ENTRE O QUANTUM E A PRIVACIDADE: DESAFIOS DA PROTEÇÃO DE DADOS EM UM CENÁRIO PÓS-QUÂNTICO

Albert Costa[1]

Editor Responsável: Jéssica Soares
Revisão textual: Tailine Hijaz

RESUMO

A emergência da computação quântica desafia os fundamentos criptográficos da segurança da informação, da proteção de dados pessoais e da privacidade. O artigo examina em que medida capacidades computacionais quânticas podem comprometer pressupostos técnicos adotados por marcos regulatórios como a LGPD e o GDPR, especialmente quanto à segurança, anonimização e gestão de riscos. Sustenta-se que a transição pós-quântica não se limita à substituição de algoritmos criptográficos, mas constitui desafio jurídico-regulatório que exige revisão de critérios de reidentificação, governança baseada em risco, políticas de crypto-agility e atuação prospectiva das autoridades de proteção de dados. A pesquisa adota metodologia qualitativa, teórica, bibliográfica e documental, com análise de literatura técnico-científica, normas e documentos institucionais nacionais e internacionais. Os resultados indicam que a criptografia pós-quântica é a resposta prioritária para mitigar riscos quânticos, enquanto a Distribuição Quântica de Chaves deve ser tratada com cautela, dadas suas limitações

[1] Doutor em Informática pelo Programa de Pós-Graduação em Informática da Universidade Federal do Amazonas. Professor Associado do Instituto Federal do Amazonas - Campus Manaus Zona Leste. Email: albertfrancajosuacosta@gmail.com. https://orcid.org/0000-0001-7445-2331.

Recebido: 22/04/2026. Aprovado: 20/06/2026.

práticas e dependência de infraestrutura específica. Conclui-se que a preparação pós-quântica requer integração entre ciência, regulação e confiança pública para preservar a efetividade da proteção de dados e da privacidade.

Palavras-chave: Computação quântica; Criptografia pós-quântica; Proteção de dados; Privacidade; Governança digital.

BETWEEN QUANTUM COMPUTING AND PRIVACY: DATA PROTECTION CHALLENGES IN A POST-QUANTUM LANDSCAPE

ABSTRACT

The emergence of quantum computing challenges the cryptographic foundations underpinning information security, personal data protection, and privacy. This article examines the extent to which quantum computational capabilities may undermine the technical assumptions embedded in regulatory frameworks such as the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR), particularly regarding security, anonymization, and risk management. It argues that the post-quantum transition extends beyond the replacement of cryptographic algorithms, constituting a legal and regulatory challenge that requires revising re-identification criteria, adopting risk-based governance, implementing crypto-agility policies, and promoting proactive action by data protection authorities. The study employs a qualitative, theoretical, bibliographic, and documentary methodology, analyzing scientific literature, legal frameworks, and national and international institutional documents. The findings indicate that post-quantum cryptography represents the primary response to mitigating quantum risks, whereas Quantum Key Distribution should be approached cautiously due to its practical limitations and dependence on specialized infrastructure. The article concludes that preparing for the post-quantum era requires integrating science, regulation, and public trust to preserve the effectiveness of personal data protection and privacy in the face of emerging technological risks.

Keywords: Quantum computing; Post-quantum cryptography; Data protection; Privacy; Digital governance.

INTRODUÇÃO

A computação quântica vem sendo apontada como uma das tecnologias mais transformadoras da atualidade, com aplicações potenciais em áreas como ciência dos materiais, inteligência artificial e comunicações seguras. Entretanto, o mesmo potencial que a torna promissora também ameaça a base tecnológica que sustenta a segurança digital contemporânea. Algoritmos quânticos, como o de Shor (1997) e o de Grover (1996), demonstraram que sistemas criptográficos amplamente utilizados, a exemplo do RSA e das curvas elípticas, podem tornar-se vulneráveis diante da capacidade de processamento de computadores quânticos em larga escala (Nielsen, Chuang, 2010; Preskill, 2018).

Essa perspectiva levanta preocupações imediatas para a proteção de dados pessoais e para a privacidade. O risco conhecido como “harvest now, decrypt later”, caracterizado pela coleta atual de dados criptografados para decriptação futura, intensifica a vulnerabilidade de informações estratégicas e sensíveis. Relatórios técnicos de organismos internacionais já alertam para essa ameaça, destacando a necessidade de adoção de padrões criptográficos resistentes a ataques quânticos (OECD, 2025; ITU-T, 2020; World Economic Forum, 2022). Embora avanços como a Distribuição Quântica de Chaves (QKD) ofereçam alternativas promissoras (Pirandola et al., 2020), sua adoção em larga escala ainda enfrenta desafios práticos. Em paralelo, a criptografia pós-quântica (PQC) emerge como resposta mais imediata, com esforços coordenados de padronização liderados pelo NIST, pela União Europeia e por outras instituições internacionais (Chen et al., 2016; NIST, 2023).

O problema ultrapassa a esfera técnica e alcança a regulação da privacidade e da proteção de dados. Marcos normativos como o General Data Protection Regulation (GDPR) da União Europeia (2016) e a Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil (2018) foram concebidos sob pressupostos de segurança que podem não se sustentar em um cenário de supremacia quântica. Questões como a anonimização e o risco aceitável de reidentificação ganham novos contornos, exigindo que autoridades reguladoras, como a ANPD, incorporem essa agenda emergente em seus planos estratégicos (ANPD, 2022a; ANPD, 2022b; ANPD, 2022c; ANPD, 2023).

