

研究论文

亮点:

- 提出"风险分级-归责适配"双维框架
- 知情同意原则的双重审查机制
- 司法裁判标准的统一化方案

*通讯作者邮箱:

13839378573@163.com

英文引用: Wan Jun, 2025. Judicial Relief of Algorithm Infringement on Personal Information Rights. Evidence in Xiangjiang Literary Studies, 1(01), 32-38.

中文引用: 万钧, 2025. 算法侵害个人信息权益行为的司法救济. 香江学刊, 1 (01), 32-38.

稿件处理节点:

接收	2025 年 7 月 5 日
修订	2025 年 7 月 24 日
接受	2025 年 7 月 29 日
发表	2025 年 8 月 3 日

基金资助:

本论文未受到基金资助。

版权:

本作品原创内容可依据《知识共享署名 4.0 国际许可协议》条款使用。任何对本作品的后续分发须标明原作者及作品标题、期刊引用及 DOI 信息。

算法侵害个人信息权益行为的司法救济

万钧

华北水利水电大学法学院, 郑州, 450046

摘要 算法作为数字时代重要的技术工具, 在满足人们对智能化生活需要的同时, 也潜藏着算法侵害的风险。数字时代背景下个人信息的数据化为算法侵害行为提供客观条件, 由于算法侵害行为具有隐蔽性、算法侵害结果具有滞后性、算法侵害方式具有机制性, 以及我国现行算法侵害归责体系的不完备, 导致对算法侵害行为的司法救济存在困难。因此, 应当完善算法侵害的归责体系, 划定算法应用的风险范围, 对高风险领域的算法应用采用严格责任原则, 对高风险领域外的其他一般领域适用过错推定原则, 同时对知情同意原则应采取形式和实质的双重审查, 提高算法侵害的免责门槛, 并通过发布指导案例统一算法侵害的司法裁判标准, 更好的维护数字时代个体的信息权益。

关键词: 算法侵害; 归责原则; 司法救济

Judicial Relief of Algorithm Infringement on Personal Information Rights

WAN Jun

Law School of North China University of Water Resources and Electric Power

Abstract As an important technical tool in the digital age, algorithms not only meet people's needs for intelligent life, but also contain the risk of algorithm infringement. The digitalization of personal information in the context of the digital age provides objective conditions for algorithm violations. Because of the concealment of algorithm violations, the lag of algorithm violations, the mechanism of algorithm violations, and the incompleteness of our current accountability system for algorithm violations, judicial relief for algorithm violations is difficult. Therefore, we should improve the accountability system of algorithm infringement, define the risk scope of algorithm application, adopt strict liability standards for algorithm application in high-risk areas, apply the principle of fault presumption to low-risk areas, and adopt the principle of informed consent to conduct both formal and substantive review, improve the threshold of exemption for algorithm infringement, and unify the judicial standards for algorithm infringement by issuing guidance cases, Better safeguard the information rights and interests of individuals in the digital age.

Keywords: algorithm violation; The principle of liability fixation; judicial remedy

1. 引言

随着数字信息技术的发展,人们的生活逐渐被算法所包围,算法的不合理应用影响了社会秩序,信息泄露、算法歧视、算法共谋等现象频发,给社会公平公正和个人合法权益带来了挑战。如何规制算法、救济被算法侵害的个人权利已成为当前法学研究的热点问题。针对该问题,不同领域的专家和学者采用不同的研究视角,提出多种解决方案,具体可归结为以下三类:一是侧重于算法的事前规制,注重对算法侵害的实施基础即数据信息的合法收集、利用等行为进行约束,以减少数据输入端算法侵害行为的发生;二是从算法程序的规制入手,通过设置专门机构对算法程序进行专业技术性审查和影响评估,以行政监管的方式实现对算法侵害行为风险的预防;三是从技术与法律融合的视角出发,提出确立算法伦理规范,要求算法程序设计者恪守算法伦理准则,将技术伦理与规范嵌入算法决策程序中,实现算法的合理利用。以上方案都是从算法侵害的事前预防与事中监管出发,本文拟从算法侵害的事后救济出发,提出算法应用的场景化归责路径,以期对算法侵害的司法救济提供可行性方案。

