IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO CIVIL CONTEMPORÂNEO

CÉSAR AUGUSTO DE CASTRO FIUZA

MARIA CREUSA DE ARAÚJO BORGES

HELENA NASTASSYA PASCHOAL PITSICA

D597

Direito civil contemporâneo [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: César Augusto de Castro Fiuza; Maria Creusa De Araújo Borges; Helena Nastassya Paschoal Pitsica – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-426-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, desenvolvimento, sustentabilidade e smart cities.

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito civil. 3. Contemporâneo. IV Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO CIVIL CONTEMPORÂNEO

Apresentação

No presente livro, são tratados vários temas. O interessante é que perpassa por todos eles, direta ou indiretamente, a ideia de responsabilidade civil. O Direito Civil Contemporâneo pode ser visto sob dois prismas. Primeiramente, como sinônimo de Direito Civil Constitucional; em segundo lugar, como Direito Civil dogmático, visto sob a ótica do Direito Privado e da autonomia privada. Nos textos que compõem este livro, pode-se verificar ambas as vertentes. Espera-se que o leitor possa tirar bom proveito.

CONTROLE E PROTEÇÃO DE DADOS NO BRASIL: A MEDIAÇÃO COMO INSTRUMENTO DE COMPLIANCE NO ÂMBITO DA LGPD

DATA CONTROL AND PROTECTION IN BRAZIL: MEDIATION AS A COMPLIANCE INSTRUMENT WITHIN THE LGPD

Alexandra Clara Ferreira Faria [1]
Maria Theresa Duarte Reis [2]

Resumo

O trabalho pretende analisar a Mediação, como instituto eficaz de resolução de conflitos de compliance de dados, na prevenção e nos conflitos da aplicação da legislação de proteção de dados. Assim, contextualizou-se a implementação da LGPD, apresentando aspectos relacionados ao compliance e a efetividade da mediação extrajudicial. Apartir disso, conclui-se que a Mediação é essencial de controle de riscos e de efetividade de compliance.

Palavras-chave: Lgpd, Dados, Mediação, Compliance

Abstract/Resumen/Résumé

The paper aims to analyze Mediation, as an effective institute for the resolution of data compliance conflicts, in the prevention and conflicts of the application of data protection legislation. Thus, the implementation of the LGPD was contextualized, presenting aspects related to compliance and the effectiveness of out-of-court mediation. From this, it is concluded that Mediation is essential for risk control and compliance effectiveness

Keywords/Palabras-claves/Mots-clés: Lgpd, Data, Mediation, Compliance

[1] Doutora e Mestre Direito. Professora Adjunto IV da Faculdade Mineira de Direito da PUC/Minas. e da Pós-Graduação do IEC da PUC/Minas. Pesquisadora do Núcleo de Estudos Novos Direitos Privados. Advogada.

[2] Graduada em Direito pela PUC/Minas. Graduanda do curso de Gestão Pública pela UFMG. Advogada.

INTRODUÇÃO

Em virtude do crescimento do impacto das tecnologias digitais na pós-modernidade e a consolidação de espaços públicos virtuais, a gestão da informação pessoal tornou-se expressão fundamental dos indivíduos, uma vez que a posse de dados por empresas passou a ter cada vez mais valor econômico e importância no mercado de consumo.

Por esta razão, pode se dizer que, atualmente, é impossível cogitar a proteção integral à liberdade, à privacidade e ao desenvolvimento da pessoa natural sem que lhe seja garantida, de forma eficaz, a defesa e o controle de seus próprios dados. Emerge nesse contexto os questionamentos que devem ser analisados, justificando a necessidade do presente estudo, tendo em vista a proteção dos Direitos da Personalidade, consagrados no Estado Democrático de Direito.

A hipótese é de identificar as sanções e os instrumentos de resolução de conflitos no desrespeito da legislação nesse mercado virtual de dados através de programas de compliance de dados.

Logo, para teste da hipótese, as vertentes teórico-metodológicas e jurídico-descritivas e sistemáticas são utilizadas, sendo o método aplicado para a elaboração do artigo a abordagem do referido tema no sentido crítico dialético. Para tanto, recorrer-se ao método histórico-comparativo, em razão de estudo dos institutos da Mediação e sua aplicação na Lei Geral de Proteção de Dados – LGPD.

Nesse cenário de proteção dos Direitos da Personalidade, considerando o direito à privacidade, disposto como direito fundamental na Constituição da República Federativa do Brasil de 1988, no contexto de uma sociedade, cuja economia se orienta cada vez mais a partir dos dados pessoais, a implementação da Lei Geral de Proteção de Dados Pessoais - LGPD, Lei Federal nº 13.709, de 2018, se mostra como fundamental para a proteção desses direitos fundamentais da pessoa humana.

Assim, a perspectiva da instituição de um novo paradigma relacionado à proteção de dados, emerge a utilidade teórico-prática do estudo, a partir da necessidade de adaptação às novas normas, como forma de garantir a proteção dos dados enquanto um direito fundamental da pessoa humana, e de prevenir a existência de conflitos e aplicação de sanções em decorrência do descuprimento da legislação. Logo, faz-se de extrema importância os programas de compliance de dados, a fim de que as empresas, imersas em mercados virtuais, possam se adaptar à legislação vigente, valendo-se, assim, de instrumentos efetivos de

cumprimentos desses programas.

Desse modo, o presente trabalho pretende apresentar os principais aspectos da LGPD, de modo a apresentar, inicialmente, o histórico de implementação de normas no ordenamento jurídico brasileiro que versam sobre a questão da proteção de dados e que, posteriormente, culminaram na elaboração da LGPD, cujos aspectos principais serão abordados.

Em seguida, o presente trabalho explorará os principais aspectos do compliance de dados, primeiro apresentando o conceito e a importância dos programas de compliance, para, assim, aplicá-los no âmbito da LGPD. Por fim, o trabalho apresentará as principais características da mediação extrajudicial e como este pode ser um instrumento de resolução de conflitos que confere efetividade aos progrmas de compliance, resolvendo e prevenindo conflitos.

Assim, pretende-se demonstrar a hipótese testada e seus efeitos, propondo juridicamente um estudo como contribuição do artigo que seja capaz de fornecer um cenário de tratamento e proteção de dados no Brasil na atualidade e quais as ferramentas importantes que as empresas, sobretudo, as atuantes no mercado de consumo, podem utilizar para se adaptarem à nova legislação.

