e³ – Revista de Economia, Empresas e Empreendedores na CPLP
Volume 08 Número 01 | 10.29073/e3.v8i1.611

Check for Updates

Uso da Tecnologia Blockchain no *Compliance* de Dados: uma análise da possibilidade e entraves a serem resolvidos

Application of Blockchain Technology in Data Compliance: an analysis of the possibility and the obstacles to be resolved

Carolina Lanzini Scatolin
Universidade Federal de Santa Catarina – UFSC
carolina.scatolin@advempresarial.com.br

Conflito de interesses: nada a declarar. Financiamento: nada a declarar.

Histórico:
Submissão | Received: 22/03/2022
Aprovação | Accepted: 28/03/2022
Publicação | Published: 31/03/2022

Resumo

Este artigo tem por objetivo analisar a possibilidade da aplicação da tecnologia blockchain nos programas de *Compliance* de dados, de modo a verificar os obstáculos e possíveis soluções destes. Para isso, foi necessário realizar uma análise da Lei Geral de Proteção de Dados (Lei n. 13.709/2018), dos conceitos e elaborações de programas de *Compliance*, além da compreensão geral da tecnologia blockchain, desde a sua origem, as suas características e as possíveis aplicações.

Palavras-chave: *Compliance*, Blockchain, *Compliance* de dados

Abstract

This article aims to analyze the possibility of applying blockchain technology in data *Compliance* programs, in order to check the obstacles and possible solutions of these. To this end, it was necessary to carry out an analysis of the General Data Protection Law (Law no. 13.709/2018), of the concepts and elaboration of *Compliance* programs, in addition to the general understanding of blockchain technology, since its origin, its characteristics and possible applications.

Keywords: *Compliance*, Blockchain, Data *Compliance*

1. Introdução

A migração da sociedade para o ambiente virtual sendo cada vez mais expressiva houve um crescente interesse comercial sobre os dados pessoais, que se tornaram um ativo para o desempenho e aprimoramento de diversas atividades (Cuevas, 2017).

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) (Lei n. 13.709/2018) trouxe mudanças significativas à coleta e tratamento de dados que as empresas realizam. Isso, pois a legislação buscou a proteção dos direitos fundamentais da liberdade e da privacidade da pessoa natural. Trouxe ainda um extenso rol de direitos atribuídos ao titular dos dados, cujo objetivo é dar a ele a efetiva participação na gestão dos dados.

Todavia, o que se busca estudar neste artigo é o fomento que essa legislação trouxe para as ações preventivas, estabelecendo procedimentos mandatórios para os controladores e operadores de dados pessoais, tais como a implementação de políticas severas de segurança para a proteção de dados cujo acesso não é autorizado.

É na preocupação com a inconformidade com a legislação de proteção de dados que os programas de *Compliance* ganham espaço. A implementação de programas de *Compliance* nas empresas além de visar a prevenção de vazamentos de dados e a adequação à LGPD tem por finalidade a combinação de diversos setores da sociedade empresária e a busca pela construção de uma cultura de boas práticas.

Para a implementação e preservação de um programa de *Compliance* de sucesso é preciso que todos os integrantes da sociedade empresária estejam engajados ao programa, principalmente a alta administração. Sem contar a constante busca pelas melhores formas para a adequação às normas vigentes, sempre buscando atualização e melhorias no programa.

Por sua vez, essa constante busca por melhorias de sistema acarreta procura por tecnologias que possam oferecer novas ferramentas para auxiliar – ou não – no cotidiano das sociedades empresariais.

O advento da tecnologia *blockchain*, ainda em 2008 juntamente com a criptomoeda *Bitcoin*, é uma dessas revoluções tecnológicas que trazem anseios e incertezas para as suas aplicações e, paralelamente, para as consequências disto.

O emprego dessa tecnologia vem ganhando espaço nas operações cotidianas, indo além da simples utilização como base para as criptomoedas e em transações financeiras passando para as cadeias de suprimentos para o rastreamento de produtos; na saúde, com o registro imutável do histórico médico; direitos autorais, por meio dos *NFTs*[1]; e como base de dados. Considerando essa última possibilidade, surge a hipótese de se aplicar a *blockchain* em programas de *Compliance* de dados.

Diante disso, o presente artigo tem por objetivo, através do uso do método dedutivo e histórico, analisar a possibilidade da implementação da tecnologia nos programas de *Compliance* de dados. Em seu primeiro capítulo será abordado a Lei Geral de Proteção de Dados e o *Compliance* como meio

[1] *NFT* é a sigla para *non-fungible token*. O token, no universo das criptomoedas, é a representação digital de um ativo – dinheiro, propriedade ou obra de arte – registrada em uma *blockchain*. O *NFT* nada mais é que a representação de um item exclusivo, como um quadro, uma música.

adequação às normativas e construção de cultura de boas práticas.

