# 个人行为轨迹信息的法律属性与分类保护研究

韩新远*

目次

一、问题的提出
二、个人行为轨迹信息的可识别性
（一）可识别是数据权益的逻辑基点
（二）可识别性的判断标准
（三）从不可识别到可识别的流变
三、个人行为轨迹信息的法律属性
（一）人格利益
（二）财产利益
（三）法教义学考察
四、个人行为轨迹信息的分类保护模式建构
（一）纳入法律评价框架
（二）基于分类的法律保护模式
（三）保护的例外情形
五、结语

**摘要** 在互联网与大数据时代，个人行为轨迹信息的价值得以彰显，成为一项重要的商业资源。应比照个人信息，对个人行为轨迹信息应否纳入法律评价和法律保护范围的问题进行探讨。可识别性是个人信息权益的逻辑基点，随着技术更迭和观念演进，识别实现了从身份到行为的扩展。通过考察识别标准，可梳理出个人行为轨迹信息从不可识别到可识别的流变。个人行为轨迹信息具有人格利益和财产利益，具备了成为受法律保护之权益或权利的条件。将个人行为轨迹信息纳入法律评价框架并不意味着要将其笼统落入个人信息的法律保护范围，而应平衡数据保护与数据自由之间的张力，构建本土化的分类保护模式，给予不同强度的保护措施。同时，应筑牢保护例外情形的原则底线。

**关键词** 行为轨迹信息 个人信息 可识别 匿名信息 民法典

## 一、问题的提出

大数据开启了一次重大的时代转型，个人信息〔1〕的电子化、规模化收集、利用成为一种态势。

* 华东政法大学法律学院博士研究生。本文系国家社会科学基金重大项目“中国特色网络内容治理体系及监管模式研究”（项目编号：18ZDA316）和2020年华东政法大学研究生创新项目“网络内容监管的法理研究”（项目编号：2020－5－037）的阶段性研究成果。

〔1〕 对于个人信息和个人数据之间的区别和联系，学界有不同意见，但在本文的语境下，个人信息和个人数据可通用：一是在法律保护客体的内涵和外延上，两者具有同质性；二是本文为了引用某部法律或某位学者的原文，只能使两者交叉出现于文章之中。

在“个体生活公共化”的背景下,[2]我们不但是信息消费者,更是生产者。[3] 在追逐、挖掘信息“神奇的钻石矿”[4]的过程中,产生了如碎屑般弥漫的个人行为轨迹信息,不同于姓名、身份证号、家庭住址、指纹、基因等能直接识别特定自然人身份的信息,它是用户在线交互的副产品,是网民在互联网上留下的“电子脚印”。[5] 在模拟数据时代和信息技术初期阶段,这类瞬时性的、不具有独立身份识别性的信息(譬如搜索引擎键入的关键词、网上购物结束后留下的浏览记录和交易信息),由于技术条件的限制、存储成本的高昂,在完成它的功能使命后,便被丢进了数据坟墓。

但是,随着信息通信技术的革命性进展,互联网和信息化浪潮席卷全球,深入社会生活的各个领域,信息的电子化和存储越来越便捷,个人信息的利用(尤其是二次挖掘的价值)得以彰显。在大数据强大的聚合、分析能力前,在数据运用利益驱动下,个人行为轨迹信息的“可识别性”不断增强,人格利益和财产利益愈加凸显,与个人信息的边界日渐模糊。面对个人行为轨迹信息的属性变迁,各国相继在立法和司法实践层面做出回应,但所持态度各异、保护模式迥异。欧盟倾向于将Cookie以及其他个人行为轨迹信息纳入个人信息保护范围,[6]美国则存在截然相反的司法判例。[7] 我国起初对个人行为轨迹信息的法律保护持排斥态度,[8]之后,北京互联网法院在黄某诉腾讯科技(深圳)有限公司广州分公司、腾讯科技(北京)有限公司隐私权、个人信息权益网络侵权责任纠纷案(以下简称“微信读书网络侵权案”)中,认定个人社交行为轨迹信息(微信好友关系)和阅读行为轨迹信息(微信读书用户的读书信息)为个人信息。[9] 从我国《民法典》第1034条对个人信息界定及其相较《网络安全法》第76条所做的文字表述变动中可以看出,民法典中的个人信息不再局限于“身份”识别的范围,而是将行踪信息纳入了其范畴。这些变化标志着国内立法、司法层面对个人行为轨迹信息的态度发生着转变。

在此背景下,我们有必要与时俱进地审视个人行为轨迹信息的可识别性,理清其法律属性,考证其被纳入法律评价和保护的必要性,从而构建基于分类前提下的本土化法律保护模式。申言之,认定个人行为轨迹信息是否属于个人信息、属于何种类别的个人信息以及给予何种强度的保

---

〔2〕 何明升:《技术与治理:中国70年社会转型之网络化逻辑》,载《探索与争鸣》2019年第12期,第41—52页。

〔3〕 参见韩炳哲:《在群中:数字媒体时代的大众心理学》,程巍译,中信出版集团2019年版,第26页。

〔4〕 [美]维克托·迈尔-舍恩伯格、肯尼思·库克耶:《大数据时代:生活、工作与思维的大变革》,盛杨燕、周涛译,浙江人民出版社2013年版,第127页。

〔5〕 个人行为轨迹信息是相对于传统个人信息概念的一个参照性、集合性的概念,指的是网络用户在使用计算机和网络的行为过程中被计算机硬件或软件记录下来的行为事件或过程数据,乃人们在线交互过程中产生的不具有独立身份识别特征的有关个人的信息。由于技术更迭和观念流变,个人行为轨迹信息的外延在不断发生变化,很难进行精确界定,只能进行开放性罗列,包括但不限于浏览器搜索关键词,用户操作记录(网站登录记录、软件使用记录、点击记录),通过互联网观看、收听、阅读一切试听内容的记录,支付软件的交易记录、翻译数据、位置轨迹、网购足迹、智能穿戴设备收集的身体体征信息、系统错误报告信息、用户改善计划等。美国学者维克托·迈尔-舍恩伯格和肯尼思·库克耶将个人行为轨迹信息比喻为“数据废气”。同上注,第146页。

