

**XXXI CONGRESSO NACIONAL DO
CONPEDI BRASÍLIA - DF**

**DIREITO, INOVAÇÃO, PROPRIEDADE
INTELECTUAL E CONCORRÊNCIA**

YURI NATHAN DA COSTA LANNES

JOÃO MARCELO DE LIMA ASSAFIM

CLAUDIA MARIA DA SILVA BEZERRA

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydée Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

D597

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA [Recurso eletrônico on-line]
organização CONPEDI

Coordenadores: Yuri Nathan da Costa Lannes, João Marcelo de Lima Assafim, Claudia Maria Da Silva Bezerra –
Florianópolis: CONPEDI, 2024.

Inclui bibliografia

ISBN: 978-65-5274-064-9

Modo de acesso: www.conpedi.org.br em publicações

Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito e inovação. 3. Propriedade intelectual e concorrência. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34



XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

Apresentação

O XXXI CONGRESSO NACIONAL DO CONPEDI, realizado em Brasília-DF, de 27 a 29 de novembro de 2024, trouxe como temática central "Um Olhar a partir da Inovação e das Novas Tecnologias", destacando a crescente influência das transformações tecnológicas no campo jurídico e social. Neste contexto, o Grupo de Trabalho "Direito, Inovação, Propriedade Intelectual e Concorrência" reuniu pesquisas que exploram as interfaces entre o Direito, os avanços tecnológicos e os desafios contemporâneos na regulamentação da inovação e da propriedade intelectual.

Os artigos apresentados abordam uma ampla gama de temas, refletindo a diversidade e a complexidade das questões que emergem no cenário jurídico contemporâneo. Desde a regulação de conteúdos digitais e o impacto das novas tecnologias na propriedade intelectual até os desafios éticos e jurídicos da inteligência artificial, as reflexões destacam como o Direito precisa se adaptar para responder às demandas de uma sociedade em constante transformação tecnológica.

Esta coletânea inclui análises sobre a formação de contratos eletrônicos com o uso de inteligência artificial, as implicações do blockchain e da Lei Geral de Proteção de Dados (LGPD) para a conformidade empresarial, e os desafios relacionados à moderação de conteúdo em plataformas digitais. Além disso, temas como os impactos das patentes farmacêuticas na saúde pública, a relação entre criação intelectual e direitos autorais no contexto da inteligência artificial, e as inovações no acesso à justiça por meio das serventias extrajudiciais são amplamente discutidos.

Os trabalhos refletem o esforço dos pesquisadores em conectar os avanços tecnológicos à proteção dos direitos fundamentais, à promoção da inovação e à garantia de concorrência justa no mercado. Este volume é um convite ao leitor para explorar as múltiplas dimensões do Direito frente à inovação, promovendo uma compreensão aprofundada e interdisciplinar sobre os desafios do presente e as oportunidades para o futuro.

Agradecemos a todos os autores, avaliadores e organizadores pelo compromisso em contribuir para o avanço do conhecimento jurídico e tecnológico. Que esta obra inspire novas reflexões e colaborações acadêmicas.

Boa leitura!

Dr. Yuri Nathan da Costa Lannes

Faculdade de Direito de Franca

Dr. João Marcelo de Lima Assafim

Universidade Federal do Rio de Janeiro

Dra. Claudia Maria da Silva Bezerra

IDEA – Direito – São Luís e PPGDIR-UFMA

EMPREENDEDORISMO, BLOCKCHAIN E LGPD: DESAFIOS E OPORTUNIDADES NA CONFORMIDADE EMPRESARIAL

ENTREPRENEURSHIP, BLOCKCHAIN AND LGPD: CHALLENGES AND OPPORTUNITIES IN BUSINESS COMPLIANCE

Thiago do Carmo Santana ¹
Deise Marcelino Da Silva ²

Resumo

Neste estudo, exploramos a interseção entre Direito, Inovação, Tecnologias emergentes, Desenvolvimento empresarial e o Sistema Jurídico, com ênfase no impacto do Blockchain e da Lei Geral de Proteção de Dados (LGPD) na conformidade empresarial. Através de uma abordagem dedutiva, investigamos os desafios e oportunidades que se apresentam para as empresas na era digital. Analisamos como a tecnologia Blockchain pode proporcionar soluções inovadoras para a segurança e transparência dos dados, elementos cruciais no ambiente empresarial atual. Paralelamente, avaliamos o impacto da LGPD na proteção de dados, destacando a importância de uma adaptação estratégica às exigências de privacidade. A convergência dessas áreas evidencia a necessidade de um Sistema Jurídico flexível e atualizado, capaz de acompanhar o rápido avanço tecnológico e de inovação, assegurando a conformidade e a competitividade das empresas no cenário global. Este estudo oferece uma compreensão aprofundada de como a interação entre o Direito e as novas tecnologias está moldando o panorama empresarial contemporâneo.

Palavras-chave: Direito, Blockchain, Lgpd, Inovação tecnológica, Conformidade empresarial

Abstract/Resumen/Résumé

In this study, we explore the intersection between Law, Innovation, Emerging Technologies, Business Development and the Legal System, with an emphasis on the impact of Blockchain and the General Data Protection Law (LGPD) on business compliance. Using a deductive approach, we investigate the challenges and opportunities that companies face in the digital age. We analyze how Blockchain technology can provide innovative solutions for data security and transparency, crucial elements in today's business environment. At the same time, we evaluate the impact of the LGPD on data protection, highlighting the importance of strategic adaptation to privacy requirements. The convergence of these areas highlights the need for a flexible and updated Legal System, capable of keeping up with rapid technological

¹ Graduação em direito pela Faculdade Objetivo. Possui Pós-graduação pela Faculdade Damáio de Jesus, Mestrando do Programa de Mestrado em "Direito, Sociedade e Tecnologia" das Faculdades Londrina.