Já no segundo capítulo será abordado a tecnologia *blockchain* voltada para a tentativa de explicar o que é essa tecnologia tão disruptiva e suas características principais. Para, então, poder ser analisada a possibilidade da aplicação dela nos programa de *Compliance* de dados.

2. Lei geral de proteção de dados e *Compliance* de dados

Antes de mais nada é preciso conhecer quais são as características centrais da Lei de Proteção de Dados (Lei n. 13.709/2018), o conceito de *Compliance* e quais são os elementos de programas de *Compliance* eficazes para, então, identificar qual o papel desse na garantia do cumprimento das normas de proteção de dados.

2.1 Lei geral de proteção de dados – Lei n. 13.709/2018

A Lei Geral de Proteção de Dados, n. 13.709 de agosto de 2018, foi criada em decorrência do grande aumento dos debates em torno dos dados pessoais e do tratamento dado a eles. A legislação brasileira foi inspirada na regulamentação europeia *General Data Protection Regulation* (GDPR). Em ambas o objetivo foi o regramento do tratamento de dados pessoais e a busca de um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade.

Como principais fundamentos para a utilização de dados pessoais, a LGPD traz o respeito à privacidade, a autodeterminação informativa, inviolabilidade da intimidade, da honra e da imagem, livre iniciativa, livre concorrência e a defesa do consumidor, além do desenvolvimento econômico e tecnológico e a inovação (Maciel, 2019).

A LGPD também elenca um extenso rol de direitos atribuídos ao titular dos dados, cuja finalidade consiste na concretização da sua efetiva atuação na gestão de dados. O artigo 18 da LGPD determina que:

> *o controlador deverá atender, de forma gratuita (§5º) às solicitações do titular realizadas mediante requerimento a qualquer agente de tratamento, garantindo-lhe (i) a confirmação da existência de tratamento de dados; (ii) acesso aos dados tratados; (iii) correção dos dados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em contrariedade à lei, ainda que o tratamento seja baseado em hipótese que dispensa o consentimento (§2º); (v) portabilidade; (vi) eliminação de dados tratados sem consentimento, quando esse for necessário ao tratamento; (vii) informação a respeito de com quais entidades houve compartilhamento; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências de negá-lo; e (ix) revogação do consentimento. (Frazão, Tepedino & Oliva, 2019, pp. 678-679).*

Para a realização dessas prerrogativas é necessária existência de regulamentação específica interna, ou seja, dentro da própria

instituição ou empresa, a fim de que sejam determinados os prazos e procedimentos para o atendimento das solicitações e para a implementação do sistema.

Em comparação com a legislação europeia, a brasileira trouxe uma inovação: a exceção à possibilidade da alteração ou exclusão do dado pessoal. Pela lei brasileira não é possível a alteração ou exclusão do dado pessoal quando a finalidade deste dado é fiscal ou quando o tratamento dos dados chegar ao fim – seja pelo cumprimento de sua finalidade, seja porque o usuário revogou seu consentimento, devendo as informações serem eliminadas (Pinheiro, 2021). Isso traz uma preocupação às sociedades empresárias, pois deve-se buscar a redução dos riscos do negócio sabendo que a má utilização dos dados pode acarretar multas e sanções à empresa.

Assim, com a preocupação com a utilização e proteção dos dados pessoais, a legislação brasileira trouxe fomento para ações preventivas de modo que os controladores e operadores de dados pessoais passassem a aplicar medidas de segurança para a proteção dos dados que possuem o acesso não autorizado e ainda evitar o vazamento destes.

Diante deste cenário em que se tem a necessidade da proteção dos dados pessoais e da mudança da forma de tratamento deles, tornou-se imperiosa a adoção de medidas de *Compliance* com o viés de prevenir a violação dos fundamentos da LGPD e auxiliar nas condutas compatíveis com a legislação vigente. Para Danilo Doneda (2006):

> *A proteção dos dados pessoais, embora sempre fundamentada pelo preceito constitucional, deve valer-se de uma estratégia integrada na qual são utilizados diversos instrumentos de tutela, que representam manifestações específicas em diversas áreas de um mesmo direito. A maleabilidade e facilidade de adaptação a novos cenários e à inovação suscitados pela ação da tecnológica é uma característica de instrumentos mais "fracos", como normas deontológicas, códigos de autorregulação e outros, das quais o direito deve se utilizar, especialmente quando os instrumentos tradicionais ao seu alcance podem se demonstrar demasiado lentos ou desproporcionais para uma tutela eficaz (Doneda, 2006, pp. 409-410).*

No meio empresarial, a adequação das sociedades à legislação vigente será uma forma de competitividade entre as empresas e, no âmbito negocial, poderá servir para o aumento da credibilidade no mercado.

