



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
CONCLUSÃO DE CURSO
ARTIGO CIENTÍFICO

CRIPTOMOEDA O MARCO LEGAL:
SEGURANÇA JURÍDICA, DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS

ORIENTANDO (A) - ADRIANO HOHL FILHO
ORIENTADOR (A) - MESTRA. FRANCISLENE PEREIRA DA SILVA

GOIÂNIA-GO
2025

ADRIANO HOHL FILHO

CRIPTOMOEDA O MARCO LEGAL:

SEGURANÇA JURÍDICA, DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito , Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS). Prof. (a) Orientador (a) - Mestra Francislene Pereira Da Silva.

GOIÂNIA-GO

2025

ADRIANO HOHL FILHO

CRIPTOMOEDA O MARCO LEGAL:
SEGURANÇA JURÍDICA, DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS

Data da Defesa: _____ de _____ de _____

BANCA EXAMINADORA

Orientador (a): Prof (a): Mestra. Francislene Pereira Da Silva	Nota
--	------

Examinador (a) Convidado (a): Prof. (a):. Ms. Sílvia Maria Gonçalves Santos de Lacerda Santana Curvo	Nota
---	------

CRIPTOMOEDA O MARCO LEGAL:

SEGURANÇA JURÍDICA, DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS

Adriano Hohl Filho¹

O presente artigo analisa a tensão existente entre o Marco Legal dos Criptoativos (Lei nº 14.478/2022) e a Lei Geral de Proteção de Dados (LGPD), especialmente após a proteção de dados ser elevada a direito fundamental pela Emenda Constitucional nº 115/2022. A partir de metodologia dedutiva, bibliográfica e documental, o estudo aprofunda o conflito entre as características técnicas da blockchain, em especial sua imutabilidade, e os direitos assegurados aos titulares pela LGPD, como a possibilidade de correção e eliminação de informações. Demonstra-se que, embora o Marco Legal busque prevenir ilícitos financeiros por meio das obrigações de KYC, sua implementação resulta na centralização de grandes volumes de dados pessoais sensíveis em Prestadores de Serviços de Ativos Virtuais (PSVAs), tornando-os alvos valiosos para ciberataques e elevando o risco de desanonimização dos usuários. Conclui-se que o Marco Legal, isoladamente, não oferece proteção suficiente à privacidade e aos dados pessoais, configurando possível inconstitucionalidade por proteção deficiente, sendo necessária uma atuação coordenada entre o Banco Central do Brasil (BCB) e a Autoridade Nacional de Proteção de Dados (ANPD) para harmonizar transparência e garantias fundamentais.

Palavras-chave: Criptomoedas; Marco legal; Privacidade; Proteção de dados; Segurança jurídica.

CRYPTOCURRENCY THE LEGAL: FRAMEWORK

LEGAL CERTAINTY, RIGHT TO PRIVACY AND DATA PROTECTION

This article examines the conflict between Brazil's Legal Framework for Cryptoassets and the General Data Protection Law (LGPD), especially after data protection became a constitutional fundamental right. It highlights the tension between blockchain's immutable design and LGPD rights, such as data correction and deletion. Although the framework aims to prevent financial crimes through KYC requirements, it unintentionally centralizes large amounts of sensitive personal data in Virtual Asset Service Providers, increasing cybersecurity risks and the possibility of user de-anonymization. The study concludes that the framework alone does not adequately protect privacy and data rights, making coordinated regulation by the Central Bank and the National Data Protection Authority essential.

Keywords: Cryptocurrencies; Legal framework; Privacy; Data protection; Legal certainty.

¹ Graduando do 9º Período do Curso de Direito da Pontifícia Universidade Católica de Goiás (PUC-GO).

INTRODUÇÃO

O advento das criptomoedas representa uma das mais significativas revoluções tecnológicas e financeiras do século XXI, desafiando paradigmas consolidados do sistema monetário tradicional. No Brasil, o crescimento exponencial do mercado de ativos digitais evidencia a necessidade urgente de um arcabouço regulatório capaz de equilibrar a inovação com a proteção dos direitos dos cidadãos. Nesse contexto, a promulgação da Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais ao status de direito fundamental, configura um marco jurídico transformador. Essa alteração na Carta Magna impõe uma reavaliação crítica de toda a legislação relacionada ao tratamento de dados, com especial atenção ao nascente Marco Legal dos Criptoativos, instituído pela Lei nº 14.478/2022.

O artigo científico aqui desenvolvido está inserido na linha de pesquisa Estado, Relações Sociais e Transformações Constitucionais do Curso de Direito da PUC Goiás, com o objetivo de discutir a projeção dos direitos fundamentais e refletir as transformações do estado constitucional, analisando a tensão entre o Marco Legal dos Criptoativos e a garantia da autodeterminação informativa frente aos riscos de inconstitucionalidade por proteção deficiente.

