欧盟《数字市场法》对个人数据保护的影响

韩天竹　禚　澳

【内容提要】 欧盟《数字市场法》的出台强化了对大型平台反垄断的监管,主要体现在对“守门人”规定了相应的义务,但在这些义务中与数据相关的义务对于个人数据安全具有影响,如为业务用户提供数据访问、确保最终用户数据的可移植性等义务存在数据泄露的风险。虽然《数字市场法》一再强调秉持与现有法律建立统一标准的精神,即其规定的义务不应与现有的数据保护相关法律相冲突,但其与欧盟《通用数据保护条例》存在不可忽视的冲突,如何协调两部法律的关系,平衡平台有序竞争和个人数据安全两种法益成为亟待解决的问题。该文聚焦《数字市场法》与《通用数据保护条例》之间的冲突,展望促进两部法律相互协调的可行路径,旨在为中国数字平台反垄断法律提供经验和教训,探索反垄断法与个人数据保护相衔接的有效途径。

【关 键 词】《数字市场法》 个人数据保护 “守门人”义务 《通用数据保护条例》 反垄断法

【基金项目】 2022 年度教育部人文社会科学研究青年基金项目“数字贸易的国际规制进路与中国因应方略研究”(项目编号:22YJC820009)。

【作者简介】 韩天竹,山东科技大学文法学院副教授、硕士生导师;禚澳,山东科技大学文法学院硕士研究生。

一　问题的源起

2020 年 12 月 15 日,欧盟委员会出台《数字市场法》[①](Digital Markets

① Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act),2020 O. J. (COM 2020) 842.

Act)和《数字服务法》(Digital Services Act)两部草案,标志着欧盟互联网监管的重要更新,提出了塑造欧洲数字未来的数字战略①。其中《数字市场法》将限制被认定为“守门人”的大型数字平台企业的某些行为,为这些数字平台明确了权利和义务,使得欧盟委员会能够进行市场调查并对其违法行为进行制裁,确保“守门人”不会滥用自己的市场地位。《数字市场法》规定的“守门人”义务,如向第三方搜索平台提供搜索数据、禁止使用业务用户的数据与其竞争、确保最终用户的数据可移植性等,保障了业务用户的权益且防止大型数字平台滥用其支配地位,而站在使用这些平台的最终用户的角度看,确保最终用户数据的可移植性为个人数据在不同平台间的传输和利用提供了便利,但在连续传输过程中也会存在信息泄露的风险;又如禁止平台合并来自不同服务的个人数据,这种做法大大降低了个人数据整合处理带来的数据安全风险。

2018 年 5 月 25 日,欧洲议会通过《通用数据保护条例》(General Data Protection Regulation)②,旨在保护个人数据与隐私,被认为是欧盟有史以来最为严厉的数据保护法律。《数字市场法》在相应条款中引入了“获得最终用户基于《通用数据保护条例》意义上的同意”作为对相关数据进行处理且共享的前提条件,在一定程度上保障了个人数据安全,但《数字市场法》在其义务规定中对个人数据的保护不完全遵循《通用数据保护条例》中的程序要求。《数字市场法》中个人数据安全条款是否与《通用数据保护条例》的相应规则产生冲突?又该怎样协调两者的关系?《数字市场法》寻求在整个欧盟的数字市场中创造可竞争和公平的条件,通过事前规制防止“守门人”平台间的垄断行为③,并为其明确了权利和义务,且欧盟委员会能够对其进行市场调查,确保它们中的任何一个都不会滥用自己的地位。《数字市场法》赋予欧盟委员会自由裁量权表面上看并不包含保障个人数据安全这一要素,然而在

① John Quinn, Regulating Big Tech: The Digital Markets Act and the Digital Services Act, Dublin Law and Politics Review, No. 2, 2021.

② Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Rrepealing Directive 95/46/EC(General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

③ Peter R. Enia, A Continental Rift? The United States and European Union's Contrasting Approaches to Regulating the Monopolistic Behavior of Gatekeeper Platforms, Brooklyn Journal of Corporate, Financial & Commercial Law, Vol. 16, Issue 2, 2022, p. 249.

