FACULDADE PARA O DESENVOLVIMENTO SUSTENTÁVEL DA AMAZÔNIA
COORDENAÇÃO DO CURSO DE BACHARELADO EM DIREITO

KARYNE LOURDES SILVA KRÜGER

AS INSEGURANÇAS DO TRATAMENTO DE DADOS NO BRASIL

PARAUAPEBAS 2023

KARYNE LOURDES SILVA KRÜGER

AS INSEGURANÇAS DO TRATAMENTO DE DADOS NO BRASIL

Trabalho de Conclusão de Curso (TCC) apresentado à Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Direito para a obtenção do Título de Bacharelado.

Profª Me. Fernanda Lopes de Freitas Rodrigues – Orientadora.

PARAUAPEBAS
2023

KRÜGER, Karyne Lourdes Silva.

AS INSEGURANÇAS DO TRATAMENTO DE DADOS NO BRASIL; Profª Me. Fernanda Lopes de Freitas Rodrigues – Orientadora.

43 f.

Trabalho de Conclusão de Curso (Graduação) - Faculdade para o Desenvolvimento Sustentável da Amazônia - FADESA, Parauapebas – PA, 2023.

Palavras Chave: LGPD; segurança; análise.

Nota: A versão original deste trabalho de conclusão de curso encontra-se disponível no Serviço de Biblioteca e Documentação da Faculdade para o Desenvolvimento Sustentável da Amazônia – FADESA em Parauapebas – PA.

Comitê de Ética Protocolo nº:
Data:

KARYNE LOURDES SILVA KRÜGER

AS INSEGURANÇAS DO TRATAMENTO DE DADOS NO BRASIL

Trabalho de Conclusão de Curso (TCC) apresentado à Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Direito para a obtenção do Título de Bacharel.

Aprovado em: _____/_____/_____.

Banca Examinadora

EM

_____

Profª Espe. Elayne Melonio – Membro

_____

Profª Me. Josele Cristina – Membro

Fernanda R

_____ Profª

Me. Fernanda Lopes de Freitas Rodrigues – Orientadora

Data de depósito do trabalho de conclusão ____/_____/_____

Maicon T

DEDICATÓRIA

Dedico este trabalho ao meu pai falecido e minha mãe que ainda está comigo, agradeço as bases que me deram para me tornar a pessoa que sou hoje. A perda do meu pai foi um grande divisor de águas na minha vida, nunca imaginei como seria um dia sem ele, então quando esse dia chegou, me senti perdida e desamparada.

Todos dias se tornaram difíceis, e acabei enfrentando uma depressão severa, quase desisti do meu curso, no qual sempre tanto sonhei, na verdade quase desisti de tudo, mas recordei-me que havia prometido para ele que terminaria e que me formaria e um dia seria uma excelente profissional.

Ele sempre me incentivou e acreditou no meu potencial e agora na fase final eu jamais poderia esquecer dele, de todas vezes que ele fazia o esforço para me buscar na instituição, de quando ajudou com livros ou até mesmo na coleção de canetas que faço como uma forma de manter viva a vontade que tinha de estudar.

Nunca me esquecerei do dia que fiquei de recuperação na matéria de processo penal, e chorei muito pois me sentia ignorante por ter conseguido aprender o conteúdo, e ele me disse “minha filha de todo esse tempo no seu curso essa sua primeira nota baixa e a primeira vez fica de recuperação e não te faz burra, você é muito inteligente e isso acontece com todo mundo.”

Minha mãe, depois do falecimento do meu pai parou sua vida para cuidar de mim e do meu irmão que sofríamos muito, eles dois não viviam mais juntos a certo tempo, e mesmo sendo dois adultos ela não deixou de se preocupar nenhum dia conosco.

Sou grata por pegar no meu pé todos dias para que eu estudasse e me dedicasse para que pudesse ter um futuro, a minha mãe é uma pessoa simples vinda de uma cidade do interior e sempre disse que só com estudo poderia ter um futuro melhor.

Agora na reta final, vem uma frase que sempre ouvia do meu pai desde quando era uma criança “ podem tirar tudo de você, menos o seu conhecimento”, obrigado pai e mãe.

Não menos importante, dedico ao meu filho que é um criança atípica e que me fez querer continuar para poder proporcionar uma vida melhor para ele.

AGRADECIMENTOS

Ao meu irmão que estava lá comigo no começo de tudo, sempre me incentivou e me ajudou a persistir, ao meu marido que se tornou crucial nessa reta final, ele me apoiou imensamente, além de ser totalmente compreensível quando estive ausente.

RESUMO

O tratamento de dados tem se tornado uma prática cada vez mais comum em todo o mundo, tanto no ambiente pessoal quanto profissional. Com a crescente digitalização de informações, tornou-se essencial a proteção desses dados para garantir a privacidade e segurança dos indivíduos envolvidos. No entanto, no Brasil, a segurança no tratamento de dados ainda é um desafio a ser enfrentado. Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), em setembro de 2020, o país deu um importante passo para a regulamentação e proteção dos dados pessoais. No entanto, ainda há muitas lacunas a serem preenchidas e desafios a serem superados, especialmente em relação à implementação da lei e à conscientização da população sobre a importância da proteção de dados. Este trabalho tem como objetivo analisar as inseguranças no tratamento de dados no Brasil, desde a coleta até o armazenamento e compartilhamento, levando em consideração os desafios da implementação da LGPD e a conscientização da população sobre a importância da proteção de dados. Serão abordados temas como o vazamento de dados, a falta de transparência no uso das informações pessoais, a vulnerabilidade das empresas em relação a ataques cibernéticos, entre outros. A Lei Geral de Proteção de Dados (LGPD) é tidos como algo muito significativo - principalmente por profissionais do Direito Digital - para a segurança da privacidade no Brasil, afetando variados ramos e empresas. Por ser de tamanha relevância é ainda bastante recente, é primordial que alguns detalhes sejam mais aprofundados. Por meio desta análise, espera-se contribuir para o debate sobre a segurança no tratamento de dados no Brasil e fornecer subsídios para a conscientização da população e para aprimorar as políticas públicas e privadas relacionadas à proteção de dados.

Palavras-chave: LGPD; segurança; análise.

ABSTRACT

Data processing has become an increasingly common practice around the world, both in personal and professional environments. With the increasing digitization of information, it has become essential to protect this data to ensure the privacy and security of the individuals involved. However, in Brazil, security in data processing is still a challenge to be faced. With the entry into force of the General Data Protection Law

(LGPD) in September 2020, the country took an important step towards the regulation and protection of personal data. However, there are still many gaps to be filled and challenges to be overcome, especially in relation to the implementation of the law and raising public awareness of the importance of data protection. This work aims to analyze the insecurities in data processing in Brazil, from collection to storage and sharing, taking into account the challenges of implementing the LGPD and raising awareness of the population about the importance of data protection. Topics such as data leakage, the lack of transparency in the use of personal information, the vulnerability of companies in relation to cyber attacks, among others, will be addressed. The General Data Protection Law (LGPD) is seen as something very significant - mainly by Digital Law professionals - for privacy security in Brazil, affecting various branches and companies. Because it is of such relevance and still quite recent, it is essential that some details are more in-depth. Through this analysis, it is expected to contribute to the debate on data security in Brazil and provide subsidies for raising public awareness and improving public and private policies related to data protection.

Keywords: LGPD; security; analysis.

LISTAS DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
IBGE - Instituto Brasileiro de Geografia e Estatística
SciELO - Scientific Electronic Library Online
TCC - Trabalho de Conclusão de Curso

SUMÁRIO

1.INTRODUÇÃO 10

2. CONCEITUAÇÃO DE DADOS 13

2.1 COMO FUNCIONA O SISTEMA DE DADOS 15

2.2 CONCEITUAÇÃO DA CAPTURA DE DADOS 16

3 DA LEGISLAÇÃO DA PROTEÇÃO DOS DADOS 18

3.1 DA LEGISLAÇÃO PROTETIVA ANTERIOR 18

3.2 LEGISLAÇÃO INTERNACIONAL DE PROTEÇÃO DE DADOS 21

3.3 LEI GERAL DE PROTEÇÃO DE DADOS 22

3.4 DADOS SENSÍVEIS E DADOS PESSOAIS 28

3.5 DIFERENCIAÇÃO DOS TRATADORES DOS DADOS 28

4. SEQUESTRO DE DADOS 29

5. SANÇÕES 29

6. METODOLOGIA 36

7. CONCLUSÃO 38

REFERÊNCIAS BIBLIOGRÁFICAS 41

1. INTRODUÇÃO

É importante entender a situação atual da sociedade várias mudanças devido à inovação tecnológica cada vez mais acelerada e muitas vezes no campo da informação, e isso afeta diretamente as relações mútuas das pessoas e suas próprias vidas. Houve muitas mudanças, atividades e situações antes deles sempre realizadas pessoalmente, mas hoje em dia muitos tomaram forma virtual que muda a forma como nos comunicamos. Nesta nova configuração passaram a ser sociais, onde a troca de informações e dados é contínua o núcleo de um gigantesco sistema financeiro virtual. Para quais mídias digitais oferecem seus serviços aos usuários sem eles pagarem diretamente a taxa, a situação não é clara financeiramente. Mesmo que não haja recibos bancários ou débito em conta acesso a um determinado site ou rede social, um objetivo financeiro, neste caso com base na coleta de dados do usuário, que na maioria dos casos fornece eles sem saber. Assim, ocorre a coleta de dados, que além de passar tratamento, que em muitos casos é vendido ou compartilhado com terceiros, gerando grandes somas de dinheiro, resultando em um mercado baseado em publicidade direcionada (GUIMARÃES, 2015).

