PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

PROJETO DE TRABALHO DE CURSO II

DESAFIOS DA LGPD: IMUTABILIDADE DA BLOCKCHAIN PÚBLICA E TRATAMENTO DE DADOS PESSOAIS PELA BASE LEGAL DE CONSENTIMENTO

ORIENTADO: WILLIAM SANTOS VIEIRA

ORIENTADOR: PROF. ERNESTO MARTIM S. DUNCK

GOIÂNIA

2022

WILLIAM SANTOS VIEIRA

DESAFIOS DA LGPD: IMUTABILIDADE DA BLOCKCHAIN PÚBLICA E TRATAMENTO DE DADOS PESSOAIS PELA BASE LEGAL DE CONSENTIMENTO

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).
Prof. Orientador: Ernesto Martim S. Dunck.

GOIÂNIA

2022

WILLIAM SANTOS VIEIRA

DESAFIOS DA LGPD: IMUTABILIDADE DA BLOCKCHAIN PÚBLICA E TRATAMENTO DE DADOS PESSOAIS PELA BASE LEGAL DE CONSENTIMENTO

Data da Defesa: 03 de dezembro de 2022

BANCA EXAMINADORA

_____

Orientador: Prof. Ernesto Martim S. Dunck. Nota:

_____

Examinador Convidado: Prof. Eurípedes Clementino Ribeiro Junior Nota:

DEDICATÓRIA

Dedico esse trabalho a todos que acreditaram em mim, em especial aos meus pais, que me apoiaram durante a trajetória acadêmica.

AGREDECIMENTOS

Agradeço ao meu orientador Ernesto Martim S. Dunck pela condução do trabalho; aos meus pais e irmãos pelo apoio durante essa trajetória; aos meus amigos, que acreditam em mim.

DESAFIOS DA LGPD: IMUTABILIDADE DA BLOCKCHAIN PÚBLICA E TRATAMENTO DE DADOS PESSOAIS PELA BASE LEGAL DE CONSENTIMENTO

RESUMO

A seguinte monografia analisou o desafio da Lei Geral de Proteção de Dados para tratar informações em uma rede descentralizada, já que a característica de imutabilidade da tecnologia blockchain pública vai de encontro com o direito de exclusão e modificação do titular na base legal de consentimento. A compreensão na elaboração do presente trabalho envolveu método de pesquisa teórica, a fim de analisar aspectos que podem contribuí na discussão sobre o tema em comento. O procedimento contou com pesquisas bibliográficas e documentais, optando-se pela análise de caráter quantitativo e qualitativo. Ademais, pesquisas no ordenamento jurídico brasileiro e doutrinas foram ferramentas no alicerce no desenvolvimento do trabalho. Por fim, foi exposto as possíveis soluções jurídicas e técnicas, a fim de que a tecnologia da blockchain pública seja compatível com regulamentação internada.

Palavras-chave: *blockchain, dados pessoais, tratamento de dados, base legal de consentimento, Lei Geral de Proteção de Dados (LGPD), incompatibilidade, imutabilidade, exclusão, modificação.*

ABSTRACT

The following monograph analyzed the challenge of the General Data Protection Law to handle information in a decentralized network, since the immutability characteristic of public blockchain technology goes against the right of the holder to delete and modify the legal basis of consent. The understanding in the elaboration of the present work involved a method of theoretical research, in order to analyze aspects that may contribute to the discussion on the topic under discussion. The procedure included bibliographic and documental research, opting for quantitative and qualitative analysis. In addition, research in the Brazilian legal system and doctrines were tools in the foundation for the development of the work. Finally, possible legal and technical solutions were exposed, so that public blockchain technology is compatible with internal regulations.

Keywords: *blockchain, personal data, data processing, legal basis of consent, General Data Protection Law (LGPD), incompatibility, immutability, deletion, modification.*

SUMÁRIO

1. INTRODUÇÃO

A ciência social do direito precisa estar em consonância com os anseios sociais, a fim de que fatos jurídicos sejam regulamentados para manter a ordem e a boa convivência entre os povos, pois sem uma imposição Estatal e previsão de atos causariam conflitos e, consequentemente, violações graves aos direitos e garantias fundamentais.

A legislação tem suma importância no campo jurídico e social para prever direitos e deves da sua população. Ao surgir novas necessidades que possam comprometer a vida em sociedade, cabe ao Estado compreender o fato e regulamenta-lo, a fim de manter a paz social.

A previsão legal é de interesse social e estatal quando determinado campo pode estar sendo interferido por ações de algo ou de alguém, sendo assim, a legislação tem suma importância em proteger direitos e deveres.

Com o advento da blockchain, por exemplo, novas necessidades foram surgindo, já que empresas utilizam esse tipo de tecnologia para armazenamento de dados, já que sua estrutura descentralizada causa uma segurança maior em relação ao modelo tradicional para tratamento de dados.

O legislador, por outro lado, não conseguiu prever na elaboração da Lei Geral de Proteção de Dados tratamento de informações pela rede blockchain, tendo em vista que sua característica de imutabilidade vai de encontro com o direito de exclusão e modificação aduzido na legislação.

A presente monografia analisará o problema gerado pela legislação em não ter em seu teor aspectos que possam resguardar os direitos dos titulares de retificação e exclusão de dados em uma blockchain pública, bem como os desafios do legislador regulamentar a tecnologia em comento para ser compatível a Lei Geral de Proteção de Dados.

Diante dessa conjuntura, é importante responde as seguintes questões: Quais são os desafios da Lei Geral de Proteção de Dados (LGPD) em tratar dados pessoais pela base legal de consentimento por meio da blockchain pública? Blockchain Pública pode contribuir na segurança do tratamento de dados pessoais? Tem meios alternativos que possa resguardar os direitos dos titulares no tratamento de dados pessoais pela base legal de consentimento no uso da Blockchain Pública? É possível identificar o agente de tratamento pela Blockchain Pública?

Assim, o objetivo principal dessa monografia é estudar a problemática enfrentada pela Lei Geral de Proteção de Dados em não ter em seu teor aspectos que possam garantir o tratamento de dados em uma rede blockchain pública, já que sua característica de imutabilidade e imodificável vai de encontro com a legislação.

Ao aprofundar sobre o tema em comento, será essencial ter como base pesquisas bibliográficas, documentais, doutrinas, cases e legislação, a fim de que o tema em comento tenha em seu teor informações pertinentes para mostrar ao leitor a importância do conteúdo estudado no sei social e jurídico.

No primeiro capítulo, será abordado o aspecto histórico da blockchain púbica, bem como sua estrutura e suas características, principalmente a imutabilidade, já que será o ponto principal a ser discutido. Ademais, será analisado alguns casos em que o uso da tecnologia da blockchain teve bons resultados.

No segundo capítulo, para compreensão do tem em comento, será trabalhado a conjunta histórica da Lei Geral de Proteção de Dados, bem como conceitos expostos na lei sobre o tratamento de dados pela base legal de consentimento, a fim de que seja garantida uma compreensão melhor do tema discutido.

Por fim, o aspecto da imutabilidade da blockchain será analisado em conjunto com as exigências aduzidas na Lei Geral de Proteção de Dados (LGPD) no tratamento de informações pela base legal de consentimento. Nesse último momento, será trabalhado os desafios da compatibilidade lei com a tecnologia, sendo exposto algumas possíveis soluções para harmonia entre os dois.

1. CONTEXTO HISTÓRICO

O mundo vivenciava, em 2008, uma das piores crises financeiras devido ao aumento abusivo dos valores imobiliários nos Estados Unidos, já que a supervalorização dos preços não acompanhou o poder aquisitivo dos cidadãos. Com a taxa de juros exacerbada e recessão econômica desenfreada, o Lehman Brothers, um dos maiores bancos de investimento do mundo, entrou com pedido de recuperação judicial em 15 de setembro de 2008 e logo depois teve sua falência decretada, causando grande impacto no mercado de ações mundial.

O cenário de incerteza causado pela crise e decretação de falência de diversos bancos na época fortaleceram a ideia de que o modelo tradicional de transação econômica vigente não gerava segurança, já que há grandes probabilidades de fraude pelo terceiro intermediador.

