

大数据犯罪预测的法律分析

朱浩文

华东政法大学, 上海

收稿日期: 2022年10月20日; 录用日期: 2022年12月1日; 发布日期: 2022年12月8日

摘要

在大数据时代下, 人工智能技术的应用已经改变了传统的侦察模式。目前, 警方可以通过大数据分析进行犯罪预测, 对犯罪行为人的犯罪动向进行提前的研判, 从而将其逮捕, 提前介入, 让犯罪行为还没有开始就已经结束, 将其消灭在萌芽之中。这种对于犯罪活动事前型的主动介入模式在侦察、治安邻域具有重大的革新意义, 但同时也带来了相应的理论问题。本文主要介绍了大数据犯罪预测的原理, 并简述了其在实践中的应用情况, 通过试析大数据犯罪预测的特征, 得出了该模式目前在实践中的割裂性、歧视性、自动化偏差和数据管理机制缺失等问题。同时, 笔者结合了大数据犯罪预测在智慧警务中的优势分析, 正视其“双刃剑”的作用, 初步得出了求同存异, 有限、合理应用该项技术的观点。

关键词

犯罪预测, 大数据, 侦察, 智慧警务, 贪污

Legal Analysis of Big Data Crime Prediction

Haowen Zhu

East China University of Political Science and Law, Shanghai

Received: Oct. 20th, 2022; accepted: Dec. 1st, 2022; published: Dec. 8th, 2022

Abstract

In the age of big data, the application of artificial intelligence technology has changed the traditional reconnaissance mode. At present, the police can predict the crime through big data analysis, study and judge the criminal trend of the perpetrator in advance, so as to arrest and intervene in advance, so that the criminal act has ended before it starts, and is eliminated at the beginning. This proactive intervention model for criminal activities in advance has great innovation significance in the reconnaissance and security neighborhood, but it also brings about corresponding theoretical problems. This paper mainly introduces the principle of big data crime prediction, and briefly describes its application in practice. By trying to analyze the characteristics of big data crime pre-

diction, we find out the problems such as fragmentation, discrimination, automatic deviation and lack of data management mechanism in the current practice of this model. At the same time, the author combined the advantage analysis of big data crime prediction in smart policing, faced up to its role as a “double-edged sword”, and initially came to the view that seeks common ground while reserving differences, and limited and reasonable application of this technology.

Keywords

Crime Prediction, Big Data, Reconnaissance, Smart Policing, Corruption

Copyright © 2022 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 大数据犯罪预测原理简述

1.1. 传统的侦察模式的突破

传统的犯罪侦查是反应型的被动侦察模式，侦察总是要劣后于犯罪行为的发生，公安机关只能做到打击犯罪而无法做到预防犯罪。但是，大数据时代，由于信息技术的发展，公安不仅仅可以通过数据搜索、数据挖掘、数据碰撞、数据建模的方式进行事后的侦察活动，甚至可以在事前进行主动型的预测和介入[1]。

1.2. 时间线性突破：从“犯罪心理画像”到“数据画像”

人类活动总是在时间轴上被裹挟前进。而在犯罪预防方面，大数据革命性地实现了这种时间线性的突破。过去，侦察活动往往只能通过“犯罪心理画像”——侦察人员根据犯罪现场遗留的痕迹、物证等信息，结合主观经验判断，对犯罪嫌疑人的外形、身份、心理活动等进行描绘。但是现在，可以通过对侦察机关数据库、社会公共数据库、大数据公司的用户数据中的数据与情报进行研判，对犯罪嫌疑人或相关人员的基本信息进行“数据画像”，从个人基本信息、形体特征、行为轨迹、消费习惯、经济状况、兴趣爱好等信息中提炼出性格特征、行为特征、职业特征，从而实现针对高危人员预警的功能[2]。目前，我国公安机关就已经构建了“刑事专业研判平台”，通过对前科犯罪人员数据库、旅馆住宿数据库、网吧上网数据库等信息进行算法处理和特征点筛选，初步实践了大数据画像的犯罪预警功能。

