

跨境电子取证的欧盟方案及启示

刘品新

【摘要】欧盟治理网络犯罪离不开构建高效的跨境电子取证机制,但遭遇传统司法协助机制不彰、网络服务提供者参与缺位、美国推行直接调取域外电子证据新规的三重挑战。在新的历史时期,欧盟积极寻求制度变革,推出了由不同成员国执法机关承认和执行的欧洲调查令,并推动构建面向网络服务提供者的欧洲提交保存令。它们是追求实现不同国家间良好分享电子证据的分层级工具,后者适应网络空间无国境性的办案需要因而更具创新的影响力。以此为契机,欧盟还同美国启动了兼顾双方法律要求的跨境电子取证机制。就共性而言,欧美的做法均在拓展“非中介获取模式”,亦即由根据数据存储地确定管辖的属地原则向依靠数据控制者的属人主义转型。我国应当密切关注由此引发的效应,提炼符合国际共识和中国智慧的经验,完善跨境电子取证规则。

【关键词】电子证据;欧洲调查令;欧洲提交保存令;网络犯罪;属人主义

【作者简介】刘品新,中国人民大学法学院教授,中国人民大学刑事法律科学研究中心、未来法治研究院研究员。

【原文出处】《国家检察官学院学报》(京),2022.5.3~23

【基金项目】本文为2020年中央高校建设世界一流大学(学科)和特色发展引导专项资金支持项目“科技革命与未来法治跨学科研究平台”的研究成果。

一、问题的提出

惩治网络犯罪是网络时代社会治理的艰巨任务。欧洲理事会于2001年推出全球第一部治理网络犯罪的国际公约——《布达佩斯网络犯罪公约》(以下简称《布达佩斯公约》^①)。其中,一项基础任务是构建高效的跨境电子取证机制。为明确各成员国执法机关收集有关网络犯罪中电子证据的权力和程序,该公约规定了敦促它们开展“最广泛”多边协助机制^②的内容,即“缔约国应当尽可能广泛地相互合作,以便侦查或审理与计算机系统和数据有关的刑事犯罪,或收集刑事犯罪中的电子证据”。^③《布达佩斯公约》被誉为欧洲“最具影响力和进步性的电子证据法”,^④一度具有良好的全球引领性。事易时移,随着近二十年来人类社会数字化水平的递增提级,各国网络犯罪司法中

关于电子证据的需求不断扩增,执法机关向网络服务提供者调取跨境电子证据的需求与日俱增。^⑤相应地,《布达佩斯公约》所设定方式在解决跨境电子取证难题方面捉襟见肘。部分成员国不得不开始自我调整式的变革,主要包括在取证方面“诉诸网络服务提供者的自愿配合”“拓展源自属地原则”的传统路径。^⑥各种“地方性”探索带给网络服务提供者较大的压力。与此同时,美国于2018年修法推行带长臂管辖色彩的跨境电子取证新规则,亦对欧盟的成员国及网络服务提供者产生了即时且深远的影响。

当前各种外在变化加速网络犯罪治理变局,各国纷纷开展跨境电子取证的制度再建。本文以有关动态为研究对象,剖析欧盟网络犯罪治理领域的主要挑战、应对及欧美相关磋商,提炼欧盟关

于网络犯罪跨境电子取证的方案及其特征,并解析欧盟的制度转向对中国的可能影响及有益启示。

二、欧盟治理网络犯罪的主要法律挑战

欧盟开展跨境电子取证制度建设由来已久,可以追溯至《布达佩斯公约》问世前。2000年5月,欧盟出台《欧洲刑事司法协助公约》,向成员国提供了一种刑事司法协助框架思路。^⑦2003年,欧洲议会通过了《关于冻结令的框架决定》;^⑧2008年,欧洲议会通过了《为获得刑事司法中使用的物品、文件和数据的欧洲证据授权状的框架决定》。^⑨加上《布达佩斯公约》所设定多边协助机制的支撑,欧盟成员国就拥有了得到互认的多种取证工具。实践中的通常做法是,欧盟成员国实施跨境电子取证需要“签发冻结令或证据授权状等,辅以刑事司法协助委托书”。^⑩然而,欧盟跨境电子取证的传统做法在现阶段遭遇到三重挑战。

挑战之一,传统司法协助机制的效率过于低下,这同网络犯罪动辄跨境的规律形成鲜明反差。网络犯罪中需要快速获取跨境电子证据,但“司法协助流程冗长、且不可预测。警察不喜欢它,隐私捍卫者不喜欢它,普罗大众也不喜欢它。”^⑪这是任何看起来精美的刑事司法协助方案都难以满足时限要求的现实状况。此外,刑事司法协助方案往往要求满足“双重归罪”的前置条件,这也构成一种“先天性”不足。^⑫总体而言,司法协助流程在获取境外电子证据方面效率低下,^⑬致使各国通过司法协助打击网络犯罪渐入困境。

挑战之二,跨境电子取证日益依赖网络服务提供者的参与,而刑事司法协助机制并未提供对接该类主体的法定路径。当下形形色色的电子证据主要存储于超大容量的网络服务器中。而有广泛影响的网络服务提供者(通常就是数据控制者)基本上是在欧盟成员国之外注册的大企业,如微软、苹果、谷歌、脸书、亚马逊等公司。它们的母公司属于美国,但其海量数据或其一部分由欧洲的

子公司、分部负责管理,其数据中心服务器可能位于欧盟境内^⑭。这使得欧盟成员国间寻求刑事司法合作显得异常复杂,不仅法律手续很繁琐、耗时,^⑮执行起来更可能碰壁。诸如冻结令、证据授权状、刑事司法协助委托书等取证工具均以有关国家的执行机关为对接对象,不以网络服务提供者作为联系对象。这一缺陷在网络服务提供者普遍采取云技术提供数据服务的背景下更加凸显。云技术意味着所需要的具体数据不存在于单一服务器中,访问和传输数据也不是同单一服务器进行“对话”,造成了国际司法协助中基于属地原则确定被请求国、提出协助请求的做法变得不切实际。直接面向网络服务提供者、寻求其提供取证协助并扩大合作的空间,是当前无法回避的课题。

挑战之三,美国新近确立了从网络服务提供者直接调取域外电子证据的机制,对欧盟构成强势的法律冲击与制度竞争。2013年12月,美国纽约南区联邦地区法院的法官针对一起贩毒案签发搜查令,要求微软公司向联邦调查局提交一名嫌疑人的电子邮件。因有关邮件存储在该公司位于爱尔兰的服务器中,法官根据1986年美国《存储通信法》^⑯签发令状。微软公司以该法对国外数据中心的没有域外效力为由拒绝提交。此案一直打到联邦最高法院,控辩双方的争议焦点为国会立法究竟有没有赋予《存储通信法》适用于域外的效力。^⑰从理论上讲,问题的焦点在于对域外存储的电子证据进行取证究竟应该采取“数据存储地标准”还是“数据控制者标准”?2018年3月,美国国会紧急通过《澄清合法使用海外数据法》(简称《云法》),修改《存储通信法》,直接规定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。^⑱这为联邦最高法院解围。^⑲至此,美国从立法到司法层面形成了执法机关直接获取域外电子证据的机制。这一新规很可能被美国政府“滥用”以获得欧盟居民的数据,更给位于欧盟境内网络服务提供者套上了美国法的枷锁。

对此,欧盟必须予以回应,拿出对等的或可对接的制度方案。

在三重压力之下,欧盟不断调整跨境电子取证方式,进行相关制度变革。2014年4月,欧洲议会和欧洲理事会发布《关于刑事案件中欧洲调查令的指令》,规定任一成员国的签发机关可以通过特定的中央机构签发欧洲调查令的方式,与另一成员国的执行机关进行直接合作,并可以通过提供标准表格、严格时限和消除跨境合作障碍等方式予以促进。^①这虽未根本性地转换跨境电子取证的轨道,但可以理解为改造刑事司法协助机制的一次有益尝试。自2018年4月开始,欧盟的相关机构又协力推动“欧盟电子证据条例”出台,拟推出专门的欧洲提交保存令,赋予成员国执法机关直接面向网络服务提供者更快获取欧盟境内外电子证据的权力。^②尽管其最终的成案版本、具体的适用范围尚未确定,但其在国际上迅速产生了重大影响。这是欧盟积极改造刑事司法协助机制的又一次重大尝试。