No plano internacional, diferentes atores vêm elaborando diretrizes para lidar com os riscos e oportunidades da era pós-quântica. A Comissão Europeia (2020) apresentou uma agenda estratégica de pesquisa em tecnologias quânticas, a OECD (2025) publicou um guia de políticas públicas destacando riscos e oportunidades da computação quântica, a União Internacional de Telecomunicações (ITU-T, 2020) definiu padrões técnicos para redes de comunicação baseadas em QKD, e o World Economic Forum (2022) estabeleceu princípios de governança que ressaltam transparência, responsabilidade e proteção de direitos fundamentais. Esses documentos refletem a urgência de alinhar políticas públicas, inovação tecnológica e direitos fundamentais em uma agenda global.

À luz desse contexto, o problema de pesquisa que orienta este artigo pode ser formulado nos seguintes termos: em que medida a computação quântica compromete os pressupostos técnicos de segurança que sustentam a proteção de dados pessoais e quais respostas jurídicas, regulatórias e institucionais devem ser mobilizadas para a transição pós-quântica? A tese defendida é que a preparação para esse cenário não se limita à adoção de novos algoritmos criptográficos, mas exige uma abordagem integrada de governança, baseada em risco, que articule criptografia pós-quântica, crypto-agility, revisão dos critérios de anonimização e reidentificação, responsabilidade dos agentes de tratamento e atuação prospectiva das autoridades reguladoras.

Metodologia

Este artigo adota abordagem qualitativa, de natureza teórica, bibliográfica e documental, com o objetivo analítico-exploratório. A pesquisa foi desenvolvida a partir da revisão de literatura técnico-científica sobre computação quântica, criptografia pós-quântica, segurança da informação, governança digital, proteção de dados pessoais e privacidade, bem como da análise de documentos normativos, regulatórios e estratégicos produzidos por organismos nacionais e internacionais.

O corpus documental foi delimitado por critérios de pertinência temática, autoridade institucional, atualidade e relevância regulatória. Foram priorizados: a) estudos técnico-científicos de referência sobre algoritmos quânticos, criptografia pós-quântica e Distribuição Quântica de Chaves; b) documentos institucionais de organismos com atuação

reconhecida em segurança, padronização ou governança tecnológica, como NIST, Comissão Europeia, ITU-T, OECD, World Economic Forum, NCSC e ANPD; e c) marcos normativos centrais para a discussão, especialmente a LGPD e o GDPR. Foram excluídas fontes jornalísticas, promocionais ou meramente opinativas, salvo quando indispensáveis para contextualização, hipótese em que não foram utilizadas como fundamento principal da análise.

O procedimento analítico foi estruturado em três eixos: a) identificação dos principais riscos que a computação quântica impõe à infraestrutura criptográfica contemporânea; b) exame dos impactos desses riscos sobre institutos jurídicos relacionados à proteção de dados e à privacidade, com destaque para segurança, anonimização, pseudonimização e reidentificação; e c) análise de estratégias regulatórias e de governança voltadas à transição para um cenário pós-quântico.

A opção metodológica por revisão bibliográfica e documental justifica-se pelo caráter emergente e interdisciplinar do tema, que demanda articulação entre literatura técnica, marcos regulatórios e documentos estratégicos de políticas públicas. Não se trata, portanto, de estudo empírico ou experimental, mas de investigação teórico-analítica orientada à compreensão dos desafios jurídicos e institucionais decorrentes da transição tecnológica para a era pós-quântica.

1. FUNDAMENTOS DAS TECNOLOGIAS QUÂNTICAS

A computação quântica representa uma mudança paradigmática em relação à computação clássica, ao introduzir conceitos baseados na mecânica quântica que permitem resolver determinados problemas de forma mais eficiente do que sistemas convencionais. Seu núcleo é o qubit, unidade básica de informação que, diferentemente do bit clássico, pode assumir simultaneamente os estados de 0 e 1 por meio da superposição. Essa característica possibilita que problemas de alta complexidade sejam processados por modelos computacionais próprios, abrindo caminho para marcos de vantagem quântica em tarefas específicas, sem que isso implique afirmar uma superação definitiva e generalizada dos supercomputadores clássicos em todos os domínios (Nielsen, Chuang, 2010; Preskill, 2018).

Outro fenômeno central é o emaranhamento quântico, correlação entre partículas que mantém seus estados interdependentes, mesmo quando separadas por grandes distâncias. Essa propriedade desafia a intuição clássica e abre caminhos para aplicações em comunicações seguras, sobretudo na Distribuição Quântica de Chaves (QKD). Nesse modelo, a transmissão de chaves por meios quânticos pode permitir a detecção de tentativas de interceptação, desde que observadas determinadas premissas físicas, operacionais e de implementação. Todavia, a QKD não deve ser descrita como tecnologia absolutamente inviolável, pois sua segurança depende do desenho do sistema, da autenticação das partes comunicantes, da qualidade dos equipamentos e da integração com mecanismos criptográficos complementares. Assim, a QKD deve ser compreendida como alternativa relevante para contextos específicos, especialmente infraestruturas críticas, mas não como solução geral ou autossuficiente para os desafios da segurança digital pós-quântica (Pirandola et al., 2020; ITU-T, 2020; NCSC, 2025a).

