从各执一词到多元平衡：人工智能与刑事司法

□熊秋红

早在20世纪80年代，作为信息社会表征的资讯技术就已经在刑事司法中得到应用。进入21世纪之后，各种自动化和人工智能技术在刑事司法中的应用更为深入。从目前的情况来看，人工智能在刑事司法中的应用主要集中在犯罪预测、犯罪侦查、审前羁押与保释、量刑、假释与罪犯矫正等领域。

与其他国家和地区相比，我国人工智能的应用更为广泛，除了上述领域之外，还包括证据的审查判断、法律文书的生成、检察机关的诉讼监督等领域。可以预见，未来人工智能在刑事司法中的应用范围还会逐步扩大，比如可能应用于制作诉讼笔录、提供外语或者少数民族语言翻译、为当事人寻找合适的律师提供帮助、对证人证言的真假进行判断，等等。

刑事司法中人工智能的应用前景

人工智能具有强大的数据收集和分析能力，在刑事司法中具有广阔的应用前景。从世界范围来看，人工智能在刑事司法中的应用引发了广泛的关注和争论。赞成者有之，反对者亦有之。

赞成者认为，人工智能的应用具有以下优势：一是一些国家面临着严重的案件积压，人工智能的应用对于解决“诉讼爆炸”而言是一个很好的工具，由于减少了诉讼拖延，当事人因为诉讼拖延而遭受的不公正对待也会相应减轻；二是人工智能的应用有助于克服人为的偏见，人工智能不会被主观情感所左右，有利于案件得到客观公正的处理；三是人工智能具有科学性和专业性，操作起来也方便快捷，有利于提高司法人员的办案质效。

反对者认为，人工智能的应用会带来以下问题：一是准确性问题，人工智能作为一个风险评估工具，它在准确性方面并不一定优于其他方法；二是公平性问题，人工智能建立在收集大量数据和设计算法的基础上，大数据中包含大量个人信息，可能引发种族偏见和歧视风险；三是透明度问题，一些设计算法的公司拒绝公开算法所考量的一些因素，导致出现算法黑箱；四是影响被追诉人的权利保障，如警方使用预测模型，可能导致从事后出警向事前出警转变，有违无罪推定原则。

理性看待泾渭分明的两种立场

在我国，学者对于人工智能在刑事司法中的应用大多持乐观态度，主要原因是看到了人工智能应用所带来的巨大优势，主要包括有利于提高侦查机关的侦查能力，有利于打击犯罪；类案检索有助于促进量刑均衡，有利于同案同判；通过人工智能辅助办案，可以减少司法人员阅卷、进行证据梳理以及撰写诉讼文书的时间，有助于提高诉讼效率。但也有部分学者对此持保留甚至反对的态度，认为人工智能在刑事司法中的应用挤压了司法人员的自由裁量权，可能导致机械司法；背离了司法的亲历性原则，使得司法人员办案变成了机器裁判；可能会造成冤错案件，破坏司法公正；人工智能辅助办案时，对于证据采信、事实认定和法律适用均无法说明理由，同时算法黑箱使得公众对司法的处理结果可能产生不信任；在大量收集涉及个人信息的大数据过程中，可能侵犯公民隐私权；人工智能辅助办案，将会模糊司法责任，一旦出现错判，承担司法责任的主体将会不明确等。

