

欧盟迈向数字宪制主义的 司法驱动逻辑

——基于欧盟法院案例的实证分析*

刘 业

摘 要：欧盟数据保护的规制理念正在向数字宪制主义不断发展。欧盟法院通过一系列司法裁决活动在这一进程中发挥着重要的驱动作用。从域内视角观察,欧盟法院通过将个人数据受保护权置于基本权利的保护逻辑之下,一方面在实践中强化个人数据受保护权这一新兴基本权利的法律地位,另一方面通过基本权利的横向适用,限制新兴数字私权力的无序扩张。从域外视角观察,因所审理数据保护案件的跨国性,欧盟法院已然扮演起“全球法院”的角色,通过扩张数据保护法律的域外管辖范围、强化对境外企业数据跨境流动的合规控制等路径,推动数字宪制主义规制理念向全球扩散。基于初步裁决这一设计良好的管辖制度,欧盟法院得以充分施展其司法能动性,并呈现愈加明显的政治倾向和意图,其影响力已不容小觑。

关键词：数字宪制主义； 欧盟法院； 司法能动； 基本权利； 数字私权力

作者简介：厦门大学 法学院 博士研究生 荷兰乌特勒支大学 联合培养博士研究生 厦门 361005

中图分类号：D99； D912.1； D814.1

文献标识码：A

文章编号：1005 - 4871(2024)01 - 0094 - 20

* 本文系 2023 年度国家社会科学基金青年项目“跨境数据流动风险防范法律规制研究”(批准号: 23CFX069)的阶段性研究成果,并受 2023 年国家留学基金委员会“国家建设高水平大学公派研究生资助项目”(项目编号:202306310128)资助。

随着欧盟内部市场一体化建设的深入推进，欧盟机构的职能已经扩展至税收、社会安全和教育等非市场领域，欧盟已然发展成为可以影响移民政策、刑事程序等政治敏感领域的全能型组织。^① 欧盟职能的全领域扩张和渗透，为欧盟法院(Court of Justice of European Union, CJEU)^②适用和解释法律开辟了广阔的司法能动空间。大数据、云计算、生成式人工智能等新兴技术迅速兴起、应用与迭代所引发的社会权力结构变迁、技术伦理失范等新的社会现象或风险，导致周期长、程序烦琐的立法活动难以及时应对，由此留下了大量法律模糊与真空地带。在“法无授权即禁止”的限权原则下，行政执法部门也难以及时展开精准有效的规制与执法。作为法律直面社会问题的第一线，司法以其及时性和灵活性的特点，通过创造性的司法解释对立法和执法起到重要的补充作用。欧盟法院的裁判意志凭依个案裁决中对各方利益的再平衡得以渗透和影响欧盟的立法与执法活动。《欧盟基本权利宪章》(Charter of Fundamental Rights of the European Union, 以下简称《宪章》)生效之后，以欧盟法院的司法判例为主要驱动，欧盟逐步迈向数字宪制主义(digital constitutionalism)^③。

欧盟法院的司法裁判活动在欧盟迈向数字宪制主义的过程中发挥着关键的驱动作用。欧盟法院在数据规制领域的重要作用也将随着其司法判例的不断做出而得到巩固和增强。有鉴于此，本文拟在欧盟迈向数字宪制主义的背景下，围绕欧盟法院的司法实践展开实证研究，分析欧盟法院驱动欧盟数字宪制主义的实践路径，揭示欧盟法院在欧盟数字宪制主义全球输出中所扮演的重要角色，并探究其背后的制度支撑以及政策考量。

一、欧盟数字宪制主义趋势与基本特征

(一)从数字自由主义到数字宪制主义

在互联网发展初期，欧盟主要遵循的是数字自由主义(digital liberalism)的监管理念。在2009年《宪章》生效之前，欧盟大体延续自《罗马条约》(Treaty of Rome)以来一直遵循的优先内部市场建设与经济发展的规制理念。以《网络空间

^① See Elise Muir/Mark Dawson/Bruno de Witte, “Introduction: The European Court of Justice as a Political Actor”, in Mark Dawson/Bruno De Witte/Elise Muir (eds.), *Judicial Activism at the European Court of Justice*, Cheltenham: Edward Elgar, 2013, pp. 1 - 10, here p. 2.

^② 为减轻欧盟法院日益积压的案件审理负担，《里斯本条约》生效后，欧盟法院内部分化为欧洲法院(Court of Justice)和一般法院(General Court)。鉴于本文所涉判例主要由欧洲法院所作，因此，除非特别说明，本文所称欧盟法院，主要指代欧洲法院。

^③ 关于 digital constitutionalism 的中文翻译存在其他多个版本，如“数字宪治主义”“数字宪政主义”，本文主要聚焦具体制度层面的探讨，不涉及更加全面与宏观的抽象理论构建，因此采取了更加贴合中文语境的“数字宪制主义”这一译法。

独立宣言》(A Declaration of the Independence of Cyberspace)为代表,^①人们最初认为新兴的网络空间有其独立的技术架构和运行逻辑,与传统的物理空间存在根本性的差异,国家权力触手不应涉及其中。但更不容忽视的背景是,最初的互联网企业只是扮演着数据存储者和转发服务提供者的消极角色,并不具备自动化处理数据和内容管控能力,数字私权力还未形成。因此,欧盟早期选择自由主义的市场规制理念治理网络空间,为境内企业提供相对自由的市场环境。^②

但随着数字技术的飞速迭代与数字经济的蓬勃发展,互联网企业的数字私权力开始形成并快速扩张,个人在“公权力—私权力—私权利”三元结构中逐渐被边缘化。一方面,传统的国家公权力在数字技术赋能下得到进一步增强。国家的权力触角借助各类数字终端设备可以渗透至非数字时代无法触达的微观社会领域,挤压个人权利和自由空间。在数字自动化处理技术赋能之下,国家机关对个人的控制权力得到了实质性扩张。另一方面,互联网企业数字私权力的出现和膨胀加剧了个人私权利的边缘化。互联网企业在数字技术赋能下逐渐从消极角色转变为积极角色,开始主动处理用户个人数据并管理用户生产的内容。拥有百千万级用户的互联网企业,在监视资本主义逻辑下持续、及时和全面收集并分析用户兴趣偏好与行为模式,推送迎合用户价值偏好的内容,影响和控制用户行为。^③互联网企业甚至可以通过信息推送影响和操纵民意,干扰一国正常的政治生态。在“公权力—私权力—私权利”这一新的社会权力结构中,个人私权利不仅面临来自国家公权力的威胁,更是不断受到互联网企业数字私权力的侵蚀。对个人私权利的保护亟待加强。

为避免个人在数字社会中沦为客体或工具,恢复三元权力结构的平衡,增强数字社会中个人的主体性地位,欧盟的规制理念逐渐迈向数字宪制主义。从二十世纪末到二十一世纪初的近三十年,欧盟将宪法基本权利引入其数字领域的立法与实践之中。立法层面,以1995年《数据保护指令》(Data Protection Directive)和2000年《电子商务指令》(Directive on Electronic Commerce)为数字自由主义之代表的早期立法,现已逐渐被体现数字宪制主义规制理念的2018年《通用数据保护条例》(General Data Protection Regulation,以下简称GDPR)和2022年《数字服务法》(Digital Service Act)等更高位阶的立法所替代;执法层面,从各成员国国内分

^① See John P. Barlow, "A Declaration of Independence of the Cyberspace," *Electronic Frontier Found*, February 8, 1996. <https://www.eff.org/cyberspace-independence>, 访问日期:2024-01-19。

^② See Giovanni De Gregorio, "The Rise of Digital Constitutionalism in the European Union", *International Journal of Constitutional Law*, Vol. 19, No. 1, 2021, pp. 41-70, here pp. 43-49.

