刑事司法科学与治理
Criminal Justice Science & Governance
2024 年 第 5 卷 第 2 期

人工智能应用于犯罪情报研判的逻辑、风险与优化

李子雄

中南财经政法大学司法鉴定与社会治理研究院，武汉

摘　要 | 作为“第四次工业革命”的关键技术，人工智能在犯罪情报研判领域彰显出巨大的潜力与优势，其价值深刻体现在应用的可能性、应用的必要性、应用的向度等逻辑层面。在应用的可能性方面，人工智能自身的机理与犯罪情报的信息性、可拓展性特点之间的天然契合，造就了人工智能在情报信息研判领域的适用可能；应用的必要性包括以技制技、降维打击、提高效率；应用的向度则反映出人工智能在数据搜索、数据深度分析、数据广度分析、数据时空分析等方面的卓越能力。然而，人工智能在犯罪情报应用过程中存在着过度依赖自动化技术而忽略传统基础情报采集、算法的透明度和种类影响情报搜索和分析结果、数据与隐私安全威胁等诸多安全风险。对此，本文尝试从新型情报研判系统的建构、以情报研判需求为导向的核心算法算力的开发、技术规制与安全管理双重保障的防护等方面进行有效“辩护”，以期促进犯罪情报研判沿着人工智能轨道发挥更大效能。

关键词 | 人工智能；情报研判；前置逻辑；风险逻辑；核心算法

一、引言

作为“第四次工业革命”[1]的关键技术，人工智能自1956年首次提出以来，到21世纪已经日臻完善。[2]作为打击犯罪的主体——侦查领域，必然也会接受人工智能的影响和洗礼。有学者在研究人工智能侦查时将人工智能在侦查中的应用分为情报搜集、证据获取、情报研判、智能缉捕四个阶

［1］第四次工业革命的核心是“在数字革命基础上互联网变得更加普及和无所不在，移动性大幅提高；传感器体积变得更小、性能更强大、成本也更低；与此同时，人工智能和机器学习也开始崭露锋芒。”关键性技术主要包括：机器人与自主系统、增材制造（3D打印）、大数据分析、人体机能增强系统、移动和云计算等。参见吕文晶，陈劲，刘进．第四次工业革命与人工智能创新［J］．高等工程教育研究，2018（3）：63–70.

［2］马飒飒，张磊，等．人工智能基础［J］．电子工业出版社，2020：193–197.

段。[1]其中，情报数据智能研判为人工智能侦查的核心范畴。在情报的存储和传递形式方面，有学者提出人工智能不仅改变了传统的情报信息的实物化存储方式，其电子信息的传输方式也大大提高了生活和工作效率。[2]在数据挖掘方面，有学者认为区别于既往的文本挖掘、数字挖掘、网络挖掘，文本与数据挖掘是人工智能时代下三者融合发展的必然趋势，可以理解为对数字形式的文本进行自动化分析或者借助智能化手段对文本资源进行数字化，进而进行数字挖掘和网络挖掘的手段。[3]在技术发展阶段方面，王秀梅等学者主张将人工智能融入证据裁判，通过数据编码、文本——数据链接、标准化司法产品输出等阶段参与证据裁判过程，以实现刑事错案的有效防范。[4]在情报工作流程及模式方面，信息领域学者冯秋燕等认为基于人工智能基础之上的情报工作不仅包括信息采集、组织存储、分析和决策支持阶段，还要实现对情报需求的智能感知、“大脑层”的动态信息整合、数据库以及物理层平台的建设等方面。[5]

从文献的研究内容来看，国内学者们对于四大组成模块的具体运作研究取得了很大进展。但是各模块的研究进度参差不齐，尤其是人工智能与情报研判的具体结合实施方面还有待进一步开拓。人工智能在情报研判模块应用研究稀缺的原因在于应用的逻辑研究不足。[6]然而，主体的价值判断需要事实判断以及在此基础上的理论思维，从而把握事物的主要矛盾。[7]因此，本文从人工智能应用于犯罪情报研判的逻辑规律出发，对具体应用的前置逻辑与安全风险进行分析与阐述。在逻辑规律梳理过程中试图揭示发展瓶颈，并提出针对性转变思路，以期促进犯罪情报研判沿着人工智能轨道发挥更大效能。

二、人工智能应用于犯罪情报研判的逻辑证成

在探讨人工智能在犯罪情报研判领域的应用之前，首先需要理解其应用逻辑——即支撑这一应用的理论基础和前提条件。对人工智能的研究，最终需要的是将这门技术依托于某种载体来实现。

