O IMPERATIVO ESTADUAL: ADOÇÃO DE MÉTODOS CRIPTOGRÁFICOS AVANÇADOS PARA PREVENIR ATAQUES QUÂNTICOS

BREVES NÓTULAS À LUZ DAS NOVAS TECNOLOGIAS

TOMÁS CARVALHO GUERRA[1]
CAROLINA LAMY[2]

RESUMO: Este artigo explora a complexa relação entre a responsabilidade do Estado pelo funcionamento anormal do serviço, a computação quântica e a proteção de dados. À medida que os avanços da computação quântica remodelam o panorama tecnológico, os Estados enfrentam obrigações acrescidas na salvaguarda da integridade e privacidade dos dados. O estudo investiga cenários em que o Estado pode ser responsabilizado pelo funcionamento anormal do serviço, salientando os desafios em evolução colocados pelos algoritmos quânticos que podem comprometer os métodos clássicos de encriptação. Analisando os quadros jurídicos e as implicações políticas, o documento sublinha a necessidade urgente de os Estados adaptarem e reforçarem os seus quadros regulamentares e práticos para atenuar as potenciais vulnerabilidades introduzidas pelos avanços quânticos.

ABSTRACT: *This paper explores the intricate relationship between state responsibility due to an abnormal service functioning, quantum computing, and data protection. As quantum computing advancements reshape the technological landscape, governments face heightened obligations in safeguarding data integrity and privacy. This study investigates scenarios where the state is implicated in abnormal service functioning, emphasizing the evolving challenges posed by quantum algorithms that can compromise classical encryption methods. Analyzing legal frameworks and policy implications, the paper underscores the urgent need for states to adapt and fortify their regulatory frameworks to mitigate the potential vulnerabilities introduced by quantum advancements.*

PALAVRAS-CHAVE: Criptografia; Computação quântica; Responsabilidade do Estado; Funcionamento Anormal do Serviço; União Europeia.

KEYWORDS: *Cryptography*; *Quantum computing*; *State responsibility*; *Abnormal Functioning of the Service*; *European Union*.

---

[1] O autor é Investigador Júnior no Observatório da Aplicação do Direito da Concorrência, Centro de Estudos em Direito Europeu, e Investigador Júnior na Cavaleiro & Associados. Para além de ter sido estagiário na AdC Advogados, na Uría Menéndez - Proença de Carvalho e na Morais Leitão, Galvão Teles, Soares da Silva & Associados, atualmente é estagiário na Garrigues.

[2] Estudante do 3.º ano da Licenciatura em Direito na Universidade Católica Portuguesa, Centro Regional do Porto.

§1. Na complexa evolução da civilização humana, a interconexão entre o direito e a ciência emergiu como uma força inevitável ("The expected societal impact of quantum technologies (QT) urges us to proceed and innovate responsibly"[3]). A sinergia entre o direito e a ciência no domínio do direito computacional não é uma mera coincidência: é uma fusão deliberada que visa dar resposta às complexidades de um mundo cada vez mais interligado e centrado na tecnologia (como é o caso da *rule of code*[4])[5].

§2. A intersecção entre o direito e a ciência, particularmente nos domínios da criptografia e da computação quântica, representa um cenário complexo e dinâmico em que os avanços tecnológicos desafiam os quadros jurídicos tradicionais[6]. A criptografia, enquanto componente essencial da segurança da informação, tem desempenhado um papel garantístico na eficácia das doutrinas e teorias relativas à privacidade, à proteção de dados e à comunicação digital[7]. No entanto, o aparecimento da computação quântica introduz novos desafios que exigem uma reavaliação dos paradigmas jurídicos existentes[8]. As implicações jurídicas da computação quântica vão para além da mera vulnerabilidade dos sistemas criptográficos. A possibilidade de os computadores quânticos quebrarem esquemas criptográficos amplamente adotados pode exigir o estabelecimento de novas normas, padrões e responsabilidades jurídicas para fazer face à evolução deste novo cenário de ameaças ("Quantum algorithms have the potential to break current cryptography protocols, threatening the information security of existing

[3] AA. VV. (2023). *Towards Responsible Quantum Technology*. *In* Harvard Berkman Klein Center for Internet & Society Research Publication Series #2023-1, Harvard University, p. 1.

[4] Sobre esta temática: WRIGHT, Aaron; FILIPPI, Primavera de (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.

[5] No entanto, esta é uma fusão complexa, uma vez que o Direito, e toda a experiência humana, está ancorada no mundo físico. "Em todas as comunidades humanas a detenção física da coisa é associada empiricamente à legitimação da sua utilização exclusiva. Não é por acaso que o direito civil reconhece à **posse** da coisa uma presunção de propriedade. Mais que uma asserção jurídica, o instituto jurídico da posse é o reconhecimento legal de uma perceção biológica", VENÂNCIO, Pedro Dias (2023). *O Digital é Real*. 48K Newsletter.

[6] "Until now, the norm has been the so-called pacing problem, which specifically refers to the notion that technological innovation is increasingly outpacing the ability of laws and regulations to keep up", MEGALE, Luca (2022). *(Meta)verse as the Next Escaper from Competition Public Enforcement. In* Market and Competition Law Review, vol. VI, n.º 2, p. 16.

[7] Tendo em conta o estonteante poder de processamento destes computadores, a grande maioria dos sistemas criptográficos tornam-se, ultimamente, obsoletos, MARELLA, Surya; PARISA, Hemanth (2020). *Introduction to Quantum Computing*. InTech, p. 14.

[8] Para uma perspetiva interessante sobre a filosofia do digital: PINTO, Eduardo Vera-Cruz (2022). *Filosofia do Direito Digital: pensar juridicamente a relação entre Direito e tecnologia no ciberespaço. In* Revista da Faculdade de Direito da Universidade de Lisboa, vol. LXIII, n.º 1 e 2.

information technologies (IT) and the privacy of its users. This could destabilize society and undermine trust in its institutions. QT could expose extensive swaths of information currently regarded as private and confidential, ranging from sensitive personal data to financial sector and national security information assets. Concretely, we already have quantum algorithms capable of breaking our widespread public key cryptosystems as soon as the quantum computer hardware is sufficiently mature"[9])[10].

