

追逃追赃案件中跨境电子数据的调取----以发挥 G20 反腐追逃追赃研究中心的平台作用为切入点

李哲¹ 欧阳楚欣²

摘要：电子数据在二十国集团（G20）反腐追逃追赃跨境调查中的地位愈发关键，而成员国在跨境取证中长期依赖的司法协助程序复杂、效率低下，面对电子数据的高流动性与分段性更显无力。因此，执法机构直接向网络服务商提出跨境取证需求与直接获取数据逐渐成为各国跨境调取电子数据的重要替代性途径。为提高追逃追赃案件中跨境调取电子数据的效率，G20 反腐追逃追赃研究中心应积极推广有关跨境电子数据调取的替代性方式，为成员国提供相关的取证技术辅助，帮助查明各成员国相关法律规定，成为各国跨境调取证据的联络中心，并积极促进成员国间就反腐败追逃追赃的跨境取证签署协议或采取其他形式的合作。

关键词：跨境取证 电子数据 司法协助 直接调取

一、G20 追逃追赃案件中跨境电子数据调取现状与司法协助困境

¹ 澳门大学法学院副教授。

² 澳门大学法学院博士研究生。

跨境调查活动在二十国集团（以下简称 G20）追逃追赃案件中普遍存在，早在 2013 年，G20 成员国集团就发布了《20 国集团司法协助高级原则》（*G20 High-Level Principles on Mutual Legal Assistance*）以帮助成员国之间就反腐败及追逃追赃的合作。³一直以来，促进成员国在追逃追赃案件中的合作也是 G20 反腐败工作组（G20 Anti-Corruption Working Group）的重点工作。⁴

即便如此，司法协助作为成员国之间唯一得到认可的官方合作渠道，表现却不尽如人意，根据 G20 反腐败工作组在 2023 年发布的报告显示，中国在 2018 到 2022 年期间共计提出了 23 个司法协助请求，经过 4 年，尚有 17 个待处理，占比高达 71.93%，其耗时之漫长可见一斑。⁵

从其他国家的司法实践来看，司法协助在跨境电子数据调取上同样表现不佳，欧盟的在关于电子证据获取规则的说明中提及，由于程序复杂，欧盟与美国的司法协助周期至少需要 10 个月以上，欧盟与美国的司法协助程序详见下图。⁶

³ G20 High-Level Principles on Mutual Legal Assistance, https://www.unodc.org/documents/corruption/G20-Anti-Corruption-Resources/Principles/2013_G20_High-Level_Principles_on_Mutual_Legal_Assistance.pdf, last accessed 08/12/2023.

⁴ Official Website of G20 Anti-Corruption Resources, <https://www.unodc.org/unodc/en/corruption/g20-anti-corruption-resources/by-thematic-area.html>, last accessed 08/12/2023.

⁵ G20 Anti-Corruption Working Group, Responses to the 2023 Accountability Report, p. 37.

⁶ *Frequently Asked Questions: New EU rules to obtain electronic evidence*, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345, last accessed 18/12/2023.



G20 成员国之间多年来在跨境取证上一味依赖耗时漫长的司法协助手段，而跨境腐败案件的犯罪方式已然日新月异，电子数据在调查取证中需求日益迫切。信息化浪潮在“云技术”“大数据”等新兴技术下迎来了新的高潮，犯罪手段的信息化以及电子数据的普遍化已然是不可避免的趋势。根据联合国的一项报告显示，预计在 2023 年，全球网络犯罪的涉案金额将高达 5.2 万亿美元；⁷而早在 2018 年，欧盟就指出超过半数的刑事调查中都涉及跨境调取电子数据。⁸同时，虚拟货币与区块链的崛起，使得非法转移财产更为隐蔽，⁹显而易见，G20 追逃追赃案件中关于电子数据的跨境调取需求必然会愈发旺盛。

如前文所述，司法协助方式需要漫长的时间周期，这与电子数据

⁷ United Nations Office on Drugs and Crime Counter-Terrorism Committee Executive Directorate, Practical Guide for Requesting Electronic Evidence Across Borders(2021), p.xii.

⁸ European Commission, Commission Staff Working Document Impact Assessment, Brussels,17.4.2018, SWD(2018) 118 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN>, last accessed 11/12/2023.

⁹ The Official Website of UN Toolkit on Synthetic Drugs, <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/laundryproceeds/moneylaundering.html>, last accessed 11/12/2023.

这一特殊的证据本身负有的高流动性、分段性存在着天然的冲突。¹⁰所谓高流动性，即作为存储在电子介质中的信息，¹¹电子数据通过网络或电子设备进行存储与转移，具有的区别于其他证据的高传输效率；所谓分段性，即电子数据在处理的过程中被分为多个区块、片段或段落。¹²具体而言，在一般的司法协助中，通常需要提出需求方能够提供取证需要的具体位置，¹³而电子数据的高流动性与分段性导致了确定其所在位置与内容皆十分困难，这就使得针对电子数据的司法协助往往在提出需求的环节就遭遇挑战；其次，各国关于电子数据的定义、分类以及提取程序等法律规定并不一致，加之实践中可能存在执法机构关于请求取证的具体数据描述不够明晰，且在翻译与传达的过程中带来的误差问题，导致司法协助的请求与实际需求偏离而无法实现取证目的；最后，就算关于电子数据的司法协助需求能够顺利地提出并得到恰当地传达，但由于电子数据的保留时间有限，以及调取数据需要网络服务提供商配合，仍然会面临着实际取证时所需电子数据已经超过数据保留期限而取证失败的问题。¹⁴

正是由于司法协助在跨境调取电子数据中存在着种种不便，一些国家或地区已经不再将司法协助作为跨境调取电子数据的主要手段，例

¹⁰ Europol & Eurojust Public Information, Common Challenges in Combating Cybercrime, <https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf>, last accessed 23/12/2023.

