1 CONSIDERAÇÕES INICIAIS

O presente artigo tematiza o tratamento de dados sensíveis no contexto da educação de nível superior em IES privadas no Brasil e a proteção conferida pela LGPD. A produção de dados sensíveis no contexto da educação de nível superior em Instituições de Ensino Superior (IES) privadas no Brasil representa uma questão de grande relevância, especialmente diante do dos avanços tecnológicos experimentados nas últimas décadas. As IES privadas, na sociedade da informação, lidam com uma vasta gama de informações pessoais dos estudantes, que incluem não apenas dados acadêmicos, mas também informações financeiras, de saúde e outras classificadas como sensíveis. A coleta, armazenamento e uso desses dados devem se dar de tal sorte a assegurar a privacidade e a segurança dos titulares dessas informações.

A ocorrência de incidentes envolvendo a segurança de dados em Instituições de Ensino Superior (IES) privadas no Brasil tem se tornado cada vez mais comum, evidenciando a vulnerabilidade dessas instituições diante de ciberataques. Recentemente, o Centro Universitário FMU comunicou a detecção de um incidente em sua base de dados que pode ter resultado na visualização não autorizada de informações pessoais. Em resposta ao ocorrido, a instituição informou que prontamente adotou medidas para mitigar possíveis danos à sua comunidade acadêmica, reafirmando seu compromisso com a privacidade e a segurança dos dados (Silva, 2022).

Esse caso não é isolado; outras instituições de ensino superior também têm sido alvos de cibercriminosos, destacando a fragilidade do setor educacional diante das ameaças digitais. Em abril deste ano, a Escola Superior do Ministério Público da União (ESMPU) foi vítima de um ataque cibernético que resultou na criptografia dos dados em seus computadores, levando à desconexão das máquinas da rede para impedir a propagação do vírus (Silva, 2022).

De forma semelhante, o Grupo Marista, que administra diversas instituições, incluindo a Pontifícia Universidade Católica do Paraná (PUCPR), sofreu um incidente no início de 2022 que resultou na suspensão temporária dos sistemas operacionais e do acesso à rede. Esses exemplos sublinham a importância de uma robusta política de segurança da informação nas IES privadas, conforme exigido pela Lei Geral de Proteção de Dados (LGPD), que busca proteger os direitos dos titulares de dados pessoais em um ambiente cada vez mais vulnerável a ameaças cibernéticas (Silva, 2022).

Desta forma, a proteção dos dados de discentes no contexto da educação superior privada no Brasil é de fundamental importância, especialmente considerando o avanço tecnológico e a crescente digitalização dos processos acadêmicos na sociedade da informação.

Com a migração de informações pessoais e acadêmicas para plataformas digitais, essas instituições acumulam um volume significativo de dados sensíveis, que incluem desde informações financeiras até registros acadêmicos e de saúde. A preservação da privacidade e a segurança desses dados não apenas cumprem as exigências legais estabelecidas pela Lei Geral de Proteção de Dados (LGPD), mas também garantem a confiança dos estudantes e preservam a integridade das instituições educacionais em um ambiente onde as ameaças cibernéticas se tornam cada vez mais sofisticadas e frequentes.

Neste sentido e considerando o tratamento de dados sensíveis no contexto do ensino superior em instituições privadas no Brasil, o problema de pesquisa pode ser assim sintetizado: quais os limites e possibilidades apresentadas pela Lei Geral de Proteção de Dados na tutela dos direitos da personalidade de discentes?

A hipótese formulada para responder ao problema proposto pode ser resumida da seguinte maneira: a proteção de dados de discentes na educação superior privada no Brasil apresenta desafios significativos a serem superados. A qualidade dos dados tratados nesse contexto pode gerar danos relevantes à esfera extrapatrimonial dos indivíduos. Nesse sentido, a sociedade da informação exige um cuidado especial com os dados pessoais, que, devido à sua importância, devem receber proteção jurídica efetiva. Para que a legislação vigente assegure a proteção de dados dos discentes, é necessário que ela esteja alinhada com os direitos da personalidade envolvidos, proporcionando uma proteção ampla e integral aos titulares desses dados.

O objetivo geral da presente pesquisa consiste em analisar sob quais aspectos a LGPD confere proteção efetiva aos direitos da personalidade de discentes em face da produção de dados sensíveis no âmbito de instituições privadas de ensino superior.

Para alcançar o objetivo geral foram estabelecidos três objetivos específicos que serão espelhados nos tópicos de desenvolvimento deste artigo: a) delinear o contexto do tratamento de dados sensíveis de discentes no âmbito das instituições privadas de ensino superior à luz da teoria dos direitos da personalidade; b) empreender uma análise da evolução legislativa da proteção de dados sensíveis no Brasil; c) avaliar os limites e possibilidades da LGPD no que se refere à proteção de dados sensíveis de discentes e tutela dos direitos da personalidade no contexto das instituições privadas de ensino superior.

Empregou-se o método de pesquisa hipotético-dedutivo que parte do problema proposto que versa sobre o tratamento de dados de discentes, contexto da educação superior privada brasileira e a proteção conferida pela LGPD com vistas aos direitos da personalidade envolvidos. Sendo que o método passou pela formulação de hipótese e por um processo de

inferência dedutiva, o qual testa a predição da ocorrência de fenômenos abrangidos pela referida hipótese, mediante aplicação da técnica de pesquisa bibliográfica e documental, consistente na análise e estudo de obras, artigos científicos e na própria legislação pátria, em especial a Lei Geral de Proteção de Dados; e demais materiais que versam sobre o tema.

2 O TRATAMENTO DE DADOS SENSÍVEIS DISCENTES NO CONTEXTO DAS INSTITUIÇÕES PRIVADAS DE ENSINO SUPERIOR À LUZ DOS DIREITOS DA PERSONALIDADE

O tratamento de dados sensíveis de discentes no contexto das instituições privadas de ensino superior no Brasil constitui uma questão de crescente relevância, especialmente quando analisado à luz dos direitos da personalidade. Com o avanço tecnológico e a consolidação da sociedade da informação, essas instituições passam a lidar com volumes cada vez maiores de dados pessoais, que incluem informações altamente sensíveis. Essas informações, se tratadas inadequadamente, podem resultar em impactos significativos na esfera privada dos indivíduos.

