第一章

“个人信息保护”何以关联“国际数字经济规则建构”？

本书的分析，以“国际数字经济规则建构”中的个人信息保护问题为中心。对此问题的分析，始于对一系列问题的回答：首先，“数字经济”作为“规则建构”的经济基础，如何影响了个人信息保护问题？数字经济语境下的个人信息保护，较于传统经济模式有何异同？其次，“国际数字经济规则建构”会在哪些领域与个人信息保护问题产生关联？在“数字经济”语境下将此问题纳入考量，较于“二战”以来的国际经济规则建构有何异同？最后，国际数字经济规则建构中的个人信息保护问题，本质上究竟反映了何种国家间利益之争？毕竟，从理论上讲，任何非经贸议题均可能与国家间经贸关系产生关联，但并非任何议题均可能通过“议程设置”程序、进入国际社会的关注范畴，乃至于国际规则的形成范畴。[1] 然而，下文对于国际数字经济规则的分析还将表明，在贸易、投资、标准设定、市场治理等多个层面，个人信息保护问题却切切实实地进入了认知议程设置乃至于规范议程设置，不仅使公众切实认识到此议题的重要意义，而且成功实现了国际规则的确立。

以上三方面问题，分别从经济基础、法律现状、政治根源三方面切入个人信息保护在国际数字经济规则建构中的重要意义；而对以上三方面问题的一一回应，也将是本章三节分别关注的内容。

第一节　逻辑起点：个人信息保护与数字经济存在关联

本节分析的问题，将构成对于“国际经贸规则构建中个人信息保护”问题研究的基础：为何在数字经济语境下，个人信息保护会作为一个“问题”

〔1〕 韦宗友 . 国际议程设置：一种初步分析框架 [J]. 世界经济与政治，2011（10）：38-52.

存在，进而需要国际法治对此专门回应？严格来讲，个人信息作为“权利”的一部分，即便在计算机技术尚未出现的传统经济语境下同样存在保护价值。对此的最典型例证，是美国早在 1890 年已有对于隐私权保护的讨论，[1] 但彼时必然不可能存在数字经济。《欧洲人权公约》（*European Convention on Human Rights*）第 8 条同样具有隐私权保护相关内容，而该公约同样缔结于 1950 年，远远早于数字经济的兴起。隐私保护虽然并不完全等同于个人信息保护，但二者之间存在大量交叠却是毋庸置疑的。同样值得注意的是，从 GATT（General Agreement on Tariffs and Trade，《关税与贸易总协定》）到 1995 年 WTO 规则初步定型，个人信息保护问题在长达数十年的国际经济规则谈判当中，从未真正成为规则关注重心。国际经济规则中唯一论及相关概念的，是 GATS（General Agreement on Trade in Services，《服务贸易总协定》）第 14 条（c）（ii）款中的“隐私例外”。此种状况足以证明，在传统经济语境下，个人信息保护与经济贸易的唯一交集，在于其可能成为自由贸易的例外，而不会成为贸易规则本身规制的内容之一。下文分析还将表明，在数字经济语境下，个人信息保护问题将在如下两方面与之产生关联：其一，作为生产要素的个人信息在数字经济语境下需要自由流动。这在本质上与“生产资料在传统经济模式下需要自由流动”别无二致。个人信息的跨境流动问题会与数字经济发展直接相关，这会变相影响个人信息保护的实现。其二，作为“公共政策”或“公共道德”，或至少是“非贸易目标”的个人信息保护必然会对以市场为导向的数字经济产生影响，这同样可以类比为“环境标准”会对货物进出口产生影响。

一、正向关联：个人信息足以成为数字经济生产要素

数字经济是继农业经济、工业经济之后的主要经济形态，是以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要

〔1〕 在美国法制史上，发表于 1890 年、由 Brandeis 与 Warren 共同署名发表于《哈佛法律评论》的《论隐私权》一文被视为首次提出隐私权概念的著述。参见：Warren S D，Brandeis L D. The Right to Privacy[J]. Harvard Law Review，1890，4（5）：193-220.

素数字化转型为重要推动力，促进公平与效率更加统一的新经济形态。[1] 其具体内容包括电子商务、云计算、大数据、物联网、人工智能、数字支付、电子政务等。上述相当一部分内容会与个人信息保护产生关联。

首先，个人信息能够用于定向广告，而定向广告则是相当一部分数字平台的重要盈利手段。以谷歌公司为例，其搜索引擎免费，但搜索引擎页面附带的广告业务则收费；而广告业务之所以能够做到精准投放，根本原因在于谷歌公司能够通过收集到的个人信息与用户访问记录定向投放广告，并根据用户的广告点击量向广告投放者收取一定费用。广告投放越精准，谷歌收益就越高。用户个人信息也因此成为谷歌公司盈利的重要支柱。与之相对，传统经济语境下虽然同样可能存在“定向广告”，但具体方式十分有限，在绝大多数情况下仅可能依据广告媒介的“定向化”实现极其粗略的受众区分：如，在儿童动画节目之间插播零食广告，在青少年杂志中刊载学科辅导书目广告，在少数民族聚居区发放民族特色食品传单等。此种“定向广告”至多可能实现基于群体的消费者细分，而无法实现基于消费者个人偏好的受众区分。因此，在传统经济语境下，个人信息对于产品销售与推广的功能相对有限。而数字技术则可以通过基于个人信息的精准定位，实现市场营销的低成本个性化。

其次，基于个人信息的精准推送，是相当一部分数字平台用户保持用户黏性的重要手段。数字平台通过分析用户的个人信息和行为数据，可以更准确地了解用户的喜好和需求，从而提供个性化的推荐内容和服务，增强用户体验和参与度。此种状况既可能出现在新媒体平台中，也可能出现在以货物买卖为主要业务模式的较为“传统”的电子商务当中。前者的范例如抖音首页视频推荐服务，后者的范例则是淘宝首页商品推荐服务。用户仅需登录平台、无须输入任何关键词或仅需输入较为模糊的关键词，就可获得更加适合其需求的商品推荐。推荐服务越精准，就越可能提升用户满意度，增强用户在平台的停留时间。而随着用户使用平台时间的不断增加，用户既往消费习惯、浏览习惯等完全可能以“滚雪球”的方式进一步便利数字平台向用户提

〔1〕 国务院 .“十四五”数字经济发展规划 [EB/OL].（2021-12-12）[2025-04-11]. https：//www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.

供更加精准的服务，进而进一步增加用户黏性。

与之相对，在传统经济语境下，从理论上讲，商家依然可能基于用户个人信息增进用户黏性，如通过会员积分制度给予老客户更多优惠等；但此种做法不仅规模较小、手段单一，而且仅会作为常规营销手段的补充而非营销手段本身推出。

再次，个人信息本身完全可能成为人工智能在线提供服务的重要依据。目前，相当一部分数字平台均基于人工智能为消费者提供了“量身定制”的算法自动推荐服务，如消费者输入身高、体重、肤色、发色等信息，平台即可自动推荐彩妆产品与服饰等；此种服务较之于定向广告与精准推送产品的重要区别在于，其基于消费者主动提供的个人信息提供服务，而非基于消费者过往浏览记录、交易记录等“被动”信息进行推送。不仅如此，生成式人工智能还可基于消费者个人信息与特定要求提供高度个性化服务，如通过自然语言生成技术，为用户提供陪聊服务，可以帮助用户缓解孤独感和压力；根据用户的个人喜好和兴趣，生成虚拟视频内容，如艺术创作、电影剪辑等，为用户带来全新的视听体验。鉴于人工智能很大限度上是依托数字经济而生的，在严格意义上的传统经济语境下，显然并不存在人工智能基于个人信息在线提供服务的可能。