¹¹ 《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》，第 116 条。

¹² Garcia-Molina, H., Ullman, J. D., & Widom, Database Systems: The Complete Book. Pearson, Pearson Education Limited 2014, p64.

¹³ 联合国毒品和犯罪办公室：《司法协助与引渡手册》，第 69-70 页、第 78 页，https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_C.pdf，最后访问时间 2023 年 12 月 23 日。

¹⁴ Europol & Eurojust Public Information, Common Challenges in Combating Cybercrime, <https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf>, last accessed 01/03/2024.

如近些年来，欧盟执法部门面临跨境电子数据提取需求时，选择司法协助作为取证方式的比例仅在 10%左右。¹⁵相比之下，G20 成员国在反腐追逃追赃案件中仍依赖于司法协助这一手段跨境调取电子数据，这显然已与实践中的需求有所背离。实际上，如何发展不同渠道，更多地利用新技术与一些非官方的新手段促进 G20 成员国之间在反腐追逃追赃案件中的合作与交流，亦是 G20 反腐败工作组在 2022-2024 年计划中的工作新重点。¹⁶G20 反腐追逃追赃研究中心（以下简称“G20 研究中心”）作为承载 G20 成员国在反腐追逃追赃方面学术交流与实践分享的平台，在进一步发展和促进 G20 成员国在追逃追赃案件中的合作上有着天然的优势，这也是 G20 研究中心应对新的需求时应有的功能延伸。由此，本文试图以 G20 追逃追赃案件中的需求为基础，借鉴目前各国跨境调取电子数据的主要方式，由 G20 反腐追逃追赃研究中心作为承载平台，探索 G20 追逃追赃案件中跨境电子数据调取的新方案。

二、跨境调取电子数据的替代性取证手段的盛行及其困境与挑战

跨境调取电子数据不是 G20 追逃追赃案件中独有的问题，亦是全世界打击犯罪中必须面对的共同问题，欧盟及美国等国家在此领域已形成一些较为通行的应对方案，主要包括执法机构直接向网络服务供应商提出跨境取证需求以及执法机构单方获取电子数据两类手段。

¹⁵ Eurojust, SIRIUS EU Digital Evidence Situation Report (2019), P.22; Eurojust, SIRIUS EU Digital Evidence Situation Report (2020), P.23, 25; Eurojust, SIRIUS EU Digital Evidence Situation Report (2021), P.39-40.

¹⁶ G20 Anti-Corruption Working Group, Anti-Corruption Action Plan 2022-2024, p. 8.

相比于司法协助，这两类新方式都更具效率，但也有其各自的问题，例如两类取证方式目前在各国都缺乏具体的法律规范；且与司法协助相同，这两类方式也同样面对着信息技术发展所带来取证困难程度攀升的冲击。需要注意的是，各国并不认为这两类方式可以完全替代传统的司法协助手段，依然强调司法协助是跨境调取电子数据中最为正式的方式。¹⁷