A tensão existente entre o propósito original de muitas criptomoedas, que é garantir pseudoanonimato e autonomia, e as exigências estatais de transparência e controle voltadas à prevenção de ilícitos financeiros, constitui um dos mais complexos desafios jurídicos contemporâneos. Com a Emenda Constitucional nº 115/2022, essa tensão ultrapassa o campo da política legislativa e passa a configurar uma questão de direitos fundamentais, tornando a presente análise não apenas oportuna, mas também constitucionalmente necessária. Diante disso, o presente trabalho busca responder à seguinte questão de pesquisa: à luz da constitucionalização da proteção de dados como direito fundamental autônomo, o marco regulatório brasileiro de criptoativos, estabelecido pela Lei nº 14.478/2022, oferece salvaguardas eficazes para a segurança jurídica e a privacidade financeira do consumidor (titular de dados) ou incorre em inconstitucionalidade por proteção deficiente?

Para responder a essa indagação, o objetivo geral é analisar a efetividade do referido marco legal, avaliando a segurança jurídica oferecida sob o novo prisma constitucional. Os objetivos específicos incluem examinar o conflito entre descentralização e regulação, avaliar a compatibilidade do Marco Legal com os princípios da Lei Geral de

Proteção de Dados (LGPD), agora dotada de fundamento constitucional direto, e propor aperfeiçoamentos regulatórios. A metodologia adotada é dedutiva, baseada em pesquisa bibliográfica e documental, com análise de doutrina, legislação e jurisprudência pertinentes. A estrutura do trabalho organiza-se em três seções: a primeira aborda os fundamentos das criptomoedas e a evolução da regulamentação brasileira; a segunda analisa o conflito entre a tecnologia e a LGPD sob o novo paradigma constitucional; e a terceira desenvolve uma análise crítica dos riscos ao consumidor, identificando as deficiências protetivas do marco legal e propondo melhorias regulatórias.

1 CRIPTOMOEDAS E MARCO REGULATÓRIO BRASILEIRO

Para compreender adequadamente a magnitude dos desafios regulatórios impostos pelos criptoativos, torna-se essencial dissecar seus fundamentos tecnológicos subjacentes, com especial atenção à arquitetura da *blockchain*.

A natureza desta tecnologia, pautada na descentralização, na criptografia avançada e na imutabilidade quase absoluta dos registros, não apenas desafia, mas colide frontalmente com os paradigmas jurídicos tradicionais de jurisdição, soberania e responsabilidade civil. Paralelamente, é imperativo analisar a trajetória da regulamentação no país, um percurso que demonstra o esforço contínuo, e frequentemente reativo, do Estado em tentar impor algum grau de controle sobre uma inovação desenhada especificamente para operar à margem da intermediação tradicional. Este esforço de enquadrar o disruptivo em moldes jurídicos preexistentes, que foram concebidos para um ecossistema financeiro totalmente centralizado, é a fonte primária das fricções que se analisarão.

É precisamente dessa incompatibilidade fundamental entre a arquitetura da confiança distribuída e a lógica do controle centralizado que emergem os riscos mais agudos para os direitos fundamentais, notadamente a privacidade e a proteção de dados, que constituem o cerne da presente investigação.

1.1 FUNDAMENTOS TECNOLÓGICOS DAS CRIPTOMOEDAS

A tecnologia *blockchain* é frequentemente descrita como um mecanismo de

banco de dados avançado, mas é mais preciso defini-la como um Livro-Razão Distribuído (DLT). Essa tecnologia permite o compartilhamento transparente de informações por meio de uma rede *peer-to-peer*, armazenando dados em blocos criptograficamente interligados em uma cadeia cronológica. O conceito de criptomoeda foi introduzido em 2008 com o Bitcoin, que propôs um sistema de dinheiro eletrônico puramente *peer-to-peer*, projetado para operar sem a necessidade de intermediários financeiros, fundamentando-se na descentralização, na criptografia assimétrica e no consenso distribuído. Nesse sistema, a segurança é garantida pela posse de chaves criptográficas privadas, que autorizam as transações, enquanto as chaves públicas funcionam como endereços de recebimento. Novas moedas são criadas e transações são validadas por meio do processo de mineração.

