TSINGHUA PBCSF 清华五道口 | IFR 金融科技研究院

研究报告

（2022 年 第 5 期 总第 109 期） 2022 年 5 月 10 日

关于金融科技安全立法的探索与研究

金融安全研究中心

【摘要】“金融是国家重要的核心竞争力，金融安全是国家安全的重要组成部分。”在金融科技 3.0 时代，金融科技安全逐渐成为国家安全不可忽视的重要内容。面对金融创新带来的多形式、多维度、多受众风险，加快推进促规范、成系统、可预期的立法活动，既是宏观视角下加强全面依法治国、提升国家治理水平的应有之义，也是微观视角下维护行业秩序、规制机构业务、提供创新指引和稳定政策环境的必由之路。

本研究主要围绕我国金融科技安全立法情况展开。结合当前立法的客观实际，本文中的金融科技安全立法意为涉及金融科技安全各个方面的立法活动与成果的总称，涵盖金融科技的机构安全、业务安全、信息安全、数据安全、技术安全、用户安全、监管安

全等方面。在文章结构上，本文从我国金融科技发展的背景出发、梳理了我国中央及地方政府在网络与信息安全领域及金融安全领域的立法现状，在此基础上，综合对比其他国家有关法律分析我国立法的特点、积极作用与难点，并相应提出我国金融科技安全立法应坚持总体国家安全观的思路、不断优化我国金融科技安全立法的法律结构、加快我国金融科技安全专业立法、借鉴国际金融科技安全立法的理念和经验，把握世界金融科技安全趋势等政策建议。

目录

关于金融科技安全立法的探索与研究

周道许 王兆峰 张恩权 饶倩 彭天择

（金融安全研究中心）

当前金融科技迅猛发展，以人工智能、区块链、云计算、大数据为代表的前沿技术与金融活动深度交织融合，数据的生产力被迅速释放，一方面通过整合重组，形成了能够产生价值的重要资产；另一方面逐渐形成了以算法为核心的行为逻辑，进而影响信用方式的重构和企业属性的转变，而新的金融风险也随这些变化产生。

“安全是发展的前提，发展是安全的保障。”[1]对于本轮由技术驱动带来的业态变革和新型风险，防化引导的重点之一就是将快速迭代的金融科技经营主体与业务等内容纳入逐步完善的、专注于或与金融科技相关联的法律体系内，通过及时调整补充或制定金融监管和网络信息安全等领域法律法规，让金融监管工作有法可依，让金融活动有章可循，从而有效保障金融科技和平台企业的规范健康发展。

[1] 2016 年 04 月习近平总书记在网络安全和信息化工作座谈会上的讲话指出：“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。我们一定要认识到，古往今来，很多技术都是“双刃剑”，一方面可以造福社会、造福人民，另一方面也可以被一些人用来损害社会公共利益和民众利益。”

1 我国金融科技安全立法的背景与现状

1.1 我国金融科技安全立法的风险背景

“当前金融科技与金融创新快速发展，必须处理好金融发展、金融稳定和金融安全的关系。”[2]在党中央、国务院印发的《法治政府建设实施纲要（2021-2025 年）》中，对数字经济、互联网金融、人工智能、大数据、云计算等相关法律制度提出了“及时跟进研究”的新要求。[3]面对金融科技带来的挑战，推进金融科技安全立法刻不容缓。

总的来说，伴随金融与技术融合的进程，网络和信息领域的风险也以“多而广、演变快”的特征迅速向金融领域扩散，对国家、社会、行业和机构造成了从宏观治理到微观守序的多维影响。

（1）机构风险：技术应用与业务经营

第一，内部管理与外部防护是机构技术应用风险的重要方面。除技术自有的缺陷与风险外，从业机构还面临着以下风险：一是外部风险——安全系统被破解和控制而泄露重要信息，二是内部风险——搭建产品或服务的底层算法因缺乏透明而形成影响准确性与安全性的不可靠黑箱，三是操作风险——产品设计缺陷或职员操作失误而招致损失。

[2] 2020 年 10 月 31 日，国务院金融稳定发展委员会召开专题会议指出，当前金融科技与金融创新快速发展，必须处理好金融发展、金融稳定和金融安全的关系。

[3] 2021 年 8 月，中共中央、国务院发布的《法治政府建设实施纲要（2021－2025 年）》第三部分规定：及时跟进研究数字经济、互联网金融、人工智能、大数据、云计算等相关法律制度，抓紧补齐短板，以良法善治保障新业态新模式健康发展。

第二，线上化、趋同化与为追求长尾用户而过度下沉是机构业务经营风险的主要来源。它包括因业务线上化和风控流程简化而产生的交易与信用风险、机构间业务模型和模式因趋同而扩大的周期与波动风险、多领域业务交叉渗透而产生的系统性危机和传染性风险，这些风险进一步凸显了金融的内在脆弱性和强外部性属性。

（2）行业风险：垄断与数据孤岛

第一，金融科技具有加速金融资源集中的能力。从行业的构成角度看，金融科技独角兽企业多具有金融业或互联网巨头背景，这些巨头企业将其资本规模、人力资源、数据资源、技术资源等多方面优势用于探索业务，不断推进混业与跨区域展业，以争夺新兴市场份额并谋求控制地位与垄断能力。在这一过程中，大型科技公司广泛与金融机构进行风控系统、智能投顾等重要商业合作或技术输出，金融与技术风险也随之传递，一旦大型科技公司本身经营状况或其技术产品出现风险，会直接殃及多领域、多地域、多行业的交易主体，在垄断基础上显现“大而不能倒”的系统性风险。

第二，与打破数据壁垒的期望相反，金融科技反而催生了行业内的“大型孤岛”。在数据作为生产要素的时代，行业巨头企业依托各自的业务平台形成了分割独立、规模庞大的“数据孤岛”，进一步垄断数据资源，市场机构与监管机构都难以利用全

面、实时、准确的数据来对行业的发展情况和面临风险情况做出及时有效的评估判断，从而在风险积累的同时再度陷入“信息不对称”难题中，放大了隐蔽性风险。

（3）社会风险：稳定就业与数据安全

第一，金融科技加速转变就业供需情况。[i]以人工智能为代表的金融科技正在兴起，逐渐提高的受教育与高技术要求正在改变金融机构的业务模式和用人需求，对金融乃至各行各业的现有就业格局造成了较大冲击。

第二，用户的数据权益面对来自机构管理和黑客盗取的多方挑战。在金融科技创造多元消费场景、优化支付渠道、发展零售业务的同时，海量的客户身份、行为与交易数据被金融科技机构所获取、处理、使用。在这一过程中，围绕着数据安全，存在着基于交易强势地位而触碰隐私红线的过度采集风险、基于智能化算法将低价值信息转化为对生活特点精确画像的过度处理和算法歧视风险、基于服务提供商对客户信息保护不周或盗卖的数据泄露风险，这些风险因常涉及客户的核心信息而极易产生社会问题。

