国际法研究

后“Schrems II 案”时期欧盟数据跨境流动法律监管的演进及我国的因应

杨　帆

内容提要：“Schrems II 案”对以隐私权和数据保护为核心构建的欧盟数据跨境流动规则体系产生重大影响，它要求无论使用何种数据跨境流动工具，都必须确保第三国能够提供与欧盟同等的保护水平。在该案的影响下，《欧盟基本权利宪章》在数据保护领域的地位进一步提高，保障措施的适用愈发严苛，欧洲数据保护委员会在数据保护领域将扮演更重要的角色，数据跨境流动欧盟法规则与国际贸易法的不兼容问题日益凸显。欧盟虽然结合 Schrems II 案的判决完善了对数据跨境的法律监管，但依然没有减少外界对其监管合理性的质疑。我国对数据跨境流动的监管存在着配套立法不健全、规则可操作性差、多元价值失衡、缺乏内外联动的“中国方案”等问题。对此，应完善我国相关立法，加强中欧国际合作，共同引领构建数据跨境流动的国际规则。

关键词：Schrems II 案　数据跨境流动　“充分性”认定　数据安全　个人信息保护法

杨帆，浙江理工大学法政学院讲师。

2020 年 7 月 16 日，欧盟法院在“Schrems II 案”中认为美国的监控立法违反了《欧盟基本权利宪章》（*The Charter of Fundamental Rights of the European Union*，下称“《宪章》”），也没有为欧盟个人提供有效的司法救济，因此欧美之间的“隐私盾”协议无效。另外，就目前广泛使用的数据保护标准合同条款（SCCs）的合法性问题，欧盟法院认为其继续有效，但需结合具体情况采取额外补充措施；在使用标准合同条款等保障措施进行数据传输时，也需确保提供了“与欧盟同等的保护水平”，否则数据保护机构（DPA）可以暂停或终止相关数据传输。〔1〕 Schrems II 案的判决结果并不出人意料，体现了欧盟法院过去几年强烈支持数据保护的立场。〔2〕 国内企业在运营过程中势必面临欧盟数据跨境流动监管

〔1〕 See Schrems II, Case C-311/18.

〔2〕 See Case C-698/15, Tele2 Sverige and Watson and Others; Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement.

带来的风险,在后 Schrems II 案时期,需要追踪欧盟立法、准确识别数据跨境流动可能面临的监管风险,提前做好预案。我国目前已经基于《网络安全法》《数据安全法》《个人信息保护法》等法律法规构筑起了以数据和信息安全为核心的数据跨境流动监管体系,未来可借鉴欧盟数据跨境流动监管模式所提供的经验和教训。鉴于中欧均在国际经贸领域享有一定话语权,双方在数字贸易规则制定领域必将是合作与竞争共存。

一 “Schrems II 案”对欧盟数据跨境流动法律监管的影响

欧盟将《宪章》作为衡量标准,以充分性认定为工具,通过独立数据保护机构的内部执法以及国际层面的积极推广,构建了一套较为成熟、完善且相互协调的数据跨境流动规则体系。下文将从标准、工具、机构以及国际影响四个层面分析 Schrems II 案的影响。

(一)标准层面:《宪章》的地位进一步增强

基于《宪章》的“基本权利测试”不仅可以用来审查欧盟次级立法的合法性,甚至国际协定、外国国内法确立的数据保护水平也要以《宪章》为准。欧盟法院对“Digital Rights Ireland 案”“EU-Canada PNR 案”等案的判决反映了欧盟宪法价值的至高地位,即使面临恐怖主义威胁,欧盟机构也并非全部认为国家安全利益高于个人基本权利。国家安全立法一般被认为是各国主权的保留事项,世贸组织(WTO)协定中的安全例外被认为是“自裁条款”,以避免这类立法被争端解决机制审查。[3] 但在欧盟法院看来,其不仅可以对影响数据保护的国家安全立法进行审查,而且依据的是欧盟的标准。[4]

首先,《宪章》构成界定“充分保护水平”的基准。欧盟法院在适用欧盟《一般数据保护条例》(*General Data Protection Regulation*)时,通过《宪章》确定了适用于第三国的“充分保护水平”的宪法内涵。[5] 为符合该要求,第三国的数据立法或其他法律必须体现对隐私权和数据权的强力保护,当第三国实施的法律措施会对这两项权利造成干涉或影响时,需要结合《宪章》第 52 条对该措施进行“必要性测试”,该测试要求对《宪章》第 7 条和第 8 条的干涉必须由法律规定,并限于《宪章》第 52(1)条规定的严格必要的情况,以及保证根据《宪章》第 47 条对欧盟个人数据主体提供有效司法保护。就“严格必要”而言,欧盟法院要求第三国的立法措施必须明确界定数据的使用范围、数据的使用目的、目的与措施之间存在客观联系等。[6] 要达到有效的司法保护,不能仅仅建立一个新的行政机构以受理来自欧盟数据执法机构的请求,而是要赋予欧盟数据主体可执行的诉讼的权利。

---

〔3〕 See Roger P. Alford, The Self-Judging WTO Security Exception, *Utah Law Review* 697, 697 – 759 (2011).

〔4〕 See Kristina Irion, Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law, https://europeanlawblog.eu/,最近访问时间[2021 – 08 – 16]。

〔5〕 See Digital Rights Ireland case, Joined Cases C-293/12 and C-594/12.

〔6〕 See EDPS, Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit, https://edps.europa.eu/sites/edp/files/publication/17 – 04 – 11_necessity_toolkit_en_0.pdf; EDPS, Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data, https://edps.europa.eu/sites/default/files/publication/19 – 12 – 19_edps_proportionality_guidelines2_en.pdf,最近访问时间[2021 – 08 – 16]。

