数字平台的“阶梯式”监管模式：以欧盟《数字服务法》为鉴*

王天凡

内容提要：在针对数字服务平台究竟应当采取何种监管模式和监管措施的问题上，美国和欧盟提供了不同的方案。欧盟《数字服务法》构建了针对中介服务提供者的“阶梯式”层层递进的监管模式：从所有中介机构的基本义务，到托管服务提供者的规则，再到在线平台的补充规定，最后到超大型平台的最严格措施。尤其是针对超大型平台设置的“超强监管”措施，可能导致其企业成本增加、商业秘密保护受到挑战，合规风险增大。《数字服务法》为各国数字平台监管立法提供了参考，却不应成为全球通用的“模板”。中国应立足于本国数字经济发展的根本需求，在利益衡量的基础上，设定差异化平台义务，构建发展与保护并重的平台监管制度。

关键词：欧盟　《数字服务法》　数字平台　监管模式　平台透明度

平台经济是国家（地区）数字经济实力的集中体现，对平台等数字服务中介机构的监管一直都是各国（地区）法律与政策考量的关键所在。鉴于各国（地区）数字经济发展状况和对数字化在社会生活中的定位与理念的差异，各国（地区）选择的规制路径也呈现出不同的特点。① 最突出的表现当属美国的“弱监管”和欧盟的“强监管”模式之别。中国学界与立法机关或出于法律继受的“惯性”，对欧盟模式更为“亲近”，并多有借鉴。但是，一方面学界对欧盟规则尚欠缺系统和深入的研究，尤其是对其立法政策的关注较少；另一方面，在“本土化”的考量上，即为何选择欧盟模式、欧盟规则是否符合中国数字经济发展的根本需求等问题却较少深究。在平台监管的路径选择上，

* 本文为北京市社会科学基金“北京数据跨境流动安全管理机制研究”（项目批准号：21JCC072）的阶段性成果。感谢周学峰教授、聂卫锋副教授和外审专家的意见，文责自负。

① 姚佳：《数据要素市场化的法律制度配置》，载《郑州大学学报（哲学社会科学版）》，2022 年第 6 期，第 43-50 页。

中国应对已有的比较法模式与规则进行深入研究,以此为鉴,结合本国数字经济立法和司法现状,设置最适宜的监管规则。

大型互联网平台在社会生活中的“权力”问题,①引起了欧盟委员会的关注。② 从一系列欧盟委员会的决议及欧盟《2030 数字罗盘:欧洲数字十年之路》③中,可以看出欧盟对美国大型互联网平台的戒备之心。欧盟开始意识到,单靠目前的竞争法手段,不足以遏制大型平台垄断所带来的一系列问题。2020 年 12 月,欧盟委员会提出了《数字服务法》(Digital Services Act, 以下简称 DSA 或条例)④和《数字市场法》(Digital Market Act, DMA)两部新的数字法草案。经过欧洲议会和欧盟理事会的批准通过,《数字服务法》于 2022 年 11 月 16 日生效。DSA 被认为是对世界范围内的大型科技公司设置了最严格限制的首部法律,⑤欧盟单一数字市场“强监管”模式再度加码,将对欧盟的数字经济生态产生深远的影响。

数字平台的监管虽然早已进入学界视野,但以往的研究大多聚焦于平台反垄断。⑥ 随着平台经济的迅猛发展和问题的不断出现,监管困境日渐明显,开始有学者意识到仅从反垄断角度对平台进行监管的不足。⑦ 欧盟《数字服务法》正是在《数字市场法》的反垄断措施之外,专门针对数字中介服务提供者设置了体系性的监管措施。无论是从监管角度,还是从中国数据服务企业参与海外竞争角度而言,对 DSA 进行深入细致的研究都刻不容缓。

---

① 如在美国国会大厦遭袭后,脸书(Facebook)、推特(Twitter)等社交网站封锁了特朗普的账户。参见 Kate Conger, Mike Isaac and Sheera Frenkel, “Twitter and Facebook Lock Trump's Accounts After Violence on Capitol Hill,” *The New York Times*, January 6, 2021。

② 如欧盟专员蒂埃里·布雷顿(Thierry Breton)认为:“正如‘9·11 事件’标志着全球安全政策的范式转变,20 年后,我们见证了数字平台在我们民主生活中的作用的更迭。”Breton, Der Sturm auf Capital Hill ist ein digitaler “9/11”-Moment, WELT.v. 5.12.2022。

③ European Commission, Communication from the Commission to The European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “2030 Digital Compass: The European Way for the Digital Decade,” COM(2021) 118 final, Brussels, 9.3.2021, https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf.

④ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A277%3ATOC.

⑤ Sam Schechner and Kim Mackrael, “EU Lawmakers Approve Sweeping Digital Regulations,” https://www.wsj.com/articles/eu-lawmakers-approve-sweeping-new-digital-regulations-11657040485.

⑥ 孙晋:《数字平台的反垄断监管》,载《中国社会科学》,2021 年第 5 期,第 101-127 页;马平川:《平台反垄断的监管变革及其应对》,载《法学评论》,2022 年第 4 期,第 174-183 页;丁晓东:《平台反垄断的法律标准——美国“运通案”的反思与互联网市场界定》,载《法律科学(西北政法大学学报)》,2021 年第 4 期,第 77-92 页;王晓晔:《数字经济反垄断监管的几点思考》,载《法律科学(西北政法大学学报)》,2021 年第 4 期,第 49-62 页。

⑦ 周汉华:《论平台经济反垄断与监管的二元分治》,载《中国法学》,2023 年第 1 期,第 222-240 页。

一 作为单一数字市场在线服务“基本法”①的《数字服务法》

(一)规制变迁

在《数字服务法》之前,欧盟在数字服务领域最为重要的规则为 2000 年生效的《电子商务指令》(2000/31/EC),②其中规定了有条件地免除中介服务提供者责任的基本框架、禁止一般监督及内部市场规则等核心原则。③ 但这一指令施行至今逾 20 年,已经显现出一定的滞后性。一方面,信息与数据在社会经济生活中的地位日益重要,数字主权、数据安全、基本权利保护、大型平台透明度、技术中立、非法内容和消费者保护等问题,越来越受到欧盟理事会和欧盟委员会的关注。另一方面,《电子商务指令》制定的初衷——确保高水平的共同体法律一体化,以便为信息社会服务建立一个没有内部边界的真实区域——却受限于其“指令”的效力,由于各国转化立法的偏差、各国在规则适用时的法律不确定性导致其最终难以实现。而这种“各自为政”的状态和成员国之间协作机制的缺乏,也导致了执法的负担与成本的叠加和重复,因而实质性地减损了《电子商务指令》的实施效果。

在《电子商务指令》之后,欧盟通过的《关于解决在线传播恐怖主义内容条例》((EU) 2021/784)④和《关于数字单一市场中的版权和相关权利指令》⑤(DSM Directive)等,均在特别法情形下松动了中介服务提供者的责任限制规则⑥。但这些个别领域的条例或指令,仅针对某些类型的服务或某些类型的非法内容,无法覆盖数字经济的所有参与者,也无法得到强制执行。近年来,欧洲议会陆续通过多项涉及数字服务

---

① Gregor Schmid and Max Grewe, Digital Services Act: Neues “Grundgesetz für Onlinedienste”? MMR 2021, 279.

② Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), https://eur-lex.europa.eu/legal-content/en/ALL/? uri=CELEX%3A32000L0031.

③ Ibid., Art.12-14, Art 15 and Art 3.

④ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=OJ:L:2021:172:FULL&from=EN.

⑤ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/? uri=CELEX:32019L0790&from=DE.

⑥ S. DIRECTIVE (EU) 2019/790 of the European Parliament and of the Council on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC, Art. 17. 3, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/? uri=CELEX:32019L0790&from=DE.

的决议,如“数字服务法——改善单一市场的运作”①“数字服务法:在线经营的商业实体的商事和民事规则适用”②“数字服务法及所涉基本权利问题”③等。这些决议几乎都主张维持《电子商务指令》所确立的核心规则,④并强调在此基础上,通过统一立法规制数字服务提供者、保护在线环境中的基本权利、内容审核及线上非法内容的处理,并呼吁加强消费者保护、公共监督和跨境执法合作等。《数字服务法》的重要目的正是对《电子商务指令》进行修订。虽然后者规定的核心原则得到了维持,但大量具体内容均被 DSA 所修正。⑤ 除此之外,DSA 的施行不影响欧盟理事会及欧洲议会制定的其他有关规范一般信息社会服务的提供、规范内部市场中介服务提供的具体规定,以及关于消费者保护、个人数据保护、版权保护的在先条例和指令的适用。⑥

(二)立法宗旨

DSA 的颁布对欧盟而言,有着至关重要的意义,也体现出欧盟在数字服务领域的核心诉求。

首先,直面数字服务带来的挑战,推动单一市场的数字化转型。欧盟委员会和欧盟理事会都清醒地认识到,作为服务贸易新形态的数字服务是如何深刻地改变着人们的日常生活,人与人之间的沟通、连接、交易和消费的方式都如同经历了“重塑”。数字服务推动了包括欧盟在内的世界各地的经济和社会转型。⑦ 尤其是“平台经济”已

---

① European Parliament, “Digital Services Act: Improving the Functioning of the Single Market (2020/2018 (INL)),” https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf? id=1636977&l=en&t=E.

② “European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on a Digital Services Act: Adapting Commercial and Civil Law Rules for Commercial Entities Operating Online (2020/2019 (INL)),” https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=uriserv%3AOJ.C_.2021.404.01.0031.01.ENG&toc=OJ%3AC%3A2021%3A404%3ATOC.

③ European Parliament, Resolution on the Digital Services Act and Fundamental Rights Issues Posed (2020/2022 (INI)).

④ “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC,” https://eur-lex.europa.eu/legal-content/en/TXT/? uri=COM%3A2020%3A825%3AFIN.

⑤ Matthias Berberich, Fabian Seip and Hengeler Mueller, Der Entwurf des Digital Services Act, GRUR-Prax 2021, 4.

