数据隐私保护的反垄断法剖析:适用困境与纾解之道

林燕萍,罗丹睿
(华东政法大学 国际法学院,上海 200042)

摘要:在平台经济背景下,传统隐私权无法满足个人对其个人数据控制的需求,因此,数据隐私的概念应运而生。隐私作为重要的竞争参数,属于消费者福利的一个关键维度,可以被视为消费者支付的对价或是质量的体现,从而纳入反垄断法的竞争分析范畴。然而,数据隐私保护与效率、创新之间的平衡相当复杂,隐私保护在一定程度上可能会限制数据流动;隐私保护法和反垄断法在数据隐私保护领域的交叉也带来了规则竞合的难题;数据隐私的损害难以量化,传统反垄断法的价格中心方法无法直接适用。欲纾解此困境,应当首先确立审慎干预的适用原则,树立市场竞争与隐私保护的兼顾目标;根据侵犯数据隐私的具体行为和情景适用规制方式,合理权衡所涉利益的保护需求;在此基础上优化隐私保护分析工具,创新反垄断法保护的理论工具。

关键词:数据;数据隐私;隐私保护;数字平台;反垄断法

中图分类号:D922.294 **文献标志码**:A **文章编号**:2096-028X(2024)01-0064-11

一、问题的提出

近年来,伴随着互联网、移动智能终端的快速发展,中国平台经济发展势头迅猛。用户的个人数据作为平台经济的核心要素,被数字平台经营者广泛收集并用于市场竞争。这些流通中的个人数据承载着用户的隐私利益,涵盖了用户的人格权和财产权,必须得到妥善的保护。数据隐私保护问题本属于数据保护法和个人信息法的范畴,近年来亦逐渐受到了一些国家、地区的反垄断执法部门的关注。例如,“Microsoft 收购 LinkedIn 案”①以及德国的“Facebook 案”②都涉及数据隐私保护与反垄断法的交叉问题,这些执法案例也引发了美国、欧盟等国家和地区反垄断执法机构对于“反垄断领域的隐私保护问题”的讨论和思考。在数字经济时代,如何在竞争法框架内更好地处理数据隐私问题成为亟待解决的挑战。

对于数据隐私保护问题是否应该纳入反垄断法分析框架,学界和业界尚存在较大争议。一方面,用户数据的获取、存储和使用已经成为数字经济下的通用商业模式,数字平台企业通过大量收集用户数据获取丰厚的利润的同时也利用数据提高服务水平,更好地满足消费者的需求。另一方面,数字平台企业大量收集数据也对用户的隐私权造成了威胁,而隐私权涉及消费者的尊严和自由,保护隐私是人类与生俱来的需求。尽管《中华人民共和国个人信息保护法》(简称《个人信息保护法》)、《中华人民共和国数据安全法》(简称《数据安全法》)等法律已经专门对于公民的隐私权进行保护,但当隐私成为企业市场竞争的一个重要参数或者当企业利用自身的市场支配地位实施侵害隐私的行为时,数据隐私保护问题与反垄断法之间的联系就尤为紧密而复杂。

二、反垄断法保护数据隐私的应然性分析

大数据时代,平台、算法、数据三元融合的特征也让隐私保护与反垄断法产生交集,三大垄断行为中都可

收稿日期:2023-07-04
基金项目:2022年度国家社科基金青年项目“智慧司法的伦理风险及其应对研究”(22CFX079)
作者简介:林燕萍,女,华东政法大学国际法学院教授、博士生导师;罗丹睿,女,华东政法大学国际法学院国际竞争法专业博士研究生。

① Case M.8124-Microsoft/LinkedIn, Decision of European Commission, 6 December 2016.
② Case KVR 69/19-Facebook, Decision of 23 June 2020.

能出现侵害数据隐私的行为。

(一)数据隐私保护纳入反垄断规制的理论与实践

数字经济条件下,企业的市场行为与用户的数据已经密不可分,然而一些新型的垄断行为如算法共谋、数据驱动型集中以及算法价格歧视,都可能涉及到数据用户的隐私问题。

在学理方面,对反垄断法是否需要将数据隐私纳入规制范围产生了较大争议,持支持观点的学者认为,数据隐私属于消费者福利。① 根据《中华人民共和国反垄断法》(简称《反垄断法》)第 1 条的规定,"维护消费者利益"是《反垄断法》的一项重要立法目的。如在算法价格歧视等经营者利用算法工具侵害消费者利益的垄断行为中,前者通过数据分析与挖掘测定消费者对商品或服务的最大支付意愿,不仅在过程中可能涉及到侵犯用户隐私信息,同时其对消费者支付意愿的测定结果也可被纳入隐私的范畴。② 因此,《反垄断法》具有保护数据隐私的必要性。而持反对观点的学者则认为,隐私保护与反垄断法的宗旨明显不符,作为"市场经济宪法"的反垄断法旨在维护市场竞争秩序,而隐私法是民法的一项制度,其以保护个人私权利为目标。③ 此外,还有学者从竞争执法的角度提出,倘若将数据隐私纳入反垄断法规制范畴,在经营者侵犯用户数据隐私时如何测定其反竞争效果将面临难题,概因为隐私具有高度主观性,其并不像传统竞争效应分析中商品或服务的价格那般具有客观性与可量化性。④ 要将隐私纳入规制范围必须要遵循反垄断法"保护市场公平竞争"的主要目标,然而如何从隐私维度去评测经营者行为对市场竞争的影响是一大难题。

在立法方面,各反垄断辖区不断提高对用户数据隐私保护的重视,这主要体现在"数字市场守门人"制度当中。德国于 2021 年通过了《反限制竞争法修正案》(数字化的竞争法 4.0),欧盟也于 2022 年 7 月批准《数字市场法案》,在这两部法案当中,无论是单一主权国德国规定的"对跨市场竞争具有重大意义的公司"还是欧盟法案中规定的"数字市场守门人",立法都为其设定了一系列义务,其中禁止自我偏好、拒绝互操作性等义务都与数据隐私保护相关。⑤ 2021 年 10 月,国家市场监管总局发布《互联网平台落实主体责任指南(征求意见稿)》以及《互联网平台分类分级指南(征求意见稿)》,也在"公平竞争示范"等条款中规定了"无正当理由,不使用平台内经营者及其用户在使用平台服务时产生或提供的非公开数据"等内容,被称为"中国版的数字市场守门人制度"。⑥ 由此观之,在立法实践中,各个国家和地区立法或反垄断执法机构已经考虑到对数据隐私的保护。

