数字经济视野中的欧盟《一般数据保护条例》

EU General Data Protection Regulation from the Perspective of Digital Economy

许　可

XU Ke

【摘　要】　数据是数字经济的关键生产要素，数据保护和利用规则构成了数字经济的底层架构。欧盟《一般数据保护条例》的出台与其重振数字经济、推动欧盟数字一体化市场的雄心密不可分。但在数据权利作为基本权利和欧盟各国作为数据经济消费国的背景下，《一般数据保护条例》对数字经济造成了不利影响，可能戕害创新、伤及互联网成熟业态、阻碍新兴产业的发展。我国应洞见其经济实质，作出有效的回应，并在《个人信息保护法》的制定中审慎借鉴相关规则。

【关键词】　数字经济　《一般数据保护条例》　个人信息保护法

【中图分类号】DF49　【文献标识码】A　【文章编号】2095－9206（2018）06－0071－13

Abstract: Data is critical means of production in the digital economy, so the rules regarding the protection and use of data consist the underlying architecture of the digital economy. The EU General Data Protection Regulation is derived by the ambition of boosting the digital economy and urging the digital single market. However, due to the data right as the foundational right and the EU members as the countries of consumption in digital economy, the General Data Protection Regulation will cause the possible negative effect on the digital economy, for instance, it probably hinders the progress of innovation, damages mature business format of Internet, and impedes the development of emerging industries. We should look through the economic essence of the General Data Protection Regulation, response effectively to this regulation, and prudently transplant its rules in the process of legislation of Chinese Personal Information Protection Act.

Key words: Digital economy　General Data Protection Regulation　Law on the protection of personal information

[收稿日期]　2018－09－28

[作者简介]　许可，男，1981 年 2 月生，对外经济贸易大学法学院助理教授，研究方向为网络信息法、民商法学。

数字经济正成为中国以及世界经济发展的新动能。通过人均资本、人均劳动产出和全要素生产率的提升，数字经济不但培育了新市场和新产业增长点，更推动了社会的包容性增长和可持续增长。而正如 2016 年 9 月《二十国集团数字经济发展与合作倡议》所指出的，作为新经济的关键生产要素，“数字化的信息”，即数据是数字经济的不竭源泉，数据保护和利用规则成为数字经济的底层架构。透过数字经济的棱镜，2018 年 5 月生效的欧盟《一般数据保护条例》（下称“GDPR”）便显现出别样的意义。立基于此，本文首先揭示 GDPR 背后欧盟的政经考量，进而探寻 GDPR 对数字经济的不利后果，并在此基础上，提出中国的应对之道。

一、GDPR 与欧盟数字经济的愿景

（一）数字经济的落后者

作为继农业经济、工业经济之后的一种新的经济社会发展形态，数字经济早已超出信息产业的藩篱。有鉴于此，无论是发达国家，还是发展中国家，均把数字经济转型视为重大的优先政策。然而，在数字经济的世界版图上，各国的发展并不均衡。中国信通院《G20 国家数字经济发展研究报告（2017）》显示：2016 年，美国数字经济规模达到 10.8 万亿美元，在世界上遥遥领先；中国以 3.4 万亿美元的总量位居第二；日本、德国和英国分列第三至五位，其平均规模约为中国的一半。中美两国在这波数字经济浪潮中的领先地位在科技企业的市值上得到鲜明体现。2017 年，全球市值前十的公司中有七家科技企业，其中，美国五家：苹果、微软、谷歌、Facebook、亚马逊；中国两家：阿里巴巴和腾讯。这一局势在各个细分领域更加显著。联合国《2017 世界投资报告——投资与数字经济》（World Investment Report 2017—Investment and the Digital Economy Report）梳理了网络平台、数字化解决方案、电子商务、数字内容、IT、电信设施等主要数字经济领域，发现全球的领导者或跟随者基本被中美两国的企业占据。

较诸中美，欧洲在数字经济中暂时落后了。2016 年 5 月，欧盟委员会发布《欧洲数字化进展报告 2016》（Europe's Digital Progress Report），指出尽管欧盟各国在移动互联网、电子政务和电子商务领域取得了进步，但欧盟科学、技术和数学（STEM）学科的毕业生人数上升缓慢，只有 16％的中小企业利用网络行销，更有 45％的人口不具备基本的数字技术。该报告进一步指出：欧盟公民和企业在使用在线工具和服务时经常遇到障碍，以至于企业和民众难以从数字转型中获益。欧盟数字经济落后的恶果已经显现：自 2009 年以来，欧盟信息和通信技术产业（ICT）一直处于结构性下滑的状态，当今全球市值最高的 20 家互联网公司也没有一家来自欧盟。

（二）通过制度发展数字经济

事实上，欧盟很早就意识到数字经济的来临。早在 1993 年，欧盟在成立之际就发布了《增长、竞争、就业——迈向 21 世纪的挑战和道路》白皮书，明确指出发展数字经济的重要性，并提出了“创建欧洲信息社会，迎接 21 世纪挑战”的战略。1996 年 3 月，为了激励数据产业的发展，欧盟理事会签署《关于数据库的法律保护的指令》（Directive 96/9/EC on the legal protection of databases），在全球首次赋予不受著作权法保护但又有实质性投资的数据库（database）以特殊权利（sui generis right protection）。然而，

法律本身的模糊性使得人们对其保护范围以及他人正当行为的边界一直充满分歧，[1] 该指令并未让欧盟数据产业蓬勃兴起，甚至到了 2004 年，欧盟数据库的发展已经回落到 1996 年的水平。[2]

