算法商业秘密的秘密性认定标准研究

萧 静　彭飞荣*

（中国计量大学法学院）

摘　要：算法作为商业秘密的保护客体已经在实证法上得到了确认，但是算法和其他一般的商业秘密相比存在着特殊性，算法秘密性与算法披露规则存在着一定程度的不兼容性，算法的黑箱性与复杂性使得其秘密性认定存在一定障碍。因此有必要对算法商业秘密的秘密性认定标准进行明确，有效落实对算法的商业秘密保护。本文将考虑到算法的特殊性以及《反不正当竞争法》第三十二条在司法适用上存在的问题，并结合相关案例提出相应的优化路径，明确算法秘密性认定标准，对《反不正当竞争法》第三十二条进行合理解释及具体适用。

关键词：算法，商业秘密，秘密性，标准

DOI编码：10.3969/j.issn.1674–5698.2024.05.010

Standard for Determining the Secrecy of Algorithmic Trade Secrets

XIAO Jing　PENG Fei-rong*

（China Jiliang University）

Abstract: Algorithm as trade secret protection object has been confirmed in the empirical law, but algorithm has its own characteristics compared to other general trade secrets, there is a certain degree of incompatibility between algorithm secrecy and algorithm disclosure rules. The black box and complexity of algorithm make it difficult to determine its secrecy. Therefore, it is necessary to clarify the standard for determining the secrecy of algorithmic trade secrets, so as to effectively protect algorithmic trade secrets. This paper takes into account the special characteristics of algorithms and the problems in the judicial application of Article 32 of the Anti-Unfair Competition Law, and puts forward corresponding optimization paths in combination with relevant cases, to clarify the standard for the determination of algorithmic secrecy, and provide a reasonable interpretation of Article 32 of the Anti-Unfair Competition Law and its specific application.

Keywords: algorithm, trade secret, secrecy, standards

基金项目：本文系浙江省高校重大人文社科攻关计划项目资助的规划重点项目“算法商业秘密的法律治理体系研究”（项目编号：2023GH077）的阶段性研究成果。

作者简介：萧静，硕士研究生，研究方向为知识产权法。

彭飞荣，通信作者，法学博士，中国计量大学法学院（知识产权学院）教授，国家知识产权培训（浙江）基地副主任，研究方向为知识产权法、标准化法。

0 引言

最高人民法院在2020年8月发布的《关于审理侵犯商业秘密民事案件适用法律若干问题的规定》(以下简称《商业秘密规定》),已经明确规定了将算法纳入商业秘密的保护范畴,由此,算法以商业秘密的形式获得了法律保护。算法作为人类所设计的一种解决特定问题的步骤方法,具有复杂性和专业性,是属于人类的智力成果,并且算法可以为企业带来巨大的竞争优势,具有一定的商业价值,企业会对相关算法采取一定的保密措施以防算法泄露以致于丧失竞争优势,若是其他企业通过各种手段获取了该算法,将该算法应用于商业活动,那么此算法的初始创作公司则会失去竞争优势,遭受巨大的商业损失。因此算法作为企业的核心竞争力面临着被侵犯的风险,有必要对算法进行商业秘密保护。而在算法商业秘密侵权案件中,对于其秘密性的认定,法官对法律条文的理解存在差异,因而容易导致不同的判决结果。秘密性作为算法商业秘密保护的核心,没有一个统一的认定标准。因此,本文旨在讨论,当算法作为商业秘密时,应当以何标准对其“秘密性”进行认定。

1 算法、商业秘密及其秘密性认定的必要性

1.1 算法与商业秘密

根据我国《反不正当竞争法》,商业秘密是技术信息、经营信息等商业信息,具备3个构成要件:价值性、秘密性、保密性。算法是由专业的技术人员运用专业的技术知识开发出来解决技术问题的,表现形式为体现在成千上万行程序代码中的解决技术问题的设计框架,属于商业信息中的技术信息。它作为人类所设计的一种解决特定问题的步骤方法,具有复杂性和专业性,是属于人类的智力成果,并且算法可以为企业带来巨大的竞争优势,成为高新企业的核心竞争力,具有一定的商业价值,企业为了维持此竞争优势,对相关算法严加保护,采取加密措施,并且内部人员对算法有着严格的接触限制,外部人员也没有接触该算法的公开渠道,因此算法满足商业秘密构成要件。