^③ See Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization", *Journal of Information Technology*, Vol. 30, No. 1, 2015, pp. 75-89.

散、宽松且标准不一的低效执法状态转变为在欧盟数据保护委员会(European Data Protection Board)专门机构的统一指导下、各成员国专门性数据保护机构贯彻落实的“一站式”跨国执法网络；司法层面，以2009年《里斯本条约》(Lisbon Treaty)为分界线，欧盟法院不仅大量受理涉数据保护案件，^①更在逐渐发挥司法能动性，利用基本权利理论强化对个人数据的保护。

(二)数字宪制主义规制理念的核心特征

1. 视个人数据受保护权为基本权利

由于社会生活数字化程度的逐步加深，物理空间与网络空间之间相互影响日益密切，个人数据也将越来越成为物理空间中的个人在网络空间中“数字孪生”的直接载体。对个人数据的随意控制和利用，其后果不亚于对个人人格尊严的直接侵害。因此，数字宪制主义的首要主张便是将个人数据受保护权作为一项基本权利，用以捍卫个人在网络空间中的人权和主体性地位，避免个人沦为权力的工具。欧盟成员国在经过激烈的谈判和妥协之后，最终于2000年通过《宪章》，《宪章》第8条正式将个人数据受保护权作为一项独立于隐私权的基本权利确立下来。^②相较于一般性的民事权利，基本权利位于一国法律权利体系中的最高位阶，由宪法确立。基本权利旨在赋予个人对抗强大国家公权力以法律武器，任何对基本权利的减损行为均受到宪法上的严格限制和审查。换言之，基本权利的保障和救济存在一套特殊且严格的制度体系。

2. 主张基本权利可以横向拓展对抗数字私权力

以大型互联网平台企业为代表的数字私权力在其平台架构内拥有广泛的准国家公权力，如制定平台规则的立法权、通过技术手段封禁账号的执法权、仲裁用户交易纠纷的司法权，甚至还具有即使是国家公权力也难以具备的对个人行为 and 思想的控制权力。根据传统宪制理论的“公权力—私权利”二元结构，个人虽然可主张基本权利以对抗国家公权力，但对于数字私权力却无能为力。基于数字私权力日益膨胀所引发的权力结构失衡问题，数字宪制主义突破了传统宪制中仅关注纵向的国家与私人之间的不平等关系的局限，主张将其拓展至横向的具备准公权力的私主体与个人之间实际的不平等关系。^③换言之，数字宪制主义主张“公权力—

^① See Ondrej Pavelek/Drahomíra Zajičková, “Personal Data Protection in the Decision-Making of the CJEU before and after the Lisbon Treaty”, *TalTech Journal of European Studies*, Vol. 11, No. 2, 2021, pp. 167–188.

^② Gloria González Fuster, *The Emergence of Personal Data Protection as A Fundamental Right of the EU*, Cham: Springer, 2014, pp. 163–212.

^③ Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge: Cambridge University Press, 2022, pp. 3–4.

私权力—私权利”的三元结构,将已经具备准监管角色和准国家状态的数字私权力纳入宪法规制框架。^① GDPR 不仅在开篇直接明确其上位法依据来源于《宪章》,更采取公私主体统一治理的模式:不仅适用于政府等公权力机构,更可直接适用于数字平台企业等私权力主体。

3. 具有内生的全球扩张特性

与传统社会相比,数字社会的运行有其特殊性,除了存在上述的数字私权力,数字社会还因互联网的全球互联而具有跨国界性。以数据处理法律关系为例,数据控制者、数据处理行为、数据主体分散于不同国家的情形较为常见,尤其是大型互联网科技巨头,其业务范围往往也是遍及全球。由此,适用于数字社会的数字宪制主义必然具有全球扩张的内在特性。^② 仅仅将数字宪制主义限制适用在一国物理的主权疆界之内,无法真正保护流于物理疆界之外的个人数据及其个人权利。遵循数字宪制主义规制理念的国家或地区,在数据保护的立法、执法以及司法等环节必然存在域外管辖的实践或意图。以 GDPR 第3条为典型代表,欧盟数据保护法律呈现出明显的域外管辖特征。欧盟法院在审理涉外数据保护案件时,也尽可能发挥司法解释的能动性,扩张数据保护法律的域外管辖范围,将欧盟数据保护法律推向世界。

二、欧盟法院驱动数字宪制主义的内部强化

欧盟法院在推动欧盟本土数字宪制主义实现的过程中发挥着重要作用。借助大量具有权威和先例地位的司法判例,欧盟法院不仅强化了个人数据受保护权的基本权利地位,更将个人数据受保护权这一基本权利拓展适用于互联网平台企业这类数字私权力。以下将从欧盟法院对基本权利保护的三种方式展开具体分析。

(一)个人数据受保护权在基本权利体系中的优先性

在2009年《宪章》生效前,欧盟法院在司法判例中很少从基本权利视角出发保护个人数据。对比2006年的《美欧旅客姓名记录传输协议》无效案^③与2017年的《欧盟-加拿大旅客姓名记录(PNR)传输协议草案》咨询意见案(以下简称欧加

^① Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights*, Abingdon: Routledge, 2023, p. 87.

^② Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, pp. 296-311.

^③ European Parliament v. Council of the European Union; European Parliament v. Commission of the European Communities, Joined Cases C-317/04 and C-318/04.

PNR 协议咨询意见案)^①，可以明显发现欧盟法院转变了个人数据保护逻辑。《宪章》第 8 条为欧盟法院运用基本权利审理个人数据保护案件提供了宪法性依据，欧盟法院借此在判例中创造性地进行司法解释和适用，不断确认和巩固个人数据受保护权的基本权利属性，迅速将其从《宪章》中的纸面条款落实为每个欧盟机构或实体都不容忽视的实然权利。

《宪章》生效后，欧盟法院首先在基本权利冲突的协调上，倾向于认可个人数据受保护权相对于言论自由、商业经营自由等基本权利的优先性。2014 年的 Google Spain 案^②主要涉及数据主体与谷歌西班牙公司以及美国谷歌总部等数字私权力之间的数据被遗忘权纠纷，谷歌公司在该案中被施加了权衡基本权利的义务，这反映出基本权利的横向适用效力。^③ 欧盟法院从《宪章》第 7 条隐私权和第 8 条个人数据受保护权出发，论证数据主体享有《数据保护指令》规定的各项权利，包括不再使数据主体的个人数据因搜索姓名而被迫与其姓名相关联的权利（即被遗忘权）。当这类权利与其他利益（如搜索引擎运营商的经济利益、互联网用户访问信息的潜在利益等）发生冲突时，一般享有更重要的地位。同时，欧盟法院也认识到，任何规则或判断一旦走向极端便容易滑向谬误，因此，这种价值优位也不能作绝对化适用。欧盟法院在裁决中强调，这种优先性判断取决于涉案个人数据的性质、该数据对数据主体私人生活的敏感度，以及社会公众对该个人数据享有的利益，如当数据主体为公众人物时便不具有优先性。

