



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS E HUMANAS - CCSAH
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

ANGÉLICA VIVIANE RIBEIRO DA SILVA

**A RESPONSABILIDADE CIVIL DOS AGENTES DE
TRATAMENTO DE DADOS À LUZ DA LEI GERAL DE
PROTEÇÃO DE DADOS PESSOAIS – LGPD**

MOSSORÓ
2024

ANGÉLICA VIVIANE RIBEIRO DA SILVA

**A RESPONSABILIDADE CIVIL DOS AGENTES DE
TRATAMENTO DE DADOS À LUZ DA LEI GERAL DE
PROTEÇÃO DE DADOS PESSOAIS – LGPD**

Artigo apresentado ao Departamento de Ciências Sociais Aplicadas para a obtenção do grau de Bacharel em Direito, pela Universidade Federal Rural do Semiárido, no curso de Direito.

Orientador: Prof. Dr. Rodrigo Vieira Costa.

MOSSORÓ
2024

ANGÉLICA VIVIANE RIBEIRO DA SILVA

**A RESPONSABILIDADE CIVIL DOS AGENTES DE
TRATAMENTO DE DADOS À LUZ DA LEI GERAL DE
PROTEÇÃO DE DADOS PESSOAIS – LGPD**

Artigo apresentado ao Departamento de Ciências Sociais Aplicadas para a obtenção do grau de Bacharel em Direito, pela Universidade Federal Rural do Semiárido, no curso de Direito.

Orientador: Prof. Dr. Rodrigo Vieira Costa.

APROVADA EM: 23/10/2024

BANCA EXAMINADORA

Prof. Dr. Rodrigo Vieira Costa (UFERSA)
Presidente

Prof. Mestrando Matheus Fernandes da Silva (UFERSA)
Primeiro Membro

Prof. Mestrando Adailson Pinho de Araújo (UFERSA)
Segundo Membro

AGRADECIMENTOS

Neste momento tão especial, gostaria expressar minha profunda gratidão a Deus que me sustentou até aqui, me fortaleceu em todos os momentos para a realização deste trabalho e em minha jornada acadêmica.

Agradeço à minha família, que sempre foi meu alicerce. Aos meus pais, José Bonifácio Pereira e Aldeci Ribeiro Pereira, pelo amor incondicional, apoio e incentivo em todos os momentos. Vocês acreditaram em mim e isso foi fundamental para que eu chegasse até aqui.

Agradeço *in memoriam* ao meu amado irmão Bonifácio Neto, amada mãe e avó Maria de Lourdes da Silva, pai e avô Djalma Ribeiro da Silva, vocês deixaram um legado de valores que continuam a me guiar. Sou eternamente grata por cada momento compartilhado e por todo o amor que me deram.

Um agradecimento especial ao meu companheiro, Junior, que compartilhou conhecimentos, exemplos, vivências e experiências cotidianas de seu trabalho, me ajudando em cada passo dessa jornada. Seu apoio e incentivo foram essenciais para que eu pudesse superar os desafios e manter o foco em meus objetivos. Sou eternamente grata por ter você ao meu lado.

Agradeço também à minha amiga Fernanda Karoliny, que se tornou uma verdadeira parceira de estudos e desafios. Sua amizade e incentivo foram fundamentais para que eu pudesse enfrentar os momentos difíceis com mais leveza. Juntas, superamos obstáculos e celebramos conquistas.

Aos meus professores, que fazem o curso de Direito da UFERSA, que compartilharam seu conhecimento e experiência de forma generosa. Vocês me inspiraram e motivaram a buscar sempre o melhor em mim. Suas aulas foram verdadeiras fontes de aprendizado e crescimento.

Um agradecimento especial ao meu orientador, Rodrigo Vieira, sua paciência e orientação foram essenciais para o desenvolvimento deste trabalho. Sua expertise e conselhos valiosos me guiaram em cada etapa do processo, e sou eternamente grata por sua dedicação e apoio.

*“Aprender é a única coisa
que a mente nunca se cansa, nunca tem
medo e nunca se arrepende.”.*
(Leonardo da Vinci.)

A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD

Angélica Viviane Ribeiro da Silva¹

Resumo: O trabalho aborda a responsabilidade civil dos agentes de tratamento de dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais (LGPD), destacando sua importância frente ao avanço tecnológico e ao crescente uso de dados pessoais. O objetivo principal é analisar a responsabilização dos controladores e operadores de dados. A pesquisa adota uma abordagem dedutiva, e metodologia bibliográfica e documental, com base em legislação e na doutrina, para explorar os princípios da privacidade e da proteção de dados e as diferentes correntes de responsabilidade civil. Os resultados principais indicam que a LGPD combina elementos de responsabilidade subjetiva e objetiva, enfatizando a prevenção e segurança no tratamento de dados. Conclui-se que o legislador introduziu uma responsabilidade subjetiva proativa, que reflete a necessidade de maior de prevenção de danos, mitigação de riscos na proteção da dignidade humana e da privacidade dos indivíduos.

Palavras-chave: LGPD; responsabilidade civil; proteção de dados; agentes de tratamento.

Abstract: The work addresses the civil liability of personal data protection agents in the light of the General Personal Data Protection Law (LGPD), highlighting its importance in the face of technological advances and the increasing processing of personal data. The main objective is to analyse the liability of data controllers and operators. The research adopts a bibliographical approach, based on legislation and doctrine, to explore the principles of privacy, data protection and the different currents of civil liability. The main results indicate that the LGPD combines elements of subjective and objective liability, emphasising prevention and security in data processing. It is concluded that the legislator has introduced proactive subjective liability, which reflects the need for greater damage prevention, risk mitigation in the protection of human dignity and the privacy of individuals.

Keywords: LGPD; civil liability; data protection; processing agents.

1 INTRODUÇÃO

O artigo apresenta uma análise sobre a responsabilidade civil dos agentes de tratamento de dados à luz da Lei Geral de Proteção de Dados Pessoais (LGPD), um tema que se torna cada vez mais relevante em virtude do avanço tecnológico e da crescente digitalização das informações pessoais. A coleta e o uso de dados pessoais por entidades públicas e privadas geraram questões importantes em relação à privacidade e à proteção dos direitos dos indivíduos. Com a promulgação da lei 13.709-LGPD em 2018, o Brasil deu um passo importante na regulamentação do tratamento de dados, estabelecendo diretrizes que visam garantir a segurança e a transparência no uso dessas informações.

A dignidade da pessoa humana, um princípio fundamental consagrado na Constituição Federal de 1988, está intrinsecamente ligada ao direito à privacidade. A LGPD

¹ Discente do décimo-segundo período do curso de Direito da Universidade Federal Rural do Semi-árido (UFERSA). E-mail: angelicavrssilva@gmail.com.

não apenas confirma essa conexão, mas também impõe responsabilidades claras aos controladores e operadores de dados. A legislação de proteção de dados garante que o tratamento de dados pessoais seja feito de maneira ética e responsável, refletindo a necessidade de proteger os indivíduos contra abusos e garantir a conformidade com as normas legais.

Este trabalho tem como objetivo geral analisar a responsabilidade civil dos agentes de tratamento de dados sob a perspectiva da LGPD, explorando as implicações jurídicas decorrentes do descumprimento das normas. Os objetivos específicos incluem: examinar os princípios que norteiam a legislação de proteção de dados no ordenamento jurídico; analisar a LGPD e garantia de direito dos titulares, quem são os agentes de tratamento e discutir as diferentes correntes de responsabilidade civil aplicável aos agentes envolvidos no tratamento de dados.

A pesquisa adota uma abordagem dedutiva, utilizando metodologia bibliográfica e documental. A análise é fundamentada em legislações vigentes, doutrinas especializadas e estudos relevantes, permitindo uma compreensão abrangente sobre como a legislação brasileira aborda a proteção de dados pessoais.

