科研人员数据访问权：欧盟网络平台内容治理的新工具

——欧盟《数字服务法》第40条及其启示*

张飞虎

摘　　要：网络平台是一把双刃剑。它一方面为信息交流提供了便利，另一方面也使非法和有害内容的传播达到了前所未有的程度。就平台内容治理而言，当前所采用的“委托治理”模式陷入了困境和僵局。作为破解这一难题的尝试，欧盟在《数字服务法》中引入了科研人员数据访问权这一新的治理工具。科研人员数据访问权的权利主体仅限于符合条件的经审查研究人员，而义务主体则是月活跃用户数达到一定标准的超大型在线平台或搜索引擎的提供者。数据访问活动本身必须符合比例原则，尤其不得侵害网络平台的合理利益和网络用户对个人数据的合法权益。此外，科研人员的数据访问活动还需要在数字服务协调人这一中介机构的协调下进行。欧盟引入科研人员数据访问权的做法对我国网络平台内容治理具有启示意义。

关 键 词：科研人员数据访问权；　网络平台内容治理；　欧盟；　数字服务法

作者简介：中南财经政法大学　法学院　讲师　硕士研究生导师　数字法治研究院　研究员　武汉　430037

中图分类号：D99

文献标识码：A

文 章 编 号：1005－4871(2023)06－0096－22

* 本文受中央高校基本科研业务项目“电商直播营销的法律规制研究”(项目批准号：31512210605)资助。

一、问题的提出

就信息交流和传播而言，网络平台是一把双刃剑。一方面，它将数十亿用户与海量内容连接起来，为用户参与广泛的在线交流提供了机会，满足了网络用户的各种需求，并不断产生新的沟通和信息渠道。[①] 另一方面，网络平台的出现也为非法和有害内容的传播打开了方便之门。恐怖暴力言论、煽动仇恨和挑起对立的言论、侮辱诽谤言论、虚假信息、恶意信息、淫秽色情信息等非法和有害内容的传播速度和广度也达到了前所未有的程度。正如欧洲人权法院所言："明显非法的言论，包括仇恨言论和煽动暴力的言论，可以在几秒钟内以前所未有的方式在全球传播，有时此类言论还会在网上存在很长时间。"[②]从寻亲男孩刘学洲、粉发女孩郑灵华自杀，武汉被撞小学生妈妈跳楼身亡，到法国因警察枪杀17岁非洲少年所引发的大骚乱，可以看出，非法和有害内容的传播不仅严重威胁人们的人格尊严乃至生命财产安全，而且还会引发更严峻的社会问题，甚至是国家安全问题。因此，如何高效监管及治理网络非法和有害内容的传播是各国监管机构所面临的共同课题。

鉴于网络平台在信息交流中所发挥的中介作用及其所具有的技术优势，各国在对网络平台内容进行治理时基本都要求网络平台也参与治理并承担相应责任。[③] 在这一思路的指导下，网络平台内容治理逐渐形成了所谓的"委托治理"模式(Delegated Governance)。[④] 在这种治理模式中，政府退居网络信息审查的幕后，但为了强化其对网络空间表达的治理角色，仍通过大量的法律法规为网络平台设置网络信息审查责任，对网络信息服务实行行政许可制，甚至直接对网络平台发布行政命令，要求平台屏蔽政府禁止访问的网站、过滤政府认定的敏感词汇、协助政府确认违法信息发布者的身份信息、协助删除违法信息并对信息发布者采取技术

① Vgl. Martin Nettesheim, „Die unionsrechtliche Regulierung großer Internet-Plattformen: Die Kommissionsentwürfe für einen Digital Markets Act und einen Digital Services Act", *Bundestagsdrucksache 19(21)136*, S. 12.

② Delfi AS v. Estonia App no 64569/09 (ECHR, 16 June 2015) [110].

③ European Commission, "Tackling Illegal Content Online — Towards an Enhanced Responsibility of Online Platforms", COM (2017) 555 final, p. 2.

④ See Jonathan Peters/Brett Johnson, "Conceptualizing Private Governance in a Networked Society", *North Carolina Journal of Law & Technology*, Vol. 18, Is. 1, 2016, pp. 15 - 68, here pp. 33 - 36. 在原文中，"委托治理"模式是指想要压制言论自由的政府官员通过向作为中介机构的网络平台施压，要求其删除有关言论的情形。但同时作者又指出，"委托治理"模式与所谓的"依法治理"模式(governance through legal compliance)在理论上是类似的。而后者同样是指政府要求网络平台删除有关言论，只不过其理由不再是压制言论自由，而是因为相关言论违反了法律规定。本文在后一种意义上使用"委托治理"这一概念，以便更好地体现其中所蕴含的行政机关向网络平台让渡部分治理权力的内容。

惩罚措施。[①]

从表面上看，这种“委托治理”模式似乎可以较好地解决网络平台的内容治理问题，具有简便、高效、隐蔽等优势，公权力监管机构可以避免与网络用户之间产生直接冲突以及可能由此引发的责任。[②] 但网络平台提供者是以营利为目的的私主体，[③]这一本质特征与其在平台内容治理过程中事实上是具有准立法权、准行政权和准司法权的市场规制主体[④]之间存在天然张力，这就会导致“委托治理”模式不可避免地出现失灵的情形。其原因一方面在于，在天然的逐利动机以及市场竞争压力的驱使之下，平台企业会利用算法、热搜、搜索排名等技术手段或技术权限，将某些信息从互联网海量信息中提取出来，以获得用户的优先浏览权，从而获取流量和经济利益。[⑤] 另一方面，平台企业又利用自己掌握的规则制定权，事先排除自己对这些信息可能引发侵权结果的责任。[⑥] 此外，由于网络平台运行过程中复杂的技术特征以及建立在大数据基础上的算法推荐、算法审核等网络技术的大规模应用，向平台追责的难度进一步增大。[⑦] 面对这种情况，监管机关通常会直接要求网络平台限期采取删除、断开链接等措施，否则就要承担罚款等行政责任。[⑧] 这又会进一步加剧作为委托人的监管机构和作为代理人的网络平台之间的紧张关系，导致“柠檬问题”的产生。[⑨] 不仅如此，“委托治理”模式下平台内容治理还存在着内容过滤过度、压制言论自由、侵害网络用户基本权利等其他问题。[⑩]

---

① 李延枫：《网络平台内容治理的公法规制》，载《甘肃政法大学学报》，2022年第2期，第50－63页，这里第52页。

② Hannah Bloch-Wehba, “Global Platform Governance: Private Power in the Shadow of the State”, *SMU Law Review*, Vol. 72, Is. 1, 2019, pp. 27－80, here p. 30；李延枫：《网络平台内容治理的公法规制》，第52页。

③ 蒋慧：《数字经济时代平台治理的困境及其法治化出路》，载《法商研究》，2022年第6期，第31－44页，这里第32页。

④ Hannah Bloch-Wehba, “Global Platform Governance: Private Power in the Shadow of the State”, pp. 29－30；刘权：《网络平台的公共性及其实现——以电商平台的法律规制为视角》，载《法学研究》，2020年第2期，第42－56页，这里第44－45页。

⑤ 参见何若：《丑闻八卦霸榜新闻热搜，真是网友“搜”出来的？》，2023－07－04，https://news.bjd.com.cn/2023/07/04/10484354.shtml，访问日期：2023－11－11。

⑥ 参见孙逸啸：《网络平台自我规制的规制：从权力生成到权力调适——以算法媒体平台为视角》，载《电子政务》，2021年第12期，第69－79页，这里第73页。

⑦ 参见 Teresa Rodríguez de las Heras Ballell, “The Background of the Digital Services Act: Looking Towards a Platform Economy”, ERA Forum (2021) 22, pp. 75－86, here p. 78；李鲤、余威健：《平台“自我治理”：算法内容审核的技术逻辑及其伦理规约》，载《当代传播》，2022年第3期，第80－84页，这里第83页。

⑧ Hannah Bloch-Wehba, “Global Platform Governance: Private Power in the Shadow of the State”, p. 31.

