Advances in Social Sciences 社会科学前沿, 2025, 14(2), 555-564
Published Online February 2025 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2025.142157

Hans汉斯

企业数据出境中个人信息泄露的法律规制研究

王鸿俐

西南科技大学法学院，四川 绵阳

收稿日期：2024年12月26日；录用日期：2025年2月14日；发布日期：2025年2月25日

摘　要

在数字经济时代，市场交易已经不再局限于传统的商品与服务市场，数据交易已经成为一种新的发展趋势，在全球数据跨境流通治理机制尚不统一的背景下，按照不同的设计理念和立法目的，目前存在以美国为典型的重数据自由流动的治理范式和欧盟注重人权保护的数据治理范式。文章旨在通过对我国目前企业数据出境合规现状及其问题进行分析，再以欧盟、美国作为国外典型的数据合规治理模式为参照，最后在此基础之上对我国跨境数据合规治理问题提出针对性的完善建议。

关键词

跨境数据流动，企业合规，数据安全，数据保护，个人信息

Research on the Legal Regulation of Personal Information Leakage of Enterprise Data

Hongli Wang

Law School, Southwest University of Science and Technology, Mianyang Sichuan

Received: Nov. 26th, 2024; accepted: Feb. 14th, 2025; published: Feb. 25th, 2025

Abstract

In the era of the digital economy, market transaction is no longer limited to the traditional commodity and service market, and data transaction has become a new development trend. Under the background that the global cross-border data circulation governance mechanism is still not unified, according to different design concepts and legislative purposes, at present, there are two paradigms: the United States, which emphasizes the free flow of data, and the European Union, which emphasizes the protection of human rights. This paper aims to analyze the current status and problems of enterprise

文章引用: 王鸿俐. 企业数据出境中个人信息泄露的法律规制研究[J]. 社会科学前沿, 2025, 14(2): 555-564.
DOI: 10.12677/ass.2025.142157

data outbound compliance in China, and then take the European Union and the United States as typical foreign data compliance governance models as reference, and finally put forward targeted suggestions on China's cross-border data compliance governance issues on this basis.

Keywords

Cross-Border Data Flows, Enterprise Compliance, Data Security, Data Protection, Personal Information

1. 我国跨境数据合规的治理现状

在数字经济时代，数据可以说是“新时代发展的石油”因此习近平总书记强调：“数据基础制度建设事关国家发展和安全大局，要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济、统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。[1]”对数据跨境流动政策的讨论起始于个人数据保护法领域，1980 年经合组织出台的《关于保护隐私和个人数据跨境流动指南》主要分为“国内使用的基本原则”及“国际适用的基本原则”，后者解决的便是个人数据跨境流动问题[2]。虽然目前学界对数据跨境流中数据类型有所扩展，但纵观各国政策仍然是以个人数据为主。事实上，对政府数据中涉及国家秘密乃至国家安全的部分，本就应当禁止跨境流动；不涉及国家秘密的部分，也应纳入政府公开调整的范围，并不牵涉企业跨境数据合规问题。因此本文将讨论的数据仅聚焦于个人数据。

当下国际竞争愈发向规则之争、法律之争演化，然而随着对个人数据的重视程度与日俱增，各国为应对个人信息保护和企业经济效益之间的平衡问题出台了许多法案，一旦涉外企业在运营过程中触犯相关法律法规，便会面临巨额罚款。如 2023 年 4 月英国数据监控发现 2018 年至 2020 年期间，TikTok 没有移除使用该软件的低龄儿童，因此罚款 1270 万英镑，与此同时爱尔兰数据保护委员会(以下简称 DPC)也发现 TikTok 在处理儿童数据方案违反了欧盟《通用数据保护条例》，决定对 TikTok 罚款 3.45 亿欧元。除此之外，滴滴全球股份有限公司由于违法收集用户手机相册中的截图信息、剪切板信息、引用列表信息，以及过度收集司机学历信息等违法违规行为，国家网信办依据《网络安全法》《数据安全法》《个人信息保护法》等法律法规，对滴滴全球股份有限公司处人民币 80.26 亿巨额罚款。

可见在不同的法律背景下，世界各国对于数据合规、个人隐私保护的规定存在差异，不同的数据法案的出台也意味着赋予了企业更多的社会责任，尤其是对涉外企业来讲，除了熟悉本国的法律以外，还需兼顾了解他国的相关法案，只有先解决好数据合规问题，明确数据权益归属，确保数据主体隐私不被泄漏，才能在跨境流通使用中激发数据的经济价值。因此，鉴于数据在当前经济领域中的极端重要性，以及企业在采集个人信息领域违规行为的严重性，本文先从宏观和微观两个层面对我国数据合规现状进行梳理，同时提出当下企业跨境数据合规存在的痛点，并进一步以欧盟、美国数据合规治理范式作为参照，尝试为我国企业跨境数据合规提出改进建议。