Duas características dessa tecnologia são centrais para o debate jurídico. A primeira é a imutabilidade, alcançada porque cada novo bloco na cadeia contém um *hash* criptográfico do bloco anterior, criando uma sequência interligada em que a modificação de um bloco anterior invalidaria, em cascata, todos os blocos subsequentes. Em redes públicas robustas, essa reversão é considerada computacionalmente inviável. Essa rigidez, embora garanta a integridade do sistema, é a principal fonte de conflito com a Lei Geral de Proteção de Dados (LGPD), que assegura aos titulares o direito de correção e eliminação de dados pessoais.

A segunda característica é o pseudoanonimato. A identidade de um usuário em uma *blockchain* pública não está vinculada a um nome legal ou CPF, mas a um endereço criptográfico, correspondente à sua chave pública. Contudo, e este é um ponto crucial para a presente análise, essa camada de privacidade é intrinsecamente frágil. O elo entre o mundo *on-chain* e a identidade *off-chain* é estabelecido no momento em que o usuário se cadastra em uma *exchange* (PSVA). Ao cumprir as regulamentações de “Conheça seu Cliente” (KYC), o usuário é obrigado a vincular seu endereço pseudoanônimo a uma identidade verificada no mundo real. A partir desse instante, a transparência radical da *blockchain*, que permite a auditoria pública de todas as transações, transforma-se em um instrumento potencial de vigilância. Passa a ser plenamente possível, por meio de técnicas de análise de *blockchain*, rastrear e associar permanentemente todo o histórico de transações àquela identidade específica, em um processo de desanonimização que expõe integralmente a vida financeira do indivíduo.

1.2 A NATUREZA DESCENTRALIZADA E O PARADIGMA DA PRIVACIDADE

A descentralização é, de fato, a característica mais distintiva e filosoficamente disruptiva das criptomoedas. Ela representa a transferência do controle e da tomada de decisão de uma entidade central, como um banco ou um governo, para uma rede distribuída e algorítmica. Essa arquitetura, por sua natureza, possibilita diferentes níveis de privacidade, que variam desde o mero pseudoanonimato do Bitcoin, no qual as transações são públicas, até o anonimato mais robusto de criptomoedas voltadas à privacidade, como Zcash ou Monero. Se, por um lado, a ausência de um centro confere uma inédita resistência à censura e ao controle arbitrário, por outro, e de forma previsível, essa mesma característica facilita a prática de atividades ilícitas. É nesse ponto que se estabelece a tensão fundamental com a necessidade de transparência regulatória exigida pelo Estado, especialmente para fins de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (CFT).

Essa dinâmica revela um paradoxo essencial que frequentemente ilude os usuários. Muitos são atraídos para as criptomoedas pela promessa de privacidade e autonomia; contudo, a tecnologia subjacente às principais delas, notadamente o Bitcoin, é construída sobre um princípio de transparência radical e permanente: um livro-razão publicamente auditável por qualquer pessoa no mundo. A privacidade, nesse ecossistema, não decorre do sigilo da transação, mas depende inteiramente da frágil desvinculação entre o endereço *on-chain* (a chave pública) e a identidade *off-chain* (o indivíduo no mundo real).

A resposta regulatória global, materializada no Marco Legal brasileiro, incide precisamente sobre esse elo. Ela impõe uma recentralização forçada ao exigir que os intermediários, como as exchanges, vinculem o endereço pseudoanônimo a uma identidade real e verificada por meio dos procedimentos de “Conheça seu Cliente” (KYC). Essa exigência não apenas elimina a privacidade originalmente pretendida, mas também expõe, de forma permanente e retroativa, toda a vida financeira do indivíduo.

1.3 EVOLUÇÃO DA REGULAMENTAÇÃO BRASILEIRA DE CRIPTOATIVOS

A trajetória regulatória brasileira no campo dos criptoativos não foi proativa, mas reativa, evoluindo gradualmente com foco na fiscalização e no controle dos intermediários. O primeiro movimento estatal significativo foi a Instrução Normativa RFB nº 1.888/2019, que impôs uma obrigação declaratória de natureza essencialmente arrecadatória e fiscalizatória, obrigando *exchanges* e usuários a reportar suas operações à Receita Federal.

O avanço legislativo subsequente, a Lei nº 14.478/2022, instituiu o tão aguardado marco legal do setor. Contudo, a análise de seu conteúdo revela a manutenção da mesma prioridade: a lei atribuiu ao Banco Central do Brasil (BCB) a competência para regulamentar e supervisionar os Prestadores de Serviços de Ativos Virtuais (PSVAs), tipificou o crime de fraude com ativos virtuais e concentrou-se na regulação dos intermediários do mercado. O objetivo declarado é o combate a crimes financeiros e a proteção do consumidor, alinhando-se a padrões internacionais de supervisão financeira concebidos em sua maioria antes da elevação da proteção de dados ao status de direito fundamental no Brasil.

