

数字时代刑事侦查公私合作研究

王志刚*

内容提要 数字技术的发展和犯罪形态的变化催生了刑事侦查中的公私合作,但其法治化程度有所不足。实践中,刑事侦查中的公私合作大致可以分为义务型、契约型和边缘型合作。刑事侦查公私合作对现行程序法治的冲击主要体现在权力配置合法性缺失、权力运行控制弱化和诉讼结构中的控辩失衡。对此,可通过重塑合法性根基、建构运行过程控制体系和确立权利保障机制三个方面作出制度回应,系统解决刑事侦查公私合作中的权力行使合法性、审批程序、过程监控、控辩平衡、监督与救济等问题,将技术效能纳入程序法治的可控框架。

关键词 刑事侦查 公私合作 合作型侦查 第三方技术协助 程序规制

目次

- 一、引言
- 二、数字时代刑事侦查公私合作的实践形态
- 三、数字时代刑事侦查公私合作的法治困境
- 四、数字时代刑事侦查公私合作的制度回应
- 五、结语

* 重庆邮电大学网络空间安全与信息法学院教授。本文系 2023 年度国家社科基金西部项目“数字时代刑事侦查权的规范化行使研究”(项目批准号: 23FX030) 的阶段性成果。

一、引言

随着大数据、人工智能等数字技术在犯罪治理中的全方位渗透,以往侦查权封闭运行模式开始被打破,越来越多的公私合作^①模式开始使用。这种合作型侦查在应对数字时代犯罪治理结构变化,有效打击网络犯罪、提升侦查效益中起到了积极作用,但不可忽视的是,当前刑事侦查的公私合作同样对传统的侦查法治体系造成冲击:一方面,传统侦查权专属原则的边界逐渐淡化,其权力行使表现出开放协作的特征;另一方面,科技企业等私人部门在侦查领域的进入,使得以权力制约、权利保障和程序理性为主要内容的程序法治正受到技术实用主义的冲击。

传统公法理论遵循“公法不得由私人协议变通”的规则,强调公权行为的不可契约性。但随着国家角色从秩序维护者向服务提供者转变,出现了“契约行政”,即在执行公共任务时采取私法手段,其本质是承认此种行为以私法方式存在但仍须受公法基本原则控制,必须在依法行政的框架内运行。^②如,美国传统上将包括刑事诉讼等“政府固有职能”列为外包禁区,^③而近年来关于政府固有职能的清单又开始弹性化。特别是在网络安全治理领域,美国实际上已陷入一种公私网络安全体系之中,其特点是私人部门在关键网络安全问题上扮演着重要且近乎政府性的角色,而联邦政府在某些情况下更像市场参与者而非传统监管者。^④公私边界的模糊引发了社会公众对政府权力边界和公民权利保障的普遍担忧。^⑤

应当承认,在数字技术快速发展的今天,公私合作的出现与快速发展有其时代背景和现实必要性。人类社会正面临深刻的数字化转型,社会系统结构与功能的深刻变化,远远超出传统社会系统的复杂性。^⑥随着技术在国家治理中的深度融入和信息技术的深入发展,国家的有效治理越来越依赖技术公司与技术精英,国家权力的行使也越来越趋向多元主体协同。^⑦传统封闭式的公权力运行模式,确实无法有效应对当前社会治理中

① 本文所提出的“公私合作”,是指在侦查活动中,公权力机关与私人部门之间为完成特定任务而进行的协作。其中,“公”主要是指依法行使侦查权的国家机关;“私”主要指各类企业、技术服务的提供者以及相应专业技术人员等非公权力主体,也包括承担公共网络服务职能的国有企业,如无特指之处,本文以“私人部门”统称。

② 参见陈军:《冲击与发展:契约行政与依法行政关系之检视——透过公私合作视角考察》,载《华南理工大学学报(社会科学版)》2015年第2期,第65页。

③ 参见黄润秋:《论“政府固有职能”对美国合同外包的约束》,载《行政法学研究》2012年第3期,第116页。

④ See Kristen E. Eichensehr, *Public-Private Cybersecurity*, *Texas Law Review*, Vol.95:467, p.467 (2017).

⑤ See Danielle Keats Citron & Jeff Stautberg, *Public-Private Partnerships After Murthy v. Missouri*, *Indiana Law Journal*, Vol.100:791, p.806 (2025).

⑥ 我国学者从三个方面分析了数字化时代对社会系统进行调控的复杂性:一是社会力量和市场主体借助数字网络和平台更加广泛地参与社会治理,治理主体更加多元化;二是数字时代社会行为方式的变革对传统的层级式调控带来冲击,治理模式和手段亟须现代化;三是公民意识不断增强,社会主体诉求复杂化,治理目标多样化。参见王芳、郭雷:《数字化社会的系统复杂性研究》,载《管理世界》2022年第9期,第213页。

⑦ 参见黄其松:《数字时代的国家理论》,载《中国社会科学》2022年第10期,第70页。

的复杂问题。在刑事领域,网络犯罪问题当前已成为各国侦查机关共同面临的沉重负担,面对案件受害人数量庞大、个体受损金额小以及犯罪手法复杂的状况,警方根本难以投入充足的时间、资源和专业知識全面调查每起案件。^⑧从发展趋势看,人工智能、机器学习的指数级增长更将从根本上改变网络犯罪形态,各类网络犯罪行为可以更快实施而更难调查。^⑨而私人部门的技术优势可以弥补侦查机关的资源和能力短板,刑事侦查中公私合作具有重大现实需求。

但是,刑事诉讼绝不仅仅是一种以查明事实真相为目标的认识活动,还包含着一系列诉讼价值的实现和选择过程。^⑩公私合作已远远超出单纯的技术辅助范畴,正在引发侦查权配置与运行模式的变迁,技术的专业壁垒使得第三方技术主体顺势进入侦查过程,引起从技术红利向司法红利转化中难以避免的侦查权扩张,^⑪第三方技术主体开始在一定程度上影响侦查进程,甚至成为侦查程序的主导者^⑫。上述现象显现出侦查权范式在数字时代的隐性重构,其突出特征是,在技术赋能背景下,国家垄断性权力的运行逻辑、作用方式与问责链条发生了深刻变化,致使程序失序风险加剧。基于此,本文对刑事侦查公私合作对程序法治的挑战与其中蕴含的机理进行分析,并在此基础上提出制度回应方案,以期将刑事侦查公私合作置入程序规制的轨道中。

二、数字时代刑事侦查公私合作的实践形态

从实践情况看,我国当前刑事侦查中的公私合作形态比较多元,学界从不同角度对当前的合作模式进行了区分,有学者聚焦数据提供义务,根据私人部门参与犯罪治理阶段的不同区分为犯罪或犯罪风险报告、调取中的数据提供;^⑬有学者从侦查协助内容的角度区分为数据留存、犯罪风险监测与报告、提供数据与技术支持以及数据披露;^⑭有学者从参与侦查场景的角度区分为数据信息供给、科技产品输出、技术支持协助以及综合协同治理;^⑮还有学者从合作样态角度区分为个案侦查协助、网络犯罪监控、联盟合作治理^⑯。上述区分虽然角度不同,但总体上可以分为义务型合作和契约型合作两种,实践中还存在着一些特殊形态的边缘型合作。

⑧ See Daniel Halpin & Sheri Todd, *Public-Private Collaboration for Combatting Cyber Fraud*, IUS Gentium, Vol.116:287, p.293 (2024).