1.1. 我国企业数据出境合规模式

从宏观层面上看，我国跨境数据治理政策大多是自“棱镜门”事件之后，从维护国家安全视角出发

提出的，因此我国的跨境数据合规模式的基本导向始终是坚持数据本地化，对数据跨境流通也一直持保守主义态度。2016 年颁布的《网络安全法》第 37 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补办进行评估；法律、行政法规另有规定的，依照其规定。”该规定首次以国家法律的形式明确了中国数据跨境流动基本政策。与美国、欧盟相比，我国在数据跨境流动治理领域确实起步较晚，至今关于数据跨境流动治理的内容仍散见于各类法律规范、部门规章之中，比如 2013 年《信息安全技术公共及商用服务信息系统个人信息保护指南》中规定，未经个人信息主体明确表示同意，或法律法规明确规定，或未经主管部门同意，个人信息管理者不得将个人信息转移给境外个人信息获得者。2011 年发布的《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》中提到，在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行，除法律法规以及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。除此之外，《网络出版服务管理规定》《地图管理条例》《网络预约出租汽车经营服务管理暂行办法》等都在不同程度上对数据本地化提出要求。

从微观层面上看，我国企业涉及企业合规与个人信息保护的行业主要集中在金融、教育培训、医疗卫生、互联网通讯几个领域[3]。近年来我国企业也在数据合规领域进行了许多有益探索，在金融行业，我国平安银行专门设立个人信息保护委员会对个人信息保护进行统筹管理，与此同时招商银行、平安银行等多家银行 APP 上都设置了“隐私政策更新”与“移动应用程序端的用户交互页面调整”等提示，以便事先征得用户同意[4]。后疫情时代线上教育培训行业兴起，截止 2020 年 12 月，我国在线教育用户规模达到 3.42 亿，手机在线教育用户规模达到 3.41 亿，相比疫情之前(2019 年 6 月)增长了 1.09 亿[5]。2021 年 3 月 16 日中国网络社会组织联合会成立在线教育专业委员会，并发布了《促进在线教育行业健康发展倡议书》要求企业需严格遵守《网络安全法》，落实网络安全等级保护、网络安全预警通报和用户信息保护制度，保障用户数据安全和隐私。在医疗卫生行业也有相关人士倡议建立完善的医疗信息保密制度，对医疗机构进行数据安全合规检查，同时对医疗机构涉及的核心数据进行盘点清查，为数据分类分级制度的开展提供数据支持[6]。

综上所述，我国无论从国家宏观立法、行政监管还是企业在微观上都对我国数据合规问题进行了有益探索，总体上为我国构建数据合规体系营造了良好的氛围。

1.2. 我国企业数据出境中存在的问题

我国企业数据出境合规问题虽然在国内取得了不小的进步，但鉴于企业当下仍然存在的“出海”难题，还需要正视我国企业在更加复杂的数据出境合规问题上，还存在以下几点问题。

首先，大数据时代背景下，用户的个人信息保护和企业数据权益之间存在着利益衡量问题。数据权益中既包括数据来源者权益，即个人或者组织对其产生的数据所享有的权益[7]。同时，还包括数据处理者对其收集、整理并最终形成的数据产品所享有的财产权。而自然人作为数据来源者时，对其产生的个人信息与个人数据均享有我国《民法典》与《个人信息保护法》等法律规定的个人信息权益，当数据处理者收集的个人数据中涉及自然人的隐私、姓名或者其他敏感个人信息时，自然人便可以就个人数据对数据处理者行使更正、补充或者被遗忘等法律明确规定的各项具体权利[8]。《数据二十条》中将“企业数据”定义为企业所生产处理的数据，既包括企业自己生产的数据，也包括企业收集(自行收集或从其他主体处取得)的数据。企业作为常见的数据处理者，同时在经济学上是市场中的理性人，为了得到更多的商业利益就必然会尽最大努力挖掘数据中的经济价值，但在这一过程中就不可避免的会涉及到对用户个人信息的利用，如果注重保护企业数据权益，对个人信息就必然会带来威胁；反之，如果注重保护个人

信息，又会对企业在利用数据进行商事活动时带来一定的限制[9]。因此如何平衡个人信息保护与企业数据权益也成为了我国构建企业跨境数据合规体系的新课题。

其次，在国际上我国进行数据出境合规时常处于被动地位。尽管我国正在不断加快对数据安全立法的步伐，《数据安全法》《网络安全法》以及《个人信息保护法》的出台也搭建了我国数据安全保护法律体系的基本框架，但我国对数据跨境流动的立法仍停留在对基本原则、制度要求的层面，虽然为数据跨境流动给出了大的合规治理方向，但是没有与数据治理现状和国内技术水平相结合提出更加详细的规制细则，在跨境数据合规中还不能作为具体依据进行落实。具体表现在，我国还没有建立起明确的跨境流动数据分类分级标准，仅对重要数据、敏感个人信息等进行了简单区分[10]。正是由于我国在数据合规方面起步较晚，缺乏对数据跨境领域国际立法的参与，进而导致我国在数据跨境合规领域一直处于被动适应的局面。

