数字时代刑事侦查程序的逻辑转变与制度回应

裴 炜

摘 要 犯罪及犯罪治理的数字化深刻转变着刑事侦查程序的内在逻辑，尤为集中地体现为犯罪“嫌疑”的概念被重构，侦查对象呈现出量化拓展的趋势，侦查行为的涉外属性不断强化，以及侦查权在私主体的深入参与下被不断稀释。在国家启动新一轮《刑事诉讼法》修订的背景下，采用法典化的修法思路意味着需要对侦查程序进行体系化的调适，从而与演变中的数字侦查逻辑相适应。基于此，侦查制度的调整应当遵循“技术导向”向“权利导向”回归的总体路径，重构侦查行为的基点，采用透明化的全流程控制的规制视角，通过引入涉外法治思路来应对犯罪治理全球化这一外部生态，并在此基础上整合和修订刑事诉讼法相关制度。

关键词 数字侦查 权利导向 全流程控制 涉外法治

DOI:10.16094/j.cnki.1005-0221.2025.03.012

引 言

数字时代新兴技术在持续赋能犯罪侦查取证的同时，也对传统侦查程序提出一系列新的挑战，诸如侦查创新措施与传统措施的关系、侦查中个人信息等新兴数字权益的保护、跨地域的数据取证、网络犯罪治理国际合作等议题成为当下国内外立法的重要关注事项。在此背景下，我国在大力推进侦查数字化、智能化的同时，也在三个维度探索相关程序规则。

第一是从电子数据的角度切入，围绕其收集、提取创设或改造侦查措施规则，典型体现在2016年最高人民法院、最高人民检察院、公安部发布的《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》（下文简称《电子数据规定》）和2019年公安部《公安机关办理刑事案件电子数据取证规则》（下文简称《电子取证规则》）之中。

第二是从打击网络犯罪角度切入，针对特定类型的网络犯罪，对管辖、境内及境外警务合作、线索的调查核实、取证措施等调整侦查程序规则，例如2022年最高人民法院、最高人民检察院、公安部发布的《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》，2021年最高人民检察院《人民检察院办理网络犯罪案件规定》，2016年和2021年最高人民法院、最高人民检察院、公安部发布的《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》及《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》，以及最高人民法院、最高人民检察院分别发布

* 裴炜，法学博士，北京航空航天大学法学院教授。本文系国家社会科学基金一般项目“数字正义视阈下刑事审判程序数字化法治路径研究”（23BFX142）的阶段性研究成果。

的一系列针对电信网络诈骗及其关联犯罪的典型案例，等等。

第三是从数字法治的角度切入，对其中涉及刑事侦查取证的部分予以规定，例如《网络安全法》第28条、《数据安全法》第35条、《反电信网络诈骗法》第26条等条文规定了网络信息业者的协助犯罪侦查义务，又如《个人信息保护法》第41条、《数据安全法》第36条等规定了国际司法协助或执法合作。此外，当前数字领域法多同时规制公私行为，这就使得针对国家机关的规定能够拓展至侦查主体，典型如《个人信息保护法》中关于国家机关处理个人信息的特殊规定。

上述三个维度的立法活动共同建构起当前我国刑事数字侦查的制度框架，其中前两者的规范性文件效力层级较低，而第三者关于刑事侦查程序的规定相对零散。同时，三个维度并非全然协调一致，并引发了一系列制度问题。

首先是与《刑事诉讼法》衔接不畅。《刑事诉讼法》所建立的侦查程序构成下位法和刑事司法外部相关规范的制度基础，但目前上述三个维度的立法与《刑事诉讼法》均存紧张关系，例如关于载体内部电子数据的收集，一直存在着是否构成“搜查”行为的探讨;[①] 又如针对境外数据的网络远程在线提取是否违反国际刑事司法协助规则，等等。[②] 上述紧张关系反映出“侦查行为”与“侦查技术”的概念混同，后者在一定程度上成为了立法重点，技术导向而非权利导向的特点突出。这种混同不仅弱化了侦查程序的权利保障基础，也使得刑事侦查措施与行政执法措施之间的界限日益模糊，二者的强制性位阶被打破。例如2024年国家市场监督管理总局制定的《市场监督管理行政执法电子数据取证暂行规定》，其尽管是行政执法规定，但其中针对电子数据的取证措施与刑事侦查高度重合，特别是规定了“技术监测”措施，即便没有采用技术侦查的表述，但强度上与后者高度类似。

其次是与相关数字法衔接不畅，具体表现在三个方面。第一是混用程序性表述，典型如《数据安全法》第35条关于公安机关刑事调取数据的规定，其采用的“严格的批准手续”在《刑事诉讼法》中特指针对技术侦查措施所采取的相较于其他侦查行为更为严格的程序性限制，该限制显然不宜适用于强制性较弱的调取。[③] 第二是忽略关键场景，例如《个人信息保护法》第24条规定了个人信息自动化决策，特别提到了“通过自动化决策方式作出对个人权益有重大影响的决定”的情形，犯罪侦查中对此类技术的应用无疑可以落入该情形中，但该条文采用的“交易价格等交易条件”、“信息推送、商业营销”等表述，又明显与刑事诉讼无关。第三是单方创设涉部门法制度，例如《个人信息保护法》第35条规定的国家机关告知义务的减免，在刑事诉讼法中并无对应条款，这也使得该条难以在具体的刑事侦查中落地。

再次是涉外程序规则的体系性缺位。一方面，国内法较少关注到跨境数据取证的普遍化趋势和程序特性，例如《刑事诉讼法》第18条仅规定了国际刑事司法协助这一种跨境取证方式，《国际刑事司法协助法》原则上也不允许我国境内的机构、组织或个人自愿协助外国执法机关（第4条第3款），从而压缩了其他跨境取证方式的空间。《电子取证规则》仅在网络在线提取这一种措施上区分了境内和境外，对远程勘验、技术侦查、数据调取、数据冻结等同样可能跨境实施的措施则无对应规定。另一方面，国内法涉外视角的缺失也在一定程度上阻碍了我国参与国际规则的制定。跨境数据取证不仅需要本国法支撑，还依赖于各国共识下的国际法依据，后者则是平衡尊重国家主权与跨

① 例如骆绪刚：《电子数据搜查扣押程序的立法构建》，载《政治与法律》2015年第6期，第153－161页；胡铭、王林：《刑事案件中的电子取证：规则、实践及其完善——基于裁判文书的实证分析》，载《政法学刊》2017年第1期，第79－89页；陈永生：《刑事诉讼中搜查手机的法律规制——以美国赖利案为例的研究》，载《现代法学》2018年第6期，第135－154页。

② 谢登科：《电子数据网络在线提取规则反思与重构》，载《东方法学》2020年第3期，第89－100页；裴炜：《论远程勘验：基于侦查措施体系性检视的分析》，载《政法论坛》2022年第4期，第156－166页。

③ 相关探讨参见谢登科：《论侦查机关电子数据调取权及其程序控制——以〈数据安全法（草案）〉第32条为视角》，载《环球法律评论》2021年第1期，第52－67页。

境打击犯罪的关键。2024 年 12 月联合国通过《联合国打击网络犯罪公约》，其中“国际合作”机制并不限于刑事定罪中的罪名，还可以拓展至“收集、获取、保存和分享任何严重犯罪的电子形式证据”（第 35 条第 1 款（c）项），但由于其中涉及的数据分类以及对应取证措施与我国国内法存在诸多差异，我国在后续谈判中将面临国际规则向国内规则转化困难的问题。

2023 年全国人大常委会正式启动《刑事诉讼法》的新一轮修改。在数字法治与涉外法治共同推进的当下，此次修法能否对信息化、数字化作出积极回应，将直接影响刑事司法改革的整体成效。侦查作为刑事诉讼的重要阶段，其相关制度设计同样需要与上述回应相协调，从而适应数字时代犯罪治理的新需求。本文正是由此出发，从数字时代刑事侦查的逻辑演变为基点，分别从总体路径、视角转换，以及外部生态三个方面，探索侦查数字化转型的制度回应。

一、刑事侦查数字化的逻辑转换

侦查活动的数字化冲击着侦查制度的传统逻辑，《刑事诉讼法》修订时的关注点不能仅停留在技术层面，更要适应刑事数字侦查的逻辑转换。这种逻辑转换既体现在侦查行为内部，主要表现为侦查依据的重构和侦查对象的量化；同时也体现在侦查行为的外部，尤为集中地表现为侦查权的涉外化和扁平化。以下分别予以分析。

