FACULDADE BAIANA DE DIREITO

**A UTILIZAÇÃO DA TECNOLOGIA BLOCKCHAIN NA PROTEÇÃO DE DADOS
TRABALHISTAS: DESAFIOS E OPORTUNIDADES EM CONFORMIDADE COM A
LGPD**

BRUNO OLIUZA OLIVEIRA

JUAZEIRO - BA

2024

BRUNO OLIUZA OLIVEIRA

**A UTILIZAÇÃO DA TECNOLOGIA BLOCKCHAIN NA PROTEÇÃO DE DADOS
TRABALHISTAS: DESAFIOS E OPORTUNIDADES EM CONFORMIDADE COM A
LGPD**

Artigo Científico apresentado ao curso de
Pós-Graduação *Lato Sensu* em Advocacia
Trabalhista da Faculdade Baiana de Direito,
como requisito parcial à obtenção do título
de especialista

JUAZEIRO-BA

2024

RESUMO

O trabalho tem como principal interesse analisar a aplicação da tecnologia blockchain no tratamento de dados trabalhistas, considerando as diretrizes estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD). A blockchain, por meio da descentralização, segurança e imutabilidade, oferece uma solução inovadora para o gerenciamento de dados sensíveis. Diante disso, essa tecnologia também enfrenta desafios relacionados à conformidade com direitos garantidos pela LGPD, como o direito ao esquecimento e a retificação de dados e investiga os obstáculos técnicos e jurídicos na implementação da blockchain, discutindo também soluções como a anonimização e a pseudonimização para minimizar os impactos da imutabilidade dos registros. Assim, a pesquisa conclui que para uma aplicação efetiva no tratamento de dados trabalhistas, são recomendadas blockchains privadas ou híbridas, equilibrando as exigências de segurança, transparência e proteção de dados, enquanto assegura a plena interação com a LGPD.

Palavras-Chave: Blockchain; LGPD; Dados Trabalhistas; Segurança; Compliance; Privacidade;

SUMÁRIO

1. INTRODUÇÃO	5
2. A PROTEÇÃO DE DADOS NO DIREITO DO TRABALHO	6
2.1. A relevância da proteção de dados nas relações de trabalho	6
2.2. A aplicação da lgpd nas relações trabalhistas	8
2.3 agentes de tratamento	9
3. BLOCKCHAIN	11
3.1. Conceito.....	11
3.2. Funcionamento da tecnologia blockchain.....	13
3.3. Características da blockchain: descentralização e segurança.....	14
3.4. Tipos de blockchains.....	16
4. BLOCKCHAIN E PROTEÇÃO DE DADOS TRABALHISTAS	18
4.1. Garantia de privacidade e segurança de dados com blockchain	18
4.1.2 a escolha da melhor blockchain para garantir a proteção de dados trabalhistas	21
4.2. Desafio do direito ao esquecimento	22
4.2.1. Anonimização e pseudonimização: benefícios no uso da blockchain para a conformidade com a lgpd	24
5. IMPLICAÇÕES JURÍDICAS DA ADOÇÃO DA BLOCKCHAIN	26
6. CONCLUSÃO	27
REFERÊNCIAS BIBLIOGRÁFICAS	30

1. INTRODUÇÃO

O avanço da tecnologia promove diversas transformações em muitos setores da sociedade, afetando de forma direta como os dados pessoais são coletados, armazenados e utilizados, principalmente nas relações de trabalho. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 2018, introduziu um novo marco regulatório, estabelecendo diretrizes para o tratamento de dados pessoais e visando garantir a privacidade e a segurança das informações. Com isso, as empresas foram obrigadas a rever seus processos de gerenciamento de dados, assegurando conformidade com a legislação e respeito aos direitos dos trabalhadores.

Nesse contexto, a blockchain surge de forma inovadora e auxilia no tratamento seguro e transparente de dados trabalhistas. As características como descentralização, segurança e imutabilidade, permitem que a blockchain ofereça uma alternativa segura para garantir a integridade das informações. No entanto, sua execução também enfrenta desafios significativos, especialmente quando relacionadas ao cumprimento de normas como a LGPD, a qual prevê o direito ao esquecimento e a possibilidade de retificação de dados, em contraste com a natureza imutável da blockchain.

O trabalho busca analisar de forma aprofundada as questões jurídicas e dificuldades técnicas associadas ao uso da blockchain no tratamento de dados trabalhistas, abordando como essa tecnologia pode ser integrada de maneira eficiente e segura ao ambiente corporativo, sem comprometer a conformidade com a LGPD. Além disso, são discutidas soluções como anonimização e pseudonimização de dados, que visam mitigar os conflitos entre a imutabilidade da blockchain e os direitos garantidos pela legislação e como a blockchain pode ser utilizada para automatizar processos no tratamento de dados e assim minimizar os riscos de manipulação nas informações.

Dessa forma, é muito importante a compreensão dos benefícios e desafios da blockchain no cenário jurídico-trabalhista, a partir da elaboração de alternativas que permitam a utilização dessa tecnologia para garantir maior confiança nos dados dos empregados, ao mesmo tempo que respeite e valorize os direitos fundamentais previstos na LGPD.

2. A PROTEÇÃO DE DADOS NO DIREITO DO TRABALHO

2.1. A relevância da proteção de dados nas relações de trabalho

No contexto das relações de trabalho, a proteção de dados pessoais assume uma importância central, uma vez que as informações dos trabalhadores são amplamente manipuladas em diversas fases do vínculo empregatício, desde o processo de recrutamento até a fase pós-contratual. A coleta, armazenamento e tratamento de dados de empregados abrangem desde informações básicas, como nome e endereço, até dados sensíveis, como informações médicas e biométricas. Diante disso, garantir a segurança e o correto manuseio dessas informações é não apenas uma questão de conformidade legal, mas também de preservação dos direitos fundamentais dos trabalhadores.

Com a promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil, surgiu um marco regulatório que busca proteger o tratamento de dados pessoais, assegurando que as informações dos indivíduos sejam usadas de forma legítima e segura. De acordo com a legislação, a LGPD aplica-se amplamente às relações de trabalho, e qualquer operação de tratamento de dados realizada pelas empresas deve estar em conformidade com a legislação e os princípios da transparência, necessidade e finalidade (Brasil, 2018), independentemente de o tratamento ser realizado de forma digital ou física.

Um aspecto crucial da relevância da proteção de dados no ambiente de trabalho reside no fato de que, durante o vínculo empregatício, o empregador detém uma posição de autoridade em relação ao trabalhador, o que pode acarretar riscos à privacidade e à liberdade dos empregados. Isso inclui o uso indevido de informações pessoais para além das finalidades estabelecidas, expondo os trabalhadores a vulnerabilidades, como fraudes, discriminação e violação de privacidade. Dessa forma, o cumprimento das diretrizes da LGPD não só reforça o direito à privacidade dos trabalhadores, mas também contribui para um ambiente de trabalho mais ético e seguro. Diante disso, 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”.