2. 问题的提出

随着数字科技的快速发展与广泛应用,人类社会逐渐向数字社会转型,人们的生产生活方式乃至自身的存在形式,都发生了深刻变化。算法作为数字时代重要的技术工具,已深入应用于平台经济领域,成为影响数字经济发展的关键力量。在算法影响下人们的生活也更加智能,如个性化定制算法在平台的运用,使用户只需在搜索框内输入目标商品类别,就可获得符合个人喜好的商品信息。然而,算法应用在满足人们对智能化生活需要的同时,也潜藏着诸多风险。首先,数字时代的个人信息以二进制代码的数据集合形式存在于计算机信息系统中,经过算法分析整合后形成相应的用户画像,此时个人隐私随时可能因为数据集合中某一部分的数据信息的泄露而全部暴露。[1]其次,算法的个性化推荐技术将用户困于算法编织的“信息茧房”,极易造成个体信息获取的同质化与思维习惯的固化,这在无形中侵害着个体的信息选择权。最后,由于算法技术的专业性、不透明性以及利用算法实施侵害行为的隐蔽性,致使传统的侵权归责方式难以认定算法实施主体的侵权责任。[2]

在立法层面,《民法典》第111条仅对保护个人信息作出原则性规定。《个人信息保护法》对《民法典》111条进一步细化,规定了个人信息处理的具体规则、权利义务、职责部门和法律责任,但仍未明确算法侵害行为应如何进行司法归责。由于缺乏统一的法律适用标准,司法机关在算法侵害案件的裁判过程中,可能会存在同案不同判的现象。鉴于此,本文认为有必要根据算法的技术特征构建算法侵害的责任认定体系,完善算法侵害的司法救济路径,实现对个人信息权利的司法保障。

3. 算法侵害行为的成因分析

3.1. 信息数字化为算法侵害行为提供客观条件

数据信息以代码形式存储于计算机系统中,缩小了信息存储所占用的空间,其所存储的信息内容也更加丰富、更具经济价值。此时,平台主体通过算法技术能够挖掘到更多的个人信息,并为其进一步实施算法侵害行为提供必要的条件。

其一,信息的数字化存在,使侵权者以低成本收集海量的个人信息成为可能。数字化信息的存储形式使个人信息基本上只需通过复制、粘贴两步,就可以实现信息的转移与传播。在这一过程中,侵权行为人利用网络爬虫类算法抓取数据,即可非法获得大量的个人数据。

其二,个人隐私的让渡,为侵权者非法利用个人信息提供必要前提。所谓隐私让渡是指政府部门基于公共利益的需要,个人通过放弃部分隐私权以实现维护公共利益的目的。但在一些情况下,个人隐私的让渡也不仅仅局限于维护公共利益,个人为获得更好的网络体验与服务,也会向平台企业主动或被动让渡个人隐私,使隐私暴露于网络生态之下,导致个人隐私权极易被侵害。

其三,算法通过对数据痕迹的挖掘分析所形成的数据集合,使个人逐渐“透明化”,导致个人信息权益极易被侵害。在互联网空间中,痕迹是一切网络活动的必然产物,个人在网络中的行动也会留下痕迹。数字时代的信息一旦流通于互联网中,个人即在很大程度上失去了对信息的控制权,若试图删除这些历史痕迹,就要同时删除多个终端的历史记录。然而对个人来说,却仅仅能够删除自己所控设备中存储的数据信息,无法一并删除网络服务器和

数字运营商保留的数据，这些无法抹除的数字痕迹将个人的以往浏览历史结合在一起，以数据集合的形式呈现人的全貌。此时，个人的一切行为被“透明化”，通过搜寻集合中的部分内容便可追溯到个人的全部信息，使个人时刻处于大数据算法所塑造的全景式监控之中，使个人的信息权益难以得到保障。

