LUCAS ADRIANO SANTOS PEREIRA

A ADESÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NOS ESCRITÓRIOS DE ADVOCACIA EMPRESARIAL

CURSO DE DIREITO – UniEVANGÉLICA

2023

LUCAS ADRIANO SANTOS PEREIRA

A ADESÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NOS ESCRITÓRIOS DE ADVOCACIA EMPRESARIAL

Projeto de monografia apresentado ao Núcleo de Trabalho Científico do curso de Direito da UniEvangélica, como exigência parcial para a obtenção de grau de bacharel em Direito sob orientação do professor M.e. Juraci Rocha Cipriano, na qual visa a compreensão e apresentação de forma clara e concisa sobre a Adesão da Lei Geral de Proteção de Dados (LGPD) Nos Escritórios de Advocacia Empresarial.

ANÁPOLIS – 2023

LUCAS ADRIANO SANTOS PEREIRA

A ADESÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NOS ESCRITÓRIOS DE ADVOCACIA EMPRESARIAL

Data: Anápolis, _____ de _____ 2023.

BANCA EXAMINADORA

_____

_____

RESUMO

Este trabalho tem como objetivo analisar de forma objetiva e clara a importância da Lei Geral de Proteção de Dados (LGPD, L.13709/18) e suas implicações nos escritórios de advocacia empresarial. Serão explorados os principais aspectos da LGPD desde seu contexto histórico com seus objetivos, fundamentos, órgãos reguladores, bem como às obrigações e responsabilidades que a LGPD impõe aos escritórios de advocacia no tratamento dos dados pessoais de seus clientes e colaboradores. Serão discutidas as medidas necessárias para garantir a conformidade com a lei, incluindo a implementação de procedimentos internos adequados, a designação de um encarregado de proteção de dados e a adoção de medidas de segurança para proteção dos dados Além disso, serão explorados os impactos da LGPD no relacionamento entre os escritórios de advocacia e seus clientes, destacando a importância da transparência na coleta e uso de dados pessoais, bem como os direitos dos titulares dos dados, como o direito de acesso, retificação e exclusão de informações.

Palavras-chave: LGPD; controlador; operador; anonimização; banco de dados.

SUMÁRIO

INTRODUÇÃO

O foco central deste trabalho acadêmico é realizar uma análise minuciosa sobre a adesão da Lei Geral de Proteção de dados nos escritórios de advocacia empresarial. Com o intuito de atingir esse propósito, foram conduzidas extensas pesquisas que englobaram revisões bibliográficas, análise de jurisprudências e exame das normas que regem o sistema jurídico nacional. A estrutura do trabalho foi organizada de forma didática, resultando em sua divisão em três partes distintas.

No início desta pesquisa, foi conduzida uma detalhada análise sobre a evolução histórica do tratamento de dados ao redor do mundo desde o início das primeiras leis nas quais viriam abordar o tema até os dias atuais em paralelo com a sua forma de utilização dentre do meio jurídico e os direitos individuais resguardados em meio a era tecnológica.

Ao passo que se avança ao segundo capitulo, nota-se a abordagem de como se estrutura os dados pessoais dentro do meio jurídico bem como os conflitos entre a real necessidade do uso de dados e os direitos individuais. Esta monografia proporciona uma análise minuciosa e abrangente das diferentes disposições presentes na Constituição Federal, Código Civil e Leis ao longo do curso histórico. O objetivo é realizar uma análise sistêmica e comparativa desses documentos legais, destacando as mudanças e evoluções ao longo do tempo.

No último capítulo, aborda-se analises profundas acerca do posicionamento jurídico bem como o tratamento legal dos dados supracitados envolvendo medidas cabíveis, consequências, Jurisprudências e posicionamentos de

Tribunais Singulares e Superiores. Ansiando fornecer uma visão abrangente e fundamentada sobre o uso de dados na atualidade.

Diante desse cenário, o objetivo central deste trabalho consiste em fornecer uma análise sucinta acerca da Lei Geral de Proteção de Dados (L.13709) bem como sua ementa Lei Nº 13.853 abordada ao longo dos capítulos, buscando promover uma compreensão aprofundada sobre a real necessidade contrapondo a todo momento o tratamento de dados sensíveis dentre o meio jurídico a ética e moral. Para atingir esse propósito, embasa-se em uma ampla variedade de referências provenientes das principais obras literárias jurídicas, atualizadas e de relevância, estabelecendo assim uma base sólida de conhecimento acerca do tema abordado.

CAPÍTULO I – LEI GERAL DE PROTEÇÃO DE DADOS

O presente capítulo trata detalhadamente sobre a aplicação da Lei Geral de Proteção de Dados (LGPD), ela que é uma legislação relativamente nova e moderna na qual transpõe o direito legal do indivíduo bem como pessoa física ou jurídica no Brasil.

No contexto é apresentado a origem histórica, a definição, uma série de conceitos, assim como o direito constitucional ao que projeta não só um axioma para a sua utilização, como serve de instrumentalização para sua aplicabilidade, bem como a impotancia de se abordar tal tema frente ao uso desenfreado de dados pessoais e dados sensíveis da população sem se importar com as problemáticas adversas devido a exposição dos mesmos.

1.1 Histórico

Antes da implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil, o panorama relacionado ao tratamento de dados pessoais e dados sensíveis era caracterizado por uma regulamentação fragmentada e lacunas significativas na proteção dos direitos dos indivíduos devido a falta de legislações.

Antes da LGPD, o Brasil não tinha uma lei específica de proteção de dados pessoais. As questões relacionadas à privacidade e à proteção de dados eram tratadas por diferentes legislações, como o Código de Defesa do Consumidor, o Marco Civil da Internet e algumas regulamentações setoriais específicas. No entanto, essas leis não ofereciam um conjunto abrangente de regras e princípios para o tratamento de dados pessoais conforme exposto por ÁVILA em sua obra “*A*

tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência":

> Apesar de todas as contradições e falta de reparos legislativos, enquanto os dispositivos acima permanecerem vigentes, algumas orientações interpretativas podem ser assentadas, sobretudo na concretização jurisprudencial dos dispositivos legais em jogo. São diretivas que podem auxiliar tanto o legislador quanto o julgador, que são órgãos do Estado encarregados de desenvolver – mas, antes disso, de defender – os preceitos constitucionais protetivos do cidadão. (ÁVILA, 2017, p. 196).

Como resultado, as empresas e organizações tinham uma ampla margem de manobra na coleta, uso e compartilhamento de dados pessoais, muitas vezes sem o consentimento adequado dos indivíduos ou sem fornecer informações claras sobre como os dados seriam utilizados. Além disso, a fiscalização e as sanções para violações de privacidade e segurança de dados eram limitadas.

> O acesso a dados sensíveis, como informações de saúde, orientação sexual, religião, opiniões políticas, entre outros, também não era protegido de forma adequada. Não havia restrições claras sobre como esses tipos de dados poderiam ser coletados, armazenados ou compartilhados, o que aumentava os riscos de discriminação e abuso. (GONÇALVES, 2018, p. 4).

Outro aspecto importante era a falta de uma autoridade nacional de proteção de dados. Antes da LGPD, não havia uma entidade específica encarregada de supervisionar a aplicação das leis de proteção de dados e de garantir a conformidade por parte das organizações. Isso dificultava a fiscalização e a imposição de medidas corretivas em casos de violação de privacidade e segurança de dados.

Em resumo, antes da LGPD, o panorama relacionado ao tratamento de dados pessoais e dados sensíveis no Brasil era caracterizado pela falta de uma legislação abrangente, pela falta de clareza nas regras e princípios de proteção de dados, pela falta de fiscalização efetiva e pela falta de proteção adequada dos direitos dos indivíduos. A implementação da LGPD foi um marco importante para a proteção da privacidade e dos direitos dos titulares de dados no país.

> No contexto da Lei de Acesso à Informação – em que a publicidade

> é a regra e o sigilo a exceção –, do Marco Civil da Internet e de decretos como o que trata da interoperabilidade de bases de dados, um dos desafios da Administração Pública brasileira é lidar com as bases de dados que contêm dados sensíveis. (GONÇALVES, 2018, p. 1).

Os tratamento de dados pessoais sempre foi uma questão sensível e relevante para a sociedade, em especial com o avanço da tecnologia e a crescente utilização de dados no mundo digital. Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) é uma legislação recente que busca proteger a privacidade e os direitos dos titulares de dados no Brasil.

O Marco Civil da Internet em 2014, trouxe algumas disposições sobre privacidade e proteção de dados. Além disso, o país também estava ansioso por casos de vazamento de dados em empresas privadas, como o caso da Cambridge Analytica em 2018, que revelou a importância de se ter uma legislação robusta sobre o assunto. Em 2018, foi aprovada a Lei nº 13.709/2018, que instituiu a LGPD. A mesma foi sancionada pelo então presidente Michel Temer em agosto de 2018 e estabeleceu um prazo de 18 meses para a sua entrada em vigor, o que ocorreu em setembro de 2020.

> Deve ser analisada é o Marco Civil da Internet, considerado uma resposta aos crescentes problemas envolvendo violações de dados e comunicações que afetam a vida privada e intimidade dos cidadãos. Na elaboração do marco, o legislador infraconstitucional buscou soluções de plena eficácia para disciplinar o uso das novas tecnologias de comunicação digitais, calcado nos princípios de universalidade, neutralidade e descentralização da rede mundial de computadores. (ÁVILA, 2017, p. 184).

A LGPD é inspirada em leis de proteção de dados de outros países, em especial o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia. Dessa forma, é possível encontrar semelhanças entre a LGPD e outras leis de proteção de dados de países de primeiro mundo, especialmente aqueles da União Europeia.

> O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. A proteção das pessoas singulares

> relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.o, n.o 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.o, n.o 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. (UNIÃO EUROPEIA, 2016).

Na União Europeia, o GDPR é a principal legislação sobre proteção de dados pessoais e se tornou a percussora da Lei em vigor no Brasil. O GDPR estabelece princípios e regras para o tratamento de dados pessoais, semelhantes aos previstos na LGPD. O GDPR também define a figura do Encarregado de Proteção de Dados (DPO) e exige que as empresas designem um DPO para garantir a conformidade com a legislação.

Nos Estados Unidos, a legislação sobre proteção de dados é fragmentada e depende do estado em que a empresa está localizada. No entanto, em 2018, a Califórnia aprovou a Lei de Privacidade do Consumidor da Califórnia (CCPA, na sigla em inglês), que estabelece regras semelhantes às da LGPD e do GDPR.

> Deveres Gerais das Empresas que Coletam Informações Pessoais (a) Uma empresa que controla a coleta de informações pessoais de um consumidor deve, no ponto de coleta ou antes dele, informar os consumidores do seguinte: (1) As categorias de informações pessoais a serem coletadas e as finalidades para as quais as categorias de informações pessoais são coletadas ou usadas e se essas informações são vendidas ou compartilhadas. Uma empresa não deve coletar categorias adicionais de informações pessoais ou usar informações pessoais coletadas para fins adicionais que sejam incompatíveis com a finalidade divulgada para a qual as informações pessoais foram coletadas sem fornecer ao consumidor um aviso consistente com esta seção. (ESTADOS UNIDOS DA AMERICA, 2018).