（4）跨境风险：非法服务与监管套利

在金融科技发展的背景下，诈骗、境外赌博和非法跨境交付等违法违规跨境金融业务依托线上渠道和去中心化技术，更加易于扩散风险并以套利方式逃避监管。具体来说，一类是服务接受

国内已有相应的法律或监管条例，但依然以伪造牌照、隐藏渠道等形式开展，如基于区块链技术开发的虚拟货币可以绕开银行，来承担洗钱或资金流转等中介职能[ii]，从而进行非法集资转移等外汇交易；另一类是服务提供国内已有专门的监管措施，而服务接受国内缺乏内容对应、惩罚力度相近的监管措施，这时便产生跨境的“监管套利”空间。非法的跨境业务不但会导致一国公民财产在“现金贷”等骗局中遭受损失，也会对当地的金融市场秩序和信用体系造成冲击与破坏。

（5）监管风险：工具更新与治理难题

第一，快速更新的业态对监管科技提出了精准识别与及时更新的更高要求。所谓“工欲善其事，必先利其器”，监管科技是现阶段监管部门监测市场的重要辅助、识别风险的基础工具、制定决策的有效支撑，但人力、资金、技术上的天然劣势和职能等多重因素决定的后发地位常使监管科技的研发与升级滞后于市场前沿，难以保障其充分实现管理目的。

第二，迅速膨胀的数据资源为监管部门带来了全面保护与统筹治理[iii]的新难题。随着个人信息、商业数据和监管数据不断纳入规范管理范围，新兴场景与业务不断生产新的数据与数据类型，市场机构和监管部门要访问、管理和保护的数据成倍增长，除去数据的私密性和公共性矛盾，仅法律规定的责任主体充分履行职责的难度就在陡然上升，持续带来企业安全防护与政府监管

资源的统筹难题。

1.2 我国金融科技安全立法的现状

（1）网络与信息安全领域的立法与政策规范

伴随金融科技阶段式发展，金融科技安全的内涵也由传统意义上的技术安全、互联网时代的网络安全逐步扩展为涵盖网络与信息等方面的金融生态安全。在此背景下，要实现现阶段的金融科技安全，重点之一就在于保障作为业务支撑的网络安全和关键生产要素的数据信息安全；要合理推进金融科技安全立法进程，首先要把握当前网络与信息安全的立法情况。

近年来，党中央、国务院高度重视网络和信息安全方面的立法工作，为促进金融科技安全发展提供了有力保障。全国人大已经出台大量专门法律，与修订后的相关法律和部门制订的各类规范性文件相配合，为网络和信息安全提供了良好保障（见表 1-1）。

表 1-1 现阶段我国网络和信息安全立法与政策规范（部分）

机构	名称	主要相关内容
全国人大及其常委会	《民法典》	涉及个人信息数据处理、虚拟财产保护与个人信息查阅更正权等内容
	《刑法》	涉及计算机系统、功能、数据、程序安全与利用计算机实施金融诈骗等内容
	《国家安全法》	涉及健全金融宏观审慎管理和金融风险防范、处置机制；防范和化解系统性、区域性金融风险；防范和抵御外部金融风险等内容
	《保守国家秘密法》	涉及非法获取持有国家秘密载体、记录传递国家秘密；卸载修改涉密系统的安全技术或管理程序；将涉密系统接入或在公网进行信息交换等行为内容
	《密码法》	将核心密码、普通密码和商业密码分类管理，

		涉及不同密码使用过程中的国家和商业秘密保护；商业密码管理标准；网络关键设备和网络安全专用产品使用检测；关键信息基础设施保护与安全性评估等内容
	《电子签名法》	涉及电子签名的认证条件、电子认证服务的提供要求等内容
	《网络安全法》	涉及网络运营者的信息使用处理管理要求和保护责任。突出体现包括关键信息基础设施在内的网络运行安全保障责任；网安管理部门与机构的保密责任；网络安全风险处置要求等内容
	《数据安全法》	涉及数据和相关活动界定；国家数据安全制度；重要数据处理和关键信息基础设施等方面的安保义务；政务数据安全与开放等内容
	《个人信息保护法》	主要保护数据处理活动中的个人信息。涉及个人信息和相关活动界定、个人享有的权利；机构在个人信息处理和跨境提供时的要求与义务；个人信息保护部门与职责等内容
国务院	《关键信息基础设施安全保护条例》	细化《网络安全法》中的关键基础设施保护内容。主要涉及国家网信部门、国务院公安部门、电信主管部门、省政府有关部门和运营者的保护责任划分等内容
网信办、工信部、公安部、市场监督管理总局	《APP 违法违规收集使用个人信息行为认定方法》	涉及移动互联网应用程序在收集使用个人信息时“未公开”、“未明示”、“未经同意”等行为认定
	《常见类型移动互联网应用程序必要个人信息范围规定》	涉及网络信贷类、投资理财类、手机银行类等移动互联网应用程序的必要个人信息收集范围等内容
网信办	《互联网信息服务算法推荐管理规定（征求意见稿）》	对算法推荐服务做出规范。涉及算法推荐服务提供者的告知责任和用户的选择权利等内容
网信办等	《网络安全审查办法》	确保关键信息基础设施供应链安全，维护国家安全。涉及审查对象、审查材料和风险评估因素等内容
深圳市人大及其常委会	《深圳经济特区数据条例》	国内数据领域首部基础性、综合性立法。[iv]涉及“告知同意为前提”的数据处理行为规范、部分数据权益保护、发展数据要素市场等内容
北京市人民代表大	《北京市信息化促进条例》	涉及北京市网络与信息系统安全建设、相关单位和运行维护管理、应急措施以及信息安全监督等

会常务委员会		相关规定
上海市人民政府	《上海市公共信用信息归集和使用管理办法》	公共信用信息采集与使用应当遵循“合法、安全、及时、准确”的原则，不得侵犯商业秘密和个人隐私。涉及对自然人采集信息范围的规定
杭州市人民代表大会常务委员会	《杭州市计算机信息网络安全保护管理条例》	涉及计算机信息系统安全的保护制度规定、违法行为界定、处罚方式规定、监督管理措施等

结合上表，从全国人大、国务院、中央部委到地方人大，来自网络与信息安全领域的多层级、多角度规制在总体上涵盖了信息数据获取、管理、处理、使用等多环节和个人信息界定、跨境数据管理等重要方面，在经营活动越来越重视数据汲取、金融创新越来越重视数据处理、业务开展越来越依赖数据管理的当下，相关立法成果由原则化向精细化、由理论化向技术化、由统一化向差异化持续转变，部分规定对参与主体从认定范围和权利义务到分级标准详细列示，纳入公安、网安、行业主管部门等多维监管主体，不但提供了金融机构“跨界开展业务就要受到相应合规监管”[v]的基础，同时也为明确法律责任认定、优化从设施保护到综合监管的现代金融网络安全保障体系、推动以数据安全等为基础的业务长远发展迈出了重要一步。