〔6〕 2009年修订的欧盟《电子隐私指令》(E-Privacy Directive,2009/136/EU)主要对利用Cookie技术及类似技术收集用户信息的行为做出明确规范,甚至被直接称为“欧盟Cookie法”。

〔7〕 美国华盛顿地区法院认为被告向第三方公司披露的“唯一的Roku设备序列号以及视频浏览记录”已被匿名化,不具有可识别性,披露行为并不违反法律,故判决原告败诉,参见 Eichenberger *v.* ESPN, INC, C14 - 463 TSZ; 2015 U. S. Dist. LEXIS 157106;美国联邦贸易委员会(FTC)基于公平信息实践原则对商业网站收集使用、处理用户的个人信息行为进行了规制,实质性地启动了对零售商Sears公司和EchoMetrix公司的调查,对他们未经同意而跟踪和记录客户浏览记录和习惯的行为进行了否定,参见丁晓东:《用户画像、个性化推荐与个人信息保护》,载《环球法律评论》2019年第5期,第82—96页。

〔8〕 参见朱某与百度隐私权纠纷案,历审裁判文书分别为:江苏省南京市鼓楼区人民法院(2013)鼓民初自字第3031号民事判决书、南京市中级人民法院(2014)宁民终字第5028号民事判决书。

〔9〕 参见北京互联网法院(2019)京0491民初16142号民事判决书。

护力度直接关系着个人信息保护的民众关切，关乎数据控制者、使用者对个人信息收集、利用的法律风险边界，关联着我国网络信息产业的良性健康发展，是该领域研究向细腻化、精致化推进的该当路径。

## 二、个人行为轨迹信息的可识别性

顾名思义，个人行为轨迹信息是相对于法律意义上的有关个人的数据——个人信息的一个对应概念，对个人行为轨迹信息进行法律保护层面的探讨不可避免要以个人信息的概念为参照，以其实质要素为比照。

### （一）可识别是数据权益的逻辑基点

之所以将部分有关个人的信息称为法律上的个人信息，其原因就在于此类信息明显的可识别性。譬如在美国，个人信息被称为“个人可识别信息”（personally identifiable information）；欧盟《统一数据保护条例》（以下简称“GDPR”）将个人数据定义为“与已识别或者可识别数据主体相关的任何数据”；我国《网络安全法》第76条第5款将个人信息界定为“单独或者与其他信息结合识别自然人身份”的信息，《民法典》第1034条认为个人信息是“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”。识别指的是根据与特定人有关的信息来认识、辨识或锁定该特定个人，英文统一表述为“identity”。易言之，不能被识别的信息不具有利益或者不属于受法律保护之利益，谈不上法益或权利，自然不在法律保护范围之列。

由此可见，“可识别”是构成法律上个人信息的核心，也是负载于信息之上的人格利益、财产利益的逻辑基点。有学者将“可识别”总结为个人信息的实质要素，[10]而不具识别性的信息可被归入匿名信息范畴。因此，对个人行为轨迹信息进行考察，就需要以个人信息的实质要素——“可识别”为切入点，对其属性和地位进行辨析论述。

### （二）可识别性的判断标准

从学理层面看，目前关于个人信息可识别性的判断基准有以下三种学说：“主观说”又被称为“信息控制者标准说”，其认为信息管理者自身的条件应作为可识别与否的判断标准；“客观说”又被称为“社会一般多数人说”，其认为应从普通大众、一般人的角度出发判断个人信息的可识别性；“任一主体说”认为，是否可识别应以社会中任何人识别的可能性来判断。[11]

从各国的操作实践来看，欧盟采取的是穷尽一切可能性的严格标准，GDPR鉴于条款第26条规定：“为确定自然人是否可识别，应考虑到所有合理可能使用的方式，包括控制者或其他人直接或间接地识别自然人所选择的方式。”“美国没有制定统一的个人数据保护法，而是形成了‘特别领域立法＋一般领域普通法’体制。”[12]美国《健康保险携带和责任法案》（Health Insurance Portability and Accountability Act/1996，简称“HIPAA”）第164.514条b款第1项规定，经专家判断不具识别性的信息不属于法案规制的“可识别健康信息”，这被称为专家标准；该款第2项规定，删除18种识别符的健康信息不是“可识别健康信息”，这被称为安全港标准。

我国目前的规范性文件中，除定义条文对个人信息的外延进行具象列举外，并无抽象识别标准。《网络安全法》第42条、《民法典》第1038条规定了网络运营者或信息处理者的责任豁免情形，即“经过处理无法识别特定个人且不能复原的除外”，可认为该法采取了“处理”加“不能复原”的技术标准。也有学者提出“社会多主体共识”标准，即对个人信息的认定应综合“行政主管部门、数据

