



跨境电子证据取证制度研究^{*}

李 上

中南财经政法大学刑事司法学院，武汉

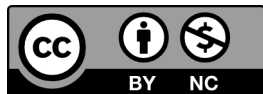
摘 要 | 随着全球化的到来以及计算机网络技术的快速发展，人与人之间的交流日益密切。与此同时，犯罪也在顺应时代要求，逐渐走出国门呈现出一种国际化、网络化的趋势。相应地，网络犯罪对公安工作提出了不小的挑战。在网络犯罪侦查中，电子数据取证处于核心地位。目前我国在跨境电子证据取证领域主要采取刑事司法协助和利用信息技术单边取证两种途径，但在实际运用过程中，两种措施均会带来一定的弊端。本文分别对我国和国外跨境电子证据取证制度进行分析，找出这些制度中尚存的一些问题，并以此为基础，对完善我国跨境电子证据取证制度提出建议。

关键词 | 电子证据；跨境电子证据取证；长臂管辖；区块链

Copyright © 2023 by author (s) and SciScan Publishing Limited

This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

<https://creativecommons.org/licenses/by-nc/4.0/>



一、引言

网络犯罪不同于传统刑事犯罪，其凭借广域性、低成本性、隐匿性等特征迅速发展、不断蔓延，不仅使得广大市民深受其害，而且也对侦查防控工作提出挑战。根据最高人民检察院统计数据显示，2021 年，起诉利用网络实施诈骗、赌博、传播淫秽物品等犯罪 28.2 万人，同比上升 98.5%。起诉非法买卖电话卡和银行卡、帮助提款转账等犯罪 12.9 万人，是 2020 年的 9.5 倍。相比于传统

犯罪，网络犯罪比例仍不断上涨，犯罪网络化趋势逐步形成。同时，在高犯罪率的背后，破案率却常年维持在一个较低的水平。以中部某省为例，其网络犯罪的破案率不足 10%。^[1]同样的，在跨境网络犯罪中，此等情形同样存在，并且由于国与国之间在制度、文化等方面的差异而表现的更加极端。笔者以为，针对上述情形，作为跨境网络犯罪中的重要组成部分，电子证据理应受到足够的关注。目前我国在跨境电子证据取证领域主

^{*}项目基金：中南财经政法大学中央高校基本科研业务费专项资金资助“跨境电信网络诈骗警务协作机制研究”（202310718）。

[1] 最高人民法院工作报告 [EB/OL]. (2021-03-15) [2021-11-09]. https://www.spp.gov.cn/zd gz/ 202103/t20210315_512716.shtml.

要采取刑事司法协助和利用信息技术单边取证两种途径,后者又包括了网络在线提取、网络远程勘验、网络技术侦查三种方法。然而,这两种途径往往会面临取证效率低、难度大、数字主权易受侵害等一系列弊端。因此,如何从制度以及技术层面改进现有跨境电子证据取证制度使其适应新时代发展要求便成了当下亟需解决的问题。

二、我国跨境电子证据取证制度——初步探究

目前,我国没有关于跨境电子证据取证的专门立法。我国仅限于借助对刑事司法协助以及网络在线提取、网络远程勘验、技术侦查等技术手段的规定来进行跨境电子证据取证的法律规制。具体来说,可以从以下几个方面加以分析。

从制度层面来看,目前,我国跨境电子证据取证主要还是沿传统的刑事司法协助或者跨境警务协作来进行。刑事司法协助是指一国司法机关根据另一国司法机关的请求,代为或协助实行与刑事诉讼有关的司法行为。^[1]具体流程如下:某国中央机关必须向他国中央发送司法协助请求,他国相关机关对该请求进行审查,若满足一定的条件(如满足双边或多边条约等),便根据国内法进行取证,最终将取得的数据转交给请求国的司法机关。我国曾在2018年的《中华人民共和国国际刑事司法协助法》中对此做出详细的规定。^[2]就跨境警务协作来说,往往需要报上一级公安机关批准,由上级机关负责联络国际刑警组织中国国家中心局(下称中国国家中心局),再

由中国国家中心局联络国际刑警组织某国国家中心局,最终完成相应的联络任务。在双方友好沟通的前提下,我国可以赴他国协助他国司法机关工作人员进行相应的追捕工作。另外,在我国侦查人员需要赴他国进行警务协助时,往往需要联络我国驻该国大使馆,向其询问当地的习俗、文化等,以便更好地开展相应的工作。

