A relação da Lei Geral de Proteção de Dados e Smarts Contracts gerados por blockchain nas empresas

Denilson Dayson Morais Alves

Jurista com ampla experiência em diversas áreas do Direito, tanto na forma contenciosa como na preventiva, possuindo sua graduação pelo Centro Universitário Uninovafapi. Pós-Graduando em Direito Tributário, Pós-graduando em Prática Trabalhista e Previdenciária e MBA em Gestão Jurídica da Saúde.

Albert Vinicius Furtado Cavalcante

Bacharel em Direito pelo Centro Universitário Uninovafapi.

Cléa Mara Coutinho Bento

Possui mestrado em Direito pela Universidade Católica de Brasília (2012) e doutorado em Direito pelo Centro Universitário de Brasília (2020). Atualmente é professora do CENTRO UNIVERSITÁRIO UNINOVAFAPI. Tem experiência na área de Direito, com ênfase em Direito, atuando principalmente nos seguintes temas: celíaco. consumidor. políticas públicas e restrições alimentares. acessibilidade atitudinal. Advogada, Mediadora Judicial e Assessora na SEED/PI.

A RELAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS E *SMARTS CONTRACTS* GERADOS POR *BLOCKCHAIN* NAS EMPRESAS

RESUMO

A presente pesquisa objetivou apontar a ausência de regulamentação adequada nos *Smart Contracts* gerados pela tecnologia *blockchain* no que se refere à inviabilidade técnica de exclusão desses dados, como tutela a Lei Geral de Proteção de Dados (LGPD). Para tanto, valeu-se de uma revisão bibliográfica e documental. Da pesquisa evidenciou-se a importância da LGPD na contemporaneidade quanto à preservação dos direitos fundamentais. Foi delineado o funcionamento da criptografia presente nos contratos digitais e a funcionalidade dos *Smart Contracts* para apontar a inaplicabilidade do direito à exclusão de dados. Constatou que a proteção jurídica introduzida pela LGPD, no que se refere ao direito do titular quanto à exclusão de seus dados é ineficiente nesses novos contratos tecnológicos. O estudo apontou como mecanismo alternativo para eliminação dos dados dentro do sistema de *blockchain* e *smart contracts*, a prévia criptografia dos contratos inteligentes antes de implantá-los na *blockchain*, de forma que apenas os participantes que estão envolvidos naquele contrato específico podem acessar o conteúdo, usando suas chaves de descriptografia. Concluiu-se pela necessidade de ampliação da proteção de dados pessoais compatíveis com a tecnologia utilizadas nos *Smarts Contracts*, gerados pela *blockchain*, por se tratar de um novo o processo de inovação tecnológica.

Palavras-chave: Lei Geral de Proteção de Dados. Direito à Exclusão de Dados. Blockchain. Smart Contracts.

1 INTRODUÇÃO

Ao longo da história as transformações na sociedade são constantes, muitas delas impactaram a própria ação humana e a forma das relações sociais, o que consequentemente passou a exigir alterações nas relações jurídicas e no ordenamento jurídico.

Na atualidade do modelo das relações sociais no meio digital, o uso da inteligência artificial passou a ser ferramenta de otimização da economia de mercado, passando o domínio da informação a ser objeto de comercialização e de interesse de empresas, com a finalidade de modernização, eficiência em suas atividades e consequentemente otimização do lucro.

No mercado de oferta de bens e serviços de consumo, a informação sempre foi elemento essencial, com a digitalização e uso da inteligência artificial e o armazenamento exponencial dos dados dos consumidores; questões envolvendo manipulação desses dados acabaram fomentando a discussão jurídica acerca dos limites de divulgação dessas informações por parte das empresas, de forma a assegurar o respeito à privacidade, aos direitos fundamentais de inviolabilidade da intimidade da honra, da imagem e da vida privada.

