主题研讨

论侦查机关电子数据调取权及其程序控制

——以《数据安全法(草案)》第32条为视角

谢登科

内容提要:《数据安全法(草案)》第32条是我国首次在立法层面明确规定电子数据调取的主体、目的和审批程序,这对于实现我国电子数据取证法治化具有重要意义。该条要求调取电子数据需要"经过严格的批准手续",在法定性质上将电子数据调取界定为与技术性侦查相类似的强制性侦查,这与现有司法解释和部门规章对电子数据调取的法律定性相互矛盾。因此,有必要先厘清电子数据调取行为及其法律条款的法律性质。电子数据作为网络信息时代案件审理的"证据之王",其存在形态和取证模式与传统实物证据存在较大差异,这就决定了电子数据调取在传统刑事诉讼制度中的三重悖论。在《数据安全法(草案)》中构建电子数据调取制度时,既应当考虑电子数据调取行为的法律性质,保持其与现有刑事诉讼制度和证据制度的融贯性,也应当设置适应电子数据自身特征的程序性保障措施。

关键词:电子数据调取　强制性侦查　任意性侦查　权利保护

谢登科,吉林大学法学院教授。

随着网络信息技术和人类生产生活的深度融合,犯罪形态也发生了变化,无论是传统的财产犯罪、暴力犯罪,还是计算机犯罪、网络犯罪、数据犯罪等新型犯罪,都会出现电子邮件、短信、微信等电子数据,电子数据已经成为网络信息时代的"证据之王"。[1] 2012年《刑事诉讼法》出台前,亦有学者将电子数据称为电子证据。[2] 电子数据的本质是"0""1"二进位数字,此种数字信息会借助于相应设备以光电信号予以显示。因此,电子数据实际上就是电子证据,电子数据侧重于内在本质,电子证据侧重于外在形式,二者之间并无本质区别。由于《刑事诉讼法》采取"电子数据"的概念,因此本文亦采纳电子数据的概

〔1〕 参见刘品新:《电子证据的基础理论》,《国家检察官学院学报》2017年第1期,第151－159页。

〔2〕 参见何家弘主编:《电子证据法研究》,法律出版社2002年版,第5页。

念。虽然《刑事诉讼法》第50条已经将电子数据列为刑事诉讼中的法定证据种类之一，但并未规定与电子数据的证据形态、取证模式相匹配的侦查取证行为类型。最高人民法院、最高人民检察院、公安部（下称“两高一部”）2016年出台《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》（下称“《电子数据规定》”），公安部2019年出台《公安机关办理刑事案件电子数据取证规则》（下称“《电子数据取证规则》”）专门规定了电子数据侦查取证行为。在网络信息时代，电子数据不仅是刑事诉讼中认定案件事实的“证据之王”，还承载了公民通信自由权、财产权、隐私权等基本权利。仅由司法解释或部门规章来规范干预或侵犯公民基本权利的电子数据取证行为，既不利于电子数据取证的法治化与规范化，也不利于网络信息时代公民基本权利保障。

《数据安全法（草案）》第32条规定了侦查机关的数据调取权和有关组织、个人的配合义务。[3] 从该草案第2条对“数据”的界定来看，其包括任何以电子或非电子形式对信息的记录，这里的“调取数据”就包括电子数据调取。这是我国首次从立法层面专门规定侦查机关电子数据调取权，对于实现我国电子数据取证规范化、法治化具有重要意义。在网络信息时代，犯罪嫌疑人虽然也自行占有和保管部分电子数据，但大部分电子数据是由作为网络运营商、服务商、系统管理人等案外第三方主体保管或占有。互联网用户、手机用户在绝大多数情况下都将其相关信息存储于第三方主体所拥有的服务器或者存储设备中，与个人用户相比，网络运营商、服务商、系统管理商等第三方主体可以较为方便地读取私人信息、查看存储信息、查看相关登录信息，也能够很方便地接触和控制上述信息，当然这种对用户信息的读取、接触和控制应当符合相关合规要求。因此，在互联网信息时代，侦查机关向案外第三人收集电子数据就成为常态。但是，电子数据调取行为的法律性质本身存在较大争议，比如对通信、通话记录的调取。有学者将通信、通话记录纳入通信秘密范畴，主张对其调取行为属于强制性调查（侦查）。[4] 也有学者从保护隐私视角，认为电子数据调取行为属于任意性调查（侦查）。[5] 而对电子数据调取行为法律性质的不同界定，将直接影响其制度设计与建构。由于《数据安全法（草案）》第32条在规定电子数据提取规则时，采取了概括性授权和空白规定的立法模式，其有效实施涉及与现有法律法规之间的衔接和融贯，可能为国家专门机关不当限缩或者扩张适用留下空间。因此，有必要以《数据安全法（草案）》第32条为基础对侦查机关电子数据调取权进行专门探讨。

一 《数据安全法（草案）》第32条的规范分析

《数据安全法（草案）》以数据安全和数据权益保障为主要立法目的，该法第32条对电子数据调取的主体、目的、程序等内容做出了明确规定。

〔3〕《数据安全法（草案）》第32条规定：“公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。”

〔4〕参见王锴：《调取查阅通话（讯）记录中的基本权利保护》，《政治与法律》2020年第8期，第107－119页。

〔5〕参见杜强强：《法院调取通话记录不属于宪法上的通信检查》，《法学》2019年第12期，第78－87页。

（一）电子数据调取主体的法定性

《数据安全法（草案）》第 32 条将电子数据调取主体限定于公安机关和国家安全机关。公安机关是国家治安保卫机关，担负着维护国家安全和社会治安保卫任务，大部分刑事案件的侦查工作都由公安机关承担。国家安全机关则是负责保卫国家安全的专门机关，也承担着对危害国家安全刑事案件的侦查工作。为了侦破刑事案件、查明案件事实，应当赋予公安机关、国家安全机关电子数据调取权。但是，从司法实践来看，电子数据调取权的主体并未局限于上述两类国家专门机关。除上述两类主体外，军队保卫部门、海警局、监狱也对某些特定类型的刑事案件享有侦查权，应当赋予上述国家专门机关电子数据调取权。在国家监察体制改革之后，监察委员会享有对国家公职人员职务犯罪的调查权，其在职务犯罪调查中也应当享有电子数据调取权。《监察法》第 18 条第 1 款就赋予了监察机关证据调取权。〔6〕 监察机关作为我国行使国家监察职能的专责机关，不仅享有对职务犯罪案件的调查权，也享有对公职人员职务违法案件的调查权。这就意味着其既可以在职务犯罪中调取证据，也可以在职务违法案件中调取证据。此外，法院作为国家的审判机关，其在查明案件事实中也享有电子数据调取权。《刑事诉讼法》第 54 条第 1 款不仅赋予公安机关、检察院证据调取权，也赋予法院证据调取权。〔7〕 最高人民法院《关于互联网法院审理案件若干问题的规定》第 5 条第 2 款就赋予电子商务平台经营者等主体向互联网法院提供涉案电子数据的义务。〔8〕 该规定虽未明确互联网法院有电子数据调取权，但却可以从电子商务平台经营者等主体的电子数据提供义务中推导出来。电子商务平台经营者等主体对涉案电子数据的提供义务，并非源于案件当事人的举证责任，而是源于其对法院调取电子数据时的配合义务。监察委员会、法院对电子数据的调取具有正当性，应当将这些主体纳入电子数据调取主体范围之内。

