

UNIVERSIDADE FEDERAL DE MINAS GERAIS

Faculdade de Direito

Programa de Pós-Graduação em Direito

Caroline Alves Martins Pires Corrêa

**ANÁLISE DA PROTEÇÃO DA PRIVACIDADE E DOS DADOS PESSOAIS DO
USUÁRIO DA CBDC BRASILEIRA**

Belo Horizonte

2024

Caroline Alves Martins Pires Corrêa

**ANÁLISE DA PROTEÇÃO DA PRIVACIDADE E DOS DADOS PESSOAIS DO
USUÁRIO DA CBDC BRASILEIRA**

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, como requisito parcial para a obtenção do grau de Mestre(a) em Direito.

Orientadora: Profa. Dra. Rubia Carneiro Neves.

Linha de Pesquisa: Poder, Cidadania e desenvolvimento no Estado Democrático de Direito

Área de Estudo: Sistema Financeiro Nacional – Negócios, regulação e tutela nos âmbitos administrativo sancionador e penal.

Belo Horizonte

2024

Ficha catalográfica elaborada pela bibliotecária Meire Queiroz - CRB-6/2233.

C824a Corrêa, Caroline Alves Martins Pires
Análise da proteção da privacidade e dos dados pessoais do usuário do
Drex [manuscrito] / Caroline Alves Martins Pires Corrêa. - 2024.
113 f.

Orientadora: Rubia Carneiro Neves.
Dissertação (mestrado) - Universidade Federal de Minas Gerais,
Faculdade de Direito.
Bibliografia: f. 87-113.

1. Direito - Teses. 2. Direito à privacidade - Teses. 3. Proteção de dados -
Teses. 4. Conselho Monetário Nacional - Teses. 5. Banco Central do Brasil -
Teses. I. Neves, Rubia Carneiro. II. Universidade Federal de Minas Gerais -
Faculdade de Direito. III. Título.

CDU: 336.76:342.721



UNIVERSIDADE FEDERAL DE MINAS GERAIS

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

UFMG

ATA DA DEFESA DA DISSERTAÇÃO DA ALUNA CAROLINE ALVES MARTINS PIRES CORRÊA

Realizou-se, no dia 19 de abril de 2024, às 09:30 horas, na Faculdade de Direito da Universidade Federal de Minas Gerais, a defesa de dissertação, intitulada **Análise da Proteção da Privacidade e dos Dados Pessoais do Usuário do Drex**, apresentada por **CAROLINE ALVES MARTINS PIRES CORRÊA**, número de registro 2022654328, graduada no curso de DIREITO, como requisito parcial para a obtenção do grau de **Mestre em DIREITO**, à seguinte Comissão Examinadora: Prof(a). Rubia Carneiro Neves - Orientador (Universidade Federal de Minas Gerais), Prof(a). Davi Monteiro Diniz (UFMG) e Prof(a). Leandro Novais e Silva (UFMG).

A Comissão considerou a dissertação:

(X) Aprovada, tendo obtido a nota 100.

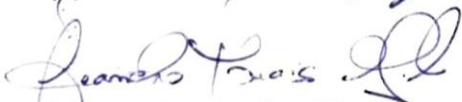
() Reprovada

Finalizados os trabalhos, lavrei a presente ata que, lida e aprovada, vai assinada por mim e pelos membros da Comissão.

Belo Horizonte, 19 de abril de 2024.


Prof(a). Rubia Carneiro Neves (Doutora) Nota: 100


Prof(a). Davi Monteiro Diniz (Doutor) Nota: 100


Prof(a). Leandro Novais e Silva (Doutor) Nota: 100

A Ele, toda honra e glória.

AGRADECIMENTOS

As nuances da vida nos conduzem ao amadurecimento. Esse processo solidificou ainda mais meu relacionamento com Deus e me fez aprender com os erros e acertos. Nesta tradicional casa, que há anos vem trazendo conhecimento acadêmico de alto nível para o Brasil e para o mundo, contei com a contribuição de inúmeras pessoas, a quem expresso minha gratidão.

Algumas delas contribuíram diretamente nessa caminhada, por isso sinto-me honrada em reconhecê-las expressamente.

À professora Rubia Carneiro Neves, especialmente, que, com extremo conhecimento e dedicação à vida acadêmica, orientou-me no processo de pesquisa e elaboração desta dissertação. Sua presença em minha vida é um presente e sou extremamente grata pela convivência, amabilidade do seu coração e profundo conhecimento na área financeira.

Ao meu esposo Lucas, pela escuta ativa e paciente, bem como pelas horas de leitura, correções e conhecimentos técnicos compartilhados. O amor é paciente, é bondoso, tudo crê, tudo suporta e tudo espera.

Às minhas preciosas, mãe e avó, que, sempre com garra, enfrentaram uma árdua vida, mas nunca deixaram de me mostrar a importância de sonhar e dedicar-se para alcançar os objetivos, em quaisquer circunstâncias.

À Universidade Federal do Estado de Minas Gerais (UFMG), que se torna constantemente lugar propício à produção séria do conhecimento. A participação no Grupo de Pesquisa CNPq Sistema Financeiro Nacional: negócios e regulação, sob a orientação da Professora Dra. Rubia Carneiro Neves, e o Grupo de Estudos em Direito e Tecnologia da Universidade Federal de Minas Gerais (DTEC-UFMG), sob a coordenação do Professor Dr. Leonardo Parentoni, permitiram-me compreender e debater com qualidade tais temas e compartilhá-los com a comunidade ao produzir artigos.

Ao Dr. Direito Carlos Frederico Braga da Silva, que exerce a magistratura com exímia dedicação social e entusiasmo pelas mudanças tecnológicas e contribuiu com seu senso crítico para a elaboração deste trabalho.

A todos do Tribunal de Justiça de Minas Gerais, bem como a toda equipe da PHV Engenharia e da Netlex, que me apoiaram e alimentaram o sonho em ser Mestre, flexibilizando jornadas e compartilhando conquistas.

Por fim, a Eliana Chiari e Sueli Pimenta, cujos cuidados emocionais me permitiram ser ainda mais forte.

RESUMO

Com base em material levantado até fevereiro de 2024, por meio de análise normativa e revisão de literatura, procurou-se verificar a hipótese de que a estrutura tecnológica e regulatória adotada pelo Banco Central do Brasil (BCB) para emitir o Drex, a *Central Bank Digital Currency* (CBDC) brasileira, oferece possibilidades de riscos da privacidade e da proteção de dados da pessoa natural do seu usuário. Primeiro, foi necessário entender os modelos que podem ser usados para emitir CBDCs, e em especial, o escolhido pelo BCB para elaborar e executar o Piloto do Drex. Depois, foram estudadas as variações da tecnologia *distributed ledger technology* (DLT), com ênfase no formato atacado com adoção de emissão de *tokens* em banco de registro de dados descentralizado, permissionado e privado, em que se usa a prova de autoridade, o *Proof of Authority* (PoA), para nele autorizar o acesso e a participação, apenas dos integrantes selecionados pela autoridade central, características escolhidas pelo BCB para a estrutura do Drex. Também foi crucial delimitar o regime jurídico brasileiro aplicável à proteção da privacidade e dos dados pessoais. Ao final, percebeu-se que o BCB assumiu expressamente o compromisso de respeitar na emissão e circulação do Drex, a legislação geral e especial que regula privacidade e a proteção de dados pessoais no Brasil. Todavia, não foi possível afirmar com certeza que estão completamente afastados os riscos de cometimento de atividades de processamento de dados, que por sua vez, geram informações sobre registros e padrões de atividades como valores de moedas e serviços utilizados que podem levar à indevida vigilância, à abusiva manipulação de banco de dados nacionais e internacionais e à perfilização dos usuários do Drex. Isso, porque, considerando o seu estágio evolutivo de criação, ainda na fase de Projeto-piloto, cujos testes não foram finalizados, não foi localizada a definição dos tipos de dados do usuário do Drex que poderão ser acessados e tratados, como também não foi identificada a delimitação da extensão da autorização para o seu tratamento e compartilhamento. Apesar de ter sido localizada previsão de atribuição de competência ao Comitê Executivo de Gestão do Piloto Drex e aos seus membros para zelar pela proteção de dados que o comitê reunir, também não ficou claro como se dará a responsabilização pelo tratamento indevido de dados e qual abordagem será adotada em relação à anonimização de dados e à atuação da Agência Nacional de Proteção de Dados (ANPD) na estrutura do Drex, especialmente, no que se refere à delimitação de padrões para a elaboração dos termos de uso de transferência internacional de dados nos planejados pagamentos transfronteiriços. Todas essas indefinições precisarão ser consideradas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil na regulação da moeda digital brasileira, assim como novas fases de investigação serão necessárias para compreender como técnicas de *privacy* e *data protection by design* e *by default* com a implementação das *Privacy Enhancing Technologies* (PETs) estudadas pelo BCB permitiriam a efetiva autodeterminação informativa dos indivíduos, retirando-os da posição de vítimas do tratamento de dados, para colocá-los como efetivos titulares do poder sobre seus dados pessoais.

Palavras-chave: Privacidade; Proteção de dados; Moeda digital de Banco Central; Central Bank Digital Currency (CBDC); Drex; Real Digital; Identificação de pontos de atenção; Regulação normativa; Conselho Monetário Nacional (CMN); Banco Central do Brasil (BCB).

ABSTRACT

Based on material collected up to February 2024, through normative analysis and literature review, we sought to verify the hypothesis that the technological and regulatory structure adopted by the Central Bank of Brazil (BCB) to issue the Drex, the Central Bank Brazilian Digital Currency (CBDC) offers risks to privacy and data protection of its user's natural person. First, it was necessary to understand the models that can be used to issue CBDCs, and in particular, the one chosen by the BCB to prepare and execute the Drex Pilot. Afterwards, variations of distributed ledger technology (DLT) technology were studied, with an emphasis on the wholesale format with the adoption of issuing tokens in a decentralized, permissioned and private database, in which proof of authority is used, the Proof of Authority (PoA), to authorize access and participation only by members selected by the central authority, characteristics chosen by the BCB for the Drex structure. It was also crucial to define the Brazilian legal regime applicable to the protection of privacy and personal data. In the end, it was clear that the BCB expressly assumed the commitment to respect, when issuing and circulating the Drex, the general and special legislation that regulates privacy and the protection of personal data in Brazil. However, it was not possible to state with certainty that the risks of committing data processing activities are completely ruled out, which in turn generate information about records and activity patterns such as currency values and services used that can lead to undue surveillance, the abusive manipulation of national and international databases and the profiling of Drex users. This is because, considering its evolutionary stage of creation, even in the Pilot Project phase, whose tests have not been completed, the definition of the types of Drex user data that can be accessed and processed was not found, nor was it the delimitation of the extent of authorization for its processing and sharing has been identified. Although a provision was made for attributing powers to the Drex Pilot Management Executive Committee and its members to ensure the protection of data that the committee gathers, it was also not clear how accountability for improper data processing would be carried out and what approach will be adopted in relation to data anonymization and the performance of the National Data Protection Agency (ANPD) in the Drex structure, especially with regard to the delimitation of standards for the elaboration of terms of use for international data transfer in the planned cross-border payments. All these uncertainties will need to be considered by the National Monetary Council and the Central Bank of Brazil in the regulation of Brazilian digital currency, as well as new phases of investigation will be necessary to understand how privacy and data protection by design and by default techniques with the implementation of Privacy Enhancing Technologies (PETs) studied by the BCB would allow the effective informational self-determination of individuals, removing them from the position of victims of data processing, and placing them as effective holders of power over their personal data.

Keywords: Privacy; Data protection; Digital currency; Central Bank Digital Currency (CBDC); Drex; Real Digital; Identification of points of attention; Normative regulation; National Monetary Council (CMN); Central Bank of Brazil (BCB).

LISTA DE FIGURAS

Figura 1 – Banco de Dados Centralizado e Distribuído.....	15
Figura 2 – Lógica básica dos contratos inteligentes.....	17

LISTA DE ILUSTRAÇÕES

Tabela 1 – Comparação entre tipos de DLTs.....	22
Tabela 2 – Semelhança e diferenças dos mecanismos de consenso PoW, PoS e PoA.....	28
Tabela 3 – Comparação entre CBDC de varejo e de atacado.....	30
Tabela 4 – Comparação entre diretrizes do Real Digital de 2021 e 2023.....	33

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
BCB	Banco Central do Brasil
BIS	Bank of International Settlements
CBDC	Central Bank Digital Currency
CCB	Código Civil Brasileiro
CDC	Código de Defesa do Consumidor
CNB	Colégio Notarial do Brasil
CVM	Comissão de Valores Mobiliários
DEFI	Decentralized Finances
DLT	Distributed Ledger Technology
DVP	Delivery versus Payment
ECB	European Central Bank
EVM	Ethereum Virtual Machine
FEBRABAN	Federação Brasileira de Bancos
FENASBAC	Federação Nacional de Associações dos Servidores do Banco Central
FMI	Fundo Monetário Internacional
IF	Instituições Financeiras
IMDB	Internet Movie Database
IP	Instituições de Pagamento
IOT	Internet das Coisas
ITU	International Telecommunication Union
LBTR	Liquidação Bruta em Tempo Real
MET	Moeda Eletrônica
PET	Privacy Enhancing Technologies
PIER	Plataforma de Integração de Informações das Entidades Reguladoras
POA	Proof of Authority
POS	Proof of Stake
POW	Proof of Work
PBOC	Popular Bank of China
PLC	Projeto de Lei Complementar
SISBACEN	Sistema de Informações do Banco Central
SPB	Sistema de Pagamentos Brasileiro
SPI	Sistema de Pagamentos Instantâneo
STN	Secretaria do Tesouro Nacional
STR	Sistema de Transferência de Reserva
STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal
SUSEP	Superintendência de Seguros Privados
MCI	Marco Civil da Internet
TPFT	Títulos Públicos Federais

SUMÁRIO

1 INTRODUÇÃO	9
2 DREX: A CENTRAL BANK DIGITAL CURRENCY (CBDC) BRASILEIRA.....	11
2.1 CBDC: conceito e justificativas para a sua criação.....	11
2.2 Tipos de CBDC.....	16
2.2.1 CBDC em conta.....	17
2.2.2 CBDC em token.....	17
2.2.2.1 <i>Blockchain</i>	19
2.2.2.2 <i>Distributed Ledger Technology (DLT)</i>	20
2.2.2.2.1 Tipos de configuração de DLTs: públicas, privadas, permissionadas e não permissionadas	21
2.2.2.2.2 Os mecanismos de consenso: Proof of Work (PoW); Proof of Stake (PoS); Proof of Authority (PoA)	24
2.2.3 CBDC atacado.....	31
2.2.4 CBDC de varejo.....	31
2.3 O processo de criação da CBDC brasileira.....	32
2.4 O modelo adotado pelo Banco Central do Brasil na estrutura do Drex	36
3 PROTEÇÃO DA PRIVACIDADE E DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO.....	40
3.1 Privacidade: surgimento e conceito	41
3.2 Dados.....	45
3.2.1 Dados pessoais.....	46
3.2.2 Dados anônimos e pseudoanonimizados.....	49
3.3 Tratamento de dados pessoais: conceito, bases legais, princípios e diretrizes.....	50
3.4 Proteção da privacidade e de dados pessoais no ordenamento jurídico brasileiro.....	56
3.4.1 No regime constitucional.....	57
3.4.2 Em legislações infraconstitucionais.....	58

4 ASPECTOS E RISCOS QUE DEVEM SER CONSIDERADOS NA FORMULAÇÃO DE NORMAS VOLTADAS À REGULAÇÃO DO DREX: A MOEDA DIGITAL BRASILEIRA.....	64
4.1 A indefinição quanto ao tipo de dados e de informações pessoais que serão tratados no Drex e à extensão da autorização para o seu tratamento e os riscos de indevida vigilância de dados e de formação de banco de informações suscetível à prática de perfilização.....	66
4.2 Agência Nacional de Proteção de Dados (ANPD): atuação de autoridade centralizada em ambiente descentralizado.....	82
CONCLUSÃO.....	88
REFERÊNCIAS.....	90

1 INTRODUÇÃO

Para se criar a Central Banking Digital Currency (CBDC) brasileira, inicialmente denominada “Real Digital” e, mais recentemente, “Drex”¹, o Banco do Central do Brasil (BCB) optou por utilizar a *Hyper Ledger Besu*², espécie de sistema descentralizado de registro de informações que se vale da tecnologia *blockchain* permissionada e privada, à qual somente os participantes autorizados têm acesso, bem como podem visualizar e registrar informações no sistema que a mantém (MATOS, 2023).

Considerando que os participantes tratarão dados pessoais de clientes do Drex, esta dissertação foi produzida, sob a perspectiva da proteção do indivíduo, com base em pesquisa realizada para investigar se **o modelo adotado pelo Banco Central do Brasil (BCB) para criar o Drex protege a privacidade e os dados da pessoa natural do seu usuário.**

Procurou-se verificar a hipótese de que o modelo do Drex não assegura completamente a privacidade e a proteção de dados de seus usuários, porque falta nos documentos oficiais que respaldam o projeto-piloto a definição: a) dos tipos de dados que serão tratados pelos participantes da *Hyper Ledger Besu*; b) dos limites para a atuação dos participantes, isto é, do Estado, dos responsáveis por validar pagamentos e transferências e dos terceiros; c) de como se dará a atuação da Agência Nacional de Proteção de Dados (ANPD) na estrutura descentralizada do Drex; d) se será ou não vedada a completa anonimização dos dados dos usuários.

Para verificar tal hipótese, foi necessário entender o que é CBDC, quais as características da tecnologia distribuída – *Distributed Ledger Technology* (DLT) –, quais os elementos do modelo adotado pelo BCB para criar o Drex, o que são dados e privacidade, como eles são protegidos pelo ordenamento jurídico brasileiro, qual é o

¹ O BCB anunciou, em 7 de agosto de 2023, o novo nome da moeda digital brasileira, anteriormente denominada “Real Digital”. O nome é composto de quatro letras, cada uma possuindo um significado pertinente. Dessa forma, o “D” e o “R” fazem alusão ao Real Digital, enquanto o “E” e o “X” remetem à modernidade e conexão (A MOEDA..., 2023)

² Resolução BCB n. 315/2023, art. 3º: “O Piloto RD tem por objetivo validar o uso de uma solução de Tecnologia de Registro Distribuído (DLT), na plataforma Hyperledger Besu, avaliando a programabilidade com ativos financeiros e a capacidade de observância aos requisitos legais e regulatórios, principalmente em relação à privacidade das informações de indivíduos e demais envolvidos nas transações na plataforma do Real Digital, bem como sua viabilidade tecnológica” (BCB, 2023b). Tal plataforma é ofertada pela Hyper Ledger Foundation, criada em 2017, para atender às demandas do mercado corporativo (DE LEON *et al.*, 2017, p. 288).

papel da ANPD quanto à sua proteção e quais as implicações da anonimização de dados.

O estudo desses itens foi realizado com uso de revisão bibliográfica e de análise de normas e de documentos produzidos por bancos centrais, levantados com a busca, principalmente, dos termos “privacidade”, “proteção de dados”, “CBDC”, *privacy*, *data protection* e *central bank digital currency* em sites, como Minha Biblioteca (MINHA...), Heinonline (HEINONLINE...), Google Acadêmico (SCHOLAR...) e o Portal de Periódicos CAPES (ACESSO..., 2023).

O resultado da investigação realizada foi dividido em três capítulos, além desta introdução, da conclusão e das referências utilizadas. No primeiro capítulo, dedicou-se à compreensão do Drex, em cuja abordagem foi utilizado, principalmente, Neves, Diniz e Silva (2022), Barroso (2022; 2023), as diretrizes do BCB de 2021 (BCB, 2021a) e as contidas no Voto BCB n. 31/2023 (BCB, 2023c).

Antes, porém, foi necessário estudar os aspectos tecnológicos da Central Bank Digital Currency (CBDC), passando por seu conceito, pelas justificativas para sua emissão e pelos seus possíveis tipos. O que foi feito com adoção de Corrêa e Leite (2023); Corrêa, Pimentel e Souza (2023); Banco de Compensações Internacionais – BIS (2023); ANBIMA (2022); Ragazzo e Cataldo (2021); Bertolai e Oliveira (2020); Organização Internacional de Comissões de Valores Mobiliários (IOSCO, 2020); Burgos e Batavia (2018); Tribunal de Contas da União – TCU (2020); União Internacional de Telecomunicações – ITU (2017); Bech e Garrat (2017); Wüst e Gervais (2018).

No segundo, foram apresentadas as salvaguardas estabelecidas no regime jurídico brasileiro sobre a proteção da privacidade e dos dados pessoais, principalmente com base na Constituição Federal de 1988 – CRFB (BRASIL, 1988a); na Lei n. 8.078/1990 – Código de Defesa do Consumidor – CDC (BRASIL, 1990); na Lei n. 9.296/1996 – Lei de Interceptação das comunicações (BRASIL, 1996); na Lei n. 9.472/1997 – Lei de Telecomunicações (BRASIL, 1997); na Lei Complementar n. 105/2001 – Lei do Sigilo Bancário (BRASIL, 2001); na Lei n. 12.414/2011 – Lei do Cadastro Positivo (BRASIL, 2011a); na Lei n. 12.527/2011 – Lei de Acesso à Informação (BRASIL, 2011b); na Lei n. 12.965/2014 – Marco Civil da Internet (BRASIL, 2014); e na Lei n. 13.709/2018 – Lei Geral de Proteção de Dados – LGPD (BRASIL, 2018).

Tomou-se Doneda (2011; 2020a; 2020b) como referencial teórico para o estudo da proteção de dados. Para conceituar privacidade como direito fundamental foram utilizadas as obras de Warren e Brandeis (1890), de Innes (1992) e de Solove (2007).

No terceiro capítulo, realizou-se análise crítica do desenho estrutural do Drex procurando-se responder à questão central pesquisada. Allan Westin (1967) e Shoshana Zuboff (2018) foram usados para trabalhar o tema relativo à vigilância algorítmica. Os aspectos técnicos da Blockchain foram estudados com base em De Fillipi e Wright (2018) e Liliane Barroso (2022; 2023). O senso crítico de Danilo Doneda (2020a; 2020b) foi fundamental para tratar a respeito da criação de banco de dados dos indivíduos e de pontos sensíveis como perfilização e suas implicações nas garantias e direitos individuais contidos na Constituição da República Federativa do Brasil (BRASIL 1988a) e na Lei n. 12.414/2011– Lei do Cadastro Positivo (BRASIL, 2011a).

Nele, portanto, cuidou-se dos aspectos e riscos que devem ser considerados na formulação de normas voltadas para regulação do Drex, sendo utilizados os materiais produzidos pelo BCB até fevereiro de 2024 sobre a temática, como o Voto n. 31 de 2023 (BCB, 2023c) e a Resolução BCB n. 315/2023 (BCB, 2023b). Isso permitiu verificar as omissões existentes no Drex e alertar o BCB e o CMN para a formulação de documentos normativos atinentes à privacidade e à proteção de dados.

Feita a apresentação geral da dissertação, passa-se a entender o que é moeda digital emitida por banco central, as principais espécies que podem ser criadas e algumas tecnologias que podem ser usadas em sua criação.

2 DREX: A CENTRAL BANK DIGITAL CURRENCY (CBDC) BRASILEIRA

Antes de passar à compreensão do Drex como peculiar tipo de CBDC, faz-se necessário apresentar algumas noções sobre as moedas digitais emitidas por bancos centrais.

2.1 CBDC: conceito e justificativas para a sua criação

Trata-se a CBDC de nova forma de representação da moeda nacional dotada de curso legal que é emitida por bancos centrais em formato digital (RAGAZZO;

CATALDO, 2021, p. 22) e que não se confunde com a moeda eletrônica ou com as moedas virtuais³ (BECH; GARRAT, 2017), muito menos com as reservas detidas pelos bancos comerciais em bancos centrais, ou seja, os valores traduzidos em moedas escriturais (IOSCO, 2020, p. 4).

Emitir ou não a CBDC decorre de decisão de cunho político que pode ser justificada conforme as peculiaridades do sistema financeiro e do sistema de pagamentos de cada país⁴.

O anúncio de criação da “stablecoin global” Libra pelo Facebook, em junho de 2019⁵, é apontado como o principal marco para que diversos países iniciassem a discussão sobre a emissão de CBDCs, em razão do potencial impacto que a *bigtech* teria sobre as finanças globais diante do volume da sua rede de usuários, que, por sua vez, liga-se a outras redes sociais como *Whatsapp* e *Instagram Pay* (DEDENKO *et al.*, 2020, p. 5-28).

Além de as moedas virtuais serem comumente associadas a atividades ilícitas, especialmente tratando-se daquelas que utilizam *blockchains* públicas e não permissionadas, com a completa anonimização dos dados das pessoas participantes (BERTOLAI; OLIVEIRA, 2020, p. 225), a possibilidade de que elas ocupem posição principal na economia monetária com priorização da valorização da obtenção de lucro

³ No Brasil, de acordo com o inciso VI do art. 6º da Lei n. 12.865/2013 (BRASIL, 2013) as moedas eletrônicas são recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar pagamentos emitidas de forma centralizada por instituições depositárias de Reais depositados em contas de pagamento pré-pagas. Podem ser usadas para efetuar pagamentos ou transferências, por exemplo, por meio do Pix ou do cartão de débito (ATIVOS VIRTUAIS..., 2023). As moedas virtuais são emitidas de forma descentralizada, se valem da tecnologia baseada em tokens e podem possuir ou não lastro nas moedas de curso legal de determinadas nações (RAGAZZO; CATALDO, 2021, p. 13). O Banco Central do Brasil, por meio do Comunicado BCB n. 25.306/2014 (BCB, 2014), afirmou que as moedas virtuais não são emitidas nem garantidas por ele enquanto autoridade monetária, e alertou não assumir custos e riscos de sua utilização (ATIVOS VIRTUAIS..., 2023), inclusive aqueles decorrentes da sua volatilidade.

⁴ A emissão da CBDC é uma decisão política que deve levar em conta situações como a disponibilidade e os custos operacionais. Assim, deve-se discutir se a liquidação das obrigações financeiras realizadas com a CBDC será atômica, em tempo real, isto é, será ofertada regime de vinte e quatro horas por dia, nos sete dias da semana (24x7), ou em horário comercial, *online* ou *offline*. Bem como saber quais os custos que estão envolvidos e se eles serão repassados ao consumidor final ou não (BIS, 2018a).

⁵ Por mais que a comunidade internacional tenha se posicionado negativamente, expondo os riscos potenciais que a Libra poderia causar ao mercado financeiro, existem pontos interessantes a serem mencionados no projeto. O primeiro deles é o fato de que a Libra apresentou *design* de plataforma próprio, rejeitando o mecanismo de consenso de Prova de Trabalho (*Proof of Work* – PoW), clássico de *blockchains* públicas. A *blockchain* utilizada pela Libra, portanto, é um sistema de código aberto (*open source*), que trabalha com mecanismo de consenso próprio denominado LibraBFT (*Byzantine Fault Tolerant*) (TRINDADE, 2021, p. 41). Essa tecnologia prometia superar o fraco desempenho e o alto gasto energético de mecanismos a base de PoW (LIBRA, 2020, p. 8), alcançando melhores níveis de escalabilidade, com o objetivo de atingir grande número de pessoas ao redor do mundo (TRINDADE, 2021, p. 41).

poderia influenciar as decisões do mercado e colocar em risco a economia popular (CARVALHO, OLIVEIRA; MONTEIRO, 2010, p. 11; TRINDADE, 2021, p. 41). Tanto é que, em 2019, apenas 42% (quarenta e dois por cento) dos bancos centrais possuíam projetos para experimentar a emissão de CBDC, percentual que aumentou para 60% (sessenta por cento) em 2020 (BOAR; WEHRLI, 2021, p. 6).

No Brasil, por exemplo, uma das justificativas para a emissão da CBDC é a necessidade de conferir atratividade ao Real com a sua oferta digitalizada de modo a concorrer com as funcionalidades das criptomoedas e das *stablecoins* e, com isso, garantir a estabilidade nacional e a centralização de poder estatal sobre a política monetária (NEVES; DINIZ; RAMOS, 2023, p. 86-87; RAGAZZO; CATALDO, 2021, p. 22-26).

O controle da inflação é, em geral, um dos objetivos fundamentais do BCB, seguindo a visão de metas de inflação estabelecidas pelo Conselho Monetário Nacional (CMN)⁶. Para alcançar esse objetivo, o Banco Central brasileiro faz uso da política monetária, isto é, ações que visam afetar a taxa de juros (custo do dinheiro) e as condições de liquidez (quantidade de dinheiro). A promessa com a CBDC, assim, é facilitar a condução dessa política de maneira sistemática e transparente (BORDO; LEVIN, 2017, p. 2).

Viabilizar pagamentos programáveis, reduzir custos operacionais, aumentar a inclusão digital e financeira, promover a rastreabilidade e fomentar alternativa aos pagamentos transfronteiriços são outras funcionalidades da CBDC que têm sido apresentadas como justificativas para sua criação.

A programabilidade relaciona-se à adoção de sistemas do tipo *Distributed Ledger Technology* (DLTs) que permitem que funções sejam programadas com inteligência integrada às regras dos negócios. Em que podem ser definidas e gravadas em código, criando os chamados *smart contracts* – contratos inteligentes (ITU, 2017, p. 19), por meio dos quais é possível gerar avisos para determinadas faixas de renda, alertas para ilícitos a depender do perfil de consumo do usuário ou indicativos para incidência de impostos automáticos. Pode-se, até mesmo, programar sinais quando determinada pessoa realiza em um dia pagamentos muito acima do normal para o seu

⁶ A atual meta para inflação estabelecida pelo CMN está expressa na Resolução do CMN n. 5.091/2023 (CMN, 2023).

perfil de consumo, representando o indicativo de que, provavelmente, houve fraude em sua conta.

Pelo fato de a população poder valer-se de *smartphones* para efetuar seus pagamentos e transferências de valores, espera-se sejam reduzidos os custos com a emissão e a circulação da moeda física (WÜST; GERVAIS, 2018, p. 6; CORRÊA; LEITE, 2023, p. 215) e com as atividades que dependem de agências e caixas eletrônicos (CORREA; PIMENTEL; SOUZA, 2023, p. 192).

Os bancos brasileiros, por exemplo, gastam anualmente cerca de 9 (nove) bilhões de reais nos processos de guarda, compensação e transporte da moeda metálica e cedular, que são constantemente alvo de roubos (BURGOS; BATAVIA, 2018, p. 4). Apesar de exigir investimentos em segurança cibernética, promete-se que a moeda digital pode eliminar esses mencionados gastos.

A facilidade de acesso a celulares e aparelhos eletrônicos também promete viabilizar a inclusão digital (RAGAZZO; CATALDO, 2021, p. 25) e financeira (BURGOS; BATAVIA, 2018, p. 4-5). Segundo pesquisa realizada pelo Global Findex Report em 2017 (KUNT *et al.*, 2017, p.7), 92% (noventa e dois por cento) dos adultos participantes tinham acesso a aparelhos celulares conectados à internet ou à internet residencial, mas apenas 70% (setenta por cento) dos adultos eram titulares de contas bancárias. Dentre os 30% (trinta por cento) dos que não eram titulares de conta, 32% (trinta e dois por cento) justificavam com a inexistência de instituição financeira próxima à sua residência e 57% (cinquenta e sete por cento), em razão dos altos custos dos serviços prestados. Em virtude dessa realidade, a Autoridade Monetária de Singapura (MAS), o Banco Central do Canadá e o Conselho da Reserva Federal nos EUA têm trabalhado em projetos que visam oferecer solução distribuída para pagamentos interbancários, para permitir maior inclusão financeira. A China (RAGAZZO; CATALDO, 2021, p. 15) com o Digital Yuan, a Nigéria com o E-Nira (KOSINK, 2022, p. 91) e o Brasil com o Drex (BCB, 2023a, p. 5) são exemplos de países que apostam na emissão de CBDCs com o propósito de maior inclusão da população no sistema financeiro.

A rastreabilidade é funcionalidade que também se relaciona à tecnologia DLT, por meio da qual se realizam registros no sistema (*record keeping*), que são rastreáveis (BERTOLAI; OLIVEIRA, 2020, p. 214). Essa característica promete permitir a formulação de políticas monetárias condizentes com a realidade de cada nação, pois a

decisão tomada será baseada em dados, propiciando, assim, maior governança (RAGAZZO; CATALDO, 2021, p. 25).

Além disso, pode incrementar o monitoramento de ilicitudes, com a identificação do autor da ilicitude em razão da rastreabilidade dos registros, o que poderá, via de consequência, inibir o cometimento de crimes de lavagem de dinheiro e financiamento ao terrorismo (BARROSO, 2022, p. 14-15). A Índia, por exemplo, vem promovendo a digitalização total de sua economia para reduzir a corrupção, melhorar os níveis de rastreabilidade dos gastos públicos e de impostos recolhidos (RAGAZZO; CATALDO, 2021, p. 15). A rastreabilidade também promete gerar impactos no cumprimento de obrigações legais, por exemplo, quando determinada judicialmente a quebra de sigilo em processo de suspeita de lavagem de dinheiro, para a busca de informações sobre a movimentação de recursos financeiros sobre a origem de determinado valor.

Para tanto, no sistema da CBDC, a base de dados do Banco Central entraria no cruzamento do Sistema Nacional de Investigação Patrimonial e Recuperação de Ativos (*Sniper*), para que seja possível chegar em todos os envolvidos⁷.

O sistema tradicional de câmbio utilizado atualmente⁸ para as transferências internacionais é considerado ineficiente em razão do alto custo de taxas agregadas para o serviço (RAGAZZO; CATALDO, 2021, p. 19), da insegurança, em razão de manipulações geopolíticas e de demora para a liquidação dos pagamentos e transferências (CORREA; PIMENTEL; SOUZA, 2023, p. 184-189). Aponta-se, ainda, a complexidade regulatória enfrentada pelas instituições privadas que desejam atuar no atual sistema (BIS, 2021).

Entendidas as funcionalidades da CBDC, é necessário explicar alguns tipos de moedas digitais.

⁷ No caso brasileiro, o *Sniper* é a solução tecnológica desenvolvida pelo Conselho Nacional de Justiça (CNJ) via Programa Justiça 4.0. Atualmente, o sistema consulta a base dos dados da Receita Federal do Brasil, Tribunal Superior Eleitoral (TSE), Controladoria-Geral da União (CGU), dentre outros, e está em processo de integração com o sistema Infojud, para dados fiscais e Sisbajud para dados bancários. Nesse sistema, o acesso ao Sisbajud e ao Bacenjud se dá apenas no modo sigiloso, conforme consta no portal oficial dessa funcionalidade (SISTEMA..., 2023).

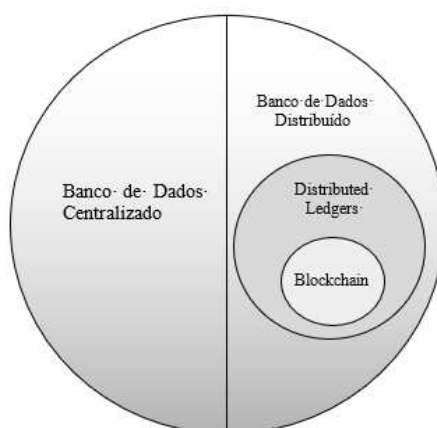
⁸ Os pagamentos e transferências de valores realizados internacionalmente são feitos pelo Society for Worldwide Interbank Financial Telecommunication (SWIFT), sistema de rede global que conecta bancos e demais instituições financeiras fora das jurisdições nacionais, transportando tais dados entre as infraestruturas dessas instituições citadas (CORREA; PIMENTEL; SOUZA, 2021, p. 188).

2.2 Tipos de CBDC

As moedas digitais podem ser emitidas pelos bancos centrais, por exemplo, com a utilização de contas ou de *tokens*⁹, no formato atacado ou no varejo (BIS, 2023, p. 5; ANBIMA, 2022, p. 6).

A escolha do formato da CBDC decorrerá do modelo de banco de dados adotado pelo banco central emissor, podendo ser centralizado ou distribuído. É comum ver a adoção de contas no modelo centralizado. No distribuído, pode-se valer, por exemplo, da *Distributed Ledger Technologies* (DLT) – ou tecnologia de livros distribuídos –, como também da tecnologia *blockchain* (ITU, 2017, p. 11). No quadro a seguir, vê-se que *blockchain* e DLT – que serão explicadas adiante – são espécies de tecnologias que permitem o registro de informações em banco de dados distribuído.

Figura 1 – Banco de dados centralizado e distribuído



Fonte: TCU, 2020, p. 11 (adaptado).

⁹ Apesar de terem sido localizadas referências bibliográficas dando notícias sobre a possibilidade de utilização de tecnologias diferentes de contas e *tokens* em moedas digitais, considerando os objetivos com esta dissertação e o exíguo prazo para finalizá-la, concentrou-se apenas nas duas referidas espécies. Para maiores detalhes, vale conferir o trabalho de Popova e Butakova (2019), em que se discutiram aplicações da tecnologia *blockchain* sem a utilização de *tokens* no mercado de pagamentos, visando à proteção de informações correlatas aos pagamentos ou transferências bancárias, tais como quantidade de valores transferidos, dados de cartões e nome dos correntistas. As autoras propuseram retirar os nós e intermediários dos pagamentos ou transferências, a fim de reduzir o número de participantes nessas atividades, implementando no lugar os contratos inteligentes (POPOVA; BUTAKOVA, 2019, p. 9). Em Amazon Web Services, também se conferiram notícias de que existem sistemas financeiros tokenizados que não são baseados na mencionada tecnologia (AWS, 2021, p. 10). Foram verificados, ainda, os apontamentos do Banco de Reserva Federal de Boston em relação ao projeto Hamilton, segundo o qual a categorização – em token ou conta – é limitada e insuficiente para revelar a complexidade da escolha de acesso, de intermediadores, de funções institucionais e de retenção de dados na CBDC (BRFB, 2022).

Com base nessas duas classificações de banco de dados centralizado ou distribuído é que existem os dois modelos de CBDC: a que é emitida em conta e a que é criada via emissão de *token*.