2. 现实运用状况

2.1. 域外(美国)现状

根据联合国的调查数据表明，刑事系统的费用支出比例往往能够达到犯罪所造成损失的 40%~50%，而采取有针对性的犯罪预防措施却能将刑事系统的支出有效减少 1/2 到 1/7。早在 1829 年，比利时的统计学家凯特就运用概率论较为精准地预估了法国 1830 年法国的犯罪行为总数和罪行种类。到了大数据时代，美国就对这种性价比极高的“预测警务”进行了大量的实践。早在 2008 年，美国就在洛杉矶警局、司法援助局和国家司法委员会的共同推动下，开始推行“预测警务”执法理念，盗窃犯罪率降低了 33%，暴力犯罪降低了 21%，财产类犯罪降低了 12% [3]。2011 年，美国《时代杂志》更是将大数据的“出警预测”程序评选为年度 50 大最佳发明[4]。该程序能够预测加利福尼亚地区的犯罪活动发生地以及发生时间。目前，芝加哥、孟菲斯地区的警方已经不满足于仅仅预测犯罪地点，而是升级到了犯罪人的预测，

引进了 IBM 研发的“Blue Crush”分析软件，该软件能够分析包括人类遗传基因在内的庞大数据，罗列出街区内最有可能犯罪的嫌疑人名字与照片，如果其基因显示犯罪可能很高，就可以对其进行逮捕[5]。此外，美国还通过 COMPAS 人工智能算法，进行了“十分”制的打分用于研判有过犯罪记录的人未来犯罪的几率，作为法官判案和警方盘查时的重要参考。

2.2. 中国现状

在我国，部分地区也已经展开了犯罪预测的实践。其中，最典型的北京和江苏、浙江、广州等地。2013 年，北京市公安局怀柔分局就开始运行了“犯罪数据分析和趋势预测系统”，有针对性性地调配人手、部署警力，使得犯罪率明显降低。苏州也使用公安 PPS 犯罪预测指导巡防工作，改“案后研判”为“案前预警”，使得财产类犯罪下降幅度超过了 15%，取得了显著成效[6]。

3. 特征及存在问题

3.1. 隐私权：公益与私益之争

关于隐私权这类伦理困境问题，是大数据语境下的一个共性问题。其中的授权行为问题、数据所有权问题在学界已经经过了广泛的讨论，本文在这里就不再做过多的赘述。只不过，在其他大数据摘取的问题上，可能还是效率和个人权利的冲突，但是在犯罪预测的刑事语境下，这种冲突可能已经上升到了公益与私益之争。为了打击犯罪的正义目的，是否能够牺牲个人的隐私，甚至允许公权力机关对你进行审查和全面的“数据画像”，直到现在还是没有有一个定论。即便是新出台的个人信息保护法，对于此问题也没有做出正面、详细的回应。同样地，即使是匿名化的技术手段在这里同样无法起到有效作用，零星的部分数据可能是单独无害、经过授权的，但是这些数据结合在一起，在量上的积累就有可能造成对隐私权甚至是声誉评价的侵害。

3.2. 割裂性：大数据并非全数据

大数据的技术手段虽然可以实现精准定位，极大地提高效率，但是大数据始终只是大数据，并非“全”数据。大数据预测系统的本身就存在着先天的固有错误率。不可避免地存在假阴性——错误地漏掉一个有罪个体；也无法回避假阳性——无辜的个体被怀疑有罪。大数据本身便是具有割裂性的，需要人工审查、传统小数据抽样的方式进行填补。并且，这种割裂不仅仅存在于大数据技术的自身，在数据的管理层级和制度上同样存在割裂。目前，我们尚不具有一个全国统一的大数据库，犯罪预测的算法、程序也没有进行统一，在各个地区、各个层级之间形成了严重的数据壁垒。这导致了犯罪预防信息分享渠道闭塞、犯罪预防上各部门各自为战、零散化、碎片化的缺陷[7]。

3.3. 相关性特征：歧视与偏见难题

大数据的核心在于预测，它让人们相信可以通过数据的分析和挖掘来预判人的行为。但是，它更加注重的是相关关系而非因果关系，这是大数据应用技术重效率而非精确的特性所决定的。例如，你在淘宝上买了一把菜刀。因为抢劫的人一般都携带刀具作为凶器犯罪预测软件分析得出在网络购买刀具和实施抢劫犯罪具有极强的关联性，那就会直接提高你的犯罪可能估值，并不会从因果关系来判断你买菜刀的用途是不是抢劫，普普通通的一把菜刀对于压制被害人反抗的威慑程度又有多少。这就导致了在缺少因果关系及理论基础的情况下，系统也会根据分析的结果来进行主动防控。这种简单、一刀切的相关性分析标准会加深特殊群体的歧视，例如一提到“黑人”、“农名工”、“难民”等词汇就经常和犯罪联系到了一起。而这种相关关系可以通过微信、QQ、微博等轻易提取，得出用户的人际关系、相似人群特征，直接描画出以地缘、血缘、学缘为纽带的关系人群，进一步加深了歧视与偏见的程度。从某种意