上述争论表明，对于人工智能在刑事司法中的应用，存在着泾渭分明的两种立场，即积极主义立场与消极主义立场（或曰保守主义立场）。综合分析论辩双方的观点，在理论层面，可将人工智能对于刑事司法所带来的挑战和冲击概括为五个方面：其一是合法性问题，由于法律发展滞后于技术发展，导致司法实践中，人工智能的应用面临着合法性赤字或合法性质疑，许多国家和地区的刑事诉讼法尚未对人工智能的应用进行规制，通过解释现有的法条来容纳人工智能的应用，容易导致合法性争议。其二是公正性问题，譬如将人工智能应用于犯罪预测和犯罪侦查，导致侦查办案的模式从回应性侦查走向了预防性侦查，警察在获知犯罪预测的结果之后，对于所谓的“犯罪热区”进行特别干预，部署警力集中打击某类犯罪，警察更倾向于在“犯罪热区”发动盘查，甚至还采取一些限制人身自由的强制措施，并且在办案时会自觉或不自觉地降低证明标准，这样会导致生活在“犯罪热区”的居民，其人身自由和隐私权更容易受到限制或者侵害。其三是民主性问题，人工智能在刑事司法中的应用是否符合法治社会的民主原则，主要看它是否具有透明性和可问责性。人工智能的应用有两大黑匣子，一个是法律黑匣子，另一个是技术黑匣子，这两个黑匣子对刑事司法的透明性和可问责性带来巨大挑战，由于算法比司法人员自由裁量具有更为不透明的特性，导致对于司法决策的监督和审查变得更加困难。大数据侦查通过相关性原理来进行分析和预测，难以对其中的因果关系进行具体说明，运用人工智能系统决策，一旦出错，算法的责任难以追查，人的责任难以追究。其四是有效性问题，如果依靠人工智能决策可以有效地避免司法人员的偏见，而且所作出的裁判结果在公正性方面明显优于人类所作裁判，那么人工智能的应用无疑具有可接受性，但目前并没有实证研究表明人工智能的应用具有如此效果。其五是伦理性问题，无论人工智能的功能有多么强大，为了确保人类的情感与尊严，将刑事司法的决策权完全移交给机器，这是人类所不能接受的。因此，任何国家或地区都只是将人工智能作为刑事司法中的辅助性工具加以使用。

在此情况下，目前所要解决的关键性问题就是司法人员如何与机器进行合作，即人机协同问题。

寻求法治主义与技治主义的有效结合

对于人工智能在刑事司法中的应用，不同国家的处理模式存在差异。

欧盟采取严格监管模式，以统一立法、强调安全、事先规制为特点；美国采取渐进规制模式，以逐步立法、强调开放、事后救济为特点；我国采取发展优位模式，积极推进人工智能在刑事司法中的应用，由于不断拓展人工智能在刑事司法中的应用领域，导致出现了人工智能的应用似乎有些泛化的局面，并因此引发了不少理论和实践争议。

对于人工智能在刑事司法中的应用，需要注意以下三点：第一，应当认识到，在刑事司法这样一个特殊领域，人工智能的应用具有较大局限性。以量刑智能辅助系统而言，设计科学的量刑智能辅助系统存在不少困难，包括案件信息数字化、结构化的困难，案件信息数字化转换存在的技术障碍，以及刑罚适用的统一性与个别性的矛盾难以调和等。第二，对于刑事司法中人工智能应用的规制，应当从数据治理、算法治理和应用系统治理三个基本层面展开。这三个层面就是人工智能系统所包含的三个主要元素。从数据治理的角度看，应当保障资料的全面性、准确性和合法性；从算法治理的角度看，应当保障算法的科学性、透明性和公正性；从应用系统治理的角度看，应当保障应用系统的安全性、有效性和诉讼主体使用该系统的平等性。第三，应当坚守司法人员在刑事司法中的主体地位，实行规则指导与智能辅助相结合。司法人员在规则指导与智能辅助下决策，要兼顾实然与应然，作为人工智能系统基础的大数据，来源于司法人员过去的办案情况，如果在过去的执法司法中存在偏差，人工智能系统将会固化这种偏差。因此，需要通过规则指导来纠正过去执法司法中的偏差，并且回应社会公众对合理执法、公正司法的期待。

人类社会从农业社会、工业社会到信息社会的演进过程中，互联网、大数据、人工智能由浅入深地进入刑事司法，使得法治主义与技治主义的结合成为数字时代刑事司法的显著特征。为了构建可信赖的人工智能应用体制机制，防止产生新的人权保障风险，需要对人工智能在刑事司法中的应用进行规则治理。由于人工智能在刑事司法中的应用涉及法律问题和技术问题，笔者认为，应当同时从法律和技术两个层面对其进行规则治理，人工智能系统的研发和有关规则的制定应当由法律专家和技术专家共同组成的专家咨询委员会进行审查。