（2）金融安全领域的立法与政策规范

金融科技的本质是金融，金融科技改变了金融业务的行为逻辑和信用分布、影响了金融机构的存在属性，但没有改变金融活动的核心功能、消除金融领域的固有风险。推进金融科技安全立

法，在关注技术管理的同时也应回归金融本源，把握金融的核心本质，以办法、条例等对新兴业务和行业间的灰色地带形成及时有效约束。近年来，金融监管部门出台了大量政策文件，结合已有法律，对较为热点的金融科技问题形成了必要规范（见表 1-2）。

表 1-2 现阶段我国金融业务监管的立法与政策规范（部分）

机构	名称	主要关联内容
全国人大及其常委会	《电子商务法》	涉及商户收集使用个人信息和向主管部门提供数据信息时的要求等内容
	《商业银行法》	涉及存款人的合法权益保护、个人业务办理信息保密等内容
	《证券法》	涉及投资者的信息保密等内容
	《反洗钱法》	涉及履行职责或义务获得的客户资料和交易信息保密等内容
央行	《个人金融信息保护技术规范》	涉及个人金融信息界定与分级；信息的全生命周期安全防护要求；安全运行技术要求等内容
	《商业银行应用程序接口安全管理规范》	涉及商业银行应用程序的参与主体、接口分类、安全技术要求和全周期安全管理要求等内容
	《金融数据安全 数据安全分级指南》	通过保密性、完整性、可用性等评估属性，对金融数据实施按照影响对象和影响程度要素进行分类的安全定级管理。涉及定级规则、定级过程与重要数据描述等内容
	《人工智能算法金融应用评价规范》	规定人工智能算法在金融领域应用的基本要求、评价方法、判断准则，适用于开展人工智能算法金融应用的金融机构、算法提供商、第三方评估机构等。涉及安全性评价、可解释性评价、精确性评价、性能评价等内容
	《中华人民共和国金融稳定法(草案征求意见稿)》	充分总结现有法律规定和此前风险处置实践基础上，合理借鉴了国际准则和经验，健全金融风险事前防范、事中化解和事后处置全流程全链条的制度安排
央行、银保监会	《系统重要性银行评估办法》	加强对系统重要性银行的识别与监管能力，防范系统性风险。涉及评估方法、指标体系、范围、流程和分工等内容

证监会	《证券基金经营机构信息技术管理办法》	涉及监管对象与经营业务、经营机构和专项业务服务机构的主体责任等内容
	《证券期货业投资者权益相关数据的内容和格式》	涉及证券、期货、基金市场投资者权益相关数据的内容和格式标准等内容
	《证券公司租用第三方网络平台开展证券业务活动管理规定（试行）》	涉及证券公司租用第三方网络平台开展证券业务活动的厘定与规范、监管主体、投资者保护等内容
银保监会	《关于规范互联网保险销售行为可回溯管理的通知》	涉及销售页面和记录等可回溯管理、消费者信息安全保护、机构内控管理等内容
	《互联网保险业务监管办法》	涉及互联网保险业务经营原则、营销行为管理、分类监管等内容
	《商业银行互联网贷款暂行管理办法》	涉及互联网贷款业务的厘定与规范；机构风险管理要求与责任；合作机构管理、消费者保护、加强事中事后监管等内容
	《监管数据安全管理办法（试行）》	涉及监管主体与内容、数据管理采集原则、风险责任等内容
	《网络小额贷款业务管理暂行办法（征求意见稿）》	涉及网络小贷业务的厘定与规范；经营网络小贷的业务条件与规则；监管规则和措施等内容
	《关于进一步规范商业银行互联网贷款业务的通知》	涉及审慎监管要求、设定监督指标、严控跨地域经营等内容
	《关于规范商业银行通	涉及定期和定活两便存款业务经营、风险评估与管理、消费者保护、业务监管等内容

	过互联网开展个人存款业务有关事项的通知》	
中国支付清算协会	《人脸识别线下支付行业自律公约（试行）》	以“用户授权、最小够用”为信息采集原则，涉及主动确权保障、资金安全保障和敏感信息保护等内容

结合上表，当前由人大、中央金融监管部委和行业自律组织构建的、涉及金融科技安全的立法规范活动主要分为两方面，即对作为技术核心的“信息保护”和对作为创新结果的“业务监管”两方面。对于前者来说，金融安全领域立法更能体现对数据保护的针对性和对有关上位法的细化。如《个人金融信息保护技术规范》中，首先将“个人金融信息”与《个人信息保护法》中的“个人信息”做出专门区分与领域限定，在引言中规定其为“个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化”[4]，基于此，其适用对象和风控要求更加针对于金融业机构，从而有助于更好地保障金融消费者的合法权益并稳定金融秩序；对于后者来说，金融安全领域立法更能体现对新兴金融业态的适应性与灵活性。金融科技风险随行业“做金融”思维的转变而加速转化扩散，对其监管的立法规范也相应逐步由事后转为源头、由处置转为识别、由刚性转为柔性，大到互联网贷款、小额贷款等业务经营的

[4] 2020 年 2 月 13 日由中国人民银行发布的《个人金融信息保护技术规范》引言规定：个人金融信息是个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化，是金融业机构在提供金融产品和服务的过程中积累的重要基础数据，也是个人隐私的重要内容。

总体规定，小到银行接口、算法应用等技术环节的具体标准，这些细化到业务的具体范围、设施的具体类型、数据的具体格式的规范依时而生、适时而变，有效促进立法步伐适应创新情况，针对特定时期的特定风险具有良好的减降效果。

2 我国金融科技安全立法的主要特点与作用

2.1 形成了以全国人大立法为纲，以行业主管部门、监管部门和地方政府规范为目，有关金融科技安全的全面立法体系

第一，由全国人大及其常委会制定的法律具有更高位阶和适用权威，其中涉及金融科技安全的法律由调整金融交易和监管关系的传统金融法律和调整信息数据存取用管等关系的网络信息法律有机结合而成。对于本质依然是金融的金融科技，《中国人民银行法》、《银行业监督管理法》、《商业银行法》、《证券法》等金融法律依然是行业发展和交易规范的总括性要求，依然是行业主管部门和监管部门等立法主体订立政策文件的基本参照；同样，对于重信息要素、受科技赋能的金融科技，《网络安全法》、《数据安全法》、《个人信息保护法》等法律及时为其划定运营、监管、使用等多方主体权责，负有监管责任的部门则在此职责范围内行使指导、监督等职能。如《网络安全法》中特别强调关键信息基础设施安全，并在其第三十二条和第三十四条规定，“负责关键信息基础设施安全保护工作的部门分别编制并组织实施

本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作”[5]、“关键信息基础设施的运营者还应当履行下列安全保护义务.....”[6]这些规定为随后的《关键信息基础设施安全保护条例》和多部金融监管部门制定的规范中细化各方职责定位与安保内容提供了范围与依据。总体来说，这些法律体现着方向性、指导性、稳定性的顶层管理思路与取向。