A relevância deste estudo reside na necessidade urgente de discutir a responsabilidade civil dos agentes que tratam dados pessoais. No mundo cada vez mais digitalizado, onde os dados são considerados um recurso importante, é crucial garantir que os direitos fundamentais dos titulares sejam respeitados e protegidos.

O artigo entra na discussão aprofundada sobre os conceitos fundamentais relacionados à privacidade, proteção de dados, como a legislação de proteção de dados pessoais evoluiu de disposições esparsas para uma legislação específica que orienta como os dados devem ser tratados e protegidos das violações. O artigo também aborda quem são os agentes de tratamento conforme a lei, suas atribuições e condutas, e como a Autoridade Nacional de Proteção de dados- ANPD, regulamenta as implicações práticas da LGPD para organizações e indivíduos.

No última parte cabe examinar os dispositivos da LGPD que tratam da responsabilização, e a aplicação da lei no contexto brasileiro, cada seção foi organizada para fornecer uma compreensão clara e sequencial do tema, culminando em considerações que destacam a importância da conformidade legal na proteção dos direitos dos cidadãos, incluindo uma análise das principais correntes doutrinárias sobre responsabilidade civil.

O avanço tecnológico tem promovido uma transformação profunda na maneira como os dados pessoais são coletados, armazenados e utilizados, tanto por entidades públicas

quanto privadas. Nesse contexto, o direito à privacidade e à proteção de dados se tornaram questões fundamentais nas sociedades contemporâneas, particularmente no Brasil, onde a Lei Geral de Proteção de Dados Pessoais, LGPD (2018) estabelece uma série de diretrizes e normas voltadas à salvaguarda desses direitos.

2 DIREITO FUNDAMENTAL À PRIVACIDADE, DADOS PESSOAIS E A PROTEÇÃO NO ORDENAMENTO BRASILEIRO

A dignidade humana no ordenamento jurídico brasileiro é um princípio fundante e nele se reconhece a vida privada como um direito primordial (art. 5º, inciso X). Esse direito de proteção à privacidade possui uma dimensão coletiva e individual, manifestada através da proteção de dados pessoais e que nela estão inclusos interesses ligados à personalidade, e suas relações (DONEDA, 2020).

Vários elementos do direito à privacidade sempre foram preservados e apreciados pelas sociedades. Contudo, até certo ponto no passado, a salvaguarda que lhes era oferecida não estava unificada sob a ideia de privacidade (DONEDA, 2020).

Na perspectiva de Doneda (2020), a privacidade deixa de ser simplesmente um direito, como qualquer outro direito subjetivo, e se transforma em um contexto jurídico complexo, estabelecido por um conjunto de relações. Dessa forma, a privacidade não seria um objetivo em si mesmo, mas sim um conceito relacional, uma ferramenta através da qual a individualidade e, em última instância, a proteção humana são resguardadas.

A privacidade e a proteção de dados pessoais são temas de destaque no ambiente jurídico. Isso se deve à orientação estrutural e significativa de outros ordenamentos com o tema, que visam garantir os direitos fundamentais, considerando o impacto do desenvolvimento tecnológico na criação de novos espaços que precisam ser regulamentados juridicamente.

A crescente digitalização da sociedade têm contribuído para o aumento exponencial na coleta, processamento e compartilhamento de dados pessoais, que constitui em bens jurídicos de valor e relevância, para os titulares, instituições, empresas, e mercados, são uma espécie de “novo petróleo”, um recurso econômico na contemporaneidade (VIANNA, 2021).

A privacidade assume uma posição de relevância na proteção da pessoa humana em sentido amplo, gerando autonomia, cidadania, atividade política, e direitos de liberdade (DONEDA, 2020).

Nesse sentido, desenvolve cada vez mais as liberdades individuais no ambiente de plataformas² onde a comunicação e a informação possuem uma posição valiosa.

Uma determinada informação pode possuir um vínculo com uma pessoa ou com um grupo de pessoas, revelando algo sobre elas, este vínculo pode se referir as características, ou ações atribuídas a uma determinada pessoa, podendo identificá-la como seu nome civil, ou endereço, ou seus atos como informações de consumo e manifestação de opinião.

Um dado pode se referir a uma pessoa indeterminada (dado anônimo), sendo utilizado para diversas finalidades com seu valor específico a uma coletividade sem que as pessoas possam ser nominadas. Essa anonimização dos dados em que se retira os vínculos da informação com as pessoas a que se referem é uma forma de salvaguarda afim de minimizar riscos que possam afetar o tratamento dessas informações, preservando o direito nessa sociedade digital (DONEDA, 2020).

A privacidade, inicialmente protegida pelo ordenamento jurídico, evoluiu para uma proteção específica dos dados pessoais. Ao longo do tempo, foram criados cada vez mais arcabouços legislativos dedicados à proteção desses dados. Acompanhando as transformações tecnológicas, as leis avançam, tornando-se mais abrangentes e contextualizadas (FULLER; TATEOKI, 2023).

A Constituição Federal já garantia o direito à inviolabilidade da vida privada com previsão no art. 5º, inciso X, (BRASIL,1988), protege e assegura o direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Esse dispositivo constitucional servia inicialmente como fundamento para garantir a proteção dos dados pessoais, uma vez que eles estão diretamente relacionados à esfera íntima e privada de cada indivíduo, assim como o sigilo das correspondências, comunicações telegráficas, de dados telefônicos, o direito de ter sua privacidade protegida pelo Estado.

A crescente valorização da proteção jurídica da privacidade dos dados pessoais como um direito fundamental foi confirmada pelo Supremo Tribunal Federal em uma decisão histórica. (ROMERO, 2024). Essa deliberação ocorreu em decisão liminar da Ministra Rosa Weber nas Ações Diretas de Inconstitucionalidade nº 6387, 6388, 6389, 6390 e 6393, que questionavam a Medida Provisória (MP) nº 954/2020.

Essa MP autorizou o compartilhamento de dados por operadoras de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a criação

² Plataformas digitais são ambientes virtuais que facilitam interações, transações e compartilhamento de informações entre indivíduos, instituições e empresas. Elas permitem a criação, distribuição e consumo de conteúdo online, abrangendo redes sociais, aplicativos, sites e serviços online (FIA, 2023).

de estatísticas oficiais durante a pandemia de Coronavírus. A decisão do Superior Tribunal Federal (STF) é considerada um ponto de inflexão, pois reafirma que todos os dados capazes de identificar uma pessoa possuem tanto implicações naturais quanto jurídicas e, portanto, necessitam de proteção garantida pela Constituição. (BEZERRA; FURTADO, 2023).

A relatora, Ministra Rosa Weber (BEZERRA; FURTADO, 2023) destacou que não existem dados neutros, uma vez que qualquer informação que possibilite a identificação de um indivíduo pode ser utilizada para formar perfis informacionais, tanto por empresas quanto pelo Estado. Assim, o uso desses dados deve ser legítimo e transparente, com a comunicação das finalidades específicas e modos de utilização aos titulares, aspectos que não eram claros na referida MP. O acórdão, publicado em 12 de novembro de 2020, certamente se torna uma referência importante na doutrina sobre a proteção de dados pessoais no Brasil.

No âmbito legislativo, o Senado Federal aprovou a Proposta de Emenda à Constituição (PEC) nº 17/2019 (CÂMARA DOS DEPUTADOS, 2019) que foi oficialmente promulgada em 10 de fevereiro de 2022, gerando a Emenda Constitucional nº 115 de 10/02/2022 (BRASIL, 2022). Essa emenda estabelece a proteção de dados pessoais, abrangendo também o ambiente digital, como um dos direitos e garantias fundamentais do cidadão. Ela insere o inciso XII-A no art. 5º e o inciso XXX no art. 22 da Constituição Federal, atribuindo à União a competência privativa para legislar sobre esse assunto.