（一）侦查依据的重构

数字技术对于犯罪侦查的首要影响，在于转变了“嫌疑”这一侦查的核心依据。传统刑事诉讼中的“嫌疑”是以具体且清晰的事实为基础所形成的理性判断，指向的是特定事件中位于特定场所内的特定个人，是根据相对分离的事实、有限的信息、局限的背景、稀缺的知识的“小数据”所形成的可能性判断。[①] 在数字技术的加持下，诸如“算法嫌疑”[②]、“自动化嫌疑”[③]、“计算式嫌疑”[④]等表述开始出现，刑事侦查对嫌疑的判断开始发生三个方面的变化。

第一是嫌疑判断的依据由经验内向经验外拓展。传统的嫌疑判断严重依赖于侦查人员的办案经验，通过其对案件的具体观察来形成自身知识网络的投射。[⑤] 在数字语境下，侦查人员的知识谱系开始向案外扩张，其可能基于信息网络汇聚的数据而形成对相对人的认知，过程中甚至可以全然排除与相对人的接触。这种判断依据的变化进一步转变着侦查行为本身，相对人的外在显见特征在嫌疑判定中的权重下降，同时获取同等知识量所需的侦查行为的复杂性显著降低，而数据推论在这一过程中扮演关键角色。

第二是嫌疑判断的对象由个体向群体拓展。依托大数据开展的嫌疑人员、行为、事件等的画像、比对或预测，其背后的逻辑是根据某一时空范围内的群体性要素进行规律提取，进而投射到特定个体。这使得侦查人员对陌生相对人的背景了解更深更广，甚至超出相对人对于自身的认知，从

---

① See Andrew Guthrie Ferguson, “Big Data and Predictive Reasonable Suspicion”, *University of Pennsylvania Law Review*, Vol. 163, No. 2 (2015), p. 329.

② See Irmak Erdogan, “Algorithmic Suspicion in the Era of Predictive Policing”, in Georg Borges & Christoph Sorge, eds., *Law and Technology in a Global Digital Society: Autonomous Systems, Big Data, IT Security and Legal Tech*, Springer, 2022, pp. 89–101.

③ See Michael L. Rich, “Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment”, *University of Pennsylvania Law Review*, Vol. 164, No. 4 (2016), p. 871; Elizabeth E. Joh, “The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing”, *Harvard Law & Policy Review*, Vol. 10, No. 1 (2016), p. 15.

④ See Wesley M. Oliver et al, “Computationally Assessing Suspicion”, *University of Cincinnati Law Review*, Vol. 92, No. 4 (2024), p. 1108.

⑤ 参见王燃：《大数据证明的机理及可靠性探究》，载《法学家》2022 年第 3 期，第 59 页。

而形成二者的认知差异。同时，关于该真实个体的现实特征又容易在这一认知过程中被掩盖，从而形成“数字人”与“自然人”的分裂。

第三是侦查启动所需嫌疑强度的弱化。刑事诉讼中的嫌疑是动态变化的，从立案时的初始嫌疑逐步发展为定罪量刑的内心确信。[①] 原则上，侦查行为的强制性越高，其适用的嫌疑标准也应当越高。但是，随着侦查基础由具象化的嫌疑向抽象化的风险转变，一些具有较强权利干预属性的措施得以仅基于普遍嫌疑而在正式立案前适用，典型如“数据调取”[②]、“远程勘验”[③] 等措施。

（二）侦查对象的量化

传统刑事侦查无论是在其可利用的信息资源上还是在面向的取证对象上，均因时空限制而相对有限。数字技术同时作用于犯罪和犯罪治理，使得面向海量数据开展犯罪侦查活动成为常态，在赋能侦查机关的同时也造成侦查取证任务量的几何式上升，并在以下方面逐步转变刑事侦查的底层思路。

第一是案件事实证明方式的转变。犯罪的数字化和网络化引发涉案电子证据的激增，这在关于人员身份、资金账户、情节轻重等犯罪事实的查证方面尤为明显。[④] 海量数据远远超出了传统侦查措施的应对能力，变通式的证据收集方法越来越常见。[⑤] 例如 2022 年《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》专门就“数量特别众多且具有同类性质、特征或者功能”的证据材料，以及“涉案人数特别众多”的信息网络犯罪的资金来源等的查证方法予以特殊规定，“抽样审查”“综合认定”等方式的适用越来越普遍化。[⑥]

第二是作为侦查行为门槛的传统信息类权益稀释。基于数据挖掘的侦查活动一定程度上模糊了措施强制性与任意性的划分。以隐私与通信秘密保护为例，传统侦查行为受到宪法、法律等对公民通信秘密和隐私保护的严格限制。但是，在数字侦查场景下，单个数据本身并不足以构成“隐私信息”或“通信信息”，这就为侦查行为规避隐私权或通信秘密权的限制提供了便利；同时，涉案数据普遍由网络服务提供者等第三方主体控制或占有，向其调取数据一定程度上弱化了侦查行为的权利干预属性。[⑦]

（三）侦查权力的扁平化

犯罪侦查效能依赖于充分的资源供给，基于侦查权的国家垄断，该资源供给传统上主要依赖国家。在数字时代，数据演变成犯罪治理的关键资源，但其并非主要汇集在国家层面，而是由网络服务提供者等私主体广泛占有或控制，后者构成了“数字社会泛在链接、信息汇聚的公共设施”。[⑧] 治理资源由国家机关向私主体的转移，在以下三个方面形成了侦查权扁平化的趋势。

第一是侦查模式由国家机关主导转向公私合作。这种合作既表现为常规化的、日常性的犯罪风险识别、预警和处置，也表现为具体案件中私主体的数据或技术协助。刑事诉讼中侦查权隶属于国家专门机关，其他人员作为相对人、见证人、辅助人等参与到侦查过程中来。随着数据资源和数字

---

① 参见施鹏鹏：《“普遍嫌疑”及其规制：以德国法为借鉴》，载《中外法学》2024 年第 1 期，第 202－203 页。

② 参见裴炜：《论个人信息的刑事调取——以网络信息业者协助刑事侦查为视角》，载《法律科学（西北政法大学学报）》2021 年第 3 期，第 80－95 页。

③ 参见谢登科：《电子数据网络远程勘验规则反思与重构》，载《中国刑事法杂志》2020 年第 1 期，第 58－68 页。

④ 参见王燃：《大数据证明的机理及可靠性探究》，载《法学家》2022 年第 3 期，第 57－58 页。

⑤ 参见刘品新：《论大数据证据》，载《环球法律评论》2019 年第 1 期，第 21－34 页。

⑥ 参见谢澍：《数字时代刑事证据理论的三重挑战及其变革》，载《法学论坛》2024 年第 3 期，第 104－113 页；陈卫东、崔鲲鹏：《电信网络诈骗犯罪数额证明的问题厘清与路径优化》，载《证据科学》2024 年第 1 期，第 6－16 页；姜丹：《电信网络诈骗犯罪数额“综合认定”的理论审视和完善进路》，载《中国刑事法杂志》2023 年第 6 期，第 54－69 页。

⑦ See, e. g., Matthew Tokson, “The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021”, *Harvard Law Review*, Vol. 135, No. 7 (2022), p. 1790.

⑧ 参见单勇：《数字平台与犯罪治理转型》，载《社会学研究》2022 年第 4 期，第 48 页。

技术优势向网络信息业者转移，上述人员分工的界限逐渐模糊化，形成国家机关以外的专业机构、专业人员实质性替代侦查人员主导侦查活动的情况，[①] 甚至在跨境数据取证等场景中，通过网络信息业者配合调取数据是侦查机关获得涉案证据材料的唯一途径。[②] 在这种情况下，私主体成为犯罪侦查的必不可少的参与者，从而逐步消解国家机关对于侦查权的垄断。

第二是私主体限定侦查能力和侦查范围。私主体的数据资源和数字技术优势进一步促使其上升为侦查活动的实际主导者。这一点在跨境调取数据中尤为明显。一方面，网络信息业者是否以及在何种程度上配合侦查机关，不仅取决于法律规定，还受到其内部规则的限制，例如微软、苹果、亚马逊等大型互联网企业均针对外国执法机关制定了详细的执法指引，是否遵守该指引直接会影响上述企业对调取命令的响应程度。[③] 另一方面，在数据控制者模式下，网络信息业者基于对诸如税收政策、行政监管、技术要求、市场规模等营商环境的综合考量选定数据的存留地，而这一选择则会间接决定其所在国侦查机关的执法管辖权的范围。

