FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Renan Guilherme Camargo

Alinhamento entre a *Blockchain* e a Lei Geral de Proteção de Dados Pessoais

Americana, SP

2021

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

RENAN GUILHERME CAMARGO

Alinhamento entre a *Blockchain* e a Lei Geral de Proteção de Dados Pessoais

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Edson Roberto Gaseta

Área de concentração: Segurança da Informação.

Americana, SP

2021

RENAN GUILHERME CAMARGO

Alinhamento entre a *Blockchain* e a Lei Geral de Proteção de Dados Pessoais

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 07 de dezembro de 2021.

Banca Examinadora:

Edson Roberto Gaseta
Mestre
Faculdade de Tecnologia de Americana

José Luiz Zem
Doutor
Faculdade de Tecnologia de Americana

Silvia Aparecida José e Silva
Mestre
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradecer aos familiares que se dispuseram a auxiliar na manutenção da motivação enquanto produzindo este trabalho e em todos os demais desafios enfrentados até então.

Agradeço aos docentes que proporcionaram experiências maravilhosas nestes atípicos e adversos dois últimos anos, o esforço e dedicação de vocês foi fonte de inspiração imensa.

Aos colegas de classe e trabalho, por todo tempo disponibilizado e pela troca de conhecimento, estes com certeza foram imprescindíveis para a execução deste trabalho.

RESUMO

A proteção aos dados pessoais e definição dos direitos dos titulares se tornaram pontos imprescindíveis na atual era da informação. Desta forma, a importância deste tema foi externalizada nas recentes leis que buscam regulamentar o tratamento de dados pessoais efetuado por terceiros. Devido a contemporaneidade destas regulamentações, existem uma preocupação quanto a adequação de algumas das tecnologias inovadoras aos padrões impostos. O presente trabalho foi formulado justamente para analisar o alinhamento entre uma tecnologia inovadora (*blockchain*) e a Lei Geral de Proteção de Dados nº 13.709/2018 (LGPD), sancionada neste ano, de forma a identificar pontos conflituosos e sugerir possíveis formas de adequação da *blockchain* ao contexto da LGPD.

Palavras-Chave: LGPD; Blockchain; Side Chain; Off-chain.

ABSTRACT

Defining the personal information holders' rights and the data protection requirements had turned into an essential task in the current world moved by data. This theme became so important that it is being expressed through some recent laws, focused on regulating the act of processing personal data by third parties. As it's a new theme in the jurisdiction around the world, there is some concerns about how some of the technologies would be adequate to the consequent impose standards. The present research has the purpose of analyzing the alignment between an innovative technology (blockchain) and the aspects of the General Data Protection Law No. 13.709/2018 (LGPD), which turns active in this year. The objective is to identify conflicting points and route suggestions to use the blockchain in compliance with the LGPD.

Keywords: LGPD; Blockchain; Side Chain; Off-chain.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de dados
DPO	*Data Protection Officer*
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados
P2P	*Peer to Peer*

1. INTRODUÇÃO

O avanço da digitalização global, alavancado pelas novas tecnologias, impôs uma crescente demanda pela necessidade da coleta, tratamento e compartilhamento de dados com o intuito de suportar, customizar e potencializar os processos e serviços prestados à sociedade. Com a mesma rapidez, as regulamentações que visam a definição e proteção dos direitos dos titulares destes dados pessoais tornaram-se além de uma tendência, mas um requisito mundial.

Como um dos principais exemplos de uma destas novas normas regulatórias, pode-se citar o Regulamento Geral de Dados (*General Data Protection Regulation* - GDPR), que rege todo o ciclo de vida do tratamento de dados pessoais na União Europeia, esta norma é vista como objeto norteador primário para a Lei Geral de Proteção de Dados - LGPD, a lei brasileira vigente desde o dia 18 de setembro de 2020. Nas palavras de Maciel (2019, p. 11), “A lei busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade [...]”.

Entretanto, se por um lado a LGPD propõe a proteção de direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade do indivíduo, do outro existe uma dúvida sobre suas relações com as tecnologias, como é o caso da *blockchain*, um dos objetos de estudo deste trabalho. Apresentada por Satoshi Nakamoto, em suma, a *blockchain* pode ser definida como uma rede distribuída, que tem entre seus principais atributos sua descentralização, a imutabilidade dos blocos e a transparência.

A ampla aplicabilidade de redes *blockchain* públicas no mercado somada a seus atributos característicos, resultam em uma discussão quanto a viabilidade de se ter os controles e medidas e protetivas para os dados e sua competência em preservar e garantir os princípios e direitos do indivíduo titular dos dados definidos na LGPD.