§3. Além disso, a intersecção do direito e da ciência no contexto da computação quântica sublinha a necessidade de os juristas adquirirem uma compreensão razoável dos princípios científicos subjacentes. A colaboração interdisciplinar entre juristas e cientistas torna-se imperativa para formular políticas eficazes que antecipem e respondam aos avanços tecnológicos Na sua essência, a relação dinâmica entre o direito e a ciência, particularmente nos domínios da criptografia e da computação quântica, exige uma abordagem proativa e adaptativa para enfrentar os desafios multifacetados colocados pela rápida inovação tecnológica[11].

§4. Com efeito, a transição da física clássica para a teoria quântica trouxe algumas inovações profundas que não foram imediatamente compreendidas nem pela lógica, nem pela comunidade científica[12]. A quântica representa um passo surpreendente na

[9] AA. VV. (2023). *Towards Responsible Quantum Technology*. *In* Harvard Berkman Klein Center for Internet & Society Research Publication Series #2023-1, Harvard University, p. 13.

[10] Tendo em conta o estonteante poder de processamento destes computadores, a grande maioria dos sistemas criptográficos tornam-se, ultimamente, obsoletos, MARELLA, Surya; PARISA, Hemanth (2020). *Introduction to Quantum Computing*. InTech, p. 14.

[11] "O pensamento tecnocientífico globalizado numa sociedade digital governada pela tecnologia, onde se concretiza a técnica informática, provoca uma rutura política a prazo, uma interrogação ética falível, uma exigência artística e uma apreensão cultural legítima que tem um inegável impacto antropológico e social, com efeito jurídico", PINTO, Eduardo Vera-Cruz (2022). *Filosofia do Direito Digital: pensar juridicamente a relação entre Direito e tecnologia no ciberespaço. In* Revista da Faculdade de Direito da Universidade de Lisboa, vol. LXIII, n.º 1 e 2, p. 302.

[12] Relativamente à teoria quântica, não há melhor ponto de partida do que o famoso *princípio da incerteza* (um dos pilares da mecânica quântica e, *ipso facto*, da computação quântica): não é possível medir exatamente, simultaneamente, a posição e o *momentum* de uma determinada partícula, nem o tempo e a energia associados a essa partícula [HEWITT, Paul (2009). *Fundamentos de Física Conceitual*. Bookman, p. 424]. Por outras palavras: a precisão da determinação do *momentum* de um eletrão diminui à medida que a precisão da determinação da posição de um eletrão aumenta; a precisão da determinação da energia de um eletrão diminui à medida que a precisão do tempo durante o qual a partícula mantém determinada energia: ΔE [KUMAR, Manjit (2010). *Quantum – Einstein, Bohr and the Great Debate about the nature of reality*. Icon Books, p. 225 e ZETTILI, Nouredine (2009). *Quantum Mechanics – Concepts and Applications*. (2.ª Edição). Wiley, pp. 28 e ss]. HEISENBERG afirma que existe uma "[...] inerente incerteza na relação entre a posição e o momentum" [HOLZNER, Steven (2013). *Quantum Physics for Dummies*. Wiley, p. 20].

descoberta científica e inicia um colossal confronto com a física clássica[13]. A quântica

Outro princípio de profunda relevância gravita em torno da conhecida *sobreposição quântica*. Em termos leigos, este conceito traduz-se na possibilidade de a mesma partícula poder estar em dois estados ao mesmo tempo [DIRAC, Paul (1947). *The principles of quantum mechanics*. (3.ª Edição). Oxford, pp. 1-10]. Um sistema quântico pode existir numa superposição linear de diferentes estados, estando suspenso entre diferentes realidades clássicas [PAHLAVANI, Mohammad (2012). *Theoretical Concepts of Quantum Mechanics*. InTech, p. 474]. A respeito deste princípio, a experiência mental mais famosa é a de SCHRÖDINGER, que concebe uma hipótese em que um gato se encontra dentro de uma caixa com uma substância radioativa. O famoso gato de Shrödinger existiria numa sobreposição de estados: vivo e morto até ser observado. SCHRÖDINGER relata o seguinte: "A cat is penned up in a steel chamber, along with the following diabolical device: in a Geiger counter there is a tiny bit of radioactive substance, so small, that perhaps in the course of one hour one of the atoms decays, but also, with equal probability, perhaps none; if it happens, the counter tube discharges and through a relay releases a hammer which shatters a small flask of hydrocyanic acid. If one has left this entire system to itself for an hour, one would say that the car still lives if meanwhile no atom has decays. The first atomic decay would have poisoned it" [SCHRÖDINGER, Erwin (1935). *Die gegenwärtige Situation in der Quantenmechanik*. Naturwissenschaften, 23, p. 157; Citado em KUMAR, Manjit (2010). *Quantum – Einstein, Bohr and the Great Debate about the nature of reality*. Icon Books, p. 316].

Em terceiro lugar, deve ser abordado o *quantum entanglement* (entrelaçamento quântico). Este é, talvez, o fenómeno mais estranho da mecânica quântica (fenómeno crucial para a próxima fase do trabalho, a computação quântica), dado que nos demonstra que duas ou mais partículas, ligadas de determinada forma, ficam conectadas, irremediavelmente, independentemente da distância a que se encontrem uma(s) da(s) outra(s). Imaginemos a partícula *A* e a partícula *B*. O estado quântico para o sistema complexo destas duas partículas é o produto tensorial dos dois estados distintos [SUSSKIND, Leonard; FRIEDMAN, Art (2015). *Quantum Mechanics - The Theoretical Minimum*. Penguin Books, p. 150]. SCHRÖDINGER atesta que "[...] any entanglement of predictions that takes place can obviously only go back to the fact that the bodies at some earlier time formed in a true sense one system, that is were interacting, and have left behind traces on each other" [SCHRÖDINGER, Erwin (1935). *Die gegenwärtige Situation in der Quantenmechanik*. Naturwissenschaften, 23, p. 161; Citado em KUMAR, M. (2010). *Quantum – Einstein, Bohr and the Great Debate about the nature of reality*. Icon Books].

