

**UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA
COORDENAÇÃO DE MONOGRAFIA**

ARNALDO JOSÉ DE LIMA JÚNIOR

**PROTEÇÃO DE DADOS DE SAÚDE E BLOCKCHAIN: PRONTUÁRIO MÉDICO
ELETRÔNICO E REGISTROS DESCENTRALIZADOS**

**JOÃO PESSOA
2023**

ARNALDO JOSÉ DE LIMA JÚNIOR

**PROTEÇÃO DE DADOS DE SAÚDE E BLOCKCHAIN: PRONTUÁRIO MÉDICO
ELETRÔNICO E REGISTROS DESCENTRALIZADOS**

Trabalho de Conclusão de Curso
apresentado ao Curso de Graduação em
Direito de João Pessoa do Centro de
Ciências Jurídicas da Universidade
Federal da Paraíba como requisito parcial
da obtenção do grau de Bacharel em
Direito.

Orientador: Prof. Dr.º Gustavo Rabay

**JOÃO PESSOA
2023**

Catálogo na publicação
Seção de Catalogação e Classificação

L732p Lima Junior, Arnaldo Jose de.

Proteção de dados de saúde e blockchain: prontuário
médico eletrônico e registros descentralizados /

Arnaldo Jose de Lima Junior. - João Pessoa, 2023.

66 f. : il.

Orientação: Gustavo Rabay Guerra.

TCC (Graduação) - UFPB/CCJ.

1. Blockchain. 2. Privacidade. 3. Proteção de dados.
4. Saúde. 5. Registros descentralizados. 6. Prontuário
médico. I. Guerra, Gustavo Rabay. II. Título.

UFPB/CCJ

CDU 34

ARNALDO JOSÉ DE LIMA JÚNIOR

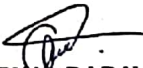
**PROTEÇÃO DE DADOS DE SAÚDE E BLOCKCHAIN: PRONTUÁRIO MÉDICO
ELETRÔNICO E REGISTROS DESCENTRALIZADOS**

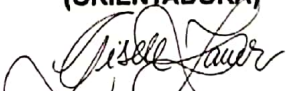
Trabalho de Conclusão de Curso
apresentado ao Curso de Graduação em
Direito de João Pessoa do Centro de
Ciências Jurídicas da Universidade
Federal da Paraíba como requisito parcial
da obtenção do grau de Bacharel em
Direito.

Orientador: Prof. Dr.º Gustavo Rabay

DATA DA APROVAÇÃO: 12/06/2023.

BANCA EXAMINADORA:


Prof. Dr. GUSTAVO RABAY GUERRA
(ORIENTADORA)


GISELE SHINOZAKI KAUER
(AVALIADORA)


VALÉRIA FERNANDES
(AVALIADORA)

A educaão   um ato pol tico.
(Paulo Freire).

AGRADECIMENTOS

Em primeiro lugar, sou profundamente grato a Deus, que me deu força, sabedoria e perseverança durante todo o período da graduação. Sua presença constante em minha vida tem sido uma fonte de inspiração e motivação para superar os desafios e alcançar meus objetivos. Gostaria de estender meus agradecimentos aos meus pais, que sempre me incentivaram a seguir o caminho do Direito e me apoiaram em cada passo da minha jornada acadêmica. Agradeço a minha amada esposa, Palloma Cordeiro, pela sua paciência, compreensão e apoio ao longo de todo o processo de graduação. Seu encorajamento constante e suporte emocional foram essenciais para me manter focado e motivado em momentos desafiadores. Não posso deixar de expressar minha gratidão aos meus estimados professores, que compartilharam seu conhecimento, experiência e paixão pelo Direito ao longo do curso. Em especial, gostaria de agradecer ao Professor Rabay, cujas orientações e ensinamentos foram fundamentais para o desenvolvimento do meu TCC. Sua dedicação e comprometimento com o ensino deixaram uma marca duradoura em minha formação acadêmica. Por fim, jamais esquecerei o gesto incrível da minha sogra, Cleonildes Cordeiro, que percorreu 400 km, da minha cidade natal até a capital, para trazer os documentos necessários para a minha matrícula no curso. Eu havia esquecido esses documentos por descuido, mas graças a ela, no último dia, com apenas trinta minutos restantes para o encerramento do expediente e finalizar a matrícula, eu consegui realizá-la. Sou imensamente grato, Cléo. Obrigado! Por fim, neste momento de conclusão do meu TCC, sou grato por todas as experiências, aprendizados e oportunidades que a graduação em Direito me proporcionou. Essa conquista não seria possível sem o apoio e contribuição de cada uma dessas pessoas especiais em minha vida. Mais uma vez, expresso minha profunda gratidão a Deus, meus pais, minha esposa, aos professores, em especial ao Professor Rabay, e a todos que me acompanharam nessa jornada. Muito obrigado!

RESUMO

A Tutela dos Dados Pessoais é um tema de extrema relevância no contexto atual, principalmente na área da saúde, visando garantir a privacidade e a segurança dos indivíduos. A proteção adequada dessas informações é fundamental para evitar consequências graves, como a exposição de informações sensíveis e o risco de utilização indevida ou abusiva dessas informações. Diante desses desafios, a tecnologia Blockchain surge como uma solução promissora para modernizar o sistema de saúde e garantir a proteção dos dados pessoais dos pacientes. O Blockchain desperta grande interesse em diversos setores e oferece uma série de benefícios quando aplicado na área da saúde. Sua essência reside na capacidade de armazenar e compartilhar informações de forma descentralizada e segura. Utilizando algoritmos criptográficos avançados e consenso distribuído, o Blockchain garante a integridade e a confiabilidade dos dados. Existem exemplos ao redor do mundo que demonstram a aplicação bem-sucedida do Blockchain no setor da saúde. Um desses exemplos é o projeto MedRec, desenvolvido pelo MIT (Instituto de Tecnologia de Massachusetts), que utiliza o Blockchain para permitir o compartilhamento seguro de informações médicas entre diferentes prestadores de cuidados de saúde. Essa solução tem como objetivo melhorar a coordenação e a continuidade dos cuidados, além de proporcionar maior controle aos pacientes sobre suas informações pessoais. Outro exemplo notável é o Estonia's e-Health, um sistema de saúde eletrônico baseado em Blockchain implementado na Estônia. Esse sistema permite que os cidadãos acessem e controlem seus próprios registros médicos, além de fornecer um registro imutável de todas as interações com o sistema de saúde. Essa abordagem aumenta a transparência e a confiança no tratamento dos dados, garantindo uma melhor proteção dos direitos dos pacientes. Esses exemplos concretos demonstram o potencial do Blockchain para modernizar o sistema de saúde e garantir a proteção dos dados pessoais. No entanto, é importante destacar que a implementação dessa tecnologia não é isenta de desafios. Questões relacionadas à interoperabilidade, padronização e escalabilidade ainda precisam ser abordadas para permitir uma adoção mais ampla e eficaz do Blockchain no setor da saúde. Em conclusão, a Tutela dos Dados Pessoais é uma preocupação crescente na sociedade contemporânea, e o uso da tecnologia

Blockchain oferece uma solução promissora para garantir a proteção adequada dessas informações, especialmente no contexto da saúde. A adoção dessa tecnologia pode trazer avanços significativos, mas requer um esforço contínuo para alcançar resultados positivos e garantir a proteção dos dados pessoais dos indivíduos.

Palavras-chave: Privacidade; Segurança; Blockchain; Modernização do sistema de saúde; Proteção dos dados pessoais; Tutela dos Dados Pessoais; LGPD.

ABSTRACT

The Protection of Personal Data is a topic of extreme relevance in the current context, mainly in the health area, aiming to guarantee the privacy and security of individuals. Adequate protection of this information is essential to avoid serious consequences, such as exposure of sensitive information and the risk of misuse or abuse of this information. Faced with these challenges, Blockchain technology emerges as a promising solution to modernize the health system and ensure the protection of patients' personal data. Blockchain arouses great interest in several sectors and offers a series of benefits when applied in the health area. Its essence lies in the ability to store and share information in a decentralized and secure way. Using advanced cryptographic algorithms and distributed consensus, Blockchain ensures data integrity and reliability. There are examples around the world that demonstrate the successful application of Blockchain in the healthcare sector. One such example is the MedRec project, developed by MIT (Massachusetts Institute of Technology), which uses Blockchain to allow the secure sharing of medical information between different healthcare providers. This solution aims to improve coordination and continuity of care, as well as provide patients with greater control over their personal information. Another notable example is Estonia's e-Health, a Blockchain-based electronic healthcare system implemented in Estonia. This system allows citizens to access and control their own medical records and provides an immutable record of all interactions with the health care system. This approach increases transparency and trust in data processing, ensuring better protection of patients' rights. These concrete examples demonstrate Blockchain's potential to modernize the healthcare system and ensure the protection of personal data. However, it is important to highlight that the implementation of this technology is not without challenges. Issues related to interoperability, standardization, and scalability still need to be addressed to allow for broader and more effective adoption of Blockchain in the healthcare sector. In conclusion, the Protection of Personal Data is a growing concern in contemporary society, and the use of Blockchain technology offers a promising solution to ensure adequate protection of this information, especially in the context of health. The adoption of this technology can bring

significant advances, but it requires a continuous effort to achieve positive results and ensure the protection of individuals' personal data.

Key-words: Privacy; Security; Blockchain; Modernization of the health system; Protection of personal data; Protection of Personal Data; LGPD.

LISTA DE ILUSTRAÇÕES

Figura 1 – Cadeia de Blockchain	24
Figura 2 – Estrutura de rede de um blockchain do bitcoin	25
Figura 3 – Sequência de Hash	26
Figura 4 – Camadas tecnológicas do Blockchain	28
Figura 5 – Esfera Concêntrica	43

SUMÁRIO

1 INTRODUÇÃO.....	12
2 FUNDAMENTOS DO BLOCKCHAIN.....	21
2.1 Conceito, Estrutura e Funcionamento do Blockchain.....	23
2.2 Desafios enfrentados pela tecnologia blockchain.....	30
3 PRIVACIDADE NA SAÚDE: LGPD E TUTELA DE DADOS PESSOAIS.....	33
3.1 Lei Geral De Proteção De Dados.....	34
3.2 Tutela dos Dados Pessoais.....	39
4 PRONTUÁRIO MÉDICO COM TECNOLOGIA BLOCKCHAIN: DESAFIOS E PERSPECTIVAS.....	46
4.1 Prontuário médico eletrônico: desafios e soluções para a garantia da privacidade e segurança dos dados.....	46
4.2 Tecnologia blockchain para modernizar o sistema de saúde.....	49
4.2.1 Exemplos ao redor do mundo.....	53
4.3 Eventuais gargalos do sistema proposto.....	56
5 CONSIDERAÇÕES FINAIS.....	60
REFERÊNCIAS.....	63

1 INTRODUÇÃO

Atualmente, estamos diante de algumas revoluções que estão emergindo e alterando o curso da humanidade, ficando evidente que estas transformações são profundas, alterando a forma como vivemos, trabalhamos e interagimos. Essas revoluções estão impulsionando mudanças em diversas áreas da sociedade, como economia, indústria, saúde, educação, comunicação e energia. Elas estão alterando a maneira como as pessoas se conectam globalmente, como as empresas operam, como as decisões são tomadas e como os problemas são abordados.

Uma delas é a revolução digital que tem levado à democratização da informação e à conectividade global, permitindo que pessoas ao redor do mundo acessem conhecimento e recursos de maneira sem precedentes. Outra é a revolução da IA que está transformando a maneira como interagimos com a tecnologia, com avanços em áreas como reconhecimento de voz, assistentes virtuais e veículos autônomos.

Já a revolução energética busca uma transição para fontes de energia mais limpas e sustentáveis, visando reduzir as emissões de carbono e mitigar as mudanças climáticas. Isso envolve a adoção de tecnologias como energia solar, eólica, armazenamento de energia e redes inteligentes.

Há ainda a revolução genômica que está proporcionando uma compreensão mais profunda do genoma humano e de outras espécies, o que tem implicações significativas para a medicina, a agricultura e a conservação ambiental. Podemos destacar ainda a revolução da indústria 4.0 que está transformando a forma como a produção industrial é realizada, com a automação, a robótica e a interconectividade das máquinas.

Contudo, diante de tantas revoluções, faz-se necessário destacar aqui um ponto de convergência entre todas elas. A utilização de dados. Atualmente, vivemos em uma era em que os dados se tornaram uma moeda valiosa e vital para as revoluções que estão ocorrendo.

Os dados são informações que representam diversos aspectos da vida: desde preferências pessoais, comportamentos de consumo e dados demográficos até informações médicas, genéticas e socioeconômicas. Esses dados sensíveis são a essência das revoluções que vivemos hoje. Eles alimentam a inteligência artificial,

possibilitam a personalização dos serviços e impulsionam a tomada de decisões informadas em todos os setores.

Na revolução digital, a coleta e análise de dados permitem uma compreensão profunda do comportamento do usuário, o que possibilita uma experiência personalizada. Empresas como Amazon, Google e Netflix utilizam dados para oferecer recomendações personalizadas, melhorando a satisfação do cliente e a eficiência operacional.

Na revolução da IA, os dados são a base do treinamento de algoritmos de aprendizado de máquina. Quanto mais dados relevantes e diversificados são disponibilizados, melhor é o desempenho dos modelos de IA. Os avanços na tradução automática, reconhecimento facial, diagnóstico médico e muitas outras áreas dependem da disponibilidade de grandes volumes de dados para treinar esses modelos.

Ainda como exemplo da importância dos dados, podemos destacar que na revolução da indústria 4.0, os dados são a base da automação e da tomada de decisões inteligentes. Sensores e dispositivos conectados coletam dados em tempo real, permitindo a análise preditiva, o monitoramento remoto e a otimização de processos industriais.

No entanto, embora as revoluções emergentes estejam trazendo avanços significativos que estão transformando o curso da humanidade, é importante reconhecer que a globalização, proveniente dessas transformações, também acarreta desafios e problemas consideráveis como o aumento da pobreza nos países em desenvolvimento, a maior concentração de renda e desigualdade social, o distanciamento entre países desenvolvidos e em desenvolvimento, a exploração de mão de obra e a crise ambiental do planeta. Além disso, há também preocupações em relação à privacidade e à segurança dos dados pessoais disponíveis, especialmente nos setores financeiro, crédito, securitário, saúde e varejo. Sendo fundamental considerar a importância da privacidade e segurança dos dados. À medida que os dados se tornam mais valiosos, é necessário garantir que haja um equilíbrio adequado entre a utilização dos dados e a proteção da privacidade das pessoas. É necessário estabelecer regulamentações e políticas robustas para proteger os dados sensíveis e garantir que sejam utilizados de maneira ética e responsável.

Desde o surgimento da internet, em meados dos anos 90, a coleta e o compartilhamento de informações pessoais se tornaram uma prática comum e indispensável em nossas vidas digitais. Porém, com o aumento do volume de dados armazenados online, também aumentaram os riscos de vazamentos de dados, colocando em risco a privacidade e a segurança de milhões de usuários em todo o mundo.