Um aspecto central dessa legislação é a garantia de que o titular dos dados, ou seja, o trabalhador, tenha controle sobre as informações pessoais tratadas. Isso

inclui o direito de saber quais dados estão sendo coletados, como são usados, e de exigir sua correção ou exclusão, caso não sejam mais necessários (Brasil, 2018). Como ressaltado por Pohlmann (2019, p. 47), "o titular dos dados tem o direito de solicitar completa informação sobre os dados tratados pelo controlador, solicitar alteração ou eliminação de dados pessoais, ou mesmo opor-se ao tratamento dos seus dados pessoais, sempre observando as regulamentações correspondentes". Esse controle reforça a importância da proteção de dados como uma medida que promove a segurança jurídica e a preservação da privacidade no ambiente de trabalho.

Além disso, a proteção de dados é relevante para evitar abusos por parte dos empregadores, como a utilização excessiva de mecanismos de monitoramento, o que poderia resultar em invasões desnecessárias à vida privada dos empregados. Nesse sentido, o empregador deve sempre agir de acordo com os princípios da finalidade e da necessidade, utilizando os dados pessoais estritamente para os fins previstos no contrato de trabalho, sem que haja desvio de função ou uso excessivo de informações. Como observado por 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.

A crescente digitalização do ambiente de trabalho também potencializa os desafios relacionados à proteção de dados. A implementação de sistemas de monitoramento digital, a utilização de ferramentas de teletrabalho e o uso de dispositivos pessoais para fins laborais aumentam significativamente o volume e a diversidade de dados coletados, exigindo das empresas medidas cada vez mais rigorosas para garantir a privacidade dos empregados.

Diante dessas circunstâncias, a proteção de dados no âmbito trabalhista emerge como uma questão de suma relevância para a preservação dos direitos dos trabalhadores. A adequação à LGPD não apenas evita sanções administrativas para as empresas, mas também fortalece o compromisso ético com a proteção dos direitos fundamentais à privacidade e à dignidade humana no ambiente laboral.

2.2. A aplicação da Lgpd nas relações trabalhistas

A Lei Geral de Proteção de Dados (LGPD) trouxe um novo paradigma para o tratamento de dados pessoais no Brasil, impactando diretamente diversas áreas, incluindo as relações trabalhistas. Antes da promulgação da LGPD, a proteção de dados no ambiente de trabalho era tratada de forma fragmentada, com respaldo em dispositivos constitucionais, no Código Civil e em legislações específicas como o Marco Civil da Internet. No entanto, esses dispositivos não eram suficientes para lidar com a complexidade e a quantidade de dados manipulados pelas empresas no curso das relações de trabalho. A LGPD veio preencher essa lacuna, estabelecendo normas claras e abrangentes para o tratamento de dados pessoais no ambiente laboral (Brasil, 2018).

No contexto das relações trabalhistas, a aplicação da LGPD envolve todas as fases do vínculo empregatício, desde a pré-contratação até o término da relação de trabalho. Durante o processo seletivo, por exemplo, as empresas coletam uma grande quantidade de informações dos candidatos, que incluem dados pessoais e, em alguns casos, dados sensíveis, como informações sobre saúde e antecedentes criminais. Nesse estágio, a empresa deve garantir que os dados coletados sejam tratados de acordo com os princípios da finalidade e necessidade, previstos no artigo 6º da LGPD, ou seja, a coleta de dados deve ser limitada ao estritamente necessário para a função pretendida (Brasil, 2018).

A fase contratual também está sujeita às diretrizes da LGPD, uma vez que o empregador coleta e armazena dados sobre a jornada de trabalho, registros de ponto, dados bancários para o pagamento de salários e, em alguns casos, dados biométricos. É imprescindível que o empregador assegure a segurança desses dados, adotando medidas técnicas e administrativas para protegê-los contra acessos não autorizados e incidentes de segurança. Além disso, a LGPD determina que o titular dos dados, no caso o empregado, tem o direito de saber como seus dados estão sendo tratados, podendo solicitar correções ou exclusão de informações, conforme o artigo 18 da lei (Brasil, 2018).

Na fase pós-contratual, a empresa continua sendo responsável pela proteção dos dados do empregado, mesmo após o término do vínculo empregatício. Informações sobre desligamento, verbas rescisórias e histórico funcional permanecem armazenadas e devem ser mantidas em segurança pelo período exigido

pela legislação trabalhista, como o prazo de prescrição de cinco anos estabelecido pela Consolidação das Leis do Trabalho (CLT). Mesmo após o fim do contrato, o empregado mantém o direito de solicitar a eliminação de seus dados, salvo nas hipóteses em que a manutenção dessas informações seja necessária para o cumprimento de obrigações legais ou regulatórias, conforme o artigo 16 da LGPD (Brasil, 2018).

Outrossim, sobre a aplicação da LGPD no ambiente laboral é o papel do consentimento do trabalhador no tratamento de dados. Embora a LGPD estabeleça o consentimento como uma das bases legais para o tratamento de dados, no contexto trabalhista, o consentimento não é sempre necessário. O tratamento de dados pode ser realizado com base na necessidade de cumprimento de obrigações contratuais e legais. Assim, a relação de subordinação entre empregador e empregado não afasta a necessidade de observar os limites e as finalidades específicas para as quais os dados são coletados, como destaca Pohlmann (2019, p. 62), ao afirmar que o consentimento só é válido se houver direcionamento a uma finalidade específica ou determinada.

Além disso, o advento da LGPD trouxe a necessidade de adaptações nas empresas para atender às exigências legais, incluindo a implementação de medidas de compliance e programas de governança de dados. O compliance trabalhista é um elemento essencial para garantir a conformidade com a legislação, promovendo a criação de políticas de proteção de dados, treinamentos, e procedimentos de controle e auditoria interna.

Em suma, a aplicação da LGPD nas relações trabalhistas é uma extensão natural da legislação de proteção de dados, que busca equilibrar o poder do empregador com os direitos fundamentais do trabalhador. A conformidade com a LGPD não só previne possíveis sanções administrativas e judiciais, mas também promove um ambiente de trabalho mais ético, transparente e seguro para ambas as partes. A proteção de dados, nesse contexto, está intimamente ligada ao respeito pela privacidade e dignidade dos trabalhadores, valores fundamentais que devem ser preservados em todas as etapas da relação de emprego.

2.3 Agentes de tratamento

A Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, introduziu o conceito de agentes de tratamento como figuras centrais na dinâmica de gestão de dados pessoais, incluindo aqueles referentes às relações trabalhistas. A LGPD define claramente os papéis de controlador e operador, ambos essenciais para garantir que o tratamento de dados seja conduzido de forma adequada, em conformidade com os princípios legais e éticos que regem a proteção de dados no Brasil (Brasil, 2018). Esses agentes possuem funções complementares, porém com responsabilidades distintas, que se aplicam diretamente às práticas de gestão de dados nas relações de trabalho, desde a coleta até o descarte dessas informações.