A conclusão é a aplicação do instituto da Mediação como uma equivalente jurisdicional na resolução de conflitos advindos da inobservância da legislação de LGPD enquanto um instrumento de compliance.

1. O ARCABOUÇO LEGAL DE PROTEÇÃO DE DADOS NO BRASIL

A proteção de dados no Brasil e as legislações pertinentes demonstram a preocupação com a privacidade das pessoas, efetivando o direito fundamental.

1.1 Contexto Legal da Proteção de dados no Brasil

O contexto de desenvolvimento tecnológico que estamos vivendo fez surgir novos meios de interação, como o Big Data[5]; os algoritmos[6] e a inteligência artificial. Todos esses meios de interação causam uma exposição virtual mais acentuada, e ao mesmo tempo ganham valor econômico no mercado digital, eis que os dados são vendidos no mercado de consumo, o que vem despertando a atenção não só do mundo jurídico, mas da sociedade em geral.

O sistema atual de proteção das informações pessoais e do exercício das garantias individuais na internet foi construído com base no importante tripé formado pela Lei de

Acesso à Informação, Marco Civil da Internet e pela Lei Geral de Proteção de Dados. Mas não só, pois o acesso à informação, a proteção aos dados pessoais e os novos meios digitais demandam um mosaico de soluções legislativas e inter-relacionadas que estabelecem diretrizes legais de regulamentação e um sistema de repsonsbailização por danos.

O primeiro arranjo legal que tem como objeto os dados, é a Lei de Acesso à Informação - Lei nº 12.527/2011 – a qual regula o acesso a informações previsto na Constituição Federal[1], no qual garante o direito fundamental de todos de receber dos órgãos públicos informações de seu interesse particular, coletivo ou geral, promovendo, assim, a participação do usuário na administração pública.

Essa lei, portanto, garante à todas as pessoas a consulta de informações públicas por meio de ações que corroboram com a transparência e a publicidade. Salienta-se que o dever de prestação de informações pelos órgãos públicos integrantes da administração diretae indireta não abarca aquelas cujo sigilo seja essencial para a segurança da sociedade e do Estado, bem como, dados que violam a intimidade.

Percebe-se, pois, que a legislação de acesso à informação não concebe os dados enquanto um bem no mercado de consumo, com alto valor econômico, até pelo contexto em que foi criada, em que começou a emergir os espaços públicos digitais. Assim, o foco dessa lei é para as organizações públicas, que até então, eram as principais coletoras de dados pessoais.

Já considerando a importância dos dados no stor econômico, foi criada a Lei do Cadastro Positivo – Lei 12.414, de 9 de junho de 2011 – que exerce uma função importante, tendo em vista às mudanças no mercado, em que as empresas, por meio dos instrumentos tecnológicos, valem-se de bancos de dados para conhecerem seus consumidores em potencial assim como o uso deliberado dos meios digitais como espaço de consumo. Assim, os dados dos consumidores ficam expostos em um ambiente não palpável e de manipulação, assim mecanismos de proteção desses dados fez-se e, ainda, faz-se, importante.

Nesse sentido, para fins de proteção dos dados desses consumidores, a mencionada lei prevê restrições quanto à seleção dos dados a serem disponibilizados, bem como da finalidade do uso destes dados. Desse modo, determina que para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado, ou seja,

[1] 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; (art. 5º)

não podem ser dados que ultrapassem a dimensão da análise de concessão de crédito, ficando então proibidos dados que não estiverem vinculadas à análise de risco de crédito ao consumidor ou que sejamsensíveis, ou seja, pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Desse modo, as informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para realização de análise de risco de crédito do cadastrado; ou subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente. Entretanto, a utilização dos dados, tem sido usado para além da análise de risco de crédito, ao contrário o contexto atual é expansão do Marketing orientado por dados (NASCIMENTO, 2019),que é marca do mercado de consumo, de modo que a sprimeiras manipulam milhares de dados, que ultrapassam apenas informações de cunho objetivo.

Posteriomente, ainda no tocante à proteção de dados, houve alteração relevante no Código Penal. Nesse sentido, um dos principais reflexos da evolução tecnológica no direito penal, foi a promulgação da Lei 12.737/2012, conhecida como "Lei Carolina Dieckman", que modificou o Código Penal ao incluir o artigo 154-A, que visa punir a publicização não autorizada de conteúdo íntimo, a partir da violação de dispositivos tecnológicos pessoais, além de alterar a redação de outros tipos para adaptá-los ao novo contexto tecnológico.

O referido delito consuma-se com a invasão não autorizada, de modo que basta que fique provada a intenção de obter, adulterar ou destruir informações, ainda que o objetivo não seja atingido pelo agente. Importante, também observar que caracteriza o crime a instalação, para obter vantagem ilícita, de vulnerabilidades no dispositivo alheio, como *spams*, vírus e programas "cavalo de tróia", possibilitando ou causando incidentes indesejados.

Ocorre, porém, que o código penal foca na proteção do sigilo e da confidencialidade, não determinando medidas específicas em relação à proteção de dados. Assim, embora a criação do art. 154-A do CP tenha sido um inegável avanço, a norma protege o titular do dispositivo invadido, sem estipular medidas preventivas.

O que deve ser o pressuposto para a criação de tipos penais voltados para a proteção de dados, é que não, necessariamente, os dados estarão armazenados em dispositivos dos titulares, mas podem estar alocados, por exemplo, em bancos de dados alheios, e ainda assim o titular terá direito sobre eles, uma vez que os dados são uma extensão da personalidade do titular. Desse modo, o próprio art. 154-A do CP se mostra ultrapassado ante a necessidade de uma tutela dos dados pessoais centrada na pessoa humana de seu titular, não na propriedade

de dispositivos.

Assim, tendo em vista a expansão do uso de espaços públicos digitais e as alterações do Código Penal não foi suficiente para estabelcer um sistema de responsbailização quanto aos danos causados pela manipulação de dados em meio virtual, foi necessária a criação de uma Lei mais ampla, que abarcasse todas as formas de manipulação de dados. Assim, foi publicado o Marco Civil da Internet - Lei nº 12.965/2014 -, o qual estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, além de determinar as diretrizes para a atuação dos entes federativos.