Para o cumprimento das normas da LGPD, a implementação de boas práticas no tratamento de dados pessoais é de grande importância. E para isso, é preciso a compreensão da relevância dos programas de *Compliance* e, também, quais suas funções e conteúdo.

2.2. Compliance de dados

Em linhas gerais o *Compliance*, para muitos, é a observância e respeito, dentro de um ambiente, a determinadas regras estabelecidas com a finalidade de evitar ou então mitigar os riscos do negócio. Nas palavras de Ana Frazão, refere-se

> *ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade (Frazão, et al., 2007, pp. 409-410).*

Apesar da conceituação apresentada anteriormente é preciso ressaltar que o *Compliance* vai além da adequação às normas

vigentes no sentido jurídico. Ele abrange a implementação de metodologias aplicadas ao trabalho, políticas de controle de estoque, estratégia de gestão de pessoas, técnica de melhoria contínua, harmonização contábil etc., segundo Endeavor (2021). Assim, verifica-se que o *Compliance*, para ter sua eficácia, necessita ter sua aplicação, em todos os níveis de uma empresa.

Além disso, para muitos, a criação de um programa de *Compliance* é sinônimo de prejuízo, pois traz aos negócios limitações. Todavia, o que ocorre é que esse instituto visa a criação de uma cultura entre todos os colaboradores e, consequentemente, dar confiança à empresa.

E é exatamente no ponto da criação de cultura que, por vezes, é encontrado o problema. Explica-se: antes de iniciar-se um programa de *Compliance* é preciso que os administradores e o alto escalão da empresa abracem a ideia, que vejam os benefícios que essa implementação pode trazer aos negócios e, desta forma, servir de exemplo para os outros níveis da sociedade.

Essa importância é tamanha que a Associação Brasileira de Bancos Internacionais (ABBI) e a Federação Brasileira de Bancos (FEBRABAN), ao se manifestarem sobre *Compliance* afirmaram que:

> *Para que a "Função de Compliance" seja eficaz, é necessário o comprometimento da Alta Administração e que esta faça parte da cultura organizacional, contando com o comprometimento de todos os funcionários. Todos são responsáveis por Compliance. Um Programa de Compliance eficaz pode não ser o suficiente para tornar uma empresa à prova de crises. Mas certamente aprimorará o sistema de controles internos e permitirá uma gestão de riscos mais eficiente. (FEBRABAN, 2009, p.6).*

A aceitação e implementação efetiva dos programas de *Compliance* dependem dos integrantes da empresa, cuja função encontra-se nos mais altos cargos, darem o exemplo seguindo os preceitos do programa e demonstrar que essa criação de cultura trará benefícios a todos.

Faz-se necessário trazer à tona os elementos mínimos para a estruturação de um programa de *Compliance* efetivo – lembrando sempre da necessidade do engajamento de todos os colaboradores, sejam internos ou externos.

Para Frazão, et al., (2019, pp. 687-693), esses elementos mínimos podem ser enumerados em dez pontos: (*i*) avaliação contínua de riscos e atualização do programa (o objetivo é tentar antecipar os riscos e tentar aplicar medidas preventivas proporcionais aos riscos encontrados); (*ii*) elaboração de Códigos de Ética e Conduta (documentos escritos em que constam os valores e princípios da entidade, que devem ser observados por todos); (*iii*) organização compatível com o risco da atividade (é necessário o estabelecimento de procedimentos e controles internos que sejam compatíveis com a avaliação dos riscos); (*iv*) comprometimento da administração (efetivo engajamento da alta administração na execução é essencial); (*v*) autonomia e independência do setor de *Compliance* (o setor deve ter poderes para supervisionar e executar as normas consubstanciadas no programa); (*vi*) treinamentos periódicos (fornecimento adequado aos funcionários para que seja permitida a integral compreensão de todos os envolvidos do comportamento esperados deles); (*vii*) criação de uma cultura corporativa de respeito à ética e às leis (as ações dentro da organização sejam sempre voltadas à observância das normais legais); (*viii*) monitoramento constante dos controles e processos, inclusive para atualização do programa (manter o programa atualizado, a fim

de prevenir e mitigar os riscos, impõe um constante monitoramento); (*ix*) canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes (possibilitar a todos fácil acesso ao esclarecimento de dúvidas e promoção de denúncias, criar confiabilidade dentro dos mecanismos de informação); e (*x*) detecção, apuração e punição das condutas contrárias ao programa (a reação adotada pela organização ao detectar um ilícito demonstra o comprometimento com o programa).