A força disruptiva da computação quântica é evidenciada também pelos algoritmos já propostos. O algoritmo de Shor (1997) demonstra que é possível fatorar grandes números inteiros em tempo polinomial, quebrando a segurança de sistemas criptográficos assimétricos como RSA e ECC, fundamentais para transações bancárias, autenticação de identidades e proteção de comunicações. O algoritmo de Grover (1996), por sua vez, apresenta aceleração quadrática em buscas não estruturadas, reduzindo significativamente o tempo necessário para localizar informações em grandes bases de dados e afetando protocolos baseados em criptografia simétrica. Esses desenvolvimentos levaram a comunidade internacional a reconhecer que a infraestrutura criptográfica atual poderá se tornar obsoleta em um futuro pós-quântico (European Commission, 2020).

Apesar de seu potencial, a tecnologia encontra-se na chamada era NISQ (Noisy Intermediate-Scale Quantum), marcada por dispositivos com dezenas a centenas de qubits, ainda instáveis e suscetíveis a erros (Preskill, 2018). Esses equipamentos não são totalmente funcionais para aplicações em larga escala, mas já permitem explorar casos práticos em áreas como otimização, simulação de novos materiais e protocolos experimentais de segurança. A European Commission (2020) considera essa fase um período preparatório, no qual políticas de transição devem ser planejadas para que

governos, empresas e instituições acadêmicas estejam prontos quando surgirem computadores tolerantes a falhas. De forma semelhante, o World Economic Forum (2022) enfatiza a necessidade de adotar políticas de crypto-agility, ou seja, mecanismos que permitam atualizar sistemas rapidamente para novos padrões criptográficos resistentes a ataques quânticos.

A compreensão desses fundamentos é indispensável para analisar impactos na proteção de dados e na privacidade. A literatura e os relatórios estratégicos vêm alertando para o risco denominado “harvest now, decrypt later”, em que dados criptografados coletados hoje podem ser armazenados e decriptados futuramente com o advento de computadores quânticos avançados (ITU-T, 2020; OECD, 2025). Esse risco é particularmente relevante para informações sensíveis ou de longa duração, como dados de saúde, registros financeiros ou dados governamentais estratégicos.

No Brasil, embora a computação quântica ainda não esteja no centro da regulação de dados pessoais, documentos técnicos da então Autoridade Nacional de Proteção de Dados, atual Agência Nacional de Proteção de Dados (ANPD, 2022a; 2022b; 2022c) já evidenciam a importância de adotar uma abordagem baseada em risco para o tratamento de dados, especialmente no que diz respeito à definição do Risco de Reidentificação Aceitável (RRA). Ainda que os estudos publicados se concentrem em técnicas de anonimização e modelos computacionais atuais, suas recomendações sinalizam a necessidade de incorporar evoluções tecnológicas, incluindo os potenciais avanços quânticos, ao desenho regulatório. Isso demonstra que a discussão sobre os fundamentos da computação quântica não deve ser restrita ao campo da física e da engenharia, mas precisa integrar a governança de dados e a proteção da privacidade.

Dessa forma, os fundamentos das tecnologias quânticas revelam uma dupla face: de um lado, oferecem novas oportunidades em simulação, comunicação e inovação científica; de outro, colocam em xeque a segurança digital que sustenta direitos fundamentais e a confiança em sistemas sociais e econômicos. Antecipar esses riscos é condição necessária para que a transição à era pós-quântica ocorra de forma segura, equilibrando inovação tecnológica, proteção de dados e salvaguarda da privacidade.

2. CRIPTOGRAFIA PÓS-QUÂNTICA E A CORRIDA PELA SEGURANÇA DIGITAL

O desenvolvimento da computação quântica representa um marco não apenas científico, mas também de segurança da informação, pois ameaça diretamente a robustez da infraestrutura criptográfica que sustenta a sociedade digital. A criptografia moderna baseia-se, em grande parte, em problemas matemáticos considerados intratáveis por computadores clássicos, como a fatoração de grandes números inteiros e o cálculo do logaritmo discreto. Entretanto, o algoritmo de Shor (1997) demonstrou que computadores quânticos tolerantes a falhas poderão resolver esses problemas em tempo polinomial, comprometendo sistemas amplamente utilizados, como o RSA, o Diffie-Hellman e a criptografia de curvas elípticas (ECC). De forma complementar, o algoritmo de Grover (1996) afeta protocolos simétricos, reduzindo o nível de segurança efetivo de chaves ao proporcionar aceleração quadrática em buscas. Essa combinação coloca em risco tanto a confidencialidade quanto a integridade de informações pessoais, corporativas e governamentais (Nielsen, Chuang, 2010; Preskill, 2018).

Esse cenário impulsionou o surgimento da criptografia pós-quântica (Post-Quantum Cryptography – PQC), campo dedicado ao desenvolvimento de algoritmos resistentes a ataques quânticos, mas passíveis de implementação em infraestruturas digitais já existentes. Diferentemente da QKD, que depende de novos dispositivos físicos, a PQC busca soluções matemáticas robustas para proteger dados contra adversários equipados com computadores quânticos. Diversos esquemas têm sido propostos, com destaque para aqueles baseados em reticulados (lattices), códigos corretores de erros, funções hash e multivariáveis polinomiais (Bernstein, Buchmann, Dahmen, 2009).