义上，这种模式甚至会固化“龙生龙，凤生凤”的偏见认识。而且在很大程度上，这种偏见的指向性并不一定是科学、客观的，而仅仅是简单的数据关联性所导致的，存在一定的局限性。

3.4. “人”的影响：弱人工智能的自我强化与自动化偏差

人工智能是基于对人类智能实质的理解而产生的，一种以智能方式对人类意识、思维、行为模拟后进行学习并能够做出反应的机器，最终达到机器能够像人类一样思考、学习、行动的目的，甚至可能产生具有超过人类智能的类人机器。但是，归根结底，目前的人工智能还是需要依靠算法模型，并且只能做出一些简单的自动化决策。我们不难发现，现阶段我们的人工智能犯罪预测技术还只是弱人工智能，其行为的起点和终点都已经被程序预设，无法通过机器的自我学习来修补隐藏算法固有的漏洞。虽然我们有神经元的信息处理模型，但是机器始终无法做到像人一样思考。这意味着我们始终需要“机器 + 人”的模式研判。可是，人们往往会迷信科学，仿佛无人因为因素介入的客观数字才是最科学的合理预测。但是，我们已经反复提及，犯罪预测系统存在着固有缺陷，谎言重复一万次就会变成真理，试问一个品德高尚的人总是和罪犯、抢劫、贪污这样的因子关联起来，你是否会对其人品产生怀疑？不幸的是，在很多时候，出于对于数据的迷恋，这种机器的错误在一遍遍的简单重复中自我强化，人类也老是陷入这一自动化陷阱之中。这在相当程度上冲击了人人平等的司法核心要义。

3.5. 数据的管理机制

之前，本文已经讨论过在信息的获取和交流上，各部门、层级之间的割裂问题[8]。但是，犯罪预测的信息在被收集和使用后如何管理？至少目前，在信息被获取后的管理制度上，也存在着相当的问题。我们并没有明确的规章制度来约束公权力、规范其信息管理行为和保密义务。举一个很普遍的例子，公安机关为了防范流窜犯、加强治安管理要求各个旅店宾馆进行身份证入住实名登记，个人认为这是十分敏感的信息。但是实际情况是，这类信息的提取查询权限被下放到了基层的派出所，刑事侦查机关这类公权力主体只要告知基层民警身份证号码就可以获取全部的入住信息。其实这是十分不合理的，尤其在我们社会主义国家和中华民族传统伦理观中，过多的和“开房”这类词条建立相关性联系不仅仅侵犯了我们的隐私，甚至会降低整个人的社会评价。而新出台的个人信息保护法对于公权力主体对于个人信息的处理、管理机制也没有进行详细的规范。这亟待具体的规章制度加以规范，在后文会做出具体论述。

3.6. 介入可行性分析：俄狄浦斯效应

目前的犯罪预测实践中，我们经常陷入一个误区“预测即干预”，而忽略了这种干预是否合理。有学者引入了“俄狄浦斯效应”来解释，人的活动结果往往与语言或者目的背道而驰。因为，我们是人，退一万步讲，即便预测系统能够做到科幻片中那样的精准不存在误差，但是我们有感情、有七情六欲、是活生生的血肉。不同于地震、海啸、天气预报，人类对自然预测是确定性的，但我们的主观随意性和非理性导致了我们的行为发展是非线性的，是充满随机性的[9]。正因如此，对于犯罪预测后的介入行为应该保持一个审慎的态度。

4. 大数据控制犯罪的运用优势——以智慧警务和反腐为例

前文我们介绍了大数据预防犯罪会产生的一系列问题，但是科技的出现与发展总是尤其原因的，大数据具有两面性，它虽然存在着相关的法律和伦理问题，但是它对预防犯罪也起到了一定的积极作用。