No contexto constitucional, também há uma garantia de salvaguarda dos dados pessoais, um “remédio constitucional³” chamado *habeas data*.

O *habeas data* e a Constituição Brasileira estão intrinsecamente relacionados, uma vez que o *habeas data* é um instrumento jurídico previsto na Constituição Federal de 1988 que visa proteger o direito à intimidade, à liberdade de informação e à autodeterminação informativa dos cidadãos. A doutrina de José Afonso da Silva (2010, p. 53) o define como:

Proteger a esfera íntima dos indivíduos contra: (a) usos abusivos de informações sobre a vida privada, honra e imagem das pessoas; (b) o acesso a informações sobre uma pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público (c) a retificação de dados, quando não se prefira por processo sigiloso, judicial ou administrativo.

³ O termo Remédio Constitucional indica uma espécie de instrumento judicial, colocado à disposição de qualquer cidadão, o qual tem a finalidade de garantir os direitos fundamentais, direitos públicos ou liberdades públicas. Nesse sentido, são meios judiciais que visam tutelar direitos fundamentais violados em alguma situação, no intuito de intervenção no poder das autoridades públicas, resguardando o direito do cidadão diante da ilegalidade ou abuso do poder cometido em detrimento dos interesses e direitos fundamentais (GOMES, 2022).

Dessa forma, há o reconhecimento da proteção de dados como um direito fundamental protegido pelo Estado que tem o dever de adotar medidas para preservar a privacidade dos cidadãos e protegê-los de abusos no tratamento de suas informações. A legislação ordinária abrange diversas situações, levando em conta os interesses relacionados à privacidade. Disposições esparsas em outros ramos do direito como: direito civil, processual, penal, tributário e consumerista⁴.

Nos contextos do consumo, é possível perceber casos frequentes nos quais ocorrem violações ao direito de privacidade, devido principalmente à utilização abusiva de informações pessoais para atrair, conquistar e fidelizar clientes. No atual modelo capitalista, no qual a informação se torna um ativo tão mais precioso do que outros recursos organizacionais, o indivíduo não apenas desempenha o papel de consumidor, mas também é considerado um produto de interesse para diversas organizações (LIMA; GARRIDO, 2022).

O Código de Defesa do Consumidor (Lei nº 8.078/90) que vem disciplinar as regras para tratar sobre o assunto, em seu art. 43, informa aos cidadãos sobre o acesso às informações existentes.

O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público (BRASIL, 1990).

Percebe-se o cuidado trazido pelo Código de Defesa do Consumidor quanto aos cadastros, fichas, registros e dados pessoais arquivados, bem como sobre as fontes, no que tange ao acesso de informações (LIMA; GARRIDO, 2022).

⁴ Código Civil (2002): Estabelece normas gerais sobre personalidade, privacidade e indenização por danos morais e materiais, Código de Processo Civil (2015): Prevê a possibilidade de segredo de justiça para proteger a intimidação em processos judiciais; Código Penal (1940): Tipifica crimes contra a honra, como calúnia, injúria e difamação, que podem envolver a divulgação indevida de informações pessoais. Lei de Crimes Cibernéticos (Lei 12.737/2012): Criminaliza a invasão de dispositivos informáticos para obter, adulterar ou destruir dados sem autorização; Código Tributário Nacional (1966): Prevê o sigilo fiscal, protegendo informações do contribuinte a Fazenda Pública.

No que diz respeito à transparência, a Lei 12.527/2011, Lei de Acesso à Informação (LAI), que regula o acesso às informações públicas, tem como objetivo principal promover a transparência administrativa e permitir que os cidadãos exerçam o seu direito fundamental de acesso à informação. A LAI se aplica a todos os órgãos e entidades da administração pública dos Poderes Executivo, Legislativo e Judiciário, em todas as esferas (Federal, Estadual e Municipal), bem como às entidades privadas que recebem recursos públicos para a realização de atividades de interesse público. Esta norma trouxe ao cidadão uma ferramenta de extrema utilidade para sua participação no governo, já que ela estabelece que o acesso às informações estatais seja a norma, e o sigilo apenas uma exceção (NASCIMENTO, 2016).

Nesta perspectiva, torna-se necessário compreender a visão de Mendes e Branco acerca dessa lei mencionada:

Trata-se de importante marco para a observância da publicidade como preceito geral e do sigilo como exceção, por meio de medidas que devem ser executadas de acordo com os princípios básicos da Administração Pública e por diretrizes que zelam e incentivam a ampla transparência (MENDES; BRANCO, 2015, p. 850).

A LAI trouxe conceitos importantes; foi a primeira legislação no Brasil a considerar a Internet como um ambiente de importância jurídica, assegurando o direito fundamental ao acesso à informação e destacando a necessidade de transparência na administração pública. Essa norma impõe que as instituições governamentais lidem com os dados pessoais de maneira clara, respeitando os direitos fundamentais à intimidade, privacidade, honra e imagem, e restringindo o acesso a informações pessoais, exceto quando houver consentimento do titular.

Pode-se afirmar que ocorreu um avanço inestimável em relação à maneira como o Estado deve fornecer tratamento ao cidadão quando o assunto é o acesso a dados e documentos públicos. O titular dos dados de posse das informações disponibilizadas, cabe a este, a partir de agora, fazer valer seus direitos e lutar pela consolidação de uma sociedade cada vez mais justa, transparente, igualitária e íntegra.

Houve outros avanços na proteção das informações pessoais no caso a Lei 12.737/2012 conhecida como Lei Carolina Dieckmann, que fez uma importante alteração no Código Penal quando inseriu o art. 154-A⁵:

⁵ Foi publicada no Diário Oficial da União a Lei nº 14.155, de 27 de maio de 2021 que atualiza a famosa “Lei Carolina Dieckmann” (Lei 12.737 de 2012), a lei criada em 2012 que tipificou, pela primeira vez, os crimes cibernéticos no Brasil.

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012).

Essa mudança no Código Penal, ocorrida no ano de 2012, foi seguida de outros exemplos legislativos benéficos no assunto da proteção de dados.

O Marco Civil da Internet (Lei 12.965/2014) norma em que estão presentes os princípios indispensáveis para garantia dos direitos onde se pode destacar desses princípios a liberdade de expressão e a proteção da privacidade, garantias essas que são conhecidas de longa data e estão presentes na Constituição Federal, além do uso da internet no Brasil, pois instituiu princípios cautelares e responsabilizou os agentes danosos.

Os preceitos trazidos pelo Marco Civil da Internet foram fundamentais para as primeiras reflexões no tema da proteção de dados. Trouxe a fundamentação normativa para abordar os casos relacionados à Internet e tecnologia da Informação, visando preencher a falta de legislação sobre os aspectos econômicos, comportamentais e tecnológicos no cenário da internet global (CESAR; BARRETO JUNIOR, 2017).

No cenário internacional, a União Europeia (UE) tomou a liderança sobre a questão da proteção de dados, com a promulgação do Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, GDPR (UNIÃO EUROPEIA, 2016), cujo objetivo principal era de abordar a proteção das pessoas físicas no que se refere ao tratamento de dados pessoais e à livre circulação desses dados.

A Lei brasileira não apenas nasceu da demanda por um aprimoramento do ordenamento jurídico interno, mas também da necessidade de uma regulamentação internacional que seja convergente em relação ao assunto, tendo em vista a realidade de uma economia digital global, onde as informações ultrapassam fronteiras territoriais. Nesse contexto, a LGPD se baseia no modelo europeu de proteção de dados (PINHEIRO, 2023).