A CCPA concede aos cidadãos da Califórnia direitos semelhantes aos previstos na LGPD, como o direito de acesso, correção e exclusão de seus dados pessoais. A lei também estabelece penalidades para empresas que não cumprem suas obrigações de proteção de dados, podendo chegar a US$ 7.500 por violação.

> (a) Qualquer empresa, prestador de serviços, contratante ou outra pessoa que viole este título estará sujeito a uma liminar e será responsável por uma penalidade civil de não mais de dois mil e quinhentos dólares (US$ 2.500) por cada violação ou sete mil e quinhentos dólares (US$ 7.500) por cada violação intencional e cada

> violação envolvendo informações pessoais de consumidores menores; tal como ajustado nos termos do n.o 5 da subdivisão (a) da Seção 1798.185, que será avaliada e recuperada em uma ação civil movida em nome do povo do Estado da Califórnia pelo Procurador-Geral. O tribunal pode considerar a cooperação de boa-fé da empresa, do prestador de serviços, do contratante ou de outra pessoa na determinação do montante da penalidade civil. (ESTADOS UNIDOS DA AMERICA, 2018).

Em resumo, as leis de proteção de dados de países de primeiro mundo, como a LGPD, o GDPR e a CCPA, estabelecem princípios semelhantes para o tratamento de dados pessoais e exigem que as empresas sejam transparentes em relação aos dados que coletam e como os utilizam. Além disso, essas leis estabelecem penalidades para as empresas que não cumprem suas obrigações de proteção de dados, com o objetivo de garantir a privacidade dos titulares dos dados.

> (1) Especifica que as informações pessoais são vendidas ou divulgadas pela empresa apenas para finalidades limitadas e especificadas. (2) Obriga o terceiro, prestador de serviços ou contratante a cumprir as obrigações aplicáveis ao abrigo do presente título e obriga essas pessoas a fornecer o mesmo nível de proteção da privacidade exigido pelo presente título. (3) Concede à empresa direitos para tomar medidas razoáveis e apropriadas para ajudar a garantir que o terceiro, provedor de serviços ou contratante use as informações pessoais transferidas de maneira consistente com as obrigações comerciais sob este título. (4) Exige que o terceiro, prestador de serviços ou contratante notifique a empresa se determinar que não pode mais cumprir suas obrigações sob este título. (5) Concede à empresa o direito, mediante notificação, inclusive nos termos do parágrafo (4), para tomar medidas razoáveis e apropriadas para interromper e remediar o uso não autorizado de informações pessoais. (ESTADOS UNIDOS DA AMERICA, 2018).

O processo de elaboração da LGPD foi bastante participativo e envolveu diversas partes interessadas, como empresas, organizações da sociedade civil, academia e governo. A discussão sobre a necessidade de uma lei de proteção de dados no país começou em 2010, quando foi criado um grupo de trabalho para discutir o tema no âmbito do Ministério da Justiça.

Ao longo dos anos seguintes, foram realizadas diversas audiências públicas e consultas públicas para debater o assunto e colocar contribuições da sociedade. Em 2018, o projeto de lei da LGPD foi aprovado pelo Congresso Nacional após intensa discussão e negociação entre os diversos setores envolvidos.

> Outro tema recorrente nos projetos de lei apresentados é a definição de critérios e limites de aplicabilidade das penalidades administrativas previstas nos artigos 52 a 54. Esse é um tema que gera grande preocupação aos agentes de tratamento, considerando que a LGPD prevê diversas sanções administrativas a serem aplicadas. (PALHARES, p. 02, 2021)

A LGPD tem como principais objetivos proteger a privacidade e os direitos dos titulares de dados, regulando o tratamento de dados pessoais por empresas e órgãos públicos. A lei estabelece direitos para os titulares dos dados, como o direito de acesso aos dados, o direito de correção e exclusão dos dados e o direito de portabilidade dos dados. Além disso, a LGPD também estabelece obrigações para as empresas e órgãos públicos, como a necessidade de obter o consentimento dos titulares dos dados para o tratamento dos mesmos, a obrigação de implementar medidas de segurança padronizadas para proteger os dados e a necessidade de os notificar.

1.2 Legislação

A LGPD é composta por diversos artigos que estabelecem os princípios e diretrizes para o tratamento de dados pessoais, bem como os direitos dos titulares desses dados. Entre as obrigações das empresas e órgãos públicos previstas na lei estão a obtenção do consentimento do titular dos dados, a garantia da segurança dos dados coletados e a comunicação ao titular sobre o uso dessas informações.

Já trazendo a ambientação da Lei Geral de Proteção de Dados para a esfera jurídica da advocacia podemos notar que a implementação ainda não se tornou completa, como explicita o redador Marcelo Crespo em sua obra intitula Lei Geral de Proteção de Dados e o Poder Público:

> A existência de legislações setoriais também não era suficiente para uma tutela adequada, justamente pelo problema da fragmentação e do constante fluxo de dados entre diferentes esferas e setores (cita-se, por exemplo, o compartilhamento de dados entre entes privados e públicos). Em razão disso, a doutrina brasileira sempre defendeu a necessidade de se reconhecer a proteção de dados pessoais como um direito fundamental autônomo, indo além da tutela da intimidade e da privacidade. Ainda, a doutrina, inspirada na experiência internacional, buscou que a proteção desse direito fosse sistematizada

> em uma legislação contemporânea, uniforme e geral sobre o tema.(CRESPO, 2021, p. 4).

Para entender melhor a legislação da LGPD, é importante consultar obras especializadas no assunto. Um exemplo é o livro "LGPD - Lei Geral de Proteção de Dados Pessoais Comentada" de Rafael Zanatta, publicado pela Editora Revista dos Tribunais em 2019. Nessa obra, a autora comenta cada um dos artigos da LGPD e traz exemplos práticos de como essas disposições podem ser aplicadas na prática bem como os pontos positivos e negativos de como está sendo utilizada a legislação nos dias atuais.

Devemos ressaltar que para a Lei Geral de Proteção de Dados, há a Agência reguladora Autoridade Nacional de Proteção de Dados (ANPD), que em 25 de outubro de 2022 houve auteração em sua lei inicial, alteração essa que transforma a Agência reguladora em uma Autarquia de natureza especial e transforma cargos comissionados.

> Art. 1º Fica a Autoridade Nacional de Proteção de Dados (ANPD) transformada em autarquia de natureza especial, mantidas a estrutura organizacional e as competências e observados os demais dispositivos da Lei nº 13.709, de 14 de agosto de 2018. Art. 2º Fica criado 1 (um) Cargo Comissionado Executivo nível 18 (CCE-18) de Diretor-Presidente da ANPD. (BRASIL, 2022).

Outra referência importante sobre a legislação da LGPD é o livro "Proteção de Dados Pessoais - A Função e os Limites do Consentimento" de Danilo Doneda Bioni, publicado pela Editora Juspodivm em 2019. Nessa obra, o autor aborda o tema do consentimento do titular dos dados, que é um dos principais pilares da LGPD, e discute como essa questão pode ser aplicada na prática destacando quê:

> O livro aborda aquele que é um dos temas mais importantes e, ao mesmo tempo, um dos mais desafiadores do campo da proteção de dados pessoais: o consentimento. Essa ambivalência corresponde justamente à alma desta obra, que faz uma investigação dogmática, mas sem perder de vista aportes empíricos, a fim de identificar quais os limites e a função do consentimento na proteção dos dados pessoais.(BIONI, 2019, p. 42).

Nesse sentido, nota-se a importância e relevância do tratamendo de tais assuntos no âmbito jurídico bem como sua legislação quê, apesar de recente vem se

transformando e reformulando ao longos dos poucos anos de existência com finalidade de se aprimorar cada vez mais para se compôr dentro das premissas garantidas a todos os cidadãos no Art 5º da CONSTITUIÇÃO FEDERAL BRASILEIRA.

Além dessas obras, existem diversas outras fontes de referência sobre a legislação da LGPD, como artigos publicados em revistas especializadas e sites de conteúdo jurídico, seminários e cursos de capacitação. O importante é buscar informações atualizadas e de qualidade sobre a LGPD para garantir que as empresas e órgãos públicos estejam em conformidade com a legislação e respeitem os direitos dos titulares de dados pessoais bem como dados sensíveis.

Apesar de ser um tema relativamente recente nota-se a abundância de conteúdos bem como livros, artigos e obras renomadas nacionais e internacionais das quais versam sobre a necessidade cada vez maior de legislações ao redor do mundo abordarem o sígilo e proteção de dados pessoais e dados sensíveis, haja vista os avanços tecnológicos quanto a modernidade digital, tudo isso deve ser analisado e exposto de forma detalhada e contundente não só por doutrinadores e especialistas mas com todos os cidadãos, pois no final são os dados de boa parte da população que estão sendo disseminados sem devido consentimento dos mesmos.

1.3 Tratamento de dados pessoais e dados sensíveis

O tratamento de dados pessoais e dados sensíveis é uma questão de extrema relevância para a advocacia, já que os escritórios de advocacia e os advogados lidam diariamente com uma grande quantidade de informações confidenciais de seus clientes, conforme exposto por Bruno Miragem em seu livro A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor:

> O acesso e utilização dos dados pessoais compreende um dos principais ativos empresariais na sociedade contemporânea e, ao mesmo tempo expressão dos riscos à privacidade frente às novas tecnologias da informação,1 repercutindo por isso, amplamente, no mercado de consumo e, consequentemente, sobre o direito do consumidor.2 O desenvolvimento da tecnologia da informação e a capacidade de processamento de imenso volume de dados variados (Big data), permite o refinamento das informações de modo a permitir uma série de utilidades, como a segmentação dos consumidores para quem se dirige uma oferta, maior precisão na análise dos riscos de contratação (seleção de risco), formação de bancos de dados com

> maior exatidão e eficiência do uso das informações coletadas, de modo a tornar a capacidade de acesso a tratamento de dados um dos valores mais relevantes atualmente. (MIRAGEM, 2019, p. 1).

De acordo com a Lei Geral de Proteção de Dados (LGPD), dados pessoais são qualquer informação relacionada a uma pessoa física identificada ou identificável. Por sua vez, dados sensíveis são aqueles relacionados a origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, genética ou biometria de uma pessoa, conforme descrito por AFFONSO na Cartilha da Lei Geral de Proteção de Dados Pessoais – LGPD, 2021.

Na advocacia, é comum que os escritórios de advocacia coletem e processem uma grande quantidade de dados pessoais e sensíveis de seus clientes, incluindo informações sobre suas ações judiciais, processos administrativos, contratos, entre outros. É fundamental, portanto, que os advogados e escritórios de advocacia estejam em conformidade com as disposições da LGPD.

