Introdução

A emergência da computação quântica como paradigma disruptivo no processamento de informação desafia os limites da computação clássica, prometendo redefinir fronteiras científicas, econômicas e sociais. Ao explorar fenômenos quânticos como superposição, emaranhamento e interferência, essa tecnologia não apenas amplifica exponencialmente a capacidade de resolver problemas intratáveis para sistemas binários, mas também redefine a própria noção de inteligência artificial (IA). A convergência entre computação quântica e IA — encapsulada no aprendizado de máquina quântico (QML) — inaugura um horizonte de possibilidades que transcende a aceleração algorítmica, propondo reformulações radicais em representação de dados, otimização e modelagem de sistemas complexos. Contudo, esse potencial está entrelaçado com desafios técnicos monumentais, dilemas éticos nascentes e um cenário geopolítico marcado por competição estratégica e investimentos bilionários.

Desde os alicerces teóricos estabelecidos por Feynman e Deutsch até as recentes demonstrações de supremacia quântica, a jornada da computação quântica revela uma dualidade: enquanto algoritmos como o de Shor ameaçam desestabilizar sistemas criptográficos globais, avanços em simulação quântica e QML apontam para revoluções na descoberta de fármacos, otimização logística e processamento de linguagem natural. No cerne dessa revolução estão os *qubits*, unidades quânticas que, em sua superposição coerente e correlações não locais, permitem a exploração paralela de espaços de Hilbert de dimensão exponencial. Plataformas como circuitos supercondutores, íons aprisionados e fótons polarizados disputam primazia técnica, enquanto a era NISQ (*Noisy Intermediate-Scale Quantum*) impõe uma realidade pragmática: sistemas ruidosos e limitados exigem abordagens híbridas que integrem clássico e quântico em sinergia.

A intersecção com a IA amplifica tanto promessas quanto paradoxos. Algoritmos quânticos variacionais, redes neurais quânticas e *kernels* de alta dimensionalidade sugerem vantagens em tarefas de classificação, regressão e geração de dados. No entanto, obstáculos como o gargalo de E/S, *barren plateaus* em otimização e a escassez de *benchmarks* práticos revelam uma lacuna entre teoria e aplicação. Paralelamente, a corrida por vantagem quântica prática alimenta investimentos globais, com iniciativas como o *Quantum Flagship* europeu, a *National Quantum Initiative* estadunidense e os megaprojetos chineses redefinindo a geopolítica tecnológica. Governos e corporações não apenas buscam liderança científica, mas também enfrentam dilemas regulatórios urgentes — da criptografia pós-quântica à governança ética de sistemas quânticos de IA.

Este artigo examina criticamente essa paisagem multifacetada, estruturando-se em quatro eixos: (1) os fundamentos da computação quântica e sua sinergia com a IA; (2) as potencialidades transformadoras em setores estratégicos; (3) os desafios técnicos, teóricos e socioeconômicos que limitam a maturidade da tecnologia; e (4) o panorama global de pesquisa, investimentos e regululação emergente. Ao sintetizar avanços recentes e debates contemporâneos, busca-se não apenas mapear o estado da arte, mas também estimular reflexões críticas sobre os caminhos para uma adoção responsável e equitativa dessas tecnologias, cujo impacto promete reconfigurar — para bem ou para mal — o século XXI.

1. O que é Computação Quântica?

Antes de mergulharmos na computação quântica, é útil entender dois conceitos fundamentais. Primeiro, o que significa "quântico"? A palavra deriva do latim "quantus", que significa "quanto" ou "que quantidade". Na física, um "quantum" (plural: "quanta") é a menor unidade indivisível de algo, como energia ou matéria (Close, 2007). A mecânica quântica é o ramo da física que descreve como a natureza se comporta nessas escalas incrivelmente pequenas, as dos átomos e partículas subatômicas. As regras nesse reino são muitas vezes bizarras e contraintuitivas em comparação com o mundo que experimentamos diretamente, envolvendo probabilidades, superposições e conexões estranhas (Gilder, 2008). A computação quântica busca justamente aproveitar essas regras peculiares do mundo microscópico para processar informações de uma maneira nova e potencialmente muito mais poderosa.

Segundo, precisamos entender o "bit", a base dos computadores que usamos todos os dias. Pense em um interruptor de luz: ele pode estar LIGADO ou DESLIGADO. Um bit clássico é exatamente isso: uma unidade de informação que só pode ter um de dois valores possíveis, tipicamente representados como 0 ou 1 (Petzold, 1999). Toda a informação em seu computador, celular ou tablet – textos, imagens, vídeos – é codificada como longas sequências desses 0s e 1s. A grande limitação é que um bit só pode ser 0 *ou* 1 em um determinado momento, nunca ambos ao mesmo tempo (Petzold, 1999). É aqui que a computação quântica introduz uma mudança radical com o "qubit".

A computação quântica representa uma abordagem fundamentalmente nova ao processamento de informações, explorando fenômenos da mecânica quântica para realizar certos tipos de cálculos de forma mais eficiente que os computadores clássicos (Nielsen; Chuang, 2010). A natureza quântica dos qubits permite que eles existam em uma superposição linear dos estados 0 e 1, significando que um único qubit pode representar uma combinação de ambos os valores simultaneamente até que uma medição seja realizada (Preskill, 2018). Esta capacidade de superposição é uma das fontes primárias do poder computacional quântico, permitindo a exploração paralela de um vasto espaço de possibilidades (Google Quantum AI, 2023). Imagine, em vez de um simples interruptor LIGADO/DESLIGADO, um dimmer que pode estar em qualquer ponto intermediário, mas com a peculiaridade quântica de estar, de certa forma, em *todos* esses pontos ao mesmo tempo até você decidir "olhar" para ele.

Além da superposição, o emaranhamento é outro pilar essencial da computação quântica, descrevendo correlações não locais entre dois ou mais qubits (Nielsen; Chuang, 2010; Horodecki et al., 2009). Quando qubits estão emaranhados, seus destinos estão interligados de tal forma que a medição do estado de um qubit instantaneamente influencia o estado dos outros, independentemente da distância que os separa (Horodecki et al., 2009; Google Quantum AI, 2023). Este fenômeno contraintuitivo, chamado por Einstein de "ação fantasmagórica à distância", é um recurso crucial explorado por muitos algoritmos quânticos para alcançar coordenação e processamento de informações de maneiras inacessíveis aos sistemas clássicos (Horodecki et al., 2009). É como ter duas moedas mágicas: se você jogar uma e der cara, sabe instantaneamente que a outra, mesmo a quilômetros de distância, dará coroa, sem que nenhuma informação clássica precise viajar entre elas (Aczel, 2002).

A realização física de qubits é um campo ativo de pesquisa e engenharia, com diversas plataformas sendo exploradas, cada uma com suas próprias vantagens e desvantagens (Ladd et al., 2010; Wendin, 2017). Entre as abordagens mais promissoras estão os

circuitos supercondutores (transmons, fluxoniums), que são pequenos circuitos elétricos resfriados a temperaturas extremamente baixas; íons aprisionados em campos eletromagnéticos, onde átomos carregados são mantidos e manipulados por lasers; átomos neutros também controlados por lasers; fótons (partículas de luz) que viajam através de circuitos ópticos; defeitos em cristais como centros de nitrogênio-vacância (NV) em diamante; e os ainda mais exóticos qubits topológicos, que prometem maior robustez contra erros (Ladd et al., 2010; Wendin, 2017; Gambetta; Chow; Steffen, 2017; Nayak et al., 2008). A escolha da plataforma impacta diretamente fatores como tempo de coerência (quanto tempo o estado quântico persiste antes de ser destruído pelo ruído), fidelidade das portas quânticas (quão precisamente as operações podem ser realizadas), conectividade entre qubits (quais qubits podem interagir diretamente) e escalabilidade do sistema (a capacidade de construir sistemas com muitos qubits) (Preskill, 2018; Gambetta; Chow; Steffen, 2017). Nenhuma plataforma emergiu ainda como a vencedora definitiva, e a pesquisa continua explorando os méritos relativos de cada uma, com intensa competição entre os laboratórios e empresas (The Economist, 2023; MIT Technology Review, 2022).

As propriedades únicas de superposição e emaranhamento, manipuladas por portas quânticas (operações lógicas análogas às clássicas AND, OR, NOT, mas que operam sobre estados quânticos), permitem que computadores quânticos executem algoritmos específicos com eficiências drasticamente superiores às clássicas (Nielsen; Chuang, 2010). Algoritmos como o de Shor para fatoração de inteiros grandes (a base da segurança de muita criptografia atual) e o de Grover para busca em bancos de dados não estruturados são exemplos canônicos que demonstram o potencial de vantagem quântica para problemas específicos (Shor, 1997; Grover, 1996). Consequentemente, a computação quântica é particularmente promissora para resolver problemas complexos em simulação de sistemas quânticos (como moléculas e materiais), otimização combinatória e certas tarefas de aprendizado de máquina (IBM Research, 2021; Bauer; Bravyi; Motta, 2020), sendo esta última uma área de intensa investigação e expectativa.

Um terceiro princípio quântico fundamental explorado em algoritmos é a interferência quântica (Nielsen; Chuang, 2010). Assim como ondas de água podem se somar (interferência construtiva) para criar uma onda maior ou se cancelar (interferência destrutiva), as "ondas de probabilidade" associadas aos estados quânticos podem fazer o mesmo. Algoritmos quânticos são projetados de forma inteligente para orquestrar essa interferência de modo que os caminhos computacionais que levam às respostas incorretas se cancelem mutuamente, enquanto os caminhos que levam à resposta correta se reforcem, aumentando significativamente a probabilidade de medir o resultado desejado ao final do cálculo (Nielsen; Chuang, 2010; Aaronson, 2013). O algoritmo de Grover, por exemplo, utiliza habilmente a interferência para amplificar a amplitude (probabilidade) do item de busca correto em um banco de dados (Grover, 1996). A capacidade de controlar a interferência é crucial para muitos algoritmos quânticos, incluindo aqueles propostos para aplicações em IA.

É importante distinguir entre diferentes modelos de computação quântica. O modelo mais geral é o de computação quântica baseada em portas (gate-based), que visa construir um computador quântico universal capaz de executar qualquer algoritmo quântico, análogo a um computador clássico universal (Nielsen; Chuang, 2010). Empresas como IBM, Google, IonQ e Quantinuum estão focadas principalmente neste

modelo, buscando construir máquinas flexíveis para uma ampla gama de aplicações, incluindo QML. Outra abordagem é a computação quântica adiabática, ou *quantum annealing*, implementada por empresas como a D-Wave Systems, que é projetada especificamente para resolver problemas de otimização, encontrando o estado de menor energia (a solução ótima ou próxima da ótima) de um sistema quântico cuidadosamente projetado que representa o problema (Das; Chakrabarti, 2008; Johnson et al., 2011). Embora menos geral que o modelo de portas, o *annealing* pode oferecer vantagens para certas classes de problemas de otimização no curto prazo, incluindo algumas tarefas de otimização que surgem no treinamento de modelos de IA (Hauke et al., 2020; D-Wave Systems, 2024; BBC News, 2022; Adachi; Henderson, 2015).

As raízes conceituais da computação quântica remontam às décadas de 1980 e 1990. O físico Richard Feynman, ganhador do Prêmio Nobel, propôs em 1981, durante uma palestra no MIT, a ideia visionária de usar sistemas quânticos para simular outros sistemas quânticos, argumentando que a natureza não é clássica e, para simulá-la, precisaríamos de um computador que operasse segundo os mesmos princípios quânticos (Feynman, 1982; MIT News, 2011). Pouco depois, David Deutsch, na Universidade de Oxford, formalizou a noção de um computador quântico universal (uma "Máquina de Turing Quântica") e mostrou que ele poderia realizar tarefas computacionais de forma diferente e, em alguns casos, mais eficientemente que as máquinas de Turing clássicas (Deutsch, 1985). Esses trabalhos seminais, juntamente com o desenvolvimento de algoritmos chave como os de Shor (que chocou a comunidade de criptografia) e Grover nos anos 90, lançaram as bases teóricas para o campo florescente que vemos hoje (Shor, 1997; Grover, 1996; Physics Today, 2000). A ideia de aplicar esses princípios a tarefas de IA começou a surgir mais tarde, ganhando tração significativa nas últimas duas décadas (Biamonte et al., 2017).

