜查人员凭经验可预见到需对现场物体进行大规模扣押，可提前向法院申请大规模扣押的令状后再执行扣押工作[29]。即在有特定令状程序保障的前提下，侦查人员才可以对搜查物进行大规模的扣押，即使在搜查现场无法对物品内容进行审查并作出其与案件是否相关的判断。除此之外，就令状所记载的内容而言，美国联邦第十巡回法院也曾作出判决，要求针对采集电脑中的数据的搜查行为，其搜索票上不仅要明确所搜查的特定客体，更是要载明就特定客体内部拟进行搜索查阅的目标，譬如某台电脑中有关毒品

交易或儿童色情等特定犯罪的记录等[30]。如果搜查证上未载明上述具体内容，则也因侵害当事人的隐私而与宪法精神相悖。

可见，与德国相似，美国也十分注重公民隐私权、财产权等宪法权利的保护，并注重通过令状这一程序对搜查扣押行为的合法性进行补强。即使隶属于于不同法系，其程序保障的做法也值得我国适当进行参考。

3.4. 中国台湾地区

早在 2001 年，我国台湾地区便修改了当地刑事诉讼法中关于搜查客体的相关条文，将原法条中“应加搜索之处所、身体或物件”修改为“应加搜索之处所、身体、物件或电磁记录”。整体而言，我国台湾地区的侦查工作以最小伤害原则和比例原则为基准进行，即某一目的可以途经诸多手段均可达到时，政府应优先采取侵害最小的方式，而不得对当事人造成不必要的侵害。具体到电子数据的搜查工作，侦查人员应优先在搜查现场制作存储载体的影像文件并将原始载体归还，或者要求电子数据及其载体的保管人或有权使用人制作所需数据的复制品，或对复制品进行扣押，或将扣押原件而将复制品交至受扣押之人[31]。

比起财产权，我国台湾地区更加重视对被扣押物所有人隐私权的保障，其也遵循“合理的隐私权期待”模式，认为侦查人员使用技术手段获取他人信息或数据的行为亦应当遵循相应的隐私保护程序规定，满足相应前提条件并需履行相应的令状程序，即使此种行为并未实质进入当事人的物理住所[32]。而就电子数据特有的过度收集问题，我国台湾地区在立法上也并未明确给出有效进路，多数学者主张[33][34]，应将所扣押的载体分为“能够作为证据使用的应当没收之物”和“仅作为案件相关数据存储载体之物”两种，对于前者，其往往属于因犯罪而产生或供犯罪所使用之物，对其进行扣押并没有问题，而对于后者若直接进行扣押则易引发学理上的瑕疵。

不难看出，我国台湾地区对于电子数据取证的做法受美国判例影响较大，其部分做法有一定参考价值但并非全部可取，比如对侦查人员现场对载体上存储的电子数据进行复制的规定不仅对取证人员的专业知识和技术水平提出了过高的要求，也不利于保证所提取证据的完整性，不仅有些不切实际，更是可能会影响到案件的侦查工作顺利、准确进行，故尽管此种做法能很大程度上保障当事人的财产权，但考虑到时间、技术及人员成本，其参考价值并不大。

4. 未来修法方向审视

我国当前立法中对电子数据取证过程中所蕴含的公民权利重视不足，而电子数据自身的特性也表明其取证思路与传统物证有较大差异，故未来修法有必要针对此作出变革，以回应司法实践中迫切面临的困境。结合上文所述，在未来刑事诉讼就电子数据取证的修法工作中，应注重以比例原则为指导，以实现司法行为合法性、正当性以及侦查效率、收益相平衡。

