【专题研究】

[文献编码]DOI：10.3969/j.issn.1004-6917.2021.05.002

人工智能嵌入预测警务的法律风险及其预防

沈国琴，齐小力

（中国人民公安大学 法学院，北京 100038 ）

摘要：将人工智能嵌入预测警务，通过预测形成预判，将违法犯罪行为扼杀在实施之前，对于实现“零违法犯罪率”似乎有着巨大的吸引力。但透过理性分析可以发现其中暗含着诸多风险。法律风险即是其中的风险之一。法律风险之所以存在，主要是因为人工智能嵌入预测警务将导致警察权运行逻辑发生改变。这些变化具体表现在警察权运行不再侧重经验判断，而是依据数据计算的结果采取行动；当前尚处于弱人工智能时代，数据计算的逻辑基于相关性形成，因此取代传统的“因果关系归责模式”，相关关系预判成为预测警务的运行逻辑；警察权运行逻辑的重要变化还表现在，警察权权力外显的特征消失。公共场所智能监控、人脸识别、GPS定位等等智能技术正在取代警察的到场，警察不必到场但却能让人感觉到无所不在的权力“在场”。警察权运行逻辑的改变带来的法律风险是多方面的，主要表现在个人权利被侵害、传统法律制度失灵、出现新的权力滥用形式等方面。应针对这些潜在的法律风险，从完善与技术发展相适应的权利保障制度、强化程序控制克服传统法律制度的失灵、通过多元参与克服权力技术化中的权力滥用等方面积极探寻预防的措施和方法，将人工智能嵌入预测警务活动纳入法治的框架之内，以免使用人工智能技术进行警务预测突破法治底线。

关键词：人工智能；预测警务；权利保障；权力制约

中图分类号：DF0-05　**文献标识码：**A　**文章编号：**1004-6917（2021）05-0010-08

当前，人工智能的出现增强了人类的预测能力，人工智能预测开始进入社会各个领域，日常生活中无人能避开的“精准推送”可以说就是人工智能预测的直接产物。人工智能预测同样吸引着政府，“能处理海量数据的智能计算机给政府提供了一种全新的革命性工具”[1]。智慧政务、智慧司法、智慧警务的“智慧”中无不包含人工智能预测的内容。其中，智慧警务对于人工智能预测有更多的期待。随着恐怖主义、极端主义的全球威胁，社会风险因素增多，能够对违法犯罪行为提前预测、预知，从而预警并进行先期控制，这些无不是各国警察部门所普遍期望的。因此，很多国家警察部门开始尝试使用人工智能预测警务，如美国不少警察部门使用PredPol软件、Hunchlab软件，英国达勒姆警察部门使用HART工具，丹麦警察部门使用POLINTEL平台等预测警情。我国智慧公安的建设中也包含通过人工智能进行警务预测的内容，如2013年北京市公安局怀柔分局开始运行“犯罪数据分析和趋势预测系统”[2]；广东公安机关构建的“13847”框架模式①中包含“智慧新防控”的内容，温州公安机关构建的“1+5+15+N”模式②中也有“情

① “13847”框架模式的具体内容是：1个愿景；3步战略；8大创新应用，即智慧新指挥、智慧新管控、智慧新侦查、智慧新防控、智慧新交管、智慧新监管、智慧新民生、智慧新警队；4大赋能工程，即大数据工程、警务云工程、视频云工程、云网端工程以及北斗7星计划。参见《广东公安智慧新警务总体规划解读》（https：//www.sohu.com/a/228039416_119778）。

② “1+5+15+N”模式所指向的内容为：“1”是市公安局“云上公安·在线警务”实战中心，“5”是联合指挥部、情报预警部、合成作战部、信息支撑部、综合协调部五大功能板块；“15”是五大功能板块下的15个分区；“N”是“云上公安，在线警务”实战分中心，“云上公安，在线警务”实战子中心等。参见温州市公安局课题组《构建立体化信息化精准化社会治安防控体系》，载《浙江警察学院学报》2019年第3期，第1-6页。

收稿日期：2021-01-12

作者简介：沈国琴（1972—），女，山西长治人，博士，中国人民公安大学法学院副教授，研究方向为宪法学与行政法学；齐小力（1961—），男，河北保定人，中国人民公安大学法学院教授，研究方向为宪法学与行政法学。

报预警部”的建设，等等。党的十九届四中全会提出“完善社会治安防控体系”的目标，要求：“坚持专群结合、群防群治，提高社会治安立体化、法治化、专业化、智能化水平……提高预测预警预防各类风险能力，增强社会治安防控的整体性、协同性、精准性。”[3]从中可以看出，智能化与提高预测预警预防各类风险能力被关联在了一起。