其次,《宪章》确立了更高的个人基本权利保护标准。一方面,《宪章》在司法保护领域的标准比成员国标准更高。在 Schrems II 案中,法院认为美国政府机构出于国家安全目的留存并获取欧盟公民个人数据的行为构成对公民基本权利的侵犯,美国只有在为其提供司法救济的情况下才会被认为符合《宪章》对有效司法保护的要求。实际上,尽管《欧洲人权公约》(*The European Convention on Human Rights*)要求无论本国人还是外国人都有权在缔约国就国家机关侵犯隐私权的行为获得司法救济,但多数欧盟国家在其国家安全机关的权力运行方面依然奉行同美国类似的逻辑,即对电子监控的国内目标和外国目标提供不同的司法保护。〔7〕 另一方面,对出于国家安全目的大规模获取个人数据的行为,欧盟《一般数据保护条例》和《宪章》的要求高于《欧洲人权公约》。欧洲人权法院关于电子监控的判例法赋予了国家安全机关自由裁量权,比如其在"Big Brother Watch 案"中确认,出于国家安全考虑,其尊重国家机关批量拦截个人数据的活动,实施这种监控活动是否与其目的相称将留给成员国自行判断。〔8〕 而《宪章》坚持严格必要原则。

欧盟的上述做法实际上将其内部标准强加给了第三国,虽然一定程度上促进了数据保护标准的统一,但也被一些学者认为构成了"法律殖民主义"。〔9〕 此外,根据 Schrems II 案判决,数据输出方与输入方也须结合《宪章》的规定评估第三国立法对输入数据的保护水平(下文详述),《宪章》适用范围的扩张进一步加强了欧盟的宪法秩序。

(二)工具层面:适用于具体场景时的不确定性增加

Schrems II 案之前,欧盟旨在塑造以充分性认定制度为主的数据跨境流动模式。然而由于过于严苛和繁琐的认证程序,迄今为止仅日本、加拿大等 12 个国家获得欧盟的充分性认定,即使《关于个人数据自动化处理的个人保护公约》(*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*)的 55 个缔约国也很难获得充分性认定。实际上,条件过于严苛的充分性认定制度已对国际数字贸易产生严重影响,有学者认为其已构成数字贸易壁垒。〔10〕 这使得自"Schrems I 案"开始,越来越多的跨国互联网公司就开始使用标准合同条款进行数据跨境传输。而在 Schrems II 案中,法院认为与欧盟法律"基本同等保护水平"的标准适用于标准合同条款等保障措施,放弃了充分性认定制度和保障措施之间的等级划分,更强化此种趋势。

但同时,Schrems II 案增加了各类保障措施适用的不确定性。一方面,尽管标准合同条款作为一种向欧盟以外传输个人数据的机制仍然有效,但需要数据输出方和输入方对每项数据传输进行逐一评估,在适当情况下需要提供补充保障措施以确保数据在第三国

〔7〕 See Kristina Irion, Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law, https://europeanlawblog.eu/,最近访问时间[2021-08-16]。

〔8〕 Big Brother Watch and Others v. the United Kingdom, Application nos. 58170/13, 62322/14 and 24960/15 (ECtHR May 25, 2021).

〔9〕 See Jan Xavier Dhont, Schrems II The EU Adequacy Regime in Existential Crisis, 26 *Maastricht Journal of European and Comparative Law* 597, 598 (2019).

〔10〕 See Elisabeth Meddin, The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services, 35 *American University International Law Review* 997, 997-1036 (2020); 田晓萍:《贸易壁垒视角下的欧盟〈一般数据保护条例〉》,《政法论丛》2019 年第 4 期,第 123 页。

得到与欧盟同等的保护水平。对于使用标准合同条款的双方而言,他们需要承担评估第三国法律体系是否提供“充分保护水平”的义务,如果通过补充措施也无法提供充分保护,那么标准合同条款将无法使用;为提供补充保障措施,标准合同条款的使用者将承担更高的经济成本。另一方面,约束性企业规则(BCRs)及其他保障措施的未来也存在不确定性。约束性企业规则为解决向政府机构披露数据而提供的具体保护措施,以及在获得批准之前进行的深度审查,使其可能成为未来最可靠的数据传输机制。然而,约束性企业规则的适用也至少面临两个障碍:其一,约束性企业规则的谈判和实施可能需要数年时间,而且内容特别繁重,因此仅由具有广泛数据传输义务的大公司使用。其二,约束性企业规则将遇到与标准合同条款相同的困难,欧洲数据保护委员会(EDPB)在隐私盾协议被判无效后的相关问答中指出“法院对使用标准合同条款设定的门槛也适用于根据《一般数据保护条例》第 46 条用于将数据从欧洲经济区转移到任何第三国的所有适当保障措施”。[11] 即使使用约束性企业规则进行数据跨境传输也需要确保第三国提供与欧盟同等的保护水平。就行为准则和认证机制而言,作为数据跨境传输的法律工具,其尚未在《一般数据保护条例》下获得批准,但作为潜在的前进方向似乎值得研究。

通过克减机制也无法改善这一状况。欧洲数据保护委员会多次声明,《一般数据保护条例》第 49 条规定的“克减机制”并不能被用于“常规”“系统”或“持续”的数据跨境传输活动,必须对克减规则进行严格解释,避免这一例外情形成为一般规则。即使是那些未明确限于“偶尔”或“非重复”数据跨境传输的克减措施,也必须以与减损本质上不矛盾的方式解释。[12] 这一立场在某种程度上关闭了试图利用《一般数据保护条例》第 49 条克减机制取代基于该条例第 45、46 或 47 条进行的系统性数据跨境传输的大门。虽然目前越来越多的公司设法基于用户的“明确同意”进行数据跨境传输,但其前提是公司通知用户他们的数据将被传输到一个没有提供充分保护水平的国家。用户此时将处于两难境地,即要么同意数据的传输,要么放弃使用特定的服务。

(三)机构层面:监管的能力和责任存在失衡

根据 Schrems II 案的裁决,数据输出方和输入方、成员国数据保护机构均承担起评估第三国立法及保障措施是否能够确保“充分保护水平”的职责。然而,对数据输出方和输入方而言,评估第三国立法是否可以达到与欧盟同等的保护水平是一项十分艰巨的任务。一方面,由于涉及评价第三国是否尊重民主、法治、人权等敏感问题,私人主体进行的评估很容易激怒作为评估对象的第三国,潜在的政治风险不利于商业经营。另一方面,私人主体也没有能力对第三国的法律制度,哪怕是仅仅对与其传输数据有关的法律制度进行充分性评估,因为需要评估的法律无论如何都要包括第三国涉及电子监控等国家安全方面的措施,外界通常难以理解和评价这类措施。数据保护机构监督和控制数据输出方和输入方对“充分保护水平”的认定也不具有可行性。两个 Schrems 案表明,即使对于拥有庞