> Acompanhando o voto do Relator pela constitucionalidade do acesso a dados bancários pelo Fisco independentemente de autorização judicial, o Min. Luís Roberto Barroso acrescenta que, no seu entendimento, o sigilo de informações financeiras não se encontra no núcleo essencial do direito à intimidade, sendo, assim, passível de restrição razoável pelo legislador, principalmente com o objetivo de compatibilizá-lo com o dever fundamental de pagar tributos. (ÁVILA, 2017, p. 184).

Para garantir o tratamento adequado de dados pessoais e sensíveis, é necessário que os advogados e escritórios de advocacia adotem medidas de segurança da informação, como a criptografia de dados, o armazenamento seguro e a implementação de controles de acesso adequados. Além disso, é importante que os escritórios de advocacia implementem políticas claras e transparentes de privacidade e de proteção de dados, incluindo a obtenção do consentimento dos clientes para o tratamento de seus dados pessoais e sensíveis.

Cabe ressaltar que o vazamento de informações confidenciais de clientes pode resultar em sanções graves para os escritórios de advocacia e advogados, incluindo multas e responsabilização civil e criminal. Dessa forma, a conformidade

com a LGPD é fundamental para garantir a segurança e a privacidade das informações dos clientes, bem como para evitar possíveis sanções.

> Art. 7º São direitos do advogado: XIII - examinar, em qualquer órgão dos Poderes Judiciário e Legislativo, ou da Administração Pública em geral, autos de processos findos ou em andamento, mesmo sem procuração, quando não estiverem sujeitos a sigilo ou segredo de justiça, assegurada a obtenção de cópias, com possibilidade de tomar apontamentos; (BRASIL, 1994).

Em suma, é fundamental que os escritórios de advocacia e advogados tratem os dados pessoais e sensíveis de seus clientes com responsabilidade e em conformidade com as disposições da LGPD. Isso contribui para a proteção da privacidade e dos direitos dos titulares dos dados, além de evitar possíveis sanções e danos à reputação do escritório e/ou empresas; clientes envolvidos.

1.4 Direito a Proteção de Dados

A proteção de dados é um direito fundamental previsto na Constituição Federal brasileira e na Lei Geral de Proteção de Dados (LGPD), aplicável tanto a pessoas físicas quanto a pessoas jurídicas. Isso significa que tanto indivíduos quanto empresas têm o direito de terem seus dados pessoais tratados de forma segura e responsável, com o objetivo de garantir a proteção da privacidade e da intimidade.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (BRASIL, 1988).

A LGPD define dados pessoais como qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso inclui dados como nome, endereço, telefone, e-mail, documentos, entre outros. Já os dados sensíveis são aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, saúde ou vida sexual, entre outros. O tratamento desses dados só é permitido em casos específicos e com consentimento expresso do titular.

Tanto pessoas físicas quanto jurídicas podem ser titulares de dados pessoais e sensíveis e, portanto, têm direito à proteção desses dados. Por exemplo, uma empresa pode ter dados pessoais de seus clientes, fornecedores e funcionários, que devem ser tratados de forma segura e responsável, com o objetivo de garantir a privacidade e a proteção dessas informações.

> Art 5º. LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022) § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata. § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 1988).

Além disso, a LGPD prevê a figura do encarregado de proteção de dados (DPO), que é responsável por garantir o cumprimento da legislação de proteção de dados dentro das organizações. É possível que tanto pessoas físicas quanto jurídicas designem um DPO para lidar com questões relacionadas à proteção de dados.

Além do direito à proteção de dados, tanto pessoas físicas quanto pessoas jurídicas também têm obrigações em relação ao tratamento de dados pessoais. A LGPD estabelece que as empresas devem seguir princípios como a finalidade, a adequação, a necessidade, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018).

Entre as obrigações das empresas em relação ao tratamento de dados

pessoais, destacam-se a obtenção do consentimento do titular dos dados para o seu uso, a adoção de medidas de segurança para proteção das informações, a manutenção de registros de atividades de tratamento de dados, a elaboração de relatórios de impacto à proteção de dados pessoais e a comunicação às autoridades competentes e aos titulares dos dados em caso de incidentes de segurança.

No caso das pessoas físicas, a LGPD garante o direito de acesso aos seus dados pessoais tratados por empresas ou organizações, bem como o direito de correção, exclusão e portabilidade desses dados. O titular também tem o direito de revogar o consentimento para o tratamento de seus dados pessoais a qualquer momento. Vale lembrar que a LGPD prevê sanções administrativas e civis para empresas que descumprem as obrigações previstas na legislação, podendo gerar multas e outras penalidades.

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência. I - a portabilidade de dados quando solicitada pelo titular; (Incluído pela Lei nº 13.853, de 2019) Vigência. II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (BRASIL, 2018)

Em resumo, tanto pessoas físicas quanto jurídicas têm direitos e obrigações relacionados à proteção de dados pessoais, sendo fundamental o cumprimento da legislação de proteção de dados para garantir a privacidade e a segurança das informações.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador. (BRASIL, 2018).

Sendo assim, nota-se que a proteção de dados é um direito fundamental tanto para pessoas físicas quanto para pessoas jurídicas, e deve ser garantida por

meio de medidas de segurança da informação e de proteção de privacidade. A LGPD estabelece regras claras para o tratamento de dados pessoais e sensíveis, e é fundamental que tanto indivíduos quanto empresas estejam em conformidade com a legislação para garantir a proteção de seus dados.

Além do mais, a utilização de dados sensíveis dos clientes vem sofrendo grandes ataques cibernéticos ao redor do mundo, especialmente em países subdesenvolvidos, nos quais não detém de grandes poderes tecnológicos afim de garantir, assegurar e resguardar tais dados, sendo assim nota-se necessário e indispensável formas de garantir tais seguranças como exposto por Fernando Hallberg em seu Artigo ‘Gestão de arquivos em nuvem na era da LGPD com enfoque em um escritório de advocacia – Unisul’:

> A LGPD passa a cobrar que toda informação pessoal seja resguardada, e mais do isso, tenham formas de controle que permitam verificar se realmente estão resguardadas. Isso significa que toda a informação deverá ser auditada e passar por sistemas de controle, sendo inclusive que a falta de controle sobre a informação poderá acarretar multa para a empresa. Com a LGPD as empresas serão obrigadas a se organizar, e inclusive disponibilizar para os clientes uma forma de seus dados serem excluídos de sua base, caso o cliente assim deseje. (HALLBERG, 2021, p. 11).

A seguir, apresenta-se o panorama geral exposto na Cartilha de Proteção de dados sobre como funciona na prática a Lei Geral de Proteção de Dados no Brasil bem como os principais princípios que versam sobre o tema supracitado:

> Observa-se a boa-fé e os 10 princípios elencados na Lei. I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; (NUNES, 2021, p. 14).

Em síntese, a LGPD estabelece regras claras para o tratamento de dados pessoais, como princípos gerais que regem perante o objetivo de proteger a privacidade e a segurança dos titulares dos dados. As empresas devem seguir as regras previstas na legislação e garantir a proteção dos dados pessoais coletados e tratados, entretanto, nota-se uma severa carência de sua utilização por empresas e escritórios (principalmente empresas nos quais seus clientes muitas vezes usam de forma branda e sem conhecimento tais dados ou tem seus dados vazados por falta se segurança de qualidade em seus sistemas de gerenciamento de aquivos), bem como lacunas de utilização devido baixos níveis tecnológicos utilizados para resguardar tais dados.

Alguns dos principais e mais úteis meios de tecnologias utilizados em países membros da União Européia para assegurar a proteção de dados sensíveis, incluem a criptografia e Anonimização, técnicas que podem ser utilizadas para garantir a privacidade dos titulares dos dados. Ambas consistem em remover informações que possam identificar os titulares dos dados, tornando-os anônimos, bem como as ferramentas de gestão de consentimento das empresas que podem utilizar ferramentas de gestão de consentimento para obter e gerenciar o consentimento dos titulares dos dados para o tratamento de seus dados pessoais dessa forma trazendo a conformidade com a Lei.

> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. (BRASIL, 2018)

Essas ferramentas permitem que os titulares dos dados possam escolher quais dados desejam compartilhar e para que finalidade. Soluções de segurança da informação: as soluções de segurança da informação são fundamentais para garantir a proteção dos dados pessoais. Elas incluem softwares antivírus, firewalls, controles de acesso, monitoramento de rede, entre outras tecnologias. Programas de conscientização e treinamento: além das tecnologias, é fundamental que as empresas invistam em programas de conscientização e treinamento para garantir que todos os

colaboradores estejam cientes da importância da proteção de dados pessoais e saibam como agir em conformidade com a LGPD.

CAPÍTULO II – *USO DE DADOS POR ESCRITÓRIOS DE ADVOCACIA*

O presente capítulo trata detalhadamente as formas como são utilizados os dados dos clientes de escritórios de advocacia no Brasil, concomitantemente com a Lei Geral de Proteção de Dados (LGPD) Lei n. 13.709, de 14 de agosto de 2018 entrou em vigor em setembro de 2020.

No contexto é apresentado a Estruturação de dados pelos escritórios de advocacia, o conflito entre a necessidade do uso e os direitos pessoais bem como a liberdade do uso de dados dos clientes empresariais, o que projeta não só um axioma para a teoria, serve de instrumentalização para sua aplicabilidade.

O uso de dados por escritórios de advocacia é de extrema importância para o desenvolvimento e aprimoramento dos serviços jurídicos bem como já vem sendo relatado por autores com propriedade como Mateus de Oliveira Fornasier (*O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados*) e Rafael Zanatta (*Manual Prático de Adequação à Lei Geral de Proteção de Dados para Organizações da Sociedade Civil).*

Os dados fornecem informações valiosas que permitem aos advogados compreender melhor os problemas legais enfrentados pelos clientes, tomar decisões embasadas e oferecer soluções mais eficientes.

2.1 Estruturação de dados pelos escritórios de advocacia

A relação entre o tratamento de dados sensíveis e a advocacia é uma questão delicada e requer um cuidado especial por parte dos escritórios de advocacia

para garantir o cumprimento da LGPD (Lei nº 13.709/2018) e a proteção adequada dessas informações sensíveis.

Conforme estabelecido no Art. 38º da LGPD (Lei nº 13.709/2018), Dados sensíveis são informações que revelam características íntimas ou detalhes pessoais dos indivíduos, como origem racial ou étnica, opiniões políticas, religião ou crenças, filiação sindical, dados genéticos, dados biométricos, dados de saúde, dados de vida sexual ou orientação sexual, entre outros.

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. (BRASIL, 2018).

A estruturação de dados pessoais e dados sensíveis nos escritórios de advocacia envolve a adoção de medidas e práticas para coletar, armazenar, processar e proteger essas informações de acordo com as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD). Esse processo é essencial para garantir a privacidade e segurança dos dados, bem como cumprir as obrigações legais impostas pela legislação de proteção de dados, conforme previstos no Art. 49º e 50º da LGPD (Lei nº 13.709/2018):

> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018).