2.2.1 CBDC em conta

O formato de conta que se vale de banco de dados centralizado para funcionamento do sistema de pagamentos é figura bem conhecida no Brasil, eis que utilizado no formato de conta de depósito (corrente ou de poupança) pelo BCB para processar as moedas escriturais emitidas pelos bancos comerciais e, mais recentemente, as contas de pagamento pré-pagas, para processar as moedas eletrônicas emitidas pelas instituições financeiras e de pagamento autorizadas a fazê-lo (NEVES; COSTA; SILVA, 2021, p. 45).

Para emitir a CBDC via contas, o banco central digitaliza, em livros de registros, os saldos mantidos pelos clientes do mercado financeiro (BOSSU *et al.*, 2020, p. 9).

Na versão da CBDC emitida em conta, o saldo do cliente pode estar associado a conta de depósito ou de pagamento aberta perante instituição intermediária, que a oferta por meio da celebração de contrato de abertura de conta com adição de variados serviços – por exemplo, o acesso às moedas digitais oficiais –, ou o saldo pode estar mantido em conta diretamente fornecida pelo banco central, que pode assumir a responsabilidade de fornecer contas de uso geral a todos os cidadãos (BIS, 2018a, p. 10).

2.2.2 CBDC em token

A CBDC, criada por meio da emissão de *token*¹⁰ – que foi o modelo escolhido pelo BCB –, pressupõe a representação de valores registrados em banco de dados distribuído, isto é, não centralizado, no qual registros contábeis de depósitos decorrentes

¹⁰ Espécie de título ou documento que prova a titularidade sobre um crédito, ou seja, um direito pessoal patrimonial de exigir objetos, conforme as informações registradas em peculiar repositório. No Voto GRC do Banco Central do Brasil n. 68/2022 (BCB, 2022c), o termo *token* é definido como a representação de ativos existentes em uma rede que adote a tecnologia de registros distribuídos (DLT).

de coleta de valores, de pagamentos ou de transferências de recursos financeiros podem, por exemplo, ser lançados em *blockchain* ou em DLT (DE LEON *et al.*, 2017, p. 287).

Token será conceituado de modo diferente conforme a abordagem teórica adotada. A tradução literal da palavra inglesa remete a “símbolo”. Na área das ciências tecnológicas em geral, usualmente é admitido como sistema ou dispositivo eletrônico com senha. Quando se volta ao universo dos modelos de bancos de dados criados com base em registro distribuído, para as finanças, o *token* é a representação de um crédito, ou seja, um direito pessoal patrimonial de exigir objeto registrado conforme o valor de mercado (BARROSO, 2022, p. 7).

Discorda-se de quem o aceita como uma técnica contábil usada para armazenar dados como saldo do cliente, sua identidade, seu endereço, sua assinatura digital, dentre outros (BARROSO, 2022, p. 6). Ora, o *token* pode ser usado para armazenar informações ou ser ele próprio a materialização do objeto avaliável economicamente, ou seja, do direito. Nessa hipótese, por exemplo, por intermédio, da tecnologia *blockchain*, bens, direitos e deveres, relacionados ao meio material ou imaterial – *off chain* – passam a ser materializados em *tokens* – *on-chain* (TCU, 2020, p. 17).

A relevância do *token* para representar objetos está relacionada à possibilidade de ser emitido em associação aos *smart contracts* ou “contratos inteligentes”¹¹, isto é, condições ou comandos fornecidos em linguagem de programação e expressos em combinação de *hardware* e *software*, e que, ao ser acionado, gera consequências preestabelecidas. Eles fazem uso do operador lógico “se...então”, como ilustrado a seguir:

Figura 2 – Lógica básica dos contratos inteligentes.



Fonte: ANBIMA, 2022, p. 20 (adaptado)

¹¹ A expressão cunhada por Szabo (1994) foi colocada entre aspas para ressaltar que ela é alegórica. Isso porque se refere à espécie de linguagem de programação para código de computador que se torna autoexecutável, daí fala-se em “inteligente” (SILVA; OLIVEIRA, 2023, p. 153). Mas é preciso ter em mente que a expressão “contrato inteligente” não se confunde com contrato como típico negócio jurídico e não possui raciocínio cognitivo próprio.

Por que não admitem violação (SZABO, 1994), os “contratos inteligentes” permitem executar os termos de condições preestabelecidas, sendo à prova de falsificação e erros de execuções humanas (CONG; HE, 2017, p. 9).

A combinação de *tokens* e *smart contracts* pode ser verificada em banco de dados distribuídos com adoção da tecnologia *blockchain* ou DLT, a seguir explicadas.

2.2.2.1 Blockchain

A *Blockchain* é uma base de dados distribuída¹² que possui três características principais. A primeira é que tal tecnologia é construída com base em livros-razão distribuídos, isto é, uma rede de banco de dados é mantida e revisada de maneira independente pelo participante (nó da rede). Nela os dados são armazenados em blocos e disponíveis em todos os pontos de maneira transparente, pois a criptografia utilizada para encadear os blocos, em rede *Peer to peer* – criptografada de ponto a ponto (SAKAMOTO, 2020, p. 29) – garante a rastreabilidade dos registros.

A segunda característica diz respeito ao carimbo de data de hora (*time stamp*), vista como uma segunda camada de segurança, pois todos os dados que entram na rede possuem registro exato de sua entrada, incluindo hora, data e histórico de modificações. Nela os dados são distribuídos em listas encadeadas de blocos (*chain* ou cadeia), vinculados entre si, protegidos por criptografia (WBG, 2017, p. 15), sendo organizados de forma linear e cronológica, e cada bloco é vinculado ao anterior. Fala-se que ela é um registro imutável (TSUCHIYA, 2022, p. 7).

A terceira é da assinatura digital com a função *hash*¹³ (SUBRAMANIAN, 2019a). Os blocos possuem identificador chamado *hash*, cujo número é único e permite identificar tanto o bloco como todo o seu conteúdo. Qualquer alteração dentro do bloco, dessa forma, fará com que o *hash* mude e invalide toda a cadeia subsequente.

¹² Importante destacar que rede distribuída não é sinônimo de rede descentralizada. O diagrama de Baran (1962), desenhado em 1964 sobre redes, que pode ser encontrado facilmente em busca na internet, ajuda a entender. A característica básica que as diferenciam é que na rede descentralizada não há autoridade central, enquanto na distribuída essa autoridade pode existir, mas a informação na rede distribuída não está concentrada, pois cada computador tem uma cópia do sistema (O QUE SÃO..., 2019; SUBRAMANIAN, 2019).

¹³ “Algoritmo matemático que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo” (DONOHUE, 2023).

Conjugadas tais características, pode-se afirmar que a *blockchain* não necessita, portanto, de intermediário para a verificação das atividades nela realizadas (SUBRAMANIAN, 2019b).

Bitcoin é exemplo de criptomoeda que faz uso da tecnologia *blockchain* (NAKAMOTO, 2008). A Pier - Plataforma de Integração de Informações das Entidades Reguladoras – é exemplo de solução *blockchain* para consultas de dados entre o Banco Central do Brasil (BCB), a Comissão de Valores Mobiliários (CVM) e a Superintendência de Seguros Privados (SUSEP) (PLATAFORMA...2020)¹⁴, mas outras aplicações podem ser encontradas além da área financeira, como é o caso das anotações de prontuários médicos e da plataforma do e-notariado do Colégio Notarial do Brasil/Conselho Federal (CNB/CF), que também podem utilizar tal tecnologia (GUSSON. 2023).

Como se verá a seguir mediante a conceituação e classificação de DLTs, a *blockchain* é um tipo de DLT que dela se diferencia pela forma de organização dos dados feitas em blocos.

2.2.2.2 Distributed Ledger Technology (DLT)

A DLT se refere a todas as tecnologias que distribuem de maneira descentralizada seus dados (TSUCHIYA, 2022, p. 7). Nela, o banco de dados compartilhado é replicado e sincronizado de forma descentralizada entre todos os membros da rede, na qual cada nó possui uma réplica do livro razão e se atualiza de forma independente (RAY, 2020). Sendo perceptível que a conceituação de DLT é muito próxima à de *blockchain*, pois DLT é gênero, do qual a *blockchain* é espécie. São exemplos de DLTs: a *blockchain*, grafos acíclicos direcionados (DAG), *Holochain* e Hashgraph, dentre outros.

¹⁴ A Pier funciona como banco de dados para consulta de informações referentes a processos punitivos de empresas e administradores, histórico de atuação no sistema financeiro e participação de pessoas físicas e jurídicas no controle acionário de empresas. Ela substitui o processo que antes era manual por ofício entre o BCB, CVM e SUSEP. E assim, a *blockchain* permite a autenticidade das mensagens trocadas, garantindo quem as acessou por meio de assinatura digital registrada. Sua funcionalidade também assegura a imutabilidade e integridade dos dados gravados, sem necessitar de entidade central (PLATAFORMA..., 2020).

2.2.2.2.1 Tipos de configuração de DLTs: públicas, privadas, permissionadas e não permissionadas

A tecnologia de registros distribuídos, isto é, a DLT pode ser configurada em quatro tipos: permissionada e pública; permissionada e privada; não permissionada e pública; não permissionada e privada. Essas classificações se relacionam ao modo de acesso que os participantes têm ao banco de dados e à espécie de mecanismo de consenso escolhida para poderem atuar na DLT.

“Acesso” é o meio pelo qual o participante é autorizado a entrar na rede e a visualizar o *log* de dados¹⁵ (BLOCKCHAIN..., 2020), por cuja via pode ler ou dar início ao registro de informações no livro-razão, como pagamentos ou transferências, que serão disponibilizados para os demais participantes do banco de dados (BENOS; GARRAT; GURROLA-PEREZ, 2017, p. 10).

Tomando o acesso como o indicador, as subdivisões das DLTs se dividem em públicas ou privadas:

- Na **DLT de acesso público**, qualquer pessoa pode ler e visualizar o livro-razão (*ledger*) (BENOS; GARRAT; GURROLA-PEREZ, 2017, p. 7), pois existem barreiras muito baixas ou inexistentes para a entrada de novos usuários (XU; WEBER; STAPLES, 2019, p. 28). No contexto hipotético de CBDC com acesso público, qualquer um pode adentrar ou sair da rede, sendo possível visualizar todo o *log* de pagamentos ou transferências realizados (BLOCKCHAIN..., 2020; ITU, 2017, p. 14).

Em 2018, o BNDES lançou consulta pública para avaliar solução denominada “BNDESToken”. O objetivo era criar DLT lastreada no Real e se voltava para registrar atividades de concessão de crédito e transferência de recursos do BNDES para entidades de financiamento, públicas ou privadas (TCU, 2020, p. 35). Como se trata de aplicação de recursos públicos em operações de crédito, o acesso a essas informações foi planejado em DLT pública (BNDES LANÇA..., 2018).

Destaque-se que o acesso público facilita a concorrência, a inovação e a produtividade, no entanto, é avaliado como o modelo mais comprometedor da privacidade e da proteção de dados (BENOS; GARRAT; GURROLA-PEREZ, 2017, p.

¹⁵ Expressão utilizada pelo BCB, que pode ser entendida como o processo de registrar eventos relevantes ocorridos no sistema computacional.

8) porque, ao entrar na rede sem necessitar de permissão, é possível obter quaisquer informações registradas no banco de dados (XU, WEBER e STAPLES, 2019, p. 22,173).

- Na **DLT de acesso privado**, o modelo escolhido pelo BCB para a CBDC brasileira, somente usuários autorizados podem entrar, pois o acesso é controlado por autoridade central (XU; WEBER; STAPLES, 2019, p. 28). Dessa forma, apenas algumas pessoas podem visualizar as atividades registradas na rede (BLOCKCHAIN..., 2020), isto é, apenas participantes aprovados têm acesso aos dados ali veiculados (BENOS; GARRAT; GURROLA-PEREZ, p. 7).

No que se refere à “participação no mecanismo de consenso”, identifica-se quem pode atuar como nó validador das informações registradas no livro-razão e qual mecanismo de consenso poderá ser utilizado para fazê-lo (BLOCKCHAIN..., 2020). A participação como validador pode ser autorizada de forma indeterminada a quaisquer sujeitos ou a um grupo previamente determinado, resultando em duas classificações¹⁶:

a) a **DLT não permissionada (*permissionless*)**, espécie de livro-razão público, em que qualquer um pode adentrar e se tornar validador do pagamento ou da transferência de forma descentralizada, isto é, não necessitando da permissão de terceiros (WÜST e GERVAIS, 2018, p. 1). Nela, todos os nós, de maneira descentralizada, mantêm a integridade da rede por meio do mecanismo de consenso escolhido (*Proof of Work* – PoW ou *Proof of Stake* – PoS). Na estrutura do sistema mantido em DLT não permissionada, cada um dos nós mantém cópia idêntica à cadeia e possuem a responsabilidade de manter a integridade do livro razão (ITU, 2017, p. 14). O exemplo clássico de rede não permissionada é o *Bitcoin*, em que qualquer pessoa pode atuar como nó validador;

b) a **DLT permissionada (*permissioned*)** de livro-razão privado, em que há necessidade de terceiro (autoridade central) permitir que participantes pré-selecionados, atuem como nós específicos, verificando a validade de cada registro e os adicionando no banco de dados (MIRCHANDANI, 2019, p. 1211), isto é, apenas participantes

¹⁶ Alguns preferem utilizar apenas blockchains públicas – abertas ou não permissionárias – e blockchains privadas – fechadas ou permissionárias (MOREIRA *et al.*, 2021, p. 47), associando as primeiras ao movimento cyberpunk (MELICHOVÁ, 2006) ou criptoanarquia (MAY, 1992; DE FILIPPI, 2018) idealizado com a criação do Bitcoin (NAKAMOTO, 2008).

autorizados podem ler o conteúdo, gravar a mensagem no livro-razão (WÜST; GERVAIS, 2018, p. 1) e atuar na rede (WÜST; GERVAIS, 2018, p. 2).

Ela se assemelha aos bancos de dados centralizados, pois depende de determinada autoridade, como departamentos governamentais ou bancos, para regular as permissões de atuação (WBG, 2017, p. 12; ITU, 2017, p. 15), que podem ser programadas para restringir a atuação dos escolhidos a determinado conjunto de dados com edições restritas na DLT (ITU, 2017, p. 16). São exemplos de DLTs permissionadas a Hyperledger Fabric (BASHIR, 2017, p. 648) e a R3 Corda (BASHIR, 2017, p. 704).

A DLT permissionada deixa de apresentar uma das características essenciais ao modelo da *blockchain*, que é o poder de resistência à censura. Na *blockchain*, geralmente, a informação cadastrada no banco de dados não pode ser interrompida ou censurada (SILVA, A. B., 2021, p. 26). De outro modo, na DLT permissionada, em que há a atuação de autoridade centralizadora e de instituições escolhidas para atuar sobre os nós da rede, pode ser que elas detenham o poder de aceitar ou não determinadas atividades executadas (BENOS; GARRAT; GURROLA-PEREZ, 2017, p. 10).

Não obstante a presença dessa crítica, localizou-se a sua adoção. A IBM, por exemplo, tem apostado no desenvolvimento de DLT permissionada voltada para resolver questões de auditoria e *compliance*, em que auditores podem visualizar e rastrear as informações sem o risco de violação ou alteração de dados (MIRCHANDANI, 2019, p. 1.214). De forma similar, a Receita Federal do Brasil (BLOCKCHAIN..., 2020), com o auxílio da plataforma baseada na tecnologia *Ethereum*, para o caso em questão é utilizado blockchain pública e permissionada, em que a Receita desenvolve mecanismo para compartilhar base de dados com o cadastro de pessoas físicas e jurídicas. A Portaria da Receita Federal do Brasil n. 34/2021 prevê o compartilhamento de dados não protegidos por sigilo fiscal com órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional e dos demais Poderes da União (art. 11, § 2º)¹⁷.

¹⁷ RFB, art. 11: “A disponibilização de dados pela RFB ao órgão ou à entidade solicitante será operacionalizada, por qualquer meio ou solução que venha a ser adotada pela Cotec, no prestador de serviços de tecnologia da informação onde estejam localizadas as bases de dados da RFB, e somente será implementada com estrita observância do disposto nesta Portaria e nas normas pertinentes à segurança da informação editadas pela RFB, mediante supervisão da Cotec. [...] § 2º Fica autorizada a disponibilização de dados do CPF e do CNPJ por meio de fornecimento de réplicas, parciais ou totais, até 31 de dezembro de 2021, período em que o órgão ou entidade solicitante deverá adotar o mecanismo

Para sintetizar o que foi explicado sobre as espécies de DLTs (ITU, 2017, p. 15), elaborou-se o seguinte esquema:

Tabela 1 – Comparação entre tipos de DLTs

Livro razão	DLT			
Classificação quanto ao tipo de acesso	Privada		Pública	
Classificação quanto ao tipo de validador da informação registrada	Permissionada	Não Permissionada	Permissionada	Não Permissionada
Quem pode ter acesso	Apenas selecionados	Apenas selecionados	Qualquer um	Qualquer um
Quem pode validar	Apenas selecionados	Qualquer um	Apenas selecionados	Qualquer um

Fonte: elaborada pela autora.

Cada algoritmo de classificação reflete um conjunto de potenciais compensações para a privacidade (RAUCHS *et al.*, 2018, p. 62). As redes privadas e permissionadas têm sido apontadas como as mais indicadas ao mercado financeiro, especialmente pela supervisão regulatória existente e pelo controle dos dados e, conseqüentemente, da privacidade dos usuários, pois os nós poderão receber funções e acessos diferentes (BENOS; GARRAT; GURROLA-PEREZ, 2017, p. 8).

2.2.2.2.2 Os mecanismos de consenso: *Proof of Work* (PoW); *Proof of Stake* (PoS); *Proof of Authority* (PoA)

O mecanismo de consenso é o procedimento usado para validar o registo de dados na DLT (RAGAZZO; CATALDO, 2021, p. 10). Pensando em registro de valores voltados para o armazenamento ou à realização de pagamentos e transferências de

de compartilhamento de dados por meio de rede permissionada blockchain ou outro autorizado pela Cotec.” (RFB, 2021)

recursos financeiros, pode-se dizer que é o mecanismo de consenso o modo como o registro de tais atividades será validado e como os negócios serão liquidados no banco de dados.

De modo geral, a escolha entre um mecanismo e outro leva em consideração: a) os níveis de segurança e privacidade que se deseja atingir; b) o gasto de energia para validar o registro de informações, como as atividades de pagamentos ou transferências; c) a escalabilidade para cada tipo no específico fim em que se deseja empregá-lo (FAHIM; RAHMAN; MAHMOOD, 2023, p. 48; TCU, 2020, p. 14).

Apurou-se que, no atual estágio de desenvolvimento das tecnologias relacionadas com validação de informações em sistemas de registros distribuídos, é perfeitamente possível configurar mecanismos de consenso conforme a necessidade e o interesse dos envolvidos. Assim, apesar de haver outros mecanismos de consenso disponíveis, para investigar se o modelo adotado pelo BCB para criar a CBDC brasileira assegura privacidade e proteção dos dados da pessoa natural do seu usuário, entendeu-se suficiente abordar apenas os três mecanismos mais conhecidos, quais sejam: o *Proof of Work* (PoW), *Proof of Stake* (PoS) e o *Proof of Authority* (PoA):

- O mecanismo de consenso denominado **Prova de Trabalho ou *Proof of Work* (PoW)** existe desde 1993, quando foi utilizado em testes¹⁸ com ataques e esgotamento de protocolos de conexão de rede. Somente em 2008, foi utilizado para viabilizar movimentação de valores como os lastreados em Bitcoin (FAHIM, RAHMAN e MAHMOOD, 2023, p. 47), em cujo contexto os validadores (nós da rede ou *nodes*), são chamados de mineradores (*miners*), pois a autenticação de blocos ocorre pela denominada atividade de mineração (FAHIM, RAHMAN e MAHMOOD, 2023, p. 48).

O processo de validação no *Proof of Work* (PoW) consiste em uma competição (*hashrate*) estabelecida entre os nós da rede (*nodes*) para adivinhar o número aleatório do *hash* (BAINS, 2022, p. 14). Para alcançar a resposta do quebra-cabeça criptográfico (*cryptographic puzzle*), o validador precisa valer-se de força bruta, fazendo uso de computadores com alto poder de processamento para chegar ao resultado da operação matemática, do cálculo do valor do *hash* (KAUR *et al.*, 2021, p. 80.935). Nesse tipo de mecanismo, o validador trabalha usando seus recursos tecnológicos para solucionar problema matemático, que exige elevado dispêndio de recursos financeiros, pois

¹⁸ Nesses testes o intuito era tentar esgotar a conexão da rede, sobrecarregando os recursos do servidor e impedindo que ele respondesse a consultas válidas, enviando a ele grande quantidade de solicitações de conexão que acabam sendo deixadas sem resposta (JUELS; BRAINARD, 1999).

envolve a aquisição de computadores de alto nível de processamento e gasto de energia. Assim, na hipótese de o validador chegar ao resultado matemático esperado, os outros nós confirmam se o resultado no qual o minerador chegou é realmente válido. Ao ser confirmada, a informação adentra na cadeia principal de dados, sendo criado um *nonce* para ela.¹⁹

Existe a possibilidade de cada um dos nós resolver o problema sozinho, ou criar cadeia de blocos paralelos com vários nós, o que é conhecido como *fork* (bifurcação) (BAINS, 2022, p. 14). Essas bifurcações da cadeia são temporárias, pois todos os nós devem se mover pela cadeia mais longa e as outras menores são descartadas pelo protocolo (ITU, 2017, p. 15). Todavia, a existência de subcadeias tornam a rede lenta, onerosa e ineficiente, pois a criação de bifurcações consome alto poder computacional (BAINS, 2022, p. 14).

A recompensa pelo trabalho do validador pode se dar de duas formas: com o recebimento de novos blocos (BAINS, 2022, p. 14) ou de taxas pelas atividades que executa. Existem formas de evitar que o nó aumente demasiadamente seu potencial de receber muitas recompensas, e detenha grande quantidade de blocos de dados na cadeia. O *Bitcoin*, por exemplo, possui protocolo de redução das recompensas a cada quatro anos, isto é, em maio de 2020, a recompensa do bloco caiu de 12,5 bitcoins para 6,25 bitcoins (BAINS, 2022, p. 14).

O principal benefício do *Proof of Work* é a escalabilidade, conceito relacionado à arquitetura do software²⁰, que significa a capacidade de suportar altos volumes de informações ao mesmo tempo e possibilitar a expansão de suas funcionalidades (SCHNEPF, 2023). Na prova de conceito baseada em trabalho permite-se que qualquer pessoa participe da rede, minerando blocos de forma independente, como visto anteriormente, o que promove maior escalabilidade da rede.

¹⁹ O bloco possui duas informações principais que permite identificá-lo: o *hash* e o *nonce*. O *hash* é o valor numérico proveniente do processo de validação, *hash rate* ou cálculo matemático em busca da descoberta do hash e permite com que um bloco esteja interligado com os demais blocos da cadeia, já o *nonce*, é o identifica um determinado bloco em específico, como se fosse seu “nome próprio”.

²⁰ A parte física dos computadores, como por exemplo, o teclado utilizado para a escrita dessa dissertação e o monitor utilizado pelo leitor são exemplos de *hardware*. Enquanto *software*, segundo a Lei n. 9.609, de 19 de fevereiro de 1998, a Lei de Software, pode ser definido como programa de computador, isto é, “a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados” conforme art. 1º da mencionada lei (BRASIL, 1998; LUCAS *et al.*, 2008, p. 3-10).

Apesar de essa característica ser interessante para a modelagem de CBDC, pois permitiria a viabilizar maior inclusão da população no sistema financeiro, ela é contraindicada para o caso brasileiro. Primeiro, porque, nas redes públicas que adotam o protocolo de consenso do *Proof of Work*, qualquer pessoa pode participar da rede. Por mais que ofereça maior escalabilidade, não seria indicada para a CBDC brasileira em razão do prévio controle de entrada que é feito pelo Estado brasileiro. Depois, porque o PoW apresenta problemas relacionados à segurança, à latência e a gasto energético (BIS, 2018b, p. 15).

A validação via PoW pode gerar riscos à segurança da rede, em razão do “ataque dos 51%”. Como explicado anteriormente, existem criptomoedas como o Bitcoin, que criam formas de reduzir o poder dos validadores na rede, diminuindo progressivamente no tempo a quantidade de recompensas. Isso é feito exatamente para evitar que os nós possuam controle sobre mais da metade da rede e, maliciosamente, realizem duas negociações ao mesmo tempo (KAUR *et al.*, 2021, p. 80.936). Nesse tipo de fraude, o usuário recebe duas vezes pela mesma moeda (PROOF..., 2023), o que se denomina “gasto duplo”. O problema do gasto duplo é apontado como potencial para *tokens* digitais, pois o usuário pode utilizar o mesmo *token* em pagamentos ou transferências diferentes, gastando aquilo que ele não possui (BARROSO, 2022).

O PoW apresenta alto nível de latência, isto é, o tempo gasto para a comunicação e o processamento de alguma informação na rede é mais lento. Isso ocorre em razão da própria arquitetura desse software, que depende de elevados níveis de energia e poder computacional para resolução do desafio. O *Bitcoin*, por exemplo, leva, aproximadamente, 10 minutos para criar o bloco (KAUR *et al.*, 2021, p. 80.935).

No caso do Brasil, é contraindicado PoW dada a eficiência do Sistema de Transferência de Reservas (STR), que realiza a Liquidação Bruta em Tempo Real (LBTR)²¹, e do Pix, que permite processar e liquidar pagamentos e transferências instantâneos e porque se espera que o Drex viabilize a liquidação atômica de negócios envolvendo objetos tokenizados em geral (BCB, 2023a, p. 2, 5).

Inegável o grande avanço alcançado para o sistema de pagamentos do início do século XXI, mas a prova de trabalho proposta por Satoshi Nakamoto (NAKAMOTO, 2008) incorre em altos gastos de energia, ao buscar soluções para os problemas

²¹ Resolução BCB n. 105/2021, art. 3º: “A finalidade do STR é possibilitar transferência de fundos entre seus participantes. § 1º As obrigações, no âmbito do STR, atinentes às transferências de fundos de que trata o caput são liquidadas em tempo real, operação por operação” (BCB, 2021a).

matemáticos criptografados (KOHLI *et al.*, 2022, p. 83). A energia consumida em um ano pela Prova de Trabalho do *Bitcoin* para minerar o bloco é comparado a 140 *Terawatt-hora*²² de consumo na Polônia (BAINS, 2022, p. 14), isto é, a mineração utilizando PoW possui consumo de energia anual compatível ao do país com quase quarenta milhões de habitantes (KOHLI *et al.*, 2022, p. 81). Ora, o desenvolvimento econômico, consubstanciado em novas formas de pagamento, não deve sobrepujar o direito de todos ao meio ambiente ecologicamente equilibrado expresso no art. 225 da CRFB (BRASIL, 1988a), sendo necessário evitar o desperdício energético.

• O *Proof of Stake* (PoS) ou prova por participação foi implementado em 2011, justamente em decorrência da busca de soluções para o alto gasto energético despendido no PoW. No *Proof of Stake*, os nós da rede são *selecionados* para validarem os blocos, não sendo necessário gasto computacional para realizar a mineração por meio de força de trabalho. No PoS, os novos blocos são *cunhados* ou *forjados* ao invés de minerados porque a seleção do nó é feita na rede com base em determinada quantidade de registros que o validador efetivou. Com isso, primeiro seleciona-se o validador, de forma aleatória com base na quantidade de registros que possui, em seguida, um bloco é apresentado a ele e, posteriormente, ele irá atuar no processo de validação do mencionado bloco (BAINS, 2022, p. 15).

A recompensa desse validador pode ocorrer, geralmente, de três formas: a) recebimento de taxas ou custos associados à atividade que realiza; b) pagamentos em *tokens* internos de ativos não contábeis dados como garantia; e c) recompensas para a reputação do validador (RAUCHS *et al.*, 2018, p. 57).

No PoS é comum a presença do problema conhecido como *Nothing at Stake*, traduzido do inglês como “nada em jogo”. Ele ocorre quando várias bifurcações na cadeia são criadas pelos validadores que desejam obter recompensas maiores por meio de taxas associadas à sua atividade de validação. Ao fazer isso, tais validadores criam incertezas no processo de finalização e liquidação dos ativos (BAINS, 2022, p. 15). A solução para esses casos é penalizar o validador monetariamente. A atualização

²² Em escalas de medidas eletrotécnicas há o Watt (W), Kilowatt (Kw), Megawatt (MWh), Gigawatt (GWh) e o Terawatt (TWh). O Watt-hora (Wh) é unidade de medida de energia, utilizada, geralmente, em eletrotécnica. Um Watt-hora, portanto, significa a potência de um Watt por período de uma hora. O Terawatt-hora são mil gigawatts-hora (KWH..., 2024).

maliciosa dos nós, portanto, é punida com a perda ou congelamento de seus investimentos (FAHIM; RAHMAN; MAHMOOD, 2023, p. 49).

O congelamento de recursos é importante para a CBDC, especialmente para o cumprimento de ordens judiciais e casos de golpes em que o BCB e a instituição financeira ou de pagamento devem ser notificados para bloquear valores mantidos nas carteiras digitais de Drex, por exemplo. Ocorre que a adesão do mecanismo de PoS para a CBDC possui alguns desafios, quais sejam: a segregação financeira, a centralização de poder e a especulação financeira, que impedem sua aplicação para a moeda digital.

O mecanismo de consenso PoS tende a desestimular a inclusão financeira, uma das motivações dos bancos centrais para a implementação de CBDCs. Isso porque, para adentrar a rede cujo mecanismo é o PoS, o validador já deve possuir criptomoedas. Tal mecanismo, assim, apresenta uma primeira barreira de entrada – a financeira. Além disso, à medida que o validador é selecionado, o algoritmo de seleção tende a escolhê-lo mais vezes, o que pode estimular usuários com menor poder monetário a sair da rede, pois não recebem recompensas.

A proposta de finanças descentralizadas – *descentralized finances* (DeFi) – existente nos modelos DLT, consequentemente, também pode ser abalada em razão do fato de que aqueles grupos de indivíduos – ou entidades mais ricas – e que detêm a maior probabilidade de serem selecionadas, recebem maiores recompensas. Isso acarreta, portanto, potencial centralização de poder e consequente segregação financeira (BAINS, 2022, p. 15).

Outro ponto do PoS que influencia negativamente sua adoção na CBDC é que, ao tentar acumular moedas para ser eventualmente selecionado como validador, o nó da rede está gerando a possibilidade de especulação financeira retirando ativos de circulação. Os participantes, para atingir altos níveis de importância dentro do sistema, podem formar cartéis de validadores, gerando maior centralização no mecanismo e manipulação do sistema financeiro (BAINS, 2022, p. 15), o que não se pode admitir em moeda digital de banco central, em razão do impacto negativo desse ponto na política monetária da nação.

- O mecanismo de **Prova de Autoridade** ou *Proof of Authority* (PoA) foi desenvolvido especialmente como resposta para as *Blockchains* ou DLTs privadas e permissionadas (XU *et al.*, 2019, p. 39) por Gavin Wood, cofundador da Ethereum, que, em 2017, utilizou o termo pela primeira vez (FAHIM; RAHMAN; MAHMOOD, 2023, p. 49). Na Prova de Autoridade, como o próprio nome sugere, apenas as autoridades

confiáveis – moderadores participantes pré-aprovados – verificam os blocos e as atividades de pagamentos ou transferências. Ademais, em razão dos validadores serem escolhidos pela autoridade central, não é necessária a rivalidade técnica existente no PoW, Tal mecanismo, dessa forma, é apontado como o que menos consome eletricidade, sendo possível, até mesmo, executar pagamentos ou transferências simultâneas (NRB, 2022, p. 38).

Esse é, portanto, o mecanismo que mais se assemelha ao proposto pelo Banco Central do Brasil (BCB, 2023). Entretanto, existem pontos de atenção que devem ser observados e são mais bem apresentados no capítulo 4 desta dissertação.

Por ora, elaborou-se a tabela a seguir, na qual são organizados os conceitos e as especificidades de cada mecanismo de consenso abordado:

Tabela 2 – Semelhança e diferenças dos mecanismos de consenso PoW, PoS e PoA.

	PoW Prova de Trabalho	PoS Prova de validação	PoA Prova de Autoridade
Descentralização	Mais alto nível de descentralização	Relativamente mais centralizado	Mais centralizado
Latência	Maior demora no processamento (10 min.)	Relativamente rápido (1 min.)	Mais rápido
Energia	Alto consumo	Baixo consumo	Baixo consumo
Segurança	Apresentado dificuldade de supervisão e Ataque dos 51%	Ainda pode ser comprometida com o ataque dos 51% por agentes maliciosos	Apontados como segura, pois reduz a possibilidade de ataque dos 51%
Método de validação	Competição entre mineradores Resolução de equações ou algoritmos criptografados	Validadores apostam suas moedas	Validadores, pré-aprovados, “apostam” sua reputação
Agentes	Mineradores (<i>miners</i>)	Validadores (<i>stakers</i>)	Autoridades (<i>authorities</i>)
Recompensa	Recebem criptomoedas	Recompensados por criptomoedas ou taxas embutidas nas atividades que realizou	Taxas embutidas nas atividades que realizou
Dependem de	Alto poder computacional	Poder aquisitivo / quantidade de blocos que o nó já possui	Autoridade central escolher os participantes

Exemplos de usos	Criptomoedas como: Bitcoin (BTC), Litecoin (LTC), Dogecoin (DOGE)	Criptomoedas como: Ethereum (ETH)	Blockchains como a Hyperledger e Ripple
------------------	--	--------------------------------------	--

Fonte: BAINS, 2022; FAHIM; RAHMAN; MAHMOOD, 2023; PROOF..., 2023; SEGURA, 2019 (adaptado).

Feitas tais considerações sobre os mecanismos de consenso mais utilizados em sistemas de tecnologia de registro distribuído, pode-se concluir que o *Proof of Authority* é o que faz sentido para a CBDC brasileira, especialmente por ser direcionado para ambientes permissionados.

Vistos os dois tipos de classificação de CBDC conforme o modelo de banco de dados adotado, centralizado para CBDC em conta e descentralizado, para CBDC em token, passa-se a tratar das duas classificações que levam em consideração a presença ou não de intermediários na criação da moeda digital emitida por banco central.

2.2.3 CBDC atacado

A CBDC de atacado (*wholesale*), justamente o modelo escolhido pelo BCB, é aquela cuja emissão ocorre diretamente pela autoridade monetária para os participantes escolhidos, semelhante ao que se tem atualmente com as instituições titulares de contas de reserva²³ e de contas de liquidação abertas perante o BCB (RAGAZZO; CATALDO, 2021, p. 23).

2.2.4 CBDC de varejo

Na opção de varejo, a CBDC é ofertada ao público em geral de forma similar a que se vê atualmente com o papel moeda emitido pelos bancos centrais. Com isso, a ela seria a representação digital da moeda física, constituindo-se de meio de liquidação de obrigações (NEVES; DINIZ; RAMOS, 2023, p. 113) no qual os bancos centrais tomariam novamente o poder de criação da moeda para si, ocorrendo a chamada

²³ Nas contas de reservas abertas perante o BCB, os bancos autorizados e a Caixa Econômica Federal (CEF) realizam o depósito das moedas que coletam da população em contas de depósito (RAGAZZO; CATALDO, 2021, p. 23; NEVES; SILVA; COSTA, 2021, p. 42-47).

“devolução monetária”, em que as autoridades estatais retomam o poder de criação da moeda antes pertencente aos bancos privados por meio da intermediação financeira (SALAMA; ZELMANOVITZ, 2023, p. 4).

Elaborou-se, a seguir, tabela comparativa ressaltando objetivamente as principais diferenças entre CBDC de atacado e de varejo:

Tabela 3 – Comparação entre CBDC de varejo e de atacado.

	CBDC de varejo	CBDC de atacado
Formato	Digital	Digital
Acesso	Amplio	Restrito
Emissor	Banco central emite e disponibiliza ao público diretamente	Banco central emite e conta com instituições financeiras para liquidar as negociações
Tecnologia	Token ou conta	Token ou conta

Fonte: adaptado de Bech e Garrat (2017).

Após a compreensão do que é CBDC, das espécies que podem ser criadas e dos aspectos tecnológicos que podem estar envolvidos com sua emissão, examina-se o modelo escolhido pelo BCB ao planejar a emissão da moeda digital brasileira.

2.3 O processo de criação da CBDC brasileira

Com intuito de gerar maior eficiência no mercado financeiro brasileiro, aumentar a inclusão da população no sistema financeiro e incrementar os pagamentos transfronteiriços, o Banco Central do Brasil planeja emitir o Real por meio representação eletrônica, isto é, sob a forma de moeda digital que terá paridade de um para um (1:1) com o Real emitido em meio físico (notas de papel e moedas metálicas). Pretende-se criar infraestrutura que possibilite transmitir a todos os usuários a confiabilidade da moeda oficial (RAGAZZO; CATALDO, 2021, p. 2) e que qualquer pessoa possa utilizá-la como meio de troca (SALAMA; PRATES, 2022, p. 449).

Esse planejamento foi oficializado por meio da Portaria BCB n. 108.092 de 20 de agosto de 2020 (BCB, 2020),²⁴ que constituiu o Grupo de Trabalho

²⁴ A Resolução BCB n. 273 de 12 de dezembro de 2022 que constituiu o Grupo de Trabalho Interdepartamental “GTI Tokenização”, foi alterada posteriormente pela Resolução BCB n. 359 de 06 de dezembro de 2023 (BCB, 2023e). Isso porque, foi acrescido em suas competências interdisciplinares a

Interdepartamental (GTI) de natureza consultiva para estudar sobre a viabilidade de emissão da moeda digital pelo BCB. Em 24 de maio de 2021, foram divulgadas as primeiras diretrizes do Real Digital, dentre elas, o interesse pela busca da promoção de novos meios de pagamentos e por acompanhar as discussões sobre moedas digitais empreendidas por outros bancos centrais ao redor do mundo (BCB, 2021a).

Ao longo do segundo semestre de 2021, o BCB promoveu *webinars* para debater a criação da CBDC com a sociedade, contando com a participação de representantes dos provedores de serviços de movimentação de recursos financeiros (*fintechs* e bancos), provedores de tecnologia (infraestrutura tecnológica para mercados financeiros e *bightechs*) e a sociedade em geral (BC PROMOVE..., 2021).