另外,随着《中华人民共和国网络安全法》的出台,数字主权的概念被提升到了前所未有的高度。例如,《中华人民共和国网络安全法》第37条规定:因业务需要确需向境外提供的,应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估;法律、行政法规另有规定的,依照其规定。该条正是体现了我国对于数字主权的重视。数字主权不同于传统的领土、领空,其对于跨境电子证据取证有着举足轻重的地位。随着贸易全球化的不断推进,全球范围内出现了一大批跨国网络巨头,其世界多个地区均部署了自己的数据中心机房以便为自己的客户提供更好的服务。在这种模式下,一个跨国公司往往掌握着海量不同国籍用户的数据,当外国司法当局想要从他国ISP或者ICP手中提取相应的电子数据时就不可避免地会涉及到该国的数据主权。

从技术层面来看,我国目前主要利用诸如网络在线提取、网络远程勘验等计算机单边取证手段。但是,我国在2005年和2014年所颁布的两部规定均是对网络远程勘验本身的规定^[3],并不涉及相关的跨境适用方面的规定。无独有偶,我国在2016年颁布的规定中虽然加入了境外元素,但同样没有

[1] 刘仁文,崔家国.论跨国犯罪的联合侦查[J].江西警察学院学报,2012,154(1):5-12.

[2] 2018《中华人民共和国国际刑事司法协助法》第9条中规定:“办案机关需要向外国请求刑事司法协助的,应当制作刑事司法协助请求书并附相关材料,经所属主管机关审核同意后,由对外联系机关及时向外国提出请求。”

[3] 2005年《计算机犯罪现场勘验与电子证据检查规则》第3条:远程勘验,是指通过网络对远程目标系统实施勘验,以提取、固定远程目标系统的状态和存留的电子数据。第23条:应当采用录像、照相、截获计算机屏幕内容等方式记录远程勘验过程中提取、生成电子证据等关键步骤。2014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》第16条:远程提取电子数据的,应当说明原因,有条件的,应当对相关活动进行录像。

做出实质性的区分^[1]（2019年亦是如此^[2]）。应当说，在我国目前没有跨境电子证据取证专门立法的前提下，利用境内的远程勘验手段进行跨境取证的现象仍然盛行。除此之外，我国还利用一些技术侦查措施进行跨境电子证据取证，例如利用嗅探技术或者抓取技术等。目前，我国对于技术侦查的门槛设置不高，这也导致了侦查实务中此种做法有被滥用的倾向。

三、我国跨境电子证据取证制度——困境犹在

不可否认，我国目前正在加大有关跨境电子证据取证相关规制的力度，这表明我国对该领域的重视。但是，我国电子证据立法相对较晚，相关规定整体呈现出较为分散的状态，处于初步探索阶段，在许多方面仍存在一定的立法空白，这也造成了我国侦查人员在办理具体案件时的效率与效益往往都不尽如人意。目前，在我国不断推进关于跨境电子证据取证立法的大背景下，相关内容然存在欠缺，主要存在以下几点问题。

（一）法律适用较为单一

这种现象导致取证手段多元化发展不足，仅局限于立法中规定的几种取证措施。电子证据取证不同于传统证据的取证，其具有及时性、完整性等特点。这要求我们不断研究，制定更多、能够与时俱进的新型取证制度，以达到与网络犯罪自身快速发展的一种均衡，即“你在我术中，我在你术外”的目的（当然这里不仅指技术上的包含关系，也指法律的相应完善）。

（二）取证措施规制不足

受制于当前的立法空白，再加上侦查权本身就具有强制性，天然具有一定的侵权倾向，使得在跨境电子证据取证过程中侦查人员具有较大的自由裁量权，相关措施不能得到及时的规制。虽然我国目前对技术侦查措施规定了严格的审查制度，但这种体制内的自我审查注定其效果不会太过显著。

（三）重实体、轻程序的思想尚未转变

这种传统思想导致了对犯罪嫌疑人以及善意第三人的人权保障不到位。例如，在取证过程中对隐私权的侵犯较为普遍。在学术界，有学者将电子证据取证分为两类，即单机电子数据取证和网络电子