最后，个人信息本身完全可能成为“大数据”的一部分，对于企业的市场调研、产品开发起到至关重要的作用。例如，通过用户的购买记录、搜索历史、社交互动等大数据的汇总，专业咨询公司可以为企业提供用户画像分析，帮助企业更好地了解用户需求和偏好，从而优化产品设计和市场定位。当然，在传统经济语境下，以问卷、电话调查、入户调研为典型手段的市场调研同样可能进行，而且同样可能获取消费者个人信息；然而，上述手段成本相对较高、获得大体量数据相对困难，且数据本身准确性存疑，因而无法与数字经济语境下的“大数据”相提并论。

综上所述，有别于传统经济，在数字经济语境下，个人信息对企业而言具有重要意义，不仅是企业服务消费者的重要依据，也是企业推测消费者需求的重要资料。正如我国学者所论述的，“数据化开启了一场‘寻宝游戏’，数据隐藏着未被发掘的价值，成为有价值的公司资产、重要的经济投入和新

型商业模式的基石。而获得这些问题的‘答案’会产生巨额的利润”。[1] 事实上，个人信息本身的商业价值同样是数据交易市场所认可的。也正是基于此，大力发展数字经济的国家，同样支持包括个人信息在内的数据的自由流动。正如欧洲议会所论及的，“数字经济与传统经济的重要区别在于……数据的自由流动对于经济发展具有重要作用”。[2] 不过，下文还将论及的是，个人信息除了具有生产要素的价值，其本身作为“权利”的一部分，同样具有重要的非经济价值。这又是个人信息较之于煤炭、铁矿石等传统经济语境下的生产要素的重要区别。对于个人信息的保护，也势必会与数据自由流动之间产生冲突，进而在一定程度上构成数字经济的障碍。

二、反向关联：个人信息保护与数字经济的潜在冲突

（一）个人信息保护具有鲜明的“权利”内涵

上文分析表明，个人信息是数字经济中的重要生产资料；然而，个人信息同样是公民权利保护的重要内容。根据联合国教科文组织的报道，目前，国际上已有 137 个国家通过了个人信息与隐私保护法律。[3] 不仅如此，相当一部分国家与地区的立法均有数十年甚至上百年的法律文化传统作为支撑。

以欧盟为例，作为人权保护重要组成部分的个人信息保护，向来是“二战”后欧洲一体化进程的重要方面。尤其是纳粹在“二战”当中对平民的种种屠杀行为，更是直接导致了“二战”过后欧洲重建时对人权保护的再认识与反思。1949 年，欧洲理事会（Council of Europe）正式成立，其下设人权专员与欧洲人权法院，并于 1950 年通过了《欧洲人权公约》，此公约于 1953 年正式生效。目前，欧洲理事会的成员已不仅限于欧盟成员国，《欧洲人权公

〔1〕 叶成城 . 数字时代的大国竞争：国家与市场的逻辑——以中美数字竞争为例 [J]. 外交评论（外交学院学报），2022，39（2）：110-132.

〔2〕 European Parliament. The EU’s digital trade policy [EB/OL]. Brussels：European Parliament，[2025-04-11]. https：//www.europarl.europa.eu/RegData/etudes/BRIE/2024/757615/EPRS_BRI（2024）757615_EN.pdf.

〔3〕 UNCTAD. Data Protection and Privacy Legislation Worldwide [EB/OL]. Geneva：UNCTAD，[2025-04-11]. https：//unctad.org/page/data-protection-and-privacy-legislation-worldwide.

约》缔约方也同样不止于欧盟成员国。在此之后，欧洲理事会又主导缔结了诸如《欧洲文化公约》《欧洲社会宪章》等一系列人权条约。[1] 不过，《欧洲人权公约》第 8 条当中虽然规定了“尊重私人和家庭生活”，且表示，“每个人的私人和家庭生活、家庭与通信均享有受到尊重的权利。”但是，整个公约当中并没有明确提到“个人信息”一词。将个人信息保护明确作为基本人权加以保护的文件，是 2000 年《欧盟基本权利宪章》。《欧盟基本权利宪章》第 7 条纳入了《欧洲人权公约》第 8 条第 1 款，仅将其中的“correspondence”一词改为“communication”，二者在本质上并无差异。而《欧盟基本权利宪章》第 8 条“个人信息保护”，则正式将“个人信息”一词作为“人权”的一种，与禁止奴役与强制劳动、禁止酷刑与不人道待遇等相并列。《欧盟基本权利宪章》第 8 条第 1 款规定，“人人均享有与其相关的个人信息的保护的权利”。第 2 款规定，“此类信息的处理必须基于如下条件公平进行：基于特定的目的、信息所有人同意或拥有其他法定的合法基础。人人均享有访问与其相关且已被收集的信息，且有权要求对其进行纠正”。除此之外，诸如 1981 年 1 月 28 日开放签署的第 108 号公约——《与自动处理个人信息相关的个人保护公约》[*The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*（CETS No. 108）]、1995 年《数据保护指令》（Directive 95/46/EC）、《通用数据保护条例》（General Data Protection Regulation，GDPR）等一系列法律文件，均将个人信息保护明确写入了欧盟立法。

对美国而言，“个人信息保护”一词的法律传统来源于美国隐私权的宪法保护，即美国《权利法案》第一修正案（言论、宗教、和平集会自由）与第四修正案（免于不合理的搜查与扣押）。不过，“隐私”一词从未出现在美国宪法文本当中。目前各种对“隐私权的宪法保护”的论证，均产生于对上述修正案的演绎。鉴于美国宪法第九修正案同时表示，即便是美国宪法未列明的权利也依然会受到保护，因此，合理推定“隐私”属于美国宪法保护的权利并不过分。当然，随着数字经济的不断发展，仅对消费者“隐私”而非“个人信息”进行保护，已远不足以保护消费者对于数字经济的信心。美国近

〔1〕 以上信息源自于欧洲理事会网站：https：//www.coe.int/en/web/human-rights-convention/our-rights.

年来虽未出现任何联邦层面的，以“个人信息保护”为题的立法，但已有相当一部分州立法以“隐私保护”或“个人信息与隐私保护”为名。较为典型的立法是2020年1月生效的美国《加利福尼亚州消费者隐私法》与2023年7月1日生效的《科罗拉多州隐私法》。此处还需说明的是，美国州法或许以“隐私法”为名，但在法律文本当中界定的实际上仍然是“个人信息”保护。举例来讲，在《加利福尼亚州消费者隐私法》当中甚至没有对“隐私”一词进行任何定义，反而对于“个人信息”一词进行了非常详细的定义。其中明确包括能够确认消费者或家庭，或与其相关的任何信息，包括姓名、化名、通信地址、IP地址、邮箱地址、账户名、财产信息、消费记录、生物识别信息等。〔1〕

（二）数字经济语境下的个人信息保护内容更加繁杂

个人信息的“权利”内涵或许植根于一国法律传统，但在数字经济语境下，个人信息保护还将具有传统经济语境下所不具有的全新特征，其权利内涵更加丰富，需对个人信息进行的保护也因而更加繁杂。

首先，数字经济语境下的个人信息收集相对容易，这就会对个人信息保护提出更加严峻的挑战。这是因为，传统经济语境下的个人信息并不必然成为生产要素，而且收集成本相对高昂，传统商家未必会注重对于相关数据的收集。其中典型的范例，是在超市、百货商店或集市当中，绝大多数交易均会以匿名的方式进行。商家并不会强行收集消费者个人信息。然而，在数字经济语境下，即便是货款金额极小的在线交易也完全可能导致消费者个人信息被商家以极低的成本收集，此种“收集”甚至可能以一种自动化方式进行，而且未必会征得消费者同意。这就意味着，传统经济语境下，个人信息保护很少会成为商事交易的注意事项之一，也未必会为立法者所重视。然而，在数字经济语境下，从“源头”治理个人信息搜集行为恰恰是当前电子商务立法的重点内容之一。

其次，数字经济语境下的个人信息更加容易遭到侵害，对此的保护也更加迫切。当个人信息存储于纸本、硬盘或光盘当中，对于个人信息的侵害只

〔1〕 California Consumer Privacy Act，at Art. 1798.140.