⑥ Directive 2010/13/EU of the European Parliament and of the Council, Regulations (EU) 2019/1148, (EU) 2019/1150, (EU) 2021/784 and (EU) 2021/1232, (EU) 2017/2394 and (EU) 2019/1020, (EU) 2016/679 of the European Parliament and of the Council, Directives 2001/95/EC, 2005/29/EC, 2011/83/EU, 2013/11/EU, 2002/58/EC, 2001/29/EC, 2004/48/EC and (EU) 2019/790 of the European Parliament and of the Council. (whereas 10-11)

⑦ “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC Context of the Proposal,” Reasons for and Objectives of the Proposal, Para.1, https://eur-lex.europa.eu/legal-content/en/TXT/? uri=COM%3A2020%3A825%3AFIN.

成为欧盟单一市场的重要组成部分。① 自欧盟《电子商务指令》通过以来,信息传递方式和交易形式等都经历了创新和数字化转型,各成员国纷纷开始着手就此类事项进行国内立法,而这种各自立法的方式将对欧盟的单一内部市场造成负面影响。因而有必要在欧盟层面建立一套有针对性、统一、有效和相称的强制性规则,以结束内部市场的碎片化,②并确保其法律确定性,③这对单一数字市场的秩序具有重要意义。④ 并且,除非 DSA 中有例外规定,否则禁止各成员国通过国内法,对中介服务提供者规定额外的要求从而进行“加码”,以维护统一市场规则。⑤

其次,确保在欧洲建立跨境数字服务创新发展的最佳条件。数字服务是数字经济的依托,后疫情时代,产业的数字化转型与绿色转型被认为是欧洲复苏计划的两大支柱。⑥ 新冠疫情大流行将对欧洲和全球经济产生持久影响,也进一步凸显了加速欧洲数字化转型的必要性。⑦ 正因如此,抓住这一转型机遇,对于欧洲的可持续增长、竞争力、就业、繁荣,以及欧洲在全球舞台上的作用来说至关重要。而欧洲目前的数字化进程相较于美国还有明显的差距,这不仅反映在数字领域的专业技术人才、数字基础设施的缺口等方面,还体现在相关领域商业主体的相对弱势。因此,DSA 被寄予厚望,通过建立一个真正数字化的单一市场,以提供一个立足欧洲的框架,使欧洲公司能够获得成长和扩大规模,⑧进而加强欧洲的数据自主权,使欧洲成为世界上共享、保护、存储和使用数据的最佳场所。另外,《数字服务法》在对平台的规制上,比较明显的特点是“抓大放小”,对互联网“巨头”平台规定了最为严苛的义务,而对于欧盟界定的“中小企业”却给予了多重豁免。这符合欧洲目前互联网产业发展的需求,因为主要的“超大型”互联网平台运营商均为非欧盟企业。因此,以“统一”“非歧视性”的规则

① “Shaping Europe's Digital Future—Council Conclusions,” 8711/20, 9 June 2020, https://www.consilium.europa.eu/media/44389/st08711-en20.pdf.

② 包括并不限于德国的《网络强制法案》(NetzDG)、奥地利的《通信平台法》(Kommunikationsplattform-Gesetz)、法国针对打击在线非法内容的阿威娅提案(Loi Avia)(此后被法国宪法委员会宣布与宪法不符),以及脱欧之前英国的《在线安全法案》提案(OnlineSafety Bill)等。

③ DSA 鉴于条款(4)。

④ Gregor Schmid and Max Grewe, Digital Services Act: Neues “Grundgesetz für Onlinedienste?” MMR 2021, 279.

⑤ DSA 鉴于条款(9)。

⑥ “Special Meetingof the European Council (1 and 2 October 2020)—Conclusions,” https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.

⑦ 国内有学者从不同角度关注欧盟面临数字时代与新冠疫情影响之下的法律应对。参见叶斌、杨昆灏:《欧洲的权利经济转型———基于对欧洲公司可持续性尽责法的考察》,载《欧洲研究》,2022 年第 6 期,第 76-107 页;程卫东:《欧洲一体化的政策选择与未来走向》,载《人民论坛》,2020 年第 14 期,第 126-129 页。

⑧ “Special Meeting of the European Council (1 and 2 October 2020)—Conclusions”.

可以制衡大型互联网平台运营商的力量,[①]同时达到促进欧盟内部创新和产业发展的目的。

再次,重申欧盟价值观,提升欧洲话语权。数字服务领域已成为国家竞争的新方向,但与此同时也给相关服务的接受者和整个社会带来了新的风险和挑战。因此,欧盟需要采取有效的措施维护欧洲价值观,确保高水平的数据安全、数据保护、基本权利和隐私保护;维护一个安全的网络环境,其中的数字服务提供者,特别是网络中介机构,应对其行为负责;同时赋权于用户,凭借以人为本的原则,增加欧洲模式的吸引力。[②] 在欧盟领导人看来,保护和加强欧盟数字主权和在战略性国际数字价值链中的领导地位极具重要性,是确保其战略自主、全球竞争力和可持续发展的关键要素。而欧盟将利用其政策工具和监管权力,参与制定数字领域的全球规则和标准,争取数字经济国际治理的主导权,并设想将《数字服务法》作为全球范围内相关标准制定的样本。[③]

在欧盟面临新的数字服务模式与内部传统产业转型、新冠疫情与经济复苏挑战的关键时刻,《数字服务法》的通过为欧盟建立真正的数字单一市场扫清障碍,是实现欧盟 2030 年数字战略目标的里程碑立法。

二 《数字服务法》“阶梯式”平台监管的基本模式与价值内核

DSA 的总体目标是建立一个安全、可预测和可信赖的在线环境,使基本权利得到保护。[④] 为实现总体目标和欧盟在数字服务领域的核心诉求,DSA 通过对其结构与内容的设置,确立了“阶梯式”的区别规范模式。

(一)“阶梯式”监管模式的基本构造

《数字服务法》在适用和规则配置上的特征是该条例最惹眼之处。“横向”观之,即从其整体的适用范围上看,《数字服务法》适用于十分广泛的网络服务。首先,就内容类型而言,包括在线购物网站、社交网络、搜索引擎等,囊括了数字服务的绝大多数类型。除此之外,DSA 还专门针对特定内容或特定行业设置了特殊规定,例如打击恐

① Nico Gielen and Steffen Uphues, Digital Markets Act und Digital Services Act, EuZW 2021, 627.

② “Special Meeting of the European Council (1 and 2 October 2020)—Conclusions”.

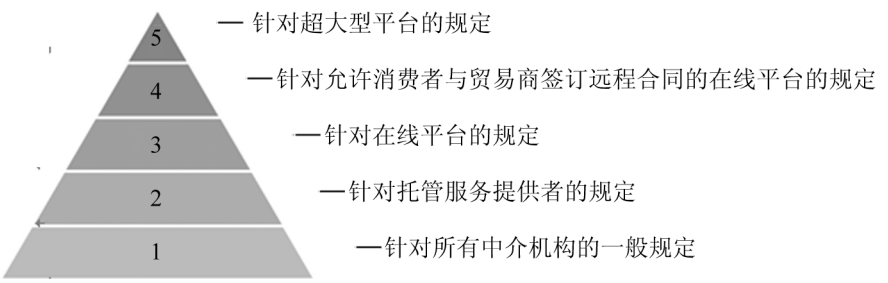
③ Proposal for DSA, Explanatory Memorandum,1, Context of the Proposal,Reasons for and Objectives of the Proposal, Para.4, https://eur-lex.europa.eu/legal-content/en/TXT/? uri=COM%3A2020%3A825%3AFIN.

④ DSA 第 1 条第 2 款 b 项。

怖主义、媒体监管和版权法的部分内容。① 其次,DSA 对“中介服务”等基本概念的界定,实际上是划定了适用范围,包括了“单纯的管道”(Mere conduit)服务、“缓存”(Caching)服务、“托管”(Hosting)服务等,并为后续区别设置“阶梯式”规则奠定了基础。

“纵向”观之,DSA 为不同的中介服务提供者设置了“阶梯式”的分级监管模式。从形式上看,整个条例的规则呈“金字塔”型,从对所有中介机构的基本义务,到对托管服务提供者的规则,再到在线平台的补充规定,最后到超大型平台的最严格措施,形成了层层的递进。其内容审查、透明度、广告、消费者保护等方面的义务,规则的严格程度都是层层进阶的,且每上一级台阶均有“补充”“添加”新的义务。不同调整类型的划分及其规则设置,是依据中介机构的性质及数字服务类型的区别而定。同属在线平台的范畴内,又依据所提供服务的特殊性(如允许消费者与贸易商签订远程合同的在线平台),以及平台的规模,进一步设定进阶监管规则。

图 1 DSA 为不同的中介服务提供者设置的“阶梯式”监管模式



注:图由作者自制。

从具体规制的技术性上看,“阶梯式”监管体现了规制的高精确度,即对“不同类型不同处理”的慎重和细致的判断。(1)“归入或排除”。例如,“考虑到有关服务的特殊性,以及使其提供者承担某些具体义务的相应需要”,DSA 在所定义的托管服务提供者这一广泛的类别中,划分出在线平台这一子类别。而允许消费者与交易者签订

① Spindler, Der Vorschlag für einneuesHaftungsregime für Internetprovider—derEU - Digital Services Act, GRUR2021, 545. 欧盟相关在先条例已有关于中介服务提供者责任特权的规定,DSA 中主要涉及在线平台的监管。

远程合同的社交网络或在线平台被定义为托管服务的提供者,他们不仅应服务接受者之要求储存其提供的信息,而且应其要求将该信息向公众传播。然而,为了避免设置过于宽泛的义务,DSA 规定如果向公众传播仅仅是次要和纯粹的附属功能,而且该功能或特性由于客观技术原因无法单独使用,则此类托管服务的提供者不应被视为在线平台。但是社交网络中的评论存储应被视为在线平台服务,只要它显然不是所提供服务的一个次要特征,即使它是发布服务接受者帖子的附属品,也被归入此类别。① 又如,超大型平台规制豁免的“扣减”。DSA 明确规定,第三章第三节及第四节不适用于微型和小型企业,或平台上消费者的交易对象为微型或小型企业的情形。但若根据第 33 条,被认定为超大型在线平台的提供者,则不得享受此豁免。② (2)“前移或后移”。与提案相比,DSA 第 18 条涉嫌刑事犯罪的报告义务、第 27 条推荐系统的透明度义务的“前移”和第 30 条交易者可追溯性的“后移”,也都体现出“阶梯式”规制中的精细度。

