欧盟《一般数据保护条例》:演进、要点与疑义*

金　晶

内容提要:欧盟《一般数据保护条例》具有明显的功能主义的立法特征,体现了数据问题的复杂本质——保护法益的多样性。这包括数据主体对数据的支配权,数据控制者和处理者对数据的使用收益权,也涉及国家(地区)的数据主权。《一般数据保护条例》借助市场地原则和个人数据处理概念拓宽适用范围;遵循保护前置理念构建数据主体权利,将类型化的数据保护前置到数据收集、处理阶段,确立了数据可携权、删除权等非绝对性权利;引入了数据"归属"不排斥"利用"的跨境传输规则。该条例存在价值困境和技术困境,这是经济全球竞争格局下法律价值序列的平衡所提出的最大挑战。数据立法区域竞争的实质是数字经济的全球竞争,而法律价值序列处于变动平衡和重组之中,是立法者对市场竞争优势、经济长期发展和社会目标实现的不同选择和不同追求。数字技术引发的问题绝不限于是否立法,更在于采取何种价值序列、以何种方式立法,及如何与既有法律监管体系相协调。无论采取何种数据立法模式,技术路径绝非可取之策,机械分离数据主体和数据控制者,采取单一价值取向的个人数据保护法的立法模式,亦非数字时代的最佳选择。

关键词:《一般数据保护条例》　个人数据　市场地原则　数据可携权　删除权

一　问题的提出

在数字经济时代,数据的商业价值日益凸显。2015 年,欧盟委员会发布了《欧盟

* 本文为 2015 年国家社科基金青年项目"丝绸之路经济带合同法区域整合研究"(项目编号:15CFX058)以及中国政法大学 2018 年科研创新项目"《民法典合同编》数字合同的规则建构与理论难点"(项目编号:10818438)的阶段性成果。本文写作得到丁道勤、聂卫锋、史明洲、谢耿亮、车宁和匿名审稿人的诸多指导,特此致谢,文责自负。

单一数字市场战略》。2016 年,欧盟数字经济价值增至 3000 亿欧元,占欧盟 GDP 的 1.99%。据欧盟委员会估算,到 2020 年这一数字将增至 7390 亿欧元,占欧盟 GDP 的 4%。① 数字经济为价值创造和福祉促进提供了巨大契机,却对个人的权利和自由构成了实质性威胁。如何创制与飞速发展的数字技术相适应的法律,如何夯实个人数据保护并最大限度利用数据潜力促进社会发展,既是传统隐私理论下个人数据保护的价值追问,也是欧盟立法机关推行单一数字市场战略时亟须解决的重大问题。但是,数据保护并不是一项轻松的任务。数据保护的法益形态多样,散见于不同的法律层面,例如信息自决权、数据主权、对数据的财产权及处分权,尊重私人和家庭生活的权利,尊重住宅和通讯的权利、隐私权,以及作为绝对权的数据保护等。数据保护法也因法益多样性而呈现出多元的部门法维度:公共领域的数据保护法是行政法的一部分,规制私主体的个人数据处理是私法的一部分。数据保护法虽未直接规制消费者,但有明显的消费者保护功能,是消费者保护法;数据保护法既是信息法、媒体法和电信法的一部分,也是经济法的一部分,更是风险法,揭示了信息技术发展对个人自由和社会公平的风险所在。②

作为一部典型的数据保护法,《一般数据保护条例》③(General Data Protection Regulation ,以下简称"GDPR")诞生于欧盟数字单一市场形成的关键时刻,具有明显的功能主义的立法特征,也体现了数据问题的复杂本质——保护多样法益。这包括数据主体对数据的支配权,数据控制者、处理者对数据的使用权和收益权,也涉及国家的数据主权。GDPR 一体规制国家、企业和个人,构建的制度涉及多个相互交叉的法律部门,无论是 GDPR 的价值目标还是具体制度,均难以清晰归入传统法教义体系中,而是呈现出多层次、多维度、多类型的复杂面貌。作为最新的立法尝试,GDPR 虽然在相当程度上代表了欧盟数据保护的水平,但其能否以及如何实现数据保护的多重目标,仍有详细辨识、分析之必要。本文从 GDPR 的演进、要点和疑义出发,通过回溯 GDPR 的演进历史,厘清欧盟数据保护法的立法和司法政策嬗变,明确欧盟法律工具策略性

① 数据来源于欧盟官网,https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy, 2018 年 6 月 24 日访问。

② Martin Eßer, Philipp Kramer und Kai von Lewinski, *Auernhammer DSGVO BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze Kommentar*, Carl Heymanns Verlag, 2017, S.16-21.

③ Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016, pp.1-88.

更迭的根源;经由制度举要,阐明其与 1995 年《数据保护指令》(DPD)①的内部承继关系和制度创新的推进方向;分析现行制度的可能缺陷,考量不同数据保护立法模式的价值分野与实践困境。事实上,面对经济全球竞争驱动下的多元法律价值序列,GDPR仅是处理多样法益保护的方案之一,也仅是特定技术条件和时代场景下的一种立法尝试,起决定性作用的,仍然是法律背后的深刻的价值序列因素。真正的问题或许在于,GDPR 的立法模式是否科学,个人数据保护法还有没有未来?

二 《一般数据保护条例》演进史

(一)立法政策演化

早在 20 世纪 70 年代的全球数据立法尝试中,数据保护和数据自由的价值分野就已初露端倪:经济合作与发展组织欲打破数据国别保护的非关税贸易壁垒,促进跨境流动;欧共体则着力于自然人的基本权利保护和内部市场建构。这种价值分野从最初的立法尝试一直渗透到 GDPR 的制度血液中。唯有回溯历史,置身于欧盟数据立法的历史图景,方能理解 GDPR 的立法价值取向,也唯有回归"基本权利保护"和"内部市场统一"的社会、经济双重价值,方能认识 GDPR 内部体系的矛盾根源。

作为数据跨境自由的倡导者,20 世纪 70 年代,经合组织成立了"跨境数据障碍专家组",并于 1980 年以"建议"形式通过《经合组织隐私保护和个人数据跨境流动准则》(简称《经合组织准则》)。②《经合组织准则》并未着眼于数据保护,也不打算保护个人隐私,而是以确保成员国间个人数据跨境流动的安全性和持续性为首要目标,追求数据自由流动,将数据保护的国别性立法视为保护主义立法和非关税贸易壁垒。尽管倡导数据跨境自由,但《经合组织准则》的缺陷也十分明显:其一,"建议"虽具有灵活性,但规则的示范性质决定了准则并非国际法上有拘束力的法律文件,成员国并无执行准则的法定义务;其二,准则包含的广泛豁免限制了效力的发挥。因此,《经合组织准则》的法律效力极为有限,成员国的法律差异仍然存在。

---

① Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281, 23.11.1995, pp.31-50.

② 《经合组织准则》的目标包括:(1)实现对个人数据隐私保护的最低程度保护标准的认可;(2)减少成员国之间立法和实践的差异;(3)避免成员国之间不当干预个人数据流动;(4)尽量消除可能导致成员国跨境数据流动障碍的原因。参见 OECD,"Policy Issues in Data Protection and Privacy", OECD Informatics Studies, No. 10, OECD, 1974, pp.169-179; OECD, "Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data", 23.09.1980。

在欧洲数据保护发展过程中,没有一个国际组织像欧洲委员会(Council of Europe)这般发挥持久深远的影响。① 在欧洲委员会框架下制定的 1950 年《欧洲人权公约》包含了隐私权条款,欧洲人权法院通过广义解释使该条款亦能保护个人数据处理。② 欧洲委员会在 20 世纪 70 年代集中表达政治主张,将个人数据视为《欧洲人权公约》第 8 条第 1 款的一部分,要求部长委员会(Committee of Ministers)检视成员国法和《欧洲人权公约》,判断其是否并能在何种程度上保护个人免遭风险。③ 1973 年和 1974 年,部长委员会分别通过私营部门和公共部门数据保护的决议。④ 意识到"决议"的法律效力较低、不足以解决个人数据保护问题后,欧洲委员会于 1976 年成立专家组准备公约,并于 1981 年颁布《个人数据自动化处理中的个人保护公约》(《第 108 号公约》),自 1985 年 10 月 1 日起生效。⑤《第 108 号公约》是欧洲数据保护立法中的一项奠基性法案,将数据保护讨论中最为重要的通说性基本原则成文化,但公约本身属于非自动执行条约(non self-executing treaty),需成员国立法才能执行。在立法之前,公约本身对成员国司法管辖并无拘束力。同一时期,欧洲议会颁布了数据处理中个人权利保护的三项立法决议,⑥要求欧委会起草数据保护法律协调法案,回应欧洲数据处理行业的现实需求。但欧洲议会的立法尝试也未产生实质性成果,"决议"无直接效力,欧委会未起草草案,而是观望成员国是否批准《第 108 号公约》。1981 年,欧委会建议成员国于 1982 年年底前批准《第 108 号公约》,同时保留了未批准公约时欧委会的建议立法权,截至 1989 年,仅七个成员国批准了公约。⑦

至 20 世纪 80 年代末,欧洲诸机构以"建议"、"公约"和"决议"等形式展开的数据

① Spiros Simitis (Hrsg.), *Bundesdatenschutzgesetz*, Nomos, 2011, S.138.