面对这一不利局面，欧盟奋起直追。2010 年，欧盟发布《2010 倡议——为了促进增长和就业的欧洲信息社会》（i2010：A European Information Society for Growth and Employment），提出深耕三大重点领域：（1）整合欧盟委员会既有法律，建立一个市场导向的数字经济法律框架；（2）推动数字化的融合以及与私营部门合作，促进欧盟在数字创新技术方面的领导力；（3）提供高效、方便、实用的在线服务，建立包容性的欧洲信息社会。作为数字经济法律的重要一环，2012 年 1 月，欧洲议会公布了 GDPR 草案。该草案预示着个人数据保护水平提升到前所未有的高度，同时意图在欧盟范围内建立更为统一和严格的立法。[3] 草案出台后，4 400 多份修改意见展现出欧盟立法中前所未见的游说博弈，充分反映了 GDPR 早已超越纯粹的个人数据规范，成为深层次融合国际政治博弈、产业经济竞争以及社会文化扩张等诸多元素的复杂综合体。[4]

2015 年，欧盟委员会再次确立欧洲“数字一体化市场”（Digital Single Market）战略，由此统合并大大推进了 GDPR 的制定。该战略旨在为欧盟个人和企业提供更好的数字产品和服务，创造有利于数字网络和服务繁荣发展的环境，以及最大化地实现数字经济的增长潜力。欧盟相信，通过确保货物、人员、服务、资本、数据自由流动，“数字一体化市场”能确保个人和企业均能在公平竞争的条件下无缝访问和在线活动，促进欧盟数字经济发展并确保欧洲在全球数字经济中的地位。该战略指出：数据是整个社会和所有经济部门经济增长、创新及数字化的催化剂，而分散的市场无法为云计算、大数据、数据驱动型科学、物联网在欧洲范围内充分发挥其潜力提供足够的规模保障，为此，欧盟需要消除一系列的技术障碍和法律障碍，[5] GDPR 便是其中最重要的举措之一。故此，倘若只将 GDPR 视为在信息科技迅速发展背景下，欧盟对欧洲公民人格尊严和人格自由的重申，未免小觑了它的意义。

（三）GDPR 推进欧盟数字一体化市场

1. 以数据自由流动为宗旨

GDPR 第 1 条“主旨与目标”开宗明义：“不得以保护自然人个人数据处理为由，限制或禁止个人数据在欧盟的自由流动。”随着数字经济的勃兴，在全球范围内收集、分析和传输个人数据的经济意义与日俱增。2014 年，价值约 30 万亿美元的商品、服务和

---

〔1〕 See Summary report of the public consultation on the evaluation of Directive 96/9/EC on the legal protection of databases, at https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-legal-protection-databases, last visited on Sep. 30, 2018.

〔2〕 See DG Internal Market and Services published the first evaluation of Directive 96/6/EC on the Legal Protection of Databases, at http://ec.europa.eu/internal_market/copyright/prot-databases/index_en.htm#maincontentSec2, last visited on Sep. 30, 2018.

〔3〕 参见王融：《大数据时代数据保护与流动规则》，人民邮电出版社 2017 年版，第 158 页。

〔4〕 参见吴沈括：“欧盟《一般数据保护条例》（GDPR）与中国应对”，《信息安全与通信秘密》2018 年第 2 期，第 13 页。

〔5〕 See Shaping the Digital Single Market, at https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market, last visited on Sep. 30, 2018.

金融发生跨境移转，其中数据流动带来的价值约为 2.8 万亿美元。〔6〕欧洲亦概莫能外。根据波士顿咨询集团的数据，2011 年欧盟公民的数据价值为 3 150 亿欧元，并有可能在 2020 年增长到近 1 万亿欧元。〔7〕然而，由于普遍担心互联网安全、基本权利保障以及数据保护问题，欧洲企业和消费者对于数据自由流动始终缺乏足够的信心。〔8〕为此，GDRP 从如下两方面重塑数字经济的信任，以强化数据的流动性。

一方面，GDPR 提升了数据主体对个人数据的控制力。GDPR 在欧盟 1995 年《关于个人数据保护与自由流动指令（95/46/EC）》（以下简称《95 指令》）基础上，进一步明确提出合法公平透明原则、完整性和保密性原则、特殊数据处理原则，并从处理的合法性、同意的要件、儿童同意等要求进一步缩限了“知情同意原则”。同时，赋予数据主体新的数据权利，如删除其数据的“被遗忘权”、要求其数据从一个控制者向他方直接传输的“可携带权”、免受基于数据画像的自动化决策权利、更加透明的知情权以及更为便利的访问权。

另一方面，GDPR 取消了数据本地化的要求。GDPR 要求各成员国应废除欧盟境内任何数据存储及处理过程中不合理的数据位置限制，不得强制服务提供商在每个地区或国家建立昂贵的本地基础设施（数据中心）。GDPR 与欧盟委员会 2017 年的《关于非个人数据自由流动框架的提案》、2018 年 4 月的《关于修订公共部门信息再利用指令的提案》《修订 2012 年访问和保存科学信息的建议》《基于公共利益由私营部门向公共部门分享数据的指导意见》相辅相成，以期一揽子解决数据可操作性、可使用性以及数据访问问题，打出一套数字自由流动的组合拳。

2. 以规则和执法的统一为依归

与《95 指令》相比，GDPR 大大提升了个人数据保护的法律位阶。从指令向条例的转变，意味着 GDPR 一经发布立即生效，无须经过各成员国以国内法律法规形式的落实措施，并且，无论对于成员国还是当事人（组织或者机构），GDPR 均具备同等法律效力，从而简化和统一了各国错综复杂的既有规则。不仅于此，执行 GDPR 构成欧盟各成员国必须履行的、不可克扣的政治责任。GDPR 特别在涉及多成员国监管的情形下，规定了主导监管机构（Lead Supervisory Authority）的监管权力，通过一致性机制相互合作和协助，最终实现一站式执法。在欧盟层面，欧洲数据保护局（EDPB）将遵循数字一体化市场的总体安排，以保护欧盟公民和统一市场为导向，协调成员国个人数据保护署的执法工作。

