

数据隐私保护的反垄断法适用困境

张晓豪

浙江理工大学法政学院、史量才新闻与传播学院, 浙江 杭州

收稿日期: 2024年3月19日; 录用日期: 2024年4月7日; 发布日期: 2024年5月27日

摘要

数据隐私保护一般被认为属于产品质量和消费者福利的组成部分, 反垄断法的实施对其具有积极的促进作用。然而, 互联网企业的双边市场特性决定其无论提供还是改善服务都离不开数据收集活动。用户则因认知局限和使用偏好致使其无法选择隐私安全程度更高的产品。非价格因素分析范式的缺失导致在隐私保护下降的同时消费者利益是否受损难以明晰。竞争的局限性和法律适用的不确定性导致通过反垄断法保护数据隐私的愿景难以实现, 优先适用数据隐私法处理隐私安全问题是应然选择。

关键词

数据隐私, 反垄断法, 消费者福利, 双边市场, 认知局限

The Application Dilemma of Anti-Monopoly Law for Data Privacy Protection

Xiaohao Zhang

School of Law and Politics, School of Journalism and Communication, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: Mar. 19th, 2024; accepted: Apr. 7th, 2024; published: May 27th, 2024

Abstract

Data privacy protection is generally regarded as a part of product quality and consumer welfare, and the implementation of anti-monopoly law has a positive role in promoting it. The two-sided market characteristics of Internet enterprises determine that they cannot provide or improve services without data collection activities. Users are unable to choose products with higher privacy security due to cognitive limitations and use preferences. The absence of analysis paradigm also makes it difficult to clarify whether consumer interests are harmed while privacy protection is declining. The limitation of competition and the uncertainty of law application make it difficult to

realize the vision of data privacy protection through anti-monopoly law, so it is an appropriate choice to prioritize data privacy law to deal with privacy security issues.

Keywords

Data Privacy, Anti-Monopoly Law, Consumer Welfare, Bilateral Market, Cognitive Limitation

Copyright © 2024 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. 引言

数字化时代，个人信息日益以二进制的数字方式呈现，消费者以自己的隐私数据为对价，交换互联网企业“免费”提供的服务。由此，数据隐私保护与反垄断开始产生交集。而基于数据的重要性和互联网的便捷性，各大数字平台开始逐步降低隐私保护水平，加大对用户数据的攫取力度，如用户在使用腾讯会议时会被腾讯公司收集设备型号、电量及 User ID 等信息并被共享至各大应用市场的运营公司，¹这与《常见类型移动互联网应用程序必要个人信息范围规定》第五条²的规定明显不符。除此之外，当企业收集用户数据后，既可以将其用于正常的经营活动，也可能实施损害用户利益的不当行为，如非法买卖他人个人信息、将用户数据作为价格歧视的工具、限制用户将自身数据转移至其他企业的产品等。

互联网企业之间对用户数据的争夺与利用存在损害消费者利益的可能，其实施的一系列行为也使得消费者对个人隐私安全的担忧不断升级。根据中国质量协会 2020 年开展的中国数字经济服务质量满意度 (DES-CSI) 调查研究显示，58.6% 的消费者在接受数字经济服务过程中有过担心或顾虑，其中 73% 的消费者最担心的是个人隐私安全问题，且对个人隐私安全的评价在所有评价指标中得分最低。³既然获取个人数据已然成为互联网企业提供服务、展开竞争过程中的重要一环，那么作为市场机制基本法律制度的反垄断法，能否直接将互联网企业降低数据隐私保护水平、索取更多用户信息的行径纳入规制范围？笔者拟从现有的理论观点和实践案例出发，结合数字市场竞争特征与反垄断法的价值目标，试图对此问题做出回答。

2. 现有观点分歧：分离模式与统一模式

随着数据驱动型业务的不断涌现，数据隐私问题已经开始为国内外学者和反垄断执法部门所关注。部分观点认为反垄断法应当关注隐私保护等非价格因素(以下称为“统一模式”)，另一部分观点则认为由于价值目标的差异和执法标准的不确定性，数据隐私保护不应当成为反垄断考量因素(以下称为“分离模式”)。到目前为止，针对反垄断法能否直接规制数据隐私问题，理论界与实务界尚未得出一个统一的结论。

