法商研究 Studies in Law and Business
Vol. 42 No. 2(2025)

我国网络安全风险的保险治理困境与法治化纾解

徐 浩 宇*

摘 要:数字经济时代,网络安全风险治理法治化是推进国家治理体系与治理能力现代化的必然要求。保险在分散网络安全风险的同时,也日益成为网络安全风险治理的重要工具。传统政府规制模式向社会自我规制模式的转换和保险社会治理功能的拓展,是网络安全风险保险治理的理论逻辑;法定义务契约化、规则制定私人化以及风险控制市场化三者间的有机联结,共同勾勒出网络安全风险保险治理的实践逻辑。在网络安全风险保险治理场域中,保险治理制度框架缺失、规范供给不足以及风险信息互联不畅的现实困境,催生政府与市场相结合的二元协同治理结构,并成为网络安全风险保险治理的应然范式选择。未来在完善网络安全风险保险治理的制度框架、补足网络安全风险保险治理的规范体系以及强化网络安全风险保险治理的信息互联之外,还应健全网络安全风险保险治理的定期汇报、同行评议与容错机制,以期协同推进网络安全风险保险治理的法治化。

关键词:网络安全风险 保险治理 网络安全保险 网络安全保护义务

当下,人工智能、物联网通信、算法等数字技术在给经济社会带来巨大变革的同时,也将用户逐渐引入所谓的“数字风险社会”,风险与数字技术在多个层面以不同方式发生耦合。由此,如何妥善因应网络安全风险已经成为国家数字能力建设的重要内容。① 事实上,保险公司已为公司应对网络安全风险提供了一种保护手段,使其尽可能规避与网络安全事件相关的财务责任。我国在实践中已经注意到网络安全保险在网络安全领域的重要价值。截至 2022 年底,我国共有 30 余家保险公司备案了 78 款网络安全保险产品,②而 2023 年 7 月 2 日发布的《工业和信息化部国家金融监督管理总局关于促进网络安全保险规范健康发展的意见》(以下简称《意见》)也指出

* 厦门大学法学院网络空间国际法研究中心助理研究员
基金项目:国家社会科学基金资助项目(23VMG013)

① 参见高奇琦:《国家数字能力:数字革命中的国家治理能力建设》,《中国社会科学》2023 年第 1 期。

② 参见国家工业信息安全发展研究中心:《网络安全保险研究报告》,http://www.secrss.com/articles/52457,2024-10-10。

“网络安全保险……日益成为转移、防范网络安全风险的重要工具”。[①] 以往对网络安全风险治理的研究,大都侧重于技术层面的攻防策略探讨,对经济法如何规制网络安全这一命题有所阙如,[②]这也致使当前对网络安全保险如何参与网络安全风险治理的理论研究仍较为匮乏。有学者从保险作为网络安全风险分散机制的视角出发,对网络安全保险未来制度构建进行了一定的探讨。[③] 也有学者将网络安全保险视为网络风险的治理工具,并指出其能够填补侵权人不明、损害范围不确定等特定场景下的部分经济损失。[④] 还有学者认为,网络安全保险在网络安全风险管理方面的独特优势,使其成为提升政府安全监管效能的有力配合手段。[⑤] 有鉴于此,笔者试图对网络安全风险保险治理的理论逻辑与现实基础进行阐明,并通过梳理当前我国网络安全风险保险治理所面临的现实困境,探寻网络安全风险保险治理法治化的应然范式,助力我国网络安全风险保险治理的制度化与规范化,进而推进国家治理体系与治理能力的现代化。

一、网络安全风险保险治理的兴起与生成逻辑

(一)网络安全风险保险治理的兴起

保险从诞生之日起就明确了其分散风险、共担损失的补偿者定位。尽管保险的商业功能突出,但也具有一定的社会治理属性,尤其是在降低经济风险、环境风险、技术风险和政治风险等方面,特殊类型的保险发挥了重要作用。

作为特殊险种的网络安全保险往往比普通商业保险在特定类型的财产损失预防上更具优势:网络安全保险产品还包括有效的网络安全实践指导、免费或折扣的技术解决方案以及数据泄露后的补救措施。也正因如此,在《欧盟通用数据保护条例》对数据保护与个人信息安全的高标准、严要求与重处罚态势下,2018 年,英国有 90%的公司拥有特定网络安全保险,而美国则为 76%,即使在网络安全保险发展缓慢的瑞典,也有近 57%的公司拥有网络安全保险。但从体量上看,在 2019 年全球网络安全保险市场份额划分中,美国占 62%,英国占 16%,而欧盟则占 14%。[⑥] 然而,由于早年间网络安全保险的定位不明确,我国国内网络安全保险往往是作为风险与收益错配的新兴险种而存在,并未充分发挥其应有的网络安全风险治理之功能。尽管《意见》在形式上只明确了网络安全保险作为网络安全风险防范、分散工具的地位,但其实质上也已默示承认了网络安全保险作为风险治理工具的属性。

(二)网络安全风险保险治理的理论逻辑

保险对风险的治理是凭借保险人充当支持和补充政府治理(监管)风险的私人监管者(私人

① 《工业和信息化部 国家金融监督管理总局关于促进网络安全保险规范健康发展的意见》,https://www.gov.cn/zhengce/zhengceku/202307/content_6892557.htm, 2024-10-10。

② 参见张守文:《经济发展、网络安全及其经济法规制》,《中国政法大学学报》2022 年第 2 期。

③ 参见唐金成、莫赐聪:《数字经济时代网络风险分散机制构建研究》,《西南金融》2023 年第 7 期。

④ 参见周瑞珏、赵精武:《网络安全保险的法理基础与实践路径》,《湖北社会科学》2023 年第 4 期。

⑤ 参见赵亚宁:《数字经济时代保险参与网络安全治理的制度困境与纾解之道》,《保险研究》2023 年第 5 期。

⑥ See Kurmaiev P., Seliverstova L., Bondarenko O. and Husarevych N., Cyber Insurance: The Current Situation and Prospects of Development, 9 Amazonia Investiga, 70(2020).

