□信息技术发展与中国法治创新

我国跨境数据流动中的金融企业合规治理

许多奇 董家杰

[摘 要] 数字经济背景下对金融数据跨境开展必要规制已成趋势，有此内在业务需求的金融企业亟须加强合规应对。基于合规的多重内涵，我国跨境数据流动中的金融企业合规应被建构为一个三维面向的综合治理体系。其一，法制立法是前提，金融数据跨境流动立法的本质即安全与自由的利益平衡，现行立法中金融企业与金融数据的关系错位却导致利益失衡，通过回归立足金融数据本位立场的金融企业合规中心视角方能实现利益再平衡。其二，内部合规是核心，既要贯彻预防性规制理念赋予金融企业强制性合规义务以实现自治的法治化，构筑起立基全周期保护义务的全流程合规体系；又要完善“规制-自我规制-元规制”三环耦合，在框架性原则下促进法治与自治良性互动。其三，行政监管是保障，为因应多头监管困境、金融科技挑战与合规动力不足现状，须由统一监管主体创新监管科技、建立多重合规激励。面对实定法依据缺位和未知动态风险，可引入监管沙盒为上述构想落地提供容错纠错的试验机制。

[关键词] 跨境数据流动；金融数据；金融企业；企业合规；治理体系
[基金项目] 国家社会科学基金项目（22BFX085）
[收稿日期] 2023-03-20 [修回日期] 2024-04-10 [DOI] 10.15939/j.jujsse.2024.03.fx1
[作者简介] 许多奇，复旦大学法学院教授，法学博士；董家杰，复旦大学法学院博士研究生。（上海 200438）

一、问题的提出

数字经济的蓬勃发展是当前全球经济的显著趋势。据统计，2022年全球51个主要国家的数字经济产值占GDP比重高达46.1%，其中我国为41.5%。[①] 数字经济的本质是数据驱动，而数据的价值只有在流动中才得以释放。在信息技术助力经济全球化纵深发展的背景之下，必然引发“跨境数据流动”（cross-border data flow）[②]。2024年3月，国家互联网信息办公室（以下简称

① 数据来源于中国信息通信研究院：《全球数字经济白皮书（2023年）》，http://www.caict.ac.cn/kxyj/qwfb/bps/202401/P020240326601000238100.pdf，2024年1月9日；中国信息通信研究院：《中国数字经济发展研究报告（2023年）》，http://www.caict.ac.cn/kxyj/qwfb/bps/202304/P020240326636461423455.pdf，2023年4月27日。

② 虽然目前对跨境数据流动的定义尚未达成共识，但国际上对其内涵与外延的界定主要包括两类：一类是数据本身的跨境；另一类是境外主体对数据的跨境访问。UNCTAD. Digital economy report 2021-Cross-border data flows and development: For whom the data flow. https://unctad.org/system/files/official-document/der2021_en.pdf, 2021-09-29；张茉楠：《数字主权背景下的全球跨境数据流动动向与对策》，《中国经贸导刊》，2020年12期。

“国家网信办”）正式发布《促进和规范数据跨境流动规定》，传达出数字经济时代促进数据依法有序自由流动的积极信号。大数据时代，跨境数据流动对全球 GDP 的贡献已超过传统货物贸易，逐渐成为全球贸易和投资增长的新支柱。①

数字经济背景下的数据跨境需求是全方位的，不同行业数据的特殊性奠定了跨境数据流动在一般规制之下分业治理的基调，而金融无疑是重要领域之一。一方面，在体量日益庞大的跨国金融服务贸易中，“数字金融”（digital finance）的兴起使得金融数据通过提高运营效率、更好预测欺诈、提高劳动力配置、减少数据中介摩擦等，可以在整个金融服务生命周期内为金融企业创造巨大的经济价值[1]；加之金融业业务复杂多样、市场瞬息万变的特点，导致金融行业数据跨境的数量需求和质量要求较之其他行业均有过之而无不及。伴随着金融高水平开放的稳步推进，金融企业“引进来”与“走出去”双向步伐不断加快，金融数据跨境的业务需求更是水涨船高。另一方面，由于金融数据之上承载着国家和社会公共利益、私人合法权益等多元利益，金融企业不是金融数据的唯一权益主体，因此无论是基于传统的规制公共利益理论，还是对其进行扬弃的规制经济理论[2]，公权力对金融企业的金融数据跨境活动进行规制以克服市场失灵中自我规制的效率障碍，都具有充分的必要性。

有规制必有合规，金融企业合规是金融数据跨境流动规制的必然结果。本文所称金融企业，作为金融数据跨境的实施者，实则指金融数据控制者，即能够单独或者共同确定金融数据处理目的及方式的营利性组织。② 《个人金融信息保护技术规范》第 3.1 条就已在持牌金融机构之外，将更多的个人金融信息处理机构也定义为金融机构。当然，金融数据的范围显然远广于个人金融信息，金融业机构在日常业务开展和经营管理中收集产生的各类数据均可归入金融数据之列。③ 可见金融数据是一种广泛而特殊的数据形式，其并非一个独立的法律类别，而是与一般数据治理框架下的分类重叠，既包括个人金融数据，也包括非个人金融数据，这一区分在以个人权利为中心的金融数据治理范式中具有关键意义。[3]然而在我国，以维护国家数据安全、保护个人信息和商业秘密为前提，以促进数据合规高效流通使用、赋能实体经济为主线的数据基本制度下，对公共数据、企业数据、个人数据开展多元一体规制。④ 金融数据跨境流动规制受此一般范式影响，非个人金融数据和个人金融数据在“重要数据”“个人信息”二分和数据分类分级保护两大共同基石支撑下跨境流动。尽管因权利属性和政策目标不同而导致金融企业所合微观规则不一，但从合规治理宏观体系来看却是共性大于个性。本文据此求同存异，对两者的跨境合规作整体讨论，仅在必要处进行区分。

企业合规（compliance）具有多重内涵。首先，字面上的企业合规就是企业对外部规制的被动遵从，因而更为重要的是所合之规，即通过立法对企业赋予合理义务以为其合规提供依据；其次，企业合规还是一个内部治理问题，强调企业为规避违反法定义务所招致的合规风险而主动将

① 详细数据参见 IBM. Digital trade and cross-border data flows. http://mddb.apec.org/Documents/2021/CTI/TPD1/21_cti_tpd1_002.pdf, 2021-05-18.

② “数据控制者”概念最早由欧盟《个人数据处理及自由流动保护指令》提出，并为《通用数据保护条例》所沿用。Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Article 2; General Data Protection Regulation (GDPR), Article 4. 我国《个人信息保护法》中所称的“个人信息处理者”实则亦指个人信息的“控制者”。参见《中华人民共和国个人信息保护法》第 73 条第 1 项。

③ 关于金融数据、个人金融信息的定义，参见中国人民银行：《金融数据安全　数据安全分级指南》，JR/T 0197-2020，第 3.10 条、第 3.11 条。在现有法律文件与研究文献中，通常将“个人金融信息”与“个人金融数据”混用，本文在表述上亦不作严格区分，但严格来说后者当为前者原始的数字化载体。

④ 2022 年 12 月 2 日《中共中央　国务院关于构建数据基础制度更好发挥数据要素作用的意见》。

合规管理作为内控的有机组成部分，建立起完备的合规计划；最后，企业的自我治理也极易失灵，故而法律规则所提出的合规要求尚需要行政监管主体依法对企业落实情况进行监督和管理，乃至最后刑事手段的介入。[4]7-12可见，针对企业合规已呈现出视角的分化，但不同视角之间并非割裂而是相辅相成，共同构成了一个综合多重制约和激励机制的治理体系。我国跨境数据流动规制中的金融企业合规也应当被定位为一个综合治理体系，包含法制立法、内部合规和行政监管三个主要面向，且三个面向之间以制约和激励作为金融数据控制者的金融企业为核心环环相扣、层层递进。

遗憾的是，在现有跨境数据流动相关研究中，尚对企业合规存在定位上的偏差。或基于立法论将企业合规理解为一种合规成本而对我国和域外的跨境数据规制模式进行评析，或单从企业治理的角度论证企业在数据跨境规则框架内如何构建合规体系从而既满足自身数据跨境需求又规避合规风险。既少有对金融企业之金融数据跨境的特殊关照，又缺乏对企业合规深入的体系性理解。党的二十大报告强调："改革开放迈出新步伐，国家治理体系和治理能力现代化深入推进，社会主义市场经济体制更加完善，更高水平开放型经济新体制基本形成。"[5]31据此，本文欲纠正上述偏差，试从法制立法、内部合规和行政监管三个角度，对如何构建我国金融数据跨境流动规制中的金融企业合规治理体系提出初步构想。

二、金融数据跨境流动立法：回归数据本位立场的合规中心视角

（一）利益平衡：安全与自由的冲突与融合

国家利益的多样性与冲突性，导致了金融数据跨境流动国际协调机制的零散支离，形成统一的国际规则还任重道远，因而当前金融数据跨境流动主要由各国国内法进行规制，形成了碎片化的国别模式。其中，欧盟和美国两大模式无疑最具话语权和影响力，并在研究中分别被冠以"安全"和"自由"的价值标签。然而，有原则恒有例外，安全与自由均是相对的，两者并非绝对冲突，而是日益呈现出相互融合的趋势。

欧盟金融数据跨境流动立法的价值标签是"安全"，并且是狭义上的人权与隐私安全。欧盟视隐私为一项基本人权的观念根深蒂固①，进而将保护承载隐私的个人数据奉作对数据主体基本权利之保障。此种价值理念在欧盟金融数据跨境流动立法中表现为，其并未为追求金融监管的一般价值目标而对金融数据跨境进行特殊规制，而是将其中的个人金融数据纳入了以《通用数据保护条例》（GDPR）为核心的个人数据跨境统一规则框架之下。GDPR 被誉为史上最严厉的隐私安全保护法律，其第 45 条确立的"充分性认定"是实现个人金融数据跨境首推的也是最便捷的方式，但由于在评估过程中需要严格考虑多种因素，截至目前仅有 15 个国家（地区）获得了此类充分性认定。② 为此，GDPR 第 46 条在"充分性认定"之外，额外增加了"基于适当安全保障的转移"（transfers subject to appropriate safeguards），提供了多样化的金融数据自由跨境流动途径，以免对数字经济发展产生不利影响。同时，GDPR 为推进单一数字市场战略，还强调促进

① Charter of Fundamental Rights of the European Union, Article 7.