² Possui doutorado em Direito pela Universidade Católica de Santos. Professora da graduação e do Programa de Mestrado em "Direito, Sociedade e Tecnologia" das Faculdades Londrina

advances and innovation, ensuring the compliance and competitiveness of companies on the global stage. This study offers an in-depth understanding of how the interaction between law and new technologies is shaping the contemporary business landscape.

Keywords/Palabras-claves/Mots-clés: Law, Blockchain, IgpD, Technological innovation, Business compliance

INTRODUÇÃO

No cenário atual de empreendedorismo digital, a rápida evolução de tecnologias disruptivas, como o Blockchain, está evoluindo profundamente o ambiente empresarial. Esse avanço tecnológico, aliado à recente implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil, cria um contexto complexo e multifacetado, desafiando as empresas a se adaptarem a um cenário em constante evolução, onde a inovação digital precisa coexistir com rigorosas exigências legais de proteção de dados.

Este estudo se apresenta como uma ferramenta essencial para compreender como as empresas podem não apenas se ajustar a esse novo cenário, mas também aproveitar as oportunidades que ele proporciona. A conformidade legal deixou de ser apenas uma obrigação e passou a ser um motor para a inovação e um diferencial competitivo no mercado global. Assim, entender e navegar nesse ambiente complexo tornou-se vital para o sucesso empresarial.

Os objetivos deste estudo são duplos. Em primeiro lugar, busque-se analisar a interseção entre empreendedorismo, Blockchain e LGPD, com o intuito de identificar os desafios e as oportunidades que emergem dessa interação. O estudo examinará especificamente o impacto do Blockchain na proteção e segurança de dados, avaliará a conformidade das empresas com a LGPD e proporá estratégias para a integração eficaz dessas empresas. Essas análises têm como objetivo fornecer insights práticos e diretrizes estratégicas para as empresas.

Por fim, o estudo parte das hipóteses de que a integração do Blockchain nos sistemas empresariais pode ser uma solução robusta para atender às exigências da LGPD. Essa integração tem o potencial de contribuição para a inovação e o desenvolvimento tecnológico, ao mesmo tempo em que garante a conformidade com as normativas de proteção de dados. Assim, esta pesquisa não apenas aborda um problema prático imediatamente, mas também contribui para o entendimento mais amplo do mundo de como as novas tecnologias podem ser harmonizadas com os critérios legais no dinamismo empresarial contemporâneo.

1. BLOCKCHAIN E EMPREENDEDORISMO - TRANSFORMANDO O ECOSISTEMA EMPRESARIAL

Antes mesmo de fazermos um paralelo entre o *Blockchain* e o Empreendedorismo precisamos elucidar alguns conceitos importantes para melhor compreensão dos assuntos tratados, para isto iremos conceituar inicialmente o *Blockchain* e depois o Empreendedorismo, para somente então estabelecer esta relação.

O *Blockchain* é uma tecnologia que surgiu em meados de 2008, com a ascensão do *Bitcoin*, esta tecnologia foi desenvolvida por Satoshi Nakamoto, nome utilizado por um programador ou grupo de programadores que criaram a criptomoeda *Bitcoin* e todo o ecossistema em torno dessa criptomoeda. O *Blockchain* é uma cadeia de blocos que armazena informações das transações, que são validadas por computadores ligados a esta rede, os chamados “nós”.

Conforme o doutrinador Klaus Schwab, o blockchain opera como um protocolo seguro, onde há uma colaboração mútua entre os computadores da rede. Esses computadores trabalham em conjunto para verificar as transações antes de aprová-las:

A tecnologia que sustenta o blockchain cria confiança, permitindo que pessoas que não o conheçam (e, portanto, não têm nenhuma base subjacente de confiança) colaborem sem ter de passar por uma autoridade central neutra – ou seja, um depositário ou livro contábil central. Em essência, o blockchain, 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. (Shwab, 2016)

Também nesse contexto, a doutrinadora Laurence (2019) detalha que as *blockchains* representam uma abordagem revolucionária em relação às bases de dados distribuídas, mesclando tecnologias já existentes de maneira inédita. Segundo ela, os blockchains são descritos como bases de dados coletivas gerenciadas por conjuntos de indivíduos, responsáveis pelo armazenamento e distribuição de informações. Esta tecnologia, variada em tipos e aplicações, encontra-se incorporada em diversas plataformas e hardwares globalmente.

A tecnologia *blockchain* é uma estrutura inovadora que possibilita a criação de um livro – razão de dados digitais, compartilhado por uma rede independente e descentralizada. O *blockchain* possui diversas aplicações práticas que vão além da já mais conhecida que é a financeira atrelada ao *bitcoin*, conforme leciona Schwab (2016):

Se, agora, a tecnologia do blockchain registra transações financeiras feitas com moedas digitais (o Bitcoin, por exemplo), futuramente ele servirá para registrar coisas bem diferentes, como nascimentos e óbitos, títulos de propriedade, certidões de casamento, diplomas escolares, pedidos às seguradoras, procedimentos médicos e votos. (Shwab, 2016)

Portanto ao analisarmos esta tecnologia disruptiva, percebe-se que a sua utilização poderá transcender os aspectos da mera checagem de transações por criptomoedas, esta tecnologia poderá ser utilizada para armazenar contratos, documentos e diversas outras formas de informações inclusive validando a autenticidade e confirmando a veracidade destas informações armazenadas nesta tecnologia.