O Marco Civil da Internet foi elaborado com base em três pilares: a liberdade, a neutralidade e a privacidade, estabelecendo que o uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, à comunicação e à manifestação de pensamento que consiste na garantia de produção, acesso e compartilhamento de conteúdo na internet.

A aludida lei também expõe como princípio a preservação e a garantia da neutralidade de rede. A empresa detentora da tecnologia que provê a conexão deve fornecer o serviço de internet de forma isonômica, não promovendo diferenciações no tratamento de quaisquer pacotes de dados. Caso haja mitigação ou diferenciação do tráfego, as empresas devem expor tal fato aos usuários de forma clara e transparente, atuando de forma a evitar danos aos usuários. Atenta-se que é proibido bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados.

Quanto à privacidade, o Marco Civil da Internet garante a inviolabilidade da intimidade e da vida privada, além da confidencialidade dos dados e mensagens dos usuários, de modo que o acesso a essas informações somente poderá ser feito mediante ordem judicial. Ainda, a mencionada norma aponta para a necessidade de manutenção dos dados e não repasse dessesà terceiros, condicionando a realização tal ação por meio do consentimento livre, expresso e informado do usuário.

Ademais, a lei impõe a transparência de informações pelas empresas tecnológicas a seus usuários quanto ao uso, coleta, tratamento e manuseio dos dados pessoais, restringindo tais ações para finalidades legais pré-estabelecidas e que justifiquem a sua coleta. O consentimento no que se refere à coleta e processamento desses dados deve ser expressa. Caso haja estipulação contratual que afronte a inviolabilidade e ao sigilo das comunicações privadas em meio digital, tal cláusula será considerada nula. Percebe-se,pois, a supremacia do direito à intimidade e à vida privada, rechaçando qualquer ato que acarrete danos aos indivíduos

conectados.

Nesta perspectiva, a Lei nº 12.965/2014 dispõe expressamente como princípio a responsabilização do agente caso sua atividade acarrete ofensa. Logo, uma pessoa física ou jurídica pode ser punida caso promova alguma ação desrespeitosa a outrem e, sendo notificada do abuso pelas empresas digitais ou por uma determinação judicial, não remova o conteúdo.

Ocorre, porém, que apesar do avanço do marco civil da internet o seu foco está na utilização de dados pelos usuários da intenet, enquanto pessoas físicas, de modo que os dados seriam ativos das empresas digitais, ao passo que começou a emergir com força econômica, empresas especilizadas na formação e comercialização de bancos de dados pessoais. Desse modo, ante reformulação do mercado, calcucaldo em dados digitais, fez-s necessária a atualização normativa para aocmpanhar as novidades do mundo digital.

1.2 A Lei Geral de Proteção de dados no Brasil – LGPD (lei nº 13.709/2018)

Na esteira de valorização dos dados e subsequente necessidade de sua proteção e controle que foi sancionada a Lei Geral de Proteção de Dados, sob forma da Lei Federal nº 13.709/2018, inspirada na *General Data Protection Regulation* da União Europeia – GDPR.

A partir da vigência da legislação ocasionou profundas alterações na forma como os dados pessoais são tratados no Brasil. Para isso, estabeleceu-se regras detalhadas que regulam qualquer operação de tratamento de dados, realizada por pessoas físicas ou jurídicas, no setor público ou privado, com o objetivo de garantir maior controledos cidadãos sobre informações pessoais.

O mercado tratava os dados coletados como ativo próprio, que poderia ser livremente utilizado e comercializado por quem deles se apropriasse. Nesse sentido, Kotler, ainda, quando os dados começam a ter relevância social, ressaltou que “um ótimo banco de dados dos clientes é um bem de propriedade da empresa que pode dar a ela uma vantagem competitiva” (KOTLER, 2000, p. 671).

Agora a perspectiva é inversa: os dados coletados continuam a pertencer às pessoas às quais se referem, de modo que o coletor dos dados deve prestar contas de seu uso. As prerrogativas, direitos e princípios contidos na LGPD se reconduzem a essa ideia básica: dever de prestar contas, já que o agente de tratamento de dados lida com bens alheios e de extrema relevância.

O risco de lesão a direitos no tráfego de dados pessoais é uma realidade como

evidenciam as corriqueiras notícias de vazamento de informações pessoais sensíveis, assim, a LGPD (Lei 13.709/18) instituiu um regime de responsabilidade civil próprio para situações envolvendo lesões ocorridas no tratamento de dados pessoais. Porém, não se pode ignorar a coerência interna do sistema de responsabilidade civil.

Tendo isso em vista, a LGPD apresenta uma grande mudança no sistema de proteção de dados brasileiros, buscando a conciliação entre o interesse público e o incentivo ao desenvolvimento econômico e tecnológico de forma vinculada à circulação e uso de informações (GUIMARÃES, 2019). Em suma, a referida lei exige o consentimento explícito do usuário para coleta e uso de seus dados, além de permitir, obrigatoriamente, opções de visualização, correção e modificação das informações captadas.

Nessa perspectiva, é relevante destacar que, não obstante ao reconhecimento da existência prévia de normas que já contemplavam o tema no ordenamento jurídico brasileiro, a LGPD se diferencia sobretudo, no que se refere à sua abrangência. Dessa maneira, a norma possui a proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da liberdade da pessoa natural como verdadeira premissa orientadora da interpretação de todos os seus preceitos. Esse princípio, traduzido como garantia da privacidade de dados da pessoa natural e seu direito de instrumentalizá-los como seu, encontra fundamento na Constituição Federal[2], que reconhece, como direito fundamental o direito inviolável à intimidade, à vida privada e a honra dos indivíduos.

Na esteira da regulamentação européia, a LGPD enuncia diversos fundamentos e princípios, atribuindo ao titular a utilização de instrumentos para garantir o controle de seus dados a respeito do uso por terceiros. Tendo isso em vista, muito mais do que apenas impedir o acesso indesejado a informações pessoais, a lei preocupa-se também com o aspecto dinâmico da proteção dos dados, ao definir um extenso rol de direitos atribuídos ao titular, cujo objetivo central consiste em concretizar sua participação ativa na gestão dos dados.