Este trabalho tem como objetivo explorar pontos que suportem o alinhamento entre a LGPD e o uso da tecnologia de redes *blockchain* no âmbito do tratamento de dados pessoais.

2. REVISÃO BIBLIOGRÁFICA

O presente capítulo tem como objetivo abordar o material usado como referencial teórico para a execução do trabalho, conceituando a legislação brasileira de proteção de dados pessoais, introduzindo a tecnologia de cadeia de blocos (*blockchain)* e por fim relacionando ambos os temas, sendo o intuito observar os gatilhos chaves que possam influenciar na coexistência e aplicação conjunta dos dois objetos de estudo.

2.1. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Baseada no Regulamento Geral de Dados 2016/679 (*General Data Protection Regulation* – GDPR) da União Europeia, a lei brasileira n. 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), entrou em vigor no dia 18 de setembro de 2020. Ambas as legislações têm como objetivo central regulamentar o tratamento de dados pessoais realizados por fins econômicos ou que extrapolem as ressalvas explicitadas em seus textos.

As legislações voltadas a regulamentação das práticas que envolvem tratamento de dados pessoais, estão sendo adotadas ao redor do mundo. Estas são resultantes da revolução tecnológica da era atual, onde se tem cada vez mais a participação de dispositivos inteligentes no dia a dia da sociedade, juntamente a tecnologia de Big Data, potencializando a capacidade de coletar e gerar dados de forma ininterrupta, assim alimentando bases de dados gigantescas, e fomentando o mercado de serviços e produtos customizados.

Devido a estreita relação entre LGPD e a GDPR, é fato de que ambos os textos contêm muitas semelhanças em suas estruturações, no entanto, diferenças pontuais e bastante significativas são evidentes, exemplificando, os tópicos como o tratamento de dados de menores, políticas de proteção de dados e a transferência internacional de dados são exemplos destas abordagens divergentes.

É possível elucidar o tema Lei Geral de Proteção de Dados Pessoais através das palavras de Donda (2020, p.11):

> A LGPD é um marco jurídico regulatório inédito no Brasil e atinge todas as instituições públicas e privadas, que agora terão que se adaptar a essa nova regulamentação, que tem como princípio proteger os direitos fundamentais de liberdade e privacidade dos cidadãos brasileiros.

2.1.1. Titular de dados

A definição presente na legislação de proteção de dados brasileira para o titular de dados é dada como toda “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (BRASIL, 2018).

Ressalta-se o requisito de o titular ser uma pessoa natural, excluindo quaisquer possibilidades de relacionar dados pessoais a uma pessoa jurídica. Sendo assim, entende-se que o titular dos dados será necessariamente um indivíduo, pessoa física, ao qual os dados pessoais são alvo de tratamento.

2.1.2. Dados pessoais e dados pessoais sensíveis

O Artigo 5º da LGPD é responsável por conceituar alguns dos elementos chaves para a composição e entendimento da lei. Neste, estão contidas as definições para alguns dos principais objetos motivadores, sendo estas a definição de dado pessoal, dado pessoal sensível e dado anonimizado presentes na Quadro 1.

Quadro 1 - Definição de dados pessoais e dados pessoais sensíveis

INCISO	DEFINIÇÃO
I - Dado pessoal	informação relacionada a pessoa natural identificada ou identificável;
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;
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;

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD)

A partir das definições, torna-se elementar que o conceito de dado pessoal para a LGPD é mais abrangente do que nomes, dados biométricos, endereços ou carteiras de identidade. Sendo imperativo considerar a correlação de diferentes tipos de dados, visto que segundo Maciel (2019, p. 18) “Há dados que sozinhos não podem identificar uma pessoa, porém quando agregados a outros passam a ter essa capacidade”, assim, sendo considerados objetos de interesse para a lei.

Observa-se que tanto a LGPD quanto a GDPR não possuem em seu texto qualquer tipo de lista que traga exemplificações de dados pessoais, sendo necessário que para a análise e avaliação, o contexto deve sempre ser levado em consideração (MALDONADO, 2019).

Compreendendo os tipos de dados que a LGPD observa como factíveis ao seu escopo, é possível identificar os dados que não estão incluídos ao mesmo. Além daqueles que não possuem relação direta ou indireta a um indivíduo, os dados que passam por um processo de anonimização, sendo este o procedimento descrito como a “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” (BRASIL, 2018).

Tornando-se evidente que os dados que passarem por recursos técnicos considerados razoáveis, objetivando a descaracterização e desassociação, eliminando assim toda e qualquer possibilidade de identificação do titular dos dados, não serão compatíveis com a definição de dados pessoais, portanto, não afetados pela LGPD.

