

# 个人行踪信息民法保护的困境与出路

朱红梅

贵州大学法学院, 贵州 贵阳

收稿日期: 2023年5月17日; 录用日期: 2023年6月5日; 发布日期: 2023年7月21日

## 摘要

个人行踪信息是敏感个人信息, 我国法律并无对其内涵的明确界定, 数字经济时代, 行踪信息的价值得以凸显, 行踪信息兼具个人信息与个人隐私的双重属性。其具有高度的敏感性、实时动态性和强法益关联性的独特性。目前行踪信息的保护面临知情同意原则被虚化、最小比例原则被逾越、数字经济驱动及公共安全优先冲突以及行踪信息范围认定之难的现实困境。对此应当合理界定行踪信息, 肯定行踪信息的法律地位; 优化知情同意原则, 强化最小必要原则; 根据个人行踪信息的类型和敏感度对其进行分类分级保护, 以实现数字时代个人行踪信息的保护和利用的利益平衡。

## 关键词

行踪信息, 隐私权, 最小必要原则, 分类保护

# The Dilemma and Way out of the Protection of Personal Whereabouts Information in Civil Law

Hongmei Zhu

Law School, Guizhou University, Guiyang Guizhou

Received: May 17<sup>th</sup>, 2023; accepted: Jun. 5<sup>th</sup>, 2023; published: Jul. 21<sup>st</sup>, 2023

## Abstract

Personal whereabouts information is sensitive personal information, and our law does not have a clear definition of its connotation. In the digital economy era, the value of the whereabouts information is highlighted, and the whereabouts information has the dual attributes of personal information and personal privacy. It has the characteristics of high sensitivity, real-time dynamics and

strong legal-interest relevance. At present, the protection of whereabouts information is faced with the realistic dilemma that the principle of informed consent is blurred, the principle of minimum proportion is exceeded, the digital economy is driven by the conflict of public security priority, and the scope of whereabouts information is difficult to identify. In this regard, we should reasonably define the whereabouts information and affirm the legal status of the whereabouts information. Optimize the principle of informed consent and strengthen the principle of least necessary; according to the type and sensitivity of personal whereabouts information, it is classified and protected to achieve the balance of interests between the protection and utilization of personal whereabouts information in the digital age.

## Keywords

Whereabouts Information, Privacy Right, Principle of Least Necessity, Classified Protection

Copyright © 2023 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

大数据时代背景下,信息技术的发展,个人信息保护成为了数字时代社会治理的新课题。数字时代,基于位置的服务(LBS)应用更加广泛,个人在享受 LBS 提供的便利服务的同时也面临着因位置、行踪信息泄露侵扰个人隐私的问题。《中华人民共和国民法典》(以下简称《民法典》)第 1034 条将行踪信息列为个人信息纳入民法的保护范围,2021 年 11 月 1 日正式施行的《个人信息保护法》第 28 条将行踪信息作为敏感个人信息加以保护。个人行踪信息具有个人隐私与个人信息的双重属性。目前民法领域对个人行踪信息的保护已有一定的研究,学者的研究集中于行踪信息的内涵、对其进行保护的正当性和必要性的论证以及行踪信息保护面临的困境等几方面。已有研究对于个人行踪信息的保护具有很大的借鉴意义,但对行踪信息的特殊性、类型以及具体的民法保护措施等方面还有待深入研究,在行踪信息日益受到重视的背景下本文以个人行踪信息为研究对象,在明晰个人行踪信息的内涵及其特殊性基础上,肯定对个人行踪信息进行保护的法律意义,并就当下个人行踪信息保护面临的困境进行分析,以完善个人行踪信息民法保护的进路。

## 2. 个人行踪信息的界定及其特殊性

行踪信息作为重要的个人信息,是数字经济时代重要的生产要素,实现对个人行踪信息的保护需要对行踪信息的内涵有科学的界定、对其特殊性有充分的认识。

### 2.1. 个人行踪信息之界定

行踪信息是敏感个人信息,关于行踪信息的内涵和外延理论界众说纷纭,司法实践中并无统一的裁判认定标准,存在认定不一的问题。从学理上看:概括来说行踪信息是自然人的静态停居信息与动态移动轨迹的结合[1]。在数字时代行踪信息是以电子方式或者其他方式记录的个人信息,该信息会反映出一个人以何种交通方式,在什么时间去过哪些地方,在哪里停留过多长时间等。行踪信息既包括自然人在特定时间的动态地理位置,也包括个人空间位置移动而形成的轨迹[2]。其具有地理空间性、实时动态性,本质上仍是实时地理位置[3]。

实时性是行踪信息的重要特性,在此存在一个颇具争议的话题,即个人网络浏览记录及IP地址能否纳入行踪信息的保护范围?对此持肯定态度的学者认为网络活动轨迹能通过IP地址定位特定的个人位置;在大数据时代通过对个人网络空间留下的“活动轨迹”的分析,可以反映出个人的兴趣爱好、性格特征、消费习惯等,这会将真实世界中的实体人以镜像形式投射到网络空间,形成了所谓的数字化身份、数字化人格,无论从形式还是实质层面我们都无法再将其排斥于法律保护范围之内<sup>1</sup>。持否定态度的学者认为以Cookie为例,网络浏览记录和实在的地理位置信息有着实质区别,虽然浏览记录包含了个人设备IP地址,但是其仍难以精准实时定位特定的个人,敏感性程度并不高。其次,法律规定了网络服务提供者收集个人信息,根据不同的目的和要求,有利用技术对个人信息“去世别化”的义务性的规定,因此收集的个人浏览记录经去识别化后不能或者难以确定到个人。<sup>2</sup>对此,本文认为对于网络浏览记录能否被认定为“行踪轨迹信息”不能采取“一刀切”的认定方式,而应当结合具体的情景和信息,看该信息是否具备“识别性”以及网络浏览记录的敏感性等对IP位置信息进行区分,以确定其是否符合行踪信息的特性,从而考虑是否加以保护,对此后文会进行详细论述。另有研究者提出借鉴国外立法,采取“定义+列举+排除”的界定方式,结合“时间”“物理位置”“技术手段”“直接识别”四要素界定行踪轨迹信息。认为行踪信息是利用定位技术获取的能够识别个人过去或者当前时间所在的物理位置的信息,不包括需结合其他个人信息才可识别个人位置的信息[4]。