DSA 规定的“颗粒度”十分细密,例如,第 15 条关于中介服务提供者的透明度报告义务的规定,具体到报告中如何对各项内容进行分类。并且,针对托管服务提供商,DSA 设置了区别于其他中介服务提供者的特别规定。纵观全局,程序性的细致规定占据 DSA 的大半内容,从某种程度上,也体现出其对可实施性与可操作性方面的重视。

(二)价值内核:监管与保护的一体两面

从 DSA 对平台监管的规定中可以观察到一个明显的特征,即义务规则与权利规则的“分离”:针对中介机构以义务性的规定为主;针对服务接受者、消费者等则几乎都是对其权利的规定。可见,欧盟清晰地认识到,现代信息社会中平台与服务接受者、消费者之间实质性的不平等状态,通过 DSA 强行性规则明确地表达了价值判断上的倾斜。

平台的义务更多的其实是公法义务,其对象不是个别服务接受者或消费者,而是面向欧盟委员会、欧洲数字服务委员会、成员国数字服务协调机构、司法或行政机关等公权力部门。例如内容审查义务、透明度报告义务、设置特别机构义务、刑事报告义务等。即使是平台针对私法主体的义务,DSA 也做出为维护欧盟价值观的严格的规定和限制。例如,DSA 针对在线平台的未成年人在线保护设置的特别规范,③要求若在

① 鉴于条款 13、15。
② DSA 第 19 条、第 29 条。
③ 此条是 DSA 在提案基础上新增的规定。

线平台可由未成年人访问,则其提供者应采取适当的、合比例的措施,以确保未成年人在其服务中享有高水平的隐私保护、安全及其他相关保障;除此之外,在合理确定服务接受者是未成年人的情况下,在线平台供应商个性化广告发布的数据使用也需遵守严格的限制。① 此类规定,以及其他涉及隐私保护、个人信息保护、特定个人数据使用的禁止等,究其本质其实都是源于基本权利的保护。如前所述,DSA 针对不同类型中介机构的规则设置呈现"阶梯式",中介服务提供者的义务依据其数字服务的内容及类型、所涉及服务接受者的基本权利的可能性及广泛度而进阶,进一步凸显欧盟对数据安全、基本权利保护等方面的核心价值的维护。

三 "阶梯式"平台监管的规范构造与制度创新

(一)所有中介服务提供者的义务与责任

1. 赔偿责任的新规则

《数字服务法》对中介的规定,虽然在较大程度上坚持了以往的"避风港"原则,即中介通常不对第三方内容负责。但根据其中一项新的、特殊的规定,如果第三方所提供的作为交易对象的信息、商品和服务足以使一般消费者误认为是平台运营商自己提供或由其授权或由其控制者所提供,则在线平台应根据消费者保护法承担责任。② 除此之外,平台自有内容和第三方内容之间的区别,以及欧洲法院所提出的平台"积极作用"③的概念仍然对中介机构十分重要。因为对于并非由服务接受者,而是由中介服务提供者本身提供的信息有关的责任,不适用 DSA 中的这些责任豁免。也就是说,如果中介作为服务提供者的角色并非不知,也并非处于控制所存储信息的纯技术、自动且被动的地位,则中介将有可能承担对第三方内容的责任。④ DSA 在遵循这一理念的同时往前更进一步,明确了平台所采取的、基于善意与勤勉的自愿、主动调查,或采取其他旨在查明、识别、删除或禁用对非法内容的访问等措施,或采取必要的以遵守欧盟法律和符合欧盟法律的各国国内法的要求的措施,不会被视为排除免责条款的适

① 不得在其界面上根据 GDPR 第 4 条第(4)点定义的特征分析,使用服务接受者的个人数据发布广告。

② DSA 第 6 条第 3 款。

③ 即中介服务提供者不是仅限于通过对服务接受者提供的信息进行技术和自动处理来中立地提供服务,而是发挥积极作用,使其了解或控制该信息。

④ EuGH GRUR 2010, 445 Rn. 114 ff. Reichweite und GrenzenzulässigerAdword-WerbungUrteilvom 23.03.2010; 不同意见参见 BGH GRUR 2015, 485 Rn. 53, 57—Kinderhochstühleim Internet III。

用。①

另外,虽然 DSA 规定禁止一般监督义务,但行政当局和法院可以发布命令,停止由特定侵权内容导致的侵权行为。② DSA 在《电子商务指令》基础上的显著推进在于,对中介服务提供者规定了两项依据命令的基本义务:对非法内容采取行动的义务和提供特定个人服务接受者信息的义务。③ 中介服务提供者在收到有关国家司法或行政当局发出的上述两项命令后,均有义务采取相应措施:一方面,应向有关当局通报该命令的生效情况,不得无故拖延,并需具体说明该命令是否和何时生效;④另一方面,在命令生效时,或依命令中规定的时间,中介服务提供者应将收到的命令和其生效情况通知有关服务的接受者。

2. 所有中介服务提供者的尽职义务

为构建透明和安全的在线环境,DSA 针对所有中介机构规定了“尽职义务”(Due diligence)。⑤

首先, DSA 要求所有符合条件的中介机构均需按照条例设置特别机构。因此,中介机构势必面临管理成本的增加。根据 DSA,所有中介机构都必须建立两个“单一联络点”(Single point of Contact)。其中一个为“成员国当局、欧盟委员会和欧盟数字服务委员会(European Board for Digital Services)⑥的联络点”。DSA 要求中介机构需使该单一电子通信联络点能够以电子方式与上述机关就条例的适用直接进行沟通。⑦另一个为“服务接受者的联络点”,即要求中介服务提供者指定一个单一的联系点,使服务的接受者能够通过电子方式和对用户友好的方式直接、快速地与其沟通,并要求其允许服务接受者选择沟通方式,不应仅依赖于自动化工具。⑧ 中介服务商应公开必要的信息,以便使其单一联络点能够被轻松地识别,并与之沟通。该信息应易于访问,并应保持更新。除此之外,DSA 要求,若中介服务提供者在欧盟提供服务,却未在欧

① DSA 第 7 条。

② 如 DSA 第 4 条第 3 款、第 5 条第 2 款及第 6 条第 4 款均规定,不妨碍司法或行政当局根据成员国的法律制度要求服务提供者终止或防止侵权的可能性。

③ 该命令仅要求中介服务提供者提供其为提供服务而收集的信息,且这些信息在其控制范围内。

④ 与提案不同者在于,正式通过的 DSA 第 9 条使用了“effect”(落实、执行)一词,应是立法者刻意与提案所使用的“action”(行动)相区别,更加注重对实效的追求。

⑤ 有学者为避免误解,将此译为“尽责”义务,参见叶斌、杨昆灏:《欧洲的权利经济转型——基于对欧洲公司可持续性尽责法的考察》,第 76 页。

⑥ 依据 DSA 第 61 条而建立。

⑦ DSA 第 11 条第 1 款、第 2 款。

⑧ DSA 第 12 条,该项要求为最终通过的条例增设,在提案中并无规定,由此亦可见欧盟对服务接受者保护的重视。

盟内设立机构,则应以书面形式在其提供服务的成员国之一,指定一名法人或自然人作为其“法定代表”(Legal Representative)。所指定的法定代表若不遵守 DSA 规定的义务,将可能被追究个人责任。① 这些规定实际上是对所有中介服务提供者提出了更高的“特别机构”设置的要求,其目的在于促进欧盟相关机构与非欧盟中介服务提供者的沟通,在“看得见摸不着”的网络环境下,促使相关中介服务提供者在欧盟境内建立更为直接的、实际的联系。但如此势必造成中介服务提供者管理成本的增加。

其次,DSA 还针对所有中介服务提供者规定了内容审查的“加强版”透明度要求。这主要包括两个方面:其一,内容审核规则的公开义务。根据 DSA,中介服务提供者应当在可公开访问的条款和条件②中,明确其使用限制和内容审核的规则,③该限制应客观、相称,并且合比例,同时应考虑服务接受者的基本权利和其他利益,④而且在条款和条件发生任何重大变更时,应当告知服务接受者。若中介服务主要面向未成年人或者主要由未成年人使用,则应当以未成年人能够理解的方式说明使用服务的条件和限制。其二,内容审核年度报告的公开义务。中介服务提供者应至少每年一次,以机器可读的格式和易于访问的方式,就其在相关期间内进行的任何内容审核提供清晰、易于理解的报告。并且对于报告中所应披露的内容做出具体详细的规定,如要求包括从成员国当局收到命令的情况、主动内容控制及其他相关的服务限制、通过内部投诉处理系统收到的投诉数量、为内容审核目的而使用的任何自动化手段等。如此详细的透明度要求,可能对中介服务提供者的商业秘密保护构成挑战。

(二)对托管服务提供者的进阶要求

之前针对托管服务提供商的“通知—删除”(Notice-and-take-down)程序将进阶到“通知—行动”(Notice-and-action)程序(第 16 条)。与以往相同的是,如果中介机构获知非法内容,但并没有立即删除或阻止,则中介机构需对该非法内容负责。DSA 在此基础上进一步明确,托管服务提供者应建立机制,允许任何个人或实体将其认为属于非法内容的具体信息通知托管服务提供者,该机制应对用户友好,并应允许完全通过电子手段完成通知提交。托管服务提供者应及时向报告者确认收到报告,不得无

① DSA 第 13 条。对法定代表的追责并不影响对中介服务提供者的追责和诉讼。

② 根据条例,“条款和条件”是指规范中介服务提供者和服务接受者之间合同关系的所有条款,无论其名称或形式如何。

③ 包括用于内容审核的任何政策、程序、措施和工具的信息,如算法决策和人工审查,以及其内部投诉处理系统的程序规则。

④ DSA 第 14 条在提案的基础上增设四项,分别为条款与条件重大变更的告知义务、对未成年人的特别说明责任、超大型平台与超大型搜索引擎的告知义务、补救机制和语言要求。