最后，我国企业数据出境合规能力较弱。造成这一现象的原因主要包括以下两点：其一，从大环境来看我国企业数据合规本就起步较晚，许多企业还尚未形成科学的合规管理体系与合规意识，对于数据合规采取亡羊补牢的态度，往往要等到触犯了相应规制才开始研究如何进行数据合规；其二，企业进行数据跨境合规的成本较高，许多中小型企业难以接受，碍于高额的合规运营成本，企业通常会选择铤而走险。仅从一些案例上就可以看出，我国企业目前在数据跨境合规问题上情况不容乐观，除了 TikTok 因数据安全问题在北美市场频遭罚款外，我国华为、中兴也因不符合数据安全问题而遭到瑞典邮政禁用，以及 Wechat 也被美国以数据跨境流动引发安全风险为由抵制[11]。

2. 参考分析：国外企业数据合规的治理规则

2.1. 美欧企业数据出境合规范式发展概况

2.1.1. 欧盟——以个人隐私保护为主

欧盟在发展过程中逐渐形成了一种“基本权利文化”，所以欧盟在制定数据跨境合规方面的政策法令时始终以“数据隐私保护”为导向，其数据保护法与《欧洲人权公约》紧密相关[12]。1973 年欧盟便开始对跨境数据流动的规制问题进行研究，在《里斯本条约》生效后，欧盟将数据保护权与隐私权的概念进行分离，确立了数据保护权基本权利的地位。到 1995 年 10 月 24 日欧盟理事会正式通过《个人数据处理中个人权利保护及促进个人数据自由流通指令》(以下简称为《95 号指令》) [13]规定禁止将个人数据转移到不能确保“充分保护水平”的非成员国家。但欧盟在审查后发现《95 号指令》制定的跨境流动规则实际运行中无法适应数据跨境流动的现状[14]，因此在 2012 年欧盟开始对个人数据保护启动立法改革。随后在 2016 年 4 月欧盟通过《通用数据保护条例》(General Data Protection Regulation，简称 GDPR)，GDPR 在《95 号指令》的基础之上引入了新规则，例如：1) 简化跨境传输机制，放弃许可管理办法，只要成员国符合 GDPR 中跨境数据流动的条件，则不再对其用许可方式进行限制；2) 扩大了“充分性”认定的对象范围，从国家到国内特定的地区、行业再到国际组织的保护水平都纳入评估范围；3) 强化行业协会等第三方作用，GDPR 规定数据持有者可以成立行业协会并提出行为准则，只要该行为准则被欧盟或者成员国监管机构认许后，可通过有约束力的承诺方式生效，并且经过认可的市场认证标志也可以作为数据跨境流通的合法机制；4) GDPR 扩展了成员国数据监管机构可以制定标准合同条款的渠道，为企业提供更多满足实际需求的数据跨境流通合同文本选择。GDPR 的出台不仅是从“指令”到“条例”的进步，还标志着欧盟对数据保护规范从柔到刚的转变。另外，欧盟出台的《关于非个人数据自由流动条例》《开放数据指令》等其核心都是践行欧盟在数据保护中“以人为本”的价值观，是在数据空间中对欧洲道德标准、基本人权理念的历史延续。

2.1.2. 美国——以产业利益和国家安全利益为主

相比之下，美国更关心如何最大限度发挥数据自由流动的经济价值，打破限制跨境数据流动的数字贸易壁垒，充分利用数据的商业价值推进和保障其在全球市场的支配地位。这种数据立法倾向也与美国一直以来的“民主”观念和“自由”文化密切相关，就比如在美国言论自由权比隐私权显得更为重要，在《美国宪法第一修正案》中保护隐私和禁止政府为保护隐私而限制言论之间的张力关系贯穿修正案的整个法理[15]。包括《梅根法》同样是美国言论自由的一个具体体现，只要目的是争议的那么言论自由便可能推翻隐私权。而美国在数据跨境流通问题上也同样沿袭了这样自由、民主的价值理念，因此美国并未在联邦层面对数据跨境流动进行统一立法，对数据跨境流动的规制也更多体现在美国和其他国家签订的协定之中。比如《欧盟—美国数据隐私框架》就为美国企业在适用 GDPR 提供豁免政策，为大西洋两岸数据进行自由流动搭建桥梁[16]。除此之外还包括《美国—韩国自由贸易协定》《跨境隐私规则体系》等均为促进美国同其他国家或者地区进行数据自由流动。与此同时，美国颁布的《澄清境外合法使用数据法案》中规定美国可以要求相关控制者向美国披露本国企业或者美国公民存储在境外的数据[17]，以此减少其他国家限制数据流通的不利影响，从而维持美国的数字优势地位。