可能以“入室盗窃”或“监守自盗”的方式进行，而且信息的复制与传播也不可避免地需要花费大量成本。然而，在数字经济语境下，个人信息自始就以电子方式产生、存储，对此的侵害也更加容易。个人信息保护问题，也更可能成为影响消费者对电子商务的信心的重要事项。

再次，数字经济语境下的个人信息保护还会引发一系列传统经济语境下几乎不可能出现的全新议题。举例来讲，“被遗忘权”〔1〕问题在传统经济语境下几乎不可能发生。一方面，这是由于，某些个人信息一旦在传统媒体中呈现，则任何人均无法全部销毁该信息的物理载体；另一方面，由于传统媒体在资源搜索方面天然的局限性，丧失时效性的信息将极难重见天日，当事人甚至无需专门主张其拥有被遗忘权。又如，算法价格歧视问题在我国向来会引发民众热议，但此种基于消费者个人信息精准追踪的价格歧视行为在传统交易当中几乎不可能发生，因而无需特别讨论。

最后，数字经济语境下的个人信息保护更容易引发国家间的法律冲突。这是因为，在传统经济语境下，个人信息出境仅在较为特殊的情形下才会发生。某一企业如无特别需要，通常不会将卷帙浩繁的个人信息专门运输至国外存储，这在传统经济语境下无疑会大幅度增加企业经营成本。即便是外商投资企业也同样如此。对于传统经济语境下的个人信息保护问题，也仅需依据属地管辖的基本原则进行法律适用即可。然而，在数字经济语境下，个人信息的频繁跨境流动是常态而非例外。一方面，这是由于数据传输成本较低，因而电子商务经营者完全可以在其母国或第三国建立统一的数据中心；另一方面，电子商务经营者完全可能以跨境提供服务的方式远程经营，其甚至未必会在服务消费地具有任何商业存在。这就极有可能引发国家间的法律摩擦与冲突：数据输出国完全可能以本国个人信息保护法律为依据阻止数据的跨境流动，而数字企业母国也完全可能对存储于本国的境外个人信息进行其认为必需的保护。这一进程完全可能引发国家间的法律冲突、国家间的立法与司法管辖权冲突，乃至于国家间的主权摩擦。

〔1〕 被遗忘权（right to be forgotten）是欧盟《通用数据保护条例》（GDPR）中规定的一项权利，个人有权要求数据控制者删除与其相关的个人数据。这一权利旨在保护个人的隐私和数据安全，确保个人能够控制自己的信息。相关信息参见：GDPR.EU, Everything you need to know about the ‘Right to be forgotten’, [July 16, 2025], https://gdpr.eu/right-to-be-forgotten/.

以上四方面原因共同意味着，数字经济语境下的个人信息保护涉及议题更广、保护力度更大，必然会由单纯的国内的人格权保护问题上升至国家间的法律协调问题。下文分析还将表明的是，数字经济的兴起固然会增加个人信息保护的复杂程度，个人信息保护本身也完全可能对数字经济发展造成障碍。

（三）作为“权利”的个人信息保护足以阻碍数据使用

上文分析足以表明，作为“权利”的个人信息保护，在国别或区域法治当中必然占有重要地位。然而，任何规制措施理论上均可能对自由市场造成限制。对于个人信息的保护，也同样足以对数字经济造成阻碍。

首先，个人信息保护会直接影响商家对于数据的自由获取，这会从“源头”影响数据如何进入市场。具体来讲，相当一部分国家和地区的个人信息保护立法，均会对企业获取个人信息的路径进行限制。例如，我国《个人信息保护法》第 13 条规定，个人信息处理者处理个人信息必须符合立法中的六类情形之一。其中，在商事交易中最为常见的合法性来源为“取得个人的同意”与“为订立、履行个人作为一方当事人的合同所必需”。这就意味着，一位电子商务经营者可以基于“履行合同所必须”这一合法性事由要求消费者填写收货地址并将其打印在快递面单，但不得强行要求消费者提供其年龄、民族等“履行合同不必需”且消费者拒绝提供的信息。事实上，App 过度索取个人信息访问权限，恰恰是我国网信办曾重点打击的行为之一。〔1〕因此，如果仅从电子商务经营者的角度而言，任何对于其获取个人信息的限制措施，均会构成对于个人信息这一生产要素进入数字市场的限制。

其次，个人信息保护法通常会对个人信息的使用进行限制。即便电子商务经营者有权合法获取个人信息，其仍然不得随意使用上述信息。仍以我国《个人信息保护法》为例，其中要求个人信息处理者在获取数据主体同意前应当告知其个人信息处理目的，而且实际处理行为不得超出该目的；个人信息的保存期限应当为实现处理目的所必要的最短时间。〔2〕个人信息处理者如将其保管的个人信息提供给其他个人信息处理者，应当取得数据主体的单独同

〔1〕 人民网 . 向 App 过度索权说“不”！这部《规定》公开征求意见 [EB/OL]. 北京：人民网，（2021-04-28）[2025-04-11]. http：//www.people.com.cn/n1/2021/0427/c32306-32089759.html.

〔2〕《个人信息保护法》第十四条、第十七条、第十九条。

意。[1] 这就意味着，电子商务经营者不得在获取个人信息后将其用于消费者未曾明确同意的目的，也不得将个人信息转售或交由第三方继续利用以获利。事实上，在我国《个人信息保护法》发布后，相当一部分典型案例均围绕互联网公司或物流公司非法销售个人信息行为展开。[2] 对此，欧盟个人信息保护立法也有明确规定。在欧盟《通用数据保护条例》（GDPR）发布之前，欧盟第 29 条数据保护工作组就曾专门发布意见表示，数据处理需服务于特定、明确、合法目标，且必须在数据处理前通知数据主体。数据处理者不得笼统表示“数据的收集与处理将用于提升用户体验”或“为市场营销目标”处理数据。此外，数据处理者对于已获取的个人信息的后续使用同样需符合最初告知消费者的初始目的。第 29 条数据保护工作组的报告当中对此明确举例，假设某一电商在获取消费者地址后，在后续交易中直接使用数据库中保存的地址向消费者寄送货物，则此种“后续使用”无疑符合“初始目的”；但该电商使用该地址寄送广告宣传页则未必符合“初始目的”，此行为的合法性还需结合消费者的合理期待进一步考量。[3]

再次，个人信息保护法通常会对算法自动决策加以规定，并限制算法利用个人信息从事某些有违公共秩序或竞争秩序的行为。举例来讲，我国《个人信息保护法》第 24 条规定，“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇”。当然，对于这一问题，国际社会看法并不统一。也有国家认为算法价格歧视可能会对消费者总体福利具有增益，或认为算法价格歧视并不会影响充分竞争市场下的消费者福利。[4] 但上述观点的核心并不在于个人信息保护而在于不正当竞争规制。又如，在欧盟人工智能立法当中，存在对于人工智能风险的划分；其中，可能造成“不可接受的风险”的人工智能系统就包含专门针对弱势群体的行为操控，如鼓励儿童从事

〔1〕《个人信息保护法》第二十三条。

〔2〕 广东政法网 . 广东高院发布个人信息保护典型案例 [EB/OL]. 广州：广东政法网，（2022-10-31）[2025-04-11]. https：//www.gdzf.org.cn/yasf/content/post_123692.html.

〔3〕 Article 29 Data Protection Working Party，Opinion 03/2013 on purpose limitation，2 April 2013，Part III.1，III.2.

〔4〕 谢宜璋 . 算法个性化定价的监管路径研究——基于欧美比较法视角 [J]. 上海法学研究，2022，7（1）：145-162.