O controlador é a pessoa natural ou jurídica, de direito público ou privado, responsável por tomar as principais decisões a respeito do tratamento de dados pessoais. Em um ambiente laboral, o controlador geralmente é o empregador, que determina como e por que os dados dos trabalhadores serão tratados. Ele é o responsável por definir os meios e as finalidades desse tratamento, bem como assegurar que todas as etapas, desde a coleta até o arquivamento ou eliminação dos dados, sejam realizadas de acordo com os princípios da LGPD, tais como a necessidade, transparência e segurança.

O operador, por sua vez, atua sob as instruções do controlador, executando as atividades de tratamento de dados. Embora o operador não tenha o poder de decisão sobre o tratamento em si, ele desempenha um papel crucial na execução prática das tarefas relacionadas ao processamento de dados, como o armazenamento, transferência e eliminação de informações. No contexto trabalhista, o operador pode ser um prestador de serviços terceirizado, uma empresa de contabilidade ou uma plataforma de gestão de recursos humanos, que lida diretamente com os dados dos empregados em nome do controlador. O operador, assim como o controlador, é igualmente responsável por garantir que os dados sejam tratados de acordo com os princípios legais estabelecidos pela LGPD.

Nesse contexto, é fundamental que as empresas que atuam como controladoras ou operadoras nas relações de trabalho invistam em programas de compliance voltados à proteção de dados. Isso inclui a implementação de políticas de segurança da informação, treinamento de colaboradores e a adoção de tecnologias que garantam o sigilo e a integridade dos dados tratados. Como ressaltado por Pohlmann (2019, p. 64), "os agentes de tratamento devem manter registros e evidências de todo o tipo de tratamento realizado com os dados dos titulares(...)", o

que demonstra a importância de uma atuação transparente e pautada em boas práticas para garantir a conformidade com a LGPD.

Portanto, o papel dos agentes de tratamento nas relações trabalhistas vai além da mera gestão técnica dos dados pessoais. Eles são fundamentais na construção de um ambiente de trabalho seguro e ético, onde os direitos dos trabalhadores são respeitados e preservados em todas as etapas do tratamento de dados. O cumprimento das obrigações legais por parte desses agentes é imprescindível para garantir não só a proteção dos dados, mas também para promover a confiança entre empregadores e empregados no contexto das relações laborais.

3. BLOCKCHAIN

3.1. Conceito

A tecnologia blockchain surgiu em 2008 com a publicação do artigo "Bitcoin: A Peer-to-Peer Electronic Cash System", de autoria sob o pseudônimo de Satoshi Nakamoto. Originalmente idealizada como a base para o funcionamento do Bitcoin, a blockchain rapidamente se expandiu para diversas áreas, destacando-se por suas características únicas de segurança, transparência e descentralização (Nakamoto, 2008).

De maneira simplificada, a blockchain pode ser definida como um banco de dados distribuído, organizado em uma estrutura de blocos interligados. Cada bloco contém um conjunto de informações, sendo criptograficamente vinculado ao bloco anterior, formando uma cadeia inquebrável de dados, o que confere à blockchain sua característica de imutabilidade. Uma vez que um bloco é inserido na cadeia, as informações contidas nele não podem ser alteradas sem que os blocos subsequentes sejam invalidados, o que confere segurança adicional ao sistema (Lucena; Henriques, 2016). Isso garante que qualquer tentativa de alteração não passe despercebida, já que a cadeia precisa ser validada por uma rede de participantes, conhecidos como nós, distribuídos ao longo da rede.

Corroborando com esse entendimento, Schwab expõe:

[...], o *blockchains*, muitas vezes descrito como um "livro-razão distribuído", é um protocolo seguro no qual uma rede de computadores verifica de forma

coletiva uma transação antes de registrá-la e aprová-la. A tecnologia que sustenta o *Blockchains* cria confiança, permitindo que pessoas que não o conheçam [...] colaborem sem ter que passar por uma autoridade central neutra – ou seja, um depositário ou livro contábil central. [...] é um livro contábil compartilhado, programável, criptograficamente seguro e, portanto, confiável; ele não é controlado por nenhum usuário único, mas pode ser inspecionado por todos (Schwab, 2014, p. 30).

Outro aspecto importante do conceito de blockchain é sua natureza descentralizada, diferentemente dos sistemas tradicionais de bancos de dados centralizados, a blockchain não depende de uma única entidade controladora. Em vez disso, utiliza uma rede de participantes que validam as transações de forma coletiva, o que torna o sistema mais seguro contra fraudes ou ataques maliciosos. Essa descentralização é essencial para garantir a transparência e a confiabilidade do sistema, visto que todos os nós da rede possuem uma cópia idêntica da cadeia de blocos.

Além disso, a blockchain é considerada uma tecnologia de rede peer-to-peer (P2P), o que significa que os participantes da rede podem interagir diretamente entre si, sem a necessidade de intermediários. Isso facilita o registro e a verificação de transações, tornando o sistema mais eficiente e resistente a falhas (Tapscott & Tapscott, 2016). Corroborando com a ideia do que é 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). Dessa forma, a blockchain promove um ambiente seguro e transparente para o armazenamento e validação de dados.

Embora tenha sido inicialmente desenvolvida para o setor financeiro, mais especificamente para a criação de criptomoedas como o Bitcoin, o conceito de blockchain rapidamente se expandiu para outras áreas, devido à sua flexibilidade e segurança. A natureza distribuída e descentralizada da blockchain permite sua aplicação em inúmeros setores, como a gestão de cadeias de suprimentos, contratos inteligentes e até mesmo a proteção de dados pessoais, tema relevante nas discussões sobre conformidade com a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Em síntese, o conceito de blockchain é fundamentado em três pilares principais: descentralização, segurança e transparência, características que tornam essa tecnologia robusta e de ampla aplicação. Com isso, seu funcionamento distribui o poder entre os participantes da rede, elimina intermediários e garante a integridade das informações, tornando a blockchain uma ferramenta poderosa na era da transformação digital.

3.2. Funcionamento da tecnologia blockchain

O funcionamento dessa tecnologia baseia-se em uma estrutura de blocos de dados que são conectados e validados de maneira descentralizada por uma rede de computadores distribuídos, denominados nós. Esses blocos contêm informações sobre transações ou qualquer outro dado a ser registrado de forma segura e transparente. Uma das principais características do funcionamento da blockchain é a imutabilidade: uma vez que um bloco é adicionado à cadeia, ele não pode ser alterado sem modificar todos os blocos subsequentes, o que tornaria a alteração evidente para todos os participantes da rede.

Campos (2018, p. 20-21) resume em:

[...] 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.

O processo começa com a transmissão de uma transação para a rede, a partir disso, essa tecnologia pode variar sua forma de atuação, desde o envio de uma criptomoeda até o registro de um contrato inteligente ou dados de qualquer natureza. Os nós da rede recebem essa transação e agrupam-se em um bloco, que será validado através de um algoritmo de consenso, esse mecanismo garante que a transação é legítima e que o bloco pode ser adicionado à cadeia.