在智搜公司诉光速蜗牛公司一案中我们可以看出[1],尽管算法的基础是公开技术,但投入商业应用的算法是企业在大量人力物力的投入下,经过选择、研发、测试等过程,为满足商业需求而构建的最优模型。在算法研发过程中,企业会对特有的数据源信息进行标记,对用户信息和环境特征信息进行拆分,并根据产品使用过程中用户的操作反馈来修正算法,这一系列步骤都具有秘密性。在司法实践中,即使是完全公开的信息,也可能因其特殊的组合方式而具备秘密性。由此可见,虽然某些具体的函数关系、模型可能处于公知领域,但如果算法对这些函数、模型的选择,或者参数的设定,是不为公众所普遍认知的,那么算法本身仍然可以作为商业秘密被保护。

1.2 算法商业秘密的秘密性认定必要性

1.2.1 算法商业秘密特殊性影响秘密性认定

算法不同于其他的技术秘密,因其具有易变性、不透明性等特性使其往往难以通过直观方式展现,因此需要通过秘密性认定来明确其作为商业秘密的属性。因算法的特殊性,所以在进行秘密性认定时亦具有特殊性。首先,算法是一种程序化的数学模型,其本质是一系列逻辑运算和数据处理的过程,其秘密性认定需要对其中的具体实现细节和参数进行深入地分析和研究,这需要相关人员具备专业的计算机科学和数学背景知识。同时,由于算法的不断更新和演化,其秘密性的认定也需要不断地进行动态的评估和调整。其次,算法在很多情况下不仅是商业运营的核心,还关系着用户隐私和数据安全,如搜索引擎的排序算法、电商平台的推荐算法等,某些算法在运行过程中可能会收集用户的个人信息或行为数据。因此,在认定算法秘密性时,企业商业利益是一个考虑要素,用户隐私和数据安全的问题也应纳入考虑,在保护算法秘密性的同时也应该遵守相应的隐私政策和法律法规。算法亦具有不透明性,算法的不透明性与公共利益之间存在一定程度的不兼容性,在对算法商业秘密进行保护时,需要在公开透

明与社会责任之间寻求适当的平衡点。

1.2.2 行业内一般认知程度影响秘密性认定

行业内对算法的一般认知程度是判断其秘密性的重要参考依据。算法具有高度复杂性与技术性，在一般情况下，本行业的一般技术人员知晓则表明此算法是公知的，其不具有秘密性，如上所说的“一般技术人员”并不要求是该行业的精英，而是指该行业中具备最基本能力的人，若是该算法只有少数的行业精英知晓，那么此类算法自然具有秘密性，在算法研发行业内，一般情况下算法研发人员往往并不会将算法公之于众，而是会经过加密用特定方式将该算法在计算机中存储起来。如果签订了保密协议或是受到竞业限制，若是算法研发人将自己所研发的算法告知所任职公司或是自己认为可以对该算法保密的其他人，亦或是在该算法需要进行测试时将其公开给必要的特定人员，应该认为该算法也并未丧失秘密性。在算法的研发过程中往往可能涉及整个团队而不仅仅是个人，作为共同的算法研发者，有些人员可能并未参与算法研发的整个过程，并未对该算法的研发投入太多的贡献，那么作为此种共同研发者知晓该算法也并不会使得该算法丧失秘密性。

1.2.3 保密措施影响秘密性认定

算法的秘密性是企业核心竞争力的体现，也是众多企业和开发者投入大量资源和心血所保护的宝贵资产。为了维护算法商业秘密，权利人会采取一系列严格的保密措施。当决定将算法及其源代码作为商业秘密来保护时，对源代码进行混淆处理可以进行有效保护。源代码混淆是一种有效的技术手段，旨在使代码在反编译后变得难以理解和分析，通过改变变量名、函数名、注释等，混淆后的代码对于非专业人士来说几乎是不可读的，从而大大提高了其安全性。然而，仅仅依靠源代码混淆并不足以完全保障算法的安全。为了进一步加强保护，权利人还会对已混淆的代码进行二次保护，即代码加固。代码加固采用多种技术手段，如：加密、签名、代码段隐藏等，以防止破解者通过静态或动态分析手段获取到关键算法和逻辑。除了上述技术措施外，权利人还会在数据传输和存储方面采取额外的安全措施。例如：使用加密通信协议以确保数据在传输过程中不被恶意复改或窃取，同时，使用内存保护技术可以防止算法在运行时被篡改或窃取。这些措施共同构成了算法商业秘密保护的多重防线。