危险行为的互动性玩具；基于个人行为或个人特征的社会评分；基于生物识别信息的人工智能系统；以及，实时远程生物信息识别系统。上述四种“不可接受的风险”均包含基于某种个人信息（如年龄、面容等）的算法自动决策。[1] 我国《生成式人工智能服务管理暂行办法》也有类似规定，其第 11 条规定，“（生成式人工智能服务）提供者对使用者的输入信息和使用记录应当依法履行保护义务，不得收集非必要个人信息，不得非法留存能够识别使用者身份的输入信息和使用记录，不得非法向他人提供使用者的输入信息和使用记录”；第 4 条第 2 款规定，“在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取有效措施防止产生民族、信仰、国别、地域、性别、年龄、职业、健康等歧视”。此处的“歧视”的产生，就必然基于上述个人信息的滥用。

最后，个人信息保护法律的另一共性内容在于，立法者完全可能基于个人信息保护目标，禁止或限制将本国个人信息传输至他国。此类规定以欧盟数据出境立法最为典型，我国《个人信息保护法》中也有类似规定。

综上，作为“权利”的个人信息在一国国内法项下需要进行保护，且此种保护完全可能从个人信息的收集、使用、删除延伸至出境。个人信息的流转限制对于数字经济而言无疑意味着生产要素流通限制。个人信息的法定使用限制也同时意味着对于数字经济的运作模式限制。当然，此处的“限制”一词是不含任何评价的客观描述，其并不代表对于个人信息保护立法本身正当性的评判。毕竟，数字经济本身并不具有超脱于其他社会目标的“理所当然”的正当性。自市场经济诞生之日起，“看不见的手”能够发挥的作用就不可避免地受到政府限制。数字经济也同样概莫能外。一国既可以基于对于数字经济的促进而采纳鼓励个人信息流转的立法，也可以基于对于数字经济负面影响的平衡而通过促进个人信息保护的立法。这些均属于各国立法主权的题中之意。而下文分析还将表明的是，当此种立法主权不可避免地具有域外效力，而且国别立法之间必然发生冲突时，则此问题还将激发国际协调的客观需求。

〔1〕 European Parliament. EU AI Act：first regulation on artificial intelligence [EB/OL]. Brussels：European Parliament，（2023-12-19）[2025-04-11]. https：//www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

第二节　制度需求：数字经济呼唤个人信息保护立法的国际协调

一、现有国际法不足以应对数字经济下的个人信息保护议题

上文分析表明，个人信息足以构成数字经济中的生产要素，且个人信息保护足以对数字经济造成阻碍。个人信息保护与数字经济发展之间的平衡，需要各国国内法或区域立法的保障。鉴于网络空间本无国界，以及数字经济不可避免地具有国际性，上述国别或区域立法不可避免地会对国际数字经济产生影响。这也能够导入本书的核心议题：个人信息保护必然需要国际协调。国际数字经济规则建构进程中，也不可避免地需将个人信息保护问题纳入考量范畴。在传统经济语境下，此种“考量”仅包含“简单例外”模式，即将隐私保护问题纳入自由贸易的例外条款、全盘排除出自由贸易规则考量范畴，典型立法例如《服务贸易总协定》（GATS）文本；然而，单纯延续传统经济语境下的“例外论”，极有可能不足以应对数字经济语境下个人信息保护可能带来的种种挑战。此种状况很大程度上是由于，传统经济语境下的个人信息保护并不是一个需要全球协调的议题，“人格权保护”更多属于一国主权范围内事项，国际法甚至完全无需对此进行任何干涉，仅需以“例外”的方式保证一国规制权获得国际法的承认即可。而在数字经济语境下，个人信息不仅是一种贸易例外，更是一种需要促进国际流转、共享共赢的生产要素。个人信息的双重属性也就意味着，仅将其作为“例外”排除出国际经济规则是不够的，对其的利用与保护还需将其积极纳入国际经贸规则加以规制。

二、个人信息保护水准的国际协调需求

首先，正如上文分析论及的，个人信息保护完全可能成为数据进入数字经济流通环节的障碍。这在国别层面成立，在国际层面也同样成立。国别个人信息保护立法完全可能存在差异，而且差异化的个人信息保护立法足以为

企业合规造成障碍。这甚至可以类比为在传统经济语境下一国检验检疫措施足以影响他国产品的进口。也正是基于此，出于消除贸易壁垒的考量，在相当一部分 FTA 当中均包含了对于个人信息保护的协调性规则。以 CPTPP 为例，其第 14.8 条“个人信息保护”就是典型的对于个人信息保护方式进行协调的规则。其第 1 款表示，缔约方认识到保护电子商务用户个人信息的经济和社会效益；但其余条款均为对于缔约国个人信息保护方式的限制性规范。第 14.8 条第 2 款要求缔约方采用或维持保护电子商务用户个人信息的法律框架，但同时要求各缔约方考虑相关国际机构的原则和指南。第 3 款要求缔约方尽量在个人信息保护方面采用非歧视做法；第 4 款要求缔约方公布个人信息保护立法相关信息，因而属于“透明度”要求；第 5 款则鼓励各缔约方建立个人信息保护机制间的兼容机制，如“对监管结果的承认……或通过更广泛的国际框架”。后四款的规定固然并未限制缔约方立法主权，但其中同时也强调了缔约方立法应尽量满足非歧视要求与透明度要求。这无疑属于立法方式上的协调。而第 2 款、第 4 款对于“国际标准”和“国际框架”“兼容性”的要求，则属于典型的国际标准协调。

其次，此处的“国际标准”目前数量并不多。已产生较广泛影响的规则包括 OECD《关于保护隐私和个人数据国际流通的指南的建议》、亚太经济合作组织（APEC）《跨境隐私规则》等，但其约束力均相对有限。即便是 CPTPP 缔约方也并未全盘采纳上述任一标准。此种现象的产生，很大程度上是由于一国个人信息保护水准是由其国内立法决定的。一国商务或外交机关即便积极参与国际谈判，亦无从左右本国立法机关决策。尤其是考虑到相当一部分个人信息保护立法均植根于本国法律传统，对其进行根本性修订无疑会阻力重重。

三、数据跨境流动的国际协调需求

如果说个人信息保护水准问题的统一主要服务于企业赴他国经营合规成本的降低，那么，个人信息出境法律标准问题，就主要服务于企业数据跨境移转合规成本的降低。对此的国际协调需求甚至高于对于个人信息保护法律标准的协调需求。毕竟，“保护水准”问题本质上仍然是一国主权范围内的事

项，而且一国如何进行个人信息保护很大程度上难以通过国际协调而随意更改。比较而言，数据出境问题显然具有更大的协调空间。

首先，数据跨境流动在相当一部分国家和地区均可通过私法安排实现，欧盟、中国与东盟目前均已通过了标准合同条款就是例证；这就意味着，数据跨境流动问题在这些国家与地区至少并不必然属于“强监管”事项。

其次，对于强制对数据输入国进行“白名单”认定的国家而言，数据跨境流动问题完全可以通过双边谈判实现规则协调。尤其是对于电子商务往来频繁、双边数据流动规模较大的经济体而言，达成此种规则协调很可能是共赢的。典型范例即为美欧三次数据跨境流动安排的达成。

最后，即便国家间无法就数据跨境流动的具体规则达成一致，各国也完全可能对于“数据跨境流动规制措施”的方式方法问题达成一致，如，CPTPP 第 14.11 条“通过电子方式跨境传输信息”中就要求数据跨境流动限制措施不得构成任意或不合理的歧视，或对贸易构成变相限制。此种要求固然无法从本质上降低企业数据跨境传输的成本，但至少能够保证企业间担负的成本大体相同，本国企业不会由于歧视性限制措施的存在而处于竞争劣势。

四、国别（区域）个人信息保护立法的域外效力及其有限协调

如果说对于个人信息保护和数据跨境传输的国际协调属于“国际造法”，那么，另一种能够影响国际数字经济法治化进程的现象，就是国别或区域个人信息保护相关立法的域外效力。“域外效力”一词，是指一国法律对于发生在其域外的事件进行管辖而产生的效力。在数字经济语境下，由于大量数字产品的销售与数字服务的提供均可以跨境进行，因此，一国只需对本国市场进行规制，就完全可以导致本国法律适用于境外的电子商务从业者。个人信息保护也是同理。一国完全可以通过对于面向本国市场进行经营的全体企业的个人信息保护标准问题提出要求，进而实现其本国法律的域外适用。在实践当中，国别或区域个人信息保护立法的域外效力可能出现如下情形。