针对文中提到的困境，具体而言，有如下几种进路。

4.1. 明确取证主体

电子数据取证本质上仍属于一种侦查活动，与传统物证的取证不同，侦查人员无法不通过任何载体对电子数据的内容进行直观感知，故而必须通过存储设备实现其的具象化，因此对电子数据进行取证，不仅涉及法学、侦查学等相关知识，更是要掌握计算机软硬件技术、密码学、通信技术等数据挖掘和分析的相关知识。而就不同类型的电子数据而言，对其进行采集时需要运行的机器、软件等都不尽相同，所提取到文件的格式更是五花八门，要求侦查人员对此全面掌握或拥有系统知识显然不切实际，但尽管如此，本文绝不赞成扩张侦查主体的观点，非但如此，考虑到上文提到的电子数据证据特征，本文倾向于未来立法将对电子数据侦查取证的主体限制为除特殊情况下由市级以上公安机关为主较为合适，原因在于市级以上公安机关不仅拥有更高的信息化建设水平，对所提取数据进行管理、整合等技术也更加成熟。当出现地域冲突或技术困境时，也应先优先求助于异地或有相关技术的公安机关进行辅助。至于《电子数据取证规则》中提到的指派或者聘请专业技术人员在侦查人员主持下进行收集、提取电子数据的规定，本文认为未来修法应明确专业技术人员的辅助地位，出于公平和专业双重因素的考量，其都不应纳入侦查主体的范畴，即使是特殊证据的案件也不例外：一方面，侦查权作为国家赋予司法机关的专属特权，天然带有十分严肃的公权力色彩，不应因任何理由将其授至其他非国家机关，另一方面，所聘请的专业技术人员不仅无法像国家机关那样保持绝对中立，其非公益属性也必然会消弭其社会责任感，当然不能成为法定的侦查主体。尽管法定的侦查主体不能作出让步，但在下一步的立法工作中，有必要就电子数据取证制定更加完善的指派或聘请有专门知识的人的取证制度，从学历、证书、职称、从业经历及年限等方面[35]明确有专门知识的人的选择标准，并附有一定的审核条件，通过审查其历史工作经历或合作对象等确认其是否与案件所涉取证对象存在利害关系，最终选择是否对其进行邀请或聘用。比起侦查主体，有专门知识的人更适合在后续的数据鉴真工作中发挥主要作用，即侦察机关可以邀请相关人员对拟作

为证据使用的电子数据的真实性和完整性通过技术手段进行鉴定并出具报告，以提高其证明力，当然在具体人员的选择上也应遵循上文提到的原则。

4.2. 限制取证范围

在对传统物证进行取证时，侦查人员所调查或扣押的物体本身即是与案件相关的证据，而无需将犯罪现场的多数物品一律扣押再进行相关性筛选，但当提取客体变为电子数据时，所扣押的载体或容器并不当然作为案件证据进行使用，真正具有证明力的是存储于其中的数字资料。故而电子数据的取证行为突破了传统侦查工作中“搜查→扣押”的行为模式，而更趋向于“针对存储载体的搜查→扣押→在载体内部再次进行搜查”[36]的新型模式，加之多数情况下为侦查需要，工作人员往往会将载体扣押数月之久，且在完成数据提取工作后仍对搜查物保持扣押，其中对搜查对象财产权和隐私权的侵害显然不言而喻。

考虑到电子数据无法脱离特定载体而被人们感知，加之其可被复制的自我属性，在对存储载体进行扣押时，可以参考美国及我国台湾地区的规定，在不影响司法活动正常进行的大前提下，对实体存储载体进行扣押后，先在一定期间内确定扣押之物存储的内容是否与案件具有一定的相关性，若不符合办案需要，应解除扣押程序并尽快退回，如果内容证据适格，则需于一定时限内对其中内容进行复制，由特定技术人员、侦查人员或鉴定人书面确定复制件与原件内容一致后，将原载体归还给被扣押人，若确因特殊原因无法归还原载体，而被扣押人又确实需要相关数据以支撑起日常工作，则可赋予被扣押人申请复制体的权利，侦查人员依申请将复制件归还设备所有人，如此阶梯式的扣押结构以实现最大限度兼顾侦查需要及公民财产权保护，在不影响正常侦查活动的前提下保证对公民个人权益的最小化干预，达到司法领域的帕累托最优值[37]。

在电子数据取证问题上，隐私权和财产权的侵害如影随形，但正如上文所述，电子数据取证行为应做到涉及公民权益的法益成本和涉及侦查效益的资源成本的有机统一[38]，故结合办案效率与证据收集质量两方面的双重考察，本文并不完全否定在搜查现场进行大规模取证扣押的做法，出于电子数据具体内容的不可直观性，严格要求侦查人员不去审视内容便只扣押与案件相关的载体几乎是天方夜谭，而若其在案件现场便对数据内容进行审视筛查，此种长时间停留在搜查现场的行为也会给被搜查人带来更多的隐私羞耻和威严压迫感，可谓是因噎废食。针对此，一方面，若因侦查需要确需大规模对第三方所有载体进行扣押时，法律应赋予当事人以自己的经营生活或商业信誉等遭受到的明确损失为证据向司法机关申请一定的补偿，另一方面，通过