Em quarto lugar, deve ser abordado o *quantum tunneling*, que se traduz na possibilidade de as partículas atravessarem barreiras de potencial. Se as partículas colidem com uma barreira de potencial limitada, a física quântica afirma que a travessia das partículas através da barreira de potencial, mesmo que a energia total da partícula seja menor que a altura da barreira, pode ser calculada quanto aos seus efeitos [GRIFFITHS, David; SCHROETER, Darrell (2018). *Introduction to Quantum Mechanics*. (3.ª edição). Cambridge University Press, p. 455].

Em quinto lugar, devemos mencionar os chamados *quantum leaps*. Um salto quântico é uma transição descontínua entre estados quânticos. Em termos muito básicos, isto quer dizer que um eletrão (com um determinado nível de energia) "salta" instantaneamente para outro nível de energia [BERNSTEIN, Jeremy (2019). *Quantum Leaps – How Quantum Mechanics took over science*. (2ª Edição). World Scientific], absorvendo ou emitindo energia no processo (não há nenhum local intermédio nesse salto; o eletrão passa instantaneamente de um sítio para outro inexistindo durante um hiato temporal estonteantemente reduzido). "*Electrons don´t always exist. They exist when they interact. They materialize in a place when they collide with something else. The quantum leaps from one orbit to another constitute their way of being real: an electron is a combination of leaps from one interaction to another*" [ROVELLI, Carlo (2017). *Reality is not what it seems*. Penguin Science, pp. 100-101].

[13] Em suma, podemos, facilmente, observar alguns pontos de fraturação, especialmente entre a teoria quântica e a teoria clássica de *Newton*: (i) enquanto nesta todas as propriedades de uma partícula seriam idóneas a ser calculadas com alta precisão, já na quântica, a posição ou o *momentum* não podem ser calculados com igual grau de precisão [VIRK, Hardev (2014). *Classical Physics Versus Quantum Physics:*

veio resolver problemas em que a física clássica estava irremediavelmente estagnada como, por exemplo, a radiação do corpo negro, o efeito fotoelétrico, a difusão de *Compton*, as ondas de matéria, os espetros atómicos, o movimento dos átomos, entre outros[14].

§5. Para além da resolução de um vasto leque de clássicos problemas, a quântica veio revolucionar, também, a área computacional com a descoberta da possibilidade de criar computadores quânticos. O sistema clássico de um computador atual é extremamente limitado. Embora possa não o parecer, na realidade o potencial teórico destas máquinas ainda não foi totalmente explorado, encontrando-se barrado por diversos fatores. É amplamente aceite que um computador clássico apenas pode ser reduzido para 5-7 nanômetros[15/16]. Por que razão há este limite? Se reduzirmos os circuitos para o tamanho de um átomo, estes circuitos vão se reger por regras diferentes[17]: as regras quânticas. Surgem, então, os computadores quânticos[18].

§6. Estes computadores serão a contraparte quântica da máquina de TURING ("Uma máquina de turing [...] é um simples aparelho clássico, baseado num processador, que transforma o número numa fita de comprimento infinito noutro número e, assim, executa uma série de operações matemáticas"[19])[20]. Por um lado, os computadores clássicos realizam operações com base numa posição definida de um estado físico

An Overview, p. 2]; (ii) por norma a mecânica clássica é lida com modelos deterministas, ou seja, conhecendo as condições e elementos originais, e podemos prever, através da matemática, com precisão o comportamento do sistema, mas a mecânica quântica é tendencialmente não determinista, *ille est*, apenas conseguimos determinar o comportamento do sistema com base em graus de probabilidade (por exemplo, nas partículas interligadas, há uma hipótese de 50% de que a outra partícula terá um *spin* de *up*); (iii) as teorias clássicas apenas permitem que uma partícula exista em um estado singular, mas a mecânica quântica desbloqueia a possibilidade de uma particular existir em diversos estados simultaneamente; (iv) nos sistemas clássicos, as partículas são tratadas como uma realidade unitária, ou seja, são apenas partículas, no entanto, o sistema quântico oferece a possibilidade de as partículas exibirem comportamentos de ondas.

[14] AA. VV. (1992). *Introdução à física*. McGraw-Hill, pp. 392-408.

[15] SUTOR, Robert (2019). *Dancing with Qubits: How quantum computing works and how it can change the world.* Packt.

[16] Um nanómetro ou nanômetro é uma unidade de medida de comprimento do sistema métrico, correspondente a 10^{-9} metro. *Vide*, AA. VV (2004). *Introduction to Nanoscale Science and Technology*. Springer, pp. 315 e ss.

[17] MARELLA, Surya; PARISA, Hemanth (2020). *Introduction to Quantum Computing*. InTech, p. 2.

[18] AA. VV. (2022). *A Quantum Approach for Secure and Optimized Metaverse Environment*. *In* Human-centric Computing and Information Sciences, vol. 12, n.º 42, p. 6.

[19] KAKU, Michio (2023). *Supremacia Quântica*. Bertrand Editora, pp. 87-88.

[20] AA. VV (2018). *Quantum Computation and Logic – How Quantum Computers have inspired logical investigations*. Springer. Trends in Logic, Vol. 48, p. 127.

geralmente binário[21]. Isto significa que as operações são baseadas em apenas uma de duas posições (1 ou 0, o qual é chamado de *bit*). Em contraste, nos computadores quânticos as operações usam o estado quântico de um objeto para produzir aquilo que é conhecido como *qubit* (um *quantum bit*)[22]. Em vez de os estados terem uma posição clara (tal como na computação clássica), os estados quânticos não medidos ocorrem em superposição[23]. Aliás, como todos os *qubits* desta máquina estão entrelaçados, então as alterações sofridas por um *qubit* influenciam todos os outros *qubits*[24].