其一，一国立法当中明确规定其对于面向本国经营的全部企业具有管辖权。以 GDPR 为例，其第 3 条分别通过“机构”标准与“目的”标准界定了

其适用范围。具体来讲，第 1 款规定，该条例适用于在欧盟境内设有机构的数据控制者或处理者，而不论其数据处理是否发生在欧盟内部。其中，“设有机构”一词并不要求数据控制者或处理者在欧盟境内设立具有法人人格的分支机构，仅要求其在欧盟境内具有稳定安排即可。第 2 款进一步规定，即便数据控制者或处理者不在欧盟设立，只要其为欧盟境内的数据主体提供商品或服务，或对欧盟境内的数据主体的行为进行监控，GDPR 同样能够对其适用。〔1〕这就意味着，除非某数字企业进行法人人格拆分或业务分割，否则，只要其面向欧盟市场进行经营，就必须符合欧盟个人信息保护规则。

其二，一国立法当中明确规定对于本国企业域外数据的管辖权。此种情形严格来讲涉及个人信息的管辖，但未必涉及个人信息保护。最为典型的立法例，就是美国《云法案》。《云法案》原则性要求在美国具有实际营业活动的企业应美国政府要求向其披露该企业占有、监管或控制之下的用户信息，即便该信息实际存储地位于美国境外也不例外。这会导致美国法的域外效力，并实际上与他国个人信息出境立法产生冲突。

上述两种情形的产生无疑将造成国家间的法律冲突，也因此具有了国际协调的必然需求。只不过，当前的国际协调效果相对有限。就欧盟个人信息保护立法的国际影响问题而言，他国的确对此提出过异议，但并不是基于对于欧盟法能否产生域外效力而提出质疑。目前有据可查的数起类似案例均是基于欧盟个人信息保护立法与他国公序良俗之间展开。其中典型争议之一就是美欧“被遗忘权”与“言论自由”之争。“被遗忘权”是欧盟《通用数据保护条例》项下明确认可的公民基本权利，但除欧盟以外的其他国家鲜少承认“删除权”以外的“被遗忘权”。在 2019 年“谷歌诉 CNIL 案”当中，核心争议即为欧盟法中的“被遗忘权”能否在欧盟以外得到强制执行。该案当中，谷歌拒绝在欧盟之外执行“被遗忘权”的重要理由即在于，这会导致他国言论自由遭到不当影响。〔2〕而对于跨境取证这一问题，目前国际社会也的确展开了协商，但成效相当有限。目前，美国仅仅与其盟友英国和澳大利亚达成

〔1〕 敖海静 . 关于《一般数据保护条例》适用的地域范围的指南 [J]. 经贸法律评论，2020（2）：135-158.

〔2〕 Case C-507/17，Google LLC，successor to Google Inc.v. Commission nationale de l’informatique et des libertés（CNIL），Opinion Of Advocate General，delivered on 10 January 2019.

了《云法案》项下的跨境取证国家间协作安排，与欧盟间的类似谈判已进行数年但尚未取得突破性进展。

五、个人信息保护单边监管的全球化

如果说一国个人信息保护法的域外效力是通过一国法律对于本国市场的规制产生国际影响，那么，“个人信息保护立法的国际影响”就是指一国法律虽未必强制适用于外国企业在外国的行为，但由于该国立法的强大影响力，导致他国企业与政府均会在企业合规或本国立法中有意识地遵循该国的政策走向。此种现象最为典型的就是“布鲁塞尔效应”。当然，“布鲁塞尔效应”一词并不必然针对数字经济或个人信息保护进行，但数字经济语境下的个人信息保护问题的确属于“布鲁塞尔效应”的典型领域。目前，相当一部分国家和地区均效仿欧盟制定了本国个人信息保护法和个人信息出境规则。此种现象也被我国学者描述为“单边监管全球化”，即一国通过市场机制将其法律法规外部化到境外，进而导致标准的全球化。[1] 当然，此种国内立法的国际影响，在实践当中并不容易实现。在历史上，也仅有“特拉华效应”和“加州效应”得到了一定程度上的公认。前者用于形容美国特拉华州公司法相对宽松，因而能够吸引大量公司前往此地注册登记，并进而实际上降低了美国公司法总体监管水准；而“加州效应”则恰恰相反，这一术语主要用于形容美国加利福尼亚州立法对于环境标准的提升直接导致大量出口企业因此提升其环境标准以进入加州市场。在数字经济领域，目前也仅有欧盟这一地区能够取得“布鲁塞尔效应”。这是由于，“布鲁塞尔效应”的实现需具备两方面的条件：第一个条件，该国家或地区具有一定规模的市场，方可通过规制市场而影响企业乃至于他国立法。如一国市场份额在国际上无足轻重，则某些企业完全可能在权衡成本收益后选择退出该地市场。从这一角度来看，美国和欧盟的数字市场份额均足以形成“布鲁塞尔效应”。然而，“布鲁塞尔效应”的实现，还需具备第二个条件：进行立法的国家或地区需具有对某一事项的监管意愿和监管能力。美国向来鼓吹数字市场自由化，因而并无意愿对于包括个人信息保护在内的数字治理事项

〔1〕 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”[J]. 中外法学，2023（1）：46-65.

通过全国性的立法，更无意于单边推进其国内数字立法的国际影响。当然，也有学者对此提出一定质疑：美国加利福尼亚州个人信息保护立法同样颇具特色，但为何至今无人主张个人信息保护领域的“加利福尼亚效应”？不过，当前的研究成果仍然表明，尽管加利福尼亚州的个人信息保护法颇具特色，而且同样具有相当的辐射范围，但在实践当中，仍有相当一部分美国企业选择接受“布鲁塞尔效应”而非“加利福尼亚效应”以节省成本。〔1〕

以上分析意味着，数字经济国际规则的建构，并不必然通过国家间缔约的方式进行。所谓的“国际规则建构”，也完全可能以制度竞争的方式出现。最终能够对国际数字经济形成约束的，完全可能是国别规范而非真正意义上的国际法律规范。

六、个人信息的“情报”属性足以引发国家安全防范

除上述四种情形之外，另一种个人信息保护相关的立法，是基于个人信息“情报”属性的国家安全防范。此种情形的特殊之处在于，以上四种情形均针对个人信息本身的保护展开，“个人信息保护”本身即为立法目的。然而，此处分析的第五种情形——基于个人信息“情报”属性的国家安全防范，“个人信息保护”本身并非目的而是手段。其真正的目的在于防范个人信息出境或被外资获得而可能带来的情报风险。其中，较为典型的立法例，是至今仍未得到完整解决的 TikTok 事件。这一事件当中，美国颁布“TikTok 禁令”的原因之一，就是 TikTok 可能将收集的敏感个人信息传送至中国政府，进而危及美国国家安全。〔2〕上述主张虽然并无任何事实佐证，但在美国政府看来，此种可能性只要“存在”，即可构成对国家安全的侵害。在 2024 年 2 月 28 日由美国拜登总统发布的行政命令当中，也再次明确表示，其用意在于防范美国人的个人信息传输至“特定国家”。其中论及，企业完全可能收集美国人个

〔1〕 Frankenreiter J. Cost-Based California Effects[J]. Yale Journal on Regulation，2022，39（3）：1155-1217.

〔2〕 The White House. Executive Order on Addressing the Threat Posed by TikTok [EB/OL]. Washington，D.C.：The White House（2020-08-06）[2025-04-11]. https：//trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-Tiktok/.

