

文章编号:1003-2053(2026)03-0644-08

量子计算的技术风险及其治理

杜娟

(吉林大学马克思主义学院,吉林长春 130015)

摘要:量子计算以量子叠加、纠缠与干涉、量子优越性为基本原理,兼具计算能力跃迁、不确定性和概率性、可逆计算等特征。其在密码破译、大规模数据分析、军事模拟与关键基础设施防护等领域展现出巨大潜能。从量子计算的基本原理与技术特质出发,有必要系统剖析其对信息安全、国家安全与市场秩序的多维影响:一方面,大数分解能力与量子搜索算法威胁既有加密体系与数据隐私,可能引发追溯性隐私泄露与关键设施瘫痪;另一方面,量子算力竞赛与军民两用属性掀起国际竞争与军控失范的双重风险,也催生市场垄断与公平竞争失衡的潜在危机。对此,可从立法规制、监管创新与国际协同三个层面构建综合治理框架:通过修订现有安全立法与制定量子技术专门法,形成分级分类的安全管控基准;结合风险评估、量子技术审查与多层次协同监管机制,细化准入、事中监管与应急处置环节;并在国际层面倡导统一标准与多边合作,防范量子霸权和算力垄断。与此同时,应推进量子伦理规范与人才培养制度建设,兼顾技术创新与社会责任,以期在保障国家安全与公共利益的同时,为量子计算的健康可持续发展奠定坚实的法治根基。

关键词:量子计算;信息安全;风险治理;国际协同

中图分类号:F920.0

文献标识码:A

习近平总书记指出,支持量子计算等新技术应用^[1]。量子计算作为21世纪最具革命性的前沿科技之一,正在深刻改变人类社会的发展进程^[2]。量子计算凭借其强大的并行计算能力,在密码破译、药物研发、气候模拟等领域展现出巨大潜力,同时也要求变革现有法治体系。

域外对量子计算及其风险治理研究走在前列。量子计算机的前景启发了对量子计算霸权(quantum computational supremacy)的追求,即利用量子计算机解决对传统计算机而言极其困难的任务^[3]。从量子计算霸权引申出社会科学意义上的量子霸权(Quantum Supremacy)概念,用以描述量子技术凭借对社会生活的颠覆性影响而产生的强制性权力的影响。从而使对量子计算的监管逐渐提上日程,有学者以“量子法律”(quantum law)来统摄在量子技术时代的法律挑战与机遇^[4]。

我国学者对量子技术的风险及其治理研究逐步走向深入。一是量子技术的基本特征。陈俊波等学者指出,量子技术正从实验室研究阶段转向商业化应用,具有新颖性、使能性、系统性和不确定性等特征^[5]。二是量子技术的多维度影响。首先是国家

安全维度,黄钊龙等学者的研究从“量子化国际关系”视角,系统分析了量子信息技术对国家安全的影响。特别是在量子计算、量子通信和量子精密测量三个方向,量子技术正深刻改变着国际安全格局^[6]。其次是法律保护维度。黄炜杰的研究聚焦量子信息技术的专利权保护问题^[7]。最后是产业发展维度。郭国平的研究对量子计算政策发展进行了系统梳理。研究显示,中国、美国、德国、英国、日本、澳大利亚等国都已将量子计算纳入国家战略,通过政策支持和资金投入推动产业发展^[8]。三是量子技术发展面临的挑战。陈俊波等学者提出,量子技术发展面临量子霸权威胁、量子竞赛隐忧、量子鸿沟差距、量子炒作困境等伦理风险,呼吁实现负责任的量子技术创新^[4]。

基于已有研究成果,本文试图构建系统化的量子计算的治理框架。首先,分析量子计算技术发展现状,厘清其对法律体系的影响;其次,探讨量子计算法律治理路径,从立法规制、监管创新和国际协同三个维度提出具体建议;最后,立足中国实践,提出量子计算法律治理的中国方案,为完善相关制度提供理论支撑。