总之，采取合理的保密措施是保护算法商业秘密的重要一环。从源代码混淆到代码加固再到数据传输和存储安全，每一步都需要精心设计和执行。只有这样，才能确保算法的商业秘密地位得到有效维护，为企业的核心竞争力提供坚实保障。

2　算法商业秘密的秘密性认定难题

2.1 算法秘密性受限于披露规则

算法黑箱的存在易导致算法权力滥用，有学者主张应该打开算法黑箱，对算法进行解释，但是算法解释权的行使受到商业秘密保护的阻碍，打开算法黑箱可能会导致算法丧失其秘密性。在司法实践中，大多算法商业秘密权利人会以商业秘密保护为由拒绝披露相关算法信息。虽然在我国司法实践中尚还缺乏直接的算法披露案件，但是从相关司法案例中我们不难看出企业对算法披露的强烈抵制态度。在北京元鼎时代科技股份有限公司、屈战斌等侵害技术秘密纠纷一案中[2]，法院认为涉案计算机源代码是否为公众所知悉，并不需要实际提交相关的计算机软件源代码作为证据，并且拥有计算机软件著作权登记证书亦并不等同于计算机软件源代码已被公开，从此判决书中我们不难推测出若是源代码进行一定披露则可能对涉案技术信息的秘密性产生不利影响。在陈某诉杭州某软件服务公司网络服务合同纠纷一案中[3]，一审法院认为“阿里妈妈可视是否涉及商业秘密等而独立决定是否披露具体认定依据”这一格式条款因显失公平而无效，这也间接说明了一审法院否认了以商业秘密为由而拒绝披露算法的请求。在美国Loomis一案中[4]，法院在量刑时利用COMPAS累犯风险评分算法对被告人Loomis做出了量刑决定，Loomis认为其权利受到侵犯，要求法院对该算法进行解释，但法院以商业秘密保护为

由拒绝披露算法。

显然，对于算法解释权和商业秘密冲突的不同态度导致案件会呈现出两种不同的结果。我国《个人信息保护法》规定了算法解释义务，算法秘密性的认定受限于披露规则，对此，我国理论界也存在莫衷一是的情况。有学者对算法解释权持反对态度，认为这会造成算法秘密性的丧失，导致商业秘密构成要件缺失[5]；也有学者认为应该提高算法透明度，对算法进行解释[6]。算法对于企业来说具有巨大的商业价值，算法的秘密性是商业秘密存在的基础。在算法商业秘密和公共利益之间应该进行利益衡量，在维持其秘密性和保护公共利益之间找到一个合理的尺度，使得算法的秘密性不因披露规则而丧失。

2.2 认定秘密性时混淆保密性要求

秘密性与保密性都是商业秘密的构成要件，而秘密性属于消极事实，对于消极事实的证明面临着极端苛刻的难度，从而可能导致待证事实即商业秘密存在的事实陷入死循环，而使得商业秘密权利人面临不利的诉讼结果。对于商业秘密的秘密性可以通过对“采取保密措施”的证明来间接达到证明目的，因为二者之间存在着一定的逻辑关系，即秘密性成立的可能性和保密措施的严密程度呈正相关。尤其是对于算法而言，企业通常会采取高强度的保密措施来保护算法，因此基于秘密性与保密性之间的逻辑关系，对于算法秘密性的认定尤其容易证明，但是这种逻辑显然不够周延。在我国司法实践中，有些法院认定涉案信息是否具有秘密性是通过原告是否对涉案信息采取了相应的保密措施来进行认定的。在我国首例算法商业秘密保护一案中即是如此，法院认为智搜公司的涉案算法能够带来商业收益和竞争优势，并采取了合理的保密措施，因此认定该算法属于商业秘密。然而，这种做法混淆了商业秘密的秘密性要件和保密性要件，错误地将客观性的秘密性认定转变为主观性的保密性认定，从而陷入循环论证的误区[7]。这些做法都是对《反不正当竞争法》第三十二条的错误理解与错误适用，出现这种错误的原因是有人错误地认为这一法律条文属于法律推定，即以权利人采取保密措施为小前提，以该信息具有秘密性作为推定结论。不难推断出，若是在算法商业秘密的秘密性认定中采用此种逻辑会出现什么结果：算法并非是有形的终端产品，而是通过源代码实现，然而，几乎所有的权利人都会对源代码采取一定的保密措施，这是毋庸置疑的，那么基于以上逻辑，是否可以直接认定算法具有秘密性呢？这显然会造成算法权利人与侵权人之间权利义务的失衡，因此此种观点值得商榷。

