

算法取证的司法应用程序风险及规制探讨*

何元迦¹ 何邦武²

(1. 南京大学法学院, 江苏 南京 210093;

2. 南京航空航天大学人文与社会科学学院, 江苏 南京 211106)

[摘要]以大数据为基础的算法在数字时代侦查取证中的广泛使用已是不争的事实。算法取证的基础是大数据和云计算,其基本原理是用数学的方法研究逻辑推理和数学计算,将推理论证、数学计算的过程演化为符号化、形式化、公理化的知识,这种植根于数理逻辑的知识因此具有符号性、形式性和公理性。算法在将人变为可计算、可预测、可控制的“客体”的同时,也带来新的权力形态,出现“算法即权力”的现象而反噬人类自身。较之传统物理空间的侦查取证方法,算法取证具有隐蔽性、广泛的侵入性等特点。由于算法取证的启动缺乏明确的法律规定与授权、取证过程不透明,因而违背了程序法定原则,使既有的程序正义的理念及其制度受到挑战,产生制度短缺效应。此外,因社会性的数字平台行为的公权力化现象,个人信息权利受到侵害,传统的正当程序原则和无罪推定原则受到冲击。应当坚守刑事程序正义的首位价值,在对算法技术理性的祛魅中驯服算法,实现算法取证技术的程序正当;完善数字取证制度的立法,确保算法取证相关算法技术的公开透明,并通过算法备案确立算法问责点,规范具体的算法取证程序;立足中国证据种类法定化的制度语境,完善证据种类的立法,将算法证据纳入法定的证据种类,以此规制此类证据。

[关键词]大数据 算法取证 算法证据 程序正义 算法正义

[中图分类号]D901; D918 **[文献标识码]**A **[文章编号]**2096-983X (2026) 04-0150-11

算法取证,即运用以算法为基础的大数据模型进行的一系列大数据收集、处理活动以取得电子数据的行为,涉及算法取证行为的主体、算法取证所涉数字技术以及取证的程序规则等。与传统物理空间刑事侦查的取证方式不同,在网络虚拟空间利用大数据和算法进行侦查取证中,其取证主体及取证程序均表现出一定的数字技术特征,甚至因为人工智能的接入,而汇入了人工智能法律主体资格问题争论

的声浪中。本文拟就算法取证的程序问题及其所涉数字技术原理进行分析。

既有大数据和算法侦查即数字侦查的研究,其重心在于此类侦查行为性质的界定以及该行为的法律规制等,目的是如何规范和约束数字侦查行为中的公权力,保障相对人的数字权利,实现侦查程序的法治化。^[1-2]本文重在关注数字侦查中的证据收集问题,可视为数字侦查行为的结果,亦可视为数字侦查行为的

收稿日期:2025-07-02; 修回日期:2025-11-19

*基金项目:海南省哲学社会科学规划课题“电信网络犯罪司法证明模式研究”(HNSK(ZC)24-219)

作者简介:何元迦,博士研究生,主要从事刑事诉讼法学、证据法学研究;何邦武,教授,主要从事刑事诉讼法学、证据法学研究。

具体展开。在研究内容上关注如何按照证据资格的要求规范取证的程序,属于数字侦查行为研究对象中的一部分,因而与数字侦查行为的研究有隶属关系。与算法取证邻近的概念还有算法证据(又叫大数据证据等等,名称不一而足),二者之间存在因果关系,即因为算法取证而有了算法证据。此外,后者与算法取证一样,尚未见于既有的刑事诉讼法律制度中,尽管算法证据在实践中已经广泛使用,且不乏与之相关的学理探究。^[3-5]司法实践中,为救制度空缺之急,一般依照电子数据的证据资格审查采纳,对该证据的特有属性未作出规范。

国内外关于算法问题的研究成果十分丰富,并且随着算法技术的更新而使整体知识呈加速累积的趋势,涉及算法的技术原理、算法的规制以及诸如ChatGPT等人工智能的应用等诸多领域,颇多学术建树。然而,尽管研究者对“算法的泛在性”及其规制的必要性等存在共识,但由于一些研究者对于算法技术理性的迷思,放大了算法的“智能性”,甚至昧于算法作为信息处理机制的认知,以致存在算法万能的执念,无法实现从科学技术到法律规制的超越。有关人工智能司法的研究中异说纷呈的现象,足以说明在算法基本原理的认知中所存在的分歧乃至认知中存在的误区。^[6-8]因此,本文将在分析算法取证对既有刑事程序和证据规制带来新挑战基础上,厘清大数据和算法的性质和技术原理,进一步探究如何从技术标准到法律规则,规范算法取证程序的路径。

一、算法取证对既有程序与证据规则的挑战

算法在数字时代的泛在性使整个社会进入一个算法统治的时代,算法的“权力”深度介入经济社会生活的各个领域、各个层次,我们

因此成为“物联网”时代的“量化自我”或“可测度自我”。^{[9](P61)}数字技术带来了新的权力形态,导致了“算法即权力”的新现象,同时也使传统上用来制衡国家权力的公民权利面临更隐蔽、更无所不在、更多元化的权力技术的侵蚀^[10],以致传统法律意义上的法律主体蜕变为“没有面庞的权利主体”,出现“人”的真正危机^{[11](P311)}。一言以蔽之,数据时代成为一个“算法”统治的世界,算法已蜕变为权力。即使主张算法公开,仍然面临着因算法技术无法公开或者公开无意义、算法歧视,以及用户算计与侵犯知识产权、个人数据赋权面临个体难以行使数据权利、过度个人数据赋权导致大数据与算法难以有效运转等诸多难题^[12-14],算法权力因此高度异化。算法取证也对既有的取证程序理念产生异化,并对既有刑事程序与证据规则构成全方位的挑战。