⑨ See Thi Ha Do & Niloufer Selvadurai, *Future Crime: A Theoretical Foundation for Designing Effective Cybercrime Laws in the Age of AI and Ransomware*, North Carolina Journal of Law & Technology, Vol.27:91, p.103-108 (2025).

⑩ 参见陈瑞华:《刑事诉讼的法理》(上卷),商务印书馆2021年版,第37页。

⑪ 参见胡铭、张传玺:《大数据时代侦查权的扩张与规制》,载《法学论坛》2021年第3期,第7页。

⑫ 参见李训虎:《技术公司参与侦查检视》,载《政法论坛》2025年第5期,第93页。

⑬ 参见裴炜:《论刑事诉讼中网络信息业者的数据提供义务》,载《上海政法学院学报》2022年第6期,第64-65页。

⑭ 参见陈雨楠:《互联网企业的侦查协助义务:类型与边界》,载《中国政法大学学报》2024年第4期,第261-262页。

⑮ 参见周玥:《信息科技企业技术型参与侦查的程序风险及其规制》,载《中外法学》2026年第2期,第345页。

⑯ 参见黎晓露:《网络犯罪侦查公私合作的兴起及其法律规制》,载《犯罪研究》2024年第4期,第53页。

（一）义务型合作

义务型合作指网络服务提供者、科技企业等私人部门,依照我国《个人信息保护法》《网络安全法》《数据安全法》《反电信网络诈骗法》等法律法规所规定的义务,向侦查机关提供数据或进行技术支持和协助。实践中主要有三种形式:

一是数据提供与调取。这种是最常见的协助方式,侦查机关出具《调取证据通知书》等法定文书后,私人部门便会启动内部合规和安全审查程序,根据指定要求向侦查机关提供数据,通常包括用户实名注册信息、登录IP和日志、通信关系链和群组信息、交易记录、云存储内容以及关联设备信息等。但现有法律法规对私人部门设置的协助义务较为宽泛和笼统,缺乏明确的标准。《个人信息保护法》《数据安全法》虽确立了个人信息处理、数据调取的必要性原则,^{①⑦}但对“必需的范围与限度”“侦查犯罪的需要”等概括性描述缺乏进一步界定。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》中要求侦查机关“全面、客观、及时”地进行数据调取,同时也要求检察院和法院对电子数据的关联性进行审查,^{①⑧}但并未明确具体审查标准。实践中侦查机关出具的调取文书对数据范围的描述往往具有较大弹性,私人部门虽然能通过内部法务团队对侦查机关的证据调取进行形式审查,但也难以对调取文书所提及的必要性与关联性作出判断,侦查机关经常存在笼统收集、处理电子数据的情况,^{①⑨}而私人部门则面临必要协助与过度提供之间的平衡困境。

二是数据格式处理。这类工作实际上是数据提供的附随义务,因为提供数据并非简单输出,私人部门还承担着目标数据格式化、完整性保障的义务。这通常包括:第一,格式转换,即将内部存储的原始数据,如特定的数据库格式、日志格式等转换成侦查机关能读取分析的通用或专用司法格式,且转换过程可追溯、无篡改。第二,对电子数据进行完整性校验和说明。即在电子数据提交时,对每个哈希值、时间戳、数据来源和提取都予以校验和说明,以此证明电子数据的完整性与真实性,满足证据链条的需求。但由于现阶段不同公司之间的数据结构差异巨大,没有统一的司法数据交付标准,所交付的数据质量参差不齐,客观上增加了侦查机关后续鉴证的难度与成本。

三是特定情形下的技术协助。我国法律法规设定了私人部门在特定情况下向侦查机关提供技术协助的义务,如《网络安全法》第30条要求网络运营者为侦查机关侦查犯罪的活动提供技术支持和协助,《反电信网络诈骗法》第25、26条分别为互联网服务提供者设定了涉诈活动监测处置、案件侦办中的具体技术支持(含网络技术、产品的制作、维护服务)和普遍协助义务。据此,私人部门需要配合提供特定的技术协助,这也是义务型合作中干预性最强的部分。技术协助主要有以下两种:第一种是实时监控和快

^{①⑦} 参见《个人信息保护法》第34条、《数据安全法》第35条。

^{①⑧} 参见《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2条。

^{①⑨} 参见梁坤:《数据安全视域下网络服务提供者协助侦查取证的规范化》,载《中国人民公安大学学报(社会科学版)》2025年第3期,第29页。

速处置。在紧急情况下,如诈骗资金止付、阻止涉恐涉暴信息扩散等,私人部门根据侦查机关指令对某些账户、链接、内容采取实时监控、限制交易、封禁或删除等措施。第二种是提供技术接口与工具。私人部门需要给予技术支持以协助侦查机关依法采取网络监控、渗透测试等技术侦查措施,向侦查机关提供必备的技术接口或者专用工具环境等,帮助其执行相关法律法规,使相关措施能够落地到技术层面。这种协助方式很可能会直接触及用户利益,私人部门在被动应对指令时实际上代替侦查机关承担了合规判断风险。例如,侦查机关要求某互联网企业对某个涉诈账号立即采取封禁措施,但若没有明确封禁时间或封禁程度,那么在实操中,企业就要自己去判断。如果封的时间太短,达不到协助的效果,而若封的时间太久,则会侵害用户的合法权益。一旦判断错误,企业就会面临被用户起诉或者被监管部门处罚的风险。

(二) 契约型合作

契约型合作指侦查机关通过政府采购、项目委托等市场化方式,通过购买私人部门提供的专业技术服务以增强自身的侦查能力。该类合作建立在具有对价性质的商业合同基础上,在一定程度上突破了刑事诉讼法、网络安全法等公法所规定的义务框架,其内容渗透到侦查分析和研判各个环节之中,也是公私合作中较为活跃、争议较大的领域。契约型合作的实践样态呈现出体系化和深度化特征,主要包括:

一是技术平台和基础能力建设。这是最为普遍的合作形式,侦查机关通过联合实验室或直接购买大数据分析平台、云计算资源、专用硬件等方式,将科技企业的算力、算法与数据模型能力嵌入到侦查体系中。例如,上海市公安局长宁分局联合8家企业成立“长宁打击治理新型网络犯罪玄武联合实验室”,针对新型犯罪预警防范和打击治理进行深层次合作,企业派员入驻联合实验室与公安机关协同开展工作。^{②①}

二是专项技术服务的深度介入。此类服务直接作用于具体案件的侦查取证核心,具备高度专业化和精细化,在实践中主要有以下几种方式:其一是数据解密与恢复。面对越来越普遍的加密通信与应用,侦查机关经常会借助科技企业的破解能力进行破解,如通过流行加密通信软件提取数据,或者对采用高强度加密的涉案硬盘进行破解。其二是复杂网络数据分析与建模。如私人部门在电信网络诈骗、网络传销等涉众型案件中受托对海量、杂乱的电子交易记录、社交关系链、物流信息进行清洗、关联分析,并建立预测模型,输出嫌疑度排序和团伙结构图,实质上承担了部分情报研判职能。其三是线索的深度挖掘与生成。一些科技企业已不再局限于被动响应侦查机关的查询需求,而是主动挖掘自身数据资源,向侦查机关输出涉案线索。例如,腾讯公司的“守护者计划”依托自有平台的用户投诉、举报及异常信息数据,进行AI智能分析比对,筛查其中的黑产、欺诈信息后,由公司反诈骗专家分析研判并通过自研反诈系统联动警方,对诈骗团伙、链条进行打击治理。^{②②}