数据取证。其中，单机是指能够独立运行或存在的单独计算机设备或电子数据存储介质。基于上述分类，笔者认为，跨境电子证据取证主要涉及网络电子证据取证的问题。网络取证不同于单机取证之处在于，其涉及网络中的多个节点，如路由节点、服务器节点、交换机节点等。计算机网络取证相较于单机取证，往往会接触到大量的数据信息。例如，目前一些ISP或ICP^[3]。特别是其中的一些跨国公司，其往往会在全球建立数据中心机房，这些服务器中通常记载着大量用户的私密信息。在侦查取证过程中，侦查人员难以区分涉案数据和非涉案数据，通常的做法是将整体数据进行复制以备检验，这一行为往往会使大量私密信息受到侵犯。

（四）传统刑事司法协助制度陷入困境

传统的刑事司法协助制度是一种类似“U”字型的构造，这种独特的结构，在应对传统犯罪方面具有一定优势。特别是在技术发展初期，这种模式能够有效的打击跨境犯罪，提高侦查效率。但随着网络时代的到来，这种传统的跨境取证方式正在面临巨大挑战。一方面，鉴于电子证据具有脆弱性，电子证据取证具有及时性等特点，传统的刑事司法协助制度的缺陷被无限放大，这种具有冗杂程序的取证模式显然无法满足电子证据取证的需要。过长

[1] 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》第9条第2款：“对于原始存储介质位于境外或者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。”第9条第3款：“为进一步查明有关情况，必要时，可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验，需要采取技术侦查措施的，应当依法经过严格的批准手续。”第29条：“网络远程勘验，是指通过网络对远程计算机信息系统实施勘验，发现、提取与犯罪有关的电子数据，记录计算机信息系统状态，判断案件性质，分析犯罪过程，确定侦查方向和范围，为侦查破案、刑事诉讼提供线索和证据的侦查活动。”

[2] 2019年《公安机关办理刑事案件电子数据取证规则》第23条：“对公开发表的电子数据、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。”第27条：“关于网络在线提取与网络远程勘验转化。”第34条：“关于网络远程勘验时应同步录像的案件的规定等。”

[3] ISP是指网络服务提供商，如中国移动、中国联通等，ICP是指网络内容服务商，如谷歌等。

的取证时间往往会导致一些及时性的电子证据无法获得,或给犯罪嫌疑人销毁、隐藏证据提供充足时间,并容易造成侦查机关在认定犯罪事实时陷入被动局面。另一方面,传统的刑事司法协助属于国与国之间的执法沟通机制,通常情况下,各个国家会在共同打击犯罪的旗帜下通力合作,以践行国际人道主义。但是,当被请求协助的国家本身并未受到犯罪的侵害时,这些国家真的会倾尽全力协助他国打击犯罪、实现人道主义至高目标吗?笔者认为,答案应是否定的。在国家利益面前,正义的天平总是会倾斜的,此种观点虽然不能说是绝对的,但应该说还是具有十足的代表性的。

(五) 公私协作机制构建不足

2018年3月17日,脸书(Facebook)的用户数据遭到了大范围泄露。据相关报道,大约27万名脸书用户使用了一款名为“这是你的数字化生活”(This Is Your Digital Life)的软件,该软件共收集了大约5000万人的数据,随后被卖给科技公司。上述脸书事件向我们展示了一个大型互联网巨头往往拥有海量用户数据的现实。回归到证据层面,侦查机关要想在跨境电子证据取证时提高效率,与一些互联网公司合作不失为一种良好选择。侦查机关受限于地理空间以及他国主权,往往不能收集到相应的主要电子证据。但在这种机制下,不仅能够弥补侦查机关自身技术能力的不足,使得电子证据的提取措施更加有力,而且在网络服务商的配合下,相关电子证据能够得到快速的保全以克服电子证据及时性、脆弱性等特性所带来的弊端。

目前,国际社会普遍规定了互联网服务提供商的信息披露义务,并将其视为侦查手段的延伸。我国在此方面起步较晚,目前《网络安全法》以及其他相关法律均作出回应,包括披露范围、披露原则等。

针对上述情况,笔者认为,可以在一定程度上借鉴外国的相关立法或国际条约,以推动我国立法的完善。

四、国外跨境电子证据取证制度——“他山之石,可以攻玉”