⑨ 参见李怡然：《网络平台治理》，上海：上海人民出版社，2021年版，第17页。

⑩ 同注①，第53页。

以上困境和问题的产生都与网络平台在事实规制主体的身份下所采取的治理行为不透明有关。因此，要求网络平台提高透明度、开放治理过程，不仅对于上述问题的解决具有重要作用，也有助于提升网络内容治理的效率和效果。在数字化的背景下，要求互联网平台开放其收集和掌握的数据可能是提高平台治理过程透明度的重中之重。这对于我们理解平台的算法如何运行、哪些内容和广告会被推荐、平台如何处理非法和有害内容、平台如何适用其制定的规则等问题具有重要意义。[①] 而在当前，我们无法获得或无法完整获得相关的数据。其原因在于，一方面，由于法律限制和保持竞争优势等多方面的原因，网络平台主动披露的数据严重不足或所提供的数据质量不高；另一方面，对于研究机构所进行的研究活动，网络平台同样态度消极甚至采取抵抗措施。[②] 在这种背景下，欧盟在《数字服务法》[③]（Digital Services Act，下文简称DSA）第40条第4款中引入了科研人员数据访问权，为在数字化背景下解决网络平台内容治理进行新的尝试。[④] 该款规定意味着研究人员的数据访问权被首次写入欧盟法律文件，具有重要的理论和实践意义。[⑤] 为了在制衡网络平台力量、避免过度干扰平台企业正常经营以及促进欧盟内部创新和产业发展等诸多目标之间实现平衡，欧盟立法者在引入科研人员数据访问权时较为谨慎，对这一权利从权利义务主体的构成要件、数据访问活动本身须满足的条件以及科研人员数据访问权的实施程序三个方面进行了限制。下文在结合DSA具体规定的基础上，从以上三个方面对科研人员数据访问权进行研究，并揭示其对我国平台内容治理可能有益的启示。

---

① 参见 Mathias Vermeulen，“The Keys to the Kingdom”，https://knightcolumbia.org/content/the-keys-to-the-kingdom，访问日期：2023－11－11。

② 以脸书（Facebook）为例，一方面它发起了所谓的“社会科学一号”（Social Science One）学术数据访问方案，然而该方案又因为脸书的拖延而进展缓慢。另一方面，对于纽约大学研究人员为进行科学研究在脸书上收集政治广告内容和数据的行为，脸书向其发送勒令停止函，信中不仅要求他们停止数据收集活动，而且还要删除已经收集的所有数据。参见 Jeff Horwitz，“Facebook Seeks Shutdown of NYU Research Project Into Political Ad Targeting”，*Wall Street Journal*，23 October 2020，https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533，访问日期：2023－11－11。

③ 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)，OJ L 277，27.10.2022，p.1.

④ 需要说明的是，DSA第40条中存在两种数据访问机制，一种是DSA第40条第1款规定的监管机构的数据访问机制，另一种是第4款中的科研人员数据访问机制。前者实际上是世界大多数国家网络监管机构都已经采用的监管手段，因此不是本文讨论的对象。

⑤ Paddy Leerssen，“Platform Research Access in Article 31 of the Digital Services Act”，*Verfassungsblog*，2021－09－07，https://verfassungsblog.de/power-dsa-dma-14/，访问日期：2023－11－11。

二、权利及义务主体的构成要件

(一)权利主体的构成要件

根据DSA第40条第4款的规定,“经审核研究人员”(vetted researchers)有权提出数据访问的请求,他们是研究人员数据访问权的适格权利人。但DSA第40条第8款规定的措辞表明,“经审核研究人员”并不是一个永久身份,也就是说,“经审核研究人员”这一身份只与特定的研究项目相关,一旦项目完成或者由于其他原因被终止,那么“经审核研究人员”的身份也将随之失效。[①] 当相关研究人员进行下一项研究时需要再次申请成为“经审核研究人员”,才能再次获得数据访问权。因此,研究人员数据访问权的权利主体资格需要根据个案进行判断。根据DSA第40条第8款的规定,研究人员只有同时满足该款规定的所有条件时,才能通过审核,成为“经审核研究人员”。其中第8款(a)(b)(c)(g)项可以视为权利主体的构成要件,具体包括隶属性要件和独立性要件。

1. 隶属性要件

隶属性是指申请获得“经审核研究人员”身份的研究人员必须隶属于欧盟2019/790号指令[②](即《数字单一市场版权指令》,以下简称《版权指令》)第2条第1款所定义的某一研究组织〔DSA第40条第8款(a)项〕。《版权指令》第2条第1款规定:“研究组织指大学(包括其图书馆)、研究机构或任何其他实体,其主要目标是开展科学研究或开展涉及科学研究的教育活动,即(a)以非营利方式或将所有利润再投资于其科学研究;或(b)符合成员国认可的公共利益使命;在这种情况下,对该组织具有决定性影响的企业不能优先获得该科研成果。”据此可以认为,在认定研究组织时,其法律形式和组织方式并不重要,关键在于该组织是否以非营利的方式或者以国家认可的方式为公共利益开展活动。其中,“以国家认可的方式为公共利益开展活动”的形式可以有多种,比如由公共部门提供研究资金、国家法律法规或公法合同对此做出明确规定等。[③]

《版权指令》第2条第1款明确规定,大学(包括其图书馆)和研究机构是毫无疑问的研究组织,其他实体在符合要求的情况下也可以被认定为研究组织。DSA

① DSA第40条第8款规定中的“for the specific research”表明“经审核的研究人员”的身份适用于特定的研究项目。

② Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copy Right and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p. 92.

③ Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, *Zeitschrift für IT-Recht und Recht der Digitalisierung* (*MMR*), MMR-Beilage, 2022, S. 827 – 837, hier S. 830.

序言第97条则进一步明确指出，研究组织可包括以支持公共利益为主要目标而开展科学研究的民间社会组织，这种民间社会组织主要指各种非政府组织（NGO）和公益协会等。[①] 根据该立法理由的措辞可以得出如下结论：与大学（包括其图书馆）和研究机构相比，民间社会组织是否属于研究组织还需要在个案中进行判断。易言之，只有在符合《版权指令》第2条第1款所规定条件的情况下，民间社会组织才可以被认定为DSA第40条第8款(a)项意义上的“研究组织”。其中，具有重要意义的是《版权指令》第2条第1款中提出的“对该组织具有决定性影响的企业不能优先获得其科研成果”这一要求，因为对于民间社会组织而言，其资金来源主要来自于社会捐助，其中来自企业或私人的捐助占有很大比例。这可能会对由企业出资设立的研究机构产生不利影响。如果研究机构受到商业企业的决定性影响，例如企业由于组织结构的原因能够以出资人或股东的身份行使控制权或决定权，从而可以优先获得研究成果，那么这些机构就不满足《版权指令》第2条第1款的规定，也就无法成为DSA第40条第8款所要求的研究组织。[②]

此外，在根据《版权指令》第2条第1款认定“研究组织”时还需要注意的是，相关组织的活动必须主要面向科学研究。虽然欧盟的立法和司法判例没有对“科学研究”这一概念进行定义，但根据德国联邦宪法法院的观点，“科学研究”是指任何以一定方法、以可验证的方式系统性地获取新知识的智力活动。[③] 这本身已经是一个内涵和范围都十分宽泛的定义，《版权指令》立法理由第12条又进一步将科学研究的范围从自然科学拓展到了社会科学领域。因此可以认为，在认定研究组织的活动是否属于“科学研究”时不应过于严苛。但需要指出的是，《版权指令》的立法者对“科学研究”这一概念加上了“主要面向”的限定词。这一限定词意味着，即使一个组织所从事的活动符合上述“科学研究”的定义，如果其并不是该活动的主要目标，那么该组织也不能被认定为“研究组织”。例如，出版机构或记者协会等类似组织可能会受到这一限定的影响。它们的活动虽然也大致符合“科学研究”的定义，但这并非其首要目标，因此它们通常不符合《版权指令》第2条第1款中“研究组织”的要求。[④]

---

① 参见DSA序言第97条。

② Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, S. 830.