第二，由国务院及其各部委、地方政府制定的各类行政法规、部门规章、地方性法规与行业自律组织出台的行业规范、公约相配合，有效形成了由规划指南到业务规范、由大类管理到专项约束、由高指导性到强执行性的中层与底层细化规范体系，充分衔接补足顶层立法设计，使全面的法律体系能够渐进落实到金融科技安全治理的方方面面。如对于个人金融信息保护问题，中国人民银行发布的《个人金融信息保护技术规范》中，依照敏感和危害程度制定的数据分级要求就体现着《网络安全法》第二十一条对数据分类保护要求的细化，而《商业银行应用程序接口安全管理规范》等更为具体的技术规范则可与《个人金融信息保护技术规范》相配合[vi]，形成信息安全的逐层防护，并使监管内容更加

[5] 2016 年 11 月 7 日由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议表决通过的《中华人民共和国网络安全法》第三十二条规定：按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

[6] 2016 年 11 月 7 日由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议表决通过的《中华人民共和国网络安全法》第三十四条规定：关键信息基础设施的运营者还应当履行下列安全保护义务：（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务。

充实明确；再如结合辖区内丰富的数据资源和较为蓬勃的金融科技创新情况，深圳市充分利用地方立法的针对性优势，将区域内的突出问题如“一揽子授权”、“大数据杀熟”、“个性化推送”等均作出专门规定，在数据市场培育等方面也有较为积极的探索，如“自然人对个人数据享有法律、行政法规及本条例规定的人格权益”[7]、“自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益”[8]等，这些规定在某种程度上可以看作是《数据安全法》中“国家保护个人、组织与数据有关的权益”[9]等内容和推动数据要素市场化的具体延伸。

2.2 反映了总体国家安全观的要义，勾勒出我国统筹发展和安全的金融科技安全立法逻辑主线

第一，坚持总体国家安全观是新时代国家安全工作的重要内容。习总书记曾对此提出“坚持统筹发展和安全，实现高质量发展和高水平安全的良性互动”[10]等要求，国务院金融委也曾指出，“当前金融科技与金融创新快速发展，必须处理好金融发展、金

[7] 2021 年 7 月 6 日，深圳市第七届人民代表大会常务委员会公布的《深圳经济特区数据条例》第三条规定：自然人对个人数据享有法律、行政法规及本条例规定的人格权益。

[8] 2021 年 7 月 6 日，深圳市第七届人民代表大会常务委员会公布的《深圳经济特区数据条例》第四条规定：自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益。但是，不得危害国家安全和公共利益，不得损害他人的合法权益。

[9] 2021 年 6 月 10 日由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议表决通过的《中华人民共和国数据安全法》第七条规定：国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

[10] 2020 年 12 月 11 日习近平总书记在中央政治局第二十六次集体学习时强调：“坚持统筹发展和安全，坚持发展和安全并重，实现高质量发展和高水平安全的良性互动。”

融稳定和金融安全的关系。”[11]统筹发展和安全，在金融科技上更多表现为平衡好业务的“创新和风险”、数据的“流通与安全”，即在鼓励发展的同时防止产生重大的金融风险和社会风险，也有力求避免“野蛮生长，大乱大治”的深层含义[12]。

第二，在有关金融科技安全的立法活动中，统筹发展与安全的思想贯穿于多部法律，并具有原则化表述，如《网络安全法》第三条规定，“国家坚持网络安全与信息化发展并重.....鼓励网络技术创新和应用”[13]；《数据安全法》第十三条规定，“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。”[14]在具体内容上，这些法律一方面谋求直接提高安全防护水平，即由国家主导的安全标准制定和由企、学、研参与的安全产品开发“双管齐下”，逐步建成科学合理的安全防护体系；另一方面，限制行为更集中于对企业可能触碰到的公民基本权益和重点风险领域，而非直接强硬限制业务发展，如对个人敏感信息、关键信息基础设施保护的严格规定等。同时相较于欧美的监管标准，我国的总体力度与范围更对宽松适度。

[11] 2020 年 10 月 31 日，国务院金融稳定发展委员会召开专题会议，指出当前金融科技与金融创新快速发展，必须处理好金融发展、金融稳定和金融安全的关系。

[12] 2020 年 10 月 31 日，国务院金融稳定发展委员会召开专题会议，指出要正确处理好政府与市场的关系。既要鼓励创新、弘扬企业家精神，也要加强监管，依法将金融活动全面纳入监管，有效防范风险。

[13] 2016 年 11 月 7 日由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议表决通过的《中华人民共和国网络安全法》第三条规定：国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

[14] 2021 年 6 月 10 日由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议表决通过的《中华人民共和国数据安全法》第十三条规定：国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

2.3 体现了“以我为主”，适合我国金融科技安全发展实际的立法精神

国外立法各有侧重，无论是起步早、规制严还是偏创新、重流转的法律内容都有只适合当地发展要求的一面。而保障金融科技安全，更需要始终坚持中国特色国家安全道路，要深度结合国内金融科技的发展目标、金融科技的业态变化、金融科技的时空差异、金融科技的监管水平，综合拟定法律规范。

我国对于金融科技安全立法国际经验的扬弃取舍之一体现在个人数据保护上。目前国外关于数据保护的代表性法律有于2018 年出台的欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）和于 2018 年通过的美国《加利福尼亚州消费者隐私法案》（California Consumer Privacy Act，CCPA）。其中前者以广管辖范围、重信息保护和高违法处罚而著称，尤其注重数据跨境监管。我国的《个人信息保护法》中的管辖范围设定、数据主体权利、信息处理原则、数据跨境监管等内容便体现了对《民法典》、《信息安全技术个人信息安全规范》等国内既有法律法规和 GDPR 等国外法律的继承、取舍与借鉴。如第三条规定了“在境外处理境内自然人个人信息的活动”受该法管辖的情形，与 GDPR“目标指向”标准相对应[vii]，体现域外管辖的新特点；第三十八条规定了“个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息”的情形，和 GDPR 的

“国家白名单”、BCR（形成有约束力的公司规则）等极其严格的、意在防止削弱数据保护能力[viii]的明确规定相比，我国的要求更侧重于体现国家网信部门对数据跨境的控制原则，在实际执行时留有更多的政策裁量空间，更易于科学管理经济全球化的背景下的跨境电商等国际商事活动[ix]，体现了“因地制宜、以我为主”的立法精神。

2.4 构建了覆盖金融科技机构、金融科技业务、金融科技运行和金融科技监管的全方位法律支撑

第一，现有立法对金融科技安全的关键概念与内容做出了必要界定，构成了相关创新和监管活动的基础性支撑。《密码法》、《电子签名法》、《数据安全法》、《个人信息保护法（草案）》等法律在整合过去网络信息领域内位阶低、碎片化、分散化的立法成果，有效确立网络和信息安全制度、与国际先进理念相接轨的同时，对密码、电子签名、数据与个人信息等金融科技所涉及的关键概念、对信息数据的处理管理使用等行为范围和基本要求等方面做出了必要界定，为规范机构活动和业务创新、监管部门出台配套实施办法等活动提供了立法基础。