Como aponta Krieger (2019), pode-se referir à luz desse cenário por exemplo, ferramentas de armazenamento chamadas cookies, dispositivos de mídia dos usuários, rastreando sua navegação e pesquisas. oh resulta na segmentação em várias classes com uma certa correlação marketing e comunicação de informação. Então percebe-se que o usuário tem tempo para proteger, coletar, armazenar e receber suas informações de publicidade de acordo com seus gostos e preferências.

Dada esta premissa, se não é regulamentação, invasão de dados pessoais a qualquer indivíduo, mesmo que viole os direitos dos proprietários relacionados às suas informações usadas por empresas para fins financeiros sem as suas o proprietário sabe que sua vida íntima online é comercializada. Isso é uma razão para pensar na proteção de dados pessoais, que são pessoais quando for necessário proteger a privacidade de cada usuário. De lá você pode ter 10 para prever legislação sobre o assunto em questão e concordar em se responsabilizar por possíveis danos (KRIEGER, 2019). Pode-se entender que os dados são transmitidos em todos os lugares Na Internet, não importa se foi uma busca no Google ou uma compra

Assinatura Netflix, cadastro de perfis em redes sociais ou até mesmo procure um local específico em aplicativos e sites locais. Claramente, todas essas atividades online são ver e analisar como os dados são armazenados e processados, incluindo realocação para outros países, seja para fins comerciais ou mesmo da política como visto neste estudo. Portanto, o comitê recomenda fortemente enfatizar que uma legislação especial é necessária neste caso lida com a proteção de dados pessoais devido a importantes desenvolvimentos técnicos e informações que o planeta dispunha. Globalização e isso propriedades deram valor à informação com resultado óbvio, tornando-se um ativo muito importante no mercado iniciativa pública e privada, portanto “quem tem acesso ele tem acesso aos dados atuais” (PINHEIRO, 2018, p. 50). Então, quando se trata da Lei Geral de Proteção de Dados - LGPD, e daí? não foi totalmente eficaz, é importante observar que este estudo não foi eficaz o objetivo é esclarecer o assunto.

No entanto, é procurado por este estudo, desenvolver a análise neste ambiente acadêmico e compartilhar as lições aprendidas em sua criação. Para fazer a pesquisa, utilizamos a pesquisa bibliográfica e um documento E estruturalmente, o trabalho foi dividido em três capítulos: Primeiro, é apresentado o panorama dos dados pessoais e da cultura da informação; oh a segunda trata do processo de criação da Lei nº 13.709 e; Finalmente, um terceiro discute dos principais conceitos relacionados ao assunto, abordando a oportunidade responsabilidade civil e sanções aplicáveis em caso de violação padrões que definem o assunto.

O objetivo geral deste trabalho de conclusão de curso (TCC) é analisar as inseguranças relacionadas ao tratamento de dados no Brasil, com o intuito de compreender os desafios e as lacunas existentes nesse contexto. Será realizado um estudo abrangente que visa investigar a conceituação de dados, o funcionamento do sistema de dados, a legislação de proteção de dados no Brasil, bem como as sanções aplicáveis em caso de violações.

E os objetivos específicos, é o de conceituar dados e fornecer uma compreensão abrangente dos diferentes tipos de dados existentes, suas características e a importância de sua proteção. Explorar como funciona o sistema de dados, incluindo a coleta, armazenamento, processamento e compartilhamento de informações, a fim de identificar potenciais vulnerabilidades e riscos associados ao tratamento inadequado dos dados.

Analisar a legislação brasileira de proteção de dados, abrangendo tanto a legislação anterior quanto a Lei Geral de Proteção de Dados (LGPD), investigando suas diretrizes, obrigações e implicações legais para as organizações.

Examinar a legislação internacional de proteção de dados e as boas práticas adotadas por outros países, a fim de comparar e contextualizar a legislação brasileira.

Compreender a diferenciação entre dados sensíveis e dados pessoais, destacando a importância da proteção adequada desses tipos de informações. Investigar a relação entre as organizações e os dados tratados, identificando as responsabilidades dos controladores e operadores de dados e as medidas de segurança necessárias para proteger a privacidade e a confidencialidade das informações.

Analisar os casos de sequestro de dados, como ransomware e ataques cibernéticos, para compreender os riscos associados à segurança dos dados e as consequências para as organizações e indivíduos afetados.

Explorar as sanções previstas na legislação brasileira em caso de violações de proteção de dados, analisando as penalidades e os impactos legais e financeiros que as organizações podem enfrentar em caso de não conformidade.

Através desses objetivos, este TCC busca contribuir para o entendimento das inseguranças relacionadas ao tratamento de dados no Brasil, fornecendo um panorama abrangente da conceituação de dados, da legislação de proteção de dados e das possíveis sanções em caso de violações. Espera-se que os resultados deste estudo possam auxiliar na conscientização sobre a importância da proteção de dados e na adoção de práticas mais seguras e responsáveis em relação ao tratamento das informações pessoais no contexto brasileiro.

2. CONCEITUAÇÃO DE DADO

Movida pela General Data Protection Regulation (GDPR) da União Europeia, a Lei Geral de Proteção de Dados (Lei 13.709/18 - LGPD), que vai começar a valer neste ano, traz mudanças significativas na proteção do direito à intimidade e dos dados pessoais como direitos individuais, além de oferecer maior estabilidade jurídica para as organizações, atualizando princípios então dispersos em várias normas segmentares.

Inicialmente, é importante compreender o que é considerado um dado. Em termos gerais, dados são informações em forma bruta, sem organização ou contexto específico. São fatos, observações ou símbolos que podem ser registrados e, posteriormente, processados para gerar conhecimento e insights.

O tratamento de dados é fundamental para o avanço da tecnologia e o uso diário de diversos serviços. No entanto, o Brasil ainda é carente de legislações eficientes para regular o armazenamento e a disseminação de dados. Existe um déficit na conceituação de dados, que pode resultar em uso ilegal dos mesmos. Um exemplo disso é a falta de leis que regulamentem a privacidade dos usuários de redes sociais. Essa insegurança afeta diretamente a manutenção de direitos básicos e a proteção dos dados. Por isso, é necessário reforçar as leis para garantir a segurança e o uso adequado dos dados no Brasil.

De acordo com Maldonado (2019, p.12), apesar dos esforços para garantir a privacidade dos dados pessoais, vivemos em uma era de big data, onde essas informações são manipuladas por empresas ou pessoas, incessantemente, em quantidade nunca observada anteriormente.

Segundo Oliveira (2020, p. 43), quando alguém ouve pela primeira vez sobre a LGPD, pode-se imaginar que ela cobre as informações empresariais, tanto as confidenciais como os dados que identificam uma empresa, como o CNPJ, o endereço ou a data de criação. Porém, ao se observar a legislação com mais atenção, nota-se que ela se destina à proteção dos dados pessoais, não necessariamente excluindo aqueles que podem ser relacionados a uma pessoa jurídica.

A defesa da intimidade tem como objetivo assegurar o crescimento do ser humano, segundo Norbert Elias, no livro “A Sociedade dos indivíduos” (1994). Um

recém-nascido é apenas um esboço inicial de uma pessoa, que desenvolverá a sua individualidade por meio das relações com a sociedade. Por isso, a Lei Geral de Proteção de Dados (LGPD) se concentrou na preservação dos dados pessoais dos indivíduos, visando à proteção da privacidade dessas pessoas, pois as entidades jurídicas não desfrutam desse tipo de defesa.

Os dados podem ser classificados em diferentes tipos, como dados estruturados, não estruturados e semiestruturados. Os dados estruturados são organizados em um formato específico, como tabelas ou bancos de dados, e possuem um esquema predefinido. Já os dados não estruturados não possuem uma organização específica e podem incluir textos, imagens, áudios e vídeos. Os dados semi-estruturados são uma combinação dos dois anteriores, possuindo algum tipo de organização, mas sem uma estrutura rígida.

Dado é um termo utilizado para se referir a informações ou fatos que podem ser armazenados, organizados e processados para produzir conhecimento. Em outras palavras, é um elemento que carrega uma informação sobre um determinado objeto ou evento.

No contexto da tecnologia da informação, os dados são considerados a matéria-prima para a geração de informações e conhecimento. Eles podem ser coletados de diversas fontes, como sensores, dispositivos móveis, redes sociais, formulários online, entre outros.

Por fim, é fundamental salientar que a coleta, armazenamento e tratamento de dados requerem cautela e atenção especial para garantir a segurança e a privacidade dos indivíduos envolvidos. É nesse contexto que a LGPD ganha grande importância no cenário atual, uma vez que estabelece normas para o tratamento de dados pessoais, visando proteger os direitos fundamentais de privacidade e liberdade de expressão.