No que se refere aos seus fundamentos, a legislação determina o respeito à privacidade, ao assegurar os direitos fundamentais da inviolabilidade da intimidade, da honra, da imagem e da vida privada; à autodeterminação informativa, ao expressar o direito do cidadão em relação ao controle, e, consequentemente; à proteção de seus dados pessoais, bem como o respeito à liberdade de expressão, de informação, de comunicação e de opinião, conforme disposição constitucional, assim como o desenvolvimento econômico e

[2] X - - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (art. 5º)

tecnológico e a inovação, a partir da criação de um cenário de segurança jurídica, que privilegia a livre iniciativa, a livre concorrência e a defesa do consumidor, por meio do estabelecimento de regras mais claras e válidas para o setor privado. Por fim, determina o respeito aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas.

Esses fundamentos se refletem nos princípios que regem o tratamento dos dados pessoais, que, por sua vez, constituem-se de: **finalidade**, com a realização do tratamento para propósitos legítimos e explícitos; **adequação**, por meio da compatibilidade do tratamento com a finalidade informada ao titular; **necessidade**, através da limitação do tratamento mínimo necessário, proporcionais e não excessivo em relação às finalidades de tratamento dos dados; **livre acesso**, com a garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento dos dados; **qualidade dos dados**, por meio da garantia de exatidão e clareza acerca da atualização dos dados; **transparência**, por meio da garantia de acesso à informação em linguagem de fácil compreensão; **segurança**, com a utilização de medidas técnicas e administrativas para a proteção dos dados; **prevenção**, por meio da adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; **não discriminação**, por meio do impedimento de realização de tratamento de dados para fins discriminatórios e ilícitos e, por último, a **responsabilização e prestação de contas**, por meio da 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.

Inicialmente, há que se destacar a abrangência incumbida à LGPD. A norma determina que toda operação de tratamento de dados, independente do meio e do país de sua sede, ou país onde os dados estiverem localizados. Não obstante, a regra se aplica desde que: a operação tenha sido realizada no Brasil; o tratamento de dados tenha por objetivo oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil; ou os dados pessoais tenham sido coletados no território nacional.

A LGPD estabelece três partes envolvidas nas operações de tratamento, sendo elas o titular dos dados, o controlador de dados e o operador de dados. O "titular dos dados" é a pessoa natural, a pessoa física, identificada ou identificável, a quem os dados se referem. O termo "controlador de dados" é atribuído à pessoa natural ou jurídica, de direito público ou privado, a quem pertencem as decisões referentes ao tratamento dos dados. A pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados em nome do

controlador é, por sua vez, denominada “operador de dados”. Dessa maneira, a LGPD estabelece que o operador deve realizar o tratamento de dados seguindo as instruções fornecidas pelo controlador, que é o responsável pela verificação do cumprimento das próprias instruções e das normas.

Outra questão relevante apresentada pela Lei refere-se aos tipos de dados por ela abrangidos. Desse modo, tem-se na legislação duas “categorias” de dados, sendo elas: os dados pessoais, enquanto informações relacionadas ao titular, podendo incluir nome, endereço, e-mail, idade, estado civil e situação patrimonial, obtido em qualquer tipo de suporte (papel, eletrônico, informático, som e imagem, etc.), e os dados sensíveis, como os dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos, etc. O tratamento desta categoria de dados é abordado com maior rigor pela LGPD, sendo vedado o seu tratamento.

Conforme visto anteriormente, a aplicação da LGPD contempla toda operação realizada com dados pessoais. Não obstante, existem casos em que a Lei excetua certos tipos de tratamento de dados, tais como os realizados por pessoas físicas para fins exclusivamente particulares e não econômicos e, no caso de pessoas jurídicas, os tratamentos realizados para fins exclusivamente artísticos, jornalísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais. Além disso, excetua-se a aplicação da Lei nas hipóteses em que os dados estejam apenas de forma temporária no Brasil, ou seja, os dados provenientes de fora do território nacional e que não seja objeto de uso ou comunicação com agentes de tratamento brasileiro ou objeto de transferência internacional de dados com outros países.

Nesse cenário, a LGPD estabelece as situações em que os agentes de tratamento podem tratar dados, sendo a principal delas aquela realizada com o consentimento do titular. Entretanto, existem outras possibilidades determinadas pela Lei que permitem o tratamento e uso dos dados mesmo quando não há consentimento do titular, sendo elas: para cumprir obrigação legal do controlador do tratamento, para tratamento e uso compartilhado para a execução de políticas públicas, para a realização de estudos por órgão de pesquisa, para a proteção da vida do titular ou de terceiro, para a tutela da saúde, para a execução de um contrato com o titular, para pleitos em processos judiciais, administrativos ou arbitrais, para interesses legítimos do controlador e para a proteção de crédito.

Não se pode deixar de mencionar o papel central que o consentimento assume na lógica da LGPD. Nos termos da Lei, o consentimento deve ser obtido para finalidades específicas, não podendo ser genérico. Além disso, ele pode ser revogado a qualquer

momento, mediante manifestação expressa do titular, através de procedimentos facilitados e gratuitos. Além disso, destaca-se que o ônus da prova de consentimento é de responsabilidade do controlador de dados, sendo dispensado somente quando os dados forem manifestados publicamente pelo titular. Como já se espera, quando é possibilitada a contratação sem fornecimento de dados pessoais, o titular deve ser informado das consequências de não autorização do uso de seus dados, tais como restrições nos serviços oferecidos ou exibição de publicidade.

Outra grande inovação inaugurada pela LGPD versa sobre as penalidades e responsabilizações em caso de descumprimento de suas determinações, que dispõe que aquele que não cumprir a Lei fica sujeito à penalidades administrativas que vão desde multa até porcentagens de faturamento da empresa, sendo limitada a cobrança de até R$50 milhões por ano, além de publicização da infração, bloqueio e eliminação dos dados. Além disso, o controlador que causar dano patrimonial, individual ou coletivo fica sujeito a inversão do ônus da prova a favor do titular dos dados e a solidariedade com o operador, quando estiver diretamente envolvido no tratamento ilegal. Para se eximir das responsabilidades, eles devem provar que não realizaram o tratamento indevido dos dados, não houve violação à legislação, ainda que tenha ocorrido o tratamento dos dados, ou que o dano foi ocasionado por culpa exclusiva de terceiros.