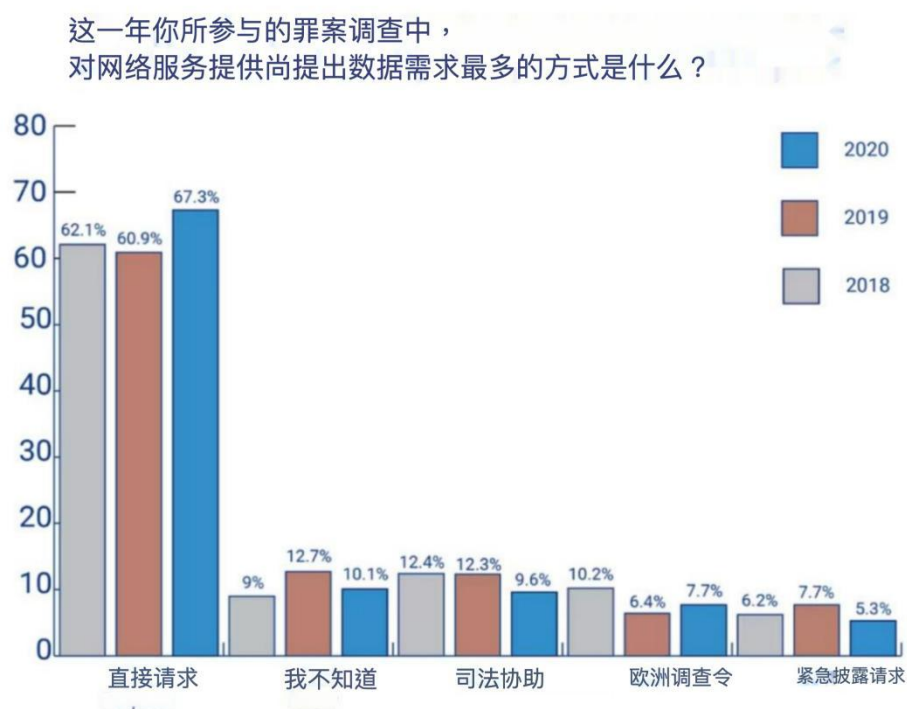
（一）直接向网络服务提供商提出跨境取证需求

直接向网络服务提供商 (Service Provider) 提出跨境取证需求是指一国执法机构基于当局和外国网络服务提供商之间自愿合作的基础，直接向外国网络服务提供商提出刑事调查所需的电子数据需求。直接向服务商提出跨境取证需求往往是合法获取非内容数据，即用户基础信息数据 (Subscribe Data) 以及流量数据 (Traffic Data) 的最便捷渠道。根据一些大型网络服务提供商的透明度报告，直接向服务提供商提出跨境取证需求通常可以在 10 个工作日内完成。¹⁸ 由于其极高的效率，直接向网络服务提供商提出跨境取证需求在欧盟已然成为执法机构最主要的跨境电子数据取证方式，且应用愈发广泛。2018 年至 2020 年期间，在获取网络服务商的电子数据的方式上，欧盟执法机构通过直接向服务商提出跨境取证需求的占比均在 60% 以上，远高

¹⁷ 据《天狼星欧盟电子数据情况报告》，司法协助依然是各国认可的最为正式的手段，且通过直接向服务商提出数据需求和单方获取电子数据所取得数据也可以作为司法协助需求提出的支撑性材料用以帮助提高司法协助的成功率与效率；美国在《云法案》(CLOUD Act) 中也强调向服务商提出数据需求的手段与司法协助并不存在矛盾，Eurojust, SIRIUS EU Digital Evidence Situation Report (2022); U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act (White Paper), April 2019, <https://www.justice.gov/opa/press-release/file/1153446/download>, last accessed 01/03/2024.

¹⁸ Eurojust, SIRIUS EU Digital Evidence Situation Report (2020), p. 65.

于司法协助 (MLA)、欧洲调查令 (European Investigation Order, EIO) 以及紧急披露请求 (Emergency Disclosure Request, EDR)，具体各种方式应用比例详见下图。¹⁹



在程序上，直接向网络服务提供商提出跨境取证需求主要包括执法当局提出需求与网络服务商接收并反馈需求两个环节。执法当局提出数据需求没有固定的模式，一般可能通过邮件、门户网站及单点联络机制 (Single Point of Contact) 提出需求。²⁰需求应当说明的内容与事项没有统一的要求，主要取决于网络服务提供商自身的要求，不同的服务商对此可能有不同的要求，某些大型的网络服务商为应对愈来愈多的数据需求，制定了相关的需求提出规则，设置了专门的门户网站用以沟通和接收需求，而有些小型的服务商对此则没有特别的规定

¹⁹ Eurojust, SIRIUS EU Digital Evidence Situation Report (2020), p. 17.

²⁰ Eurojust, SIRIUS EU Digital Evidence Situation Report (2020), p. 65.

或应对。²¹

直接向服务商提出跨境取证需求还有一种特别情形下的适用，即当涉及直接威胁生命或严重的身体伤害，紧迫、严重威胁国家安全或关键的基础设施和装置，或者针对未成年人的犯罪时，可向服务商提出紧急披露请求（Emergency Disclosure Request），当申请符合要求时，服务提供商会在几小时甚至几分钟内，向外国执法当局披露非内容数据。²²紧急披露请求近年来的适用显著上升，以欧盟为例，在 2018 年至 2020 年期间，欧盟当局提交的紧急披露请求有 112.1% 的增长。

23

（二）单方获取跨境电子数据

《网络犯罪公约》第 32 条正式确定了单方获取跨境电子数据这一跨境电子数据获取方式，具体是指一国执法机构在无需协助的情况下，通过网络获取位于另一国境内可公开获得的计算机数据以及经数据持有人的合法同意后直接访问或接受存储在另一国境内的计算机数据。²⁴

公开资源具体指在互联网上任意公众皆可获取的信息及订阅的服务，如若公共网站或服务存在不对公众开放的部分，则此部分并不视为公开资源。²⁵对于跨境搜索公开资源，即使不存在《网络犯罪公

²¹ 部分大型网络服务提供商的门户网站链接如下所示：Google, https://lers.google.com/signup_v2/landing ; Microsoft: <https://leportal.microsoft.com/home> ; Twitter, https://legalrequests.twitter.com/forms/landing_disclaimer; Airbnb, https://airbnb-legal.force.com/s/login/?language=en_US, 最后访问日期 2023 年 12 月 17 日。

²² Eurojust, SIRIUS EU Digital Evidence Situation Report (2021), p. 18.

²³ Eurojust, SIRIUS EU Digital Evidence Situation Report (2021), p. 19.