^{②①} 参见汪昊:《首家打击治理新型网络犯罪联合实验室成立》,载《上海法治报》2021年9月27日,第A5版。

^{②②} 参见陈姝:《科技防骗! 腾讯成立智能反诈中枢》,载《深圳商报》2019年8月7日,第A12版。

三是专家智力支持。私人部门的技术专家除了提供培训之外,还会以专家辅助人或者有专门知识的人的身份参与诉讼,出庭说明数据提取方法、分析结论的可靠性等,他们的意见能直接影响电子数据的采信情况。这也使得技术专家从幕后协助走向台前论证,其行为已经与司法证明紧密相连。

四是定制化工具开发。科技企业根据侦查机关的特殊侦查需求,有针对性地设计开发软件工具,在一定程度上帮助解决侦查中存在的难题并在某种意义上确立了侦查方法。侦查行为围绕这些工具的能力边界展开,形成了“侦查依赖产品,产品决定侦查”的深度融合状态,企业在某些场景中甚至起到主导作用。^②此外,由于双方合同中常包含“驻场服务”或者“技术支撑”条款,导致部分科技企业的技术人员可以长期、深入参与具体案件的侦查取证环节,甚至代替侦查人员对重要数据进行提取、恢复和分析。

(三) 边缘型合作

除了上述两种常见模式之外,实践中还存在三类特殊合作模式。这三类合作模式的法律地位未明,其内容缺乏实质性的法律授权,处于法律边缘的模糊地带,笔者称之为边缘型合作。

第一种是“案源经营”。网络犯罪“沾边就能管”的现状造成了侦查管辖权泛化,^③导致个别科技企业从侦查机关急于侦办经济案件压力^④中发现了“商机”。这些科技企业假借“主动防御”或者“威胁情报”等名义,利用技术手段或人力卧底等方式对暗网、特定社群等进行长期监控和信息采集,并将获取到的信息进行整合分析,形成从嫌疑人身份、作案手法、资金流向乃至证据材料都相对完整的“案件线索包”,然后有偿提供给侦查机关;或由科技企业提供线索并协助取证,侦查机关落地控人,之后根据最终的案件罚没所得进行“分成”获利。更严重的是,部分企业后续还会以专家辅助人的身份参与甚至主导电子取证工作,甚至以企业背景的鉴定机构出具鉴定意见,既充当专家辅助人,又充当鉴定人、见证人、报案人等多个诉讼参与人,使得这些科技企业同案件结果形成事实上的重大利益关系。^⑤

第二种是虚拟货币处置委托。在加密货币相关的犯罪中,由于虚拟货币具有匿名性、去中心化、跨国流动和价格高波动等特征,对虚拟货币进行先行处置是非常必要的。但是侦查机关目前在技术水平、操作渠道以及合规经验方面都存在短板,不能独立完成对侦查环节查封扣押的比特币、以太坊等虚拟货币的保管、变卖和处理。因此,侦查机关越来越多地委托拥有技术、资质的私人部门从事包括私钥安全托管、评估资产价值、划转到合适平台、兑换合规法币以及后续冻结和移交等各个环节的处置工作。由于没有统一

^② 参见前注^①,周玥文,第348页。

^③ 参见刘艳红:《以有利于被告解释对抗趋利性司法和执法》,载《中国刑事法杂志》2025年第1期,第64页。

^④ 例如,有的公安机关经侦大队在年度预算压力下,将打击网络虚假交易列为“重点项目”,把罚没收入返还比例写入考核指标,驱动侦查权向“能罚”“好罚”的案件倾斜。参见王天民:《“远洋捕捞”式司法中的管辖权异议问题审思》,载《厦门大学学报(哲学社会科学版)》2026年第3期,第156页。

^⑤ 参见刘品新:《论非法电子证据排除》,载《清华法学》2025年第3期,第84页。

标准,私人部门参与处置的方式多元,逐渐暴露出私人部门所存在的法律地位不明、逐利本质隐忧、准入资质较低且监管不足等制度性风险。^{②6}

第三种是司法鉴定人提前介入侦查。在侦查机关遇到复杂的技术问题时,除了通过内部技术力量和向科技企业采购服务之外,也经常会寻求技术专家提供技术支持。一些司法鉴定机构的鉴定人有可能早在案件开展初期就已经根据侦查机关的要求,直接参与关键电子证据的提取、固定及初步分析工作,如对加密设备进行解锁、对损坏的存储介质进行恢复或者针对某个特定应用程序进行后台数据提取等。由于这类技术支持往往仅基于内部沟通或非正式委托方式开展,相关参与的具体手段、获得的原始数据很少记录于《搜查笔录》《提取电子数据清单》等正式侦查文书中,即便侦查机关后续以补办《鉴定委托书》的形式,将鉴定人之前提取的数据转化成形式上符合法律规定的“司法鉴定意见”,但仍无法消除鉴定人角色混同带来的程序正当性疑虑:侦查人员参与刑事侦查基于法律授权,鉴定人参与刑事侦查基于专门性知识;前者是客观证据的收集者与证据收集过程的客观记录者,后者是意见性证据的生产者,同一案件中侦查人员与鉴定人具有角色单一性、身份排斥性。^{②7}若同一人员身兼侦查取证的“技术实施者”和检验诉讼证据的“中立鉴定人”双重身份,既不符合刑事诉讼法规定,又破坏了司法鉴定自身的独立性。

三、数字时代刑事侦查公私合作的法治困境

前述三类合作模式对现行侦查法治体系的冲击方式和程度有所不同。义务型合作以法定义务为基础,其风险点主要是程序执行虚化和程序控制失位;契约型合作以商业合同为纽带,其风险点主要是权力来源合法性模糊和责任归属不清;案源经营、虚拟货币处置委托、司法鉴定人提前介入侦查等边缘型合作则在侦查启动正当性、财产处分权边界、鉴定主体的中立性等方面造成更大的冲击。下面从权力配置合法性、运行过程控制与诉讼构造平衡三个维度进行分析。

(一) 权力配置的合法性困境

传统刑事侦查制度预设侦查权为国家专属、封闭行使的公权力。然而,三类公私合作模式以不同方式挑战了前述预设,当侦查权在形式上仍归属于国家、实质上却依赖私人部门技术能力运行时,其合法性基础面临挑战。

首先,义务型合作的合法性困境表现为实体法授权与程序法约束的脱节。从形式上看,这种合作具有合法性的外观。《网络安全法》《反电信网络诈骗法》等法律都规定了私人部门向侦查机关提供技术支持和协助的义务,但对于支持和协助的范围、方式、强度与限度均没有在法律中加以明确规定。因此造成了一种“半悬空”状况,侦查机关可以

^{②6} 参见龚炜博:《论涉虚拟货币犯罪第三方配侦行为适法性》,载《求是学刊》2025年第4期,第147-149页。

^{②7} 参见陈如超:《金析为证:大数据分析报告证据化的二元模式》,载《中国法学》2026年第2期,第153页。

援引上述法律要求私人部门提供技术支持和协助,但《刑事诉讼法》并未给出相应程序约束。也就是说,虽然法律赋予了侦查机关向私人部门寻求帮助侦查犯罪的权力,但没有同时规定该项权力的行使方式。正是由于授权的概括与约束的缺位,义务型合作在实体法上“有据可依”,而在程序法上却“无规可循”,它既不是刑事诉讼法预先设立的侦查行为,也未纳入特别法的程序框架之内,在制度层面处于模糊地带。