第三是技术逻辑和技术规范主导侦查行为。侦查权的国家机关专属衍生出一系列规制侦查行为的诉讼规则，但在私主体深度参与侦查活动的情况下，上述规制被逐渐打破。首先，技术企业介入具体案件侦查不限于分析专业问题，还会进一步涉及法律问题的判断，例如第三方机构数据挖掘所形成的犯罪线索，往往能够成为开展具体侦查措施的依据。[④] 其次，当前智慧公安、智慧警务建设所依赖的技术架构，也多由科技企业开发完成，与其他领域的数字技术开发相比“仅仅是技术难度上的区别而非技术逻辑上的相异”，[⑤] 并未充分适应刑事司法的特殊需求。再次，侦查主体在形式和实质上的分离一定程度上架空了刑事诉讼法针对侦查行为的限制，例如海量数据分析报告在实践中体现为鉴定意见、专家辅助人意见、检查笔录、破案经过材料等多种形式，[⑥] 反映出的是同一套技术内核之外，侦查机关在不同程序规则间选择的任意性。

（四）侦查措施的涉外化

网络空间弱地域性使得其间的犯罪活动得以超越时空的限制而开展，涉案的人、财、证等要素也随之在全球范围内分散分布。[⑦] 在此背景下，侦查机关开展跨境犯罪追诉的实践需求越来越普遍，与传统以地域为核心的刑事诉讼管辖制度形成紧张关系。这种紧张关系促使各国探索跨境数字侦查规则，其尽管主要由国内法确立，但却具有强烈的效力域外溢出的性质，是典型的涉外法治范畴。[⑧] 这些探索在更深层次上重塑了侦查行为的逻辑，具体表现以下两个方面。

首先是执法管辖权与立法管辖权分化。在尊重主权原则的前提下，相较于立法管辖权，一国侦查机关的执法管辖权受到严格的地域限制，即便一国司法机关根据刑事实体法对某一涉外犯罪享有定罪量刑的权力，原则上对该罪的侦查取证仍然限于本国境内。在数字革命兴起之前，跨境侦查相对较少，跨境执法管辖权未受关注。但犯罪普遍触网引发跨境侦查的常态化，传统的国际刑事司法协助已然捉襟见肘，如何在尊重主权的前提下兼顾跨境侦查的实践需求，成为世界各国普遍关注的议题。

---

① 参见陈如超：《以鉴代侦：电子数据司法鉴定的扩张趋势及其制度回应》，载《法学研究》2024 年第 3 期，第 181－183 页。

② See “SIRIUS EU Digital Evidence Situation Report (3rd Annual Report) 2021”, *Eurojust*, December 3, 2021, https://www.eurojust.europa.eu/sites/default/files/assets/sirius_eu_digital_evidence_situation_report_2021.pdf, last visited at July 5, 2024.

③ See “SIRIUS EU Electronic Evidence Situation Report”, *Europol*, November 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS%20EUEESR%202023.pdf, last visited at July 7, 2024.

④ See Andrew Guthrie Ferguson, “Big Data and Predictive Reasonable Suspicion”, *University of Pennsylvania Law Review*, Vol. 163, No. 2 (2015), p. 338.

⑤ 参见左卫民：《从通用化走向专门化：反思中国司法人工智能的运用》，载《法学论坛》2020 年第 2 期，第 20 页。

⑥ 参见冯俊伟：《机器生成的电子数据之可采性》，载《中国刑事法杂志》2024 年第 3 期，第 60－76 页；参见刘品新：《论大数据证据》，载《环球法律评论》2019 年第 1 期，第 21－34 页。

⑦ 参见冯俊伟：《刑事证据分布理论及其运用》，载《法学研究》2019 年第 4 期，第 174－190 页。

⑧ 参见裴炜：《涉外法治视野下刑事诉讼的数字化进路》，载《中国刑事法杂志》2024 年第 2 期，第 124－142 页。

其次，侦查行为涉外属性的强化也促使权利保障的国际融合。长期以来，制约侦查行为的公民基本权利主要以国内法为基础，国际法仅设置最低限度要求，至于外国法则极少与本国侦查行为发生关系。但是跨境侦查使得一国侦查机关不可避免地触及他国的权利保障体系，特别是会干预一些新兴数字权益。这种张力既源于不同国家对于特定网络空间刑事执法行为的法律性质界定差异，也源自各国公民基本权利结构差异，例如个人信息相关权益与隐私权、通信秘密权等的关系。在此背景下，协调和统一不同国家间的权利保障体系、避免出现跨境犯罪追诉中的权利洼地，就成为当前网络空间犯罪治理国际合作的重点。例如美国《云法》在授权与其他国家签订双边协议以便利跨境数据取证的同时，要求协议方必须证明本国法律制度提供了足够的隐私和人权保障（第 103 条）。与之类似，《联合国打击网络犯罪公约》（以下简称《公约》）在序言部分强调了“保护个人隐私不受任意或非法干涉的权利，以及保护个人数据的重要性”，并进一步在第 24 条“条件和保障措施”中细化了相关执法程序中的权利保障要求。①

二、制度回应的基点重构：技术导向回归权利导向

在侦查逻辑发生变化的当下，传统刑事诉讼制度在规制数字侦查行为时开始出现不兼容的状况，而新侦查措施的创设具有强烈的技术导向，使得技术措施与侦查行为在概念上混淆，进而产生以下三方面的问题。第一是规避可以涵盖网络空间侦查活动的既有概念，如针对计算机信息系统中的数据收集，《电子数据规定》和《电子取证规则》采用了“提取”而非“搜查”概念。② 第二是将强权利干预性质的措施冠以任意性侦查措施之名，例如“远程勘验”与“勘验”、③“数据调取”与“调取”。④ 第三是侦查行为的强制性层级的倒置，例如《电子数据规定》和《电子取证规则》中将强制性更高的技术侦查措施放置在远程勘验项下。对此，有必要系统审视当前侦查行为体系混乱的现状，以权利导向整合新型数字侦查行为与传统侦查行为，使其形成内在逻辑一致的结构。

（一）厘清“侦查行为”的概念

根据《刑事诉讼法》第 108 条，“侦查”是指“公安机关、人民检察院对于刑事案件，依照法律进行的收集证据、查明案情的工作和有关的强制性措施”，该条文常被视为“侦查行为”的定义，⑤ 但其并未充分揭示各类侦查行为的本质，也无法说明为何《刑事诉讼法》中仅规制某些而非全部侦查活动。

对此，首先需要明确的是，“侦查行为”不同于“侦查技术”，前者是国家刑罚权经由有权机关具象化、动态化的过程，体现的是国家权力本身，而后者指向的是解决具体问题的方法及方法原理，前者而非后者是刑事诉讼规制的对象。⑥ 其次，值得刑事诉讼法予以规制的“侦查行为”，主要指向的是干预公民基本权利的活动，进而适用法律保留原则；对权利的干预性不仅构成侦查行为

① 参见《联合国打击网络犯罪（使用信息和通信技术系统实施的犯罪）公约》，2024 年 8 月 7 日发布，引自 https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/AC.291/22/Rev.3&Lang=C，2024 年 8 月 31 日访问。

② 参见谢登科：《电子数据网络在线提取规则反思与重构》，载《东方法学》2020 年第 3 期，第 89－100 页。

③ 参见谢登科：《电子数据网络远程勘验规则反思与重构》，载《中国刑事法杂志》2020 年第 1 期，第 58－68 页。

④ 参见裴炜：《论个人信息的刑事调取——以网络信息业者协助刑事侦查为视角》，载《法律科学（西北政法大学学报）》2021 年第 3 期，第 80－95 页；参见谢登科：《论侦查机关电子数据调取权及其程序控制——以〈数据安全法（草案）〉第 32 条为视角》，载《环球法律评论》2021 年第 1 期，第 52－67 页。

⑤ 例如陈光中主编：《刑事诉讼法》（第 7 版），北京大学出版社、高等教育出版社 2021 年版，第 301 页。

⑥ 参见王敏远主编：《刑事诉讼法学》（第 2 版），知识产权出版社 2023 年版，第 546 页。

强制性与任意性的区分标准，也成为侦查行为类型化的依据之一。再次，侦查行为的核心功能在于“保全犯罪的证据、保全犯罪嫌疑人的人身”。①

从侦查行为的概念出发，意味着此次《刑事诉讼法》在吸纳并整合下位法创设的新型电子数据取证措施时，需要将侦查技术归入到对应的侦查行为予以规制。其中，最为典型的是电子数据提取。无论是现场提取还是网络在线提取，“提取”本身并非一种侦查行为，而是对侦查技术的描述，其本质仍然是“对犯罪嫌疑人以及可能隐藏罪犯或者犯罪证据的人的身体、物品、住处和其他有关的地方”进行搜索检查的行为，因此宜纳入《刑事诉讼法》“搜查”的章节项下，并就目前第 136 条中规定的“有关的地方”做拓展解释以使其能够适用于网络空间。至于目前嵌套于网络在线提取项下的“网络远程勘验”和“技术侦查”，则应按照其功能定位归属于勘验和技术侦查。