Os primeiros casos de vazamento de dados remontam ao início dos anos 2000, quando as empresas começaram a coletar e armazenar grandes quantidades de informações sobre seus clientes. Em 2005, o gigante do varejo americano, TJX, sofreu um dos maiores vazamentos de dados de cartões de crédito da história, comprometendo as informações pessoais de mais de 45 milhões de clientes (BBC Brasil, 2007). O incidente foi seguido por outros grandes vazamentos de dados em empresas como Heartland Payment Systems, Sony e Target.

Em 2013, o ex-consultor de inteligência Edward Snowden vazou uma série de documentos confidenciais da Agência de Segurança Nacional dos Estados Unidos, revelando programas de vigilância em massa e coleta de dados de cidadãos americanos e estrangeiros, (G1, 2013). O caso abriu um debate mundial sobre a privacidade online e levou à adoção de novas leis e regulamentos de proteção de dados em todo o mundo.

No mesmo ano, a empresa de segurança cibernética Hold Security descobriu um dos maiores vazamentos de senhas da história, com mais de 1,2 bilhão de senhas roubadas de sites e serviços populares como LinkedIn, Dropbox e Yahoo. O caso demonstrou a vulnerabilidade de empresas que não investem em segurança cibernética adequada e ressaltou a importância de políticas de senha robustas e medidas de segurança adicionais.

Em 2018, o Facebook foi envolvido em um escândalo de privacidade de dados que abalou o mundo todo. A empresa foi acusada de permitir que a empresa de consultoria política Cambridge Analytica coletasse dados de mais de 87 milhões de usuários sem o consentimento deles, para serem usados em campanhas políticas nos Estados Unidos e no Reino Unido, (NEWS BRASIL, 2018) O caso gerou uma série de questionamentos sobre a ética da coleta de dados em grande escala e levou a um aumento nas regulamentações de privacidade de dados em todo o mundo.

Em 2021, o Facebook novamente enfrentou um grande vazamento de dados, desta vez afetando mais de 533 milhões de usuários em todo o mundo. As informações pessoais, incluindo nomes completos, números de telefone, endereços de e-mail e datas de nascimento, foram publicadas em um fórum de hackers, colocando milhões de usuários em risco de roubo de identidade e outros crimes cibernéticos.

Os casos de vazamento de dados ao longo dos anos destacam a necessidade de tratar a privacidade e a segurança dos dados pessoais como questões críticas que devem ser abordadas com seriedade por empresas e governos em todo o mundo. A proteção de dados deve ser reconhecida como um direito fundamental dos indivíduos, em vez de ser considerada apenas uma preocupação comercial ou técnica.

Machado ressalta a importância da proteção de dados e da segurança da informação, enfatizando que as vulnerabilidades em sistemas de informação pessoais ou empresariais podem causar problemas graves para os negócios e para nossa vida pessoal. Ele destaca a necessidade de compreender os conceitos necessários para combater essas vulnerabilidades e nos proteger contra possíveis ataques às informações pessoais ou empresariais. Com a interconexão de centenas de sistemas vitais todos os dias, incluindo sistemas médicos, controle aéreo, sistemas de trânsito, monitoramento de vulcões e sistemas de compras e vendas online, a vida das pessoas se torna mais fácil, mas também mais perigosa (Machado, 2014).

O autor menciona as polêmicas denúncias de Edward Snowden em 2013, que estão diretamente relacionadas à segurança da informação e ao acesso não autorizado a informações e dados de pessoas, empresas e órgãos governamentais. Essas denúncias revelaram a burla de controles de segurança e o aproveitamento da ausência desses controles para obter informações privilegiadas para diversos fins (Machado, 2014).

Diante do aumento dos ataques cibernéticos e da exposição de dados, é evidente a importância de contar com profissionais qualificados em segurança da informação e implementar boas práticas para minimizar riscos e preservar os ativos das empresas. É crucial estabelecer processos e promover uma cultura de segurança nas organizações.

Na área da saúde, há relatos de inúmeros problemas relacionados à exposição de dados. Segundo a escritora Fabiana Cambrioli, em 2020, ocorreu uma falha de segurança no sistema de notificações de COVID-19 do Ministério da Saúde, resultando na exposição de dados pessoais de mais de 200 milhões de brasileiros na internet por pelo menos seis meses. Além dos pacientes diagnosticados com COVID-19, também foram expostas informações pessoais de qualquer brasileiro cadastrado no Sistema Único de Saúde (SUS) ou beneficiário de um plano de saúde (Cambrioli, 2020).

Outra matéria jornalística, mencionada por Ramon Souza, relata que durante a crise causada pelo coronavírus, uma clínica médica tradicional em Cascavel (PR) deixou vaziar mais de 2,3 mil laudos de pacientes, incluindo arquivos PDF com resultados de exames de endoscopia e colonoscopia. A investigação foi iniciada a partir de uma denúncia de um pesquisador de segurança, Giovanni Zadinello, que identificou que a instituição havia falhado em proteger um diretório em seu servidor web. O acesso ao diretório exposto não exigia conhecimentos técnicos e podia ser realizado por qualquer pessoa através de um botão na página "Fale Conosco" do site da clínica (Souza, 2020).

Esses incidentes de exposição de dados podem permitir que um invasor utilize as informações para diversas finalidades, como enviar e-mails para os pacientes usando o endereço de e-mail do administrador, que estava contido nos arquivos. Além da violação da privacidade dos dados pessoais, é importante ressaltar que o vazamento também viola o sigilo médico, o que é contrário ao Código de Ética Médica estabelecido pelo Conselho Federal de Medicina.

Para enfrentar esses desafios, é necessário que as regras sociais, jurídicas e culturais se adaptem às transformações da sociedade. O Direito deve apresentar respostas adequadas a essas inovações, levando em conta que diante de uma realidade globalizada, é necessária uma interpretação afinada com esses fatos apresentados. As fronteiras jurídicas devem ser menos rígidas, para que novos direitos possam surgir.

É importante destacar que a globalização é um processo contraditório e seletivo, que representa um novo momento do capitalismo moderno. Há uma enorme desigualdade social e uma crescente insegurança na sociedade. Para alcançar soluções inovadoras, é necessário que haja mudanças radicais nos

padrões de comportamento da sociedade. Essas mudanças devem ser adaptadas à realidade de cada país, dentro do contexto global.

Portanto, é fundamental que o Direito acompanhe essas mudanças e ofereça soluções para os novos desafios que surgem. Isso implica em uma revisão constante das leis e normas que regulam as relações sociais e comerciais. Além disso, é necessário que haja um debate amplo e democrático sobre as mudanças necessárias na sociedade. Afinal, o Direito deve estar a serviço da sociedade e garantir que os direitos de todos sejam respeitados, independentemente de sua condição social, econômica ou cultural.

O compartilhamento de dados pessoais, incluindo informações sensíveis, como dados genéticos, religião, orientação sexual e etnia, é uma preocupação crescente em relação à privacidade e segurança. A violação desses dados pode levar a danos à honra e dignidade das pessoas, bem como riscos à sua vida pessoal e profissional. A proteção desses dados é fundamental, respeitando os direitos fundamentais previstos na legislação, tais como o direito à intimidade, à vida privada e à proteção de dados pessoais. Quando ocorre um vazamento de dados, pode haver consequências jurídicas graves para todos os envolvidos, desde indivíduos até instituições e o Estado.

Ao meu entendimento, podemos destacar cinco pontos sobre como essa violação de dados pode influenciar e interferir nesses agentes. O primeiro ponto é o impacto nos cidadãos comuns, que têm direito ao controle de seus dados pessoais, e podem sofrer roubo de identidade e violação de privacidade. O segundo ponto é o impacto na sociedade, que pode perder a confiança nas empresas e organizações envolvidas, afetando negativamente a economia e a imagem do país, além de expor a riscos de segurança. O terceiro ponto é o impacto no Estado, que pode precisar intervir para proteger os cidadãos e investigar o ocorrido, levando a gastos públicos adicionais e impacto na imagem do país.

O quarto ponto é o impacto nas instituições responsáveis, que podem enfrentar consequências jurídicas e afetar sua imagem e reputação, levando à perda de confiança por parte do público e de seus stakeholders. Por fim, o quinto ponto é o impacto nos demais envolvidos, como outras empresas, parceiros e fornecedores, levando a prejuízos financeiros e perda de confiança entre os envolvidos.

Para garantir a segurança e privacidade dos dados pessoais, é essencial que empresas e organizações adotem medidas preventivas e de segurança para evitar o vazamento de dados. Caso ocorra, é fundamental tomar medidas para proteger os indivíduos afetados e investigar as causas do incidente. Além disso, é necessário cumprir rigorosamente a legislação de proteção de dados.

Neste trabalho, abordaremos o impacto negativo que o vazamento de dados pode ter na vida das pessoas e no Estado, e como a legislação, incluindo a Lei Geral de Proteção de Dados (LGPD), pode ajudar a reduzir esses riscos. Também exploraremos como a tecnologia blockchain pode ser utilizada para adicionar uma camada extra de segurança nesse contexto. Embora nunca possamos estar totalmente seguros, é importante conhecer mecanismos que podem ser aplicados para tornar o sistema mais resistente a invasões, vazamentos e possíveis ataques, incluindo a adoção de leis como a LGPD e a incorporação de novas tecnologias.

A tecnologia blockchain vem sendo cada vez mais explorada em diferentes setores da sociedade, e o campo da saúde não poderia ser diferente. Com a crescente preocupação com a privacidade e segurança dos dados pessoais, surge a necessidade de uma solução efetiva e confiável para armazenar informações sensíveis, como é o caso das informações do prontuário médico, que é uma fonte de dados importantes e delicados. A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020, veio para estabelecer as diretrizes sobre a coleta, armazenamento e compartilhamento desses dados, impondo regras mais rígidas e punições para quem descumprir a lei. Nesse contexto, a tecnologia blockchain surge como uma opção segura e confiável para a construção do prontuário médico unificado, com proteção da privacidade e segurança dos dados. Mas afinal, Como a tecnologia blockchain pode ser utilizada na construção de um prontuário médico unificado seguro e que garanta a proteção da privacidade e dos dados sensíveis, prevenindo vazamentos de dados e garantindo o controle do paciente sobre o acesso e compartilhamento dessas informações? É o que iremos descobrir ao longo do trabalho.

Desde o surgimento do Bitcoin em 2009, a tecnologia blockchain tem ganhado destaque e tem sido aplicada em diferentes áreas, como finanças, logística, eleições e agora, saúde. A tecnologia foi criada para permitir transações financeiras sem intermediários, ou seja, sem a necessidade de um órgão regulador

ou um banco, por exemplo. Seu funcionamento se baseia em uma rede descentralizada de nós, que registra todas as transações realizadas e garante a segurança e integridade dos dados, evitando a falsificação e a exclusão indevida de informações.

No entanto, apesar dos benefícios trazidos pela tecnologia, a sociedade ainda enfrenta problemas como o vazamento de dados sensíveis, o que coloca em risco a privacidade e a segurança das pessoas. Nesse sentido, a adoção de soluções que protejam a privacidade dos usuários é essencial para garantir o pleno exercício dos direitos fundamentais.

A gestão do prontuário médico é um exemplo em que essa proteção é fundamental. Atualmente, o prontuário médico é gerenciado de forma fragmentada, com informações dispersas em diferentes instituições de saúde, o que dificulta o acesso dos profissionais da área e a continuidade do tratamento. Além disso, a utilização de prontuários físicos em muitos hospitais também pode trazer problemas relacionados à integridade das informações.

Em relação à proteção dos dados pessoais, a Constituição Federal de 1988, em seu artigo 5º, inciso X, estabelece a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. Isso significa que o direito à privacidade é um direito fundamental que deve ser protegido pelo Estado e pela sociedade como um todo.

Nesse contexto, faz-se a necessidade de adoção de mecanismos, como o caso da tecnologia blockchain para a construção do prontuário médico unificado, como uma solução capaz de unificar as informações de diferentes instituições de saúde em um único local seguro e confiável, garantindo a privacidade e a segurança dos dados dos pacientes. A utilização da tecnologia blockchain, além de facilitar o acesso às informações dos pacientes pelos profissionais de saúde, também poderia proporcionar maior transparência e rastreabilidade de todas as atividades envolvidas no tratamento médico, desde a coleta dos dados até a sua utilização pelos profissionais da saúde.

Dessa forma, este trabalho, até o momento, buscou delimitar a problemática ao qual se propõe, que nada mais é do que: Como garantir a proteção eficaz dos dados sensíveis presentes nos prontuários médicos, considerando os potenciais impactos negativos dos vazamentos de dados na vida das pessoas e no sistema de saúde como um todo? Além disso, em conformidade com a Lei Geral de Proteção de

Dados (LGPD), é viável utilizar a tecnologia blockchain como uma solução efetiva para assegurar a segurança e a privacidade desses dados? Quais são os desafios, benefícios e limitações associados à implementação do blockchain nesse contexto específico da área da saúde?

Portanto, o objetivo geral deste trabalho é analisar o potencial da tecnologia blockchain na construção do prontuário médico unificado, em conformidade com a Lei Geral de Proteção de Dados, justificando sua adoção como uma solução para os problemas enfrentados pela sociedade em relação à gestão de dados sensíveis de saúde, vazamento de dados e segurança da informação. Com isso, busca-se garantir a proteção da privacidade e dos dados sensíveis por meio de medidas regulatórias e tecnologias que evitem a exposição de informações confidenciais, respeitando os direitos fundamentais previstos na legislação, como o direito à intimidade, à vida privada e à proteção de dados pessoais.

Para atingir esse objetivo, serão demonstradas as implicações causadas pelo vazamento de dados, além de evidenciar que a utilização de mecanismos presentes na Lei Geral de Proteção de Dados, juntamente com a adoção de tecnologias, como o blockchain, pode ser uma alternativa para a construção e aplicação do prontuário médico unificado, com o intuito de garantir privacidade, eficiência e proteção aos dados e informações sigilosas do paciente e do médico.

Além disso, serão apresentados objetivos específicos, como demonstrar que a tecnologia blockchain é a única responsável pela garantia da proteção dos dados sensíveis presentes nos prontuários, uma vez que ela oferece segurança, imutabilidade e transparência nas transações e registros. Será também evidenciado que a implementação de mecanismos da LGPD no ambiente hospitalar pode ser uma forma efetiva de garantir a privacidade dos pacientes e a proteção dos dados contidos nos prontuários médicos, pois a lei estabelece diretrizes claras sobre o tratamento de informações pessoais e sensíveis. Será apresentado ainda, cases de sucesso da implementação da tecnologia blockchain, no prontuário médico, ao longo do mundo.