Tem -se que ter em mente que a rede blockchain não é limitada a apenas um tipo de rede em si, mas possui vários tipos de redes *blockchain* que podem ser utilizadas para armazenar informações. São elas:

Blockchain públicos: São amplas redes difundidas, como o Bitcoin, que são administradas por meio de um token nativo. Esses blockchains são abertos à participação de qualquer pessoa e possuem o código aberto mantido pela comunidade;

Blockchain permissionados: São blockchains, como o Ripple, que controlam as funções que as pessoas podem desempenhar dentro da rede. Apesar de serem sistemas amplos e difusos que utilizam um token nativo, o código central pode ser aberto ou não;

Blockchain privados: Esses blockchains tendem a ser menores e não utilizam tokens. Sua adesão é controlada de forma rigorosa, sendo protegidos por associações que possuem membros conceituados e informações comerciais confidenciais. (Laurence, 2019).

Cabe analisar que estes conceitos sobre os tipos de *blockchains* existentes serão importantes no terceiro tópico deste trabalho quando for realizado um paralelo entre a aplicação desta tecnologia disruptiva com a proteção de dados pessoais, especialmente a aplicação da Lei Geral de Proteção de Dados Pessoais.

Outro ponto importante a ser debatido quando se menciona a tecnologia *blockchain* trabalhado pela doutrinadora Fabíola Greve e col. As características desse sistema de armazenamento de dados fornecem aos negócios realizados por meio dele incluem:

a) **Descentralização e Desintermediação:** as aplicações são realizadas de forma distribuída, com base na confiança entre as partes, dispensando a necessidade de um intermediário confiável para regular o negócio, graças ao sistema ponto a ponto;

b) **Disponibilidade e Integridade:** os dados registrados na cadeia de blocos são replicados em nós distribuídos por toda a rede, garantindo a segurança e disponibilidade do sistema;

c) **Transparência e Auditabilidade:** as transações no blockchain são públicas e podem ser verificadas e auditadas a qualquer momento;

d) **Imutabilidade e Irrefutabilidade:** uma vez inseridas no bloco, as informações das transações tornam-se imutáveis e não podem ser apagadas ou alteradas; atualizações só são possíveis por meio de novas transações registradas em novos blocos que indiquem as alterações;

e) **Privacidade e Anonimato:** as partes envolvidas têm a capacidade de controlar a publicidade e a privacidade de seus dados, utilizando suas chaves privadas para gerenciar essas informações.

Empreendedorismo é o ato de iniciar e gerenciar novos projetos, resolvendo problemas ou situações desafiadoras. Este termo é amplamente utilizado no ambiente de negócios, frequentemente associado ao lançamento de novas ou produtos inovadores.

Ser empreendedor envolve a habilidade de conquistar oportunidades e convertê-las em empreendimentos rentáveis. Um empreendedor, ao identificar uma necessidade no mercado, cria soluções que atendem a essa demanda, desenvolvendo produtos ou serviços que melhoram a experiência do cliente e agregam valor. Esse processo de solução de problemas pode ser canalizado em uma oportunidade de negócio lucrativo.

O termo "empreendedorismo" foi utilizado pela primeira vez pelo economista Joseph Alois Schumpeter (1883-1945), originário da Áustria. No livro "Capitalismo, Socialismo e Democracia", publicado em 1942, Schumpeter desenvolve uma "Teoria da Destruição Criativa". Esta teoria descreve o empreendedorismo, que engloba a inovação em produtos, serviços ou na criação de novas empresas, como uma forma de atender às necessidades não atendidas dos consumidores, identificadas pelo empreendedor.

O conceito moderno de empreendedorismo, desenvolvido por Robert D. Hisrich em seu livro "Empreendedorismo", descreve o termo como o processo de criar algo novo e valioso, que envolve a dedicação de tempo e esforço, a aceitação de possíveis riscos financeiros, psicológicos e sociais, e a obtenção de recompensas econômicas e pessoais como resultado desse empenho.

O empreendedorismo em blockchain está transformando o ecossistema empresarial, oferecendo oportunidades e desafios únicos. A tecnologia blockchain permite a criação de um registro público, imutável e descentralizado de transações, o que pode revolucionar diversos setores da economia e criar novas oportunidades para empreendedores inovadores.

O Blockchain oferece inúmeras características inovadoras e benefícios para os empreendedores como por exemplo rastreabilidade e prova de prejuízos, permitindo que os empreendedores sigam o histórico de transações e forneçam uma trilha de auditoria confiável para seus produtos e serviços. Os Contratos Inteligentes, uma funcionalidade do Blockchain, automatizam acordos e transações, gerando a necessidade de intermediários e custos. A tecnologia tem desempenhado um papel crucial para facilitar o acesso a investimentos por meio de ICOs¹ e STOs², permitindo que empresas alcancem investidores globais de forma mais eficiente. Uma das aplicações mais promissoras é a tokenização de ativos, que melhora a liquidez e facilita a transferência de propriedade.

No entanto, o empreendedorismo no campo do Blockchain enfrenta desafios importantes. As questões regulatórias e legais, decorrentes da natureza descentralizada do

¹ ICOs (Ofertas Iniciais de Moedas).

² STOs (Ofertas de Tokens de Segurança).

Blockchain, podem entrar em conflito com leis de privacidade e proteção de dados. Além disso, desafios técnicos como escalabilidade e desempenho são críticos, especialmente com o aumento no volume de transações e usuários. A adoção do Blockchain por empresas e consumidores também encontra barreiras, incluindo a resistência às novas tecnologias e a desconfiança dos consumidores.