Portanto, nota-se a necessidade da efetiva participação de todos os componentes da organização, começando na alta administração atingindo todos os colaboradores internos e externos, para então alcançar os objetivos traçados no programa de *Compliance*.

2.3. Compliance de dados pessoais

Considerando as características centrais da Lei Geral de Proteção de Dados e do conceito de *Compliance* apresentados anteriormente, identifica-se o papel deste na garantia do cumprimento das normas impostas pela LGPD.

Lembra-se que a LGPD trouxe a mudança da propriedade dos dados pessoais. Hoje a titularidade dos dados é atribuída à pessoa natural e os dados pessoais não são mais tratados como ativos, que poderiam ser comercializados por quem deles se apropriassem. Os princípios trazidos pela LGPD carregam o dever de quem coleta dados de prestar conta ao titular dos dados, sendo que este dever é fundamentalmente gratuito.

A proteção de dados instituída pela LGPD não possui a finalidade de inviabilizar a coleta de dados para conhecimento do público-alvo e aprimoramento da atividade empresarial, ela esclarece que todos os dados coletados para essa finalidade pertencem às pessoas físicas as quais os dados se referem e precisam ser tratados e coletados em respeito a essa relação de pertencimento (Frazão, et al., 2019).

Com a mudança no tratamento dos dados, o *Compliance* de dados pessoais objetiva auxiliar os agentes de tratamento na efetiva aplicação das normas impostas na Lei n. 13.709/2018.

O programa de *Compliance* de dados pessoais passa a demandar uma estrutura com mecanismos direcionados exclusivamente para garantir o respeito às normas instituídas sobre o tratamento destes dados. A exemplo disso, tem-se o artigo 37, com o dever de manter registro de todas as atividades de tratamento realizadas), o artigo 38, da apresentação de relatório do impacto à proteção de dados pessoais, o artigo 46 com a observância das normas de tratamento, as quais em caso de não comprovação induz, automaticamente, à responsabilização e o artigo 50 com a comprovação da efetividade do programa de governança em privacidade que foi adotado – todos esses artigos são da LGPD.

Para a implementação de um programa de *Compliance* que venha a abranger todos os requisitos e princípios da LGPD é preciso saber de todo o fluxo de dados existentes na organização, devendo ser mapeado todo o ciclo dos dados e quais são as suas características.

Deve ser considerado os riscos constantes no tratamento dos dados pessoais, um desses riscos é ter que garantir que o sistema utilizado no tratamento irá permitir o pleno exercício dos direitos dos titulares. Basicamente os dados precisam ser acessíveis pelos titulares, se a tecnologia utilizada nesse tratamento permite o efetivo apagamento e se é possível a identificação de todos os dados de uma mesma pessoa.

Assim, é a partir da identificação dos riscos que as entidades poderão adentrar no segundo passo, já mencionado anteriormente, que é a

elaboração do código de conduta, a fim de especificar os processos adotados pela pessoa jurídica no tratamento de dados (Frazão, et al., 2019).

Além disso, a LGPD traz a necessidade desses dados coletados poderem ser apagados ao mudar o consentimento do titular no tratamento de seus dados. Ou seja, é impositiva o constante monitoramento dos dados tratados a fim de que estes estejam sempre em conformidade com o titular deles.

O artigo 38 da LGPD expressa a possibilidade de a Agência Nacional de Proteção de Dados requerer a emissão de relatório de impacto da proteção de dados pessoais, referente as suas operações de tratamento de dados, o que acaba por impor à organização uma transparência e segurança dos dados inseridos no sistema.

Portanto, para que um programa de *Compliance* de dados pessoais tenha sua efetividade alcançada, além dos requisitos referentes ao *Compliance* em geral, é necessária a observância e implantação de sistemas que respeitem os requisitos e princípios normativos constantes da Lei n. 13.709/2018.

3. Tecnologia *Blockchain*

Quando se fala na tecnologia *blockchain* a primeira informação que vem à mente é o *Bitcoin*. A tecnologia surgiu em 2008, com a publicação do *white paper* de Satoshi Nakamoto intitulado "*Bitcoin: A Peer-to-Peer Eletronic Cash System*" (Nakamoto, 2008). Inicialmente ela era vista como uma forma segura de realizar as transferências que envolviam *bitcoins*.