Um aspecto crucial e muitas vezes desconcertante da mecânica quântica é o ato da medição. Enquanto um qubit pode estar em superposição de 0 e 1 durante o cálculo, assim que tentamos "ler" seu valor, o estado quântico "colapsa" para um dos estados clássicos (0 ou 1) com uma certa probabilidade determinada pelas amplitudes quânticas (Nielsen; Chuang, 2010; Jaeger, 2007). Esse processo é irreversível e destrói a superposição original. Isso significa que não podemos simplesmente "ver" todo o paralelismo quântico diretamente; os algoritmos precisam ser projetados para que a resposta desejada tenha alta probabilidade de ser obtida quando a medição final é realizada (Jaeger, 2007). O "problema da medição" – o que exatamente causa o colapso e a transição do quântico para o clássico – ainda é um tópico de debate filosófico e de pesquisa fundamental na física quântica (Schlosshauer, 2005). Em QML, isso implica que frequentemente precisamos executar um circuito quântico muitas vezes (realizar muitas "shots") para estimar estatisticamente o resultado desejado, como o valor de uma função de perda ou a classificação de um ponto de dados (Schuld; Petruccione, 2018).

2. Potenciais Benefícios e Aplicações

O potencial transformador da computação quântica abrange diversas áreas científicas e industriais, com pesquisas ativas explorando aplicações concretas. Um dos campos mais promissores é a química quântica e a ciência de materiais, onde a capacidade de simular com precisão o comportamento de moléculas e elétrons – tarefas extremamente difíceis para computadores clássicos devido à complexidade quântica inerente – pode revolucionar a descoberta de novos fármacos, catalisadores mais eficientes (por

exemplo, para produção de fertilizantes com menor consumo de energia) e materiais com propriedades inéditas, como supercondutores à temperatura ambiente (que eliminariam perdas na transmissão de energia) ou baterias de maior desempenho e segurança (Bauer; Bravyi; Motta, 2020; Cao et al., 2019; Reiher et al., 2017). A colaboração entre IBM e Moderna para aplicar métodos quânticos e de IA na descoberta de terapias de mRNA exemplifica essa convergência (IBM Research & Moderna, 2023), e outras gigantes farmacêuticas como a Roche, Boehringer Ingelheim e Merck KGaA também estão explorando ativamente a tecnologia em parcerias ou pesquisas internas (Roche, 2023; Boehringer Ingelheim, 2021; Merck KGaA, 2022).

Problemas de otimização, onipresentes em finanças (otimização de portfólios de investimento, precificação de derivativos complexos, gerenciamento de risco), logística (roteamento de veículos para entregas, planejamento da cadeia de suprimentos global), engenharia (design de estruturas, otimização de processos industriais) e pesquisa operacional, representam outra área de aplicação chave (Orús; Mugel; Lizaso, 2019; Herman et al., 2023). Muitos desses problemas envolvem encontrar a melhor solução entre um número astronômico de possibilidades (NP-hard problems). Algoritmos quânticos, como o Quantum Approximate Optimization Algorithm (QAOA) e a computação quântica adiabática (quantum annealing), oferecem novas abordagens para encontrar soluções ótimas ou de alta qualidade para esses problemas combinatórios complexos que são intratáveis para os métodos clássicos (Farhi; Goldstone; Gutmann, 2014; Herman et al., 2023). Empresas como a D-Wave Systems têm focado especificamente em hardware de annealing para tais problemas (D-Wave Systems, 2024), e aplicações em otimização de tráfego (Volkswagen), design de antenas (Multiverse Computing/Bosch), e otimização de produção industrial já estão sendo testadas em colaborações com empresas globais (Neukart et al., 2017; Financial Post, 2021; Multiverse Computing, 2023).

2.1. Aprofundando em Computação Quântica para Inteligência Artificial (QML)

A intersecção entre computação quântica e inteligência artificial, conhecida como Aprendizado de Máquina Quântico (Quantum Machine Learning - QML), é uma fronteira de pesquisa em rápida expansão e uma das áreas mais empolgantes e debatidas do campo quântico (Biamonte et al., 2017; Schuld; Petruccione, 2018; Dunjko; Briegel, 2018). A premissa central é que os princípios quânticos – superposição, emaranhamento e interferência – podem oferecer novas maneiras de processar informações e aprender a partir de dados, potencialmente superando algoritmos de IA clássicos em certas tarefas (Wittek, 2014). Além de acelerar potencialmente certas sub-rotinas computacionalmente intensivas do treinamento de modelos de IA clássicos (como álgebra linear ou otimização) (Google Quantum AI, 2023; Rebentrost; Mohseni; Lloyd, 2014), algoritmos quânticos podem oferecer novas formas de representar dados, explorar espaços de características de dimensão exponencialmente maior e identificar padrões complexos ou correlações sutis que métodos clássicos poderiam negligenciar (Biamonte et al., 2017; Schuld; Sinayskiy; Petruccione, 2015).

Diversas classes de algoritmos de QML estão sendo ativamente pesquisadas. Uma categoria importante são os métodos de kernel quântico, como as Máquinas de Vetores de Suporte Quânticas (QSVMs) (Rebentrost; Mohseni; Lloyd, 2014; Havlícek et al., 2019). A ideia aqui é usar um computador quântico para mapear eficientemente os dados de entrada para um espaço de características quântico de dimensão muito alta

(potencialmente exponencial), onde os dados podem se tornar linearmente separáveis, e então calcular a "matriz de kernel" (que mede a similaridade entre os pontos de dados nesse espaço) de forma mais eficiente que classicamente. A classificação final é então realizada por um SVM clássico usando esse kernel quântico. Embora promissor teoricamente, o desempenho prático depende crucialmente da escolha do mapeamento quântico e da capacidade de demonstrar vantagem sobre kernels clássicos sofisticados (Schuld; Killoran, 2019; Huang et al., 2021).

Outra área proeminente são as Redes Neurais Quânticas (QNNs) ou circuitos quânticos variacionais (Benedetti et al., 2019; Cerezo et al., 2021; Farhi; Neven, 2018). Estes são modelos híbridos onde um circuito quântico parametrizado (cujas portas quânticas dependem de parâmetros clássicos ajustáveis) é otimizado usando um computador clássico. O circuito quântico atua como um componente do modelo de IA, processando dados quânticos ou clássicos codificados em estados quânticos. A otimização busca ajustar os parâmetros do circuito para minimizar uma função de custo, de forma análoga ao treinamento de redes neurais clássicas. QNNs são vistas como uma abordagem promissora para o hardware NISQ, pois podem se adaptar ao ruído e à arquitetura específica do dispositivo. Elas estão sendo exploradas para tarefas de classificação, regressão e até mesmo como modelos generativos (Benedetti et al., 2019; Mitarai et al., 2018). No entanto, o treinamento de QNNs enfrenta desafios como a otimização em paisagens de custo complexas e o fenômeno dos "barren plateaus" (platôs áridos), onde os gradientes se tornam exponencialmente pequenos com o aumento do número de qubits, dificultando o treinamento (McClean et al., 2018; Cerezo et al., 2021).

Modelos generativos quânticos também são uma área de grande interesse, buscando aproveitar a capacidade quântica de representar distribuições de probabilidade complexas. As Redes Adversariais Generativas Quânticas (QGANs) propõem usar circuitos quânticos como gerador e/ou discriminador dentro do framework GAN clássico (Lloyd; Weedbrook, 2018; Dallaire-Demers; Killoran, 2018). A esperança é que QGANs possam aprender e amostrar distribuições mais complexas do que suas contrapartes clássicas, potencialmente evitando problemas como o colapso de modo (onde o gerador produz apenas uma pequena variedade de amostras) (Zoufal; Lucchi; Woerner, 2019; IonQ & Hyundai, 2025). Similarmente, Autoencoders Variacionais Quânticos (QVAEs) exploram o uso de circuitos quânticos (seja em annealers ou gate-based) para aprender representações latentes compactas de dados e gerar novas amostras (Khoshaman et al., 2018; D-Wave Systems, 2024). Aplicações potenciais incluem a geração de novas estruturas moleculares com propriedades desejadas na descoberta de fármacos ou a modelagem de cenários complexos em finanças (Romero et al., 2017; Accenture, 2021).

A computação quântica também pode oferecer aceleração para sub-rotinas matemáticas fundamentais em muitos algoritmos de IA clássicos. O exemplo mais famoso é o algoritmo HHL (Harrow, Hassidim, Lloyd), que pode resolver sistemas de equações lineares exponencialmente mais rápido que os melhores algoritmos clássicos, sob certas condições (Harrow; Hassidim; Lloyd, 2009). Como a solução de sistemas lineares e a manipulação de matrizes são centrais em IA (por exemplo, em regressão linear, máquinas de vetores de suporte, métodos de Newton), o HHL gerou grande entusiasmo. No entanto, suas condições de aplicabilidade são restritivas (a matriz precisa ser esparsa e bem condicionada, e a preparação do estado de entrada e a leitura do estado de saída são

desafios significativos), limitando sua utilidade prática direta no momento atual (Aaronson, 2015; Childs; Kothari; Somma, 2017). Outros algoritmos quânticos para álgebra linear, como a Análise de Componentes Principais Quântica (qPCA) (Lloyd; Mohseni; Rebentrost, 2014), também prometem speedups, mas enfrentam desafios semelhantes de entrada/saída de dados.

A otimização, um componente central do treinamento da maioria dos modelos de IA (ajustar os parâmetros do modelo para minimizar erros), é outra área onde a computação quântica pode ter impacto. Algoritmos como QAOA ou quantum annealing podem ser aplicados para encontrar melhores parâmetros para modelos de IA, ou mesmo para otimizar a arquitetura de redes neurais (uma tarefa combinatória difícil) (Farhi; Goldstone; Gutmann, 2014; D-Wave Systems, 2024; Wilson et al., 2022). Além disso, o aprendizado por reforço quântico (Quantum Reinforcement Learning - QRL) explora como agentes quânticos poderiam aprender políticas ótimas em ambientes complexos potencialmente mais rápido ou de forma mais eficiente que agentes clássicos, explorando superposição para avaliar múltiplas ações simultaneamente (Dunjko; Taylor; Briegel, 2016; Lamata, 2017). Esta é uma área ainda mais especulativa, mas com potencial interessante para robótica e sistemas autônomos.

Devido às limitações do hardware quântico atual (era NISQ), a maioria das pesquisas e aplicações práticas de QML hoje se concentra em abordagens híbridas quântico-clássicas (McClean et al., 2016; Perdomo-Ortiz et al., 2018; Bharti et al., 2022). Nestes modelos, um computador clássico lida com a maior parte do processamento de dados, gerenciamento de memória e fluxo de controle geral, enquanto um processador quântico (QPU) é usado como um co-processador ou acelerador para executar sub-rotinas específicas que são consideradas difíceis para o clássico, mas potencialmente tratáveis para o quântico. Os algoritmos quânticos variacionais (VQAs), como VQE (Variational Quantum Eigensolver) e QAOA, e as QNNs mencionadas anteriormente, são exemplos primários de algoritmos híbridos projetados para hardware NISQ (Cerezo et al., 2021). Esta abordagem pragmática tenta extrair valor dos dispositivos quânticos atuais, mesmo com suas imperfeições, e é a estratégia adotada pela maioria das empresas que exploram aplicações de QML em setores como finanças, química e logística (Zapata Computing, 2023; Quantinuum, 2023; Deloitte, 2022).

Finalmente, o Processamento de Linguagem Natural Quântico (QNLP) busca aplicar princípios e algoritmos quânticos à análise e geração de linguagem humana (Coecke; Meichanetzidis; Toumi, 2020; Zeng; Coecke, 2016). A ideia central é que a estrutura matemática da mecânica quântica (espaços de Hilbert, tensores) pode ser mais adequada para modelar a composição de significados em linguagem (como o significado de uma frase emerge do significado das palavras e da estrutura gramatical) do que os modelos de espaço vetorial clássicos. Frameworks como o DisCoCat (Distributional Compositional Categorical) propõem mapear palavras para estados quânticos e regras gramaticais para operações quânticas (portas e medições). Ferramentas de software como lambeq, desenvolvida pela Quantinuum (anteriormente Cambridge Quantum), permitem implementar e testar esses modelos em hardware quântico real ou simulado (Cambridge Quantum, 2022; Kartsaklis et al., 2021). Embora ainda em estágio inicial e experimental, o QNLP espera oferecer modelos de linguagem mais eficientes em termos de parâmetros, capazes de capturar nuances semânticas, ambiguidades e raciocínio de senso comum de forma mais eficaz (Lorenz et al., 2021).

