AI 犯罪前瞻及人工智能侦查系统构建

■ 聂江波

摘　要　人工智能用于犯罪和侦查已然成为一种技术趋势。犯罪的 AI 化以及 AI 犯罪对总体国家安全、新型犯罪治理均构成系统性风险挑战。“时空－信息－数据－人机”的重新组合，将变换出新型多样的犯罪形态和侦查模型，解决的关键在于技术、信息、合成、流转的畅通与共享，从而达到更多层级、更快速度、更高效能、更加精准的响应、协同、研判与行动。在此背景之下，人工智能侦查也就应运而生。

关键词　人工智能　ChatGPT　AI 犯罪　AI 侦查系统

ChatGPT 的出现预示着全新智能时代的来临。人工智能技术在犯罪和侦查领域交叉融合所产生的复杂性和不确定性势必衍生和传导出一系列连锁反应，由此带来的犯罪挑战和技术风险足以颠覆和促使整个社会结构和运行逻辑发生改变，人工智能用于犯罪和侦查已然成为一种技术趋势。从物证、信息、数据到智能的迭代演进中，AI 犯罪与人工智能侦查终将站在时代科技的聚光灯下，成为新型犯罪研究和智能侦查探索的最前沿。

一、人工智能时代的科技前沿

人工智能（Artificial Intelligence）是指一台人造机器如能具备“像人一样思考，像人一样行动，合理的思考，合理的行动”的能力与特征，便可称之为人工智能，英文缩写为 AI。“智能”是对未来做出预测以及能够解决复杂问题的能力。AI 就是通过机器来展示这种能力，如智能软件、无人驾驶或聊天机器人。现代无人化趋势和数字化图景由人工智能技术支撑和实现，如无人超市、无人书店、虚拟认证、智能识别都是基于信息数据获取的“无人似有人”的技术能力，高级阶段则能达到“无人胜有人”的速度、效率和体验。从家庭陪伴、工作支持到警务任务，只要获得需要的数据，算法就可以按人们要求的速度做任何能够被写成编码的事

作者：中国人民公安大学侦查学院讲师

本文系中国人民公安大学侦查学双一流专项（2023SYL02）研究成果。

务，并在设计框架内执行所确定的任务。算法的有效性通过“大数据”不断得到提升，大量关于全世界人类活动和其他进程的数据都可获得。这就使一种被称为“机器学习”的人工智能类型可以通过模式检测推断未来，而且算法在比人类表现更好。

二、AI 犯罪的挑战与理论前瞻

Al 犯罪即人工智能犯罪，是犯罪主体利用人工智能技术实施的犯罪行为。如利用 AI 技术进行窃取或恶意攻击行为，技术上称为“人工智能威胁”或“人工智能滥用”。犯罪的 AI 化以及 AI 犯罪演变对总体国家安全、新型犯罪治理及其犯罪主体认定、刑事责任划分等均构成系统性风险挑战。

（一）人工智能犯罪的现实挑战

近年来各地曝出多起人工智能诈骗案件。犯罪人运用“AI 换脸”“AI 拟声”“AI 虚拟场景”技术，“深度伪造”冒充领导、熟人、亲友“换脸”后身份转换、表情自然，声音逼真，编造事实合理急迫，受害人极易放松警惕、转账被骗。利用此技术实施诈骗成为新型网络诈骗手段，究其原因主要是一些人网络“出镜率”“发声率”较高，丰富的样本为 AI 技术合成提供了充足的面部、声音、体态、衣着等生物特征和训练“素材”。而人工智能技术的发展也使 AI 诈骗的精准性、迷惑性、隐蔽性增强。从技术上讲，只要具备“音、视、图”素材样本，就可以通过 AI 技术“换脸、拟声、变装”，深度伪造合成虚拟逼真形象，实施精准盗号、精准诈骗。

AI 犯罪使耳听眼见不一定为实，这是由 AI 犯罪的技术特性决定的：一是假脸假声技术。这种“假”是由 AI 技术模拟训练、虚拟合成出的非真实图像和声音，然而从仿真性和相似度上看，又是无限接近于“真”的。二是深度伪造技术，犯罪人利用深度学习算法伪造高仿真音视图，制作虚拟逼真工作生活场景，目前还没有针对深度伪造技术进行识别和取证的专业设备。三是数据滥用技术，犯罪人利用 AI 技术进行大规模信息搜集、挖掘关联和数据整合及不当使用，利用 AI 算法操纵用户数据和侵入个人账号用于非法活动。四是自动攻击技术，犯罪人利用 AI 技术辅助开发智能软件和网络攻击工具，生成钓鱼网站，侵入信息数据系统，破坏网络安全环境和数据运行程序。