欧盟法院对个人数据受保护权的严格保护，起初也遭到部分机构反对。2016 年欧盟法院在 Tele2 Sverige AB 案^④做出的裁决，就曾被欧盟的执法部门批评过度优先保护个人权利，而忽视了对包括安全在内的其他竞争性利益的保护。^⑤ 但经过随后一系列裁决的反复确认和加强，欧盟法院构筑了个人数据基本权利保护的防御堡垒，欧盟的数据保护机构也开始承接并在实践中贯彻欧盟法院的意志。

^① European Parliament, Opinion procedure 1/15, July 26 2017, <https://curia.europa.eu/juris/document/document.jsf?docid=193216&mode=req&pageIndex=2&dir=&occ=first&part=1&text=&doclang=EN&cid=6471067>, 访问日期:2024-01-19。

^② Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12.

^③ Eleni Frantziou, *The Horizontal Effect of Fundamental Rights in the European Union*, Oxford: Oxford University Press, 2019, pp. 110-111.

^④ Tele2 Sverige AB v. Post- Och Telestyrelsen; Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, Joined Cases C-203/15 and C-698/15.

^⑤ See Orla Lynskey, “Tele2 Sverige AB and Watson et al. : Continuity and Radical Change”, January 12, 2017, <https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/>, 访问日期:2024-01-19。

(二) 倾向从严保护个人数据的司法解释路径

立足于个人数据受保护权的基本权利地位之上,欧盟法院对数据保护法律会逐渐倾向严格解释,甚至超越其原本意涵。在2015年的Schrems I案^①中,欧盟法院遵循先例,以2009年生效的《宪章》基本权利条款溯及解释1995年的《数据保护指令》。一方面,欧盟法院进一步强化数据保护机构的独立性地位。《宪章》第8条第3款中对数据保护机构的独立性要求,是监督个人数据保护规则实践落地的有效保障。为履行法定职责,数据保护机构应具备案情调查的权力、有效干预的权力,以及进行法律诉讼的权力。^②即使欧盟委员会对涉及美国的数据跨境流动做出了充分性认定,也不能消除或减少《宪章》和《数据保护指令》赋予数据保护机构的监督执法权力。^③这与欧盟法院在Google Spain案中的解释一致。另一方面,欧盟法院将数据跨境流动规则中的“适当性”(adequate)要求上升为“实质等同”(substantially equivalent)要求。《数据保护指令》对第三国数据保护水平的“适当性”要求,旨在确保个人数据被转移至第三国时仍能获得高水平的保护。但欧盟法院认为,虽不能要求第三国的数据保护水平与欧盟完全一致,但必须这样理解“适当性”:要求第三国根据其国内法或国际承诺,确保自身对个人数据基本权利和自由的保护水平在事实上“实质等同”于欧盟。质言之,第三国的保护手段可以与欧盟不同,但这些手段所产生的效果必须在实践中证明可以达到实质等同于欧盟的程度。^④

对个人数据从严保护的过程,换言之,也是对数字私权力不断限制的过程。欧盟法院率先认识到互联网平台企业所拥有的数字私权力,并通过加重其责任以达到限权的目的。在2010年的Google France案^⑤中,欧盟法院还认为互联网服务提供者只是消极的数据存储者和传播服务提供者,并未形成所谓的数字私权力。该案的总检察长也认为谷歌的搜索结果是遵循客观标准的自动化算法的产物,即使谷歌在提供搜索结果方面具有经济利益,也并未在搜索结果的筛选中加入自身意志。^⑥然而,随着互联网平台企业的商业模式转变为通过分析用户数据提供精

^① Maximilian Schrems v. Data Protection Commissioner, Case C-362/14.

^② 同上, paras. 41 - 43.

^③ 同上, para. 53.

^④ 同上, paras. 73 - 74.

^⑤ Google France SARL, Google Inc. v. Louis Vuitton Malletier SA; Google France SARL v. Viaticum SA, Luteciel SARL; Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL. Joined Cases C-236/08 to C-238/08.

^⑥ Google France v. Louis Vuitton Malletier SA, Google France SARL v. Viaticum SA and Luteciel SARL, and Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and others, Opinion of Advocate General Poiares Maduro (Sept. 22, 2009), Cases C-236/08, C-237/08, and C-238/08, at 144.

准广告推送服务，欧盟法院开始认识和确认平台企业的数字私权力。以避风港规则为例，这一免责规则诞生于仅存在提供信息存储和传播媒介服务的互联网企业的 web 1.0 时代。由于当时互联网企业还不具备全面的内容审查能力，因此对于用户利用企业提供的互联网服务实施的内容侵权行为，企业只要事后及时发现并妥当处置，就不承担责任。如今互联网平台企业的角色已经发生重大变化，该规则也需要做出调整。^①

于是，在 2011 年的 eBay international 案^②中，欧盟法院认定提供优化、展示或推广销售等服务并不属于互联网服务提供者的中立性活动。这一裁决的积极意义是，欧盟法院首次在裁决中承认，数字自动化处理技术已经使互联网服务提供者从消极的数据存储、传输服务提供者转变为分析和管控数据内容的积极管理者。新近生效的《数字服务法》在一定程度上削弱了避风港规则中平台对第三方侵权行为的责任豁免。首先，如果平台对其所存储的第三方信息不是一种纯技术中立、自动且被动的控制，而是掺杂着平台主动意志的信息控制，那么平台应对第三方内容承担责任。其次，如果平台上第三方所提供的商品或服务，消费者有合理理由误认为其为平台自身提供或授权提供，那么平台应当对第三方所造成的损害承担相应责任。

（三）以比例原则审查基本权利限制措施的合法性

《宪章》第 52 条第 1 款规定，任何对基本权利的限制措施都必须经受比例原则的审查。欧盟法院在裁决中充分利用了这一规则。

欧盟法院在 2014 年 Digital Rights Ireland 案^③中裁决欧盟《数据留存指令》(Data Retention Directive)不符合比例原则，由此认定其无效。欧盟法院认为，《数据留存指令》虽然可以通过比例原则的适当性测试，但无法通过必要性测试。理由在于：其一，《数据留存指令》第 3 条和第 5 条第 1 款没有对监控对象的范围做出任何限制，存在无差别监控任何人和任何通讯工具的风险；^④其二，《数据留存指令》第 1 条第 1 款仅说明了监控的目的是应对“严重犯罪”，但何为严重犯罪则交由成员国具体解释，并未严格限定监控目的，由此导致情报部门可以不受限制地获取通

^① 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 54 页。

^② L'Oréal SA and Others v. eBay International AG and Others, Case C. 324/09, para. 124.

^③ Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General; Digital Rights Ireland Ltd v. Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, Joined Cases C-293/12 and C-594/12.