1 量子计算的技术特征与法律属性

量子计算引发了数理逻辑和人文逻辑的双重变化,应在对量子技术基本原理的解析基础上,进一步探求量子技术的技术特性,从而为量子技术的法律属性分析打好基础。

1.1 量子计算的基本原理

(1) 量子比特与量子叠加

量子计算以量子比特(qubit)为基本信息单位,突破了经典计算的二进制限制。量子比特可以同时处于多个状态的叠加态,从而极大地扩展了信息的表示空间^[9]。传统计算机使用二进制,就像一个开关只能处于“开”或“关”两种状态。而量子比特则像一个特殊的开关,可以同时处于“开”和“关”的状态,就像硬币可以既是正面又是反面,直到我们观察它时才确定下来。因此,某些在传统计算机上需要运行数百年的复杂计算,可能在量子计算机上只需要几分钟就能完成,计算能力呈指数级增长。

(2) 量子纠缠与量子干涉

量子纠缠是指,当多个量子比特处于纠缠态时,它们的量子态无法被分解为独立的单粒子态的乘积,表现出强相关性^[10]。像双胞胎之间的心灵感应,一个人的情绪会立即影响另一个,但其比心灵感应更加精确和可靠。量子计算机可以同时处理大量数据,类似于有成千上万个处理器在并行工作。量子干涉则是通过相位差的叠加与抵消来实现计算,使得某些问题的求解复杂度可以从指数级降至多项式级^[11]。就像往平静的水面扔两颗石子,两组水波相遇时会产生干涉现象。通过精确控制这种“波”的相位,可以让有用的信息相互增强,无用的信息相互抵消。

(3) 量子优越性的实现机制

量子优越性是指量子计算机能够解决经典计算机在实际可行时间内无法完成的计算任务^[12]。假设有一个巨大的迷宫,传统计算机就像一个人,必须一条路一条路地尝试,可能需要几年才能找到出口;量子计算机则像是可以同时出现在迷宫所有位置的超能者,可能几分钟就能找到答案。量子优越性的实现依赖于量子态的制备与操控、量子门操作的精确控制、以及退相干效应的抑制等关键技术的突破。

1.2 量子计算的技术特性

(1) 计算能力的爆炸性增长

量子计算能力的爆炸性增长主要体现在两个维度。一是与传统计算相比,量子计算突破了形式计算系统的局限性,超越了不可计算性和计算复杂性上的诸多限制。对 n 个量子比特的计算机而言,其处理数据的能力是经典计算机的 2^n 倍^[13]。二是与其他计算范例相比,量子计算的优越性也首屈一指。符号逻辑、神经网络、遗传演化和基因计算等都难以与量子计算匹敌^[14]。

(2) 不确定性与概率性

首先,量子所具有的不确定性、不可克隆等特征^[15],一方面可以用作量子通信的安全保障,另一方面也产生了会降低量子计算的速度^[16]。它需要使用称为“门”(gates)的噪声敏感设备来运行,而这会导致量子计算机运行核心的脆弱量子态发生退相干。其次,量子计算结果具有概率性,以致依赖于精确计算测量概率的标准技术无法提供高效模拟的量子计算。

(3) 可逆计算特征

量子计算的可逆性代表了规律性,从而保证了信息传递的可塑性以维护信息的完整,规避了信息丢失的可能^[17]。该特性为数据安全加密、电子取证和防证据篡改、使用轨迹追踪和识别等用途提供了技术基础。

1.3 量子计算的法律属性界定

(1) 价值维度:技术中立性原则的适用

量子计算在本质上具有双重属性:一方面,作为信息处理技术,其发展应当遵循技术中立原则,保障创新自由;另一方面,其颠覆性计算能力可能威胁现有安全体系,需要审慎监管。因此,技术中立性原则在量子计算领域需要重新定位。从法理基础看,技术中立性原则强调法律规制应当关注行为结果而非技术本身^[18]。但量子计算的特殊性在于,其技术特征本身就蕴含重大风险。例如,量子计算对现有密码体系的潜在威胁,决定了不能采取完全中立的监管立场。立法实践中应当采取“有限中立”原则。对基础研究和低风险应用维持中立立场,对高风险应用如密码破解、军事模拟等领域进行针对性规制。差异化监管能既尊重技术发展规律,又能有效防范系统性风险。

(2) 功能视角:军民两用属性的认定

从功能视角上审视,量子技术是军民两用的。军事用途着重于维护国家安全。用于军事应用的量子技术引入了新的能力,提高了有效性并增加了精

确度,从而导致“量子战争”。量子技术在各种战争领域(如陆地、空中、太空、电子、网络和水下战争以及 ISTAR—情报、监视、目标获取和侦察)中有特定军事应用^[19]。民事用途着重于大规模的商业应用,可用于市场分析、风险研判、信息加密、医学成像等领域。由于民事用途更新迭代速度更快,也可以被改造来服务于军事。