〔10〕 参见韩旭至：《个人信息概念的法教义学分析——以〈网络安全法〉第76条第5款为中心》，载《重庆大学学报（社会科学版）》2018年第2期，第154—165页。

〔11〕 同上注，第159页。

〔12〕 高富平：《论个人数据保护制度的源流——域外立法的历史分析和启示》，载《河南社会科学》2019年第11期，第39—49页。

代理商、技术与法律专家以及第三方机构”和“各方专业人士和社会公众”意见。[13]

（三）从不可识别到可识别的流变

之前之所以将搜索关键词、登录网站的时间、地点、时长及浏览内容记录等信息区分于个人信息，有两个原因。原因一：其曾经不具有独立的身份识别效用，处于边缘地位；原因二：其一度不被广泛记录，缺乏便捷载体。但随着网络信息技术的更迭和人们观念意识的演进，个人行为轨迹信息经历了从不可识别到可识别的角色流变。

1. 技术因素，使个人行为轨迹信息模糊个人信息边界。在进入信息社会后，尤其是存储成本的降低、大数据的运用，计算机在信息处理的速度、精度和深度上能力有了极大提升，“使得原来不具有意义的信息片段同样具有了意义”。[14] 由此，立法上的“个人信息”范围发生扩张，[15]乃至“无所谓‘不重要’数据存在问题”。[16] 不论采取“客观说”还是“主观说”的识别标准，均无法回避个人行为轨迹信息不断被新的技术手段所识别从而模糊个人信息界限的事实，譬如Cookie收集的可以体现用户爱好偏向、性格特征的网页浏览记录等轨迹信息从边缘走向舞台中央，成为“追踪用户行为、投放定向广告中最重要的基础数据”。[17]

2. 认识因素，从身份识别到行为识别或特征识别。《网络安全法》第76条认定个人信息是单一的身份识别；《电信和互联网用户个人信息保护规定》第4条将识别对象扩展为“用户信息以及用户使用服务的时间、地点等信息”；最高人民法院和最高人民检察院联合发布的《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》第1条将信息识别范围进一步扩展为“身份”和“活动情况”（行踪轨迹等）。对此，有学者提出了“行为识别”（activity recognition）和认知型识别（recognition identifiability）概念，[18]也有学者认为“识别”除身份识别外，还包括步态、语音等个体特征识别。[19]

上述观念的演进，使个人信息涵摄更多识别对象，使持续性的浏览痕迹、位置轨迹、软件操作痕迹等部分行为轨迹信息能独立或与其他信息关联而轻易识别具体对象成为一种认知和实践。[20] 美国学者丹尼尔·索洛夫（Daniel Solove）和保罗·舒格瓦兹（Paul Schwartz）正是基于该国隐私法中核心概念“可以识别个人身份的信息”所面临的困境，即难以在技术发展和具体场境差异的情形下有效界定可识别信息的难题，从而提出应将前述概念升级改造为“可以识别个人身份的信息”（第2版）（PII 2.0）、包含“已识别个人身份”的个人信息和“可用来识别个人身份”的个人信息，[21]而行为轨迹信息恰恰符合“可用来识别个人身份”的个人信息特征。

---

〔13〕 参见苏宇、高文英：《个人信息的身份识别标准：源流、实践与反思》，载《交大法学》2019年第4期，第54—71页。

〔14〕 郭明龙：《个人信息权利的侵权法保护》，中国法制出版社2012年版，第2—4页。

〔15〕 谢琳：《大数据时代个人信息边界的界定》，载《学术研究》2019年第3期，第69—75页。

〔16〕 谢永志：《个人数据保护法立法研究》，人民法院出版社2013年版，第103页。

〔17〕 朱芸阳：《定向广告中个人信息的法律保护研究——兼评“Cookie隐私第一案”两审判决》，载《社会科学》2016年第1期，第103—110页。

〔18〕 行为识别指的是基于计算机科技的发展而产生的一种对于用户行为方式的识别，通过一个未知主体某种行为的时间、地点和活动场景等能推断出其真实身份，参见苏今：《〈民法总则〉中个人信息的“可识别性”特征及其规范路径》，载《大连理工大学学报（社会科学版）》2020年第1期，第82—90页。认知型识别可在不与显名的个人产生联系的情况下对其进行认知。See Ronald Leenes, *Do They Know Me? Deconstructing Identifiability*, 4 University of Ottawa Law & Technology Journal 135 - 142(2007).

〔19〕 参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018年第3期，第84—101页。

〔20〕 在“庞理鹏诉北京趣拿信息技术有限公司案”中，趣拿公司与东航涉嫌泄露了庞理鹏的姓名、手机号码及航班信息。该案的判决书确认“公民个人信息包括身份识别信息和活动情况信息”。参见北京市第一中级人民法院民事判决书，（2017）京01民终509号。

〔21〕 See Daniel Solove & Paul Schwartz, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 New York University Law Review 1815 - 1894(2011).