(一) 算法不透明、算法黑箱等对程序法定、程序公开原则及其理念的挑战

程序法定和程序公开原则及其理念的实质,就是要求所有涉及公权力的行为必须于法有据,受到法律的约束,是公开和明确的,以保护相对人的基本权利,打破“刑不可知,则威不可测”的魔咒,实现程序公平和公正,使刑事程序符合法治的精神。同时,必须在法律上明确相应的规则以及此类规则的刚性和正当性,对公民的人身、自由、财产、信息权益等的限制,还应遵守法律保留原则,不得将此类规定设置在作为刑事诉讼的基本法律即刑事诉讼法之外。^①然而,在算法取证中,算法不透明、算法黑箱是算法使用中的常见问题,这一问题还因算法的技术保护等原因而很难找到均衡的解决方案,技术的广泛使用和刑事调查中对数字取证的日益依赖,助长了算法取证的不法行为。

首先是算法取证的启动没有明确的法律规定和授权,启动时间、对象等均不明确,有违程

^①笔者坚持认为,刑事诉讼中程序法定的“法”必须包含以下两方面的意思,一是必须是基本的法律或者最低限度有基本法的授权,而不能是低于基本法立法层级的规则或者某一司法部门自己拟定的规则;二是由于正当程序与程序法定的一体性价值选择,此“法”应为良法。这些应当是不言自明的常识,不能以任何理由回避拒绝。

序法定原则。算法取证是利用数字技术对海量数据进行采集、储存、清洗、分析、比对等,其核心技术是数据挖掘,即通过特定的计算机算法对大量的数据进行自动分析,从而揭示数据之间隐藏的关系、模式和趋势等。^{[15](P98)}例如,某犯罪嫌疑人涉嫌非法制造枪支的犯罪,其犯罪手法是利用网络购买各类枪支配件进行组装。为逃避刑事侦查,嫌疑人采用反侦查手段,同时在网上注册了几个账号用于交易,并将收货地点写成几个地方。但网络平台通过对海量数据进行清洗、检索和逐层筛选,终于将购买主体,收货主体等锁定为嫌疑人一人。网络平台将犯罪线索提交给公安部门后,后者在嫌疑人住所找到了组装的枪支,其中各类配件与网络上交易的配件一一对应。在平台上述系列证据收集分析过程中,并未确定地启动取证的时间节点,而是在对海量数据进行收集、共享、清洗、碰撞、对比和挖掘后发现犯罪线索、证据信息或者犯罪嫌疑人。上述行为并无明确的取证对象,甚至平台进行这一数据分析行为本身也未有来自警方的授权。以传统的侦查取证规则衡量,显然缺乏合法性和合理性。

在中国的刑事侦查制度语境中,算法取证还面临着由于启动的时间节点前移而逃逸于立案程序规制的问题。^①尽管可以将算法取证比拟于初查,但与传统初查行为的任意性不同,算法取证行为是基于数据库分析进行的,期间对个人信息甚至敏感信息的广泛介入显然远远超过传统任意侦查手段。无可否认,使用数字侦查手段使中国针对恐怖主义、危害国家安全等特定领域犯罪的侦查手段向普通犯罪侦查蔓延,无疑使程序的正当性受到质疑。^[16]

其次是算法取证的过程缺乏透明度,甚至基于技术保密的考量而必须要求该过程不透明,与程序公开原则存在冲突。英国国家警察局长理事会指出,如今90%的刑事调查都有数字元素,并将标准化和自动化确定为数字取证

进一步发展的核心原则。^[17]

这种泛数字技术使用的结果,必然产生以下两方面的效应。一方面,与上述取证难以符合程序法定从而碍难实现取证的合法性与合理性相一致,算法取证过程还与程序正义所要求的程序公开原则相悖。由于平台在使用算法模型进行数据挖掘和数据处理时,会涉及平台自身技术开发而拥有且需要保护的技术专利,同时出于预防犯罪嫌疑人采用反侦查技术手段的考虑,平台在算法取证中所采用的数据处理技术将处于保密状态。尤其是上述算法会随着网络大数据的指数级增长及算法技术的发展而不断创新,其纯技术性面目更难以为专业技术人员以外的人员所掌握,因此,算法取证的内在要求决定其具有不透明的属性。另一方面,基于保护个人隐私等个人信息权益的考量,当前的算法取证中,还出现了隐私计算的取证方式。这种出于保护隐私等个人数据信息权益的隐私计算,在一套包含符号化、公式化以及量化评价等技术标准中,加剧了算法的不透明,颠覆了刑事诉讼固有的程序公开原则及理念。总之,由于保密需要或者算法本身的技术性难以为外人知晓等原因,算法取证的程序运作某种程度上使程序正义从看得见的正义转而成为看不见的正义,解构了程序正义的应然价值内涵。

(二) 算法对既有侦查程序价值目标的冲击

总体而言,在数字时代,数据、网络等的安全价值直接关系到国家的生存与发展等一系列重大战略,因之冲击着传统物理空间的法律价值位阶,法的正义价值在数字法领域一定程度上受到限缩。这是因为,算法取证除了传统的作为公权力主体的侦查机关的正常履职外,还需要社会数字平台的配合,出现所谓平台行为的公权力化现象。其结果,因数字时代普遍存在的监视主义,极易导致公权力的越位乃至外溢,以致更加容易对相对人的个人信息权利造成侵害。这一现象还因前文所述的算法黑箱、