Neste período, as instituições financeiras perderam bastante credibilidade e, por coincidência, o protocolo Bitcoin teve sua primeira aparição com a publicação de um documento intitulado "Bitcoin: Um Sistema de Dinheiro Eletrônico Ponto-a-Ponto", pelo pseudônimo Satoshi Nakamoto.

Sobre o objetivo do Bitcoin, Uhdre (2021, p. 33) discorre que:

> O objetivo último do sistema era possibilitar a troca de representações de valores diretamente entre as partes, sem a necessidade da presença dos intermediários de confiança (middleman). Em outras palavras, o Bitcoin substitui o papel exercido atualmente pelos bancos e demais intermediários das transações financeiras. Confia-se no protocolo tecnológico que possibilita o envio de valores diretamente de parte-a-parte (P2P, peer-to-peer), sem necessitar de um terceiro de confiança a quem se outorgue a função de zelar para evitar que o mesmo recurso seja gasto mais de uma vez.

Satoshi Nakamoto, então, propôs no seu trabalho o Bitcoin como um novo sistema de dinheiro eletrônico, sendo capaz de resolver gastos duplos sem a necessidade de um intermediador, bem como registro do histórico de todos os usuários do sistema via uma rede peer-to-peer.

Nesse sentido, Ulrich (2014, p. 18) assevera que:

> Todas as transações que ocorrem na economia Bitcoin são registradas em uma espécie de livro-razão públicos e distribuído chamado de blockchain (corrente de blocos, ou simplesmente um registro público de transações), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações realizadas

O suposto criador do Bitcoin criou um sistema eletrônico completamento descentralizado, a fim de que as transações financeiras não dependessem de um órgão central para emissão de moeda ou para a liquidação e validação de transações, sendo uma inovação e um grande avanço tecnológico no setor financeiro (ANTONOPOULOS. 2017, p. 13).

Ademais, Satochi Nakamoto preocupou-se em evitar com que gasto duplo de um mesmo bitcoin fosse realizado, por meio de validação de blocos de transação pelos mineradores, sejam pessoas, sejam empresas (ou grupos deles, chamadas mining pools), que disponibilizam seus computados para resolverem complexos algoritmos, destinados a verificar a higidez dos blocos de transações (UHDRE. 2021, p. 38).

O Bitcoin pode ser referido de duas maneiras: com letra maiúscula ou letra minúscula. Refere-se a moeda digital quando grafada em letra minúscula e máscula quando se refere ao protocolo que trata de um programa que cria, sobre a camada da internet, uma rede global e distribuída (Distributed Ledger Technology) de registros de transações relativas à transferência de valores diretamente entre partes distintas (peer-to-peer ou P2P), isto é, sem intermediários (UHDRE. 2021, p. 33).

A tecnologia Blockchain Pública utilizada no Bitcoin, conhecida como Distributed Ledger Technology (DLT) ou livro razão distribuído, deixou de ser exclusivamente utilizado no campo financeiro para se tornar, depois de uma década, um novo segmento no tratamento de dados pelas empresas, tendo em vista que há elementos que inibem violações à rede, bem como confere uma segurança e integridade maior nas informações registradas.

Com a evolução da Blockchain desde do seu surgimento, empresas de diversos ramos do conhecimento interessaram no seu potencial e aderiram sua tecnologia para desenvolver projetos próprios.

2. ESTRUTURA E SUA CARACTERÍSTICA DE IMUTABILIDADE

Antes de adentrar na estrutura da Blockchain, é necessário abordar alguns pontos da base de dados centralizados, já que é o modelo tradicional utilizado nas empresas. O banco de dados da arquitetura centralizada fica armazenada em apenas em um único servidor, ou seja, apresenta um único ponto de vulnerabilidade.

Ademais, sua escalabilidade possui recursos finitos, sendo assim, seu trafego é limitado ao número de usuários, deixando o processamento de dados mais lento, bem como exigi mais desempenho da capacidade de armazenamento do servidor.

Diferente do modelo centralizado, a tecnologia da Blockchain, conhecida como Distributed Ledger Technology (DLT) ou livro razão distribuído, tem integrada na sua estrutura programações complexas que servem para diversos segmentos na sociedade, já que apresenta características que podem contribuir na segurança e na integridade nas informações contidas.

No caso em tela, Pertile (2021, p. 42) comenta:

> Blockchain é um livro-razão público e descentralizado, cuja confiança se dá na tecnologia em que é construída. Normalmente, é descrito como tendo as seguintes características: consenso, proveniência, imutabilidade, finalidade e descentralização. A primeira, porque, em uma blockchain, a validade de um bloco é definida através de consenso entre os nós (computadores habilitados a validar um bloco, processo que será explicado adiante); a segunda, porque toda a cadeia de informações registradas é passível de verificação e conferência; a terceira, porque a edição das informações em um bloco consolidado é impossível; finalidade, porque todos os dados e histórico de transações e registros se encontram em uma única fonte confiável; descentralização, porque todos os registros são compartilhados/distribuídos entre todos os nós ou usuários da blockchain, então, caso um dos nós falhe, a rede continua funcionando, e os registros permanecem salvos em todos os computadores conectados.

A validação de informações inseridas em uma Blockchain é realizada automaticamente pelos partícipes da rede, ou seja, sua estrutura descentralizada permite que as bases de dados sejam processadas em diversos servidores espalhado pelo mundo, tornando-se mais segura em relação ao modelo tradicional, já que o tratamento de dados não está concentrado em apenas um local.

Assim que um dado é inserido na Blockchain, é necessário que todos os mineradores (ou “Nodos”) envolvidos, computadores distribuídos pelo mundo que fornecem o poder de processamento, validam as informações inseridas para não acarretar fraudes e modificações incondizentes com a rede.

Pertinele (2021, p. 41) discorre:

> Os mineradores analisam as informações inseridas e as confirmam, se verdadeiras. Após determinado número de informações ou transações registradas, consolida-se um “bloco” de informações, que recebe uma numeração criptográfica própria (através do processo de hashing), a qual é acrescentada no início do bloco seguinte, e assim por diante, criando uma cadeia de blocos criptografados que, em tese, não podem ser alterados

Diante do exposto, cada bloco contém um “hash” e sempre uma referência o anterior, sendo assim, qualquer modificação faz com que um bloco recalcule as informações de todos os blocos subsequentes, fazendo com que essa programação complexa garante coesão e integridade no seu sistema.

A função hash em um bloco é como se fosse uma digital, já que cada bloco tem um próprio que o identifique. Os hash subsequentes são atrelados ao hash do bloco anterior, portanto, qualquer alteração de dado um determinado bloco altera o hash desse bloco adulterado e, por conseguinte, de todos os subsequentes, denunciando a adulteração feita (UHDRE. 2021, p. 34).

Recapitulando, os nós são interligados entre si, porém em uma grande rede ponto a ponto, deste modo, não há um terceiro, como o modelo centralizado, para validação das informações. Assim que um dado é inserido, caso seja validado, será incluído em uma lista provisória (“memory pool”) daquele nó de transações e repassado para os demais.

Caso o dado inserido seja rejeitado será colocado em uma área temporária de espera (“orphan pool”). Isso ocorre quando, por exemplo, há alguma tentativa de exclusão de alguma informação no sistema, já que vai em desacordo com as características da Blockchain.

Se os nós constatarem que o bloco não entra em conflito com os demais e está de acordo com os elementos que norteiam a Blockchain, esse será inclusa, portanto, na lista dos “confirmados”.

O bloco de uma Blockchain é gerado pelos nós que validam aquela rede, contendo diversas informações que ainda não foram confirmadas. Cada bloco contém um identificador de 32 bytes, conhecida como “hash”, que serve como uma espécie de “digital”. Ademais, cada bloco inclui o registro de data/hora e um link que interliga com o anterior por meio do seu hash.