2 FUNDAMENTOS DO BLOCKCHAIN

Embora os detalhes técnicos e operacionais da tecnologia blockchain estejam além do escopo deste trabalho, é fundamental destacar alguns conceitos, recursos e terminologias relacionados ao blockchain que irão auxiliar na melhor compreensão de como essa tecnologia é aplicada em diferentes contextos. Termos como estrutura, conceito, funcionamento e devidas aplicações, serão previamente abordados, de maneira sucinta, para que possamos elaborar, de maneira mais eficiente possível, um entendimento acerca dos possíveis benefícios no que se refere a tecnologia blockchain no prontuário médico de saúde.

O termo "blockchain" originalmente se referia a uma estrutura de dados usada na área de informática para compartilhamento de informações de forma segura e descentralizada. Com o surgimento do Bitcoin em 2009, o conceito de blockchain foi ampliado e popularizado como um registro público e imutável de transações financeiras que funciona por meio de consenso distribuído entre os participantes da rede. Desde então, o uso da tecnologia de blockchain tem se expandido para outras áreas, além das finanças, incluindo a saúde, logística, votação eletrônica, entre outras. Como resultado, muitos especialistas acreditam que a tecnologia blockchain representa uma nova era na computação e é considerada a "quinta evolução" da computação, após as eras do mainframe, da computação pessoal, da internet e da mobilidade. A capacidade de garantir a integridade dos dados e possibilitar transações diretas entre as partes, sem a necessidade de intermediários, são algumas das principais vantagens oferecidas pela tecnologia blockchain.

No contexto abordado, Laurence (2019) explica que as blockchains são uma forma inovadora de bases de dados distribuídas que incorporam tecnologias antigas de maneiras novas. Ela descreve as blockchains como bases de dados compartilhadas controladas por grupos de pessoas, que armazenam e compartilham informações. Essa tecnologia possui diversos tipos e aplicações, e está integrada em plataformas e hardwares ao redor do mundo.

A autora também destaca que um blockchain é uma estrutura de dados que possibilita a criação de um livro-razão de dados digitais, compartilhado por uma rede

de grupos independentes. Ela menciona a existência de diferentes tipos de blockchains: 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.

Em todas as categorias de blockchains, a criptografia é utilizada para permitir que os participantes da rede gerenciem o livro-razão de forma segura, sem a necessidade de uma autoridade central. A ausência de uma autoridade central é um dos aspectos mais importantes das blockchains. Embora os registros de transações sejam permanentes em um blockchain, eles podem ser alterados se uma grande parcela da comunidade concordar em fazer mudanças nas informações. No entanto, uma vez que os dados são registrados em um blockchain, é difícil alterá-los ou removê-los. Os usuários na rede verificam as transações propostas antes de adicioná-las ao blockchain, mas cada blockchain possui sua própria interpretação sobre como isso deve ser feito e quem pode validar as transações.

Ao lidar com o Blockchain, ainda é evidente a grande dificuldade de defini-lo, pois é possível encontrar várias interpretações que abrangem determinados aspectos específicos dessa tecnologia. Mougayar (2017) argumenta que isso ocorre devido à visão unidimensional ainda atribuída ao Blockchain. O autor destaca que a compreensão dessa tecnologia pode variar a depender de como será implementada. Swan (2015), demarca três categorias de evolução do Blockchain:

Blockchain 1.0: aplicações em criptomoedas, como Bitcoin.
Blockchain 2.0: usos relacionados a contratos de todo o tipo, que vão muito além de transações em dinheiro. Nessa utilização podem ser realizados contratos relacionados a ações, empréstimos, hipotecas, títulos e contratos inteligentes; **Blockchain 3.0:** categoria que compreende as aplicações que vão além dos usos mencionados anteriormente. Nesta, destacam-se as áreas governamentais, de saúde, ciência, literatura, cultura e artes.

Portanto, a classificação proposta por Swan em relação à evolução do blockchain em três categorias distintas, ajuda a compreender como a tecnologia blockchain evoluiu ao longo do tempo e como pode continuar a evoluir no futuro, abrindo novas possibilidades de aplicação e uso da tecnologia. Isso pode ser útil para entender o impacto potencial do blockchain em diferentes setores e áreas, bem como para identificar oportunidades de inovação e desenvolvimento em relação à tecnologia.

2.1 Conceito, Estrutura e Funcionamento do Blockchain

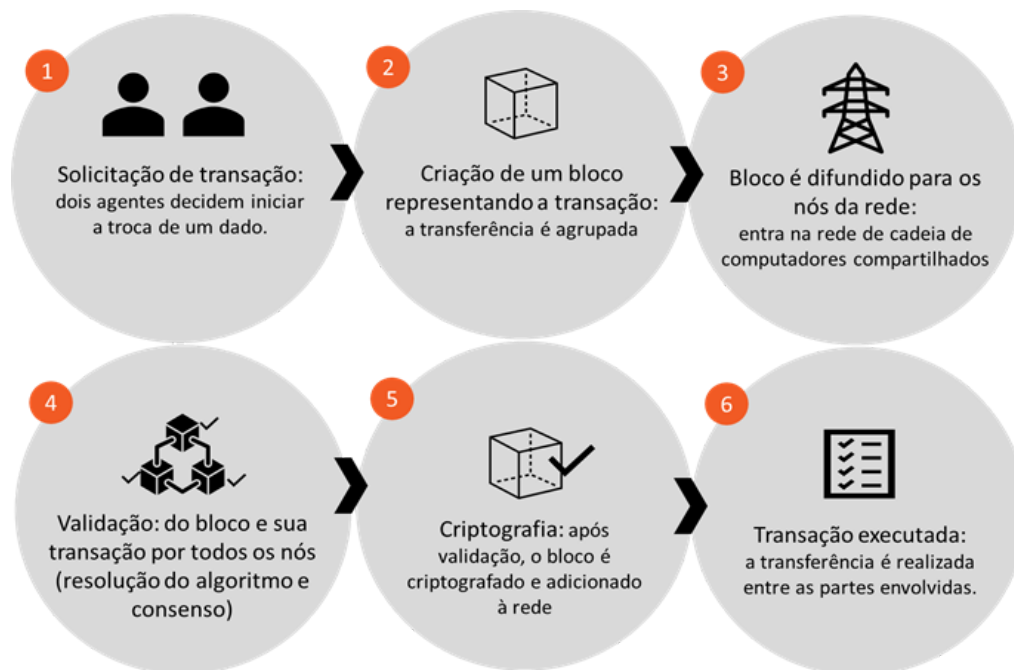
Mas afinal o que significa Blockchain? Como já foi mencionado, o termo "Blockchain" significa "cadeia de blocos" em tradução literal. Embora essa definição possa não ser muito clara à primeira vista, ela revela o princípio estrutural fundamental da tecnologia, que é baseado em blocos de registros interconectados que formam uma cadeia.

A tecnologia é baseada, portanto, em um registro distribuído e imutável que guarda informações em blocos encadeados. Cada bloco contém informações, como transações financeiras, e um ponteiro para o bloco anterior. Isso cria uma cadeia de blocos que é muito difícil de ser alterada ou corrompida. Além disso, a tecnologia blockchain é geralmente baseada em criptografia para garantir a segurança e a privacidade das informações. Isso permite que as pessoas confiem na veracidade das informações armazenadas na cadeia de blocos sem depender de um único ponto de falha ou de um intermediário confiável.

A visão apresentada anteriormente pode ser facilmente comprovada pelo seguinte entendimento do autor, para Swan (2015), o blockchain é uma tecnologia distribuída que permite a criação de registros permanentes e imutáveis de transações em uma rede descentralizada. Ele é composto por uma cadeia de blocos, onde cada bloco contém um conjunto de transações validadas por nós da rede por meio de algoritmos matemáticos. Conforme será demonstrado na figura a seguir. Essa validação é feita por consenso, o que garante a segurança e a transparência do registro. Além disso, o blockchain é descentralizado, o que significa

que não há um único ponto de controle e todos os participantes da rede têm acesso ao registro completo de transações. Vejamos a (figura 1):

FIGURA 1 - Cadeia Blockchain



Fonte: Elaborado pelo autor (2023)

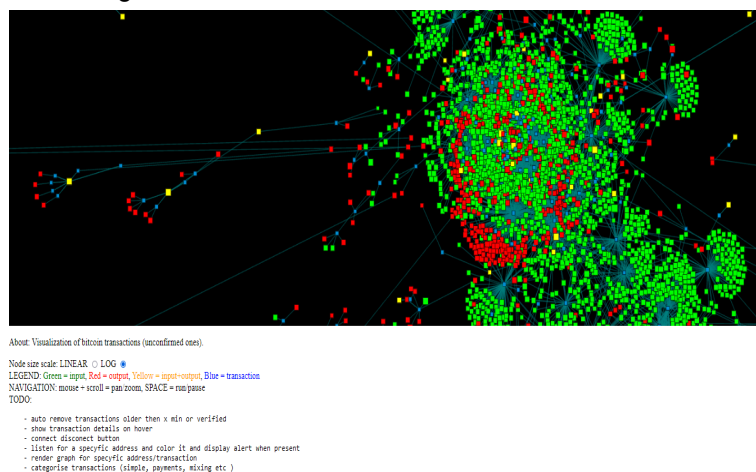
Logo, com base nesses conceitos e informações, podemos definir a tecnologia blockchain como um avançado mecanismo de banco de dados que permite o compartilhamento e transporte seguro de informações na rede. Embora seja uma tecnologia emergente, ela tem se mostrado cada vez mais promissora, com aplicações em diversas áreas e objetivos. A importância da tecnologia blockchain reside em sua capacidade de fornecer segurança, transparência e descentralização na armazenagem de informações e transações. Além disso, por ser uma tecnologia imutável e compartilhada por vários participantes, ela ajuda a eliminar a necessidade de intermediários confiáveis e pontos únicos de falha. Isso é especialmente relevante em indústrias financeiras, onde a confiança e a segurança são fundamentais.

A tecnologia blockchain tem sido amplamente aplicada em diversos setores devido às suas características de segurança e descentralização. No setor financeiro, a blockchain possibilita não apenas maior segurança, mas também a redução de custos e a eficiência em processos como pagamentos internacionais, transferências

de valores e operações de câmbio. Já na área da saúde, a tecnologia permite o armazenamento seguro de informações médicas, como registros de pacientes e históricos médicos, e o acesso confiável por diferentes profissionais de saúde autorizados, contribuindo para a melhoria da qualidade dos serviços prestados. Na logística, a blockchain é utilizada para rastrear a trajetória de um produto desde a origem até o destino final, o que garante maior transparência e rastreabilidade do processo, sendo útil para produtos perecíveis ou sensíveis. Além disso, na votação eletrônica, a blockchain tem o potencial de garantir a segurança e integridade do processo de votação, prevenindo fraudes e aumentando a confiança no sistema eleitoral.

Mas afinal, o que de fato um blockchain faz? Para a pesquisadora Laurence (2019) há um grande gerenciamento de fluxo de dados, que não é administrado por nenhuma autoridade central. Este gerenciamento é feito pelo sistema ponto a ponto, conhecido como, *peer-to-peer*. A figura central aqui é substituída por uma rede ampla e distribuída e descentralizada de usuários independentes. Portanto, é compreensível que esses computadores estejam distribuídos em diversos locais, formando uma grande rede, conhecida como full nodes (nós completos). Essa estrutura¹ pode ser visualizada na figura a seguir.

Figura 2 - Estrutura de rede de um blockchain do bitcoin.¹



Fonte: ("Blockchain visualisation", [s.d.]

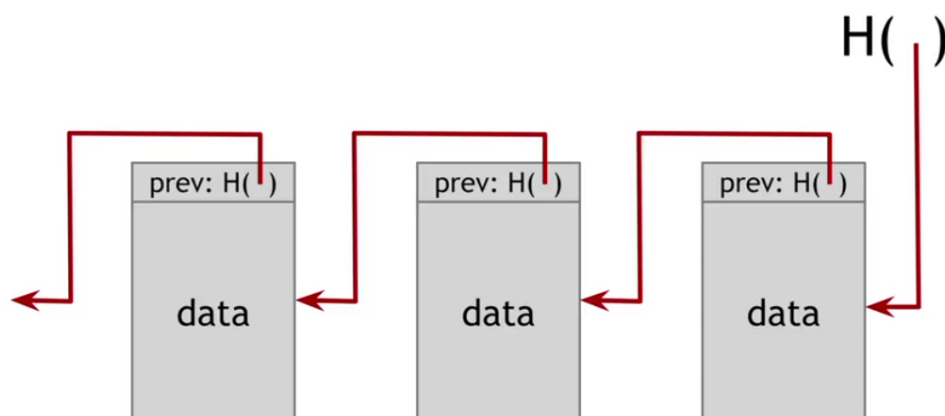
A junção de vários blocos, de modo encadeado, forma a denominada cadeia de blocos ou blockchain. Cada bloco contém um conjunto de transações, um

¹ Estrutura: para visualizar a rede de um blockchain do bitcoin, acesse:



carimbo de data/hora e um hash do bloco anterior. Essa estrutura torna a cadeia de blocos imutável, pois qualquer tentativa de alterar um bloco afetará o hash do bloco subsequente, o que será imediatamente detectado por todos os nós da rede. A organização dos blocos na cadeia é feita de forma que sempre o último bloco adicionado possua o hash do bloco anterior, formando assim uma sequência inquebrável de blocos.

Figura 3 - Sequência de hash



Fonte: Elaborado pelo autor (2023)

Conforme dito e posteriormente mostrado na figura acima, a organização dos blocos é feita de tal forma que cada novo bloco adicionado sempre contém o hash do bloco anterior, criando assim uma cadeia contínua e imutável de blocos interconectados. Essa estrutura é que irá garantir a segurança e a integridade dos dados armazenados na blockchain, pois qualquer tentativa de alterar um bloco afetará todos os blocos subsequentes, tornando a cadeia imediatamente inconsistente e invalidando a transação.

Indo mais adiante no assunto, a estrutura do Blockchain é composta por pilares fundamentais que garantem sua segurança e confiabilidade, conforme ressalta (Braga, 2017). O primeiro pilar é a **segurança**, que se baseia nos princípios de integridade, confidencialidade e disponibilidade, considerados os mais importantes para a segurança de computadores (Stalling, 2015). A **arquitetura descentralizada** é outro pilar, em que os registros não são armazenados em um único servidor, mas distribuídos entre diversas máquinas. A **integridade dos dados** é assegurada pelo encadeamento de cada bloco adicionado ao hash do bloco

anterior, tornando qualquer tentativa de modificação de um bloco impossível sem afetar a estrutura dos demais blocos. Por fim, a **imutabilidade** é garantida pela estrutura cronológica do Blockchain, que torna qualquer dado adicionado em seu bloco histórico temporal e impossível de ser apagado ou alterado.