3.2. 算法的技术性壁垒使算法侵害行为具有特殊性

算法侵害行为有别于传统的侵权行为。主要有以下特征，一是算法侵害行为具有隐蔽性。互联网平台借助算法为用户提供优质服务，使得用户往往沉浸于享受平台提供服务的喜悦中，放松了对平台可能会利用算法对其信息权益实施侵害行为的警惕，致使平台企业可以在无形之中索取了用户权利。二是算法侵害结果具有滞后性。算法侵害结果不同于以往易于观察的财产损失，可能侵害行为发生于个人信息被侵害之时，但侵害结果却在未来的电信诈骗、敲诈勒索等违法犯罪活动中才能显现出来。同时，算法侵害行为有别于传统的单一主体的侵权模式，算法造成的侵害往往呈现为群体性侵害后果，且由于算法决策的速度更快、效率更高，更容易大范围扩展其损害结果。三是算法侵害方式具有机制性。相较于以往基于人脑决策形成的具有个别性、随机性“黑箱”，算法决策形成的“算法黑箱”则是普遍性的、连续性的。“算法黑箱”是一种自动化决策系统，会根据已设定的程序形成自动化的歧视性或者侵权性决策结果，甚至通过算法的自主学习得到延展升级。[4]换句话说，算法侵害具有一套运行系统，一旦系统中存在算法歧视、侵犯隐私等问题，就会成为常规性动作，产生机制化的侵害后果，对被侵权人造成持续性影响。

3.3. 归责体系的不完备导致对侵权者追责困难

相比于传统的侵害行为，算法侵害行为更加复杂、隐蔽、不透明，导致不仅很难要求算法设计者对算法决策机制做出人们能够理解的解释，更难以依据传统的侵权认定标准追溯到具体的侵害主体。

首先，不同于传统侵权行为与侵权结果间的因果关系认定，算法侵害行为与侵害结果之间的因果关系的断裂，导致认定算法侵害主体的责任承担认定

问题存在困难。然而确定算法侵害行为与侵害结果间的因果关系，是要求算法主体承担责任的前提条件。从本质上来说，算法是由人类设计和操作执行的，复杂的算法可以通过拆分与组合得出相同或者多样的结果，算法主体能够控制最终得出的算法结论[5]。但由于“算法黑箱”的存在，算法主体与被侵权人所遭受的损失之间的关联，通常难以被缺乏相关专业知识的群体所知晓，存在规范评价上的困难。[6]

其次，算法侵害责任主体的主观过错难以认定。个人数据是个人特征在数字层面的反映，算法主体通过对其挖掘到的不同群体的数据进行归类与分析，可能会反映特定人群的区别性特征，但这些区别性特征是数据本身的客观表现，并不能将基于此类数据产生的歧视性侵害结果归因于算法主体的数据挖掘行为。同时，认定算法主体是否未尽注意义务，对侵害结果的发生存在过失责任，也存在实践困境。因为现行法律或司法判例中尚未形成关于算法应用的注意义务标准。[7]

最后，算法侵害主体与被侵权人信息能力的不对等，使二者之间存在证据偏在困境，加剧了证明的难度。在算法侵害案件中，双方当事人在证据掌握上严重不平衡，算法主体拥有强大的算法资源，相比之下个人能力的有限使其难以知晓算法侵害行为的产生是否存在技术上的过错。[8]因此，以加害人过错为前提的普通侵权责任在算法侵害认定中面临适用难题，阻碍了被侵权人正常的私力救济渠道。

4. 算法侵害行为的司法救济路径

4.1. 根据算法应用的风险范围适用不同的归责原则

算法的不当应用可能会引发侵权风险，在一些以自动化方式运行的、具有严重侵害一人或多人合法权益的高风险算法应用领域，一旦算法应用失范，将会对个人和社会秩序产生不可逆冲击，造成大规模的权利侵害。[9]因此，为规范算法活动、引导行为主体合法谨慎运用算法，立法者应当在考虑算法应用行业以及预期用途的基础上，划分算法应用的风险范围，对高风险应用范围的算法主体采取更为严格的证明责任标准，通过严格责任破解“算法黑箱”带来的因果关系断裂与主观过错难以认定等现实难题，对高风险范围外的其他一般领域

的算法应用适用过错推定原则，以确定算法侵害责任的承担主体，实现对算法主体的归责。

4.1.1 算法应用的高风险范围应适用严格责任原则

目前，以风险为基础的分级分类治理理念在国际上得到了广泛应用。例如，欧洲议会为解决人工智能算法民事赔偿责任问题，于2020年通过了《欧洲议会关于人工智能民事赔偿责任制度的决议》（以下简称《AI决议》），明确了人工智能高风险系统的范围，建立了统一的严格责任制度。2021年欧盟委员会发布的《关于制定人工智能统一规则》[10]，与2020年《AI决议》的规定保持一致，基于“以风险为路径”的构想，根据风险等级的等级对人工智能系统进行分类。例如，将监控系统、公正和民主程序等可能对人类基本权利造成影响的人工智能技术确定为高风险范围。被划分为高风险的算法应用，应当依照《AI决议》的规定适用严格责任制度，即在领域内发生算法侵害时，被侵权人无需证明算法主体的主观过错，即可要求算法主体承担责任。