4.1. 智慧警务的新理念和新模式

智慧警务是“数据 + 业务”双智能驱动的新型警务发展，当前大数据背景下的智慧警务应用仍处于

发展探索阶段。智慧警务的应用已逐渐深入到犯罪侦查、犯罪预警、执法监督、民生服务等各项日常公安工作中。在数据和技术方面，智能警务以业务智能化为目标，通过洞察、挖掘警务数据规律和价值，来提升警务智能应用能力，加速实现业务驱动到数据驱动警务的转型。在业务方面，整合刑侦、反恐、禁毒、情报、科信等部门实现警种联动，进行智能情报分析、侦查行动、指挥调度、惠民服务，推动公安各项业务的信息化融合。犯罪预警作为智慧警务业务之一，将合成作战、预警布控和情报研判等业务进行一体化整合，对违法犯罪行为进行预警、预测和预防。在前文中，我们已经讨论过智慧警务在实践中对于犯罪预测的推动作用。接下来，我将进行把大数据运用到智慧警务的内部优势和外部机会的分析。

4.2. 内部优势

大数据是在各领域中搜集汇总，从而形成庞大的数据。在公安侦查工作中，公安机关可通过网络、监控、线报等多种途径提前获取有关犯罪嫌疑人的情报信息。获取信息种类也多种多样，如通话上网记录、活动轨迹，以及现在公安机关可以与各大购物、外卖平台合作，获取更多的数据信息。公安机关对潜在犯罪分子信息的获取途径更广，数据类型更多，可以更有效地对犯罪行为进行提前预警。同时，在犯罪行为发生后，在对犯罪嫌疑人进行抓捕工程中需要进行分析排查。利用对大数据分析技术从海量数据信息中逐步筛选出有用的线索，获取犯罪嫌疑人信息、逃离路线等，为迅速有效侦破案件提供可靠的情报。本文的重点主要在于前者对于犯罪预测的讨论，公安机关通过建立数据分析库，对犯罪分子信息、被害人信息等进行收集存储，并对再犯罪可能性较大的前科人员进行重点监控，通过对对方的手机、账户、资金来源动向等进行合法监控。同时，大数据的应用为公安机关打击高发的电信网络诈骗犯罪提供了有力的技术支持。反电话诈骗系统和伪基站实时监测系统的研发为公安机关对此类案件的防范预警能力，同时对潜在受害人进行劝阻工作，或根据大数据分析得出的重点受害群体和区域中进行宣传教育工作，在源头上减少此类犯罪的发生。最后，在传统的公安工作模式中，公安民警在警情发生后需要手动查阅警情发生地的监控和摄像头，从而追踪目标轨迹，往往依靠个人的分析和经验判断。大数据在公安工作中的普及和应用大大提高了侦查办案的效率，节省了人力和物力。

4.3. 外部机会

大数据时代是通过分析与某事物相关的所有数据，来获得有价值的信息。在我国公安信息化发展进程中，犯罪热点分析、预警模型等技术已广泛应用于警务工作中。我国已建立警用地理信息系统，也在外与大数据公司合作开发大数据犯罪模型的同时，不断举办公安建模大赛，鼓励在职民警借助大数据和人工智能技术实现对犯罪打击和预防。

大数据是警用机器人等技术的未来发展方向。以警用无人机为例，无人机可以对犯罪嫌疑人及其手机进行精确定位和监控，对情报信息实时进行分析研判，公安机关可以结合警用地理信息系统制定抓捕方案。无人机通过大数据对人物图像精准采集和监测，并将这些非结构化数据转化为结构化数据，与数据挖掘技术的有机结合，揭示犯罪活动及犯罪嫌疑人的内在规律和趋势，从而达到预测犯罪的目标。

智慧警务与人工智能的结合正在不断地消除传统警务模式的弊端，重构警务组织框架，重组警务工作模式，在以海量数据和多边算法为特征的数字社会基础上，人工智能技术凭借其智性与算法在驱动警务决策、警务组织、警务技术、警务服务及警务监管变革的同时，也为建设数字中国 and 平安中国提供了强大的技术支撑和智慧支持。总之，面向人工智能时代的智慧警务是云端警务、网状警务、智能警务和协同警务。