（二）人工智能犯罪的理论前瞻

一是技术犯罪的通用性适用于人工智能犯罪。技术犯罪是利用计算机、互联网及其衍生系统、工具实施的犯罪。人工智能犯罪作为新型技术犯罪，具有技术犯罪的基本特点和通用特征。通用性是指技术、模型、算法摆脱为某一领域、行业、场景专用设计和服务的局限，应用路径和服务链接面向全行业开放共享，所达到的功率和功能是一致的。概言之，技术犯罪的基本理论和一般规律适用于人工智能犯罪。一是技术犯罪和人工智能犯罪都依赖技术，特别是新兴技术手段和装备，如移动互联、智能软件、网络爬虫、深度学习等技术，这意味着技术犯罪都具有严重的技术依赖性，随着科技发展和深度应用，包括人工智能犯罪在内的技术犯罪变化变种也会同步提速。二是技术犯罪和人工智能犯罪的工具和手段具有很高的多样性和灵活性，随着 AI 技术产品的产业化布局、市场化推广和生态化应用，其技术规避和智能对抗侦查的科技强度只会提升，AI 犯罪难以被监测和识别，取证打击的难度加大。

二是对 AI 犯罪的特殊性及其“类主体”分析发现，人工智能犯罪的特殊性源于

技术的先进性。AI 技术拥有对数据分析深度学习、模型训练、自主决策、智能交互等特点，而且支持个性化技术定制和程序开发。从技术和实践来看，人工智能犯罪可能且大概率发展出智能诈骗、网络攻击、信息窃取和破坏、滥用、篡改数据等犯罪类型。在 AI 技术参与、支撑甚至主导的犯罪过程中，犯罪主体是人还是机器？虽然由人授意利用 AI 技术犯罪，但过程中“无人化”“类人化”甚至“超人化”的自动攻击、模型操控、数据滥用等行为主体是机器而非人，作为 AI 技术载体的机器已从纯粹理性的技术工具演变为“人格化”的犯罪工具，这关乎人工智能犯罪“主体”的认定与识别。主体（Subjeckt）概念属于哲学范畴。马克思提出人的实践活动是其确立主体性的根本原则，人们从事什么样的实践活动就有什么样的主体地位。“谁”实践则“谁”为主体，因为“同活动对象的客体相反，主体是活动的承担者和执行者”。人工智能将人类的思维和知识数字化并编织算法程序来模拟人类智能，使其能够模仿人脑“从事推理、规划、设计、思考、学习等思维活动”。因此，在人工智能的技术领域和逻辑范畴内，所谓 AI 犯罪的“主体性”问题就是将 AI 犯罪活动赋予“人格化”特征，将机器视为具有相对独立思考和决策能力的“类主体”或“类行为主体”。如果可行，还将衍生出 AI 犯罪主体“人权化”等法律问题，这可能构成未来犯罪学、侦查学、法理学研究的重大技术转向。

三、AI 侦查系统的逻辑范式

技术对侦查的影响广泛而深远，信息比对、远程勘验、数字取证、智能识别，侦查的工具和路径越来越智能。犯罪和侦查固定在一个时空、一类场景、一种模式下的状态将被 AI 技术打破，“时空－信息－数据－轨迹”的人机组合，将变换出多种多样的犯罪形态和侦查模型，关键是信息、技术、信息、数据流转的畅通与共享，才能达到更高层级、更多层面、更快速度、更高效率的启动、协同、研判与行动。在强大的科技引擎助推下，继“信息化”“数据化”后，“人工智能”走进侦查已经成为必然，人工智能侦查应运而生。