§7. Em termos simples, e de forma a ilustrar a capacidade dos computadores quânticos, imaginemos um labirinto que se estende por quilómetros. A tarefa de encontrar a via correta para sair do labirinto é entregue a um computador clássico e a um computador quântico. O computador clássico irá tentar, uma a uma, todas as hipóteses possíveis (imagine-se, para efeitos de compreensão, que o computador viaja rapidamente pelos diferentes caminhos). O computador quântico fará algo similar, mas que está vedado ao computador clássico (esta capacidade do computador quântico é lhe atribuída pelos princípios da mecânica quântica supramencionados); o computador vai percorrer todos os caminhos possíveis, contudo, fará isso ao mesmo tempo, instantaneamente. Sendo assim, um computador quântico tem o potencial de ser 100-158 milhões de vezes mais rápido do que um computador de base clássica[25].

§8. Mas, então, de que forma é que a criptografia atual[26], escudo fundamental do mundo digital moderno, se mantém para lá de uma mera ilusão de segurança ("É fundamental que se compreenda que os novos riscos obrigam a novas respostas, e que a adesão ao digital implica, também da parte das organizações públicas, uma capacidade reforçada de proteger o que é de todos, num contexto de ameaça que é, também, um desafio para a nossa própria soberania e modo de vida"[27])[28]?

---

[21] WHITE, Ron (2020). *How Computers Work – The Evolution of Technology*. (10.ª Edição). QUE, p. 30.
[22] POLAK, Wolfgang; RIEFFEL, Eleanor (2011). *Quantum Computing – A Gentle Introduction*. MIT Press, p. 2.
[23] MARELLA, Surya; PARISA, Hemanth (2020). *Introduction to Quantum Computing*. InTech, p. 6.
[24] KAKU, Michio (2023). *Supremacia Quântica*. Bertrand Editora, pp. 88.
[25] CHAKRABORTY, Utpal. *Quantum Computing and Future*. (1st edition). BPB Publications, p. 29.
[26] Existem diversos tipos de encriptação, por exemplo, AES, RSA, ECC, TLS, DES, CBC, CFB, OFB, XTS.
[27] NUNES, Adolfo Mesquita (2022). *A Responsabilidade das Entidades Públicas em Tempo de Ciberataques. In* Advocatus, disponível em https://eco.sapo.pt/advocatus/.
[28] A criptografia é a ciência e a arte de proteger informação por meio de codificação, garantindo que apenas pessoas autorizadas possam decifrá-la e, *ipso facto*, lê-la. Em geral, os principais objetivos da criptografia hodierna gravitam em torno: da segurança, garantindo que os utilizadores possam transmitir e aceder a

§9. Todas as plataformas digitais, em princípio, são protegidas por algo a que chamamos de criptografia. Isto significa que terceiros estão impedidos de aceder às nossas mensagens/conversas/telefonemas/fotos/vídeos. Embora ciberataques sejam frequentes, a verdade é que os nossos sistemas de encriptação são bastante eficazes contra computadores clássicos. Todavia, a utilização de um computador quântico permite que a esmagadora maioria dos nossos sistemas de encriptação se tornem obsoletos ("[...] there is the ability of quantum computers to break current encryption protocols, potentially exposing health data or commercially sensitive information to cybercriminals. This raises the prospect of a rush of negligence class actions from consumers, commercial disputes between businesses, customers and vendors, and shareholder and securities litigation over the impact of a breach on the business and its stock price"[29])[30]. Os sistemas criptográficos mais utilizados atualmente, RSA-2048, RSA-3072, DH-3072, 256-bit ECDSA (esta utilizada, por exemplo, na troca de *bitcoins*), quando desafiados por um computador

informação de forma segura e confidencial; e da integridade, assegurando que os dados permanecem inalterados (ou ilegíveis) durante a transmissão e armazenamento. Em geral, a criptografia é especialmente crucial na proteção de dados sensíveis, nomeadamente transações financeiras e informações pessoais, contra o acesso não autorizado da informação transmitida e/ou armazenada. A sua aplicação é vasta, abrangendo a cibersegurança, o comércio eletrónico, as comunicações governamentais e vários domínios digitais, garantindo a privacidade e a confiança num mundo cada vez mais tecnológico.

Para entender o que é a criptografia, devemos, primeiro, começar por estabelecer o conceito de algoritmo e de cifra: (a) por algoritmo entende-se uma sequência finita de regras precisas que culminam na solução de um problema [DIAS, Ariel da Silva (2023). *Algoritmos e Linguagens de Programação*. Senac, Capítulo 1]; (b) por cifra entende-se um sistema que transforma texto legível em texto não legível e vice-versa [BERTACCINI, Massimo (2022). *Cryptography Algorithms*. Packt Publishing, p. 4]. Assim, o texto que se pretende "esconder", através da operação de encriptação, designa-se como *plaintext* e o texto que resulta da aplicação do algoritmo de encriptação designa-se como *ciphertext*. Com efeito, a criação de cifras gravita em torno da tentativa de tornar informação inelegível para terceiros, sendo o armazenamento de dados e a transmissão de dados através da internet os principais usos deste sistema [PIPER, Fred; MURPHY, Sean (2002). *Cryptography – A Very Short introduction*. Oxford University Press, p. 7].

Passando a explicar a tramitação da encriptação: a partir do momento em que o *plaintext* é enviado, este é filtrado através de um algoritmo de encriptação (utilizando a cifra de encriptação correta). O *ciphertext*, depois, passa por um algoritmo de desencriptação (utilizando a cifra desencriptação correta) para o reverter à sua forma original (*plaintext*). Como consequência, se um terceiro intercetar a mensagem entre o momento de envio e o momento em que *ciphertext* é desencriptado.