A relevância da PQC foi reconhecida por organismos internacionais de padronização. O National Institute of Standards and Technology (NIST) iniciou, em 2016, um processo internacional de seleção de algoritmos pós-quânticos, que resultou na publicação, em 2024, dos primeiros padrões federais: FIPS 203, relativo ao mecanismo de encapsulamento de chaves baseado em reticulados; FIPS 204, referente a assinaturas digitais baseadas em reticulados; e FIPS 205, relativo a assinaturas digitais baseadas em funções hash. Essa evolução desloca o debate da mera seleção de candidatos para a fase de planejamento e execução da migração criptográfica. O desafio, entretanto, não se limita

à adoção formal dos algoritmos, mas envolve inventário de ativos criptográficos, interoperabilidade, atualização de sistemas legados, gestão de fornecedores e políticas de crypto-agility, isto é, a capacidade de organizações substituírem ou atualizarem mecanismos criptográficos sem comprometer a continuidade de suas operações (NIST, 2024a; NIST, 2024b; NIST, 2024c; World Economic Forum, 2022).

O risco do chamado “harvest now, decrypt later” amplia a urgência dessa transição. Dados sensíveis, como registros médicos, informações financeiras e segredos industriais, podem ser coletados e armazenados hoje, aguardando o advento de computadores quânticos capazes de decriptá-los futuramente. Esse fenômeno ameaça diretamente a proteção de dados pessoais e estratégicos, sobretudo em países que ainda não possuem estratégias nacionais claras para a era pós-quântica. Relatórios técnicos, como o da União Internacional de Telecomunicações (ITU-T, 2020), alertam que a Distribuição Quântica de Chaves (QKD) e os mecanismos de criptografia pós-quântica devem ser vistos como complementares, constituindo camadas de defesa contra as vulnerabilidades futuras (ITU-T, 2020).

No Brasil, embora a discussão sobre computação quântica ainda seja incipiente no campo regulatório, documentos da então Autoridade Nacional de Proteção de Dados, atual Agência Nacional de Proteção de Dados (ANPD) oferecem uma base importante para reflexão. Estudos técnicos sobre anonimização de dados (ANPD, 2022a; 2022b; 2022c) destacam a necessidade de adotar modelos baseados em risco e de revisar continuamente o Risco de Reidentificação Aceitável (RRA) diante de novas capacidades tecnológicas. Embora não tratem explicitamente de computação quântica, esses documentos reforçam a premissa de que a evolução das ameaças demanda constante atualização dos instrumentos técnicos e regulatórios. Nesse sentido, a incorporação da PQC como estratégia de segurança deve ser compreendida como extensão natural da agenda de proteção de dados, integrando-se a legislações como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Europeu (GDPR).

A corrida pela segurança digital, portanto, envolve uma mobilização global que extrapola a dimensão técnica. Requer investimentos em pesquisa e inovação, coordenação regulatória internacional e políticas públicas que promovam soberania tecnológica e

cooperação. Relatórios estratégicos, como o da Comissão Europeia (2020), enfatizam que países e organizações que retardarem a adoção da PQC correm o risco de se tornar altamente vulneráveis, tanto no plano econômico quanto no da segurança nacional. Essa perspectiva se alinha à visão da ANPD (2023), que em seu Plano Estratégico destaca a importância de acompanhar tecnologias emergentes como parte de sua missão institucional.

Assim, a criptografia pós-quântica deve ser compreendida não apenas como uma resposta técnica ao desafio imposto pela computação quântica, mas como um componente central de uma nova governança digital. Sua implementação antecipada representa uma oportunidade de alinhar inovação e proteção de direitos fundamentais, garantindo que a transição para a era pós-quântica ocorra de maneira segura, inclusiva e sustentável.

3. PROTEÇÃO DE DADOS E PRIVACIDADE EM UM CENÁRIO PÓS-QUÂNTICO

A proteção de dados pessoais e a preservação da privacidade constituem pilares centrais da sociedade digital contemporânea. Marcos regulatórios como o *General Data Protection Regulation* (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD) foram concebidos sob a premissa de que instrumentos técnicos de segurança, em especial a criptografia e a anonimização, seriam capazes de mitigar riscos de acesso não autorizado e de reidentificação (União Europeia, 2016; Brasil, 2018). No entanto, a evolução da computação quântica desafia esses pressupostos e exige uma reavaliação profunda dos fundamentos técnicos que sustentam a legislação vigente.

Antes de examinar os impactos da computação quântica, é necessário distinguir privacidade e proteção de dados pessoais. A privacidade corresponde a uma esfera mais ampla de autonomia, reserva, controle contextual e não interferência indevida na vida individual. A proteção de dados pessoais, por sua vez, constitui regime jurídico-instrumental voltado a disciplinar operações de tratamento, atribuir responsabilidades, garantir direitos aos titulares e impor deveres de segurança, transparência e prestação de contas aos agentes de tratamento. No cenário pós-quântico, essas duas dimensões são afetadas de modo interdependente: a fragilização de mecanismos técnicos de confidencialidade pode

comprometer não apenas a segurança do tratamento, mas também a capacidade dos titulares de controlar os usos presentes e futuros de suas informações.

A criptografia, embora não seja o único mecanismo de proteção, ocupa posição central na segurança do tratamento de dados pessoais. Algoritmos quânticos, como o de Shor, podem comprometer sistemas assimétricos amplamente utilizados, enquanto o algoritmo de Grover reduz a margem de segurança efetiva de determinados esquemas simétricos. Essa fragilidade repercute diretamente sobre deveres jurídicos de segurança e prevenção previstos na LGPD e no GDPR. O impacto, contudo, não deve ser descrito como eliminação automática da anonimização ou da criptografia, mas como alteração relevante do juízo sobre o estado da arte, o custo de ataque, a probabilidade de reidentificação e a adequação das medidas técnicas adotadas em determinado contexto.