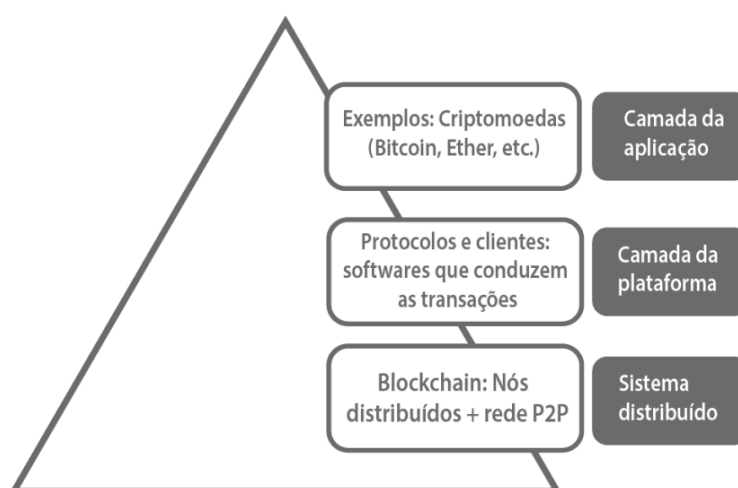
Segundo Mougayar, a tecnologia apresenta definições interessantes, que são baseadas em suas capacidades técnicas, corporativas e legais. Segundo o autor, o Blockchain é uma base de dados back-end que funciona por meio de registros distribuídos e possibilita a realização aberta de inspeções. Além disso, ele é uma rede de troca de fatos entre partes que dispensa a assistência de intermediários, o que o torna corporativamente eficiente. Por fim, o Blockchain funciona como um mecanismo de validação que não exige apoio de intermediários, tornando-se, assim, uma alternativa legalmente viável para diferentes tipos de transações. (MOUGAYAR, 2017).

Ainda segundo o autor, em relação aos conceitos, todos estão relacionados a aspectos presentes na tecnologia e, portanto, demonstram suas diversas possibilidades. É possível observar, por exemplo, na definição apresentada por Mougayar (2017), os benefícios do Blockchain, que se tornam mais claros quando se examinam as capacidades técnicas dessa tecnologia identificadas nos negócios que a utilizam.

As propriedades técnicas que demonstram esses benefícios são identificadas nas empresas que utilizam essa tecnologia, como apontado por Braga (2017), e incluem: Atualização periódica com autenticidade e legitimidade em tempo curto; Imutabilidade incremental por consenso das partes; Irrefutabilidade dos registros validados e distribuídos para todos os nós da rede; Prevenção contra duplicação de registros; Transparência com todos os registros acessíveis para todos os nós da rede e clientes com acesso somente para leitura; Visibilidade pública e legitimidade acessível a todos os nós da rede; Descentralização com todos os nós como coproprietários e contribuindo para atualização das cópias; Disponibilidade da rede mesmo quando alguns nós não estão disponíveis; Desintermediação emergente nas aplicações do Blockchain, eliminando intermediários e simplificando processos. Portanto, esses benefícios verificados, são traduzidos em mais eficiência, segurança e simplificação do processo, o que resulta em custos operacionais menores.

De acordo com Braga (2017), o Blockchain possui três camadas em sua aplicação: a **primeira** consiste no sistema distribuído, responsável por implementar a rede P2P e suas funcionalidades básicas, como protocolos de comunicação, armazenamento de rede e método de consenso. A **segunda** camada envolve serviços de apoio e infraestrutura, geralmente relacionados à plataforma e responsáveis pela segurança de dados, criptografia, gestão de identidade e disponibilidade de nós na rede. Por fim, a **terceira** camada é composta pela lógica de negócios e contratos inteligentes que asseguram a implementação das aplicações.

Figura 4: Camadas tecnológicas do Blockchain



Fonte: Adaptada de Braga (2017)

A tecnologia blockchain é considerada a quinta evolução da computação devido à sua capacidade de fornecer uma camada de confiança para a internet. Uma das principais razões para o potencial dessa tecnologia é sua capacidade de tornar impossível a remoção ou edição de informações em sua base de dados, gerando assim um fundo de dados digitais permanentes e confiáveis. Isso leva a uma série de possibilidades de negociação online, como direitos de propriedade e identidade, além de benefícios como agilidade, segurança, redução de custos, organização e produtividade. As primeiras aplicações foram criadas para explorar a transferência segura de valor digital. Aqui, temos uma divisão em três partes, que segundo Laurence (2019), são elas:

Block: Uma lista de transações registradas em um livro-razão durante um determinado período. O tamanho, o período e o evento gerador para blocos são diferentes para cada blockchain.

Nem todos os blockchains registram e asseguram um registro da movimentação de suas criptomoedas como objetivo principal. Mas todos os blockchains registram a movimentação de suas criptomoedas ou tokens. Pense na transação simplesmente como o registro de dados. Atribuir um valor a ela (como acontece em uma transação financeira) serve para interpretar o que os dados significam.

Chain: Uma hash que liga um block a outro, “encadeando-os” juntos, matematicamente. Este é um dos conceitos mais difíceis de compreender em blockchain. Ele também é a mágica que une blockchains e permite-lhe criar fiabilidade matemática.

A hash no blockchain é criada a partir dos dados que estavam no block anterior. A hash é a impressão digital desses dados, e trava blocks em ordem e prazo.

Rede: A rede é composta de “full nodes”. Pense neles como o computador executando um algoritmo que está protegendo a rede. Cada nó contém um registro completo de todas as transações que já foram registradas naquele blockchain.

Os nós estão localizados no mundo inteiro, e podem ser gerenciados por qualquer um. Gerenciar um full node é difícil, caro e consome tempo, então as pessoas não fazem isso de graça. Elas são incentivadas a gerenciar um nó porque querem ganhar criptomoedas. O algoritmo blockchain subjacente as recompensa por seus serviços, e a recompensa geralmente é um token ou uma criptomoeda, como o bitcoin.

Portanto, verifica-se que a tecnologia blockchain tem como objetivo eliminar intermediários responsáveis por validar transações, proporcionando maior segurança e redução de custos nas operações.

Existem três tipos básicos de blockchain: blockchain **público**, **privado** e o de **consórcio**. O blockchain público é aberto a todos e qualquer pessoa pode realizar transações nele, como o Bitcoin e Ethereum. Já o blockchain privado é controlado por uma única entidade ou grupo de entidades e é geralmente utilizado em aplicações empresariais para aumentar a privacidade e conformidade regulatória. O blockchain de consórcio é controlado por um grupo selecionado de participantes e é usado para aplicações que exigem cooperação entre várias entidades.

Existem também outros tipos de blockchain com características específicas, como o blockchain federado, que compartilha o controle entre várias entidades para aumentar a escalabilidade e segurança; o blockchain híbrido, que combina as vantagens do público e do privado para manter a privacidade e a escalabilidade; o

blockchain com contrato inteligente, que permite que as transações sejam executadas automaticamente com regras pré-definidas, reduzindo a necessidade de intermediários e aumentando a segurança; o blockchain sharding, que divide o blockchain em fragmentos para melhorar a velocidade e escalabilidade; e o blockchain de prova de capacidade, que utiliza a capacidade de armazenamento dos nós para provar o consenso e aumentar a escalabilidade. A escolha do tipo de blockchain adequado dependerá das necessidades específicas da aplicação. É importante avaliar as características de cada tipo antes de escolher o mais adequado para um projeto.

Para Laurence (2019), atualmente, existem projetos de blockchain mais amplos e de longo prazo em desenvolvimento, como sistemas de registro respaldados pelo governo, identidade e aplicações de segurança em viagens internacionais. As possibilidades de um futuro com o uso de blockchains têm entusiasmado pessoas em negócios, governos, grupos políticos e humanitários em todo o mundo. Países como Reino Unido, Singapura e os Emirados Árabes Unidos estão investindo ativamente e explorando o blockchain como um meio de cortar custos, criar novos instrumentos financeiros e manter registros limpos.

2.2 Desafios enfrentados pela tecnologia blockchain

Nos últimos anos, o Blockchain tem sido uma das tecnologias mais comentadas e gerado muita expectativa. No entanto, muitas empresas começaram a perceber que a tecnologia Blockchain pode não conseguir cumprir todas as expectativas criadas em torno dela. Vários fatores podem gerar essa frustração, incluindo a adoção limitada dessa tecnologia em diferentes mercados. Embora o Blockchain tenha sido bem-sucedido no campo das criptomoedas, sua implementação em outras áreas tem sido desafiadora. É importante destacar que a adoção do Blockchain requer um esforço conjunto de todos os agentes envolvidos, desde os desenvolvedores até os usuários finais, para garantir que a tecnologia seja implementada de maneira eficaz e atenda às necessidades específicas de cada setor.

Nessa esteira, podemos identificar tendências e desafios a serem enfrentados por essa tecnologia emergente. Segundo Moraes (2021), os desafios

enfrentados pelo blockchain incluem questões relacionadas à privacidade, escalabilidade, interoperabilidade e regulamentação, enquanto as tendências apontam para a evolução do blockchain em direção a soluções mais maduras e mais amplas de aplicação em diversos setores, incluindo saúde, logística, educação e governo.

Essa tecnologia gerou preocupações iniciais quanto à sua segurança e confiabilidade, mas atualmente, suas aplicações mais promissoras estão em setores como e-commerce, mercado financeiro, logística, governo digital, saúde, educação e agricultura. O crescimento do Blockchain será impulsionado pelo aumento da adoção de contratos inteligentes e iniciativas de startups. O Blockchain deve gerar empregos e fomentar a especialização de estudantes universitários em Tecnologia da Informação. Além disso, observa-se uma integração crescente entre o Blockchain e tecnologias de Inteligência Artificial, o que deve resultar em decisões mais rápidas e confiáveis de sistemas baseados em IA. Em resumo, apesar de alguns desafios, o Blockchain tem um grande potencial em várias áreas e deve continuar evoluindo e integrando-se com outras tecnologias para oferecer soluções cada vez mais inovadoras.

A tecnologia do Blockchain é muito mais ampla do que o seu uso em rede de Bitcoins, e existem inúmeros casos de uso em diferentes mercados, tais como compartilhamento de dados médicos, medição de royalties pagos pela execução de músicas, contratos inteligentes digitais, transferência internacional de recursos, detecção de lavagem de dinheiro, logística e cadeia de suprimentos. Uma das principais aplicações do Blockchain é nos chamados contratos inteligentes, eliminando a necessidade de um cartório ou instituição que registre o contrato, uma vez que ele ficaria armazenado no livro-razão do Blockchain, que é seguro o suficiente para cumprir com as regulamentações e o compliance necessários, conforme Moraes (2021).

Em resumo, podemos observar que a tecnologia blockchain, ainda emergente, apresenta um enorme potencial de aplicação devido à sua característica fundamental de inviolabilidade. Isso a torna especialmente relevante na proteção de dados sensíveis, trazendo para realidade do trabalho, tanto de médicos como de pacientes, garantindo a segurança e proteção dessas informações. Nos próximos

capítulos, abordaremos outras questões relacionadas à proteção de dados e à viabilidade da tecnologia blockchain no contexto de prontuários médicos.

3 PRIVACIDADE NA SAÚDE: LGPD E TUTELA DE DADOS PESSOAIS

Nos últimos anos, o avanço tecnológico e a crescente conectividade digital expuseram vulnerabilidades no que se refere à privacidade individual e à proteção de dados pessoais. Dessa forma, o dado, como informação, se tornou um dos bens mais valiosos da atualidade, exigindo regulamentação jurídica para termos como big data, inteligência artificial e proteção de dados pessoais, entre outros. Esse cenário aumentou a vulnerabilidade do direito à privacidade e à intimidade, fundamentais para a construção teórica desde o século XVIII. O direito à privacidade é um valor moral predominante nas culturas ocidentais, associado aos ideais democráticos, à autonomia e à liberdade, inerente ao ser humano.

A proteção de dados pessoais é fundamental para garantir a privacidade e a dignidade das pessoas, especialmente na área da saúde, onde informações sensíveis e pessoais são compartilhadas. Nesse sentido, Capurro(2012) entende que a proteção da privacidade está diretamente ligada à autonomia individual e que o conceito de "autonomia informacional" diz respeito ao poder de escolha que o indivíduo tem sobre o uso das suas informações em ambientes eletrônicos. Quando a autonomia é violada, a liberdade do indivíduo é ameaçada.

A autonomia, anteriormente citada, está diretamente ligada à utilização dos dados pessoais e sensíveis do indivíduo. Para LIMA, (2021), antes de mais nada, é necessário examinar, de modo que possamos distinguir e delimitar, os conceitos de dados pessoais e dados sensíveis, conforme disposto na Lei n. 13.709/2018. Segundo a autora:

De acordo com o art. 5º, inc. I, da LGPD, dado pessoal refere-se à "informação relacionada a pessoa natural identificada ou identificável". Já o art. 5º, inc. II, dispõe que os dados pessoais sensíveis correspondem aos "dados pessoais concernentes à origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Portanto, dado pessoal é qualquer informação que possa identificar uma pessoa natural, enquanto o dado pessoal sensível é um tipo específico de dado

peçoal que se refere a informações sobre origem racial ou étnica, convicção religiosa, opinião política ou filosófica, filiação a sindicato, dados referentes à saúde, vida sexual, dados genéticos ou biométricos que possam identificar uma pessoa natural.

A Lei Geral de Proteção de Dados (LGPD) é uma resposta a essa realidade, estabelecendo diretrizes claras para o tratamento de informações pessoais e sensíveis, incluindo aquelas relacionadas à saúde. A LGPD busca garantir o respeito à privacidade e à dignidade das pessoas, garantindo a segurança no uso de seus dados pessoais. Sendo assim, é essencial que haja uma conscientização sobre a importância da proteção de dados pessoais, principalmente na área da saúde, a fim de garantir a autonomia e liberdade do indivíduo.

3.1 Lei Geral De Proteção De Dados

A lei geral de proteção de dados, LGPD, criada em 2018, tem como principal objetivo proteger os dados pessoais de indivíduos, coletados por empresas sobre seus funcionários, clientes, parceiros, acionistas e outros. Inspirada na lei europeia de proteção de dados, conhecida como General Data Protection Regulation (GDPR), a LGPD é composta por 65 artigos e é a legislação mais recente e específica no Brasil. É importante ressaltar que a LGPD não é a única lei que regula a privacidade. Seus objetivos consistem na proteção dos direitos fundamentais de liberdade e privacidade, no livre desenvolvimento da personalidade da pessoa natural, na promoção da intimidade do cidadão, na garantia dos direitos de personalidade dos indivíduos e no fomento à inovação.

Durante a década de 1970, as primeiras normas específicas que relacionavam a proteção de dados pessoais ao direito à privacidade surgiram em todo o mundo. Esses instrumentos foram importantes marcos na proteção de dados pessoais e incluíram várias leis alemãs, como a Lei de Hessen de 1970, a Lei de Dados Sueca de 1973, o Estatuto Alemão de Proteção de Dados de Rheinland Pfalz de 1974, a Lei Federal de Proteção de Dados Alemã de 1977 e a Lei Francesa de Proteção de Dados Pessoais de 1978. Nos Estados Unidos, o Fair Credit Reporting Act (1970) e o Privacy Act (1974) também foram criados. Portugal se tornou o primeiro país a estabelecer o direito fundamental à autodeterminação informativa em

sua Constituição, no artigo 35, em 1976. A proteção dos dados pessoais foi consolidada com a Convenção nº108 do Conselho da Europa em 1981 e a Diretiva 95/46 da União Europeia em 1995. A Carta dos Direitos Fundamentais da União Europeia, em 2000, avançou ainda mais e estabeleceu que todos têm o direito à proteção de seus dados pessoais, os quais devem ser tratados com lealdade e para fins específicos, com o consentimento do titular dos dados, permitindo inclusive a sua correção quando necessário. Posteriormente, na União Europeia, veio a ser sancionado o Regulamento Geral de Proteção de Dados.