2.1.3. Os agentes de tratamento e o encarregado

De acordo com a Lei Geral de Proteção de dados, os agentes de tratamento são o controlador e o operador. Sendo que as definições de ambas também se encontram no artigo 5º, como apresentados na Quadro 2.

Quadro 2 - Controlador e operador de dados

INCISO	DEFINIÇÃO
VI - Controlador	pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - Operador	pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD)

Ambos controlador e operador deverão ser juridicamente responsabilizados por garantir além da segurança, a privacidade dos dados pessoais que são objetos de tratamento. Sendo implicitamente de competência do controlador, além de tomar as decisões referentes ao tratamento, habilitar e executar a fiscalização e auditoria das ações do operador que opera em seu nome.

É importante reconhecer, que ao caso dos agentes de tratamento, o requisito de ser uma pessoa física não se aplica, sendo regular a definição de uma empresa, comitê ou grupo de trabalho para desempenhar este papel (DONDA, 2020).

A figura do encarregado de dados, recentemente oficializado o título de *Data Protection Officer* (DPO), é outra definida neste mesmo artigo e que desempenha papel fundamental no contexto da LGPD. Sendo de responsabilidade dos agentes de tratamento a indicação de uma pessoa ao cargo de DPO, “para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” (BRASIL, 2018).

2.1.4. Escopo, abrangência e exceções

O escopo da Lei Geral de proteção de Dados Pessoais torna-se explícito em seu Artigo 1º, definindo a sua aplicação em tratamento de dados pessoais feitos por pessoa natural ou jurídica, de direito público ou privado, ressaltando a inclusão daqueles tratados tanto em meios físicos quanto nos digitais:

> Art. 1º Esta lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Neste contexto, é fato que o destinatário da proteção é o indivíduo titular dos dados, estando este resguardado em toda situação em que seus dados pessoais sejam o objeto de um tratamento irregular, efetuado por qualquer pessoa física ou jurídica, pública ou privada (COTS; OLIVEIRA, 2019, p. 42).

Então pode-se dizer que a LGPD “mira a transparência das relações, bem como busca outorgar aos usuários (pessoas naturais) uma proteção contra eventuais violações de seus dados pessoais” (FONTENELLE NETO, 2020, p. 55).

O Art. 3º trata sobre a abrangência da nova legislação, definindo a amplitude de sua aplicação a todo tratamento de dados realizado por pessoa natural ou jurídica de direito público ou privado, independente do país sede, 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; ou
>
> III - os dados pessoais objeto do tratamento tenha sido coletados no território nacional (BRASIL, 2018).

A partir do artigo 3º da LGPD, é percebido que a superfície de atuação da Lei 13.709/2018 tem alcance extraterritorial, e nas palavras de Donda (2020, p.17) sendo aplicável aos tratamentos executados em território nacional, ou em caso dos dados, objeto alvo de tratamento, tiverem sido coletados em território nacional, independendo da localização da sede da empresa ou dos países aos quais os dados sejam transportados.

Existem, também, as exceções, onde as normatizações da Lei Geral de Proteção de Dados não se aplicam, estas estão explícitas no Art. 4º da legislação, onde Donda (2020, p. 18) sintetiza que:

> “[…] a lei não se aplica na coleta e no tratamento de dados pessoais por pessoa natural e para fins particulares, jornalísticos, artísticos e também para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.”

2.1.5. Premissas e hipóteses

O conceito de tratamento de dados para a LGPD é uma caracterização muito abrangente, englobando toda e qualquer tipo de operação realizada em dados pessoais durante todo o seu ciclo de vida, sendo exemplificado no texto da lei como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

E para que se possa existir as hipóteses de tratamento, é preciso de antemão, se enquadrar nos princípios definidos, estes devem ser seguidos pelos agentes de tratamento no âmbito de operações e atividades enquadradas como tratamento de dados pessoais. O Artigo 6º é o responsável por definir estas premissas básicas que devem ser levadas em consideração para o tratamento de dados pessoais legítimo, sendo estas listadas:

> 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;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> 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;
>
> 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;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> 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;
>
> 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;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

A adequação às premissas é requisito para que se habilite as hipóteses para o tratamento dos dados pessoais. A lei apresenta estas condições, que são requisitos primordiais para o tratamento de dados pessoais feito por pessoa natural ou por pessoa jurídica de direito público ou privado. Importante deixar claro que tais hipóteses não possuem um nível hierárquico ou ordem de precedência, todas legitimam o tratamento de dados, desde que os princípios previstos sejam cumpridos (DONDA, 2020).