故拖延,并且需及时、谨慎和客观地进行处理,①对结果提供合理反馈。如果所涉内容被阻止或删除,则必须以通俗和合理的方式通知上传者理由和说明。

除此之外,DSA 规定了广泛的涉刑事犯罪的通报义务。这被认为是超出《电子商务指令》的“新行动义务”,即如果托管服务提供者所获信息使其怀疑存在刑事犯罪,②则有义务通知相关成员国执法或司法当局。在提案中,涉嫌刑事犯罪的通报义务被规定在专门针对在线平台提供者的附加条款一节(第三章第三节第 21 条),而在最终通过的条例中被置于适用于包括在线平台在内的托管服务提供者的附加条款一节(第三章第二节第 18 条)。在层层递进的“阶梯式”监管中,DSA 通过扩大可能涉及刑事犯罪的信息获取与通报义务的主体范围,明确表达了尊重与保护个体生命及安全的价值取向。由此也课以托管服务提供者更为明确的“守门人”的职责。

(三)对在线平台规制的再升级

对在线平台③的规制属于 DSA 的重点之一,其对在线平台所应承担的义务方面总体上提出了更进一步的要求。

1.内部投诉处理系统

在线平台的一项新的核心义务是创建“内部电子投诉处理系统”(Internal Complaint-handling System)。在服务接受者(包括提交通知的个人或实体)不同意网络平台提供者在收到通知后做出的决定,或者反对在线平台提供者以服务接受者提供的信息构成非法内容等为由做出的决定时,④在决定做出后六个月内,在线平台应向服务接受者提供有效的内部投诉处理系统。该系统必须易于访问、对用户免费、不得仅自动化处理,并且网络平台提供者必须及时、无歧视、勤勉、非武断地处理投诉。

此外,用户有权选择任何获得认证的庭外争端解决机构来解决与投诉处理决定有关的争议,相关服务的接受者也有权在任何阶段依法向法院提起诉讼,对网络平台提供者的这些决定提出异议。同时,DSA 明确规定庭外争端解决机构无权将具有约束力的争端解决方案对当事人强制执行。在费用承担方面,DSA 规定,如果庭外争端解

① DSA 第 16 条,如果托管服务提供者使用自动化手段进行处理或决策,还应当告知报告人。

② S. Directive 2011/36/EU of the European Parliament and of the Council, Directive 2011/93/EU or Directive (EU) 2017/541 of the European Parliament and of the Council.

③ 在 DSA 规范语境下,“在线平台”(Online Platform)是区别于一般托管服务提供商的特别主体。根据第 3 条 i 款,“在线平台”是指应服务接受者的要求,为公众存储和传播信息的托管服务,除非该活动是另一项服务的次要和纯粹的辅助功能,或主要服务的次要功能,并且由于客观和技术原因,不能在没有其他服务的情况下使用,而且将该功能或特性纳入其他服务并不是规避本条例适用的手段。

④ 包括删除或禁止访问信息的决定、暂停或终止服务的决定、暂停或终止收款人账户的决定,以及暂停、终止或限制将服务接受者提供的信息货币化的能力的决定。

决机构做出有利于服务接受者的裁决,则网络平台提供者应承担庭外争端解决机构收取的所有费用,并赔偿服务接受者为解决争端而支付的任何其他合理费用。在这方面,DSA 把握住了内部冲突解决及庭外争端解决的趋势。①

2.设置“受信任的举报人”(Trusted Flaggers)与防止滥用措施

成员国可以授予公共或非公共机构“受信任的举报人”②地位,这些机构具有特殊的专业知识、能独立代表集体利益,并以谨慎和客观的方式提交通知。在线平台提供者应采取必要的技术和组织措施,确保“受信任的举报人”在其指定的专业领域内,通过前述“通知—行动”机制提交的通知得到优先考虑,并不得无故拖延相关的处理和决定。但如果在线平台提供者发现“受信任的举报人”提交了大量不够精确、不准确或未经充分证实的通知,应该告知并提供相应材料给授予该“受信任的举报人”地位的数字服务协调机构。如果数字服务协调机构认为有正当理由展开调查,则应立即进行,不得无故拖延,并且在调查期间应暂停该“受信任的举报人”的身份。

针对频繁提供明显违法内容的服务对象,在线平台提供者在明确而详细的标准公示的前提下,并在发出事先警告后的合理期限内,应暂停对其提供服务。同时,针对经常提交明显没有根据的通知或投诉的投诉人,应暂停处理其通知和投诉。

3.在线平台提供者透明度的进阶义务

根据 DSA 规定,在线平台提供者的透明度报告除需符合条例第 15 条针对所有中介服务提供者的透明度报告义务的规定之外,关于上述电子投诉处理及防止滥用措施的情况应被纳入其透明度报告。除此之外,从 2023 年 2 月 17 日起,至少每六个月一次,每个在线平台或在线搜索引擎均需在其在线界面的公开部分,公布该服务在欧盟范围内平均每月的活跃接受者的信息。在线平台或在线搜索引擎提供者应与数字服务协调机构和欧盟委员会建立联系,依其要求提供上述信息,该信息应更新至被要求之时,并不得无故拖延(第 24 条)。③

DSA 要求,若在线平台提供者在其在线界面上展示广告,则必须提高在线广告的透明度,确保用户能够清晰、明确地识别每个显示的信息是否属于广告(通过醒目的标记)、是何自然人或法人的广告、广告付费人、向目标群体显示的主要参数及其可能

① RL 2013/11/EU, TMG nF; § § 13 ff.

② “受信任的举报人”可由机构依申请获得,这些机构可以是公共性质(如“欧洲刑警组织”等)、私人性质或半公共性质(如 INHOPE 等)。参见 DSA 鉴于条款 61。

③ 数字服务协调机构或欧盟委员会可要求在线平台或在线搜索引擎的提供者提供有关该款所述计算的额外信息,包括对所使用数据的解释和证实,但该信息不应包括个人数据。

的修改方式。这一要求能够提高个性化广告的可识别性。需要注意的是,目前 DSA 虽并未完全禁止个性化广告,但限制了使用目标对象信息的范围。①

备受关注的算法透明度问题,也反映在 DSA 的规定中最终通过的条例,在提案的基础上新增了在线平台提供者的推荐系统透明度义务。② DSA 要求,使用推荐系统的网络平台提供者应在其条款和条件中,以通俗易懂的语言说明其推荐系统中使用的主要参数,以及服务接受者修改或影响这些主要参数的选择。前述主要参数应解释为向服务接受者推荐的某些信息,至少包括:(1)确定向服务接受者推荐信息的最重要的标准。(2)这些参数相对重要性的原因。如果推荐系统提供了几种选择,已确定向服务接受者呈现信息的相对顺序,则在线平台的提供者还应当提供使服务接受者能够选择并随时修改其首选项的功能,且该功能能够直接而便利地被访问。因此,DSA 无疑对在线平台提供者提出了重大的考验,要求其进行艰难的平衡:一方面必须将其算法作为商业秘密对竞争对手保密;另一方面又要以可理解的方式向用户解释各种因素如何影响这些推荐系统。

4.在线界面设计与组织的“不干涉”义务

与传统影响他人意思自治的情形相比,在线平台借助数字服务的特殊性,可能通过更为隐蔽的方式,对相对人做出决定的过程施加影响。鉴于此,DSA 新增规定(第 25 条),要求在线平台的提供者在设计、组织或操作其在线界面时,不得欺骗或操纵其服务对象,或以其他方式实质性地干扰或损害其服务对象在自主和知情的情况下做出决定的能力。③ DSA 明确,欧盟委员会可就此类内容进行具体限制,例如在要求服务接受者做出决定时,更加突出某些选择项;反复要求服务的接受者在已经做出选择的情况下再做出选择,尤其是通过呈现干扰用户体验的弹出窗口等方式;使终止服务的过程比订阅服务更困难等。

(四)适用远程合同④的在线平台提供者的特别义务

DSA 在提案的基础上,新设置了一节适用于允许消费者与交易者签订远程合同

① 在线平台的提供者不得使用欧盟 2016/679 号(GDPR)第 9(1)条提及的特殊类别的个人数据或根据第 4 条第(4)点定义的解释,向服务接受者展示广告。

② 推荐系统的透明度义务,在提案中规定在超大型在线平台及超大型在线搜索引擎提供者义务(第 29 条)之中。但在正式通过的 DSA 中将其“前移”,规定为一般在线平台的义务(第 27 条)。

③ 前述这一禁令不适用于 2005/29/EC 指令或(EU) 2016/679 法规中所涉及的行为。

④ 根据条例规定,“远程合同”(Distance Contract)是指第 2011/83/EU 号指令第 2 条第(7)款所定义的“远程合同”。

的在线平台提供者的附加条款。①

商家提供商品的在线市场平台需履行新的“商家追踪”义务(第 30 条)。② 在线市场平台应当按 DSA 的要求收集商家的信息,包括:(1)名称、地址、电话号码及电子邮件地址;(2)符合要求的身份证明文件或其他电子身份证明的副本;(3)商家的支付账户信息;(4)商家的登记簿信息及其登记号等识别信息;(5)商家承诺仅提供符合欧盟法律适用规则的产品或服务的承诺书。虽然商家应对上述信息的准确性负责,但 DSA 要求此类平台在允许商家使用其服务之前,应尽最大努力评估及核实其信息,可要求商家更正、更新和补全不完整的信息,并在必要时暂停有关服务。③ 平台对所掌握的商家信息负有安全储存的义务,直到与有关商家的合同关系结束后的六个月,随后应删除。平台应在展示相关商家产品或服务的界面,以清晰、便利和易于理解的方式向服务接受者披露上述第(1)(4)(5)项信息。只有根据法律规定要求、DSA 第 10 条的命令、成员国主管当局或欧盟委员会发布的命令,平台才能向第三方披露商家其他信息。平台的在线界面设计需满足信息披露的合规要求。允许消费者与交易者签订远程合同的在线平台提供者应确保其在线界面的设计和组织方式,能够使商家遵守其在欧盟法律下关于先合同信息、合规性和产品安全信息的义务,例如,商家需提供的关于运营商的名称、地址、电话号码和电子邮件地址的信息;应确保其在线界面的设计和组织方式,能够允许商家提供为清晰明确地识别其产品或服务所必需的信息,包括商标、Logo 等识别商家的标志和符合欧盟产品安全与合规性的标识等。并且,平台应尽最大努力评估及随机核查商家所提供的产品或服务是否为非法。