2.3 秘密性的举证规则不明确

2019年新修订的《反不正当竞争法》第三十二条规定了商业秘密侵权的举证责任[8]，但对于此条关于秘密性的举证责任尚还存在分歧，这一条文虽将降低商业秘密维权难度作为修订的重要目标之一，但其文义表述不甚清楚、规范立场相对模糊，从而导致秘密性举证责任不甚明确。

我国司法实务中对商业秘密的秘密性存在着几种不同的认定标准，认定标准的混乱导致举证责任不一。有些案件在原告明确了密点之后则完成了初步举证责任，此时否定秘密性要件的举证责任则转移给了被告[9]。但是有些案件则要求原告不仅需要提交秘密点，还需要原告提供查新报告或者非公知性鉴定等其他证明秘密性的证据[10]。不可否认的是，对于那些深度性较为欠缺的信息，原告除了明确其密点外，还需进一步提供补强证据以证明其诉请信息具有秘密性。但是对于算法而言，其区别于一般的技术秘密，具有很强的复杂性、专业性和深度性，其固有的特性使其秘密性的认定不能完全适用一般技术秘密现有的认定规则，算法具有高度专业性和复杂性，需要相关人员充分了解算法核心思想、演变路径等，其秘密性的认定极其依靠专业人员，因此，对于算法秘密性的认定可以在现行法律框架下放宽其举证责任要求，建立起一个有序且操作性强的司法认定标准，进一步明确其举证责任。

3 优化算法商业秘密的秘密性认定标准的具体路径

3.1 明确算法披露标准

为了化解算法秘密性与公共利益之间的冲突，基于利益衡量理论，可以对算法实行定限披露，设定合理的适度披露制度，将算法“掀开最小缝隙”[11]，以“非必要不公开”为基本原则，在特定范围内优先面向特定群体进行信息披露，缩小了解算法秘密的人员范围，比如：可以将对个人权益造成重大影响作为算法披露的前提，将算法披露的受众范围限定在利益相关者和政府监管部门、司法机关等群体。算法披露，并不意味着算法权利人放弃了对算法的商业秘密保护，算法权利人披露的并非算法本身，而是数据处理的基本逻辑[12]，在对算法进行解释时，不必对算法的具体技术细节进行公开，只需披露算法逻辑的有用信息[13]。当算法商业秘密合理披露时，有关机构应该通过制定相关规定明确该算法仍不丧失秘密性，这样既可以满足国家机关对算法的监管需求，又可以保障公共利益，同时也确保算法权利人仍对该算法享有商业秘密权益。

3.2 厘清秘密性与保密性的边界

秘密性是一个客观标准，普遍知悉和容易获得都属于客观事实，这些事实的存在与否，仅取决于该信息是否已以某种形式进入公有领域、权利人形成该信息所耗费的成本以及他人以正当途径获取该信息的难易程度等客观因素，并不会因为任何人的主观愿望发生改变。而保密性的判断则需要从主观和客观两方面来进行考虑，主观上有将信息作为商业秘密进行保护的意识，客观上也采取了与该信息相适应的保密措施。虽然非公知性与保密性之间存在一定的正相关性，但是并不能简单地将它们画上等号。仅仅因为权利人对涉案信息采取了合理的保密措施，并不能直接判定该信息具有秘密性。同样，仅仅因为权利人未对涉案信息采取合理的保密措施，也不能因此判定该信息不具有秘密性。这种简单的等同观念违背了法院在认定商业秘密各项构成要件时应当遵循的基本原理，法院在认定商业秘密时，需对信息的秘密性、保密性、价值性进行综合分析。并且就秘密性和保密性存在的逻辑关系而言，权利人所采取的保密措施应该与其所主张的商业秘密的内容相适配。对于算法商业秘密而言，因其价值位阶较高，所以权利人应当采取更为谨慎且复杂的保密措施，仅仅依据劳动合同中约定的原则性的保密条款亦或是竞业限制都不能成为法院认可的合理的保密措施。