^①中国目前的立案标准是“有犯罪事实需要追究法律责任”,数字侦查因没有明确的主体、犯罪事实等而无法符合这一标准的要求。尽管取消立案程序的呼声一直存在,但在没有取消这一程序之前,数字侦查与既有制度的冲突将一直存在。

算法滥用等造成的有意识或者无意识的侵害,对相对人的权利产生叠加影响的效应。面对网络犯罪日益严峻的态势,必须容忍在惩治犯罪时对相关数据的处理和使用,这触及相对人个人信息权利的保护。易言之,如果说在传统物理空间的侦查取证程序中,其程序价值的首要目标是通过限制国家公权力、保障相对人的权利而实现程序的正义,突出在取证中的人权保障价值,那么在算法取证中则表现为一种算法的正义,即一种技术性正当程序。^[18]

一般意义上的算法正义,即如何确保算法的公平使用,以及在算法运行过程中如何减少乃至杜绝对特定群体的歧视而导致算法结果的不公正,涉及算法设计和开发过程中的偏见如何消除,以及算法如何进行更公正的决策等。而在算法取证中所涉的算法正义,则关涉相对人的隐私、数字权利保护以及算法取证程序自身的公正无偏见,等等。所有这些算法正义,都以代码的形式呈现出来而使程序代码化,以致有研究者认为这种程序等于算法加数据结构。传统公权力因此披上数字权力的外衣,在改善传统物理空间公权力装扮的同时,也使公权力戴上数字的面具。

其二,算法取证对个人权利深度干涉的结果是传统的正当程序原则和无罪推定原则均受到前所未有的挑战。由于自动性算法具有广泛的侵入性,不仅使服务于刑事诉讼的数据收集、存留及共享义务得到扩张,而且在风险防控思维下,犯罪治理活动启动时点也提前,以致突破了传统侦查取证的被动性、回应性。数字信息技术的高度发展使信息的获取、传递和交流更加便捷,以致任何人及其活动所形成的信息都很容易被追踪、记录,社会结构的“粒度”更加精细化,数据在被高度解析后,所有人均无隐私可言。这种大规模监控的结果是使取证程序中的人权保障受到一定程度的限缩。^[16]实践中,因算法取证对“潜在证据”的广泛访问和收集,相对人甚至一般公众的个人信息都会成为这种“潜在证据”。

就无罪推定原则而言,在数字领域,无罪推定原则还可以被解释为在程序上减少并尽量减轻数字取证的偏见、不确定性和错误的影响。由于数字证据在实质上是人机交互的结果,通过算法取证似乎能在一定程度上减少人为错误。并且,法官们“似乎急于接受技术进步的产物”^[19],并经常假设数字媒体来源的证据运作正常。然而过度依赖自动化工具获取和分析证据可能导致一种误解,即技术可以减少错误和偏见,算法工具获取的结果更加可靠。实际上,这种技术保护谬误并未考虑到数字侦查中的大量错误、偏见和不确定性,而这些因素恰恰可能对无罪推定和公正审判产生不利影响。^[20]例如,尽管刑法和算法语言从结果导向的角度存在一定的相似性。刑法规制的范围虽然非常广,但作为一部法律,它为是否犯罪提供二分式(0或1)的答案,以保障公民的基本权利并作为公权力的谦抑性规范。如果用计算机语言去表达刑法规则的适用框架,就会出现以下情况:如果“相关法律规定”能够与“案件客观事实”相匹配,并且排除了所有的不确定性,那么系统就会输出根据抽象的规则定罪量刑的结果。然而,用0/1的二分法解决算法取证存在的问题是,法律、工具和程序如何在解释数字人工制品时处理这种不确定性。因为,“基于数字产品的结论得出的相关证据是不完整的,它来自我们的猜测和观察,所以这些证据由于各种原因都不是完全可信的”^{[21](P13)},从这些证据得出的推论本质上只能是概率性的。因此,仅仅是统计证据的概率“无论在数字上有多高,都不能为刑事定罪提供充分的基础”,如果缺少必要的证据,或者它不“容易受到最大限度的个性化检验”,或者“检验破坏了它的可信度”,就会使被告面临被错误甚至非法定罪的风险。需要注意的是,无罪推定并不等于某人是无辜的或某人可能有罪,在制定数据保留规则后或允许用新算法技术破案,可以考虑对案件进行这种概率分析。但是,如果国家不能在审判前或审判期间为证据制定适当的测

试标准,可能会导致个人隐私的侵犯或违反公平原则。此外,由于数字侦查远离现实世界,仅仅依赖于泛化而非个性化、基于潜在线索的调查——如果在调查的早期阶段不加强对潜在证据和潜在证据来源的无罪推定,可能会获得完全不准确的、随机的结果。

此外,由于数字侦查的技术性规则尚不明晰,很难判断其使用过程中的相关技术是否与无罪推定原则有关。一方面,合理怀疑的概念既不够充分也不够精确,很难满足取证数据分析的需要。由于比例原则和平衡测试在实践中的使用含糊不清,甚至完全有可能在审查数字取证过程时变得不切实际。因此,在缺乏相关法律法规的情况下,对复杂的算法取证技术的评估越过了司法人员甚至专业领域的专家,难以符合无罪推定和法治原则。另一方面,任何用于执法目的的新型数字取证技术都必须从其设计到应用的准确性、侵入性和PI合规性进行仔细审查,这需要从“通用工具”过渡到“侦查时使用的数字取证方法”,并且在审查中需要考虑到在调查中使用的技术是否存在侵犯个人隐私的可能。^[17]