（二）以权利为核心类型化侦查行为

多种侦查活动是否构成同一种类的侦查行为，在判断功能性的同时，还需考量其干预的权利属性和强度。例如《联合国打击网络犯罪公约》考虑到不同国家对于同种侦查行为的不同表述，采用了“搜查或以类似方式访问”、“扣押或以类似方式保全”等表述，强调行为在实质功能上的等同；② 而美国近年来围绕《宪法》第四修正案中“搜查”概念在网络空间中的适用所形成的一系列判例，集中于对作为搜查行为构成基础的“合理隐私期待”在虚拟场域中的阐释。③ 强调以权利为核心建构侦查行为体系至少具有以下五方面的功能。

第一是用以明确侦查行为的种类，例如目前《电子数据规定》中的“远程勘验”措施尽管称之为“勘验”，但当该措施指向进入虚拟私密空间并提取数据的行为时，会对数据主体的隐私权等形成实质干预，此时“远程勘验”实则与搜查无异，应当与单纯的勘查检验相区别。

第二是用以精细定性特定侦查行为，例如数据所承载权益的复杂性使得调取措施很难再概括定性为“任意性侦查”，其具体性质需要以目标数据的范围、体量、性质等要素予以精细化评估。④ 我国《刑事诉讼法》目前仅在第 54 条第 1 款规定了公安司法机关的“收集、调取证据”行为，但是出于其“任意性侦查”的定位，在后续侦查章节中并未再规定。对此，有必要在“侦查”之下单设一节“调取”，一则吸收公安部、最高人民检察院、最高人民法院在其各自规范性文件中关于调取的规定，二则明确其适用于电子数据的条件、范围、期限等程序要素。

第三是避免忽略相关主体的权益保障，例如数据冻结措施不仅会涉及个人信息保护问题，还可能干预占有或控制该数据的网络信息业者的正常经营活动，后者也需要纳入侦查行为的规范考量之中。⑤《联合国打击网络犯罪公约》在程序措施部分强调要考虑相关权力和程序“对第三方权利、责任以及合法利益的影响”，正是这一思路的体现。

---

① 参见［日］田口守一：《刑事诉讼法》（第 7 版），张凌、于秀峰译，法律出版社 2019 年版，第 47 页。

② 参见《联合国打击网络犯罪（使用信息和通信技术系统实施的犯罪）公约》，2024 年 5 月 23 日发布，引自 https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/AC.291/22/Rev.3&Lang=C，2024 年 7 月 8 日访问。需要注意的是，英文版本中的表述是“search or similar access”、“seizure or similar securing”，中文版本中对于“access”的翻译不尽相同，本文采用的是其中使用频次最高的“访问”；同时中文版本中将“披露”也纳入到了扣押的类似方式中，但对应的英文“disclosure”实际是一种单独的取证措施，因而在本文中将其排除。英文版参见 https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/AC.291/22/Rev.3&Lang=E。

③ 关于相关案例的系统介绍，参见 Matthew Tokson, “The Carpenter Test as a Transformation of Fourth Amendment Law”, U. Illinois Law Review Vol: 2023, No. 2, p. 507; See, e. g., Matthew Tokson, “The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021”, *Harvard Law Review*, Vol. 135, No. 7 (2022), p. 1790.

④ 参见谢登科：《论侦查机关电子数据调取权及其程序控制——以〈数据安全法（草案）〉第 32 条为视角》，载《环球法律评论》2021 年第 1 期，第 52－67 页。

⑤ 参见裴炜：《论刑事跨境取证中的数据先行冻结》，载《当代法学》2023 年第 2 期，第 124－135 页；孙明泽：《刑事诉讼电子数据冻结的程序规制研究》，载《中国人民公安大学学报（社会科学版）》2020 年第 1 期，第 58－66 页；谢登科：《电子数据冻结：一种新兴的证据保全措施》，载《东岳论丛》2023 年第 6 期，第 156－165 页。

第四是搭建起新型权益进入侦查行为规制体系的通道，典型如个人信息相关权益，数字侦查不可避免地会有所触及，而是否需要予以保护、保护到何种程度，则需要以该权益嵌入刑事诉讼法权利体系中为前提。[①] 我国《个人信息保护法》专门规定了国家机关处理公民个人信息的相关要求，《刑事诉讼法》在与其衔接时，可以考虑在侦查章节的“一般规定”部分补充个人信息的处理原则，即“公安机关收集、处理个人信息应当遵循合法、正当、必要和诚信原则，应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式”。

第五是以此判断电子证据合法性，进而引入非法证据排除规则，以此确保侦查行为不偏离权利保障的刑事诉讼价值。[②] 其中，应当明确将《刑事诉讼法》第56条中关于非法实物证据的排除规则拓展至物证、书证以外的证据种类。

（三）基于精细化的比例原则构建侦查行为阶层

以权利为核心构建侦查行为体系，关键在于形成所涉权利与侦查行为之间的层级化匹配，而比例原则在这一过程中发挥重要作用。[③] 我国当前刑事诉讼法关于侦查行为的比例性规制，主要体现在任意性侦查与强制性侦查的概括区分之上，标准在于是否限制相对人的人身、财产权利。但这一划分具有明显缺陷，即便是归入“任意性侦查”的行为，也并不全然与相对人的人身、财产权利无涉；换言之，一项侦查活动之所以需要纳入刑事诉讼法的规制视野之下，恰恰在于其之于公民基本权利的干预性。据此有观点认为凡刑事诉讼法所规定的侦查行为必然具有强制性；所谓强制性与任意性的划分，标准应当在于是否“侵害重要利益”。[④]

在进入到所涉利益“重要性”的衡量层面之后，比例原则的适用就不能停留于强制性与任意性的简单二分框架，而是需要深入到各种侦查行为内部，进行更为精细化的制度设计。数据作为侦查对象，其所承载的权益高度复杂。首先，同一数据可能同时承载多个主体的权益，例如个人信息既牵涉单个信息主体，也可以构成网络信息业者的重要数据资产。其次，数据的汇集和挖掘可能形成新的权益类型，而不同数据权益之间会动态转化，例如碎片化的个人信息的聚合可能清晰揭示出信息主体的私密信息，从而落入到隐私权的范围之中。再次，在大数据的背景下，权利主体与权利客体的对应性被稀释，一个数据集合可能牵涉海量的数据主体。最后，数据权益主体与数据控制能力相分离，典型如个人信息，信息主体实则无力控制自身信息的处理行为。[⑤]

数据权益的复杂性意味着“重要利益”衡量的复杂性，并进一步传递至侦查行为的强制性判断上。侦查行为的强制性不应当再是单纯的“有或无”的问题，而是在一条渐变谱系上的精细化衡量。就衡量要素而言，可以从刑事诉讼法对于技术侦查的严格规制中大致归纳出来，包括但不限于所涉权利性质、犯罪性质、措施强度、措施必要性、权利主体类型等。将这些因素结合分析，一方面意味着同一种侦查行为仍然可能存在强制性的内部分层，另一方面则意味着不同强制性的侦查行为之间在程序控制的强弱上应当有所区分。此外，精细化的强制性衡量也意味着对于侦查措施的程序性控制是个案判断，这就为辩方的介入提供了空间，同时也使得中立评价者的参与成为必要。

---

① 参见郑曦：《刑事诉讼个人信息保护论纲》，载《当代法学》2021年第2期，第115－124页。

② 参见谢登科：《非法电子数据排除的理论基点与制度建构：以数字权利的程序性救济为视角》，载《上海政法学院学报（法治论丛）》2023年第3期，第62－80页；梁坤：《论初查中收集电子数据的法律规制——兼与龙宗智、谢登科商榷》，载《中国刑事法杂志》2020年第1期，第39－57页。

③ 参见裴炜：《比例原则视域下电子侦查取证程序性规则构建》，载《环球法律评论》2017年第1期，第80－95页；秦策：《刑事程序比例构造方法论探析》，载《法学研究》2016年第5期，第153－170页。