对于预防违法犯罪的警务工作而言，技术赋能的预测警务具有现实意义，“能够使警务活动更有效率、更为精确”[4]。但与此同时，预测警务也面临诸多质疑。一方面，学界对预测警务的技术前景有不同的声音。有学者指出，“预测警务这个概念从诞生起就受到犯罪预测的可能性及其精确度的争议与质疑”[5]。很多要素无法预测，其中“如不少刑事案件中犯罪者的动机和目的”[6]。另一方面，人们对预测警务可能会带来的道德、伦理、法律等方面的问题充满忧虑，“基于大数据的警务预测难以避免会引发道德、伦理、法律等方面的冲突”[7]。这些忧虑是值得关注的，因为只有保持必要的理性认识和批判才能避免技术为恶的结果。其中尤其值得关注的是法律风险问题。法律是人类发展历程中所形成的行为底线标准。警察权是重要的执法权力形式之一，其必须遵守依法执法的基本要求。因此，及时认识人工智能嵌入预测警务所存在的法律风险，并在此基础上找到预防和化解风险的措施与方法是迫切且重要的。

一、人工智能嵌入预测警务中警察权运行逻辑的转变

关于预测警务的概念，一般认为是基于概率统计方法形成的预判。2013 年美国兰德公司曾撰写题为《预测警务——犯罪预测在执法机构业务运作中的角色》的研究报告，其中将预测警务界定为“通过应用分析技术，特别是量化分析技术，实现统计预测，为警察干预、预防犯罪或者解决已发犯罪提供可能的目标”[8]。这一概念符合人工智能技术嵌入预测警务的发展方向，强调警务预测基于大数据统计而形成。

人工智能与预测警务相结合使得警察权运行逻辑较之前有了很大的差别。这是理解人工智能预测警务中存在法律风险的前提。

（一）从侧重经验推断到依赖数据计算

人工智能技术运用于警务活动之前，预测警务建立在小样本数据基础之上，概率统计方法难以发挥作用。这往往导致警务预测在很大的程度上依据经验进行推断，“警务运行的质态或工作生态主要表现为警务工作判断、决策中具有明显的经验惯性，太过依赖于以前的警务经验积累和警务惯性思维，即经验型警务”[9]。而经验型预测的最大困境是过于依赖特定的个人，富有经验者与缺乏经验者之间差距非常明显。而即使是富有经验者，也存在很多难以克服的局限性，如受制于自身主观性和有限理性等问题。

人工智能的出现则使警务预测得以在大样本数据的基础上通过概率统计的方式运行，“让数据发声，运用大数据开展情报分析进而合理调配警力资源的预测警务，是预防和打击违法犯罪、保障社会公共安全、解决当下警力资源不足的新思路”[10]。人工智能预测警务依赖于大数据的采集和基于大数据的智能算法。随着智能技术的不断推进，大数据的采集涵盖的领域越来越广，采集的渠道越来越多，包括“图像（含人像模型）、视频、RFID、GPS、DNA、指纹等。数据的采集可通过移动互联网、物联网传感等技术来进行智能化的多方位立体采集”[11]。海量数据在人工智能算法的框架内开始变得有了生命力，“将来源不同的数据筛选和综合碰撞在一起，进一步生产出新的具有实际意义的相关犯罪信息”[12]。从整个人工智能预测警务的流程来看，从采集形成海量的结构化和非结构化数据开始，到通过智能化技术进行数据挖掘、比对、分析，再到数据画像、绘制犯罪热点地图，可以发现通过“数据驱动”而形成“数据计算”是人工智能预测警务的主线。人工智能警务预测使得很多看似不相关的数据信息联系在了一起，完成了大量人脑无法完成的任务。与经验推断相比，数据推算摆脱了对具体的有经验的个人的依赖，克服了因为选择性记忆、个人偏好等原因而产生的主观性问题，也在很大程度上克服了人的有限理性问题。

（二）从因果关系归责到相关关系预判

警务活动的核心任务是维护公共安全和秩序，不可避免地涉及对违法、犯罪行为进行制止、惩戒的强制性权力的使用。在已形成的法律追责体系中，警察权对违法、犯罪行为的追惩往往遵循因果关系法则，要求违法、犯罪行为与产生的危害后果之间必须存在因果关系。尽管对于法律上的因果关系如何理解，其要素包括哪些等问题长期以来一直颇有争议[13]，但法律责任必须基于“因果关系”的观点却不曾改

变，属于基本共识。

人工智能预测警务从根本上改变了惩戒违法犯罪行为的认知模式，算法决策基于建模计算和数理逻辑，这样就在决策系统中改写了知识逻辑，实现了数理逻辑的加持。此时，人们“不再热衷于寻找因果关系”[14]。关于违法犯罪的归责模式开始从“因果关系归责”模式向“相关关系预判”模式转变。可能随着强人工智能的出现，弱人工智能的“相关关系”特点会向“因果关系”方向转变，“在强人工智能证成中，图灵奖获得者朱迪亚·珀尔（J.Pearl）的因果推断理论是最具特色的理论”[15]。但是，就现有的人工智能发展水平来看，人工智能预测警务仍然只能采用具有“相关关系”特点的弱人工智能。