规制者)的身份而实现的,[①]网络安全保险亦是如此。私人规制可弥补政府规制在特定领域资源与智识的缺陷,对某些行政任务的执行更具效率。[②] 保险则是这种私人规制的显著代表,因为它既需要制定和执行标准,又要在监管其他各方行为时承受许多与国家相同的经济和社会压力。对于保险人缘何能作为私人规制者,学术界一直存在着"私人推进论"与"国家让步论"之争。[③]持私人推进论者认为,私人规制的出现是因为私主体实施规制活动有利可图,所以企业有动力承担标准制定与执行等一系列规制成本。[④] 例如,有学者在对以消费电子行业为代表的新兴商业领域的研究中发现,以利益驱动为导向的私营企业比国家机构更有能力与动力为复杂技术问题制定最优解决方案。[⑤] 而主张国家让步论者则指出,私人规制是国家行动缺失的产物,并非私人行为者抓住了所谓的商业机遇,其可能源于国家对某些领域的疏于管控,也可能是国家选择对私人行为者进行相应的监管责任配置以减少详细的标准制定和执行成本的结果。[⑥] 在公权力监管难以发挥有效作用的领域,如面对新兴科技或复杂金融产品实施监管时,国家更有可能退缩,正因如此,相关专业知识更为丰富的私人行为者就有动力介入并提供最低限度的规制从而代替政府规制,对于国家而言,在直接成本花费考量上反而是收益较高的结果。

1.传统政府直接规制模式的转向

作为国家让步论的理论支撑,在法律自创生理论框架中针对政府及法律子系统去中心化的理论构想,有助于回应当下科技革新与法律系统稳定性之间存在的博弈和张力,不仅解释了法律系统应如何适应科技发展变化,而且也是网络安全风险保险治理的宏观理论基础。

在传统规制手段于众多新兴领域的规制效果并不尽如人意的背景下,社会系统论指出,对"命令—控制"模式的路径依赖,致使法律系统认知的全能性被过度推崇,从而忽视了社会子系统的运行的自洽性。[⑦] 相较于传统规制,法律自创生理论更为强调法律应着重发挥在其他社会子系统自我界定过程中的支撑作用,为社会子系统间设定边界。[⑧] 有效的规制模式应当具备以下3个特征:(1)规制主体应由单一政府主导拓展至多元主体参与。其理由在于,传统层级权力以金字塔形式结构呈现,而数字社会内嵌的去中心化技术手段弱化了上下层级权力间的"键能",经济、科技等子系统也因其独立的运作方式而瓦解和重新分配实施规制所必需的权力和资源。[⑨](2)规制的方式应从"命令—控制"转向为自我规制提供指引。根据法律自创生理论,此种间接规

① 参见何启豪:《国家治理现代化背景下的保险法理论新范式——以保险人作为私人监管者为中心的考察》,《现代法学》2019年第4期。

② 参见高秦伟:《私人主体的行政法义务?》,《中国法学》2011年第1期。

③ See Trey Herr, Cyber Insurance and Private Governance: The Enforcement Power of Markets, 15 Regulation & Governance, 100(2021).

④ See Lecraw Donald J., Some Economic Effects of Standards, 16 Applied Economics, 519－520(1984).

⑤ See Knill C. and Lehmkuhl D., Integration by Globalization: The European Representation of the Consumer Electronics Industry, 8 Current Politics and Economics of Europe, 131－153(1998).

⑥ See Tim Büthe and Walter Mattli, The New Global Rulers: The Privatization of Regulation in the World Economy, Princeton University Press, 2011, pp.203－207.

⑦ 参见谭冰霖:《环境规制的反身法路向》,《中外法学》2016年第6期。

⑧ 参见张骐:《直面生活,打破禁忌:一个反身法的思路——法律自创生理论述评》,《法制与社会发展》2003年第1期。

⑨ 参见周尚君:《数字社会对权力机制的重新构造》,《华东政法大学学报》2021年第5期。

制路径更有助于激发被监管者提升自我表现的积极性与创造性,同时也能更好地利用多元主体的智识优势以形成合力,弥补政府规制过程中执法资源的不足与信息获取的劣势。(3)规范的形式应从具体详细的规则转变为设立更为抽象的规范。亦即,在各个社会子系统中法律是作为起支撑作用的“四梁八柱”而存在的,旨在为不同子系统中的具体规则与决策程序的设立提供规范性指引。①

可以看出,法律自创生理论视角下有效规制模式对传统规制主体的拓展以及规制方式的转变与规范形式的调整,亦与网络安全保险实施私人规制的内在逻辑相契合:一方面,法律通过抽象性规范的设定发挥规则的指引与社会子系统的支撑作用;另一方面,网络安全保险人作为私人规制者,直接参与该社会子系统内网络安全风险的规制,协同发挥自身的智识资源优势以实现社会子系统内直接、高效的自我规制。

2.保险社会治理功能学说的发展

近年来,理论界与实务界对保险社会治理功能认识的深入,奠定了网络安全风险保险治理的微观理论基础,也有助于解释网络安全保险人的私人规制者身份是由私人资源优势而推进形成的观点。

在保险功能论层面,早期持“一元说”者指出,保险的基本功能是为损失提供经济补偿,是分散风险与转移目标的具体实现。而持“二元说”者认为保险在经济补偿功能之外还兼具资金融通、财富管理的功能;持“三元说”者则对保险的功能有了更为深刻的认识,通过实践洞见保险的社会治理效用,亦即保险通过内在机制协调,在分散风险的前提下,提供经济补偿、合理配置金融资产,甚至还可以促进政府职能转变,参与社会治理。② 而肇始于美国的“保险即治理”的理论与实践则进一步厘清了保险实现社会治理的内在机理。“保险即治理”的实现与作为“第三方监管者”的保险公司对既得利益损失的厌恶密不可分,他们倾向于通过制定保险策略和采取预防潜在风险事件的手段,尽可能确保被保险人遵守维护被保险标的之职责,最大化地降低潜在的保险赔偿可能。换言之,即保险人通过保险合同直接影响被保险人的行为模式,从而引导被保险人主动采取措施以降低潜在风险。此种借由保险的方式所实施的风险治理,实际上是对传统国家治理模式的补充。在该理论的指引下,研究人员对各种保险产品如责任险、地震险及恐怖主义风险保险进行了具体的实证研究,也为保险如何在风险管理领域发挥其有效的治理功能提供了充足的理据。③ 由此,现代保险的功能除传统的事后损失填补机制外,事前损失预防与控制机制也内嵌其中,进而在现行法律框架下实质承担了部分监管职能。④ 不难发现,保险治理理论与实践的发展,同样为网络安全保险实施私人规制的正当性证成在微观层面提供了充分的论据。

综上,可以得出这样一个结论,即网络安全保险人充当支持和补充政府治理(监管)风险的私人规制者,并非私人推进或国家让步的单一结果,而是两者共同作用的结果。在新兴科技领域,出于成本与效率的考量,国家选择鼓励市场中的私人主体进行规则与标准的自我设定、监督与管

① 参见刘岳川:《科技创新的法律规制》,《华东政法大学学报》2023 年第 3 期。

② 参见袁成:《商业保险的功能演进与中国经济社会高质量发展》,南京大学出版社 2022 年版,第 11~17 页。

③ 参见何启豪:《国家治理现代化背景下的保险法理论新范式——以保险人作为私人监管者为中心的考察》,《现代法学》2019 年第 4 期。

④ See John Rappaport, How Private Insurers Regulate Public Police, 130 Harvard Law Review, 1543-1545 (2017).

