Dispute Settlement 争议解决, 2026, 12(6), 187-194
Published Online June 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.126200

Hans汉斯

商业秘密视域下商业数据的保护边界与路径构建

余　愿

南京理工大学知识产权学院，江苏　南京

收稿日期：2026年5月16日；录用日期：2026年6月17日；发布日期：2026年6月26日

摘　要

数据要素在推动产业发展中起着至关重要的作用，且其商业价值使得数据侵权行为频繁发生。在这种背景下，利用商业秘密保护数据符合促进经济发展的法治趋势。然而，从目前的司法实践来看，商业秘密的保护范围对于数据的适用较为有限，且由于数据和算法的界定模糊，司法机关往往无法直接判定其是否受到保护。对于超出商业秘密保护范围的公开数据集合，需通过转换公开数据为秘密信息的方式，纳入保护，避免竞争者借机“搭便车”。因此，完善数据商业秘密保护的法律框架，有助于激励数据的深入开发与利用，同时促进数据流通和共享，为建立全面的数据权益保护体系提供基础。

关键词

企业数据，商业秘密，数据集合

Protection Boundaries and Pathway Construction for Commercial Data from the Perspective of Trade Secrets

Yuan Yu

School of Intellectual Property, Nanjing University of Science and Technology, Nanjing Jiangsu

Received: May 16, 2026; accepted: June 17, 2026; published: June 26, 2026

Abstract

Data elements play a crucial role in driving industrial development, and their commercial value has led to frequent occurrences of data infringement. Against this backdrop, protecting data through trade secret law aligns with the rule-of-law trend of promoting economic development. However,

文章引用: 余愿. 商业秘密视域下商业数据的保护边界与路径构建[J]. 争议解决, 2026, 12(6): 187-194.
DOI: 10.12677/ds.2026.126200

judicial practice reveals that the scope of trade secret protection is relatively limited when applied to data. Moreover, due to ambiguous definitions of data and algorithms, judicial authorities often cannot directly determine whether such subject matter is protectable. For publicly available data sets that fall outside the scope of trade secret protection, they should be brought under protection by converting public data into confidential information, so as to prevent competitors from "free-riding". Therefore, improving the legal framework for the trade secret protection of data will help incentivize the in-depth development and utilization of data, facilitate data circulation and sharing, and lay the foundation for establishing a comprehensive system for the protection of data rights and interests.

Keywords

Enterprise Data, Trade Secrets, Data Sets

Copyright © 2026 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. 问题的提出

在我国的法律体系中，保护商业秘密的法律涵盖了《中华人民共和国反不正当竞争法》(后文简称《反不正当竞争法》)、《中华人民共和国民法典》和《中华人民共和国刑法》等，以及相关的司法解释。这些法律对商业秘密进行了分散的规定。2019 年，《反不正当竞争法》的修订扩大了商业秘密保护的范围。2020 年，最高人民法院发布的司法解释将“数据”认定为重要的商业信息，并明确指出，具备“秘密性”、“保密性”和“价值性”的信息可以作为商业秘密受到保护。不过在具体的司法实践当中，数据通过商业秘密保护存在司法认定的难点，商业秘密保护对数据的保护存在困难。本文通过数据领域的两起案例来分析数据商业秘密保护的现有难题。