③ BVerfG 35, 79, 113. 鉴于德国《基本法》和《欧盟基本权利宪章》第13条之间的密切关系，德国联邦宪法法院对科学研究所作的定义对欧盟也具有借鉴意义。Matthias Ruffert, in Christian Calliess/Matthia Ruffert (Hrsg.), *EUV/AEUV*, München: C. H. Beck, 6. Aufl., 2022, GRCh Art. 13, Rn. 1; Thilo Weichert, „Die Forschungsprivilegierung in der DS-GVO“, *Zeitschrift für Datenschutz* (*ZD*), Heft 1, 2020, S. 18 – 24, hier S. 19; Alexander Rossnagel, „Datenschutz in der Forschung“, *Zeitschrift für Datenschutz* (*ZD*), Heft 4, 2019, S. 157 – 164, hier S. 158.

④ 同注②。

2. 独立性要件

独立性是指申请“经审查研究人员”身份的研究人员要独立于商业利益〔DSA第40条第8款(b)项〕。为了保证科研人员的独立性,DSA立法者又在第8款中提出了两项要求。首先,根据第8款(c)项,申请研究数据访问权时,研究人员应当在其申请中披露其研究资金的来源情况。公开研究资金来源情况有利于审核人员判断提交申请的研究人员是否满足独立性要求,由此可以在一定程度上防止假借科学研究之名实则追求商业利益情况的发生。其次,第8款(g)项还规定,在研究活动结束之后,科研人员还需要在保护知识产权的前提下无偿公开其研究成果,使公众可以在一定时期内自由获取。该项规定有助于进一步支持研究人员的独立性,因为如果研究成果被强制无偿公开,研究活动的资助人、发起人和执行人将无法独享研究成果,这会降低以追求商业利益为目标的资金对数据访问活动的支持兴趣,从而阻断研究人员和商业利益之间的关联。

独立性要件表明,欧盟立法者可能不愿意将数据访问权授予这样一些研究机构,即它们开展的研究活动虽然属于成员国认可的公共利益使命范畴,但它们同时也追求商业利益,而且其所获商业利益没有被全部再投资于科学研究(参见《版权指令》第2条第1款规定)。[①] 依此理解,非政府组织和企业作为控制人或者股东的研究机构可能不符合独立性要求。由于它们与出资企业之间存在密切联系,再加上“商业利益”这一概念的内涵和外延都具有一定的模糊性,因此,如何判断研究机构所获商业利益涵盖的范围以及这些商业利益的使用是否被全部再投资于科学研究等都面临着非常大的不确定性。由此,独立性要件可以在很大程度上避免科研人员数据访问权被滥用并蜕变为企业或商业组织获取他人数据的工具。

(二)义务主体的构成要件

根据DSA第40条第4款的规定,科研人员数据访问权的义务主体是超大型网络平台或搜索引擎的提供者,他们有义务向获得“经审查研究人员”身份的研究人员提供其研究所需的数据。[②]

1. 网络平台范围的限缩

在DSA第3条(i)项中,欧盟立法者将“网络平台”定义为一种应服务接受者的要求,存储并向公众传播信息的托管服务。但同时又指出,如果这种信息托管服务仅仅是与另一服务有内在联系、具有次要且纯粹附属的功能,或者是主要服务的次要功能,并且由于客观的和技术上的原因,这种信息托管服务在没有相应

① Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, S. 830.

② 需要指出的是,根据DSA第40条的规定,无论是监管机构的数据访问权还是科研人员的数据访问权,其义务主体都是超大型网络平台或搜索引擎的提供者。

的另一服务或主要服务的情况下无法使用，并且两种服务的整合不是规避DSA中适用于网络平台规则的手段，则不应将托管服务提供者视为网络平台。[①] 例如，在线新闻服务的评论服务很明显就是在线新闻服务的次要和附属功能，相比之下，社交媒体的评论服务，即使表面上看附属于社交媒体的发帖功能，但只要其不具有明显的次要服务的特征[②]即可被视为信息托管服务。[③] 由此可以将一部分以生成内容为主要业务的平台，例如在线新闻平台排除出科研人员数据访问权的义务主体范围。

出于尊重通信自由和言论自由等基本权利的考虑，DSA立法者还将电子邮件和私人通讯服务提供者排除出“网络平台”的范畴，理由是“网络平台”定义中的“向公众传播信息”是指向潜在的不受人数限制的人群提供信息〔DSA第3条(k)项〕。易言之，不论实际的信息访问是否发生，网络平台的任意用户都可以方便地获取信息，而不需要提供信息的服务接受者人为决定或选择哪些人可以访问这些信息。而在电子邮件和私人通讯服务中，用户如果想要获得信息还需要满足登记注册或通过验证等信息提供者所设置的条件，如此一来，这就是一种在提供信息的服务接受者所确定的有限人数之间的信息传播服务，而不属于“向公众传播信息”。但这种排除也并非绝对，如果电子邮件或私人通讯服务的提供者能够代表用户向潜在的无限数量用户提供信息，而这些用户并不是由信息提供者决定的，例如通过公共聊天群组，则也可以适用DSA。[④] 根据上述理解，对于微信和WhatsApp这样的即时通讯服务而言，当其作为用户之间的聊天工具时，它们便不属于“网络平台”；但是，当它们通过自有频道或管理权限向不特定用户发送信息时，它们就符合了DSA第3条(i)项中“网络平台”的定义，从而成为DSA的规制对象。

2.“超大型”平台的判断

DSA第40条第4款明确规定，只有“超大型”网络平台和搜索引擎服务的提供者才是科研数据访问权的义务主体。[⑤] 这也就意味着，不符合“超大型”标准的平台或搜索引擎没有提供科研数据访问的义务。根据DSA立法理由第76条的规定，判断一个平台或搜索引擎是否属于“超大型”平台或搜索引擎的唯一标准是其

① 参见DSA第3条(i)项及DSA序言第13条。

② 例如，可能构成“显然不具有次要服务的特征”的情况是发帖者并非单纯地输出内容，而是存在与网络用户交流或讨论的主观意图或者客观情况。

③ 参见DSA序言第13条。

④ 参见DSA序言第14条。

⑤ DSA为网络服务提供者设置了“阶梯式”的监管模式，其中超大型平台或搜索引擎处于这种“阶梯式”监管模式的顶端，是重点监管对象。参见王天凡：《数字平台的“阶梯式”监管模式：以欧盟〈数字服务法〉为鉴》，载《欧洲研究》，2023年第2期，第50－77页，这里第55－56页。

活跃用户的数量，即如果平台或搜索引擎在过去六个月的月平均活跃用户总量超过4500万的门槛，即欧盟人口总数的10%，那么该平台或搜索引擎就属于“超大型”平台或搜索引擎。根据DSA第3条(p)和(q)项的规定，月活跃用户是指所有在相应月份内通过接触平台或搜索引擎界面上发布的内容，或者通过自己提供内容，至少与平台或搜索引擎进行过一次互动的用户。用户与平台或搜索引擎互动的形式多种多样，主要包括点击、上传、下载、评论、链接、分享、购买或在平台进行交易等。①