理;同时,基于利益驱动与结构性权力的获取与维持等原因,私人主体也有动力承担标准制定与执行等一系列规制成本进而开展私人规制。

(三)网络安全风险保险治理的实践逻辑

保险对网络安全风险的治理,在运行机制上主要是通过法定义务契约化、规则制定私人化以及风险控制市场化三者间的相互配合而实现的。

1.法定义务向约定义务的转化

网络安全保险发挥其风险治理功能主要是将法定义务内化于合同条款的解释活动中,并将保险合同作为治理规则载体进而开展对网络安全风险的治理。

在法定义务维度,《中华人民共和国网络安全法》(以下简称《网络安全法》)第9条与第21条通过"逐项列举+兜底规定"的方式规定了网络运营者应履行的网络安全保护义务及其内容,而《关键信息基础设施安全保护条例》(以下简称《条例》)第6条则对关键基础设施运营者提出了更高程度的网络安全保护义务,同时《中华人民共和国数据安全法》(以下简称《数据安全法》)第8条和第27条也对数据处理者施加了数据安全保护义务。需要说明的是,此类"安全保护义务"并非新设义务,其实质是《中华人民共和国民法典》(以下简称《民法典》)侵权责任编中的安全保障义务在网络安全领域适用时的特殊表达。[①] 而在保险法语境下,因被保险人投保了网络安全保险,故其承担网络安全保护义务的基础源于保险法中固有的风险控制条款。在我国保险法中,被保险人在保险法场域内对网络安全保护义务的履行是通过将《中华人民共和国保险法》(以下简称《保险法》)第51条规定(被保险人具有维护保险标的安全之义务)作为转介条款而实现的。在保险合同私法自治的范围内,可通过约定的形式为当事人配置层级更高且更为详细的安全维持义务,也可授权保险人享有对保险标的物的检查权与安全防护权。[②] 此外,《保险法》对网络安全风险的规制,还有赖于第16、21、22、52、57条之间的协同配合,以保险事故发生为分界点,分别从事前、事中以及事后3个环节对保险期间发生的网络安全风险进行规制,这同时也是被保险人在保险法框架内履行网络安全保护义务的规范来源。

就约定义务而言,在安全保护(法定)义务合同化的理论框架下,保险人对被保险人网络安全风险的规制可看作保险人辅助被保险人履行安全保护义务。与传统民法中的"履行辅助人"不同,保险人通过合同介入义务履行的行为,类似于履行义务的"实际辅助人"。然而,这种保险人干预义务履行仅是保险合同中被保险人履行维护保险标的安全之义务的外在表现形态,亦即两者并非债务共担者。但是,若换一个视角观察,保险人对被保险人网络安全风险的治理或也可视为保险人对不真正义务的履行行为。不真正义务是一种强度较弱的义务,相对人通常不得请求履行,违反该义务亦不发生损害赔偿责任,仅使此义务负担者遭受权利减损或灭失的不利益。[③] 例如,从对象上看,不真正义务指向被保险人标的的安全维护,即被保险人的信息资产安全性的维持。从结果上看,不真正义务的违反不发生损害赔偿责任,相比之下,"真正义务/法定义务"的违反需要承担损害赔偿责任。在网络安全保险合同中则体现为,保险人若不履行该"不真正义务",即不对被保险人的网络安全保护情况进行检查与督促,其将遭受赔付保险赔偿金之不利益。

① 参见杨显滨:《论场内数据交易的法律制度建构》,《政治与法律》2024年第5期。

② 参见武亦文、杨勇:《保险法对价平衡原则论》,《华东政法大学学报》2018年第2期。

③ 参见申卫星:《对民事法律关系内容构成的反思》,《比较法研究》2004年第1期。

2.市场私人标准的制定与执行

私人标准制定与执行下的市场控制,在一定程度上形塑了保险人作为风险治理者的身份,同时也使保险治理逐渐成为缓和公共规制与社会风险之间张力的重要手段。在实践中,私人标准的制定与执行,不仅在某些领域实现了对公共规制空白的填补,而且也在一定程度上对公共标准进行了细化。①

在制定标准层面,保险公司治理权能的获取与其作为特殊金融服务机构所发挥的关键作用密不可分。此类特殊金融服务机构的一个突出例子是信用评级机构。在实践中,这些评级机构利用评估风险的指标制定行为标准,而市场中的投资者则通过改变自身资本配置的方式实现对此种行为标准的遵循。在此过程中,信用评级机构创建了一种特殊机制,将市场的不确定性转化为更有条理的风险评估,从而提高了资本市场的运行效率。② 事实上,保险公司与信用评级机构的运作方式具有内在相似性,两者皆是帮助客户选择有效的风险控制手段、帮助改进风险评估方法以及通过转移责任的方式限制潜在的财务不确定性,尽可能规避未知风险可能带来的高昂交易成本。保险公司以制定供一方或双方使用的安全标准的方式,帮助市场交易减少不确定性从而降低风险,同时还会为其客户设定安全标准基线,并利用规范化标准评估客户风险状况,将此作为行为参数相应调整保费。可以说,是实践中市场对保险的需求逐渐将这种风险管理能力转化为一种执行权力。

在执行标准层面,保险公司利用安全标准来评估和管理客户的风险,并通过保单中的条款直接执行这些标准,开展对客户的风险治理服务。在实践中,大量网络安全保险的保单条款中包含了各种履行网络安全标准的要求,涵盖了第三方制定的行业标准以及部分保险公司制定的标准。在网络安全事件发生后,若被保险人未执行保单中所约定的标准,保险公司可能会对网络安全事件所造成的损失仅给予部分赔付,甚至拒绝赔付。