Os dados desempenham um papel fundamental na sociedade contemporânea. Com o advento da era digital, a quantidade de dados gerados e coletados tem aumentado exponencialmente. Essas informações são utilizadas em diversas áreas, como ciência, tecnologia, saúde, economia, entre outras.

Os dados são a base para a tomada de decisões embasadas e a geração de conhecimento. Eles permitem identificar padrões, tendências e insights que podem levar a melhorias significativas em diversos setores. Além disso, os dados são

utilizados para personalização de serviços, otimização de processos, desenvolvimento de produtos e serviços inovadores, entre outros.

A privacidade e a segurança dos dados são aspectos críticos no tratamento das informações pessoais. A crescente digitalização e a coleta massiva de dados trazem consigo preocupações relacionadas à proteção da privacidade das pessoas. A exposição indevida de informações pessoais pode levar a consequências negativas, como fraudes, roubo de identidade e invasões de privacidade.

Garantir a segurança dos dados é essencial para manter a confiança e o respeito dos usuários. Medidas de proteção devem ser adotadas para prevenir o acesso não autorizado, o vazamento de dados e o uso indevido das informações pessoais.

2.1 COMO FUNCIONA O SISTEMA DE DADOS

A coleta de dados é a primeira etapa do processamento de dados. Os dados podem ser coletados de várias fontes, como formulários, questionários, sensores, dispositivos móveis, etc. É importante ressaltar que a coleta de dados deve obedecer às leis e regulamentações aplicáveis, como a LGPD no Brasil, para garantir privacidade e segurança de dados pessoais.

Depois de coletados, os dados são armazenados em um local seguro, como um banco de dados ou servidor. Os dados devem estar seguros e os dados pessoais devem ser protegidos contra uso não autorizado e fluxos de dados. É importante lembrar que com a digitalização cada vez maior das informações, é necessário implementar medidas de segurança para garantir a privacidade das informações armazenadas. O processamento de dados envolve a organização e análise dos dados coletados. Os dados podem ser processados de várias maneiras, como análise estatística, mineração de dados, aprendizado de máquina, etc.

O objetivo do processamento de dados é produzir informações e insights a partir dos dados coletados. O compartilhamento de informações é uma prática comum em muitos setores. As informações coletadas podem ser compartilhadas com outras empresas, organizações ou indivíduos para diversos fins, como prestação de serviços, pesquisa, publicidade, etc. Para evitar o uso indevido, é importante garantir que as informações sejam compartilhadas com segurança de acordo com as leis e regulamentos aplicáveis de dados pessoais.

Por fim, a informação é utilizada para diversos fins como tomada de decisão, desenvolvimento de produtos e serviços, personalização de experiências, e.g. É importante ressaltar que os dados devem ser utilizados de forma ética e responsável, respeitando a privacidade e a segurança dos dados pessoais.

2.2 CONCEITUAÇÃO DA CAPTURA DOS DADOS

A mineração de dados, também conhecida como mineração de dados, é uma técnica usada para obter informações em formato eletrônico. Esta tecnologia permite ler, extrair e armazenar dados em sistemas de computador. Assim, possibilita a digitalização de documentos, a automatização de processos e a aquisição de informações utilizadas na tomada de decisões. Além disso, a coleta de dados é uma forma eficaz de reduzir custos e melhorar a qualidade do serviço. Portanto, a mineração de dados é um método importante para otimizar o processo de coleta, armazenamento e análise de dados, proporcionando maior velocidade, segurança e precisão.

Na Internet, os usuários tornam-se compradores que comunicam e compartilham suas opiniões sobre suas experiências com determinado bem ou serviço, passam a participar ativamente do ciclo de compra, o que afeta a própria criação do produto ou serviço: são criadores (prosumidores). A web permite assim a classificação gradual dos dados pessoais, tornando-se uma parte importante e transformadora de toda a publicidade, porque oferece experiências cada vez mais individualizadas, oferecendo um cruzamento entre as necessidades dos compradores e o produto certo.

Nessa perspectiva, os dados pessoais dos consumidores são ativos no contexto da economia da informação, pois maximizam o sucesso na promoção do consumo por meio do marketing direcionado. Isso ocorre porque os dados pessoais refletem nossas atividades sociais e individualidade.

Nesta realidade, a capacidade de obtenção de informação atingiu um nível surpreendente, permitindo o acesso a dados de consumo recolhidos através de cadastros ou bases de dados de consumo. Melhorias significativas nas previsões exigem o preenchimento de bancos de dados com todos os tipos de dados, não apenas nomes e endereços IP, mas também hábitos matinais, caminhadas e muito mais. Hoje vemos o monitoramento contínuo do comportamento das pessoas, cuja

informação é o principal meio de geração de riqueza (BIONI, 2020, p.6). Em outras palavras, a economia baseada no conhecimento e o capitalismo de vigilância estão intimamente relacionados, pois a expansão do mercado em tal lógica de acumulação exige maior vigilância. No entanto, os usuários não têm informações precisas sobre os custos ou benefícios reais dessa troca de informações. Tal como é feito atualmente, o consentimento caracteriza-se antes por uma ação única, cujo resultado deverá permitir o tratamento de determinados dados pessoais. Esse entendimento fica claro quando Frazão afirma:

> [...] o mercado de dados em geral cresce a partir da difusão de visões como a de que o modelo de negócios é justo, já que os usuários recebem contrapartidas adequadas pelos seus dados, ou mesmo necessário, dado que haveria um verdadeiro trade-off entre inovação e privacidade, de maneira que a violação desta última seria o preço a pagar ou o mal necessário para o progresso tecnológico e os novos serviços que daí decorrem. Até a forma como a questão é apresentada já reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares. (FRAZÃO, 2019, p. 31).

Desta forma, a política de privacidade assemelha-se a um acordo de consentimento, uma vez que se pressupõe que o utilizador concorda com tudo o que está descrito ao decidir utilizar os serviços disponibilizados. O objetivo desta tecnologia contratual é garantir o consentimento do usuário para validar todas as operações de processamento de dados. O que geralmente acontece é que o usuário clica no botão "Concordo" sem ler as condições detalhadas e complexas e a política de privacidade, e muitas vezes não possui conhecimento técnico suficiente para compreender a linguagem utilizada nesses textos.

A coleta de dados é o processo de coletar dados e armazená-los em um sistema de armazenamento de dados. Essas informações podem ser obtidas de várias fontes, como formulários preenchidos pelos usuários, sensores, dispositivos eletrônicos, bancos de dados externos, etc.

O objetivo da coleta de dados é garantir que as informações relevantes sejam coletadas com precisão e eficiência, para que possam ser usadas para análise e tomada de decisão. Esse processo pode ser feito de forma manual ou automática,

dependendo da complexidade e quantidade de dados coletados. A qualidade da coleta de dados é essencial para garantir a precisão e integridade dos dados coletados. É importante lembrar que os dados coletados devem ser validados, limpos e devidamente formatados antes de serem armazenados no sistema de banco de dados para que possam ser utilizados de forma eficaz no futuro.

3. DA LEGISLAÇÃO DA PROTEÇÃO DOS DADOS:

A legislação de proteção de dados tem se tornado cada vez mais relevante na era digital, onde a coleta, o armazenamento e o processamento de informações pessoais ocorrem em larga escala. Com o avanço da tecnologia e o aumento das atividades online, a preocupação com a privacidade e a segurança dos dados tornouse uma questão crucial para governos, empresas e indivíduos.

A legislação nesse campo tem como objetivo estabelecer diretrizes e regulamentações para garantir a proteção adequada das informações pessoais, bem como definir os direitos e as responsabilidades dos envolvidos no tratamento desses dados. Ela busca equilibrar a necessidade de coleta e uso legítimo das informações com a preservação da privacidade e a mitigação dos riscos associados ao seu manuseio.

A legislação de proteção de dados desempenha um papel fundamental na garantia da privacidade e da segurança das informações pessoais, buscando equilibrar os interesses das organizações que necessitam dos dados e os direitos dos indivíduos que são titulares dessas informações. É essencial compreender e aderir a essas regulamentações, tanto por parte das empresas, para evitar sanções e danos à reputação, quanto por parte dos indivíduos, para proteger sua privacidade e exercer seus direitos relacionados aos seus dados pessoais.

3.1 DA LEGISLAÇÃO PROTETIVA ANTERIOR

Antes da entrada em vigor da Lei Geral de Proteção de Dados (LGPD) no Brasil, a legislação protetiva de dados pessoais no país era fragmentada e baseada em diversos dispositivos legais e normas setoriais. Embora houvesse algumas disposições esparsas que tratavam da privacidade e da proteção de dados, não existia

uma legislação abrangente e específica para lidar com essa questão de forma adequada.

Nesse contexto, a principal referência legal era o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Embora o Marco Civil da Internet tenha trazido alguns avanços em relação à privacidade e à proteção de dados, seu foco principal era a governança da Internet e a neutralidade da rede, não abordando detalhadamente as questões relacionadas à proteção dos dados pessoais.

Além do Marco Civil da Internet, algumas leis setoriais também tratavam da proteção de dados em âmbitos específicos, como o Código de Defesa do Consumidor, que prevê a proteção do consumidor no tratamento de seus dados pessoais por empresas. Outras normas, como a Lei do Cadastro Positivo (Lei nº 12.414/2011) e a Lei do Sigilo Bancário (Lei Complementar nº 105/2001), estabeleciam regras para o tratamento de dados em setores específicos.