② P. De Hert and S.Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", in S.Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt eds., *Reinventing Data Protection?* Springer 2009, p.3.

③ Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 04.11.1950; Council of Europe, Parliamentary Assembly Recommendation 509, Human Rights and Modern Scientific and Technological Developments, 31.01.1968.

④ Council of Europe, Committee of Ministers, Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sectors, 26.09.1973; Council of Europe, Committee of Ministers, Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 20.09.1974.

⑤ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, 28.01.1981.

⑥ European Parliament, Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing, OJ C60/48, 13.03.1975; European Parliament, Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing, OJ C100/27, 03.05.1976; European Parliament, Resolution on the Protection of the Rights of the Individual in Connection in the Face of Technical Developments in Data Processing, OJ C 140/34, 05.06.1979.

⑦ European Commission, Commission Recommendation of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, OJ L 246, 29.08.1981, p.31.

保护法律立法皆无疾而终,但毋庸置疑,上述立法尝试为国际上广泛认可数据保护夯实了前提基础。在担忧成员国数据保护法的分歧可能阻碍内部市场发展的情况下,1990 年欧委会发布一系列指令草案,其中包含《数据保护指令草案》,欧委会在解释性备忘录中明确指出:“成员国法律欠缺或不足之现状,无法体现共同体基本权利保护之承诺。”①《数据保护指令草案》吸取了《第 108 号公约》中一般规范无法实现预期效果的经验教训,延续了《经合组织准则》关于限制数据处理、数据开放性和数据安全保障的基本价值,引入了诸多精细化规则,并在历经五年谈判之后于 1995 年以“指令”形式通过欧洲数据保护法上具有里程碑意义的《数据保护指令》(DPD)。②

欧盟数据立法的政策演进表明,其数据立法动机源于基本权利保护,这是其区别于其他区域性数据立法的显著特征,也决定了欧盟对数据权利法律性质的特殊进路:在公私法二分的传统下,基本权利意义上个人对数据的控制权或自决权,与私法上个人对数据的支配权,两者分属不同维度,但互有交叉。欧盟的数据保护法是一种“主题式”的碎片化立法,并未恪守传统法教义学的部门法划分,而是采取了功能规制路径。例如,GDPR 序言第 4 条规定,对个人数据的权利保护并不是绝对,而应当与其他权利平衡。在个人数据保护的立法逻辑上,欧盟并未采取纯粹私法意义上的绝对权保护路径,而是在基本权利保护的维度上致力于基本权利的权衡,在私法维度建构不同类型的数据主体权利,这在欧洲法院的判例变迁中可见一斑。

(二)司法政策变迁:从“内部市场整合论”到“基本权利权衡论”

欧洲法院早期判例在解释《数据保护指令》(DPD)时持“内部市场整合论”,否认指令仅适用于具有跨境因素的数据处理者,申明要克服个人数据在内部市场的流动障碍,由此大幅扩大指令适用范围。③ 但在后续判例中,欧洲法院转而采取“基本权利权衡论”,试图平衡协调不同基本权利的保护要求。例如,法院试图协调隐私权和财产权保护的关系;试图平衡知识产权保护和数据保护、经营自由的关系;试图回应个人数据保护和信息接收自由、传递自由的关系。④ 欧洲法院对指令的解释路径虽不连贯,

① Proposal for a Council Directive concerning the Protection of Individuals in Relation to the Processing of Personal Data [1990] OJ C 277, 05.11.1990; European Commission, Communication to the Council on a Community Data-processing Policy SEC (73) 4300 final, 15.

② 在成员国层面,德国黑森州于 1970 年颁布了首部《数据保护法》。1973 年,瑞典颁布首部国家数据保护立法,德国和法国分别于 1977 年和 1978 年颁布数据保护国家立法。

③ 代表性判例包括 Rundfunk 案和 Lindqvist 案。参见 C-139/01, Österreichischer Rundfunk and Others, 20.05.2003; C-101/01, Bodil Lindqvist, 06.11.2003。

④ 代表性判例包括 Promusicae 案、Scarlet 案和 Bonnier 案。参见 C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, 29.01.2008; C-70/10, Scarlet Extended SA v. Societe Belge des auteurs, compositeurs et dditeurs SCRL (SABAM), 24.11.2011; C-461/10, Bonnier Audio Ab et al. v. Perfect Communication Sweden, 19.04.2012。

但对基本权利的立场始终恒定——法院始终不愿直接支持指令的基本权利目标,认为内部市场统一是指令的首要目标,基本权利保护位居其次,直接支持基本权利目标或将危及内部市场统一的"更高"目标。① 欧洲法院之所以对指令目标如此排序,是因为当时基本权利保护在欧盟法律体系中的法律地位:指令颁布时,《欧盟基本权利宪章》尚无约束力,欧盟无权进行基本权利立法,因此,欧盟法尚未确立"数据保护权"的明确依据,DPD 的法律基础是《欧盟运行条约》第 114 条的法律协调,并未涉及基本权利保护。②

但在欧盟基础性立法明确纳入"数据保护"后,欧洲法院的立场出现了根本转折。《欧盟基本权利宪章》获得了基础性法源地位,并于第 8 条明文规定个人数据保护,《欧盟运行条约》第 16 条为数据保护立法确立了独立的法律基础。③ 由此,欧洲法院开始在判例中逐步夯实促进数据保护的基本权利目标,在具有转折意义的 Eifert 判例中,法院首次判定派生性法律因违反《欧盟基本权利宪章》所保障的数据保护和隐私权而无效,认为个人数据保护的减损和限制必须且仅能在严格必要情形之下做出。④ 至此,数据保护的基本权利目标重回欧洲法院视野。在后续判例中,法院愈发重视欧盟数据立法的基本权利维度,在信息自由权、言论自由等个人数据保护问题上的立场一致。⑤

欧洲法院是一支极易被忽视的重要力量。它不仅在欧盟数据立法演进中发挥了独特作用,甚至在一定程度上形塑了欧洲数据保护法的理论内核。此种司法能动性的根源在于,欧盟数据保护法使用了大量一般性的法律概念。此类概念为司法裁判、司法政策预留了充分裁量空间,也因其本身的概念灵活性能够合理回应时刻变革发展中的数据技术。自 1970 年以来,欧洲法院通过 70 多例判决彰显了其在解释、调整甚至建构欧洲数据保护法上的中流砥柱的作用。欧洲法院从"内部市场整合论"到"基本权利权衡论"的判例变迁过程也表明,欧盟的数据保护政策是一种经济社会目标兼具的混合政策,其本身无法回避内部价值孰轻孰重的选择和评价难题。无论 DPD 还是 GDPR 均需直面"内部市场"和"基本权利"的价值选择和评价问题,而且由于立法价

① Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law, Oxford University Press, 2015, pp.87-88.

② Ibid..

③ 《欧盟基本权利宪章》第 8 条规定,人人有权享有个人数据保护,有权获得个人数据并予以纠正,个人数据须为特定目的且在数据当事人同意或其他法律规定的正当依据之下公平处理。此外,个人数据处理中的自然人保护也是《欧洲人权公约》和《个人数据自动化处理中的个人保护公约》等相关国际法律文件确保的一项基本权利,例如《欧洲人权公约》第 8 条规定了尊重私人和家庭生活的权利。

④ C-92/09, Volker und Markus Schecke and Eifert, 09.11.2010.

⑤ C-28/08, Commission v Bavarian Lager, 29.06.2010; C-131/12, Google Spain, 13.05.2014.

值的内部关系较欧洲数据保护法最初形成之时更趋复杂,未来甚至可能引发监管困境。① 不仅如此,欧盟数据保护法最初的重点是基本权利保护和消费者保护,而非商业交换问题。但自 2015 年以来,数据的价值衡量进入了新的层面,私人数据法的功能需要通过法律规范来实现和平衡不同目的、不同价值。这不仅符合利益法学的分析路径,②为欧洲法院的判例发展提供了新的方向,也对欧盟数据保护立法提出了新的要求。

(三)立法形式策略性更迭:从"碎片化"到"一体化"规制

欧盟数据保护的立法形式经历了从"建议"、"公约"、"决议",再到"指令"、"条例"的策略性更迭,呈现出法律效力从弱到强、法律规则从一般到特殊再到抽象、立法体系从碎片化到一体化的渐进特征。

作为派生性立法的一般规则,DPD 旨在协调成员国个人数据保护水平,克服不同层级数据保护法导致的跨境数据传输障碍,在欧共体内保护基本权利和基本自由。欧共体在 20 世纪 90 年代初以"指令"形式立法并无不妥。因为当时并无欧盟范围内的统一法令,指令可谓对成员国数据保护立法的初步协调,其最低限度协调的立法技术有助于在欧盟层面确立最低标准,由此实现成员国数据保护法的平等保护水平。当然,指令的最低限度协调技术会引发成员国碎片化立法的负效应,成员国基于指令建立的个人数据保护制度各有不同,指令中的"利益平衡条款"的解释也取决于各国数据保护本身的价值取向,法律和实务之间的巨大差距很难形成欧盟数据保护的统一标准,甚至可能阻碍欧盟的经济活动,引发不当竞争。

在 DPD 一般规则的基础上,欧盟围绕特定行业、特定数据类型立法,形成了一系列指令"孤岛"。这些指令虽是对 DPD 一般规则的具体化和补充,但加剧了欧洲数据保护立法的碎片化。以电子通信行业为例,1997 年,欧盟基于 DPD 首先颁布《电信行业个人数据处理的隐私保护指令》,后于 2002 年通过《隐私和电子通信指令》取代前

① Orla Lynskey, *The Foundations of EU Data Protection Law*, pp.87-88.