与弱人工智能相结合的预测警务一般被应用于违法犯罪热点的预判和具体的违法犯罪人或受害人的预判。就违法犯罪热点预判而言，其主要是对违法犯罪风险高发地区的概率推测，“对过去犯罪数据中的模式和相关性进行识别和分析，预测发生犯罪概率较高的时间和地点，并将警力部署到可能发生犯罪的地区”[16]。而就具体的违法犯罪人或受害人的预判而言，则指向明确具体的个体，“通过智能技术分析过去犯罪活动的社交网络，使用机器学习和算法来识别可能的肇事者或受害者”[17]。通过人工智能预测警情无疑对警察权运行产生巨大影响。当获得对违法犯罪风险较高的地区和时间节点的预判结果时，就可提前部署警力，预防违法犯罪行为的出现；当获得对违法犯罪人的预判结果时，就可提前介入避免违法犯罪人犯罪。可以看出，无论那种预判，都是以统计模式为基础而形成的算法，通过大数据运算而计算出的结果。从这一过程可知，通过计算所形成的结果实际上是一种概率上的可能性，是一种不确定性。这意味着对警情的预测只是基于算法而形成的推算结果而已，至于是否会发生，则可能会有正相变化，也可能会有负相变化。

（三）从权力符号外显到权力的技术化内置

警察权的设置是一个社会公共安全秩序的基本保障。警察被视为街头官僚，其常常通过权力符号外显达到向社会展示权威的目的。着警服出现于公众面前，且佩戴警械、武器等都是权力符号外显的具体表现。警察的权力符号外显具有“劝说”社会公众自愿服从并配合警务活动的作用，也隐含“威慑”和“强制性”作用，意味着警察可以使用强制手段处置违法犯罪行为，使失序的社会状况回归正常。见警率一度是城市安全的重要标识。人工智能的介入改变了警察权的权力符号外显的运行逻辑，警察权越来越多地被内置在人工智能技术之中。“公共权力部门则在智慧政务、智慧司法、智慧检务的战略目标下，把网络技术、数字技术和人工智能技术作为一种技术赋能，在其权力运作过程中加以日益广泛和深入地应用，如智能监控、人脸识别、智能辅助办案系统等，这些算法决策和代码规制便形成了权力技术化的态势。”[18]公共场所智能监控、人脸识别、GPS定位等等智能技术正在取代警察的到场，人们往往看不到警察，但却能感觉到无所不在的权力“在场”。警察权无需在场就能完成信息的收集。并且这些信息与警方数据库中已经采集到的身份证、车牌号码、违法犯罪记录等各种信息比对、碰撞，关于个人的立体画像就得以形成。“慢慢地积累所有数据，直至在计算机数据库中形成一个‘人’”[19]。在警察权面前，人成为立体透明的，甚至个人未来发生违法犯罪的概率也一并被计算了出来。

在人工智能与警务相结合的场景中，警察权运行逻辑发生变化的同时，也带来了与社会公众之间关系的改变。警察权符号外显的目的无非是为了减少对抗，强化相对人的服从及社会公众的配合。但当人工智能介入时，关于服从及配合的讨论竟然失去了意义，因为无论服从与否、配合与否，个人的行为及其轨迹均可以一览无遗地进入公权力监视的范围之内；无论服从与否、配合与否，算法已预设，代码已生成，关于个人行为的预测，以及针对预测应采取何种措施的预判在悄悄地做出。不必见警，警察就在身边，警察权已内置在技术之中，这是人工智能预测警务的真实写照。

二、预测警务中人工智能嵌入存在的法律风险

人工智能预测警务蕴含了警察权运行逻辑的巨大变化。这套新的逻辑背后隐藏着诸多法律风险，对此必须给予必要的关注。

（一）个人权利被侵害的隐忧

人工智能预测警务运行的基础在于数据，“数据犹如‘智慧公安’的‘血液’，是‘智慧公安’中最基本、最重要的因素，影响和决定了‘智慧公安’的效用。”[20]数据的重要性已为人所共知，不言而喻。但数