Tais discussões levaram à criação do desafio LIFT Challenge Real Digital, cujo objetivo foi selecionar ideias de soluções viáveis para a emissão da moeda digital brasileira. Por meio de parceria firmada entre a Federação Nacional de Associações dos Servidores do Banco Central (FENASBAC) e o BCB, 9 (nove) dos 43 (quarenta e três) inscritos foram selecionados e propuseram, por exemplo, o desenvolvimento de infraestrutura que considerasse a privacidade das informações empregadas, com observância da legislação pertinente²⁵ (BCB, 2022b).

O diálogo firmado entre o BCB, as instituições privadas e a sociedade, levou à consolidação da concepção quanto à importância da manutenção da intermediação de instituições financeiras para a promoção da alavancagem de crédito e à atualização das diretrizes do Real Digital por meio da edição do Voto BCB n. 31/2023 (BCB, 2023c), com expressa adoção de plataforma distribuída (DLT) (AGENDA..., 2023).

Na tabela a seguir, a lista das primeiras diretrizes (BCB, 2021a) é comparada com a lista das novas (BCB, 2023b), tendo sido dado destaque em negrito e itálico para os itens relacionados ao problema principal investigado. Na coluna dessa lista, apresenta-se classificação que toma os seguintes parâmetros como indicadores: a) a ausência de mudanças, nos casos em que o texto da diretriz permaneceu inalterado; b) mudanças leves para aquelas em que houve alterações semânticas e de sintaxe textual,

proposição de recomendações sobre atividades referentes às tecnologias de registro distribuído (Distributed Ledger Technologies - DLTs).

²⁵ O desafio continha quatro eixos temáticos, além da privacidade já citada. Deviam compor, também, a estrutura a ser desenvolvida pelos participantes: a interoperabilidade com outros sistemas de pagamento, disponíveis tanto no atacado quanto no varejo; a escalabilidade da solução, voltada para aplicações de varejo nacionais; e, por fim, a programabilidade, no intuito de permitir a inovação e a construção de novas soluções e produtos com base da plataforma criada (BCB, 2022b).

mas que preservaram o cerne do conteúdo da diretriz original ou o alteraram de maneira sutil; c) mudanças altas para as alterações estruturais significativas do que havia sido proposto inicialmente.

Tabela 4 – Comparação entre diretrizes do Real Digital de 2021 e 2023.

Diretrizes 2021	Diretrizes 2023	Conclusões – Classificação da mudança
Ênfase na possibilidade de desenvolvimento de modelos inovadores com base em evoluções tecnológicas, como contratos inteligentes (<i>smart contracts</i>), internet das coisas (<i>IoT</i>) e dinheiro programável;	Ênfase no desenvolvimento de modelos inovadores com a incorporação de tecnologias, como contratos inteligentes (<i>smart contracts</i>) e dinheiro programável, <i>compatíveis com liquidação de operações por meio da “internet das coisas” (IoT)</i> ;	Mudança leve
Previsão de uso em pagamentos de varejo;	Emissão do Real Digital pelo BCB, como meio de pagamento, a fim de dar suporte à oferta de serviços financeiros de varejo liquidados por meio de tokens de depósitos em participantes do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB);	Mudança alta
Emissão pelo BCB, como extensão da moeda física, com a distribuição ao público intermediada por custodiantes do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB);		
Capacidade para realizar operações online e eventualmente operações offline;	Foco no desenvolvimento de aplicações online, mantendo em vista a possibilidade de pagamentos offline;	Mudança leve
Ausência de remuneração;	(sem correspondência)	Mudança alta
Garantia da segurança jurídica em suas operações;	Garantia da segurança jurídica nas operações realizadas na plataforma do Real Digital;	Não houve mudança
Aderência a todos os princípios e regras de privacidade e segurança determinados, em especial, pela Lei Complementar n. 105, de 2001 (sigilo bancário), e pela Lei Geral de Proteção de Dados Pessoais;	Observância a todos os princípios e regras de privacidade e segurança previstos na legislação brasileira, em especial na Lei Complementar n. 105, de 10 de janeiro de 2001 (sigilo bancário), e na Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);	Leve
Desenho tecnológico que permita integral atendimento às recomendações internacionais e normas legais sobre prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa, inclusive em cumprimento a ordens judiciais para rastrear operações ilícitas;	Desenho tecnológico que permita integral atendimento às recomendações internacionais e normas legais sobre prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa, inclusive em cumprimento a ordens judiciais para rastreamento de operações ilícitas;	Não houve mudança
Adoção de solução que permita interoperabilidade e integração visando à realização de pagamentos transfronteiriços; e	Adoção de solução tecnológica baseada em DLT que permita: a. registro de ativos de diferentes naturezas; b. descentralização no provimento de produtos e serviços; c. interoperabilidade com sistemas domésticos legados e com outros sistemas de registro e transferência de informação e de negociação de ativos digitais regulados; e d. integração a sistemas de outras jurisdições, visando à realização de pagamentos transfronteiriços;	Mudança alta

Adoção de padrões de resiliência e segurança cibernética equivalentes aos aplicáveis a infraestruturas críticas do mercado financeiro.	Adoção de padrões de resiliência e segurança cibernética equivalentes aos aplicáveis a infraestruturas críticas do mercado financeiro.	Não houve mudança
(sem correspondência)	Aplicação do arcabouço regulatório vigente às operações realizadas na plataforma do Real Digital, evitando assimetrias regulatórias;	Mudança alta

Fonte: Elaborada pela autora com base nas diretrizes do BCB (2021; 2023).

A comparação realizada permitiu verificar relevantes alterações que podem impactar no tratamento da proteção da privacidade e dos dados pessoais, conforme análise a ser feita no Capítulo 4 desta dissertação. Por hora, cabe apenas apresentá-las.

Primeiro, a redação da diretriz que previa o uso do Real Digital em pagamentos de varejo foi aglutinada à diretriz que o admitia como extensão da moeda física. Com isso, a CBDC que era de varejo passou a ser de atacado, permitindo a oferta de serviços de pagamentos de varejo apenas por meio de *tokens* de depósitos emitidos pelas instituições financeiras e de pagamento.

A segunda alteração refere-se à previsão de observância da legislação referente à proteção da privacidade e dados pessoais, cuja nova redação, além de ter ficado mais clara, submeteu o tema a toda a legislação brasileira, além da Lei n. 13.709/2018, a LGPD (BRASIL, 2018), e da Lei Complementar n. 105/2001, a Lei do Sigilo Bancário (BRASIL, 2001).

A terceira alteração relaciona-se à realização de pagamentos transfronteiriços, para o qual a diretriz original previa a necessidade de se encontrar solução de interoperabilidade e integração, ao passo que a nova impõe a integração a sistemas de outras jurisdições.

Por fim, a quarta alteração refere-se à previsão do arcabouço regulatório vigente às atividades desenvolvidas na Plataforma do Real Digital, de modo a evitar assimetrias entre os participantes do mercado, para qual não havia diretriz original correspondente.

O BCB previu a oferta dos seguintes serviços no projeto-piloto: a) moeda de banco central oriunda de: contas de reservas bancárias; conta de liquidação e da conta única do Tesouro Nacional; b) depósitos bancários à vista; c) moeda eletrônica, na forma da Lei n. 12.865/2013 (BRASIL, 2013); e d) títulos públicos federais. Dessa forma, para operacionalizar o projeto do Real Digital, foi instituído, em abril de 2023, o Comitê Executivo de Gestão (CEG) do projeto-piloto da plataforma do Real Digital (RD), bem como aprovado o regulamento do Piloto RD, tudo por meio da Resolução BCB n. 315/2023 (BCB, 2023b).

Estabeleceu, também, que na primeira fase do piloto os testes serão realizados para avaliar a privacidade e a programabilidade mediante a implementação de protocolo de entrega contra pagamento – *Delivery versus Payment* (DvP) – de título público federal entre usuários finais (clientes) de instituições diferentes (PILOTO DREX, 2024). O mencionado teste promove a troca de informações entre os participantes da plataforma, o que permitirá a análise da privacidade do sistema, bem como a programabilidade dos serviços e, conseqüentemente, sua interoperabilidade (BCB, 2023c).

Em 26 de junho de 2023, no Fórum Real Digital (FÓRUM..., 2023), o BCB reafirmou a descentralização, a programabilidade e a privacidade como pilares a serem perseguidos no projeto de criação do Drex, apresentou alguns contratos em teste, os 16 (dezesesseis) participantes escolhidos para atuar como nós na rede DLT multiativos e os seis validadores responsáveis pelo mecanismo de consenso a ser seguido na rede, sendo quatro no site do BCB em Brasília e dois no Rio de Janeiro, no sistema Selic (DOCUMENTAÇÃO..., 2023).

Feita a explanação geral sobre o processo de criação da moeda digital brasileira e seu piloto, apresentam-se os elementos que caracterizam o modelo adotado pelo BCB na estrutura do Drex.

2.4 O modelo adotado pelo Banco Central do Brasil na estrutura do Drex

O projeto-piloto, ainda em fase de testes, pode sofrer alterações (PILOTO DREX, 2023)²⁶, por isso, o recorte temporal de análise eleito foi até fevereiro de 2024, em que apurou-se a existência de três tipos de participantes na estrutura de atacado pensada para o Drex:

²⁶ Nas palavras do BCB o “Piloto Drex” consiste na fase de testes da moeda digital brasileira. Nessa etapa, estão sendo avaliados os benefícios da programabilidade da Plataforma Drex, chamada pelo BCB de “ecossistema de tecnologia de registro distribuído multiativo”, ocasião em que estão sendo simuladas atividades com ativos digitais tokenizados liquidados (PILOTO DREX..., 2023). Em agosto e dezembro de 2023 o atual presidente do Banco Central do Brasil, Roberto Campos Neto, apostou na evolução da tecnologia aliada ao *Open Banking* para a criação do “superApp”, formalmente chamado de “agregador financeiro”, que vai agregar as instituições financeiras e de pagamento em um único local para acesso do cidadão a todas as suas contas (AGREGADORES..., 2023). Ora, seja por apostas otimistas de futurologia, seja pelo contido na Agenda BC# (AGENDA BC#, 2023) para a competitividade as potencialidades da portabilidade do Open Banking, podem até mesmo congregam as CBDCs.

- Primeiro, as **instituições autorizadas** que possuem acesso direto às contas e passivo digital do BCB e que funcionarão como os nós (*nodes*), isto é, os nós validadores do registro distribuído. Tais instituições autorizadas têm permissão concedida pelo Banco Central para conectar suas infraestruturas ao banco de dados distribuídos do Drex. Dessa forma, elas podem instalar seus nós de homologação na rede *Hyper Ledger Besu*, tendo em vista que aqui se trata de DLT privada e permissionada (MATOS, 2023).

Os 16 participantes selecionados²⁷ englobam instituições financeiras públicas e privadas, pertencentes aos segmentos prudenciais S1 a S4, instituições de pagamento, desenvolvedores de serviço de criptomoedas e de infraestruturas de mercado financeiro e instituidores de arranjos de pagamento.²⁸

- O segundo grupo de participantes são os **clientes finais**, pessoas naturais e pessoas jurídicas não financeiras, destinatárias finais da moeda. Por ora, eles são apenas usuários simulados, em razão de o piloto ainda estar na fase de testes. Tais usuários possuem em sua conta saldos mantidos em instituições financeiras (depósito à vista) ou de pagamento (moeda eletrônica) e vão acessar as versões tokenizadas desses depósitos ou moedas nas instituições financeiras (IFs) e instituições de pagamento (IPs).

- O terceiro grupo de participantes é representado pela **Secretaria do Tesouro Nacional (STN)**. No projeto, a STN emite os Títulos Públicos Federais e realiza a liquidação dos pagamentos envolvendo tais títulos, por meio da Entrega contra Pagamento – *Delivery versus Payment (DVP)* – ao usuário final.

Quanto à estrutura da CBDC brasileira, percebe-se que o Real Digital não veio para resolver problemas de pagamento de varejo, tendo em vista o sucesso de utilização do Sistema de Pagamentos Instantâneos (SPI) via Pix. Ou seja, o Drex não se propõe a substituir as moedas eletrônicas ou moedas escriturais, tampouco alterar o formato do

²⁷ O Comitê Exclusivo de Gestão (CEG), criado pela Resolução BCB n. 315/2023 (BCB, 2023b), selecionou as seguintes instituições interessadas para participar de sua execução: Nubank, Bradesco, Banco Inter, Microsoft e 7Comm, Santander, Santander Asset Management, FIRST, Toro CTVM, Itaú Unibanco, Basa, Tecban, Pinkbank, Dinamo, Cresol, Banco Arbi, Ntokens, Clear Sale, Foxbit, CPqD, AWS, Parfin, SFCoop, Ailos, Sicoob, Sicredi, Unired, XP, Visa, Banco BV, Banco BTG, Banco ABC, Hmsa, LoopiPay, Banco B3, BE Digitais, Consórcio ABBC e Banco do Brasil.

²⁸ O Anexo II à Resolução do Banco Central do Brasil n. 315/2023 (BCB, 2023b), estabelece o Regulamento do Projeto-Piloto da Plataforma do Real Digital. Nele ficaram expressos os requisitos para a participação e a seleção das instituições aptas a participar do projeto. Posto isso, o Comitê Executivo de Gestão (CEG), com base nos critérios estabelecidos no Regulamento do Piloto Drex, selecionou 16 propostas das instituições mencionadas.

SPB, pois o acesso das pessoas naturais continuará a ser viabilizado pelos agentes autorizados pelo BCB (NEVES; DINIZ; RAMOS, 2023, p. 111). Propõe-se, sim, fomentar a CBDC de atacado, com suporte a serviços de varejo liquidados por meio de *tokens* de depósito em participantes do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB)²⁹, exemplifica-se bancos, outras instituições financeiras³⁰ e instituições de pagamento³¹. Dessa forma, originam-se duas possibilidades de liquidação da moeda digital:

a) liquidação interbancária: o *token* de depósito é emitido pelas autoridades selecionadas, integrantes do SFN e do SBP. Aqui, tem-se a CBDC em seu conceito mais puro, o próprio Real Digital propriamente dito;

b) liquidação de varejo: o *token* de depósito emitido será chamado de “Real tokenizado” e destina-se à liquidação no mercado de consumo, no varejo (BARROSO, 2023, p. 5).

A opção pela tokenização é justificada pelo BCB como tendência mundial de descentralização financeira – *Decentralized Finances* (Defi) – cujo objetivo é permitir que o Brasil também tenha moeda brasileira compatível com esse ambiente. A ausência de infraestrutura harmonizável com a economia tokenizada, na visão do BCB, comprometeria até mesmo a estabilidade financeira do Brasil, tendo em vista que tais ofertas já existem no mercado privado – por exemplo, as *stablecoins*. Dito isso, a expectativa da tokenização para o Brasil amolda-se em ganhos com programabilidade,

²⁹ “13. A evolução das discussões demanda, dessa forma, a atualização do conjunto de diretrizes do Real Digital, adequando-as ao atual estágio de desenvolvimento da iniciativa. Propõe-se, com isso, o seguinte conjunto de diretrizes gerais para a plataforma do Real Digital: [...] iii) emissão do Real Digital pelo BCB, como meio de pagamento, a fim de dar suporte à oferta de serviços financeiros de varejo liquidados por meio de *tokens* de depósitos em participantes do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB); [...]” (BCB, 2023, p. 9).

³⁰ As instituições financeiras, segundo o art. 17 da Lei n. 4.595/1964 (BRASIL, 1964), são as pessoas jurídicas públicas ou privadas, que tenham como atividade principal ou acessória a coleta, intermediação ou aplicação de recursos financeiros próprios ou de terceiros, em moeda nacional ou estrangeira, e a custódia de valor de propriedade de terceiros. Podem equiparar-se às instituições financeiras, as pessoas físicas que realizam tais atividades mencionadas, seja de forma permanente, seja eventual

³¹ A instituição de pagamento é a pessoa jurídica que viabiliza serviços de compra e venda e de movimentação de recursos em arranjo de pagamento, sem a possibilidade de conceder empréstimos e financiamentos a seus clientes (BRASIL, 2013).

liquidação atômica, rastreabilidade e multiativos, conforme item 6 do Voto n. 31/2023³² (BCB, 2023c, p. 2; FANTI; POCHER, 2022, p. 15).

Por fim, a respeito da tecnologia escolhida, pode-se dizer que o Brasil optou por confiar e escolher para os testes do piloto uma solução empresarial de *blockchain* já consolidada, qual seja, a *Hyperledger Besu* (FANTI; POCHER, 2022, p. 15)³³, conforme art. 3º do Regulamento do projeto (BRASIL, 2023b)³⁴. Na coletiva feita à imprensa em 06 de março de 2023, o BCB justificou a escolha afirmando que tal tecnologia era compatível com a *Ethereum Virtual Machine* (EVM), tendo maior disponibilidade de fornecedores dessa tecnologia no Brasil e no mundo (YOUTUBE, 2023). Ademais, outra motivação expressa pelo BCB é o fato dessa plataforma ser de código aberto (*open source*), existindo vasta documentação e desenvolvimento ativo pela comunidade Hyper Ledger.

A *Hyperledger Besu* apresenta os seguintes recursos que se destacam em prol da CBDC brasileira (BARBÉ, 2017, p. 18):

- a) Programabilidade: podem fazer uso de contratos inteligentes na *blockchain Ethereum*;
- b) validação: fazem uso de mecanismo de consenso de Prova de Autoridade;
- c) armazenamento de dados e privacidade: Por se tratar de uma DLT permissionada, os dados armazenados somente serão acessíveis às pessoas autorizadas que apresentarem a chave de acesso correspondente.³⁵

³² Voto BCB n. 31/2023: “6. Os benefícios esperados da tokenização incluem: i) programabilidade: *smart contracts* oferecem novas formas de automação; ii) liquidação atômica: a troca de tokens de forma automatizada, representando a liquidação da operação e reduzindo os riscos da contraparte; iii) fontes únicas de verdade: substituem os registros em silos informacionais; e iv) multiativos: ativos de diferentes naturezas podem ser tokenizados em um mesmo ambiente de DLT” (BCB, 2023c).

³³ Em 2017 foi criada a Hyper Ledger Foundation a fim de atender demandas do mercado corporativo de sistema privado e permissionado (DE LEON, 2017, p. 288). O produto ofertado pela fundação é a plataforma tecnológica Hyperledger Besu, que é uma dentre as várias opções disponíveis no mercado de tecnologia de registro distribuído.

³⁴ Resolução BCB n. 315/2023, art. 3º: O Piloto RD tem por objetivo validar o uso de uma solução de Tecnologia de Registro Distribuído (DLT), na plataforma *Hyperledger Besu*, avaliando a programabilidade com ativos financeiros e a capacidade de observância aos requisitos legais e regulatórios, principalmente em relação à privacidade das informações de indivíduos e demais envolvidos nas transações na plataforma do Real Digital, bem como sua viabilidade tecnológica” (BCB, 2023b)

³⁵ O *Besu* mantém informações em grupo denominado “grupo privado”, que possui níveis maiores de controle e compartilhamento. Assim sendo, no *Open Finance*, em exemplo hipotético, determinada instituição financeira pode acessar atividades genéricas do usuário, mas não pode acessar dados de um grupo privado de privacidade, pois não tem acesso a ele (BARBÉ, 2017, p. 26).

d) rastreabilidade e monitoramento: essa a tecnologia apresentada que o nó validador pode ser monitorado, utilizando técnicas como *Block Explorer*³⁶.

Expostos os principais aspectos tecnológicos do Drex, a seguir abordam-se alguns pontos referentes à temática normativa da moeda digital brasileira.

Compreendido modelo adotado pelo BCB para criar o Drex, antes de enfrentar a questão principal que norteou a produção desta dissertação, passa-se ao estudo do que se deve entender por privacidade e dados pessoais e de como são regidos e protegidos pelo ordenamento jurídico brasileiro.

3 PROTEÇÃO DA PRIVACIDADE E DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

O ordenamento jurídico brasileiro protege a privacidade e os dados pessoais dos clientes do SFN e do SPB, com a imposição de limites ao Governo e às instituições financeiras e de pagamento quanto ao tratamento e armazenamento dos dados dos indivíduos. Essa postura relaciona-se, principalmente, ao fato de que os pagamentos e as transferências de valores efetuados nesses sistemas deixam rastros informacionais e históricos que denotam comportamentos dos indivíduos que os realizam. Isso pode sujeitá-los, por exemplo, a ter seus dados vendidos à sua revelia ou ser alvo da prática de fraudes. Para evitar essas e outras consequências negativas, impõe-se às prestadoras de serviços de movimentação profissional de recursos financeiros o dever de zelar pelo controle e pela integridade das informações a respeito de seus clientes e dos negócios que eles celebram nesses sistemas, bem como de cuidar para que seja processada sua devida leitura, modificação ou exclusão, conforme o caso.

A proteção de tais direitos, todavia, não é absoluta, eis que podem ser restringidos diante da necessidade de salvaguardar específicos interesses – por exemplo, coibir a prática do crime de lavagem de dinheiro. Assim é que, apesar de o usuário dos serviços prestados nesses dois sistemas ter a prerrogativa de decidir sobre como e onde investe seus recursos financeiros, o Estado pode quebrar seu sigilo bancário e rastrear as transferências de valores que ele fizer no mercado financeiro.

³⁶ A *block explorer* é uma ferramenta online que permite pesquisar em tempo real o histórico e as informações sobre a *blockchain*, incluindo dados relacionados aos blocos, atividades de pagamento e transferências eventualmente realizadas, identificando o endereço de destino, dentre outras (WHAT IS..., 2022).

Por isso, a seguir será exposto o conceito e surgimento da privacidade, dos dados pessoais, princípios e leis que norteiam seu tratamento, a nível constitucional e infraconstitucional.

3.1 Privacidade: surgimento e conceito

Como um dos fundamentos do regime jurídico de proteção de dados (BRASIL, 2018)³⁷, a privacidade pode ser conceituada conforme a vertente teórica – clássica, utilitarista, pluralista ou humanista.

O início da defesa do respeito à privacidade relaciona-se à busca da proteção da liberdade de escolha, do anseio de não ser discriminado e da igualdade no século XIX (DONEDA, 2020b, p. 31), marcado pelo surgimento da fotojornalismo³⁸ (QUEIROZ, 2009, p. 15).

Ao ser utilizada nos jornais de circulação para documentar acontecimentos históricos – por exemplo, a guerra de secessão nos Estados Unidos da América (1861 a 1865) –, a fotografia impressa passou a expor fatos relacionados ao meio empresarial ou à vida doméstica, colocando em público situações privadas ou íntimas que diziam respeito somente aos seus titulares. Naquele contexto, Warren e Brandeis (1890, p. 195), conhecidos como fundadores da privacidade moderna, defenderam que a lei deveria fornecer remédio à circulação não autorizada de retratos de pessoas particulares e invasão da privacidade por parte dos periódicos.

Surgiu, assim, o conceito clássico de privacidade, que, remarcado pela perspectiva do indivíduo e de seu direito de ser deixado só (*the right to be let alone*), admitia que nenhum conteúdo poderia ser publicado sem o consentimento do titular da informação (WARREN; BRANDEIS, 1890, p. 199). O indivíduo é quem deveria deter o controle da informação, no que se refere ao seu acesso e à decisão sobre o seu uso, especialmente se fossem informações pessoais, pois, segundo essa concepção, elas faziam parte da vida do sujeito (INNES, 1992, p. 56). A privacidade, então, estaria

³⁷ Lei n. 13.709/2018, art. 2º: “A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; [...]” (BRASIL, 2018).

³⁸ A fotojornalismo é estilo de atuação jornalística do século XIX. Seus primeiros entusiastas apontavam suas câmeras para os fatos históricos no intuito de tornar a fotografia a testemunha do acontecimento (SOUSA, 2002, p. 16-17). A título de exemplo, a foto tirada por Mathew Brady, conhecido como o primeiro fotógrafo a documentar a guerra de secessão ocorrida nos Estados Unidos em 1861 (SMYTHL, 2022), é apresentada como marco inicial da fotografia de pessoas e acontecimentos históricos.

relacionada ao controle da informação que o indivíduo possui sobre si mesmo (*information based*), àquilo que é disponibilizado aos outros e que os possibilitam acessar sobre o indivíduo (*access based*), bem como as informações sobre as decisões íntimas de suas ações (*decision based*) (INNES, 1992, p. 56).

Ocorre que a influência das novas tecnologias do século XX permitiu maior exposição do indivíduo de maneira geral. Dessa forma, o conceito de privacidade baseado somente na perspectiva individual de ser deixado só começou a ser visto como algo demasiadamente amplo, tornando a privacidade conceito genérico e de pouca aplicação prática (SOLOVE, 2007. p. 755). Ademais, essa conceituação clássica de controle mesclava os conceitos de privacidade e intimidade, que são institutos diferentes.

A variedade – e por vezes, o atrito – entre interesses públicos e privados, existentes quando se trata de dados pessoais das pessoas naturais no século XX, conduziram ao surgimento e ao fortalecimento da vertente utilitarista da privacidade (DECEW, 1997, p. 22), segundo a qual se passou a admitir que o indivíduo, baseado em seus interesses, diante do conflito entre direitos, teria o poder para determinar, por si mesmo, o equilíbrio entre a sua privacidade e os seus demais direitos (CLARKE, 1999, p. 60).

Para teoria utilitarista, a privacidade é admitida como direito de propriedade privada, para cujo exercício depende apenas da vontade do seu titular (HUNTER, 1995, *apud* TAVANI; HIMMA, 2008, p. 134). Tal concepção admite, por exemplo, que o Estado restrinja direitos individuais em casos especificados em lei, de modo a promover a segurança pública e o controle de crimes.

Esse entendimento, em termos absolutos, não tem cabimento no Estado Democrático de Direito que, apesar de assegurar prerrogativas para os cidadãos, lhe impõe, bem como às entidades privadas e ao Governo, a observância de uma série de deveres. Inexiste, portanto, direitos individuais absolutos, tal como propõe o utilitarismo individual. Também não cabe falar em poder total do Estado, como defende o utilitarismo estatal, eis que pode dar guarida ao cometimento da vigilância pelo Estado e ao descumprimento de garantias democráticas como o contraditório e a ampla defesa.

As ameaças aos direitos individuais, causadas em especial pelo terrorismo³⁹ do século XXI, motivaram a incongruente compreensão de que, se o indivíduo não tem informação sensível, constrangedora ou ilegal para ocultar, não há nada o que temer, sendo admitido, portanto, que tais informações sejam reveladas (SOLOVE, 2007, p. 747). A privacidade, entretanto, não se resume a “não ter algo a esconder” (*nothing to hide*), e o paradoxo entre privacidade e segurança é falacioso (SOLOVE, 2007, p. 62; SOLOVE, 2020).

Para tentar conter essa ampla concepção, surge o conceito pluralista da privacidade (SOLOVE, 2007, p. 758), segundo o qual o mapeamento dos problemas e dos danos decorrentes da sua violação depende de salvaguarda de situações genéricas e específicas (SOLOVE, 2007, p. 758). Assim, o resguardo da privacidade visa proteger o indivíduo e sua personalidade, mas também propósitos coletivos, como a preservação da democracia (MENDES, 2008, p. 42).

Apesar de a perspectiva pluralista trazida por Solove ter sua importância diante da revolução promovida pela disponibilidade de dados em razão das novas tecnologias que transformaram os indivíduos em “pessoas digitais”⁴⁰ (SOLOVE, 2004, p. 226), a sua amplitude também torna vago o instituto jurídico da privacidade. Ainda mais considerando-se a vigilância governamental das décadas de 1930 e 1940 e as violações à pessoa humana, especialmente sua vida privada e sua intimidade, vivenciadas durante as grandes guerras mundiais ocorridas no século XX⁴¹. Tais fatos serviram de alerta à Europa pós-guerra a respeito dos perigos decorrentes da coleta de informações privadas, pelos Estados totalitários e pelos democráticos.

Esse alerta fez ressoar a necessidade de conferir prevalência à privacidade, em prol da dignidade da pessoa humana, o que levou à introdução da concepção humanista em documentos legais de nações ao redor do mundo, criando a denominada

³⁹ O terrorismo é a prática de atos cometidos com a finalidade de provocar terror social ou generalizado, expondo a pessoa, o patrimônio, a paz pública ou a incolumidade pública, regulamentado pela Lei n. 13.260/2016 (BRASIL, 2016). Destaque-se que a Constituição Federal de 1988 (BRASIL, 1988a) considera tal ato insusceptível de graça ou anistia (art. 5º, XLIII), além disso, o repúdio ao terrorismo é um dos princípios que regem a nação brasileira em suas relações internacionais (art. 4º, VIII).

⁴⁰ A expressão “pessoa digital”, do inglês *digital person*, é usado para qualificar a personalidade de alguém em formato digital, isto é, seus registros, fragmentos de dados e informações que são captados na rede formam e atualizam a pessoa humana digitalizada (SOLOVE, 2004, p. 226).

⁴¹ A Primeira Guerra Mundial foi desavença armada que deixou milhões de mortos entre 28 de julho de 1914 a 11 de novembro de 1918. A Segunda Guerra Mundial foi conflito militar iniciado em 1º de setembro de 1939, com a invasão da Polônia pelo Estado nazista, com término em 2 de setembro de 1945, com a rendição formal do Japão. Diante das atrocidades cometidas durante os seis anos em que ocorreu a Segunda Guerra, foi criada a Organização das Nações Unidas (ONU) em 1945, com intuito de promover as relações amistosas entre as nações em prol dos direitos humanos.

convergência internacional em prol da proteção da privacidade (BENNET, 1992, p. 49). Dessa forma, o debate acerca da privacidade como direito fundamental encontrou abrigo nos discursos políticos e nos textos de declarações internacionais de direitos humanos após a Segunda Guerra Mundial⁴² – por exemplo, o art. 5º da Declaração Americana dos Direitos e Deveres do Homem (DADH), de 2 de maio de 1948 (OEA, 1948), previu que toda pessoa tem direito à proteção legal em razão de ataques abusivos à sua honra, reputação, vida particular e familiar. Poucos meses depois, isto é, em 10 de dezembro de 1948, a Declaração Universal dos Direitos Humanos (DUDH), aprovada pela Assembleia-Geral das Nações Unidas, estabeleceu que ninguém será sujeito a interferências em sua vida privada, família, lar ou correspondência, tampouco a ataques à sua honra e reputação (art. 12). Esse documento prevê que todas as pessoas possuem direito à proteção da lei contra referidos ataques ou interferências. A proteção da privacidade como direito fundamental também foi aceita na Convenção Europeia de Direitos do Homem de 1950 e no Pacto de São José da Costa Rica, nome popular dado à Convenção Americana dos Direitos do Homem de 1969⁴³.

A Carta de Direitos Fundamentais da União Europeia de 2000 reforçou a tese do direito fundamental, pois previu que todas as pessoas possuem direito à privacidade⁴⁴ e à proteção de dados⁴⁵ de caráter pessoal. Conforme tal documento, esses dados podem ser tratados desde que destinados a fins específicos mediante o consentimento do interessado, sendo expresso que tal consentimento somente pode ser afastado nos casos legais⁴⁶. Com essas previsões, a privacidade passa a ser aceita como um direito fundamental.

⁴² Importante mencionar que a criação de institutos jurídicos em prol da proteção aos direitos humanos não surge simplesmente em 1945, mas trata-se de processo histórico, pois havia instrumentos de proteção aos direitos individuais antes dessa data. Como por exemplo, a Declaração de Direitos individuais nos Estados Unidos da América de 1776 que reforçava a proteção aos direitos individuais como a vida, a liberdade e a busca pela felicidade. Bem como a Declaração do Homem e do cidadão na França em 1789 que promovia aos franceses a liberdade, a propriedade e a resistência à opressão.

⁴³ Após o processo de ratificação, tal documento foi incorporado ao conjunto normativo brasileiro por meio do Decreto n. 678/1992 (BRASIL, 1992).

⁴⁴ “Art. 7º Respeito pela vida privada e familiar: Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações” (CARTA..., 2000).

⁴⁵ “Art. 8º Proteção de dados pessoais. 1. Todas as pessoas tem direito à proteção dos dados de caráter pessoal que lhes digam respeito” (CARTA..., 2000).

⁴⁶ “Art. 8º [...] 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação” (CARTA..., 2000).

De tudo o que se viu e considerando que nem todas as informações ou decisões privadas relacionadas ao indivíduo devem se classificar tão somente como íntimas, nesta dissertação, admite-se a privacidade como direito da personalidade, porquanto esculpido no Código Civil⁴⁷, bem como um direito fundamental (DONEDA, 2020b). No contexto da utilização do Drex como meio de pagamento, tal direito garante ao seu usuário a proteção jurídica para que possa exercer sua autodeterminação informativa, mantendo-se empoderado pela titularidade de seus dados e fornecendo apenas os dados necessários à realização de pagamentos ou transferências de valores em modo tokenizado, sem comprometer sua privacidade.

A seguir conceituam-se dados e suas espécies, isto é, dados pessoais, anonimizados e pseudoanonimizados.

3.2 Dados

A Lei n. 12.527/2011 (BRASIL, 2011b) – Lei de Acesso à Informação (LAI) – conceitua informação como dados, processados ou não, que podem ser utilizados para a produção e transmissão de conhecimento, armazenados em qualquer meio ou formato e adota para informação pessoal similar definição utilizada para dados pessoais na Lei n. 13.709/2018 (BRASIL, 2018) – Lei Geral de Proteção de Dados (LGPD). Na LAI (BRASIL, 2011b), informação pessoal é admitida como aquela relacionada à pessoa natural identificada ou identificável (inciso IV do art. 4º da LAI)⁴⁸ A LGPD repete a definição de informação pessoal da LAI quando conceitua dado pessoal, ou seja, o entende como a informação relacionada a pessoa natural identificada ou identificável – inciso I do art. 5º da LGPD⁴⁹ (BRASIL, 2018).

O Decreto n. 97.057/1988 (BRASIL, 1988b), que regulamentou a Lei n. 4.117/1962 – Lei Geral de Telecomunicações (BRASIL, 1962) –, conceituou dado como “informação sistematizada, codificada eletronicamente, especialmente destinada a

⁴⁷ “Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2002).

⁴⁸ Lei n. 12.527/2011, art. 4º: “Para os efeitos desta Lei, considera-se [...] IV – **informação** pessoal: aquela relacionada à pessoa natural identificada ou identificável;” (BRASIL, 2011b, grifo nosso)

⁴⁹ “Art. 5º Para fins desta Lei, considera-se [...] I – **dado** pessoal: aquela relacionada à pessoa natural identificada ou identificável;” (BRASIL, 2018b, grifo nosso).

processamento por computador e demais máquinas de tratamento racional e automático da informação”⁵⁰.

Com base na interpretação dessas normas e na revisão das obras de Parentoni (2015, p. 550) e de Doneda (2020a, p. 139; 2020b), admite-se o dado como o gênero e a informação como uma espécie de dado. O dado é o registro em meio físico ou eletrônico que ainda não foi tratado e nem processado. A informação, por sua vez, é uma espécie de dado que foi tratado e processado. O primeiro é o registro que se apresenta em seu estado primitivo e sem a devida organização, por isso, é matéria prima que ainda não atingiu todo o seu potencial de informar ao tomador de decisões. A informação, por sua vez, apresenta elementos que podem transmitidos ou interpretados para fins de tomada de decisões (BRASIL, 1988b)⁵¹.

Justamente por ser a informação a depuração do conteúdo dos dados, obtida com base em seleção prévia, organização racional e estrutural realizadas com específica abordagem e finalidade (PARENTONI, 2015, p. 550), ou seja, decorrente do tratamento de dados, é sobre ela que recai a proteção jurídica da privacidade (DONEDA, 2011, p. 94) e da proteção de dados (SIMÃO FILHO; SCHWARTZ, 2020, p. 220).

Como a LGPD apenas protege o tratamento de dados pessoais, não abrangendo os dados anonimizados⁵² porque, a princípio, não têm o condão de prejudicar sujeitos individualizados (PARENTONI, 2015, p. 551), distingui-os a seguir.

3.2.1 Dados pessoais

Os dados pessoais são registros individualizados ou individualizáveis que se relacionam à pessoa natural (BRASIL, 2018b), podendo abranger o nome, o endereço, a profissão e outros atributos que podem conduzir à identificação do indivíduo de forma precisa (PARENTONI, 2015, p. 551).

⁵⁰ Decreto n. 97.057/1988, art. 6º: “Para os efeitos deste Regulamento Geral, dos Regulamentos Específicos e das Normas complementares, os termos adiante enumerados têm os significados que se seguem: [...] 23º) Dado – informação sistematizada, codificada eletronicamente, especialmente destinada a processamento por computador e demais máquinas de tratamento racional e automático da informação” (BRASIL, 1988b).

⁵¹ Decreto n. 97.057/1988, art. 6º: [...] 43º) “Informação – elemento de conhecimento passível de interpretação” (BRASIL, 1988b).

⁵² Lei n. 13.709 de 2018, art. 12: “Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.” (BRASIL, 2018b)

A identificação do sujeito pode ocorrer, dentre outras possibilidades, por meio da apresentação do documento oficial, como o passaporte, o documento de identidade ou a carteira profissional, além de nome de usuário (*nickname*) em uma rede social. Para exemplificar essa última forma, tome-se o jogador brasileiro Edson Arantes do Nascimento, que, sendo identificado pela alcunha de Pelé, aparece em sua rede social no X (antigo Twitter) como “@Pele”, sendo possível sua identificação. Por outro lado, a placa do carro que ele utiliza, o número de seu cartão de crédito, o IP do seu computador, são dados que, sozinhos, não identificam sua pessoa, mas quando conjugados com outros registros, o tornam identificável.

Assim, admite-se que o termo “identificável” se relaciona a características que podem conduzir à individualização em potencial da pessoa (GOYANNA, 2021, p. 17) titular do direito de ter controle sobre seus dados pessoais, tendo em vista que são extensão de sua personalidade (BIONI, 2019).

Em decorrência da utilização de informações intrínsecas aos indivíduos em contextos sociais diversos (DONEDA; MENDES, 2014; DONEDA, 2020a, p. 144), criou-se a espécie de dados pessoais classificada como dados sensíveis (PARENTONI, 2015, p. 551), podendo abranger registros envolvendo a raça, a crença religiosa ou política, a opção sexual, dados genéticos, biométricos, históricos médicos, dentre outros relacionados à pessoa (BRASIL, 2018b)⁵³.