3.风险定价对信用风险的控制

在市场实践中,信用风险定价范式下的经济激励是网络安全保险开展风险治理的重要依托。社会分工结构的客观性与市场运行规律的必然性决定了信息不对称的出现难以避免。与政府规制机构相比,保险人对网络安全风险的治理更为及时、高效且更具有针对性,有助于减少网络安全风险治理中的信息不对称。保险人作为私主体,与企业主体(被保险人)之间具备二重关系。一则,两者为利益共同体。在保险条款约束下,被保险人与保险人处于利益相互绑定的损失共担之状态,被保险人能否获得保险金以及金额的多寡取决于其自身行为;③二则,双方存在利益博弈。出于更多地获取经济利益的目的,被保险人易于引发道德风险,而保险人为了维护自身利益不受损失,则有极强的动力规制被保险人所可能存在的风险。在网络安全风险规制中,通过网络安全保险这一“转接口”,网络安全风险以投保这一方式进行转化——作为新兴风险的网络安全风险与具有较为成熟规制体系的金融风险之间发生实质链接——并将其置于互联网金融风险的

① 参见高秦伟:《跨国私人规制与全球行政法的发展——以食品安全私人标准为例》,《当代法学》2016 年第 5 期。

② See A. Claire Cutler, Virginia Haufler and Tony Porter, eds., Private Authority and International Affairs, Suny Press, 1999, pp.159－160.

③ 参见武亦文:《保险法上道德风险控制机制省思》,《中外法学》2022 年第 6 期。

规制范式之中，便实现了对网络安全风险的规制工具补足。在这一范式下，信息的弱势方被授予了筛选信息的主动权，同时也获得了先发优势及制定规则的权利，从而能够有效预测和制约信息优势方的潜在逆向选择与道德风险。该范式通过以完全信息市场为依托的风险－收益逻辑，对信息不对称和信用风险问题进行化解。换言之，当信用风险得到合理定价，道德风险和逆向选择的问题也就转化为信息问题，进而被内化进价格之中。① 在网络安全风险规制中，信用风险定价范式对网络安全风险的控制主要体现为保险人对被保险人网络安全风险的事前风险防范与事中风险评估。在事前的风险防范层面，保险公司通过保费减免激励等方式，促进被保险人提升网络安全防护级别或执行比法定标准更高的网络安全标准，尽可能防范网络安全风险；在事中的风险评估层面，则通过实时分析被保险人数据安全保护情况，督促其进行风险防护措施的动态调整与优化。

二、我国网络安全风险的保险治理困境

以前，我国企业对网络安全风险的危害性认知不足、投保意识不强，故我国的网络安全保险市场长期处于低迷状态，相关法律规范并不健全，间接导致当前我国网络安全风险保险治理面临制度框架缺失、规范供给不足以及信息互联不畅等困境，使得网络安全风险的保险治理无法发挥其应有作用。

（一）制度框架缺失

当前网络安全风险的保险治理制度框架缺失，在实践中主要表现为以下两个方面：一是对于网络安全保险的适用对象是否应包括政府机关以及医院、学校等公共机构，无明确规定；二是对于网络安全保险是否应采取强制险模式以更好地实现风险控制，也无明确规定。

就政府机关以及医院、学校等公共机构能否作为网络安全保险的被保险人而言，当前法律规范层面尚无规定。事实上，因公共性使然，政府机关、学校以及医院等公共机构必然掌握着大量公民个人隐私数据以及公共数据，理应承担更为严苛的网络安全保护义务，但作为商业险的网络安全保险介入此类公共机构有无必要，加之具体措施又该如何落地，均无明确规定。而另一个关涉网络安全风险保险治理的制度问题便是，网络安全保险在定位上是否应设定为强制险。由于网络安全保险在我国仍属于相对较新的险种，对网络安全保险是否应像“机动车交通事故责任强制保险”一样设置为强制险，以及相应的配套机制该如何设计与执行，当前同样处于空白状态。

反观域外，关于网络安全保险的适用对象是否应包括政府机关以及医院、学校等公共机构，以及是否应采取强制险模式，其他各国所采取的制度范式不一。基于国别差异，我国难以直接适用。基于当前这些规范实践，可抽象出 3 种主要模式，即强制险、商业险以及强制险＋商业险混合。

第一，将网络安全保险规定为强制险。在实践中，韩国是第一个引入广泛而全面的强制性网络安全保险的国家。韩国于 2001 年便开始强制规定互联网数据中心必须投保数据泄露责任险，2005 年则将强制投保范围拓展至金融机构或电子金融业务实体，2018 年的修法又扩大了投保范围，强制要求企业购买网络责任保险，或提供相当于规定保单限额的资本准备金（《韩国促进信息

① 参见杨东：《互联网金融的法律规制——基于信息工具的视角》，《中国社会科学》2015 年第 4 期。

和通信网络利用和信息保护法》第 46 条)。尽管韩国网络安全立法多次进行大幅修改,但时至今日,强制互联网数据中心购买网络安全保险这一规定仍被保留。与韩国相比,我国企业大多为中小微企业且数字化程度不高,若我国径直将网络安全保险规定为强制险,或要求企业尽数投保或提供相当于规定保单限额的资本准备金,恐难以达致应有的网络安全风险防范的效果,而且也会对企业运营的资金流造成负担。

第二,适用单一商业险模式。有学者认为,应在维持网络安全保险商业险的基础上拓展政府的服务职能,通过政策引导或立法强制的方式设立最低保险标准,并建立风险历史数据收集机制。① 此外,还有学者指出,政府在网络安全保险规制网络安全风险的过程中应起到后备支援作用,可效仿新加坡政府建立网络安全保险风险资金池的做法,或可由国家财政作为网络安全保险中"再保险"的资金来源。② 上述做法均有可资借鉴之处,但由于现阶段我国企业对网络安全风险认知程度不高,本应为网络安全保险所覆盖的数字化程度较高的重点企业并未自主投保,致使作为商业险的网络安全保险难以发挥其应有的风险治理功效。加之,与新加坡的国情不同,我国幅员辽阔且企业众多,若我国直接采用由国家财政作为商业保险的风险资金池的做法,不仅需要调整大量法律规范为其制度创设提供法理支撑,而且势必对国家财政造成巨大的压力,结合我国目前网络安全保险所处的发展阶段,此举尚不可行。