由于月活跃用户数量是判断平台或搜索引擎“超大型”与否的唯一标准，所以，在计算时尤其需要注意以下几点：②一是不能简单地以平台或搜索引擎的注册用户数量来替代月活跃用户数量，多数情况下，两者并不相同，甚至可能相差甚大。二是搜索引擎的活跃用户仅包括那些在其在线界面查看信息的用户，而不包括被索引网页的提供者，因为后者并没有与搜索引擎的提供者进行互动，被索引网页的提供者没有主动提供内容的行为。三是要避免重复计算活跃用户数量。一项服务的活跃用户的数量应该是指使用该特定服务的所有唯一的接收者数量。为此，使用不同在线界面(如网站或应用程序)的服务接收者，包括通过不同的统一资源定位器(URL)或域名访问服务的情况，应尽可能只计算一次。此外，平台或搜索引擎活跃用户还不应包含其他中介服务提供者的用户对平台或搜索引擎的附带使用，例如，第三方中介服务提供者通过自己的在线界面提供内容，而这些内容由网络平台提供者所托管或者由在线搜索引擎提供者编制索引就属于这种情况。③

由于活跃用户数量是判定超大型在线平台或搜索引擎的唯一指标，而且其具体计算具有一定的难度，因此DSA授权欧盟委员会在必要时通过授权法案(delegated acts)更新具体的用户数量标准或者规定确定平台或搜索引擎活跃用户数量的方法。④

三、数据访问活动本身须满足的要求

除了对权利和义务主体的主体资格提出要求，DSA立法者还要求数据访问活

① 参见DSA序言第77条。

② Vgl. Markus Rössel, „Digital Services Act: Regulierung von Big Tech Sezierung verabschiedeter Änderungen aus dem Trilog in drei Akten — Teil 3“, *IT-Rechtsberater* (*ITRB*), Heft 3, 2023, S. 68 - 75, hier S. 70.

③ 同注①。

④ 参见DSA序言第76和77条。

动本身应该在符合比例原则的要求下展开。[①] 根据DSA第40条第8款(e)和(f)项的规定，符合比例原则的科研人员的数据访问活动主要是指：第一，数据访问活动要符合DSA所明确规定的目的；第二，数据访问活动不得侵害超大型在线平台或搜索引擎服务提供者以及第三人的合法权益。

(一)符合DSA规定的目的

根据DSA第40条第8款(f)项的规定，需要进行数据访问的研究活动必须符合DSA第40条第4款中授予研究人员数据访问权所欲实现的目标，即“开展有助于检测、识别和理解第34条第1款规定的欧盟内部系统性风险的研究，以及根据第35条的规定评估风险缓解措施的充分性、效率和影响”。这也就意味着，不具有上述两个目的的科研活动是无法获得数据访问权的，即使这些科研活动具有其他合理目的且这些研究目的的实现也需要访问数据，也不能获得DSA第40条意义上的科研人员数据访问权。[②]

DSA第34条第1款对何为欧盟内部的系统性风险做出了明确规定。该款将以下四类情形定性为系统性风险：第一类风险是传播非法内容。DSA立法者对非法内容的含义进行了扩展，使其不仅包含狭义的非法信息，而且包含与非法内容、产品、服务和活动有关的信息，比如未经同意共享私密图片、在线跟踪、销售不合格或假冒商品、销售或提供违反消费者保护法的产品或服务、未经授权使用受版权保护的材料、非法销售活体动物等。[③] 第二类风险是在行使基本权利的过程中产生的任何实际或可预见的负面影响，尤其是《欧盟基本权利宪章》中规定的保护人的尊严、尊重私人和家庭生活、保护个人信息、维护言论和信息自由、不受歧视、尊重儿童权利以及消费者保护等权利。所谓可预见的系统性风险是指由于超大型平台或搜索引擎算法系统的设计或平台内规则的制定而可能造成上述基本权利被压制或被阻碍的情况。[④] 第三类风险涉及对民主进程、社会讨论或选举过程以及公共安全的实际或可预见的负面影响。第四类风险是与性别暴力、保护公众健康和未成年人有关的任何实际或可预见的负面影响，以及严重影响个人身心健康的负面影响。第三、四类风险可能是由对超大型平台或搜索引擎所提供服务的不真实使用或自动利用而产生的，比如创建虚假账户、利用机器

① DSA序言第97条指出：“所有在该框架下提出访问数据的请求都应当是成比例的。”

② Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, S. 831.

③ 参见DSA序言第12和80条以及第3条(h)项；Simon Gerdemann/Gerald Spindler, „Das Gesetz über digitale Dienste (Digital Services Act) (Teil 1)“, *Gewerblicher Rechtsschutz und Urheberrecht* (*GRUR*), Heft 1-2, 2023, S. 3 – 11, hier S. 4.

④ 参见DSA序言第81条。

人等欺骗性地使用服务以及对自动转发等功能的不当使用等。[①] 虽然DSA立法者区分了四种系统性风险，但多数情况下，这四种风险可能是相互交织而无法进行明确区分的，比如与新冠疫情有关的错误信息的传播就可能会同时触发以上四种系统性风险。[②]

由于上述四类系统性风险的发生与平台或搜索引擎的设计、运行或使用密不可分，因此为了减少这些系统性风险的发生及其所造成的危害，DSA立法者要求超大型平台或搜索引擎的提供者在尊重基本权利的前提下，采取合理、适度和有效的缓解措施，比如调整其服务或算法的设计、特性或功能，或者调整其内部审核系统或审核流程等，[③]以尽可能地减少系统性风险的发生或降低其所造成的影响。但超大型平台或搜索引擎提供者是否采取了风险缓解措施、其所采取的措施是否有效、是否需要完善以及如何完善等问题的解决离不开外部监督以及专业人员的参与，因此，DSA立法者将评估风险缓解措施的充分性、效率和影响也作为授予科研人员数据访问权的一种合法理由。

这里产生了一个问题，即一项研究计划是否必须同时以“检测、识别和理解系统性风险”及“评估风险缓解措施的充分性、效率和影响”为研究目的时才能获得数据访问权？通常而言，根据“发现问题—解决问题”的研究思路，一项研究计划不仅要提出问题，更重要的是要解决问题。按照这一逻辑，申请数据访问权的研究计划需要同时具备上述两个目的。但如果就此认为DSA第40条第8款(f)项中的目的正当性是要求研究计划必须同时具备第40条第4款中提到的两个目的，就可能会限制科研人员数据访问权的适用范围，而且也可能不符合实践需求。例如，随着人们对某类系统性风险认识的深入，研究的重点可能就转向如何缓解乃至消除这种风险，那么在这种情况下，一项以解决该类系统性风险为目标的研究计划就不需要再浪费时间、精力和经费去检测、识别和理解这种系统性风险，而是应该直接进入解决问题的阶段，评估平台或搜索引擎所采取的风险缓解措施的充分性、效率和影响。因此可以认为，一项研究计划只需要具备DSA第40条第4款所列目的中的任何一个，即可被视为满足了DSA第40条第8款(f)项所提出的目的正当性要求。[④]

(二)不得侵害义务主体和第三人的合法利益

根据DSA第40条第8款(e)项以及序言第97条的内容，数据访问活动要“适

① 参见DSA序言第83和84条。

② See European Commission, “European Commission Guidance on Strengthening the Code of Practice on Disinformation”, COM (2021) 262 final, p. 1.