第二，现有立法逐渐覆盖金融科技安全的各方主体和业务内容，构成了相关创新和监管活动的必要性支撑。各类立法文件囊括了金融科技的技术提供方、业务运营方、用户方、监管方等各

类参与主体，覆盖了金融与关联行业、重要与一般机构、核心与常规业务等各类管理内容，容纳了资本、技术、数据、设施等各类运行基础，构成了保障金融科技安全的全方位法律体系。

2.5 划出了金融科技安全的界线、红线与防线，通过政策导向和重点管理内容使安全体系日臻成熟

第一，相关立法活动划出了包罗机构、业务、信息、数据、技术、用户、监管等多个维度安全的金融科技安全界线。这些要素因与现阶段金融活动深度融合而将金融安全的内涵不断向外延伸拓展，通过立法活动渗透到多个领域、多个行业当中。如提供支付服务的机构在保障其金融业务必须满足资本、杠杆等规定之余，还要满足传统金融安全界线之外的，由电信、网信等部门发布的，诸如移动端的系统等不受破解侵害，收集的数据处于“必要范围”之中等安全要求。即一切与金融科技密切关联的内容，都将受到法律规制，并处于金融科技安全的“界线”之内。

第二，相关立法活动划出了涵盖个人隐私至上和系统性风险防范等方面的金融科技安全红线。金融科技带来的风险，最终都要作用到具体的人或企业上。对用户来说，公民个人可能因接受金融服务而成为隐私数据泄露、窃取、非法买卖等行为的受害者，所享有的最基本权利直接面临不法威胁；对企业来说，机构间可能存在交易密切关联、业务复杂嵌套、算法技术近似等现象，一

旦存在密切往来的庞大机构出现严重问题，就可能连带恐慌情绪猛烈冲击行业声誉，进而发生恐慌挤兑，造成企业连环倒闭等系统性破坏。基于以民为本和对系统性风险“零容忍”的一贯监管取向，当前的立法活动将大量可能触及这两方面的内容均作出了层层限制或禁止规定，划定了金融科技安全发展的“红线”。

第三，相关立法活动划出了由控制重点事项、限制业务风险、鼓励安全研发构建的的金融科技安全防线。如对于“在公共通信、能源等重要领域或行业内，及其他一旦遭到破坏、丧失功能或者数据泄露，就可能严重危害国家安全、国计民生、公共利益”[15]的关键信息基础设施，《密码法》、《网络安全法》等法律和一系列条例法规中均将对其的保护工作作为重点强调，这也正体现了当前的各领域信息保护框架下，打造从基础设施至服务平台、从运营商到用户、从信息严格管理到产业长远发展的全方位防护体系关键一环的政策取向；对于金融业务中的风险，各类立法从机构自身的资本充足率和内控管理、交易对手的安全资质、业务开展的杠杆水平与技术应用等角度入手，逐步压实风险防控责任，结合鼓励各类主体参与研发安全产品、提升安全技术水平的规定，有效筑牢了金融科技安全的“防线”。

[15] 2021 年 4 月 27 日，国务院公布的《关键信息基础设施安全保护条例》第二条规定：本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

2.6 突出了对用户隐私的保护，从多层次、多方面、多角度维护用户的合法权益

作为有效保护各类参与主体合法权益的权威途径，金融科技安全立法活动以明确金融科技安全的核心与重要事项权责为路径，来自中央和地方、法律与规章、针对采集端和服务端的要求从多层次、多方面、多角度对在接受服务时常处于劣势地位的用户群体予以突出保护。以《数据安全法》、《个人隐私保护法》等关于用户隐私保护的内容为引领，各部门和地方政府制定的综合法规、技术规范围绕有关金融科技安全的社会热点和纠纷焦点层层推进，以反垄断、反“杀熟”来消减用户群体的交易劣势，以限采集、选协议来消减用户群体的使用劣势，以限推荐、反跟踪来消减消费者的认知劣势，这些规定切实体现了以人民安全为宗旨，切实维护广大人民群众安全权益的安全管理要求。

2.7 缓解了当前金融科技安全方面的突出矛盾，并为金融科技发展充分预留创新空间

第一，除上文中提到的个人信息保护问题外，金融科技安全立法亦对“赢者通吃”与系统性风险防化等随金融科技发展产生的突出矛盾着手处理。如在金融科技加速行业规模扩张、加深机构关联和业务关联的背景下，为防化银行业的“大而不能倒”风险，央行和银保监会以《中国人民银行法》、《银行业监督管理法》、

《商业银行法》等为根据制定了《系统重要性银行评估办法》，根据规模、关联度、可替代性和复杂性等指标对系统重要性银行进行评估识别，并采取信息披露等差异化监管，为提升银行业抵御风险、加强自救能力起到了积极作用。

第二，金融科技安全立法在着力缓解突出矛盾之余，也为行业企业充分预留了创新空间。如《数据安全法》中规定“开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理”[16]；《金融数据安全数据安全分级指南》中依照影响对象和影响要素等因素对各类金融数据进行了安全定级与细分。这些科学合理的技术标准与全面客观的业务约束实际上为金融科技创新发展构建了相对稳定的政策环境和渐趋公平的营商环境，统一的标准为企业间数据共享和价值挖掘提供了坚实基础。在行业企业满足了这些原则性和基本约束性要求后，便可以在方向相对明确、空间较为广阔的法律环境中长期开展“守正创新、安全可控、普惠民生、开放共赢”[17]的创新活动。

[16] 2021 年 6 月 10 日由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议表决通过的《中华人民共和国数据安全法》第二十八条规定：开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

[17] 2019 年 9 月 6 日，中国人民银行发布的《金融科技（FinTech）发展规划（2019-2021 年）》指出：金融业要秉持“守正创新、安全可控、普惠民生、开放共赢”的基本原则。

3 我国金融科技安全立法存在的难点和问题

3.1 关于数据所有权、交易权、收益分配权确权和数据交易的法律问题

数据的所有权是围绕数据进行交易与收益分配活动，进而激励数据价值挖潜、促进要素市场培育等行为的基础。但基于交易场景的数据确权，在已有的法律中尚未存在关于原始数据权属的详细规定。在实践中，对于个人在数据控制者即运营方进行数据交易活动时，是否具有及如何行使所有权依然存在空白，交易权和收益分配权也因而无从谈起。

目前来说，数据相关权利迟迟未能立法确权的原因可能有如下几点：一是数据本身是生产要素，围绕数据进行的交易行为会涉及要素分配，进而影响社会公平。[x]将数据交易产生的收益统归于运营方无疑会扩大财富不均，甚至诱发平台“掠夺式”收集数据的可能。但能直接产生价值的往往是大数据及其处理活动，而非极特定用途下的单一数据。在大数据具有“1+1>2”特点的前提下，难以确定单一数据的交易价值；二是基于商业目的的数据交易也常常伴随着用户人格权被侵犯的风险，需要配套设计较为科学严谨的保护制度；三是确权行为基于确权对象的成本收益考量，过于严格的产权限制与保护会严重减缓数据交易、数据市场、数据产业和数据生态的发展，进而影响将数据外部性内在化