数字经济时代,反垄断与数据隐私保护不可避免地出现交叉重叠。未来,中国如何将个人数据保护理念纳入数字平台反垄断法,实现个人信息保护法和反垄断法相应规则的双向衔接是值得思考的问题。

二　欧盟数据保护法律框架

欧盟是全球个人数据保护最为严格的地区,是世界上最早对个人数据进行立法保护的地区,也是对个人数据保护采用统一立法形式、建立统一监管机构的地区。欧盟的个人数据保护经历了从隐私权向个人数据保护权的发展过程,《欧洲人权公约》规定关于个人数据的保护,开启了个人数据保护的先河,欧盟第 108 号《关于个人数据自动化处理之个人保护公约》和《关于涉及个人数据处理的个人保护以及此类数据自由流动的指令(95/46/EC)》使得隐私权在个人数据保护领域基础权利的地位得到确立。《欧洲联盟基本权利宪章》(2000/C364/01)提出个人数据保护权的概念,2018 年生效的《通用数据保护条例》沿用了这一概念并对其进行了明确界定,个人数据保护权从实质上脱离隐私权基础,形成全新的个人数据保护权体系①。欧盟委员会前主席让 - 克洛德·容克(Jean - Claude Juncker)如此评价《通用数据保护条例》:“作为一名欧洲人,这就意味着个人的数据隐私将受到欧盟强有力的法律保护。因为在欧洲隐私是人权的一个十分重要的方面。”②

《通用数据保护条例》包括 11 章,共 99 条,其中序文部分提到:“自然人在其个人数据处理过程中获得保护是其拥有的一项基本权利”,第 1 条第 2 款也指出:“本条例保护自然人的基本权利与自由,尤其保护其个人数据保护权。”《欧洲联盟基本权利宪章》(2000/C364/01)第 8 条第 1 款和《欧盟运行条约》第 16 条第 1 款均规定,“人人享有就涉及其个人数据处理而寻求保护的权利。”《通用数据保护条例》规定了一些重要的定义。例如,个人数据指能够直接或间接识别个人身份的信息,如姓名、地点、生物识别数据、宗教信仰等;数据处理指对收集的数据进行的任何处理操作,无论是自动还是手动,

① 项焱、陈曦:《大数据时代欧盟个人数据保护权初探》,《华东理工大学学报(社会科学版)》2019 年第 2 期。

② 刘泽刚:《欧盟个人数据保护的“后隐私权”变革》,《华东政法大学学报》2018 年第 4 期。

如记录、组织、存储、使用等。该条例将相关主体分为三类:数据主体,即信息被处理的人,如客户或网站访问者;数据控制者,即决定个人数据处理目的和方式的人;数据处理者,代表数据控制者处理个人数据的第三方。条例还强调了针对这些个人和组织的特殊规则①,并且赋予数据主体的权利具体包括知情权、访问权、更正权、删除权、限制处理权、反对权、可携带权等②。《通用数据保护条例》定义了数据主体的“同意”,第 4 条第 11 款将“同意”定义为“数据主体自愿作出的具体的、清晰的、确定的、对与其相关的个人数据进行处理的意思表示”,第 7 条进一步细化规定数据主体撤回“同意”的权利、数据控制者对数据主体的“同意”负有证明责任、对书面“同意”附加特殊限定等。这样,“同意权”就具有更多现实可行性,权利主体的真实意思得到尽可能保护和落实③。该条例还确立了数据处理过程中应当遵守的七项基本原则:合法、公平、透明;目的限制;数据最小化;准确;存储限制;完整与保密;问责与合规④。《通用数据保护条例》力图通过完善和细化个人信息权利,实现全面保障个人对其信息的控制权⑤。

为进一步增强数字战略自主,欧盟加强顶层设计,从 2020 年年初起陆续发布《塑造欧洲的数字未来》《欧洲数据战略》《欧洲新工业战略》《欧洲的数字主权》等一系列旨在推动数字化转型的战略规划文件⑥。2022 年又批准通过《数字服务法》、《数字市场法》以及《数据治理法案》(Data Governance Act)⑦。其中,《数据治理法案》于 2023 年 9 月生效,是第一个通过监管营利

① Pavan Kumar R. ,Data Protection Regulations in European Union,International Journal of Law Management & Humanities,Vol. 4,Issue 3,2021,pp. 3095 – 3103.

② 贾文山、赵立敏:《数字经济时代的个人数据保护:欧美立法经验与中国方案》,《首都师范大学学报(社会科学版)》2022 年第 5 期。

③ 刁胜先、何琪:《论我国个人信息泄露的法律对策——兼与 GDPR 的比较分析》,《科技与法律》2019 年第 3 期。

④ 夏菡:《国际法视野下欧盟数据治理立法发展及对中国的启示》,《武大国际法评论》2023 年第 4 期。

⑤ 刘云:《欧洲个人信息保护法的发展历程及其改革创新》,《暨南学报(哲学社会科学版)》2017 年第 2 期。

⑥ 易磊:《欧盟法中个人数据保护与商业利用的平衡模式研究》,《德国研究》2022 年第 5 期。

⑦ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act),https://eur – lex. europa. eu/eli/reg/2022/868/oj

