Computação quântica e o seu potencial para a quebra de cifras criptográficas: uma análise técnico-jurídica

Quantum computing and its potential for breaking cryptographic ciphers: A technical-legal analysis

10.29073/j2.v9i1.1139

Recebido: 12 de março de 2026.
Aprovado: 04 de abril de 2026.
Publicado: 08 de abril de 2026.

Autor/a 1 (Correspondente): João Sousa, ESTG-IPP, jsampaiodesousa@gmail.com.
Autor/a 2: Rui Sousa, ESTG-IPP, ruisousa3@hotmail.com.

Resumo

A Computação Quântica constitui um paradigma tecnológico de forte potencial disruptivo, alicerçado em princípios como a superposição e o entrelaçamento, capazes de ultrapassar determinados limites da computação clássica. Não obstante, esta capacidade introduz vulnerabilidades significativas no domínio da cibersegurança, colocando em causa os fundamentos da criptografia contemporânea. Algoritmos quânticos como os de Shor e Grover podem comprometer sistemas criptográficos assimétricos, designadamente RSA e ECC, e reduzir a margem efetiva de segurança da criptografia simétrica.

O presente artigo analisa os fundamentos da computação quântica e o seu impacto sobre infraestruturas digitais e de comunicação. Em face deste cenário, examina-se a transição para a Criptografia Pós-Quântica (PQC) enquanto resposta técnica e normativa. Em paralelo, procede-se a uma análise jurídico-regulatória centrada na responsabilidade das organizações à luz do Regulamento Geral sobre a Proteção de Dados (RGPD), do Regulamento DORA e da Diretiva NIS2.

Conclui-se que a manutenção de mecanismos criptográficos desatualizados pode configurar não apenas uma fragilidade técnica, mas também um risco jurídico material. O artigo formula recomendações práticas e normativas orientadas para a resiliência digital num contexto de risco emergente.

Palavras-Chave: Cibersegurança; Computação Quântica; Conformidade Regulatória; Criptografia Pós-Quântica; Direito Digital.

Abstract

Quantum Computing constitutes a technologically disruptive paradigm, grounded in principles such as superposition and entanglement, which make it possible to surpass certain limits of classical computing. Nevertheless, this capability introduces significant vulnerabilities in the field of cybersecurity, calling into question the foundations of contemporary cryptography. Quantum algorithms such as Shor's and Grover's may compromise asymmetric cryptographic systems, namely RSA and ECC, and reduce the effective security margin of symmetric cryptography.

This article analyses the foundations of quantum computing and its impact on digital and communication infrastructures. In light of this scenario, the transition to PQC is examined as a technical and normative response. In parallel, a legal and regulatory analysis is conducted, focusing on organizational liability in light of the GDPR, the DORA Regulation, and the NIS2 Directive.

It is concluded that the continued use of outdated cryptographic mechanisms may constitute not only a technical weakness, but also a material legal risk. The article puts forward practical and normative recommendations aimed at digital resilience in an emerging risk context.

Keywords: Cybersecurity; Digital Law; Post-Quantum Cryptography; Quantum Computing; Regulatory Compliance.

1. Introdução

A Computação Quântica afirma-se como uma das áreas mais promissoras e transformadoras da ciência contemporânea. Assente na física quântica, permite representar e processar informação de modo substancialmente distinto da computação clássica. As suas bases modernas remontam à década de 1980, quando Richard Feynman salientou a dificuldade de simular sistemas quânticos com computadores clássicos, sugerindo a necessidade de máquinas assentes nesses mesmos princípios (Feynman, 1982). Posteriormente, David Deutsch formalizou a ideia de um computador quântico universal (Deutsch, 1985).

A principal rutura teórica com relevância para a criptografia ocorreu na década de 1990, quando Peter Shor apresentou um algoritmo capaz de fatorar inteiros e resolver logaritmos discretos em tempo polinomial (Shor, 1994), seguido do algoritmo de Grover, concebido para acelerar pesquisas em bases de dados não estruturadas (Grover, 1996). Com marcos experimentais como a demonstração de supremacia quântica pela Google (Arute et al., 2019), a viabilidade prática desta tecnologia tornou-se mais tangível. Todavia, a sua evolução projeta impactos profundos sobre a segurança da informação, colocando em risco infraestruturas criptográficas essenciais à economia digital e à proteção da privacidade.