2.1. 理论上的分歧

统一模式的主张者认为反垄断法应当关注数据隐私保护，其论点主要有二：一是产品质量本身就包

¹深圳市腾讯计算机系统有限公司：《第三方信息共享清单及 SDK 目录》(2023 年 9 月 13 日)，来源：

<https://privacy.qq.com/document/preview/8f04105d68304fc8b7fa0acd4b991ea>，2024 年 1 月 31 日访问。

²《常见类型移动互联网应用程序必要个人信息范围规定》第 5 条第 26 项：“远程会议类，基本功能服务为通过‘网络提供音频或视频会议’，必要个人信息为：注册用户移动电话号码。”

³中国质量报：《数字经济服务质量满意度大幅提升消费者隐私保护仍是痛点》，来源：

https://www.cqn.com.cn/zgzlb/content/2021-03/23/content_8675562.htm，2024 年 1 月 31 日访问。

括数据隐私,既然产品质量能够在市场竞争中提升,那么隐私保护水平同样能够通过反垄断法促进竞争得以提高[1]。二是认为数据隐私寓于消费者福利之中,企业针对用户所进行的越来越多的数据收集处理行为是消费者福利下降的表现,而消费者福利是现代反垄断法的主要目标之一[2]。也许是出于对反垄断法的信心,目前国内研究者基本都主张适用反垄断法以进一步强化对用户数据隐私权的保障。

支持分离模式的学者则从以下三个方面对其主张进行了论证:一是相较于其他基础性权利和公共政策问题,隐私保护并无特殊之处,如果反垄断法考虑隐私问题可能破坏其分析范式的确定性和专业性[3]。二是如果将隐私作为产品质量的一部分,隐私保护水平的下降程度难以量化,最优的隐私保护水平也难以确定[4],垄断行为的分析结果最终取决于审查机关对待隐私的主观态度,具有很强的不确定性。而且挖掘用户数据就一定对用户有害的观点本身,忽视了企业获得这些数据后改进服务的情形,从结果上看可能阻碍企业的发展与创新,同时对于那些不看重隐私、愿意用自身隐私换取便利与服务质量的消费者而言并谈不上有利[5]。三是适用反垄断法规制需要证明企业的市场支配地位,还需要确立有关数据过度收集、剥削性滥用的判断标准,可操作性不强[6]。

总体来说,统一模式主张将数据隐私保护水平视为产品质量的一部分,而产品质量作为企业之间除价格外另一重要的竞争维度,反垄断法能够通过恢复竞争秩序的方式重启企业在数据隐私保护方面的竞争,从而提升消费者福利。而分离模式的主张则更侧重于反垄断法的功能定位和实际适用过程中的可操作性,以数据隐私保护的非特殊性、操作的高难度性以及结果的不确定性为由,拒绝将数据隐私保护纳入反垄断法规制范畴。

2.2. 实践中的分歧

在实践层面,数据隐私保护已经与反垄断法执法产生了关联,不过就目前而言,将数据隐私保护纳入反垄断法的实践并不成功。绝大部分竞争执法机构都认为两者之间存在明显的界限,应当分别交由数据法和竞争法来解决各自领域内的问题。

从实际案例来看,早在2006年的“Asnef-Equifax案”中,欧洲法院就认为任何可能涉及个人数据敏感性的问题完全不属于竞争法的范畴,应当全部交由数据法规制。⁴这一主张贯穿了欧盟委员会之后处理的案件。在2008年“Google/DoubleClick案”中,欧盟委员会明确表示Google/DoubleClick在数据保护层面应当承担的职责并不在此次竞争评估范围内,委员会仅对该项并购交易是否符合欧盟竞争规则予以评估。⁵在2014年“Facebook/WhatsApp案”中,欧盟委员会指出,合并产生的隐私安全忧患应当属于欧盟数据保护规则的范围,委员会分析潜在的数据集中的目的仅在于审查是否可能加强Facebook在在线广告市场或其任何细分市场的地位。⁶在2016年“Microsoft/LinkedIn案”中,欧盟委员会在假设集中交易导致的数据聚合符合数据保护立法后继续对该行为可能引发的竞争问题进行讨论。⁷换言之,数据聚合行为是否违法应当首先参照数据保护法的相关规定,对竞争问题的讨论应当在行为不违反数据保护法的前提下展开。美国反垄断执法机构对待“Google/DoubleClick案”的态度与欧盟委员会类似。曾有人以数据聚合可能侵害用户隐私为由提议联邦贸易委员会禁止这项交易,但联邦贸易委员会指出:“对并购行为进行反托拉斯审查的唯一目的是识别和救济竞争损害,委员会无权对并购中的企业施加与竞争无关的要求;而且对一家公司的隐私提出监管要求,本身就可能对这个迅速发展的庞大行业的竞争构成严重损害。”⁸