② 当前获得欧盟委员会充分性认定的具体国家（地区）包括安道尔、阿根廷、加拿大（商业组织）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、韩国、瑞士、英国（根据 GDPR 和 LED）、美国（加入欧盟-美国数据隐私框架的商业组织）和乌拉圭。European Commission. Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, 2024-01-15.

个人金融数据在欧盟内部的自由流动。《关于内部市场支付服务的指令》也旨在专门推动欧盟内部金融账户信息的合作与交换。① 而针对不涉及隐私的非个人金融数据，《非个人数据自由流动条例》（RFFND）不仅强调其在欧盟内部的自由流动原则，对超出欧盟范围的跨境流动也未规定统一的必要条件。

美国则以“自由”为其金融数据跨境流动立法的价值标签。在白宫 2011 年发布的《网络空间国际战略》中，美国就旗帜鲜明地将“信息自由流动”作为基本原则。② 基于此，在国际层面，美国凭借其强大的政治经济影响力，竭力在双边和区域贸易协定中推动金融数据跨境自由流动；就国内法而言，尽管美国也开始逐渐重视隐私保护，但无论是联邦层面的《公平信用报告法》《金融隐私权法》《金融服务现代化法案》，还是州层面的《加州消费者隐私法案》，虽都从金融消费者保护角度逐步明确金融企业的隐私保护要求并日臻严格，但对金融数据跨境流动的额外限制始终持留白态度。[6] 然而值得注意的是，美国在促进金融数据自由流动原则之外也基于安全考虑设置了相应的限制性例外：一方面，其主导的双边或区域贸易协定往往存在隐私保护或审慎监管例外条款，典型者如 TPP（并为 CPTPP 所继受）；另一方面，在其国内法中也出于国家安全的考量对金融数据跨境作出了限制，例如美国自 2010 年开始建立和实施受控非密信息（controlled unclassified information，CUI）管理制度，CUI 共分为 20 个类别、126 个子类，金融数据是其中重要一类③，在包括出境等方面受到较为严格的限制。

通过上述分析可知，基于原则的抽象性和利益的多元性，无论是安全原则还是自由原则在金融数据跨境立法中并非以“全有或全无”的方式加以适用，而是原则与例外相济，冲突与融合并存。[7] 因此，在金融数据的跨境流动立法中，重要的并非在安全与自由中明定孰为原则而孰为例外，而是为平衡金融数据本身所承载的多元主体的多重利益，在按照一定标准进行权衡的基础上进行利益整合。对此，各国应坚持“两点论”，基于本国国家安全形势、金融开放水平、数字产业发展情况等多种因素考量作出利益权衡与抉择，以谋求安全与自由之间的中道。

（二）利益失衡：金融企业与金融数据的关系错位

我国的金融数据跨境流动规制立法起步较晚，逐步形成了“一般+特殊”的规制模式。《中华人民共和国网络安全法》（以下简称《网络安全法》）《中华人民共和国数据安全法》（以下简称《数据安全法》）和《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）共同构筑了规制金融数据跨境的一般上位法框架。其中，《网络安全法》第 37 条（以下简称“37 条”）奠定了我国跨境数据流动规制的基本原则和框架。该条不仅提出了具有数据控制者含义的“关键信息基础设施运营者”（CIIO）概念，作出了“重要数据”和“个人信息”两类重要的数据范围分类，创设了数据跨境程序意义上的“安全评估”机制[8]，还被《数据安全法》第 31 条、《个人信息保护法》第 40 条所引用和重申。正是由于 37 条拥有如此提纲挈领的重要意义，其所存在的问题便会引发连锁反应，其中最甚者便是因金融企业与金融数据关系错位所导致

① 《关于内部市场支付服务的指令》在规定“应允许账户信息服务提供商等受益于‘护照规则’而可以跨境提供服务”的同时，要求“账户支付服务提供商除非出于客观合理且有充分证据的理由（如客户未授权），否则不得拒绝账户信息服务提供商或支付发起服务提供商等第三方访问支付账户”。Directive（Eu）2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market，Amending Directives 2002/65/EC，2009/110/EC and 2013/36/EU and Regulation（EU）No 1093/2010，and Repealing Directive 2007/64/EC，Whereas（48），Article 68.5.

② The White House. International strategy for cyberspace：Prosperity，security，and openness in a networked world. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf，2011-05-16.

③ The U.S. National Archives and Records Administration. CUI categories. https://www.archives.gov/cui/registry/category-list，2024-01-31.

的利益失衡。

《网络安全法》作为我国网络安全领域的基本法，贯穿了“等级保护”理念，在把“信息安全等级保护制度”升级为“网络安全等级保护制度”的基础上，规定了“关键信息基础设施保护（CIIP）制度”。加之网络、数据与个人信息这三个概念本身所具有的关联重合性，因此37条在数据跨境流动规制上也自然而然地采取了“关键信息基础设施（CII）标准”，即在需要进行出境安全评估的重要数据和个人信息前加上了“关键信息基础设施运营者”（CIIO）这一主语限定。金融作为《网络安全法》第31条明确列举的重要行业和领域，金融企业极易被认定为CIIO，但问题在于，作为CIIO的金融企业是一个整体概念，是综合考虑其控制的所有数据后作出的认定，是一种数据控制者本位立场；而金融数据的跨境却是个别进行的，因此需要采取数据本位立场，即考虑数据本身的性质。以作为主体的金融企业来界定作为客体的金融数据之保护，便发生了关系的错位，由此产生了以下后果：

首先，以CIIO来界定需要出境安全评估的金融数据，其本意或旨在强调需经此严格出境程序的数据应当如CII定义那般具有危害国家安全、国计民生、公共利益的性质，但“重要数据”这一概念本身就蕴含了这层含义，反而多此一举，并导致《数据安全法》第31条需要对“其他数据处理者”出境“重要数据”进行补充说明，才使“重要数据”的跨境规则得以周全。在《数据出境安全评估办法》（以下简称《评估办法》）中，就摒弃了这一数据控制者本位立场，而直接采用了不带有任何价值判断色彩的“数据处理者”一词。其第4条综合前述两法，不区分是否为“关键信息基础设施运营者”而直接规定“数据处理者向境外提供重要数据”需要进行安全评估。因此，金融数据出境仅需考虑其本身是否属于“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据”①，而与金融企业的CIIO属性并无绝对关联，反映出对数据本位立场的回归。

其次，错误的金融企业本位立场还扩大了需要出境安全评估的个人金融数据范围，加重了金融企业的合规负担。根据当前37条的表述，CIIO在境内收集和处理的所有“个人信息”都须遵循“原则本地存储+例外确因业务需要须经安全评估”的跨境程序，因此部分金融企业所控制的所有个人金融数据便都落入了此范围。然而问题在于：一方面，个人金融数据本身就可据其不同敏感程度进行分级②，部分个人金融数据根本不会危及国家安全、公共利益，不应也不必一刀切地要求安全评估；另一方面，这也将导致《个人信息保护法》第38条所确立的个人信息出境“四选一”的选择性条件在一定程度上被架空，而使“安全评估”成为唯一的必要性条件。[9]换言之，虽因个人金融数据之上承载着各类私益而在跨境时需要额外设置相应程序③，但毕竟个人金融数据属于事实判断，而就是否须经安全评估这一最严格的出境程序则应立基于数据本位进行价值判断，即判断该数据在跨境过程中“一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度”④。因此，“金融重要数据”和“个人金融数据”两者之间并非截然的二分关系，而是存在交叉关系，且在出境安全评估语境下

① 国家互联网信息办公室：《数据出境安全评估办法》，国家互联网信息办公室令第11号，第19条。

② 《个人金融信息保护技术规范》根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别。参见中国人民银行：《个人金融信息保护技术规范》，JR/T 0171－2020，第4.2条。

③ 如《个人信息保护法》要求个人信息处理者必须在明确告知的基础上取得个人的单独同意（第39条），并且采取必要措施以保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准（第38条第3款）。

④ 《数据安全法》第21条。

对“金融重要数据”的判定更具现实意义。37 条在错误的金融企业本位立场之下将两者并列显然易生混淆，导致《信息安全技术　重要数据识别指南（征求意见稿）》第 3.1 条作出了“重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据”这样模棱两可的界定，而《信息安全技术　数据出境安全评估指南（征求意见稿）》（以下简称《评估指南》）将个人金融数据统归入重要数据之列却又矫枉过正。①

综上，虽然金融企业作为金融数据跨境的主体理应受到重视，但在规制金融数据跨境时仍应注意出境客体和出境主体间应有的层次，在客体界定层面就引入金融企业无疑是一种关系的错位，进而导致数据本位的缺失，结果就是出境行为规制有趋于“本地化”之嫌。这不仅在立法层面就直接因禁止性规定有余而因势利导不足，导致对金融企业的激励不相容[10]，不利于我国的金融数字化转型和金融开放；更可能因过重的合规负担迫使金融企业将金融数据的违规出境作为一种必要的经营成本而采取理性违法策略[11]，使得相关规定形同虚设。在出境行为和责任承担之间，公权力的过度提前介入，目的固然在于把好安全关，但也会因为清单式的审查方式、试错空间的提供，而使金融企业的数据出境过度依赖于官方的评估结果，降低合规的自主性、全面性和灵活性，最终事与愿违。良性的合规市场无从培育和发展，政府行政负担和企业合规负担亦同步增长。究其根本，正在于金融数据控制者层面的整体安全不当压制金融数据出境层面的个别自由，造成了所谓的利益失衡。

（三）利益再平衡：立足数据本位的企业合规中心视角

错误的金融企业本位立场造成了我国金融数据跨境流动立法中的利益失衡，而在数据本位立场下回归企业合规中心视角则是实现利益再平衡的不二法门。即遵循从“传输什么”到“谁来传输”再到“如何传输”的逻辑顺序，在以数据本位为指导建立数据分类分级的基础上，以具有传输主体和合规主体双重身份的金融企业为核心，为其匹配不同程度的金融数据跨境权利义务。