O presente trabalho visa analisar o impacto da computação quântica na cibersegurança, avaliando a vulnerabilidade dos sistemas criptográficos atuais e discutindo as respostas oferecidas pela PQC. Em paralelo, integra-se um enquadramento jurídico centrado na eventual violação de deveres de segurança, diligência e resiliência, à luz do RGPD (Regulamento [UE] 2016/679, 2016), do Regulamento DORA (Regulamento [UE] 2022/2554, 2022) e da Diretiva NIS2 (Diretiva [UE] 2022/2555, 2022). O artigo estrutura-se em sete secções, da fundamentação técnica às estratégias de mitigação e às implicações jurídico-éticas, culminando em recomendações práticas para uma transição gradual e juridicamente conformada.

2. Fundamentos e Paradigmas da Computação Quântica

A computação quântica assenta num paradigma interdisciplinar enraizado na mecânica quântica. O elemento central deste modelo é o *qubit*, ou bit quântico. Ao contrário do bit clássico, que assume de forma exclusiva os valores 0 ou 1, o *qubit* pode existir numa combinação linear de estados, o que lhe confere propriedades de superposição e paralelismo computacional.

Em acréscimo, o entrelaçamento (*entanglement*) permite que múltiplos qubits fiquem correlacionados de forma não clássica, tornando o sistema conjunto sensível à medição e à manipulação do estado das suas partes (Nielsen & Chuang, 2010). O processamento de informação é efetuado por portas lógicas quânticas, como Hadamard e CNOT, que exploram interferência para amplificar amplitudes associadas às soluções corretas e atenuar as incorretas.

Não obstante a sua relevância teórica, a tecnologia enfrenta o desafio da de coerência, isto é, a perda rápida das propriedades quânticas devido à interação com o ambiente. Tal exige infraestruturas altamente controladas e códigos sofisticados de correção de erros. Assim, os computadores quânticos não tendem a substituir os clássicos em tarefas correntes, mas antes a funcionar como aceleradores para classes específicas de problemas, entre as quais se inclui a quebra de certos esquemas criptográficos.

3. Ameaças Algorítmicas à Criptografia Atual

A robustez da criptografia moderna depende da dificuldade computacional de certos problemas matemáticos para máquinas clássicas. A chegada de algoritmos quânticos altera este paradigma, afetando tanto cifras assimétricas como simétricas.

O impacto mais severo decorre do algoritmo de Shor, que demonstrou a capacidade de fatorar grandes inteiros e calcular logaritmos discretos em tempo polinomial (Shor, 1994). Este avanço compromete diretamente a segurança de algoritmos assimétricos amplamente utilizados, nomeadamente RSA e ECC. Protocolos de comunicação segura na Internet, como TLS, SSH e VPNs, que dependem destas primitivas para troca de chaves e assinaturas digitais, podem tornar-se inadequados num cenário em que exista um computador quântico suficientemente robusto (Mosca, 2018).

Figura 1: Fluxo simplificado do algoritmo de Shor aplicado à fatoração.

Por outro lado, o algoritmo de Grover oferece uma aceleração quadrática para pesquisa em bases de dados não estruturadas (Grover, 1996). Aplicado à criptografia simétrica, como o AES, tal traduz-se numa redução relevante da segurança efetiva contra-ataques de força bruta. Um algoritmo simétrico com chave de 128 bits passa a oferecer uma margem equivalente substancialmente menor, razão pela qual a adoção de chaves mais longas, como AES-256, se torna prudente.

4. Avaliação de Risco e Cibersegurança nas Infraestruturas

Atualmente, não existe evidência pública de um computador quântico criptograficamente relevante capaz de comprometer esquemas de cifragem assimétrica de elevado comprimento de chave em tempo útil. Ainda assim, a ameaça já se materializa no presente através de estratégias como *Store Now, Decrypt Later* (ENISA, 2021). Atores maliciosos podem intercetar e armazenar tráfego cifrado hoje, com o objetivo de o decifrar futuramente, quando a capacidade quântica se revelar suficiente.

Neste contexto, coloca-se uma questão jurídica particularmente relevante: a determinação do momento da violação de dados pessoais. Caso a interceção ocorra no presente, mas a decifração apenas no futuro, poderá defender-se uma conceção de violação diferida, com implicações ao nível dos deveres de notificação previstos nos artigos 33.º e 34.º do RGPD.

Os setores mais vulneráveis incluem finanças, saúde, infraestruturas críticas e defesa, em virtude da exigência de confidencialidade prolongada e da relevância operacional dos dados em causa. A eventual erosão da confiança em assinaturas digitais e mecanismos de não repúdio poderá produzir efeitos sistémicos na economia digital.