第一个案例是杭州“嗨狗公司诉汪勇商业秘密纠纷”案[1]。杭州嗨狗网络科技有限公司(以下简称嗨狗公司)有两个直播平台，主播收到用户打赏礼物兑换成现金后需与公司按约定比例分配收益。嗨狗公司在打赏过程中设置了中奖机制，将一定比例的打赏金额放入奖池，以某一时段的礼物赠送数量设为一个索引，后台程序会随机抽取索引中的散落礼物作为中奖礼物，期间到达一定数值的用户会从奖池中获得打赏金额的 N 倍作为奖金。汪某之前是嗨狗公司运营总监，在其任职期间汪某利用自己的权限，查看后台数据并进行分析，发现一定时间段中有些时候开奖的中奖率会高于其他时间，并通过自己的多个关联账号进行“刷奖”，每次都取得巨额奖金。后汪某入职同一行业另一家公司，在入职前公司已注销汪某的原账号，汪某离职后又通过其获取嗨狗公司员工胡某的账号继续上线查询数据进行刷奖。一年多来多次重复同样的行为，并通过数十名主播提现。嗨狗公司诉称汪某在职期间利用程序员所拥有的高权限账号查看后台数据掌握从中获得最大收益的时间段，利用关联账号“刷奖”的方式，离职后入职同一行业其他公司继续用高权限账号登录后台查询数据“刷奖”，极大损害了公司的商业利益，侵犯其商业秘密。

初审法院认为，嗨狗公司主张的经营信息具有秘密性、保密性和商业价值，依法应当按照有关商业秘密的规定进行保护。汪某登录嗨狗公司系统实际上接触使用了嗨狗公司的商业秘密，主观上存在过失，客观上实施了侵权行为，构成对商业秘密的侵犯。二审法院认为，嗨狗公司通过与职工签订保密协议等多种手段对其进行了保护，这些数据具有还原打赏场景、总结中奖规律的实际价值，还有预测用户行为、

[1]嗨狗公司诉汪勇商业秘密纠纷案。杭州市中级人民法院（2021）浙 01 民终 11274 号。

审视经营策略的深层潜在价值，内容具体明确，符合保密性、秘密性和商业价值的构成要件，构成商业秘密。但是，嗨狗公司主张其在本案中主张的通过实时数据推算得出的中奖概率，是通过特定算法对系统后台数据进行计算而得出的，其保护的内容其基础实际上是后台数据和算法本身，而不是一个具体明确的、可以独立使用的客体，因而不应该与后台数据并列作为独立的经营信息予以保护。本判决对数据的秘密性、保密性和价值性三方面的特征进行了确认。但是二审法院提出的中奖概率主要依靠算法技术的应用，即使为嗨狗公司带来了经济利益，但仍然不能作为商业秘密保护，算法本身能否获得商业秘密保护也并未明确。

第二个案件是“北京微播视界公司诉上海六界公司、厦门扒块腹肌公司、浙江淘宝公司不正当竞争纠纷案件”[2]。微播公司开发了“抖音”应用，六界公司是“小葫芦官网”的运营者，“小葫芦官网”提供“直播红人榜”“礼物星光榜”“土豪排行榜”服务，其中，用户可查询不同时间段内抖音平台上按照礼物价值与收入排行榜名的主播的头像、昵称、具体礼物数额、送礼人数、直播记录等信息，还可查询按照打赏礼物的总价值排行的用户头像、昵称、累计礼物贡献值、送礼总额、喜欢的主播、送礼详情等信息。随机选择的抖音直播主播都能查到各自的信息以及直播数据分析。微播公司诉称，六界公司未经其授权，长期通过不正当技术手段非法抓取抖音平台上用户的直播打赏记录等与主播收益相关的数据，并以付费的方式向网站用户开放提供，构成不正当竞争。六界公司辩称通过 OCR 识别技术获得了抖音平台的数据，并通过整理生成了数据包，并非不正当竞争。

初审法院认为，六界公司使用技术手段非法获取抖音平台上用户直播打赏记录和主播收益等非公开数据，并整理后公开展示的行为是不正当的，侵犯了微播公司、抖音主播及打赏用户的合法权益，扰乱了市场竞争秩序，构成了不正当竞争；二审法院认为，抖音平台主播的收入和用户打赏的具体金额，属于非公开信息，不能通过抖音直播间前端页面完整获取，六界公司使用不正当的技术手段获取抖音平台上的非公开数据并在小葫芦平台进行展示和销售，威胁到微播公司的数据安全，侵犯了抖音产品和服务用户的隐私，影响了抖音及相关产品和服务的商业策略的实施，严重削弱用户对抖音平台的信任，造成了用户流失和商誉受损，其行为构成了不正当竞争。本案当中，数据公开但信息内容并未主动公开，并且微播公司对该非公开信息采取了保密措施，该信息符合了秘密性、保密性、价值性的要求，从商业秘密角度保护数据具有合理性。二审法院也意识到数据集合中存在非公开信息，但并未适用商业秘密的规定对数据集合进行保护，反映在商业秘密保护数据集合存在适用难点。