④ 参见［日］田口守一：《刑事诉讼法》（第7版），张凌、于秀峰译，法律出版社2019年版，第55页。

⑤ 参见裴炜：《论个人信息的刑事调取——以网络信息业者协助刑事侦查为视角》，载《法律科学（西北政法大学学报）》2021年第3期，第80－95页。

三、制度回应的视角切换：基于透明性的全流程控制

传统刑事诉讼法对于侦查行为的规制更多聚焦于行为端口，例如令状主义强调的是通过司法审查来事前限定侦查活动的时间、地点、范围等，从而合理控制侦查行为。[①] 考虑到侦查是一个过程，在实施过程中是否超出令状范围则需要进一步的监督机制，而笔录类证据、情况说明材料、同步录音录像、见证人制度等能够在一定程度上发挥过程监控的功能，[②] 并构成后续判断证据合法性的关键依据。当前侦查数字化的规定部分沿用了传统的规制思路，例如针对电子数据的收集提取，《电子数据规定》第 14 条列举了制作笔录、见证、录像等用以记录取证过程的方式，尽管从立法表述上看其功能主要在于保障电子数据的完整性与可靠性，但对于规范取证过程仍具有积极意义。

但是，侦查行为数字化的逻辑转换强化了我国传统侦查制度的固有缺陷。第一是在原本令状主义就较为薄弱的情况下，进一步规避了某些受到严格事前控制的侦查行为，典型如电子数据取证中以“提取”取代“搜查”，不仅模糊了取证行为的法律性质，也回避了搜查令这一程序控制机制。第二是将物理空间的侦查行为直接延伸至虚拟空间，例如对于原始存储介质进行扣押时，扣押行为直接扩展至其内部的电子数据，尽管数据与载体承载的公民权益存在差异，但后者不再适用单独的审批程序。第三是对于以大数据或人工智能技术为基础的侦查行为缺乏有效的规制手段，例如数据分析报告是否构成启动侦查程序的法定条件，目前立法并未提供明确的指引。

在上述三方面的共同作用下，辩护的空间被压缩，前文论及的权利导向难以真正落地。对此，有必要破除网络空间侦查行为法律规制的“名实不符”的情况，将权利保障从形式穿透至侦查行为内部和全流程。

（一）合理规制侦查行为的嵌套

当前刑事电子证据规则普遍存在某一侦查行为嵌套其他侦查行为的情形，即仅着重规制前行为，对于后续关联侦查行为不再单独设置程序启动条件，例如在对电子数据的原始存储介质进行扣押之后，对介质内部数据的提取分析不再归入面向外部的“收集提取”，而是转入侦查机关的内部“检查”。[③]

这种侦查行为相互嵌套的模式承袭了传统物理场域的规制思路。我国刑事诉讼法本身对于附带侦查行为的规制就相对有限，例如对于扣押邮件、电子邮件、电报等信息载体时，自然而然地就拓展至其内容的搜索、检查，后者未再设置单独的适用条件；[④] 又如在执行拘留、逮捕时，针对犯罪嫌疑人、被告人人身的强制措施可以在特定情形下无需搜查证，直接附带针对该人人身的搜查措施，同时该搜查行为又可以不经审批直接附带对随身物品的扣押措施，从而形成一个附带行为链条。[⑤]

上述规定主要基于两方面的考量。第一是在物理场域中，附带侦查行为的客体相对有限，因而所承载的公民基本权利也相对有限，附带行为本身的权利干预性较弱。第二是考虑到情况的紧急性，例如证据可能损毁灭失、随身凶器可能威胁侦查人员人身安全、国家或社会公共利益以及公民

① 参见李世阳：《令状主义的例外及其限制》，载《政治与法律》2020 年第 4 期，第 81－98 页。

② 参见陈瑞华：《论刑事诉讼中的过程证据》，载《法商研究》2015 年第 1 期，第 81－91 页；谢小剑：《讯问录音录像的功能发展：从过程证据到结果证据》，载《政治与法律》2021 年第 8 期，第 149－161 页。

③ 根据 2019 年《电子数据规定》，对已扣押的原始存储介质中的电子数据进行检查，被规定在“第三章电子数据的检查和侦查实验”之中，与第二章所规定的一系列收集提取措施相区别。

④ 参见《公安机关办理刑事案件程序规定》第 232 条第 1 款。

⑤ 根据《公安机关办理刑事案件程序规定》第 224 条，这些情形主要包括：“（一）可能随身携带凶器的；（二）可能隐藏爆炸、剧毒等危险物品的；（三）可能隐匿、毁弃、转移犯罪证据的；（四）可能隐匿其他犯罪嫌疑人的；（五）其他突然发生的紧急情况。”

重大人身、财产权益可能面临即时性的危险。上述两方面的考量划定了可附带侦查行为的范围，其遵循的是不附带为原则、附带为例外，且这种例外应是个案判断。

在虚拟场域中，上述考量并不必然成立。首先，数据载体的物理体积并不直接对应其内部的数据体量，例如日常所用的手机内部可能存储海量数据。其次，虚拟场域中数据海量、复杂、多样，其承载的权益类型和性质远远超出了传统附带载体的有限性；对于数据的搜索、检查、分析可以对数据主体形成深刻且全面的画像，进而严重干预公民的隐私或通信自由，权利的干预性并不亚于其所附着的主侦查行为。再次，并非所有案件都具有紧急情况，例如犯罪嫌疑人随身携带的手机，很难被解释为“凶器”从而威胁到侦查人员的人身安全，其中的数据也并不经常面临即时损毁、灭失风险。①

在这个意义上，脱离个案审查而进行的常规化的侦查行为嵌套，是在套用物理场域规制框架时对虚拟场域的侦查行为进行了过于简化的处理，实则不再强调权利保障基础上的合法性判断，因而也缺乏必要的可抗辩与可救济的程序性规定。对此，有必要将附带侦查行为从常规化回归到个案化，侦查行为的分别规定、启动和实施是原则，仅在特定情形中允许有限的附带。具体而言，此次《刑事诉讼法》修改需要对已有制度做几个方面的调整。

第一是避免直接套用传统侦查规定，例如数据冻结的功能主要在于证据保全，传统冻结中适应财产保全目的的规则就不适宜套用在数据冻结之上。《公约》单独规定了“已存储数据的快速保全”措施，并鼓励各国之间在该措施方面开展国际合作，考虑到后续《公约》签批和转化，我国《刑事诉讼法》宜在第 144 条规定的“查询、冻结”项下增设“电子数据保全冻结”一款，其适用应当主要针对数据面临紧迫且现实的损毁灭失风险的情形。

第二是区分针对物理载体的行为与针对数据的行为。目前比较典型地规定了附带行为的是《反间谍法》第 24 条，该条授权国家安全机关在检查身份时对有嫌疑的人员“可以查看其随带物品”，这种概括性授权主要是出于国家安全这一领域的特殊性。在普通刑事案件的侦查中，仍然应当以二者分别规制为原则，前者附带后者为例外。对此，宜在目前《刑事诉讼法》第 136 条规定的搜查措施的适用对象中补充“载体、系统、以及其中存储或处理的数据”。

第三是明确针对数据的侦查行为的性质和类别，例如以搜查代替当前性质不明的“提取”等措施，从而对数据主体的隐私权予以保护；又如将持续占有或控制数据的侦查行为定义为“扣押”，从而规范数据提取之后的相关处理行为。同时，考虑到搜查、扣押可能面临的诸如加密技术等方面的障碍，结合我国《网络安全法》等相关法律中规定的第三方主体的协助和配合义务，《刑事诉讼法》在修订搜查、扣押措施时，应当明确规定有关人员提供必要信息或技术协助的义务。

（二）明确“紧急情况”与“有碍侦查”

在侦查过程中，“紧急情况”与“妨碍侦查”是侦查机关豁免告知义务的常见事由，前文提及的执行拘留、逮捕中的附带性搜查就是典型例证。同时，这两项事由也形成控辩双方判断侦查行为合法性的重点交锋区域；侦查行为能否控制在合理范围内，很大程度上取决于这两项事由的界定。

与侦查行为相关的数字法律规范中，已经有条款涉及“紧急情况”与“有碍侦查”，例如《个人信息保护法》中关于国家机关处理公民个人信息时告知义务的豁免，设置了“法律、行政法规另有规定”（第 18 条第 1 款）、“紧急情况”（第 18 条第 2 款），以及“妨碍履行法定职责”（第 35 条）三种情形。考虑到《刑事诉讼法》中并不存在对告知义务的概括性豁免，后两者成为告知义务能否在个案中减免的判断重点。

① 参见陈永生：《刑事诉讼中搜查手机的双重司法审查机制》，载《北京航空航天大学学报（社会科学版）》2022 年第 2 期，第 34－37 页。

当前《刑事诉讼法》中有部分条款涉及“紧急情况”与“妨碍侦查”，前者如紧急情况下的无证搜查（第 138 条第 2 款），后者如拘留后不通知家属（第 85 条第 2 款）、适用指定居所监视居住（第 75 条第 1 款）等。结合相关规范性文件，“紧急情况”与“有碍侦查”的核心内容均主要指向人身保全和证据保全。其中，人身保全主要指向的是犯罪嫌疑人或其同案犯可能自残、自杀、逃跑，或者面临人身危险；证据保全主要指向的是毁灭或伪造证据、干扰证人作证、串供等情形。[①] 同时，二者均为个案判断。