O debate sobre a anonimização e o Risco de Reidentificação Aceitável (RRA) ganha relevância nesse cenário. Estudos técnicos elaborados pela então Autoridade Nacional de Proteção de Dados, atual Agência Nacional de Proteção de Dados (ANPD, 2022a; 2022b; 2022c), destacam que a anonimização deve ser entendida como processo dinâmico e contextual, cuja eficácia depende do estado da arte tecnológica, dos meios razoavelmente disponíveis e do risco concreto de reidentificação. A progressão para um ambiente pós-quântico pode alterar os limiares de risco considerados aceitáveis, especialmente em bases sensíveis, de longa duração ou combináveis com outras fontes de informação. Nesses casos, dados considerados anonimizados em determinado momento podem demandar reavaliação periódica, sem que isso implique afirmar, de modo abstrato, que todos os modelos atuais de anonimização se tornarão automaticamente obsoletos.

O risco descrito como “harvest now, decrypt later” adiciona uma dimensão temporal ao problema regulatório. Dados cifrados hoje podem ser coletados, armazenados e explorados futuramente, quando capacidades computacionais mais avançadas tornarem insuficientes os mecanismos de proteção originalmente empregados. Essa possibilidade afeta a interpretação dos princípios da segurança, da prevenção, da finalidade e da responsabilização, pois obriga agentes de tratamento a considerarem não apenas o risco presente, mas também a durabilidade esperada da confidencialidade dos dados. Em tratamentos envolvendo dados sensíveis, bases governamentais, informações financeiras

ou registros de saúde, a avaliação de impacto e a governança de segurança devem incorporar cenários de obsolescência criptográfica.

Outro ponto de tensão refere-se à responsabilidade dos agentes de tratamento. Se medidas de segurança consideradas adequadas no presente se tornarem ineficazes em razão da obsolescência criptográfica, será necessário discutir em que medida controladores e operadores poderão ser responsabilizados por incidentes futuros. Esse debate aproxima-se da ideia de responsabilidade prospectiva, já discutida por autores como Hildebrandt (2015) e Floridi (2014), que defendem a necessidade de um olhar jurídico voltado para riscos tecnológicos em constante evolução.

No plano internacional, o European Data Protection Board (EDPB, 2021) já publicou recomendações defendendo a adoção de medidas suplementares para garantir a equivalência da proteção de dados em transferências internacionais. O World Economic Forum (2022) reforça essa perspectiva ao propor a adoção de políticas de crypto-agility, permitindo que sistemas possam ser atualizados rapidamente frente a novas ameaças. A European Commission (2020) também destaca que a proteção de dados deve incorporar desde já estratégias específicas para a era pós-quântica, reconhecendo que a inação pode gerar vulnerabilidades sistêmicas.

No Brasil, a ANPD já reconhece em seu Plano Estratégico 2023–2025 a importância de monitorar tecnologias emergentes como parte de sua atuação regulatória (ANPD, 2023). A incorporação explícita do tema quântico à agenda da Agência poderá fortalecer a resiliência normativa nacional e garantir maior alinhamento com os debates internacionais. Além disso, iniciativas como os Radares Tecnológicos sobre inteligência artificial generativa e neurotecnologias (ANPD, 2024; ANPD, 2025) indicam que já existe espaço institucional para incluir a computação quântica em relatórios de monitoramento, promovendo uma abordagem de governança digital alinhada a tendências globais.

Portanto, a proteção de dados em um cenário pós-quântico não pode ser vista como mera continuidade das práticas atuais. A obsolescência das técnicas de segurança atuais exige uma redefinição conceitual, regulatória e tecnológica. A integração entre criptografia pós-quântica, gestão de riscos baseada em evidências e políticas públicas de proteção da privacidade será determinante para garantir que o avanço da ciência não

comprometa a efetividade da LGPD, do GDPR e de outros marcos regulatórios. Preparar-se para esse cenário significa reconhecer que a privacidade, enquanto direito fundamental, dependerá cada vez mais da capacidade institucional e técnica de antecipar riscos e de promover soluções que conciliem inovação e proteção.

4. GOVERNANÇA GLOBAL E ESTRATÉGIAS REGULATÓRIAS

A consolidação da computação quântica impõe desafios que transcendem fronteiras nacionais e requerem respostas coordenadas no plano internacional. A vulnerabilidade das atuais infraestruturas criptográficas não se restringe a um país ou setor específico, mas ameaça a confiança global em sistemas financeiros, de comunicação e de proteção de dados. Nesse contexto, a governança da era pós-quântica emerge como uma prioridade estratégica, envolvendo organismos multilaterais, governos e autoridades nacionais de proteção de dados.

A Comissão Europeia (2020) tem desempenhado papel central na antecipação dos impactos da computação quântica, elaborando uma Agenda Estratégica de Pesquisa em Tecnologias Quânticas que estabelece prioridades científicas, industriais e regulatórias. Essa iniciativa reconhece que a supremacia quântica pode comprometer a resiliência da infraestrutura digital europeia, o que exige investimentos em pesquisa aplicada, programas de formação e políticas de incentivo à adoção de criptografia pós-quântica.