从以上案例可知，算法和公开数据能否纳入商业秘密保护都存在较大不确定性，导致司法机关容易绕过商业秘密而适用反不正当竞争法处理数据类案件，这就会导致存在的法律模糊地带一直得不到明确，也不能充分保护数据权益。因此，应当明确算法属性，积极将公开数据转换为非公开信息，明确纳入商业秘密保护范围。

2. 商业秘密保护数据的必要性

实践中最常适用反不正当竞争法互联网专条或一般条款保护数据。但是法院在判决中受制于“不告不理”原则，回避了数据纠纷中的许多深层次问题，且由于互联网专条和一般条款的固有缺陷，商业秘密保护路径相比起来似乎更加契合对数据的保护。

1、互联网专条存在缺陷

2017 年《反不正当竞争法》修订时，在面对互联网迅猛发展下，新增第十二条规定了互联网领域的不正当竞争行为，学术界又称为“互联网专条”。其中互联网专条第二款前三段规定了网络软件之间的

[2]北京微播视界公司与上海六界公司、厦门扒块腹肌公司、浙江淘宝公司不正当竞争纠纷案，杭州市中级人民法院（2022）浙 01 民终 1203 号。

三种典型互联网不正当竞争行为，例如流量拦盘、流量干扰和恶意不兼容支持等，主要是对网络软件之间的不正当竞争行为进行了列举式规定，但对侵犯商业数据的行为，规制效果较差。而在对上述行为的规制效果不明显时，则会通过兜底性条款来寻求相应的帮助。而由于兜底条款的过于笼统、过于模糊，使得兜底条款同样会在司法实践中将其与互联网专条的概括性条款以及《反不正当竞争法》的立法目的相结合作出解读。综合概括互联网专条的条款，能够适用于兜底性条款的要素主要有三个方面：利用了技术手段、影响或干扰客户的自由选择、阻碍或阻碍遭受侵害的网络商品或综合服务等。

首先，“利用技术手段”的规定无疑限制了对侵犯商业数据行为的适用范围，部分未通过技术手段侵犯商业数据的行为无法纳入规制；而“影响或干扰客户选择”这一标准，在市场经济调节的环境下较难界定，因为消费者应当依据自身判断作出独立决策，且只有消费者才能评估是否因商业数据被盗用而做出选择改变，法律无法替代这一判断；至于“阻碍或损害网络商品或综合服务”，若以此作为规制商业数据侵犯行为的依据，其适用逻辑应针对对数据的直接破坏或妨碍，但在现实中，商业数据的侵犯通常表现为复制而非破坏，因此，兜底条款的适用存在一定的局限性[1]。

2、反不正当竞争法一般条款保护存在的问题

由于一般条款本身具有抽象与模糊性，相应地也就具有使用时的随机性与不稳定性，因此难免产生若干层面的困难。一方面，由于缺乏统一的评价标准，各级人民法院在通过一般条款评判商业数据竞争行为时，很容易根据主观意见得出结论，究其原因无外乎如何界定商业道德、案涉行为是否违反商业道德两大问题，而这恰恰又是其众口难调的重要原因，属于绝对自由裁量范畴[2]。因此，这就不可避免地带来主观性，从而导致法律适用相互矛盾，同案不同判，同时也损伤了法院的公平性与权威性。另一方面，从商业数据规制层面来看，虽然一般条款可以在一定程度上起到救济商业数据的功效，但其高度抽象与宽泛的性质却不可避免地使数据经营者在遵循商业道德方面缺乏清晰的判断标准，甚至缺少商业道德这一概念的可参照对象，这些都会给企业带来巨大的困惑，并加重数据合法合规及真正应用成本[3]。对企业来说，因为没有绝对可行的评价标准，会导致企业降低或放弃目前的数据应用行为，以保证企业自身合法合规，但这又会使数据的应用和流动受到一定程度上的限制，对整个数字经济的极速发展造成极其不利的影响。