据收集、处理过程却暗藏着侵害个人权利的风险。

人工智能预测警务的数据收集和处理的过程中，易于受到侵害的权利主要有“信息权益”和“个人隐私权”。这两类权利虽然在《中华人民共和国宪法》中尚没有明确规定，但是从宪法教义学的角度分析，宪法第三十八条关于公民人格尊严的规定，第三十九条关于住宅权的规定，第四十条关于通信自由和通信秘密的规定中包含有信息权益和隐私权的内容。2017年颁布的《中华人民共和国民法总则》中，第一百二十七条、一百一十条、一百一十一条分别关注数据保护、隐私权和个人信息保护等方面的问题，及至2020年《中华人民共和国民法典》（以下简称《民法典》）出台，这种立法思路得到延续，其在第一百二十七条中规定了法律对数据保护的内容；对信息保护的规定则内容较多，在第四编人格权中专门规定了一章内容，即第六章“隐私权和个人信息保护”。由此对隐私权和个人信息保护规定更加全面。同时，个人信息保护的专门立法已开启，《中华人民共和国个人信息保护法（草案）》（以下简称《个人信息保护法（草案）》）已于2020年向社会公布。综上可以看出，隐私权和个人信息权益等权利形式正在茁壮成长，在要求平等主体不得侵害的同时，也要求国家公权力机关不得侵害。

对于人工智能预测警务而言，所涉及的信息保护对象是以数据为载体而形成的信息内容，即“数据信息”，因此主要涉及“数据信息权益”的内容。人工智能预测警务活动中常见的侵害“数据信息权益”的问题主要集中在数据真实权、知情权、数据修改权和删除权等方面。要避免个人数据信息权益不被侵害首先要避免出现数据库中数据失真的问题。可能导致数据失真的原因有很多，可能是欺骗性数据，如基于“换脸技术”而收集的数据；也可能是注水数据，如网络水军注水而形成的数据；或者仅仅因为数据没有及时更新而导致数据失真，等等。无论何种原因都极有可能使人工智能预测警务形成致命的预测错误，造成严重的后果。数据真实与否直接关系人工智能预测警务的结果，是其发挥作用的前提，更会与相关个体的合法权益有密切关系。数据真实在人工智能预测警务中至关重要。但是，现实的问题是数据是否真实，数据权主体往往自己都不知道，这会导致侵害权利的风险无法被消除，且不断向后传递，带来更多侵权的结果。而这种现象又与数据知情权、数据修改权和删除权等权利未能得到保障直接相关。

在数据收集、数据融合过程中，个人的隐私权也存在被侵害的风险。一方面，存在公共空间隐私权被侵害的风险。传统空间隐私权的理论一般认为公共空间不存在隐私权。但是在公共视频监控被大量使用的年代，这一理论并不周延。在没有拍照和摄影设备的年代，公共空间内不愿被他人看到的隐私和尴尬瞬间即可被忘记，但公共视频所具有的长期保存、一键定格且可被反复观看的特点使得隐私和尴尬瞬间成为“永久画面”，此时隐私权保护就成为必要。比如一位女士在公共场所时，她的裙子不小心被风吹起，这本是瞬间就可化解的尴尬，但公共视频的拍摄却有了不同的结果。因此，一般认为“即便他人身处某一公共场所，他人的某些事务仍然可能是其私人事务”[21]。另一方面，存在个人的隐私信息被侵害的风险。警察部门利用自己所掌握的或者共享的庞大的数据库资源进行数据融合、碰撞，往往形成对预测对象的洞察，描摹出个人的立体画像，某些个人不愿意为人所知晓的行为特征、价值取向也被呈现出来。显然，这其中包含了侵害个人隐私权的风险。“无处不在的数据分析、数据画像和精准推送，已经扯开了传统隐秘空间上的面纱，个人很难再找回自己那个曾经无人知晓的‘后花园’，成为‘无隐私的公众’”[22]。透明人是对数字时代中的人的真实描述，而透明，尤其是在公权力面前的透明，正在不断消解个人的隐私权。

（二）传统法律制度失灵的风险

人工智能预测警务虽以预测为目的，但是预测并非终点，预测结果要为警务工作服务。“预测警务并不仅仅停留于预测，而是要求执法人员以数据分析结果为依据，将特定主体与犯罪行为进行预判性匹配，并基于该预判采取针对特定个人的犯罪控制措施。”[23]人工智能对违法犯罪行为或者违法犯罪人的预测往往要求在违法犯罪行为发生之前就加以制止。“对我们而言，危险不再是隐私的泄露，而是被预知的可能性——这些能预测我们可能生病、拖欠还款和犯罪的算法会让我们无法购买保险、无法贷款、甚至在实施犯罪前就被预先逮捕”[24]。基于人工智能警务预测而形成实施犯罪之前预先逮捕的做法尽管带来“零犯罪率”的美好预期，但是却会从根本上动摇着人类长久以来积累形成的刑事侦查制度，解构既有规则。