（一）应用的可能性

一是基于人工智能的机理。人工智能带来的智能生产力之所以能够对犯罪情报进行分析研判，得出侦查人员可以信赖的结果，是以人工智能自身的要素、机能和特点为基础的。[8]人工智能是以信息科技为基础，以基于大数据的复杂算法为核心，以对人类智能的模拟、延伸和超越为目标的高新科学技术。[9]人工智能一方面可以通过编写程序来模仿和检验有关人类智能的理论，以能够更好地理解人类智能；另一方面，可以通过创造具备高度灵活性的程序来执行通常需要人类专家才能实现的或复杂重复的任务。[10]正是因为理解性和创造

［1］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，2018，36（6）：49–51.

［2］任珉．人工智能发展及其在情报领域中的应用趋势［C］//2017年北京科学技术情报学会年会论文集，2017：374–377.

［3］庞丽，王利鹏，郑春雨，等．科技期刊文本与数据挖掘人工智能应用的研究进展［J］．中国科技期刊研究，2023，34（8）：1008.

［4］王秀梅，唐玲．人工智能在防范刑事错案中的应用与制度设计［J］．法学杂志，2021，42（2）：97.

［5］冯秋燕，朱学芳．人工智能在情报工作中的应用研究［J］．情报理论与实践，2019（11）：27–31.

［6］张夏恒．ChatGPT的逻辑解构、影响研判及政策建议［J］．新疆师范大学学报（哲学社会科学版），2023，44（5）：113–123.

［7］陈锡喜，冯冉．理论基础、辩证思维与价值判断——社会主要矛盾转化研究的三个维度》［J］．江西社会科学，2022（11）：10–11.

［8］王水兴，刘勇．智能生产力：一种新质生产力［J］．当代经济研究，2024（1）：36–45.

［9］孙伟平．人工智能与人的“新异化”［J］．中国社会科学，2020（12）：119.

［10］刘海滨．人工智能及其演化［M］．北京：科学出版社，2019：6–8.

性[1]，人工智能才可以对情报进行深入的智能化分析。

二是基于犯罪情报的信息性和可拓展性。犯罪情报分析是将大量零散的与犯罪有关的信息加以集中、比较和重新组合从而发现新信息的过程。[2]作为一种序化后的高层次信息[3]，犯罪情报是分析研判的结果，是在一定的目的下，通过对犯罪信息的收集、评估、综合后，经过分析得出的一种结论或推论。[4]此外，情报研判并非仅针对情报信息本身，其内容也囊括了情报系统与情报活动等方面[5]，研判内容的拓展极大增加了犯罪情报研判的难度。然而，人工智能具备人力难以企及的数据收集能力、信息处理能力以及深度学习能力。因此，人工智能在犯罪情报研判中展现出独特的优势，为情报分析提供了前所未有的精准度和效率。

三是基于人工智能在情报信息研判中的适用可能性。其适用可能性主要体现在以下几个方面：在操作层面，人工智能具有正面的嵌入性，可以对情报信息进行梳理、提取、分类、综合、拓展、升级等，保证与信息源实现良好的对接；[6]在研判过程中，人工智能凭借精确多元的算法和强大的信息综合分析能力，能够发挥至关重要的辅助甚至主体性功能；[7]在研判结果上，人工智能的分析建立在对人类智能模拟的基础上，从而确保了推理和实施的科学性与可行性。

（二）应用的必要性

1. 以技制技

犯罪分子在某些方面对数据资源的利用能力比公共管理部门具备“一定的优势”[8]。尤其是面对新型犯罪所特有的“无痕化”[9]交易模式，传统的摸底排查、实地搜查等侦查手段已难以有效提取犯罪过程中的关键证据。消除科技手段被滥用于犯罪活动的负面影响，唯有依靠更为先进的科技手段进行预防、替代和化解。[10]

2. 降维打击

在大数据时代，犯罪活动的猖獗与犯罪分子所依赖的先进作案手段存在直接关系。[11]为有效应对这一挑战，在以技制技的基础之上，人工智能、大数据等技术赋予了侦查机关进行降维打击的资格和优势。由此看来，针对科技犯罪行为之

---

［1］人工智能的创造性表现在通用领域和专业领域两个维度：在通用领域，主要体现为自然语言文字与多模态融合的艺术创作；在专业领域则体现在程序开发、数学与科学研究、技术与工程应用等领域。参见胡卫平，张阳，吕元婧，等．人工智能创造力探究［J］．现代教育技术，2024，34（1）：17–25.