A computação quântica também tem implicações profundas para a criptografia e segurança da informação. O algoritmo de Shor representa uma ameaça existencial para muitos dos sistemas criptográficos de chave pública atualmente em uso, como o RSA (usado em HTTPS, VPNs, assinaturas digitais) e a Criptografia de Curvas Elípticas (ECC) (usada em muitas criptomoedas e comunicações móveis), que dependem da dificuldade computacional da fatoração de inteiros grandes e do problema do logaritmo discreto para computadores clássicos (Shor, 1997; Mosca, 2018). A perspectiva de computadores quânticos suficientemente poderosos (provavelmente na era FTQC) quebrarem a criptografia que protege dados financeiros, segredos governamentais, propriedade intelectual e infraestrutura crítica levou a uma corrida global para desenvolver e padronizar novos algoritmos criptográficos resistentes à quântica (Post-Quantum Cryptography - PQC) (Alagic et al., 2022; The New York Times, 2022; The Guardian, 2024). O NIST (National Institute of Standards and Technology) dos EUA está liderando esse esforço de padronização, tendo selecionado os primeiros algoritmos (baseados principalmente em reticulados e hashes) em 2022 e continuando a avaliar outros candidatos, com a expectativa de que a transição para PQC leve muitos anos e exija um esforço considerável de empresas e governos (NIST, 2024; Wired, 2023). A urgência deriva da ameaça "harvest now, decrypt later", onde adversários podem estar coletando dados criptografados hoje para decifrá-los quando computadores quânticos potentes estiverem disponíveis (Mosca, 2018).

Por outro lado, a mecânica quântica também oferece soluções para comunicações seguras. A Distribuição Quântica de Chaves (QKD) utiliza princípios como o teorema da não-clonagem (que afirma ser impossível criar uma cópia idêntica de um estado quântico desconhecido) e a sensibilidade à medição para permitir que duas partes estabeleçam uma chave secreta compartilhada com segurança garantida pelas leis da física, tornando qualquer tentativa de espionagem detectável (Gisin et al., 2002; Scarani et al., 2009). Redes QKD já estão sendo implementadas em projetos piloto e comerciais em vários países (como China, Coreia do Sul, Suíça e Reino Unido), oferecendo uma camada adicional de segurança, especialmente para infraestruturas críticas, instituições financeiras e governos (Nature Photonics, 2021; Toshiba, 2023). No entanto, desafios relacionados à distância de transmissão (a perda de fótons em fibras ópticas limita o alcance), à taxa de geração de chaves e à necessidade de nós confiáveis em redes maiores ainda limitam sua adoção em larga escala (Lo; Curty; Tamaki, 2014). Pesquisas em repetidores quânticos e QKD baseada em satélites (como o projeto Micius da China) buscam superar essas limitações (Nature, 2020; Muralidharan et al., 2016).

Além das áreas mencionadas, a computação quântica pode impactar a modelagem de sistemas complexos em outras disciplinas. Por exemplo, a simulação de processos relacionados às mudanças climáticas, como a dinâmica atmosférica detalhada, a química do ciclo do carbono ou a interação oceano-atmosfera, poderia se beneficiar da capacidade quântica de lidar com alta complexidade e múltiplas variáveis interconectadas (Fingerhuth et al., 2018; Ollitrault; Kandala; Tavernelli, 2020). Da mesma forma, a descoberta de novos materiais para captura de carbono mais eficiente, para tecnologias de energia renovável (como células solares com maior conversão ou materiais para fusão nuclear) ou para armazenamento de hidrogênio é uma área de aplicação potencial onde simulações quânticas precisas poderiam acelerar o desenvolvimento (Bauer; Bravyi; Motta, 2020; Voronin; Sedykh; Mastiukova, 2023).

Outra aplicação emergente e promissora reside nos sensores quânticos. Utilizando a extrema sensibilidade dos estados quânticos (como spin de elétrons ou níveis de energia atômica) a perturbações externas (campos magnéticos, elétricos, gravitacionais, temperatura, rotação), é possível construir dispositivos de medição com precisão e sensibilidade sem precedentes, superando os limites dos sensores clássicos (Degen; Reinhard; Cappellaro, 2017; Pirandola et al., 2018). Aplicações potenciais incluem relógios atômicos mais precisos (importantes para GPS, telecomunicações e ciência fundamental), sistemas de navegação inercial que não dependem de GPS (cruciais para defesa e exploração submarina ou espacial), imageamento médico de altíssima resolução (como magnetoencefalografia baseada em sensores quânticos para mapear atividade cerebral com precisão espacial e temporal sem precedentes) e detecção de campos gravitacionais ou magnéticos minúsculos para geofísica (prospecção de recursos, monitoramento vulcânico) ou ciência fundamental (busca por matéria escura) (Degen; Reinhard; Cappellaro, 2017; Boto et al., 2018; Ludlow; Boyd; Ye, 2015). Sensores quânticos podem ser uma das primeiras tecnologias quânticas a ter um impacto comercial significativo em nichos específicos (McKinsey & Company, 2021).

Apesar do entusiasmo e do progresso rápido, é crucial manter expectativas realistas sobre os prazos para a concretização desses benefícios. Muitas das aplicações transformadoras, especialmente aquelas que exigem computadores quânticos tolerantes a falhas em larga escala (FTQC) com milhões de qubits lógicos – como quebrar a criptografia RSA-2048 ou realizar simulações químicas complexas com alta precisão – ainda estão provavelmente a uma década ou mais de distância, talvez até várias décadas (MIT Technology Review, 2023; The Economist, 2023; BCG, 2021). A era atual é frequentemente descrita como a era NISQ (Noisy Intermediate-Scale Quantum), onde os dispositivos têm dezenas a milhares de qubits físicos que são ruidosos (propensos a erros) e sem correção de erros completa (Preskill, 2018). O desafio central da era NISQ é encontrar "vantagens quânticas" significativas – problemas onde mesmo esses dispositivos imperfeitos podem superar os melhores supercomputadores clássicos – em aplicações práticas e comercialmente relevantes. Até agora, demonstrações de "supremacia quântica" (como as do Google e da China) foram realizadas em problemas artificiais, e encontrar vantagens práticas em problemas do mundo real com hardware NISQ provou ser extremamente difícil, *especialmente no domínio do aprendizado de máquina*, onde algoritmos clássicos são altamente otimizados e muitas vezes beneficiados por enormes conjuntos de dados (Daley et al., 2022; Wired, 2022; Huang et al., 2022). Há um debate ativo na comunidade sobre se a era NISQ por si só trará valor comercial substancial ou se o verdadeiro impacto, particularmente em QML, só virá com a computação quântica tolerante a falhas (FTQC) (Martinis, 2021; Babbush et al., 2021).

3. Limitações e Desafios Atuais

Apesar do progresso notável, a construção de computadores quânticos tolerantes a falhas em larga escala enfrenta desafios científicos e de engenharia formidáveis, que precisam ser superados para que a tecnologia atinja seu pleno potencial (Preskill, 2018; Gyongyosi; Imre; Nguyen, 2018). A escalabilidade, ou seja, aumentar o número de qubits de alta qualidade, permanece uma barreira primária (IBM Research, 2022). Embora o número de qubits em protótipos tenha crescido (com processadores superando a marca de 1000 qubits físicos sendo anunciados), manter a alta fidelidade das operações quânticas (tipicamente acima de 99.9% para permitir QEC eficaz) e a conectividade

necessária entre eles (permitindo que qubits interajam eficientemente) à medida que o sistema cresce é tecnicamente exigente (Preskill, 2018; Krantz et al., 2019; IBM Newsroom, 2023). Aumentar a contagem de qubits sem comprometer a qualidade, ou mesmo melhorando-a, é um dos maiores obstáculos de engenharia, exigindo avanços em fabricação, controle e arquitetura (Martinis, 2021; Gambetta, 2023).

O desafio mais onipresente e fundamental é a decoerência, a tendência dos delicados estados quânticos (superposição e emaranhamento) de se degradarem rapidamente devido a interações indesejadas com o ambiente circundante (Zurek, 2003; Preskill, 2018). Ruído proveniente de flutuações térmicas, campos eletromagnéticos espúrios, vibrações mecânicas, raios cósmicos e imperfeições nos materiais e no controle experimental limitam o tempo durante o qual um qubit pode manter sua informação quântica (tempo de coerência, T1 e T2) e a precisão com que as portas quânticas podem ser aplicadas (fidelidade das portas) (Zurek, 2003; Google Quantum AI, 2023; Krantz et al., 2019). Esses erros, mesmo que pequenos em cada operação, acumulam-se rapidamente em algoritmos longos, tornando o resultado final inútil. A fragilidade inerente dos estados quânticos exige ambientes operacionais extremamente controlados e isolados, o que contribui para a complexidade e o custo dos sistemas atuais (Schlosshauer, 2007).

A correção de erros quânticos (QEC) é considerada a solução de longo prazo para a decoerência e os erros de operação, sendo essencial para a computação quântica tolerante a falhas (FTQC) (Terhal, 2015; Preskill, 2018; Devitt; Munro; Nemoto, 2013). A ideia básica da QEC é utilizar redundância: codificar a informação de um único qubit "lógico" (ideal e protegido) em muitos qubits "físicos" (reais e ruidosos) de uma forma inteligente, permitindo que o sistema detecte e corrija erros que afetam os qubits físicos individuais sem destruir a informação lógica armazenada (Gottesman, 2010). No entanto, os códigos QEC mais promissores, como o código de superfície (surface code), impõem uma sobrecarga massiva, potencialmente exigindo centenas ou até milhares de qubits físicos de alta qualidade para criar um único qubit lógico robusto (Fowler et al., 2012; Terhal, 2015). Alcançar o limiar de erro físico necessário para que a QEC seja eficaz (onde adicionar mais qubits físicos realmente *reduz* o erro lógico líquido, em vez de aumentá-lo) e reduzir drasticamente essa sobrecarga de qubits são áreas críticas de pesquisa ativa e um dos maiores desafios no caminho para a FTQC (Google Quantum AI, 2023; Sivak et al., 2023; Nature News, 2023). Além disso, realizar operações lógicas (portas) diretamente nos qubits lógicos codificados de forma tolerante a falhas adiciona outra camada de complexidade significativa (Campbell; Terhal; Vuillot, 2017).

Outras limitações práticas incluem a dificuldade em desenvolver uma memória quântica estável e de longa duração para armazenar estados quânticos intermediários durante cálculos complexos (Heshami et al., 2016; Google Quantum AI, 2023). Os tempos de coerência atuais, embora melhorando, ainda são curtos (na faixa de microssegundos a milissegundos para muitas plataformas líderes), limitando a profundidade (número de passos) dos algoritmos que podem ser executados. A interface entre o processamento quântico (operando em níveis de energia baixíssimos e com sinais delicados) e os sistemas de controle e leitura clássicos (operando em temperatura ambiente com eletrônica convencional), incluindo o carregamento eficiente de dados clássicos em estados quânticos (input) e a extração dos resultados da computação (output), também apresenta desafios significativos de engenharia e pode se tornar um gargalo (o "I/O bottleneck") à medida que os sistemas escalam (IonQ & Hyundai, 2025; Preskill, 2018; Fu

et al., 2019). A necessidade de interconexões quânticas eficientes e de baixa perda para conectar diferentes módulos de processamento quântico (para construir máquinas maiores) ou para estabelecer redes quânticas distribuídas é outro gargalo tecnológico em desenvolvimento ativo (Awsalom et al., 2019; Pompili et al., 2021).

Muitas das plataformas de qubits mais avançadas, como as baseadas em circuitos supercondutores (usadas por Google, IBM, Rigetti) ou alguns qubits de spin em semicondutores, exigem condições operacionais extremas, notadamente temperaturas criogênicas próximas do zero absoluto (na faixa de 10-100 milikelvins) para minimizar o ruído térmico e permitir o comportamento quântico desejado (Wendin, 2017; Krantz et al., 2019). Isso requer o uso de refrigeradores de diluição – máquinas grandes, caras (custando centenas de milhares a milhões de dólares), complexas e que consomem energia considerável – além de um isolamento rigoroso contra vibrações e campos magnéticos externos usando múltiplas camadas de blindagem (The Verge, 2021; Physics World, 2019). Esses requisitos ambientais severos aumentam significativamente o custo e a complexidade da construção e operação de computadores quânticos, limitando sua implantação fora de laboratórios de pesquisa especializados ou grandes data centers e representando um desafio para a miniaturização e portabilidade (Financial Times, 2022). Plataformas como íons aprisionados ou fótons podem operar em condições menos extremas (vácuo e temperatura ambiente ou resfriamento moderado), mas enfrentam seus próprios desafios de escalabilidade e controle (Bruzewicz; Chiaverini; McConnell, 2019).