^④ Digital Rights Ireland, paras. 56-57.

讯服务商数据,且该行为无法受到独立的有权机关的监督;^①其三,《数据留存指令》第6条笼统地规定监控的期限,没有根据数据的不同类别适用不同的保存期限,也未表明监控期限的确定是否基于客观中立的标准;^②其四,《数据留存指令》第7条没有对通讯服务商留存的数据提供充分的安全保障,没有从数据规模大小、数据敏感程度,以及数据被非法获取的风险等角度制定具体规则,没有确保数据销毁后的不可逆,等等。^③

紧接着,欧盟法院在 Schrems I 案中进一步强调对基本权利之干涉必须受到严格限制。由于欧盟委员会的充分性决定中并无相关的限制性规则,这也成为美欧数据跨境流动的安全港框架被废止的重要原因。^④又如,在欧加 PNR 协议咨询意见案中,针对加拿大政府部门收集和处理欧盟旅客个人数据的行为,欧盟法院从协议草案是否构成对《宪章》第7条和第8条基本权利的干涉,以及此种干涉是否是适当的和必要的等步骤展开合比例性审查。^⑤欧盟法院最终出具咨询意见,要求按照比例原则对协议草案进行一系列整改。这反映出欧盟法院严格审查平衡国家安全与基本权利的措施,以及对数据保护标准的高度要求。^⑥

欧盟法院在限制互联网平台企业对数据实施全面监控时亦践行比例原则。以 Scarlet 案^⑦为例,Scarlet 公司主要提供互联网接入服务,由于其用户未经授权下载和传播受版权保护的数字作品,版权管理公司 SABAM 据此请求 Scarlet 公司安装信息过滤系统,以阻止其用户的侵权行为。欧盟法院认为,通过法院命令的方式强迫 Scarlet 公司安装信息过滤系统会导致该公司不得不积极监控平台内所有用户的数据传输,而这正是《电子商务指令》第15条第1款所禁止的。欧盟法院进一步解释道,这种禁止主要源于对个人数据受保护权、商业经营自由以及信息传播自由等基本权利的保护。^⑧尽管对知识产权的保护也是《宪章》第17条第2款明确规定的一项基本权利,但为保护知识产权而要求互联网服务提供者全面监控用户数据,会过度减损其他基本权利,有违比例原则。^⑨欧盟法院严格限制平台企业的全面

① Digital Rights Ireland, paras. 60 - 61.

② 同上, paras. 63 - 64.

③ 同上, paras. 66 - 68.

④ Maximillian Schrems v. Data Protection Commissioner, Case C-362/14, paras. 88 - 92.

⑤ European Parliament, Opinion Procedure 1/15, paras. 137 - 139.

⑥ Monika Zalnieriute, "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement", *Modern Law Review*, Vol. 81, No. 6, 2018, pp. 1046 - 1063.

⑦ Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10.

⑧ 同上, paras. 53 - 54.

⑨ 同上, para. 36.

监控行为，意在防止数字私权力的无序扩张。随后欧盟法院在 Netlog 案中进一步重申了该意见。^①

三、欧盟法院驱动数字宪制主义的域外扩散

以《宪章》第 7 条和第 8 条作为全球扩张的法律基础和价值核心，^②欧盟法院主要通过扩大欧盟法律的适用范围和增强对海外企业的数据跨境流动合规控制，做出具有全球影响力的裁决，将数字宪制主义扩张至全球。

（一）扩大欧盟数据保护法律的域外管辖范围

扩大欧盟法律的域外管辖范围这一方式，可称之为“领土延伸模式”（Territorial Extension Model）。所谓领土延伸模式，主要指通过对外扩张境内法律的管辖范围，将落入管辖范围的境外实体拟制于境内，从而使其直接、全面地受控于境内法律秩序。以《数据保护指令》第 4 条第 1 款 c 项为例，其规定，若境外数据控制者为处理个人数据而利用欧盟境内的数据处理设备，则该行为受指令管辖。基于此项规则，当境外数据控制者的数据处理行为落入《数据保护指令》调整范围时，从法律效果上看，境外数据控制者必须将自身视为欧盟的本土合规者，严格遵守《数据保护指令》对数据处理行为的各项规则，理论上也存在承受境内数据保护机构直接执法的可能。

欧盟法院分别通过 Google Spain 案和 Weltimmo 案的裁决，进一步扩大了《数据保护指令》的域外管辖范围，并增强了域外管辖的针对性以精准识别和控制境外实体的数据处理行为。下文分述之。

其一，欧盟法院通过 Google Spain 案中的扩张性司法解释，将“境外数据处理行为”纳入《数据保护指令》第 4 条第 1 款 a 项的适用范围。该项规定，若数据控制者的数据处理行为发生在其位于欧盟境内的实体经营活动场景中，则应当适用《数据保护指令》。谷歌西班牙是总部位于美国的谷歌公司在西班牙设立的一个经营场所，但谷歌西班牙实际上并未参与数据搜索这一数据处理行为，数据搜索行为实际上由美国的谷歌总部实施。那么在谷歌西班牙完全没有参与境外数据搜索行为的情况下，如何对境外的数据处理行为主张管辖权？欧盟法院为将这一案件纳入其管辖范围，通过扩张性司法解释，认为谷歌西班牙推广和出售线上广告位的业务活动，与谷歌总部提供的搜索引擎服务存在密不可分的业务联系。前者是后者盈

^① Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, Case C-360/10, para. 51.

^② See Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism*, Oxford: Hart Publishing, 2021, p. 162.

利变现的重要方式,而后者是前者商业盈利模式得以实现的重要技术支撑。^① 据此,欧盟法院认定,数据搜索这一数据处理行为应包括在谷歌西班牙这一经营实体开展业务活动的场景之中,即便这一搜索行为不是欧盟境内的分支机构所为。^② 通过将境外数据处理行为纳入欧盟法律管辖范围,欧盟法院实际上也间接将其裁决效力辐射至美国总部。可能受欧盟法院裁决的影响,GDPR第3条第1款相比《数据保护指令》新增了“无论数据处理行为是否发生于欧盟”这一解除管辖地域限制的条文,以立法形式将欧盟法院的裁决意志上升为法律。

需要澄清的是,在本案被遗忘权的实际执行阶段所衍生的 Google LLC 案^③ 中,欧盟法院将被遗忘权的执行范围限制在欧盟境内,未要求谷歌在全球范围内删除链接,但这并不意味着欧盟法院不愿对外扩张,而是考虑到在全球范围内执行被遗忘权可能导致国际社会误认为欧盟存在文化霸权下对他国的法律殖民威胁,所采取的一种战略性回退策略。^④ 因为随后,欧盟法院明确该案裁决仅具有个案效力,对其他类似案例不具有广泛约束力,否决了该意见成为先例的可能性。欧盟法院强调,欧盟并未禁止其法律在全球范围内适用,各成员国监管机构或司法机关仍有权在对相关基本权利进行适当权衡之后,命令搜索引擎运营商在全球所有版本上解除链接。^⑤

其二,欧盟法院通过 Weltimmo 案中的扩张性司法解释,增强了《数据保护指令》域外管辖的针对性。Weltimmo 公司是一家位于斯洛伐克、提供线上财产交易服务的互联网企业,该公司的服务市场扩及匈牙利,由此也会收集匈牙利居民的个人身份信息和财产信息等个人数据。该案的主要争议点是匈牙利的数据保护机构是否有权对位于斯洛伐克的 Weltimmo 公司进行执法,换言之,匈牙利的数据保护法是否适用于 Weltimmo 公司的数据处理活动。本案同样涉及对《数据保护指令》第4条第1款 a 项的解释。欧盟法院在本案以及既往案例中一再强调,为了确保有效和全面保护个人数据基本权利,在解释该项“实体的活动范围”时不应进行限缩解释。^⑥

^① Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, para. 56.