在执法方面,各个国家和地区对涉及到消费者数据隐私的新型垄断行为的执法存在差异。在欧盟的一些案例中,虽然考虑到隐私对竞争的影响,但并未将纯隐私问题直接纳入反垄断法分析框架。例如,在"Google 与 DoubleClick 合并案"⑦中,尽管欧盟委员会考虑到合并可能会造成消费者数据库的合并,从而建立个人的超级档案,但是最终还是无条件地批准了并购交易,并指出在反垄断法中不应当考虑任何隐私问题。在"Facebook 与 WhatsApp 合并案"⑧中,欧盟委员会认识到隐私正在成为消费者通信服务领域竞争的一个相关参数,该交易可能导致 Facebook 控制范围内的数据日益集中,但强调其在用户数据集中分析方面仅关注竞争而非隐私问题,由此产生的一切隐私损害都不应该以反垄断法来调整。然而,在一些案例中,如"Microsoft 收购 LinkedIn 案",欧盟委员会考察了合并对于市场上具有更高隐私保护水平的企业的影响,并认定合并可能会使得隐私级别更高的企业被边缘化或者难以进入市场,它并未将纯粹的隐私问题纳入反垄断法分析框架,而是将数据隐私保护水平的降低看作是竞争性损害的一种,这表明欧盟反垄断执法机构已经

---

① 参见任超、李雅瑜:《数字经济时代数据隐私的反垄断保护:理论证成、适用困境及破解之道》,载《重庆邮电大学学报(社会科学版)》2023 年第 4 期,第 66 页。

② 《中华人民共和国民法典》(简称《民法典》)第 1032 条第 2 款规定:"隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。"从这一界定中可以认为消费者对商品或服务的支付意愿也属于其不愿为他人知晓的私密信息。

③ Noah Joshua Phillips, *Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy*, Federal Trade Commission(30 January 2020), https://www.ftc.gov/system/files/documents/public_statements/1565039/phillips_-_stanford_speech_10-30-20.pdf.

④ Nils-Peter Schepp & Achim Wambach, *On Big Data and Its Relevance for Market Power Assessment*, Journal of European Competition Law & Practice, Vol.7: 120, p.124(2016).

⑤ 参见袁嘉:《德国数字经济反垄断监管的实践与启示》,载《国际经济评论》2021 年第 6 期,第 67-68 页。

⑥ 参见薛克鹏、赵鑫:《平台反垄断规制理念转型的制度障碍及破解》,载《探索与争鸣》2022 年第 7 期,第 57 页。

⑦ Case No COMP/M.4731-Google/DoubleClick, Decision of European Commission, 11 March 2008, para.368.

⑧ Case M.7217-Facebook/WhatsApp, Decision of European Commission, 3 October 2014, para.164.

将第二种数据隐私损害行为纳入了反垄断审查之中。至少在欧盟竞争法视野下,当对涉及数据聚集的经营者集中进行竞争影响评估时,数据聚集是否会减损隐私保护水平已成为一个考量因素。

(二)保护数据隐私符合反垄断法的立法宗旨

在探讨数据隐私保护纳入反垄断规制的理论与实践后,不难发现,随着数字经济的发展,隐私保护逐渐成为反垄断法领域不可忽视的议题。然而,将隐私保护与反垄断法相结合是否切实可行,以及如何在法律层面确立这种结合的原则和方法,仍是一个充满挑战的议题。

第一,多国将保护消费者利益作为反垄断法目的。《反垄断法》第1条明确指出其制定之目的在于减少乃至杜绝垄断行为,促进市场公平竞争,提高经济效率,维护消费者利益和社会公共利益以及市场经济的健康稳定发展。由此可见,中国的反垄断法采取的是多元目标的立法模式,不仅注重市场公平竞争,还强调保护消费者的权益。

第二,消费者利益中包含非价格利益。现行的反垄断法通常使用消费者福利标准来保护消费者权益。该标准有两种解释:一种是强调经济效率的总体福利标准,[①]即芝加哥学派所倡导的,侧重于社会总体福利,包含生产者剩余和消费者剩余,但不考虑消费者和生产者之间如何分配福利;另一种则申明消费者利益不包含生产者剩余,强调福利向消费者一侧倾斜,以价格利益为主,辅之以消费者的其他非价格利益。[②] 一般认为,后者更具有正当性、可行性,其强调不损害消费者的利益,在此基础上提升经济效率,生产者的福利如果是以消费者的利益受损为前提的,则可能违反反垄断法从而受到规制。数据隐私作为一个重要的非价格利益因素,对于消费者利益具有重要影响。

第三,数据隐私是数字经济市场中重要的竞争参数。在用户满意度、更新迭代速度、使用便捷度、隐私保护力度以及广告投放量等衡量质量的指标中,反垄断执法机构应当尤为关注数据隐私保护水平。[③] 消费者数据构成了在在线市场上所支付的实际"价格",与"隐私计算"的经济概念密切相关。消费者在进行在线交易或选择免费在线服务时,会权衡披露数据的成本和利益,以最大化收益。[④] 因此,将消费者为免费服务支付的"信息价格"与数据隐私保护的成本进行比较,可以理解为数据隐私保护的损失等同于价格的增加。

(三)反垄断法适用的必要性与可能性

在立法价值相符的基础上,进一步审视反垄断法在保护数据隐私方面的必要性与可能性,可以得出反垄断法适用的应然性。

1.必要性:市场机制并未回应消费者的隐私期待

消费者具有强烈的隐私关切,但是市场却可能由于缺乏有意义的竞争而无法提供消费者期待的隐私保护水平。[⑤] 首先,企业缺乏在隐私维度展开竞争的动机。理论上,消费者应该能够约束企业收集和使用消费者个人信息,即消费者可以自由选择和转换企业使用其数据的方式。然而,若消费者不了解数据的收集、使用和价值,其在考虑隐私问题时难以作出明智决策,就会减少企业在隐私领域的竞争动机。

其次,市场中竞争不充分,少数数据驱动企业主导市场,难以提高隐私保护水平。这些企业缺乏提升隐私保护的激励,加之竞争压力较小,又存在网络效应[⑥]和锁定效应[⑦],即使不具备消费者期待的隐私保护水平,也不担心消费者的流失,因为市场上没有提供较高级别的隐私保护水平的竞争替代选项。当数据驱动型

---

① Heyer Kenneth, *Consumer Welfare and the Legacy of Robert Bork*, The Journal of Law and Economics, Vol.57: S19, p. S25(2014).