Cada novo bloco gerado contém, além dos dados da transação, um hash criptográfico, que é uma sequência de caracteres gerada a partir dos dados contidos no bloco. Esse hash também inclui a referência ao hash do bloco anterior, formando uma cadeia contínua e inseparável de blocos, é essa estrutura de encadeamento de blocos que garante a integridade dos dados registrados na blockchain, pois qualquer

alteração em um bloco anterior resultaria em uma modificação nos hashes subsequentes, invalidando a cadeia. Assim, os dados registrados na blockchain são extremamente seguros contra tentativas de adulteração ou fraude.

É fundamental o papel dos nós na rede blockchain, pois eles são responsáveis pela validação das transações e pelo armazenamento da cópia completa da cadeia de blocos. Cada nó verifica a validade dos novos blocos propostos, garantindo que todos os dados sejam consistentes com o restante da rede. A descentralização proporcionada pelos nós é uma das principais razões pela qual a blockchain é considerada uma tecnologia tão segura, pois não há uma autoridade central controlando os dados, mas sim uma rede distribuída que assegura a integridade e a transparência das informações (Nakamoto, 2008).

Após a validação, o bloco é adicionado à cadeia e a transação é considerada concluída. Esse modelo garante a transparência e a auditabilidade dos dados, uma vez que todas as transações e alterações ficam registradas de maneira pública e acessível a qualquer participante da rede. Além disso, como todos os nós possuem uma cópia completa da cadeia de blocos, é possível reconstruir o histórico de transações a qualquer momento, assegurando que os dados não sejam perdidos ou alterados.

O funcionamento da blockchain se baseia em um mecanismo de validação descentralizada e permite que o sistema continue funcionando mesmo que alguns nós sejam comprometidos ou retirados da rede. Isso garante uma alta resiliência ao sistema, uma vez que não depende de um único ponto de falha, algo comum em sistemas centralizados. Essa característica, combinada com a imutabilidade dos blocos e a transparência do sistema, faz da blockchain uma tecnologia amplamente aplicável em setores que demandam segurança e confiança na manipulação de dados.

3.3. Características da blockchain: descentralização e segurança

A tecnologia blockchain destaca-se por diversas razões, duas das principais características fundamentais que sustentam sua aplicação em diversos setores são: a descentralização e a segurança. Esses dois pilares estão na base que torna a blockchain uma tecnologia confiável e robusta, especialmente em um cenário cada vez mais dependente da integridade e proteção dos dados.

A descentralização é um dos aspectos mais inovadores da blockchain. Diferentemente dos sistemas centralizados, onde uma autoridade única controla e gerencia todas as operações e dados, a blockchain opera em uma rede distribuída de nós, a qual possibilita que todos os participantes tenham acesso às mesmas informações. Isso elimina a necessidade de intermediários, tornando as transações mais rápidas e reduzindo custos operacionais. Além disso, a descentralização dificulta tentativas de fraude, uma vez que não há um ponto central de vulnerabilidade que possa ser comprometido.

No modelo descentralizado, as transações e informações registradas na blockchain precisam ser validadas por um mecanismo de consenso, que pode variar de acordo com o tipo de blockchain, sendo o Prova de Trabalho (PoW) um dos mais utilizados. O PoW exige que os nós validem transações resolvendo problemas matemáticos complexos, garantindo que apenas transações legítimas sejam incluídas na cadeia. Esse processo de consenso distribuído impede que uma única entidade controle ou manipule o sistema, tornando-o resiliente a ataques e garantindo que todas as decisões sejam tomadas de maneira coletiva.

A segurança da blockchain está intimamente ligada à sua estrutura de blocos encadeados e ao uso de hashes criptográficos. Cada bloco contém um conjunto de transações que é validado pela rede e, uma vez validado, é criptograficamente vinculado ao bloco anterior através de um hash. Isso cria uma cadeia inquebrável de blocos, onde qualquer tentativa de alterar um dado em um bloco resultaria na modificação dos hashes de todos os blocos subsequentes, tornando a fraude evidente para toda a rede (Lucena; Henriques, 2016). Essa arquitetura imutável é uma das principais razões pelas quais a blockchain é considerada altamente segura.

Além disso, a blockchain adota medidas de segurança criptográfica que garantem a integridade dos dados. Ao utilizar algoritmos de hash, como o SHA-256, qualquer alteração mínima nos dados gera uma sequência de hash completamente diferente, impossibilitando que uma modificação passe despercebida. Os hashes criptográficos garantem que uma vez que uma transação é registrada, ela não pode ser alterada sem que toda a cadeia de blocos subsequentes seja invalidada, preservando assim a integridade das transações.

A combinação da descentralização com mecanismos de consenso distribuído e segurança criptográfica faz da blockchain uma tecnologia especialmente robusta para aplicações que demandam alta integridade e confiança nos dados. Essas

características tornam a blockchain uma solução amplamente aplicável em ambientes que exigem transparência e proteção, como no setor financeiro, na gestão de contratos inteligentes e até na proteção de dados pessoais em conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD).

Em suma, a descentralização garante a transparência e resiliência da rede, ao passo que a segurança proporcionada pelos mecanismos criptográficos e pela imutabilidade dos blocos protege a integridade das informações armazenadas. Esses atributos tornam a blockchain uma tecnologia inovadora, confiável e cada vez mais relevante em um cenário global que demanda soluções seguras para a proteção de dados e transações.

3.4. Tipos de blockchains

A tecnologia blockchain pode ser dividida em três categorias principais, de acordo com o nível de acesso, governança e privacidade dos dados: blockchains públicas, blockchains privadas e blockchains híbridas (ou consorciadas). Cada tipo de blockchain possui características específicas que determinam sua aplicabilidade e adequação a diferentes cenários, seja no setor público ou privado.

As blockchains públicas são aquelas que permitem a participação de qualquer pessoa na rede, sem restrições de acesso. Nesses sistemas, todos os participantes podem ler, enviar e validar transações. Essa arquitetura descentralizada e aberta é a base de criptomoedas como o Bitcoin e o Ethereum. A principal característica desse tipo de blockchain é a transparência, uma vez que todos os nós da rede possuem uma cópia do histórico completo de transações, garantindo que qualquer tentativa de alteração seja facilmente detectada.

Ademais, a governança da blockchain pública é distribuída entre os participantes, o que significa que não há uma autoridade central para tomar decisões sobre as regras da rede. Isso torna a blockchain pública mais segura contra manipulações, mas também pode ser menos eficiente em termos de velocidade e consumo de energia, especialmente quando utiliza mecanismos de consenso como o Proof of Work (PoW), que demanda alto poder computacional para validar transações.