^② 同上, para. 100.

^③ Google LLC, successor in law to Google Inc., v. Commission nationale de l'informatique et des libertés (CNIL), Case C-507/17.

^④ Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism*, p. 164.

^⑤ 同注^③, para. 72.

^⑥ Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14, para. 25; Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, para. 53.

因此,欧盟法院在认定位于斯洛伐克、提供网站服务的 Weltimmo 公司是否在匈牙利存在实体经营范围内真实有效的商业活动时,会从财产交易网站运营中财产位于匈牙利且网站使用匈牙利语言等方面,综合判断该网站主要或者完全针对匈牙利,由此认定 Weltimmo 公司在匈牙利存在真实有效的商业活动。^① 该裁决据此确立了欧盟数据保护法律关于域外管辖范围的针对性标准。虽然该案几乎被同时期更具影响力的 Schrems I 案所掩盖,但其深远影响不容小觑。^② GDPR 第 3 条第 2 款几乎完整体现了欧盟法院在该案中的裁决意志,该款规定,当数据控制者或处理者位于欧盟境外时,若其主观上以针对欧盟境内居民为特定目的而实施数据处理行为,则落入 GDPR 管辖范围。

(二)增强对海外企业数据跨境流动的合规控制

相比领土延伸模式要求境外实体直接适用欧盟本土的法律规则,欧盟法院通过增强对海外企业数据跨境流动的合规控制〔可称之为境外等效模式(Extraterritorial Equivalence Model)〕,寻求一种更为温和有效的法律全球扩张路径。境外等效模式仅要求境外实体采取实质等同于欧盟境内法律保护标准的合规措施,遵从结果导向,对境外实体采取何种合规措施概不过问。境外实体可在遵守本国法的基础上,针对欧盟法律保护标准中的各个维度,如公正有效的权利救济机制、政府信息获取的限制机制等,调整相应的合规措施,以达到实质等同的标准。欧盟《数据保护指令》第四章和 GDPR 第五章在数据跨境流动上便是采用境外等效模式的典型例证。具体而言,在《数据保护指令》的基础上,GDPR 形成了以充分性认定、适当保障措施(包括标准合同条款、可约束性公司规则等法律工具)和克减条款为核心的数据跨境流动法律框架,其中充分性认定和适当保障措施均以“境外等效”为实质要件。具言之,境外实体与欧盟开展数据跨境流动,只有其所在国家的数据保护水平具备实质等同于欧盟这一要件,或者采取的适当保障措施能够达到实质等同于欧盟的保护水平,才能符合欧盟法律的合规要求。欧盟法院充分利用数据跨境流动法律框架中的境外等效模式,成功塑造了如 2015 年 Schrems I 案和 2020 年 Schrems II 案^③,以及 2017 年欧加 PNR 协议咨询意见案等经典案例,间接推动了欧盟数字宪制主义的全球扩散。

“后 GDPR 时代,数据传输规则的解释与适用案件频出,欧洲法院通过司法审

^① Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14, para. 66.

^② Dan Jerker B. Svantesson, “The CJEU’s Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, yet so very Important”, *Maastricht Journal of European and Comparative Law*, Vol. 23, No. 2, 2016, pp. 332-341, here p. 337.

^③ Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems, Case C-311/18.

查机制,成为全球数据流动监管的‘新权威’。”^①以 Schrems II 案的后续发展为例,欧盟委员会与美国商务部等部门展开数据跨境流动的充分性认定谈判,并最终达成以隐私盾框架为核心的协议。通过该协议,美国承诺将对传输至美国的欧盟公民个人数据提供充分性保护。但该协议并非正式的国际条约,而是被内嵌至欧盟委员会做出充分性决定的事实依据之中,使得具有“国际性”的协议内化为“国内”行政决定的决策材料。由此,借助初步裁决程序,欧盟法院可通过对欧盟机构行政决定的审查,将司法意志嵌入数据跨境流动的国际博弈舞台之中。借审查欧盟内部法律文件效力之机,欧盟法院可利用数据跨境流动的境外等效模式实质审查第三国数据保护法律体系,将数字宪制主义的规制理念以合规为由强制推向第三国,在全球范围普及欧盟数据保护标准。

这方面的一个现实例证是,美国在限制情报监控权力的立法上,不断迎合欧盟法院的要求,进行了相当程度的法律修改。这种努力最终推动了欧盟委员会做出新的充分性决定,形成了新的跨大西洋数据流动法律框架。同理,在欧加 PNR 协议咨询意见案中,由于数据传输协议涉及欧盟个人数据的跨境传输,欧盟法院需要审查数据传输协议能否提供等同于欧盟的数据保护标准。在出具的咨询意见中,欧盟法院要求加拿大监管机构在将旅客姓名记录披露给第三国之时,需要确保第三国与欧盟存在与协议草案同等的协议,或者第三国通过了欧盟委员会的充分性认定。欧盟法院之所以能够实质干预国际协议的生成,亦是因为其以审查欧盟委员会的行政行为是否符合欧盟一级立法为切入点,借此影响他国立法。

四、欧盟法院发挥司法能动性的制度基础与政策逻辑

在迈向数字宪制主义过程中,欧盟法院通过强化对个人数据基本权利的保护和利用基本权利横向限制数字私权力,回应数字社会权力结构失衡问题。同时,网络的技术无界性促使欧盟法院将欧盟内部的数字宪制主义规制模式强制推广至其他国家。下文将尝试追问并解答,为何欧盟法院得以发挥如此重大的影响力,以及是否存在深层次的动机驱动欧盟法院的司法裁决。

(一) 欧盟法院裁决中的司法能动性

司法能动(judicial activism),有学者也将其称之为“司法创制”,^②即法院在法律适用中遇到法律规则漏洞或为实现特定的价值目的时,所进行的超出规则外延的扩张性司法解释或直接创设规则的司法活动。欧盟法院的司法能动对欧洲一体

^① 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89-109页,这里第101页。

^② 米健:《司法创制对欧洲一体化的推动》,载米健主编:《欧洲法在欧洲一体化进程中的作用》,北京:法律出版社,2009年版,第1-10页。

化进程起到了重要的推动作用。甚至可以说，“没有司法创制，就没有欧洲一体化，就没有欧盟的今天”。^① 例如，欧盟法院分别通过 Van Gend en Loos 案^②和 Costa 案^③推动塑造了欧盟新法律秩序的两大原则，即直接效力原则(Doctrine of Direct Effect)与最高效力原则(Doctrine of Supremacy)。前者使成员国法院以及案件的当事人可以直接援引欧盟条约，给个人创设权利或义务的条款；后者明确了当成员国法律与欧盟法律相冲突时，欧盟法律的效力高于成员国法律这一规则。依据两案的裁决，欧盟法院成功推动塑造了欧盟“新的法律秩序”，即欧盟法秩序相对于成员国国内法秩序的独立性和优位性。^④