Para ficar mais compreensivo, já que a estrutura da Blockchain é bastante complexa, suponhamos que uma empresa deseja registrar informação pessoais de um usuário no bloco “A”. Posteriormente foi necessário acrescentar mais duas informações, sendo criado o bloco “B” e “C” para registrar cada uma delas.

Quando a informação “C” é inserida no bloco de dados, por exemplo, modifica o hash desse bloco adulterado e, por conseguinte, de todos os subsequentes, isto é, primeiro o “B” e depois o “A”, sendo assim, não tem como acrescentar algo sem informar todos os blocos, já que são encadeados entre si.

A validação das informações embutidas é feita pelos nodes distribuídos em diversos locais, ou seja, os dados em blocos encadeados entre si só podem ser adicionados, sendo impossível exclusão de dados e retificação já armazenados.

A modificação da Blockchain é considerada impossível, pois o invasor deve criar uma cadeia mais longa que as que já estão integradas, isto é, mais de 51% dos computadores devêm ser atacados ao mesmo tempo, conhecido como "51% attack".

É necessário ressaltar, que além do invasor deter um ataque em massa de grande proporção, tem o custo energético que precisaria ser gasto, no caso do consenso proof-of-work, o que torna a pratica da violação ainda mais impossível (UHDRE. 2021, p. 47).

O algoritmo de consenso do Bitcoin (Proof of Work), por exemplo, inibi que ataques a rede não sejam bem sucedidos, uma vez que sua estrutura descentralizada impossibilita uma invasão em massa, já que os blocos estão distribuídos em diversos locais. A segurança contra ataques e adulteração de dados, portanto, aumenta quanto maior a rede.

O banco de dados descentralizado e validação de armazenamento de informações por diversos nós, portanto, tornam a blockchain mais integra e transparente, tendo em vista que todos os participantes têm acesso a todas as transações registradas devido à garantia de rastreabilidade.

Nesse sentido, Uhdre (2021, p. 33) assevera que:

> Note-se que os blocos de dados só podem ser adicionados aos anteriores, o que torna as transações irreversíveis. Da mesma forma, é de se pontuar que, justamente por serem os hashs subsequentes atrelados ao hash do bloco anterior, qualquer alteração de dado contido em um determinado bloco modifica o hash desse bloco adulterado e, por conseguinte, de todos os subsequentes, denunciando a adulteração feita: é essa transparência que torna o sistema mais confiável relativamente à veracidade dos dados.

A tecnologia da blockchain, considerada como um livro razão ou um livro de registro, tornou-se única e popular devido, principalmente, ser um banco de dados seguro e integro, já que possui as seguintes características: descentralização; imutabilidade; transparência; rastreabilidade; segurança.

3. OFF-CHAIN E SIDECHAIN

Tem certos dados que são confidenciais e sensíveis, deste modo, seriam inviáveis armazena-los em uma blockchain pública. As Informações que precisam ser restritas para o público podem ser armazenados em uma off-chain (registro em rede

separada da convencional) ou em uma sidechains (redes paralelas à blockchain principal, com restrições de acesso).

A vinculação dos dados inseridos na off-chain na blockchain seria identificada por meio da hash da cadeia principal. O banco de dados em uma cadeia diversa possibilita com que dados pessoais não sejam acessados por qualquer pessoa, apenas para os habilitados.

Sobre o tema em comento, discorre Belo Horizonte (2021, p. 193):

> As informações contidas nos hashes armazenados na cadeia devem servir de rota para que os interessados tenham acesso aos dados pessoais, cujo armazenamento ocorre em outro banco de dados que não esteja sujeito aos problemas relacionados à imutabilidade de registros que o Blockchain fornece. Neste contexto, the right to erasure é proporcionado pela possibilidade de que seja apagada a "vinculação" do hash no blockchain para com os dados armazenados nos servidores off-chain.

A sidechain, por outro lado, é uma Blockchain que valida dados de outra Blockchain, a fim de que uma nova camada paralela seja criada sem modificar a estrutura da principal.

Sendo uma Blockchain secundária vinculada a Blockchain principal, a Sidechain permite que o tratamento de dados seja feito em um bloco fora da blockchain principal e, logo em seguida, seja movida de volta.

4. TIPOS DE BLOCKCHAIN: PÚBLICA, PRIVADA E FEDERADO

Embora o termo Blockchain seja mencionado ao modo como os dados estão estruturando, o seu termo acaba, muita das vezes, confundido com os projetos em DLT ("Distributed Ledger Technology"), que podem ou não estruturar os dados em blocos cripotograficamente encadeados, cujos dados só podem ser adicionados (UHDRE. 2021, p. 43).

Embora há diferença entre os dois termos; o Blockchain tem mais popularidade, sendo usado pela maioria para referir, também, os projetos distribuídos em outras estruturas.

Blockchain ou DLT's, portanto, pode ser estruturada de várias formas, porém as principais são as seguintes**:** públicas; privadas; federado ou de consórcio**,** sendo que cada uma tem elementos destintos.

Na blockchain pública, os dados inseridos são validados por diversos computadores que são distribuídos em diversos locais para manter a integridade da rede, cujas informações integradas estão acessíveis para qualquer pessoa ler ou visualizar.

O Bitcoin, por exemplo, foi o primeiro blockchain pública, sendo assim, possui a maior cadeia de blocos entre as demais, já que sua estrutura descentralizada permite que sua participação seja aberta para qualquer pessoa que deseja participar.

Com sua popularidade, outras Blockchain Pública surgiram para atender a necessidade de diversos campos do conhecimento e, inclusive, algumas com uma tecnologia mais atraente, já que a atualização é constante e necessária para manter sua integridade e confiabilidade.

A Ethereum, a segunda maior Blockchain do mundo, constantemente passa por atualizações na sua estrutura, a fim de que sua funcionalidade não seja ultrapassada, pois a tecnologia, como o direito, vive em transformação diariamente. O Hard Fork Londom, uma das mudanças na sua estrutura considerada mais importante desde o seu surgimento e ocorrida em 2021, mudou o sistema de transação da Ethereum, a fim de que seja, aos poucos, movida sua rede de consenso de prova de trabalho para um consenso de prova de participação.

Ademais, a plataforma de blockchain pública Solana, fundada em 2017 por Anatoly Yakovenko e oficialmente lançada em 2020, tem uma tecnologia inovadora que proporciona uma escalabilidade de rendimento mais barata e rápida em relação as demais, já que o tempo de criação de cada bloco é, em média, de 400 milissegundos, sendo que da Ethereum é de 15 segundos e o do Bitcoin 10 minutos.

Fica evidenciado, portanto, que a Blockchain Pública permanece constantemente em transformação para atender as necessidades do mercado.

Atualmente (2022), há diversos tipos de tecnologia descentralizada, que apresentam elementos distintos e semelhantes na sua estrutura. Além das apresentadas, há outros tipos de Blockchain pública, como o Litcoin, a Zcash, a Polkadot e Eos...

Já na Blockchain Privada, diferente da pública, tem na sua estrutura banco de dados centralizado, isto é, sua arquitetura foi planejada para atender um determinado grupo de pessoas, ou seja, para participar da rede é necessário seguir condições pré-estabelecidas e apenas membros que têm permissão podem acessar as informações registradas.

Sobre o tema em comento, discorre Uhdre (2021, p. 44):

> Falar-se em blockchains públicas ou privadas tem por critério o acesso às informações, aos dados registrados naquele sistema. Assim, blockchains públicas (como Bitcoin ou Etherium) seriam aquelas cujas informações estão, estão “abertas”, acessíveis para qualquer pessoa ler e visualizar. Já as blockchains privadas são aquelas cujos dados só podem ser visualizados por um grupo de pessoas predefinidas ou autorizadas (caso da Ripple, por exemplo ou da Libra), ou mesmo por uma única organização (ou conglomerado organizacional)

A Blockchain federado ou de Consórcio mantém a transparência e a descentralização dos dados, porém seu acesso é controlado por um conjunto de entidades ou organização, ou seja, o grupo poderá determinar que um dado inserido seja confidencial ou disponível publicamente.

