III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

T255
Tecnologias disruptivas, direito e proteção de dados II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Tais Ramos, Caio Augusto Souza Lara e Rubens Beçak – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-376-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 3 discute os impactos das tecnologias destrutivas no campo jurídico, com foco na aplicação da Lei Geral de Proteção de Dados e nas novas fronteiras da privacidade digital. As apresentações analisam o papel da inovação, da transparência e da responsabilidade jurídica em contextos digitais complexos. O grupo contribui para o debate sobre como a tecnologia pode ser aliada na proteção da dignidade humana e da segurança informacional.

PRIVACIDADE, PROGRAMABILIDADE E DESCENTRALIZAÇÃO: UMA ANÁLISE DO TRILEMA TÉCNICO-JURÍDICO DO DREX

PRIVACY, PROGRAMMABILITY AND DECENTRALIZATION: AN ANALYSIS OF THE TECHNICAL-LEGAL TRILEMMA OF DREX

Clara Cristina De Barros [1]
Enzo Bondan de Lima [2]

Resumo

O Drex, moeda digital em desenvolvimento pelo Banco Central do Brasil, propõe a modernização da infraestrutura financeira nacional por meio da adoção de tecnologias como blockchain permissionada e provas criptográficas. No entanto, sua arquitetura enfrenta sérios desafios jurídicos e operacionais, especialmente quanto à concentração de poder, à limitação da programabilidade e à compatibilidade com a Lei Geral de Proteção de Dados. A pesquisa, fundamentada em revisão bibliográfica e análise documental, conclui que a efetiva implementação do Drex exige adaptações técnicas e revisão normativa para garantir segurança jurídica, transparência, rastreabilidade, governança democrática e proteção de direitos fundamentais.

Palavras-chave: Drex, Lgpd, Governança

Abstract/Resumen/Résumé

Drex, the digital currency under development by the Central Bank of Brazil, proposes to modernize the national financial infrastructure through the adoption of technologies such as permissioned blockchain and cryptographic proofs. However, its architecture faces serious legal and operational challenges, especially regarding power concentration, programmability limitations, and compatibility with the Brazilian General Data Protection Law (LGPD). Based on bibliographic review and documentary analysis, this research concludes that the effective implementation of Drex requires technical adjustments and regulatory revision to ensure legal certainty, transparency, traceability, democratic governance, and the protection of fundamental rights.

Keywords/Palabras-claves/Mots-clés: Drex, Lgpd, Governance

[1] Discente de Direito na UNIVAG. Extensionista do Nexo Governamental XI de Agosto da Faculdade de Direito da Universidade de São Paulo. E-mail: claracrsbarros@gmail.com. Lattes: http://lattes.cnpq.br /5743087718406198

[2] Discente de Ciência da Computação na UFMT. E-mail: enzo.bondan@gmail.com. Lattes: http://lattes.cnpq.br /5293690846570343

I. INTRODUÇÃO

A digitalização do sistema financeiro brasileiro tem avançado significativamente, e o Drex, projeto de moeda digital do Banco Central do Brasil, representa uma iniciativa estratégica nesse processo. Seu objetivo é estruturar uma infraestrutura digital capaz de modernizar o sistema financeiro, ampliar a inclusão e permitir a adoção de ativos programáveis e modelos inovadores de negócios. Inspirado em tecnologias como blockchain e contratos inteligentes, o Drex adota uma arquitetura permissionada, com contratos autoexecutáveis, mecanismos criptográficos de proteção de dados e um modelo de governança sob responsabilidade do Banco Central (Banco Central do Brasil, 2025, p. 28). Entre esses mecanismos, destacam-se as chamadas provas de conhecimento zero (ZKPs), que, conforme definido por Sheybani et al. (2025), são "primitivas criptográficas que permitem a um provador demonstrar conhecimento de um valor secreto a um verificador, sem revelar qualquer informação sobre o segredo em si", sendo amplamente utilizadas em soluções voltadas à privacidade e segurança digital.

Contudo, essa configuração tecnológica impõe desafios relevantes. A análise da arquitetura revela tensões entre os objetivos declarados do projeto, como privacidade, descentralização e programabilidade, e as limitações impostas pelo desenho técnico da solução (Banco Central do Brasil, 2025, p. 10-11). Entre os principais entraves identificam-se riscos relacionados à escalabilidade, à segurança da rede, à auditabilidade das operações e ao controle dos ativos digitais. Esses aspectos comprometem não apenas a eficiência do sistema, mas também sua conformidade com os parâmetros jurídicos exigidos para a operação de uma infraestrutura financeira estatal.