传统的侦查是一种对过去事实的回溯性重构，通过客观证据在嫌疑人与违法犯罪行为之间建立关

系。侦查启动以及刑事强制措施的采用往往要基于“嫌疑”“有证据证明”[①]或者“合理根据”或“相当理由”等条件[②]。这些条件虽然可能存在程度上的差异，但构成“嫌疑”的本质是存在客观证据能够证明行为人与具体案件之间具有直接、明确、紧密的关联关系。但是，人工智能介入之后，通过数据运算形成对违法犯罪的提前预判，此时侦查启动或强制性措施的采用所依据的就不再是基于客观证据而形成的“嫌疑”，仅仅是依据数据画像而形成的概率上的可能性，仅仅是基于类型化的预测。如英国2015年的Beghal案就展示了这样的趋势。该案中当事人Beghal在机场遭到警方的盘问和搜查，这并不是因为Beghal实施了任何具体的可疑行为，只是因为警方在相关性信息的汇总、筛选之后发现Beghal的丈夫因实施恐怖主义犯罪正处于羁押中[③]。显然，依据算法形成“嫌疑”，并进而采取强制措施的做法正在打破传统制度的要求。

传统的侦查制度基于对侦查权滥用的警惕构建了较为严格的约束机制，主要包括：启动侦查必须遵循严格的程序规则和对被立案侦查对象的程序性权利予以保障。但是随着警方掌控的技术手段的增加，严格的规则能够被绕开，存在无法发挥程序约束的风险。传统程序约束规则所针对的是物理上强制措施，如搜查、扣押等，或采取传统技术手段进行的监听或监视，而新的技术手段完全可以在不接触当事人，不进入私人空间，当事人不知晓的情形下静悄悄地进行。通过数据计算形成对具体个体的嫌疑时，特定指向性技术手段就可以随之跟进，形成对特定个体的特定监控。而从普遍化监控、类型化监控到具体个体的监控的推进往往已经内置于技术之中，程序控制无法发挥作用。尤其需要注意的是，由于人工智能技术存在算法错误、算法偏差、算法偏见、数据分析挖掘结果存在误差等问题，无辜的人极有可能被算法计算成“嫌疑人”，而传统制约制度的失灵必然会带来令人恐怖的后果。

（三）无法消解权力滥用的问题

在人工智能将权力内化为算法、代码的过程中，出现了新形式的权力滥用问题。

首先，对法律规范再解释时的权力滥用问题。通过人工智能的方式预测警情或者违法犯罪人，首要的前提是把法律语言“翻译”成计算机语言，把法律规范“转换”为机器代码。在这个过程中，“翻译”、“转换”的本质就是“解释”。尽管对于抽象的法律规范往往会通过立法解释或者司法解释的方式对其具体化，使其具有可操作性，但即使如此，很多法律概念、法律条件仍然存在模糊性。在这种情况下，代码编写中对法律概念的再解释，对法律条件的再认识就会深刻地嵌入其中。如《中华人民共和国刑法》第一百一十四、一百一十五条规定了“以危险方法危害公共安全罪”，其中“危险方法”“公共安全”等不确定法律概念就需要加以解释。为此，大量的司法解释出现。其中2020年《关于依法惩治妨害新型冠状病毒感染肺炎疫情防控违法犯罪的意见》是众多司法解释中一个。该司法解释中规定：“新型冠状病毒感染肺炎疑似病人拒绝隔离治疗或者隔离期未满擅自脱离隔离治疗，并进入公共场所或者公共交通工具，造成新型冠状病毒传播的。”属于以危险方法危害公共安全罪。而此解释中关于“疑似病人”“公共场所”“公共交通工具”等概念均没有明确的列举。这意味着，把这些概念解释清楚，并列举出来就有了非常大的解释空间。而此类法律规范再解释的问题是在编写算法，形成代码时的普遍现象。由此看来，为编写代码提供标准和依据的执法主体就成为再解释主体，其受外在约束较小，再解释权滥用的风险极大。

其次，基于偏见而产生的权力滥用的问题。人工智能预测警务以预测警情或者违法犯罪人为目的，这种目的必然要求对“什么样的人更容易违法犯罪”进行判断。对于预测违法犯罪人的智能系统而言，运算出这种判断结论需要向其输入“与可能发生的违法犯罪行为相关的要素特征”。如果警察部门为编写代码者提供的判断要素本身就存在偏见，将某些地方打上犯罪高发地区的标签，把某些特定身份或者经历的人群打上高发违法犯罪人群的标签，那么即使算法中立，最终的运算结果也将是充满偏见的。“将贫困、家庭状况、种族或民族、社会经济地位等维度输入进去……从这个角度说，犯罪人预测是显失公平正义的，他们被预测是危险的‘犯罪人’并据此受到惩罚，不是因为他们做过什么，而是因为他们是谁、他们的家庭怎么样以及他们的口袋里有多少钱。”[25]以偏见为前提的代码编写，将会把程序运行的结果引向错