DSA 保障消费者的信息获取权。如果在线平台提供者通过某种方式获知,商家已通过其服务向位于欧盟的消费者提供了非法产品或服务,则在线平台提供者应告知该消费者关于产品或服务为非法的事实、交易者的身份、相关的补救措施等。若无相关消费者的联系方式,则应在其在线平台公开这些信息。

(五)对超大型平台与超大型搜索引擎的“超强监管”

DSA 广为人知的突出特点在于专门针对“超大型在线平台”(Very Large Online Platforms, VLOPs)和“超大型在线搜索引擎”(Very Large Online Search Engines, VLO-

① 该节规定不适用于允许消费者与符合 2003/361/EC 号建议所定义的微型或小型企业(包括其失去该地位后的 12 个月内)的交易商签订远程合同的在线平台提供商。

② 类似于金融领域的“尽职调查”,即“了解你的客户”原则(Know Your Customer)。该条在提案中规定在第 22 条,因而提案中是针对在线平台的义务,而通过的条例是(后移一步)针对提供远程合同签订可能的在线平台。由此也显示了较为明显的“阶梯式”监管及追求条例适用的精确性。

③ 商家若有异议,可依据条例第 20 条、第 21 条提出投诉。

SEs)[①]提供者规定了管理系统性风险的额外义务。欧盟委员会认为,其对公共舆论的影响,及其作为交换意见的信息来源功能可能引发特殊风险。[②]

“超大型”的标准,是指在欧盟内平均每月活跃的服务接受者人数等于或高于4,500万的网络平台和网络搜索引擎。欧盟委员会可依据欧盟人口的情况调整这一标准,使其相当于欧盟届时人口的10%。该计算方法可由欧盟通过授权法案的方式规定,DSA特别明确,该方法的确定必须考虑到市场和技术的发展。若在线平台或在线搜索引擎的提供者未遵守关于活跃用户透明度报告义务,“超大型”的身份也可以直接由欧盟委员会指定。但是,如果在连续一年的期间内,在线平台或搜索引擎的月平均活跃用户数低于上述标准,则由欧盟委员会确定终止该项指定。相关平台及搜索引擎在被指定或终止指定的情形下,均享有四个月的缓冲期。DSA要求欧盟委员会在欧盟官方公报上公布所指定的超大型在线平台和超大型在线搜索引擎的名单,并保持更新。对VLOPs提供者,DSA规定了前所未有的“超强监管”。

1.风险评估、风险减轻和管理的特殊合规义务

(1)风险评估义务。VLOPs的提供者应努力识别、分析和评估欧盟内因其服务及相关系统(包括算法系统)的设计或运作,或因使用其服务而产生的任何系统性风险。在评估的时点方面,DSA要求评估应至少每年进行一次,并需在部署可能对此风险产生关键性影响的功能之前进行评估。评估的风险包括:通过其服务传播非法内容、对行使基本权利的负面影响、对公共舆论和公共安全的负面影响、对基于性别暴力的负面影响、对保护公共卫生的负面影响、对未成年人的负面影响,以及对个人身心健康的严重不利影响等。VLOPs应针对其服务,特别是其推荐系统、其他相关算法系统的设计和内容审核、适用的条款和条件及其执行、选择和展示广告的系统、供应商的数据等因素进行风险评估。其评估应与系统性风险相称,考虑到其严重性和概率。评估还应分析风险是否以及如何受到有意操纵及其对服务的影响,包括:对服务的非真实使用或自动利用、非法内容和不符合其条款与条件信息的放大、潜在的快速、广泛传播的可能性。

(2)风险减轻和管理义务。VLOPs应针对特定系统性风险制定合理、相称、有效的减轻措施,但需特别考虑其对基本权利的影响。此类措施包括:调整服务的设计、特

① 为行文便利,本文以下以VLOPs同时指代超大型在线平台和超大型在线搜索引擎二者,多数情况下DSA对二者的规定一致,若对二者有区分规定之处,本文将特别说明。

② DSA鉴于条款第54条。

性或功能(包括其在线界面、条款和条件及其执行、内容审核程序、算法系统及推荐系统、广告系统、信息标记等);启动或调整“受信任的举报人”,与其他在线平台的合作;加强系统性风险的监测;特别针对未成年人规定包括年龄验证和家长控制工具,帮助未成年人发出遭受虐待信号或酌情获得支持的工具等。在关于 VLOPs 不合规的处理上,DSA 较为明显地提高了官方来源内容的公开度。①

与 DSA 的提案相比,上述两个部分规定的内容有了较为明显的扩展和细化,而 DSA 更进一步,新增一条针对 VLOPs 的危机响应机制(第 36 条)。DSA 规定,如果极端情况导致对欧盟或其中重要部分的公共安全或公共健康造成严重威胁,则应视为发生了“危机”。此时,欧盟委员会可以根据欧盟数字服务委员会的建议做出决定,要求 VLOPs 评估其服务与运作是否促成危机,确定并应用具体、有效和相称的措施等。欧盟委员会做出该项决定所要求的行动必须是绝对必要、合理和相称的,附有合理的准备期限和实施期限,且必须及时通知决定所针对的网络服务提供者,并予以公开。鉴于危机的后续演变,欧盟委员会可以根据欧盟数字服务委员会的建议对决定进行修正。

2.独立审计义务

VLOPs 的提供者应接受至少每年一次自费的独立审计。所谓“独立”,即要求审计机构独立于有关的 VLOPs 提供者,以及与该提供者有关的任何法人,并与其不存在任何利益冲突。符合条件的审计机构必须在风险管理、技术能力等方面具有公认的专长,并且具有经证明的客观性和职业道德,遵守业务守则或适当标准。VLOPs 的提供者应提供必要的配合和协助,允许审计机构审查所有相关数据和场所,回答口头或书面问题,不得阻碍、不当影响或破坏审计工作。因此,DSA 体现出在系统性风险、商业秘密保护和公共安全之间的平衡拿捏:首先,要求 VLOPs 协助配合、提供数据和场所;其次,课以审计机构严格的保密义务(第 37 条第 2 款第 2 段);再次,为防止滥用而要求保密义务的遵守不得妨害关于透明度、监督和执行的规则。如果 VLOPs 提供者收到非“正面”②的审计报告,审计机构应适当考虑向其提出业务建议,并建议其采取必要的措施予以落实。在收到这些建议后一个月内,VLOPs 应制定一份审计实施报告,并且对于不予执行的业务建议,在审计执行报告中说明理由和替代措施。

3.严苛的透明度要求

---

① Matthias Berberich, Fabian Seip and Hengeler Mueller, Der Entwurf des Digital Services Act, GRUR-Prax 2021, 4.

② “正面”与否的界定参见 DSA 第 37 条第 4 款。

DSA 针对 VLOPs 规定了近乎苛刻的数据及算法的透明度要求。首先,表现在接受数据访问与审查的义务。DSA 要求 VLOPs 提供者应依设立地数字服务协调机构或欧盟委员会的合理要求,于合理期限内,向其提供必要数据的访问权限,以监测和评估对 DSA 的遵守。同时,VLOPs 应依要求解释其算法系统,包括其推荐系统的设计、逻辑、运作和测试。① 数字服务协调机构和欧盟委员会由此所获取的数据应仅用于监测和评估 VLOPs 的合规情况,并充分考虑提供者和有关服务接受者的权利和利益,包括保护个人数据、保护机密信息(特别是商业秘密),以及维护其服务的安全。其次,符合特定资格(第 40 条第 8 款)的研究人员可以向 VLOPs 设立地的数字服务协调机构申请②作为“经过审查的研究人员”(Vetted Researcher),从而通过协调机构的要求而获得对特定 VLOPs 的数据访问权,但其唯一目的是进行有助于发现、识别和了解欧盟系统性风险的研究。VLOPs 提供者除非由于无法获取该数据或者获取数据将导致其服务安全或保护机密信息(特别是商业秘密)方面的重大漏洞这两个原因,否则不可向协调机构申请修改访问要求。且 VLOPs 提出修改请求,还需包含替代手段的建议,而协调机构尚可再次做出决定。再次,欧盟委员会在 DSA 授权下还可以进行补充立法,对 VLOPs 与研究人员共享数据的具体条件、客观指标、程序等进行规定,同时需顾及服务接受者的个人信息保护和 VLOPs 的商业秘密保护。

在透明度报告方面,DSA 对 VLOPs 设定了补充性的“最高台阶”规则。除需满足前述透明度要求之外,还需针对其“进阶”义务进行透明度报告。DSA 根据所涉事项之不同而区别规定报告的期限及间隔:第一类,依据第 16 条、第 20 条及第 22 条,关于提供不同语言文本等义务的落实情况的报告;第二类,依据第 34 条、第 35 条及第 37 条,关于风险、审计等义务的落实情况的报告。在此,DSA 明确,如果 VLOPs 认为上述第二类报告中公布的信息可能导致 VLOPs 或服务接受者的机密信息被泄露、对其服务的安全造成重大漏洞、破坏公共安全或损害服务接受者,则可以从公开报告中删除这些信息。但仍应将完整的报告转交给设立地的数字服务协调机构和欧盟委员会,并附上从公开的报告中删除信息的理由说明。