Além dos desafios de hardware, o desenvolvimento do software e dos algoritmos quânticos ainda está em sua infância relativa em comparação com o ecossistema de software clássico maduro. Traduzir problemas do mundo real em algoritmos quânticos eficientes que possam rodar em hardware ruidoso é uma tarefa não trivial que exige expertise especializada e, muitas vezes, novas abordagens algorítmicas (Gyongyosi; Imre; Nguyen, 2018; Montanaro, 2016). A pilha de software quântico – incluindo linguagens de programação de alto nível (como Qiskit, Cirq, Q#), compiladores que traduzem esses algoritmos em sequências de pulsos de controle físico para os qubits específicos, ferramentas de otimização, simuladores clássicos para teste e depuração, e bibliotecas de algoritmos – ainda está em rápido desenvolvimento e carece da maturidade, padronização e facilidade de uso das ferramentas de software clássicas (Fingerhuth et al., 2018; Microsoft Research Blog, 2022; LaRose et al., 2019). A criação de um ecossistema de software robusto, eficiente e acessível é crucial para tornar a computação quântica utilizável por um público mais amplo de cientistas, engenheiros e desenvolvedores.

Finalmente, existe um crescente reconhecimento de um "gap de talento" ou escassez de mão de obra qualificada no campo da computação quântica, que pode se tornar um gargalo significativo para o progresso (Forbes, 2022; Nature, 2022; McKinsey & Company, 2021). A natureza altamente interdisciplinar do campo exige expertise combinada em física quântica, ciência da computação, engenharia elétrica, engenharia de software, ciência de materiais e matemática. Há uma demanda crescente por engenheiros quânticos (hardware e software), pesquisadores de algoritmos, especialistas em aplicações setoriais e técnicos para operar e manter os sistemas, mas a oferta de profissionais com o treinamento e a experiência necessários ainda é limitada (Quantum Computing Report, 2023; The Quantum Insider, 2023). Universidades e empresas estão lançando novos programas educacionais, cursos online e iniciativas de treinamento para

tentar preencher essa lacuna, mas desenvolver a força de trabalho quântica necessária levará tempo e investimento contínuo (Nature, 2022; QURECA, 2023).

O custo de desenvolvimento e construção de computadores quânticos também é um fator limitante significativo. Estima-se que a construção de um único processador quântico avançado e sua infraestrutura de suporte possa custar dezenas a centenas de milhões de dólares (Financial Times, 2022; BCG, 2021). Esses custos elevados restringem o desenvolvimento de hardware a grandes corporações, laboratórios governamentais bem financiados e startups com acesso a capital de risco substancial. Para a maioria dos pesquisadores e potenciais usuários, o acesso à computação quântica depende de plataformas de nuvem oferecidas pelos principais players, o que, embora democratize o acesso, ainda pode envolver custos significativos para uso extensivo (Wired, 2022). A questão da viabilidade econômica e do retorno sobre o investimento para aplicações quânticas, especialmente na era NISQ, permanece uma consideração importante para a adoção industrial (McKinsey & Company, 2021).

Outro desafio metodológico importante é o benchmarking – avaliar e comparar de forma justa e significativa o desempenho de diferentes computadores quânticos (hardware e software) (Lubinski et al., 2023; Tomesh; Gokhale; Chong, 2022). Dada a diversidade de plataformas de qubits, arquiteturas e métricas de desempenho (número de qubits, conectividade, fidelidade, tempos de coerência, velocidade de clock quântico, etc.), e a sensibilidade dos algoritmos ao ruído específico do hardware, é difícil estabelecer métricas universais ou benchmarks padronizados que capturem o desempenho real em aplicações relevantes. Desenvolver benchmarks robustos e "agnósticos de hardware" é crucial para acompanhar o progresso, orientar o desenvolvimento e, eventualmente, demonstrar de forma convincente a vantagem quântica prática sobre os computadores clássicos (Lubinski et al., 2023; Mills et al., 2021). Isso é particularmente complexo para QML, onde a comparação deve ser feita não apenas com algoritmos clássicos equivalentes, mas com os *melhores* algoritmos clássicos disponíveis para a tarefa, que são frequentemente heurísticos altamente otimizados (Huang et al., 2022).

3.1. Desafios Específicos para QML

Além dos desafios gerais da computação quântica, o campo de QML enfrenta obstáculos particulares. Um dos mais citados é o gargalo de entrada/saída de dados (I/O bottleneck) (Preskill, 2018; Schuld, 2021). Muitos algoritmos de IA clássicos operam sobre conjuntos de dados massivos. Carregar eficientemente esses dados clássicos em estados quânticos (amplitude encoding, por exemplo) é uma tarefa difícil e demorada, que pode anular qualquer speedup quântico obtido na etapa de processamento. A proposta teórica de uma RAM Quântica (QRAM), que permitiria acesso rápido a dados clássicos armazenados em superposição, ainda está longe de ser realizada experimentalmente e enfrenta seus próprios desafios de construção e correção de erros (Giovannetti; Lloyd; Maccone, 2008; Prakash, 2014). Sem QRAM eficiente, a aplicação de QML a problemas de "big data" é severamente limitada.

Outro desafio significativo, especialmente para QNNs e circuitos variacionais, é o fenômeno dos "barren plateaus" (platôs áridos) (McClean et al., 2018; Cerezo et al., 2021). Em paisagens de otimização de alta dimensão (com muitos parâmetros), descobriu-se que os gradientes da função de custo (usados para guiar a otimização) tendem a se tornar exponencialmente pequenos com o aumento do número de qubits ou

da profundidade do circuito, para circuitos quânticos "aleatórios" ou pouco estruturados. Isso significa que o treinamento pode estagnar completamente, tornando a otimização impraticável para problemas de larga escala. Pesquisas estão em andamento para entender as causas dos platôs áridos e desenvolver estratégias para evitá-los, como inicialização inteligente de parâmetros, escolha cuidadosa da arquitetura do circuito ou métodos de otimização adaptados (Grant et al., 2019; Pesah et al., 2021).

Além disso, provar uma vantagem quântica rigorosa e prática em tarefas de aprendizado de máquina do mundo real é notoriamente difícil (Huang et al., 2022; Tang, 2019). Algoritmos clássicos de IA, especialmente deep learning, são extremamente poderosos e altamente otimizados, beneficiando-se de décadas de desenvolvimento e hardware especializado (GPUs, TPUs). Muitas vezes, speedups quânticos teóricos desaparecem quando comparados com os melhores algoritmos clássicos disponíveis, ou quando se considera o custo total (incluindo preparação de estado, leitura e correção de erros). Além disso, alguns resultados surpreendentes mostraram que certos algoritmos quânticos propostos para ML podem ser "desquantizados", ou seja, simulados eficientemente por algoritmos clássicos inspirados na abordagem quântica, eliminando a necessidade do hardware quântico (Tang, 2019; Chia; Lin; Wang, 2020). Identificar tarefas onde a computação quântica oferece uma vantagem genuína e robusta sobre os melhores métodos clássicos continua sendo um objetivo central e desafiador para a comunidade de QML (Preskill, 2018; Babbush et al., 2021).

4. Iniciativas Globais e Pesquisas

O reconhecimento do potencial estratégico e disruptivo da computação quântica impulsionou investimentos massivos e iniciativas coordenadas em pesquisa e desenvolvimento em todo o mundo, criando um cenário global dinâmico e competitivo (Gibney, 2019; Riedel et al., 2019; The Quantum Insider, 2023). Governos nacionais lançaram programas ambiciosos para fomentar a pesquisa fundamental, o desenvolvimento tecnológico, a criação de ecossistemas de inovação e a formação de mão de obra qualificada, impulsionados em parte pelo potencial transformador previsto em áreas como criptografia, ciência de materiais e *quantum-enhanced artificial intelligence*. Nos Estados Unidos, a National Quantum Initiative (NQI), assinada em lei em 2018 e reautorizada e expandida desde então, coordena esforços e financia centros de pesquisa e infraestrutura através de agências como o Department of Energy (DOE), National Science Foundation (NSF) e NIST, com um investimento inicial autorizado de US$ 1,2 bilhão e financiamento adicional significativo nos anos seguintes (National Quantum Initiative Act, 2018; The White House, 2022; AIP, 2023). A União Europeia estabeleceu o Quantum Flagship em 2018, um programa de pesquisa e inovação de longo prazo e grande escala, com um orçamento inicial de €1 bilhão para 10 anos, financiando projetos colaborativos em computação, comunicação, simulação e sensores quânticos em toda a Europa (Quantum Flagship, 2023; European Commission, 2021). Muitos estados membros da UE, como Alemanha e França, também lançaram seus próprios planos nacionais multibilionários para complementar a iniciativa europeia (German Federal Ministry of Education and Research, 2023; Reuters, 2021).

A China declarou as tecnologias quânticas uma prioridade estratégica nacional de longo prazo, investindo pesadamente em pesquisa e infraestrutura, com estimativas de gastos governamentais totais (embora difíceis de verificar precisamente) potencialmente superando os de outros países (Xinhua News Agency, 2020; Center for Security and

Emerging Technology, 2021; The Diplomat, 2023). O país alcançou marcos notáveis tanto em computação quântica (com os processadores supercondutores Zuchongzhi e fotônicos Jiuzhang demonstrando vantagem quântica em tarefas específicas de amostragem) quanto em comunicação quântica (com o lançamento bem-sucedido do satélite Micius para QKD intercontinental e a construção de extensas redes QKD terrestres) (Science, 2021; Nature, 2020; The Wall Street Journal, 2021). Outros países como Reino Unido (com seu National Quantum Technologies Programme estabelecido em 2014 e um novo plano estratégico de £2,5 bilhões anunciado em 2023), Canadá (com forte pesquisa acadêmica histórica e apoio governamental contínuo através de agências como NSERC e programas como a National Quantum Strategy), Japão (com investimentos focados em computação, comunicação e materiais), Austrália (com centros de excelência e foco em qubits de silício), Coreia do Sul, Cingapura e Israel também possuem iniciativas nacionais significativas e investimentos crescentes para se posicionarem neste campo tecnológico emergente (Riedel et al., 2019; GOV.UK, 2023; Government of Canada, 2023; Japan Science and Technology Agency, 2022; CSIRO Australia, 2023).

Grandes empresas de tecnologia globais, incluindo Google (Google Quantum AI, 2023), IBM (IBM Research, 2023), Microsoft, Intel e Amazon Web Services (AWS), estão investindo bilhões de dólares no desenvolvimento de hardware quântico (usando diferentes tecnologias de qubits), software, algoritmos e plataformas de nuvem quântica (Gibney, 2019; Forbes, 2023). Essas plataformas de nuvem (ex: IBM Quantum Experience/Platform, Google Quantum AI Cloud, Amazon Braket, Microsoft Azure Quantum) desempenham um papel crucial na democratização do acesso a hardware quântico real (embora ainda experimental) para pesquisadores, estudantes e desenvolvedores em todo o mundo, permitindo-lhes experimentar, aprender e desenvolver aplicações sem a necessidade de construir seus próprios laboratórios quânticos (Chancellor, 2017; Wired, 2022). Essas empresas também publicam roadmaps ambiciosos, prometendo máquinas cada vez mais potentes e com correção de erros nos próximos anos, impulsionando a competição e o progresso (IBM Newsroom, 2023; Google I/O, 2023). Muitas dessas empresas possuem grupos de pesquisa dedicados especificamente a QML, explorando algoritmos e aplicações potenciais.

Paralelamente aos gigantes da tecnologia, um ecossistema vibrante e crescente de startups e empresas especializadas em computação quântica emergiu globalmente, muitas vezes originadas de pesquisas universitárias (Riedel et al., 2019; PitchBook, 2023; The Quantum Insider, 2023). Empresas como IonQ (focada em íons aprisionados, listada na NYSE), Rigetti Computing (supercondutores, também listada publicamente), Quantinuum (resultante da fusão da divisão quântica da Honeywell e Cambridge Quantum, focada em íons aprisionados e software/química quântica/QNLP), D-Wave Systems (pioneira em quantum annealing), PsiQuantum (buscando construir um computador fotônico tolerante a falhas com um milhão de qubits), Orca Computing (fotônica baseada em memória), Xanadu (fotônica e software, incluindo a popular biblioteca PennyLane para QML), ColdQuanta (agora Infleqtion, focada em átomos neutros), e muitas outras estão inovando com diferentes abordagens de hardware, software, ou focando em componentes específicos ou soluções para verticais da indústria. Várias startups, como Zapata AI, QC Ware, e a própria Multiverse Computing, têm um foco particular no desenvolvimento de software e algoritmos quânticos para aplicações em IA e otimização. Essas startups atraem investimentos significativos de

capital de risco, contribuindo para a diversidade tecnológica e a aceleração do desenvolvimento (PitchBook, 2023; TechCrunch, 2022).