个人数据和信任是当今数字经济的货币，GDPR 意图建立一个强大且面向未来的监管框架，以保证消费者和企业增强信心和相互信任，从而为欧洲铺平数字时代的道路。

（四）GDPR 成为面向非欧盟国家的新壁垒

推动欧盟内部市场的一体化并不是 GDPR 的唯一效果，对欧盟外市场参与者来说，

---

〔6〕 See Digital globalization: The new era of global flows, at https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows, last visited on Sep. 30, 2018.

〔7〕 See Ernst-Oliver Wilhelm, The GDPR: Fostering Trust in the Digital Single Market, at https://blog.gft.com/blog/2016/04/05/the-gdpr-fostering-trust-in-the-digital-single-market/, last visited on Sep. 30, 2018.

〔8〕 一份调查显示：三分之二的欧洲人表示他们担心无法控制他们在网上提供的信息，而另一半则担心成为欺诈的受害者。See Special Eurobarometer 431, Data Protection Report, June 2015.

GDPR 更承担着贸易和投资新壁垒的角色。

1. GDPR 为全球个人数据保护竖立新标杆

迄今为止，全球个人数据保护法已经经历了三代。[9] 第一代以经合组织 1980 年《关于隐私保护与个人数据跨境流通指引》（the Guidelines on the Protection of Privacy and Transborder Flow of Personal Data）以及 1981 年欧洲理事会（the Council of Europe）《有关个人数据自动化处理之个人保护公约》为起点，其奠定了现代个人数据保护法的基本框架。第二代以欧盟《95 指令》为代表，其在第一代原则的基础上加入了包括“数据最少够用”“删除”“敏感信息”“独立的个人信息保护机构”等要素。第三代即为 GDPR。与第二代相比，GDPR 大大拓展了数据主体权利，并确立了一系列新型保护制度，如“企业内部设立数据保护官”“经设计和默认的数据保护”“数据保护影响评估”“数据控制者与数据处理者均承担直接侵权责任”“境外数据控制者的代表人”“发生数据安全事件后对数据保护机构的报告和对个人的通知”“数据控制者可展示的问责”“集体诉讼制度”，等等。

截止到 2018 年 6 月，世界已有 126 个国家拥有个人数据保护法。根据上述三代的划分，各国均达到了第一代的标准，目前正向第二代迈进。其中，所有欧盟国家均已完成了转变，在非欧盟的 75 个国家中，大体也行程过半。其中，南非和韩国实现了 90%，阿根廷、哥伦比亚、马来西亚实现了 80%，加拿大、中国台湾地区实现了 70%，澳大利亚、新西兰、中国香港地区实现了 60%，以色列、日本、墨西哥、新加坡实现了 50%，但美中两国均不在这一表单中。[10] 随着 GDPR 的出台，欧盟个人数据保护高地的地位进一步稳固。

2. 作为国际经济新壁垒的 GDPR

所谓国际经济新壁垒，是指包括技术壁垒、绿色壁垒和社会壁垒在内的所有阻碍国际商品、服务、资金、数据自由流动的新型壁垒。[11] GDPR 包含着“同意”“透明度”“自动化决策和数据画像”“数据影响评估”“数据记录”等大量指南、建议和标准，体现出技术壁垒特征；同时，通过宣示《欧洲人权公约》第 8 条、《欧盟基本权利宪章》第 7 条项下的“个人数据获得保护的基本权利”，GDPR 又具有鲜明的社会壁垒特征。[12] GDPR 对跨境经济活动的阻碍集中反映在如下层面：

首先，GDPR 限制了跨境提供货物或服务。根据 GDPR 第 3 条第 2 款，如果欧盟以外的企业为欧盟境内的数据主体无偿或有偿地提供货物或服务，或者对数据主体在欧盟境内的行为进行监控，就落在 GDPR 的长臂管辖之下。更重要的是，在涉及个人特殊数据处理时，企业还应在欧盟境内授权一名“代表”，以履行 GDPR 下所有的义务和责任。

其次，GDPR 限制了数据的跨境流动。根据 GDPR 第五章的规定，欧盟内的个人数据只允许流入欧盟认可的能提供“充分保护”或“适当保障措施”的国家或地区。其

---

〔9〕 See Graham Greenleaf, International data privacy agreements after the GDPR and Schrems, 139 Privacy Laws & Business International Report, 2016.

〔10〕 See Graham Greenleaf, Global Convergence of Data Privacy Standards and Laws, at http://www.ssrn.com/link/UNSW-LEG.html, last visited on Sep. 30, 2018.