No entanto, a falta de uma legislação unificada e abrangente gerava insegurança jurídica e dificultava a proteção efetiva dos direitos dos titulares de dados. A ausência de normas claras e específicas sobre consentimento, finalidade, segurança e responsabilidade no tratamento de dados pessoais deixava espaço para interpretações divergentes e práticas abusivas.

Diante desse cenário, a promulgação da LGPD representou um marco importante na proteção de dados pessoais no Brasil. A nova legislação trouxe um arcabouço legal abrangente, inspirado em princípios internacionais, para regulamentar o tratamento de dados pessoais, estabelecendo direitos e responsabilidades claras tanto para as organizações que coletam e processam os dados quanto para os titulares dessas informações.

Com a entrada em vigor da LGPD, o Brasil se alinha às tendências internacionais de proteção de dados e fortalece sua posição no contexto global, proporcionando uma maior segurança jurídica para os titulares de dados pessoais e incentivando as empresas a adotarem práticas mais transparentes e responsáveis no tratamento dessas informações.

O ordenamento jurídico brasileiro, especialmente conforme previsto no artigo 5º, inciso X, da Constituição Federal e no artigo 21, do Código Civil, está pautado na

proteção da área íntima do cidadão e de sua vida privada. Antes da implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil em agosto de 2020, a legislação de proteção de dados era fragmentada em várias regras e regulamentos específicos para setores e atividades específicas.

Alguns exemplos de legislação protetiva anterior à LGPD incluem: Marco Civil da Internet (Lei nº 12.965/2014): estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo a proteção da privacidade e dos dados pessoais dos usuários; Lei do Cadastro Positivo (Lei nº 12.414/2011): regula a formação e consulta a bancos de dados com informações de crédito dos consumidores; Lei de Acesso à Informação (Lei nº 12.527/2011): regulamenta o acesso a informações públicas pelos cidadãos, incluindo a proteção dos dados pessoais contidos nesses registros; Código de Defesa do Consumidor (Lei nº 8.078/1990): prevê a proteção dos direitos dos consumidores, incluindo a proteção dos dados pessoais fornecidos durante a compra de produtos ou serviços.

Embora essas leis contivessem disposições sobre a proteção de dados pessoais, nenhuma delas era específica o suficiente para atender aos desafios e complexidades do tratamento de dados pessoais no mundo digital de hoje. Portanto, a LGPD foi criada para estabelecer regras e princípios abrangentes para o tratamento de dados pessoais no Brasil.

A ausência de uma legislação específica para a proteção de dados pessoais no Brasil antes da LGPD deixava margem para interpretações divergentes e gerava insegurança jurídica tanto para os titulares de dados quanto para as empresas que coletam e processam essas informações.

Essa lacuna na legislação também refletia um descompasso em relação aos avanços tecnológicos e às práticas de tratamento de dados que vinham se tornando cada vez mais comuns em diversas áreas, como o comércio eletrônico, as redes sociais, os serviços de nuvem e a publicidade online. Com o aumento do fluxo de informações e a crescente preocupação com a privacidade, fazia-se necessário estabelecer normas claras e específicas para regular essas práticas.

A LGPD veio suprir essa lacuna ao trazer um conjunto de direitos e princípios fundamentais para o tratamento de dados pessoais. Ela estabelece que o tratamento de dados só pode ocorrer mediante o consentimento do titular ou quando amparado por outras bases legais, como o cumprimento de obrigação legal ou contratual, o

exercício regular de direitos, a proteção da vida e da saúde, o legítimo interesse ou a execução de políticas públicas.

Além disso, a LGPD prevê a adoção de medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, incidentes de segurança e o uso indevido ou ilícito dessas informações. As empresas também são responsáveis por garantir a transparência no tratamento de dados, fornecendo informações claras e acessíveis aos titulares sobre como seus dados são coletados, usados, armazenados e compartilhados.

A nova legislação também estabelece os direitos dos titulares de dados, como o direito de acesso, retificação, exclusão, portabilidade, revogação do consentimento e o direito de ser informado sobre o tratamento de seus dados. Esses direitos conferem aos indivíduos um maior controle sobre suas informações pessoais e fortalecem sua autonomia e privacidade.

A LGPD também prevê sanções e penalidades para o descumprimento da lei, que podem incluir advertências, multas e até mesmo a suspensão do tratamento de dados. Essas penalidades visam incentivar o cumprimento da legislação e garantir a responsabilidade das empresas no tratamento adequado dos dados pessoais.

Contudo, a LGPD representa um importante avanço na proteção de dados pessoais no Brasil, trazendo maior segurança jurídica, transparência e controle para os titulares de dados, além de incentivar as empresas a adotarem práticas mais responsáveis e éticas em relação ao tratamento de informações pessoais.

3.2 LEGISLAÇÃO INTERNACIONAL DE PROTEÇÃO DE DADOS

Existem várias leis internacionais de proteção de dados que definem as regras e princípios para o processamento de dados pessoais que visam proteger os direitos de dados e garantir a privacidade e segurança dos dados. Alguns exemplos de direito internacional incluem: Regulamento Geral de Proteção de Dados da União Europeia (RGPD): O GDPR entrou em vigor em maio de 2018 e contém disposições sobre o processamento de dados pessoais em todos os estados membros da União Europeia. O RGPS define princípios como o consentimento expresso do titular dos dados, a finalidade específica do tratamento, a minimização dos dados e a segurança dos dados.

Convenção do Conselho da Europa 108: A Convenção 108 é um acordo internacional adotado pelo Conselho da Europa em 1981, que visa proteger os direitos fundamentais dos indivíduos no processamento de dados pessoais. O acordo contém regras para a coleta, processamento, uso e transferência de dados pessoais. Lei de Privacidade do Consumidor da Califórnia (CCPA): A CCPA é uma lei estadual dos EUA que entrou em vigor em janeiro de 2020 e contém regras para lidar com as informações pessoais dos consumidores da Califórnia. A lei garante ao consumidor o direito de receber, verificar e eliminar os seus dados pessoais, bem como o direito de recusar a venda dos seus dados pessoais.

Lei de Proteção de Dados Pessoais do Japão: A Lei de Proteção de Dados Pessoais do Japão entrou em vigor em maio de 2017 e contém regras sobre a coleta, uso e transferência de dados pessoais. A lei exige que as empresas obtenham o consentimento do titular dos dados antes de coletar dados pessoais e prevê penalidades para uso não autorizado ou uso indevido de dados pessoais.

Estas são apenas algumas das leis internacionais de proteção de dados. Cada país ou região pode ter suas próprias regras e regulamentos, mas é importante que todas as leis de proteção de dados respeitem os direitos fundamentais dos titulares de dados e defina regras claras para o processamento de dados pessoais.

3.3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que entrou em vigor em setembro de 2020 e contém regras para o tratamento de dados pessoais para garantir a proteção da privacidade e dos direitos de dados.

A LGPD se aplica a todas as empresas e órgãos públicos que tratam dados pessoais, independentemente do meio ou finalidade do tratamento. A lei define princípios como a finalidade precisa do tratamento, minimização dos dados, transparência, segurança dos dados e consentimento dos dados. Além disso, a LGPD garante aos titulares de dados direitos como acesso aos seus dados, correção de dados incorretos, exclusão de dados desnecessários ou excessivos, portabilidade de dados e o direito de não ficar sujeito a decisões automáticas com base em seus dados.

A LGPD também impõe obrigações às empresas e órgãos públicos, como nomear um responsável pela proteção de dados, avaliar os impactos da proteção de

dados, relatar violações de segurança de dados e implementar medidas de segurança apropriadas quando os dados processados estiverem em risco.

A LGPD prevê sanções administrativas e judiciais para o descumprimento das regras de proteção de dados, que podem incluir multa, bloqueio ou exclusão de dados e proibição de operações relacionadas ao tratamento de dados pessoais. Em suma, pode-se dizer que a LGPD é um importante ato jurídico, cujo objetivo é garantir a proteção dos dados pessoais e a privacidade dos dados, além de criar regras claras e direitos fundamentais quanto ao tratamento de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que foi promulgada em agosto de 2018 e entrou em vigor em setembro de 2020. Ela tem como objetivo principal proteger os direitos fundamentais de privacidade e de liberdade dos cidadãos, estabelecendo diretrizes claras para o tratamento de dados pessoais por parte de empresas e organizações.

A LGPD é baseada em princípios fundamentais, como o respeito à privacidade, à autodeterminação informativa, a transparência, a finalidade específica e a necessidade adequada do tratamento de dados. Esses princípios norteiam todas as disposições da lei e visam garantir que as empresas coletem, armazenem, utilizem e compartilhem os dados pessoais de forma legítima, segura e responsável.

Um dos aspectos principais da LGPD é o consentimento do titular dos dados. A lei estabelece que o tratamento de dados pessoais só pode ser realizado com o consentimento livre, informado e inequívoco do titular. Além disso, o consentimento deve ser específico para cada finalidade e pode ser revogado a qualquer momento pelo titular.

A LGPD também prevê a figura do Encarregado de Proteção de Dados (DPO), que é responsável por garantir a conformidade com a lei dentro das organizações. O DPO atua como um canal de comunicação entre o controlador de dados, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela fiscalização e aplicação das penalidades previstas na lei.