Diante desse cenário, é imperativo compreender como os direitos da personalidade são protegidos pela legislação vigente, em especial pela Lei Geral de Proteção de Dados (LGPD), no âmbito do ensino superior privado. A análise desse tema revela não apenas os desafios enfrentados pelas instituições na proteção desses dados, mas também a necessidade de uma atuação jurídica eficaz para assegurar a integridade e a confidencialidade das informações pessoais dos discentes.

No contexto das Instituições de Ensino Superior (IES) privadas, o tratamento de dados sensíveis dos discentes exige um cuidado redobrado, dado o caráter altamente pessoal e potencialmente prejudicial dessas informações. A Lei Geral de Proteção de Dados (LGPD) estabelece um arcabouço normativo para a proteção de dados, mas sua aplicação prática nas instituições educacionais revela desafios específicos, como garantir a conformidade com as normas de consentimento e segurança.

2.1 IES privadas e o tratamento de dados sensíveis dos discentes

A era da informação trouxe mudanças profundas nas interações sociais, remodelando a forma como o tempo e o espaço são vivenciados (Castells, 2022). O avanço tecnológico tem eliminado as limitações tradicionais de tempo e espaço, possibilitando um acesso, coleta e manipulação de dados digitais com uma agilidade sem precedentes. A tecnologia moderna

transformou a maneira como as informações são geridas e compartilhadas, permitindo que essas operações ocorram instantaneamente e de maneira global.

Atualmente, a sociedade está imersa na "Era Digital", uma época caracterizada pela crescente imersão no universo virtual. A predominância do ambiente online resultou em uma intensa interconexão entre os indivíduos, gerando uma vasta quantidade de dados sobre suas preferências e comportamentos. Esse fenômeno sugere que a natureza humana está se tornando cada vez mais complexa e multifacetada, conforme observado por Siqueira, Lara e Alves (2021).

O fenômeno da datificação surge da geração massiva de dados na era digital, levando ao conceito de Big Data, que descreve a capacidade de extrair novas informações ao analisar grandes volumes de dados. Esse processo não apenas proporciona insights valiosos, mas também agrega valor a produtos e serviços. A datificação, por sua vez, refere-se à coleta abrangente de informações sobre praticamente todos os aspectos da vida para utilização futura (Botelho, 2020). Esse avanço na datificação tem acelerado e intensificado sua importância na sociedade contemporânea, uma vez que a abundância de dados permite direcionar estratégias empresariais, otimizar lucros e até influenciar campanhas políticas e decisões nacionais.

A datificação oferece uma maneira superior de moldar as demandas do mercado ao se basear nas preferências identificadas através das escolhas pessoais. Esta abordagem inovadora utiliza as informações individuais para direcionar as estratégias de mercado, evidenciando a capacidade de capturar e aplicar dados de forma estratégica. Como resultado, a datificação se estabelece como uma ferramenta crucial para as empresas que desejam entender e prever as necessidades dos consumidores, desempenhando um papel vital na adaptação aos desafios e oportunidades da economia digital (Zuboff, 2020).

Os avanços no Big Data e na datificação têm causado impactos profundos na vida pessoal, na intimidade e na privacidade dos indivíduos. Esses processos se tornaram recursos cruciais tanto para instituições públicas quanto privadas na análise e aproveitamento de dados (Botelho, 2020). Além disso, a tecnologia tem transformado significativamente as instituições de ensino, permitindo a coleta e análise de uma quantidade crescente de informações sobre alunos e professores. Embora esses dados possam ser utilizados para aprimorar serviços e tomar decisões mais precisas, é crucial abordar a coleta, armazenamento e uso dessas informações com ética e responsabilidade, assegurando sempre a proteção dos direitos e da privacidade dos envolvidos.

A interação entre alunos e instituições de ensino superior privadas está fundamentada em um processo rápido e extenso de coleta de dados. Tradicionalmente, o foco dessa coleta é

visto como algo restrito ao preenchimento das fichas de matrícula. No entanto, essa visão está bastante dissociada da realidade, que revela uma coleta e produção de dados muito mais complexas e abrangentes envolvendo todos os participantes desse processo

Além das notas e registros de frequência, que são naturalmente gerados durante o processo de ensino-aprendizagem, outras informações também são produzidas, frequentemente sem o pleno conhecimento dos indivíduos envolvidos. Um exemplo disso são os relatórios sobre o desempenho e o comportamento dos alunos. Esses documentos, sem dúvida, constituem dados sensíveis que, em caso de vazamento, podem acarretar sérios danos à esfera dos direitos personalíssimos de seus titulares.

As instituições de ensino, sejam públicas ou privadas, enfrentam o desafio de equilibrar a proteção de dados com a continuidade de suas operações. Para garantir a conformidade com a Lei Geral de Proteção de Dados, é crucial revisar e ajustar os modelos de trabalho em diversas áreas da instituição. Isso implica em investimentos significativos em formação de pessoal e na implementação de novas tecnologias (Jesus; Canevari; Silva, 2020).

2.2 Os direitos da personalidade em face do tratamento de dados sensíveis nas IES privadas

O tratamento de dados sensíveis nas Instituições de Ensino Superior (IES) privadas tem suscitado importantes discussões sobre a proteção dos direitos da personalidade, que incluem a dignidade, a privacidade, a honra e a imagem dos indivíduos. Esses direitos, que possuem status constitucional, são fundamentais para a preservação da integridade pessoal em um contexto em que o armazenamento e a manipulação de informações digitais se tornaram corriqueiros. No ambiente acadêmico, os dados sensíveis dos discentes, como histórico escolar, informações financeiras, registros de saúde e até mesmo convicções políticas ou religiosas, exigem um tratamento rigoroso e ético para evitar violações que possam comprometer a esfera íntima desses indivíduos.

As IES privadas, ao coletarem e processarem tais dados, assumem a responsabilidade de garantir que esses direitos sejam respeitados, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD). Esta legislação impõe uma série de obrigações às instituições, desde a obtenção do consentimento dos titulares para o tratamento dos dados até a implementação de medidas de segurança que previnam acessos não autorizados e vazamentos. A falta de conformidade com a LGPD pode não apenas resultar em sanções legais, mas também em danos irreparáveis à reputação das instituições e à confiança dos discentes.