## 三、个人行为轨迹信息的法律属性

个人行为轨迹信息具有了身份或行为的可识别性是认定其法律属性的前提，接下来还需考察该类信息是否具有法律可予保护的利益，成为权益或权利内容。[22] 关于个人信息的法律属性学界存在争议，有学者将现有学说归纳为人格利益说（包括隐私权说和具体人格利益说）、个人信息权说和人格兼财产权说，[23]也有学者提出新型权利或知识产权的论断。不论做何种类别的划分，均无法绕开人格利益和财产利益之内核。要考察个人行为轨迹信息能否化升为法律保护对象，就需从人格利益和财产利益两个维度展开。

### （一）人格利益

对个人信息进行法律评价肇始于隐私权益的凸显。隐私权理论滥觞于美国塞缪尔·沃伦（Samuel Warren）与路易斯·布兰代斯（Louis Brandeis）合著的《隐私权》（*The Right to Privacy*）一文，[24]之后在美国演变出信息隐私权这个分支，而法国、德国等欧盟国家却采取了由“信息自决权”演化到具体人格权的进路，我国则概括性地采取后一模式。[25] 两种模式的保障核心均为人格利益，关乎自由和尊严。

孤立的搜索而得的关键词、个人网站访问日期、时长及光标操作等信息，在不和姓名、用户名等显性标识结合时，不能单独识别个人。但随着行为重复和事件叠加，由点成线，便会描绘出相应主体的购买记录、行踪信息、搜索历史、健康状况等动态过程，勾勒出用户的“虚拟画像”。此类“画像”信息在与传统个人信息结合时被归为个人信息，这点已无须赘言；也可通过指纹识别（fingerprinting）技术交叉对比（非个人信息）来验证身份；甚至通过国际移动设备身份码（IMEI）、网络设备硬件地址（MAC）、广告标识符（IDFA）或其他任意标注，从而无须识别特定主体，即可进行信息标签化，实现画像功能。

对此类行为轨迹信息的不当处理，会让相应主体的实体形象与虚拟人设产生偏差，导致外在形象被操纵；会刺穿阿兰·威斯丁教授提出的“面具”理论，[26]导致精神安宁被打破；使数据控制者基于算法对数据主体进行意识诱导、行为预判，导致决策自由被剥夺，思维方式被简化，甚至陷入乔治·奥威尔（George Orwell）笔下的《一九八四》所描绘的全景监视场景之中。

### （二）财产利益

随着大数据出现和数据产业兴起，数据的经济价值（尤其是二次利用的潜在价值）日益凸显，个人在网络空间留下的活动痕迹被记录、收集、加工、分析，成为互联网企业精准广告投放、个性化推荐以及其他增值服务的数据支撑，是互联网“依靠广告提供免费服务”这一商业模式的基本条件。[27] 姓名、电话号码、证件号码、生物识别信息等传统身份要素的价值愈加依附于其衍生出的行为轨迹信息，甚至反映个体活动情况或特征的网络行为轨迹信息与身份要素脱离而成为未知的标签信息，这些信

---

〔22〕 笔者在此采用学者杨立新的“民事利益的三段论”，即某种民事利益，法律规定以权利进行保护的，就是权利；某种民事利益法律予以保护，但未规定为权利者，即为法益；其余则是不受民事权利和法益保护的民事利益。参见杨立新：《个人信息：法益抑或民事权利——对〈民法总则〉第111条规定的“个人信息”之解读》，载《法学论坛》2018年第1期，第34—45页。

〔23〕 参见梅夏英：《在分享和控制之间 数据保护的私法局限和公共秩序构建》，载《中外法学》2019年第4期，第845—870页。

〔24〕 See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4(5) Harvard Law Review 193－220 (1890).

〔25〕 参见王秀秀：《个人数据权：社会利益视域下的法律保护模式》，华东政法大学2016年博士学位论文，第42页。

〔26〕 阿兰·威斯丁教授提出的“面具”理论认为“每个人都意识到他想成为的人和实际上的自己之间存在差距，他人眼中的自己和他知道的更加复杂真实的自己存在差距”。如果个人的活动规律、偏好、能力，甚至所思所想都可以被第三人所搜集、呈现，无疑会让人们产生严重的精神负担。See Alan F. Westin, *Privacy and Freedom*, Atheneum Press, 1967, p.33.

〔27〕 参见刘金瑞：《个人信息与权利配置——个人信息自决权的反思与出路》，法律出版社2017年版，第229—230页。

息都可实现相应商业利益。〔28〕由此可见，行为轨迹信息已然成为个人信息财产利益的源泉。

为调和数据保护和数据流通之矛盾，美国司法实践认为“有必要对网络个人信息保护在援引隐私权规则方面进行适度软化”，赋予用户积极的自决功能；欧盟亦突破人格权不可让渡的原则，将个人信息权由消极人格权向积极自决人格权方向加以改造，允许用户通过合同方式进行约定或授权收集和使用。〔29〕包括我国在内的诸多法域均不同程度开启了数据财产化的趋势，区别是对个人数据财产属性的表述不一，譬如“个人数据的财产权”和“商业秘密”〔30〕“财产性人格利益”〔31〕“平台或企业数据财产”〔32〕等。

若认可行为轨迹信息的财产利益，将不可避免牵扯出错综复杂又富有争议的产权配置与归属问题，〔33〕本文对此暂不予展开。分散的行为轨迹信息对数据主体而言并无直接财产价值，但可能会因被区别对待而蒙受间接经济损失。〔34〕对行为轨迹信息青睐有加的是各大网络平台和众多的数据从业者。

