上海法治報 <u>B2</u>

圆桌论は

2025年 4月28日 **星期一**

■本期嘉宾

厉永佳 上海市人民检察院第三分院检察

官

许朝晖 上海市人民检察院第三分院综合

办公室副主任

孙建伟 上海市法学会研究部主任

近年来,检察机关深化实施数字检察战略,紧紧围绕"业务主导、数据整合、技术支撑、重在应用"要求,积极推进数字检察工作,构建了一批大数据法律监督模型,人工智能技术在检察履职办案中的应用深度和广度日益扩展,以数字检察赋能法律监督的成效愈发明显。人工智能作为专注于算法突破的高新科技产业,若融入到检察工作体系中,势必会带来办案模式、司法监督等全链条的变革,进而也势必对检察工作带来挑战。

警惕 AI"造假"

厉永佳:DeepSeek等大语言模型在实践应用中,有一些问题需要我们预判和解决:

一是数据来源问题,特别是监督类数据。数据互联互通工作已经推进了很多年,但实务中还是存在跑数据、要数据。有些数据还涉及保密,而不同机构的网络保密等级不同。二是存在数据真假辨识问题。此前,媒体曾报道美国有律师提交辩护意见,其中多个判例另外一方检索不到,法庭经核实后发现是 AI 自动生成的

虚假案例。最近我们涉外团队 检索相关资料时,发现有个 "上海三中院判决的走私案 件",但是经查证我们院并没 有起诉过,该案例是虚假的。 关于数据虚假的问题,我能想 到的解决方法就是要标记数 据出处,进行人工复核。以生 成审查报告为例,证据证明部 分,以及侦查监督线索是依据 哪些数据形成,上述数据的原 始出处在哪里,这些都需要标 记并由检察官人工复核。与此 同时,还需要给数据库的数据 写保护,禁止 DeepSeek 对原 始数据进行篡改。

AI 可能带来新型犯罪

许朝晖:我认为人工智能技术对检察工作带来的挑战主要是会带来一些新型犯罪,比如声音、图像等深度伪造问题,以及反向提取信息等数据犯罪问题,还会出现技术失误,产生犯罪主体是谁的问题。

比如,当人工智能自动驾驶时,发生了交通事故,那么责任主体到底是谁?

此外,我认为人工智能还会对检察 官的权威性以及整体的工作方式带来很 大的挑战,检察人员势必需要思考如何 利用好人工智能作为辅助办案工具,使 得工作效率最大化。

针对前面提到的大语言模型自身存在的不足与问题,可以采取相应的对策

予以应对。

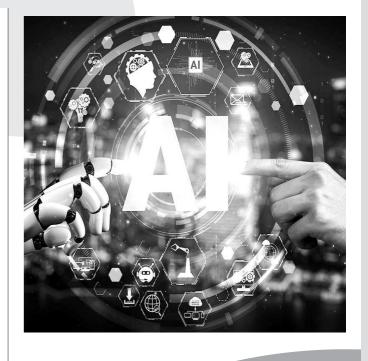
一是我们可以预先了解一下上级检察机关或者其他地方检察机关的 人工智能部署方案,避开他人已经或正 在探索的,再结合我们自身办理的案件特点,进行具有自身特色的数字化部署。

二是我们要找到合适规格的大模型,既 能满足成本控制,又能实现较好的效果。

三是可以通过 Manus 等智能体的运用, 或者搭建 RAG 知识库、优化提示词、参数微 调等方式,来帮助解决生成式 AI 的幻觉倾 向、专业力不足和时效性差等固有缺陷。

在部署推进的过程中,我们需要注意几个平衡:一是安全与效率的平衡;二是人工与智能的平衡;三是成本与效益的平衡。





在利用人工智能 与保护隐私权之间取得平衡

孙建伟:大语言模型的 便利和快捷为检察工作注入 了新的活力,我们要牢牢抓 住这一机会来推动大语言模 型在检察领域的运用,但同 时要时刻警惕人工智能带来 的风险,充分发挥检察机关 的法律监督职能。

在司法工作中涉及大量 敏感信息和隐私数据,大语 言模型的训练通常依赖大规 模的数据集,而在数据采集、 传输储存中,如何防范敏感 信息泄露成为司法工作中一 个亟待解决的问题。如果数 案件当事人隐私的泄露。因 此,如何在利用人工智能致 案件当事人隐私的泄露。因 此,如何在利用人工智能验 私权之间取得平衡,我认平方 检察机关在维护社会公本了

有更大的作为的空间。 一是加强跨部门 协同监管。大语言模 型涉及的数据 广泛,既有商业 数据,也有公共 数据和个人 敏感数据、隐 私数据。检察 机关可以与 网安、网络、 市场监管部 门建立高效 的信息共享 和联合监管 机制,形成多 部门的联动监管体系。通过 统一标准、共享数据和信息 互通,实现大语言模型在数 据使用过程中的隐私风险全 链条监管,确保违法违规行 为能够被及时发现和制止。

二是加强公益诉讼与刑事诉讼监督。当发现大语言模型企业或相关业务存在非法采集、滥用个人信息的违法行为时,可以依法提起公益诉讼,针对一些利用大语言模型实施诈骗、数据泄露等犯罪活动,可以通过监督公安机关刑事立案、侦查取证,严厉打击相关违法犯罪行为。

三是健全证据采信与技 术鉴定机制。大语言模型在 数据处理方面涉及复杂的技 术问题,这对传统的证据采 信和司法鉴定提出了挑战。 检察机关应该加强与技术部 门的合作, 引进先进的数据 鉴定手段,建立专门的司法 技术团队,通过技术手段确 认数据来源,追溯数据流向, 确保在案件处理中能充分准 确认定违法事实,为依法追 责提供有力证据。随着技术 的不断迭代和法治社会理念 的更新,司法机关在大语言 模型隐私保护方面也在不断 探索与创新, 尤其是技术不 断的迭代发展,如何建立一 套科学、高效、灵活的信息保 护机制, 我觉得可能是检察 机关未来面临的工作挑战。

(召集人:上海市人民检察院 第三分院 周春燕;发言整理: 上海市人民检察院 樊华中 上海市检察院第三分院 胡伟 东 孙钰程 王岚)

责任编辑/陈宏光 E-mail:lszk99@126.e