3、商业秘密保护路径与数据保护更加契合

相比较其它的保护路径，采用商业秘密来保护数据权益时由于避免了讨论相关数据是否具有所有权，具有明显优势，即其保护对象明确，能够规制具体侵害行为；以及其相较于一般条款法律语义更为宽松，因而更容易容忍数据利用行为；并且其非专有性的保护作用能够避免数据垄断，且在企业利益和公共利益的博弈当中能够比较容易保持适度。

对于企业数据保护而言，采取商业秘密保护的路径也有利于促进企业间的合作，促进数据流动、共赢。企业可以事先约定，预判避免事后侵权，减少未来争议。合作之后，企业可以以更低的成本获得更多数据，也可以避免重复数据收集、处理的开支。所以，将数据作为商业秘密进行保护，利用数据以利益最大化的方式进行利用，能够实现企业双赢。

总体来说，对商业秘密利用的保护路径更符合企业实际在数据利用中的需求，相较于《反不正当竞争法》中对一般条款的保护模式有着一定的局限，无法满足数据保护的需求，商业秘密的保护路径更具针对性，可以促进数据开发的投入、数据共享、数据经济的发展。

3. 数据及算法纳入商业秘密保护的分歧

1、数据及算法能否受商业秘密保护存在分歧

数据是算法运行的基础，它们之间存在密切的关系。然而，即使数据在能够获得商业秘密保护的情

况下，也不能简单地认为数据与算法的结合所产生的结果应当享有商业秘密保护，更不能因此推断出算法本身可以受到商业秘密的保护。

关于算法是否纳入商业秘密保护的问题，目前在法律实践和理论界仍存在一定的分歧。一方面，算法作为人工智能和数字经济的核心技术，其研发需要大量的人力、物力和时间投入，具有显著的商业价值，符合《反不正当竞争法》中商业秘密的构成要件。2025 年最高人民法院发布的“智能检索算法”侵害商业秘密案[3]中，法院明确指出，涉案算法通过模型优化和协调，为企业带来竞争优势，且采取了合理保密措施，符合商业秘密的法定条件。然而，另一方面，算法作为商业秘密保护也引发了诸多争议。首先，算法的保密性可能导致“算法黑箱”问题，即算法的运行机制和决策过程不透明，可能引发算法歧视、算法杀熟等社会问题。例如，在“Viacom v. YouTube”[4]案中，Google 以商业秘密为由拒绝公开其算法源代码，法院支持了这一主张，但引发了公众对算法透明度和公平性的质疑。

此外，算法透明与商业秘密保护之间的冲突在公法领域也有所体现。例如，在“State v. Loomis”[5]案中，法院以商业秘密为由驳回了被告要求公开算法的诉求，但这一判决引发了对司法公正性和算法透明度的广泛讨论。为解决上述冲突，有学者建议在算法透明与商业秘密保护之间寻求平衡。一方面，应适度放宽算法的专利保护规则，引导企业更多地采用专利而非商业秘密保护算法；另一方面，可在“掀开最小缝隙”的理论框架下，仅公开算法运行逻辑而非算法本身，同时要求受算法影响者承担初步证明责任[4]。