② Robert H. Lande, *Proving the Obvious: The Antitrust Laws Were Passed to Protect Consumers (Not Just to Increase Efficiency)*, Hastings Law Journal, Vol. 50: 959, p.962 (1998).

③ 参见殷继国:《大数据经营者滥用市场支配地位的法律规制》,载《法商研究》2020年第4期,第75页。

④ Tamara Dinev & Paul Hart, *An Extended Privacy Calculus Model Fore-Commerce Transactions*, Information Systems Research, Vol.17: 61, p.62 (2006).

⑤ 参见[美]莫里斯·E.斯图克、[美]艾伦·P.格鲁内斯:《大数据与竞争政策》,兰磊译,法律出版社2019年版,第61页。

⑥ 网络效应(也称网络外部性或需求方规模经济)是一个经济学术语,用于描述对于一个产品(或服务),每增多一名用户,都会对该产品的其他用户产生新的价值。当网络效应出现时,产品(或服务)的价值会随着使用该产品(或服务)的人数的增加而增加。

⑦ 经济学家阿瑟·沃德(Arthur Ward)基于产业集群在其生命周期演进过程中产生的一种"路径依赖"现象提出了"锁定效应"。新推进市场的产品采用了新技术,而新技术有收益递增的特征,而且能实现自我增强的良性循环,从而在竞争中取胜;而另外一种技术更具优势的产品,由于晚到一步,即便技术有优势,但市场中的消费者已经在使用先进入市场上的产品,而且习惯了该种产品,进入到"舒适区",被该种产品"锁定"了,不太容易接受另一款后进入的产品,而这款后进入的产品由于没有足够的支持者而被挤出市场。

企业市场势力足够强大，很可能会忽视消费者在隐私保护方面的偏好。

最后，即使位于市场上的企业未提供符合期待的隐私保护水平，也不一定会吸引新企业进入或促使其他企业提供差异化的隐私服务以改善局面。有学者提出一种“失常均衡”的状态，即市场上企业对于隐私的保护级别很低，缺乏监测承诺执行能力，导致消费者感到失望并对企业信任不足。① 即使新进企业或小企业希望通过提供更好的隐私保护水平来破坏这种平衡，隐私政策也可能无法对消费者的购买决策或产品价值感知起主要作用，从而难以在市场机制失灵的情况下推动需求转向。

概言之，尽管消费者期望通过市场提升企业的数据隐私保护水平，市场的竞争机制却可能无法实现这一期待。企业的竞争动机有限，市场竞争不足，导致隐私维度的竞争难以展开。此问题常被反垄断执法机构忽视，但消费者仍期待市场能在隐私保护方面发挥积极作用，反垄断法或许能提供解决该问题的新的视角。

2.可能性：以反垄断法保护数据隐私的优势

由于隐私保护在市场中可能受到限制，所以需要借助反垄断法的优势来保护数据隐私。

第一，反垄断法在激励企业在隐私维度展开竞争方面具有潜在优势。在市场竞争中，消费者的选择权和信息透明度至关重要。然而，在“失常均衡”状态下，用户对市场上企业的数据使用行为产生不信任感，即使一些企业希望通过提高隐私保护水平来参与竞争，消费者也不愿意相信企业能兑现自己的隐私保护承诺，因此它们也无法获得原本在一个有效竞争的市场上所能看到的消费者需求转向，这将阻碍企业采取更多的保护政策和更清晰的披露来吸引用户。在这种情况下，反垄断法可以通过创造竞争隐私的动机，激励企业将积累数据的一些外部性内部化给其他消费者和整个社会，有助于企业更积极地采取保护政策和更清晰的披露，吸引用户，并创造有利于整个社会的数据使用环境。

第二，反垄断法的事前审查机制可以在保护数据隐私方面发挥预防性作用。在大数据时代下，数据驱动型企业围绕着个人数据展开激烈的角逐，以合并数据库为目的的数据驱动型经营者集中案例在国内外频频上演，如果在合并审查中事先考察合并对于消费者隐私的影响，则能够使事前和事后规制相结合，更好地保护消费者的个人信息安全。《反垄断法》规定满足特定条件的经营者集中必须要事先履行申报程序，反垄断执法机构按照一定标准对申报主体进行审查，并作出批准、附条件批准和否决的决定。通过反垄断法的事前审查程序来防止合并后的企业利用其主导力量侵害用户隐私并获得不公平的竞争优势，从而减少用户在隐私方面遭受侵权的威胁，同时也能够维护市场的竞争秩序。

第三，相较于司法机关，反垄断执法机构拥有较高的执法效率。作为公权力机关，反垄断执法机构拥有查阅相关数据和资料的权力，以及在调查环节采取行政机关独有强制措施的能力，使其可以迅速、完整地进行调查取证和存证。此外，反垄断执法机构可提供给数据隐私被侵权者的救济措施多样，可以在综合评判的基础上对违反反垄断法的企业采取不同的惩处措施，从而能够更有效地纠正企业的违法行为，维护数据隐私被侵权者的合法利益。

三、数据隐私保护的反垄断法适用检视与困境剖析

综上所述，反垄断法框架对于数据隐私保护具备合理性和必要性。然而，如何在实际中适用这一理念，以及在适用过程中可能出现的困境，仍需要更进一步深入探讨。

（一）如何适用：反垄断法视角下数据隐私的基本阐释

以反垄断法的视角剖析数字经济竞争中影响数据隐私保护的行为，能够揭示出消费者隐私权益和维护市场公平竞争之间错综复杂的关系。企业可能通过合并、利用自身市场支配地位以及合谋等方式直接或者间接降低数据隐私保护水平。

首先，企业合并可能会导致经营者集中，不利于数据隐私的保护。具体而言有两种情况：一是合并后直接降低相关市场提供的数据隐私保护水平，或者是通过合并消费者数据提高进入壁垒或提高竞争对手的成本；二是企业通过合并排挤出市场上数据隐私保护水平更高的企业。此外，收购一方还可以通过“隐私政策

① Joseph Farrell, *Can Privacy Be Just Another Good*, Journal on Telecommunications and High Technology Law, Vol.10: 251, p.257(2012).