---

① 在推荐系统方面,条例要求超大型网络平台和超大型网络搜索引擎的提供者除了遵守前述针对在线平台所使用的推荐系统的规则之外,还必须为其各个推荐系统分别提供至少一个不基于 GDPR 第 4 条第(4)点进行分析的选项。依据 GDPR 第 4 条第(4)点,“分析”指任何形式的个人数据自动处理,包括使用个人数据评估与自然人有关的某些个人方面,特别是分析或预测有关该自然人的工作表现、经济状况、健康、个人偏好、兴趣、可信度、行为、位置或活动。

② 根据 DAS 第 40 条第 9 款,研究人员也可以向他们所属研究机构的成员国的数字服务协调机构提交申请。该数字服务协调机构在收到根据本段提出的申请后,应对各研究人员是否符合第 8 款规定的条件进行初步评估,然后将申请、证明文件和初步评估结果,发送给(VLOPs)设立地数字服务协调机构。

关于在线广告透明度,DSA 要求提供在线广告的 VLOPs,应当通过“应用程序接口”(Application Programming Interfaces,API)及允许多标准查询的可搜索的、可靠的工具,在其在线界面的一个特定部分汇编并公开提供一个自动访问的“存储库”(Repositories),其中包含有关广告的内容、广告商和针对特定目标群体等信息。VLOPs 应尽合理努力,确保信息的准确性和完整性,并且应确保存储库中不包含任何广告服务接受者的个人数据。

除此之外,DSA 还在多处体现了针对 VLOPs 进阶的透明度要求,包括要求 VLOPs 应以清晰明确的语言向服务接受者提供简明、易于访问的条款和条件的摘要、可用的补救措施和补救机制(第 14 条)、以其提供服务的所有成员国的官方语言发布其条款和条件。

4.合规职能部门作为必设机关

DSA 对 VLOPs 的合规要求是以在 VLOPs 的核心治理结构中“安插”合规审查部门为保障的。DSA 对合规部门的级别、负责人地位、职责及任职保护均进行了尽可能周密的安排。具体而言,DSA 要求 VLOPs 应设立独立于其运营职能的合规职能部门,且 VLOPs 的管理机构为确保合规职能部门的独立性,应界定、监督、负责其治理结构的实施,包括组织结构内的责任划分、防止利益冲突、健全系统性风险的管理。合规职能部门应由一名或多名合规专员组成,包括合规职能部门的负责人。该部门应具有足够的权力、地位和资源,并有权接触(公司)管理机构,以监督其合规情况。DSA 要求:VLOPs 确保合规职能的负责人是独立的高级管理人员,其应对合规职能负有明确责任;合规部门负责人应直接向管理机构报告,并可在存在前述风险或不合规情况将影响或可能影响 VLOPs 时,向管理机构提出关切和发出警告;在合规部门任职保护方面,未经管理机构事先批准,VLOPs 不得解除合规职能部门负责人的职务;合规部门的合规专员有义务与设立地数字服务协调机构和欧盟委员会合作,确保条例规定的所有风险得到识别、适当报告,同时采取合理、相称和有效的风险减轻措施;合规部门还应当组织和监督与独立审计相关的活动,告知和建议 VLOPs 的管理层和雇员条例规定的相关义务,并监督其合规情况等。

这些要求实际上使得合规部门与(公司)监事会或独立董事的地位类似,但 DSA 却未明确是否可由这些部门及其负责人“兼任”此职务,抑或必须再单独设立合规职能部门。并且,从根本上而言,合规专员必然仍为 VLOPs 的雇员,这可能是带在企业血液里的先天性矛盾,他们之间如何能够避免利益冲突,以实现 DSA 预设的合规部门

的独立地位不无疑问。

四 《数字服务法》平台监管的影响与评价

欧盟在 DSA 的立法准备阶段,对于平台监管措施的选择曾提出“一个基准线,三个方案”。所谓“一个基准线”,是指保留并继续执行彼时已有的规则,即“鸵鸟战术”:一方面对数字服务日益增长的风险视而不见;另一方面放任成员国各自立法。这样不仅无法有效打击非法活动、保护整个欧盟公民的基本权利,还将阻碍新的创新服务在内部市场扩大规模,成员国和数字服务提供者都将面临过高的成本,单一数字市场越发遥不可及。鉴于此,欧盟提出“三个方案”:方案一是较为保守的“最小改动”方案:针对在线非法内容,为在线平台规定一系列程序性义务,包括必要的保障措施;同时,主张成员国当局建立行政合作机制,并建议通过“数字清算所”(Digital Clearing House)解决跨境问题,促进信息流动。方案二是在方案一所提出的措施之外,建议取消数字服务提供者对在线非法内容采取自愿措施的阻滞,并采取提高推荐系统和广告透明度的措施。在执法合作方面,在每个成员国任命一个中央协调机构。方案三是相对而言措施最为强硬的,以前述措施为基础,设计了一套有针对性的、不对称的措施,对极易给欧盟社会和经济带来最高风险的超大型在线平台课以更严格的义务,并建立一个联结欧盟及成员国的、强化监督和执法权力的综合系统。

DSA 最终选择在方案三的基础上进行建构。虽然目前 DSA 刚实施,还无法评估其实际影响,但可以预期的是 DSA 将给欧盟内部带来一系列的积极影响。首先,充分支持欧盟中介服务提供者,尤其是初创企业,在统一内部市场的发展与扩大。虽然对这些企业来讲,DSA 规定其履行尽职义务,这在一定程度上增加了固定成本,但是这一成本是可预期和可计算的。据估计,这一增加的成本可以与通过规则的统一而减少的由成员国立法分散带来的合规成本相抵消。① 并且,伴随着平台企业的发展,相关受其支撑及向其提供支撑的实体经济产业也将连带受益。② 其次,对各成员国当局而言,DSA 将显著降低各成员国现有各自立法模式下,在合作中的低效、重复及分别协

① Proposal for DSA, Explanatory Memorandum, Impact Assessment, https://eur-lex.europa.eu/legal-content/en/TXT/? uri=COM%3A2020%3A825%3AFIN.

② 据欧盟委员会估计,2020 年,欧盟境内贸易将增长 1%至 1.8%,即相当于跨境产生的营业额增加 86 亿欧元,最高可达 155 亿欧元。“Impact Assessment of the Digital Services Act,” 15 December 2020, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act.

商带来的成本。虽然成员国将承担设置新的机构的费用或承担已有的主管当局的相关费用,但预计效率收益将远超成本。再次,DSA 在赋权平台打击非法内容的同时,也提供了欧盟公民在平台上表达意见等基本权利的保障。如获得有效补救的权利、不受歧视的权利、儿童权利,以及获得个人数据和隐私保护的权利。

然而,DSA 的实施一方面依赖企业的合规,另一方面依赖执法。① 在各成员国内部,其实仍有欧盟委员会未提及(却未必是未曾考虑)的困境,可能对 DSA 的实施效果产生一些影响。首当其冲的就是各成员国在 DSA 生效之后,仍需处理 DSA 和各国已有相关立法之间的关系问题。② 如在德国,欧盟《电子商务指令》第 12—15 条已通过德国的《电信媒体法》(Telemediengesetz,TMG)第 7—10 条转化为德国法律。但这些责任规则在《数字服务法》的立法中被删除并"重写",规定在第 4 条及其后的条款中,大大扩展了对中介机构的监管。③ 因而 TMG 中的相应规范将面临挑战。有学者主张 TMG 中相应条款在将来应被废除。也有学者认为,基于《数字服务法》所调整的仅限于信息社会服务,也就是仅适用于调整基于商业基础提供的服务,而 TMG 的调整范围并不限于此,因而 TMG 第 7—10 条应可保留,④但出于法律明确性的原因,应明确其范围将仅限于非商业服务提供商。而 TMG 第 7 条第 4 款⑤也可以不受任何限制地保留,因为《数字服务法》没有规范相关责任基础的规则。并且,在德国境内,与证据相关的制度规则依然由 TMG 等国内法来规制。此外,德国在 2017 年出台的《网络执法法》(Netzwerkdurchsetzungsgesetz,NetzDG)及其修正案,是打击网络犯罪内容的核心支柱。从德国的角度来看,主要问题是 DSA 的规则能否改善对犯罪内容的打击。但有学者对 DSA 能否达到德国国家层面规定的保护水平持怀疑态度。⑥ 这势必也涉及标准更高的成员国法律,在 DSA 实施之后,能否以及如何适用的问题。此类成员国内部立法的整合,势必也将带来不小的成本,毕竟《电子商务指令》运行已久,在此基础上

① Niko Härting and Max Valentin Adamek, Digital Services Act—ein Überblick, CR 2021, 165-171.

② Ruth Janal, Friendly Fire? Das Urheberrechts-Diensteanbieter-Gesetz und sein Verhältniszum künftigen Digital Services Act, GRUR2022, 211; Jürgen Kühling, "Fake News" und "Hate Speech"—Die Verantwortungder Medienin-term-ediäre zwischen neuen NetzDG, MStV und Digital Services Act, ZUM 2021,461.

③ 根据鉴于条款第 16 条,欧盟电子商务指令中规定的,中介服务提供者有条件免责的横向框架应予以保留。然而,考虑到在国家层面转换和应用相关规则时存在的分歧,并出于清晰和一致的原因,该框架应被纳入《数字服务法》中。考虑到欧盟法院的判例法,也有必要对该框架的某些内容进行澄清。

④ Sesing- Wagenpfeil, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 18.5 Beweisfragen, Rn. 156f.

⑤ 该条是关于知识产权受侵害的规则:如果用户使用远程媒体服务侵犯了他人的知识产权,并且该权利的所有者没有其他方法可以补救其受侵害的权利,该权利的所有者可以根据第 8 条第 3 款要求服务提供者阻止该信息的使用,以防止侵权行为的再次发生。阻止必须是合理和相称的。除第 8 条第 1 款第 3 句的情况外,不应存在根据第 1 句要求服务提供者补偿主张和执行的庭前和庭外费用的索赔。

⑥ Eisenreich: Digital Services Act—ein wirksames Instrument gegen Hass undHetze im Netz? RDi 2021,289.