综上,本文认为对行踪信息的界定应当考虑到行踪信息作为敏感个人信息的敏感性,其内涵不得随意扩张,应当认识到位置信息与行踪轨迹信息存在差异,与静态的位置信息相比,行踪信息更为强调动态的过程[1]。简而言之行踪信息是具备识别性的个人实时位置信息和移动轨迹。

## 2.2. 个人行踪信息的特殊性

个人信息的核心特征是“可识别性”,行踪信息作为敏感个人信息在具备一般个人信息共性的同时有其特殊性,其特殊性是法律对其进行区别保护的前提。

### 2.2.1. 行踪信息具备高度敏感性

《个人信息保护法》第28条规定,敏感信息是指一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产遭受危害。此法律规定语境下的“敏感”是指造成自然人危害后果的容易性和严重性。行踪信息作为一种敏感个人信息,其具有的高度敏感性主要体现在行踪信息的隐私性和人身依附性上。具体而言可以从行踪信息被泄露造成的危害中得以窥见。行踪信息泄露可导致以下后果:一是个人人格尊严容易遭受侵害。我国法律对人格尊严的保护体现在明确的法律规范中,《宪法》第38条,《民法典》第109条、第990条第2款都列明对人格尊严的法律保护。个人行踪信息尤其是具有私密性的行踪信息诸如出入同型恋酒吧、宗教场所、看望精神科医生等私密社交活动信息等被非法泄露极有可能侵害个人的人格尊严和隐私权。二是自然人的人身、财产安全受到危害。行踪信息与个人日常生活密切相关,其真实的反映着信息主体的日常活动轨迹,承载着信息主体的隐私等人格利益[5]。可以说行踪信息具有极强的人身依附性。通过收集一个人的行踪信息不仅可以轻易地知道该自然人在什么时间去过什么地点还可以进一步通过行踪信息分析出行为人的习惯、爱好、工作等信息,因此不法分子就其所掌握的信息实施相应的犯罪行为就变得轻而易举。笔者在梳理涉及个人行踪信息侵权的案例中发现,国内<sup>1</sup>认为网络行踪轨迹信息可以加以法律保护主要在以下学者的研究中可以窥见:参见:李延舜《位置何以成为隐私?——大数据时代位置信息的法律保护》,载《法律科学(西北政法学报)》2021年第2期;高完成:《大数据传播时代个人行踪信息的法律保护》,载《青年记者》2020年第3期;武东方《“行踪轨迹信息”刑法差异化保护思考》,载《商丘职业技术学院学报》2021年第5期;张璐:《个人网络活动踪迹信息保护研究——兼评中国Cookie隐私权纠纷第一案》,载《河北法学》2019年第5期。

<sup>2</sup>不赞成将网络浏览记录等轻易定义为个人行踪信息加以法律保护的观点参见:文进宝,肖冬梅:《我国行踪轨迹信息保护范围认定困境与出路》,载《图书馆论坛》2022年第07期55-64页。

外都存在因个人行踪信息的泄露，被不法分子知悉利用而导致个人被杀害的案例。典型如新冠肺炎疫情期间个人信息被非法收集、信息权益遭受侵害的案件频发，一些案件中因个人信息的泄露导致个人沦为诈骗犯的“重点关注对象”，因个人行踪信息的不当披露导致个人的隐私泄露，引发“受害主体”的社会性死亡等严重的后果。

### 2.2.2. 行踪信息具备实时动态性

实时动态性是行踪信息区别于个人的姓名、身份、基因、健康信息等其他个人信息的重要特征，行踪信息具有明显的时间和空间特性。行踪信息能够记录个人在某个时间段内的活动轨迹，这些时间可能是准确的时间点、日期或者时间段；也记录个人到过的地点、包括住所、工作地点、商店、餐厅等；记录了个人在不同时间出行的交通方式，如乘坐的具体交通工具；还能实时记录个人的旅游活动，个人旅行的目的地、入住的旅馆、旅游的景点等；还能记录个人的消费行为，记录个人在餐厅、商场等场所的消费行为以及参加的社交活动，如与朋友聚餐、婚礼、生日派对等。互联网时代，个人行踪信息还能记录个人的在线活动，记录个人在互联网上的活动，如浏览网页、使用社交媒体、发送电子邮件等。通过对这些行踪信息的分析能轻而易举的得出一个人的行为习惯、能够为商业营销、社会研究、个人健康、刑事侦查等领域的相关组织、机构提供有用的信息。