我国《数据安全法》第21条提出要依据数据的重要程度，实行数据分类保护制度。国务院发布《“十四五”数字经济发展规划》进一步提出，要在推动数据分类分级管理的基础上，强化数据安全风险评估、监测预警和应急处置。这意味着未来对于数据的保护，国家提出了更高的要求。在法律和政策的指引下针对互联网领域的算法治理问题，国家互联网信息办公室、工业和信息化部等部门陆续发布《指导意见》《算法推荐规定》等文件，提出了根据算法应用的场景或算法引发的风险等级，采用分级分类的治理方式，进一步明确了在算法推荐领域，将算法推荐服务的内容、数据重要程度等因素作为风险等级划分的重要依据。

本文认为，我国亦可参考欧盟的“风险设定”方式，出台具体的实施细则，将算法应用的场景予以区分，将生物识别、公共管理或服务等可能对个人基本权利及安全造成损害的领域划定为高风险范围，适用严格责任原则。将高风险范围外的领域作为一般领域，适用过错推定原则。考虑到适用严格责任作为算法侵权的归责原则，其并不以算法主体对损害结果是否有过错作为法定责任构成要件，这就增加了算法主体的责任义务。适用严格责任可能

会影响平台企业的创新动力，不利于算法技术的创新发展。因此，应当在司法实践中根据风险范围谨慎适用严格责任，实现被侵权人权益保障与技术创新的动态平衡。

4.1.2 算法应用的一般领域内适用过错推定原则

算法是按照一定规则，解决某一类问题程序或步骤，是算法设计者、运营者人为意志的体现，并非完全客观中立。算法决策结果也是在人为设定的编程框架下产生的，若被侵权人能够证明在该过程中具有引起算法侵害的故意或者过失，传统的过错责任原则就仍能够得以适用。对于算法主体主观过错的认定，有学者认为算法的程序设计部署体现了算法主体的主观意图和价值判断，可将算法程序作为算法侵权行为的归责依据，并通过设置算法备案与评估等制度追溯主观过错。[11]如《数据安全法》第30条对数据的处理设定了基础性规则，就体现了重要数据的处理者应当履行安全风险评估及报告义务，并将风险评估报告报送有关部门备案。国家网信办等九部委发布的《关于加强互联网信息服务算法综合治理的指导意见》（以下简称《指导意见》）提出要建立算法备案制度，主动公布备案情况，接受社会监督。[12]此外，国家网信办等四部门出台《互联网信息服务算法推荐管理规定》（以下简称《算法推荐规定》），细化了算法推荐的规则，其中第16条进一步将推荐算法备案制度具体化，要求算法推荐主体公开算法的基本原理、推荐意图以及主要运行机制。[13]本文认为，这些规定在一定程度上能够解决算法主体主观过错认定困难的问题，也就是说，算法主体应当依照相关规定履行备案义务，对于应当备案而未备案的，就可以推定其存在过错。

虽然算法的不当使用造成个人权利的侵害在某种程度上仍然可以适用传统过错责任原则。但从现实情况来看，证明算法主体主观存在过错需要专业人员的技术支持，个人基于证据偏在、能力不足等客观因素在维权过程中往往难以履行证明责任。本文认为，应当合理分配算法主体与被侵权人的证明责任，适用过错推定原则，实行举证责任倒置，由算法主体就其信息处理行为与侵害结果之间不存在因果关系承担证明责任，以解决证明难题，维护被侵权人合法权益。如《个人信息保护法》第69条明确了处理个人信息，侵害个人信息权益造成损害后果

的,个人信息处理者不能证明自己没有过错时,应当承担损害赔偿等侵权责任。笔者认为,算法实施主体将算法作为侵权工具实施损害个人信息权益的行为,也应当适用于该条所规定的过错推定原则。