第三,区分购买对象的"强制险+商业险"模式。有学者认为,应采取区分购买对象的"强制险+商业险"模式,即依照体量进行划分,对医院、学校等公共机构和大型企业采强制责任保险模式,而对中小型企业则采任意责任保险模式;③或进行私人企业与政府机构的划分,对私人企业适用商业险,对政府机构以及学校、医院等公共机构适用强制险,设立一个广泛的网络安全责任保险项目,并以国家税收收入支付保险金。④ 对我国而言,相较于前两种方案,此类混合险模式颇具可行性,但仍难直接适用。这是因为网络安全保险通常分为第一方险与第三方险,而将网络安全保险设置为强制险旨在以公共利益维护为核心,此种"强制险/商业险"的简单二分法显然更侧重于企业或政府等公共机构自身的利益保障,并未充分关照企业私人利益与社会公共利益之间的平衡关系,因此我国未来在借鉴此种方案时,须对其进行相应的调整与细化。

(二)规范供给不足

网络安全风险的保险治理规范供给不足,不仅导致网络安全保险合同条款规范性阙如,也造成被保险人义务履行的认定规则缺位。

第一,当前网络安全保险合同的规范性仍不尽人意。网络安全保险合同条款的设定,不仅涉及保险人能否在可承受范围内向被保险人提供更为充分的保障问题,而且其承保范围设置、损害

① See Brendan Heath, Before the Breach: The Role of Cyber Insurance Incentivizing Data Security, 86 George Washington Law Review, 1124(2018).

② See Kenneth S. Abraham and Daniel Schwarcz, Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe, 27 Connecticut Insurance Law Journal, 468-472(2020).

③ See Minhquang N. Trang, Compulsory Corporate Cyber-liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches, 18 Minnesota Journal of Law, Science & Technology, 389(2017).

④ See Sean Andrés Rapela, The Ugly Truth about Cyber Insurance&Governmental Data Breaches, 21 Journal of High Technology Law, 277(2021).

结果的认定等问题也与网络安全法律规范有着密切关联。[①] 对于因网络安全事件所导致的业务链上下游牵连性损失，哪些属于网络安全保险的损害填补范围，网络安全保险合同尚未明确。同时，对于因行政行为而造成的损失是否属于网络安全保险的损害赔偿范围的认定问题，不同的网络安全保险合同规定不同。

第二，认定被保险人是否履行法定义务与约定义务的义务履行规则缺位。以告知义务为例，对于被保险人是否履行如实告知义务的认定标准仍有待进一步细化。尽管关于网络安全保险中如实告知义务的履行，我国尚未出现相关案例，但现有的网络安全保险保单均无一例外地以“投保人是否严格按照字面意思告知保险人询问事项”作为认定投保人是否履行如实告知义务的判断标准。在德国首个网络安全保险判决中，涉案法院在秉持上述判断标准的前提下，认为该案中保险人以简单且宽泛的问题询问投保人相关事项，并未针对投保人是否更新最新信息系统和安保措施等关键问题进行详细询问，已构成事实上对这些事项所对应的潜在风险之接受，故认为投保人在应对保险人询问时，所给出的宽泛回答并不构成对如实告知义务的违反。[②] 此案的判决显然更倾向于保护投保人的利益，但也从侧面说明，若如实告知义务的履行认定标准过于模糊，在法官自由裁量权的行使下容易造成同案不同判的情况，难以形成保险人与投保人的合理预期。

当前与网络安全保险相关的法律规范指引，我国仅有《民法典》《保险法》以及《意见》，并无着眼于网络安全保险机制如何运行的微观层面的规范性文件可供遵循。虽然上海市保险同业公会发布的《网络安全保险服务规范（征求意见稿）》与全国信息安全标准化技术委员会发布的《信息安全技术 网络安全保险应用指南（征求意见稿）》，为网络安全保险的条款制定提供了可供参考的指导性方针，但囿于此类规范的强制力不足且尚未施行，难以实现网络安全保险保单标准化的有效推进。加之近年来国家对网络安全风险治理的重视程度提升，日益完善的网络安全保护法律规范为网络运营者施以多重网络安全保护义务，在网络安全保险实践先行的态势下，当前法律规范却并未明确规定此类义务如何与原有的保险法相关法律规范进行有效衔接，这也使得保险人对被保险人是否履行网络安全保护义务的认定面临新的挑战。

（三）信息互联不畅

充分的信息披露及其获取有助于避免因信息不对称与不充分所造成的风险扩散。实践中网络安全风险信息的交换不足阻滞了网络安全风险保险治理的效能发挥。在投保前，市场主体双方均处于信息不对称的状态，保险人往往难以依据被保险人的真实情况制定合理的保费，这造成大部分网络安全保险的保费金额虚高，使众多原本具有投保意愿的企业望而却步，导致网络安全保险这一风险治理工具难以充分推行；在投保后，网络安全信息交换的不顺畅、不充分也对保险人辅助被保险人对网络安全标准的执行、动态调整保费以及后续的理赔等一系列活动的开展造成了阻碍。

网络安全风险保险治理的信息互联不畅，不仅源于保险人私主体身份而引发的执行强度不足之困，而且也与当前网络安全事件信息互联机制缺失有着密切关系。网络安全防护所倡导的“零信任”原则决定了网络安全保险在开展保险业务活动时，难以完全依循传统保险活动中所仰仗的完全相互信任之逻辑。尽管被保险人与保险人之间的网络安全风险信息互联越充分，越有

① 参见何启豪：《应对网络安全风险的保险保障机制论要》，《比较法研究》2024年第3期。

② Vgl. Tübingen 4. Zivilkammer 4 O 193/21, 1(1－17).

利于保险人评估、控制承保风险,但这与“零信任”原则下网络安全防护所追求的内部信息有条件访问与有限公开的理念相背离。从被保险人视角观之:一方面,在双方开展的网络安全风险信息互通过程中,任何人为失误或信息系统故障都有可能使其内部防护措施置于被“公之于众”的风险之中;另一方面,此种信息互联还存在商业秘密、经营数据等企业内部的核心商业数据被不当泄露之可能。因此,被保险人通常不会给予保险人访问网络安全事件相关数据的完全权限,这无疑将形成新的数据壁垒,加剧信息不对称。进而言之,网络安全事件一旦发生,所涉及的企业通常具有牵连性,但保险人对被保险人供应链上下游相关企业涉网络安全事件数据访问不存在强制性的规范基础,而仅出于企业间的自愿协助,导致保险人在网络安全风险规制过程中难以开展风险的预防、评估和定损。

当前的法律规范并未就网络运营主体的风险信息共享义务进行相应规定,仅依靠作为私主体的保险人所掌控的市场力量,难以建立起有效的网络安全事件数据库。① 虽然 2023 年 12 月国家互联网信息办公室发布的《网络安全事件报告管理办法(征求意见稿)》第 2 条明确了运营网络或者通过网络提供服务的网络运营者在发生网络安全事件时应履行风险报告义务,并对网络安全事件告知义务的履行主体、告知对象、告知内容、告知程序以及不履行该义务的处罚进行了相应规定,但是网络安全事件数据库的构建事宜并未被纳入管理事项,无法为保险人参与网络安全风险治理提供充足的数据支持。