2.2. 美欧企业数据出境合规范式对比分析

2.2.1. 美欧企业数据出境合规范式相同点

欧盟、美国作为目前全区两大主要经济体，在数据跨境流动合规过程中两种模式虽然由于不同的文化传统、政治制度，导致法规的核心价值理念存在区别，欧盟以自身独特的历史背景形成了以保护个人隐私、注重人权保护为特色的规制模式，美国也因其在全球所处的经济地位、科技实力，以及“911 恐怖袭击事件”的影响在跨境数据规制模式上以挖掘产业利益、维护国家安全利益为核心。但二者都在政策上不约而同的采取了“双重标准”，以实现增强自身网络领域竞争优势的实际目的。

欧盟一直以来都坚持外紧内松的规制态度。一方面致力于促进数据在欧盟境内自由流动，另一方面对外在数据保护政策上又采取高标准严要求的倾向。对内 2016 年 GDPR 出台促进了欧盟成员国之间数据跨境流动的效率，减少了数据传输的时间和成本。同时，欧盟也一直在试图创建“虚拟申根区域”(Vritual Schengen area)和“欧洲云”(Europe-only cloud)，“虚拟申根区域”旨在将互联网数据流动限制在国家边界或者申根地区，“欧洲云”则是将云处理的数据控制在欧洲境内[12]。两种措施的目的都是将数据的流动范围限制在欧盟境内，强化欧盟对数据的掌控能力。《人工智能白皮书》的发布也表明欧盟如今已经完全认识到对数据的掌控与经济发展之间的共生关系。但是对外，欧盟在与他国进行跨境数据传输过程中，却呈现保守且严格的态势。同样是 GDPR 在对非成员国家通过充分性标准认定、标准合同条款和认证机制等制定了严格的数据保护标准，并且欧盟通过 GDPR 中“地域范围”的规定，以“设立机构”“目标指向”“因国际公法而适用”三个标准拓展了 GDPR 在全球的适用范围，使欧盟的数据保护标准在全球范围内得到进一步认证。同时，2020 年与《人工智能白皮书》同时发布的《塑造欧洲数字未来》《欧洲数据战略》提出应当制定欧洲标准，甚至欧盟内部市场委员 Thierry Breton 提出要让欧盟占据标准制定领域，成为标准的制定者[18]。可见欧盟利用单一市场将其数据保护法律制度的规制标准推向世界，并迫使其他国家改革国内法律制度向欧盟范式对标，通过制定规则将数据的控制权牢牢掌握。

美国拥有众多全球巨型互联网企业，譬如 Facebook、Google、Amazon 等企业作为瓜分全球数据市场的主力军，因此美国在对外政策上急需扫清数据自由流动障碍，为国内互联网企业的发展提供源源不断的数据支持，但由于各国在数据保护措施上存在差异，导致规则之间共通性较低，使美国企业运营成本大幅度上升，尤其对美国小型企业而言更加不利。所以美国一边积极倡导签订跨境数据流动的双边或者多边协定，比如《APEC 隐私框架》；一边在 2018 年通过《澄清境外数据的合法使用法案》(Cloud Act)

发挥“长臂管辖机制”调取境外数据，挖掘全球数据市场的生产利润。美国在国际舞台上似乎对别国的数据流动规制不太关注，甚至将所谓的“数据保护主义”看作是数字贸易发展的一大阻碍，努力塑造出一种积极推动数据自由流动的国家形象。然而在其国内，却在悄然加强数据安全保护的力度。比如美国每年公布的《国家贸易壁垒报告》，内容包括对全球各国数据本地化措施情况进行跟踪，以及对各国限制措施的最新动向进行干预和指责，但却从未整理、公布美国自身的数据流动限制措施。美国在处理跨境数据流动问题时，常依据 WTO 的“安全例外条款”来实施各种限制措施，其出发点是保护本国的国家安全。然而，在对待其他国家基于相同国家安全考量所采取的法律制度和限制措施时，美国却持有不同的态度，其往往不太认可这些措施的合理性，这种态度差异或许可以被视为一种选择性的关注。美国在推动数据自由流动的同时，也在努力维护其在全球数据流动中的主导地位，这在一定程度上反映了其对数据流动控制权的重视。

2.2.2. 美欧之间企业数据出境合规范式对比

通过以上分析可见，欧美在数据本地化规则中都不约而同的采取“双重标准”，既认可数据本地化措施构成数字贸易壁垒，又都在一定程度上施行数据本地化措施来实现增强数据控制能力和国际话语权的真实目的。但是，欧美在数据跨境合规形式上仍存在以下几点不同。