### 2.2.3. 行踪信息的强法益关联性

提到“法益”一词更多时候我们是在刑法的语境下来讨论，在此提到行踪信息的强法益关联性与行踪信息的重要性和受到刑法的重点保护是难以分开的。在刑法规定的侵犯公民个人信息罪中，行踪信息关乎公民人身、财产安全，同时还会涉及到公共安全。刑法对侵犯个人行踪信息的行为设立了较低的入罪门槛。行踪信息的强法益关联性和行踪信息的价值密切相关。行踪信息在维护公共安全、解决刑事案件和民事纠纷、保障人民生命财产安全等多个方面具有重要的价值意义，其能帮助解决刑事案件和民事纠纷，可以为刑事案件和民事纠纷的调查提供重要依据。例如，一些案件中，被害人或嫌犯的行踪信息可以为案件的调查提供关键证据；能帮助保障公共安全的行踪信息可以用于维护公共安全。例如，警方可以通过监控来监视公共场所，以及特殊事件和场合，如体育比赛、大型集会等，来避免和预防恐怖袭击和其他犯罪事件的发生；还能帮助提高社会治安水平，其可以为公共安全和社会治安的管理提供数据支持。例如，社区警务可以通过监控公共场所，掌握人员流动情况，及时发现和处理安全隐患，提高社会治安水平。行踪信息的强法益关联性还体现在其具有复合法益性上，法益复合性是指行踪信息易于和其他个人信息发生融合而体现出信息复合的特性，诸如个人的消费记录、出入寺庙、同性恋酒吧等特定场所的轨迹，不仅可以知道一个人的活动轨迹还能推测出个人的财产状况、宗教信仰以及性取向等<sup>[6]</sup>。具有重要价值作用的个人行踪信息一旦泄露、被滥用将会使个人的人身财产，甚至公共安全遭受巨大的危险。

## 3. 个人行踪信息民法保护的实证分析

### 3.1. 个人行踪信息保护的立法考察

我国目前关于行踪轨迹信息规定的法律有两部：《民法典》和《个人信息保护法》，有 7 个司法解释涉及个人行踪轨迹信息的规定，12 部部门规章涉及个人行踪信息方面的规定。我国个人行踪信息相较于姓名、身份等其他一般个人信息而言纳入法律明确保护的时间较晚。2017 年发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(以下简称《解释》)将“行踪轨迹信息”列为公民个人信息的重要类型予以刑法的保护，这是我国法律首次规定对行踪信息的保护。2021 年颁布的《民法典》第

1034 条<sup>3</sup>第 2 款将个人行踪信息列为个人信息，同年 11 月 1 日施行的《个人信息保护法》第 28 条<sup>4</sup>将个人行踪信息作为敏感个人信息予以保护，行踪信息在我国已经得到立法的重视。

目前，世界上各国和地区都在加强对个人行踪信息的保护。欧盟对个人信息的保护较为全面，欧盟于 2018 年 5 月 25 日正式实施了《通用数据保护条例》(GDPR)，该条例规定了对于任何与欧盟公民相关的个人数据保护要求，包括位置数据和轨迹信息。根据该条例，所有处理个人行踪信息的企业都必须取得用户明确的同意，并遵守相关的安全和保密规定。美国目前没有像欧盟 GDPR 那样的一部适用于所有州的全国性隐私保护法律。但是，一些州已经出台了个人隐私保护法，如加利福尼亚州的《加利福尼亚消费者隐私法》(CCPA)，这是美国的第一个隐私法案，该法规定了对于个人行踪信息的保护要求，该法将“精准地理位置”数据纳入敏感个人信息，并规定精准地理位置的含义。<sup>5</sup>日本于 2020 年实施了新的个人信息保护法案，该法案将位置数据、设备识别码等信息纳入到受保护的个人信息范围内，并规定了处理个人行踪信息的企业需要事先告知用户数据的使用目的，并取得明确的同意。韩国于 2020 年实施了新的个人信息保护法，该法规定了对于个人行踪信息的保护要求，要求处理个人行踪信息的企业需要尽力保障个人行踪信息的安全，并采取适当的技术和组织措施来保护个人行踪信息。

总的来说，国际上越来越多的国家和地区开始关注并制定法律来保护个人行踪信息涉及的隐私权。尽管各个国家的个人隐私保护法律存在差异，但都强调了对于个人行踪信息的保护，尤其是对于敏感性的个人行踪信息的保护，这有助于推动全球个人隐私保护的发展。

### 3.2. 个人行踪信息侵权形态之分析

为分析司法实践中个人行踪信息的侵权行为类型和行踪信息的司法保护现状，笔者以“行踪信息”和“行踪轨迹信息”在中国裁判文书网和北大法宝数据库中进行检索，截止 2023 年 3 月 11 日共检索到 784 个案例，去除重复和无关的文书后共筛选到 50 余个有效的案例，作为对行踪信息侵权形态的主要案例支撑。通过整理分析检索的案例发现司法实践中对个人行踪信息的侵权形态主要有以下三类：

一是盗取个人行踪信息，主要是侵权人通过非法手段获取他人的行踪信息，如通过雇佣“私家侦探”进行跟踪拍摄、通过黑客攻击、假冒网站等方式盗取他人的位置信息、行踪轨迹信息等。这些情节根据严重程度的不同会涉及刑法规定的侵犯公民个人信息罪，有的没有达到刑法的入罪标准需要民法对行踪信息进行保护，主要体现在企业、平台等信息处理者没有遵循个人信息处理的原则和规则，尤其是《个人信息保护法》所规定的对敏感个人信息的“明确告知”和“特定目的”的处理规则，过度收集个人行踪信息构成侵权，典型的案例是中国人脸识别第一案<sup>6</sup>。该案中动物园在未明确告知原告并取得原告同意的情况下就将入园的方式由指纹改为人脸识别，最终原告诉至法院请求删除其录入动物园的相关个人信息。

二是泄露行踪信息，指未经授权而公开、泄露他人的行踪信息，如未经本人同意将个人位置信息公开在社交媒体上、将他人移动轨迹泄露给第三方等。泄露个人行踪信息的案例在新冠疫情防控期间屡见不鲜。一个具有警示意义案例是“成都确诊女孩遭网暴案”<sup>7</sup>。2020 年 12 月 8 日，成都卫健委通报了一名 20 岁女子赵某确诊新冠肺炎的消息。当天上午，涉及赵某的姓名、照片、身份证号码、家庭住址、行

<sup>3</sup> 参见《中华人民共和国民法典》第 1034 条第 2 款：第 1034 条 自然人的个人信息受法律保护。

个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

<sup>4</sup> 《中华人民共和国个人信息保护法》第 28 条：敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

<sup>5</sup> The California Consumer Privacy Act [EB/OL]. [2021-12-02]. <https://www.oag.ca.gov/privacy/ccpa>.