①如《中华人民共和国刑事诉讼法》第一百零九条规定立案的条件是“发现犯罪事实或者犯罪嫌疑人”，第八十一条规定逮捕的条件是“有证据证明有犯罪事实”；第一百三十六条规定搜查的条件是“犯罪嫌疑人以及可能隐藏罪犯或犯罪证据”。

②英美法系刑事侦查启动条件的确立是在与盘查相区别的过程中形成的，侦查一般须有“合理根据”或“相当理由”，盘查则根据“合理怀疑”。参见王兆鹏《路检、盘查与人权》，台湾元照出版有限公司2003年版，第94页。

③见Beghal v Director of Public Prosecutions〔2015〕UKSC 49.

误的预测，从而导致权力的滥用。

最后，人工智能预测结果不当使用的问题。人工智能预测警务被设计出来的目的无非是得到预判，采取预防措施制止违法犯罪行为，减少社会的不安全因素。但是，由于惩罚违法、犯罪的制度设计中包含“经济罚”的内容，经济收益在一定程度上会成为执法权力滥用的动力。实践中也曾出现过此类案例，“荷兰警方通过分析TomTom导航仪记录的道路速度数据，在那些最可能创收的地方设置限速陷阱”[26]。从这种典型的“数据钓鱼”执法中可以看到，由于技术的加持使得权力滥用更加精准、更有收益。

权力的技术化内置的过程中，权力滥用的形式多种多样，上述所列只是非常典型的形式而已。在实践中，甚至还存在为特定目的，或者为特殊人群布设“后门”而带来的权力滥用问题。总的来看，权力的技术化内置并没有消解权力滥用的问题。

三、预测警务嵌入人工智能法律风险的预防

预测警务嵌入人工智能后出现了大量法律风险，有些属于制度滞后导致的；有些属于制度落实上不严格的问题；还有些属于技术发展本身的问题。在人工智能预测警务发展的推进过程中应当针对不同的法律风险确定不同的预防方案。

（一）完善与技术发展相适应的权利保障制度

技术发展的目的是要让人更自由、生活更美好，因此人的权利和尊严应当是技术创新和发展的首要价值，“在价值上申言数字科技必须以人为本，必须把人的权利及尊严作为其最高目的，并以人权作为其根本的划界尺度和评价标准”[27]。随着技术发展，一些不曾被人们所认识的权利类型开始出现，如前文所谈及的“数据信息权益”“个人隐私权”即属于此种类型。法律有必要及时回应技术发展确立这类权利的地位，并明确法律保护的范围。《民法典》中写入“数据保护”，“隐私权和个人信息保护”都是对时代回应的最直接体现。但是民法上所规定的仅是民事权利，所对抗的对象是平等主体。而人工智能预测警务所涉及到的是公权力与公民权利之间的关系，保护内容、方式等方面都会存在较大的差别。有必要在公法体系中完善与技术发展相适应的权利保障制度。

我国关于信息权益保护的公法体系正处于建设之中。2017年公布的《信息安全技术个人信息安全规范》（以下简称《安全规范》）中就关涉公权力收集、处理个人信息的规则。2020年10月21日公布的《个人信息保护法（草案）》中专门有“国家机关处理个人信息的特别规定”的内容。相较于《安全规范》而言，该法对公权力处理个人信息权益规则有了重大突破。《安全规范》规定公权力收集信息、使用信息等方面都可遵循“知情同意例外”的原则，即公权力在收集和处理信息时不必征得当事人同意；《个人信息保护法（草案）》则改变了绝对例外的态度，对国家机关处理“个人信息”采用“告知+同意”的模式①。这一改变极有意义，有助于督促公权力在处理个人信息时尊重当事人的意愿，保持谨慎处理的态度。《个人信息保护法（草案）》的精神虽然带来公权力与数据信息权益关系的崭新变化，但是对技术发展复杂程度的考量仍不够充分。如前文所述，人工智能预测警务极有可能因为数据失真把某些个体预测为违法犯罪嫌疑人。为避免此种情况出现，有必要确立针对公权力的“告知+确认”规则。若数据处理之后出现对当事人不利的或者负面的评价或者预测时，被预测者享有“数据信息真实权”，由此而派生出“告知+确认”权，由其确认所处理的信息真实无误；一旦出现信息错误，个人享有修改和删除的权利。至于数据收集、数据融合过程中个人隐私权保护的问题，需要特别注意公权力在收集时尽可能明确标识，保障当事人形成合理的隐私期待。同时对于收集到的信息使用也应有相应的规则。这些权利保障内容开始获得《个人信息保护法（草案）》的关注。因此，个人信息保护法的出台值得期待。不过个人信息保护法的目标定位是信息权益保障的基本法，这意味着其规定是原则性的，更为具体规定有待于个人信息保护法出台后对公共视频监控中涉及到的隐私权作专门规定。