到目前为止,仅德国竞争机构认定Facebook在使用数据方面构成滥用市场支配地位,侵害用户隐私。

⁴See C-238/05, *Asnef-Equifax and Administración del Estado v. Asociación de Usuarios de Servicios Bancarios (Ausbanec)*, [2006] ECR I-11145, para. 63.

⁵See Case M. 4731-Google/DoubleClick (2008), para. 368.

⁶See Case M. 7217-Facebook/WhatsApp (2014), para. 164.

⁷See Case M. 8124-Microsoft/LinkedIn (2016), para. 179.

⁸Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170, December 20, 2007, p. 2.

根据调查，德国联邦卡特尔局发现，Facebook 收集了用户使用 WhatsApp 和 Instagram 时生成的相关数据并将其与自己平台上的用户信息联系起来，但并未将此举告知用户请求其同意。最终联邦卡特尔局确定 Facebook 的行为侵害了用户隐私，构成剥削性滥用。Facebook 案是目前针对数据过度收集问题唯一的反垄断执法案例。

3. 统一模式的适用困境

如果试图利用反垄断法保护数据隐私，那么一个必要的前提是，数据隐私安全是消费者决定是否使用某一产品的重要考量因素，互联网企业提供的产品在隐私保护层面存在差异化竞争且能为消费者所感知。但事实上，由于隐私保护水平的不易感知性和“零价格偏好”，消费者无法对不同程度的隐私政策做出差异化反馈。互联网企业则由于用户数据内涵重要价值而总是倾向于获取更多数据以增强自身竞争力。此外，非价格因素反垄断分析范式的缺失导致消费者利益是否受损难以明晰，反垄断法的适用并不具备确定性。

3.1. 质量竞争损害与评估前提

损害理论是法律分析的基础。反垄断法上的损害指的是竞争损害，我国《反垄断法》将其表述为“排除、限制竞争”。在传统市场，反垄断执法的积极效果大多表现在有关商品或服务的产量更高、价格更低，价格影响因素通常是主要考虑焦点。而随着数字产品“零价格模式”的迅速铺开，反垄断执法对非价格因素的关注度逐步提升。由于质量是消费者除价格外最为重视的属性，因此在评估平台的反竞争效应时，除去价格和产出外，还应该考虑产品的多样性、质量降低以及扼杀创新的风险。⁹

数字市场是典型的“零价格市场”，但数字产品各方面的质量并非都需要被纳入反垄断分析范围。具体而言，判断质量是否属于数字市场竞争中的重要因素可以参考以下几个方面：首先，消费者根据特定产品在某些质量特征方面的差异在不同经营者之间进行选择；其次，相关市场经营者根据竞争者的产品在某些质量特征方面的变化调整自身产品的价格或质量特征；最后，经营者会投资于特定研发，以改善产品的某些质量特征或开发新产品或服务[7]。将这些条件聚焦于数据隐私问题则不难得出这样一个结论：如果隐私保护属于数字市场竞争中一个重要的质量因素，那么数据隐私安全是消费者决定是否选择某一产品的重要因素，互联网企业提供的数字产品在隐私保护层面也应当存在差异以满足不同的隐私保护偏好。但细看竞争激化情形下互联网企业与用户的反应可以发现，数据隐私保护难以纳入产品质量的考量范围，竞争规律在促进隐私保护水平提升中发挥的作用相当有限。