²⁴ 《网络犯罪公约》第三十二条, <https://rm.coe.int/cets-185-and-expl-rep-chinese/1680a39f77>, 最后访问时间 2023 年 12 月 30 日。

²⁵ United Nations Office on Drugs and Crime, Investigation, Prosecution and Adjudication of

约》第 32 条，一般也被视为国际习惯法的一部分，在主权活动的框架内，跨境访问网络中的公开资料的行为经常发生，一般也没有国家对此类行为感到冒犯，这意味这种行为已被默许，并认为是合法的。

²⁶执法人员利用公共资源一般可以获得以下基本信息：其一，通过 ip 地址等公开的、在线的工具定位使用者的位置；其二，识别域名的所有者；其三，通过公开的社交媒体获得个人发布的图片、视频或是犯罪行为的罪证。随着信息搜索分析工具的发展，通过不同的工具或软件可以在公开资源中挖掘更多潜在信息。²⁷

跨境直接获取数据具体指一国执法机关在明确电子数据的存储地时，不经过协助，也无需通知另一国，经由提供访问者或披露数据的人的同意，单方面访问或收集处理合法存储在另一国方的电子数据。需要注意的是，同意必须合法自愿，不可通过强迫或欺骗手段获得，且一般情况下，这种同意都应当是明示的同意。在第 32 条第 2 款的规定中，并没有强制要求知悉数据所在地为跨境直接获取数据的前提条件，但是根据欧洲委员会网络犯罪委员会（Cybercrime Convention Committee）的报告，接受调查的成员国都表示不接受在不确定数据存储地的情况下跨境直接获取数据的行为。²⁸

由于跨境直接获取数据涉及非公开数据，执法人员在适用该手段

Foreign Terrorist Fighters Cases for South and South-East Asia(2018), p. 71.

²⁶ Nicolai Seitz, *Transborder search: A new perspective in law enforcement?*, Yale Journal of Law & Technology, p. 25-50, (2005).

²⁷ Official Website of Versatile InfoRmation Toolkit for end-Users oriented Open Sources exploItation, <https://cordis.europa.eu/project/id/242352>, last accessed 30/12/2023.

²⁸ Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?* <https://rm.coe.int/16802e79e8>, last accessed 30/12/2023.

时，需要满足以下三个条件：其一，明确数据存储之地；其二，数据存储之地为《网络犯罪公约》缔结国；其三，获取内容者的合法自愿同意。其中涉及的两个问题较为关键，包括能够作出同意的主体的范围；以及关于合法同意的构成要件，在面对不同的主体时适用不同的认定条件。在能够作出同意的主体范围上，并不仅限于自然人，在欧洲委员会网络犯罪委员会关于第 32 条的讨论报告中，也都包括了机构法人作为同意主体的情况。在不同的同意主体如何达成合法同意的条件上，当同意的主体为自然人时，一般认为其应为有能力作出同意的人，且同意行为与同意披露的内容不能为其所在地国内法所禁止的内容。根据有些国家的国内立法，未成年人或精神病人可能就无法成为有能力作出同意的适格主体。²⁹当作出同意的主体为服务提供商时，其所需要满足的条件则更为复杂，即需要满足《通用数据保护条例》中的规定，又要符合服务商所在地国内法的规定。³⁰

（三）困境与挑战：规范的欠缺与新技术的不断出现

显而易见，上述的两种跨境调取电子数据的方式相较于司法协助，程序简洁，沟通直接，在调取效率上有了较大的提升，但区别于司法协助在主体、程序以及权责上都有国内法及条约的明确规范，无论是

²⁹ Cybercrime Convention Committee, *Trans-Border Access to Stored Computer Data under Article 32 of The Budapest Convention on Cybercrime and Extraterritorial Powers*, <https://www.eurojust.europa.eu/sites/default/files/assets/trans-border-access-to-stored-computer-data-under-article-32-of-the-budapest-convention-on-cybercrime-and-extraterritorial-powers.pdf>, last accessed 30/12/2023.

³⁰ Cybercrime Convention Committee, *Trans-Border Access to Stored Computer Data under Article 32 of The Budapest Convention on Cybercrime and Extraterritorial Powers*, <https://www.eurojust.europa.eu/sites/default/files/assets/trans-border-access-to-stored-computer-data-under-article-32-of-the-budapest-convention-on-cybercrime-and-extraterritorial-powers.pdf>, last accessed 30/12/2023.

直接向网络服务提供商提出跨境取证需求还是单方获取数据,都欠缺法律上的明确规定,这也是这两类手段在应用上产生的主要问题及根源所在。

直接向网络服务提供商提跨境取证据需求首先要面对的就是网络服务商向境外执法机构披露数据是否合法的问题,一方面,网络服务商并没有配合境外执法者的义务,另一方面,披露数据与保障用户隐私与数据之间存在冲突。其次,由于欠缺统一的规范,执法机构难以提出有效的取证需求,提出的需求是否顺利反馈完全取决于网络服务提供商,执法机构在面对提供模版或专门沟通网站的大型服务商时,对跨请取证的成功率尚且存在较高的可期待性,而在面对没有提供模版或专门处理部门的小型服务商时,对调取成功与否则完全无法预测。此外,欠缺统一规范在紧急披露请求中引发了另一突出问题,即关于“紧急情况”的界定不明的问题,这使得执法机构在获取与网络服务提供商的迅速联络以及快速提出符合服务商认可的请求上困难重重。

单方获取数据则一直面临极大的主权与管辖权的争议,我国对经同意直接获取数据一直持反对立场,认为这实际上是一种跨境行使管辖权的取证行为。³¹且其虽然有《网络犯罪公约》第32条作为依据,但实际上,第32条只是粗略地规定了方式,而没有对其中涉及的具体内容作出规定或解释,经同意直接获取或保存数据中关于“同意”的界定与条件不明,各国的实践也各不相同。³²