捆绑”策略来损害市场竞争。“隐私政策捆绑”策略是指企业可以通过收购其他企业从其用户那里获得广泛的消费者同意,增加收集的消费者数据量,合并后的实体通过共享参与集中各方的消费者数据增加竞争对手的进入成本。[①] 合并后的实体集中消费者数据,并对集中后的数据进行后续利用、分析,如果超出了用户原先同意的范围和认知,可能构成降低平台隐私保护质量的行为。[②]

其次,占市场主导地位的企业还可能通过利用自身的市场支配地位降低其向消费者提供的隐私和数据保护水平。对于数据驱动型企业而言,其商业模式有赖于个人数据的收集和使用,因此,数字市场上的主导企业有动机将其隐私保护降低到竞争水平以下,并在竞争水平以上收集个人数据从而进一步巩固其主导地位。例如,通过隐私政策最大限度地收集和使用消费者数据,既损害了消费者的数据隐私利益,也可能会引发排除、限制市场竞争的问题。[③]

最后,如果经营者之间就向消费者提供的隐私保护程度达成一致的串通,可能与任何其他质量、产量或价格协议一样产生反垄断法上的竞争损害。在数字平台企业领域,提高数据隐私保护水平可能会增加运营成本,而降低数据收集则会减少利润。因此,企业之间可能通过合谋来降低数据隐私保护水平。[④]

(二)适用困境一:数据隐私保护与效率的利益平衡难题

反垄断法在维护市场公平竞争秩序的同时,也能够通过规制企业行为来保护个人数据隐私。然而,数据隐私的保护往往需要限制数据的收集、使用和共享,可能会对数据驱动型企业的经营模式和市场竞争产生一定的影响,数据隐私保护与市场效率之间存在价值取向的冲突。企业对于数据的挖掘不断地向纵深处发展,并逐渐渗入到人们生活的方方面面,如果不加以规范和约束,数据的过度收集、无序流通乃至滥用行为将给隐私保护带来巨大隐患。因此,用户对其数据享有的隐私权益构成了数据的另一层属性,数据隐私权益强调用户对其数据的控制,在数据流通的基础上进行一定限制。当然这并非是将数据隐私与数据的流动置于二元对立的位置,而是强调应当协调数据隐私保护与促进数据自由流动之间的关系,衡量数据隐私的价值与数据带来的效率的价值并在此基础上找到一个平衡点。既不能大量让渡隐私去换取效率,也不能一味地强调数据隐私,阻碍数据流通。在数字经济时代精准地平衡数据隐私与效率之间的关系,以及在法律框架内确立数据隐私权益与效率价值的保护边界,成为反垄断法机构难以回避的重大挑战。

(三)适用困境二:隐私保护法和反垄断法的规则竞合问题

目前,中国涉及隐私保护的法律很多,《数据安全法》《个人信息保护法》《民法典》《中华人民共和国消费者权益保护法》《中华人民共和国网络安全法》等多部法律均有隐私保护条款。尽管上述隐私保护法律在保护隐私时存在着一定缺陷,但是其在数据隐私保护方面仍然发挥着不可替代的作用。然而,单纯靠隐私保护法律无法解决所有的问题,比如,尽管企业在征求了用户的同意之后收集数据,但是这种同意可能是基于消费者选择的缺乏,而企业因此巩固了自身的市场支配地位,提高了市场进入壁垒,排除或者限制了市场竞争,此时反垄断法的干预就十分必要。反垄断法与其他法律在数据隐私保护方面具有不同的调整范围,但如何确定反垄断法规制数据隐私损害行为的适用条件成为摆在立法者面前棘手的问题,只有明确在反垄断法中考量隐私问题的起点与范围,才能够防止隐私问题均落入反垄断法的分析框架,避免产生不当的干预和不必要的协调成本,规避反垄断法适用泛化、适用范围过度扩张的问题。

(四)适用困境三:传统价格中心方法的局限问题

数字经济时代,传统的反垄断法分析方法遭遇了一系列挑战,特别是在免费市场和隐私保护领域。传统反垄断法通常依赖于价格上涨的假定垄断者测试(简称 SSNIP 测试法)来界定相关市场,然而,这种方法在数字经济中的应用受到了局限。数字经济时代的商业模式往往是数字平台经营者为消费者提供“免费”的服务,这种“零价格”市场不存在确定的市场价格,而只有市场上的产品或者服务具有市场价格才能够适用

---

① Daniele Condorelli & Jorge Padilla, *Harnessing Platform Envelopment in the Digital World*, Journal of Competition Law & Economics, Vol.16: 143, p.161(2020).

② 参见杨东、臧俊恒:《数据生产要素的竞争规制困境与突破》,载《国家检察官学院学报》2020年第6期,第150页。

③ Maurice E. Stucke, *Should We Be Concerned About Data-Opolies*? Georgetown Law Technology Review, Vol.2: 275, p.285-286(2017).

④ 参见焦海涛:《个人信息的反垄断法保护:从附属保护到独立保护》,载《法学》2021年第4期,第120页。

SSNIP 测试法。如果将原先的“免费”服务进行一个小幅但显著的价格上涨,尽管大部分用户会转向其他替代产品,但是用户流失导致数字平台无法涨价的现象并不能说明其不具备市场势力。因此,工业经济时代的商业模式下创设的基于价格的相关市场界定工具已经无法应用于“免费市场”。① 例如,在“北京奇虎科技有限公司诉腾讯科技(深圳)有限公司、深圳市腾讯计算机系统有限公司滥用市场支配地位纠纷案”的判决中,最高人民法院指出,在免费的互联网业务中,传统的 SSNIP 测试法并不能十分有效地界定相关市场。② 此外,数字经济模式的复杂性也导致相关地域市场和产品市场的界限模糊不清。

同时,由于隐私损害难以量化,将隐私作为质量的一部分纳入反垄断的分析框架也存在着诸多困难。与价格不同,产品质量(包括隐私在内)是一个难以衡量的多维度主观概念,而隐私和产品质量的其他特征之间的关系也是模糊的,因为访问更多的用户数据也可以使在线平台提高整体产品质量。由于传统的竞争违法行为通常会导致有形的经济损害,如过高价格导致消费者支付过多,这种损害相对容易评估和量化,传统的分析方法只是假设产品质量实际上反映在调整价格中,因此更关注垄断行为对价格的影响,缺乏足够的工具和方法来将隐私作为产品质量的非价格因素来考虑。然而,对消费者数据隐私的损害通常是无形的,如人格冒犯和自主权丧失。在数字市场,数字平台若利用隐私数据实施价格歧视等,虽可带来经济利益,但难以证明数字平台从特定隐私数据中获益,或消费者因隐私侵害蒙受经济损失;若仅过度收集数据而无后续利用,隐私损害则主要在人格层面,消费者可能丧失与隐私期待相关的内心平静与舒适感。

