UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

FABIAN ANDRADE SILVA

MODELO COMPUTACIONAL PARA CADEIA DE CUSTÓDIA DIGITAL: IDENTIFICAÇÃO E COLETA COM BASE EM TECNOLOGIA BLOCKCHAIN

CURITIBA

2024

FABIAN ANDRADE SILVA

MODELO COMPUTACIONAL PARA CADEIA DE CUSTÓDIA DIGITAL: IDENTIFICAÇÃO E COLETA COM BASE EM TECNOLOGIA BLOCKCHAIN

Digital Chain of Custody Computational Model: Blockchain-based Identification and Collection

Dissertação apresentada como requisito para obtenção do título de Mestre do Programa de Pós-Graduação em Computação Aplicada da Universidade Tecnológica Federal do Paraná (UTFPR).
Orientador: Dr. Gustavo Alberto Gimenez Lugo.

CURITIBA

2024

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba

FABIAN ANDRADE SILVA

MODELO COMPUTACIONAL PARA CADEIA DE CUSTÓDIA DIGITAL: IDENTIFICAÇÃO E COLETA COM BASE EM TECNOLOGIA BLOCKCHAIN

Trabalho de pesquisa de mestrado apresentado como requisito para obtenção do título de Mestre Em Computação Aplicada da Universidade Tecnológica Federal do Paraná (UTFPR). Área de concentração: Engenharia De Sistemas Computacionais.

Data de aprovação: 27 de Março de 2024

Dr. Gustavo Alberto Gimenez Lugo, Doutorado - Universidade Tecnológica Federal do Paraná

Dr. Cesar Augusto Tacla, Doutorado - Universidade Tecnológica Federal do Paraná

Dr. Robinson Vida Noronha, Doutorado - Universidade Tecnológica Federal do Paraná

Dr. Rubens Alexandre De Faria, Doutorado - Universidade Tecnológica Federal do Paraná

Documento gerado pelo Sistema Acadêmico da UTFPR a partir dos dados da Ata de Defesa em 28/03/2024.

Dedico este trabalho à minha família, cuja paciência e incentivo foram fundamentais nesta jornada. Ao meu orientador Prof. Dr. Gustavo Gimenez Lugo, que sempre acreditou em mim, meu eterno agradecimento.

AGRADECIMENTOS

Ao término desta dissertação, não consigo deixar de olhar para trás e reconhecer o imenso apoio e as contribuições de muitas pessoas, sem as quais este trabalho não seria possível. Este é um momento de grande emoção e gratidão, e quero expressar meus mais sinceros agradecimentos a todos que, de alguma forma, estiveram ao meu lado nesta jornada.

Primeiramente, agradeço a Deus pela força e sabedoria para enfrentar os desafios ao longo deste percurso. Sua presença constante foi meu alicerce em momentos de dúvida e cansaço.

A Denise, pelo amor, paciência e apoio constante. Sua compreensão nos momentos de ausência e sua capacidade de me animar nos momentos de desânimo foram fundamentais.

Agradeço por estar ao meu lado e por acreditar em mim incondicionalmente.

As minhas filhas Giovanna, Manuella e Esther que me inspiram cada dia a procurar a melhora das batalhas cotidianas.

Ao meu orientador, Gustavo Alberto Gimenez Lugo, minha profunda gratidão por sua orientação, paciência e incentivo ao longo deste processo. Suas sugestões valiosas, críticas construtivas e a confiança depositada em mim foram essenciais para a realização deste trabalho. Agradeço por me guiar com sabedoria e humanidade, e por sempre me desafiar a buscar o melhor de mim. E participou de momentos muito difíceis na minha vida pessoal.

Aos professores do programa de pós-graduação, que contribuíram significativamente para minha formação acadêmica. Cada aula, cada discussão e cada feedback foram dados de forma cirúrgica para o desenvolvimento deste trabalho. Agradeço as orientações que foram particularmente valiosas.

Por fim, mas não menos importante, aos meus amigos dentro e fora do ambiente acadêmico, que compreenderam minhas ausências e me apoiaram incondicionalmente. Vocês trouxeram leveza e alegria para minha vida, mesmo nos momentos de maior pressão. Agradeço por me lembrar da importância do equilíbrio e por estarem sempre ao meu lado. Este trabalho é o culminar de muitos esforços e sacrifícios, não apenas meus, mas de todos que estiveram comigo. A vocês, minha eterna gratidão.

Ao navegarmos pelo futuro digital, a convergência entre tecnologias disruptivas e a Lei Geral de Proteção de Dados representa o compromisso de harmonizar inovação com transparência. Nesse equilíbrio, construímos a base para uma sociedade mais justa e segura.
(Fabian Andrade Silva, 2024)

RESUMO

As atuações jurídicas relativas à cadeia de custódia digital são cada vez mais importantes, considerando o surgimento do número de atividades de crimes cibernéticos. Em uma investigação forense, é necessário seguir diversas leis para que seja garantida a transparência processual e o direito de defesa das partes. Dessa forma, a cadeia de custódia consiste em um procedimento para a realização da documentação das provas em eventos cronológicos. Atualmente, há diversas iniciativas relacionadas ao controle físico das evidências, porém, os dados lógicos são, nos casos de crimes, cruciais para a resolução de um conflito ou a correta aplicação de penalidade prevista na legislação. A Lei Geral de Proteção de Dados (LGPD) harmoniza e regula a proteção da privacidade e dos dados pessoais no Brasil. Foi inspirada nas discussões que culminaram na proteção de dados segundo a União Europeia (GDPR), e tem por objetivo não apenas conferir às pessoas maiores controles sobre seus dados, mas lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais. A transição para a documentação eletrônica com suporte na tecnologia *blockchain* melhora a legibilidade, a autenticidade, a utilidade dos documentos e, portanto, a interação entre as partes interessadas em relação ao devido processo legal. Neste trabalho, apresenta-se uma visão abrangente da extensão de problemas e desafios enfrentados na cadeia de custódia digital. Além disso, propõe-se uma solução para a identificação de evidências digitais, fundamentada na tecnologia de cadeia de blocos.

Palavras-chave: GDPR, LGPD. Brasil, União Européia. Blockchain. Cadeia de Custódia. Evidência Digital.

ABSTRACT

Legal actions in relation to the digital chain of custody become increasingly important considering the emergence of the number of cybercrime activities. In a forensic investigation it is necessary to follow several laws in order to guarantee procedural transparency and the right of defense of the parties, in this way, the chain of custody is a procedure to carry out the documentation of evidence in chronological events. It is possible to verify that there are already several initiatives related to the physical control of evidence, however, in the cases of crimes, logical data are often crucial for the resolution of a conflict or the correct application of the penalty provided for in the legislation. The General Data Protection Law (LGPD) harmonizes and regulates the protection of privacy and personal data in Brazil. It was inspired by the discussions that culminated in data protection according to the European Union (GDPR) and aims not only to give people greater control over their data, but to deal with the most innovative business models based on the use of personal data. The transition to electronic documentation supported by blockchain technology improves the readability, authenticity and usefulness of documents and therefore improves communication between stakeholders within due process. This work gives an overview of the extent to which problems and challenges are faced in the digital chain of custody and proposes a solution for identifying digital evidence based on blockchain technology.

Keywords: *LGPD, GPDR. Brazil, UE. Blockchain. Chain of Custody. Digital Evidence.*

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Na Era Digital, a sociedade experimenta uma transformação significativa, caracterizada pelo domínio da tecnologia, impactando, consideravelmente, as práticas jurídicas. Em relação à cadeia de custódia digital, estas tornam-se cada vez mais importantes, considerando o surgimento de atividades de crimes cibernéticos; sejam eles como meio para a prática ilícita ou como o próprio crime. Essa é uma das consequências do desenvolvimento da tecnologia da informação e da melhoria da infraestrutura de telecomunicações, o que facilita a conexão de cada indivíduo em um ambiente virtual quase sem limites. A atuação de profissionais de segurança da informação e peritos digitais requer habilidades especializadas para a realização de investigações em dispositivos eletrônicos e dispositivos móveis como: registros de dados de chamadas, ordens de busca, extração forense, recuperação de dados e perícias audiovisuais. Consideram-se, também, os dados *offline* ou fora dos equipamentos nesse escopo, bem como o ecossistema ciberfísico altamente integrado com o qual se interage com os ambientes em nuvens cada vez mais indispensáveis (Al-Khateeb Haider; Epiphaniou, 2019).

Em uma investigação forense, é necessário seguir diversas normas para que seja atendida a transparência processual e o direito de defesa das partes. Nesse sentido, de acordo com Giova *et al.* (2011), a cadeia de custódia constitui um procedimento que implica a documentação das

provas em eventos cronológicos. Para Ć Osić *et al.* (2011), a cadeia de custódia é uma parte importante do processo de investigação que garantirá que as provas possam ser aceitas no sistema judicial. Para o poder judiciário brasileiro, as provas físicas e digitais complementam o processo de investigação. Dessa forma, supõe-se que o tratamento de provas físicas ou digitais seja o mesmo, ou, pelo menos, tenha um mecanismo semelhante.

A respeito da cadeia de custódia, na legislação vigente, tratam-se os equipamentos físicos e os dados lógicos como um único elemento. Nesse contexto, efetuam-se os procedimentos pertinentes à documentação e ao controle dos dispositivos eletrônicos ou mídias de armazenamento, desde o momento em que são apreendidos até sua análise e eventual apresentação como evidência em um processo judicial. No entanto, podem ocorrer diversos problemas nesse processo, comprometendo a parte lógica da evidência, ou seja, os dados. A cadeia de custódia

dos dados lógicos refere-se à documentação e ao controle dos dados extraídos dos equipamentos eletrônicos durante processos forenses, o que representa um obstáculo, contemporaneamente, nos processos judiciais (Prayudi; SN, 2015).

Há diversas iniciativas relacionadas ao controle físico das evidências, porém, nos casos de crimes cibernéticos, os dados lógicos são, muitas vezes, cruciais para a resolução de um conflito ou a correta aplicação de penalidade prevista na legislação. É de grande importância que todas as modificações sejam documentadas e rastreáveis, permitindo que se reconstrua o histórico das ações realizadas durante o processo forense. Esses dados lógicos não passam pelo processo de rastreio, uma vez que, para a cadeia de custódia, o equipamento físico já foi identificado (Prayudi; SN, 2015).

Determina-se, por meio da admissibilidade da prova digital, uma evidência digital que, por sua vez, poderá se tornar uma evidência verdadeira. Para que os dados lógicos sejam admissíveis em um tribunal, é necessário que a cadeia de custódia digital demonstre a integridade e a autenticidade dos dados. Isso envolve a apresentação de registros detalhados das etapas de coleta, extração, análise, armazenamento e transferência dos dados, bem como a qualificação dos profissionais envolvidos. A autoridade judiciária ou colegiado judicial decide qual evidência será apresentada ao longo do Devido Processo Legal (COSIC, 2017).

As inovações tecnológicas, por meio da implementação de segurança de dados e criptografia, impulsionam uma indústria significativa. Além disso, diversos governos internacionais utilizam essas inovações. A tecnologia *Blockchain* constitui um exemplo dessas inovações, e é composta por uma lista básica de registros, ou seja, blocos, vinculados por meio de algoritmos criptográficos. A sólida conexão e a continuidade dos blocos impedem a modificação dos blocos de dados existentes e qualquer conteúdo escrito é, portanto, verificável e acessível. Ela pode ser incorporada em novos sistemas para facilitar a modernização dos rastreamentos de uma prova digital e alcançar uma a criação de uma Cadeia de Custódia para ser mantida no contexto mais amplo de uma investigação digital (Ewald, 2019).

Da mesma forma, a transição para a documentação eletrônica, com suporte na tecnologia *blockchain*, melhora a legibilidade, a autenticidade a utilidade dos documentos e, portanto, a interação entre as partes interessadas no devido processo legal. Por outro lado, a falta de controle de dados pode levar ao abuso do sistema, fraudes e, inclusive, ao comprometimento da qualidade do serviço público prestado.

Podem-se resolver essas preocupações com a implementação de uma cadeia de custódia *online* que tenha seus registros compartilhados na esfera do judiciário, assim como ocorre com o compartilhamento de informações processuais realizado entre os países europeus (AL-Khateeb Haider; Epiphaniou, 2019).

Diante desse cenário, envolvendo a problemática da dissociação entre cadeia de custódia física e lógica atrelada, consideram-se as novas tecnologias disruptivas como um novo fator crítico à recente legislação sobre a proteção geral de dados pessoais, a LGPD. Muitas vezes os dados coletados contêm informações pessoais sensíveis. Essa lei exige que o tratamento de dados pessoais tenha uma base legal válida. Para forense, é necessário que haja uma base legal específica para acessar, coletar e tratar esses dados lógicos, o que pode ser ser obtido por meio de autorização judicial, desde que sejam demonstradas a necessidade e a proporcionalidade do acesso aos dados para o andamento do processo legal (Cunha, 2020).

Reforça-se, na legislação brasileira, a importância de proteção da privacidade e dos direitos dos indivíduos de forma ampla, mesmo em um contexto forense. Os profissionais auxiliares da justiça e os peritos digitais devem sempre estar em conformidade com as disposições da lei, adotando medidas de segurança adequadas e garantindo que os direitos dos titulares dos dados sejam respeitados (Cunha, 2020).

Há desafios e oportunidades para o campo da investigação forense e da perícia digital em relação à interseção entre a cadeia de custódia digital das evidências cibernéticas. A adoção de práticas para propor uma possível solução com o uso de tecnologias inovadoras é fundamental para superar as dificuldades e abrir um campo ainda pouco explorado em busca da integridade dos dados, do respeito à privacidade, em conformidade com a legislação de proteção de dados.

1.1 PROBLEMA

O problema envolvendo a cadeia de custódia — *blockchain* e LGPD — tem muita relevância no cenário atual da sociedade digital em constante atualização. Esse contexto se desenrola em um momento em que crimes cibernéticos têm se tornado cada vez mais comuns, exigindo uma abordagem específica para lidar com a coleta, preservação e identificação de evidências digitais em processos judiciais.

A cadeia de custódia constitui um procedimento fundamental em investigações forenses. Ela se concentra em documentar a sequência cronológica dos eventos relacionados à coleta e à manipulação de evidências, garantindo a transparência do processo e o direito de defesa das partes envolvidas. No entanto, o desafio surge quando se trata de evidências digitais, pois os dados, quando coletados, seguem um novo caminho e precisam de um rastreamento (Cunha, 2020).

A LGPD (Lei Geral de Proteção de Dados) é a legislação brasileira que visa proteger a privacidade e os direitos dos indivíduos no que diz respeito ao tratamento de seus dados pessoais. Ela estabelece regras rigorosas para a coleta, uso e o compartilhamento de informações pessoais. Portanto, ao lidar com evidências digitais em investigações forenses, é crucial estar em conformidade com a LGPD, para garantir os direitos dos titulares dos dados (Nunes, 2019).

Nesse contexto, surge a tecnologia *blockchain*. O *blockchain* é uma tecnologia que utiliza algoritmos criptográficos para criar uma cadeia de blocos interligados, tornando os dados imutáveis e verificáveis. Isso é especialmente valioso ao lidar com evidências digitais, pois auxilia a preservação da rastreabilidade dos dados ao longo do tempo. Registra-se cada transação ou manipulação dos dados de forma permanente no *blockchain*, criando um histórico transparente e à prova de adulteração (Bartlett, 2021).

Investiga-se, nesta dissertação, uma possível solução para o problema entre a cadeia de custódia, o *blockchain*. Além disso, busca-se compreender se a LGPD apresenta desafios e oportunidades para o campo da investigação forense, da perícia digital e para a aplicação das legislações. É fundamental encontrar soluções inovadoras que permitam a integridade dos dados, o respeito à privacidade e a conformidade com a legislação de proteção de dados. Isso requer a adoção de práticas que permitam o uso apropriado do *blockchain* para rastrear evidências digitais, preservando sua integridade, e garantindo, simultaneamente, a conformidade com as disposições da LGPD, mediante autorizações judiciais, quando necessário.

O domínio problemático que envolve a cadeia de custódia, *blockchain* e LGPD, refere-se à necessidade de preencher um vazio existente das evidências digitais em investigações forenses, cumprindo as regulamentações da LGPD. A adoção de tecnologias inovadoras, como o *blockchain*, pode ser uma possível solução para esse desafio em constante evolução.

1.2 OBJETIVOS

Propõe-se, neste trabalho, a identificação da evidência lógica extraída de equipamentos informatizados em uma cadeia de custódia de forense digital que preencha a lacuna existente entre o formato estabelecido de rastreamento atualmente estabelecido na legislação, tornando-se uma evidência digital respaldada pela tecnologia de cadeia de blocos, e em conformidade com as formalidades legais de proteção de dados.

Para atingir esse objetivo, estabeleceram-se os seguintes objetivos específicos:

- **analisar os princípios gerais de proteção de dados:** realização de uma análise aprofundada dos princípios e normas legais relacionados à proteção de dados pessoais, inicialmente criado pela União Europeia o Regulamento Geral de Proteção de Dados (GDPR) e que obteve grande influência na legislação brasileira, com destaque para a LGPD.
- **Compilar bibliografia sobre os temas:** realização de uma revisão bibliográfica abrangente sobre a cadeia de custódia digital, a tecnologia *blockchain*, forense digital e proteção de dados, a fim de embasar, teoricamente, a proposta do trabalho.
- **Realizar a comparação entre as soluções existentes para Cadeia de Custódia Digital:** condução de uma análise comparativa das soluções existentes para a cadeia de custódia digital, considerando os aspectos previstos na legislação brasileira.
- **Indicar como a tecnologia blockchain pode ser uma solução viável para manter a cadeia de custódia de forense digital no contexto da legislação brasileira de proteção de dados:** apresentação de uma análise sobre como a tecnologia *blockchain* pode ser aplicada, de forma viável e eficiente, para manter a integridade e a rastreabilidade da cadeia de custódia de forense digital, considerando os requisitos específicos da legislação brasileira.
- **Elaborar uma proposta que atenda aos requisitos centrais desta pesquisa: desenvolvimento,** com base nos resultados obtidos na pesquisa e nas análises realizadas, de uma proposta concreta para a implementação de um cenário experimental de cadeia de custódia de forense digital apoiada na tecnologia *blockchain*, considerando-se as necessidades do contexto brasileiro.

Com base nesses objetivos, estabeleceram-se os limites de escopo de

trabalho. Assim, desconsideraram-se as seguintes temáticas:

- assuntos que competem os atos de fé Pública, ou seja, uma prerrogativa de crédito atribuída aos agentes públicos para que estes possam exercer as suas incumbências específicas do direito subjetivo;
- itens de isolamento, fixação, acondicionamento, transporte recebimento, processamento, armazenamento e descarte dos procedimentos da cadeia de custódia, tendo foco exclusivo na coleta;
- itens de adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação, responsabilidade e prestação de contas dos princípios estabelecidos na legislação de proteção de dados;
- armazenamentos de dados *off-chain*, os dados de uma solução *blockchain* podem ser registrados usando armazenamentos de dados tradicionais, e o único valor compartilhado é a evidência do estado do artefato em um determinado momento;
- solução completa para rastreio total de todos os passos dos procedimentos, com enfoque para a coleta de dados das evidências.

Ressalta-se que, em relação ao esclarecimento da existência de vários domínios de problemas em um mesmo contexto, estabelece-se, neste trabalho, uma proposta para apontar um único domínio em que seja possível diminuir as incertezas e reduzir ao máximo as interveniências sem registros de acessos.

Ao alcançar esses objetivos, busca-se contribuir para a melhoria da cadeia de custódia digital na esfera forense, proporcionando maior confiabilidade, segurança e conformidade com a legislação de proteção de dados, por meio da utilização adequada da tecnologia *blockchain*.

1.3 MOTIVAÇÃO

O sistema judicial já se tornou flexível em relação à aceitação de provas digitais, em virtude de o mecanismo de tratamento das provas digitais se assemelhar à forma de tratamento de provas físicas. A esfera de pesquisa digital e perícia forense mantém sua trajetória ascendente, demandando que peritos forenses e investigadores digitais possuam as habilidades essenciais para capturar a cena do crime, avaliar registros de dados, examinar os registros obtidos, recuperar informações e participar, ativamente, do processo de perícia digital (Alruwaili, 2021).

Para Alruwaili, 2021, os desafios enfrentados por uma equipe forense em

relação às evidências digitais derivam da natureza intrínseca das informações digitais. Estas podem estar sujeitas a alterações ou remoção de dados cruciais para o caso. Questões como a identificação do responsável pelo tratamento da evidência, o estabelecimento do nível de controle de acesso apropriado, a segurança no armazenamento das provas, e a confiabilidade para a transmissão das evidências para outras jurisdições, seja em diferentes estados ou, inclusive, em países distintos, são preocupantes. Essa realidade, sem dúvida, representa um desafio crescente para a cadeia de custódia no sistema judicial brasileiro.

Por esses motivos, espera-se contribuir para o estabelecimento de um padrão mais adequado a respeito da manutenção das cadeias de custódia e do ciclo de vida das evidências digitais, bem como para auxiliar o poder judiciário brasileiro, explorando a tecnologia que revoluciona a forma de lidar com informações digitais para apoiar o controle, transferência, análise e monitoramento da preservação e exclusão das evidências.

1.4 JUSTIFICATIVA

A cadeia de custódia desempenha um papel fundamental para a asseguração da integridade e rastreabilidade das evidências, preservando a confiabilidade e transparência em relação à produção da prova. Diante disso, é inquestionável a adoção dos procedimentos relativos à cadeia de custódia (Lone; Mir, 2019a).

Os vestígios cibernéticos ou dados lógicos não recebem os mesmos tratamentos dados aos vestígios físicos; a cadeia de custódia trata os dados lógicos extraídos dos equipamentos, apenas, como uma parte dos dispositivos físicos que foram lacrados na coleta, porém, nesse momento, separam-se os vestígios e não há um "lacre digital"para garantir o rastreio de acessos e os limites de utilização das informações relevantes para o processo judicial (Velho *et al.*, 2016).

A etapa de análise de um vestígio digital computacional, na fase interna da cadeia de custódia, deve ser regida por ambientes e requisitos rígidos. Dessa forma, é necessária a identificação dos atores que terão algum tipo de contato com os dados e o permissionamento adequado (Velho *et al.*, 2016).

Neste trabalho, defende-se a utilização da tecnologia *blockchain* para melhorar o processo de cadeia de custódia e o ciclo de vida do tratamento de evidências digitais. Essa tecnologia fornece segurança integrada para controlar o

acesso às informações e rastrear alterações ao longo do período de vida dos dados. Nesse sentido, propõe-se um modelo conceitual de *blockchain* para preencher a lacuna relativa à separação entre os dados e os equipamentos físicos da cadeia de custódia, e abordar os desafios enfrentados para o tratamento de evidências digitais, a fim de aumentar a eficiência nos processos judiciais, aplicando como base a legislação de proteção de dados.