Seus dados são controlados por diversas autoridades que fazem parte do grupo, tornando – o descentralizado. Os nós da rede são pré-criados e pré-configurados antes da organização se unirem a rede, sendo assim, há possibilidade de que determinado dado seja restrito ou aberto para envio ou visualização, já que o grupo “administra” a Blockchain de Consórcio.

Ademais, sua diferença entre as demais está na velocidade da validação das informações inclusas, tendo em vista que a validação de um bloco é realizada por um determinado grupo selecionado deixa a rede mais rápida.

Como a Blockchain de consórcio possibilita que determinado dado seja restrito ou aberto ao público sem modificar sua estrutura descentralizada, bem como sua segurança a ataques externos, empresas de diversos segmentos tem tido interesse na sua utilização.

A Voltron, por exemplo, é um ecossistema que utiliza a Blockchain Federado e foi projetado pela R3 e pela CryptoBLK, que une doze banco na mesma rede.

Cada tipo de Blockchain, portanto, apresenta características distintas, não sendo pior nem melhor do que a outra, já que cada estrutura possui elementos que podem adaptar diferentes necessidades.

5. CASES DE ADESÃO DA BLOCKCHAIN

As características da Blockchain Pública de transparência, de descentralização e de imutabilidade deixaram de ser usado apenas no Bitcoin para ser integrado em outros projetos com segmento distintos.

De acordo com a revista Forbes, publicada em 19 de fevereiro de 2020, grandes empresas já adotam a tecnologia da Blockchain Pública para acelerar processos de negócios, aumentar a transparência e potencialmente economizar nas transações.

A Amazon, uma das maiores empresas no serviço eletrônico do mundo, oferece ferramentas de blockchain para as empresas que não querem desenvolver a sua própria. A Nestlé, por exemplo, usa a tecnologia da blockchain desenvolvida pela Amazon para permitir que os usuários consigam identificar, por meio do QR code, em que fazenda os grãos de café foram plantados e onde eles foram torrados.

A Baidu, um dos navegador de busca mais utilizado no mundo e na República Popular da China, usa a rede da blockchain pública produzida pela IBM para adoção de cachorros digitais, bem como oferece serviços de empréstimo estudantil.

Nos dois casos mencionados, percebe-se que a tecnologia da blockchain pública pode ser utilizada em diversos projetos com segmento distintos, não havendo limite para sua implementação.

Além de grandes empresas globais, os elementos de transparência, de confiança e de privacidade da Blockchain têm chamado atenção de diversos países que buscam prestar serviço público de maneira mais digital e menos burocrático.

A Estônia, localizado no mar Báltico e no norte da Europa, tornou-se referência em tecnologia e informação, já que a maioria dos serviços prestados pelo Estado ocorre de maneira digital.

De acordo com um texto publicado no dia 4 de setembro de 2017 pelo Pedro Vilela Resende Gonçalves no blog Instituto de Referência em Internet e Sociedade (Iris), o país da Estônia, conhecido pela sua adesão incessante da tecnologia, passou a oferecer serviços diversos serviços eletrônicos, sendo o mais conhecido entre eles o “Estonian e-Residency”.

O governo da Estônia permiti que qualquer pessoa pode criar uma identidade digital única para possibilitar adesão dos seguintes serviços: registrar uma empresa estoniana eletronicamente; assinar documentos digitalmente, de forma autenticada; declarar impostos online; envio e recebimento de documentos criptografados; transferências bancárias online.

Essa identidade digital usa uma tecnologia chamada Blockchain KSI, que permite garantir a integridade dos registros, identidades, transações e da privacidade dos dados dos usuários desse sistema.

No Brasil, o Estado da Bahia inaugurou, no dia 09 de julho de 2021, um aplicativo com a tecnologia Blockchain denominado como Soluções Online de Licitação (SOL), que será utilizada por mais de mil associações e comparativas de agricultura dos Estados da Bahia e Rio Grande do Norte para realizar licitações com mais segurança e praticidade.

Deste modo, Blockchain tem sido aderida em diversos segmentos e países, já que sua característica atraí diversos ramos que buscam segurança e confiabilidade no tratamento de dados.

II. TRATAMENTO DE DADOS PESSOAIS

1.CONTEXTO HISTÓRICO DA LEI GERAL DE PROTEÇÃO DE DADOS

O desenvolvimento do avanço tecnológico contribuiu na interligação entre os povos e impactou diversas áreas do conhecimento, como, por exemplo, a ciência social do direito, que visa regulamentar a vida em sociedade, a fim de que a segurança e a pacificação social sejam mantidas.

A tecnologia proporcionou novas relações sociais e, consequentemente, impactou na qualidade de vida, na econômica e no campo social, deste modo, transformando vidas, seja para melhor, seja para pior.

Com o desenvolvimento da ciência, novos mecanismos passaram a ser utilizadas com frequência, sendo algumas fundamentais no dia a dia, como, por exemplo, programas que contribuem na gestão de uma empresa e redes sociais, que são usados por milhares de pessoas.

Com o desenvolvimento de softwares em diversas áreas, novos fatos sociais e jurídicos surgiram, sendo assim, o campo do direito precisou regulamentar situações antes não previstas, já que as pessoas começaram a usufruir dessas novas ferramentas em desrespeito aos direitos e garantias fundamentais.

Diante da ausência de regulamentação de novos fatos jurídicos que a tecnologia proporcionou, a União Europeia regulamentou um campo bastante explorado pelo o mundo: a internet.

Diante da falta de penalização dos atos contra o mal uso dos dados pessoais de terceiros pelas pessoas e pelas empresas, a União Europeia aprovou em

2016 a regulamentação General Data Protection Regulation (GDPR), que ficou vigente em 2018, após dois anos de vacatio legis (POHLMANN. 2019, p. 25).

Essa nova regulamentação aprovada na União Europeia impactou a forma das pessoas, seja física, seja jurídica, tratarem os dados pessoais de terceiros, já que a nova implementação trouxe algumas novidades antes não previstas em lei, como, por exemplo, a fixação de multa e a figura do oficial de proteção de dados (DPO), que fica responsável pelo controle dos titulares dos dados pessoais.

Ademais, a nova regulamentação Europeia visa proporcionar aos titulares de dados o controle maior dos seus dados pessoais, já que era comum empresas utilizarem essas informações sem restrições de uso, o que acabava acarretando em diversas violações aos direitos fundamentais.

Não sendo diferente, o Brasil sancionou a Lei nº 13.709 em 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), que foi originada PLC n. 53/2018 e promulgada pelo presidente Michel Temer no dia 14 de agosto de 2018.

Fica claro, portanto, que a regulamentação da União Europeia sobre tratamento de dados pessoais inspirou e “obrigou” o Brasil a se adequar as exigências advindo do exterior, tendo em vista que a não adequação das mudanças externas impactaria negativamente no Brasil, principalmente na economia.

A Lei Geral de Proteção de Dados (LGPD) trouxe em seu bojo garantias sobre tratamento de dados em qualquer meio, principalmente no campo virtual, já que é um local onde tem a maior concentração de informações pessoais e violações.

Nesse sentido, Pinheiro (2021, p. 10) discorre:

> A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso

> de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

Além da Lei Geral de Proteção de Dados (LGPD), foi sancionada a Emenda Constitucional Nº 115 em 11/02/2022, que altera, conforme aduz sua ementa, a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Ademais, a autoridade Nacional de Proteção de Dados (ANPD), no mesmo ano (2022) da referida ementa que considerou dados pessoais como direito e garantia fundamental, foi transformada em autarquia especial, por meio da medida provisória nº 1.124, de 13 de junho de 2022.

A regulamentação sobre tratamento de dados no Brasil, portanto, impactou positivamente no mercado externo, já que a globalização impulsionou os países a se alinharem cada vez mais sobre aspectos que envolvam direitos e garantias fundamentais.

2. CARACTERISTICAS DO TRATAMENTO DE DADOS PESSOAIS PELA BASE LEGAL DE CONSENTIMENTO

Dado pessoal é toda informação relacionada à pessoa natural identificada ou identificável, por exemplo, o nome, a data de nascimento, a origem, o endereço, o número de telefone., ou seja, dados esses que possam de alguma forma caracterizar alguém.