人信息，并将其销售至某些特定国家或由特定国家控制的企业，为外国情报机关、军事机关获得，最终导致情报泄露、敲诈勒索与其他国家安全问题。[1]

此类事件有别于前述四种情形的另一个因素在于，在前述四种情形当中，国家间至少均存在“协调”的意愿。个人信息保护水准问题虽然难以取得国际共识，但至少在区域范围内能够达成有限度的一致。数据跨境流动虽然无法实现全球自由流动，但国家间自由流动至少能够小范围实现。国别立法的单向全球化虽然并非国家间协商的结果，但至少是主权国家可以主动防范的现象。国别或区域个人信息保护的域外效力虽然并不总能通过国家间的协调划定边界，但其中至少出现过国家间的礼让。然而，与上述情形相对的是，此处讨论的第五种情形足以对国际数字经济造成不利影响，而且相当一部分主权国家与国际法学者均在积极探讨将国家安全问题法制化的可能；但是由于国家安全属于典型的“高政治”议题，因此，此问题目前仅有国际协调的呼声而无实际进展。

七、“国际协调”的非典型方式：跨境数字平台内部政策的国际影响

除上面五种情形之外，最后一种“非典型”国际协调的方式，是缺乏主权国家参与的个人信息保护规则统一化进程——跨境数字平台内部个人信息保护规范随着平台自身对全球市场的占领而产生国际影响。此种影响固然存在积极的一面，如对于尚无成熟个人信息保护立法的国家而言，数字平台隐私政策至少能够维护该国较为稳定的电子商务秩序；然而，数字平台个人信息保护规则也完全可能携带其母国的价值取向，进而对东道国当地法治与公共政策造成威胁。数字平台甚至可能由于响应其母国跨境取证政策而危及东道国个人信息保护秩序。对东道国或数字服务输入国而言，此种由数字平台带来的“国际协调”需要批判性看待。

---

〔1〕 The White House. FACT SHEET：President Biden Issues Executive Order to Protect Americans’ Sensitive Personal Data [EB/OL]. Washington，D.C.：The White House（2024-02-28）[2025-04-11]. https：//bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

八、小结

综上，从经济基础角度来讲，个人信息对于数字经济的促进作用是毋庸置疑的。个人信息保护问题因而在一定程度上需与数字贸易发展目标相统一。从法律博弈角度来看，个人信息保护问题既存在国家间的合作与协调，也存在单边立法对于国际社会的影响，更存在国际规则力所不能及之时的国别权力滥用。本书随后将更加详细分析的“国际数字经济规则建构”，同样既包括已经成型的数字经济规则（如 CPTPP 与 DEPA），也包括正在谈判中的数字经济规则（如 WTO 电子商务规则），同时还会包含存在国际协调意愿，但暂时难以达成一致的数字经济规则（如国家安全语境下的个人信息保护）。

对此进一步抽象还将发现，当前，个人信息保护与国际法治的互动，又可分为三种情形：国家间谈判、国别法律的隐性影响，以及一国单向决定法治发展进程。

其中，“国家间谈判”通常出现在个人信息保护与数字经济联系最为紧密的领域——数据跨境流动以及数据本地化问题。数据跨境流动问题直接关系到个人信息能否作为生产要素进入数字市场，但由于数据出境问题属于一国主权典型的规制事项，因此，一国除了以谈判的方式促使他国放宽本国政策要求，就无法通过其他方式实现数据本身的自由流动。当然，此处的“谈判”并不仅仅包含“两国就个人信息保护水准问题达成一致”一种情形。此种情形的确能够发生，欧盟与日本间的数据跨境流动安排就是例证；但此种安排往往以个人信息保护水准更低一方主动更改本国立法以适应较高水平一方为代价。更加常见的“谈判”则体现为贸易协定谈判。此种谈判既可能就个人信息保护水准达成一致（如《美墨加协定》），也可能就个人信息保护方法达成一致（如“缔约方应努力以非歧视的方式”达成个人信息保护目标），同时也完全可能是在一方在其他领域主动做出让步的情况下，另一方同意接受双边的数据自由流动安排。

“国别法律的隐性影响”，主要体现在个人信息保护与数字经济存在联系，但并不十分紧密的场景之下。较为典型的范例，是与数据出境并不直接相关的个人信息保护水准问题。这些问题更多属于传统人格权保护的范畴，主权国家对此未必具有国际协调的迫切需求，因而无需将其纳入贸易谈判或数据出境谈

判当中。然而，一国法律完全可能由于其先进性，或由于其实践中的域外效力，而促使企业主动选择遵从该国法律。他国政府也完全可能出于同一原因而效仿他国法律制订本国立法。此种情形的特征在于，“隐性影响”更多是一种“软实力”。国别法律产生隐性影响并不必然依赖一国强制他国遵循其法律。

“一国单向决定法治发展进程”，通常出现在国际法治尚未达成共识的场合。与个人信息相关的此类场合，最为典型的当属一国法律的管辖权扩张（如欧盟个人信息保护法的域外适用）和外资安全审查（典型事例如美国以“敏感个人信息可能泄露至外国”为由禁止 TikTok 进入本国市场）。值得一提的是，此处的“单向”，仅仅用于描述决策的达成方式，并不涉及该国相关立法或司法本身的国际合法性问题。他国完全可能对此提出异议甚至抵制。

还需说明的是，对于同一事项，国际法治往往并不必然通过唯一一种渠道实现。例如，个人信息保护水准的确立，完全可以同时体现出上述三种方式的叠加。

个人信息保护纳入与数字经济相关的国际法治的整体图景可如表 1.1 所示。

表 1.1　个人信息保护如何纳入国际法治

事项	个人信息保护纳入国际法治的具体手段	国际法上的合法性评判
个人信息的跨境流动	国家间谈判	国际造法
个人信息保护水准统一化	国别法律的隐性影响	不涉及合法性问题
	国家间谈判	国际造法
	国别法律的单边监管	需进一步讨论
	跨境数字平台隐私规则的国际适用	需进一步讨论
基于个人信息“情报”属性的规制措施	国别法律的单边监管	需进一步讨论

如果仅从法律角度分析，本章的探讨完全可以告一段落。然而，综观国际法的历史将会发现，国际法治建构向来不是目的而只是手段。“国际法是国际关系发展到一定程度时的产物，成为‘另一种方式的国际交往的继续’，或者说是国际行为主体之间建立某种国际关系的手段或工具，反映的是国际关系对秩序、稳定与可预测的需求。”[1] 基于此，完全有必要进一步追问国际

〔1〕 刘志云 . 国际机制理论与国际法的发展 [J]. 现代国际关系，2004（10）：36-41+5.

数字经济规则建构中的个人信息保护相关规则的成因：个人信息保护即便对于数字经济具有积极意义，那么，是什么促使其被纳入国际数字经济规则建构？上文同样论及的是，“议程设置”本身即为国家权力的体现之一。那么，究竟是何种国家权力决定了个人信息保护这一议题被写入国际条约？又是何种国家权力导致一国可以通过单边个人信息保护立法实际上实现国际趋同？对于国家间难以达成一致的安全问题而言，又是何种因素决定其无法获得国家间协调？对于上述问题的分析，也将是本章第三节将要关注的内容。

第三节　政治原因：国际社会需要就个人信息保护问题制订规范

一、“议程设置”的必要性

国际关系呼唤国际秩序，而国际秩序的建立又是国家间权力博弈的产物。本章前两节对于将个人信息保护纳入国际法治的现状进行了描述；但仅从“经济基础”的角度，并不能完全揭示个人信息保护可以进行国际规制的全部原因。毕竟，一个问题具有国际性，并不必然代表其足以成为国际议题。对此的典型例证，就是“自由贸易”已有数百年历史，但“自由贸易”作为国际议题的历史至今不足百年。个人信息保护议题也同样如此。国家间决定就此进行协商、单边或者隐性地扩张此问题的国际影响，这本身就是一种“议程设置”。而议程设置的根本原因，仍然在于国家间的权力博弈。更具体地讲，一项议程能够进入国家间共同关注的范畴，其首先需要国家间强烈共鸣，即对此问题的解决至少符合相当数量国家的共同利益，而非仅仅有少数国家对此进行关注。不仅如此，该议程还需寻找到恰当的切入点，构建强有力的议题联盟网络，以正式进入国际关注，减少议题设置的阻碍。〔1〕

〔1〕 杨娜，程弘毅 . 理解国际议程设置：议题传播与框架互动 [J]. 当代亚太，2022（5）：135-165+168.