Os dados pessoais sensíveis referem-se aos principais aspectos da personalidade ou do comportamento do indivíduo (PARENTONI, 2015, p. 551) e, por isso, seu tratamento exige regras mais rígidas, pois traços da personalidade ali revelados podem ser utilizados para fins discriminatórios ou prejudiciais ao seu titular (DONEDA, 2020a, p. 144).

Antes da publicação da LGPD, os dados relativos aos números que descrevem a atividade financeira de um sujeito como o faturamento, o valor de mercado, a margem de lucro, adiante denominados como dados financeiros, já eram protegidos pela Lei Complementar n. 105/2001 (BRASIL, 2001) e pela Resolução CMN n. 4.658/2018, atualmente revogada e substituída pela Resolução CMN n. 4.893/2021 (CMN, 2021), que dispõe sobre a política de segurança cibernética, armazenamento e processamento

⁵³ Lei n. 13.709 de 2018, art. 5º: “Para os fins desta Lei, considera-se: [...] II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;” (BRASIL, 2018b)

de dados e computação na nuvem. De acordo com esse regime jurídico, sem violar o dever de sigilo, as instituições financeiras possuem a prerrogativa legal de fornecer tais dados para a formação do histórico de crédito do cliente do mercado financeiro (BRASIL, 2001)⁵⁴.

Ao serem tratados e analisados, por exemplo, os dados financeiros extraídos das demonstrações contábeis de um empresário tornam-se *informações financeiras* relevantes para a tomada de decisão de credores e investidores, pois espelham a situação econômico-financeira do seu titular (DINIZ, 2015, p. 39-40). Os vulgarmente conhecidos como “dados transacionais”⁵⁵ também se tornam “informações financeiras” relevantes (BCB, 2023b) – por exemplo, referentes aos históricos de investimento, de pagamento e de transferências realizadas pelo cliente do mercado financeiro (ZAGO, 2023).

Apesar de a LGPD não especificar em que categoria se enquadram os dados financeiros, admite-se, neste trabalho, que eles são dados pessoais que não devem ser qualificados como sensíveis (LUPIN, 2020, p. 10), pois abarcam informações relativas à pessoa natural identificada ou identificável sem envolver aspectos relacionados à sua personalidade ou a comportamentos ligados à sua pessoa.

No que se refere a dados cadastrais registrados em formato físico ou eletrônico – art. 2º, IV, da Resolução CVM n. 50/2021⁵⁶ (CVM, 2021) – como o nome do titular, o número da agência e da conta corrente ou da conta de pagamento e, futuramente, o número do token Drex –, embora possam ser qualificados como dados pessoais por serem necessários à identificação da pessoa do cliente do mercado financeiro, não são protegidos pelo sigilo bancário, eis que permitida a sua troca entre as instituições que profissionalmente prestam serviços relativos à movimentação de recursos financeiros

⁵⁴ Lei Complementar n. 105/2001, art. 1º: “As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. [...] § 3º Não constitui violação do dever de sigilo: [...] VII – o fornecimento de dados financeiros e de pagamentos, relativos a operações de crédito e obrigações de pagamento adimplidas ou em andamento de pessoas naturais ou jurídicas, a gestores de bancos de dados, para formação de histórico de crédito, nos termos de lei específica” (BRASIL, 2001).

⁵⁵ A expressão “dados transacionais” é utilizada entre aspas pois, mesmo que sua utilização é frequente pelo Banco Central do Brasil como sinônimo de dados provenientes de atividades de pagamento ou transferência de valores, entende-se nesse trabalho, inadequada sua utilização. Isso porque “transação” é negócio jurídico no qual os interessados podem terminar um litígio mediante concessões mútuas (art. 840 do Código Civil) (BRASIL, 2002)

⁵⁶ “Art. 2º Para fins da presente Resolução, considera-se: [...] IV – cadastro: registro, em meio físico ou eletrônico, das informações e dos documentos de identificação de clientes com os quais a instituição mantém relacionamento direto em função da prestação de serviços no mercado de valores mobiliários;” (CVM, 2021)

(BRASIL, 2001)⁵⁷. Tanto é que a jurisprudência nacional possui entendimento consolidado de que os dados cadastrais dos correntistas não representam, por si sós, dados que devem ser protegidos pelo sigilo bancário, isto é, não possuem garantia de inviolabilidade e de não serem objeto de comunicação (BRASIL, STF, 2006; BRASIL, STF, 2012; BRASIL, STF, 2018).

3.2.2 Dados anonimizados e pseudoanonimizados

Os dados anonimizados⁵⁸ são, por exclusão, todos aqueles que não levam à identificação do sujeito, isto é, não representam um dado pessoal (PARENTONI, 2015, p. 551), considerando os meios técnicos razoáveis e disponíveis na ocasião do seu tratamento (BRASIL, 2018)⁵⁹. Os dados anonimizados não são considerados dados pessoais para fins de aplicação da LGPD, salvo quando houver a reversão das informações (BRASIL, 2018)⁶⁰.

Já os dados pseudoanonimizados são aqueles que perderam a possibilidade de associação ao seu titular, seja de maneira direta seja indireta⁶¹, mas que podem ser novamente transformados em dados pessoais, identificando a pessoa de seu titular,

⁵⁷ Lei Complementar n. 105/2001, art. 1º “As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. [...] § 3º Não constitui violação do dever de sigilo: I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;” (BRASIL, 2001)

⁵⁸ Destaque-se que dado anônimo não é a mesma coisa que dado anonimizado. O dado anonimizado passou por técnicas de criptografia, mas seu titular pode vir a ser conhecido, caso utilizadas técnicas de reidentificação. Já o dado anônimo perde essa possibilidade, isso é, é um dado incapaz de revelar a identidade de uma pessoa (BIONI, 2020). Além disso, anonimização não se confunde com anonimato. Aquela consiste no procedimento técnico que retira o vínculo existente entre o dado e o seu titular, ao passo que o anonimato se refere aos esforços de não revelar a identidade do sujeito (OLIVER; LOPES, 2021, p. 161).

⁵⁹ Lei n. 13.709/2018, art. 5º: Para os fins desta Lei, considera-se: [...] III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;” (BRASIL, 2018)

⁶⁰ Lei n. 13.709/2018, art. 12: “Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.” (BRASIL, 2018)

⁶¹ Encontra-se na literatura crítica sobre tal conceito, sendo afirmado que se trata de forma “assistemática” de caracterização do instituto da pseudoanonimização (BIONI, 2020, p. 194). Isso porque essa palavra aparece expressamente na LGPD apenas duas vezes, no *caput* e no parágrafo quarto do art. 13, no contexto do tratamento de dados para saúde. Tal posicionamento enfatiza que o conteúdo da pseudoanonimização está contido na expressão “sempre que possível” em diversos momentos da lei. Por ora, a autora opta por não aprofundar a discussão dessa temática, por razões de pertinência ao objeto central desse estudo, tendo em vista que a pseudoanonimização é técnica comumente utilizada em prol da privacidade, seja na área da saúde ou nas diversas outras.

tendo em vista que o controlador mantém em ambiente controlado e seguro as informações adicionais que permitirão essa reversão (BRASIL, 2018)⁶². Como exemplo, cita-se o caso de pagamento ou de transferência em que o CPF do cliente é omitido com asteriscos (*). Nesse tipo de situação, a instituição que tratou o dado pode reverter a pseudoanonimização, eis que desde o início quando a pessoa fez seu cadastro teve acesso ao CPF do cliente que o informara.

3.3 Tratamento de dados pessoais: conceito, bases legais, princípios e diretrizes

O tratamento de dados pessoais é a atividade de processamento de registros, utilizando-se de métodos estatísticos, algoritmos ou de técnicas de inteligência artificial (DONEDA, 2020a, p. 149) para realizar a coleta, a classificação, a utilização, o acesso, a reprodução, a transmissão, a eliminação, dentre outros procedimentos elencados no inciso X do art. 5º da LGPD (BRASIL, 2018)⁶³. No Brasil ele pode ser realizado nas hipóteses autorizadas nos dez incisos do art. 7º da LGPD (BRASIL, 2018), que não apresentam ordem de hierarquia entre eles (PARANTONI, 2021, p. 28), ou seja, quando:

- a) houver consentimento do titular;
- b) for para cumprir dever decorrente de previsão legal ou de norma regulatória endereçada ao controlador dos dados;
- c) destinar-se à execução de políticas públicas;
- d) voltar-se para a realização de estudos por órgão de pesquisa;
- e) relacionar-se à execução de contrato ou à prática de procedimento preliminar relacionada a contrato celebrado;

⁶² Lei n. 13.709/2018, art. 13: “Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. [...] § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.” (BRASIL, 2018).

⁶³ Lei n. 13.709/2018, art. 5º “[...] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;” [...] (BRASIL, 2018).

- f) decorrer do exercício regular de direitos em processo judicial, administrativo ou arbitral;
- g) for para proteger a vida ou a incolumidade física do titular ou de terceiros;
- h) endereçar-se à tutela da saúde, exclusivamente conduzida por profissionais de saúde, prestadores de serviços de saúde ou autoridade sanitária;
- i) for para atender a interesses legítimos do controlador dos dados ou de terceiros;
- j) voltar-se à proteção do crédito.

Em reflexão sobre os possíveis relacionamentos que poderão ser estabelecidos pelo usuário do Drex com os participantes da estrutura desenhada pelo BCB para a CBDC brasileira, concluiu-se pela perspectiva de aplicação em seu contexto das seguintes hipóteses de autorizações para as instituições financeiras e de pagamento tratarem dados do cliente de moeda digital tokenizada: consentimento, cumprimento de dever normativo, realização de estudos, execução de contrato, atendimento de legítimos interesses ou proteção do crédito.

O consentimento é a manifestação da vontade do titular fornecida de forma livre e inequívoca, no qual ele expressa sua concordância com o tratamento de seus dados pessoais para uma finalidade determinada (DONEDA, 2020a, p. 13). Trata-se de importante autorização para tratamento de dados existentes nos mais diversos setores sociais, isto é, em sistemas utilizados por instituições financeiras ou de pagamentos, nas redes sociais, em sites comerciais ou de busca e em outros locais nos quais estejam disponibilizados produtos e serviços, digitais ou analógicos (RICHARDS; HARTZOG, 2019, p. 1.463).

Apesar da sua relevância, o vocábulo “consentimento” se tornou simples *pop up*⁶⁴ que aparece para o usuário solicitando que ele concorde com os termos de privacidade, e política de *cookies*⁶⁵ e outras práticas comerciais, cujo conteúdo desses termos não são, nem mesmo lidos (BROWN, 2001; NORBERG; HORNE; HORNE, 2007; KOKOLARIS, 2015). Trata-se do paradoxo da privacidade (*privacy paradox*), pois, embora a LGPD exija que o consentimento seja fornecido de maneira livre e inequívoca, em que o usuário tenha ciência dos dados que serão tratados e das

⁶⁴ *Pop up* é um recurso de publicidade simbolizado por uma pequena tela que se abre dentro do navegador quando determinada página é acessada. Ela pode ser usada para dar informações, chamar a atenção, fazer anúncios de publicidade, dentre outros (SIGNIFICADO..., 2024).

⁶⁵ As políticas de *cookies* são formas de coleta de dados durante a navegação do usuário em uma plataforma (POLITICA DE COOKIES..., 2021).

finalidades determinadas para aquele tratamento, na prática, observa-se reiterado comportamento em que o usuário está disposto a seguir cedendo seus dados pessoais em troca de continuar com a utilização do serviço ofertado, aceitando os termos de uso e políticas de privacidade, sem efetivamente apor seu consentimento esclarecido (KOKOLARIS, 2015; DONEDA, 2020, p. 12).

A autorização legal para o tratamento de dados em virtude do cumprimento de dever previsto em norma legal ou regulatória endereçada ao seu controlador, seja instituição privada, seja pública, conforme incisos II e III do art. 7º da LGPD⁶⁶, permite que a instituição financeira ou de pagamento realize tratamento de dados de seu cliente, por exemplo. Isso pode se dar em razão do cumprimento de ordem judicial ou em decorrência do Sistema de Informações do Banco Central do Brasil (Sisbacen), formado por sistemas e recursos de tecnologia da informação endereçados à constante coleta de informações que formam base de dados suscetíveis a serem consultadas por órgãos e entidades do Poder Público, observados os preceitos de sigilo que legalmente envolvem essas informações (BCB, 2024).

A realização de tratamento em prol de estudos por órgão de pesquisa se mostra recorrente no mercado financeiro. Como exemplo, tem-se a 31ª edição da Pesquisa Febraban de Tecnologia Bancária 2023, realizada pela Deloitte que apontou que 66% (sessenta e seis por cento) das transferências e pagamentos realizados por correntistas de dezoito bancos participantes, representando no total 86% (oitenta e seis por cento) dos dados bancários ativos no Brasil, eram realizados por meio do telefone celular – *mobile banking* (LGPD, 2023, p. 7). Outro exemplo, diz respeito à pesquisa realizada em 2023 pela TechBan⁶⁷, em parceria com o Datafolha, de forma online e com abrangência nacional, do qual participaram 1.519 (mil, quinhentas e dezenove) pessoas. Com base nesse estudo, apenas 18% (dezoito por cento) dos brasileiros sabem o que é Drex (PESQUISA..., 2023). Pode-se inferir de tal informação sobre a necessidade de educação da população sobre os impactos do Real Digital. Em relação a essa hipótese de autorização de tratamento de dados, cabe dizer que, conforme o disposto na LGPD,

⁶⁶ Lei n. 13.709/2018, art. 7º “[...] II – para o cumprimento de obrigação legal ou regulatória pelo controlador; III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas [...]em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; [...]” (BRASIL, 2018).

⁶⁷ Administradora dos caixas eletrônicos mantidos pelo sistema Banco24Horas.

deve-se garantir, sempre que possível, a anonimização dos dados pessoais (BRASIL, 2018)⁶⁸.

Possivelmente, as hipóteses de autorizações para tratamento de dados na estrutura do Drex que mais serão utilizadas referem-se à execução de contrato, de procedimentos preliminares relacionados ao contrato – art. 7º, inciso V – ou para conferir algum tipo de proteção do crédito – art. 7º, inciso X (BRASIL, 2018).

No caso da autorização de tratamento de dados para atender a legítimo interesse do controlador ou de terceiros – art. 7º, IX (BRASIL, 2018) –, cabe dizer que, apesar da indeterminação do que venha a ser o sentido do termo “legítimo”, sabe-se o tratamento realizado com base nesse tipo de permissão deve ser feito com observância dos princípios da boa-fé e da responsabilização (*accountability*) do controlador (PARENTONI, 2021 p. 4-6; BRASIL, 2018).

Além da boa-fé, a LGPD enumera um rol de princípios que devem ser observados durante a atividade de tratamento de dados (art. 6º I a X, BRASIL, 2018): finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Conforme a doutrina de Doneda (2020b), tais princípios trazidos pela LGPD podem ser organizados em grupos temáticos, consistindo em espécie de diretrizes para quem vai tratar dados ou quem vai fiscalizar o cumprimento das imposições normativas previstas no ordenamento jurídico brasileiro quanto a tal atividade: finalidade, exatidão, livre acesso, publicidade, segurança física e tecnológica.

Prevista no inciso I do art. 6º da LGPD (BRASIL, 2018) o princípio/diretriz da finalidade⁶⁹ pode ser entendido como o dever de obedecer ao conteúdo do termo de consentimento assinado pelo interessado, seja em formato digital ou eletrônico, sabendo-se que não é possível a realização de tratamento posterior que não diga respeito às finalidades autorizadas (DONEDA, 2020a, p. 171) – por exemplo, a avaliação

⁶⁸ Lei n. 13.709/2018, art. 7º: “O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IV – para a realização de estudos por órgão de pesquisa, garantida, **sempre que possível, a anonimização dos dados pessoais**; [...] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: [...] c) realização de estudos por órgão de pesquisa, garantida, **sempre que possível, a anonimização dos dados pessoais sensíveis**; [...] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: [...] II – estudo por órgão de pesquisa, garantida, **sempre que possível, a anonimização dos dados pessoais**; [...] (BRASIL, 2018, grifos nossos)

⁶⁹ Lei n. 13.709/2018, art. 6º: “[...] I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; [...]” (BRASIL, 2018).

socioeconômica de determinado banco para conceder empréstimo ou aumento do limite de cartão de crédito demanda o tratamento de dados cadastrais, histórico de adimplemento de dívidas, dentre outros. Nesse contexto, não está autorizado o tratamento de dados relativos à crença religiosa e filiação partidária, pois fogem, a princípio, à finalidade do tratamento autorizado, qual seja, analisar o risco de inadimplemento.

De acordo com o inciso I, do art. 15 da LGPD (BRASIL, 2018)⁷⁰, é crucial para que seja marcado o término do prazo para tratamento de dados conforme a finalidade para a qual foi autorizado tenha sido alcançada e os dados não são mais pertinentes ou necessários. Assim, em observância ao princípio da necessidade, o tratamento deve ser realizado utilizando-se o *mínimo* de dados necessários relacionados às finalidades para as quais a autorização foi conferida (BRASIL, 2018)⁷¹.

A diretriz correspondente à exatidão relaciona-se diretamente com os princípios da adequação e da não discriminação, respectivamente, previstos nos incisos II⁷² e IX⁷³ do art. 6º da LGPD (BRASIL, 2018), segundo os quais os dados devem ser armazenados de forma fidedigna à realidade (DONEDA, 2020a, p. 171) e, caso isso não seja respeitado, as decisões automatizadas podem ser objeto de revisão, conforme determina o art. 20 da LGPD (BRASIL, 2018)⁷⁴.

A instituição bancária, por exemplo, que traça o perfil de consumo do usuário, como investidor de risco ou conservador, levando em conta rápido “quiz” contendo perguntas e respostas diretas, que não oferecem margem para análise de suas pretéritas aquisições de títulos e valores mobiliários, está traçando perfil com base em exame superficial, o que pode conduzir a algoritmos de predição⁷⁵ e, eventualmente, gerar

⁷⁰ Lei n. 13.709/2018, art. 15: “O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; [...]” (BRASIL, 2018).

⁷¹ Lei n. 13.709/2018, art. 6º “[...] III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; [...]” (BRASIL, 2018).

⁷² Lei n. 13.709/2018, art. 6º: “[...] II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; [...]” (BRASIL, 2018).

⁷³ Lei n. 13.709/2018, art. 6º: “[...] IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; [...]” (BRASIL, 2018).

⁷⁴ Lei n. 13.709/2018, art. 20: “O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade” (BRASIL, 2018).

⁷⁵ Importante diferenciar que algoritmos de predição podem ou não gerar discriminação. No contexto do aprendizado de máquinas (*machine learning*), existem vários tipos ou formas de fornecer dados para que a máquina possa extrair deles padrões, o que consiste na atividade de mineração de dados (*data*

discriminação⁷⁶. Dessa forma, o tratamento deve ser feito com cuidado, sobretudo, permitindo correções e atualizações periódicas na hipótese de tratamento automatizado, como no caso exemplificado.

O livre acesso possui correlata correspondência com o inciso IV do art. 6º da LGPD (BRASIL, 2018)⁷⁷, em que o usuário deve ter o direito de acessar de maneira facilitada e gratuita informações sobre a forma e duração do tratamento de seus dados, bem como a integralidade de seus dados pessoais. A observância dessa diretriz e do princípio em que se baseia pode influenciar na efetividade de proteção de outros direitos – por exemplo, o direito ter corrigidos dados incorretos advindos do tratamento automatizado descrito no art. 20 da LGPD (DONEDA, 2020a, p. 171).

Tal diretriz também encontra respaldo no princípio que determina a observância de tratamento dos dados com qualidade. Assim, deve ser garantido ao titular de dados a exatidão, a clareza, a relevância e a atualização dos dados, sempre em acordo com a necessidade e a finalidade estabelecidas na autorização para seu tratamento – art. 6º, V, da LGPD (BRASIL, 2018).

A diretriz correspondente à publicidade se refere ao inciso VI do art. 6º da LGPD⁷⁸, ou seja, ao princípio da transparência, segundo o qual deve ser garantido ao usuário informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. A diretriz e o respectivo princípio que a sustentam endereçam comando ao usuário, que deve ter ciência a respeito da existência de banco de dados e que seus dados pessoais estão nele inseridos (DONEDA, 2020a, p. 171). Trata-se de comando alinhado ao princípio geral da administração

mining). A análise preditiva é, via de consequência, a descoberta de padrões no histórico de dados para prever resultados futuros (SAIAS *et al.*, 2018, p. 3).

⁷⁶ Santos (2006), em pesquisa para o Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Minas Gerais, aplicou modelo preditivo de mineração de dados para apoio à decisão de crédito, classificando pessoas como boas pagadoras ou más pagadoras e o risco que elas apresentam para instituições financeiras. Na oportunidade, concluiu-se que esse tipo de análise de risco para crédito deve basear-se em dados que vão além de reduzir custos, maximizar receitas, pois existem informações chamadas pelo autor de “memória organizacional” que devem ser levadas em consideração para aumentar a quantidade de dados disponíveis para a análise (SANTOS, 2006, p. 85).

⁷⁷ Lei n. 13.709/2018, art. 6º: “[...] IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; [...]” (BRASIL, 2018).

⁷⁸ Lei n. 13.709/2018, art. 6º: “[...] VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; [...]” (BRASIL, 2018).

pública (BRASIL, 1988a)⁷⁹, que deve ser estendido para o Drex, ao exigir que o BCB apresente, tal como tem feito, de maneira transparente a agenda institucional do Drex por meio de divulgação constante de notícias sobre o assunto no site da instituição, em fóruns e plenárias.

A diretriz da segurança física e tecnológica decorre dos princípios da segurança e da prevenção contidos nos incisos VII⁸⁰ e VIII⁸¹ da LGPD, respectivamente. Trata-se de comando que tem por objetivo assegurar que, no tratamento de dados pessoais, sejam utilizadas técnicas capazes de protegê-los, daí falar-se em segurança e de prevenir a ocorrência de danos (DONEDA, 2020a, p. 171).

Tais comandos devem nortear o tratamento de dados dos usuários da CDBC brasileira, praticado com observância de técnicas de segurança e medidas administrativas aptas a proteger os dados pessoais contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O agente de tratamento deve, portanto, demonstrar a adoção de medidas eficazes em relação à observância e ao cumprimento das normas de proteção de dados pessoais – art. 6º, X, da LGPD (BRASIL, 2018). Aquele que obtiver acesso a esses dados de maneira indevida será responsabilizado pelo ocorrido – art. 31, § 2º, da Lei 12.527/2011⁸² –, devendo responder o controlador de forma solidária com o operador pelos danos patrimoniais, morais, individuais ou coletivos (BRASIL, 2018)⁸³.

3.4 Proteção da privacidade e de dados pessoais no ordenamento jurídico brasileiro

⁷⁹ CRFB/1988, art. 37: “A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: [...]” (BRASIL, 1988a).

⁸⁰ Lei n. 13.709/2018, art. 6º: “[...] VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; [...]” (BRASIL, 2018).

⁸¹ Lei n. 13.709/2018, art. 6º: “[...] VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; [...]” (BRASIL, 2018).

⁸² Lei 12.527/ 2011, art. 31: “O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. [...] § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido” (BRASIL, 2011b).

⁸³ Lei n. 13.709/2018, art. 42: “O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; [...]” (BRASIL, 2018).

A disciplina da proteção de dados pessoais, que decorre do dever de respeitar a privacidade (DONEDA, 2020a, p. 165; BRASIL, 2018⁸⁴), abarca normas constitucionais e infraconstitucionais, sendo algumas delas pautadas pela garantia da liberdade de expressão e do direito à informação (DONEDA, 2011, p. 103), conforme se apresenta a seguir.

3.4.1 No regime constitucional

Desde sua redação original, a CRFB de 1988, no inciso X do art. 5º (BRASIL, 1988a), prevê que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, para cuja violação admite-se indenização por dano material ou moral. (CARVALHO, 1998, p. 55). Assegura, também, a inviolabilidade de domicílio, nos termos do inciso XI do art. 5º (BRASIL, 1988a), segundo o qual a casa é asilo inviolável. Assim, ninguém pode nela adentrar sem o consentimento do morador, salvo em caso de flagrante delito, desastre, prestação de socorro, ou, ainda, em casos de cumprimento de determinação judicial a ser realizado durante o dia.

De modo similar, o inciso XII do art. 5º (BRASIL, 1988a) assegura sigilo aos indivíduos, garantindo proteção contra a inviolabilidade das correspondências, dos dados e das comunicações telegráficas e telefônicas, salvo em caso de ordem judicial para fins de investigação criminal ou instrução processual penal.

Outrossim, apesar de a CRFB de 1988 não fazer referência expressa à palavra “privacidade” em si, a Emenda Constitucional n. 115/2022 incluiu a proteção de dados pessoais no rol dos direitos fundamentais previstos no art. 5º⁸⁵ e passou a atribuir competência privativa à União para legislar sobre tal assunto⁸⁶ (BRASIL, 1988a).

Embora procedentes as críticas quanto à aplicação em termos práticos para o cidadão⁸⁷, faz parte da disciplina jurídica de proteção da privacidade e de dados pessoais, a previsão constitucional do *habeas data* como direito fundamental, regulamentado pela Lei n. 9.507/1997 (BRASIL, 1997), que visa assegurar ao cidadão o

⁸⁴ Lei n. 13.709/2018, art. 2º: “A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; [...]” (BRASIL, 2018).

⁸⁵ CRFB/1988, art. 5º: “[...] LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (BRASIL, 1988a).

⁸⁶ CRFB/1988, art. 22: “Compete privativamente à União legislar sobre: [...] XXX – proteção e tratamento de dados pessoais” (BRASIL, 1988a).

⁸⁷ Para manejá-lo, é necessário a recusa de fornecimento de dados por parte do administrador público, bem como a presença de advogado (DONEDA, 2011, p. 104).

conhecimento de informação relativa a seu respeito e que esteja armazenada em registro ou banco de dados de caráter público, bem como garante o direito de retificação desses dados⁸⁸.

3.4.2 Em legislações infraconstitucionais

A proteção da privacidade e dos dados pessoais no Brasil que foi reforçada pela LGPD, já era endereçada por algumas leis, como: Lei n. 8.078, de 1990 (BRASIL, 1990) – Código de Defesa do Consumidor (CDC); Lei n. 9.296/1996 (BRASIL, 1996) – Lei de Interceptação das Comunicações; Lei n. 9.472/1997 (BRASIL, 1997) – Lei de Telecomunicações; Lei Complementar n. 105/2001 (BRASIL, 2001) – Lei do Sigilo Bancário; Lei n. 12.414/2011 (BRASIL, 2011a) – Lei do Cadastro Positivo; a Lei n. 12.527/2011 (BRASIL, 2011b) – Lei de Acesso à Informação (LAI); e Lei n. 12.965/2014 (BRASIL, 2014) – Marco Civil da Internet (MCI).

O CDC prevê, no *caput* do art. 43, que o consumidor tem a prerrogativa de acessar as informações existentes em fichas, cadastros, registros e dados pessoais e de consumo arquivados sobre ele (BRASIL, 1990) em bancos de dados governamentais e privados⁸⁹ (DONEDA, 2011, p. 104), e no § 1º do art. 43 o CDC assegura ao consumidor o direito à transparência (BRASIL, 1990)⁹⁰. Cadastros e dados dos consumidores devem, assim, ser objetivos, claros, verdadeiros e apresentar linguagem de fácil compreensão, cujo prazo de armazenamento das informações negativas não pode ultrapassar cinco anos.

A Lei do Cadastro Positivo (BRASIL, 2011a), alterada pela Lei Complementar n. 166 de 2019 (BRASIL, 2019), admite a formação e a consulta de banco de dados com

⁸⁸ CRFB/1988, art. 5º: “Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] LXXII – conceder-se-á ‘habeas-data’: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; [...]” (BRASIL, 1988a).

⁸⁹ Lei n. 8.078/1990, art. 43: “O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes” (BRASIL, 1990).

⁹⁰ Lei n. 8.078/1990, art. 43: [...] § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos” (BRASIL, 1990).

informações de adimplemento para formação de histórico de crédito, tanto de pessoas físicas quanto jurídicas (FREITAS; MAFFINI, 2020, p. 35).

A Lei de Telecomunicações (BRASIL, 1997) prevê a proteção à inviolabilidade de comunicações⁹¹ admitida a sua quebra em caso de situações excepcionais.⁹² Em reforço, Lei de Interceptação das comunicações prevê como crime a realização de interceptação, seja telefônica, telemática ou informática, sem autorização judicial ou com objetivos não autorizados em lei (BRASIL, 1996).⁹³

No mercado financeiro, destaca-se a Lei Complementar n. 105 de 2001 (Lei do Sigilo Bancário), segundo a qual as instituições⁹⁴ devem conservar o sigilo de dados relativos aos serviços que prestam envolvendo recursos financeiros, como pagamentos e transferências de valores, sendo excepcionalmente autorizada a quebra desse sigilo, nos casos previstos em lei ⁹⁵(BRASIL, 2001).

Há divergências a respeito da natureza jurídica do sigilo. Para uma corrente (BARBEITAS, 2003, p. 43), com fundamento nos incisos X, XII e LX do art. 5º da CRFB/1988, trata-se de direito fundamental. Conforme outra abordagem (SAMPAIO, 1992, p. 443), o sigilo enquadra-se como um direito, como qualquer outro, que possui regramento próprio contido na Lei Complementar n. 105/2001 (BRASIL, 2001).

⁹¹ Lei n. 9.472/1997, art. 3º “O usuário de serviços de telecomunicações tem direito: [...] V – à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucionais e legalmente previstas; [...]” (BRASIL, 1997).

⁹² No Brasil existia, até 2014, divergência jurisprudencial para a interpretação acerca da necessidade de autorização judicial em casos de interceptação de telefones e dados armazenados no próprio celular. Isso ocorreu em razão do HC n. 91.867/PA do STF, que entendeu como legal a atuação de autoridade policial que, mesmo sem autorização judicial, acessou dados armazenados no celular do suposto autor do crime (BRASIL, STF, 2012). Tal caso ocorreu com celular analógico, isto é, que não possuía acesso à internet. Outrossim, na tentativa de se atualizar, o STJ, por meio do HC n. 51.531/RO (BRASIL, STJ, 2016) destacou que o uso de celulares com acesso à internet mudou o cenário de análise casuística do HC 91.867/PA (BRASIL, STF, 2012), decidido na era analógica (BRASIL, STF, 2016). Esse julgado, elaborado na era digital e com acesso à internet, reforçou os pressupostos, expressos na lei, de tratar como ilegal o acesso a dados armazenados em celular sem autorização judicial.

⁹³ Lei n. 9.296/1996, art. 10: “Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no *caput* deste artigo com objetivo não autorizado em lei” (BRASIL, 1996).

⁹⁴ “Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados” (BRASIL, 2001).

⁹⁵ Lei Complementar n. 105/2001, art. 10: “A quebra de sigilo, fora das hipóteses autorizadas nesta Lei Complementar, constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos, e multa, aplicando-se, no que couber, o Código Penal, sem prejuízo de outras sanções cabíveis. Parágrafo único. Incorre nas mesmas penas quem omitir, retardar injustificadamente ou prestar falsamente as informações requeridas nos termos desta Lei Complementar” (BRASIL, 2001).

Para Barbeitas (2003), o sigilo é intrínseco à inviolabilidade prevista no inciso XII do no art. 5º da CRFB (BRASIL, 1988a), em que é “inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas”. Desse modo, por integrar a inviolabilidade da própria intimidade consagrada no inciso X do art. 5º da CRFB, o sigilo estaria abrangido pelo resguardo da vida privada, da honra e da imagem das pessoas (BRASIL, 1988a).

Para a segunda corrente, deve-se afastar a vinculação do sigilo das informações – em especial do sigilo bancário – como direito fundamental de privacidade porque seu conteúdo intrínseco confere uma faculdade ao seu titular, e não direito absoluto (SAMPAIO, 1992, p. 443). Conforme essa visão, o sigilo não é o bem protegido, não é o objeto do direito fundamental, mas, sim, a faculdade de agir, isto é, de manter sigilo ou de resistir ao devassamento. Tornando-se tão somente o conteúdo estrutural do direito, o sigilo bancário não constitui manifestação dos direitos da personalidade ou do direito à intimidade (MUSSI FILHO, 1991, p. 11), a menos que o conceito de personalidade e de intimidade sejam extensamente alargados, de modo que se tornem amórficos, o que não se considera o melhor caminho porque dificultaria sua proteção (PRODANOFF, 2008, p. 21).

Concorda-se com a segunda corrente, porque nem sempre que se adquire bens de consumo, mediante o pagamento ou a transferência de recursos financeiros, o indivíduo projeta sua personalidade de tal forma que se justifique a tutela do sigilo bancário como expressão da proteção constitucional do resguardo à intimidade e à vida privada. Mesmo que assim fosse, teriam de ser sopesados outros interesses atinentes à vida em comunidade (PRODANOFF, 2008, p. 22).

Apesar de o sigilo bancário não ser direito fundamental e não ser direito absoluto, entende-se, no entanto, que as ordens dadas pelo Poder Judiciário de disponibilização de informações devem ser cumpridas com a verificação e observância de seu caráter sigiloso, permitindo acesso restrito às partes da lide, conforme Lei do Sigilo Bancário⁹⁶ (BRASIL, 2001). Embora a norma mencione somente as partes, também deve ser estendida aos seus procuradores para que o princípio da ampla defesa, que inclui a defesa técnica, seja preservado (BALTAZAR JR., 2005, p. 106). Ademais,

⁹⁶ Lei Complementar n. 105/2001, art. 3º: “Serão prestadas pelo Banco Central do Brasil, pela Comissão de Valores Mobiliários e pelas instituições financeiras as informações ordenadas pelo Poder Judiciário, preservado o seu caráter sigiloso mediante acesso restrito às partes, que delas não poderão servir-se para fins estranhos à lide” (BRASIL, 2001).

a lei somente poderia restringir a publicidade dos atos processuais nos casos de defesa da intimidade ou interesse nacional, conforme inciso LX do art. 5º da CRFB (BRASIL, 1988a)⁹⁷.

Apesar de a Lei Complementar n. 105/2001 (BRASIL, 2001) não proibir a instituição financeira de informar ao seu cliente de que seu sigilo bancário foi quebrado (BALTAZAR JR., 2005, p. 110)⁹⁸, o inciso II do art. 11⁹⁹ da Lei da Lavagem de Dinheiro a impõe o dever de abstenção de realizar comunicação sobre o assunto.

Tal imposição parece colidir com o que estabelece o art. 48, da LGPD que prevê o dever de o controlador comunicar incidente capaz de violar a proteção de dados pessoais¹⁰⁰ à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados (BRASIL, 2018). Prevalece, contudo, a previsão da legislação especial por se considerar a complexidade do assunto e, principalmente, as consequências jurídicas de sua divulgação para o andamento do processo ou da investigação em casos, por exemplo, envolvendo crime de lavagem de dinheiro, nos quais investigação controlada em que se monitora as movimentações financeiras (BRASIL, 1998)¹⁰¹, e nas quais, a manutenção do sigilo é crucial para a preservação da prova, evitando eventuais adulterações (BALTAZAR JR., 2005, p. 110).

A LAI (BRASIL, 2011b) protege dados pessoais, estabelecendo importantes marcos para o acesso a informações disponíveis nos bancos de dados administrados pelo poder público. Ela surge no contexto de valorização da transparência nas diversas relações jurídicas perpetradas na administração pública direta ou indireta e no seio

⁹⁷ CRFB/1988, art. 5º: “[...] LX – a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem” (BRASIL, 1988a).

⁹⁸ Lei Complementar n. 105/2001, art. 1º: “As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. [...] § 3º Não constitui violação do dever de sigilo: [...]” (BRASIL, 2001).

⁹⁹ Lei n. 9.613/1998, art. 11: “As pessoas referidas no art. 9º: [...] II – deverão comunicar ao Coaf, abstenendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização: [...]” (BRASIL, 1998).

¹⁰⁰ Lei n. 13.709/2018, art. 48: “O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares” (BRASIL, 2018).

¹⁰¹ A ação controlada é técnica especial de investigação criminal, utilizada como meio de obtenção de prova para o inquérito policial e processo penal. Nela, a ação criminosa é mantida sob a vigilância policial para tornar mais efetiva e oportuna a ação policial (VILARES, 2014, p. 33). Sua inclusão na Lei n. 9.613 de 1998 (BRASIL, 1998) se deu por meio do “Pacote anticrime” – Lei n. 13.964/2019 (BRASIL, 2019). Texto na íntegra: “Art. 1º “Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. § 6º Para a apuração do crime de que trata este artigo, admite-se a utilização da ação controlada e da infiltração de agentes. (Incluído pela Lei n. 13.964, de 2019)” (BRASIL, 1998).

privado (BRASIL, 1988a)¹⁰². A título de exemplo, nela está previsto que o Estado tem o dever de controlar o acesso a divulgação das informações sigilosas que são produzidas nos seus órgãos e entidades, sendo certo que o acesso é restrito a pessoas devidamente credenciadas e que tenham a “necessidade” de conhecer tais informações (BRASIL, 2011b)¹⁰³.

O MCI (BRASIL, 2014), por sua vez, ao instituir os princípios, as garantias, os direitos e os deveres que devem ser observados no uso da internet no Brasil, conceitua dados em transmissão¹⁰⁴ e os armazenados¹⁰⁵, e prevê a inviolabilidade e sigilo das comunicações privadas realizadas via internet, isto é, que estão sendo transmitidas, compartilhadas e armazenadas. O MCI já tratava da necessidade de consentimento expresso e informado como necessário para o tratamento de dados pessoais, antes mesmo da publicação da LGPD (BRASIL, 2014)¹⁰⁶. Ademais, o Marco Civil da Internet também delimita prazo para que os registros de conexão sejam mantidos sob sigilo, isto é, por um ano,¹⁰⁷ bem como a guarda de registros de acesso pelo prazo de seis meses¹⁰⁸ (BRASIL, 2014), sendo expresso que, a parte que desejar ter acesso a tais registros de conexão e acesso à aplicação poderá pleiteá-los judicialmente.

¹⁰² CRFB/1988, art. 5º: “[...] XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; [...]” (BRASIL, 1988a).

¹⁰³ Lei n. 12.527/2011, art. 25: “É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção. § 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei. § 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo” (BRASIL, 2011b).