> Art. 7º 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 no 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, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
>
> 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.

É de grande valia destacar que o cumprimento de ao menos uma das hipóteses é requisito para que se tenha o tratamento de dados, entretanto, isso não significa que o tratamento de dados será realizado durante tempo indeterminado. Ao término da

finalidade prevista, o tratamento do dado em questão deverá ser interrompido, a mesma medida é aplicável para revogação do consentimento por parte do titular.

De acordo com Oliveira e Lopes (2019, p. 75), referido dispositivo traz em seu bojo o princípio da necessidade, segundo o qual os dados coletados são restritos ao estritamente necessário para a finalidade informada, podendo ser eliminados mediante requisição do titular ou cessado o tratamento, isto é, quando os dados deixam de ser necessários.

Este princípio torna-se contundente na seção IV, no Art. 15º, este que trata das hipóteses para o término do tratamento de dados, sendo permitida a paralização nas seguintes considerações: Término do período de tratamento, cumprimento da finalidade para qual os dados foram coletados ou a mando do órgão fiscalizador. Também está previsto o direito a revogação por parte do titular quando o tratamento de seus dados pessoais é feito baseando-se no consentimento.

A LGPD reconhece que, para que o cidadão seja capaz de controlar o fluxo de seus dados pessoais, é necessário lhe atribuir certos direitos subjetivos em face daqueles responsáveis pelo controle de tais dados (FEIGELSON; SIQUEIRA, 2019).

2.2. BLOCKCHAIN

Conceituada em novembro de 2008 com a publicação do artigo Bitcoin: *A Peer-to-Peer Electronic Cash System,* que tem autoria sobre um pseudônimo denominado Satoshi Nakamoto, a *blockchain* é uma das tecnologias emergentes que estão em alta no mercado global, isso é devido a sua gama de aplicabilidade em diversos setores da indústria e a expectativa de grande valor criado em seu uso.

Esta tecnologia implementa uma rede *peer-to-peer* (P2P) de armazenamento distribuído, sendo suas principais características a confiabilidade, a resiliência, a imutabilidade dos dados armazenados e a transparência para com as partes interessadas. A *blockchain* pode ser definida como um banco de dados distribuídos onde cada nó armazena um conjunto de blocos, e cada bloco da cadeia aponta para o seu antecessor (NAKAMOTO, 2008).

2.2.1. Relação entre Blockchain e Criptomoedas

Apesar de amplamente divulgada juntamente das criptomoedas (moedas digitais), a *blockchain* e o bitcoin não são sinônimos, na verdade, a *blockchain* é a tecnologia que torna possível todo o ecossistema de grande parcela dos criptoativos disponíveis hoje.

O ecossistema do Bitcoin tem sua própria rede *blockchain* pública, esta tem a função parecida a de um livro contábil, registrando as transações processadas. Cada participante da *blockchain*, denominados “nós”, possui uma cópia do livro de registros, tendo livre acesso para verificar todas as transações já realizadas. Emília Malgueiro Campos (2018, p. 20-21) sintetiza que:

> Na Rede Bitcoin, as transações são agrupadas para validação em blocos e esses são ligados entre si por *hashes*, ou seja, códigos-criptográficos representados por um conjunto de caracteres alfanuméricos, por isso o nome *Blockchain*, ou cadeia de blocos. [...] cada bloco possui em sua configuração o número de *hash* do bloco anterior, formando um encadeamento entre os blocos.

Neste mesmo contexto, o sistema de prova de trabalho é o utilizado na rede *blockchain* do Bitcoin. Alguns dos nós participantes das redes podem voluntariamente contribuir para a rede na função de “mineradores”, competindo para decifrar o “*puzzle*” de cada bloco primeiro. Após decifrar, a resolução do bloco é validada, junto as transações nele presente, pelos demais nós, sendo necessária a aprovação de mais da metade dos participantes para ser aceito na cadeia de blocos (KOTAMRAJU, 2019).

O nível de dificuldade para a resolução de cada bloco é ajustado conforme o *nonce*, este é um número de 32 bits que é alterado continuamente pelos mineradores, a fim de encontrar o valor correto que atenda o requisito para a geração do *hash* deste bloco.

Uma vez que um bloco é aprovado pelo montante necessário de participantes, os nós aceitam o bloco e os integram a sua cópia da cadeia de blocos. Sendo o responsável pela resolução do bloco recompensado em um valor de criptomoedas pelo uso de seus recursos computacionais.