Diante desse cenário, esta pesquisa propõe uma análise crítica dos principais problemas estruturais do Drex, com atenção especial às suas implicações práticas e jurídicas no contexto brasileiro.

II. OBJETIVOS

O objetivo deste trabalho é analisar as principais limitações técnicas da arquitetura do Drex com base no relatório publicado pelo Banco Central (Banco Central do Brasil, 2025). A pesquisa busca identificar os desafios relacionados à descentralização, à privacidade e à programabilidade, avaliando seus impactos na segurança, interoperabilidade e auditabilidade

do sistema. Pretende-se ainda discutir as contradições entre os princípios tecnológicos adotados e as decisões práticas de governança aplicadas à plataforma.

III. METODOLOGIA

A pesquisa foi realizada por meio de revisão bibliográfica, com base em livros, artigos, periódicos, legislações e documentos institucionais voltados à temática jurídico-regulatória.

Além da literatura, foi examinado o Relatório da Fase 1 do Piloto Drex (Banco Central do Brasil, 2025) como fonte documental principal. A partir dessa análise, delimitou-se o trilema técnico-jurídico envolvendo privacidade, programabilidade e descentralização, com fundamento na Lei nº 13.709/2018 (Brasil, 2018), a Lei Complementar nº 105/2001 (Brasil, 2001) e em princípios constitucionais aplicáveis à atividade estatal no campo econômico e informacional.

IV. DESENVOLVIMENTO

IV. I. ARQUITETURA DREX E LIMITAÇÕES DA PLATAFORMA

A arquitetura do Drex utiliza a blockchain permissionada Hyperledger Besu. A rede opera com 26 nós, sendo 10 administrados pelo Banco Central (BC). Destes, 6 atuam como validadores (responsáveis por processar transações e blocos), enquanto os 4 restantes atendem exclusivamente a aplicações internas do BC, sem participação no consenso. Os 16 nós remanescentes, controlados por instituições autorizadas, não são validadores. A topologia em estrela (Banco Central do Brasil, 2025, p. 30) subordina todos os nós não validadores exclusivamente aos validadores do BC. Trata-se de uma rede privada permissionada com controle institucional centralizado, operando na Rede do Sistema Financeiro Nacional (RSFN) sem conexão com a internet pública (Banco Central do Brasil, 2025, p. 29, 31).

O consenso é alcançado por meio do protocolo Quorum Byzantine Fault Tolerance, que exige a concordância de dois terços dos validadores. Embora proporcione certa segurança, esse modelo apresenta limitações operacionais, sobretudo em cenários com mais de 16 participantes, conforme apontado pelo relatório técnico (Banco Central do Brasil, 2025, p. 32). A inclusão de novos participantes e a definição de permissões permanecem sob controle exclusivo do Banco Central, o que reforça a centralização do sistema.

No campo da privacidade, o Drex incorpora técnicas como as provas de conhecimento zero (ZKP), que permitem verificar informações sem revelá-las diretamente. Essas tecnologias possibilitam, por exemplo, comprovar saldo suficiente para uma transação sem expor o valor total. No entanto, os testes indicaram atrasos consideráveis, inviabilizando seu uso em larga escala (Banco Central do Brasil, 2025, p. 36). Além disso, o aumento da proteção de dados pode dificultar a supervisão de autoridades e comprometer investigações relacionadas a fraudes e lavagem de dinheiro.

IV. II. PRIVACIDADE, SIGILO E TRATAMENTO DE DADOS NO AMBIENTE DO DREX

A implementação do Drex impõe desafios significativos à proteção de dados pessoais, especialmente no que tange à conformidade com a Lei Geral de Proteção de Dados (Brasil, 2018) e à Lei Complementar nº 105/2001, que trata do sigilo bancário. A LGPD assegura a autodeterminação informativa dos titulares e impõe obrigações específicas aos agentes de tratamento, prevendo responsabilidade objetiva mesmo na ausência de dano efetivo. Ivani Contini Bramante (2021, p. 88) destaca que a omissão quanto à adoção de medidas de segurança já enseja responsabilização, "independente de causar efetivo dano", sendo devida a reparação por danos morais e materiais.