A mais das vezes, os ataques a informação encriptada visam determinar qual é a chave de encriptação imbuída no algoritmo de encriptação. Portanto, quando comumente se afirma que um algoritmo foi quebrado, na verdade o que se está a afirmar é que se descobrir uma forma prática de determinar a chave utilizada. Se o algoritmo criptográfico for conhecido, mas a chave não, então resta ao potencial atacante uma alternativa: um ataque de força bruta (*brute force attack*), ou seja, tentar todas as chaves possíveis

[29] https://www.allenovery.com/en-gb/global/news-and-insights/publications/the-opportunities-and-legal-risks-of-quantum-computing

[30] MARELLA, Surya; PARISA, Hemanth (2020). *Introduction to Quantum Computing*. InTech, p. 14.

quântico, revelaram-se insuficientes para resistir ("Quantum computers will increase the probability of intellectual property theft or data breaches as cryptography attacks become more frequent, and companies responsible for critical infrastructure, such as transportation, energy distribution systems, or communications, will be particularly vulnerable"[31])[32].

§10. Veja-se que, a bom rigor, a forma mais eficaz de combater as capacidades um computador quântico é desenvolvendo cifras quânticas[33]. Note-se, contudo, de todo o modo, que uma cifra capaz de resistir a um computador quântico não precisa, necessariamente, de ser desenvolvida por um computador quântico, embora a quântica nos permita construir códigos mais seguros[34], especialmente no que toca a métodos de distribuição de chaves[35].

§11. Assim sendo, há que levantar a questão: pode o Estado ser responsabilizado, face a um ataque quântico, em caso de utilização de meios criptográficos antiquados ("Do que se trata é de recordar que as entidades públicas, em virtude das suas atribuições e competências, estão presentes em quase todos os campos da nossa vida, interagem continuamente connosco: guardam os nossos dados, licenciam as nossas actividades, registam as nossas interacções, autorizam as nossas pretensões, prestam serviços, cobram impostos [...]"[36])?

§12. Atualmente, o Regime da Responsabilidade Civil Extracontratual do Estado

[31] RODRÍGUEZ, Andrea (2023). *A Quantum Cybersecurity Agenda for Europe.* European Policy Centre, discussion paper, julho, p. 5.
[32] RODRÍGUEZ, Andrea (2023). *A Quantum Cybersecurity Agenda for Europe.* European Policy Centre, discussion paper, julho, p. 4.
[33] LUTKENHAUS, Norbert (2006). *Quantum Cryptography*. *In* Elsevier Journal of Progress in Optics, pp. 9-10.
[34] BERNHARDT, Chris (2019). *Quantum Computing for everyone*. MIT Press, p. 175.
[35] "The US arguably leads the transition to post-quantum cybersecurity [...], in which post-quantum cryptography will be the protagonist. In 2016, the US NIST initiated a standardisation process of post-quantum cryptography algorithms, noticing the fast development of quantum computing and its potential impact on information security. Out of the many algorithms submitted in 2022, NIST selected four of them with the perspective of finalising standardisation efforts in 2024. In parallel with the standardisation process, the US has sped up the number of policies dedicated to securing sensitive information against quantum cyberattacks. In 2022, the US passed the Quantum Cybersecurity Preparedness Act, which sets up a roadmap to migrate government information to post-quantum cryptography. Furthermore, the White House issued a series of memorandums6 urging federal agencies to report an inventory of cryptographic systems and start the transition to post-quantum cryptography", RODRÍGUEZ, Andrea (2023). *A Quantum Cybersecurity Agenda for Europe.* European Policy Centre, discussion paper, julho, p. 6.
[36] NUNES, Adolfo Mesquita (2022). *A Responsabilidade das Entidades Públicas em Tempo de Ciberataques. In* Advocatus, disponível em https://eco.sapo.pt/advocatus/.

e demais Entidades Públicas ("RREEP") regula a responsabilidade civil extracontratual da Administração Pública, nomeadamente no exercício da função administrativa[37], dando-se concretização ao art. 22.º da Constituição da República Portuguesa ("CRP"), do qual se tinha vindo a extrair a consagração do princípio de responsabilização do Estado e demais entidades públicas pelos danos que causem no exercício das suas funções, sendo de relevo tanto ações como omissões[38]/[39]. Em causa está, também, o princípio do respeito pelos direitos e interesses legalmente protegidos dos particulares, art. 266.º, n.º 1, da CRP, e art. 4.º do Código do Procedimento Administrativo ("CPA") - "[...] a responsabilidade civil da Administração, representa a 'ultima linha de defesa' do Estado de Direito"[40].

§13. Em matéria de responsabilidade por facto ilícito, temos por base a

[37] Entre outros, como a função jurisdicional e legislativa.

[38] ALMEIDA, Mário Aroso de (2022). *Teoria Geral do Direito Administrativo*. (9.ª edição). Almedina, pp. 657 e 658.