Outro aspecto importante da LGPD é o direito do titular dos dados. A lei estabelece uma série de direitos para os indivíduos em relação aos seus dados pessoais, como o direito de acesso, o direito de retificação, o direito à exclusão, o direito à portabilidade, entre outros. Esses direitos conferem aos indivíduos um maior

controle sobre suas informações pessoais e permitem que eles exerçam seus direitos em relação ao tratamento de seus dados.

A LGPD também estabelece a obrigatoriedade de medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, incidentes de segurança e o uso indevido dessas informações. As empresas devem adotar medidas técnicas e organizacionais para garantir a confidencialidade, integridade e disponibilidade dos dados.

No que diz respeito às sanções, a LGPD prevê penalidades para o descumprimento da lei, que podem variar de advertências e multas de até 2% do faturamento da empresa, limitadas a um valor máximo, a suspensão do tratamento de dados e até mesmo a proibição total ou parcial das atividades relacionadas ao tratamento de dados.

Em resumo, a Lei Geral de Proteção de Dados (LGPD) é uma legislação abrangente que estabelece diretrizes claras e princípios fundamentais para o tratamento de dados pessoais no Brasil. Ela visa proteger os direitos dos indivíduos, garantir a segurança dos dados e promover práticas mais transparentes e responsáveis por parte das empresas.

A Lei Geral de Proteção de Dados (LGPD) veio introduzir uma série de mudanças significativas na forma como as empresas e organizações lidam com o tratamento de dados pessoais. Antes da LGPD, o Brasil não possuía uma legislação específica e abrangente sobre proteção de dados, o que deixava uma lacuna na proteção dos direitos dos cidadãos em relação à privacidade e ao uso adequado de suas informações pessoais.

Com a entrada em vigor da LGPD, as empresas foram obrigadas a rever suas práticas de coleta, armazenamento, uso e compartilhamento de dados pessoais, a fim de se adequarem aos requisitos legais estabelecidos. Dessa forma, a lei veio trazer mais transparência, segurança e controle para os titulares de dados, bem como responsabilidades mais claras para as empresas que lidam com essas informações.

Uma das mudanças mais significativas trazidas pela LGPD é a necessidade de obtenção de consentimento explícito e específico do titular dos dados para o tratamento de suas informações pessoais. Esse consentimento deve ser informado de forma clara e inequívoca, possibilitando que o indivíduo compreenda e decida sobre a forma como seus dados serão utilizados.

Além disso, a LGPD estabelece uma série de direitos para os titulares de dados, como o direito de acesso às informações, o direito de retificação, o direito à exclusão, o direito à portabilidade dos dados, entre outros. Esses direitos conferem aos indivíduos um maior controle sobre suas informações pessoais, permitindo que eles solicitem correções, atualizações ou exclusão de dados quando necessário.

Outro aspecto importante é a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar e aplicar as sanções previstas na LGPD. A ANPD tem o papel de orientar empresas e titulares de dados, além de fiscalizar o cumprimento da lei e aplicar penalidades em caso de infrações.

A LGPD também estabelece a obrigação das empresas de adotarem medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, vazamentos ou incidentes de segurança. Isso inclui a implementação de políticas de segurança, a adoção de práticas de criptografia, o treinamento de funcionários e a realização de auditorias regulares para garantir a conformidade com a lei.

No âmbito das relações comerciais e contratos, a LGPD trouxe a necessidade de adequação dos termos de uso, políticas de privacidade e contratos para se adequarem aos requisitos da lei. As empresas também passaram a ter a obrigação de celebrar contratos específicos com os chamados "operadores de dados", que são terceiros que realizam o tratamento de dados em nome da empresa controladora.

Destarte, a LGPD veio mudar a forma como as empresas e organizações tratam os dados pessoais no Brasil. Ela introduziu uma série de direitos e responsabilidades, aumentando a proteção da privacidade e da segurança dos dados dos cidadãos.

A Lei Geral de Proteção de Dados (LGPD) foi criada no Brasil como uma resposta à necessidade de proteção da privacidade e dos dados pessoais dos cidadãos. Ela foi inspirada por outras legislações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia.

A jornada para a criação da LGPD começou em 2010, quando o Brasil sediou a Conferência Internacional de Proteção de Dados. Esse evento internacional impulsionou a discussão sobre a necessidade de uma legislação específica para proteção de dados pessoais no país.

Em 2012, foi criado um anteprojeto de lei que serviu como base para a construção da LGPD. Esse anteprojeto passou por diversos debates e consultas públicas, envolvendo a participação de especialistas, acadêmicos, setor empresarial e sociedade civil. O objetivo era garantir uma ampla discussão e receber contribuições de diferentes partes interessadas.

Após anos de discussões e revisões, o projeto de lei foi finalmente aprovado pelo Congresso Nacional em 2018. O então presidente Michel Temer sancionou a lei em agosto de 2018, estabelecendo um período de transição de dois anos para que as empresas e organizações se adequassem às novas exigências.

Durante esse período de transição, várias empresas e entidades começaram a se preparar para a implementação da LGPD, revisando suas políticas de privacidade, adotando medidas de segurança e buscando o consentimento adequado dos titulares dos dados.

Em setembro de 2020, a LGPD entrou em vigor, trazendo consigo uma nova abordagem para a proteção de dados pessoais no Brasil. A Autoridade Nacional de Proteção de Dados (ANPD) foi criada como um órgão regulador responsável por fiscalizar e orientar a implementação da lei.

A criação da LGPD foi impulsionada pela crescente importância dos dados pessoais na sociedade moderna, bem como pela necessidade de proteger os direitos individuais em um mundo cada vez mais digital. A lei estabelece diretrizes claras para o tratamento de dados pessoais, visando equilibrar a utilização legítima dessas informações com a proteção da privacidade e da segurança dos cidadãos.

A Lei Geral de Proteção de Dados (LGPD) foi criada após um processo extenso de discussões, consultas públicas e revisões legislativas. Ela foi sancionada em 2018 e entrou em vigor em 2020, estabelecendo um marco importante na proteção dos dados pessoais no Brasil e alinhando o país a padrões internacionais de privacidade e segurança de dados.

No contexto atual, a proteção de dados tornou-se uma questão cada vez mais relevante devido ao avanço da tecnologia e ao crescente volume de informações pessoais compartilhadas online. A rápida digitalização de serviços, a proliferação de dispositivos conectados à internet e as práticas de coleta e análise de dados por

empresas têm levantado preocupações sobre a privacidade e a segurança das informações pessoais.

Nesse cenário, a Lei Geral de Proteção de Dados (LGPD) surge como uma resposta do Brasil para lidar com essas questões. Ela reflete a necessidade de regulamentação para garantir a proteção dos dados pessoais dos indivíduos e estabelecer diretrizes claras para o tratamento dessas informações.

A LGPD é influenciada por outros marcos legais de proteção de dados em todo o mundo, como o GDPR da União Europeia, e busca harmonizar as práticas brasileiras com os padrões internacionais. Ela estabelece os direitos dos titulares dos dados, como o direito à privacidade, à transparência, ao consentimento informado e à exclusão dos dados, e impõe obrigações às empresas e organizações que coletam e processam dados pessoais.

Além disso, a LGPD também estabelece sanções e penalidades para o descumprimento das suas disposições, o que reforça a importância da conformidade com a lei.

O contexto atual envolve um crescente debate sobre a proteção de dados, a privacidade e a ética no uso das informações pessoais. A conscientização do público em relação aos seus direitos e à importância da segurança dos dados está aumentando, levando a uma maior demanda por medidas de proteção e regulamentação adequadas.

As empresas e organizações estão se adaptando ao novo cenário, implementando políticas de privacidade mais robustas, revisando seus processos de coleta e tratamento de dados, investindo em segurança cibernética e promovendo a conscientização sobre a importância da proteção de dados entre seus colaboradores e clientes.

Em suma, o contexto atual é marcado pela crescente preocupação com a proteção de dados pessoais e a necessidade de estabelecer regras claras para o tratamento dessas informações. A LGPD surge como uma resposta a essas demandas, buscando equilibrar a utilização legítima dos dados com a proteção da privacidade e da segurança dos indivíduos.

3.4 DADOS SENSÍVEIS E DADOS PESSOAIS

Os dados pessoais são dados que permitem a identificação direta ou indireta de uma pessoa singular. Isso pode incluir informações como nome, endereço, CPF, endereço de e-mail, número de telefone e outras informações que possam ser usadas para identificar um indivíduo. Informações confidenciais são informações cujo uso indevido pode danificar ou confundir os dados. Essas informações incluem, entre outras, informações sobre raça ou etnia, opiniões políticas, crenças religiosas, informações genéticas e informações biométricas.

A LGPD estabelece que o tratamento de dados pessoais sensíveis é permitido apenas em determinadas situações especiais, por exemplo, quando o titular dos dados dá consentimento especial para o tratamento ou quando o tratamento é necessário para cumprir uma obrigação legal ou regulamentar. Em todo o caso, o tratamento de dados sensíveis deve ser efetuado com ainda mais cuidado do que o tratamento de dados pessoais não sensíveis, tendo em conta as medidas de segurança adequadas e respeitando os direitos fundamentais dos interessados.