三、欧盟改进跨境电子取证的制度创新

(一)欧洲调查令的推出

欧盟的实践表明,以冻结令、证据授权状为代表的法律工具组合过于复杂且实用性不强,甚至在奥地利、意大利、瑞典等国家未能得到执行。^③2009年,也就是在《欧洲证据授权状框架决定》实施一年后,欧盟理事会发布斯德哥尔摩计划,宣布寻求一种新的综合性方案解决此问题。^④部分成员国还明确建议另外颁行一种确认新取证工具的法令。经过多方的共同努力,2014年4月3日欧洲议会和欧洲理事会共同通过《欧洲调查令指令》(以下简称《指令》)。

《指令》在欧盟层面获得通过,被认为是刑事司法合作变革的里程碑事件。《指令》规定,自2017年5月22日起取代受约束成员国适用的下列公约条款:(1)1959年4月欧洲理事会通过的《欧洲刑事司法协助公约》及其两份附属议定书,以及依照第

26条缔结的双边协议;(2)《申根协定实施公约》;(3)欧盟成员国《刑事司法协助公约》及其议定书。^⑤此外,《指令》也完全取代了前述《欧洲证据授权状框架决定》《关于冻结令的框架决定》。^⑥截至2019年,欧盟多数成员国(除丹麦和爱尔兰外)均完成了国内法认可的手续。

《指令》不仅做出了一般性的规定,还单列了一些取证措施,诸如通过视频或电话会议进行听证、收集有关银行或其他金融账户或运营的信息、控制下交付、隐蔽侦查等。《指令》规定了两种情况下的电子证据专门规则:(1)请求识别持有特定电话号码或IP地址账户的个人;^⑦(2)请求电信拦截。^⑧《指令》未对后文提到的“提交令”作出前瞻性的规定,但显然也是清楚地囊括在内。可以说,欧洲调查令可以在采取任何取证措施的行动中签发。这是着眼于取证措施的令状,不同于着眼于具体证据的欧洲证据授权状。这将极大地改善网络犯罪案件的办理效果。那么,如何准确理解欧洲调查令呢?

简言之,它是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。^⑨前一成员国为签发国,后一成员国为执行国。展开来说,欧洲调查令的签发主体是成员国中适格的执法机关、人员。它具体由成员国法律确定,既可以限定为法官、侦查法官、检察官等主体,也可以做出开放式的规定,如明确为“有权力命令收集刑事证据的其他适格主体”。当然,无论作何种确定,都必须防止欧洲调查令的签发脱离司法控制、进而引发社会对警察权过度使用的担忧。^⑩

欧洲调查令可以用于获取执行国执法机关尚未掌握的证据,也可以用于获取其已经掌握的证据。在任一种情况下签发欧洲调查令,均需满足必要性和相称性标准。一种简单的判断方法是,该措施必须对签发国国内是适当的,即签发国在

处理国内案件时遇到类似情况下可以签发相关令状。^③执行国的执行机关未援引拒绝理由的,应当承认欧洲调查令并以同国内措施一样的方式实施。除非与其国内法的基本原则相抵触,执行国的执行机关实施时应当“遵守签发机构明确规定的手续和程序”。^④执行该措施原则上应当接受签发国的法律规制,以保证有关证据具有可采性。^⑤

总体来看,欧洲调查令仍然属于刑事司法协助的范围,是在不同成员国执法机关间实施的。它建立在成员国互认原则的基础上,每一个成员国都有义务承认和执行欧洲调查令。同时,它也相当于欧盟自身的域内取证,具有单独执法的性质。

相比传统司法协助工具,欧洲调查令在克服运行复杂性和提升办案效率方面进步明显。化繁为简方面的进步不仅体现为将许多工具聚合为一种,更体现在一些基本原则的适用性得到调整。如,依照《指令》的适用条款,欧洲调查令这一新工具就替代了冻结令、证据授权状等传统工具组合。又如,“双重归罪”原则不再作为签发欧洲调查令的一项条件,其仅可以由执行国执法机关用作拒绝的理由。^⑥另外,在效率提升方面的进步体现为欧洲调查令所设定的时限得到一定程度的压缩。执行国的执行机关应当按照国内相似措施的要求对待和执行欧洲调查令,并尽可能考虑签发国的要求。通常执行国签收后30天内作出确认或执行决定,并在做出决定后的90天内执行。^⑦但这些时限不是绝对的,确认或执行决定的做出期限可以延长30天;执行不能遵守前述时限的,执行国与签发国的执法机关经协商也可以再延长。^⑧此外,为了保障刑事调查或起诉进程中的利益,执行国也可以延迟对欧洲调查令的认可或执行期。^⑨诚然,《指令》在实施中也引发了一些争议,特别是关于互联网空间电子证据收集方面的问题。于是,欧盟在“JUST-2015-JCOO-AG”项目^⑩下发起了“LIVE_FOR”计划^⑪,有关举措提升

了《指令》在成员国中的认可度,推动其得到有力执行。^⑫

(二)欧洲提交保存令的推动

欧洲调查令虽有助于欧盟成员国开展跨境电子取证,但仍未摆脱司法协助机制的整体定性及缺陷。重大缺陷之一是,执行期限过长的顽疾虽有所缓解,但未得到根本改变,仍容易造成电子证据灭失或改变的风险。^⑬重大缺陷之二是,它亦未能解决执法的地域性问题。^⑭具体来说,《指令》虽然可以打破将执法权限与数据存储地联系起来的逻辑,但其条款并未明确做出这样的表述。对此,欧洲理事会要求欧盟委员会进行检讨以寻求解决之道。^⑮欧盟委员会检讨中的一个关键问题是,应否引入一项致力于允许网络服务提供者根据成员国执法当局要求提供数据的专门工具。该工具可以是任意性的,不用于强制网络服务提供者,以消除成员国立法上的壁垒;也可以是强制性的。^⑯支持引入专门工具的肯定观点占据上风。

随后欧盟的相关机构采取了一系列举措。2018年4月17日,欧盟委员会提出关于一项条例、一项指令的两份提案:(1)《关于制定欧洲刑事电子证据提交令与保存令条例的提案》^⑰,以“在欧盟建立一种共同框架制度,减轻成员国与其他成员国、非成员国因获取数据的执法手段差异而产生的法律上不确定性”。^⑱这也被简称为“电子证据包”(e-evidence package),其否定了将数据存储地作为管辖权依据。^⑲在新制度下,成员国执法机关被授权发布电子证据提交令、保存令,要求网络服务提供者收集或保存电子证据,无论数据存储在何处;^⑳有关指令将同时适用于包括用户数据、访问数据或交易数据在内的非内容数据和内容数据。^㉑(2)《关于制定要求委任法律代表的统一规则之指令的提案》^㉒,规定“在成员国提供服务的公司,即便其总部位于非欧盟的第三国,必须在欧盟建立法律代表处,以代表其接收和遵从电子取证的命令”,^㉓以实现“所有在欧盟提供同类服务的公

司,不论其在何处成立,均可享有公平的竞争环境。”^③欧盟委员会还同步提出了一份影响评估报告。^④

同年9月26日,欧洲数据保护委员会就有关提案发表意见,^⑤明确拟推出有关条例应当在欧盟中保持较高的数据保护水平,并注意与未来国际协议之间的相互影响。欧盟委员会工作组对两份提案进行了审查,形成了多份修订版本,将关于提案的妥协版本提交至欧盟司法与内务理事会进行讨论。^⑥2018年12月8日、2019年3月8日,欧洲理事会分别针对两份提案发布了“通则”版本,^⑦表明其基本立场。欧洲议会之后启动对有关提案的审议准备。2019年11月8日,报告人西佩尔议员发表了《关于电子证据条例草案的报告草稿》,^⑧提出了267条修改意见,并附有不同政治团体提出的修改建议。针对该报告的批评声很多,实为欧盟后续的立法拓宽了道路。2021年12月,欧洲议会和欧洲理事会在一份关于成员国之间信息交流指令的提案中,再次提到了“欧洲提交保存令”工作并强调持续推进。^⑨