② Artur-Axel Wandtke, „Ökonomischer Wert von persönlichen Daten:Diskussion des Warencharakters von Daten aus persönlichkeits- und urheberrechtlicher Sicht", *MMR*, Heft 01, 2017, 6.

者,并于 2009 年颁布《cookie 指令》以进一步补充细化《隐私和电子通信指令》。① 就数据分类保护而言,欧委会基于《通向共同欧洲数据空间》提出数据分类设置不同规则,通过《公共部门信息重复使用指令》《科学信息保存获取的建议》和《私营部门数据分享指引》释放不同类型数据的再利用潜力。② 为确保数据保护规则切实实施,欧盟还颁布了《数据保护法执行指令》,保护刑事执法机构在使用个人数据时保护公民基本权利。③

指令立法初步建构了欧盟数据保护法的法律基础和体系,对"从无到有"建构欧盟数据法而言是妥当的,但指令碎片化的固有缺陷使得数据保护法缺乏协调性,增加了额外成本和行政负担,尤其是在多个成员国设立的数据控制者必须符合当地国家的规定。对数据主体和数据控制者而言,国别性差异导致指令本身的平等保护目标无法实现。④ 欧盟亟须进一步整合派生性立法,侧重欧盟数字内部市场的统一立法和统一监管,"条例"就是一体化规制的典型法律工具。

"条例"一体化规制数据保护的典型尝试是 2016 年通过(2018 年 5 月 25 日起实施)的 GDPR,该法取代 DPD,确保数据处理的个人权利保护规则一体化适用于所有成员国,建构更一致的个人数据保护框架。GDPR 的核心内容是根据技术发展调整数据保护规则,规制个人数据处理,促进个人数据自由流动,强化数据主体权利,确立单一

---

① 《隐私和电子通信指令》不仅保护电子通信中的个人数据处理,也保护通信机密性,故包含与法人有关的非个人数据规则,但 DPD 和 GDPR 均仅保护个人数据,不适用于法人。Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, OJ L 24, 30.1.1998, pp.1-8; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), OJ L 201, 31.7.2002, pp.37-47; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws (Text with EEA Relevance), OJ L 337, 18.12.2009, pp.11-36.

② Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a Common European Data Space", 25.4.2018, COM (2018) 232 final; Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Re-use of Public Sector Information, OJ L 345, 31.12.2003, p.90; European Commission, Commission Recommendation (EU) 2018/790 of 25 April 2018 on Access to and Preservation of Scientific Information, OJ L 134, 31.04.2018, pp.12-18; European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-personal Data in the European Union, 13.9.2017, COM (2017) 495 final.

③ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp.89-131.

④ European Commission, Commission Staff Working Paper, Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final, Annex 2, 21f.

监管机构的企业监管“一站式”原则,促进交易便利化。[①] GDPR 确立了接收、处理个人数据的合法公平透明原则、最小必要原则、目的限制原则、准确性原则、存储限制原则、完整性和保密性原则,对数据的控制者和处理者提出了严格要求,还制定了严格的监督惩罚机制,设立了专门的政府监管机构,要求企业指定数据保护专员。对一般违法行为,对涉事企业处以上限一千万欧元或上年度全球总营业收入 2%的罚款,对严重违法行为,罚款上限为上年度全球营收总额的 4%或两千万欧元,代表了全球个人信息违法处罚最高水平。

数据保护的一般规则从指令转为条例,特定行业、特定类型的数据保护立法也处于一体化规制的转型之中。2017 年,欧委会通过《隐私和电子通信条例草案》[②],旨在取代《隐私和电子通信指令》。同年,《非个人数据自由流动条例草案》[③]确立了非个人数据跨境自由流动的基本原则,形成了欧盟对个人数据和非个人数据自由流动的基本法律框架。

经过策略性更迭后,欧盟数据保护的立法工具进入检视规范、建构体系的新阶段,在 GDPR 的先导下,基于统一适用和统一监管目标,欧盟数据保护的立法触角从个人数据逐步扩张到非个人数据,数据立法的价值目标从严格的基本权利保护,逐步发展到与数字产业监管发展相融合的多维视角。

三 《一般数据保护条例》的制度突破

(一)拓宽适用范围

1.实质管辖的开放性

GDPR 适用于构成或拟构成文件系统的全部或部分以自动化方式处理的个人数据。[④] 立法者欲借助广义解释,涵盖所有个人数据处理行为,扩大管辖范畴并确立高

---

① Daniel Rücker and Tobias Kugler, *New European General Data Protection Regulation, A Practitioner's Guide, Ensuring Compliant Corporate Practice*, C.H.Beck, 2018, p.4.

② Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.01.2017, COM (2017) 10 final.

③ European Commission, Commission Recommendation (EU) 2018/790 of 25 April 2018 on Access to and Preservation of Scientific Information, OJ L 134, 31.04.2018, pp.12-18; European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-personal Data in the European Union, 13.9.2017, COM (2017) 495 final.

④ GDPR 第 2 条。

水平保护标准。[①] “个人数据”和“处理”概念的界定和解释直接决定了 GDPR 的实质适用范围,而概念构成要件的界定包括 GDPR 规范文义和欧洲法院判例两部分,GDPR 确立了一般性规范,法院拥有广泛裁量空间。事实上,自 DPD 和电信行业诸项指令颁行以来,法院判例已确立一系列识别规则。关键的问题包括以下四类。

第一,何为“处理”? GDPR 对“处理”概念采取了非穷尽性列举的开放界定立法技术。数据“处理”指对个人数据或个人数据集合所做的任何一项或一组操作,例如,收集、记录、组织、结构化、储存、修改、检索、查阅、使用、传播或以其他方式利用、排列或组合、限制、删除或销毁。[②] 这一界定承继了 DPD 第 2 条第 b 项的“处理”概念。无论是浏览器缓存等暂存于 IT 系统的个人数据,还是显示于电脑屏幕的个人数据,抑或是通过电脑、智能手机、网络或无人机摄像头进行的数据处理,甚至是借助可穿戴设备或汽车等智能设备收集的个人数据,所有数据处理都属于 GDPR 的数据“处理”。手动处理也构成 GDPR 的“处理”,当数据被包含或意图包含于文档系统,且文档应依特定标准建构时,处理行为亦受 GDPR 管辖。[③] “处理”须具备合法性前提,包括数据主体(明示)同意、为履行合同必须、履行法定义务必须,以及数据控制者的合法利益。[④] 开放界定“处理”概念能够防止产生规避风险,使自然人的权利保护处于技术中立立场,不依赖于所用技术,使 GDPR 的适用范围独立于技术变革。[⑤] 这种立法技术也为司法裁判预留了裁量空间,欧洲法院通过判例进一步补充和明确了“处理”概念,例如,发布新闻稿、网页加载个人数据、在光盘上收集、传输或通过短信转发数据、响应访问文档请求传递数据、获取和存储指纹、通过 ANAF 传输数据和 CNAS 的后续处理都构成数据处理行为。[⑥]

第二,如何界定“个人数据”? GDPR 仅适用于个人数据,这种个人数据包括任何已识别或可识别的数据主体相关信息,通过识别直接或间接归至某一主体的数据即个人数据,例如,通过物理、生理、遗传、心理、经济、文化或社会认同特征识别,以及姓名、身份、位置数据和在线识别码等信息。[⑦] 假名化处理后的个人数据若可能合理识别到

---

① Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR), A Practical Guide*, Springer International Publishing AG, 2017, p.9.

② GDPR 第 4 条第 2 项。

③ GDPR 第 2 条第 1 款;序言第 15 项。

④ GDPR 第 6 条。

⑤ GDPR 序言第 15 项。

⑥ T-259/03, Nikolaou v. Commission, 12.9.2007; C-230/14, Weltimmo, 1.10.2015; C-101/01 BodilLindqvist, 06.11.2003;C-73/07, Satakunnan Markkinaporssi and Satamedia, 16.12.2008;C-28/08, Commission v Bavarian Lager, 29.06.2010;C-291/12, Schwartz, 17.10.2013;C-201/14, Bara and Others, 1.10.2015.