¹⁰⁴ Lei n. 12.965/2014, art. 7º: “O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; [...]” (BRASIL, 2014).

¹⁰⁵ “Art. 7º [...] III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]” (BRASIL, 2014).

¹⁰⁶ Lei n. 12.965/2014, art. 7º: “[...] IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; [...]” (BRASIL, 2014).

¹⁰⁷ Lei n. 12.965/2014, art. 13: “Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento” (BRASIL, 2014).

¹⁰⁸ Lei n. 12.965/2014, art. 15: “O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento” (BRASIL, 2014).

Com eixos de correspondência com o Regulamento Geral Europeu para a Proteção de Dados – *General Data Protection Regulation* (GDPR)¹⁰⁹, desde o anteprojeto de 2010¹¹⁰ até sua aprovação em 2018, a vigência da LGPD passou por sucessivas prorrogações, mas somente entrou em vigor em 2020 (BRASIL, 2018), tornando-se o principal texto legislativo da disciplina da proteção da privacidade e dos dados pessoais.

A LGPD traz detalhes sobre o tratamento de dados por pessoas físicas e jurídicas, públicas ou privadas, realizado tanto no meio físico quanto digital, e o faz sob os seguintes fundamentos¹¹¹: respeito à privacidade; observância da autodeterminação informativa; respeito à liberdade de expressão, de comunicação, de informação e de opinião; a inviolabilidade da intimidade, honra e da imagem; a promoção do desenvolvimento econômico e tecnológico e da inovação; garantia da livre iniciativa, livre concorrência e da defesa do consumidor; respeito aos direitos humanos, ao livre desenvolvimento da personalidade, dignidade e ao exercício da cidadania pelas pessoas naturais¹¹² (BRASIL, 2018).

Entendido o desenho adotado pelo BCB na estruturação do Drex e o regime jurídico brasileiro de proteção da privacidade e dos dados pessoais dos cidadãos, passa-se à análise conjunta desses conhecimentos para avaliar em que medida o modelo adotado pelo Estado brasileiro consegue ou não assegurar a privacidade e a proteção dos dados da pessoal natural do cliente da CBDC brasileira.

¹⁰⁹ A GDPR é apontada como o padrão internacional de legislação sobre a temática e, no Brasil, não foi diferente. Muitos direitos elencados na LGPD são inspirados no regulamento europeu – por exemplo, o consentimento – expressando algumas diferenças, especialmente no que concerne à aplicação de multas. (PARENTONI; LIMA, 2019, p. 502-507).

¹¹⁰ O Projeto de Lei n. 4.060 de 2012 (BRASIL, 2012) teve poucos avanços até a consulta pública de 2015, promovida pelo Ministério da Justiça. Todavia, aponta-se que fatores externos foram determinantes para a aprovação da Lei, como os escândalos envolvendo o tratamento ilícito de dados pessoais dos usuários do Facebook e *Cambridge Analytica* (PARENTONI; LIMA, 2019, p. 489).

¹¹¹ Lei n. 13.709/2018, art. 3º: “Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I – a operação de tratamento seja realizada no território nacional; II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (Redação dada pela Lei n. 13.853, de 2019) III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei” (BRASIL, 2018).

¹¹² Cf. art. 2º da Lei n. 13.709/2018 (BRASIL, 2018).

4 ASPECTOS E RISCOS QUE DEVEM SER CONSIDERADOS NA FORMULAÇÃO DE NORMAS VOLTADAS À REGULAÇÃO DO DREX: A MOEDA DIGITAL BRASILEIRA

A avaliação do nível de proteção da privacidade e dos dados pessoais do usuário do Drex foi feita com base no material levantado entre março de 2023 e fevereiro de 2024, sendo analisados, principalmente, os seguintes:

a) Normas editadas pelo BCB sobre o assunto. Para localizá-las, foram utilizadas as palavras-chave “real digital” e “CBDC” no período de 1º de janeiro de 2020 a 2 de março de 2024, tendo sido encontrados três resoluções e os respectivos votos levados à deliberação da Diretoria Colegiada do BCB para dar origem à sua edição (MAIA, 2023, p. 42-43). Assim, analisou-se **a.1)** a Resolução BCB n. 185/2022 (BCB, 2022b), que instituiu o Comitê Executivo do Lift Challenge Real Digital, e o Voto BCB n. 32/2022 (BCB, 2022); **a.2)** Resolução BCB n. 273/2022 (BCB, 2023a), que constituiu o grupo de trabalho “GTI Tokenização”, e o Voto do Comitê de Governança, Riscos e Controles (GRC), Voto BCB n. 68/2022 (BCB, 2022c); **a.3)** a Resolução BCB n. 315/2023 (BCB, 2023b), que instituiu o Comitê executivo de Gestão do Projeto-Piloto Real Digital (RD) e aprovou o regulamento do Piloto RD e o Voto BCB n. 73/2023 (BCB, 2023d)¹¹³.

b) Voto BCB n. 31/2023. Na página criada pelo BCB para divulgação de informações sobre o Drex (BCB, 2023c), no ícone Piloto Drex, aparece item “regulamentação”, no qual, foi possível localizar o Voto BCB n. 31/2023 (BRASIL, 2023c), que atualizou as diretrizes do Real Digital para dar início ao desenvolvimento do projeto-piloto e que autorizou a abertura de canal de comunicação de informações sobre o tema para a população;

c) Relatório Integrado do Banco Central (RIg) de 2022 (BCB, 2022a). Na página inicial do BCB, em publicações e pesquisa, na sequência de ícones “mais publicações” e “outros relatórios do BC”, localizou-se o Relatório Integrado do Banco Central (RIg) de 2022 (BCB, 2022a), que apresentou resultados da Agenda BC#, aí incluídos aqueles relacionados ao andamento do Real Digital em 2022, ano em que o BCB iniciou a avaliação de casos de uso e viabilidade tecnológica da moeda digital brasileira por meio do *Lift Challenge*;

¹¹³ Com pesquisa para o período de 1º de janeiro 2020 a 2 de março de 2024, não foram encontrados documentos com a palavra-chave “Drex” na página em que se encontra o sistema de busca de normas no sítio eletrônico do BCB (BUSCA..., 2024).

d) Resultados do *Lift Challenge* e *Lift Papers*. A busca no Google pela expressão *Lift Challenge* levou à localização do Relatório de 25 de abril de 2023 (LIFT..., 2023), em que foram apresentados os Resultados do *Lift Challenge*. Apesar de não terem sido localizadas propostas direcionadas de modo específico para tratar a proteção da privacidade e de dados pessoais na plataforma Drex, tal material levou à identificação de dois trabalhos, os chamados *Lift Papers*, especificamente voltados para debater sobre a privacidade (BUELAU; SANTOS, 2023; CRUVINEL; PRESTES, 2023); e

e) Informações disponíveis no GitHub. Com base nos vídeos produzidos pelo BCB para divulgar informações sobre o Drex, foi indicado site onde foi possível ter acesso à documentação técnica produzida e disponibilizada pelo BCB no GitHub¹¹⁴ para a participação no piloto do Real Digital (DOCUMENTAÇÃO, 2023).

Pela análise dessa documentação percebeu-se o compromisso expresso do BCB em respeitar as normas gerais e especiais de proteção à privacidade e aos dados pessoais de usuários do Drex (BRASIL, 2023a).

Todavia, não foi possível localizar a definição de que tipos de dados e informações do usuário do Drex poderão ser acessados e tratados, bem como não foi possível apurar o nível e a extensão da autorização que serão dados a tratamento dos dados que forem coletados durante a liquidação de transferências e pagamentos efetuados com o Drex.

Dependendo de como essas indefinições vierem a ser tratadas nas normas que serão instituídas pelo BCB e no aparato tecnológico por ele adotado para criar a moeda digital brasileira, pode-se estar diante do risco de ocorrência de vigilância indevida de dados, de manipulação de dados endereçada à formação de banco de dados, cujo acesso pode conferir poder abusivo a quem detiver seu controle, criando, ainda, condições para que seja praticada a perfilização de diferentes naturezas e até aquela cometida com o intuito discriminatório.

¹¹⁴ O GitHub é um repositório público que hospeda códigos-fontes, arquivos e informações de aplicações. O código fonte do Drex não foi disponibilizado, mas apenas os padrões para configuração da implantação dos nós validadores na rede do sistema Financeiro Nacional (RSFN) e da interação com os *smart contracts* (DOCUMENTAÇÃO..., 2023).

4.1 A indefinição quanto ao tipo de dados e de informações pessoais que serão tratados no Drex e à extensão da autorização para o seu tratamento e os riscos de indevida vigilância de dados e de formação de banco de informações suscetível à prática de perfilização

Apurou-se com o exame da documentação do *Kit Onboarding* produzido pelo BCB no GitHub que para a realizar transferências simuladas de Real Tokenizado durante os testes executados no Piloto do Drex devem ser utilizados dados capazes de permitir a identificação e a recuperação de carteiras contendo os *tokens* de titularidade dos clientes da nova moeda digital. Tais como: a chave de identificação do usuário¹¹⁵, o número do seu CPF¹¹⁶, o código do participante, o número da sua conta, de sua agência e de sua carteira e o CNPJ do participante envolvido com a oferta de serviços de transferências ou pagamentos com Drex (DOCUMENTAÇÃO..., 2023).

Além do acesso a esses dados cadastrais, os profissionais autorizados a atuar na plataforma Drex e seus parceiros, os terceiros prestadores de serviços de armazenamento em nuvem e os provedores de serviços de internet acessarão e poderão acessar e tratar os dados relativos aos padrões de atividades praticadas pelo usuário da moeda digital – por exemplo, saques, empréstimos, transferências e pagamentos, aos valores movimentados pelo usuário e aos seus metadados – por exemplo, a localização da pessoa quando se realiza uma transferência de valores, a data e hora em que foi praticada, o endereço de IP do remetente e do destinatário (BATISTELLA, 2020).

Claro que a realização de pagamentos ou de transferência de valores com uso do Drex dependerá da disponibilidade de determinada quantidade de dados para a correta identificação do remetente da moeda digital, do destinatário e do intermediário envolvidos com sua remessa. Ora, a liquidação de *tokens* de depósito pelos participantes do SFN e do SPB envolverá o acesso a dados e a informações, bem como o seu tratamento¹¹⁷.

¹¹⁵ A chave aqui mencionada é o identificador único, gerado pelo participante, que deve ser salvo no formato *hash* (DOCUMENTAÇÃO..., 2023).

¹¹⁶ A inscrição no Cadastro de Pessoas Físicas (CPF), a partir da entrada em vigor da Lei n. 14.534/2023 (BRASIL, 2023) será considerado como número único e suficiente para identificar o cidadão no banco de dados dos serviços públicos

¹¹⁷ No inciso X do art. 5º da LGPD, considera-se o que significa tratamento: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados (BRASIL, 2018).

Ao se analisar a Resolução BCB n. 315/2023 (BCB, 2023b) apurou-se que o inciso V do seu art. 6º diz que compete ao Comitê Executivo de Gestão (CEG) do Projeto-Piloto da Plataforma do Real Digital zelar pelo registro adequado das atividades e pela proteção dos dados que ele reunir. O inciso IV do art. 8º dessa resolução (BCB, 2023c) prevê que são atribuições dos membros do CEG zelar pela proteção de dados reunidos pelo Comitê.

Verificou-se ainda que o § 3º do art. 19 da Resolução BCB n. 315/2023 (BCB, 2023b) menciona dados referentes ao *Know-how* e a outros segredos dos negócios protegidos pelo regime jurídico da propriedade intelectual a que o CEG tiver acesso.

Mas em tal resolução não foi possível localizar regra que defina os tipos de dados e de informações pessoais que poderão ser acessados e tratados pelos participantes do processo da validação e de seus parceiros comerciais. Também não foi possível localizar regra sobre a responsabilização dos envolvidos com indevidos acesso e tratamento desse tipo de dados.

Igualmente não se localizou tal definição no Voto BCB n. 31/2023 (BCB, 2023c) nem no Voto BCB n. 73/20223 (BCB, 2023d).¹¹⁸ O subitem “vi”, do item 13 do Voto n. 31 coloca como uma das diretrizes a

observância a todos os princípios e regras de privacidade e segurança previstos na legislação brasileira, em especial na Lei Complementar n. 105, de 10 de janeiro de 2001 (sigilo bancário), e na Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) (BCB, 2023c) [...];

E o item 41 faz expressa referência que

a atuação do BCB em tal canal de comunicação será pautada pelos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, que regem a Administração Pública, e obedecerá a legislação relativa ao sigilo bancário e ao sigilo de dados, bem como os padrões éticos impostos aos servidores públicos (BCB, 2023c).

Os votos (BCB, 2023c; BCB, 2023d), no entanto, também são omissos quanto aos tipos de dados pessoais que serão acessados e tratados e como se dará a responsabilização por práticas ilícitas envolvendo esse tipo de conduta.

Considerando que, de acordo com a LGPD, toda manipulação realizada com dados pessoais é considerada tratamento de dados, é importante deixar claro quais os tipos desses dados ou informações poderão ser tratados e a extensão da autorização para

¹¹⁸ No Voto BCB n. 31/2023 foram fixadas as diretrizes do projeto piloto (BCB, 2023c), e percebendo que o projeto demandará a edição de atos administrativos diversos e coordenação entre as unidades da autarquia, foi proposto por meio do Voto BCB n. 73/2023 a criação do Comitê Executivo de Gestão (CEG) e aprovado o Regulamento do Piloto RD (BCB, 2023d).

esse tratamento no Drex, por mais que por hora estejam sendo testados usuários fictícios.

Claro que no Brasil, de acordo com as normas editadas pelo CMN e pelo BCB¹¹⁹, o acesso a dados dos clientes do SFN e do SPB é autorizado às instituições financeiras e de pagamento¹²⁰, eis que é obrigatório o registro e a manutenção do registro centralizado do cadastro de clientes dessas instituições que são titulares de contas¹²¹.

Dados já são solicitados aos clientes na abertura de contas de depósito ou de pagamentos pelas instituições financeiras e prestadoras de serviços de pagamento (FANTI; POCHER, 2020, p. 9) que são autorizadas a confrontar tais informações com bancos de dados de caráter público ou privado (BCB, 2019; NEVES; SILVA; COSTA, 2021, p. 19).¹²²

O problema é que o exercício das atividades de processamento de dados pode gerar informações sobre registros e padrões de atividades, como valores e serviços utilizados (FANTI; POCHER, 2020, p. 9) . Isso pode conduzir à indevida vigilância, à

¹¹⁹ Voto BCB n. 31/2023 Item.13: “[...] iii) emissão do Real Digital pelo BCB, como meio de pagamento, a fim de dar suporte à oferta de serviços financeiros de varejo liquidados por meio de tokens de depósitos em participantes do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB); [...]” (BCB, 2023c).

¹²⁰ Existem, para tanto, regras de funcionamento para as instituições que querem fazer parte do SFN dependendo da atividade, do risco que essa atividade pode causar e da sua atuação internacional, sendo segmentadas em S1 até S5, conforme expresso na Resolução BCB n. 4.553/2017 (BCB, 2017). A título de exemplo, o Segmento 1 (S1) é composto de bancos comerciais que tenham porte igual ou superior a 10% do Produto Interno Bruto (PIB) ou que exerçam atividade internacional relevante, independentemente do porte da instituição. Cujo texto legal é: “Art. 2º As instituições relacionadas no art. 1º devem se enquadrar em um dos seguintes segmentos: I – Segmento 1 (S1); II – Segmento 2 (S2); III – Segmento 3 (S3); IV – Segmento 4 (S4); ou V – Segmento 5 (S5). § 1º O S1 é composto pelos bancos múltiplos, bancos comerciais, bancos de investimento, bancos de câmbio e caixas econômicas que: I – tenham porte igual ou superior a 10% (dez por cento) do Produto Interno Bruto (PIB); [...]” (BRASIL, 2017).

¹²¹ Houve alteração da Lei de Lavagem de Dinheiro – Lei n. 9.613/1998 (BRASIL, 1998) – pela Lei n. 10.701/2003 (BRASIL, 2003), em que foi feita a inclusão do art. 10A, cujo texto expressa que “o Banco Central manterá registro centralizado formando o cadastro geral de correntistas e clientes de instituições financeiras, bem como de seus procuradores.” (BRASIL, 1998). Para cumprimento dessa obrigação legal foi instituído o Cadastro de Clientes do Sistema Financeiro Nacional (CCSFN), que registra a relação de instituições financeiras com as quais o cliente se relaciona, seja como titular de conta corrente, poupança ou investimentos (CADASTRO..., 2023).

¹²² Tal possibilidade está expressa no art. 2º da Resolução BCB n. 4.753/2019: “Art. 2º As instituições referidas no art. 1º, para fins da abertura de conta de depósitos, devem adotar procedimentos e controles que permitam verificar e validar a identidade e a qualificação dos titulares da conta e, quando for o caso, de seus representantes, bem como a autenticidade das informações fornecidas pelo cliente, inclusive mediante confrontação dessas informações com as disponíveis em bancos de dados de caráter público ou privado. [...] § 2º É admitida a abertura de conta de depósitos com base em processo de qualificação simplificado, desde que estabelecidos limites adequados e compatíveis de saldo e de aportes de recursos para sua movimentação” (BCB, 2019).

abusiva manipulação de banco de dados nacionais e internacionais e à indevida perfilização dos usuários do Drex.

A **vigilância de dados** (*Data surveillance*) é uma das ameaças à privacidade viabilizada por aquele que detém seu controle (WESTIN, 1967, p. 68). Na atualidade, os indivíduos são conhecidos e conhecimento é poder (WESTIN, 1967, p. 158). Ou seja, a “privacidade informacional” (TAVANI; HIMMA, 2008, p. 140) relacionada à quantidade de informações e de dados coletados, armazenados e transmitidos em alta velocidade e em larga escala, deve ser cuidadosamente controlada para evitar a vigilância governamental ou privada (WESTIN, 1967, p. 158), como também para evitar o poder decorrente da formação de **bancos de dados**, ou seja, ferramenta que possibilita sistematizar volumes de informações estruturadas de acordo com determinada lógica, cuja perspectiva utilitarista comumente admite que poderia perfeitamente ser direcionada à obtenção do maior proveito lucrativo possível dessa base (DONEDA, 2011, p. 92). Nesse sentido, as experiências humanas, durante o uso da internet, podem, por exemplo, ser tratadas por *big techs* e oferecidas como produtos para outras sociedades empresárias aumentarem seus lucros com efeitos negativos para quem é sujeito de tal prática (ZUBOFF, 2018, p. 75).

Esses dois riscos devem ser bem dimensionados na estruturação do Drex, especialmente quando forem iniciados os testes de interoperabilidade com outros sistemas tokenizados ao redor do mundo, em razão de possível manipulação indevida de banco de dados no meio internacional, que pode levar ao monitoramento global de dados pessoais dos usuários da moeda digital brasileira. Ao fomentar os pagamentos transfronteiriços e a transferência internacional de dados, que consiste na transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro¹²³ será necessário analisar os limites desse compartilhamento de dados (BRASIL, 2018)¹²⁴ bem como a extensão do tratamento, levando em consideração que

¹²³ Lei n. 13.709/2018, art. 5º: “[...] XV – transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;” (BRASIL, 2018).

¹²⁴ Lei n. 13.709/2018, art. 12: “Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. [...] § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais” (BRASIL, 2018).

eventual infração cometida nesse contexto é considerada como grave para a aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD) (ANPD, 2023b)¹²⁵.

Deve-se considerar em pagamentos transfronteiriços viabilizados pela CBDC brasileira ao redor do mundo que podem existir nações que não atendam aos requisitos de *design* para a privacidade e proteção de dados exigidos pela legislação brasileira (DARBHA; ARORA, 2020). Uma possibilidade seria o uso da diplomacia para realizar a criação de padrões internacionais para a proteção de dados trabalhados (DONEDA, 2020a, p. 228) ou a aplicação do princípio da extraterritorialidade das leis nacionais para a proteção dos dados e privacidade dos indivíduos (REIDENBERG, 2001, p. 749)¹²⁶. A LGPD já traz hipóteses expressas em que a transferência internacional de dados é permitida, dando destaque para a necessária compatibilização do grau de proteção de dados pessoais entre um país e outro (BRASIL, 2018)¹²⁷. De qualquer modo, é necessário o respeito ao consentimento específico e destacado a respeito da transferência internacional de dados (BRASIL, 2018).¹²⁸

O Drex, viabilizado por plataforma de registros de multiativos, poderá contribuir cada vez mais para o fortalecimento do Brasil no mercado regional e global, por meio do aumento da eficiência nas atividades financeiras, de pagamento ou transferências entre fronteiras (BCB, 2023)¹²⁹, mas esse movimento não deve resultar no comprometimento da estabilidade dos direitos e garantias constitucionais dos cidadãos brasileiros. Ao contrário, o Estado, representado na figura do Banco Central do Brasil, outros agentes do Sistema Financeiro Nacional e eventualmente os bancos centrais de outras nações, nos casos de pagamentos transfronteiriços – devem observar as regras atinentes à privacidade e à proteção de dados pessoais dos brasileiros (DUDENA, 2022,

¹²⁵ Lei n. 13.709/2018, art. 52: “Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]” (BRASIL, 2018).

¹²⁶ Essa vertente se apoia no princípio do *Arm's Length* muito comentado na literatura de compliance e lavagem de dinheiro. Em outro exemplo prático, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) estabeleceu padrão internacional de preços para transferências financeiras entre países membros com base nesse princípio, assim sendo, empresas multinacionais que adotam essa orientação devem respeitar padrões pré-definidos de tributação, com intuito de evitar erosão da base tributária ou transferência de lucros para jurisdições com impostos mais baixos (MOSQUERA, 2020)

¹²⁷ Lei n. 13.709/2018, Art. 33: “A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;” (BRASIL, 2018)

¹²⁸ Lei n. 13.709/2018, Art. 33: [...] “VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades;” (BRASIL, 2018)

¹²⁹ Voto BCB n. 31/2023: “9. [...] iv) favoreça a integração do Brasil aos cenários econômicos regional e global por meio do aumento da eficiência nas transações transfronteiriças.” (BCB, 2023c)

p. 44) conforme tenham acesso a diversas informações dos usuários do Drex (FANTI; POCHER, 2020, p. 7).

Como se viu no capítulo 3, o direito à privacidade supera o direito ao mero isolamento. Com isso, prevalece o entendimento em favor da tese que abandona a vertente pessoa-informação-segredo e que aceita a abordagem pessoa-informação-controle (RODOTÁ, 2020, p. 39).

Mas, é sabido o quão tênue é a linha divisória entre a regra que autoriza o dever de fiscalização do Estado e a que proíbe a **vigilância governamental**. Isso porque, tem sido afirmado que, com a implementação do Drex, o Governo poderá monitorar e rastrear todas as atividades financeiras, associando-as aos indivíduos e empresas, bem como conciliando-as aos contratos digitais da moeda digital (OS IMPACTOS..., 2022, p. 6). Também se tem dito que a moeda digital emitida pelo Banco Central permitirá o forte controle de informações financeiras e liberdade dos indivíduos semelhante a regimes totalitários (PIMENTA, 2013, p. 2).

A emissão da moeda digital brasileira se dará, todavia, em meio ao Estado Democrático de Direito altamente regulado, tendo o Estado o papel de agente normativo e regulador da atividade econômica, ao qual incumbe o dever de fiscalização, inventivo e planejamento da atividade econômica (BRASIL, 1988a)¹³⁰. Para executar tais atividades e efetivar políticas públicas, absorve informações pessoais para o aprimoramento da gestão pública (DONEDA, 2020a, p. 34; PIMENTA, 2013, p. 2).¹³¹ Tal acesso à informação, dessa forma, não deve ser reduzido à vigilância (SAMPAIO, 1992, p. 441).

Outro ponto que também precisa ser esclarecido é que nem todo banco de dados conduz à vigilância. Ora, no Brasil há a Lei n. 12.414/2011 – Lei do Cadastro Positivo (BRASIL, 2011a) – que estabelece que os dados podem ser armazenados com a finalidade de subsidiar a concessão de crédito, realização de venda a prazo ou de outras atividades comerciais ou empresariais que impliquem risco financeiro¹³².

¹³⁰ CRFB, 1988, art. 174: “Como agente normativo e regulador da atividade econômica, o Estado exercerá, na forma da lei, as funções de fiscalização, incentivo e planejamento, sendo este determinante para o setor público e indicativo para o setor privado” (BRASIL, 1988).

¹³¹ O dever de fiscalização geral, contido no ar. 197 do Código Tributário Nacional (CTN), determina que os bancos e demais instituição financeiras são obrigadas a prestar à autoridade administrativa as informações que possuem com relação aos bens, negócios ou atividades de terceiros (BRASIL, 1966)

¹³² Lei n. 12.414/2011, art. 2º: “Para os efeitos desta Lei, considera-se: I – banco de dados: conjunto de dados relativo a pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de

No caso do sistema financeiro, o cuidado com acesso e tratamento de dados deve ser redobrado, pois em todas as atividades de pagamento e transferência são gravadas informações que podem ser observáveis (WESTIN, 1967, p.165). Isso porque a coleta dos dados de cartão de crédito, saques de moeda, compras online, a mera utilização do *Near Field Communication* (NFC)¹³³ no celular e, futuramente, movimentações financeiras de compra e venda de títulos públicos em moeda digital são monitorados e podem gerar a preocupação com a coleta de fluxos de informações qualitativas, definindo **perfis de consumo** (TAVANI; HIMMA, 2008, p. 140).

A formação de perfil de consumo por meio de tratamento de dados, também conhecida como “perfilização” ou *profiling* (DONEDA, 2020a, p. 149), não é, em si mesma, um ato discriminatório, pois são traçados quadros de preferências e tendências presentes e futuras, dentre outros registros que podem auxiliar as tomadas de decisões do titular de dados (ANBIMA, 2018, p. 41). O problema, entretanto, começa quando tal perfil é utilizado para manipular a decisão do indivíduo, seu estilo de vida, estimulando-o a consumir ou negando e concedendo acessos a produtos e serviços, isto é, quando ocorre a chamada discriminação algorítmica¹³⁴. Destaque-se que, quanto maior o número de sujeitos e a disponibilidade dos dados, cada vez mais detalhado e preciso será o volume de informações sobre determinado sujeito. O estudo acerca desses dados torna-se crucial para a definição de autonomia do indivíduo, sua liberdade e identidade (DONEDA, 2011, p. 93).

O controle sobre dados pessoais é meio de empoderar o “eu digital” promovendo a autonomia e capacidade do indivíduo de gerenciar informações sobre si e a forma como ele é visto pela sociedade (LAZARO, 2015, p. 5). A transformação tecnológica alterou a sociedade e uma não pode ser representada mais sem a outra, uma vez que, por meio da tecnologia, informações outrora dispersas, podem ser organizadas e compartilhadas eletronicamente (CASTELLS, 1999, p. 43). Mas isso deve acontecer

crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro; [...]” (BRASIL, 2011a).

¹³³ A tecnologia *Near Field Communication* (NFC) é uma comunicação sem fio, presente nos *smartphones*, *smartwatches* e cartões de crédito (*contactless*), em que se permite a troca de dados por aproximação entre dois dispositivos. Atualmente, ela é utilizada para diversas finalidades – por exemplo, realizar pagamentos, abrir portas e acessar o transporte público.

¹³⁴ São casos de discriminação algorítmica a redução de crédito da American Express feita ao sr. Kevin D. Johnson em razão dos parâmetros de análise de dados, com base nos locais que ele frequentava que possuíam históricos de inadimplimento (LIEBER, 2009). Outro exemplo clássico é o da Decolar.com, que possuía tabelas de preços mais convidativos para pessoas que estavam fora do Brasil durante as Olimpíadas de 2016 no Rio de Janeiro (DECOLAR, 2022; FALEIROS JÚNIOR, 2022, p. 82).

sempre com respeito à boa-fé, sendo vedada qualquer prática discriminatória (BRASIL, 2018), inadmissível na moeda digital brasileira¹³⁵.

O Comitê Europeu para a Proteção de Dados – *European Data Protection Board* (EDPB) – já elaborou recomendação para que haja especificação e detalhamento dos tipos de dados e informações dos usuários que podem ser objeto de tratamento na criação da CBDC, de modo a deixar claro o que pode ser acessado e tratado e o que deve ser restringido: dados de identificação do usuário; informações sobre contas de pagamento e atividades de pagamento, número único de pagamento para a moeda digital (EDPB, 2023b).

O cuidado com a extensão do tratamento de dados também abrange a autorização para o seu compartilhamento, em geral, prevista nos termos de uso, em que normalmente se inclui cláusula que o admite – por exemplo, o termo de uso e a política de privacidade da Febraban preveem a possibilidade de compartilhamento dos dados cadastrais dos clientes do sistema com bancos, independentemente de o titular ter *relacionamento prévio* (FEBRABAN, 2020)¹³⁶.

Apurou-se, também, que a redação dos termos e das condições de privacidade de três instituições selecionadas como nós validadores – a Microsoft, a Unicred e o Banco BV – não estão devidamente compatibilizados com a legislação brasileira – por exemplo, a política de privacidade da Microsoft¹³⁷ segue o padrão da legislação estadunidense (MICROSOFT..., 2024). Enquanto a Unicred admite, sem ressalvas, o

¹³⁵ Lei n. 13.709/2018, art. 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; [...]. Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo” (BRASIL, 2018).

¹³⁶ “2. [...] A FEBRABAN poderá solicitar o seu consentimento específico para realizar o compartilhamento de dados com os Bancos, com os quais você tenha relacionamento ou não, conforme sua preferência, para possibilitar que você use os pontos acumulados na sua educação financeira para obtenção de benefícios junto aos Bancos” (FEBRABAN, 2023).

¹³⁷ A Microsoft faz parte de dois grupos de nós validadores selecionados pelos BCB, quais sejam, o formado pelo Banco ABC, Hamsa e LoopiPay; e outro formado por Consórcio ABBC: Banco Brasileiro de Crédito, Banco Ribeirão Preto, Banco Original, Banco ABC Brasil, Banco BS2 e Banco Seguro, ABBC, BBChain e BIP (BC ANUNCIA..., 2023). Destaca-se a diretriz de compartilhamento seguindo as leis do Estado da Califórnia, cujo texto a seguir se traduz: “Compartilhar. Poderemos “compartilhar” seus dados pessoais, conforme definido pela Califórnia e outras leis estaduais aplicáveis dos EUA, para fins de publicidade personalizada. Conforme observado em nossa seção Publicidade, não fornecemos publicidade personalizada a crianças cuja data de nascimento na conta da Microsoft as identifique como menores de 18 anos.”. Texto na íntegra em inglês: “Share. We may “share” your personal data, as defined under California and other applicable U.S. state laws, for personalized advertising purposes. As noted in our Advertising section, we do not deliver personalized advertising to children whose birthdate in their Microsoft account identifies them as under 18 years of age”(MICROSOFT, 2024).

compartilhamento de dados em meios internacionais¹³⁸ (POLÍTICA..., 2024a), o Banco BV aceita o compartilhamento dos “*dados financeiros*” com prestadores de serviços de armazenamento de dados em nuvem e prestadoras de serviço do BV destinadas a campanhas de publicidade (Banco BV) (POLÍTICA..., 2024b).¹³⁹

Claro que os três termos analisados não se referem ao Drex, mas sua análise deixa margem para questionamento sobre como a participação das três será endereçada no sistema da moeda digital brasileira em relação ao acesso, compartilhamento e tratamento de dados pessoais do usuário do Drex.

No piloto, os nós da rede vão receber, armazenar e processar os dados provenientes dos históricos de pagamentos e transferências financeiras (FANTI; POCHER, 2020, p. 4). Quando for implementado, imagina-se que, para usufruir produtos e serviços desenvolvidos pelas entidades, o usuário vai precisar concordar com os termos de uso dessas aplicações que serão disponibilizadas no futuro (BCB, 2023c)¹⁴⁰.

Considerando os riscos das práticas de vigilância, formação de banco de dados voltados para a perfilização, há que se ter cautela com esse tipo de autorização para compartilhamento de dados no Drex, devendo haver previsão de determinados limites para vedar, por exemplo, o compartilhamento de dados sensíveis e de credenciais de autenticação usadas pelo cliente com instituições terceiras desconexas à finalidade inicialmente estabelecida. A título de exemplo, o *open finance* registra esses limites (BCB, 2020)¹⁴¹.

¹³⁸ A Uniced, cooperativa de crédito, é uma das selecionadas que faz parte do grupo SFCoop: Ailos, Cresol, Sicoob, Sicredi e Uniced (BC ANUNCIA..., 2023). Em sua política há a seguinte pergunta e resposta sobre o compartilhamento internacional: “Realizamos a transferência internacional de dados? Sim. Com o objetivo de oferecer uma elevada qualidade dos serviços e garantir que os dados pessoais estejam disponíveis independentemente do acesso e localidade para consulta e processamento. pode ser necessário encaminhá-los para prestadores de serviço em outros países. Nestes casos, aplicamos todas as medidas organizacionais, contratuais e legais pertinentes para garantir que os dados pessoais sejam processados com segurança, em observância aos requisitos estabelecidos pela LGPD” (POLÍTICA..., 2024a).

¹³⁹ Prevê expressamente o compartilhamento com terceiros, prestadores de serviços do BV exemplificando, dentre elas as de publicidade e computação na nuvem com a finalidade de, entre outras “Realizar a cobrança de valores devidos em contraprestação pelo uso das Plataformas; Oferecer novas ofertas de produtos e Serviços” (POLÍTICA..., 2024b).

¹⁴⁰ Voto BCB n. 31/2023: “39. De uma maneira geral, o Piloto RD deverá, dentro do possível, prever a capacidade de acomodação de desenvolvimentos do sistema em direção às diretrizes gerais do Real Digital e a observância às regras de privacidade e segurança, em consonância com a visão de longo prazo estabelecida para a plataforma do Real Digital” (BCB, 2023c).

¹⁴¹ Portaria BCB n. 108.092/2020, art. 5º: “O Open Finance abrange o compartilhamento de, no mínimo: [...] § 4º O compartilhamento de dados de cadastro de que trata o inciso I, alínea “c”, do caput, deve abranger: I – os dados fornecidos diretamente pelo cliente ou obtidos por meio de consulta a bancos de

Entende-se necessário a padronização dos termos de uso e privacidade entre elas, pois isso é consequência da diretriz do BCB que estabelece a necessidade de adoção de padrões de resiliência e segurança cibernética equivalentes às aquelas aplicáveis a infraestruturas do mercado financeiro (item “ix”, do Voto BCB n. 31/2023) (BCB, 2023c), bem como compatibilidade com a legislação nacional.

Tal raciocínio vale para os prestadores de serviço contratados pelas instituições selecionadas para atuar como nós validadores para armazenamento e processamento de dados e de computação na nuvem. Eles não podem e não devem manipular ou tratar quaisquer tipos de dados ou informações que forem trafegados em sua infraestrutura. Somente admite-se que o tratamento seja realizado pelas entidades previamente selecionadas a participar do Drex¹⁴² que tenham acesso à Rede do Sistema Financeiro Nacional (RSFN) com base na Resolução BCB n. 315/2023 (BCB, 2023b)¹⁴³.

No caso do Drex, as entidades selecionadas se obrigam a disponibilizar e implantar infraestruturas de processamento, comunicação e segurança (*hardware* e *software*)¹⁴⁴ para atuarem no piloto (BCB, 2023b)¹⁴⁵. Quando tais serviços forem executados tanto por prestadores de serviço quanto por empresas de tecnologia (O QUE É...) será necessária atenção especial elas (*big techs*) e sua influência nas finanças

dados de caráter público ou privado, exceto: a) os dados classificados como dado pessoal sensível pela legislação; b) as notas ou pontuações de crédito; e c) as credenciais e outras informações utilizadas com o objetivo de efetuar a autenticação do cliente; [...]” (BCB, 2020).

¹⁴² As empresas, para serem selecionadas como nós validadores, precisaram demonstrar as atividades que pretendiam simular no Piloto, seu histórico de testes em outros projetos no âmbito do SFN ou do SPB e sua experiência com serviços em DLT, especialmente aqueles compatíveis com a EVM (BRASIL, 2023b).

¹⁴³ Resolução BCB n. 315/2023, art. 11: “Os interessados em participar do Piloto RD deverão apresentar sua candidatura, acompanhada de documentos ou informações que declarem ou comprovem, em cada caso: I – as transações de emissão, de resgate ou de transferência dos ativos financeiros referidos no art. 16 que pretendam simular no Piloto RD, bem como os fluxos financeiros decorrentes de eventos de negociação, quando aplicável ao ativo financeiro sujeito ao teste, correlacionando a adequação dessas operações ao seu modelo de negócio, ou da adequação de seu modelo de negócio ao ambiente proposto; II – seu histórico de testes em projetos de tecnologia da informação (TI) coordenados pelo Banco Central do Brasil no âmbito do Sistema Financeiro Nacional (SFN) ou do Sistema de Pagamentos Brasileiro (SPB), tais como os testes de homologação necessários para a participação no arranjo Pix ou no Open Finance; e III – sua experiência com operações ou com a pesquisa aplicada e o desenvolvimento de produtos ou serviços baseados em DLT, preferencialmente compatível com Ethereum Virtual Machine (EVM)” (BRASIL, 2023b).

¹⁴⁴ As entidades autorizadas a atuar como nós validadoras devem prover a infraestrutura de tecnologia da informação com serviços de *hardware* (computadores, servidores, etc.), de *software* (sistemas operacionais, aplicativos, bancos de dados, etc.), de rede (internet) e de pessoas.

¹⁴⁵ Resolução BCB n. 315/2023, art. 19: “As entidades selecionadas para participar do Piloto RD, ao aderirem a este Regulamento por meio da subscrição do Termo de Participação constante do Anexo III a esta Resolução, se obrigam, em especial, a: [...] II – disponibilizar e implantar infraestruturas de processamento, comunicação e segurança (*hardwares* e *softwares*) que suportarão o Piloto RD em sua ponta de atuação;” (BRASIL, 2023b).

(FANTI; POCHER, 2020, p. 7). No caso em questão, caso seja autorizado esse tratamento aos terceiros, elas devem observar a Política de Segurança Cibernética contida na Resolução CMN n. 4.893 de 2021 (CMN, 2021b). Mesmo sabendo que tal Resolução é aplicável, inicialmente, às instituições autorizadas a funcionar pelo BCB, defende-se sua extensão a esses terceiros prestadores de serviços no caso do Drex, pois eles atuarão na infraestrutura dessa moeda digital, ainda que indiretamente, provendo rede, armazenamento e processamento (CMN, 2021b). Reforça-se aqui a necessária limitação ao tipo de dados e informações que poderão ser objeto de tratamento.