［2］王志华．刑事情报学［M］．北京：中国人民公安大学出版社，2001：24.

［3］张薇．国家安全情报研究（上）［M］．北京：金城出版社，2021：3.

［4］李小猛．大数据侦查情报的分析运用风险及其规制［J］．情报杂志，2023，42（2）：17–21.

［5］靳娟娟．情报研判的问题研判之研究［J］．图书情报工作，2011（2）：254–256.

［6］何大安，许益怀．政府大数据思维下宏观调控的理论分析［J］．浙江社会科学，2024（1）：39–45.

［7］丁晓蔚，苏新．基于区块链可信大数据人工智能的金融安全情报分析［J］．情报学报，2019，38（12）：1297–1309.

［8］“一定的优势”体现在多个方面，比如犯罪主体是通过破坏他人利益从而获取自身利益，是低成本的，而侦查主体则是通过牺牲自身利益维护他人利益，是高成本的；犯罪主体胜利是通过使用技术成功实现一次犯罪目的即可，成功条件简单；侦查主体则是通过使用技术防止每一次的犯罪主体实现目的，成功条件困难；获取数据信息的阻力也不同，在信息获取过程中犯罪遇到的阻力小，而侦查遇到的阻力大。参见谢波，李晨炜．生成式人工智能对犯罪和侦查的双重形塑及其演变逻辑［J］．中国人民公安大学学报（自然科学版），2023，29（4）：95–96.

［9］在网络犯罪中，利用Tor软件服务将用户的IP地址模糊化以逃避流量分析，使用加密数字货币支付系统与Tumbler技术处理非法交易，采取PGP软件加密信息是暗网中用来隐藏犯罪人活动等方法使得犯罪活动呈现“无痕化”的特点。参见谢玲．暗网犯罪刑事治理研究［J］．学术论坛，2020，43（5）：13–24.

［10］郑浩剑．金融科技助力支付机构反赌反诈［J］．中国金融，2021（24）：61–63.

［11］张佳华．大数据时代新型网络犯罪的惩治困境及进路［J］．学习与实践，2022（5）：85–95.

“名片”[1]，在治理过程中只有应用人工智能、大数据等现代科技工具获得高维优势，才能实现对特定类案的降维打击。

3. 提高效率

对于提高犯罪侦查效率而言，时间概念尤为重要，主要包涵两个方面：案件侦办时间与信息处理时间。[2]首先，我国每年的犯罪底数，尤其是经济犯罪案件数量庞大[3]，因此实践中分摊于每一案件的时间并不充裕亦不平均。其次，随着经济社会的发展，案件数据筛选和分析工作超出人工负荷极限，耗费大量时间精力。[4]然而，司法实践要求侦查机关既要遵守案件的法定侦查时限，又要节约侦查成本、提高侦查效率。

（三）应用的向度

情报研判贯穿着案件侦查的始终，是整个案件侦查中具有决定性和方向性的重要一环。[5]情报研判的深刻影响不仅体现在侦查模式的抉择上，更在于对整个侦查流程科学性和效率的深远影响。尤其在当下，人工智能在情报研判环节的应用程度和应用类型，已经成为提升研判精准度、优化研判流程乃至全面提高侦查效率的关键因素。[6]具体而言，人工智能在犯罪情报研判中具有以下几个应用向度：

第一，数据搜索。数据的搜索是以各行业的数据库[7]为基础的，其质量决定了后期情报研判的准确性和可信性。侦查人员通过人工智能技术将各行业及各种既成信息库的数据进行网络信息化整合，把特定的目标数据与关联信息进行指向性比对，以供后期侦查使用。[8]通过数据搜集与碰撞比对产生的重合数据、交叉数据往往是案件重要节点信息，可以在发现节点数据后进一步分析研判，揭示节点之间的潜在关系并作出侦查预测分析。[9]

第二，数据深度分析。深度重在强调海量的数据信息在集合后进行数据碰撞、拓展、证据有效性关联等进一步的操作。[10]在众多数据的深度集合过程中，很多情况下情报的存在形态[11]并不统一，无论是定性还是定量的规整都离不开数据的分析和整合，其形态相应地从整到零再到整地经历了质的变化和螺旋式的上升。

第三，数据广度分析。从本质来看，广度分析

---

［1］“名片”一词引自拉·别尔金的《刑事侦察学随笔》，他指出，罪犯如果多次犯罪，一般都会使用他所喜欢的同样的方法，结果就形成了他的“笔迹”，而根据“笔迹”是可以找到主人的。因此，虽然每一罪行具备特有的“面貌”，但是犯罪方法仍然可能相似，此为罪犯的“名片”。参见拉·别尔金．刑事侦察学随笔［M］．李瑞勤，译．北京：群众出版社，1985：97–98.