A partir dessas disposições, discute-se, se a Lei contempla uma resposnabilidade objetiva ou subjetiva do controlador e operador de dados. O mencionada lei contém uma cláusula geral de responsabilidade, imputando a obrigação de indenizar ao controlador ou operador que, descumprindo a legislação de proteção de dados, causar dano patrimonial ou extrapatrimonial aos titulares dos dados pessoais violados e de forma similar ao regime implantado pelo Código de Defesa do Consumidor, a LGPD estabeleceu a solidariedade dos agentes que causaram a lesão e, para mitigar a assimetria na relação entre controladores, operadores e titulares de dados pessoais, permitiu a inversão do ônus da prova por critério judicial, o que, a rigor cientifico, implica um sistema de presunção legal do dano sofrido pela vítima lesada.

NOVAKOSK e NASPOLINI (2020) concluem, em que pese as discussões doutrinárias, que a LGPD contempla uma responsabilidade objetiva, o que, de fato, é mais compatível partindo de uma análise teleológica da Lei, uma vez que a teoria da culpa, sobretudo relacionado à violação das normas d etratamento dos dados, dificulta o acesso da vítima à justiça e a afasta da reparação do dano, esvaziando, assim, o conteúdo normativo, e a finalidade a que a norma propõe que é conceber os dados, enquanto um direito fundamental.

Nesse sentido, deve-se, ainda, observar o disposto na Convenção Interamericana de Direitos Humanos, segundo o qual, a interpretação das regras jurídicas envolvendo direitos humanos deve priorizar a norma mais favorável à pessoa humana, sendo, portanto, a responsabilidade objetiva mais adequada ao contexto da LGPD.

Ademais, deve-se compreender que a LGPD dispõe de obrigações de resultado, as quais só podem ser afastadas se houver a ruptura do nexo causal (NOVAKOSK e NASPOLINI, 2020, p.15), o que evidencia a adoção da sistemática da repsonsabilidade civil objetiva.

Ultrapassando a concepção da repsonsabilidade civil objetiva, Maria Celina Bodin de Moraes (MORAES, 2019, p. 5), trata da chamada responsabilidade proativa aplicada à LGPD, calcada em um sistema de prestação de contas, de modo que a Lei não dispõe apenas da reparação do dano, em caso de violação aos seus preceitos, mas para além, estabelece um sistema que impõe a prevenção de forma eficaz dessas violações.

Ante a essa sistemática de responsabilização, a LGPD determina a possibilidade de atenuação de punições à empresa que demonstre que implementou um programa de governança em privacidade, baseado em boas práticas de segurança da informação, como forma de garantir que irão atender às diretrizes da LGPD, minimizando riscos de eventuais irregularidades, o que evidencia a sistemática da responsbailização proativa. Dessa forma, a atenuação de punições é um incentivo para que as empresas implementem programas de compliance.

2. O COMPLIANCE NO ÂMBITO DA PROTEÇÃO DE DADOS

Diante dessa inovação legislativa e a consolidação de um novo paradigma quanto aos dados pessoais, que reflete em um novo marco regulatório, as empresa, em especial as que atuam no mercado de consumo, devem se adaptar às novas regras que ensejam uma responsabilidade civil específica. As empresas, portanto, devem pautar sua atuação em observância à Lei Geral de Proteção de Dados, sobretudo, em um contexto, em que se sobressai o mercado digital, cuja atuação se pauta nas informações expressas nos dados coletados de usuários do meio virtual.

Ademais, dentro desse contexto de proteção de dados, tem-se, ainda, a noção contemporânea de que a empresa é um ente político (WOOT, 2013), cujo paradigma causa impacto significativo quando às obrigações impostos à pessoa jurídica, de modo que além de

estar submetida à Lei, a empresa tem como finalidade a proteção do interesse público. Isto significa que se deve reconehcer que todas as atividades da empresa não importa apenas à ela e ao seus sócios, mas tem impacto, sobretudo, em toda a sociedade.

É, portanto, nesse contexto que se reforça a importância do compliance, no sentido de auxiliar os agentes econômicos a se manterem em conformidade com a Lei, mediante a fixação de controles internos, cujo objetivo é garantir o exer cicio de sua atividade pautada na ética e se prevenir contra a aplicação de sanções pelo Estado, ante, a ampliação de seu papel sancionador no atual contexto econômico, sobretudo, para a proteção dos agentes econômicos mais vulneráveis.

Nesse sentido, segundo a autora Ana Frazão, o compliance se refere "ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade"(FRAZÃO, 2007, 42).

Vale ressaltar que cumprir a Lei é uma obrigação de todos os sujeitos jurídicos, entretanto a noção de compliance é inovadora, na medida em que coloca essa obrigação como um problema para a empresa, de modo que para a sua solução *"é necessário repensar a forma como a entidade é organizada*"[3] (SANCLEMENTE-ARCINIEGAS, 2021, pg.05) , além de conceber a empresa enquanto um ente político a serviço da proteção do ser humano.

Portanto, o compliance implica na reorganização da empresa, a partir de *"funções básicas de administração: controle e supervisão*[4]" (SANCLEMENTE-ARCINIEGAS, 2021), para que a conduta da empresa esteja em conformidade com o ordenamento jurídico, sobretudo com vistas à proteção dos direitos fundamentais da pessoa humana, a fim de evitar prejuízos pelo exercício do papel sancionador do Estado.

Nesse sentido, aplicado à LGPD, que consolidou o paradigma de que a titularidade dos dados é da pessoa natural a eles referente, e que garante direitos para o controle do titular sobre as suas informações, implementar programas de compliance se faz importante para garantir boas práticas no tratamento de dados pessoais, como forma de prevenir violações à esses direitos e, por conseguinte, sanções de cunho cível, administrativo e penal, que oneram a atividade econômica.

Tem-se, portanto, que o compliance é um instrumento de autorregulação, voltado à elaboração de documentos corporativos, cuja natureza é de Código de Conduta, a fim de manter o cumprimento dos ditames legais, mas que, no âmbito da LGPD está vinculado à atividade

[3] *es necessário repensar la forma en la que la entidad se organiza*
[4] *funciones básicas de la administración: el control y la supervisión*

reguladora do Estado, que estabelece diretrizes mínimas que devem ser observados quando da implementação dos programas de compliance, conforme enumera o seu art. 50, caput, segundo o qual o operador deve estabelecer, enquanto requisitos mínimos, condições de organização do regime de funcionamento, dos procedimentos (inclusive de reclamações e petições de titulares), das normas de segurança, dos padrões técnicos, das obrigações específicas para todos os envolvidos, das ações educativas a serem empreendidas, dos mecanismos de supervisão e de mitigação de risco.