随着网络技术的迅速发展,数据流转已成为常态。数据的跨境输入与输出成为当今各国必须面对

的问题。这些数据一方面能够成为一国的宝贵财富,其中所蕴含的信息价值不可估量。例如,随着大数据技术的快速发展,这些信息往往在“大数据+”的模式下将转化为财富的源泉,推动企业的良好发展。另一方面,其也会带来大量的安全风险。海量流转数据是一国数据主权的组成部分,其甚至关系到一国的国家安全和社会问题。基于此,近年来,国际社会对跨境电子证据取证进行了积极的探索。以下将从欧盟以及美国的相关制度入手,以期能够获得一些有益的启发。

(一) 欧盟相关制度分析

实际上,自从欧洲理事会于2001年推出《布达佩斯公约》以来,欧盟一直致力于解决跨境电子证据取证所带来的挑战。近些年,欧盟提出了大量的应对方法,受篇幅所限不能一一列举。笔者拟从以下几个方面入手,浅析欧盟在跨境电子证据取证中的相关制度。

1. 欧盟调查令

在欧盟调查令提出之前,欧盟曾于2003年以及2008年分别通过了《关于冻结令的框架决定》以及《为获得刑事司法中使用的物品、文件和数据在欧洲证据授权状的框架决定》。在这一时期,欧盟各国之间进行跨境电子证据取证往往需要签发冻结令或者证据授权状。但是,上述两种方法实质上仍应隶属于传统刑事司法协助的框架下,这使得无论是冻结令还是证据授权状都无法克服传统司法协助所带来的弊端——协作效率低下、取证过程冗长。随着网络犯罪的不断发展,司法人员运用上述方法打击犯罪时,逐渐显得有些力不从心。

为了尽快摆脱上述困境,欧盟在2014年4月3日通过了《关于刑事案件中欧洲调查令的指令》(以下称《指令》)^[1]。随着《指令》的运行,调查令也逐渐取代了以往的冻结令和证据授权状成为欧盟跨境电子证据取证中较为主流的做法。调查令实质上是指,欧盟一个成员国的执法机关为获取证据,根据《指令》签发或确认效力的、包含由另一成员国执行的一项或多项具体调查措施的一种司法决定。调查令相较于证据授权状等措施拥有更为

[1] 刘品新. 跨境电子取证的欧盟方案及启示[J]. 国家检察官学院学报, 2022, 30(5): 3-23.

广泛的适用空间。应当说,调查令在一定程度上缓解了跨境取证时所面临的冗杂程序的问题。但是,究其本质,调查令仍处于刑事司法协助的范畴之内。其签发主体以及适用对象决定了其只是司法协助内部的制度改良。面对互联网世界不断变化的复杂形势,理应寻求跨境电子证据取证的新路径。

2. 欧盟电子提交保存令

在欧洲调查令推出后,跨境电子证据取证的困境的确得到了一些改善。但是随着时间的推移,新的困境逐渐展现在欧洲各国面前。其一,欧洲调查令无法突破传统司法协助机制的固有局限性。其二,网络犯罪侦查中公私合作问题日益突出。传统刑事司法协助中的执法机关—执法机关模式难以满足当前侦查实务的需要。在此背景下,欧盟提出了电子提交保护令制度,以期能够解决上述困境。所谓欧洲提交保存令是欧盟拟推出的一种证据制度,其打破了传统的执法机关—执法机关的协助模式,构建出执法机关—网络服务提供者的新型取证模式,极大地提高了跨境电子证据取证的效率,缩减了相应的司法反馈周期。^[1]该制度最大的特征就在于,在一国与网络服务提供者具有一定“实质联系”^[2]的情形下,可以简化以往的取证流程,直接对接相应的网络服务提供者且不受属地原则的限制。这极大地改善了原有的制度缺陷。可以预想到,在欧盟《刑事电子证据条例(草案)》正式通过后,欧洲提交保护令必定会为跨境电子证据取证带来新的活力。

3. 《布达佩斯网络犯罪公约》

虽然《网络犯罪公约》(以下简称《公约》)距今已经过去很多年,但是仍对世界范围内打击网络犯罪发挥着举足轻重的作用。在颁布之初,其重心是位于“实体法意义”的范畴内。这一时期,《公约》虽也规定了一些程序性规制,但总体来说,还是一部对网络犯罪入罪的规制法。过于追求实体法上的入罪问题也使得《公约》难以应对新时代的网络犯罪发展。在此之后,《公约》曾增加过两次附加议定书。其中,《〈布达佩斯公约〉第二议定书》不同于第一议定书^[3],更多地关注跨境电子证据取证等程序性问题。例如,在A6中设立了调取域名注册信息的相关规定,在A7中设立了要求披露注册人信息的相关规定,在A9中设立了紧急情况下存储计算机数据的便捷提供的相关规定,在A10