③ 详细内容参见DSA第35条第1款。

④ 参见 Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, S. 832。

当保护超大型在线平台或搜索引擎以及任何其他有关各方（包括服务接受者）的权利和合法利益，包括保护个人数据、商业秘密和其他机密信息”。[①]

1. 保护超大型平台企业的机密信息

在DSA中，立法者使用了一个模糊的概念，即“机密信息”，并且同时将商业秘密置于机密信息的范畴之内。[②] 这表明欧盟立法者有意为超大型在线平台或搜索引擎提供者提供范围更广的保护，因为商业秘密只是机密信息的一种或者一个子集。[③] 有些信息虽然不符合商业秘密的构成要件，[④]但如果按照行业惯例或经营需要且应当对其保密的，则属于机密信息。特别是对于数据这种新型信息载体而言，[⑤]其是否以及在何种情况下构成商业秘密，在理论和实践中还存在诸多争议，而且数据具有一经泄露便无可挽回的特点，因此有必要对其提供更全面的保护。尽管如此，从DSA的措辞可以看出，对于超大型在线平台或搜索引擎而言，其机密信息的核心和重点依然是商业秘密。根据DSA第40条第5款(b)项的规定，如果准许对某些类型数据的访问导致机密信息（特别是商业秘密）的保护出现重大漏洞，那么超大型在线平台或搜索引擎提供者可以要求修改访问请求，甚至最终拒绝提供数据访问。因此，科研人员数据访问权下的数据访问活动不能侵害超大型在线平台或搜索引擎提供者的商业秘密。

对于商业秘密保护，欧盟制定了《商业秘密保护指令》。[⑥] 根据该指令第2条第1项的规定，一项或一类数据只有在同时满足秘密性、价值性和保密性三项要求时，才会被视为商业秘密并得到保护。[⑦] 同时，与知识产权保护不同，数据的商业秘密保护不要求数据具有创造性、原创性或新颖性。[⑧] 因此，原则上来说，任何一

---

① Spring Nature的一项调查显示，数据泄露的安全风险与数据利益损失的担忧是数据主体不愿意进行数据分享的两个主要原因。参见闫志开：《欧盟对数据中介服务提供者的规制模式及其镜鉴》，载《德国研究》，2023年第2期，第124－143页，这里第126－127页。

② 参见DSA序言第97条以及第40条第5款(b)项。

③ Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, S. 832－833.

④ 例如，商业秘密所保护的信息必须具有秘密性，即有关信息“不为所属领域的相关人员普遍知悉且不容易获得”。平台内容治理所涉及的信息通常是网络用户在网络上已经公开的信息，通常不满足现有商业秘密中秘密性要件的要求。参见张浩然：《数字时代商业秘密制度理论基础的再检视》，载《知识产权》，2023年第9期，第88－107页，这里第89页。

⑤ 关于信息和数据这两个概念之间的关系，可参见梅夏英：《信息和数据概念区分的法律意义》，载《比较法研究》，2020年第6期，第151－162页，这里第152－153页。

⑥ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, OJ L 157, 15. 6. 2016, p. 1.

⑦ 我国《反不正当竞争法》第9条也有相同的规定。

⑧ 参见陶乾：《商业秘密保护法的规范构造研究》，北京：法律出版社，2022年版，第66－68页。

项数据都可以被视为商业秘密,[①]因此超大型在线平台或搜索引擎可以主张的商业秘密保护的范围可能非常大,这在个案中可能会导致科研人员无法获得有效的数据,从而使科研项目质量下降,甚至研究目的完全落空。

为了解决这一问题,在对《商业秘密指令》进行转化立法时,德国立法者在结合《商业秘密指令》序言第14条的基础上认为,即使寻求商业秘密保护的信息满足了秘密性、价值性和保密性的要求,那么也只有在权利主体对信息的保护具有正当利益时,该信息才能获得商业秘密保护。[②] 但这一要求也应当受到严格限制,只有当根据个案的具体情况,权利主体主张商业秘密保护没有"明显、可信以及经济上可理解的理由"时,才可以认为不存在正当利益。[③] 因不存在正当利益而不得主张商业秘密保护的一种典型情况是保护客体本身不为法律所认可。[④] 这一要求对于数据访问权而言可能具有重要的实践意义。在当前经营者收集数据的实践当中,经常发生违反数据保护法律法规要求过度收集或秘密收集用户数据的情形,[⑤]而根据以上观点,对于以违法违规方式获取的数据,超大型在线平台或搜索引擎是没有正当利益的,因此不得对此主张商业秘密保护,进而也就不能对抗科研人员数据访问权。[⑥]

2. 保证超大型在线平台或搜索引擎服务的安全性

DSA对数据访问活动的第二个要求是,不得对超大型在线平台或搜索引擎所提供的服务构成重大安全漏洞,否则也可能会导致数据访问请求被拒绝。虽然DSA立法者并没有进一步规定何种情形构成对服务安全的重大漏洞,但从"重大漏洞"这一措辞中可以看出,对于数据访问活动所引发的不属于重大安全漏洞的安全性威胁,超大型在线平台或搜索引擎的提供者应该予以容忍。对安全性威胁的严重性的评价是一个利益衡量的过程,需要结合个案的具体情况、研究计划的具体情况以及研究人员及其所属研究机构对保障数据安全所采取的技术和组织措施等因素进行综合考虑。[⑦] 但无论如何,超大型在线平台或搜索引擎都不得提供违反

① BGH MMR 2006, 815 III. 1.

② 需要注意的是,欧盟《商业秘密保护指令》中并没有这一要求。参见 Christian Alexander, in Helmut Köhler/Joachim Bornkamm/Jörn Feddersen (Hrsg.), *Gesetz gegen den unlauteren Wettbewerb*, München: C. H. Beck, UWG, 40. Aufl., 2022, GeschGehG § 2 Rn. 74 ff。

③ Christian Alexander, in Helmut Köhler/Joachim Bornkamm/Jörn Feddersen (Hrsg.), UWG, 40. Aufl., 2022, GeschGehG § 2 Rn. 77.

④ Ronny Hauck, in MüKoLauterkeitsrecht, München: C. H. Beck, 3. Aufl., 2022, GeschGehG § 2 Rn. 67; Christian Alexander, in Helmut Köhler/Joachim Bornkamm/Jörn Feddersen (Hrsg.), UWG, 40. Aufl., 2022, GeschGehG § 2 Rn. 78.

⑤ 参见国家互联网信息办公室:《关于抖音等105款App违法违规收集使用个人信息情况的通报》,2021-05-20,http://www.cac.gov.cn/2021-05/20/c_1623091083320667.htm,访问日期:2023-09-02。

⑥ Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E", S. 833.

⑦ 参见DSA第40条第8款(d)项。

网络安全或数据安全法律法规的数据。[①]

需要强调的是，科研人员的数据访问对平台或搜索引擎服务安全性的威胁不可被夸大。首先，在申请科研人员数据访问权时，根据DSA第40条第8款(d)项的规定，研究人员要在申请中说明他们"有能力履行每项申请所对应的数据安全和保密规定以及对个人信息的保护，并在申请中描述了为实现此目的所采取的技术和组织措施"。据此可以认为，获得数据访问权的研究人员已经具备了一定保证数据访问安全性的能力并且采取了相应的技术和组织措施。其次，虽然科研人员获得了数据访问权，但数据访问权的实施离不开超大型在线平台或搜索引擎提供者的配合，因此，后者在提供数据访问时可以采取相应的措施，比如建立适当的数据访问应用程序接口(API)、设置不同的访问认证机制、经过渗透测试的安全功能等措施，以缓解甚至避免数据访问活动对服务安全性所产生的不利影响。[②] 此外，超大型在线平台或搜索引擎所采取的保护其服务安全性的措施还能够弥补科研人员或其所属科研机构在数据安全保护措施和保护能力上的不足，这反过来又会进一步降低数据访问活动对服务安全性所造成的负面影响。

3. 保护第三人利益

数据访问活动除了不得侵害超大型在线平台或搜索引擎提供者对商业秘密等机密信息和服务安全性的合理利益，还要兼顾第三人的合法权益，而这当中最重要的是作为平台或搜索引擎服务接受者的网络用户对个人信息保护的合理诉求。为了实现DSA第40条第4款中的立法目的，科研人员数据访问权下的数据活动可能需要访问并处理作为超大型在线平台或搜索引擎服务接受者的网络用户的个人数据，甚至是敏感个人数据。[③] 因此，数据访问活动必须符合欧盟《通用数据保护条例》(GDPR)中有关个人数据保护的规定。

首先需要注意的是，对于科研人员数据访问权框架下的数据处理活动，作为数据主体的网络用户可能会失去其同意权。因为，根据GDPR第6条第1款(f)项以及第9条第2款(g)(i)(j)项的规定，出于第三人合法利益和公共利益的需要处理个人数据和敏感个人数据可以在没有获得数据主体同意的情况下进行。虽然第三人利益的合法性和公共利益需要经过利益衡量才能确定，[④]但一般认为

① Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E", S. 834.