〔11〕 参见彭继增：“新贸易壁垒的内容、特点及其对策”，《价格月刊》2005 年第 9 期，第 18 页。

〔12〕 类似地，欧盟同样将中国《网络安全法》视为贸易和投资壁垒，参见“欧委会发布 2017 年度贸易和投资壁垒报告”，载 http://www.mofcom.gov.cn/article/i/jyjl/m/201807/20180702762125.shtml，最后访问时间：2018 年 9 月 30 日。

中，获得欧盟的充分性认定是数据跨境流动的最佳途径，但由于个人数据保护整体水平、数据流动现状，以及与欧盟的政治、贸易关系，秉持的价值观和目标等相关标准过于严苛，对中国在内的大多数国家而言，这近乎是不可能完成的任务。而在所谓“适当保护措施”中，不论是采用有约束力的企业规则、欧盟批准的标准数据保护条款，还是遵守经欧盟认可的第三方认证，其实质均在于通过柔性规则，将 GDPR 的强制性规定扩张适用到欧盟外国家。正因如此，美国商务部长罗斯指出：GDPR 对美国和欧盟以外的所有国家制造不必要的贸易壁垒，导致美国企业丧失数据的访问权，扰乱欧美之间在金融监管、医学研究、应急管理协调以及重要商业方面的合作。〔13〕

最后，GDPR 限制了资金的跨境流动。根据 GDPR 第 3 条第 1 款，只要营业机构/营业场所设在欧盟境内，企业均不得不承担 GDPR 施加的高昂合规成本，而不论其个人数据处理活动是否发生在欧盟境内。这无疑让计划进入欧盟的企业进退维谷。

总之，GDPR 具有双重效果：它一方面试图通过统一的个人数据保护立法和执法，推动欧盟境内数字经济的发展，另一方面通过制度先发优势，搅动欧盟外的全球数字市场。就后者来说，欧盟实际上是利用 GDPR 向中美两国企业和政府开出了一道难以回答的选择题：要么让企业操作规程或国内法与 GDPR 保持一致，要么被 5 亿富有消费者的市场排除在外。

二、GDPR 对数字经济的可能的不利后果

甘瓜苦蒂，物无全美。GDPR 必将产生正反两方面的影响。不过，欧盟鉴于其在数字经济领域的相对落后地位以及数字生产和消费不平衡的市场结构，无须过多顾忌 GDPR 的副作用，但从全球数字经济的宏观视角观察，GDPR 绝非福音。

（一）GDPR 可能戕害创新

企业合规成本的飙升是 GDPR 对数字经济最直观的影响。Paul Hastings 律师事务所调查了 100 家富时 350 指数公司和 100 家世界 500 强企业的总法律顾问和首席安全官，发现富时 350 指数公司平均将为 GDPR 增加 43 万英镑的支出，而世界 500 强企业增加的支出更高达 100 万美元。〔14〕

不过，仅仅是合规成本的增多并不当然损及创新。正如波特假说所洞见的，在考虑市场不完美和竞争者之间策略互动的情形下，基于安全的规制有可能激励企业进行创新补偿，提高企业的利润率，从而实现双赢。〔15〕但更细致的研究表明：因为合规成本的异质性，强化规制对于规模不同的企业有着不同的影响，简言之，规制可以提升合规成本相对较低的大企业的利润率和数量，却降低了合规成本相对较高的小企业的利润率和

〔13〕 参见罗斯：“欧盟数据隐私新规或制造贸易壁垒”，载 http：//www.ftchinese.com/story/001077857？full＝y&archive，最后访问时间：2019 年 9 月 30 日。

〔14〕 See Fortune and FTSE Firms to Spend Millions Gearing up for GDPR Compliance, New Survey Shows, at https：//www.paulhastings.com/news/details/？id＝1c74ed69-2334-6428-811c-ff00004cbded, last visited on Sep. 30, 2018.

〔15〕 See Adam B. Jaffe & Karen Palmer, Environmental Regulation and Innovation：A Panel Data Study, The Review of Economics and Statistics, MIT Press, Vol. 79 (4), 1997, pp. 610～619.

数量。〔16〕

不幸的是，在数字经济中，恰恰小企业才是创新的主体。这是因为，与工业时代的创新大多是改进既有技术、产品或商业模式的“维持性创新”不同，互联网时代的创新大多是打破既有市场结构的“颠覆性创新”。在这一创新过程中，遵循传统轨道的在位大企业往往无法应对动态创新而遭遇失败，最终被新进入的小企业所替代。这一点业已被实证研究所证实。针对高新技术产业的调查表明：企业规模和颠覆性创新的成功负相关。〔17〕因此，在数字经济中，在位大企业能成功地继续保持其行业领先地位的唯一办法，就是成立一个完全独立的组织，并全权授权它使用全新商业模式创建一个全新的企业。

显然，GDPR 中数据控制者、数据处理者周密而细致的义务，对于小企业而言，是难以承受之重。相反，凭借着超大规模，GDPR 对大企业的成本影响有限。不仅如此，随着数据保护标准的提升，用户更可能通过他们熟悉的网络服务提供者或者必不可少的网络平台（例如领先的社交和商业网络），而非新的不熟悉的竞争对手来进行数据处理。如此，GDPR 最终可能会增强现任科技巨头的地位，而不是促进其竞争对手的兴起。事实上，在 GDPR 生效后不久，谷歌成功增加了其在线广告市场的份额，因为它以高于同行的速度获得用户对定向行为广告的明确同意。

事实上，欧盟并非没有意识到 GDPR 对小企业的危害。考虑到小企业缺乏充分的财力、人力来履行 GDPR 规定的书面记录义务，其第 30 条第 5 款对雇员人数少于 250 人的企业或组织，给予了特别豁免。但 GDPR 同时指出，该义务免除有着三种限制：（1）数据处理行为可能给数据主体的权利或自由带来风险。尽管该款在文意上没有说明权利或自由的具体内容，可从立法目的上看，只有处理行为有可能对数据主体的主要权利或实质自由造成侵害时，该款才有适用的余地，从而将较小的风险排除在外。（2）数据处理行为是经常性的。只有临时性和辅助性的数据处理才能豁免，换言之，如果数据处理构成营业的主要部分，则即便是小企业也不得免除书面记录的义务。（3）涉及敏感数据或与刑事定罪或犯罪有关的信息。根据 GDPR 第 9 条第 1 款的规定，“敏感数据”包括种族、民族、政治观点、宗教信仰、哲学信仰、工会成员资格、个人基因数据、生物特征数据、健康数据、性生活/性取向数据。鉴于敏感数据和犯罪数据一旦泄露就会给数据主体造成威胁，因此与该等数据相关的处理，不论方式如何均不得豁免。不过，根据 GDPR 第 9 条第 2 款的规定，企业为雇佣目的，对员工健康数据的处理不在此限。