总之,作为有科技手段辅助的侦查活动,如果没有立法的干预及相关规则的规范,那么数字侦查活动就是对无罪推定原则的威胁,并可能对案件结果造成消极影响。这种数据驱动的“有罪推定”对公平性必然产生不利影响,还因为它没有将嫌疑人定位为取证过程中的一方,而是要求嫌疑人证明自己的清白,导致事实上的举证责任倒置。嫌疑人也更难提供解释、交叉询问或收集反证,因为证据是在任何刑事诉讼开始之前“准备好”的。^[17]置身于中国的刑事司法语境,这将直接解构正在推进的审判中心主义改革。

(三) 算法取证规则缺位所产生的制度短缺效应

作为一种新生的取证方法,中国现行的刑

事诉讼和证据规则对算法取证尚无明确的规则可以援引适用。在既有的中国制度系统中,与算法取证较为接近的有现行《刑事诉讼法》中规定的搜查与技术侦查,以及公安部《公安机关办理刑事案件程序规定》中规定的调取等三种侦查取证方式。但笔者认为,比照算法取证必须满足的大数据和算法两大核心要素,上述三种侦查方式的规则均仅指向传统物理空间犯罪侦查行为,均有明确的搜查、侦查和调取对象,难以作为大数据侦查的规范依据。^①当前,仅有《个人信息保护法》第34条作了原则性规定,即为了履行法定职责而处理个人信息的国家机关,“应当依照法律、行政法规规定的权限、程序进行,不得超出履行法定职责所必需的范围和限度”,其内容极为模糊,无法为算法取证提供明确的可操作性规则。

在刑事诉讼法有关证据种类的规定中,虽然勉强可以通过解释将算法取得的证据纳入电子数据中,但终究不是法定证据的一种,因此也无相关基于算法证据特有属性的证据资格的规定。应当是相关部门已经认识到当前的制度体系难以适应算法取证的需要,因此,公安部在《公安机关执法细则(2024年第四版)》(以下简称《执法细则》)中将“查询、检索、比对数据”单列为一种侦查措施,规定进行下列侦查活动时,应当利用有关信息数据库查询、检索、比对有关数据:1) 核查犯罪嫌疑人身份的;2) 核查犯罪嫌疑人前科信息的;3) 查找无名尸体、失踪人员的;4) 查找犯罪、犯罪嫌疑人线索的;5) 查找被盗抢的机动车、枪支、违禁品以及其他物品的;6) 分析案情和犯罪规律,串并案件,确定下步侦查方向的。然而,从上述规定中很难合逻辑地作出使用算法的扩张解释。《公安机关电子数据取证规则》也无算法取证的规定,只在该规定第3条关于电子数据取证中作了“不限于”规定方式的概括性

^①具体可参见公安部2019年颁布实施的《公安机关办理刑事案件电子数据取证规则》(以下简称《公安机关电子数据取证规则》)第7条;另外,有关现行刑事诉讼和证据制度中缺乏算法取证制度元素的详尽分析,可参见程雷:《大数据侦查的法律控制》,载《中国社会科学》2018年第11期,第166-168页。

授权,即电子数据取证包括但不限于:(1)收集、提取电子数据;(2)电子数据检查和侦查实验;(3)电子数据检验与鉴定。但从该规定的原义解析,该规定有关电子数据取证实际上均指向既存的数据信息,似乎难以将经过算法形成的算法证据纳入其中。即使2016年最高人民法院、最高人民检察院和公安部(以下简称“两高一部”)《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第1条以“概括+列举+排除”方式所列明的电子数据,也难以将算法证据列入其中。正是由于这种制度设置的真空状态,才使有关算法证据的地位、性质及在司法实践中的规范路径呈现诸家异说的态势,成为一大实践难题。

二、算法取证的技术原理及困境

算法取证正在重塑证据生成与审查的逻辑结构,对传统程序正当性和证据规则带来了深层冲击。其原因不仅在于规则的迟滞,更在于算法本身原理的复杂与封闭。因此,澄清算法的技术原理与逻辑基础并正确界定人机关系,分析算法取证造成挑战的原因,并在此基础上完善对算法的规制,已成为规制算法取证的首要和基础性问题。

(一) 算法的计算原理

事实上,人类的社会生活与交往自其初民时代开始,就是一种数字化管理并不断完善的过程,因此,人类对于算法并不陌生,本文所讨论的算法即为数字3.0时代的智能算法。^{[22](P259)}就其表现形态及实际功能而言,算法作为一种泛存的计算机技术,包括边缘计算、雾计算和云算三种。其中,云计算是算法的基础,边缘计算与雾计算均以云计算为中心,是计算方式的分工,但并非算法的主流。