截至目前,欧盟出现了欧盟委员会的初始提案和欧洲理事会的通则两个版本。鉴于该提案尚未成为正式法律,本文合称为前述的“欧盟电子证据条例”(后文进一步简称为“条例”)。对于两个版本有差异的部分内容,后文也将进行必要的补充说明。一旦“条例”获得通过,在欧盟范围内,一个成员国执法机关原则上可以在不与另一成员国执法机关接触的情况下,向另一成员国网络服务提供者发出一种特殊的“通知”。为实现这一愿景,“条例”的核心任务就是推出欧洲提交保存令。

所谓欧洲提交保存令(European Production and Preservation Orders,简称为EPO)是欧盟拟推出的、旨在允许一个成员国的执法部门直接向另一成员国的网络服务提供者签发的数据指令统称。它可以分解为欧洲提交令、欧洲保存令两种。^⑩欧洲提交令是由一个成员国的执法机关向

欧盟范围内提供服务的、在另一成员国设立分支机构或代表的网络服务提供者签发的一项具有约束力的决定,命令其提交电子证据;^⑪欧洲保存令是由一个成员国的执法机关向欧盟范围内提供服务的、在另一成员国设立分支机构或代表的网络服务提供者签发的一项具有约束力的决定,命令其保全电子证据以便事后进行提交。^⑫欧洲提交保存令看起来针对“数据”,实则指向获取各种电子证据。“条例”还对术语“电子证据”做了专门限定,即“在网络服务提供者收到指令时以电子形式存储的证据”,包括“注册信息、访问数据、交互数据、内容数据四种数据”。

“条例”按照电子证据的类型对欧洲提交保存令的签发主体做了区分。其一,成员国的法官、法院或侦查法官可以针对注册信息、访问数据、交互数据、内容数据等所有数据签发相关指令。其二,成员国的检察官签发相关指令的权限限于注册信息、访问数据两种。这是因为此两种数据被认为具有较低的侵扰性,不需要在采取措施前进行司法审查”^⑬。其三,除前述两种主体外,各成员国在刑事诉讼中根据本国法行使侦查权、收集证据的其他主管机关,在经过有权机构确认后,也可以签发相关指令。

根据“条例”,欧洲提交保存令的接受者是向欧盟范围内提供服务的、在另一成员国设立分支机构或代表的网络服务提供者。它们是提供电子通讯服务、信息社会服务、互联网域名和IP地址分配服务的自然人、法人或者其他组织。^⑭“条例”确定的网络服务提供者既包括建立在欧盟范围内的、也包括仅在欧盟内提供服务的主体。之所以如此界定,是基于欧盟秉持的基本理念——网络服务提供者在欧盟内获得商业服务利益,就应当在同一地域范围内对执法机关承担义务,同本地网络服务提供者面对同等的公平竞争环境,避免因执法机关区别对待而形成沟隙。^⑮当然,若其提供的网络服务仅仅在欧盟内可以访问获得,则不

足以被纳入管辖范围。关于特定的网络服务提供者是否属于欧洲提交保存令的对象,一个简单的判断标准是,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,进而确立其同有关成员国是否有“实质联系”。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”^④做出判断。

欧洲提交保存令的具体签发对象是网络服务提供者的法律代表。为此,网络服务提供者必须在欧盟的一个成员国中派驻有代表。根据“条例”,所有网络服务提供者需要明确注明其地址,有义务在欧盟指定至少一名法律代表负责“接收、遵守和执行”命令。^⑤如果网络服务提供者不予指定,则成员国执法机关可以将指令签发给其在欧盟区域内的任何部门。^⑥“条例”设定了用以确保有关指令能够传送到网络服务提供者的诸多规则,包括对网络服务提供者不指定代表的制裁以及向网络服务提供者任一分支机构发送指令的可能性。“条例”排除纯粹适用于国内法的情况,即欧洲提交保存令不能在一国范围内使用。新制度放弃以往做出有关指令所遵循的属地原则^⑦,转向了基于网络服务提供者的属人主义。也就是说,数据所在的位置对于指令签发及向何处发出指令已经不再重要;网络服务提供者是否“在联盟中提供服务”,这一因素则变得尤为重要。这虽不意味着在欧盟可接触的每项服务都归属于该指令和法规的适用范围,但也是相当广泛的。

签发欧洲提交保存令还需要满足一些基本条件。第一,“在签发国国内类似情况下,对同一刑事犯罪可以采取类似措施”。第二,指令签发是必要的、符合比例原则的。第三,签发指令受限于所查犯罪的可能罪名、刑期。如果针对交互数据、内容数据签发欧洲提交保存令,则要求有关罪行“在

签发国可能被处以三年以上监禁刑”,或者属于“条例”列举的恐怖主义、欺诈、对儿童的性虐待和性剥削、儿童色情、攻击信息系统等罪行。针对注册信息、访问数据签发欧洲提交保存令的,不受上述限制。^⑧在这三个条件中,前两个条件类似于签发欧洲调查令。欧洲理事会的“通则”版本在此基础上又增加了额外条件,即避免出现与作证豁免权和特免权规则相冲突问题,避免出现有关新闻自由、言论自由的刑事责任问题。

欧洲提交保存令以经过签发并辅以经认证的证书形式传输给网络服务提供者及其代表。^⑨其中,证书可以是保障接受者核实其真实性的任何书面形式。^⑩这一点在欧洲理事会的“通则”版本中被进一步强调为“以安全可靠的方式”传递。这种传递方式并不如某些国家的国内法要求那么严格,这就为借助取证平台或其他适当的数字方式简化、加快提供了可能。这些取证平台可以由网络服务提供者建立,如已建立的商业性质取证平台;^⑪也可以由政府公共部门提供,如e-Codex^⑫,即欧盟委员会基于欧洲调查令、刑事司法协助要求建设的平台。^⑬证书中包括一些标准化的内容,以确保网络服务提供者对指令做出正确的反应。为避免对案件办理产生负面影响,指令的具体内容,尤其是签发指令的必要性、相称性以及案件细节,均不在传递范围之内;否则,将难以防范嫌疑人获得相关信息。^⑭

网络服务提供者的默认响应是将被请求的数据直接传输到签发机关,同样亦无须经由网络服务提供者所在国的执法机关。这一任务应当在收到指令后的10天内或者所要求的更短时间内完成,情况紧急的应当在6个小时内完成。^⑮如果网络服务提供者发现无法遵从指令的,可以按照“条例”规定启动沟通机制,由网络服务提供者予以必要的说明,再由签发机关决定是否撤回指令。具体事由包括个案中出现了指令不完整、包含明显错误、缺乏足够可执行信息或事实上不可行等情

形。当然,在是否撤回指令的问题上,签发机构处于主动地位,有权依据“条例”不予撤回。^⑥如果网络服务提供者发现遵从指令可能会导致与第三国法律相冲突的,应当告知指令的签发机关,并提供拒绝指令的理由,特别是有关法律、义务冲突性质的各种细节。^⑦基于前述放弃属地原则的指导思想,网络服务提供者不得仅以所涉第三国不存在同提交令相类似的法律规定、或有关数据储存在第三国等事由提出异议。

如果网络服务提供者无法定事由拒不遵从指令的,可能会导致制裁、强制执行两种程序后果。关于如何制裁,“条例”将交由成员国去做规定。但究竟是哪一成员国(签发国、所在国或其他国家)负责实施和执行,“条例”尚未明确。此外,欧洲理事会的“通则”版本中还增加了一项条款,希望成员国确保有关制裁的可能额度不超过网络服务提供者全球年总营收额的2%。^⑧如果该方案被成员国接受,那么有关制裁可能是不合比例原则的,其对于大型网络服务提供者会是一个天文数字的罚金。关于强制执行程序,它可能将欧洲提交保存令变成一个类似于欧洲调查令的经典互认工具。签发国的签发机关可以将该指令移送至执行国(系不同于欧洲调查令的执行国)的合适机关。后者将对指令予以确认和执行,当然也可以援引经典刑事司法协助的拒绝事由而不予确认和执行。