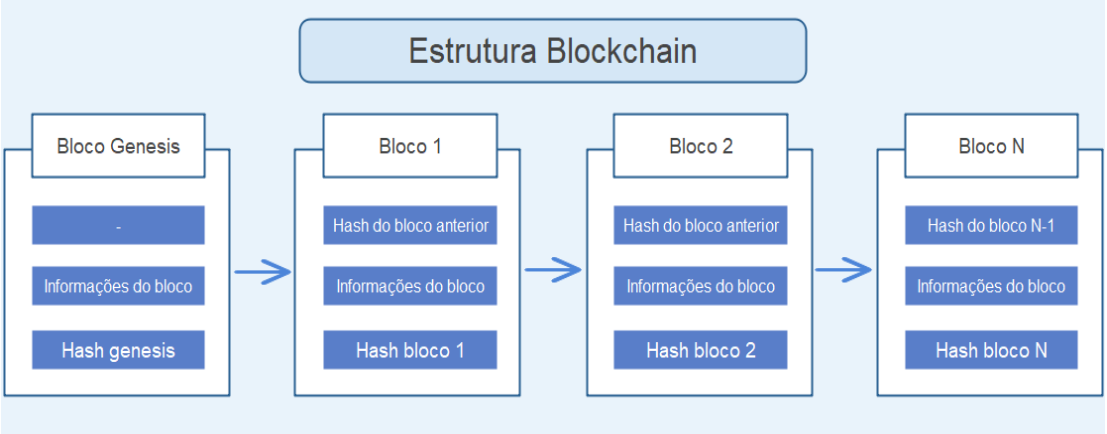
Muitas vezes falsamente apresentadas com a característica de anonimidade total, as cadeias utilizadas como plataforma para as transações de criptoativos podem carregar dados considerados como pessoais, no contexto em que estes podem identificar o titular daquela transação registrada. O uso das chaves pares de chaves assimétricos utilizados nas operações são um exemplo de um possível dado pessoal armazenado como informação de uma transação registrada em um bloco.

2.2.2. O encadeamento dos blocos

Lucena e Henriques (2016) explicam que a *blockchain* utiliza a função *hash* com o intuito de impossibilitar modificações dos arquivos digitais armazenados dentro deles, além de cada novo bloco utilizar a saída (*output*) da função do bloco anterior para gerar um novo bloco, interligando todos os blocos.

A interligação entre os blocos é o que caracteriza o encadeamento. Este se inicia no bloco gênesis, que é o primeiro bloco que será minerado e validado na rede. A partir deste bloco os próximos constituintes da cadeia são gerados, sendo que, cada novo bloco leva em sua composição o valor de *hash* referenciado do bloco anterior (FIGURA 1).

Figura 1. Estrutura do encadeamento dos blocos



Fonte: QUEIROZ (2020, p. 22)

Esta interação entre os blocos, juntamente a descentralização dos blocos, funcionam como uma camada de segurança, evitando que um bloco alterado de forma

maliciosa por um dos nós seja validado e adicionado a *blockchain*. Todo bloco terá sua resolução avaliada, e caso um *hash* inválido seja identificado, o bloco é imediatamente invalidado. Isso é possível devido as validações independentes feitas por cada nó, resultando em um consenso decentralizado para cada transação realizada (NAKAMOTO, 2008).

Devido a esta característica de inter-relacionamento dos blocos, caso seja necessário a alteração em um bloco já validado, é imperativo que este e todos os blocos subsequentes sejam minerados novamente, de forma a serem revalidados e estarem em *compliance* com o protocolo da rede (BROWNWORTH, 2016).

Essa medida de segurança é extremamente eficaz, a menos que um agente malicioso tome controle de mais da metade dos nós da rede, tendo assim, liberdade para validar e publicar blocos não íntegros aos demais pares.

2.2.3. Funções *hash* criptográfico

As funções matemáticas de *hash* criptográfico unidirecionais tem como entrada um valor de comprimento variável que resulta em uma saída de comprimento fixo (NAKAMOTO, 2008). Este tipo de função é amplamente utilizado como forma de garantia da integridade dos dados, já que qualquer alteração no valor de entrada resulta em uma saída completamente diferente.

Para exemplificar, ao utilizar uma ferramenta web online para calcular o *hash* da frase “Olá, mundo!”, sendo escolhida a função *hash* sha256, tendo como saída o seguinte valor de comprimento igual a 64:

9583b013baa520d3a893c4270d0c67732d7ef1768eb0a13533b4e7b134d4b131

No entanto, ao substituir o carácter de exclamação por um ponto de interrogação, sendo a frase de entrada, “Olá, mundo?”, ao recalcular o *hash*, o resultado de saída, respeitando o comprimento fixo de 64 caracteres, é completamente diferente:

f861ef1576eac45f0275b3a3e9aa53b661639d61f3bb384e62a5cd9cda5eadef

Atualmente, não existe meios conhecidos de se executar uma engenharia reversa de forma a chegar na entrada original de uma função *hash* criptográfica. Assume-se que os algoritmos de *hash* evoluem na mesma linha em que os algoritmos responsáveis por os quebrar (KOSBA, 2016).