〔11〕 关于 EDPB 对该案的相关看法,参见 https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqonecjeuc31118_en.pdf,最近访问时间[2021-08-16]。

〔12〕 See EDPB, Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf,最近访问时间[2021-08-16]。

大技术专长的官僚和高水平律师团队的欧盟委员会而言,也无法准确认定第三国立法的保护水平;欧洲人权法院往往也需要数年时间才能对监控案件作出判决,更何况已经有其他繁重任务、人手严重不足且对国家安全立法缺乏专业能力的数据保护机构。评估主体的"能力赤字",使得"充分保护水平"的评估呈碎片化趋势。

欧洲数据保护委员会的监管权能也需进一步澄清。不同成员国的数据保护机构就同一第三国的法律制度进行充分性评估,可能得出不同的评估结论。在 Schrems II 案第 147 段中,法院提出了一项解决方案,即如果不同成员国保护机构对数据传输存在异议,欧洲数据保护委员会负有责任解决此类纠纷。有学者认为该方案将会使欧洲数据保护委员会取代欧盟委员会,成为"全球立法充分保护水平的全能评估者"。[13] 欧洲数据保护委员会在充分性评估领域承担更重要的角色有助于协调地方数据保护机构的工作,但是也存在以下问题:第一,私人主体和成员国数据保护机构对外国国家安全立法进行"碎片化"评估时所面临的困难在这里依然存在。欧洲数据保护委员会固然比单个数据跨境流动参与者拥有更多的专业知识,但欧洲人权法院的经验表明,这项任务非常困难且耗时耗力。第二,需澄清欧洲数据保护委员会的决定与欧盟委员会充分性认定之间的联系。欧盟与美国刚达成隐私盾协议时,欧洲数据保护委员会就对该协议以及美国法律体系是否满足"充分保护水平"表达过担忧,[14] 当时欧洲数据保护委员会只是表达观点,不会影响谈判结果。但是 Schrems II 案之后,欧洲数据保护委员会也有权在未作出充分性认定的情况下评估外国法律的保护水平,发表具有法律约束力的意见。在谈判结束前宣布第三国法律不符合欧盟标准,将阻碍欧盟对其他国家作出充分性认定;如果欧洲数据保护委员会已经认定第三国的法律制度可以确保与欧盟同等的保护水平,这会对欧盟委员会的工作产生何种影响依然有待解决。第三,欧洲数据保护委员会的评估结果也要受到法院的审查,问题是当欧洲数据保护委员会和欧盟委员会都认为第三国提供了充分保护水平时,如果其中一方的充分性决定被法院认定为无效,会对另一方产生何种效果?如果数据输出方不认可数据保护机构的评估结果并提起诉讼,在诉讼过程中,欧洲数据保护委员会否决或认可了数据保护机构的评估结果,会对成员国法院或欧盟法院产生何种影响?

(四)国际层面:与国际贸易规则的不兼容加剧

1. 重新在欧盟引发数据本地化问题

虽然 Schrems II 案没有提出数据本地化的法律要求,但其对数据跨境流向美国和其他国家构成的阻碍,也会迫使许多企业选择数据本地化措施。然而,数据本地化措施之前在欧盟一直存在争议:一方面,《一般数据保护条例》指出个人数据的自由流动对国际贸易具有重要意义,数据本地化措施使跨国经营的公司产生了更高的成本,构成对外国服务

〔13〕 See Theodore Christakis, After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe (21 JULY 2020), https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/,最近访问时间[2021-08-16]。

〔14〕 See EDPS, Opinion on the EU-U.S. Privacy Shield Draft Adequacy Decision, https://edps.europa.eu/sites/default/files/publication/16-05-30_privacy_shield_en.pdf,最近访问时间[2021-08-16]。

提供者的歧视性待遇;另一方面,欧盟数据跨境流动监管制度的逻辑是确保流向第三国的数据能够在当地得到与欧盟同样的保护水平。但越来越多的观点认为,数据本地化措施无法有效保护数据安全。[15] 另外,不同国家数据保护的立法水平和技术水平存在参差,数据本地化存储会导致在保护水平较低的国家存储的数据成为重点攻击对象。

2. 欧盟的监管措施与世贸组织一般例外的要求不符

世贸组织承认维护“公共道德”“公共秩序”等价值对于成员国的重要意义,允许相关国家援引“一般例外原则”为违反世贸组织其他条款的国内措施“免责”。作为例外条款,其在适用时必须满足各种条件和限制,尤其是“必要性测试”,确保争议措施不超过实现目标所必要的贸易限制程度。而《宪章》规定了严格必要原则,以评估影响基本人权的措施是否超过措施为实现其他目标所需的程度。两个“必要性测试”在适用中会产生冲突。

第一,从世贸组织法的角度来看,即使按照最宽松的标准适用必要性测试,欧盟对个人数据跨境传输的限制也不满足这一条件。世贸组织争端解决机构在大多数情况下都是根据“是否存在合理可用的贸易限制较少的替代方案”来认定措施是否符合必要性原则,与“比例性测试”相比,这是一个更宽松的认定方法。[16] 世贸组织争端解决机构可能认为欧盟数据流动框架并不是对贸易限制最少的,尤其考虑到第三国企业适用欧盟数据跨境流动工具的前提是在欧盟设立机构或商业伙伴。其他限制较少的选项,例如《亚太经合组织隐私框架》(*APEC Privacy Framework*)等,对欧盟而言都是“合理可用的替代方案”。另外,欧盟数据传输框架对符合条件的任何个人数据适用相同的限制措施,且不根据个人基本权利受到干涉风险的严重程度校准限制性措施,都可以证明欧盟可以“合理利用”其他更精细、总体贸易限制更少的法律框架。在 Schrems II 案之前,欧盟可以辩称除了充分性认定制度,《一般数据保护条例》还规定了标准合同条款、约束性企业规则等保障措施作为数据跨境流动工具,这些保障措施对贸易的限制更少,可以作为合格的替代措施。但是 Schrems II 案之后,在适用任何保障措施之前,都需要对第三国的立法进行充分性评估,甚至在一定情况下还需要采取补充措施,这导致不同数据跨境流动工具在贸易限制方面逐渐趋同。

第二,从欧盟法的角度来看,遵守世贸组织一般例外或执行争端解决机构(DSB)作出的裁决都可能构成对个人权利保护标准的减损,需要适用《宪章》第 52 条第 1 款规定的必要性测试以评估这种减损是否可行。近几年,在 Tele2 Sverige 案、EU-Canada PNR 案等案中,欧盟法院将《宪章》规定的必要性测试提升到了“严格必要”的水平。而《亚太经合组织隐私框架》等数据隐私保护规则本身没有法律约束力,实践中根本无法约束第三国公共机构获取个人数据的行为;从内容上看,这些规则没有就外国公共机构在何种情况下可以访问个人数据以及访问的程度作出明确且准确的规定,也没有建立独立的数据监督机构和有效的司法补救机制。正如有学者所言,《亚太经合组织隐私框架》的实质是通过构建较低保护水平的个人数据跨境流动秩序,确保参与的国家不会以“自身国内提供了

〔15〕 See Anupam Chander, Is Data Localization a Solution for Schrems II, 23 *Journal of International Economic Law* 1, 1 – 14 (2020).