妥善的程序监督机制明确令状规则及赋予其救济的权利亦是重中之重，关于此，将在下文详细论证。

4.3. 完善审批程序

承接上文，合理的程序监督机制是缓和侵权冲突的必要手段之一，2021年通过并施行的《数据安全法》在第35条也明确了国家机关因侦查需要调取数据时须经严格的批准手续并依法进行。因此在下一步的刑事诉讼修法中，有必要完善电子数据取证的审判程序，除现行司法解释或文件中规定的两种取证手段外，应将配套的令状制度拓展到涉及电子数据取证的全部五种取证手段之中，即只要对电子数据进行取证，均需获得办案机关负责人的批准并制作令状。而另一方面，负责人进行审查时，除普通物证侦查程序中需具备的进入特定场所的正当理由外，还可参照证据的特性着重考量下述因素：是否有一定理由确信所涉及实体载体内部存在电子数据以及该电子数据是否必然与案件事实有一定的相关性。且上述条件的判断标准应结合案件事实和客观条件，不能只依靠纯粹的主观推理或内心怀疑。不仅如此，令状上应明确限定本次取证的时空范围及客体范围，如果侦查机关能实现查明案件相关证据所承载于的特定载体，则应在令状上加以注明，现场取证时亦不能超越其范围额外扣押与案件无关的存储载体，以最大程度上减少对当事人权益的侵害。当然，立法时也应考虑必要的程序例外情况，本文认为，若须提取的电子数据涉及危害国家安全、社会公共安全等重大权益或确有证据表明处于紧急情况时，也可径行进行搜查扣押，后续再对相关材料进行补齐。但要注意的是，一方面，需有明显证据表明案件本身必须符合危险性、紧迫性的要求，另一方面，也应给予被扣押者一定的异议权利，允许其就相关程序提出复议并提供妥善的救济途径。

另一方面，就令状制度而言，在未来修法时应特别规定侦查人员应严格遵循令状所记载的案由进行取证，若在对载体中存储的电子数据进行排查时，发现与本案无关但却可独立成案的数据，不应直接提取并作为另案证据使用，而应向上级部门汇报并提交申请，取得新的批准程序后再对相关数据进行整理取证[39]。毕竟此时实物载体处于侦察机关的控制之下，其中数据也不会无理由地消失或丧失证明能力，故此时要求侦察机关就新案由重新申请侦查令状并无不妥，亦不会影响案件的侦办，而后续若涉及管辖等其他问题，也应按照法定程序申请或依职权主动变更。不仅如此，对于未经申请便擅自提取的数据应否认其证据能力并予以排除，同时也要赋予被搜查者一定的救济权利，如果其发现侦察机关所扣押的客体及后续主张的罪名与当初向其展示令状中记载的范围不一致，可以向上级侦查机关或法院提出救济申请，如此一

来从事前审批和事后保障两个维度来限制侦察机关可能出现的违法取证行为，以防止侦查权滥用情况的发生。

此处需要额外论证的是，对于采用秘密侦查等侵犯他人隐私权利所取得的证据，有学者主张可以通过审视证据所指向犯罪之轻重来决定其是否具有证据能力，如果其指向的是重罪或者恐怖活动，则可作为证据使用，反之指向轻罪则不能[40]。故而有主张认为对于侦查中发现的预料之外的另案证据也可采用类似的采纳标准[36]，本文则不赞成此种观点，一方面，此做法看似符合比例原则的背后实则是对被搜查者隐私权利等的重大侵害，在取证手段相同的前提下，不能因为拟定的犯罪客体的轻重来补充此种侵权行为的正当性；另一方面，在我国当前以幅度量刑占主流的刑罚立法之下，重罪的标准难以得到明确或统一，此种自由裁量权必不能过度赋予侦查人员，是故此种主张并不合理。而 21 年通过的《个人信息保护法》中明确规定的目的限制原则也可为本文观点提供一定的理论基础，侦察机关无论是提取还是使用处理电子数据都不应与令状上预先记载的目的相背离。