Essa regulação converge diretamente, e de forma acrítica, com as recomendações do Grupo de Ação Financeira (GAFI), que buscam aplicar as tradicionais e centralizadoras obrigações de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/FT) a um setor tecnologicamente novo e descentralizado. O ponto central e mais controverso dessa convergência é a implementação da “Travel Rule”, correspondente à Recomendação 16 do GAFI. Essa regra exige que os PSVAs não apenas obtenham e retenham dados por meio do procedimento de “Conheça seu Cliente” (KYC), mas também transmitam ativamente informações sobre o remetente e o destinatário de transferências de ativos virtuais acima de um determinado valor. Essa exigência transforma a coleta estática de dados do KYC em uma obrigação de compartilhamento dinâmico, contínuo e interinstitucional.

É nesse ponto que se materializa o conflito com a Lei Geral de Proteção de Dados (LGPD), pois a “*Travel Rule*” colide frontalmente com o princípio da minimização, ao demandar o compartilhamento de um vasto conjunto de dados; com o princípio da finalidade, ao criar um novo propósito de vigilância interbancária; e com o princípio da segurança, ao ampliar exponencialmente a superfície de ataque para vazamentos de informações sensíveis.

Desde a promulgação da lei, o avanço da regulamentação infralegal pelo BCB tem reforçado essa priorização. As Consultas Públicas nº 109, 110 e 111 de 2024, por exemplo, concentram-se de maneira exaustiva em aspectos prudenciais. Elas detalham regras para o funcionamento dos PSVAs, como exigências de capital mínimo e de governança, o complexo processo de autorização para operar no país e a integração ao mercado de câmbio. O que se observa, contudo, é um silêncio sintomático: ao priorizar a estabilidade financeira e a autorização dos agentes do mercado, o regulador demonstra uma omissão preocupante em abordar as complexas intersecções com a LGPD, tratando o risco de dados como um problema secundário, e não como o pilar central da regulação, como seria de se esperar após a Emenda Constitucional nº 115/2022.

2 PROTEÇÃO DE DADOS E PRIVACIDADE NO CONTEXTO DAS CRIPTOMOEDAS

A intersecção entre a arquitetura tecnológica da *blockchain* e o regime jurídico da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) não gera meras tensões, mas um antagonismo jurídico profundo e complexo. Esse conflito latente foi significativamente intensificado e elevado a um patamar constitucional com a promulgação da Emenda Constitucional nº 115/2022. Tal emenda não representou uma simples adição normativa; ela instaurou um novo paradigma ao consolidar a proteção de dados como um direito fundamental autônomo, conferindo à LGPD uma força normativa de natureza constitucional que exige uma releitura de toda a legislação infraconstitucional, incluindo o Marco Legal dos Criptoativos. O cerne desse conflito reside na aparente incompatibilidade entre as características estruturais de cada sistema.

De um lado, encontra-se a *blockchain*, cuja lógica se sustenta na imutabilidade, na transparência radical e na descentralização, com o propósito de eliminar a necessidade de um agente central. De outro, está a LGPD, agora dotada de status constitucional, fundada precisamente na existência de agentes de tratamento identificáveis (o controlador e o operador) e na garantia de direitos flexíveis aos titulares, como a retificação, a oposição e, sobretudo, a eliminação de dados.

2.1 O NOVO PARADIGMA CONSTITUCIONAL: DA PRIVACIDADE À AUTODETERMINAÇÃO INFORMATIVA

Historicamente, a proteção da esfera pessoal no Brasil era fundamentada de forma restritiva no artigo 5º, inciso X, da Constituição. Essa cláusula assegura a inviolabilidade da intimidade e da vida privada, mas sua interpretação tradicional limitava-se a uma concepção puramente defensiva, o chamado "direito de ser deixado em paz" (*the right to be left alone*), voltado a impedir a intrusão de terceiros. A ascensão da sociedade da informação, contudo, tornou essa visão anacrônica. Em um contexto em que os dados pessoais se transformaram no principal ativo econômico e em um poderoso instrumento de vigilância, a proteção não poderia mais ser passiva; ela exigiu uma evolução para o conceito de autodeterminação informativa.

Esse novo paradigma, importado do direito constitucional alemão, não representa apenas um escudo, mas também uma espada: confere ao indivíduo o controle

ativo e positivo sobre o fluxo de seus dados, garantindo-lhe o direito de saber quem os detém, para quais finalidades são utilizados e, sobretudo, o poder de retificá-los ou eliminá-los.