Embora a Lei Geral de Proteção de Dados (LGPD) traga inovações para o ordenamento jurídico brasileiro, a proteção de dados e informações não é uma novidade no país. Leis como a Lei de Acesso à Informação (Lei 12.527/2011), o Marco Civil da Internet (Lei 12.965/2014) e o Código de Defesa do Consumidor (Lei 8.078/1990) já preveem regras para garantir a privacidade e a segurança dos dados pessoais de indivíduos e consumidores. Portanto, a LGPD se soma a um conjunto de normas importantes para a proteção dos direitos fundamentais dos cidadãos. Para a Doutora Patrícia Peck Pinheiro (2018) a respeito da 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)

Considerando a proteção de dados pessoais como um direito fundamental, torna-se evidente a importância de uma legislação específica que garanta a salvaguarda dessas informações, tendo em vista que sua proteção impacta diretamente na identidade individual e na manutenção da privacidade. Direitos inerentes de qualquer ser vivo.

De início, é fundamental ressaltar que a lei se aplica a todas as operações de tratamento de dados, tanto por indivíduos quanto por empresas, independentemente do país em que estão estabelecidos. De acordo com o artigo 3º, a lei se aplica a todas as operações de tratamento de dados realizadas dentro do

território nacional, bem como aquelas cujo objetivo seja fornecer bens ou serviços a indivíduos brasileiros, independentemente de onde ocorra o tratamento dos dados. É importante destacar que a LGPD engloba todos os tratamentos de dados que utilizem informações coletadas de usuários brasileiros, independente da nacionalidade do prestador de serviço. Em outras palavras, se um prestador de serviço capturar dados de usuários no Brasil, estará sujeito à lei geral de proteção de dados, independentemente de sua origem.

Para melhor exemplificar, empresas de streaming, como a Prime Video, Star Plus e Netflix, têm um grande número de clientes em todo o país, apesar de serem empresas estrangeiras. Por essa razão, elas têm acesso a uma grande quantidade de dados dos brasileiros e, portanto, estão completamente sujeitas às disposições da LGPD.

Importante destacar que, os princípios que embasam a Lei Geral de Proteção de Dados têm como base o regulamento europeu, apresentando diversos pontos em comum. É, portanto, imprescindível que se realize uma análise minuciosa de cada princípio, a fim de compreendermos a relevância e eficácia dessa legislação no contexto nacional.

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)

Além dos princípios gerais de proteção de dados apresentados, a legislação brasileira estabelece outros princípios com conteúdo semelhante e complementar, como os princípios da 1. Adequação, 2. Necessidade, 3. Prevenção, 4. Não Discriminação. O Princípio da Adequação exige que o tratamento de dados seja compatível com as finalidades informadas ao titular dos dados, enquanto o Princípio da Necessidade estipula que o tratamento deve ser mínimo para atingir a finalidade buscada. O Princípio da Prevenção, por sua vez, está intimamente relacionado ao Princípio da Segurança Física e Lógica, pois envolve medidas de segurança para evitar a perda de dados. Por fim, o Princípio da Não Discriminação visa a impedir a discriminação decorrente do tratamento de dados.

Além disso, é importante destacar as situações em que o tratamento de dados é considerado legal, conforme descrito nos artigos 7º a 16º da LGPD, que levam em conta os requisitos, as hipóteses de tratamento, a proteção de dados pessoais de crianças e adolescentes e o término do tratamento de dados.

Ao longo do texto normativo da referida lei geral de proteção de dados, podemos encontrar os cabimentos legais para o devido tratamento dos dados pessoais, observa-se em:

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.

Obter o "consentimento" é uma das principais expressões relacionadas à conformidade legal no tratamento de dados. Tendo em vista a legislação em vigor, é obrigatório que os proprietários dos dados concedam autorização para o processamento dessas informações, conforme estabelecido no inciso I do artigo 7º. Ademais, o artigo 8º da mesma legislação reforça essa exigência, indicando que o consentimento deve ser formalizado por escrito ou por outros meios que evidenciem claramente a vontade do proprietário dos dados.

Sem sombra de dúvida, o consentimento é um dos pontos mais delicados abordados pela LGPD. A problemática do consentimento para o tratamento de dados pessoais não se restringe somente à legislação, mas vem sendo debatida há algum tempo. No entanto, é possível vislumbrar uma solução a partir do que essa lei nos apresenta. Embora existam outras formas de legitimar o tratamento de dados, o consentimento continua sendo uma perspectiva de extrema importância.

Em sua obra, Bruno Ricardo Bioni (2019) aborda analiticamente os limites do consentimento na LGPD. Ele defende que os dados pessoais representam um novo "ativo econômico" e um novo direito da personalidade, e que o consentimento não garante necessariamente a efetivação da autodeterminação informacional. Isso ocorre porque, diante da vulnerabilidade, o titular não tem condições de conhecer efetivamente todas as consequências do tratamento de dados e, portanto, não pode barganhar melhores condições (BIONI, 2019).

Apesar de outros escritores, como Patrícia Peck Pinheiro (2018, p. 65), afirmarem que o consentimento e o contrato podem resolver o problema da

liberdade e privacidade, Bruno Bioni acredita que a LGPD é um avanço significativo porque reconhece a vulnerabilidade do proprietário dos dados. Por exemplo, a norma consumerista é vista como subsidiária à Lei de Dados, permitindo novas formas de regulação e proteção dos dados pessoais. Destaco ainda que, esse trabalho corrobora com a crítica apresentada por Bioni, ao qual se verifica uma transformação do direito da personalidade em objeto de contratos.

Além disso, a criação da Autoridade Nacional de Proteção de Dados (“ANPD”, [s.d.]), juntamente com outras regras de regulamentação, torna o consentimento incluído na LGPD um avanço significativo, pois dá ao proprietário dos dados uma prerrogativa de empoderamento. Com a regulamentação informacional, isso garantirá a efetiva liberdade do proprietário.

3.2 Tutela dos Dados Pessoais

A proteção da privacidade é um conceito amplo que visa preservar a autonomia individual e as relações entre indivíduos e a sociedade, incluindo governos, empresas e outras entidades. A definição de privacidade pode variar de acordo com as experiências e entendimentos culturais de cada país e indivíduo. Os autores, Bastos e Martins conceituam a privacidade como:

[...] 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).

Podemos entender que a privacidade é um direito fundamental e uma expressão da dignidade humana, envolvendo não apenas o desejo de ocultar informações pessoais, que dizem respeito a sua própria intimidade, mas também o controle, acesso e processamento dessas informações.

Antes de ser conceituada juridicamente, a privacidade era vista como um elemento fundamental do ser humano pela filosofia, com raízes no pensamento cristão. Santo Agostinho mencionava a intimidade como um momento em que o indivíduo refletia sozinho sobre si mesmo e sua relação com Deus. Embora a

privacidade tenha evoluído ao longo de séculos, foi somente no século XX, especialmente após o surgimento da Internet, que ela se tornou conhecida da forma como a entendemos hoje.

O artigo chamado *The Right To Privacy*, dos escritores Samuel D. Warren e Louis D. Brandeis, pode ser considerado uma marco, na qual, se insere um divisor, no entendimento a respeito da privacidade. É nesse contexto ao qual é cunhado o termo e o conceito de “ser deixado só”. Samuel D. Warren e Louis D. Brandeis destacam que as mudanças sociais, políticas e econômicas, juntamente com o surgimento de novas tecnologias, como foi o caso da fotografia, tiveram um papel relevante na transformação da privacidade, o que mais tarde veio a resultar na sua violação.

Tal fato pode ser melhor entendido no caso, ainda nebuloso e conturbado, que foi a morte da princesa Diana. Ao qual, tudo indica que, apesar dos paparazzi não poderem ser responsabilizados completamente, mas sua conduta pode ter contribuído para a situação em questão, pois, segundos relatos, os mesmos estavam perseguindo Diana e seu carro na noite em que ocorreu o acidente fatal em Paris, em 31 de agosto de 1997. Algumas fontes afirmam que a perseguição dos fotógrafos pode ter contribuído para o acidente, já que o motorista do carro em que Diana estava tentava fugir da perseguição.

Para FRUET (1997) há uma dificuldade em estabelecer um limite entre o que é de interesse público e o direito à privacidade das pessoas, especialmente em relação à atuação da imprensa. Ele destaca que há uma tensão entre o direito e o dever da imprensa de informar e o direito de cada indivíduo à honra, privacidade e intimidade. O autor ressalta a necessidade de um equilíbrio entre a liberdade de imprensa, o direito à informação e o respeito aos direitos essenciais de cada indivíduo. Além disso, ele menciona a dificuldade de se estabelecer fórmulas legais precisas que possam balizar essa questão, uma vez que há uma tendência em reduzir as relações sociais a aspectos legais. Eis um trecho do artigo:

[...] o lamentável episódio da morte da princesa Diana recoloca a discussão sobre eventuais limites. A tradição inglesa é de total liberdade, não possuindo um pacto solene para garantia dos direitos públicos e qualquer sugestão de lei regulamentando a matéria, sempre foi tida como intromissão, ao contrário de países vizinhos como a França (*Loi de la presse*) e a Itália (*Legge sulla stampa*).

Uma das iniciativas inglesas foi a criação de um conselho, o press council. E todas estas tentativas decorrem, principalmente, de fatos envolvendo a família real, como a publicação das fotos da princesa Diana fazendo exercício numa academia particular de ginástica, divulgadas pelo jornal Sunday Mirror e depois pelo jornal Daily Mirror, do mesmo grupo. Outro episódio que também provocou a discussão sobre um código de conduta profissional ocorreu depois que a revista The People publicou uma foto do filho do príncipe Charles e Diana, Harry, então com sete anos, urinando num parque. Vários mecanismos já foram propostos, sem haver um definitivo ou abrangente. Mesmo assim, o direito consuetudinário não deixa de constituir um verdadeiro direito de imprensa, um press law, como verifica-se com a permanente interpretação da constituição americana através da Suprema Corte.

Neste sentido, destaque-se que a justiça inglesa apresenta resposta rápida nos processos de indenização, quer aplicando multas consideráveis em casos de crime contra a honra, quer rejeitando e aplicando multas contra aqueles que pretendem beneficiar-se de uma demanda desta natureza.

Não se trata, porém, de distorção exclusiva dos dias atuais. Conforme o historiador e professor da Universidade de Princeton Robert Darnton, a difamação já existia nas batalhas políticas das cortes italianas do século XVI. (FRUET, 1997)

Torna-se evidente a necessidade de uma regulação mais rigorosa da privacidade, para que haja uma coexistência harmoniosa entre a esfera privada e a esfera pública. Como mencionado pelo autor, é crucial estabelecer um limite claro entre o que é de interesse público e o direito à privacidade das pessoas, principalmente em relação à atuação da imprensa.

Ainda sobre o artigo, *The Right To Privacy*, os próprios autores examinam certa quantidade de decisões tomadas em tribunais ingleses e americanos, tendo em conta a existência de um princípio geral na common law, que é o direito à privacidade. No artigo, foi afirmado que fotógrafos e empresas jornalísticas violavam o espaço sagrado da vida privada, sendo que um dos prejudicados foi o próprio Samuel Warren, que estava descontente com a intromissão da imprensa em sua vida familiar. Como mostra o artigo:

1. O direito a privacidade não proíbe qualquer publicação da matéria que é de interesse público ou geral. [...] 2. O direito à privacidade não proíbe a divulgação de qualquer matéria, apesar de sua natureza privada, quando a publicação é feita mediante circunstâncias que tornem uma informação privilegiada de acordo com a lei de calúnia e difamação. [...] 4. O direito a privacidade cessa após a publicação dos fatos pelo indivíduo ou com seu consentimento. [...] Os remédios para uma invasão do direito a privacidade também são sugeridos por

aqueles administradores da lei de difamação e na lei da propriedade literária e artística, nomeadamente: 1. Uma ação de responsabilidade civil por dados em todos os casos. (WARREN E BRANDEIS, 1890, p. 13, Tradução própria)

Os autores consideram, em seu trabalho, que a invasão de privacidade é uma questão que afeta profundamente a noção de individualidade, dignidade, independência e honra de uma pessoa. Desde a publicação do artigo sobre o direito à privacidade, em 1890, essa temática tem sido objeto de discussão e análise em tribunais em todo o mundo, com a constatação de que a privacidade é um direito fundamental e inerente à dignidade humana.

Nos dias de hoje, a importância da privacidade de dados é ainda mais evidente diante do crescente uso da tecnologia em nossas vidas cotidianas. Com a coleta e o compartilhamento de informações pessoais por empresas e governos, a privacidade dos indivíduos corre o risco de ser violada. Por isso, é fundamental que haja leis e regulamentações que assegurem a privacidade dos dados pessoais e que as pessoas se conscientizem sobre seus direitos e a importância de manter suas informações pessoais seguras.

A privacidade é um direito fundamental na Constituição do Brasil e é considerada como uma cláusula pétrea e um dos direitos de personalidade. Tendo em vista ser um aspecto frágil, a privacidade pode ser facilmente violada. A nossa Constituição brasileira estabelece dois tipos de instâncias em relação à privacidade do indivíduo: a primeira, se refere a intimidade e a segunda, tem referência com a vida privada, o que leva a diferentes interpretações por parte da doutrina.

O artigo 5º, inciso X, da Constituição assegura de forma independente o conceito de vida privada e diferencia-o da intimidade. É suposto que a expressão "vida privada" seja usada em sentido restrito como uma das esferas da intimidade. A prática jurídica francesa, que é uma influência significativa na doutrina civilista ocidental, é uma das fontes para distinguir constitucionalmente a intimidade da vida privada, considerando o direito de intimidade como um aspecto mais limitado do direito à vida privada.

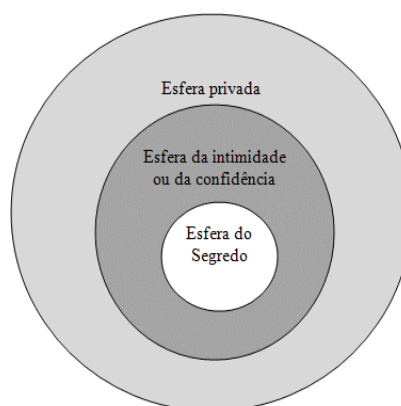
Levando em consideração que em 1957, durante o Fórum Jurídico Alemão, Heirinch Henkel, apresentou a Teoria dos Círculos Concêntricos ou das Esferas.