A segurança e a privacidade são preocupações constantes. Embora o Blockchain seja geralmente considerado seguro, ele não é imune a ataques maliciosos, vulnerabilidades de softwares e falhas humanas. Superar esses desafios requer uma abordagem conjunta e inovadora, envolvendo tanto os empreendedores quanto as partes interessadas no ecossistema Blockchain.

Para ter sucesso no empreendedorismo com Blockchain, é essencial adotar estratégias que envolvam um entendimento profundo da tecnologia, identificar nichos de mercado promissores e alinhar a proposta de valor com as necessidades do mercado. A validação de ideias de negócio é crucial, assim como a flexibilidade para ajustar e iterar essas ideias. O Blockchain permite a criação de modelos de negócios inovadores e disruptivos, como a tokenização de ativos e os contratos inteligentes. Nenhum financiamento de startups e projetos em Blockchain, estratégias como ICOs, STOs, captação de investimentos de capital de risco e participação em programas de vantagem são acessíveis.

A colaboração e a formação de parcerias estratégicas são fundamentais no ecossistema Blockchain, exigindo integração com outras startups, instituições financeiras e governamentais, além da participação em consórcios e iniciativas setoriais. O empreendedorismo no Blockchain exige visão, inovação, colaboração e um conhecimento profundo de um ecossistema em constante transformação.

Além disso, construir um ecossistema empresarial é uma iniciativa vital para empresas de qualquer tamanho que desejam sustentar suas operações a longo prazo. Um ecossistema empresarial envolve a formação de parcerias e a criação de uma rede de contatos, o que pode viabilizar a personalização das soluções oferecidas e aumentar a produtividade.

Por fim, o futuro do empreendedorismo em Blockchain é promissor, com potencial para transformar diversos setores da economia e criar novas oportunidades de inovação. A tecnologia oferece novas perspectivas para o desenvolvimento de serviços e produtos, embora ainda enfrente desafios como escalabilidade, adoção em massa e questões regulatórias. As implicações sociais, econômicas e tecnológicas do Blockchain no contexto do empreendedorismo são vastas, com impactos potenciais na democratização do acesso a serviços e recursos, redução da dependência de intermediários e aumento da confiança nas transações.

Contudo, é essencial que os inovadores considerem questões como privacidade, segurança de dados e exclusão digital ao soluções desenvolvidas baseadas em Blockchain.

2. LGPD E CONFORMIDADE EMPRESARIAL - NAVEGANDO NO NOVO AMBIENTE LEGAL

Como mencionado anteriormente, um dos maiores desafios para a implementação do sistema Blockchain nas empresas é a adequação desse sistema à legislação que protege e regula os dados pessoais das pessoas físicas. Nesse sentido, é fundamental, antes de analisarmos a aplicação do Blockchain nas empresas, esclarecer como se dá a tutela dos dados pessoais no sistema jurídico brasileiro e quais são os conceitos abrangidos pela Lei Geral de Proteção de Dados Pessoais (LGPD).

A proteção da privacidade busca garantir a autonomia pessoal e assegurar as interações entre os indivíduos e a sociedade, abrangendo governos, empresas e outras organizações. É importante notar que a noção de privacidade pode variar de acordo com contextos culturais e individuais.

Para os estudiosos Bastos e Martins, o direito à privacidade é definido como o direito de cada pessoa de evitar interferências externas em sua vida privada e familiar, além de controlar o acesso a informações pessoais. A privacidade é considerada um direito fundamental e uma expressão da dignidade humana, pois envolve o controle sobre os dados pessoais de cada indivíduo.

[...] faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre essa área da manifestação existencial do ser humano. (Bastos; Martins, 1989, p. 63).

Historicamente, a privacidade tem sido um elemento central na filosofia, com raízes profundas no pensamento cristão. Santo Agostinho, por exemplo, considerava a intimidade como um espaço de reflexão pessoal e espiritual. Ao longo do tempo, a compreensão da privacidade evoluiu, especialmente com o advento da Internet e as transformações sociais que ela provocou. Um marco importante nessa discussão foi o artigo "The Right to Privacy", de Warren e Brandeis, que destacou como as mudanças sociais e tecnológicas impactam esse direito fundamental.

Hoje, com a proliferação das redes sociais e a constante disseminação de informações na mídia, torna-se cada vez mais difícil estabelecer uma linha clara entre o que é público e o que pertence à esfera privada dos indivíduos. Nesse contexto, o doutrinador Fruet aborda a

complexidade de definir limites legais precisos para proteger a privacidade sem comprometer a liberdade de imprensa. É essencial encontrar um equilíbrio entre os direitos individuais e o interesse público.

No ordenamento jurídico brasileiro, o direito à privacidade está profundamente enraizado na Constituição Federal de 1988, especificamente no artigo 5º, inciso X, onde é considerado um direito de personalidade. A Constituição diferencia entre intimidade e vida privada, cada uma com suas próprias implicações legais.

O doutrinador Heirinch Henkel apud Frota (2007) desenvolveu a teoria dos Círculos Concêntricos, ou das Esferas, para ilustrar como a privacidade é composta por diferentes camadas de exposição pessoal. Nesse contexto, identificam-se três camadas distintas de privacidade que refletem os diferentes níveis de exposição de um indivíduo, são elas:

Esfera Privada (ou Anonimato): Esta é a camada mais externa e se refere ao conjunto de informações e atividades que uma pessoa prefere manter ocultas ou privadas do público em geral. Aqui, a ênfase está na proteção contra a intromissão não desejada e no controle sobre o que é compartilhado com o mundo exterior. Por exemplo, hábitos pessoais, local de residência, ou detalhes sobre a vida cotidiana de uma pessoa podem se enquadrar nesta esfera.