其次,契约型合作的结果造成了公法关系私法化运作的境遇。侦查机关通过政府采购、项目委托等市场化方式将数据建模、线索挖掘等侦查业务外包,并以《民法典》等私法作为合作的基本规范。由此带来的问题是,刑事诉讼法律关系是一种公法关系,它应当由公法而非私法规定。若一份商业合同可以决定侦查线索的来源、技术分析的方法甚至证据生成的路径,那么侦查权的行使就脱离了刑事诉讼法对侦查主体资格、权限范围和程序要求的规制,使得法律对侦查权设置的制度屏障在事实上被绕过。

最后,边缘型合作的合法性困境最严峻。三种形态的合法性缺陷有所不同,以下分别进行分析:

其一,“案源经营”存在侦查启动合法性问题。侦查启动是刑事诉讼的入口,如何实现侦查启动正当化关乎后续程序的合法性。我国以报案、控告、举报和自首等为主要来源的侦查启动机制具有共同的特征,即通过社会公众或系统内部输入的信息进行启动,而不是由私人部门经营“产出”。但是,“案源经营”使得侦查线索的来源、筛选、初步加工均由私人部门完成,且以商业对价的方式提供给侦查机关。这就意味着侦查启动的判断权被前移至私人部门手中,其依据自身的商业逻辑而非法律规定的立案条件去决定哪些信息值得提交、哪些行为值得侦查。如果侦查的方向和范围在制度起点上受到了商业利益的隐性塑造,那么侦查权的正当性便会发生偏移。

其二,虚拟货币处置委托存在侦查权与财产处分权关系错位的问题。刑事诉讼中的财产处分权往往由司法机关专属行使,正当性来源于法律对公权力的严格约束和程序控制。但在虚拟货币处置委托中,私人部门实际控制涉案数字货币的私钥,并可以决定何时以何种方式进行处置,这无疑代替了本应属于司法机关的财产处分权。虚拟货币具有较高的价值波动,选择处置变现的时机和方式本身就是一种实质性判断,若将处理虚拟货币的权限交给受商业利益驱动的私人部门来行使,则意味着财产处分这类公法行为脱离了刑事诉讼程序的约束框架。

其三,司法鉴定人提前介入侦查造成制度角色的错位。司法鉴定制度之所以具有正当性是因为它预设了一个基本前提:司法鉴定人应该是处于控辩双方之外的中立第三方,^{②⑧}他作出的结论之所以具有证据价值,在于他的立场超然、判断独立。但若同一人在侦查初期就已经以非正式方式参与了证据的提取和固定,而后又以鉴定人的身份对同一证据出具鉴定意见时,其在制度逻辑上便发生了错位:鉴定人不再是对既有证据进行独立检验的中立第三方,而是对自己前期取证行为进行自我验证的利益相关者。这种角色

^{②⑧} 参见《司法鉴定程序通则》第5条。

混同使得鉴定意见赖以存在的制度正当性根基遭受了挑战,无论鉴定意见的内容多么客观,法庭和辩方都不知道鉴定人所鉴定的究竟是证据本身的客观属性,还是鉴定人自身前期取证行为的正确性。

此外,在合作过程中一旦发生违法取证、数据泄露等情况,侵害行为的定性和追责也面临难题:侵害行为是侦查机关的职务行为,还是私人部门的商业行为?案件应该由刑事訴訟确认证据非法并启动国家赔偿,还是应当通过民事诉讼追究私人部门侵权责任?现行法律并没有给出清晰规则。这种情况下,权力行为的可问责性已经在制度层面提前消解,合法性之困从授权模糊延伸至问责不能。^{②⑨}

(二) 权力运行的过程控制困境

从实践情况来看,三类合作模式都以不同方式削弱了侦查机关对权力行使过程的控制能力,但其生成机制有所不同。

首先,义务型合作的控制性困境源于侦查机关和私人部门存在协助范围上的理解差异。侦查行为程序控制的制度基础来自法律对执行方式、范围和限度的预先规定,侦查机关如何执行、执行到何种程度一般都有相对明确的标准可循。但由于当前法律对电子数据相关性缺乏审查标准,侦查机关对于需要提取数据的范围并不明确,私人部门在履行数据提供义务时往往会依靠自己对数据分类、合规的理解来回应侦查机关的需求。因此,私人部门虽然“履行义务”却又承担着“范围裁量”功能。这种裁量权的事实转移,使得程序控制从一开始就脱离了侦查机关单方掌控。

其次,契约型合作的控制性困境来自决策与执行的功能性分离。从法律形式来看,侦查程序的决定权依然在侦查机关手中,如启动侦查、确定方向、签发文书等仍由侦查机关掌握。但一旦科技企业以提供科技侦查软硬件、数字技术服务等方式介入侦查活动,技术平台深度嵌入侦查体系、算法模型成为线索来源、定制化工具限制取证路径时,执行环节已经变相让渡给了私人部门。也就是说,侦查机关可以决定调取哪些数据、采用何种算法,实际上却无法控制数据交付的质量,也难以审查模型的训练偏差和可靠性。于是,便形成了一种“前台决策、后台执行”的分离结构:前台(侦查机关)享有法定权限,后台(科技企业)掌握实质操作;前台承担法律责任,后台主导证据生成。这种分离,使得侦查机关难以对取证过程实时把控与全程把关。

最后,边缘型合作的控制性困境来自程序环节的行为隐匿。在“案源经营”模式中,侦查启动的线索源于私人部门的前期监控、情报加工等,而这一阶段信息的收集、筛选和整合完全游离于侦查程序之外。当侦查机关接手该案件时,所面对的是已被商业逻辑进行预处理后的“案件线索包”,无论其原始状态还是加工过程都无从追溯。在虚拟货币处置委托模式中,涉案资产的私钥托管、跨平台划转与变现处置均由私人部门在商业渠道中完成,整个操作过程同样缺乏与侦查程序的制度衔接;在司法鉴定人提前介入侦查模式中,鉴定人则在正式接受鉴定委托之前即参与取证,其前期操作过程的技术手段、数

^{②⑨} 参见高童非:《数字时代司法责任伦理之守正》,载《法制与社会发展》2022年第1期,第155页。

据范围与实施过程都不会载入正式的侦查文书中。上述三种边缘型合作模式下,侦查权运行中线索形成、先行处置、证据生成皆通过商业合同、内部沟通或非正式委托完成,由此从刑事诉讼法所设计的程序框架中脱逸出去,即便侦查机关有意对其进行过程控制,也因为控制对象的程序外移而难以实现。

(三) 诉讼构造的控辩失衡困境

侦查机关通过公私合作实现的能力跃升显著增强了控方指控犯罪的能力,但辩方的权利保障却没有相应跟进,由此造成诉讼结构上的控辩失衡。

首先,义务型合作为控方提供了单向的、强制性的数据获取渠道。侦查机关依照相关法律规定就能快速调取各种数据,但对于辩护律师而言,无论是自行取证,还是申请调查取证,都存在现实困难。2013年6月颁布的《中华全国律师协会律师办理电子数据证据业务操作指引》中虽然列举了律师开展电子数据证据取证工作的方式及要求,^⑩但这类指引只是指导建议或行为参考,并无强制约束力。实践中,辩护律师的取证诉求经常被私人部门以“涉及用户隐私”“属于公司商业秘密”或者“需经侦查机关同意”等理由拒绝。辩护律师申请调取证据的效果也不乐观,控方通常仅向法院提交筛选的部分电子数据,而将包含海量原始记录的完整数据排除在外,此时,即便辩护律师申请调取全部数据,也常因法院援引“涉及隐私”“数据过多”等理由而不予准许。^⑪可见,控辩双方获取证据能力之间的不对称使得辩方在诉讼的起点就处于不利地位。程序的平等武装和有效对抗是公正审判的基础,它意味着控辩双方在参与诉讼、影响裁判等方面具备实质对等的能力和机会。假如控辩双方在对抗能力上处于天生不平等状态,那么即便法庭审判环节形式上对等,也免不了弱肉强食的局面。^⑫