② 同上。

③ Vgl. Alexander Rossnagel, „Datenschutz in der Forschung", S. 158.

④ Vgl. Marion Albers/Raoul-Darius Veit, in Heinrich Amadeus Wolff/Stefan Brink/Antje v. Ungern-Sternberg (Hrsg.), *BeckOK Datenschutzrecht*, 46. Ed., 1. 8. 2023, DS-GVO Art. 6, Rn. 68; Sebastian Schultz, in Peter Gola/Dirk Heckmann (Hrsg.), *DS-GVO BDSG*, München: C. H. Beck, 3. Aufl., 2022, DS-GVO Art. 9, Rn. 61.

其包括所有值得特别保护的公众利益和社会利益，例如人格尊严、和平、自由和安全。[①] 就DSA第40条第4款的规定而言，以“检测、识别和理解系统性风险”和/或“评估风险缓解措施的充分性、效率和影响”为目标的科研人员数据访问权背后的科研人员的研究利益以及公众对自由、和平和可信的网络环境的利益应当被视为属于GDPR第6条第1款(f)项和第9条第2款(g)(i)(j)项规定中的“合法利益”或“重大社会公共利益”的范畴。[②] 因此，科研人员数据访问权框架下的数据访问和处理活动可以在不经过数据主体同意的情况下进行。

其次，根据GDPR第14条第5款(b)项的规定，当出于公共利益目的处理数据时，数据主体亦会失去其知情权。这也就意味着，对于在科研人员数据访问权框架下开展的数据处理活动，科研人员可以不再向数据主体提供诸如控制者身份、数据处理目的、数据主体的权利以及与数据处理有关的风险和责任等方面的信息。[③] 按照体系解释，虽然GDPR第14条第5款仅适用于从非数据主体处获取个人数据的情形，[④]但这恰恰是科研人员行使数据访问权的场景。根据DSA的设计，科研人员数据访问权的实现并不是科研人员直接从数据主体处获取数据，而是要求作为义务主体的超大型在线平台或搜索引擎提供相关数据。[⑤] 由此，作为控制者的科研人员得以免除自己的信息义务。

在数据主体失去同意权和知情权的情况下，对于保护数据主体在科研人员数据访问权框架下的合法利益而言，具有重要意义的可能就是GDPR第5条第1款(c)项和(f)项规定的数据最小化原则(data minimisation)和完整保密原则(integrity and confidentiality)。

数据最小化原则是指所处理的个人信息应当充足、相关并且要限于数据处理目的的最小必要范围〔GDPR第5条第1款(c)项〕。数据最小化原则要求数据处理活动所涉及的个人数据的范围要限制在与处理目的相适应的范围内，而不要求将数据处理限制到绝对最低的程度。[⑥] 根据GDPR第25条第2款的规定，对于科研人员数据访问权而言，数据最小化原则要求作为控制者的科研人员采取适当的技术性和组织性措施以确保在默认方式下仅处理对每个特定处理目的有必要的个人数据，这一义务涵盖所收集个人数据的数量、处理范围、存储期限和数据的可访

① Sebastian Schultz, in Peter Gola/Dirk Heckmann (Hrsg.), 3. Aufl., 2022, DS-GVO Art. 9 Rn. 37.

② Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, S. 835.

③ 关于控制者信息义务所涵盖的范围可参见GDPR第14条第1－4款。

④ Martin Eßer, in Martin Eßer/Philipp Kramer/Kai von Lewinski (Hrsg.), *Auernhammer DSGVO-BDSG Kommentar*, Köln: Carl Heymanns Verlag, 8. Aufl., 2023, Art. 14 DSGVO Rn. 42.

⑤ 具体内容参见下文第四部分“科研人员数据访问权的实施”。

⑥ Paul Voigt, in Jürgen Taeger/Detlv Gabel (Hrsg.), *DSGVO-BDSG-TTDSG*, München: dtv Verlag, 4. Aufl., 2022, Art. 5, DSGVO Rn. 27.

问性等多个方面。但需要指出的是，上述数据最小化原则中的“个人信息限于数据处理目的的最小必要范围”并不仅限于不处理便无法实现目的的情形，还包括不如此处理就无法及时实现目的、无法完全实现目的或需要付出极大成本才能达到目的的情形。[①] 因此，在个案中可能会出现科研人员为了实现研究目的要求所访问的数据在数量、类型以及时间上跨度非常大的情况，但这也并不意味着其违反了数据最小化原则。[②] 此外，GDPR 第 89 条第 1 款明确规定，在为了公共利益存档目的、科学或历史研究目的、统计目的进行数据处理时，如果可以通过不允许或不再允许对数据主体进行身份认证的进一步处理实现上述目标，则应当以此种方式进行数据处理。对于保护数据主体的合法利益而言，该款规定表明，保持身份不被识别是数据主体的重要利益，控制者应当采取合理的匿名化或假名化措施来保护数据主体的此种利益。[③]

完整保密原则要求控制者保护被访问网络用户个人数据的安全，不能发生非法处理、数据泄露、意外遗失或灭失毁损等情况〔GDPR 第 5 条第 1 款(f)项〕。这一结论当然也可以从 DSA 第 40 条第 8 款(d)项要求研究人员具有一定保证数据安全能力的规定中得出。从保护数据主体合法利益的角度而言，保护数据主体的个人信息安全不仅要求不能发生数据泄露问题，而且还要求控制者采取适当的技术性和组织性措施，如匿名化和数据最小化等，以有效的方式防止前述情况的发生或将其危害后果降到最低。

四、科研人员数据访问权的实施

根据欧盟立法者的设计，科研人员数据访问权是一项针对超大型在线平台或搜索引擎提供者的具有原权利性质的主观权利。[④] 研究人员数据访问权的这种法律性质可以从 DAS 序言第 97 条以及第 40 条第 4 款规定的措辞中体现出来。前者指出 DAS“提供了一个框架，强制要求隶属于(EU)2019/790 号指令第 2 条所指的研究组织的、经过审查的研究人员从超大型在线平台或搜索引擎获取数据(compelling access to data)”；后者则规定“在机构数字服务协调员提出合理请求

① Alexander Roßnagel, in Spiros Simitis/Gerrit Hornung/Indra Spiecker (Hrsg.), *Datenschutzrecht*, Baden-Baden: Nomos Verlag, 1. Aufl., 2019, Art. 5 DSGVO, Rn. 121.

② 参见 DSA 序言第 96 条；Laura Edelson/Inge Graef/Filippo Lancieri, “Access to Data and Algorithms: For an Effective DMA and DSA Implementation”, p. 56, https://cerre.eu/publications/access-to-data-andalgorithms-for-an-effective-dma-and-dsa-implementation/, 访问日期：2023－11－30。

③ Vgl. Holger Greve, in Martin Eßer/Philipp Kramer/Kai von Lewinski (Hrsg.), *Auernhammer DSGVO-BDSG Kommenta*r, Köln: Carl Heymanns Verlag, 8. Aufl. 2023, Art. 89, DSGVO, Rn. 9；并参见 GDPR 序言第 156 条。

④ Alexander Wehde, „Datenzugang über Art. 31 Abs. 2 DAS-E“, S. 828.