中设立了紧急情况下的协助方面的规定等。可以说,在此方面,《公约》的“进化史”也为全世界各个国家相关领域的发展指明了方向。

(二) 美国相关制度分析

近年来,美国的跨境电子证据取证得到了长足的发展。其中具有代表性的当属长臂管辖原则。所谓长臂管辖原则最早产生于美国,其诞生之初被应用于民事诉讼方面。其是指,当被告人的住所不在法院地州,但和该州有某种最低联系,而且所提权利要求的产生已和这种联系有关时,就该项权利要求而言,该州对于该被告人具有属人管辖权,可以在州外对被告人发出传票。^[4]目前,该原则已经发展到了域外适用领域。笔者认为,长臂管辖原则的长足发展与美国的世界霸主地位不无关系。

微软诉美国案在此问题上具有较强的说明价值。2013年12月4日,美国纽约南区联邦地区法院治安法官根据《存储通信法》签署了一封搜查令,其要求微软公司提供一部分客户的电子信息。但该问题的特殊之处在于,这些用户的电子信息有一部分并非存储在美国本土,而是存储在位于爱尔兰首都都柏林的数据中心服务器中。作为回应,微软仅提供了位于美国本土的那部分用户数据。该案经过重重上诉,最终上诉法院推翻了之前拒绝执行搜查令的判决。可以说该案表明了美国一定时期的域外执法态度。^[5]

然而,在2017年6月23日,美国司法部向联

[1] 欧洲提交令、欧洲保存令通常被简写为EPOC、EPOC-PR。

[2] 所谓实质联系是指,其提供的服务能否让欧盟中至少一个成员国的自然人、法人接受。如果某一网络服务提供者在至少一个成员国中建立了分支机构,这一事实就构成了“实质联系”。在不能进行简单判断的情况下,还可以基于“其大量用户存在于一个或多个成员国中,或其活动目的系针对一个或多个成员国。”

[3] 《〈布达佩斯网络犯罪公约〉第一议定书》其主要关注与儿童色情方面。

[4] 余涛. 美国司法长臂管辖权的演进逻辑[J]. 国际经济法论, 2022(3): 75-89.

[5] 叶开儒. 数据跨境流动规制中的“长臂管辖”——对欧盟GDPR的原旨主义考察[J]. 法学评论, 2020, 38(1): 106-117.

邦最高法院提交了关于调卷令的诉请,其旨在夺回过去失去的域外数据获取权力。随后在2018年3月,美国国会紧急通过《澄清境外数据合法使用法》(或称“云法”),该法被认为是对此前《存储通信法》的改善,其中直接规定了在美国的网络服务提供者有义务依法保存和披露其在全球范围内的数据。^[1]虽然该法属于美国本土的国内法,但美国试图通过该法扩展到与其他国家的双边协议,进而赋权执法机关能够直接对接相应的网络服务商,提高取证效率。^[2]实质上,美国的执法机关就拥有了“域外执法权”。相应的其所依赖的取证模式也从之前的“数据存储地”模式转变为了“数据控制者”模式。不同于法国等欧洲国家^[3],可以说美国在此方面走在了世界的前列。

五、对我国跨境电子数据取证机制新路径的探索——一起向未来

从宏观层面上来说,我国跨境电子证据取证制度新路径的探索可以分为两个阶段,即过渡阶段和发展阶段。

(一) 过渡阶段

在过渡时期,如果采用大刀阔斧的改革思路,例如对现行制度进行全盘否定并完全以新制度予以取代,从经济学角度来说,所获得的收益往往远低于所付出的成本。当然,这里的成本不仅包括经济成本,还包括诸如社会成本、外交成本等等。因此,笔者认为在这一时期,应当以现有制度为基础,循序渐进地进行相应制度的改革。其中,IPv4到