其次,契约型合作进一步将控方的数据优势转化为压倒性的指控能力。侦查机关委托私人部门运用专有算法对海量数据进行挖掘、建模,生成“诈骗团伙关系图谱”“资金流向研判结论”等技术分析报告,这类报告能否作为证据使用、作为什么证据使用本身在理论上就存在很大争议。^⑬辩方对此类证据的质证面临三重障碍:一是难以接触生成报告所需的原始数据集、算法参数及训练资料,无法审查数据清洗、分析的完整过程,其质证意见只能建立在经控方筛选后的片段之上,从而流于形式;二是即使获得部分技术材料,缺乏相应专业训练的律师也难以穿透其复杂逻辑,进行有实质意义的审查;三是公私合作场景下,证据的形成、筛选与分析往往经过多环节、多主体的处理,这一过程本身就存在较大的证据失真风险,而当指控最终依赖一个无法被解释内部推理路径的“算法黑箱”模型时,质证便失去了可供交锋的具体靶标。如此一来,法庭辩论便沦为辩方对控方单方技术输出的被动接受,有效辩护无从实现。此处还暗含着一项更为严峻的风险:在以数据结构驱动犯罪治理体系中,刑事诉讼归责路径面临着从“事实可查”向“标

^⑩ 参见《中华全国律师协会律师办理电子数据证据业务操作指引》第7.1条。

^⑪ 参见王志刚、刘言:《电子数据鉴定意见的认证困境与体系化应对》,载《证据科学》2026年第1期,第65页。

^⑫ 参见陈瑞华:《程序正义理论》(第2版),商务印书馆2022年版,第192页。

^⑬ 参见张中:《刑事证据制度现代化的中国标准与制度安排》,载《国家检察官学院学报》2024年第5期,第15页。

签已设”的结构转向,^{③④}裁判者面对复杂的技术性证据时,为了减少认知负荷,可能对看似客观的算法结论产生“盲从”,^{③⑤}从而剥夺了被告人获得公正、审慎审查的权利。

最后,边缘型合作对控辩平衡的冲击更为直接和难以修复。“案源经营”模式带来的直接问题是侦查启动的程序前环节对辩方完全不可见。刑事诉讼程序对侦查启动的规制旨在从源头上保障侦查权行使的正当性,而当侦查的入口实质上由私人部门的商业判断所预设时,上述制度安排在起点就被绕过了,即使辩方可以审查立案后的程序合法性,却无法知晓立案之前线索生成、筛选、加工等程序前环节。虚拟货币处置委托带来定罪量刑信息形成过程的制度外移。违法所得、经济损失是影响犯罪情节、衡量后果严重性的重要因素,而这与虚拟货币的价值认定存在密切联系,虚拟货币的变现时机或交易平台的选择不同,都会直接决定涉案金额,进而影响最终定罪量刑。若影响定罪量刑事实的形成环节脱离了刑事诉讼程序对财产处分的制度性约束,则辩方根本无法追溯为何此时变现、为何以这种方式变现等处置决策的合理性与合规性。司法鉴定人提前介入侦查则使得辩方的质证活动陷入实质无效的困境。当同一主体在侦查初期已参与证据提取,此后又以鉴定人身份出具意见时,辩方质证的逻辑前提便被瓦解,因为并不存在一个对证据形成过程保持中立超然立场的鉴定主体可供质询,无论是质疑鉴定过程,还是质疑取证过程,都指向了同一主体,要求该主体对自己前期行为的正确性作出评价,结论可想而知。

四、数字时代刑事侦查公私合作的制度回应

刑事侦查公私合作要走上法治轨道,合法性根基、运行过程控制与权利保障三个层面缺一不可,需要形成制度上的协同支撑。

(一) 合法性根基的重塑

对刑事侦查公私合作问题作出制度回应的首要任务是合法性根基的重塑,从而解决权力从何而来、边界止于何处、由谁参与并担责三个基础性问题。

1. 明确公私合作的刑事诉讼法依据

《刑事诉讼法》再修改时,建议在“侦查”一章中增设“第三方技术协助”专节,由该专节对公私合作的具体环节作出程序规定,从而在不影响“技术侦查”等既有制度的前提下,为公私合作设置专门的规范接口,主要包括:(1)启动环节。明确侦查机关向第三方提出协助请求应当通过《第三方技术协助申请书》,并附上初步证据、必要性说明等材料,使得公私合作的依据和边界清晰可辨。(2)审批环节。根据协助措施对公民权利干预的严重性,由不同机关实行差异化审批。(3)执行环节。要求侦查机关对协助方给

^{③④} 参见裴炜:《刑事诉讼数字化的逻辑演化与制度重构》,载《数字法治》2025年第6期,第34页。

^{③⑤} 参见[英]凯伦·杨、马丁·洛奇编:《驯服算法:数字歧视与算法规制》,林少伟、唐林垚译,上海人民出版社2020年版,第255页。

出具体的书面指令,并对数据查询和算法调用等重要节点进行强制性的实时日志记录,保证全程可追溯。

在此制度框架下,应该区分处理上述三种合作模式的合法性问题。对于义务型合作,应当厘清私人部门技术支持和协助的具体范围、方式与程序等内容,将当前过于原则化的授权转换为可操作的程序规则,使之脱离“有实体法依据、无程序法约束”的半悬空状态。对于契约型合作,任何涉及数据调取、线索挖掘等侦查关键环节的工作不得以商业合同代替法定程序,侦查机关只有获得法定授权后才能向私人部门提出需求。对于边缘型合作,“案源经营”和“司法鉴定人提前介入侦查”两种合作形式严重冲击刑事程序正当性,应予禁止。虚拟货币处置委托虽然有现实需要,但存在虚拟货币属性认定、跨境资产处置等问题,这些问题并非通过刑事诉讼程序本身就能解决,需由专门的实体法或特别程序立法予以解决。^{③6}

2. 限定公私合作的边界

首先,侦查机关凡需启动此类技术协助,都应以《第三方技术协助申请书》为载体,建立一套明确的必要性证明机制。申请书不能停留在概括性描述层面,而应要求侦查机关证明以下事项:一是案件实质关联性,即依托初步证据,说明拟采用的技术协助措施,无论是特定数据的调取,还是算法分析与已立案案件待证事实之间存在实质、具体、合理的关联。以此将第三方技术协助限定在“为查明案情所必需”的范围之内,防止侦查权借数据挖掘之名不当扩张。二是侦查手段的必要性,即在书面材料中说明,常规侦查方法在具体案件中存在哪些局限、哪些障碍,为何必须借助该技术协助才能达成侦查目的。通过这种方式,可与《个人信息保护法》中“必需的范围与限度”和《数据安全法》中“侦查犯罪的需要”等规定形成程序法配套衔接,^{③7}从而将概括性授权转化为可控边界、可供审查的刑事诉讼标准。