³¹ 《中国代表团出席联合国网络犯罪问题专家组首次会议并做发言》, http://vienna.china-mission.gov.cn/chn/hyyfy/201101/t20110128_8858969.htm, 最后访问时间2023年12月25日。

³² Cybercrime Convention Committee (T-CY), Transborder access and jurisdiction: What are the

除了明确规范的欠缺之外，直接向服务商提出数据需求与单方获取数据同样也面临信息领域新兴技术所带来的挑战。“阅后即焚”的加密技术 (End-to-End Encryption)、点对点网络 (Peer to Peer Networks) 的兴起以及虚拟私人网络 (Virtual Private Network)、网络代理商 (Proxy Server) 以及云端 (Cloud) 技术的应用，加剧了电子数据位置的不确定性与分段性，也就使得执法当局通过跨境公共资源搜索以及直接获取数据的手段获取电子数据愈发困难。³³

三、G20 反腐败追逃追赃研究中心的功能重构——推广替代性跨境调查取证手段

正如上文所述，G20 追逃追赃案件中跨境调取电子数据惯用的司法协助手段因程序繁琐等原因效率较为低下，另一方面，当下电子数据跨境调取方式的新尝试，即直接向服务商提出跨境取证需求与单方获取电子数据两类方式虽然在效率上得到了极大的提升，但在 G20 追逃追赃跨境取证中应用不足，且仍面临着缺乏法律依据与新技术的挑战等等问题。作为具有专业人才储备、承担成员国间反腐败追逃追赃工作交流的 G20 反腐败追逃追赃研究中心，应当发挥现有优势，在当前尚未形成更加适应电子证据取证特点的国际司法协助协议的情况下，向成员国推广司法协助以外的替代性跨境电子证据调取方式，对电子数据种类与跨境取证具体流程提供技术辅助及法律查明、为各国提供单点联络机制及促进成员国间合作与签署协议，全方位重塑

options? p. 38, <https://rm.coe.int/16802e79e8>, last accessed 13/12/2023.

³³ Internet Organised Crime Threat Assessment, Internet Organised Crime Assessment (IOCTA) 2023, p. 6, https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf, last accessed 13/12/2023.

G20 研究中心在促进成员国追逃追赃的跨境电子数据调取中的功能, 帮助提高 G20 追逃追赃案件中电子数据跨境调取成功率。以下将分别论述这四种功能的具体内容。

(一) 教育推广功能: 推广司法协助以外的其他跨境取证手段

G20 追逃追赃案件中跨境电子数据调取过于依赖程序繁琐的司法协助手段, 提高电子数据调取的效率, 首当其冲地, 就是要改善目前单一路径依赖的问题, 2020 年的《二十国集团领导人利雅得峰会宣言》(以下简称《利雅得宣言》) 以及 G20 反腐工作组《2022-2024 反腐计划》(*Anti-Corruption Action Plan 2022-2024*) 等对此也强调 G20 未来应积极推动应用非正式手段以提高跨境取证的效率。³⁴故此, 研究中心应当发挥教育推广功能, 向成员国推广介绍有关电子数据跨境取证的新方式、分享当中的优秀案例以及促进成员国侦查机关与互联网服务提供商之间的沟通。

在介绍各种取证方式及其注意事项上, 可通过编写指南、成立取证方式推广工作坊及制作相关网上教程的方式, 对直接向网络服务商提出需求及单方获取数据的一般方式、程序、涉及的电子数据类型、服务商类型及要求、时效及其注意事项等等展开具体介绍。

除了介绍方式, 分享具体的优秀案例可进一步帮助成员国学习新

³⁴ 《二十国集团领导人利雅得峰会宣言》, https://www.mfa.gov.cn/web/gjhdq_676201/gjhdqzz_681964/ershiguojituan_682134/zywj_682146/202011/t20201123_9383352.shtml, 最后访问时间 2024 年 3 月 3 日; G20 Anti-Corruption Working Group, *Anti-Corruption Action Plan 2022-2024*, https://www.unodc.org/documents/corruption/G20-Anti-Corruption-Resources/Action-Plans-and-Implementation-Plans/2021_G20_Anti-Corruption_Action_Plan_2022-2024.pdf, last accessed 03/03/2024.

的跨境调取电子数据方式以及如何完善司法协助程序。事实上，G20 成员国之间的对非正式手段的应用程度并不一致，有些国家之间的应用已经较为成熟，例如英、美两国，已通过《英美电子数据访问协议》(Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime) (以下简称《英美协议》)，赋予双方直接向对方国家境内服务提供商提出跨境取证需求的法律依据。³⁵《英美协议》规定了数据调取令、保存程序以及用户信息程序三种取证方式，截至 2023 年 7 月，英国已通过《英美协议》向美国境内的网络服务提供商提出了 7000 逾份数据需求，《英美协议》在两国跨境调取刑事电子数据上成绩斐然。³⁶G20 研究中心可对类似英、美两国的成功尝试展开分享，邀请两国执法人员与网络服务商，分享三种取证方式的具体运行以及他们目前实践当中面临的主要问题，帮助成员国系统性学习了解跨境调取电子数据新方式的展开可能及注意事项。

另一方面，跨境电子数据调取并非侦查机关纯粹的单方行为，即便在单方获取电子数据这一方式当中，单方所强调也是无需他国当局或数据持有者参与传送的具体过程，但仍需获得数据所有者的合法同意；且电子数据相关的信息技术日新月异。故而，促进执法机构人员

³⁵ Remarks of Richard W. Downing, *The CLOUD Act: A New Model for International Law Enforcement Cooperation*, at the International Symposium on Cybercrime Response, Seoul, Korea, <https://www.justice.gov/media/1315386/dl?inline>, last accessed 20/01/2024.