IPv6的过渡具有相当的启发作用。^[4]针对现行制度,笔者以为应当从以下几个方面入手加以完善。

首先,应当构建数据保护制度。在传统的国际司法协助中,请求国和被请求国完成协助程序往往需要较长的时间。笔者认为,我国应在相关法律中规定国家间的数据保护制度,以期能够避免在协商时间内关键犯罪数据的丢失。这一制度的确立能够在一定程度上缓解传统刑事司法协助的冗长程序所带来的弊端。

其次,应当加大国内关于跨境电子证据的专门立法力度。一方面,应当完善网络在线提取以及网络远程勘验的相关规定,使其能够与境内的取证手段相区别,体现出应有的“跨境化”特征。另一方面,应当提高技术侦查措施的准入门槛。目前,国际社会上关于技术侦查的准入门槛均高于我国。美日两国启动侦查措施的最低标准是必须满足一定的证据门槛或者说是达到“足以怀疑”的地步。此外,还有一些国家要求侦查机关在应有技术侦查措施前要经过法官的司法审查,以达到限制侦查机关公权力以及保障一般民众个人权利的目的。

根据我国《刑事诉讼法》第150条^[5],可以看出我国目前的技术侦查措施的启动条件仅仅满足“在立案后”的时间条件以及“根据侦查犯罪的需要”的事件条件即可。这种门槛过低必将导致使用的混乱,而技术侦查又往往与个人隐私相关。此外,我国技术侦查措施本质上是没有时间限制的。针对上述问题,笔者认为,有必要适度提高我国现有的技术侦查措施的准入门槛,严格遵循比例原则,在

[1] 刘品新. 跨境电子取证的欧盟方案及启示[J]. 国家检察官学院学报, 2022, 30(5): 3-23.

[2] 该法的特色在于美国通过开放他国向本国公司取证的权力来换取本国执法机关在他国的执法权;目前美国已于2019年与英国签署协议,2021年与澳大利亚签署协议。另外,美国与欧盟的协议也正在研讨之中。

[3] 2003年法国公民希瑞尔案中凡尔赛上诉法院维持了对希瑞尔的有罪判决,该案表明了法国的相关立场:法国担忧跨境属性所隐含的域外执法过度“越界”为保护本国司法,法国采取了相对保守的策略。

[4] 目前随着互联网的发展,起初划分的IPv4地址面临着“资源短缺”的尴尬问题。为了满足互联网发展的需要,目前国际上提出了IPv6的概念,旨在扩充所需的IP地址的数量。其所选择的方案并非是直接“全覆盖式”部署IPv6,先借助IPv4的载核部分运输IPv6,在逐步完成“孤岛”扩大化。

[5] 《中华人民共和国刑事诉讼法》第150条:公安机关在立案后,对于危害国家安全犯罪、恐怖活动犯罪、黑社会性质的组织犯罪、重大毒品犯罪或者其他严重危害社会的犯罪案件,根据侦查犯罪的需要,经过严格的批准手续,可以采取技术侦查措施。人民检察院在立案后,对于利用职权实施的严重侵犯公民人身权利的重大犯罪案件,根据侦查犯罪的需要,经过严格的批准手续,可以采取技术侦查措施,按照规定交有关机关执行。

立法中规定适当的程序以加强事前审查、事后监督的力度,进而起到一定的限制作用。

最后,应当树立“共治”的思想,电子证据的取证通常会涉及一些技术手段,在跨境电子证据取证中,我国侦查机关通常会采取远程勘验提取等技术手段。在此过程中往往会产生一些有关个人隐私保护以及数据主权的问题。当合法的行为也会导致对公民个人权利的侵害时,我们就应当反思问题到底出在何处。

笔者认为,在当今我们这种多元异质的社会治理当中,有许多主体在发挥作用。上述问题的根本原因之一就在于没有处理好多元治理主体——法律与科技之间的关系。目前我国所采取的做法是单向赋权,即通过法律制定一些授权性的规则来开展技术工作。在这种情景下,权力必然会无限扩张且不受控制,科技侵权也时常发生。笔者认为,针对上述问题,我们应当改变单项赋权的模式,采取二元互动的模式取而代之。通过法律制度规则限制科技,同样的科技通过自己的技术规则以及技术效果(这里是指科技在运用过程的所产生的效果有好的效果也有不好的效果)来向法律反馈,法律再通过这些反馈来不断完善自己的条文,从而达到一定的限制权力扩张以及使得权力有序发展的目的。