一方面,个人与算法主体的互动中,个人始终处于弱势地位,无法通过协商充分表达个人意志,双方在看似平等的条件下,进行着实质不平等的数据服务交换,[14]在此交换过程中,算法主体成为信息处理的直接受益者,个人信息被泄露、滥用造成的风险却由个人承担,这显然是不公平的。[15]另一方面,行为主体利用算法实施信息处理的行为所产生的法定义务,是算法主体承担过错推定责任的实质性基础。[16]算法主体运用技术手段使用户既无法逃离技术的控制,也无法知晓技术程序的运行,[17]更无法监督算法主体是否采用违法手段处理个人信息,算法主体履行证明责任正是对其先行行为,即合法收集处理个人信息行为的印证。在法律范围内,先行行为是产生法定作为义务的正当事由,也是追究特定义务人承担不作为责任的重要依据。《个人信息保护法》第5条规定信息处理者在处理个人信息时,应当秉持合法正当必要和诚信原则,据此规定,算法主体处理个人信息过程中,也应当合法正当必要收集处理个人信息,并就自己没有违法行为承担证明责任,这种证明责任本身是算法主体负有的法定作为义务。因此,只要算法主体处理个人信息行为的违法性得以确认,且算法主体不能证明自己没有过错,就应当推定算法主体存在过错。

4.2. 提高算法侵害的免责门槛

知情同意原则是算法主体收集、处理个人信息需要遵循的基本原则,同时也是权利主体实现信息处分自由的基本前提。[18]算法主体基于用户的同意,能够处理用户个人信息。在法律层面,《民法典》第1036条规定,在自然人或其监护人同意的范围内处理个人信息的,信息处理者不承担民事责任,由此可见自然人或其监护人的同意是侵权的法定免责事由。[19]但在实际操作中,面对信息处理者所提供的知情同意格式条款,用户仅有两种选择,或是全部接受条款内容,或是全部拒绝并退出交易。这种方式看似便于操作,但会使知情同意原则流于形式,使形式告知与实质同意之间形成看不见的鸿沟。[20]因此,对于以知情同意为免责事由的算法侵害行为,应当在坚持知情同意内核的基础

上,通过对知情同意进行双重审查,提高免责门槛,实现对被侵权人的权利保护。

4.2.1 初步审查信息收集的形式合法性

首先,法官应审查算法主体提供的告知界面是否易得、告知文字是否简洁易懂。当专业化的法律术语被大量应用于日常出现的动辄数页的告知同意书时,普通人一般没有能力或耐心全部阅读并真正理解这些文字内容,亦无法预知同意授权会给他们带来何种风险。[21]因此,为保证用户在完全知悉风险的基础上做出同意授权选择,应当将普通人能够读懂作为审查知情同意书是否通俗易懂的标准。

其次,个人敏感信息与人格尊严紧密相关,针对不同敏感等级的信息设置不同层级的限制收集措施,能够在一定程度上保护个人信息权利。法官应当审查算法主体是否依据个人信息与人格尊严的紧密程度划分信息的敏感等级,采用不同的分类收集措施。敏感分级制度应秉持宽严有序的理念,通过设定诸如明示同意、禁止收集、书面授权、一般告知等不同程度的限制措施,实现对个人信息多样化、差异化的保护。例如,将部分生物特征类信息设置为高度敏感不得收集的信息,算法主体一旦收集此类信息,其行为违法性即得以确认。

最后,审查算法主体是否采用区分授权方式,通过区分核心与非核心功能,赋予用户就个别条款分别授权的权利。区分授权的目的在于解决以格式合同和一揽子授权模式限制用户自主权的难题,允许用户根据条款内容分别多次协商签约,解决用户所面临的不授权即退出的困境。[22]但当前对于区分授权机制的建立仍有待完善,比如对于核心功能与非核心功能的区分标准尚未明确,算法主体可能会利用该弱点,以核心功能之名收集非核心功能的信息。因此,司法机关可通过出台司法解释或发布指导案例的方式,在司法实践中积累形成具体区分标准,为司法裁判提供参考。

4.2.2 实质性审查同意的内容

知情同意是法律意义上的行动,但法律意义上的行动并非物理性的举动,因为“纯粹客观的外在举动不能取代主观的内心意愿”[23],这就要求在知情同意形式合法的基础上,法官还需要对同意内容进行实质性审查。

其一,审查同意信息处理的告知场景是否与实际应用场景一致。用户的授权行为可能会产生信息

泄露的风险,事先将信息应用场景告知用户能够使其合理预测风险程度,若信息实际应用场景发生变化,个人却无法预知实际场景中存在何种风险,那么此前的授权同意已然失效,实际场景中的信息处理行为就丧失合法性基础。