Isso é necessário para que seja possível pontuar a extensão da responsabilidade do controlador e operador de dados no Drex¹⁴⁶, nos termos do art. 42 da LGPD.¹⁴⁷ Sendo necessário o esforço em prol da supervisão das atividades dos validadores, e estes para com seus contratados, pois são eles que atuam diretamente com os dados dos usuários (NRB, 2022, p. 38), possuindo acesso a grandes redes financeiras com extensa atividade de dados (DOERR; FROST; GAMBACORTA, 2023, p. 5).

Outro cuidado que se deve ter refere-se à anonimização completa dos dados e informações dos usuários na moeda digital (ANPD, 2023a). Em análise superficial e precipitada, pode-se entender que essa seria a solução ideal para proteger o usuário da moeda digital brasileira (BACH e GARRAT, 2017, p. 65; CHAUM, 1998, p. 199), sob o argumento de que por meio dela é possível conferir ao titular maior controle sobre seus dados pessoais e privacidade (CRUVINEL; PRESTES, 2023, p. 2; ARRABAL, ENGELMANN; MELO, 2017, p. 70). Todavia, a decisão política de utilização de técnicas de anonimização completa na CBDC (EDPB, 2021, p. 3) não cabe no caso brasileiro, em razão do necessário equilíbrio entre os direitos individuais e o interesse público (ECB, 2020b, p. 27; BIS, 2020, p. 6-8).

Como se viu no capítulo 2, a anonimização somente é pertinente diante da necessidade justificada conforme a finalidade do tratamento (ANPD 2023a, p. 11) e no caso do sistema financeiro, isso não pode ser adotada por completo, pois cabe ao BCB adotar medidas de prevenção à ilícitos como lavagem de dinheiro, financiamento ao

¹⁴⁶ Os incisos VI e VII do art. 5º da LGPD tratam de auxiliar na diferenciação desses dois conceitos. O controlador de dados pode ser pessoa jurídica ou natural, de direito público ou privado, cuja característica principal é de ter poder de decisão sobre as atividades relativas ao tratamento de dados. O operador é aquele que realiza o tratamento em nome do controlador (BRASIL, 2018).

¹⁴⁷ Lei n. 13.709/2018, art. 42: “O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo” (BRASIL, 2018)

terrorismo, financiamento de armas de destruição em massa e dar cumprimento a ordens judiciais para rastreamento de atividades ilegais, o que exige acesso a dados não anônimos (BCB, 2023a).

Além disso, o anonimato completo é ilusório (BIONI, 2020, p. 191; NARAYANAN; SHMATIKOV, 2010, p. 24-26; ROGOFF, 2016, p. 106), pois sempre será possível a reidentificação em termos tecnológicos (OLIVEIRA e LOPES, 2021, p. 162). O ato de reconstruir a identidade do usuário – reidentificação – é árduo, pois necessita do cruzamento (OHM, 2010, p. 1.716) e o confrontamento (PARENTONI, 2014, p. 603) de grande quantidade de dados dispersos em variados bancos de dados. Mas não é impossível (EDPB, 2023a, p. 6). Então, nesse caso, os usuários, pessoas naturais do Drex, poderiam ser colocadas em situação de vulnerabilidade, mesmo com a anonimização ou pseudoanonimização.

Por fim, o anonimato não deve ser confundido com a garantia do sigilo na CBDC, pois ambos podem atuar no mesmo contexto jurídico, mas não são sinônimos (OLIVEIRA; LOPES, 2021, p. 172). O usuário da CBDC precisa ser identificado, por exemplo, para a Receita Federal, em prol do exercício da fiscalização intermitente da administração fazendária para evitar sonegação fiscal (SAMPAIO, 1992, p. 445) conforme art. 12 da Lei Complementar n. 70 de 1991 (BRASIL, 1991)¹⁴⁸.

Para isso, o BCB tem estudado as *Privacy Enhancing Technologies* (PETs)¹⁴⁹ (BCB, 2023a, p. 24) que são tecnologias de aprimoramento da privacidade por meio de criptografia. Na segunda plenária do Drex, ocorrida em 27 de setembro de 2023, foram apresentadas três soluções empresariais que estão sendo testadas no Piloto do Drex: a *Anonymous Zether*, a *Starlight* e a *Parchain* (FÓRUM..., 2023). Essas soluções são algoritmos de criptografia para fazerem prova da identidade dos usuários, isto é, elas

¹⁴⁸ Lei Complementar n. 70/1991, art. 12: “Sem prejuízo do disposto na legislação em vigor, as instituições financeiras, as sociedades corretoras e distribuidoras de títulos e valores mobiliários, as sociedades de investimento e as de arrendamento mercantil, os agentes do Sistema Financeiro da Habitação, as bolsas de valores, de mercadorias, de futuros e instituições assemelhadas e seus associados, e as empresas administradoras de cartões de crédito fornecerão à Receita Federal, nos termos estabelecidos pelo Ministro da Economia, Fazenda e Planejamento, informações cadastrais sobre os usuários dos respectivos serviços, relativas ao nome, à filiação, ao endereço e ao número de inscrição do cliente no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Geral de Contribuintes (CGC)” (BRASIL, 1991).

¹⁴⁹ Existem vários tipos de PETs e diversas outras são criadas para atender às demandas tecnológicas. São exemplos de PETs: Homomorphic encryption, Ring Signatures, Bling Signatures, Secure multi-party computation, Federated learning, Trusted execution environments, Zero-knowledge proofs (ZKP), Tiered Ledger Systems, Privacy Threshold Limits, Differential privacy (Privacidade Diferida) e Anonymization, dentre outras. (CHAUM, 1998; THE PET..., 2023; GENTRY, 2009; RAKHMELEVICH, 2023).

permitem verificar as atividades sem relevar informações do usuário em si, em prol da privacidade.

- O início dos testes com a *Anonymous Zether* se deu em outubro de 2023 (EYBLOCKCHAIN, 2024) e tal PET foi desenvolvida pela JPMorgan e incorporada pela companhia Consensus. Ela funciona como sistema privado de rastreamento de valor no qual o contrato inteligente mantém os saldos das contas criptografadas utilizando criptografia homomórfica¹⁵⁰, sendo acessível a determinadas pessoas pela criptografia assimétrica.

A criptografia homomórfica foi proposta inicialmente por Ronald Rivest (RIVEST, ADLEMAN e DERTOUZOS, 1978), Leonard Adleman e Michael Dertouzos em 1978 (ADAMS, 2021, p. 257) e sua utilização está atrelada à garantia de confidencialidade (ADAMS, 2021, p. 249). Todavia, foi apenas em 2009 que o sistema de criptografia totalmente homomórfica começou a ser viabilizado para sistemas de pagamento por Craig Gentry (GENTRY, 2009). A *Fully Homomorphic Encryption (FHE)* ou apenas *Homomorphic Encryption*, traduzida literalmente como criptografia homomórfica, pode ser entendida como forma de criptografar dados, tornando-os ilegíveis total ou parcialmente, antes do seu compartilhamento.

Ela pode ser utilizada para a proteção de dados e para assegurar a privacidade na CBDC, especialmente para cumprimento do princípio da finalidade e segurança no tratamento dos dados. Isso porque, os dados de identificação podem ficar ofuscados, e mesmo com as identidades criptografadas ainda é possível analisar os valores da movimentação financeira que foi realizada, seja de débito ou crédito, sem necessidade de descriptografá-los (REVOREDO, 2022). Ademais, tal forma de criptografia é indicada em razão de seu alto nível de interoperabilidade (WEF, 2021, p.14).

A *Anonymous Zether* também se vale de criptografia assimétrica, isso é possui o par de chaves pública e privada (DOCUMENTAÇÃO..., 2023), o que faz com que apenas o titular da chave privada consiga gerir e visualizar os fundos (THE PET..., 2023). Esse é um ponto importante para a garantia da autodeterminação informativa do indivíduo, que passará a ter controle sobre quem acessa seus dados. Todavia, devem ser tomados cuidados em relação ao manuseio e a guarda das chaves públicas pelos bancos

¹⁵⁰ A criptografia homomórfica é uma técnica que permite tratar dados que estejam criptografados, sem a necessidade de descriptografá-los.

centrais, ou no caso brasileiro, pelas entidades autorizadas, e das chaves privadas pelos próprios usuários (ECB, 2020a, p. 16).

As outras duas soluções estão em fase de discussões técnicas.

- A Starlight, criada pela Ernest Young, é proposta de código aberto (*open source*) para a privacidade, que utiliza o protocolo *Zero Knowledge Proof*, cujo intuito é comprovar a veracidade de informação sem que ela seja completamente revelada a todas as partes da transação (EYBLOCKCHAIN, 2024). A título de exemplo, o teste com a Starlight consiste em permitir ao usuário final do Drex comprovar que possui saldo para efetivar transferência ou pagamento, sem precisar exigir a sua revelação (DOCUMENTAÇÃO..., 2023).

No projeto piloto, o Brasil testa essa solução para a transferência de Real digital entre duas instituições e a compra e venda de títulos públicos federais tokenizados.

- Já a solução Parchain, foi desenvolvida pela fintech brasileira especializada em blockchain denominada Parfin. Trata-se de uma das selecionadas como entidades autorizadas para realizar os testes do piloto Drex. Nesse caso, também é utilizado o protocolo *Zero Knowledge Proof*, bem como a computação multipartidária (*Multi-Party Computation* - MPC) que torna possível soluções de interoperabilidade da blockchain para outra, seja ela pública ou privada. Como apresentado pelo Banco Central do Canadá, a computação multipartidária é proposta positiva para se pensar em economia globalizada de CBDC's, especialmente pelo fato de que por meio dela, diversas entidades podem contribuir com dados para a detecção global de fraudes, mantendo a privacidade uns dos outros (DARBHA; ARORA, 2020).

É necessário ainda entender o funcionamento prático dessas técnicas (PETs) mesmo sabendo que tais técnicas, em geral, já são indicadas como possíveis soluções para a detecção global de fraudes, mantendo a privacidade dos envolvidos com remessa de valores (DARBHA; ARORA, 2020; CORRÊA; LEITE, 2023, p. 209-231). Mas tanto o Brasil (BOMFIM, 2024)¹⁵¹ quanto o Japão (ECB, 2020a, p.28)¹⁵² já apontam o

¹⁵¹ O obstáculo encontrado para a privacidade e escalabilidade do sistema impactará até mesmo no cronograma dessa funcionalidade para o Brasil. Sendo apontado na fala do coordenador do Drex, Fábio Araújo em painel “Explorando as Fronteiras do Drex” ocorrido no evento WebSummit de 17 abril de 2024 que até a metade desse ano serão divulgados para a população os relatórios desse projeto (YOUTUBE, 2024).

¹⁵² O Banco Central Europeu, conjuntamente com o Banco Central do Japão em 2020, quando do estudo do Projeto Stella (Stella Project) (ECB, 2020a) fizeram o balanceamento entre confidencialidade e auditabilidade em sistema de registro distribuído, apontando as principais técnicas de aprimoramento da

receio quanto à privacidade e escalabilidade do sistema pois o tipo de PET escolhido influencia diretamente na carga computacional que será atraída para a CBDC, impactando precipuamente na escalabilidade e latência do sistema.

Por mais que o BCB afirme seu compromisso de obedecer a legislação nacional, em especial a LGPD e a Lei de Sigilo Bancário, bem como reforce que a infraestrutura tecnológica do Piloto deve permitir o teste de “privacidade das informações empregadas” nos casos de uso¹⁵³, “em observância à legislação brasileira” (BCB, 2023c; BCB, 2023d)¹⁵⁴, na avaliação feita da documentação disponibilizada pelo BCB até fevereiro de 2024, entende-se que as normas a editar para reger a criação e o funcionamento do Drex devem ser elaboradas com maior detalhamento quanto a que dados serão acessados, tratados e compartilhados e como será a responsabilização por práticas indevidas envolvendo dados de usuários do Drex.

Reforça essa preocupação antecipada ao lançamento do Drex para a população, por exemplo, a pesquisa divulgada pela Febraban em que se apurou que 80% (oitenta por cento) das instituições brasileiras ainda não se adequaram completamente à lei de proteção de dados (FEBRABAN, 2023).

As normas editadas pelo CMN e pelo BCB são mais protecionistas do que a própria LGPD, pelo fato de tratarem de assuntos específicos (BRAGUIM, 2023), mas pela documentação do Drex analisada durante a produção desta dissertação, não foi possível observar com clareza como o BCB pretende, normativa e tecnologicamente, observar a legislação de proteção da privacidade e dos dados pessoais do usuário da moeda digital brasileira.

Espera-se que as próximas normas possam pelo menos explicitar que tipo de dado (se dado pessoal, dado sensível, dado anonimizado e dado pseudoanonimizado)¹⁵⁵ que poderá ser objeto de tratamento, sabendo-se dos diferentes níveis de proteção e complexidade do tratamento deles. Isso porque é certo que o tratamento de dados sem o

privacidade, divididas em PET's de segregação, PET's de ocultação (hiding) e desvinculação (unlinking).

¹⁵³ Por enquanto, os casos de uso testados no piloto são: moeda digital de banco central (CBDC), representações em token depósitos bancários a vista, moeda eletrônica e título público federal.

¹⁵⁴ Voto BCB n. 31/2023, Art. 16: “[...] § 2º A infraestrutura tecnológica construída no Piloto RD deverá permitir o teste e a avaliação dos seguintes potenciais da tecnologia empregada: [...] III – privacidade das informações empregadas nos casos de uso, em observância à legislação brasileira pertinente” (BCB, 2023c).

¹⁵⁵ Recomenda-se abstrair as diversas polêmicas e múltiplas classificações encontradas na literatura sobre dados (PARENTONI, 2015, p. 550), sendo seguro para o BCB discorrer somente sobre quatro tipos de dados mencionados.

devido consentimento¹⁵⁶ e sem adequação ao princípio da finalidade (BRASIL, 2018)¹⁵⁷ é comparável, pela literatura, à violação de sigilo (BALDUCCINI *et al.*, 2020). Espera-se, também que as normas que forem criadas possam endereçar orientações sobre a elaboração das políticas de privacidade e termos de uso, exigindo, por exemplo, que apresentem o consentimento expresso para o compartilhamento internacional de dados, em prol dos pagamentos transfronteiriços – item viii, “d” do Voto BCB n. 31/2023 (BRASIL, 2023c) – e a adequação ao princípio da finalidade. É necessário, ainda, que seja regulada a atuação dos terceiros na rede do Drex, restringindo determinados acessos e tratamento a tipos de dados e informações, bem como pontuando os limites da criptografia para que não se chegue ao anonimato completo.

A *privacy and data protection by design* e *privacy and data protection by default*¹⁵⁸ (CAVOUKIAN, 2011) são conceitos que devem estar presentes tanto nos aspectos técnicos do desenho estrutural do Drex, quanto em legislações e normativas sobre o tema¹⁵⁹, mas também é preciso a orientação aos usuários, pessoas naturais e

¹⁵⁶ Lei n. 13.709/2018, art. 7º: “O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular; [...]” (BRASIL, 2018).

¹⁵⁷ Lei n. 13.709/2018, art. 6º: “As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; [...]” (BRASIL, 2018).

¹⁵⁸ A privacidade como padrão (*privacy by default*) significa tratar a privacidade de maneira intrínseca em qualquer sistema de tecnologia, assim sendo, mesmo que o indivíduo não atue, sua privacidade permanecerá intacta (PRIVACY... 2019). Isso pois, foram lançadas sobre o software configurações de privacidade que devem ser aplicadas por padrão. A título de exemplo, o direito à exclusão de própria conta e dos dados pessoais a ela vinculados, devem estar disponíveis na aplicação, em razão da privacidade como padrão. Outro exemplo, é que as políticas de Cookies devem estar sempre desativadas por padrão e, somente a concordância do usuário é que deve haver esse rastreo dos cookies. A privacidade como desenho (*privacy by design*) se caracteriza por atitudes tomadas para prever o resultado danoso e diminuir o risco, em todas as fases de desenvolvimento da aplicação (GUIA, 2022, p.12). Por exemplo, criptografar parcialmente o CPF em um extrato bancário é uma forma de coibir a publicidade desse dado.

¹⁵⁹ Levando em consideração ao que prevê a Lei n. 13.874 /2019 – Lei da Liberdade Econômica (BRASIL, 2019) – e o Decreto n. 10.411/2020 (BRASIL, 2020), para a criação de atos normativos sobre esse assunto de segurança para atingimento da privacidade e da proteção de dados do Drex, entende-se que é necessário apresentar relatório prévio analisando o impacto regulatório dessa matéria caso seja inevitáveis alterações ou inovações legais (BRASIL, 2020). É isso que prevê o Decreto que regulamenta a Lei de Liberdade Econômica, cujo texto é transcrito a seguir: “Art. 2º Para fins do disposto neste Decreto, considera-se: I – análise de impacto regulatório – AIR – procedimento, a partir da definição de problema regulatório, de avaliação prévia à edição dos atos normativos de que trata este Decreto, que conterá informações e dados sobre os seus prováveis efeitos, para verificar a razoabilidade do impacto e subsidiar a tomada de decisão; II – ato normativo de baixo impacto – aquele que: a) não provoque aumento expressivo de custos para os agentes econômicos ou para os usuários dos serviços prestados; b) não provoque aumento expressivo de despesa orçamentária ou financeira; e c) não repercuta de forma substancial nas políticas públicas de saúde, de segurança, ambientais, econômicas ou sociais; [...]” (BRASIL, 2020).

assegurar para que os indivíduos possam ter a “efetiva” autodeterminação informativa¹⁶⁰ nas finanças descentralizadas.

Ora, o usuário, então ao adentrar, no Drex, que possui padrões de privacidade e proteção de dados *by design* e *by default*, poderá aceitar os termos de uso e políticas de privacidade dessas aplicações de forma livre e esclarecida, realizando suas atividades de pagamento e transferências de moeda digital de maneira efetiva. Afasta-se, portanto, a ideia de que o titular dos dados é vítima em uma arquitetura assimétrica, pautada pela assimetria informativa entre Estado/privados para com o usuário, e aproximando-se de sua autonomia e protagonismo sobre seus próprios dados. Ele se torna autônomo em suas decisões e pretensões, assumindo a responsabilidade pelas escolhas feitas (SASDELLI, 2023, p. 263), o que pode ser chamado, “efetivamente”, de autodeterminação informativa.

Por mais que existam apontamentos no sentido de que bancos de dados em redes *blockchain* são desafiadoras quanto a acarretar problemas com relação à propriedade intelectual (SUBRAMANIAN, 2019a), deve-se pontuar que o poder e a titularidade sobre os dados pessoais são sempre do cidadão, nos termos da LGPD, e o consentimento para o tratamento não deve (e nem pode) significar abdicar de tal direito, pois a privacidade, como direito da personalidade, e a proteção de dados, como direito fundamental, são irrenunciáveis.

Além dessas preocupações com a definição de limites para a atuação das instituições – públicas ou privadas – que farão parte da rede do Drex, não foi possível localizar na documentação analisada como se dará a atuação da Autoridade Nacional de Proteção de Dados (ANPD) no sistema descentralizado do Drex.

4.2 Agência Nacional de Proteção de Dados (ANPD): atuação de autoridade centralizada em ambiente descentralizado

Considerando que a ANPD é autarquia, de natureza especial, vinculada ao Ministério da Justiça, isto é, ao Poder Executivo e que possui autonomia técnica e decisória para o exercício da proteção de dados pessoais, cabe questionar como se dará

¹⁶⁰ A autodeterminação informativa é um dos fundamentos da disciplina da proteção de dados pessoais (BRASIL, 2018).

sua atuação regulatória no sistema distribuído do Drex, tendo em vista tratar-se de uma autoridade centralizada.

Embora a ANDP tenha reconhecido a importância da tecnologia de registro distribuído de dados, ressaltou que é necessário adequá-la à legislação de proteção da privacidade e dos dados pessoais (BLOCKCHAIN, 2023).

Ora, a ANDP possui a prerrogativa de dispor sobre padrões e técnicas para processos de anonimização, bem como de realizar verificações de segurança (BRASIL, 2018),¹⁶¹ mas seu poder de atuação na rede em questão ainda não está bem definido, sendo necessário avaliar com maior aprofundamento em pesquisas futuras sobre se ela deve ou não atuar na rede descentralizada do Drex.

Por ora, apenas analisando a competência normativa da ANDP, tudo indica ser impositiva sua atuação no contexto do Drex, em razão de dois principais motivos:

- Primeiro, porque ela tem o poder de aplicar sanções administrativas aos diversos setores sociais que tratam dados, incluindo o setor financeiro, conforme previsto na LGPD (BRASIL, 2018)¹⁶² e na Resolução CD/ANDP n. 4/2023 (ANPD, 2023b). Não obstante, quando da aplicação de sanções a instituições financeiras selecionadas para atuar como nós validadoras, por exemplo, a ANPD deva dar ciência ao BCB para que ele se manifeste, se for o caso, sobre eventuais consequências da imposição desse tipo de sanção para o exercício da atividade econômica, da estabilidade do sistema financeiro (ANPD, 2023b)¹⁶³. Esse tipo de previsão tem o condão de tentar reduzir eventual divergência entre os reguladores (OLIVEIRA NETO; ARANTES, 2023).

- O outro fato que justifica a atuação da ANPD no contexto do Drex diz respeito aos pagamentos transfronteiriços e transferência internacional de dados. Atualmente, não se encontram regulamentados os procedimentos que vão orientar a atuação da ANPD no tocante à definição do conteúdo de cláusulas-padrão contratuais ou à verificação de cláusulas contratuais específicas relativas à transferência internacional de dados pessoais (BRASIL, 2018), o que precisa ser enfrentado para que seja possível

¹⁶¹ Cf. art. 12 da LGPD (BRASIL, 2018).

¹⁶² Cf. Art. 52 da LGPD (BRASIL, 2018).

¹⁶³ Resolução CD/ANDP n. 4/2023, Art. 3º: “[...] § 2º “Na hipótese do § 1º deste artigo, a ANPD dará ciência ao principal órgão ou entidade reguladora setorial, com competências sancionatórias, a que se submete o controlador, durante a fase de instrução, para que se manifeste sobre eventuais consequências da imposição das sanções para o exercício de atividades econômicas reguladas desenvolvidas pelo controlador, especialmente na prestação de serviços públicos, assim como forneça outras informações que entender pertinente” (ANPD, 2023b).

falar em pagamentos transfronteiriços via Drex, até mesmo por questões diplomáticas¹⁶⁴.

No material levantado até fevereiro de 2024, não foi possível localizar documentos, relatórios ou encontros que pudessem denotar alinhamento de expectativas ou de atuação entre o BCB e a ANPD. Entende-se, no entanto, que a ANPD deve ter espaço no debate entre as autoridades que idealizam e conduzem o Piloto do Drex, visando potencializar a proteção de dados e privacidade financeira dos brasileiros usuários que o utilizarem como meio de pagamento. Uma possível tecnologia que pode permitir a entrada da ANPD na rede *on chain*¹⁶⁵ é o oráculo (do inglês *oracles*) para o exercício do seu dever de fiscalização e aplicação de sanções.

Em redes distribuídas, geralmente, os participantes devem atuar *on chain*, tendo acesso somente aos dados de sua própria rede, sem interação com o mundo real. (BAMBARA, 2018, p. 89). É o denominado “Problema do Oráculo” (*Oracle Problem*) em que as *blockchains* são incapazes de acessar dados externos, tornando-se redes isoladas (THE BLOCKCHAIN..., 2023).

Com o crescimento, entretanto, das aplicações distribuídas para as diversas áreas sociais, fruto da geração *Blockchain* 3.0, viu-se a necessidade de propor solução capaz de interagir com o mundo real (*off chain*), mas que permanecesse dentro da rede *blockchain* (*on chain*) (SOUSA, 2023, p. 22). No ambiente descentralizado, esse agente denominado “Oráculo”, nome misterioso e curioso, que, no contexto de registros distribuídos, é representando por terceiros de confiança, que não fazem parte do mecanismo de consenso, isto é, se orientam fora da rede distribuída (*off chain*), podendo trazer-lhe dados externos e adicionar funções de contratos inteligentes (TCU, 2020, p. 18; BAMBARA, 2018, p. 7).

Os oráculos podem entrar na *Blockchain* de duas maneiras. Na primeira delas, sua participação é fixa, em todos os contratos inteligentes, seja por solicitação, seja prestando resposta àquele evento. A segunda maneira é mais flexível, pois os oráculos

¹⁶⁴ Lei n. 13.709/2018, art. 35: “A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional” (BRASIL, 2018).

¹⁶⁵ O termo “on chain” diz respeito àquilo que ocorre dentro da rede, enquanto “off chain” refere-se a tudo aquilo que ocorre em ambiente externo, fora dessa rede distribuída (RAUCHS *et al.*, 2018, p. 34). A princípio, sistemas DLTs devem ser independentes do mundo real, possuindo autonomia decisória de maneira endógena, mas existem sistemas que podem ser híbridos ou até mesmo totalmente exógenos (RAUCHS *et al.*, 2018, p. 50). Há também a expressão “Governança On Chain” relacionada à incorporação de recursos de governança nas camadas de dados dos sistemas DLTs.

podem ser eventualmente chamados à *Blockchain* quando certas condições do contrato inteligente são atendidas – por exemplo, o “Oráculo XXX” será notificado quando o valor de pagamento utilizando-se da moeda digital Drex for superior a um milhão de reais, isto é, a proposição lógica resultaria em “se atingido determinado preço, então acionar o oráculo” (BAMBARA, 2018, p. 154).

Agentes – geralmente relacionados às autoridades públicas¹⁶⁶, no cumprimento de deveres legais e demais ocorrências no mundo físico (*off chain*) – podem, portanto, por meio do oráculo, alterar e enviar informações para a *blockchain*, desencadeando mudanças na rede descentralizada. Para tanto, é necessário que esse terceiro autorizado a atuar no fluxo do contrato inteligente como oráculo seja confiável o suficiente, tendo em vista que sua atuação é imutável e irreversível (BAMBARA, 2018, p. 154).

A Autoridade Nacional de Proteção de Dados poderá atuar como “Oráculo Drex” quando for implementada a moeda digital brasileira. Isso porque a Autoridade Nacional emitirá opiniões técnicas ou recomendações referentes ao tratamento de dados para fins de segurança pública, defesa nacional e atividades de investigação e repressão de infrações penais pertinentes à temática da proteção de dados (art. 4º, III, e § 3º da LGPD)¹⁶⁷. Esse órgão, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, poderá enviar padrões e técnicas utilizados em processos de anonimização¹⁶⁸ diretamente para a rede descentralizada. Além disso, pode determinar o término do tratamento de dados¹⁶⁹, solicitar informações específicas sobre o âmbito e a natureza

¹⁶⁶ O Departamento de Trânsito (Detran) existente nos Estados brasileiros pode ser exemplo de possível oráculo para transferência de veículos (SILVA, 2019).

¹⁶⁷ Existem casos de tratamento de dados que não precisam da aplicação da LGPD, por exemplo, aqueles realizados em prol da segurança pública, defesa nacional, segurança do estado ou atividades de investigação e repressão de infrações penais – inciso III do art. 4º da LGPD (BRASIL, 2018). Nessas hipóteses, a ANPD deverá emitir opiniões técnicas ou recomendações sobre esse assunto, solicitando aos responsáveis pelo tratamento relatórios de impacto à proteção de dados – § 3º do art. 4º da LGPD (BRASIL, 2018).

¹⁶⁸ Lei n. 13.709/2018, art. 12: “Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. [...] § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais” (BRASIL, 2018).

¹⁶⁹ Lei n. 13.709/2018, art. 15: “O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: [...] IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei” (BRASIL, 2018).

dos dados¹⁷⁰, estabelecer normas complementares para a comunicação e o uso compartilhado de dados pessoais¹⁷¹, bem como aplicar sanções¹⁷².

No Relatório de Economia Bancária do BCB de 2022, os oráculos são citados no protótipo do Real Digital (BCB, 2022a, p. 5), sendo responsáveis pelo fluxo de informação entre as camadas dedicadas (SCHÄR, 2021) de protocolo, aplicações e agregação da CBDC brasileira¹⁷³. Essa informação, no entanto, não foi localizada no Voto BCB n. 31/2023 (BCB, 2023c), na Resolução BCB n. 315/2023 (BCB, 2023b), tampouco no Kit Onboarding do Piloto RD disponível no GitHub (DOCUMENTAÇÃO..., 2023).

A comunicação entre o mundo *on chain* e o mundo *off chain* precisa ser construída para que a CBDC brasileira possa ser interoperável com os dados do mundo real. Assim, a figura do oráculo pode ser exercida por outras entidades, tendo em vista que existem situações como alíquotas tributárias e taxas de câmbio que são alteradas e precisam, por exemplo, ser comunicadas ao sistema da CBDC, o que pode ser feito via oráculo para a garantia da integridade das informações obtidas de entidades externas fora da rede (WEF, 2023, p. 31).

O complicador consiste no fato de que, ao trazer mais autoridades para dentro da rede, aumenta-se cada vez mais o nível de centralização sobre ela, desnaturando completamente a ideia de finanças descentralizadas (DeFi). Somado a isso, está o fato de que a existência de oráculo pode potencializar a possibilidade de vulnerabilidade do sistema, que dependerá cada vez mais de dados externos para sua execução (E-HKD..., 2023, p. 13; EUROPEAN COMMISSION, 2020, p. 59). Deixando assim, que o *design* do sistema fique, cada vez mais, propenso à censura e a fragilidades não somente de

¹⁷⁰ Lei n. 13.709/2018, art. 29: “A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei n. 13.853, de 2019)” (BRASIL, 2018).

¹⁷¹ Lei n. 13.709/2018, art. 30: “A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais” (BRASIL, 2018).

¹⁷² Lei n. 13.709/2018, art. 52: “Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]” (BRASIL, 2018).

¹⁷³ A arquitetura do ambiente das finanças descentralizadas (DeFi) é organizada em cinco camadas (SCHÄR, 2021, p. 155-156), quais sejam: liquidação, ativos, protocolo, aplicações e agregações. Por ora, para a temática dos oráculos importa saber apenas na camada de protocolo são definidos padrões para o negócio; enquanto na de aplicações, ocorre o desenvolvimento das aplicações; e, por fim, na de agregação, é apresentado o resultado final, voltado especialmente para os objetivos do *open finance* de promover serviços agregados de forma ágil, ou como o BCB afirma, de maneira atômica (BCB, 2023c).

segurança, como também de desempenho, impactando negativamente nas compensações e escalabilidade do sistema (RAUCHS *et al.*, 2018, p.45).

Feitas tais reflexões, novas pesquisas devem abranger a pertinência ou não da entrada da ANPD na rede do Drex pelos motivos já expostos, afim de viabilizar as sanções administrativas, por exemplo. Sendo necessário refletir até que ponto trazer tal autoridade é interessante até mesmo para o Estado, em razão de custos com pessoal. Ademais, deve-se refletir também se é possível substituir sua atuação *on chain* pela autoexecutoriedade dos contratos inteligentes, pois se o próprio sistema conseguir reconhecer a falha, poderia aplicar a sanção. O problema é cuidar do devido processo legal nestes casos.

CONCLUSÃO

Do estudo realizado, apurou-se que as moedas digitais emitidas por bancos centrais podem ser criadas com formatos diferentes – por exemplo, no modelo atacado ou varejo, com a adoção de bancos de dados centralizados em que se tem o uso das contas ou com adoção de banco de dados distribuído, mediante a emissão, por exemplo, de *tokens*. Nesse último caso, pode-se valer, do gênero da tecnologia DLT, ou tecnologia de livros distribuídos, ou da espécie de DLT que envolve a tecnologia da *blockchain*.

O banco de registros de dados do tipo “DLT”, por sua vez, pode ser desenhado com formatos variados que vão impactar no modo de acesso e de autorização para tratar e compartilhar os dados ali registrados. Foi possível verificar que os desenhos podem envolver, por exemplo, bancos de registro de dados, comumente chamados de “redes”, permissionadas e públicas; permissionadas e privadas; não permissionadas e públicas; não permissionadas e privadas.

O registro e a alteração do registro de dados em redes nas quais são criadas moedas digitais emitidas por bancos centrais no formato tokenizado dependem da observância de condições estabelecidas para o acesso e o funcionamento do banco de dados, os chamados “mecanismos de consenso”. Foram estudados os três mecanismos de consenso mais usados nas redes de DLT disponíveis no mercado: *Proof of Work* (PoW), *Proof of Stake* (PoS); e *Proof of Authority* (PoA), cuja identificação ocorre conforme o nível de descentralização, latência, energia, segurança e método de validação do registro de dados na rede, por exemplo.

Pela análise da documentação levantada até fevereiro de 2024, pode-se dizer que a CBDC brasileira – isto é, o Drex – foi desenhado para ser emitido no formato atacado, tokenizada, com uso de redes DLT permissionada e privada, bem como a adoção do mecanismo de consenso do tipo PoA.

Em tal desenho, planeja-se que o BCB emita a moeda digital para as instituições financeiras e de pagamento selecionadas para fazer parte da Rede Drex, e elas emitam para os seus clientes *tokens* que representam a moeda digital lastreada no Real.

Como base no material a que se teve acesso, conforme o recorte temporal informado, apurou-se que apesar de o BCB ter expressamente se comprometido a observar a legislação geral e especial de proteção da privacidade e dos dados do usuário do Drex, não foi possível localizar a definição de quais dados pessoais poderão ser

acessados na rede da moeda digital brasileira, quem terá acesso a eles e qual será a extensão da autorização para seu tratamento e compartilhamento.

Além da ausência dessas definições, apesar de se ter localizado previsão de atribuição de competência ao Comitê Executivo de Gestão do Piloto Drex e a seus membros para zelar pela proteção de dados que o comitê reunir, não ficou claro como se dará a responsabilização pelo tratamento indevido de dados.

Assim, considerando o estágio evolutivo da criação do Drex no Brasil, ainda na fase de projeto-piloto, cujos testes não foram finalizados, não é possível afirmar com certeza que a privacidade e os dados pessoais do usuário da moeda digital brasileira restarão comprometidos.

Todavia, as indefinições identificadas alertam sobre a necessidade de as futuras normas que serão editadas pelo CMN e pelo BCB deixarem claros tais aspectos, sob pena de que a falta de definição de que dados pessoais podem ser acessados, tratados e compartilhados e por quem, leve à prática de atividades de processamento de dados, que, por sua vez, gerem informações sobre registros e padrões de atividades como valores de moedas e serviços utilizados, os quais, por consequência, podem conduzir à indevida vigilância, abusiva manipulação de banco de dados nacionais e internacionais e à perfilização dos usuários.

A regulação a cargo do CMN e do BCB precisará enfrentar, além disso, o tema da anonimização, que conforme se viu, jamais pode ser permitida que seja completa, para que se possa compatibilizar de forma equilibrada a proteção da privacidade e dos dados pessoais do Drex com o interesse público ligado à identificação dos sujeitos para o fim de evitar, coibir ou punir o cometimento de fraudes e crimes, como o de lavagem de dinheiro.

Por fim, os reguladores do mercado financeiro brasileiro precisam definir padrões para a elaboração dos termos de uso, o que, inevitavelmente, dependerá de atuação conjunta com a ANPD, responsável por definir padrões internacionais de transferência de dados. Isso, em especial, para a realização dos planejados pagamentos transfronteiriços.

Apesar de se ter apresentado posicionamento em favor da participação da ANPD na rede do Drex, inclusive com a adoção do mecanismo do oráculo para viabilizá-la, admite-se que tal aspecto precisa ser mais bem estudado dos pontos de vista político e tecnológico, pois, do ponto de vista jurídico, demonstrou-se que ela tem competência

para fiscalizar o cumprimento das normas de proteção da privacidade e dos dados pessoais em qualquer setor da sociedade brasileira.

Ainda que o CMN, o BCB e a ANPD regulem de maneira clara os dados que serão acessados, tratados e compartilhados e quem poderá fazê-lo, é preciso investigar em nova etapa de pesquisa sobre quão eficiente será essa regulação para de fato proteger a privacidade do usuário do Drex. Ora, o que usualmente se vê é a situação em que as pessoas renunciam à sua privacidade com um clique em *softwares* com disponibilidade de termos de uso, apondo seu consentimento para instituições acessarem e tratarem seus dados pessoais em troca do “acesso gratuito” a aplicativos e a outros serviços ofertados no mercado brasileiro e internacional.

Outro aspecto a merecer nova agenda investigativa refere-se aos efeitos da implementação prática das técnicas de criptografia por meio das PETs, que ainda estão sendo testadas pelo BCB e que, até o recorte temporal pesquisado, enfrenta grande embate entre a privacidade e a escalabilidade. Ademais, será necessário estudar ainda a viabilidade da exclusão de dados pessoais no Drex, direito assegurado ao seu titular conforme o inciso IV do art. 18 da LGPD.

REFERÊNCIAS

A MOEDA digital brasileira ganha um nome e agora se chama Drex. *Banco Central do Brasil*, 7 ago. 2023. Disponível em:

<<https://www.bcb.gov.br/detalhenoticia/17946/nota>>. Acesso em: 11 fev. 2024.

ACESSO CAFe. *Periódicos CAPES*. Disponível em: <<https://www-periodicos-capes.gov-br.ezl.periodicos.capes.gov.br/index.php?>>>. Acesso em: 6 out. 2023.

ADAMS, Carlisle. *Introduction to Privacy Enhancing Technologies: A Classification-Based Approach to Understanding PETs*. School of Electrical Engineering and Computer Science. University of Ottawa. *Editora Springer*, 2021.

AGENDA BC#. *Banco Central do Brasil (BCB)*. 2023. Disponível em:

<<https://www.bcb.gov.br/acessoinformacao/bchashtag>>. Acesso em: 13 jan. 2024.

AGREGADORES financeiros: entenda a próxima fronteira do Open finance. *Instituto Propague*. 1º set. 2023. Disponível em: <<https://institutopropague.org/open-finance/agregadores-financeiros-entenda-a-proxima-fronteira-do-open-finance/>>. Acesso em: 15 nov. 2023.