总体而言，人工智能在刑事司法中的应用应当趋利避害、扬长避短，妥善处理安全与自由、公正与效率、实然与应然的关系，达到多元法律价值的兼顾与平衡。

（作者为中国政法大学诉讼法学研究院院长、教授）

隐私计算：让数据安全“触手可及”

——专访蚂蚁集团隐私智能计算部总经理、可信隐私计算开源框架“隐语”负责人王磊

□本报记者 李娜
见习记者 高航

记者：大数据产业高速发展，规范数据治理，保障数据安全是重中之重。当前，数据流通的现状如何？如何有效实现数据的安全可信流通？

王磊：随着数据安全法、个人信息保护法的相继出台与施行，在中共中央、国务院印发的《关于构建数据基础制度更好发挥数据要素作用的意见》等相关政策的支持与鼓励下，大数据产业迎来爆发式成长。在快速发展的背后，数据隐私安全等相关问题也逐渐显现。传统“复制式”的数据流通方式让商业秘密、个人隐私信息等面临被泄露的风险，无法满足使用数据合法合规的要求。如果在数据提供方展开相关数据计算，虽然可以让数据不出域，但会暴露业务需求方的计算规则与计算模型，进而泄露业务需求方的商业隐私。因此，要兼顾数据提供方和数据需求方的不同“偏好”，让数据要素实现良好的市场化配置，必须要完善数据可信流通机制的建设。

隐私计算为我们提供了可行性路径。隐私计算是用于保障数据安全流通、处理和分享的一系列技术的总称。目前国内使用比较广的技术主要有多方安全计算（基于密码学的隐私计算技术）、联邦学习（人工智能与隐私保护技术融合衍生的技术）、可信执行技术（基于可信硬件的隐私计算技术），其他一些如同态加密、零知识证明等技术目前主要作为辅助技术在使用。

从隐私计算的发展历程看，国外企业布局较早。早在2008年第一家专攻多方安全计算解决方案的技术厂商Partisia就已在丹麦成立，为商务合同、加密拍卖等场景提供安全方案。科技巨头中，微软从2011年开始深入研究多方安全计算，谷歌在全球率先提出联邦学习的概念，Intel打造的SGX是目前使用最广泛的商业可信执行环境方案。但从总体的应用场景来看，目前国外很大一部分的隐私计算项目都是面向区块链和加密虚拟货币的场景。

记者：隐私计算技术的优势具体体现在哪里？又会产生哪些叠加效应？

王磊：隐私计算的目的是让多个数据拥有者在不暴露数据本身的前提下，实现数据的共享、互通、计算、建模，最终产生超出自身数据的价值，同时保证数据不泄露给其他参与方。其技术可以分成两类，一是计算过程安全类技术，用于确保数据只能在指定意图下进行计算；二是结果反推安全类技术，用于确保使用方无法利用逆向工程，从输出结果反推出原始数据。

相比传统数据安全的方式，隐私计算可以完全凭借技术手段，实现参与方数据间的“可用不可见”，对数据使用可以做到“可控可计量”，从根源上切断对人的信任依赖。在运作过程中，隐私计算可以防备参与方之间出现潜在攻击的情形，能够有效维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用。

在应用实践中，隐私计算还可以与其他技术相融合产生叠加效应，如融合区块链技术来强化在数字身份、算法、计算、监管等方面的信任机制，进一步完善数据要素的确权、流通等可信体系建设。

事实上，没有任何一种单一技术路线是完美的，业务应用的实际技术选型，还需根据具体的安全假设、硬件条件和性能要求等因素综合考量，选择最适合业务场景的解决方案。在一个隐私计算项目中，各个子类隐私计算技术结合的模式也很常见。例如，在联邦学习场景中，可以通过差分隐私技术（密码学中的一种手段，旨在提供一种当从统计数据库查询时，实现数据查询最大化的准确性，同时最大限度减少识别其记录的机会）提升对中间信息的隐私保护，在多方安全计算中，可以结合可信执行环境提升计算性能。