Ao proteger a imagem e os dados pessoais, objetiva-se a preservação de como o indivíduo é visto e sente-se perante a sociedade. Nesse contexto, sugiram diversas leis, sendo a primeira delas a Lei nª 12.965, de 23 de abril de 2014 (conhecido como o Marco Civil da Internet) em seguida o decreto, que a regulamentou, Decreto nº 8.771 de 11 de maio de 2016 e, mais recentemente a Lei nº 13.709 de 14 de agosto de 2018 a então Lei Geral de Proteção de Dados (LGPD).

A recente LGPD confere poder ao titular dos dados que passa a ter o direito de pedir acesso, eliminação, portabilidade, bloqueio e até mesmo a revogação do consentimento sobre o uso de seus dados e de seus familiares, especialmente se os mesmos estão em situação de vulnerabilidade.

Um direito previsto na LGPD é o direito de exclusão de dados dos bancos de informações digitais, porém a lei em vigor ainda deixa lacunas acerca da impossibilidade de tais atos como o caso dos *smarts contracts* gerados pela tecnologia *blockchain*. É importante destacar que se trata de um fenômeno perfeitamente normal visto que a normatização sempre estará um passo atrás dos desenvolvimentos tecnológicos e sociais, pois somente em decorrência destas que surgem a necessidade da tutela jurisdicional.

Desta forma, o presente artigo tem como objetivo identificar e apontar a impossibilidade da exclusão de dados previstas na LGPD em contratos inteligentes (*smarts contracts*) gerados

pela tecnologia *blockchain*, apontando as consequências e evidenciando problemas jurídicos decorrentes dessa relação contratual.

Portanto, a questão norteadora consistiu em identificar como aplicar a proteção constante na LGPD, quando as empresas utilizam *smarts contracts* gerados por *blockchain* do qual não permitem a exclusão de dados.

Nesse contexto, o objetivo geral foi identificar e apontar a lacuna legislativa da LGPD, em face da omissão sobre a exclusão dos dados em situações de impossibilidade tecnológica, limitando-se apenas a impor a exclusão como um direito ao titular dos referidos dados.

Para atingi-lo, há alguns objetivos específicos: discutir o processo de transformação da legislação brasileira em relação a proteção de dados, contextualização de contratos inteligentes (*smarts contracts*) e a tecnologia *blockchain* como forma de segurança e modernização da atividade empresarial e sua impossibilidade de exclusão de dados; ressaltar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada.

A relevância do tema faz-se pelas constantes inovações tecnológicas que afetam as mais distintas áreas sociais, econômicas e jurídicas, justificando a contínua reflexão e modernização do próprio setor mercantil que busca se manter de forma segura a oferta de bens e/ou serviços, buscando o equilíbrio e respeito aos direitos fundamentais previstos na constituição.

Para responder a problemática e atender aos objetivos delineadas, utilizou-se como estratégia metodológica a pesquisa bibliográfica narrativa por meio de livros, manuais, artigos de revisão, publicações jornalísticas buscando ao decorrer do artigo evidenciar a lacuna legislativa, suas consequências jurídicas e demonstrar a importância da modernização da empresa.

Neste sentido, estruturou-se esta pesquisa em três tópicos, sendo o primeiro uma contextualização histórica do direito e relação dos dados pessoais desde o surgimento da internet até a então última norma regulamentadora em vigor.

2 O CAMINHO LEGISLATIVO A LEI GERAL DE PROTEÇÃO DE DADOS

A rápida evolução das tecnologias e da inteligência artificial proporcionou um mundo totalmente novo onde não existia um amparo jurídico as novas atividades e formas de negócio (LONGHI et al., 2020). Nesse contexto de desenvolvimento tecnológico, as informações passaram a circular com uma rapidez nunca vista, junto dessas informações passaram também a circular os mais diversos tipos de dados dos usuários.

Diante disso, os legisladores pátrios foram aperfeiçoando e criando séries de normatizações com o preceito de garantir os direitos fundamentais à privacidade, da inviolabilidade da intimidade da honra, da imagem e da vida privada.