综上所述,“条例”直击由电子证据的易变性及国际性引发的具体问题,寻求同网络服务提供者的合作机制以应对当前网络犯罪的新变化。它规定成员国的执法机关有权命令其他成员国的网络服务提供者披露有关信息,这是在尝试构建一套全新的、强力的跨境电子取证机制和权利保护机制。对于成员国有关当局、网络服务提供者和其他受影响人员来说,“条例”维护了执法请求的高标准,亦保障了基本权利、透明度和问责制,提高了法律确定性。

(三)两种创新工具的比较

作为化解跨境电子取证挑战的两种法律应对工具,欧洲调查令与欧洲提交保存令存在着一些不同之处:(1)两者的跨国因素部分不同,分别为“证据在国外”“网络服务提供者在国外”。这会形成理念与程序不同的跨境取证双体系。(2)前者是通过指令引入的,许多内容(如制裁、救济内容)有待成员国立法进行具体化;后者拟通过条例引入,无需成员国进行配套立法。(3)前者涵盖各种证据;后者将电子证据单列出来进行规范。(4)两者的适用范围不尽一致。这主要体现为有关版本对欧洲提交保存令的适用做了特殊限制。欧洲理事会的“通则”版本还特别规定,欧洲提交保存令适用于执行监禁判决;^⑨适用于针对法人的诉讼中;^⑩不适用于出于向另一成员国或第三国提供司法协助的目的进行电子证据收集。^⑪(5)更为重要的一点差异是,前者依然落入刑事司法协助的窠臼,而后者则根本性地脱离了刑事司法协助的轨道。

第五点差异同两种指令的签发对象不一样不无关系。欧洲调查令关注不同成员国执法机关之间的关系处理,欧洲提交保存令更关注一个成员国执法机关同占有电子证据的网络服务提供者之间的关系对接。实践中,欧洲调查令始终经由执法机关的环节,执法机关要进行必要的审查。即便执行欧洲调查令需要私人单位参与合作时,合作的对象仍然是请求国与被请求国的执法机关。欧洲提交保存令则完全不同。其第一步就是与网络服务提供者进行联系,向其发出关于提交、保存数据的指令,要求其对所要求的数据予以回应。网络服务提供者无须同当地执法机关进行接洽,当地执法机关通常不介入或者介入程度很低。也就是说,“条例”在执法机关和网络服务提供者之间架设了一种全新的关系。无论是否愿意,网络服务提供者都要接受、遵从相关指令。网络服务提供者成了执法机关的延展触角,取代了所在国执法机关的固有角色。

这一点差异也体现在审查理据及风险承担方面。首先,欧洲调查令赋予被请求国的执法机关大量拒绝事由,如以维护基本权利为由进行拒绝等;欧洲提交保存令给予网络服务提供者的拒绝事由则少很多,主要事由是“实际不可执行”。举例来说,双重归罪原则在是否执行欧洲提交保存令时就被取消了——虽然欧盟委员会的“条例”初始提案版本中仍然保留着通用的基本权利条款,但却是作为例外条款;^⑧欧洲理事会的“通则”版本中干脆删除了这些用作拒绝事由的维护基本权利条款。欧洲提交保存令的如此设计必然会影响到被告人、嫌疑人、第三方等主体的基本权利。其次,欧洲提交保存令中网络服务提供者还面临着不遵从指令将被制裁的风险。个中道理是,网络服务提供者进行审查时主要考量的是商业利益因素,它们会判断遵从或拒绝指令哪个更符合商业利益,在存有疑问的情况下拒绝指令要大于配合的可能性,苹果公司和美国联邦调查局之间的圣贝纳迪诺枪手一案就是一个例证。苹果公司作为网络服务提供者更愿意向所有用户做出承诺——“我们保护您的数据”,即便由此可能受到有关机关的制裁。^⑨例证中的案件是一起恐怖主义犯罪案件,联邦调查局期望苹果公司解锁已死亡凶手圣贝纳迪诺枪手的苹果手机。在这样的案件中,社会大众不会认为对已死亡凶手有什么出格的隐私侵犯问题。然而,苹果公司同国家执法部门的逻辑是不一样的:后者坚持履职保护公民享有不受暴力侵犯的基本人权;而前者更考虑商业利益,对股东负责是其首责,拒绝执行联邦调查局的指令显然更符合其利益。正因为网络服务提供者主要考量的是潜在利益,所以有时候会选择拒绝配合指令,从而导致可能面临被制裁的风险。

两种指令的前述差异也可以理解为它们之间的重要连接点,从中可以管窥两者的共性之处。两种指令都是面对跨国电子取证的需要,以推动电子证据等在不同国家被加速“分享”用于办案为

基本导向。欧洲调查令是在不同成员国的执法机关之间实现证据方面的“请求—协助”,欧洲提交保存令是在一个成员国执法机关与另一国网络服务提供者之间实现电子证据方面的“指令—配合”。两者在规则细节方面确有“小异”,但就促进电子证据的高速固定、流转、运用方面堪称“大同”,且无论是欧洲调查令还是欧洲提交保存令,在被签发之前均需要进行必要性和正当性审查。值得注意的是,“条例”文本已经明确,欧洲提交保存令不妨碍继续使用欧洲调查令。^⑩这将形成两种指令长期共存的状态,构成了欧盟“分享电子证据”的不同层次方案。它们在不同程度上满足了网络犯罪治理上快速获取证据的根本性需求,打破了获取数据需要进行烦琐物理定位的传统做法;它们使得互联网的平等精神在跨境电子取证领域得到了良好的彰显。

长期以来,互认一直是促进在刑事司法事项上实现跨国合作的一种手段。欧洲调查令产生于人员自由流动和边界管控废除的需要,是一种基于成员国“明示”互认的跨境取证机制;相比而言,欧洲提交保存令不需要通常作为指令接收端的执法机关参与。从这一点来看,它可能比欧洲调查令更具争议性,人们可能会质疑欧洲提交保存令中是否仍然存在由执法机关积极认可指令而出现的任何承认。^⑪因为当且仅当网络服务提供者拒绝遵从指令时,执法机关之类的机构才会介入。这个问题的答案可以归结为一种特殊的互认——默认。可以肯定的是,欧洲提交保存令也是重视互认的。欧盟标榜“信任”,但其成员国保持着审查其他成员国是否值得信任的习惯,欧洲提交保存令则对成员国的互认提出了更高的要求。欧洲提交保存令是另一种基于成员国“默示”互认的跨境取证机制。从欧洲调查令到欧洲提交保存令,反映了欧盟范围内成员国治理网络犯罪互认理念的一次飞跃。

欧洲提交保存令源于网络空间无国境性的办

案需要。^⑧即便是对那些嫌疑人、被害人、侦查机关及法律手续均处于一国境内的案件,也可能有签发欧洲提交保存令的需要,如办案所需数据为另一成员国的网络服务提供者所拥有的。从“明示互认”到“默示互认”的跃升,使用欧洲提交保存令比欧洲调查令对欧盟成员国执法更具吸引力,也具有更大创新性的影响力。在两者并行的情况下,很难想象欧盟成员国执法机关会不选择欧洲提交保存令,因为该指令的程序更简单、响应期限更短、执行力度更大。即便网络服务提供者未能提供所请求数据,类似于欧洲调查令的程序仍可以启动,且麻烦会减少(比如在这种情况下网络服务提供者更不好被拒绝等)。

四、欧美完善跨境电子取证机制的协商

当下欧盟转向通过欧洲提交保存令为主的跨境电子取证,是不容逆转的趋势。这一转变几乎是与美国颁布《云法》形成跨境电子取证新规同步发生的,二者都规定了执法机关可以直接向网络服务提供者签发令状获取域外电子证据;它们都是在缩窄2013年《欧美司法协助约定》所确立的、由不同国家执法机关开展协助的途径,尝试着开拓司法协助约定之外的、由网络服务提供者直接提供所控制数据的做法。如此,欧盟迎来了同美国协商促成新衔接制度的调整期,虽然有关协商和制度建设因全球疫情爆发而进程有所缓慢。