A arquitetura do Drex, baseada em registros imutáveis e compartilhados, entra em tensão com direitos como exclusão e retificação de dados, dificultando sua efetivação. Também há entraves na identificação dos responsáveis pelo tratamento, o que pode caracterizar os participantes como co-controladores (art. 41 da LGPD), configurando cenário de co-responsabilidade nos termos do art. 42, §1º, da LGPD.

Embora o projeto adote o princípio da privacidade desde a concepção (privacy by design), sua aplicação demanda mais que enunciados formais. Como explica Rosana Kim Jobim (2023, p. 39), trata-se de uma diretriz que "envolve a adoção da privacidade como diretriz do processamento de dados pessoais em todas as etapas, desde a concepção até a execução, incluindo a estrutura, a escala e o volume das operações, bem como as políticas institucionais".

Apesar de operar em rede privada e permissionada, o Drex adota uma DLT com traços da blockchain pública, como a imutabilidade dos registros, o que gera tensões com a LGPD,

especialmente quanto à exclusão e retificação de dados, dificultando a efetivação do direito ao esquecimento (Vieira, 2022).

Estudo de Farias Júnior, Vasconcelos e Ribeiro (2024) sobre zero-knowledge proofs (ZKP) e ring signatures ressalta que a dependência técnica dos dados para autenticação dificulta sua exclusão posterior, inviabilizando o cumprimento integral da legislação. Embora essas tecnologias reforcem a proteção contra acessos indevidos, prejudicam a rastreabilidade e dificultam a responsabilização, comprometendo os princípios da transparência e da prestação de contas. Segundo os autores, "a aplicação do ZKP pode obscurecer quem está realizando o processamento dos dados e como isso tem sido feito", enquanto as ring signatures "podem impedir os indivíduos de saber quem está realizando o processamento dos dados e para quais fins", inviabilizando o consentimento informado, fundamento central da LGPD.

Outro desafio é a ausência de agentes claramente identificáveis. Ao contrário das redes públicas, a validação é feita por milhares de nodes distribuídos de acesso aberto, dificultando a individualização do controlador. No caso do Drex, o governo atua como controlador da rede e, mesmo sob supervisão do Banco Central, os participantes atuam como co-responsáveis, exigindo acordos de governança que delimitem funções, conforme o art. 41 da LGPD.

Por fim, a complexidade dessas soluções afeta a resposta a incidentes. Embora o ZKP auxilie na anonimização e pseudonimização, sua natureza criptográfica dificulta a detecção e notificação de violações de dados, conforme exige a LGPD. O desafio é conciliar altos níveis de proteção com auditabilidade e reação eficaz diante de incidentes de segurança.

IV. III. PROGRAMABILIDADE E LIMITAÇÕES OPERACIONAIS

A plataforma Drex permite a automação de operações financeiras por meio de contratos inteligentes, como as liquidações simultâneas de ativos. No entanto, essa funcionalidade enfrenta importantes limitações técnicas e jurídicas. A imutabilidade da rede inviabiliza alterações em contratos após sua implantação, o que compromete a flexibilidade do sistema diante de falhas (Banco Central do Brasil, 2025, p. 40). Nesses casos, restam apenas soluções alternativas, como a criação de novos contratos ou transações compensatórias, que podem gerar custos e riscos adicionais.

No campo normativo, a ausência de regulamentação específica para contratos autoexecutáveis gera insegurança jurídica quanto à sua validade, especialmente em situações não previstas no código. Embora o Banco Central utilize ferramentas automatizadas de verificação, elas não substituem auditorias especializadas, necessárias para garantir a segurança e a conformidade em ambientes financeiros sensíveis (Banco Central do Brasil, 2025, p. 58).

IV. IV. DESCENTRALIZAÇÃO E MODELO DE GOVERNANÇA DO DREX

O Drex opera como rede privada e permissionada, sob controle do Banco Central, com governança restrita a instituições autorizadas. Apesar do uso de tecnologia DLT, a descentralização é limitada, diferindo das blockchains públicas.

Prevê-se o desenvolvimento descentralizado de serviços via contratos inteligentes, cuja validade pode ser analisada, subsidiariamente, à luz do Código Civil. No entanto, esse modelo enfrenta restrições da rede permissionada e do controle sobre os nós validadores (Banco Central do Brasil, 2025, 2025, p. 10–11).