上述程序设计思路也有比较法上的参照。《德国刑事诉讼法》对“电讯通信监察”(第100a条)、“线上搜索”(第100b条)等措施不仅要求检察官申请、法官核准,更要求核准命令以书面形式详细载明措施相对人、犯罪事实、持续时间、资讯类型以及其对刑事程序的意义等内容,还需要详细叙明上述措施与个案相关的构成犯罪嫌疑的特定事实、措施必要性及比例原则的考量等事项。^{③8}《日本刑事诉讼法》第99条之2、第218条第1款建立了“附带记录命令扣押”,附带记录命令扣押处分对象是作为证据的必要电子记录(数据),所以法官在令状中必须记载应该记录或打印的电子记录范围,以及记录或打印该电子记录的人(第219条第1款),从而避免扣押大容量记录载体本身。^{③9}

^{③6} 如有学者建议由最高人民法院、最高人民检察院联合公安部、中国人民银行等部门共同制定《关于刑事涉案虚拟货币处置的若干规定》的司法解释,对虚拟货币的扣押、保管、变现等全流程作出具体规定。参见刘仁文:《刑事涉案虚拟货币处置的检视与完善》,载《中国应用法学》2026年第2期,第56页。

^{③7} 参见《个人信息保护法》第34条、《数据安全法》第35条。

^{③8} 参见[德]维尔纳·薄逸克、萨比娜·斯沃博达:《德国刑事诉讼法教科书》(第15版),程捷译,北京大学出版社2024年版,第653-654页。

^{③9} 参见[日]酒卷匡:《日本刑事诉讼法》,李子龙、唐春杨译,清华大学出版社2026年版,第139-140页。

其次,禁止以预防性监控作为程序开启依据。刑事侦查指向的是已经发生或正在发生的犯罪,不能扩展为对未来不确定风险的普遍筛查,更不能仅仅因为身份特征就限制或剥夺一个公民的合法权利。^{④①}法律有必要清晰划定禁区,避免将公私合作应用于与具体案件侦查无关的数据情报获取与研判,防止出现将侦查活动情报化而带来的对象弥散化、运行自动化、手段隐秘化、程序虚置化、个体同质化等一系列风险。^{④②}

3. 规范技术协助机构的准入管理

基于法定义务提供技术协助机构的主体资格无需专门规定,需要解决的是市场化主动提供技术协助服务机构的准入问题。解决这一问题,可借鉴司法鉴定机构的准入管理经验,将技术协助服务从市场化商业服务转化为诉讼辅助专门执业行为。

司法鉴定通过统一登记、名录管理、执业限制等前置规制,从主体适格性层面确保证据的合法性。参照这一逻辑,可由司法行政机关会同公安机关制定适用于侦查技术协助机构的统一准入条件,包括设备条件、人员资质、技术规范与保密义务,实施统一登记审核与动态名录管理。纳入法定协助名录的机构方可接受委托从事涉案电子数据的技术性辅助工作,未登记机构所形成的技术成果原则上不具备证据资格。在权责方面,技术协助机构除享有依约获酬等合同权利以外,还应当履行忠实执行指令、全程留痕报告、严格保密和数据安全合规等公法性义务。因技术协助行为造成侵权后果的,由侦查机关作为程序主导者对外负国家责任,确保相对人权利救济通道畅通。对于故意或重大过失造成侵权后果的技术协助机构及人员,依法追究其法律责任。

(二) 运行过程控制体系的建构

数字时代的侦查取证极为复杂,公私合作的场景也非常多元,很难设计一套单一的运行过程控制体系进行规制,如特雷佩尔在评述 Carey-Tamura 方法^{④③}时所指出,“没有哪个单一规则能够充分解决问题”,各种方案“各有其固有的优势,但也存在非常现实的缺陷”。^{④④}我国现行刑事诉讼法规定的过程控制体系主要围绕传统实物证据与言词证据构建,缺乏基于数据类型与权利影响的分类规制,难以适应数字时代差异化取证场景中有效侦查与权利保障的平衡需求。因此,有必要为其匹配差异化的程序要求。

1. 以权利干预强度为标准设定审批程序

作为程序控制体系的基石,审批环节至关重要,应以权利干预程度为标准设定不同的审批要求。之所以将权利干预强度作为分类标准,理由有三点:

一是体现比例原则的要求。比例原则要求公权力对公民权利的干预程度与审查密

^{④①} 参见陈永生:《大数据预测警务的运作机理、风险与法律规制》,载《中国法学》2024年第5期,第181-182页。

^{④②} 参见李训虎:《侦查情报化之批判》,载《法学》2024年第7期,第130-133页。

^{④③} Carey-Tamura 方法是将传统“文件混杂原则”用于计算机搜查的程序性规则,其目的在于防止数字搜查成为无限制的“通用搜查令”。该方法要求执法人员扣押含有大量混杂数据的计算机后不可自行全面审查所有电子文件,而应申请中立司法官员预先筛选哪些属于令状授权范围,即整体扣押、限缩搜查。

^{④④} See Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, Yale Journal of Law and Technology, Vol.10:120, p.133-135 (2007).

度成正比,干预越强,审批层级应当越高,程序要求也应当越严,这条贯穿公法的基本法理同样适用于侦查领域。来自特别法中的概括授权,如“必需的范围与限度”或“侦查犯罪的需要”本身都是程度性概念,不同场景下对其理解和把握自然也会不同,因而需要根据具体场景予以权衡。在不同案件的侦查取证中,第三方技术协助行为对公民基本权利的干预程度会存在明显差异,有的仅涉及非敏感数据的格式转换,有的则直接触及通信内容、行踪轨迹等核心私密领域,还有的可能通过算法分析生成直接影响定罪量刑的关键证据。如果对上述差异悬殊的行为适用同一审批程序,要么导致对低干预行为的过度规制而损害侦查效率,要么导致对高干预行为的约束不足而损害权利保障。

二是参照域外立法与判例实践。域外国家在侦查程序的制度设计中,普遍以权利干预强度作为配置程序保障的基准。《德国刑事诉讼法》规定线上搜索措施只能由检察官申请、法院合议庭核准才可实施,即便存在紧急情形,也必须由合议庭的审判长核准。而对于电信通讯监察措施原则上应由检察官申请后由法院核准,但紧急情况下检察官也可以自行核准。^④《日本刑事诉讼法》规定,侦查机关在逮捕嫌疑人的情况下,必要时可以在逮捕现场进行无令状搜查、查封、扣押(第220条第1款第2项、第3款);对于“附带记录命令的扣押”以及从通过电子通信线路连接的记录媒体进行复制(第218条第1款),则要求必须依据法官签发的令状执行。^⑤美国联邦最高法院关于“卡彭特诉美国案”的判决也提供了参考:过去视为元数据或者是第三方记录的信息类型在数字时代因聚合效应可能产生质变,进而受到更高层次的宪法保护。^⑥梅洛伊在分析此案时指出,之所以法院认定基站位置信息(CSLI)受到宪法第四修正案的保护,除了其本身极具揭示性的本质和执法部门获得这些信息后拥有的巨大权力范围外,最重要的原因就是它们的收集具有不可避免且自动生成的性质,用户无需经过任何积极同意,只要使用手机,就在持续不断地生成和分享这些信息。^⑦上述立法和判例的实质,都体现了以对公民权利产生影响的程度为标准设置差异化审批程序。

三是考虑实践中的可操作性。权利干预强度不是一个空洞的概念,而是具备实际判断和执行的指标。综合比较法经验以及我国司法实践,干预强度可以通过如下几个指标作出判断:第三方协助是否直接生成了定罪量刑的重要证据,该项协助是否涉及宪法或法律特别保护的私密领域,该项协助是否涉及大规模、持续性的数据分析。这三个指标分别代表着证据价值、私密程度与影响范围,其中任一方面达到高值就应当适用更严格的程序。这种框架既有明确的操作指向,又保留了必要的规范弹性,便于在案件中被侦查机关、检察机关或法院把握和判断。

^④ 参见前注^③,维尔纳·薄逸克、萨比娜·斯沃博达书,第653页。

^⑤ 参见前注^③,酒卷匡书,第133页。

^⑥ See *Carpenter v. United States*, 585 U.S. 296, 138 S. Ct. 2206 (2018).