［2］王守宽．公正与效率视野下的我国刑侦体制改革研究［D］．武汉：华中师范大学博士学位论文，2007：85–87.

［3］2019年公安机关刑事立案总数为4862443起，其中经济类案件3714039起；2020年公安机关刑事立案总数为4780624起，经济类案件3589996起；2021年公安机关刑事立案总数为5027829起，经济类案件3571483起；2022年公安机关刑事立案总数为4423259起，其中经济类案件2815218起。数据来源：国家数据统计网，https://data.stats.gov.cn/easyquery.htm?cn=C01&zb=A0S0B&sj=2023.

［4］朱琳，赵涵菁，王永坤，等．全局数据：大数据时代数据治理的新范式［J］．电子政务，2016（1）：34–42.

［5］李佳．大数据背景下情报信息引导职务犯罪案件调查研究［D］．北京：中国人民公安大学博士学位论文，2019：30.

［6］岳佳．人工智能时代侦查思维的变革与理论因应［J］．甘肃政法大学学报，2023（4）：120–129.

［7］各行业的数据库种类繁多，至少包括金融行业交易数据库、客户数据库，零售行业的商品数据库、客户数据库、销售数据库，医疗行业的患者数据库、药物数据库、医疗设备数据库，教育行业的学生数据库、教学资料数据库等等。

［8］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）：50.

［9］卞建林，钱程．大数据侦查的适用限度与程序规制［J］．贵州社会科学，2022（3）：78–86.

［10］聂洪涛，韩欣悦．大数据侦查技术在知识产权犯罪中的应用分析［J］．科技与法律，2020（4）：57–64.

［11］在传统的媒介时代，不同媒介之间存在较大壁垒，同时传统的媒介方法只针对特定的数据形态的分析与处理，难以保证相关数据搜集的全面性。而人工智能利用多元算法实现了不同形态数据的有效整合。参见李楠．人工智能赋能媒介素养教育的逻辑、限度与超越［J］．教育理论与实践，2023，43（31）：10–15.

是数据之间存在信息交换与流通的情形。[1]在深度分析过程中不可避免地存在信息的片面性和封闭性，需要在分析研判过程中加强关联信息的连接性，发挥贯穿作用，使侦查人员在研判中占据优势地位。

第四，数据时空分析。所谓时空分析，是指对数据所指向的重点标的进行时间和空间等物理性特征的确认。[2]从整体来看，行为标的的分析有助于判断其发生的客观环境，从而为犯罪预警和后期侦查提供基本的依据。时空分析经过算法延伸得出容易爆发相关行为的时段、地段的范围和变化趋势。[3]因此，数据时空分析是一种预测型思维方式。

三、人工智能应用于犯罪情报研判中的风险剖析

随着人工智能技术的不断革新，其在犯罪情报研判领域的影响日益深刻。习近平总书记强调："科技是发展的利器，也可能成为风险的源头。"[4]因此，深入地剖析人工智能在犯罪情报研判中的潜在风险，对于确保人工智能技术的发展方向，推动其在犯罪情报研判领域的应用具有重要意义。

（一）过度依赖自动化技术而忽略传统基础情报采集

随着计算机和网络技术的快速发展，各种人工智能终端的应用大大解放了侦查人员劳动力。既往挨家挨户式的摸底排队在一定程度上由图像、视频、硬盘介质取而代之。[5]无论在效率还是准确性上，人工智能都具有无法比拟的优越性。

然而，过度或完全依赖于现代化的人工智能技术进行信息的采集也暴露出诸多不足。第一，主体的自动上传上报导致信息的客观性较低。主体的行为动机必然会趋向于有利于自己的方向[6]，因此主体自动上传信息无法保证信息源头的准确性和客观性。第二，规模化的采集控制容易产生漏网之鱼，给侦查活动留下很大的漏洞和破绽。第三，侦查人员的传统侦查技术退化，容易产生怠惰心理，导致传统技术的退步。[7]

（二）算法的透明度和种类影响情报搜索和分析结果

一方面，AI算法作为人工智能的核心与底层技术，成为影响人工智能发展的关键工具因素。[8]算法并非特定不变的，其动态性与多元性致使AI

[1] 赵正，郭明军，马骁，等. 数据流通情景下数据要素治理体系及配套制度研究[J]. 电子政务，2022（2）：40–49.