Com o surgimento da Lei Nº 8.078, de 11 de setembro de 1990, O Código de Defesa do Consumidor - (CDC), normatizou e regularizou o uso dos dados dos consumidores estabelecendo que o consumidor possui o direito a ratificação dos dados quando estes imperfeitos. Surgindo uma das primeiras regulações de dados em que as empresas e empresários devem se atentar aos cuidados aos dados (BRASIL,1990).

Seguindo a sequência da normatização surge a Lei nº 9.296, de 24 de julho de 1996, a Lei de Interceptação Telefônica e Telemática, reconhecendo o direito à privacidade. Restringindo e normatizando como as informações poderiam ser utilizadas em tais circunstâncias. Assomou-se, então, a Lei nº 9.507, de 12 de novembro de 1997 - Lei do Habeas Data, que regulava o direito constitucional ao acesso as informações pessoais (BRASIL, 1996; BRASIL, 1997).

A Lei n° 12.965/2014 conhecida como Marco Civil Da Internet foi um mecanismo legislativo para estabelecer princípios, direitos e deveres que logicamente afetaram as empresas em relação ao uso das novas tecnologias.

Em fomento e aperfeiçoamento chegou-se ao contexto da Lei Geral de Proteção de Dados, a nova lei baseada no sistema de proteção de dados europeu *General Data Protection Regulation, GDPR*, que segundo Maciel (2019, p.350) esta Lei em Fomento busca um "equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade, preocupação cada vez mais em pauta no debate público".

Nota-se que antes da Lei em fomento a regulação de dados era feita de forma espaça em normas, leis e na própria constituição. Agora, com a vigência da LGPD os empresários tanto quanto os titulares de dados têm ao seu dispor uma simplificação de gerenciamento de seus direitos e deveres com a relação de dados.

Ademais a LGPD trouxe princípios enumerados no seu Art. 6º que tramontana o seu funcionamento sendo eles:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> 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).

Com efeito, da transcrição acima, os princípios delineados na LGPD objetivam respeitar e viabilizar o direito do titular dos dados, que assume um papel de protagonismo na relação entre empresa e o titular.

A LGPD deixa claro em seu art. 2º, II, a autodeterminação informativa dos dados, desta forma, o usuário tem direito a decidir como seus dados poderão ser utilizados, podendo, inclusive, optar pela exclusão dos dados, como estabelece o Art. 18 em seu parágrafo VI. *Litteris*:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> [...]
> IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> [...]
> VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. [...] (BRASIL, 2018).

A concessão do uso dos dados exige um processo de guarda e proteção por parte do controlador, responsável pela manipulação dos dados, e uma das vertentes para essa segurança é o uso da tecnologia *blockchain*. Essa tecnologia permite o uso dos dados com um nível de segurança raro e é a presente nos *smart contracts*.

Percebe-se que mesmo sendo a LGPD a mais atual legislação que trata a respeito da proteção de dados ela ainda não é capaz de abranger todas as situações fáticas-econômicas da realidade mercantil que se encontram em constante desenvolvimento e aperfeiçoamento. A Lei impõe uma situação que é incabível em determinadas ocasiões; o direito à eliminação dos dados do usuário. Isto significa que a lei dá o direito ao titular de exclusão de seus dados em contratos gerados pela tecnologia *blockchain* do qual é impossível a exclusão, sendo assim, inaplicável nos *smart contracts*.

Ressalta-se ainda que os *Smart Contracts* não possuem a finalidade de armazenamento de informações dos usuários como meio de enriquecimento, mas sim propiciar uma autonomia nas relações contratuais. Decorrente disto, propiciar maior economia mercantil.

3 A EXCLUSÃO DE DADOS E A INCOMPATIBILIDADE DO DIREITO AO ESQUECIMENTO NA CONSTITUIÇÃO

No Brasil, o direito fundamental à privacidade foi inserido de forma direta, por meio da Constituição de 1988, em seu art. 5º, inc. X: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

Uma das teses que foram levantadas em virtude do direito à privacidade foi a do direito ao esquecimento. O direito ao esquecimento faz-se pela premissa de impedir, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos em meios de comunicação.