（一）AI 侦查系统的底层逻辑

AI 侦查系统的“底层逻辑”涵盖数据收集、储存、分析、处理以及线索生成、预警指令、信息推送等多环节的逻辑运转。以 ChatGPT 为代表的人工智能工作原理尚不清楚，但并不妨碍其底层逻辑搭建完善。因为任何事物的发生发展都有其客观存在的背景、条件和规则来支撑事物的表现和运行。无论呈现形式多么繁杂，但本质都是简洁稳定的，这是事物发生发展的底层逻辑。从思维论上讲，它是从事物的基本构成和根本规则出发寻找和发现事物规律并解释和解决基本问题的方法论。从技术论上看，则是计算机或者软件系统中最基础、最核心的控制链路和运行规制，也可理解为系统的核心算法或数据架构。AI 侦查系统的底层逻辑一旦搭建完成并经充分测试与优化，就可为整个系统提供安全、高效且易于操控的基础支撑。

AI 侦查系统“底层逻辑”的技术原理类似搭建侦查“黑箱”“盲盒”，用数字优化求解器解决“随机规划问题”，在浩如烟海的随机解答中，寻究可行的最优解。而这就离不开经验知识、数据案例、侦查模型及 AI 算法算力，需要案例样本数据抽取和侦查模型的迭代训练，需要 AI 侦查系统算法指令与算力支撑。在实际侦查过程中，现场采集和历史积累的犯罪信息数据是海量的，

“百千万亿”级的数据信息的“随机变量”有无限种组合可能，计算机运算速度的提升打破了算法瓶颈和算力限制，使随机展开的数据信息“随机规划模型”短时间内完成，在数据组合的无穷可能性中，隐藏着一条最优解决方案。这种理论上最优方案的寻找和选取过程，就是在刑事侦查数字场景中进行“预知决策”，将“数据组合”生成新的信息指令，在无数随机解答和信息指令中寻求最优解，生成并输出最优化的数字侦查方案。

（二）AI 侦查系统的技术支撑

AI 侦查是一种依托和利用人工智能技术进行数据筛选、信息分析和犯罪侦查的智能系统，其运行逻辑整合了数据分析、决策支撑、警务应用等多项技术集成。AI 侦查系统通过智能算法和超级算力预测犯罪热点、预判侦查方向、预警高危指数、预防犯罪风险，为侦查人员提供智能精准的犯罪信息和行动决策。相比前智能时代的侦查平台，AI 侦查集成了更加智能的技术系统：

一是数据分析类技术集成，包括数据采集技术，自动采集和批量转存公安管理、社会信息和网络数据；数据清洗技术，将采集数据进行过滤，清理重复数据，补充不完整数据，去除错误数据，确保数据质量。数据预处理技术，将清洗数据进行标准化处理，按照侦查要素，如人员、案件、物品、地址、轨迹等进行整理分类；数据存储技术，将预处理的数据存储到数据集，方便应用；数据关联技术，将存储数据进行关联分析，挖掘数据之间和背后的关联与嫌疑，研判和构建侦查模型。二是决策支撑类技术集成，包括物品识别技术，智能识别作案工具或涉案物品及痕迹特征，并与犯罪数据库自动比对。通过语义分析技术分析网络数据，提取关键字词和语义关系，在对应数据库中查找线索；利用行为分析技术捕捉异常行为，粘贴数据标签，提炼作案模式，建构数据模型；依托“视频 + 数智”技术解析监控图像及视频数据，进行目标锁定、轨迹追踪与行为分析，发现涉案嫌疑线索，获取犯罪证据，为侦查人员提供决策依据和研判支撑，为侦查行动矫正技术参数和数据指向。三是警务应用类技术集成，包括人脸识别技术和步态追踪技术，用于嫌疑人身份识别和定位追踪等。自然语言处理技术用于犯罪信息收集分析和语音、声纹识别鉴定等；聚类分析技术可识别嫌疑人之间的关联性与相似度，展示数据与行为之间的关系模式；深度学习技术用于信息收集、数据分析和监测预警，结合数据挖掘技术提高侦查效率和精准度；警用无人机和侦查机器人技术通过自主探测、图像捕捉、智能识别、即时传输等技术应用，为指挥中心提供现场数据和实时信息。