3.2. 竞争激化下互联网企业弱化隐私政策

双边市场特性是互联网企业的显著特征，这使得平台其在服务提供与市场竞争中离不开对数据的收集和使用。大多数情况下，更好的预测、匹配水平都与更多的数据量挂钩，这导致互联网企业需要大量隐私数据为日益激烈的竞争水平做支撑，提高隐私保护水平并非其首要考量。

用户数据对互联网企业的重要性至少表现在三个方面。第一，互联网企业利用用户数据投放个性化定制广告，直接创造利润，这也是非交易型平台¹⁰最主要的盈利方式。互联网企业的商业模式普遍具备双边市场特性，第三方在线广告商则是该模式中最常见的支付经济费用的一方。相较于传统的广告投放模式，个性化定制广告通过隐私数据推算用户喜好并向其推送相应广告，极强的针对性可以显著减少广

⁹KFTC Establishes Guidelines on Anticompetitive Conducts in the Platform Sector, https://www.ftc.go.kr/solution/skin/doc.html?fn=3f6848cbcadf63a97f87accd6400b8ce5d2b65a537490de4adc0313932e2cc2&rs=/fileupload/data/result/BBSMSTR_000000002402/, last visited on 31 January 2024.

¹⁰在非交易型平台中，由平台分别向双方收取一定费用，平台上的参与者之间则不会直接发生交易关系。浏览器、视频软件均属于非交易型平台。

告商的投放费用和用户接收广告时的反感度，从而提升广告效果，助推广告商利益的实现。在“谷歌比价购物案”中，欧盟委员会认为，虽然用户不用为使用一般的搜索服务支付金钱，但他们每次查询而留下的数据，为企业盈利做出了贡献。¹¹ 第二，互联网企业利用用户数据改善服务。通过分析用户的使用历史、评价、反馈等信息，企业可以更好地迎合用户需求，进一步改进自身服务，提供更高质量的产品。如滴滴打车等网约车平台可以通过记录、分析用户的用车偏好、行程轨迹等信息，进而优先为用户呼叫其常用车型并实时改进导航路线选择，甚至实现实时的行车路线优化。此种情况下，个人信息构成在线服务的关键投入品[8]，是确保互联网企业能够长期良性运营的重要资源。第三，互联网企业利用用户数据拓展业务领域，助推企业系统化、平台化。数字经济时代，互联网企业之间的竞争激烈非常，业务的系统化、平台化使得用户只需注册一个账号就可以使用数个同一平台推出的软件服务，提升使用体验与用户粘性。如果缺乏用户数据的积累，跨领域的业务经营将困难非常，无论是自行整合、搭建平台业务还是接入其他大型互联网企业现有业务都将举步维艰。

在互联网发展的早期阶段，平台用户只需允许企业收集个人 ID、手机号等必要基础信息，完成账号注册即可享受互联网企业提供的全部服务。这既是因为初期的市场竞争并不激烈，也是互联网企业为了尽可能扩大受众规模而有意为之。但在数字经济急速发展的今天，为了扩大竞争优势，数字平台往往需要更多的数据来实现更好的交易匹配和预测。就打车平台而言，互联网企业所提供的网约车服务与传统的出租车公司相比在服务质量上并无明显差异，两者最大的区别在于通过互联网带来的信息匹配成本的下降。在网约车平台上，乘客可以自主预约用车的时间和地点并选择心仪的车型，司机则可以通过平台智能接单，缩短空窗期时间。在这些环节中，信息匹配得越准确，乘客和司机的使用体验越好，平台的竞争优势才得以体现。而为了实现这种精细化的匹配，收集并分析大量用户数据是不可或缺的一环。可以说，现阶段企业的竞争力越来越多地依赖于及时获得有关数据和利用这些数据开发新的创新应用程序和产品的能力。¹² 正是基于这样的逻辑，腾讯公司才会从腾讯 QQ、微信等消费者使用频率较高的即时通讯类软件入手，将业务逐渐拓展至音乐、办公、地图等领域，并与其他第三方平台共享信息。通过这样的拓展和合作，腾讯公司能够获得更多数据样本，从而将其他竞争对手甩在身后，成为行业的领头羊和常青树。尽管也存在一些企业在隐私保护层面展开竞争的案例，如搜索引擎 Duck-DuckGo 主推隐私增强保护功能并承诺不会以任何方式“跟踪”用户[9]，HushMail、RiseUP 和 Zoho 等免费电子邮件提供商也在隐私保护方面展开竞争，以便将自己的服务与 Gmail 等相区分[10]。但是受制于前述互联网企业的商业模式，这种竞争在今天并不普遍，也不激烈。