Essa teoria se fundamenta na medida em que as pessoas estão suscetíveis a interferências externas, estabelecendo diferentes níveis.

A esfera privada (o círculo da vida privada em sentido amplo) encerra três círculos concêntricos (camadas dentro de camadas): o círculo da vida privada em sentido restrito (a camada superficial), que contempla o círculo da intimidade (a camada intermediária), no qual se acomoda o mais denso desses três compartimentos, o círculo do segredo (núcleo) (FROTA, 2007).

A privacidade é composta por três esferas concêntricas, que correspondem a diferentes graus de exposição da pessoa. Na primeira esfera, chamada de anonimato ou esfera privada, encontram-se as condutas ocultas e protegidas por questões de privacidade. Embora alguns dados possam ter interesse público, a maioria dos indivíduos deseja mantê-los em segredo, como sua imagem e hábitos pessoais. No segundo estágio, a intimidade, estão as informações mais restritas, compartilhadas com um círculo reduzido de pessoas de confiança, como familiares e amigos íntimos. Já a esfera final, segredo, é o ponto mais interno e oculto da privacidade, abrigando informações pessoais que o indivíduo não deseja compartilhar, exceto em circunstâncias muito restritas, como suas escolhas sexuais, religiosas e filosóficas. Costa Jr. (2007) defende que essas esferas concêntricas são fundamentais para a proteção dos direitos individuais e privacidade. Essa teoria pode ser melhor visualizada conforme imagem a seguir:

Figura 5 - Esfera concêntrica



Fonte: Elaborado pelo autor (2023)

Agora que abordamos o entendimento da privacidade, bem como, apresentamos a Teoria dos Círculos Concêntricos ou das Esferas, entendemos que a preocupação com os dados pessoais está intimamente ligada à privacidade, aqui já abordada. Além do mais, é possível considerar que os dados pessoais, na teoria dos círculos, estão localizados entre a esfera do espaço privado e a esfera do espaço íntimo. Isso porque os dados pessoais são informações sensíveis e íntimas, que geralmente não devem ser compartilhadas com terceiros sem o consentimento expresso do titular dos dados.

Assim, os dados pessoais estão em uma posição privilegiada dentro do modelo dos círculos concêntricos, estando localizados no centro ou próximos dele, juntamente com outras informações pessoais e íntimas. Isso ressalta a importância de garantir a proteção e a privacidade dos dados pessoais, especialmente em um mundo cada vez mais conectado e com maior circulação de informações.

A proteção dos dados pessoais dos pacientes é uma questão fundamental que deve ser levada a sério pelos profissionais de saúde e pelas instituições que mantêm os prontuários médicos. A exposição dessas informações pode ter consequências graves e afetar a vida das pessoas de várias maneiras.

No contexto da saúde, a proteção dos dados pessoais é ainda mais crítica. O prontuário médico contém informações sensíveis e pessoais dos pacientes, como histórico médico, tratamentos realizados, medicamentos prescritos e outros detalhes. O vazamento dessas informações pode comprometer a privacidade do paciente, afetando sua dignidade e intimidade.

Além disso, o acesso indevido às informações de saúde pode prejudicar o tratamento médico e afetar a segurança do paciente. Por exemplo, um paciente que tem suas informações de saúde expostas pode sofrer discriminação, ter seu emprego afetado ou sofrer consequências graves em relação à sua saúde mental.

Portanto, é fundamental que os profissionais de saúde e as instituições que mantêm os prontuários médicos sigam as regras da LGPD e adotem medidas de segurança adequadas para proteger os dados pessoais dos pacientes. Isso inclui a proteção física dos prontuários, o controle de acesso às informações, o uso de senhas e criptografia, entre outras medidas, como por exemplo a utilização da tecnologia blockchain, ao qual estamos discutindo e expondo aqui.

Em resumo, a proteção dos dados pessoais dos pacientes é uma questão crítica que deve ser tratada com seriedade e responsabilidade. O vazamento de informações pessoais pode ter consequências graves e afetar a vida das pessoas de várias maneiras. É importante que as instituições de saúde adotem medidas adequadas de proteção e estejam em conformidade com a LGPD para garantir a privacidade e a segurança dos dados pessoais dos pacientes.

4 PRONTUÁRIO MÉDICO COM TECNOLOGIA BLOCKCHAIN: DESAFIOS E PERSPECTIVAS

Segundo dados do Ministério da Saúde do Brasil de 2021, cerca de 70% dos hospitais do país são públicos, ou seja, pertencem ao Sistema Único de Saúde (SUS) e são mantidos pelo governo. Esses hospitais atendem a grande maioria da população brasileira que depende do sistema público de saúde. Os outros 30% são hospitais privados ou filantrópicos, que atendem principalmente pacientes que possuem planos de saúde ou recursos para pagar pelos serviços de saúde, (MINISTÉRIO DA SAÚDE, [s.d.]). É importante ressaltar que a distribuição desses hospitais não é uniforme pelo país e há regiões com carência de unidades de saúde pública. Podemos destacar ainda que, a existência de um sistema descentralizado de saúde, como é o caso do SUS, apresenta muitos desafios em relação à sua gestão, organização e controle financeiro, especialmente considerando a enorme diversidade populacional e econômica do país.

Esses desafios se refletem na realidade do trabalho ao qual se propõe, como, por exemplo, na dificuldade de organizar e gerenciar os prontuários em meio a uma grande variedade de hospitais, regiões do país e realidades diferentes. Portanto, é necessário que haja investimento em recursos humanos, tecnologia e infraestrutura para garantir que o sistema de saúde brasileiro possa atender às necessidades da população de forma eficiente e equitativa.

4.1 Prontuário médico eletrônico: desafios e soluções para a garantia da privacidade e segurança dos dados

No contexto da área de saúde, a coleta de informações é essencial para garantir um atendimento adequado aos pacientes, sendo essas informações registradas em um documento conhecido como “Prontuário do Paciente” ou “Prontuário Médico”. É importante ressaltar que todas as informações contidas neste documento são de propriedade exclusiva do paciente e, por isso, a equipe de saúde, composta por diversos profissionais além do médico, é responsável por manter esses registros precisos e atualizados. O processo de coleta e armazenamento de informações dos pacientes pode variar de acordo com a instituição de saúde. Em

alguns casos, a abordagem é manual, com o uso de fichas físicas, enquanto em outros, é eletrônica, utilizando computadores ou bancos de dados.

Segundo o Conselho Federal de Medicina (CFM), através da Resolução nº 1.638/2002, o Prontuário Médico é definido como "um documento único, constituído de um conjunto de informações, de sinais e de imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros de uma equipe multiprofissional e a continuidade da assistência prestada ao indivíduo." (BRASIL, 2002). Essa definição enfatiza que o prontuário tem o propósito de reunir e registrar dados relevantes sobre a saúde do paciente, bem como o cuidado oferecido, visando à comunicação efetiva entre os profissionais de saúde envolvidos e à manutenção da continuidade do atendimento.

Essa mesma resolução ainda determina as principais informações que devem constar no prontuário médico, sendo elas, de acordo com art. 5º:

Art. 5º Compete à Comissão de Revisão de Prontuários:

I - Observar os itens que deverão constar obrigatoriamente do prontuário confeccionado em qualquer suporte, eletrônico ou papel:

a) Identificação do paciente - nome completo, data de nascimento (dia, mês e ano com quatro dígitos), sexo, nome da mãe, naturalidade (indicando o município e o estado de nascimento), endereço completo (nome da via pública, número, complemento, bairro/distrito, município, estado e CEP);

b) Anamnese, exame físico, exames complementares solicitados e seus respectivos resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento efetuado;

c) Evolução diária do paciente, com data e hora, discriminação de todos os procedimentos aos quais o mesmo foi submetido e identificação dos profissionais que os realizaram, assinados eletronicamente quando elaborados e/ou armazenados em meio eletrônico;

d) Nos prontuários em suporte de papel é obrigatória a legibilidade da letra do profissional que atendeu o paciente, bem como a identificação dos profissionais prestadores do atendimento. São também obrigatórias a assinatura e o respectivo número do CRM;

e) Nos casos emergenciais, nos quais seja impossível a colheita de história clínica do paciente, deverá constar relato médico completo de todos os procedimentos realizados e que tenham possibilitado o diagnóstico e/ou a remoção para outra unidade. (BRASIL, 2002).

Para Araújo e Mota (2020), o prontuário médico é uma das principais fontes de informação sobre o histórico de saúde do paciente, e o acesso às informações contidas nele deve ser realizado com autorização do paciente ou de seu representante legal, por meio de consentimento. Dessa forma, é fundamental que se solicite a autorização do paciente antes de acessar qualquer informação contida em seu prontuário médico.

Assim, esse documento contém informações sigilosas e confidenciais, as quais surgem da relação de confiança entre o médico e o paciente. Essas informações devem ser armazenadas, da melhor forma possível, à disposição do médico e protegidas contra vazamentos ou adulterações, uma vez que a exposição desses dados pode causar danos significativos à imagem do paciente. É importante ressaltar que o prontuário contém diversas informações sobre a vida privada e a intimidade do paciente, as quais são registradas por toda a equipe de saúde envolvida em sua assistência direta. Dessa forma, o acesso e a utilização dessas informações por terceiros só podem ocorrer mediante autorização expressa do paciente.

Segundo Siqueira e Hoch (2019), as informações presentes no prontuário do paciente não devem ser acessadas ou utilizadas indevidamente por terceiros não autorizados, já que esses dados são confidenciais e sigilosos. O uso indevido pode incluir, por exemplo, compartilhar informações sem consentimento, acessar informações além do necessário para a prestação de cuidados médicos, ou utilizar informações para fins comerciais ou de marketing sem autorização do paciente. Quando essas informações são utilizadas indevidamente, o direito à privacidade do paciente é desrespeitado e banalizado.

Como garantir a integridade das informações médicas e pessoais dos pacientes, armazenando, tratando e utilizando de maneira adequada e em conformidade com a Lei Geral de Proteção de Dados (LGPD)? Atualmente, existem diversas medidas e soluções que podem ser adotadas para garantir a integridade dos dados sensíveis dos indivíduos, considerando a LGPD.

Entre as medidas estão: 1 - o consentimento informado dos pacientes para coletar, armazenar e utilizar seus dados pessoais e sensíveis; 2 - segurança adequada para proteger as informações pessoais e sensíveis, incluindo a criptografia, senhas seguras, restrição de acesso aos dados e backups regulares; 3 -

coleta de informações apenas necessárias para realizar as atividades, minimizando danos em caso de vazamentos; 4 - transparência sobre práticas de coleta, armazenamento e utilização de dados pessoais e sensíveis; 5 - direito ao esquecimento; 6 - treinamento de funcionários; 7 - auditoria e monitoramento constante.

Contudo, apesar de todas essas maneiras, ainda é notório os inúmeros casos que noticiamos de ataques hackers, vazamento de dados, entre outros, já destacados aqui nesse trabalho. Portanto, essa dissertação, busca abordar o uso da tecnologia blockchain na problemática da segurança e privacidade dos dados sensíveis, tão presentes na área da saúde. Logo, além dessas medidas mencionadas anteriormente, uma nova tecnologia está sendo cada vez mais utilizada em prontuários eletrônicos é a blockchain. Ela permite o armazenamento de informações de forma segura e descentralizada, dificultando a ação de hackers e garantindo a privacidade, segurança, transparência e imutabilidade dos registros. Hospitais ao redor do mundo já começam a adotar essa tecnologia em seus sistemas de prontuários eletrônicos.

É importante salientar a relevância da adoção de medidas de segurança adequadas para garantir a proteção dos dados sensíveis dos pacientes e aprimorar a qualidade do atendimento médico e da saúde em geral. Nesse sentido, a utilização de tecnologias avançadas como a blockchain pode ser uma solução promissora.

4.2 Tecnologia blockchain para modernizar o sistema de saúde

Deve-se ter em mente que, o direito à privacidade, sigilo, autonomia e dignidade são garantidos pela Constituição no artigo 5º, inciso X. Esse artigo estabelece a inviolabilidade da intimidade, vida privada, honra e imagem, assegurando o direito à indenização por danos materiais e morais em caso de violação desses direitos. “[...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988).

Além disso, a legislação brasileira conta com a moderna Lei Geral de Proteção de Dados, que, como já destacado nos capítulos anteriores, estabelece a proteção dos dados pessoais como um dos seus principais fundamentos, tendo em

vista o respeito à privacidade, conforme previsto no artigo 2º, inciso I. Proteger esses dados significa garantir a sua segurança e evitar que sejam utilizados de forma indevida, ao passo que o respeito à privacidade é um elemento crucial para estabelecer uma relação de confiança entre as partes envolvidas.

Dentro desse contexto, o prontuário médico é um documento que contém informações sigilosas e confidenciais, tendo um papel relevante na defesa legal e ética dos profissionais que prestam assistência ao paciente. Além do que, se mostra um documento fundamental e abrangente que contém informações relevantes sobre o paciente, desde o diagnóstico inicial até sua evolução clínica. A fim de garantir a segurança e a proteção dessas informações, diversas normas e regulamentações foram estabelecidas.

A Resolução CFM 1.638/2002 define o prontuário médico e exige a criação da Comissão de Revisão de Prontuário nas instituições de saúde (BRASIL, 2002). Além disso, a Resolução CFM 1.821/2007 aprova as normas técnicas para digitalização e utilização de sistemas de armazenamento e manuseio de documentos do prontuário dos pacientes (BRASIL, 2007). Essas medidas têm como objetivo garantir a integridade e a confidencialidade dos dados, bem como proteger a privacidade dos pacientes.

A Lei 13.783/2018 (BRASIL, 2018), além de regulamentar a digitalização e o uso de sistemas informatizados para armazenamento, guarda e manuseio do prontuário médico, tem como objetivo assegurar a segurança e integridade das informações registradas nesse documento. Com a informatização dos dados, o acesso ao prontuário médico tornou-se mais ágil e eficiente, permitindo que a equipe multidisciplinar que presta assistência ao paciente tenha acesso a informações mais precisas e atualizadas.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) reforça a importância da proteção das informações contidas no prontuário médico, que são consideradas dados sensíveis e podem expor a privacidade dos pacientes em caso de vazamento ou uso indevido, como já mencionado. Além disso, a LGPD visa garantir a proteção dos direitos fundamentais. Embora não traga especificidades sobre o prontuário médico, sua aplicação é determinada pela Lei 13.787/2018 (BRASIL, 2018).

Se verifica, portanto, que as legislações, aqui mencionadas, acabam se completando. Conforme, Lóssio (2020):

O prontuário digitalizado deverá estar em conformidade com a Lei de Proteção de Dados Pessoais, com a Lei 13.787, visto que, contudo, são complementares pois qualquer desses diplomas legais tutelam de forma geral a relação dos princípios da segurança informação diante das liberdades, direitos e garantias fundamentais individuais de seus titulares. (LÓSSIO, 2020, p. 6).