As blockchains privadas, por outro lado, operam em redes permissionadas, onde o acesso e a participação são controlados por uma entidade central ou por um

grupo de organizações. Nesse modelo, apenas usuários autorizados podem participar da rede e validar transações, o que garante maior controle e privacidade sobre os dados processados. As blockchains privadas são frequentemente adotadas por empresas e governos que precisam garantir a confidencialidade dos dados sensíveis, como no gerenciamento de contratos e cadeias de suprimentos.

Uma das vantagens desse tipo de blockchain é a maior eficiência em termos de tempo e custo, uma vez que o número de nós validadores é menor, e os algoritmos de consenso podem ser mais rápidos, como o Proof of Authority (PoA). No entanto, as blockchains privadas dependem de uma entidade central para governança, o que pode reduzir o nível de confiança e descentralização em comparação com as blockchains públicas.

As blockchains híbridas, também chamadas de blockchains de consórcio, combinam elementos das blockchains públicas e privadas. Nesse modelo, a governança é compartilhada entre um grupo de organizações, onde determinadas partes da blockchain podem ser públicas, enquanto outras são mantidas privadas e acessíveis apenas por participantes autorizados. Esse tipo de blockchain é particularmente útil para indústrias em que diferentes empresas ou instituições precisam colaborar, como o setor financeiro e a saúde.

Nas blockchains híbridas, os participantes têm controle sobre quem pode acessar determinadas transações ou dados, ao mesmo tempo em que podem usar a blockchain pública para garantir a transparência e a imutabilidade de outras informações. Dessa forma, combina-se o melhor dos dois mundos: a transparência das blockchains públicas com a privacidade e controle das blockchains privadas.

Cada tipo de blockchain apresenta características que tornam sua aplicação adequada a diferentes cenários, dependendo das necessidades de transparência, controle e privacidade. No contexto da Lei Geral de Proteção de Dados (LGPD), a blockchain pode ser uma ferramenta poderosa para garantir a conformidade com os requisitos de segurança e governança de dados, especialmente em relação à transparência no tratamento de dados e à capacidade de rastrear acessos e modificações.

As blockchains públicas oferecem imutabilidade e visibilidade completas das transações e são mais indicadas para contextos em que a transparência total é crucial, como em auditorias públicas. No entanto, para empresas que tratam de dados sensíveis, como informações pessoais protegidas pela LGPD, a adoção de

blockchains privadas ou híbridas tende a ser a melhor solução. Blockchains privadas garantem controle rígido sobre quem pode acessar e modificar os dados, atendendo às exigências de privacidade da LGPD. Elas permitem que apenas usuários autorizados acessem as informações, oferecendo maior segurança e facilitando a conformidade com os princípios da LGPD, como o princípio da necessidade e o direito à portabilidade dos dados pessoais.

As blockchains híbridas apresentam uma solução equilibrada para empresas que precisam compartilhar certos dados entre parceiros ou dentro de consórcios empresariais, mas ainda exigem níveis mais elevados de controle sobre dados sensíveis. A capacidade de definir quem pode ver ou modificar diferentes tipos de dados é essencial para garantir que as empresas permaneçam em conformidade com a LGPD, enquanto ainda aproveitam os benefícios da transparência e auditabilidade inerentes à tecnologia blockchain.

Por fim, os diferentes tipos de blockchains oferecem diferentes benefícios e desafios, dependendo das necessidades de segurança, governança e transparência das aplicações em que são utilizados.

4. BLOCKCHAIN E PROTEÇÃO DE DADOS TRABALHISTAS

4.1. Garantia de privacidade e segurança de dados com blockchain

A proteção de dados trabalhistas no contexto corporativo, especialmente à luz das exigências impostas pela Lei Geral de Proteção de Dados (LGPD), é um desafio crescente para as empresas. O uso de tecnologias emergentes, como a blockchain, tem se mostrado uma solução promissora para lidar com esse desafio, fornecendo segurança, transparência e controle no tratamento de dados sensíveis dos empregados.

A blockchain, ao oferecer uma infraestrutura descentralizada e imutável, fornece uma garantia adicional de que os dados dos empregados não serão manipulados ou acessados indevidamente por terceiros. Um dos pontos fortes dessa tecnologia é sua capacidade de proteger dados sensíveis, como informações pessoais e trabalhistas (nomes, endereços, registros de pagamento, e dados sobre saúde), por meio de técnicas de criptografia e hashing. Uma vez que essas informações são registradas na blockchain, qualquer tentativa de alterar os dados

resulta em uma mudança evidente em toda a cadeia de blocos subsequente, tornando-a facilmente detectável por todos os participantes da rede.

Ao implementar a blockchain no ambiente corporativo, os dados dos empregados podem ser organizados e gerenciados de forma que apenas pessoas autorizadas tenham acesso às informações, atendendo ao princípio da minimização de dados, estabelecido pela LGPD, esse princípio determina que apenas os dados necessários para o cumprimento de uma função específica devem ser acessíveis. A tecnologia blockchain, ao limitar o acesso por meio de chaves criptográficas e ao possibilitar a criação de registros de acesso rastreáveis, garante que os dados dos empregados só serão manipulados ou acessados quando necessário, e com o consentimento do titular dos dados.

Outro ponto relevante é a capacidade da blockchain de lidar com os registros de consentimento dos empregados para o tratamento de seus dados. As empresas podem utilizar contratos inteligentes para registrar e gerenciar os consentimentos dos empregados de maneira automatizada e imutável, permitindo que o empregado tenha controle sobre como seus dados estão sendo utilizados, em conformidade com a LGPD. Isso cria um ambiente de maior confiança e transparência, onde os empregados podem verificar quem acessou seus dados, quando isso aconteceu e para qual finalidade.

Além disso, a imutabilidade dos dados registrados na blockchain proporciona uma camada extra de segurança contra fraudes e manipulações. No contexto trabalhista, isso é particularmente importante em áreas como o controle de ponto eletrônico, folha de pagamento e histórico de desempenho. Ao garantir que esses registros não possam ser alterados de forma não autorizada, a blockchain assegura que os direitos dos empregados sejam respeitados e que as empresas cumpram suas obrigações de forma precisa e transparente.

Entretanto, um dos desafios para a adoção da blockchain no tratamento de dados trabalhistas é a sua imutabilidade, que pode entrar em conflito com o direito do empregado de solicitar a retificação ou exclusão de seus dados, conforme previsto na LGPD. Para lidar com esse obstáculo, técnicas como a anonimização e a pseudonimização de dados são frequentemente adotadas, permitindo que os dados sejam removidos ou modificados sem comprometer a integridade da blockchain. Essas técnicas garantem que os dados possam ser alterados ou retirados quando

necessário, sem violar as obrigações da empresa em relação à proteção e segurança da informação.

Ao integrar a tecnologia blockchain no lugar dos intermediários humanos responsáveis pelo tratamento de dados, surgem vários benefícios cruciais para as empresas que visam garantir a proteção dos dados pessoais e trabalhistas de forma eficiente e em conformidade com a LGPD.