3.3 明晰举证规则

加强算法的保护与治理是新时代应有之义，并且我国多项司法政策文件一直主张要强化对商业秘密的法律保护力度。减轻算法商业秘密权利人的举证责任负担正凸显了我国加强对于商业秘密保护的政策倾向。但是，一味地抑强扶弱有违法律公正的实现，因此，在解释算法商业秘密秘密性的举证责任时要综合考量利益的平衡。

在明确其举证责任之前，权利人应该先明确其所主张算法秘密的秘密点，这是进行秘密性认定的基础。权利人在确定算法商业秘密的秘密点时，不仅需要算法的源代码，还需要合理描述算法核心思想，即该算法是怎样被设计出来解决问题的，各个步骤是怎样被安排的，部分与部分之间是怎样架构的，框架是怎么安排的以及算法的设计方案是如何形成的等等。在秘密点确定之后，方能明确其举证责任。首先应该对《反不正当竞争法》第三十二条关于秘密性的举证责任进行规范解读。根据第三十二条第一款，在涉及商业秘密的案件中，权利人需初步证明已采取合理保密措施且被诉方存在侵权行为，此时，权利人无需进一步证明商业秘密的秘密性，而是由被诉方负责证明该信息不具有秘密性。另一方面，第三十二条第二款指出，当权利人能提供初步证据合理表明商业秘密已被侵犯，并对列出的3种情形之一提供证据时，涉嫌侵权人应证明其未实施侵犯商业秘密的行为。这两款规定共同构成了举证责任转移的前提条件，即权利人可以通过证明“采取保密措施”“合理表明被侵犯”使得算法秘密性的举证责任转移至对方。

即明确了第三十二条属于举证责任转移，那么对于“采取保密措施”“合理表明被侵犯”应证明到何种程度呢？换言之，“初步证据”“合理表明”的证明标准应是什么呢？“采取保密措施”“合理

表明被侵犯”属于积极事实，权利人很容易通过举证来证明，算法在研发时其所有人会采取各种保密措施来保护算法，比如运用区块链技术、时间戳技术来对算法提供有力的保密措施，并且算法的表现形式一般为源代码，其很难通过反向工程进行破译。算法作为技术秘密，针对它的保密措施要求的标准应适当低于其他的一般商业秘密，因为技术信息中蕴含的技术天然具有获取并使用的难度，并不需要商业秘密权利人采取过于严格的保密措施[14]，所以针对“采取保密措施”的证明标准的关键点在于对“合理性”的理解。对于算法商业秘密来说，作为一个合理的保密措施，应该能够防止一般人员毫不费力地获取。其次，对于“合理表明被侵犯”，根据《反不正当竞争法》第九条第一款，侵犯商业秘密的行为可以分为两种类型，即不正当获取和不正当披露、使用行为。针对前种类型，在算法商业秘密侵权纠纷中，权利人提供证据证明涉嫌侵权人有接触和非法获取该算法的可能性且被诉信息与该算法实质相同，鉴于算法的固有特性，如：高度的隐蔽性和非公开性，对涉嫌侵权人更有可能采取了不正当手段进行合理的推断，因此，可以初步认定涉嫌侵权人通过不正当方式获取了该算法，除非侵权人能提供证据证明其是通过合法途径获得。在第二类情况中，权利人仅需出示证据表明商业秘密存在被侵权人披露、使用或面临此风险的情况，并不要求其行为的实际发生。值得注意的是，我国民事诉讼中一般遵循“高度盖然性”证明标准，但此处所提及的“初步证据”则暗示了一种相对较低的证明标准，即低于一般民事诉讼中的“高度盖然性”要求。在以往的司法实践中，许多法院也尝试着降低原告对于“秘密性”证明标准的要求，但是一方面既要降低权利人的举证难度，一方面也不能一味地降低举证难度以防发生滥诉。因此在对算法商业秘密秘密性的证明标准进行明确时，需要充分考虑到权利人所采取的保密措施，若采取的保密措施越强，那么证明标准可以适当低于高度盖然性标准。

据此可以看出，提供初步证据的要求是清晰的，但“合理表明被侵犯”则具有一定的弹性。对于算法这种具有高度专业性与深度性的技术信息，根据第三十二条规定的“提供初步证据合理表明”，应当被解释为明显低于“高度可能性”标准，甚至可以低于优势证据标准。