Diante disso, o direito constitucional à privacidade abrange também os dados dos indivíduos independentes de sua forma de captação seja de maneira física ou digital. Nesse contexto, a LGPD trouxe a aplicação de princípios que guiam o uso dos dados da maneira mais ética possível possibilitando o direito de exclusão dos dados pessoais.

Importante julgado ocorreu na Espanha e serviu de diretriz para a análise do direito ao esquecimento. “Mario González, cidadão espanhol, moveu, perante a Agencia Española de

Protección de Datos, demanda contra o jornal La Vanguardia Ediciones SL (La Vanguardia) e contra a Google. Em revisão RE 1010606 / RJ Spain e a Google Inc., arguindo violação de sua privacidade e da proteção de seus dados, pois em pesquisa por seu nome em tais provedores de busca encontrava-se informações passadas que desagradavam o autor do desígnio" (RODRIGUES JUNIOR, 2014).

No referido caso, o autor da demanda e da tese estavam em desacordo com informações relacionadas a negativação de seu nome em decorrência de dívidas com a seguridade social espanhola e pleiteava que a busca por seu nome não o levasse mais a informações negativas a respeito às dívidas sociais passadas.

Na demanda espanhola surgiu então a pretensão da existência do direito ao esquecimento no âmbito virtual e em decorrência de razões econômicas. Trazendo ênfase aos contratos inteligentes com *blockchain*, do qual principiologicamente possuem natureza comercial, como se estenderia no Brasil a impossibilidade de exclusão dos dados em virtude da essência do formato de negócio (jurídico)?

O julgado Google Espanha (Caso González) teve forte impacto na percepção do direito, influenciando a doutrina, a jurisprudência e mesmo as pretensões legislativas no Brasil.

Em 2021, o Suprema Tribunal Federal analisou e posicionou-se sobre a possibilidade constitucional da existência do direito ao esquecimento tendo como resultado a incompatibilidade constitucional com a tese.

Sobre o caso que gerou discussão o site jurídico conjur profere breve resumo que permite guiar o entendimento do caso concreto (RODAS, 2021):

> O recurso chegou ao Supremo ajuizado pelos irmãos de Aída Curi, vítima de um crime de grande repercussão praticado nos anos 1950 no Rio de Janeiro. Eles buscam reparação da TV Globo pela reconstituição do caso no programa televisivo "Linha Direta" sem a autorização da família. O programa foi exibido em 2004. Os irmãos de Aída questionam a decisão do Tribunal de Justiça do Rio de Janeiro, que entendeu que a Constituição garante a livre expressão de comunicação, independentemente de censura ou licença. Os desembargadores definiram que a obrigação de indenizar ocorre apenas quando o uso da imagem ou de informações atingirem a honra da pessoa retratada e tiverem fins comerciais. Ainda segundo o TJ-RJ, a Globo cumpriu sua função social de informar, alertar e abrir o debate sobre o caso.
> No Supremo, os ministros reconheceram a repercussão geral da matéria em junho de 2017. A maioria dos ministrou votou para negar o recurso e a reparação pedida. "Casos como o de Aída Curi, Ângela Diniz, Daniella Perez, Sandra Gomide, Eloá Pimentel, Marielle Franco e, mais recentemente, da juíza Viviane Vieira, entre tantos outros, não podem e não devem ser esquecidos", afirmou o relator, Dias Toffoli. Fachin reconheceu a existência, em abstrato, do direito ao esquecimento, mas entendeu que ele não se aplica ao caso concreto. Nunes Marques e Gilma Mendes avaliaram que o direito ao

> esquecimento é incompatível com o Direito brasileiro. Contudo, opinaram que a TV Globo deve indenizar a família de Aída Cury por noticiar de forma vexatória a morte da jovem.

Como se extrai a corte aprovou a tese com repercussão geral com o seguinte dizer: É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais (RODAS, 2021).

Absorve-se do caso a impossibilidade do direito ao esquecimento em relação as informações públicas. Trazendo ao contexto das *blockchain* e dos *smart contracts* não há que se falar em dados expostos. O seu próprio sistema criptográfico permite a segurança de suas informações entre aqueles que fazem parte do negócio em questão.