Assim, no âmbito da LGPD discute-se a existência do gênero da corregulação (FRAZÃO, 2017, pg.684), uma vez que os programas de compliance atuam como normas complementares à Lei, havendo, assim, nesta seara, a atuação complementar entre a iniciativa privada e o Estado, principalmente, porque a LGPD estabelece normas com conceitos abertos, que necessitam de cada agente econômico para dar concretude aos comandos legais, de forma a adaptá-las à sua realidade, o que se faz a partir da atividade de regulamentação corporativa, sobretudo pelos programas de compliance.

Pode-se, portanto, concluir, que o progrma de compliance visa a adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD, além das vantagens tradicionalmente atribuídas a esse programa, as quais sejam:

> (i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas (IDEM, pg. 668)

Assim, cabe à corporação especificar, de acordo com o seu contexto econômico, detalhadamente os procedimentos a serem adotados pela pessoa jurídica no tratamento de dados, de modo que o compliance tonar-se um instrumento essencial para adequar as atividades da empresa, de forma eficaz, às diretrizes da LGPD, auxiliando no uso de dados, tão importante para a atuação no mercado de rede, com segurança, de forma a evitar incidentes que impliquem em responsabilização empresarial e, sobretudo, que implique em danos à sociedade.

Percebe-se, pois, que a LGPD compreende a empresa enquanto um agente político, colocando-a como a principal responsável pela concretização do direito à proteção dos dados pessoais, alterando o paradigma de que os dados seriam de titularidade da empresa, e, portanto, poderiam ser manipulados à seu critério, enquanto um bem de expressão puramente

economica, para o paradima atual de que os dados são objeto de proteção social, sendo de titularidade da pessoa em relação à qual os dados dizem repseito, e, portanto, sendo extensão de sua personalidade.

Assim, a fim de proteger os titulares desdes dados, a LGPD estabelece um mosaico de responsbailização civil das empresas que desrespeitarem suas disposições, com a imposição de penalidades, conforme já exposto, tendo em vista que esses dados carregam informações sensíveis de seus titulares, cuja manipulação, traz benefícios econômicos às empresas, mas podem tarzer prejuízos aos seus titulares se houver incidentes.

Nesse sentido, é essencial que as empresas valham do compliance de dados a fim de fazer uma análise de risco, especialmente, quanto às características dos dados tratados, a forma como são coletados, utilizados, armazenados e como são destinados, justamente, para evitar tais incidentes que possam causar prejuízos de ordem moral e material aos seus titulares.

Para dar efetividade a essa análise de risco, bem como ao código de conduta e a todo o programa de compliance, deve-se implementar mecanismos de detecção, apuração e punição de condutas contrárias ao programa, uma vez que o grau de comprometimento da empresa com o cumpriemnto da Lei e de suas normas, não é medido só pelas regras e mecanismos de controle, mas pela reação rápida e adequado na identificação e repressão de ilícitos.

Por esta perpsectiva, tem-se que a detecção, apuração e punição de condutas devem-se pautar tanto no âmbito interno da corporação, em relação aos seus funcionários e alto comando, quanto na relação da empresa com os titulares dos dados tratados por ela, caso haja, para estes algum prejuízo.

Nesse sentido, quanto à apuração e detecção de ilícitos, um dos mecanismos importantes para implementação são “Canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes” (FRAZÃO, 2017, p.692), os quais permitem, por um lado, que os funcionários possam solicitar esclarecimentos para cumprir o programa de compliance adequadamente, e por outro, permitem que a empresa tenha conhecimento de atos ilícitos e possa adotar medidas necessárias para punir tais atos e prevenir condutas semelhantes.

Ao apurar e detectar atos contrários à LGPD e às normas internas da corporação, cabe à empresa aplicar penalidades, seja ao funcionário infrator, seja a ela própria, assumindo os erros cometidos para com o titular dos dados, por meio de procedimentos que seja ingualitário aos envolvidos.

Também se faz importante o monitoramento dos controles internos, como forma de auxiliar na análise de efetividade do programa, auxiliando, assim, eventual atualização. O

objeto deste monitorament é se há o cumprimento do programa de compliance por seus destnatários, bem como a se há profícua reação às violações legais e quais pontos carecem de ser reforçados, identificando, assim, as violações que persistem.

A partir destes processos essenciais à implementação do programa de compliance de dados, que diz respeito à apuração, detecção, punição e monitoramento, tem-se que a implementação da mediação privada, no âmbito da corporação, é um mecanismo eficaz para a eficácia destes processos, tanto no âmbito interno, quanto às infrações cometidas por funcionários e pelo alto comando, tanto no âmbito externo, quando a violação de normas que causam danos aos titulares de dados. á que a instituição demonstra transparência, credibilidade e abertura ao diálogo em casos de problemas de relacionamento no decurso do tempo.

3. A MEDIAÇÃO ENQUANTO INSTRUMENTO DE COMPLIANCE NO ÂMBITO DA LGPD

Os meios alternativos de resolução de litígios são institutos jurídicos, que surgiram a partir da introdução dos métodos autocompositivos pelas legislações processuais, ante o monopólio estatal da Jurisdição, que consiste na exclusividade de o Estado fazer cumprir o direito, (LEAL, p.44, 2017) de modo que, havendo um conflito, as partes podem utilizar, no âmbito desses institutos jurídicos, as formas antigas de autocomposição *renúncia, submissão, desistência e transação*[5].

Esses métodos, além de simplificarem e agilizarem a solução de problemas, aproximam os cidadãos ente si e, por isso, tem ganhado destaque na atualidade, de modo que os ordenamentos jurídicos tem privilegiado a forma de tribunais multiportas, tal como proposto por Frank Sander, (JOHSON, 2012), segundo o qual, diferentes meios de solução de conflitos, são aplicáceis a cada caso, a depender das particularidades, se restringindo apenas à jurisdição.