〔16〕 See Donald H Regan, The Meaning of “Necessary” in GATT Article XX and GATS Article XIV: The Myth of Cost-Benefit Balancing, 6 *World Trade Review* 347, 347 – 369 (2007).

高水平保护”为由限制数据跨境流动,由此实现数据向美国或美国企业的汇聚。[17] 因此所谓的“替代措施”无法满足欧盟法所要求的“严格必要”标准。

3. 欧盟监管措施无法满足现有高水平数字贸易协定的要求

目前,高水平数字贸易协定都承认缔约国对数据跨境流动享有监管权,允许各国为实现合理的公共政策目标维持和采取一些与数据自由流动不符的措施,同时为这类措施设置了需要满足的条件。比如,《全面与进步跨太平洋伙伴关系协定》(*Comprehensive and Progressive Agreement for Trans-Pacific Partnership*,CPTPP)第 14.11 条第 3 款规定,“本条的任何规定均不得阻止一方采取或维持不一致的措施,以实现合理的公共政策目标,前提是该措施:(1)不构成任意或不合理的歧视或变相的贸易限制;且(2)对信息传输施加的限制不超过实现目标所需限度。”目前,学界就“公共政策目标”的内涵和外延、它与适用于整个协定的一般例外和安全例外的关系如何等问题尚未有定论,但就如何具体适用该条款,国内外学者形成了较为一致性的观点,即可以参考世贸组织一般例外条款适用,对于(1)项所针对措施的适用方式,可以参考《关税及贸易总协定》(GATT)第 20 条和《服务贸易总协定》(GATS)第 14 条的前言性规定;对(2)项的适用偏重于对措施的实体性要求,即所采取的措施是实现特定目标所必需的,且满足比例原则,为此可以结合世贸组织相关规则的法理进行“必要性测试”。[18] 《全面与进步跨太平洋伙伴关系协定》要求(1)项和(2)项规定须同时满足,其实是《关税及贸易总协定》、世贸组织例外规则法理中两步测试法的体现,既注重对措施的实体考察,也关注对措施的适用要求。[19] 如果一项措施援引“公共政策目标”条款失败,那么也很难满足一般例外的要求,反之亦然。[20]

二 欧盟数据跨境流动法律监管的新发展

(一)澄清补充措施的实施步骤和内容

欧洲数据保护委员会在 2021 年 6 月通过了《对数据跨境转移工具补充措施的建议 2.0》,[21] 其规定补充措施的实施可以分为四步:第一步,了解数据传输的情况。比如数据的去向,转移的数据必须是充分的、相关的且仅限于与目的有关的必要数据。第二步,验证所

〔17〕 参见熊鸿儒、田杰棠:《突出重围:数据跨境流动规则的“中国方案”》,《人民论坛·学术前沿》2021 年第 Z1 期,第 56 页。

〔18〕 关于 CPTPP 是否监管以及如何监管数据本地化措施的研究,参见 Abe Yoshinori, Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures, 16 *Public Policy Review* 1, 1-28 (2021);米切尔和米什拉认为 GATS 一般例外是 CPTPP 中公共政策目标例外的基础,CPTPP 中关于数据传输和数据本地化的例外可能不会像预期那样给各国的监管措施提供更大的灵活性,see A. D. Mitchell and N. Mishra, Data at the Docks: Modernizing International Trade Law for the Digital Economy, 20 *Vanderbilt Journal of Entertainment and Technology Law* 1073, 1073-1134 (2018).

〔19〕 参见洪延青:《数据竞争的美欧战略立场及中国因应——基于国内立法与经贸协定谈判双重视角》,《国际法研究》2021 年第 6 期,第 69 页。

〔20〕 参见马光:《FTA 数据跨境流动监管的三种例外选择适用》,《政法论坛》2021 年第 5 期,第 15 页。

〔21〕 See EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance With the EU Level of Protection of Personal Data, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en,最近访问时间[2021-08-16]。

适用的数据跨境流动工具。第三步,评估第三国的法律或实践中是否有任何因素可能会影响所依赖的数据跨境流动工具的有效性,其中第三国的监控立法是重要的评估对象。第四步,确定并采取必要的补充措施,使得数据在第三国得到与其在欧盟同等的保护水平。只有在第三国的立法会影响到依据《一般数据保护条例》第 46 条采取的数据跨境流动工具的有效性时,才有必要采取补充措施。这里的补充措施主要包括:技术措施,比如数据的匿名化处理;额外的合同措施,比如使用特定技术的义务;组织措施,比如数据治理的内部政策。

(二)基于 Schrems II 案的要求更新标准合同条款模板

欧盟委员会 2021 年 6 月 4 日通过了最新版的标准合同条款,它将取代原跨境传输标准合同条款。[22] 最新版跨境传输标准合同条款项下划分了数据控制者至数据控制者、数据控制者至数据处理者、数据处理者至数据控制者以及数据处理者至数据处理者之间的数据传输,采用“一般条款 + 模块化”的创新结构设计,可以实现一套规则适用于不同情境的数据传输。[23] 新版标准合同条款最大的改变在于体现了 Schrems II 案的判决。它要求数据跨境传输各方应保证其有理由相信数据接收方所在国的法律和实践不会阻碍其履行该标准合同条款下的义务,各方在作出上述保证时应综合评估考量数据传输的具体情况、相关已实施的补充性合同、技术或组织保障措施等。对于公共机构访问个人数据的要求,标准合同条款规定数据接收方在可能的情况下应及时将这类请求通知数据传输方。同时数据接收方应对公共机构提出的要求进行合法性评估,并且在允许范围内提供最少数据。