1.5 PERSPECTIVA

A perspectiva desse problema é complexa e envolve diversos aspectos que precisam ser cuidadosamente abordados. Em primeiro lugar, há a cadeia de custódia, essencial para qualquer investigação forense, seja esta relacionada a crimes cibernéticos ou não. A cadeia de custódia envolve a documentação precisa de cada passo no manuseio de evidências, garantindo que elas permaneçam íntegras e confiáveis ao longo do processo legal. Contudo, em relação às evidências digitais, acentua-se a complexidade, uma vez que a abordagem não se restringe a objetos físicos, mas sim a dados eletrônicos suscetíveis a alterações ou corrupções. Além disso, surge a consideração da LGPD (Lei Geral de Proteção de Dados), que define diretrizes para o manuseio de informações pessoais. A LGPD visa proteger a privacidade e os direitos dos indivíduos, o que é fundamental em um mundo digital cada vez mais conectado. Portanto, é necessário encontrar um equilíbrio entre a necessidade de coletar evidências para fins legais e a obrigação de proteger os dados pessoais, conforme estabelecido pela LGPD. A terceira questão refere-se à tecnologia *blockchain* como uma possível solução. O *blockchain* utiliza criptografia e registro distribuído para garantir a integridade e a rastreabilidade dos dados. Cada ação relacionada às evidências digitais pode ser registrada de forma imutável no *blockchain*, o que torna as evidências altamente confiáveis e à prova de adulteração. No entanto, a implementação eficaz do *blockchain*, em processos de investigação forense, exige a definição de padrões e práticas específicas, bem como a conformidade com a LGPD.

A perspectiva desse problema envolve a busca por uma abordagem que permita a coleta, preservação e apresentação de evidências digitais de forma íntegra e autêntica, respeitando os direitos de privacidade estabelecidos pela LGPD. A

tecnologia *blockchain* apresenta oportunidades para alcançar esses objetivos, mas também requer um esforço conjunto de profissionais da área jurídica, peritos digitais e especialistas em tecnologia para garantir sua implementação eficaz e legalmente compatível.

1.6 ESTRUTURA DO DOCUMENTO

Apresenta-se, nesta dissertação, uma pesquisa relativa à utilização da tecnologia *blockchain* para o controle da cadeia de custódia em relação à identificação de evidências digitais. Dividiu-se este trabalho em sete capítulos. No primeiro, a introdução, contextualiza-se a temática de pesquisa; no segundo, descreve-se a revisão de literatura, buscando aspectos das legislações relacionadas à proteção de dados e à cadeia de custódia das evidências digitais, bem como à busca pelo estado da arte da aplicação da tecnologia *blockchain*, além da tendência de utilização da cadeia de custódia digital. No terceiro capítulo, descreve-se o método aplicado, como realizaram-se os experimentos e como se pretende medir o potencial de aplicabilidade do *blockchain* para melhorar a cadeia de custódia. No quarto, apresenta-se uma proposta para a criação de um modelo que possa demonstrar como o *Blockchain* poderia, efetivamente, apoiar os registros de identificação e rastreio dessas informações em relação ao ciclo de vida de uma evidência digital. No quinto, demonstram-se os cenários experimentais. No sexto, expõem-se os resultados obtidos ao experimentar a cadeia de custódia digital e a discussão que abrange a exploração do ponto de vista do domínio do problema. Por fim, no capítulo sétimo, apresentam-se as considerações finais e sugestões de trabalhos futuros.

2 CADEIA DE CUSTÓDIA E ALTERNATIVAS COMPUTACIONAIS

Apresenta-se, neste capítulo, o referencial teórico sobre legislação, cadeia de custódia e tecnologia *blockchain* para fundamentar este trabalho e permitir uma melhor compreensão do estudo. Inicialmente, abordam-se os conceitos básicos sobre as legislações de proteção de dados, sobre a cadeia de custódia no Brasil e sobre as tecnologias de *blockchain*. Posteriormente, apresentam-se os trabalhos correlacionados com o estudo. Por fim, relacionam-se estes à discussão proposta nesta dissertação.

2.1 GDPR

A legislação do Regulamento Geral de Proteção de Dados (GDPR) entrou em vigor em maio de 2018 em todos os países da União Europeia (UE). As disposições gerais do GDPR garantem que os dados pessoais somente possam ser coletados legalmente, sob condições específicas, para um propósito legítimo. Além disso, deve devolver o controle total aos proprietários dos dados (Kuner *et al.*, 2020).

O GDPR trouxe a proteção de dados em todos os estados membros da UE, com o objetivo de alcançar a proteção da liberdade, direitos e privacidade de qualquer indivíduo em relação ao armazenamento, uso ou exploração de dados pessoais e reduzir as barreiras entre empresas dentro da UE, além de permitir a livre circulação de dados em toda a União.

O GDPR aplica-se, automaticamente, a cada Estado-Membro sem a necessidade de complementação de legislação adicional. Ela retrata, claramente, o objetivo da UE de criar um Mercado Único Digital. Além disso, a UE procura alcançar um conjunto consistente e harmonizado de leis que devem ser usadas para proteger e regular a proteção de dados e o fluxo de dados nos países membros. Ressalta-se que a proteção de dados pessoais também se estende a organizações com sedes fora da UE, que monitoram ou visam cidadãos da UE para a venda de seus bens ou serviços (Kuner *et al.*, 2020).

2.1.1 Princípios gerais

Os princípios norteadores, garantidos pelo GDPR, são: Princípio da Licitude, Lealdade e Transparência, Princípio da Adequação e Limitação da Finalidade, Princípio da Necessidade ou Minimização, Princípio da Qualidade dos Dados ou Exatidão, Princípio da Limitação da Conservação, Princípio da Segurança, Integridade e Confidencialidade, Princípio da Prestação de Contas ou Responsabilização. Aplicam-se esses princípios, direta e independentemente de criação de lei, por parte dos estados membros, por meio da legislação em cada nação.

Esses princípios constavam na Diretiva 95/46, com exceção dos princípios da necessidade ou minimização e Princípio da Prestação de Contas ou Responsabilização. O primeiro prevê que os dados pessoais devem ser adequados, pertinentes e limitados em relação aos fins para os quais serão processados a fim de diminuir a quantidade de dados, coletando, apenas, aqueles que sejam essenciais para o produto ou serviço ofertado. O segundo exige que as organizações implementem medidas técnicas e organizacionais apropriadas, e sejam capazes de prestar contas e demonstrar sua eficácia, quando solicitadas. Para tal, instituiu-se o controlador de dados, profissional responsável por demonstrar que a organização está agindo em conformidade com os demais princípios estabelecidos pelo Regulamento (Alsenoy, 2016).

2.1.2 Direitos fundamentais do titular dos dados

O GDPR não fornece aos indivíduos propriedade sobre seus dados, mas o controle sobre o que acontecerá com eles, por exemplo: como serão armazenados, para que fim serão utilizados e com quem serão compartilhados. O titular dos dados tem o direito de obter informações do controlador de dados e saber se houve processamento de algum de seus dados pessoais. Em caso positivo, o titular terá o direito de acessar os dados armazenados e o direito de obter informações sobre o uso de seus dados, como o motivo pelo qual esses dados foram processados, as partes que receberam esses dados, o local onde estão armazenados e o período durante o qual esses dados devem ser ser armazenados. Essa disposição contempla a garantia para que os dados sejam coletados de maneira justa e transparente (Kuner *et al.*, 2020).

Os titulares dos dados têm, também, o direito de apagar os seus dados

pessoais imediatamente, em caso de a razão para o processamento não mais existir ou em retirada, por parte do titular, do seu consentimento, ainda que autorizado explicitamente ou em caso de processamento ilegal de dados. Os titulares dos dados também têm o direito de restringir o tratamento dos seus dados pelo responsável pelo tratamento em caso de alguma imprecisão no processamento. A cláusula de portabilidade de dados estipula que o titular dos dados tem o direito de obter os seus dados pessoais, que ele próprio submeteu previamente ao responsável pelo tratamento, e transmiti-los a outro responsável pelo tratamento da sua escolha. Essa disposição pode ser invocada em caso de o processamento ser baseado, principalmente, no consentimento dado (Alsenoy, 2016).

2.1.3 Funções do controlador de dados e processador de dados

A Diretiva de Proteção de Dados da UE que estava em vigor antes da promulgação do GDPR não reconhecia a privacidade desde o *design* como um direito humano fundamental, isso já era protegido pela Convenção Europeia de Direitos Humanos. Porém, o GDPR reconhece e protege esse direito fundamental que impede o acesso não autorizado aos dados pessoais dos titulares. O Regulamento atribui ao responsável pelo tratamento a responsabilidade de implementar medidas como encriptação, minimização de dados e anonimização. Utilizam-se esses métodos para reduzir os riscos de violações de dados (Alsenoy, 2016).

2.1.4 Privacidade dos dados

O GDPR exige que o controlador de dados

> implemente medidas técnicas e organizacionais apropriadas, como a pseudonimização, projetadas para implementar princípios de proteção de dados, como a minimização de dados, de maneira eficaz e para integrar as salvaguardas necessárias no processamento para cumprir os requisitos do presente regulamento e proteger os direitos dos titulares dos dados. (UE, 2018).

No entanto, isso não estabelece qualquer requisito absoluto para cumprir este artigo, pois o Regulamento não sugere que o desenvolvimento deva ocorrer dessa maneira. (Alsenoy, 2016).

2.2 LGPD

No Brasil, assegura-se a proteção de dados pessoais com base em algumas disposições diretas, mas também no dito "guarda-chuva"da privacidade (Europeia, 2019). A Lei Geral de Proteção de Dados (LGPD) surgiu para garantir o tratamento de dados pessoais. Nesse sentido, além dos dados simples, tem como missão proteger o direito de intimidade e vida privada, assegurando a privacidade relativa aos dados de origem racial, religiosa, opinião, saúde, vida sexual, entre outros (Nunes, 2019).

Regular o uso e o tratamento de dados pessoais constitui o principal objetivo das leis de proteção de dados que visam não somente à proteção da privacidade, mas também a outros direitos fundamentais e liberdades individuais, que somente podem ser exercidos na sua completude caso seja garantido o uso adequado dos dados pessoais que, muitas vezes, funcionam como representação do indivíduo. Dessa forma, as leis de proteção de dados constituem estruturas regulatórias que protegem outros direitos. A LGPD, que transplanta o sistema setorial de proteção nacional para um geral, abrange o tratamento de dados pessoais, independentemente do contexto, setor e mercado. Monteiro (2018) teve como objetivo analisar os mecanismos institucionais, preventivos e repressivos de proteção de dados pessoais previstos na LGPD sob a ótica da efetividade da lei em um ambiente digital.

A LGPD é reiteradamente exposta como um espelho relativo à proteção das pessoas físicas no que diz respeito ao tratamento dos dados pessoais e à livre circulação destes (Masseno *et al*., 2020).

2.2.1 Fundamentos e princípios da LGPD

Além das bases fundamentais, há a autodeterminação informativa e a livre iniciativa, pressupostos necessários para o desenvolvimento econômico e tecnológico da sociedade. Assim, para Santos e Silva (2019), os fundamentos previstos no artigo 2º seriam:

I. o respeito à privacidade;

> II. a autodeterminação informativa;
> III. a liberdade de expressão, de informação, de comunicação e de opinião;
> IV. a inviolabilidade da intimidade, da honra e da imagem;
> V. o desenvolvimento econômico e tecnológico e a inovação;
> VI. a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Lei n. 13709, 2018).

Com relação aos princípios (Monteiro, 2018) esclarece que, ao incluir 10 princípios gerais de proteção de dados pessoais, a Lei garante aos titulares dos dados o direito à transparência, ou seja, o direito de obter "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". No mesmo sentido, em seu trabalho, Europeia (2019) destaca que foi reservado um artigo inteiro pelo legislador para indicar quais princípios devem reger a legislação. Além disso, descreve as definições adotadas, quais sejam:

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 das suas finalidades, com 7 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 dos 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; e

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, inclusive da eficácia das medidas.

2.2.2 Hipóteses legais para o tratamento de dados

A LGPD parte da ideia de que todo dado pessoal tem importância e valor, e que qualquer pessoa que trate dados, seja ela natural ou jurídica, de direito público ou privado, inclusive em atividade realizada nos meios digitais, deverá ter uma base legal para fundamentar os tratamentos de dados pessoais que realizar (Teffé; Viola, 2020).

A LGPD procura estabelecer limites mais rígidos ao tratamento de dados, esclarecendo, entre outros, seu escopo de aplicação, as circunstâncias que legitimam o tratamento de dados, as definições dos termos técnicos, os princípios que regem as operações de dados pessoais, os direitos que possuem os titulares de dados e a responsabilidade dos agentes de tratamento. Além disso, o diploma legal trata também do tratamento de dados sensíveis, da transferência internacional de dados, das medidas de segurança de informação que devem ser adotadas pelos agentes de tratamento e, ao fim, estabelece as sanções aplicáveis para os casos de descumprimento das suas disposições (Souza *et al.*, 2019).

2.2.3 O direito ao esquecimento

As liberdades de informação e expressão, quando comparadas aos direitos da personalidade, abrangem o direito ao esquecimento. Ressalta-se essa perspectiva pelas liberdades de expressão e informação reconhecidas em documentos internacionais, como a Declaração Universal dos Direitos Humanos e a Convenção Americana de Direitos Humanos, representando progressos democráticos significativos. A revolução tecnológica, especialmente a internet, amplificou essas liberdades, permitindo que indivíduos se comuniquem globalmente e troquem

informações em tempo real, mas também gerou desafios quanto à proteção da privacidade (Silva; Carvalho, 2017).

O direito ao esquecimento é um desdobramento dos direitos da personalidade, surge como uma resposta às potenciais violações decorrentes da perpetuação de informações pessoais na internet. Ele concede às pessoas o direito de requerer a remoção ou limitação da divulgação de informações passadas que possam prejudicar sua dignidade ou integridade. Entretanto, sua aplicação enfrenta o dilema da colisão com as liberdades de expressão e informação, uma vez que a censura prévia é contrária à essência democrática (Silva; Carvalho, 2017). Isso levanta questões sobre como equilibrar esses interesses concorrentes.

Adota-se o critério da ponderação de princípios para resolver essa colisão. Este envolve a análise concreta dos valores e interesses em jogo, buscando preservar tanto a liberdade de expressão quanto os direitos da personalidade. A doutrina apresenta critérios para orientar essa ponderação, como a preservação do contexto original da informação, a utilidade pública da informação, o caráter público dos fatos e a preservação dos direitos da personalidade na recordação (Martinez, 2014).

Ainda para Martinez (2014), a discussão sobre o direito ao esquecimento também se estende à legislação de proteção de dados, principalmente em jurisdições como a União Europeia. A GDPR introduziu o "direito de ser esquecido", permitindo que indivíduos solicitem a remoção de seus dados pessoais em certas situações, e consequentemente herdado pela legislação brasileira. No entanto, essa implementação enfrenta desafios, como a definição de critérios claros para determinar quando o direito deve ser aplicado. A questão do direito ao esquecimento reflete o equilíbrio delicado entre a proteção da privacidade e a promoção das liberdades fundamentais na sociedade da informação. A abordagem da ponderação de princípios fornece um método para enfrentar esses conflitos, garantindo que tanto a liberdade de expressão quanto os direitos da personalidade sejam respeitados. Contudo, sua aplicação eficaz depende de uma análise cuidadosa das circunstâncias específicas de cada caso, considerando os valores em jogo e as implicações mais amplas para a sociedade.

2.2.4 Um comparativo entre GDPR *VERSUS* LGPD

Em sua pesquisa, Europeia (2019) explica que houve uma comparação

principiológica entre o GPDR e a LGPD, em que se nota a intenção do legislador brasileiro em estabelecer princípios amplos, alinhando-se ao GDPR, à medida que espelha os princípios de adequação e limitação da finalidade, necessidade, qualidade e *accountability*.

É importante reconhecer que a referida lei recebeu uma forte influência do direito comunitário europeu, desde a Diretiva de Proteção de Dados de 1995 até o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em vigor a partir de maio de 2018. No que diz respeito ao tratamento de dados sensíveis, a LGPD conceituou, de forma semelhante, senão idêntica, ao GDPR, o conceito de dados pessoais sensíveis, sendo certo que a lei brasileira é bastante inspirada no regulamento europeu (Mulholland, 2018).

A LGPD complementa, harmoniza e unifica um ecossistema de mais de quarenta normas setoriais que regulam, de forma direta e indireta, a proteção da privacidade e dos dados pessoais no Brasil. Foi inspirada nas discussões que culminaram na GDPR europeia e tem por objetivo não somente conferir às pessoas maior controle sobre seus dados, mas também fomentar um ambiente de desenvolvimento econômico e tecnológico, mediante regras flexíveis e adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais (Monteiro, 2018).

2.3 CADEIA DE CUSTÓDIA

É fundamental entender o conceito dado à cadeia de custódia da prova. Primeiramente, ressalta-se que o processo penal condenatório constitui um processo probatório, ou seja, a força da prova e sua qualidade devem ser tão elevadas ao ponto de acabar com quaisquer dúvidas sobre a materialidade e a autoria do crime, indo ao encontro do que preconiza um estado de direito (Prado, 2019). A cadeia de custódia é composta de elos, que dizem respeito a um vestígio que, por sua vez, eventualmente, será considerado uma prova. Um elo é qualquer pessoa que tenha manejado esse vestígio. É dever do Estado — e, também, direito do acusado — identificar, de maneira coerente e concreta, cada elo, desde o momento da descoberta do vestígio (Edinger, 2016).

No Brasil, aprovou-se a Lei n. 13.964/2019, que alterou diversos dispositivos legais. Entre eles, destaca-se o Código de Processo Penal (Decreto-Lei n.

3.689/1941), cujos arts. 158-A a 158-F, inseridos no capítulo relativo ao exame de corpo de delito, cadeia de custódia e perícias, são de especial interesse para este estudo. Dentre as inovações trazidas, destaca-se a inserção da Teoria da Cadeia de Custódia da prova no Código Processual Penal Brasileiro, o que acarretou uma grande evolução para a qualidade e credibilidade da prova (Junior; Rosa, 2015).

Nas palavras de Cunha (2020), a sistematização de procedimentos dispostos na nova legislação objetiva a preservação do valor probatório da prova pericial caracterizada, mais precisamente, da sua autenticidade.

O art. 158-B da Lei n. 13.964/2019, por sua vez, definiu que a cadeia de custódia equivale ao rastreamento do vestígio em dez seguintes etapas:

I. **reconhecimento:** ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;

II. **isolamento:** ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;

III. **fixação:** descrição detalhada do vestígio conforme o local de crime ou o corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;

IV. **coleta:** ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;

V. **acondicionamento:** procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;

VI. **transporte:** ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;

VII. **recebimento:** ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;

VIII. **processamento:** exame pericial em si, manipulação do vestígio de acordo

com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;

IX. **armazenamento:** procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;

X. **descarte:** procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

Ressalta-se que, para Matida *et al.* (2020), mesmo com a evolução recente, a legislação pátria não cuidou de assuntos como o momento processual adequado para se fazer o exame da regularidade ou irregularidade da cadeia de custódia. Da mesma forma, isso também se aplica às consequências que surgem em decorrência de provas manipuladas indevidamente, ou seja, quando a cadeia de custódia não é devidamente observada. Aliás, acerca dessa temática, a dogmática penal diverge-se entre os que entendem que a consequência da ruptura da cadeia de custódia deva ser, necessariamente, a exclusão da prova maculada, e os que defendem ser o juiz o responsável por sopesar a prova custodiada irregularmente conforme o caso concreto.

2.3.1 Vestígio digital, indício digital e a evidência digital

Os vestígios são os elementos remanescentes de eventos passados, podendo ser físicos ou lógicos. Eles servem como pontos de partida para investigações mais profundas. Vestígios não físicos ou lógicos podem incluir lendas, tradições orais ou memórias culturais transmitidas ao longo do tempo, bem como o registro destes em arquivos digitais em dispositivos eletrônicos (Velho *et al.*, 2016).

Indícios, por outro lado, constituem pistas ou sinais que sugerem a possibilidade de algo ter ocorrido. Eles são frequentemente usados em investigações para direcionar a atenção e conduzir pesquisas mais aprofundadas. Na ciência, indícios podem ser dados que apontam para uma possível relação causal entre variáveis, mas não estabelecem uma prova definitiva. Em investigações criminais, um indício pode ser uma testemunha que fornece informações suspeitas, mas sem evidências sólidas de apoio (Velho *et al.*, 2016).

Evidências, por sua vez, são informações, dados ou objetos que fornecem

um suporte sólido para uma conclusão ou afirmação. Elas são cruciais para estabelecer a verdade de forma convincente. Em pesquisa científica, evidências podem ser resultados de experimentos rigorosos e repetíveis que confirmam teorias. Em um tribunal de justiça, evidências podem ser documentos, análises de DNA ou testemunhos periciais que estabelecem, com um elevado grau de certeza, a culpa ou inocência de um acusado (Velho *et al.*, 2016).

2.3.2 Evidência para a forense digital

Em um processo judicial, utiliza-se uma evidência para demonstrar a verdade de um fato e, como consequência, muitas vezes, estes afetam o resultado do caso. As práticas modernas do Direito Processual conferem à autoridade judicial independência nas questões relativas à admissão de provas, tendo como limite que essa discricionariedade deve ser compatível com os princípios básicos do direito, equidade, racionalidade, razoabilidade e eficiência. A produção de provas em ambientes cibernéticos é uma atividade complexa, por isso consideram-se estas essenciais e aceitas como válidas em juízo. A produção de provas em ambientes digitais é uma atividade complexa, por isso é essencial que essas provas sejam aceitas como válidas em juízo somente se a cadeia de custódia puder assegurar, exatamente, qual foi a prova, por que foi coletada e analisada e como se identificaram os dados probatórios, coletados, analisados e relatados. Além disso, a cadeia de custódia deve demonstrar, exatamente, onde, quando e quem entrou em contato com as provas eletrônicas em cada etapa da investigação e qualquer manipulação das provas (Giova *et al.*, 2011).

Nesse sentido, conforme mencionado por Giova *et al.* (2011), a crescente complexidade da ciência forense, na área digital, leva pesquisadores a afirmarem que a computação forense tradicional “está à beira de um precipício”, especialmente pela grande diversidade de dispositivos eletrônicos dimensionados e pelo intenso crescimento da quantidade de dados que devem ser coletados e examinados durante uma investigação forense digital.

A Cadeia de Custódia para Forense Digital (CCFD) pode ser definida como um processo usado para manter e documentar a história cronológica do manuseio de evidências digitais. A CCFD desempenha um papel importante em qualquer investigação forense digital porque ela registra cada detalhe minucioso, referente à

evidência digital, durante sua passagem por diferentes níveis de hierarquia, ou seja, desde o primeiro correspondente até as autoridades superiores que lidam com a investigação de crimes cibernéticos. A CCDF também registra as informações como as evidências foram Identificadas, coletadas, analisadas e preservadas para produção, quando, onde e quem entrou em contato com as evidências. No entanto, a CDFD é suscetível ao comprometimento se a documentação não for devidamente mantida e preservada durante o ciclo de vida da evidência digital, tornando inadmissível, em juízo, a comprovação de qualquer fato relacionado ao crime cibernético. Assim, é extremamente importante preservar a integridade da CDFD para que a evidência seja admitida no processo judicial (Lone; Mir, 2019b).