将个人信息作为支付给经营者的对价这一损害理论路径也存在着很大障碍。首先,个人信息作为支付的基准量难以准确定义,因为个人信息的价值难以测量和把握。其次,个人信息作为非货币价格与货币价格的特征不同,货币按照其面值对每个人的价值都是确定的,而无需判断消费者的偏好。此外,在进行反垄断分析时,由于个人信息具有可复制性和非稀缺性的特点,与实际货币有很大不同,这种特征上的差异意味着基于货币报酬标准的法律规定不能简单地应用于未经重大调整的个人信息。单位货币对于每个人的效用都是相同的,但是个人信息的价值具有不确定性,个人信息的价值需要衡量每个信息主体从信息中可以获取的效益,其价值与信息的类型高度相关,不易测量。

四、构建数据隐私的反垄断法保护路径

传统的反垄断法分析方法在数字经济时代面临诸多挑战,特别是在处理免费市场、隐私保护和个人信息等问题时的适用性受到限制。

(一)价值重塑:兼顾市场竞争与隐私保护

在数字市场中,数字平台垄断可能限制消费者在数据隐私保护方面的选择空间,从而损害其个人信息权益。反垄断法可以通过规制数字平台垄断,确保消费者能够充分选择数据隐私保护服务。然而,可能并不适宜在中国反垄断法中建立数据隐私与行为规制的直接联系,因为数据隐私并不属于反垄断法的直接保护对象,也难以通过反垄断诉讼来维护。因此,数据隐私的反垄断法保护路径需要在综合维度下加以重构,平衡个体隐私权益与市场效率,以确保数据驱动型企业在保护消费者隐私的同时,不滥用其市场支配地位。

尽管数字平台企业的行为有损害市场竞争秩序的可能,但为了防止阻碍创新和效率价值的发挥,反垄断执法机构在对数字平台企业进行干预时仍然应当保持谦抑,贯彻审慎干预的原则,防止出现公权力机关对于自由市场的任意和过度介入。反垄断执法机构在适用反垄断法维护竞争秩序、保护用户个人隐私时,应始终保持克制,力求实现消费者利益保护与市场创新的平衡,在促进效率的同时实现实质正义。

首先,反垄断执法机构的介入应当具有正当性和必要性,正当性要求反垄断执法要有明确的法律依据,并经过严格的法律论证和分析;必要性则是指对于能够通过市场自身机制和其他法律规制调节的活动,只有在达到足够的可罚性时才考虑通过适用反垄断法进行规制。例如,在审查数字平台企业是否利用市场支配地位过度或不当收集和使用消费者数据并侵犯消费者隐私时,需要使用比例原则在数据流动与隐私保护之

① 参见丁春燕:《论我国反垄断法适用中关于“相关市场”确定方法的完善——兼论 SSNIP 方法界定网络相关市场的局限性》,载《政治与法律》2015 年第 3 期,第 89 页。

② 参见最高人民法院(2013)民三终字第 4 号民事判决书。

间进行权衡,把握数据隐私反垄断法规制的限度,既不能因为过度看重新业态的发展而忽视数据隐私保护,也不能过于激进而损害市场的效率和创新。

其次,反垄断执法机构在执法过程中,执法方式不宜过于激进,防止阻碍创新和效率价值的发挥。在处理数字平台企业的案件时,执法机构应该秉持维护市场竞争和保护用户隐私权益的双重目标。一方面,要对数字平台的行为进行审慎评估,确定其是否存在扭曲市场竞争、削弱消费者权益的行为。另一方面,也要认识到数字经济时代的创新特点,避免不必要的干预。这需要反垄断执法机构具备充分的专业知识,能够深入理解数字市场的运作机制和特点,以便在权衡不同因素时作出明智的决策。

(二)适用细化:区分侵犯数据隐私的具体行为与情景

在探讨数据隐私保护与反垄断法的结合时,必须始终将市场竞争作为连接点。为了确保数据隐私问题得到妥善处理,应对隐私问题进行严格区分,分为与竞争性评估严格相关的隐私问题,以及与竞争性评估无关的隐私问题。对于与竞争无关的隐私问题,可通过《民法典》《个人信息保护法》《数据安全法》等相关法律进行调整。反垄断法保护数据隐私应当以排除和限制市场竞争为前提,避免反垄断法成为万能法,防止所有隐私问题均落入反垄断法的分析框架,以更好地协调法律规则之间的竞合问题。否则,反垄断执法和其他部门执法之间可能产生重复执法,既造成执法资源的浪费,又无法有效实现隐私保护的目标。

1.适用经营者集中规制损害行为

在经营者集中审查程序中,应考虑数据隐私的前置条件。当满足以下三个累积条件时,反垄断执法机构才能在并购审查程序中分析隐私问题:首先,根据定量或定性证据,隐私被视为相关市场竞争的重要非价格参数,换言之,根据产品和服务的类型,判断隐私保护是否是消费者作出选择时重要的参考因素,或者是经营者之间在隐私保护维度展开竞争;其次,交易后隐私保护的削弱风险主要是合并带来的竞争过程或者市场结构变化的结果,即并购交易完成造成的反竞争效应损害隐私保护水平;最后,关注隐私保护水平削弱问题主要是因为隐私在相关市场竞争中构成重要维度。①