其二,审查信息应用场景变更时是否进行风险评估。一般而言,特定场景下个人信息所面临的风险是相对稳定的,在相同或高度类似的场景下对同一用户信息的利用并未增加其风险负担,无需再次授权[24]。但若信息处理者超出信息收集的原始场景再次处理个人信息,则可能产生信息的不合理利用行为,应当对再次处理行为予以风险评估,评估后具有较高的风险的,需要向用户说明具体风险类别,由用户决定是否再次授权。

其三,审查信息处理者是否告知用户享有撤回同意权,是否为用户提供便捷的撤回方式。《个人信息保护法》第15条规定了对于以个人同意授权为合法性基础的信息处理行为,个人有权撤回同意,信息处理者应当采用便捷的方式保证用户行使撤回权。同意撤回权作为信息广义“退出”的方式之一,能够有效破解告知同意形式化的困境,[25]避免在缺乏认知和信息弱势的情况下的“不真实授权”同意给个人带来的过重负担,[26]有助于实质同意的实现。

4.3 统一司法裁判尺度

案例指导制度作为我国法律适用的一种重要方式,通过个案中的价值判断、裁判规则等为法官裁判同类案件提供方法论上的指引,使当事人对案件的裁判结果形成合理预期,实现同案同判的司法目标。由于算法侵害场景化归责的最大缺陷在于缺乏统一的判断标准,而案例指导制度能够缓解场景标准的不确定性问题,通过个案的参照适用形成统一的裁判规则。虽然最高人民法院尚未公布算法侵害类指导案例,但当前已有一些地区的法院将与算法相关的案件作为典型案例予以公布,为其他各地区法院提供了审判参考。

如淘宝(中国)软件有限公司诉安徽美景信息科技有限公司不正当竞争纠纷案中,[27]针对微信数据权益归属以及使用算法抓取数据抓取行为正当性的认定问题,法院确立了数据分类保护原则,并提出了利用算法抓取数据的正当性认定标准与方法,为此类案件的审理提供了可借鉴的司法例证。又如

天津顾某诉兰州物业公司个人信息保护纠纷一案中,[28]天津市第一中级人民法院在终审判决中适用过错推定原则,认定物业公司在使用人脸识别算法时存在主观过错,充分保障了个人的同意撤回权,为涉及人脸识别算法类案件的审理提供了新思路。

算法侵害行为以算法技术为依托,通过程序代码的设计、应用才能够得以实施,因此个案中实际应用的算法程序就成为判定案件相似性所必须要审查的因素。以造成歧视性结果的算法程序的审查为例,不同主体设计的算法程序代码排列组合方式有所区别,歧视性结果的产生原因也具有多样性。[29]因此,不管基于何种程序或何种原因,法官在审理类似案件时,只要能够认定算法程序存在歧视性意图,都可以作为同类案件进行处理。

5. 结论

网络法时代,人们逐渐发现并用法律理论发展证明“网络并非法外之地”。人工智能算法时代,人们也将证明算法并非责任的真空地带。当前针对算法技术的程序性规则为规制算法侵害提供了重要的制度性工具,但难以实现对算法侵害的归责与救济。算法的技术特征带来的归责难题并不意味着算法侵害行为可以免受法律制裁,应检验传统责任理论在算法应用场景中的适用性,根据算法技术特征构建算法侵害责任框架,依照算法应用的风险程度适用归责原则,对高风险范围适用严格责任原则,其他一般领域适用过错推定原则。同时为避免算法应用主体以形式化的知情同意作为侵权行为的抗辩事由,应通过对知情同意进行双重审查提高知情同意规则的免责门槛。此外,考虑到算法侵害的场景化归责带来的司法适用标准不一的问题,最高人民法院可以发布指导性案例统一司法裁判的尺度,为法官裁判案件提供指引,实现对个人信息权益的司法救济。

参考文献

- [1] 杨学科.第四代人权论:数字时代的数字权利总纲[J].山东科技大学学报(社会科学版),2022,(2):10-22.
- [2] 参见王莹.算法侵害责任框架刍议[J].中国法学,2022,(3):165-184.
- [3] 郝喜.数字化“圆形监狱”:算法监控的规训与惩罚[J].昆明理工大学学报(社会科学版),2021,(6):39-45.
- [4] 马长山.智慧社会背景下的“第四代人权”及其保障[J].中国法学,2019,(5):5-24.
- [5] 孙建丽.算法自动化决策风险的法律规制研究[J].法治研究,2019,(4):108-117.