各国的不同门类的专项立法不在少数。

此外,DSA 在版权与数据保护等个别方面的规制也被认为是不充分的,可能会造成大量的监管“逃逸”。① 同时,尽管 DSA 已经尽量明晰、细致,但监管机构和科技巨头之间可能会就如何应用 DSA 展开数月甚至数年的冲突。尽管世界主要大型科技平台企业表示将遵守规则,但其面对如此严厉的“掣肘”不会束手就擒。

DSA 设置的“阶梯式”监管及其对超大型平台的“超强监管”,可以说是“板子打在别人身上”,对欧盟内部企业影响不大,眼下至多也是监管成本问题,而承担较重义务的超大型平台企业大多来源于欧盟以外。对此,欧盟委员会认为,虽然超大型平台在风险管理、尽职等方面承担了较重的义务,但这些公司具有最广泛的影响力、营业额甚巨,因而这些要求是与他们的合规能力相匹配的。② 同时,DSA 规定:成员国对未能遵守本条例规定义务的最高罚款金额为有关中介服务提供者在上一财政年度全球营业额的 6%;对提供不正确、不完整或有误导性的信息,未答复或未纠正不正确、不完整或有误导性的信息,以及未接受检查的行为,可处以最高罚款金额为中介服务提供者或有关人员上一财政年度年收入或全球营业额的 1%。并且,服务的接受者有权根据欧盟及成员国法律,就中介服务提供者因违反 DSA 规定的义务而遭受的任何损害或损失向中介服务提供者寻求赔偿。这种“超强惩罚”也构成对超大型平台企业的威慑。作为“假想敌”的超大型平台确实对“超强监管”表现出焦虑和遗憾:DSA 的规则可能会抑制全球科技公司开发创新数字工具,而这些创新工具能够帮助欧洲企业重建业务。③ 因此,DSA 的负面影响当然并不止步于超大型平台,因为受其支持而销售产品或提供服务的企业,以及支持超大型平台的上下游科技企业都可能受到不同程度的波及。所以,DSA 的实施可能反而会在一定程度上减缓欧洲的经济复苏。

除此之外,ChatGPT 等“大型生成式 AI 模型”(Large Generative AI Models, LGAIMs)在内容的形成方面所具有的强大能力已日益引发人们的关注。而对其所形成的内容仅依靠 AI 自身的算法控制远非足够,如果不对此加以适当控制,可能会将假新闻和仇恨言论引至前所未有的水平。而 DSA 的适用范围并未包括 LGAIM,④因此,

---

① Gerald Spindler, Ein europäischer Neuanfang in der Haftung und Plattformregulierungdurch den Digital Services Act? GRUR2022, 593.

② Proposal for DSA, Explanatory Memorandum, Impact Assessment, https://eur-lex.europa.eu/legal-content/en/TXT/? uri=COM%3A2020%3A825%3AFIN.

③ Karan Bhatia, “The Digital Services Act Must not Harm Europe's Economic Recovery,” https://blog.google/around-the-globe/google-europe/the-digital-services-act-must-not-harm-europes-economic-recovery/.

④ 可能最接近的是托管服务提供商,但其要求信息是由服务接受者(用户)所提供(DSA 第 3(g)(iii)条)。然而,在使用 LGAIM 的情况下,相关内容显然不是由用户提供的,而是由 LGAIM 本身形成的内容。

对 LGAIM 内容的监管就只能由成员国的立法来完成,因而差异化、碎片化、响应迟缓,以及成员国之间协调工具的缺乏将是可预见的未来。

五 中国平台监管的路径选择

欧盟的立法者所期待的规则扩张和成为全球范围内的标准制定者的目标会实现多少?毕竟欧盟在这方面曾经有过一定的经验,①并期待热衷于对平台企业"强干预"的立法者能够从 DSA 中寻找灵感,模仿制定本国规则,借此实现规则的输出,并作为被继受一方而掌握价值判断和解释的话语权。另外,欧盟期待全球科技公司认为,实施全球统一的合规策略来监管内容更具成本效益,而欧盟的法规基准相对更严格,以此为全球统一的标准,不合规的风险较小。

在欧盟的"强监管"模式之外,美国作为超大型平台的"强输出"端,在 1996 年颁布的《通信规范法》(Communication Decency Act,CDA)第 230 条(以下简称 CDA230 条)设立了平台豁免规则,互联网平台无须为第三方使用者张贴的言论内容负法律责任;同时,允许互联网平台基于"善意原因封锁和屏蔽冒犯性内容"。这一规则是美国"互联网自由"价值理念的体现,并进一步在网络平台等领域被确立为"网络中立"原则,即互联网服务提供商必须同等对待来自各方的所有内容。② 2009 年颁布的《美国复兴与再投资法》(American Recovery and Reinvestment Act of 2009),被认为是对"网络中立"原则的确认。③ 但在近十年之后,2018 年的《恢复互联网自由指令》(FCC Releases Restoring Internet Freedom Order)却一举废除了该原则,④由此,网络服务提供者可以为用户提供差异化服务而无须承担责任。2023 年 1 月 11 日,拜登再次呼吁通过国会立法,进一步加强对于大型科技公司的监管,加强隐私保护,使大型科技公司对其

① 即所谓"布鲁塞尔效应"问题,如 GDPR 的全球性规则输出,参见金晶:《个人数据跨境传输的欧盟标准——规则建构、司法推动与范式扩张》,载《欧洲研究》,2021 年第 4 期,第 107-108 页。

② Tim Wu, "Network Neutrality, Broadband Discrimination," *Journal of Telecommunications and High Technology Law*, Vol.2, 2003, p.141. 据此原则,互联网服务提供商(ISP)应属于公用设施,不同类型的网络服务与内容不应被区别对待;公众有权"自由"地访问,反对内容屏蔽与付费优先等歧视性规则。

③ https://www.fcc.gov/general/american-recovery-and-reinvestment-act-2009.

④ 在此之前的 2017 年,联邦通信委员会(Federal Communications Commission,FCC)通过投票废除了该原则。S. Keith Collins, "Why Net Neutrality Was Repealed and How It Affects You," *The New York Times*, December 14, 2017.而 FCC 对提案的考量可能受到大型科技公司的"民意造假"影响,参见 S. Edward Walker, "Millions of Fake Commenters Asked the FCC to End Net Neutrality. 'Astroturfing' is a Business Model," *The Washington Post*, May 14, 2021。

传播的内容和使用的算法负责,包括推动对 CDA230 条的修改等。① 在司法方面,谷歌案②与推特案③均涉及 CDA230 条款,被认为是挑战了网站享有的(提供托管服务并推荐恐怖主义内容的)广泛责任豁免。④ 然而,从立法层面来看,无论是在隐私保护还是平台责任方面,美国的做法其实是“雷声大雨点小”。⑤ 这其中除了两党议员的争议和分歧之外,经济复苏与鼓励数字经济国际竞争也是核心的政策考量,因而美国未来确立如欧盟“强监管”模式的可能性很小。

英国脱欧后,在立法方面也开始逐渐偏离欧盟立场,2022 年,查尔斯王子在代表伊丽莎白女王发表的“女王议会演讲”中表示,将促进《数据改革法案》(Data Reform Bill)的通过,以体现英国在数据与隐私保护方面区别于欧盟《一般数据保护条例》(以下简称 GDPR)的立场,简化并明确数据保护框架制度及规则,减轻企业的风险和负担,支持充满活力的竞争和创新,以推动经济增长。⑥

近年来,中国出台了一系列推进国家数字经济快速转型和升级的重要文件。如 2022 年 12 月发布的《关于构建数据基础制度更好发挥数据要素作用的意见》,构建了中国数据基础制度的“四梁八柱”,⑦其中不难发现“安全”“监管”等词语出现的频率并不逊于“发展”“促进”等关键词。可见中国已经意识到应当通过立法等制度措施,使数字经济在安全的大前提下,通过科学的、最小成本的规制激活发展潜能,面向未来发展壮大。但是,反观中国近年来在数字领域的立法,几乎是对欧盟相关法规亦步亦趋的跟随和效仿。如在隐私与数据保护方面,中国《个人信息保护法》《数据安全法》等均不同程度地借鉴并对标欧盟 GDPR,⑧国家互联网信息办公室公布的《网络数据

① https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411.

② Gonzalez v. Google, https://law.justia.com/cases/federal/appellate-courts/ca9/18-16700/18-16700-2021-06-22.html.在该案中,恐怖主义受害者家属声称,被告的社交媒体平台允许 ISIS 发布视频和其他内容来传达恐怖组织的信息,谷歌、推特和脸书对 ISIS 的国际恐怖主义行为负有直接和次要责任。原告冈萨雷斯对谷歌提出了直接和次要责任索赔。

③ Twitter, Inc. v. Taamneh, https://www.scotusblog.com/case-files/cases/twitter-inc-v-taamneh/.

④ Greg Stohr, “Social Media Company Liability Draws Supreme Court Scrutiny,” Bloomberg News, Retrieved October 4, 2022.

⑤ 在 2021 年中美两国都对数字平台“重拳出击”后,统计发现(截至 2021 年 11 月底)和 2020 年同期比,中国多个互联网企业,如腾讯、阿里股价分别跌了超过 20%和 50%,但美国科技巨头谷歌、微软、苹果的股价涨幅都超过 40%。美国的“强监管”似乎有“适得其反”的促进作用。

⑥ Department for Digital, Culture, Media & Sport, “Data: A New Direction,” https://www.gov.uk/government/consultations/data-a-new-direction.