（二）电子数据调取目的的正当性

《数据安全法（草案）》第 32 条要求国家安全机关、公安机关“因依法维护国家安全或者侦查犯罪的需要”，才可以调取电子数据。由于电子数据可能承载着公民通信自由权、财产权、隐私权等基本权利，而这些基本权利要求排除他人干涉或侵犯，除非基于正当目的和法定程序。“因依法维护国家安全或者侦查犯罪的需要”就构成了电子数据所承载基本权利的边界，基本权利主体此时就对电子数据调取具有容忍义务。国家安全机关、公安机关可以基于上述目的调取电子数据，若不能调取，则可能会阻碍查明犯罪事实，损害国家安全和社会秩序。作为证据使用的电子数据，不仅会出现在刑事案件侦查中，在其他案件事实的调查中也可能会涉及。比如监察机关作为我国行使国家监察职能的专责机

〔6〕《监察法》第 18 条第 1 款规定：“监察机关行使监督、调查职权，有权依法向有关单位和个人了解情况，收集、调取证据。有关单位和个人应当如实提供。”

〔7〕《刑事诉讼法》第 54 条第 1 款规定：“人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。”

〔8〕《关于互联网法院审理案件若干问题的规定》第 5 条第 2 款规定：“互联网法院审理案件所需涉案数据，电子商务平台经营者、网络服务提供商、相关国家机关应当提供，并有序接入诉讼平台，由互联网法院在线核实、实时固定、安全管理。”

关,除了享有对职务犯罪案件的调查权外,还享有对公职人员职务违法案件的调查权,因此可以在职务违法案件中调取电子数据。法院在民事案件审理中也可能调取电子数据,比如在债务纠纷中,法院向网络平台调取微信转账记录。在互联网法院管辖的案件中,法院可以向电子商务平台经营者、网络服务提供商等第三方主体调取涉案电子数据。此时,法院依职权调取电子数据是为了弥补当事人取证能力不足或者为了保护国家利益、社会公共利益。此种目的也具有正当性,应将其纳入电子数据调取范围。

(三)调取电子数据审批程序的严格性

《数据安全法(草案)》第32条要求调取电子数据"应当按照国家有关规定,经过严格的批准手续"。其采取了空白规定的方式,条款本身虽然要求调取电子数据需要经过"审批手续",但并未规定审批标准、审批主体、审批程序等内容,其审批手续则需要参照其他法律、法规的规定。《刑事诉讼法》第54条第1款赋予法院、检察院、公安机关证据调取权,但并未规定证据调取的批准程序,即并未要求调取证据应当经过批准。最高人民检察院发布的《人民检察院刑事诉讼规则》(下称"《刑事诉讼规则》")第169条在规定初查阶段调查措施时,明确了在初查阶段可以调取证据材料。[9]此规定显然是将"证据调取"定位为任意性侦查,这就意味着"证据调取"无须经过审批程序,办案人员就可以决定是否采取"证据调取"。而《电子数据取证规则》第41条虽然规定公安机关调取电子数据需要经过审批,[10]但从该条所规定的批准主体来看,其仅要求"办案部门负责人批准",而无需取得县级以上公安机关负责人批准。这与搜查、冻结等强制性侦查措施的批准主体形成鲜明对比,因为适用这些强制性侦查措施都需要取得县级以上公安机关负责人批准。仅从批准主体角度来看,《电子数据取证规则》第41条所规定的批准程序,并没有体现出《数据安全法(草案)》第32条中批准手续"严格性"的要求。若从用语表述来看,我国《刑事诉讼法》仅在技术侦查中要求"经过严格的批准手续",其通常对审批主体的行政级别会有更高要求。而对于电子数据调取是否要求和技术侦查同样的审批程序,则直接涉及对其法律性质的定位,关于这一点后文将详细分析。

(四)有关组织、个人负有配合电子数据调取的义务

证据调取与证据搜查不同,搜查通常由侦查机关自行搜寻、查找被调查对象所占有或控制的证据,而被搜查对象通常没有主动交出其占有或者控制证据材料的义务。证据调取在本质上属于双方行为,即它是作为侦查机关在知悉有关组织或者个人占有、控制相关证据材料时,通知有关组织或者个人交出该证据材料,有关组织或者个人在收到调取证据通知后,需要将其占有、控制的证据材料交给侦查机关。若缺乏有关组织或者个人的配合,则取证主体通常无法完成证据的调取工作。因此,在证据调取中,通常需要被调取的

〔9〕《刑事诉讼规则》第169条规定:"进行调查核实,可以采取询问、查询、勘验、检查、鉴定、调取证据材料等不限制被调查对象人身、财产权利的措施。不得对被调查对象采取强制措施,不得查封、扣押、冻结被调查对象的财产,不得采取技术侦查措施。"

〔10〕《电子数据取证规则》第41条规定:"公安机关向有关单位和个人调取电子数据,应当经办案部门负责人批准,开具《调取证据通知书》,注明需要调取电子数据的相关信息,通知电子数据持有人、网络服务提供者或者有关部门执行。"

组织或者个人予以配合。比如《刑事诉讼法》第 54 条第 1 款在授予公检法机关证据调取权时,也规定了有关单位和个人如实提供证据的义务。《数据安全法(草案)》第 32 条也注意到电子数据调取的特性,在赋予侦查机关电子数据调取权时,规定了有关组织和个人的配合义务。此种配合义务在本质上是一种附条件的信息披露义务。[11] 由于电子数据往往承载着公民通信自由权、财产权、隐私权等基本权利,而作为网络运营商、网络服务商的第三方主体,需要按照其与网络服务使用者之前订立的合同履行保密义务和基本权利保护义务。在电子数据调取中,第三方主体配合义务的履行,则可能意味着其对网络服务使用者保密义务和隐私保护义务的违反。这就需要在第三方主体的信息保密义务和披露义务之间建立一种有效平衡机制,主要体现为对其适用条件和运行程序的设置。对于第三方信息披露义务,若缺乏法定程序和正当事由的控制,很容易侵害网络服务使用者的通信自由权、财产权、隐私权等基本权利。因此,在电子数据调取中,第三方主体的配合义务应当以其调取主体合法、目的正当和审批程序合法为前提。这就要求国家专门机关在调取电子数据前,向网络运营商、网络服务商等第三方主体出示身份证件、调取通知书等手续。第三方主体在履行上述配合义务前,需要对上述手续予以审查。