Em resumo, a maior diferença entre dados pessoais e dados sensíveis é a sensibilidade e o risco potencial envolvido no processamento desses dados. Ambos os tipos de informação são protegidos pela LGPD e devem ser tratados adequadamente de acordo com os princípios e regras previstos na legislação.

3.5 DIFERENCIAÇÃO DOS TRATADORES DE DADOS

Na LGPD, duas categorias de representantes participam do tratamento de dados: o controlador e o operador. O responsável pelo tratamento é a pessoa singular ou coletiva que decide sobre o tratamento dos dados pessoais e determina as finalidades, meios e medidas de segurança adequadas ao tratamento dos dados. Em outras palavras, é responsável por como os dados são coletados, usados e protegidos.

O operador, por outro lado, é uma pessoa física ou jurídica que realiza o processamento de dados em nome do controlador, ou seja, executa as funções de processamento de dados prescritas pelo controlador. Em regra, o responsável pelo tratamento é a pessoa que tem relação direta com o titular dos dados e é responsável pela proteção dos dados pessoais.

Por outro lado, o operador é responsável por garantir que as operações de processamento de dados ocorram de acordo com as instruções do controlador e

devem seguir as medidas de segurança definidas por ele. Ambos os representantes têm obrigações importantes no tratamento de dados e devem agir de acordo com os princípios e regras estabelecidos pela LGPD, que garante a proteção de dados pessoais e respeita os direitos dos dados. É importante ressaltar que ambos os representantes podem ser processados por violação da legislação de proteção de dados.

4. SEQUESTRO DE DADOS

A captura de dados, também conhecida como ransomware, é um tipo de ataque cibernético no qual um invasor bloqueia dados em um sistema e exige um resgate (geralmente na forma de criptomoedas) para recuperar o acesso aos dados. A captura de dados geralmente ocorre quando um invasor consegue infectar um sistema com malware específico para esse tipo de ataque. O malware se espalha pelo sistema criptografando os dados armazenados e impedindo o acesso a eles. O invasor então envia uma mensagem exigindo um resgate para descriptografar e emitir novamente os dados.

Em alguns casos, o invasor também ameaça vazar dados se o resgate não for pago. As violações de dados podem ser extremamente prejudiciais para empresas e indivíduos, causando a perda de dados importantes, interrupções de negócios e perdas financeiras significativas.

É importante tomar medidas de segurança apropriadas, como backups regulares e atualizações de segurança para minimizar o risco de coleta de dados. Além disso, ter um plano de resposta a incidentes de segurança é essencial para agir rapidamente no caso de um ataque de ransomware ou outra violação de segurança.

5. SANÇÕES

É necessário começar este assunto recordando o papel que a LGPD terá quando estiver plenamente em operação. Nesta linha, Roque afirma que

> A Lei n.º 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), veio para implementar uma verdadeira revolução na proteção dos dados pessoais no Brasil. Claramente inspirada na regulação europeia sobre o tema – General Data Protection Regulation (GDPR),

> aprovada pelo Parlamento europeu em 2016 e em vigor desde maio de 2018 –, a LGPD brasileira enuncia, entre suas finalidades, “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º) (2019, p. 2).

Para que se possa existir uma responsabilização civil, que é importrante para a caracterização de um prejuizo e posteriormente o seu reparo, esse manuseio de dados deve ser feito sem a autorização.

Esta entidade pode abranger duas categorias:

A primeira, sendo a responsabilidade contratual, que surge de daños causados por descumprimento de cláusulas previstas em contratos ou por falha na execução de uma tarefa (VIEIRA, 2019);

E a segunda, aborda a responsabilidade civil extracontratual, que se refere à obrigação de reparar danos causados pela violação de direitos alheios, tais como os direitos da personalidade (VIEIRA, 2019). Portanto, quem infringir estes direitos e causar danos a outra pessoa, terá que ressarcir o prejuízo causado (VIEIRA, 2019).

Desta forma, o próprio Código Civil fundamenta a responsabilidade em duas noções, sendo a primeira a de ato ilegal, segundo o artigo 186, e a segunda a de abuso de prerrogativa, como estabelecido no artigo 187. Em outras palavras:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes (BRASIL, CC, 2020).

Logo, passa-se a compreender que quando alguém comete uma ação contrária ao que a legislação determina, causando danos ou lesões a outro indivíduo, deve, de alguma forma, indenizar pelos prejuízos causados. E pode existir mais de um modo de se fazer a indenização, como é afirmado por Vieira (2019, p. 29), ao discorrer que

> O ato ilícito, portanto, é aquele praticado em desacordo com a ordem jurídica que ocasiona a violação de direitos e causa prejuízos a outrem. O ato ilícito pode ser penal, administrativo ou civil bem como pode acarretar dupla ou

> tripla responsabilidade, por exemplo, um crime ambiental que ofende os particulares (ilícito civil), a sociedade (ilícito penal) e é passível de sanções administrativas. A consequência do ato ilícito civil é a obrigação geral de reparar o dano, disposta no caput do art. 927 do Código Civil de 2002. Além disso, existem situações em que se responde por terceiros, devendo existir uma conexão entre o responsável e o executor do ato. Há também a hipótese de dano causado por coisa da qual se é proprietário. Por outro lado, nos moldes do art. 187 do CC, a noção de ato ilícito foi ampliada, para considerar como ilícito aquele ato que, originalmente é lícito, mas foi exercido fora dos limites impostos pelo seu fim econômico ou social, pela boa-fé objetiva ou pelos bons costumes.

Logo, para que se manifestem os resultados da responsabilidade civil, é necessário compor três elementos fundamentais, a saber: o proceder, a associação causal e o prejuízo. De acordo com Vieira (2019, p. 28),

> A conduta pode ser ação ou inação; comissiva ou omissiva; própria ou de terceiro; lícita ou ilícita; derivada de fato, coisa, produto ou animal. O nexo de causalidade liga a conduta do agente ao dano sofrido pela vítima. Para que surja o dever de indenizar é preciso que o dano verificado seja consequência da ação ou omissão do agente. O dano é a lesão a um bem jurídico.

É compreensível que a LGPD conceda responsabilidades a dois agentes criados após o estabelecimento da legislação em questão: o responsável e o executor, segundo o artigo 5°, VI e VII, respectivamente. Em outras palavras:

> Art. 5º [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (BRASIL, LGDP, 2020).

A LGPD estabelece a responsabilidade dos responsáveis pelo tratamento de dados no que tange aos danos decorrentes da prática da atividade de tratamento, de maneira análoga ao disposto no 47º Código de Defesa do Consumidor. O artigo 43 da LGDP, porém, isenta esses agentes se forem comprovados os seguintes fatos:

> Art. 43 Os agentes de tratamento só não serão responsabilizados quando provar: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, LGDP, 2020).

É importante destacar que o artigo 42 da mesma lei, em relação ao operador e ao controlador, prevê que, se como resultado de suas atividades no processamento de dados, estes provocarem prejuízos ou infrações, sejam elas morais ou materiais, eles serão responsabilizados por isso. O novo dispositivo também estabelece uma disposição expressa sobre as funções, de modo que os dois sejam solidariamente responsáveis pelas ações realizadas. (BRASIL, LGPD, 2020).

É interessante como Vieira (2019, p. 29) aponta, quando afirma que

> A LGPD traz, ainda, previsão expressa de responsabilidade solidária dos operadores e controladores. Nesse sentido, conforme disposição do inciso I do §1º do art. 42. o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções explícitas do controlador. Já os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, conforme inciso II do §1º do art. 42 da LGPD, respondem solidariamente. O direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso, é assegurado àquele que reparar o dano ao titular dos dados consoante §4º do art. 42 da LGPD. Nos termos do art. 44 da LGPD, será considerado irregular o tratamento de dados pessoais quando for observada a legislação ou quando não for fornecida ao titular a segurança que ele poderia esperar, levando-se em conta as seguintes circunstâncias: o modo pelo qual o tratamento é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

É importante destacar a punição administrativa imposta pela nova lei para aqueles responsáveis pelo tratamento de dados. Se eles infringirem qualquer regra estabelecida na lei, sofrerão as consequências descritas no artigo 52. Em outras palavras:

> Art. 52 Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; 48 IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração" (BRASIL, LGPD, 2020).

Contudo, há a procura de dar maior controle e domínio ao titular em relação aos seus dados, com o objetivo de juntar a utilização da internet com elementos dentro da proteção aos direitos, como a privacidade e a intimidade. Isso significa que, ao explorar o meio virtual, desde quando começou a ser usado, mostrou-se algo onde as pessoas têm liberdade. No entanto, esta liberdade não é incondicional, logo, sejam empresas ou o próprio Estado, eles serão responsabilizados por qualquer violação dos direitos dos titulares dos dados (SILVA; SILVA, 2013).