A colaboração entre academia, governo e indústria é uma característica marcante do cenário quântico global, reconhecendo que os desafios são grandes demais para serem resolvidos isoladamente (Riedel et al., 2019; National Academies, 2019). Consórcios de pesquisa (como o Quantum Economic Development Consortium - QED-C nos EUA, ou projetos do Quantum Flagship na UE), parcerias público-privadas (PPPs), e projetos conjuntos entre universidades e empresas são comuns, visando acelerar o progresso em desafios fundamentais (como QEC ou materiais para qubits), desenvolver a força de trabalho e explorar aplicações setoriais específicas (IBM Research & Moderna, 2023; IonQ & Hyundai, 2025; QED-C). Projetos de pesquisa relevantes continuam a avançar o estado da arte, como demonstrado por trabalhos em simulações químicas mais precisas, algoritmos de otimização aprimorados, demonstrações de princípios de QEC, e desenvolvimento de software, *incluindo novas abordagens e benchmarks para QML* (Google Quantum AI, 2023; Sivak et al., 2023; Nature News, 2023; Lubinski et al., 2023). O desenvolvimento de software de código aberto (como Qiskit da IBM, Cirq do Google, Pennylane da Xanadu, Q# da Microsoft) e esforços de padronização (como no QED-C ou em comitês técnicos) também são vitais para construir uma comunidade global robusta, interoperável e colaborativa (Qiskit; Cirq; Pennylane; QED-C).

A intensa atividade global e os vultosos investimentos, juntamente com as implicações de segurança nacional (especialmente relacionadas à criptografia e IA), introduziram uma dimensão geopolítica significativa, frequentemente descrita como uma "corrida quântica" ou competição estratégica, particularmente entre os Estados Unidos e a China (Foreign Policy, 2021; The Economist, 2022; Financial Times, 2023). A liderança em tecnologias quânticas é vista como crucial para a futura competitividade econômica, a soberania tecnológica e a segurança nacional (Center for a New American Security, 2022; RAND Corporation, 2022). Isso levou a um aumento nos controles de exportação de tecnologias sensíveis, no escrutínio de investimentos estrangeiros em empresas quânticas, e em debates sobre "tecno-nacionalismo" versus colaboração científica internacional aberta (The Wall Street Journal, 2023; Science Business, 2022). Equilibrar a colaboração científica necessária para o progresso fundamental com as preocupações de segurança nacional é um desafio contínuo para os formuladores de políticas.

O financiamento privado, especialmente através de capital de risco (Venture Capital - VC), também desempenha um papel cada vez mais importante e visível no ecossistema quântico global (PitchBook, 2023; Quantum Computing Report, 2023; McKinsey & Company, 2021). Startups quânticas atraíram bilhões de dólares em investimentos nos últimos anos, um aumento dramático em relação à década anterior, impulsionando a inovação, a contratação de talentos e a comercialização de diferentes abordagens tecnológicas (TechCrunch, 2022; The Quantum Insider, 2023). Essa injeção de capital privado complementa os investimentos governamentais de longo prazo, acelerando o desenvolvimento de hardware, software e soluções quânticas. No entanto, também aumenta a pressão por resultados comerciais de curto prazo e levanta questões sobre avaliações potencialmente infladas e a sustentabilidade de longo prazo de algumas empresas, dada a incerteza sobre os prazos para a computação quântica verdadeiramente útil e lucrativa, *especialmente para aplicações complexas como QML* (Financial Times, 2022; The Economist, 2023).

Embora a maior parte do investimento e da atividade de pesquisa de ponta esteja concentrada na América do Norte, Europa e Ásia Oriental (especialmente China, Japão, Coreia do Sul), iniciativas quânticas também estão surgindo e ganhando força em outras regiões do mundo. Na América Latina, países como Brasil (com a Iniciativa Brasileira de Tecnologia Quântica e centros de pesquisa em universidades como UNICAMP e UFRJ), Chile, México e Colômbia estão começando a desenvolver programas de pesquisa, a formar redes de colaboração (muitas vezes em parceria com centros internacionais) e a investir na formação de talentos locais, buscando capacitar suas comunidades científicas e explorar nichos de aplicação relevantes para suas economias (Agência FAPESP, 2022; Ministério da Ciência, Tecnologia e Inovação - Brasil, 2023; Nature Index, 2021). Esforços semelhantes, embora talvez em estágio mais inicial, podem ser encontrados em países da África (como a África do Sul) e do Sudeste Asiático (além de Cingapura). Embora em escala menor que os grandes hubs globais, esses esforços são importantes para a disseminação global do conhecimento, a diversificação do ecossistema e a garantia de que os benefícios da tecnologia quântica possam, eventualmente, ser compartilhados de forma mais ampla (UNESCO, 2023).

Finalmente, à medida que a computação quântica avança, começam a surgir discussões sobre as implicações éticas e sociais mais amplas da tecnologia (Dowling; Milburn, 2003; Floridi et al., 2018; Responsible Quantum). Questões incluem o potencial impacto no emprego devido à automação de tarefas de otimização complexas, a necessidade de garantir acesso equitativo à tecnologia (evitando um "fosso quântico"), a governança de dados usados em QML (incluindo privacidade e viés), a transparência e explicabilidade de algoritmos quânticos (que podem ser ainda mais "caixas-pretas" que a IA clássica), e o potencial uso duplo da tecnologia (por exemplo, em aplicações militares ou de vigilância). Embora muitas dessas questões sejam de longo prazo, considerando o estágio atual da tecnologia, é importante iniciar discussões sobre desenvolvimento responsável e estruturas de governança antecipadamente para orientar o campo de forma ética e benéfica para a sociedade como um todo (World Economic Forum, 2022; IEEE Standards Association, 2023).

5. Regulação, Riscos Cibernéticos e Implicações Éticas

O desenvolvimento acelerado da computação quântica, com seu potencial transformador, inevitavelmente levanta questões complexas sobre regulação, segurança e ética (Jaeger; Sergienko, 2021). A natureza de "uso duplo" (dual-use) da tecnologia – com aplicações benéficas em medicina e materiais, mas também com potencial para quebrar sistemas de segurança e possivelmente para uso militar – torna a governança um desafio particularmente delicado (European Parliament, 2019; Cave; ÓhÉigeartaigh, 2019). Os formuladores de políticas, a indústria e a sociedade civil estão começando a lidar com como maximizar os benefícios da computação quântica enquanto mitigam seus riscos potenciais.

O risco cibernético mais imediato e amplamente discutido associado à computação quântica em larga escala é a ameaça à criptografia de chave pública (PKC), que sustenta a segurança de grande parte da nossa infraestrutura digital atual (Mosca, 2018; The New York Times, 2022). Como mencionado anteriormente, o algoritmo de Shor, executável em um computador quântico tolerante a falhas suficientemente grande, pode quebrar eficientemente os algoritmos RSA e ECC, tornando vulneráveis comunicações seguras na internet (HTTPS), transações financeiras, assinaturas digitais, e a segurança de muitas

redes governamentais e corporativas (Shor, 1997; Bernstein; Lange, 2017). Embora a construção de tal computador ainda esteja a anos (ou décadas) de distância, a ameaça é considerada séria o suficiente para exigir ação imediata devido ao risco de "Harvest Now, Decrypt Later" (HNDL) (Alagic et al., 2022; Schneier, 2021). Nesse cenário, adversários (estados-nação ou grupos criminosos sofisticados) podem estar coletando e armazenando grandes volumes de dados criptografados hoje, com a intenção de decifrá-los retrospectivamente assim que um computador quântico capaz estiver disponível, expondo segredos de longo prazo (Mosca, 2018; Wired, 2023).

A principal resposta global a essa ameaça criptográfica é o desenvolvimento e a padronização da Criptografia Pós-Quântica (PQC) – novos algoritmos criptográficos projetados para serem seguros contra ataques tanto de computadores clássicos quanto quânticos (Alagic et al., 2022; Bernstein; Buchmann; Dahmen, 2009). O Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA tem liderado um processo internacional de vários anos para selecionar e padronizar algoritmos PQC para criptografia de chave pública e assinaturas digitais (NIST, 2024). Em 2022, o NIST anunciou os primeiros quatro algoritmos selecionados para padronização (CRYSTALS-Kyber para estabelecimento de chaves e CRYSTALS-Dilithium, Falcon, SPHINCS+ para assinaturas), baseados principalmente em problemas matemáticos de reticulados (lattices) e funções de hash, que se acredita serem resistentes ao algoritmo de Shor (NIST News, 2022). O processo continua com a avaliação de algoritmos adicionais e a finalização dos padrões. Outros órgãos de padronização internacionais, como ISO e ETSI, também estão ativos na área (ETSI, 2023).

No entanto, a transição global para a PQC é um desafio monumental, muitas vezes comparado em escala à atualização do problema do ano 2000 (Y2K) ou à transição para o IPv6 (The Register, 2023; Forbes, 2024). Exigirá que organizações em todo o mundo identifiquem todos os sistemas que usam criptografia de chave pública vulnerável, selecionem e implementem os novos algoritmos PQC (que podem ter chaves maiores ou desempenho diferente dos atuais), testem a interoperabilidade e atualizem hardware e software em vasta escala (S&P Global, 2023). Isso envolverá custos significativos, complexidade técnica, gerenciamento de riscos e um longo período de transição, possivelmente uma década ou mais, durante o qual sistemas híbridos (combinando criptografia clássica e PQC) podem ser necessários (McKinsey & Company, 2022; CSA, 2021). A falta de "agilidade criptográfica" (a capacidade de atualizar facilmente algoritmos criptográficos) em muitos sistemas legados é uma preocupação adicional (ENISA, 2021). A regulamentação governamental pode desempenhar um papel em impulsionar essa transição; por exemplo, o governo dos EUA emitiu memorandos exigindo que as agências federais iniciem o inventário de sistemas e se preparem para a migração para PQC (The White House Memoranda, 2022).

Embora a quebra da PKC seja a ameaça mais premente, a computação quântica pode apresentar outros riscos cibernéticos no futuro. O algoritmo de Grover oferece uma aceleração quadrática (menos dramática que a exponencial de Shor, mas ainda significativa) para buscas não estruturadas (Grover, 1996). Isso poderia, em teoria, reduzir a segurança efetiva de algoritmos de criptografia simétrica (como AES) ao acelerar ataques de força bruta contra as chaves. A contramedida geralmente aceita é dobrar o tamanho das chaves simétricas (por exemplo, usar AES-256 em vez de AES-128) (Bernstein, 2010). Além disso, especula-se que algoritmos de QML poderiam ser usados

para fins maliciosos, como desenvolver ataques cibernéticos mais sofisticados, quebrar sistemas de detecção de intrusão baseados em IA clássica, ou criar deepfakes mais convincentes (Cave; ÓhÉigeartaigh, 2019; RAND Corporation, 2022). No entanto, essas ameaças são mais especulativas e dependem de avanços significativos tanto em computação quântica quanto em QML, e provavelmente só se materializariam em prazos mais longos.

O cenário regulatório para a computação quântica em si (além da criptografia) ainda está em seus estágios iniciais e é largamente dominado por estratégias nacionais de promoção e investimento, em vez de regulamentações restritivas (The Quantum Insider, 2023; OECD, 2023). No entanto, a natureza de uso duplo da tecnologia levou alguns países a implementar controles de exportação sobre hardware, software e conhecimentos técnicos relacionados à computação quântica, visando impedir a proliferação de capacidades avançadas para adversários geopolíticos (The Wall Street Journal, 2023; Bureau of Industry and Security - USA, 2022). Esses controles podem, por vezes, entrar em conflito com a necessidade de colaboração científica internacional aberta para acelerar o progresso (Science Business, 2022). A falta de um regime de governança internacional coeso para tecnologias quânticas é uma lacuna notável (Geneva Science and Diplomacy Anticipator - GESDA, 2023).

Organismos internacionais e fóruns multilaterais estão começando a discutir a necessidade de cooperação e possíveis normas de comportamento no domínio quântico, mas o progresso é lento, dificultado pelas tensões geopolíticas (United Nations Institute for Disarmament Research - UNIDIR, 2021). Iniciativas como os Princípios de Governança de Computação Quântica do Fórum Econômico Mundial buscam promover o desenvolvimento e uso responsável da tecnologia, abordando questões de ética, segurança, acesso equitativo e impacto social (World Economic Forum, 2022). Discussões sobre a ética da pesquisa quântica, incluindo o potencial para viés algorítmico em QML (semelhante à IA clássica) e a necessidade de transparência, também estão começando a emergir na comunidade acadêmica e em grupos de reflexão (Federici; Abel, 2023; Responsible Quantum).