O resgate às formas primitivas de resolução de conflitos se deu como resposta à morosidade e a falta de efetividade da atividade jurisdicional, que ensejou, já, na década de 70 nos Estados Unidos, o movimento denominado *Alternative Dispute Resolution*, na tentativa de encontrar soluções à crise do Judiciário.

[5] A renúncia consistia em se tornar silente o prejudicado ante o fato agressor a si mesmo ou a seu patrimônio. Submissão era a aceitação resignada das condições impostas nos conflitos ou pugnas individuais ou sociais. A desistência era o abandono da oposição já oferecida à lesão de um direito ou o não exercício de um direito já iniciado. A transação distinguia-se pela troca equilibrada de interesses na solução dos conflitos (LEAL, 2017, p.44).

Percebe-se que houve um movimento, em expansão, de transferência do poder de solução dos conflitos particulares ao Estado, de modo que, mesmo questões de baixa complexidade, que poderiam ser resolvidas em âmbito privado, são levadas ao crivo do Estado-Juiz. Nesse sentido, os métodos alternativos se colocam como instrumento de pacificação social, de disseminação de uma cultura do diálogo, devolvendo, aos próprios envolvidos no conflito, o poder de encontrarem a melhor solução possível.

Nesse sentido, tem-se que a desjudicialização e a implementação da autocomposição pelas partes é uma realidade, pois visa:

> Resolver os problemas estruturais da justiça, mas, acima de tudo, como meio de se atingir uma satisfação mais plena por parte dos envolvidos nos conflitos, destacando-se, neste último caso, os benefícios da mediação na pacificação social, já que esta técnica se aprofunda nas razões emocionais que cercam as relações conflituosas, trazendo mais legitimidade aos ajustes e mais chance de acabar em definitivo com o dilema estabelecido. (CABRAL, 2017, p. 369)

Da perspectiva empresarial, considerando os agentes econômicos, sobretudo no mercado de consumo, tem-se que a atividade jurisdicional, sobretudo nesse contexto de sobrecarga, gera altas despesas às partes, tanto empresas, quanto clientes, além de o tempo dos processos não acompanharem o tempo dos negócios, que são, em grande medidas, mais céleres, gerando, assim, soluções não compatíveis com a realidade, pelas mudanças de condições ocasionadas pelo lapso temporal.

É nesse cenário que a mediação, enquanto um método alternativo de resolução de litígios se coloca como um procedimento eficaz, que privilegia o diálogo e a construção conjunta da solução, a partir de um procedimento simplificado, o qual segue uma tendência liberal, ante a dificuldade do formalismo judicial.

A Mediação "constitui-se, historicamente, na manifestação de transigência entre particulares, para encontrar a solução de seus conflitos, sem intervenção do Estado, pela indicação consensual de um ou vários intermediários que lhes pacifiquem os interesses" (LEAL, 2017, p. 41).

Apesar de a Mediação, enquanto método alternativo de resolução de litígios, ter sido introduzido nos ordenamento jurídicos e utilizado, amplamente, pelos tribunais, é essencialmente, uma forma privada de resolução de litigios. Nesse sentido, a Lei de Mediação[6], trata da mediação privada ou, denominada, extrajudicial, a qual pode ser realizada por profissional escolhido pelas partes, independentemente de vínculo com o Judiciário.

[6] Lei nº 13.140, de 26 de Junho de 2015

Alinhado a esta legislação, a LGPD dispõe a respeito de vazamento de dados poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação de penalidades. Há, portanto, disposição expressa, em Lei, autorizando métodos de transação em conflitos relacionados ao tratamento de dados.

Depreende-se desta disposição legal que, ainda que a proteção aos dados seja um direito fundamental do seu titular, este é um direito indisponível que admite transação, conforme legislação específica.

Assim, havendo a possibilidade de conflitos, em decorrência da atividade empresarial, sobretudo quanto ao tratamento de dados, tem-se que são muitas as vantagens de se utilizar a mediação, eis que facilita o diálogo, é um procedimento célere, econômico e simplificado, confidencial e flexível, o que traz mais segurança às empresas para tratar de conflitos relativos à LGPD, principalmente, porque estão sujeitas ao controle estatal e à imposição de severas penalidades se descumprirem as disposições desta lei.

Ademais, tem-se que, tão importante quanto se adequar à legislação, é a utilização do compliance no gerenciamento de conflitos, como formar de salvaguardar direitos, no caso, os de proteção de dados, bem como, de ter acesso ao caso concreto e possibilitar um programa de integridade constantemente atualizado e eficaz.

Assim, a mediação extrajudicial, a ser adotada pelas companhias, é uma forma de gerenciamento de conflitos no âmbito do compliance, que permite cumprir a etapa de monitoramento, tão importante ao programa, pois mais que cumprir as normas e a legislação, deve a empresa identificar os conflitos gerados, de fato, por sua atividade e como ela impacta a realidade. Nesse sentido, faz-se imprescindível, identificar os focos dos conflitos gerados, e essas informações é obtida de forma primordial, a aprtir do procedimento de mediação.

Isto porque a mediação permite o conhecimento profundo do conflito, reconhecendo suas causas e consequências, para a construção de soluções criativas, pautadas no diálogo e no vínculo de confiança entre as partes. Esta é, portanto, uma técnica de resolução de conflitos interessante, principalmente, se considerarmos que as relações com clientes são duradouras, e tratar conflitos com eficácia é de suma importância, para manter esse vínculo, especialmente, em situação relacionadas às questões sensíveis à pessoa, como os dados.

Internamente, a utilização da mediação também é interesante, pois gera, em caso de descumprimento do programa de compliance, no âmbito da empresa, um relação mais harmônica entre sócios, funcionários e acionistas, em detrimento de punições pautadas em arbitrariedades, que podem inclusive gerar longos processos judiciais para a resolução, além

de construir um ambiente de diálogo e de confiança no âmbito da empresa.

Por ser um método de procedimento flexível, é possível às empresas, adaptá-lo ao mercado altamente digitalizado, em que as atividades empresas são pautadas, principalmente, em ambientes digitais, como forma inclusive de redução de custos, tempo e dinheiro. Assim, tem sido cada vez mais comum a utilização de Plataformas de mediação online, para tratar de conflitos relacionados à LGPD, como forma de expansão da mediação privada.