性数据中介服务和非营利性数据利他主义组织来实现第三方数据治理的立法①。该法案定义了一套提供数据中介服务的特殊规则,为向欧盟以外输出数据建立了合规体系,同时引入了应确保实施数据利他主义的权利②,目的是构建数据交换、数据共享机制,提升数据共享服务,增强数据的可用性。

以上与个人数据保护相关法律的出台,使欧盟建立了数据隐私保护与数据治理的基本法律框架,其中《通用数据保护条例》不仅仅是为了保护个人数据,从数字产业发展角度来看,是为顺应经济发展、数字时代发展的规律,协调数字流通过程中用户与数据处理者、控制者之间的关系,重点保护个人数据在数据共享和使用中的安全性,所以在构建欧盟单一数字市场的过程中应秉持该条例保护个人数据的基本理念,促进数据治理相关法律与该条例数据保护制度相衔接。

三 《数字市场法》中数据相关义务对数据安全的影响

《数字市场法》于2022年获得通过,欧洲将配备专门的旨在规范科技行业竞争的全新法律。然而,欧盟必须在竞争法和隐私保护法之间取得微妙的平衡③。《数字市场法》规定"守门人"义务的基本理由在于其规模和在市场上的主导地位,"守门人"负有额外的责任以确保开放和公平的市场环境④,该法为"守门人"设计了两类义务:一类是对"守门人"自动适用的义务;另一类是欧盟委员会与"守门人"通过对话确定的义务⑤。在这些义务中,与数据相关的义务虽然有助于促进公平的竞争环境,但个人数据安全却存在风险。

---

① Anna B. Suman, Citizen – Gathered Data to Support Public Services under Emergencies: Promises and Perils of Openness, Journal of Open Access to Law, Vol. 11, No. 2, 2023, pp. 1 – 24.

② Lusine Vardanvan, Hovsep Kocharyan, The GDPR and the DGA Proposal: Are They in Controversial Relationship? European Studies – the Review of European Law, Economics and Politics, Vol. 9, No. 1, 2022, pp. 91 – 109.

③ Elyssa Diamond, Distrust & Antitrust: Using Facebook to Understand Competition Law's Role in Regulating Data and Data Privacy Concerns Around the World, Fordham International Law Journal, Vol. 45, 2022, p. 873.

④ John Quinn, Regulating Big Tech: The Digital Markets Act and the Digital Services Act, Dublin Law and Politics Review, No. 2, 2021.

⑤ 李世刚、包丁裕睿:《大型数字平台规制的新方向:特别化、前置化、动态化——欧盟〈数字市场法(草案)〉解析》,《法学杂志》2021年第9期。

(一)提供数据访问的义务

1. 向第三方在线搜索提供商提供访问搜索数据义务

一个搜索引擎需要向其他搜索引擎提供由其用户生成的查询、点击和查看数据。《数字市场法》要求平台按照公平、合理和非歧视性的原则向实际或潜在竞争对手提供第三方数据的访问权,此义务是克服市场中可能存在数据壁垒的一种手段,因为企业在市场中需要大量用户数据的支持才能有效参与竞争。

《数字市场法》第 6 条第 11 款①规定,“守门人”必须按照公平、合理和非歧视性的原则向第三方在线搜索提供商提供最终用户生成的排名、查询、点击和查看数据的访问。但是提供数据访问的前提是“守门人”对个人数据的匿名化,且《数字市场法》序言第 61 条②要求“守门人”“应通过适当的手段确保对最终用户的个人数据保护,且不会大幅度降低数据的质量或有用性。”该项规定在一定程度上保证了个人信息的安全适用,但是对于何为“不会大幅度降低数据的质量或有用性”并没有说明具体的标准,无法解释数据质量或有用性的降低在多大程度上构成实质性的降低,对于个人数据如何通过匿名化处理而不降低其有用性,这应取决于作为接收者的第三方搜索引擎对该数据的使用情况,因为数据的有用性必然取决于对它的使用,且匿名化处理在很大程度上会破坏数据的价值,但是《数字市场法》并没有说明“守门人”是否需要在授予访问权限之前评估请求访问此类数据的第三方搜索引擎的使用情况,或者是否需要“守门人”主动提供评估的文件,而是将预测此类用途的负担以及在匿名化与保持质量或有用性之间取得适当平衡的负担放在了“守门人”身上③。在互联网竞争市场中,数据构成了竞争的关键因素,通过对海量数据的整合分析可以提高搜索服务的相关性,更精准地投放相关广告,吸引广告商等,但《数字市场法》这种不确定性的规定不仅会破坏数据传输的价值意义,还会影响数据安全,使得数据没有真正为第三方搜索引擎提供经济价值,实现反垄断的根本目的,也使得个人数据安全处于危险的边缘,