Para gerir este risco, as organizações devem migrar de uma postura reativa para um paradigma de *crypto-agility*, isto é, uma capacidade contínua de inventariar ativos criptográficos, avaliar dependências e substituir algoritmos sem disrupção do serviço. Esta preparação é hoje amplamente recomendada por entidades europeias e internacionais dedicadas à cibersegurança (ENISA, 2021).

5. Estratégias de Mitigação e Criptografia Pós-Quântica

A resposta técnica ao desafio quântico divide-se, em linhas gerais, entre soluções baseadas em *hardware* e soluções baseadas em *software*. No primeiro grupo, destaca-se a Distribuição Quântica de Chaves (QKD), que recorre a propriedades da física quântica para detectar tentativas de interceção. Apesar do interesse científico, enfrenta limitações de escalabilidade e de infraestrutura (Pirandola et al., 2020).

A solução com maior aplicabilidade generalizada é a PQC. Esta assenta em problemas matemáticos considerados resistentes a ataques clássicos e quânticos, incluindo abordagens baseadas em redes euclidianas e funções *hash* (Bernstein et al., 2009). O processo global de padronização é liderado pelo *National Institute of Standards and*

Technology (NIST), que já publicou padrões federais para algoritmos pós-quânticos, incluindo os ML-KEM, ML-DSA e SLH-DSA (NIST, 2024).

Durante a transição, uma estratégia híbrida pode ser especialmente útil, combinando mecanismos clássicos e pós-quânticos para reduzir riscos de migração e preservar compatibilidade com sistemas existentes (ENISA, 2021). Esta abordagem permite reforçar a robustez operacional enquanto os novos padrões são integrados de forma faseada.

6. Enquadramento Ético e Jurídico

A transição para a era pós-quântica insere-se num contexto normativo em que a segurança da informação deixou de ser apenas uma boa prática técnica para assumir a natureza de um verdadeiro dever jurídico. Num cenário em que a confidencialidade, a integridade e a autenticidade da informação podem ser fragilizadas por avanços na computação quântica, as organizações passam a ter de demonstrar não apenas que utilizam mecanismos criptográficos, mas também que estes permanecem adequados ao estado da arte, ao risco concreto e à natureza dos dados tratados.

Do ponto de vista ético, a questão central reside na preservação da confiança digital. A sociedade contemporânea depende de sistemas de autenticação, assinatura eletrónica, troca segura de chaves e encriptação para assegurar comunicações privadas, transações económicas, serviços públicos e relações contratuais. Se tais mecanismos se tornarem obsoletos sem substituição atempada, poderá verificar-se uma erosão da confiança nas infraestruturas digitais, com impacto direto sobre direitos fundamentais, em especial o direito à proteção de dados pessoais, à vida privada e à autodeterminação informativa. Neste sentido, a preparação para a ameaça quântica não se esgota numa preocupação meramente técnica, mas traduz uma exigência ética de responsabilidade, prudência e proteção intergeracional.

No plano jurídico, o artigo 32.º do RGPD impõe ao responsável pelo tratamento e ao subcontratante a adoção de medidas técnicas e organizativas adequadas para assegurar um nível de segurança compatível com os riscos apresentados pelo tratamento, tendo em conta, entre outros fatores, a cifragem, a pseudonimização, a capacidade de assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência permanentes dos sistemas e serviços, bem como a capacidade de restaurar a disponibilidade e o acesso aos dados em tempo útil em caso de incidente físico ou técnico. Este dever é dinâmico e deve ser interpretado à luz do estado da arte, o que significa que a adoção continuada de algoritmos já conhecidos como vulneráveis, sem planeamento de migração, pode fragilizar a demonstração de conformidade.

A ameaça quântica introduz, além disso, uma dimensão particularmente relevante para a aplicação do princípio da prevenção. Mesmo na ausência de um computador quântico criptograficamente relevante no presente, a possibilidade de recolha e armazenamento de dados cifrados para decifração futura torna plausível um risco diferido, mas juridicamente significativo (ENISA, 2021). Em termos práticos, isto significa que a proteção insuficiente de hoje pode converter-se numa violação consumada amanhã, especialmente quando estejam em causa dados com vida útil longa, como informação médica, financeira, contratual, governamental ou estratégica. A avaliação de risco deixa, assim, de poder limitar-se ao momento imediato do tratamento e passa a incorporar horizontes temporais alargados.