AMAZON WEB SERVICES (AWS). *Central Bank digital currency (parte 2): technology options and performance criteria*. 2 fev. 2021. Disponível em:

<https://pages.awscloud.com/rs/112-TZM-766/images/AWSPS_cbdc_2_Feb-2021.pdf>. Acesso em: 15 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIROS E DE CAPITAIS (ANBIMA). *Ética, regulamentação e análise do perfil do investidor*: material de estudos da certificação CPA-10. 2018. Disponível em: <<https://www.anbima.com.br/data/files/10/40/99/33/466A4810EA926748882BA2A8/CPA-10-Cap2.pdf>>. Acesso em: 8 dez. 2023.

ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIROS E DE CAPITAIS (ANBIMA). *Tokenização de ativos*: conceitos iniciais e experimentos em curso, 2022, p. 1-24. Disponível em: <<https://www.anbima.com.br/data/files/02/30/82/CB/68001810C27A8F08882BA2A8/Tokenizacao%20de%20ativos.pdf>> Acesso em: 15 out. 2023.

ATIVOS VIRTUAIS (moedas virtuais, criptomoedas ou criptográficas). Moedas virtuais. *Banco Central do Brasil (BCB)*. 2 ago. 2023. Disponível em: <<https://www.bcb.gov.br/meubc/faqs/p/moedas-virtuais-criptomoedas-ou-criptograficas>>. Acesso em: 3 dez. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Estudo técnico sobre a anonimização de dados na LGPD*: análise jurídica. Versão 1.0. Brasília, nov. 2023a. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd___analise_juridica.pdf>. Acesso em: 16 mar. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD n. 4, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Órgão: Ministério da Justiça e Segurança Pública/Autoridade Nacional de Proteção de Dados. *Diário Oficial da União*: Brasília, 27 fev. 2023b. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucao4CDANPD24.02.2023.pdf>>. Acesso em: 16 mar. 2024.

BAINS, Parma. Blockchain consensus mechanisms: a primer for supervisors. fintech notes. Internacional Monetary Found, *FinTech Notes* n. 3, 26 jan. 2022. Disponível em: <<https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/25/Blockchain-Consensus-Mechanisms-511769>>. Disponível em: 6 mar. 2024.

BALDUCCINI, Bruno; GIACCHETTA, André; FREITAS, Ciro Torres; VAN HEEMSTEDE, Felipe Tucunduva; MELLO, Marcelo Junqueira de; FAUSTO, Ana Cristina Val; CURTI, Kauê Almeida; MACHADO, Alexandre de Arruda. *Análise da Lei Geral de Proteção de Dados e da Lei de Sigilo Bancário, vis-à-vis as regras de prevenção à lavagem de dinheiro e ao financiamento do terrorismo*. Anbima. Out. 2020. Disponível em: <https://www.anbima.com.br/data/files/EA/44/6B/57/D2EF471095F9BF476B2BA2A8/Memorando-LC-105_LGPD_PLD-FT-Pinheiro-Neto.pdf>. Acesso em: 08 dez. 2023.

BALTAZAR JUNIOR, José Paulo. *Sigilo bancário e privacidade*. Porto Alegre: Livraria do Advogado, 2005, 208 p.

BANCO CENTRAL divulga as diretrizes gerais de uma moeda digital para o Brasil. *Banco Central do Brasil*, 24 maio 2021. Disponível em: <<https://www.bcb.gov.br/detalhenoticia/17398/nota>>. Acesso em: 24 maio 2023.

BANCO CENTRAL DO BRASIL (BCB). Boxe 9: Real digital: uma plataforma para as finanças “tokenizadas”. In: _____. *Relatório de Economia Bancária*. Brasília: Banco Central do Brasil, 2022a, p. 168-175. Disponível em: <<https://www.bcb.gov.br/content/publicacoes/relatorioeconomiabancaria/reb2022p.pdf>>. Acesso em: 13 fev. 2024.

BANCO CENTRAL DO BRASIL (BCB). Comunicado BCB n. 25.306 de 19 de fevereiro de 2014. Esclarece sobre os riscos decorrentes da aquisição das chamadas “moedas virtuais” ou “moedas criptografadas” e da realização de transações com elas. *Diário Oficial da União*, Brasília: 20 fev. 2014. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=comunicado&numero=25306>>. Acesso em: 2 dez. 2023.

BANCO CENTRAL DO BRASIL (BCB). Portaria BCB n. 108.092, de 20 de agosto de 2020. *Diário Oficial da União*, Brasília: 21 ago. 2020. Disponível em: <<https://www.in.gov.br/en/web/dou/-/portaria-n-108.092-de-20-de-agosto-de-2020-273476769>>. Acesso em: 2 dez. 2023.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 105, de 9 de junho de 2021. Aprova o Regulamento do Sistema de Transferência de Reservas (STR), da conta Reservas Bancárias e da Conta de Liquidação no Banco Central do Brasil. *Diário Oficial da União*, Brasília: 10 jun. 2021a. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=105>>. Acesso em: 15 ago. 2023.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 185, de 15 de fevereiro de 2022. Institui o Comitê Executivo de Gestão (CEG) da Edição Especial Laboratório de Inovações Financeiras e Tecnológicas de Desafio do Real Digital (LIFT Challenge Real Digital). *Diário Oficial da União*, Brasília: 17 fev. 2022b. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=185>>. Acesso em: 15 ago. 2023.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 2.025 de 24 de novembro de 1993. Altera e consolida as normas relativas à abertura, manutenção e movimentação de contas de depósitos. *Diário Oficial da União*, Brasília: 25 nov. 1993. Disponível em: <https://www.bcb.gov.br/pre/normativos/res/1993/pdf/res_2025_v5_L.pdf>. Acesso em: 06 jan. 2024.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 273, de 12 de dezembro de 2022. Constitui o Grupo de Trabalho Interdepartamental “GTI Tokenização”, no âmbito do Banco Central do Brasil, para realizar estudo sobre as atividades de registro, custódia, negociação e liquidação de ativos financeiros em infraestruturas de registro distribuído (Distributed Ledger Technologies – DLTs). *Diário Oficial da União*, Brasília: 13 dez. 2023a. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=273>>. Acesso em: 15 ago. 2023.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 315, de 27 de abril de 2023. Institui o Comitê Executivo de Gestão (CEG) do Projeto-Piloto da Plataforma do Real Digital (Piloto RD) e aprova o Regulamento do Piloto RD. *Diário Oficial da União*, Brasília: 28 abr. 2023b. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=315>>. Acesso em: 8 mar. 2024.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 359, de 06 de dezembro de 2023. Altera a Resolução BCB nº 273, de 12 de dezembro de 2022, que constitui o Grupo de Trabalho Interdepartamental “GTI Tokenização”, no âmbito do Banco Central do Brasil, para realizar estudo sobre as atividades de registro, custódia, negociação e liquidação de ativos financeiros em infraestruturas de registro distribuído (Distributed Ledger Technologies – DLTs). *Diário Oficial da União*, Brasília: 06 dez. 2023e. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=359>>. Acesso em: 8 abr. 2024.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 366, de 17 de janeiro de 2024. Divulga o Regulamento do Sistema de Informações Banco Central (Sisbacen). *Diário Oficial da União*, Brasília, 19 jan. 2024. Seção 1, p. 131-132. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=366>>. Acesso em: 11 fev. 2024.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 4.553 de 30 de janeiro de 2017. Estabelece a segmentação do conjunto das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil para fins de aplicação proporcional da regulação prudencial. *Diário Oficial da União*, Brasília, 31 jan. 2017. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50335/Res_4553_v1_O.pdf>. Acesso em: 15 ago. 2023.

BANCO CENTRAL DO BRASIL (BCB). Resolução BCB n. 4.753 de 26 de setembro de 2019. Dispõe sobre a abertura, a manutenção e o encerramento de conta de depósitos. *Diário Oficial da União*, Brasília, 30 set. 2019. Disponível em: <https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50847/Res_4753_v3_L.pdf>. Acesso em: 6 jan. 2024.

BANCO CENTRAL DO BRASIL (BCB). *Voto BCB n. 31, de 14 de fevereiro de 2023*. Assuntos de Política Monetária e assuntos de Administração – Propõe a atualização das Diretrizes do Real Digital, o estabelecimento de diretrizes para o desenvolvimento do piloto da plataforma do Real Digital e a autorização para abertura de canal de comunicação com a sociedade sobre o desenvolvimento do piloto da plataforma do Real Digital e outros temas relacionados ao Real Digital. Brasília: Banco Central do Brasil, 2023c. Disponível em: <https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/voto_bcb_31_2023.pdf>. Acesso em: 8 abr. 2023.

BANCO CENTRAL DO BRASIL (BCB). *Voto BCB n. 73, de 26 de abril de 2023*. Assuntos de Política Monetária, assuntos de Regulação e assuntos de Administração – Propõe a criação do Comitê Executivo de Gestão (CEG) do Projeto-Piloto da Plataforma do Real Digital (Piloto RD) e aprova o regulamento do Piloto RD, conforme

diretrizes estabelecidas no Voto 31/2023-BCB, de 14 de fevereiro de 2023. Brasília: Banco Central do Brasil, 23 abr. 2023d. Disponível em: <https://normativos.bcb.gov.br/Votos/BCB/202373/Voto_do_BC_73_2023.pdf>. Acesso em: 08 mar. 2024.

BANCO CENTRAL DO BRASIL (BCB). *Voto GRC n. 68, de 8 de dezembro de 2022*. Assuntos do Presidente, assuntos de Regulação e assuntos de Organização do Sistema Financeiro e de Resolução – Propõe a constituição de Grupo de Trabalho Interdepartamental (GTI) para realizar estudo sobre tokenização de ativos, compreendendo as atividades de escrituração, registro, depósito, custódia, negociação e liquidação de ativos financeiros em infraestruturas de registro distribuído (Distributed Ledger Technologies – DLTs). Brasília: Banco Central do Brasil, 2022c. Disponível em: <https://normativos.bcb.gov.br/Votos/GRC/202268/Voto_do_GRC_68_2022.pdf>. Acesso em: 24 mar. 2024.

BANCO DA RESERVA FEDERAL DE BOSTON (BRFB). *Project Hamilton Phase 1: executive summary*. Federal Reserve Bank of Boston e Massachusetts Institute of Technology Digital Currency Initiative, 3 fev. 2022. Disponível em: <<https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx>>. Acesso em: 18 out. 2023.

BANK FOR INTERNACIONAL SETTLEMENTS (BIS). *Central bank digital currencies: report submitted by Working Groups chaired by Klaus Löber (European Central Bank) and Aerd Houben (Netherlands Bank)*. *Bank for International Settlements*, mar. 2018a. Disponível em <<https://iepecdg.com.br/wp-content/uploads/2018/03/d174.pdf>>. Acesso em: 5 abr. 2023.

BANK FOR INTERNACIONAL SETTLEMENTS (BIS). Central Bank Digital Currencies: foundational principles and core features. Report n. 1 in a series of collaborations from a group of central banks. *Bank for International Settlements*, 2020. Disponível em: <<https://www.bis.org/publ/othp33.pdf>>. Acesso em: 5 abr. 2023.

BANK FOR INTERNACIONAL SETTLEMENTS (BIS). Committee on payments and market infrastructures. Central Bank Digital Currencies. *Bank for International Settlements*, mar. 2018b. Disponível em: <https://www.bis.org/cpmi/publ/d174.pdf>>. Acesso em: 8 abril 2023.

BANK OF INTERNATIONAL SETTLEMENTS (BIS). Central bank digital currencies for cross-border payments. *Report to the G20*, jul. 2021. Disponível em: <<https://www.bis.org/publ/othp38.htm>>. Acesso em: 12 fev. 2024.

BANK OF INTERNATIONAL SETTLEMENTS (BIS). Project Polaris. Part 1: a handbook for offline payments with CBDC. *BIS Innovation Hub*, maio 2023. Disponível em: <https://www.bis.org/publ/othp64.pdf>. Acesso em: 1º set. 2023.

BARAN, Paul. On distributed communications networks. *White paper*, 1964. Disponível em: <<http://shannon.usu.edu.ru/Papers/Baran/RM3762.pdf>>. Acesso em: 24 mar. 2024.

BARBÉ, Marc Muro. *Deployment of a decentralized application over a permissioned blockchain based on Besu*. Orientador: Prof. José Luiz Muñoz. 2017. 62 f. (Mestrado

em Cybersecurity) – Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona. Universitat Politècnica de Catalunya. Teclecos BCN. 2017. Disponível em: <<https://upcommons.upc.edu/bitstream/handle/2117/361428/Deployment%20of%20a%20decentralized%20application%20over%20a%20permissioned%20blockchain%20based%20on%20Besu.pdf?sequence=2&isAllowed=y>>. Acesso em: 13 fev. 2024.

BARBEITAS, André Terrigno. O sigilo bancário e o resguardo da intimidade e da vida privada. *Boletim Científico* da Escola Superior do Ministério Público da União, Brasília, a. 2, n. 6, p. 37-46, jan./mar. 2003. Disponível em: <<https://escola.mpu.mp.br/publicacoes/boletim-cientifico/edicoes-do-boletim/boletim-cientifico-n-6-janeiro-marco-de-2003/o-sigilo-bancario-e-o-resguardo-da-intimidade-e-da-vida-privada>>. Acesso em: 08 mar. 2024.

BARROSO, Liliane Cordeiro. Central Bank Digital Currency (CBDC): desenho de uma nova moeda. Banco do Nordeste. *Informe ETENE*. a. 7, n. 3, abr. 2022. Disponível em: <https://www.bnb.gov.br/s482-dspace/bitstream/123456789/1170/1/2022_INET_03.pdf>. Acesso em: 12 abr. 2023.

BARROSO, Liliane Cordeiro. Real digital: nova moeda à vista. *Informe ETENE*, a. 8, n. 1, jul. 2023. Disponível em: <https://www.bnb.gov.br/s482-dspace/bitstream/123456789/1803/1/2023_INET_01.pdf>. Acesso em: 14 jan. 2024.

BASHIR, Imran. *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained*. Second Edition. *Packt Publishing Ltd*. 2017. Disponível em: <https://users.cs.fiu.edu/~prabakar/cen5079/Common/textbooks/Mastering_Blockchain_2nd_Edition.pdf>. Acesso em: 5 nov. 2023.

BASTISTELLA, Carla. *Metadados: o que são e como se relacionam à LGPD. Certifiquei*, dez. 2020. Disponível em: <<https://www.certifiquei.com.br/metadados/>>. Acesso em: 7 mar. 2023.

BC ANUNCIA instituições selecionadas para participação no projeto-piloto do real digital. *Banco Central do Brasil*, 26 maio 2023. Disponível em: <<https://www.bcb.gov.br/detalhenoticia/686/noticia>>. Acesso em: 14 fev. 2024.

BC DIVULGA lista de selecionados a participar do Projeto Piloto do Real Digital. Disponível em: <<https://www.bcb.gov.br/detalhenoticia/17897/nota>>. Acesso em: 25 maio 2023.

BC PROMOVE série de webinars “O Real Digital” a partir de julho. *Banco Central do Brasil*, 2021. Disponível em: <<https://www.bcb.gov.br/detalhenoticia/563/noticia>>. Acesso em: 10 jan. 2023.

BECH, Morten Linnemann; GARRAT, Rodney. Central bank cryptocurrencies. *BIS Quarterly Review*, Brasília, Suíça, p. 55-70, set. 2017. Disponível em: <https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf>. Acesso em: 25 nov. 2023.

BENOS, Evangelos; GARRAT, Rodney; GURROLA-PEREZ, Pedro. The economics of distributed ledger technology for securities settlement. *Staff Working Paper*, Bank of England, n. 670, 24 ago. 2017. Disponível em:

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3023779>. Acesso em: 24 mar. 2024.

BERTOLAI, Jefferson Donizeti Pereira; OLIVEIRA, Victor Augusto de Almeida. Criptomoedas e teoria monetária: uma introdução. *Análise Econômica*, Porto Alegre, v. 38, n. 76, p. 197-236, jun. 2020.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*, São Paulo, a. 21, n. 53, p. 191-201, mar. 2020.

Disponível em:

<https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimizac%C3%A7%C3%A3o_e_dado.pdf>. Acesso em: 4 fev. 2024.

BLOCKCHAIN: tecnologias emergentes. *Governo Digital*, 11 ago. 2020. Disponível em: <<https://www.gov.br/governodigital/pt-br/governanca-de-dados/Blockchain>>. Acesso em: 6 out. 2023.

BNDES lança consulta pública em busca de componentes *blockchain* para o BNDESToken. *BNDES*, 6 set. 2018. Disponível em: <<https://www.bndes.gov.br/wps/portal/site/home/imprensa/noticias/conteudo/bndes-lanca-consulta-publica-em-busca-de-componentes-blockchain-para-o-bndestoken>>. Acesso em: 12 fev. 2024.

BOAR, Codruta; WEHRLI, Andreas. Ready, steady, go?: results of the third BIS survey on central bank digital currency. *BIS Papers*, n. 114, jan. 2021. Disponível em: <<https://www.bis.org/publ/bppdf/bispap114.pdf>>. Acesso em: 1º out. 2023.

BOMFIM, Ricardo. Coordenador do Drex diz que solução privacidade deve estar amadurecida, mas não pronta no meio do ano. *Valor Econômico*, 16 abr. 2024.

Disponível em: <

<https://valor.globo.com/financas/criptomoedas/noticia/2024/04/16/coordenador-do-drex-diz-que-solucao-privacidade-deve-estar-amadurecida-mas-no-pronta-no-meio-do-ano.ghtml>>. Acesso em: 24 abr. 2024.

BORDO, Michael; LEVIN, Andrew T. Central bank digital currency and the future of monetary policy. Universidade de Stanford. Hoover Institution. *Economics Working Paper*, n. 17.104, ago. 2017. Disponível em: <https://www.nber.org/system/files/working_papers/w23711/w23711.pdf>. Acesso em: 8 abr. 2023.

BOSSU, Wouter; ITATANI, Masaru; CATALINA, Arthur Rossi; WEENINK, Hans; YOSHINAGA, Akihiro. Legal aspects of Central Bank Digital Currency. *IMF Working Papers*, n. 254, 20 nov. 2020. Disponível em:

<<https://www.imf.org/en/Publications/WP/Issues/2020/11/20/LegalAspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations49827>>. Acesso em: 14 out. 2023.

BRAGUIM, Guilherme Cunha. Pix e incidentes de segurança envolvendo vazamento de dados pessoais: obrigações da Resolução BCB n. 342 de 2023. *Itshow*, nov. 2023.

Disponível em: <<https://itshow.com.br/pix-e-incidentes-de-seguranca-envolvendo->

vazamento-de-dados-pessoais-obrigacoes-da-resolucao-bcb-no-342/>. Acesso em: 12 nov. 2023.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 4.060 de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília, Câmara dos Deputados, 2012. Disponível em: <

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066#:~:text=PL%204060%2F2012%20Inteiro%20teor,Projeto%20de%20Lei&text=Disp%C3%B5e%20sobre%20o%20tratamento%20de%20dados%20pessoais%2C%20e%20d%C3%A1%20outras%20provid%C3%A2ncias.&text=NOVA%20EMENTA%3A%20Disp%C3%B5e%20sobre%20a,23%20de%20abril%20de%202014.&text=Garantia%2C%20prote%C3%A7%C3%A3o%2C%20requisitos%2C%20tratamento,dados%20pessoais%2C%20privacidade%2C%20honra.>> Acesso em: 07 mar. 2024.

BRASIL. Constituição da República Federativa do Brasil de 1988. Texto constitucional de 5 de outubro de 1988 com alterações adotadas por emendas constitucionais de revisão. *Diário Oficial da União*, Brasília, 5 out. 1988a. Disponível em:

<https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 12 nov. 2023.

BRASIL. Decreto n. 678, de 6 de novembro de 1992. Convenção Americana dos Direitos do Homem (Pacto de São José da Costa Rica) de 22 de novembro de 1969. *Diário Oficial da União*, Brasília, 9 nov. 1992. Disponível em:

<<https://www2.camara.leg.br/legin/fed/decret/1992/decreto-678-6-novembro-1992-449028-norma-pe.html>>. Acesso em: 18 jun. 2023.

BRASIL. Decreto n. 97.057 de 10 de novembro de 1988. Altera os Títulos I, II e III do Regulamento Geral para e execução da Lei n. 4.117, de 27 de agosto de 1962. *Diário Oficial da União*, Brasília, 11 nov. 1988b. Disponível em:

<https://www.planalto.gov.br/ccivil_03/decreto/1980-1989/D97057.htm>. Acesso em: 12 nov. 2023.

BRASIL. Decreto n.10.411 de 30 de junho de 2020. Regulamenta a análise de impacto regulatório, de que tratam o art. 5º da Lei n. 13.874, de 20 de setembro de 2019, e o art. 6º da Lei n. 13.848, de 25 de junho de 2019. *Diário Oficial da União*, Brasília, 1º jul. 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10411.htm>. Acesso em: 12 fev. 2024.

BRASIL. Lei Complementar n. 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. *Diário Oficial da União*, Brasília, 11 jan. 2001. Disponível em:

<https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em: 12 nov. 2023.

BRASIL. Lei Complementar n. 70, de 30 de dezembro de 1991. Institui contribuição para financiamento da Seguridade Social, eleva a alíquota da contribuição social sobre o lucro das instituições financeiras e dá outras providências. *Diário Oficial da União*, Brasília, 31 dez. 1991. Disponível em:

<http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp70.htm>. Acesso em: em: 08 mar. 2024.

BRASIL. Lei n. 10.406 de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*, Brasília, 11 jan. 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/10406compilada.htm>. Acesso em: 15 nov. 2023.

BRASIL. Lei n. 10.701, de 9 de julho de 2003. Altera e acrescenta dispositivos à Lei no 9.613, de 3 de março de 1998, que dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – Coaf, e dá outras providências. *Diário Oficial da União*, Brasília, 9 jul. 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.701.htm>. Acesso em: 1º set. 2023.

BRASIL. Lei n. 12.414 de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. *Diário Oficial da União*, Brasília, 10 jun. 2011a. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/12414.htm>. Acesso em: 1º set. 2023.

BRASIL. Lei n. 12.527 de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União*, Brasília, 18 nov. 2011b. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/12527.htm>. Acesso em: 8 dez. 2023.

BRASIL. Lei n. 12.865 de 9 de outubro de 2013. Autoriza o pagamento de subvenção econômica aos produtores da safra 2011/2012 de cana-de-açúcar e de etanol que especifica e o financiamento da renovação e implantação de canaviais com equalização da taxa de juros; dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB); [...]. *Diário Oficial da União*, Brasília, 10 out. 2013. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/12865.htm>. Acesso em 28 nov. 2023.

BRASIL. Lei n. 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, 24 abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm>. Acesso em: 8 dez. 2023.

BRASIL. Lei n. 13.260 de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n. 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. *Diário Oficial da União*, Brasília, 17 mar. 2016. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/13260.htm>. Acesso em: 3 jan. 2023.

BRASIL. Lei n. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, 15 ago. 2018. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 18 jun. 2023.

BRASIL. Lei n. 13.964 de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. *Diário Oficial da União*, Brasília, 24 dez. 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>. Acesso em: 14 fev. 2024.

BRASIL. Lei n. 14.534, de 11 de janeiro de 2023. Altera as Leis n. 7.116, de 29 de agosto de 1983, 9.454, de 7 de abril de 1997, 13.444, de 11 de maio de 2017, e 13.460, de 26 de junho de 2017, para adotar número único para os documentos que especifica e para estabelecer o Cadastro de Pessoas Físicas (CPF) como número suficiente para identificação do cidadão nos bancos de dados de serviços públicos. *Diário Oficial da União*, Brasília, 11 jan. 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14534.htm>. Acesso em: 08 mar. 2024.

BRASIL. Lei n. 4.595 de 31 de dezembro de 1964. Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, cria o Conselho Monetário Nacional e dá outras providências. *Diário Oficial da União*, Brasília, 31 dez. 1964. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l4595.htm>. Acesso em: 15 nov. 2023.

BRASIL. Lei n. 5.172, de 25 de outubro de 1966. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. *Diário Oficial da União*, Brasília, 27 out. 1966. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l5172.htm>. Acesso em: 08 mar. 2024.

BRASIL. Lei n. 8.078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*, Brasília, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 15 out. 2023.

BRASIL. Lei n. 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. *Diário Oficial da União*, Brasília, 25 jul. 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm#:~:text=Constitui%20crime%20realizar%20intercepta%C3%A7%C3%A3o%20de,a%20quatro%20anos%2C%20e%20multa>. Acesso em: 8 dez. 2023.

BRASIL. Lei n. 9.472 de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional n. 8, de 1995. *Diário Oficial da União*, Brasília, 17 jul. 1997. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9472.htm>. Acesso em: 8 dez. 2023.

BRASIL. Lei n. 9.613, de 6 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. *Diário Oficial da União*, Brasília, 4 mar. 1998. Disponível em:

<https://www.planalto.gov.br/ccivil_03/leis/l9613compilado.htm>. Acesso em: 07 mar. 2024.

BRASIL. Superior Tribunal de Justiça (STJ). Penal. Processual penal. Recurso ordinário em *habeas corpus*. Tráfico de drogas. Nulidade da prova. Ausência de autorização judicial para a perícia no celular. Constrangimento ilegal evidenciado. Recurso em *Habeas Corpus* (RHC) n. 51.531/RO (2014/0232367-7). Min. Rel. Nefi Cordeiro. *Diário de Justiça eletrônico*, Brasília, 9 maio 2016. Disponível em: <<https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=RHC%2051531>>. Acesso em: 9 dez. 2023.

BRASIL. Supremo Tribunal Federal (STF). 1. Decisão judicial: alegação de omissão de análise de teses relevantes da defesa: recurso extraordinário: descabimento. 2. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acordo não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. 3. Decreto de busca e apreensão: validade. 4. Proteção constitucional ao sigilo nas comunicações de dados – art. 5º XVII da CF: ausência de violação no caso. 5. Prescrição pela pena concretizada. Recurso Extraordinário n. 418.416/SC, Min. Relator Sepúlveda Pertence. *Diário de Justiça Eletrônico*, Brasília, 19 dez. 2006. Disponível em: <<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>>. Acesso em: 4 fev. 2024.

BRASIL. Supremo Tribunal Federal (STF). Nulidades: (1) Inépcia da denúncia. (2) Ilícitude da prova produzida durante o inquérito policial. Violação de registros telefônicos do correú, executor do crime, sem autorização judicial; (3) Ilícitude da prova das interceptações telefônicas de conversas dos acusados com advogados, porquanto essas gravações ofenderiam o disposto no art. 7º, II, da Lei 8.906/96, que garante o sigilo dessas conversas. Vícios não caracterizados. Ordem denegada. *Habeas Corpus* n. 91.867/PA. Rel. Min. Gilmar Mendes. *Diário de Justiça eletrônico*, Brasília, 24 abr. 2012. Disponível em: <<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328>>. Acesso em: 9 dez. 2023.

BROWN, Barry. Studying the internet experience. *HP Laboratories Technical Report*, mar. 2001. Disponível em: <<https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf>>. Acesso em: 4 fev. 2024.

BURGOS, Aldenio. BATÁVIA, Bruno. Currency in the digital era. *Banco Central do Brasil*, Rio de Janeiro, 2018. Disponível em: <<https://www.bcb.gov.br/htms/public/inovtec/Currency-in-the-Digital-Era.pdf>>. Acesso em: 12 fev. 2024.

BUSCA de normas. *Banco Central do Brasil*. 23 mar. 2024. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/buscanormas>>. Acesso em: 12 fev. 2024.

CARTA dos Direitos Fundamentais da União Europeia (CDFUE). *Jornal Oficial das Comunidades Europeias*, n. 364/01, 2000. Disponível em: <https://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 4 fev. 2024.

CARVALHO, Carlos Eduardo; OLIVEIRA, Guiliano Contendo de; MONTEIRO, Marcelo Balloti. *O Banco Central do Brasil: institucionalidade, relações com o Estado e com a sociedade civil, autonomia e controle democrático*. Instituto de Pesquisa Rio de Janeiro: Econômica Aplicada (IPEA) Série: Texto para discussão, n. 1.518, dez. 2010, p. 73. Disponível em:

<https://repositorio.ipea.gov.br/bitstream/11058/1563/1/TD_1518.pdf>. Acesso em: 8 dez. 2023.

CARVALHO, Luis Gustavo Grandinetti Castanho de. Direito à privacidade. *Revista da EMERJ*, Rio de Janeiro. v. 1, n. 2, p. 51-76, 1998. Disponível em:

<https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista02/revista02_51.pdf>. Acesso em: 8 dez. 2023

CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999. v.1.

CAVOUKIAN, Ann. *Privacy by design: the 7 foundational principles: information and Privacy Commissioner of Ontario*. Privacy by Design (PbD). Canadá, 2011. Disponível em: <<https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>>. Acesso em: 24 abr. 2024.

CHAUM, David. Blind signatures for untraceable payments. *Advances in Cryptology, proceedings of Crypto, Springer*, n. 82, p. 199-203, 1998. Disponível em: <<https://scweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF>>. Acesso em: 8 abr. 2023.

CLARKE, Roger. Internet privacy concerns confirm the case for intervention. *Communications of the ACM. ACM Digital Library*, 1999, p. 60-67. Disponível em <<https://dl.acm.org/doi/abs/10.1145/293411.293475>>. Acesso em: 17 jun. 2023.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Resolução CVM n. 50, de 31 de agosto de 2021. Dispõe sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa – PLD/FTP no âmbito do mercado de valores mobiliários e revoga a Instrução CVM n. 617, de 5 de dezembro de 2019 e a Nota Explicativa à Instrução CVM n. 617, de 5 de dezembro de 2019. *Diário Oficial da União*, Brasília, 2 set. 2021. Disponível em: <<https://conteudo.cvm.gov.br/legislacao/resolucoes/resol050.html>>. Acesso em: 6 jan. 2023.

CONSELHO MONETÁRIO NACIONAL (CMN). Resolução CMN n. 4.893 de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. *Diário Oficial da União*, Brasília, 1º mar. 2021. Seção 1, p. 82. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.893-de-26-de-fevereiro-de-2021-305689973>>. Acesso em; 15 nov. 2023.

CONSELHO MONETÁRIO NACIONAL (CMN). Resolução CMN n. 5.091 de 30 de junho de 2023. Fixa a meta para a inflação e seu respectivo intervalo de tolerância para o ano de 2026. *Diário Oficial da União*, Brasília, 30 jun. 2023. Seção 1, p. 1. Disponível em:

<<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5091>>. Acesso em: 15 out. 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Sistema Nacional de Investigação Patrimonial e Recuperação de Ativos* (Sniper). Disponível em: <<https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/sniper/>>. Acesso em: 12 abril 2023.

CORRÊA, Caroline Alves Martins Pires; LEITE, Jessica Silveira. Análise de riscos de comprometimento da Privacidade, dos dados e do sigilo bancário do Usuário pessoa natural do real digital (Drex). In: NEVES, Rubia Carneiro (Org.). *Novas fronteiras do sistema financeiro nacional*. Belo Horizonte: Expert, 2023. v. 2., p. 209-242. Disponível em: <<https://experteditora.com.br/wp-content/uploads/2023/12/NOVAS-FRONTIERAS-DO-SISTEMA-FINANCEIRO-NACIONAL-v.-2-1.pdf>>. Acesso em: 12 fev. 2024.

CORRÊA, Caroline Alves Martins Pires; PIMENTEL, Guilherme Barroso; SOUZA, Larissa Lima de. *Um exercício de avaliação da dependência do real digital (Drex) em relação ao SWIFT para permitir a efetivação de pagamentos transfronteiriços*. v.2023. v. 2, p. 181-206. Disponível em: <<https://experteditora.com.br/wp-content/uploads/2023/12/NOVAS-FRONTIERAS-DO-SISTEMA-FINANCEIRO-NACIONAL-v.-2-1.pdf>>. Acesso em: 12 fev. 2024.

CRUVINEL, Aline; PRESTES, Jeff. *Caminhos para um Real Digital on-chain compatível com o direito à privacidade e proteção de dados pessoais desde a concepção*. 7 fev. 2023. Disponível em: <https://www.bcb.gov.br/conteudo/eventos/Documents/moedas_digitais/tokenizacao/WorK-TOK-Mimeo-TECH_3A_A_Caminhos_para_um_Real_Digital_on-chain_compativel_com_o_direito_a_privacidade_desde_a_concepcao.pdf>. Acesso em: 7 dez. 2023.

DARBHA, Sriram; ARORA, Rakesh. Privacy in CBDC Technology. *Staff Analytical Note*. Bank of Canada, jun. 2020. Disponível em: <<https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/>>. Acesso em: 17 abr. 2023.

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

DE LEON, Daniel Conte; STALICK, Antonius Q.; JILLEPALLI, Ananth A.; HANEY, Michael A.; SHELDON Frederick T. Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and Entrepreneurship*, Bingley, v. 11, n. 3, p. 286-300, Dec. 2017.

DECEW, Judith Wagner. *In pursuit of privacy: law, ethics and the rise of technology*. Ithaca, Nova York: Cornell University Press, 1997, 199 p.

DEFI: Como as finanças descentralizadas podem transformar o mercado. *Accenture*, 2023. Disponível em: <<https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-179/accenture-decentralized-finance.pdf>>. Acesso em: 1º out. 2023.

DINIZ, Natália. *Análise das demonstrações financeiras*. Rio de Janeiro: SESES, 2015. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/4277771/mod_resource/content/1/Livro_An%C3%A1lise%20dos%20Relat%C3%B3rios%20Financeiros.pdf>. Acesso em: 4 fev. 2024.

DOCUMENTAÇÃO e arquivos de configuração para participação no Piloto do Real Digital. *Bacen/pilotord-kit-onboarding*. 2023. Disponível em: <<https://github.com/bacen/pilotord-kit-onboarding>>. Acesso em: 12 mar. 2023.

DOERR, Sebastian; FROST, Jon; GAMBACORTA, Vatsala Shreeti. Big techs in finance. *BIS Working Papers*, out. 2023. Disponível em: <<https://www.bis.org/publ/work1129.pdf>>. Acesso em: 6 nov. 2023.

DONEDA, Danilo Cesar Maganhoto. *A proteção de dados em tempo de coronavírus: a LGPD será um elemento fundamental para a reestruturação que advirá após a crise*. 25 mar. 2020a. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020>>. Acesso em: 10 dez. 2023.

DONEDA, Danilo Cesar Maganhoto. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico. *Journal of Law*, v. 12, n. 2, p. 91-108, 2011. Disponível em: <<https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315>>. Acesso em: 8 dez. 2023.

DONEDA, Danilo Cesar Maganhoto. *Da privacidade à proteção de dados pessoais: elementos da formação da lei geral de proteção de dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020b.

DONEDA, Danilo Cesar Maganhoto; MENDES, Laura Schertel. *Data protection in Brazil: developments and current challenges*. out. 2014, p. 3-20. Disponível em: <https://www.researchgate.net/publication/301079248_Data_Protection_in_Brazil_New_Developments_and_Current_Challenges>. Acesso em: 9 dez. 2023.

DONOHUE, Brian. *Hash: o que são e como funcionam*. Disponível em: <<https://www.kaspersky.com.br/blog/hash-o-que-sao-e-como-funcionam/2773/>>. Acesso em: 10 out. 2023.

DUDENA, Regis. Regulação do sistema financeiro nacional: entre a estabilidade, o fomento à concorrência e a proteção aos dados pessoais? In: NEVES, Rubia Carneiro (Org.). *Novas fronteiras do sistema financeiro nacional*. Belo Horizonte: Expert, 2022. v. 1, p. 23-58. Disponível em: <<https://pos.direito.ufmg.br/downloads/Novas-fronteiras-do-sistema-financeiro-nacional.pdf>>. Acesso em: 13 nov. 2023.

E-HKD: a policy and design perspective. 2023. Disponível em: <https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/e-HKD_A_Policy_and_Design_Perspective.pdf>. Acesso em: 16 mar. 2024.

EUROPEAN CENTRAL BANK (ECB). Eurosystem. *Bank of Japan*. Stella – joint research project of the European Central Bank and the Bank of Japan. Balancing confidentiality and auditability in a distributed ledger environment. *European Central Bank and the Bank of Japan*. Fev. 2020a. Disponível em:

<https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf>. Acesso em 13 abril 2023.

EUROPEAN CENTRAL BANK (ECB). Eurosystem. *Report on a digital euro*. Outubro 2020b. Disponível em: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf. Acesso em 13 abril 2023.

EUROPEAN COMMISSION. Central Bank Digital Currencies and a Euro for the Future. *EU Blockchain Observatory and Forum*, 2020. Disponível em: <<https://www.eublockchainforum.eu/sites/default/files/reports/CBDC%20Report%20Final.pdf>>. Acesso em: 16 mar. 2024.

EUROPEAN DATA PROTECTION BOARD (EDPB). Digital euro: ensuring the highest data protection and privacy standards. *European Data Protection Board*, out. 2023a. Disponível em: <https://edpb.europa.eu/news/news/2023/digital-euro-ensuring-highest-data-protection-and-privacy-standards_en>. Acesso em: 10 dez. 2023.

EUROPEAN DATA PROTECTION BOARD (EDPB). EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro. *European Data Protection Board*, 2021. Disponível em: <https://edpb.europa.eu/system/files/2021-07/edpb_letter_out_2021_0111-digitaleuro-toecb_en_1.pdf>. Acesso em: 11 fev. 2024.

EUROPEAN DATA PROTECTION BOARD (EDPB). Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro. *European Data Protection Board*, out. 2023b. Disponível em: <https://edpb.europa.eu/system/files/2023-10/edpb_edps_jointopinion_022023_digitaleuro_en.pdf>. Acesso em: 10 dez. 2023.

EYBLOCKCHAIN. Starlight. Ernest Young. GitHub. 2024. Disponível em: <<https://github.com/EYBlockchain/starlight>>. Acesso em: 27 abr. 2024.

FAHIM, Shahriar; RAHMAN, SM Katibur; MAHMOOD, Sharfuddin. Blockchain: a comparative study of consensus algorithms PoW, PoS, PoA, PoV. *International Journal of Mathematical Sciences and Computing (IJMSC)*, ago. 2023. Disponível em: <<https://www.mecs-press.org/ijmsc/ijmsc-v9-n3/v9n3-4.html>>. Acesso em: 13 fev. 2024.