Esfera da Intimidade: A camada intermediária concentra-se em informações e aspectos da vida de uma pessoa que são compartilhados apenas com um círculo restrito de pessoas de confiança, como familiares e amigos íntimos. Esta esfera abriga detalhes mais pessoais e sensíveis, que não são divulgados publicamente, mas que podem ser compartilhados em um ambiente íntimo e de confiança.

Esfera do Segredo: Esta é a camada mais interna e privada, que contém informações extremamente sensíveis e pessoais que o indivíduo deseja manter completamente confidenciais. Essas informações podem incluir pensamentos íntimos, desejos, escolhas sexuais, crenças religiosas ou outras informações que a pessoa considera como parte integral de sua identidade pessoal e que raramente, se alguma vez, são reveladas a outros.

Cada uma dessas esferas de privacidade destaca a complexidade do conceito, sublinhando que a privacidade não se resume apenas ao ocultamento de informações, mas também à gestão de quem tem acesso a diferentes níveis de dados pessoais. Esse modelo é particularmente útil para compreender como diferentes tipos de informações ocultas, níveis variados de proteção e atenção, especialmente em um contexto em que a tecnologia e a coleta massiva de dados envolvem a privacidade um desafio crescente.

Hoje, a proteção da privacidade de dados tornou-se essencial, devido à presença cada vez maior da tecnologia em nossas vidas. Leis e regulamentações são fundamentais para proteger os dados pessoais, especialmente em áreas sensíveis como a saúde.

No Brasil, o ordenamento jurídico já conta com várias normas externas para a proteção de dados pessoais e informações. Exemplos disso incluem a Lei de Acesso à Informação (Lei n.º 12.527/2011), o Marco Civil da Internet (Lei n.º 12.965/2014) e o Código de Defesa do Consumidor (Lei n.º 8.078/1990), que estabelece diretrizes para garantir a privacidade e a

proteção dos dados pessoais de indivíduos e consumidores. No entanto, essas normativas se mostraram insuficientes para garantir uma proteção abrangente aos dados pessoais, o que levou à necessidade de criação da Lei Geral de Proteção de Dados (LGPD), elaborada em 2018. A LGPD foi concebida com o objetivo de proteger os dados pessoal dos indivíduos, coletado por empresas sobre seus funcionários, clientes, parceiros, acionistas e outros.

Conforme a Doutora Patrícia Peck Pinheiro (2018) sobre a LGPD:

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

A Lei Geral de Proteção de Dados (LGPD) do Brasil, que contém 65 artigos, foi inspirada na General Data Protection Regulation (GDPR) da Europa, uma legislação focada na proteção de dados pessoais dos indivíduos. Esta regulamentação brasileira é fundamentada em princípios que asseguram sua eficácia e relevância no cenário nacional. Ela tem como objetivo a proteção dos direitos fundamentais de liberdade e privacidade, além de promover a intimidade do cidadão. A LGPD tem como objetivo promover o livre desenvolvimento da personalidade da pessoa natural, a garantia dos direitos de personalidade dos indivíduos e o fomento à inovação.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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

Um ponto fundamental a ser destacado sobre a LGPD é que esta protege e resguarda dois tipos de dados em seu artigo 5º, inciso I e II, que são: os dados pessoais que inclui toda e qualquer informação relacionada a um indivíduo que seja passível de identificar ou identificável como por exemplo nome, documentos pessoais, endereço, entre outros e os dados sensíveis que são aquelas informações que se forem reveladas podem causar desconforto ou constrangimento ao titular, como posição política, orientação sexual, condições de saúde, entre outras.

Esse regramento brasileiro possui a função de resguardar a proteção de dados pessoais e sensíveis de todos os brasileiros natos ou naturalizados em território nacional, portanto possui aplicabilidade para todas as pessoas jurídicas sejam elas empresas estrangeiras, organizações não governamentais, empresas de pequeno porte, microempresas, empresas de grande porte, médias empresas, empresas brasileiras, startups entre outras tanto na modalidade online como off line, independentemente do seu tamanho, área ou setor de atuação ou localidade devem se adaptar suas operações para cumprir os regramentos e diretrizes desta Lei. Sendo assim esta adaptação deve incluir a alocação de recursos para a segurança da informação e outros recursos técnicos, humanos e operacionais essenciais para proteger os dados coletados e armazenados de seus clientes. Essa medida é vital para evitar penalidades, multas ou danos irreparáveis à reputação da empresa em casos de escândalos ou vazamentos de dados.

Neste contexto, é apropriado que as empresas assumam total responsabilidade pelo tratamento, coleta e armazenamento de dados, alinhando-se com os três fundamentos da segurança da informação: confidencialidade, integridade e disponibilidade. Esta tríade, conhecida como CIA, concentra-se na proteção e privacidade online, na liberdade de expressão e na segurança dos dados de pessoas físicas (Peixoto, 2020).

Para cumprir os requisitos estabelecidos pela LGPD, as empresas que lidam com a coleta e manipulação de dados devem garantir que seus sistemas estejam protegidos contra o risco de vazamentos nos locais de armazenamento. É fundamental que a segurança da informação seja uma prioridade dentro das organizações, geralmente renovada por meio de uma política interna de segurança robusta. Por outro lado, Frazão (2018) destaca que essas situações podem ter um impacto significativo na vida dos indivíduos, influenciando fatores como acesso a crédito, oportunidades de emprego e serviços, além do risco de os dados serem incompletos ou desatualizados.