的进程。

最后，确权立法的难点可能需要在数据交易的商业实践中逐步解决。[xi]现阶段央行等部门依据《数据安全法》进行的金融数据分级分类立法活动对推进数据交易起到了重要推进作用。有了不断细化的行业分级标准，商业机构就可以据此在权属未定的商业活动中积极自主探索数据交易内容、范围与定价，并重点关注重要数据分级内容，以规避未来可能产生的金融或法律风险。而最终的立法结果，可能就产生于这一围绕各方权益不断博弈的、平衡公平与效率的过程中。

3.2 关于网络数据与司法证据间的法律问题

第一，网络数据规模呈几何式膨胀，流转路径庞大复杂，产生了溯源取证的客观难题。从信息收集环节看，在同业机构的信息收集范围受相同约束的情况下，不同机构有对相同用户提供服务并收集相似信息的可能；从信息流转环节看，相同信息被多领域、多地域、多主体共享，且外界难以知晓机构对某一数据的实际掌握情况。一旦出现数据泄露，难以就被侵权的数据片段进行溯源取证并相应追责。[xii]

第二，国际间的数据政策壁垒加大了跨境取证难度。于 2018 年生效的美国《澄清境外数据合法使用法案》（the Clarifying Lawful Overseas Use of Data Act，the CLOUD Act，别称“云

法案”）中规定，“云上存储数据的美国企业”和“与美国有足够关联且受美国管辖的企业”都要在美国政府提出要求时对其转交数据[xiii]，这便构建了美国对境外数据实施“长臂管辖”的法律基础。而针对这一法律，欧盟的 GDPR 中规定，“任何法庭判决、仲裁裁决或第三国行政机构的决定，若要求控制者或处理者对个人数据进行转移或披露，需满足如下条件.....”[18]；我国的《数据保护法》第三十六条对此要求“应当向主管机关报告，获得批准后方可提供”，这些对抗立法[xiv]在客观上增厚了国际间的数据壁垒，加大了跨境司法取证协作的难度。

第三，由网络数据得出的分析结论需满足一定条件才能成为司法证据。基于证据的客观真实性、合法性和关联性要求，网络数据本身需要保证其与事实相关内容的全面、完整、真实性，不能存在因故意隐瞒或增删改原始材料而形成有利结论的基础；提供的网络数据需被合法取得，处理的过程和得出的结论也需要满足个人信息保护等要求；数据的处理分析过程需要保证真实、科学、严谨，分析方法与工具通常应得到业界的普遍认同[xv]或司法的认证同意，并得出与认定事实有关的结论，才应被考虑认定为司法证据。

18 欧盟通用数据保护条例 GDPR 第四十八条规定：任何法庭判决、仲裁裁决或第三国行政机构的决定，若要求控制者或处理者对个人数据进行转移或披露，同时满足以下条件时方能得到认可或执行：一是该判决、裁决或决定必须基于提出请求的第三国与欧盟或其成员国之间订立的法律互助协议等国际条约，二是该判决、裁决或决定不会对本章规定的其他转移形式产生消极影响

3.3 关于人工智能等金融科技参与交易决策和法律责任认定的关系问题

当人工智能等金融科技作为辅助或自主进行交易决策，并产生歧视、损失或可能导致进一步损失的风险时，对机构的法律责任认定却可能因“技术中性”或“技术黑箱”而被规避。

“技术中性”即技术本身无善恶、无目的，客观的数学模型或程序在进行决策时不具有人类的主观思考能力。但看似消除主观偏见的算法却可能在建构之初隐含着运营者的价值取向与利益导向，最初设置的歧视倾向也会在自主学习中逐渐成型，进而在形式上将主观问题包装成为客观失误，将自身从主要责任中剥离[xvi]。

上述情形实际上就体现着“技术黑箱”或“算法黑箱”问题。“技术黑箱”有两层含义，一是因底层算法的交织嵌套与不透明性而对用户与监管部门及时了解识别风险造成阻碍的“外部黑箱”；二是由人工智能深度学习自动优化的算法形成了可能对机构自身风险管理构成一定影响的“内部黑箱”。无法辨明有关主体是否有主观恶意并尽到保护责任，黑箱的存在使归责难度陡然上升。

要明确人工智能参与交易决策活动中的法律责任，首先需要“拆解黑箱”，定期全面评估算法的运行逻辑与可靠性。当前，央行发布的《人工智能算法金融应用评价规范》构建了基于资金

类与非资金类场景的人工智能金融应用安全性、可解释性、精准性和性能评估框架，分别针对可用性、适用性与应用水平做出了详细规定，形成了黑箱治理的初步基础。即对于人工智能决策的业务，其安全性和精准性情况不但逐渐为监管部门所掌握，且将被指标化披露以对消费者及时做出风险提示。但在此基础之上，仍需探讨的还有两部分：责任分类与惩罚措施。一方面，鉴于金融科技创新速度快、频次高的特点，已有评估框架不一定能及时调整并建立起实质性约束，此时对于创新最快、风险最大的应用领域应当做出重要性区分，将该领域的责任事先划定，从而避免机构在过度创新的同时规避惩罚；另一方面，对于在各项评价中表现不佳的应用，对其做何种方式与程度的处罚，以满足业务安全开展、市场秩序稳定与消费者信任维持的需要，亦为与法律责任相关的重要问题。

3.4 关于基于区块链的智能合约的法律问题

智能合约是参与方基于双方意思表示一致而达成并自动执行的数字化契约。基于区块链的智能合约具有不可篡改的特征，在智能合约代码被编制到链上并经双方确认同意后，代码就能实现不被修改、不被终止地依据预设条件自动运行。基于这一特征，便产生了智能合约法律有效性的多个问题。

第一，智能合约是否应当被视为法律意义上的合同。如果按

照有关定义将智能合约看作专用于执行的代码或应用程序，则更应将其视为合同履约工具[xvii]；也有观点认为，如果将智能合约视为满足主体平等、意思表示一致等全部合同特征的契约，且满足《民法典》合同编中关于合同成立和生效等内容的规定[xviii]，便可以将其视为生效的合同。

第二，现有法律缺少对智能合约的约束能力。代码不可篡改且自动执行的设计突出了智能合约“代码即法律”的特点。这代表着，在区块链中，代码不依赖于由司法提供的强制力保障[xix]，同时司法也不直接具有干涉合约自动执行的能力。这种代码至上、逻辑至上的设计无疑构成了对法律约束力的挑战。

第三是智能合约执行时的归责问题。代码是智能合约的存在基础，当因合同双方或由其聘请的第三方编写的代码出现错误而导致交易不能执行或错误执行，抑或是在合同执行中一方因发现合约漏洞而要求另一方返还所得并重新订立合约时，造成的损失应由谁来担责尚不明确，而归责的基础依然建立在智能合约的法律认定之上。