（三）法教义学考察

基于可识别性和人格、财产利益，行为轨迹信息具备了个人信息的形式、实质要件，域内外的规范性文件对此均予以不同程度的回应——将其有差别地纳入个人信息的范畴。

**表1 域外列举范畴**

| 规 范 来 源 | 个人信息列举式规范中的行为轨迹信息 |
|---|---|
| 1995年《个人数据保护指南》(欧盟)第2条(a)项 | 自然人所特有的身体、生理、精神、经济、文化和社会识别因素 |
| 2002年《隐私和电子通讯指令》(欧盟)第2条(c)项 | 定位数据 |
| 欧盟《通用数据保护条例》(GDPR)第4条第1项 | 位置数据，针对自然人的身体、生理、心理、经济、文化等要素 |
| 日本《个人数据保护法》第2条第1项 | 金融交易记录 |
| 奥地利联邦《个人数据保护法》第4条第2项 | 关涉健康的数据 |
| 比利时《关于个人数据处理的隐私权利保护法》第1条第1项 | 物理的、生理的、心理的、经济的、文化的、社会的特征 |
| 加拿大《个人数据保护法》第3条 | 有关财务交易的信息 |
| 《美国隐私权法》第1条第5项 | 金融交易 |

**表2 域内列举范畴**

| 规 范 来 源 | 个人信息列举式规范中的行为轨迹信息 |
|---|---|
| 《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》法释〔2014〕11号第12条 | 私人活动 |

〔28〕 参见前注〔18〕，苏今文，第86页。

〔29〕 参见龙卫球：《数据新型财产权构建及其体系研究》，载高鸿钧、申卫星主编：《信息社会法治读本》，清华大学出版社2019年版，第156—164页。

〔30〕 参见丁晓东：《什么是数据权利？——从欧洲〈一般数据保护条例〉看数据隐私的保护》，载《华东政法大学学报》2018年第4期，第39—53页。

〔31〕 参见前注〔22〕，杨立新文，第42页。

〔32〕 参见姚佳：《企业数据的利用准则》，载《清华法学》2019年第3期，第114—125页。

〔33〕 参见高富平：《数据生产理论——数据资源权利配置的基础理论》，载《交大法学》2019年第4期，第5—19页。

〔34〕 参见李飞翔：《大数据“杀熟”背后的伦理审思、治理与启示》，载《东北大学学报(社会科学版)》2020年第1期，第7—15页。

续表

| 规　范　来　源 | 个人信息列举式规范中的行为轨迹信息 |
| --- | --- |
| 2015年全国民事审判工作会议纪要 | 上下线时间、网络浏览日志、网页地址、使用的搜索引擎关键词 |
| 《最高人民法院、最高人民检察院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》法释〔2017〕10号第1条 | 反映特定自然人活动情况，如行踪轨迹 |
| 《刑法》第253条之一 | 行踪轨迹 |
| 《电信和互联网用户个人信息保护规定》第4条 | 用户使用服务的时间、地点 |
| 2020年《信息安全技术 个人信息安全规范》附录A | 个人财产信息中的交易和消费记录，个人上网记录（通过日志储存的用户操作记录，包括网站浏览记录、软件使用记录、点击记录等），以及个人位置信息（包括行踪信息、精准定位信息、住宿信息、经纬度等） |
| 《民法典》第1034条 | 健康信息、行踪信息 |

表2为我国规范性文件中的个人信息定义列举的行为轨迹信息，表1为域外相关情况。从来源规范中对个人数据的定义可看出，各国大都采用了开放性的定义描述，运用了“相关”“任何”“等”“包括但不限于”的语词，“个人信息的‘识别性’边界逐步扩大”，〔35〕从而使个人信息与行为轨迹信息交融、交错，在范围上呈现一种前者扩张、后者压缩的态势。我国新近亮相的《个人数据保护法》（草案二次审议稿）第4条规定“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息”，从文义解释角度可知，该草案同样体现了个人信息外延扩张的态势。虽然各国将特定行为轨迹信息纳入个人信息范畴予以法律保护，但对可认定为个人信息的行为轨迹信息种类、范围并未呈现共识态势。

## 四、个人行为轨迹信息的分类保护模式建构

无论是对数据主体，还是对数据控制者和处理者，行为轨迹信息游走于法律评价范围之外都不是一件有益之事。面对方兴未艾的大数据时代，我们有必要在充分借鉴域外经验的基础上，结合国内社会发展实际，参照《民法典》（将有关个人的信息划分为一般个人信息、私密信息、匿名信息）、《个人信息保护法》（草案二次审议稿）（将有关个人的信息划分为个人信息、敏感信息、匿名信息）的规范实践，建构本土化的行为轨迹信息分类保护模式。

### （一）纳入法律评价框架

能够反映个人习惯、兴趣偏好、性格特征、思维方式的行为轨迹信息，将真实世界中的物理人以镜像形式投射到了网络空间，形成了所谓的数字化人格（computer persona），无论从形式还是实质层面我们都无法再将其排斥于法律评价范围之外。然而，不管是将个人信息视为一种隐私权、人格权、人格财产混合权，抑或独立的个人信息权，均无法回避我国目前个人数据方面理论探讨与法律创制不足的现实，法律资源供给不足的矛盾自然体现在对行为轨迹信息属性的区分、认定上。

正如上文的法教义学考察，相较于欧盟国家大多以专门的数据保护法规给予行为轨迹信息法律评价的做法，我国更多以司法解释、指导性的行业标准予以指涉，要么适用范围狭窄，要么效力等级不足，要么直接跨越到强制力顶格的刑法。即使是被称为数据保护基本法的《网络安全法》，