Em linha semelhante, a OECD (2025) publicou o Quantum Technologies: Policy Primer, documento que analisa os impactos da computação quântica sobre a economia, a segurança digital e a governança da informação. O relatório destaca que a transição para padrões pós-quânticos deve ser compreendida não apenas como desafio técnico, mas também como processo de grande relevância socioeconômica. A adoção desigual de mecanismos de proteção pode ampliar assimetrias globais, favorecendo países com maior capacidade de investimento em pesquisa e infraestrutura tecnológica, ao passo que economias em desenvolvimento permanecem mais vulneráveis a riscos de segurança e dependentes de soluções externas.

A União Internacional de Telecomunicações (ITU-T, 2020) também tem contribuído para o debate ao identificar as implicações da computação quântica para a segurança de redes e comunicações. Suas recomendações enfatizam a necessidade de desenvolver

padrões de interoperabilidade e mecanismos de cooperação entre países, especialmente no que se refere à implementação de tecnologias como a Distribuição Quântica de Chaves (QKD).

O World Economic Forum (2022), por sua vez, propôs os Princípios de Governança da Computação Quântica, que incluem recomendações voltadas à transparência, responsabilidade e proteção de direitos fundamentais. O relatório destaca que a governança da era pós-quântica não pode ser conduzida apenas pela indústria ou pela comunidade científica, mas deve incluir participação de autoridades regulatórias, sociedade civil e setor privado em um modelo multistakeholder.

No Brasil, a Agência Nacional de Proteção de Dados (ANPD) já possui instrumentos que podem ser mobilizados para o debate sobre tecnologias quânticas. O Plano Estratégico 2023–2025 menciona a necessidade de monitoramento de tecnologias emergentes e de sua integração à agenda regulatória (ANPD, 2023). Além disso, os Estudos Técnicos sobre Anonimização (ANPD, 2022a; 2022b; 2022c) e os Radares Tecnológicos sobre inteligência artificial generativa e neurotecnologias (ANPD, 2024; 2025) revelam uma preocupação crescente da Agência em alinhar regulação de dados à evolução científica. Embora não tratem diretamente da computação quântica, esses documentos oferecem uma base metodológica e institucional para que o tema seja incorporado futuramente às prioridades nacionais.

A governança global da computação quântica exige, portanto, mais do que a padronização técnica de algoritmos pós-quânticos. Trata-se de criar estruturas jurídicas e políticas capazes de antecipar riscos, promover a cooperação internacional e assegurar que os benefícios da inovação sejam distribuídos de forma equitativa. A integração entre relatórios internacionais, como os da Comissão Europeia, da OECD, da ITU-T e do World Economic Forum, e iniciativas nacionais como as da ANPD, representa caminho fundamental para construir um ecossistema regulatório resiliente.

Assim, a governança da era pós-quântica deve ser entendida como um processo global e colaborativo, no qual a proteção de dados e a privacidade ocupam posição estratégica. A articulação entre políticas públicas, padrões técnicos e marcos jurídicos será determinante para assegurar que o avanço das tecnologias quânticas não fragilize direitos

fundamentais, mas contribua para o fortalecimento da confiança digital e da soberania tecnológica.

5. AGENDA PROPOSITIVA

A transição para a era pós-quântica impõe a necessidade de uma agenda que combine soluções técnicas, instrumentos regulatórios e estratégias de pesquisa. Não se trata apenas de responder a um desafio tecnológico, mas de estabelecer um marco de governança que garanta a resiliência da infraestrutura digital e a proteção de direitos fundamentais em longo prazo.

No campo técnico, a prioridade é a implementação da criptografia pós-quântica (PQC). A experiência internacional, especialmente o processo conduzido pelo National Institute of Standards and Technology (NIST), demonstra que a discussão já avançou da seleção de candidatos para a etapa de migração aos primeiros padrões publicados em 2024, com destaque para FIPS 203, FIPS 204 e FIPS 205. Além disso, a literatura destaca a importância da crypto-agility, isto é, a capacidade de migrar rapidamente entre algoritmos à medida que novas vulnerabilidades ou padrões forem identificados (World Economic Forum, 2022). Paralelamente, soluções baseadas em Distribuição Quântica de Chaves (QKD) devem ser avaliadas com cautela e em contextos específicos, sobretudo na proteção de infraestruturas críticas, pois sua adoção em larga escala depende de condições técnicas, econômicas e operacionais próprias (Pirandola et al., 2020; ITU-T, 2020; NCSC, 2025a).

No campo regulatório, torna-se imprescindível revisar e adaptar os marcos jurídicos de proteção de dados. O GDPR e a LGPD foram construídos em um contexto em que a criptografia clássica era considerada segura. A chegada da computação quântica exige reinterpretação de conceitos como anonimização e pseudonimização, além da redefinição do parâmetro de Risco de Reidentificação Aceitável (RRA). Nesse aspecto, os estudos técnicos da ANPD (2022a; 2022b; 2022c) já oferecem um caminho ao adotar a gestão de risco como abordagem central, mas é necessário incorporar de forma explícita o cenário quântico como vetor de fragilidade. Também é essencial promover mecanismos de responsabilização adaptados, evitando lacunas jurídicas que poderiam eximir controladores e operadores de responderem por incidentes decorrentes da obsolescência tecnológica.