As DLTs surgiram para eliminar o controlador central, substituído por um sistema colaborativo com dados replicados e validados por diversos participantes. No Drex, essa distribuição é restrita. A privacidade, baseada em pseudoanonimato e criptografia, dificulta a verificação de contratos inteligentes quando as regras ficam ocultas. Surge, assim, o dilema entre sigilo e verificabilidade.

O Piloto Drex busca testar soluções tecnológicas que conciliem privacidade, funcionalidade e conformidade legal. Apesar das ZKPs, a centralização dificulta auditoria e favorece a vigilância estatal, em tensão com a LGPD (Farias Júnior; Vasconcelos; Ribeiro, 2024). O desafio é compatibilizar tecnologias voltadas à descentralização com um modelo estatal de controle, garantindo transparência, proteção de dados e segurança jurídica.

V. CONSIDERAÇÕES PARCIAIS

A análise técnica e jurídica do Drex evidencia que o projeto segue em fase experimental, com diversos entraves técnicos já reconhecidos pelo próprio Banco Central. Apesar da ampla divulgação na mídia sobre um possível lançamento em 2025, ainda não há

previsão oficial para sua implementação, sendo precipitado considerá-lo próximo de um produto final, diante da complexidade dos desafios normativos e operacionais enfrentados.

Juridicamente, a arquitetura do sistema ainda colide com legislações vigentes, não pensadas para tecnologias como blockchain, contratos inteligentes e validação distribuída. A viabilidade do projeto exige, assim, ou a atualização de marcos como a LGPD, a LC nº 105/2001 e a legislação civil atual, ou uma reformulação do próprio desenho do Drex para que se adeque às exigências regulatórias já existentes. Importa acompanhar ainda as discussões legislativas em torno do novo Código Civil, que já propõe dispositivos específicos sobre contratos inteligentes e novas formas de responsabilidade civil digital.

No campo técnico, persistem entraves ligados à segurança, à escalabilidade e à compatibilização entre privacidade e rastreabilidade. O relatório evidencia uma construção progressiva de funcionalidades sem definição prévia dos limites técnicos e jurídicos, o que revela certa subestimação da complexidade envolvida na implementação de uma moeda digital soberana e funcional. Além disso, a dificuldade de realizar auditorias externas, especialmente em razão da adoção de tecnologias como ZKP, impõe desafios adicionais à transparência institucional exigida em projetos estatais. Diante disso, é razoável supor que o cronograma de execução venha a sofrer novos atrasos.

Em síntese, embora represente um avanço na modernização da infraestrutura financeira, a efetivação do Drex depende de amadurecimento normativo, técnico e institucional, além de constante reflexão sobre os limites jurídicos da inovação.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. Relatório Piloto Drex – Fase 1. Brasília, 2024. Disponível em:https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/piloto/Relatorio_Drex_piloto_fase_1.pdf. Acesso em: 26 jun. 2025.

BRAMANTE, Ivani Contini. Proteção de dados pessoais na relação de trabalho. São Paulo: Juruá, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Lei Geral de Proteção de Dados – LGPD). Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 jun. 2025.

BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 26 jun. 2025.

FARIAS JÚNIOR, André; VASCONCELOS, Danilo; RIBEIRO, Patrícia. Um estudo comparativo entre zero-knowledge proof (ZKP) e ring signatures visando as implicações legais e regulatórias com a Lei Geral de Proteção de Dados (LGPD) e General Data Protection Regulation (GDPR). 2024. Disponível em: https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/download/3098/2241/8126. Acesso em: 26 jun. 2025.

JOBIM, Rosana Kim. Privacidade by design. In: ESTUDOS SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS. Porto Alegre: Tribunal Regional do Trabalho da 4ª Região – Escola Judicial, 2023. Disponível em: https://www.trt4.jus.br/portais/media/1063693/E-book-EstudosLGPD-Edjud4.pdf. Acesso em: 26 jun. 2025.

SHEYBANI, Nojan et al. *Zero-Knowledge Proof Frameworks: A Survey*. arXiv preprint arXiv:2502.07063v1, 2025. Disponível em: https://arxiv.org/abs/2502.07063. Acesso em: 30 jun. 2025.

VIEIRA, William Santos. Desafios da LGPD: imutabilidade da blockchain pública e tratamento de dados pessoais pela base legal de consentimento. Goiânia: Pontifícia Universidade Católica de Goiás, 2022. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/5402/1/WILLIAM%20SANTOS%20VIEIRA.pdf. Acesso em: 26 jun. 2025.