后，超大型在线平台或搜索引擎的提供者应当在请求中推定的合理期限内，向符合本条第8款要求的经审查的研究人员提供数据访问权”。

作为一种主观权利，权利人（经审查科研人员）可以向义务主体（超大型在线平台或搜索引擎的提供者）主张权利，即可以要求后者履行自己承担的提供数据访问的义务。然而，按照DSA第40条第4条的规定，科研人员数据访问权仅是一种间接请求权，即作为权利主体的“经审查科研人员”无法直接向作为义务主体的超大型在线平台或搜索引擎的提供者主张自己的权利，而必须借助于一个中介机构——机构所在地数字服务协调人（Digital Services Coordinator of Establishment）。根据DSA的设计，机构所在地数字服务协调人在科研人员数据访问权的实施过程中发挥着关键作用，它不仅负责“经审查研究人员”身份的审核，而且负责向义务主体，即超大型在线平台或搜索引擎的提供者发出数据访问的申请。

这里需要区分数字服务协调人（Digital Services Coordinator）与机构所在地数字服务协调人这两个角色。根据DSA第49条第1和2款，前者是欧盟各成员国中负责对互联网中介服务提供者进行监管以及执行DSA的政府机构；而后者则是指互联网中介服务提供者的总部所在地、其法人代表居住地或成立地所在成员国的数字服务协调人〔DSA第3条（n）项〕。就科研人员数据访问权而言，由于苹果、谷歌、脸书、微软等符合条件的超大型在线平台或搜索引擎公司的欧洲总部基本位于爱尔兰，因此通常情况下，爱尔兰的数字服务协调人是DSA第40条第4款中的机构所在地数字服务协调人，并在科研人员数据访问权的实施过程中发挥关键的中间作用。[①] 只有当科研人员数据访问权的权利主体和义务主体恰好位于同一个成员国时，才会发生数字服务协调人和机构所在地数字服务协调人重合的情况。

具体而言，科研人员数据访问权的实施按照如下步骤进行，详见图1。

第一步，研究人员提交需要进行数据访问的研究申请。这里需要指出的是，为了便于研究人员提交申请、提高审核效率并减轻机构所在地数字服务协调人的工作量，DSA第40条第9款规定，除了向机构所在地数字服务协调人直接提交申请，研究人员也可以向其所隶属研究机构所在地的数字服务协调人，即研究机构所在地成员国的数字服务协调人提交研究申请，后者根据DSA第40条的规定，对研究人员的主体身份、义务主体以及科研活动本身等内容进行初步审查，然后将审查结

① Vgl. Mathias Vermeulen, “Researcher Access to Platform Data: European Developments”, *Journal of Online Trust and Safety*, September 2022, pp. 1 – 8, here p. 4.

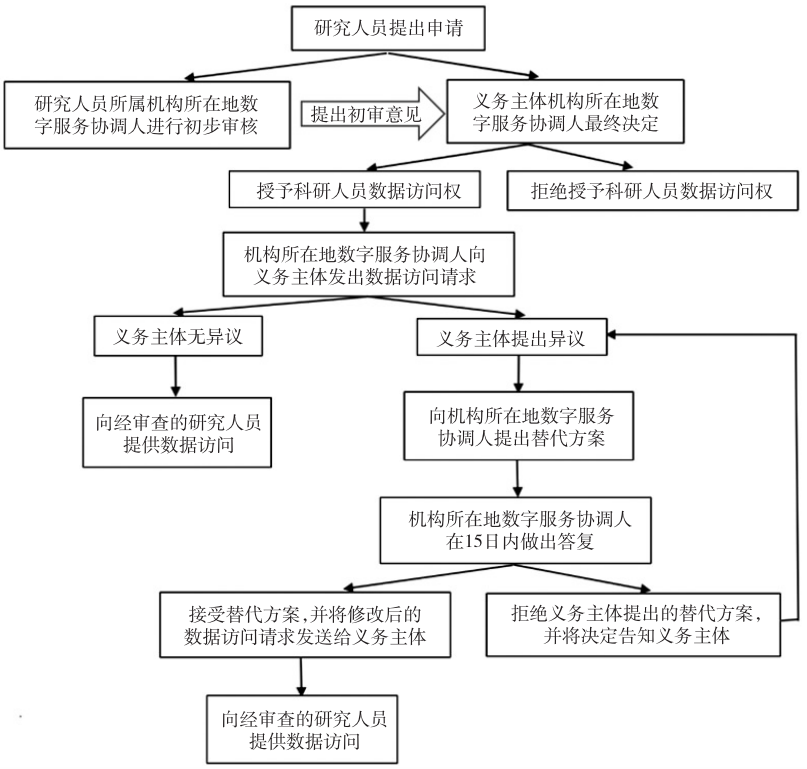

图 1　科研人员数据访问权的实施步骤

来源：作者自制。

论以及研究申请等相关材料发送给机构所在地数字服务协调人，由后者做出最终决定。由此可见，只有机构所在地数字服务协调人才有权力授予“经审查研究人员”的身份，而承担初审任务的数字服务协调人只有建议权。

第二步，根据研究人员提交的材料，机构所在地数字服务协调人依据 DSA 第 40 条的规定做出授予或拒绝申请人“经审查研究人员”身份的决定，即授予或拒绝授予其科研人员数据访问权。

第三步，如果机构所在地数字服务协调人决定授予申请人科研人员数据访问权，那便需要向超大型在线平台或搜索引擎服务提供者发出数据访问申请，要求其在合理期限内向前者提供数据访问。

第四步，超大型在线平台或搜索引擎服务提供者在接到机构所在地数字服务协调人发来的申请后对经审查研究人员的数据访问活动进行审查，如果其发现存在以下情况：(1)无法提供相应数据的访问或(2)提供数据访问会导致其服务的安全性或机密信息(尤其是商业秘密)保护出现重大漏洞(DSA 第 40 条第 5

款),那么它可以要求机构所在地数字服务协调人修改其提出的数据访问申请。根据DSA第40条第6款,如果超大型在线平台或搜索引擎提供者要求机构所在地数字服务协调人修改访问申请,那么其必须提出一个或多个替代方案,通过这些替代方案可以获取所申请的数据或其他对于研究目的而言适当或充分的数据。

第五步,如果超大型在线平台或搜索引擎服务的提供者提出了修改申请,那么机构所在地数字服务协调人需要在15天内做出接受或拒绝的决定。如果前者没有提出修改申请,则必须在申请规定的时间内通过适当的方式,比如通过在线数据库、编程接口或JSON文件等向相关研究人员提供数据访问权限。

五、对我国网络平台内容治理的启示

诚然,关于科研人员数据访问权还有很多问题需要澄清,比如,如何确定被访问数据的范围和类型?如何判断数据访问活动本身是否符合比例原则?如何协调科研人员数据访问权与个人数据保护之间的紧张关系?然而,这些问题都不能否认欧盟在网络平台内容治理中引入科研人员数据访问权的重要意义,欧盟的这一尝试对我国平台内容的治理具有启示意义。

(一)网络环境的变化与平台治理困境需要引入新监管工具

自最高人民法院于2000年底公布《关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》开始,从2006年《信息网络传播保护条例》再到2010年《侵权责任法》第36条,我国基本确立了以"红旗规则""避风港规则"为核心内容的互联网内容治理规则。[①] 这些规则和制度的适用空间是第一代互联网,即Web 1.0时代。然而,当前的网络环境与二十年前相比已经发生了很大变化,数字经济已经成为时代主题。人工智能、物联网、大数据、深度学习等第二代数字技术已经深深融入网络平台之中,互联网治理规则的适用空间已经发生了深刻改变。中央全面深化改革委员第二十六次会议指出,数据作为新型生产要素,是数字化、网络化、智能化的基础,已快速融入生产、分配、流通、消费和社会服务管理等各个环节,深刻改变着生产方式、生活方式和社会治理方式。[②] 数字经济的快速发展和平台企业的迅速转型带来了新的法律问题,既有规则的适用面临着新的障碍。与此同时,新商业模式的出现、市场结构的重塑以及平台现在发挥的突出作用也要求在这种新