（二）强化程序控制克服传统法律制度的失灵

警察部门根据人工智能所确定的“嫌疑人”进行针对性监控时，有必要加强程序的控制。我国现在的

①《个人信息保护法（草案）》第三十五条规定：“国家机关为履行法定职责处理个人信息，应当依照本法规定向个人告知并取得其同意；法律、行政法规规定应当保密，或者告知、取得同意将妨碍国家机关履行法定职责的除外。”

刑事诉讼制度对于使用技术侦查措施规定了严格的批准手续，但仍被置于公安机关内部。鉴于预测警务只是基于相关性数据的挖掘、处理的基础上而形成的“嫌疑”，不同于基于因果关系而形成的“嫌疑”，误判的风险较大，因此应当给予更为严格的程序控制。严格程序控制的典型方法就是引入第三方进行权力制约，核心是引入司法权。司法机关作为审查机关，在确定是否有必要采取针对性侦查措施时不能仅依据数据分析结果，“仅有数据分析结果不足以确认‘有犯罪事实’或单独作为定案根据，需要有其他类型证据予以补强和印证”[28]。如果不引入第三方进行权力约束，警察部门往往并无动力在数据分析结果之外收集其他类型的证据。同时应当注意的是，人工智能从大规模监控到对具体的推算出来的“嫌疑人”进行监控的“转变”可能已经内置在了技术之中，此时司法审查程序就有被规避的可能。因此可以考虑把司法制约程序内化到程序之中，当进行针对性的“监控”时自动推送到司法机关的审查平台上，由司法机关进行必要的审查。并且，将审查处理结果也内置化到技术之中：审查同意，具体的针对性“监控”程序继续进行；审查未获得通过的，“监控”程序则无法启动。通过此种方式有效回应传统法律制度的失灵问题。

（三）通过多元参与克服权力技术化中的权力滥用

人们已经意识到，人工智能所存在的倾向和偏见源于人类自己，“由于这种倾向根植于人类社会本身，因此不应归咎于大数据等信息技术的运用”[29]。技术的作用仅在于它会不断迭代强化这种倾向或者偏见。因此，从源头减少不恰当的倾向、减少偏见至关重要。源头减少的方式应当是在警务预测技术化过程中不仅要考虑警察权的权力运行需求，而且也要考虑制约警察权的各方面要求。应当考虑使预测警务从单纯关注警察权运行的模式转变为吸纳多元主体参与的模式，以减少算法、代码中的偏见和歧视。一是法律再解释时应吸纳立法机关、裁量基准制定机关的意见。如果只由使用预测警务系统的警察部门形成对法律再解释的意见，并形成相关算法的话，会使得关于预防、打击违法犯罪的法律认识的模型中潜藏部门意见，而这往往是一种不全面或者有偏见的模型，是一种“残缺的模型”。“模型是以往经验与未来推断之间的桥梁，人们只有借助模型才能看到已然与未然的联系。所以，残缺的模型是对原始样本信息和人们集体经验的肢解。”[30]为了避免法律再解释权被滥用，有必要在把法律内容转化为代码时，充分吸纳更有权威机关的解释意见，其中主要包括立法机关、裁量基准制定机关等对法律规范把握更准确的机关。二是违法犯罪特征代码化的过程中应吸纳社会公众的意见。关于违法犯罪的特征，不同的群体有不同的认识。警察部门在打击违法犯罪过程中随着经验的积累，往往能够形成专业化认识，但是同样也会带来固化思维，极易对特定群体形成标签化认识；也极易仅从单一角度认识问题，无法在公共秩序与个人权利之间进行兼顾。如果警察权在封闭的框架内运行则难以走出固化的、单一化的思维模式，因此有必要打破这种封闭权力运行模式，把社会公众的认识也纳入其中。这意味着在技术赋权进程中，“必须与民众所生活的社会维度、政治维度以及个体维度相结合，以便让赋权实践与包容、参与以及社会正义相结合”[31]。从不同的角度认识违法犯罪行为的特征，一定程度上有助于减少基于权力的偏见而导致算法的偏见。

综上，人工智能技术正在剧烈影响着人类的生活方式和活动方式。人工智能技术与权力的结合使得公权力具有更大的社会影响力，“干涉他人的能力、维稳能力和法律强制力不断增强”[32]。同样，人工智能和预测警务的结合也深刻地改变着警察权的运行逻辑及其影响社会的方式，基于大数据计算而形成的警务预测对于预防违法犯罪具有不可低估的意义。但是，在这种新的预测警务方式之中却也隐藏着诸多法律风险。对此，必须保持必要的警惕。当然，对于嵌入人工智能的预测警务所潜藏的法律风险的分析并非要否定这种技术带来的积极价值，而是要通过制度建设遏制风险，在技术向善的框架内找到公共安全和秩序及个人权利之间恰当的平衡点，推动嵌入人工智能的预测警务在法治的框架中前进，为推动“法治中国”、“平安中国”的建设发挥积极的作用。

参考文献：

[1]乔治·扎卡达基斯.人类的终极命运——从旧石器时代到人工智能的未来[M].陈朝，译.北京：中信出版集团，2017：296.