综合上述限制情形，不难发现，因为 GDPR 表述的模糊性，小企业将面临非常不确定的执法，由此它们可能不得不费时费力，像大企业一样保留数据，这削弱了小微企业豁免的立法功能。GDPR 对小企业的损害后果已显。2018 年 5 月底，几家小型美国公司和科技创业公司已退出欧盟市场，以免与监管相冲突并影响其存续。

（二）GDPR 可能伤及互联网成熟业态

2013 年 12 月，为评估 GDPR 对数字经济的影响，著名会计师事务所德勤对英国、法国和德国的 750 家企业和 6 000 名消费者进行了访谈，针对数据收集和处理的四大数据产业，即直销、行为定向广告、网页分析和信用信息进行了深入分析，发现 GDPR 将直接或间接地导致 1 730 亿欧元的 GDP 损失以及 280 万人的就业损失。这是仅限于欧盟之内的数

〔16〕 参见龙小宁、万威：“环境规制、企业利润率与合规成本规模异质性”，《中国工业经济》2017 年第 6 期，第 171 页。

〔17〕 See C. Markides, Disruptive Innovation: In Need of Better Theory, The Journal of Product Innovation Management, 23, No. 1, 2006, pp. 19～25.

据，考虑到 GDPR 的跨境管辖和数据的跨境管控，这一数字肯定会进一步放大。[18]

1. 直销产业（Direct Marketing）

直销是指通过信件、电话和电子邮件等多种方式向选定的潜在用户直接进行商业推广的广告活动，系典型的数据密集型产业。由于成本低、效率高，对于小企业和立足利基市场的创新性产品而言，直销是非常重要的销售渠道。仅在 2012 年，欧盟的直销产业就高达 470 亿欧元。随着 GDPR 的到来，只有在用户主动、明确、具体地授权企业使用其个人数据之时，直销才能开展，这大大改变了之前的数据“选择退出”（opt-out）机制。但调查发现：一旦转为明示授权，人们的决定就非常谨慎，只有 40％左右的人同意企业利用直接收集的数据直销，而同意利用间接收集数据直销的更是不足 20％，显然，这将大幅影响直销获取客户（acquisition）、维系客户（retention）和交叉行销（cross-selling）的范围和效率，从而进一步影响直销行业的收入、直销使用企业的投资回报率和消费者福利。据估计，上述损失分别是 330 亿欧元、280 亿欧元和 240 亿欧元，合并计算即 850 亿欧元，130 万人的就业也受到影响。

2.“行为定向广告”行业（online behavioral advertising）

行为定向广告是指通过深入观察网站用户的行为，利用网页特性，准确地把握用户的特征，根据其行为特征反映出用户需求，再根据用户的需求与偏好，针对性地投放广告。行为定向广告和互联网普遍免费服务相结合，构成了互联网最主流的经营模式，人们将之戏称为“羊毛出在狗身上”。以谷歌 2017 年第四季度财报为例，行为定向广告依旧是其最赚钱的业务，收入达 272.7 亿美元，占了总收入的 84％。更有甚者，世界最大社交网站 Facebook 的广告收入占其总收入的比例高达 98％。为了让广告投放精准高效，互联网企业必须遵循几千年来的一贯技巧——“了解你的客户”（Know your customer）。幸运的是，凭借着日新月异的信息技术，要完成这一工作，互联网公司不再需要费时费力的人际交流，通过代码和软件收集、分析尽可能多的用户信息便已足够。但在 GDPR 下，用户的 IP 地址、Cookies 和设备 ID 等个人数据的处理变得非常困难，利用用户画像的成本上升，由此欧盟遭受 42 亿欧元的 GDP 损失并减少 6 600 个工作岗位。

3. 网页分析行业（web analytics）

网页分析是指通过收集和分析网页访问者的访问数据以及电子邮件回应率、销售与客户资料、使用者效能资料等基础数据，以帮助企业满足客户的访问期待。通过网页分析，客户能够获得更贴心的线上体验，便利其浏览信息、网站导航和电子交易。该行业在欧盟发展迅速，2012 年至 2014 年，其收入就由 8 000 万欧元增长到 1.1 亿欧元。为了不影响用户使用，网页分析所使用的数据搜集技术（如“网页埋点”）大多是嵌入式和隐蔽性的，这使其难以满足 GDPR 的要求。据测算，GDPR 将降低网页分析及其相关行业 8.8 亿欧元的收入，同时影响 1.4 万人的就业。

4. 信用信息行业（credit information）

如果信用制度是金融的基础设施，信用信息就是金融的血液。在欧盟，信用调查机构（credit reference agency）信息收集的来源非常广泛，既包括负面信息也包括正面信息，既来自金融机构，也来自公共机构和日常零售商。GDPR 不但增加了相关信息收集、使用和分享的成本，更重要的是，用户的删除权可能导致信用评分失真。德勤的调

〔18〕 See Deloitte, Economic impact Assessment of the Proposed European General Data Protection Regulation.