O Supremo Tribunal Federal (STF) demonstrou notável sensibilidade a essa transformação, mesmo antes da atuação do legislador constituinte. No julgamento da ADI 6387, que suspendeu os efeitos da Medida Provisória nº 954/2020, a qual previa o compartilhamento massivo de dados de telecomunicações com o IBGE, a Corte reconheceu a existência de um direito fundamental autônomo à proteção de dados. O STF derivou tal direito da dignidade da pessoa humana e da interpretação conjunta dos incisos X (privacidade) e XII (sigilo de dados) do artigo 5º da Constituição.

A Emenda Constitucional nº 115/2022, portanto, não criou esse direito, mas consolidou essa vanguarda jurisprudencial, conferindo-lhe assento explícito no rol dos direitos fundamentais. Ao inserir o inciso LXXIX no artigo 5º, a emenda tornou a proteção de dados uma cláusula pétrea, imune até mesmo a propostas de emenda que visem à sua abolição. Esse movimento possui uma consequência prática de grande magnitude: confere fundamento constitucional direto e inequívoco à Lei Geral de Proteção de Dados, fortalecendo sua hierarquia normativa. Assim, qualquer análise de leis infraconstitucionais, como o Marco Legal dos Criptoativos, que conflite com a LGPD, deixa de configurar um mero debate legal e passa a representar uma violação constitucional direta.

2.2 O CONFLITO TÉCNICO-JURÍDICO: IMUTABILIDADE VS. DIREITOS DO TITULAR

O conflito técnico-jurídico entre a *blockchain* e a LGPD, agora um conflito de nível constitucional, manifesta-se em duas frentes principais: imutabilidade contra direitos do titular e descentralização contra responsabilidade. A imutabilidade, concebida como a maior virtude da *blockchain* para garantir a integridade e a audibilidade dos registros, colide frontalmente com os direitos fundamentais do titular de dados, previstos no artigo 18 da LGPD. Direitos como a eliminação e a correção de informações pessoais não encontram apenas um obstáculo; eles encontram uma impossibilidade técnica. Em uma rede *blockchain* pública, a exclusão de um dado, uma vez validado e encadeado em um bloco, é computacionalmente inviável sem comprometer a integridade de toda a cadeia. Na prática, o "direito ao esquecimento" é efetivamente anulado, e o direito à retificação torna-se uma barreira quase intransponível, transformando garantias constitucionais em mera ficção jurídica no contexto *on-chain*.

Adicionalmente, todo o sistema de freios e contrapesos da LGPD fundamenta a responsabilidade nas figuras jurídicas do controlador e do operador de dados. A lei exige agentes de tratamento identificáveis que definam a finalidade e os meios do processamento. Contudo, em redes descentralizadas, a própria arquitetura é desenhada para eliminar entidades centrais, tornando a identificação desses agentes um desafio conceitual significativo. Mineradores ou nós da rede, que apenas validam transações de forma automatizada e distribuída, não se enquadram claramente na definição de controlador, pois seu papel é puramente técnico (executar o código e validar o consenso) e não decisório; eles não definem a finalidade do tratamento dos dados pessoais que, incidentalmente, validam. Essa indefinição estrutural, inerente à descentralização, cria um perigoso vácuo de responsabilidade, dificultando a aplicação das sanções previstas na lei e, mais criticamente, tornando o exercício dos direitos pelos titulares inexecutável, pois eles não encontram um destinatário claro para suas requisições.

É crucial, no entanto, distinguir o tipo de rede. O conflito é agudo e mais relevante em *blockchains* públicas e não permissionadas, como a do Bitcoin, que são o objeto principal da inovação financeira. Em *blockchains* privadas ou permissionadas, frequentemente adotadas em ambientes corporativos, o acesso controlado e a governança centralizada facilitam a identificação de responsáveis e a implementação de mecanismos de conformidade, mitigando o conflito com a LGPD. Contudo, esta solução trai a própria filosofia de descentralização que define o fenômeno das criptomoedas.

3 SEGURANÇA JURÍDICA E PROTEÇÃO DOS USUÁRIOS BRASILEIROS

Embora a Lei nº 14.478/2022 represente um avanço formal para a segurança jurídica do mercado, ao estabelecer regras de autorização e supervisão para os PSVAs, sua arquitetura revela uma priorização unilateral. A ênfase esmagadora da norma recai sobre a regulação financeira prudencial e a prevenção a crimes financeiros, importando a lógica do sistema tradicional para um novo paradigma tecnológico. Essa abordagem, no entanto, foi construída sobre um preocupante silêncio legislativo: ela falha em endereçar adequadamente as complexidades técnicas da *blockchain* e sua colisão direta com a LGPD, que, como visto, foi alçada ao status de direito fundamental. Este vácuo não é uma omissão trivial; ele gera riscos severos e vulnerabilidades concretas para os milhões de brasileiros que investem nesses ativos, deixando-os desprotegidos exatamente onde o novo paradigma constitucional exigia maior tutela.