As leis sobre proteção de dados contêm a peculiaridade de possuir uma redação principiológica pautada em indicadores de ordem técnica que permitam auferir de forma auditável se os compromissos estão sendo cumpridos através de vários itens de controle para garantir uma melhor governança de dados pessoais. Com isto, houve a necessidade de que os outros países e as empresas que desejassem obter relações comerciais com a UE deveriam possuir uma legislação adequada ao mesmo nível que o GDPR, pois o Estado que não tivesse legislação neste nível poderia sofrer com algum tipo de barreira econômica, comercial ou qualquer dificuldade de realizar negócios com os países da UE (PINHEIRO, 2023).

O GDPR tem como objetivos: contribuir com a realização de espaço de liberdade e segurança, justiça e de união econômica para progresso social, consolidação e progresso econômicos, e convergência das economias a nível de mercado interno para o bem estar das pessoas físicas; assegurar um nível coerente de proteção das pessoas físicas; garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e a sociedade como um todo; impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais e possibilitar a cooperação efetiva entre autoridade e Estados-Membros (PINHEIRO, 2023).

Destaque-se que a proteção ao tratamento de dados pessoais das pessoas físicas é um direito garantido em diversos países que possuem legislações de proteção de dados. Segundo o site *Privacy Tools* (2019), na América Latina podemos citar: Chile, Argentina, Uruguai e Colômbia. A lei chilena, de 1999, limita o uso dos dados ao propósito informado no ato da coleta, com a exceção de registros tornados públicos.

A análise da evolução legislativa, culminando na promulgação da LGPD, revelou um avanço significativo na forma como o Brasil reconhece e regulamenta esses direitos.

A LGPD distribuiu um marco regulatório claro e abrangente, que não apenas unificou as normas existentes, mas também princípios dinâmicos modernos e específicos para a proteção de dados pessoais. Com a criação de direitos específicos para os titulares de dados e a designação de uma autoridade competente para supervisionar e garantir a aplicação da lei, o Brasil deu passos importantes na direção à proteção da privacidade dos cidadãos.

Contudo, é fundamental que a implementação da LGPD continue a ser monitorada e aprimorada, garantindo que os direitos dos cidadãos sejam cumpridos e que a legislação seja atualizada em face das constantes mudanças tecnológicas e sociais.

3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A GARANTIA DOS DIREITOS DOS TITULARES.

Os dados pessoais possuem uma relevância excepcional no cenário socioeconômico atual. Através da coleta dessas informações, órgãos governamentais e outras empresas obtiveram financiamentos essenciais para tomar decisões estratégicas e alcançar seus objetivos.

A independência garantida à salvaguarda das informações individuais em comparação com o direito à privacidade atinge o seu ponto máximo com a promulgação das

primeiras legislações de proteção de dados pessoais. Isso culmina na categorização desse conjunto de regulamentos.

Segundo Bioni (2019), informações pessoais são entendidas como aquelas associadas a um indivíduo, desvendando ou revelando algum aspecto concreto da pessoa. É necessário esclarecer o conceito importante sobre o que se entende por dados pessoais, que podem ser resumidas em duas correntes principais: a expansionista e a reducionista.

Na perspectiva expansionista, considera-se que todas as informações relacionadas a uma pessoa que pode ser identificada, direta ou indiretamente, são tratadas como dados pessoais. Assim, essas informações estariam protegidas por dispositivos legais que têm como objetivo resguardar esse direito. A pessoa a quem os dados dizem respeito pode ser indefinida, e a conexão com esses dados pode ser "mediata, indireta, imprecisa ou inexata", conforme aponta Bruno Bioni (2019). Por outro lado, a abordagem reducionista limita a definição de dados pessoais apenas às informações que identificam diretamente uma pessoa. Nesse caso, essa pessoa se torna específica e definida por esses dados, estabelecendo um vínculo que é "imediato, direto, preciso ou exato".

De acordo com a teoria expansionista, a LGPD estipula de maneira clara, em seu art. 5º, inciso I, que dado pessoal é definido como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Dessa forma, no contexto jurídico brasileiro, considere que todos os dados que têm potencial para identificar uma pessoa natural possuem implicação legal. Esta interpretação ampla da definição de dados pessoais está alinhada com a perspectiva expansionista, que entende que informações relacionadas a uma pessoa que podem ser identificadas, direta ou indiretamente, devem ser tratadas como dados pessoais e, portanto, protegidas por dispositivos legais.

Ao adotar uma definição abrangente de dados pessoais, a LGPD busca garantir uma proteção efetiva dos direitos fundamentais de liberdade e privacidade dos indivíduos, reconhecendo que as mesmas informações que não identificam diretamente uma pessoa podem, quando combinadas com outros dados, revelar sua identidade. Logo, seria pertinente abordar o conceito de métodos de "desidentificação" de dados pessoais, com o intuito de evitar que esses dados possam ser vinculados a uma pessoa específica.

O art. 5º, II da LGPD, conceitua os dados sensíveis como:

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (BRASIL, 2018).

Em outras palavras, os dados sensíveis estão ligados a aspectos mais internos e comportamentais da pessoa, o que resulta em um potencial maior de possíveis danos, e como consequência, e um conjunto de regras mais abrangente e protetivo a fim de evitar condutas de caráter discriminatório que possam ameaçar a personalidade individual.

Ainda que seja uma lei recente que já passou por algumas atualizações – como a MP nº 869/2018 que foi convertida na Lei nº 13.853, de 8 de julho de 2019, o principal objetivo dessa lei é alterar a LGPD e criar a Autoridade Nacional de Proteção de Dados⁶ (ANPD) – sua importância se dá pela contribuição voltada para eficácia e aplicação prática da legislação elevando o nível da proteção de dados ao mesmo patamar do GDPR, garantindo mais estabilidade e segurança.

Em seu art. 55-J, a LGPD estabelece as competências da ANPD, que consistem em: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança, promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional, editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação (PINHEIRO, 2023).

A aplicação da lei atinge a todos aqueles que realizam o tratamento de dados, sejam por instituições públicas, privadas, pessoas físicas ou jurídicas que realizam qualquer tipo de operação de tratamento de dados pessoais, seja por qualquer meio envolvendo pelo menos um dos elementos como: Ocorrer em território nacional, que tenha por objetivo a oferta ou fornecimento de bens ou serviços ou tratamento de indivíduos localizados em território nacional e que os dados tenham sido coletados no território nacional (PINHEIRO, 2023).

Conforme os critérios acima, a LGPD não está relacionada com questões de cidadania, nacionalidade dos dados pessoais ou residência do titular dos dados. De outro modo a lei não se aplica a tratamento realizado por pessoa física com fins particulares não econômicos, fins jornalísticos e artísticos, para fins de segurança pública e defesa nacional.

⁶ A ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2024).

O alcance da lei é extraterritorial possuindo efeitos internacionais na medida que se aplicam a dados tratados fora do país, que foram coletados em território nacional e neste sentido sujeitam as empresas e instituições fora do território a aplicação da LGPD.

A legislação protege a privacidade do titular de dados à medida que fortalece o direito fundamental através de um controle procedimental em conformidade com a proteção jurídica que vem garantir aos indivíduos a liberdade de expressão, de informação, comunicação e inviolabilidade da intimidade, honra e imagem, ou seja de sua privacidade (PINHEIRO, 2023).

A LGPD se baseia na premissa de que o indivíduo é o titular de seus dados sensíveis e deve ter controle sobre como essas informações são coletadas, mantidas e utilizadas por terceiros.