首先,欧美开展旨在完善跨境电子取证机制的协商具有必要性,必须减少两个法域之间发生法律矛盾的可能性和冲突地带。假如双方均只是单方面执行各自法律,那一定会陷各种数据公司于两难境地:它们要么遵从请求国提交证据的相关指令,要么遵从数据存储国保护数据的法律。具体来说这种冲突体现在,欧盟成员国可以根据“欧盟电子证据条例”要求美国公司提供数据获取等协助,而美国《存储通信法》却禁止提供此类获取协助,除非有关国家与美国达成双边协议;^⑨同时,美国当局要求获取存储在欧盟成员国的数据

时,有关企业可能会面临违反欧盟《通用数据保护条例》等法律的风险。^⑩前述微软公司一案^⑪便反映了这种尴尬处境,欧洲也有许多这样的案件。如2013年1月法国巴黎地区法院曾向美国推特公司发出一份命令,要求其提供关于一些种族主义或反犹太信息的制作者的身份数据,而推特公司同样予以拒绝,理由是涉及的信息“存储于美国”。巴黎地区法院坚持认为推特公司有义务提交数据,因为法国用户的注册数据受到法国法律和推特公司使用条款的规制。^⑫因此,虽然“同一公司被迫违反一国法律以遵守另一国法律”并非新事物,欧盟“条例”相关条款亦规定“网络服务提供者认为数据请求将损害基本权利或违反第三国法律时有权选择司法审查”,^⑬但是欧美两个法域积极协商化解法律冲突显然更加具有建设性。

司法实践证明欧美达成新的跨境电子取证协议具有坚实需求。从欧盟的视角来看,若法律冲突得不到解决,必然会危害欧洲提交保存令的效果。当下全球主要网络服务提供者在欧盟境内注册的相对较少,使得这一问题对欧盟一方更为凸显。从美国的视角来看,如果没有欧盟的支持,其通过《云法》强制位于美国的网络服务提供者保存和披露其在欧盟范围内的数据也存在很大的困难,因为欧盟大多数成员国的法律都不允许一国执法机关访问另一国网络服务提供者的数据(只有西班牙和法国允许国内网络服务提供者直接对外国执法请求做出响应)。^⑭如果欧美达成协议,这类需求便能获得有效满足。

其次,欧美开展旨在完善跨境电子取证机制的协商具有可行性。欧美关于跨境电子取证的新机制不约而同地开始重视网络服务提供者的协助地位,均属于“通过司法协助之外的机制获取数据”的“非中介获取模式”(Unmediated Access Model)。^⑮它们的共同法律机理是,将用户和公司的位置作为管辖权的决定因素。它们共同放弃了长期存在的属地原则,即数据的实际存储地标准,而在

权衡考量的基础上选择了赋予公司以提供数据的义务,而不管数据存储的位置为何。从呈现表象上看,这是跨境电子取证转向了“数据控制者”标准。从深层实质来看,这也可以被理解为由根据数据存储地确定管辖的属地原则向依靠数据控制者的属人主义转型。这里的属人“因素”是特定的网络服务提供者。它们控制着拟用作证据的各种数据,能够简单地从“境内”场所访问“境外”的数据,完成配合取证的义务。

无论是美国的《云法》方案,还是欧盟的“条例”方案,都并未试图颠覆现有刑事司法协助制度,均只是提议增加一种在少数互信国家间快速跨境获取电子证据的机制。^⑨而且它们并不排斥不同法域之间达成新的跨境取证协议。实际上,部分欧洲国家同美国达成协议已经走向前台。据报道,2019年10月3日美国已经同脱欧的英国签署了一项关于电子证据跨境访问的双边协议,允许美国网络服务提供者按照《云法》规定提供来自英国的内容数据。“通过在欧盟层面引入一种跨境电子证据交换工具,欧盟应成为美国的首选合作伙伴”。^⑩显然,与其零碎地拼凑具体国家间的“一对一”协议,不如达成一项欧美法域间的整体性协议。

最后,欧美开展旨在完善跨境电子取证机制的协商需要求同互认。这是方法论问题,即扩大共同点、实现互相认可。欧美两法域的新规存在较多差异。有些差异是形式上的。例如,美国《云法》仅适用于在美国注册的网络服务提供者,不适用于在美国提供服务的其他国家、地区注册的网络服务提供者;欧盟“条例”追求更广泛的覆盖权限,包括无论是否在欧洲注册成立的“所有在欧盟经营的网络服务提供者”。^⑪又如,美国《云法》解除了现行法律《电子通信隐私法》的限制,允许有关公司自愿提供信息;而欧盟“条例”则力推具有约束力的证据“指令”。^⑫有些差异是实质性的。这集中体现为美国的做法是否行使了治外法权,是否沦为鲜明的司法单边主义。在欧洲人看来,

《云法》赋予了美国法官以全球管辖权,不仅涉嫌侵犯有关国家的司法主权,更不符合欧洲《通用数据保护条例》等法律的要求。2015年欧洲政策研究中心在《第三国执法机关获取电子证据》中指出,“美国执法机关以无中介的方式访问受欧盟管辖的私人公司控制的数据,这对刑法、人权法以及欧盟基本权利法中的管辖权概念均构成根本性的挑战。它直接而明显地绕过了欧美司法协助约定范围内所预设的、具有法律约束力的现有渠道。这样做可以避开被请求的欧盟成员国及其指定的中央机构(通常是司法部)表示‘同意’,可以避开所设定独立司法机构的监督。”^⑬而在美国人看来,美国法官根本不存在域外法适用的问题,因为美国司法部认为只要可以从美国领土访问到有关数据,这些数据就属于美国法律可以轻松“领土化”的地区;有关令状“并未将在外国实施的行为定罪”“并不涉及美国执法人员在海外开展工作”,美国政府不存在行使治外法权的问题。^⑭对于以上两种差异,欧美均可以通过协商扩大求同、达成互认。

以消解美国做法的“治外法权”色彩为例,这需要双方通过谈判方式就具体主张进行沟通。在什么情况下,一国执法机关可以被允许向网络服务提供者要求进行跨境数据提交?在什么情况下,下达指令即构成一种规避主权国家法律的行为,是不被允许的?这需要欧美应用谈判的智慧。欧洲政策研究中心出具的报告中,就提出过一种大胆设想的方案——“迈向跨大西洋调查令(Transatlantic Investigation Order,简称TIO)系统,以加快和提升欧美执法机关之间在刑事司法领域的合作”;“跨大西洋调查令将以现行欧洲调查令的‘基准’作为欧美合作的核心基础”。^⑮这是要设计一种比欧洲提交保存令更高层级的跨境电子取证工具。

2019年2月5日,欧洲理事会做出的一份授权决定——“关于授权启动同美国就欧美刑事司法合作中访问跨境电子证据之国际约定相关谈判的

建议”。^⑧欧盟委员会采纳决定后部署了相关工作,特别强调“在有关跨境电子取证的国际条约谈判中保持欧盟范围内数据保护的较高水平应当成为参考”。^⑨自此,欧美两地开始寻求在域外电子证据合法获取的途径上进行新合作,致力于搭建一个尊重司法主权、保护数据权益的新条约系统。诸如跨大西洋调查令等各种设想显得雄心勃勃,可以防止有关国家简单粗暴地在域外执行本国法律。在新形势下,人们绝不能低估这种弃用属地原则的双边、多边制度协商可能引发的效应。