① Digital Markets Act, Article 6(11), http://data.europa.eu/eli/reg/2022/1925/oj

② Digital Markets Act, Recital 61, http://data.europa.eu/eli/reg/2022/1925/oj

③ Bridging the DMA and the GDPR – – Comments by the Centre for Information Policy Leadership on the Date Protection Implications of the Draft Digital Markets Act, Hunton Andrews Kurth LLP: Ctr. for Info. Pol'y Leadership, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl comments on the data protection implications of the draft digital markets act 6 dec2021.pdf

难以在此项义务的履行中得到很好的保护。

除此之外,《数字市场法》第 6 条第 11 款的宽泛措辞,即“任何第三方在线搜索引擎提供商”意味着只要提供搜索服务的平台都可以依赖“守门人”获取搜索数据。先不谈将数据共享给“守门人”平台中的任何第三方在线搜索引擎提供商会不会对反垄断造成过犹不及的影响,数据共享首先就存在风险,当数据在实体之间大量收集、处理和共享时,数据泄露的风险就会增加①,并且针对上文所述对个人数据进行匿名化处理的同时保证数据的质量或有用性并没有规定适当的标准,使得个人数据在传输过程中没有得到系统全面的保护。

2. 向业务用户提供数据的连续和实时访问

《数字市场法》第 6 条第 10 款②要求“守门人”必须为业务用户或其授权的第三方提供对数据进行连续和实时的访问,该数据主要是业务用户和最终用户所提供的或在活动中生成的。对于个人数据,最终用户应予以同意,并且在序言第 60 条③中也要求,“守门人”应使业务用户能够获得其最终用户基于《通用数据保护条例》和第 2002/58/EC 号《电子隐私指令》的“同意”,所以,只有在相关最终用户同意共享的情况下,他们才能与业务用户共享数据④。该项义务充分考虑到个人数据的安全问题,将个人数据处理与访问的决定权交予个人手中,同样,《数字市场法》第 5 条第 2 款要求“守门人”不得将来自核心服务平台的任何个人数据与来自其他“守门人”或者第三方的个人数据合并或者交叉使用,也不得将最终用户登录到“守门人”提供的其他服务平台以合并个人数据,除非已向最终用户提供特定选择而最终用户提供了《通用数据保护条例》意义上的“同意”。然而数据共享本身就存在风险,经济合作与发展组织也曾指出与数据共享相关的几个风险,包括使“守门人”平台和消费者面临数字安全威胁⑤、损害消费者利益,特别是此项义务下涉及

---

① Peter R. Enia, A Continental Rift? The United States and European Union´s Contrasting Approaches to Regulating the Monopolistic Behavior of Gatekeeper Platforms, Brooklyn Journal of Corporate, Financial & Commercial Law, Vol. ,16, Issue. 2, 2022.

② Digital Markets Act, Article 6(10), http://data. europa. eu/eli/reg/2022/1925/oj

③ Digital Markets Act, Recital 60, http://data. europa. eu/eli/reg/2022/1925/oj

④ Philipp Baschenhof, The Digital Markets Act(DMA): A Procompetitive Recalibration of Data Relations? University of Illinois Journal of Law, Technology and Policy, No. 1, 2022.

⑤ OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re - use across Societies(Nov. 26, 2019), https://www. oecd - ilibrary. org/sites/15c62f9c - en/index. html? itemId = /content/component/15c62f9c - en

最终用户的相关数据访问。此外,研发一种安全算法可能会确保专有信息不受侵犯,但由于数字市场中第三方商业用户交易的数量巨大,完成这一算法的设计所投入的成本会很昂贵,并且对“守门人”来说具有很大的挑战性。数据共享本身存在的风险加上缺失严谨全面的规范标准保障数据的处理与传输,最终将无法实现数据共享的根本目的。

(二)确保业务用户或最终用户数据的可移植性

根据《数字市场法》第 6 条第 9 款①,“守门人”必须为最终用户或最终用户授权的第三方提供数据的有效可移植性,这些数据包括最终用户提供的和其在活动中所产生的数据,特别是应根据《通用数据保护条例》为最终用户提供工具,以促进数据可移植性的有效行使,包括提供连续的、实时的访问。数据可移植性规则的支持者认为,它通过降低转换成本和减少用户锁定来刺激平台间的竞争②。数据可移植性在《通用数据保护条例》中也有规定,但与《数字市场法》存在不同之处。《通用数据保护条例》中的数据可移植性仅限于个人数据,根据条例中数据主体的范围,数据可移植性仅限于数据主体提供给控制者的数据,而《数字市场法》中的数据除最终用户提供的个人数据外,还包括最终用户在活动中产生的数据。在序言 59 条③中列出了用户“在使用‘守门人’服务的情况下提供或生成的”这两种数据,拓宽了数据可移植性概念的同时也扩大了个人数据移植的范围,促进了更广泛的数据流动,但也增加了数据安全风险,且数据安全措施的规定充满了不确定性,个人数据可移植范围的扩大使得风险系数增加,由此产生的数据风险问题不容小觑。