(三)明确第三国监控措施所应满足的欧盟法标准

欧洲数据保护委员会在 2020 年 11 月 10 日制定了《关于欧洲监督措施基本保障的建议》,其目的是帮助审查允许第三国的公共机构(国家安全机构或执法机构)访问个人数据的监控措施是否可以被视为合理的干预。[24] 首先,对个人数据的处理应“出于特定目的,并基于当事人的同意或法律规定的一些其他合法依据”。对基本权利的限制应基于明确且准确的规则,规定有关措施的适用范围和情景、最低限度的保障措施等。其次,需要证明监控措施的必要性和相称性。就相称性而言,对隐私权和数据保护权的限制是否合理的问题必须进行评估,比如衡量这种限制所带来的干扰的严重性,以及限制措施所追求的公共利益目标的重要性。就必要性而言,监控措施必须特别指出何时及何种条件下可以采取处理这些数据的措施,从而确保干预仅限于严格必要的情况。如果没有根据所追求的目标对访问数据作任何区分、限制或例外,也没有制定客观标准来确定公共机构获取和使用数据所带来的干扰是出于合理的目,将违反必要原则。再者,第三国立法需要建立独立的监督机制,对监控权力进行有效制衡。最后,第三国立法需要确保向受监控措施影响的欧盟个人提供有效的补救措施。这里的补救机关不一定是司法机关,但必须确保

〔22〕 See Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

〔23〕 参见陈际红等:《欧盟个人数据传输的两项新工具:历史演变、法律影响和应对策略》,https://www.pkulaw.com/lawfirmarticles/ecb930c8bf32c28e23ca18336675e1b3bdfb.html,最近访问时间[2022 - 01 - 07]。

〔24〕 See EDPB, Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, https://edpb.europa.eu/our - work - tools/our - documents/recommendations/recommendations - 022020 - european - essential - guarantees_en,最近访问时间[2021 - 08 - 16]。

它的独立性以及作出的决定对监控部门有法律约束力。

（四）推动在国际贸易立法层面赋予欧盟更大的监管自主权

由于欧盟数据跨境流动制度与世贸组织协定以及现有双边贸易协定中的非歧视原则存在不兼容风险，且无法通过“一般例外条款”证明其合法性，欧盟开始努力构建欧式数字贸易协定模板，以保障其在数字贸易领域的监管自主权。这主要体现在：第一，作为预防措施，《欧盟运行条约》（*Treaty on the Functioning of the European Union*）允许欧盟成员国及欧盟机构就拟议的国际协议与欧盟条约（包括《宪章》）的兼容性向欧洲法院征求意见。这一机制在“欧盟加拿大 PNR 协定案”中被使用。[25] 第二，欧盟 2018 年在其数字贸易章节提出了数据跨境流动示范条款，其中隐私和数据保护的具体例外情况参考了世贸组织协定中“国家安全例外”的立法模式，赋予国家自裁的权利。[26] 欧盟已将这些示范条款纳入其目前与澳大利亚、新西兰等国的贸易谈判提案中。[27] 由于示范条款中的例外极为特定，对欧盟的贸易伙伴来说，根据这些拟议的具体条款挑战欧盟的监管措施将更加困难。第三，因数据跨境流动、个人数据保护和隐私保护问题产生的争议不适用争端解决机制，避免国际争端解决机制对欧盟法规则的解释和适用，保留欧盟法律监管的自主权。

三　欧盟数据跨境流动法律监管的合理性考量

欧盟的数据保护理念在世界范围内迅速传播，许多国家和地区都以《一般数据保护条例》为借鉴蓝本制定了相关立法。然而，欧盟的数据跨境流动监管模式是建立在其长期奉行高水平人权保护和完善的司法审查制度之上，在产业竞争力不足的背景下构建的防御式监管模式。我国在借鉴时应注意该欧盟模式存在的问题，在此基础上扬长避短。

第一，欧盟对数据跨境流动的监管过于强调保护个人权利，忽视了多元价值的协调。数据的跨境流动不仅涉及对个人隐私和数据权的保护，还影响到数字经济发展和国家安全，需要在多元价值之间选择平衡点，以达到合理的保护数据安全与实现数据自由流动的协调发展。[28] 欧盟比美国等国家更加注重数字领域的监管，并把严格的监管视为欧盟的竞争优势，但是过于严格的监管必然不利于新兴数字产业的发展。[29] 欧盟法院在 Schrems II 案的裁决中认为，国家机关出于国家安全、打击犯罪的考虑可以获取个人数据，但对此进行了非常严格的限制，以至于第三国的监控立法或侦查立法很难通过欧盟的审查。欧盟实质上将个人权利保护凌驾于经济发展和国家安全之上。

第二，欧盟对“充分保护水平”的认定存在较大主观性且政治色彩浓厚。Schrems II

〔25〕 See Christopher Kuner, International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15, 55 *Common Market Law Review* 857, 858 (2018).

〔26〕 See EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf，最近访问时间[2021 - 08 - 16]。

〔27〕 参见周念利：《数字贸易规则“欧式模板”的典型特征及发展趋向》，《国际经贸探索》2018 年第 3 期，第 96 页。

〔28〕 参见杨署东、谢卓君：《跨境数据流动贸易规制之例外条款：定位、范式与反思》，《重庆大学学报（社会科学版）》2021 年。

〔29〕 参见朱贵昌：《欧盟数字化发展面临诸多挑战》，《人民论坛》2020 年第 19 期，第 122 页。

案后,“充分保护水平”是贯穿欧盟数据跨境流动法律监管的重要概念,可以结合《宪章》和《一般数据保护条例》第45条第2款规定的三个因素考虑。其中,第一个因素要求考虑第三国的“法治、人权和自由状况”“有关国家安全和公共安全领域的立法”以及“有效的司法和行政救济”。仔细分析这些要求可以发现,由于缺乏具有可操作性的具体标准,它们涵盖的范围非常广泛,相关概念不仅具有政治敏感性,而且内容开放,缺乏普遍意义。有关公共安全、国防、国家安全和刑事犯罪的相关立法以及公共机构对个人数据的获取毫无疑问属于国家主权问题,对第三国的这些立法进行审查势必引起政治争议。[30] 我国应当避免为通过欧盟“充分保护水平”的认定,而接受不合理的要价。