云计算又称网格计算,是一种分布式计算。它将大数据程序分割成小任务,经由云网络由服务器系统处理分析后整合输出,可快速处理海量数据。依靠计算机网络形成强大计算能

力,能存储、配置资源并按需提供个性化服务。通过资源共享和自动化管理,只需少量人员参与即可快速提供资源,使计算能力像水电煤气一样作为商品在互联网上流通,价格低廉。

(二) 算法的逻辑基础

算法的表现形式是计算机语言的运用。所谓计算机语言,其实是一种以人类语言为参照物的隐喻,由编码、语汇和语法组成,即按照规定的语法规则,使用数字、字符来编写程序,使得计算机能够按照指令完成各种工作的形式化语言。在不同的程序设计模型中,字符和语法规则构成的语句按照不同的指令执行操作,其运行流程是:接收输入,匹配对象,输出回答。例如,计算机首先接收人类输入的指令,并对此指令进行转换翻译,应用程序源代码由相应语言的解释器翻译成目标代码机器的语言,再进行编译操作,将程序源代码翻译成目标代码的机器语言。这一过程大致如图1所示。

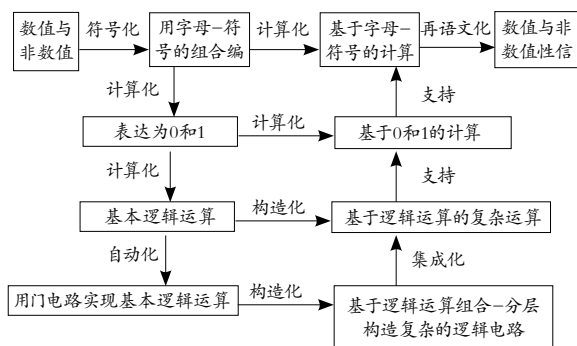


图1 算法的运行逻辑图

显然,算法的基础是在计算机系统中运用的数理逻辑,一种用数学的方法研究逻辑推理和数学计算,将推理论证、数学计算的过程符号化、形式化、公理化的知识。在计算机科学中,数理逻辑被广泛应用于编程语言的设计、算法的证明、计算机系统的验证等应用领域。以强大的算力为基础,计算机的自主学习能力也在不断增强,从而推动了人工智能从弱人工智能向强人工智能不断地“智能化”,以致有观点认为未来人工智能将会替代人脑,成为新型的数字人主体,并由此引发学术争议。笔者认

为,经过多年的发展,人工智能已经取得了长足的进步,演绎为三个不同但又相互联系的学派:符号主义学派、连接主义学派和行为主义学派。这三个学派主张及其理据虽各有不同,此处不再赘述,但就其共性而言,算法、算力和数据仍然是三者共同依存的核心要素。无论何种层级何种理论基础的算法,其基本计算主义的思维,系以数理逻辑为始基,而最终的路径仍然依赖0、1二进制的计算方法。

(三) 算法的“人为”本质

算法取证之所以冲击既有程序与规则,根源在于其以技术理性取代了人之主体理性,算法的运行逻辑与生成机制恰好揭示了在看似客观中立的技术形态中潜藏着人的意志与偏向。换言之,算法黑箱并非纯粹的技术黑箱,而是一种被人为设计、选择并维持的认知遮蔽。

其一,算法相关数据来源及收集方式由人操控。数据收集行为本身蕴含着人脑对特定事物的价值判断,而收集对象与收集方法同时反映着收集主体对某个既定目标的预设。首先,算法的数据来源从网上发布的公开各类数据,到网络用户使用某平台服务时自愿向平台提供而留下的数据,再到模型设计师训练模型时向其投喂的资料库数据,这些数据诞生的背后都是人。算法选择从哪里收集数据、用什么方式收集数据、抓取哪些数据,以上种种行为都深深植根于背后设计者和使用者的隐形预期,有关数据被纳入模型而其他“无关”信息被自动忽略反映的是人脑无意识的认知偏差。

其二,数据的处理方式及算法模型由“人”设计。数据被收集之后,需要使用特定的由人设计的算法模型处理数据,而模型在实际运用中的具体表现,一方面源于它学习的数据,另一方面源于人类设计模型的具体框架以及训练方法,即人决定了相关的算法模型如何有效地从海量数据中提取、利用和分析人类需求主导的信息。另外,在算法模型的架构和训练过程中,各类模型参数的调试始终充满“人为”色彩:从模型设计伊始,明确算法模型希望解决的

问题是什么、希望模型达到什么样的目标以及模型最终如何在实践中投入使用等等。因此,算法的“黑箱”特性实际上并非纯粹的技术问题,而是背后人脑对部分概念的“前见”“主动”选择的结果。当模型的设计者拒绝构建可解释的、公开透明的模型时,本质上是通过技术手段规避法律要求的说明责任。

然而,这种立足于二进制的人工语言的计算主义充其量只是机械主义地解释了计算机和人脑在信息处理上的某种相似性,无法化约人脑的复杂意志因素及其功能。易言之,所谓算法取证实际上是人类搭乘了信息科技的便利,通过自己设计的算法模型而进行的一系列大数据收集、处理活动。亦即,算法模型的设计者是算法承担法律责任的主体。以算法的所谓科技理性而视算法无偏见乃至以算法中立性作为免责的主张不能成立。对算法的归责应当且必须通过对算法模型的公开、备案等作为将来问责的基础,为算法承担法律的主体仍然是算法的设计者,即自然人主体。

三、规范算法取证司法程序的设想

算法取证对既有刑事诉讼和证据制度及其价值、理念提出的挑战,说明必须立足于数字法学的视野,以应然的刑事诉讼和证据制度及其理论为导向,厘清算法的数理逻辑,实现对算法从技术规制到法律规制的转变,在刑事诉讼和证据制度及其理论的系统性和一体性思维中,完善算法取证的程序制度设计,遏制算法权力,保障相对人的权利。