As empresas enfrentaram diversos desafios para se adequarem às exigências dessa legislação, que entrou em vigor há pouco mais de um ano, após uma *vacatio legislativa* de dois anos, apesar de ter sido promulgada em 2018. Embora todos os segmentos e tamanhos de empresas enfrentem dificuldades, já que multinacionais e grandes corporações têm mais facilidade para se ajustar à legislação. Devido aos seus recursos disponíveis, assessoria jurídica e estruturas organizacionais complexas, muitas empresas dessas iniciaram o processo de adequação logo após a promulgação da lei.

Em contrapartida, as micro e pequenas empresas enfrentam maiores desafios na adaptação à LGPD, devido a seus recursos mais limitados e estruturas organizacionais enxutas, onde, muitas vezes, uma única pessoa acumula múltiplas responsabilidades.

Para apoiar essas empresas menores, a Autoridade Nacional de Proteção de Dados (ANPD), criada pela própria lei, publicou em 27 de janeiro de 2022 a RESOLUÇÃO CD/ANPD N° 2, que define os agentes de pequeno porte e estabelece um tratamento diferenciado para eles na aplicação da Lei 13.709/2018. Essa resolução inclui flexibilizações em prazos, registros de operações de tratamento de dados, comunicações de incidentes de segurança, indicação de responsável pelo tratamento de dados e políticas de segurança.

A RESOLUÇÃO CD/ANPD N° 2 detalha medidas específicas para agentes de tratamento de pequeno porte, como microempresas e startups. Entre essas medidas, há a possibilidade de manter registros de tratamento de dados de forma simplificada, procedimentos simplificados para a comunicação de incidentes de segurança, e a autorização da obrigação de nomear um encarregado pelo tratamento de dados. Além disso, esses agentes têm prazos estendidos para cumprir diversas obrigações previstas na LGPD, o que facilita sua adaptação às exigências da legislação.

Art. 9º Os agentes de tratamento de pequeno porte podem cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do art. 37 da LGPD, de forma simplificada.

Art. 10. A ANPD disporá sobre flexibilização ou procedimento simplificado de comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da regulamentação específica.

Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.

Art. 13. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Art. 14. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro: I - no atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, §§ 3º e 5º da LGPD, nos termos de regulamentação específica;

II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos de regulamentação

específica, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada regulamentação;

III - no fornecimento de declaração clara e completa, prevista no art. 19, II da LGPD;

IV - em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento. (Brasil, 2018)

O primeiro passo para qualquer empresa que deseja se adequar à LGPD é realizar o mapeamento dos dados pessoais. Esse processo envolve identificar e documentar todo o fluxo de dados pessoais de clientes, colaboradores e fornecedores dentro da organização, desde a coleta até o armazenamento, necessidade, compartilhamento e tempo de retenção desses dados. A ANPD exige transparência sobre quais tipos de dados são coletados, se incluem informações sensíveis, e como são armazenados, com o objetivo de prevenir vazamentos ou usos indevidos. Embora ainda não exista um padrão único para o mapeamento, é essencial que as empresas adotem métodos eficazes para realizá-lo.

Outro aspecto crucial para a conformidade com a nova legislação é a gestão do consentimento. É obrigatório obter o consentimento do titular dos dados, que deve ser plenamente informado sobre quais dados estão sendo coletados, para qual finalidade e como serão compartilhados. As informações devem ser apresentadas de forma clara e acessível, para evitar qualquer vício de consentimento. Preferencialmente, a coleta de consentimento deve ser feita por escrito, o que pode exigir ajustes nos processos de atendimento ao cliente, como a inclusão de termos de consentimento e o treinamento dos funcionários. De acordo com o Art. 8º da LGPD, o consentimento deve ser expresso por escrito ou de maneira que demonstre claramente a vontade do titular. Assim, as empresas precisam estar atentas às exigências da lei para evitar consequências negativas decorrentes do não cumprimento.

É também essencial considerar as circunstâncias em que o processamento de dados é legalizado, conforme estipulado pelos artigos 7º a 16º da LGPD. Esses artigos estabelecem os critérios e condições para o tratamento de dados, incluindo a proteção dos dados pessoais de menores e as regras para o encerramento do processamento de dados pelas empresas, independentemente do seu tamanho, localização ou setor de atuação.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de

políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

- IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (Brasil, 2018)

Essas adaptações que as empresas devem implementar para se alinhar à nova legislação têm como principal objetivo evitar o descumprimento das normas estabelecidas. Isso se torna ainda mais relevante considerando que o artigo 52 da referida legislação detalha uma série de penalidades que podem ser aplicadas aos responsáveis pelo tratamento de dados em caso de infrações. Estas medidas punitivas vão desde advertências e multas até a proibição parcial ou total das atividades da empresa, o que pode impactar significativamente seus negócios.

3. SINERGIA ENTRE BLOCKCHAIN E LGPD - ESTRATÉGIAS PARA INOVAÇÃO E CONFORMIDADE

A relação entre o blockchain e a Lei Geral de Proteção de Dados (LGPD) suscita diferentes perspectivas. Por um lado, a Juíza e Pesquisadora de blockchain Renata Baião argumenta que o blockchain oferece um ambiente seguro para o armazenamento de informações pessoais, permitindo que o titular dos dados tenha controle sobre suas informações. Baião ressalta que, embora os registros no blockchain sejam permanentes, eles podem se tornar inacessíveis, inclusive por meio da ação do titular, ao excluir a chave privada ou o arquivo original.

Por outro lado, especialistas como Silva (2019) apontam para potenciais conflitos entre o tratamento de dados sensíveis e a natureza do blockchain. Um ponto de divergência é a possibilidade de atualização e exclusão de dados, prevista pela LGPD, para garantir a precisão das informações e permitir que os indivíduos solicitem a exclusão de dados desnecessários. No entanto, a imutabilidade do blockchain, que permite apenas adições, não facilita a exclusão de dados, o que gera desafios para a conformidade com a LGPD.