> Ao observar essa situação e examinando o contexto presente experimentado pelos titulares de informações, é necessário ficar atento ao fato de que
> Com a evolução tecnológica, a proteção jurídica dos dados pessoais, incluído, os dados sensíveis, tornou-se deveras relevante, na medida em que a desproteção dessas informações pode acarretar a vulnerabilidade de direitos e princípios constitucionais, perante, por exemplo, práticas como a apropriação e o repasse no ambiente digital, sem autorização do usuário. No presente artigo científico, observou-se que as cláusulas da Lei n. 12.737/14, conhecida como Marco Civil da Internet, bem como da Lei Geral de Proteção de Dados Pessoais (LGPD) de n. 13.709/18 são promulgadas com o objetivo

> de proteger os internautas no ambiente digital, tendo por base as premissas do livre desenvolvimento da personalidade da pessoa natural, boa-fé nas relações de tratamento de dados pessoais e cumprimento de princípios da segurança da informação. Nesse viés, o direito à privacidade ganhou novo amparo jurídico específico, na medida em que a reunião desses instrumentos normativos colaborou para tutelar os direitos e garantias de forma mais efetiva no ambiente digital e "online", posto que anteriormente não era regulamentado de forma satisfatória. Entretanto, vislumbra-se que, mesmo após a edição da Medida Provisória nº 869/2018, que instituiu a criação da Autoridade Nacional de Proteção de Dados, a necessidade de complementação da legislação infraconstitucional, pois as disposições nacionais à proteção de dados deixam lacunas na efetividade da segurança informacional do internauta perante seus próprios dados, a exemplo, a previsibilidade de penalidades mais severas quando se descumpre os comandos dispostos na LGPD. Enfatiza-se que o tema acerca da proteção de dados é um assunto imprescindível a ser estudado, analisado e entendido, face a sociedade globalizada, que, constantemente, utiliza, tem acesso e usa informações pessoais nas relações, especialmente, jurídicas, deve-se, dessa forma, garantir relações traçadas na confiabilidade, integridade, com o viés de proporcionar maior segurança jurídica e respeito à autodeterminação informativa, incluindo o dever se proteger o direito à privacidade. E, por fim, sabe-se que, quando se trata de 49 meios para se garantir a segurança da informação e a proteção de dados pessoais, é necessário o aperfeiçoamento constante das legislações, dos instrumentos para torná-la aplicável efetivamente, bem como dos modos de conscientização dos usuários/proprietários dos seus próprios dados, sendo, portanto, um trabalho constante, tanto do Poder Público, quanto da Sociedade (CARVALHO; PEDRINI, 2019, p. 379).

Logo, é claro que o sistema legal necessita se ajustar às transformações sociais, pois

> Diante dos desafios do mundo moderno é impensável a exploração de atividade econômica sem que haja a utilização de dados pessoais, vivemos na era da informação e numa sociedade digital. Esse ambiente, entretanto, não pode servir como salvo-conduto para revogação tácita de direitos constitucionalmente assegurados, muito pelo contrário, este cenário deve impulsionar o fortalecimento do arranjo institucional que preserve o cidadão, pois quanto maior o avanço tecnológico maior é a possibilidade de obtenção e utilização indevida dos dados pessoais. Assim, plenamente justificada a

> elaboração da LGPD com previsão de inúmeras obrigações e severas penalizações (SANTOS, A., 2019, p. 21-22).

Quanto à proteção das informações pessoais, visando o estabelecimento de direitos, verifica-se que neste setor, pode-se sugerir proteções coletivas. Representa mais uma asseguração no tocante aos direitos difusos, deste modo, Roque sustenta que

> Dessa forma, torna-se absolutamente relevante aprofundar o estudo da tutela coletiva de dados pessoais, o que se buscou realizar mediante o presente estudo, no qual se concluiu que: (i) a proteção de dados pessoais na esfera coletiva pode dar origem a direitos difusos, coletivos em sentido estrito ou individuais homogêneos; (ii) são legitimados coletivos para a proteção de dados pessoais todos aqueles relacionados no art. 5º da Lei n.º 7.347/1985 e no art. 82 do CDC, sem prejuízo da legitimação do indivíduo, em situações excepcionais; e (iii) deve-se admitir a formulação de pedido genérico de reforma estrutural, na forma do art. 324, § 1º do CPC, havendo fundamento legal para a adoção das medidas estruturantes, sobretudo na fase de cumprimento de sentença, nos arts. 139, IV e 536, §1º do CPC (2019, p. 16).

Além disso, é significativo o que aponta Doneda ao mencionar que a responsabilidade civil tem, portanto, função de destaque na disciplina de proteção de dados pessoais, principalmente se houver a definição de casos específicos de responsabilidade objetiva – vide que a imensa dificuldade na demonstração do dano é um dos problemas clássicos enfrentados pela 50 consolidação da tutela da privacidade. (2008, p. 1).

Sendo assim, uma disciplina de responsabilidade objetiva específica para o setor de tratamento de dados pessoais pode ser um instrumento essencial, tanto para a satisfação de interesses lesados como para fomentar uma determinada cultura de respeito às informações pessoais nas atividades que impliquem no tratamento destas (2008, p. 1).

6. METODOLOGIA

A metodologia adotada para realizar a pesquisa sobre as inseguranças do tratamento de dados no Brasil, foi realizada com base em uma abordagem bibliográfica. O objetivo desta pesquisa foi investigar e analisar as questões relacionadas à segurança e proteção de dados pessoais no contexto brasileiro, considerando as lacunas existentes e as possíveis soluções propostas.

O problema identificado foi a existência de inseguranças no tratamento de dados no Brasil, levando em consideração a proteção insuficiente dos dados pessoais e as consequências negativas para os indivíduos e a sociedade em geral.

Os objetivos desta pesquisa foram: Compreender o conceito e funcionamento do sistema de dados, incluindo a captura de dados, analisar a legislação relacionada à proteção de dados no Brasil, incluindo a legislação protetiva anterior, a legislação internacional de proteção de dados e a Lei Geral de Proteção de Dados (LGPD), explorar a diferenciação entre dados sensíveis e dados pessoais, assim como os papéis e responsabilidades dos tratadores de dados, investigar o sequestro de dados como uma insegurança do tratamento de dados e analisar as sanções relacionadas ao tratamento inadequado de dados pessoais.

A pesquisa foi baseada em uma abordagem bibliográfica, utilizando fontes secundárias como livros, artigos científicos, relatórios governamentais, normas e legislação relacionada à proteção de dados no Brasil. Foram consultadas bibliotecas digitais, repositórios acadêmicos, portais de agências reguladoras e órgãos governamentais, bem como sites de organizações especializadas no assunto.

Foram realizadas buscas em bases de dados acadêmicas, como Google Scholar, Scopus e Web of Science, utilizando termos de pesquisa relevantes, como "inseguranças do tratamento de dados no Brasil", "proteção de dados pessoais", "LGPD", entre outros. Os materiais selecionados foram avaliados quanto à sua relevância, atualidade e credibilidade, considerando sua contribuição para a compreensão do tema.

Os dados obtidos a partir das fontes selecionadas foram analisados de forma qualitativa, buscando identificar padrões, tendências e lacunas no tratamento de dados no Brasil. As informações relevantes foram organizadas em categorias temáticas, correspondentes aos capítulos do trabalho, incluindo a conceituação de dados, legislação de proteção de dados, sequestro de dados e sanções.

Os resultados da pesquisa foram discutidos à luz da legislação brasileira de proteção de dados, como a LGPD, e das teorias e conceitos relevantes no campo da segurança de dados. Foram destacadas as principais inseguranças identificadas e discutidas possíveis medidas de mitigação e melhores práticas para o tratamento seguro de dados

7. CONCLUSÃO:

Identificado o processo de construção da LGPD, foi possível entendê-lo antes ou mesmo antes desta lei ser aprovada Vai entrar em vigor, já existiam muitas normas no ordenamento jurídico brasileiro sobre a proteção de dados pessoais, como o

próprio CDC (lei n. 8.078/1990), MCI (Lei nº 12.965/2014), Lei de Acesso à Informação (Lei nº 12.527/2011) por exemplo Vendo todo esse hardware legítimo, sabíamos que estava lá quebra-cabeça, várias peças espalhadas que não se encaixavam, dificultando você pode agrupá-los.

Portanto, é claro que com a entrada em vigor da nova lei isso teve um efeito positivo, porque antes não era possível estruturar o sistema perfeito, embora existam grandes regulamentos sobre este assunto. termina que embora existam várias leis setoriais para a proteção de dados pessoais, Na verdade, eles eram uma grande salada porque todos esses padrões e as regras foram quebradas e a maior peça desse quebra-cabeça ainda estava faltando, o que é a LGDP do Brasil. A partir daí foi possível ver que todos os principais conceitos foram consolidados em um único regulamento, o que facilitou o trabalho de todas as comunidades e cidadãos que desejavam seguir o novo Regras. Quando a LGPD entrar em vigor, o estado começará a aplicá-la no novo regulamento relacionado com dados pessoais. É para isso que serve para fornecer mecanismos eficazes e válidos para manter salvaguardas de transparência apropriada relacionada à privacidade neste processo.