3.1 A CRIAÇÃO DE "HONEYPOTS" E O RISCO DE VAZAMENTOS

O principal e mais previsível risco da nova legislação decorre diretamente da obrigação imposta aos PSVAs de implementarem rigorosos procedimentos de "Conheça seu Cliente" (KYC). Esta exigência legal força a coleta e o armazenamento centralizado de um volume extraordinário de dados pessoais e sensíveis, que vão muito além do nome e CPF, incluindo frequentemente biometria (como *selfies* de verificação de identidade), comprovantes de residência e, por vezes, informações patrimoniais detalhadas. Ao impor essa centralização, o próprio Marco Legal converte as *exchanges* em "*honeypots*" (potes de mel). Elas se tornam, por mandato estatal, alvos de altíssimo valor para ataques cibernéticos, possuindo um potencial devastador para vazamentos em massa, muito mais perigosos do que vazamentos de credenciais comuns, pois contêm o conjunto completo de dados necessários para fraudes de identidade complexas.

Este perigo não é, de forma alguma, teórico, mas uma realidade estatística. O caso da *fintech* brasileira Atlas Quantum, que em 2018 expôs dados de 264 mil clientes, ilustra perfeitamente o perigo em solo nacional, demonstrando a vulnerabilidade mesmo antes de a plataforma ser subsequentemente revelada como um esquema de pirâmide. Contudo, os ataques a gigantes internacionais demonstram a escala sistêmica desta vulnerabilidade. O ataque à *Bybit*, que levou a perdas financeiras astronômicas, revela a intensidade e os recursos empregados por criminosos contra esses alvos. Mais alarmante, o caso da *Coinbase* expõe uma faceta ainda mais perigosa: ali, hackers subornaram funcionários para obter dados de clientes. Este incidente prova que a superfície de ataque não é apenas digital; os *honeypots* criados pela lei são vulneráveis também a falhas humanas e ataques de engenharia social, tornando a proteção eficaz desses dados uma tarefa hercúlea que o legislador impôs, mas para a qual não proveu salvaguardas proporcionais.

3.2 A AMEAÇA DA DESANONIMIZAÇÃO E A INCONSTITUCIONALIDADE POR PROTEÇÃO DEFICIENTE

A ameaça da desanonimização é, talvez, o risco mais subestimado pelo legislador e o que possui as consequências mais graves e irreversíveis. A combinação dos

dados de KYC, que estabelecem a identidade civil verificada do indivíduo, com as ferramentas de análise forense de transações na *blockchain*, que é um livro-razão público, transparente e eterno, permite a desanonimização completa e retroativa dos usuários. O elo, uma vez criado, expõe todo o histórico financeiro do indivíduo, passado e futuro, de forma indelével, aniquilando a privacidade que muitos originalmente buscaram nesse sistema. A transparência radical da tecnologia, quando atrelada a uma identidade real, cria um mapa público da riqueza. Essa exposição cria riscos graves e concretos de crimes direcionados, como sequestro, extorsão e fraude de identidade, pois os criminosos podem identificar e classificar alvos com base em seus saldos publicamente visíveis.

Sob a ótica constitucional, é precisamente aqui que a Lei nº 14.478/2022 incorre em inconstitucionalidade por proteção deficiente. Este vício, derivado da doutrina do *Untermassverbot* (proibição da proteção insuficiente), ocorre quando o Estado falha em seu dever positivo de tutela. Um direito fundamental, especialmente um recém-constitucionalizado como o da proteção de dados (EC nº 115/2022), não impõe ao Estado apenas um dever de abstenção (não violar), mas um dever positivo (*Schutzpflicht*) de criar ativamente as condições para sua proteção efetiva. O paradoxo é que o legislador, ao impor um dever (a coleta massiva de dados via KYC), gerou um risco severo, iatrogênico e perfeitamente previsível, transformando PSVAs em *honeypots*. Sem, contudo, estabelecer salvaguardas robustas, tecnologicamente avançadas e proporcionais para mitigar esse mesmo risco que criou, o legislador foi omissos. Essa omissão parcial não é um detalhe técnico; ela viola a essência do direito fundamental que a lei, ironicamente, alega observar, tornando-se um instrumento que, na prática, expõe o consumidor a mais riscos do que o protege.