4.4. 智能警务的运用实践——以贪污贿赂犯罪预测为例

接下来，本文将通过贪污受贿型犯罪的实例，具体阐述犯罪预测在该类案件中的作用。犯罪大数据

通过对犯罪主体特征进行“大数据画像”，提高腐败惩治精准性、腐败预防科学性和腐败问题研究客观性。通过监察机关公开的贪污犯罪腐败起诉书，利用大数据对文本的非结构性数字进行多维度分析，重点研究贪污贿赂罪犯罪主体的年龄、学历、职务等因素及其与犯罪类型、犯罪金额、犯罪潜伏期等的关系，通过统计数据揭露当前腐败现象的部分规律性特征。一部分学者认为，贪污腐败的年纪呈现两极分化的趋势，一方面，“59现象”在20世纪末，21世纪初是一个热词，主要是指个别领导在退休之际，受到“有权不用、过期作废”和退休之后高枕无忧等想法的影响，在退休前贪污腐化。另一方面，腐败低龄化也越来越严重。但是经过大数据的对比分析发现，事实却并非如此。通过将犯罪年纪和金额做相关性分析，可以得知，初犯年龄与贪污金额呈现显著的负相关，初犯金额与贿赂金额呈正相关，但是初犯年龄与挪用公款却不存在相关关系[10]。通过大数据将学历与贪污腐败罪做相关性分析，可以得知学历与犯罪罪名呈显著相关关系，受贿罪中，高等学历占比百分之八十六，在贪污罪中，受过高等教育的占比百分之四十五，在挪用公款罪中，受过高等教育的占比百分之七十一，由此可见，受过高等教育的被告人更偏向于受贿的方式，未受过高等教育的被告人更偏向于贪污。而且学历与犯罪次数也有明显的相关关系，学历高的往往犯罪次数更多。但是被告人的学历与犯罪人数却呈现明显的负相关，学历高者倾向于独自犯罪，学历低者倾向于共同犯罪。这些大数据犯罪预测的研究成果完成了贪污受贿类犯罪的“数据画像”，对于反腐具有重要的理论价值[11]。

贪污是人类社会的顽疾，腐败治理更是一项系统性工程，在新的起点上，研究贪污腐败“数据画像”具有更加重要的政治价值、法律价值、社会价值和时代意义。尤其在党的十九大以后，领导干部更是实现中华民族伟大复兴过程中的“关键少数”。通过贪污腐败犯罪的大数据画像分析，有利于进一步提升新时代腐败惩治的精准化。犯罪现状的测量评估和研判，是“宽严相济”的刑事立法政策、刑事司法政策、刑事执行政策订立的犯罪学基础，也是明确监察调查、刑事侦查的重点领域和优先方向的事实依据。在信息时代，对贪污贿赂犯罪已办结案件的大样本、甚至全样本分析，可以辅助纪检监察机关、司法机关将有限的人力、物力、财力资源集中到腐败的多发高发领域，防止腐败的蔓延和扩散。贪污贿赂犯罪的大数据分析画像分析也有利于进一步提升新时代预防腐败的科学性与对腐败贪污研究的客观性。

5. 发展前景

5.1. 保持谦抑性

按照目前美国的治安实践，犯罪预测已经具有了提前介入、逮捕的趋势。但是，众所周知，刑法是不处罚除了故意杀人、恐怖犯罪等特定犯罪之外的预备犯的，更不用说是处罚一种犯罪的思想和趋势。如果仅仅依据犯罪预测系统的结果过度介入，会造成侦查权的过度扩张，以及导致刑法的延伸和去边界化，这会最终导致自由和权利保障的解除后果[12]。而且，我们前面也已经讨论过这种介入本身是否合理都尚且存疑。因此，笔者愚以为，尤其在刑法领域，涉及公民自由权利和国家公权力的重要博弈，我们先谨慎地暂缓打击犯罪的效率追求，等大数据相关立法在商业、民事领域趋于成熟之后再展开后续的介入，保持刑事司法的谦抑性。例如，可以针对类案而非具体到个案进行预测、进行犯罪热点地区预控而非针对个人采取措施、即便是对于刑释人员，也可以将预测重点放在“犯罪人关注和改善”上而非“犯罪人预测”，避免“天生犯罪人理论”、“相面学”这类品格犯的缺陷理论乘势而上。