- [6] 参见陈吉栋. 个人信息的侵权救济[J]. 交大法学, 2019(4): 40-53.
- [7] 参见王莹. 算法侵害责任框架刍议[J]. 中国法学, 2022, (3): 165-184.
- [8] 证据偏在是指大量能够证明案件事实的证据被一方当事人所控制, 且往往是加害当事人一方。参见蒋丽华. 无过错归责原则: 个人信息侵权损害赔偿的应然走向[J]. 财经法学, 2022, (1): 32-44.
- [9] 林涸民. 自动决策算法的风险识别与区分规制[J]. 比较法研究, 2022, (2): 188-200.
- [10] 参见王伟洁, 邓攀科, 吕志远. 欧盟 2021 年《人工智能法》研究[J]. 信息安全研究, 2022, 8(2): 117-121.
- [11] 张凌寒. 网络平台监管的算法问责制构建[J]. 东方法学, 2021, (3): 22-40.
- [12] 参见国家互联网信息办公室、中央宣传部、教育部等关于印发《关于加强互联网信息服务算法综合治理的指导意见》的通知, 国信办发〔2021〕7 号。
- [13] 参见国家互联网信息办公室、中华人民共和国工业和信息化部、中华人民共和国公安部、国家市场监督管理总局令第 9 号, 《互联网信息服务算法推荐管理规定》。
- [14] 李齐. 数字时代的权力生产与政府责任[J]. 中国行政管理, 2019, (11): 75-81.
- [15] 周汉华. 探索激励相容的个人数据治理之道[J]. 法学研究, 2018, (2): 3-23.
- [16] 王道发. 个人信息处理者过错推定责任研究[J]. 中国法学, 2022, (5): 103-121.
- [17] 马治国, 占妮. 数字社会背景下超级平台私权力的法律规制[J]. 北方工业大学学报(社会科学版), 2022, (6): 1-16.
- [18] 赵龙. 个人信息权法益确证及场景化实践归责[J]. 北京理工大学学报(社会科学版), 2021, (5): 169-178.
- [19] 衣俊霖. 论个人信息保护中知情同意的边界——以规则与原则的区分为切入点[J]. 东方法学, 2022, (3): 55-71.
- [20] 程啸. 论个人信息处理中的个人同意[J]. 环球法律评论, 2021, (6): 40-55.
- [21] 郭春镇. 对“数据治理”的治理——从“文明码”治理现象谈起[J]. 法律科学(西北政法大学学报), 2021, (1): 58-70.
- [22] 林凯, 张建肖. 知情同意权的功能失灵与应对——兼评《数据安全管理办法(征求意见稿)》相关规定[J]. 中国应用法学, 2020, (2): 162-186.
- [23] 袁国何. 诈骗罪中的处分意识: 必要性及判例[J]. 法学研究, 2021, (3): 133-151.
- [24] 邹晓玫, 杜静. 大数据环境下个人信息利用之授权模式研究——重要性基础上的风险评估路径探索[J]. 情报理论与实践, 2020(3): 37-43.
- [25] 万方. 个人信息处理中的“同意”与“同意撤回”[J]. 中国法学, 2021(1): 167-188.
- [26] 叶敏, 玛丽亚木·艾斯凯尔. 论个人信息同意撤回权的现实困境与完善建议[J]. 财贸研究, 2021(11): 62-71.
- [27] 杭州市中级人民法院(2018)浙 01 民终 7312 号民事判决书。
- [28] 新京报. 天津一起人脸识别案胜诉, 小区以刷脸作为唯一通行方式被判违法[EB/OL]. (2022-06-05) [2022-11-]
- [29] 算法歧视性决策结果产生原因可能是算法设计者将个人偏见嵌入算法程序, 也可能是算法使用者输入了带有歧视性的数据, 还可能产生于算法的自我学习或者其他环节中。参见张典. 反算法歧视: 理论反思与制度构建[J]. 华中科技大学学报(社会科学版), 2020, 34(5): 60-71.