CONCLUSÃO

O marco legal brasileiro dos criptoativos, inaugurado pela Lei nº 14.478/2022, constitui um passo essencial para conferir segurança jurídica ao mercado em expansão. Contudo, a presente análise demonstrou que a legislação, ao focar-se obsessivamente em aspectos prudenciais e de prevenção a ilícitos, mostra-se não apenas insuficiente, mas constitucionalmente deficiente para, de forma isolada, garantir a proteção efetiva dos direitos fundamentais à privacidade e aos dados pessoais. Essa falha é particularmente grave após a elevação da proteção de dados a direito fundamental pela EC nº 115/2022. A tensão irresolvida entre a imutabilidade da *blockchain* e os direitos da LGPD, somada à

criação estatal de "*honeypots*" de dados nos PSVAs e ao risco de desanonimização, cria uma zona de incerteza que expõe os usuários a riscos desproporcionais, configurando a inconstitucionalidade por proteção deficiente.

Conclui-se, portanto, que a consolidação de um ambiente de inovação seguro no Brasil depende de um aperfeiçoamento regulatório urgente e tecnicamente informado. O caminho para essa correção exige, em primeiro lugar, uma atuação coordenada entre o Banco Central do Brasil e a Autoridade Nacional de Proteção de Dados (ANPD). É imperativa a criação de normas complementares, elaboradas em conjunto, que finalmente harmonizem as exigências de transparência financeira com as garantias fundamentais de privacidade. A atuação da própria ANPD no caso Worldcoin, onde suspendeu a coleta de dados biométricos por vício de consentimento, exemplifica seu papel crucial e indelegável neste ecossistema.

Esta atuação coordenada, contudo, não deve limitar-se a textos normativos, mas deve incentivar ativamente a adoção de Tecnologias de Aprimoramento da Privacidade (PETs). A regulação deve ir além da mera sanção, fomentando soluções que permitam o cumprimento da lei sem a violação de direitos. Em especial, as provas de conhecimento-zero (*Zero-Knowledge Proofs* - ZKPs) surgem como a solução técnica mais elegante: elas permitem a um usuário provar uma afirmação (como sua idade ou a origem de um fundo) sem revelar o dado subjacente, cumprindo os requisitos regulatórios enquanto aderem estritamente ao princípio da minimização de dados da LGPD. Criptomoedas como a Zcash (ZEC) já implementam essa tecnologia, provando sua viabilidade prática.

Enquanto tais soluções tecnológicas avançadas não são universalmente adotadas, torna-se essencial um dever imediato de transparência e educação do consumidor. A regulação deve exigir que os PSVAs eduquem os consumidores de forma clara e ostensiva sobre os riscos reais e permanentes da imutabilidade da blockchain e da possibilidade de desanonimização, em estrita conformidade com o Código de Defesa do Consumidor.

Somente através de uma abordagem regulatória que reconheça a proteção de dados não como um obstáculo à inovação, mas como o pilar central da confiança e da segurança jurídica, o Brasil poderá equilibrar o fomento à tecnologia e a salvaguarda efetiva dos direitos dos cidadãos neste novo paradigma financeiro digital.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD** determina suspensão de incentivos financeiros por coleta de íris. Gov.br, 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-de-incentivos-financeiros-por-coleta-de-iris>. Acesso em: 30 set. 2025.

ÁVILA, Humberto. **Segurança Jurídica: Entre permanência, mudança e realização no Direito Tributário**. São Paulo: Malheiros, 2011.

BANCO CENTRAL DO BRASIL. Consulta Pública nº 109/2024. Proposta de regulamentação da prestação de serviços de ativos virtuais (PSAVs). Brasília, DF: Banco Central do Brasil, 2024. Disponível em: <https://www.gov.br/participamaisbrasil/edital-de-participacao-social-n-109-2024-proposta-de-regulamentacao-do->. Acesso em: 30 set. 2025.

BANCO CENTRAL DO BRASIL. Consulta Pública nº 110/2024. **Proposta de regulamentação dos processos de autorização das SPSAVs, SCCs, SCTVMs e SDTVMs**. Brasília, DF: Banco Central do Brasil, 2024. Disponível em: <https://www.gov.br/participamaisbrasil/edital-de-participacao-social-n-110-2024-proposta-de-regulamentacao-do->. Acesso em: 30 set. 2025.

BANCO CENTRAL DO BRASIL. Consulta Pública nº 111/2024. **Proposta de regulamentação da inclusão de serviços de ativos virtuais no mercado de câmbio**. Brasília, DF: Banco Central do Brasil, 2024. Disponível em: <https://www.gov.br/participamaisbrasil/consulta-publica-n-111>. Acesso em: 30 set. 2025.