记者：隐私计算技术具体可以应用在哪些场景？

王磊：隐私计算技术应用的场景非常广泛，在涉及解决数字化发展中的安全可信、协作共识、大规模复杂数据关联分析、存储计算规模爆发、降低耗能等难题时，隐私计算技术都可以发挥相应功效。

比如在政务场景中，政府部门掌握城市的大部分数据资源，在政务数据内部共享方面，政府可通过隐私计算技术搭建政务公共数据密文开放共享交换平台，打通跨域数据的应用价值链，使得数据基于政务应用需要在各部门条线之间实现安全共享和流通；在政务数据开放方面，政府可通过建设保护各方隐私安全的公共数据开放平台，使用隐私计算技术融合政府数据和社会、企业数据进行安全计算，联合统计，联合建模，实现数据融合价值。

再比如在金融场景中，数据提供方主要是互联网平台、运营商、政府部门等。金融机构一般作为数据需求方，通过隐私计算技术引入外部数据来实现普惠金融、风控管理等效果。在合规方面，隐私计算技术在确保银行自身数据安全的情况下，以合规高效的方式获取外部数据，从技术上解决了缺乏数据源支持的难题。

记者：隐私计算技术如何在大数据赋能法律监督时发挥有效作用？

王磊：具体到检察应用场景，隐私计算能力模块可保证参与到检察机关开展法律监督的相关单位，在不泄露各自原始数据的前提下，通过协作，对其数据进行联合分析和联合建模。在隐私计算框架下，参与方的原始数据可以不出本地，在保护数据安全的同时实现多源数据跨域合作，破解数据保护与融合应用难题。此外，可通过加密流转、隐私计算等数据交互方式，实现多方数据安全接入，打造“端+链”模式，进行基于隐私保护的接口服务、共享交换、计算建模，满足不同密级数据和检察业务场景的需求。目前，浙江省杭州市检察院已率先在空壳公司监督治理工作中探索应用隐私计算技术，正推进建设中的多跨隐私协作平台可安全联通司法机关、政府部门、互联网企业等多方数据，为数字检察工作提供安全高效的实践样例。

走近科技

科技助力短视频平台“查漏补缺”

□彭伶

近年来我国短视频发展迅速，不少人担心未成年人从游戏网瘾转向刷屏网瘾，甚至有观点认为应当禁止未成年人使用短视频。然而，在短视频已经成为全民化应用的数字网络时代，未成年人使用短视频的风险并非通过简单粗暴的物理隔绝就可以化解。未成年人如何才能科学、安全、有序地使用短视频？笔者认为，平台应当充分利用技术手段，减少短视频应用风险。

目前各国对于短视频应用呈现严管趋势。今年4月26日，欧盟委员会根据《数字服务法》(DSA)作出一项决定，明确要求不能收集未成年人的个人数据来对其进行定向广告投放，强调对部分大型在线平台（包括短视频平台）和搜索引擎进行额外审查，如要求平台提交风险评估报告、采取系统性风险防范的技术措施、提供强大的内容审核工具、实现更高标准的透明度和问责制等，这些都体现了对未成年人的保护。

对此，我国短视频平台必须重新设计系统，以确保未成年人的隐私安全，重新设计界面、推荐系统、服务条款等，对于存在虚假信息传播和不真实服务等情形的，平台需区分情况分析化解风险；加大技术手段的升级换代，提升过滤信息的能力，通过技术手段网聚用户力量，完善举报查处机制。

互联网时代，算法至关重要。短视频平台应当通过技术手段完善推送机制，用正确的价值观指导算法、改进算法。不得向未成年人推送可能引发未成年人模仿的不安全行为、违反社会公德行为及可能诱导未成年人产生不良嗜好等信息，不得利用算法推荐服务诱导未成年人沉迷网络。定期审核、评估、验证算法机制机理、模型、数据和应用结果等，主动向社会公布未成年人保护风险评估报告。