3.3. 消费者的选择困境

消费者是市场竞争中的重要参与者，如果他们对平台降低数据隐私保护水平的行为表现出极大反感，可以预见互联网企业一定会致力于加强隐私保护以增加对用户的吸引力。但由于难以真正了解互联网企业实际的隐私保护水准，加之自身对隐私保护的偏好不足，隐私安全无法成为消费者选择产品时的决定性因素。

首先，消费者难以通过隐私条款感知保护水平差异。用户与互联网企业在数据交易过程中存在明显的信息差异[11]，具体表现为用户在使用数字产品前会收到一份由互联网企业单方拟定的隐私政策条款，且用户只能选择同意与否而无法对其进行修改。甚至在大多数情况下，用户如果不同意协议内容将无法使用该软件。此外，互联网企业提供的隐私协议大都条目繁多且内容晦涩，几乎没有用户愿意逐字逐句阅读并充分理解其涵义。一项测算显示，对于一个普通用户而言，如果真的去仔细阅读每一个所登陆网

¹¹See CASE AT.39740-Google Search (Shopping) (2017), para. 320.

¹²See European Commission, Competition Policy for the Digital Era, p. 73.

站给出的隐私协议条款,平均每年要花费 244 小时,足足占据了其上网总时长的一半以上。¹³退一步讲,即便确有用户能够浏览全部的隐私政策,其也可能因缺乏专业知识而无法理解其中内容,且协议的最终解释权也不在用户手中。以上种种因素导致用户无法通过阅读隐私条款评估企业的隐私保护水平。

第二,消费者在产品使用过程中难以感知隐私保护水平差异。由于隐私数据的重要性,大部分国家都要求数据的采集需要被收集者同意;但也由于这种重要性和程序的复杂性,企业往往会隐蔽地搜集并不真的寻求用户的同意[12],而对于隐私数据的收集可以通过技术工具非常隐蔽地完成。用户如果试图保护数据隐私,那么他必须知道企业到底于何时通过何种方式采集了何种数据信息,但是基于双方的技术差距,用户根本无法察觉和控制企业的数据收集行为。此外,基于工作学习的需要,一个用户通常同时使用数十个平台的软件,接受数家互联网企业提供的服务。即使发现疑似侵害数据隐私、违法违规收集数据的行为,用户也需要花费极大的时间与精力调查究竟是何者所为,维权的难度和成本都非常之大。故而在现实情境中,用户难以了解自身隐私是否被侵犯以及被何者侵犯,隐私保护水平的难感知性导致消费者无法针对不同的隐私政策做出差异化反馈。

第三,隐私保护并非消费者选择数字产品的首要考量因素。虽然绝大部分用户看上去都十分关注隐私安全,但在产品选择过程中,他们的首要关注点仍在于数字产品的价格与便利性。诺顿 LifeLock 曾对超过 1000 名中国成年人进行了线上调查,结果显示,尽管 91%的中国用户对于自身的隐私安全表示担忧,但高达 62%的用户依旧愿意承担一定隐私泄露的风险以追求便利,其中包括互联网搜索历史和位置信息,有些受访者甚至愿意提供身份证明文件。¹⁴究其原因,自互联网发展的早期阶段开始,企业向个人消费者提供的产品大都是“零价格”的,甚至目前这类“零价格”服务模式仍是主流。多年的使用习惯导致消费者在选择产品时偏好“零价格”而反感正价格。只要产品的使用对价不表现为货币价格,即便用户在付出数据隐私,他们也可以接受。调查显示,54%的中国消费者不愿意在使用社交媒体时向供应商付费以确保他们的个人信息被妥善保护。¹⁵相较于隐私保护水平上的差异,用户通过不自觉地付出隐私换得的产品使用便利性上的提升可以更明显地被感知。基于上述原因,用户在实际选择产品过程中对隐私保护的重视程度远不如价格和便利性,隐私安全差异很难成为其选择或放弃某个产品的关键原因。