欧盟法院推动数字宪制主义实践的主要方式是在个案裁决中充分发挥其司法能动性，于立法空白或自由裁量空间之处做出创造性司法解释，指引法律实践发展。在数据保护案件中，一方面，欧盟法院主动将《宪章》中的基本权利保护逻辑引入《数据保护指令》，朝增强数据保护方向能动性地解释《数据保护指令》中的各项数据保护规则，例如将“适当性”保护解释为“实质等同”保护，率先确认互联网平台企业的积极管理角色，并通过削弱避风港规则以应对平台企业日益增强的数字私权力等。另一方面，欧盟法院对欧盟数据保护法律的域外管辖持积极态度，持续发展其造法性功能。欧盟法院不仅推动数据保护法律的域外管辖范围进一步明确和扩大，更通过严控数据跨境流动合规迫使第三国企业甚至国家遵从欧盟的规制理念。“在欧盟法院的推动下，欧盟的价值、欧盟的标准和欧盟的规则在全球产生了相当的溢出效应。”^⑤

(二) 欧盟法院发挥司法能动性的制度基础

在数据保护相关司法实践中，欧盟法院主要依靠以咨询意见程序为主的事前控制渠道和以裁决无效程序、初步裁决程序为主的事后控制渠道发挥其司法能动性。^⑥

事前控制渠道主要是指咨询意见程序。根据《欧盟运行条约》(The Treaty on the Functioning of the European Union)第 218 条第 11 款，成员国、欧洲议会、欧盟理事会或欧盟委员会可就草拟中的协议是否符合两部条约的规定征求欧盟法院的

① 米健：《司法创制对欧洲一体化的推动》，第 9 页。

② Van Gend en Loos v Administratie der Belastingen, Case C-26/62.

③ Flaminio Costa v E. N. E. L., Case C-6/64.

④ 刘衡：《论重建欧洲国际法律秩序的司法进路——基于欧洲法院实践的考察》，载《国际观察》，2016 年第 1 期，第 121-134 页，这里第 124 页。

⑤ 蒋小红：《论欧盟法院在欧盟对外关系法中的作用》，载《国际法研究》，2023 年第 6 期，第 46-63 页，这里第 59 页。

⑥ See Theodore Christakis/Fabien Terpan, “EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options”, *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 81-106.

意见。若欧盟法院做出否定性意见,除非重新按意见拟定协议或对上位法条约进行修改,否则协议不得生效。在数据保护领域,最具有代表性的是上文提及的欧加PNR协议咨询意见案。法院认为所涉协议的部分条款不符合《宪章》的第7条、第8条和第52条的要求,导致协议通过受阻。欧洲议会对该程序的启动享有自由裁量权。因顾虑欧盟法院的咨询意见会阻碍协议的通过进程,欧洲议会主动启动该程序存在高度不确定性。例如,在欧盟与美国签订《保护伞协议》、分别与澳大利亚和美国签订PNR协议时,即便受到外界的反对,欧洲议会也并未启动该程序。

事后控制渠道主要包括裁决无效程序和初步裁决程序。裁决无效程序来源于《欧盟运行条约》第263条的规定,目的在于保障欧盟机构的次级立法(如条例、指令和决定等)与《欧盟条约》(The Treaty on European Union)、《欧盟运行条约》和《宪章》等上位立法的一致性。欧洲议会、欧盟理事会、欧盟委员会和成员国在启动该程序时无需证明自身与所涉立法存在任何特殊利益,但自然人或法人等启动程序则必须证明所涉立法侵犯其具体利益,由此导致该程序难以启动。初步裁决程序来源于《欧盟运行条约》第267条,旨在确保欧盟法律在所有成员国的解释和效力的一致性。成员国任何法院或法庭在审理案件中,若遇到涉及欧盟层面立法的有效性和解释问题时,可以请求欧盟法院就此法律问题出具裁决意见。

观察可知,欧盟法院做出的诸多具有里程碑意义的重要裁决均诞生于初步裁决程序,该程序也因此被视为欧盟法律的一项基石性制度。欧盟法律一体化中具有重要地位的直接效力原则、最高效力原则、默示权力原则(Doctrine of Implied Powers)、人权原则(Doctrine of Human Rights)等,均由欧盟法院通过初步裁决程序确立。^①在欧盟迈向数字宪制主义过程中,欧盟法院绝大部分具有重大影响力的裁决也主要是在初步裁决程序的框架下做出的(参见表1)。

初步裁决程序的制度优势如下:第一,启动初步裁决程序的门槛较低。初步裁决程序可以由成员国各个层级的法院或法庭发起,而非限制在成员国的最高司法机关。此外,在Vaassen案中,^②欧盟法院从功能主义视角对“法院或法庭”的概念进行扩张性司法解释,认为其并不局限于国家司法机关,还应包括实质行使司法功能、解决法律纠纷的国家认可的其他机构,如仲裁庭、行业工会等。欧盟法院倾向于对有资格发起初步裁决程序的主体进行扩大解释,以便拓宽自身的管辖范围。^③

^① See J. H. H. Weiler, “The Transformation of Europe”, *Yale Law Journal*, Vol. 100, 1991, pp. 2403 – 2483, here pp. 2413 – 2419; Laurence R. Helfer/Anne-Marie Slaughter, “Toward a Theory of Effective Supranational Adjudication”, *Yale Law Journal*, Vol. 107, No. 2, 1997, pp. 273 – 391, here pp. 291 – 292.

^② G. Vaassen-Göbbels (a widow) v. Management of the Beambtenfonds voor het Mijndbedrijf, Case C-61/65.

^③ 张华:《欧洲一体化与初步裁决制度的互动性剖析》,载《国际论坛》,2005年第1期,第69–73页,这里第69–70页。

表 1 数据保护领域欧盟法院管辖程序的案例总结

作用阶段	管辖程序	典型案例	案例编号
事前控制	咨询意见程序	2017 年欧加 PNR 协议咨询意见案	Opinion 1/15
事后控制	裁决无效程序	2006 年美欧 PNR 协议无效案	C-317/04 and C-318/04
		2010 年 Google France 案	C-293/12 and C-594/12
	初步裁决程序	2011 年 eBay international 案	C-314/12
		2011 年 Scarlet 案	C-362/14
		2011 年 Netlog 案	C-230/14
		2014 年 Google Spain 案	C-236/08 to C-238/08
		2014 年 Digital Rights Ireland 案	C-324/09
		2015 年 Schrems I 案	C-70/10
		2015 年 Weltimmo 案	C-360/10
		2019 年 Google LLC 案	C-311-18
2020 年 Schrems II 案	C-131/12		