第一，立法价值取向不同。欧洲的隐私概念都是基于人权保护的基础之上具体展开，是以维护人格尊严为目的。因此欧盟将个人数据隐私纳入基本权利进行保护。与之相比，美国的隐私权观念则立足于个人自己基础之上，将保护隐私等同于保护个人的自由[19]。两种不同的立法价值取向也是由于美欧在政治、数字经济实力方面的差异所导致的。欧盟虽坐拥全球最大的单一数字市场，且该市场具有高利润增长潜力，但其数字经济规模和本土互联网产业实力却不及美国，谷歌、脸书等美国大型数字平台长期“盘踞”其中。因此，在数据治理方面，欧盟秉持“权利话语”至上理念，倾向于保守立场，即在确保个人数据基本权利的前提下，仅允许数据有限自由流动，坚决反对将个人数据基本权利当作经济利益的交换物。而美国凭借在数字经济和互联网产业的绝对优势，无需采取阻碍数据自由流动的举措。美国把数据隐私置于市场环境中考量，倡导以市场为主导、以行业自律为核心来保护个人数据。这从根本上决定了美国在跨境数据流动上的价值取向，即更看重数据自由流动和经济利益，其目标清晰地指向维护自身全球贸易主导地位和信息优势。

第二，规制形式上欧盟在数据跨境的规制形式上采取“预防性合规范式”。无论是《95 号指令》还是 GDPR，欧盟在数据跨境合规过程中以统一立法为主要手段，形成以“充分性保护”为主，“适当性保障措施”和“例外情况”为辅的预防性合规范式[20]欧盟长期以来在数据进行跨境传输时就预先设置一道防御机制，这种可预见性强的合规范式也为欧盟向外输出欧洲标准提供信任基础，同时使数据在跨境传输过程中除了受到本国充分保护外，也能受到接受国同样水平的保护。然而，美国在数据跨境的规制形式上则采取“问责型合规范式”。与欧盟不同在于，美国采取通过设立不同的组织，制定符合各方共同利益的规范或者协定，推动各方以充分的行业自律来保障数据在跨境传输过程中顺利、高效地运行。同时，美国也构建了一套完善的监管体系对不同领域数据跨境进行事后监管。例如美国在消费者保护领域成立了联邦贸易委员会(Federal Trade Commission，简称 FTC)，在 Facebook 因涉嫌违背数据保密承诺、Google 用户虚假陈述等案件中 FTC 向涉案公司要求签署同意令并支付相应罚款，否则将提起相应民事诉讼。除此之外，还包括在通信领域成立的联邦通信委员会(Federal Communications Commission)以及在卫生领域设立的美国卫生与公众服务部(U.S Department of Health and Human Services)等事后监管专门机构。

第三，美国与欧盟在构建制度体系的形式上呈现出显著差异。美国倾向于采用分散的监管架构与立法方式，按领域和行业进行区分；而欧盟则偏好高度统一的立法与监管模式。这种数据保护价值理念的

差异，导致美欧在制度体系的组织架构、执法方式以及数据保护的严格程度等方面存在明显区别。首先，就监管体系的构建而言，欧盟遵循自上而下的立法路径。依据《通用数据保护条例》(GDPR)，欧盟及其成员国均需设立独立的数据保护机构与数据保护官，以协助数据控制者或处理者遵循条例规定，提升其合规性。此外，欧盟还成立了欧洲数据保护委员会，旨在保障数据流动保护规则在欧盟范围内的统一实施，并协调成员国监管机构之间的合作。相比之下，美国长期以来主要在州层面构建数据隐私保护的法律框架，强调各州在数据治理中的自主权，且侧重于对特定行业和数据类型实施多监管机构的分类监管，如联邦贸易委员会(FTC)、联邦通信委员会(FCC)和金融消费者保护局(CFPB)等。其次，在数据保护的严格程度和数据处理的合法性方面，欧盟的规定更为严格。《通用数据保护条例》第五条明确列举了六种数据合法处理的情形，包括数据主体的同意、履行合同、履行法定义务等。只有符合至少一种情形，个人数据的处理才被视为合法。而美国则遵循“法无禁止即可为”的原则。总体而言，欧盟的跨境数据流动制度体系在执法一致性方面表现更强，其数据保护规定也更为严格，但这种高度统一的做法也可能导致“一刀切”的问题。相对地，美国的跨境数据流动制度体系更具针对性，但由于联邦层面难以统一各州的法律规定，容易导致标准不一致的情况。

3. 难题纾解：企业数据出境合规的完善建议

3.1. 引入“区块链”技术，降低用户不安全感

如前所述，当下我国在数据跨境合规上面临着企业利益与个人信息保护的利益衡量问题，笔者认为用户对个人信息权益应当优于企业利益，企业也理应承担起更多的社会责任，引入更为优越的技术，降低用户在被采集个人信息时的不安全感。在当下“区块链”技术在多领域得到适用，鉴于其去中心化架构、集体维护数据、共识机制以及数据安全性高等核心技术特征[21]。尝试将区块链技术应用到企业数据出境合规过程中，对增强对个人数据的保护，降低用户的不安全感，具备以下几点可行性。