O primeiro passo na estruturação de dados pessoais e dados sensíveis quando utilizadas por escritórios de advocacia, é realizar um mapeamento detalhado

das informações que são coletadas e processadas assim como explicita Fornasier em sua obra *"O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados"*, isso inclui identificar quais dados são coletados, a finalidade da coleta, a base legal para o processamento, a duração do armazenamento e as categorias de destinatários com os quais os dados podem ser compartilhados.

De acordo com Fornasier, é importante identificar quais dados são considerados pessoais e sensíveis. Dados pessoais são aqueles que permitem identificar uma pessoa física, como nome, endereço, número de telefone, e-mail, entre outros. Já os dados sensíveis referem-se a informações mais delicadas, como origem racial ou étnica, opiniões políticas, religião, filiação sindical, saúde, vida sexual, entre outros, que exigem um tratamento ainda mais cuidadoso.

> É possível mobilizar seus conceitos e acrescê-los com os termos elaborados por outros autores para analisar o papel do titular de dados pessoais, confinado a uma estrutura social de mediação digital por meio da infraestrutura das big techs, em que a participação do cidadão é restrita ao papel de usuário/consumidor. (FORNASIER, 2021, p. 1016).

Outro ponto de extrema relevância é a obtenção de consentimento, na qual é uma etapa crucial na estruturação de dados pessoais assim como expõe Rafael Zanatta. Os escritórios de advocacia devem solicitar o consentimento explícito dos indivíduos para coletar, armazenar e processar seus dados pessoais. O consentimento deve ser livre, informado, específico e inequívoco, e as finalidades para as quais os dados serão utilizados devem ser claramente comunicadas.

> Nos primeiros anos de regime democrático e civil, nós tivemos no Brasil uma legislação muito avançada para proteção do consumidor: o Código de Defesa do Consumidor (Lei 8.078/1990). No artigo 43 existem regras para obtenção de consentimento para criação de bancos de dados. Nesta lei, dispõe-se que o consumidor "terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivoados sobre ele, bem como sobre suas respectivas fontes". Além disso, diz que a abertura de cadastros e dados pessoais "deverá ser comunicada por escrito ao consumidor, quando não comunicada por ele" (Art. 43, § 2°). Não há, no entanto, a estipulação clara de direitos à proteção de dados pessoais, como acesso, transparência, respeito à finalidade de uso e remoção. (ZANATTA, 2015, p. 452).

Além do consentimento, os escritórios de advocacia devem ter uma base legal para o processamento de dados pessoais e sensíveis assim como previsto no Art.7º da LGPD (Lei nº 13.709/2018), salvo resguardo quando tais dados são informações públicas.

Os escritórios de advocacia devem estar cientes das categorias de dados sensíveis e entender as bases legais para o tratamento dessas informações. É essencial obter o consentimento explícito dos titulares dos dados quando necessário e estabelecer uma finalidade legítima para o tratamento dessas informações.

> 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. (BRASIL, 2018).

Isso pode incluir o cumprimento de obrigações contratuais, cumprimento de obrigação legal, proteção de interesses vitais do titular, exercício regular de direitos em processos judiciais, entre outras bases previstas na LGPD. Os escritórios de advocacia devem adotar medidas de segurança adequadas para proteger os dados pessoais e sensíveis que possuem. Isso pode incluir a implementação de políticas de segurança da informação, controle de acesso aos dados, criptografia, anonimização, pseudonimização, backup regular dos dados e monitoramento de atividades suspeitas.

A LGPD (Lei nº 13.709/2018) em seu art. 17º, estabelece os direitos dos titulares dos dados pessoais, como o direito de acesso, retificação, exclusão, oposição, portabilidade e a revogação do consentimento. Os escritórios de advocacia devem estar preparados para atender a solicitações relacionadas a esses direitos e garantir que os procedimentos adequados estejam em vigor para facilitar o exercício desses direitos. Os escritórios de advocacia devem ter cautela ao compartilhar dados pessoais, uma vez que possa gerar diversas problemáticas advindas de vazamentos.

Em suma, a relação entre o tratamento de dados sensíveis e a advocacia requer uma abordagem cuidadosa e diligente por parte dos escritórios de advocacia.

A LGPD (Lei nº 13.709/2018), impõe obrigações claras e específicas para garantir a proteção adequada dessas informações sensíveis.

Medidas de segurança adequadas devem ser implementadas para proteger a confidencialidade, integridade e disponibilidade dos dados sensíveis. O compartilhamento dessas informações deve ser realizado com cautela, garantindo que exista uma base legal válida e que medidas de segurança adequadas estejam em vigor.

> A regulação em torno da proteção de dados reconhece o problema do extrativismo de dados, mas fornece a segurança jurídica da liberdade contratual sob a disponibilidade desses dados. No Brasil, a LGPD é um marco de criação dessa figura, o titular de dados pessoais, sujeito de direito capaz de fornecer seus dados pessoais comportamentais por meio de um processo de consentimento. A autoderminação informativa é um dos fundamentos dessa lei; mas tal qual ocorre com a autonomia privada sob o manto da igualdade jurídica, esse sujeito carece de condições materiais para exercício de plena liberdade sobre os dados pessoais, pois a escolha está somente na forma de consentimento em que os dados serão rendidos aos prestadores de serviços digitais. (FORNASIER, 2021, p. 1012).

Além disso, os escritórios de advocacia devem respeitar o sigilo profissional e garantir que suas equipes estejam cientes das obrigações éticas e legais de proteger a confidencialidade das informações sensíveis reveladas pelos clientes assim como exposto por Hallberg, em sua obra Gestão de arquivos em nuvem na era da LGPD com enfoque em um escritório de advocacia.

> A informação está distribuída de maneira desorganizada, sem uma diretriz definida, dificultando sua rastreabilidade e controle dos arquivos, bem como o backup, pois a maior parte das pessoas (80%) armazena arquivos diretamente no computador. (HALLBERG, 2021, p. 16).

Ao adotar uma abordagem diligente no tratamento de dados sensíveis, os escritórios de advocacia poderão cumprir as exigências da LGPD, proteger a privacidade dos indivíduos e manter a confiança de seus clientes, consolidando sua reputação como prestadores de serviços jurídicos seguros e responsáveis.

2.2 O conflito entre a necessidade do uso e os direitos pessoais

Este capítulo examina os conflitos inerentes entre a necessidade do uso de dados sensíveis e os direitos pessoais, destacando as questões éticas e legais envolvidas e as possíveis formas de equilibrar essas duas dimensões.

Explanação sobre o conceito de dados sensíveis e direitos pessoais embasadas na obra Gestão de arquivos em nuvem na era da LGPD com enfoque em um escritório de advocacia de Fernando Hallberg, incluindo exemplos de categorias comumente reconhecidas, como origem racial ou étnica, opiniões políticas, religião, saúde, orientação sexual, entre outros enquanto isso, os direitos pessoais consiste na apresentação dos principais direitos pessoais relacionados à privacidade e proteção de dados, tais como o direito à autodeterminação informativa.

> Nesse sentido, devem ser mapeados todos os processos internos que envolvam tratamento de dados pessoais, inclusive com a classificação entre dados pessoais e dados pessoais sensíveis, para que então sejam sugeridas as mudanças nos processos da empresa para que esteja em conformidade com a LGPD (HALLBERG, 2021, p. 16).

Ao analisar a necessidade do uso de tais dados, é necessário mencionar as justificativas legítimas, na qual explora as circunstâncias em que o uso de dados sensíveis é necessário e justificado, destacando exemplos nas áreas da saúde, pesquisa científica, segurança pública e no contexto jurídico, em que os escritórios de advocacia lidam com informações confidenciais para a defesa dos interesses dos clientes.

> Imprescindível a definição de processos para tratamento dos arquivos, bem como a eliminação de acesso a rede e ao computador por fontes não monitoradas como hd externo, pen drive e e-mail pessoal, inclusive podendo chegar ao ponto de monitorar as portas USB de todos os computadores, e só permitir acesso a rede de computadores autorizados. (HALLSBERG, 2021, p. 17).

Outra discussão legítima se faz sobre os benefícios sociais que podem resultar do tratamento adequado de dados sensíveis, conforme estabelecido na lei supracitada, como avanços científicos e médicos, prevenção de crimes, promoção da igualdade e justiça, entre outros, bem como os conflitos entre a necessidade do uso de dados sensíveis e os direitos pessoais.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. (BRASIL, 2018).

No âmbito ético e moral do campo jurídico, surge um conflito complexo entre a necessidade do uso de dados e os direitos pessoais dos indivíduos. Os escritórios de advocacia enfrentam o desafio de equilibrar essa necessidade com a proteção dos direitos de privacidade e confidencialidade dos clientes, uma vez que surge a necessidade advinda de novas tecnologias assim como é exposto por Fernando Zanatta:

> Nesse modelo, há uma responsabilidade compartilhada para a proteção de dados pessoais. Estados nacionais podem elaborar acordos e criar instrumentos regulatórios específicos, porém as empresas privadas e a sociedade civil também assumem papéis importantes para a proteção de dados pessoais, via códigos deontológicos ou tecnologias que podem, por default, proteger os dados pessoais (anonimizando os dados ou criando ferramentas técnicas do tipo do not track me42 ou disconnect43). Tal perspectiva também foi notada por Dennys Antonialli e Francisco Brito Cruz, reconhecendo as insuficiências e limites de uma abordagem regulatória pautada exclusivamente em instrumentos jurídicos. (ZANATTA, 2015, p. 465).

Por um lado, a necessidade do uso de dados é fundamentada na busca pela prestação de serviços jurídicos eficientes e estratégicos. O acesso a informações detalhadas sobre os clientes permite que os advogados entendam melhor seus problemas e necessidades específicas, proporcionando um atendimento mais personalizado e direcionado. No entanto, esse uso de dados deve ser realizado de forma responsável e respeitando os direitos pessoais dos indivíduos. Os direitos à privacidade, à confidencialidade e à proteção de dados são fundamentais e devem ser salvaguardados em todas as etapas do processo.

Esse conflito ético e moral requer uma reflexão cuidadosa por parte dos profissionais do direito. É essencial adotar práticas transparentes, obter consentimento informado dos clientes e implementar medidas de segurança adequadas para proteger os dados pessoais pois nota-se a falta de crendencialidade atualmente nos escritórios no brasil, conforme exposto por Hallsberg:

> Ou seja, se por si só as empresas adotassem condutas éticas no tratamento de informações pessoais, a LGPD não seria necessária. Porém essa não é a realidade das condutas praticadas, sendo necessário a adoção de uma lei que garanta a conformidade e o respeito a privacidade das informações pessoais. (HALLSBERG, 2021, p. 15).

Além disso, os advogados têm a responsabilidade de lidar com os dados dos clientes de maneira confidencial, evitando qualquer forma de uso indevido ou compartilhamento não autorizado. A confiança e a integridade são valores essenciais na relação entre advogados e clientes, e o respeito aos direitos pessoais contribui para fortalecer essa confiança.

Os riscos de discriminação e estigmatização deve ser realizado uma Análise dos riscos associados ao tratamento de dados sensíveis, incluindo o potencial de discriminação, preconceito e estigmatização de indivíduos com base nessas informações sensíveis assim como da invasão de privacidade e consentimento informado, exploração dos desafios em obter um consentimento livre e esclarecido para o tratamento de dados sensíveis.