4 BLOCKCHAIN

Inúmeras mudanças ocorreram na história comercial e elevaram a realidade econômica atual da sociedade. Não foi diferente nas relações mercantis. Mudanças recentes têm reconhecido o fenômeno da descartularização como inerente do setor econômico e aprimorando um dos mais tradicionais princípios dos títulos de créditos. Este é só um dos exemplos de como a tecnologia vem mudando a forma de se ver o Direito.

Como alerta Coelho (2016):

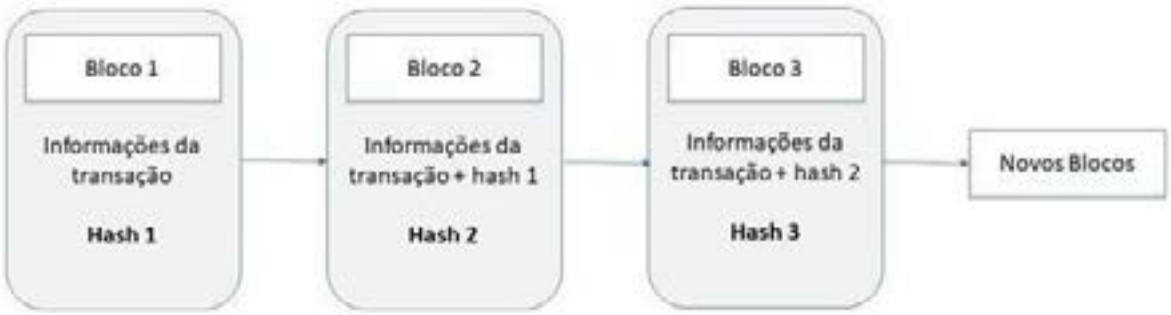
> "os empresários, ao venderem seus produtos ou serviços a prazo, cada vez mais não têm se valido do documento escrito para o registro da operação. Procedem, na verdade, à apropriação das informações, acerca do crédito concedido, exclusivamente em meio eletrônico, e apenas por esse meio as mesmas informações são transmitidas ao banco para fins de desconto, caução de empréstimos ou controle e cobrança do cumprimento da obrigação pelo devedor. Os elementos identificadores do crédito concedido, na hipótese de inadimplemento, são repassados pelos bancos aos cartórios de protesto apenas em meio eletrônico" (Coelho, 2016, p. 459).

Este fenômeno chamado *Legal informatics* tem por objetivo apresentar uma visão geral inédita de informática jurídica, que é uma área do Direito, Tecnologia, Inovação e Economia. Seguindo esse entendimento uma das mais atuais tecnologias que vem sendo inseridas na realidade empresarial é a tecnologia *BLOCKCHAIN*. Pode-se definir *Blockchain* como uma espécie de livro contábil digital, *ledger*, do qual registra as informações por meio de blocos

sucessíveis de informações através de uma criptografia avançada. Cada registro na lista de uma cadeia de blocos possui um *hash*. Este algoritmo possui uma função de converter uma entrada de letras e números, que serve como identificação de um bloco e em uma saída criptografada de forma sucessiva comunicando as informações entre si (TAPSCOTT, 2017).

A título de exemplo segue uma demonstração visual do procedimento na Figura 1.

Figura 1 - O sistema de *blockchain*



Fonte: Dicionário Financeiro, 2021.

Todo esse complexo criptográfico busca a garantia de segurança, atualmente esse sistema de proteção de dados é considerado inquebrável uma vez que para que seja corrompida uma informação presente na cadeia de blocos seria necessário um esforço quase irreal. Pois em se tratando de uma informação contida no sistema ela não poderia ser removida ou alterada, mas somente atualizada no bloco subsequente.

Ainda enumerando as vantagens da tecnologia, pode-se evidenciar a descentralização do sistema que permite uma autonomia com um potencial de uso para as mais diversas atividades com total autonomia. Isto significa que nas palavras de "Uma pessoa terá a capacidade de eliminar o intermediário e os especialistas reformando efetivamente todos os negócios no mundo". Um exemplo que já é de notório conhecimento do uso dessa autônima da tecnologia são as criptomoedas, em especial a Bitcoin hoje mundialmente conhecida e valorizada (ALEXANDRE, 2020).