FANTI, Giulia; POCHER, Nadia. *Privacy in cross-border digital currency: a transatlantic approach*. Atlantic Council – Geoeconomics Center. Frankfurt Forum on US – European Geoeconomics. Disponível em: <https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf>. Acesso em: 13 fev. 2024.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). Termo de consentimento para tratamento de dados pessoais. *Febraban Tech*, jan. 2023. Disponível em: <https://pefmbddiag.blob.core.windows.net/cdn-pi/termos_consentimento.pdf>. Acesso em: 6 jan. 2023.

FÓRUM Drex debateu desenvolvimento da moeda digital criado pelo BC. Segunda Plenária do Fórum Drex, realizada no dia 27 de setembro de 2023. *bcb.gov*, 5 out. 2023.

Disponível em: <<https://www.bcb.gov.br/detalhenoticia/726/noticia>> Acesso em: 7 mar. 2024.

FREITAS, Cinthia Obladen de Almeida; MAFFINI, Maylin. A proteção dos dados pessoais no crédito bancário e a Lei Geral de Proteção de Dados frente ao cadastro positivo. *Revista Jurídica Cesumar*, v. 20, n. 1, p. 29-42, abr. 2020. Disponível em: <<https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/7989/6312>>. Acesso em: 8 fev. 2024.

GENTRY, Craig. *A fully Homomorphic encryption scheme*. Doutorado – Faculdade de Ciência da Computação. Universidade de Stanford. Set. 2009. Disponível em: <<https://crypto.stanford.edu/craig/craig-thesis.pdf>>. Acesso em: 27 abr. 2024.

GOYANNA, Eduardo Vasconcelos. *Dado pessoal e dado anonimizado e a regulamentação no Brasil e na França*. Orientadora: Professora Doutora Laura Schertel Mendes. 2021, 82 f. Monografia (Bacharel em Direito) – Faculdade de Direito. Universidade de Brasília, Brasília, 2021. Disponível em: <https://bdm.unb.br/bitstream/10483/29647/1/2021_EduardoVasconcelosGoyanna_tcc.pdf>. Acesso em: 24 mar. 2024.

GUIA de requisitos mínimos para a privacidade e segurança da informação para aplicações web. *Programa de Privacidade e Segurança da Informação (PPSI)*. Brasília, 2022. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_requisitos_minimos_web.pdf>. Acesso em: 24 abr. 2024.

GUSSON, Cassio. *Câmara dos Deputados debate modernização de cartórios com novas tecnologias como blockchain*. 19 out. 2023. Disponível em: <<https://br.cointelegraph.com/news/chamber-of-deputies-debates-modernization-of-registry-offices-with-new-technologies-such-as-blockchain>>. Acesso em: 6 mar. 2024

HAFNER, Katie. And if you liked the movie, a Netflix contest may reward you handsomely. *The New York Times*, 2 out. 2016. Disponível em: <<https://www.nytimes.com/2006/10/02/technology/02netflix.html>>. Acesso em: 10 dez. 2023.

HEINONLINE. Disponível em: <<https://heinonline.org/HOL/Welcome?>> Acesso em: 10 out. 2023.

HUNTER, Larry. Public image. In: JOHNSON, Deborah G.; NISSENBAUM, Helen (Ed.). *Computers, ethics and social values*. New Jersey: Prentice Hall, 1995, p. 293-299.

INNES, Julie. *Privacy, intimacy and isolation*. Oxford: Oxford University Press, 1992.

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). Global Stablecoin Initiatives. Public Report. *Focus Group Technical Report*. OR01/2020. mar. 2020. Disponível em: <<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf>>. Acesso em: 15 out. 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). *Distributed Ledger Technologies (DLT) and financial inclusion*. ITU-T Focus GRoup on digital financial

services. *Focus Group Technical Report*, 3 mar. 2017. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-on-DLT-and-Financial-Inclusion.pdf>. Acesso em: 10 out. 2023.

KAUR, Mnapreet; KHAN, Mohammad Zubair; GUPTA, Shikha; NOORWALI, Abdulfatah; CHAKRABORTY, Chinmay; PANI, Subhendu Kumar. *MBCP: Performance analysis of large scale mainstream blockchain consensus protocols. IEE Explore*. Jun. 2021. Disponível em: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9444429>>. Acesso em: 7 ago. 2023

KHATRIL, Arun; KAUSHIK, Anjali. *Systematic literature review on Blockchain adoption in banking*. Journal of Economics, Finance and Accounting, v. 8, p. 126 a 146, 2 set. 2021. Disponível em: <<https://dergipark.org.tr/en/download/article-file/2005884>>. Acesso em: 15 out. 2023.

KIVIAT, Trevor. *Beyond bitcoin: issues in regulating blockchain transactions. Duke Law Journal*, Duke, v. 65, p. 569-608, 2015.

KOHLI, Varun; CHAKRAVARTY, Sombudda; CHAMOLA, Vinay; SANGWAN, Kuldip Singh; ZEADALLY, Sherali. *An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions*. Cornell University, 20 fev. 2022. Disponível em: <<https://arxiv.org/abs/2203.03717>>. Acesso em: 7 nov. 2023.

KOKOLAKIS, Spyros. Privacy attitudes and privacy behaviour: a re-view of current research on the privacy paradox phenomenon. *Computers & Security*, jul. 2015. Disponível em: <https://www.researchgate.net/publication/280244291_Privacy_attitudes_and_privacy_behaviour_A_review_of_current_research_on_the_privacy_paradox_phenomenon/link/5a1bdb5a4585155c26ae08e2/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6IjB1Ym91dG8iLCJwYXZlIjoicHVibGljYXRpb24ifX0>. Acesso em: 11 fev. 2024.

KOSINSK, Daniel S. As Central Bank Digital Currencies como instrumentos de superação do subdesenvolvimento: o caso da Nigéria. *Sul Global*, 2022, p. 78-102. Disponível em: <<https://revistas.ufrj.br/index.php/sg/article/view/50219>>. Acesso em: 11 fev. 2024.

KUNT, Asli Demirgüç-Kunt. KLAPPER, Leora. SINGER, Dorothe. ANSAR, Saniya. HESS, Jake. *The Global Findex Database 2017*. Measuring Financial Inclusion and the Fintech Revolution. Word Bank Group. 2017. Disponível em: <<https://microdata.worldbank.org/index.php/catalog/3270/download/44216>>. Acesso em: 05 mar. 2024.

KWH: o que é kilowatts e como converter kW para kWh. *Portal Solar*. Disponível em: <<https://www.portalsolar.com.br/kw-e-kwh-qual-e-a-diferenca>>. Acesso em: 11 jan. 2024.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LUPIN). *Open Banking & LGPD: entraves e eficiências*. 2020. Disponível em: <<https://lapin.org.br/wp->

content/uploads/2020/11/Relatorio-Open-Banking-LGPD_LAPIN.pdf>. Acesso em: 7 jan. 2024.

LAZARO, Christophe. LE MÉTAYER, Daniel. *Control over personal data: true remedy or fairy tale?* *SCRIPT-ed*. v. 12, n. 1, p. 3-34, jun. 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689223>. Acesso em: 05 mar. 2024.

LGPD está fora da realidade de 80% das empresas no Brasil, diz estudo. 4 jan. 2023. Disponível em: <<https://febrabantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo>>. Acesso em: 13 fev. 2024.

LIBRA ASSOCIATION. Cover letter. *White paper*, 2.0. abr., 2020, p. 1-29. Disponível em: <<https://www.accc.gov.au/system/files/public-registers/documents/54.%20Libra%20Whitepaper%20v2.0%2C%20April%202020.pdf>>. Acesso em: 1º out. 2023.

LIEBER, Ron. American Express Kept a (very) watchful eye on charges. *New York Times*, 30 jan. 2009. Disponível em: <<https://www.nytimes.com/2009/01/31/your-money/credit-and-debit-cards/31money.html>>. Acesso em: 11 fev. 2024.

LIFT CHALLENGE. *Real Digital*. 2023. Disponível em <<https://liftchallenge.bcb.gov.br/site/liftchallenge>>. Acesso em: 11 fev. 2024.

LUCAS, Ana; PEDRON, Cristine; NAVES, Fernando; CAMACHO, José; HENRIQUES, Luis Vaz. *Conceitos de tecnologias de informação*. Lisboa: Universidade de Lisboa: Instituto Superior de Economia e Gestão (ISEG). 2008. Disponível em: <<https://www.iseg.ulisboa.pt/aquila/getFile.do?fileId=8204&method=getFile>>. Acesso em: 11 fev. 2024.

MAIA, Alexandre Forte. Processo regulatório do Sistema Financeiro Nacional: etapas de edição de normas a cargo do Banco Central do Brasil e do Conselho Monetário Nacional. In: NEVES, Rubia Carneiro (Org.). *Novas fronteiras do sistema financeiro nacional*. Belo Horizonte: Expert, 2023. v. 2, p. 22-50. Disponível em: <<https://experteditora.com.br/wp-content/uploads/2023/12/NOVAS-FRONTIEIRAS-DO-SISTEMA-FINANCEIRO-NACIONAL-v.-2-1.pdf>>. Acesso em: 24 mar. 2024.

MATOS, Gino. CBDC terá como desafio a privacidade do usuário. *Mercado Bitcoin*, 3 maio 2022. Disponível em: <<https://www.bloomberglinea.com.br/2022/05/03/cdbc-tera-como-desafio-a-privacidade-do-usuario/>>. Acesso em: 5 abr. 2023.

MAY, Timothy. *The crypto anarchist manifesto*. 1992. Disponível em: <<https://libinst.cz/wp-content/uploads/2020/08/havel.pdf>>. Acesso em: 24 abr. 2024.

MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito. Universidade de Brasília, Brasília, 2008. Disponível em: <<http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>>. Acesso em: 17 abr. 2023.

MELICHOVÁ, Silvia. *Cyberpunk as Subculture*. Universidade de Masaryk. Monografia (Graduação) - Faculdade de Artes. 2006. Disponível em: <https://is.muni.cz/th/z2tqx/FINAL_THESIS.pdf>. Acesso em: 24 abr. 2024.

MICROSOFT privacy statement, mar. 2024. Disponível em: <<https://privacy.microsoft.com/en-us/privacystatement>>. Acesso em: 14 fev. 2024.

MINHA Biblioteca. Contrate a sua nova biblioteca jurídica: mais de 3 mil livros de Direito para aprimorar a sua experiência de leitura e consulta. Disponível em: <https://materiais.minhabiblioteca.com.br/biblioteca-juridica?utm_source=google&utm_medium=cpc&utm_campaign=microessentials&utm_content=marketing_performance&gad_source=1&gclid=Cj0KCQiA5rGuBhCnARIsAN11vgQrH9KTRihIpS8StF8EJBIMPHjOdqRyejNnI9rM5BPPOcxbGLJdp3IaAqD2EALw_wcB>. Acesso em: 2 out. 2023.

MIRCHANDANI, Anisha. The GDPR-Blockchain paradox: exempting permissioned blockchains from the GDPR. *Law Journal*, a. 29 v. 29, n. 4, art. 5, 2019. Disponível em: <<https://ir.lawnet.fordham.edu/iplj/vol29/iss4/5>>. Acesso em: 12 out. 2023.

MOSQUERA, Juan. Arm's Length Principle in Transfer Pricing. *Ariantass*, 2020. Disponível em: <<https://www.arintass.com/arms-length-principle-in-transfer-pricing/#:~:text=The%20Arm's%20Length%20Principle%20was,profits%20to%20low%20tax%20jurisdictions>>. Acesso em: 13 jan. 2024.

MOREIRA, Arthur Salles de Paula. DELGADO, Camila Campos Baumgratz. SANTOS, Gabriel Gonçalves. Repensando a tecnologia blockchain: por que nem tudo o que você leu até hoje era verdade? In: _____ (Org.). Leonardo Parentoni, Marcelo de Oliveira Milagres, Jeroen van de Graaf. Belo Horizonte: Editora Expert, 2021, v. 3, p. 23-60. Disponível em: <<https://pos.direito.ufmg.br/downloads/Direito-tecnologia-e-Inovacao-1.pdf>>. Acesso em: 24 abr. 2024.

NAKAMOTO, Satoshi. *Bitcoin: A peer to peer eletronic cash system*. 31 out. 2008. Disponível em: <https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf>. Acesso em: 15 out. 2023.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and fallacies of “personally identifiable information”. *Communications of the ACM*, Nova York, v. 53, n. 6, jun. 2010. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/1743546.1743558>>. Acesso em: 4 fev. 2024.

NEVES, Rubia Carneiro. SILVA, Leila Bitencourt Reis da. COSTA, Daniel Rodrigues. *Regulação das contas de depósito & Inovações da Agenda BC#*. São Paulo: Instituto Propague, 2021. Disponível em: <<https://institutopropague.org/pagamentos/ebook-regulacao-das-contas-de-deposito-e-inovacoes-da-agenda-bc/>>. Acesso em 11 fev. 2024.

NEVES, Rubia Carneiro; DINIZ, Davi Monteiro. RAMOS, Yasmin Oliveira Melgaço. A moeda digital de banco central como instrumento para se manter a exclusividade da União na emissão e no controle da moeda oficial. In: _____ (Org.). *Novas fronteiras do sistema financeiro nacional*. Belo Horizonte: Editora Expert, 2023, v. 1, p. 85-127. Disponível em: <<https://experteditora.com.br/wp-content/uploads/2023/12/NOVAS->

FRONTEIRAS-DO-SISTEMA-FINANCEIRO-NACIONAL-v.-2-1.pdf>. Acesso em 12 fev. 2024.

NEVES, Rubia Carneiro; DINIZ, Davi Monteiro; SILVA, Leila Bitencourt Reis da. A atuação concorrente da instituição de pagamento com os bancos comerciais: uma opção regulatória associada a novas tecnologias e indícios de benefícios à população brasileira. In: _____ (Org.). *Novas fronteiras do sistema financeiro nacional*. Belo Horizonte: Editora Expert, 2022. v. 1, p. 189-2016. Disponível em: <<https://pos.direito.ufmg.br/downloads/Novas-fronteiras-do-sistema-financeiro-nacional.pdf>>. Acesso em: 13 nov. 2023.

NORBERG, Patricia A.; HORNE, Dan; HORNE, David. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, v. 41, n. 1, p. 100-126, mar. 2007. Disponível em: <https://www.researchgate.net/publication/229897938_The_Privacy_Paradox_Personal_Information_Disclosure_Intentions_Versus_Behaviors>. Acesso em 11 fev. 2024.

O QUE SÃO bases de dados centralizadas, descentralizadas e distribuídas? *Foxbit*, 19 dez. 2019. Disponível em: <<https://foxbit.com.br/blog/diferenca-entre-as-bases-de-dados-blockchain/>>. Acesso em: 24 mar. 2024.

OECD transfer pricing guidelines for multinational enterprises and tax administrations. 20 jan. OECD, 2022. Disponível em: <<https://www.oecd.org/tax/transfer-pricing/oecd-transfer-pricing-guidelines-for-multinational-enterprises-and-tax-administrations-20769717.htm>>. Acesso em: 18 jun. 2023.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 1.701-1.778, 2010. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006#>. Acesso em: 18 jun. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Declaração Universal dos Direitos Humanos*: adotada e proclamada pela Assembleia Geral das Nações Unidas (Resolução 217 A III). Roma, dez. 1948. Disponível em: <https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/por.pdf>. Acesso em: 18 jun. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Convenção Europeia dos Direitos do Homem*. Roma, nov. 1950. Disponível em: <<https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=536&lID=4>>. Acesso em: 18 jun. 2023.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). *Declaração Americana dos Direitos e Deveres do Homem*. Aprovada na Nona Conferência Internacional Americana. Bogotá, 1948. Disponível em: <https://www.cidh.oas.org/basicos/portugues/b.declaracao_americana.htm>. Acesso em 18 jun. 2023.

OS IMPACTOS de Central Bank Digital Currencies no mercado mundial. *Accenture*, 2022. Disponível em: <<https://www.accenture.com/content/dam/accenture/final/capabilities/strategy-and->

consulting/strategy/document/Accenture-Os-impactos-De-CBDC-No-Mercado-Mundial.pdf>. Acesso em: 10 dez. 2023.

PARENTONI, Leonardo. O direito ao esquecimento (*right to oblivion*). In: DE LUCCA, Newton. SIMAO FILHO, Adalberto. LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & internet III: marco civil da internet* (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. t. 1: Disponível em: <https://www.researchgate.net/publication/299821661_O_Direito_ao_Esquecimento_Right_to_Oblivion>. Acesso em: 4 fev. 2024.

PESQUISA TecBan/Datafolha aponta: brasileiro ainda conhece o Drex. TechBan. Nov. 2023. Disponível em: <<https://www.tecban.com.br/release/pesquisa-tecban-datafolha-aponta-brasileiro-ainda-nao-conhece-o-drex>>. Acesso em: 4 fev. 2024.

PILOTO Drex. *Banco Central do Brasil*. Disponível em: <<https://bcb.gov.br/estabilidadefinanceira/piloto-drex>>. Acesso em: 13 fev. 2024.

PIMENTA, Ricardo. *Big data e controle da informação na era digital: tecnogênese de uma memória a serviço do mercado e do Estado. Tendências da Pesquisa Brasileira em Ciência da Informação. Brapci*, v. 6, n.2, dez. 2013. Disponível em: <<https://brapci.inf.br/index.php/res/download/152159>>. Acesso em: 18 abr. 2023.

PINHEIRO, Patrícia Peck. OLIVEIRA NETO, Antonio Alves de; ARANTES, Gabriel. A aplicação de sanções administrativas e seu impacto no setor financeiro. *Febraban Tech*, 23 mar. 2023. Disponível em: <<https://febrabantech.febraban.org.br/especialista/patricia-peck-pinheiro/a-aplicacao-de-sancoes-administrativas-e-seu-impacto-no-setor-financeiro>>. Acesso em: 16 mar. 2024.

PLATAFORMA que usa blockchain para autorizações no sistema financeiro entra em funcionamento. *Banco Central do Brasil*, 01 abr. 2020. Disponível em: <<https://www.bcb.gov.br/detalhenoticia/431/noticia>>. Acesso em: 15 out. 2023.

POLÍTICA de cookies: entenda a importância dessa política para a adequação das plataformas digitais. *BL Consultoria*, 17 set. 2021. Disponível em: <<https://blconsultoriadigital.com.br/politica-de-cookies/>>. Acesso em: 4 fev. 2024.

POLÍTICA de privacidade de dados. *Unicred*. Disponível em: <<https://unicred.com.br/politica-de-privacidade>>. Acesso em: 4 fev. 2024a.

POLÍTICA de privacidade. *Banco BV*. Disponível em: <https://www.bv.com.br/politica-de-privacidade?idcmpit=bv_menufooter-institucional_politica-privacidade-bv_all-visits-nova-home_campanha-nova-home_link-text-redirect-footer-institucional>. Acesso em: 4 fev. 2024b.

POPOVA, Natalia A; BUTAKOVA, Natalia G. *Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. Rússia, 2019. Disponível em: <<https://ieeexplore.ieee.org/document/8657279>>. Acesso em: 15 out. 2023.

PRODANOFF, Cristina Rodrigues Leitão. *Sigilo bancário*. Orientadora; Beatriz Vargas. Universidade de Brasília. 2008. 47 f. Monografia (Especialização em Direito

Processual Tributário) – Universidade de Brasília, Rio de Janeiro, 2008. Disponível em <<https://repositorio.enap.gov.br/bitstream/1/4743/2/Cristina%20Rodrigues%20Leit%C3%A3o%20Prodanoff.pdf>>. Acesso em: 18 jun. 2023.

PROOF of stake: o que é e como funciona nas criptomoedas? *Coinext*, 1º ago. 2023. Disponível em: <<https://coinext.com.br/blog/proof-of-stake>>. Acesso em: 2 out. 2023. 1º ago. 2023.

PROOF of Work (PoW) x Proof os Stake (PoS): uma análise comparativa. *Mercado Bitcoin*. 6 abr. 2023. Disponível em: <<https://www.mercadobitcoin.com.br/economia-digital/criptomoedas/proof-of-work-vs-proof-of-stake/>>. Acesso em: 6 mar. 2024.

QUEIROZ, Fernando Frazão de. Agência *Fotocom*: fotojornalismo a serviço da publicidade. Orientador: Prof. Ms. Dante Gastaldoni. 2009. 81 f. – Trabalho de Conclusão de Curso (Graduação em Comunicação: Habilitação em Jornalismo) – Escola de Comunicação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2009. Disponível em: <<https://pantheon.ufrj.br/bitstream/11422/2274/3/FFQueiroz.pdf>>. Acesso em: 17 jun. 2023.

RAGAZZO, Carlos. CATALDO, Bruna. Moedas digitais: entenda o que são criptomoedas, *stablecoins* e CBDCs. White Paper, Instituto Propague, set. 2021. Disponível em: <<https://institutopropague.org/wp-content/uploads/2021/09/Moedas-digitais-entenda-o-que-sao-criptomoedas-stablecoins-e-CBDCs-White-Paper-Instituto-Propague.pdf>>. Acesso em: 2 nov. 2023.

RAKHMILEVICH, Mark. *Privacy, ledger design, scalability, and cross-border integrations in Central Bank Digital Currency*. LinkedIn, 17 jul. 2023. Disponível em: <<https://www.linkedin.com/pulse/privacy-ledger-design-scalability-cross-border-bank-mark-rakhmilevich/>>. Acesso em: 27 abr. 2024.

RAUCHS, Michel GLIDDEN, Andrew; GORDON, Brian; PIETERS, Gina; RECANATINI, Martino; ROSTAND, François; VAGNEUR, Kathryn. ZHANG, Bryan. *Distributed ledger technology systems: a conceptual framework*. University of Cambridge, ag. 2018. Disponível em: <<https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf>>. Acesso em: 5 nov. 2023.

RAY, Shaan. The difference between blockchain and distributed ledger technology. *Towards Data Center*, fev. 2020. Disponível em: <<https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92>>. Acesso em: 2 nov. 2023.

RECEITA FEDERAL DO BRASIL (RFB). Portaria n. 34, de 14 de maio de 2021. Dispõe sobre o compartilhamento de dados não protegidos por sigilo fiscal com órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional e dos demais Poderes da União. *Diário Oficial da União*, Brasília, 18 maio 2021. Disponível em: <<https://www.in.gov.br/en/web/dou/-/portaria-n-34-de-14-de-maio-de-2021-320353196>>. Acesso em: 12 out. 2023.

REIDENBERG, Joel R. E-commerce and trans-atlantic privacy. *Houston Law Review*, v. 31, 2001. Disponível em: <https://ir.lawnet.fordham.edu/faculty_scholarship/38/>. Acesso em: 18 jun. 2023.

RICHARDS, Neil; HARTZOG, Woodrow. The pathologies of digital consent: trust and privacy in the digital age. *Washington University Law Review*, v. 96, 2019. Disponível em: <https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11>. Acesso em: 10 dez. 2023.

RIVEST, Ronald. ADLEMAN, Len. DERTOUZOS, Michel L. *On Data banks and privacy homomorphisms*. Massachusetts Institute of Technology. Academic Press Inc. 160- 179, 1978. Disponível em: <<https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf>>. Acesso em 9 abril 2023.

ROGOFF, Kenneth. *The curse of cash*. Princeton, Nova Jersey: Princeton University Press. Princeton and Oxford, set. 2016.

SAIAS, José; MAIA, Miguel; RATO, Luis; GONÇALVES, Teresa. *Machine learning: um estudo sobre conceitos, tarefas e algoritmos relacionados com predição e recomendação*. Universidade de Évora. Projeto APRA-CP, dez. 2018, Portugal. Disponível em: <<https://dspace.uevora.pt/rdpc/handle/10174/30174>>. Acesso em: 11 fev. 2024.

SAKAMOTO, Sarah Gomes. *Segurança, privacidade e blockchain no contexto de internet das coisas*. Orientador: Prof. Dr. Jamil de Araujo Farhat. 2020. 65 f. Pós-graduação (especialização em Internet das Coisas). Universidade Tecnológica Federal do Paraná (UTFPR), Curitiba, 2020. Disponível em: <<http://repositorio.utfpr.edu.br/jspui/handle/1/19677>>. Acesso em: 24 mar. 2024.

SALAMA, Bruno Meyerhof; PRATES, Marcelo Madureira. Moeda digital de banco central: casos e conceito. In: GOMES, Daniel de Paiva; GOMES, Eduardo de Paiva; CONRADO, Paulo Cesar. *Criptoativos, tokenização, blockchain, metaverso: aspectos filosóficos, tecnológicos, jurídicos e econômicos*. São Paulo: Ed. Revista dos Tribunais, 2022. p. 441-449.

SALAMA, Bruno Meyerhof; ZELMANOVITZ, Leonidas. *Crítica à proposta de criação de Real Digital de “Varejo”*. 29 maio 2023. Disponível em: <https://www.bcb.gov.br/conteudo/eventos/Documents/moedas_digitaais/tokenizacao/WorkTOK-Mimeo-Direito_1B_C_Critica_a_Proposta_de_Criacao_de_Real_Digital_de_Varejo.pdf>. Acesso em: 10 dez. 2023.

SANTOS, Roberto de Souza. *Aplicação de um modelo preditivo de mineração de dados para apoio à decisão de crédito*. Orientador: Prof. Dr. Marcello Peixoto Bax. 2006. 92 f. Dissertação (Mestrado em Ciência da Informação) – Programa de Pós-graduação em Ciência da Informação Universidade Federal de Minas Gerais, Belo Horizonte, 2006. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/VALA-6T7R6V/1/mestrado___roberto_de_souza_santos.pdf>. Acesso em: 8 fev. 2024.n

SCHÄR, Fabian. Decentralized finance: on blockchain and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 2021, v. 103, n. 2, p. 153-

174, 8 mar. 2021. Disponível em:

<<https://files.stlouisfed.org/files/htdocs/publications/review/2021/04/15/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.pdf>>. Acesso em: 13 fev. 2024.

SEGURA, José. O que é PoA (Prova de Autoridade – Proof of Authority)? *Bit2me Academy*, abr. 2019. Disponível em: <<https://academy.bit2me.com/pt/que-es-proof-of-authority-poa/>>. Acesso em: 6 mar. 2024.

SIGNIFICADO de pop-up. O que é pop-up. In: ENCICLOPÉDIA dos significados. Disponível em <<https://www.significados.com.br/pop-up/#:~:text=Pop%20Dup%20%C3%A9%20uma%20janela,dos%20casos%2C%20publicidades%20e%20an%C3%Bancios.>>. Acesso em: 8 fev. 2024.

SILVA, Aleksander Bôvo. *Central bank digital currency: análise das diretrizes iniciais do Banco Central do Brasil*. 2021. 59 f. Orientadora: Profa. Dra. Aline O. Nasche. Monografia (Curso de Ciências Econômicas) – Universidade Federal do Tocantins (UFT). Campus Universitário de Palmas/TO, 2021a. Disponível em: <https://repositorio.uft.edu.br/bitstream/11612/3856/1/Monografia_ALEKSANDER%20B%C3%94VO%20SILVA.pdf>. Acesso em: 15 out. 2023.

SILVA, Elijunior Maciel da. *Blockchain como alternativa para segurança e privacidade em dispositivos IoT*. Orientador: Prof. Dr. Areolino de Almeida Neto. Universidade Federal do Maranhão. Curso de Ciência da Computação (monografia) – São Luis, 2021. Disponível em <<https://monografias.ufma.br/jspui/bitstream/123456789/6375/1/ElijuniorMacieldaSilva.pdf>>. Acesso em 12 fev. 2024.

SILVA, Leandro Novais; OLIVEIRA, Aline Corrêa. Real digital: as funções regulatórias da CBDC e a competência do Banco Central do Brasil. In: NEVES, Rubia Carneiro (Org.). *Novas fronteiras do sistema financeiro nacional*. Belo Horizonte: Ed. Expert, v. 2, p. 131-177, 2023. Disponível em: <<https://experteditora.com.br/wp-content/uploads/2023/12/NOVAS-FRONTIEIRAS-DO-SISTEMA-FINANCEIRO-NACIONAL-v.-2-1.pdf>>. Acesso em: 12 fev. 2024.

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. *Big data em tempo de internet das coisas*. In: PARENTONI, Leonardo (Coord.). *Direito, tecnologia e inovação*. Belo Horizonte: D'Plácido, 2019. v. I, p. 217- 245.

SISTEMA de busca de ativos do Poder Judiciário (SIBAJUD). Conselho Nacional de Justiça (CNJ). Disponível em: <<https://www.cnj.jus.br/sistemas/sisbajud/>>. Acesso em: 13 nov. 2023.

SMYTH, Jonathan. Matthew Brady: the father of american photojournalism. *The Anglo-Celt*. 17 abr. 2022. Disponível em: <<https://www.anglocelt.ie/2022/04/17/matthew-brady-the-father-of-american-photojournalism/>>. Acesso em: 8 dez. 2023.

SOLOVE, Daniel J. I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, v. 44, p. 745-772, 2007. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565>. Acesso em: 29 dez. 2023.

SOLOVE, Daniel J. *The digital person: technology and privacy in the information age*. New York: New York University Press, 2004. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899131>. Acesso em: 29 dez. 2023.

SOLOVE, Daniel J. The mity of the privacy paradox. GW Law faculty publications & other works. *George Washington Law Review*, v. 89, n. 1, 2020. Disponível em: <https://scholarship.law.gwu.edu/faculty_publications/1482/>. Acesso em: 9 jan. 2024.

SOUSA, Francisco Eberto. *Sistema de verificação da integridade de dados baseado em oráculo de Blockchain para Internet das Coisas (IoT)*. Orientador: Prof. Dr. Cleonilson Protásio de Souza. 2023. 48 f. Programa de Pós-Graduação (Mestrado) – Universidade Federal da Paraíba, João Pessoa, 2023. Disponível em: <https://repositorio.ufpb.br/jspui/bitstream/123456789/27082/1/FranciscoErbertoDeSouza_Dissert.pdf>. Acesso em: 13 fev. 2024.

SOUSA, Jorge Pedro. *Fotojornalismo: uma introdução à história, às técnicas e à linguagem da fotografia na imprensa*. Porto: Universidade do Porto, 2023. Disponível em: <<https://www.bocc.ubi.pt/pag/sousa-jorge-pedro-fotojornalismo.pdf>>. Acesso em: 8 dez. 2023.

STANLEY, Andrew. *The ascent of CBDCs*. International Monetary Found, set. 2022. Disponível em: <https://www.imf.org/en/Publications/fandd/issues/2022/09/Picture-this-The-ascent-of-CBDCs>. Acesso em: 8 abril 2023.

SUBRAMANIAN, Srimukessh. Blockchain: a regulatory overview. *Acess Partnership*, 29 jul. 2019ba. Disponível em: <<https://accesspartnership.com/blockchain-a-regulatory-overview/>>. Acesso em: 24 mar. 2024.

SUBRAMANIAN, Srimukessh. Blockchain: an introduction. *Acess Partnership*, 10 jul. 2019ab. Disponível em: <<https://accesspartnership.com/blockchain-an-introduction/>>. Acesso em: 24 mar. 2024.

SZABO, Nick. *Smart contracts*. 1994. Disponível em: <<https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LTOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>>. Acesso em: 13 fev. 2024.

TAVANI, Herman T.; HIMMA, Kenneth Einar (Ed.). *The handbook of information and computer ethics*. New Jersey: John Wiley & Sons, Inc. Hoboken, 2008. Disponível em: <http://www.cems.uwe.ac.uk/~pchatter/2011/pepi/The_Handbook_of_Information_and_Computer_Ethics.pdf>. Acesso em: 18 jun. 2023.

TENSINI, Eduardo Henrique. *A lavagem de dinheiro e a evasão de divisas pelo criptoativo*. Orientador: Prof. Doutor Orlando Luiz Zanon Junior. 2023. 159 f. Programa de Pós graduação (Mestrado) – Dupla titulação. Universidade do Vale do Itajaí. Widener University Delaware Law School. 2023. Disponível em: <<https://www.univali.br/Lists/TrabalhosMestrado/Attachments/3169/Dissertac%CC%A7a%CC%83o%20Eduardo.pdf>> Acesso em: 18 fev. 2024.

THE BLOCKCHAIN oracle problem. *Chainlink*, 29 nov. 2023. Disponível em: <<https://chain.link/education-hub/oracle-problem>>. Acesso em: 16 mar. 2024.

THE PET Guide. The United Nations Guide on privacy enhancing Technologies for official statistics. *United Nations Big Data*. 2023. Disponível em: <https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf>. Acesso em 27 abr. 2024.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). *Aplicações blockchain no setor público do Brasil*. Brasília: Tribunal de Contas da União, Secretaria das Sessões (Seses), 2020. Apêndice 1. Disponível em: <https://portal.tcu.gov.br/data/files/58/02/CE/5E/C4854710A7AE4547E18818A8/Block_chain_apendice1.pdf>. Acesso em: 12 out. 2023.

TRINDADE, Lara Micaela Pereira da Costa e Fonseca. *Investigação de suporte tecnológico para criptomoedas de bancos centrais*. Orientador: Prof. Doutor Paulo Rupino da Cunha. 2021. 137 f. (Mestrado em Engenharia Informática) – Faculdade de Ciências e Tecnologia. Departamento de Engenharia Informática. Programa de Pós-Graduação, Universidade de Coimbra, Coimbra, 2021. Disponível em: <https://estudogeral.uc.pt/bitstream/10316/95551/1/Tese_Lara_Trindade.pdf>. Acesso em: 12 out. 2023.

TSUCHIYA, Alexandre Kenji. *Web 3.0, tecnologias relacionadas, e impactos econômicos e tributários no Brasil*. Chamada Pública n. ENAP 01/2021. Projeto: Produção de dados e conhecimento estratégico na tomada de decisão da gestão governamental. Brasília: Escola Nacional da Administração Pública (ENAP), 2022. Disponível em: <<https://repositorio.enap.gov.br/bitstream/1/7252/1/Relat%C3%B3rio%20de%20pesquisa%20-%20WEB%203.0.pdf>>. Acesso em: 12 nov. 2023.

UNIÃO EUROPEIA (UE). Carta dos direitos fundamentais da União Europeia. *Jornal Oficial das Comunidades Europeias*, 18 dez. 2000. Disponível em: <https://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 12 abr. 2023.

UNIÃO EUROPEIA (UE). *Regulation EU 2016/679*. General Data Protection Regulation (GDPR). União Europeia, 2016. Disponível em: <<https://gdpr-info.eu/>>. Acesso em: 18 jun. 2023.

VILARES, Fernanda Regina. *Ação controlada e criminalidade organizada: os controles necessários à atividade investigativa*. Orientador: Prof. Dr. Maurício Zanoide de Moraes. 2014. 231 f. (Doutorado) – Universidade de São Paulo (USP), São Paulo, 2014. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2137/tde-19112015-164630/publico/ACAO_CONTROLADA_FERNANDA_REGINA_VILARES_integral.pdf>. Acesso em: 12 fev. 2024.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: <<https://www.jstor.org/stable/1321160>>. Acesso em: 12 abr. 2023.

WENHAO, Shen. Cryptocurrency laws and regulations in China. *Asia Business Law Journal*, 12 jul. 2018. Disponível em: <<https://law.asia/cryptocurrency-law-china/>>. Acesso em: 14 out. 2023.

WERLE, Tania Daniele. Criptomoedas: natureza Jurídica e Reflexos tributários. *Revista de Direito Tributário Atual*, São Paulo, n. 49, p. 345-372, 2021.

WESTIN, Alan F. *Privacy and freedom*. New York: Atheneum, 1967.

WHAT IS a block explorer: block explorers enable you to search for information on a particular blockchain. *Cryptopedia Staff.*, 28 jun. 2022. Disponível em: <<https://www.gemini.com/cryptopedia/what-is-a-block-explorer-btc-bch-eth-ltc>>. Acesso em: 13 fev. 2024.

WORLD BANK GROUP (WBG). Distributed Ledger Technology (DLT) and Blockchain. International Bank for Reconstruction and Development. *FinTech Note* n. 1, Washington, 2017. Disponível em: <<https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>>. Acesso em: 2 nov. 2023.

WORLD ECONOMIC FORUM (WEF). Central bank digital currency global interoperability principles. White Paper, jun. 2023. Disponível em: <https://www3.weforum.org/docs/WEF_Central_Bank_Digital_Currency_Global_Interoperability_Principles_2023.pdf>. Acesso em: 13 fev. 2024.

WORLD ECONOMIC FORUM (WEF). *Central Banks and distributed ledger technology: how are Central Banks exploring blockchain today? Committed to improving the state of the world*. White paper. *World Economic Forum*, mar. 2019.

WÜST, Karl; GERVAIS, Arthur. Do you need a Blockchain? In: CRYPTO VALLEY CONFERENCE ON BLOCKCHAIN TECHNOLOGY (CVCBT). Zug, Suíça, 20-22. *Research Gate*, 20-22, jun. 2018. p. 45-54. Disponível em: <<https://www.computer.org/csdl/proceedings/cvcbt/2018/17D45VtKiqk>>.

XU, Xiwei; WEBER, Ingo; STAPLES, Mark. *Architecture for blockchain applications*. Suíça: Springer Nature, 2019.

YOUTUBE. Coletiva Real Digital. *Banco Central do Brasil*, 6 mar. 2023. Disponível em: <<https://www.youtube.com/watch?v=LCyCE9mfH2U>> Acesso em: 2 out. 2023.

YOUTUBE. Live BC#12 DREX: fatos, fakes e todas as dúvidas sobre a moeda digital. *Banco Central do Brasil*, 21 ago. 2023. Disponível em: <<https://www.youtube.com/watch?v=GCGbbA5o6mI&t=727s>>. Acesso em: 25 nov. 2023.

YOUTUBE. Web Summit - Beyond Banking - Explorando as Fronteiras do Drex. *Banco BV*, 17 abr. 2024. Disponível em: <<https://www.youtube.com/watch?v=SsSho4rZLBs>>. Acesso em: 27 abr. 2024.

ZAGO, Bruno. Como usar dados financeiros para tomar decisões de investimento. *CedroTech*. 24 jan. 2023. Disponível em: <<https://www.cedrotech.com/blog/como-usar-dados-financeiros-para-tomar-decisoes-de-investimento/>>. Acesso em: 6 mar. 2024.

ZUBOFF, Soshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs, 2018.