[2] 马晓悦，薛鹏珍. 大数据环境下的信息时空分析与应用研究评述[J]. 情报理论与实践，2020，43（2）：164–170.

[3] 曾子明，杨倩雯. 城市突发事件智慧管控情报体系构建研究[J]. 情报理论与实践，2017，40（10）：51–55.

[4] 习近平. 加快建设科技强国实现高水平科技自立自[J]. 求是，2022，65（9）：4–15.

[5] 周亚萍，王亮. 犯罪情报分析[M]. 北京：中国政法大学出版社，2016：45–47.

[6] 如动机理论认为，人们的行为动机通常是为了满足自己的需求、欲望或目标，这些需求、欲望或目标对个体而言具有积极的价值或意义。因此，个体的行为动机自然会趋向于那些有利于自己、能够满足自己需求的方向；参见谢才凤，邬家骅，许丽颖，等. 算法决策趋避的过程动机理论[J]. 心理科学进展，2023，31（1）：60–77. 自我决定理论认为，人们有一种内在的动机，追求自我成长、自我实现和自我满足。在这种动机的驱使下，个体会倾向于选择那些能够带来内在满足感、符合自己价值观和目标的行为。因此，个体的行为动机也会趋向于有利于自己的方向，以实现自我价值和自我满足。参见王水，袁勤俭. 自我决定理论及其在信息系统研究领域的应用与展[J]. 现代情报，2023，43（5）：146–155.

[7] 金益锋，马忠红. 刑事侦查中人工智能的应用：实践样态、风险挑战与发展策略[J]. 科技导报，2023，41（7）：15–27.

[8] 曲亮，张智敏，刘瑾. 人工智能算法技术异化研究框架的整合构建——"内涵特征——异化归因——算法治理"的逻辑视角[J]. 科技管理研究，2023，43（21）：238–246.

技术也具有一定的不确定性[1]。人类对于人工智能算法的自主学习与决策过程尚未达到充分的认知程度，导致以纵向和横向深度学习为主要导向的人工智能算法经常被视作一个无人理解的“黑箱”。[2]

另一方面，算法种类繁琐，涵盖四大类型及数十种细分类型[3]，直接影响到预测输出结果的确定性和稳定性。在人工智能情报研判领域中，算法代表着从前期数据进行深度分析到最终预测结论得出的计算路径。[4]算法的核心在于构成一系列解决问题的精确指令。因此，一个完整的算法体系是建立在坚实的数学基础之上的，诸如矩阵论、数值分析、经典变换、Python编程基础等都是不可或缺的重要支撑。在实践中，不同的情报预测系统中预置和实际使用的算法千差万别，这导致了未能形成统一的结果认证标准的尴尬局面。

（三）数据与隐私安全威胁

数据安全与国家经济运行、社会治理、国防安全等领域紧密联系，事关国家安全和社会稳定，是一种极为重要的新兴安全类型。[5]一方面，由于人工智能的基础——以算法为核心的软件系统和以计算机为核心的硬件系统——在搭配使用时存在一定的脆弱性，容易受到外部不法分子的攻击和侵扰[6]，另一方面，随着人工智能的广泛应用，公民隐私受侵犯的风险也日益加剧。对隐私的保护需求源于人的羞耻本能[7]，是人类的一种自然情感。信息技术对社会生产和生活的全方位渗透，使得数据收集以完成社会治理与公民强调个人隐私的护持之间形成激烈冲突。[8]

四、人工智能应用于犯罪情报研判的优化路径

人工智能与犯罪情报研判领域的结合，形成了一个伴随诸多社会风险的虚拟情报研判数字空间。因此，应立足于人工智能数字技术与情报研判的双重特征，将人工智能优势赋能犯罪情报研判工作，同时对人工智能进行规制以保障数字安全与公民的隐私权，构建符合当下的新型情报研判体系。