总之，司法审查制度的建立是完善电子数据合法性规则体系的必备前提，也是未来改革的基础性课题之一[12]。而广泛覆盖的侦查行为审批机制和严格配套的令状程序不仅可以限制侦查权的滥用，更是有利于保护被搜查人的隐私及财产权益。不仅如此，留存下来的书面证明和录音录像也为后续当事人救济提供了路径遵循。

4.4. 加强取证合法性建设

为保证电子数据取证工作的合法性，未来修法应明确电子数据的提取、固定、登记及保管各流程的规范程序，首先，应明确电子数据提取前的准备程序，一方面，明确侦察机关在实施搜查前向被搜查人出示证据提取通知书，并于上面详细记载具体案由、所涉数据、拟扣押范围等；另一方面，要求侦查人员提前对网络环境进行监控，必要时可实施诸如切断网络、屏蔽信号等控制及保护措施，以防相应数据被后台操作或远程控制改变或丢失，在提取过程中，应保证全程录音录像；其次，应规定对于数据信息发生流转的每一截点进行书面记录，而非仅口头交接。不仅如此，在对电子数据进行内容审查时，不仅要配备相应的加密存储系统、访问权限系统及身份认证系统，更是要对各人员的审批及使用历史形成书面记录，并附每次访问时间、访问人员及访问目的的书面文书留存备查[41]。再次，若需要对提取到的数据进行二次分析，须先将其复制到另一载体上再进行操作，避免直接在原始载体使用技术手段以防止破坏其原始状态。不仅如此，未来立法中应避免只关注收集获取电子数据的程序保护，再提取到数据后对其的进一步审查、处理以及分

析工作也同样需要法律的规制[42]。是故对于电子数据这一特殊证据类型，立法者的应做到法律中心主义到技术中心主义的思维转变，不能局限于传统视角审视问题，在立法上对电子数据取证的各环节进行明确和规范，有助于促进电子数据取证的合法性建设，保障所提取证据的真实性及可溯源性。基于电子数据证据的特殊性，当立法出现缺失时，无论是类推适用还是直接援引一般规范来适用都是不合适的，这就会使得立法的特别授权被架空[16]。这也要求电子数据取证的相关立法需建设完备且正当的特殊程序条款，促使司法实践有法可依。当前立法中对违法取证所得的电子数据并未建立明确的排除规则，立法的不清晰必然会带来实务中的侦查权滥用问题，从而损害当事人的诉讼权益，瑕疵证据的补正和非法证据的排除绝对不可替代，故本文认为下一步立法应明确将电子数据列入可被排除的证据范围并增设违法取证情形的规定，从电子数据取证的启动程序、现场调查及固定、数据分析、移交、保存等多方面进行规制，通过制定事后的非法取证审查及排除机制，也有利于倒逼侦查人员取证行为的合法性。

5. 结语

每个个体的存在和活动，若要获致一安全且自由的领域，须建立某种看不见的界限，然而这一界限的确立又需依凭某种规则，这种规则便是法律[43]。为衡量保护公民权益和切实惩治犯罪的需要，对于电子数据的取证而言，以法律作为防线进行程序上的约束显然必不可少。除本文详细讨论的问题外，诸如跨境电子数据取证、算法规制的问责机制等也是当下面临的棘手问题。在未来的修法过程中，不仅要注重保障侦查效率和获得证据的真实性及与案件的关联性，更是要将保护公民的隐私权和财产权作为最终落脚点。我们必须要遵循认识论的客观规律，尊重电子证据本身特有的属性，构建真正属于这一新生事物的证据规则[44]。加强《刑事诉讼法》与《个人信息保护法》《网络安全法》《数据安全法》等的衔接，保持法与法之间的协调性，在立法层面逐步建立起专门化、专业化、具体化的电子数据取证规范。

参考文献

[1] 陈卫东. 《刑事诉讼法》第四次修改前瞻[J]. 政法论坛, 2024, 42(1).

[2] 谭秀云. 刑事电子数据取证的法律困境及其程序控制[J]. 时代法学, 2023, 21(5): 56-65.

[3] Serena Quattrocolo. Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion[M]. Cham: Springer, 2020: 73.

[4] 北京市第一中级人民法院（2016）京 01 刑终 592 号刑事裁定书.

[5] Olmsted v. United States, 277 U.S. 438, 474 (1928).