Bioni (2019) ressalta que o conceito de autodeterminação informacional ultrapassa a noção de mero consentimento, o que significa que os indivíduos devem ter uma gestão mais abrangente de suas informações pessoais, e assim como a forma de consentimento como uma questão de processo destaca que o consentimento precisa ser obtido de forma clara e transparente, mas também deve estar inserido em um processo mais amplo de proteção de dados, que envolve a avaliação de riscos e a adoção de medidas de segurança. Na prática, o consentimento pode apresentar desafios, especialmente em situações em que os titulares de dados não possuem uma verdadeira liberdade de escolha ou quando o consentimento é obtido de maneira coercitiva. Não deixando de mencionar outras fundamentações legais para o tratamento de dados, como o interesse legítimo, que podem ser mais aplicáveis em determinadas circunstâncias, diminuindo assim a primazia do consentimento.

De toda forma, a LGPD confere autonomia para os titulares dos dados, com o intuito de garantir o exercício do direito, e para isto é essencial que todas as informações sobre o uso dos dados pessoais sejam fornecidas aos seus titulares de forma que estes estejam cientes de como os seus dados serão coletados, manipulados e utilizados para uma finalidade específica e reservadas as devidas exceções como: realização de estudos por órgãos de pesquisa, garantindo sempre que possível anonimização dos dados pessoais; cumprimento de obrigação regulatória ou legal pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos e convênios ou instrumentos congêneres e outros (BRASIL, 2018).

Há também a garantia aos detentores de informações, que é o direito à portabilidade dos dados pessoais, que ainda é um ponto que gera discussão no que diz respeito ao rol de direitos do art. 18:

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (BRASIL, 2018).

A LGPD se destaca pela sua abordagem detalhada na proteção dos dados pessoais em relação à autonomia do titular de dados, permitindo-lhe autorizar e restringir a forma como suas informações são manipuladas por terceiros, conceito conhecido como autodeterminação informativa. A utilização do consentimento é o principal mecanismo que legitima a coleta de dados nas redes sociais e em outras plataformas digitais similares. Muitos programas e aplicativos necessitam que os usuários forneçam uma autorização prévia para que os seus dados possam ser armazenados e processados. Apenas após concederem essa permissão e aceitarem os Termos de Uso e Políticas de Privacidade é que poderão acessar todas as funcionalidades disponíveis. O consentimento requer uma comunicação clara e antecipada ao titular, informando-o sobre a finalidade da coleta e do uso de seus dados pessoais, em conformidade com o princípio da transparência. Essa explicação visa assegurar que o titular tenha a capacidade de decidir quando e para quais propósitos ele opta por compartilhar suas informações (CARVALHO FILHO; GONDIM, 2023).

O art. 9º da LGPD oferece uma visão clara sobre a extensão das informações que devem ser disponibilizadas ao usuário em relação ao processamento de seus dados, sob risco de invalidar o consentimento solicitado. Conforme estipulado no artigo, é necessário esclarecer de maneira detalhada a finalidade específica do tratamento, a metodologia e a duração, respeitando os segredos industrial e comercial. É essencial que o usuário esteja ciente dos riscos mais comuns associados à manipulação de seus dados, ao mesmo tempo em que compreende suas responsabilidades pessoais ao utilizar as redes.

Dessa forma, o usuário terá um maior controle sobre suas informações pessoais, evidenciando que o exercício de sua autonomia implica uma série de responsabilidades, tanto para si quanto para quem trata e controla seus dados.

3.1 Agentes de Tratamento de Dados

A LGPD demonstra, de forma objetiva, a atuação dos agentes de tratamento de dados no capítulo VI, define os agentes de tratamento de dados em duas categorias principais: controlador e operador.

O controlador é o agente responsável pelo tratamento de dados pessoais, incumbido de tomar decisões sobre como esses dados serão tratados. Por outro lado, o operador executa o tratamento de dados seguindo as orientações do controlador. O controlador pode ser tanto uma pessoa física quanto uma jurídica, seja de direito público ou privado, e é ele quem tem a competência para tomar decisões relacionadas ao tratamento de dados. Portanto, é considerado o principal agente responsável.

O operador também pode ser uma pessoa física ou jurídica, de direito público ou privado, e sua função é realizar o tratamento de dados pessoais em nome do controlador. A diferença fundamental entre esses dois papéis é o poder decisório, pois o controlador pode delegar a um terceiro (o operador) a tarefa de tratar os dados em seu nome (CARLOTO; MOSELE, 2022).

O operador tem a limitação de decidir apenas sobre determinados tópicos, como a escolha do software, a segregação de acessos e outras medidas técnicas e administrativas relacionadas à segurança da informação, sem que isso mude sua função como operador. Essa distinção é crucial especialmente na implementação por parte de empresas ou entidades, em função do papel do controlador, que é o responsável pelas atividades de tratamento e possui autoridade para tomar decisões.

O "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado" é um documento elaborado pela ANPD (2021) que visa esclarecer e orientar sobre as definições e responsabilidades dos agentes de tratamento de dados pessoais, bem como sobre o papel do encarregado. Orienta que os agentes de tratamento tanto o controlador quanto o operador podem ser indivíduos ou entidades, sejam elas de direito público ou privado, e devem ser identificados com base em sua natureza institucional.

Ao se referir a uma pessoa jurídica, a organização será considerada o agente responsável pelo tratamento de dados nos termos da LGPD. Cabe a ela estabelecer as diretrizes para a gestão desses dados, que serão aplicadas por seus representantes ou designados. Sempre que uma pessoa jurídica estiver presente, ela atuará como agente de tratamento, podendo ser caracterizada como controlador ou operador. Será considerada controlador quando tomar decisões e emitir instruções sobre as atividades de tratamento, ou

como operador ao seguir essas instruções e tratar os dados conforme as orientações legais do controlador. Os gerentes, sócios e colaboradores do controlador têm uma vinculação direta a ele, sendo este o responsável. Da mesma forma, funcionários e outras pessoas físicas vinculadas ao operador agirão em seu nome (CARLOTO; MOSELE, 2022).

A definição legal de controlador não deve ser interpretada como uma norma que distribui internamente funções e responsabilidades. Na verdade, trata-se de uma disposição legal que impõe deveres específicos à pessoa jurídica, a qual assume a responsabilidade pelos atos realizados por seus representantes e prepostos em relação aos titulares e à ANPD.

O operador deve agir em conformidade com as obrigações previstas pela LGPD e seguir as instruções legítimas do controlador; caso contrário, ele será responsabilizado solidariamente pelos danos resultantes do tratamento de dados pessoais realizado, a LGPD impõe uma responsabilidade maior ao controlador, mesmo que haja responsabilidade solidária entre os agentes de tratamento.

Entre suas atribuições, o controlador deve elaborar um Relatório de Impacto à Proteção de Dados Pessoais, comunicar incidentes à ANPD elaborar o Registro das Atividades de Tratamento de Dados Pessoais e sua responsabilidade é definida nos artigos 42 a 45 da LGPD que trataremos a seguir.

4 A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DOS DADOS PESSOAIS

A responsabilidade decorre da realização de atividades relacionadas à proteção de dados que infrinjam a legislação de proteção de dados. Com essa formulação, o legislador admite que a proteção de dados constitui um microssistema, composto por normas estabelecidas em diferentes legislações, tendo a LGPD como seu alicerce fundamental (CAPANEMA, 2020).

A responsabilidade civil é abordada na Seção III do Capítulo VI da LGPD, que se intitula “Da Responsabilidade e do Ressarcimento de Danos”. Vale destacar que essas normas não se aplicam a todos os casos de responsabilidade civil, podendo, conforme a natureza da relação jurídica, serem substituídas por normas específicas, como as do Código de Defesa do Consumidor. Essa possibilidade é reconhecida de forma explícita pela LGPD em seu art. 45 (BRASIL, 2018).