5.2. 统一的预测机构与制度：企业平台与公权力机关

前文多次提及，目前的犯罪预测实践中，急需出台统一的数据管理机构和制度。虽然，随着《个人信息保护法》的出台，公民的个人信息得到了较为充分的保护，但是在本文犯罪预测的语境下，依然存在许多的制度空白值得探讨。下面，本部分将展开对于之前问题的集中探讨。

1) **侦察机关的合法性基础不明确。**虽然《个人信息保护法》通过第 13 条的相关规定,在《网络安全法》的合法性基础上进行的扩充,并延续了《民法典》“同意的例外”思路,增加了订立或履行合同所必须、保护自然人的重大利益以及公共利益等情形。但是,如果把犯罪预测的数据采集行为进行具体归类,却会发现非常得困难。其中,最合适的合法性基础唯有第三款的“为履行法定职责或者法定义务所必需”和第四款的“为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需”。如此,对于第三款,我们就不得不将预防犯罪解释为全体公民的“法定”职责和义务,这其实和前文所述的谦抑性不符,对于公众的道德要求过高;对于第四款,大数据信息的攫取更是只能针对“事后型”的犯罪侦察、罪犯逮捕等“紧急情况”,并不涵盖事前型的犯罪预测。因此,除了对三、四款做出扩大解释(甚至是类推解释)以外,在犯罪预测的语境下,公权力的合法性基础只能引用第七款的兜底性条款。

2) **公权力机关的信息处理者义务。**根据《个人信息保护法》第 51 条的规定,个人信息处理者应当个人信息的处理目的、方式、信息种类,通过制定内部管理制度和操作规程、个人信息实行分类管理等措施,履行个人信息的安全保障义务。但是,这类规定还是较为笼统,没有做出具体性要求,最后还是要回归到公权力机关自身的内部规章制度,这无疑有监守自盗、与虎谋皮之嫌。就比如前文所提及的开房记录查询问题,经过本人向几名老律师的询问,在实践中依然可以通过公安系统的熟人查取到相关信息,只要注意不要留下书面、电子纪录即可(多通过电话语音告知)。由此可见,指望信息处理者自己给自己增设义务是行不通的,这亟待法律做出统一性的规范。

3) **企业平台提供个人信息的合法性。**《个人信息保护法》第 58 条将 QQ、微信、淘宝等企业平台定义为“重要互联网平台服务”,对其进行了更进一步的制度规范,而上述企业平台的信息又正是犯罪预测中重要的信息来源。其实,企业平台提供个人信息是具有相当的合法性基础的,除了前文所述的对《个人信息保护法》第 13 条三、四款进行扩大解释以外,第 26 条“所收集的图像、身份识别信息只能用于维护公共安全的目的”也赋予了其一定的合法性基础。并且,从行政法的角度考虑,在犯罪预测的过程中,企业平台受公权力侦察机关的指令提供信息的行为,本质上是行政行为的辅助者,该问题还是要回归到前文的侦察机关合法性基础项下进行讨论。然而,即便企业平台提供个人信息的行为具备一定的合法性,但是在一些具体问题上的操作依然存在探讨的空间。例如,企业对于向侦察机关这类“第三方”提供其处理的个人信息是否需要满足第 23 条所规定的取得个人的“单独同意”,企业平台是否需要履行第 55、56 条规定的“个人信息保护影响评估义务”以及第 57 条规定的“安全事件通知义务”,这些问题法律尚没有做出具体的规定。

5.3. 比例原则

大数据犯罪预测无疑是人类的一项智慧发明,它可以辅助公安机关更高效率的打击犯罪甚至是预防犯罪,可是大数据对犯罪行为的预测,会在一定程度上侵害受监视人的隐私和利益,所以大数据对犯罪预测的应用应该遵循一定的比例原则,这与《个人信息保护法》第六条的“目的明确和最小必要原则”的要求也是不谋而合的[13]。笔者以为,比例原则在犯罪预测项下主要反映为信息攫取对象的适当性、必要性。对于普通公民的犯罪行为监视与分析应该在一定的范围内进行,不能打着预测犯罪的名号去提取老百姓生活中的各种数据,比如在哪家超市买了什么,做哪一站公交车到了哪里等等,在无事发生的情况下,对于公民正常生活的监控就属于过度预防,不但会增加分析成本,还会侵犯人们的隐私权,打乱老百姓本来的正常生活秩序,对他们造成本不必要的负面影响。因此,我们需要将预防的对象进行合理限缩,例如只能针对刑满释放人员[14]和官员才能采取预测分析手段。针对刑满释放人员的合法性在于其先前的犯罪行为导致了其接受社会矫正的义务,是其自身行为导致其危险性系数提高的合理预控方法[15];针对