（一）建立新型情报研判体系

建立以情报系统为依托、以侦查人员为主导、以人工智能为助力、以传统情报采集分析为补充的新型情报研判系统。新型情报研判体系应当满足以下几个条件：

一是针对情报信息的可信度筛查。Flanagin认为可信度囊括三部分：内容可信度、信源可信度、设计可信度。[9]因此，在犯罪情报研判领域，应

---

［1］世界的本质是不确定的，人类的认知过程也是不确定的，作为人类认知工具的人工智能也必然是不确定的。就人工智能而言，不确定性首先体现为算法与数据的不确定，数据的缺失和预设条件的不合理将直接影响机器学习的输出；其次，人工智能的应用后果也是不确定的，可能是积极的作用，也可能是消极的影响。此外，这种不确定性是不可避免的，只能通过一定的方式进行消减。参见程海东，王以梁，侯沐辰．人工智能的不确定性及其治理探究［J］．自然辩证法研究，2020，36（2）：36-41.

［2］吴椒军，郭婉儿．人工智能时代算法黑箱的法治化治理［J］．科技与法律（中英文），2021（1）：19-28.

［3］按照模型训练方式的不同，可以将算法分为监督学习、无监督学习、半监督学习以及深度学习四大类。其中常见的监督学习算法包括线性回归、逻辑回归等；常见的无监督学习算法包括聚类分析、关联规则学习等；常见的半监督学习算法包括生成模型、低密度分离等；常见的强化学习算法包括Q学习、SARSA、策略梯度等。参见伊恩·古德费洛，约书亚·本吉奥．深度学习［M］．赵申剑，李凯等，译．北京：人民邮电出版社，2017：88-90.

［4］马海群，张涛．区块链赋能智能情报分析算法风险治理机制研究［J］．图书与情报，2023（1）：48-56.

［5］梅传强，盛浩．数据安全刑法保护的模式转换：从管理安全到利用安全［J］．重庆大学学报（社会科学版），2024（1）：1-18.

［6］斜晓东．论生成式人工智能的数据安全风险及回应型治理［J］．东方法学，2023（5）：106-116.

［7］张新宝．从隐私到个人信息：利益再衡量的理论与制度安排［J］．中国法学，2015（3）：40.

［8］陈锦波．从私法到公法：数字时代隐私权保护的模式延展［J］．政治与法律，2023（11）：25-26.

［9］Flanagin A J，Metzger M J．The role of site features，user attributes，and information verification behaviors on the perceived credibility of web-based information［J］．New Media&Society，2007，9（2）：319-342.

当在对信息采集源、信息提供者信誉以及采集者专业见解的深入理解基础之上，制定科学有效的分类标准。同时，通过引入先进的二分类、多分类、回归分类[1]等多元的针对性算法，切实提升数据处理的智能化水平和精准度。同时应当充分发挥研判人员的专业优势，确保情报信息的真实性和准确性。

二是情报数据的采集。情报数据的采集不仅仅是简单的信息收集过程，更是情报研判中不可或缺的关键环节，涉及对信息的深度挖掘、分析和研判，为后续的决策和行动提供重要的支撑和依据。[2]因此，情报数据采集的全面与精细对整个研判过程具有重要意义。在情报数据采集环节，通过对采集区域进行精细化的网格划分，不仅能够实现数据采集与地域特征的深度融合，还能够揭示数据背后的空间分布和趋势变化。此种可视化分析的方法能够将隐晦的数字特征转变为直观、全面的情报信息，有助于及时发现高危区域并采取相应的预警措施。

三是应当在人工智能的基础上发挥传统侦查的优势。人工智能在数据处理、模式识别和预测分析等方面具有显著优势，能够为情报研判提供科学、客观的依据。然而，传统的侦查理念、策略和经验代表着侦查人员的智慧和直觉，在情报研判中同样具有不可忽视的价值。因此，构建新型情报研判体系时，应将人工智能的研判结果作为重要参考，同时充分发挥侦查人员的专业判断和实战经验，将传统的领导论、博弈论、侦查经验等应用于其中[3]，做到传统与现代相结合。