2 量子计算风险剖析

从“个人—国家—市场”的角度,量子计算风险可分为信息安全风险、国家安全风险和市场风险。

2.1 信息安全风险

(1) 现有密码体系可能失灵

现有密码体系建立在特定数学难题的基础上,而量子计算的出现从根本上动摇了这一安全基础。具言之,其一,公钥密码体系面临崩塌风险^[20]。基于大数分解和离散对数的 RSA、ECC 等加密算法,在量子计算面前将失去安全性。现有数字签名的有效性受到威胁,还可能导致历史加密数据被破解。其二,密码基础设施体系需要重构。量子计算对 PKI(公钥基础设施)体系构成系统性冲击,证书认证、身份验证等核心机制需要升级改造。其三,密码应用场景遭遇挑战。从电子合同到数字货币,从身份认证到通信加密,大量依赖现有密码技术的应用场景都将面临安全威胁,而技术维护的步伐慢于技术换代的速度。

(2) 数据隐私保护机制失效

首先是存量数据的隐私风险。大量历史数据基于传统加密方式存储,一旦量子计算实现破解,将导致隐私数据大规模泄露^[21]。其次是增量数据的保护困境。现有数据脱敏、匿名化等技术手段可能被量子计算突破,个人隐私边界面临重新界定。在大数据分析领域,量子计算的强大算力可能实现个体数据的精确还原。最后是跨境数据流动的安全隐患。国际数据传输的保护机制需要重新设计,否则可能出现数据主权受损、个人隐私遭受跨国侵害等问题。

(3) 关键基础设施安全威胁

量子计算可能突破工业控制系统的安全防护,影响能源、交通等核心设施的稳定运行。现有的纵深防御体系可能被量子计算一举突破。特别是在智能电网、核电站等领域。架构层面,关键信息基础设

施的整体安全架构需要重新设计^[22]。

2.2 国家安全风险

(1) 量子军事应用的管控困境

量子军事应用的管控面临以下困境:一是技术识别难度高。量子计算军事应用与民用技术高度重合,难以建立有效的识别标准。例如,量子优化算法既可用于民用物流规划,也可用于军事部署优化,双重属性使得管控基准难以确立。二是管控措施实施难。由于量子计算具有分布式特征,传统的物理隔离和准入管控方式难以奏效。即使对核心设施实施严格管控,分散的量子节点仍可能被用于军事目的。三是国际协调机制缺失。各国在量子军事应用领域的竞争加剧,而缺乏有效的国际管控框架。现有的军控机制未能覆盖量子军事应用,造成监管真空。

(2) 量子算力竞争的规制难点

在国际竞争领域,由于量子算力的军民两用价值日益凸显,量子算力竞争用以描述各个国家为了获取、开发和升级自身的量子计算能力而展开的竞争。然而,现如今量子算力竞争呈现恶性竞争的局面,西方国家对关键量子技术对我国实行“卡脖子”,违背技术造福于整个全人类的宗旨。与此同时,量子技术算力的监管需要特殊监管形式,以确保算力资源的合理利用,对治理方式和能力提出了更高的要求。

2.3 市场风险

(1) 量子计算垄断风险

量子计算领域的垄断风险主要体现在三个层面:一是研发垄断。量子计算研发具有高投入、长周期特征,形成了以少数科技巨头为主导的市场格局^[23]。研发垄断影响技术创新路径,还可能导致标准制定被操控,阻碍行业良性发展。二是应用垄断。在商业应用层面,量子计算的高门槛特性可能强化现有市场优势,使头部企业通过控制量子计算资源来巩固市场地位。应用层面的垄断会加剧数字鸿沟,影响市场公平。三是生态垄断。量子计算生态系统涉及硬件、软件、算法等多个环节,垂直整合趋势明显。完整生态链的垄断将形成极高的市场准入壁垒,损害创新创业空间。

(2) 金融市场稳定威胁

量子计算对金融市场稳定的威胁表现为:一是交易系统脆弱性。量子计算可能突破现有金融交易系统的安全防护,影响交易数据的完整性和可信度。特别是在高频交易领域,量子优势可能导致市场操纵行为激增。二是定价机制失衡。量子计算在金融