数据分类分级保护制度能够促进数据的充分利用、有序流动和安全共享，是加强数据治理的前提与基础，《数据安全法》第 21 条更是在法律层面上对此进行了确认。然而现实是，一方面金融领域的重要数据目录抑或一般数据清单尚付阙如，且前者在实践中存在泛化倾向，有违“法不禁止即自由”的基本法治原则②；另一方面，在出境安全评估之外，非重要、非个人数据出境机制却受到忽视，使得金融企业的数据跨境合规义务出现割裂断层。尽管《证券期货业数据分类分级指引》《金融数据安全　数据安全分级指南》等推荐性标准对金融数据的分类分级提出了方案，但仍停留于“传输什么”的层面，既没有正视金融企业差异化的合规建设水平和数据安保能力作出区别对待，也未与跨境直接挂钩而提出金融企业针对不同级别的金融数据应当“如何传输”。因此，当务之急便是在采取正面清单取并集与负面清单取交集相结合两端逼近的动态调整方式明定数据界限的前提下，思考针对不同类型级别的金融数据，如何为不同金融企业在认证的基础上提供有区别的数据出境权限和途径，并匹配相应的数据安保义务，以实现安全与自由之间的利益再平衡。退一步而言，若坚持安全评估的必要性，则可考虑在其框架下结合金融企业认证机制开展区别性评估，对经认证合规体系健全有效、数据保护水平较高的金融企业简化评估条件、压缩流程时限、增加评估有效期等，甚至允许以备案替代实质审查，由此提高评估效

① 参见国家质量监督检验检疫总局、国家标准化管理委员会：《信息安全技术　数据出境安全评估指南（征求意见稿）》，20173853-T-469，附录 A.19。

② 对此，国家网信办发布的《促进和规范数据跨境流动规定》第 2 条规定：“未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估”。重要数据目录制定的重要性更加凸显。

率，将有限的规制资源集中于真正可能危及国家安全和公共利益的金融数据出境活动，破解当前过低的评估申请通过率对金融企业开展国际业务的桎梏。

在方法论上，金融数据的跨境流动规制是国家基于多重安全因素考量对金融企业经营活动的干预，但由于包含国家安全、公共利益、私人权益在内的安全因素本身所固有的原则性和模糊性，为防止公权力的恣意性，应通过比例原则加以限制。[12] GDPR 就为了协调个人数据使用与其他同样重要的基本权利，而强调要运用比例原则加以平衡。[13] 比例原则在立法中的适用就是三个子原则循序渐进的利益衡量过程，尤其需要注意金融数据跨境流动规制中的利益层次。① 在利益衡量的适当性原则层面，凸显的是金融数据跨境流动立法整体上的价值取向，彰显其制度利益，具体体现为一种安全和自由在价值位阶上的静态权衡，而在开展规制的语境前提下，安全价值的正当性显然已得到承认。至于要根据“权衡法则”（the law of balancing）论证应在多大程度上限制自由原则从而在多大程度上满足安全原则，则属于必要性原则和狭义比例原则的管辖范围。此时静态的价值位阶比较显然已失去作用，而应深入到作为合规主体的金融企业而动态考察其具体利益，因为整体上的安全与自由价值最终落实到金融企业便表现为其合规成本与收益。额外出境限制的施加必要性唯有在金融数据本身属性之外纳入考量金融企业的数据保护现状方得以真正确定，具体合规义务的赋予也需考虑金融企业的可操作性。故而，应在保证金融企业切实可行的基础上实现数据分类分级与金融企业分类分级的双向匹配，在保证安全价值得到最大程度满足而自由价值受到最小程度损害的前提下，使合规成本尽可能小于合规收益，从而激发金融企业在金融数据跨境中的合规积极性。

总之，金融企业合规在金融数据跨境流动立法中不应被简单地视为一种合规成本而归入利益天平的一端，其恰恰是在这架安全与自由、成本与收益互为两端的天平上左右移动的游码。立法者所需做的，就是在金融企业中心视角之下动态地将合规这颗游码拨到恰到好处的位置，既不至于因过度放纵自由而使金融企业无规要合进而危及安全，也要为企业合规自治留下必要余地，不因过严监管的对抗性立场而完全排除了协作性的新治理方式，而使企业合规在虚假的责任委托面纱下完全沦为外部“硬法”（hard law）的工具。[14]

三、金融企业数据跨境合规：法治与自治良性互动的规制体系

（一）强制性合规义务：自治的法治化

在金融数据本地化必要性日益丧失的背景之下，政府一味加强对金融数据跨境的管制，往往会取得适得其反的效果。正确的出路，则是在前述以金融数据分类分级为基础的利益再平衡过程中，充分发挥金融企业合规效能，实现其“自我监管”（self-policing）② 乃至“自我规制”（self-regulation）③。这也正体现出金融企业数据跨境合规的核心含义：金融企业通过完整内部治

① 在立法利益衡量中，当事人的具体利益、制度利益和社会公共利益形成了一个有机的层次结构，并且是一种由具体到抽象的递进关系。参见梁上上：《利益衡量论》，北京：北京大学出版社，2021 年，第 120 页。

② 自我监管（self-policing），是指将合规监管和不合规报告的职责从政府转移至私主体，使企业等私主体自行监管其自身的合规情况，乃至自愿报告不合规情况。Short J L, Toffel M W. Coerced confessions: Self-policing in the shadow of the regulator. *The Journal of Law, Economics, and Organization*, 2008, 24 (1): 45-71.

③ 尽管关于自我规制（self-regulation）有多种理解，但其本质上是当前“去中心化规制”（decentred regulation）趋势下的一种体现，强调并非由政府来直接设定行为标准并进行监管，而是一种自己为自己设定行为准则的回应型规制。Black J. Decentring regulation: Understanding the role of regulation and self-regulation in a post-regulatory world. *Current Legal Problems*, 2001, 54 (1): 103-146.

理体系的建立来实现对金融数据跨境合规风险的有效防范、识别和应对。[15]

金融企业的数据跨境合规是法治下的自治，在法律要求之外彰显着独特价值。且不论本就崇尚金融数据自由流动的美国模式，采取了以“问责制”（accountability）为基础的“组织机构基准”（organizationally based），强调通过行业和企业的自律来实现数据保护要求[16]；即便是强调充分性保护的欧盟，在其 GDPR 中也将“拘束性公司规则”（binding corporate rules）作为提供适当安全保障的方式之一①，使得金融企业能够通过制定适合自身特殊需求的行为准则来实现更为灵活的个人金融数据跨境。在我国，针对金融重要数据跨境的安全评估机制可谓是政府强力控制的典型，但从《评估办法》的“自评估”要求②中却仍可觅见自治的意涵。

金融企业之所以愿意进行数据跨境合规，远非社会责任的承担可简单解释，而是更多地为合规背后所固有的一套内在激励机制所驱动。虽然社会责任的承担被视为企业合规的核心价值，但是以利益为根本动力的经济行为通常是与道德伦理无涉的。从正面来说，金融企业作为一个理性的“经济人”，为了以适当的成本实现最优合规，势必会衡量内部监督的实施成本与预期收益，呈现出典型的“市场驱动”特征。[17]从反面来说，当前我国正在逐步完善金融数据保护机制，一旦违规跨境传输金融数据，金融企业不仅将承担相应的民事责任和行政处罚，甚至受到刑事追究，因此为避免上述违规风险，金融企业具有建立有效金融数据跨境合规体系的强大动力，以有限的合规成本置换高昂的违规成本。

更为重要的是，在数据互联的经济全球化背景之下，金融企业的数据跨境合规具有境内和境外双重面向。截至 2021 年底，全球 194 个国家中有 137 个进行了数据和隐私保护立法③，其中大部分均包含数据跨境规则，但理念立场与具体规则各异。如此复杂的外部法律环境使我国金融企业面临多样化的境外合规场景：其一，在“走出去”过程中，金融企业势必基于属地原则受到东道国金融数据跨境规则的管辖。其二，即便是境内的金融企业，也会因国内法间接的域外效力而必须将域外数据保护规则纳入合规考虑，典例如《个人信息保护法》对境内个人信息处理者提出的境外接收方同等保护标准保障要求。④ 其三，当前各国数据立法管辖权扩张的普遍趋势给我国金融企业带来了境外合规新考验，欧盟 GDPR 的“设立机构”标准和“目标导向”标准、美国“云法案”（CLOUD Act）的“数据控制者”标准等均从传统的属地和属人管辖延伸出了新的域外管辖连接点。可以说，金融企业不仅面临“走出去”和“引进来”的双向合规风险[18]，更面临着外部管辖规范意义上的多向合规挑战。尽管各国管辖和规则上的冲突固非金融企业能够解决，但正所谓“授人以鱼不如授人以渔”才能够“以不变应万变”，成熟有效的金融数据跨境合规体系至少可以助其规避对其不利的连接点，提早识别合规风险，防止落入不同法域夹击下的合规困境。

强制性合规义务的赋予，则正实现了自治的法治化。当前，我国金融企业数据保护意识仍较欠缺，金融数据安全事件时有发生，仅金融监管总局 2023 年开出的涉及信息保护、数据治理、信息系统的罚单就有近 40 张。⑤ 金融数据跨境这一新兴领域的合规意识和合规措施更是遑论完

① GDPR, Article 46, Article 47.

② 参见国家互联网信息办公室：《数据出境安全评估办法》，国家互联网信息办公室令第 11 号，第 5 条。

③ 数据参见 UNCTAD. Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, 2021-12-14.