4 .1 Smart Contracts

Os *Smart Contracts* são softwares refinados com a tecnologia *blockchain* do qual são programados para seguirem determinados comandos estabelecidos previamente quando

circunstâncias se concretizarem de forma autônoma sem vínculo com um terceiro de confiança. Comumente esses contratos possuem um personagem de confiança normalmente uma instituição financeira, como o Banco. Visando eliminar intermediários e facilitar as relações mercantis os *smart contracts* eliminam o terceiro sendo este substituído por um software. Assim sendo, pode ser pensado como um sistema que libera ativos digitais para todas ou algumas das partes envolvidas, uma vez que as regras pré-definidas tenham sido atendidas, caracterizando a autoexecutabilidade dos contratos (CORRALES; FENWUCK; HAAPIO, 2019).

As diferenças na interpretação dos contratos e as falhas na elaboração do contrato são historicamente conhecidas como as principais causas de disputas judiciais. Disputas e resoluções de contratos foram identificadas como os riscos legais mais importantes enfrentados pelas organizações e, apesar das evidências, a adoção de técnicas de aprimoramento das relações continuam por enfrentar barreiras. Estudos também relatam que a maioria das disputas societárias está relacionada a contratos, revelando as correlações entre gastos com litígios e receitas. Além disso, clientes e as empresas desafiam cada vez mais a qualidade, entrega e custos legais de serviços e começam a reconsiderar a necessidade de contratar profissionais nas áreas onde soluções automatizadas podem ser implementadas (NORTON ROSE FULBRIGHT, 2016).

Todo contrato possui suas cláusulas, geralmente, essas versam sobre os mais diversos pontos e possibilidades de circunstâncias de um negócio jurídico. Quando acontece o descumprimento de uma destas cláusulas existe um custo que se move para efetivação do direito ali salvaguardado. Com os *smart contracts*, a efetivação das circunstâncias clausulais é feita de maneira automática. Sendo assim, uma das características mais evidenciada, a autonomia e autoexecutoriedade.

Existem dois tipos de contratos inteligentes, a saber, contratos inteligentes determinísticos e não determinísticos. O *Smart Contracts* determinístico quando executado, não requer nenhuma informação de uma parte externa (de fora do *blockchain*). Um contrato inteligente não determinístico é um contrato que depende de informações de uma parte externa, fazendo a necessidade do oráculo (ALEXANDRE, 2020).

Para efetivação desses contratos alguns elementos fazem parte sendo eles: a assinatura digital, Oraculo, *Peer to Peer*, *Machine to Machine* e *Wallet*. Ao detalhar cada um deles podemos entender melhor o funcionamento destes contratos.

A assinatura digital funciona como uma identificação formal de uma pessoa, empresa ou até mesmo de uma máquina. Baseia-se em um código gerado de forma criptografada. Essa identidade consiste em um aplicativo que faz a verificação de dados e documentos,

comprovando que a pessoa responsável por acessá-lo realmente existe. A comprovação se dá por meio de senha, chaves de segurança, mecanismos de comprovação de identidade, entre outros recursos (ALEXANDRE, 2020).

Oráculo são terceiros que fornecem informações *off-chain*, visto que os contratos inteligentes não podem acessar informações fora do seu sistema. Ou seja, são os responsáveis por alimentar o *blockchain* com informações de fora do sistema (ALEXANDRE, 2020).