（二）施用以情报研判需求为导向的核心算法算力

在处理复杂的算法问题时，应当坚持两个关键原则以确保情报研判的准确性与效率。一方面，算法算力的选择以具体需求为导向。在人工智能的实际应用中，数据、算法、算力三者相互联系，密不可分：数据是人工智能的基础，是一种新型的生产资料；算力指的是处理海量数据的能力，是实现智能的生产力；算法则构建了人工智能的供给与分配关系，可以视为“中枢神经系统”。[4]犯罪情报研判是一个涉及大量数据处理、模式识别、信息提取和决策支持的过程，需要保证研判的效率与质量。因此，应当将优势的算法算力资源投入到情报研判的具体或迫切的需求之中。需求的认定应当结合三个指标：情报数据的特性分析、情报预测的标的以及研判结果的难易程度评估。首先是情报数据的特征。数据是人工智能的基础，算法是人工智能的底层技术[5]，因此算法的计算和运行方法应当和数据的收集、排列、搜索征象一致。其次是情报预测的标的。情报预测的标的指引算法运行的路径，主要表现为在多种算法均可达到目标时，侦查主体需要基于算力和综合效果的考量，选择最优的算法路径。最后是研判结果的难易程度。算法的复杂程度和研判结果的难易程度是呈现相关关系的，因此，应当充分认识两者之间的内在联系，把握好二者的对应关系，以便在实际应用中找到最佳的平衡点。

另一方面，数据的整合与分析是发现数据潜在价值的关键环节，既要实现无序数据资源的有序整

---

［1］二分类、多分类、回归分类算法都是机器学习中常用的技术，主要用于处理不同的问题。二分类算法通常用于处理和预测非连续性事件的发生与否；多分类算法的任务主要涉及多个类别数；回归算法主要用于预测连续值的输出。参见周志华。机器学习［M］. 北京：清华大学出版社，2016：53–66.

［2］张范军，陈海洋，陈涵煜. 以数据为中心开展电子对抗侦察情报整编工作的几点思考［J］. 电子信息对抗技术，2022，37（4）：1–4.

［3］例如将博弈论应用于人工智能情报研判中，博弈焦点在于犯罪分子与侦查主体在技术应用地位的差异、公私数据信息获取之间的对抗以及“人–机–物”对抗策略的动态调整。参见谢波，李晨炜. 生成式人工智能对犯罪和侦查的双重形塑及其演变逻辑［J］. 中国人民公安大学学报（自然科学版），2023，29（4）：95–96.

［4］兰帅辉，尹素伟. 数据、算力和算法：智能传播的多维特征、问题表征及应对［J］. 当代传播，2022（5）：93–96.

［5］郑久良. 人工智能时代算法新闻伦理治理范式研究［J］. 青年记者，2024（1）：98–102.

合与有效收集，又要保证所得数据的合理性、关联性和系统性，而这离不开智能算法的建模。[1]情报研判工作目的便在于挖掘各种数据或线索之间的隐藏关系，因此构建和优化情报研判系统的核心算法算力是提升整体效能的关键。为此，应当在满足实际需求的基础上，通过深度学习和强化学习等技术手段不断推进算法的升级和迭代，持续提高算法的适应性和运行效率，使其更好地应对复杂的情报研判任务。同时，应当注意到算力的提升也是一项长期而艰巨的任务，对此可以从信号处理速度、模块数据[2]提取速度、解码能力等多个方面入手，通过研发更先进的计算机系统和优化算法设计，为情报研判提供更强大的计算支持。

（三）建立技术规制与安全管理双重保障

人工智能作为系统性的存在，无法将其孤立地视作单一事物、客体而仅从传统法律视角进行规制，否则将会面临“见树木而不见森林”的短视困境。[3]因此，应当以安全管理为前提，坚持宏观的技术规制。从我国的《新一代人工智能发展规划》到《促进新一代人工智能产业发展三年行动规划（2018–2020）》[4]，尽管已对人工智能的发展和应用作出了一定的规划和指导，但在法律保障和伦理规则方面仍存在诸多空白[5]。因此，加强相关具体法规的制定尤为关键。其一，通过立法明确人工智能系统的法律地位，界定其与人类行为之间的界限，并确立相应的责任主体和归责原则。[6]其二，针对人工智能应用中涉及的隐私和数据保护问题，制定专门的法规来规范数据的收集、使用、存储和传输等行为，确保个人隐私和数据安全得到切实保障。其三，制定人工智能应用的伦理准则，明确禁止应用的领域或场景，并建立相应的审查机制来监督人工智能系统的开发和应用过程。

人工智能诞生及发展的目的是为人类福祉服务，应基于人权保护而开发利用，遵循人类社会的各种伦理道德体系，同时对潜在风险制定应对方案，使其做出的决策符合人类整体利益。[7]因此，在技术规制层面，应构建一套科学、系统的人工智能安全标准体系，并辅以有效的评估机制来识别和控制潜在风险。