三、我国网络安全风险保险治理困境的法治化纾解

随着国家治理任务的扩张与治理资源有限的约束之间的张力愈发显著,协同治理这种通过差异化互补提升整体治理效能的方式,逐渐成为因应新兴风险的最优选项。作为一种值得追求的目标,保险治理范式下的网络安全风险协同治理,既应是一个静态的结构,更应体现为一个动态的过程,其最终实现不仅应考虑各部分组成要素应如何构建,还关涉整体应如何具体行动与运行。②

(一)完善网络安全风险保险治理的制度框架

协同治理强调包括政府部门与非政府利益相关者在内的多元主体参与公共治理,以协调、裁定和整合多方利益相关者的目标和利益。③ 具体而言,应由法治作为形塑保险治理框架的根本遵循,并使政府与市场相结合,构建网络安全风险保险治理的二元协同治理结构。

第一,政府在宏观层面为保险治理提供制度支撑与规则指引。具体而言:(1)明确网络安全保险适用的对象包括企业、政府机构以及事业单位等公共机构。基于健全政府机关、医院以及学校等公共机构网络安全风险管理的需要,以及向未来可能遭受个人信息损害的公民提供及时补偿的目的,此类公共机构有必要使用网络安全保险,并通过政府购买服务的方式将保费纳入财政预算。④ (2)借鉴现有的强制责任保险制度的设计范式,以行政法规的形式将网络安全保险中的

① 参见王新雷、王玥:《论网络安全保险发展初级阶段的问题与对策》,《情报杂志》2017 年第 12 期。

② 参见靳文辉:《金融风险的协同治理及法治实现》,《法学家》2021 年第 4 期。

③ See David Levi Faur, The Oxford Handbook of Governance, Oxford University Press, 2012, p.498.

④ 参见赵亚宁:《数字经济时代保险参与网络安全治理的制度困境与纾解之道》,《保险研究》2023 年第 5 期。

第三方责任险确立为强制险。但需要予以明确的是，网络安全保险通常分为第一方损失险与第三方责任险，此处应规定强制保险的种类仅限于网络安全保险中保障第三方损失的责任保险，而不包括保障企业或公共机构自身损失的财产损失保险，后者因不涉及第三方利益且企业或公共机构对自身财产享有保护与否的自由，故仍应采取任意商业保险模式。此外，在网络安全保险制度构建初期，强制投保义务应被配置给《条例》所指的对关键信息基础设施承担保护义务的主体，自然包括医院、学校和政府机构。而网络安全保险强制险的保险责任范围则应以网络安全事件引起的对第三方个人或机构需要承担的赔偿责任为主，初期可以《工业和信息化部办公厅关于组织开展网络安全保险服务试点工作的通知》的规定为参照，如包括数据泄露责任、网络安全事件责任、媒体侵权责任等。

第二，明确保险人作为私人规制者的地位。明确保险人作为私人规制者的地位，应在法治化框架内从以下两个方面着力：(1)在立法层面明确保险人作为网络安全风险治理参与者的身份。在传统的分散风险功能之外，明晰保险的风险治理功能，对保险人基于关系网络、社会资本等比较优势下所享有的独立的社会权力和市场自律管理能力予以肯认。同时，提高保险人在网络安全风险保险治理领域创设规则的参与程度，或委托保险人在具有专业优势的领域探索网络安全风险保险治理的新模式。政府作为元治理者，主要发挥设置宽泛治理目标以及制定指导性规范的作用，构建创新激励机制，[①]鼓励私人规制者自行设定、解释、优化风险治理的具体标准，并依法确立私人规制的治理方案。[②] (2)在执行层面对保险人对网络安全风险的私人规制予以赋权增能。例如，可通过《保险法》《网络安全法》的修改或出台更为详细的规范性文件的方式，确认保险人在保险理赔中指引被保险人履行协助、防灾减损等义务的合理裁量权。

第三，在政府与市场相结合的二元协同治理的实现机制上，以风险规制体制的 3 个构成要素即信息获取、标准设定以及行为矫正为指引，[③]着重考虑定期汇报机制、同行评议机制、容错机制的构建。(1)政府协调保险人构建定期汇报机制。在汇报内容上，各保险公司应就各自在保险治理实践中的具体情况进行汇报，包括网络安全保险细分险种创新探索情况、网络安全保险承保典型案例展示、保费厘定精算模型探索经验分享、保险合同条款设计等。在汇报对象上，尽管保险人实质参与了网络安全风险的保险治理过程，但基于其私人主体身份并不存在强制信息公开之义务，可由其向保险监管机构汇报，再由作为行政机关的保险监管机构将保险治理的情况通过报告形式向社会主动公开。(2)政府组织保险人开展不定期的同行评议。保险监管机构应组织保险公司定期阐述为实现既定目标而采取的管理策略、实践决策及其背后的原因；针对保险公司做出的引发公众广泛关注或涉及民生的重要决定，应组织其开展公开论证。此外，还应以同一阶段的目标和评估标准为准绳，推进各保险公司之间开展交叉互查、同行评议，总结出优秀的治理经验，并要求保险公司根据反馈进行相应的调整。[④] (3)在网络安全风险保险治理的二元协同治理结构下，探索构建双重容错机制。一方面，在复杂多变的新业态新形势面前，监管部门往往被要求在短时间内尽可能在有限资源、积极行动和有效干预三者间取得平衡，并快速做出最为合理的

① 参见王兰：《论互联网金融的公私协同共治》，《厦门大学学报》(哲学社会科学版)2022 年第 4 期。

② 参见胡斌：《私人规制的行政法治逻辑：理念与路径》，《法制与社会发展》2017 年第 1 期。

③ 参见宋亚辉：《风险立法的公私法融合与体系化构造》，《法商研究》2021 年第 3 期。

④ 参见黄丽娟：《重大突发公共事件中保险治理的法治路径》，《保险研究》2023 年第 7 期。

反应,这无疑是一个巨大的挑战。若径直对监管部门的失误采取过于严厉的问责措施,可能会对其监管创新与探索积极性造成打击。[①] 因此,应构建保险治理领域针对监管部门等行政主体的容错机制,激励监管部门积极探索制度创新,以达至在不断变化的市场环境中找到最为合适的治理方案的目标。另一方面,政府作为元治理者制定保险治理规范时,同样应为保险人私人规制治理预留容错空间,从"刚性主导"转向"因势利导",配置相应的试验性与激励性的政策工具。[②]例如,可设置容错条件与"观察期",探索实施客观过失"首违不罚"制度。对保险人在网络安全风险治理过程中在法律规定的限度内为探寻创新的治理方式而不可避免造成的错误,并采取了必要措施进行防错或纠正的,可通过一定的程序认定方式对其予以减免责任处理。