（三）AI 侦查系统的设计架构

AI 侦查系统的设计与开发，需要在算力支撑下注入算法“灵魂”，使其智能系统有效“激活”。根据技术运行和逻辑路径的复杂程度不同，AI 侦查系统的设计架构要满足数据收集和存储、数据清洗和处理、数据分析和挖掘、线索生成和推送、智能识别和追踪、信息研判和预警、辅助决策与智能导侦等实战化需求。落实到技术实践中，AI 侦查系统的设计和运行包括以下步骤：

一是数据收集与存储。AI 侦查系统通过爬虫技术集中或分布式采集犯罪信息，数据来源于网站、社会等开源渠道，包括警务信息、新闻视图、网络资讯、公共服务、行业管理等数据，经过清洗、整合和标注后存储到各类数据库中，为数据分析和研判提供信息资源。二是数据分析与处理。AI 侦查系统利用机器学习和数据算法，对各类数据

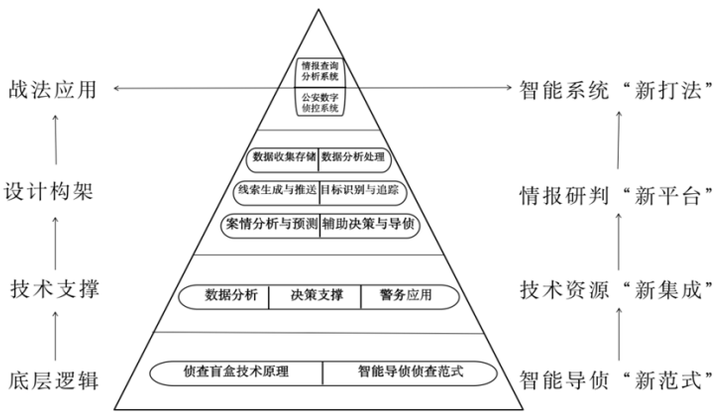

图 1 AI 侦查系统原理及应用示意图

库中的数据进行预处理，包括文本分析、图像识别、行为解读、异常标注、聚类研判等，从中抽取筛选有价信息和标签数据，为侦查线索的梳理、查证、深挖以及犯罪证据的获取、检验、证明提供数据支撑。三是线索生成与推送。AI 侦查系统根据数据分析与处理结果，智能生成侦查线索和取证指引。如通过文本分析，检索高危信息、高频词汇及追查线索；通过图像分析识别嫌疑特征，分析作案工具，研判行为轨迹。在此基础上，智能系统建立模型算法推送信息指令，循线查证取证。四是目标识别与追踪。AI 侦查系统通过人脸、指纹、声纹识别以及步态、车辆、手机定位追踪等智能技术匹配，将采集汇总的人、物、案、网、轨、迹信息与数据库中的犯罪信息、案件数据进行自动比对和关联匹配，挖掘、解析和获取涉案目标的数字 ID 认证和网络 IP 定位。五是数据标注与模型训练。AI 侦查系统整合刑事案件的案件数据，标注并抽取犯罪样本进行侦查模型训练，预测预警犯罪热力图和发展态势，如构建侦查数字模型进行信息分析研判，预测某类新型犯罪发展的高峰、拐点，解构某个具体案件的要素、物证，发出分色预警和行动指令。六是辅助决策与智能导侦。AI 侦查系统将信息研判指令呈报各级侦查人员，为其提供科学决策依据和行动指引，助其更好地研究态势、案情分析，辅助其更快地优化方案。“打防治宣”相结合，提高侦查的精度和取证的效率，减少认知误判和行动盲区，实现智能研判和精准打击。

（四）AI 侦查系统的战法应用

人工智能侦查（Artificial Intelligence Investigation）是侦查主体依法使用 AI 技术和智能工具收集证据、查明案情、确定嫌疑、证实犯罪的理论和实践体系。AI 侦查系统基于公安大数据，整合拓展多平台综合功能，嵌入式运行人工智能技术，对人、物、案、网、轨、迹等侦查要素和涉案数据进行监测预警、模型解构和智能筛查，为侦查决策提供“一键快查式”信息支持、行动指导和取证索引，实现“打防控治宣教”多维一体的数字大脑和智慧平台。AI 侦查系统从原理到应用是其底层逻辑、技术支撑、设计架构、战法应用的集成体系，涉及侦查资源重组、技术路径优化、作战平台整合与数字系统融合。如图 1 所示，AI 侦查系统的底层逻辑是智能导侦的“新范式”，技术支撑是技术资源的“新集成”，设计架构是信息研判的“新平台”，战法应用是智能系统的“新打法”。