在《通用数据保护条例》第 20 条中,要求数据控制者以常用格式向数据主体提供个人数据④,其中数据控制者通过自动化方式处理个人数据,在技术上可行的情况下,数据主体有权将自己的数据从一个控制者直接传输到另一个控制者。但《数字市场法》中没有提供传输数据的标准化格式用以履行该法义务下的强制数据共享,使得数据传输的形式不确定,任意形式的格式无法达到统一的数据安全保障水平。在身份验证薄弱和身份盗窃猖獗的时代,数据以通用的、可传输的格式保存时,恶意参与者更容易访问数据,或者

① Digital Markets Act, Article 6(9), http://data.europa.eu/eli/reg/2022/1925/oj

② Thomas A. Lambert, Addressing Big Tech's Market Power: A Comparative Institutional Approach, SMU Law Review, Vol. 75, Issue 1, 2022, p. 73.

③ Digital Markets Act, Recital 59, http://data.europa.eu/eli/reg/2022/1925/oj

④ Christina Etteldorf, DMA – Digital Markets Act or Data Markets Act? European Data Protection Law Review, 2022, pp. 255 – 261.

即使是用户授权的数据共享也可能在传输过程中泄露出去,损害其隐私权,黑客也可以轻松地将自己的虚假身份移植到许多平台上来获取数据资源①,在这种情况下,只有不断精进数据安全保障措施、统一数据安全保护形式、增加数据安全技术的研发成本,才能实现数据资源保护和利用的双重效益。

同时应注意到,一份数据可能涉及不同数据主体的数据信息,在一个数据主体要求访问并传输数据时,可能侵犯其他数据主体的隐私权,这该如何解决,《数字市场法》并没有给出答案。

(三)免费且有效的互操作性义务

《数字市场法》第6条第7款②关于互操作性的义务要求规定,"'守门人'应允许业务用户和替代服务提供商与核心平台服务一起提供或支持核心平台服务,进行免费、有效的互操作,以及以互操作为目的访问相同的操作系统、硬件或软件,不管这些功能是不是操作系统的一部分。"这可能在"守门人"的业务实践中与数据保护和网络安全等方面的法律法规及需求产生冲突。虽然该法要求互操作性等义务须同时保证高水平的安全措施和个人数据保护,但对于高水平的技术并没有具体的标准,很可能涉及隐私和数据保护相关的争议问题。该法第7条规定了"守门人"对独立电话号码的人际通信服务的互操作性义务,根据该条款,"守门人"应收集并与要求互操作的提供商交换绝对必要的个人数据,虽然这是在追求遵守《通用数据保护条例》的数据最小化原则,但该规定仍然有些模糊③。

综上所述,《数字市场法》中数据相关义务的规定虽涉及对个人数据安全的保护措施,但数据处理、传输等具体过程中的保障标准并不明确,仍有待进一步的解释和细化,同时也看到《数字市场法》与《通用数据保护条例》在个人数据保护方面存在突出问题,造成两部法律在个人数据保护方面的冲突,也给《数字市场法》条款项下的数据访问与共享义务带来一定数据安全风险,如果不能将《数字市场法》与《通用数据保护条例》的有关数据活动标准进行有效衔接和协调,那么,《数字市场法》所保护的法益与造成另一法益的损失将不成比例,该法最终也无法实现其真正的规制目的。

---

① Barbara Engels, Data Portability among OnLine Platforms, Internet Policy Review, Vol. 5, 2016, p. 2.

② Digital Markets Act, Article 6(7), http://data.europa.eu/eli/reg/2022/1925/oj

③ Christina Etteldorf, DMA – Digital Markets Act or Data Markets Act? European Data Protection Law Review, 2022, pp. 255 – 261.

四 《数字市场法》与《通用数据保护条例》的冲突与协调

(一)《数字市场法》与《通用数据保护条例》的冲突

1. 数据可移植性义务规定的冲突

《数字市场法》的数据披露义务仅涉及与最终用户对相关业务用户提供的产品或服务使用“直接相关”的数据,“直接相关”的定义有待机构和法院在实践中确定,但根据可以传输的数据范围可能会使“守门人”违反《通用数据保护条例》第 20 条,该条规定了授予最终用户“不受阻碍”地从数据控制者那里移植个人数据的权利。“守门人”遵守《数字市场法》第 6 条并限制个人数据的数据可移植性有违反《通用数据保护条例》第 20 条的风险,或者说,“守门人”提供了该条例第 20 条规定的“无障碍”数据可移植性则可能违反《数字市场法》。