2.2.4. Tipos de *blockchain*

A *blockchain* pode ser classificada em três categorias, sendo estas: públicas, privadas e híbrida.

Como Alves (2018, p. 6) bem aponta, “uma *blockchain* pública, como o próprio nome sugere, é uma rede *blockchain* que tem suas informações abertas ao público e permite a participação de qualquer usuário como nó no processo de consenso”.

Este tipo de cadeia de blocos, também conhecida como “não permissionada”, é descentralizada e não sujeita a uma entidade central, dessa forma as decisões são tomadas a partir de um protocolo em comum. Para garantir a integridade dos dados entre os pares em uma rede P2P, primeiro é preciso que estes determinem e concordem o que é dado é válido (NAKAMOTO, 2008).

Um exemplo de protocolo implementado em *blockchains* públicas é onde os dados somente podem ser modificados, e que o estado da *blockchain* somente pode ser atualizado, para alterar novos dados mediante consenso de mais de 50% (cinquenta por cento) dos usuários da rede (REVOREDO, 2019a).

As cadeias de blocos privadas, também denominadas como “permissionadas”, geralmente possuem uma entidade central e os participantes devem ser pré-aprovados e restritos ao contexto da *blockchain* para participar. Neste tipo de *blockchain*, o algoritmo utilizado para aprovar mudanças é variável, não sendo obrigatório o uso do consenso.

Por fim, as chamadas cadeias híbridas mesclam características das *blockchains* privadas e públicas. Um cenário onde este tipo se torna aplicável, por exemplo, onde duas ou mais empresas criam em conjunto uma rede *blockchain*, sendo estas as detentoras dela, possibilitando ou não direitos de acesso e modificação ao público (ALVES, 2018).

A grande flexibilidade existente nesta tecnologia possibilita a exploração de novas formas de uso para solução de problemas em vários âmbitos, com isto, novos tipos de *blockchain* emergem, cada um destes com particularidades desenvolvidas para atender as necessidades estabelecidas.

2.3. A RELAÇÃO ENTRE LGPD E BLOCKCHAIN

Existe uma relação pontual evidente entre a tecnologia de cadeia de blocos e a Lei Geral de Proteção de Dados, o art. 18 da lei é o que onde estão definidos quais são os direitos do titular dos dados, mais precisamente no inciso VI, que garante o direito a eliminação dos dados pessoais tratados baseando-se no consentimento do titular, excetuando as hipóteses previstas no art. 16, que autorizam a retenção dos dados para fins de cumprimento de obrigações legais do controlador do dado, estudo por órgão de pesquisa, transferência a terceiro ou para uso exclusivo do controlador, e desde que os dados estejam anonimizados.

Destaca-se que conforme disposto no Art. 8, parágrafo segundo da Lei Geral de Proteção de Dados:

> O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei (BRASIL, 2018).

Dentro deste contexto, a inabilidade de apagar os registros de uma *blockchain* pública pode impedir o exercício do direito garantido ao titular dos dados, pois como bem define Rebelo (2019) em princípio todos os dados lançados no *blockchain* seriam tendencialmente indestrutíveis, imutáveis e impassíveis de modificações.

Há também uma possível inadimplência com o inciso III do Art. 18, que habilita o titular de dados a requisitar ao controlador a correção de dados incompletos, inexatos ou desatualizados.

2.4. ALTERNATIVAS PARA O TRATAMENTO DE DADOS PESSOAIS ALINHADOS A TECNOLOGIA BLOCKCHAIN

A continuidade da adoção da tecnologia blockchain nos processos de tratamento de dados pessoais das empresas, depende imensamente da capacidade de adequação com a LGPD, assim como com as demais leis aplicáveis.

Com a identificação da possível problematização no que tange a relação entre os dois objetos em mãos, é pertinente olhar para o mercado atual e avaliar as possíveis soluções que ajustadas ao contexto da LGPD, podem atuar como objeto de suporte a conformidade.

2.4.1. Armazenamento *Off-chain*

Em alguns casos em que não é possível garantir os direitos dos titulares de dados e o armazenamento dos dados pessoais é imprescindível para o negócio, uma opção viável é o armazenamento fora da *blockchain*, isto é, um banco de dados a parte.