④ 《中华人民共和国个人信息保护法》第 38 条第 3 款。

⑤ 孙海波：《最全数据！2023 年金融监管总局行政处罚!》，https://mp.weixin.qq.com/s/C0M-NCb-cZhge4d4NaJ58g，2024 年 1 月 30 日。

备。其背后的原因是，企业合规最初产生的目的本就在于通过自我监管防止政府过度干预，带有明显的“去监管”（deregulation）色彩，而金融企业作为具有强烈营利性的有限理性主体，在合规机制内在激励不足的情况下，就会缺乏金融数据跨境合规的动力，而完全转向逃避监管。因此，在通过内在机制激励金融企业合规的同时，以“行政主导”的方式赋予金融企业强制性合规义务，无疑对于督促其“从无到有”地建立起基本的金融数据跨境合规体系具有不可替代的积极意义。[11]国外调查结果也显示，对于营利性机构来说，其不可能投资于成本高昂但收益不明确的自愿性合规计划，但有可能将有限的资源用于强制性合规计划。[19]某种意义上，强制合规义务辅以相应的法律责任，也为金融企业创设了一种基于避免惩罚考虑的外部激励机制，从而以法治化的方式确保合规计划的有效实施。

我国已初步建立起了强制性的金融企业数据跨境合规体系。首先，从行业领域专项合规看，我国对强制合规的推行便始于具有高风险特点和严监管传统的金融行业，并逐步通过银行、保险、证券等各金融专门领域合规管理指引（办法）的颁布，基本构建起了金融业的合规管理制度体系。① 其次，从风险事项专项合规看，数字经济时代数据安全问题日益突出，数据合规越来越受到重视。《网络安全法》《数据安全法》《个人信息保护法》均在专章中规定了企业独立的数据合规义务②，标志着数据领域强制合规制度的建立。同时，针对上述两者的交叉领域，即金融业的数据合规，原银保监会还发布了针对数据治理的专门指引，明令银行业金融机构在公司治理中建立起自上而下、协调一致的数据治理体系。③《刑法修正案（九）》新增的“拒不履行信息网络安全管理义务罪”对于金融企业的合规内控，更是在行政主导之外增添了强烈的刑事威慑。无论是直接提供金融服务的金融机构，抑或在金融数据跨境过程中提供接入、计算、存储、传输等服务的金融科技公司，都是适格该罪的“网络服务提供者”④；金融企业的金融数据跨境合规义务从解释上亦可归入一般“信息网络安全管理义务”之列[20]；而无论是个人金融数据违规出境致使金融消费者信息泄露造成严重后果，还是非个人金融数据违规出境产生危害国家安全、扰乱金融秩序等严重情节，均满足实害结果要件。基于行政义务与刑事义务的内在关联性，风险刑法观之下的强制性数据刑事合规义务由此得以确立，金融企业的金融数据违规出境行为可能同时触犯该罪与其他具体罪名，虽一事不二罚，但至少在数据流动基础上谋求数据安全的刑事法网得以周密。然而，这一受到行刑多方重视的体系当前仍存在两个主要问题：一是面对金融数据控制者范围的扩张，尚欠缺针对所有金融企业普遍适用的数据合规指引；二是随着金融数据跨境合规标准逐步提高、执法司法机制日益严格，还未就金融数据跨境专门发布强制性专项合规要求和指引。金融企业的金融数据跨境合规法治化、精细化程度仍有待进一步提升。

（二）预防性规制：立基全周期保护义务的全流程合规体系

金融企业的数据跨境合规，是一种针对金融数据跨境风险的预防性规制手段。其背后的理论依据在于风险预防性原则，即身处风险社会必须坚持防患于未然，采取预防措施以避免风险的实害化。且相较于同样旨在预防风险的事前评估等外部强制措施，自内向外的合规在效率性、灵活

① 早在2006年我国就以巴塞尔银行监管委员会的《合规与银行内控部门》为蓝本颁布了《商业银行合规风险管理指引》，随后又分别于2016和2017年发布了《保险公司合规管理办法》（前身为2007年以《商业银行合规风险管理指引》为模板发布的《保险公司合规管理指引》）和《证券公司和证券投资基金管理公司合规管理办法》。

② 参见《中华人民共和国网络安全法》第三章“网络运行安全”和第四章“网络信息安全”、《中华人民共和国数据安全法》第四章“数据安全保护义务”、《中华人民共和国个人信息保护法》第五章“个人信息处理者的义务”。

③ 参见银保监会：《银行业金融机构数据治理指引》，银保监发〔2018〕22号，第4条。

④ 最高人民法院、最高人民检察院：《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》，法释〔2019〕15号，第1条。

性、持续性等方面更具优势。

与预防性规制相对应的是事后惩罚性规制，强调以禁止和惩罚法益侵害行为为手段实现法益保护之目的。金融数据跨境领域本身并不缺乏事后惩罚性规制：在公益保护方面，《国家安全法》第 25 条要求实现重要领域数据的安全可控，因金融数据跨境危害国家安全、公共安全的行为，不仅将面临行政处罚，还可能触犯《刑法》相关罪名；而针对私益保护，一旦涉及侵犯隐私、商业秘密等合法权益，更需要承担民事侵权责任。即便如此，在金融数据跨境中仍要坚持风险预防原则，是因为事后惩罚性规制往往在相关法益受到侵害后才会介入，因而在该领域具有极强的不适用性：一方面，金融数字化背景下金融行业的数字亲和性获得飞跃式发展，金融企业在不同场景下广泛吸收和产生了大量来源众多、结构复杂的各类金融数据，加之金融数据天然的敏感性，使得其在跨境过程中具有极大的风险不确定性。如果一律采用事后惩罚的方式进行规制，极易发生难以事后补救的严重后果。另一方面，跨境这一因素的叠加更是阻碍了此种事后规制手段的有效实施。事后规制启动的前提是发生实害结果（或至少产生危险），而金融数据跨境场景中境外主体的危害行为和损害结果大多发生于境外。虽然针对侵犯我国国家安全、公共利益或者私人合法权益的行为，《网络安全法》第 75 条、《数据安全法》第 2 条、《个人信息保护法》第 42 条等以及《刑法》第 8 条等均出于拓宽域外管辖范围、强化数据主权的考虑而确立了保护管辖原则，但即便取得管辖，之后的域外调查取证、执行等依然道阻且长，在寻求民事救济时还会涉及国际私法中的管辖法院确定、法律适用等难题，维权成本高、获得救济难。综上，事后惩罚性规制只宜作为金融数据跨境规制的“退路”[21]，而以合规为代表的预防性规制，才能有效降低金融企业违规数据出境行为所带来的净社会成本。有效的内部合规体系辅之以持续性的事中监督和精准化、严格化的事后问责，便可充分稀释事前限制金融数据跨境自由流动的必要性。

金融企业通过合规来预防金融数据跨境风险，固然应主要着眼于跨境阶段，但更为重要的是树立风险预防全局观，建立全流程金融数据合规体系。所谓全流程，是指金融企业的金融数据保护合规，要贯彻到数据业务的全线程，实现对数据生命周期的全覆盖。① 对此，GDPR 在其第 25 条确立了“设计和默认的数据保护”（data protection by design and by default）原则，主张在产品或服务设计之始就将个人数据保护嵌入其中，旨在借此将隐私保护纳入各种处理个人数据的技术和应用程序的完整生命周期之中[22]；我国《数据安全法》第 27 条也强调“建立健全全流程数据安全管理制度”。虽然金融数据的跨境流动主要涉及传输和提供，但是金融数据本身固有之生命周期链条上的每一步都环环相扣而不能孤立看待：一方面，各个环节之间具有风险传导和放大效应，例如金融数据收集环节作为生命周期的“源头”，一旦收集行为违规，之后的每一环节无论多么合规都无法洗涤违规的“原罪”[23]，且随着流程的推进，数量的汇集叠加跨境因素，更会放大先前环节违规行为的风险性；另一方面，金融数据具有广泛的出境可能性，非以跨境传输与访问为直接目的的处理活动同样包含着潜在的间接出境风险。

企业合规的原意就是“遵循”，全流程金融数据合规体系的建立离不开全周期金融数据保护义务的赋予。在合规计划中居于核心地位的合规政策，本质上就是外部行为义务的内部化。因此，只有赋予金融企业涵盖金融数据出境“事前-事中-事后”的全周期保护义务，金融企业建立全流程金融数据合规体系才有规可依、有的放矢，从而使合规自治有了法治保障。目前，基于数据本身的物理属性以及数据主体和处理者在控制力上的现实差距，我国《网络安全法》《数据

① 数据业务全线程具体包括研发、设计、生产、销售、服务等，数据生命全周期具体包括收集、存储、使用、加工、传输、提供、公开、删除等。参见毛逸潇：《数据保护合规体系研究》，《国家检察官学院学报》，2022 年 2 期。

安全法》和《个人信息保护法》及其配套规范立足“行为主义”已从整体上针对金融企业等数据处理者作出了覆盖数据生命周期的行为规范安排。[24]同时，针对金融数据这类特殊数据，中国人民银行还发布了《金融数据安全　数据生命周期安全规范》，明确规定了金融数据采集、传输、存储、使用、删除等各阶段的处理要求，用以指导金融机构建立完善的金融数据生命周期防护机制。① 当然，出境等数据生命周期各环节的具体保护要求，应以金融数据的分类分级为基本依据并结合金融企业能力现状进行细化明确，既要未雨绸缪也要防止过犹不及。其中，个人金融数据以可识别性和去识别化、敏感性与脱敏为核心，而非个人金融数据则以其他保护法益的确认和危害程度的判断为要点。

（三）框架性规制：“规制-自我规制-元规制”的三环互动

全周期金融数据保护义务之下的金融企业数据跨境合规，仍停留在自我监管的阶段，属于金融企业对外部性公权规制的落实。此种“命令与控制型规制”（command and control regulation）②之下相对被动的合规尚不能满足金融数据跨境的规制要求：首先，由于我国金融数据跨境规制起步较晚，在立法现状上表现为因缺少顶层设计系统而较为零散，尤其是在出境安全评估重要数据范围不明确、缺乏执行细则的情况下，针对不同类别层级金融数据的出境要求尚未明晰，无法为金融企业直接提供明确的合规指引；其次，立法者等外部规制主体因其有限理性，面对金融数据数量的爆炸式增长和处理风险的不断加剧，规制手段存在滞后性实属必然。因故，加强金融企业的自我规制，是完善我国金融数据跨境规制体系的必由之路。