Nesse sentido, Basan (2022, p. 104) relata o seguinte sobre proteção de dados:

> [...] o dado pessoal como toda informação relacionada à pessoa natural identificada, como o seu nome, sua foto ou seu número de identificação (CPF, por exemplo). Além disso, é também considerada dado pessoal toda informação relacionada à pessoa identificável, de maneira indireta, como os dados de geolocalização, endereço, ou demais informações que, conjugadas, são capazes de identificar o seu titular.

Em relação aos dados identificável, a Lei Geral de Proteção de Dados utilizou critérios expansionista, já que considerada dados aquelas informações que não identifica uma pessoa de forma imediata ou indireta, isto é, considera pessoais também os dados que, unidos, são capazes de identificar a pessoa, promovendo evidente alargamento de qualificação do dado como pessoal (BASAN.2022, p. 105).

Entre os diversos dados pessoais, há certas informações que merecem atenção especial e tratamento diferenciado, conhecida como dados sensíveis, já que seu teor pode acarretar a discriminação, já que atingi aspectos subjetivos e particular de uma pessoa.

Esses dados estão relacionados, conforme aduz o artigo 5º, inciso II, da Lei Geral de Proteção de Dados, aos aspectos 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.

Tratamento de dados pessoais, de acordo com a lei geral de proteção dados (LGPD), é toda operação realizada com dados, podendo ser coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, ou controle de informação, modificação, comunicação, transferência, difusão ou extração.

É necessário ressaltar, que no artigo 4º da lei 13.709, aduz algumas situações que o tratamento de dados não tem proteção legal pela referida regulamentação, sendo as que segue: realizado exclusivamente por pessoa natural para objetivos particulares/não econômicos; para fins jornalístico e artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais, devendo ser aprovada legislação especial para tais situações [...] (PALLA. 2021, p. 14).

De acordo com o artigo 7º da Lei Geral de Proteção de Dados (LGPD), o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

> I – mediante o fornecimento de consentimento pelo titular; 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; IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O artigo 7º da referida lei aduz uma série de bases legais de tratamento de dados pessoais, sendo o fornecimento de consentimento pelo titular o mais conhecido e utilizado.

Nos termos do artigo 5º da Lei Geral de Proteção de Dados (LGPD), inciso XIII, informa que o consentimento é qualquer manifestação informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, seja de forma expressa, seja de forma oral.

Sendo de forma expressa, o conteúdo da clausula do consentimento deve está destacado e de forma pormenorizado, a fim de que interpretações abrangentes não sejam realizadas e que não haja vicio de consentimento para tornar o contrato entre as partes nulas.

Diferente das demais bases legais de tratamento de dados pessoais, como, por exemplo, a exigência para o exercício regular de direitos em processo judicial, administrativo ou arbitral prevista no artigo 5º, inciso VI da lei em comento, em que há previsão legal especifico para exigir o urso das informações de alguém, o consentimento atribui ao titular dos dados o direito de revogação, de modificação e de excluir de suas informações a qualquer momento.

Em relação aos direitos do titular, Pohlmann (2019, p. 47) expõe:

> Define os direitos atribuídos ao titular dos dados, como sejam a possibilidade de solicitar completa informação sobre os dados tratados pelo controlador, solicitar alteração ou eliminação de dados pessoais, ou mesmo opor-se ao tratamento dos seus dados pessoais, sempre observando as regulamentações correspondentes.

No que diz respeito à revogação, o titular dos dados pessoais pode, por meio da base legal de consentimento, revogar seus dados a qualquer momento mediante manifestação expressa, por procedimento gratuito e facilitado. A revogação do tratamento de dados pelo titular ocorre geralmente quando o seu interesse em dispor cessar e/ou quando as informações estão sendo manuseadas para outros fins.

Sobre o assunto em comento, Pohlmann (2019, p. 62) discorre o seguinte:

> O consentimento do titular, só é válido, nos termos da LGPD, se tiver direcionamento a uma finalidade específica ou determinada. E, havendo uma modificação quanto à finalidade específica para a qual um determinado consentimento tenha sido concedido, o titular deverá ser informado, tendo, novamente, assegurados, os seus direitos de aceitação ou revogação do consentimento.

Caso haja alguma informação incondizente, o titular pode solicitar, em qualquer momento, sua modificação, a fim de preservar aos direitos e garantias fundamentais.

Ademais, o titular pode exigir a qualquer momento a exclusão dos seus dados no banco de armazenamento, desde que não há outra base legal expressa no artigo 7º da Lei Geral de Proteção de Dados (LGPD) que exigi a sua permanência.

Sobre o assunto em comento, Pohlmann (2019, p. 62) expõe
:

> A revogação do consentimento não implica, obrigatoriamente, na eliminação dos dados. O titular pode, a qualquer momento, solicitar a eliminação dos seus dados pessoais, procedimento que deve ser realizado pelo operador ou controlador, salvo nas exceções previstas em lei (alguma outra base legal que justifique a permanência do dado).

Diante do exposto, a Lei Geral de Proteção de Dados (LGPD), em seu artigo 7º, trouxe em seu bojo tratamento de dados por meio de diversas bases legais.

A base legal do consentimento, diferente das demais, oportuniza o titular dos dados requerer a qualquer momento a revogação, a modificação e a exclusão dos seus dados.

3. AGENTES DE TRATAMENTO

A importância dos dados no mundo digital trouxe reflexões no seio jurídico para assegurar uma proteção maior para o tratamento de dados por terceiros, já que seu uso de forma desenfreada estava desencadeado violações aos direitos e garantias fundamentais.

Antes de uma lei especifica para regulamentar o tratamento de dados no Brasil, o ordenamento jurídico já previa, de maneira esparsa, alguns dispositivos sobre proteção legal de dados, como, por exemplo, a própria Constituição Federal, o Código de Processo Penal e o Marco Civil da Internet (DUTRA; KOHLS; WELTER, 2021 p. 17).

O agente de tratamento tem que ser uma pessoa comprometida e apta a adotar técnicas que asseguram a proteção de dados de terceiros, bem como uma gestão eficiente no tratamento das informações obtidas para coibir qualquer atividade ilícita que possa comprometer os direitos fundamentais dos seus titulares.

Sobre o assunto em comento, Pohlmann (2019, p. 64) aduz:

> Os Agentes de Tratamento devem manter registros e evidências de todo o tipo de tratamento realizado com os dados dos titulares. Também cabe aos agentes de tratamento a realização de medidas de segurança que permitam (ou tentem) garantir a segurança dos dados tratados

A Lei Geral de Proteção de Dados (LGPD), por outro lado, trouxe em seu bojo a figura do agente de tratamento, que é classificado, em seu artigo 5º, inciso IX, como controlador e operador, ambos tendo papeis fundamentais no tratamento de dados do titular.

O controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem determinar as questões relacionadas ao tratamento de dados pessoais, ou seja, fica responsável pelas decisões das seguintes atribuições: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, ou controle de informação, modificação, comunicação, transferência, difusão ou extração.

O operador é pessoa natural ou jurídica, de direito público ou privado, que realizada atividades sobre controle de dados de acordo com os limites determinados pelo controlador.

A autoridade nacional poderá exigir do controlador a elaboração do Relatório de Impacto à Proteção dos Dados Pessoais, devendo descrever de forma pormenorizada os tipos de dados coletados, a metodologia utilizada e mitigação de riscos adotados.

O RIPD (Relatório de Impacto à Proteção de Dados Pessoais) é um documento que assegura que o controlador medidas preventivas antes de tratar dados que possam causar riscos aos direitos e garantias fundamentais de alguém.

Nesse sentido, Feichas (2022, p. 634) discorre:

> O RIPD, previsto na LGPD, tal como o DPIA no RGPD/GDPR, diante dos exemplos postos, deve considerar não apenas os riscos de conformidade, mas perigos mais amplos para os direitos e liberdades dos indivíduos, incluindo o potencial para qualquer desvantagem social ou econômica significativa. O foco está no potencial de dano – aos indivíduos ou à sociedade em geral –, seja físico, material ou imaterial, mormente por se tratar de um processo contínuo sujeito a revisão regular.