二者的主要区别在于三个方面。首先，“紧急情况”最核心的要素在于紧迫性，不立即采取措施则可能导致损害后果的发生，这是“有碍侦查”所不要求的。其次，“紧急情况”的“紧迫性”在人身保全与证据保全之外，还会涉及国家利益、社会公共利益，以及公民人身及财产安全，也正是在这个意义上，《个人信息保护法》第 18 条在规定紧急情况暂缓告知时，将其进一步表述为“为保护自然人的生命健康和财产安全”。再次，二者对于侦查行为条件的豁免程度和方式不同。“紧急情况”并不实质性改变侦查人员的程序义务，而仅仅是将相关义务从事前延后至事中或事后。换言之，侦查人员在根据“紧急情况”便宜地开展侦查行为的同时，也需要尽早履行程序义务，该义务不以“紧急情况”是否仍然存在为条件，而是在侦查资源许可下立即履行。相较而言，“有碍侦查”则有可能导致侦查人员程序义务的减免，原则上在妨碍情形消失后，侦查人员仍需履行相关义务；如果妨碍情形实质性地不可消除，则可能导致程序义务的变通履行乃至彻底免除。[②]

从侦查数字化的逻辑出发，未来会有众多侦查行为牵涉到“紧急情况”与“有碍侦查”的判断，典型如以下三种场景。第一是涉及处理个人信息的告知义务，这是《刑事诉讼法》与《个人信息保护法》相衔接所必须回应的问题，概括性的侦查保密原则显然无法再为此提供充分的法律依据。[③] 第二是涉及电子数据的保全，考虑到此类证据全球快速流转和易损毁灭失的属性，诸如冻结等前置性的保全措施的重要性会不断提升。第三是涉及跨境数据取证，基于传统国际刑事司法协助机制的复杂性与冗长，诸如侦查机关直接取证或通过第三方调取等变通性措施也会更为普遍，而“紧急情况”则会为其提供必要的正当性基础。

有鉴于此，此次《刑事诉讼法》修改有必要就具体侦查行为补充必要的“紧急情况”与“有碍侦查”例外，以此统筹规范传统侦查与数字侦查所面临的各种需要特殊处理的情形。具体而言，在调取、搜查、扣押等具体涉及第三方协助收集、提取个人信息的侦查行为中，增设两种情形下协助方的保密义务，从而与《个人信息保护法》第 18 条和第 35 条相衔接：第一是告知可能有碍侦查的情形；第二是自然人的生命健康和财产安全面临紧迫且重大的损害风险的情形。

（三）穿透性的算法规制

数字侦查全流程规制不仅需要从外部关注侦查行为的界分，还需要深入到具体侦查行为内部，应对大数据、人工智能等技术应用过程中形式合法性背后的实质合法性缺失的问题。这就要求对于数字化的侦查行为进行穿透性规制，其既依赖于侦查机关自身对于所应用的数字技术的控制，同时

---

① 根据《公安机关办理刑事案件程序规定》，“有碍侦查”主要适用于羁押或监视居住中不许辩护律师会见（第 52 条第 5 款）、适用指定居所监视居住（第 111 条第 2 款）、拘留后不予通知家属（第 127 条第 3 款）这三种情形，尽管三者关于何为“有碍侦查”的解释略有差异，但总体上仍然指向的是人身保全与证据保全两个事项。“紧急情况”的表述同样多次出现，例如口头传唤（第 125 条第 2 款）、拘留逮捕暂缓通报政协（第 168 条）、现场讯问（第 198 条第 1 款）、无证搜查（第 224 条）、边控措施（第 278 条第 2 款）等。相较于“有碍侦查”，上述条文对于“紧急情况”的内涵缺乏必要的说明，仅在无证搜查部分列举了一些具体情形。

② 从这个角度讲，《个人信息保护法》第 18 条第 2 款规定的“紧急情况消除后及时告知”的表述实际上并不准确，将“紧急情况”与“有碍侦查”混淆规定了。

③ 相关探讨参见裴炜、张桂贤：《论刑事诉讼中个人信息保护的知情规则》，载《成都理工大学学报（社会科学版）》2022 年第 4 期，第 50－62 页。

也更为依赖于外部的审查与监督，而这些都需要通过规则转换才具有现实意义。

就侦查机关对数字技术的控制而言，当前用于刑事诉讼的数字技术是否在其底层逻辑上与其他领域有本质区别，本身存在疑问；而这些数字技术尽管在不断提供更为个性化的服务，但其本身实际上并不关心真实自然人的个体实际情况。① 如同数字产品的普通用户一样，侦查机关并不必然熟悉相关技术原理，而相关核心技术也受到知识产权保护。② 在此背景下，侦查机关实则难以自行判断数字技术的可靠性以及与犯罪侦查场景的匹配性，而国家和社会关于数字技术赋能犯罪侦查的整体想象又会持续迫使侦查机关采用其并不熟悉的技术产品，③ 两相结合实际上在削弱侦查机关的专业判断以及以此为基础开展侦查行为的合理性。④

对此，需要将技术审查向事前推进。第一是刑事司法领域的数字技术开发需将数字无罪理念纳入其中，并以专门性的国家和行业技术标准为评测依据。第二是在应用具体数字技术之前，特别是在该技术应用可能干预相对人合法权益时，侦查机关需要考量该技术与具体案件在时、空、人等要素上的匹配度，并就技术应用和更新做出事前的影响性评估。⑤ 第三是技术开发者与作为技术应用者的侦查机关需要在事前明确该项技术的可靠性，包括对于模型训练数据、训练方法、适用场景、错误率等事项的说明，应当纳入可被查阅的卷宗之中。上述三方面将构成后续关于侦查行为正当性审查的重点。

就外部主体对侦查数字技术的监督而言，其核心在于审查数字推论的合理性与正当性，这主要依赖于三方面的思路转变。

首先，数字技术应用所形成的事实认知应当同步纳入传统诉讼程序条件的考量因素之中，由此形成二者的同步转变。这意味着在后续司法审查过程中，一方面，司法机关对于数字侦查的审查不应仍延续物理场域和小数据的思路，而是需要将传统刑事诉讼中的“嫌疑”“合理怀疑”“社会危险性”“人身危险性”等概念同步拓展到大数据等相应的数字技术；另一方面需要在评价时将根据基于更广泛社会群体或行为特征所形成的评价回归到相对人本身，建构起由大数据回归到小数据、数字人回归到自然人的考察路径。

其次，针对侦查机关应用数字技术的有效控制也依赖于辩护职能的充分发挥。在控辩数字能力不平等的背景下，辩护的有效性需要以强化控方的披露和说明义务为条件。基于此，数字技术应用如果产生干预相对人基本权利的效果，则关于该技术的原理说明、应用说明、影响性评估等均应当涵盖在阅卷权的范围内；同时控方应当就所用技术的错误率等其他可能有利于辩方的事项进行主动披露和说明。

再次，外部监督的闭环需要引入获得合理推论的权利。数字侦查的外部监督不仅需要关注技术入口，还需要在出口上予以规制，后者主要针对基于数据分析所形成的针对具体相对人的具体推论，而这恰恰是目前包括刑事诉讼法和新兴数字法均关注较少的事项。⑥ 获得合理推论的权利旨在

---

① See Alberto Romele, *Digital Habitus: A Critique of the Imaginaries of Artificial Intelligence*, New York: Routledge, 2024, p. 4.

② See Rebecca Wexler, “Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System”, *Stanford Law Review*, Vol. 70, No. 5 (2018), p. 1343.

③ See Federal Judicial Center, “An Introduction to Artificial Intelligence for Federal Judges”, *Federal Judicial Center*, February 13, 2023, https://www.fjc.gov/sites/default/files/materials/47/An_Introduction_to_Artificial_Intelligence_for_Federal_Judges.pdf, last visited at July 19, 2024.

④ See Anna Lvovsky, “Rethinking Police Expertise”, *The Yale Law Journal*, Vol. 131, No. 2 (2021), p. 475.

⑤ See Hannah Bloch-Wehba, “Visible Policing: Technology, Transparency, and Democratic Control”, *California Law Review*, Vol. 109, No. 3 (2021), p. 973.