3.4. 缺乏反垄断分析工具

在数据隐私保护中,有不少学者持这样一种观点:在零价服务模式流行的数字经济时代,个人信息保护虽未必具有取代价格的地位,但在数字时代至少与价格同等重要,二者共同构成消费者福利的两大核心内容[2]。但当前将数据隐私纳入反垄断保护存在分析方法上的困难,这也是统一模式面临的最直接的难题。

首先,保护消费者利益并非反垄断法唯一的价值追求,隐私保护水平下降不意味着反垄断法必然介入。反垄断法之所以被冠以“经济宪法”、“自由企业大宪章”的称号并不是因为它保护消费者,而是因为其有助于维护企业自由和经济民主。正如美国联邦最高法院指出,“反垄断法,尤其是《谢尔曼法》,是自由企业的大宪章。它们对于保全经济自由及我国自由企业系统的重要性与权利法案对于保护我国基本个人自由的重要性不相上下。”¹⁶除消费者利益外,受竞争机制作用的市场经济还可以带来其他多种利益,例如经济分析揭示出垄断造成无效率,而竞争促进效率,从而保护竞争、反对垄断与提高经济效

¹³European Data Protection Supervisor, *Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection*, 2014, p. 2.

https://www.edps.europa.eu/sites/default/files/edpsweb_press_releases/edps-2014-06-big-data_en.pdf, last visited on 31 January 2024.

¹⁴《网络安全报告:中国消费者隐私意识居全球前列》,来源:<http://it.people.com.cn/n1/2019/0409/c1009-31020946.html>, 2024 年 1 月 31 日访问。

¹⁵《网络安全报告:中国消费者隐私意识居全球前列》,来源:<http://it.people.com.cn/n1/2019/0409/c1009-31020946.html>, 2024 年 1 月 31 日访问。

¹⁶United States v. Topco Assocs. Inc. 405 U.S. 596, 610 (1972).

率三者被联系起来。我国反垄断法在制定时，除保护消费者利益外也提出了保护竞争、鼓励创新、提高效率等其他目标，体现出多元化的价值取向。这意味着在适用反垄断法时，不能将其中一种价值目标至高化或绝对化，更不能以其作为反垄断法介入的唯一标准。倘若隐私保护方面的损失小于其他层面所得的收益，则该行为未必构成对反垄断法的违反，执法机构也无法就该行为进行介入。

第二，缺乏系统客观的评价范式，消费者利益是否受损难以明晰。不同于价格因素可以通过货币单位和经济学分析范式进行客观衡量，包括产品质量在内的所有非价格因素都具有一定的主观性，缺乏客观明确的判断标准。尽管有学者提出对于质量分析可以采用 SSNDQ 测试，以替代价格分析的 SSNIP 测试来界定相关市场[13]，但隐私损害如何衡量的难题仍未得到解决。这种分析方法上的不确定性造成了反垄断执法标准的模糊性。另外，数据隐私受损并不能简单地与消费者利益受损划等号。反垄断法维护消费者利益包含两层含义。一层是抽象的消费者利益，凡是市场竞争机制能够为消费者带来的利益都可以归入此范畴。另一层是具体的消费者利益，也即在认定垄断行为时需要考虑的特定且具体的消费者利益，通常表现为价格、质量等，数据隐私亦可以被包含于此范畴。需要注意的是，消费者利益的内涵不仅包括数据隐私，加大对用户数据的收集力度虽然意味着数据隐私保护水平的下降，但往往也伴随着使用便利性的上升，消费者利益最终是否受损并不明确。亚马逊一直致力于通过大数据分析为定位顾客和获得顾客反馈而努力，而所有业务流程都离不开“数据驱动”的努力。推荐功能(购买 x 的消费者搭配购买了 y)看似简单却非常有效，而得出这种正确推荐结果的过程需要非常复杂的数据测算；预测功能则是通过过去的用户数据预测未来用户的需求，当前算法下，该功能对于书籍、手机、家电等产品的预测非常精准。对亚马逊来说，大数据意味着大销量，对数据的持续关注可以使亚马逊以更低的价格提供更好的服务。综上所述，消费者福利是否受损需要结合其中各项利益进行综合考量后作出判断，而在非价格因素判断标准不明确的前提下，针对数字市场中消费者利益的分析衡量在实际操作过程中注定是举步维艰。