2.4 *BLOCKCHAIN*

Uma *blockchain* é uma tecnologia baseada em contabilidade distribuída em forma de um livro razão, é um software que permite o acesso a dados por vários usuários de vários nós ou computadores (Finck, 2018). Os dados são criptografados por meio de processo de *hash* e armazenados nos blocos de dados. Todos os blocos são vinculados de maneira cronológica pelo livro-razão e constroem uma cadeia (Shah *et al.*, 2019). Cada vez que uma nova transação é feita no *blockchain*, uma cópia do livro é atualizada, simultaneamente, na rede ponto a ponto. Isso garante a consistência em todo o sistema e é um dos benefícios de segurança da tecnologia. Se um agente mal-intencionado tentar editar o registro distribuído armazenado em um nó, o registro não corresponderia ao registro mantido nos nós restantes da rede e seria rejeitado (Bartlett, 2021).

Esta é uma das tecnologias mais requisitadas dos últimos anos (Shah *et al.*, 2019), e tem um elevado potencial de desenvolvimento que levanta muitas questões. Além disso, é uma tecnologia na qual o processamento de dados pessoais pode depender, mas não é uma operação de processamento de dados com finalidade própria (Finck, 2018).

2.4.1 Modelos de *blockchain*

A diferença entre um *blockchain* privado e público é que o privado pode ser controlado por um único indivíduo, entidade ou consórcio que determina a base de

usuários (Bartlett, 2021). Não está aberto para qualquer participante disposto a participar, mas é restrito àqueles que o administrador do *blockchain* deseja convidar; Já um *blockchain* público está aberto ao público para participar de validação das transações (Manteghi, 2021).

O modelo público significa que é acessível a todas as pessoas. Todos podem se tornar um dos nós e fazer contribuições para obter as recompensas seguindo as regras. Não há relações de confiança entre os nós. Ele é completamente aberto e descentralizado. Todas as transações no *blockchain* público nunca podem ser alteradas ou revogadas. O modelo privado significa que o proprietário do *blockchain* tem a mais alta autoridade para alterar as informações. O restante dos nós tem acesso limitado para leitura. Comparado ao *blockchain* público, o *blockchain* privado tem características de fácil modificação e baixo custo de transação. A verificação de transações do modelo privado somente precisa de alguns nós de alto crédito designados. A *blockchain* privada é aplicada a redes mais fechadas (Mingxiao *et al.*, 2017).

Para o modelo privado, significa que o proprietário do *blockchain* tem a mais alta autoridade para alterar as informações. O restante dos nós tem acesso limitado para leitura. Comparado com o modelo público, o *blockchain* privado tem características de fácil modificação e baixo custo de transação. A verificação de transações do *blockchain* privado somente precisa de alguns nós de alto crédito designados. A *blockchain* privada é aplicada a redes mais fechadas, como a intranet. É mais importante resolver as falhas de colisão do que as falhas de algum membro da rede enviando informações inconsistentes a outros sobre transações (Mingxiao *et al.*, 2017).

Blockchain com permissão significa que a rede é composta por muitas partes e os nós principais são pré-especificados pelos participantes. Os membros do *blockchain* autorizado não confiam totalmente uns nos outros. Cada participante seleciona seu próprio nó de consenso de acordo com as regras. As transações precisam ser reconhecidas pela maioria dos nós de consenso. O grau de abertura e centralização do consórcio ocorre entre a *blockchain* pública e privada. O *blockchain* autorizado é adequado para a rede semifechada, construída por diferentes empresas (Mingxiao *et al.*, 2017).

2.4.2 Algoritmos de consenso

Um dos elementos centrais da tecnologia *blockchain* é um mecanismo de consenso que, geralmente, requer a verificação da legitimidade de cada transação pelos usuários e sua concordância para que ocorra aquela transação. Além disso, há uma diferenciação entre *blockchains* públicos sem permissão e privados com permissão

As *blockchains* públicas permitem a participação de qualquer pessoa e de vários nós, aplicando um mecanismo de consenso. As *blockchains* privadas, geralmente, restringem o acesso a dados e locais de armazenamento envolvendo, apenas, pequenos grupos de participantes (Finck, 2018).

O consenso é um conceito central em sistemas distribuídos e não está restrito ao *blockchain*, aplica-se a cenários em que vários processos ou nós precisam manter um estado comum de item de dados em modelos de *blockchain* sem permissão, os nós são anônimos, um novo bloco de transação adulterado pode ser adicionado resultando em uma bifurcação, isso ocorre quando uma transação válida não combina com a inválida (Chaudhry; Yousaf, 2018). O objetivo principal do algoritmo de consenso é alcançar um acordo entre os nós, de tal forma que cada nó concorde com um valor verdadeiro. No *blockchain* com permissão, os nós não são anônimos e considerados como entidades conhecidas. O consenso, ainda, é importante nesse caso, pois os nós não são confiáveis. É importante considerar o consenso em que os nós de uma rede estão com defeito ou se comunicam de maneira não confiável. O consenso é alcançado em sistemas distribuídos em relação a algumas falhas (Kraft, 2016).

A corrente de blocos da tecnologia possui propriedades que provam os benefícios às aplicações e sistemas baseados nela. As principais propriedades da corrente de blocos, segundo Zheng *et al.* (2018) são:

I. **descentralização:** as correntes de blocos executam de maneira distribuída, através do estabelecimento de consenso entre todos os participantes da rede. Não há uma entidade centralizadora;

II. **desintermediação:** a corrente de blocos elimina a necessidade de um intermediário confiável para a troca de ativos. Os ativos podem ser trocados diretamente pela rede e a confiança é estabelecida através de consenso;

III. **imutabilidade:** os dados armazenados em uma corrente de blocos são imutáveis. Não é possível modificar ou recriar qualquer dado incluído na corrente de

blocos de forma retroativa. Toda atualização na corrente de blocos é realizada de forma incremental;

IV. **irrefutabilidade:** os dados são armazenados na corrente de blocos em forma de transações assinadas, que não podem ser alteradas devido à propriedade de imutabilidade da corrente de blocos. Portanto, o emissor de uma transação jamais pode negar sua existência;

V. **transparência:** todos os dados armazenados na corrente de bloco são acessíveis por todos os participantes da rede. Em correntes de blocos públicas, como o Bitcoin e o Ethereum, as transações são abertas para qualquer usuário com acesso à Internet;

VI. **auditabilidade:** como consequência da transparência, todo participante pode verificar, auditar e rastrear os dados inseridos na corrente de blocos para encontrar possíveis erros ou comportamentos maliciosos. No caso de correntes de blocos federadas, o processo de auditagem pode responsabilizar um malfeitor na rede;

VII. **disponibilidade:** as correntes de blocos são estruturas replicadas em cada participante da rede e, portanto, a disponibilidade do sistema é garantida mesmo sob falhas, devido à redundância de informações;

VIII. **anonimidade:** os usuários e nós mineradores de uma corrente de blocos são identificados por chaves públicas ou identificadores únicos que preservam suas identidades. Ainda, é possível utilizar uma chave pública em cada transação, evitando a rastreabilidade do usuário e conferindo um grau a mais de anonimidade.

Entre os algoritmos de consenso, o de prova de trabalho, de prova de participação e de prova de capacidade são escolhas comuns na atualidade (Mingxiao *et al.*, 2017).

- **Prova de trabalho** (*PoW – Proof-of-Work*): sua ideia central é alocar os direitos contábeis e recompensas por meio da competição de poder de hashing entre os nós. Com base nas informações do bloco anterior, os diferentes nós calculam a solução específica de um problema matemático. É difícil resolver o problema de matemática. O primeiro nó que resolve esse problema matemático pode criar o próximo bloco e obter uma certa quantidade de recompensa em bitcoin (Mingxiao *et al.*, 2017).
- **Prova de participação** (*PoS – Proof-of-Stake*): o criador de um novo bloco na rede é eleito deterministicamente dependendo de sua riqueza (participação). Não há recompensa associada à mineração ou geração de blocos. É mais econômico, pois os mineradores não precisam competir para abordar a solução matemática primeiro

(Chaudhry; Yousaf, 2018).

• **Prova de autoridade** (*PoA – Proof-of-Authority*): esse protocolo visa alcançar um consórcio por meio de nós ou validadores autorizados. Os validadores são restritos a um conjunto fixo de "n" nós autorizados, chamados participantes. O mecanismo de aceitação e validação de novos blocos na rede depende da configuração da respectiva rede *blockchain*. Nesse protocolo, a reputação do participante é crucial, tornando, assim, o comportamento malicioso muito prejudicial à reputação da entidade (Toyoda *et al.*, 2020).

Em seu trabalho, Baars (2016) fez uma comparação dos três principais algoritmos relacionados à velocidade, consumo de energia, segurança, maturidade e custo, conforme O Quadro 1.

Quadro 1 – Quadro de comparação de algoritmos de consensos

[Medidas]	[PoW]	[PoS]	[PoA]
Velocidade	Lento	Médio	Rápido
Consumo de energia	Ineficiente	Eficiênte	Eficiênte
Segurança	Sem Permissão, Não Confiável	Sem Permissão, Não Confiável	Permissionado, Confiável
Maturidade	Testado	Não Testado	Seguro
Custo	Dispendioso	Baixo custo	Sem Custo

Fonte: BAARS (2016).

2.4.3 Contratos inteligentes

O termo “contrato inteligente” propõe a tradução das cláusulas de um contrato para código, integrando-as em *software* ou *hardware* para torná-las autoexecutadas, a fim de minimizar o custo de contratação entre as partes transacionais e evitar exceções acidentais ou ações maliciosas durante a execução do contrato. Atualmente, pessoas de diferentes áreas utilizam o termo “contrato inteligente” de maneiras diferentes. Alguns se referiam a “contrato inteligente” como um contrato legal que poderia ser representado por *software*. Outros tomaram “contrato inteligente” como *scripts* de códigos projetados para executar certas tarefas uma vez que as condições pré-definidas sejam atendidas (Zou *et al.*, 2019).

Em seu trabalho, Clack *et al.* (2016) propuseram uma ampla definição de

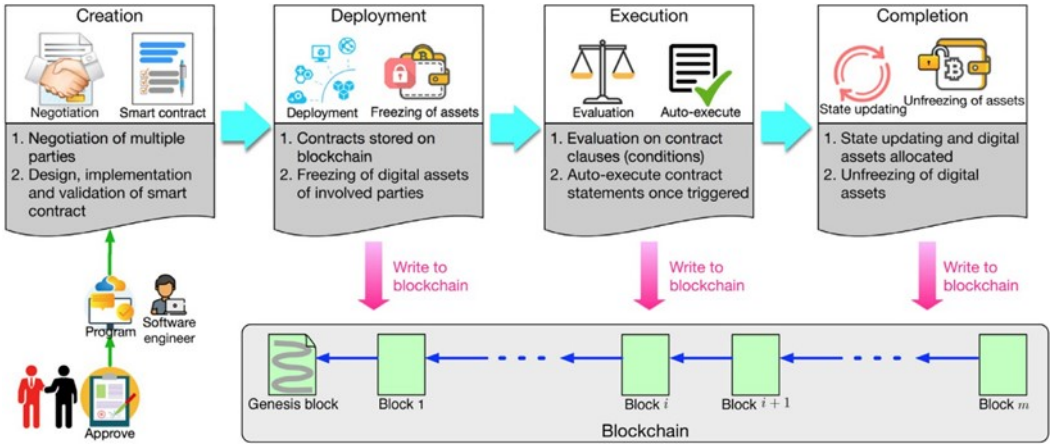
contrato inteligente. Eles definiram um contrato inteligente como um acordo automatizável e executável. Automatizável por computador, embora algumas partes possam exigir entrada e controle humano. Exequível por meio de aplicação legal de direitos e obrigações ou por meio de execução inviolável de código de computador.

Os contratos inteligentes garantem controle adequado a aplicação das cláusulas contratatuais. Eles são validados e podem então ser implantados em plataformas sobre *blockchains*. Os contratos armazenados nas *blockchains* não podem ser modificados devido à imutabilidade das cadeias de blocos. Qualquer emenda exige a criação de um novo contrato. Depois que os contratos inteligentes são implantados em *blockchains*, todas as partes podem acessar os contratos por meio dos *blockchains*. Além disso, os ativos digitais, de ambas as partes envolvidas no contrato inteligente, são bloqueados por meio do congelamento das carteiras digitais correspondentes. Após a implantação dos contratos inteligentes, as cláusulas contratuais foram monitoradas e avaliadas. Uma vez alcançadas as condições contratuais, os procedimentos contratuais serão executados automaticamente. Vale a pena ressaltar que um contrato inteligente consiste em uma série de declarações com conexões lógicas. Quando uma condição é acionada, a instrução correspondente será executada automaticamente, consequentemente uma transação sendo executada e validada pelos mantenedores na rede, a conclusão de contrato inteligente acontece quando as ações contratuais são realizadas e os ativos digitais das partes envolvidas são desbloqueados. Dessa forma, o contrato completou todo o ciclo de vida (Kolvart *et al.*, 2016).

A execução de cada declaração de contrato é registrada como uma transação imutável armazenada no *blockchain*. Os contratos inteligentes garantem o controle de acesso adequado e a execução do contrato. Em particular, os projetos podem atribuir permissão de acesso para cada função do contrato uma vez que qualquer condição em um contrato inteligente for satisfeita, a instrução acionada executará, automaticamente, a função correspondente de maneira previsível (Zheng *et al.*, 2020).

Na figura 1, demonstra-se uma referência sobre o ciclo de vida de um contrato inteligente, que consiste em quatro fases principais: criação, implantação, execução e conclusão.

Figura 1 – ciclo de vida do contrato Inteligente



Fonte: Zheng *et al.* (2020).

Conforme Zheng *et al.* (2020), representam-se as quatro fases da seguinte forma:

• **Criação de contratos inteligentes** – o processo de criação de contratos inteligentes envolve várias etapas. A primeira refere-se a como as partes envolvidas negociam os detalhes do contrato, como obrigações, direitos e proibições. Após várias rodadas de discussões, alcança-se um acordo, e advogados ou conselheiros auxiliam a redação do contrato inicial. Em seguida, engenheiros de *software* transformam esse contrato escrito em linguagem natural em um contrato inteligente, codificado em linguagens de programação de computador, incluindo linguagens declarativas e baseadas em regras lógicas. Destaca-se que a criação de contratos inteligentes é um processo iterativo, envolvendo múltiplas rodadas de negociações e ajustes. Diferentes partes interessadas, como advogados de defesa e acusação e os tribunais, estão envolvidas nesse processo.

• **Implantação de contratos inteligentes** – a implantação de contratos inteligentes envolve a validação e a inserção desses contratos em plataformas baseadas em *blockchains*. Uma vez armazenados na *blockchain*, esses contratos não podem ser alterados devido à natureza imutável da tecnologia. Qualquer mudança requer a criação de um novo contrato. Após a implantação, as partes têm acesso aos contratos por meio das *blockchains*. Além disso, os ativos digitais das partes envolvidas são congelados. As partes podem ser identificadas por meio de suas credenciais.

• **Execução de contratos inteligentes** – após a implantação dos contratos inteligentes, monitoram e avaliaram-se as cláusulas contratuais. Uma vez alcançadas as condições contratuais, as cláusulas contratuais serão executadas

automaticamente. Ressalta-se que um contrato inteligente consiste em várias declarações interconectadas logicamente. Quando se aciona uma condição, executa-se a instrução correspondente automaticamente. Consequentemente, executa e valida-se uma transação pelos validadores nas *blockchains*. Então, registram-se nas *blockchains* as transações confirmadas e, posteriormente, registram-se os estados atualizados.

• **Conclusão de contratos inteligentes** – a conclusão dos contratos inteligentes resulta na atualização dos estados de todas as partes participantes. Registram-se essas mudanças nas *blockchains*, juntamente com as transações ocorridas durante a execução do contrato. Isso leva ao desbloqueio dos ativos digitais das partes envolvidas, marcando o completo ciclo de vida do contrato inteligente.

Ressalta-se que a apresentação das fases descritas por Zheng *et al.* (2020) descreve um cenário básico que pode ser parametrizado com as tecnologias e algoritmos adequados para a realização da proposta desta pesquisa. No capítulo 4, detalha-se a utilização de todos os componentes envolvidos.

2.4.4 Armazenamento dos dados

Conforme já mencionado no capítulo 1, não serão abordados, nesta dissertação, os estudos mais aprofundados sobre o armazenamento, porém necessita-se estudar as formas de armazenamento, considerando a excepcionalidade legislativa conforme 2.2, referente, especificamente, ao tópico de direito ao esquecimento.

O armazenamento das informações é um desafio para a proposta tendo em vista a propriedade de imutabilidade da tecnologia e, como solução, realiza-se uma combinação com sistemas de armazenamento existentes (POP *et al.*, 2019). Essa estratégia, denominada "off-chain", possibilita o armazenamento em banco de dados fora da *blockchain* sem sacrificar características fundamentais dos dados (Shukla; Samet, 2020).

O armazenamento de uma *blockchain* pode ser considerado como um livro público em que cada bloco contém registros de algumas transações. A *blockchain* não é armazenada em um único local, mas em uma rede de nós, em que cada nó da rede possui uma cópia dessa *blockchain*. Isso significa que todos os registros são públicos e facilmente verificáveis. Uma vez que um bloco é anexado ao *blockchain*, é

extremamente difícil modificar as transações do bloco sem alcançar o consenso de todos os nós; esse armazenamento é chamado de On-Chain (Zou *et al.*, 2019).

Armazenamento *Off-Chain* tem sido uma nova área de pesquisa observada em *blockchains* que têm potencial para aumentar a escalabilidade e privacidade do sistema. O *off-chain* consiste em terceirizar o armazenamento de dados (não o livro-razão) e os cálculos para um subsistema confiável de terceiros sem sacrificar a essência fundamental dos *blockchains*, ou seja, imutabilidade e disponibilidade de dados. Essa pesquisa é especialmente relevante para *blockchains* públicos, pois avalia e executa as transações processadas no sistema em todos os nós da rede, levando a uma menor taxa de transferência. E, no que diz respeito aos dados específicos do usuário, mantê-los disponíveis em todos os nós do sistema não implica a privacidade destes. Nesses casos, o armazenamento *Off-chain* tem recursos para eliminar as limitações (Shukla; Samet, 2020).

A tecnologia *blockchain* permite que duas partes não confiáveis façam transações com segurança sem a participação de um terceiro confiável. Isso torna as tarefas de manutenção de registros mais confiáveis. Devido à natureza da tecnologia *blockchain*, contratos inteligentes implantados em *blockchains*, ou seja, contratos inteligentes que utilizam a abordagem *on-chain*, geralmente, precisam ser executados e validados por cada nó, com todas as transações relevantes visíveis para toda a rede *blockchain*. Isso reduz a privacidade dos contratos inteligentes (Zou *et al.*, 2019). Além disso, para contratos inteligentes, especialmente aqueles com computação complexa, o custo da transação pode ser elevado e a validação de transações relevantes pode levar muito tempo, devido à execução replicada de contratos inteligentes entre nós. Uma alternativa para esses problemas refere-se à concepção de contrato inteligente "*offchain*"proposta (Eberhardt; Tai, 2017).

Executam-se os contratos inteligentes fora da cadeia do *blockchain*. Ao contrário dos contratos inteligentes *on-chain*, um contrato inteligente *off-chain* somente precisa ser assinado e executado pelos participantes interessados. Conforme proposto por Eberhardt; Tai, 2017), um contrato inteligente *off-chain*, geralmente, é projetado para encapsular funções envolvendo computação de alto custo ou informações privadas sobre os participantes; enquanto um contrato inteligente *on-chain* é sugerido para realizar algumas tarefas de baixo custo e não confidenciais. Para preservar as propriedades e benefícios de uma *blockchain*, na prática, os resultados de contratos inteligentes fora da cadeia devem ser registrados

na cadeia (Zou *et al.*, 2019).

Neste trabalho utiliza-se uma estratégia de utilização híbrida de armazenamento para atender aos requisitos legais de direito ao esquecimento, bem como os trâmites judiciais protegidos por sigilo processual. No capítulo 4, detalha-se o funcionamento do armazenamento.

2.5 CONEXÕES CONCEITUAIS

Constituem um confronto de conceitos para oferecer uma visão abrangente e detalhada das interações e influências mútuas entre os conceitos de Cadeia de Custódia, LGPD e Tecnologia *Blockchain*. No quadro 2, que compara a Cadeia de Custódia com a LGPD, evidencia-se que a proteção dos dados pessoais e a integridade das evidências estão intrinsecamente relacionadas.

Quadro 2 – quadro de conceitos Cadeia de Custódia *versus* LGPD

Cadeia de Custódia	LGPD (Legislação de Proteção de Dados)
Coleta	Finalidade, Adequação, Necessidade, Qualidade dos Dados

Fonte: próprio Autor.

O isolamento adequado de uma evidência, por exemplo, está em sintonia com os princípios de segurança e prestação de contas da LGPD. Da mesma forma, a coleta de dados pessoais deve seguir padrões de qualidade, alinhando-se às demandas de adequação e finalidade da legislação. A segurança aplicada às evidências também reflete a necessidade de proteger informações sensíveis, estabelecendo uma conexão com a legislação.

Ressalta-se que a etapa de coleta se torna o melhor ponto de entrada para realizar os processos de registros e rastreamento, tendo em vista que oferece mais conexões entre os conceitos.

Conexão da cadeia de custódia e LGPD

Como discutido, a definição precisa das finalidades da coleta de dados na cadeia de custódia de evidências cibernéticas não apenas é uma exigência legal, mas também uma garantia fundamental dos direitos dos indivíduos envolvidos. Os titulares dos dados têm o direito de saber por que suas informações estão sendo coletadas e

como serão usadas. Isso reforça a transparência, outro princípio da LGPD. A Finalidade dos Dados, um dos princípios fundamentais da LGPD no Brasil, tem um papel relevante para a coleta de dados da cadeia de custódia de evidências digitais. A LGPD estabelece que a coleta e o processamento de informações pessoais devem ter propósitos específicos, legítimos e transparentes. Esse conceito se aplica, de forma significativa, no contexto das evidências cibernéticas. A coleta de dados, na cadeia de custódia, envolve a obtenção, preservação das informações digitais que são vitais para uma investigação bem-sucedida em processos judiciais. Nesse contexto, a finalidade dos dados é crucial. A LGPD exige que os dados pessoais sejam coletados para finalidades legítimas e claramente definidas. Isso significa que terá suporte para apoiar um processo legal.

O Princípio da Finalidade, conforme definido pela LGPD, desempenha um papel fundamental no que diz respeito à coleta de dados na cadeia de custódia de evidências digitais. Ele contribui para assegurar que as informações digitais sejam adquiridas e empregadas de maneira legítima e transparente, respeitando os direitos dos indivíduos envolvidos e contribuindo para a integridade das investigações e processos legais, sem comprometer a privacidade das partes interessadas (Masseno *et al.*, 2020).