No plano da governança internacional, recomenda-se o fortalecimento da cooperação entre organismos multilaterais. Documentos estratégicos da Comissão Europeia (2020), da OECD (2025), da ITU-T (2020) e do World Economic Forum (2022) evidenciam a urgência de um esforço coordenado para harmonizar padrões técnicos, evitar fragmentação regulatória e reduzir assimetrias entre países desenvolvidos e em desenvolvimento. Nesse contexto, países como o Brasil devem buscar alinhar-se a essas iniciativas, utilizando a atuação da ANPD como eixo de integração regional e global.

Outro elemento central dessa agenda é o estímulo à pesquisa científica e à formação de recursos humanos. Investimentos em ciência básica e aplicada são determinantes para que os países não se tornem dependentes de tecnologias importadas, perpetuando vulnerabilidades estratégicas. A capacitação de profissionais especializados em criptografia pós-quântica, física quântica aplicada e governança digital deve ser prioridade em políticas nacionais de inovação e educação.

Por fim, a agenda deve considerar a dimensão social da confiança digital. A percepção de que dados coletados hoje poderão ser violados futuramente pelo advento da computação quântica pode comprometer a legitimidade de instituições públicas e privadas, enfraquecendo o próprio exercício da cidadania digital. Garantir transparência, comunicação clara e participação multissetorial no debate é, portanto, tão importante quanto os avanços técnicos e regulatórios.

Dessa forma, a agenda propositiva para o cenário pós-quântico deve articular quatro eixos complementares: adoção técnica da PQC e, em contextos específicos, avaliação da QKD; adaptação regulatória dos marcos de proteção de dados; fortalecimento da cooperação internacional; e promoção da pesquisa e da confiança social. Somente a integração desses eixos permitirá enfrentar os desafios e aproveitar as oportunidades trazidas pela computação quântica de maneira segura, equitativa e sustentável.

CONCLUSÃO

A emergência da computação quântica representa um dos maiores desafios contemporâneos para a proteção de dados e a privacidade. Ao mesmo tempo em que inaugura possibilidades inéditas de inovação científica e tecnológica, essa revolução

ameaça os fundamentos criptográficos que sustentam a sociedade digital. A análise realizada neste trabalho mostrou que algoritmos quânticos, como os de Shor (1997) e Grover (1996), têm o potencial de tornar obsoletos os sistemas de segurança atualmente utilizados, criando vulnerabilidades que impactam diretamente direitos fundamentais.

Nesse contexto, a criptografia pós-quântica (PQC) surge como resposta prioritária. A publicação, pelo NIST, dos primeiros padrões federais de criptografia pós-quântica em 2024 indica que a transição deixou de ser apenas prospectiva e passou a exigir planejamento concreto de migração, inventário de ativos criptográficos e políticas de crypto-agility. Paralelamente, tecnologias como a Distribuição Quântica de Chaves (QKD) mostram-se promissoras para contextos específicos, especialmente infraestruturas críticas, ainda que sua implementação em larga escala permaneça desafiadora e não dispense mecanismos complementares de autenticação e governança de segurança (Pirandola et al., 2020; ITU-T, 2020; NCSC, 2025a).

No plano regulatório, torna-se evidente que legislações como a LGPD (Brasil, 2018) e o GDPR (União Europeia, 2016) precisarão ser reinterpretadas à luz do cenário quântico. Conceitos como anonimização, pseudonimização e risco de reidentificação aceitável exigem atualização constante, uma vez que sua validade depende do estado da arte das tecnologias de processamento e análise de dados. Os estudos técnicos da ANPD (2022a; 2022b; 2022c) já sinalizam a importância de uma abordagem baseada em risco, mas será necessário incorporar explicitamente a perspectiva quântica a essas análises.

A governança global assume papel estratégico. Relatórios da Comissão Europeia (2020), da OECD (2025), da ITU-T (2020) e do World Economic Forum (2022) demonstram que a preparação para a era pós-quântica requer esforços coordenados, evitando fragmentações regulatórias e ampliando a cooperação internacional. Países que retardarem a adoção de padrões pós-quânticos poderão ver-se em desvantagem não apenas tecnológica, mas também econômica e geopolítica. Nesse cenário, a ANPD pode desempenhar papel relevante, articulando a realidade brasileira a essas iniciativas internacionais e fortalecendo a soberania digital do país.

Por fim, este trabalho evidenciou que a proteção de dados em um cenário pós-quântico não é apenas uma questão técnica. Trata-se de um desafio jurídico, político e

social, que exige a integração entre ciência, regulação e confiança pública. A construção de uma agenda propositiva baseada em inovação tecnológica, adaptação normativa, cooperação internacional e promoção da confiança social é essencial para assegurar que os avanços da computação quântica não comprometam a privacidade, mas sim contribuam para fortalecer os direitos fundamentais na sociedade da informação.

REFERÊNCIAS

ALAGIC, Gorjan; ALPERIN-SHERIFF, Jacob; APON, Daniel; COOPER, David; DANG, Quynh; LIU, Yi-Kai; MILLER, Carl; MOODY, Dustin; PERALTA, Rene; PERLNER, Ray; ROBINSON, Angela; SMITH-TONE, Daniel. Status report on the second round of the NIST post-quantum cryptography standardization process. **National Institute of Standards and Technology**, 2020. Disponível em: https://doi.org/10.6028/NIST.IR.8309. Acesso em: 25 jun. 2026.

ANPD. **Estudo técnico sobre anonimização de dados na LGPD**: Uma visão de processo baseado em risco e técnicas computacionais. Agência Nacional de Proteção de Dados, 2022a.