首先，区块链技术能够增强用户安全感。区块链技术是基于非对称加密算法达成数学共识，通过分布式存储方式实现系统内部全不节点对经过验证的数据进行存储、备份。企业利用区块链去中心化的特点，可以确保每次数据跨境流动的记录达到完全一致，实现企业跨境流动记录存储的稳定性，从根本上杜绝数据跨境流动过程中被篡改和删除的可能性。同时，区块链技术的利用可以避免传统中心化互联网架构“单点故障”造成网络瘫痪，进而导致个人信息泄漏的风险。除此之外，区块链技术引入数据出境，可以简化既有的信息记录和存储模式，使企业在采集、存储数据和数据出境过程中无需再借助第三方中介机构来确保数据的精确性。可以直接与用户构建点对点式的社会合作，提高企业数据采集用户个人信息的效率和准确率。

其次，区块链技术利于强化企业数据监管。区块链是通过链式结构将数据区块和哈希链链接组成，数据区块可以通过哈希链检查其前后区块的完整性与真实性[22]。因此区块链技术从本质上讲是一个不可被篡改的分布式数据平台。其内部庞大的数据区块集合了企业采集的每一项用户个人信息，可以实现对企业数据资源从采集、转换到出境的全过程周期记录。这一特性赋予了企业在进行数据出境交易过程中的可追溯性，便于企业对流通过程中的数据进行监管。例如，由马士基与 IBM 合作的 TradeLens 项目就利用区块链技术对重要信息进行存储和分配，通过区块链来确保交易记录等信息不被篡改和可供审计，实现了包括进出口清关在内的全球贸易跨组织业务流程数字化和自动化，并且利用分布式网络保障数据的隐私性和机密性。

最后，区块链技术利于搭建共享加密数据库。区块链所采取的“网状拓扑结构”意味着不存在核心节点，在公开链中用户可以随时在授权范围内读取、修改或者删除有关的个人信息，在企业与用户之间

建立稳定、透明的“分布式共享加密数据库”[23]增强用户对个人信息的掌控。用户可以在个人信息出境之前，正确并有效地绑定并登记存储确权信息，该操作可以确保并验证确权信息的准确性，做到精准识别信息的权利所属者。企业也可以根据合同预设的利益分配方案，在系统内直接根据合约规定与用户进行利益分配，以此避免经济纠纷，提高企业数据出境的效率。

当然，区块链技术作为一种新兴技术，要引入企业数据出境合规还存在一系列技术难题，但不可因噎废食。在将区块链引入企业数据合规过程中仍需秉持理性、谨慎的态度。

3.2. 增强国际话语权，形成我国数据跨境“白名单”

首先，鉴于我国与欧美国家在历史文化、价值观念以及法律体系方面存在显著差异，导致后者对中国在数据跨境流动模式上持有疑虑。其次，我国在数据跨境合规领域的立法工作起步较晚，尚未能构建出与通用数据保护条例(GDPR)相媲美的统一法规体系。基于上述因素，我国在国际数据跨境合规领域的影响力尚显不足。然而，我国在该领域正处于发展初期，可以借鉴美国和欧洲在跨境数据流动管理方面的经验，以完善我国跨境数据流动的治理体系。

基于此，本文提出我国应依据个人信息保护的实际情况及对等原则，构建数据跨境流动的“白名单”机制，将那些个人信息保护水平与我国相当的国家和地区纳入可与我国自由进行数据传输的名单。在制定“白名单”的过程中，应将“同等保护”作为核心评估标准之一，对不同国家和地区的个人信息保护水平进行细致评估。同时，结合对等原则和我国管理的实际需求，制定以数据保护为基本原则、辅以特定例外情况的综合评估体系，将经过评估的国家或地区纳入数据流动的“白名单”，以降低我国企业与这些国家和地区进行数据流动时产生的不必要的成本。

然而，考虑到短期内我国难以与其他国家建立相互协调的数据流动规制体系，因此，在实施数据跨境流动“白名单”机制的同时，可以参考美国、欧洲与日本、韩国在数据跨境流动方面的谈判经验。在实施过程中，将“白名单”机制嵌入双边或多边贸易谈判之中，根据各国、各地区的具体状况，制定动态、灵活的解决方案。此外，为了进一步提升我国在国际数据跨境流动领域的话语权和影响力，还需加强国际合作与交流。具体而言，可以通过参与国际数据保护组织、加入相关国际协议或公约等方式，积极参与国际数据流动规则的制定和修订过程。同时，加强与主要数据流动伙伴的沟通与协调，共同推动建立公平、合理、透明的国际数据流动秩序。