〔35〕 谢琳：《大数据时代个人信息边界的界定》，载《学术研究》2019年第3期，第69—75页。

对网络运营者收集用户网络活动痕迹的行为也无明确规定。相比之下，国内大型网络企业的隐私政策对行为轨迹信息有明确表述，对其法律化时可资借鉴。〔36〕

若不计成本，从技术上实现行为轨迹信息与特定个人一一对应绝非难事，这也是学者所称的大数据下没有非个人信息的依据。〔37〕但如果就此将行为轨迹信息笼统纳入个人数据的保护范围，则会导致明显弊端：其一，限制信息自由流通，使网络企业畏首畏尾，可能导致商业垄断，最终影响用户体验、减损网民福利；其二，行为轨迹信息的动态性和模糊性将泛化个人信息，反而使真正需要保护的信息失去保护；其三，会增加信息保护的社会成本，限制本土互联网企业发展。

（二）基于分类的法律保护模式

要建立对行为轨迹信息的法律保护必须平衡信息保护和信息自由的价值冲突。为此，我们可在利益衡量理念、“激励相容之道”〔38〕的指引下进行分析，参照《民法典》对个人信息的三类区分，既要考虑识别所需的成本、时间和处理数据时可以采用的技术及技术发展，又要考量“个人信息迟钝者”〔39〕和部分用户为获得免费网络服务而贡献个人信息的主动意愿，〔40〕结合行为轨迹信息的存在形态、样本数量、与其他信息的结合程度进行倾向性层级归类（而非做概念性认定），使其外延呈现一个放射状扇形结构，从而采用不同程度的保护标准，以界定信息收集者、使用者的不同责任。

1. 私密信息类的强保护模式

此类行为轨迹信息可涵摄通过硬件或软件持续性追踪或开展特定业务而获取的有关性取向、性生活、疾病史、私密物品购买记录、未公开的违法犯罪记录等。从信息类型看，其可归于《民法典》私密信息范畴；从信息存在样态看，此类信息只要和任一身份识别符、标签信息等相结合，均可归为私密信息，不论数量多少、种类多寡。对此类信息须强化防御性保护，非特定情形不得处理，否则将承担相应的停止侵害、赔礼道歉、赔偿损失等侵权责任。《民法典》第1034条第3款对个人信息中的私密信息进行了区分和着重；第1032条第2款对“隐私”进行了界定，强调了“私人生活安宁”和“不愿为他人知晓”两个特征。由此可知，划入隐私的个人信息，应强调其“私密性”，进而与其他层级的个人信息在收集、存储、使用、加工、传输、提供、公开等方面形成相区别的授权同意、技术安全、信息处理之规范等。〔41〕

---

〔36〕《百度隐私政策总则》将设备信息、位置信息、日志信息、唯一应用程序编号视为个人信息；《小米浏览器隐私政策》认为搜索关键词在与其他信息结合具有身份识别性时才属于个人信息；2345加速浏览器《用户体验改善计划隐私保护声明》认为单独的设备信息、日志信息为非个人信息，而行踪轨迹、住宿信息、健康生理信息则属于个人信息；《微信隐私政策》认为接入网络的方式、类型和状态，网络质量数据，设备加速器（如重力感应设备）、操作日志、服务日志信息为提供服务所必须收集的基础信息，至于其法律属性则不置可否，《支付宝隐私权政策》采取了与之相似的策略。上述内容查阅日期截止于2020年7月。

〔37〕参见[德] Winfried Veil：《GDPR：皇帝的新衣——论新旧数据保护法的结构性缺陷》，朱家豪编译，载微信公众号“腾讯研究院”2019年4月24日，https：//mp.weixin.qq.com/s/pLH6C4_ElzN4L4cpmDKjag。

〔38〕学者周汉华提出了“激励相容的个人数据治理之道”，“在大数据时代，由于数据本身的特性，信息控制者有很强的利用激励而缺乏同等程度的保护激励。如果法律规则不能因势利导，只是简单施加各种禁止性或者强制性规定，势必因为激励不相容影响有效实施”。参见周汉华：《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》，载《法商研究》2018年第2期，第3—23页。

〔39〕张新宝：《我国个人信息保护立法主要矛盾研讨》，载《吉林大学社会科学学报》2018年第5期，第45—55、204—205页。

〔40〕参见前注〔27〕，刘金瑞文，第230页。

〔41〕需要说明的是，有学者认为私密信息不属于个人信息权利保护的范畴，因为个人信息权利保护的适用前提是存在持续性的信息不平等关系，是一种新民法关系，而非传统民法关系，易言之，本文所列的后三类行为轨迹信息属于商业性或专业性收集的个人信息，对此，笔者予以认同。参见丁晓东：《个人信息权利的反思与重塑 论个人信息保护的适用前提与法益基础》，载《中外法学》2020年第2期，第339—356页。

私密类行为轨迹信息一般宜采取“任一主体说”的严格识别标准。关于“不愿为他人知晓”的“私密性”的认定，毋庸讳言，首先要遵循当事人主观意愿，但该主观意愿又不能单纯取决于隐私诉求者的个体意志，同时，也应符合社会一般合理认知。而社会一般合理认知的边界，又受地域、文化传统、法治理念、宗教信仰、风俗习惯、经济发展状况、主流价值观等因素影响。

2. 敏感信息类的次强保护模式

此类行为轨迹信息可涵摄个人财产信息中的交易消费记录、虚拟财产信息，以及个人的行踪轨迹、网页浏览记录、购买记录、住宿信息、精准定位信息。从信息类型看，此类行为轨迹信息属于《个人信息保护法》（草案二次审议稿）中的敏感信息；从数据存在样态看，其是一种“动态”且“混合”的信息。“动态”类指对行为主体进行持续性追踪所形成的数据集；“混合”类指捆绑如姓名、IP等显性识别符的信息束，或将多个类型的行为轨迹信息混合收集的信息包（比如能进行交叉验证的位置信息与网上交易记录的混合）。