衍生品定价、风险评估等领域的应用,可能打破现有定价模型的有效性。算力优势持有者可能获得超额定价能力,扰乱市场价格机制。

3 量子计算的治理路径分析

量子技术的治理路径可从国内维度的立法和监管创新出发,同时从国际治理层面加以探索。

3.1 立法规制体系的完善

(1) 量子计算安全立法框架拟定

量子计算安全立法框架应从抽象维度的立法理念、目标、基本原则和具体维度的法律规则组成。在立法理念上,量子计算的安全立法应平衡发展与安全,采用包容性治理、适应性治理和预防型治理的理念。包容性治理是指在容纳量子技术进步空间的前提下,审慎监管其带来的风险,防止因噎废食阻碍量子技术带来的创新效应。适应性治理是指要符合自身国情特色,顺从本国量子技术发展实际进行治理。预防型治理是指将量子技术风险“治于未病”,防止风险或后果到难以挽回的地方再进行补救式治理。因此,量子技术安全立法的目标应是促进量子技术创新,保障国家安全、公共利益和私人利益。在基本原则方面,应坚持安全优先、创新引领、协同治理、绿色发展四项原则。

深入到具体维度的法律规则,应首先衔接已有的法律体系中有关量子技术的规定。从“算法—算力—数据”的角度,可以适用《个人信息保护法》《数据安全法》《网络安全法》中的已有规定。同时,从已有的立法例中可以类推进行立法,2023年8月我国出台了世界上第一部有关生成式人工智能的成文行政法规《生成式人工智能服务管理暂行办法》。对典型的新兴技术通过行政法规来加以规制,能够弥补法律的滞后性和修改的繁复性。以此类推,可以制定《量子技术管理暂行办法》,以对量子计算技术研发、应用、安全保护等作出系统规定。

(2) 量子技术标准体系确立

如果说前述量子计算安全立法框架拟定属于硬法规制的角度,那么建立量子技术标准体系则属于软法治理的范畴,软硬结合能够形成治理的最大合力。从行业法治的角度,应形成国家标准引领、行业标准铸基和企业标准自律的技术标准体系。

首先,国家标准引领是指国家标准应致力于实现节约技术协调成本,促进量子技术市场一体化的

发展,避免标准的碎片化。国家标准应该廓清基础通用标准,包括概念定义、符号标志等。此外,技术标准应规范量子技术硬软件产品的技术要求。其次,行业标准铸基是指量子技术行业应以服务应用为标准,明确量子计算服务、量子算法应用的服务标准或规范。同时需要注意的是行业标准应制定清晰完备的安全保障标准,对量子通信等技术的安全标准加以明晰。再次,企业标准自律是指应鼓励企业制定高于国家标准和行业标准的企标,以自律突围商业竞争,在良性竞争中促进量子技术的安全和稳定。

3.2 监管机制的创新

(1) 量子计算风险评估机制

借鉴欧盟《人工智能法案》,建立量子计算风险评估机制能够有效应对量子技术风险。量子技术风险合规性评估可在监管沙盒中进行,以给予量子技术研发企业以容错和试错空间。在评估主体方面,应区分量子技术的不同应用场景,进行不同主体的评估。如果量子技术用作基础研发类,则应由数据主管部门用作监管沙盒的监督主体;如果量子技术用作应用技术类,则应由行业主管部门负责监管沙盒的实施。关于评估对象,应根据前述划分的信息安全风险、国家安全风险、市场风险进行综合评估。在评估方法上,应采用定性分析与定量测算相结合的方法。定性分析主要从技术特征、应用影响、安全隐患等角度进行研判;定量测算则通过设置风险系数、建立数学模型等方式,对风险程度进行量化评估。在评估程序方面,应分为主动评估和被动评估两种方式。现阶段量子技术风险不明的情况下,应以“主动评估为原则,被动评估为例外”的方式进行。在评估结果方面,应实行评估结果分级,等级分为风险等级“高、中、低”三个粗略层次,并辅助以详细的文字描述。