Além disso, é crucial considerar duas formas de chaves de segurança no blockchain: chaves privadas e chaves públicas. A chave privada permanece com o proprietário, enquanto a chave pública é amplamente conhecida e possibilita o compartilhamento de informações com outros (Aranha, 2021, p. 106).

Isso levanta questões controversas, como o direito ao esquecimento dentro do blockchain, um direito reforçado pela LGPD. A imutabilidade dos dados registrados na blockchain, uma característica central da tecnologia, gera dilemas, pois esses registros, uma vez inseridos em um contrato inteligente, permanecem permanentemente na rede e são autoexecutados conforme as condições disposições pelas partes envolvidas.

Apesar das críticas de que a conformidade regulatória de proteção de dados pessoais com a tecnologia blockchain seria impossível, essa visão não é totalmente verdadeira. É possível que o gestor, seja ele driver ou processador, avalie e decida como tratar os dados pessoais e sensíveis, considerando os custos e riscos associados a cada abordagem.

Para adaptar a tecnologia blockchain às leis de proteção de dados pessoais, é essencial observar qual legislação será aplicada em cada caso específico, determinado pela territorialidade e pela decisão do gestor controlador ou processador de dados pessoais, que deve identificar a base legal para o processamento, garantindo o cumprimento dos direitos dos titulares.

Em redes abertas de blockchain, o desafio principal é garantir que todas as partes que acessam os dados pessoais tenham uma autorização legal para fazê-lo, além de distribuir responsabilidades em casos de uso indevido. No entanto, ao utilizar redes de blockchain fechadas e permissivas, essa dificuldade é minimizada, pois geralmente há uma relação contratual entre aceleração/controladores e usuários.

Existem várias soluções blockchain que podem ser aplicadas para alcançar a conformidade com a proteção de dados, incluindo configurações on-chain/off-chain, armazenamento de dados em hash na blockchain, controles de acesso baseados em funções, Zero Knowledge Proofs e Fully Homomorphic Encryption (FHE). Cada uma dessas soluções apresenta suas próprias vantagens e limitações em termos de privacidade, desempenho e conformidade regulatória.

Configurações On-chain/Off-chain: Esta abordagem envolve decidir quais dados serão armazenados diretamente na blockchain (on-chain) e quais serão mantidos fora dela (off-chain). Manter dados sensíveis off-chain pode melhorar a privacidade, pois esses dados não estão diretamente acessíveis na blockchain. No entanto, isso pode reduzir a transparência e a eficácia da blockchain em fornecer um registro imutável.

Armazenamento de Dados de Hash na Blockchain: Esta técnica envolve armazenar apenas o hash de dados sensíveis na blockchain, mantendo os dados reais off-chain. Isso oferece um equilíbrio entre segurança e privacidade, pois os hashes são imutáveis

e verificáveis, mas não revelam diretamente os dados subjacentes. No entanto, se os hashes puderem ser combinados com outras informações para identificar indivíduos, eles ainda podem ser considerados dados pessoais sob a legislação de proteção de dados.

Zero Knowledge-Proof (Prova de Conhecimento Zero): Esta tecnologia permite que uma parte comprove a validade de uma afirmação sem revelar os próprios dados. É útil para manter a privacidade dos dados, mas pode ser desafiador implementar devido à complexidade técnica e ao potencial de aumento na latência (tempo de processamento) das transações.

Fully Homomorphic Encryption (FHE): Esta técnica permite a realização de cálculos em dados criptografados, resultando em um resultado criptografado. Isso significa que os dados podem ser compartilhados e processados sem a necessidade de descriptografá-los, oferecendo um alto nível de segurança e privacidade. No entanto, o FHE é notoriamente lento e pode não ser prático para algumas aplicações devido ao seu desempenho limitado. (Revoredo, 2020)

4. CONCLUSÃO

O empreendedorismo, ao se deparar com a tecnologia emergente do blockchain e conforme as exigências da Lei Geral de Proteção de Dados (LGPD), enfrenta uma dualidade complexa de desafios e oportunidades. A interação entre essas inovações gerou uma série de opiniões divergentes, destacando tanto o potencial transformador quanto as implicações específicas dessa relação.

Por um lado, o blockchain promete um ambiente seguro e eficiente para a gestão de dados, utilizando técnicas avançadas de criptografia que têm o poder de revolucionar operações e finanças em diversos setores. A flexibilidade dessa tecnologia permite que as empresas controlem a quantidade de dados compartilhados, ajustando-se às suas necessidades de confidencialidade e funcionalidade. No entanto, esta inovação apresenta desafios como a limitação na velocidade das transações, altos custos computacionais e o risco de incluir dados irrelevantes no sistema.

Do ponto de vista jurídico, a evolução do direito digital, marcada por legislações como o Marco Civil da Internet e a LGPD, tenta acompanhar o rápido avanço das tecnologias. Contudo, ainda há um caminho a ser percorrido para tecnologias globais emergentes como o blockchain.

Um desafio significativo no uso do blockchain é sua natureza imutável, que, embora garanta segurança nas transações, entra em conflito com direitos fundamentais como a privacidade e o direito ao esquecimento, ambos protegidos pela LGPD. Essa contradição evidencia a necessidade de um equilíbrio delicado entre a preservação da integridade dos dados e a proteção dos direitos dos indivíduos.