<sup>6</sup> 参见浙江省杭州市富阳区人民法院(2019)浙 0111 民初 6971 号民事判决书。

<sup>7</sup> 参见《光明日报》，《成都确诊女孩，凭什么被“网暴”？》2020 年 12 月 9 日。 [https://www.thepaper.cn/newsDetail\\_forward\\_10327360](https://www.thepaper.cn/newsDetail_forward_10327360)

踪信息等个人隐私的信息在多个平台上被转发。与此同时,赵某遭致网友无端的谩骂和指责,指责其一晚上转场多个酒吧,是个行为不端之人。其个人信息疑似被泄露。赵某不过是一个不幸感染了新冠肺炎的患者却因为其行踪信息泄露遭到了网友的无端谩骂和指责。后其姓名、照片、家人的信息完全暴露于网络环境中,其隐私遭泄露,导致其人格尊严被侵害,引起受害人“社会性死亡”。更为严重的有收集泄露个人行踪信息用于违法犯罪活动,诸如王某、邹某组织领导参加黑社会等多起犯罪案<sup>8</sup>中,多名被告人利用警方内部人员向其提供的被害人的行踪信息,对多个被害人实施非法催收、威胁恐吓、故意伤害等违法犯罪行为,被告利用被害人的上网信息找到被害人并实施了侵害,法院认为被害人的上网信息能够反应其身份及位置属于个人行踪信息,理应得到法律的保护。泄露行踪信息的案例不胜枚举,在国际上还有诸多因行踪信息泄露引发广泛关注的案例,诸如 2018 年处于全球社交媒体领军地位的美国 Facebook 数据泄露事件引发国际社会广泛关注和热议[7]。

三是滥用行踪信息,主要体现在将获取到的他人行踪信息用于不正当用途,如利用他人位置信息进行商业广告推销、非法跟踪等。在互联网时代各大平台应用商收集定位个人的位置、行踪信息再通过算法分析对个人进行商业广告推送的行为已经成为了一种普遍现象。早在 2015 年就有平台收集个人的行踪轨迹信息进行广告推送个人提起隐私权侵权之诉的案例,这是我国 Cookie 隐私第一案,基本案情是原告在百度中搜索了“减肥”这一检索词,在后续的浏览中发现百度收集了其网络轨迹数据并提供了个性化的推荐服务,原告朱某主张百度公司未经其同意过度收集利用其网络轨迹信息侵害了其隐私权,该案一审法院支持了原告的诉讼请求,一审法院认为被告在原告不知情未获得授权同意的情况下用 Cookie 技术收集原告信息并进行个性化推荐服务等商业利用,侵害了原告的隐私权<sup>9</sup>。二审法院的意见与一审截然不同,二审法院审理认为:被告的行为不构成侵权,理由是:被告未对外公布泄露原告个人信息且未强制网络用户必须接受个性化的推荐服务,未对原告的生活安宁产生实质影响<sup>10</sup>。时隔几年,信息技术的发展,对个人行踪信息的收集利用更加普遍化,诸如网络浏览记录的保护亦引起了人们的重视,此案对个人行踪信息保护的问题值得我们深思。

以上是目前实践中存在的侵害个人行踪信息的典型形态,既包括以涉嫌公民个人信息罪的严重行为,也有违反个人信息保护法等民法的侵权行为。

### 3.3. 个人行踪信息司法保护的评析

总的来说,虽然《民法典》、《个人信息保护法》等民事法律规定已经规定对个人行踪信息的保护,但是目前司法实践中民法对个人行踪信息的保护仍存在的问题,一方面,我国的《民法典》确立了个人隐私的保护原则,规定了个人信息的保护标准和承担法律责任的规则,从理论上保障了行踪信息的隐私权。但是另一方面,在司法实践中,由于涉案需要,法院和公安机关等机构对个人行踪信息的获取和使用缺乏有效的监管和限制,同时对行踪信息的保护缺乏细化的法律规定和监管措施,因此执法难度大是对行踪信息进行保护存在的一大难题,另外法院在案件的裁判中总是会进行利益权衡,对于涉及个人行踪信息侵害不大的情况,法院多数做出不予支持当事人请求的裁判,典型如“我国人脸识别第一案”和“我国 Cookie 隐私第一案”,原告主张其行踪轨迹被侵害的主张均未得到法院的支持,法院支持行踪轨迹信息的保护请求的情形多存在于有视频监控记录收集个人行踪信息的案例中<sup>11</sup>。

另外我们可以看到,涉及侵犯行踪信息侵权案例中当事人多是以侵犯了隐私权主张权利救济,救济

<sup>8</sup> 参见湖南省长沙县人民法院刑事判决书(2019)湘 0121 刑初 157 号。

<sup>9</sup> 江苏省南京市鼓楼区人民法院民事判决书(2013)鼓民初字第 3031 号。

<sup>10</sup> 江苏省南京市中级人民法院(2014)宁民终字第 5028 号。

<sup>11</sup> 参见北京市第三中级人民法院发布 2021 年度十大涉民生侵权纠纷典型案例:王某与西某隐私权、个人信息保护纠纷案、江苏省无锡市中级人民法院民事判决书(2019)苏 02 民终 5307 号。

的方式主要有停止侵害、排除妨害、进行损害赔偿等侵权救济方式。对于涉及侵犯个人隐私权的情形法院对权利人的请求给予支持,但是单纯的涉及行踪信息权益的请求法院对权益侵害程度的要求更高。