2、算法满足条件可以纳入商业秘密保护范围

按照我国《反不正当竞争法》的规定，商业秘密指的是尚未为公众所知、具有商业价值，并且权利人已采取相应保密措施加以保护的技术信息和经营信息等商业信息。首先是关于算法性质的认定－算法是否属于商业信息。而根据《最高人民法院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》中的第一条，与技术有关的结构、原材料、成分、配方、材料、样品、样式、植物新品种繁殖材料、工艺、方法或其步骤、算法、数据、计算机程序及其相关文档等信息，可能被法院认定为反不正当竞争法第九条第四款所指的技术信息。此规定明确指出，算法被认为是技术信息。那么算法该类技术信息与其他商业秘密一样，只要在满足三性的前提下，就能纳入商业秘密保护范围。

第一，要纳入商业秘密保护的算法必须是未公开的技术信息，且具备一定的保密性。如果算法涉及的技术信息原本是公开的，但经过重组后形成的技术信息仍未为公众所知，则该重组后的信息也可以视为具有秘密性，进而符合商业秘密的保护条件[5]。

第二，适用商业秘密保护的数据和算法需要采取相应的保密措施，保护数据和算法不为他人普遍知悉或容易获得。数据元素对企业的成长具有重要的价值，而单一数据的作用较为有限。企业通过对大量存储的数据进行分析，可以获得竞争优势和商业价值，因此采取适当的保密措施以确保数据的专有权益显得尤为重要。然而，在实际司法过程中，企业所持有的数据和算法是否能够得到商业秘密的保护依然存在一定的不确定性，这主要受到数据和算法保护条件的限制，从而导致了关于数据要素保护的争议[6]。在嗨狗公司诉汪勇的商业秘密纠纷案件中，企业对实时打赏数据采取了保密措施，但法院未对由这些数据推算出的中奖概率进行明确认定，因此无法确定该信息是否能从公开渠道获得。二审法院排除了中奖概率纳入商业秘密保护的范围，因为中奖概率是通过企业数据和算法推导而来，且这种概率无法独立地进行保密处理，尽管它在企业运营中具有重要商业价值，法院认为无法将其视为可单独保密的信息，因此对是否应当纳入商业秘密保护范围存在争议。

第三，关于价值性的要求，算法技术的商业秘密保护需要考虑其本身能否为企业带来竞争优势。数

[3]广东省深圳市中级人民法院（2021）粤 03 民初 3843 号。
[4]Viacom International Inc., v. YouTube Inc., 253 F.R.D. 256, 259-261 (S.D.N.Y. 2008).
[5]State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016).

据的保护与算法技术的应用密切相关。通过算法对计算机中大量数据的处理，企业能够更好地开发和利用数据，从而创造商业价值并获得竞争优势。在嗨狗公司与汪勇的商业秘密纠纷案中，二审法院排除了将通过算法得出的中奖概率视为商业秘密的可能性，认为对企业有竞争优势的是直播间的实时打赏数据，而算法本身未能满足带来竞争优势的条件，因此不适合纳入商业秘密保护。与此不同的是，在“深圳智搜诉光速蜗牛商业秘密纠纷”案件中，深圳市中级人民法院将算法纳入商业秘密保护范畴，认为算法能够提供更精准的检索服务，为智搜公司带来商业利益和竞争优势，符合商业秘密的构成要求，因此决定将算法作为商业秘密加以保护。

因此，符合商业秘密条件的算法技术可以纳入商业秘密的保护范围。

4. 商业秘密保护范围外的公开数据保护探讨

1、公开数据和信息与秘密性冲突

公开的数据集合不能满足商业秘密的保护要求，主要是因其不具有秘密性、保密性。公布之后的信息，就意味着任何人均可得以访问及获取，自然不符合商业秘密的保护要求。按传统的商业秘密标准，秘密性要求信息不为公众所知或者不易获得，并只需要满足其中一个均可为秘密性。保密性要求权利人主观上要有保密之意，并客观上采取有效的保护措施，所采取的措施也必须是可以被人所感知的。由于数据集合向公众开放，证明权利人并没有保密之意，并且没有采取保密措施，反之他人可以很容易地访问及获取数据，均不能满足商业秘密的秘密性、保密性要素。