(二)补足网络安全风险保险治理的规范体系

1.细化被保险人网络安全保护义务具体规定

第一,对被保险人的网络安全保护义务予以补充规定。结合网络安全风险的特殊性,对风险的如实告知、安全维护等义务进行细化补充,并为被保险人设置网络安全信息共享义务,进一步提升保险人将此类法定义务以契约的形式转化为约定义务并具体执行的能力。具言之,将《数据安全法》第 29 条规定的企业数据安全事件报告义务的设置作为起点,探索施加被保险人信息共享义务之路径,从公法层面为保险人提供广泛且真实的风险评估信息。例如,可将《网络安全法》第 21 条第 3 款作为规范依据,探索出台相应的网络安全保险条例,并在其中规定"企业作为被保险人应向保险人指定的第三方机构(通常为政府机构下属)提供网络安全风险信息数据"。此外,在网络安全风险信息告知的内容确定方面,应提倡以"关键事实"为界限的规定模式,亦即将"是否足以影响保险人一方关于承保或调整保险费用的决策"作为客观准则。其中涵盖必须强制共享的数据,既包括网络安全漏洞的数量和网络攻击的频次等事实性信息,也包括被保险人在日常运营中的网络运行状况等自愿共享的安全日志数据。

第二,明确网络安全保险义务的充分履行标准。在域外司法实践中,"汉德公式"[③]就过失法下的不合理风险给出了具有操作性的定义,或可对其进行重新阐释,作为网络安全保险中被保险人义务是否得以充分履行的判断标准。若将"汉德公式"置于被保险人是否充分履行网络安全保护义务的判断场景中,则其中预防事故发生的成本便具象为被保险人为预防网络安全风险所投入的成本,一旦发生事故所造成的实际损失体现为网络安全事故所带来的实际损失,事故发生的概率则是指网络安全事故发生概率(由权威第三方网络安全机构对被保险人进行测算),而原先"汉德公式"中事故预先可能造成的损失即表现为网络安全事故发生概率与网络安全事故所带来的实际损失的乘积。在网络安全风险的保险治理实践中,若被保险人为预防网络安全风险所投入的成本多于或持平于网络安全事故预先可能造成的损失金额时,则推定致害者已充分履行义务,保险人应依照保险合同条款开展相应的理赔;若被保险人为预防网络安全风险所投入的成本少于网络安全事故预先可能造成的损失金额时,则推定致害者未充分履行义务,存在义务履行瑕

① 参见刘权:《数字经济视域下包容审慎监管的法治逻辑》,《法学研究》2022 年第 4 期。

② 参见蒋慧:《数字经济时代平台治理的困境及其法治化出路》,《法商研究》2022 年第 6 期。

③ 在"汉德公式"中,存在 3 个要素,即 B、P、L,其中 B 指预防事故发生的成本,L 指一旦发生事故所造成的实际损失,P 指事故发生的概率,PL 指事故的预期损失。若 B<PL,即如果预防意外事故发生的成本小于意外事故所造成的预期损失,则推定致害者未充分履行义务,存在过失;若 B≥PL,则推定致害者已充分履行义务,不存在过失。参见冯珏:《汉德公式的解读与反思》,《中外法学》2008 年第 4 期。

疵，保险公司可由此主张减免赔付，由此实现对网络安全保险中网络安全保护义务履行标准认定规则的统一。

2.统一网络安全保险的标的及损害填补范围

第一，统一网络安全保险损害填补范围的前提，是明确网络安全保险的标的。2022年上海市保险同业公会发布的《网络安全保险服务规范（征求意见稿）》，为网络安全保险的承保范围提供了指导性方针。该规范为网络安全保险行业明确了“网络安全事件”的概念，将其定义为那些对信息系统构成威胁或对社会产生负面影响的事件，这包括但不限于计算机病毒的感染、特洛伊木马病毒的攻击、服务拒绝攻击以及漏洞利用等外部攻击引起的网络安全事件。然而，随着网络安全风险评估技术的不断发展，网络安全保险的覆盖范围已然显著扩张。目前，网络安全保险不仅涵盖外部攻击引起的网络安全事件，还包括由于被保险人内部人员的疏忽、技术缺陷或管理上的失误等内部原因引发的网络安全事件，该类网络安全事件由于通常会触发被保险人在个人信息和数据保护法规下的民事责任，亦有必要得到网络安全保险的保障。因此，保险标的即保险保障的损失应明确分为两类：一类是直接损失，如业务中断导致的收入损失和数据恢复费用；另一类是间接损失，如网络安全事件损害第三方权益导致的经济损失。

第二，对业务链上下游的牵连式损失是否予以赔偿进行明确规定。从损害类型来看，上游引发的连锁损失与网络安全保险的承保范围存在高度契合性。例如，若云服务平台或数据中心出现访问障碍，则被保险人将面临无法持续正常运营的风险，此种因网络安全事件而引起的营业中断及其预期利润的可能减损属于使用损失的一种，性质上应认定为财产损失，属于网络安全保险应当承担的损害赔偿情形。而且，业务链上游的“第三者”范围是能够予以确定的，这有助于保险公司在向被保险人赔付后行使代位求偿权。业务链下游的企业因被保险人业务中断而造成损失的情况不应纳入保险责任。其理由在于，在实践中业务链下游企业与被保险人之间的业务关系难以准确判定，很可能存在多层级间接损害，将因被保险人业务中断而造成的损失纳入保险责任范畴与网络安全保险的合同目的（即恢复信息系统的正常运行、数据存储状态的私密性，包括恢复被保险人的营业能力和状态）不符。①

第三，明确行政处罚的罚款排除网络安全保险的赔偿范围。保险法上的损害赔偿，是指保险人在被保险人因其他因素而招致损害时所提供的损失填补。② 虽然网络安全保险赔偿的实质是一种商业化的“补偿”，但其在顺应商业逻辑的同时亦应遵循公平正义的原则。若将行政处罚的罚款纳入网络安全保险的赔偿范围，则明显有悖于“任何人不因不法行为获利”的法理，不仅会发生保险私人规制与政府规制之间的冲突，还可能会增加道德风险，变相鼓励企业降低对网络安全规范的遵守程度，背离设立网络安全保险制度的初衷。