Nesse sentido, a proteção dos dados pessoais sensíveis contidos no prontuário médico se torna fundamental para garantir a privacidade e os direitos do paciente. A legislação, por meio da LGPD, reconhece a sensibilidade dessas informações e sua utilização inadequada que podem gerar consequências prejudiciais, incluindo discriminação bem como a exploração comercial.

Os locais de atendimento médico e hospitalares precisam urgentemente aprimorar seus processos de segurança da informação para garantir a proteção efetiva dos dados sensíveis dos pacientes. Isso inclui consultórios, hospitais e clínicas que utilizam sistemas eletrônicos ou fichas em papel. Como trabalham com informações delicadas, é essencial que exista uma segurança robusta na proteção desses dados. Dessa forma, é imprescindível que esses estabelecimentos se adequem à LGPD para assegurar a integridade e privacidade dos pacientes.

Apesar da adoção de vários mecanismos presentes na LGPD e dos cuidados no armazenamento e segurança de dados sensíveis, ainda há relatos frequentes de vazamentos de informações e ataques hackers, dentre outras atividades ilícitas. No período da pandemia, houve, diversos incidentes como podemos verificar:

[...] nova falha do Ministério da Saúde expôs dados de cerca de 243 milhões de brasileiros na internet [...] O número de registros expostos é maior que o da atual população brasileira porque há também informações de pessoas que já morreram. Desde junho, os sistemas da pasta mostram fragilidade de proteção a dados. CPF, nome completo, endereço e telefone estão entre os dados vazados. Esse conteúdo veio de qualquer brasileiro cadastrado no Sistema Único de Saúde (SUS) ou em plano de saúde, disse o jornal. (G1, 2020).

Como podemos solucionar o problema de segurança na armazenagem de informações médicas? A tecnologia blockchain oferece uma solução eficiente, pois as informações são armazenadas de forma descentralizada, dificultando a ação de hackers e garantindo maior integridade, segurança, privacidade, transparência e imutabilidade dos registros dos pacientes. A blockchain funciona através de um sistema de blocos, no qual cada novo registro é verificado por outros participantes da rede antes de ser adicionado ao bloco, garantindo a autenticidade das informações. Essa verificação é feita por meio de criptografia, o que torna quase impossível a alteração de um registro já inserido na blockchain.

Dessa forma, tal tecnologia pode ser uma solução para garantir a segurança e privacidade dos dados dos pacientes no sistema de Prontuário Eletrônico do Paciente. Além disso, também pode permitir que os pacientes controlem o acesso às suas informações médicas, concedendo autorizações específicas para cada perfil de usuário identificado no sistema: paciente, profissional da saúde, instituição de saúde, laboratório médico e pesquisador.

O sistema de Prontuário Eletrônico do Paciente baseado em blockchain, tem como objetivo fornecer maior segurança e privacidade para as informações médicas dos pacientes. No caso do prontuário, tal ferramenta funcionaria como uma espécie de livro de registro das informações médicas do paciente, que é compartilhado entre alguns agentes, devidamente identificados, podendo ser: Paciente, Profissional da Saúde, Instituição de Saúde, Laboratório Médico e Pesquisador. Cada usuário tem acesso a um conjunto específico de informações, de acordo com sua necessidade.

No caso do paciente, por exemplo, pode cadastrar anonimamente seus dados pessoais em um banco de dados de pesquisa e autorizar o acesso de profissionais da saúde a informações específicas. Já o profissional da saúde tem acesso às informações do paciente relacionadas ao seu tratamento, enquanto a instituição de saúde pode acessar informações administrativas e financeiras. O laboratório médico pode acessar informações relacionadas a exames e testes realizados, e o pesquisador pode ter acesso a informações específicas para fins de pesquisa.

Entre os pontos positivos da tecnologia blockchain, destacam-se a segurança, privacidade, transparência e imutabilidade dos registros. A tecnologia blockchain permite que as informações sejam armazenadas de forma

descentralizada, o que dificulta a ação de hackers e garante maior segurança aos dados do paciente. Além disso, o paciente tem maior controle sobre suas informações médicas e pode autorizar ou não o acesso de terceiros às mesmas. Por outro lado, existem alguns pontos negativos relacionados à tecnologia blockchain que precisam ser considerados. Um deles é a complexidade do sistema, que pode dificultar a adoção em larga escala. Além disso, o tempo de processamento e mineração das transações pode ser mais lento em comparação a outros sistemas.

Por fim, é importante ressaltar a importância de garantir a segurança e privacidade das informações na área da saúde, que são extremamente sensíveis. O uso da tecnologia blockchain no sistema de Prontuário Eletrônico do Paciente pode ser uma alternativa viável para garantir a proteção das informações médicas dos pacientes e dos demais agentes envolvidos.

4.2.1 Exemplos ao redor do mundo

Como vimos, a tecnologia blockchain é uma das inovações mais importantes do século XXI. Ela permite o registro descentralizado, seguro e privado de informações, tornando-a adequada para inúmeras aplicações. Entre as áreas em que a tecnologia blockchain está sendo aplicada, uma das mais promissoras é a saúde. Atualmente, já existem várias iniciativas em todo o mundo que estão explorando o uso da tecnologia blockchain no prontuário médico.

A utilização dessa tecnologia no prontuário médico tem vários benefícios, conforme foi mencionado ao longo do trabalho. Um dos principais é que ela garante a privacidade e a segurança dos dados do paciente. Isso porque a blockchain permite o registro de informações em uma rede descentralizada, sem a necessidade de intermediários. Dessa forma, os dados do paciente são criptografados e protegidos de forma eficaz, impedindo que hackers e outros criminosos possam acessá-los.

Além disso, a utilização da blockchain na área da saúde permite que os pacientes controlem seus próprios dados e compartilhem informações com mais facilidade e segurança. Isso pode ser especialmente útil em situações em que um paciente precisa mudar de médico ou procurar um especialista. Em termos práticos, a tecnologia blockchain no prontuário médico está sendo utilizada para permitir que

os pacientes controlem seus próprios registros médicos, compartilhem informações com seus médicos e provedores de saúde de forma segura e privada e rastrear medicamentos à medida que eles se movem pela cadeia de suprimentos. À medida que a tecnologia blockchain evolui e novas iniciativas surgem, é provável que vejamos ainda mais inovações no campo da saúde baseadas em blockchain.

Existem várias iniciativas em todo o mundo que estão explorando o uso da tecnologia no prontuário médico. Nesse cenário, há diversas plataformas baseadas em blockchain que foram desenvolvidas para resolver problemas relacionados aos registros eletrônicos de saúde e melhorar o gerenciamento e o acesso aos dados dos pacientes.

Uma dessas plataformas é o MedRec, um projeto desenvolvido no MIT Media Lab. O objetivo do MedRec é criar uma plataforma segura de gerenciamento de registros médicos eletrônicos, utilizando a tecnologia blockchain. Essa abordagem permite que os pacientes tenham controle sobre seus próprios dados de saúde e possam compartilhá-los com os profissionais de saúde de sua escolha. Além disso, a utilização do blockchain proporciona transparência, redução de custos e facilita o suporte aos cuidados de saúde prestados aos pacientes (MIT MEDIA LAB, 2019).

Outra plataforma que se destaca nesse contexto é a Medicalchain. Essa plataforma utiliza a tecnologia blockchain para criar uma solução descentralizada de troca de dados médicos. Ela garante segurança e rapidez na troca de informações médicas dos pacientes, permitindo que diferentes agentes de saúde acessem os registros médicos de forma auditável, transparente e segura (MEDICALCHAIN, 2015).

Além disso, a Hu-manity.co é uma plataforma que utiliza inteligência artificial para analisar contratos relacionados a dados. Essa plataforma é amplamente utilizada por várias instituições, principalmente na área médica, para garantir a conformidade com a legislação. Com a combinação da inteligência artificial e a tecnologia blockchain, a Hu-manity.co torna a gestão de dados mais transparente e confiável, contribuindo para restaurar a confiança no ambiente digital (“Restoring Trust in Digital”, [s.d.]).

Essas plataformas baseadas em blockchain trazem benefícios como segurança, transparência e maior controle dos pacientes sobre seus dados de

saúde. Elas representam avanços importantes no campo dos registros eletrônicos de saúde, facilitando o compartilhamento de informações entre os profissionais de saúde e melhorando a qualidade do atendimento médico.

Dentre as diversas iniciativas e softwares apresentados, é importante destacar ainda que alguns hospitais também têm adotado a tecnologia blockchain na implementação de seus prontuários médicos. Um exemplo disso é o hospital *Seoul Medical Center*, localizado na Coreia do Sul, que em parceria com a Samsung, implantou um registro médico eletrônico baseado em blockchain para garantir mais segurança e privacidade aos pacientes. Esta iniciativa é uma das primeiras na Coreia do Sul e permite que os pacientes controlem seus próprios registros médicos e compartilhem informações com mais confiança. Além disso, o *Taipei Medical University Hospital*, em Taiwan, também implantou a tecnologia blockchain em seu sistema de registro médico eletrônico para melhorar a segurança e a privacidade dos dados do paciente. Com isso, os pacientes têm mais controle sobre seus próprios dados e a compatibilidade entre os sistemas de saúde é aprimorada. Vejamos:

Diante de um sistema médico hierárquico e da crescente necessidade de cuidados de longo prazo, o superintendente Chen espera que o lançamento da Healthcare Blockchain Platform aumente significativamente o número de encaminhamentos de pacientes no TMUH. Por meio da segurança de dados, transparência e facilidade de compartilhamento de registros médicos, as pessoas podem entender melhor suas próprias condições de saúde e escolher o curso médico mais adequado para si. Somente quando a confiança e a segurança dos dados forem estabelecidas entre os diferentes níveis do instituto, um ecossistema inteligente e saudável será estabelecido. (TMUH, [s.d.]).

A confiança e a segurança dos dados são essenciais para estabelecer um ecossistema inteligente e saudável. É o que espera o superintendente Chen. Que a Healthcare Blockchain Platform aumente os encaminhamentos de pacientes no Taipei Medical University Hospital, oferecendo segurança de dados, transparência e facilidade de compartilhamento de registros médicos.

Portanto, se verifica que a tecnologia blockchain é uma das mais promissoras da atualidade e está sendo amplamente utilizada em diversos setores. No campo da saúde e da medicina, não poderia ser diferente, a tecnologia tem se

mostrado particularmente útil, pois permite que os registros médicos eletrônicos sejam gerenciados de forma segura e privada, garantindo a privacidade dos dados dos pacientes. Conforme vimos, hospitais em todo o mundo já adotaram a tecnologia blockchain em seus prontuários médicos, como o Seoul Medical Center, na Coreia do Sul, e o Taipei Medical University Hospital, em Taiwan, entre outros. Essas instituições têm relatado uma melhoria significativa na segurança e privacidade dos dados do paciente e uma maior transparência na troca de informações médicas.

No Brasil, o Sistema Único de Saúde (SUS) enfrenta muitos desafios relacionados à gestão de dados médicos e à interoperabilidade entre diferentes sistemas. A tecnologia blockchain pode ser uma solução para muitos desses problemas, permitindo que os pacientes controlem seus próprios dados de saúde e compartilhem informações com os profissionais de saúde de sua escolha, melhorando a acessibilidade e a qualidade do atendimento médico. Além disso, a utilização da tecnologia blockchain no SUS poderia melhorar a eficiência e reduzir os custos, além de permitir a rastreabilidade de medicamentos e outras informações importantes para a saúde pública. Embora ainda haja muitos desafios a serem enfrentados na implementação da tecnologia blockchain no SUS, sua adoção pode levar a uma transformação significativa no setor de saúde brasileiro.

4.3 Eventuais gargalos do sistema proposto

A tecnologia blockchain tem ganhado destaque no setor de saúde, principalmente no que se refere ao armazenamento e compartilhamento de informações dos pacientes. Embora seja uma tecnologia promissora, sua implementação no prontuário médico ainda enfrenta alguns desafios em relação à regulamentação e à adoção por parte dos hospitais e profissionais de saúde.

A utilização do blockchain no prontuário médico apresenta diversos benefícios, sendo a segurança e a privacidade dos dados dos pacientes um dos principais. A tecnologia permite a criação de um registro descentralizado e criptografado, o que garante proteção contra ataques cibernéticos e vazamento de informações. Além disso, o blockchain possibilita que o paciente tenha maior controle sobre seus próprios dados, permitindo que ele compartilhe suas

informações com profissionais de saúde de confiança. Por exemplo, um paciente que muda de médico pode facilmente autorizar o acesso aos seus registros, sem precisar passar por um processo burocrático. Outros benefícios incluem a redução de erros médicos, a agilidade no acesso às informações e a possibilidade de pesquisas clínicas mais precisas. Em resumo, a adoção do blockchain no prontuário médico pode revolucionar a forma como cuidamos da saúde, trazendo mais transparência, eficiência e segurança para todos.

Por outro lado, a implementação do blockchain no prontuário médico também apresenta desafios. Em primeiro lugar, é preciso considerar a complexidade do sistema de saúde em si, com seus vários profissionais e instituições envolvidos. Integrar o blockchain em um ambiente já complexo pode exigir um esforço significativo de adaptação e treinamento.

Além disso, é preciso considerar a interoperabilidade. O prontuário médico é um documento que precisa ser compartilhado entre diferentes profissionais e instituições de saúde. Para que isso ocorra de maneira eficiente, é necessário que haja padrões claros de interoperabilidade. O blockchain pode ajudar a garantir a segurança dessas informações, mas é preciso que haja um esforço conjunto para garantir que diferentes sistemas possam se comunicar entre si.

Ainda assim, um grande desafio que os apoiadores e entusiastas do blockchain enfrentam está relacionado à sustentabilidade da energia consumida pelo processo de hashing, que é fundamental para validar e resolver um bloco. Embora esse mecanismo seja crucial para proteger a rede, mantendo os nós autênticos e seguros até o final, o consumo de energia da rede blockchain é alarmante. Segundo Izabella Kaminska (KAMINSKA, 2014), o gasto energético da rede equivale ao consumo de energia elétrica de países inteiros. De acordo com a CIA (CIA, 2020), o consumo de energia da rede pode superar 4.409 bilhões de quilowatts-hora, o que é maior do que as emissões de gás carbônico do Chipre no mesmo período, que foram de 8801 milhões de megatons métricos. Portanto, a sustentabilidade da energia é um desafio significativo que deve ser enfrentado.

Outro desafio importante é a privacidade dos dados. Embora o blockchain seja conhecido por ser uma tecnologia segura e resistente a fraudes, é preciso garantir que as informações dos pacientes sejam protegidas de maneira adequada. É necessário que haja um esforço conjunto de todas as partes envolvidas para

garantir que as informações dos pacientes sejam armazenadas e compartilhadas de maneira segura e confiável.

Por fim, é preciso considerar a questão da regulamentação. Embora o blockchain possa oferecer muitos benefícios para o sistema de saúde, é importante que a implementação seja feita de maneira responsável e em conformidade com as regulamentações aplicáveis. É preciso que os profissionais e instituições de saúde entendam as implicações legais e éticas da utilização do blockchain no prontuário médico.