五、对中国的影响与启迪

欧盟围绕欧洲调查令、欧洲提交保存令进行的制度变革在国际上产生了重大影响。其针对欧洲提交保存令的持续推动工作,更为改造《布达佩斯公约》提供了新契机。2019年2月5日,欧洲理事会在授权欧盟委员会就跨境电子取证进行欧美谈判的同时,也作出了另一项授权决定——“关于授权参加《欧洲理事会网络犯罪公约》第二附加议定书谈判的建议”。^⑩显然,欧洲提交保存令的最终问世将续展《布达佩斯公约》的域外取证方案,缓解各成员国执法机关受困于接收、承认和执行杂乱命令的繁重压力,并通过分享电子证据提升各成员国治理网络犯罪的实际成效。

我国必须对这一动态予以高度的关注。一方面,欧盟的创新将产生一种类似于美国《云法》分享跨境电子证据的“国际范”机制。2018年4月,美国国会研究服务中心的立法律师穆里根指出,某些核准《云法》的国家在办理严重犯罪案件中,只要不针对美国人或位于美国的个人,且满足《云法》的条件,便可以直接要求美国网络服务提供者提供数据。^⑪欧盟的“(电子证据)条例”设计的方案与《云法》路径同属“非中介获取模式”,而且还会经由欧美协商再行靠拢。而鉴于欧美数据市场规模巨大,大多数知名网络服务公司或数据公司都位于美国,因此欧美制定的标准和法规有可能会形成“国际标准”。^⑫另一方面,欧美谈判会在不同

国家之间建立一种“俱乐部”制度。欧盟与美国一旦谈判成功,将可以通过“互认”方式允许对方访问、获取己方相关公司持有的数据。这是一个近30个国家的“大俱乐部”区域,它们之间的规则肯定会吸引到更多关系密切国家的效仿甚至参与。对于被排除在“俱乐部”外的国家,特别是这些国家的网络服务公司或数据公司,都有可能陷入是否遵从欧美法律的尴尬境地。我国当下的处境就像二十年前面对《布达佩斯公约》出台一样。为了避免“历史重演”,我国应当力戒再次因无所作为陷入跟与不跟的窘境。

同时,我国可以从这一动态中获得有益的启迪。网络空间有国家主权,这是我国长期坚持的一项法律原则。这一原则在跨境电子取证领域的体现就是要尊重相互的网络空间主权、数据主权。然而,在现阶段“领网”还不是一个像领陆、领水、领空一样界域清晰的概念。在实践中,我国对位于境外服务器无法直接获取的电子证据,习惯于采取远程访问的方式进行提取。这一措施通常会被贴上远程勘验、网络在线提取甚至技术侦查等侦查措施的标签。2016年,最高人民法院、最高人民检察院、公安部联合发布的《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条做出明确:“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。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。”这一条文及背后实践,同我国的国家主张存在一定的冲突。2019年1月,公安部出台《公安机关办理刑事案件电子数据取证规则》,第23条将“网络在线提取”的数据调整限定为“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”。新规定似乎表明我国并不对“域外计算机信息系统非公开发表的电子证据”进行提取,这缓解了跨境电子取证遭遇的合法性质疑。然而,侦查人员在境内对“域外计算机信息系统公开发表

的电子证据”进行提取,就不会遭到合法性挑战么?还有,对“域外计算机信息系统非公开发布的电子证据”,如何进行除刑事司法协助之外的合法取证呢?这都是需要我们进一步思考的问题。

2021年,最高人民检察院施行的《人民检察院办理网络犯罪案件规定》第56条对跨境电子取证的原则做了重申,明确了“尊重协作国司法主权”等原则。此类立法例意味着我国现阶段需要找到既坚持原则又寻求扩大共识的智慧。显而易见,欧盟改造跨境电子取证机制的前述经验,可以启发我国对国家主权原则下跨境电子取证方案做出有理据的教义解释。同美国一样,欧盟以成员国的“网络服务提供者”作为“中介”进行跨境电子取证,本质是放弃“属地原则”,走向“属人主义”。这里是将“网络服务提供者”作为成员国有管辖权的一种特殊的诉讼参与人,也就是作为跨境电子取证的直接实施者即连接点。这就避免了以属地管辖权进行解释难以自圆其说的困境,而走进了基于属人管辖权进行阐释的另一片天地。借鉴这一种解释思路,对于中国侦查人员在境内对“域外计算机信息系统公开发布的电子证据”进行提取,是不是可以理解为将“所有人”作为本国管辖权的诉讼参与人,亦即作为跨境电子取证的连接点,用以解释取证的合法性?以此类推,我国还可以进一步将侦查人员实施的网络在线提取等跨境电子取证,改造为由侦查人员要求案件中证人、被害人、嫌疑人及其他诉讼参与人远程下载提交。这将是一个基于“属人主义”进行跨境电子取证合法性规则改造的初步构想。我国若能从这个角度进行法条解读、制度调整,则能提炼出符合国际共识和中国智慧的经验。这将是拓展属人主义管辖权的中国方案。

欧盟完善跨境电子取证规则的大幕已经展开。有人预测,这一改变所促成的《欧洲理事会网络犯罪公约》第二附加议定书谈判预计会持续两年半的时间。虽然前行之路困难重重,但是没有

什么可以阻止欧盟及其成员国加快处理其执法机关获取域外电子证据的进程。这是电子证据领域的具体变革。它走向欧盟不同成员国的共同规则,走向欧美两个法域的共同规则,也对世界范围内统一规则的形成产生着深刻的影响。从乐观主义的立场来看,欧盟关于欧洲调查令、欧洲提交保存令的探索是在建设一种区域性的“电子证据法”,也可以理解为推出一种全球法律一体化的电子证据法的前奏。“各国法律制度都面临着处理电子证据的同样问题……各国相似的处理是否会导致全球性或区域性的电子证据法?这是可行的,可期待的,也许是不可避免的。”^⑩未来的变化充满想象空间。

注释:

①《布达佩斯公约》实际上是欧洲理事会成员国、国际刑警组织、欧洲刑警组织、经济合作与发展组织、八国集团、英联邦和联合国等国家、国际组织机构致力于惩治网络犯罪的共同成果。See Jerman-Blažič B & Klobučar T, A New Legal Framework for Cross-Border Data Collection in Crime Investigation amongst Selected European Countries, *International Journal of Cyber Criminology*, vol. 13: 2, p. 273(2019).

②《布达佩斯公约》所规定的多边协助机制主要包括“有关临时措施的多边协助”“有关侦查措施的多边协助”“24/7协作网络”三大机制,分别涉及成员国相互之间协助开展紧急数据保护、搜查扣押以及建立七天24小时不间断的联络点等内容。See The Council of Europe, *Convention on Cybercrime*, Art. 29-35, European Treaty Series-No. 185, Nov. 23, 2001.

③Ibid, Art. 23.

④J. P. Mifsud Bonnici, M. Tudorica & J. A. Cannataci, The European Legal Framework on Electronic Evidence: Complex and in Need of Reform, in M. A. Biasiotti et al. eds., *Handling and Exchanging Electronic Evidence Across Europe*, Springer, 2018, p. 232.

⑤据有关统计,近年欧洲大约有85%的刑事案件侦查活动有收集电子证据的需要,这其中2/3的案件有向网络服务提供者调取跨境电子证据的需要。See European Commission Staff Working Document, *Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament*

and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying down Harmonized Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, 2018, p. 14.

⑥前者指向网络服务提供者发送非法定配合义务的、非强制性的电子取证请求,后者是修改国内法中关于跨境电子取证遵循属地原则的规定。比利时是后者的代表,其先确立新判例、后修改《刑事诉讼法》,明确面向该国公民的网络服务提供者具有提供合作的义务,而不论数据存储的地点或提供服务的总部具体在哪里。See Stanislaw Tosza, All Evidence is Equal, but Electronic Evidence is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order, *New Journal of European Criminal Law*, Vol. 11: 2, p. 169(2020).

⑦The Council of the European Union, Council Act of 29 May 2000 Establishing in Accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000/C 197/01, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000F0712\(02\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000F0712(02)&from=EN), Last Accessed on Jan. 23, 2022.

⑧The Council of the European Union, Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence, OJ L196, 2003, p. 45–55, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003F0577&qid=1596071422007&from=EN>, Last Accessed on Jan. 23, 2022.