来源：作者自制。

第二，初步裁决程序下欧盟法院与成员国法院地位相对独立。初步裁决程序可看作是欧盟法院与成员国法院之间的一种合作机制，在保持司法权相对独立的同时，探索彼此合作的互补方案，以保证欧盟法律统一实施于欧盟全境。^① 欧盟法院的初步裁决并不会取代成员国法院做出判决，仅针对成员国法院提出的欧盟法律适用问题出具裁决意见，此类问题一般构成成员国法院适用法律的前置性问题。这种法院之间彼此相互独立的制度设计，不仅充分尊重了成员国法院的司法独立性，而且也能纾解成员国法院与欧盟法院审理敏感议题的政治压力。一方面，成员国法院可以将涉及敏感议题的决断转移给欧盟法院，通过间接援引欧盟法院的裁决意见，避免直接做出裁决所招致的政治压力，减轻成员国法院审理案件的社会负担；另一方面，欧盟法院也能借成员国法院提出的初步裁决请求，得到施展自身影响的舞台，推进欧盟法统一适用于各成员国。

第三，裁决具有权威先例效力。虽然理论上欧盟法院做出的初步裁决仅在特定个案中产生一定的约束力，但基于对欧盟法院权威的信赖，其他成员国法院遇到相似案件时往往会遵循欧盟法院既往的初步裁决。欧盟法院在 CILFIT 案裁决中也曾鼓励成员国法院在类案中积极援引欧盟法院的既往裁决。^② 在审理新案件的过程中，欧盟法院亦不断援引先例，这既有力保障了其裁决的一致性和确定性，也能将遵循先例的理念潜移默化渗透至各成员国法院。欧盟司法、执法乃至立法都

^① 鲍禄：《构建动态、开放的基本法解释制度——欧盟法院初裁制度的启示》，载《山东社会科学》，2008 年第 10 期，第 10-14 页，这里第 12 页。

^② Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health, Case C-283/81.

已经在不同程度上受到欧盟法院初步裁决先例的影响,裁决的先例效力使初步裁决的影响力从具体个案最终扩散至整个欧盟法体系。

(三) 欧盟法院司法裁决中的政策逻辑

欧盟法院在司法裁决活动中存在政治考量。诚然,法院审理裁决案件是一项高技术性和专业性性的工作,法院也会以其特有的法律技术语言和客观中立的推理逻辑否认裁决中的政治意志。这种法律专业知识与逻辑为中立化的裁决提供了非政治性的正当性依据。^① 然而,裁决的政治意志恰巧就隐藏在裁决中的技术性法律语言之中。面对欧盟职能的不断扩大,欧盟法院审理的具有政治敏感性的案件也越来越多,这迫使法院不得不进行微妙的价值裁判和利益评估。^② 法院即便秉持中立客观的法律适用立场,也难以完全避免在自由裁量中潜在的政治倾向影响。

步入数字时代后,欧盟在全球数字经济格局中处于不利地位,扭转这一不利局势的目标主导着欧盟现阶段的政策选择。欧盟虽然在全球制造业中长期占据领先地位,但却没能踏上数字经济蓬勃发展的快车道,在数字产业领域落后于美国和中国。尽管欧盟成员国在数字基础设施建设和通信技术的社会普及方面付出了卓有成效的努力,但这无疑是替美国互联网科技巨头做了嫁衣,为其快速占领欧盟数字市场培育了优质的数字市场环境。欧盟在数字领域的弱势地位可从数字平台产业^③、云服务产业^④以及芯片半导体产业^⑤中欧盟企业所占比例中得到直观反映。

^① See Anne-Marie Burley/Walter Mattli, "Europe before the Court: A Political Theory of Legal Integration", *International Organization*, Vol. 47, No. 1, 1993, pp. 69 - 73.

^② See R. D. Kelemen, "The Court of Justice of the European Union in the Twenty-first Century", *Law and Contemporary Problems*, Vol. 79, No. 1, 2016, pp. 117 - 140, here p. 126.

^③ 根据联合国贸易与发展委员会《2021年数字经济报告》的统计数据,在数字平台市场份额的地理分布上,美洲独占67%,亚太地区占29%,而欧洲仅占3%。从各地区全球前100数字平台企业的数量占比来看,美洲占41%,亚太地区占45%,欧洲占12%。See UNCTAD, "Digital Economy Report 2021, Cross-border Data Flows and Development: For Whom the Data Flow", <https://unctad.org/publication/digital-economy-report-2021>, 访问日期:2024-01-19。

^④ 根据 Statista 网站公布的 2023 年第一季度全球云服务市场的统计数据,美国以亚马逊云(32%)、微软云(23%)、谷歌云(10%)和 IBM 云(3%)等企业超 68% 的份额处于绝对领先地位。中国以阿里云(4%)和腾讯云(2%)等超 6% 的份额分据一角。相比之下,欧盟并无大型云服务企业,市场份额占比过小,严重依赖美国等外国企业的云服务。See Felix Richter, "Big Three Dominate the Global Cloud Market", April 28, 2023, <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>, 访问日期:2024-01-19。

^⑤ 欧盟虽然在制造业等大型芯片制造上占有一定优势,但在作为数字产业基础的小型芯片的制造和供给上仍无法与美国抗衡。美国通过英特尔、超威和英伟达等芯片企业几乎垄断了全球芯片产业链的核心环节。截至 2021 年第四季度,英特尔占据全球 60% 的 CPU 市场份额,而 AMD 市场份额比例同样高达 39.3%。See Distribution of Intel and AMD x86 Computer Central Processing Units (CPUs) Worldwide from 2012 to 2022, Quarter, Statista, <https://www.statista.com/statistics/735904/worldwide-x86-intel-amd-market-share/>, 访问日期:2024-01-19。

欧盟在数字技术领域严重依赖外国,尤其是在数字平台企业方面,会造成欧盟本地居民的个人数据大量外流至美国等国家的大型数字平台企业,引发对个人隐私和自由的侵犯、产业技术发展受阻、国家安全受到威胁等风险。欧盟数字服务市场已经由外国公司所控制且不断强化,而数字技术发展需要以一定的用户和技术生态作为支撑,这导致欧盟难以通过常规手段发展数字技术、培育本土企业,^①只能选择树立高标准的规则壁垒,依靠其规范性力量针对性地打击和削弱外国数字科技巨头市场竞争力,为本土企业创造生存与发展空间。^②

欧盟法院在裁判案件过程中始终掺杂着实现这一政策目标的倾向。例如,在 Schrems II 案中,欧盟法院裁决《隐私盾决定》无效的主要理由是,美国限制政府情报监控权力的法律——《第 28 号总统政策指令》《外国情报监控法》《第 12333 号行政命令》——并未达到欧盟的限制标准。欧盟《宪章》第 52 条要求,任何授权干涉基本权力的法律文件本身必须明确界定授权监控行为的行使范围与必要限制,但美国的这三份法律文件均未满足该条要求。《宪章》限制标准的模糊性赋予了欧盟法院较大的自由裁量空间,其裁决难免会受到自身政策倾向的影响。欧盟法院裁决的公正性由此受到外界质疑,美国学者认为欧盟选择性执法,有针对性地打击美国互联网企业。^③即便是欧盟的学者,也表达过与美国学者相似的意见。^④ 欧盟法院之所以做出“有失公正”的裁决,可能意在回应欧盟在数据跨境流动领域严重的赤字问题,希望借此实现欧盟数据的本地化,培育和发展本地数字产业,捍卫欧盟的数字主权与技术主权。^⑤