^⑦ See John Melloy III, *I Agree: Why Society's Dependence on E-Mail in the Face of Non-Negotiable Terms of Service and Privacy Policies Requires Fourth Amendment Protections*, *George Mason University Civil Rights Law Journal*, Vol.34:261, p.262-263 (2024).

建议以权利干预强度的不同将第三方技术协助行为区分为以下三类,并设定对应的、层级清晰的审批门槛。

其一是关键证据生成型协助。这一类型是指直接产出影响案件事实认定关键证据的技术活动,如加密通信数据破解、特定算法模型对海量数据的关联分析并直接生成嫌疑人图谱或行为结论、对涉案设备进行深度数据恢复与解析等。此类行为直接塑造侦查心证,原则上应报请上级检察机关审查批准,并严格限定适用范围及授权期限。

其二是重大权利干预型协助。此类协助虽然不直接生成关键证据,但涉及对不特定多数人或特定对象大规模个人敏感数据(如行踪轨迹、通信记录)的调取与批量性分析。对此类协助,应设立内部审批机制,由设区市以上侦查机关负责人批准。这一层级的设定逻辑也可从相关制度动向中得到参考,如公安部2026年5月发布的《公安机关电子数据取证规则(征求意见稿)》第39条即作出规定,公安机关向互联网服务提供者调取电子邮件等个人通讯内容应当经地市级以上公安机关负责人批准。

其三是一般技术支持型协助。这类协助主要是指数据格式转换、非涉密环境的云计算资源提供、公开或低敏感度数据的初步整理等。此类行为技术性、辅助性强,权利干预性较弱,对其可适用一般的内部申请与备案流程。

2. 构建一事一授权的动态化过程监管机制

刑事侦查公私合作中的授权必须摒弃笼统的框架协议模式,而转向具体化、场景化的任务制授权,当前实践中普遍存在的概括性协助请求应予禁止,改为每次数据调取、每项技术协助均须单独授权,从根本上遏制必要范围被随意扩大。具体可从以下两方面着手:

首先,授权文书内容要具体明确。每份授权文书都要叙明具体的技术任务目标、需要处理的数据范围(时间区间、对象标识、数据类型)、授权使用的技术方法或工具、禁止性规定、有效期限等。授权文书明确化的目的在于避免因概括性授权而导致侦查权力扩大,同时也能够为后续审查与监督提供明确的判断依据。在授权文书有效期限设定和延长上,德国法可以提供参考,德国刑事诉讼中,对于线上搜索措施,地方法院合议庭或审判长核准的执行期限不得超过1个月,必要时可以延长,但每次延长不得超过1个月;如果延长期整体达到6个月,那么后面是否继续延长应由高等法院决定。^④正是由于德国法对授权期限和延长条件的严格限制,使得授权文书成为包含时间期限和审查程序的法律指令。

其次,动态评估与全流程留痕。在授权有效期内,执行过程也可能会因为任务变更、技术更新或者合作异化而偏离初始的授权范围。因此,应建立动态评估和再授权触发机制,实现从静态授权到动态监管的延伸。对于驻场服务这类长期项目,应要求在侦查机关设置专岗人员定期审查节点,避免合作性质从特定项目协助变成持续性职能外包;若

^④ 参见前注^③,维尔纳·薄逸克、萨比娜·斯沃博达书,第653页。

出现任务目标发生重大改变、数据范围需要扩展、技术方法需要更新等情况时,则启动重新审批程序,获取新的授权。同时,为了将技术协助的操作全过程置于可回溯、可验证的记录体系之下,所有涉及数据访问、查询、分析、输出等关键操作指令与日志都应当通过可信时间戳服务或接入区块链存证平台进行实时固定,做到完整清晰且时序不可篡改。

3. 明确程序违法行为的纠正与追责

为确保程序控制的刚性,法律应当明确规定对未获得授权、超越授权或者违反授权中禁止性规定的技术操作的纠正与追责。对于存在违法行为的,侦查机关应立即停止技术协助程序并要求协助方删除相关数据;技术协助机构擅自留存、使用和泄露合作中接触到的数据,侦查机关除追究其民事违约责任外,情节严重的还应依法适用侵犯公民个人信息罪等相关罪名进行刑事追责。

(三) 权利保障机制的确立

对刑事侦查公私合作进行程序控制的最终落脚点在于保障公民的诉讼权利,如果辩方在审判中无力对公私合作产出的技术证据进行有效审查与质疑,那么前两个层面的制度设计便可能落空。因此,应从证据规则、辩方权利与监督救济三个方面确立起权利保障机制,以填补控辩双方之间因技术能力落差而形成的鸿沟。

1. 优化证据审查规则

证据能力审查方面,首先应明确未严格遵循刑事诉讼法关于第三方技术协助专门程序所获取的电子数据及其衍生材料原则上不具备证据资格,应予排除,侦查机关不能以真实性或关联性来补救程序重大瑕疵。其次,由控方承担程序合法性的证明责任。控方在庭前会议或庭审中,不仅需出示电子数据本身,还须主动随案移送并出示一套完整的技术协助程序合法性证明材料。在证据属性上,技术协助程序合法性证明材料属于取证笔录范畴,其功能在于佐证电子数据及其衍生材料获取程序的合法性。在形式要件上,技术协助程序合法性证明材料应当形成完整证据链条,其要素包含技术协助方的资质证明、《第三方技术协助申请书》和授权文书、关键操作过程日志记录、数据移交与保管记录等;在法律后果上,无法提供技术协助程序合法性证明材料或材料存在重大缺陷的,相关电子数据应被排除。最后,确立辩方的程序性异议与审查机制。法律应明确赋予辩方在诉讼各阶段对电子数据取证、分析程序合法性提出异议的权利。法庭应优先就该程序性问题举行独立的审前听证,并可依申请或依职权调取后台日志、审批记录等进行核实。

证明力审查方面,对于通过公私合作中的算法建模、大数据分析产生的衍生证据,对其证明力的审查不应沿用传统物证、书证的经验法则,而应参照科学证据或专家证据的审查逻辑,重点关注数据及生成方法的科学可靠性与可验证性。这就意味着法庭审查的重心须从单纯关注分析报告的结论,转向深度审查生成该结论的算法及数据的可靠性。主要包括以下内容:一是算法的可靠性验证。该算法是否在其声称的领域内经过公认的、可重复的验证,其错误率、不确定性是否已知并得以充分披露。二是逻辑的可解释性与透明度,即算法决策的基本逻辑在原理上是否可以被理解。三是训练数据的相关性与

潜在偏见。用于训练和调整模型的数据集是否与当前案件情境具有充分的相关性,数据集中是否存在导致算法歧视或偏见的系统性缺陷。具体审查可通过三步进行:第一,检验算法是否可靠,如果不可靠则排除或者降格使用,如果可靠则继续到第二步;第二,检验算法是否有可解释性,如果是完全黑箱则排除或者降格使用,如果可解释、可理解则继续到第三步;第三,检验训练的数据是否具有相关性及是否存在潜在偏见,如果不相关或存在偏见就排除或者降格使用;如果相关且无偏见则可将该算法证据作为定案参考。上述审查步骤如图 1 所示。