A adequação dos dados, como prevista na LGPD, em vigor no Brasil, estabelece requisitos estritos para apoiar que a coleta e o tratamento de dados pessoais ocorra de maneira apropriada, ética e legal, e essa adequação se estende ao contexto das evidências digitais. A adequação dos dados significa que a coleta na cadeia de custódia e o uso dessas informações devem estar em conformidade com a lei e com as finalidades legítimas da investigação. A LGPD exige que haja uma base legal sólida para a coleta de dados pessoais, o que se aplica, igualmente, às evidências digitais. Ao coletar evidências digitais, é crucial informar os titulares dos dados sobre o motivo da coleta, a finalidade do processamento e seus direitos em relação aos dados pessoais envolvidos. A divulgação de informações claras é fundamental para que os indivíduos compreendam como suas informações estão sendo usadas no contexto de uma investigação cibernética.

A LGPD estabelece que apenas os dados estritamente necessários devem ser coletados e utilizados, evitando a coleta excessiva e desproporcional (Masseno *et al.*, 2020). Na cadeia de custódia de evidências digitais, isso significa que apenas os dados relevantes para a investigação devem ser obtidos, mantendo o foco nas

informações necessárias para esclarecer o caso. Outro ponto importante é a retenção adequada dos dados. As evidências devem ser mantidas pelo tempo necessário para cumprir as finalidades da investigação ou do processo legal, mas não podem ser retidas indefinidamente. Isso garante que os dados sejam usados apenas enquanto forem relevantes e necessários (Santos; Silva, 2019).

Conforme o Princípio da Adequação, a coleta e o tratamento desses dados deve ocorrer de maneira legal, ética e transparente, respeitando os direitos dos titulares dos dados. Isso é essencial para uma aplicação justa da lei e para a proteção dos direitos dos envolvidos em casos que envolvem evidências digitais (Santos; Silva, 2019).

A LGPD enfatiza a necessidade de base legal para a coleta de dados, inclusive na cadeia de custódia de evidências digitais. Os investigadores e peritos precisam ter uma base legal sólida para coletar esses dados, o que pode incluir: o cumprimento de obrigações legais ou a proteção de interesses legítimos. Quando evidências digitais são coletadas, os titulares dos dados devem ser informados sobre o motivo da coleta, a finalidade do processamento e seus direitos em relação aos dados pessoais envolvidos. A LGPD exige que apenas os dados estritamente necessários sejam coletados e utilizados, o que é relevante na cadeia de custódia, em que informações excessivas podem ser obtidas de forma ilegal (Europeia, 2019).

O Princípio da Necessidade é incontestável em relação à coleta de dados da cadeia de custódia de evidências digitais. Ela estabelece diretrizes rigorosas para apoiar a coleta de dados pessoais de forma legal e ética (Europeia, 2019).

Conexão da cadeia de custódia e princípios da *Bockchain*

Quando se trata da coleta de dados na cadeia de custódia de evidências cibernéticas, o Princípio da Qualidade dos Dados é de grande importância para a integridade e a eficácia de qualquer investigação ou processo legal. A LGPD demanda que os dados pessoais coletados sejam precisos e, sempre que possível, atualizados (Matida *et al.*, 2020). No contexto de evidências digitais, isso significa que as informações coletadas devem refletir a realidade de maneira precisa. A LGPD também estipula que os dados coletados devem ser protegidos contra acessos não autorizados e modificações não autorizadas, para que a informação permaneça inalterada ao longo do processo de investigação (Masseno *et al.*, 2020). Isso é especialmente relevante nas evidências digitais, em que a manipulação indevida dos dados pode comprometer a validade das provas. As informações coletadas na cadeia

de custódia devem estar diretamente relacionadas à investigação ou ao processo legal em questão, evitando a coleta de dados excessivos ou irrelevantes (Lone; Mir, 2019b).

O Princípio da Qualidade dos Dados assenta-se na precisão, integridade, relevância e transparência dos dados, contribuindo para a legitimidade das investigações digitais, a proteção dos direitos individuais e a segurança jurídica nos casos que envolvem evidências digitais (Matida *et al.*, 2020).

Quadro 3 – quadro de conceitos Cadeia de Custódia *versus Blockchain*

Cadeia de Custódia	Tecnologia *Blockchain*)
Coleta	Imutabilidade, Transparência, Segurança, Auditabilidade

Fonte: próprio Autor.

No quadro 3, relativo à Cadeia de Custódia e à Tecnologia *Blockchain*, observou-se como a imutabilidade e a transparência inerentes à *blockchain* se alinham, perfeitamente, aos requisitos de rastreabilidade e integridade da cadeia de custódia. A capacidade da *blockchain* de garantir a autenticidade das transações e a impossibilidade de alterações não autorizadas está em sintonia com a necessidade de manter a integridade das evidências ao longo do processo judicial. A transparência e a auditabilidade proporcionadas pela *blockchain* também têm paralelos com a necessidade de rastrear e documentar cada etapa da cadeia de custódia com mais precisão para a realização da coleta na cadeia de custódia.

A imutabilidade é um dos pilares da tecnologia *Blockchain*, o que significa que, uma vez que se registram os dados em um bloco, eles se tornam permanentes e inalteráveis. Isso é fundamental para a coleta de evidências digitais, em que a integridade e a autenticidade dos dados são essenciais para a validação das informações. Criou-se a tecnologia para não permitir a modificação ou para apagar registros de evidências, sem deixar o rastro, o que garante a preservação de informações críticas para investigações futuras (Shah *et al.*, 2019).

Os contratos inteligentes, por sua vez, desempenham um papel central na

coleta de evidências digitais, automatizando processos e garantindo a conformidade com os procedimentos estabelecidos. Por exemplo, um contrato inteligente pode ser usado para rastrear, automaticamente, a coleta das evidências, registrando cada passo do processo. Isso não apenas economiza tempo, mas também elimina erros humanos.

Ressalta-se que a imutabilidade da *blockchain* e os contratos inteligentes ajudam a resolver desafios comuns na coleta de evidências digitais, como a autenticação de dados e a preservação de sua integridade ao longo do tempo necessário ao processo judicial. Ao usar contratos inteligentes para automatizar a coleta e a rastreabilidade das evidências, as organizações e órgãos de justiça podem obter uma grande melhoria no processo das informações coletadas (Zheng *et al.*, 2020).

A transparência inerente à *blockchain* permite que todas as partes envolvidas em uma investigação tenham acesso a um registro público e imutável de evidências, o que é fundamental para a confiabilidade do processo. Ela desempenha um papel fundamental parav a validação das informações coletadas. Qualquer pessoa autorizada pode verificar a autenticidade de uma evidência e sua jornada desde o momento da coleta até o presente. Isso aumenta a confiança em todo o processo de coleta de evidências cibernéticas, especialmente em casos judiciais, em que a credibilidade das provas é crítica (Bartlett, 2021).

A transparência da *blockchain* e os contratos inteligentes ajudam a resolver problemas de confiabilidade nas investigações cibernéticas. As informações são registradas de forma imutável, conforme mencionado no tópico acima, tornando muito difícil a adulteração ou manipulação das evidências (ZOU *et al.*, 2019). Isso é vital para garantir que as evidências sejam aceitáveis em tribunal e que os direitos dos envolvidos sejam protegidos. Essa combinação simplifica e aprimora a coleta de dados da cadeia de custódia de evidências digitais. Ela oferece um sistema de registro confiável, que não apenas aumenta a confiança nas evidências, mas também torna o processo mais eficiente, economizando tempo e recursos. Os órgãos que adotarem essa abordagem estão melhor preparados para enfrentar os desafios em constante evolução do mundo digital (Bartlett, 2021).

Quadro 4 – quadro de conceitos LGPD *versus Blockchain*

LGPD (Legislação de Proteção de Dados)	Tecnologia *Blockchain*)
Finalidade	Transparência, Segurança, Auditabilidade
Adequação	Transparência, Segurança, Auditabilidade
Necessidade	Transparência, Segurança
Qualidade dos Dados	Imutabilidade, Segurança

Fonte: próprio autor.

Por fim, no quadro 4, compararam-se os princípios da LGPD com a Tecnologia *Blockchain*. Percebeu-se como a transparência e a segurança proporcionadas pela *blockchain* podem contribuir, diretamente, para o cumprimento dos princípios da legislação. A capacidade de melhorar a qualidade dos dados, prevenir discriminação e facilitar a responsabilização é fortalecida pela capacidade da *blockchain* de oferecer registros confiáveis e auditáveis. Destaca-se, também, a anonimidade proporcionada pela tecnologia *blockchain*.

Conexão da cadeia de custódia e LGPD

Analisada à luz dos princípios da finalidade estabelecidos pela LGPD, a transparência total pode entrar em conflito legal, o que exige que os dados pessoais sejam tratados com sigilo e apenas para fins específicos e legítimos (Matida *et al.*, 2020). Nesse sentido, surge o primeiro desafio: como equilibrar a transparência da *blockchain* com o requisito de finalidade da LGPD? Uma possível solução é a utilização de técnicas de anonimização e pseudonimização para proteger a identidade dos titulares de dados. Os contratos inteligentes podem ser programados de forma a garantir que apenas partes autorizadas acessem informações pessoais, respeitando a finalidade para a qual os dados foram coletados.

Os contratos inteligentes, por sua vez, desempenham um papel fundamental para a automatização de transações, para cumprir com a LGPD. É importante que os contratos sejam programados de maneira a incorporar cláusulas que respeitem os princípios de finalidade, minimização de dados e consentimento informado. A solução proposta neste trabalho também fornece uma trilha de auditoria completa, permitindo que os titulares de dados e os detentores dos dados tenham controle sobre como utilizam-se suas informações. Eles podem rastrear todas as transações relacionadas aos seus dados e verificar se estão sendo usados de acordo com os propósitos estabelecidos (Zheng *et al.*, 2020).

A segurança é um dos pilares da tecnologia *blockchain*, o uso de criptografia forte torna as redes altamente resistentes a fraudes e invasões. No entanto, a LGPD requer que o tratamento de dados pessoais seja limitado à finalidade para a qual foram coletados. Isso significa que os dados armazenados em uma *blockchain* devem ser usados, estritamente, para os propósitos originais de uma investigação digital. A criptografia permite que apenas partes autorizadas tenham acesso a informações sensíveis. Dessa forma, a integridade da *blockchain* é mantida, ao mesmo tempo que se cumpre a LGPD.

A respeito desse quesito, neste trabalho, o modelo escolhido tem um suporte extra no controle de acesso aos dados de armazenamento externo, devido ao direito de esquecimento da legislação brasileira.

Para realizar o confronto desses princípios, é fundamental implementar medidas de privacidade eficazes em uma *blockchain* que possibilite a conformidade com a LGPD. No qual incluem a utilização de técnicas de separação dos dados e metadados, de modo que os dados pessoais não sejam expostos para quem não tem permissão de acesso. Apenas as partes autorizadas devem ser capazes de acessar informações pessoais, melhorando a conformidade com a finalidade original da coleta de dados para os fins da investigação. Outro fator importante são os contratos inteligentes que podem também desempenhar um papel fundamental nesse processo. Eles podem ser programados para exigir a autorização explícita dos titulares de dados antes que qualquer informação pessoal seja acessada ou usada. Isso permite que os juízes, delegados ou tribunais mantenham o controle sobre como as informações são usadas, respeitando os princípios da LGPD.

A transparência da tecnologia *blockchain* e dos contratos inteligentes precisar ser compatível com os princípios da adequação da LGPD, desde que medidas apropriadas de controle de acessos e segurança sejam implementadas de forma adequada, usando, apenas, os dados necessários para os fins da investigação e autorizados e explícitos, obtendo consentimento quando necessário. A capacidade de modificação ou exclusão de informações pessoais deve ser implementada nos contratos inteligentes, para atender às solicitações dos titulares e detentores dos dados coletados para atender um requisito da LGPD.

Esses confrontos de conceitos, em particular, necessitam de muito cuidado na interpretação, pois é necessário implementar medidas de segurança eficazes que permitam a conformidade com a LGPD. A complexidade desses conceitos consiste

em entender que o dado adequado para uma pessoa pode não ser para outra. Uma abordagem consiste em criptografar os dados armazenados fora da *blockchain*. Isso auxilia a proteção da privacidade dos titulares e dos detentores de dados enquanto mantém a integridade da *blockchain*.

Para conciliar esses princípios, é importante que sejam observadas medidas que permitam a conformidade com a LGPD. Neste trabalho, utiliza-se abordagem que consiste na possibilidade de assegurar que o tratamento de dados pessoais sejam realizados de maneira compatível com as finalidades previamente estabelecidas em relação aos limites da investigação e de acordo com a legislação vigente. A tecnologia simplifica o processo de auditoria, uma vez que os dados são facilmente acessíveis e confiáveis para quem possui o devido acesso. Isso é fundamental para preservar a integridade do processo judicial.

O conceito relacionado ao Princípio da Necessidade enfatiza que os dados devem ser coletados apenas para finalidades específicas e legítimas, evitando a coleta excessiva de informações. Isso está diretamente relacionado à proteção da privacidade dos indivíduos, pois impede a coleta de dados desnecessários, reduzindo, assim, os riscos de vazamentos de outros dados. Por outro lado, o Princípio da Transparência exige que os órgãos informem, claramente, os titulares de dados sobre como seus dados serão usados. Isso envolve a comunicação transparente da finalidade da coleta. A solução apresentada nesta pesquisa revela que a tecnologia de blocos em cadeia melhora a transparência de dados e o Princípio da Necessidade na LGPD promove a compatibilidade das organizações com a legislação de proteção de dados.

As necessidades específicas e legítimas, quando associadas ao conceito de segurança promovido pela tecnologia, podem proporcionar muitos ganhos. Neste trabalho, apresentou-se, no capítulo 5, um experimento que mostra como a segurança pode ser tratada em um cenário utilizando a tecnologia *blockchain* e os contratos inteligentes para atender aos requisitos propostos de segurança, confiabilidade e a integridade das transações e dos acordos da LGPD.

Todas as transações registradas em um *blockchain* são visíveis para todos os participantes da rede. Isso significa que se registra qualquer alteração nos dados de forma transparente e este pode ser rastreada ao longo do tempo. Esses dois conceitos estão alinhados à LGPD e ao procedimento tecnológico. Porém, em relação aos desafios encontrados, a transparência não pode ultrapassar o limiar da

legislação que impede outros tipos de direitos individuais já conquistados. Então, neste trabalho, utilizaram-se outras tecnologias associadas para resolver problemas específicos e conseguir a melhor proposta possível para a solução dos problemas apresentados.

A qualidade dos dados é uma preocupação essencial quando em confronto com os conceitos de segurança de uma *blockchain*. É importante que os dados sejam precisos, confiáveis e estejam em conformidade com as regras e protocolos da *blockchain* em questão. Isso ocorre pela natureza do registro inicial da coleta de uma evidência, pois, uma vez registrado com falha anterior, não será mais alterado o registro na cadeia. Na pesquisa apresentada nesta dissertação, aplicou-se um cenário em que se obtém a qualidade dos dados de forma mais clara possível e indicado a realização dos tratamentos de rastreabilidade com base na primeira coleta, o que demonstra uma proposta segura para a implantação da solução.

Por fim, esses cruzamentos de conceitos revelam que a Cadeia de Custódia, a LGPD e a Tecnologia *Blockchain* não constituem conceitos isolados, mas sim peças de um quebra-cabeça maior. Quando aplicados em conjunto, eles reforçam os Princípios de Integridade, Segurança, Transparência e Prestação de Contas, proporcionando uma abordagem abrangente e sólida para lidar com a gestão de evidências, a proteção de dados pessoais e a garantia da confiabilidade das transações. Essas conexões complexas e interdependentes destacam a importância de uma abordagem holística para a aplicação desses conceitos em diversos contextos (Shah *et al.*, 2019).

2.6 PLATAFORMAS E TRABALHOS RELACIONADOS

Há mais de uma década, em todo o mundo, realizam-se estudos relativos à cadeia de custódia digital. Giova *et al.* (2011), em seu trabalho, apresentou uma síntese de estudos científicos e técnicos a respeito da importância dos metadados e da cadeia de custódia para trazer provas digitais mais confiáveis aos tribunais. Porém, evidencia, que há problemas a serem resolvidos. Entre eles, a identificação das principais características para o controle da cadeia de custódia.

No trabalho apresentado por Lone; Mir (2019a) "Forensic-Chain": uma cadeia de custódia para forense digital baseada em *Blockchain*, há um modelo baseado em um conjunto de ferramentas de código aberto que permite a criação de sistemas em

blockchain destinados a criar, a excluir, a transferir e a exibir as informações de evidência do *Blockchain*.

Esse modelo busca processar evidências digitais para capturar detalhes sobre objetos específicos e suas propriedades contextuais, seus carimbos de data e hora associados para oferecer suporte a um novo esquema DFAX (*Digital Forensic Analysis Exchange Expression*) que fornece uma abordagem padrão para representar fatos digitais, seus relacionamentos, detalhes de proveniência associada e comportamentos em forense digital para padronização e representação de informações forenses digitais (Casey *et al.*, 2015).

Em seu trabalho, enfoca o desenvolvimento de uma cadeia de custódia confiável e segura por meio do conceito de DEMC (*Digital Evidence Management Framework*). Sua proposta é realizar a garantia ao longo de todo o ciclo de vida da evidência digital, evitar ameaças que podem afetar sua integridade e, portanto, a decisão do poder judiciário. Ele mostra as fraquezas que são consequência de problemas na cadeia de custódia e define um ciclo de vida para as evidências digitais (Cosic; Cosic, 2012).

De uma perspectiva de privacidade de dados (RIEGER *et al.*, 2019), identifica três abordagens potenciais de solução *blockchain*:

- autoridade Central;
- pseudonimização e anonimização;
- responsabilidade compartilhada.

Os projetos de *blockchain* podem identificar outras maneiras de garantir que cumpram os requisitos do GDPR, a conformidade com o GDPR não é sobre a tecnologia, é sobre como a tecnologia é usada. Ele consegue demonstrar que a tecnologia *blockchain* e o GDPR são compatíveis e sugere que as organizações devem continuar a explorar e desenvolver soluções *blockchain* que envolvam o processamento de dados pessoais.

No trabalho realizado por Salmensuu (2018), afirma-se não ser surpresa que as *blockchains* não sejam adequadas para tudo o que se quer alcançar em áreas que precisam de mais eficiência transacional. As *blockchains* possibilitam inovar preservando a conformidade com os regulamentos existentes. Dessa forma, discute a irreversibilidade de dados, o momento em que as legislações podem exigir reversibilidade, porém acredita que não há problema de GDPR para o *blockchain*; mas uma incompatibilidade de design e uma revisão estruturada de discussão para

encontrar uma solução funcional.

Os autores propuseram o conceito de Armários de Evidências Digitais para aprimorar o manuseio de provas digitais e o registro de sua cadeia de custódia. O conceito em geral é composto por três partes: estrutura de gerenciamento de evidências digitais, responsável por lidar com a interação dos investigadores em diferentes níveis do processo de investigação, o conceito de armário de etiquetas, responsável pela representação do armário de evidências digitais e o conceito de controle de acesso e comunicação segura, responsável por fornecer suporte em termos de ambientes computacionais baseado em confiança (Alruwaili, 2021).

2.7 CONSIDERAÇÕES FINAIS

Neste capítulo apresenta-se uma revisão literária do conteúdo que abrange os domínios do problema de pesquisa apresentado nesta dissertação, bem como a realização da interpolação entre conceitos. A seguir, estudam-se os métodos utilizados para a realização da pesquisa e para a realização do experimento.

3 MÉTODOS

Neste capítulo apresenta-se o método utilizado ao longo do trabalho, compreendendo a conceituação teórica do tipo de estudo e o desenvolvimento dos instrumentos para obtenção dos critérios e a compreensão da exploração de alternativas a uma proposta de solução do problema apresentado.

Classifica-se este estudo como uma pesquisa exploratória qualitativa e, para atingir os objetivos propostos e testar as hipóteses experimentais formuladas, realizou-se este estudo em duas fases distintas. A primeira consistiu na inventariação de pesquisas científicas divididas em três frentes: a legislação, sobre a proteção de dados; a Cadeia de custódia digital e as tecnologias disruptivas aplicadas aos cenários existentes na atualidade. Na segunda fase, procedeu-se ao estudo do confronto dos pontos críticos e particularidades entre as três frentes por meio da observação individual.

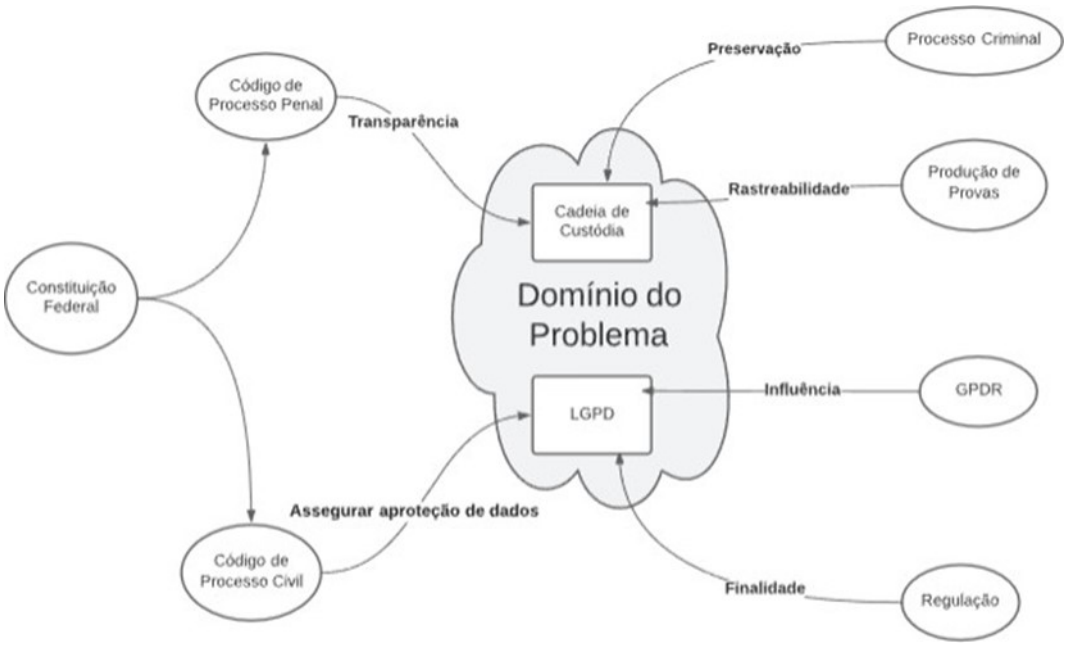
3.1 DELINEAMENTO EXPERIMENTAL

O método utilizado para averiguar e construir estruturas conceituais é a abordagem de “análise de estrutura conceitual” usada para conceber a proposta neste trabalho. Por meio deste, busca-se identificar os fatores-chave de um fenômeno, e, quando organizados, esclarecem a solução proposta. Cada fator chave tem seus atributos, pressupostos e papéis que possuem uma função específica em relação ao modelo proposto.