最后,司法实践中普遍存在一个问题,即各法院对行踪信息的认定不一致、存在认定宽泛情况;还普遍存在判决书中未经分析论证直接以“行踪轨迹信息”进行表述。法院的说理不够明晰,这对于行踪信息的保护是不利的。

## 4. 个人行踪信息的民法保护困境

承前所述个人行踪信息已经明确纳入了我国法律的保护范围之内,《民法典》和《个人信息保护法》对此有明确的规定。目前对行踪信息的保护在立法层面已经受到重视,但实践中切实保护个人行踪信息却非易事,特别是从民法层面保护个人行踪信息仍需进一步深入研究,目前行踪信息的保护面临如下现实困境。

### 4.1. 忽视部分个人信息保护的基本原则

#### 4.1.1. 知情同意原则的虚化

在数字经济时代,信息的利用和保护之间的矛盾和冲突日益加剧,传统的个人信息保护框架之下,知情同意原则是一项重要的原则,在世界范围内得到认可,但在数据和算法的冲击下,其似乎逐渐失灵。信息主体在个人信息收集过程中没有得到足够的信息披露,知情同意原则被虚置和异化。例如目前各平台 app 隐私条款,虽然平台在用户进入应用时有征得信息主体同意的协议,但是通常这些隐私政策条款冗长、复杂难以阅读以及信息处理者和权利人失衡的地位,使得知情同意规则的有效性备受质疑[8]。另外信息主体在教育背景、认知结构、文化程度等方面存在差异,故无法期待每一位信息主体能够完全知悉与理解隐私政策所提供的同意规则[9]。在对个人行踪信息处理问题上,我们应当看到行踪信息具有“获取隐蔽性”与“广泛可得性”的特征,会让信息主体低估行踪信息交换的风险,甚至一些企业和个人认为个人行踪信息不存在隐私权问题,隐私意识的缺乏使信息主体难于做出理性的选择。具体而言:首先,在数字时代,通常网络服务器的升级会将位置信息作为升级的基本或者补充要素,而不一定是核心要素,经常被隐式使用,这不易被人们所知晓从而忽视其价值的重要性。其次,在实践中第三方处理者(如网络服务合作方)通常可以在无需事先征得个人授权同意的情况下,通过“互登”“关联分享”等功能跨设备收集个人位置数据,增加了行踪轨迹信息利用的隐私风险。最后,在一些特定的场景下行踪信息和其他信息存在关联,通过无需事先获得信息主体同意的情况下,信息的处理者就可以获得诸如交通信息、刷卡记录等交易信息、住宿信息,这些信息和行踪信息相关联,在不直接获取行踪信息的情况下并没有去征得信息主体的单独同意,这无疑是对获取行踪信息需要知情同意原则的违反,存在侵害个人行踪隐私的风险[10]。

再次,在大数据时代获取同意的难度增大,获取个人的同意需要时间、金钱和技术成本,数字时代,数据的收集处理量大而频繁,征集同意的次数也相应的增加;同时,同意只在特定的范围有效,服务和系统的更新或者超出原有的同意范围需要更新同意,这可能使信息处理者陷入无休止的同意征集中,这无疑增加获取同意的时间成本和金钱成本。面对这样的现实难题,法律明确规定的信息处理的知情同意原则被“选择性”地执行或者直接被“虚置”。

最后,知情同意原则的设立目的是为了保障个人的信息自决,然而,在大数据条件下,个人信息自决有形无实,数字经济时代信息主体对于各种信息收集的要求很难开口说不,可以说拒绝同意也就意味着无法享受服务。在此现实境遇中,用户不假思索地点击网上同意按钮成为麻木的常规操作。在这种形式化的同意中,自决的成分就算有也微乎其微,同意的作用被虚化和弱化[11]。

### 4.1.2. 最小比例原则被逾越

最小比例原则是个人信息处理中的一项义务性的规定，它是指各类主体只应处理与其提供服务和收集目的直接相关的个人信息，即非必要不收集、非必要不使用、非必要不传输，是一种对个人信息处理的法定限制<sup>[12]</sup>。比例原则被认为是公法的原则，但其在私法中仍有适用的空间。互联网时代，收集和储存个人信息变得便利且便宜，加之数据的重要性，信息处理者为了掌握数据获取竞争优势在收集个人信息时会有意和无意地忽视比例原则，特别是对信息收集的最小必要原则的遵守。《个人信息保护法》第28条明确规定了信息处理者处理敏感个人信息必须受到“特定的目的”和“充分的必要性”的“双重约束”。在数字时代背景下，个人信息处理平台具有强大的信息收集处理能力，其实则已具有“准公权力”或影响公共活动的强大“私权力”特征<sup>[13]</sup>。总体而言平台所具有的技术及其基于提供服务而产生的管理能力，个人和平台在事实上根本不可能形成实质平等关系。很多情况下信息处理者或者服务的提供者甚至在没有履行告知义务的情况下就私自收集利用个人信息，对个人信息的收集利用完全违背了最小必要原则的规定。如在中国“人脸识别第一案”<sup>12</sup>中，动物园在将入园方式由指纹识别变为人脸识别仅仅以殿堂告示和群发短信通知的方式告诉办卡用户激活人脸识别。像这样类似的案例不得不让人反思，信息处理者所做的信息处理行为是否具备充分必要性和特定的目的，或者进一步说该处理行为是否是必须所为的？在现有法律的规定下如何合理规制信息处理者对最小比例原则的逾越是保护个人信息的关键。