二、“议程设置”动因之一：国家间需要就数字经济制订规范

就个人信息保护这一议题而言，其能够进入国际议程设置，重要原因在于个人信息保护的确能够与数字经济产生关联，而数字经济则是近年来发展中国家与发达国家共同关注的经济增长点。正如本章第一节所言，个人信息足以成为数字经济当中的生产要素，但此种生产要素能否在数字市场当中发挥作用、如何发挥作用，还要取决于主权国家对于个人信息的保护与利用的平衡性安排。更加偏好数字经济发展的国家会倾向于降低个人信息保护可能造成的合规成本，而本土数字经济欠发达的国家可能强化个人信息保护，以避免跨国企业攫取本国数据，并凭借自身的数据优势阻碍本土数字经济发展。基于此，从正反两方面考量，个人信息保护问题均会随着数字经济的全球化发展而成为国际议程的重要组成部分。事实也的确如此。从本章第二节的分析可知，不论是个人信息的保护还是利用，在国际社会均已初步形成了利益群体。不论是美式自由贸易协定还是欧式个人信息保护立法，其背后均有相当数量的支持者。不仅如此，一些国家甚至还可能成功寻求“第三条道路”，在美欧之间寻求适应本国利益需求的平衡性安排。其中，日本就是一个典型范例。其在与欧盟达成个人信息保护“充分性”认定的同时，还能与美国签订专门的数字贸易协定。与之相对，也有少数国家试图在区域范围内进行个人信息规则统一化，但效果相对并不明显。其典型范例是东盟地区的个人信息保护统一立法，以及非洲国家间的个人信息保护公约缔结。下文还将对其具体立法动向进一步分析。

三、“议程设置”动因之二：国家对跨境数字平台进行制约的客观需求

除大国间规则制定的博弈之外，数字经济中的个人信息保护问题之所以能够成为国际议程设置的内容之一，另一个重要原因则在于，相当一部分国家均具有对于跨境数字平台进行约束的客观需求。此处“主权国家与数字平台之间的博弈”又可分为两个层面。

其一，是这一表述的字面阐释，即主权国家具有进行个人信息保护的客观需求，但数字平台完全可能对此加以破坏。数字平台具有足以匹敌主权国家的经济实力与政治影响力，甚至具有比肩主权国家的互联网空间控制力。具体到个人信息保护问题，数字平台需要个人信息作为重要生产要素，其利益主张不言自明地与主权国家存在差异。此种差异既体现为主权国家“人权保护”与数字平台“经济利益实现”之间的冲突，也体现为主权国家“竞争秩序维护”与数字平台“经济利益实现”之间的冲突。基于此，将个人信息保护议题纳入国际数字经济规则建构，一个重要原因即在于主权国家需要通过规则制订乃至于规则趋同，对数字平台的行为进行控制，以免平台行为对其国家利益造成损害。

其二，是“主权国家与数字平台背后母国利益诉求”之间的博弈。数字平台本身具有自身的利益需求，但其完全可能主动或被动承载其母国的利益诉求。“主动”一词是由于，数字平台与其母国完全可能具有相同的利益。如，数字平台母国完全可能认为，数字平台的全球扩张符合其国家利益，因而通过 FTA 缔约等诸多手段为数字平台的全球扩张扫清贸易壁垒；又如，数字平台母国完全可能认为，数字平台对于母国价值观的传播符合该国地缘政治需求，因而出于政治而非经济原因鼓励平台的海外扩张。〔1〕而“被动”则是由于，数字平台母国完全可能做出不符合平台利益，但符合母国总体利益的立法或执法行为，数字平台也因而不得不遵循这一立法，典型范例即为“微软诉美国司法部案”。但不论如何，数字平台与东道国之间的博弈，背后均有可能体现平台母国与东道国之间的利益博弈。从这一角度来讲，个人信息保护问题进入国际议程，完全可能由于主权国家希望通过规则谈判与制定，实

〔1〕 参见《美国国际网络空间与数字战略》。其中表示：“几乎所有外交政策问题——从国际安全到民主和人权，再到全球健康和气候变化——都将受到当今在网络空间和数字技术外交方面的投资的影响。美国国务院将领导跨机构进程，以制定、协调和整合网络与数字技术外交努力，从而在未来十年乃至更长时期推进美国的国家利益和价值观。”“因此，美国应当在促进技术平台问责制方面发挥领导作用。我们需要帮助引领下一波技术的负责任设计、开发、治理和使用，使其符合民主价值观和尊重人权。”U.S. Department of State, The United States International Cyberspace & Digital Policy Strategy, Towards an Innovative, Secure, and Rights-Respecting Digital Future, (2024-05-06) [2025-07-16], https://www.state.gov/wp-content/uploads/2024/06/United-States-International-Cyberspace-and-Digital-Strategy.pdf.

现对数字平台的合法规制，并最终制胜于国家间博弈。

当然，个人信息保护问题能够进入国际议程设置，并不代表其必然能够得到解决。“进入国际议程设置”仅仅意味着其能够获得讨论渠道，但问题的解决仍然有赖于国家间利益的趋同。目前来看，个人信息保护问题能够成为国际法治建构的内容之一，但距离真正的多边规则建构尚有相当的障碍有待跨越。对此的典型例证，是 WTO 电子商务谈判至今尚无一份承载国家间共识的最终文本。而在国际社会态度相对割裂的今天，对于个人信息保护现状的研究，就必须关注各主要利益集团对于数字经济的整体看法，以及对于数字经济和个人信息保护之间关系的看法，借以预测此问题上国际议程设置的未来走向。

第四节　个人信息保护议题对于我国参与数字经济合作的意义

以上三节分别从经济关联、制度需求与政治目标三方面分析了个人信息保护这一议题与数字经济规则建构之间的关联。上述三节的分析当中固然包含了对于我国现行的个人信息保护立法、我国正在参与的国际缔约实践的分析，但其中并未专门针对我国国情，分析我国究竟需要如何将个人信息保护议题与国际数字经济规则建构进行关联。我国对于个人信息保护的重视是毋庸置疑的，典型证据即为我国《个人信息保护法》《民法典》当中的种种规定。不过，除民法意义上的“人格权保护”之外，鉴于本书的分析的重心在于数字经济规则构建，本节分析的重心在于个人信息保护议题对于我国参与国际数字经济合作的意义，以便为随后各章节对于诸领域的逐一分析奠定基调。

一、个人信息保护是我国国内数字经济治理的客观需求

正如本章第一节所言，个人信息保护问题在数字经济语境下早已不再是一个单纯的人格权保护问题。个人信息究竟如何保护，很大程度上关系到消

费者保护、数字市场秩序维护，以及诸如人工智能等数字技术的规制。就数字平台经营问题而言，我国 2018 年通过的《电子商务法》第二章“电子商务经营者”当中明确规定，包括数字平台在内的电子商务经营者需在向消费者“提供商品或服务的搜索结果时”，“同时提供不针对其个人特征的选项”（第 18 条）；“明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件”（第 24 条）。2024 年 5 月出台的《网络反不正当竞争暂行规定》第 20 条再次强调，经营者不得利用技术手段“对条件相同的交易相对方不合理地提供不同的交易条件”。

这其中，“提供不针对消费者个人特征的选项”与“明示用户信息查询、更正、删除权”均为与消费者个人信息相关的电子商务经营者义务设置。前者有助于防范算法歧视的产生，后者有助于保护消费者对于个人信息的控制权。