⑦ GDPR 第 4 条第 1 项。

特定主体,则属于个人数据;匿名化处理的数据因无法识别特定主体,故不构成个人数据。① 欧盟法中的个人数据概念的判定标准始终如一,尽管 DPD 第 2 条以能否"特定化"为标准,GDPR 将规范措辞改为"可识别性",但两者内涵并无变化。欧洲法院也基于"可识别性"标准确立了一系列示例规则,例如,与自然人的电话、工作或兴趣信息相关的姓名、超过特定收入阈值的姓名、参会人姓名、ISP 地址、指纹、传输的税务信息以及与服务提供商掌握的其他数据结合就能间接识别自然人的动态 IP。这些信息都因具有可识别性而构成个人数据。②

第三,为何特别保护"敏感数据"? GDPR 将个人数据分为一般数据和特别类型数据。前者指任何能以直接或间接方式识别个人身份的任何数据,包括通过 IP、浏览记录产生的数字轨迹并可追踪识别特定主体的身份信息。后者指揭示人种、政治倾向、宗教、哲学信仰、生物特征、基因、健康相关、性生活与性倾向的数据,亦称"敏感数据"。两类数据的处理规则不同,一般类型的个人数据可以基于数据主体同意前提处理,特殊类型的个人数据处理原则上禁止,但非绝对禁止。细分个人数据类型并对敏感数据提供特别保护的理由明确:由于敏感数据具有高度人身性,与基本权利和基本自由关联密切,对此类数据进行的处理行为可能给基本权利和基本自由带来显著风险。尽管如此,对此种分类的批评意见不绝如缕,在大数据时代数据挖掘技术发展背景下,单一的类型细分存在一定的功能障碍。

第四,实体适用的有限例外。GDPR 对实质适用范围的宽泛界定,意味着立法者对适用例外的解释采取限制和狭义的解释思路。不受 GDPR 管辖的数据处理行为包括:(1)欧盟法律管辖外的活动;(2)《欧盟条约》第 5 编第 2 章的共同外交和安全政策;(3)刑事犯罪领域;(4)纯粹的个人或家庭生活中的数据处理。③ 上述四种例外在通常的商事经营活动中并不常见,其中最可能出现的例外情形应当是"纯粹的个人或家庭生活中的数据处理"。依一般社会观念,解释"纯粹的个人或家庭生活"概念时应包括为休闲活动、度假等活动所为之个人数据处理,基于"纯粹"一词,应对"个人或家庭生活"作狭义解释。④

2.地域管辖的扩张性

---

① GDPR 序言第 28-29 项。

② C-101/01, Bodil Lindqvist, 06.11.2003; C-73/07, Satakunnan Markkinaporssi and Satamedia, 16.12.2008; C-28/08, Commission v. Bavarian Lager Co., 29.6.2010; C-70/10, Scarlet Extended SA v. Societe Belge des auteurs, compositeurs et dditeurs SCRL (SABAM), 24.11.2011; C-291/12, Schwartz, 17.10.2013; C-201/14, Bara and Others, 1.10.2015; C-582/14, Patrick Breyer v Bundesrepublik Deutschland, 19.10.2016.

③ GDPR 第 2 条第 2 款。

④ GDPR 序言第 18 项。

虽为欧盟立法,GDPR 的适用却未止于欧盟疆界。GDPR 的地域管辖具有明显的扩张性:无论数据处理行为是否发生于欧盟,设立在欧盟境内的控制者或处理者均适用 GDPR;设立在欧盟境外的控制者或处理者在提供产品服务过程中处理了欧盟境内数据主体的个人数据,即受 GDPR 管辖。这种扩张管辖糅合了属地原则、住所原则、设立原则和市场地原则,一体适用于数据控制者和处理者,尤其是市场地原则构成条例的一项重大更新。GDPR 的跨境管辖意图明确,一方面,欧盟跨国企业存在跨境数据传输的现实需求,因此,管辖规则为内部市场保证公平竞争条件并保障隐私;另一方面,此种管辖能够有效预防选择法院现象,防止企业通过选择设立地来挑选数据保护水平较低的成员国法为准据法。① 从 GDPR 的条款看,以下问题值得关注。

第一,何为"设立"? 依据设立原则,GDPR 适用于设立在欧盟的控制者或处理者进行的个人数据处理行为,无论处理行为是否发生在欧盟内部。② 第 3 条仅用"设立"(establishment)一词,未提及住所概念。但欧洲法院判例表明,符合公司章程的住所亦为设立地。③ 换言之,住所的确定与数据处理技术是否在欧盟境内无关,与服务器是否在欧盟境外无关,也与处理的是欧盟公民的还是第三国国民的个人数据无关,甚至与数据主体居住地无关。GDPR 未界定"设立"概念,仅于序言中阐明:设立是指通过稳定安排从事有效真实经营的法律形式,无论其是否通过有法人资格的子公司或分支机构。④ 这一概念承继了 DPD 序言第 19 项和欧洲法院判例,具体判定适用欧盟法中就"设立"概念确立的一系列判定规则。例如,为确保个人数据高水平保护,应对"设立"作限缩解释;⑤应依据实体活动的具体性质判定"设立"概念中的"稳定安排"要件,例如公司是否仅通过互联网提供服务,亦应平衡"稳定安排"和(经营)活动对数据处理的贡献。稳定安排中的经济活动可能是次要因素,例如运行一个提供服务的网站。⑥ 在成员国内拥有银行账户、信箱和代表处作为成员国客户专属联系点的非欧盟实体,应将其在成员国的人力资源和实体资源视为一种稳定安排,进而构成"设立"。⑦

第二,GDPR 是否管辖非欧盟的数据控制者? 依据市场地原则,即便数据控制者和处理者未在欧盟境内设立,只要数据处理行为是向欧盟数据主体提供商品或服务(无论是否支付对价),或监控数据主体行为且受监控行为发生在欧盟境内,即受条例

---

① Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR), A Practical Guide*, p.22.

② GDPR 第 3 条第 1 款。

③ EuGH, *NJW*, 2015, 3636, Rn. 29; EuGH, *EuZW*, 2014, 541, Rn. 49.

④ GDPR 序言第 22 项,EuGH, *NJW*, 2015, 3636, Rn. 19; EuGH, *EuZW*, 2014, 541, Rn. 19。

⑤ C-131/12, Google Spain, 13.05.2014.

⑥ C-230/14, Weltimmo, 1.10.2015.

⑦ C-230/14, Weltimmo, 1.10.2015.

管辖。① 市场地原则扩大了 GDPR 的适用范围,向数据保护和消费者保护倾斜,旨在解决欧盟境外的数据处理是否以及在何种程度上保护本国国民。② 受管辖扩张影响最为显著的是欧盟境外的数据处理主体,即便非欧洲国家的服务提供商的住所地或设立地不在欧盟,亦受 GDPR 管辖。③ 例如,非欧洲企业的数据处理行为以欧盟境内主体为对象时,企业纵使未提供商品服务,仍受之管辖。④ GDPR 地域管辖亦辐射欧洲经济区和欧洲自由贸易区国家。欧洲经济区联合委员会于 2018 年 7 月 19 日通过《纳入 GDPR 的联合委员会决议》并于 7 月 20 日生效,⑤欧洲经济区和欧洲自由贸易区国家的议会须相应修改内国法,GDPR 在议会批准后才适用于整个欧洲经济区,在此之前仍适用 DPD。⑥

尤其值得关注的是,地域扩张管辖在一定程度上影响了 GDPR 数据跨境传输的规则设计。例如,在扩张管辖下,数据跨境传输的控制者自然存在通过政府"充分性决定"或跨国企业"BCR 规则"来弱化 GDPR 监管的巨大动力,能否适用允许跨境传输的例外情形在很大程度上将会体现为相关国家、地区、企业与欧盟之间的利益博弈。换言之,经由扩张管辖及关联的例外允许跨境传输规则,欧盟为己方赢得了相关领域贸易谈判的有利地位。

(二)数据主体权利的非绝对性

欧盟数据立法将个人数据权利构建为一种需要平衡的权利。数据主体权利是一种非绝对权,应与其他权利和正当利益适当平衡,这种非绝对性明确体现于数据主体的权利体系:除了规定数据主体权利行使的一般前提和法律效果外,GDPR 确立了大量但书条款和限制条款,以限制数据主体权利的无限扩张。就具体的数据主体权利类型而言,GDPR 在访问权、限制处理权和拒绝权之外,确立了数据可携权和被遗忘权概念,这在某种程度上构成制度创新,但更确切而言,应当是对权利内在体系的发展:数

① GDPR 第 3 条第 2 款、序言第 23-24 项。

② GDPR 第 3 条。

③ Boris P. Paal und Daniel A. Paul(Hrsg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz (DS-GVO BDSG)*, C.H.Beck, 2. Aufl. 2018, Art. 3 Rn 13-20.

④ Ibid..

⑤ European Economic Area, Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 Amending Annex XI (Electronic Communication, Audiovisual Services and Information Society) and Protocol 37 (Containing the list Provided for in Article 101) to the EEA Agreement [2018/1022], OJ L 183/23, 19.07.2018.