二 电子数据调取权的法律性质

对于电子数据调取法律性质的分析,既有助于深入分析其现有规则和实践运行,也有助于指导构建科学的电子数据调取制度。基于对电子数据调取法律性质的不同定位,对具体制度的建构可能存在截然不同的方案,对于其实践运行也存在截然不同的评判。因此,有必要先厘清电子数据调取的法律性质。

(一)强制性侦查权抑或任意性侦查权

《数据安全法(草案)》第 32 条要求调取电子数据需“经过严格的批准手续”。此种“严格批准手续”的要求,《刑事诉讼法》仅在技术侦查措施的规定中有类似的表述。该法第 150 条第 1 款规定公安机关只有“经过严格的批准手续”,才可以采取技术侦查措施。从适用对象来看,技术侦查仅适用于重大刑事案件;从审批主体来看,技术侦查对审批主体行政级别要求更高。由于我国尚未建立强制性侦查的司法审查程序,不是由处于中立、超然地位的法官通过签发令状来赋予强制侦查权,而主要是由侦查机关内部通过行政化审查方式赋予强制侦查权。提高审批机关的行政级别就成为实现“严格批准”程序的重要方式。[12] 对于搜查、冻结等强制性侦查措施的适用,仅需要县级以上公安机关负责人审批。而根据公安部的《公安机关办理刑事案件程序规定》(下称“《刑事案件程序规定》”)第 265 条第 1 款之规定,适用技术性侦查措施,需要“报设区的市一级以上公安机关负责人批准”,即地级市以上公安机关负责人才有权批准。因此,也有学者将技术侦查

〔11〕 参见王学光著:《电子证据法律问题研究》,法律出版社 2019 年版,第 142 – 144 页。

〔12〕 参见胡铭:《技术侦查:模糊授权抑或严格规制——以〈人民检察院刑事诉讼规则〉第 263 条为中心》,《清华法学》2013 年第 6 期,第 36 – 45 页。

称为“超强制性侦查措施”。若仅从《数据安全法(草案)》第32条规定中对调取电子数据所要求的“严格批准手续”来看,其法律性质应当与技术侦查相同,即都属于超强制性侦查措施,其审批层级要求应当更高,适用对象应当更为严格。在适用电子数据调取时,也应当取得地级市以上公安机关负责人批准。从这个角度来看,《数据安全法(草案)》是将电子数据调取定位为与技术侦查具有相同法律性质的侦查措施。

但是,我国现有的司法解释和部门规章主要是将电子数据调取定性为任意性侦查。《电子数据取证规则》第41条规定,调取电子数据仅需要“经办案部门负责人批准”,并不像搜查等强制性侦查措施,需经“县级以上侦查机关负责人”审批,这显然降低了审批主体的行政层级。上述规定主要吸收了《刑事案件程序规定》第62条规定的内容,仅要求公安机关在调取证据时,应“经办案部门负责人批准”。也就是说,《电子数据取证规则》和《刑事案件程序规定》都将电子数据调取界定为任意性侦查,其审批程序要比搜查等强制性侦查措施的审批程序更为宽松。《刑事诉讼规则》第169条在列举初查中可以采取的调查措施时,明确将“调取证据材料”列入其中。由于在初查时,刑事诉讼程序尚未启动,仅能采取不侵犯被调查对象人身权利和财产权利的任意性侦查措施,而禁止适用侵害公民人身、财产权利的强制性侦查措施。《刑事诉讼规则》第169条允许在初查中“调取证据材料”,显然认为这种调取行为不会侵犯公民人身权、财产权等基本权利,在法律性质上将其界定为任意性侦查。而“调取电子数据”作为“调取证据材料”的下位概念,其法律性质也自然属于任意性侦查。任意性侦查通常并不会侵犯公民基本权利,故法律对其程序控制就相对宽松。

通过对《数据安全法(草案)》第32条和我国司法解释、部门规章中有关电子数据调取规范的分析发现,它们对调取电子数据法律性质的界定是相互矛盾和冲突的。这就导致其各自对电子数据调取行为的程序控制措施存在较大差异。因此,在设计电子数据调取制度前有必要厘清其法律性质。强制性侦查与任意性侦查的主要区别,并不在于其是否直接使用有形的强制力,而在于是否会侵犯被调查人的基本权利。[13] 如若某一侦查行为会侵犯被调查对象的基本权利,则属于强制性侦查,反之则属于任意性侦查。在确定“调取电子数据”法律性质时,应当考察电子数据是否承载公民基本权利和第三人意愿。电子数据不仅种类繁多,且其范围有逐渐扩大的趋势。有些电子数据可能承载公民基本权利,比如电子邮件、手机短信、网盘信息、电子交易记录、计算机程序、数据库等,它们承载着公民通信自由和通信秘密权、隐私权、财产权等基本权利;有些电子数据可能并未承载公民基本权利,比如网页、微博上公开发布的信息等。从司法实践来看,侦查机关在刑事案件中调取的电子数据绝大多数都是通信类电子数据和交易类电子数据,这些电子数据都承载着通信自由和通信秘密权、隐私权、财产权等基本权利。而对于网上公开发布的电子数据通常无需借助于网络服务商等第三方调取,侦查机关可以自行通过下载、提取等方式来收集。从这个角度看,电子数据调取在法律性质上,有些属于强制性侦查,有些属于任意性侦查。

〔13〕 参见[日]田口守一著:《刑事诉讼法》,张凌、于秀峰译,法律出版社2019年版,第53-58页。

在强制性侦查和任意性侦查理论中,若被调查人自愿同意侦查机关采取强制性侦查措施,就意味着其自愿放弃权利,此时强制性措施就会转化为任意性措施。比如在搜查中,房屋所有权人自愿同意侦查机关搜查,则侦查机关可以采取无证搜查,因为被搜查人的同意就表示其自愿放弃基本权利中的排他效力,侦查机关的搜查并不会侵害被调查人的基本权利。但是,在电子数据调取中,电子数据的控制主体与基本权利主体相分离。比如调取电子邮件,电子邮件存贮于网络服务商的服务器中,网络服务商占有控制服务器及其中存储的电子数据,但是电子邮件所承载的通信自由和通信秘密权的主体是电子邮箱用户。作为第三方主体的网络服务商、网络运营商不能替代客户决定是否放弃电子数据上所承载的基本权利,即便其作出了同意侦查机关调取电子数据的意思表示,也不能让具有强制侦查性质的电子数据调取行为转化为任意侦查。由于电子数据承载着公民隐私等基本权利,作为网络运营商、网络服务商的第三方主体,需要按照其与用户之间订立的合同履行保密义务和基本权利保护义务。这种义务决定了网络服务商、网络运营商等第三方主体不能随意处分及披露其用户电子邮件、交易记录等信息。因此,第三方主体虽然有配合调取电子数据的义务,但却无权代替用户放弃电子数据所承载的基本权利。