所谓金融企业的自我规制，强调在外部公权规制缺位的情况下，将命令和结果强加于自身。[25]150在自我规制过程中，金融企业既是自我的立法者，也是自我的监督执行者，在违规时还是自我的裁判者，从而实现了规制主体和规制对象双重身份的合一。在金融数据跨境流动中，金融企业的自我规制具有如下优势：第一，面对多场景的金融数据跨境，金融企业能够根据自身特殊需求，利用专业经验克服传统外部公权规制的失灵，从而实现更具弹性与效率的动态规制[26]；第二，金融企业更强的自主性往往伴随着更高的服从性[27]，从而在提高其主体责任感的同时更好实现金融数据跨境的规制目标；第三，在国家公共资源紧张的当下，金融企业的自我规制可以有效降低规制成本，减轻监管部门的行政负担。然而，自我规制也并非完美，其在透明度、可靠性、问责性等方面均面临质疑，甚至可能牺牲公共利益而满足私人利益而被认为具有低公共性。因此，在自我规制和公权规制之间并不存在明确的二分法，而是存在一个连续统一体，纯粹的自我规制同纯粹的公权规制一样都是不存在的。[28]两者并非相互替代之对立关系，而应交融互补。基于金融企业合规法治与自治的双重视野，更为重要的是建立起“规制-自我规制-元规制”“三环”（triple loop）互动的规制框架。[29]xi

首先，在金融企业自我规制的前端，必要的公权规制不可或缺。但是此种公权规制不应是传统上大包大揽、事无巨细的介入干预，而应表现为一种重在设定原则目标的框架性规制，唯有如此才能适应既发挥自我规制的专业性和灵活性，又强调并用公权规制的基本趋势。[30]诚然，不能否认“宜细不宜粗”的金融数据跨境立法是提高安全效力的有力保障，也符合从粗放到精细的现代立法趋势，在全周期金融数据保护义务的基础之上，根据金融数据分类分级为不同金融企业设定差异化的出境权利义务本就体现了此种理念。然而，面对金融数据跨境本身处于快速发展的

① 中国人民银行：《金融数据安全　数据生命周期安全规范》，JR/T 0223-2021，引言、第7条。

② 命令与控制型规制在过去一直作为政府规制的主导手段，是一个由各种法律、行政法规、许可程序、标准、司法裁判和其他可执行政策组成的复杂网络，并以各种惩罚为基础。Sinclair D. Self-regulation versus command and control? Beyond false dichotomies. *Law & Policy*, 1997, 19（4）: 529-559.

动态过程之中，为实现既确保法律到位以防社会失范，又能够为新现象的发展留有余地，先行根据规制目标搭建框架性秩序的粗放型立法，以为金融企业的金融数据跨境自我规制的提供原则性指导，再逐步实现精细化立法，则是缓解当前规制落后与出境需求旺盛之间矛盾更为现实和有效的路径。[31]在与金融数据跨境相关的国际规则中，《亚太经合组织隐私框架》（APEC Privacy Framework，以下简称《隐私框架》）就是一个由一系列信息隐私原则构筑而成的保护框架①，这固然有因其属于推荐性指南而有待各国国内法进一步细化之考量，但根本上还是因为其本身就采取了以企业为中心的“数据控制者担保模式”[32]，因而只需以原则形式为企业的自我规制提供目标导向。我国《个人信息保护法》除了用“个人信息跨境提供的规则”这一专章为金融企业的个人金融数据跨境提供了明确的具体行为标准，其第一章“总则”中更是以 6 个条文规定了合法、正当、必要、诚信、目的限制、公开透明、质量、安全等 8 项基本原则，在确立个人信息保护框架的同时，有助于在具体规则阙如时为金融企业如何实现个人金融数据跨境提供补充解释。此外，尽管各国具体规则各异，金融数据保护的基本原则却有最大公约数可取，据此建立的合规框架可在金融企业因应数据跨境多向合规过程中兼具通用性与应变性。

其次，在金融企业自我规制的后端，需要加强“元规制”（meta-regulation）②。所谓元规制，也被称为后设规制，简言之就是“对自我规制的规制”（the regulation of self-regulation）[29]245，即外部规制者在诱导规制对象针对公共问题发展内部自我规制的同时[25]150，通过各种激励和惩罚手段来对自我规制进行必要的干预以避免市场失灵[33]3-20。因此，元规制本质上可以视为是一种具有回应性（responsive）的“强制型自我规制”（enforced self-regulation）。③ 在此，国家的角色转向承担一种“小而美”的担保责任，在将部分金融数据跨境规制的公共职能转由金融企业履行的情况下，通过事后的评估和管制措施担保其行为最终符合公共福祉。[34]欧盟的 GDPR 就切实反映了此种元规制模式，第 5 条在规定了“个人数据处理原则”④ 的基础上要求数据控制者采取保护个人数据安全之合理技术手段和组织措施，一定程度上赋予了数据控制者自我规制的自由裁量权，但其中的透明性原则和可问责性原则显然又为传统命令与控制型规制中外部压力的介入留下了必要通道。[35]根据我国《个人信息保护法》第七章规定，金融企业若在个人金融数据出境过程中虽未违反第三章关于个人信息跨境提供的具体规则，但违反了总则所规定之原则，仍有可能承担相应的法律责任。因此，一方面，金融企业要充分发挥自主性和能动性开展框架性原则之下的金融数据跨境合规并进行充分的自我评估；另一方面，国家机关在对金融企业自我规制进行规制时，既要确保相关原则配套问责机制的实现，也要在限缩性解释的基础上“禁止向一般条款逃逸”，以免过度加重金融企业合规负担。由此才能在政府与金融企业的协同治理之下以期达成最佳的监管效能，实现“规制-自我规制-元规制”三环框架性规制之下法治与自治的良性互动。

---

① 其第三章“亚太经合组织信息隐私原则”以专章形式，在损害预防原则的统领下规定了通知原则、收集限制原则、个人信息使用原则、选择原则、个人信息完整性原则、安全保障原则、获取与修正原则等。APEC Privacy Framework，Part III.

② 某种意义上，前述通过框架性立法设定公共规制的原则目标、企业根据相应原则目标开展自我规制，都属于整个“元规制”体系不可分割的一部分。但本文为论述方便，主要着眼于“元规制”根据既定原则目标对自我规制进行后续监管、跟踪评估这一层含义。

③ “强制型自我规制”（enforced self-regulation）是“回应型监管”（responsive regulation）的代表模式，是一种试图打通强监管和去监管之间鸿沟的新设想。自我规制的强制性体现为两方面：一是国家强制要求企业实行自我规制；二是自我规制的规则能够被公共执行。Ayres I，Braithwaite J. *Responsive Regulation：Transcending the Deregulation Debate*. New York：Oxford University Press，1992，p. 101.

④ 包括合法性、合理性、透明性、目的限制、数据最小化、准确性、限期储存、数据的完整性与保密性和可问责性。

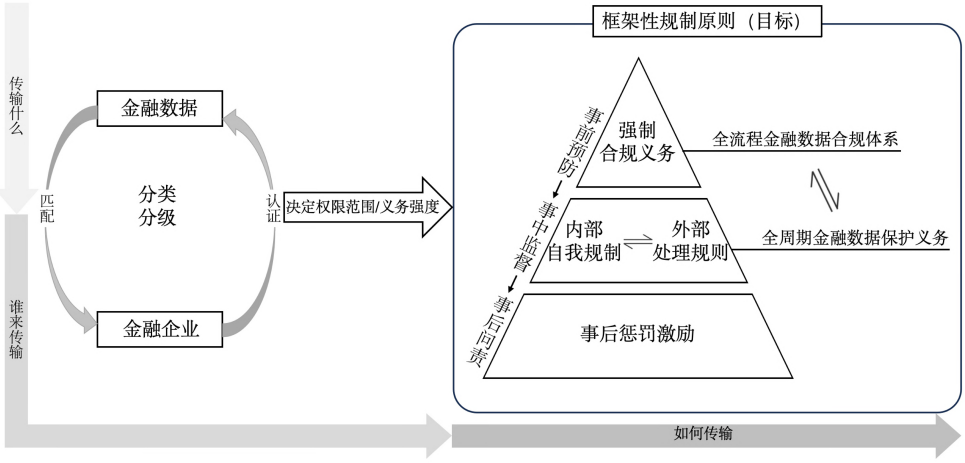

图 1　金融企业数据跨境合规治理体系

综上，在框架性的规制目标之下，从建立全流程金融数据合规体系的强制性合规义务，到外部处理规则和内部自我规制协调互补形成全周期金融数据保护义务，最后由事后问责机制提供惩罚救济和激励保障，一个以金融企业数据跨境合规为出发点和主抓手，贯穿“事前-事中-事后”呈现完整金字塔结构的金融数据保护规制体系得以成功构建（见图 1）。当然，前一部分中讨论的金融数据与金融企业分类分级的双向匹配认证是该规制体系构建的前提基础，决定了体系内部的权限范围与义务强度。

四、金融数据跨境行政监管：统一主体基础上的创新与激励

（一）统一监管主体：多头监管现实困境的出路

“连接良好的法律与自觉守法之间的通道是完整通畅的执法与监管。”[18]一方面金融数据跨境流动立法需要行政监管部门进行细化执行，另一方面金融企业的合规自治也需要行政监管部门加以监督管理。基于我国《数据安全法》第 6 条所确立的“网信部门统筹监管+各行业主管部门分业监管”模式，当前金融企业的金融数据跨境流动面临多头监管的局面。由于统一监管机构的缺乏，网信部门和金融部门的监管细则不一致、执法标准各异，既存在重复监管，又易形成监管空隙，加剧了金融企业在金融数据跨境流动中的合规不确定性，进而加重其合规负担。

网信部门针对金融数据跨境流动，总体上呈现出“以本地化为原则、以安全评估出境为例外”的规制思路。作为《网络安全法》数据跨境安全评估机制的执行细则，国家网信办制定的《评估办法》延续了 37 条的要求，而作为配套标准的《评估指南》则将几乎所有金融数据都归入了重要数据的范畴。① 虽然《评估指南》至今仍未能落地，但其中已不难管窥网信部门针对金融数据跨境流动重安全而轻流动的规制思路且一以贯之。上述现象在某种程度上或可归咎于网信部门缺乏对各行业发展情况和数据信息的专业认识。