查显示：之前有过拒绝贷款记录的消费者中，有 60％有意愿删除个人数据，而没有被拒绝历史的消费者中，只有 20％打算删除。经济学研究早已发现，个人数据权利的提升与信用的有效利用并不兼容。以金融隐私指数（Financial Privacy Index）为指标，美国的个人数据保护弱于欧盟，但美国的信贷获取比例高于欧盟各国。〔19〕

无独有偶，就个人信息共享是否需要明示同意这一议题，美国加州各地采取了不同的规定，基于这一政策差异的经济学分析表明：在需要用户明示同意才能共享信息的情形下，贷款违约率都上升了。〔20〕个人数据权利和信用功能的此长彼消，给金融机构、小企业和普通消费者均带来不利后果。金融机构风控能力下降导致其面临更高的信用风险，因此更不倾向于向小企业放贷，而消费者获得房屋、汽车等消费贷款的几率亦随之下降。综合来看，GDPR 将令消费信贷下降 19％，拖累 GDP 增速 0.65 个百分点，相当于造成每年 830 亿欧元的损失并引发 140 万人失业。

（三）GDPR 可能阻碍新兴产业的发展

众所周知，信息技术的 ABC——人工智能（AI）、区块链（Blackchain）和云计算（Cloud Computing）——将塑造数字经济的未来，然而，GDPR 对此却缺乏远见，无法回应其挑战。

1. 人工智能

2018 年年初，《终极算法》作者、人工智能著名学者、华盛顿大学教授 Pedro Domingos 在社交网络中写道：“自 5 月 25 日起，欧盟将会要求所有算法解释其输出原理，这意味着深度学习成为非法的方式。”这并非空穴来风。针对算法向数据主体作出的自动化决定，GDPR 予以明确规制。其第 13 条（f）和第 14 条（g）规定，如果个人数据将用于自动化决定，那么至少应当向个人提供相关决定的重要性、对个人预期的影响以及有关运算逻辑的“有用信息”。比如，在银行收集个人数据时，应当告知其可能使用人工智能对贷款人资质进行审核，而审核的最坏结果（如不批贷）也应一并披露。并且，根据 GDPR 第 22 条的规定，如果个人对自动化决定不满，则有权主张人工介入，以表达自己的观点并提出质疑。

上述两个条款的结合，产生了针对人工智能的所谓“解释权”，而这正是 Pedro Domingos 的担忧所在。虽然有学者认为这一说法系对 GDPR 的误读，但根据 WP29 指南的要求，一旦用户提出质疑，数据控制者必须确保关于该决定的审查是有意义的。审查必须由有授权和有能力改变决定的人执行。鉴于算法模型越复杂，就越需要投入更多的时间和专家开展人工审查，这些成本必将最终影响对 AI 的投资。〔21〕

2. 区块链

区块链的分布式、匿名性、不可篡改性等典型特性与 GDPR 的规定存在先天抵牾。一方面，区块链的去中心架构使得识别数据控制者非常困难。倘若将参与多点记账和多方共识的所有节点都视为控制者，那么令每个节点均承担同等且严苛的数据控制者义务是不现实的；更严重的是，这意味着只要在欧盟境内存在任一节点，全球化的公共链

〔19〕 See N. Jentzsch, The Regulation of Financial Privacy: The United States vs Europe, ECRI Research Report No. 5, European Credit Research Institute (Brussels, 2003).

〔20〕 See Jin-Hyuk Kim and Liad Wagman, Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis, The RAND Journal of Economics 46 (1), 2015, pp. 2～22.

〔21〕 See Nick Wallace and Daniel Castro, The Impact of the EU's New Data Protection Regulation on AI, at http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf, last visited on Sep. 30, 2018.

（如比特币或以太坊）就全部落入 GDPR 的管辖下，这显然是荒谬的。另一方面，除非以超过全系统一半以上的算力改写，计入区块链的信息将被永久储存，从而与 GDPR 赋予个人的更正权、删除权、被遗忘权直接冲突。总之，GDPR 这一以数据控制者和数据处理者为对象的中心化规制思路与去中心化的区块链格格不入，〔22〕只有 GDPR 在具体场景下作出适当的妥协，才能与之兼容。

3．云计算

云计算是现代企业运营的一个组成部分，因为它通过降低成本提升了小企业竞争优势，根据国际数据公司（IDC）的预测，到 2020 年，超过 80％的新兴企业将使用云作为平台。但 GDPR 将对这一产业造成严重影响。首先，GDPR 对作为数据处理者的云服务商（CSP）施加了与数据控制者几乎同等的义务和责任，例如设定数据保护官、数据泄露报告义务、数据可携带权，等等，即便 CSP 在欧盟境外亦是如此。其次，GDPR 不当介入到云计算客户与 CSP 的合同关系中，限制了双方的经营自由。质言之，由于 GDPR 明确要求数据控制者对数据处理者的事前授权，目前常见的云服务集成、转售业态都将面临业务风险，因为控制者（云客户）随时可以行使反对权。〔23〕最后，GDPR 默认的数据控制者与处理者二元主体划分不能涵盖云计算中多样化的业务角色，CSP 的地位在 IaaS（基础设施即服务）、PaaS（平台即服务）、SaaS（软件即服务）的不同场景中各有差异，难以统一适用 GDPR。〔24〕

三、GDPR 的中国应对之道

（一）积极化解我国法律与 GDPR 的冲突

考虑到 GDPR 对于欧盟的重大意义，其后续执法力度和持续影响不可轻忽。2 000 万欧元或者企业上一年度全球营业收入的 4％的重罚与长臂管辖相结合，构成了针对中国企业的真实威吓。因此，中国政府和企业应对 GDPR 保持高度关注，尤其要避免因法律冲突将中国企业陷入困境。