O método refere-se a conceitos de dados na base de conhecimento, ou seja, casos de literatura, e injetar o procedimento dedutivo para gerar a relação entre os fatores-chave do modelo. O processo geral enfatiza uma interação entre os dados indutivos e as fases de análise, o que resulta em um exame sólido do potencial e aplicabilidade da tecnologia *blockchain* para avançar a cadeia de custódia e o modelo de manipulação de evidências digitais, e para melhorar a rastreabilidade das fontes de evidências (Jabareen, 2009).

Este estudo experimental tem como objetivo alinhar os aspectos de legislações jurídicas sobre proteção de dados, de uma forma abrangente e em etapas de refinamentos, a fim de identificar onde se localiza o domínio do problema estudado conforme a figura 2.

Figura 2 – macro identificação de domínio do problema



Fonte: próprio Autor.

Busca-se aprofundar os assuntos interligados nas respectivas legislações, e, onde é possível incluir a tecnologia *blockchain* para propor uma solução viável, realizou-se um detalhamento das etapas da cadeia de custódia na legislação brasileira e dos princípios que regem a proteção de dados descritos no Capítulo 2.

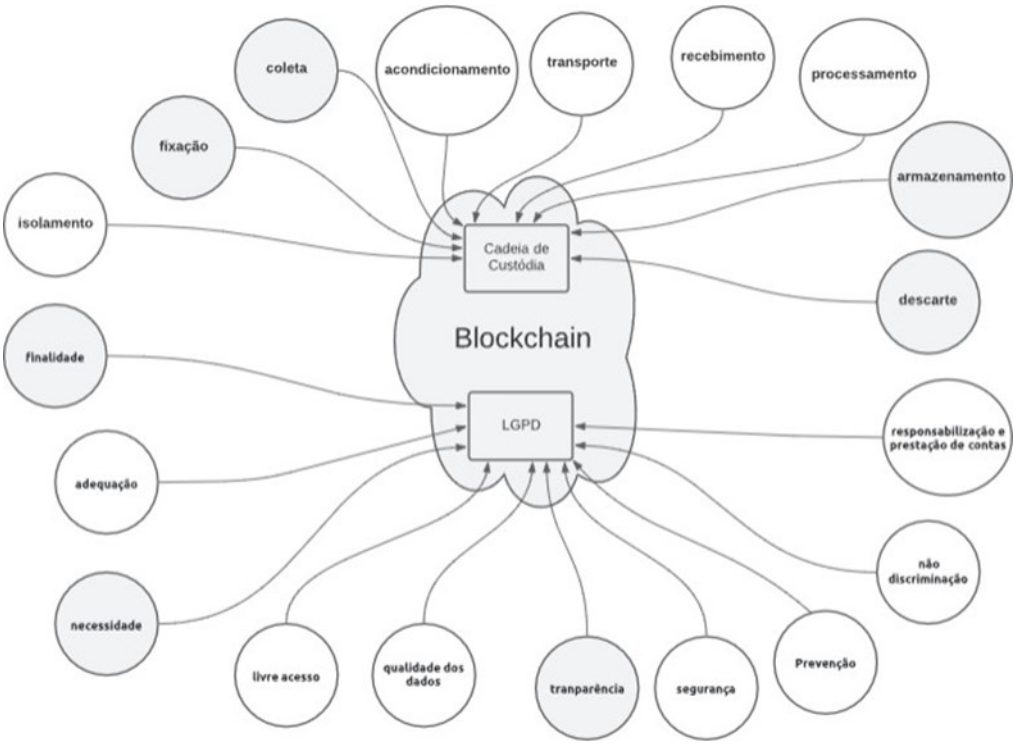
Inicialmente, conduziram-se análises da estrutura conceitual para identificar o ponto mais próximo do início dos procedimentos de registros da cadeia de custódia. Isso se deve à ausência, até o momento, de uma distinção clara entre uma entidade e as informações extraídas no contexto da aplicação desse conceito às experiências e às vivências das situações ocorridas nos ambientes jurídicos. Nesse ponto em diante, separaram-se as influências diretamente citadas na legislação de proteção de dados pessoais que gerou um conflito e abriu uma lacuna, deixando o tratamento do rastreamento de forma subjetiva uma vez que são inseparáveis conjuntos de dados objeto de apreensão e outros conjuntos de dados pessoais que devem ser protegidos.

Como primeiro refinamento para buscar, com maior precisão, o conflito

legislativo que gerou essa lacuna, realiza-se o confronto entre os conceitos envolvidos com as etapas de rastreamento de evidências digitais com os princípios declarados para a proteção de dados pessoais.

Destaca-se o segundo refinamento aplicado aos conceitos dos procedimentos da custódia em quatro etapas que contêm as maiores relações com interligação entre elas: a fixação, a coleta, o armazenamento e o descarte. Para a proteção de dados, elencaram-se três princípios de maior incidência na solução proposta: a finalidade, a necessidade e a transparência, conforme a Figura 3.

Figura 3 – detalhamento do domínio do problema



Fonte: próprio Autor.

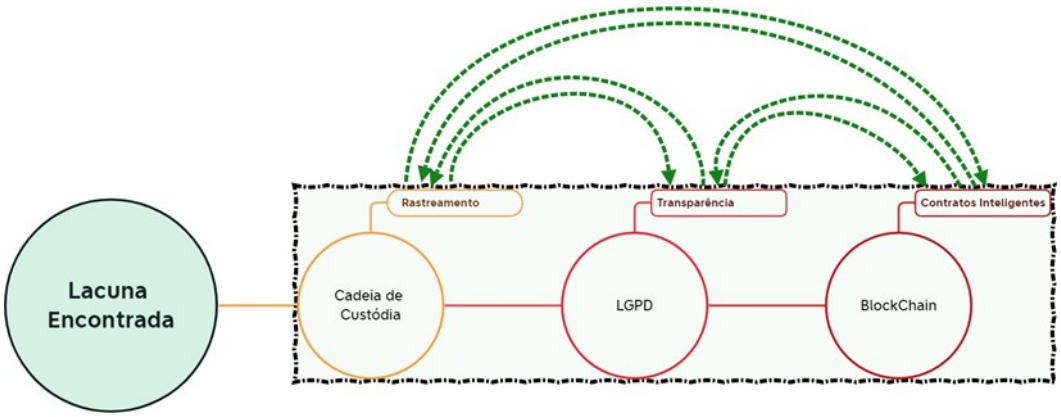
Utilizou-se um método qualitativo para construir estruturas conceituais a fim de melhor compreender fenômenos ligados a múltiplos corpos de conhecimento situados em múltiplas disciplinas. O conceito tem alguns componentes que o definem e são caracterizados por uma série de características oriundas de outros conceitos e elementos que podem ser rastreados. A integração desses conceitos tem por objetivo agrupar os que tenham mais semelhanças entre si. Esta é uma fase do método que reduz, drasticamente, a quantidade deles e permite manipular um número razoável de conceitos em um trabalho de pesquisa (Jabareen, 2009). Essa

realização permite uma verificação mais detalhada das interações entre os procedimentos da cadeia de custódia e os princípios descritos na legislação de proteção de dados, para dar suporte à construção de uma proposta de solução viável. Dessa forma, realizou-se o cruzamento entre cada conceito destacado neste estudo para buscar uma possível solução apoiada na tecnologia de cadeia de blocos e contratos inteligentes que observe todas as particularidades legais.

A aplicação desse método levou a encontrar lacunas observadas no processo de evidências digitais coletadas em processos judiciais, pois, em todas as referências legais, o legislador deixou a atribuição da confiança depositada na palavra e nos atos desses servidores em relação ao exercício de suas funções. Essa confiança é fundamental para o funcionamento adequado dos procedimentos legais e administrativos, pois permite que a sociedade e as instituições confiem que os documentos, informações e decisões produzidos pelos servidores públicos sejam autênticos e verdadeiros. Porém, quando o sistema legal brasileiro presume que as ações são genuínas, sem meios contraditórios prévios, deixa de proteger os cidadãos contra fraudes, irregularidades e abusos no âmbito da administração pública.

Ao término do processo, realizou-se uma terceira fase de refinamento, incorporando-a às características tecnológicas. Isso permite determinar, com maior precisão, os pontos nos quais as potenciais soluções propostas poderiam, efetivamente, intervir para preencher a lacuna identificada na legislação. Nesse ponto, observou-se onde podem ser encaixados os conceitos da *backchain* e os contratos inteligentes para identificar a evidência digital.

Figura 4 – lacuna encontrada

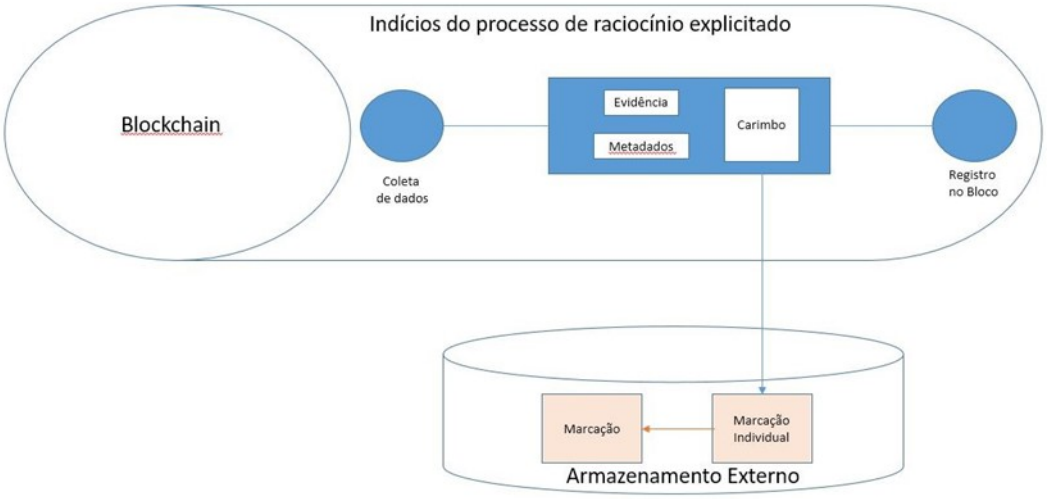


Fonte: próprio Autor.

A adoção de mecanismos tecnológicos como a aplicação das tecnologias disruptivas com uso de criptografia como uma das possíveis soluções para a lacuna encontrada. A tecnologia de *blockchain* e os contratos inteligentes se destacam como uma solução promissora para a cadeia de custódia digital devido às suas características, como: imutabilidade, transparência, rastreabilidade.

O esboço macro desses mecanismos será representado de forma esquemática na figura 5, enquanto uma análise minuciosa sobre suas aplicações e potencialidades será detalhada na proposta de solução, conforme discutido no Capítulo 4.

Figura 5 – lacuna encontrada



Fonte: próprio Autor.

3.2 PERGUNTAS DE PESQUISA

Após a revisão de literatura realizada no capítulo 2, e para o melhor entendimento do trabalho, formularam-se perguntas para esclarecer as conexões e explanar como a proposta de solução possui vantagens competitiva frente a outras soluções.

Quadro 5 – quadro de perguntas de pesquisa

Pergunta	Descrição
PP 1	Quais são os principais desafios a respeito da preservação dos dados lógicos durante investigações forenses e por que necessita de um modelo

	computacional?
PP 2	Como a evolução das tecnologias disruptivas, em especial Blockchain, pode melhorar a cadeia de custódia digital em investigações forenses, sem ofender a legislação de proteção de dados?
PP 3	Quais são os principais impactos da LGPD nas práticas de investigação forense e na cadeia de custódia digital da solução proposta?
PP 4	Qual a lacuna existente na regulamentação atual em relação à cadeia de custódia digital, evidências cibernéticas e a *bockchain* e como ela é coberta nesta pesquisa?
PP 5	Quais são os impactos das inovações tecnológicas na evolução das leis de proteção de dados e sua aplicação em investigações forenses?
PP 6	Os métodos propostos são eficientes para melhorar a transparência processual na cadeia de custódia digital no contexto de proteção de dados?
PP 7	Como a implementação de uma cadeia de custódia digital compartilhada pode beneficiar o sistema judicial e a rastreabilidade das evidências digitais?
PP 8	Como as práticas de cadeia de custódia digital podem ser aprimoradas para manter a conformidade com a LGPD sem comprometer a eficácia das investigações forenses?

Fonte: próprio Autor.

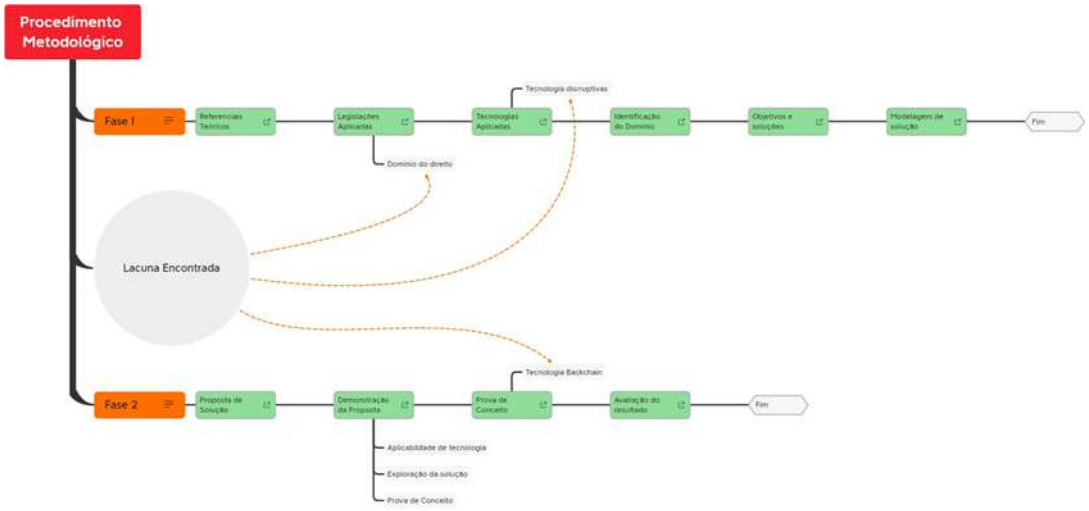
Tendo em vista as perguntas de pesquisa listadas anteriormente no quadro 5, elaborou-se o seguinte conjunto de hipóteses a serem testadas:

1. **H1:** as tecnologias utilizadas no modelo proposto é adequado ao contexto da cadeia de custódio digital preservando a legislação de proteção de dados;
2. **H2:** como os impactos previstos em cada domínio do problema pode afetar o modelo proposto.

3.3 PROCEDIMENTOS METODOLÓGICOS

De acordo com a figura 6, que ilustra os procedimentos metodológicos realizados nesta dissertação, esclarecem-se os passos aplicados a fim de garantir a sua replicabilidade.

Figura 6 – procedimentos experimentais



Fonte: próprio Autor.

A seguir, descrevem-se os passos do procedimento metodológico utilizados neste trabalho, adaptados da metodologia proposta por Jabareen (2009). Divide-se a primeira fase em cinco subfases para um melhor esclarecimento de realização deste trabalho de pesquisa.

Legislações aplicadas

A primeira tarefa foi mapear o espectro da literatura multidisciplinar sobre o fenômeno da aplicação das legislações de proteção de dados. Conforme Europeia (2019), há intenção de o legislador brasileiro estabelecer princípios amplos, alinhados ao GDPR, à medida que espelha os princípios, mantendo, em alguns casos, os mesmos conteúdos. Dessa forma, buscou-se explorar a literatura com base na legislação inspiradora da Lei de Proteção de Dados do Brasil.

Tecnologias aplicadas

Para fornecer um forte embasamento teórico conceitual, elencaram-se trabalhos correlatos com a cadeia de custódia digital de forma geral e outros trabalhos relevantes, apoiados pela tecnologia *blockchain*, a fim de proporcionar uma análise descritiva sobre o funcionamento detalhado das novas tecnologias aplicadas, para tornar o conhecimento mais explícito e, posteriormente, propor um modelo de arquitetura computacional. A leitura dos dados selecionados e categorizados tanto por disciplina quanto por uma escala de importância e poder representativo em cada uma das disciplinas maximiza a eficácia em apurar fatos e garante a representação eficaz de cada conceito (Jabareen, 2009).

Identificação do domínio do problema

A leitura e releitura dos dados selecionados na literatura permite "descobrir" novos conceitos derivados e seu resultado é uma lista contendo vários conceitos concorrentes e às vezes contraditórios (Jabareen, 2009). Diante da realização da identificação dos conceitos trazidos em cada uma das legislações estudadas, foi possível encontrar caminhos entre os fundamentos, os princípios estabelecidos e os procedimentos definidos, e, como resultado dessa avaliação, encontrou-se uma lacuna que encaixa a realização de uma proposta de solução que atenda os requisitos dos regramentos legais sem ferir os normativos essenciais para a efetividade de cada legislação aplicada. Atualmente, ainda não há tecnologia que permita a realização das etapas iniciais de isolamento de um vestígio cibernético de qualquer tipo de entidade sem a intervenção humana no processo. Dessa forma, este trabalho tem por base a coleta das entidades como a etapa inicial para a realização do rastreamento dessas entidades. A partir da coleta, também será possível realizar o procedimento de fixação descrito nos normativos.

Objetivos e soluções

Assim, a lacuna observada entre o início do processo de coleta é o ponto mais próximo para a realização da fixação das evidências e início da rastreabilidade de qualquer entidade lógica no processo de cadeia de custódia de evidências cibernéticas. A adoção de mecanismos tecnológicos padronizados como a aplicação das tecnologias de Contratos Inteligentes em ambientes de *Blockchain* pode possibilitar aos operadores do Direito, e aos envolvidos em processos judiciais, a garantia dessa rastreabilidade e das Evidências Digitais como prova válida nos processos.

Modelagem da solução

A realização da segunda fase inicia-se com a validação dos conceitos estudados e a verificação da viabilidade mínima da aplicabilidade da proposta. Para isso, construiu-se um modelo formal, que será apresentado mais adiante no capítulo Capítulo 4, incluindo a inserção de metadados como parâmetros identificadores que garantam a segurança ao serem registrados em um livro razão digital.

Tecnologia de mecanismos utilizados

Diante dos estudos realizados, e com base nos conceitos mais importantes, demonstrados no capítulo Capítulo 2, elencaram-se, cuidadosamente, os mecanismos a serem utilizados para elaborar uma proposta abrangente, que

englobe a solução completa e considere as particularidades descritas em cada disciplina.

Demonstração da proposta

Em um processo de síntese e ressíntese repetitivas até que o pesquisador reconheça uma estrutura geral que faça sentido para o trabalho, os métodos qualitativos precisam ser construídos, à medida que a análise avança, porque essa construção, inevitavelmente, influenciará e restringirá os dados, o desenho e a verificação de conclusões (Jabareen, 2009). Tendo como base esse processo de construção para demonstrar a proposta, realizaram-se três etapas:

I. **aplicabilidade das tecnologias:** após o mapeamento holístico e a coleta completa de textos e dados relacionados, selecionaram-se as tecnologias e mecanismos que mais se aplicaram à solução proposta para o problema encontrado.

II. **Exploratória descritiva da solução:** em posse das possíveis tecnologias, criou-se a descrição da proposta de solução, contendo seus relacionamentos e encaixes para tornar a proposta viável e responder as perguntas dessa pesquisa.

III. **Prova de conceito:** por fim, a criação de um Contrato Inteligente que abranja os cenários que demonstrem a efetiva operacionalização da proposta e a eficácia da solução do problema deste trabalho.

Avaliação dos resultados, discussão e trabalhos futuros

Ao final da realização dessas etapas, para demonstrar uma simulação com o intuito de avaliar o desempenho de um cenário próximo da realidade, discutem-se os resultados encontrados. Além disso, apresentam-se as estruturas e seus conceitos que têm relevância não apenas para o pesquisador, mas também oferecem contribuições significativas para a comunidade científica. O desfecho da validação do referencial teórico multidisciplinar culmina na apresentação de uma proposta de solução que aborda os desafios legislativos em um modelo computacional, visando otimizar, tecnicamente, as evidências em processos judiciais. Serão elencados pontos não observados neste trabalho que poderão ser objeto de estudos complementares no futuro.

3.4 AMBIENTE PARA O CENÁRIO EXPERIMENTAL

Neste experimento, utilizou-se a linguagem *Solidity*, a qual tem se destacado como uma ferramenta fundamental para o campo da *blockchain* e da tecnologia de contratos inteligentes. Desenvolvida, especificamente, para a plataforma *Ethereum*, a *Solidity* oferece um ambiente de programação seguro e versátil que permite aos pesquisadores criar contratos inteligentes de maneira eficaz e eficiente.

A *blockchain* Ethereum, conhecida por sua capacidade de suportar aplicações descentralizadas e contratos inteligentes, tem sido um campo fértil para inovação e pesquisa. Contratos inteligentes são programas autônomos executados na *blockchain* e podem ser usados para automatizar e garantir acordos entre partes sem a necessidade de intermediários. A construção de contratos inteligentes exige uma linguagem de programação especializada, e, nesse sentido, a *Solidity* se destaca. A *Solidity*, projetada com foco na segurança e na clareza de código, oferece aos pesquisadores uma ferramenta poderosa para traduzir algoritmos e lógica de negócios em contratos inteligentes executáveis. Ela fornece uma variedade de recursos e bibliotecas que simplificam a implementação de funcionalidades complexas em contratos inteligentes, como gerenciamento de acessos aos conteúdos digitais, validações descentralizadas e outros. Isso permite que pesquisadores foquem na criação de lógica de negócios inovadora em vez de se preocupar com os detalhes de implementação de baixo nível. Pesquisadores podem explorar novos modelos de negócios, experimentar mecanismos de incentivo e examinar as implicações legais e éticas dos contratos inteligentes (Dannen, 2017).

Para realizar o experimento deste trabalho, utilizou-se o Remix Ethereum que é uma ferramenta de desenvolvimento amplamente usada para criar contratos inteligentes na rede Ethereum. Trata-se de um Ambiente de Desenvolvimento Integrado (IDE), acessado diretamente por meio de um navegador web, o que simplifica o processo de criação, teste e implantação de contratos inteligentes. Nesse ambiente, o pesquisador tem acesso a um editor de código que oferece vários recursos, tornando mais fácil escrever código seguro e eficiente. A ferramenta permite organizar projetos, criando pastas e subpastas para manter a organização em projetos complexos.

Uma das características notáveis é o compilador *Solidity* integrado, que permite compilar contratos inteligentes diretamente no ambiente, auxiliando a identificação

de erros antes da implantação na *blockchain*. A depuração é outra funcionalidade poderosa, permitindo que os desenvolvedores definam pontos de interrupção, inspecionem variáveis de estado e rastreiem a execução do contrato para corrigir problemas (Taş ; Tanriöver, 2019).

O Remix também oferece a capacidade de simular a execução de contratos inteligentes antes da implantação na rede Ethereum, possibilitando testes sem gastar ether real. Além disso, ele se conecta a várias redes Ethereum, como a rede principal e redes de teste, facilitando o desenvolvimento e os testes em ambientes controlados.