Entretanto, é preciso ressaltar que a tecnologia *blockchain* e *bitcoins* não são a mesma coisa. O *Bitcoin* é apenas uma das formas de aplicação da *blockchain*. O *Bitcoin* foi apenas o primeiro a usar a tecnologia (Gupta, 2018).

Para Alves et al. (2018, p. 2) a *blockchain* pode ser conceituada como "uma tecnologia que faz uso de uma arquitetura distribuída e descentralizada para registrar transações de maneira que um registro não possa ser alterado retroativamente, tornando este registro imutável".

Para melhor compreender a *blockchain*, é preciso entender que em seu surgimento ela possuía como objetivo a remoção do intermediário nas operações financeiras. Explica-se: no *Bitcoin*, o objetivo da *blockchain* era a retirada do banco como intermediário nas transações. Observa-se que o banco, neste caso, é um a instituição utilizada para dar confiança às partes da transação de que esta será efetivamente realizada.

As instituições são ferramentas utilizadas para diminuir a incerteza e a insegurança da sociedade e conectá-la de modo a efetuar vendas, compras, trocas de todos os tipos de ativos. Com a tecnologia *blockchain* acredita-se ser possível de diminuir essa incerteza e insegurança.

A *blockchain*, em linhas gerais, é uma base de dados descentralizada que armazena o registro de ativos e transações por meio de uma rede ponto a ponto. É um registro público de quem tem o que e quem transacionou o que. As transações são asseguradas por criptografia e com o tempo esse histórico de transações é selado em blocos de dados que estão

criptografados e ligados uns aos autos, ficando assim, seguros. Isso cria um registro imutável e – até hoje – impossível de fraudar.

A *blockchain* não é um aplicativo ou uma companhia, para Bettina Warburg, o mais próximo que se pode ter da *blockchain* é a *wikipedia*, nas palavras dela em uma palestra do TEDx Talks – *How the blockchain will radically transform the economy*:

> *Conseguimos ver tudo na wikipedia. Ela é uma composição que está constantemente mudando e sendo atualizada. Nós conseguimos também rastrear essas mudanças com o tempo e criar nossa própria wikipedia, porque na sua essência, são apenas infraestrutura de dados. Na Wikipedia tem-se uma plataforma aberta, que armazena palavras e imagens e as mudanças dos dados inseridos com o tempo. Na blockchain, pode-se pensar como uma infraestrutura aberta que armazena muitos tipos de ativos. Armazena a história da custódia, propriedade e localização de ativos como, por exemplo, o Bitcoin ou outros ativos digitais como a propriedade de um IP, um certificado, um contrato e até mesmo informações de identificação pessoal (Warburg, 2016).*

Assim, quando voltada para uma visão de que a *blockchain* é utilizada para transações financeiras, de acordo com Dom Tascott and Alex Tapscott (2016, p. 37), a *blockchain* é "um livro-razão distribuído que representa um consenso de cada operação que já ocorreu na rede".

Já para a perspectiva empresarial, tem-se o conceito de que a *blockchain* é uma rede de negócios segura, da qual os participantes transferem ativos, por meio de um *ledger* (livro-razão) comum distribuído, do qual cada participante possui uma cópia, e cujo conteúdo está em constante sincronia com os outros (Castagna, 2020).

Assim, pode-se definir que a *blockchain* é, basicamente, uma base de dados, podendo ser aplicada em diversos setores como, por exemplo, cadeias de abastecimento, transações financeiras, armazenamento de dados e contratos.

A tecnologia *blockchain* vem ocupando cada vez mais espaço nos debates sobre suas possíveis aplicações na sociedade atual. Isso, pois possui características que são cada vez mais relevantes à população. Pode-se citar como principais características da tecnologia *blockchain* a descentralização, a imutabilidade, a transparência, a criptografia e a segurança.

Para melhor compreender essas características, tem-se que a segurança decorre em razão da *blockchain* ser uma base de dados descentralizada, ou seja, cada participante daquela rede possui uma cópia de todas as movimentações já realizadas sendo esta cópia, sempre atualizada por ser sincronizada em tempo real. Além disso, a criptografia envolvida na segurança dos dados inseridos faz com que a segurança do programa se torne ainda maior.

A descentralização, além de trazer segurança, traz maior transparência dos dados, uma vez que todos os dados ali inseridos podem ser acessados a qualquer tempo pelos participantes daquela rede.

A base de dados criada por meio da *blockchain* possui a característica de ser imutável. Isso se dá em razão de a tecnologia encriptar todos os dados inseridos na rede e, juntamente com a informação, deixar marcada a data e a hora da inserção do dado na rede. Com isso, a *blockchain* torna-se uma base de dados encadeados na ordem cronológica.