A Diretiva NIS2 reforça este enquadramento ao impor obrigações mais exigentes de gestão de riscos de cibersegurança, incluindo medidas de governação, prevenção, deteção, resposta e recuperação (CNCS, 2024). A lógica subjacente é a de que a cibersegurança deixou de ser um tema meramente operacional e passou a integrar a governação das organizações, incluindo a cadeia de abastecimento digital e a dependência de terceiros tecnológicos. A segurança criptográfica, neste contexto, não é um elemento acessório: é uma componente estrutural da resiliência organizacional.

No setor financeiro, o Regulamento DORA acentua ainda mais esta exigência, ao instituir um modelo robusto de resiliência operacional digital e de controlo do risco tecnológico. A utilização de criptografia vulnerável em

infraestruturas financeiras pode comprometer não apenas a confidencialidade de dados sensíveis, mas também a continuidade de serviço, a integridade transacional e a confiança sistémica. O problema não é apenas a exposição de dados, é também a eventual quebra de mecanismos de autenticação, validação e o não repúdio que sustentam o funcionamento quotidiano dos mercados, pagamentos e serviços críticos.

Importa ainda salientar a relevância do enquadramento probatório. A eventual fragilização de assinaturas digitais baseadas em criptografia clássica pode afetar a robustez jurídica de atos eletrónicos, contratos e comunicações formalmente autenticadas (eIDAS, 2014). Mesmo antes de uma quebra efetiva, o simples facto de uma tecnologia se tornar previsivelmente vulnerável pode conduzir a uma necessidade acrescida de diligência, migração tecnológica e revisão de políticas internas. Em termos de boa governação, a inércia pode deixar de ser defensável quando a literatura técnica e os organismos de normalização já identificam soluções pós-quânticas viáveis.

Neste quadro, a resposta mais adequada é a adoção de uma estratégia de *crypto-agility*, isto é, a capacidade de identificar, substituir e atualizar mecanismos criptográficos sem perturbação significativa dos serviços. Essa abordagem pressupõe inventário de ativos criptográficos, análise de dependências, testes piloto, segmentação de riscos, integração progressiva de algoritmos pós-quânticos e monitorização contínua. A criptoagilidade é, portanto, uma expressão concreta da diligência organizacional e da conformidade com o princípio da segurança desde a conceção e por defeito.

Em suma, a computação quântica obriga a uma leitura preventiva da segurança jurídica: as organizações não devem esperar pela materialização plena da ameaça para agir. A antecipação, neste domínio, é uma forma de conformidade, mas também uma forma de ética aplicada à proteção da confiança digital.

7. Conclusões e Perspetivas Futuras

7.1. Conclusão

A análise desenvolvida permite concluir que a computação quântica representa uma transformação estrutural no domínio da segurança digital, com impacto direto sobre os fundamentos da criptografia moderna. Algoritmos como os de Shor e Grover alteram profundamente a relação entre custo computacional, proteção da informação e robustez dos sistemas atualmente em uso. Assim, a ameaça quântica não deve ser entendida como uma hipótese remota ou meramente especulativa, mas como um fator real de reconfiguração das políticas de cibersegurança e das obrigações de conformidade.

Do ponto de vista técnico, a principal conclusão é a de que os sistemas criptográficos baseados em problemas matemáticos vulneráveis à computação quântica exigem substituição gradual por alternativas resistentes, com especial destaque para a criptografia pós-quântica. Do ponto de vista jurídico, a conclusão é igualmente clara: a segurança criptográfica passou a integrar o núcleo das obrigações de diligência, prevenção e gestão de risco das organizações, seja no âmbito da proteção de dados pessoais, seja no domínio da resiliência operacional e da segurança das redes e sistemas de informação. A manutenção de soluções previsivelmente obsoletas pode, em determinados contextos, assumir relevância para efeitos de responsabilidade regulatória e civil.

A análise permitiu ainda demonstrar que a migração não deve ser feita de forma abrupta e desarticulada. Pelo contrário, a transição mais eficaz assenta em inventário criptográfico, avaliação de dependências, testes piloto, soluções híbridas e atualização faseada de infraestruturas. Esta combinação reduz riscos operacionais, evita ruturas de compatibilidade e permite às organizações ajustar-se ao progresso tecnológico sem comprometer a continuidade dos seus serviços.

Por fim, conclui-se que a preparação para a era pós-quântica não é apenas uma questão de competitividade tecnológica, mas também uma exigência de governação responsável. A confiança digital depende da capacidade das organizações em proteger dados, garantir autenticidade e preservar a integridade das comunicações num ambiente de risco crescente. Nesse sentido, a criptografia pós-quântica não constitui apenas uma inovação

técnica: representa uma resposta necessária para assegurar a sustentabilidade jurídica, técnica e ética do ecossistema digital.