借欧盟法院裁决之手做出政治决策往往能够发挥缓和利益冲突并推动政策实

① 余南平、冯峻锋:《新技术革命背景下的欧洲战略重塑——基于技术主权视角的分析》,载《欧洲研究》,2022年第5期,第1-28页,这里第6页。

② 金晶:《欧盟的规则,全球的标准?——数据跨境流动监管的“逐顶竞争”》,载《中外法学》,2023年第1期,第46-65页,这里第51页。

③ See Kenneth Propp/Peter Swire, “Geopolitical Implications of the European Court’s Schrems II Decision”, Lawfare Blog, <https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision>, 访问日期:2024-01-19; Kenneth Propp/Peter Swire, “After Schrems II: A Proposal to Meet the Individual Redress Challenge”, Lawfare Blog, <https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge>, 访问日期:2024-01-19。

④ See Theodore Christakis, “Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)”, European Law Blog, <https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/>, 访问日期:2024-01-19。

⑤ 刘业:《美欧数据跨境流动博弈中的欧盟技术主权战略及其实现》,载《国际法研究》,2023年第6期,第64-85页,这里第77-79页。

行的作用。^① 借助自身的司法权威和高度技术化的法律推理,法院可以巧妙斡旋和调停多方利益集团之间的冲突,提出倾向性的解决方案。例如,当预感其政治决策可能遭到激烈反对时,政府可能更加倾向于借法院的司法裁决做出此种政策决断。政策反对派出于对法院专业性和公正性的信赖,不会轻易公然质疑承载政治意志的法院裁决。法院由此作为缓冲机制以缓和不同利益团体间的冲突,从而利于政策的推行。当预料到做出的裁决结果可能招致外界质疑时,法院一般通过援引先例保证法律适用的一致性,增强论证逻辑以做出高质量裁决。在程序公正、论证缜密、说理充分的法院裁决面前,任何非法律性的质疑声浪均难以撼动法院的权威。质疑者只能选择在法律话语体系之内表达意见。例如,在美欧隐私盾框架事件中,欧盟法院的裁决直接导致美欧数据跨境流动隐私盾框架的废止,严重影响了美国对欧盟的数字经贸活动。作为法院裁决的最大反对方,美国虽然间接表达了对裁决的质疑和不满,但受制于司法权威和现实影响,主要还是在欧盟法律以及欧盟法院裁决框架内进行法律应对。例如,2020年,美国发布了关于标准合同条款和其他传输机制的《白皮书》;2022年,美国总统发布《加强美国情报活动监管的行政命令》;美国与欧盟谈判拟定新的传输框架,并最终在2023年促成欧盟委员会出台《关于欧盟-美国数据隐私框架的充分性决定》。

五、代结语:评价与回应

欧盟法院发挥其司法能动性,不仅推动了域内数字宪制主义实践,更源源不断地向全球释放其裁决的影响力。中国数字社会和数字经济也在快速形成和发展之中,与欧盟之间的数字联结日益加深。在欧盟法院的助推下,中国势必面临欧盟数字宪制主义的影响和冲击,因此应当理性辨识欧盟数字宪制主义司法实践的良莠成分,并做出适当回应。

欧盟法院驱动下的数字宪制主义存在内外有别的双重标准嫌疑。欧盟法院过度拔高数据跨境流动的合规标准,要求第三国政府或第三国企业提供实质等同于欧盟的保护水平,但实质等同所比较的对象并非欧盟实际的保护水平,而是立法所追求的理想水平。欧盟法院以此种理想的保护水平苛责第三国或第三国企业将其在实践中落地。虽然保护基本权利是欧盟法院对外如此行动的正当理由,但更重要的还是为了从外国强势的科技产业入侵中夺回本土产业的生存与发展空间,掌控技术主权。欧盟法院的双重标准,也并非仅表现在数据跨境流动领域。例如,在对直接效力原则的解释上,欧盟法院作为欧盟法的守护者,为避免外部规则随意进

^① See Michael Blauberger, "The Court of Justice in Times of Politicisation: 'Law as a Mask and Shield' Revisited", *Journal of European Public Policy*, Vol. 27, No. 3, 2020, pp. 382 - 399.

入欧盟法领地,对国际协定的直接效力认定和对欧盟措施的直接效力认定采取了双重标准。^①与欧盟相比,中国数字产业实力强劲。对此,中国应当为本土科技企业顺利走出国门营造与他国之间平等和开放的国际合作环境,而非盲目设置歧视性的高标准规则壁垒。

尽管如此,欧盟在增强个人数据的基本权利保护方面的努力仍值得肯定。无论科技如何进步,人类社会应当始终坚持将尊重人的尊严、维护人的主体性地位作为价值基准。这不仅是欧盟数字宪制主义意图实现和捍卫的价值,也是我国学者提出“数字人权”的初衷。^②随着数字产业经过一段时期的野蛮发展,中国可能会面临数字私权力过度膨胀所带来的社会权力结构严重失衡的问题,这促使中国亟须通过“数字人权”加强对个人权利的保护,捍卫数字社会中个人的主体性地位。作为“数字人权”在法律上的具体呈现,个人信息受保护权已通过专门的《个人信息保护法》这一宪法性法律予以落实和保障。“根据宪法,制定本法”作为连接《中华人民共和国宪法》与《个人信息保护法》的桥梁,意在为个人信息受保护权寻求宪法第33条第3款“国家尊重和保障人权”和第38条第1句“公民人格尊严不受侵犯”的条款依据,使个人信息受保护权获得基本权利的法律地位。^③中国尽管可以通过法律解释将个人信息受保护权定性为基本权利,但目前仍缺乏将基本权利适用于具体案件的司法实践。对个人信息的保护,往往也只借助传统的民事或行政途径,最终导致国家难以针对数字社会的特殊情势,给予个人私权利制衡国家公权力和数字私权力以有效的法律保障。对此,中国法院应当充分发挥司法能动性,在传统的民事或行政路径存在保护乏力或法律漏洞之时,积极运用基本权利的规制理论补强对个人私权利的保护,推动中国数字宪制实践的发展。

责任编辑:郑春荣

^① 蒋小红:《论欧盟法院在欧盟对外关系法中的作用》,第56-57页。

^② 代表性论述参见张文显:《新时代的人权法理》,载《人权》,2019年第3期,第12-27页;马长山:《智慧社会背景下的“第四代人权”及其保障》,载《中国法学》,2019年第5期,第5-24页;龚向和:《人的“数字属性”及其法律保障》,载《华东政法大学学报》,2021年第3期,第71-81页;高一飞:《数字时代的人权何以重要:论作为价值系统的数字人权》,载《现代法学》,2022年第3期,第150-165页;丁晓东:《论“数字人权”的新型权利特征》,载《法律科学(西北政法大学学报)》,2022年第6期,第52-66页;等等。

^③ 张翔:《个人信息权的宪法(学)证成——基于对区分保护论和支配权论的反思》,载《环球法律评论》,2022年第1期,第54-55页。