Ainda, quando há a inserção de novo dado na rede forma-se um novo bloco e, à essa informação, é somada a informação do bloco anterior, de maneira que se forma uma cadeia,

pois todos os dados acabam por ficar encadeados – daí o nome *blockchain*: uma cadeia de blocos – e esses dados, por possuírem informações dos blocos anteriores, acabam impedidos de sofrerem modificações sendo, portanto, imutáveis.

Nota-se que a soma dessas características torna o sistema, até o momento, incorruptível. A exemplo do *Bitcoin*, a operação realizada ocorre em uma rede com inúmeras máquinas computacionais funcionando simultaneamente e compartilhando a mesma cópia da *blockchain*, caso houvesse uma tentativa de falsificação de informação seria rechaçada pelo próprio sistema.

Explica-se: uma vez que todos os blocos possuem uma ordem cronológica e um encaixe sistemático, fundado em cálculos matemáticos complexos, não é possível encaixar uma informação que não possua o encaixe certo. E, para deixar claro, esse encaixe certo só ocorre ao inserir nova informação e não ao tentar alterar a informação já constante.

O que pode acontecer é a alteração de informação na cópia constante em um computador. No entanto, essa modificação não seria realizada na cópia dos outros usuários.

Como consequência das características, conforme André Salem (2018) expôs na TEDx Talks – *Blockchain* e Impacto Social, a *blockchain* apresenta as seguintes vantagens: confiança – por seus registros serem imutáveis e poderem ser verificados por qualquer usuário; *ledger* (livro-caixa) distribuído – o livro-razão, sistema de registro das transações e blocos, é compartilhado por toda a rede, de modo transparente; privacidade – é possível garantir a visibilidade para a rede, já que as transações conseguem ser verificáveis, mas determinados atributos pessoais dos usuários podem ser omitidos, sem comprometimento da verificação de segurança; contrato inteligente – um documento que não pode ser alterado depois de escrito, de modo que se pode firmar contratos e autorizar (ou não) transações de acordo com os termos estabelecidos; e consenso – as transações são verificadas pelos participantes da rede e não podem ser fraudadas, atribuindo segurança ao sistema.

Além disso, essas características permitem a formação de três formas de *blockchain*: pública, na qual suas informações são visíveis a todos e permite a participação de qualquer usuário; privada, a qual possibilita o acesso somente ao grupo criador da *blockchain*, sendo a participação dos usuários definida por este grupo fechado; e híbrida, em que somente um grupo de indivíduos ou organizações que tenham decidido compartilhar informações entre si pode inserir dados, mas a visualização informações seja disponível a qualquer indivíduo ou empresa (Alves et al., 2018).

A tecnologia *blockchain*, portanto, possui características que a tornam viável para a aplicação em diversos setores da sociedade, seja para fins de transação ou para simples base de dados.

4. Uso da tecnologia blockchain no *Compliance* de dados

Com a promulgação da Lei Geral de Proteção de Dados em agosto de 2018, os programas de *Compliance* ganharam espaço nas empresas a fim de adequar o fluxo de dados aos preceitos

da legislação. E ganharam ainda mais destaque na gestão de risco ao analisar possível vazamento ou tratamento em desacordo com a legislação, os quais podem acarretar prejuízos à sociedade empresária.

Assim, a tecnologia *blockchain* que, ainda em 2015, foi considerada pela revista britânica *The Economist* como "*The next big thing*" (2015) gera muita expectativa por suas características e os benefícios que seu uso pode trazer às empresas.

O atrativo que essa tecnologia tem é voltado para a capacidade de transformar muitos processos do cotidiano empresarial em processos mais ágeis, transparentes e, principalmente, seguros, em razão da imutabilidade assegurada pela criptografia. Além da tendência de eliminação dos custos, dos atrasos, dos erros e dos retrabalhos nos processos de gestão de negócios.

Para Hanoff (2020), a consequência da aplicação da *blockchain* é um "melhor desempenho da gestão de riscos corporativos e do monitoramento de conformidade regulatória da organização, ademais da facilitação de auditorias (internas e externas)". Ela ainda complementa que a aplicação da tecnologia serviria como um forte indutor de *Compliance* por impedir a prática de ilícitos a fim de ludibriar fornecedores.

Não só isso, como também a *blockchain* assume papel importante na certificação do cumprimento dos regulamentos e de exclusão da necessidade de um intermediário para atestar e confirmar a existência ou não do *Compliance*.