人工智能是通过制造智能代理来实现人类智慧的各种能力。借此进行大数据分析和

样本自主训练，AI 侦查系统就能进行犯罪信息的筛选搜集、自动分析、逻辑推理和自主判断，并从海量数据中智能检索关键信息，挖掘关联数据，辅助指导侦查方案的制定和校正，提高侦查行动的效能和精度。近年来，各级公安机关顺应大数据和人工智能的技术趋势，建设信息作战系统和数据分析平台，仅公安部就建设了包括云搜索、云鉴、交通管理综合查询、刑侦专业信息系统等查询分析系统。实战中，公安数字智能侦控系统是一个安全、高效、精准的智能作战体系，基于大数据、人工智能的技术构架，可以实现数据智能分析，通过采集、整合和分析各种数据资源，对涉案人员物品的轨迹与身份进行智能辨识和自动比对，协助警方对犯罪嫌疑信息进行精准判断、轨迹追踪和认定排除。

（五）AI 侦查系统的智能范式

人工智能侦查是以信息数据为基础、算法算力为核心、智能智慧为目标的“智能导侦”新范式。其优势在于依托 AI 技术平台，自动收集、整理和研判有价值的信息数据，利用机器深度学习训练习得智能算法以及超强算力分析处理涉案数据流，通过数据挖掘、数据标签、数据建模、数据碰撞、数据画像等技术预判趋势、预警风险、捕捉异常、刻画嫌疑，为侦查活动提供精准、智能的数字线索和数据证明，减少人力产生的误判。人工智能侦查具有数据规模、智能算法、超强算力等多重特征，具备模型优化、战法增强、资源整合、效能提升等诸多优势，在数字重建、电子取证、信息研判、监测预警等方面拥有超前的智能优势。人工智能技术对侦查体制机制、资源配置、分工协作、指挥协调等也能解构与重塑，在 AI 侦查“智能导侦”新型范式面前，大楼大厅大屏时代也将结束。

未来由人工智能技术架构的“数字大脑”和“智能系统”将颠覆以往一切的信息技术和数据战法，AI 赋能的单兵作战、现场研判足以媲美甚至取代后台中心的数据比对和信息研判。靠大楼大厅大屏指挥协调的数据平台、信息系统与作战中心，本质是一种“金字塔”式的单中心警务模式，AI 侦查系统构建的是去中心或多中心的作战体系，二者的底层逻辑和运行规则之所以迥异，是由于单中心警务模式强调的是侦查资源和技术权限向上集中，这需要对技术、资源向下的多层级控制与分层级配置，但层级层次越多，资源损耗和效能衰减就越快；多中心实战化体系突出的是数字资源和智能技术的平行配置与按需使用，关键是建立数据流转和信息共享机制，开放数字授权，形成多量级、扁平化的次级中心，每个中心都能发挥协调资源、协作共享、协同行动的枢纽作用。

参考文献：

[1]【美】罗素、诺维格．殷建平等译．人工智能：一种现代的方法（第三版）[M]．2013．3

[2]【美】马蒂亚斯·里塞、张馨月．人权与人工智能：一个亟待解决的议题 [J]．2019．5

[3] 吴帅帅、刘懿德、兰天鸣．警惕！“AI 换脸”诈骗出现涉政苗头 [N/OL]．http://lw. news. cn/2023-07/03

[4] 娄延强．人工智能的伦理困境与正解 [J]．道德与文明．2022．1

[5]【美】E·丽奇．李卫华、汤怡群、文中坚译．人工智能引论 [M]．1986．1

[6] 梁坤、周韬．当前人工智能侦查的应用困境及突破进路 [J]．山东警察学院学报．2018．3

[7] 孙智慧．地理深度教学路径：底层逻辑与高阶思维 [J]．地理教学．2023．9

[8] 范煜．人工智能与 ChatGPT[M]．清华大学出版社．2023

[9] 江悦、邵爽、张金波．人工智能视域下智慧侦查发展现状及前瞻 [J]．中国刑事警察．2021．4

[10] 任惠华、金浩波．人工智能侦查的实践应用与制度构建 [J]．河北法学．2018．6

责任编辑　韩笑尘