Enquanto a computação quântica oferece promessas imensas, ela também apresenta riscos significativos, especialmente para a segurança cibernética global através da ameaça à criptografia atual. A resposta primária é a transição urgente para a criptografia pós-quântica (PQC), um esforço global complexo e de longo prazo. A regulação da própria tecnologia quântica ainda é incipiente, focada principalmente em promoção e controles de exportação relacionados à segurança nacional, com desafios significativos para a cooperação internacional e a governança ética. À medida que a tecnologia amadurece, um diálogo contínuo entre cientistas, indústria, formuladores de políticas e a sociedade será crucial para navegar neste cenário complexo e garantir que o desenvolvimento quântico ocorra de maneira segura, ética e benéfica.

Conclusão

A computação quântica representa, inequivocamente, uma fronteira tecnológica disruptiva, cujo potencial transcende a mera aceleração computacional para redefinir os paradigmas de diversas áreas, desde a ciência fundamental até a inteligência artificial e a segurança da informação. Contudo, a análise detalhada revela uma dualidade intrínseca: de um lado, promessas de avanços transformadores na medicina, materiais e otimização

complexa; de outro, uma tecnologia ainda em estágio embrionário (a era NISQ), permeada por desafios técnicos colossais como decoerência, escalabilidade e correção de erros, que impõem um sobering reality check sobre os cronogramas de aplicação prática em larga escala.

Do ponto de vista jurídico e regulatório, esta dualidade gera tensões e desafios únicos. A implicação mais imediata e talvez mais palpável reside na ameaça existencial à criptografia de chave pública contemporânea. O algoritmo de Shor não é uma especulação distante, mas uma consequência matemática da computação quântica tolerante a falhas. A urgência da migração para a Criptografia Pós-Quântica (PQC) transcende a mera atualização técnica; configura-se como um imperativo de segurança nacional e estabilidade econômica global. A inércia ou a demora na adoção da PQC podem gerar vulnerabilidades sistêmicas massivas, com potencial para litígios futuros baseados na violação do dever de diligência (duty of care) por parte de organizações que falharam em proteger dados sensíveis contra a ameaça quântica futura, especialmente considerando o risco de "Harvest Now, Decrypt Later". Propõe-se, assim, a necessidade de se discutir marcos regulatórios *proativos* que não apenas incentivem, mas potencialmente *exijam* um cronograma para a transição PQC em setores críticos (financeiro, saúde, infraestrutura), estabelecendo padrões mínimos de segurança "quantum-safe" e mecanismos de certificação. A cooperação internacional na padronização e implementação da PQC é vital, mas deve ser acompanhada por discussões sobre responsabilidade em caso de falhas ou atrasos na transição que resultem em danos.

No que tange à intersecção com a Inteligência Artificial (QML), o panorama é ainda mais complexo e especulativo. Enquanto vislumbramos o potencial de algoritmos quânticos para otimizar modelos de IA, descobrir padrões ocultos em dados complexos ou potencializar modelos generativos, devemos nos precaver contra o "hype" e reconhecer os desafios formidáveis, como o gargalo de I/O, os platôs áridos e a dificuldade em demonstrar vantagem prática sobre métodos clássicos altamente refinados. Juridicamente, a QML levanta questões críticas:

1. **Amplificação de vieses:** Poderiam algoritmos QML, ao explorar espaços de características mais vastos, inadvertidamente amplificar vieses presentes nos dados de treinamento de formas novas e mais difíceis de detectar? Isso exige uma reavaliação dos frameworks de auditoria de vieses para o contexto quântico.

2. **Opacidade Algorítmica:** Se a explicabilidade já é um desafio na IA clássica, a natureza contraintuitiva da mecânica quântica e a complexidade dos circuitos variacionais podem tornar os modelos QML ainda mais "caixas-pretas". Como atribuir responsabilidade por decisões ou predições de sistemas QML cuja lógica interna é fundamentalmente difícil de interpretar? Urge desenvolver novas abordagens para a "explicabilidade quântica" (Quantum Explainable AI - QXAI) e adaptar os princípios de devido processo algorítmico.

3. **Responsabilidade e Propriedade Intelectual:** Quem é responsável por danos causados por um sistema autônomo otimizado por QML? Como a legislação de propriedade intelectual deve tratar invenções ou descobertas feitas por sistemas híbridos quântico-clássicos de IA, onde a contribuição específica de cada componente é difícil de discernir? São necessárias novas reflexões sobre

personalidade jurídica algorítmica e regimes de titularidade em P&D assistida por quantum.

O cenário geopolítico, marcado por uma intensa "corrida quântica" e investimentos massivos, adiciona outra camada de complexidade legal. Os controles de exportação, embora justificados por preocupações de segurança nacional, arriscam fragmentar a comunidade científica global e retardar o progresso em desafios fundamentais que exigem colaboração. Propõe-se a exploração de mecanismos de governança internacional mais robustos, que vão além dos controles unilaterais, buscando equilibrar segurança com cooperação científica e, crucialmente, garantir um acesso mais equitativo à tecnologia, prevenindo um aprofundamento da clivagem digital global (o "quantum divide"). O acesso democratizado, facilitado pelas plataformas de nuvem, deve ser acompanhado por discussões sobre soberania de dados e jurisdição em ambientes de computação quântica distribuída.

Considerando a natureza nascente e a trajetória incerta da tecnologia, a regulação deve adotar uma abordagem adaptativa e antecipatória. Modelos como "sandboxes regulatórias" poderiam permitir a experimentação com aplicações quânticas em ambientes controlados, informando o desenvolvimento de normas futuras sem sufocar a inovação. É fundamental que a comunidade jurídica e de ética não espere a materialização dos riscos, mas se engaje *proativamente* com cientistas e engenheiros para co-desenvolver princípios de desenvolvimento e implementação responsável (Responsible Quantum Development). Isso inclui a incorporação de avaliações de impacto ético e social (Quantum Ethical and Social Impact Assessment - QESIA) desde as fases iniciais de pesquisa e desenvolvimento.

A computação quântica nos coloca diante de um futuro de possibilidades extraordinárias e riscos não triviais. Para nós, advogados e pesquisadores dedicados ao direito digital e à IA, o chamado é claro: precisamos ir além da compreensão superficial da tecnologia e mergulhar em suas implicações jurídicas, éticas e sociais. É imperativo fomentar um diálogo interdisciplinar robusto, desenvolver novas ferramentas conceituais e legais – talvez uma incipiente "jurisprudência quântica" – e trabalhar ativamente na construção de um arcabouço regulatório e de governança que possa guiar essa revolução tecnológica de forma segura, justa e benéfica para a humanidade. A complexidade não pode ser pretexto para a inação; pelo contrário, exige um esforço redobrado de antecipação, preparação e adaptação do Direito à iminente era quântica.

Referências

AARONSON, S. Quantum Computing Since Democritus. Cambridge: Cambridge University Press, 2013.

AARONSON, S. Read the fine print. *Nature Physics*, v. 11, p. 291–293, 2015.

ACCENTURE. Quantum computing for financial services. Report, 2021.

ACZEL, A. D. Entanglement: The Greatest Mystery in Physics. New York: Four Walls Eight Windows, 2002.

ADACHI, S. H.; HENDERSON, M. P. Application of Quantum Annealing to Training of Deep Neural Networks. *arXiv preprint arXiv:1510.06356*, 2015.

AGÊNCIA FAPESP. Brasil avança na criação de rede de comunicação quântica. 2022.

AIP - AMERICAN INSTITUTE OF PHYSICS. Funding for Quantum Information Science Continues Upward Trend. 2023.

ALAGIC, G. et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8413. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2022.

AWSALOM, D. D. et al. Development of Quantum Interconnects (QuICs) for Next-Generation Quantum Systems. *PRX Quantum*, v. 2, n. 1, p. 010302, 2019.

BABBUSH, R. et al. Focus on quantum simulation. *Nature Physics*, v. 17, p. 565, 2021.

BAUER, B.; BRAVYI, S.; MOTTA, M. Quantum algorithms for quantum chemistry and quantum materials science. *Chemical Reviews*, v. 120, n. 22, p. 12685-12717, 2020.

BBC NEWS. Quantum computing: Is the revolution finally here? 2022.

BCG - BOSTON CONSULTING GROUP. What Happens When 'If' Turns to 'When' in Quantum Computing? 2021.

BENEDETTI, M. et al. Parameterized quantum circuits as machine learning models. *Quantum Science and Technology*, v. 4, n. 4, p. 043001, 2019.

BERNSTEIN, D. J. Grover vs. McEliece. In: *International Workshop on Post-Quantum Cryptography*. Berlin, Heidelberg: Springer, 2010. p. 73-80. * (Grover vs Criptografia Simétrica/Pública)*. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-12929-2_6. Acesso em: 15 abr. 2025.

BERNSTEIN, D. J.; BUCHMANN, J.; DAHMEN, E. (Eds.). Post-quantum cryptography. Berlin: Springer, 2009. * (Livro PQC)*.

BERNSTEIN, D. J.; LANGE, T. Post-quantum cryptography. *Nature*, v. 549, n. 7671, p. 188-194, 2017. * (Ameaça Quântica à Criptografia)*. Disponível em: https://www.nature.com/articles/nature23461. Acesso em: 15 abr. 2025.

BHARTI, K. et al. Noisy intermediate-scale quantum (NISQ) algorithms. *Reviews of Modern Physics*, v. 94, n. 1, p. 015004, 2022.

BIAMONTE, J. et al. Quantum machine learning. *Nature*, v. 549, n. 7671, p. 195-202, 2017.

BOEHRINGER INGELHEIM. Boehringer Ingelheim and Google Quantum AI Partner to Accelerate Drug Discovery. Press Release, 2021.

BOTO, E. et al. Moving magnetoencephalography towards real-world applications with a wearable system. *Nature*, v. 555, n. 7698, p. 657-661, 2018.

BRUZEWICZ, C. D.; CHIAVERINI, J.; McCONNELL, R.; SAGE, J. M. Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, v. 6, n. 2, p. 021314, 2019.

BUREAU OF INDUSTRY AND SECURITY (BIS), U.S. Department of Commerce. Commerce Adds Four Quantum Computing Companies to the Entity List. Press Release, 2022. *

(Controles de Exportação)*. Disponível em: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3188-2022-11-28-bis-press-release-quantum-computing-additions-to-entity-list/file. Acesso em: 15 abr. 2025.

CAMBRIDGE QUANTUM. lambeq: An open-source Python library for quantum natural language processing. 2022.

CAMPBELL, E. T.; TERHAL, B. M.; VUILLOT, C. Roads towards fault-tolerant universal quantum computation. *Nature*, v. 549, n. 7671, p. 172-179, 2017.

CAO, Y. et al. Quantum chemistry in the age of quantum computing. *Chemical Reviews*, v. 119, n. 19, p. 10856-10915, 2019.

CAVE, S.; ÓHÉIGEARTAIGH, S. S. Bridging the gulf between quantum computing and ethical reasoning. *Philosophical Transactions of the Royal Society A*, v. 378, n. 2166, p. 20190434, 2019. * (Ética, Uso Duplo)*. Disponível em: https://royalsocietypublishing.org/doi/10.1098/rsta.2019.0434. Acesso em: 15 abr. 2025.

CENTER FOR A NEW AMERICAN SECURITY (CNAS). Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership. 2022.

CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET). China's Quantum Technology Landscape. 2021.

CEREZO, M. et al. Variational Quantum Algorithms. *Nature Reviews Physics*, v. 3, n. 9, p. 625-644, 2021.

CHANCELLOR, N. Modernizing quantum annealing using local searches. *New Journal of Physics*, v. 19, n. 2, p. 023024, 2017.

CHIA, N.-H.; LIN, H.-H.; WANG, C. Quantum-inspired algorithms for solving low-rank linear systems. *Journal of the ACM*, v. 67, n. 5, p. 1-33, 2020.

CHILDS, A. M.; KOTHARI, R.; SOMMA, R. D. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, v. 46, n. 6, p. 1920-1950, 2017.

CIRQ. Cirq Quantum Computing Framework. Google Research. Disponível em: https://quantumai.google/cirq. Acesso em: 15 abr. 2025.

CLOSE, F. The New Quantum Universe. Cambridge: Cambridge University Press, 2007.

CLOUD SECURITY ALLIANCE (CSA). Preparing Enterprises for the Quantum Computing Cybersecurity Threats. White Paper, 2021. * (Transição PQC)*. Disponível em: https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/. Acesso em: 15 abr. 2025.