4. 反垄断与数据隐私保护困境之解决

4.1. 分离模式的比较优势

相对于统一模式下反垄断法介入前置条件的不足和非价格因素分析范式的缺失，分离模式可以使反垄断法与数据隐私法在实际执法过程中摆脱彼此的桎梏，具有更强的可操作性，也更有助于促进反垄断与数据隐私保护双重目标的实现。

第一，分离模式下反垄断法与数据隐私法能够继续专注于各自的价值目标，延续并发展各自之前的分析方式，增强执法过程中的可操作性。数字经济的快速发展带来的新问题，诸如相关市场的界定、竞争损害分析、损害赔偿数额认定等，已经为新时代反垄断法的实施提出了不小的挑战。当前我国对于数字平台的治理尚处于探索阶段，各项法律、政策更新的速度远不及数字经济日新月异的发展来得迅速。在这一前提下，分离模式理论使得反垄断法不必专注于主观性较强的隐私保护因素，而可以聚焦于相关市场界定等传统分析要件在数字市场所遭遇的障碍与完善路径，进而发展出针对数字平台的更有效的分析执法工具，增强传统反垄断分析工具在数字经济时代的可操作性。同样，分离模式下的数据隐私法也具备更强的可执行性。抛开反垄断因素，判断互联网企业是否履行了法定的数据隐私保护要求、消费者的隐私利益是否受到侵害并不存在分析方法上的困难。民法典“隐私权和个人信息保护”一章不仅对隐私和个人信息的基本概念进行清晰划分，也确定了侵害隐私权的行为类型、处理个人信息应遵循的原则与合法性要件、个人信息的合理使用，更对隐私权和个人信息保护的关系问题作出了规定。数据安全法和个人信息保护法的出台也意味着我国已经初步建立了个人信息保护的法制保障，在信息保障方面建立起较为完善的体系。倘若某一数字平台未能充分尽到保护用户数据隐私的义务导致用户信息泄露，监管机构可以直接依据相关法律责令行为主体限期改正，用户也可以通过举报、诉讼等方式寻求对个人隐私

利益的救济。

第二，分离模式有助于促进反垄断与数据隐私保护双重目标的充分实现。当反垄断与隐私保护两大价值目标相冲突时，如大型数字平台以数据隐私保护为由拒绝将数据交易交给中小企业使用，相较于统一模式下对双方利益进行抽象的比较考量并作出取舍，分离模式下可以就拒绝交易与隐私保护不足的问题进行分别执法，推动反垄断与数据隐私保护在价值目标上的“双赢”。针对交易相对人数据安全程度不足的问题，监管机关可以依据数据隐私法要求其履行法定的隐私保护义务，责令其提供不低于法定水平的数据隐私保护服务。而对于数字平台拒绝数据交易流通的行为，应当由反垄断法执法机关根据拒绝交易的行为要件判断案涉行为是否属于垄断行为，数据隐私保护水平不足不能够成为大型数字平台拒绝数据交易流通的正当性事由。而当反垄断与隐私保护两大价值目标一致时，数据隐私保护执法则可以提高执法效率，更好地保护消费者利益。如果数个互联网企业通过协议的方式集体降低数据隐私保护水平，一旦其提供的隐私保护未达到法定标准，相较于反垄断法执法机关需要启动冗长的调查程序，数据隐私监管机关可以直接介入责令其改正，并与反垄断法相配合，在更迅速及时保护用户隐私利益的同时打击垄断行为。