① 《民法典》第1194—1197条是在原《侵权责任法》第36条规定的基础上经过大幅补充完善而形成的,并没有实质性改变后者所确立的基本规则。参见杨立新:《侵权责任法(第四版)》,北京:法律出版社,2021年版,第314页。

② 新华社,《习近平主持召开中央全面深化改革委员会第二十六次会议》,2022-06-22,https://www.gov.cn/xinwen/2022-06/22/content_5697155.htm,访问日期:2023-11-16。

背景之下重新考虑既有规则所提供的法律解决方案。[①]

第二代数字技术的发展和应用将网络平台的经营推向了一个新高度。算法、大数据和人工智能的发展和广泛应用大幅度提高了理解互联网技术及其运行机制的难度。如前文所述，网络平台会利用不同的技术手段或技术权限处理信息，以获得用户的优先浏览权，从而获取流量和经济利益。由此在网络平台的提供者和监管机构之间形成了一道知识鸿沟。因此，监管机构也应当与时俱进，及时根据技术的发展更新和扩充其监管工具箱，跟上网络平台采用新技术的速度和步伐，从而提高自身的监管能力和监管水平，避免出现监管漏洞。其中，打开黑箱对于识别风险和问题、检测结果以及防止潜在伤害具有重要意义。[②] 但监管机构凭自己的力量恐怕难以胜任，需要专业机构的协助，以便能够及时准确地发现问题并找出其根源之所在。从这个角度而言，在我国网络平台内容监管中引入科研人员数据访问权具有强烈的现实需要。

此外，科研人员数据访问权背后的中立第三方力量的引入还有利于打破当前网络平台内容治理在“委托治理”模式下所形成的治理僵局，纠正“监管机构—网络平台—网络用户”之间存在的明显的信息不对称问题。研究人员及其所属的研究机构作为主要的专业力量可以通过科学研究使社会公众、监管机构以及网络平台经营者自己认识、了解和理解网络平台的运行机制、技术的运行逻辑以及非法和有害内容的传播机理和规律，比如网络平台如何塑造公共话语、它们鼓励或阻止了哪些关系、它们放大或压制了哪些信息等，从而可以帮助公众、监管机构和网络平台发现平台内容治理过程中所出现的问题和僵局的症结之所在，提高网络平台内容治理的透明性。[③] 在这个基础之上，监管机构可以制定出更有针对性和更科学的监管规范，而网络平台则可以在设计平台架构和制定算法时提前采取措施，尽可能将网络风险的发生概率或其可能产生的危害降至最低。对于平台内容治理而言，网络平台上非法和有害言论的出现和传播有其自身的规律，只有在掌握了这些规律之后才能制定出行之有效的监管措施，[④]从而不仅提高网络平台内容治理的效率和效果，也有助于提高法律的确定性和可行性，消除监管机构和网络平台之间在

① Teresa Rodríguez de las Heras Ballell, “The Background of the Digital Services Act: Looking Towards a Platform Economy”, p. 80.

② 参见[德]托马斯·威施迈耶、蒂莫·拉德马赫：《人工智能与法律的对话》，韩旭至、李辉等译，上海：上海人民出版社，2020年版，第83页。

③ Alex Abdo/Ramya Krishnan/Stephanie Krent/Evan Welber Falcón/Andrew Keane Woods, “A Safe Harbor for Platform Research”, January 19, 2022, https://knightcolumbia.org/content/a-safe-harbor-for-platform-research, 访问日期：2023－11－15。

④ Lena Isabell Löber, „Der Forschungsdatenzugang nach den neuen Art. 40 DSA“, *Newsdienst ZD-Aktuell*, Heft 21, 2022, 01420.

当前“委托治理”模式之下的紧张关系。

(二)结合我国实际设计科研人员数据访问权的具体实施规则

DSA中关于科研人员数据访问权的实施规则是在结合欧盟数字经济客观现实基础的背景下制定的。欧盟在数字经济领域以及数字化进程方面落后于美国,而且在欧盟市场上活跃的大型网络平台均为非欧盟企业,因此,DSA对网络服务提供者的监管模式具有鲜明的“阶梯式”特点,即对来自欧盟之外的网络平台巨头企业规定了严格的义务,而对欧盟界定的“中小企业”(多为欧盟本土网络平台企业)则给予了多重豁免,欧盟希望由此实现制衡大型网络平台力量和促进欧盟内部创新及产业发展的双重目标。[①] 这一点与我国在数字服务领域面临的状况有一定的相似性。一方面,我国拥有具有国际影响力的大型网络平台企业,因此具有制衡平台力量的现实需要。另一方面,面对全球科技竞争,我国还需要鼓励和促进具有竞争力的平台企业继续发展,积极参与国际竞争,引领科技创新。因此,我国科研人员数据访问权的具体规则的构建要非常谨慎,需要在网络平台监管和保护之间保持微妙的平衡。为了实现监管和保护的双重目标,我国在设计具体规则时尤其要注意以下两点。

其一,从网络平台监管的角度而言,规则的设计要保证科研人员数据访问权得到真正执行。如果科研人员数据访问权沦为纸面上的权利,那么前述的提高平台内容治理监管水平、打破网络平台治理僵局等目标均无法实现。由于科研人员数据访问权是要打破网络平台治理的“黑箱”,提高网络平台“自治”过程的透明度,因此平台企业可能不会积极配合甚至顽强抵抗,从而导致科研人员数据访问权落空。因此,为了实现前述科研人员数据访问权的理论效果,可以参照DSA的做法,在科研人员数据访问权实施的过程中引入公权力监管机构的监督力量,由监管机构作为中介力量从中协调和推动科研人员数据访问权的实施。具体到我国的实际情况,国家网信部门作为网络平台的监管机构适合承担此项职责。另外,由于科研人员数据访问权涉及平台企业的数据和算法等,具有较高的专业性和技术性,从这个角度而言,新成立的国家数据局因其专业优势,可能也是一个合适的中介机构。

其二,从网络平台保护的角度而言,科研人员数据访问权的实施要注重保护平台企业的合法利益。在数字化时代,平台企业所收集的数据形成的数据集、所采用的算法等都可能构成其核心秘密,是其市场竞争力的依托,一旦泄露可能会造成重大损失,因此平台对这些内容的保密具有合理利益。即使是以公共利益为目的,科研人员数据访问权的实施也要兼顾平台企业在这方面的合法利益。

① 王天凡:《数字平台的“阶梯式监管模式”:以欧盟〈数字服务法〉为鉴》,第54-55页。

为了做到这一点，首先，要对执行数据访问和研究的科研人员在资质和水平方面提出较高的要求。研究机构必须具有一定的技术和组织条件，以保证所取得的数据和算法的安全性。科研人员必须保持中立性和独立性，防止科研人员数据访问权沦为窃取数据和商业机密的工具，同时这对于保证研究结果的客观性和真实性也具有重要意义。为了保证研究人员的中立性和独立性，除了在事前严格设置授予科研人员数据访问权的条件，还可以考虑在科研人员发生违规违法行为之后引入相应的惩罚措施，比如剥夺并禁止违规人员再次申请研究人员数据访问权、罚款乃至承担相应的赔偿责任。其次，数据访问活动本身需要严格遵守比例原则，将数据访问活动限制在必要范围内，尽可能地降低科研人员数据访问权对平台企业所造成的影响。这同时也是保护网络用户数据合法权益的必然要求。最后，为了更好地实现保护平台企业合法利益的目的，也应当赋予网络平台企业提出抗辩的权利。不过，为了避免平台企业的抗辩导致科研人员数据访问权的实施落空，可以考虑使上述为推动科研人员数据访问权实施而作为中介力量引入的监管机构在此种情况中发挥监督作用，避免平台企业滥用其抗辩权利阻碍公共利益的实现。

责任编辑：朱苗苗