(二) 发展阶段

发展阶段不同于过渡阶段。过渡阶段主要是针对我国国内的一些现有制度的完善与创新;而发展阶段则是在过渡阶段的基础上,将视野扩大至国际社会,以便共同应对跨境网络犯罪所带来的危害。

1. 国际条约与双边、多边条约之探索

2021年《北京宣言》第七点提出,要支持各方深化司法执法领域合作,推动缔结双边引渡条约和司法协助条约。^[1]笔者认为,应当利用好“一带一路”这个已有的互联平台,并在此基础上树立“警务共享、数据互联”理念,以引导各国签订跨境电子证据取证的区域双边或多边条约。目前,我国已与世界上80多个国家签订了诸如引渡条约、司法协助条约等双边或者多边条约并且加入了以联合国公约为代表的多个国际条约。近些年来,我国跨境电信网络诈骗案件频发,多项数据表明东南亚国家

通常与其有着不可分割的联系。对此我国在2016年签署了《中国与东盟关于非传统安全问题领域合作联合宣言》以及《关于加强合作打击电信诈骗犯罪谅解备忘录》等双边或多边条约。这些条约旨在为我国与东南亚国家合力打击跨境电信网络诈骗案件开创法律通路。

在电子证据的发展史上,此种做法并非现今之首创。相比于各个国家奉行国内法的各自为战,在国际条约的大背景下,各个国家能够最大限度地达成一致。这种做法既是减少管辖冲突、认识冲突的需要,也是顺应当下网络犯罪发展趋势的需要。从性质上来看,国际条约属于一种“软法”。在跨境电子证据取证的范畴内,相比于国内法,这种“软法”具有其独特的优势。^[2]

首先,这种软法是在各个国家商讨的基础上颁布的,其制定主体是政府间或者非政府间组织而非某个国家的立法机关。这使得相关权力较为分散,容易使各个国家之间更快地达成共识。其次,这种软法不是真正意义上的“国际法律”,它并不要求每个国家都必须强制遵守,而只是提供了一种蓝图框架。各个国家具有较多的“自由裁量权”,能够在该框架内灵活选择,最高能够达到与本国法律较好的结合效果。例如,在国际社会中,由于每个国家的文化、制度存在或多或少的差异,这就导致了关于犯罪的入罪方面可能会有冲突,进而给跨境电子证据取证带来不必要的麻烦。例如,在我国法律中,明文禁止赌博行为,而在美国的拉斯维加斯,这种行为似乎并未违法。但是,在国际条约或者双边、多边条约的框架下,这种冲突能够被“软化”,相应地被化解到各国的法律中,最终实现在该框架下的实质上的共识。可以说,国际条约在化解国家间主权问题、取证冲突问题上有着举足轻重的地位。^[3]

[1] 中国法治国际论坛(2021)北京宣言[N]. 人民日报,2021-11-13(005).

[2] 赵海乐. RCEP争端解决机制对数据跨境流动问题的适用与中国因应[J]. 武大国际法评论,2021,5(6): 39-55.

[3] 赵龙跃,高红伟. 中国与全球数字贸易治理: 基于加入DEPA的机遇与挑战[J]. 太平洋报,2022,30(2): 13-25.

笔者认为,在我国跨境电子证据取证制度的完善中,应当在适合我国法律的前提下,尽可能全面吸收相应的国际条约,有选择地吸收双边或者多边区域条约,并充分发挥这种“软法”的优势作用,助推我国跨境电子证据取证制度的快速发展。

2. 打造数据共享新平台——构建跨境联盟链

一般来说,数据共享机制的良好与否决定着跨境电子证据取证措施实效效果的优劣。目前,国际社会正在积极打造跨境数据共享平台。网络犯罪具有弱地域化的特点,其在实施过程中可能在网络中的任何一个区域、任何一个节点留下相应的电子痕迹。一国侦查机关要想凭借一己之力获取全部的、其想要的电子数据几乎是天方夜谭。基于上述原因,应当说,打造跨境数据共享平台,集多国之力收集电子痕迹是可行的办法。

然而,这种模式往往会遇到一些困境。跨境数据共享平台不同于境内平台,其数据标准往往难以统一。不同国家之间对数据的处理能力不同,这会导致向平台输入数据时的标准有所不同。在这种情况下,通常还需要通过签订相关条约或者由一国帮助他国进行技术培训,以期最终达到统一数据标准的目的。但是,这一过程往往要消耗大量的时间。在网络世界日新月异的“新社会”中,以上问题显然值得我们关注。