³⁶ Remarks of Richard W. Downing, *The CLOUD Act: A New Model for International Law Enforcement Cooperation*, at the International Symposium on Cybercrime Response, Seoul, Korea, <https://www.justice.gov/media/1315386/dl?inline>, last accessed 24/10/2023.

与电子数据主要持有人的互联网服务提供商之间的沟通、对话与探讨是使执法机构了解电子数据的存在形式与发展情况、服务商在面对需求时的审查条件尤其是对“紧急情况”的审查标准等调取电子数据关键信息的必要需求。G20 研究中心可通过组织交流会，利用在《利雅得宣言》成立的 globE 反腐案件信息分享平台、³⁷国际刑警及 EGMONT 金融情报交换平台³⁸等在线平台展开交流沟通。

（二）跨境取证的法律查明及技术辅助功能

电子数据身负的技术性为具体取证带来了挑战，无论是司法协助程序面临的各国对于电子数据种类分类不一、在程序流转中翻译造成的误差、直接向服务商提出跨境取证需求以及单方获取电子数据中需要面临的法律风险，都需要提供进一步的技术支撑，才能使跨境调取电子数据的方式得以有效应用。G20 研究中心在此应当发挥法律查明与技术辅助的功能，为成员国提供各国相关的法规查明与解释、共享技术方法、协助成员国执法机构提出需求及开发成员国内通用的关于电子数据调取的申请模版等辅助，以帮助成员国在跨境追逃追赃案件中的关于电子数据的具体取证行为。

其一，提供法规查明及解释。正如前文所述，G20 成员国间对于电子数据的定义、分类以及保护方式存在诸多差异，这对成员国执法机构跨境调取电子数据造成了诸多不便。面对各成员国对电子数据不同的法律规定，帮助查明各国法规及解释是提出司法协助与其他调取电子数据方式的基础。G20 研究中心可设立专门网页，分类汇集各

³⁷ Official Website of globE, <https://www.globe.gov>, last accessed 01/03/2024.

³⁸ Official Website of EGMONT, <https://egmontgroup.org>, last accessed 01/03/2024.

成员国关于电子数据及其调取程序相关的法律规定、司法解释及判例的原文或链接；并对涉及跨境调取电子数据的关键规定，例如《网络犯罪公约》第二附加议定书及其条约国的国内法转化、美国《云法》及欧盟关于调取数据的《调取令和保全令条例》等，组织专家论证，编写相关的解释。

其二，共享跨境调取电子证据的技术方法，帮助执法机构更新与完善关于电子数据的调查技术。例如欧盟建立的开源工具平台 VIRTUOSO，专门用来分享收集及分析公共数据的方法及工具，以提高从公共资源中查找、选择和获取信息的效率，帮助进行数据分析及决策建议等。³⁹

其三，协助各成员国执法机构完善其司法协助请求及直接向服务商提出的跨境取证请求，使其符合被请求方的要求。各成员国在提出司法协助请求或直接向服务商提出的跨境取证请求时，对于需求的具体内容可咨询 G20 研究中心，例如所需电子数据在被请求国的分类、提出的渠道、涉及的程序以及应当提供的说明内容等。

其四，开发成员国之间通用的电子数据需求提出模板。除了直接协助完善提出的司法协助或直接向服务商提出的跨境取证请求，通过开发有关调取电子的申请模板也可高效提高需求完成的效率。根据部分网络服务商提供的需求模版及现有经验，数据需求一般需要包括请求机构的名称、基本案情、要求披露的数据及其法律依据、披露数据的必要性与合目的性理由、相关的用户及本案程序、是否有法庭出

³⁹ Official Website of Versatile InfoRmation Toolkit for end-Users oriented Open Sources exploitation, <https://cordis.europa.eu/project/id/242352>, last accessed 23/01/2023.

具的调令等等，具体模板详见下图。⁴⁰

⁴⁰ 参照天狼星项目与联合国毒品和犯罪问题办公室（United Nations Office on Drugs and Crime）、联合国反恐怖主义委员会执行局（United Nation Counter-Terrorism Committee Executive Directorate）、欧洲司法网络（European Judicial Network）和欧盟执法训练局（European Union Agency for Law Enforcement Training）创建的标准化申请表格（Standardised Model Forms）Eurojust, SIRIUS EU Digital Evidence Situation Report (2021), p.66.