这种精细分析的方法在欧盟委员会对"Microsoft 收购 LinkedIn 案"的决定中得到了充分体现。欧盟委员会认为,在该案中,合并将产生集团反竞争效应,因为在交易后,被合并的实体将有能力和动机取消专业社交网络服务的其他竞争者的供应商资格。比如,通过在 Windows 系统上预装 LinkedIn,合并后的实体可以实现 LinkedIn 平台使用率的大幅增长。由于网络效应的存在,专业社交网络服务市场最终可能会向 LinkedIn 倾斜,这可能会阻止与 LinkedIn 竞争的更多隐私保护平台的发展,并构成有意义的竞争约束,从而减少与隐私相关的消费者选择。委员会的分析即满足了上述三个条件:其一,隐私是在专业社交网络服务市场竞争的一个重要的非价格参数;其二,对隐私的负面影响是交易带来的竞争过程或者结构条件变化的结果,这笔交易将增强 LinkedIn 平台的优势,从而边缘化 LinkedIn 的竞争对手,最终损害消费者隐私;其三,"对隐私负面影响的评估"与"隐私在相关市场构成了竞争参数"之间存在因果关系,该交易将限制消费者对这一重要竞争参数的选择,即职业社交网络的隐私选择。欧盟委员会在决定中没有评估仅仅因为个人数据的集中可能对隐私产生的任何影响,也没有以任何方式适用欧盟关于隐私的规则。② 如果一项合并涉及与竞争分析严格相关的隐私问题,换言之,如果满足上述的三个条件,反垄断执法机构则可以在并购控制程序中处理隐私问题,这是因为如果不考虑并购交易中的隐私问题,就不可能充分评估反竞争效果。③

2.适用滥用市场支配地位规制损害行为

当数字平台经营者利用自身的市场支配地位不当地收集和使用消费者的数据,侵害消费者隐私,从而获取不公平的竞争优势时,可以适用滥用市场支配地位规则。目前,滥用市场支配地位的违法类型可分为剥削性滥用和排他性滥用。剥削性滥用是指经营者利用自身的市场支配地位向交易相对人施加不公平的高价或者是附加不合理的交易条件;排他性滥用则是指经营者利用自身的市场支配地位排除、封锁其他竞争者或者

---

① Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, Antitrust Law Journal, Vol.80: 121, p.156(2015).

② Case M.8124-Microsoft/LinkedIn. REGULATION (EC) No.139/2004.

③ Ben Holles De Peyer, *EU Merger Control and Big Data*, Journal of Competition Law & Economics, Vol.13: 767, p.785(2017).

潜在竞争者以巩固和强化地位的行为。①

一方面，在经营者利用自身的主导地位，不当地收集和使用消费者的数据，导致消费者隐私利益严重受损的情况下，可以通过剥削性滥用条款来进行规制。具体而言，可以通过两种损害理论来分析此类行为。理论一，将个人信息当作是消费者支付给数字平台经营者的对价，当经营者实施此类行为时，可以类比为消费者支付的对价过高，从而适用不公平的高价条款。理论二，将不当收集和使用消费者数据视为不合理的交易条件，隐私作为质量维度的一个重要指标，不当收集和使用个人信息即减少隐私保护水平标志着质量的降低，因此在消费者福利受损的情况下，也可以适用不合理的交易条件这一条款。②《反垄断法》第 17 条中列举了剥削性滥用的两种典型表现，即施加不公平的高价和在交易时附加不合理的条件，为规制剥削性滥用中过度收集和使用个人信息的行为提供了法律基础。

不可否认的是，在中国反垄断法的多元目标中包含维护消费者利益以及当下越来越强调竞争促进公平的背景下，确立以消费者福利为基础的剥削性滥用规则的空间越来越大。但受《反垄断法》第 6 条“经营者可以通过公平竞争、自愿联合，依法实施集中”的限制，中国实际上并未确立类似欧盟的强调消费者福利减损的剥削性滥用规则。目前，中国在认定企业滥用市场支配地位时，仍然是以是否排除、限制市场竞争为前提，对剥削消费者的滥用行为未给予足够的关注。

另一方面，目前运用滥用市场支配地位规制不当收集和使用个人数据的行为时，仍然应当以反竞争效果为基础，即通过排他性滥用条款来进行规范。将“主导地位的数字平台损害数据隐私的行为损害市场的竞争秩序”作为反垄断法调整的必要前提，明晰反垄断法规则的适用条件，可以划清反垄断执法和其他部门执法之间的界限，防止出现多个部门共同执法的状况，更好地配置执法资源。如果具有主导力量的平台仅仅是存在损害数据隐私的事实，但并未产生反竞争的损害，则仍然应当由其他与隐私保护相关的法律来对其进行规范。③

以反竞争效果作为侵犯隐私行为的滥用市场支配地位的规制条件，反垄断执法部门可以从以下几个角度入手：第一，侵犯数据隐私的行为可能损害围绕非价格利益竞争的市场机制，也有可能间接损害围绕价格利益竞争的市场机制；第二，在判断市场上的隐私保护竞争是否受损时，需要对相关市场的消费者的隐私偏好以及市场上是否围绕着隐私保护级别展开竞争作深入全面的调查研究；第三，具有市场支配地位的当事企业是否通过不合理地收集或者使用数据获得了不公平的竞争优势，并导致反竞争效果。

（三）方法创新：优化隐私保护分析工具

隐私损害往往难以量化，部分因隐私性质复杂多变，部分因损害具有非经济性和无形性。为解决这一问题，方法创新成为应对隐私保护和市场竞争挑战的重要策略。一种创新性方法将数据隐私损害与市场势力相结合，以更全面地评估隐私损害。这一方法可以借鉴质量经济学理论，将数据隐私保护水平下降视为一种类似于价格上涨的压力。④ 通过这种方法，可以分析企业数据行为对市场格局的影响，评估隐私保护水平的下降是否会导致反竞争效应和消费者损害。通过比较合并前后市场势力的变化，可以判断是否产生竞争优势和损害。这种方法不仅能够应对隐私的非经济性质，还能够综合考虑市场势力和效率因素，从而更准确地评估隐私损害。

另一种创新性方法则是引入数据隐私保护的价格机制，以实现数据隐私的市场化评估。类比传统反垄断框架中的价格分析，可以首先确定不同服务中的数据隐私保护标准，类似于传统市场中的“市场价格”。这一标准需要在合理范围内，既不阻碍行业发展，又能有效保护隐私。同时，考虑到不同产品和服务的特性，隐私保护标准应该动态适应市场变化。随后，分析平台企业在处理用户数据隐私时的保护程度，类似于传统市场中的“自身价格”，包括企业制定的用户条款、数据共享方式、数据保护措施等。最后，将市场保护度和

---

① 参见王先林：《竞争法学》，中国人民大学出版社 2015 年版，第 219 页。

② 参见陈兵、赵青：《我国剥削性滥用行为违法性判定基准审视——以非价格型剥削性滥用为视角》，载《上海大学学报（社会科学版）》2020 年第 3 期，第 78 页。