Os direitos da personalidade no contexto do tratamento de dados sensíveis ganham especial relevância quando consideramos os possíveis impactos negativos que a má gestão dessas informações pode gerar. Um exemplo disso é o vazamento de dados, que pode expor os discentes a situações de discriminação, exclusão social ou mesmo fraudes. Ademais, o uso inadequado de dados sensíveis pode afetar a imagem e a honra dos indivíduos, principalmente quando informações pessoais são compartilhadas sem o devido consentimento ou são utilizadas para fins diversos daqueles originalmente previstos.

Em suma, o respeito aos direitos da personalidade no tratamento de dados sensíveis nas IES privadas é um desafio constante que exige uma abordagem multidisciplinar, envolvendo aspectos jurídicos, tecnológicos e éticos. A conformidade com a LGPD é essencial para garantir que os dados dos discentes sejam protegidos de forma adequada, preservando sua dignidade e privacidade. As instituições que investem na proteção desses direitos não apenas cumprem suas obrigações legais, mas também fortalecem a confiança de seus alunos, contribuindo para um ambiente educacional mais seguro e respeitoso.

3 EVOLUÇÃO LEGISLATIVA NA PROTEÇÃO DE DADOS NO BRASIL: ANTECEDENTES DA LEI GERAL DE PROTEÇÃO DE DADOS E SEUS ASPECTOS DESTACADOS

3.1 Antecedentes no direito internacional

A relação entre o direito à privacidade e a tecnologia da informação possui tanto esferas positivas quanto negativas. No tocante ao lado negativo, destaca-se a necessidade de proteção abrangente dos dados pessoais, especialmente daqueles considerados sensíveis. Sob a ótica positiva, incluem-se o direito de acessar as informações pessoais e o direito ao esquecimento. Contudo, o exercício desse último direito torna-se cada vez mais desafiador devido ao armazenamento prolongado de dados, evidenciando a importância de estabelecer na legislação um prazo definido para a retenção dessas informações (Limberger, 2009).

A evolução da legislação de proteção de dados pessoais tem sido marcada por desenvolvimentos significativos ao longo dos anos. O conceito de proteger a privacidade e as informações pessoais dos indivíduos tornou-se cada vez mais importante na era digital. Nas fases iniciais, as leis de proteção de dados focavam principalmente em salvaguardar a privacidade das pessoas no contexto do processamento manual de dados. No entanto, com o rápido avanço da tecnologia, especialmente com o uso generalizado da internet e ferramentas

digitais, a necessidade de leis de proteção de dados mais abrangentes e robustas tornou-se evidente (Souza, 2024).

A primeira onda de legislações sobre proteção de dados pessoais surgiu a partir da crescente preocupação com o tratamento extensivo das informações dos cidadãos no contexto do desenvolvimento do Estado Moderno. Naquele período, a abordagem regulatória concentrou-se em gerenciar a própria tecnologia, garantindo que ela fosse moldada e orientada pelos princípios democráticos. Havia um receio significativo de que uma vigilância invasiva, semelhante à figura distópica do Grande Irmão descrito por Orwell, pudesse ameaçar a liberdade individual. Assim, a estratégia escolhida foi a de regular a criação e operação de bancos de dados através da concessão de permissões específicas para seu funcionamento (Bioni, 2020).

Resumidamente, a característica distintiva da primeira fase da proteção de dados pessoais é sua ênfase na regulação do setor governamental e na imposição de normas rigorosas para controlar o uso da tecnologia. No entanto, à medida que o processamento de dados se expandiu além da esfera governamental, houve um aumento significativo no número de envolvidos e, consequentemente, no volume de bancos de dados que precisavam ser regulamentados e autorizados (Bioni, 2020).

A segunda geração de legislações sobre proteção de dados pessoais marca uma transformação no foco regulatório, abrangendo não apenas os bancos de dados governamentais, mas também aqueles pertencentes ao setor privado (Doneda, 2021).

Dessa forma, a abordagem regulatória anterior, que atribuía ao Estado a responsabilidade de autorizar a criação e a operação de todos os bancos de dados, mostrou-se impraticável. Na segunda geração de legislações, a proteção dos dados pessoais passa a ser responsabilidade do próprio titular. Em vez de depender da autorização estatal para o fluxo de informações pessoais, agora é o indivíduo quem deve exercer controle sobre a coleta, uso e compartilhamento de seus dados, estabelecendo suas próprias preferências por meio do consentimento (Bioni, 2020).

A crescente importância atribuída ao papel do indivíduo na proteção dos dados pessoais marca a transição para a terceira geração de leis. Nesta fase, as normas passaram a garantir que o titular dos dados tivesse uma participação ativa em cada etapa do tratamento de suas informações, desde a coleta até o compartilhamento. Esse avanço reflete a idealização da "autodeterminação informativa", permitindo ao indivíduo um controle mais abrangente e detalhado sobre suas informações pessoais (Bioni, 2020).

A quarta geração de leis surgiu para abordar essas limitações, introduzindo autoridades independentes responsáveis pela aplicação das normas de proteção de dados e criando novas regulamentações. Essas mudanças diminuíram a centralidade do consentimento, ao permitir o processamento de certos tipos de dados pessoais sem depender exclusivamente da autorização do indivíduo (Bioni, 2020).

No cenário internacional, um marco histórico fundamental para o direito à privacidade é o artigo "The Right to Privacy", escrito por Samuel Warren e Louis Brandeis e publicado na Harvard Law Review em 1890. Neste trabalho, os autores consolidaram a jurisprudência existente sobre o tema e introduziram o conceito de "right to be let alone" (direito de ser deixado em paz), abordando a tradicional dicotomia entre as esferas pública e privada (Tavares, 2022). Além disso, o artigo levantou uma preocupação crescente com a interação entre o avanço tecnológico e a proteção da privacidade, uma questão que se tornaria cada vez mais relevante com o passar dos anos. Esse estudo é amplamente reconhecido como um dos pilares jurídicos mais significativos para a evolução do direito à intimidade e à vida privada, impactando tanto o *common law* quanto o *civil law* (Robl Filho, 2013).

Os avanços tecnológicos geraram uma crescente preocupação com o gerenciamento e processamento de dados, o que levou, em 1960, à rejeição por parte do Congresso Americano de um projeto de lei que visava criar um banco de dados centralizado conhecido como National Data Center. O principal argumento contra a proposta foi o risco significativo que representaria para a privacidade dos indivíduos (Tavares, 2022).