总而言之，我国应立足当前、着眼长远，从构建“白名单”机制、加强国际合作与交流、完善国内数据跨境合规体系以及提升技术保障能力等方面入手，全面提升我国在国际数据跨境流动领域的影响力和话语权。通过这些措施的实施，将有助于推动我国数据跨境流动的健康发展，为构建数字中国贡献积极力量。

3.3. 从源头治理，强化企业数据出境的合规建设

2023 年 4 月 24 日，中国信息通信研究院发布的《中国数字经济发展研究报告(2023 年)》中指出，在 2022 年我国数字经济规模达到 50.2 万亿元，数字经济占 GDP 比重相当于第二产业占国民经济的比重，41.5% [24]。可见，数字经济俨然成为我国当下以及未来经济增长的重要驱动力，对外数字贸易更是数字经济发展的重要组成。在数字经济时代，我国企业经常面临欧美国家的数据监管和安全审查，唯有从源头治理，增强企业合规能力建设，才能避免被欧美国家的数据法律钳制造成巨额罚款甚至被迫退出海外市场的法律风险。为给出更具可操作性的合规意见，以下将主要对金融、互联网、医疗健康三类涉及数据出境的典型企业提出针对性的合规意见。

首先，在金融数据本地化必要性日渐减弱的环境下，政府不应再一味强化对金融数据出境的管制，

不论是以个人隐私保护为主的欧盟，在其 GDPR 中提出的“拘束性公司规则”(Binding Corporate Rules)，还是推动数据自由流动的美国采取的“组织机构基准”(Organizationally Based)都主张激励金融企业通过企业自律完成企业内部数据管理体系，来实现更为灵活的符合金融企业需要的行为准则，更为有效地规避个人金融数据出境的潜在风险。除要求金融企业自我规制以外，也应当根据中国人民银行发布的《金融数据安全 数据生命周期安全规范》文件赋予金融企业对金融数据从采集到出境的“全周期保护义务”[25]，明确各阶段的数据处理要求，指导金融企业建立相应的数据生命周期预防机制，对其中涉及的个人金融数据坚持以可识别性和去识别、敏感性与脱敏为核心进行处理。

其次，互联网企业要应对目前国际上日趋复杂的数据出境合规形式，互联网头部企业应携手建立良好的合作同盟，通过共享合规信息、交流合规经验等方式强化企业间业务交流，中小型企业应主动向头部企业学习合规经验，积极营造互联网企业间互学合作的良好合规氛围。同时，考虑到部分中小企业由于技术缺陷或资金紧张，自身难以搭建有效的风险评测机制，可以借助第三方专业机构的力量，进行事前风险测试和方案设计，补齐企业合规短板。

最后，对于医疗健康企业而言，在进行医疗数据出境过程中由于其逐利性，导致容易忽视对个人信息的合规保护。而医疗健康数据中涉及的个人信息往往对其用户又较为重要，因此医疗企业亟需构建以数据收集着和使用者责任为核心的保护机制[26]。在构建保护机制的过程中，企业应对重点关注以下几点：第一、形成个人信息可识别评估系统，对涉及的数据进行可识别性评估，对可能带来的隐私泄漏风险采取相应的事先规制措施；第二、对涉及隐私信息的医疗数据采取严格的匿名化措施，确保根据该信息或信息集合体无法识别到信息主体；第三、在数据传输过程中，以引入区块链技术或者其他安全措施来提高数据在传输过程中的安全系数，防止数据被篡改、窃取或者删除。

4. 结语

企业进行对外数字贸易的过程中，巨大的企业数据利益与个人信息保护之间存在利益衡量问题，这就将数据安全推向了比以往任何时期都更容易与国际贸易体制发生冲突的境地。尝试在数据出境合规过程中引入“区块链”新兴技术，最大化保护企业数据在跨境流动过程中的安全，同时防止用户个人信息泄漏，消除数据主体的不安全感，以此在企业数据利益同个人信息保护之间，通过引入“区块链”技术达到制衡。除此之外，我国目前就数据出境合规还存在着内外两个主要问题，一是国内企业数据出境合规意识不强；二是我国在国际上就数据出境合规领域缺乏话语权。根据当下的国内、国际形式，我国应当提高对国内涉外企业，特别是中小企业的财政扶持，打消中小企业面临高昂合规成本时的顾虑。同时，发挥企业领导班子带头作用，学习我国数据合规相关立法，从根源上治理企业缺乏数据合规意识问题。在国际层面，从欧美对中国企业数据出境的钳制，应当意识到欧美将我国政策定义为“数字贸易壁垒”仅是问题表象，真正问题的本质在于各国目前的发展阶段、价值理念、法律制度的不同，才导致中美欧在数据跨境合规和个人隐私保护两方面治理观念上的差异。我国应当借鉴美欧的发展经验，通过 WTO、G20 等国际平台，向外输出中国治理范式，引入数据跨境流动“白名单”机制，争取同各国家和地区根据实际情况制定数据流通方案。总而言之，我国应当从国家安全战略顶层设计出发，向世界提出以我国数据权益为核心的中国话语体系，在企业数据利益与个人信息保护之间寻找利益平衡点，并依托政府、企业自身等多元化主体践行规制路径。未来，数据跨境流动的国际规则不应是某一主体的单方意志体现，而应当是全球各国主体共同参与、协商制定的体现多元化价值观和共识的产物。

参考文献

[1] 孟繁哲. 让海量数据合规高效流通[N]. 人民日报, 2024-03-19(005).