(二)概括性授权抑或特别性授权

《刑事诉讼法》第 54 条第 1 款赋予法院、检察院和公安机关证据调取权;第 115 条赋予公安机关立案后的证据材料调取权。有学者将上述规定界定为"概括性条款",[14]认为仅是一般性赋予侦查机关调取证据的权力,至于采取何种措施调取证据,则需要根据《刑事诉讼法》在"侦查"一章中对具体侦查措施所做的规定。概括性条款仅能为权利干预性较小的侦查措施提供法律依据,而不得作为可能会对基本权利造成严重侵犯的侦查措施的授权依据。参与《刑事诉讼法》修订的专家也持相同观点,认为该条仅概括性赋予了三机关收集、调取证据的权力,而公检法机关收集、调取证据的具体程序和规范,则在《刑事诉讼法》关于侦查、起诉和审判的章节中予以具体规定。[15]

在概括授权条款与特别授权条款的相互关系上,可能存在不同理解。如果从狭义层面界定概括授权条款,将概括授权条款与特别授权条款理解为相互对立的关系,即特别授权条款仅适用于强制性侦查,故需要法律的明确授权,而概括授权条款仅适用于任意性侦查,法律规定可以相对概括。而如果从广义层面界定概括授权条款的话,则将特别授权条款作为对概括授权条款的细化和具体化,无论是对任意性侦查的授权,还是对强制性侦查的授权,都是对概括授权条款的具体化。将"调取证据"作为概括性授权规定,就意味着其可以涵盖不同类型和形态的证据调取行为。从司法解释和实践运行来看,调取证据有时也被作为一项独立的、具体的侦查措施,这主要是在狭义层面做出的界定。比如《刑事诉讼规则》第 169 条将"调取"与勘验、询问等侦查措施并列为可以在初查阶段开展的调查活动。将"调取证据"作为侦查概括条款,主要源于侦查行为类型具有多样性和动态性的特点,《刑事诉讼法》不可能详尽而明确地规定所有侦查措施,只能对具有较强权利干

〔14〕 参见艾明:《刑事诉讼法中的侦查概括条款》,《法学研究》2017 年第 4 期,第 155 - 172 页。

〔15〕 参见李寿伟著:《中华人民共和国刑事诉讼法解读》,中国法制出版社 2018 年版,第 130 页。

预性的侦查措施予以特别规定，而对于权利干预性较轻的侦查措施则只能由概括性条款作为其法律授权依据，以满足法律保留主义的底线要求。〔16〕 因此，将“调取证据”作为侦查概括性条款，可以兼顾法律保留主义和侦查程序自由形成原则的需要。

但是，《数据安全法（草案）》第 32 条中对调取电子数据的规定并未采取广义层面的概括性条款，而是将其作为具体授权的特别性规定；同时也没有采取狭义概括性授权条款，而是将其作为一项独立强制性侦查措施的具体授权条款。该条明确规定了电子数据调取的主体、目的、程序等要件，虽然对于审批程序的具体规定需要援引其他法律规定，但其明确要求电子数据调取需要“经过严格的批准手续”。该条对调取电子数据采取具体授权的特别性规定，主要源于其将“调取电子数据”界定为强制性侦查，调取电子数据需要采取强制性措施，会干预或侵害公民基本权利。强制性侦查措施只能在法律限定的领域，其实施需要取得法律授权和令状授权。将电子数据调取作为一种具体授权的特别性规定，有利于该规则的稳定性与明确性，更有利于保障电子数据所承载的通信秘密权、财产权、隐私权等基本权利，但是可能无法有效适应侦查活动所具有的流动性、灵活性等特点。

另外，由于电子数据种类繁多、生成机理差异较大，并且信息技术的不断发展会带来更多新型电子数据，比如云存储电子数据、区块链电子数据等，由此可能会衍生出很多新型电子数据调取技术和措施，电子数据存在形态、生成机理、占有主体等因素的差异决定了对其“调取”的法律性质也不尽相同。以视频数据的调取为例，在信息技术与视频技术高度融合的时代，绝大多数视听资料已经变成了视频数据，视频数据在本质上属于电子数据的一种。视频监控广泛存在于道路交通、街面安防、智能卡口、营业场所等领域。在侦查实践中，对视频数据的调取，可能是在现场勘验检查中发现的某一具体计算机及其视频数据，可能是在搜查中发现的某一具体移动硬盘及其视频数据，也可能是在案件现场附近出现的具体网盘及其视频数据，还有可能是在扣押中遇到的具体移动终端及其视频数据。〔17〕《数据安全法（草案）》第 32 条对调取电子数据作具体授权的特别性规定，可能无法有效涵盖上述电子数据调取的不同行为形态。

三　侦查机关电子数据调取的三重悖论

传统刑事诉讼制度和刑事证据制度，主要是以物质世界中实物证据和言词证据为基础进行设置，这些取证规则和证据审查规则能够有效适应物质世界中惩罚犯罪和权利保障的需求。但是，电子数据作为网络信息空间的“证据之王”，其存在形态、取证模式与传统实物证据存在较大差异，这就决定了电子数据调取与现有刑事诉讼制度可能存在各种悖论。

（一）电子数据海量性与调取范围确定性的悖论

侦查机关在调取证据时，需要在《调取证据通知书》中详细列明调取证据的名称、内

〔16〕 参见［日］田口守一著：《刑事诉讼法》，张凌、于秀峰译，法律出版社 2019 年版，第 155－172 页。

〔17〕 参见李双其、林伟著：《侦查中电子数据取证》，知识产权出版社 2018 年版，第 202－211 页。

容等信息,否则第三方主体因无法清楚知悉调取证据的范围而无法有效配合执行。通过详细列明调取证据的范围,既保障了调取证据的关联性,防止与案件不具有关联性的材料进入诉讼程序中,也可以防止在向第三方调取证据中扩大或者限缩证据范围,从而损害被调查人的基本权利或者阻碍案件事实认定。物证、书证等传统实物证据具有的物质形态,可以被人们所直接感知,通常可以在《调取证据通知书》中较为清晰、明确地予以描述。但是,电子数据具有无形性与海量性的特征,在形态上是存储于虚拟空间的各种"0""1"数字组合,这就决定了用肉眼无法直接观察和感知,只有借助于特定软件和硬件设备以及相关技术才能生成和展示,从而被肉眼所见。因此,对于很多电子数据的调取范围可能无法在《调取证据通知书》中予以清晰描述和界定,可能导致电子数据调取范围不当扩大或限缩。