(2) 量子技术审查制度设计

为了防止审查形式化、虚置化,对量子技术审查制度的设计应采用“形式审查+实质审查”的双重审查机制。形式审查侧重于伦理审查,实质审查侧重于责任审查。前者的审查主体一般为技术应用或研发的伦理委员会,主要核查项目研发或技术应用材料的形式完整性和合规性。后者的审查主体一般为技术应用或研发的审查委员会,其在形式审查的基础上,深入评估技术方案的成熟度、必要性、可能性、可行性和风险性。有必要的情况下还应建立量

子技术应用或研发的审查矩阵,以综合研判量子技术应用风险。此外,为了提高审查效率和针对性,应结合量子计算风险评估机制加以展开,对量子计算核心技术、关键设备和重要应用实行重点审查。

3.3 国际治理的协同

(1) 量子技术国际标准制定

国际技术标准是一种战略性商业工具,涉及到技术、市场和政府三方^[24]。争夺量子技术国际标准的制定权是我国实现技术引领的核心。首先,应推动量子技术基础研究的国际合作,批判西方发达国家对发展中国家设置的技术标准壁垒,逐渐瓦解西方国家建立起来的技术壁垒和屏障。以促进量子技术科研资源共享和技术交流互惠为宗旨,明确量子技术转让向发展中国家倾斜的原则。其次,制定统一的产业发展规则,构建量子计算产业国际标准,以建立公平竞争机制。最后,为规范量子技术的跨境技术转移,防止量子国际霸权显现和量子国际帝国主义出现,应建立国际间互认的量子计算安全评估机制和审查机制。

(2) 量子安全国际合作机制

在量子技术国际标准制定基础上,夯实量子安全国际合作机制是“量子化国际关系”走向稳定的基石,以合作超越隔阂和矛盾。为了最大程序地消减国家之间的信息差,可建立起量子安全威胁情报共享机制,以有效获取量子风险评估和预警信息。同时,可构筑统一的防护系统,建立跨境量子安全事件的响应机制。定期召开技术安全会晤机制,形成国家间的联合审查组、工作组或调查组。

(3) 量子计算全球治理框架

建立量子计算全球治理框架是实现可持续发展的必然要求。治理结构设计可采用“多中心”模式。设立全球量子计算治理委员会,统筹协调重大事项;成立专业委员会,负责技术标准、安全规范等具体工作;建立区域协调机制,推动区域合作。同时,建立利益相关方参与机制,确保各方诉求得到充分表达。在治理机制方面,构建复合治理模式。规则层面制定具有约束力的国际公约,明确各方权责;标准层面建立统一的技术标准体系,促进互联互通;合作层面搭建多样化的合作平台,推动资源共享。治理工具创新是框架有效运行的关键。发展数字化治理工具,建立量子计算全球监测系统;运用智能化治理手段,提升治理效率;创新金融支持工具,建立量子计算发展基金。

4 量子计算法律治理的中国方案

因地制宜治理量子技术,彰显中国的地域特色和大国担当可引领量子技术的中国之治走向深处。

4.1 基础制度设计

(1) 量子计算产业促进与安全管理并重

量子计算技术的发展既需要政策激励,又需要有效管理。构建促进与管理并重的制度体系,应立足中国国情,充分发挥举国体制下有组织科研的制度优势。

从促进维度看,我国已在建立量子计算重大科技专项支持机制积累了一定经验。2018年教育部建立了量子信息前沿科学中心。国家自然科学基金委员会在近几年也相继发布了与量子计算有关的重大研发计划,设立了专门的研发资金,对量子芯片、量子算法等关键技术攻关给予持续支持。在此基础上,应构建产学研协同创新体系。支持建设量子计算创新平台,推动高校、科研院所、企业深度合作。建立成果转化激励机制,加快科技成果产业化。此外,应设立量子计算特殊人才支持计划,加大对领军人才和青年人才的培养力度。完善人才评价机制,建立以创新能力和实际贡献为导向的评价体系。

从管理维度看,需要构建以下制度:首先,建立量子计算技术目录管理制度。对量子计算技术进行分类管理,明确不同类别技术的管理要求。其次,实施量子计算项目审批制度。对重要研发项目、产业化项目实行审批管理,确保项目合规性。再次,建立量子计算知识产权保护机制。完善专利申请和保护制度,加强商业秘密保护,防范核心技术流失。对敌对势力窃取或挪用我国量子技术的潜在可能性切实评估,对其出口实施应更严格控制。