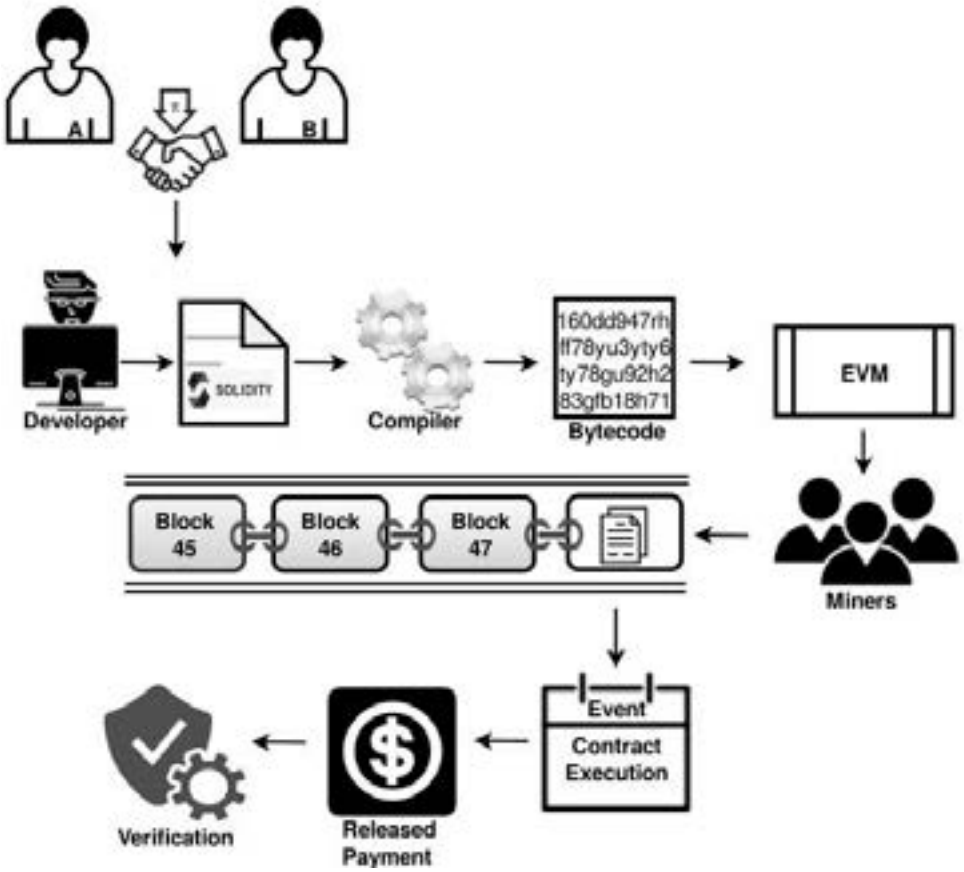
Peer to Peer "é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central" (ALEXANDRE, 2020).

Machine-to-Machine "refere-se a tecnologias que permitem tanto sistemas com fio quanto sem fio a se comunicarem com outros dispositivos que possuam a mesma habilidade" (ALEXANDRE, 2020).

Wallet é uma carteira digital que permite aos usuários armazenar e gerenciar seus ativos (ALEXANDRE, 2020).

Entendendo a forma de criptografia e o funcionamento do sistema dos *smart contracts* é de notável reconhecimento que a codificação e imutabilidade das informações são imprescindíveis para o desenvolvimento da proposta de negócio. Ademais a exclusão dos dados não se ver cabível nesse sistema de negócio uma vez que afetaria toda a essência do negócio, encontrando-se outros mecanismos para aparar a efetivação da proteção de dados do usuário.

Figura 2 - Estrutura de um *Smart Contract*



Fonte: SAYEED; MARCO-GISBERT; CAIRA, 2020

Mister destacar que os objetivos gerais do projeto de *smart contracts* são satisfazer as condições contratuais comuns e minimizar exceções maliciosas e acidentais assim como minimizar a necessidade de terceiros. Os objetivos econômicos relacionados incluem redução de perdas por fraude, custos de arbitragem e execução e outros custos de transação. Evidenciando a inerência tecnológica como meio de otimização das empresas nas suas relações comerciais.

5 CONSIDERAÇÕES FINAIS

Evidenciou-se nesta pesquisa a importância e o avanço normativo que representou a LGPD na contemporaneidade, quanto à preservação dos direitos fundamentais.