[39] Tradicionalmente, e segundo a secular frase "The King can do no wrong", vigorava a mentalidade de que o Estado não podia ser responsabilizado. Este panorama era especialmente cristalino na época absolutista - século XVI até meados do século XIX [AMARAL, Diogo Freitas do (2011). *Curso de Direito Administrativo - Volume II*. (4.ª edição). Almedina, p. 575]. Apesar de, gradualmente, os ordenamentos jurídicos começarem a permitir um certo nível de responsabilidade estadual, por exemplo através da responsabilização dos municípios ou dos atos *ius gestionis* do Estado.
De todo o modo, foi no segundo quartel do séc. XX que se passou a admitir a responsabilidade do Estado também por atos de autoridade, tendo a revisão de 1930 do Código de Seabra consagrado a responsabilidade solidária do Estado para com os seus funcionários que praticassem atos ilícitos no exercício das suas funções (art. 2399.º, com as alterações introduzidas pelo Decreto-Lei n.º 19126, de 16 de dezembro de 1930). Ademais, a própria Constituição de 1933 inseria o direito dos cidadãos à reparação dos danos causados pelo Estado (art. 8.º, n.º 17).
A partir de 1950, abriram-se portas também à responsabilidade administrativa pelo risco (art. 2397.º do Código de Seabra), abandonando-se o princípio da tipicidade quanto a estes casos, tendo a Administração o dever de indemnizar mesmo nas hipóteses não previstas pela lei [AMARAL, Diogo Freitas do (2011). *Curso de Direito Administrativo - Volume II*. (4.ª edição). Almedina, p. 578]. O Código Civil de 1966 veio dar autonomia à responsabilidade do Estado, dispondo apenas sobre a atuação do Estado em vestes particulares, deixando para a lei administrativa a disciplina dos atos de gestão pública [BARRA, Tiago Viana (2011). *A Responsabilidade Civil Administrativa do Estado. In* Revista da Ordem dos Advogados, ano 71, n.º 1, p. 136].
A nível constitucional, em 1976, foi autonomizada expressamente pelo Decreto-Lei n.º 48051, de 21 de novembro de 1967, a responsabilidade do Estado e demais entidades públicas dos seus funcionários e agentes, respondendo os primeiros solidariamente pelos segundos [AMARAL, Diogo Freitas do (2011). *Curso de Direito Administrativo - Volume II*. (4.ª edição). Almedina, p. 579]. Denota-se, portanto, a par da aproximação dos particulares e da Administração Pública, uma cada vez maior responsabilização desta, em ordem à proteção dos lesados (A "[...] irresponsabilidade só era concebível na época em que a coisa pública pertencia a um só indivíduo ou a uma só classe, sendo até sacrilégio duvidar da impecabilidade das autoridades, como sob a tirania bizantina", GONÇALVES, Luíz da Cunha (1905). *A Responsabilidade da Administração Pública pelos Actos dos seus Agentes*. Coimbra, p. 18).

[40] AMARAL, Diogo Freitas do (2011). *Curso de Direito Administrativo - Volume II*. (4.ª edição). Almedina, p. 568.

responsabilidade subjetiva, ou seja, aquela que assenta na culpa do agente[41]. Refere FREITAS DO AMARAL que, por ser a culpa uma noção eminentemente subjetiva, "[...] para se considerar que uma pessoa coletiva agiu com culpa é necessário imputar essa culpa a um ou mais indivíduos que tenham atuado, no exercício das suas funções, ao serviço dessa pessoa coletiva"[42]. Mas, como se pode imaginar, será muitas das vezes difícil ou mesmo impossível apurar de quem foi a culpa de uma atuação no âmbito de um serviço público no caso concreto - tendo em conta a crescente complexidade da estrutura de organização administrativa -, imputando-se então a atuação lesante ao serviço globalmente considerado e promovendo-se a proteção da vítima[43]/[44].

§14. Em Portugal, curiosamente, estamos perante um exemplo de *case law*[45], tendo sido a jurisprudência que mais contribuiu para a evolução deste instituto em

[41] CORTEZ, Margarida (2000). *Responsabilidade Civil da Administração por Atos Administrativos Ilegais e Concurso de Omissão Culposa do Lesado*. Coimbra Editora, p. 93.

[42] AMARAL, Diogo Freitas do (2011). *Curso de Direito Administrativo - Volume II*. (4.ª edição). Almedina, pp. 615-616.

[43] Bem como a variação de serviços, a morosidade dos seus processos, a oscilação de titulares de cargos públicos; todos estes fatores tornam possível a cumulação de pequenas falhas desculpáveis ou mesmo legítimas, transformando-se, no limite, num facto ilícito culposo, AMARAL, Diogo Freitas do (2011). *Curso de Direito Administrativo - Volume II*. (4.ª edição). Almedina, pp. 616-617.

[44] Em França, ordenamento de onde Portugal muito se inspirou, é pioneira neste âmbito da responsabilidade administrativa. Em 1873 (Acórdãos *Blanco*, de 8 de fevereiro de 1873, n.º 00012, e *Pelletier*, de 30 de julho de 187, n.º 00035, *Tribunal des Conflits*), havia já indícios de responsabilidade administrativa e de desvalorização da responsabilidade pessoal dos funcionários. Da jurisprudência francesa, importou a portuguesa o conceito *faute du service*, a partir dos anos sessenta do século passado [SOUSA, Ana Pereira de (2012). *A culpa do serviço no exercício da função administrativa. In* Revista da Ordem dos Advogados, ano 72, pp. 340-341].

Em Espanha, tendo ocorrido um dano, assente ele numa atuação lícita ou ilícita do poder público, ter-se-á de ponderar a responsabilização do Estado. Tendo havido funcionalmente anormal, basta demonstrar tal facto, não sendo sequer necessário provar que houve culpa (Constituição Espanhola e Lei 30/1992).

Na Alemanha, o funcionamento é algo diferente. O Estado apenas será obrigado a indemnizar um terceiro lesado quando o funcionário, desempenhando as suas funções, atue com culpa (§ 839 do *Bürgerliches Gesetzbuch*). Sucede que, e sendo indispensável o pressuposto da culpa, nos casos em que apenas tenha havido mera negligência a responsabilidade do Estado será subsidiária, pois o terceiro terá a possibilidade de recorrer a outros meios para se tornar indemne [SOUSA, Ana Pereira de (2012). *A culpa do serviço no exercício da função administrativa. In* Revista da Ordem dos Advogados, ano 72, p. 344]. Não o fazendo, mas tendo possibilidade para tal, não se responsabilizará o Estado pela inércia do lesado, apenas o fazendo, subsidiariamente, quando o lesado não possa recorrer a qualquer outra via (§ 839(1) do *Bürgerliches Gesetzbuch*).

Em Itália, relativamente à responsabilidade civil extracontratual do Estado e demais entes públicos, é de relevo a *Sentenza* n.º 500, *Corte di Cassazione*, de 22 de julho de 1999, que põe em destaque o requisito da culpa: releva não apenas a ilegalidade em si considerada, mas também o comportamento administrativo que a ela levou, destacando como parâmetros o princípio da boa-fé, da imparcialidade e da boa administração.