但是，公开的数据集合不适用商业秘密保护，但这并不代表着数据集合没有任何财产性价值。由于企业运营平台的过程中产生大量的数据，而企业通过整合数据形成数据集合的过程中耗费了大量的时间和精力。同时，随着数据量的不断积累，企业控制的数据集合也越来越大，价值也越来越高。为了增加平台用户粘性，有可能会将数据和信息内容向公众公开，而数据抓取方也将抓取公开数据的内容传给最终用户以此获取经济利益[7]。如果没有任何限制地允许竞争者抓取这些公开数据内容，再利用这些数据内容获取经济利益，就侵犯了企业在抓取这些数据过程中的劳动投入和资本投入所形成的财产权利。前文所提及的案例中，微播公司将自己信息内容公开后，被创锐公司获取并进行传播，法院认定创锐公司侵犯了微播公司的合法权益，认为创锐公司的行为构成不正当竞争，而法院的这一认定也间接地认可了微播公司对其公开数据内容享有财产权[8]。

最后，对公开数据集合的保护。企业通过收集数据集合付出了大量的劳动成本，如果竞争者都能去自由地抓取这些公开的数据并从中获利，则会侵犯企业的流量经济与财产性权益，因此若企业要求对其实行保护，对于公开数据集合的保护，如果完全采取排他性的方式则会阻碍数据的内容流通、共享，进而导致数据的后续开发与利用，所以公开数据集合的保护是需要平衡企业与社会的利益，保证数据有序流通的前提下，避免数据的垄断和不公平竞争[9]。基于此数据是否纳入商业秘密的范围就有了不确定性，因为商业秘密的保护是有范围的[10]。但从数据集合的角度来说，公开数据并不会对商业秘密对未公开信息的保护造成影响，但对公开的数据集合则需综合分析企业的权益与公共利益。

2、公开数据转为非公开信息纳入商业秘密保护范围

关于公开数据集合的保护问题，本文认为，数据集合仍然可以被商业秘密保护。换言之，数据集合中的内容层信息可以纳入商业秘密保密范围。虽然数据本身具有公开性特征，但这并不影响整个数据集合获得商业秘密的保护。对客体范围的界限，往往忽略数据和信息的区分，容易认为公开的数据不能构成商业秘密，应该根据《反不正当竞争法》当中的一般条款或互联网特殊条款得到统摄[11]。然而，信息与数据本身是两个层次的概念，数据公开，但信息未必公开，数据是信息的载体，载体公开，并不意味着内容也公开，数据和信息是可以分离的。虽然数据的内容有可能是公开的，但是数据集合中的信息仍

然处于机密状态，仍然可以构成商业秘密的条件。通过将公开的数据转变为私密的信息，只要这些信息仍然符合秘密性条件就可以纳入商业秘密的“袋子”里面[12]。

5. 结语

目前，随着数字经济的快速发展，数据作为一种重要的生产要素，其保护问题日益引起广泛关注。在当前的法律框架下，《反不正当竞争法》在数据保护方面发挥着一定的作用，但其适用范围和保护力度仍然存在不足。特别是在面临越来越复杂的数据交易和流通时，现有法律体系显得不够完善，因此，如何从更宏观的角度完善数据的法律保护，成为亟待解决的问题。《反不正当竞争法》主要通过对商业秘密的保护来实现对数据的间接保护，其中第 2 条明确规定了不正当竞争行为，包括窃取、披露、非法使用他人商业秘密等。然而，这一条款在具体适用中仍显得较为抽象，对于数据在不同场景下的法律保护，未能提供清晰明确的框架。在这一背景下，商业秘密保护作为一种更加具体的法律路径，逐渐成为数据保护的重要选择。