Desta forma, com os dados pessoais armazenados fora da cadeia de blocos, é possível cumprir com o direito do titular de retificar ou apagar seus dados quando objeto de tratamento de dados (REVOREDO, 2019b).

2.4.2. Armazenamento em *Side-chain*

Há também uma outra abordagem além do armazenamento *off-chain*, esta seria o uso de uma *sidechain*, que em tradução livre seria “cadeia lateral”. Na prática, a *sidechain* é uma *blockchain* independente que roda de forma paralela a *blockchain* principal. Essa cadeia lateral, pode adicionar recursos à cadeia principal, sem necessariamente criar uma nova *blockchain*, visando aumentar sua velocidade e aspectos a respeito da privacidade (MEHTA; AGASHE; DETROJA, 2019).

Neste modelo, a *blockchain* considerada como “principal” armazena apenas um *hash* que trabalha como uma espécie de ponteiro para um bloco na *sidechain*, sem revelá-lo, teoricamente atendendo aos parâmetros estabelecidos na GDPR e, também pela LGPD (BAIÃO, 2020).

No momento em que a informação necessitar ser alterada ou excluída, é possível reindexar o *hash* para outro bloco, onde o dado encontra-se retificado, ou desindexá-lo completamente, privando-o de qualquer referência, tornando-o inacessível.

2.4.3. Provas de conhecimento nulo

Esta é uma técnica criptográfica usada para aumentar a privacidade das comunicações, sendo este base para muitos protocolos complexos. Como introduzido e exemplificado por Schwerin (2018, p. 68):

> “O uso das provas de conhecimento nulo [...] habilitam a validação de dados pessoas através de um resultado binário. O resultado demonstra se a informação é aprovada por uma série de regras predefinidas. Um exemplo é a prova de idade de uma permissão para dirigir que não iria requerer o da idade, mas ao invés disto, somente um “Sim” ou “Não” indicando se o indivíduo tem permissão ou não. A idade real se mantém privada”.

Desta forma, entende-se que a descaracterização do dado pessoal habilita o atributo de dado anonimizado, deixando de ser um objeto de interesse para a LGPD. Como já destacado, o art. 12 da lei define que “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”.

Destacando-se a necessidade de avaliação da aplicabilidade, já que, em certas circunstâncias, mesmo este resultado binário pode ser utilizado como forma de identificação do proprietário do dado pessoal, invalidado a atribuição de dado anonimizado.

3. CONCLUSÃO

A elaboração de uma lei que trata da proteção dos dados pessoais de indivíduos foi imprescindível para a adequação do país aos novos requisitos globais resultantes da reformulação do tema adotadas por múltiplas nações. Porém, a introdução dos requisitos previstos no texto da lei ao contexto das tecnologias já atuantes no mercado é vista de forma incerta. A tecnologia escolhida como objeto de estudo deste trabalho, a *blockchain*, é uma entre outras tecnologias que são afetadas diretamente pelas legislações de proteção de dados.

O intuito geral deste trabalho foi introduzir e analisar a relação entre os objetos de estudo, através de pesquisas bibliográficas. Deste objetivo foi possível identificar um ponto conflitante chave entre os temas, a característica de imutabilidade dos blocos na *blockchain* e a necessidade de se corrigir e/ou excluir dados, sendo este direito garantido na LGPD ao titular dos dados, portanto, mandatório.

O próximo objetivo foi identificar possíveis alternativas que possibilitassem o alinhamento entre a LGPD e a tecnologia de cadeias de blocos tratando-se do conflito identificado anteriormente. Como resultado obtido das pesquisas propostas, foram identificadas três hipóteses onde o tratamento de dados pessoais poderia ser feito em conformidade com a lei, sendo estas através do uso de tecnologias e conceitos já presentes no mercado, o armazenamento *off-chain*, o armazenamento em *side-chain* e o uso da prova de conhecimento nulo.

3.1. LIMITAÇÕES

Baseada na lei da União Europeia GDPR, a lei variante brasileira LGPD, se comparada as demais leis relacionadas, é relativamente nova, assim como o tema a que se refere. Durante a execução deste trabalho, foram percebidos os seguintes bloqueios que atuaram como limitadores:

- A escassez de conteúdo específico que trate da relação entre a LGPD e a tecnologia *blockchain*. Dificultando a pesquisa e a formulação de hipóteses para a resolução da problemática.

- No decorrer da revisão bibliográfica, não foram encontrados materiais de pesquisa que introduzissem a aplicabilidade prática das soluções propostas.