官员在于其作为领导干部这一“关键少数”的政治性、社团性质的附加义务，对其进行数据采集和预控来源于其自身权利的让渡。简而言之，两者都可以解释为取得了授权的“单独同意”。笔者认为，大数据犯罪预测的对象应该合理地限制在该类有限群体之中。

6. 总结

总之，大数据在预测犯罪方面其实是一把双刃剑。它在预防犯罪方面起到了突破性的作用：可以刻画犯罪行为主体的特征，甚至是研判下一次的犯罪信息，能够使得公安机关提前掌握相关的信息以及犯罪因子的存在，并提前介入，减少犯罪的产生并节约司法成本。从智慧警务、社会治安的角度，大数据犯罪预测具有极其重大的意义。

但是，大数据犯罪预测也具有一定的局限性：大数据毕竟是冷冰冰的数据，算法再厉害也不可能完全取代人的智慧与灵活性。在目前的实践中也存在着割裂性、歧视性、自动化偏差和数据管理机制缺失等一系列问题。如果一味地将大数据运用于社会，就会产生一系列的伦理问题，人类社会是非常神奇的，它奇妙于算法和硅片并不能完全预测人类的走向。文艺复兴时期，人类举起了人文主义的大旗，第一次战胜了神。而现在，我们使用大数据技术进行犯罪预测的目的并非给人类再造一个新的神。从刑法的谦抑性角度，本文还是持审慎试用的态度。

笔者认为，尤其是当下正尚处于弱人工智能技术条件，目前阶段需要我们主动、积极作为地优化算法，建立完善、统一的法律机制，在侦测对象上采取比例原则(严格限缩为刑释人员、领导干部等有限群体)；在侦测类型上加强地区、案件种类的整体防控，审慎适用具体人员的犯罪预测分析。

参考文献

- [1] 张威. 大数据时代犯罪防控困境及出路探讨[J]. 铁道警察学院, 2018, 28(1): 52-57.
- [2] 章光明, 黄王志. 大数据在犯罪侦查中的应用[J]. 上海公安高等专科学校学报, 2016(1): 84-89.
- [3] 李春笛, 靳高风. 犯罪预防学[M]. 北京: 中国人民公安大学出版社, 2016: 8.
- [4] 张蓓蓓. 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.
- [5] 松尾丰, 盐野诚. 大智能时代: 智能科技如何改变人类的经济, 社会与生活[M]. 北京: 机械工业出版社, 2016.
- [6] 何祺. 预测警务在我国公安工作中的应用研究[D]: [硕士学位论文]. 北京: 中国人民公安大学, 2019.
- [7] 胡向阳, 丁寒. 人工智能犯罪预测[J]. 中国刑警学院学报, 2020(6): 5-11.
- [8] 王彬. 犯罪侦查中的大数据应用分析[J]. 中国刑警学院学报, 2017(4): 31-37.
- [9] 阎耀军. 社会预测学基本原理[M]. 北京: 社会科学文献出版社, 2005: 320-336.
- [10] 赵晨光. 腐败与年龄无关[J]. 人民检察, 2002(6): 52-53.
- [11] 金鸿浩, 李凌, 刘思敏. 我国贪污贿赂犯罪主体特征的“大数据画像”研究——基于 8133 份公开起诉书的大数据分析[J]. 犯罪研究, 2020(1): 2-15.
- [12] 孙煜华. 侦查权的宪法控制[M]. 北京: 法律出版社, 2014: 3.
- [13] 理查德·A·斯皮内洛. 世纪道德: 信息技术的伦理方面[M]. 刘钢, 译. 北京: 中央编译出版社, 1999: 53.
- [14] 叶良芳, 张勤. 大数据时代网络恐怖主义犯罪的防治: 大数据时代下的犯罪防控[C]//中国犯罪学学会年会论文集(2017年). 北京: 中国检察出版社, 2017: 480-481.
- [15] 马国富, 王子贤, 马胜利. 基于大数据的服刑人员危险性预测[J]. 河北大学学报(自然科学版), 2016, 36(6): 657-666.