A mediação por meio online promove uma maior aproximação entre empresas e titulares de dados, principalmente, em um meio de atuação empresarial que extrapola os limites territoriais, sendo, portanto, um meio que possibilita o efetivo diálogo entre as partes, sem que haja custos desproporcioanis para a solução.

Esse esforço para implementar procedimentos de gerenciamento de conflitos, demonstra a tentativa de promover meios de efetivar os programas de compliance, pois busca o cumprimento das diretrizes internas, e, por consequência, da legislação, de forma ética e transparente.

Tem-se, pois, que a Mediação é um instrumento importante no âmbito de um programa de compliance, pois além de produzir efeitos de forma rápida e eficiente, permite conhecer as causas e consequência dos conflitos, possibilitando, assim, prevení-los e mapear os erros cometidos e, de modo que permite atualizar o programa de compliance para prevenir novos conflitos, sendo, pois, uma ferramenta importante de controle do programa:

> Mediação e compliance se completam e devem, sempre, interagir dentro dos processos de gestão, na medida que os responsáveis pela elaboração das normas de conduta devem estabelecer regras com o objetivo de evitar os conflitos e podem aprender, na mediação, de que forma evitá-los. A comunicação entre os responsáveis pelo compliance e a gestão de conflitos deve ser essencial para a eficiência de um departamento jurídico de uma empresa. 29 (PENNA, 2017, p. 18).

Nesse sentido, considerando a importância de desenvolver programas de integridade no âmbito da LGPD, a fim de garantir maior credibilidade, a mediação garante um sistema de compliance que gera resultados eficientes, que promove um processo integrado de resolução de conflitos, mas também de prevenção, bem como facilita o ambiente de negócios, melhora as relações humanas no interior das empresas, colabora para menos gastos, menos desgastes, menos exposições. Além de aproximar as empresas dos titulares de dados por elas manipulados, através do diálogo, formando assim uma imagem pautada na confiabilidade, gerando mais valor à empresa no mercado de consumo.

4. CONSIDERAÇÕES FINAIS

O direito à proteção de dados pessoais, enquanto um direito fundamental, que se manifesta como uma expressão dos Direitos da Personalidade, vem sendo garantido na legislação brasileira a partir de um mosaico de leis que visam um acesso seguro aos dispositivos de tecnologias que retêm os dados de seus usuários. Nesse sentido, pode-se concluir que a legislação brasileira vem se adaptando à Quarta Revolução Industrial, com a criação de diversos mecanismosde proteção nas searas administrativa e civil.

Assim, a criação da LGPD – Lei Geral de Proteção de Dados se fez necessária na medida em que garantiu mais transparência à maneira como os dados pessoais dos usuários, em especial, digitais, são tratados, coletados e armazenados por empresas públicas e privadas, além de expandir a proteção a todo o universo de dados, e não só àqueles relativos ao crédito, como se propôs, inicialmente, a Lei do Cadastro Positivo. Ressalta-se, ainda, o avanço na criação de um parâmetro de responsabilidade civil na manipulação indevida desses dados, com a previsão de sanção no âmbito administrativo.

Desse modo, fica evidente a necessidade de as empresas se adequarem ao novo paradigma imposto pela legislação, o que pode ser feito com mais efetividade com a implementação de programas de compliance, principalmente, incluindo nele procedimento de controle de riscos, pautados na mediação, que garantirá a efetiva resolução de conflitos, com menos danos possíveis à empresa, ao mesmo tempo em que possibilita mapear os erros e prevenir novos conflitos e violações à Lei.

Neste sentido, como resposta a hipótese testada a Mediação constitui um importante instrumento de resolução de conflitos no âmbito das compliances, como forma autocompositiva que privilegia o diálogo entre as partes envolvidas no descumprimento das determinaçãoes de proteção de dados instituídas pela LGDP, visto que estabeleceu um equilíbrio entre interesses sociais e econômicos, ao tutelar a proteção dos dados pessoais, com a observância da dignidade da pessoa humana, da privacidade, da honra e da imagem das pessoas, mas, ao mesmo tempo, ao reconhecer o valor econômico dos dados, respeitando a livre iniciativa e o uso desses dados de forma legítima, responsável e razoável.

REFERÊNCIAS

BRASIL. Código Penal. Decreto-lei nº 2.848 de 07 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em: 31ago2021

BRASIL. Constituição da República Federativa do Brasil, 05 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 31ago2021

BRASIL. Lei 12.527 de 18 de novembro de 2011 . Lei de Acesso à informação. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 31ago2021

BRASIL. Lei 12.965 de 23 de abril de 2014. Lei do Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 31ago2021

BRASIL. Lei Federal nº 13.140, de 26 de junho de 2015. Lei de Mediação. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13140.htm> Acesso em: 18 set 2021.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm> Acesso em: 18set 2021.

FRAZÃO, Ana.; OLIVA, Milena Donato. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. Thomson Reuters Brasil, 2019.

____ FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42.

LEAL, Rosemiro Pereira. Teoria geral do processo: primeiros estudos. – 14. ed. - Belo Horizonte : Fórum, 2018.

MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito ―proativo‖. Revista Civilistica, ano 8, n. 3, Rio de Janeiro, 2019. Disponível em: http://civilistica.com/lgpd-um-novo-regime/. Acesso: 27 ago 2021.

NOVAKOSKI, André Luis Mota e NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade Civil Na Lgpd: Problemas e Soluções. 2019. Disponível em: https://www.indexlaw.org/index.php/conpedireview/article/view/7024

PENNA, Saulo Versiani. Mediação, arbitragem e compliance: prevenir, gerir e resolver conflitos de forma eficiente. CBMAE. Ano 12, n. 57, p. 18, abr/jul. 2017.

SANCLEMENTE-ARCINIEGAS, Javier. Revista Escuela de Administración de Negocios N° 90, enero a junio de 2021, ISSN: 0120, 8160 (Impreso)-ISSN: 2590-521X (En línea). Disponível em: https://journal.universidadean.edu.co/index.php/Revista/article/view/2975/2223. Acesso em: 20 de Setembro de 2021.

SANTOS, Dhiulia de Oliveira. A validade do consentimento do usuário à luz da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018). UniCEUB: Brasília, 2019.