基于上述问题,国际社会理应寻找打造跨境数据共享平台的新路径——构建联盟区块链。区块链是指由分布式计算机网络构成的去中心化的数据库,区块链本身也可以认为是一种共享平台。区块链具有分布式储存(点对点)、不可篡改(哈希难题、51%的算力)、可溯源(时间戳、父哈希)、可信任(共识机制、不可篡改)、安全(非对称密码)等特点。

目前来说,区块链有几种形态,分别为公链、私链、联盟链。三种形态各有其不同的特点。具体来说,首先,公链的去中心化程度最高,可以称为完全的去中心化。在公链上,所有的peer节点都可以平等地加入到区块链当中,享有相同的权限。区块链上的信息完全公开,所有节点都可以自由查阅相关信息,具有较高的透明度。其次,私链是仅面向特定对象的区块链,具有一定的中心化属性。但是,私链的优点在于其具有较低的花费与较高的效率。最后,联盟链是指若干机构形成联盟共同控制

共识机制的区块链。其去中心介于上述二者之间。其共识机制有特定的节点商议得出。例如,超过一定数量的节点同意后“交易”才能被确认。^[1]

针对跨境犯罪中信息共享难、侦查取证难的问题,笔者认为运用跨区域的联盟区块链可以有效应对其中在传统模式下难以解决的问题。例如,在传统模式下,跨境取证往往会面临多个部门的审批以及国家之间的沟通和交流。但是这个过程通常情况下非常冗杂。特别是对于一些时效性较强的证据来说,这种模式下往往会导致证据证明力的下降甚至丧失。有些学者曾提出建立“一”字化模式,即通过签订协议继而使得侦查机关可以直接对接他国的证据提供机构,或者自己开展跨国的证据获取。但是因为国家间取证通常会涉及一个国家的主权问题,所以往往困难重重。例如,在跨国电子证据收集时,对于侵犯个人隐私的证据的收集是否侵犯了他国的数据主权,目前还有较大的争议。

跨国或者跨区域的联盟区块链可以使得各个国家可以作为一个节点而上链,在运行过程中,各个国家的侦查机关不仅可以访问区块链上的信息以获取对自己有利的国外犯罪信息,而且在跨区域侦查协作中,将整个侦查过程以及收集的相关证据打包广播,通过权限节点的确认最终被纳入联盟区块链中。这样可以使得相关国家能够清晰地查看侦查协作中或者说是他国侦查机关在本国收集的证据是否侵犯自己的相关主权。

笔者认为,通过构建跨境联盟区块链的方法不仅可以削弱主权国家对于他国侦查机关在本国侦查是否“越界”的顾虑,同时也为他国侦查机关构建了直接沟通的机会,构建出了一种类似于“一”字型的高效侦查方式。并且也解决了数据共享的问题,对于多国联合打击跨国犯罪集团提供了便利。在跨国协助请求中,信任通常是制约协作能否顺利进行的关键所在。而区块链技术正是以其共识机制、算法保障、安全性、防伪性等特性,在不同节点之间建立起来一种信任体制。

(责任编辑:李娜)

[1] 刘品新.论区块链存证的制度价值[J].档案学通讯,2020(1):21-30.

Research on Cross-border Electronic Evidence Collection System

Li Shang

School of Criminal Justice, Zhongnan University of Economics and Law, Wuhan

Abstract: With the advent of globalization and the rapid development of computer network technology, the communication between people is getting closer and closer. At the same time, crime is also adapting to the requirements of the times, gradually going abroad to show an international and networked trend, and correspondingly cyber crime poses a lot of challenges to public security work. In cybercrime investigation, electronic data forensics plays a central role. At present, China mainly adopts two ways of criminal justice assistance and unilateral evidence collection using information technology in the field of cross-border electronic evidence collection, but in the actual application process, both measures will bring certain drawbacks. This paper analyzes the cross-border electronic evidence collection systems in China and abroad, identifies some remaining problems in these systems, and makes suggestions on improving China's cross-border electronic evidence collection system on this basis.

Key words: Electronic evidence; Cross-border electronic evidence collection; Long-arm jurisdiction; Blockchain