> Nessa parte, destaco o posicionamento dos atores com relação à criação da Comissão Nacional de Proteção de Dados Pessoais no Brasil. Na terceira parte, faço uma breve análise da Lei 12.965/2014 e busco identificar os limites do Marco Civil da Internet para a devida proteção de dados pessoais. Por fim, retomo a ideia de um “sistema regulatório híbrido” e exploro possibilidades de construção dessa agenda, identificando os papéis e responsabilidades de diferentes atores. (ZANATTA, 2015, p. 448).

À discussão sobre os riscos de segurança associados ao tratamento de dados sensíveis, destacando a necessidade de medidas de proteção robustas para evitar vazamentos e acesso não autorizado a essas informações. Algumas abordagens para equilibrar a necessidade do uso de dados sensíveis e os direitos pessoais Minimização e anonimização seria a realização de um exame das

estratégias adotadas de minimização de dados sensíveis, buscando limitar a coleta e o armazenamento apenas ao necessário, bem como o uso de técnicas de anonimização para proteger a identificação dos indivíduos.

Quanto a Governança e transparência, a ênfase na importância da implementação de políticas de governança de dados sensíveis, envolvendo procedimentos claros para o tratamento e compartilhamento dessas informações, bem como a transparência na comunicação com os titulares dos dados bem como uma avaliação de impacto à privacidade, a exploração da necessidade de realizar avaliações de impacto à privacidade antes do tratamento de dados sensíveis, visando identificar e mitigar possíveis riscos e garantir que os direitos pessoais sejam preservados conforme abordado na obra “A Proteção de Dados Pessoais entre Leis, Códigos e Programação: Os limites do Marco Civil na Internet” de Rafael Zanatta:

> Para um estudo detalhado da experiência de governança colaborativa para proteção de dados pessoais (lei geral estatal combinada com produção de códigos pelo setor privado) e a influência dessa abordagem nas propostas da administração para regulação da privacidade (ZANATTA, 2015, p. 448).

A necessidade do uso de dados sensíveis muitas vezes entra em conflito com os direitos pessoais e a proteção da privacidade. Embora haja justificativas legítimas para o tratamento dessas informações, é crucial adotar medidas adequadas para minimizar os riscos de discriminação, invasão de privacidade e vazamento de dados sensíveis.

A implementação de estratégias como minimização, anonimização, governança, transparência e avaliação de impacto à privacidade pode ajudar a equilibrar essas duas dimensões, assegurando o respeito aos direitos pessoais enquanto permite o uso necessário e responsável dos dados sensíveis. É essencial que escritórios de advocacia e outras entidades que lidam com dados sensíveis adotem práticas éticas e cumpram as leis e regulamentações de proteção de dados para garantir a confiança dos indivíduos e a preservação dos seus direitos fundamentais, tais fundamentações podem ser encontradas na obra “O Impacto Da Lei Geral De Proteção De Dados Pessoais (LGPD) Nos Escritórios De Contabilidade” de Matheus Passaroto:

> O conjunto de fundamentos disciplinados pela LGPD promove não só a privacidade e segurança dos dados pessoais, mas também a livre iniciativa e liberdade de expressão do titular dos dados. Ou seja, o dono dos dados ganha novas camadas de proteção e autonomia, sem que, para isso, ele precise renunciar a sua liberdade em nível de informação, tecnologia e comunicação de modo geral. Estes são direitos garantidos por lei, e tais fundamentos devem ser respeitados por todos. (PASSAROTO, 2021, p. 4).

O aumento dos atos de concentração é um fenômeno resultante de um período de estabilidade econômica, no entanto a situação tende a agravar em períodos de desequilíbrio financeiro, onde um grande número de empresas passa a enfrentar dificuldades em cumprir seus compromissos financeiros, ingressando em um status de crise econômica.

> Para dados manifestamente públicos, ou seja, que estão disponíveis em bases do governo, como salários de funcionários/as do setor público, o consentimento é dispensado, porém continua sendo necessário justificar o tratamento com uma das outras bases legais. Ainda há discussão sobre se perfis e posts de redes sociais são considerados dados públicos. O tratamento desses dados deve ser feito, então, mediante a informação quanto à finalidade do uso e o consentimento do/a titular (ZANATTA, 2021, p. 25).

Visa, de maneira direta, a aplicação de atos de concentração por meio de fusão e compra e venda de capital dessas empresas em crise por outras do mesmo ramo econômico. Possui por objetivo impedir a perda de ativos e um posterior desequilíbrio no mercado financeiro.

2.3 Liberdade do uso de dados dos clientes empresariais

O uso de dados dos clientes por parte de escritórios de advocacia empresariais tem se tornado uma prática cada vez mais comum, impulsionada pela transformação digital e pela necessidade de oferecer serviços jurídicos personalizados e eficientes. Neste ensaio, iremos explorar de forma mais aprofundada os desafios éticos e legais envolvidos no uso de dados dos clientes por escritórios de advocacia, bem como a importância de encontrar um equilíbrio adequado entre a utilização dos dados e a proteção da privacidade conforme exporto por Fernando Hallsberg:

> De nada adiantará o LGPD ser implantado no papel, se disso não resultar na proteção de dados real, e mais, se na ocorrência de um vazamento de dados, não houver uma maneira de descobrir como e quando ocorreu esse vazamento, e isso só será possível com a adoção de ferramentas e políticas que suportem o controle, a rastreabilidade a auditoria da informação na empresa. (HALLSBERG, 2021, p. 23).

A liberdade do uso de dados dos clientes empresariais tem um impacto significativo nos advogados e nos escritórios de advocacia. Essa liberdade permite que os advogados acessem informações valiosas sobre as empresas clientes, auxiliando na prestação de serviços jurídicos mais eficientes e estratégicos.

Ao ter acesso aos dados dos clientes empresariais, os advogados podem personalizar seus serviços de acordo com as necessidades específicas de cada empresa. Isso significa que podem oferecer soluções jurídicas mais direcionadas e eficazes, levando em consideração as particularidades do setor de atuação, as demandas comerciais e as metas empresariais.

> Em que pese nesse escritório exista uma relação de confiança muito grande entre as pessoas que trabalham nele e que estão juntas há bastante tempo, a Lei Geral de Proteção de Dados obrigará a empresa a documentar todo o tratamento de dados pessoais, e com isso, o tratamento de arquivos que contenham dados pessoais, fazendo assim com que os escritórios consam prestar serviços mais exclusivos. (HALLSBERG, 2021, p. 23).

Além disso, a liberdade do uso de dados dos clientes empresariais permite que os advogados identifiquem padrões e tendências, contribuindo para a prevenção de problemas legais e para a antecipação de questões jurídicas que possam surgir no futuro. Com acesso a um conjunto abrangente de informações, os advogados podem oferecer aconselhamento proativo e estratégico, ajudando as empresas a tomar decisões embasadas e a mitigar riscos legais. A liberdade do uso de dados dos clientes empresariais também facilita a pesquisa e análise de precedentes legais relevantes, jurisprudência e regulamentações específicas. Essa informação é essencial para embasar os argumentos jurídicos e fortalecer a posição das empresas diante de litígios ou negociações.

Existem uma série de benefícios e justificativas para o uso de dados dos clientes, os escritórios de advocacia empresariais dependem do uso de dados dos clientes para oferecer serviços de alta qualidade e estratégicos. Alguns dos benefícios e justificativas para esse uso podem ser citadas a personalização dos serviços e Tomada de decisões embasadas em dados.

> Existe um amplo debate na literatura sobre diferentes “concepções de regulação”8 . Para alguns, “a regulação é algo que é feito exclusivamente por governos, uma questão de enforcement jurídico e estatal; para outros, regulação é principalmente um trabalho de atores sociais que monitoram outros atores, incluindo governos” (Levi-Faur, 2010, p. 4). Como nota a professora Julia Black, existem visões “centradas no Estado”, que privilegiam o controle focado e sustentado por uma agência pública sobre atividades que são valorizadas por uma comunidade, e visões “não centradas no Estado”, que consideram qualquer tipo de influência social e econômica, inclusive cultural, privilegiando atores não estatais. 9 Uma é mais jurídica, outra é sociológica. (ZANATTA, 2015, p. 449).

A análise dos dados dos clientes permite uma compreensão mais aprofundada de suas necessidades e demandas específicas, possibilitando a personalização dos serviços jurídicos para atender às suas expectativas. O acesso aos dados dos clientes possibilita uma análise mais precisa das situações jurídicas, permitindo que os advogados tomem decisões embasadas em dados concretos e aumentem a eficácia de suas estratégias.

É plausível e real os desafios éticos no uso de dados dos clientes por escritórios de advocacia empresariais, apresenta desafios éticos que devem ser cuidadosamente considerados. Alguns desses desafios incluem consentimento informado e confidencialidade e segurança.

É fundamental obter o consentimento informado dos clientes para o uso de seus dados. Isso envolve fornecer informações claras e transparentes sobre como os dados serão utilizados, conforme estipulado, iria garantindo que os clientes tenham plena compreensão e controle sobre o uso de suas informações pessoais.

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: XII - consentimento:

> manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (BRASIL, 2018).

A proteção da confidencialidade dos dados dos clientes é essencial para manter a confiança e a reputação do escritório de advocacia. Medidas robustas de segurança da informação devem ser implementadas para evitar acesso não autorizado e garantir a integridade dos dados.

Além dos desafios éticos, há também considerações legais importantes a serem levadas em conta no uso de dados dos clientes. As leis de proteção de dados, como a GDPR na União Europeia e a LGPD no Brasil, estabelecem diretrizes claras sobre como os dados pessoais devem ser coletados, armazenados e utilizados. Os escritórios de advocacia devem estar em conformidade com essas leis para garantir a proteção.

> Além disso, o uso de dados contribui para a melhoria da qualidade dos serviços jurídicos. Ao contar com informações precisas e atualizadas, os advogados podem embasar suas estratégias de defesa ou aconselhamento jurídico em dados concretos, aumentando a confiança e a credibilidade de seus argumentos. (HALLSBERG, 2021, p. 23)

Os dados também desempenham um papel fundamental na tomada de decisões informadas. Ao ter acesso a informações relevantes sobre casos similares, jurisprudência e precedentes legais, os advogados estão melhor equipados para orientar seus clientes e buscar soluções jurídicas mais favoráveis. Além disso, o uso de dados promove a eficiência e a otimização dos processos internos dos escritórios de advocacia. Com a automação e digitalização dos dados, os advogados têm acesso rápido e fácil a informações essenciais, reduzindo o tempo gasto em tarefas administrativas e permitindo que se concentrem em questões jurídicas de maior complexidade.

Em síntese, o uso de dados por escritórios de advocacia é de vital importância para o aprimoramento dos serviços jurídicos. Os dados fornecem insights valiosos, possibilitam a personalização dos serviços, contribuem para a tomada de decisões embasadas e aumentam a eficiência e a qualidade dos processos jurídicos. Portanto, é essencial que os escritórios de advocacia adotem práticas responsáveis e

éticas no uso dos dados, garantindo a privacidade e a proteção das informações de seus clientes.