A responsabilidade civil dos agentes que tratam dados pessoais é uma questão debatida entre a natureza subjetiva e objetiva dessa responsabilidade. O art. 5º, II, da LGPD define dados sensíveis, mas é importante observar que o tratamento de dados não

classificados como tais também pode resultar em discriminação, o que a LGPD busca evitar ao proteger essa categoria. Assim, tanto dados sensíveis quanto não sensíveis estão sujeitos a tratamentos que podem causar danos aos titulares, e não deve haver distinção na responsabilidade civil.

O art. 41 da LGPD fala sobre a figura do encarregado de dados (*Data Protection Officer*) que possui as seguintes atribuições: receber queixas e comunicações tanto dos titulares de dados pessoais quanto da ANPD, oferecer esclarecimentos e adotar as medidas necessárias, orientar internamente a empresa sobre as melhores práticas para a proteção de dados pessoais, além de outras responsabilidades que possam ser definidas pelo controlador, sem esquecer de cumprir ainda as funções que forem estabelecidas por normas complementares.

A LGPD não menciona diretamente a responsabilidade civil do encarregado, mas essa responsabilidade pode emergir, por exemplo, quando a função é desempenhada por uma pessoa física ou jurídica que não é parte do controlador ou do operador em uma relação de consumo. Como se trata de alguém envolvido na cadeia produtiva, essa pessoa poderá ser responsabilizada solidariamente pelos danos ocasionados (CAPANEMA, 2020).

A LGPD estabelece diversas obrigações para ambos os agentes, com o legislador definindo um padrão de conduta para esses profissionais. A ANPD enfatiza que tanto os controladores quanto os operadores devem ser transparentes em suas práticas de tratamento. Isso inclui a obrigação de prestar contas sobre as atividades realizadas e a implementação de políticas claras que demonstrem como os dados são tratados e protegidos.

Segundo o “Guia Orientativo. Tratamento de dados pessoais pelo Poder Público”, a ANPD também recomenda que as organizações desenvolvam relatórios de impacto à proteção de dados pessoais quando necessário, documentando os riscos associados ao tratamento e as medidas adotadas para mitigá-los (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2023).

De acordo com o art. 42⁷caput da lei, os controladores e operadores devem adotar medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados e vazamentos. Analisando, é possível observar a menção aos agentes de tratamento, que são classificados como controlador e operador.

⁷ Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (Lei nº 13.709/2018, art. 42 Caput).

Ambos têm a obrigação de reparar danos patrimoniais, morais, individuais ou coletivos, e são responsáveis de forma individual pelos danos que provocarem em decorrência do tratamento de dados pessoais. No entanto, há uma exceção a essa norma, prevista no § 1º do art. 42 da LGPD, que estabelece a possibilidade de responsabilidade solidária, quando ocorrerem evidentes violações à legislação de proteção de dados pessoais, decorrentes do exercício de suas atividades de tratamento.

O parágrafo 2º do art. 42 também se baseia no Código de Defesa do Consumidor no que se refere à questão da prova, com o objetivo de reduzir as desigualdades entre os agentes de tratamento e os titulares dos dados.

Embora a LGPD trate da inversão do ônus da prova na seção que aborda a responsabilidade civil, é possível compreender que o titular dos dados tem o direito de invocar essa cláusula em qualquer disputa relacionada ao tratamento de seus dados pessoais e é justificada pela hipossuficiência do titular de dados inserido em uma sociedade digital, onde seus dados são coletados numerosamente e por vezes de forma desnecessária. Nesse contexto, o titular dos dados se encontra em uma posição desfavorável, quase impossível de saber quais de seus dados estão sendo tratados, como isso acontece e quem são os agentes responsáveis pelo tratamento (SURIS; DIAS, 2024).

A responsabilidade civil prevista na LGPD exige a verificação da culpa e do nexo causal entre a ação do agente e o dano sofrido pelo titular. A ANPD enfatiza que a simples ocorrência de um incidente não é suficiente para caracterizar a responsabilidade; é necessário demonstrar que houve falha na observância das normas de proteção de dados pessoais.

No art. 43, encontram-se as excludentes de responsabilidade civil no que se refere ao tratamento de dados pessoais. A primeira hipótese, descrita no inciso I, aplica-se quando um terceiro causa o dano, não havendo o nexo de causalidade que possibilite a responsabilização dos envolvidos. O inciso II, por sua vez, estabelece que os agentes estão isentos de responsabilidade se não houve violação à legislação de proteção de dados, isto é, quando o tratamento for realizado de maneira regular, essa é a hipótese em que há a ocorrência de um dano, mas não há ilícito por parte do agente; é o caso, por exemplo, de uma decisão automatizada (MEDEIROS, 2021).

Cabe explicar que o art. 43⁸, inciso III, utiliza a expressão "culpa exclusiva" do usuário ou de terceiros, no entanto, o uso da palavra "culpa" neste contexto é impróprio. Isso

⁸ “Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

porque a excludente não requer a demonstração da culpa da vítima, mas sim a limitação da sua colaboração causal na ocorrência do dano, dessa forma é possível concluir que, para que os agentes sejam responsabilizados, é necessário que haja uma violação de um dever fundamental, afastando a ideia de que a simples ocorrência de um dano seria suficiente para a responsabilização (SURIS; DIAS, 2024).

O art. 44⁹, caput, da LGPD, define as situações em que o tratamento de dados pessoais é considerado irregular, mas não especifica as consequências jurídicas decorrentes dessa irregularidade. Conforme esse artigo, existem duas situações que caracterizam o tratamento inadequado: a primeira refere-se ao tratamento que não está em conformidade com as normas legais; a segunda envolve a falta de segurança esperada pelo titular dos dados, o caput do art. 44 não atribui efeitos legais ao tratamento irregular, e isto fica a cargo da ANPD a tarefa de garantir a proteção dos dados pessoais, conforme estipulado no art. 55-J da LGPD (SURIS; DIAS, 2024).

O art. 45 da LGPD trata da responsabilidade civil no contexto das relações de consumo, que continuam a ser reguladas pelo Código de Defesa do Consumidor (CDC), isso atribui ao titular dos dados um sistema de responsabilidade considerado mais seguro. Nesse sentido, a LGPD possui uma estrutura normativa semelhante à do CDC, priorizando a proteção do titular em detrimento dos interesses de terceiros. Para o legislador quem fornece os seus dados é a parte vulnerável na relação, ou seja, carece de recursos jurídicos para fiscalizar o tratamento dos seus dados pessoais, dada a importância desses dados na sociedade da informação. Neste sentido é necessário observar que a violação de dados de consumidores com a incidência do Código de Defesa do Consumidor, asseguram a presença de mais de um regime de responsabilidade civil (MAIMONE, 2022).

Os artigos 46 e seguintes da LGPD abordam a proteção de dados, governança e as sanções administrativas cabíveis em casos de incidentes de segurança. Esses dispositivos reconhecem a importância de boas práticas no tratamento de dados pessoais, destacando a necessidade de implementar medidas que previnam e evitem prejuízos aos titulares de dados.

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.”

⁹ Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

A LGPD adota a teoria subjetiva da responsabilidade civil, exigindo que se comprove a culpa do agente de tratamento no momento do dano. Essa responsabilidade se baseia em dois critérios: a falha em implementar medidas de segurança adequadas para o tratamento dos dados por exemplo: quando não fornecer a segurança que o titular pode esperar; e o descumprimento das obrigações estabelecidas na lei: violar a legislação de proteção de dados pessoais ou deixando de cumprir a legislação.

Na visão de (GUEDES; MEIRELES, 2019), a violação da lei seria elemento subjetivo da obrigação de indenizar e indicaria a conduta culposa do agente de tratamento de dados, dessa forma não haverá obrigação de indenizar quando o agente de tratamento de dados tiver demonstrado que qualquer incidente que ocorreu não foi em razão de sua conduta culposa.