第三,欧盟未对跨境的数据进行分类,而是采取“一刀切”的监管方式。《一般数据保护条例》第9条规定了个人敏感数据的特殊处理规则,但该条例的数据跨境流动章节并没有对数据类型进行区分,而是一般性的适用于所有个人数据。结合世贸组织一般例外条款中的“必要性测试”,同样的数据跨境流动监管措施不加区分地适用于个人敏感数据和非个人敏感数据,很难认定该措施是所欲实现的政策目标之所需。为此,必须在数据跨境监管领域落实个人数据分类分级制度。

第四,对主权国家实施公共政策的权力进行了严格限制,欧式数字贸易协定的接受度较低。为维护在个人数据和隐私保护领域所奉行的高标准,欧盟在世贸组织数字贸易谈判文本中专门约定“各成员可采取并维持其认为适当的保障措施,以确保对个人数据和隐私的保护”。与《全面与进步跨太平洋伙伴关系协定》《区域全面经济伙伴关系协定》(*Regional Comprehensive Economic Partnership*,RCEP)相比,缔约国在欧式数字贸易协定中只能以保护隐私和个人数据为由对数据跨境流动进行限制,而不能出于实现“合理公共政策目标”实施其他的监管措施,很显然限制了主权国家的监管空间。[31] 尽管欧盟正在与多个国家谈判缔结国际贸易协定,但相较美式和亚太数字贸易协定,欧式数字贸易协定的影响力还有待提升。

第五,欧盟的监管要求与我国法律制度存在冲突。欧盟对数据跨境流动进行有效监管的前提是欧盟法院能够结合《宪章》对行政机关的决定进行合宪性审查,通过审查结果促进监管制度的完善。对于违宪审查制度不发达的国家而言,照搬欧盟监管制度将会出现水土不服的现象。虽然我国以数据安全为核心构建的数据跨境流动规则在个人信息保护方面同欧盟存在一定契合,但二者的价值取向依然存在差异,尤其是国家安全事项构成中欧双方在数据跨境监管方面的重大分歧。以数据加密措施为例,欧洲数据保护委员会发布的指南将加密视为一种有效的补充措施,密钥由欧洲境内数据传输方掌握。根据我国《密码法》的规定,除非是大众消费类产品所采用的商用密码,否则需要根据商用密码进出口许可程序提交商用密码的技术说明,数据输出方和输入方在使用加密措施向中国传输数据时需要提交中国密码管理部门审批,这与欧盟的监管要求存在冲突。

---

〔30〕 See Jan Xavier Dhont, Schrems II The EU Adequacy Regime in Existential Crisis, 26 *Maastricht Journal of European and Comparative Law* 598, 597 – 601 (2019).

〔31〕 参见洪延青:《数据竞争的美欧战略立场及中国因应——基于国内立法与经贸协定谈判双重视角》,《国际法研究》2021年第6期,第77页。

四 欧盟监管经验对完善我国数据跨境流动监管制度的启示

（一）当前数据跨境流动法律监管存在的问题

我国目前已经基于《网络安全法》《数据安全法》以及《个人信息保护法》初步构建起以安全为核心价值的数据跨境流动监管制度。然而具体到规则层面，仍存在以下问题。

1. 出境安全评估制度有待健全

《网络安全法》第 37 条首次确立了“本地化存储 + 出境安全评估”制度，构成了我国数据跨境流动监管的基础，但关键信息基础设施运营者（CIIO）的具体范围没有明确界定。2021 年 8 月国务院颁布的《关键信息基础设施安全保护条例》，通过非穷尽列举和抽象概括的方式界定了关键信息基础设施的范围，导致涵盖的设施和系统非常广泛，缺乏可预测性。至于“出境安全评估”，《网络安全法》没有制定评估标准和评估程序，而是交给网信部门和国务院有关部门制定评估办法。网信部门先后发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》《个人信息出境安全评估办法（征求意见稿）》《数据出境安全评估办法（征求意见稿）》，前两份征求意见稿最终没有出台，后一版本依然处于征求意见阶段。三份征求意见稿在安全评估对象上都指向个人信息和重要数据，与《网络安全法》《个人信息保护法》的规定相一致，不包括非重要数据和非个人信息。然而，2021 年网信办发布的《网络数据安全管理条例（征求意见稿）》第 35 条规定，数据处理者向境外提供数据的，应通过国家网信部门组织的数据出境安全评估，但该条例并未将需要出境安全评估的数据局限于个人信息和重要数据，还可能包括非重要数据和非个人信息，因此需要协调法律和行政法规的规定，确定哪些数据在向境外提供时应当进行出境安全评估。如果非重要数据和非个人信息不适用出境安全评估，那么应当尽快制定适用于这类数据的出境办法。就进行安全评估的义务主体而言，《网络安全法》规定的是关键信息基础设施运营者，《个人信息保护法》规定的是关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，上述三个“评估办法”将义务主体扩大到所有的网络运营者或数据处理者，这表明向境外提供个人信息变得更加严格。

2. 其他信息出境措施和“个人的单独同意”要求有待澄清

我国《个人信息保护法》第 38 条规定了数据跨境流动的方式，除了安全评估机制，还可以通过个人信息保护认证、标准合同以及其他方式进行。不过，具体到实施层面，尚未建立起配套的法律法规。标准合同借鉴了欧盟的标准合同条款，由于国家网信部门组织的安全评估过于严格，标准合同未来可能成为向境外提供个人信息的重要方式，因此应当尽快制定合同细则。第 39 条规定了个人单独同意制度，与欧盟、日本等国家和地区个人信息保护法不同，其并非独立的为境外提供个人信息的方式，而是必须同第 38 条规定的安全评估制度、标准合同、个人信息保护认证结合使用，从而构成对境外提供个人信息的双重限制。这将会严重阻碍个人数据的跨境流动，加重我国境内企业的合规压力。