4.2. 采取分离模式处理反垄断与数据隐私保护的关系是应然选择

结合统一模式与分离模式的优劣以及目前的执法实践，采取分离模式分开解决反垄断与数据隐私保护问题应当成为处理两者间关系的应然选择。如前文所述，从数字市场竞争现状来看，由于消费者对隐私保护的感知不明显且偏好不足，加之数据隐私价值对于互联网企业发展的重要性，现阶段各大数字平台在隐私保护方面展开竞争的程度并不激烈，甚至存在向底部竞争的现象，数据隐私保护难以成为产品质量竞争损害评估的一个方面。从反垄断分析工具来看，隐私保护作为非价格因素具备极强的主观性，而当前反垄断法缺乏相应的分析范式，将数据隐私保护纳入反垄断考量缺乏可操作性，增加了执法的不确定性。相较之下，分离模式建立在延续两者既有执法模式的基础上，具备更强的可操作性，也更有助于实现各自的价值目标。同时，尽管学界对将数据隐私保护纳入反垄断法的呼声络绎不绝，但是各国目前的执法实践来看，除去德国的 Facebook 一案，优先适用数据隐私法处理隐私保护问题仍是主流模式。综合以上因素，我国反垄断法不宜将数据隐私保护纳入考量范围。不论在现实中两者利益是一致还是相冲突，都应当强化在各自领域内的执法，以期共同促进互联网行业的健康发展。在反垄断法之外强化数据隐私保护，应当是更恰当的维护用户隐私利益的方式。

5. 结语

竞争虽然是市场经济不可或缺的因素但也并非全能，数据隐私不能当然地认为可以通过促进竞争的方式予以提升。通过观察互联网企业与消费者的行为模式，不难发现二者对于数据隐私的重视程度均远不如价格、便利性等其他因素，竞争机制在数据隐私保护方面难以有效发挥作用。在非价格因素分析范式尚未确立的情况下，适用反垄断法保护数据隐私存在理论与实践的双重困境。事实上，恰恰是基于对用户和互联网企业之间不平等地位的考量以及市场机制在隐私保护中存在的不足，具备更强可执行性的个人信息保护法、数据安全法等数据专门立法才相继出台，以直接明确信息收集者的权利义务、规范个人信息处理活动的原则和方式。在数据隐私保护日益强化的背景下，这种分离的执法模式应当是我国处理隐私与竞争两者关系的更好选择。

参考文献

- [1] 杨东. 论反垄断法的重构: 应对数字经济的挑战[J]. 中国法学, 2020(3): 206-222.

- [2] 焦海涛. 个人信息的反垄断法保护: 从附属保护到独立保护[J]. 法学, 2021(4): 115-120.
- [3] Lamadrid, A. and Villiers, S. (2017) Big Data, Privacy and Competition Law: Do Competition Authorities Know How to Do It? *CPI Antitrust Chronicle*, **1**, 343-345.
- [4] Schepp, N.-P. and Wambach, A. (2015) On Big Data and Its Relevance for Market Power Assessment. *Journal of European Competition Law & Practice*, **12**, 291-293.
- [5] Cooper, J.C. (2013) Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity. *George Mason Law Review*, **4**, 1129-1133.
- [6] Kerber, W. and Zolna, K.K. (2022) The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law. *European Journal of Law and Economics*, **54**, 235-237.
- [7] 韩伟. 数字市场经营者集中的质量效应评估: 以成瘾性为例[J]. 中国社会科学院大学学报, 2022, 42(5): 70-71.
- [8] Geradin, D. and Kuschewsky, M. (2013) Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue. <https://ssrn.com/abstract=2216088>
- [9] Dnes, S. (2021) Browser Tying and Data Privacy Innovation. <https://ssrn.com/abstract=3867625>
- [10] Farrell, J. (2012) Can Privacy Be Just Another Good? *Journal on Telecommunications and High Technology Law*, **3**, 256-259.
- [11] 张占江. 个人信息保护的反垄断法视角[J]. 中外法学, 2022, 34(3): 690-691.
- [12] 李剑. 互联网反垄断能促进数据隐私保护吗? [J]. 商业经济与管理, 2021(5): 94-96.
- [13] 丁晓东. 论数据垄断: 大数据视野下反垄断的法理思考[J]. 东方法学, 2021(3): 115-117.