Em 1970, a Alemanha deu um passo importante ao promulgar sua Lei de Proteção de Dados, que foi pioneira na formalização da proteção de dados como um direito fundamental. Essa legislação surgiu após intensos debates na segunda metade da década de 1960, que foram cruciais para o desenvolvimento da proteção de dados, agora presente de forma robusta em mais de 140 países (Doneda, 2021).

Na sequência, outras nações seguiram o exemplo da Alemanha, como a Suécia com sua Lei de Controle de Bancos de Dados em 1973, e a França e Dinamarca, que também introduziram suas leis de proteção de dados em 1978 (Zanon, 2013). Paralelamente, a União Europeia começou a estabelecer as bases para a proteção de dados como um direito fundamental, com a adoção da Diretiva 95/46/CE, que regulamentava o tratamento e a livre circulação de dados na Europa, e que foi substituída pelo Regulamento Geral de Proteção de Dados (RGPD) em 2016 (Doneda, 2021).

Este desenvolvimento legislativo reflete a influência significativa dos marcos regulatórios europeus, embora o conceito de proteção de dados tenha origens e influências

também nos Estados Unidos. Assim, a proteção de dados é resultado de uma interação dinâmica entre diferentes sistemas jurídicos, principalmente na Europa e nos Estados Unidos, e está fortemente ligada ao avanço econômico e tecnológico que demandou a criação de mecanismos regulatórios para salvaguardar as liberdades individuais e o direito à privacidade (Doneda, 2021).

O Regulamento Geral de Proteção de Dados (RGPD) entrou em vigor em 25 de maio de 2018, com a finalidade de fortalecer e uniformizar a proteção de dados para todos os cidadãos da União Europeia. Substituindo a Diretiva 95/46/CE, de 1995, o RGPD tem como principal objetivo harmonizar as leis de privacidade de dados em toda a Europa, proporcionando maior segurança aos residentes da região. Desde sua publicação, o regulamento é diretamente aplicável sem necessidade de implementação adicional por parte dos governos nacionais, sendo portanto, obrigatório e vinculativo (Magrani, 2019). Como uma norma do direito comunitário, o RGPD é válido nos 28 países da União Europeia, bem como na Islândia, Liechtenstein e Noruega (Fachin, 2022).

O Regulamento Geral de Proteção de Dados (RGPD) é frequentemente citado como um dos principais impulsionadores da disseminação de normas de proteção de dados ao redor do mundo. A legislação europeia adota uma abordagem rigorosa para a proteção de dados pessoais, considerando o direito à privacidade como um direito fundamental, conforme estabelecido nos artigos 7º[1] e 8º[2] da Carta dos Direitos Fundamentais da União Europeia. Isso demonstra que há uma sólida base legal que visa garantir aos usuários de redes e aos sujeitos da RGPD um controle mais efetivo e a autodeterminação sobre seus dados pessoais (Bradford, 2020).

No cenário da América do Sul, Chile foi pioneiro ao abordar a proteção de dados pessoais com a Lei 19.628, sancionada em 1999, que estabelece a proteção de dados pessoais. Em seguida, a Argentina implementou sua legislação sobre o tema em 2000, por meio da Lei de Proteção de Dados Pessoais 25.326 (PDPL, na sigla em inglês), complementada pelo Decreto Regulamentar 1558/2001 e outras normas da Direção Nacional de Proteção de Dados Pessoais (Andréa; Arquite; Camargo, 2020).

---

[1] Artigo 7.o - Respeito pela vida privada e familiar - Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. (Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 27 nov 2022).

[2] Artigo 8.o - Proteção de dados pessoais - 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. (Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 27 nov 2022).

Os antecedentes no direito internacional revelam uma trajetória contínua de evolução na proteção dos dados pessoais, refletindo a crescente importância da privacidade e da segurança da informação no cenário global. A partir dos primeiros esforços normativos, como a Convenção 108 do Conselho da Europa, até as modernas legislações como o Regulamento Geral de Proteção de Dados da União Europeia, o direito internacional tem demonstrado um compromisso crescente com a proteção dos dados pessoais como um direito fundamental.

Essas iniciativas não apenas estabeleceram padrões globais, mas também influenciaram a adoção de regulamentações semelhantes em diversas jurisdições, promovendo uma abordagem mais coesa e abrangente para enfrentar os desafios emergentes na era digital. A evolução dos antecedentes no direito internacional ressalta a necessidade contínua de adaptação e fortalecimento das normas para garantir a proteção eficaz dos dados pessoais em um mundo cada vez mais interconectado.

Desta forma, influenciado pela produção legislativa mundial, em especial a RGPD da União Europeia, o Brasil em 2018, promulgou a Lei Geral de Proteção de Dados, uma lei que versa exclusivamente sobre essa temática, embora, a proteção de dados já fosse mencionada mesmo que transversalmente em outros diplomas legislativos. Sendo assim, a proposta do próximo tópico deste artigo é a análise da evolução legislativa brasileira para a compreensão de como esse direito tão importante na era digital foi e está sendo construído domesticamente.

3.2 Antecedentes no direito nacional

A estruturação da proteção de dados pessoais no Brasil como um conjunto normativo unificado é um fenômeno relativamente recente. Historicamente, essa proteção foi construída de maneira fragmentada, através de diversas disposições legais que se integravam e eram interpretadas à luz da cláusula geral dos direitos da personalidade. Antes do surgimento de uma abordagem específica e autônoma para a proteção de dados, essa matéria era, em grande parte, efetivada por meio de mecanismos como a defesa do consumidor, que forneciam as bases para garantir a segurança e a privacidade das informações pessoais (Doneda, 2021).

É importante destacar que a Constituição brasileira abordou inicialmente a questão da informação por meio das garantias relacionadas à liberdade de expressão e ao direito à informação. Ademais, a Constituição protege a vida privada e a intimidade, declarando invioláveis essas esferas pessoais. Especificamente, a Constituição também prevê a inviolabilidade das comunicações telefônicas, telegráficas e de dados, além de instituir o habeas

data, que assegura o direito de acesso e correção de dados pessoais, garantindo assim uma forma de proteção às informações individuais (Doneda, 2021).