CAPÍTULO III – *POSIÇÃO JURÍDICA E O TRATAMENTO LEGAL*

O presente capítulo trata detalhadamente sobre a posição jurídica e o tratamento legal perante a LGPD (Lei Nº 13.709, de 14 de Agosto de 2018), ela que é a Lei na qual regulamenta o tratamento de dados na internet, bem como todo o posicionamento jurídico ao seu entorno.

No contexto é apresentado as medidas judiciais cabíveis, as consequências possíveis em caso de violação da LGPD (Lei Nº 13.709), o tratamento ético e moral perante o tratamento de dados, critérios para definição de quantum indenizatório e jurisprudências e posicionamentos do magistrado e Tribunais Singulares e Superiores.

3.1 Medidas Judiciais Cabíveis

Ao se analisar a Lei Geral de Proteção de Dados, deve-se atentar as sanções possíveis para casos de violação das regras previstas expressamente na Lei Nº 13.709**/**18, a mesma é fiscalizada pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD) L.13.853, DE 8 DE JULHO DE 2019, na qual iniciou suas atividades em 2020, juntamente com a LGPD começando a vigorar, conforme estipulado pelo texto de lei:

> Art. 1º Fica a Autoridade Nacional de Proteção de Dados (ANPD) transformada em autarquia de natureza especial, mantidas a estrutura organizacional e as competências e observados os demais dispositivos da Lei nº 13.709, de 14 de agosto de 2018.Art. 2º Fica criado 1 (um) Cargo Comissionado Executivo nível 18 (CCE-18) de Diretor-Presidente da ANPD. (Produção de efeito)Parágrafo único. O cargo de

> que trata o caput deste artigo fica criado sem aumento de despesa, mediante a transformação de 1 (um) CCE-17 e de 1 (um) CCE-2 alocados na estrutura da ANPD. (BRASIL, 2022)

Em Termos Simples, relacionado a efeitos de responsabilidade cível, trata-se de formas diversas visto que em sua maioria, há enormes divergências situacionais de casos como aborda Cunha em sua obra *Lei Geral de Proteção de Dados e a Responsabilidade Civil dos Agentes de Proteção de Dados*:

> Para efeitos da responsabilidade civil, é destacável definir quem é o controlador e o operador em cada tratamento. Não pode haver dúvidas para o titular ou para a ANPD, visto que a responsabilidade de cada agente de proteção, em caso de violação à Lei Geral de Proteção de dados, é diferente (CUNHA, 2021, p. 25).

Uma das medidas judiciais cabíveis previstas pela LGPD (L.13.709/18) é o direito de os titulares de dados solicitarem o acesso aos seus próprios dados pessoais. Isso significa que qualquer pessoa pode requerer informações sobre quais dados estão sendo coletados, como estão sendo utilizados e com quem estão sendo compartilhados.

> Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: § 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento. (BRASIL, 2018).

Uma das medidas importantes é o direito de o titular de dados solicitar a correção ou retificação de informações incorretas ou incompletas que estejam sendo tratadas por uma empresa ou organização. Isso é fundamental para garantir a precisão e a veracidade dos dados pessoais e permitir que os titulares tenham controle sobre as informações que estão sendo armazenadas.

Além disso, a LGPD (L.13.709/18) também assegura o direito de os titulares solicitarem a exclusão de seus dados pessoais, especialmente nos casos em que o tratamento dessas informações não é mais necessário ou é realizado de forma irregular. Essa medida é conhecida como "direito ao esquecimento" e tem

como objetivo permitir que as pessoas possam eliminar registros que não são mais relevantes ou que desejam que sejam removidos.

> 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; (BRASIL, 2018).

Outra medida judicial cabível é a possibilidade de o titular de dados requerer indenização por danos morais ou materiais decorrentes do tratamento inadequado de seus dados pessoais. Se uma empresa ou organização não tomar as medidas necessárias para proteger os dados pessoais e ocorrer um vazamento de informações, por exemplo, o titular dos dados pode buscar compensação pelos prejuízos causados.

> 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. § 1º A fim de assegurar a efetiva indenização ao titular dos dados. (BRASIL, 2018).

Ademais, a Autoridade Nacional de Proteção de Dados (ANPD) também possui poderes de fiscalização e aplicação de sanções administrativas. Caso uma empresa descumpra a L.13.709/18, a ANPD L.13.853/19 pode impor advertências, multas, bloqueio ou eliminação dos dados pessoais, entre outras penalidades, pois conforme o Art. 5º estabelece que, “a autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. ” BRASIL, 2018

Em resumo, as medidas judiciais cabíveis previstas pela L.13.853 incluem o direito de acesso, retificação e exclusão dos dados pessoais, além do direito de indenização por danos, com a possibilidade de recorrer ao Poder Judiciário. A LGPD visa garantir a proteção dos direitos dos titulares de dados e a adequada utilização de suas informações pessoais, tudo isso respaldado pelos termos da Lei já supracitados acima.

3.2 Consequências possíveis em caso de violação da Lei Geral de Proteção de Dados

A violação da Lei Geral de Proteção de Dados (L.13.709/18) pode acarretar em diversas consequências para as empresas e organizações envolvidas. A LGPD foi criada para proteger a privacidade e os direitos dos titulares de dados, e o texto de lei possui disposições claras quanto às medidas a serem tomadas em casos de descumprimento.

Uma das consequências mais imediatas é a possibilidade de aplicação de sanções administrativas pela Autoridade Nacional de Proteção de Dados (L.13.853/19). A ANPD é o órgão responsável pela fiscalização e aplicação das penalidades previstas na lei. Essas penalidades podem variar desde advertências e multas até a suspensão temporária das atividades relacionadas ao tratamento de dados pessoais assim como já descrito anteriormente.

O Artigo 42 da Lei Geral de Proteção de Dados (LGPD) estabelece a responsabilidade do controlador ou do operador de dados em reparar os danos patrimoniais, morais, individuais ou coletivos causados a terceiros em decorrência do tratamento inadequado de dados pessoais, em violação à legislação de proteção de dados. Essa disposição legal tem como objetivo principal proteger os direitos dos titulares de dados e garantir que haja um mecanismo para reparação em caso de prejuízo causado pela má utilização ou violação das informações pessoais. A responsabilidade recai tanto sobre o controlador quanto sobre o operador de dados. O controlador é a pessoa física ou jurídica que decide sobre a finalidade e os meios de tratamento de dados pessoais, enquanto o operador é aquele que realiza o tratamento em nome do controlador, seguindo suas instruções.

> 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. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos

> casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. (BRASIL, 2018).

As multas impostas pela ANPD podem chegar a valores significativos, podendo alcançar até 2% do faturamento da empresa no último exercício fiscal, limitado a R$ 50 milhões por infração. Em casos de infrações mais graves, as multas podem ser dobradas, chegando a 4% do faturamento, limitado a R$ 50 milhões. Essas multas podem ter um impacto financeiro considerável nas empresas, especialmente nas de grande porte.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; (BRASIL, 2018).

Além das sanções administrativas, as empresas também podem enfrentar consequências jurídicas por meio de ações judiciais movidas pelos titulares de dados afetados. Os titulares têm o direito de buscar indenizações por danos morais ou materiais decorrentes da violação de seus dados pessoais. Se ficar comprovado que a empresa negligenciou as medidas de segurança ou utilizou os dados de forma indevida, ela pode ser condenada a pagar compensações financeiras aos titulares de dados afetados.

> 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. § 1º A fim de assegurar a efetiva indenização ao titular dos dados (BRASIL, 2018).

Outra consequência importante é a reputacional. A violação da LGPD pode resultar em danos significativos à imagem e à reputação da empresa. A perda de confiança dos clientes e do público em geral pode afetar a relação comercial, causando a redução de vendas e a perda de clientes. A má reputação pode levar

anos para ser reconstruída, e a empresa pode enfrentar dificuldades para se recuperar do impacto negativo.

Além disso, a empresa pode enfrentar consequências operacionais e comerciais, como a proibição ou restrição de atividades relacionadas ao tratamento de dados pessoais. Caso a ANPD determine a suspensão temporária de tais atividades, a empresa pode sofrer interrupções em seus processos, o que pode afetar diretamente sua capacidade de conduzir negócios normalmente.

> Art. 5º Para os fins desta Lei, considera-se: XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018).

Assim como é exposto no Art.18 da Lei nº 13.709/2018, a LGPD permite que os órgãos de defesa do consumidor e de proteção do direito à privacidade também atuem em casos de violação. Esses órgãos podem impor sanções adicionais, como a aplicação de multas ou até mesmo a interdição das atividades da empresa.

Em resumo, as consequências em caso de violação da LGPD (L.13709) são diversas e podem ter um impacto significativo nas empresas. Além das sanções administrativas e das multas impostas pela ANPD (L.13.853), as empresas podem enfrentar ações judiciais, danos à sua reputação, perda de clientes, interrupção de atividades e sanções adicionais por parte de órgãos de defesa.

3.3. Tratamento ético e moral perante ao tratamento de dados

O tratamento ético e moral dos dados é um tema de extrema relevância e é central na Lei Geral de Proteção de Dados (L.13709/18) no Brasil, a qual foi criada com o objetivo de proteger a privacidade e os direitos dos indivíduos em

relação ao tratamento de seus dados pessoais, estabelecendo princípios éticos e morais que devem guiar as práticas das empresas e organizações.

Um dos princípios fundamentais da L.13709/18 é o princípio da finalidade. Esse princípio determina que o tratamento de dados pessoais deve ser realizado com propósitos legítimos, específicos e informados aos titulares dos dados. Isso significa que as empresas devem ter uma base legal para coletar e utilizar os dados, devendo ser transparentes sobre os motivos pelos quais estão fazendo isso. O tratamento de dados deve ser pautado por uma finalidade legítima, evitando qualquer tipo de uso abusivo ou indevido das informações pessoais dos indivíduos.

> Todos esses objetivos que, integradamente, conformam a finalidade admitida pelo normativo, devem ser informados ao titular, o qual, com ele concordando, delimitará o objeto do tratamento, domínio esse que não poderá ser subsequentemente alterado, salvo se nova, especifica e expressa concordância for obtida desse titular. (PESTANA, 2020 p. 2).

Outro princípio importante é o da necessidade. Ele estabelece que o tratamento de dados pessoais deve se limitar ao mínimo necessário para alcançar a finalidade pretendida. Isso implica que as empresas devem evitar a coleta excessiva de dados e garantir que apenas as informações estritamente necessárias sejam tratadas. Ao adotar uma abordagem baseada na necessidade, as organizações demonstram seu compromisso com a proteção da privacidade e o respeito aos direitos dos indivíduos.