不仅如此，在我国数字市场竞争秩序建设进程当中，个人信息保护也被用作维护竞争秩序的重要工具。以 2021 年《国务院反垄断委员会关于平台经济领域的反垄断指南》为例，其第 16 条“搭售或者附加不合理交易条件”，禁止具有市场支配地位的平台经济领域经营者从事滥用市场支配地位、无正当理由搭售或附加不合理交易条件的行为。而在确定某一行为是否构成“搭售或附加不合理交易条件”时，考量因素的第 5 项就包含了“强制收集非必要用户信息”。其第 17 条“差别待遇”进一步规定，具有市场支配地位的平台经济领域经营者滥用市场支配地位的行为可能包括“基于大数据和算法，根据交易相对人的支付能力、消费偏好、使用习惯等”，对于“交易条件相同的交易相对人”“实行差异性交易价格或者其他交易条件”。此处的“交易相对人”可能包含“B2B”交易当中的“企业”，也可能包括“B2C”交易当中的自然人。这一论断的证据在于，该《指南》第 17 条明确规定，“平台在交易中获取的交易相对人的隐私信息、交易历史、个体偏好、消费习惯等方面存在的差异不影响认定交易相对人条件相同”。能够具有“隐私信息”的“交易相对人”仅可能包含自然人。

就人工智能治理问题而言，我国 2022 年《互联网信息服务算法推荐管理规定》当中就明确表示，其立法依据包括《个人信息保护法》在内。其中第

10 条要求算法推荐服务提供者应当“完善记入用户模型的兴趣点规则和用户标签管理规则，不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息”。这因而属于对于服务提供者如何科学使用消费者个人信息的限制性规定。第三章“用户权益保护”也同样如此。其中第 17 条要求算法推荐服务提供者向用户提供“不针对其个人信息的选项”或提供“关闭算法推荐服务”选项；第 18 条、第 19 条要求算法推荐服务提供者向未成年人、老年人提供适合其年龄特点的服务，不得通过算法诱导未成年人沉迷网络，依法开展电诈网络信息监测。这属于根据用户个人信息对于算法推荐服务提供者提出的积极性义务要求。我国 2023 年《生成式人工智能服务管理暂行办法》当中同样存在与个人信息保护相关的内容。其中要求，生成式人工智能服务提供者开展预训练、优化训练等训练数据处理活动，“涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形”（第 7 条第 3 款）；服务提供者应当“依法承担个人信息处理者责任，履行个人信息保护义务”（第 9 条第 1 款）；“对使用者的输入信息和使用记录应当依法履行保护义务，不得收集非必要个人信息，不得非法留存能够识别使用者身份的输入信息和使用记录，不得非法向他人提供使用者的输入信息和使用记录”、尊重用户删除权（第 11 条）。

综上，个人信息保护在我国并不是单纯的人格权保护问题，还关系到消费者保护、数字经济竞争秩序建构与人工智能规制。这意味着，个人信息保护问题植根于我国内生需求，并且关联我国国内数字经济治理的方方面面。与此相关的国际缔约也必须尊重我国个人信息保护安排的政策空间。

二、现行数据出境规则是我国平衡数字经济与非经济利益的重要安排

上文对于我国个人信息保护立法的分析足以表明，个人信息保护不仅关系到人格权保护，还会影响到我国数字经济整体竞争格局构建。个人信息保护本身就是我国建构数字经济秩序的重要一环，我国并未出于发展数字经济的目标而有意对于个人信息保护水准进行克减。除此之外，个人信息与数字经济的另一个重要关联在于，个人信息出境规则既会影响作为生产要素的

“数据”的国际流通，也会影响对一国主权、安全等非贸易利益的保护。因此，探讨我国个人信息保护问题与国际数字经济发展的互动，就必须同时探讨个人信息出境的条件与限制问题。

我国跨境数据流动立法进程较为曲折。2016 年《网络安全法》首次规定了数据跨境流动的法律要求，不过其中仅原则性要求“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”，确需出境的应当进行安全评估（第 37 条）。具体安全评估办法——《个人信息和重要数据出境安全评估办法》的征求意见稿于 2017 年 4 月 11 日由我国网信办对外公布。2019 年 6 月 13 日，我国网信办再次发布《个人信息出境安全评估办法（征求意见稿）》，这也是与《网络安全法》相配套的、专门针对个人信息出境问题的部门规章。除《网络安全法》之外，我国《数据安全法》于 2021 年 6 月 10 日正式公布，其中并未专门针对数据跨境问题制定具体规则。随后发布的《个人信息保护法》于 2021 年 8 月 21 日正式通过，其中专门针对个人信息跨境传输进行了规定，其第 38 条要求，个人信息的境外传输需通过国家网信部门组织的安全评估、进行个人信息保护认证或签订标准合同。

在以上立法的基础之上，我国立法工作逐渐由粗到细，更加详尽的数据出境规则逐渐付诸实施。正式版本的《数据出境安全评估办法》于 2022 年 5 月 19 日对外公布，其中首先表示，该《办法》的立法目标在于“促进数据跨境安全、自由流动”，而且规范数据出境的目标同时在于个人信息保护与“维护国家安全和社会公共利益”。该《办法》第 4 条对于申报数据出境安全评估的具体条件进行了列举。其中，“关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息”和“自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息”两种情形均需提交安全评估。其中，评估内容除包括“数据安全和个人信息权益能否得到充分有效保障”之外，还包括境外接收方国家的数据安全保护政策和网络安全环境对于出境数据安全的影响。不符合上述第 4 条所列举情形的数据出境固然不需提交安全评估，但仍需通过个人信息保护认证或使用标准合同。上述规定也因而完全可能在客观上增加中小企业经营成本。与之相对，2024 年 3 月 22 日发布并施行的《促进和规范数据跨境流动

规定》首次对于数据出境问题做出了变通性规定。其中第 5 条规定，特定情形下产生的数据即便涉及个人信息，也同样可以免于申报数据出境安全评估、通过个人信息保护认证或订立个人信息出境标准合同。此类情形包括“订立、履行个人作为一方当事人的合同”、因跨境人力资源管理向境外提供员工个人信息、紧急情况下为保护自然人的生命健康和财产安全向境外提供个人信息，以及，除关键信息基础设施运营者以外的数据处理者年度提供官方信息不足 10 万条。

综上，我国数据出境规则与个人信息保护规则的共性在于，其中均会涉及个人信息的保护；但二者区别在于，国内法意义上的个人信息保护规则以“个人信息保护”为唯一目的，同时服务于数字市场经济秩序维护；而数据出境规则需努力在数字经济发展与包括公共利益、国家安全、个人信息保护在内的一系列非经济目标之间取得平衡。此种平衡实际上在 2017 年《网络安全法》当中就已有所彰显。我国彼时并未要求任何个人信息均需在本国境内存储，而是以数据流动自由为原则，特定情形下的数据本地存储和出境审查为例外。随后的立法对此进行了细化。但主导思想并未发生根本性变化。我国 2024 年最新立法的重要意义在于，其中并未一律要求个人信息出境必须符合法定的三种条件之一，且对于特定情形中的个人信息出境给予了明确豁免。这无疑属于对于数据出境风险的预估，以及在此基础上对于数据风险和经济收益之间的平衡性安排。尽管从理论上讲，任何形式的个人信息出境均可能造成被数据接受者滥用的风险；但 2024 年最新立法默示特定情形下的个人信息出境风险相对较小，且不会造成情报泄露或国家安全风险。此种风险与收益的平衡性安排彰显了我国涉外法治建设的利益取向。从这一角度来讲，我国在个人信息跨境流动问题上的态度既区别于欧盟式的严格个人信息保护路径，也区别于美国对于贸易自由的高度偏好。较之于美欧，我国立法的独到之处固然在于对于情报安全的高度强调，但此处的“情报安全”同样有别于美国以“情报安全”为由对外资的歧视性待遇，而是更加强调经济发展与国家安全之间的平衡发展。这一利益需求，在我国未来的国际缔约当中应当得到关注。