3. 数据自由流动和个人权利保护有待加强和完善

数据跨境流动涉及数字经济发展、个人基本权利保护、国家安全等多元价值，对它的

监管需平衡不同价值间的关系。在充分保证数据安全的前提下,应进一步促进数据自由流动和加强个人信息保护。2021 年《数据出境安全评估办法(征求意见稿)》第 4 条规定了应当进行出境安全评估的情形,包括处理个人信息达到一百万人的个人信息处理者向境外提供个人信息、累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息等情形。考虑到我国数十亿计的网民数量,这里设置的出境安全评估门槛实际上是偏低的。2021 年 9 月发布的《重要数据识别指南(征求意见稿)》规定了促进数据流动的基本原则,明确重要数据安全有序流动,非重要的一般数据依法自由流动;但从具体内容来看,重要数据的涵盖范围过于宽泛,且对“安全有序”“依法自由流动”缺少更细化说明。这些因素将导致安全评估活动的泛滥,阻碍安全评估制度的高效运行。另外,我国“个人单独同意”要求会进一步对数据跨境自由流动造成限制。

《个人信息保护法》第 38 条与《一般数据保护条例》第 46 关于保障措施的规定类似,要求境内外个人信息处理者必须采取措施提供数据输出国所要求的保护水平,但在实践中将面临诸多问题。首先,对“个人信息保护标准”缺乏明确界定;欧盟界定“充分性保护水平”的标准尽管存在主观性和政治色彩,但《一般数据保护条例》毕竟明确规定了几个评估因素。其次,没有界定个人信息处理者应当采取的“必要措施”的内容,对企业而言缺乏可操作性。再次,结合其他相关立法分析,我国个人信息保护标准并不高。《个人信息保护法》的出台极大提高了我国个人信息保护的水平,但是在安全领域,侦查机关获取个人数据的权力普遍缺乏有效限制。比如,《数据安全法》第 35 条规定了在数据调取方面配合公安机关侦查犯罪的义务。由于电子数据往往承载公民通信自由权、财产权、隐私权等基本权利,披露这些数据将构成对个人基本权利的干涉,为此应对侦查机关电子数据调取权的条件设置契合侦查比例原则,同时为个人提供行政或司法救济。[32] 然而本条唯一限制条件是可能在实践中被扩大解释的“严格的批准手续”。最后,《个人信息保护法》在个人信息保护的机构设置上并没有较大突破,只是笼统地规定了“履行个人信息保护职责的部门”,依然缺乏独立的个人信息保护机构。

4.“中国方案”仍有待提出

欧盟数据跨境流动法律监管的内外联动是通过两套互相配合的机制实现的:第一套机制是欧盟的充分性认定制度,让潜在第三国接受与欧盟同等的数据保护标准,从而实现《一般数据保护条例》和《宪章》所确立标准的全球化;[33] 第二套机制是缔结欧式数字贸易协定,将其隐私权和数据保护标准与国际贸易挂钩,赋予欧盟充分的监管空间。我国目前很难实现国内法和国际法的内外联动:其一,由于数据跨境安全评估制度过于严苛、配套法律制度不健全、个人数据权利保护水平不高等内在原因,迄今未在国内建立起完善的数据跨境流动法律标准;其二,与欧盟要求第三国立法应当达到“充分保护水平”不同,《个人信息保护法》第 38 条关于境外接收方应满足我国数据保护标准的规定主要针对个人、企业等非国家实体,而非主权国家;其三,我国在数字贸易领域的地位和话语权严重不

〔32〕 参见谢登科:《论侦查机关电子数据调取权及其程序控制——以〈数据安全法(草案)〉第 32 条为视角》,《环球法律评论》2021 年第 1 期,第 66 页。

〔33〕 参见汤霞:《数据安全与开放之间:数字贸易国际规则构建的中国方案》,《政治与法律》2021 年第 12 期,第 29 页。

匹配。欧美利用自身贸易优势及先进的立法技术,相继推出了反映各自国内数字经济政策的贸易协定范本;而我国由于受到本国数据跨境流动严格监管的掣肘,只能被动接受《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》(*Digital Economy Partnership Agreement*,DEPA)等高水平数字贸易协定所确立的标准。

(二)我国数据跨境流动法律监管的完善路径

1. 国内层面

第一,应当首先完善数据出境安全评估,尽快出台配套立法,以构建我国数据跨境流动监管的核心制度。比如加快完善数据分级分类管理机制,进一步细化适用安全评估机制的关键基础设施及重要数据类型;出台《数据出境安全评估办法》,确立安全评估原则、明确需要评估的具体情形、重点评估的对象、细化评估流程;明确适用数据出境安全评估的数据类型,制定非重要且非个人信息的出境办法。考虑到国家网信部门在安全评估方面承担着巨大压力,可以考虑建立专门的安全评估机构。

第二,标准合同未来可能成为在我国进行数据跨境传输的重要工具,可以参考欧盟的标准合同条款制定标准合同模板,采纳欧盟"政府预先批准+市场主体自主适用"治理模式。[34] 欧盟的标准合同条款是建立在其以个人权利保护为核心的数据跨境监管模式之上,我国在拟定具体条款时应围绕数据安全等我国注重的价值目标,兼顾《个人信息保护法》《数据安全法》等法律中有关保护个人权利的规定,避免对欧盟实践生搬硬套。

第三,加强企业向政府报送个人数据的程序规范性,进一步明确国内现行法律法规中涉及"公民、组织配合协助义务"条款的法律适用范围、法定正当程序和司法协助例外情形。[35] 我国立法对企业施加了广泛的个人数据报送义务,比如交通运输部《网络预约出租汽车监管信息交互平台运行管理办法》要求,网约车平台公司应向部级平台传输驾驶员相关许可信息、订单信息、经营信息、定位信息、服务质量信息等运营数据。这些规定没有基于措施的目的对需要报送的个人数据的范围进行限制,经常使用"……等运营数据""与……有关的信息"等模糊表述,与《个人信息保护法》有关个人数据处理的基本原则不符。对于涉及政府获得个人数据的立法,必须明确立法的目的,精确界定个人数据的范围,对于个人权利的干扰必须符合比例性和必要性原则。

第四,在特定行业或地区建立数据跨境流动试点,实施限制更少的监管措施,积累高水平数据跨境监管经验,补充我国现行数据跨境流动机制。我国目前已经在特定行业领域和地区建立了数据跨境流动试验区,比如上海市、浙江省、海南省的相关实践。[36] 通过试点,可在完善安全保障机制、建立数据保护能力认证机制、部署国际互联网数据专用通道、推进与特定地区信息互通或特定类型数据跨境传输等方面积累丰硕经验。