Nesse sentido, a proteção de dados pessoais no Brasil passou por um processo de amadurecimento que começou com a Constituição Federal de 1988, que, ainda que de forma indireta, já abordava questões relacionadas à proteção de dados no contexto dos direitos da personalidade, liberdade de expressão (art. 5º, IX) e direito à informação (art. 5º, XIV). A Constituição também garantiu a inviolabilidade da vida privada e da intimidade (art. 5º, X), o direito ao habeas data (art. 5º, LXXII) e regulamentou a interceptação de comunicações (art. 5º, XII). Em 2022, a proteção de dados foi elevada a direito fundamental por meio da Emenda Constitucional nº 115, que incluiu o direito à proteção de dados pessoais, inclusive nos meios digitais (art. 5º, LXXIX).

Antes da promulgação da Lei Geral de Proteção de Dados (LGPD), a legislação brasileira já contemplava, de forma geral, a proteção de dados em normas específicas, como o Código de Defesa do Consumidor, que regulamenta os bancos de dados e cadastros de consumidores, estendendo essa proteção a todos os dados pessoais (Brasil, 1990). Em 2011, foi sancionada a Lei 12.414/2011, conhecida como Lei do Cadastro Positivo, que trouxe novas diretrizes para o tratamento de bancos de dados e ampliou a aplicação do Código de Defesa do Consumidor, exigindo consentimento prévio para o compartilhamento de dados com terceiros (Brasil, 2011).

A regulação das relações no ambiente digital no Brasil avançou ainda mais com a criação do Marco Civil da Internet (Lei nº 12.965/2014), que foi desenvolvido para proteger direitos fundamentais, como a privacidade e a intimidade nas comunicações digitais. Ao contrário de abordagens anteriores que focavam em legislações penais, o Marco Civil adotou uma perspectiva baseada em princípios, garantindo direitos aos cidadãos no uso da internet. Mesmo antes da LGPD, o Marco Civil já mencionava a necessidade de consentimento para o tratamento de dados, destacando a importância da participação do titular no controle de suas informações (Brasil, 2014).

A aprovação da LGPD em 2018 representou um marco na proteção de dados no Brasil, estabelecendo um sistema robusto para garantir o exercício da autodeterminação informacional e existencial dos indivíduos. A LGPD trouxe uma nova era de segurança jurídica no tratamento de dados, sendo fundamental para o desenvolvimento de uma cultura de proteção de informações pessoais. Essa legislação não se limita ao ambiente virtual; ela também abrange o tratamento de dados em meios físicos, demonstrando uma preocupação abrangente com a privacidade e a liberdade dos indivíduos (Brasil, 2018).

Além disso, ressalta-se que fortemente inspirada pela GDPR, a Lei nº 13.709/2018 foi sancionada em maio de 2018, com o propósito de regulamentar o tratamento de dados pessoais, abrangendo tanto os meios digitais quanto físicos, por pessoas físicas ou jurídicas, de direito público ou privado. O principal objetivo dessa legislação é assegurar a proteção dos direitos fundamentais relacionados à liberdade, à privacidade, e ao pleno desenvolvimento da personalidade dos indivíduos (Oliveira; Lanzillo, 2021).

O direito à proteção dos dados pessoais deve ser integrado como uma nova categoria dentro dos direitos da personalidade, permitindo uma maior flexibilidade na proteção dos direitos humanos. Sem essa inclusão, há o risco de que ele permaneça restrito ao conceito tradicional de privacidade, o que não abordaria adequadamente as especificidades e os desafios associados ao tratamento de dados pessoais na era da Sociedade da Informação[3] (Bioni, 2020).

A trajetória legislativa brasileira demonstra o reconhecimento crescente da importância de proteger os direitos fundamentais, como a liberdade, a privacidade e o desenvolvimento da personalidade, em um contexto em que a circulação de informações se torna cada vez mais central. A inclusão recente de disposições sobre direito digital no anteprojeto de reforma do Código Civil corrobora essa tendência de atualização e aprimoramento, garantindo que o arcabouço legal brasileiro esteja apto a enfrentar os desafios impostos pela era digital.

3.3 A emenda constitucional nº 115/2022 e a LGPD em sua conformação atual

Em fevereiro de 2022, foi aprovada por unanimidade a Emenda Constitucional (EC) nº 115/2022, que incorporou o direito à proteção de dados pessoais ao rol de direitos e garantias fundamentais da Constituição Federal (art. 5º da CF). Além disso, a emenda estabeleceu a competência exclusiva da União para legislar sobre a proteção e o tratamento de dados pessoais (Scheuermann, 2023).

No entanto, antes da promulgação desta emenda, o Supremo Tribunal Federal (STF) já havia intensificado o debate sobre o tema por meio das Ações Diretas de Inconstitucionalidade (ADI) nº 6.387, 6.389 e 6.393. Segundo Mendes, Rodrigues Junior e Fonseca (2021, p. 79), o STF reconheceu o direito à proteção de dados pessoais como um direito fundamental autônomo, mesmo antes de sua formalização constitucional (Scheuermann, 2023).

[3] De acordo com Manuel Castells (2022, p. 560), a sociedade atual, denominada sociedade da informação, caracteriza-se por uma nova ordem social, que ele define como uma "sociedade em rede". Esta sociedade é composta por uma sucessão automática e aleatória de eventos, resultante da lógica incontrolável dos mercados, da tecnologia, da organização geográfica e de fatores biológicos.

A emenda constitucional mencionada teve sua origem na Proposta de Emenda à Constituição (PEC) 17/2019, cuja justificativa se baseou em quatro aspectos fundamentais. Primeiro, reconheceu-se que o avanço tecnológico traz benefícios, mas também pode acarretar danos aos cidadãos se não for regulamentado por princípios éticos e morais. Segundo, foi destacada a necessidade de distinguir o direito à proteção de dados do direito à privacidade, valorizando-o de forma autônoma. Terceiro, observou-se que muitos países já haviam implementado legislações abrangentes e discutido extensivamente a proteção de dados. Por fim, a PEC visou prevenir a fragmentação dos conceitos e princípios fundamentais relacionados ao tema (Brasil, 2019).

Em que pese a origem do direito a proteção de dados remonte ao direito à privacidade, há que se entender que se trata de um direito autônomo, decorrente dos avanços tecnológicos. Conforme Sarlet (2021), a interconexão entre esses dois direitos não implica uma sobreposição total de suas esferas de proteção. Em vez disso, os conceitos envolvidos refletem distinções essenciais que impedem a simples inferência de que se tratam de direitos fundamentais completamente interligados.