4 结论

《商业秘密规定》虽然将算法纳入了商业秘密的保护范畴，但是对于其秘密性的认定标准上仍存在诸多难题。算法的商业秘密保护与公共利益存在冲突，算法披露规则在一定程度上对其秘密性认定造成了影响。并且由于《反不正当竞争法》第三十二条语义模糊与逻辑上存在争议，使得算法商业秘密构成要件以及秘密性举证规则混乱。通过相关法律以及相关案例的分析，使应然引导实然，在对算法的秘密性进行认定时需要对算法披露的限度进行界定，并且应该进一步明确界定算法商业秘密的构成要件，并明确其秘密性举证规则，构建一个相对统一的秘密性认定标准。

总而言之，鉴于算法商业秘密的复杂情况，实践中对其的保护仍存在诸多问题，更遑论算法商业秘密的秘密性认定问题。在这个算法泛在的时代，我国对于算法商业秘密的研究仍处于萌芽阶段，对于算法商业秘密的秘密性认定标准的研究更是凤毛麟角。本文对此虽给出了几点拙见，但是对算法商业秘密秘密性的认定标准仍需要开展更深入的研究，并结合实际案例验证其可行性。

（下转第78页）

参考文献

[1] 李爽,黄福才,李建中. 旅游公共服务内涵、特征与分类框架[J]. 旅游学刊, 2010,25(04):20–26.

[2] 李爽,甘巧林,刘望保. 旅游公共服务体系：一个理论框架的构建[J]. 北京第二外国语学院学报, 2010,32(05):8–15,30.

[3] 董培海,李伟. 关于“旅游公共服务体系”的解读——兼评我国旅游公共服务体系建设[J]. 旅游研究, 2010,2(04):86–9.

[4] 河池康. 旅游公共服务体系建设研究[D]. 北京：中央民族大学, 2011: 41–42.

[5] 徐菊凤,潘悦然. 旅游公共服务的理论认知与实践判断——兼与李爽商榷[J]. 旅游学刊, 2014,29(01) :27–38.

[6] 何建民. 我国旅游公共服务体系的构建及优化研究——基于新加坡与中国香港经验及上海案例分析[J]. 旅游导刊, 2017,1(01)：21–41.

[7] LB/T 022–2013, 城市旅游公共服务基本要求[S].

[8] 国家旅游局. “十三五”全国旅游公共服务规划[Z].北京：国家旅游局, 2017.

[9] 韩小威,尹栾玉. 基本公共服务概念辨析[J]. 江汉论坛, 2010(09)：42–44.

[10] 郁建兴,秦上人. 论基本公共服务的标准化[J]. 中国行政管理, 2015(04)：47–51.

[11] 钱振明. 新时代基本公共服务体系的现代化发展：基于均衡性和可及性的考察[J]. 中国行政管理, 2023,39(10)：54–61.

[12] 孙九霞,李菲,王学基. “旅游中国”：四十年旅游发展与当代社会变迁[J]. 中国社会科学, 2023(11):84–104+206.

（上接第71页）

参考文献

[1] 深圳市中级人民法院（2021）粤03民初3843号民事判决书[Z].

[2] 最高人民法院（2021）最高法知民终2389号判决书[Z].

[3] 浙江省杭州铁路运输法院（2017）浙8601民初3306号民事判决书[Z].

[4] See State v. Loomis, 881 NW2d 749 (2016)[Z].

[5] 辛巧巧. 算法解释权质疑[J]. 求是学刊, 2021,48(03):100–109.

[6] 李安. 算法透明与商业秘密的冲突及协调[J]. 电子知识产权, 2021(04):26–39.

[7] 黄武双,戴芳芳. 论技术秘密构成要件的认定——以定作产品技术秘密为视角[J]. 科技与法律(中英文), 2022(04):10–19+122.

[8] 反不正当竞争法[Z].

[9] 广东省深圳市中级人民法院（2020）粤03民初5073号判决书[Z].

[10] 辽宁省大连市中级人民法院（2020）辽02民初325号判决书[Z].

[11] 刘琳. 算法解释权与商业秘密保护的冲突化解[J]. 行政法学研究, 2023(02):168–176.

[12] 陶乾. 商业秘密保护法的规范构造研究[M]. 北京: 法律出版社, 2022:187.

[13] 吕炳斌. 论个人信息处理者的算法说明义务[J]. 现代法学, 2021,43(04):89–101.

[14] 吴锦汶. 商业秘密侵权行为举证责任分配：理性反思与制度建构[J]. 贸大法学, 2021,6(00):60–72.