---

〔34〕 参见王轶、张浩、唐琦:《欧盟标准合同对我国完善数据安全监管机制的启示》,《中国计算机报》2021 年 11 月 29 日第 14 版。

〔35〕 参见熊鸿儒、田杰棠:《突出重围:数据跨境流动规则的"中国方案"》,《人民论坛·学术前沿》2021 年第 Z1 期,第 56 页。

〔36〕 参见郑磊:《健全完善我国跨境数据流动规则体系,助推数字贸易发展水平迈上新台阶》,http://www.cinn.cn/gyrj/202103/t20210309_239488.shtml,最近访问时间[2021-08-16]。

2. 中欧合作层面

中欧同为全球重要的数字贸易市场，任何一方想要在数字经济领域有所突破必须要重视对方。同时，中欧都面临着美式数字贸易范本在全球扩张给各自数据跨境监管带来的挑战。由是观之，中欧数据跨境流动监管合作具有坚实基础。

第一，根据《一般数据保护条例》第 45 条第 1 款，欧盟委员会“充分性”认定的适用对象可以是国家，也可以是第三国境内的地区、一个或多个特定行业、国际组织。理论上来讲，在一国无法获得欧盟充分性认定的情况下，如果该国的某一地区存在综合性的数据保护法案、设置了独立的数据保护机构、能够有效限制政府访问个人数据、阻止数据被继续传输到该国的其他地区等，则该地区依然可能被授予充分性认定。〔37〕 不过，这种理论的可能性在实践中可能困难重重。对我国而言，虽然目前已经建立了诸多数据跨境流动试点，实施更严格的数据保护执法，但是这些特定地区依然处于《国家安全法》《网络安全法》等法律的管辖之下，区域内的企业和个人依然有遵守国家安全、协助打击犯罪的义务。

第二，中国与欧盟的法律都允许直接通过国际协定进行数据跨境传输（《个人信息保护法》第 38 条、《一般数据保护条例》第 50 条）。目前，许多没有获得欧盟充分性认定的国家都与欧盟签署了特定行业或领域的数据传输协议，比如 2021 年欧盟委员会和土耳其药品和医疗器械局之间达成个人数据传输行政安排，实现医疗器械数据的跨境传输；该协议详细列举了个人数据保护的保障措施，比如处理目的、数据质量和相称性、透明度等。与充分性决定相比，第三国更容易满足这些条件。〔38〕 这不仅对我国开展数据跨境流动试点有重要意义，而且有助于实现中欧在数据跨境领域的监管合作。

第三，在数字贸易国际立法领域进行合作，联手应对美式数据跨境流动国际规则的冲击。美国出于维护本国互联网巨头在全世界的经济利益，一直主张数据自由流动原则，这集中体现在以《美墨加协定》（*United States-Mexico-Canada Agreement*，USMCA）、《全面与进步跨太平洋伙伴关系协定》为代表的美式数字贸易协定中。这类协定允许各国出于保护个人信息、隐私权等“合理的公共政策目标”对数据跨境流动进行限制，不过限制措施需要满足类似世贸组织规定的严格的“必要性测试”。为此，欧盟通过欧式数字贸易协定、我国通过《区域全面经济伙伴关系协定》分别设计了一套与美式规则不同的数据跨境流动国际规则，赋予了缔约方自主决定何为“合法公共政策”的权能，相比《美墨加协定》《全面与进步跨太平洋伙伴关系协定》，更加尊重各个缔约方的规制自由。不过，《区域全面经济伙伴关系协定》除了“公共政策目标”例外，还规定了“基本安全利益”例外，给我国留下了足够的监管空间。考虑到欧式数字贸易协定没有类似的规定，未来中欧进行数字贸易立法国际合作时应当重视数据安全领域的监管合作。

［本文为作者主持的 2021 年度浙江省哲学社会科学规划课题“后疫情时期欧盟主导的国际投资争端解决机制改革及对我国的影响”（21NDQN238YB）的研究成果。］

〔37〕 参见单文华、邓娜：《欧美跨境数据流动规制：冲突、协调与借鉴》，《西安交通大学学报（社会科学版）》2021 年第 5 期，第 101 页。

〔38〕 See *Administrative Arrangement between the European Commission and the Turkish Medicines and Medical Devices Agency in the Context of the Turkish Participation in the EU Regulatory System for Medical Devices Eudamed*.

［**Abstract**］ The Schrems II case has a significant impact on the EU's cross-border data flow legal system, which is built with privacy and data protection as its core and requires that whatever cross-border data flow instrument is used, it must ensure that the third country can provide the level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU by virtue of GDPR read in the light of the Charter of Fundamental Rights of the EU. Under the influence of the Schrems II case, the status of the Charter in the field of data protection has been further enhanced, and the EU intends to make it a global standard. The application of appropriate safeguards has become more stringent, and supplementary measures requested by CJEU will increase the compliance costs of entities operating outside the region; EDPB will play a bigger role in data protection but needs to coordinate its functions with the EU Commission; and the incompatibility between EU law on cross-border data flow and international trade law has become increasingly prominent and the EU is in urgent need of more space for the operation of its regulatory power. In light of the Schrems II judgment, the EU has published a new version of Standard Contract Clauses, clarified the additional supplementary measures, made more specific the standards to be met by third country surveillance legislation, and promoted the EU's digital trade model agreement. However, doubts on the rationality of EU's regulation model have not been alleviated, especially considering that problems such as the imbalance of multiple values, highly political overtones, and lack of classification of cross-border data remain unresolved. On the basis of the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, China has now built a preliminary regulatory system for cross-border data flow with security as the core value. But the regulation of cross-border data flow in China still has many problems, such as imperfect supporting legislation, poor operability of rules, imbalance between multiple values, and lack of internal and external legal linkage. On the premise of fully guaranteeing data security, the free flow of data and the protection of personal information should be further promoted. To solve these problems, on the one hand, China should improve the security assessment system of data exit and establish the data classification and gradation management mechanism on the basis of absorbing the EU's regulatory experience that is reasonable and suitable for its own national conditions and improve the protection level of the individual's basic rights. On the other hand, confronted with common opportunities and challenges, China and the EU may strengthen international cooperation in many ways, for example, realizing the free flow of data in specific fields through international agreements, and jointly shaping the connotation of important concepts such as "reasonable public policy objectives" and "essential security interests" in digital trade agreements.

（责任编辑：余佳楠）