在此输入请求机构的名称			
在资源的基础上要求披露提供数据			日期:
请求机构:			
详细信息			
全名或个人身份识别号码		职位	
当局代表联系方式			
官方电子邮件地址和电话号码			
诉讼程序编号			
案例编号		以前的请求编号	
收件人地址		地址	
<p>该权威机构正在进行涉及来自您平台的一个或多个用户的刑事调查。电子数据已被认为与此事有关。我特此要求自愿公开有关以下所述用户) 和/或账户的电子数据。为响应此请求而提供的任何和所有信息或数据将仅用于所述调查，而不会向未经授权的人员披露。</p>			
案情			
附件			
要求自愿披露数据			
<p>本模型表格由联合国毒品和犯罪问题办公室，联合国反恐怖主义委员会执行局、欧洲刑警组织（通过欧洲司法与欧洲警察的小天狼星项目）提供。这些机构没有审查义务，也不对这一要求的内容负责。在提出和处理任何请求时，您有遵守有关数据分类和隐私的相关法律和程序的责任。</p>			
法律依据			
国内法律程序			
<p>如果服务提供者要求，请根据贵国的法律规定，附上所需数据的国内法律程序</p>			
详细文件 附件			
有关的用户或账户			
详细文件			
附件			
请表明您之前是否提交了账户的数据需求			
信息要求:			
<p>此请求适用于以下指定的项目，无论是电子形式还是其他形式，包括存储在备份介质上的信息。以下是要求披露这些数据集的正当理由。</p>			
提供全名		账单信息/付款方式	
假名、昵称或登陆名称		账户的开始日期和结束日期	
用户ID		账户状态	
电话号码		注册ip地址、包括时间戳	
有点地址		关联设备（包括设备ID、IMEI MAC地址和可用的UDID）	
出生日期			
订阅用户的身份证或护照复印件			
登记类型、合同副本、登记时的身份核查方式、认购人提供的文件副本			
与用户/订阅人身份有关的任何其他信息			
针对注册机构和注册商:			
指定域名的注册人、技术和管理名称、地址、电话、传真号码和电子邮件地址			
指定域名的创建、更新日期、当前状态和名称服务器			
其他信息			
流量数据			
IP地址日志，包括时间戳		消息日志和聊天日志	
活动日志/日志文件，包括时间戳			
路由信息（源 IP 地址、目标 IP 地址、端口号、浏览器、电子邮件标题、信息 ID、数据传输量、从账户发送或接收的任何电子信息的来源或目的地）			
加密货币地址			
其他信息			
其他数据			
理由，包括必要性和相称性:			
时间段/阶段:			
保密性:			
<p>我请求贵方不要向用户或任何其他人披露本请求的存在，除非是为遵守本请求所必需。如果遵守本要求可能导致永久或临时终止对帐户的服务，或采取以其他方式提醒帐户的任何用户注意您披露上述信息的行动，请在采取行动前尽快与我联系。</p>			
如有法庭命令，请附上			
如适用PDG公匙，请附上			
所附文件摘要:			
<p>如对本申请有任何疑问，请与我联系。 我特此证明，我拥有提交此申请的合法授权，并且就我所知，所提供的信息均属实。</p>			
		签名 盖章 电子签名	
<p>插入签名和印章作为图像，然后以电子方式签署文件； 或打印手动签名和盖章的文件，请使用黑色或蓝色钢笔。</p>			

(三) 构建跨境调查取证的单点联络机制

帮助成员国在追逃追赃案件中跨境调取电子数据的具体取证行为，除了提供技术支撑与法律查明，G20 研究中心作为专业人才交流平台，可为成员国提供机制性的辅助，构建单点联络机制，负责处理审核成员国之间的电子数据调取请求以及处理请求的接受、转发服务商的回复等。所谓单点联络机制，即由具有专门知识的执法人员集中处理跨境电子数据调取请求或在这一过程中提供支持，单点联络机制主要包括两种运行形式，一种是用于集中处理请求的单点联络机制，另一种是用于知识共享和支持请求的单点联络机制。⁴¹

从欧盟已有的实践效果来看，单点联络机制的运行有利于提高执法当局提出的需求的质量，能够保证需求的合法性以及与网络服务提供商联络的渠道和方法的正确性；且其降低了执法当局了解不同网络服务商披露数据的程序与政策的成本，使得调取数据的过程更为快捷。另一方面，单点联络机制的运行便利了跨境追逃追赃相关统计数据的收集，有助于分析利用网络进行的犯罪趋势。⁴²

本文此处所提之 G20 研究中心应当构建的单点联络机制，属集中处理型单点联络机制。在单点联络机制的构建上，G20 研究中心以中心研究人员为基础创建中心单点联络机制，并可进一步促进成员国当局指定已有经验或具备相关知识的执法人员成立国内的单点联络点，与研究中心对接。在具体运行上，执法部门将数据披露请求统一发送给研究中心构建的单点联络点，单点联络点审核该请求是否符合

⁴¹ Eurojust, SIRIUS EU Digital Evidence Situation Report (2020), p. 55.

⁴² Eurojust, SIRIUS EU Digital Evidence Situation Report (2020), p. 56.