《电子数据规定》第 13 条规定,需要注明调取电子数据的相关信息,这里的"相关信息"既包括直接反映案件事实的信息,也包括反映涉案数据存储状态及其背景的信息。[18] 从司法实践来看,为了防止遗漏相关电子数据和再次调取所导致的重复性工作,第三方主体在执行中会倾向于扩大电子数据调取范围,正如"顺亨汽贸公司走私普通货物案"所反映的情况。[19] 在该案中,侦查机关就通过网络服务商调取了 30 个涉案邮箱中的 20 万封电子邮件。但这些邮件并不是都和案件具有关联性,网络服务商显然不当扩大了电子邮件的调取范围。电子邮件承载的公民通信自由和通信秘密权属于宪法性权利,不当扩大电子邮件的调取范围就意味着违法干预或侵犯了公民基本权利。电子邮件调取范围的不当扩大,与电子数据的海量性和虚拟性不无关系。电子邮件的虚拟性决定了 20 万封电子邮件的存储不会占据大量的物理空间,而仅用一个体积很小的 U 盘便可将其拷贝存储。电子邮件的海量性决定了第三方主体没有时间和精力查阅 20 万封电子邮件的关联性。另外,搜查电子数据和调取电子数据的执行机制不同也可能导致扩大调取的数据范围。搜查通常由侦查人员搜寻、查找电子数据,办案人员和搜查的执行人员内部通常具有同一性。此种同一性可以保障侦查人员熟知案情,在搜查中可以依照搜查证中记载的范围收集与案件有关的证据。在证据调取中,办案人员和调取执行人不具有同一性,调取的执行主体通常是占有和控制证据材料的第三方主体,其可能对电子数据的所在位置、存储状态等信息较为熟悉,但对与案件事实的有关情况可能并不知悉,这就可能会导致第三方主体在调取数据中扩大范围,从而损害电子数据所承载的公民基本权利。

(二)电子数据多样性和调取性质二元性的悖论

《数据安全法(草案)》第 32 条在法律性质上将"电子数据调取"界定为强制性侦查,

〔18〕 参见李双其、林伟著:《侦查中电子数据取证》,知识产权出版社 2018 年版,第 100 - 101 页。

〔19〕 参见《刑事审判参考》2013 年第 4 集(总第 93 集)第 873 号案例。该案中,被告人及其辩护人认为侦查机关违法调取的电子数据不能作为定案依据。法院经审理后认为:本案的非法交易没有采用传统的电话、传真等传输手段,而选择了网络传输途径。从签订合同、单证往来到付汇、收款等,均用电子邮件、MSN、QQ 等进行。向中立第三方调取电子数据,是计算机取证体系的重要组成部分。在我国,向第三方调取电子数据具有明确的法律依据。本案侦查机关向网络服务商调取 30 个涉案电子邮箱中的 20 万封电子邮件,经筛选后将其中部分作为电子数据提交法庭。侦查机关在调取电子数据时,向网络服务商出示了《调取证据通知书》《介绍信》等材料。上述电子数据调取程序符合法律、法规规定,故可以作为定案依据。

故其适用需要经过“严格的审批程序”。但是,强制性侦查和任意性侦查区分的主要标准是调查行为或者侦查行为是否会侵犯被调查人的基本权利。在网络社会中,电子数据涵盖范围广泛、种类繁多,有些电子数据可能承载公民基本权利,有些电子数据可能并未承载公民基本权利。在构建电子数据调取制度时,若不考虑电子数据性质及其承载权利情况,一概将其界定为强制性侦查或者任意性侦查,可能都不利于有效侦查和权利保障的实现。但是,若严格遵循《数据安全法(草案)》第32条的要求,对于并未承载公民基本权利电子数据的调取,也要求经过“严格的审批程序”,不仅无法实现审批程序特别授权中保护公民基本权利的价值功能,也不利于提高侦查效率和实现侦查程序自由形成原则,比如在“黎某、张某非法获取计算机信息系统数据案”中,[20]作为比特币交易价格信息的电子数据,通常是对社会公众公开发布,其本身并不承载公民财产权、隐私权等基本权利。任何普通公民都可以登录网站下载复制,侦查机关自然也可以提取复制该电子数据。若按照《数据安全法(草案)》第32条的要求,对于此类电子数据的调取也需要“严格的审批程序”,显然是司法资源的浪费。电子数据的多样性决定了并非所有电子数据都承载公民基本权利,一概将其界定为任意性侦查或强制性侦查可能都不合理。在该案中,辩护方虽然对电子数据调取程序的合法性提出异议,但其主要并不是从调取程序侵犯公民基本权利的角度来主张电子证据排除,而是认为调取电子数据违反相应的固定和保全程序,无法保证电子证据的真实性与完整性,从而主张证据排除。这表明由于强制性侦查会干预公民基本权利,其程序设置不仅需要考虑在取证过程中如何保障公民的基本权利,也需要考虑如何保障电子数据的真实性和完整性。而任意性侦查不会干预公民基本权利,其制度设计的重点在于如何通过相应程序保障电子数据的真实性与完整性。

(三)电子数据依附性与调取模式双重性的悖论

电子数据的虚拟性决定了其需要依附于相应存储介质而存在,这种存储介质既可以是其原始存储介质,也可以是原始存储介质以外的其他存储介质。这就决定了电子数据取证存在“一体收集”模式和“单独提取”模式。[21] 在不同模式中,电子数据取证对权利干预形态、证据鉴真程序等方面并不完全相同。比如电子数据的“一体收集”模式,通常需要两步搜索,即先对其原始存储介质予以搜查、扣押,然后再对其中存储的电子数据进行搜查。在美国刑事司法中,此两步搜索通常需要两次分别向法官申请签发搜查令。[22]具体到电子数据的调取,也有两种模式,即“一体调取”模式和“单独调取”模式。前者是侦查机关将电子数据连同其原始存储介质一并向第三方主体调取;后者是侦查机关仅向第三方主体调取涉案电子数据,第三方主体将所调取电子数据存储在其他存储介质之中,

〔20〕 参见辽宁省阜新蒙古族自治县人民法院(2019)辽0921刑初120号刑事判决书。该案中,侦查机关在乐酷达网络公司调取了2016年11月25日至2016年11月28日的比特币交易价格信息。黎某的辩护律师提出:公安机关向有关单位调取电子数据,应当经办案部门负责人批准,开具《调取证据通知书》,注明需要调取电子数据的相关信息,通知电子数据持有人、网络服务提供者或者有关部门执行。检方出示的卷宗材料中,公安机关调取的电子数据,未附完整性校验值等保护电子数据完整性方法的说明,也未采用录音或录像固定证据内容及取证过程。所调取电子数据不符合法律规定的形式,不可以作为定案依据。