Há uma corrente que sustenta a teoria objetiva da responsabilidade, argumentando que o simples fato de ocorrer um dano em decorrência do tratamento de dados pessoais já implica na obrigação, independentemente da análise da culpa do agente. (DONEDA; MENDES, 2018), defendem essa perspectiva ao enfatizar que uma atividade de tratamento de dados envolve riscos intrínsecos, uma vez que existe uma possibilidade considerável de danos caso esses direitos sejam violados, os quais possuem a natureza de direitos personalíssimos e fundamentais. Os autores partem do princípio de que a legislação voltada à proteção de dados tem como um de seus pilares a mitigação de riscos de prejuízos. De fato, a lei estabelece como um de seus princípios, no art. 6º, inciso III, a necessidade de limitar o tratamento aos dados estritamente necessários para alcançar suas finalidades, assegurando que os dados sejam pertinentes, proporcionais e não excessivos em relação aos objetivos do tratamento. Esse dever está diretamente ligado ao fator de risco associado ao tratamento de dados (DONEDA; MENDES, 2018).

Em outro posicionamento, BODIN DE MORAES; QUEIROZ (2019) defendem que a LGPD adota o que se denomina teoria ativa ou proativa da responsabilidade civil. Essa abordagem ressalta a importância de avaliar a responsabilidade civil a partir de uma perspectiva otimista, fundamentada na necessidade de os agentes de tratamento de dados adotarem atitudes que promovam a prevenção de danos, considerando que a obrigação de reparação deve ser uma exceção. Afirmam que a proteção da privacidade, por meio da mera abstenção de interferência na esfera individual, abre espaço para um cuidado positivo e proativo, que assegura ao titular o pleno conhecimento sobre as formas de tratamento, as finalidades e o destino de seus dados.

Isto reforça que a responsabilidade proativa está respaldada no art. 6º, inciso X, da LGPD, que estabelece o princípio da responsabilização e da prestação de contas. Esse princípio obriga os agentes de tratamento de dados pessoais a comprovar, por meio de evidências, que adotaram medidas eficazes que asseguram o cumprimento e a observância das normas de proteção de dados pessoais, além de confirmar a eficácia dessas ações (BODIN DE MORAES; QUEIROZ, 2019).

Fazendo uma avaliação dos artigos relacionados à responsabilidade civil na LGPD e uma interpretação sistemática da lei, o que se extrai é que a responsabilidade civil adotada pela LGPD não é objetiva. Considerando que o modelo de conduta que impõe obrigações aos controladores e operadores, e o descumprimento dessas obrigações pode resultar em culpa.

A implementação de uma responsabilidade proativa deve ser priorizada, e está alinhada com as melhores práticas, como também fomenta uma cultura de prevenção essencial para a proteção eficaz de dados pessoais. Segundo Maria Celina Bodin de Moraes (2019), ao discutir a responsabilidade civil proativa, ela destaca que essa abordagem se concentra na prestação de contas, sendo responsabilidade das empresas e da Administração Pública identificar os riscos associados às suas atividades de tratamento de dados pessoais e selecione as medidas mais adequadas para mitigá-los.

É fundamental estabelecer uma definição legal que esteja em harmonia com a doutrina sobre qual tipo de responsabilidade deve ser aplicada aos agentes de tratamento de dados. Isso pode incluir a integração de diferentes modelos de responsabilidade civil, garantindo que os agentes sejam incentivados a adotar medidas preventivas e, ao mesmo tempo, responsabilizados especificamente em casos de violações (ROCHA, 2024).

5 CONCLUSÃO

Este artigo teve como finalidade analisar a responsabilidade civil dos agentes de tratamento de dados pessoais à luz da Lei Geral de Proteção de Dados (LGPD). A pesquisa buscou compreender como a legislação brasileira estabelece diretrizes para a responsabilização dos controladores e operadores de dados, considerando as implicações jurídicas do descumprimento das normas.

A problemática central dessa pesquisa se concentrou em analisar como a LGPD regula a responsabilidade civil dos agentes de tratamento de dados, mediante a necessidade de garantir a proteção dos direitos dos titulares de dados em um contexto de crescente digitalização e uso significativo de informações pessoais.

Entretanto, algumas limitações foram identificadas ao longo da pesquisa. A análise se concentrou na legislação brasileira e na comparação com o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, podendo não abranger completamente as nuances e variações nas práticas de proteção de dados em outros países. Além disso, a evolução contínua da legislação e das práticas relacionadas à proteção de dados pode tornar algumas contribuições temporárias, exigindo revisões futuras para manter a relevância do estudo.

Os resultados da pesquisa indicam que a LGPD introduz uma abordagem híbrida em relação à responsabilidade civil, combinando elementos de responsabilidade subjetiva e objetiva. Essa dualidade reflete uma preocupação com a prevenção de danos e a segurança no tratamento de dados, enfatizando a necessidade de que os agentes adotem medidas proativas para proteger os direitos dos titulares. Nesse sentido a teoria da responsabilidade subjetiva proativa, está mais alinhada com as necessidades reais, com medidas de prevenção, transparência e autodeterminação informacional do titular de forma ampla e clara.

As contribuições deste estudo são significativas, pois não apenas esclarecem as responsabilidades legais dos agentes de tratamento, mas também promovem a compreensão sobre a importância da proteção de dados pessoais na sociedade contemporânea.

O trabalho oferece um panorama sobre as implicações práticas da LGPD para organizações e indivíduos, destacando a relevância da conformidade legal na proteção dos direitos fundamentais. Ao discutir as diferentes correntes doutrinárias sobre responsabilidade civil, o artigo contribui para o debate acadêmico e jurídico sobre o tema, incentivando futuras investigações que possam aprofundar ainda mais o entendimento sobre a responsabilidade civil no contexto da proteção de dados pessoais.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Perguntas Frequentes. 3.1 - O que é a Autoridade Nacional de Proteção de Dados Pessoais - ANPD?** Portal Gov.br, 2024. Disponível em: <<https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes>>. Acesso em: 13 out. 2024.

BRASIL. **Senado Federal aprova Proposta de Emenda à Constituição 17 (PEC 17/2019) que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais.** 2021. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais>>. Acesso em: 9 set. 2024.

BRASIL. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Brasília: ANPD, 2023. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>>. Acesso em: 10 out. 2024.

BRASIL. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília: ANPD, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf>. Acesso em: 10 out. 2024.

BEZERRA, Daniel Teixeira; FURTADO, Gabriel Rocha. **A (in)constitucionalidade da Medida Provisória nº 954/2020: o marco jurisprudencial brasileiro do direito fundamental à proteção de dados pessoais.** *Civilistica.com*, Rio de Janeiro, v. 12, n. 1, p. 1–13, 2023. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/849/692>>. Acesso em: 16 ago. 2024.

BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento.** 1 ed. 2 reimp. Rio de Janeiro: Forense, 2019.

BODIN DE MORAES, Maria Celina. **LGPD: um novo regime de responsabilização civil dito proativo.** *Civilistica.com*, Rio de Janeiro, v. 8, n. 3, p. 1–6, 2019. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/448>>. Acesso em: 13 out. 2024.

BODIN DE MORAES, Maria Celina; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP.** *Cadernos Adenauer*, v. 3, ano XX, 2019. Rio de Janeiro: Fundação Konrad Adenauer. Disponível em: <https://www.academia.edu/41132175/Autodetermina%C3%A7%C3%A3o_informativa_e_responsabiliza%C3%A7%C3%A3o_proativa_novos_instrumentos_de_tutela_da_pessoa_humana_na_LGDP?auto=download>. Acesso em: 10 set. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 13 out. 2024.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Rio de Janeiro, RJ: 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 13 out. 2024.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em: 13 out. 2024.