对此类行为轨迹信息可给予敏感个人信息强度的法律保护。数据控制者收集该类数据必须获得数据主体明示同意，即数据主体通过书面声明或主动做出肯定性动作来完成对其个人数据进行特定处理的明确授权，其中，肯定性动作包括数据主体主动做出声明（电子或纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”等。

私密信息不能概括等同于敏感信息，前者是后者中的特殊情形。敏感信息属于兼具防御性期待及积极利用期待的个人信息，判断针对此类信息的处理是否侵权，宜采取“客观说”的识别标准，需要结合信息内容、处理场景、处理方式等，进行符合社会一般合理认知的判断。

3. 一般信息类的弱保护模式

此类行为轨迹信息可涵摄智能穿戴设备收集的身体体征信息、系统错误报告信息，用户改善计划，用户接入网络的方式、类型和状态，网络质量数据等。从信息存在样态看，此类行为轨迹信息与敏感信息一致，属于持续性追踪所形成的动态且混合的行为轨迹信息。另外需要注意“标签化”行为轨迹信息，即与 IMEI、MAC、IDFA 及唯一应用程序编号等进行绑定的信息，其虽然不能实现“身份识别”，却能实现“行为识别”或“特征识别”。识别针对此类信息的处理是否侵权，宜采取“主观说”标准。

对该类行为轨迹信息可给予一般个人信息的保护强度，其保护强度弱于敏感信息。“弱”主要体现在数据控制者收集该类数据只需获得数据主体默示同意即可。默示方式指行为人虽没有以语言或文字等明示方式做出意思表示，但以特定作为或不作为的沉默方式做出了意思表示，比如阅读“使用即同意”的条款、浏览默认勾选的对话框等。敏感信息类和一般信息类的行为轨迹信息可被归类为民法典中的个人信息，数据控制者均须遵循合法收集、目的限制、最小够用等原则，数据主体享有查询、更正、删除、撤回同意等权利。

4. 匿名信息（anonymous information）类的选择保护模式〔42〕

此类信息存在两类样态，其一为单一的行为轨迹信息，即只收集用户的浏览记录、踪迹信息或鼠标点击历史等单一种类的数据，而没有与用户 ID、IP 等识别符进行捆绑，也没有和其他种类的行为轨迹信息混合收集且单独存储，具有高度离散化特征；其二为偶然的“标签化”信息，即个体偶尔使用搜索引擎产生的关键词或使用翻译软件留下的文字碎片，即使其和特定标签信息捆绑，因具有稀少、随机的特征而宜被归为匿名信息范畴。

对该类行为轨迹信息须在分类的基础上进行选择性保护。依照是否投入智力、物力加工为标

〔42〕 根据 1995 年欧盟《数据保护指令》鉴于条款第 26 条、2018 年生效的欧盟《通用数据保护条例》（GDPR）鉴于条款第 26 条规定，匿名数据指不能再对所属自然人的身份进行确认的不受保护的数据。美国政府 2010 年发布的《个人信息保护指引》的相似表述为“通过移除足够的个人可识别信息以至于剩余的信息不能识别特定个人，以及没有合理的理由相信这些信息能被用于识别特定个人”的信息。我国《网络安全法》第 42 条中的相似表述为“经过处理无法识别特定个人且不能复原的”信息。

准可将此类信息分为原始信息和加工信息：前者指直接从数据主体收集而来的信息，其属于纯粹的匿名信息，不受法律保护，人人共享；后者指数据控制者和使用者对原始信息加工后的信息，在“淘宝公司诉美景公司不正当竞争案”中被称为网络大数据产品。该类匿名信息虽然经脱敏而与数据主体脱离了关系，但经过了网络运营者大量的智力劳动投入，经过了深度开发与系统整合，故网络运营者对其享有财产性权益，其他网络运营者不能擅自抓取，否则构成不正当竞争。〔43〕当然，该问题的探讨又将开启企业数据的权属争议，〔44〕本文对此不予展开。

（三）保护的例外情形

个人信息具有人格、财产双重特性，其背后始终交织着信息保护、信息自由、公共利益等价值冲突，因此，各国会基于特定事项对个人信息权益制定相应的保留和克减条款，从而表述有所差异，但核心内容基本一致，诸如“国家安全”“公共安全”“公共卫生”“重大公共利益”“执行公务”“诉讼”“维护个人信息主体权益”等。

1. GDPR中有关个人数据保护的例外条款

GDPR对数据保护的限制体现在执行公务或处理突发紧急事件两个方面：鉴于条款第45条明确公共卫生构成重大公共利益，依据条例第6条1(e)的规定，当个人数据处理为“基于公共利益目的执行任务或履行被赋予的公共职能所必要”时，可不征得数据主体的同意；鉴于条款第46条明确传染病监测除构成公共利益之外，还构成“重大生命利益”，依据条例第6条1(d)规定，当个人数据处理为“保护数据主体或其他自然人的重要利益所必要”时，可不征得数据主体的同意；等等。

2. 美国立法、司法层面有关个人数据保护的例外条款

美国《隐私权法》(也称《私生活秘密法》)规定，在紧急情况下，为了某人的健康或安全而使用个人记录的情形下，行政机关公开个人记录无须征得本人同意。另外，美国《健康保险携带和责任法案》规定公共卫生事件属于“国家利益优先”情形，可以不经个人同意而披露及使用健康信息。美国法院在处理数据协助义务案件中一般会应用“第三方原则”，即第三方机构(如医院、电信运营商、保险公司等)应政府部门要求提供其掌握的个人信息，不受美国宪法第四修正案(公民免受无理由搜查和扣押)的限制。〔45〕