COECKE, B.; MEICHANETZIDIS, K.; TOUMI, G. Quantum Natural Language Processing on Near-Term Quantum Computers. *arXiv preprint arXiv:2012.03755*, 2020.

CSIRO AUSTRALIA. Quantum Technologies. CSIRO Website. Acessado em 2023.

DALEY, A. J. et al. Practical quantum advantage in quantum simulation. *Nature*, v. 607, n. 7920, p. 667-676, 2022.

DALLAIRE-DEMERS, P.-L.; KILLORAN, N. Quantum generative adversarial networks. *Physical Review A*, v. 98, n. 1, p. 012324, 2018.

DAS, A.; CHAKRABARTI, B. K. Colloquium: Quantum annealing and analog quantum computation. *Reviews of Modern Physics*, v. 80, n. 3, p. 1061-1081, 2008.

D-WAVE SYSTEMS. Quantum Variational Autoencoder. 2024.

DEGEN, C. L.; REINHARD, F.; CAPPELLARO, P. Quantum sensing. *Reviews of Modern Physics*, v. 89, n. 3, p. 035002, 2017.

DELOITTE. Quantum computing and its potential impact on financial services. Report, 2022.

DEUTSCH, D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, v. 400, n. 1818, p. 97-117, 1985.

DEVITT, S. J.; MUNRO, W. J.; NEMOTO, K. Quantum error correction for beginners. *Reports on Progress in Physics*, v. 76, n. 7, p. 076001, 2013.

DOWLING, J. P.; MILBURN, G. J. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, v. 361, n. 1809, p. 1655-1674, 2003.

DUNJKO, V.; BRIEGEL, H. J. Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, v. 81, n. 7, p. 074001, 2018.

DUNJKO, V.; TAYLOR, J. M.; BRIEGEL, H. J. Quantum-enhanced machine learning. *Physical Review Letters*, v. 117, n. 13, p. 130501, 2016.

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. Post-Quantum Cryptography: Current state and quantum mitigation. Report, 2021. * (Agilidade Criptográfica)*. Disponível em: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. Acesso em: 15 abr. 2025.

ETSI - EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. Quantum-Safe Cryptography (QSC). ETSI Website. Acessado em 2023. * (Padronização PQC)*. Disponível em: https://www.etsi.org/technologies/quantum-safe-cryptography. Acesso em: 15 abr. 2025.

EUROPEAN COMMISSION. Quantum Technologies Flagship: Mid-term review report. 2021.

EUROPEAN PARLIAMENT. Quantum technologies and geopolitics. Briefing, 2019. * (Uso Duplo, Geopolítica)*. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640181/EPRS_BRI(2019)640181_EN.pdf. Acesso em: 15 abr. 2025.

FARHI, E.; GOLDSTONE, J.; GUTMANN, S. A Quantum Approximate Optimization Algorithm. *arXiv preprint arXiv:1411.4028*, 2014.

FARHI, E.; NEVEN, H. Classification with Quantum Neural Networks on Near Term Processors. *arXiv preprint arXiv:1802.06002*, 2018.

FEDERICI, C.; ABEL, M. Ethical considerations for quantum technology research and innovation. *AI & SOCIETY*, 2023. * (Ética)*. Disponível em: https://link.springer.com/article/10.1007/s00146-023-01636-3. Acesso em: 15 abr. 2025.

FEYNMAN, R. P. Simulating physics with computers. *International Journal of Theoretical Physics*, v. 21, n. 6/7, p. 467-488, 1982.

FINANCIAL POST. Denso, Toyota Tsusho, D-Wave optimize logistics with quantum computing. 2021.

FINANCIAL TIMES. Quantum computing: a bubble or the future of technology? 2022.

FINANCIAL TIMES. The quantum computing cold war. 2023.

FINGERHUTH, M. et al. Quantum Computing: A Primer for Drug Discovery. *Journal of Chemical Information and Modeling*, v. 58, n. 6, p. 1192-1204, 2018.

FLORIDI, L. et al. Ethical Framework for Quantum Computing. Report. Oxford: Digital Ethics Lab, University of Oxford, 2018.

FORBES. The Quantum Computing Talent Gap Is Real And Growing. 2022.

FORBES. Big Tech's Quantum Computing Arms Race Heats Up. 2023.

FORBES. The Y2Q Countdown: Preparing For The Post-Quantum Cryptography Transition. 2024. * (Transição PQC)*. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2024/...?h=.... (URL específica do artigo). Acesso em: 15 abr. 2025.

FOREIGN POLICY. The Quantum Computing Race Is Geopolitics by Other Means. 2021.

FOWLER, A. G. et al. Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, v. 86, n. 3, p. 032324, 2012.

FU, X. et al. A cryogenic interface for controlling many qubits. *arXiv preprint arXiv:1907.04446*, 2019.

GAMBETTA, J. M.; CHOW, J. M.; STEFFEN, M. Building logical qubits in a superconducting quantum computing system. *npj Quantum Information*, v. 3, n. 1, p. 2, 2017.

GAMBETTA, J. M. The Path Towards Useful Quantum Computing. IBM Research Blog, 2023.

GENEVA SCIENCE AND DIPLOMACY ANTICIPATOR (GESDA). Quantum computing governance: A new frontier for diplomacy. Report, 2023. * (Governança Internacional)*. Disponível em: https://gesda.global/quantum-computing-governance-a-new-frontier-for-diplomacy/. Acesso em: 15 abr. 2025.

GERMAN FEDERAL MINISTRY OF EDUCATION AND RESEARCH (BMBF). Quantum technologies – from basic research to market. 2023.

GIBNEY, E. Quantum gold rush: the private funding pouring into quantum computing. *Nature*, v. 574, p. 22-24, 2019.

GILDER, L. The Age of Entanglement: When Quantum Physics Was Reborn. New York: Alfred A. Knopf, 2008.

GIOVANNETTI, V.; LLOYD, S.; MACCONE, L. Quantum random access memory. *Physical Review Letters*, v. 100, n. 16, p. 160501, 2008.

GISIN, N. et al. Quantum cryptography. *Reviews of Modern Physics*, v. 74, n. 1, p. 145-195, 2002.

GOTTESMAN, D. An introduction to quantum error correction and fault-tolerant quantum computation. In: *Quantum Information Science and Its Contributions to Mathematics, Proceedings of Symposia in Applied Mathematics*, v. 68, p. 13-58. American Mathematical Society, 2010.

GOOGLE I/O. Quantum Computing Announcements. 2023.

GOOGLE QUANTUM AI. Quantum Supremacy Using a Programmable Superconducting Processor. *Nature*, v. 574, p. 505–510, 2019.

GOOGLE QUANTUM AI. Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, v. 614, p. 676–681, 2023.

GOOGLE QUANTUM AI. What is Quantum Computing? Google Quantum AI Website. Acessado em 2023/2024.

GOVERNMENT OF CANADA. National Quantum Strategy. 2023.

GOV.UK. National Quantum Technologies Programme. 2023.

GRANT, E. et al. An initialization strategy for addressing barren plateaus in parametrized quantum circuits. *Quantum*, v. 3, p. 214, 2019.

GROVER, L. K. A fast quantum mechanical algorithm for database search. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. New York: ACM, 1996.

GYONGYOSI, L.; IMRE, S.; NGUYEN, H. V. A Survey on Quantum Computing Technology. *Computer Science Review*, v. 31, p. 51-71, 2018.

HARROW, A. W.; HASSIDIM, A.; LLOYD, S. Quantum algorithm for linear systems of equations. *Physical Review Letters*, v. 103, n. 15, p. 150502, 2009.

HAUKE, P. et al. Perspectives of quantum annealing: Methods and implementations. *Reports on Progress in Physics*, v. 83, n. 5, p. 054401, 2020.

HAVLÍCEK, V. et al. Supervised learning with quantum-enhanced feature spaces. *Nature*, v. 567, n. 7747, p. 209-212, 2019.

HERMAN, D. et al. A Survey of Quantum Computing for Finance. *arXiv preprint arXiv:2302.01336*, 2023.

HESHAMI, K. et al. Quantum memories: emerging applications and recent advances. *Journal of Modern Optics*, v. 63, n. 20, p. 2005-2028, 2016.

HORODECKI, R. et al. Quantum entanglement. *Reviews of Modern Physics*, v. 81, n. 2, p. 865-942, 2009.

HUANG, H.-Y. et al. Quantum advantage in learning from experiments. *Science*, v. 376, n. 6598, p. 1182-1186, 2022.

HUANG, H.-Y. et al. Power of data in quantum machine learning. *Nature Communications*, v. 12, n. 1, p. 2631, 2021.

IBM NEWSROOM. IBM Unveils 1,121-Qubit Condor and 433-Qubit Osprey Processors, Updates Quantum Roadmap. 2023.

IBM RESEARCH. Quantum computing for chemistry and materials. IBM Research Website. Acessado em 2021.

IBM RESEARCH. IBM Quantum breaks the 100-qubit processor barrier. IBM News Room, 2022.

IBM RESEARCH. IBM Quantum. IBM Research Website. Acessado em 2023.

IBM RESEARCH & MODERNA. Moderna and IBM Announce Agreement to Explore Quantum Computing and AI for mRNA Medicine Development. IBM News Room, 2023.

IEEE STANDARDS ASSOCIATION. Quantum Computing Governance. Initiative Website. Acessado em 2023.

IONQ & HYUNDAI. IonQ and Hyundai Motor Company Partner To Use Quantum Computing To Improve Effectiveness of Next Generation Batteries. IonQ Press Release, 2025.

JAEGER, G. Entanglement, Information, and the Interpretation of Quantum Mechanics. Berlin: Springer, 2007.

JAEGER, G.; SERGIENKO, A. (Eds.). Quantum Metrology, Imaging, and Communication. Cham: Springer, 2021. *(Inclui discussões sobre segurança e ética)*.

JAPAN SCIENCE AND TECHNOLOGY AGENCY (JST). Quantum Technology Innovation Hubs. JST Website. Acessado em 2022.

JOHNSON, M. W. et al. Quantum annealing with manufactured spins. *Nature*, v. 473, n. 7346, p. 194-198, 2011.

KARTSAKLIS, D. et al. lambeq: A Python library for experimental quantum NLP. *arXiv preprint arXiv:2110.04236*, 2021.

KHOSHAMAN, A. et al. Quantum variational autoencoder. *Quantum Science and Technology*, v. 4, n. 1, p. 014001, 2018.

KRANTZ, P. et al. A quantum engineer's guide to superconducting qubits. *Applied Physics Reviews*, v. 6, n. 2, p. 021318, 2019.

LADD, T. D. et al. Quantum computers. *Nature*, v. 464, n. 7285, p. 45-53, 2010.

LAMATA, L. Basic protocols in quantum reinforcement learning with superconducting circuits. *Scientific Reports*, v. 7, p. 1609, 2017.

LAROSE, R. et al. Overview and Comparison of Gate Level Quantum Software Platforms. *Quantum*, v. 3, p. 130, 2019.

LLOYD, S.; MOHSENI, M.; REBENTROST, P. Quantum principal component analysis. *Nature Physics*, v. 10, n. 9, p. 631-633, 2014.

LLOYD, S.; WEEDBROOK, C. Quantum generative adversarial learning. *Physical Review Letters*, v. 121, n. 4, p. 040502, 2018.

LO, H.-K.; CURTY, M.; TAMAKI, K. Secure quantum key distribution. *Nature Photonics*, v. 8, n. 8, p. 595-604, 2014.

LORENZ, R. et al. QNLP in Practice: Running Compositional Models of Meaning on a Quantum Computer. *arXiv preprint arXiv:2102.12846*, 2021.

LUBINSKI, T. et al. Application-Oriented Performance Benchmarking for Quantum Computing. *arXiv preprint arXiv:2302.01973*, 2023.

LUDLOW, A. D.; BOYD, M. M.; YE, J. Optical atomic clocks. *Reviews of Modern Physics*, v. 87, n. 2, p. 637-701, 2015.

MARTINIS, J. M. Quantum supremacy using a programmable superconducting processor. *Philosophical Transactions of the Royal Society A*, v. 380, n. 2216, p. 20210048, 2021.

MCCLEAN, J. R. et al. Theory of variational hybrid quantum-classical algorithms. *New Journal of Physics*, v. 18, n. 2, p. 023023, 2016.

MCCLEAN, J. R. et al. Barren plateaus in quantum neural network training landscapes. *Nature Communications*, v. 9, n. 1, p. 4812, 2018.

MCKINSEY & COMPANY. Quantum computing's application potential. 2021.

MCKINSEY & COMPANY. The impending quantum computing transition. 2022. * (Transição PQC)*. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-impending-quantum-computing-transition. Acesso em: 15 abr. 2025.