Os pesquisadores podem gerenciar contas Ethereum no ambiente para assinar transações e implantar contratos. O Remix é altamente personalizável, permitindo a adição de plugins e extensões para atender às necessidades individuais (Taş; Tanriöver, 2019).

3.5 CENÁRIO DO CICLO DE VIDA UMA *BLOCKCHAIN*

A criação de um canário para o ciclo de vida de um contrato inteligente em *Solidity* com a representação de um sistema de cadeia de custódia descentralizada é um processo complexo para tentar atender os requisitos de rastreabilidade, integridade e acesso controlado às evidências digitais. Esse contrato inteligente permitirá que diferentes papéis interajam com as evidências, solicitando acesso, confirmando ou recusando o armazenamento, bem como acessando as informações armazenadas externamente. Elaborou-se, cuidadosamente, o projeto do contrato para estabelecer níveis de autorização e segurança, a fim de que as ações realizadas estejam em conformidade com as regras predefinidas estabelecidas na legislação.

O ciclo de vida começa com a criação do contrato inteligente na *blockchain* do tipo permissionada. Configuram-se os parâmetros iniciais, incluindo os papéis e suas permissões. Em seguida, implanta-se o contrato na *blockchain*, o tornando acessível a todos os participantes da rede descentralizada.

A primeira fase é a solicitação de armazenamento do metadado das evidências, ou seja, a realização da coleta inicial. O dono deve ser o responsável que envia uma transação ao contrato solicitando o armazenamento de uma nova evidência digital. Essa transação contém detalhes relevantes, como descrito no

quadro 8, apresentada no capítulo 4. O contrato valida a solicitação com base nas regras definidas e cria um registro único para os metadados da evidência digital e, consequentemente, efetua o armazenamento externo do conteúdo.

Após a validação, realiza-se a confirmação ou recusa do armazenamento pelos atores autorizados. Cada ator pode aceitar ou rejeitar a solicitação com base em sua análise. A decisão é registrada na *blockchain*, fornecendo um histórico transparente das ações tomadas. Uma vez armazenada, a evidência é protegida por meio de criptografia e integridade de dados. Qualquer tentativa de alteração indevida será detectada, assegurando a confiabilidade das informações.

Os atores autorizados podem acessar as evidências armazenadas de acordo com suas permissões, por meio de chaves de acesso e identificação única, garantindo que apenas os indivíduos apropriados tenham acesso às informações relevantes. À medida que o tempo passa, mais interações podem ocorrer, como solicitações de transferência de custódia ou atualizações de informações. Cada interação é registrada na *blockchain*, criando um histórico abrangente e imutável. Eventualmente, a evidência pode ser considerada não mais relevante ou válida. Nesse caso, procedimentos para arquivamento ou exclusão seguro podem ser iniciados por atores autorizados.

3.5.1 Estrutura do cenário proposto

O contrato começa com a definição do "Perfil", que representa os diferentes tipos de atores que podem interagir com o contrato: dono, criador e envolvido. Além disso, há outra definição, chamada "EstadoEvidencia", que define os possíveis estados de uma evidência: "Estado Inicial", "Validar Permissão", "Realizar Transação", "Registrar Transação", "Transação Negada", "Completar Transação Sucesso", "Finalizar Transação Falha". Em seguida, define-se uma estrutura chamada Evidencia, que contém informações sobre cada evidência, incluindo seu número, criador, descrição, número do caso, rótulo, estado, *timestamp*, endereço externo e o solicitante de armazenamento. Executa-se o construtor do contrato quando este é implantado e define o endereço do dono como o endereço que fez o *deploy* do contrato.

3.5.2 Eventos importantes

• **EvidenciaCriada:** emitida quando uma nova evidência é criada. Ele registra o número da evidência e o número do caso associado.
• **ArmazenamentoSolicitado:** emitido quando um envolvido solicita o armazenamento de uma evidência. Ele registra o número da evidência e o endereço do solicitante.
• **ArmazenamentoConfirmado:** emitido quando o dono confirma o armazenamento de uma evidência. Além do número da evidência, esse evento também registra o endereço IPFS em que os dados externos foram armazenados.
• **ArmazenamentoRecusado:** emitido quando o dono recusa o armazenamento de uma evidência. Ele registra o número da evidência.
• **EvidenciaAcessada:** emitida quando uma evidência é acessada. Registra o número da evidência.

3.5.3 Modificadores

• **somenteDono:** garante que somente o dono do contrato possa executar determinadas funções, como criar uma nova evidência ou confirmar/recusar o armazenamento.
• **SomenteCriador e somenteEnvolvido:** restringem o acesso a funções específicas para o criador da evidência ou envolvidos (criador ou solicitante de armazenamento).

3.5.4 Funções

• **coletarEvidencia:** permite que o dono do contrato crie uma nova evidência. Essa função recebe os parâmetros necessários para criar uma nova instância de Evidência no contrato.
• **solicitarArmazenamento:** permite que o criador ou o envolvido solicite o armazenamento de uma evidência. A evidência deve estar no estado "Criada"para que a solicitação seja possível.
• **confirmarArmazenamento:** permite que o dono do contrato confirme o armazenamento de uma evidência após uma solicitação ter sido feita. Isso muda o estado da evidência para "Armazenada"e registra o endereço IPFS em que se armazenaram os dados externos.

• **recusarArmazenamento:** permite que o dono do contrato recuse o armazenamento de uma evidência após uma solicitação ter sido feita. Isso muda o estado da evidência de volta para "Criada".
• **acessarEvidencia:** permite que qualquer pessoa acesse uma evidência que tenha sido armazenada. Isso muda o estado da evidência para "Acessada".

3.6 CONSIDERAÇÕES FINAIS

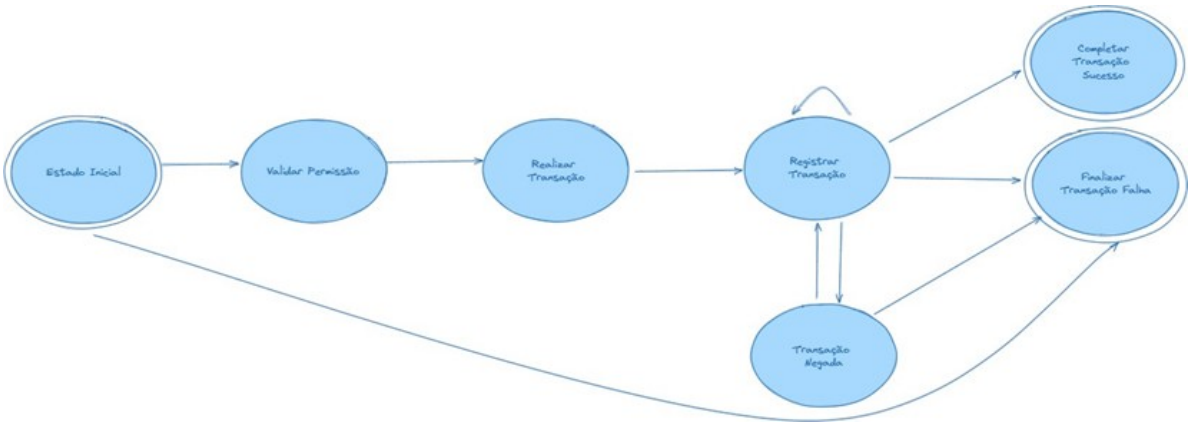
Neste capítulo, apresentaram-se os métodos utilizados neste trabalho para reunir os trabalhos mais qualificados sobre o domínio do problema apresentado no capítulo 2 e a formulação de perguntas de pesquisa a fim de compreender a complexidade dos apontamentos realizados entre cada fator do domínio do problema, bem como os procedimentos realizados para efetuar o experimento da pesquisa. No próximo capítulo, detalha-se a proposta de pesquisa.

4 PROPOSTA DE PESQUISA

4.1 PROPOSTA DE CADEIA DE CUSTÓDIA DIGITAL

Nesta seção, definem-se os recursos do sistema, funções e responsabilidades do modelo proposto. A arquitetura da proposta inclui participantes, a escolha de um algoritmo de consenso, criação de contratos inteligentes, funções criptográficas e armazenamento distribuído para atender requisitos de legislação. Na figura x, de forma geral, demonstra-se o funcionamento dos estados da proposta.

Figura 7 – máquina de estados



Fonte: próprio Autor.

4.1.1 Modelo proposto

Uma solução *blockchain* para processar dados em cadeia de custódia que requer que dois ou mais participantes compartilhem atribuição para adicionarem informações, como é o caso dos processos judiciais, implica a utilização de uma abordagem de rede *blockchain* privada e com permissão que funciona em um ambiente restritivo e que está sob o controle de uma única entidade (Lone; Mir, 2019a). Essa entidade é a central de custódia prevista na legislação brasileira descrita no artigo 158-C do Código de Processo Penal (CPP). Até o presente momento, a legislação brasileira trata os fatores que influenciam as primeiras etapas da cadeia de custódia como um processo subjetivo na coleta de evidências digitais. Por esse motivo, o modelo proposto servirá como uma espinha dorsal para qualquer investigação forense digital ou uma trilha de auditoria cronológica feita por uma organização,

permitindo que eles usem um modelo de processo de registro de acessos e a individualização dos pontos relevantes com consequente controle de manuseio de dados digitais e a validação das entradas apoiadas pela tecnologia *Blockchain*.

Apresenta-se, na seção 4.1, uma máquina de estado para a proposta de solução, que constitui uma demonstração simples da possibilidade de controle das transições para atender os requisitos mínimos e que possam também garantir que, a partir da coleta inicial das evidências, sejam também iniciados o completo rastreamento para garantir a cadeia de custódia.

- **Estado inicial** – representa o estado inicial e realiza a validação da transação, esta validação tem a função de garantir que todos os parâmetros estejam corretos e válidos para que o registro seja efetuado na rede.
- **Validar permissão** – esse estado representa a garantia de que quem esteja manipulando uma evidência possui as autorizações necessárias para executar a transação.
- **Realizar transação** – o estado Realizar Transação é responsável por garantir que a transação seja efetuada dentro da rede blockchain e acompanhando os registros efetuados autorizados ou não autorizados.
- **Registrar transação** – esse vértice representa a persistência do rastreamento garantindo que os dados imutáveis sejam gravados e os dados passíveis de esquecimento tenham seu rastreamento completo.
- **Transação negada** – o estado A4 é um estado terminal, ele é a representação de falha em um nó que poderá indicar se houve erro no registro do vestígio na rede externa (off-chain) e o registro ponto de específico de falha.
- **Completar transação sucesso** – esse estado é terminal e confirma que a transação aconteceu de forma completa e com sucesso em todas as fases internas e externas.
- **Finalizar transação falha** – esse estado é terminal e transitado em caso de falha de validação ou verificação de autorização.

Ressalta-se que a validação **Estado Inicial** possui duas possibilidades de transição de estados e, quando não há validade dos dados a serem registrados, essa informação não é gravada e transita, diretamente, para o estado **Finalizar Transação Falha**. Por sua vez, caso os dados sejam válidos, mas não autorizados pelo estado **Validar Permissão**, o registro é efetuado na rede para a obtenção das intenções de acesso, porém não será registrado na rede externa (*off-chain*). Por

esse motivo, pode ocorrer uma tramitação entre **Realizar Transação** para **Registrar Transação** e, devolvendo a confirmação, é transitado do estado **Realizar Transação** para **Finalizar Transação Falha**. Uma vez que há todos os estados válidos, executam-se os registros em suas respectivas redes *blockchain* (internas e externas), e estes são transitados do estado **Registrar Transação** para **Completar Transação Sucesso**. Em caso de erros ou falhas na rede, transita-se do estado **Registrar Transação** para **Transação Negada**, indicando o ponto específico da falha.

No quadro 6, apresentam-se as transições para cada estado de entrada.

Quadro 6 – quadro de transição de estados

Estado de Entrada	Saídas
Estado Inicial	Validar Permissão, Finalizar Transação Falha
Validar Permissão	Realizar Transação
Realizar Transação	Registrar Transação, Finalizar Transação Falha
Transação Negada	Realizar Transação, Transação Negada, Completar Transação Sucesso

Fonte: próprio Autor.

Considerando-se os pontos problemáticos discutidos no capítulo 2, essa proposta parte do ponto específico da coleta, tendo em vista que é onde existe a melhor opção sem intervenção humana proposta pela legislação brasileira. Dessa forma, é possível utilizar as características da cadeia de custódia de vestígios cibernéticos de forma a garantir a cronologia dos fatos digitais integralmente. A separação dos dados lógicos do equipamento físico é uma parte da etapa de coleta de dados na investigação digital. Então, essa proposta é uma forma de garantir, no primeiro momento da desvinculação entre o vestígio físico e o vestígio digital, a realização da criação de uma entidade e o seu conjunto de entidades.

Torna-se necessário, para a efetivação da proposta, a identificação dos intervenientes ligados diretamente ao processo inicial dos registros das evidências e registrar quem foram os criadores, o dono e a lista inicial dos envolvidos que poderá acessar as evidências digitais. Estes papéis são essenciais para que seja possível cumprir requisitos legais de proteção de dados. No quadro 7, apresenta-se a especificação de função de cada papel proposto.

Quadro 7 – quadro de papéis e funções

Papel	função
Criador	O papel do criador é o primeiro envolvido a registar os dados lógicos na Blockchain
Dono	O papel de Dono é o mandatário com permissão de conceder outras permissões
Envolvidos	Este papel é realizado pelos interessados que precisam manipular as evidências

Fonte: próprio Autor.

4.1.2 Representação formal da solução

Melhore sem modificar o conteúdo: o processo de investigação digital torna-se completo quando a evidência digital é formalmente aceitável. Para isso, algumas condições devem ser cumpridas, dentre elas a cópia da evidência digital deve conter uma função de resumo calculada (“valor de hash”) para preservar a integridade com a evidência original, outros dados como: coordenadas de localização, procedimentos realizados, motivo do acesso, hora do acesso, é considerada evidência formalmente aceitável em um processo judicial.

Nessa proposta a identificação unívoca de cada vestígio e de seu conjunto identificador deve ser criada para que seja possível rotular cada acesso realizado e possa garantir a cadeia de custódia sem deixar de proteger outros dados contidos (Cosic, 2017). Sendo assim, a junção de alguns dados e metadados foram selecionados e formam a marcação de identificação produzindo um "Lacre Digital" para registrar, na rede *blockchain*. Descrevem-se os dados propostos no quadro 8.

Quadro 8 – quadro de dados para registro de metadados

Dado	Sigla	Descrição
Número da Evidência	(NE)	Número identificador da evidência física para o Processo Judicial.
Criador	(CRI)	Responsável pela coleta digital e primeiro registro de dados digital.
Descrição da Evidência	(DE)	Descrição geral do dispositivo coletado.
Número do Caso	(NC)	Numeração identificadora do caso, processo dos autos judiciais.
Data e Hora	(DH)	Carimbo de Data e Hora da coleta.
Rótulo de Evidência	(RE)	Numeração individual gerada no momento do primeiro registro.
Rótulo de Conjunto	(RC)	Numeração de classificação gerada no momento do primeiro registro.

Fonte: próprio Autor.

Intitula-se a entrada na cadeia de custódia digital de Fonte de Dados (FD) que representa a extração de dados dos equipamentos conforme descritos no capítulo 2, como itens de interesse para a investigação. Nesse sentido, os FD's devem ser lacrados conforme são "lacradas" as evidências encontradas em uma cena de crime cibernético. Cada vestígio tem sua integridade e pode ser acessado ou modificado. Essa é a primeira garantia que se pretende preservar da etapa de coleta. Em seguida, há a necessidade de garantir o conjunto completo de tipos de dados armazenados para facilitar as consultas e, consequentemente, os registros de acessos do vestígio.

A marcação do conjunto de dados da evidência pode existir de diferentes granularidades e deve ser realizada em uma etapa que possa ser feita a análise do tipo de dados ou aplicativo, por exemplo, e criar uma etiqueta que marque uma classificação do vestígio. Dessa maneira, será possível garantir que estarão resguardados os primeiros dos registros e para isso é preciso criar um analisador de dados. Ele fará a classificação dos grupos a serem etiquetados com marcadores únicos para o grupo de evidências. Isto implica a representação da Fontes de dados em que FD = {fd | fd seja um arquivo válido da fonte de dados}. Para garantir que esses dados tenham suas marcações, devem-se executar dois processos para a criação das etiquetas de item e de grupo de itens. Essa execução implica realizar a criação dos vínculos de vestígios (V) onde, $V = \{v \mid v \subseteq FD\}$. A saída desse processo é a realização de processo de encapsulamento de dados em que a marcação de M(V) é, $M(V) = \{M(v) \mid v \in V\}$ e representa $M(fd) = \{M(fd) \mid fd \in v\}$. Dessa forma, é

possível dizer que fd(v) = {P(fd | fd ∈ v)}.

4.1.3 Fator de retroalimentação

A admissibilidade da prova constitui um conceito de direito processual e consiste em uma valoração prévia feita pelo legislador, destinada a evitar que elementos provenientes de fontes espúrias, ou meios de prova reputados inidôneos, tenham ingresso no processo e sejam considerados pelo juiz na reconstrução dos fatos. As leis brasileiras permitem, em diversos momentos da vida útil do conjunto probatório de um processo legal, que sejam utilizados em momentos diferentes e que podem, a qualquer momento, solicitar tipos de "Entidades" diferentes que possam ser admitidas ou que possam ser desentranhadas do processo. Nessa proposta, criou-se um fator de retroalimentação para suprir a necessidade da movimentação dos itens considerados admissíveis como prova do processo judicial (Edinger, 2016).

4.1.4 Mecanismo de consenso e o contrato inteligente

Os mecanismos de consenso para redes privadas permissionadas podem oferecer uma oportunidade mais eficientes e mais barata em termos de custo computacionais. O motivo da privacidade é uma característica que limita a entrada e permanência de participantes na rede, principalmente as indesejáveis. As permissões possibilitam a configuração de diferentes papéis para os nós participantes da rede. Além disso, oferecem flexibilização para que as aplicações façam parte do processo de consenso ou limitam alguns participantes à geração da sequência de blocos. Essa proposta combinam a configuração de uma *blockchain* privada e uma rede permissionada, ou seja, somente pessoas com permissão podem participar dessa rede, tornando-a muito menos descentralizada e mais próxima dos modelos de registro de informação centralizados como os já existentes, porém ser perder as vantagens fornecidas por esta tecnologia. Descreve-se, no capítulo 2, a Prova de Autoridade (PoA), em que a identidade do indivíduo está em jogo na validação. Com o PoA, os validadores devem ter sido autorizados preventivamente e suas identidades são conhecidas. Assim, agir maliciosamente resulta na perda de reputação pessoal e, por fim, na expulsão do conjunto de validadores (Mingxiao *et*

al., 2017).

Destaca, em seu trabalho, que a criação de contratos inteligentes envolve várias partes que, primeiramente, negociam as obrigações, direitos e proibições dos contratos. Após várias rodadas de discussões e negociações, pode-se chegar a um acordo. Os contratos armazenados nas blockchains não podem ser modificados devido à imutabilidade das cadeias de blocos.

Qualquer mudança exige a criação de um novo contrato. Depois que os contratos inteligentes são implantados em *blockchains*, todas as partes podem acessar os contratos por meio dos *blockchains*. A criação de um contrato inteligente para registrar todas as ações que ocorram nas evidências garante os registros rastreados e o estabelecimento das diretrizes legislativas de proteção de dados (Zheng *et al.*, 2020).

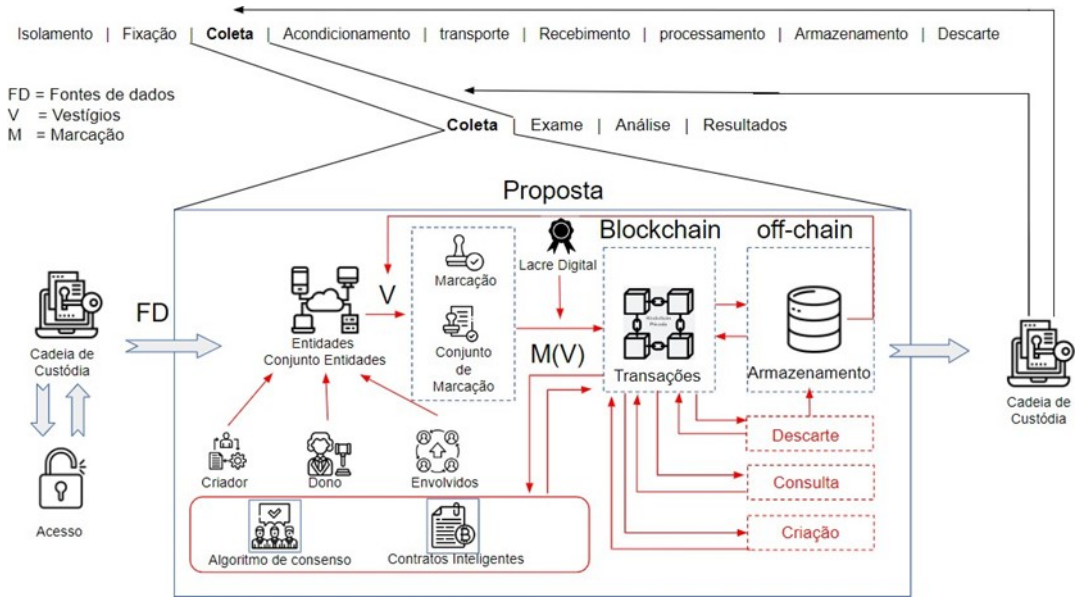
4.1.5 Controle de acesso

O mecanismo de controle de acesso de uma *blockchain* privada pode variar: os envolvidos existentes podem decidir futuros participantes; uma autoridade reguladora poderia emitir licenças para participação; ou um consórcio poderia tomar as decisões. Depois que uma entidade ingressar na rede, ela desempenhará um papel na manutenção de maneira descentralizada (Lone; Mir, 2019a).

A proposta neste trabalho mostra as organizações jurídicas brasileiras como as partes integrantes do processo de validação e a separação dos papéis descritos no quadro 7, em que cada participante poderá ter diferentes papéis e realizar diferentes ações em cada momento do ciclo de vida da evidência.

Para conseguir atender todos os requisitos que garantam a legislação corrente e as tecnologias mencionadas neste trabalho, apresenta-se a Figura 7, em que se relaciona todo o ecossistema da proposta.

Figura 8 – modelo Computacional para Cadeia de Custódia Digital



Fonte: próprio Autor.

Na figura 7, expõe-se o modelo construído por meio da abordagem conceitual que corresponde aos aspectos legais, armazenamento confiável, conceito de manutenção de registros e documentação baseado em marcações inequívocas dos elementos, bem como proposta da infraestrutura baseada em modelo de computação.