3.2. PROPOSTAS PARA TRABALHOS FUTUROS

Analisando os resultados das pesquisas e o as limitações identificadas, a parcela colaborativa deste trabalho pode ser acrescida futuramente:

- Pesquisa prática-teórica da aplicabilidade das alternativas de adequação propostas neste trabalho, explorando e avaliando pontos como dificuldade na implementação, custo e eficácia na adequação com a lei.
- Uso da tecnologia de *blockchain* como ferramenta de auxiliadora na conformidade com a LGPD.

4. REFERÊNCIAS BIBLIOGRÁFICAS

Alves, P. H. et al. **Desmistificando blockchain: Conceitos e Aplicações**. Computação e Sociedade. Rio de Janeiro: Sociedade Brasileira de Computação, 2018. p. 1–24.

BAIÃO, Renata Barros Souto Maior. Afinal, blockchain é incompatível com a LGPD? **Serpro**, 2020. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/blockchain-lgpd-dados-pessoais-brasil>. Acesso em: 07 de setembro de 2021.

BRASIL, Presidência da República. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Diário Oficial da União.

BROWNWORTH, Anders, **Introdução a Blockchain - Uma demonstração visual**. Youtube. 5 de nov. de 2016. 1 vídeo (17:49 min). Disponível em: <https://www.youtube.com/watch?v=_160oMzblY8>. Acesso em: 07 de setembro 2021.

CAMPOS, Emília Malgueiro. **Criptomoedas e Blockchain: O Direito no Mundo Digital**. Rio de Janeiro: Lumen Juris, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de dados pessoais comentada. 2**. ed. São Paulo: Revista dos Tribunais, 2019

DONDA, Daniel. **Guia prático de implementação da LGPD**. São Paulo: Labrador, 2020, 144 p.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral deproteção de dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019.

FONTENELLE NETO, José Edilson da Cunha. **Proteção de Dados Pessoais: uma leitura para além do direito à privacidade**. Florianópolis: EMais, 2020.

KOSBA, Ahmed. et al**.“Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,”** in Security and Privacy (SP), 2016 IEEE. 2016, p. 839–858.

KOTAMRAJU, Prasanna. What is a Nonce in Blockchain? **Tutorialspoint**, 2019.

Disponível em <https://www.tutorialspoint.com/what-is-a-nonce-in-block-chain>. Acesso em 07 de setembro de 2021.

LUCENA, Antônio Unias de; HENRIQUES, Marco Aurélio Amaral. **Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum**. In: IX Encontro de Alunos e Docentes do DCA/FEEC/UNICAMP, 9, 29-30 de setembro, Campinas, São Paulo, 2016. Disponível em <https://www.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcaix/artigos/lucena_henriques.pdf>. Acesso em: 13 maio 2020.

MACIEL, Rafael Fernandes. **MANUAL PRÁTICO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (Lei no 13.709/18).**: atualizado com a medida provisória no 869/18. Goiânia: RM Digital Education, 2019.

MALDONADO, Viviane Nóbrega (coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais. manual de implementação.** São Paulo: Revista dos Tribunais, 2019.

MEHTA, Neel; AGASHE, Adi; DETROJA, Parth. Buble or Revolution? **The Present and The Future of Blockchain and Cryptocurrencies.** Seattle: Paravane Ventures, 2019.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system. Working Paper**, 2008.

OLIVEIRA, Marco Aurélio Belizze de; LOPES, Isabela Maria Pereira. **Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 53-83.

REBELO, Maria Paulo. **OS DESAFIOS DO RGPD PERANTE AS NOVAS TECNOLOGIAS BLOCKCHAIN**, Revista de Bioética y Derecho, Universitat de Barcelona, 2019.

REVOREDO, TATIANA. **Blockchain como uma arquitetura reguladora: smart contracts como ferramenta ao direito**. In: Revista Criptomoedas e Blockchain Descomplicadas para Advogados. v. 01. n. 01. São Paiulo: Enalaw, 2019a. p. 13-37.

REVOREDO, Tatiana. **Blockchain: Tudo o que você precisa saber.** 1. ed. São Paulo: The Global Strategy, 2019b.

QUEIROZ, Daniel Rodriguez. **OS CONFLITOS ENTRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A TECNOLOGIA *BLOCKCHAIN***. Goiânia, 2020. 38 p. Monografia (Bacharelado em Engenharia de Computação) - Pontifícia Universidade Católica de Goiás.

SCHWERIN, Simon. **Blockchain and Privacy Protection in Case of The European General Data Protection Regulation (GDPR): A Delphi Study**. Berlim, 2018 76 p. Berlin School of Economics and Law, Germany.