〔21〕 参见谢登科:《电子数据的鉴真问题》,《国家检察官学院学报》2017年第5期,第50-72页。

〔22〕 参见陈永生:《论电子通讯数据搜查、扣押的制度建构》,《环球法律评论》2019年第1期,第5-20页。

而并不调取电子数据的原始存储介质。从权利保障角度来看,电子数据“一体调取”模式,不仅会干预或侵犯电子数据自身所承载的财产权、隐私权、通信秘密权等基本权利,也会侵犯电子数据所依附原始存储介质的财产权。从权利主体来看,电子数据所承载的基本权利通常归属于犯罪嫌疑人、被告人,而原始存储介质的财产权则通常归属于网络服务商、运营商等第三方主体。而“单独调取”模式并不调取、扣押电子数据的原始存储介质,仅涉及电子数据自身所承载的公民基本权利。故而,电子数据调取的两种模式对权利干预的不同决定了审批程序可能存在差异。

从《数据安全法(草案)》第 32 条的表述来看,仅考虑了电子数据调取中的“单独调取”模式,要求调取电子数据需要经过严格的批准程序,并未考虑“一体调取”模式。从实践运行来看,侦查机关调取电子数据绝大多数都采取“单独调取”模式。因为“单独调取”模式相对而言具有更小的权利干预性,仅干预或侵犯电子数据自身所承载的公民基本权利,而不会侵犯原始存储介质的财产权利。对于网络服务商、运营商等第三方主体而言,单独调取电子数据不会对其正常经营行为产生较大影响,他们通常也会自愿配合侦查机关的电子数据调取工作。但是,这并不意味着电子数据的“一体调取”模式在司法实践中并不存在。电子数据调取的执行和调取其他种类证据相同,由侦查人员通知电子数据持有人、网络服务提供商或者有关部门执行。对电子数据调取而言,最佳方案是连同其电子设备、存储介质等原物一并调取;若原始存储介质不便调取或不能调取,才可以采取仅提取电子数据本身的做法,但是,需要在电子数据调取笔录中注明调取过程、原始存储介质所在地点。

四 电子数据调取的制度建构

《数据安全法(草案)》第 32 条对于电子数据调取制度的设计与建构,既应当符合电子数据调取行为的法律性质,也应当契合电子数据虚拟性、可复制性、海量性等特征。具体来说,可以考虑从以下方面建构我国电子数据调取规则。

(一)电子数据调取的广义界定

对于电子数据调取规定应当界定为广义层面的概括性授权条款,以便涵盖不同类型的电子数据调取行为。作为实践中较为常见的取证手段,调取是司法机关依法收集留存于有关单位和个人手中的物证、书证、电子数据等证据材料的一种侦查活动。这里的“有关单位和个人”通常是犯罪嫌疑人、被告人以外的第三方主体。电子数据除了存储于个人电脑、手机等电子设备之中,也海量存储于网络服务商、网络运行商等第三方主体的服务器等电子设备中,他们占有和管理网站网页、微博客、电子邮件、交易记录等大量电子数据。对于电子数据调取的法律规定应采取概括性授权条款,可以根据电子数据的不同形态或其承载不同类型的基本权利,将其区分为不同类型的侦查行为或侦查措施。

对于从网络服务商处调取电子邮件,虽然也称为“调取”,但其对应的具体侦查措施是“邮件检查”和“邮件扣押”。《刑事诉讼法》第 143 条要求扣押邮件,须经公安机关或者检察院批准,然后通知邮电部门检交扣押。在网络信息时代,电子邮件已经替代纸质信件

而成为人们沟通交流的重要途径，在刑事侦查中传统的“纸质信件扣押”就大量演变为“电子邮件扣押”。《刑事诉讼法》第143条并未明确将电子邮件纳入其中。不过，《刑事案件程序规定》第232条规定将电子邮件和邮件、电报纳入“邮件扣押”范围之内，要求扣押应当经县级以上公安机关负责人批准，制作扣押电子邮件通知书，通知网络服务单位检交扣押。在司法实践中，侦查机关往往通过向网络服务商调取电子邮件方式收集涉案电子数据，而不是通过扣押方式来收集。这既源于纸质邮件和电子邮件表现形态的差异性，也源于调取证据和扣押措施的复杂关系。在纸质邮件中，信件中记载的交流信息与其所依附纸质载体具有不可分离性，侦查机关收集纸质邮件证据须对其实际占有、控制；而电子数据所承载的信息与其原始存储介质之间具有可分离性，可以进行具有高度准确性的复制，[23]这就意味着电子邮件收集可以不用实际占有、控制其原始电子数据及原始存储介质。但是，调取邮件主要涉及的并不是干预或侵害公民的财产权，其主要是侵犯公民通信自由和通信秘密权，这种基本权利主要承载于邮件信息之中，而并不取决于侦查机关是否占有控制电子邮件原件及其原始存储介质。在采取邮件扣押措施过程中，需要邮政部门、网络服务商等第三方主体的配合，这就具备了调取证据的基本形态。有学者将调取证据看作是扣押措施的执行和实现方式。[24]此种观点注意到了调取证据和扣押措施之间的竞合关系，但将调取证据作为扣押措施的实现手段，则可能降低调取证据的法律地位。

对于交易记录类电子数据的调取，比如微信、支付宝转账记录等电子数据，在本质上属于对财产状况及其变动信息的查询。财产信息的“查询”仅仅是手段行为，最终是要获取财产状况及其变动信息的证据材料。在传统社会中，个人财产信息主要是以纸质账目方式保存；而在网络信息时代，个人财产信息和交易信息则主要以电子数据方式予以保存。《刑事诉讼法》第143条要求“依照规定”查询存款、汇款等财产信息，主要是考虑到查询措施涉及公民个人隐私，涉及企业正常经营，只有具有侦查权的检察院或者公安机关依照法律规定才可查询。[25]《刑事案件程序规定》第238条规定查询财产信息须经县级以上公安机关负责人批准，[26]实际上是将“查询财产”作为与“搜查”性质相同的强制性侦查。查询是为了知悉犯罪嫌疑人的财产及其变动情况，本身并不会限制或者剥夺犯罪嫌疑人的财产，但是公民财产状况及其变动情况属于个人隐私，查询财产信息会侵犯公民隐私权。公民向金融机构提供自己的财产及其信息是为了进行管理或者获得服务，并不意味着其愿意对外公开财产信息，这些财产信息仍然承载着个人隐私利益。[27]个人财产信息即便被金融机构、网络服务商等主体收集控制，也并不意味着其丧失私密性。对于其他不会干预公民基本权利或者权利干预性较低的电子数据调取，比如前文所