ANPD. **Estudo de casos sobre anonimização de dados na LGPD**. Agência Nacional de Proteção de Dados, 2022b.

ANPD. **Estudo técnico sobre anonimização de dados na LGPD:** Análise jurídica. Agência Nacional de Proteção de Dados, 2022c.

ANPD. **Plano Estratégico 2023–2025**. Agência Nacional de Proteção de Dados, 2023.

ANPD. **Radar Tecnológico – Inteligência Artificial Generativa**. Agência Nacional de Proteção de Dados, 2024.

ANPD. **Radar Tecnológico – Neurotecnologias**. Agência Nacional de Proteção de Dados, 2025.

BERNSTEIN, Daniel J.; BUCHMANN, Johannes; DAHMEN, Erik. (Eds.). **Post-quantum cryptography**. Springer, 2009.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**: Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, 2018.

CHEN, Lily; JORDAN, Stephen; LIU, Yi-Kai; MOODY, Dustin; PERALTA, Rene; PERLNER, Ray; SMITH-TONE, Daniel. **Report on post-quantum cryptography**, 2016. National Institute of Standards and Technology. Disponível em: https://doi.org/10.6028/NIST.IR.8105. Acesso em: 25 jun. 2026.

EUROPEAN COMMISSION. **Quantum technologies flagship**: Strategic research agenda. Publications Office of the European Union, 2020. Disponível em: https://doi.org/10.2777/06090. Acesso em: 25 jun. 2026.

EUROPEAN DATA PROTECTION BOARD. **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**, 2021. Disponível em: https://edpb.europa.eu. Acesso em: 25 jun. 2026.

FLORIDI, L. **The fourth revolution**: How the infosphere is reshaping human reality. Oxford University Press, 2014.

GROVER, L. K. A fast quantum mechanical algorithm for database search. In: **Proceedings of the twenty-eighth annual ACM symposium on theory of computing,** pp. 212–219. ACM, 1996. Disponível em: https://doi.org/10.1145/237814.237866. Acesso em: 25 jun. 2026.

HILDEBRANDT, M. **Smart technologies and the end(s) of law:** Novel entanglements of law and technology. Edward Elgar, 2015.

ITU-T. **Overview on networks supporting quantum key distribution** (Recommendation Y.3800). International Telecommunication Union, 2020. Disponível em: https://www.itu.int/rec/T-REC-Y.3800-202002-I. Acesso em: 25 jun. 2026.

NIELSEN, Michael A; CHUANG, Isaac L. **Quantum computation and quantum information** (10th anniversary ed.). Cambridge University Press, 2010.

NIST. **Post-quantum cryptography standardization**: Round 3 report. National Institute of Standards and Technology, 2023. Disponível em: https://doi.org/10.6028/NIST.IR.8413. Acesso em: 25 jun. 2026.

NIST. **FIPS 203:** Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology, 2024a. Disponível em: https://doi.org/10.6028/NIST.FIPS.203. Acesso em: 25 jun. 2026.

NIST. **FIPS 204**: Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology, 2024b. Disponível em: https://doi.org/10.6028/NIST.FIPS.204. Acesso em: 25 jun. 2026.

NIST. **FIPS 205**: Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology, 2024c. Disponível em: https://doi.org/10.6028/NIST.FIPS.205. Acesso em: 25 jun. 2026.

NCSC. **Quantum networking technologies**. National Cyber Security Centre, 2025a. Disponível em: https://www.ncsc.gov.uk/paper/quantum-networking-technologies. Acesso em: 25 jun. 2026.

NCSC. **Timelines for migration to post-quantum cryptography**. National Cyber Security Centre, 2025b. Disponível em: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines. Acesso em: 25 jun. 2026.

OECD. **Quantum technologies**: Policy primer. OECD Publishing, 2025. Disponível em: https://doi.org/10.1787/9789264656717-en. Acesso em: 25 jun. 2026.

PIRANDOLA, S.; ANDERSEN, U. L.; BANCHI, L.; BERTA, M.; BUNANDAR, D.; COLBECK, R.; ENGLUND, D.; GEHRING, T.; LUPO, C.; OTTAVIANI, C.; PEREIRA, J. L.; RAZAVI, M.; SHAMSUL SHAARI, J.; TOMAMICHEL, M.; USENKO, V.; VALLONE, G.; VILLORESI, P.; WALLDEN, P. Advances in quantum cryptography. **Advances in Optics and Photonics**, v. 12, n. 4, pp. 1012–1236, 2020. Disponível em: https://doi.org/10.1364/AOP.361502. Acesso em: 25 jun. 2026.

PRESKILL, J. Quantum computing in the NISQ era and beyond. **Quantum**, v. 2, n. 79, 2018. Disponível em: https://doi.org/10.22331/q-2018-08-06-79. Acesso em: 25 jun. 2026.

SHOR, Peter W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM Journal on Computing**, v. 26, n. 5, pp. 1484–1509, 1997. Disponível em: https://doi.org/10.1137/S0097539795293172. Acesso em: 25 jun. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016: Regulamento Geral sobre a Proteção de Dados (GDPR), 2016. Jornal Oficial da União Europeia.

WORLD ECONOMIC FORUM. **Quantum computing governance principles**, 2022. World Economic Forum. Disponível em: https://www.weforum.org. Acesso em: 25 jun. 2026.