BRASIL. **Lei nº 5.172, de 25 de outubro de 1966.** Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília, DF: 1966. Disponível em:

<https://www.planalto.gov.br/ccivil_03/leis/L5172Compilado.htm>. Acesso em: 13 out. 2024.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2022. Institui o Código Civil. Brasília, DF: 2022. Disponível em:

<https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm>. Acesso em: 13 out. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: 2012. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Acesso em: 13 out. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: 2014 . Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 13 out. 2024.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Brasília, DF: 2015. Disponível em: <[https://www.planalto.gov.br/ccivil_03/_ato2015-](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm)

2018/2015/lei/113105.htm>. Acesso em: 13 out. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: 2018 . Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 13 out. 2024.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: 2019 . Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm>. Acesso em: 13 out. 2024.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: 2021. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm>. Acesso em: 13 out. 2024.

BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: 2018 .

Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 13 out. 2024.

BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço

Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv954.htm>. Acesso em: 13 out. 2024.

CARLOTO, Selma; MOSELE, Rafael. **Agentes de tratamento com base na LGPD**. Site Consultor Jurídico, 2022. Disponível em: <<https://www.conjur.com.br/2022-abr-06/carloto-mosele-agentes-tratamento-base-lgpd/>>. Acesso em: 13 out. 2024.

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 163-170, jan.-mar. 2020. Disponível em: <<https://bdjur.stj.jus.br/jspui/handle/2011/142288>>. Acesso em: 10 set. 2024.

CARVALHO FILHO, Geovana de; GONDIM, Glenda Gonçalves. **“Automatização” do usuário: o consentimento irrefletido para tratamento de dados pessoais como contrapartida ao exercício do direito à informação**. Civilistica.com, Rio de Janeiro, v. 12, n. 2, p. 1–20, 2023. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/907>>. Acesso em: 10 set. 2024.

CÉSAR, Daniel; BARRETO JUNIOR, Irineu Francisco. **Marco civil da internet e neutralidade da rede: aspectos jurídicos e tecnológicos**. Revista Eletrônica do Curso de Direito da UFSM, [s. l.], v. 12, n. 1, p. 65–88, 2017. DOI: 10.5902/1981369423288. Disponível em: <<https://periodicos.ufsm.br/revistadireito/article/view/23288>>. Acesso em: 18 nov. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo; MENDES, Laura Schertel. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2018. Disponível em: <<https://typeset.io/pdf/reflexoes-iniciais-sobre-a-nova-lei-geral-de-protecao-de-3lrj4cysu6.pdf>>. Acesso em: 10 set. 2024.

FULLER, Greice Patricia; TATEOKI, Victor Augusto. **Os dados pessoais como bem jurídico a ser penalmente tutelado na sociedade da informação**. Revista Em Tempo, [S. l.], v. 22, n. 1, p. 110-124, fev. 2023. DOI: <https://doi.org/10.26729/et.v22i1.3264>. Disponível em: <<https://revista.univem.edu.br/emtempo/article/view/3264>>. Acesso em: 9 set. 2024.

FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO (FIA). **Plataformas digitais: o que são, tipos e as mais usadas**. 2023. Disponível em: <<https://fia.com.br/blog/plataformas-digitais/>>. Acesso em: 10 set. 2024.

GOMES, Samuel. **O que é e quais são os Remédios Constitucionais?** Site Jusbrasil, 2022. Disponível em: <<https://www.jusbrasil.com.br/artigos/o-que-e-quais-sao-os-remedios-constitucionais/1672264748#:~:text=O%20termo%20Rem%C3%A9dio%20Constitucional%20indica,direitos%20p%C3%ABlicos%20ou%20liberdades%20p%C3%ABlicas>>. Acesso em: 13 out. 2024.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. **Término do tratamento de dados**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Org.). Lei Geral de Proteção de Dados Pessoais. São Paulo: RT, 2019, p. 231.

LIMA, Ricardo Alves de; GARRIDO, Guilherme Leite. **Lei Geral de Proteção de Dados Pessoais (LGPD) e compliance: um panorama da adequação normativa para organizações contemporâneas**. Revista Eletrônica do Curso de Direito da UFSM, [s. l.], v. 17, n. 1, p. e68680, 2022. DOI: 10.5902/1981369468680. Disponível em: <<https://periodicos.ufsm.br/revistadireito/article/view/68680>>. Acesso em: 18 nov. 2023.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade civil na LGPD: efetividade na proteção de dados pessoais**. Indaiatuba, SP: Editora Foco, 2022.

MEDEIROS, Thais Carneiro. **Responsabilidade Civil pela Violação ao Direito à Proteção de Dados Pessoais**. 2021.47 f. Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2021.

MENDES, Gilmar Ferreira.; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 12 ed. São Paulo: Saraiva, 2015.

NASCIMENTO, Dijeison Tiago Rios. **A importância da Lei de Acesso à Informação no desenvolvimento da cidadania participativa e no controle da res publica**. Caderno Virtual, [S. l.], v. 1, n. 33, 2016. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/1200>>. Acesso em: 18 nov. 2023.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei N 13.709/2018 (LGPD)**. 4. ed. São Paulo, SP: SaraivaJur, 2023.

PORTAL DA CÂMARA DOS DEPUTADOS. **Proposição: 2210757**. Senado Federal. Brasília, DF: 2019. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>>. Acesso em: 21 ago. 2024.

PRIVACY TOOLS. **Quais são os países com maior proteção de dados pessoais?** 2019. Disponível em: <<https://www.privacytools.com.br/quais-sao-os-paises-com-maior-protecao-de-dados-pessoais/>>. Acesso em: 5 out. 2024.

ROCHA, Bruna Aparecida. **Da Responsabilidade Civil dos Agentes de Tratamento de Dados Pessoais no Brasil**. Site Jusbrasil, 2024. Disponível em: <https://www.jusbrasil.com.br/artigos/da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-no-brasil/2717371610?_gl=1*18gn6qd*_gcl_au*MjEzNTczNjg5Mi4xNzIyNzM5MjYx*_ga*NjkzODA4ODY5LjE2ODAyMjc1MjA.*_ga_QCSXBQ8XPZ*MTcyODc5Nzg5My42NC4xLjE3Mjg3OTc5MTkuNjAuMC4w>. Acesso em: 13 out. 2024.

ROMERO, Adriana. **STF e proteção de dados pessoais: Decisões da Corte marcaram a evolução de um novo direito fundamental**. Site <https://noticias.stf.jus.br/>. Brasília, DF: 2024. Disponível em: <<https://noticias.stf.jus.br/postsnoticias/stf-e-protecao-de-dados-pessoais-decisoes-da-corte-marcaram-a-evolucao-de-um-novo-direito-fundamental/>>. Acesso em: 21 ago. 2024.

SURIS, J.; BRASIL DIAS, Ádamo. **UMA ANÁLISE CRÍTICA ACERCA DO REGIME DE RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS**. Revista da Defensoria Pública do Estado do Rio Grande do Sul, Porto Alegre, v. 1, n. 34, p. 286–305, 2024. Disponível em: <<https://revistadpers.emnuvens.com.br/defensoria/article/view/643>>. Acesso em: 13 out. 2024.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, v. 33, 2010.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. EUR-Lex - 02016R0679-20160504 - PT - EUR-Lex . Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>>. Acesso em: 13 out. 2024.

VIANNA, Fernando. **Se os Dados são o Novo Petróleo, Onde Estão os Royalties? O Neoliberalismo na Era do Capitalismo de Vigilância**. Revista Gestão & Conexões, [S. l.], v. 10, n. 3, p. 123–143, 2021. DOI: 10.47456/regec.2317-5087.2021.10.3.36014.128-147. Disponível em: <<https://periodicos.ufes.br/ppgadm/article/view/36014>>. Acesso em: 13 out. 2024.