⑥ 在纳入程序上,欧洲经济区汇集了欧盟成员国和冰岛、列支敦士登和挪威三个欧洲自由贸易区国家。为确保同质性,与欧洲经济区相关的欧盟法案须被纳入《欧洲经济区协议》,使欧盟法扩大适用于欧洲自由贸易联盟国家,纳入程序须以欧洲经济区联合委员会决议形式完成。参见 Agreement on the European Economic Area-Final Act-Joint Declarations-Declarations by the Governments of the Member States of the Community and the EFTA States -Arrangements-Agreed Minutes-Declarations by One or Several of the Contracting Parties of the Agreement on the European Economic Area, OJ L 1, 3.1.1994, pp.3-36。

据可携权进一步夯实了传统意义上的访问权,被遗忘权是对传统意义上的删除权的升级和扩张。

需要强调的是,GDPR 遵循保护前置(Vorfeldschutz)理念构建数据主体权利。保护前置,即将数据保护前置到数据收集、处理阶段。原因在于,数据保护是保护人本身的价值,一旦侵害了人的内在,就无法恢复到不受侵害的状态,这有别于金钱的损害赔偿,故需保护前置,在数据收集处理阶段进行类型化保护。但由于各种规制中的多层次前置保护,其类型化反而使其离本来要保护的法益越来越远,无法"穿透"或"回归"最初欲保护的法益,甚至导致功能失调,故而需要借助比例原则来限制前置性保护的适用。①

1.数据可携权②:数据权利内容的客体化

数据可携权是 GDPR 的一项制度创新,旨在平衡数据流动的自由和管制,使数据主体能以简明方式迁移数据并更好地控制个人数据。③ 可迁移能力是数据移动、复制或传输的能力,这一制度是促进服务提供商竞争、防止锁定效应的关键因素。④ GDPR 将数据可迁移性固化为数据可携权,是指数据主体有权以结构化的、通常使用的、机器可读的、可互操作的形式接收其提供给数据控制者的个人数据,并有权将之传输给其他控制者。⑤ 这是一项高度人身性的权利,不得移转给第三人,不得继承,但可代理行使。⑥ 这一权利在一定程度上有助于澄清数据归属,即控制者对个人数据不具有控制权,仅负有配合义务,由此避免控制者争夺用户数据,促进数据流动。GDPR 序言用"可互操作的方式"⑦界定数据可携权,能从源头上改变用户数据锁定现象,使锁定效应最小化。⑧ 可携权的创新还在于从数据主体视角设计数据流动规则,重构"数字服务用户/提供商"、"数字产品服务市场上的竞争者"之间的关系,由此影响个人数据控

① Martin Eßer, Philipp Kramer und Kai von Lewinski, *Auernhammer DSGVO BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze Kommentar*, S.6-7.

② 数据可携权,亦译为数据迁移权。笔者使用数据可携权概念的理由有二:其一,数据可携权强调的是数据主体对于个人数据的一种具有高度人身性的权利,这种权利不可以移转给第三人,也不可以继承,而数据迁移权很难体现出人身性权利这一特性;其二,目前国内多个译本以及行业已经通行使用数据可携权概念,为了尊重目前通行说法,本文也继续使用数据可携权这一概念。

③ GDPR 序言第 68 项。

④ Commission Staff Working Document, "On the Free Flow of Data and Emerging Issues of the European Data Economy", Accompanying the Document Communication Building a European Data Economy, 10.01.2017, SWD (2017) 2 final.

⑤ GDPR 第 20 条第 1 款。

⑥ Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel und Winfried Veil (Hrsg.), *Kommentar Datenschutz-Grundverordnung*, Bundesanzeiger Verlag, 2018,S.600.

⑦ GDPR 序言第 68 项。

⑧ Boris P. Paal und Daniel A. Paul (Hrsg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz (DS-GVO BDSG)*, Art. 20 Rn 4-6.

制格局。鉴于 GDPR 第 20 条未全面界定数据可携权的构成要件,第 29 条工作组在 2017 年最终版本的《数据可携权指引》中阐明了一些关键问题。①

数据可携权由两项相互独立的请求权构成,即(1)数据主体获得个人数据的权利,和(2)要求数据控制者和处理者向其他主体提供个人数据的权利。前者是获取个人数据副本的权利,后者是将数据从某一控制者直接传输到另一控制者的权利。常见适用场景如社交网络、员工离职、更换保险公司时的数据携带。数据可携权不适用于符合公共利益的执行职务行为或委托数据控制者行使公权力进行必要处理之情形。这意味着,基于公共利益或行使公权力情形下的数据处理行为会限制数据可携权的行使。② 可携权不得优先于删除权行使,不应影响其他主体的权利和自由,涉及第三方个人数据时,数据主体行使可携权应尊重第三方的基本权利和自由。违反数据可携权规定时,可处以上限为 2000 万欧元的行政罚款,或对企业而言,最高罚款为上一财务年度全球总营业额 4%上限,以金额较高者为准。③

2. 删除权(被遗忘权):数据权利作为一项限制性支配权

数据错误、不完整或非法时,数据处理可能对数据主体自由权产生消极影响。有鉴于此,GDPR 确立了删除权、更正权和限制处理权等不同类型的权利,使数据主体能够限制或影响控制者的处理行为。更正权和限制处理权是删除权的缓和形式,前者是数据主体有权要求控制者及时更正不准确的个人数据,④后者则是依据数据主体要求将可删除信息作限制处理。⑤

在规范构成上,删除权的规定有三款:第 1 款规定数据主体删除个人数据的权利;第 2 款以信息权形式对欧洲法院判例中的被遗忘权进行规范转化;⑥第 3 款对适用范围予以限制。删除权(第 1 款)是一项主观权利,相对方负有删除数据的客观义务。⑦

---

① 鉴于 GDPR 对数据可携权的适用范围和前提要件存在开放性,第 29 条工作组于 2016 年起草《数据可携权指引》并于 2017 年公布最终版本,为数据控制者提供指引。参见 WP29, "Guidelines on the Right to Data Portability", 13.12.2016, 16/EN WP 242; WP 29, "Guidelines on the Right to Data Portability", 05.04.2017, 16/EN WP 242 rev.01.

② GDPR 第 20 条第 3 款。

③ GDPR 第 85 条第 5 款第 b 项。

④ GDPR 第 16 条。

⑤ 京东法律研究院:《欧盟数据宪章〈一般数据保护条例〉GDPR 评述及实务指引》, 北京:法律出版社 2018 年版,第 61 页。

⑥ 尤须注意,欧盟数据保护法早已确立删除义务,GDPR 的删除权规定并非新创。GDPR 的删除权与源于 DPD 的被遗忘权也存在差异:在 Google Spain 案中,欧洲法院认可基于 DPD 第 12 条第 b 项和第 14 条第 a 项提出的针对搜索引擎的类似删除的请求权,进而创设了被遗忘权。GDPR 第 2 款的规定是对欧洲法院 Google Spain 判例的一种体现和转化,但较之更进一步,即删除权不应与判例认可的请求权混淆(判例中将搜索引擎本身界定为责任主体),删除权仅被设计为相关数据主体的一项权利,删除权本身不同时构成责任主体的义务。参见 C-131/12, Google Spain, 13.05.2014。

⑦ BeckOK DatenschutzR/Worms, 24. Ed. 1.8.2017, DS-GVO Art. 17 Rn. 22-24.

删除权肯认了数据主体对个人数据的支配权,是一项高度人身性权利,不得移转给第三人,不得继承,但可以代理行使。① 就权利行使的前提要件而言,在处理目的消失、同意撤回、反对处理、非法处理、履行法定义务和儿童个人数据的六类情形下,控制者负有删除义务;并且,无论数据主体是否申请,控制者的删除义务独立持续存在,一旦满足前提,控制者须立即删除。"立即删除"亦表明,删除权规则不适用 GDPR 第 12 条第 4 款的处理期限。删除权的法律效果以获得期望结果为特征,法案虽未界定删除概念,但删除意味着数据控制者无法再次使用数据,故可通过所有可能的技术手段销毁数据。无论方式如何,删除的核心在于控制者和第三人都无法再访问、阅读或处理数据,数据理论上的重建可能性并不重要。② 就删除形式而言,数据主体主张的删除形式取决于数据本身的呈现形式和尽力删除数据所需费用。由于数据销毁须回溯至数据最初的处理和存储方式,有效销毁数据仍依赖于控制者。在删除义务的体系位置上,由于删除权的构成要件需参引 GDPR 其他条款,故其体系归属具有特别意义。责任主体的删除义务源于两种不同进路:删除义务既可能源于责任主体应遵守的一项法定持续义务。也可能源于数据主体有效行使一项需申请的形成权。③具体而言,一方面,删除义务可源于责任主体应遵守的一项法定持续义务。此种义务独立存在,不以数据主体积极行使删除权为前提,具体指 GDPR 第 5 条第 1 款第 d 项规定的"应采取一切合理措施,确保不正确的个人数据立即被删除"。这种个人数据的"正确性"要求包括"处理目的消失"、"违法处理"或"履行法定删除义务"(第 17 条第 1 款第 a 项、第 d 项和第 e 项)。④ 另一方面,删除义务也可能源于数据主体有效行使其删除权,前提是数据主体"撤回数据处理同意"或"提出异议"(第 17 条第 1 款第 b 项、第 f 项和第 c 项)。此种删除权系形成权,数据主体可以单方面决定并直接影响是否以及如何处理其个人数据。⑤

被遗忘权的规范基础是第 2 款,这是第 1 款删除权的法律后果,亦对其构成补充,将删除义务扩张到公开个人数据的控制者,以社交网络和搜索引擎为主要适用场景,这一权利是欧洲法院判例的成文化。当数据主体请求删除数据且控制者已公开数据时,负有删除义务的控制者应在考虑技术、实施成本的前提下采取合理步骤,通知正在

① Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel und Winfried Veil (Hrsg.), *Kommentar Datenschutz-Grundverordnung*, S.525.

② BeckOK DatenschutzR/Worms, 24. Ed. 1.8.2017, DS-GVO Art. 17 Rn. 54-57.

③ Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel und Winfried Veil (Hrsg.), *Kommentar Datenschutz-Grundverordnung*, S.525.

④ Ibid., S.522.

⑤ Ibid..

处理数据的相关控制者。控制者在删除义务外还负有实现网络中被遗忘权的告知义务,从而扩张了传统意义上的删除权。

个人数据保护应符合比例原则,删除权虽与个人权利联系紧密,但可能与言论自由、信息自由、公共知情权等公共价值存在矛盾。删除权的限制情形(第 3 款)意味着,在五种情形下免除责任主体的删除义务:(1)行使言论自由权;(2)遵守法律义务或符合公共利益的职务执行或委托数据控制者行使公权力所必须;(3)为实现公共卫生领域的公共利益理由;(4)为实现公共利益、科学历史研究或统计目的;或(5)为确立、行使或防御法律上请求时,应在必要范围内进一步保留个人数据合法。① 较特别的是,由于删除权的限制适用情形中明确提及言论自由和信息自由,这意味着 GDPR 为这两项基本权利直接确立了免除删除义务的例外。此外,例外情形中较为重要的是第 3 款第 e 项的法律主张。该主张与意定之债关系紧密,仅在合同主给付义务和从给付义务均履行完毕时,方才免除删除义务。此外,履行侵权等法定之债的义务后,也会免除删除义务。

删除权的规范体系折射出不同利益群体对数据利益的深层次矛盾。搜索引擎、网站运营商和社交网络是典型的删除义务主体。事实上,删除个人数据体现了公众信息利益和不愿公开特定信息的数据主体利益之间的紧张关系,处理这种紧张关系时需要平衡公众的数据使用利益和已公开数据中的人格保护的可能性。② 以搜索引擎为例,公众的信息利益和数据主体利益之间存在紧张关系,欧洲法院判例原则上将数据主体权利置于优先地位。法院认为,原则上,数据主体的权利比搜索引擎经营者的经济利益重要,也比公众基于特定姓名搜索到该主体个人信息的公众利益重要。③ 这种利益权衡不仅直接影响了公众和私人的数据使用利益,其对基本权利的位阶排序也会深刻影响数据主体、公众和数据控制者的关系,甚至行使删除权(被遗忘权)可能与言论自由,尤其是与新闻自由之间存在严重冲突,这是欧洲法院个案裁判时无法回避的现实。

(三)数据跨境传输:“归属”不排斥“利用”

数据主权亦构成数据保护法的一个重要维度。基于市场地原则和实质管辖,GDPR确立了欧盟对个人数据的宽泛管辖,进而建构了“归属”不排斥“利用”的数据跨境传输规则。欧盟在宣誓数据主权立场的同时,也在某种程度上实现了通过“塑造新

① GDPR 第 17 条第 3 款。

② Peter H. Klickermann, „Die Privilegierung des Lösungsrechts, Das Recht auf Vergessenwerden im Fokus der beruflichen Tätigkeit“, *MMR*, Heft 04, 2018, S.210.

③ C-131/12, Google Spain, 13.05.2014.

的全球标准”①来增强相关贸易谈判筹码的实质效果。

GDPR 对数据跨境传输采取“原则禁止、例外允许”的规制模式。这一模式承袭于 DPD,只不过 DPD 的数据传输规定较严格,难以适应数据跨境流动的现实,因此 GDPR 适度放松了数据跨境流动管制,确立了更多跨境传输的合法方式,以提高跨境传输的灵活性。GDPR 未界定“传输”概念,从第 4 条第 2 项“处理”概念中的“通过传播披露”的界定可得,“传输”指对个人数据的任何形式的披露。因此,识别“传输”的判定因素是数据受领人是否在第三国或是否是一个国际组织,数据披露形式不甚重要,数据是否到达第三方亦不重要,不限于数据物理传送,涵盖与他方共享、向他方传输,或披露/允许他方获得数据的行为。② GDPR 第 44 条是一项预防性禁止规定,在一般性禁止下仅保留三类允许传输的例外情形:(1)国家/地区获得充分性认定;(2)企业自主采用符合规范的适当保护措施;(3)数据主体明确同意等其他例外情形。③ 这三种情形中,前两种分别指向政府的事前背书和市场导向的自我拘束,前者为欧盟和其他地区、国家的数据流通谈判预留了政策口径,后者则为跨国集团的整体“安全港”设置创设了可能性。

1. 政府事前背书:充分性决定

符合充分性决定是 GDPR 框架下数据跨境传输最为便利确定的方式。充分性决定源于 DPD 第 26 条第 1 款第三国数据保护水平评估的“白名单”制度,但 GDPR 的充分性决定不涉及有关确立充分性决定的谈判机制,而是全面规定了欧委会进行充分性决定应遵守的实体和程序规则,并在充分性决定的评估对象上新增了除国家外的特定区域、行业领域和国际组织。充分性决定的实体标准包括但不限于有效的数据保护体系、有效的数据保护监管和国际协定条约义务三个维度。其认定程序应由当事国主动提出,双方进行技术对话后,由欧盟内部独立专家出具评估报告,欧委会提案送交欧洲数据保护委员会(EDPB)并由欧盟国家代表批准是否具有充分性。GDPR 第 45 条确认欧委会基于 DPD 通过的决定继续有效,已通过充分性认定的“白名单”国家继续有效。④ 尽管是目前 GDPR 框架下数据跨境传输最为便利的解决方式,但由于 GDPR 对充分性决定的实体标准采取了开放性列举的立法方式,因此,欧委会对充分性决定的

① Beata A. Safari, “Intangible Privacy Rights: How Europe’s GDPR Will Set a New Global Standard for Personal Data Protection”, *Seton Hall Law Review*, Vol. 47, pp.809-848.

② Paal/Pauly/Pauly, 2. Aufl. 2018, DS-GVO Art. 44 Rn. 3-8.

③ GDPR 第 40 条以下。

④ “白名单”国家与地区目前包括安道尔、阿根廷、澳大利亚、法罗群岛、根西岛、马恩岛、以色列、泽西岛、新西兰、瑞士、乌拉圭和加拿大。欧盟和美国在《隐私盾框架》下,保护基于商事目的将欧盟公民个人数据传输到美国的数据主体的基本权利。

衡量存在较大的裁量空间,更多的是一种政治或政策考量,甚至可能成为欧盟与其他地区、国家谈判或利益交换的一种合法工具。

2. 市场导向的自我拘束:有拘束力的公司规则

如果涉及数据跨境传输的企业未取得充分性决定,第三国的数据控制者和处理者可以在提供适当保护措施的前提下进行跨境传输。这些措施主要包括:(1)经批准的个人数据保护格式条款;(2)有拘束力的公司规则;(3)行为准则;(4)认证四种方式,其中有拘束力的公司规则是 GDPR 新增的数据跨境合法机制。

有拘束力的公司规则(BCR)指欧盟境内的公司集团内部或从事共同经济活动的公司集团之间在传输个人数据时应遵守的保护政策。跨国公司内部存在数据跨境传输、数据库访问权限开放需求。例如,在集团范围内处理客户或供应商数据时,尤其是集团内部的全球客户数据管理或在人力资源管理系统下,若集团或其关联公司的经营模式以数据为基础,这一经营模式需以整个集团内部可以使用相关个人数据为前提。但企业集团公司通常不会全部设立于欧盟内部或设立于能充分保护个人数据的第三国,此时就会产生能否向第三国传输数据的问题。BCR 是集团型跨国企业可以优先考虑的机制,集团遵循一套完整并经个人数据监管机构认可的数据处理机制,使集团内部成为一个“安全港”。如果集团公司获得 BCR 认可,个人数据可从集团内的一个成员合法传输给另一个成员。例如,宝马、惠普等公司的 BCR 规范已获得部分成员国监管机构的认可。BCR 的风险在于,GDPR 第 2 款的 14 项规则对企业集团提出了较高合规要求,必须确保个人信息在各个环节都得到充分保障,当住所地不在欧盟的集团成员违规时,其在欧盟成员国内的控制者或处理者应承担责任,那么集团面临的违规风险无疑是巨大的。①

四 对《一般数据保护条例》的质疑与批评

(一)价值困境:数据保护与监管的多元价值追求

数据保护的分类理论鲜少从监管的角度进行分类,若从目标角度观察则会发现,在 GDPR 的经济目标和基本权利保护目标下,数据保护监管涵盖了经济监管和社会监管两种典型的形式。②

数据保护监管是经济监管的表现。经济监管与国家调控关系密切,旨在构建市场

① GDPR 第 47 条第 2 款第 f 项。

② 基于监管角度的例外性探索,参见 Luiz Costa, “Privacy and the Precautionary Principle”, *Computer Law and Security Review*, Vol. 28, 2012, p.14; Orla Lynskey, *The Foundations of EU Data Protection Law*, p.76。

直接干预市场决策并影响市场实践,纠正特定的市场失灵。数据保护监管即是如此,其强调对个人数据保护的协调,消除数据流动障碍,实质是通过赋予数据主体主观权利,减少数据主体和数据控制者之间的信息不对称,降低歧视、数据泄露等风险。①