1．数据主体权利的法律限制问题

GDPR 允许国家通过立法限制数据主体和数据控制者权利，但根据其 23 条“限制条款”的规定，该等限制有着严格条件。

一是实质要件，即相关法律应符合基本权利和自由的本质，且是民主社会应采取的必要的适当的措施，以维护（a）国家安全；（b）防卫；（c）公共安全；（d）刑事犯罪的预防、调查、侦查、起诉或者刑事处罚的执行，包括对公共安全威胁的防范和预防；（e）一般公共利益的其他重要目标，包括经济或财政利益、公共卫生或社会保障；（f）司法独立与司法程序的保护；（g）违反职业道德规范的预防、调查、侦查和起诉；（h）监督、检查或相关的监管职能；（i）对数据主体或其他人的权利与自由的保护；（j）民事请求权的执行。

---

〔22〕 See Michèle Finck，Blockchains and Data Protection in the European Union，Max Planck Institute for Innovation and Competition Research Paper No. 18－01.

〔23〕 参见王融：“《欧盟数据保护通用条例》：十个误解与争议”，载 http：//www.sohu.com/a/229319518_455313，最后访问时间：2018 年 9 月 30 日。

〔24〕 See Sohail Razi Khan，Luis Borges Gouvia，The implication and challenges of GDPR's on Cloud Computing Industry，International Journal of Computer Science，Volume 5，Issue 7，2017，pp. 106～110.

二是形式要件，即任何立法措施均应至少包括如下方面的具体措施：（a）处理的目的或处理的类别；（b）个人数据的分类；（c）限制的范围；（d）防止滥用或非法使用或传输的保障措施；（e）控制者具体情况或控制者类型；（f）存储期限和适用的保障措施，且需要考虑性质、范围和处理的目的或分类；（g）对数据主体权利和自由产生的风险；（h）数据主体被告知限制的权利。

GDPR 的上述规定，是基于“数据权利是一项基本权利”这一共识。早在 2007 年 12 月，欧盟议会、欧盟委员会就颁布了旨在保障欧盟公民权利的《欧盟基本权利宪章》，其第 8 条将“个人数据受保护的权利”明确列入基本的自由权中。2016 年，《欧盟数字基本权利宪章》（Charter of Digital Fundamental Rights of the European Union）进一步细化了数据权利的内涵。作为一项基本权利，对数据权利的限制必须以高位阶规范——法律方可作出。

但在中国，尽管《民法总则》第 111 条规定了“个人信息应受法律保护”，但其权利性质仍无定论。在实践中，一方面通过行政法规、部门规章，甚至规范性文件限制数据权利的情形不胜枚举，另一方面，即使通过法律加以限制，也大多缺乏形式要件。以向政府报送个人数据的法律为例，尽管《网络安全法》第 28 条、《电子商务法》第 27 条均有明文，但并未规定防止滥用或非法使用或传输的保障措施、存储期限和适用的保障措施、对数据主体权利和自由产生的风险以及数据主体被告知限制的权利。因此，在企业遵守中国法律、法规、规章、规范性文件而降低个人数据的保护标准或违反其对数据主体的承诺，将难以使用 GDPR 第 23 条作为责任免除或减轻的抗辩理由。

有鉴于此，针对数据报送问题，我国宜及时立法，合理确定数据报送范围，确立报送数据的合法性原则、比例原则、保密性原则、正当程序原则以及相关法定程序，进一步明确政府相关部门的数据保护义务与责任。

2．数据本地化存储的问题

我国对数据本地化存储的规定主要见于《网络安全法》第 37 条，该条规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”此外，国务院 2013 年的《征信业管理条例》、卫计委 2014 年的《人口健康信息管理办法（试行）》、中国人民银行 2011 年的《关于银行业金融机构做好个人金融信息保护工作的通知》、国家新闻出版广电总局和工业和信息化部 2016 年的《网络出版服务管理规定》、交通运输部等部委联合发布于 2016 年的《网络预约出租汽车经营服务管理暂行办法》等，都对数据本地化提出了明确要求。根据上述规定，相关数据的存储、处理、访问都必须在境内进行。

我国数据本地化的要求与 GDPR 的监管要求存在冲突。GDPR 第 58 条“权力”条款赋予了欧盟各监管机构普遍的调查权力，特别是：命令数据控制者和处理者提供监管机构执行任务所需的任何信息；以数据保护审计的方式开展调查；获得所有个人数据的访问路径以及执行任务所必要的信息；获得控制者和处理者任何资产的访问路径，包括任何数据处理设备和处理方法。一旦欧盟监管机构向相关中国企业发出上述命令，则中国企业不得不陷入要么违反我国数据本地化规定，要么违反欧盟监管机构要求的两难。

3．跨境传输限制的问题

由于我国在短期内难以达到欧盟“充分性认定”的要求，GDRP 对数据跨境传输的

限制不可避免地与我国对中国企业及其数据的管辖权发生冲突。对此，GDPR 第 48 条“未被欧盟法律授权的传输或披露”明确规定：“根据第三国法庭或审理委员会的判决和行政机构的决定，要求控制者或处理者传输或披露个人数据的，当且仅当提出要求的第三国与欧盟或成员国存在有效的国际条约且不影响本章规定的其他传输依据时，判决和决定才可以被承认或执行。”

为此，我国政府宜积极与欧盟委员会以及欧洲各层级数据保护机构进行双边谈判和磋商，推动形成多样化的数据跨境流动方案，通过国际条约协定，尽快实现数据合理有序的跨境传输。