(一) 坚守程序正义的首位价值,实现算法取证技术的程序正当

尽管如前文所述,数据特有的无界性、高流动性和高风险性等,使数字时代对数据安全价值的强调和维护更加凸显,个人基本权利在面对国家和社会安全时将不得不有所克减。然而,在数据安全与算法取证所涉的程序正义之间,后者的基础性地位仍然不容撼动。原因在

于, 算法取证中所涉的相对人权利, 是现代宪法意义上公民的基本权利, 兼及“主观权利”和“客观法”的双重属性, 尤其是后者已被认为是宪法所确立的“客观价值秩序”, 对公权力而言, 是必须自觉遵守的价值秩序, 并尽一切可能创造和维护有利于基本权利实现的条件。^①在公权力与公民个人权利冲突至为激烈的刑事侦查程序中, 公权力主体对约束公权力的程序规则的恪守, 将直接影响公权力的公信力, 因此尤为重要。或者说, 面对数字时代个人权利面临的高风险, 更应该加强对基本权利的保护。

基于对刑事程序正义的信守, 有关技术性正当程序即应以程序正义为首要目标而须臾不得背离。否则, “当新的算法决策者掌管了个人生活的方方面面, 法律和正当程序在此领域若有缺席, 我们就将为这种不负责任的权力中介人建立的一种新的封建秩序打开了方便之门”^[23]。因此, 有研究者关于技术性正当程序系程序法与算法的双重变奏的主张^[24], 不应将其理解为算法规制的目标自外于程序法, 而应当是算法内嵌于程序正义之中, 因而实际是一种受到来自技术标准和法律制度的双重规制。从更为根本的意义上说, 算法取证仍然是作为主体的人的行为, 而所涉对象则是与人的尊严相关的数字权利。因而并非纯粹的科技性活动, 自然人的“人为”属性仍然是其底色。就算法取证而言, 则应当按照程序的正义要求, 以算法公开透明原则为基础, 参酌既有的侦查取证程序和证据的制度与理论等知识, 就算法取证的程序和算法证据制度, 设置相应的制度规范, 力求使算法取证成为看得见的正义。

(二) 完善算法取证制度的立法, 规范算法取证程序

一般意义上的算法规制应该克服规制思维、规制对象、规制主体以及规制工具的局限性, 形成一个完整、系统的制度体系。就算法取

证程序中对算法的规制而言, 主要涉及算法的公开和透明, 以及对算法的刑事程序化改造。

首先是算法取证中使用的相关算法需要公开透明。依照《个人信息保护法》第33条规定, 进行数据处理时, 应遵守该法的规定而履行相应的义务, 承担安全保障、合规审计、影响评估、泄漏补救措施等责任。同时, 根据《数据安全法》第8条关于数据处理的规定, 公权力机关在处理数据时, 也应履行数据安全保护义务, 承担社会责任, 不得危害国家安全、公共利益, 不得损害个人、组织的合法权益。这些规定界定了公权力机关包括相关平台在进行算法取证时的权力边界, 应当得到遵从。结合上述规定, 就算法取证而言, 从事算法取证的平台应当进行算法报备、公开源代码、说明数据的来源及其依据等, 同时还应负责解释有关取证的算法原理, 接受相关部门的监管。其中, 算法备案就是向监管部门提交算法设置的目的、风险、评估过程控制方案或自行备案, 以便进行算法评估, 及时发现算法缺陷并采取必要的安全性措施, 也便于监管部门日后对算法使用者是否具有主观过错进行考量, 确立算法问责点, 以及对算法运行监管以及算法审计。^[25]根据算法取证适用的场域、适用的主体等的特殊性, 结合算法规制的场景化要求^[14], 即针对不同的场景类型对算法采取不同的规制方式, 并作为算法问责的依据。具体而言, 应根据《个人信息保护法》第54~56条有关审计及风险评估制度, 制定算法取证中相关部门执行算法风险的审计与评估制度。同时, 根据《网络安全法》第21条有关网络运行中重要数据备份的规定, 制定有关算法备案中数据备份制度的详尽规则。此外, 通过算法解释^①加强算法取证的事后监督, 确保算法取证过程中算法运算具备合法性和合理性。

其次是算法取证程序的规范化。如前文所

^①关于个人基本权利的论述详见张翔:《基本权利的规范建构》, 法律出版社2023年第三版, 第23页。中国《个人信息保护法》提出处理个人信息应当遵循“合法、正当、必要和诚信原则”, 确保个人在信息处理过程中的尊严。并根据“识别+关联”标准, 对个人赋予知情权、决定权、查阅复制权、携带转移权、更正补充权、删除权、解释说明权以及信息权利救济权等, 涉及信息决定权、信息保密权、信息查询权、信息更正权、信息封锁权、信息删除权和信息报酬请求权等。

述,算法取证在启动的方式、启动的时间节点、取证的对象等方面,与传统物理空间中的初查高度相似,具有较强的任意性,因此几乎不受既有刑事程序制度的控制。然而,传统物理空间的初查尚可以通过行政执法化改革,使其纳入行政执法程序,防止以初查之名行侦查之实以得到相应的约束。^[26]算法取证则因其任意性、对象与目标的不确定性,以及参与算法取证主体的社会性等,而更加难以被纳入有效的程序规制。应当明确算法取证的基本原则、法定的取证主体和法定的取证程序,以此规范算法取证的相应程序。