BARBOSA, Rafael. **Bitcoin: dados pessoais de 264 mil brasileiros vazam de fintech nacional**. Tudocelular.com, 2018. Disponível em: <https://www.tudocelular.com/seguranca/noticias/n129866/bitcoin-dados-264-mil-brasileiros-vazam-fintech.html>. Acesso em: 30 set. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais [...]. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 30 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 set. 2025.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. **Dispõe sobre as diretrizes a serem observadas na prestação de serviços de ativos virtuais [...]**. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14478.htm. Acesso em: 30 set. 2025.

BRASIL. Receita Federal do Brasil. **Instrução Normativa RFB nº 1.888, de 3 de maio de 2019**. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos. Brasília, DF: Receita Federal do Brasil, 2019.

Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-rfb-n-1.888-de-3-de-maio-de-2019-155554580>. Acesso em: 30 set. 2025.

BRASIL. **Supremo Tribunal Federal**. Ação Direta de Inconstitucionalidade n.º 6.387/DF. Relatora: Ministra Rosa Weber. Julgamento em 07 maio 2020. Diário da Justiça Eletrônico, Brasília, DF, 12 maio 2020.

BRUMMER, Chris. **Cryptoassets: Legal, Regulatory, and Monetary Perspectives**. Oxford: Oxford University Press, 2019.

CAMPOS, Emília Malgueiro. **Criptoativos e Regulação Financeira**. São Paulo: Almedina, 2022.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Processo Administrativo Sancionador CVM nº 19957.011029/2019-64**. Gov.br, 2024. Disponível em: https://conteudo.cvm.gov.br/export/sites/cvm/sancionadores/sancionador/anexos/2024/SEI_19957011029_2019_64.pdf. Acesso em: 30 set. 2025.

DE FILIPPI, Primavera; WRIGHT, Aaron. **Blockchain and the Law: the rule of code**. Cambridge: Harvard University Press, 2018.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FINCK, Michèle. **Blockchain Regulation and Governance in Europe**. Cambridge: Cambridge University Press, 2019.

HACKEN. **Crypto Travel Rule: Global VASP Requirements in 2025**. Hacken.io, 2025. Disponível em: <https://hacken.io/discover/crypto-travel-rule/>. Acesso em: 30 set. 2025.

INFOMONEY. **Corretora cripto Bybit sofre maior hack da história e perde quase US\$ 1,5 bi**. InfoMoney, 2025. Disponível em: <https://www.infomoney.com.br/mercados/2a-maior-corretora-cripto-do-mundo-bybit-perde-us-15-bi-em-maior-hack-da-historia/>. Acesso em: 30 set. 2025.

IPLD. **Criptoativos e as Recomendações do GAFI. Instituto de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo**, [s.d.]. Disponível em: <https://ipld.com.br/series/criptoativos-recomendacoes-do-gafi/>. Acesso em: 30 set. 2025.

KRIPTOBR. ZCash (ZEC): **Privacidade e Segurança na Era das Criptomoedas**. KriptoBR, [s.d.]. Disponível em: <https://kriptobr.com/zcash-zec-privacidade-e-seguranca-na-era-das-criptomoedas/>. Acesso em: 30 set. 2025.

LESSIG, Lawrence. **Code and Other Laws of Cyberspace**. 2. ed. New York: Basic Books, 2006.

NARAYANAN, Arvind et al. **Bitcoin and Cryptocurrency Technologies**. Princeton: Princeton University Press, 2016.

PARENTONI, Leonardo. **Moedas Virtuais: aspectos jurídicos e econômicos**. São Paulo: Quartier Latin, 2021.

QUEIROZ, Luiz. ANPD: **blockchain não está 100% em conformidade com a LGPD**. Capital Digital, 2023. Disponível em: <https://capitaldigital.com.br/anpd-blockchain-nao-esta-100-em-conformidade-com-a-lgpd/>. Acesso em: 30 set. 2025.

SCORECHAIN. **Crypto Compliance and Travel Rule Regulations in Brazil**. Scorechain, [s.d.]. Disponível em: <https://www.scorechain.com/resources/crypto-glossary/crypto-travel-rule-compliance-brazil>. Acesso em: 30 set. 2025.

SEU DINHEIRO. **Coinbase é vítima de vazamento de dados e se recusa a pagar US\$ 20 milhões a criminosos; veja que informações foram expostas**. Seu Dinheiro, 2025. Disponível em: <https://www.seudinheiro.com/2025/criptomoedas/coinbase-e-vitima-de-vazamento-de-dados-e-se-recusa-a-pagar-us-20-milhoes-a-criminosos-veja-que-informacoes-foram-expostas-gcsb/>. Acesso em: 30 set. 2025.

WERBACH, Kevin. **The Blockchain and the New Architecture of Trust**. Cambridge: MIT Press, 2018.

WIKIPEDIA. **Zcash**. Wikipédia, a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/Zcash>. Acesso em: 30 set. 2025.