③ 参见韩伟：《数字经济中的隐私保护与支配地位滥用》，载《中国社会科学院研究生院学报》2020 年第 1 期，第 45 页。

④ 参见杨祖卿：《数字市场中的数据隐私保护：维度拓展、实践困境及路径突破——基于反垄断法视角》，载《南方金融》2023 年第 1 期，第 70 页。

企业保护度进行比较,判断是否存在垄断行为以及损害程度。

此外,在界定相关市场时,传统的SSNIP测试法无法适用于互联网多边市场和零价免费市场,新型工具如基于隐私保护水平下降的假定垄断者测试(简称SSNDQ测试法)和持续性成本上涨的假定垄断者测试(简称SSNIC测试法)能够更准确地应对免费定价和多边市场的特点,[①]从而解决了传统工具的限制。SSNDQ测试法关注互联网平台用户隐私降级导致产品质量下降的情形,通过模仿SSNIP测试法,定量评估降低隐私保护水平5%至10%时的用户转移情况,避免了免费效应的影响。而SSNIC测试法则强调成本的改变,不仅考虑直接的经济成本,也包括时间成本、个人数据换取免费服务的成本以及对广告的注意力成本。这两种工具的应用能更精确地界定相关市场。[②]

(四)监管延伸:加强协同监管与事前预防

除了反垄断法本身的规制,隐私保护和竞争问题的复杂性促使监管机构采取更加综合和协同的方法对数据隐私进行保护。数据保护法、消费者权益保护法和竞争法虽然各有侧重,却在数据隐私保护领域拥有共同目标。

对于在数字经济领域具有强大市场力量的企业,数据保护法保障用户在向企业转移其个人数据前能够拥有知情同意权;竞争法则关注企业不得滥用其市场力量排除、限制竞争,产生不公平的竞争优势;而竞争法对于市场竞争秩序的维护也使消费者有了更多、更优质的选择,提升了消费者福利,使消费者权益得到保障。在数据隐私保护领域,三者并不能完全割裂开来,数据保护法和消费者权益保护法中的隐私保护条款能够为反垄断法中的竞争损害评估提供判断基准,如果三者缺乏互动,可能会削弱执法的效果,导致消极对待隐私保护服务。因此,只有各执法机构之间通力合作,才能够更好地应对数字经济领域隐私保护问题带来的一系列挑战:一方面促进市场充分有效的竞争,另一方面也激发企业在隐私保护维度的竞争动机,提高市场整体的隐私保护水平,从而满足消费者的隐私关切。当然,合作监管并非是需要各方协同执法,共同作出相关决定,对于应当由反垄断法规制的范围,其他执法机构可以从旁协助,从而辅助反垄断执法机构作出更加符合反垄断法精神的决定。例如,对于涉及数据隐私损害的案件中的市场支配力,各执法机构可以联合研究一套更有效更具针对性的评估方法。[③] 相关执法机构之间应当找到平衡点,营造一个不仅仅关注价格而且重视消费者隐私的数据驱动型市场,使得告知同意原则并非流于形式,这些都是数据驱动型社会不可忽视的问题。

在强化协同监管的同时,事前预防也应作为一项重要的策略。事前预防旨在通过制定前瞻性的规则和准则,防范隐私和竞争问题的发生。这需要各执法机构根据数字经济的特点,共同研究和制定适用于各自领域的预防性措施。例如,针对新兴科技和业务模式的监管,可以建立监管沙盒,为创新提供试验场所,同时确保公平竞争和隐私保护的原则。此外,数字化工具的应用也能够提升协同监管和事前预防的效能。执法机构可以利用大数据分析和人工智能技术,实时监测市场和企业行为,发现潜在问题和风险。通过建立预警系统,执法机构能够更迅速地作出反应,防止问题扩大和蔓延。数字化工具的运用有助于提高监管的精准性和时效性,增强执法机构的应对能力。

(五)救济弹性:完善反垄断救济措施

从广义上来说,针对侵害数据隐私行为的反垄断救济措施有两种方式:第一,减少当事企业对用户数据的控制。如剥离当事企业的一些产品或者减少当事企业利用这些产品收集大量数据并建立综合性的"超级档案"的可能性。第二,增强用户对于个人数据的控制,为用户数据创造真正的市场。如赋予用户数据可移植权,允许用户携带数据在市场上自由的切换。同时,增加企业使用数据的透明度,在收集"敏感数据"时,应获得用户"明确的同意",隐私政策的任何修改都需要详细和明确地向用户披露,并获得同意。以上两类方式并不互斥,可以择一适用,也可以合并适用。

---

① 参见袁嘉:《互联网平台竞争的反垄断规制》,中国政法大学出版社2021年版,第118页。

② 参见李晓楠、王嘉徽:《数据隐私保护的反垄断法路径》,载《河南财经政法大学学报》2022年第5期,第62页。

③ 参见李绕娟:《欧盟〈大数据时代背景下隐私与竞争力〉调研报告介评》,载韩伟主编:《数字市场竞争政策研究》,法律出版社2017年版,第189页。

在经营者集中审查案件中,如果企业被认定合并通过将损害消费者隐私权益,排除、限制隐私维度的竞争,那么行为性救济的方式可能是更为适当的选择。① 相比于结构性救济方式,首先,行为性救济方式具有较高的灵活性和可修复性,互联网行业复杂多变,行为性救济方式更能适应互联网行业的特点。其次,行为性救济相对柔性的处理方式可以避免公权力机关过度干预市场主体的交易活动,将隐私损害纳入反垄断法分析框架对于反垄断执法机构而言尚属较新的领域,采取相对温和的救济方式可能更有利于市场的发展。因此类似于第一种方式中剥离企业产品的结构性救济方式不是最优的选择。反垄断执法机构可以附条件批准经营者集中,对参与集中的企业附加行为性救济条件。例如,要求当事企业承诺不得在无正当理由的情况下降低隐私保护水平,限制合并后的企业合并消费者数据的能力等。此外,为了持续监督企业的实施情况,可以引入监督受托人制度,确保企业具体实施被附加的义务,保证救济的效果。