2. 同意数据处理条件的冲突

《数字市场法》第 6 条规定“守门人”应根据业务用户和经业务用户授权的第三方的请求,免费提供有效、高质量、连续和实时的访问以及使用聚合和非聚合数据,这些数据是业务用户和最终用户在使用相关核心平台服务提供的产品或服务时产生的;对于个人数据,是在最终用户同意的情况下进行的数据共享。每当最终用户选择加入共享时,该法都会要求“守门人”将数据传输给业务用户①。但是在最终用户首次向业务用户注册时,经过最终用户的一次性普遍接受,业务用户便可以过度地接收来自“守门人”的任何个人数据,在最终用户还没有完全意识到使用“守门人”服务时,其产生的数据就将被大量业务用户所取得,因此可能与《通用数据保护条例》规定的用户同意数据处理的条件相冲突。例如,该条例第 7 条第 4 款禁止为履行合同而对个人数据进行不必要的处理,然而,《数字市场法》中“守门人”可能会要求与业务用户共享超出提供服务所必需的数据。可以说,《数字市场法》第 6 条中关于“守门人”向第三方在线搜索提供商以及业务用户提供数据访问的义务可能会与它们在《通用数据保护条例》下的义务相冲突。而根据该条例,数据传输涉及个人数据时,“守门人”必须证明数据传

① Aurelien Portuese, The Digital Markets Act: A Triumph of Regulation Over Innovation, https//itif. org/publications/2022/08/24/digital - markets - act - a - triumph - of - regulation - over - innovation

输的正当性,并在数据传输的两端建立数据安全机制,《数字市场法》则侧重强调不妨碍数据的传输。《通用数据保护条例》序言第 32 条规定,“‘同意’涵盖为相同的一个或多个目的进行的所有数据处理活动。数据处理涉及多个目的的,每一个目的均须征得数据主体的同意”,《数字市场法》中的数据相关义务要求可能会破坏《通用数据保护条例》的“目的限制原则”①,因为《数字市场法》第 5 条第 2 款(d)项可能不需要对某些目的进行明确限制②。

《通用数据保护条例》第 4 条第 11 款中“同意”一词指数据主体根据意愿和自由给予的具体的、知情的和明确的指示,通过声明或明确的肯定行动表示同意处理与本人相关的个人数据,这里的“自由给予”“具体”“知情”“明确”等术语还需要通过漫长的诉讼实践进行进一步解释③。《数字市场法》第 5 条第 2 款(d)项中使用了《通用数据保护条例》中的“同意”。《数字市场法》使用《通用数据保护条例》标准受到了普遍的批评④,是否应该依赖《通用数据保护条例》来制定标准仍有待研究,是侧重隐私保护还是侧重竞争,“同意”标准应根据目标的不同采用不同的界定方法,因为不同的“同意”标准在实践中可能会造成混淆,进而给企业带来双重负担。

(二)促进《数字市场法》与《通用数据保护条例》相互协调的展望

《数字市场法》在个人数据安全方面已经提出了积极的举措,其第 5 条第 2 款最能体现与《通用数据保护条例》之间的联系,该条款规定了不允许“守门人”对个人数据进行处理的几种行为,包括不允许基于提供在线广告服务的目的处理个人数据、在“守门人”单独提供的其他服务中交叉使用个人数据等。如果最终用户已经根据《通用数据保护条例》第 4 条第 11 款、第 7 条表示明确的“同意”,则该条款不适用,这使得《数字市场法》与《通用数据保护条例》的关系非常明确,最终用户仍然可以按照《通用数据保护

① GDPR, Article 5 1(b), http://data/europa. eu/eli/reg/2016/679/2016 - 05 - 04

② Irish Council for Civil Liberties, Greater Protection in Article 5 (a) of the Commission's Proposal for a Digital Markets Act, https://www. iccl. ie/wp - content/uploads/2021/01/Alexandra - Gesses - re - Article - 5 - from - ICCL · pdf

③ Rupprecht Podszun, Should Gatekeepers Be Allowed to Combine Data? - Ideas for Art. 5(a) of the Draft Digital Markets Act, SSRN Electronic Journal, Vol. 71, No. 3, 2021.

④ Romina Polley, Friedrich Andreas Konrad, Der Digital Markets Act - Brüssels neues Regulierungskonzept für digitale Märkte, WuW, p. 198, 2021.