⑨The Council of the European Union, Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters, OJ L 350, 2008, p. 72–92, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0978&from=EN>, Last Accessed on Jan. 23, 2022.

⑩Marcello Daniele, Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles, *New Journal of European Criminal Law*, vol. 6: 2, p. 180(2015).

⑪Andrew K. Woods, Why Does Microsoft Want a Global Convention on Government Access to Data? February 19, 2014, <https://www.justsecurity.org/7246/microsoft-global-convention-government-access-data/>, Last Accessed on Jan. 23, 2022.

⑫如《布达佩斯公约》第29条明确了请求开展临时协助的“双重归罪”原则。该条第4款规定,除了依照本协定第2条至第11条确定的犯罪,要求将双重犯罪作为提供有关搜查或类似访问、没收或类似取得、或数据的公开的相互协助的请求的条件,在该签约方有理由认为在公开情况下双重犯罪的条件不可能得到满足时,可以保留拒绝本条款下的保存请求的权利。

⑬Cybercrime Convention Committee, T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, Council of Europe, p. 123(2014).

⑭如脸书公司的大数据中心处于瑞典的吕勒市。See Yevgeniy Sverdlik, Facebook Data Center Investment in Sweden Nears US \$1B, <https://www.datacenterknowledge.com/facebook/facebook-data-center-investment-sweden-nears-us1b>, Last Accessed on Jan. 23, 2022.

⑮European Commission, Non-paper: Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2016, 15072/16, p. 5, <https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf>, Last Accessed on Jan. 23, 2022.

⑯Stored Communications Act, Pub. L. 99–508, Title II, § 201[a], Oct. 21, 100 Stat. 1860(1986).

⑰2016年7月14日,美国联邦第二巡回上诉法院曾经做出裁定,美国政府不能强迫微软公司提交位于境外服务器上的电子邮件,理由是“国会没有给《存储通信法》适用于域外的效力,依据该法律签发的令状仅适用于存储在美国的数据”。*Microsoft Corp. v. United States.*, 829 F. 3d 197(2nd Cir. 2016).

⑱Clarifying Lawful Overseas Use of Data (CLOUD) Act, H. R 1625, 115th Cong. div. V, § 103(a)(1)(2018).

⑲United States v. Microsoft Corp., 138 S. Ct. 1186, 200 L. Ed. 2d 610(2018).

⑳例如,《欧洲调查令指令》第32条规定,签发机关可以发布欧洲调查令采取任何措施,以暂时性地防止销毁、改造、消除、转移或清理可用作证据的物品;执行机关应当在收到欧洲调查令的24小时内,尽可能快地做出并传达一项临时性的决定;第10(2)(e)条、第11(2)条规定,根据欧洲调查令对特定电

话号码、IP地址的使用者进行识别的,不受双重犯罪要求的限制。Directive 2014/41/EU of the European Parliament and of the Council, of 3 April 2014, regarding the European Investigation Order in Criminal Matters, Official Journal of the European Union, L 130, 2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN>, Last Accessed on Jun. 17, 2020.

② European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM(2018)225 final, p. 1-54, https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF, Last Accessed on Jun. 17, 2020.

② EJM Secretariat, Status of Implementation of "2008/978/JHA: Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant (EEW) for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters", <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:EN:PDF>, Last Accessed on Jan. 23, 2022.

② Council of the European Union, The Stockholm Programme: An Open and Secure Europe Serving and Protecting the Citizens, OJ C 115, 2010, p. 1-38, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF>, Last Accessed on Jan. 23, 2022.

② EIOD, Art. 34(1).

② EIOD, Art. 34(2).

② EIOD, Art. 10(2)e.

② EIOD, Art. 30.

② EIOD, Art. 1.

② Inés Armada, The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?, *New Journal of European Criminal Law*, Vol. 6: 1, p. 11-12(2015).

③ EIOD, Art. 6(1).

③ EIOD, Art. 9(1)and(2).

③ Daniele, Evidence, p. 182.

③在维护国家安全利益或不符合双重归罪原则等情况下,执行国的执行机关可以拒绝执行签发国的请求。See

EIOD, Art. 11(1).

③ EIOD, Art. 12.

③ EIOD, Art. 12(5)and(6).

③ EIOD, Art. 15.

③这是欧盟实施的一项支持反恐怖主义、激进暴力行为领域刑事司法合作的年度行动资金。2015年度项目的预算是100万欧元,3个选择性计划。See European Commission, Communication from the Commission to the European Parliament, the European Council and the Council: Eighth Progress Report towards an Effective and Genuine Security Union, COM/2017/0354 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0354>, Last Accessed on Jan. 23, 2022.

③该计划的全称为“云在线取证中电子证据的刑事收集”(Criminal Justice Access to Digital Evidences in the Cloud-LIVE_FORensics)计划。

③“LIVE_FOR”计划的主要目标包括:(1)归整《指令》实施中的问题与障碍;(2)促进司法机关掌握云计算环境下在线取证领域的最新科教成果。Jerman-Blažič & Klobučar, A New Legal Framework for Cross-Border Data Collection in Crime Investigation, *International Journal of Cyber Criminology*, Vol. 13: 2, p. 277-278(2019).

④ European Commission, Commission Staff Working Document, Impact Assessment, Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, SWD/2018/118 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN>, Last Accessed on Jan. 23, 2022.

④ Dan Jerker B. Svantesson, Solving the Internet Jurisdiction Puzzle, Oxford University Press, 2017, quoted from Tosza, All Evidence, p. 169.

④ Council of the European Union, Council Conclusions on Improving Criminal Justice in Cyberspace, 2016, p. 1-5, <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>, Last Accessed on Jan. 23, 2022.

④ Non-paper from the Commission Services, Improving

Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward, 2017, p. 4-5, https://ec.europa.eu/home-affairs/system/files/2017-05/20170522_non-paper_electronic_evidence_en.pdf, Last Accessed on Jan. 23, 2022.

④④ European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM(2018)225 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595206697885&uri=CELEX:52018PC0225>, Last Accessed on Jan. 23, 2022.

④⑤ Eleni Kyriakides, Digital Free for All Part Deux: European Commission Proposal on E-Evidence, Just Security, May 17, 2018, <https://www.justsecurity.org/56408/digital-free-part-deux-european-commission-proposal-e-evidence/>, Last Accessed on Oct. 27, 2021.

④⑥ European Commission, Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence, http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm, Last Accessed on Oct. 27, 2021.

④⑦ Ibid.

④⑧ Ibid.

④⑨ European Commission, Proposal for a Directive of the European Parliament and of the Council Laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, COM(2018) 226 final-2018/0107(COD), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN>, Last Accessed on Jan. 23, 2022.

⑤⑩ Ibid, Art. 3.

⑤⑪ Ibid, Art 7.

⑤⑫ Commission Staff Working Document Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on the Law Applicable to the Third-party Effects of the Assignment of Claims Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Applicable Law to the Proprietary Effects of Transactions in Securities, SWD/2018/052 final/2-2018/044(COD), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=>

CELEX%3A52018SC0052%2801%29, Last Accessed on Jan. 23, 2022.

⑤⑬ European Data Protection Board, Summary of the Opinion of the European Data Protection Supervisor on Proposals regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters, OJ C 32, 2020, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XX0131\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XX0131(01)), Last Accessed on Jan. 23, 2022.

⑤⑭ Council of the European Union, Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters-general Approach, <http://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf>, Last Accessed on Oct. 27, 2021.

⑤⑮ Council of the European Union, EPOR (General Approach version), 2018/0107(COD), <https://data.consilium.europa.eu/doc/document/ST-6946-2019-INIT/en/pdf>, Last Accessed on Jan. 23, 2022.

⑤⑯ Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, 2018/0108(COD), 2019, https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf, Last Accessed on Jan. 23, 2022.

⑤⑰ European Commission, Proposal for a Directive of the European Parliament and the Council on Information Exchange Between Law Enforcement Authorities of Member States, Repealing Council Framework Decision 2006/960/JHA, COM(2021)782 final-2021/0411(COD), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0782&from=EN>, Last Accessed on Jan. 23, 2022.