[2]黄洁.抢劫案件同比下降超过五成[N].法治日报，2014-06-17（02）.

[3]中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的

决定[EB/OL].(2020-11-05)[2019-11-05].http://www.12371.cn/2019/11/05/ARTI1572948516253457.shtml.

[4]Berk Richard A.Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement[J].The Annual Review of Criminology Volume 4, 2021: 209-237.

[5]郭伟.美国预测警务的发展与启示[J].公安教育, 2019(5): 73-77.

[6]马长山.司法人工智能的重塑效应及其限度[J].法学研究, 2020(4): 23-40.

[7]彭志辉.基于大数据的警务预测: 局限性及其顺应之道[J].中国人民公安大学学报(社会科学版), 2016(2): 37-45.

[8]Perry W L, Mclnnis B, Price C C, et al.Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations[M].RAND Corporation, 2013: 1.

[9]汪勇.关于中国警务改革若干问题的思考[J].中国人民公安大学学报(社会科学版), 2003(2): 30-36.

[10]张葆葆.大数据时代下犯罪预测的应用与限制研究[J].犯罪研究, 2020(1): 16-23.

[11]曹艳红.浅谈"智慧公安"建设中的大数据应用[J].大众科技, 2015(11): 24-28.

[12]丁欣荣, 夏军, 孙树峰.智慧公安视域下运用大数据进行犯罪分析与犯罪预测研究[J].上海公安学报, 2020(3): 5-12.

[13]陈兴良.刑法因果关系: 从哲学回归刑法学[J].法学, 2009(7): 22-42.

[14]维克托·迈尔-舍恩伯格, 肯尼斯·库克耶.大数据时代: 生活、工作和思维的大变革[M].盛杨燕, 等译.杭州: 浙江人民出版社, 2013: 17-18.

[15]涂良川.因果推断证成强人工智能的哲学叙事[J].哲学研究, 2020(12): 110-121.

[16][17]James Capotosto.Data Opportunities and Risks: The Dynamic of Public, Personal, and Commercial Interest[J].Journal of Community Safety & Well-being, Vol. 2, 2017(1): 19.

[18]马长山.数字社会的治理逻辑及其法治化展开[J].法律科学(西北政法大学学报), 2020(5): 103-111.

[19]约翰·帕克.全民监控——大数据时代的安全与隐私困境[M].关立深, 译.北京: 金城出版社, 2015: 14.

[20]祁筱.浅谈当前"智慧公安"建设中数据方面存在的问题及对策[J].信息化研究, 2019(10): 77-80.

[21]张民安.美国当代隐私权研究[M]. 广州: 中山大学出版社, 2013: 190.

[22]约翰·帕克.全民监控——大数据时代的安全与隐私困境[M].关立深, 译.北京: 金城出版社, 2015: 1.

[23][28]裴炜.数据侦查的程序法规制——基于侦查行为相关性的考察[J].法律科学(西北政法大学学报), 2019(6): 43-54.

[24]维克托·迈尔-舍恩伯格, 肯尼斯·库克耶.大数据时代: 生活、工作和思维的大变革[M].盛杨燕等, 译.杭州: 浙江人民出版社, 2013: 22.

[25]SonjaStarr.The Odds of Justice: Actuarial Risk Prediction and the Criminal Justice System. CHANCe, 2016, 29(1): 49-51.

[26]TomTom被曝道歉后继续向警方出售用户超速数据[EB/OL].(2011-05-09)[2021-03-01]. people.techweb.com.cn/2011-05-09/1031330.shtml.

[27]马长山.数字时代的人权保护境遇及其应对[J].求是学刊, 2020(3): 103-111.

[29]Jenia I.Turner.Managing Digital Discovery in Criminal Cases[J]J.Crim.L.&Criminology.2019(3): 107-109.

[30]白建军.法律大数据时代裁判预测的可能与限度[J].探索与争鸣, 2017(10): 95-100.

[31]Robert Adams.赋权、参与和社会工作[M].汪冬冬, 译.上海: 华东理工大学出版社, 2013: 201.

[32]约翰·帕克.全民监控——大数据时代的安全与隐私困境[M].关立深, 译.北京: 金城出版社, 2015: 1.

责任编辑: 邓双霜