Em caso de dano a outrem no exercício de atividade de tratamento de dados pessoais, aduz o artigo 42 da Lei Geral de Proteção de Dados (LGPD) que 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 e os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados

respondem solidariamente, salvo nos casos de exclusão previstos no artigo 43 da referida lei. Vejamos:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

A Lei Geral de Proteção de Dados (LGPD), portando, classifica o agente de tratamento em controlador e operador, tendo ambos papéis de suma relevância nas atividades que envolvam tratamento de dados pessoais.

III. BLOCKCHAIN PÚBLICA NO TRATAMENTO DE DADOS PESSOAIS

1. DESAFIOS DA LGPD: IMUTABILIDADE DA BLOCKCHAIN PÚBLICA E DIREITO À EXCLUSÃO E RETIFICAÇÃO NO TRATAMENTO DE DADOS PESSOAIS PELA BASE LEGAL DE CONSENTIMENTO

A Tecnologia da Informação proporcionou um mundo mais globalizado devido aos softwares serem necessários para expansão econômica, política e cultural de um país, já que as trocas comerciais dependem de programas específicos para facilitar a interligação de comunicação entre os Estados-Membros.

O avanço da tecnologia vem interferindo diretamente na vida das pessoas, principalmente na comunicação, já que as redes sociais são utilizadas diariamente para diversos fins. Além dos aplicativos de interação, há programas de computação fundamentais no desenvolvimento das empresas e responsáveis por zelar informações.

As redes sociais e os programas empresarias, sejam em órgão público, sejam em órgão privado, tornaram-se fontes primárias de tratamento de dados, já que necessitam ou utilizam atividades com dados pessoais dos usuários.

O Instagram, por exemplo, é uma rede social utilizado por milhares de pessoas, tendo em vista que a troca de informações é realizada de forma instantânea, diferente da idade média, em que uma simples mensagem poderia demorar horas ou dias para chegar ao seu receptor, pois seu envio era realizado de maneira manual e dependia de um terceiro, seja por meio de mensageiros, seja por bilhetes.

Nos dias atuais, o tratamento de dados ainda ocorre por um terceiro, porém no mundo digital, já que o avanço tecnológico presenciado nos últimos anos contribuiu com um mundo mais interligado e dependente devido à disposição da população softwares de tratamento de dados, na sua maioria, desenvolvidos e controlados por empresa com sede administrativa localizada em outros países.

A ligação pluricontinental de informações pelos sistemas de armazenamento e tratamento de dados trouxe o benefício de uma comunização mais eficiente, porém esse modelo tradicional em que a gestão das informações está centralizada em um servidor de uma empresa ou um órgão público tende a uma segurança mais vulnerável devido à concentração dos dados em um único servidor e manuseador por terceiro.

Diante da fragilidade do modelo centralizado de dados, em que direitos fundamentas poderiam ser violados com mais facilidade, foi desenvolvido, então, a bases de dados descentralizados, conhecido como Blockchain, sendo seu termo utilizado pela primeira vez pelo Satoshi Nakamoto, um pseudônimo do suposto criador do Bitcoin, em plena crise econômica de 2008.

O tema do seu trabalho foi: “Bitcoin: um sistema financeiro eletrônico peer-to-peer”, sendo seu artigo uma crítica ao Sistema Financeiro Nacional do modelo tradicional das transações financeiras em que depende de um terceiro mediador, isto é, um banco. Naquele momento, não se falava em Blockchain em outras áreas de conhecimento a não ser o seu uso para descentralizar o mercado financeiro.

Sabendo da sua confiabilidade e uma segurança maior no armazenamento de informações, já que há vários servidores conectados entre si, bem como não tem necessidade de um terceiro intermediado igual ao sistema tradicionais e outros

benefícios, o Blockchain atiçou curiosidades em outros ramos do conhecimento, principalmente o Direito, que necessita se atentar com a realidade social e caminhar junto com os anseios da população, bem como lidar com as novas ferramentas que atingem direitos, deveres e obrigações.

Diante da necessidade maior na proteção de dados dos indivíduos, foi sancionada em 2020 a Lei Nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), que tem por objetivo, de acordo com o seu artigo 1º, proteger os direitos fundamentais de liberdade, de privacidade e o de livre desenvolvimento da personalidade da pessoa natural.

A referida lei trouxe em seu teor aspectos fundamentais no tratamento de dados, isto é, previu sanções para os agentes de tratamento que realizar qualquer atividade que causa dados a terceiro por meio do tratamento de dados.

Por outro lado, a Lei Geral de Proteção de Dados (LGPD) não trouxe em seu bojo o tratamento de dados em um banco de dados descentralizado, ou seja, a Lei em comento foi pensada, na sua criação, atingir o modelo tradicional; já que a tecnologia da Blockchain Pública tem características de imutabilidade, deste modo, confronta com algumas exigências no tratamento de dados pessoais pela base legal de consentimento, no seu artigo 7º, inciso I da LGPD.

Operações realizadas como eliminação e modificação, por exemplo, vão de encontro com alguns princípios norteadores da Blockchain Pública, pois sua arquitetura foi programada para ser imutável, ou seja, uma vez que determinado dado é inserido, não há possibilidade de alteração e exclusão.

Nesse sentido, Pertile (2021, p. 67) assevera que:

> [...] deve-se ter cuidado ao armazenar dados pessoais em uma blockchain, uma vez que o titular pode requerer sua alteração ou remoção, o que, a depender da blockchain, seria impraticável, gerando uma violação, por parte do agente de tratamento, à LGPD.”

Sobre a incompatibilidade entre o tratamento de dado e Blockchain Pública, Pertile (2021, p. 76) discorre:

> [...] a Lei Geral de Proteção de Dados Pessoais não previu a hipótese de armazenamento em bancos de dados distribuídos, e há, do ponto de vista legal, total incompatibilidade com a guarda de dados pessoais em uma blockchain pública, visto que o titular dos dados estaria impossibilitado de exercer diversos dos seus direitos.

Destarte, a ausência de legislação para tratar dados na blockchain pública vai de encontro com a adesão do mercado em querer cada vez mais usar a rede descentralizada em seus negócios, tendo em vista que sua característica possibilita uma segurança maior em relação ao modelo tradicional.

Com a expansão da blockchain pública, outros diversos tipos foram surgindo para se adequar as necessidades de casa setor. Os quatros tipos mais conhecidos são a publica, a privada, a consorcio e semiprivado.

De acordo com um artigo publicado pelo Artur Nicoceli em 18/08/2022 no site CNN Brasil Business, empresas e instituição estão usando blockchain para receberem doações, tendo em vista que as suas características de rastreabilidade e transparência evitam que duplicidade de fornecimentos de produtos aconteçam.

Em 22/07/2022, Victor Marques publicou no site IstoÉ Dinheiro startups brasileiras que estão usando blockchain para ajudar as empresas na gestão ambiental. De acordo com o site em comento, dentro da blockchain é gerenciado a emissão de notas fiscais e documentação de saída e entrada de resíduos. “A empresa não precisam organizar toda essa estrutura, é só comprar o token”, disse Paquet.

Outra case de adesão da blockchain em seus negócios é a GreenPlat, q primeira startup ambienta que usa o banco de dados descentralizado para acelerar a produção mais limpa por meio de gerenciamento da rastreabilidade e monitoramento de tratamento de lixo.

Destarte, fica evidente que ao mesmo tempo que aumenta a adesão da tecnologia Blockchain Pública no Brasil, cresce, também, a preocupação com

proteção de dados dos envolvidos, já que exclusão e modificação, mediante o consentimento do titular de dados, são direitos inerentes aos usuários.

Devido à imutabilidade e inalteração da Blockchain Pública, fica evidenciado que o armazenamento de dados pessoais nessa tecnologia viola a legislação interna em relação ao tratamento de dados.