Em resumo, a implementação do blockchain no prontuário médico pode apresentar desafios significativos, mas também oferece muitas oportunidades para melhorar a segurança, privacidade e eficiência do sistema de saúde, como um todo. É fundamental que haja um esforço conjunto para assegurar que a implementação do blockchain seja feita de forma responsável e em conformidade com as regulamentações aplicáveis. Os benefícios são inúmeros: segundo Swan (2015), é possível utilizar a tecnologia blockchain para criar um vasto sistema de prontuários médicos eletrônicos, permitindo o armazenamento e a gestão de registros médicos pessoais. Conforme Gates (2017) e outros profissionais da saúde pode ser uma ferramenta crucial para salvar vidas, especialmente em casos de complicações cirúrgicas. Com acesso a todo o histórico médico do paciente, desde informações básicas como tipo sanguíneo até alergias a medicamentos, o cirurgião de plantão pode tomar decisões informadas e agir rapidamente para garantir o melhor tratamento possível.

Por fim, diante da possível regulamentação do blockchain, a tarefa dos agentes envolvidos é prever e evitar o sufocamento da tecnologia, repelindo reações exageradas e adaptando regras já existentes. Isso permite que investidores continuem a alavancar o desenvolvimento global da tecnologia por meio de acordos entre Estados e instituições. A governança deve se afastar da regulação e se aproximar do gerenciamento de recursos, pois a linha entre a ação perfeita e a omissão estratégica é tênue.

A segurança jurídica é requisito para que tenhamos justiça. Daí a necessidade de a ciência jurídica aproximar-se das novas tecnologias e prover princípios capazes de tutelar a dinâmica dos negócios digitais sem “engessá-los” [...]. Diante da velocidade com que a tecnologia se desenvolve, é impossível normatizar

determinado dispositivo de modo específico, sob pena de ser a lei ultrapassada rapidamente. Na esteira desse pensamento, os legisladores e operadores do direito, que contribuem com a discussão legal no contexto virtual, têm, primordialmente, priorizado a elaboração de dispositivos legais principiológicos, ou seja, textos que rejam a essência e os objetivos das tecnologias. Assim, ainda que se desenvolvam novos equipamentos, estes poderão ser protegidos e regidos legalmente pelos princípios em vigor. (LOPES; TEIXEIRA, 2017, p.8)

Embora os pessimistas apresentem diversas razões para o possível fracasso do blockchain, o otimismo prevalece quanto à possibilidade de um mundo melhor se aproximando. Todas as tecnologias têm o poder de mudar rapidamente o contexto social, empresarial e financeiro, mas isso não significa que elas estejam destinadas a criar desigualdades ou avanços. As inovações são moldadas pela escolha dos indivíduos que as utilizam. O blockchain pode ser uma tecnologia libertária e descentralizadora, desde que seja utilizada por pessoas responsáveis e com a mentalidade correta. Portanto, é fundamental buscar garantir oportunidades iguais para todos por meio de uma onda de inovação econômica e institucional liderada por indivíduos comprometidos com o bem comum.

5 CONSIDERAÇÕES FINAIS

Ao longo do trabalho vimos que, diante do desenvolvimento tecnológico, cada vez mais presentes em nossas vidas, é preciso levar em consideração a segurança e privacidade dos dados pessoais. O avanço tecnológico trouxe, além de benefícios, malefícios e implicações que afetam diretamente a sociedade. Um desses malefícios são os vazamentos de dados pessoais, que podem ocorrer em diversas áreas, inclusive na saúde.

No setor da saúde, a proteção de dados é ainda mais crucial, pois as informações compartilhadas são sensíveis e pessoais, relacionadas diretamente à privacidade e à dignidade das pessoas. A Lei Geral de Proteção de Dados (LGPD) surgiu como uma medida necessária para garantir a proteção dos dados pessoais, incluindo os dados sensíveis, presentes no prontuário médico.

Vimos ainda que, o surgimento da tecnologia blockchain trouxe uma nova possibilidade para garantir a segurança e privacidade das informações, em diversas áreas, bem como na saúde. A tecnologia blockchain consiste em um registro imutável, descentralizado e criptografado de transações, que garante a confiabilidade dos dados e a integridade do sistema. Os hospitais podem utilizar a tecnologia blockchain para garantir a segurança e privacidade dos dados de seus pacientes. A implementação dessa tecnologia no prontuário médico eletrônico permite a eliminação de riscos relacionados à perda, vazamento e invasões de dados, que são comuns em sistemas convencionais de banco de dados.

Mais adiante, em nosso trabalho, vimos que a Lei Geral de Proteção de Dados (LGPD) tem como objetivo principal proteger os dados pessoais, inclusive os dados sensíveis presentes no prontuário médico. A lei estabelece diretrizes claras sobre a coleta, armazenamento, tratamento e compartilhamento desses dados, garantindo a privacidade e a segurança das informações. A LGPD possui artigos específicos que tratam do tratamento dos dados pessoais que podem ser aplicados na área da saúde, como o artigo 11, que estabelece a necessidade de consentimento do paciente para o compartilhamento de suas informações de saúde. Como se verifica:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

Nesse sentido, se verifica que a implementação do prontuário médico eletrônico com tecnologia blockchain pode enfrentar desafios, mas as perspectivas para a evolução do tratamento dos dados sensíveis no âmbito da saúde são promissoras. A tecnologia blockchain oferece uma solução segura e confiável para a proteção dos dados pessoais, e pode ser utilizada em diferentes setores da saúde, como hospitais, clínicas e laboratórios. Prova disso, é a utilização já consolidada, por alguns hospitais, pioneiros, ao longo do globo, conforme demonstrado no trabalho.

Além disso, a aplicação da tecnologia blockchain no prontuário médico eletrônico também traz outros benefícios importantes, como a possibilidade de acesso remoto e seguro às informações de saúde pelos pacientes e profissionais autorizados. Isso pode melhorar significativamente a eficiência dos serviços de saúde, reduzir erros médicos e otimizar o tratamento dos pacientes.

No entanto, apesar dos inúmeros benefícios e perspectivas promissoras que a tecnologia blockchain pode oferecer para a proteção e segurança dos dados médicos, ainda existem alguns desafios a serem superados para sua implementação efetiva. Um dos principais obstáculos é a resistência cultural e a falta de conhecimento dos profissionais de saúde em relação à tecnologia blockchain. Além disso, o alto custo de implementação e a necessidade de interoperabilidade entre sistemas também são desafios importantes.

É fundamental, portanto, que as instituições de saúde invistam em programas de treinamento e capacitação dos profissionais de saúde para compreenderem os benefícios e possibilidades da tecnologia blockchain. Além disso, é necessário que sejam estabelecidos padrões e diretrizes claras para a interoperabilidade e integração de sistemas, a fim de garantir a efetividade da tecnologia blockchain na proteção e segurança dos dados médicos.

Em resumo, a viabilidade da tecnologia blockchain no prontuário médico eletrônico representa um avanço fundamental e imprescindível para assegurar a salvaguarda e o sigilo das informações de saúde dos pacientes, em um cenário de incessante progresso tecnológico e aumento constante das ameaças cibernéticas.

Embora tenham sido enfrentados alguns desafios na implementação da tecnologia, tais como a carência de profissionais capacitados e o alto custo financeiro, estes se revelaram facilmente superáveis diante das inúmeras vantagens, benefícios e seguranças que a aplicação da tecnologia traz consigo. Ademais, constatamos que a Lei Geral de Proteção de Dados figura como um marco relevante nessa seara, definindo diretrizes claras e rígidas para a proteção de dados pessoais sensíveis. Nesse sentido, a integração da tecnologia blockchain com a referida lei resulta em uma proteção maior para todos os atores envolvidos, sejam eles pacientes, médicos, instituições de saúde ou quaisquer outros. Cabe, portanto, às instituições de saúde e aos profissionais do setor capacitarem-se e adaptarem-se à nova realidade tecnológica, a fim de assegurar a segurança e a privacidade dos dados médicos dos pacientes.

REFERÊNCIAS

ANPD. Disponível em: <<https://www.gov.br/anpd/pt-br>>. Acesso em: 06 abril. 2023

ARAUJO, N. C.; MOTA, F.R.L. Prontuário de paciente: questões éticas. Informação em Pauta, Fortaleza, v.5, n. especial. P. 52-67, março 202º. Disponível em: <https://doi.org/10.36517/2525-3468.ip.v5iespecial1.2020.43512.52-67>. Acesso em: 07 abril. 2023.

BBCBrasil.com | Reporter BBC | Hackers roubam detalhes de 45 milhões de cartões. Disponível em: <https://www.bbc.com/portuguese/reporterbbc/story/2007/03/070330_hackerscartoes_is>. Acesso em: 26 mar. 2023.

BIONI, B. R. Proteção de dados pessoais: a função e o limite do consentimento.

BITENCOURT, G. GDPR: tudo o que você precisa saber sobre a lei europeia de proteção de dados. Disponível em: <<https://www.mutuus.net/blog/gdpr-lei-protecao-dados-europeia/>>. Acesso em: 14 mar. 2023.

BRAGA, Alexandre Melo. Tecnologia Blockchain: fundamentos, tecnologias de segurança e desenvolvimento de software. Campinas: CPQD, 2017. Disponível em: <<https://docplayer.com.br/67466015-Fundamentos-tecnologias-de-seguranca-e-desenvolvimento-de-software.html>> Acesso em: 26 jan. 2023.

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: 27 set. 2022.

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 [

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

Brasil. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. [Internet]. 1990

Blockchain visualisation. Disponível em: <<https://dailyblockchain.github.io/>>. Acesso em: 27 set. 2022.

CAMBRICOLI, F. Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. Disponível em: <https://www.estadao.com.br/saude/nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes/>. Acesso em: 26 mar. 2023.

Capurro R, Eldred M, Nagel D. It and privacy from an ethical perspective digital whoness: identity,

CIA. Europe :: Cyprus — The World Factbook – Central Intelligence Agency. Disponível em: <https://www.cia.gov/library/publications/resources/the-world-factbook/geos/cy.html>. Acesso em: 17 abr. 2023.

Conselho Federal de Medicina. RCFM. Resolução nº 1.821/2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. DOU. Brasília, 11. Jul. 2007. Disponível em: <https://www.portalmédico.org.br/resolucoes/cfm/2007/18212007.htm>. Acesso em: 06 abril. 2023

Conselho Federal de Medicina. RCFM. Resolução nº 1.638/2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. 2002. D.O.U. Brasília, 10 jul. 2002. Disponível em: [https://www.portalmédico.org.br/esolucoes/cfm/2002/1638 2002.htm](https://www.portalmédico.org.br/esolucoes/cfm/2002/1638%2002.htm). Acesso em: 06 abril. 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.

FRUET, G. Lady Di e a Privacidade. Disponível em: <https://www.folhadelondrina.com.br/opiniaolady-di-e-a-privacidade---gustavo-fruet-39542.html?d=1>. Acesso em: 17 mar. 2023.

G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. Disponível em: <https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 26 jan. 2023

G1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>. Acesso em: 02 abr. 2023.

KAMINSKA, Izabella. Bitcoin's Wasted Power – and How It Could Be Used to Heat Homes, FT Alphaville, Financial Times, 5 de setembro de 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: 27 set. 2022

Lei nº 13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informativos para a guarda, o armazenamento e o manuseio de prontuário do paciente. Presidência da República Secretaria - Geral. 2018. Diário Oficial da União. Brasília. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm. Acesso em: 09 abril. 2023

Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 jan. 2023.

LIMA, Cíntia Rosa Pereira de. ANPD e LGPD: Desafios e perspectivas. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2021. E-book. ISBN 9786556272764. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786556272764/>. Acesso em: 05 mar. 2023.

LOPES, Alan Moreira; TEIXEIRA, Tarcisio. Direito no Empreendedorismo (entrepreneurship law). IN: Tarcisio Teixeira e Alan Moreira Lopes. Startups e Inovação: direito no empreendedorismo (entrepreneurship law). Barueri, SP: Manole, 2017.

MACHADO, Felipe Nery R. Segurança da informação - princípios e controle de ameaças - 1ª edição - 2014. [Digite o Local da Editora]: Editora Saraiva, 2014. E-book. ISBN 9788536531212. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788536531212/>. Acesso em: 26 mar. 2023.

MEDICALCHAIN. Medicalchain – Blockchain for Electronic Health Records. Disponível em: <https://medicalchain.com/en/>. Acesso em: 16 abril 2023.

MINISTÉRIO DA SAÚDE. Página inicial. Disponível em: <https://www.gov.br/saude/pt-br>. Acesso em: 12 mar 2023

MIT MEDIA LAB. News + Updates – MIT Media Lab. Disponível em: <https://www.media.mit.edu/>. 16 abril 2023.

MORAES, Alexandre Fernandes de. Bitcoin e Blockchain: a revolução das moedas digitais. [Digite o Local da Editora]: Editora Saraiva, 2021. E-book. ISBN 9786558110293. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786558110293/>. Acesso em: 23 fev. 2023.

MOUGAYAR, William. Blockchain para negócios: promessa, prática e aplicações da nova tecnologia da internet. Rio de Janeiro: Alta Books, 2017. 224 p. Acesso em: 23 fev. 2023.

NEWS BRASIL, B. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>>. Acesso em: 18 fev. 2023.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13709/2018 (LGPD). 2ª edição. São Paulo: Saraiva Educação, 2020. Acesso em: 18 fev. 2023.

Restoring Trust in Digital. Disponível em: <https://hu-manity.co/>>. Acesso em: 16 abril 2023.

SIQUEIRA, S. Leticia; HOCH, A. Patrícia. Os dados pessoais e a proteção de dados de saúde: análise a partir das iniciativas de e-saúde. Anais. 5º Congresso Internacional de Direito e contemporaneidade. Ed. 2019. UFSM - Universidade Federal de Santa Maria. Santa Maria. RS. Disponível em: <https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/congressodireito-anais>. Acesso em: 09 abril. 2023.

SOUZA, R. Exclusivo: clínica médica deixa vaziar mais de 2,3 mil laudos de pacientes. Disponível em: <https://thehack.com.br/exclusivo-clinica-medica-deixa-vazar-mais-de-2-3-mil-laudos-de-pacientes/>>. Acesso em: 26 mar. 2023.

STALLING, William. Criptografia e segurança de redes: princípios e práticas. 6. Ed. São Paulo: Pearson Education do Brasil, 2015. 578 p. Acesso em: 26 jan. 2023.

SWAN, Melanie. Blockchain: blueprint for a new economy. Sebastopol: O'Reilly, 2015. 128 p. Acesso em: 26 jan. 2023.

TMUH, AIPEI M. U. H. 臺北醫學大學附設醫院. Disponível em: <https://www.tmu.org.tw/single/3778>>. Acesso em: 17 abr. 2023.

WARREN, S. D. BRANDEIS, L. D. S. The right to privacy. Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890). Disponível em: <http://www.jstor.org/stable/1321160?seq=2>> Acesso em: 19 mar. 2022.