No estudo, identificou-se o funcionamento da tecnologia dos contratos inteligentes, gerados pela *blockchain*, enumerando as vantagens mercantis que com ela são disponíveis, apontando o uso dos *smart contracts* como uma ferramenta de autonomia contratual e não como

mecanismo de enriquecimento por uso dos dados dos usuários, demonstrando a relevância do tema que vem transformando a economia mundial.

A partir da análise da proteção vigente, o estudo demonstrou que a proteção jurídica introduzida recentemente pela LGPD, no que se refere ao direito do titular quanto à exclusão de seus dados, é ineficiente nesses novos contratos tecnológicos.

O estudo apontou mecanismos alternativos para eliminação dos dados dentro do sistema de *blockchain* e *smart contracts* que consistem em criptografar os contratos inteligentes antes de implantá-los na *blockchain*, de forma que apenas os participantes que estão envolvidos em um contrato, podem acessar o conteúdo do contrato usando suas chaves de descriptografia, o que amplia a privacidade na guarda desses dados e evita vazamentos despropositais.

Neste sentido, há necessidade de ampliação da proteção de dados pessoais compatíveis com a tecnologia utilizadas nos *Smarts Contracts* gerados pela *blockchain*, por se tratar de um novo o processo de inovação tecnológica.

REFERÊNCIAS

ALEXANDRE, F. **BLOCKCHAIN:** Desvende os segredos da tecnologia blockchain, criptomoedas e o futuro da Internet (Bitcoin, Blockchain & Criptomoedas). Kindle, 2020. ASIN: B08MZ64XB2.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 abr. 2021.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Diário Oficial da União, Brasília, DF, 11 maio. 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 04 abr. 2021.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Diário Oficial da União, Brasília, DF, 25 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 04 abr. 2021.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Diário Oficial da União, Brasília, DF, 13 nov. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 04 abr. 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988, 292 p. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

COELHO, F. U. **Curso de direito comercial**. 18. ed. São Paulo. Saraiva, 2014. Volume I.

CORRALES, M; FENWICK, M; HAAPIO, H (Ed.). **Legal Tech, Smart Contracts and Blockchain**. Springer, 2019. 276 p., ISBN 978-981-13-6085-5.

DICIONÁRIO FINANCEIRO. **Blockchain**: entenda o que é e como funciona de maneira simples. Disponível em: https://www.dicionariofinanceiro.com/blockchain/. Acesso em: 11 maio. 2021.

LONGHI, J. V. R. et al. **Fundamentos do direito digital**. LAECC, 2020. 480 p., ISBN 978-65-99099-21-2.

MACIEL, R. F. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a MP 869/18 eBook Kindle**. 1 ed. RM Digital Education, 2019. ASIN: B07QWHS193.

NORTON ROSE FULBRIGHT RELEASES. **Norton Rose Fulbright releases 2016 Litigation Trends Annual Survey**. Norton Rose Fulbright Releases, 15 de setembro de 2016. Disponível em: http://www.nortonrosefulbright. com/news/142350/norton-rosefulbright-releases-2016-litigation-trends-annualsurvey. Acesso em: 19 abr. 2021.

RODAS, S. **Direito ao esquecimento é incompatível com a Constituição, decide STF**. Consultor Jurídico, 11 de fevereiro de 2021. Disponível em:

https://www.conjur.com.br/2021-fev-11/direito-esquecimento-incompativel-constituicaostf2. Acesso em 13 abr. 2021.

RODRIGUES JUNIOR, O. L. **Direito de apagar dados e a decisão do tribunal europeu no caso Google Espanha**. Consultor Jurídico, 21 de maio de 2014. Disponível em: https://www.conjur.com.br/2014-mai-21/direito-apagar-dados-decisao-tribunal-europeugoogle-espanha. Acesso em 13 abr. 2021.

SAYEED, S; MARCO-GISBERT, H; CAIRA, T. **Smart contract**: Attacks and protections. IEEE Access, v. 8, p. 24416-24427, 2020.

TAPSCOTT, D. **Blockchain revolution**. São Paulo. SENAI-SP, 2017. 392 p.