请求国及被请求国的法律和政策，而后通过所请求之网络服务提供商所认可或指定的渠道，按照其所要求的格式和需求发送给网络服务提供商。网络服务提供商向单点联络点提供所请求的数据或反馈意见，单点联络点再把网络服务提供商的回复转发给执法部门。

（四）促进跨境取证合作及协议签署功能

司法协助程序的繁琐以及新的取证方式在法律依据上的欠缺，实际上是上是系统性的问题，无论是简化司法协助的程序，抑或是为其他调取电子数据的方式提供法律依据，均需要 G20 成员国之间达成一致，签订具有规范效力的法律文件。⁴³G20 研究中心作为既有的交流平台，自然应当承担促进成员国间就追逃追赃案件中跨境调取电子数据相关事项的合作及相关协议签署的功能。根据目前司法协助存在的问题、推广非官方的新取证方式的需要，以及《二十国集团司法协助高级别原则》中构建及时回应工作重点的机制与促进各国通过其他机制的交流的规定，⁴⁴合作的展开与协议的签署主要应当围绕着优化司法协助流程、赋予成员国境内网络服务商向成员国执法机构披露数据以及建立紧急情况的数据保全制度这三方面展开。

其一，促进各成员国就追逃追赃专门事项签订相关的电子数据跨境调取司法协助条例，优化现有的流程。例如针对反腐追逃追赃案件的司法协助程序的期限作出明确规定，当涉及紧急情况时，期限应进一步缩短；推行司法协助的电子化，尝试构建司法协助电子平台，在

⁴³ 罗斌：《反腐败国际合作：追逃劝返制度的规则构建》，载《东方法学》2019 年第 6 期，第 152-158 页。

⁴⁴ G20 High-Level Principles on Mutual Legal Assistance, <https://www.oecd.org/g20/topics/anti-corruption/High-Level-Principles-on-Mutual-Legal-Assistance.pdf>, last accessed 30/01/2024.

线处理与传达需求及回复；⁴⁵促进司法协助程序前的沟通，进一步缩短司法协助所需要的层层审核与传达时间；构建司法协助与其他非正式取证方式的配合机制，明确可适用非正式取证方式的情况下应当优先适用非正式取证方式，以及通过非正式方式获取的电子数据可成为司法协助提出需求中的有力材料，帮助司法协助的达成。

其二，促进各成员国为打击严重腐败案件的目的，允许其本国的互联网服务提供商向其他成员国的执法机构提供电子数据。就严重腐败的定义与适用的案件范围作出明确规定，例如从案件标的、作案方式等方面划分界限；对于涉及严重腐败案件中的电子数据形成类型化共识，在类型化的基础上区分披露方式、披露程序及披露的期限和其他注意事项，使网络服务提供商披露数据与国内法及成员国参与的国际条约对网络服务提供商义务尽可能不发生冲突。

其三，促进各成员国就在紧急情况下的跨境电子数据保全及提供机制达成共识。促进各成员国对“紧急情况”形成共识，具体可借鉴欧盟在《调取令和保全令条例》中的定义——“对个人生命或身体完整性或者关键基础设施存在立即威胁的情况”⁴⁶。对紧急情况下可保全或提供的电子数据类型、保全及提供数据的主体与程序、处理的时效以及保全的期限作出明确规定，紧急情况下的处理时效应显著短于一般情形，具体时效的确定可参照欧盟规定个时效，即 8 小时内的回

⁴⁵ 冯俊伟：《数字时代跨境刑事取证制度的转型》，载《地方立法研究》2022年第4期，第18-31页。

⁴⁶ Article 2(a) of Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection

复时效与被请求方拒绝时 96 小时的拒绝时效。⁴⁷建立紧急情况下的电子数据保全在跨境取证启动前与取证过程中双重运行机制,以应对电子数据的毁损灭失风险。此机制指在适用取证过程中的电子数据保全基础上,引入适用于跨境取证启动前的电子数据保全程序,形成电子数据在取证前及取证中可双重保全的机制。这一取证前保全程序的引入主要参考《网络犯罪公约》第 29 条所规定的一种针对紧急情况的快速保全程序,所谓快速保全程序,是指有数据调取需求,但在正式数据调取程序开始前,面临证据在后续程序中存在灭失、伪造、变造、藏匿或其他难以取得的情形时,可请求数据所在国当局保存数据。⁴⁸取证前保全程序为正式取证中的电子数据的保全与获取提供条件,取证中的数据保全与调取是取证前保全的启动前提,双重保全机制的运行有利于对抗电子数据毁损灭失风险,提高取证的成功率。

四、结语

面对当前日新月异的腐败犯罪方式及转移资产的手段, G20 跨境追逃追赃显然需要方式与技术上的全面革新。电子数据在案件调查中的重要地位已无须多言,其对传统跨境取证方式带来的结构性冲击亦是无可避免,替代性取证方式的适用一定程度缓解了司法协助存在的效率问题,但法律依据的欠缺与面对新兴技术的无力仍是不得不考虑

⁴⁷ Para (56) of Regulation (EU) 2023/1543:

The European Parliament and The Council, Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543>, last accessed 31/01/2024.

⁴⁸ 《网络犯罪公约》第二十九条, <https://rm.coe.int/quets-185-and-expl-rep-chinese/1680a39f77>, 最后访问时间 2024 年 3 月 3 日; Council of Europe, Explanatory Report to the Convention on Cybercrime, 2001/11/23, p.50.

的问题。本文所论述之 G20 研究中心的功能重建，试图以当前世界尝试的替代传统司法协助取证途径的主要替代性跨境调取电子数据方式为基础，构建一套适用于 G20 反腐追逃追赃案件中跨境调取电子数据的新体系，但其中涉及的细节、有效性论证以及风险应对的具体展开，均有待进一步研究补充。