① 国家质量监督检验检疫总局、国家标准化管理委员会：《信息安全技术　数据出境安全评估指南（征求意见稿）》，20173853-T-469，附录 A. 19。

金融部门作为金融领域的专业部门，虽通过各种规章监管金融数据跨境流动起步更早，但其规制思路则呈现出一定的摇摆横跳。以中国人民银行为例，2011 年《中国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》（以下简称《通知》）对在中国境内收集的个人金融信息明确规定了本地化要求，虽存在但书，但在当时并未有例外规定的情况下，实质上就是完全禁止个人金融信息跨境。① 而时隔不久的《中国人民银行上海分行关于银行业金融机构做好个人金融信息保护工作有关问题的通知》（以下简称《新通知》）却采取了与上述《通知》截然相反的立场，允许在满足“业务必需+书面授权同意+保密义务”的情况下实现个人金融信息的自由跨境。② 随后于 2016 年发布的《中国人民银行金融消费者权益保护实施办法》，吸收了《通知》与《新通知》的相关规定，实际上是直接将后者作为了前者的例外规定以满足金融企业的业务需求，但还需“符合法律、行政法规和相关监管部门的规定”，如彼时已颁布的《网络安全法》37 条。③ 2020 年的《个人金融信息保护技术规范》则对基于业务需要的个人金融信息出境，提出了“符合法律规定+获得明示同意+依规安全评估+明确监督保障”的多重并列要求④，较之次年颁布的《个人信息保护法》中的个人信息跨境要求条件有过之而无不及。此外，若将金融数据跨境流动的监管职责完全交由金融主管部门，其固然可结合金融业发展需求发挥其专业优势，不过亦可能因本行业利益发生监管俘获或与其他行业产生监管竞次，不利于保护金融数据安全。

随着越来越多的国家开始对数据跨境流动展开规制，数据保护机构（data protection authorities，DPAs）的设立和合作也在逐年增加。[36]101 在 APEC 的“跨境隐私规则体系”（CBPRS）⑤ 之下，作为其重要组成部分的《隐私框架》建议其成员国应考虑建立和维护独立的隐私执法机构⑥，具备通过认证的隐私执法机构是该国企业申请加入该体系的先决条件。欧盟作为个人数据保护的先驱，在 1995 年就提出了各成员国须建立独立监管机构的要求⑦；随后又于 2001 年宣布在欧盟层面设立独立的数据保护专署（EDPS）⑧；2016 年更是在此基础上成立了由上述各成员国监管机构和数据保护专署组成的欧盟数据保护委员会（EDPB）⑨。其他还有如新加坡于 2013 年成立的个人数据保护委员会（PDPC）、日本于 2015 年设立的个人信息保护委员会

① 中国人民银行：《中国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》，银发〔2011〕17 号，第 6 条。

② 中国人民银行上海分行：《中国人民银行上海分行关于银行业金融机构做好个人金融信息保护工作有关问题的通知》，上海银发〔2011〕110 号，第 4 条。

③ 中国人民银行：《中国人民银行关于印发〈中国人民银行金融消费者权益保护实施办法〉的通知》，银发〔2016〕314 号，第 33 条。现行 2020 年《中国人民银行金融消费者权益保护实施办法》直接放弃了对消费者金融信息的跨境流动作出特别规定。

④ 中国人民银行：《个人金融信息保护技术规范》，JR/T 0171-2020，第 7.1.3 条 d 项。

⑤ APEC 的 CBPRS 体系是一项由政府支持的数据隐私认证系统，企业可参加该认证以证明其遵守了国际公认的数据隐私保护标准。APEC. What is the cross-border privacy rules system. https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System, 2023-06.

⑥ APEC Privacy Framework, Article 41.

⑦ 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, Article 28.

⑧ 其职责为确保和监督各机构和成员方实施欧盟关于在个人数据处理中保护自然人基本权利和自由的各项法规，或者向其提供关于个人数据处理任何相关事项的建议。Regulation（EC）No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, Article 41.

⑨ GDPR, Article 68.

（PIPC）、巴西于2020年成立的国家数据保护局（ANPD），美国在一项名为《“控制我们的数据”法》（Control Our Data Act）的立法提案讨论稿中也建议设立独立的“消费者隐私保护和数据安全局”①。

在此现实困境和国际趋势下，我国也应设立独立、权威、专业的数据监管机构并明确其法律地位，在网信部门与行业主管部门之间平衡安全与发展，一方面专门负责履行国内数据跨境流动规制等各项职能，另一方面密切加强国际监管合作与对接、强化域外执法；同时考虑到诸如金融数据等各专门行业领域数据的特殊性，可以分设相应的子机构在其统一领导之下开展工作。2023年《党和国家机构改革方案》提出设立的国家数据局，不失为我国独立数据监管机构的可行选择，从而缓解当前各部门职能交叉、缺乏顶层设计等问题。但根据方案，目前其作为国家发改委管理的国家局，承担的仅仅是协调推进数据基础制度建设等数据领域的宏观职能，而并未改变金融数据出境具体监管职能的离散现状，未来能否以此为契机统合协调跨境数据流动的发展与监管职能，尚待进一步观察。退一步而言，若考虑到新设独立监管机构可能成本高、周期长、部门利益纠葛大，那么在维持分业监管模式下发挥金融主管部门在重要数据目录和一般数据清单制定、金融数据出境正反面案例发布、金融企业数据安全管理认证等方面的主导作用，将网信部门的职责定位重新回归并强化《数据安全法》第6条规定的“统筹协调”而弱化安全评估之外具体的监管执行，也是一种适合我国国情的解决当前因金融数据跨境监管职能不当配置所诱发之合规困境的替代方案。

（二）监管科技创新：金融科技发展的必然要求

监管与创新总是水乳交融，呈现出一种既相互冲突又相互促进的关系。[37]在金融数据跨境领域表现为：“金融科技”（FinTech）快速发展之下从“了解你的客户”（KYC）到“了解你的数据”（KYD）的范式转变正在逐字节地改变传统规制模式，强烈要求“监管科技”（RegTech）的创新。[38]具体言之，在金融科技助力下，金融业的数字化转型日益加快，数据驱动的特征也日益明显，这既是需要对金融数据跨境流动加强规制的根源所在，也对传统监管构成了重大挑战：首先，合规不仅对于企业来说是一项耗时耗力耗费的艰巨任务，对于监管机构而言更甚，金融数据跨境规制中全周期保护义务的赋予要求监管机构实现全流程监管，但是当前相对落后的监管手段受限于其自动化和集成性程度，无法实现对金融企业合规的实时全程监管。其次，在数据驱动的金融数字化进程中，监管机构在金融数据跨境流动监管中面对的是数量级极其庞大的金融数据，其种类和格式较先前大为丰富，加之金融科技的发展使得金融数据的跨境流动范围更广、速度更快、方式更为多样，监管机构若无强大的数据分析能力和安全技术，则根本难以识别其中复杂的金融风险，更难言在风险发生时及时介入加以阻断。总之，面对金融科技创新，监管能力若未得到有效改进，则监管失灵在所难免，进而诱发市场失灵。正基于此，USMCA在其“数字贸易”一章专门强调，考虑到数字贸易中的网络安全威胁，各成员国应加强建设其负责网络安全事件处置的国家机构的各项能力。② 综上，在金融科技日新月异、金融数据跨境流动方兴未艾的当下，除了统一监管主体之外，亟须通过监管科技创新变革监管手段、提高监管能力、提升监管效率。

① 该提案讨论草案由众议院能源和商业委员会和消费者保护及商业小组在2021年提出，建议在该委员会内部设立“消费者隐私保护和数据安全局”以执行委员会的管辖范围内有关消费者隐私保护或数据安全法律法规、教育消费者并向其提供指导、向寻求遵守本法的中小型实体提供支持和援助等。House Energy and Commerce Committee, House Consumer Protection and Business Committee. The discussion draft of a bill of “Control Our Data Act” § 114. https://republicans-energycommerce.house.gov/wp-content/uploads/2021/11/2021.11.02-Republican-CODA-Draft-.pdf, 2021-11-02.

② USMCA, Article 19.15.

更为重要的是，监管科技还有其面向企业合规的一面。监管科技在金融企业端可以表现为一种合规科技，即金融企业通过利用技术创新来更好地满足合规要求、降低合规成本①，这既是在金融数据跨境流动规制中金融企业负担全周期保护义务、建设全流程合规体系的必然选择，也是与行政端监管科技相匹配对接的应有之义。而且，监管科技的进步可以改变金融数据跨境流动立法的价值取向，从而更加注重以金融企业合规为中心而非“一刀切”地强调本地化。金融数据的跨境流动规制将随着行政监管能力的变化发展呈现出动态性的特征[21]，若能通过扎实提高监管技术水平来保障数据安全，想必也不会选择制定容易惹人非议的本地化法规。因此，监管科技创新是建立以金融企业合规为中心的金融数据跨境流动规制体系、实现安全与自由价值平衡的基础与保障。

金融数据跨境流动规制中的监管科技创新，必须实现“以数据监管为核心”[39]。当前，为了在金融数据跨境中能够实现对数据走向和总量的控制，准确分析识别各类风险，必要时及时抓取留存证据并采取强制脱敏或阻断传输等措施，监管机构可以考虑提供统一的金融数据跨境传输通道平台，辅之以区块链、隐私计算等技术，实现金融数据跨境的防篡改、可追溯，同时兼顾金融企业的商业秘密保护需求。金融企业在金融跨境传输时本就需要借助第三方网络数据公司提供相应的服务器和网络传输通道，若转由监管机构统一提供同价位、同质量的数据传输平台，在不增加金融企业成本负担的同时，既满足了其金融数据出境需求，也可大幅提高监管机构的数据路由控制能力。但是，其中尚需要注意两个问题：一是监管机构的数据安保责任，监管机构在依照法定职责通过统一跨境传输平台对金融数据跨境进行监管过程中收集、使用的相关数据符合《数据安全法》第 38 条对“政务数据”的定义，故应当依照第 39 条之规定履行落实相应数据安保义务以保障政务数据安全；二是对行政垄断的防范，监管机构向金融企业强制性指定统一的有偿金融数据传输平台可能涉及是否构成行政垄断的争议，对此监管机构应当明确其通过行政权限制竞争的界限应局限于为履行法律、法规授权的公共事务管理职能，其目的应在于谋求国家或社会的公共利益，如此方可排除滥用行政权力之质疑。