在涉及隐私保护领域的滥用市场支配地位案件中,目前可参考的案例只有德国的“Facebook 案”。德国联邦卡特尔局要求 Facebook 修改其隐私政策并禁止 Facebook 收集其旗下 WhatsApp、Oculus、Masquerade、Instagram 等平台的用户信息及设备(如手机、电脑)关联数据和 Facebook 用户在访问第三方网站和手机应用软件时留下的数据,同时要求其不得将这些数据与 Facebook.com 的账号信息进行匹配整合,此外,处罚决定中还要求 Facebook 进行整改,提高其处理个人信息的透明度并出具详细列明各种技术细节的整改方案。卡特尔局将持续追踪整改情况,并不定期对 Facebook 进行技术检测。在过度收集或不当使用个人数据的滥用市场支配地位案件中,反垄断执法机构可以借鉴德国的做法,禁止所涉企业不当收集和使用个人数据,要求其作出提高隐私保护水平的承诺,并对企业的后续行为进行持续的监督与检查。此外,要求企业为用户提供撤回个人信息或者向用户开放移植其个人信息的权限也不失为一个好的选择,促进个人数据可移植性,在保障个人的信息控制权的同时也有利于促进市场竞争秩序的完善。个人数据可携带权的行使能够在一定程度上破除锁定效应,并有利于第三方进入市场参与竞争。

五、结语

在传统工业经济时代,隐私保护问题与反垄断法并未显露直接关联。随着数字经济时代的到来,各类依托于数据的数字平台企业蓬勃发展。数据的收集、沉淀和应用给数字平台企业带来了丰厚的效益,数据背后承载的消费者隐私利益保护问题也日益凸显。于是,在隐私权的基础上衍生出数据隐私的概念,消费者对于其个人数据应当享有一定的控制权。但平台出于降低成本或者培育自身竞争优势的目的,倾向于大量收集消费者数据或者降低隐私保护级别。隐私保护问题也因此纳入了反垄断执法机构的视野。

将数据隐私保护问题纳入反垄断法规制的逻辑链条如下:中国的反垄断法立法目标包含着维护消费者利益,而消费者利益的内涵中本应包含着质量、消费者选择和创新等非价格利益。数据隐私保护作为重要的非价格竞争参数自然应当属于消费者福利的一部分,因此在应然性层面,反垄断执法机构不应当回避数据隐私保护问题。

然而,在将反垄断法适用于数据隐私保护问题时,需考虑以下几个问题:第一,如何确保数据隐私保护与市场竞争的平衡,以免过度干预市场和创新活动。第二,适用的标准和方法应当明确,以避免适用泛化导致的模糊和不确定性。第三,应当探索与其他法律规范的协调机制,确保数据隐私保护与消费者权益、创新激励等方面的法律目标不产生冲突。第四,适用过程中的监管合作和信息共享也是关键,各执法机构需要通力合作,共同解决交叉领域的问题。第五,适用的效果和救济方式应当得到审慎评估,以避免对市场和企业造成不必要的负面影响。

将反垄断法应用于数据隐私保护是一个道阻且长的过程。在平衡促进创新、维护竞争和保障消费者权益的同时,反垄断执法机构应将数据隐私保护问题纳入其视野,并借助合作与协同,为数字经济的健康发展提供有力的法律框架和监管指引。

---

① 参见孙晋:《谦抑理念下互联网服务行业经营者集中救济调适》,载《中国法学》2018 年第 6 期,第 166-167 页。

The Dilemma and Solution of Data Privacy Protection from the Perspective of Antitrust Law

LIN Yanping, LUO Danrui

(International Law School, East China University of Political Science and Law, Shanghai 200042, China)

Abstract: In digital era, the platform economy, powered by rapid technological advancements such as the Internet, big data, and artificial intelligence, has fundamentally transformed the global stage. Personal data has gained unprecedented importance, become a critical factor in business competition and sparked essential discussions about data privacy. This transformation signifies a shift in economic interactions and consumer engagement in a world driven by digital technology, where effective data management and privacy have become paramount concerns for enterprises, regulators, and consumers. The traditional concept of privacy rights, once conceived in a period of limited interconnectivity, is now being outstripped by the multifaceted challenges of the digital economy. This has given rise to a deeper understanding of data privacy, elevated it to a central aspect of consumer rights and a vital factor influencing market dynamics. Data privacy is becoming a key determinant of product and service quality, profoundly affecting consumer decisions and shaping business practices. This pivotal role of data privacy has necessitated its integration into the heart of antitrust law and competition analysis, underscored its critical influence in molding market behaviors and formulated regulatory strategies in digital era. This evolution in the understanding of data privacy reflects a broader societal shift toward greater recognition of the importance of personal data protection, calls for updating legal and regulatory frameworks and business models to prioritize privacy in a world increasingly connected by digital technology. The challenge of balancing data privacy with market efficiency and innovation is a multifaceted issue that presents considerable complexities. Overly stringent privacy regulations may impede the free flow of data, which is essential for healthy competition and innovation, and is vital for economic growth and technological advancement. This complexity is heightened by the intersection of privacy laws and antitrust regulations, which often have divergent objectives and methodologies, potentially lead to conflicts in their practical application. Additionally, the task of quantifying the impacts of data privacy breaches poses a significant obstacle, as this does not align well with traditional antitrust methodologies that are predominantly focused on pricing dynamics. This problem demands a nuanced and carefully considered approach, aiming to reconcile the need for robust privacy protections while ensuring the vitality and dynamism of a market driven by innovation. This approach requires a balanced consideration of privacy rights, economic growth, and technological progress, in order to ensure that they can coexist and complement each other in a rapidly evolving digital landscape. It is essential to establish prudent intervention principles that carefully balance the need for competitive markets with robust privacy protections. Regulatory strategies must be flexible and tailored to specific instances of data privacy infringement, in order to balance individual privacy concerns against the broader requirements for market functionality and continuous innovation. Further, it is crucial to enhance and adapt the analytical tools used for assessing privacy protections. Traditional methodologies must evolve to effectively address the unique challenges posed by data privacy in the digital economy. Additionally, developing innovative theoretical frameworks within antitrust law is vital. These frameworks should adeptly navigate the intricate relationships among consumer rights, market competition, and privacy protection, in order to ensure that efforts to maintain market efficiency do not undermine fundamental privacy rights. This comprehensive strategy aims to harmonize the protection of personal data privacy with the dynamics of market competition and innovation. It seeks to ensure balanced and sustainable development in the digital economy, reflecting the evolving nature of technology, law, and consumer rights in an interconnected world.

Key words: data; data privacy; privacy protection; digital platform; antitrust law