⑤⑱ 欧洲提交令、欧洲保存令一般分别被简写为EPOC、EP-OC-PR。这种简称容易造成混淆,有人建议分别简写为EP-dO、EPsO。

⑤⑲ See European Production and Preservation Orders Regulation (EPOR), Art. 2(1).

⑥⑰ EPOR, Art. 2(2).

⑥⑰ European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, Explanatory Memorandum[hereinafter EPOR Explanatory

Memorandum], COM/2018/225 final- 2018/0108(COD), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>, Last Accessed on Jul. 31, 2020.

⑥2EPOR, Art. 2(3).

⑥3EPOR Explanatory Memorandum, Art. 3.

⑥4Ibid.

⑥5 Council of the European Union, Directive of General Approach, Art. 3(1).

⑥6EPOR, Art. 7(2).

⑥7该原则要求将管辖原则同数据存储位置联系在一起, 前述微软公司案件阐释了该原则。Microsoft Corporation v. United States of America, 829 F. 3d 197(2nd Cir. 2016), p. 215.

⑥8EPOR, Art. 5(4).

⑥9条例的附录对证书进行了标准化。European Commission, Annexes to the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM (2018)225 final, April 17, 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_2&format=PDF, Last Accessed on Jan. 23, 2022.

⑦0EPOR, Art. 8(2).

⑦1如 Facebook 公司提供有在线取证平台。See Facebook, Law Enforcement Online Requests, <https://www.facebook.com/records/login/>, Last Accessed on Jan. 23, 2022.

⑦2“e-Codex”是由欧盟提供资金赞助开发的,旨在促进欧盟内数字司法服务部署的一种数字服务基础平台,可以用于实现跨境电子证据的安全及标准化流转。EVIDENCE2e-CODEX, Matching Evidence to E-CODEX, <https://evidence2e-codex.eu/a/matching-evidence-to-ecodex>, Last Accessed on Jan. 23, 2022.

⑦3EUROJUST, Eurojust Meeting on the European Investigation Order, 2018, p. 15, https://www.ejtn.eu/Documents/About%20EJTN/Criminal%20Justice%202019/CJSWG%20Lisbon/2018-12_Outcome-Report_Eurojust-meeting-on-EIO-Sept2018_EN.pdf, Last Accessed on Jan. 23, 2022.

⑦4EPOR Explanatory Memorandum, p. 18.

⑦5EPOR, Art. 9(1)and(2).

⑦6EPOR, Art. 9(3)-(6).

⑦7EPOR, Art. 15(1)and(2), Art. 16(1)and(2).

⑦8EPOR (General Approach version), Art. 13.

⑦9EPOR (General Approach version), Art. 3(2).

⑧0Ibid.

⑧1EPOR (General Approach version), Art. 3(1a).

⑧2Tosza, All Evidence, p. 178.

⑧3Matt Zapotosky, FBI has Accessed San Bernardino Shooter's Phone Without Apple's Help, https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html, Last Accessed on Jan. 23, 2022.

⑧4EPOR, Art. 23.

⑧5See Elodie Sellier & Anne Weyembergh, Criminal Procedural Laws Across the European Union: A Comparative Analysis of Selected Main Differences and the Impact They have over the Development of EU legislation, Study Requested by the LIBE Committee of the EU Parliament, PE 604. 977, August 2018, p. 31, quoted from Tosza, All Evidence, p. 177.

⑧6Tosza, All Evidence, p. 177.

⑧7目前尚不清楚欧盟作为一个整体能否与美国达成执行协议。欧盟各成员国亦可能同美国以双边方式达成此类协议,作为对《云法》的回应。See Jennifer Daskal & Peter Swire, A Possible US-EU Agreement on Law Enforcement Access to Data?, Just Security, May 21, 2018, <https://www.justsecurity.org/56527/euagreement-law-enforcement-access-data/>, Last Accessed on Nov. 3, 2021.

⑧8根据《通用数据保护条例》第48条,第三国行政当局要求控制人或处理人转移或披露个人数据的判决或决定,只有在基于国际协议的情况下,如国际司法协助制度,才可能被认可或执行。因此,《通用数据保护条例》第46条成为欧洲方面的“封锁条例”。2020年7月16日,欧洲法院推翻了欧美之间达成的《欧美隐私盾牌》,驳回了允许在欧盟开展业务的公司将数据传输到美国的协议。See Kate Cox, US-EU Privacy Shield Data Sharing Agreement Struck Down by Court, July 17, 2020, <https://arstechnica.com/tech-policy/2020/07/court-tosses-us-eu-data-sharing-agreement-amid-us-surveillance-concerns/>, Last Accessed on Nov. 3, 2021.

⑧9United States v. Microsoft Corp.

⑧0See Cybercrime Convention Committee (T-CY) Cloud Evidence Group, Application of Article 18. 1. b Budapest Conven-

tion on "Production Orders": Compilation of Replies to the Questionnaire, 18 February 2016, T-CY(2015)22, p. 15, <https://rm.coe.int/09000016805a0873>, Last Accessed on Nov. 3, 2021.

⑨ See Mirko Hohmann & Sophie Barnett, System Upgrade: Improving Cross-border Access to Electronic Evidence, Global Public Policy Institute (GPPi), 2018, p. 18, https://www.gppi.net/media/GPPi_2018_Hohmann_Barnett_System_Upgrade.pdf, Last Accessed on Jan. 23, 2022.

⑩ European Commission, Questionnaire on Improving Criminal Justice in Cyberspace Summary of Responses, https://ec.europa.eu/home-affairs/system/files/2020-09/summary_of_replies_to_e-evidence_questionnaire_en.pdf, Last Accessed on Jan. 23, 2022.

⑪ Sergio Carrera et al., Access to Electronic Data by Third-Country Law Enforcement Authorities, Challenges to EU Rule of Law and Fundamental Rights, Centre for European Policy Studies (CEPS), 2015, p. 9.

⑫ Hohmann & Barnett, System, p. 5-6.

⑬ European Commission, Recommendation of 5 February 2019 for a Council Decision Authorising the Opening of Negotiations in View of an Agreement Between the European Union and the United States of America on Cross-border Access to Electronic Evidence for Judicial Cooperation in Criminal Matter, COM(2019)70 final, p. 1-2, https://eur-lex.europa.eu/resource.html?uri=cellar:b1826bff-2939-11e9-8d04-01aa75ed71a1.0001.02/DOC_1&format=PDF, Last Accessed on Jul. 17, 2020.

⑭ European Commission, Frequently Asked Questions.

⑮ Bertrand de la Chappelle, IGF 2018-Day 2-Salle VI-WS #393 CLOUD Act & E-Evidence: Implications for the Global South, Internet Governance Forum, 2018, <http://65.1.20.49/content/igf-2018-day-2-salle-vi-ws-393-cloud-act-e-evidence->

implications-for-the-global-south, Last Accessed on Jan. 23, 2022.

⑯ Carrera et al., Access, p. 61.

⑰ Christakis T. Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States), The White Book: Lawful Access to Data: The US v. Microsoft Case, Sovereignty in the Cyber-Space and European Data Protection, CEIS & The Chertoff Group White Paper, 2017, p. 26.

⑱ Carrera et al., Access, p. 80.

⑲ European Commission Staff Working Document, Impact.

⑳ Wojciech Rafał Wiewiórowski, Summary of the Opinion of the European Data Protection Supervisor on Proposals regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters, OJ C 32, 2020, p. 1, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XX0131\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XX0131(01)&from=EN), Last Accessed on Jan. 23, 2022.

㉑ European Commission, Recommendation for a Council Decision Authorising the Participation in Negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No 185), COM(2019)71final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:0071:FIN>, Last Accessed on Jan. 23, 2022.

㉒ Stephen P. Mulligan, Cross-border Data Sharing under the CLOUD Act. Congressional Research Service, 2018, p. 23.

㉓ Hohmann & Barnett, System, p. 14.

㉔ Mason S., Towards a Global Law of Electronic Evidence? An Exploratory Essay, The Journal of the Society for Advanced Legal Studies, Vol. 103, p. 20(2015).