（作者为北京师范大学未成年人检察研究中心兼职高级研究员）

监管实现可视化

为破解非羁押人员监管难题，重庆市渝中区检察院与该区公安分局、区法院、重庆市先进区块链研究院合作，共同研发区块链非羁押数字管控云平台——“渝e管”，该款微信小程序于2022年7月上线。该平台具备可视化实时监控、社会危害性评价、诉讼全流程监督等功能，可对非羁押人员实施全流程监管，助推实现公检法办案数据融合共享。该平台上线以来，共对1800余名非羁押人员启动数字监管，无一人脱管。图为该院检察官读取分析“渝e管”区块链非羁押管控平台可视化大屏数据。

（本报记者满宁 通讯员陈琳 代宛珈/文图）

数字漫谈

创建大数据法律监督模型需理念先行

□贾茂林

随着数字检察工作的不断深入，大数据法律监督理念逐步与检察官办案思维融合，“个案办理—类案监督—社会治理”的办案模式逐步确立。坚定信心、保持定力，在不远的未来，用数字检察这把“金钥匙”打开法律监督新天地可期可见。

在数字检察的当前工作阶段，大数据法律监督模型是实现法律监督模式重塑的重要工具和抓手。今年3月，最高检数字检察工作领导小组办公室下发《关于举办2023年全国检察机关大数据法律监督模型竞赛的通知》（下称《通知》），各地更是掀起监督模型应用的热潮，伴随而来的是广大检察官对大数据法律监督的理论研究、技术实现等各种问题的探索、实践和研讨。

大数据法律监督本质是要实现主动依法履行监督职能。目前各地的实践已经充分证明，诸如对于以合法形式掩盖非法目的的犯罪行为，损害国家利益和社会公共利益，因数据壁垒、信息不对称造成的盲区和行业潜规则，检察官在办案中如果不具备大数据法律监督理念，不去主动依法开展监督，便无法从源头解决问题。等待、被动、就案办案的工作思路肯定做不出好的大数据法律监督模型，更无法有效监督破解社会治理难题。同样，过犹不及，如果不立足于法律监督履职点，不立足于国家治理，就会出现越俎代庖的情况，被人诟病手伸得太长，反而给工作开展带来阻力。

大数据法律监督模型最重要的是要体现办案检察官的理念和思路。监督模型是开展大数据法律监督工作的主要工具和手段，技术实现是关键，好的模型会让检察官把精力集中于办案本身，让检察官办案实现事半功倍的成效。监督模型本质上是把检察官经实践检验成功的、可复制的办案经验技术化、工具化，其中，办案理念和思路是监督模型的灵魂和最主要的价值所在。大部分模型在各地推广应用、复制落地的过程中，都要结合本地需求和本地数据展开，对于很多简单模型，并不需要过多技术元素，用好模型思路（大数据思维）就可以产生很好的办案效果；对于部分复杂模型，需要引入科技“外脑”辅助创建，此时，检察官和技术人员可分工配合，各扬所长，但主导权仍是检察官，模型必须要适应检察官的办案思路，才能取得好的应用效果。各地特别是相对落后的地区，在数字检察工作实践中不能单纯“等靠要”，觉得没有平台、没有模型就不能开展工作；另一方面，更不能“蛮干快上”，一味靠“买买买”来推动工作，这必将适得其反。要以工具论推进大数据法律监督模型应用，但要切忌陷入唯工具论，这会导致只要“面子”不要“里子”，最终走向形式主义。

工作成效是检验大数据法律监督模型的试金石。最高人民检察院检察长应勇指出，数字检察工作要“业务主导”“重在应用”，大数据法律监督模型就是要服务业务、赋能业务进而融合业务，把着眼点和发力点放在解决社会治理难点问题、构建社会治理有效机制上。《通知》中明确要求“参赛作品必须是已经在办案中进行了实际应用，并取得成效的应用类监督模型”，这就是以工作成效作为检验模型成功与否的主要标准，把“重在应用”真正落到实处。无论从哪个角度来说，大数据法律监督的理念等不来，更买不来，我们要立足工作实际，转换理念，不断加强实践，要把竞赛作为推进数字检察工作的契机，不能本末倒置。

（作者为最高人民检察院数字检察工作领导小组办公室处长）