（三）多重激励机制构建：克服合规动力不足的监管策略

现代企业合规肇始于刑事合规，而刑事合规最重要的面向就是合规激励，即以非与惩罚相孪生的独立刑事利益促使企业建立有效的刑事风险防控体系。自 2020 年最高人民检察院开始推动企业合规不起诉制度试点以来，刑事合规激励在我国逐渐铺开深入。金融企业实现金融数据跨境合规在现行法律体系下可能获得的刑事利益包括无罪、不起诉、量刑从轻、强制措施优遇等。[40]不过，现有刑事合规激励实践多针对传统中小微企业，金融与数据合规在该领域的存在感依然偏低，法治化、场景化、标准化、精细化、普及化程度尚待提升。而在金融与数据两股强监管趋势汇流的背景下，金融企业数据跨境合规的行刑衔接问题日益突出。金融数据法益的多样性、出境行为的复杂性、违规出境危害的重大性，加剧了金融企业数据犯罪治理的难度。然“冰冻三尺非一日之寒”，犯罪行为往往是行政违法行为的递进。这一点从当前数据犯罪相关罪名多以空白规范引致行政义务就可见一斑，例如个人金融数据违规出境可能触犯的侵犯公民个人信息罪即以“违反国家有关规定”为前提。面对实体层面的双层违法和责任竞合，金融企业数据跨境合规的行刑衔接不能再局限于简单的移送对接[41]，而应在“诉前-诉中-诉后”双轨互动的基础上强化

① 监管科技最初正是由英国金融行为监管局在合规科技意义上使用，后续才扩展至行政监管端。FCA. Call for input：Supporting the development and adoption of RegTech. https://www.fca.org.uk/publication/call-for-input/regtech-call-for-input.pdf，2015-11-23.

双重激励。相较于单纯的刑事合规激励，行政合规激励机制的构建既能在统一法秩序下通过激励前置实现数据出境安全风险的防控关口前移，亦可在恩威并施下实现行政机关、司法机关与金融企业三者的协同共治。

平衡论指出，在现代行政法机制中唯有制约机制与激励机制互相配合，方能实现行政法治与企业自治之间的良性互动。[42]无论是强制合规义务的赋予，还是通过技术创新实现对合规的有效监管，都仅体现了制约的一面而显激励不足。因此，有必要在金融数据跨境流动规制领域将合规激励机制引入行政执法程序，即行政监管部门为鼓励金融企业建立起有效完善的全流程合规体系，在保留传统事后惩罚机制的同时，确立以合规换取宽大行政处理的监管策略。[43]通过将监管策略由侧重威慑转向侧重激励，化对抗为协作，以增强外部规制对内部合规的渗透性。

具体言之，一是将有效合规体系的建立作为法定的责任减免事由。基于金融数据本身所具有的复杂性、敏感性，即便金融企业努力建立了合规体系也难免“智者千虑必有一失”，若此时仍照常处罚，必将从客观上导致金融企业不敢贸然从事金融数据跨境、也不愿建立合规体系。对此，在保留严刑峻法的基础上，为了给予金融企业即便要付出成本也要制定和遵守合规计划这样的激励，如果经营者制定实施了合理有效的合规计划，应当基于其已履行了必要的监督义务而承认对其免责或减责的可能性。[44]41二是将合规计划引入行政执法和解制度。所谓行政执法和解，是指立足于行使行政自由裁量权的正当性基础，监管执法机构在执法过程中与行政相对人为消除行政争议而订立的一种公私融合的行政合同。行政执法和解是提高监管效能、减轻监管负担的有效手段，因而成为域外行政执法中的惯用手段。据统计，美国证券交易委员会98%的执法案件都通过行政和解解决。① 在数据保护领域美国联邦贸易委员会也曾与脸书公司就其使用欺骗手段非法获取和共享用户隐私数据的行为达成和解协议，在让其支付50亿美元巨额罚款的基础上还对其施加了史无前例的业务运营新限制，要求重建多个合规渠道。② 在金融数据跨境流动这样复杂的监管场景中，监管机构本就有较大的自由裁量空间，而将企业合规引入行政执法和解（包括将企业合规作为和解适用的前提或者作为和解协议条款），可使行政执法和解的达成成为一套更多依靠金融企业内控优化的规范化体系，实现对金融数据跨境行政纠纷的源头治理。

我国当前初步建立了上述对企业合规的行政激励机制。在将企业合规作为法定责任减免事由方面，《证券公司和证券投资基金管理公司合规管理办法》第36条明确将证券基金机构有效的合规管理作为了依法从轻、减轻处理乃至不予追究责任的条件，《行政处罚法》第32条也将“主动消除或者减轻违法行为危害后果”作为从轻或者减轻行政处罚的法定情节。在将企业合规引入行政执法和解方面，证监会于2015年发布的《行政和解试点实施办法》（以下简称《试点办法》）被认为是我国第一次在行政监管执法中引入行政和解，同时也在其中引入了合规机制，要求行政和解协议应当载明整改措施及其履行期限③；随后国务院于2021年颁布了《证券期货行政执法当事人承诺制度实施办法》，正式确立了本质上属于行政执法和解的行政执法当事人承

① Aguilar L A. A stronger enforcement program to enhance investor protection. https://www.sec.gov/news/speech/2013-spch102513laa, 2013-10-25.

② Federal Trade Commission. FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook—FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook, 2019-07-24.

③ 中国证券监督管理委员会：《行政和解协议试点实施办法》，中国证券监督管理委员会令第114号，第26条。

诺制度①；证监会于 2022 年重新发布了《证券期货行政执法当事人承诺制度实施规定》作为其实施细则，具体规定与前述《试点办法》类似。

我国的上述规定虽可被视为初步构建起了金融企业合规的行政激励机制，在监管执法实践中也出现了少量案例，但就金融企业金融数据跨境合规的行政监管而言还存在不少问题：第一，上述规定目前仍多仅限于由证监会作为监管主体的证券执法领域，在当前金融数据控制者扩张的背景下适用范围十分有限，是否适用于金融数据跨境监管领域也不无疑问；第二，上述部分规定其实并未直接明确将合规作为行政责任的减免事由或者行政和解的条件和内容，能否将合规纳入其中还存在较大的解释空间，因此未能发挥出推动企业合规的最大激励作用。因此，我国仍需进一步推动在统一金融数据跨境流动监管主体之下构建起完整、普遍、明确、有效的多重行政激励机制，并实现与刑事合规的有效衔接。

五、余　论

阿尔文·托夫勒在《第三次浪潮》中指出：裹挟于历史的滔滔不绝的变革浪潮之中，只有在前进过程中孜孜不倦地探求浪潮前锋、识别变革前景，我们才能在崭新的视角之下认清和掌控变革的形势。[45]55当全球经济成为一台在“消耗数据-处理数据-生产数据”之间永续循环的数据永动机[46]，如何对金融企业的金融数据跨境流动进行规制正是当前需要我们探求和识别的数字经济浪潮的前锋之一。对此，本文从金融企业合规治理这一崭新视角，提出了在安全和自由利益平衡的数据本位立法之下，通过统一监管主体基础上的监管科技创新与多重激励机制，构建以预防性和框架性规制理念为指导、以金融企业内部强制合规为中心的金融数据跨境流动规制框架。但当前该框架若要真正落地，其中不少在实定法上仍处于模糊或空白地带，甚至会产生冲突。面对这一复杂系统中的诸多不确定动态因素，贸然突破当前相对抑制的金融数据跨境监管现状，可能造成覆水难收的风险局面。对此，建议可引入“监管沙盒”（regulatory sandbox）② 机制以实现治理体系创新与金融数据安全的双赢。如果说包含三重维度的金融企业数据跨境合规治理体系是最终实现兼顾安全与发展规制目标的必要手段，那么监管沙盒则旨在创设一个被监视和受控制的相对隔离的试验运行环境：监管机构在严守监管目标和底线、做好风险管理预案的前提下，通过事先设定原则标准和限制条件，允许经过甄选的金融企业在真实的市场业务场景中，以真实的金融数据与数据接收方为对象测试金融数据跨境流动全过程，以评估上述合规治理体系的成效和影响。其本质上与我国的试点机制类似，在小范围针对性试点中包容创新、容错纠错，在总结经验教训的基础上相机决策是否全面推广。在金融数据跨境流动的相对安全观之下，通过创造一个新的监管环境促进创新和未知风险方案之间的良好平衡[47]，借助“双层容错”[48]机制促成监管者与被监管者在可信可控、动态灵活的互动合作机制中发挥各自能动性持续矫正监管与市场之间的区隔，这恰恰与本文以金融企业合规为中心实现金融数据跨境安全和自由之间的平衡这一核心论点高度契合。

① 《证券期货行政执法当事人承诺制度实施办法》（国务院令第 749 号）第 2 条规定：“本办法所称行政执法当事人承诺，是指国务院证券监督管理机构对涉嫌证券期货违法的单位或者个人进行调查期间，被调查的当事人承诺纠正涉嫌违法行为、赔偿有关投资者损失、消除损害或者不良影响并经国务院证券监督管理机构认可，当事人履行承诺后国务院证券监督管理机构终止案件调查的行政执法方式。”

② 监管沙盒，是指一个可供身处其中的金融企业进行创新测试而享有正常监管豁免的安全空间。FCA. Regulatory sandbox. https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf, 2015-11-10.