Além disso, o direito fundamental à proteção de dados abrange um escopo mais amplo do que pode inicialmente parecer. Esse direito se estende não apenas à proteção da privacidade individual, mas também a qualquer tipo de dado pessoal. A definição de "informação" dentro desse contexto é vasta e inclui todos os tipos de dados pessoais, abrangendo desde aspectos da vida íntima e privada até dados relacionados a interações sociais e outras esferas da vida do indivíduo (Mendes, 2018).

Portanto, a abrangência do direito à proteção de dados reflete a complexidade e a multiplicidade das informações pessoais que podem ser coletadas e processadas. Isso significa que, independentemente da natureza do dado, seja ele referente à vida pessoal ou social do indivíduo, ele está sujeito à proteção e à regulamentação prevista por esse direito fundamental. A amplitude do conceito de "informação" é crucial para garantir que todas as formas de dados pessoais recebam a devida consideração e proteção, assegurando que a privacidade do indivíduo seja respeitada em todas as suas dimensões (Mendes, 2018).

A proteção dos dados pessoais é considerada um direito fundamental devido ao seu impacto significativo na identidade e personalidade de um indivíduo. No cenário atual, em que muitas interações e relacionamentos ocorrem no ambiente digital, a forma como os dados pessoais são utilizados e analisados reflete aspectos essenciais da vida pessoal. Portanto, a proteção desses dados se torna crucial, uma vez que a construção do perfil de uma pessoa a

partir das suas informações representa um elemento vital no contexto contemporâneo (Assad; Leite, 2018).

A proteção de dados vai além de ser apenas um direito fundamental; ela é um reflexo crucial da condição humana na era moderna. Destacar sua importância constantemente não é meramente retórico, pois qualquer alteração nas regras que regem a proteção de dados influencia diretamente o nível de democracia que podemos vivenciar (Rodotà, 2008).

A crescente comercialização e manipulação de dados pessoais não apenas desafiam a privacidade, mas também afetam diretamente os direitos fundamentais dos usuários. Portanto, a inclusão da proteção de dados na constituição é uma resposta adequada às demandas da era digital, assegurando a preservação da dignidade e dos direitos dos indivíduos em um ambiente cada vez mais complexo e interconectado.

Como direito fundamental, a proteção de dados pessoais impacta todas as esferas das relações sociais e jurídicas, impondo a necessidade de adequação para assegurar esse direito. Quando se trata de direitos fundamentais, há uma prevalência formal, o que confere a esses direitos uma importância especial dentro do ordenamento jurídico. Assim, a inclusão da proteção de dados pessoais nesse nível hierárquico na Constituição reforça sua relevância e prioridade no contexto das normas constitucionais (Scheuermann, 2023).

Ante a relevância que a proteção de dados se apresenta na Sociedade da Informação, seus impactos atingem todas as relações sociais e econômicas ultrapassando a dicotomia estabelecida entre público e privado. A evolução tecnológica alterou o mundo e a forma de se viver, relativizou aspectos temporais e espaciais. Sendo assim, é possível verificar seus impactos no contexto educacional, o que será analisado na seção a seguir.

4 LIMITES E POSSIBILIDADES DA LGPD NO TRATAMENTO DE DADOS SENSÍVEIS DISCENTES NO ÂMBITO DAS IES PRIVADAS NO BRASIL E A TUTELA DOS DIREITOS DA PERSONALIDADE

A Lei Geral de Proteção de Dados (LGPD) não dedica um capítulo específico para a proteção de dados no contexto educacional, o que significa que suas diretrizes são geralmente amplas e podem não considerar as particularidades de cada setor. Apesar disso, a aplicação da LGPD ao ambiente educacional é clara, pois seu artigo 1º define que a lei abrange o tratamento de dados pessoais em qualquer contexto, incluindo plataformas digitais, e se aplica tanto a entidades públicas quanto privadas (Brasil, 2018).

Diante das práticas de coleta, produção e tratamento de dados no âmbito educacional, é fundamental considerar o que dispõe o Capítulo II da LGPD sobre o tratamento de dados pessoais. Em particular, o artigo 7º define as condições para que o tratamento de dados pessoais seja considerado legal. Entre essas condições estão a obtenção de consentimento explícito do titular (inciso I) e a necessidade de tratamento para a execução de um contrato ou para procedimentos pré-contratuais solicitados pelo titular (inciso V). Essas disposições são pertinentes ao contexto das relações entre discentes e instituições de ensino superior, uma vez que elas abrangem as situações em que o tratamento de dados é autorizado pela lei (Brasil, 2018).

No primeiro tipo de autorização para o tratamento de dados, o titular expressa seu consentimento para a realização de determinadas atividades. Esse cenário levanta várias questões, especialmente no que diz respeito à validade do consentimento em contratos de adesão (Tepedino; Teffé, 2020). Nas relações entre discentes e instituições de ensino superior, assim como entre docentes e essas instituições, os contratos são predominantemente de adesão, não permitindo negociação ou modificações. O titular dos dados simplesmente aceita os termos estabelecidos, sem a possibilidade de contestar ou alterar as condições previstas nesses contratos.

Ao analisar o conceito de consentimento conforme previsto na lei, especialmente no que diz respeito à exigência de que a manifestação seja livre, percebe-se que o legislador permitiu ao titular dos dados a opção de conceder ou negar seu consentimento para o tratamento de suas informações (Tepedino; Teffé, 2020). No contexto das relações discutidas, porém, fica claro que essa liberdade é praticamente inexistente, já que a recusa em fornecer consentimento resultaria na impossibilidade de firmar o contrato.

Além disso, no que tange à exigência de que o consentimento seja informado, é crucial que o titular dos dados tenha acesso a todas as informações necessárias e suficientes para compreender plenamente as condições e métodos pelos quais seus dados serão tratados (Viola; Teffé, 2021).

Devido à intricada natureza das relações no ambiente educacional, as exigências legais relacionadas à qualidade do consentimento frequentemente não são totalmente atendidas. Assim, os titulares podem acabar autorizando o tratamento de dados que ainda não foram gerados e sobre os quais talvez nunca sejam informados. Isso levanta um dilema: como alguém pode consentir com o tratamento de dados que ainda não existem? Se essa prática for considerada válida, caberia à instituição de ensino superior a obrigação de informar o titular sobre a geração, armazenamento, finalidade, utilidade e eventual eliminação desses dados.