MERCK KGaA. Merck KGaA, Darmstadt, Germany, Collaborates with Classiq and PASQAL on Quantum Computing Applications for Chemical Research. Press Release, 2022.

MICROSOFT RESEARCH BLOG. Developing the quantum software stack. 2022.

MILLS, D. et al. What is the Robust Quantum Advantage? *arXiv preprint arXiv:2111.01998*, 2021.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO (MCTI) - BRASIL. Iniciativa Brasileira de Tecnologia Quântica (IBrTQ). 2023.

MIT NEWS. Richard Feynman and The Connection Machine. 2011.

MIT TECHNOLOGY REVIEW. Let's get real about quantum computing's timeline. 2023.

MIT TECHNOLOGY REVIEW. Which quantum computer will win? 2022.

MITARAI, K. et al. Quantum circuit learning. *Physical Review A*, v. 98, n. 3, p. 032309, 2018.

MONTANARO, A. Quantum algorithms: an overview. *npj Quantum Information*, v. 2, p. 15023, 2016.

MOSCA, M. Cybersecurity in an era with quantum computers: will we be ready?. *IEEE Security & Privacy*, v. 16, n. 5, p. 14-17, 2018.

MULTIVERSE COMPUTING. Multiverse Computing Collaborates with Bosch to Optimize Spot Welding Process Using Quantum Computing. Press Release, 2023.

MURALIDHARAN, S. et al. Optimal architectures for long distance quantum communication. *Scientific Reports*, v. 6, p. 20463, 2016.

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press, 2019.

NATIONAL QUANTUM INITIATIVE ACT. Pub. L. 115-368. U.S. Congress, 2018.

NATURE. Quantum-computing pioneers win Nobel Prize in Physics. 2022.

NATURE. Quantum computational advantage using photons. *Nature*, v. 588, p. 260–264, 2020.

NATURE INDEX. Quantum science takes off in Latin America. 2021.

NATURE NEWS. Quantum error correction is finally here. 2023.

NATURE PHOTONICS. Quantum key distribution over 1,120 kilometres. 2021.

NAYAK, C. et al. Non-Abelian anyons and topological quantum computation. *Reviews of Modern Physics*, v. 80, n. 3, p. 1083-1159, 2008.

NEUKART, F. et al. Traffic flow optimization using a quantum annealer. *Frontiers in ICT*, v. 4, p. 29, 2017.

NIELSEN, M. A.; CHUANG, I. L. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press, 2010.

NIST. Post-Quantum Cryptography. National Institute of Standards and Technology Website. Atualizado em 2024.

NIST NEWS. NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. 2022. * (Seleção PQC)*. Disponível em: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Acesso em: 15 abr. 2025.

OECD - ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Quantum Technologies. OECD Policy Responses. 2023. * (Políticas Nacionais)*. Disponível em: https://www.oecd.org/sti/emerging-tech/quantum-technologies.htm. Acesso em: 15 abr. 2025.

OLLITRAULT, P. J.; KANDALA, A.; TAVERNELLI, I. Quantum computing for climate change. *arXiv preprint arXiv:2012.02222*, 2020.

ORIGIN QUANTUM. Origin Quantum releases new quantum computing cloud platform, makes progress on quantum chip production line. Global Times, 2024.

ORÚS, R.; MUGEL, S.; LIZASO, E. Quantum computing for finance: Overview and prospects. *Reviews in Physics*, v. 4, p. 100028, 2019.

PENNYLANE. PennyLane Quantum Computing Software. Xanadu. Disponível em: https://pennylane.ai/. Acesso em: 15 abr. 2025.

PERDOMO-ORTIZ, A. et al. Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers. *Quantum Science and Technology*, v. 3, n. 3, p. 030502, 2018.

PESAH, A. et al. Absence of barren plateaus in quantum convolutional neural networks. *Physical Review X*, v. 11, n. 4, p. 041011, 2021.

PETZOLD, C. Code: The Hidden Language of Computer Hardware and Software. Redmond, WA: Microsoft Press, 1999.

PHYSICS TODAY. Quantum Computing: A Physics Perspective. 2000.

PHYSICS WORLD. The challenge of quantum computing. 2019.

PIRANDOLA, S. et al. Advances in quantum sensing. *Nature Photonics*, v. 12, n. 12, p. 724-733, 2018.

PITCHBOOK. VC Investment In Quantum Computing Reaches New Heights. 2023.

POMPILI, M. et al. Realization of a multinode quantum network of remote solid-state qubits. *Science*, v. 372, n. 6539, p. 259-264, 2021.

PRAKASH, A. Quantum computation vs. communication complexity. *arXiv preprint arXiv:1405.5760*, 2014.

PRESKILL, J. Quantum Computing in the NISQ era and beyond. *Quantum*, v. 2, p. 79, 2018.

QED-C - QUANTUM ECONOMIC DEVELOPMENT CONSORTIUM. Website. Disponível em: https://quantumconsortium.org/. Acesso em: 15 abr. 2025.

QISKIT. Qiskit Quantum Computing Framework. IBM Quantum. Disponível em: https://qiskit.org/. Acesso em: 15 abr. 2025.

QUANTINUUM. Quantinuum researchers demonstrate cheminformatics application on H-Series quantum computer. Press Release, 2023.

QUANTUM COMPUTING REPORT. Quantum Computing Talent Shortage – A Growing Concern. 2023.

QUANTUM FLAGSHIP. About the Quantum Flagship. European Commission Website. Acessado em 2023/2024.

QURECA - QUANTUM RESOURCES & CAREERS. Quantum Education & Training. Website. Acessado em 2023.

RAND CORPORATION. The Military Applications of Quantum Computing. 2022.

REBENTROST, P.; MOHSENI, M.; LLOYD, S. Quantum support vector machine for big data classification. *Physical Review Letters*, v. 113, n. 13, p. 130503, 2014.

REIHER, M. et al. Elucidating reaction mechanisms on quantum computers. *Proceedings of the National Academy of Sciences*, v. 114, n. 29, p. 7555-7560, 2017.

RESPONSIBLE QUANTUM. Initiative Website. World Economic Forum. Disponível em: https://initiatives.weforum.org/responsible-use-of-technology/responsible-quantum. Acesso em: 15 abr. 2025.

REUTERS. France unveils 1.8 billion euro quantum technology plan. 2021.

RIEDEL, M. F. et al. The landscape of academic and industrial research in quantum technologies. *arXiv preprint arXiv:1909.01930*, 2019.

ROCHE. Roche partners with Cambridge Quantum to accelerate drug discovery using quantum computing. Roche News, 2023.

ROMERO, J. et al. Strategies for quantum computing molecular energies using the unitary coupled cluster ansatz. *arXiv preprint arXiv:1701.02691*, 2017.

S&P GLOBAL. The Quantum Computing Threat to Cybersecurity. 2023. * (Transição PQC)*. Disponível em: https://www.spglobal.com/marketintelligence/en/news-insights/research/the-quantum-computing-threat-to-cybersecurity. Acesso em: 15 abr. 2025.

SCARANI, V. et al. The security of practical quantum key distribution. *Reviews of Modern Physics*, v. 81, n. 3, p. 1301-1350, 2009.

SCHLOSSHAUER, M. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern Physics*, v. 76, n. 4, p. 1267-1305, 2005.

SCHLOSSHAUER, M. Decoherence and the Quantum-to-Classical Transition. Berlin: Springer, 2007.

SCHNEIER, B. Harvesting Attack Data. Schneier on Security Blog, 2021. * (HNDL)*. Disponível em: https://www.schneier.com/blog/archives/2021/09/harvesting-attack-data.html. Acesso em: 15 abr. 2025.

SCHULD, M. Quantum machine learning: challenges and opportunities. *Philosophical Transactions of the Royal Society A*, v. 380, n. 2216, p. 20210046, 2021.

SCHULD, M.; KILLORAN, N. Is quantum advantage the right goal for quantum machine learning? *PRX Quantum*, v. 3, n. 3, p. 030101, 2022.

SCHULD, M.; PETRUCCIONE, F. Supervised Learning with Quantum Computers. Cham: Springer, 2018.

SCHULD, M.; SINAYSKIY, I.; PETRUCCIONE, F. An introduction to quantum machine learning. *Contemporary Physics*, v. 56, n. 2, p. 172-185, 2015.

SCIENCE. Strong quantum computational advantage using a superconducting quantum processor. *Science*, v. 373, n. 6562, p. 1473-1477, 2021.

SCIENCE BUSINESS. Quantum research: Balancing national security with international collaboration. 2022.

SHOR, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, v. 26, n. 5, p. 1484-1509, 1997.

SIVAK, V. V. et al. Real-time quantum error correction beyond break-even. *Nature*, v. 616, p. 50-55, 2023.

TANG, E. A quantum-inspired classical algorithm for recommendation systems. In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. New York: ACM, 2019.

TECHCRUNCH. Quantum startups raised over $X billion in 2022. 2022.

TERHAL, B. M. Quantum error correction for quantum memories. *Reviews of Modern Physics*, v. 87, n. 2, p. 307-346, 2015.

THE DIPLOMAT. China's Quantum Computing Push. 2023.

THE ECONOMIST. The quantum computing hype cycle is peaking. 2023.

THE ECONOMIST. America and China are in a quantum tech race. 2022.

THE GUARDIAN. Quantum computers could break encryption within five years, scientists warn. 2024.

THE NEW YORK TIMES. The Race to Save Our Secrets From Quantum Hackers. 2022.

THE QUANTUM INSIDER. Global Quantum Computing Market Reports & Forecasts. 2023.

THE REGISTER. Migrating to post-quantum crypto will be the Y2K of our time. 2023. * (Transição PQC)*. Disponível em: https://www.theregister.com/2023/...?/pqc_migration_y2k/. (URL específica do artigo). Acesso em: 15 abr. 2025.

THE VERGE. Inside Google's quest for quantum supremacy. 2021.

THE WALL STREET JOURNAL. China's Quantum Leap. 2021.

THE WALL STREET JOURNAL. U.S. Tightens Curbs on Quantum Computing Exports to China. 2023.

THE WHITE HOUSE. FACT SHEET: Biden-Harris Administration Announces New Actions to Advance National Quantum Initiative. 2022.

THE WHITE HOUSE MEMORANDA. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). 2022. * (Regulação PQC EUA)*. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/. Acesso em: 15 abr. 2025.

TOMESH, T.; GOKHALE, P.; CHONG, F. T. Quantum benchmarking: From protocols to applications. *arXiv preprint arXiv:2203.08276*, 2022.

TOSHIBA. Quantum Key Distribution (QKD). Toshiba Website. Acessado em 2023.

UNESCO. Quantum technologies and sustainable development. 2023.

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR). Quantum Technologies and International Security. Report, 2021. * (Governança Internacional)*. Disponível em: https://unidir.org/publication/quantum-technologies-and-international-security. Acesso em: 15 abr. 2025.

VORONIN, G. L.; SEDYKH, D. A.; MASTIUKOVA, A. S. Quantum Computing for Green Energy Technologies. *Energies*, v. 16, n. 7, p. 3074, 2023.

WENDIN, G. Quantum information processing with superconducting circuits: a review. *Reports on Progress in Physics*, v. 80, n. 10, p. 106001, 2017.

WILSON, C. et al. Optimizing Variational Quantum Algorithms using Pontryagin's Minimum Principle. *arXiv preprint arXiv:2208.04808*, 2022.

WIRED. Quantum Computing Is Coming. What Can It Do? 2022.

WIRED. The WIRED Guide to Post-Quantum Cryptography. 2023.

WITTEK, P. Quantum Machine Learning: What Quantum Computing Means to Data Mining. Cambridge, MA: Academic Press, 2014.

WORLD ECONOMIC FORUM. Quantum Computing Governance Principles. 2022.

XINHUA NEWS AGENCY. China achieves quantum computational advantage. 2020.

ZAPATA COMPUTING. Zapata AI Announces Multi-Year Agreement with BMW Group to Optimize Automotive Production Lines. Press Release, 2023.

ZAPATA COMPUTING & VECTOR INSTITUTE. Generative AI meets quantum computing. 2024.

ZENG, W.; COECKE, B. Quantum algorithms for compositional natural language processing. *arXiv preprint arXiv:1608.01406*, 2016.

ZOUFAL, C.; LUCCHI, A.; WOERNER, S. Quantum Generative Adversarial Networks for learning and loading random distributions. *npj Quantum Information*, v. 5, n. 1, p. 103, 2019.

ZUREK, W. H. Decoherence, einselection, and the quantum origins of the classical. *Reviews of Modern Physics*, v. 75, n. 3, p. 715-775, 2003.