〔23〕 参见王立梅、刘浩阳著：《电子数据取证基础研究》，中国政法大学出版社2016年版，第10页。

〔24〕 参见艾明：《调取证据应该成为一项独立的侦查取证措施吗?》，《证据科学》2016年第2期，第155－166页。

〔25〕 参见李寿伟著：《中华人民共和国刑事诉讼法解读》，中国法制出版社2018年版，第341－344页。

〔26〕 《刑事案件程序规定》第238条规定：“向金融机构等单位查询犯罪嫌疑人的存款、汇款、证券交易结算资金、期货保证金等资金，债券、股票、基金份额和其他证券，以及股权、保单权益和其他投资权益等财产，应当经县级以上公安机关负责人批准，制作协助查询财产通知书，通知金融机构等单位协助办理。”

〔27〕 参见王利明：《论个人信息权的法律保护》，《现代法学》2013年第4期，第62－72页。

述比特币交易价格的调取,则属于任意性侦查的电子数据调取,可以纳入狭义层面的概括性授权条款。

(二)在数据分类基础之上对不同性质的电子数据调取进行程序控制

需要根据电子数据的不同法律性质和所承载基本权利的状况建立数据分类制度,并以此为基础将电子数据调取界定为强制性侦查或任意性侦查施加不同的程序控制。不同类型的电子数据所承载的信息具有不同的法律性质,是否承载以及承载何种基本权利也存在差异,由此决定了电子数据取证对公民基本权利的侵犯程度存在差异。[28] 这就需要结合电子数据具体类型及其法律性质,分析电子数据取证行为的法律性质。在确定电子数据调取的法律性质时亦不例外,需要考察具体类型的电子数据是否承载基本权利以及承载何种基本权利。不过,对电子数据的现有分类主要是考虑到电子数据的生成机理和技术特点,侧重于从信息技术角度对电子数据进行分类,比如将其区分为静态电子数据和动态电子数据,电子生成数据、电子存储数据与电子交互信息,封闭电子数据与网络电子数据,数字电文数据、附属信息数据和系统环境数据等。[29] 上述分类对于从取证技术角度保障电子数据的真实性、可靠性具有积极意义,但却存在电子数据取证中权利保障不足的缺陷。

在为数不多的以法律性质和基本权利为基础对电子数据分类的研究成果中,主要有两种不同区分方法。《电子数据规定》第 1 条在界定电子数据概念和范围时列举了实践中较为常见的四类电子数据,[30] 有学者认为网页等电子平台发布的信息属于公共信息而不涉及公民基本权利,对其调取主要属于任意性侦查;而电子邮件、通信记录、数字证书等后三类电子数据均涉及公民基本权利,对其调取可以归为强制性侦查。[31] 亦有学者将第三方主体所占有和控制的电子数据界定为“部分涉及基本权利”的电子数据,其中第三方主体所掌握的电子通信及云存储“非内容数据”,并未承载涉及公民通信权、隐私权等基本权利内容,对其取证属于任意性侦查;第三方主体所掌握的电子通信、登录凭证保护云存储“内容数据”承载着公民基本权利,对其取证属于强制性侦查。[32] 上述两种分类看似不同,但二者对强制性侦查与任意性侦查的区分标准并无差异,其分类的理论基点也无本质差异,即都将电子数据是否承载公民基本权利作为其区分电子数据取证行为法律性质的理论基点。此两种观点分歧的焦点在于,某些具体类型的电子数据是否承载公民基本

〔28〕 参见裴炜:《比例原则视域下电子侦查取证程序性规则构建》,《环球法律评论》2017 年第 1 期,第 80 – 95 页。

〔29〕 参见赵长江著:《刑事电子数据证据规则研究》,法律出版社 2018 年版,第 47 – 65 页;王立梅、刘浩阳著:《电子数据取证基础研究》,中国政法大学出版社 2016 年版,第 11 – 12 页;李双其、林伟著:《侦查中电子数据取证》,知识产权出版社 2018 年版,第 4 – 13 页。

〔30〕 《电子数据规定》第 1 条规定:“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。电子数据包括但不限于下列信息、电子文件:(一)网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息;(二)手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息;(三)用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息;(四)文档、图片、音视频、数字证书、计算机程序等电子文件。”

〔31〕 参见龙宗智:《寻求有效取证与保证权利的平衡——评“两高一部”电子数据证据规定》,《法学》2016 年第 11 期,第 7 – 14 页。

〔32〕 参见梁坤:《论初查中收集电子数据的法律规制——兼与龙宗智、谢登科商榷》,《中国刑事法杂志》2020 年第 1 期,第 39 – 57 页。

权利的内容,其中就包括第三方主体所占有和控制的电子数据。上述分歧,会直接影响电子数据调取的法律性质界定和具体制度建构。

在建立数据分类保护制度时,是否承载公民基本权利以及承载何种基本权利,应当是电子数据分类的重要标准和依据。涉及公民基本权利的电子数据,通常包括言论表达类电子数据、财产信息类电子数据、通信信息类电子数据、隐私信息类电子数据等。从前人们主要通过报刊、书籍、集会等方式行使言论自由权,而随着网络信息时代的到来,言论信息大量借助网页、博客、朋友圈等网络信息平台来传播。公开的言论表达本身就是为了让公众知悉论者所要表达的思想和内容,对于此类电子数据的调取并不会阻碍言论自由权的行使,因此,对言论表达类电子数据的调取通常属于任意性侦查。此外,人们的财产很多时候也会以电子数据形式存在,比如数字货币、操作系统、软件程序等,这些电子数据自身就具有财产价值。实物财产的交易价值或使用价值往往会依附于物质载体,对实物财产的调取会影响其占有使用。〔33〕但是,电子数据具有虚拟性、可复制性等特征,若电子数据调取行为本身并不影响财产类电子数据的交易、使用价值,则此种调取行为并不会损害其财产权,但可能损害其财产信息所承载的隐私权。若电子数据调取行为本身会影响其交易价值或使用价值,则会侵犯或者干预其所承载的财产权。因此,对财产类电子数据的调取通常属于强制性侦查。以往人们主要借助于纸质信件行使通信自由和通信秘密权,而网络信息时代的通信自由则主要借助于电子邮件、短信、微信等方式。对于此类电子数据的调取会侵害通信自由和通信秘密权。因此,对于通信类电子数据的调取通常属于强制性侦查。过去个人隐私信息通常依附于住宅、汽车等实物,实物所有权和隐私权多数情况下依附于相同主体。而网络信息时代的隐私信息,不仅依附于实物,也海量承载于云盘数据、微信聊天记录、网络登录日志等电子数据之中。这些电子数据可能会被网络运营商、服务商等第三方主体占有,侦查机关在向此类主体调取电子数据时,可能会侵犯公民的隐私权。因此,对隐私类电子数据的调取也应归为强制性侦查。