[45] No sistema jurídico português sempre houve um predomínio do direito legislado.

Portugal, depois de ter sido constituído pela lei o regime geral da responsabilidade administrativa[46].

§15. A jurisprudência portuguesa procedeu à importação da *faute du service* do Direito francês, que imputa às entidades públicas a responsabilidade civil extracontratual por danos resultantes do funcionamento anormal do serviço, não sendo possível, no caso concreto, imputá-los à conduta de determinado agente[47]. Por outras palavras, responsabiliza-se a Administração pelos "[...] danos resultantes do seu funcionamento que o lesado não tenha obrigação de suportar [...]", já que não teriam sido causados se o serviço tivesse funcionado normalmente[48]/[49]. A responsabilidade por funcionamento anormal do serviço encaixa-se, assim, no entendimento de AROSO DE ALMEIDA, numa das modalidades de ilicitude da responsabilidade extracontratual do Estado[50].

§16. O art. 7.º, n.º 3, RREEP, consagra a responsabilidade exclusiva do Estado e demais entidades públicas quando se verifique uma situação de funcionamento anormal do serviço, quer na modalidade de falta anónima[51], quer na de falta coletiva[52]. Assim, nos n.ºs 3 e 4 do artigo 7.º, somos remetidos especificamente para o funcionamento anormal do serviço, em que a antijuricidade tende a ser reflexo de um elemento objetivo caracterizador do dano indemnizável, e não de um elemento subjetivo da conduta lesiva[53]. Neste sentido, refere VIEIRA DE ANDRADE a objetificação do campo tradicional da responsabilidade subjetiva, havendo uma ampliação do conceito de ilicitude e objetificação da culpa, desvalorizando-se o conceito de culpa como censura ético-comportamental[54]. Importa, ainda, sublinhar que o funcionamento anormal do serviço

[46] ALMEIDA, Mário Aroso de (2013). "Responsabilidade do Estado e demais pessoas coletivas de direito público", in *Comentário ao Regime da Responsabilidade Civil Extracontratual do Estado e demais Entidades Públicas* (org. de Rui Medeiros). Universidade Católica Editora, p. 217.
[47] *Idem*, p. 218.
[48] Atendendo aos "padrões médios de resultado", art. 7.º, n.º 4, RREEP.
[49] ALMEIDA, Mário Aroso de (2022). *Teoria Geral do Direito Administrativo*. (9.ª edição). Almedina, p. 672.
[50] ALMEIDA, Mário Aroso de (2022). *Teoria Geral do Direito Administrativo*. (9.ª edição). Almedina, p. 683.
[51] Quando o dano é imputável à conduta de determinado agente, mas não é possível averiguar a autoria pessoal da ação/omissão.
[52] Quando o dano não é consequência de um determinado agente, mas de uma atuação global do serviço.
[53] ALMEIDA, Mário Aroso de (2013). "Responsabilidade do Estado e demais pessoas coletivas de direito público", in *Comentário ao Regime da Responsabilidade Civil Extracontratual do Estado e demais Entidades Públicas* (org. de Rui Medeiros). Universidade Católica Editora, p. 220.
[54] ANDRADE, José Carlos Vieira de (1997). *Panorama Geral do Direito da Responsabilidade "Civil" da Administração em Portugal. In* "La Responsabilidade Patrimonial de los Poderes Públicos", III Coloquio

deve ser aferido de acordo com as circunstâncias e a padrões médios de resultado, analisando se era razoavelmente exigível ao serviço uma atuação suscetível de evitar os danos produzidos (art. 7.º, n.º 4, RREEP).

§17. Portanto, e reintroduzindo a pergunta colocada no § 11., pode o Estado ser responsabilizado por funcionamento anormal do serviço, face a um ataque quântico, em caso de utilização de meios criptográficos antiquados? Para concluir e alcançar uma resposta, há que, então, averiguar qual é o patamar exato a que o serviço devia estar a funcionar para, assim, determinar se estamos perante um serviço abaixo desse limiar.

§18. Com uma responsabilidade acentuada pela confiança que é depositada no Estado, é crucial que este cumpra cabalmente o seu dever de salvaguardar os dados dos cidadãos e de várias instituições. Ademais, este conceito de salvaguardar os dados (arts. 8.º e 15.º da Carta Portuguesa de Direitos Humanos na Era Digital, 35.º, n.º 2, da Constituição da República Portuguesa e 7.º da Convenção 108) vai além da mera recolha e armazenamento seguro, estendendo-se à proteção contra o acesso não autorizado, roubo e demais violações. A criptografia inadequada, que se refere à utilização de técnicas de encriptação fracas ou desatualizadas, pode tornar estes dados vulneráveis a terceiros. Quando o Estado não adota medidas criptográficas fortes, coloca em risco tanto os indivíduos como a comunidade como um todo ("[...] we can foresee potentially disruptive effects to fundamental human rights such as privacy and data protection, including large scale loss of privacy, human identity theft, loss of confidentiality and integrity of digital communication on the Internet, obstruction of commercial transactions, leaking of highly sensitive trade and state secrets, and other unwanted global surveillance disclosures"[55]).

§19. Um dos principais pontos de aferição ancora-se no Decreto-Lei n.º 65/2021, de 30 de Julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço. O artigo 9.º reza que as entidades referidas no art. 1.º, n.º 2, al. a), devem cumprir as medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, devendo, para o efeito, realizar uma análise dos riscos. Ademais, e de extrema importância, dispõe o n.º 2 do mesmo preceito que as "[...] medidas referidas no número anterior devem garantir um nível de segurança adequado ao

Hispano-Luso de Derecho Administrativo, de 16-18 de outubro de 1997, (coords.) ANTONIO CALONGE VELÁZQUEZ, JOSÉ LUIS MARTÍNEZ LÓPEZ-MUÑIZ, p. 45.