⑥ See Sandra Wachter & Brent Mittelstadt, “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI”, *Columbia Business Law Review*, Vol. 2019, No. 2 (2019), p. 495; see also Margot E. Kaminski and Jennifer M. Urban, “The Right to Contest AI”, *Columbia Law Review*, Vol. 121, No. 7 (2021), p. 1957.

填补这一制度空缺，是从控辩平等武装角度出发，通过赋权来强化辩方的数字对抗能力，其对应上述事项中涉及的各类公安司法机关的主动披露和说明义务，同时也构成事后相对人挑战数字推论以及依此实施的侦查行为的基础。①

四、制度回应的生态适应：纯国内法视角向涉外法治拓展

犯罪的全球化需要全球化的犯罪治理予以应对。近年来，我国针对涉外电信网络诈骗等犯罪发布了众多典型案例，② 相关规范性文件也频繁谈及跨境追诉问题，已然反映出跨境侦查取证在整体犯罪治理中的重要性。相较于境内犯罪侦查，跨境侦查面临着更为复杂的外部环境，本国制度建设在这一场景中主要发挥三方面功能：第一是提供合法性基础，这是实施任何侦查行为的前提，跨境场景亦不例外；第二是建构行为边界，特别是建立起侦查行为在权利保障基础上的合比例性体系；第三是划定行为底线，这是达成网络空间犯罪治理国际共识、强化国际合作的基础。

当前刑事诉讼法主要采用的是国内法视角，对于涉外犯罪追诉的规范建设明显不足，这也形成了司法实践中跨境犯罪侦查取证的制度障碍，不仅无法对具体侦查行为提供必要的合法性依据，也会进一步影响到基于该侦查行为获取到的证据材料在后续诉讼程序中的证据能力和证明力，同时还会阻碍中国的治理经验向国际规则的转化。对此，数字时代的刑事诉讼法需要对跨境犯罪追诉做出积极回应，以适应网络空间跨境侦查取证的现实需求。

（一）整合跨境犯罪侦查规则

针对跨境犯罪侦查取证，当前我国《刑事诉讼法》仅在第 18 条规定了国际刑事司法协助这一种机制，《国际刑事司法协助法》以及《关于实施〈中华人民共和国国际刑事司法协助法〉若干问题的规定（试行）》（下文简称《司法协助法实施规定》）进一步明确了其实施程序。但是，除国际刑事司法协助以外，我国通过下位法已建立起其他跨境侦查取证机制，这些机制同样应当整合到跨境侦查的总体制度体系之中。

第一是补充国际间警务合作机制。根据《公安机关办理刑事案件程序规定》，除《刑事诉讼法》第 18 条规定的国际刑事司法协助以外，我国公安机关可以和外国警察机关开展警务合作（第 13 条），合作事项包括但不限于确认外国籍犯罪嫌疑人身份（第 360 条）、犯罪情报信息交流合作、调查取证、安排证人作证或协助调查、涉案财物处置、诉讼文书送达、被追诉人引渡、缉捕、递解等（第 375 条）。同时，边境地区公安机关还可以按照管理开展情报信息交流等日常化的警务合作（第 376 条）。可以看到，警务合作涵盖的范围与国际刑事司法协助相近，但其可以通过国际刑事警察组织这一国际平台更为高效地开展跨境犯罪侦查工作，是国际刑事司法协助机制的必要补充。

第二是系统性规制具体侦查行为的境外适用。如前所述，当前我国多数电子取证措施并未区分境内或境外适用。但借由弱地域性的网络空间，这些措施不仅容易产生涉外效果，有些甚至对于跨境取证具有重要作用，例如数据冻结可以在快速保全证据材料的同时，尽可能弱化跨境取证对他国主权的干预程度；远程勘验则是明确目标数据所处位置不可或缺的前置性措施；而向网络信息业者等第三方主体调取境外数据有时是获取境外证据材料的唯一方式。

由此出发，在明确侦查行为类型的基础上，需要进一步划分同一侦查行为的境内与境外适用。

① 关于获得合理推论权的论述，参见裴炜：《论刑事诉讼中的算法推论及其规制》，载《安徽师范大学学报（人文社会科学版）》2022 年第 6 期，第 107－115 页。

② 典型如 2024 年最高人民法院发布的跨境电信网络诈骗及其关联犯罪典型案例。

首先，涉及跨境的侦查行为无论在适用条件、审批程序、实施程序、权利保障等要素上均需要与该行为的境内实施加以必要区分，从而在尊重国家主权与保障侦查效率之间形成平衡。其次，相关规制需要考虑到跨境场景中可能出现的紧急情况，在遵守严格的适用条件和程序的前提下，在国际刑事司法协助与警务合作之外，补充设置紧急情况下的直接跨境取证机制，并建立起各类机制之间的衔接程序。再次，考虑到境内外刑事诉讼制度的差异性，需要统一规定不同机制下境外取证获得的证据材料在后续刑事诉讼程序中的可采性。

基于上述考量，此次《刑事诉讼法》修改需要针对涉外犯罪追诉的实践需求予以系统性回应，主要涉及《刑事诉讼法》两个部分的条款变动。

第一部分是总则的第 18 条，具体涉及以下三方面的事项：一是增加国际间警务合作，具体的警务合作程序仍然可以交由公安部规定予以细化；二是增加紧急情况下的直接跨境取证条款，一方面需要有条件地确认善意情况下的跨境侦查取证行为的正当性，另一方面对于远程勘验等可以用于明确目标数据位置的具体措施，在直接跨境取证上予以必要的容许；三是增设 24/7 全天候联络机制条款，主要功能在于与《联合国打击网络犯罪公约》的国际合作章节相衔接，以提升未来国际间开展网络犯罪跨国追诉的合作便利性。

第二部分是在侦查章节中，需要针对具体侦查行为的管辖权范围予以明确：一是区分数据调取措施适用的相对人类型，针对自然人的数据调取应当要求该人位于我国境内，针对网络服务提供者等企业主体的调取，则适用于在我国境内提供服务的相对人；二是明确搜查、扣押的对象应当是位于本国境内的系统、载体，以及其中存储的数据；三是针对技术侦查中的动态数据的实时收集，应当限于在我国境内传输的数据。

（二）均衡设置第三方主体的协助义务

网络信息业者等第三方主体所具有的数据和技术优势，使其在犯罪治理中的作用和协助义务不断强化。这一点在跨境场景中尤为明显，一国侦查机关因执法管辖权的地域限制而难以直接开展境外取证时，向占有或控制目标数据的第三方主体调取该数据就成为化解上述制度障碍的重要途径，这也成为当前国际层面相关制度探索的重点。

从我国当前制度状况来看，我国刑事诉讼法原本对于调取的规定就相对简单，调取电子数据缺少必要的程序控制。同时，《国际刑事司法协助法》第 4 条第 3 款原则上禁止本国单位、组织和个人自愿协助外国执法机关，基于平等互惠原则，该规定也适用于我国侦查机关向外国网络信息业者调取数据的情形，这与司法实践情况并不相符，例如根据微软的《执法请求报告》，微软每年都会收到来自中国执法机关的涉刑事案件数据调取申请。[①] 此外，跨境数据处理是新兴数字立法的关注重点之一，而《个人信息保护法》《数据安全法》等法律中关于跨境数据流动和数据调取的规则尚未与刑事诉讼规则形成良性互动。

上述情况在一定程度上导致现有规范与实践操作相脱离，不仅使得调取等相关侦查行为处于立法的灰色地带，也进一步导致第三方主体在协助侦查中的义务边界模糊。在跨境取证的场景下，这种模糊性可能导致第三方主体面临合规困境，例如遵守一国协助侦查义务而提供境外数据的行为，可能与数据所在国基于个人信息保护、数据安全等事由而设置的数据处理限制规定相违背，而违反任意一者均可能引发相应的法律责任。

基于此，考虑到第三方主体在跨境侦查中的地位和作用不断强化，有必要从以下方面完善《刑

① See Microsoft, "Law Enforcement Requests Report", *Microsoft*, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report, last visited at July 25, 2024.