Entender dados pessoais e informações confidenciais tornou isso possível para entender melhor o assunto do consentimento, incluindo sanções incluídas se esta disposição não for seguida um elemento importante. Entendeu-se que a nova lei é norteada pelos princípios do que pode ser feito lançando uma iniciativa públicoprivada para transformar a Internet democrático No entanto, nota-se que pode haver enganos, erros ou intromissões, No entanto, espera-se que a proteção legal seja maior. Então no caminho previsibilidade, segurança jurídica garante direitos. É claro que há um desafio contínuo com barreiras empresas cumprem a LGPD, 52 desenvolvimento e renovação da política de proteção e gestão de acordo com a assistência jurídica estabelecida, além de sempre atualizar as condições as leis que eles propõem em relação aos dados do usuário de seus clientes, por exemplo parâmetros do tempo de uso e coleta de dados pessoais, Portanto, as empresas devem se adaptar o mais rápido possível a lei realmente entra em vigor porque eles tratam de direitos básico Deve-se entender que a nova lei, quando implementada como um todo traz mudanças significativas nas relações comerciais usuário/consumidor de serviços e produtos.

Considerando as novas mudanças, os usuários também precisam ter mais informações, por isso é importante que eles tenham um uma melhor compreensão do

mundo digital para que todos possam controlá-lo proteção e segurança dos seus dados pessoais. Isso significa que ao usar cidadãos devem estar cientes de seu consentimento e sua provável coleta e armazenamento de sua informação O objetivo desta lei é assegurar o pleno uso, seguindo as diretrizes legais e de proteção de dados pessoais, garantir, acima de tudo, o respeito pela proteção de dados pessoais o direito fundamental à privacidade.

No entanto, o uso de dados pessoais, dados excepcionais os dados pessoais são valiosos para seu proprietário, portanto, eles têm o direito de restringi-los que esta informação é usada de forma inadequada na medida em que lhe traz em relação às violações do princípio da dignidade humana, isso pode ser confirmado processamento dessas informações por pessoas jurídicas públicas e privadas têm direito à normalização interna, que pressupõe e determina a participação controladores e operadores.

Considerando que a mídia online é extensa e muito extensa, pode-se considerar complexo e difícil o controle das informações em circulação. pela internet, então vazamentos podem ocorrer em diversas situações dos dados na base de dados, pois nem sempre é possível garantir integridade dos dados no mundo virtual, pois erros podem acontecer problemas técnicos ou roubo de dados.

Assim, após a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), é possível rever o método escolhido pelo legislador clareza em relação aos direitos, autonomia e devida diligência legal personagem É claro que a nova legislação aumentará a relação entre agentes de processamento de dados e titulares de dados é aberta, etc. a relação deve ser de boa fé. A normalização do processamento de dados coloca o Brasil em pé de igualdade outros países do Mercosul, que possuem legislação própria, destroem também a questão da necessidade de jurisdição em certos contextos informações são necessárias e não serão fornecidas com base no fato de que a lei não foi recebida por unanimidade a este pedido. Este é um desenvolvimento importante não só legalmente, mas também mas também interesse comercial em nosso país. Esta lei autoriza a emissão de responsabilidade para com as pessoas que efetivamente a ela pertencem e em caso de violação à conformidade legal, regulamentos administrativos e requisitos são fornecidos compensação e reparação. Isso garante alta confiabilidade legal não só para o proprietário dos dados, mas também para os representantes ao controle.

Por fim, acredita-se também que com a entrada em vigor da lei geral Proteção de Dados no Brasil Agosto de 2020 que seus mecanismos, sejam eles quais forem material, processual ou administrativo, é possível em muitos casos em situações úteis como incentivo ao cumprimento de ordens e remoção de conteúdo da Internet. Se a LGPD realmente entrar em vigor, espera-se que aqueles que os dados pessoais já cumprem a legislação que os impede por violação de dados cadastrais e os usuários/consumidores possam conhecer todos os direitos decorrentes do contrato maior direito à privacidade.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, D. B. et al. Tecnologia da informação no setor de alimentos e bebidas: o uso de aplicativos de entrega na pandemia da COVID-19. Revista Brasileira de Pesquisa em Turismo, v. 15, n. 1, p. 155-173, 2021;

ANTUNES, R. Os sentidos do trabalho: ensaio sobre a formação e a negação do trabalho São Paulo, SP: Boitempo. 2020;

BERTOLDO, R. C.; FERNANDES, T. F. Tecnologia e a pandemia da COVID-19: a importância dos aplicativos de delivery na manutenção do comércio alimentício. In: CONGRESSO DE INICIAÇÃO CIENTÍFICA EM DESIGN E TECNOLOGIA, 7., 2020, Porto Alegre. Anais do VII CONGIC, p. 1-7, 2020;

BAKER, S. R. et al. How does household spending respond to an epidemic? Consumption during the 2020 COVID-19 pandemic. The Review of Asset Pricing Studies, v. 10, n. 4, p. 834-862, 2020;

BARROS, Marilisa Berti de Azevedo. Relato de tristeza/depressão, nervosismo/ansiedade e problemas de sono na população adulta brasileira durante a pandemia 25 de COVID-19. Epidemiol. Serv. Saúde, Brasília, v. 29, n. 4, e2020427, set. 2020;

DEITOS, G. L. B.; MARCÍLIO, R. O impacto dos aplicativos de delivery alimentício durante a pandemia de COVID-19. Anais do Congresso Nacional de Administração, v. 1, n. 1, p. 1-12, 2020;

DEGEN, Ronald. J. O Empreendedor: Fundamentos da Iniciativa Empresarial. 8ª ed. São Paulo: 1989;

DE REZENDE, Joffre Marcondes. Epidemia, endemia, pandemia, epidemiologia. Revista de Patologia Tropical/Journal of Tropical Pathology, v. 27, n. 1, 1998;

ENGENHARIA DE PRODUÇÃO, 30., 2020, Bauru. Anais do XXX SIMPEP, p. 1-10, 2020;

FERREIRA, Adriano. Aplicativos delivery: veja cinco aplicativos para entrega de comida e produtos, disponível em: http://repositorio.aee.edu.br/jspui/bitstream/aee/9394/1/THAYS%20CARVALHO.pdf. Acesso em: 18 abril. 2023;

FINKLER, Raquel; ANTONIAZZI, Nathalia; DE CONTO, Suzana Maria. Os Impactos da Pandemia de Covid-19: uma análise sobre a situação dos restaurantes. Revista Turismo & Cidades, v. 2, p. 88-103, 2020;

GRALAK, S et al. COVID-19 and the future of food systems at the UNFCCC (UN Framework Convention on Climate Change). v.4, n. 8, E309-E311, August 01, 2020;

KOTLER, P. KELLER, K. L. Administração de marketing. 15. ed. São Paulo: Pearson Prentice Hall, 2012;

Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm;

SILVA, D. M. da; SOUZA, L. S. S. de. Tecnologia da informação em tempos de pandemia: o papel dos aplicativos de delivery de comida. Anais do Congresso Brasileiro de Pesquisa e Desenvolvimento em Tecnologia da Informação e Comunicação, v. 13, n. 1, p. 426-435, 2021;

TURBAN, E. et al. Tecnologia da informação para gestão: transformando os negócios na economia digital. 9. ed. Porto Alegre: Bookman, 2011.

Elayne M

Elayne Melonio
058.318.693-93 Signatário

HISTÓRICO

18 jul 2023 08:32:07 — **Elayne Dos Santos Silva Melonio** criou este documento. (E-mail: elayne_jc@hotmail.com, CPF: 058.318.693-93)

18 jul 2023 08:32:07 — **Elayne Dos Santos Silva Melonio** *(E-mail: elayne_jc@hotmail.com, CPF: 058.318.693-93)* visualizou este documento por meio do IP 177.87.165.140 localizado em Parauapebas - Para - Brazil

18 jul 2023 08:32:15 — **Elayne Dos Santos Silva Melonio** *(E-mail: elayne_jc@hotmail.com, CPF: 058.318.693-93)* assinou este documento por meio do IP 177.87.165.140 localizado em Parauapebas - Para - Brazil

Fernanda R

Fernanda Rodrigues
072.298.084-13 Signatário

HISTÓRICO

09 ago 2023 21:16:23 — **Fernanda Lopes De Freitas Rodrigues** criou este documento. (E-mail: fernandarodrigues.fadesa@gmail.com, CPF: 072.298.084-13)

09 ago 2023 — **Fernanda Lopes De Freitas Rodrigues** *(E-mail: fernandarodrigues.fadesa@gmail.com, CPF: 072.298.084-13)* 21:16:24 visualizou este documento por meio do IP 45.7.26.109 localizado em Parauapebas - Para - Brazil

09 ago 2023 21:16:49 — **Fernanda Lopes De Freitas Rodrigues** *(E-mail: fernandarodrigues.fadesa@gmail.com, CPF: 072.298.084-13)* assinou este documento por meio do IP 45.7.26.109 localizado em Parauapebas - Para - Brazil

Maicon T

Maicon Tauchert
986.590.490-04 Signatário

HISTÓRICO

10 ago 2023 15:25:53 **Maicon Rodrigo Tauchert** criou este documento. (E-mail: direito@fadesa.edu.br, CPF: 986.590.490-04)

10 ago 2023 **Maicon Rodrigo Tauchert** *(E-mail: direito@fadesa.edu.br, CPF: 986.590.490-04)* visualizou este documento 15:25:53 por meio do IP 170.239.200.14 localizado em Curionopolis - Para - Brazil

10 ago 2023 **Maicon Rodrigo Tauchert** *(E-mail: direito@fadesa.edu.br, CPF: 986.590.490-04)* assinou este documento por 15:26:25 meio do IP 170.239.200.14 localizado em Curionopolis - Para - Brazil