⑦ 王轶:《加快构建数据基础制度,助推数字经济和数字文明建设》,国家发展和改革委员会, https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221219_1343657.html。

⑧ 如《个人信息保护法》在个人信息的定义、个人信息处理的合法性基础、同意规则、敏感信息的处理规则、数据出境制度、信息主体的知情权、行政监管方面均对标 GDPR。

安全管理条例(征求意见稿)》《个人信息出境标准合同规定(征求意见稿)》,以及国家市场监督管理总局制定的《互联网平台分类分级指南(征求意见稿)》《互联网平台落实主体责任指南(征求意见稿)》中很多内容亦均向欧盟看齐。

中国数字经济发展状况与美国、欧洲均不相同。① 中国平台企业价值规模虽居于世界第二位,但头部平台与美国的差距在不断扩大,而欧盟则几乎没有头部平台。② 毫无疑问,欧盟的"强监管"将对中国大型、超大型数字企业构成一定程度的束缚,而中国国内规则如果依旧"加码",而非如美国般在国内对自己的企业"放水""补血",再加上近年来愈演愈烈的美国对中国大型数字企业的"围剿",③那么中国的数字企业生存的综合环境堪忧。

欧盟《数字服务法》在立法理由、立法技术、规制思路和规范设置等方面,为各国数字经济立法与监管提供了参考,通过对《数字服务法》的立法研究,能够获得一些有益的经验和启示。但是,《数字服务法》是在欧盟的数字服务产业及利益背景下制定的,中国的平台监管不应该不加区分地照搬照抄。

(一)规制升级与体系性整合

鉴于《数字服务法》的立法理由,反观中国在数字服务领域的法律规制,能够发现一些存在的问题,最突出地表现在规定的分散性,从《民法典》《电子商务法》《网络安全法》《个人信息保护法》《互联网信息服务管理办法》《信息网络传播权保护条例》等法律法规,到《网络主播行为规范》《互联网视听节目服务管理规定》等规章,再到包括国家网信办的《网络数据安全管理条例(征求意见稿)》等系列规范性文件、最高人民法院发布的相关司法解释,以及各行业协会制定的细则。目前中国的规范模式是按照"事项"进行立法,即平台内不同的内容受不同规范调整。这将进一步衍生出几个问题:首先,缺乏针对所有类型互联网平台的总括性规则。然而,目前综合类平台日益增长,平台内容和服务多元化,最典型的例子就是在线社交平台扩展到音视频传播、再扩展到直播带货等电子商务。同时,基于对创新与发展的鼓励,中性平台增多,"事项"型立法必然会存在一些不适应之处。其次,规出多门,必然导致各方较高的执行成本。对于不同主管部门而言,执法过程中肯定会带来较多的重复并提高协调成本;对平台

① 中美欧形成全球数字经济发展的三极格局。2021年,从规模看,美国数字经济蝉联世界第一,中国位居第二,欧洲已成为全球数字经济的"第三极"。参见中国信息通信研究院:《全球数字经济白皮书(2022年)》。

② 参见中国信息通信研究院政策与经济研究所:《平台经济与竞争政策观察(2021年)》。

③ 拜登政府以"国家安全"为由,要求"字节跳动"出售其持有的TikTok股份,否则该应用程序将在美国遭到封禁,https://www.wsj.com/articles/u-s-threatens-to-ban-tiktok-if-chinese-founder-doesnt-sell-ownership-stake-36d7295c。

而言,分散的规则相较于统一规则将带来较高的合规成本;对于消费者及平台服务使用者而言,如涉及侵权、投诉等问题,多头规定一方面加重了其认识负担,另一方面也容易造成重复处理。因此,借鉴欧盟 DSA 的立法,中国在数字服务领域针对互联网平台监管制定统一的上位规定有其合理之处。具体而言,建议制定行政法规级别的规范性文件,统一调整数字服务领域的平台监管。

在规制思路方面,DSA 的“阶梯式”规制有一定合理性,一定程度上考虑到平台经营模式、所涉事项的内容和规模,把不同类型平台的“权力”和所涉法律关系背后的利益格局与价值取向作为规则区别设置的依据。例如,超大型平台因其所涉用户(包括平台内经营者及消费者、服务接受者等)范围之众,其行为及所造成的影响可能直接关涉到公共利益,因此,其在风险控制及涉及公共安全方面必然需要承担比小型企业更多的注意义务。

同时,正如有的学者指出,在诸多法律领域,可以看到一种趋势,即由于复杂性增加,立法机关对实体法律和法规的关注度越来越弱,而对程序规范(程序化规则)的关注度越来越强。① DSA 的立法也体现出这种趋势,一方面注重程序性规定,保证条例的操作和执行;另一方面注重负责机关的设置、机关之间职权和协调的规定。而中国现有法律和行政法规的规则制定大多不够细致,缺乏可操作性。与作为欧盟层面的立法相比,中国的法律和行政法规的“颗粒度”更粗,稍微细致化的规则大多都在规章层面。但由于针对不同事项的主管部门亦不相同,程序化与细致化的规则必然不尽一致,在执法端与平台企业合规端都会造成困境。中国的统一上位规则也应该借鉴 DSA 在这方面的思路,指定统一部门作为专门负责机构,②并且对其职权、机构间协调、执法等制定较为细致的规定。

(二)发展与保护并重的监管策略

中国在数字服务领域既有反对美国数字霸权的需求,又有鼓励和促进本国有竞争力的企业参与国际市场的需求,这就意味着必须在欧盟和美国模式之外探求一条适合中国的平台监管与规制路径。中国平台监管应该确立发展与保护并重的监管策略:立足于中国数字服务领域发展现状,着眼数字经济未来竞争,考虑到对本国平台经济的影响,确立平衡保护数字服务企业和服务接受者、消费者以及公共利益的监管规则。

在具体规则的设置上,应分析不同规则的调整内容和规范目的,评估其规范的功

① Sheplyakova, Prozeduralisierung des Rechts, Mohr Siebeck, 2018, S. 2.

② 在既往研究中,也有学者主张应建立独立专业的平台监管机构,参见高薇:《平台监管公用事业理论的话语展开》,载《比较法研究》,2022 年第 4 期,第 171-185 页。

能与利弊,包括与中国立法的价值判断及产业政策是否一致,不可一概而论。如 DSA 明确,在平台属于微型和小型企业时,关于在线平台的附加义务的规定(除透明度报告义务外)及关于针对允许消费者与交易者签订远程合同的在线平台提供商的附加条款可豁免适用。这一做法能够在对一般或大型平台企业设定较强监管措施的同时,促进小微企业的创新和创业。①

另外,DSA 针对超大型平台设置的风险管控义务、透明度义务、独立审计义务、合规职能部门设置义务等“超强监管”措施,涉及数据安全与开放、算法公开、隐私保护等问题,②必须立足于中国数字产业发展的具体情况进行分析。企业对其经营策略、商业秘密等享有正当权益,在数据时代,无论对于成功的大型平台企业,还是对于初创的数字服务企业而言,对算法的保护都应属于其核心商业秘密,是其市场竞争力的依托。中国的数字产业发展现状与欧盟有较为明显的差异,具有竞争力的大型数字企业是国际竞争的排头兵,而对创新型小微企业的培育、保护和发展也关乎中国数字经济的未来竞争力,因此,在设置监管措施时应合理考量企业的正当权益。

其一,DSA 中针对 VLOPs 规定的多数义务,性质上均属于公法义务,例如风险评估与管理义务、独立审计和透明度义务等。而对于市场主体的企业课以公法义务,应当分别论证其足够充分的、基于公共利益的合理性和合比例性的边界。③ 仅以履行诸项义务之报告为例,DSA 针对 VLOPs 规定了风险评估年度报告、部署特定功能前的评估报告、风险减轻报告、危机响应报告、审计报告、透明度报告等诸多类型的报告义务,若在加上前序几个“阶梯”所要求的报告义务,可想而知,企业仅为履行此类事无巨细而烦琐的报告,就将付出极大的成本,其合理性、合比例性和实际效用均有待考量。尤其是在履行失当之时,将会面临基于全球年度营业额的巨额罚款,这是“超强监管”与“超强干预”的“达摩克利斯之剑”。

其二,DSA 对上述各项报告与信息披露事项要求之具体,在大数据时代可能对企业的经营秘密构成挑战,至少会增加企业在保护商业秘密方面的成本。除此之外,DSA 还规定,VLOPs 有接受数据访问与审查的义务,除应向官方解释其算法系统之

① 鉴于 DSA 设置的制度优惠,中国应鼓励具有竞争力的中小型数字服务企业积极参与欧洲市场。

② 已有学者关注到相关问题,如关于数据公开和访问问题,参见王锡锌、黄智杰:《公平利用权:公共数据开放制度建构的权利基础》,载《华东政法大学学报》,2022 年第 2 期,第 59-72 页;王洪亮、叶翔:《数据访问权的构造——数据流通实现路径的再思考》,载《社会科学研究》,2023 年第 1 期,第 71-84 页。

③ 非基于公共利益等足够充分且正当理由,不应限制民事主体之自由,参见王轶:《民法价值判断问题的实体性论证规则——以中国民法学的学术实践为背景》,载《中国社会科学》,2004 年第 6 期。中国已有学者关注到涉及平台责任的合比例性相关问题,参见余佳楠:《网络服务提供者的妨害人责任以合比例性为中心》,载《中外法学》,2021 年第 6 期,第 1638-1657 页。

外,还需要对“经过审查的研究人员”开放数据访问权。虽然,DSA 对审查机构和研究人员均提出保密要求,也看似赋予了 VLOPs 适当的“防御性”手段,但也难掩 DSA 在基本立场上的严苛,可见,该义务将对 VLOPs 的商业秘密构成严峻挑战。因此,中国在平台监管的立法中亦应对此慎之又慎,毕竟对于面临全球竞争的互联网企业而言,商业秘密将是其核心竞争力。

其三,DSA 中引发美国数字巨头反抗最多的严格限制是“定向化广告”及“推荐系统透明度”等规定,其本质上是将基于公民信息自由权的基本权利延伸至民法上对弱势意义上平等主体之间[①]自决权的干预。这种干预在涉及 DSA 所援引的 GDPR 第 4 条第(4)点,即对服务接受者的个人数据进行分析的限制,尤其是对于未成年人等弱势群体的保护上,具有充分的合理性。但除此之外,以尊重自决为前提,以比例原则为限制,赋予用户选择权是否即为足够,以及在何种范围和程度上需对平台推送的算法进行披露和公开不无疑问。对于此类 DSA 中的监管措施,包括而不限于上述所举诸项,中国均不应不加斟酌地借鉴。

(**作者简介**:王天凡,北京航空航天大学法学院副教授;**责任编辑**:蔡雅洁)

① 王轶:《民法价值判断问题的实体性论证规则——以中国民法学的学术实践为背景》,第 104-116 页。