一是确立算法取证的合法性规则。应当根据强制侦查的基本原则精神,结合算法取证的数字技术特点,确立规范算法取证的原则,确保算法取证的合法性。由于算法取证与数字侦查行为之间存在深度勾连,其合法性问题实际上就是数字侦查行为的合法性问题。后者除了涉及前文所述的算法公开制度外,还涉及数字侦查行为应该遵循的基本原则、如何实施事后监督以及如何使在数字侦查中得到有效落实个人信息保护等系统性制度设计和完善问题,笔者拟专门进行分析论述。这里仅就规范算法取证的合法性提出如下构想:应当建立个人信息分类管理制度,确立一般个人信息和敏感信息的分类标准;建立数据保护的负责人制度,定期进行信息和算法安全风险评估等;在涉及处理敏感信息时,做好此类个人信息处理过程中的去标识化工作,强化风险防范。同时规定,只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下,个人信息处理者方可处理敏感个人信息。与此同时,规范各类数据库建设,逐渐实现数据基础设施的建设主体与使用主体分离,数据资源收集主体与使用主体分离,以此抑制侦查权的过度扩张和侦查启动节点的过度前移。^[27]针对“知情同意原则”

存在例外且无时间限制的情形,其产生的法律效果是豁免而非延后告知,以及例外情形模糊而极易普遍化等问题,应在立法或通过解释形成实施细则等方面予以完善。这样的规制,还能转变执法人员在个人信息使用中的理念,使个人信息保护得到根本性落实。二是明确算法取证的主体。应当明确,算法取证属于国家公权力机关的行为,必须对履行主体进行严格限制,不能随意扩张。目前,尽管掌握数据的平台事实上已经成为一种社会性的公权力组织,但是,此类平台在参与数字侦查行为时,并不属于《个人信息保护法》所界定的“国家机关”,因此,此类平台在算法取证行为中只能视为国家公权力机关技术上的委托行为,其实施过程必须有前者的严格监管。严格遵照公安部《公安机关电子数据取证规则》第6条的规定:“收集、提取电子数据,应当由两名以上侦查人员进行。必要时,可以指派或者聘请专业技术人员在侦查人员主持下进行收集、提取电子数据。”三是明确算法取证的程序规则。由于算法取证是一种自动化决策的行为,因此,对算法取证的规制应当集中在取证前的算法模型设计及算法使用数据的监管。应严格参照并遵守《公安机关电子数据取证规则》第2条及第23条的规定,对算法模型设计及数据使用进行监管,具体而言,可以由专业技术人员就算法模型的设计及数据使用情况作出解释,侦查人员也可以在算法取证启动时对专业技术人员的操作在场进行监督。对于算法取证结果所呈现的数据的提取、保管等,则适用既有的关于电子数据收集、提取的规定。

(三)完善证据种类的立法,将算法证据纳入法定的证据种类

由于法定的证据种类是刑事证据具有证据资格的基本要件,应当根据《刑事诉讼法》第50条“可以用于证明案件事实的材料,都是证

①算法解释包括内部解释和外部解释,内部解释针对的是技术人员,其标准是可诊断性,目的是解决技术问题。从法律规制的角度来看,所谓的算法规制指涉的是其外部解释,目的是实现算法公开、公平,消除算法歧视、算法暴力、算法黑洞等,最终使算法得到规制,使那些与算法有关的人员在其数据权利受到侵害时有救济的机会。

据”的规定,结合“两高一部”2022年颁布实施的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第1条第1款关于电子数据的定义,即案件发生过程中形成的,以数字化形式存储、处理、传输的,能够证明案件事实的数据,以及该条第2款“电子数据包括但不限于下列信息、电子文件”的规定,可以通过扩张同时也是符合原义的解释,将算法证据纳入既有的八种证据种类之中,作为电子数据的一种亚类型。通过这一方法,可以使目前理论与实践算法证据成立与否及实践中使用的障碍得以克服。

在将来的刑事诉讼法修订中,应当结合“两高一部”等关于电信网络电子数据适用的相关解释,明确赋予算法证据独立的证据种类地位,唯有如此,方能最终解决算法取证理论和实践中的纷争,使人们不再无所适从。此外,在算法证据资格的规定上,应该根据前述“两高一部”2022年《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第6条的规定,将算法证据作为初查证据的一种,予以采用。在具体的审查采信上,仍应借鉴该规定,同时结合有关鉴定意见的审查规则,对算法证据从算法原理、算法运行程序、证据存储等方面进行审查,以判断其证据资格。

四、结语

算法取证是数字时代人工智能日益发达,科技反哺人类的应然之果。伴随着生成式人工智能的迅捷发展,算法生成的证据以更加丰富的方式呈现在司法实践中,在为人类解决纠纷带来便捷的同时,也将挑战人类基于传统物理空间的思维理念而设计的既有诉讼和证据制度。迎接数字科技之于传统法律制度的冲击,变革既有的诉讼和证据制度及其理念,使传统物理空间的法律能积极有效回应数字虚拟空间的法律吁求,将是理论研究并使其服务于法律实践的必由之路。然而,由于对算法技术在认知