> O princípio da necessidade consubstancia-se na limitação da realização do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. A regra geral, portanto, trazida pela LGPD, é não se realizar o tratamento; a exceção, ao reverso, é a de realiza-la, se e quando o atingimento de determinada finalidade se mostrar relevante para que o tratamento seja realizado. No caso, somente deverão ser tratados os dados pertinentes, ou seja, aqueles que se mostrem imprescindíveis para que o objetivo previamente tracejado seja atingido. Nem poderia ser diferente, pois seria de todo impróprio serem tratados dados que não se mostrassem pertinentes e relevantes para o tratamento em questão. (PESTANA, 2020 p. 4).

A L.13709/18 também enfatiza a importância do consentimento informado dos titulares dos dados. O consentimento é um dos fundamentos legais para o tratamento de dados e deve ser obtido de forma clara, específica e inequívoca. As empresas devem informar aos titulares sobre as finalidades do tratamento, os tipos de dados coletados, os destinatários das informações e os direitos que os titulares possuem em relação aos seus dados pessoais. É fundamental que o consentimento seja livremente dado, sem qualquer tipo de coerção ou pressão, e que os titulares possam revogá-lo a qualquer momento, caso desejem.

Além disso, a L.13709/18 estabelece a responsabilidade das empresas em proteger os dados pessoais de maneira adequada. As organizações devem implementar medidas técnicas e organizacionais para garantir a segurança dos dados, evitando o acesso não autorizado, a perda, a alteração ou a divulgação indevida das informações pessoais. Essas medidas incluem a implementação de controles de acesso, a criptografia de dados, a realização de auditorias de segurança e a adoção de políticas de retenção adequadas.

> Apesar da utilidade deste critério, que por ser objetivo, antitruste traz segurança aos agentes econômicos, ele pode, como atualmente vem sendo demonstrado, ser insuficiente para submeter à análise aquisições voltadas à obtenção de dados relevantes, em termos quantitativos e qualitativos (RODRIGUES, 2018 p. 4).

No contexto do tratamento ético e moral dos dados, é essencial que as empresas promovam a transparência e a responsabilidade. Isso implica fornecer informações claras e acessíveis aos titulares dos dados, explicando como seus dados são coletados, utilizados e protegidos. As organizações também devem assumir a responsabilidade por suas ações, sendo capazes de prestar contas pelo tratamento de dados que realizam.

> Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das

> normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (AFFONSO, 2021 p. 14).

É importante ressaltar que o tratamento ético e moral dos dados vai além do cumprimento da legislação. Embora a LGPD estabeleça os parâmetros legais para o tratamento de dados, é fundamental que as empresas adotem uma abordagem ética e moral para além das exigências legais. Isso implica respeitar a privacidade dos indivíduos, evitar práticas discriminatórias, garantir a segurança dos dados e tomar medidas para promover a equidade e a justiça no tratamento de informações pessoais.

> O Estado Brasileiro tem, dentre tantas incumbências descritas em sua Carta Magna, a obrigação de defender a livre concorrência (artigo 170, IV), promovendo por meio da ordem econômica, justiça social, sendo, dessa forma, a garantia desse princípio um meio de promover a dignidade da pessoa humana. Havendo então modificações desvantajosas à ordem competitiva, é uma função-dever do Estado criar mecanismos para retornar à situação de equilíbrio. (RODRIGUES, 2018 p. 10).

No que diz respeito aos direitos dos titulares dos dados, a LGPD reconhece a importância de garantir a autodeterminação informativa. Os titulares têm o direito de acessar seus dados, corrigi-los, excluir informações desnecessárias, solicitar a portabilidade dos dados para outros serviços e obter informações claras e transparentes sobre o tratamento de seus dados pessoais. É fundamental que as empresas estejam preparadas para atender a essas demandas e tratar os direitos dos titulares com seriedade e respeito.

Além das sanções administrativas, conforme estabelece no § 4º do Art. 42 da L.13709/18, a empresa também pode enfrentar ações judiciais movidas pelos titulares dos dados afetados. Os titulares têm o direito de buscar reparação por danos patrimoniais, morais, individuais ou coletivos decorrentes da violação da LGPD. Nesse sentido, é essencial que as empresas estejam cientes das suas obrigações legais e éticas e implementem práticas de tratamento de dados em conformidade com a lei.

Em suma, o tratamento ético e moral dos dados é um princípio fundamental na LGPD. As empresas devem adotar uma abordagem ética e

responsável, garantindo a privacidade, a segurança e o respeito aos direitos dos titulares dos dados. Ao fazer isso, as organizações fortalecem a confiança dos indivíduos, demonstram seu compromisso com a proteção de dados e contribuem para a construção de uma sociedade digital mais ética e responsável.

> Apesar dos grandes desafios enfrentados, é possível afirmar que o debate das implicações do Big Data no meio jurídico pelos órgãos responsáveis por regular a concorrência evoluiu. Embora ainda muito incipiente no cenário brasileiro, no âmbito da União Europeia, significativas discussões já estão sendo travadas com finalidade te tornar o compartilhamento de dados cada vez mais ético e moral (RODRIGUES, 2018 p. 9).

3.4. Critério para definição de quantum indenizatório

A definição do quantum indenizatório na Lei Geral de Proteção de Dados LGPD (L.13709/18) é um tema relevante e complexo. O quantum indenizatório refere-se ao valor da indenização que deve ser concedida quando ocorre uma violação da LGPD que cause danos patrimoniais, morais, individuais ou coletivos aos titulares dos dados.

A LGPD estabelece que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dad0os pessoais, causar dano a outrem em violação à legislação de proteção de dados pessoais é obrigado a repará-lo (conforme disposto no Art. 42 da lei). No entanto, a lei seca não especifica critérios precisos para a definição do valor da indenização, deixando essa tarefa para o Judiciário.

Entretanto, passando-se para o legislativo, o artigo 944 do Código Civil brasileiro trata do princípio da reparação integral do dano, estabelecendo que aquele que causar um dano a outra pessoa tem a obrigação de repará-lo integralmente. O referido artigo dispõe o seguinte:

> "Art. 944 - A indenização mede-se pela extensão do dano. Parágrafo único - Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização. Art. 945. Se a vítima tiver concorrido culposamente para

> o evento danoso, a sua indenização será fixada tendo-se em conta a gravidade de sua culpa em confronto com a do autor do dano. " (BRASIL, 2002)

O primeiro parágrafo do artigo 944 estabelece que a indenização deve ser proporcional à extensão do dano causado. Isso significa que a pessoa que causou o dano é responsável por reparar integralmente todas as consequências dele advindas. O objetivo é garantir que a vítima seja colocada na mesma situação em que se encontrava antes da ocorrência do dano.

O parágrafo único do artigo 944 estabelece uma ressalva ao princípio da reparação integral do dano. Caso haja uma desproporção excessiva entre a gravidade da culpa do causador do dano e o dano efetivamente sofrido pela vítima, o juiz pode reduzir equitativamente o valor da indenização. Essa redução visa evitar que a indenização seja excessiva em relação à gravidade da culpa, prezando pela equidade na fixação do valor a ser indenizado.

No contexto da Lei Geral de Proteção de Dados (LGPD), o artigo 944 do Código Civil pode ser aplicado na determinação do quantum indenizatório em casos de violação de dados pessoais. A LGPD prevê a obrigação de reparação por danos patrimoniais, morais, individuais ou coletivos causados em razão do tratamento inadequado dos dados pessoais. Assim, o princípio da reparação integral do dano estabelecido pelo artigo 944 do Código Civil será levado em consideração na definição do valor da indenização, buscando compensar integralmente os prejuízos sofridos pelos titulares dos dados.

Em suma, o artigo 944 do Código Civil brasileiro estabelece o princípio da reparação integral do dano, segundo o qual aquele que causa um dano tem a obrigação de repará-lo integralmente. Esse princípio é aplicável na determinação do quantum indenizatório em casos de violação da LGPD, garantindo que a vítima seja compensada adequadamente pelos danos sofridos.

3.5. Jurisprudências e Posicionamentos do Magistrado e Tribunais Singulares e Superiores (STJ e STF)

A jurisprudência é um importante elemento para a interpretação e

aplicação da Lei Geral de Proteção de Dados (LGPD). Magistrados e tribunais têm desempenhado um papel fundamental na definição de entendimentos e posicionamentos sobre a lei, contribuindo para sua efetividade e compreensão. Neste texto, abordaremos algumas jurisprudências e posicionamentos do magistrado e dos tribunais superiores, como o Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF), em relação à LGPD (Lei 13.709/2018).

Desde a entrada em vigor da LGPD, houve um crescimento significativo na produção jurisprudencial relacionada à proteção de dados pessoais. Os tribunais têm sido acionados para resolver disputas e questões relacionadas ao tratamento de dados, responsabilização de empresas e garantia dos direitos dos titulares.

Um tema recorrente na jurisprudência é a interpretação dos princípios e direitos estabelecidos na LGPD. Os tribunais têm reafirmado a importância dos princípios da finalidade, necessidade, consentimento e transparência no tratamento de dados. Além disso, têm reconhecido os direitos dos titulares, como o direito de acesso, retificação, exclusão e portabilidade dos dados, bem como o direito à não discriminação e à privacidade.

No que diz respeito à responsabilidade das empresas, a jurisprudência tem sinalizado que tanto os controladores quanto os operadores de dados podem ser responsabilizados por violações da LGPD. Os tribunais têm entendido que as empresas devem adotar medidas adequadas para garantir a segurança e a proteção dos dados pessoais, sendo passíveis de sanções e indenizações em caso de descumprimento das obrigações legais.

Outro ponto relevante é a discussão sobre a competência da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela fiscalização e aplicação da LGPD. Os tribunais têm se posicionado no sentido de reconhecer a legitimidade e a autoridade da ANPD para impor sanções administrativas e regular as atividades de tratamento de dados. A jurisprudência tem destacado a importância da atuação da ANPD na promoção da conformidade com a lei e na garantia da proteção dos direitos dos titulares dos dados.

No que diz respeito aos tribunais superiores, tanto o STJ quanto o STF têm tido participação ativa na construção da jurisprudência sobre a LGPD conforme exposto em sítios governamentais. O STJ, em diversos julgados, tem se posicionado no sentido de garantir a proteção dos direitos dos titulares e de responsabilizar as empresas em caso de violação da lei. O tribunal tem entendido que a LGPD deve ser interpretada de forma ampla e em consonância com a Constituição Federal, garantindo a privacidade, a segurança e a dignidade dos indivíduos.

Por sua vez, o STF também tem se debruçado sobre questões relacionadas à LGPD. Em alguns casos, o tribunal tem abordado temas como a constitucionalidade da LGPD, a proteção de dados sensíveis e a aplicação da lei no âmbito das relações de trabalho. A atuação do STF tem contribuído para a consolidação da interpretação da LGPD e para a definição de parâmetros importantes na aplicação da lei.

É importante ressaltar que a jurisprudência relacionada à LGPD está em constante evolução e que novos posicionamentos e entendimentos podem surgir à medida que mais casos são julgados. A interpretação e aplicação da LGPD pelos tribunais são fundamentais para garantir a segurança jurídica e a proteção dos direitos dos titulares dos dados.