[2] 王融. 数据跨境流动政策认知与建议——从美欧政策比较及反思视角[J]. 信息安全与通信保密, 2018, 16(3): 41-53.

[3] 孙佑海. 我国企业数据合规的理论基础、现实检视与路径选择[J]. 贵州大学学报(社会科学版), 2023, 41(6): 78-87.

[4] 魏倩. 守住隐私!银行数据安全治理升级在行动[N]. 上海证券报, 2021-11-11(003).

[5] 第 47 次《中国互联网络发展状况统计报告》发布[J]. 新闻世界, 2021(3): 96.

[6] 陈颖婷. 筑牢保护个人医疗信息的“防水墙” [N]. 上海法治报, 2024-01-23(A05).

[7] 程啸. 论数据来源者权益[J]. 比较法研究, 2024(6): 28-41.

[8] 王苑. 中国语境下被遗忘权的内涵、价值及其实现[J]. 武汉大学学报(哲学社会科学版), 2023, 76(5): 162-172.

[9] 韦昕彤, 王若凡. 数据经济背景下涉个人信息的企业数据之权利平衡路径——兼“原则普适化+行为场景化”之搭建[C]//上海市法学会. 《上海法学研究》集刊 2023 年第 6 卷——2023 年世界人工智能大会青年论坛论文集. 北京师范大学法学院, 中南财经政法大学法学院, 2023: 74-83.

[10] 康兆逸. 论数据跨境流动安全保护体系的构建[C]//《法治实务》集刊 2023 年第 3 卷——国家安全工作研究文集. 北京: 国际关系学院, 2023: 88-96.

[11] 傅娟. RCEP 对数据跨境流动的规制及我国企业合规应对策略[J]. 现代商业, 2024(2): 36-39.

[12] 伍艺. 欧美个人数据跨境流动规则比较研究[D]: [博士学位论文]. 重庆: 西南政法大学, 2020.

[13] European Parliament and of the Council (1995) Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995.

[14] 王融, 陈志玲. 从美欧安全港框架失效看数据跨境流动政策走向[J]. 中国信息安全, 2016(3): 73-78.

[15] Cate, F.H. (1999) The Changing Face of Privacy Protection in the European Union and the United States. *Social Science Electronic Publishing*, **33**, 173-232.

[16] 梅傲, 潘子俊. 企业跨境数据合规的治理模式、难题审视及合规进路[J/OL]. 情报理论与实践,1-9. http://kns.cnki.net/kcms/detail/11.1762.G3.20240112.1248.002.html, 2024-05-06.

[17] 王燕. 跨境数据流动治理的国别模式及其反思[J]. 国际经贸探索, 2022, 38(1): 99-112.

[18] 金晶. 个人数据跨境传输的欧盟标准——规则建构、司法推动与范式扩张[J]. 欧洲研究, 2021, 39(4): 89-109.

[19] 阙天舒, 王子玥. 美欧跨境数据流动治理范式及中国的进路[J]. 国际关系研究, 2021(6): 76-96, 155.

[20] 王倩, 刘杨钺, 牛昊. 欧美跨境数据流动规制模式对比及博弈分析[J]. 情报杂志, 2023, 42(3): 173-180.

[21] 蔡莉妍. 区块链环境下个人数据权利保护的困境与突破——以欧盟《一般数据保护条例》为例[J]. 北京航空航天大学学报(社会科学版), 2022, 35(6): 43-52.

[22] 吴花平, 刘自豪. 基于区块链的内审数据安全框架构建研究[J]. 会计之友, 2022(6): 155-161.

[23] 马琳琳. 论区块链背景下数据跨境流动的规制路径及中国应对[J]. 对外经贸, 2020(5): 35-39.

[24] 中国信息通信研究院. 中国数字经济发展研究报告(2023 年) [EB/OL]. http://221.179.172.81/images/20230428/59511682646544744.pdf, 2023-04-27.

[25] 许多奇, 董家杰. 我国跨境数据流动中的金融企业合规治理[J]. 吉林大学社会科学学报, 2024, 64(3): 41-60, 235.

[26] 郭子菁, 罗玉川, 蔡志平, 等. 医疗健康大数据隐私保护综述[J]. 计算机科学与探索, 2021, 15(3): 389-402.