Nesse cenário, o processamento de dados, incluindo aqueles provenientes do ambiente educacional, tornou-se uma constante na vida cotidiana. Observa-se que tanto a sociedade quanto a economia estão cada vez mais direcionadas e operam com base nesses indicadores que identificam os indivíduos. Esses perfis digitais configuram uma nova modalidade de identidade, o que torna fundamental que contenham informações exatas para refletir a identidade do titular de maneira fidedigna. Esse aspecto sustenta a classificação dos dados pessoais como parte integrante dos direitos da personalidade (Bioni, 2020).

A proteção de dados nas instituições de ensino superior privadas é uma questão crucial que envolve não apenas a conformidade com a legislação vigente, mas também a responsabilidade ética de preservar a privacidade e os direitos dos discentes. Diante do volume crescente de dados gerados e processados no ambiente acadêmico, essas instituições enfrentam o desafio de equilibrar a eficiência administrativa e educacional com a proteção dos direitos dos titulares de dados. Portanto, é imperativo que as instituições adotem práticas transparentes e rigorosas de gerenciamento de dados, assegurando que as informações pessoais sejam tratadas de forma segura e respeitosa, em consonância com os princípios estabelecidos pela LGPD.

5 CONSIDERAÇÕES FINAIS

A evolução da proteção de dados no Brasil, especialmente após a promulgação da Lei Geral de Proteção de Dados (LGPD), representa um marco significativo na tutela dos direitos fundamentais, incluindo os direitos da personalidade. A LGPD surge em um momento crucial, onde a sociedade digital está cada vez mais permeada pela coleta, processamento e utilização de dados pessoais. No contexto das instituições de ensino superior privadas, essa legislação assume uma importância ainda maior, dada a complexidade e a amplitude das informações pessoais envolvidas nas relações educacionais. Desde dados de matrícula até informações comportamentais e de desempenho, os dados dos discentes são coletados em grande escala, exigindo uma proteção adequada para garantir sua privacidade e integridade.

A vulnerabilidade dos discentes em relação ao tratamento de seus dados pessoais torna-se evidente quando se considera a assimetria de poder entre as instituições de ensino e seus alunos. Essa assimetria se manifesta na forma como os dados são coletados, muitas vezes sem que os discentes tenham pleno conhecimento ou controle sobre a extensão e o uso dessas informações.

A aplicação da LGPD, portanto, é fundamental para equilibrar essa relação, garantindo que os direitos dos discentes sejam respeitados e que o consentimento para o tratamento de

dados seja obtido de maneira livre, informada e específica. No entanto, a realidade demonstra que, em muitos casos, o consentimento é obtido de forma automática e sem a devida transparência, o que compromete a efetividade da proteção conferida pela lei.

Além disso, é necessário considerar os limites da LGPD no contexto educacional, em que a produção de dados não se restringe ao ambiente digital, mas permeia toda a vivência acadêmica dos discentes. A lei, em sua abrangência, muitas vezes não leva em conta as particularidades do setor educacional, tratando-o de forma genérica e desconsiderando as especificidades das relações entre discentes e instituições de ensino.

Nesse sentido, há uma lacuna na legislação que precisa ser abordada para que a proteção de dados seja realmente eficaz no contexto educacional, especialmente em instituições privadas, onde a lógica de mercado pode colocar em risco a privacidade e a segurança dos dados dos alunos.

A necessidade de tutelar os dados dos discentes à luz dos direitos da personalidade é indiscutível. O tratamento inadequado dessas informações pode acarretar sérios danos à dignidade e à autonomia dos alunos, afetando não apenas sua vida acadêmica, mas também sua vida pessoal e profissional.

A responsabilidade das instituições de ensino superior privadas, portanto, não se limita à conformidade com a LGPD, mas abrange uma postura ética e proativa na gestão dos dados dos discentes. Isso inclui a implementação de políticas de privacidade claras, a adoção de tecnologias seguras para o tratamento de dados e a garantia de que os alunos tenham pleno acesso e controle sobre suas informações pessoais. A vulnerabilidade dos discentes, exacerbada pela falta de transparência e pela complexidade das práticas de coleta e processamento de dados, exige uma abordagem que priorize a proteção de seus direitos em todas as etapas do processo educacional.

Por fim, a aplicação da LGPD no contexto das instituições de ensino superior privadas no Brasil revela tanto possibilidades quanto limitações. Embora a lei represente um avanço significativo na proteção dos direitos da personalidade, sua eficácia depende da capacidade das instituições de adaptar suas práticas às exigências legais e de promover uma cultura de respeito à privacidade e à autonomia dos discentes.

A evolução da proteção de dados no Brasil ainda está em curso, e o contexto educacional é um campo onde esses desafios se manifestam de forma particularmente acentuada, exigindo atenção contínua e ações concretas para garantir que os direitos dos discentes sejam plenamente respeitados.

REFERÊNCIAS

ANDRÉA, Gianfranco Faggin Mastro. ARQUITE, Higor Roberto Leite. CAMARGO, Juliana Moreira. Proteção de dados pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil. **Revista de Direito Constitucional e Internacional,** vol. 121/2020, p. 115 – 139. Set – Out., 2020. Disponível em: https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/revistas-especializadas/rdci-121-gianfranco-andrea-e-outros.pdf. Acesso em 20 ago. 2024.

ASSAD, Frederico Jorge Vaz De Figueiredo. LEITE, Flavia Piva Almeida. Aspectos do direito fundamental à proteção de dados pessoais. In: LIMBERGER, Têmis; CARMO, Valter Moura; ROVER, Aires Jose. **Direito, governança e novas tecnologias I.** Florianópolis: CONPEDI, 2018. Disponível em: http://site.conpedi.org.br/publicacoes/34q12098/9l053031/55dfpNn0G509WEvB.pdf. Acesso em 15 out. 22. (p. 187-205)

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª. ed. Rio de Janeiro: Forense, 2020.

BOTELHO, César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista de Direitos Sociais e Políticas Públicas**, vol. 8, n. 2, 2020. Disponível em: https://www.unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/705. Acesso em: 09 nov. 2023.