(2) 量子安全分级分类规制

量子安全分级分类规制是实现精准监管的重要手段,能够根据量子技术的特性进行分类管理,防止“一刀切”,从而实现良好的军民两用分流的局面。建立科学合理的分级分类体系,需要从规制对象、规制标准和规制措施等方面进行设计。

在规制对象方面,按照风险程度和重要性,将量子计算系统分为核心级、重要级和一般级。核心级主要包括涉及国家安全的量子计算系统;重要级包括关系国民经济运行的重要系统;一般级包括其他民用商用系统。同时,根据技术特征,将量子计算技

术分为基础技术、关键技术和应用技术三类,实施差异化管理。

4.2 配套机制构建

(1) 量子技术知识产权保护

量子技术知识产权保护需要创新性制度设计。从保护客体、保护方式和保护措施等维度构建全方位保护体系。

保护客体范围应与技术特征相适应。将量子算法、量子芯片设计、量子软件等纳入专利保护范围;对量子计算源代码、技术文档等实施著作权保护;针对工艺流程、商业模式等建立商业秘密保护制度。建立量子技术专利分类体系,提高审查效率。

在保护方式上采取整体性保护策略。完善专利保护制度,延长特定领域专利保护期限;加强商业秘密保护,提高侵权赔偿标准;建立技术许可制度,规范技术转让行为。同时,建立知识产权预警机制,防范侵权风险。

在保护措施方面,构建多层次保护体系。行政保护方面,加强知识产权行政执法;司法保护方面,完善证据规则,建立技术事实查明机制;行业保护方面,发挥行业组织自律作用。建立知识产权评估机制,合理确定技术价值。

(2) 量子计算人才培养机制

构建系统化的量子计算人才培养机制,需要从培养模式、支持政策和评价体系等方面进行整体设计。培养模式应体现前瞻性和针对性。构建学科交叉培养体系,强化物理学、计算机科学等学科融合;建立产教融合培养平台,推动校企协同育人;完善国际合作培养机制,拓展人才培养渠道。设立量子计算专业,开发课程体系。

4.3 治理能力提升

(1) 量子安全应急处置机制

构建快速高效的应急处置机制可提升量子安全治理能力。从系统论的角度审视,应急处置机制应包含预警、响应和恢复三个环节。

首先,在预警环节,预警系统应整合多源信息,形成立体化感知能力。量子安全威胁往往具有高技术性与隐蔽性,从而要求预警系统必须具备高敏感度的异常行为检测能力。其次,在应急响应环节,应建立基于网络化指挥的扁平化响应结构,缩短决策链,提高响应速度。同时,技术处置与战略决策应相对分离。前者需要专业团队的技术支持,后者则需要高层决策者的战略判断。二者分而治之,方能应

对复杂的量子安全危机。再次,在恢复环节,则需关注系统韧性的重建。韧性超越了传统的恢复概念,强调系统在受到冲击后不仅能恢复原状,更能适应新环境并持续发展。同时应重视风险沟通机制的构建,防止信任危机扩散。

(2) 量子治理技术支撑体系

量子技术风险治理的技术支撑是实现技术内循环的必要基础。构建系统化的技术支撑体系,需要从基础设施、技术工具和运行机制等方面进行设计。基础设施建设应注重先进性。建设量子安全监测网络,实现全域覆盖;部署量子加密系统,保障通信安全;构建量子计算云平台,提供计算支持。完善基础设施维护机制,确保稳定运行。技术工具研发应强调实用性。开发量子安全评估工具,提升风险识别能力;研制量子态势分析系统,增强形势研判能力;建设量子安全防护平台,提高防护水平。建立技术工具评估机制,保证工具实效性。运行机制设计应突出协同性。建立技术资源共享机制,提高资源利用效率;完善技术标准体系,促进系统互联互通;构建技术创新平台,推动关键技术突破。建立运行监督机制,确保系统安全稳定。

5 结语

量子技术的出现是人类计算能力的又一次极限拓展,在底层计算逻辑发生转变的情况下,社会生活现实的变化也对法治体系的动态运转提出了新需求。伴随着国际量子技术竞争的是国际监管规则的博弈,其治理复杂性远胜从前,考验治理新兴技术风险的能力。唯有兼顾多种价值的情况下,进行通盘和全景的审视,治理量子技术才不会变成一把利刃,既消除了风险,又阻碍了量子技术发展本身。

参考文献:

- [1] 陈一鸣,宋静思.习近平出席亚太经合组织第三十次领导人非正式会议并发表重要讲话[N].人民日报,2023-11-19. Chen Y M, Song J S. Xi Jinping Attends the 30th APEC Economic Leaders' Informal Meeting and Delivers an Important Speech [N]. People's Daily, 2023-11-19.
- [2] Hossain K A. The potential and challenges of quantum technology in modern era[J]. Scientific Research Journal, 2023, 11(6): 41-49.
- [3] Harrow A W, Montanaro A. Quantum computational su-

- premacv[J]. *Nature*, 2017, 549(7671): 203 – 209.
- [4] Gromova E A, Petrenko S A. Quantum law: The beginning[J]. *Journal of Digital Technologies and Law*, 2023, 1(1): 62 – 88.
- [5] 陈俊波,夏保华. 试论量子技术创新的伦理治理[J/OL]. 科技进步与对策. <http://kns.cnki.net/kcms/detail/42.1224.G3.20241217.1016.012.html>. Chen J B, Xia B H. On ethical governance of quantum technology innovation[J/OL]. *Science & Technology Progress and Policy*. <http://kns.cnki.net/kcms/detail/42.1224.G3.20241217.1016.012.html>.
- [6] 黄钊龙,韩召颖. 量子信息技术发展与国家安全[J]. 武汉大学学报(哲学社会科学版), 2024, 77(2): 51 – 60. Huang Z L, Han Z Y. Quantum information technology development and national security[J]. *Wuhan University Journal (Philosophy & Social Sciences)*, 2024, 77(2): 51 – 60.
- [7] 黄炜杰. 量子信息技术专利权保护的困境与出路[J]. 科技与法律(中英文), 2022(6): 64 – 72. Huang W J. Dilemma and solution of patent protection for quantum information technology[J]. *Science Technology and Law*, 2022(6): 64 – 72.
- [8] 郭国平. 量子计算政策发展与应用研究综述[J]. 人民论坛·学术前沿, 2021(7): 57 – 63. Guo G P. A review of quantum computing policy development and application research[J]. *Frontiers*, 2021(7): 57 – 63.
- [9] 施郁. 揭开“量子”的神秘面纱[J]. 人民论坛·学术前沿, 2021(7): 14 – 20. Shi Y. Unveiling the mystery of "quantum"[J]. *Frontiers*, 2021(7): 14 – 20.
- [10] 刘燊,汪澜,韩逸雪,等. 国际量子认知的研究回溯、热点发掘与整合展望[J]. 自然辩证法通讯, 2025, 47(1): 105 – 116. Liu S, Wang L, Han Y X, et al. Research retrospect, hot spots exploration and integrated prospect of international quantum cognition[J]. *Journal of Dialectics of Nature*, 2025, 47(1): 105 – 116.
- [11] 刘燊. 量子认知的研究回溯、核心应用领域与未来展望[J]. 自然辩证法通讯, 2024, 46(4): 41 – 48. Liu S. Research retrospect, core application areas and future prospects of quantum cognition[J]. *Journal of Dialectics of Nature*, 2024, 46(4): 41 – 48.
- [12] 张薇薇. 中美构建科技竞合关系的必要与可能[J]. 和平与发展, 2023(3): 1 – 26. Zhang W W. The necessity and possibility of China – US constructing a competitive – cooperative relationship in science and technology[J]. *Peace and Development*, 2023(3): 1 – 26.
- [13] 汪勇,孟香君,沈维萍. 量子计算在经济与金融领域中的应用[J]. 经济学动态, 2023(1): 126 – 143. Wang Y, Meng X J, Shen W P. Applications of quantum computing in economics and finance[J]. *Economic Perspectives*, 2023(1): 126 – 143.
- [14] 周昌乐. 对新型量子计算范例的哲学透视[J]. 自然辩证法通讯, 2003(1): 94 – 99. Zhou C L. Philosophical perspective on new quantum computing paradigms[J]. *Journal of Dialectics of Nature*, 2003(1): 94 – 99.
- [15] 杨东. 量子技术是金融科技的终极形态吗? [J]. 人民论坛·学术前沿, 2021(7): 84 – 97. Yang D. Is quantum technology the ultimate form of fintech? [J]. *Frontiers*, 2021(7): 84 – 97.
- [16] Wong R. 量子计算与不确定性原理[J]. 计算机科学, 2020, 47(1): 40 – 50. Wong R. Quantum computing and the uncertainty principle[J]. *Computer Science*, 2020, 47(1): 40 – 50.
- [17] 王凯宁. 从粒子到信息: 统计物理与量子信息基础研究的关联与进展[J]. 科学技术哲学研究, 2017, 34(1): 31 – 35. Wang K N. From particles to information: Correlation and progress of statistical physics and quantum information basic research[J]. *Studies in Philosophy of Science and Technology*, 2017, 34(1): 31 – 35.
- [18] 张新平. 算法与法律的冲突及其化解[J]. 法律科学(西北政法大学学报), 2024, 42(2): 135 – 146. Zhang X P. Conflicts between algorithms and law and their resolution[J]. *Science of Law (Journal of Northwest University of Political Science and Law)*, 2024, 42(2): 135 – 146.
- [19] Krelina M. Quantum technology for military applications[J]. *EPJ Quantum Technology*, 2021, 8(1): 24.
- [20] 祁笑稚,孙光明. 基于密码技术的互联网安全性分析[J]. 情报科学, 2006(9): 1391 – 1394. Qi X Z, Sun G M. Analysis of internet security based on cryptography technology[J]. *Information Science*, 2006(9): 1391 – 1394.
- [21] 郭全中. 互联网平台: 迈向空间计算新形态[J]. 社会科学辑刊, 2024(6): 216 – 224. Guo Q Z. Internet platforms: Towards a new form of spatial computing[J]. *Social Science Journal*, 2024(6): 216 – 224.
- [22] 边赛,李家胜. 美印网络空间合作新态势评析[J]. 印度洋经济体研究, 2024(6): 133 – 153. Bian S, Li J S. Analysis of new trends in US – India cyberspace cooperation[J]. *Indian Ocean Economic and Political Review*, 2024(6): 133 – 153.
- [23] 杨玉华. 中美经贸摩擦及其战略思考——基于生产率优势演进视角[J]. 当代经济研究, 2024(12): 59 – 75. Yang Y H. China – US trade friction and strategic