条例》的规定自由决定如何处理他的数据。如果最终用户拒绝或者撤回此“同意”,“守门人”在一年内不得为同一目的重复请求其“同意”,为此,《数字市场法》禁止了在线平台常见的模式,如通过反复出现的“cookie”框、弹窗、更新使用条款等促使用户同意,欧洲数据保护委员会在“持续提示”标题下的指导原则中也提到了此种做法①,认为这种行为违反了《通用数据保护条例》第 4 条第 11 款、第 7 条以及第 42 条的自由同意原则。总的来说,《数字市场法》是构建在《通用数据保护条例》之上的,它没有对个人数据或者非个人数据、同意数据处理等术语进行新的定义,而是完全本着与现有的法律文书建立统一标准的精神,强调其规定的义务不应违反现有的数据保护法。

但针对《数字市场法》与《通用数据保护条例》中相冲突的规定,作为规制大型平台的反垄断法,在规范平台竞争的同时兼顾保障个人数据安全、平衡两种法益,还需加强与《通用数据保护条例》现有个人数据保护规定的协调性,以下将提出几点针对《数字市场法》与《通用数据保护条例》相互协调的可行路径。

1. 明确相同数据规则下的数据范围

《数字市场法》与《通用数据保护条例》都对数据可移植性进行了规定,数据可移植性的目标主要分为两类:第一类涉及增强数据主体对其数据的自主权,第二类旨在激发数字市场的竞争和创新②。不同的目标需要不同范围的数据遵守可移植性规则,《通用数据保护条例》优先考虑个人,因此,数据可移植性仅适用于数据主体向数据控制者已提供的数据,而《数字市场法》旨在通过更大范围的数据可移植性来适应市场目标,因此,该法规定除了数据主体向数据控制者已提供的数据之外,“通过最终用户在相关核心平台服务的活动中生成的任何数据”也包括在内③。这就造成了相同数据权利在不同法律之间数据范围的冲突,对此,《数字市场法》可给出明确的解释以确保该法在实际应用中“不损害”《通用数据保护条例》,也使它能更好地发挥治理大型数字平台垄断问题的能力。

---

① Christina Etteldorf, DMA – Digital Markets Act or Data Markets Act? European Data Protection Law Review, 2022, pp. 255 – 261.

② Salomé Viljoen, A Relational Theory of Data Governance, The Yale Law Journal, Vol. 131, No. 2, 2021, pp. 573 – 621.

③ Jiawei Zhang, The Paradox of Data Portability and Lock – in Effectse, Harvard Journal of Law & Technology, Vol. 36, 2023, p. 657.

2. 明确取得“同意”的数据活动范围

《数字市场法》中部分数据相关义务条款适用了《通用数据保护条例》中的“同意”标准。《通用数据保护条例》第 9 条规定了对处理敏感个人信息的“同意”,并且处理行为是为履行数据主体作为合同一方当事人的必要行为。其序言第 32 条规定,“‘同意’涵盖为相同的一个或多个目的进行的所有数据处理活动,数据处理涉及多个目的,每一个目的均须征得数据主体的同意”。而《数字市场法》仅指出适用《通用数据保护条例》意义上的“同意”,但具体适用的程度以及适用范围并没有具体说明。也就是说,《数字市场法》与《通用数据保护条例》“同意”标准所适用的数据范围可能存在冲突,对此,《数字市场法》不能简单引入《通用数据保护条例》中的“同意”标准,未来可以考虑明确并完善具体的适用制度,与《通用数据保护条例》现有规定相衔接,保证取得“同意”的数据范围是统一的或至少不存在冲突。

除此之外,“同意”标准应根据目标的不同采用不同的界定方法,应重新考虑该规则的目标,该规则可能会有多种目标,应具有明确的偏向性①。保护个人数据本身就是一个目标。这要求用户作为其个人信息的权利持有人可以自行决定如何处理他们的个人数据。更重要的是,《通用数据保护条例》将以促进数据最小化②方式作为一项原则,即将数据的收集和使用限制在相关目的所必需的范围内③。应秉持条例中数据处理的基本原则,对数据处理范围进行限制性规定。

在数字商业模式中,公平竞争的市场和个人数据的保护可以被视为同一枚硬币的两面。拥有权利的数据主体即最终用户位于“守门人”与业务用户之间④,在“守门人”和业务用户挖掘数据的经济价值时,侵犯数据主体隐私的情况时有发生,利用《数字市场法》这一强有力的反垄断法约束大型数据平台的相关行为,推进《数字市场法》与《通用数据保护条例》相关规定

① Heike Schweitzer, The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What Is Fair: A Discussion of the Digital Markets Act Proposal, Forthcoming, ZEuP, No. 3, 2021.

② GDPR, Article 5 1(c), http://data. europa. eu/eli/reg/2016/679/2016 - 05 - 04

③ Rupprecht Podszun, Should Gatekeepers Be Allowed to Combine Data? - Ideas for Art. 5(a) of the Draft Digital Markets Act, SSRN Electronic Journal, Vol. 71, No. 3, 2021, pp. 197 - 205.