4 加强我国金融科技安全立法的政策建议

4.1 坚持总体国家安全观的立法思路，走中国特色的金融科技安全立法道路，防范和化解重大金融科技安全风险

（1）做好宏观统筹，发挥安全立法的引领性

金融科技安全立法活动要立足于金融科技的转型引擎、防化利器定位，统筹国内外、各领域、各区域、各主体发展情况，更好引领金融科技安全创新。结合人类命运共同体理念，建立与国际主要国家相接轨的制度标准，提高跨境法律的数据主权保护能力，推动数字法币等前沿创新，加强中国制定国际金融安全标准的话语权与行动力；增强安全立法的普遍覆盖性，逐步健全涵盖金融科技安全主要业务领域、技术环节和金融产品全研发周期的全面立法体系，补充完善数据安全等监管标准和逆周期等监管政策工具；结合不同区域金融科技业务的发展差异与风险可能，在中央侧重重大风险管理的立法框架下分批鼓励区域性立法探索与制度试水；划清政府与市场边界，变强制为引导，制定完善政务数据开放目录，合理制定定性定量监管指标，科学制定对运营方的准入与业务评估等监管要求，加强合规审计；逐步打破行业数据孤岛，关注对长尾用户开展服务的规范性与风险，统筹好发展与安全。

（2）加强重点管理，突出安全立法的针对性

金融科技安全立法活动要围绕金融安全管理核心，加强重点管理，形成重大风险防化屏障。完善宏观审慎政策框架，明确定义政策目标，结合已有的评估指标与办法全面识别监管对象的风险防范能力，根据结果制定对系统重要性个体的一致与差异管理办法；探索人工智能、大数据等前沿科技在金融科技监管的应用

方向，推进政企金融基础设施安全建设，鼓励企业积极参与安全技术研发与安全人才培养，加强监管部门对行业各类安全信息的获取效率与态势总体感知把握能力，化解影子银行风险，提升穿透性监管水平；科学制定突发重大风险应急预案，健全行业应急管理能力；关注数字平台垄断情况，定期评估其与银行业金融机构的业务关联与杠杆水平；充分保障用户与儿童等特殊群体权益，制定重要金融机构对经营状况、数据保护能力的信息披露要求，逐步解决信息不对称问题与隐私隐患。

4.2 不断优化我国金融科技安全立法的法律结构，加强我国金融科技安全立法的统筹协调，提高金融科技安全立法的质量和效率

（1）完善法律体系，增强安全立法的系统性

从系统论的视角来看，脱离了系统的元素难以有效发挥其在系统中原应发挥的功能。因此，金融科技安全立法活动要结合行业发展战略，探索在法治领域建立专注于金融科技安全的完善体系。持续充实金融科技安全立法的总体框架，统筹立法部门与行政部门立法规划，逐步整合清理过去行政部门出台的规范性文件，将碎片化、短暂性的监管成果转化为整体性、长效性的法律体系，将零散的各类规范性文件有机整合成逐渐完善的系统。全面推进人大立法进程，加快形成高位阶、重针对、成系统的立法

成果，以期形成对从业主体或交易行为的长远约束；科学推进部门立法进程，发挥中央部门、地方政府、行业协会立法定规的灵活性与实践优势，建构完善从法律到指引指南再到公约标准的三层体系，补足细化金融业务快速创新下缺位的法律规制。

（2）协调部门立法，缓解安全立法的冲突性

金融科技安全立法活动要加强不同部门立法过程中多方面、多环节、多层级、多主体的协调联动，平衡好立法秩序与管理目的，拓宽规制领域。基于金融科技跨领域、跨市场、跨地域的融合特点，及时完善更新国内法律法规目录检索工具，严格比照现有立法文件，避免多头监管时的规则适用冲突及监管空白、监管套利问题。严防因客观形势急剧变化而“急转弯”式制定政策，进而导致相关领域主管监管部门产生立法或执行不稳定、不确定的负面效应，科学有效提升监管效率。

（3）厘清监管职责，提高安全立法的有效性

金融科技安全立法活动要形成清晰的权责边界。及时明确监管主体与职责，加强对灰色地带的创新行为监管。完善既有实践，将对混业监管行之有效的国务院金融委和金融委办公室地方协调机制及时纳入法律框架，在横向与纵向的有效沟通中压实主体责任；细化监管内容与要求，健全技术标准、重大违法违规行为的类型化认定标准与归责内容[xx]，如将算法模型纳入金融风险的评估体系，在市场份额之外增加对数字平台垄断的认定要素，以

良好补充现有立法中的原则性规定，提高定量或定性监管与处罚执行的能力。

4.3 加快我国金融科技安全专业立法，更好地适应金融科技快速发展变化的需要，更好地保障金融科技行业安全发展

(1)科学调整周期，降低安全立法的滞后性

金融科技安全立法活动要遵循金融科技发展规律，有层次、渐进式科学推进安全立法进程。把握金融创新的逐利性、技术发展的两面性等客观实际，提高关键性、基础性法律的立法速度与修订频率，使法律充分发挥应有的发展指导作用，避免专门法律缺位带来的处罚不对等和限制业务引进创新等问题；重视行政部门出台规范性文件的重要性与必要性，结合所涉行业、演化路径、变动方向等创新趋势，分别制定中期或长期专项发展规划来提高行业主管与监管部门对混业、跨区展业经营的认识与应对水平，以评估标准、技术规范为基础，先行培育有序的创新发展环境，并在商业实践探索中及时跟进确立管理原则，逐步填补对象、要件、权利、要求与罚则等立法内容。

(2)加快专业立法，提升安全立法的预见性

金融科技安全立法活动要围绕管理效率提高立法的专业性和预见性，成为提高国家金融治理效能的有力支撑。从总体上促进金融风险处置思路由运动式向回应式转变[xxi]，调整重事后、

少前瞻的危机补救式立法逻辑。完善行业机构信息披露与报送机制，定期开展金融风险排查与技术攻防演练，结合安全策略合理性、流程严密性等因素科学设计安全评估内容，强化源头治理；警惕人工智能自主学习可能产生的偶发性交易风险，研究确定对其法律责任的判定原则；优化牌照管理制度，充分发挥牌照制度对行业准入的风险限制与资质过滤作用，对经营限定业务的主体颁发有限牌照，对同类业务采取一致性监管；重点强化地方金融监管能力，研究地方金融监管部门对跨域展业的管理权责安排，选择事权适度上移或尝试建立中央指导下的多地协调监管机制；重视一线风险预警作用，疏通政府部门与行业组织、用户群体的反映申诉渠道，对风险及时识别处置，避免造成更大损失。