4. 数据存储期限的问题

GDPR 第 5 条“与个人数据处理相关的原则”中（e）规定：“允许以数据主体可识别的形式保存数据的时间不得超过数据处理目的之必要。”这一被称为“存储期限必要最短”（storage limitation）的原则与 GDPR 第 17 条“删除权（被遗忘权）”相结合，构成了数据控制者对数据存储的期限要求。然而，由于中国法律、法规、规章对数据存储期限的强制性要求，个人数据可能被超过处理目的的长期存储，或者无法毫不迟延地回应数据主体删除数据的主张。例如，《电子商务法》第 31 条规定：“……商品和服务信息、交易信息保存时间自交易完成之日起不少于三年……”《征信业管理条例》第 16 条规定：“征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为 5 年；超过 5 年的，应当予以删除。……”《网络预约出租汽车经营服务管理暂行办法》第 27 条规定：“网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年……”

面对这一问题，我国宜及时进行法规清理，提升法律位阶，立足于公共利益，在坚持保存期限“必要最短”的前提下，统一规定个人数据保存期限。同时，仅在例外情形下，才恰当、合理地设定特殊保存期限。

（二）审慎借鉴 GDPR 规则

当前我国正处于制定《个人信息保护法》的关键时期，如何平衡数字经济发展和个人信息权利之间的关系，是其首要定位问题。作为全球个人数据保护的引领者，GDPR 不但有着丰富详尽的规则指引，还占据了人格尊严和人格自由的价值制高点，成为多国竞相效仿的对象。但是，正如本文所揭示的，我们必须直抵其本质，发掘其内在的逻辑理路，权衡得失利弊，探索我国自己的发展道路。

我们应首先认识到：GDPR 在个人数据保护与数字经济间的平衡远非成功。GDPR 前言第 2 条将“加强欧盟内部市场经济体融合”和“增进自然人福祉”作为其双重目标，前言第 4 条进一步规定：“个人数据受保护的权利并非绝对权利；还必须考虑其社会功用，并依据比例原则与其他基本权利保持平衡”，这与前述 GDPR 正文第 1 条下“个人数据保护”与“数据自由流动”的宗旨宣示相呼应，然而，GDPR 具体规则的设计却显著倒向前者，双重目标显著失衡了。〔25〕

这首先是因为数据权利条款是明确和可执行的，而例外条款是模糊和不确定的。〔26〕其次，从法理上看，实因欧盟对个人数据权利设定多基于大陆法系绝对权的进路，其固

〔25〕 参见方禹：“GDPR 前言强调个人信息保护与自由流动的平衡”，载 https://new.qq.com/omn/20180620/20180620A146VO.html，最后访问时间：2018 年 9 月 30 日。

〔26〕 例如，GDPR 第 6 条规定了六种数据处理合法性基础，但除了“数据主体同意”外，其他如“公共利益”“数据控制者正当利益”等尚不存在明确的指引。

然引入了风险概念，但并没有根据数字经济业态和企业不同场景，进行因地制宜地公法调整，从而与美国个人数据保护形成鲜明对照。2012 年的美国《消费者隐私权利法案》以“透明度”“尊重场景”“集中收集与有责利用”“安全维护”“责任界定”为核心，并规定由业界根据此纲领性内容制定实施细则予以细化。〔27〕亦如人们广泛比较欧盟和美国个人数据法律后所言：诸如目的限定、存储期限必要最短等保护规则，美国同样存在，但更为缓和与富有弹性。〔28〕而在欧盟整齐划一执法的同时，就可能引发过分规制或规制不足的问题，甚至造成杀鸡用牛刀、得不偿失的结果。最后，在更深的层次上，GDRP 的这一失衡，未尝不是为了服务于欧盟保护本地企业，压制数字经济先发国家的隐藏企图。

我们还应认识到：在个人信息保护和数字经济之间，不可能有完美的中间点，而只有动态均衡一途。然则，如何取舍？要言之，我们应“执其两端，用其中于民”，这里的“民”就是坚持经济发展以满足人们对美好生活向往的大方向。在我国经济长期处在新常态的背景下，数字经济已经成为重要的增长点和就业渠道。〔29〕尽管我国数字经济的成就为世人瞩目，但正如麦肯锡《数字中国：为经济带来全球竞争力》的报告所表明，美国的数字化水平仍比我国高出 4.9 倍，我们还有很长的路要走。正因如此，在坚持个人数据保护底线的前提下，适当促进数字经济增长才是当下我国制度选择的“中道”。

结　语

2018 年 4 月 20 日到 21 日，在全国网络安全和信息化工作会议上。习近平总书记强调指出，要发展数字经济，加快推动数字产业化，依靠信息技术创新驱动，不断催生新产业新业态新模式，用新动能推动新发展。可以预见，在未来很长时期内，数字经济依然是我国的优位目标。我们应洞察 GDPR 的经济实质和对数字产业的不利影响，立足中国问题、坚持中国立场，在我国未来制定《个人信息保护法》时应审慎借鉴相关规则，作出符合我国长远利益的制度设计。

参考文献

［1］王融．大数据时代数据保护与流动规则［M］．北京：人民邮电出版社，2017.

［2］吴沈括．欧盟《一般数据保护条例》（GDPR）与中国应对［J］．信息安全与通信秘密，2018（2）.

（责任编辑：刘　权　赵建蕊）

〔27〕 See Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online, at https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights, last visited on Sep. 30, 2018.

〔28〕 See LIBE Committee, A Comparison between US and EU Data Protection Legislation for Law Enforcement, at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf, last visited on Sep. 30, 2018.

〔29〕 2018 年 9 月，发改委出台《关于发展数字经济稳定并扩大就业的指导意见》，要求以大力发展数字经济促进就业为主线，不断拓展就业创业新空间，着力实现更高质量和更充分就业。