4.2 EXEMPLO DE UTILIZAÇÃO DO MODELO PROPOSTO

Como exemplo, considera-se um tribunal que tenha implementado o projeto proposto nesta dissertação, em um cenário aplicado a uma investigação criminal envolvendo dados digitais em um caso de fraude financeira. Nesse contexto, o tribunal, ciente da importância de seguir os princípios da LGPD, garante que todos os dados pessoais envolvidos na investigação estejam em conformidade com a legislação. O modelo projetado deve ter recursos de anonimização e pseudonimização de dados sensíveis, assegurando que as informações pessoais dos indivíduos envolvidos sejam protegidas durante a análise forense. Isso significa que, mesmo durante a coleta e análise dos dados financeiros e transações suspeitas, medidas são aplicadas para preservar a identidade dos indivíduos não relacionados ao crime.

A respeito das práticas de investigação forense, será permitido aos

investigadores acessar dados de maneira controlada e estruturada, seguindo os procedimentos legais e éticos descritos na LGPD. Dessa forma, é possível registrar todas as etapas do processo de investigação, desde a coleta até a análise, garantindo uma documentação detalhada para a cadeia de custódia digital. A cadeia de custódia digital utiliza o modelo proposto rastreia e registra todas as interações e manipulações dos dados durante a investigação. Essa abordagem, orientada por tecnologia de cadeia de blocos, contribui para a eficiência do sistema judicial, promovendo a justiça e o cumprimento das leis de proteção de dados, enquanto mantém a qualidade e a rastreabilidade das evidências digitais utilizadas nos processos legais.

4.3 CONSIDERAÇÕES FINAIS

Neste capítulo, detalhou-se uma proposta de modelo computacional para cadeia de custódia digital, contendo a representação formal da solução, o fator de retroalimentação, os mecanismos de consenso e o funcionamento dos contratos inteligentes e o funcionamento do controle de acesso permissionado, por fim, um exemplo da utilização do modelo. Mais adiante, no capítulo 5, apresenta-se um cenário experimental da materialização da proposta.

5 CENÁRIO EXPERIMENTAL

Neste capítulo, apresenta-se a aplicação de um cenário experimental da utilização de contratos inteligentes em uma rede *blockchain* para demonstrar a efetividade da utilização da proposta apresentada no capítulo 4. O tipo de *blockchain* define o controle de associação no algoritmo de consenso. Isso deve ser considerado ao avaliar os algoritmos de consenso para verificar o tipo de associação assumida no projeto. O tipo de *blockchain* deve ser escolhido de acordo com a natureza da aplicação de negócios (Chaudhry; Yousaf, 2018).

5.1 CENÁRIO PROPOSTO

Propõe-se um cenário experimental de um contrato inteligente com metadados para uma cadeia de custódia e dados armazenados "off-chain". Conforme o ambiente descrito no capítulo 3, esse cenário implementa uma possível situação de registro e verificação de evidências de forma imutável, transparente, porém respeitando a legislação vigente.

O contrato é composto por variáveis e funções fundamentais para o seu funcionamento. A variável "Dono" armazena o endereço do proprietário do contrato, garantindo que apenas essa entidade tenha permissão para realizar operações cruciais no contrato. Nesse ponto, destacam-se os tribunais e varas judiciais que podem iniciar um processo digital.

É importante esclarecer que o contrato mantém um mapeamento chamado "endereço", que associa cada *hash* de evidência a um valor para indicar se a evidência correspondente foi registrada na cadeia de custódia.

Aciona-se o método construtor do contrato no momento da criação e define-se o endereço do criador como o proprietário do contrato, reforçando o conceito de autoridade e controle sobre as operações a serem executadas.

Um aspecto vital para o funcionamento seguro do contrato é o uso de modificadores, como o "SomenteDono". Esse modificador é aplicado a determinadas funções, como "coletarEvidencia", garantindo que somente o proprietário do contrato tenha permissão para executá-las. Isso é crucial para manter a integridade e a confiança no sistema, assegurando que apenas a corte que trâmita o processo judicial tenha o poder de registrar novas evidências na cadeia de custódia. A função

"coletarEvidencia"apresentada é uma função externa de um contrato inteligente que opera na *blockchain*. Ela recebe vários parâmetros, incluindo o número da evidência, descrição, número do caso, data e hora, rótulos associados à evidência e ao conjunto, além de um novo parâmetro, o endereço *off-chain*.

```
function coletarEvidencia(
    uint256 _numeroEvidencia,
    string memory _descricaoEvidencia, uint256
    _numeroCaso,
    string memory _rotuloEvidencia
) external somenteDono {totalEvidencias++;
    evidencias[totalEvidencias] = Evidencia(
        _numeroEvidencia, msg.sender,
        _descricaoEvidencia,
        _numeroCaso,
        _rotuloEvidencia,
        EstadoEvidencia.A0, block.timestamp,
        address(0),"
    );

emit EvidenciaCriada(_numeroEvidencia, _numeroCaso);
}
```

Ao ser invocada, essa função cria uma nova instância de evidência e a armazena no contrato. A estrutura de metadados "evidencias"é atualizada com os valores fornecidos, incluindo o número da evidência, o endereço do remetente, a descrição, o número do caso, data e hora, rótulos relevantes e um endereço *off-chain*.

A função incrementa a quantidade total de evidências registradas e emite um evento "EvidenciaAdicionada", informando o número da evidência adicionada e o remetente que realizou a adição.

Aplica-se esse cenário a uma rede privada e permissionada; o algoritmo de consenso desempenha um papel crucial para a validação de transações e a inclusão de novos blocos no *blockchain*. Esse ambiente controla a seleção cuidadosa do algoritmo de consenso "Proof of Authority"(PoA), definido para a

utilização do experimento, e envolve a designação de um conjunto limitado de validadores que são reconhecidos como autoridades confiáveis. Essas autoridades têm permissão para criar novos blocos e validar transações com base em critérios predefinidos de reputação ou identidade. Dessa forma, é possível validar se os acessos para leitura de informações nas evidências são de membros autorizados para buscar o rastreamento completo de uma evidência digital.

Quando uma evidência é coletada, o criador ou a parte envolvida tem o direito de solicitar o armazenamento dessa evidência, desde que esta esteja no estado "Criada". Ao fazer essa solicitação, atualiza-se o estado da evidência para "ArmazenamentoSolicitado", e gera-se um evento para registrar essa requisição. Somente o dono do contrato pode confirmar o armazenamento de uma evidência que se encontra no estado "ArmazenamentoSolicitado". Ao confirmar o armazenamento, altera-se o estado da evidência para "Armazenada", e registra-se o endereço IPFS para referência futura. Um evento é emitido para comunicar a bem-sucedida confirmação do armazenamento. No caso do proprietário do contrato decidir recusar o armazenamento de uma evidência no estado "ArmazenamentoSolicitado", a evidência retorna ao estado "Criada", e ocorre a remoção do solicitante de armazenamento. Um evento é então emitido para indicar a recusa do armazenamento da evidência.

Quando a evidência está armazenada e pronta para ser acessada, qualquer parte auto rizada pode chamar essa função. Elas atualizam o estado da evidência para "Acessada". Essa função não apresenta restrições sobre quem pode acessar a evidência, desde que ela esteja no estado "Armazenada", conforme a função "acessarEvidencia".

```
functionacessarEvidencia(uint256 _numeroEvidencia) ex
    ternal {require(
    evidencias[_numeroEvidencia].estado== EstadoEvide
    ncia.Arma "A evidencia deve estar no estado
    Armazenada"
      );

      evidencias[_numeroEvidencia].estado = EstadoEvide
      ncia.Acessada;
```

```
        emit EvidenciaAcessada(_numeroEvidencia);
    }
```

Nesse contexto experimental, o contrato proposto para a gestão de cadeia de custódia de evidências digitais representa uma tentativa inovadora de utilizar tecnologia descentralizada para melhorar a integridade e a rastreabilidade de informações cruciais, como evidências digitais em procedimentos legais e forenses. Nesta pesquisa, investiga-se, detalhadamente, o funcionamento, estrutura e possíveis considerações para a utilização desse contrato.

O experimento realizado adota uma abordagem estruturada e lógica para gerenciar a cadeia de custódia. Nele, definem-se três papéis principais, cada um com permissões específicas para realizar determinadas ações dentro do contrato. Estabelecem-se, também, diferentes estados para as evidências, refletindo o fluxo de trabalho da cadeia de custódia digital.

A estrutura do contrato se baseia em componentes fundamentais. Empregam-se enumerações para definir os papéis e os estados possíveis; enquanto se utiliza uma estrutura de dados para representar cada evidência, incluindo detalhes e outras informações pertinentes. Adicionalmente, o contrato faz uso de mapeamento para relacionar identificadores únicos de evidências com suas estruturas correspondentes, juntamente a variáveis públicas para armazenar informações sobre os atores envolvidos e o número total de evidências registradas.

Há, na realização do experimento, a presença de modificadores que atuam como condições prévias para a execução de determinadas funções, garantindo, assim, a permissão correta para cada operação. Emitem-se os eventos para registrar e notificar atividades relevantes realizadas no contrato, oferecendo transparência e rastreabilidade das ações executadas.

Esse contrato pode se beneficiar de considerações adicionais para sua melhoria. Desconsideram-se do escopo dessa implementação questões de segurança, especialmente já discutidas no capítulo 2. No entanto, consideram-se aspectos relacionados à privacidade e à proteção de dados sensíveis presentes nas evidências, reforçando a importância de restringir o acesso a informações confidenciais apenas a partes autorizadas.

Contudo, o experimento em estudo representa uma iniciativa promissora na gestão de cadeia de custódia de evidências digitais, explorando o potencial da

tecnologia *blockchain* para a consolidação e adoção bem-sucedida deste tipo de abordagem em ambientes legais e forenses. Esse cenário experimental oferece valiosos *insights* para aprimoramentos futuros, destacando a importância do desenvolvimento iterativo e do aperfeiçoamento constante dessas soluções inovadoras e disruptivas.

5.2 CONSIDERAÇÕES FINAIS

Neste capítulo, apresentou-se a execução do experimento do modelo computacional para uma solução de cadeia de custódia digital. No próximo capítulo, será realizada uma análise e discussão dos resultados obtidos com esse experimento, especificando, também, se as hipóteses e questões de pesquisa foram atendidas.

6 RESULTADOS E DISCUSSÃO

6.1 ANÁLISE DE RESULTADOS E DISCUSSÃO

O emprego da tecnologia *blockchain* como uma solução viável para manter a cadeia de custódia na área de forense digital, de acordo com a legislação brasileira, requer uma compreensão abrangente das nuances legislativas, diante de um amplo leque de opções de soluções.

A utilização de redes de *blockchains* privadas permissionadas está alinhada ao requisito de acesso restrito, exigindo permissão para a leitura das informações contidas em sua cadeia. Esse acesso é concedido mediante convite validado pelo iniciador da rede ou por um conjunto predefinido de regras, como ilustrado no capítulo 4, incluindo órgãos responsáveis (Tribunais e Varas), bem como partes envolvidas (Juiz, Promotor e Advogados).

O mecanismo de consenso mais viável para essa solução foi a utilização da prova de participação, evidenciando maior eficiência, velocidade e consumo energético reduzido em comparação a outros métodos. Além disso, oferece controle de acesso por meio de permissões gerenciadas, sendo considerado seguro e confiável, viabilizando transações sem custos financeiros para os envolvidos nos processamentos.

A marcação individual de cada evidência é uma ação fundamental na proposta, permitindo o registro de qualquer dado acessado ou excluído. A criação de um conjunto de marcações visa facilitar a recuperação rápida de uma evidência, especialmente em casos de grande volume de informações. Essas marcações atuam como "lacres digitais", possibilitando o rastreamento dos dados.

Considerando as restrições legais, a questão do esquecimento pode ser problemática. Portanto, a criação de uma estrutura de armazenamento desacoplada oferece maior segurança, solucionando, definitivamente, esse problema, embora introduza complexidade na construção do modelo.

A análise realizada no cenário experimental demonstrou que os atributos da tecnologia *blockchain* podem contribuir, significativamente, para a gestão da rastreabilidade de dados, em conformidade com a Lei Geral de Proteção de Dados Pessoais. Outras vantagens relevantes incluem a redução significativa do risco de vazamento de informações, garantia de integridade dos dados, eliminação de duplicação de informações e aumento da transparência.

É fundamental destacar que o modelo de negócios proposto, conforme a figura 7, referente ao capítulo 4, aborda um ciclo de vida completo para a identificação de uma cadeia de custódia digital, com o objetivo de ressaltar a importância e o posicionamento da cadeia de custódia e rastreabilidade da prova digital. Por fim, é possível inferir que a tecnologia *blockchain* pode contribuir para mitigar possíveis erros ou fraudes em organizações públicas, oferecendo garantias fundamentais previstas em leis aos titulares dos dados.

6.2 RESPOSTA À PERGUNTA DE PESQUISA

PP 1 – quais são os principais desafios na preservação dos dados lógicos durante investigações forenses e por que necessita de um modelo computacional?

A preservação da integridade dos dados lógicos durante investigações forenses é crucial, mas enfrenta vários desafios substanciais. A possibilidade de alterações, corrupções ou contaminações nos dados é uma ameaça significativa, comprometendo a integridade dos dados originais e, consequentemente, a validade das evidências.

Assegurar a autenticidade e a rastreabilidade dos dados coletados é essencial. A falta de procedimentos adequados para o registro e rastreamento pode diminuir a credibilidade das evidências apresentadas, tornando fundamental garantir a origem confiável da coleta dos dados. A cadeia de custódia, envolvendo o registro detalhado de manuseios, acessos e mudanças nos dados, é outro ponto importante para a admissibilidade das evidências digitais em processos judiciais.

A complexidade tecnológica, com uma variedade de dispositivos, sistemas operacionais e tecnologias, torna a coleta e a preservação de dados desafiadoras. Para lidar com essa multiplicidade, apresentou-se, neste trabalho, um modelo computacional para uma possível solução. Esse modelo propõe respeitar os direitos de privacidade e a conformidade legal, como a LGPD na obtenção e análise de dados que devem seguir, estritamente, os limites legais estabelecidos. Ainda há o risco de destruição acidental ou intencional de dados relevantes durante a investigação, exigindo a implementação de medidas preventivas para proteger os dados contra perda ou exclusão, que não fez parte desse trabalho.

PP 2 – como a evolução das tecnologias disruptivas, em especial *Blockchain*,

pode melhorar a cadeia de custódia digital em investigações forenses, sem ofender a legislação de proteção de dados?

A evolução das tecnologias disruptivas, apresenta um potencial significativo para aprimorar, consideravelmente, a cadeia de custódia digital em investigações forenses. A tecnologia *blockchain* tem características cruciais para o fortalecimento da integridade, autenticidade e rastreabilidade das evidências digitais em processos. Uma vez que se registram os dados em um bloco, eles se tornam praticamente imutáveis. Isso permite a integridade das informações ao longo do tempo, reduzindo, substancialmente, a possibilidade de adulterações ou manipulações não autorizadas.

Além disso, o *Blockchain* oferece transparência e rastreabilidade. Registra-se cada inclusão ou acesso às evidências em um bloco e distribui-se esta em uma rede descentralizada de participantes. Isso significa que os investigadores rastreiem a origem e a manipulação dos dados, desde sua criação até o descarte da evidência.

Ressalta-se outro ganho na simplificação dos processos, pois, o *Blockchain* reduz a possibilidade de erros ou manipulações, proporcionando um sistema mais eficiente e confiável de preservação e documentação de evidências.

PP 3 – quais são os principais impactos da LGPD nas práticas de investigação forense e na cadeia de custódia digital da solução proposta?

Inspirada em padrões internacionais de proteção de dados pessoais conforme revisado no capítulo 2. Atualmente, autoridades e peritos forenses são obrigados a aderir, rigorosamente, aos protocolos estabelecidos para obter, processar e preservar evidências digitais, assegurando-se do consentimento ou embasamento legal para acesso a dados pessoais.

A cadeia de custódia digital, fundamental para a documentação minuciosa do percurso e administração das evidências digitais, também sofre influência direta da LGPD, que implica a necessidade de uma documentação extremamente detalhada das atividades realizadas, a fim de assegurar que não ocorram violações e que todas as etapas estejam em estrita conformidade com a legislação vigente.

Diante desses impactos, a proposta de solução apresentada neste trabalho deve demonstrar como se adaptar às exigências da LGPD, especialmente ao respeitar os direitos fundamentais, ao modelar uma solução computacional capaz de auxiliar no entendimento do domínio do problema.

PP 4 – qual a lacuna existente na regulamentação atual em relação à cadeia de custódia digital, proteção de dados e a *blockchain* e como ela é coberta nesta

pesquisa?

No contexto atual das regulamentações, é evidente a presença de lacunas significativas no que concerne à gestão da cadeia de custódia digital e à manipulação de evidências digitais. As normas em vigor carecem de uniformidade e diretrizes abrangentes para assegurar a integridade da cadeia de custódia digital em investigações forenses. Essa carência pode resultar em disparidades nos procedimentos adotados por diferentes entidades ou jurisdições, comprometendo, a confiabilidade e admissibilidade das evidências digitais em processos legais. A ausência de orientações claras sobre a aplicação de tecnologias como a *Blockchain* na gestão da cadeia de custódia digital e na preservação de evidências pode gerar incertezas quanto à sua aceitação e eficácia nos processos judiciais.

Embora leis como a LGPD representem avanços, ainda persiste uma falta de clareza sobre como aplicar tais princípios em investigações forenses, especialmente a respeito da utilização de dados sensíveis como evidências. A interseção entre a preservação da integridade das evidências e o respeito à privacidade dos indivíduos e as tecnologias disruptivas requer um equilíbrio delicado que, frequentemente, não está definido nas regulamentações existentes. Neste estudo, busca-se validar um modelo computacional capaz de abordar algumas das lacunas e ambiguidades relacionadas à coleta e registro na cadeia de custódia digital, apresentando, assim, uma solução robusta para a intersecção desses três domínios.

PP 5 – quais são os impactos das inovações tecnológicas na evolução das leis de proteção de dados e sua aplicação em investigações forenses?

O aumento exponencial da interdependência global e a expansão do volume de dados digitais têm confrontado os sistemas legais em escala mundial, demandando ajustes regulatórios contínuos para acompanhar a rápida evolução tecnológica e garantir a proteção dos direitos individuais. A acelerada progressão das inovações, nas ferramentas forenses, apresenta tanto desafios quanto oportunidades significativas. Enquanto as novas metodologias e ferramentas promovem investigações mais eficientes, capacitadas para lidar com grandes volumes de dados, elas também levantam preocupações sobre a integridade das evidências digitais, a rastreabilidade dos dados coletados e a preservação dos direitos individuais durante o processo investigativo.

Destacaram-se, neste estudo, questões éticas e legais que surgem ao buscar um equilíbrio entre a obtenção de informações para fins investigativos e a proteção

dos direitos dos indivíduos. A colaboração entre especialistas em tecnologia, juristas e legisladores é de extrema importância para elaborar legislações aptas a enfrentar os desafios em constante mutação decorrentes das inovações tecnológicas.

PP 6 – os métodos propostos são eficientes para melhorar a transparência?

A garantia da transparência processual na cadeia de custódia digital é um elemento crucial para preservar a integridade das evidências digitais em processos judiciais. Diversos métodos e práticas se mostram eficazes para assegurar essa transparência e confiabilidade ao longo do ciclo de vida dos dados digitais. Nesta dissertação, utilizou-se um método que atende aos requisitos para fechar uma parte da lacuna aberta nos três domínios do problema discutido no capítulo 2.

A utilização de tecnologias baseadas em *blockchain*, apresentada nesta pesquisa, constitui uma abordagem promissora. Ela oferece um registro descentralizado, contribuindo para assegurar a integridade dos dados ao longo do tempo e viabilizando uma verificação independente de qualquer alteração na cadeia de custódia.

Verificou-se, no experimento realizado, que se alcança a transparência na cadeia de custódia digital por meio da implementação conjunta de registros detalhados, técnicas de criptografia e tecnologias inovadoras. Esses métodos combinados são uma base sólida para uma solução robusta das evidências digitais em processos judiciais.

PP 7 – como a utilização de uma cadeia de custódia digital compartilhada pode beneficiar o sistema judicial e a rastreabilidade das evidências digitais?

No contexto contemporâneo, a crescente digitalização dos processos e a proliferação de evidências digitais têm sido um desafio para o sistema judicial. Nesse sentido, a utilização de uma cadeia de custódia *online* compartilhada surge como uma solução fundamental para aprimorar o sistema judicial e desfrutar de todo o pontencial que existe nas inovações tecnológicas.

Em relação ao experimento realizado nesta dissertação, compreendeu-se a importância desses resultados para o contexto legal. Demonstrou-se o resultado de registro documentado e ininterrupto do histórico de posse, controle, transferência, análise e preservação de evidências. Evidenciou-se, nesse sentido, que a tecnologia proporciona a transparência ao processo, permitindo que as partes interessadas tenham acesso às informações sobre a evidência desde sua coleta até sua apresentação em tribunal. Isso promove a confiança no sistema, reduzindo

potenciais questionamentos sobre a autenticidade e a integridade das provas.

A utilização de um modelo computacional com essas características agiliza o fluxo de informações entre os diferentes intervenientes do processo judicial, como advogados, juízes, peritos e órgãos de interesse. Essa agilidade pode reduzir os prazos de resolução dos casos, contribuindo para a eficiência do sistema judicial.

Por fim, a implementação de uma cadeia de custódia *online* também pode reduzir custos operacionais, uma vez que simplifica e automatiza parte do processo de gestão de evidências, minimizando erros humanos e otimizando recursos.

PP 8 – como as práticas de cadeia de custódia digital podem ser aprimoradas para manter a conformidade com a LGPD sem comprometer a eficácia das investigações forenses?

A proposta realizada neste estudo científico é para aprimorar as práticas de cadeia de custódia digital e manter a conformidade com a LGPD sem comprometer a eficácia das investigações forenses. O uso de técnicas que preservem os dados sensíveis é uma das estratégias mais eficazes. Isso permite ocultar ou substituir informações pessoais, mantendo a integridade das evidências sem comprometer a identidade dos envolvidos.

A solução mostrou que é possível manter registros precisos de todas as etapas da cadeia de custódia digital, incluindo quem teve acesso aos dados, quando e por quê. Isso é essencial para assegurar a conformidade com a LGPD. Essa documentação adequada pode validar a legitimidade das informações obtidas. Ela é a harmonização entre a proteção de dados pessoais e a eficácia das investigações é um desafio em constante atualização que requer equilíbrio e estratégias cuidadosas para preservar tanto a integridade quanto a rastreabilidade das evidências.

6.3 RESULTADOS OBTIDOS

Para a realização dos testes, criou-se um contrato inteligente utilizando o ambiente descrito no capítulo 3 para validar a proposta, analisaram-se três cenários.