O *Compliance*, poderia ser desmembrado em três elementos principais: a integridade, a qual diz respeito à honestidade e a confiança de que as informações prestadas são verdadeiras; a conformidade representando o estar de acordo com as legislações e regulamentações vigentes; e a governança, a qual importa independência do conselho, política de remuneração da alta administração, diversidade na composição do conselho de administração, estrutura dos comitês de auditoria e fiscal, ética e transparência.

No caso da integridade a *blockchain* permite que os participantes tenham a certeza de que as informações estão escrituradas e estejam alinhadas aos valores de integridade – honestidade, consideração pelo interesse dos outros, responsabilização pelas consequências de suas decisões e ações e a transparência na tomada de decisões (Tapscott & Tapscott, 2016).

Entretanto, ainda há muitas dúvidas a respeito da aplicação da *blockchain* no *Compliance* de dados, com destaque para a impossibilidade da ingerência de dados – seja pela ausência de um controlador ou pela imutabilidade da tecnologia.

Começando pela ingerência de dados devido a ausência de um controlador deve-se atentar para a característica da *blockchain* de ser descentralizada. Conforme visto anteriormente, a *blockchain* pode ser configurada em diversos níveis de descentralização, podendo ser totalmente pública, em que a descentralização atinge seu grau máximo, em que todo usuário pode fazer parte da verificação e ter acesso a todos os dados. Ou ela pode ser privada, que representam um menor nível de descentralização, entretanto a validação de informações pode ficar mais concentrada.

O nível de descentralização da *blockchain* utilizada é um dos pontos que a torna segura, pois na tentativa de modificar informações constantes, quantos mais usuários fazendo parte da verificação, mais difícil se torna a alteração.

Para muitos, essa ausência de centralização da inserção e verificação das informações na rede

vai de encontro à determinação do artigo 5º, VI da Lei Geral de Proteção de Dados, uma vez que o controlador seriam vários usuários que realizam a verificação das informações, por meio do consenso.

Já a outra característica que pode parecer empecilho para a aplicação da tecnologia *blockchain* nos programas de *Compliance* de dados é a imutabilidade. Ou seja, a capacidade que a tecnologia tem de armazenar, em ordem cronológica e permanente, todos os dados inseridos. O problema encontra-se na determinação do artigo 18, incisos IV, VI e IX, da LGPD, onde se mostra necessário a possibilidade de alteração dos dados inseridos na *blockchain*. Juliana Costa (2020) afirma que:

> *Por esse motivo é fundamental ressaltar que essa funcionalidade não resolve totalmente o processo de gestão empresarial, pois com a LGPD, obrigatoriamente, os dados devem ser mutáveis, não bastando apenas a obtenção de sua guarda e registro, mas também a possibilidade de alteração ou até mesmo de descarte por aqueles que os detém, incluindo-se aí também o chamado "direito ao esquecimento" ou "right to be forgotten", influenciado pelo RGPD europeu. Desse modo, utilizar o blockchain para alocação de todos os dados de uma empresa pode acabar esbarrando nos regramentos legais e atingindo diretamente os direitos fundamentais abrangidos e protegidos pela nossa Constituição (Costa, 2020, p.12).*

Nota-se que ainda há muita restrição à aplicação da tecnologia no âmbito do *Compliance* de dados, exatamente pela característica que fornece segurança. Para isso, uma das soluções que pode ser adotada é que as empresas deixem claro ao fornecer o termo de consentimento, a respeito dos dados a serem coletados e a forma de tratamento, que os dados serão tratados por meio de uma rede *blockchain* e que uma vez inseridos serão permanentemente mantidos no acervo de dados.

Todavia, também é preciso deixar claro que em caso de revogação de consentimento ou alteração dos dados essas podem ser feitas adicionando a nova informação fazendo referência ao dado que houve a revogação ou alteração.

Outro ponto que poder-se-ia alegar para a não aplicação da tecnologia é o problema que ao ser inserido um dado errado há uma prova incontestável de que aquele dado está em desconformidade com a legislação. E para esse obstáculo a solução que pode ser encontrada é exatamente o caminho da honestidade. Admitir que foram cometidos erros e demonstrar que já está sendo solucionado.

Além desses pontos, que podem ser considerados obstáculos para o uso da *blockchain*, deve-se ressaltar as vantagens de sua aplicação. Uma delas é a transparência que essa tecnologia provê para os dados inseridos, todos os dados estão disponíveis para quem tiver acesso à rede.

E o simples fato de os dados inseridos estarem encadeados, em ordem cronológica e sempre referenciados ao dado inserido anteriormente acarreta uma segurança contra fraudes e possibilita a emissão de relatórios com agilidade e sem a interferência.