BRADFORD, Anu. **The Brussels Effect**: how the European Union rules the world. New York: Oxford University Press, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 ago. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Diário Oficial da União: Brasília, DF, 15 ago. 2018. Seção 1, p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 de ago. 2024.

BRASIL. **Projeto de Emenda à Constituição nº 17, de 2019.** Altera a Constituição Federal de 1988 para incluir o direito à proteção de dados pessoais no rol dos direitos fundamentais. Câmara dos Deputados: Brasília, DF, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2184967. Acesso em:

CAPPELLETTI, Monica. SIQUEIRA, Julio Pinheiro Faro Homem de. Transplantes jurídicos ou análise comparativa de direitos, qual a vocação do legislador brasileiro no processo de elaboração de suas leis? **Revista Bimestral de Direito Público**. Editora: Fórum. Disponível em: https://www.researchgate.net/profile/Monica-Cappelletti-2/publication/311086516_Transplantes_juridicos_ou_analise_comparativa_de_direitos_qual_a_vocacao_do_legislador_brasileiro_no_processo_de_elaboracao_de_suas_leis/links/583d6c9708ae2d2175548f04/Transplantes-juridicos-ou-analise-comparativa-de-direitos-qual-a-

vocacao-do-legislador-brasileiro-no-processo-de-elaboracao-de-suas-leis.pdf. Acesso em: 06 ago. 2024.

CASTELLS, Manuel. **A sociedade em rede.** 24. ed. rev. ampl. Rio de Janeiro: Paz e Terra, 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 3ª. ed., São Paulo: Thompsob Reuters Brasil, 2021.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: Mendes, Schertel Laura. Doneda, Danilo. SARLET, Ingo Wolfgag Sarlet. RODRIGUES JR, Otavio Luiz. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

FACHIN, Zulmar; SILVA, Deise Marcelino da. Avanços tecnológicos e a pessoa humana no século XXI: a (des)proteção do direito à privacidade no marco civil da internet. **Revista Juridica**, [S.l.], v. 5, n. 67, p. 230 - 254, out. 2021. ISSN 2316-753X. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/5629>. Acesso em: 13 ago. 2024. doi:http://dx.doi.org/10.26668/revistajur.2316-753X.v5i67.5629.

JESUS, Dilça Cabral de; CANEVARI, Carlabianca Cabral de Jesus; SILVA, Silvio Bitencourt da. Responsabilidade civil pela violação de dados em contratos educacionais. In. FIUZA, César Augusto; COSTA, Ilton Garcia da; BORGES, maria Creusa de Araújo. **Direito civil contemporâneo II. Florianópolis: CONPED**I, 2020. Disponível em: http://site.conpedi.org.br/publicacoes/nl6180k3/o5bw94o1/wvTmLxE0VZDw062a.pdf. Acesso em: 19 ago. 2024.

LIMBERGER, T. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí (SC), v. 14, n. 2, p. 27–53, 2009. DOI: 10.14210/nej.v14n2.p27-53. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 1 set. 2024.

LUGATI, L. N.; ALMEIDA, J. E. de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, *[S. l.]*, v. 12, n. 02, p. 01–33, 2020. DOI: 10.32361/2020120210597. Disponível em: https://beta.periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 1 set. 2024.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. 2 ed., Porto Alegre: Arquipélago Editorial, 2019.

MENDES, Laura Schertel Ferreira. Habeas Data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**. Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655/905. Acesso em: 24 ago. 2024.

OLIVEIRA, Fabiane Araújo de. LANZILLO, Anderson Souza da Silva. Estado, novas tecnologias e proteção de dados pessoais como direito fundamental. Revista de Direito, Governança e Novas Tecnologias. v. 7, n. 1, p. 92 – 107 | Jan/Jul. 2021. Disponível em: https://pdfs.semanticscholar.org/847d/ce847c598440d3bd992cd73290fdcb9cd43c.pdf. Acesso em 29 ago. 2024.

ROBL FILHO, Ilton Norberto. **Direito, intimidade e vida privada:** paradoxos jurídicos e sociais na sociedade pós-moralista e hipermoderna. Curitiba: Juruá, 2013.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang; Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SCHEUERMANN, G. F. Dados pessoais como um direito fundamental autônomo a partir da Emenda Constitucional nº 115/2022. **Revista da Defensoria Pública do Estado do Rio Grande do Sul**, Porto Alegre, v. 2, n. 33, p. 253–274, 2023. Disponível em: https://revistadpers.emnuvens.com.br/defensoria/article/view/600. Acesso em: 1 set. 2024.

SILVA, Bruno. FMU comunica incidente envolvendo base de dados dos alunos. **Security Report.** São Paulo, p. 1-1. 20 jul. 2022. Disponível em: https://securityleaders.com.br/fmu-comunica-incidente-envolvendo-base-de-dados-dos-alunos/. Acesso em: 29 ago. 2024.

SIQUEIRA, D. P.; LARA, F. C. P.; ALVES, N. G. Direitos de personalidade, proteção de dados pessoais e o poder público. **Revista Húmus**, [S. l.], v. 11, n. 31, 2021. Disponível em: http://periodicoseletronicos.ufma.br/index.php/revistahumus/article/view/16011. Acesso em: 28 ago. 2024.

SOUZA, J. F. de. Privacidade e dados pessoais: o debate ético sobre o uso de big data. **Revista Ilustração**, *[S. l.]*, v. 5, n. 6, p. 27–51, 2024. DOI: 10.46550/ilustracao.v5i6.340. Disponível em: https://journal.editorailustracao.com.br/index.php/ilustracao/article/view/340. Acesso em: 1 set. 2024.

TAVARES, Giovanna Milanez. **O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD.** Rio de Janeiro: Processo, 2022.

TEPEDINO, Gustavo. TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana. TEPEDINO, Gustavo. OLIVA, Milena Donato. Lei Geral de **Proteção de dados e suas repercussões no direito brasileiro**. 2.ed. São Paulo: Thomson Reuters Brasil, 2020.

VIOLA, Mario. TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: Mendes, Schertel Laura. Doneda, Danilo. SARLET, Ingo Wolfgag Sarlet. RODRIGUES JR, Otavio Luiz. **Tratado de proteção de dados pessoais. Rio de Janeiro: Forense**, 2021.

ZANON, João Carlos. **Direito à proteção dos dados pessoais.** São Paulo: Revista dos Tribunais, 2013.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.