[55] AA. VV. (2023). *Towards Responsible Quantum Technology*. *In* Harvard Berkman Klein Center for Internet & Society Research Publication Series #2023-1, Harvard University, p. 13.

risco em causa, tendo em conta os progressos técnicos mais recentes, através da utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia".

§20. Sublinhe-se, também, o plasmado nos arts. 32.º e 35.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016: "Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento", art. 32.º; "Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais", art. 35.º[56].

§21. No entanto, há que debater, brevemente, se é razoável impor ao Estado a consideração da tecnologia quântica, desde logo tendo em conta a incerteza relativamente à existência de uma verdadeira supremacia quântica hodiernamente. Ainda que não se considere que, atualmente, seja razoável impor aos Estados a tomada de medidas (note-

[56] "From a legal perspective, current privacy and cybersecurity regimes operate on the principle of 'reasonable security'; *i.e.*, companies expect to implement appropriate technical and organizational measures to guard their systems from attack based on their understanding of the external threat environment. However, in a world where quantum computers are edging closer to the mainstream, the concept of 'reasonable' in the eyes of regulators and the courts may change. Businesses, therefore, need to be aware of developments in quantum technology and understand exactly how their data and that of their supply chain partners is protected. They should ensure they are implementing the most robust measures to depersonalize any data they hold, and potentially update their privacy notices to ensure their 'quantum-proofing' actions are visible to the public", https://www.allenovery.com/en-gb/global/news-and-insights/publications/the-opportunities-and-legal-risks-of-quantum-computing

se, medidas dispendiosas) idóneas a proteger os dados contra computadores quânticos, tal paradigma não se manterá *ad eternum*. A bom rigor, e dando verdadeiro cumprimento aos imperativos constitucionais, talvez as engrenagens políticas se devessem começar a movimentar no sentido de investir no desenvolvimento da criptografia pós-quântica.

§22. Aliás, este investimento esperava-se que partisse, *prima facie*, da União Europeia, uma vez que, nos últimos anos, a União Europeia tem vindo a desenvolver uma política ativa em matéria de cibersegurança. Contudo, a repercussão da computação quântica no espaço cibernético europeu tem sido amplamente ignorada no seio da mencionada discussão, apesar de serem feitas menções honorárias a este tema na Estratégia da EU para a Cibersegurança 2020 ou no Regulamento n.º 2023/588 que estabelece o Programa da União Europeia Segura 2023-2027 ("Quantum computing, a field developing rapidly, will disrupt online security by compromising cryptography - the algorithms that keep information safe - or by facilitating cyberattacks such as those on digital identities")[57].

§23. No sentido de uma possível responsabilização do Estado em caso de ciberataques, embora não mencione a computação quântica, cite-se as palavras de ADOLFO MESQUITA NUNES: "Com a recente publicação do Decreto-Lei n.º 65/2021, de 30 de Julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço (Lei n.º 46/2018, de 13 de Agosto, que transpôs a Directiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de Julho de 2016), as entidades públicas ficaram obrigadas a cumprir medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, garantindo um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes"[58].

§24. Em conclusão, cada época encara, inevitavelmente, os seus desafios. A par dos muitos que vivemos no séc. XXI, focámo-nos, nesta reflexão, no desenvolvimento tecnológico e nas consequências que poderá repercutir na esfera estadual. Sabendo que a tecnologia altera, a ritmo estonteante, a realidade que o legislador procura regular, é, então, para o Direito, um enorme desafio acompanhar e regular os progressos que tão

[57] AA. VV. (2023). *Towards Responsible Quantum Technology*. *In* Harvard Berkman Klein Center for Internet & Society Research Publication Series #2023-1, Harvard University, p. 4.

[58] NUNES, Adolfo Mesquita (2022). *A Responsabilidade das Entidades Públicas em Tempo de Ciberataques. In* Advocatus, disponível em https://eco.sapo.pt/advocatus/.

rapidamente se inserem no quotidiano comum. Por muito desafiante que seja, não deixa, no entanto, de ser um dever seu munir-se das ferramentas necessárias para que tal aconteça. O Direito e a evolução têm de continuar a andar lado a lado, por muito que a evolução tecnológica, célere e disruptiva, torne esta tarefa difícil. Sendo quase certo que o caminho que tomámos é um caminho sem retorno e uma realidade à qual não podemos fugir[59], é nevrálgico que os juristas acompanhem esta nova realidade, de preferência, antecipando os problemas que poderão surgir: se não os anteciparem, mais tarde terão de os resolver.

§25. Havendo casos omissos não previstos pela lei, mas verificando-se já a possibilidade, perante o *status quo*, de os prever e prevenir, pelos danos resultantes de tais lacunas deverá responder a entidade que não os acautelou. É precisamente o caso em estudo: a computação quântica está a um passo de substituir os computadores tradicionais e acarreta novas possibilidades que, se não reguladas, representam um perigo à segurança e proteção dos dados em geral[60]. *In casu*, considerando que a Administração Pública procura expandir o seu acesso a dados pessoais aumentando o seu poder informacional, é de sua responsabilidade manter afastado o risco de violação dos direitos dos cidadãos, já que num Estado Democrático, em que o exercício do poder se baseia na participação popular, se revela de especial relevo a proteção dos interesses da população.

§26. Em todo o caso, será sempre impossível projetar um sistema perfeito, sem erros e imprecisões, que torne obsoleta a possibilidade de litígios e danos. Mesmo sem culpa[61], haverá de se encarregar a Administração pela responsabilidade inerente ao armazenamento e proteção de dados sensíveis, suportando os riscos consequentes e protegendo-se, assim, no mínimo, o direito à privacidade dos indivíduos.

[59] Atualmente, o indivíduo encontra-se, muitas das vezes, obrigado a fornecer dados e informações pessoais para que possa aceder a serviços públicos básicos.
[60] Que se tornaram um valioso recurso, sendo cada vez mais transacionáveis.
[61] À luz do princípio *ubi commoda, ibi incommoda*.