Volume 08 Número 01 | 10.29073/e3.v8i1.611

5. Conclusão

Parece não haver dúvidas que a tecnologia *blockchain* tem potencial para ser aplicada nos mais diversos campos da sociedade atual. Entretanto, por ser uma tecnologia recente, em que ainda há pouca aplicação, gera receios e ainda possui obstáculos que precisam ser vencidos.

Assim, da pesquisa realizada, confirma-se a possibilidade da aplicação da *blockchain* nos programas de *Compliance* de dados. Devendo, no entanto, ser observada as soluções indicadas para os obstáculos que aparecem ao se tratar de proteção de dados.

Portanto, entende-se que a aplicação da tecnologia não só é possível, como também traz maior segurança tanto para o titular dos dados como para a empresa que realiza o seu tratamento. Para o titular a segurança se encontra no respeito aos seus direitos elencados no artigo 18 da LGPD. Já para a empresa, encontra-se na inviolabilidade que os dados adquirem, evitando o vazamento dos dados e assim, melhorando a gestão de riscos.

.

BIBLIOGRAFIA

Alves, P., Laigner, R., Nasser, R., Robichez, G., Lopes, H. & Kalinowski, M. (2018). *Desmistificando Blockchain: Conceitos e Aplicações*. In: MACIEL, Cristiano; VITERBO, José (Orgs). "Computação e Sociedade", Sociedade Brasileira de Computação. Disponível em: http://www-di.inf.puc-rio.br/~kalinowski//publications/AlvesLNRLK20.pdf.

Associação Brasileira de Bancos Internacionais (ABBI) e a Federação Brasileira de Bancos (FEBRABAN). (2009). Função do *Compliance*. Disponível em: http://www.abbi.com. br/download/funcaode*Compliance*_09.pdf. Acesso em 21 abr 2021.

Bassani, A. & Alves, M. (2020). *Blockchain e LGPD: desafios de Compliance*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/blockchain-lei-geral-protecao-dados-*Compliance*-27102020 Acesso em 23 abr 2021.

Castagna, R. et al. (2020) *Direito e Novas Tecnologias*. Coordenação André Costa-Corrêa e outros. São Paulo: Almedina.

Costa, J. (2020). *Blockchain x Compliance: facilidades e limitações impostas pela LGPD*. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/*Compliance*-blockchain-lgpd-dados-pessoais-empresas.

Doneda, D. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

Doneda, D. et al. (2021). *Tratado de Proteção de Dados Pessoais.* Coordenação Bruno Bioni. Rio de Janeiro.

Endeavor do Brasil. (2021). *Prevenindo com o Compliance para não remediar com o caixa.* Disponível em: https://endeavor.org.br/*Compliance*/. Acesso em 21 abr 2021.

Frazão, A., Tepedino, G. & Oliva, M. (2019). *A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro.* Thomson Reuters Brasil.

Frazão, A., Tepedino, G. & Oliva, M. (2019). *Grandes Temas do Direito Brasileiro: Compliance.* Coordenação Ana Cristina Kleindienst. São Paulo.

Gupta, M. (2018). *Blockchain for dummies®, 2nd IBM Limited Edition.* United States of America: John Wiley & Sons, Inc.

Hanoff, R. (2020). *Blockchain e Compliance: como a tecnologia pode auxiliar a conformidade e transparência dos negócios?* Disponível em: https://studioestrategia.com.br/2020/10/13/relacao-blockchain-e-*Compliance*/ Acesso em 01 mai 2021.

BIBLIOGRAFIA

Lei n. 13.709/2018 da Presidência da República. (2018). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Maciel, R. & Ofrante, R. (2019). *Manual Prático sobre a Lei de Proteção de Dados Pessoais.* RM Digital Education.

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Eletronic Cash System*. https://bitcoin.org/bitcoin.pdf Acesso em 21 abr 2021.

Pinheiro, P. (2021). *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD).* São Paulo: Editora Saraiva.

Salem, A. (2018). *Blockchain e impacto social | André Salem | TEDxMauá - YouTube*. Disponível em: https://www.youtube.com/watch?v=LqLA-PGAb-o (Accessed: 24 March 2022).

Tapscott, D. & Tapscott, A. (2016). *Blockchain Revolution: How the tecnology behind bitcoin and Other cryptocurrencies is changing the world.* New York: Portifolio, 2016.

The Economist. (2015). *The next big thing.* Disponível em: <https://www.economist.com/special-report/2015/05/07/the-next-big-thing> Acesso em 14 set 2020.

Warburg, Bettina. (2016). How the blockchain will radically transform the economy | Betttina Warburg | TEDx Talks - Youtube. Disponível em: https://www.youtube.com/watch?v=RplnSVTzvnU Acesso em 11 jan 2021.