Em uma estrutura tradicional, o controlador e o operador são responsáveis por gerenciar o tratamento de dados, o que pode introduzir vulnerabilidades, como erros humanos e o risco de manipulação indevida. A substituição desse modelo pela blockchain elimina a necessidade desses intermediários, automatizando processos por meio de contratos inteligentes (smart contracts). Esses contratos são autoexecutáveis e garantem que as ações de tratamento de dados ocorram de maneira automatizada, segura e transparente, sem a necessidade de intervenção humana direta. Assim, pode ser concebido como um sistema que distribui ativos digitais para uma ou mais das partes envolvidas, desde que as condições previamente estabelecidas sejam cumpridas, o que caracteriza a auto execução dos contratos (Corrales; Fenwuck; Haapio, 2019). Isso não só reduz erros, mas também aumenta a confiabilidade no processo de tratamento, já que as regras e condições definidas nos contratos são automaticamente aplicadas e auditáveis por todas as partes envolvidas.

Além disso, a eliminação do intermediário humano reduz o risco de vazamentos e acessos não autorizados aos dados. Enquanto os agentes de tratamento podem, intencionalmente ou por negligência, acessar ou modificar dados de forma inadequada, a blockchain garante que as transações sejam imutáveis e auditáveis por todos os participantes da rede, isso torna qualquer tentativa de manipulação praticamente impossível sem ser detectada. A ausência de intermediários também aumenta a eficiência operacional, uma vez que o processo de verificação e validação de dados é feito automaticamente pela própria rede, sem a necessidade de revisões manuais demoradas.

A melhoria da transparência é um grande benefício, pois não depende de relatórios fornecidos por operadores ou controladores humanos, a blockchain registra todas as transações e acessos de forma descentralizada e distribuída. Qualquer auditoria ou verificação de conformidade pode ser realizada diretamente na blockchain, em tempo real, o que fortalece a segurança jurídica e garante o

cumprimento de requisitos da LGPD, como a prestação de contas sobre o tratamento de dados dos titulares.

Ao remover o intermediário humano, a blockchain também facilita a gestão de consentimento dos empregados para o tratamento de seus dados, garantindo que suas preferências sejam respeitadas e registradas de forma imutável. Esse controle automatizado sobre o consentimento melhora a confiança dos empregados no uso de seus dados pela empresa e garante que eles tenham total controle sobre como e quando suas informações estão sendo utilizadas, o que é crucial para a conformidade com a LGPD.

Portanto, ao substituir os intermediários humanos por tecnologia de blockchain, as empresas podem otimizar seus processos de tratamento de dados, aumentar a segurança e a transparência e reduzir significativamente os riscos de violação de dados e não conformidade. Fato que reforça o papel da blockchain como uma ferramenta fundamental para garantir a integridade e a proteção dos dados pessoais e trabalhistas no ambiente corporativo.

4.1.2 a escolha da melhor blockchain para garantir a proteção de dados trabalhistas

Para garantir que o tratamento de dados dos empregados ocorra de maneira eficiente e em conformidade com a LGPD, o tipo de blockchain mais adequado seria a blockchain híbrida. Esse modelo oferece o equilíbrio ideal entre privacidade e transparência, combinando os aspectos positivos das blockchains públicas e privadas. Isso porque, os dados sensíveis dos empregados podem ser mantidos em uma parte privada da blockchain, onde apenas usuários autorizados têm acesso, enquanto outros dados menos sensíveis podem ser armazenados em uma parte pública, acessível por todos os participantes da rede, garantindo transparência e auditabilidade em processos que não envolvem informações protegidas.

Essa abordagem híbrida possibilita o controle granular sobre quem pode acessar e manipular certos dados, assegurando a conformidade com a LGPD e, ao mesmo tempo, oferecendo a auditabilidade necessária para processos corporativos. Permite também, que as empresas utilizem contratos inteligentes para automatizar operações e gerenciar permissões de dados de maneira mais eficiente. Assim, garante-se que o tratamento de dados ocorra dentro dos parâmetros legais, com maior segurança e redução de riscos de violação de privacidade.

Logo, ao optar por uma blockchain híbrida, as empresas podem tirar proveito da transparência das blockchains públicas e da privacidade e controle das blockchains privadas, equilibrando a necessidade de proteção de dados sensíveis com a flexibilidade necessária para processos empresariais eficientes.

4.2. Desafio do direito ao esquecimento

O direito ao esquecimento é uma das principais garantias previstas pela Lei Geral de Proteção de Dados (LGPD), assegurando que os titulares dos dados tenham o direito de solicitar a exclusão de suas informações pessoais quando elas não forem mais necessárias ou relevantes para os fins pelos quais foram coletadas. No entanto, o uso da blockchain no tratamento de dados apresenta um desafio significativo para a implementação desse direito, devido à natureza imutável da tecnologia.

A imutabilidade é um dos principais benefícios da blockchain, garantindo que os dados inseridos no sistema não possam ser alterados ou excluídos sem que isso seja registrado de forma transparente para todos os participantes da rede.

Pensando unicamente na tecnologia existente, a imutabilidade é bastante importante, mas quando se trata de inserir a LGPD, há alguns possíveis desafios. Diante disso, o art. 18, VI, da LGPD expõe:

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:

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

Com isso, essa característica torna a exclusão de dados um processo extremamente difícil, uma vez que qualquer tentativa de remover ou alterar informações conflita com a estrutura básica de uma cadeia de blocos. Esse dilema coloca em evidência o conflito entre as exigências da LGPD, que prevê o direito à exclusão de dados pessoais, e a tecnologia blockchain, que se baseia na permanência e rastreabilidade dos registros.

Para enfrentar esse desafio, várias soluções vêm sendo propostas, como o uso de anonimização e pseudonimização de dados. A anonimização refere-se à remoção de todos os identificadores pessoais de um conjunto de dados, de modo que o titular não possa ser reidentificado, tornando os dados inutilizáveis para fins de identificação.

Uma vez que os dados são anonimizados, eles deixam de ser considerados "dados pessoais" pela LGPD, o que pode ser interpretado como uma maneira de cumprir com o direito ao esquecimento sem alterar o funcionamento da blockchain. No entanto, essa abordagem tem suas limitações, pois pode ser tecnicamente desafiadora em certos contextos, e a reidentificação dos dados ainda pode ser possível em algumas situações, dependendo da técnica utilizada.

Nesse sentido, Feigelson e Siqueira (2019, p.18) opinam:

[...] As normas de proteção de dados não serão aplicadas às informações anônimas, ou seja, àquelas que não digam respeito a uma pessoa natural identificada ou identificável nem a dados pessoais tornados de qualquer modo anônimos por meio de procedimento que impeça que seu titular seja identificado, direta ou indiretamente.