（三）强化网络安全风险保险治理的信息互联

网络安全风险信息的共享对应对网络安全挑战至关重要。③ 在作为私人规制者的保险人力所不逮之处，政府应介入其中，为其建立网络安全风险信息互联机制。

① 参见周瑞珏、赵精武：《网络安全保险的法理基础与实践路径》，《湖北社会科学》2023年第4期。

② 参见樊启荣：《保险损害补偿原则研究——兼论我国保险合同立法分类之重构》，《中国法学》2005年第1期。

③ 参见陈越峰：《关键信息基础设施保护的合作治理》，《法学研究》2018年第6期。

可借鉴美国国土安全部国家保护和计划署创建匿名的网络安全事故共享数据库的做法,[①]对我国当前仅限于在关键基础设施范围内开展的网络安全信息共享进行拓展,构建涵盖更大范围的网络安全信息共享机制。《网络安全法》第 29 条规定,“国家支持网络运营者之间在网络安全信息收集、分析……方面进行合作……”,第 39 条第 3 款也对国家网信部门负有促进运营者之间网络安全信息共享的义务做出了规定,这充分表明国家鼓励、支持运营者之间的网络安全信息共享合作。具言之,在信息收集类别的设定层面,我国网络安全事件数据库应当搜集的关键信息包括:网络安全事件的类别和严重性等级;遭受攻击的机构所采取的信息安全措施和程序;事件发生的时间线;事件检测技术的类别和效率;应对措施的策略和效果;人员、流程或技术问题发生的原因;事件造成的商业、声誉或财产损失;相关网络损失诉讼案件的详细数据等。在具体实施机制上,企业为遵守网络安全法律规范要求,将网络安全事故数据及时统一报送至网络安全事件数据库,网络安全保险人则可通过有偿获取的方式从该数据库获取数据,丰富自身网络安全风险池的基础数据,并通过这些数据对风险评估模型进行优化训练,以提升保险人的信用风险精准定价能力。进一步而言,通过政府设置的数据共享平台,保险人在匿名共享历史损失数据、索赔记录和合规审计等信息的基础上,根据被保险人可能面临的网络安全风险等级以及其对网络安全保护的投入等多种因素综合分析后,进行差异化定价。与火灾保险和其他财产与意外伤害保险类似,保险人可以企业对自身信息安全基础设施的投入为参照,进行折扣调整以降低保费。[②] 而且,这种信息共享还可以降低进入网络安全保险市场的成本,吸引更多的保险公司与现有的网络安全保险公司竞争,在市场的作用下使网络安全保险的价格越来越低廉,直至维持在合理水平。

若规则的制定可与被管理者实现激励相容,将能极大地降低规制成本并激发被规制者的自我执行动力。因为激励型制度规制通常采用的是利益诱导的方式,并注重制度的复合利益设置,[③]也就能够更好地实现规则制定者与被管理者共同合作的目标。所以在网络安全事件数据库构建前期,或可采取激励相容的机制设计:网络安全保险人每月可享有一定量的免费数据获取额度,当网络安全保险人获取数据超出免费额度时,可参照当地的公共数据产品价格进行付费获取;此外,还可采取赔付款抵充数据获取额的设计,即网络安全保险人可将自身向被保险人赔付的网络安全保险赔付额作为依凭,按一定比例换算向数据库方申请数据获取费用减免,以构成“数据获取—合理定损—有序赔付—激励补偿—数据获取”的闭环,通过经济补偿引导网络安全保险人的合理赔付,激励保险人积极利用数据促进网络安全风险评估模型优化,强化其对网络安全风险的规制能力。

四、结 语

目前网络安全保险在我国仍处于初步发展阶段,《意见》的出台昭示着国家对网络安全风险保险治理的重视。法治是国家治理的基本形式,网络安全风险治理法治化寓于国家治理现代化

① 参见王新雷、王玥:《论网络安全保险发展初级阶段的问题与对策》,《情报杂志》2017 年第 12 期。

② See Liam M. D. Bailey, Mitigating Moral Hazard in Cyber—risk Insurance, 3 Journal of Law & Cyber Warfare, 7—8(2014).

③ 参见靳文辉:《公共规制:话语、理论与实践》,中国社会科学出版社 2022 年版,第 90 页。

之中，同时也是中国式现代化的必然要求。本文旨在对网络安全保险参与风险治理的理论逻辑与现实基础进行阐明，为网络安全风险保险治理的正当性提供充足理据，并力图在梳理当前我国网络安全风险保险治理困境的基础上，探索网络安全风险保险治理法治化之路径。立足于新的时空境遇，数字经济已然成为驱动全球经济发展的新引擎，而网络安全则是护航数字经济高质量发展的重要保障，在维护网络安全方面，没有任何一个国家能独善其身。作为具有数字经济先发优势的中国应发挥制度优势，积极探索网络安全风险综合治理体系构建方案，为全球网络安全治理贡献中国智慧。

Abstract: In the era of the digital economy, the legalization of cybersecurity risk governance is an inevitable requirement for advancing the modernisation of the national governance system and governance capabilities. Insurance is becoming an increasingly important tool for cybersecurity risk governance while also achieving the dispersion of cybersecurity risks. The theoretical logic of cybersecurity risk insurance governance is based on the transformation of the traditional governmental regulation model to the social self－regulation model and the expansion of the social governance functions of insurance. The organic connection between the contractualisation of legal obligations, the privatization of rule－making, and the marketization of risk control together outline the practical logic of cybersecurity risk insurance governance. The difficulties faced by cybersecurity risk insurance governance are mainly due to the lack of an insurance governance system framework, insufficient supply of norms, and a lack of interconnection of risk information. A dual collaborative governance structure combining government and market has become the preferred paradigm for cybersecurity risk insurance governance. In the future, in addition to improving the institutional framework for cybersecurity risk insurance governance, supplementing the normative system for cybersecurity risk insurance governance, and strengthening the information interconnection for cybersecurity risk insurance governance, it is also necessary to establish and improve regular reporting, peer review, and a fault tolerance mechanism for cybersecurity risk insurance governance, with a view to promoting the rule of law in cybersecurity risk insurance governance.

Key Words: cybersecurity risk, insurance governance, cybersecurity insurance, cybersecurity protection obligations

责任编辑　　翟中鞠