Em suma, a jurisprudência tem desempenhado um papel essencial na definição de entendimentos e posicionamentos sobre a LGPD. Magistrados e tribunais, incluindo o STJ e o STF, têm se debruçado sobre questões relacionadas à interpretação dos princípios e direitos da lei, responsabilidade das empresas e competência da ANPD. A jurisprudência contribui para a consolidação da LGPD, a proteção dos direitos dos titulares dos dados e a promoção de uma cultura de proteção de dados no Brasil.

CONCLUSÃO

Este estudo abrangeu de forma ampla a progressão da Lei Geral de Proteção de Dados, desde os estágios iniciais em outros países até a atualidade. É claro que o tópico ainda suscita incertezas na sociedade em relação aos efeitos dos benefícios e malefícios e a necessidade da responsabilidade redobrada no uso de tais dados. Portanto, um dos objetivos desta pesquisa é esclarecer todas as questões relevantes sobre o tema.

Em suma, a Lei Geral de Proteção de Dados (LGPD) representa um marco significativo para os escritórios de advocacia empresarial no que diz respeito à proteção e tratamento adequado das informações pessoais de seus clientes e funcionários. A implementação e conformidade com essa legislação demonstram o comprometimento dessas organizações em salvaguardar a privacidade e a segurança dos dados, promovendo uma cultura de transparência e confiança.

Ao adotar medidas de conformidade, como a nomeação de um encarregado de proteção de dados, a realização de avaliações de impacto e a adoção de políticas e procedimentos robustos, os escritórios de advocacia empresarial podem garantir a conformidade com a LGPD. Além disso, a adoção de soluções tecnológicas adequadas, como criptografia de dados e sistemas de armazenamento seguro, contribui para a proteção efetiva das informações sensíveis.

Além dos benefícios diretos da conformidade com a LGPD, os escritórios de advocacia empresarial também podem aproveitar as oportunidades que surgem a partir da adequação a essa legislação. A LGPD estabelece diretrizes claras sobre a coleta, uso, armazenamento e compartilhamento de dados pessoais, o que permite aos escritórios desenvolverem práticas mais eficientes e seguras no tratamento das informações dos clientes.

A conformidade com a LGPD não apenas evita possíveis sanções e penalidades, mas também confere credibilidade e reputação às empresas de advocacia empresarial, demonstrando o respeito aos direitos fundamentais dos indivíduos e à privacidade. Ao investir em medidas de segurança cibernética e na educação de seus colaboradores, os escritórios de advocacia podem se posicionar como parceiros confiáveis para seus clientes, capazes de lidar com questões de proteção de dados com responsabilidade e expertise.

Ademais, a LGPD também contribui para a criação de um ambiente de negócios mais seguro e confiável. Ao promover a conscientização sobre a importância da proteção de dados e estabelecer diretrizes claras, a legislação incentiva uma cultura de responsabilidade e transparência em relação ao tratamento das informações pessoais. Isso pode gerar um impacto positivo tanto para os escritórios de advocacia empresarial quanto para seus clientes, que se sentirão mais protegidos e amparados em relação à privacidade de seus dados.

Em síntese, a implementação efetiva da LGPD nos escritórios de advocacia empresarial é fundamental para a proteção dos direitos de privacidade dos indivíduos e para o fortalecimento da confiança entre advogados e clientes. O compromisso com a conformidade demonstra uma postura proativa em relação à segurança dos dados e à proteção de informações sensíveis.

Em conclusão, a conformidade com a LGPD nos escritórios de advocacia empresarial vai além do cumprimento legal, sendo uma oportunidade de fortalecimento do relacionamento com os clientes, diferenciação no mercado e desenvolvimento de práticas mais eficientes e seguras. Ao abraçar essa legislação e adotar medidas adequadas de proteção de dados, os escritórios podem se posicionar como líderes na proteção da privacidade e na garantia dos direitos dos indivíduos, ao mesmo tempo em que impulsionam seu próprio crescimento e sucesso no mercado jurídico contemporâneo.

BIBLIOGRAFIA

ÁVILA, Ana Paula Oliveira. A tutela jurídica da privacidade e do sigilo na era digital. **Revista de Investigações Constitucionais**, Curitiba, vol. 4, n. 3. p. 167-200, set./dez. 2017.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor**. Civilistica**. com, v. 9, n. 3, p. 1-23. Rio de Janeiro. 2020,

BIONI, Ricardo B. Proteção de Dados Pessoais, A Função e os Limites do Consentimento, Editora **Forense.** Rio de Janeiro, 2019.

BRASIL. **Cartilha da Lei Geral de Proteção de Dados Pessoais – LGPD.** Diário Oficial da União, Brasília, DF. 2021;

BRASIL. **Constituição da República Federativa do Brasil.** Brasília: Congresso Nacional. 1988.

BRASIL. **Ementa de Lei Nº 13.853,** de 08 de julho de 2019. **para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.** (Lei Geral de Proteção de Dados). Diário Oficial da União, Brasília, 2019.

BRASIL. **Lei Nº 12.965,** de 23 de abril de 2014. **Marco Civil da Internet Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Diário Oficial da União, Brasília, 2014.

BRASIL. **Lei Nº 13.709,** de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Diário Oficial da União, Brasília, 2018.

BRASIL. **Lei Nº 14.460,** de 25 de outubro de 2022. **Autoridade Nacional de Proteção de Dados**. Diário Oficial da União, Brasília. 2022.

BRASIL. **Lei Nº 10.406** (Código Civil). Brasília: Congresso Nacional. 2002.

BRASIL. **Lei Nº 8.906,** de 04 de julho de 1994. **Sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB).** Diário Oficial da União, Brasília, 1994.

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

CRESPO, Marcelo. Lei Geral De Proteção De Dados E O Poder Público. Disponível em: ebook_lgpd_e_poder_publico_23052021.pdf (procempa.com.br). **Tribunal de Contas do Estado.** p. 16**,** Porto Alegre. 2021.

CUNHA, Giovana, Raulino. **Lei Geral de Proteção de Dados e a Responsabilidade Civil dos Agentes de Proteção de Dados.** Monografia. Faculdade de Direito da Universidade do Sul de Santa Catarina**.** Florianópolis. p. 29. 2021.

DA CRUZ, U. L.; PASSAROTO, M.; JUNIOR, N. T. O Impacto Da Lei Geral De Proteção De Dados Pessoais (LGPD) Nos Escritórios De Contabilidade. **ConTexto - Contabilidade em Texto**, Porto Alegre, v. 21, n. 49, p. 30–39, 2021. Disponível em: https://seer.ufrgs.br/index.php/ConTexto/article/view/112561. Acesso em: 15 abr. 2023.

DIAS, G. A.; VIEIRA**,** A. A. N. Big data: questões éticas e legais emergentes**. Ciência da Informação**, [S. l.], v. 42, n. 2, 2015.

ESTADOS UNIDOS DA AMERICA. **Lei do Senado Norte Americano Nº 561.** 22 de fevereiro de 2019**. Amendment to California Consumer Privacy Act (CCPA).** Sacramento. 2019. Disponível em: Texto do projeto de lei - SB-561 California Consumer Privacy Act of 2018: consumer remedies.

ESTADOS UNIDOS DA AMERICA. **Lei do Senado Norte Americano Nº 1121.** 23 de setembro de 2018. **California Consumer Privacy Act (CCPA).** Sacramento. 2018. Disponível em: Texto do projeto de lei - SB-1121 California Consumer Privacy Act of 2018.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. **Revista de Direito Brasileira**, [S.l.], v. 23, n. 9, p. 284-301, fev. 2020. ISSN 2358-1352. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343>. Acesso em: 12 mar. 2023.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis,** v. 12, p. 1002-1033, Rio de Janeiro. 2021.

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo. Os desafios da Administração Pública na disponibilização de dados sensíveis, **Revista Direito GV. v. 14 N. 2,** ISSN 2317-6172. São Paulo. 2018.

HALLBERG, Fernando Bottega. **Gestão de arquivos em nuvem na era da LGPD com enfoque em um escritório de advocacia.** Relatório de pesquisa. Curso de Tecnólogo em Gestão da Tecnologia da Informação. Universidade do Sul de Santa Catarina. Palhoça. p. 24. 2021. Disponível em:ModeloparaDigitação(animaeducacao.com.br). Acesso em: 23 mar. 2023.

Jesus, Johnatan Douglas Andrade de. **A nova realidade do tratamento e da proteção de dados dos trabalhadores frente a LGPD e o Compliance jurídico**. São Cristóvão, 2021. Monografia (graduação em Direito) – Departamento em Direito, Centro de Ciências Sociais Aplicadas, Universidade Federal de Sergipe, São Cristóvão. 2021. Disponível em: https://ri.ufs.br/jspui/handle/riufs/14531. Acesso em 5 mai. 2023.

MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor.** Revista dos Tribunais, v. 1009**,** 2019.

PALHARES, Felipe; ISZLAJI, Bárbara de Oliveira. O Congresso e as discussões para alterar a Lei Geral de Proteção de Dados Pessoais. **Revista Consultor Jurídico**, 22 de agosto de 2021. Disponível em:ConJur-IszlajiePalhares:OCongressoeasdiscussõesparaalteraraLGPD.

PELOSO PIURCOSKY, Fabrício. et al. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de negocios,** v. 10, n. 23, p. 89-99, 2019.

PESTANA Marcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). **Revista Consultor Jurídico**, 25 de maio de 2020. Disponível em: ConJur-MarcioPestana:OsprincípiosnotratamentodedadosnaLGPD.

RAPÔSO, Cláudio Filipe Lima. et al. LGPD-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática**. RACE-Revista de Administração do Cesmac, v. 4, p. 58-67,** 2018;

RODRIGUES Laura Domingos. **OS DESAFIOS OCASIONADOS PELO BIG DATA PARA O DIREITO ANTITRUSTE:** Seria possível e, em o sendo, como dificultar a dominação do mercado por grandes agentes que se utilizam do Big Data?. 42-53 Artigo Universidade de São Paulo. São Paulo. 2018. Disponível em: IInovacao-Desafios-Cunha-Rodrigues.pdf(usp.br). Acesso em 11 jun. 2023.

UNIÃO EUROPEIA**, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho** de 27 de abril de 2016 **General Data Protection Regulation**. Jornal Oficial da União Europeia. 2016. Disponível em: EUR-Lex-32016R0679-EN-EUR-Lex(europa.eu)

VIANNA, Renata Seixa. **A LGPD no Poder Judiciário:** a implementação das medidas referentes ao exercício do direito dos titulares previstas na resolução CNJ n. 363/2021 nos tribunais. 2021. 244 f., il. Dissertação (Mestrado em Direito) — Universidade de Brasília, Brasília, 2021.

ZANATTA Rafael. **A proteção de dados pessoais entre leis, códigos e programação:** os limites do Marco Civil da Internet, Artigo, p. 447–470. São Paulo. 2015.

ZANATTA, Rafael; ROSA, Maraísa. **Manual Prático de Adequação à Lei Geral de Proteção de Dados para Organizações da Sociedade Civil,** p. 55. São Paulo 2021;