7.2. Perspetivas Futuras

As perspetivas futuras nesta matéria são particularmente relevantes, uma vez que a evolução da computação quântica e da criptografia pós-quântica deverá ocorrer em paralelo durante os próximos anos. A curto e médio prazo, é expectável a coexistência de soluções clássicas, híbridas e pós-quânticas, à medida que os organismos de normalização consolidam padrões e as organizações adaptam os seus sistemas. Este período de transição exigirá elevada coordenação entre indústria, academia e reguladores, para que a migração ocorra de forma segura, interoperável e auditável.

Uma primeira linha de desenvolvimento futuro reside na consolidação internacional dos padrões pós-quânticos. A normalização técnica será decisiva para assegurar compatibilidade entre plataformas, fornecedores e setores de atividade (NIST, 2024). A adoção progressiva de algoritmos padronizados permitirá reduzir a fragmentação e reforçar a confiança nos mecanismos de segurança adotados. Simultaneamente, será necessário acompanhar a evolução das recomendações regulatórias europeias e internacionais, de modo a harmonizar exigências técnicas e deveres jurídicos.

Uma segunda linha prende-se com a gestão de sistemas legados. Muitas organizações continuarão a depender de infraestruturas antigas, com limitações estruturais de integração e substituição. Por isso, a investigação futura deverá concentrar-se em modelos de migração faseada, automação da descoberta criptográfica, gestão dinâmica de chaves e avaliação contínua da exposição ao risco quântico. A questão não é apenas substituir algoritmos, mas garantir que todo o ecossistema tecnológico suporta essa substituição sem comprometer a operação.

Uma terceira linha de estudo diz respeito ao impacto da transição pós-quântica em setores de elevada sensibilidade, como banca, saúde, administração pública, telecomunicações e infraestruturas críticas. Nestes domínios, a proteção de dados e a continuidade operacional são particularmente exigentes, o que torna a adaptação à nova realidade quântica uma prioridade estratégica. Além disso, a dimensão probatória da assinatura digital e da autenticidade eletrónica deverá merecer atenção crescente, sobretudo em contextos contratuais e administrativos.

Por fim, a investigação futura deverá também aprofundar as dimensões éticas e de governação associadas à cibersegurança pós-quântica. A questão não se limita à proteção técnica de sistemas, mas inclui justiça digital, distribuição equitativa dos custos de migração, soberania tecnológica e responsabilidade institucional. A transição para a era pós-quântica será bem-sucedida apenas se conjugar inovação, regulação e confiança pública.

A preparação para a era pós-quântica deve ser encarada não como uma opção tecnológica, mas como uma exigência de governação prudente, conformidade jurídica e preservação duradoura da confiança digital.

Referências

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Assembleia da República. (2018). Lei n.º 46/2018, de 13 de agosto: Estabelece o regime jurídico da segurança do ciberespaço. *Diário da República*, 1.ª série, n.º 155.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-quantum cryptography*. Springer.

Centro Nacional de Cibersegurança (CNCS). (2024). *Diretiva SRI 2 (NIS 2)*. https://www.cncs.gov.pt/pt/diretiva-sri-2-nis-2/

Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society A: Mathematical and Physical Sciences, 400*(1818), 97–117. https://doi.org/10.1098/rspa.1985.0070

European Parliament, & Council of the European Union. (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)*. *Official Journal of the European Union, L 257*, 73–114.

European Parliament, & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation—GDPR)*. *Official Journal of the European Union, L 119*, 1–88.

European Parliament, & Council of the European Union. (2022). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA)*. *Official Journal of the European Union, L 333*, 1–79.

European Union Agency for Cybersecurity (ENISA). (2021). *Post-quantum cryptography: Current state and quantum mitigation*. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics, 21*(6), 467–488. https://doi.org/10.1007/BF02650179

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th annual ACM symposium on theory of computing* (pp. 212–219). Association for Computing Machinery. https://doi.org/10.1145/237814.237866

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

National Institute of Standards and Technology (NIST). (2024). *Post-quantum cryptography standardization*. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th ed.). Cambridge University Press.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., et al. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics, 12*(4), 1012–1236. https://doi.org/10.1364/AOP.361502

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th annual symposium on foundations of computer science* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

U.S. Congress. (2022). *Quantum Computing Cybersecurity Preparedness Act* (H.R. 7535, Pub. L. 117–260). U.S. Government Publishing Office.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.