Diante disso, as empresas que buscam explorar as potencialidades do blockchain devem considerar a formação de consórcios e a colaboração com reguladores e outras partes interessadas para estabelecer padrões práticos e específicos. Essa abordagem colaborativa não apenas facilita a conformidade regulatória, mas também abre novas possibilidades de negócios, agregando valor e promovendo uma cooperação eficaz entre diferentes entidades.

Em resumo, o blockchain oferece um horizonte promissor para o empreendedorismo moderno. Com uma abordagem estratégica e colaborativa, é possível superar os desafios e aproveitar as oportunidades que essa tecnologia disruptiva proporciona. À medida que a legislação evolui para integrar as inovações digitais, os empreendedores precisam estar preparados para navegar nesse cenário dinâmico, buscando sempre a harmonia entre a inovação tecnológica e a conformidade legal.

REFERÊNCIAS

ARANHA, Christian. Bitcoin, Blockchain e muito dinheiro: uma nova chance para o mundo. 2ª Ed. Rio de Janeiro: Valentina, 2021.

BAIÃO, Renata B. S. M.. Afinal, blockchain é incompatível com a LGPD?. Disponível em: <<https://www.serpro.gov.br/lgpd/noticias/2019/blockchain-lgpd-dados-pessoais-brasil>>. Acesso em: 08 de dezembro de 2023.

BARROS, Jéssica. Blockchain: A disruptiva fronteira do Empreendedorismo. RapaduraTech. 08 de agosto de 2023. Disponível em: <https://rapaduratech.com.br/blockchain-e-empreendedorismo/> Acesso em: 06.dez.2023

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. Comentários à Constituição do Brasil. São Paulo: Saraiva, 1989, vol. 2, p. 63.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 07 dez.. 2023.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. [Internet]. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 07 dez. 2023

BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal [...]. [Internet]. 2011. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 07 dez. 2023

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. [Internet]. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 07 dez. 2023

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).. [Internet]. 2018 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm Acesso em 07 dez. 2023

BRASIL. RESOLUÇÃO CD/ANPD Nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. [Internet]. 2022 Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019> Acesso em 07 dez. 2023

COUTO, Marcela. O que é empreendedorismo e como ser um empreendedor?. BlogNuvemshop.2023. Disponível em: <https://www.nuvemshop.com.br/blog/o-que-e-empreendedorismo/> Acesso em: 06 dez. 2023

FRAZÃO, Ana. Data-driven economy e seus impactos sobre os direitos de personalidade, Jota, publicado em 17.7.2018. Disponível em <<https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade-17072018>>. Acesso em: 07.dez. 2023.

FRUET, G. Lady Di e a Privacidade. Disponível em: <<https://www.folhadelondrina.com.br/opiniao/lady-divo-fruet-39542.html?d=1>>. Acesso em: 07 dez. 2023.

FROTA, H. A. A proteção da vida privada, da intimidade e do segredo no Direito Brasileiro Comparado. Revista Jurídica Unijus. V.9, n. 11, Uberaba. 2007.

GREVE, Fabíola Greve et al. Blockchain e a Revolução do Consenso sob Demanda. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) - Minicursos, [S.l.], may 2018. Disponível em: <<http://143.54.25.88/index.php/sbrccminicursos/article/view/1770>>. Acesso em: 07 dezembro 2023

HISRICH, Robert D.; et al. Empreendedorismo. Tradução: COSTA, Francisco Araújo da. The MCGraw Hill Education: AMGH. 9ª Edição. Porto Alegre: 2014.

LAURENCE, Tiana. Blockchain Para Leigos. Editora Alta Books, 2019. E-book.
ISBN 9788550808024. Disponível em:
<https://integrada.minhabiblioteca.com.br/#/books/9788550808024/>. Acesso em: 07 dez. 2023

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer electronic cash system, 2008.
Disponível em:<<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 06 dez 2023

PEIXOTO, Andrea Stefani. Lei de Proteção de Dados: entenda em 13 pontos!
Disponível em: <<https://www.politize.com.br/lei-de-protecao-de-dados/#:~:text=A%20LGPD%20complementa%20o%20escopo,da%20seguran%C3%A7a%20das%20informa%C3%A7%C3%B5es%20pessoais>>. Acesso em: 07.dez. 2023

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13709/2018 (LGPD). 2ª edição. São Paulo: Saraiva Educação, 2020. Acesso em: 07 dez. 2023.

PORTAL DA INDÚSTRIA. Empreendedorismo: o que é, significado, desafios e tipos.
Disponível em: <https://www.portaldaindustria.com.br/industria-de-a-z/empreendedorismo/>.
Acesso em: 06 dez. 2023

REVOREDO, Tatiana. Blockchain, proteção de dados e o controle dos dados comercialmente sensíveis. IT Forum. 21 de abril de 2020. Disponível em:
<https://itforum.com.br/colunas/blockchain-protecao-de-dados-e-o-controle-dos-dados-comercialmente-sensiveis/> Acesso em 08 dez. 2023

SEBRAE. Conheça os benefícios de construir um ecossistema na sua empresa.
30janeiro de 2023. Disponível em:
<https://sebrae.com.br/sites/PortalSebrae/ufs/pe/artigos/conheca-os-beneficios-de-construir-um-ecossistema-na-sua-empresa,202f290599406810VgnVCM1000001b00320aRCRD>.
Acesso em: 06.dez.2023

SILVA, Gabriel G. V. S.. **Criptoativos: Aspectos legais e regulatórios no cenário brasileiro**. Copyright, 2019. E-book.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016.

WARREN, S. D. BRANDEIS, L. D. S. The right to privacy. Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890). Disponível em: <<http://https://www.jstor.org/stable/1321160?seq=2>> Acesso em: 07 dez. 2023.