### 4.2. 个人行踪信息范围认定之难

行踪信息的保护在面临上文中提及的规范层面的困境之外，行踪信息的保护还面临着行踪信息多样、难以认定其范围的难题。互联网时代，行踪信息的属性出现了诸多特别之处，除了地理空间的行踪轨迹信息需要纳入法律保护的范围，近年来对于网络空间中的网络浏览记录的保护问题也引起了人们的关注，目前是否需要对个人“线上”活动轨迹和“线下”活动轨迹进行一致保护是一个颇具争议和值得深思的问题。

在司法实践中对于不同的行踪轨迹信息，法院的认定不一致，在朱某、张某犯公民个人信息罪一案中<sup>13</sup>，公诉机关指控的行踪轨迹信息中包括民航订票、铁路售票、出入境、车辆卡口、滴滴打车等信息，而法院并未采纳该意见，认为行踪轨迹信息系直接涉及人身安全的公民个人信息，只宜理解为GPS定位、车辆轨迹信息等可以直接定位特定自然人具体坐标的信息，上述民航订票、铁路售票、滴滴打车等信息虽涉及公民个人的轨迹，但上述单个信息反映的内容需结合其他信息及查询者的目的使用，因此法院并未采纳公诉方的意见。

结合实际生活来看行踪轨迹信息并不仅限于GPS等定位技术收集获取的信息，还包括了大量的具备定位功能的设备收集的行踪信息，诸如滴滴出行记录、出行购票信息、车辆轨迹信息、航班车票信息等，同时行踪信息还会和其他个人信息融合而具有法益上的复合性，如购物信息同时体现了财产信息和行踪信息，另外除IP地址、设备ID和Cookie等信息之外，因为技术的发展人们观念的转变，网络行踪轨迹信息的外延在不断的扩大，难以对其进行精完整的界定。因此如何对不同的行踪信息进行界定区分，建立科学的行踪信息分类标准是目前行踪信息保护面临的一大困境。

### 4.3. 数字经济驱动及公共安全优先

数字经济发展下个人的生活离不开信息时代的技术带来的便利，日常生活基于位置的服务多种多样，与我们的日常生活息息相关，我们出门打车、订购外卖、甚至购买周边的服务和商品都需要我们的定位

<sup>12</sup> 参见浙江省杭州市富阳区人民法院(2019)浙0111民初6971号民事判决书。

<sup>13</sup> 参见江苏省苏州工业园区人民法院(2017)苏0591刑初814号刑事判决书。

信息,这是为我们提供便捷服务所必须。因此在数字经济时代若严格限行踪信息的流通会增加交易的成本同时阻碍数字经济的发展,如何平衡好数据的流通和个人信息权益利益之间的平衡是行踪信息保护面临的一大难题。

其次,行踪信息不仅在提供个人服务促进数字经济的发展方面有着举足轻重的作用,其还在政府进行公共治理、警方利用行踪信息侦破案件中扮演“重要作用”。经历过三年疫情防控的我们都对政府利用行程码收集个人的行踪信息进行及时有效的疫情防控深有体会。在疫情期间公众对自己居住活动场所内的涉疫人员的信息,尤其是行踪信息有知情的“渴望”,在这种重大疫情期间公众知情权的主张更为明显,比如2021年众所周知的南京毛老太案,该案充分反映了疫情下公众对妨碍公共利益的个人的行踪轨迹的关注[14],这其中虽有规避自身感染风险的目的,但也掺杂了公众对知情权的“期盼”。

个人行踪信息是一种敏感个人信息,在大数据时代个人信息的识别性已经实现了从身份到行为的转变,现在利用现代信息技术,通过对数据的分析就可以轻而易举识别出特定的个人,如前述“成都确诊女孩遭网暴案”<sup>14</sup>中,其因个人信息的泄露使其遭受了巨大的伤害。像这样的案例不是个案,这促使我们反思在数字时代如何平衡公众的知情权和个人隐私权、数字经济驱动及公共安全优先的冲突,这是个人行踪信息保护面临的又一现实困境。

## 5. 个人行踪信息民法保护之完善进路

### 5.1. 个人行踪信息保护基本原则的完善

#### 5.1.1. 优化知情同意原则

知情同意原则作为个人信息保护的基本原则,是个人信息保护之基石。在个人信息保护视域下,知情同意原则具有不可替代的作用,恰如意思自治原则在民法中的地位[15]。知情同意原则的初衷是为了维护个人的信息自决[16]。知情同意的内涵是指在收集、使用、处理个人信息的过程中,个人信息控制者应该在明确告知个人信息主体相关信息的基础上,征得其明确、自由、具有同等地位的同意。也就是说,当个人信息控制者需要收集、处理、使用个人信息时,应该向个人信息主体告知收集、处理、使用个人信息的目的、方式、范围、后果、保护措施等信息,并征得其同意。个人信息主体需要在充分了解这些信息的基础上,自主选择是否同意。以此确保个人信息的合法、公正、透明、安全处理,并保护个人信息主体的权益。这是民法上意思自治、平等自愿原则在个人信息保护领域的具体应用[17]。数字时代,知情同意原则失灵的困境下不应当抛弃知情同意原则,而应当对此原则进行优化。面对信息化、智能化以及数字经济发展的需要,对个人行踪信息的收集和处理具有现实的需要,那么在传统的告知同意模式下应当实现从告知同意到告知选择的转变、部分弱化同意规则、坚守知情原则,以实现知情同意原则之实用。

具体而言,根据《个人信息保护法》的规定处理敏感个人信息应当取得信息主体的单独同意,这是对敏感个人信息的处理的特别规定,但是涉及公共利益时,我们需要对知情同意原则结合实际情况做出变通,诸如在重大疫情防控中,需要收集个人的健康、基因、行踪等敏感个人信息时知情同意原则的适用就应当缓和。在疫情防控的特定时期对个人行踪信息的收集可以例外放宽知情同意中同意规则。