3. 我国规范文件中的例外条款

《网络安全法》第42条但书规定“经过处理无法识别特定个人且不能复原的”信息可获得责任豁免。《信息安全技术 个人信息安全规范》有“在与公共安全、公共卫生、重大公共利益直接相关的情形中，数据控制者无须征得数据主体的授权同意”之规定。《传染病防治法》第12条和《国务院突发公共卫生事件应急条例》第11条赋予了有关部门和机构出于疾病防控目的而收集个人信息的权力。《民法典》第1036条规定了包括“个人同意”“维护公共利益”等三种不承担民事责任的信息处理情形。

作为个人信息的伴生概念，举重以明轻，上述保护例外情形自然适用于行为轨迹信息。根据上文的分类认定，私密信息类、敏感信息类、一般信息类行为轨迹信息已经被纳入个人信息范畴，直接适用例外情形；匿名信息类行为轨迹信息已脱敏，数据主体已失去保护权能，只有大数据产品开发者方能提出相应权益主张。另外，在适用例外条款时同样要把握个人信息权益限制的“目的明确”“比例原则”“公开原则”“安全原则”等基本原则。〔46〕

---

〔43〕 参见安徽美景信息科技有限公司、淘宝(中国)软件有限公司商业贿赂不正当竞争纠纷案，浙江省杭州市中级人民法院民事判决书(2018)浙01民终7312号。

〔44〕 参见丁晓东：《论企业数据权益的法律保护——基于数据法律性质的分析》，载《法律科学(西北政法大学学报)》2020年第2期，第90—99页。

〔45〕 参见《专家观“疫”疫情下的数据利用和个人信息保护再权衡》，载新浪科技网，https://tech.sina.com.cn/roll/2020-02-17/doc-iimxyqvz3601138.shtml。

〔46〕 参见韩新远：《收集、使用个人数据宜遵循五项原则》，载《检察日报》2020年3月28日，第03版；李晓楠：《“数据抗疫”中个人信息利用的法律因应》，载《财经法学》2020年第4期，第108—120页。

## 五、结　　语

在数据成为“信息石油”的当下，对个人行为轨迹信息的审视和保护逐渐进入理论研究和司法实践的视野。本文以个人信息概念为参照，从信息权益的逻辑基点“可识别”入手，比照个人信息的识别标准，辨析行为轨迹信息从不可识别到可识别的流变，接着以个人信息所具有的人格、财产利益为抓手，发现行为轨迹信息利益已然获致成为权益或权利的资质和条件，继而引出结论，即应将行为轨迹信息纳入法律评价框架，但并非笼统落入个人信息的保护范畴，而是构建本土化的分类保护模式。

自此，本文对行为轨迹信息法律保护所开展的论证研究暂告一段落，但对行为轨迹信息乃至个人信息的保护治理来言，仅仅是万里长征的第一步，许多问题亟待解决。比如，一般认为匿名原始信息不再属于个人信息，任何组织和个人可自由收集和抓取，并用于合法目的，使之成为一种不受法律保护的一般利益，但识别技术的进步可能使匿名信息被再次识别，〔47〕让人不禁产生隐私权死亡的悲观论断；〔48〕又比如，对个人信息本身的权利性质争论依旧没有定论，〔49〕个人信息的权属问题莫衷一是，〔50〕参照系的摇曳，直接导致对行为轨迹信息相关问题探讨的困惑。上述问题的解决，需要理论与实务两界上下求索，使大数据的运用真正实现“技术归化”，只有这样才能为个人生活安宁、网络企业运营和智慧社会发展提供稳定的心理预期和健全的法律保障。

**Abstract**　In the age of the Internet and digital data, the value of personal behavior track information is highlighted and becomes an important commercial resource. To discuss whether the personal behavior track information should be included in the scope of legal evaluation and legal protection or not, the discussion should be carried out in the light of personal information. Identification is the logical basis of personal information interests. With the change of technology and the evolution of ideas, identification has realized the extension from the identity to the behavior. By examining the identification criteria, the evolution of the individual behavior track information from unrecognizability to identifiability can be sorted out. The personal behavior track information has both the personality interest and the property interest, and has the condition to be upgraded to the rights and interests protected by law. Integrating personal behavior track information into the legal evaluation framework does not mean that it should fall into the legal protection scope of personal information in general, but the tension between data protection and data freedom should be balanced; the localized classified protection mode should be constructed; protection measures with different intensities should be given. At the same time, the bottom line of protecting exceptional cases should be firmly established.

**Keywords**　Behavior Track Information, Personal Information, Identification, Anonymous Information, The Civil Code

（责任编辑：宾凯）

〔47〕 See Paul Ohm, *Broken Promise of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701－1777(2010).

〔48〕 参见[美] A. Michael Froomkin：《隐私权的死亡》，黄淑芳译，载张民安主编：《信息性隐私权研究——信息性隐私权的产生、发展、适用范围和争议》，中山大学出版社 2014 年版，第 253—254 页。

〔49〕 参见前注〔23〕，梅夏英文，第 846—853 页。

〔50〕 参见韩旭至：《数据确权的困境及破解之道》，载《东方法学》2020 年第 1 期，第 97—107 页。