thinking: Based on the perspective of productivity advantage evolution [J]. Contemporary Economic Research, 2024(12): 59 – 75.

[24] 张利飞,唐鸿娟,于长永.技术标准国际化竞争的大国效应研究[J/OL]. 科研管理. <http://kns.cnki.net/kcms/detail/11.1567.G3.20241216.0910.002.html>.

Zhang L F, Tang H J, Yu C Y. Research on great power effect in international competition of technical standards [J/OL]. Science Research Management. <http://kns.cnki.net/kcms/detail/11.1567.G3.20241216.0910.002.html>.

Legal risks and governance of quantum computing

DU Juan

(School of Marxism, Jilin University, Changchun 130015, China)

Abstract: Quantum computing, based on the fundamental principles of quantum superposition, entanglement, interference, and quantum supremacy, features characteristics such as computational power leaps, uncertainty and probabilistic nature, and reversible computation. It demonstrates enormous potential in fields like cryptography breaking, large – scale data analysis, military simulation, and critical infrastructure protection. Starting from the basic principles and technical attributes of quantum computing, this paper systematically analyzes its multidimensional impacts on information security, national security, and market order: on one hand, the capability of large number factorization and quantum search algorithms threatens existing encryption systems and data privacy, potentially leading to retrospective privacy breaches and critical facility paralysis; on the other hand, the quantum computing power race and its dual – use nature trigger dual risks of international competition and arms control dysfunction, while also creating potential crises of market monopoly and unbalanced fair competition. In response, a comprehensive governance framework can be constructed from three levels: legislative regulation, regulatory innovation, and international coordination. This includes revising existing security legislation and establishing specialized quantum technology laws to form hierarchical security control benchmarks; combining risk assessment, quantum technology review, and multi – level collaborative regulatory mechanisms to refine market entry, in – process supervision, and emergency response procedures; and advocating unified standards and multilateral cooperation at the international level to prevent quantum hegemony and computing power monopoly. Meanwhile, the development of quantum ethics norms and talent cultivation systems should be promoted to balance technological innovation with social responsibility, thereby laying a solid legal foundation for the healthy and sustainable development of quantum computing while safeguarding national security and public interests.

Key words: quantum computing; information security; risk governance; international coordination