(3)探索包容立法，强化安全立法的支持性

金融科技安全立法活动要突出对创新的包容和指引性，形成宽严相济的呵护环境。以业务分级分类为基础，允许行业机构在高风险高危害范围外适度创新，避免过早框定与过严管束对新兴业态的巨大阻滞；对国内已有充分试点经验和良好效果的监管沙盒等制度的具体要求用立法活动确定下来，包括准入机构、类别、期限与内容，用户资质、监管权责与处罚清单等；实行差异化监管，对重技术、重数据的领域可以考虑适当对初创企业放宽资本门槛或提供支持性贷款，对低风险而发展成熟的领域适当简化审批程序；建立监管部门与市场的沟通对话机制，促进双方相互了

解行业发展趋势与监管方向要求。

4.4 借鉴国际金融科技安全立法的理念和经验，把握世界金融科技安全趋势，共同推进金融科技的全球安全

从消费者信息与权益保护立法的国际经验上看，上文中提到的 GDPR 和 CCPA 具有很多值得关注的，关于消费者权利和处理者义务的特色规定。在消费者权利方面，有数据主体拥有提出要求时的删除权、未基于个人同意处理时的反对权[xxii]以及不因积极保护隐私而受歧视的权利，可选择的信息不被销售和退出权利等；在处理者义务方面，则有多处体现着处理者履行义务时的成本考量和企业主体保护。如实施成本是保障数据处理安全的要素之一，当需要付出不相称的努力时可以不履行向数据主体通知泄露情况的义务，要求企业设置具有专业能力的数据保护官（Data Protection Officer，与我国的个人信息保护责任人有些类似）来提供合规帮助和主体的数据权利实现等。再如对于消费者的信息完整性和隐私保护上，美国《全面信用法案》（Comprehensive Credit Reporting Enhancement, Disclosure, Innovation, and Transparency Act of 2020）[xxiii][xxiv]中提到了诸如当消费者对自身信用报告提出质疑时，信用报告机构和信息提供者分别负有信息披露和真实性证明责任；当提供者在规定的时间内提供特定负面信息时必须让消费者知悉；要求信用报告机构删除或缩短部

分不良信息在信用报告停留的时间等内容。

从加强金融科技监管水平立法的国际经验上看，于 2019 年提交美国国会审议的《金融科技法案》（Facilitating Innovation and New Technology so Entrepreneurs Create and Hire Act of 2019）[xxv]和新加坡的《支付服务法案》（PAYMENT SERVICES ACT 2019）[xxvi]对我国加强监管协调和细化具体业务监管有一定启示。如前者建议专门设立管理金融科技初创公司的机构，并规定金融科技初创公司诸如技术创新、改善产品或服务的可得性、不对消费者保护构成风险、不产生金融系统性风险等证明要件；要求监管机构在采取行动时需要沟通协调；设立向监管机构提供有关优化监管、执法失误等非强制性建议的咨询委员会等[xxvii]。后者则针对支付服务的准入门槛（持许可证方可经营，机构能够提供的支付种类或数额受许可证类别限制）、支付机构向当局定期报告的事项、一般和紧急情形下监管部门的监管权力与提供国际监管援助时的条件、因素与援助范围等内容。

从促进金融科技创新创业立法的国际经验上看，于 2019 年批准的《菲律宾创新法案》（Philippine Innovation Act）与《创新型创业法案》（Innovative Startup Act）是政府直接支持创新创业活动和中小微企业发展的典型案例。主要包括成立旨在“制定国家的创新目标、优先事项和长期国家战略”，由总统、多部门领导和商界、学界成员组成的专门机构——国家创新委员

会，并由这一机构负责制定重要支持计划和长期创新发展战略[xxviii]；积极支持国家重点和可持续发展行业创新，包括可持续农业、数字经济、教育、卫生、安全、基础设施、气候等；由相关部门制定涵盖技术推广、会计、专利等方面的辅导项目和创业援助计划，推动中小微企业发展合并并走向国际化；设立 10 亿比索的初始循环基金用于商业补贴、自主研发等[xxix]。这对于我国围绕因资本限制而具有较弱风险抵御能力的初创企业制定专门的鼓励、保护与支持政策有一定借鉴意义。

参考文献：

[i] http://thuifr.pbcsf.tsinghua.edu.cn/1783.html
[ii] https://www.sohu.com/a/241354142_99955888
[iii] https://mp.weixin.qq.com/s/fl_Y9hnNXi0z39RulYSQ-g
[iv] http://www.sz.gov.cn/szzsj/gkmlpt/content/8/8935/post_8935483.html#19236
[v] https://www.freebuf.com/articles/neopoints/221180.html
[vi] https://2ly4hg.smartapps.cn/pages/article/article?authorId=742686&spm=smbd.content.share.0.1629461949733aB179Wt&_trans_=010005_wxhy_shw&hostname=bdlite&articleId=407636536&_swebfr=1
[vii] https://baijiahao.baidu.com/s?id=1681511555547520051&wfr=spider&for=pc
[viii] https://www.163.com/dy/article/GEALK2KJ05315Y1B.html
[ix] https://www.sohu.com/a/427058592_455313
[x] https://baijiahao.baidu.com/s?id=1692359923850707977&wfr=spider&for=pc
[xi] https://36kr.com/p/1283514213564929
[xii] http://app.myzaker.com/news/article.php?pk=60c86df08e9f0946a75c0f74&f=huangli
[xiii] https://baijiahao.baidu.com/s?id=1670531652191204520&wfr=spider&for=pc
[xiv] https://www.weiyangx.com/366331.html
[xv] https://www.chinacourt.org/article/detail/2016/12/id/2365614.shtml
[xvi] https://www.sohu.com/a/374932278_778854
[xvii] http://www.zhonglun.com/Content/2020/01-09/1556473454.html
[xviii] http://blog.sina.com.cn/s/blog_7fecd5ee0102z2l7.html
[xix] http://www.elecfans.com/blockchain/845464.html
[xx] http://www.china.com.cn/opinion/think/2015-04/13/content_353046

85.htm

[xxi] https://www.163.com/dy/article/EG1GNS5005198R91.html

[xxii] https://xw.qq.com/cmsid/20210823A0D07600

[xxiii]

https://www.congress.gov/bill/116th-congress/house-bill/3621?__cf_chl_jschl_tk__=pmd_ecb79d35a56ab21ad0ce85dbd252896b96d01114-1628993178-0-gqNtZGzNAfijcnBszQl6

[xxiv] https://www.sohu.com/a/372692486_115173

[xxv]

https://www.congress.gov/bill/116th-congress/house-bill/1491/text?q=%7B%22search%22%3A%5B%22FINTECH+Act+of+2019%22%5D%7D&r=1&s=2

[xxvi]

https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220

[xxvii] https://www.sohu.com/a/397831936_99955888

[xxviii]

https://fintechnews.sg/32772/fintechphilippines/philippines-duterte-innovation-act/

[xxix] https://www.sohu.com/a/294933448_324617

作者简介：

周道许　清华大学金融科技研究院金融安全研究中心主任

王兆峰　北京周泰律师事务所主任

张恩权　中国财政科学研究院 硕士研究生

饶　倩　清华大学金融科技研究院金融安全研究中心研究专员

彭天择　北京大学光华管理学院 本科生