数据保护监管包含社会监管要素,是一种向弱势主体倾斜的监管。社会监管追求社会目标,但不追求明显的经济目标;经济监管却能考虑诸如信息权、消费者保护等更广泛的公共利益问题。由于市场失灵会阻碍社会目标的实现。因此,社会监管虽不追求经济目标,但以纠正市场失灵的经济目标为前提。市场失灵包括因信息不对称导致的市场扭曲或市场未能解释外部因素或保护公共利益,而数据保护监管旨在通过确保数据处理者参与考虑外部因素,由此实现社会目标。因此,当商品或服务产生的影响给其他人带来成本时,倘若成本并未体现于所提供的商品或服务的价格中,就存在负外部性。例如,为特定目的持有个人数据的公司(超市)通过出售数据或将数据用于市场营销获利,公司将个人数据用于出售商品之外的次要目的并获利,这种二次使用可能导致数据主体的有形或无形损失。缺乏数据保护法规时,数据控制者可能继续基于重复利用个人数据获利并损害数据主体利益。数据保护监管可以防止市场失灵,确保外部负效应的内部化,促进社会福祉。②

GDPR 兼收并蓄式的目标设定,导致其既是一种基本权利政策,也是促进市场协调的监管工具,这使得数据保护法本身性质不明。严格而言,GDPR 的双重目标设定不符合基础性法律依据。有别于 DPD,GDPR 的法律基础并非内部市场协调(《欧盟运行条约》第 114 条),而是数据保护(《欧盟运行条约》第 16 条),后者并不要求促进内部市场统一。不仅如此,GDPR 统一监管的预期目标存在实践瓶颈。欧盟数据保护法自 1995 年生效以来已逾 20 年,但成员国在数据保护制度的目标和实现目标应采取的最佳手段等问题上仍存在分歧。③ 采用条例形式后,法律监管将对欧盟统一适用数据保护规则发挥关键作用,但可能存在负面效应:在协调成员国法律时,GDPR 即便能够掌控程序性协调事宜,但因其为成员国预留了自由裁量空间,实质性协调仍难实现。尤其是在如何平衡数据保护和相互竞争的权利利益上,成员国之间的关系可能因条例的统一效力变得愈发紧张。对数据控制者和处理者而言,GDPR 的广泛管辖和高度合规要求不切实际。在震慑性罚则之下,数据控制者可能不再关注如何全面评估数据处理本身的公平性和必要性,转而借助“合规代理人”,通过专业服务为数据控制者或处理者创建问责工具、认证标志体系等形式性合规表象。这种合规代理服务的专业性私

① Orla Lynskey, *The Foundations of EU Data Protection Law*, pp.76-79.
② Ibid..
③ Ibid., pp.87-88.

人实体毋宁是提供一种形式保障,向股东、数据主体、监管机构表明其处理行为的合规性,降低违规风险,形为专业合规,实为分散数据主体和监管机构的注意力。①

GDPR 和欧洲法院如何协调经济和社会监管的关系,如何纠正数据社会弱势主体的信息失衡和经济力量失衡,仍是未来欧盟数据保护监管亟须解决的难题。欧洲法院虽然强调数据保护的基本权利保护价值,但并未明确数据保护是否比隐私保护更加重要。这意味着,数据保护在欧洲法院仍存在身份危机。② 欧盟数据保护法的目标从一开始就有双重性,这也暗示着,数据保护法的目标既不清晰、也不确定,欧洲法院的早期判例亦有所体现。③ 尽管《欧盟基本权利宪章》为欧洲法院论证欧盟数据保护的具体目标提供了一些视角,但法院目前忽视了这一点,而将数据保护权利和隐私权视为混合形式。④ 倘若欧盟数据保护法的明确目标无法确立,欧洲法院也将无法在未来协调指导欧盟数据保护法的发展,数据保护监管也将始终处于平衡不同主体利益和权衡立法目标的摇摆之中。

(二)技术困境:个人数据的监管障碍

1."个人数据-非个人数据"分类的功能障碍

"个人-非个人数据"的分类标准值得商榷。欧盟的数据保护法建立在个人、非个人数据区分的二分类型之上,其考量或许是前者易引发法律保护,而后者则不然。事实上,任何数据处理都需评估产生损害的可能性。数据分类的前提应当是类型的"原型-例外"选择。GDPR 的规则意味着,限定个人数据范畴外的剩余空间归属于非个人数据,即个人数据是例外,这是一种可疑的分类标准。本质上,个人数据和非个人数据的"原则-例外"的分类标准本身可能存在问题,或许应放弃以个人数据概念作为数据保护的基石的做法,选择其他标准,例如以"数据引发的损害"为标准,对处理个人数据或非个人数据产生的负面结果进行类型化。⑤ "个人-非个人数据"的分类易引发监管困境。GDPR 仅适用于个人数据,即与识别或可识别的个人有关的数据,但并未明确透明性原则、合意原则、数据最小化原则等监管原则以及诸如数据可访问性、删除权、可携权等数据保护规则是否适用于基于个人数据获得或发现的信息,尤其当个人

① Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law", *Law, Innovation and Technology*, Vol.10, No.1, 2018, pp.40-81.

② Orla Lynskey, "From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis", in Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet eds., *European Data Protection: Coming of Age*, Springer, 2013, pp.80-81.

③ Ibid..

④ Ibid..

⑤ Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law", pp.40-81.

数据被转化为组文件从而被匿名化或一般化的时候,上述原则规则能否继续适用?从技术上而言,数据挖掘技术可从个人数据,也可从非个人数据中提取信息。GDPR 仅监管个人数据,将使数据挖掘技术在很大程度上规避监管。①

2.“敏感数据”与大数据的监管错位

欧盟的数据保护政策以建构数据分层体系为基础,对某些形式的数据类别和数据集的处理方式有别于其他形式的数据。例如,DPD 第 8 条第 1 款禁止处理披露种族、政治观点、宗教或哲学信仰、工会资格和有关健康或性生活的数据,并设置有限例外。这种数据类型区分在 GDPR 第 9 条得到延续,GDPR 不仅规定了特殊类型的数据处理规则,还新增了基因数据、生物特征数据、健康相关数据,仅在特定必要例外情形下才允许处理这类敏感信息。事实上,此类敏感数据很难区分。但在大数据时代,正因此类数据可能产生重大损害,更需谨慎对待。因此,加强保护特定类型数据虽具有合理性,但更多的是象征意义。② 然而,大数据技术对现有的数据分类模式带来了挑战:大数据技术可能会瓦解数据分类保护的正当性,即便是象征意义上的保护理由亦不例外。③ 大数据环境中的歧视因素和敏感因素有别于传统歧视概念:以保险为例,被保险人的运动记录、饮食习惯、消费记录都可能通过大数据来评估个人未来健康状况,促使保费个人化,而欧盟对特殊类型数据的特别保护反而可能使具有此类特征的人暴露于歧视之中。④ GDPR 保护特殊类型数据若要防止歧视,而基于数据类型的反歧视路径看似能防止数据智能下的差别对待,但数据的超碎片化和指数式增长提供了新的建模可能,这种建模可能与数据处理同时发生。该模式正在取代此前基于特征现象的统计学体系,正在取代用于识别预先配置的法律结构或政治形式。⑤ 结果是,新的歧视形式不一定出于歧视意图,而特殊类型数据主要的目标是在象征和实际意义上实现保护,目前的歧视是受数据驱动,通常无涉意图。未来,基于数据的歧视不一定会遵循 GDPR 的特殊或一般数据的简单二分类型发生。这种类型区分显然无法适应大数据的发展。大数据是一种基于海量数据进行数据挖掘的更强大的形式,也是一种新的分析工具。GDPR 过于依赖“知情选择”的监管模式。但这一模式并不可靠,无法与大数据的发展趋势相协调。

---

① Ira Rubinstein, “Big Data: The End of Privacy or a New Beginning?”, *International Data Privacy Law*, Vol. 3, No. 2, 2013, pp.74-87.

② Tal Zarsky, “Incompatible: The GDPR in the Age of Big Data”, *Seton Hall Law Review*, Vol.47, Issue 4, Article 2, 2017, p.1013.

③ Michael Denga, „Gemengelage privaten Datenrechts“, *NJW*, 2018, 1371.

④ Antoinette Rouvroy, “Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data”, Council of Europe, Directorate General of Human Rights and Rule of Law, T-PD-BUR (2015)09REV, p.17.

⑤ Ibid..