完善知情同意原则在例外放宽同意规则的情况下并不是知情规则的舍弃,相反应当坚守知情规则,主要原因有两个,一是知情规则的坚守并不会对疫情防控这样特定情况产生阻碍,反而会有利于信息主体在知悉相关的信息收集规则情况下理解防疫的需要,做好配合和保护自己权益的工作,其二,保护信息主体对个人信息的知情可以实现对政府处理个人信息行为的实时监督,典型的例证如新冠肺炎防控期间因为不知“健康码”的赋码规则,健康码“多变”等处理个人信息的不透明使个人担忧信息的安全,因此对于知情同意原则的完善需要例外弱化同意规则同时加强对知情规则的落实。

<sup>14</sup> 参见《光明日报》,《成都确诊女孩,凭什么被“网暴”》2020年12月9日。[https://www.thepaper.cn/newsDetail\\_forward\\_10327360](https://www.thepaper.cn/newsDetail_forward_10327360)。

### 5.1.2. 强化最小必要原则的应用

最小必要原则包括相关性、最小化、合比例性三个子原则，其内涵是在个人信息收集、使用、处理和保存过程中，仅收集、使用、处理和保存必要的信息，且不超出其特定用途范围，以减少个人信息泄露的风险。前文已述及知情同意原则在个人信息保护中的失灵。数字时代背景下若要切实实现对个人行踪信息等敏感个人信息的保护，需要注重比例原则的价值，尤其是强化最小必要原则。对个人行踪信息的保护上应当从以下几方面强化最小必要原则的运用：第一，从个人信息保护角度而言应当针对不同的个人信息采取不同的收集、使用规则：根据不同类型的个人信息及其不同用途，明确不同的采集、使用规则。如个人身份证号码、敏感行踪信息等核心信息采取“严格控制、多层次保护”的措施，对于非核心信息则采取相对松散的控制措施。第二，限制个人信息的使用和分享范围：在收集、使用和保存个人信息时，应该尽可能限制信息的使用和分享范围。例如，通过实施数据匿名化、去标识化等措施来降低个人行踪信息的风险。第三，需要加强对最小必要原则的监管和制度落实，为个人信息保护提供有效保障。相关机构和企业需要建立相应的管理制度和流程，加强对个人信息的合规审查和内部审计，确保最小必要原则的落实。

综上，涉及公共利益需要对个人信息权益限制的也只能在合理的范围内限制，此限制需符合比例原则的要求。在个人行踪信息适用最小必要原则上要求必须明确国家机关收集个人行踪信息的范围、目的和标准，如若国家机关收集个人信息时缺少法律授权作为合规支撑和限制，就会导致其收集过程具有很强的主观随意性，超出收集的目的与范围只会加剧社会公共利益与公民个人隐私的冲突与失衡[18]。

## 5.2. 实行个人行踪信息的分类分级保护

2021年12月21日国务院办公厅《要素市场化配置综合改革试点总体方案》第20条指出，要分类分级、分步有序推动部分领域数据流通应用，推动完善数据分类分级安全保护制度。在新冠疫情防控时期时就有学者针对性地提出：政府在疫情防控中收集的个人信息在一定程度上具有公共数据的属性，考虑到数据体量大且重要性程度有所差异，再加上个人信息形态的多样性，政府在披露个人涉疫信息时应当采取分类分级的规则[16]。对于行踪信息这样的敏感个人信息而言对其保护应当根据具体情形进行区分。要实现对个人行踪信息的有效保护必须平衡好信息保护和信息利用之间的矛盾。为此可在利益平衡的理念下，参照《民法典》将个人信息区分为个人信息、私密信息和《个人信息保护法》将个人信息分为一般个人信息和敏感个人信息的分类对个人行踪信息进行细化分类保护，以实现数字时代个人行踪信息的利用和保护利益之间的动态平衡。在此背景下可根据行踪信息的存在形态、与其他信息的结合程度和其受保护的敏感度进行倾向性分类而非概念性的认定层级保护，从而明确行踪信息不同类别的民法保护。

### 5.2.1. 私密信息类的强保护模式

根据《民法典》1033条第5项规定了处理他人私密信息要么取得个人的“明确同意”要么根据法律的明确规定，否则，任何组织和个人处理他人的私密信息的行为都构成对隐私权、个人信息权的侵犯。行踪信息既属于敏感信息也属于私密信息，对于私密的行踪信息应该纳入隐私权的保护之中，适用侵权损害赔偿过错推定的归责原则。显然法律对于私密类信息采取了严格的保护范式。同时《民法典》1034条第3款规定：个人信息中的私密信息适用有关隐私权的规定，隐私强调其“私密性”，是不愿被他人所知晓的。个人行踪信息中涉及个人隐私的行踪，该行踪信息不关乎公共利益、不违背法律规定的情况下，应当尊重个人的隐私权，诸如个人出入同性恋酒吧、看望一些不想被他们所知晓的疾病的看病行程信息完全属于个人的隐私，个人有隐私权。

### 5.2.2. 敏感信息类的中度保护模式

此类型的行为轨迹信息和《个人信息保护法》第 28 条所界定的敏感个人信息在敏感度上具有相当性，在其保护上应当遵循敏感个人信息的保护规则即需要处理此类获得信息主体的单独同意，在数字时代，个人的住宿信息、上班打卡精准定位信息等都属于此类信息，从信息的属性上看该类信息具有“复合性”，该类信息通常会捆绑了个人的显性识别符号，如个人的姓名、身份证号、住址等。对此类信息的处理应当遵循《个人信息保护法》的规定采取单独同意，获取信息主体的授权同意，否则构成对个人信息的违法处理。