五、结语

人工智能技术在犯罪情报研判中的应用，基于一种深刻的逻辑关联，不仅体现在情报数据搜索与分析过程中与人工智能结合的可能性、必要性和方向性上，更在于人工智能对于海量数据的处理优势，恰好迎合了情报工作多元化的现实需求。这种技术与需求的契合，正是人工智能在犯罪情报研判中展现其巨大潜力的关键所在。作为风险逻辑的

---

［1］郝志远，马捷，赵冠壹，等．生命周期视域下的工业大数据价值发现研究［J］．图书情报工作，2023，67（15）：14–24.

［2］S1000D是欧洲航天和国防工业协会（ASD）发布的一个关于技术资料数字化的规范，包括技术资料数据的组织生成、格式要求等方面的内容。依据S1000D规范创建的技术文档的典型特点是：数据不是以传统的“章节”形式而是以“数据模块（Data Module，DM）”的形式来组织的。参见周伟祝，唐金国，孙媛，等．ASD S1000D规范中的数据模块编码分析［J］．世界标准化与质量管理，2008（6）：52–56.

［3］李锋．类ChatGPT人工智能背景下国家安全情报工作的机遇、挑战和应对［J］．情报理论与实践，2024（1）：1–8.

［4］除此之外，为推动人工智能技术的发展与落地，政府还颁布了《人工智能白皮书》（2022年）、《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》等文件。与此同时，国家新一代人工智能治理专业委员会发布了《新一代人工智能伦理规范》，旨在将伦理道德融入人工智能全生命周期，为从事人工智能相关活动的自然人、法人和其他相关机构等提供伦理指引。

［5］如人工智能法律资格的问题、人工智能产品问题举证责任的分配等。参见韩凌月，张安毅．人工智能产品质量的法律规制研究［J］．河南财经政法大学学报，2023，38（6）：76–82.

［6］高诗宇．人工智能体法律主体资格之争的商谈理论解决方案［J］．哲学分析，2023，14（5）：121–132.

［7］梁健．人工智能运用于社会公共行政管理创新的优势、领域与路径探析［J］．兰州学刊，2024（1）：1–16.

一种可期待“辩护”，人工智能在犯罪情报研判中的应用应当进一步综合多元学科知识，通过优化算法、提升算力等双重途径实现技术的升级与革新，以提升情报研判的准确性和效率。值得注意的是，无论是人工智能还是犯罪情报研判，都是复杂而专业的领域，本文在宏观上对人工智能应用于犯罪情报研判的逻辑、风险与优化的论述难以触及技术细节与具体场景。因此，研究应当更加关注于算法、数据等具体技术在不同类型犯罪中的实现与验证，以确保人工智能将在犯罪情报研判领域发挥更加重要和广泛的作用，为社会的安全与稳定贡献更多的力量。

（责任编辑：李秀玲）

Logic, Risk and Optimization of Artificial Intelligence Applied to Criminal Intelligence Research and Judgment

Li Zixiong

Institute of Forensic Expertise and Social Governance, Zhongnan University of Economics and Law, Wuhan

Abstract: As a key technology of the “Fourth Industrial Revolution”, artificial intelligence has shown great potential and advantages in the field of criminal intelligence research and judgment, and its value is deeply reflected in the logical level of application possibility, application necessity, application dimension and so on. In terms of the possibility of application, the natural fit between the mechanism of artificial intelligence itself and the characteristics of information and extensibility of criminal intelligence creates the possibility of application of artificial intelligence in the field of intelligence information research and judgment; The necessity of application includes making technology with technology, reducing dimension and improving efficiency; The application dimension reflects the excellent ability of artificial intelligence in data search, data depth analysis, data breadth analysis, data space-time analysis and so on. However, there are many security risks in the application of artificial intelligence in criminal intelligence, such as over-reliance on automation technology and neglect of traditional basic intelligence collection, influence of transparency and types of algorithms on intelligence search and analysis results, data and privacy security threats. In this regard, the author tries to effectively “defend” from the construction of new intelligence research and judgment system, the development of core algorithm computing power oriented by intelligence research and judgment demand, and the protection of technical regulation and security management, so as to promote the criminal intelligence research and judgment along the artificial intelligence track to play a greater role.

Key words: Artificial intelligence; Intelligence research and judgment; Pre-logic; Risk logic; Core algorithm