总而言之，数字金融的深入发展不可逆转，“金融即数据”终成定局。面对金融与数据在全球化变局下不断碰撞出新的火花，本文所提出的金融企业数据跨境合规治理体系试图以一种多主体协同、多环节联动的方式探求一条多目标平衡的金融数据跨境流动规制新路径。然而作为典型的交叉领域，如何实现金融监管与数据治理的同步异构演进，进而协调一般金融监管与数字金融监管、一般数据治理与金融数据治理的政策目标与具体规则，最终达致和谐有效的全球金融数据治理新格局，是金融数据跨境流动规制所折射出的一个更为宏大复杂的命题。同时，技术的发展也同样带来了新问题。区块链、云、人工智能、隐私计算等技术的发展，不仅可以为金融数据跨境传输使用提供更加高效安全的手段，甚至将突破金融数据跨境流动的基本范畴界定，这既是机遇也是挑战，未来的金融数据跨境流动治理范式应作出何等因应，值得关注与进一步研究。

[参考文献]

[1] McKinsey. Financial data unbound: The value of open data for individuals and institutions. https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/financial%20data%20unbound%20the%20value%20of%20open%20data%20for%20individuals%20and%20institutions/financial-data-unbound-discussion-paper-june-2021.pdf, 2021-06-24.

[2] Posner R A. Theories of economic regulation. *The Bell Journal of Economics and Management Science*, 1974, 5 (2): 335-358.

[3] Arner D W, Castellano G G, Selga E K. Financial data governance. *Hastings Law Journal*, 2022, 74 (2): 235-292.

[4] 陈瑞华：《企业合规基本理论》，北京：法律出版社，2021 年。

[5] 习近平：《高举中国特色社会主义伟大旗帜　为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告》，北京：人民出版社，2022 年。

[6] 范思博：《个人金融数据跨境流动的治理研究》，《重庆大学学报》（社会科学版），2021 年 7 月 27 日，网络首发。

[7] 许可：《自由与安全：数据跨境流动的中国方案》，《环球法律评论》，2021 年 1 期。

[8] 马兰：《金融数据跨境流动规制的核心问题和中国因应》，《国际法研究》，2020 年 3 期。

[9] 张凌寒：《个人信息跨境流动制度的三重维度》，《中国法律评论》，2021 年 5 期。

[10] 周汉华：《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》，《法学研究》，2018 年 2 期。

[11] 陈瑞华：《论企业合规在行政监管机制中的地位》，《上海政法学院学报（法治论丛）》，2021 年 6 期。

[12] 张舵：《刍议跨境数据流动的公共利益保护》，《河北法学》，2018 年 5 期。

[13] Dumas J. General Data Protection Regulation (GDPR): Prioritizing resources. *Seattle University Law Review*, 2019, 42 (3): 1115-1128.

[14] Baer M H. Governing corporate compliance. *Boston College Law Review*, 2009, 50 (4): 949-1019.

[15] 陈瑞华：《企业合规的基本问题》，《中国法律评论》，2020 年 1 期。

[16] 许多奇：《个人数据跨境流动规制的国际格局及中国应对》，《法学论坛》，2018 年 3 期。

[17] 尹云霞、李晓霞：《中国企业合规的动力及实现路径》，《中国法律评论》，2020 年 3 期。

[18] 许多奇：《论跨境数据流动规制企业双向合规的法治保障》，《东方法学》，2020 年 2 期。

[19] Tovino S A. Assumed compliance. *Alabama Law Review*, 2020, 72 (2): 280-325.

[20] 谢望原：《论拒不履行信息网络安全管理义务罪》，《中国法学》，2017 年 2 期。

[21] 蔺捷、田晨：《个人金融数据跨境流动规制研究》，《上海大学学报》（社会科学版），2021 年 6 期。

[22] Jasmontaite L, Kamara I, Fortuna G Z, *et al*. Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, 2018, 4 (2): 168-189.

[23] 罗文华：《基于生命周期的数据跨境流动程序性与实质性监管》，《中国政法大学学报》，2021 年 5 期。
[24] 蔡立东、展海晴：《论个人信息权益保护范围的厘定——以行为违法判断为核心》，《吉林大学社会科学学报》，2023 年 2 期。
[25] Coglianese C，Mendelson E. Meta-regulation and self-regulation. In BaldwinR，Cave M，Lodge M（eds.）*The Oxford Handbook of Regulation*. Oxford：Oxford University Press，2010.
[26] 陈松：《公私合作的公法调适——以国家担保责任为中心》，《武汉理工大学学报》（社会科学版），2015 年 5 期。
[27] 刘鹏、王力：《西方后设监管理论及其对中国监管改革的启示》，《新视野》，2016 年 6 期。
[28] Gunningham N，Rees J. Industry self－regulation：An institutional perspective. *Law & Policy*，1997，19（4）：363-414.
[29] Parker C. *The Open Corporation*：*Effective Self－Regulation and Democracy*. Cambridge：Cambridge University Press，2002.
[30] 高秦伟：《社会自我规制与行政法的任务》，《中国法学》，2015 年 5 期。
[31] 王起超：《粗放和精细：论立法技术的秩序建构路径》，《河北法学》，2021 年 5 期。
[32] 张金平：《跨境数据转移的国际规制及中国法律的应对——兼评我国〈网络安全法〉上的跨境数据转移限制规则》，《政治与法律》，2016 年 12 期。
[33] Coglianese C，Nash J. Management-based strategies：An emerging approach. In Coglianese C，Nash J（eds.）*Leveraging the Private Sector*. Washington，D. C.：Resources for the Future Press，2006.
[34] 杨彬权：《论国家担保责任——担保内容、理论基础与类型化》，《行政法学研究》，2017 年 1 期。
[35] 程莹：《元规制模式下的数据保护与算法规制——以欧盟〈通用数据保护条例〉为研究样本》，《法律科学（西北政法大学学报）》，2019 年 4 期。
[36] Kuner C. *Transborder Data Flows and Data Privacy Law*. Oxford：Oxford University Press，2013.
[37] 许多奇：《金融科技的“破坏性创新”本质与监管科技新思路》，《东方法学》，2018 年 2 期。
[38] Arner D W，Barberis J N，Buckley R P. Fin Tech，Reg Tech，and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*，2017，37（3）：371-413.
[39] 杨东：《监管科技：金融科技的监管挑战与维度建构》，《中国社会科学》，2018 年 5 期。
[40] 刘品新：《论数据刑事合规》，《法学家》，2023 年 2 期。
[41] 郭华：《企业合规整改行刑衔接的协调机制》，《华东政法大学学报》，2022 年 6 期。
[42] 罗豪才、宋功德：《现代行政法学与制约、激励机制》，《中国法学》，2000 年 3 期。
[43] 陈瑞华：《论企业合规在行政和解中的适用问题》，《国家检察官学院学报》，2022 年 1 期。
[44] 佐伯仁志：《制裁论》，丁胜明译，北京：北京大学出版社，2018 年。
[45] 阿尔文·托夫勒：《第三次浪潮》，朱志焱、潘琪、张焱译，北京：生活·读书·新知三联书店，1983 年。
[46] Slaughter M J，Mc Cormick D H. Data is power：Washington needs to craft new rules for the digital age. *Foreign Affairs*，2021，100（3）：54-63.
[47] Piri M M. The changing landscapes of FinTech and RegTech：Why the United States should create a federal regulatory sandbox. *Business & Finance Law Review*，2019，2（2）：233-255.
[48] 许多奇：《论监管科技的双层容错机制》，《政治与法律》，2024 年 1 期。

［责任编辑：李佳欣］

wards to a practical logic based on the intermediary between scientific theory and value ideal. On the one hand, scientific theories serve value purposes, and so that the choice of their fields and objects is guided or limited by value ideals. On the other hand, this service is performed by mediating the value ideal, which means by defining the aims and means of action in the light of the revealed factual laws, and so that it could be concretized into feasible solutions. Such an interactive mediation between value ideals and scientific theories, and between value logic and scientific logic, constitutes the framework of the real practical activity of human objectivity. Accordingly, the interpretation of *Das Kapital* should be carried out in the view of the third kind of logic, which synthesizes the scientific logic and the value logic.

Keywords: *Das Kapital*; critical logic; value logic; scientific logic; practical logic

Governing Financial Corporate Compliance in the Cross-Border Data Flow Regulation of China

XU Duo-qi, *DONG Jia-jie* (41)

Abstract: In the context of the digital economy, it has become a trend to carry out necessary regulation on cross-border financial data flows, and financial corporations with this inherent business requirement urgently need to strengthen responsive compliance. Due to the multiple connotations of compliance, the financial corporate compliance on cross-border data flows in China should be constructed as a comprehensive governance system that encompasses the following three dimensions. Legislation is a prerequisite, and the essence of legislation on cross-border financial data flows is the balance of interests between security and freedom. The misalignment between financial corporation and financial data in current legislation leads to an imbalance of interests, which can only be redressed by returning to the central perspective of financial corporate compliance based on financial data standard. Internal compliance is the core, which requires not only imposing mandatory compliance obligations on financial corporation under the concept of preventive regulation to achieve the rule of law for autonomy, and then setting up a full-process compliance system with full-cycle protection obligations as a basis; but also improving the triple-loop coupling of regulation, self-regulation and meta-regulation, to promote the positive interaction between the rule of law and autonomy within a framework of principles. Administrative supervision is a guarantee. In order to cope with the dilemma of multi-authority supervision, the challenges caused by FinTech and the insufficiency of compliance motivation, it is necessary for a unified supervisory authority to innovate RegTech and establish multiple compliance incentives. In the face of the absence of a positive law basis and unknown dynamic risks, the regulatory sandbox can be introduced to provide a fault-tolerant and error-correcting experimental mechanism for the implementation of the above ideas.

Keywords: cross-border data flow; financial data; financial corporation; corporate compliance; governance system

Function Status and Risk Regulation of Judicial Artificial Intelligence: In Evidence Review's Boundary

XIE Deng-ke, *ZHOU Hong-fei* (61)

Abstract: One of the important applications of artificial intelligence in judicial activities is evidence review. Artificial intelligence provides scientific and technological capabilities for evidence review, reduces the arbitrariness of judicial judgment, and improves the effectiveness of evidence review. However, the application of artificial intelligence in evidence review has some risks and problems, such as insufficient case samples for constructing evidence mode, incomplete structural transformation of evidence rules and lack of visual justice in evidence review procedures. In order to cope with the above risks of artificial intelligence in evidence review, it is necessary to clarify the auxiliary status of artificial intelligence in judicial trial and evidence review, improve the quantity and quality of the case samples of judicial artificial intel-