Para tanto, é fundamental que o processo de anonimização impeça a identificação do titular por quaisquer meios suscetíveis de serem razoavelmente utilizados, seja pelos agentes de tratamento, seja por terceiro. Para aferir a possibilidade de reversão da anonimização, deve-se considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, bem como a tecnologia disponível na data do tratamento dos dados e a evolução tecnológica. Caso seja possível atribuir dados pessoais que tenham sido anonimizados a um indivíduo específico, mediante a utilização de informações suplementares, a LGPD será necessariamente aplicável.

Conforme analisado, a legislação atual dificulta bastante a utilização da anonimização, especialmente em um ambiente tecnológico que evolui constantemente e oferece novas formas de reidentificação de dados, mesmo que anonimizados. Nesse cenário específico, a única forma de garantir plena conformidade com a LGPD seria avaliar cuidadosamente o contexto em que a anonimização está sendo aplicada. Embora a tecnologia respeite os principais aspectos da norma, sua aplicação precisa ser acompanhada de mecanismos adicionais de segurança e uma análise contínua de risco para assegurar que a reidentificação dos dados não seja possível, sob pena de tornar a LGPD aplicável e exigir adequações adicionais por parte das empresas.

Assim, não se trata de abandonar a tecnologia, mas sim de complementá-la com boas práticas de governança de dados, que incluam a anonimização como uma das várias camadas de proteção, garantindo que os direitos dos titulares de dados sejam preservados, e que a conformidade legal seja mantida ao longo do tempo.

Outra solução envolve o uso de pseudonimização, que mantém os dados parcialmente identificáveis, mas os separa de informações diretas que permitiriam a

identificação do titular. Embora a pseudonimização não cumpra totalmente o direito ao esquecimento, ela limita o risco de exposição dos dados e pode ser uma estratégia temporária para melhorar a conformidade com a LGPD, principalmente em sistemas onde a exclusão completa dos dados não é viável.

Adicionalmente, o uso de contratos inteligentes (smart contracts) pode ajudar a automatizar a gestão de dados pessoais em uma blockchain. Esses contratos poderiam incluir cláusulas para o tratamento e a eventual remoção dos dados, controlando os acessos e revogando permissões conforme os titulares solicitarem. Embora essa abordagem não resolva completamente o problema da imutabilidade, ela pode oferecer maior flexibilidade no gerenciamento dos direitos dos titulares, ajudando as empresas a balancearem a necessidade de transparência com as obrigações legais.

Por conseguinte, o direito ao esquecimento representa um dos maiores desafios legais no uso da blockchain para o tratamento de dados sensíveis, incluindo os dados trabalhistas. Embora a tecnologia blockchain consiga oferecer benefícios significativos em termos de segurança e transparência, sua estrutura rígida precisa ser adaptada para atender aos requisitos regulatórios da LGPD. Soluções como a anonimização, pseudonimização e o uso de contratos inteligentes são algumas das opções disponíveis para garantir que o direito ao esquecimento seja respeitado, mas é evidente que ainda há um caminho a ser percorrido para harmonizar plenamente essa tecnologia com as exigências legais.

4.2.1. Anonimização e pseudonimização: benefícios no uso da blockchain para a conformidade com a lgpd

Com o objetivo de superar as barreiras contidas no uso da blockchain para garantir a conformidade da LGPD no tratamento de dados dos trabalhadores, o uso de técnicas como a anonimização e a pseudonimização emerge como uma solução eficaz. Essas ferramentas tecnológicas ajudam a garantir a privacidade dos dados pessoais, enquanto preservam a integridade e segurança proporcionadas pela blockchain.

A anonimização é o processo pelo qual os dados pessoais são modificados de tal forma que o titular não pode ser identificado, direta ou indiretamente. De acordo com a LGPD, uma vez que os dados são anonimizados, eles deixam de ser

considerados "dados pessoais", o que os exclui das obrigações legais relacionadas à proteção de dados, como o direito ao esquecimento. A anonimização deve ser irreversível, garantindo que os dados não possam ser associados ao titular, mesmo que combinados com outras informações disponíveis (LGPD, Art. 12).

Do ponto de vista tecnológico, a anonimização pode ser alcançada por meio de técnicas como hashing, onde os dados são convertidos em uma sequência fixa de caracteres que não podem ser revertidos ao original. Outra técnica comumente usada é a agregação, onde os dados são combinados em grupos maiores, eliminando qualquer vínculo individual com o titular dos dados.

Por outro lado, a pseudonimização é o processo de substituir identificadores diretos, como nome e CPF, por um pseudônimo ou código. Ao contrário da anonimização, a pseudonimização ainda permite a reidentificação dos dados se houver acesso aos identificadores correspondentes. A LGPD considera que dados pseudonimizados ainda são dados pessoais, mas oferece uma camada adicional de segurança ao separar os identificadores diretos dos dados sensíveis (LGPD, Art. 13).

A pseudonimização é amplamente utilizada em situações em que é necessário manter a possibilidade de reidentificação, como em auditorias ou investigações internas, mas garante que os dados não possam ser prontamente identificados por terceiros não autorizados.

A tecnologia de blockchain pode incorporar ambas as técnicas, oferecendo maior flexibilidade para as empresas que precisam tratar dados sensíveis dos trabalhadores. Por exemplo, ao utilizar anonimização, os dados podem ser registrados na blockchain sem qualquer identificação direta do titular. Mesmo em uma cadeia de blocos pública e acessível, a anonimização protege a identidade dos trabalhadores, garantindo conformidade com a LGPD, ao mesmo tempo em que preserva a transparência e a imutabilidade das transações na blockchain.

Por outro lado, a pseudonimização permite que as empresas utilizem os benefícios de uma blockchain híbrida ou privada, onde os identificadores reais podem ser mantidos fora da blockchain ou em uma parte privada da rede e apenas pseudônimos são registrados na parte pública. Isso cria uma separação entre os dados sensíveis e os registros imutáveis, oferecendo controle e flexibilidade ao mesmo tempo em que respeita a necessidade de proteção dos dados.

A blockchain oferece vantagens claras em termos de segurança e transparência, a natureza imutável dessa tecnologia impõe dificuldades para a

implementação do direito ao esquecimento. No entanto, ao incorporar a anonimização, os dados podem ser tratados de maneira que o titular não possa ser identificado, reduzindo a necessidade de exclusão posterior. Da mesma forma, a pseudonimização preserva a privacidade dos dados ao minimizar o risco de exposição, permitindo que as empresas mantenham a flexibilidade necessária para operações contínuas, como auditorias e gestão interna, sem comprometer a conformidade legal.

5. IMPLICAÇÕES JURÍDICAS DA ADOÇÃO DA BLOCKCHAIN

A blockchain altera a dinâmica da responsabilidade no tratamento de dados. Em modelos tradicionais, os controladores e operadores de dados são os principais responsáveis pelo cumprimento da legislação de proteção de dados, devendo garantir a segurança e confidencialidade das informações tratadas. Quando a blockchain é utilizada, essa responsabilidade pode se dispersar, pois a governança da rede é, muitas vezes, distribuída entre diversos nós, o que dificulta a identificação de um único responsável em caso de violação de dados ou tratamento inadequado.