(三)电子数据调取中权利保障和程序性保障并举

在电子数据调取制度中除了应当遵循传统的权利保障措施外,还应当设置适应电子数据自身特征的程序性保障措施。传统刑事诉讼制度和刑事证据制度,主要是以现实世界中实物证据和言词证据为基础而进行设置,这些取证规则和证据审查规则能够有效适应现实世界中惩罚犯罪和保障权利的需求。但是,电子数据作为网络信息时代的“证据之王”,存在形态和取证模式与传统实物证据存在较大差异。这就决定了构建和设计电子数据调取制度时,不仅需要考虑其与传统刑事诉讼制度和刑事证据制度之间的协调性、融贯性,还应当设置适应电子数据自身特征的程序性保障措施。数据安全立法在构建侦查机关数据调取权制度时,应当采取与《刑事诉讼法》第54条第1款相同的立法表述,采用广义层面概括性授权条款规定侦查机关数据调取权。尽管《数据安全法(草案)》对电子数据调取的具体条件和程序采取了空白规范,但可以适用《刑事诉讼法》《监察法》等法律中关于证据调取的条件和程序。为了保障将来《数据安全法》能够得到有效贯彻和落

〔33〕 参见谢登科:《论电子数据收集中的权利保障》,《兰州学刊》2020年第12期,第33-45页。

实,应当对《刑事诉讼法》中侦查机关电子数据调取权的条件和程序予以细化。对于作为强制性侦查的电子数据调取,应当遵循法律保留主义、比例原则和令状主义的限制。在适用目的上只能为了查明犯罪事实、收集证据材料而使用,在适用程序上应当取得县级以上侦查机关负责人审批。

对于作为强制性侦查的电子数据调取,其程序控制的具体路径主要有两种:一是将其纳入现有特定类型的强制性侦查措施之中。比如将电子邮件等通信类电子数据的调取纳入"邮件检查"程序之中;将微信转账记录等财产类电子数据的调取纳入"财产查询"程序之中。此种方式的优势在于仅需对现有法律进行立法解释或者司法解释,而无需对现有法律进行修改或者变动,可以保持现有立法的连续性和稳定性。但其弊端在于可能无法将作为强制性侦查的某些新型电子数据调取纳入其中。二是对作为强制性侦查的电子数据调取予以专门规定。《数据安全法(草案)》第 32 条之表述显然就采取了此种路径,这样的表述很容易混淆广义概括性授权条款与狭义概括性授权条款的关系,而存在将任意性侦查的电子数据调取纳入其中的弊端。

在构建电子数据调取制度时,可以考虑在对电子数据类型化区分的基础上综合使用上述两种路径,将第二条路径的适用范围限定于强制性侦查措施所无法涵盖的新型电子数据调取。对于作为任意性侦查的电子数据调取,可以遵循狭义概括性授权条款的调整,而无需遵循令状主义的特别授权。当然,出于侦查机关内部管理的需要,对作为任意性侦查的电子数据调取,也需要取得办案人所在部门负责人的审批。从保障电子数据完整性和真实性角度来看,还需要在调取程序中设置笔录制度、见证人制度、同步录像制度等电子数据鉴真制度。

除了遵循传统刑事诉讼制度外,还应当设置适应电子数据自身特征的程序措施,具体来说,需要从以下方面对侦查机关电子数据调取权予以程序控制。

其一,明确第三方主体数据调取配合义务的法定条件。在立法上赋予网络服务商等第三方主体数据披露义务,此种设置在本质上是对侦查机关侦查权的延伸与扩展,这就需要在权利保障与查明事实之间寻求平衡点。[34] 这种平衡既要求对侦查机关电子数据调取权的条件设置契合侦查比例原则,也要符合电子数据自身形态和特征所衍生的权利保障要求。比如电子数据调取原则上应优先适用"单独调取"模式,尽量避免对其原始存储介质所有权和第三方主体正常经营活动的侵害,仅在确有必要的情况下,才可以采取"一体调取"模式。

其二,建立侦查机关对调取电子数据的筛查机制。电子数据具有无形性与虚拟性的特征,一块很小的 U 盘或者硬盘就可以存储海量电子数据。信息技术的摩尔定律,每年也引发了数据运算能力和数据存储能力的翻倍增长,这也可能导致"摩尔不法定律",即数据性权利侵犯或者干预的程度翻倍。[35] 在电子数据调取中,网络营运商等第三方主体

〔34〕 参见裴炜:《犯罪侦查中网络服务提供商的信息披露义务——以比例原则为指导》,《比较法研究》2016 年第 4 期,第 92 - 104 页。

〔35〕 参见[加]唐·塔普斯科特、亚力克斯·塔普斯科特著:《区块链革命:比特币底层技术如何改变货币、商业和世界》,凯尔、孙铭、周沁园译,中信出版社 2016 年版,第 4 页。

对案件事实及相关情况可能并不知悉,这也可能会导致第三方主体在调取数据中扩大范围,从而损害电子数据所承载的公民基本权利。为了防止此种情况的发生,就需要建立调取电子数据的筛查机制,侦查人员经筛查后发现与案件无关的电子数据,应当及时退还或者删除。

其三,设置侦查机关在电子数据调取中的告知义务。电子数据具有虚拟性和可复制性的特征,实际占有电子数据的控制主体与权利主体可能出现分离,此种分离现象在电子数据调取中普遍存在。由于网络营运商等第三方主体可能会对侦查机关违法调取电子数据的行为视而不见,也不会积极通过申诉、控告等方式寻求权利救济;电子数据所承载基本权利的权利主体,由于不知悉侦查机关违法调取电子数据的情况,也不可能寻求权利救济。为了避免发生此种情况,应当设置侦查机关在电子数据调取中的告知义务,从而保障基本权利主体有机会知悉电子数据调取情况,为其监督调取行为、寻求权利救济奠定制度基础。

[本文为作者主持的2020年度中国人权研究会部级一般课题“电子数据取证中的人权保障研究”(CSHRS2020-17YB)的研究成果。]

[**Abstract**] Article 32 of the (Draft) Chinese Data Security Law lays down rules on the subjects, purposes and approval procedure of electronic evidence taking at the legislative level for the first time in China. As such, it is of great significant to bringing electronic evidence taking under the rule of law in China. Under this article, electronic evidence taking must go through strict approval procedure. As far as its legal nature is concerned, electronic evidence taking is a compulsory investigation measure similar to technical investigation, which is in contradiction with existing judicial interpretations and departmental rules in China. Therefore, it's necessary to clarify the legal nature of electronic evidence taking and that of the legal rules on electronic evidence taking. As the "king of evidence" in judicial cases in the Internet and information age, electronic evidence is different from traditional physical evidence in both the form and the evidence taking mode, resulting in the triple paradox in traditional criminal procedure law and its application in electronic evidence taking. In constructing the electronic evidence taking system under the Data Security Law, China should not only consider the legal nature of electronic evidence taking and maintain its coherence with the existing criminal procedure law and evidence law, but also lay down procedural protection measures adapted to the characteristics of electronic evidence itse lf.

(责任编辑:王雪梅)