Embora as características de transparência e integridade da informação seja em comum entre ambos, o aspecto de exclusão e de modificação da tecnologia descentralizada vai de encontro com a lei interna Brasileira, sendo, portanto, um desafio para o legislador adequar a legislação à tecnologia da blockchain pública.

Sobre os seus objetivos em comum, Pertile (2021, p. 42) comenta:

> [...] a blockchain quanto as leis de proteção de dados possuem, em última análise, pelo menos alguns objetivos em comum, como transparência, integridade e precisão das informações. Entretanto, ainda que os objetivos sejam parecidos, uma interpretação restritiva da lei pode inviabilizar o armazenamento de dados pessoais em uma blockchain

Portando, o direito deve se adequar aos anseios sociais, deste modo, o tratamento de dados pessoais, por meio do consentimento do titular, necessita se adequar aos elementos que estão em desarcado com tecnologia da Blockchain Pública, já que a adesão do protocolo descentralizado pelas empresas está presente cada vez mais.

2. IDENTIFICAÇÃO DO AGENTE DE TRATAMENTO NA BLOCKCHAIN

A Lei Geral de Proteção de Dados atribuiu ao agente de tratamento a responsabilidade de tratar todos os dados de terceiro, sendo assim, esse profissional arcará com as consequências por qualquer irregularidade no manuseio da informação que possa causar danos a outrem.

A escolha do agente de tratamento, portanto, dar-se, por exemplo, por uma pessoa competente em uma empresa, seja por um administrador, seja por alguém

com atribuição de exercer esse papel, sendo assim, todos sabem identificar os responsáveis pelo tratamento de dados.

Por outro lado, caso um dado seja armazenado na blockchain pública, não será possível a identificação do agente de tratamento, tendo em vista que a validação das informações embutidas é feita pelos nodes distribuídos em diversos locais, ou seja, em vez de apenas uma pessoa responsável por tratar esses dados, no caso do banco de dados descentralizado será milhares de computadores espalhados pelo mundo.

Nesse sentido, Pertile (2021, p. 67) discorre:

> [...] Outro ponto de conflito, já antecipado por Tarcisio Teixeira e Carlos Alexandre Rodrigues, é a inexistência de um único agente de tratamento que possa ser responsabilizado, uma vez que, em razão da descentralidade do registro, dezenas, centenas ou milhares de nós estão processando dados conjuntamente, sem sequer se conhecerem (pelo menos no caso de uma blockchain pública)

Nesse diapasão, os autores sankievicz e Pinheiro publicaram, por meio do site jota, a seguinte informação:

> Blockchains, no entanto, são fundadas na descentralização, o que implica a substituição de uma entidade central — que seria responsável pelo tratamento — por diversos atores distintos. Isso torna mais difícil a alocação de responsabilidades e até mesmo a definição sobre a jurisdição competente para o ajuizamento de eventual demanda, especialmente quando considerada que a gestão da base de dados, frequentemente, ocorrerá de maneira conjunta.

Em remate, não é possível a identificação do agente de tratamento pela blockchain pública, tendo em vista que há milhares de responsáveis no tratamento de dados espalhados pelo mundo, em vez que uma informação guardada na rede descentralizada precisa de validação de diversos computadores.

No caso, é possível identificar o agente, por exemplo, por meio da blockchain privada, só que diferente da pública, tem na sua estrutura banco de dados centralizado, isto é, sua arquitetura foi planejada para atender um determinado grupo de pessoas, ou seja, para participar da rede é necessário seguir condições pré-estabelecidas e apenas membros que têm permissão podem acessar as informações registradas.

3. POSSÍVEIS SOLUÇÕES NO TRATAMENTO DE DADOS PESSOAIS EM BLOCKCHAIN

Na base legal de consentimento, a exclusão e modificação de informações são elementos do tratamento de dados que devêm ser cumpridas quando há exigência dos titulares, porém a Blockchain pública tem característica de imutabilidade, ou seja, uma vez inserido dados neste protocolo, será impossível ocorrer sua modificação e sua exclusão.

Nesse sentido, Pertile (2021, p. 67) discorre:

> O principal ponto de choque entre as exigências legais e tecnologias baseadas em blockchain é, possivelmente, a necessidade de excluir ou modificar determinado dado armazenado – o que, em um primeiro momento, é tido como impossível em determinados tipos de blockchain.

Já que os dados armazenados na Blockchain pública não podem ser retificados ou excluídos, as possíveis soluções técnicas seriam em relação à legislação ou utilização de outro tipo de blockchain.

A Lei Geral de Proteção de Dados (LGPD) não abordou em seu teor aspectos da tecnologia descentralizada, já que suas exigências são incompatíveis com algumas características da blockhain, como, por exemplo, a imutabilidade. Sendo assim, para acompanhar os anseios sociais, é necessário a intervenção do legislador para prever tratamento de dados pessoais em blockchain pública.

Por outro lado, o tratamento de dados pode ser realizado por meio de uma Blockchain Privada, já que há possibilidade de resguardar os direitos de modificação e de exclusão pelo agente de tratamento. Ocorre que, nesse banco de dados as informações estão centralizadas, ou seja, quem busca os aspectos de segurança da blockchain pública não vai se interessar tratar dados em uma rede privada.

Outra possível solução, no caso, seria armazenar dados pessoais em um registro à parte, como, por exemplo, a off-Chain e Sidechain, desde de que esteja vinculada na hash da blockchain. Não há muitas informações sobre esse tipo de

registro, ficando difícil sua compreensão devido ao uso de termos técnicos da ciência da programação.

Por fim, tem a Blockchain federado ou de Consórcio, que mantém os aspectos de transparência e descentralização. Nesse tipo de banco de dados, o acesso é controlado por um conjunto de entidades ou organização**,** ou seja, o grupo poderá determinar que um dado inserido seja confidencial ou disponível publicamente.

Como os dados são controlados por diversas autoridades que fazem parte do grupo, a característica de descentralização é mantida, o que aumenta a sua segurança em relação a rede privada. Os nós da rede são pré-criados e pré-configurados antes da organização se unirem a rede, sendo assim, há possibilidade de que determinado dado seja restrito ou aberto para envio ou visualização, já que o grupo “administra” a Blockchain de Consórcio.

Ademais, a blockchain federado possibilita a identificação do agente de tratamento, ou seja, é um tipo de banco de dados compatível com a Lei Geral de Proteção de Dados (LGPD) pela base legal de consentimento, já que possibilita ao titular o direito de exclusão e retificação de dados a qualquer momento.

Destarte, embora a característica de imutabilidade da Blockchain Pública seja incompatível com Lei Geral de Proteção de Dados, seus elementos de transparência e de segurança, por outro lado, contribuem na integridade no tratamento de dados pessoais.

CONCLUSÃO

A presente monografia pormenorizou os principais aspectos do contexto histórico da tecnologia Blockchain Pública, conhecida como Distributed Ledger Technology (DLT) ou livro razão distribuído, que popularizou em diversos segmentos social e deixou de ser algo exclusivo da criptomoeda bitcoin.

Em seguida, foi abordada a estrutura de um banco de dados descentralizado, descomplicando termos técnicos para garantir uma melhor compreensão em relação ao seu aspecto de imutabilidade. Ainda, outros tipos de

blockchain foram discorridos, sendo mostrado que cada uma tem uma característica distinta que se enquadra em determinado meio.

Para mostrar a importância do tema discutido, foi exposto alguns exemplos de casos em que empresas aderiram a blockchain em seus negócios, o que motivou o presente tema ser trabalhado em conciliação com a Lei Geral De Proteção de Dados, já que a lei em comento não previu tratamento de dados em uma rede descentralizada, já que trouxe em seu bojo aspectos que vão de encontro com a tecnologia.

Com essa ausência, o segundo capítulo traz o conjunto histórico da Lei Geral de Proteção de Dados para compreender a ausência de previsão em sua legislação o uso da blockchain pública em tratamento de dados pessoais pela base legal do consentimento.