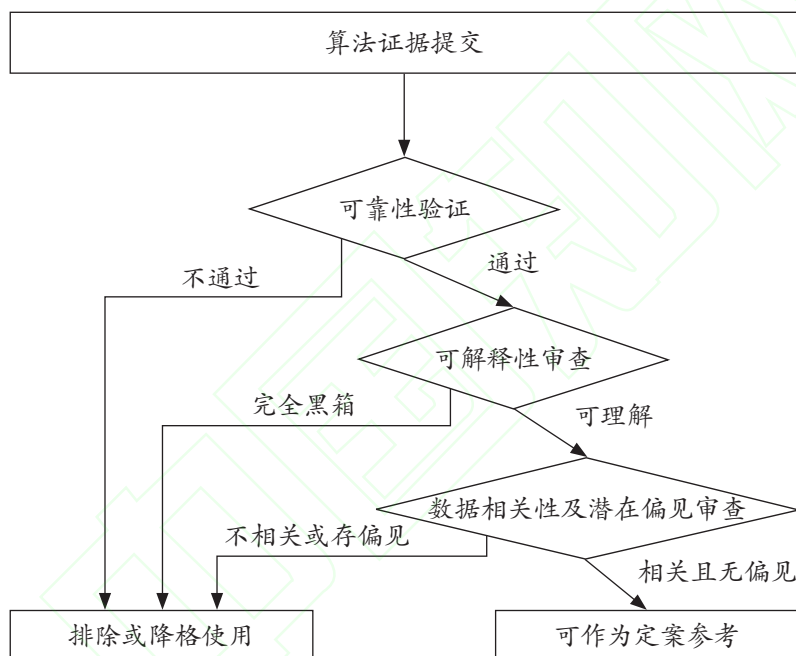


图 1 算法证据审查步骤

法庭在必要时,应委托双方认可的或从权威机构名册中指定的中立第三方技术机构,对涉案算法及其输出结论进行技术分析和原理解释。此外,最高人民法院也可通过司法解释或指导性案例确立审查算法证据证明力的考量因素清单,引导法官进行科学、审慎的判断。

2. 保障辩方取证和质证权

首先,法律应明文规定辩护律师为辩护之目的有权向持有相关电子数据的网络服务提供者等第三方调取证据,第三方无正当理由不得拒绝。对于拒绝配合的情况,辩护律师有权申请法院签发证据调取令,将辩方的取证请求权转换成具备司法强制力的命令。其次,设立针对算法证据的双重开示规则。控方除了要开示通过技术协助获取的完整基础电子数据外,也应该给出用于生成技术证据的算法模型的基本原理、关键参数、训练数据

概况以及可能产生偏差的说明。^{④⑨}唯有如此,质证才能触及核心而不是流于形式。最后,完善技术质证的程序支持体系。一方面要保障辩方委托专家辅助人的权利,另一方面探索建立技术专家援助制度,为因经济困难无法自行委托的被追诉人提供公共技术支持。

3. 建立全流程的监督与救济机制

对侦查权进行外部控制,是对侦查机关内部自律式控制方式的主要补充,可以弥补侦查机关自我监督的先天缺陷。在我国现有制度框架下,应当拓展检察机关侦查监督的视角,将其延伸至侦查活动中的公私合作行为。在制度建设层面,应构建以检察机关为中心的同步程序监督机制,检察机关可根据技术协助行为的敏感性、权利干预强度及数据规模,实施分类化监督。除了关键证据生成型协助需要报请上级检察机关审查批准后方可启动外,对于其他类型的技术协助,也应赋予检察机关随时调阅全部程序文书、技术日志的权力,从而使监督嵌入公私合作流程。此外,检察机关要着力解决数字时代监督能力的局限性问题,从事相关监督工作的人员应具备评估技术方案安全性、数据管理合规性及算法模型合理性的专业能力,将法律监督建立在扎实的技术认知基础之上,从而提升监督实效。

在救济方面,应以当事人权利为核心,构建多层级的救济通道。首先,可探索建立事后告知制度。在不妨碍后续侦查的情况下,侦查机关可在合理期限内以书面方式通知被采取公私合作侦查措施的公民,告知其法律依据、概略内容、所涉罪名以及申请复议、提出异议的途径。^{⑤⑩}其次,完善程序性制裁机制。被追诉人如果认为公私合作行为侵犯其合法权益,涉嫌程序性违法,有权在法庭审理阶段对此提出异议。法庭应就此举行专门调查,一旦认定存在重大程序违法,应排除由此获取的证据。最后,构建实体损害救济机制。因公私合作中的违法行为造成公民实体合法权益损害的,当事人有权依法申请国家赔偿。

五、结 语

数字技术的广泛运用,使得刑事侦查由传统的封闭办案模式转向多方参与、公私协同的开放模式。这种转变在提高办案效率的同时,也改变了侦查权的配置方式与行使边界。对此,应当肯定公私合作在犯罪治理效能提升方面发挥的积极作用,但也需要正视侦查实践中存在的权力运行不规范、程序约束不到位和责任边界不清晰等问题,通过严

^{④⑨} 有学者提出,证据开示中的算法公开应以适度为限。一是仅在特定案件的特定情况下要求公开算法;二是可以通过解释特定算法决策结果的原因和理由实现算法公开;三是可以通过要求各方签订保密协议等方式控制算法公开的范围,防止算法公开的后果扩大,以保护科技企业的研发积极性和合法商业利益。参见郑曦:《数字时代刑事证据开示制度之重塑》,载《华东政法大学学报》2023年第4期,第47页。

^{⑤⑩} 事后告知制度的意义在于不妨碍侦查活动顺利进行的同时,保障当事人的知情权,方便其进行权利救济。参见王仲羊:《侦查中个人信息知情同意制度的引入与调适》,载《中国人民公安大学学报(社会科学版)》2023年第1期,第108页。

密的制度设计确保侦查权始终运行在法治轨道上。本文在对当前刑事侦查公私合作状况进行归类分析的基础上,从健全程序规则、明确权力边界、规范协作流程、强化监督制约等方面着手,力图构建起一套可监督可问责的制度体系,将刑事侦查公私合作置于法律规制框架之内。毫无疑问,数字技术将持续快速发展、不断迭代,犯罪治理领域也面临着新的挑战,刑事侦查公私合作的形态将会更加复杂多元,本文仅仅对该问题进行了初步探索,许多问题还有待继续观察和更为深入的研究。

Abstract: The development of digital technology and changes in the forms of crime have given rise to public-private partnerships in criminal investigations, but the legal process has lagged significantly. In practice, public-private partnerships in criminal investigations can be roughly divided into obligatory, contractual, and marginal cooperation. The impact of public-private partnerships on the existing procedural rule of law system is mainly reflected in the lack of legitimacy in the allocation of power, the weakening of control over the exercise of power, and the imbalance between prosecution and defense in the litigation structure. To address this, institutional responses can be made in three aspects: reshaping the foundation of legitimacy, constructing a system for controlling the operational process, and establishing a rights protection mechanism. This will systematically resolve issues related to the legitimacy of power exercise, approval procedures, process monitoring, balance between prosecution and defense, and supervision and remedies in public-private partnerships, thus incorporating technological effectiveness into a controllable framework of procedural rule of law.

(责任编辑:王 楷)