④ Christina Etteldorf, DMA - Digital Markets Act or Data Markets Act? European Data Protection Law Review, 2022, pp. 255 - 261.

的协调性,加强对个人数据的保护,也是加强欧盟数字化单一市场数据监管的需要。

五　对中国数字平台反垄断法律的借鉴意义

在数字经济时代,数据隐私既是平台竞争的核心资源,也是平台垄断力量的关键来源①,而《数字市场法》的出台表明欧盟关注到了用户隐私安全与反垄断两个领域存在的密切关系。

中国有关大型平台反垄断问题的法律主要为《中华人民共和国反垄断法》(以下简称《反垄断法》)和《国务院反垄断委员会关于平台经济领域的反垄断指南》(以下简称《指南》)。《反垄断法》的立法目标是多元而非单一的,个人数据保护应在《反垄断法》的立法价值中有所体现,数据保护也是竞争中的重要因素,《反垄断法》第 1 条②就反映了该法的多元价值追求,包含公正的竞争秩序、消费者利益及社会公共利益。在竞争中不能忽视对数据主体利益的保护,保护用户数据隐私是《反垄断法》的题中应有之义。而《指南》也立足于中国平台经济领域发展现状和特点,对涉及平台经济领域的《反垄断法》适用问题作出较为细化的规定。其中部分规定体现了中国在反垄断中对保护用户数据隐私的肯定态度③。2021 年 10 月,国家市场监督管理总局又公布了《互联网平台分类分级指南(征求意见稿)》和《互联网平台落实主体责任指南(征求意见稿)》,同样创设了超大型平台管理制度并对其施加了特殊的竞争义务。但现行反垄断相关法律对于平台数据可携带性以及互操作性等规定尚不明确,可借鉴欧盟立法经验,加强对数字平台的监管、探索平台数据可携带等相关数据权利的本土路径,同时,数据安全也应同等重视。《中华人民共和国个人信息保护法》的出台也预示着应当更加重视数字经济领域中的竞争问题和隐私保护问题,该法为个人信息提供专门保护,《反垄断法》

① 承上:《数据隐私的权利保护与反垄断监管的协同实施》,《情报杂志》2023 年第 6 期。

② 《中华人民共和国反垄断法》第 1 条规定:“预防和制止垄断行为,保护市场公平竞争,提高经济运行效率,维护消费者利益和社会公共利益,促进社会主义市场经济健康发展。”

③ 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》,《重庆邮电大学学报(社会科学版)》2023 年第 4 期。

可以实现强化保护,两者之间相互补充①、相互协调,做到有效对接。然而,中国现行反垄断相关法律对个人数据安全保护的规定并不明确,没有具体引入个人数据保护相关制度,如《中华人民共和国个人信息保护法》中有“同意”制度,而《反垄断法》并没有明确数据保护的相关规定,仅仅在《互联网平台落实主体责任指南(征求意见稿)》第18条中提到,未经用户同意互联网平台经营者不得将经由平台服务所获取的个人数据与来自自身其他服务或第三方服务的个人数据合并使用,并规定超大型平台经营者应确保数据安全。

监管机构已经发布相关文件支持在反垄断规则中引入个人信息保护②,未来,中国反垄断相关法律应以欧盟《数字市场法》与《通用数据保护条例》的冲突与协调为鉴,具体规则设定应明确个人数据以及敏感个人数据的实质内涵,与《中华人民共和国个人信息保护法》相一致,为个人数据保护设置明确规则。此外,实施数据开放应坚持“同意”原则,个人信息保护的本质是“控制”,对于垄断平台而言,用户的信息应受到平台和用户自己的双重控制③。美国知名学者弗兰克·帕斯奎尔(Frank Pasquale)也认为,作为个人信息保护中已经被普遍运用的“通知—同意”原则可以被用于反垄断中④。同时应明确“同意”标准、单独取得个人同意、重新取得个人同意的情形以及“同意”处理的数据范围等,避免设置的个人数据保护制度与现行个人数据保护相关法律发生冲突。

除此之外,可以借鉴欧盟的做法,对超大型平台实行事前监管,在强化公平竞争规则的同时注重个人数据保护和平台透明度,对数字平台设立相应义务,有效减少超大型平台对数据隐私带来的隐患。

(责任编辑:**李丹琳**)

---

① 曾雄:《在数字时代以反垄断制度保护个人信息的路径与模式选择》,《国际经济评论》2022年第3期。

② 同①。

③ Erika Douglas, Monopolization Remedies and Data Privacy, Virginia Journal of Law & Technology, No. 24, 2020, pp. 1 – 88.

④ Frank Pasquale, Privacy, Antitrust, and Power, George Mason Law Review, Vol. 20, No. 4, 2013, pp. 1009 – 1015.