No Brasil, a LGPD estabelece que os agentes de tratamento respondem solidariamente por violações. No entanto, em redes blockchain, especialmente as públicas, a identificação clara de controladores e operadores pode ser complexa. Nesse contexto, surge uma zona de incerteza quanto a quem será responsabilizado em caso de descumprimento das normas de proteção de dados. Em blockchains privadas ou híbridas, o controle é mais centralizado, o que facilita a definição de responsabilidades, mas ainda há questões abertas em termos de repartição de responsabilidades quando múltiplas entidades participam de uma mesma rede de blockchain.

A validade jurídica dos contratos inteligentes ("smart contracts") é indispensável, visto que, esses contratos são autoexecutáveis e podem ser utilizados para automatizar a execução de cláusulas contratuais, sem a necessidade de intervenção humana. No contexto trabalhista, isso pode ser extremamente útil para garantir o cumprimento de contratos de trabalho, pagamento de salários e outras obrigações legais. Contudo, a ausência de regulamentação específica sobre a utilização de contratos inteligentes no direito brasileiro e em outras jurisdições levanta dúvidas quanto à sua validade em disputas legais. Embora eles sejam reconhecidos

por sua eficiência, a interpretação jurídica dos termos desses contratos ainda precisa ser consolidada no cenário jurídico brasileiro.

A blockchain também apresenta desafios significativos em relação à transferência internacional de dados, especialmente em redes públicas que operam em uma infraestrutura global. A LGPD e o GDPR impõem regras rígidas sobre como e quando os dados podem ser transferidos para fora do país de origem, exigindo garantias contratuais e de segurança para proteger os dados durante essas transferências. Nas blockchains públicas, onde os dados são distribuídos globalmente entre diversos nós, pode ser difícil garantir que as transferências internacionais estejam em conformidade com as legislações de proteção de dados. Além disso, a governança descentralizada torna a supervisão e o controle dessas transferências mais complexas, criando um desafio adicional para empresas que precisam aderir a normas de conformidade internacional.

As implicações jurídicas da adoção da blockchain são vastas e desafiadoras, especialmente no que diz respeito à conformidade com a LGPD e outras legislações de proteção de dados. Embora a tecnologia ofereça avanços significativos em termos de segurança e eficiência, sua implementação exige atenção cuidadosa às normas jurídicas vigentes, especialmente no que tange à responsabilidade legal, validade de contratos inteligentes, e transferência internacional de dados. Para que as empresas possam aproveitar plenamente os benefícios da blockchain, será essencial desenvolver uma infraestrutura jurídica que contemple as especificidades dessa tecnologia, garantindo a proteção dos direitos dos trabalhadores e a segurança dos dados tratados.

6. CONCLUSÃO

A evolução tecnológica correlacionada à blockchain, traz inovações para a avaliação de dados trabalhistas, proporciona maior segurança e transparência quando comparada com métodos tradicionais. Entretanto, a aplicação dessa tecnologia no ambiente corporativo deve ser efetuada conforme a Lei Geral de Proteção de Dados (LGPD), sobretudo em relação aos direitos fundamentais dos titulares de dados, como a privacidade, o direito à retificação e o direito ao esquecimento.

O estudo mostrou que a blockchain, por suas características de imutabilidade e descentralização, oferece uma camada adicional de proteção contra fraudes e manipulações no que tange à proteção de dados pessoais de trabalhadores, controlando o acesso e rastreando as transações de forma automatizada. Porém, essas características impõem desafios legais, como a impossibilidade de remover ou alterar dados na blockchain, o que entra em conflito com a flexibilidade exigida pela LGPD, em casos de solicitações de exclusão ou alteração de dados.

Para superar esses obstáculos, o uso de técnicas de anonimização e pseudonimização surgiram como soluções viáveis. A anonimização, que torna os dados irreconhecíveis e impossíveis de associar ao seu titular, oferece uma saída para a manutenção da conformidade com a LGPD, evitando a necessidade de exclusão dos dados registrados na blockchain. A pseudonimização, por sua vez, atua como uma camada adicional de segurança, protegendo os dados sem comprometer sua rastreabilidade, embora mantenha a possibilidade de reidentificação sob condições específicas. Essas técnicas reduzem os impactos da imutabilidade da blockchain e garantem que as empresas possam continuar utilizando a tecnologia sem infringir os direitos dos titulares.

Outro ponto relevante abordado foi a substituição dos agentes de tratamento humanos por mecanismos automatizados, como os contratos inteligentes (smart contracts). Esses contratos permitem a autoexecução de cláusulas previamente acordadas, eliminando a necessidade de intermediários e reduzindo significativamente os riscos de manipulação ou erro humano.

É possível perceber que ainda existem obstáculos legais e técnicos que limitam a plena adoção da blockchain. A falta de clareza jurídica sobre a responsabilidade dos agentes de tratamento em redes descentralizadas, o desafio de garantir a validade dos contratos inteligentes e os riscos associados à transferência internacional de dados são questões que precisam ser enfrentadas para garantir a e plena legislação vigente. Além disso, problemas de escalabilidade e compatibilidade com sistemas legados também foram identificados como barreiras técnicas que devem ser solucionadas para garantir que a tecnologia seja viável para o uso em larga escala, especialmente no setor corporativo.

Portanto, embora a blockchain ofereça um caminho promissor para o tratamento seguro de dados trabalhistas, sua concretização precisa ser acompanhada de uma revisão detalhada das estruturas jurídicas e técnicas

atualmente em vigor. O uso de blockchains privadas ou híbridas parece ser a melhor opção para as empresas que desejam adotar essa tecnologia enquanto garantem a proteção de dados pessoais e o respeito aos direitos dos trabalhadores, conforme estabelecido pela LGPD.

Por fim, a aplicabilidade da blockchain deve ser vista como um processo gradual e planejado, por meio de soluções jurídicas e técnicas que garantam a segurança e a privacidade dos dados, sem comprometer a confiança do sistema. À medida que as regulamentações evoluem e a tecnologia se adapta, é possível que a blockchain se consolide como uma ferramenta essencial no tratamento de dados, promovendo um ambiente benéfico para as empresas e os trabalhadores.

REFERÊNCIAS BIBLIOGRÁFICAS

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

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02/07/2024.

CORRALES, M; FENWICK, M; HAPIO, H (Ed.). **Legal Tech, Smart Contracts and Blockchain.** Springer, 2019. 276 p.,

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

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://diegoazziufabc.wordpress.com/wp-content/uploads/2017/08/estudo-de-arquiteturas-dos-blockchains.pdf>. Acesso em: 21/08/2024.

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

NAKAMOTO, Satoshi. Bitcoin. **A peer-to-peer electronic cash system.** 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 08/08/2024.

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

SCHWAB, Klaus. **A 4ª Revolução Industrial.** São Paulo, Edipro, 2016.

Tapscott, D., & Tapscott, A. (2016). **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the world.** Penguin, New York.