商业秘密保护框架下的法律机制相比《反不正当竞争法》具有更强的针对性和可操作性。商业秘密保护不仅涉及企业经营过程中的敏感信息，还包括了数据、技术和其他非公开的资料。因此，商业秘密本身作为一种集多种法律保护手段于一体的概念，它能更好地平衡各方利益，为数据保护提供更全面的法律支持。商业秘密的保护体系可以通过多种方式进行，如民事诉讼中的损害赔偿、行政处罚、刑事责任等，使得数据的泄露和非法使用能够受到多层次的遏制。

自 2019 年《反不正当竞争法》修订以来，针对商业秘密的相关条款进行了多次调整和完善。修订后的法律明确了商业秘密的定义、保护范围以及举证责任的分配等内容，特别是减轻了原告在诉讼中的举证负担，并扩展了保护范围。这一系列修改使得数据保护的法律框架更加清晰和具备实际操作性，同时也为司法实践提供了更为明确的法律依据。法院在认定侵权行为时的标准更加简便，确保了数据保护案件能得到及时处理和公正裁决。

然而，要进一步完善商业秘密保护路径，我国仍需在几个方面进行深入改革。首先，司法解释应当更加明确商业秘密的构成要件，界定数据在不同情境下是否可以被认定为商业秘密。例如，数据的来源、处理方式、使用范围等因素都应在司法解释中明确规范。其次，应进一步完善侵权行为的规制，加强对数据保护过程中的法律责任的追溯，特别是对于数据流通中可能涉及的跨境问题，应当有更加明确的法律指引。

此外，在诉讼过程中，如何确保商业秘密的保密性也应得到更高的重视。在法律诉讼中，涉及商业秘密的数据材料可能会泄露，因此应采取更加严格的保密措施，防止在司法审理过程中对当事人的商业利益造成进一步损害。

总体来说，商业秘密作为数据保护的重要法律路径，具备了较为完善的法律框架和执行机制。我国应进一步细化商业秘密的构成要件、侵权行为的标准以及法律责任，使其能够更好地适应数据产业的发展需求，并通过相关司法解释推动商业秘密保护向更细致、更全面的方向发展。

参考文献

[1] 陈兵. 互联网新型不正当竞争行为审裁理路实证研究[J]. 学术论坛, 2019, 42(5): 26-38.

[2] 魏远山. 我国反不正当竞争法商业数据专条的制度构建——兼评《反不正当竞争法(修订草案征求意见稿)》第 18 条[J]. 环球法律评论, 2023, 45(6): 80-96.

[3] 邓社民, 侯燕玲. 企业数据竞争法保护的现实困境及其出路[J]. 科技与法律(中英文), 2021(5): 1-10.

[4] 程旭鹏. 美国商业秘密法律体系的发展及其对中国的启示[C]//上海市法学会.《上海法学研究》集刊(2021 年第

12 卷 总第 60 卷)——上海市法学会知识产权法研究会文集. 2021: 191-198.
[5] 马一德, 汪婷. 商业秘密“延伸保护”制度构建[J]. 电子知识产权, 2021(9): 43-54.
[6] 张一泓. 商业秘密中的保密措施判断[J]. 成都大学学报(社会科学版), 2020(4): 28-35.
[7] 龙卫球. 数据新型财产权构建及其体系研究[J]. 政法论坛, 2017, 35(4): 63-77.
[8] 张素伦. 论数据集合的反不正当竞争法保护[J]. 河南财经政法大学学报, 2023, 38(5): 57-67.
[9] 冯晓青. 数据财产化及其法律规制的理论阐释与构建[J]. 政法论丛, 2021(4): 81-97.
[10] 刘志鸿. 企业公开数据法律保护范式选择——从赋权论的证成到否定[J]. 中国流通经济, 2022, 36(6): 117-126.
[11] 崔国斌. 公开数据集合法律保护的客体要件[J]. 知识产权, 2022(4): 18-53.
[12] 赵加兵. 论作为数据权益客体的数据集合[J]. 河北法学, 2021, 39(7): 111-127.