[6] 温祖德. 调取历史性行动电话基地台位置资讯之令状原则——自美国 Carpenter 案之观察[J]. 月旦法学杂志, 2020(2): 98-115.

[7] 龙宗智. 寻求有效取证与保证权利的平衡[J]. 法学, 2016(11): 120-133.

[8] [日]田口守一. 刑事诉讼法(第七版)[M]. 张凌, 于秀峰, 译. 北京: 法律出版社, 2019: 53.

[9] [日]酒卷匡. 刑事诉讼法[M]. 东京: 有斐阁, 2015: 105.

[10] [日]酒卷匡. 新的证据收集手段——提出命令[J]. 法学家, 2002(1228).

[11] Riley v. California，134 S.Ct.2473，2491.

[12] 褚福民. 电子数据合法性规则体系研究[J]. 证据科学, 2023, 31(4): 5-20.

[13] [日]川出敏裕. 计算机犯罪与侦查程序[J]. 法曹时报, 2001, 53(10).

[14] [日]长沼范良. 高科技犯罪与刑事程序的完善[J]. 法学家, 2003(1257).

[15] [日]酒卷匡. 新的证据收集手段——提出命令[J]. 法学家, 2002(1228).

[16] [日]长沼范良. 通讯监听与通讯企业员工的一般协助义务[J]. 研修, 2003(656).

[17] [德]托马斯·魏根特. 德国刑事程序法原理[M]. 江溯, 等译. 北京: 中国法制出版社, 2021: 37.

[18] Wohlers, “ξ94” (n67): 41.

[19] 51 BGHSt 211 (2007).

[20] 120 BVerfGE 274, 319-20, 327-28 (2008).

[21] Tobias Singelnstein. Verhältnismäßigkeitsanforderungen für strafprozessuale Ermittlungsmaßnahmen[J]. Juristenzeitung, 2012: 601.

[22] 103 BVerfGE 142; 113 BVerfGE 29.

[23] [德]托马斯·魏根特. 德国刑事程序法原理[M]. 江溯, 等译. 北京: 中国法制出版社, 2021: 92.

[24] U.S. Dep’t of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, pts.77 n.13 (2002).

[25] United States v. Bryant, 1995 WL 555700 (S.D.N.Y. Sept. 18, 1995).

[26] 王兆鹏. 美国刑事诉讼法[M]. 北京: 北京大学出版社, 2005: 102.

[27] Warden v. Hayden, 387 U.S. 294 (1967).

[28] Katz v. United States, 389 U.S. 347 (1967).

[29] Tamura v. United States, 694 F.2d 591 (9th Cir. 1982).

[30] United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005).

[31] 李荣耕. 电磁记录的搜索及扣押[J]. 台大法学论丛, 2012, 41(3): 1089-1134.

[32] 台湾最高法院 99 年度台上字第 4117 号判决.

[33] 王兆鹏. 刑事诉讼法讲义[M]. 台北: 元照出版公司, 2009: 86.

[34] 黄朝义. 刑事诉讼法[M]. 台北: 元照出版公司, 2009: 221.

[35] 谢登科. 电子数据的取证主体：合法性与合技术性之间[J]. 环球法律评论, 2018, 40(1): 83-99.

[36] 谢登科. 电子数据的取证主体：合法性与合技术性之间[J]. 环球法律评论, 2018, 40(1): 83-99.

[37] Julian Rivers. Proportionality and Variable Intensity of Review[J]. 65 Cambridge Law Journal, 2006: 198.

[38] J. Bomhoff. Balancing the Global and the Local: Judicial Balancing as a Problematic Topic in Comparative (Constitutional) Law[J]. 31 Hastings Int. & Comp. L. Rev., 2008: 555.

[39] United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

[40] William J. Stuntz. Local Policing after the Terror[J]. 111 Yale L.J., 2002: 2137, 2184-85.

[41] 彭俊磊. 大数据侦查法治化研究[M]. 北京: 北京大学出版社, 2023: 188.

[42] Radina Stoykova. The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations[J]. 49 Computer Law & Security Review, 2023: 9.

[43] [英]弗里德里希·冯·哈耶克. 自由秩序原理(上册)[M]. 邓正来, 译. 北京: 三联书店, 1997: 183.

[44] 樊崇义, 李思远. 论电子证据时代的到来[J]. 苏州大学学报(哲学社会科学版), 2016, 37(2): 99-106.