Ademais, foi aduzido o papal do agente de tratamento e as sanções previstas na lei, a importância dos dados pessoais, as características do tratamento de dados, ou seja, foram explicados os principais aspectos que estrutura a importância do trabalho.

Por fim, a Lei Geral de Proteção de Dados (LGPD) e Blockchain Pública foi discutido conjuntamente, a fim de mostrar possíveis soluções para manter a compatibilidade entre a lei e tecnologia, que cada vez mais está sendo aderida.

Conclui-se no último capítulo que o desafio de manter os dois pontos harmônicos em discussão poderá ser feita das seguintes maneiras: 1) mudança na legislação para prever o tratamento de dados em uma blockchain pública; 2) utilização de outro tipo de blockchain que possibilita a exclusão e modificação, por exemplo, a federado; 3) ou armazenar dados pessoais em um registro à parte, como, por exemplo, a off-Chain e Sidechain.

A pesquisa discorrida atendeu os seus objetivos, já que os seguintes pontos foram abordados: 1) os desafios da Lei Geral de Proteção de Dados no tratamento de dados pessoais pela blockchain pública; 2) características compatíveis

e incompatíveis com a tecnologia descentralizada e a legislação; 3) os benefícios da blockchain no tratamento de dados.

Em relação à problemática trazida no presente trabalho, foi discutido outros tipos de rede para tratar dados, bem como a dificuldade de localizar um agente de tratamento em uma blockchain pública.

A estrutura da monografia utilizou método de pesquisa teórica, a fim de analisar aspectos que podem contribuí na discussão sobre o tema em comento. Foi utilizada no procedimento pesquisas bibliográficas e documentais, optando-se pela análise de caráter quantitativo e qualitativo. Ademais, pesquisas no ordenamento jurídico brasileiro e doutrinas foram ferramentas no alicerce no desenvolvimento do trabalho.

REFERÊNCIAS

ALMEIDA, Dionice de; LIMA, Ana Paula Moraes Canto de; MAROSO, Eduardo Pereira. Lei *Geral de Proteção de Dados: sua empresa está pronta?* São Paulo SP: Literare Books Internacional, 2020.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: senado, 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD*). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm. Acesso em: 14 set. 2020.

BROTTO, Natália; RIBEIRO, Aleff. *A LGPD e a tecnologia blockchain são compatíveis?* Jota: 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lgpd-e-atecnologia-blockchain-sao-compativeis-05112019. Acesso em: 16 set. 2020.

CREIMER, Marcelo. *Blockchain, Sidechain e Off-Chain*. Disponível em: https://www.blockmaster.com.br/artigos/blockchain-sidechain-e-off-chain/. Blockmaster: 2018. Acessado em: 1 abril. 2022.

CONSUMIDOR MODERNO. *Entendendo em Detalhes a Lei Geral de Proteção de Dados.* Disponível em*: https://www.consumidormoderno.com.br/2021/07/07/entendendo-detalhes-protecao-dados>. Acesso em: 1 abril. 2022.*

ECO, *Humberto. Como se faz uma tese*. 23. ed. Tradução de Gilson Cesar Cardoso de Souza. São Paulo: Perspectiva, 2010

DUTRA, Luiz Henrique; KOHLS, Cleize; WELTER, Sandro. *LGPD: da Teoria à implementação nas empresas.* 1 ed. São Paulo: Rideel, 2021.

ETHEREUM. Sobre Ethereum. Disponível em: https://www.infomoney.com.br/cotacoes/cripto/ativo/ethereum-eth/. Acessado em: 04 abril. 2022.

EZLY. *Blockchain, Sidchain e Off-chain*. Disponível em: https://ezly.com.br/blockchain-sidechain-e-off-chain/. Acessado em: 03 abril. 2022.

FALEIROS JÚNIOR, Jose Luiz de Moura; LONGHI, João Victor Rozatti; MARTINS, Guilherme Magalhães. *Comentário à Lei Geral de Proteção de Dados Pessoais, lei 13.709/2018.* Indaiatuba, SP: Editora Foco, 2022.

JOSA, Lucas. *Blockchains e sua conformidade com leis de proteção de dados.* Exame .2021. Disponível em: *https://exame.com/colunistas/tatiana-revoredo/blockchains-e-sua-conformidade-com-leis-de-protecao-de-dados/amp/.* Acessado em: 1 abril. 2022.

LAMOUNIER, Lucas. *2019: O Ano Do Blockchain Federado – O Que É Blockchain De Consórcio?.* Disponível em: https://101blockchains.com/pt/blockchain-federado/. Acessado em: 05 abril. 2022.

MARQUES, Thiago. *Transações off-chain: Quais as vantagens e desvantagens de pagar menos para transferir criptomoedas*. Disponível em: https://www.meliuz.com.br/blog/transacoes-off-chain-vantagens-e-desvantagens/#:~:text=Off%2Dchain%20%C3%A9%20um%20termo,s%C3%A3o%20feitas%20em%20off%2Dchain. Acessado em: 20 julho. 2020.

MONTEIRO, Renato, et al. Lei Geral de Proteção de Dados e GDPR: *Histórico, análise e impactos*. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em 26 de nov. de 2020.

NAKAMOTO, Satoshi. Bitcoin**.** *A peer-to-peer electronic cash system*. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 3 ago. 2020.

NUNES, Antônio Rizzato. *Manual da monografia jurídica: como se faz uma monografia, uma dissertação, uma tese*. 10. ed. São Paulo: Saraiva, 2013.

PADRÃO, Márcio. *GreenPlat é a primeira startup ambiental a usar blockchain. Disponível em: https://canaltech.com.br/startup/greenplat-e-primeira-startup-ambiental-a-usar-blockchain-197921/. Acessado em:* 08 agosto. 2022.

PERTILE, Fernando Bottega. Blockchain e Lei Geral de Proteção de Dados Pessoais: *Desafios legais e tecnológicos para o tratamento de dados pessoais em bancos de dados distribuídos* [recurso eletrônico] / -- Porto Alegre, RS: Editora Fi, 2021.

PINHEIRO, Patrícia Peck*. Proteção de Dados Pessoais: Comentários à Lei N. 13.709/2018 (LGPD).* 2 ed. São Paulo: Saraiva Educação, 2020.

POHLMANN, Sérgio Antônio. *LGPD Ninja: Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas.* Editora Fross, 2019.

OLIVEIRA, Sandro Lima. *Entendendo Privacidade de Dados Pessoais na LGPD*. Dados Eletrônico. 2021. E-book. Disponível em: https://lelivros.love/book/baixar-livro-

entendendo-privacidade-de-dados-pessoais-na-lgpd-sandro-oliveira-em-pdf-epub-mobi-ou-ler-online/. Acesso em: 1 abril. 2022.

REVOREDO, Tatiana. *Blockhain e sua Conformidade com Leis de Proteção de Dados*. Disponível em: https://exame.com/colunistas/tatiana-revoredo/blockchains-e-sua-conformidade-com-leis-de-protecao-de-dados/. Acessado em: 05 maio. 2022

SANTOS, Cleórbete. *Blockchain Públicas, LGPD e Direito ao Esquecimento*. Disponível em: https://www.masterhouse.com.br/blog/artigo-9. Acessado em: 01 abril. 2022.

SILVA, Mariana Maria. *Startup que usa blockchain para reciclagem lança 1ª plataforma de gestão hídrica no Brasil.* Disponível em: *https://exame.com/future-of-money/startup-que-usa-blockchain-para-reciclagem-lanca-1a-plataforma-de-gestao-hidrica-no-brasil/. Acessado em: 20 agosto. 2022.*

SOL. *Solução Online de Licitação.* Disponível em: https://www.sol-app.net/sol-o-que-e. Acessado em: 01 junho. 2022.

TOSTES, Marcelo. *Lei Geral de Proteção de Dados x Blockchain*. Disponível em: https://diariodocomercio.com.br/opiniao/lei-geral-de-protecao-de-dados-x-blockchain/. Acessado em: 03 maio. 2022.

UHDRE, Dayana de Carvalho. *Blockchain, tokens e criptomoedas: análise jurídica*. São Paulo: Almedina, 2021.