### 5.2.3. 一般信息类的弱保护模式

在司法实践中并不是所有的行踪信息都会得到法律的保护，其能否成为法律保护的行踪信息应当看该信息是否具有个人信息的本质特征即“识别性”。例如明星的航班信息、行车记录仪等与个人人身关系关联不大的信息，更多应该倾向于对这些信息的利用，发挥数字时代数据的效益和价值。诸如航班信息、行程记录仪等类似的信息虽然也会有定位的功能，但是其相较于 GPS 定位能具体定位到点位，程度上明显不够，对此类信息采取一般个人信息的弱保护模式，可在默示或者形式或者授权后处理。对于普通的个人行踪信息，当其处于一般个人信息和敏感个人信息的模糊地带时，可以将其划分至较低的分类级别中<sup>[19]</sup>。

## 5.3. 加强个人行踪信息的技术安全防护

信息技术的发展，对行踪信息的保护除了健全相关的配套制度，完善法律法规，还应当注重从技术层面实现对行踪信息的技术安全防护。结合上文中对行踪信息的分类应当对不同级别的行踪信息采取不同程度的技术安全防护。首先对于已经实现了信息利用目的的个人信息，可以对个人行踪信息进行匿名化的处理，去除与个人身份有关的识别信息，使得他人无法从该信息中确定具体的个人；其次，可以利用数据脱敏技术，对个人的行踪信息进行删除或者替换，从而使得该信息在不影响数据分析结果的前提下保护个人隐私；再次，还可在技术上设置限制访问，对个人行踪信息的访问进行权限控制，限制只有特定人员可以访问和使用这些信息，保证信息被妥善保护；同时对行踪信息进行传输时应当加密传输，以确保数据在传输过程中不会被非法获取和篡改。最后，应当对个人行踪轨迹信息的接收方、共享方的使用用途、数据安全保护能力进行必要的审查，防止个人行踪轨迹信息因第三方原因而泄露。

## 6. 结语

行踪信息作为敏感个人信息兼具个人信息与个人隐私的双重属性，互联网时代行踪信息的价值日益凸显，数字时代更应当重视对个人行踪信息等信息的保护。面对目前行踪信息保护的现实困境，首先应当肯定行踪信息的法律地位，优化知情同意原则，对同意规则作例外的放宽，坚守知情规则，实现知情同意到知情选择的转变；强化最小必要原则；其次根据行踪信息敏感度、存在形态和其他信息结合的程度不同同时结合其应用场景将行踪信息分类为私密信息倾向隐私权的保护，敏感信息类适用敏感个人信息单独同意的特别保护和一般信息类弱保护模式，对行踪信息给予不同层级的分类保护。也需要从技术层面加强对个人行踪信息的技术安全防护，另外应当注意对信息进行保护的目的是为了促进信息的安全流通，在数字时代只有坚持保护和利用利益的平衡，才能促进信息社会的健康发展。

## 基金项目

本文是贵州省 2022 年度哲学社会科学规划课题一般项目《智能时代生物识别技术法律规制研究》的阶段成果。项目编号：22GZYB23。

## 参考文献

- [1] 韩旭至. 敏感个人信息的界定及其处理前提——以《个人信息保护法》第 28 条为中心[J]. 求是学刊, 2022, 49(5): 132-145.
- [2] 程潇. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021: 57.
- [3] 雷澜珺. 论侵犯公民个人信息罪中行踪轨迹信息的认定[J]. 中国检察官, 2020(2): 8-12.
- [4] 文进宝, 肖冬梅. 我国行踪轨迹信息保护范围认定困境与出路[J]. 图书馆论坛, 2022, 42(7): 55-64.
- [5] 高完成. 大数据传播时代个人行踪信息的法律保护[J]. 青年记者, 2020(3): 78-79.
- [6] 韩新远. 个人行为轨迹信息的法律属性与分类保护研究[J]. 交大法学, 2021(3): 69-79.
- [7] 张志成. Facebook 数据泄露事件研究[J]. 青年记者, 2018(24): 89-90.  
<https://doi.org/10.15997/j.cnki.qnjz.2018.24.054>
- [8] 黄怡帆. 个人信息保护中知情同意的困境及重构[J]. 东南大学学报(哲学社会科学版), 2022, 24(S1): 110-114.
- [9] 廖丽环. 个人信息处理中同意规则弱化适用的路径优化——基于情境脉络完整性理论的场景细分[J]. 法制与社会发展, 2022, 28(6): 156-180.
- [10] 刘恒, 吴易泽. 网络消费者行踪轨迹信息交换的规制困境及路径优化——基于社会交换理论的视角[J]. 学术研究, 2022(5): 46-53.
- [11] 吴泓. 信赖理念下的个人信息使用与保护[J]. 华东政法大学学报, 2018, 21(1): 22-36.
- [12] 卢家银. 网络个人信息处理中必要原则的涵义、法理与适用[J]. 南京社会科学, 2021(12): 118-125.
- [13] 王锡锌. 个人信息国家保护义务及展开[J]. 中国法学, 2021(1): 145-166.
- [14] 张宇轩. 扬州 1 号病例“毛老太”出逃记[J]. 中国经济周刊, 2021(16): 55-56.
- [15] 齐爱民. 信息法原论[M]. 武汉: 武汉大学出版社, 2010: 58.
- [16] 田野. 大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例[J]. 法制与社会发展, 2018, 24(6): 111-136.
- [17] 刘艳红. 智慧法院场景下个人信息合规处理的规则研究[J]. 法学论坛, 2022, 37(6): 38-50.
- [18] 苏海雨, 李欣潮. 行政信息电子化收集的法律控制[J]. 新疆社会科学, 2020(6): 77-84.
- [19] 完颜邓邓, 陶成煦. 美国政府数据分类分级管理的实践及启示[J]. 情报理论与实践, 2020, 43(12): 172-177+155.