上的迷思,尤其是因生成式人工智能的“自主学习”“自动化决策”等算法功能的日渐强大,而产生人工智能将来一定会战胜人脑的理念,更使人在如何规制算法、防止出现算法专制与歧视等现象时,常常感到束手无策,甚至陷入对算法的非理性盲从。因此,唯有突破算法取证在司法实践中的诸多困境,揭开算法的技术面纱,认清算法的“人为”属性,澄清其间的数字技术原理,以及作为规范算法技术的法律制度法理,并以此为基础,遵照现代刑事侦查取证对公权力必须进行限制的要求,找准算法技术标准与既有刑事侦查及证据规则的契合点,才能实现算法取证从技术性规制到法律规制的转型,突破算法的技术壁垒。

参考文献:

- [1]程雷. 大数据侦查的法律控制[J]. 中国社会科学, 2018(11): 157-179.
- [2]林冬梅. 国家治理视下大数据侦查犯罪治理功能: 问题、内涵及边界[J]. 中国人民公安大学学报(社会科学版), 2023(5): 33-40.
- [3]刘品新. 论大数据证据[J]. 环球法律评论, 2019(1): 22-25.
- [4]张迪. 刑事诉讼中的算法证据: 概念、机理及其运用[J]. 河南大学学报, 2023(3): 37-41.
- [5]林喜芬. 大数据证据在刑事司法中的运用初探[J]. 法学论坛, 2021(3): 27-35.
- [6]季卫东. 人工智能时代的法律议论[J]. 法学研究, 2019(6): 32-49.
- [7]刘东亮. 新一代法律智能系统的逻辑推理和论证说理[J]. 中国法学, 2022(3): 145-164.
- [8]栗峥. 人工智能与事实认定[J]. 法学研究, 2020(1): 117-133.
- [9]Sander k, Nart W. We are big data: The future of the information society[M]. Dordrecht: Atlantis Press, 2016.
- [10]郑戈. 算法的法律和法律的算法[J]. 中国法律评论, 2018(2): 66-85.
- [11]颜厥安. 法与实践理性[M]. 北京: 中国政法大学出版社, 2003.
- [12]张凌寒. 算法权力的兴起、异化及法律规制[J]. 法商研究, 2019(4): 63-74.
- [13]汪庆华. 算法透明的多重维度和算法问责[J]. 比较

法研究, 2020(6): 163-173.

[14]丁晓东. 论算法的法律规制[J]. 中国社会科学, 2020(12): 138-159.

[15]涂子沛. 大数据: 正在到来的数据革命, 以及它如何改变政府、商业与我们的生活[M]. 桂林: 广西师范大学出版社, 2013.

[16]裴炜. 个人信息大数据与刑事正当程序的冲突及其调和[J]. 法学研究, 2018(2): 42-61.

[17]Radina S. Digital evidence: Unaddressed threats to fairness and the presumption of innocence[J]. Computer Law&Security Review, 2021(42): 105575.

[18]Citron D K. Technological due process[J]. Washington University Law Review, 2007(85): 1249-1313.

[19]Edmond G, Roberts A. Procedural fairness, the criminal trial and forensic science and medicine[J]. The Sydney Law Review, 2011(33): 359-394.

[20]Dror I E. Cognitive and human factors in expert decision making: Six fallacies and theeight sources

of bias[J]. Analytical Chemistry, 2020(12): 7998-8004.

[21]Schum D A. The evidential foundations of probabilistic reasoning[M]. Evanston, IL: Northwestern University Press, 2001.

[22]涂子沛. 数据之巅: 大数据革命, 历史、现实与未来[M]. 北京: 中信出版社, 2014.

[23]Citron D K, Pasquale F. The scored society: Due process for automated predictions[J]. Washington Law Review, 2014(89): 1.

[24]刘东亮. 技术性正当程序: 人工智能时代程序法和算法的双重变奏[J]. 比较法研究, 2020(5): 64-79.

[25]何邦武. 数字法学视野下的网络空间治理[J]. 中国法学, 2022(4): 89.

[26]张泽涛. 初查的行政执法化改革及其配套机制——以公安机关“行刑衔接”为视角[J]. 法学研究, 2021(2): 108-121.

[27]胡铭, 张传玺. 大数据时代侦查权的扩张与规制[J]. 法学论坛, 2021(3): 13-14.

【责任编辑 邱佛梅】

Procedural Risks and Regulatory Approaches of Algorithmic Forensics in Judicial Application

HE Yuanjia & HE Bangwu

Abstract: The widespread application of big data-based algorithms in investigative evidence collection in the digital era is undeniable. Rooted in big data and cloud computing, algorithmic forensics is grounded in mathematical logic, which transforms logical reasoning and computation into symbolic, formalized and axiomatic knowledge. While reducing individuals to computable, predictable and controllable “objects,” algorithms give rise to a new power paradigm—the “algorithm as power” phenomenon—that backfires on humanity. Compared with traditional evidence collection methods in physical space, algorithmic forensics features covertness and pervasive intrusiveness. Lacking explicit legal authorization for initiation and operating opaquely, it violates the principle of statutory procedure, challenges established procedural justice institutions and creates an institutional deficit. Furthermore, the quasi-public power exercised by social digital platforms infringes on personal information rights, undermining the traditional principles of due process and the presumption of innocence. We must uphold the paramount value of criminal procedural justice. By demystifying algorithmic technical rationality, we should tame algorithms to ensure procedural due process. This requires improving digital evidence legislation, guaranteeing algorithmic transparency, establishing accountability points through algorithm filing, standardizing evidence collection procedures, and amending evidence legislation to formally include algorithmic evidence as a statutory category under China’s evidence system.

Keywords: big data; algorithmic forensics; algorithmic evidence; procedural justice; algorithmic justice