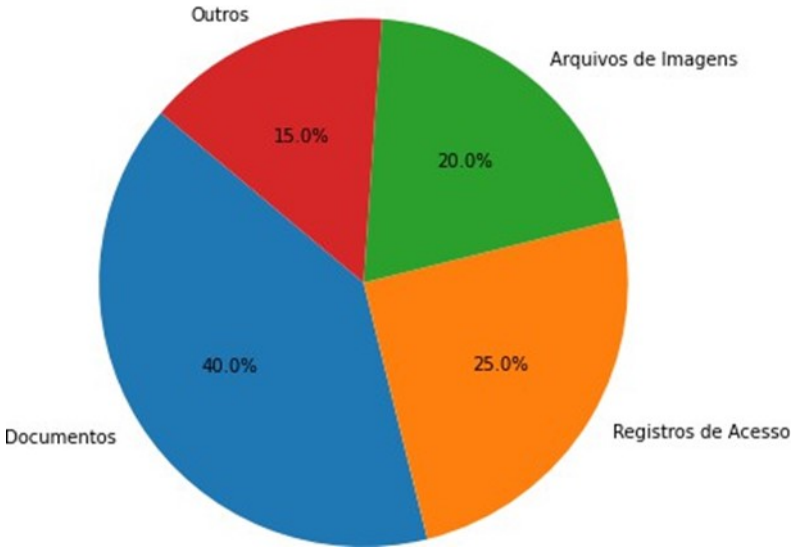
O estabelecimento do primeiro cenário de teste foi concebido com o propósito de representar a distribuição das evidências de forma categorizada, considerando tipos específicos: documentos, registros de acesso, imagens de arquivos e outras formas de evidência. Essa segmentação inicial permitiu identificar que as marcações atribuídas às evidências possuem a capacidade de facilitar a separação dos dados

por categoria, viabilizando o acesso seletivo por parte dos intervenientes envolvidos no processo.

A condução de 200 solicitações de coleta de evidências na *blockchain*, conforme a figura 8, considerando tais tipos de classificação, demonstrou a utilidade e eficácia da proposta de categorização no contexto da economia de armazenamento externo. Por exemplo, constatou-se que, aproximadamente, 40% das evidências classificadas como "documentos"poderiam ser descartadas em situações forenses específicas relacionadas, apenas, a imagens.

Essa abordagem estruturada revelou-se vantajosa não apenas na categorização e acesso seletivo dos dados, mas também na potencial economia de recursos de armazenamento, indicando a relevância prática e operacional da proposta para otimização de processos forenses e gerenciamento de evidências em ambientes relacionados à *blockchain*.

Figura 9 – distribuição de tipos de evidência

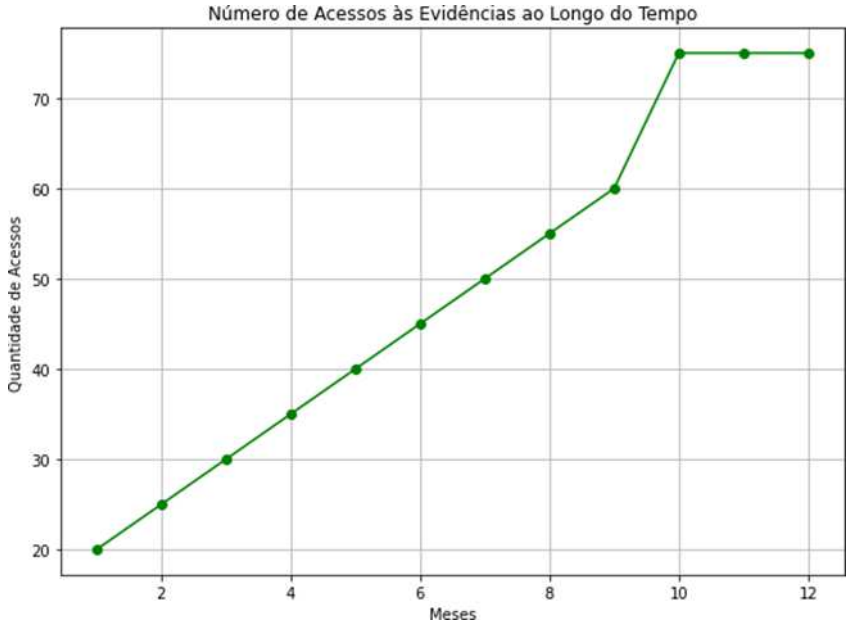


Fonte: próprio Autor.

O segundo cenário de teste mostra a evolução temporal do número de acessos às evidências ao longo de 12 meses, conforme o gráfico 9. Utilizaram-se, no experimento realizado nesse segundo cenário, dados simulados (Apêndice 1) para representar o número mensal de acessos a evidências digitais ao longo de um período de 12 meses. A análise do gráfico revela padrões e flutuações nos acessos mensais às evidências, bem como a estabilização da quantidade de acesso quando os nós atingem um equilíbrio.

A análise desses padrões temporais pode contribuir, significativamente, para a preservação da integridade das evidências digitais, mantendo sua admissibilidade e confiabilidade em procedimentos legais. O entendimento das tendências de acesso ao longo do tempo é importante para manter a integridade e a validade das evidências, reforçando a importância do controle rigoroso dentro deste contexto.

Figura 10 – número de acesso às evidências

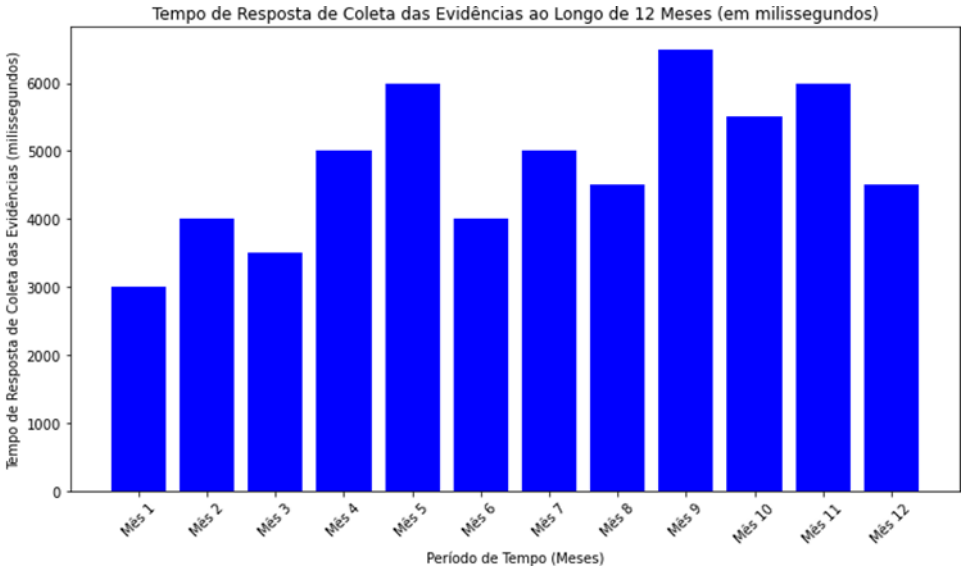


Fonte: próprio Autor.

O terceiro cenário de teste do experimento apresenta uma simulação de coleta de evidências digitais ao longo de um período de 12 meses, com foco na medição dos tempos em milissegundos despendidos nesse processo, conforme o gráfico 10.

O experimento realizado visa identificar padrões, tendências ou discrepâncias nos tempos consumidos para a coleta das evidências digitais em meses distintos, com o intuito de verificar a viabilidade de sua utilização. Dentre os objetivos, destaca-se a possibilidade de identificar meses com tempos de resposta mais elevados ou inferiores, sugerindo áreas potenciais de melhoria no processo de coleta, considerando as configurações da infraestrutura local. Além disso, a análise possibilita a detecção de tendências temporais, fornecendo suporte para a previsão de demandas futuras e a implementação de estratégias para otimizar o tempo de resposta em uma rede *blockchain*.

Figura 11 – Quantidade de acesso no tempo



Fonte: próprio Autor.

6.4 CONSIDERAÇÕES FINAIS

Neste capítulo, apresentou-se uma análise e discussão sobre os resultados obtidos no experimento realizado e também as respostas de perguntas de pesquisas. No próximo capítulo, apresentam-se as conclusões e trabalhos futuros.

7 CONCLUSÕES E TRABALHOS FUTUROS

7.1 CONCLUSÕES

A execução de uma pesquisa abrangendo os três temas centrais do domínio do problema em estudo proporcionou uma extensa bibliografia proveniente da comunidade acadêmica internacional. Contudo, destaca-se a escassez de estudos centrados na legislação brasileira. Da mesma forma, verifica-se uma lacuna nos trabalhos relacionados à tecnologia disruptiva, como a blockchain, especialmente no contexto das frentes governamentais que buscam integrar temas de grande relevância para a sociedade. Essas considerações ampliaram a abordagem deste trabalho, permitindo uma análise mais abrangente da maturidade e do comportamento da União Europeia, considerando as semelhanças nas disposições legais apresentadas. Diante disso, acredita-se que a proposta apresentada neste estudo é relevante para a comunidade acadêmica e também para a indústria, abrindo caminho para a utilização de novas tecnologias em ambientes jurídicos que mantêm dados pessoais.

A contaminação de documentos apreendidos compromete a integridade jurídica e suscita dúvidas quanto à possível inserção fraudulenta de determinados eventos, consequentemente descredibilizando provas de elevada relevância. A cadeia de custódia, adicionalmente, desempenha o papel de associar um artefato físico a um sujeito. Como desígnio primordial, a documentação pormenorizada de todas as diligências e transferências de evidências entre os agentes, desde a coleta lógica de dados, deve ser escrupulosamente verificável, assegurando que nenhuma outra entidade tenha alterado ou acessado tais evidências.

Embora os avanços científicos possam contribuir com as ciências forenses no sentido de aprimorar a capacidade de reunir evidências suficientes para a solução das questões levadas à Justiça, tais evidências, particularmente aquelas relacionadas com a necessidade posterior de exames laboratoriais, como são as provas digitais, só podem ser aceitas como meios de prova se a coleta, o manuseio e a análise das amostras observarem condições mínimas de segurança de modo a garantir a integridade do material a ser examinado e a idoneidade dos meios empregados. A tecnologia de cadeia de blocos por design impõe integridade, transparência, autenticidade e auditabilidade, tornando-se possivelmente a melhor escolha para manter e rastrear a cadeia de custódia forense. O Blockchain ajuda na redução de

conflitos por meio do aumento da confiança e, portanto, traz a verdadeira promessa para a comunidade jurídica e forense. Atualmente, existe uma aparente tensão entre a aplicação da tecnologia *blockchain* e a Lei de Proteção de Dados na legislação do Brasil. É difícil conciliar a forma de governança “descentralizada”, como as novas tecnologias, com uma estrutura legal que visa regular um sistema de gerenciamento de dados centralizado. O conflito substancial entre o LGPD e a tecnologia descentralizada resulta em um alto nível de insegurança jurídica neste campo. Para resolver o conflito, a questão deve ser observada tanto do ponto de vista legal quanto técnico. Assim, uma das maneiras de garantir a compatibilidade da proteção de dados e da tecnologia blockchain é adotar a lei de proteção de dados às mudanças tecnológicas nos entes públicos.

Em resposta à hipótese H1 de adequação das tecnologias utilizadas ao contexto da Cadeia de Custódia Digital e à Legislação de Proteção de Dados, o modelo proposto emprega contratos inteligentes. A natureza transparente e rastreável da *blockchain* se mostrou promissora para o cumprimento das exigências de conformidade com a legislação de proteção de dados, e requer não apenas a seleção criteriosa de tecnologias, mas também a implementação efetiva de políticas e práticas relacionadas ao gerenciamento de dados. Em relação à hipótese H2, os impactos previstos em cada um desses domínios críticos possuem a capacidade de afetar a conformidade e a eficácia do modelo proposto de gestão de evidências. Reduzir esses impactos requer uma abordagem holística, abrangendo não apenas aspectos tecnológicos, mas também práticas, políticas e regulamentações para aperfeiçoar a rastreabilidade e integridade das evidências.

A contribuição deste trabalho se dá em três segmentos: a primeira nas questões legais onde é apresentado uma análise aprofundada de cruzamento de conceitos legislativos relacionados a princípios de proteção de dados e procedimentos de cadeia de custódia. A segunda contribuição é a identificação da lacuna legislativa encontrada a partir dessa análise que abre espaço para futuras propostas no campo estritamente legal e, por fim, a apresentação de uma proposta de um modelo computacional que é o resultado da compilação de estudos científicos e técnicos a respeito da importância da proteção de dados e da cadeia de custódia para trazer provas processuais mais confiáveis. Explorou-se o potencial das tecnologias atuais desenvolvendo uma prova de conceito e analisando os resultados dos experimentos apresentados, nesta dissertação, para que outros pesquisadores possam reproduzir

os resultados e aplicá-los na indústria. Para avançar nesta pesquisa futuramente, é necessário buscar o encaixe das legislações com foco em interoperabilidade entre duas *blockchains*.

REFERÊNCIAS

AL-KHATEEB HAIDER E EPIPHANIOU, Gregory e Daly Herbert. Blockchain para análise forense digital moderna: A cadeia de custódia como um livro razão distribuído. *In*: **Blockchain and Clinical Trial**. *[S.l.]*: Springer, 2019. p. 149–168.

ALRUWAILI, Fahad F. Custodyblock: A distributed chain of custody evidence framework.
Information, Multidisciplinary Digital Publishing Institute, v. 12, n. 2, p. 88, 2021.

ALSENOY, Brendan Van. Regulating data protection: the allocation of responsibility and risk among actors involved in personal data processing. 2016.

BAARS, DS. **Towards self-sovereign identity using blockchain technology**. 2016. Dissertação (Mestrado) — University of Twente, 2016.

BARTLETT, Sean Richard. **Reconciling blockchain technology with the General Data Protection Regulation in light of controllership and the rights of data subjects.** 2021. Dissertação (Mestrado), 2021.

CASEY, Eoghan; BACK, Greg; BARNUM, Sean. Leveraging cybox™ to standardize representation and exchange of digital forensic information. **Digital Investigation**, Elsevier,
v. 12, p. S102–S110, 2015.

CHAUDHRY, Natalia; YOUSAF, Muhammad Murtaza. Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. *In*: IEEE. **2018 12th International Conference on Open Source Systems and Technologies (ICOSST)**. *[S.l.]*, 2018. p. 54–63.

CLACK, Christopher D; BAKSHI, Vikram A; BRAINE, Lee. Smart contract templates: foundations, design landscape and research directions. **arXiv preprint arXiv:1608.00771**, 2016.

COSIC, Jasmin. Formal acceptability of digital evidence. *In*: **Multimedia Forensics and Security**. *[S.l.]*: Springer, 2017. p. 327–348.

COSIC, Jasmin; COSIC, Zoran. Chain of custody and life cycle of digital evidence. **Computer technology and application**, David Publishing Company, Inc., v. 3, n. 2, 2012.

ĆOSIĆ, Jasmin; ĆOSIĆ, Zoran; BAČA, Miroslav. An ontological approach to study and manage digital chain of custody of digital evidence. **Journal of Information and Organizational Sciences**, Fakultet organizacije i informatike Sveučilišta u Zagrebu, v. 35, n. 1, p. 1–13, 2011.

CUNHA, Rogério Sanches. Pacote anticrime. **Salvador: JusPodivm**, 2020.
DANNEN, Chris. **Introducing Ethereum and solidity**. *[S.l.]*: Springer, 2017. v. 1.

EBERHARDT, Jacob; TAI, Stefan. On or off the blockchain? insights on off-chaining computation and data. *In*: PAOLI, Flavio De; SCHULTE, Stefan; JOHNSEN, Einar Broch (Ed.). **Service-Oriented and Cloud Computing**. Cham: Springer International Publishing, 2017. p. 3–15.

EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, v. 120, p. 237–257, 2016.

EUROPEIA, E DA UNIÃO. Análise comparativa entre os princípios informadores do regulamento geral de proteção de dados da União Europeia e as normas do direito brasileiro. 2019.

EWALD, Uwe. Digital forensics vs. due process: Conflicting standards or complementary approaches? *In*: **Proceedings of the Third Central European Cybersecurity Conference**. *[S.l.: s.n.]*, 2019. p. 1–2.

FINCK, Michèle. **Blockchain regulation and governance in Europe**. *[S.l.]*: Cambridge University Press, 2018.

GIOVA, Giuliano *et al.* Improving chain of custody in forensic investigation of electronic digital systems. **International Journal of Computer Science and Network Security**, v. 11, n. 1,
p. 1–9, 2011.

JABAREEN, Yosef. Building a conceptual framework: philosophy, definitions, and procedure.
International journal of qualitative methods, SAGE Publications Sage CA: Los Angeles, CA,
v. 8, n. 4, p. 49–62, 2009.

JUNIOR, Aury LOPES; ROSA, Alexandre Morais da. A importância da cadeia de custódia para preservar a prova penal. **Revista Consultor Jurídico,[S. l.]**, 2015.

KOLVART, Merit; POOLA, Margus; RULL, Addi. Smart contracts. *In*: **The Future of Law and etechnologies**. *[S.l.]*: Springer, 2016. p. 133–147.

KRAFT, Daniel. Difficulty control for blockchain-based consensus systems. **Peer-to-peer Networking and Applications**, Springer, v. 9, n. 2, p. 397–413, 2016.

KUNER, Christopher; BYGRAVE, Lee; DOCKSEY, Christopher; DRECHSLER, Laura. **The EU General Data Protection Regulation: A Commentary**. *[S.l.]*: Oxford University Press. Available at: https://global. oup. com/academic . . . , 2020.

LONE, Auqib Hamid; MIR, Roohie Naaz. Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer. **Digital investigation**, Elsevier, v. 28, p. 44–55, 2019.

LONE, Auqib Hamid; MIR, Roohie Naaz. Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer. **Digital Investigation**, v. 28, p. 44–55, 2019. ISSN 1742-2876. Disponível em:

https://www.sciencedirect.com/science/article/pii/ S174228761830344X.

MANTEGHI, Maryna. Blockchain and the european union's general data protection regulation: from conflict to "peaceful" coexistence? **Available at SSRN 3805647**, 2021.

MARTINEZ, Pablo Dominguez. Direito ao esquecimento: a proteção da memória individual na sociedade da informação. **Rio de Janeiro: Lumen Juris**, p. 30–35, 2014.

MASSENO, Manuel David; MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. A segurança na proteção de dados: Entre o rgpd europeu e a lgpd brasileira. **Revista do CEJUR/TJSC: Prestação Jurisdicional**, v. 8, n. 1, p. e346–e346, 2020.

MATIDA, Janaina *et al.* A cadeia de custódia é condição necessária para a redução do riscos de condenações de inocentes. **Revista da Defensoria Pública do Estado do Rio Grande do Sul**,
n. 27, p. 17–26, 2020.

MINGXIAO, Du; XIAOFENG, Ma; ZHE, Zhang; XIANGWEI, Wang; QIJUN, Chen. A review
on consensus algorithm of blockchain. *In*: IEEE. **2017 IEEE international conference on systems, man, and cybernetics (SMC)**. *[S.l.]*, 2017. p. 2567–2572.

MONTEIRO, Renato Leite. Existe um direito à explicação na lei geral de proteção de dados do brasil. **Artigo estratégico**, n, v. 39, p. 1–14, 2018.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159–180, 2018.

NUNES, Cláudia Mietlicki. Lei 13.709/18–lei geral de proteção de dados (lgpd) e os reflexos no campo da pesquisa clínica. **Revista de Direito, Governança e Novas Tecnologias**, v. 5, n. 2, p. 92–107, 2019.

POP, Claudia; ANTAL, Marcel; CIOARA, Tudor; ANGHEL, Ionut; SERA, David; SALOMIE, Ioan; RAVEDUTO, Giuseppe; ZIU, Denisa; CROCE, Vincenzo; BERTONCINI, Massimo. Blockchain-based scalable and tamper-evident solution for registering energy data. **Sensors**, MDPI, v. 19, n. 14, p. 3033, 2019.

PRADO, Geraldo. A cadeia de custódia da prova no processo penal. **São Paulo: Marcial Pons**, 2019.

PRAYUDI, Yudi; SN, Azhari. Digital chain of custody: State of the art. **International Journal of Computer Applications**, Foundation of Computer Science, v. 114, n. 5, 2015.

RIEGER, Alexander; LOCKL, Jannik; URBACH, Nils; GUGGENMOS, Florian; FRIDGEN, Gilbert. Building a blockchain application that complies with the eu

general data protection regulation. **MIS Quarterly Executive**, v. 18, n. 4, 2019.

SALMENSUU, Cagla. The general data protection regulation and the blockchains. **Liikejuridiikka**, v. 1, 2018.

SANTOS, André Luis Mattos; SILVA, Rubens Alves Da. Proteção dos dados pessoais no ordenamento jurídico brasileiro com advento da lei 13.709 de 2018. **Revista Artigos. Com**, v. 7,
p. e1869–e1869, 2019.

SHAH, Pritesh; FORESTER, Daniel; BERBERICH, M; RASPÉ, C; MUELLER, H. Blockchain
technology: Data privacy issues and potential mitigation strategies. **Practical Law**, 2019.

SHUKLA, Parth Anand; SAMET, Saeed. Systematization of knowledge on scalability aspect of blockchain systems. *In*: SPRINGER. **Future of Information and Communication Conference**. *[S.l.]*, 2020. p. 130–138.

SILVA, Lucas Gonçalves da; CARVALHO, Mariana Amaral. Direito ao esquecimento na sociedade da informação: análise dos direitos fundamentais no meio ambiente digital. **Revista Brasileira de Direitos e Garantias Fundamentais**, v. 3, n. 2, p. 66–86, 2017.

SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; PADRÃO, Vinicius. Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais. **Direito Público**, v. 16, n. 90, 2019.

TAŞ, Ruhi; TANRIÖVER, Ömer Özgür. Building a decentralized application on the ethereum blockchain. *In*: IEEE. **2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)**. *[S.l.]*, 2019. p. 1–4.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na lgpd: estudo sobre as bases legais. **Civilistica. com**, v. 9, n. 1, p. 1–38, 2020.

TOYODA, Kentaroh; MACHI, Koji; OHTAKE, Yutaka; ZHANG, Allan N. Function-level bottleneck analysis of private proof-of-authority ethereum blockchain. **IEEE Access**, IEEE, v. 8,
p. 141611–141621, 2020.

VELHO, Jesus Antônio *et al.* Tratado de computação forense. **Campinas, SP: Millenium Editora**, 2016.

ZHENG, Zibin; XIE, Shaoan; DAI, Hong-Ning; CHEN, Xiangping; WANG, Huaimin. Blockchain challenges and opportunities: A survey. **International journal of web and grid services**, Inderscience Publishers (IEL), v. 14, n. 4, p. 352–375, 2018.

ZHENG, Zibin; XIE, Shaoan; DAI, Hong-Ning; CHEN, Weili; CHEN, Xiangping; WENG, Jian; IMRAN, Muhammad. An overview on smart contracts: Challenges, advances

and platforms. **Future Generation Computer Systems**, Elsevier, v. 105, p. 475–491, 2020.

ZOU, Weiqin; LO, David; KOCHHAR, Pavneet Singh; LE, Xuan-Bach Dinh; XIA, Xin; FENG, Yang; CHEN, Zhenyu; XU, Baowen. Smart contract development: Challenges and opportunities. **IEEE Transactions on Software Engineering**, IEEE, v. 47, n. 10, p. 2084–2106, 2019.