大数据将给知情选择和数据最小化原则带来巨大挑战。GDPR 监管的技术基础并不可靠,即便 GDPR 大量赋予数据主体权利,大数据仍可能会抵消上述努力。或许,数据保护立法应与消费者赋权和鼓励新型商业模式相结合,使企业能从数据密集型的新型服务中获益,强调自律性质的企业行为准则的意义。监管机构也应鼓励控制者和处理者运用基于用户授权的新型商业模式,提供更多的监管弹性。①

3. 数据可携权与竞争法的冲突

数据可携权概念可能存在严重缺陷:可携权概念在解释上存在不确定性,概念适用范围不明,具体适用的服务类型并无定论。虽然欧委会在起草时特别指向社交网络,但可携权广泛适用于处理个人数据的其他在线服务提供商,将之广泛适用于尚未形成用户锁定效应的提供商,或将给企业带来不合理负担。GDPR 虽欲借助第 20 条第 2 款"在技术可行的情况下直接传输"的前提要件限制可携权的适用范围,但鉴于数据转移义务仅适用于已存在所需技术措施情形,上述限制反而可能阻碍控制者发展数据交换标准。

数据可携权的最大挑战来自竞争法。数据是一种竞争要素的体现,竞争法对数据的评估非常灵活,是否对特定数据主体或平台提出数据可迁移要求,在很大程度上取决于特定目标数据集、是否在相关市场,以及是否构成竞争所需要素,仍须个案斟酌。竞争法主要从竞争机制的角度判断特定主体所控制的数据集在竞争机制中的功能与角色。例如,如果数据构成重要的竞争要素,可能特定数据控制主体要附加竞争法上的义务,例如数据要确保可迁移。竞争法对迁移性要求的前提应是数据控制者的市场力量达到一定程度甚至是支配地位,并且滥用该地位损害了正当的市场竞争。竞争法对于数据迁移性的程序前提复杂,GDPR 将可携权构建为数据主体的一项基本权利,适用于不占市场支配地位的主体,无须满足滥用支配地位前提。可携权过于广泛的适用可能会抑制创新。而且,可携权的行使与竞争法上的排他性滥用规则存在一定矛盾,基于欧盟法的限制竞争对手的滥用行为概念,很难显示排除行为的主要类型,例如拒绝提供、拒绝访问关键设施。② 再者,欧盟竞争法规定,可基于《欧盟运行条约》第 102 条实施执行数据迁移性,但可携权并未排除基于竞争法理由的便于可迁移性的在线服务中的干预行为。最后,可携权可能降低消费者福利,这与竞争法的价值相悖。由于互操作性在技术上常难实现,而数据迁移义务将给供应商带来数据导入其他系统

① Ira Rubinstein, "Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, Vol. 3, No. 2, 2013, p.74.

② Peter Swire and Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique", *Maryland Law Review*, Vol. 72, 2013, p.350.

的高昂成本,这一成本将最终转嫁到消费者。不仅如此,即便互操作性看似便利了消费者,但在实务中,限制互操作性却能有效降低应用程序对个人数据的不必要访问风险,反而能够提高数据的安全性和隐私性。①

数据可携权体现了竞争法与数据相关法律规制存在交叉、竞合的趋势。若要与竞争政策协调,应从市场力量角度限缩解释义务主体范围。否则,过于强化个人数据权利保护,在数字经济中,企业基于数据的诸多有利于消费者长期利益的商业模式演化将受到严重抑制。事实上,可携权针对的核心问题,即锁定用户的成本和用户转换服务时遇到的阻碍,这两个核心问题完全可以通过竞争法解决。相较于可携权,竞争法的理论规则更为严密,既能顾及用户的锁定成本,也考虑到了锁定本身会带来的消费者福利。从长远考虑,一定的转换成本反而可以鼓励对新技术的投入,这也不失为一种有效率的制度安排。鉴于竞争政策在欧盟的基础地位并未动摇,欧盟需要进一步斟酌可携权与竞争法的协调衔接措施。

4. 删除权难以行使

被遗忘权的首要缺陷是概念不明,诸如“合理步骤”、“现有技术”和“公开”等不确定概念的实务适用规则不明。例如,采取合理步骤行使被遗忘权时,“合理性”的判定标准不明,学界对是否应以控制者的主观情况判定,抑或应遵循客观标准存有争议。② 由于 GDPR 区别对待微型、中小型企业与大型企业,③倘若统一适用客观标准,合理措施的技术实施成本将给小微企业和中型企业造成较大负担。因此,主观解释或许是一种较妥当的方案。此外,由于控制者在当删除行为在其努力范围之外时免于删除义务,依此推导,也应对合理性采取主观解释路径。再者,被遗忘权适用于个人数据,但不明确的是,被遗忘权是否适用于基于个人数据的推论或预测,而这种基于数据的推断或预测恰是大数据分析技术的产物。被遗忘权的地理范围亦不明晰。例如,控制者的删除义务是否应考虑实施删除措施的具体地理位置,存储于欧盟境外服务器上的数据是否受到删除义务影响;或者,如果数据仍能针对欧盟境外的用户提供访问时,控制者是否违反了删除义务。不仅如此,由于被遗忘权使控制者的信息义务扩张到其公开传播的数据的其他第三方控制者,但信息义务的极度扩张事实上缺乏操作性,在开放网络空间中要求控制者确定并通知所有第三方的可能性较低。

---

① Peter Swire and Yianni Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique”, p.378.

② 对合理性的解释标准,学界观点不一。采用客观解释标准,参见 Kamlah, in Plath, BDSG/DSGVO, Art. 17 (2016), rec. 15; 采用主观解释标准的,参见 Paal, in Paal/Pauly, DSGVO, Art 17 (2017), rec. 36; Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 48。

③ GDPR 序言第 13 项、第 98 项、第 132 项和第 167 项。

最后,被遗忘权缺乏实际操作性。例如,行使被遗忘权要求控制者采取“包括技术措施在内的合理措施”删除,并通知第三方的控制者。事实上,这一规定缺乏操作可能。删除权存在例外情形,当用户提出删除申请时,控制者需首先审查其是否属于例外情形,由于现有规定中的例外情形多为一般抽象概念,例如表达自由、公共利益等,这些概念判断存在裁量空间,缺乏确定性。

五 经济全球竞争驱动下的法律价值序列:个人数据保护法是否有未来?

数据立法区域竞争的实质,是数字经济的全球竞争。在数字经济全球竞争的驱动下,法律价值序列处于变动、平衡和重组之中。数字经济下法律价值序列的实质,是重新平衡言论自由、个人隐私、经营自由、流动自由和公共利益等基本价值和利益。这种平衡既是立法者对商业创新和个人保护的权衡取舍,也必然是在既有数字产业的现状下对市场竞争优势、经济长期发展和社会目标实现的不同选择和不同追求。因此,数字技术引发的问题绝不限于是否立法,更在于采取何种价值序列、以何种方式立法,并如何与既有法律监管体系相协调。① 以中美欧为例,各国数据立法的价值各异,对个人数据的保护路径亦有不同。美国强调网络开放和数据自由流动,将个人数据纳入隐私保护框架之下,采取隐私权规制模式,在私法层面缺乏一般性的个人数据保护法律体系,而是通过《云法案》、加利福尼亚州《消费者隐私法》等分散立法形成了相互独立的制度,法院判例亦不承认信息自决权,而通过解释将个人信息纳入隐私权中。② 欧盟虽允许数据流动,但对个人数据保护设置了严苛要求,采取“个人数据-非个人数据”的分类规制模式,保护基本权利的 GDPR 强监管模式甚至可能抑制大数据行业创新。中国《民法总则》第 111 条和第 127 条采取个人信息和数据分置的立法思路,第 111 条规定个人信息受法律保护,第 127 条规定数据和虚拟财产保护。《关于加强网络信息保护的决定》和《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》均对个人信息采取列举式的开放界定,以可识别性作为判断标准,《网络安全法》《电信和互联网用户个人信息保护规定》《网络交易管

① 对法律价值序列的平衡问题,我国学者已经提出,应区分个人信息和数据资产,分别进行权利建构。应就个人信息配置人格权益和财产权益,为数据经营者建构企业数据财产权概念,分别配置数据经营权和数据资产权,同时配置相应的权利行使的限制结构,例如市场经济秩序限制、公共利益限制、数据安全限制、大数据应用的特殊限制。参见龙卫球:“数据新型财产权构建及其体系研究”,《政法论坛》2017 年第 4 期,第 63 页;龙卫球:“再论企业数据保护的财产权化路径”,《东方法学》2018 年第 3 期,第 59 页。

② 谢远扬:“信息论视角下个人信息的价值——兼对隐私权保护模式的检讨”,《清华法学》2015 年第 3 期,第 108 页。

理办法》《信息安全技术数据出境安全评估指南》和《网络安全等级保护条例(征求意见稿)》针对数据出境、网络安全等级保护和个人数据保护等问题开始初步建构规范体系。①

无论是数字经济时代,抑或是不同的现实基础条件,背后都隐藏着最为深刻的权利主体与相对人的复杂关系。在个人数据问题上,这表现为“数据主体人格性的保护”与“数据控制者和处理者对数据权利的商业利用”之间的关系。这是一定的经济条件以及多元价值因素驱动下,个人和他人(们)的关系,GDPR 仅是此种关系的解决方案之一,仅是特定技术条件和时代场景下的一种立法尝试。起决定性作用的,仍然是深刻的法律价值序列因素,这也是数据立法必须深刻认识的问题本质。立法机构的使命在于,如何根据不断变化的社会和技术进行适当监管,如何保护数字经济中处于弱势的自然人的基本价值,如何最大程度促进经济创新和社会福祉,如何协调法律与技术的衔接以及如何使法律在技术前沿有效运行。机械分离数据主体和数据控制者,采取单一价值取向的个人数据保护法的立法模式,可能并非数字时代的最佳选择。

(**作者简介:**金晶,中国政法大学民商经济法学院民法研究所讲师、法学博士;**责任编辑:**张海洋)

① 亦有学者提出,编纂中的民法典之侵权责任编应当发挥后发优势,建构明晰的个人信息侵权规则。参见叶名怡:“个人信息的侵权法保护”,《法学研究》2018 年第 4 期,第 102 页。