事诉讼法》中的相关制度。

第一是明确调取在境外适用的正当性、范围与条件，原则上针对本国或者在本国开展业务的网络信息业者来说，所调取的数据范围和类型应当与《数据安全法》《个人信息保护法》等所确立的数据分级分类和出入境要求相协调，调取应当事前明确其范围、作用、限制、使用方式等要素，同时就相关数字法项下诸如告知等义务的减免作出具体规定。

第二是适当允许网络信息业者在诸如纯本国案件、紧急情况等特定情形下自愿协助他国侦查机关，或者设置程序便宜的快速协助通道。根据《司法协助法实施规定》，我国境内机构、组织、个人收到外国执法机关的直接协助请求后，不能自行提供协助，而是需要向工作机制办公室做书面报告，能否提供、以何种方式提供，则由该办公室会商后决定（第 13 条）。这一流程缺乏明确的响应及会商期限，总体上难以保障运行效率。在特定条件下适当允许自愿协助，一方面可以为我国侦查机关寻求他国网络信息业者协助留下空间，另一方面也能够提升跨境数据取证的效能。对此，一方面需要在《刑事诉讼法》第 18 条中对自愿协助的情形予以规定，另一方面需要同步修订《国际刑事司法协助法》第 4 条第 3 款，从而为此种制度设计留下空间。

第三是针对我国侦查机关在调取境外数据时调和网络信息业者面临的国内外法律义务冲突，建立相应的冲突应对程序。一方面，需要允许网络信息业者基于法律义务冲突等事由提出抗辩，并就该抗辩设置相应的受理、评估、决定、救济程序，期间原则上应当暂停协助调取义务的履行。另一方面，针对该法律义务冲突，应当建立起与他国有权机关的及时沟通机制，该机制可以纳入已有双边协议之中，也可以利用国际组织等平台开展。

（三）推动国内规则转化为国际规则

网络空间跨境侦查取证的普遍化，促使各国之间的法律碰撞日益频繁，一方面，一国国内法可能对他国国家、社会、组织、个人的权益产生切实影响，而平等互惠原则也意味着各国需要强化共识并提升侦查程序的契合度。基于此，国际规则的协同制定成为当前世界范围内网络犯罪国际治理合作的重点之一。

《公约》是第一份由中国积极推动形成的具有国际法效力的网络空间治理规范性文件，是中国深度融入网络空间国际治理新秩序建构、提升中国网络空间治理国际话语权和影响力的重要机遇。2023 年最高人民检察院发布《关于加强新时代检察机关网络法治工作的意见》，其中特别强调“积极参与网络空间国际治理”，提出“积极参与《联合国打击网络犯罪公约》的谈判，提出和阐释我国推进网络空间法治化的理念和做法”。[①] 聚焦在侦查领域，则主要需要考虑以下方面的事项。

第一是程序性措施的适用范围。我国当前关于数字侦查程序的创新，许多是与特定类型的网络犯罪治理相绑定，这与《公约》目前采用的实体法与程序法范围分立的思路存在差异。《公约》之所以采用了“使用信息和通信技术系统实施的犯罪”这一表述，即在于观察到并非仅某些类型的犯罪会牵涉到网络和数字技术，而犯罪的普遍触网化需要普遍化的数字侦查行为予以应对。这也进一步强化了我国此次《刑事诉讼法》修订时全局性、综合性、系统性整合数字侦查规则的必要性。

第二是数据类型化基础上的数字权益保障。《公约》中程序性规则建构的基础在于人权保障，其中尤为重要的是对新兴数字权益的保障，核心思路是以不同数据类型为基准配置相应强度的侦查行为。《公约》采用了注册人信息（subscriber information）、流量数据（traffic data）、内容数据（content data）的分类，与我国目前的数据分类差异较大。后续数字侦查规则在构建过程中，需要

① 参见最高人民检察院：《关于加强新时代检察机关网络法治工作的意见》，载最高人民检察院官网 https://www.spp.gov.cn/spp/xwfbh/wsfbt/202304/t20230418_611553.shtml#2，2024 年 7 月 26 日访问。

充分考虑两套数据分类间的对应关系，内容数据大致可归入通信秘密和隐私信息，而注册人信息和流量数据则可能同时涉及一般个人信息和敏感个人信息。

第三是两套规范中侦查行为的对应性。《公约》基本上建立起了针对电子数据的取证措施体系，包括快速保全、调取、搜查、扣押、实时收集、内容监听等。考虑到各国法律差异，《公约》整体上采用了功能等同的立法思路，这就需要我国在系统梳理侦查行为类型的基础上，建立起本土侦查行为与《公约》侦查行为的对应关系。

第四是侦查行为的正当程序限制。国家间在刑事侦查程序上的差异性有其深刻的本土渊源，因此各方合作的基础不在于统一刑事侦查规则，而在于达成底线共识。正当程序正是这一共识的核心。据此，《公约》第 24 条针对侦查取证等程序行为提出了一系列基础条件和保障措施，例如遵守比例原则、司法机关等中立机关的独立审查、权利获得有效救济、具备正当性依据、设置范围或期限限制等，并特别强调对第三方合法权益的保护。目前这一条文已经获得成员国的一致认可，未来也将成为我国参与网络空间打击犯罪国际合作的制度基础，因此同样需要在我国侦查制度的调整中予以充分体现。

结　论

社会治理正在高速步入数字时代，一方面，任何一门部门法都面临着转型的任务；另一方面，新兴数字法也不能全然超脱传统部门法而另起炉灶。对数字时代犯罪治理做出积极且系统化的回应，是此次《刑事诉讼法》修改应当承担的任务，也是其所面临的严峻挑战之一。此次修法涵盖面广、所涉事项众多，不可能也不需要对数字侦查的各方面制度设计均予以考量，一些具体规则可以留到后续的下位规范性文件中予以进一步明晰。但是，此次修法至少需要完成以下四方面的任务：第一是理清侦查行为的内部架构，以权利为导向、以比例原则为主线明确其中的阶层关系；第二是为新技术发展留有必要的空间，避免后续因为技术更迭而反复突破前述架构；第三是搭建好与相关法律规定的衔接桥梁，特别是协调与新兴数字法的关系；第四是引入涉外法治视角，结合当前国际层面对于中国具有影响力的立法进程，对涉外侦查行为制度进行体系化设计。

（责任编辑：魏晓娜）

exercised with caution. Self-preferencing by platforms is the product of platform organization and internal power structuring, and essentially represents the improper exercise of digital private power. As an external regulatory tool for platforms, anti-monopoly law has deficiencies in terms of application premises, conditions, and effects when dealing with self-preferencing by platforms. Self-preferencing by platforms violates the obligation of platform neutrality and falls under the category of presumed fault liability, with its illegality requiring individual case judgments based on the principle of proportionality. In making specific judgments, it should be differentiated into resource allocation type self-preferencing and order maintenance type self-preferencing, which leads to different judgment standards. Starting from the essence of the abuse of private power in self-preferencing by platforms, comprehensive regulation can be achieved through the coordination of systems such as procedural settings, granting of merchant rights, democratization of internal platform decision-making, strengthening of platform's main responsibility, and infringement liability and administrative penalties at the pre-event, in-event, and post-event stages.

Key Words Digital Private Power; Self-preferencing; Platform Neutrality Obligation; Tort Liability; Anti-Monopoly Law

Huang Shaokun, Ph.D. in Law, Lecturor of Wuhan University Law School.

The Logical Transformation and Institutional Response to Criminal Investigation Procedures in the Digital Age *PEI Wei · 40 ·*

The digital transformation of crime and crime governance is profoundly altering the intrinsic logic of criminal investigation procedures. The concept of "suspect" is being reconstructed, the scope of investigation targets is quantitatively expanding, the extraterritorial nature of investigative actions is continuously strengthening, and investigative powers are being increasingly diluted with the deep involvement of private entities. Against the backdrop of the state's initiation of a new round of amendments to the Criminal Procedure Law, adopting a codified approach to legislative amendments necessitates systematic adjustments to investigative procedures to align with the evolving logic of digital investigations. Consequently, the adjustment of the investigation system should follow the general path of returning from a technology-oriented to a rights-oriented approach, adopting a penetrating full-process control perspective, and addressing the globalization of crime governance through the introduction of international legal principles.

Key Words Digital Investigation; Rights-Oriented Approach; Full-Process Control; Foreign-Related Rule of Law

Pei Wei, Ph.D. in Law, Professor of Beihang University Law School.

Doctrinal Analysis of the Exemption Clauses for the Crime of False Issuance of VAT Special Invoices *CHEN Xingliang · 56 ·*

Article 10 Clause 2 of the Interpretation by the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Tax Evasion establishes exemption clauses, excluding from the scope of the crime of false issuance of VAT special invoices those acts that are not committed with the purpose of defrauding state taxes and do not result in actual tax losses to the state. This provision restricts the constitutive elements of the crime from both the purpose and result dimensions. Purpose Restriction: The exemption clause characterizes the crime as a non-statutory purpose crime by requiring the subjective element of "intent to defraud state taxes." This represents a substantive reasoning approach that incorporates purposive analysis into the constitutive elements of the crime. Result Restriction: The clause mandates that the crime must result in actual tax losses caused by the use of the falsely